



Cloud Backup 설명서

Cloud Backup

NetApp
June 20, 2022

목차

Cloud Backup 설명서	1
클라우드 백업의 새로운 기능	2
2022년 6월 14일	2
2022년 6월 8일	2
2022년 5월 2일	3
2022년 4월 4일	3
2022년 3월 3일	4
2022년 2월 14일	4
2022년 1월 2일	5
2021년 11월 28일	5
2021년 11월 5일	5
2021년 10월 4일	6
2021년 9월 2일	6
2021년 8월 1일	6
2021년 7월 7일	7
2021년 6월 7일	7
2021년 5월 5일	7
시작하십시오	9
Cloud Backup에 대해 자세히 알아보십시오	9
Cloud Backup에 대한 라이선스 설정	11
ONTAP 데이터를 백업 및 복원합니다	17
클라우드 백업을 사용하여 ONTAP 클러스터 데이터를 보호합니다	17
Cloud Volumes ONTAP 데이터를 Amazon S3에 백업	23
Azure Blob 저장소에 Cloud Volumes ONTAP 데이터 백업	30
Cloud Volumes ONTAP 데이터를 Google 클라우드 스토리지에 백업	36
사내 ONTAP 데이터를 Amazon S3에 백업	42
온프레미스 ONTAP 데이터를 Azure Blob 저장소에 백업	53
사내 ONTAP 데이터를 Google 클라우드 스토리지로 백업	62
사내 ONTAP 데이터를 StorageGRID에 백업	70
ONTAP 시스템의 백업 관리	76
백업 파일에서 ONTAP 데이터를 복원하는 중입니다	91
Kubernetes 데이터 백업 및 복원	108
Cloud Backup을 사용하여 Kubernetes 클러스터 데이터를 보호합니다	108
Kubernetes 영구 볼륨 데이터를 Amazon S3에 백업	111
Kubernetes 영구 볼륨 데이터를 Azure Blob 스토리지에 백업	117
Kubernetes 영구 볼륨 데이터를 Google Cloud 스토리지에 백업	122
Kubernetes 시스템 백업 관리	127
백업 파일에서 Kubernetes 데이터를 복원하는 중입니다	138
사내 애플리케이션 데이터를 백업 및 복원합니다	140

온프레미스 애플리케이션 데이터를 보호합니다	140
사내 애플리케이션 데이터를 클라우드에 백업	141
애플리케이션 보호 관리	144
애플리케이션 데이터를 복원합니다	147
가상 머신 데이터 백업 및 복원	150
가상 시스템 데이터 보호	150
데이터 저장소를 클라우드에 백업합니다	152
가상 시스템 보호 관리	153
클라우드에서 가상 머신을 복구합니다	155
클라우드 백업 API	156
시작하기	156
API 사용 예	158
API 참조입니다	161
참조하십시오	162
AWS S3 아카이브 스토리지 클래스 및 복원 검색 시간	162
Azure 아카이브 계층 및 복원 검색 시간	163
지식 및 지원	165
지원을 위해 등록하십시오	165
도움을 받으십시오	166
법적 고지	168
저작권	168
상표	168
특허	168
개인 정보 보호 정책	168
오픈 소스	168

Cloud Backup 설명서

클라우드 백업의 새로운 기능

Cloud Backup의 새로운 기능에 대해 알아보십시오.

2022년 6월 14일

인터넷에 연결되지 않은 사이트에서 사내 **ONTAP** 클러스터 데이터를 백업하는 데 지원이 추가되었습니다

사내 ONTAP 클러스터가 인터넷 액세스가 연결되지 않은 사이트에 있는 경우, 다크 사이트 또는 오프라인 사이트라고도 합니다. 이제 Cloud Backup을 사용하여 볼륨 데이터를 동일한 사이트에 있는 NetApp StorageGRID 시스템에 백업할 수 있습니다. 이 기능을 사용하려면 Cloud Manager Connector(버전 3.9.19 이상)도 오프라인 사이트에 배포해야 합니다.

"[오프라인 사이트에 커넥터를 설치하는 방법을 알아봅니다](https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html)". <https://docs.netapp.com/us-en/cloud-manager-backup-restore/task-backup-onprem-private-cloud.html>["오프라인 사이트에서 ONTAP 데이터를 StorageGRID에 백업하는 방법을 알아봅니다"].

2022년 6월 8일

Cloud Backup for Virtual Machines 1.1.0이 현재 **GA**로 제공됩니다

SnapCenter Plug-in for VMware vSphere를 Cloud Manager와 통합하면 가상 머신의 데이터를 보호할 수 있습니다. 데이터 저장소를 클라우드에 백업하고 VMware vSphere용 사내 SnapCenter 플러그인으로 가상 머신을 간편하게 복원할 수 있습니다.

"[가상 시스템을 클라우드로 보호하는 방법에 대해 자세히 알아보십시오](#)".

ONTAP 찾아보기 및 복원 기능에는 클라우드 복원 인스턴스가 필요하지 않습니다

S3 및 Blob 스토리지에서 파일 레벨 찾아보기 및 복원 작업에 사용되는 별도의 클라우드 복원 인스턴스/가상 머신. 이 인스턴스는 사용하지 않을 때 종료되지만 파일을 복원할 때 약간의 시간과 비용이 추가되었습니다. 이 기능은 필요 시 Connector에 배포되는 무료 컨테이너로 대체되었습니다. 다음과 같은 이점을 제공합니다.

- 파일 레벨 복구 작업에 대한 추가 비용 없음
- 파일 레벨 복구 작업 속도 향상
- Connector가 사내에 설치된 경우 클라우드에서 파일에 대한 찾아보기 및 복원 작업 지원

이전에 클라우드 복원 인스턴스/VM을 사용한 경우 자동으로 제거됩니다. Cloud Backup 프로세스는 모든 이전 Cloud Restore 인스턴스를 삭제하기 위해 하루에 한 번 실행됩니다. 이 변경 사항은 완전히 투명하게 나타납니다. 데이터에는 영향을 주지 않으며 백업 또는 복원 작업이 변경되지 않습니다.

Google Cloud 및 StorageGRID 스토리지에서 파일에 대한 찾아보기 및 복원 지원

위에서 설명한 대로 Browse & Restore 작업에 대한 컨테이너가 추가되어 Google Cloud 및 StorageGRID 시스템에 저장된 백업 파일에서 파일 복원 작업을 수행할 수 있습니다. 이제 Browse & Restore를 사용하여 모든 퍼블릭 클라우드 공급자 및 StorageGRID에서 파일을 복원할 수 있습니다. "[ONTAP 백업에서 볼륨 및 파일을 복원하기 위해 Browse & Restore를 사용하는 방법을 확인하십시오](#)".

끌어서 놓기를 통해 **Cloud Backup**을 **S3** 스토리지로 설정합니다

백업에 대한 Amazon S3 대상이 Canvas의 작업 환경으로 존재하는 경우, 온프레미스 ONTAP 클러스터 또는 Cloud Volumes ONTAP 시스템(AWS에 설치됨)을 Amazon S3 작업 환경으로 끌어서 설정 마법사를 시작할 수 있습니다.

Kubernetes 클러스터에서 새로 생성된 볼륨에 백업 정책을 자동으로 적용합니다

Cloud Backup을 활성화한 후 Kubernetes 클러스터에 새로운 영구 볼륨을 추가한 경우에는 이전에 해당 볼륨에 대한 백업을 구성해야 했습니다. 이제 새로 생성된 볼륨에 자동으로 적용되는 정책을 선택할 수 있습니다 "[백업 설정 페이지에서](#)" 이미 Cloud Backup을 활성화한 클러스터의 경우

이제 **Cloud Backup API**를 사용하여 백업 및 복원 작업을 관리할 수 있습니다

API는 에서 사용할 수 있습니다 <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>. 을 참조하십시오 "[이 페이지](#)" API에 대한 개요입니다.

2022년 5월 2일

검색 및 복원은 이제 **Google Cloud Storage**의 백업 파일에서 지원됩니다

4월에 AWS에 백업 파일을 저장한 사용자를 위해 볼륨 및 파일 복원 검색 및 복원 방법이 도입되었습니다. 이제 Google Cloud Storage에 백업 파일을 저장하는 사용자가 이 기능을 사용할 수 있습니다. "[검색 및 amp;Restore를 사용하여 볼륨 및 파일을 복원하는 방법을 확인하십시오](#)".

Kubernetes 클러스터에서 새로 생성된 볼륨에 자동으로 적용할 백업 정책을 구성합니다

Cloud Backup을 활성화한 후 Kubernetes 클러스터에 새로운 영구 볼륨을 추가한 경우에는 이전에 해당 볼륨에 대한 백업을 구성해야 했습니다. 이제 새로 생성된 볼륨에 자동으로 적용되는 정책을 선택할 수 있습니다. 이 옵션은 새 Kubernetes 클러스터에 대한 Cloud Backup을 활성화할 때 설정 마법사에서 사용할 수 있습니다.

이제 작업 환경에서 **Cloud Backup**을 활성화하려면 라이선스가 필요합니다

Cloud Backup에서 라이선스를 구축하는 방법은 다음과 같이 몇 가지 변경되었습니다.

- Cloud Backup을 활성화하려면 먼저 클라우드 공급자로부터 PAYGO Marketplace 구독에 가입하거나 NetApp에서 BYOL 라이선스를 구입해야 합니다.
- 30일 무료 평가판은 클라우드 공급자가 PAYGO 구독을 사용하는 경우에만 사용할 수 있으며 BYOL 라이선스를 사용하는 경우에는 사용할 수 없습니다.
- 무료 평가판은 마켓플레이스 가입이 시작되는 날부터 시작됩니다. 예를 들어, Cloud Volumes ONTAP 시스템에 대해 30일 동안 Marketplace 구독을 사용한 후 무료 평가판을 활성화하면 클라우드 백업 평가판을 사용할 수 없습니다.

"[사용 가능한 라이선스 모델에 대해 자세히 알아보십시오](#)".

2022년 4월 4일

SnapCenter에 기반을 둔 애플리케이션 클라우드 백업 1.1.0 이 현재 **GA**입니다

새로운 Cloud Backup for Applications 기능을 사용하면 Oracle 및 Microsoft SQL에 대한 기존 애플리케이션 정합성 보장 스냅샷(백업)을 사내 운영 스토리지에서 Amazon S3 또는 Azure Blob의 클라우드 오브젝트 스토리지로 오프로드할 수 있습니다.

필요한 경우 클라우드에서 사내로 데이터를 복원할 수 있습니다.

["사내 애플리케이션 데이터를 클라우드로 보호하는 방법에 대해 자세히 알아보십시오."](#)

모든 **ONTAP** 백업 파일에서 볼륨 또는 파일을 검색하는 새로운 검색 및 복원 기능

이제 일부 또는 전체 볼륨 이름, 일부 또는 전체 파일 이름, 크기 범위 및 추가 검색 필터를 통해 * 모든 ONTAP 백업 파일 * 에서 볼륨 또는 파일을 검색할 수 있습니다. 이 방법은 어떤 클러스터나 볼륨이 데이터의 소스인지 잘 모르면 복원하려는 데이터를 찾을 수 있는 새로운 방법입니다. ["검색 및 amp;Restore 사용 방법에 대해 알아봅니다"](#).

2022년 3월 3일

GKE Kubernetes 클러스터에서 **Google Cloud** 스토리지로 영구 볼륨을 백업하는 기능

GKE 클러스터에 NetApp Astra Trident가 설치되어 있고 Cloud Volumes ONTAP for GCP를 클러스터의 백엔드 스토리지로 사용하는 경우, Google Cloud 스토리지와 영구 볼륨을 백업 및 복원할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

Cloud Data Sense를 사용하여 **Cloud Backup** 파일을 검사하는 베타 기능은 이 릴리즈에서 더 이상 제공되지 않습니다

2022년 2월 14일

이제 단일 클러스터의 개별 볼륨에 백업 정책을 할당할 수 있습니다

과거에는 클러스터의 모든 볼륨에 단일 백업 정책만 할당할 수 있었습니다. 이제 단일 클러스터에 대해 여러 백업 정책을 생성하고 여러 볼륨에 서로 다른 정책을 적용할 수 있습니다. ["클러스터에 대한 새 백업 정책을 생성하고 이를 선택한 볼륨에 할당하는 방법을 알아보십시오"](#).

새 옵션을 사용하면 새로 생성된 볼륨에 기본 백업 정책을 자동으로 적용할 수 있습니다

과거에는 Cloud Backup을 활성화한 후 작업 환경에서 생성된 새 볼륨을 수동으로 백업 정책을 적용해야 했습니다. 이제 Cloud Manager, System Manager, CLI 또는 API에서 볼륨이 생성되었는지에 관계없이 Cloud Backup은 볼륨을 검색하고 선택한 백업 정책을 기본 정책으로 적용합니다.

이 옵션은 새 작업 환경에서 백업을 설정하거나 기존 작업 환경의 _Manage Volumes_ 페이지에서 백업을 설정할 때 사용할 수 있습니다.

새 작업 모니터를 사용하여 모든 백업 및 복원 작업의 진행 상태를 확인할 수 있습니다

백업 정책 변경 또는 백업 삭제와 같이 여러 볼륨에 대해 작업을 시작한 경우 작업 모니터를 사용하면 모든 볼륨에서 작업이 완료된 시점을 확인할 수 있습니다. ["작업 모니터 사용 방법을 참조하십시오"](#).

2022년 1월 2일

AKS Kubernetes 클러스터에서 Azure Blob 스토리지로 영구 볼륨을 백업할 수 있습니다

AKS 클러스터에 NetApp Astra Trident가 설치되어 있고 Azure용 Cloud Volumes ONTAP를 클러스터용 백엔드 스토리지로 사용하는 경우, Azure Blob 스토리지간에 볼륨을 백업 및 복원할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

업계 표준에 더욱 부합하도록 이번 릴리스에서 Cloud Backup Service 요금이 변경되었습니다

백업 파일의 크기에 따라 NetApp의 용량을 지불하는 대신, 현재 백업 중인 소스 ONTAP 볼륨의 논리적 사용 용량(ONTAP 효율성 이전)을 기준으로 계산한, 보호하는 데이터에 대해서만 비용을 지불하면 됩니다. 이 용량을 FETB(Front-End Terabytes)라고도 합니다.

2021년 11월 28일

EKS Kubernetes 클러스터에서 Amazon S3로 영구 볼륨을 백업하는 기능

EKS 클러스터에 NetApp Astra Trident가 설치되어 있고 Cloud Volumes ONTAP for AWS를 클러스터의 백엔드 스토리지로 사용하는 경우 Amazon S3로 볼륨을 백업 및 복원할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

DP 볼륨을 백업하는 향상된 기능

Cloud Backup은 이제 SVM-DR 관계의 타겟 ONTAP 시스템에 있는 DP 볼륨의 백업을 생성할 수 있도록 지원합니다. 몇 가지 제한 사항이 있습니다. 을 참조하십시오 ["제한 사항"](#) 을 참조하십시오.

2021년 11월 5일

온프레미스 ONTAP 시스템으로 볼륨을 복원할 때 개인 엔드포인트를 선택할 수 있습니다

Amazon S3 또는 Azure Blob에 있는 백업 파일에서 온프레미스 ONTAP 시스템으로 볼륨을 복원할 때 온프레미스 시스템에 안전하게 비공개로 연결하는 프라이빗 끝점을 선택할 수 있습니다.

이제 며칠 후 오래된 백업 파일을 아카이브 스토리지에 계층화하여 비용을 절감할 수 있습니다

클러스터에서 ONTAP 9.10.1 이상이 실행 중이고 AWS 또는 Azure 클라우드 스토리지를 사용 중인 경우 백업을 아카이브 스토리지에 계층화할 수 있습니다. 에 대한 자세한 내용을 참조하십시오 ["AWS S3 아카이빙 스토리지 클래스"](#) 및 ["Azure Blob 아카이브 액세스 계층"](#).

Cloud Backup BYOL 라이선스는 Digital Wallet의 Data Services Licenses 탭으로 이동했습니다

Cloud Backup에 대한 BYOL 라이선스는 Cloud Backup Licenses 탭에서 Cloud Manager Digital Wallet의 Data Services Licenses 탭으로 이동했습니다.

2021년 10월 4일

이제 볼륨 또는 파일 복원을 수행할 때 백업 페이지에서 백업 파일 크기를 사용할 수 있습니다

불필요한 대용량 백업 파일을 삭제하거나 백업 파일 크기를 비교하여 악성 소프트웨어 공격으로 인해 발생할 수 있는 비정상적인 백업 파일을 확인할 수 있는 경우에 유용합니다.

TCO 계산기를 사용하여 클라우드 백업 비용을 비교할 수 있습니다

총 소유 비용 계산기는 Cloud Backup의 총 소유 비용을 파악하고 이러한 비용을 기존 백업 솔루션과 비교하고 잠재적인 절감 효과를 추정하는 데 도움이 됩니다. 확인해 보십시오<https://cloud.netapp.com/cloud-backup-service-tco-calculator>["여기"].

작업 환경의 클라우드 백업 등록을 취소하는 기능입니다

이제 손쉽게 할 수 있습니다 **"작업 환경의 클라우드 백업 등록을 취소합니다"** 해당 작업 환경에 더 이상 백업 기능을 사용하지 않거나 비용이 청구되지 않는 경우

2021년 9월 2일

볼륨의 필요 시 백업을 생성하는 기능입니다

이제 언제든지 주문형 백업을 생성하여 볼륨의 현재 상태를 캡처할 수 있습니다. 이 기능은 볼륨에 중요한 변경 사항이 있고 예약된 다음 백업이 해당 데이터를 보호할 때까지 기다리지 않으려는 경우에 유용합니다.

"필요 시 백업을 생성하는 방법을 확인하십시오".

Amazon S3에 대한 보안 백업을 위해 전용 인터페이스 연결을 정의하는 기능

온-프레미스 ONTAP 시스템에서 Amazon S3로 백업을 구성할 때 이제 활성화 마법사에서 전용 인터페이스 끝점에 대한 연결을 정의할 수 있습니다. 이를 통해 사내 시스템을 AWS PrivateLink 기반의 서비스에 안전하게 비공개로 연결하는 네트워크 인터페이스를 사용할 수 있습니다. **"이 옵션에 대한 자세한 내용을 참조하십시오"**.

이제 데이터를 **Amazon S3**에 백업할 때 데이터 암호화에 대해 자체 고객 관리 키를 선택할 수 있습니다

추가 보안 및 제어를 위해 기본 Amazon S3 암호화 키를 사용하는 대신 활성화 마법사에서 데이터 암호화에 대해 고객이 관리하는 키를 직접 선택할 수 있습니다. 이 기능은 사내 ONTAP 시스템 또는 AWS의 Cloud Volumes ONTAP 시스템에서 백업을 구성할 때 사용할 수 있습니다.

이제 **30,000**개 이상의 파일이 있는 디렉토리에서 파일을 복원할 수 있습니다

2021년 8월 1일

Azure Blob에 대한 보안 백업을 위해 프라이빗 엔드포인트 연결을 정의하는 기능입니다

온프레미스 ONTAP 시스템에서 Azure Blob으로 백업을 구성하는 경우 활성화 마법사에서 Azure 프라이빗 엔드포인트의 연결을 정의할 수 있습니다. 이를 통해 Azure Private Link가 지원되는 서비스에 개인 및 안전하게

연결하는 네트워크 인터페이스를 사용할 수 있습니다.

이제 시간별 백업 정책이 지원됩니다

이 새로운 정책은 기존 일일, 주별 및 월별 정책에 추가됩니다. 시간별 백업 정책은 최소 RPO(복구 시점 목표)를 제공합니다.

2021년 7월 7일

이제 다른 계정과 다른 지역을 사용하여 백업을 만들 수 있습니다

이제 Cloud Backup을 사용하면 Cloud Volumes ONTAP 시스템에 사용 중인 계정/가입과 다른 계정/가입을 사용하여 백업을 생성할 수 있습니다. 또한 Cloud Volumes ONTAP 시스템이 배포된 영역과 다른 영역에 백업 파일을 만들 수도 있습니다.

이 기능은 AWS 또는 Azure를 사용하는 경우, 기존 작업 환경에서 백업을 사용하도록 설정할 때만 사용할 수 있으며, 새로운 Cloud Volumes ONTAP 작업 환경을 생성할 때는 사용할 수 없습니다.

이제 데이터를 **Azure Blob**에 백업할 때 데이터 암호화에 사용할 자체 고객 관리 키를 선택할 수 있습니다

추가 보안 및 제어를 위해 기본 Microsoft 관리 암호화 키를 사용하는 대신 활성화 마법사에서 데이터 암호화에 대해 고객이 관리하는 키를 직접 선택할 수 있습니다. 이 기능은 사내 ONTAP 시스템 또는 Azure의 Cloud Volumes ONTAP 시스템에서 백업을 구성할 때 사용할 수 있습니다.

이제 단일 파일 복원을 사용할 때 한 번에 최대 **100**개의 파일을 복원할 수 있습니다

2021년 6월 7일

ONTAP 9.8 이상을 사용할 때 **DP** 볼륨에 대해 제한 사항이 해제되었습니다

데이터 보호(DP) 볼륨 백업에 대해 알려진 두 가지 제한 사항이 해결되었습니다.

- 이전에는 다중 구간 백업은 SnapMirror 관계 유형이 Mirror-Vault 또는 Vault인 경우에만 작동했습니다. 이제 관계 유형이 MirrorAllSnapshots인 경우 백업을 수행할 수 있습니다.
- 이제 Cloud Backup은 SnapMirror 정책에 구성된 한 백업에 레이블을 사용할 수 있습니다. 매일, 매주 또는 매월 이름이 있는 라벨을 요구하는 제한은 사라졌습니다.

2021년 5월 5일

온프레미스 클러스터 데이터를 **Google** 클라우드 스토리지 또는 **NetApp StorageGRID** 시스템으로 백업합니다

이제 사내 ONTAP 시스템에서 Google 클라우드 스토리지 또는 NetApp StorageGRID 시스템으로 백업을 생성할 수 있습니다. 을 참조하십시오 ["Google Cloud Storage로 백업"](#) 및 ["StorageGRID에 백업 중입니다"](#) 를 참조하십시오.

이제 **System Manager**를 사용하여 클라우드 백업 작업을 수행할 수 있습니다

ONTAP 9.9.1의 새로운 기능을 사용하면 System Manager를 사용하여 사내 ONTAP 볼륨의 백업을 클라우드 백업을 통해 설정한 오브젝트 스토리지로 전송할 수 있습니다. "[System Manager를 사용하여 Cloud Backup을 사용하여 볼륨을 클라우드에 백업하는 방법을 알아보십시오.](#)"

몇 가지 향상된 기능을 통해 백업 정책이 개선되었습니다

- 이제 일일, 주별 및 월별 백업을 조합하여 사용자 지정 정책을 생성합니다.
- 백업 정책을 변경할 때 변경 사항은 원래 백업 정책을 사용하는 모든 볼륨에 대한 모든 새 백업 * 및 * 에 적용됩니다. 이전에는 새 볼륨 백업에만 변경 사항이 적용되었습니다.

기타 백업 및 복원 기능 향상

- 백업 파일에 대한 클라우드 대상을 구성할 때 이제 Cloud Volumes ONTAP 시스템이 상주하는 지역이 아닌 다른 영역을 선택할 수 있습니다.
- 단일 볼륨에 대해 생성할 수 있는 백업 파일 수가 1,019에서 4,000개로 증가했습니다.
- 단일 볼륨에 대한 모든 백업 파일을 삭제하는 이전 기능 외에도 볼륨에 대해 하나의 백업 파일만 삭제하거나, 필요한 경우 전체 작업 환경에 대한 모든 백업 파일을 삭제할 수 있습니다.

시작하십시오

Cloud Backup에 대해 자세히 알아보십시오

Cloud Backup은 데이터의 보호 및 장기 아카이브를 위한 백업 및 복원 기능을 제공하는 Cloud Manager 작업 환경을 위한 서비스입니다. 백업은 자동으로 생성되어 퍼블릭 또는 프라이빗 클라우드 계정의 오브젝트 저장소에 저장됩니다.

필요한 경우 백업에서 전체 _volume_을 동일하거나 다른 작업 환경으로 복원할 수 있습니다. ONTAP 데이터를 백업할 때 또는 백업에서 하나 이상의 _files_를 동일하거나 다른 작업 환경으로 복원하도록 선택할 수도 있습니다.

["Cloud Backup에 대해 자세히 알아보십시오"](#).

백업 및 복원을 사용하여 다음을 수행할 수 있습니다.

- Cloud Volumes ONTAP 및 사내 ONTAP 시스템에서 ONTAP 볼륨을 백업 및 복원합니다. ["자세한 기능은 여기에서 확인하십시오"](#).
- Kubernetes 영구 볼륨의 백업 및 복원 ["자세한 기능은 여기에서 확인하십시오"](#).
- 클라우드 백업 for Applications를 사용하여 사내 ONTAP에서 클라우드로 애플리케이션 정합성을 보장하는 스냅샷을 백업합니다. ["자세한 기능은 여기에서 확인하십시오"](#).
- Cloud Backup for VMware를 사용하여 데이터 저장소를 클라우드에 백업하고 가상 머신을 사내 vCenter로 복구합니다. ["자세한 기능은 여기에서 확인하십시오"](#).



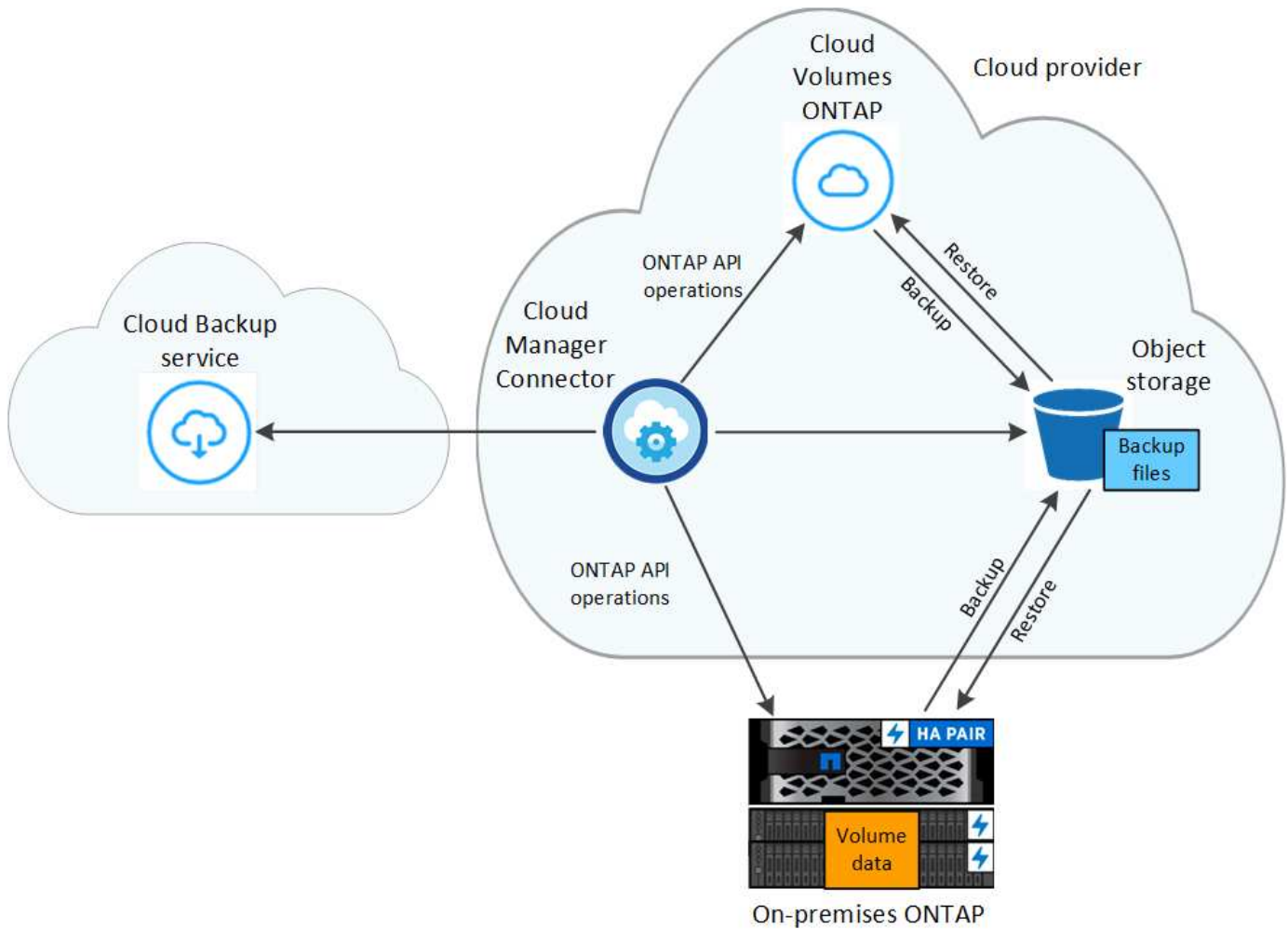
Cloud Manager Connector를 클라우드의 정부 지역 또는 인터넷에 액세스할 수 없는 사이트(어두운 사이트)에 구축하면 Cloud Backup은 ONTAP 시스템의 백업 및 복원 작업만 지원합니다. 이러한 대체 구축 방법을 사용할 때 Cloud Backup은 Kubernetes 클러스터, 애플리케이션 또는 가상 시스템의 백업 및 복원 작업을 지원하지 않습니다.

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 백업이므로 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"](#).

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.

백업은 자정에 수행됩니다

- 매시간 백업은 시간 5분 전에 매시간 시작됩니다.
- 매일 백업은 매일 자정 직후에 시작됩니다.
- 매주 백업은 일요일 아침 자정이 지난 직후에 시작됩니다.
- 매월 백업은 매월 첫 번째 날에 자정이 지난 직후에 시작됩니다.

시작 시간은 각 소스 ONTAP 시스템에 설정된 표준 시간대를 기준으로 합니다. UI에서 사용자가 지정한 시간에 백업 작업을 예약할 수 없습니다. 자세한 내용은 시스템 엔지니어에게 문의하십시오.

백업 복사본은 **NetApp** 계정과 연결됩니다

백업 복사본은 와 연결됩니다 **"NetApp 계정"** 커넥터가 있는 위치.

동일한 NetApp 계정에 여러 커넥터가 있는 경우 각 커넥터는 동일한 백업 목록을 표시합니다. 여기에는 Cloud Volumes ONTAP 및 다른 커넥터의 온-프레미스 ONTAP 인스턴스와 연결된 백업이 포함됩니다.

Cloud Backup에 대한 라이선스 설정

클라우드 공급자로부터 PAYGO(Pay-as-you-Go) 마켓플레이스 구독을 구입하거나 NetApp에서 BYOL(Bring-Your-Own-License)을 구입하여 Cloud Backup의 라이선스를 부여할 수 있습니다. 작업 환경에서 Cloud Backup을 활성화하고, 운영 데이터의 백업을 생성하고, 백업 데이터를 운영 시스템에 복원하려면 유효한 라이선스가 필요합니다.

추가 내용을 읽기 전에 몇 가지 참고 사항을 확인하십시오.

- 클라우드 공급자의 Cloud Volumes ONTAP 시스템 시장에서 PAYGO(Pay-as-you-Go) 구독을 이미 구독한 경우 클라우드 백업도 자동으로 구독됩니다. 다시 가입하지 않아도 됩니다.
- Cloud Backup BYOL(Bring-Your-Own-License)은 Cloud Manager 계정과 연결된 모든 시스템에서 사용할 수 있는 부동 라이선스입니다. 따라서 기존 BYOL 라이선스에서 충분한 백업 용량을 제공하는 경우 다른 BYOL 라이선스를 구입할 필요가 없습니다.
- 온프레미스 ONTAP 데이터를 StorageGRID에 백업할 경우 BYOL 라이선스가 필요하지만 클라우드 공급자의 스토리지 공간에는 비용이 들지 않습니다.

"Cloud Backup 사용과 관련된 비용에 대해 자세히 알아보십시오."

30일 무료 평가판

Cloud Backup 30일 무료 평가판은 클라우드 공급자 마켓플레이스의 선불 종량제 구독에서 제공됩니다. 무료 평가판은 마켓플레이스 목록에 등록할 때 시작됩니다. Cloud Volumes ONTAP 시스템을 구축할 때 Marketplace 구독에 대한 비용을 지불하고 Cloud Backup 무료 평가판 을 10일 후에 시작하면 20일 동안 무료 평가판을 사용할 수 있습니다.

무료 평가판이 종료되면 중단 없이 PAYGO 구독으로 자동 전환됩니다. Cloud Backup을 계속 사용하지 않기로 결정한 경우 **"작업 환경에서 클라우드 백업 등록을 취소합니다"** 평가판 사용 기간이 끝나기 전에는 요금이 부과되지 않습니다.

Cloud Backup PAYGO 구독 사용

사용한 만큼만 지불하는 용량제 방식을 사용하면 클라우드 공급업체에 오브젝트 스토리지 비용을 지불하고, NetApp 백업 라이선스 비용을 단일 정액제로 지불할 수 있습니다. 무료 평가판을 가지고 있거나 BYOL(Bring Your Own License)을 사용하는 경우에도 가입해야 합니다.

- 구독하면 무료 평가판이 종료된 후에도 서비스가 중단되지 않습니다. 평가판이 종료되면 백업하는 데이터의 양에 따라 매시간 요금이 부과됩니다.
- BYOL 라이선스에서 허용하는 것보다 더 많은 데이터를 백업하는 경우 용량제 가입형 모델을 통해 데이터 백업을 계속 수행할 수 있습니다. 예를 들어, 10TiB BYOL 라이선스가 있는 경우 PAYGO 구독을 통해 10TiB를 초과하는 모든 용량이 충전됩니다.

무료 평가판 사용 중 또는 BYOL 라이선스를 초과하지 않은 경우 용량제 구독을 통해 비용을 지불할 필요가 없습니다.

클라우드 백업을 위한 몇 가지 PAYGO 계획이 있습니다.

- Cloud Volumes ONTAP 데이터와 사내 ONTAP 데이터를 백업할 수 있는 "클라우드 백업" 패키지
- Cloud Volumes ONTAP와 클라우드 백업을 번들로 제공할 수 있는 "CVO Professional" 패키지입니다. 여기에는 이 라이선스에 대해 청구된 Cloud Volumes ONTAP 볼륨에 대한 무제한 백업이 포함됩니다(백업 용량은 라이선스에 포함되지 않음). 이 옵션을 사용하면 사내 ONTAP 데이터를 백업할 수 없습니다. ifdef::Azure[]

다음 링크를 사용하여 클라우드 공급자 마켓플레이스에서 Cloud Backup을 구독하십시오.

- AWS: "[가격 세부 정보는 Cloud Manager Marketplace 오퍼링을 참조하십시오](#)".
- Azure(Azure): "[가격 세부 정보는 Cloud Manager Marketplace 오퍼링을 참조하십시오](#)".
- GCP: "[가격 세부 정보는 Cloud Manager Marketplace 오퍼링을 참조하십시오](#)".

AWS를 통해 연간 계약을 구독하십시오

에서 2개의 연간 계약을 사용할 수 있습니다 "[AWS 마켓플레이스 페이지를 참조하십시오](#)" Cloud Volumes ONTAP 및 사내 ONTAP 시스템: 1년, 2년 또는 3년 조건으로 제공됩니다.

- Cloud Volumes ONTAP 데이터와 사내 ONTAP 데이터를 백업할 수 있는 '클라우드 백업' 계획

이 옵션을 사용하려면 마켓플레이스 페이지에서 구독을 설정한 다음 "[가입 정보를 AWS 자격 증명과 연결합니다](#)". Cloud Manager에서 AWS 자격 증명에 활성 구독을 하나만 할당할 수 있으므로 이 연간 계약 가입을 통해 Cloud Volumes ONTAP 시스템에 대한 비용을 지불해야 합니다.

- 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). 이 옵션을 사용하면 사내 ONTAP 데이터를 백업할 수 없습니다.

를 참조하십시오 "[Cloud Volumes ONTAP 라이선스 항목을 참조하십시오](#)" 이 라이선스 옵션에 대해 자세히 알아보십시오.

이 옵션을 사용하려면 Cloud Volumes ONTAP 작업 환경을 생성할 때 연간 계약을 설정하고 Cloud Manager에서 AWS 마켓플레이스를 구독하라는 메시지를 표시합니다.

Cloud Backup BYOL 라이선스 사용

NetApp에서 제공하는 자체 라이선스는 1년, 2년 또는 3년간 제공됩니다. 백업 중인 소스 ONTAP 볼륨의 논리적 사용 용량(_before_any 효율성)으로 계산되어 보호하는 데이터에 대해서만 비용을 지불하면 됩니다. 이 용량을 FETB(Front-End Terabytes)라고도 합니다.

BYOL Cloud Backup 라이선스는 Cloud Manager 계정과 연결된 모든 시스템에서 전체 용량을 공유하는 부동 라이선스입니다. ONTAP 시스템의 경우 백업하려는 볼륨에 대해 CLI 명령 'volume show-space-logical-used'를 실행하여 필요한 용량을 대략적으로 계산할 수 있습니다.

Cloud Backup BYOL 라이선스가 없는 경우 Cloud Manager 오른쪽 아래에 있는 채팅 아이콘을 클릭하여 라이선스를 구입하십시오.

선택적으로 사용하지 않을 Cloud Volumes ONTAP에 대해 할당되지 않은 노드 기반 라이선스가 있는 경우 동일한 달러

당량 및 만료 날짜가 있는 클라우드 백업 라이선스로 전환할 수 있습니다. ["자세한 내용을 보려면 여기를 클릭하십시오"](#).

Cloud Manager의 Digital Wallet 페이지를 사용하여 BYOL 라이선스를 관리할 수 있습니다. Digital Wallet에서 새 라이선스를 추가하고, 기존 라이선스를 업데이트하고, 라이선스 상태를 볼 수 있습니다.

Cloud Backup 라이선스 파일을 얻습니다

Cloud Backup 라이선스를 구입한 후에는 Cloud Backup 일련 번호 및 NSS 계정을 입력하거나 NLF 라이선스 파일을 업로드하여 Cloud Manager에서 라이선스를 활성화합니다. 아래 단계에서는 NLF 라이선스 파일을 가져오는 방법을 보여 줍니다(해당 방법을 사용하려는 경우).

인터넷에 액세스할 수 없는 사내 사이트에서 Cloud Backup을 실행 중인 경우, 즉 오프라인 사내 사이트의 호스트에 Cloud Manager Connector를 배포했다면 인터넷에 연결된 시스템에서 라이선스 파일을 얻어야 합니다. 일련 번호 및 NSS 계정을 사용하여 라이선스를 활성화하는 것은 오프라인(다크 사이트) 설치에 사용할 수 없습니다.

단계

1. 에 로그인합니다 ["NetApp Support 사이트"](#) 시스템 > 소프트웨어 라이선스 * 를 클릭합니다.
2. Cloud Backup 라이선스 일련 번호를 입력합니다.

Serial #	Cluster SN	License Name	License Key	Host ID	Value	End Date
4810		CLOUD_BKP_SERVICE	Get NetApp License File		100	12/31/9998

3. 라이선스 키 * 열에서 * NetApp 라이선스 파일 가져오기 * 를 클릭합니다.
4. Cloud Manager 계정 ID(지원 사이트에서 테넌트 ID라고 함)를 입력하고 * 제출 * 을 클릭하여 라이선스 파일을 다운로드합니다.

Get License

SERIAL NUMBER: 4810

LICENSE: CLOUD_BKP_SERVICE

SALES ORDER: 3005

TENANT ID:

Example: account-xxxxxxx

[Cancel](#) [Submit](#)

Cloud Manager 상단의 * Account * (계정 *) 드롭다운을 선택한 다음 계정 옆의 * Manage Account * 를 클릭하여 Cloud Manager 계정 ID를 찾을 수 있습니다. 계정 ID는 개요 탭에 있습니다.

Cloud Backup BYOL 라이선스를 계정에 추가

NetApp 계정에 대한 Cloud Backup 라이선스를 구입한 후 Cloud Manager에 라이선스를 추가해야 합니다.

단계

1. 모든 서비스 > 디지털 지갑 > 데이터 서비스 라이선스 * 를 클릭합니다.
2. 라이선스 추가 * 를 클릭합니다.
3. Add License_대화 상자에서 라이선스 정보를 입력하고 * Add License * 를 클릭합니다.
 - 백업 라이선스 일련 번호가 있고 NSS 계정을 알고 있는 경우 * 일련 번호 입력 * 옵션을 선택하고 해당 정보를 입력합니다.

드롭다운 목록에서 NetApp Support 사이트 계정을 사용할 수 없는 경우 "[NSS 계정을 Cloud Manager에 추가합니다](#)".

- 백업 라이선스 파일이 있는 경우(어두운 사이트에 설치할 때 필요) * 라이선스 파일 업로드 * 옵션을 선택하고 메시지에 따라 파일을 첨부합니다.

Add Cloud Backup License

A Backup License must be installed with an active subscription. A Backup license enables you to use Cloud Backup for a certain period of time and for a maximum amount of backup space.

☒ Enter Serial Number ☐ Upload License File

Serial Number

Enter Serial Number

NetApp Support Site Account

Select Support Site Account

Add Backup License Cancel

☐ Enter Serial Number ☒ Upload License File

To install a license, follow these instructions:

- 1 Obtain the license file from the "System > Software Licenses" tab at [NetApp Support Site](#). You will need to provide your cloud service serial number and Cloud Manager Account ID.
- 2 Click Upload File and then select the file.

Upload License File

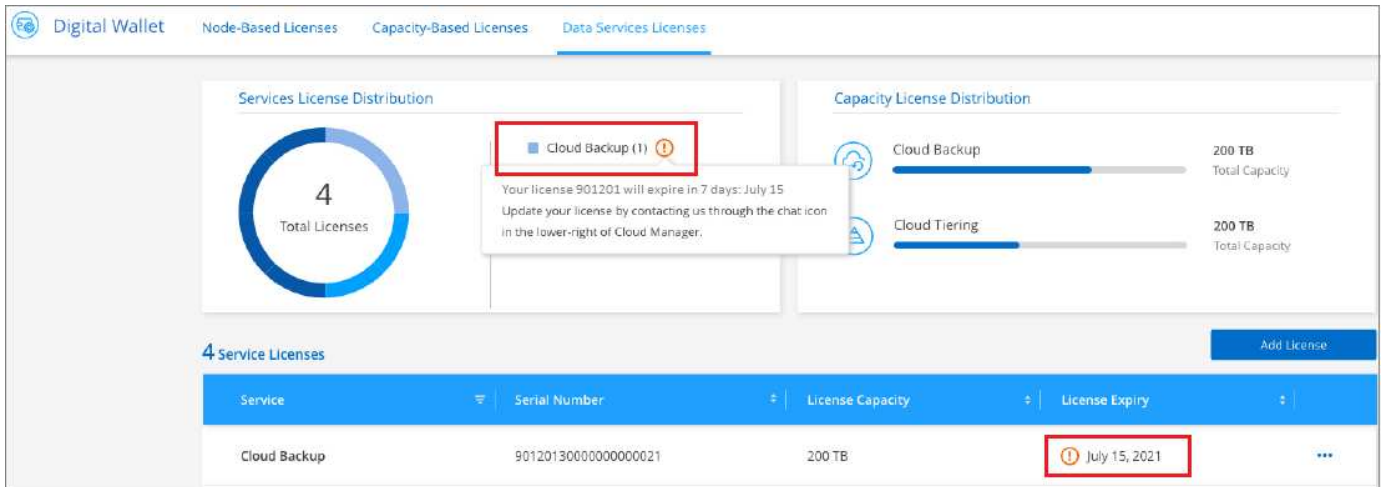
Upload License File **Upload**

Add Backup License Cancel

Cloud Manager에서 라이선스를 추가하여 Cloud Backup을 활성화합니다.

Cloud Backup BYOL 라이선스 업데이트

라이선스가 부여된 기간이 만료일에 가까워지고 있거나 라이선스가 부여된 용량이 한도에 도달한 경우 백업 UI에서 알림을 받게 됩니다. 이 상태는 Digital Wallet 페이지와 에도 표시됩니다 "[알림](#)".



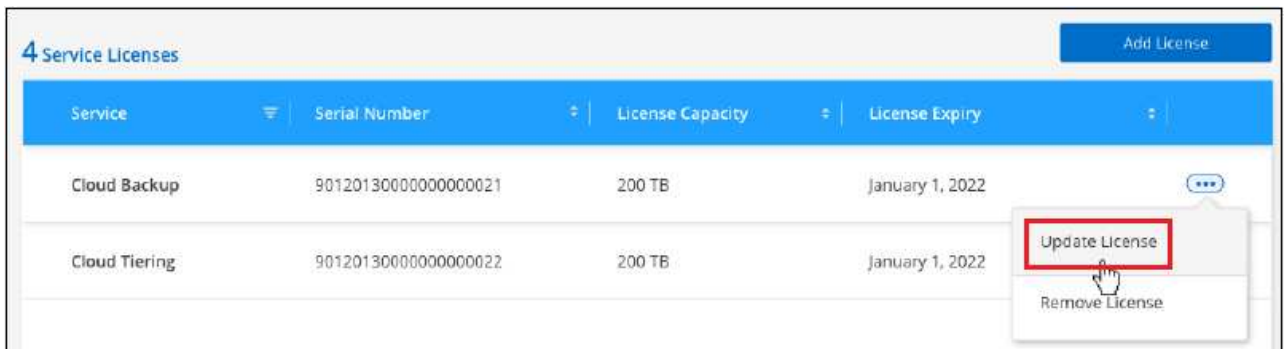
Cloud Backup 라이선스가 만료되기 전에 업데이트하여 데이터 백업 및 복원 기능에 중단이 발생하지 않도록 할 수 있습니다.

단계

1. Cloud Manager의 오른쪽 아래에 있는 채팅 아이콘을 클릭하거나 지원 팀에 문의하여 특정 일련 번호에 대한 Cloud Backup 라이선스 기간 연장 또는 추가 용량을 요청하십시오.

라이선스 비용을 지불하고 NetApp Support 사이트에 등록된 Cloud Manager는 Digital Wallet의 라이선스를 자동으로 업데이트하며, 데이터 서비스 라이선스 페이지에는 변경 사항이 5~10분 안에 반영됩니다.

2. Cloud Manager에서 라이선스를 자동으로 업데이트할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 라이선스 파일을 수동으로 업로드해야 합니다.
 - a. 가능합니다 [NetApp Support 사이트](#)에서 **라이선스 파일**을 받으십시오.
 - b. Digital Wallet page_Data Services Licenses_탭에서 를 클릭합니다 ... 업데이트하는 서비스 일련 번호에 대해 * Update License * 를 클릭합니다.



- c. Update License_page에서 라이선스 파일을 업로드하고 * Update License * 를 클릭합니다.

Cloud Manager는 Cloud Backup을 계속 활성화할 수 있도록 라이선스를 업데이트합니다.

BYOL 라이선스 고려사항

Cloud Backup BYOL 라이선스를 사용하는 경우, 백업하는 모든 데이터의 크기가 용량 제한에 근접하거나 라이선스 만료 날짜가 임박한 경우 Cloud Manager에서 사용자 인터페이스에 경고를 표시합니다. 다음과 같은 경고가 표시됩니다.

- 백업이 라이선스 용량의 80%에 도달한 경우 제한에 도달하면 다시 한 번 백업을 수행합니다
- 라이선스가 만료되기 30일 전에 라이선스가 만료되고 라이선스가 만료되면 다시 만료됩니다

이러한 경고가 표시되면 Cloud Manager 인터페이스 오른쪽 아래에 있는 채팅 아이콘을 사용하여 라이선스를 갱신하십시오.

BYOL 라이선스가 만료되면 다음 두 가지 상황이 발생할 수 있습니다.

- 사용 중인 계정에 마켓플레이스 계정이 있는 경우 백업 서비스가 계속 실행되지만 PAYGO 라이선스 모델로 이전됩니다. 백업이 사용 중인 용량에 대한 비용이 청구됩니다.
- 사용 중인 계정에 마켓플레이스 계정이 없는 경우 백업 서비스가 계속 실행되지만 경고가 계속 표시됩니다.

BYOL 구독을 갱신하면 Cloud Manager에서 라이선스를 자동으로 업데이트합니다. Cloud Manager가 보안 인터넷 연결을 통해 라이선스 파일에 액세스할 수 없는 경우(예: 어두운 사이트에 설치된 경우) 직접 파일을 얻고 Cloud Manager에 수동으로 업로드할 수 있습니다. 자세한 내용은 ["Cloud Backup 라이선스를 업데이트하는 방법"](#)을 참조하십시오.

PAYGO 라이선스로 전환된 시스템은 자동으로 BYOL 라이선스로 돌아갑니다. 라이선스 없이 실행 중이던 시스템에서는 경고가 표시되지 않습니다.

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 계층화합니다(ONTAP 9.10.1 이상을 사용할 때 지원됨).
- 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 카탈로그입니다.

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 <code>ifdef::AWS[]</code>
AWS의 Cloud Volumes ONTAP	Amazon S3 엔디프::AWS[]ifdef::Azure[]
Azure의 Cloud Volumes ONTAP	Azure Blob endif::Azure []ifdef::GCP[]
Google의 Cloud Volumes ONTAP	Google Cloud 스토리지 엔디프::GCP[]

소스 작업 환경	백업 파일 대상 ifdef::AWS[]
사내 ONTAP 시스템	ifdef::AWS[]Amazon S3 endif::AWS[]ifdef::Azure[]Azure Blob endif::Azure[]ifdef::GCP[]Google Cloud Storage endif::GCP[]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 * ifdef::AWS[]
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	Cloud Volumes ONTAP in AWS on-premises ONTAP system endif::AWS[]ifdef::Azure[]
Azure Blob	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP endif::Azure []ifdef::GCP[]
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP::GCP []
NetApp StorageGRID를 참조하십시오	사내 ONTAP 시스템	사내 ONTAP 시스템

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

인터넷 연결이 없는 사이트에 대한 지원

클라우드 백업은 인터넷에 연결되지 않은 사이트("오프라인" 또는 "다크" 사이트라고도 함)에서 로컬 사내 ONTAP 시스템의 볼륨 데이터를 로컬 NetApp StorageGRID 시스템으로 백업하는 데 사용할 수 있습니다. 이 경우 어두운 사이트에 Cloud Manager Connector(최소 버전 3.9.19)를 배포해야 합니다. 을 참조하십시오 ["사내 ONTAP 데이터를 StorageGRID에 백업"](#) 를 참조하십시오.

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.

- 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 파일에서 볼륨 데이터를 복구해야 하는 경우, 클라우드 공급자로부터 추가 Per-GiB 검색 비용 및 요청당 수수료를 받을 수 있습니다.
- 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. 세 번째 옵션은 NetApp에서 직접 라이선스를 구매하는 것입니다. 를 읽습니다 [라이센싱](#) 섹션을 참조하십시오.

라이센싱

Cloud Backup은 몇 가지 라이선스 옵션으로 제공됩니다.

- PAYGO(Pay As You Go) 구독
- AWS Marketplace에서 연간 계약 체결
- BYOL(Bring Your Own License)

PAYGO 구독으로 처음 등록하면 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

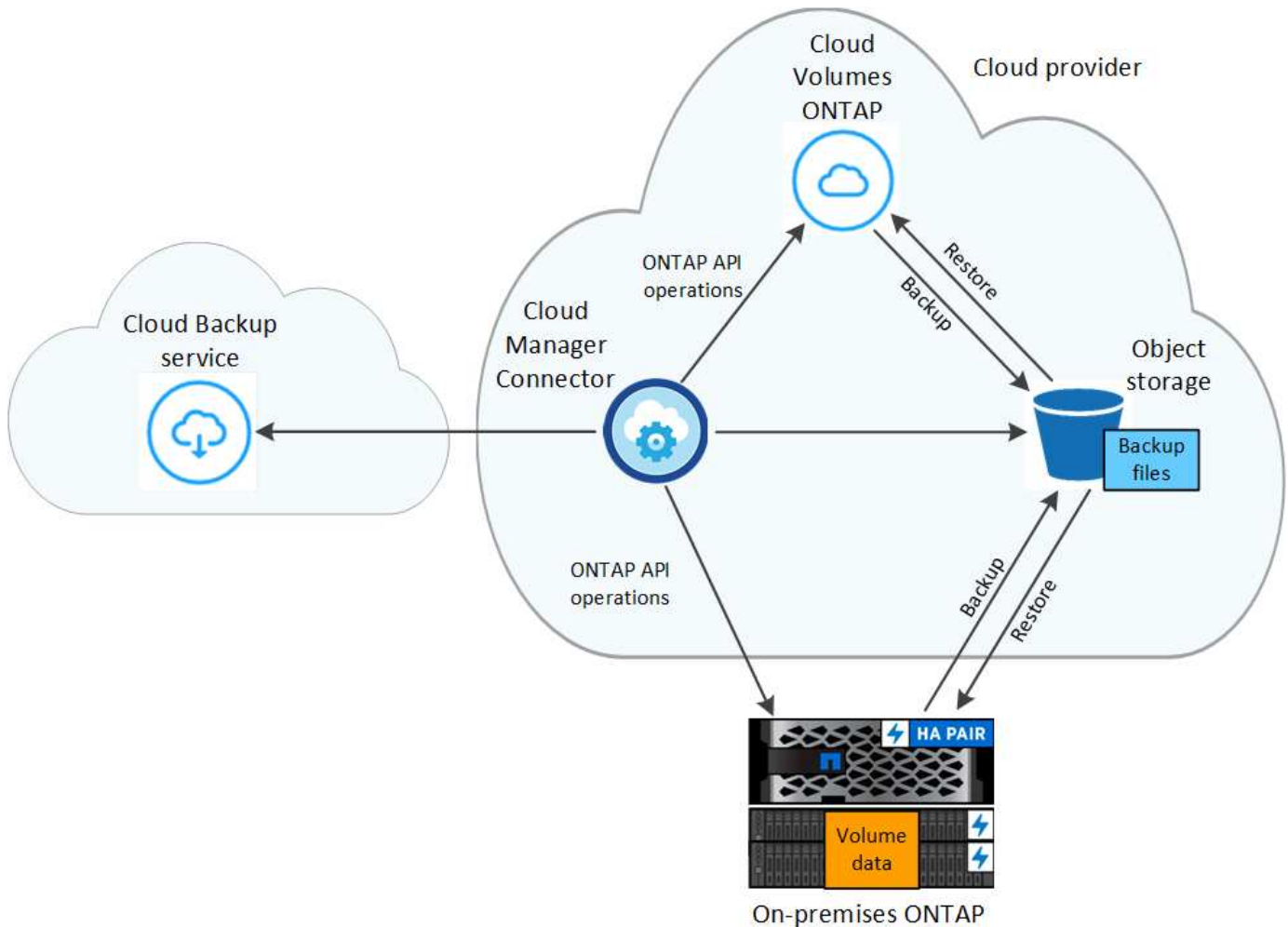
Cloud Volumes ONTAP 또는 사내 ONTAP 시스템에서 클라우드 백업을 활성화하면 서비스가 데이터의 전체 백업을 수행합니다. 볼륨 스냅샷은 백업 이미지에 포함되지 않습니다. 초기 백업 후에는 모든 추가 백업이 증분 백업되므로 변경된 블록과 새 블록만 백업됩니다. 이렇게 하면 네트워크 트래픽이 최소로 유지됩니다.

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

백업 정책 이름입니다	간격당 백업...			최대 백업
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 이상이 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 클라우드로 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(* 미리 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 서브넷에서 서로 다른 클라우드 관리자와 동일한 계정을 사용하는 경우 파일 레벨 복원이 지원되지 않습니다.
- 백업 파일이 아카이브 스토리지에 있는 경우 개별 파일을 복원할 수 없습니다.
- 인터넷 액세스(다크 사이트)가 없는 사이트에 Connector가 설치된 경우 검색 및 복원을 사용하여 파일 수준 복원이 지원되지 않습니다.

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.

- 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".

span class="image">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.



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_Account_1

AWS Access Key

Enter AWS Access Key

AWS Secret Key

Enter AWS Secret Key

Location & Connectivity

Region

us-east-2

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

<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 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

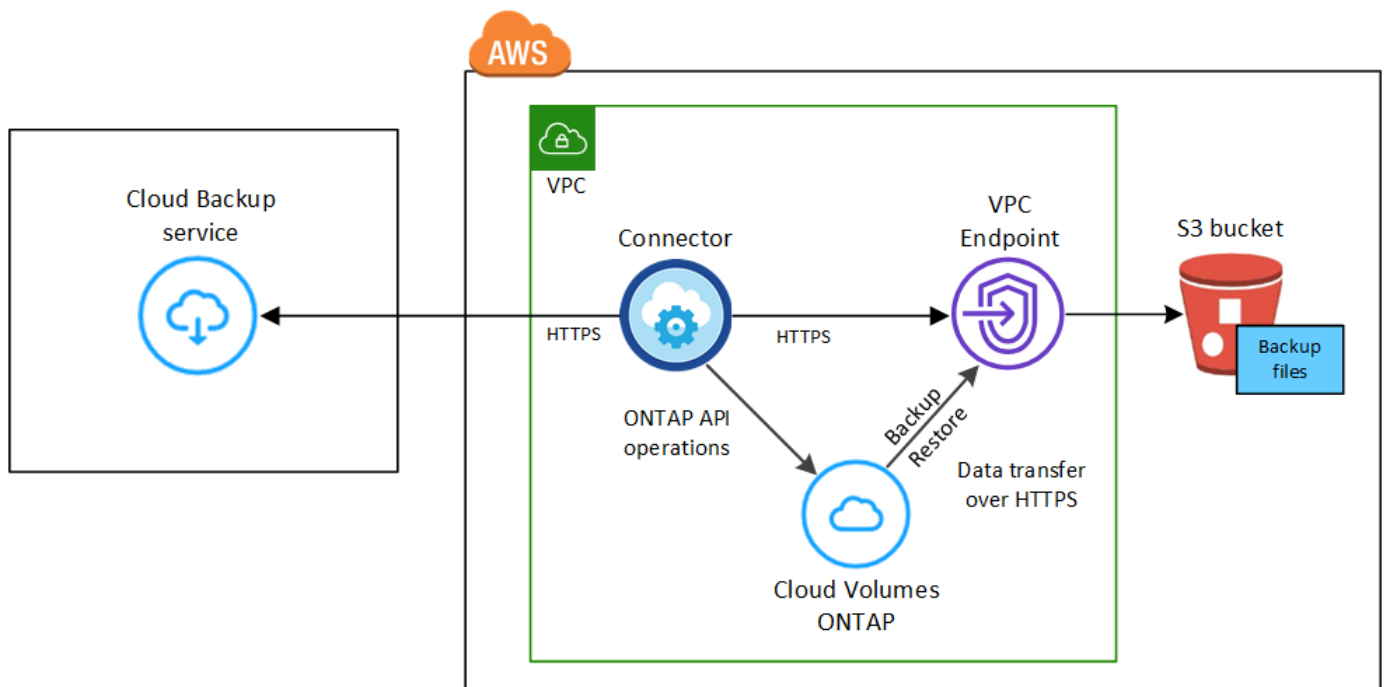
S3 Bucket Cloud Manager will create the S3 bucket for you. Wizard

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

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.



지원되는 **ONTAP** 버전

ONTAP 9.6 이상, ONTAP 9.8P11 이상 권장

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 에 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.

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 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.

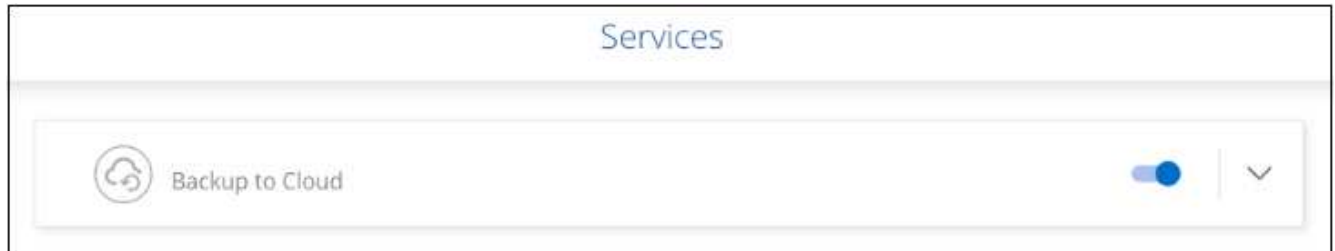
새로운 시스템에서 **Cloud Backup**을 활성화합니다

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.

백업에 대한 Amazon S3 대상이 Canvas에서 작업 환경으로 존재하는 경우 클러스터를 Amazon S3 작업 환경으로 끌어서 설정 마법사를 시작할 수 있습니다.



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.
 - 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.

Provider Settings

Provider Information

AWS Account:

AWS Access Key:

AWS Secret Key:

Location & Connectivity

Region:

Encryption ⓘ

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

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

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

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						
<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 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-1.png>

href="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-2.png""
class="bare">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 활성화 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.

A screenshot of a 'Provider Settings' form. It contains several sections: 'Azure Subscription' with a dropdown menu showing 'Azure_Subscription_1'; 'Region' with a dropdown menu showing 'Default_CM_Region'; 'Resource Group' with radio buttons for 'Create a new' (selected) and 'Use an existing'; 'Encryption Managed Keys' with radio buttons for 'Microsoft-managed' (selected) and 'Customer-managed'; and a 'Resource Group Name' text input field.

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): Access Tier: Azure Archive

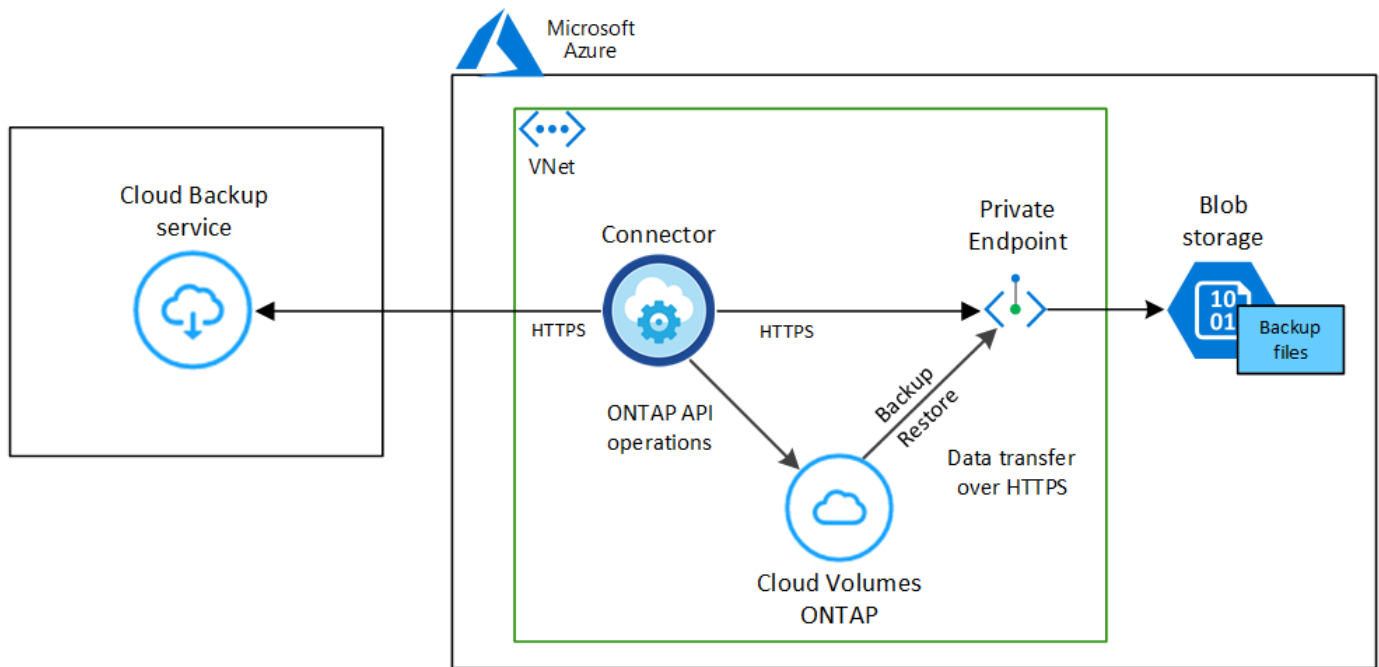
Storage Account Cloud Manager will create the storage account after you complete the wizard

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.



지원되는 **ONTAP** 버전

최소 ONTAP 9.7P5, ONTAP 9.8P11 이상을 사용하는 것이 좋습니다.

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.

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](#)".

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. 의 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.
 - 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

30

52

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 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

- 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

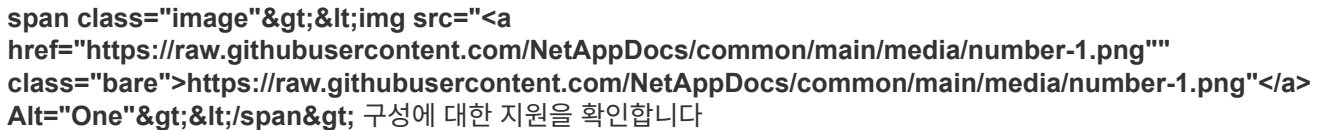
볼륨 또는 개별 파일을 복원합니다" Azure의 Cloud Volumes ONTAP 시스템 또는 사내 ONTAP 시스템으로 데이터를 이동합니다.

Cloud Volumes ONTAP 데이터를 Google 클라우드 스토리지에 백업

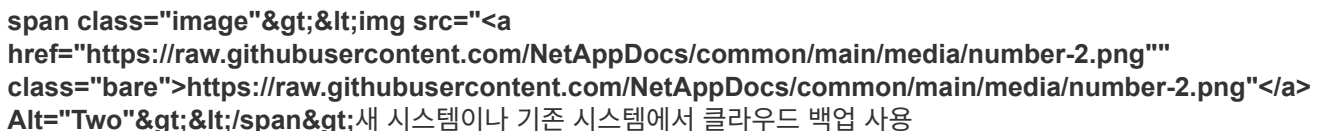
Cloud Volumes ONTAP에서 Google 클라우드 스토리지로 데이터 백업을 시작하는 몇 가지 단계를 완료하십시오.

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

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

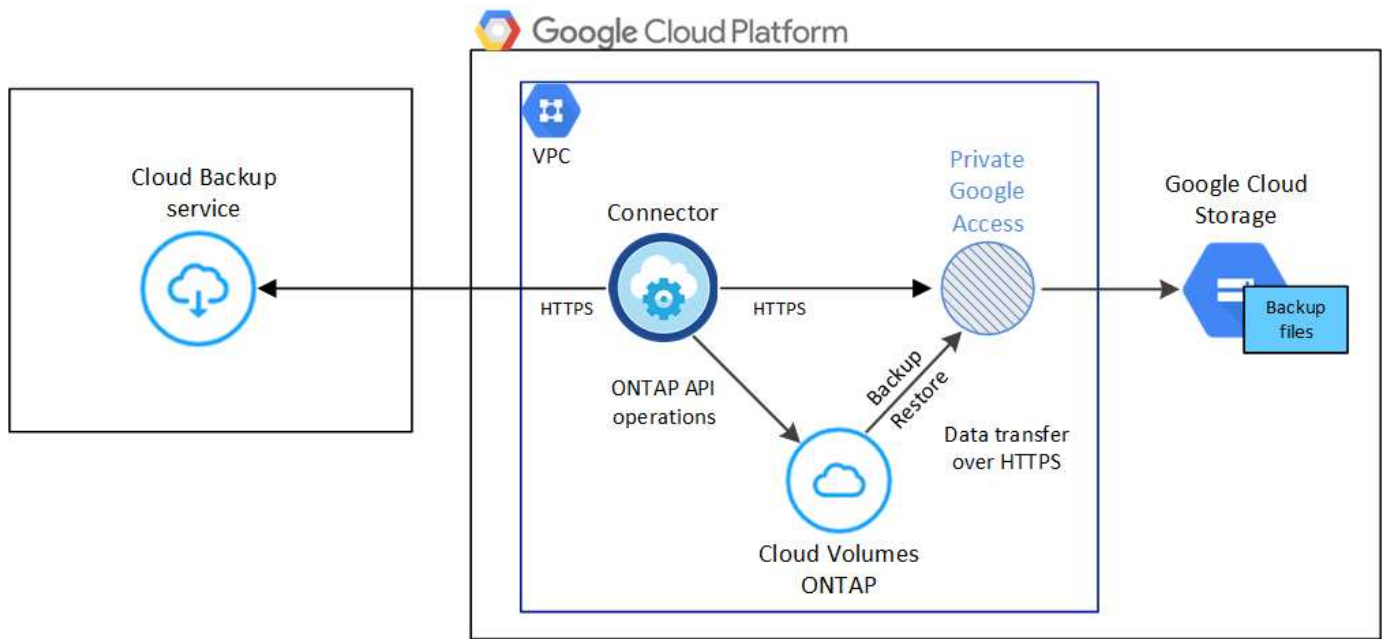
Google Cloud Storage Bucket Cloud Manager will create the Google Cloud Storage Bucket after you complete the wizard

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

최소 ONTAP 9.7P5, ONTAP 9.8P11 이상을 사용하는 것이 좋습니다.

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 가 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](#)".

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.

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.

Details & Credentials


Project1
Google Cloud Project

MPAWSSubscription1222
Marketplace Subscription

Edit Project

Details

Working Environment Name (Cluster Name)
TamiVSA

Service Account 

Service Account Name
ServiceAccount1

+ Add Labels Optional Field | Up to four labels

Credentials

User Name
admin

Password

Confirm Password

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.



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.

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

30

52

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".

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

☒ 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 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 생성하고 관리합니다. 또한 S3 버킷에서 데이터를 읽고 쓸 수 있도록 사내 ONTAP 클러스터에 대한 권한을 설정해야 합니다.

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.

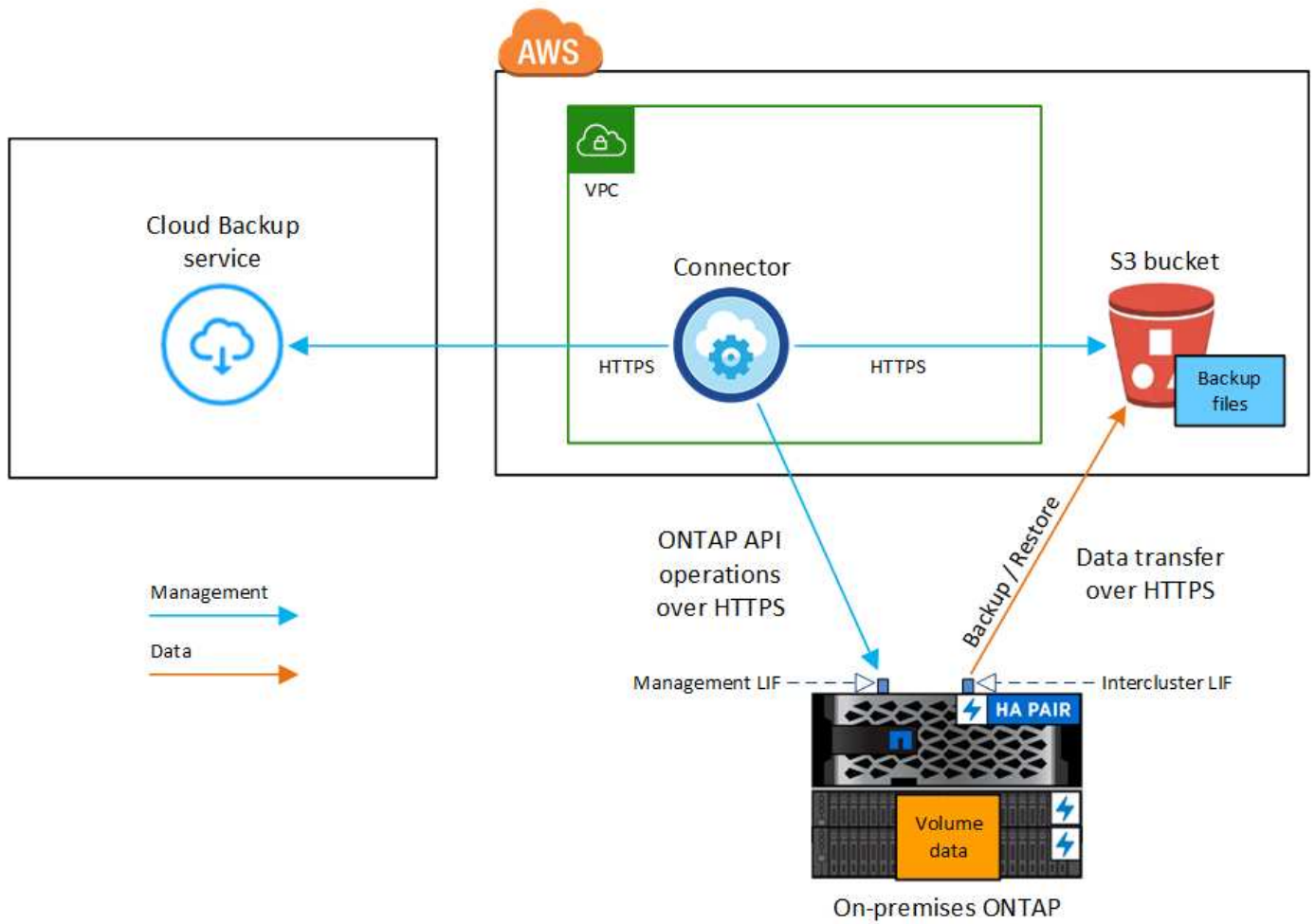
[볼륨에서 Cloud Backup을 활성화하는 방법을 확인하십시오.](#)

연결 옵션에 대한 네트워크 다이어그램

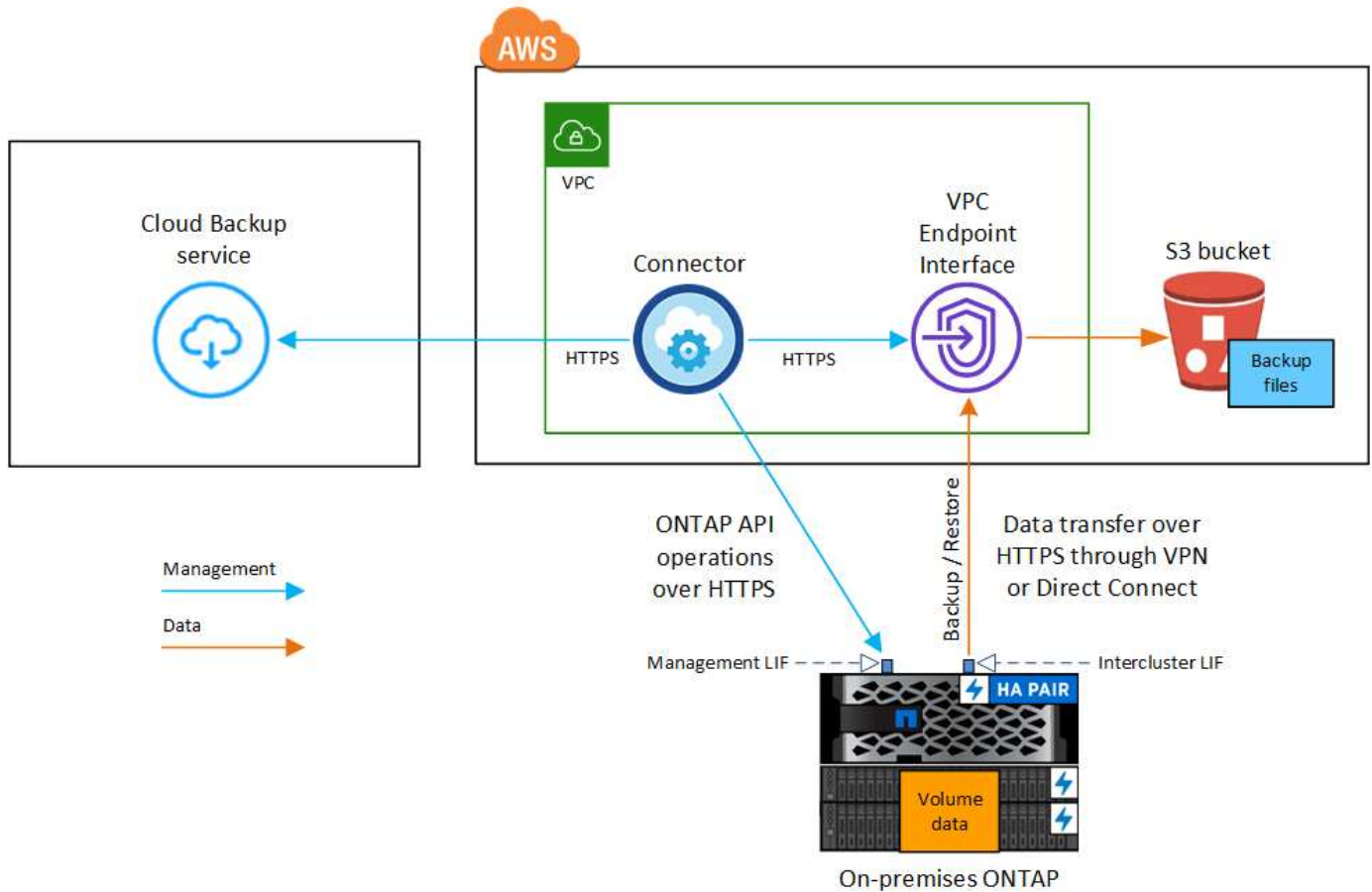
사내 ONTAP 시스템에서 AWS S3로 백업을 구성할 때 두 가지 연결 방법을 사용할 수 있습니다.

- 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.



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.

- 볼륨이 있는 스토리지 VM에 대해 DNS 서버가 구성되어 있어야 합니다. 자세한 내용은 를 참조하십시오 ["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.

- Connector의 S3 버킷 생성 및 관리 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. 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.

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"](#).

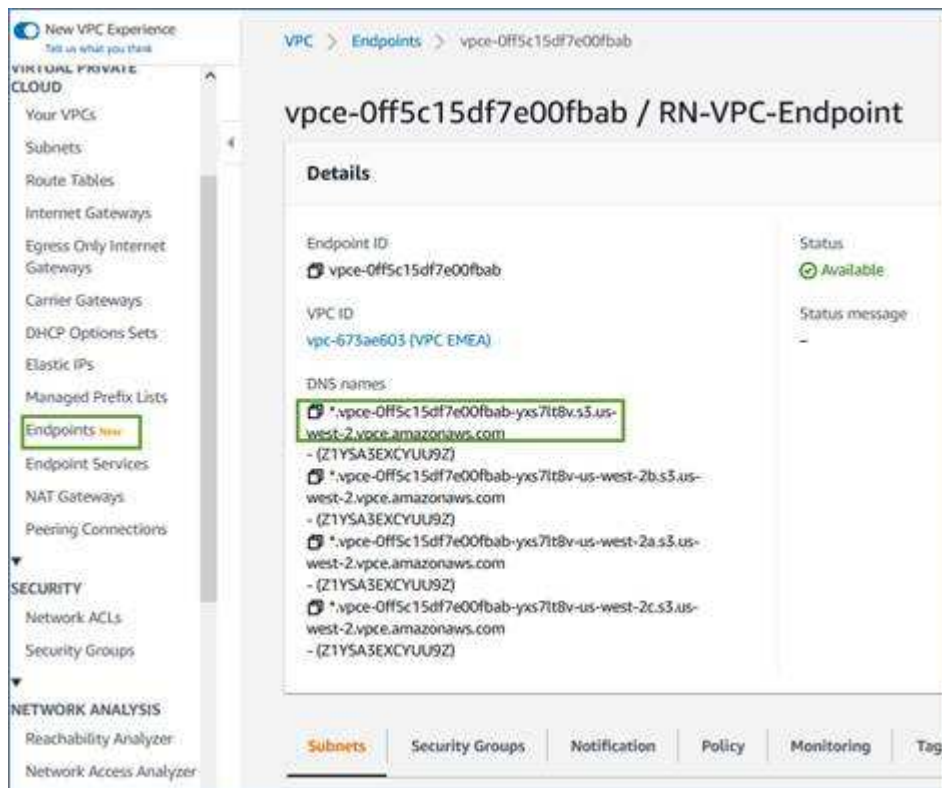
1. Amazon VPC 콘솔 또는 명령줄을 사용하여 인터페이스 엔드포인트 구성을 생성합니다. ["Amazon S3에 AWS PrivateLink를 사용하는 방법에 대한 자세한 정보를 확인하십시오"](#).
2. Cloud Manager Connector와 연결된 보안 그룹 구성을 수정합니다. 정책을 "사용자 지정"("전체 액세스"에서)으로 변경해야 하며 반드시 다음을 수행해야 합니다 [백업 정책에서 S3 권한을 추가합니다](#) 앞서 설명한 것처럼.



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 표시된 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.

백업에 대한 Amazon S3 대상이 Canvas에서 작업 환경으로 존재하는 경우 클러스터를 Amazon S3 작업 환경으로 끌어서 설정 마법사를 시작할 수 있습니다.



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	Location & Connectivity
AWS Account AWS_Account_1	Region us-east-2
AWS Access Key Enter AWS Access Key	Encryption Encryption Key Type: AWS SSE-S3 Change Key
AWS Secret Key Enter AWS Secret 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

IP_Space_1

☒ 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.

- 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 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) 30

Storage Class S3 Glacier

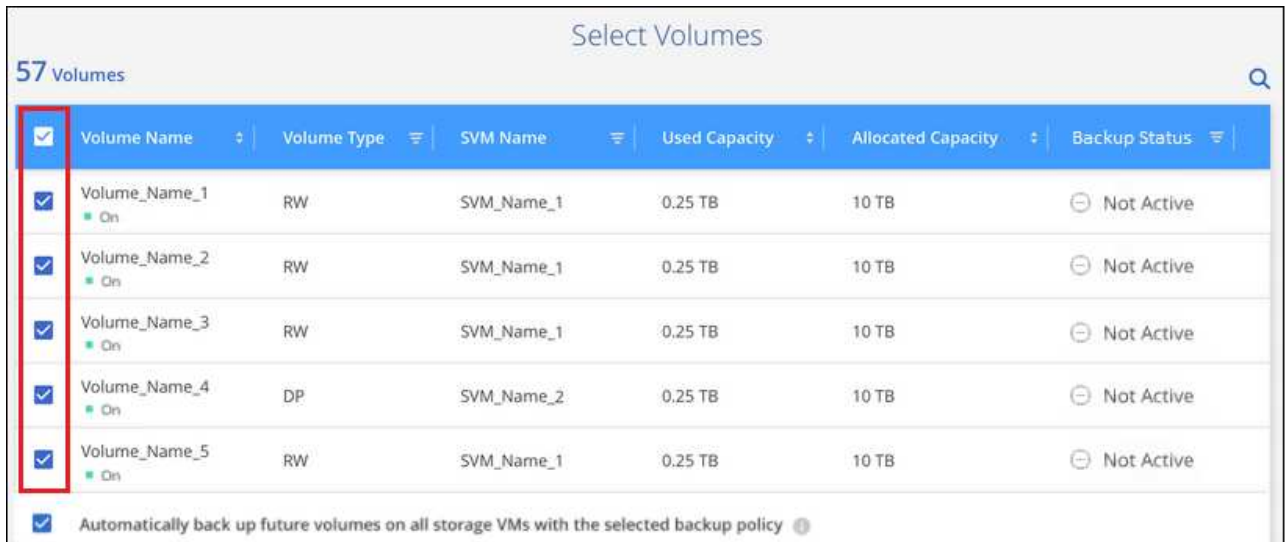
S3 Glacier

S3 Glacier Deep Archive

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

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.



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

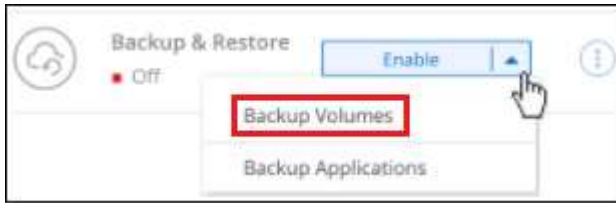
다음 단계를 따라 빠르게 시작하거나 나머지 섹션을 아래로 스크롤하여 자세한 내용을 확인하십시오.

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

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

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 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 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

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

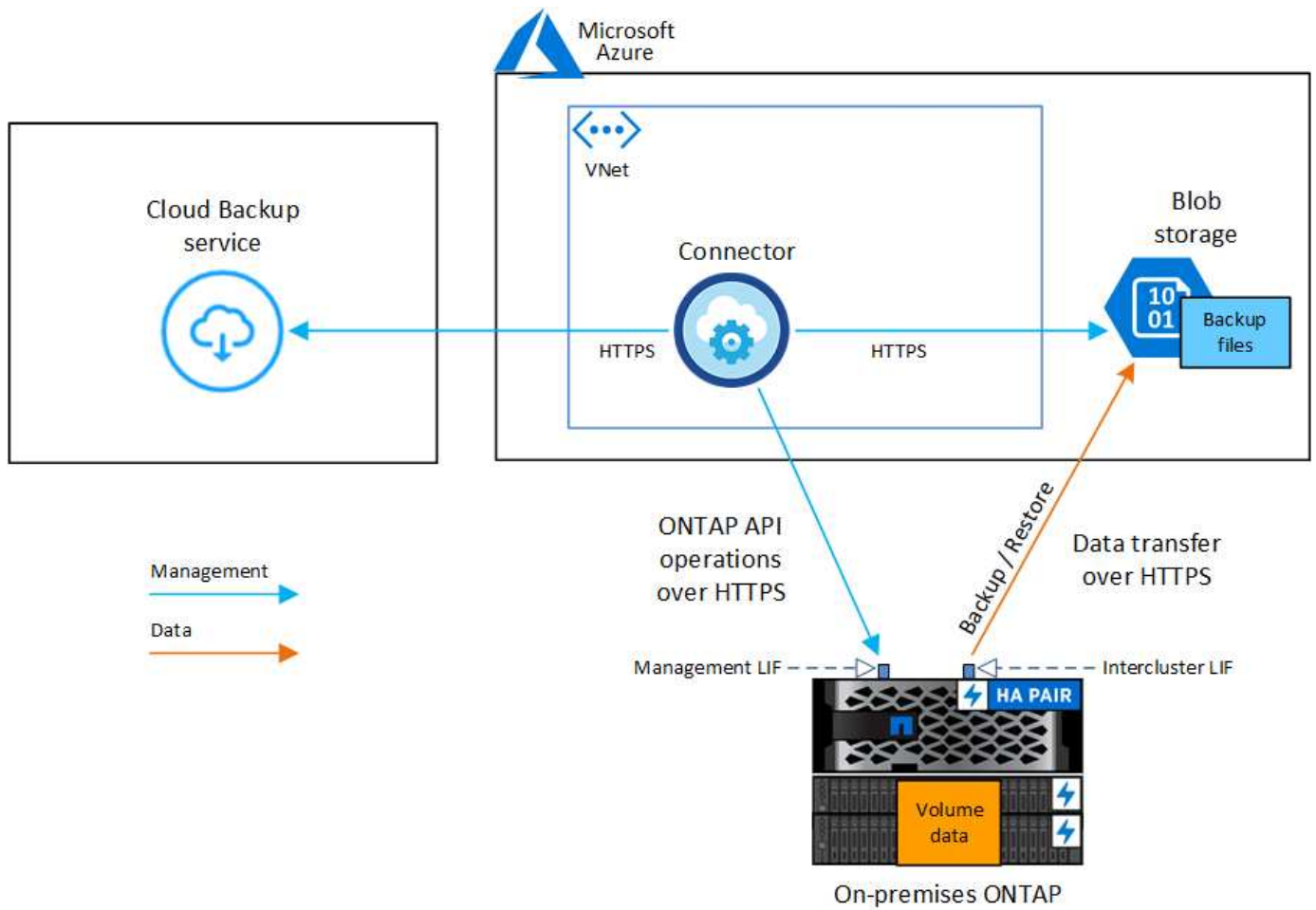
온프레미스 볼륨을 Azure Blob 저장소에 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

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

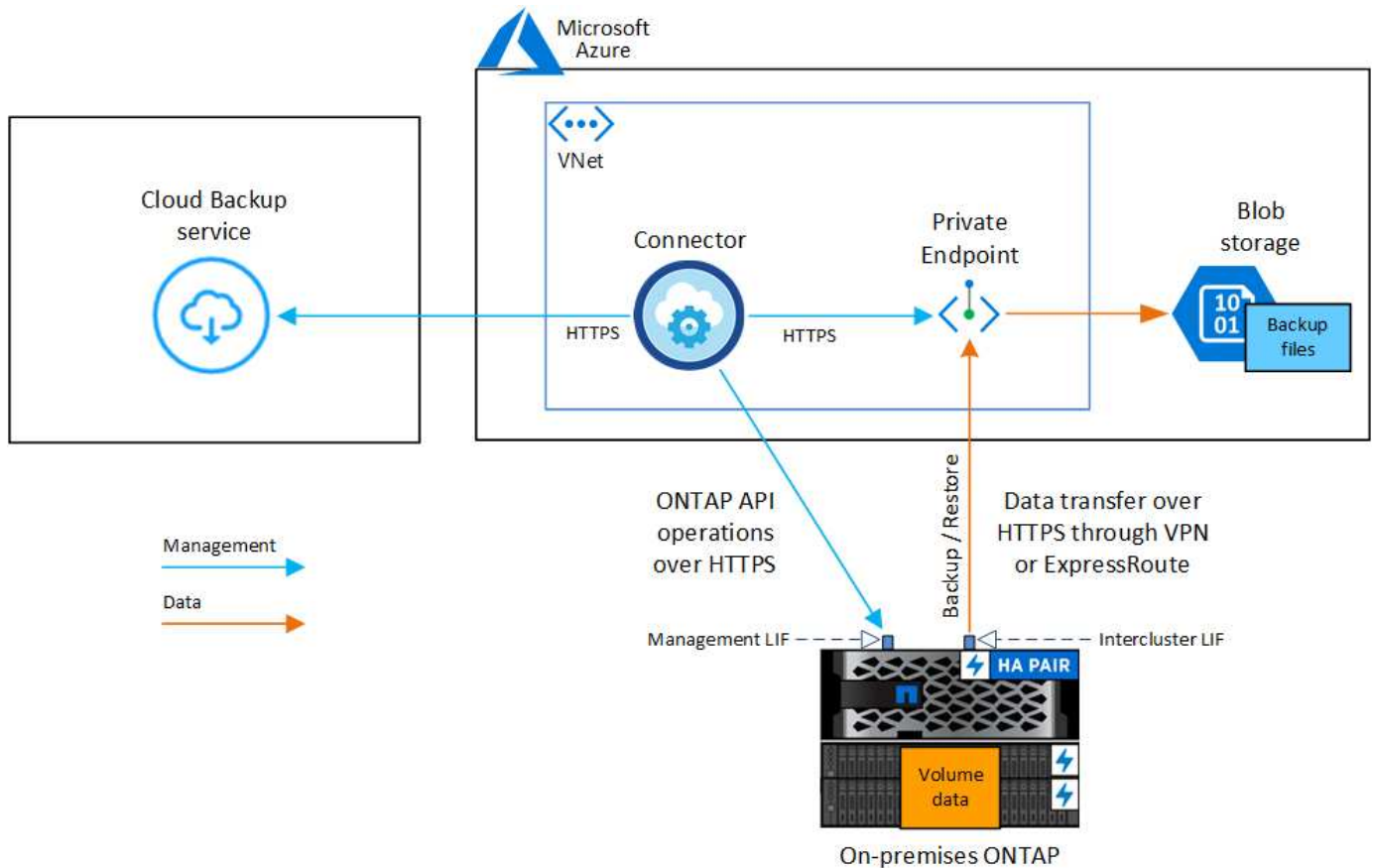
- 공용 연결 - 공용 Azure 끝점을 사용하여 ONTAP 시스템을 Azure Blob 저장소에 직접 연결합니다.
- 비공개 연결 - VPN 또는 ExpressRoute를 사용하여 전용 IP 주소를 사용하는 VNET 전용 엔드포인트를 통해 트래픽을 라우팅합니다.

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

55



다음 그림에서는 * private connection * 메서드와 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

- 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

- ONTAP 클러스터는 백업 및 복원 작업을 위해 인터클러스터 LIF에서 Azure Blob 스토리지로의 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. 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 [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

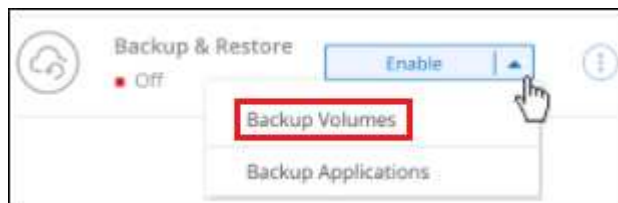
- 기본 Microsoft 관리 암호화 키를 사용하는 대신 정품 인증 마법사에서 데이터 암호화에 사용자 지정 관리 키를 사용할 수 있습니다. 이 경우 Azure 가입, 키 저장소 이름 및 키가 필요합니다. "[자신의 키를 사용하는 방법을 확인하십시오](#)".
- 온프레미스 데이터 센터에서 VNET로 공용 인터넷을 통해 보다 안전하게 연결하려면 활성화 마법사에서 Azure 프라이빗 끝점을 구성하는 옵션이 있습니다. 이 경우 이 연결에 대한 VNET 및 서브넷을 알아야 합니다. "[개인 엔드포인트 사용에 대한 자세한 내용을 참조하십시오](#)".

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.



- 공급자로서 Microsoft Azure를 선택하고 * 다음 * 을 클릭합니다.
- 제공업체 세부사항을 입력하고 * 다음 * 을 클릭합니다.
 - 백업에 사용되는 Azure 가입 및 백업을 저장할 Azure 지역
 - Blob 컨테이너를 관리하는 리소스 그룹 - 새 리소스 그룹을 만들거나 기존 리소스 그룹을 선택할 수 있습니다.
 - 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.
- 백업할 볼륨이 상주하는 ONTAP 클러스터의 IPspace 이 IPspace용 인터클러스터 LIF는 아웃바운드 인터넷 액세스를 가져야 합니다.
 - 필요에 따라 Azure 프라이빗 끝점을 구성할지 여부를 선택합니다. ["개인 엔드포인트 사용에 대한 자세한 내용을 참조하십시오"](#).

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

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ Monthly

Number of backups to retain:

☐ Hourly
 ☒ Daily
 ☐ Weekly
 ☐ 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

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 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_2 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_3 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_4 <small>On</small>	DP	SVM_Name_2	0.25 TB	10 TB	<input type="radio"/> Not Active
<input checked="" type="checkbox"/>	Volume_Name_5 <small>On</small>	RW	SVM_Name_1	0.25 TB	10 TB	<input type="radio"/> 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" 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.

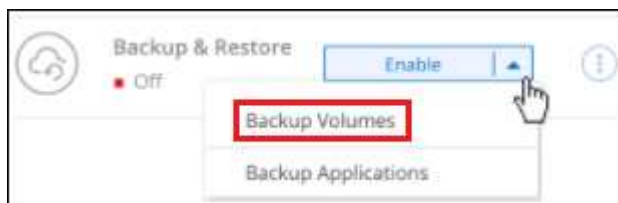
빠른 시작

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

`span class="image"><img src="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 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

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

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.

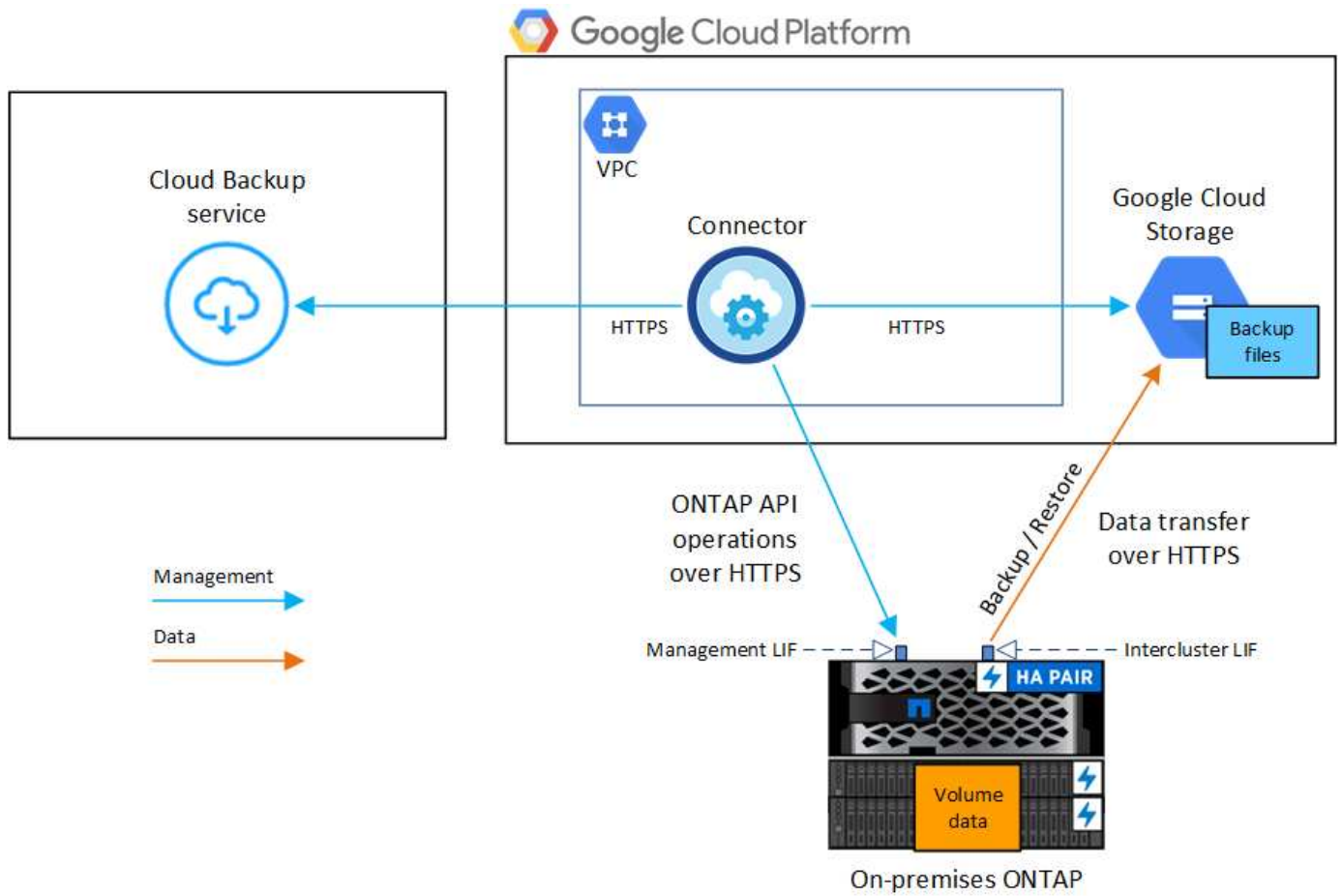
요구 사항

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

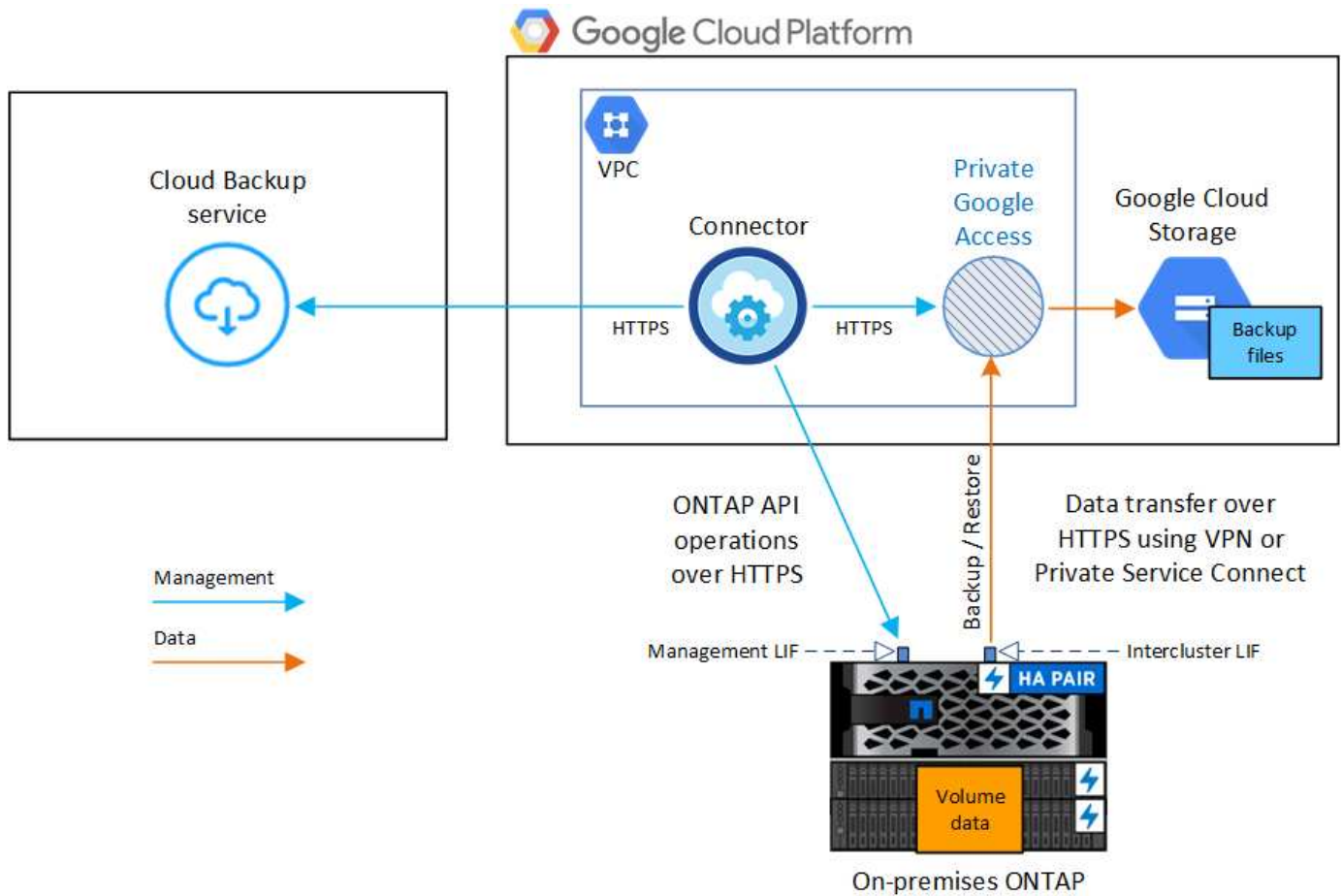
사내 ONTAP 시스템에서 Google 클라우드 스토리지로 백업을 구성할 때 두 가지 연결 방법을 사용할 수 있습니다.

- **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 * public connection * 메서드와 구성 요소 간에 준비해야 하는 연결을 보여 줍니다.



다음 그림에서는 * private connection * 메서드와 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

- 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

- 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.

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

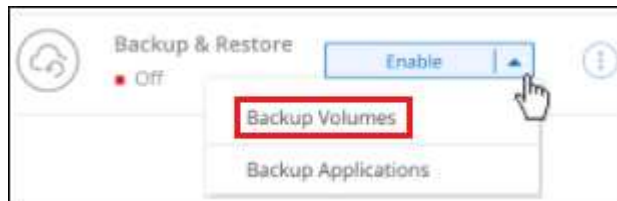
나중에 백업 서비스를 구성할 때 Cloud Backup에 키를 입력해야 합니다.

클라우드 백업 활성화

사내 작업 환경에서 언제든지 직접 Cloud Backup을 사용할 수 있습니다.

단계

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



2. 공급자로 Google Cloud를 선택하고 * 다음 * 을 클릭합니다.

3. 제공업체 세부사항을 입력하고 * 다음 * 을 클릭합니다.

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

4. 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.

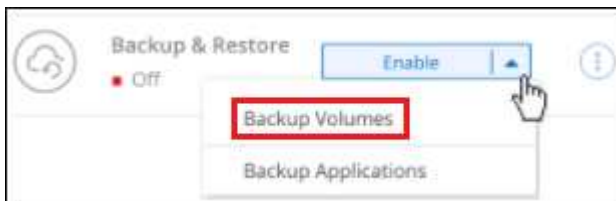
빠른 시작

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

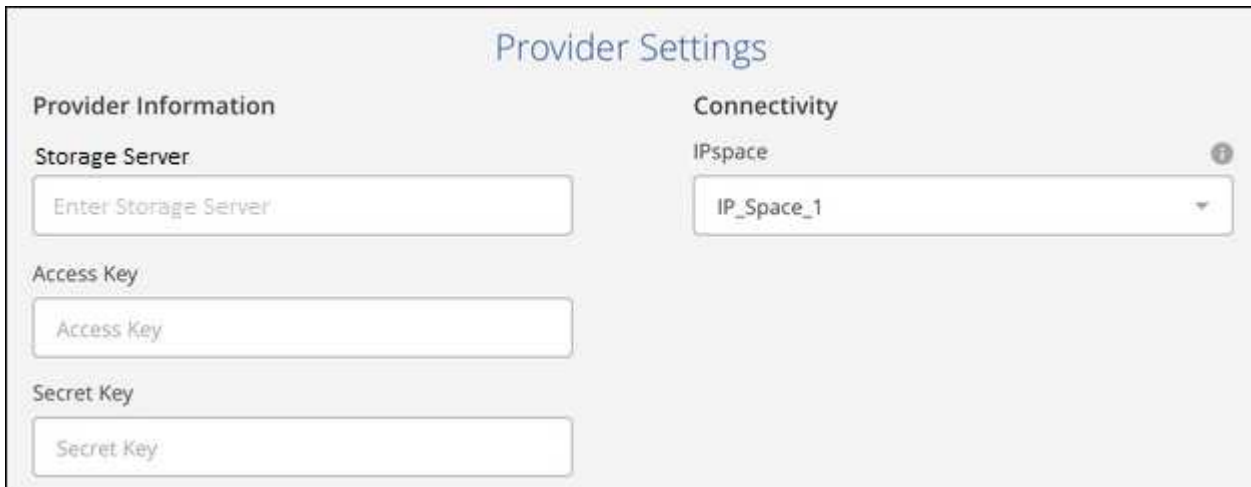
`span class="image">&img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png" Alt="One">&span>` 구성에 대한 지원을 확인합니다

- 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.
 - 커넥터는 인터넷에 접속하거나 접속하지 않고 사이트에 설치할 수 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 방법을 따릅니다.

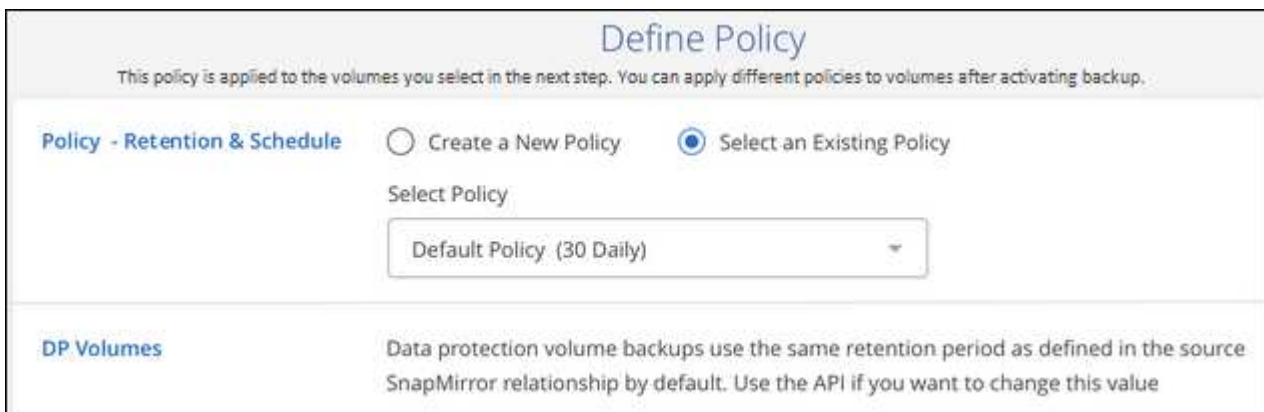


공급자로 StorageGRID를 선택하고 StorageGRID 서버 및 서비스 계정 세부 정보를 입력합니다. 또한 볼륨이 상주하는 ONTAP 클러스터에서 IPspace를 지정해야 합니다.



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 'IP_Space_1' selected. A small information icon is visible next to the dropdown.

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 title bar and a subtitle: '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 'Default Policy (30 Daily)' selected. At the bottom, there is a section titled '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'.

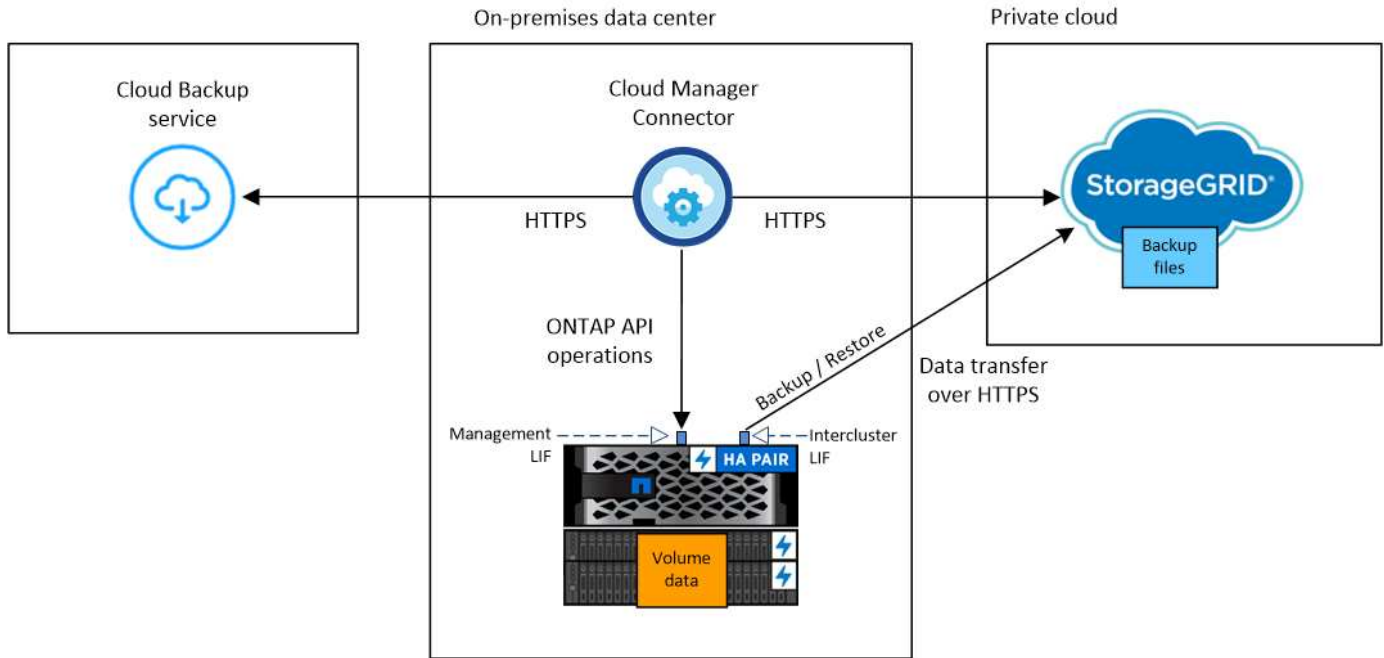
Select Volumes(볼륨 선택) 페이지의 기본 백업 정책을 사용하여 백업할 볼륨을 식별합니다. 특정 볼륨에 서로 다른 백업 정책을 할당하려면 추가 정책을 생성한 후 나중에 볼륨에 적용할 수 있습니다.

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.



커넥터와 사내 ONTAP 시스템이 인터넷에 연결되지 않은 온프레미스 위치에 설치된 경우 StorageGRID 시스템은 동일한 사내 데이터 센터에 있어야 합니다.

ONTAP 클러스터 준비

볼륨 데이터 백업을 시작하려면 Cloud Manager에서 사내 ONTAP 클러스터를 검색해야 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

- 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(Connector가 "어두운" 사이트에 설치된 경우 필요하지 않음).
- 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. 커넥터는 인터넷에 접속하거나 접속하지 않고 사이트에 설치할 수 있습니다.

- "[커넥터에 대해 자세히 알아보십시오](#)"

- "인터넷에 액세스할 수 있는 Linux 호스트에 커넥터 설치"
- "인터넷에 액세스하지 않고 Linux 호스트에 커넥터 설치"
- "커넥터 간 전환"



Cloud Backup 기능은 Cloud Manager Connector에 내장되어 있습니다. 인터넷에 연결되지 않은 사이트에 설치한 경우 새 기능에 액세스하려면 커넥터 소프트웨어를 정기적으로 업데이트해야 합니다. 를 확인하십시오 "클라우드 백업 새로운 기능" 각 Cloud Backup 릴리즈의 새로운 기능을 보려면 ~ 단계를 따르십시오 "Connector 소프트웨어를 업그레이드합니다" 새 기능을 사용하려는 경우

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(커넥터가 "어두운" 사이트에 설치된 경우 필요하지 않음)

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: S

3.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(커넥터가 "어두운" 사이트에 설치된 경우 필요하지 않음).

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

The screenshot shows the 'Provider Settings' configuration page. It is divided into two main sections: 'Provider Information' and 'Connectivity'. Under 'Provider Information', there are three input fields: 'Storage Server' (placeholder: Enter Storage Server), 'Access Key' (placeholder: Access Key), and 'Secret Key' (placeholder: Secret Key). Under 'Connectivity', there is a dropdown menu for 'IPspace' with 'IP_Space_1' selected. A small information icon is visible next to the IPspace dropdown.

서비스가 시작된 후에는 이 정보를 변경할 수 없습니다.

- 3. Define Policy_페이지에서 기본 백업 일정 및 보존 값을 선택하고 * Next * 를 클릭합니다.

The screenshot shows the 'Define Policy' configuration page. At the top, it states: '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 for 'Select Policy' with 'Default Policy (30 Daily)' selected. At the bottom, there is a section titled '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'.

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 볼륨 또는 개별 파일을 복원합니다" 사내 ONTAP 시스템으로.

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.



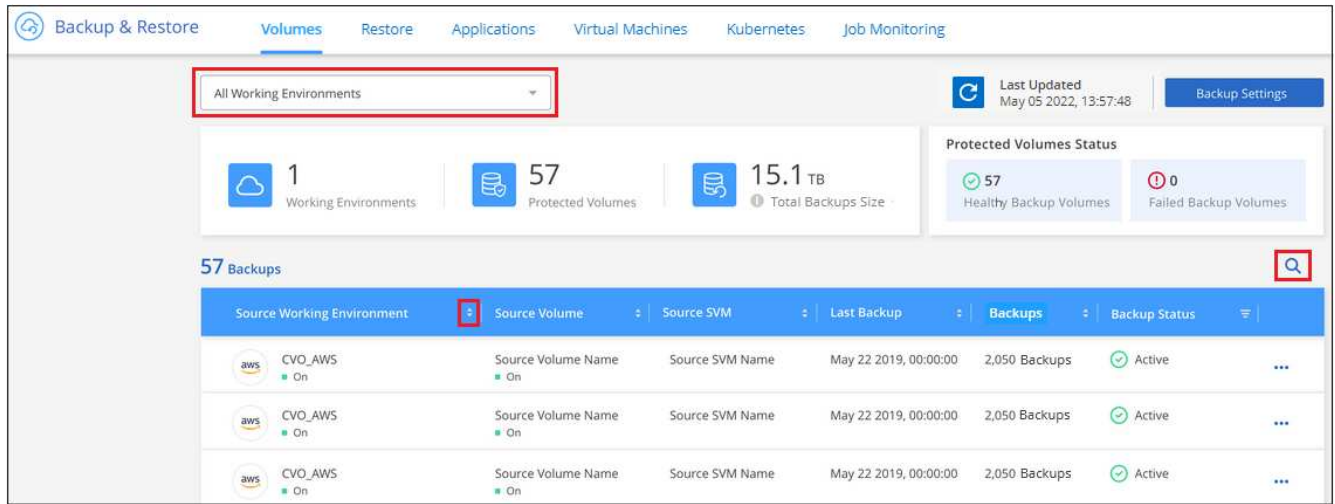
클라우드 공급자 환경에서 직접 백업 파일을 관리하거나 변경하지 마십시오. 이로 인해 파일이 손상되어 지원되지 않는 구성이 발생할 수 있습니다.

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.



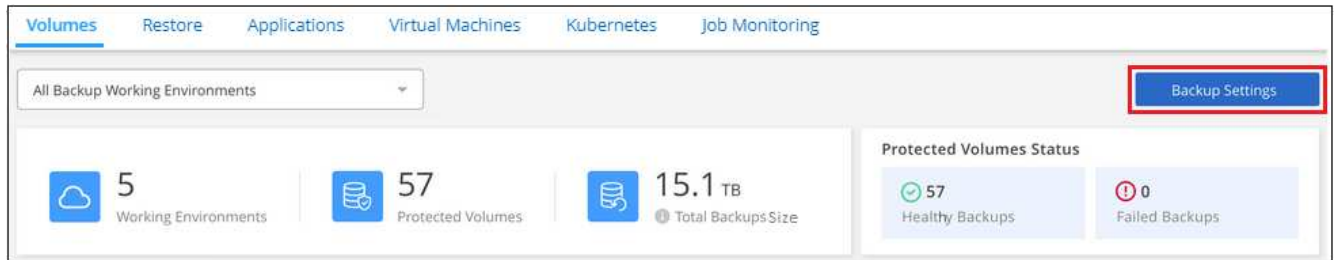
특정 작업 환경에서 특정 볼륨을 찾는 경우 작업 환경 및 볼륨으로 목록을 세분화하거나 검색 필터를 사용할 수 있습니다.

볼륨 백업 활성화 및 비활성화

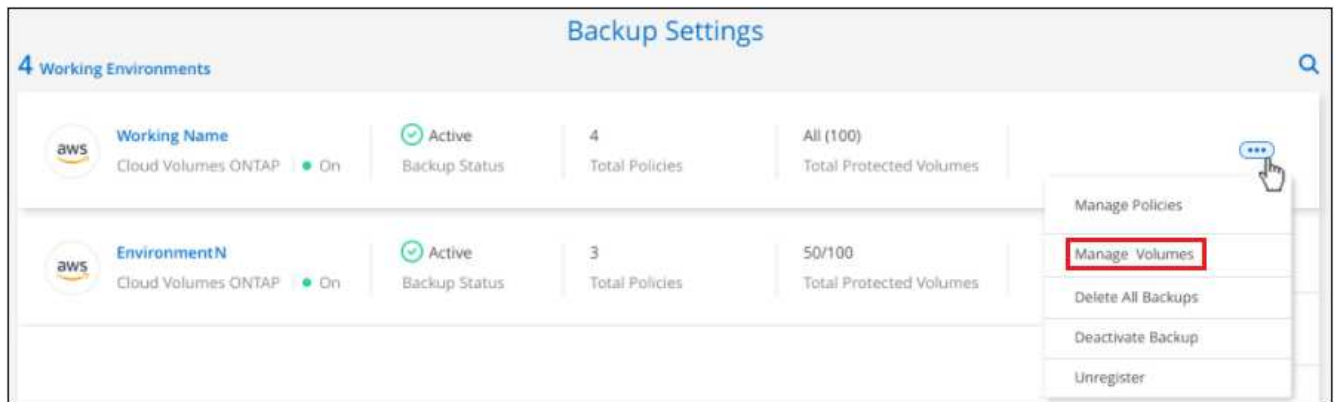
해당 볼륨의 백업 복사본이 필요하지 않고 백업 저장 비용을 지불하지 않으려는 경우 볼륨 백업을 중지할 수 있습니다. 현재 백업 중이 아닌 경우 백업 목록에 새 볼륨을 추가할 수도 있습니다.

단계

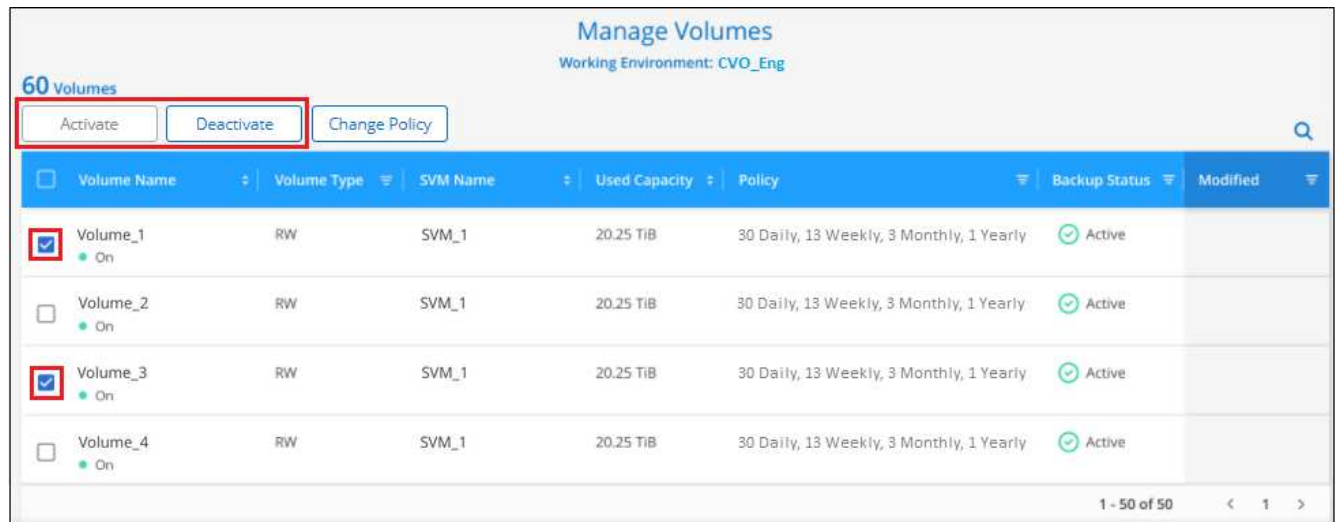
1. 볼륨 * 탭에서 * 백업 설정 * 을 선택합니다.



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.

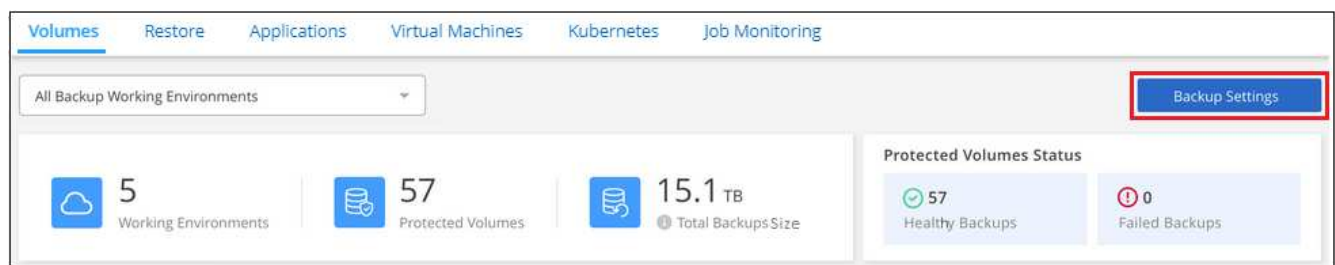
- 참고: * 볼륨이 백업되지 않도록 하는 경우 클라우드 공급자가 백업이 사용하는 용량에 대한 객체 스토리지 비용을 계속 청구합니다 백업을 삭제합니다.

기존 백업 정책 편집

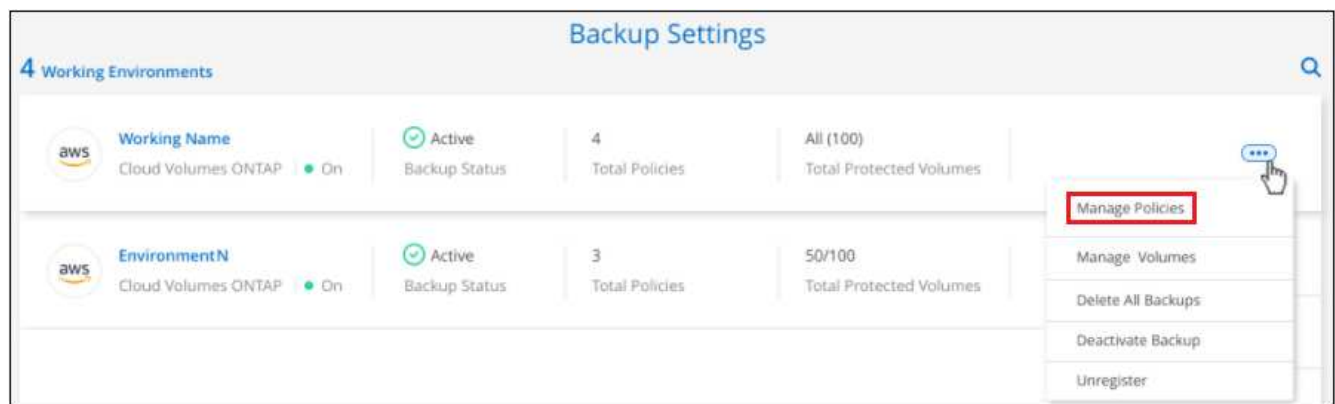
작업 환경의 볼륨에 현재 적용된 백업 정책의 속성을 변경할 수 있습니다. 백업 정책을 변경하면 정책을 사용하는 모든 기존 볼륨에 영향을 줍니다.

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.

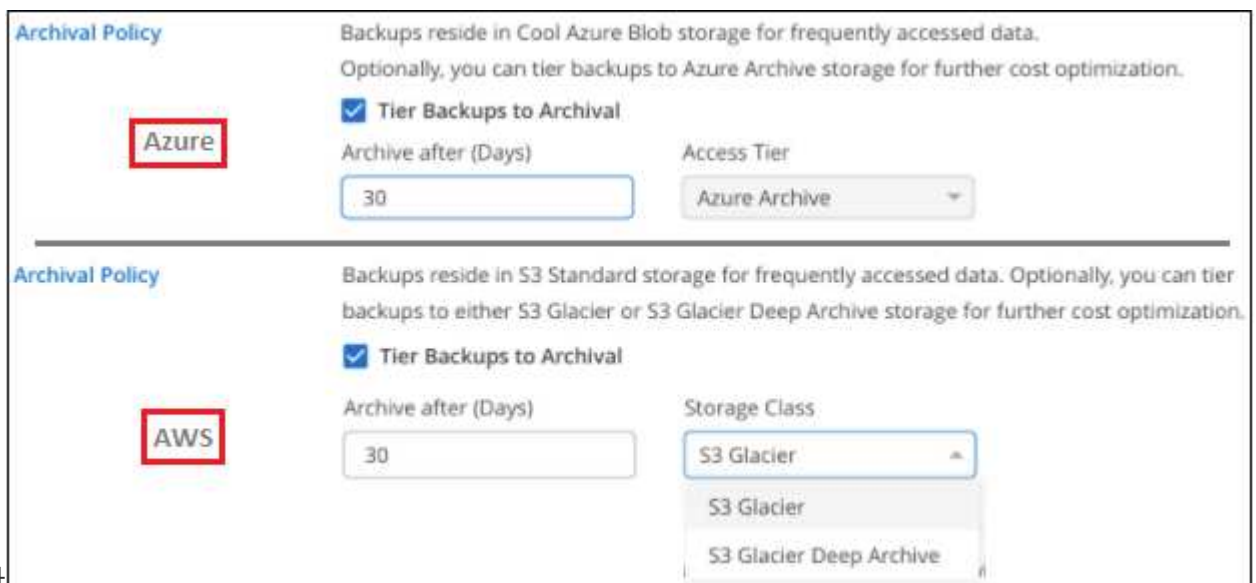


클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 일정 일 후에 아카이브 스토리지에 대한 백업 계층화를 활성화 또는 비활성화할 수도 있습니다.

"AWS 아카이브 스토리지 사용에 대해 자세히 알아보십시오".

"Azure 아카이브 스토리지 사용에 대해 자세히 알아보십시오".

를



누릅니다

+ 아카이브 스토리지로 계층화된 백업 파일은 아카이브로 백업을 계층화하는 것을 중지하면 해당 계층에 남아 있습니다.

이러한 백업 파일은 자동으로 표준 계층으로 다시 이동되지 않습니다.

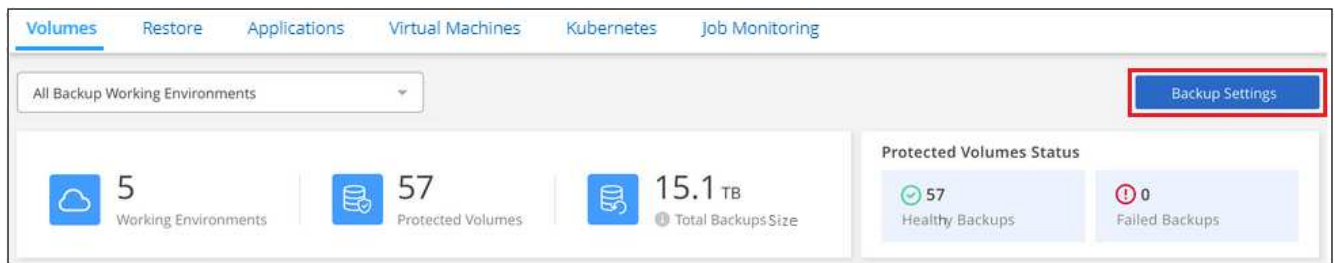
새 백업 정책 추가

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.

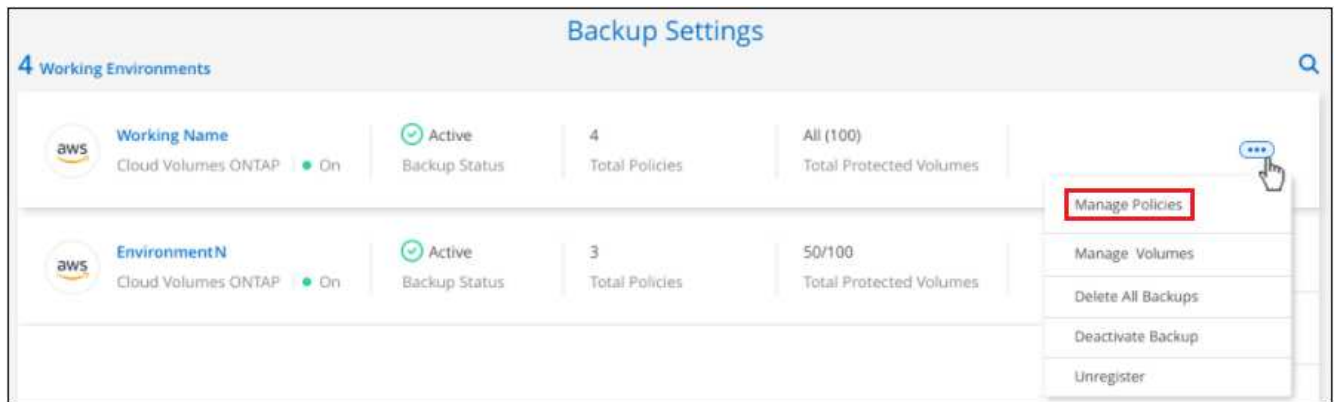
작업 환경의 특정 볼륨에 새 백업 정책을 적용하려면 먼저 작업 환경에 백업 정책을 추가해야 합니다. 그러면 됩니다 [해당 작업 환경의 볼륨에 정책을 적용합니다](#).

단계

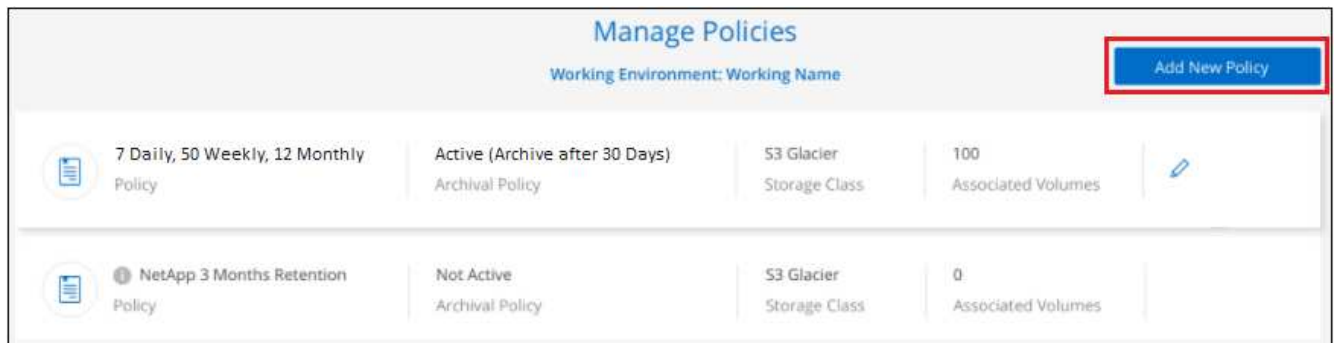
1. 볼륨 * 탭에서 * 백업 설정 * 을 선택합니다.



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 xx

☒ Daily Number of backups to retain 30

☐ Weekly Number of backups to retain xx

☐ Monthly Number of backups to retain xx

클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 일정 일 후에 아카이브 스토리지에 대한 백업 계층화를 활성화 또는 비활성화할 수도 있습니다.

"AWS 아카이브 스토리지 사용에 대해 자세히 알아보십시오".

"Azure 아카이브 스토리지 사용에 대해 자세히 알아보십시오".

를

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
 30 Azure Archive

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
 30 S3 Glacier
 S3 Glacier
 S3 Glacier Deep Archive

누릅니다

기존 볼륨에 할당된 정책을 변경합니다

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

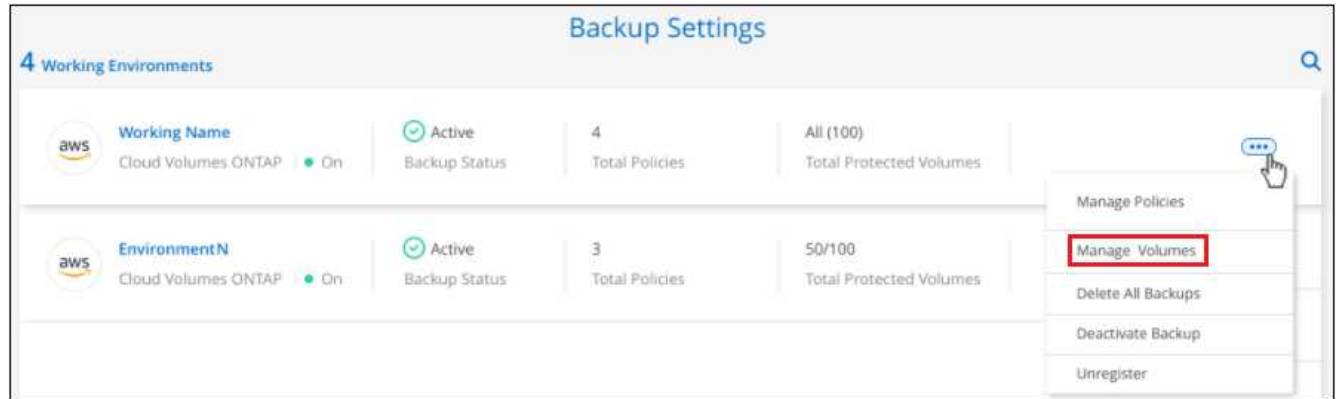
볼륨에 적용할 정책이 이미 있어야 합니다. [작업 환경에 대한 새 백업 정책을 추가하는 방법에 대해 알아보십시오.](#)

단계

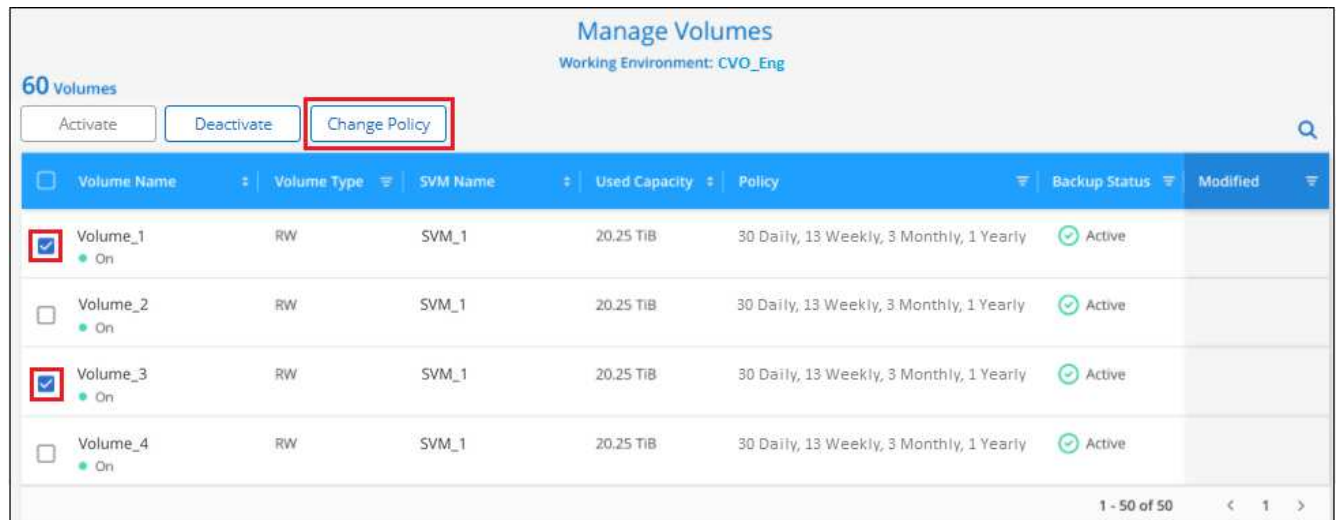
1. 볼륨 * 탭에서 * 백업 설정 * 을 선택합니다.



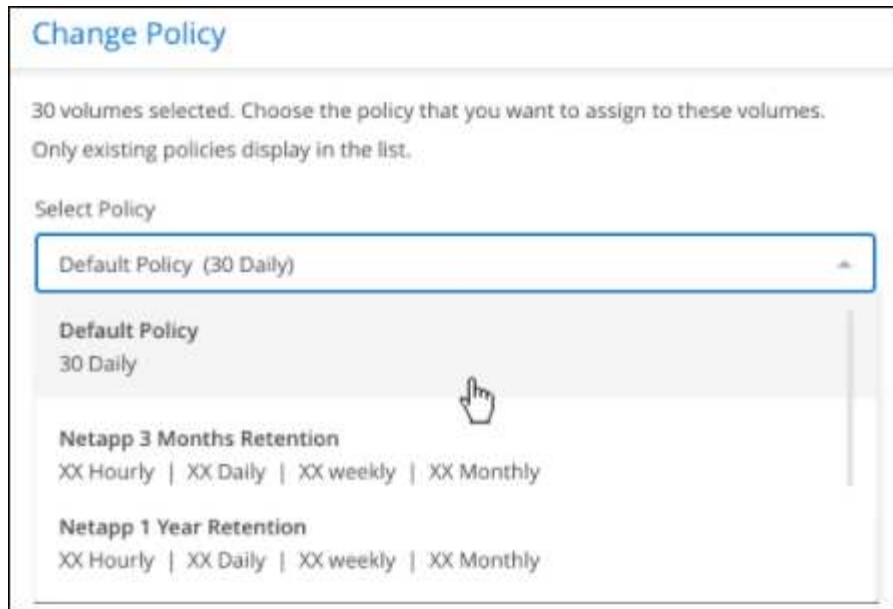
2. 백업 설정 페이지에서 _을(를) 클릭합니다 ... 볼륨이 있는 작업 환경의 경우 * 볼륨 관리 * 를 선택합니다.



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

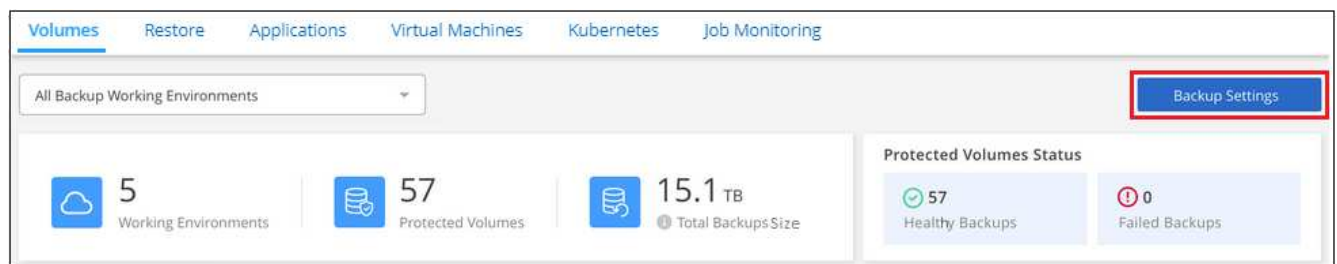
ONTAP 클러스터에서 클라우드 백업을 처음 활성화할 때 새로 생성된 볼륨에 백업 정책을 자동으로 할당하는 옵션을 선택하지 않은 경우 나중에 백업 설정 페이지에서 이 옵션을 선택할 수 있습니다. 새로 생성된 볼륨에 백업 정책을 할당하면 모든 데이터가 보호됩니다.

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

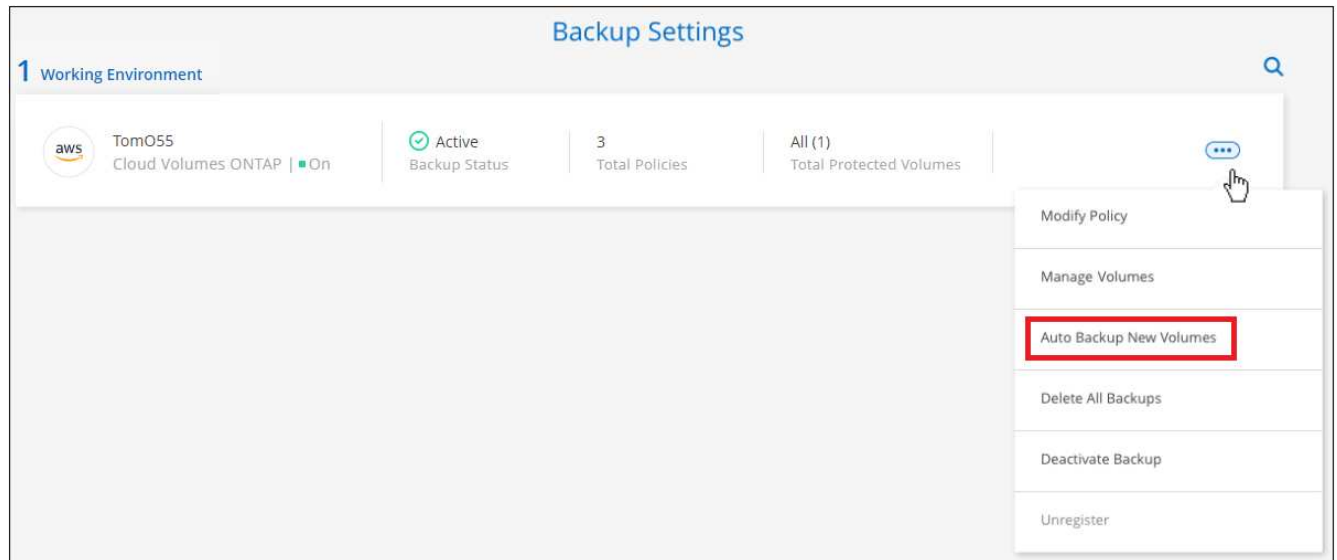
새로 생성된 볼륨이 자동으로 백업되지 않도록 이 설정을 비활성화할 수도 있습니다. 이 경우 나중에 백업하려는 특정 볼륨에 대해 백업을 수동으로 설정해야 합니다.

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"](#)

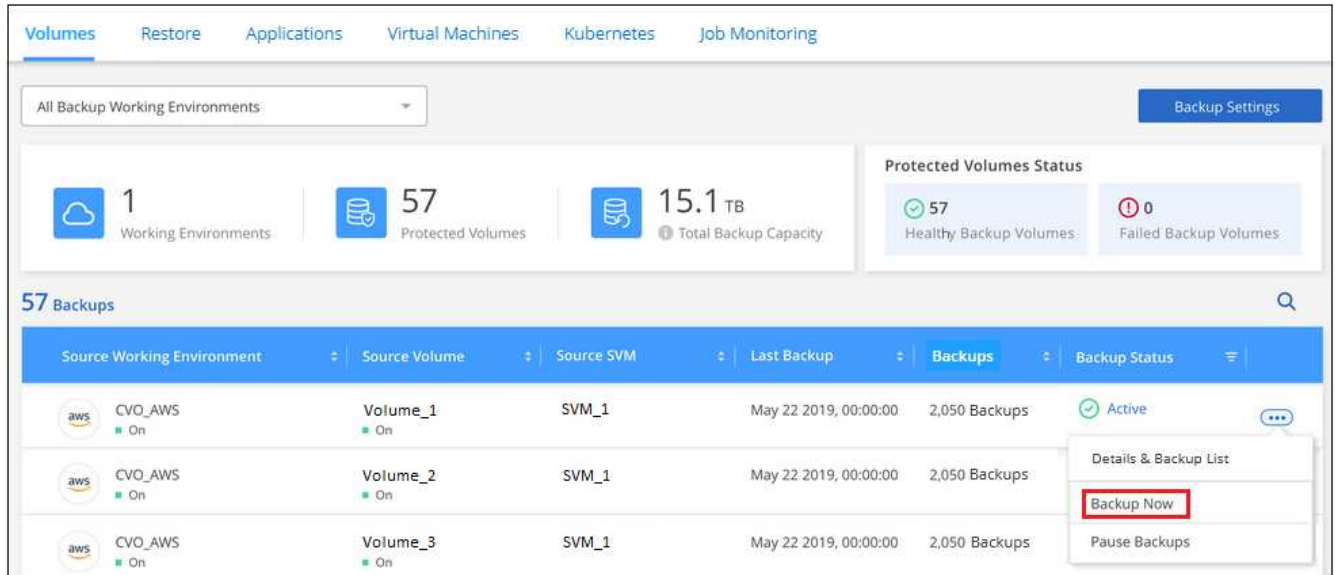
스냅샷을 삭제하는 방법을 알아봅니다".



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, Applications, Virtual Machines, Kubernetes, and Job Monitoring. Below the tabs, there's a dropdown menu for 'All Backup Working Environments' and a 'Backup Settings' button. The main dashboard displays statistics: 1 Working Environments, 57 Protected Volumes, and 15.1 TB Total Backup Capacity. A 'Protected Volumes Status' section shows 57 Healthy Backup Volumes and 0 Failed Backup Volumes. Below this, a table lists 57 backups. The first backup is highlighted, and a dropdown menu is open, showing options: 'Details & Backup List', '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 information is organized into three columns: Source, Destination, and Backup Information. Below the columns is a table of 2,050 backups.

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

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

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

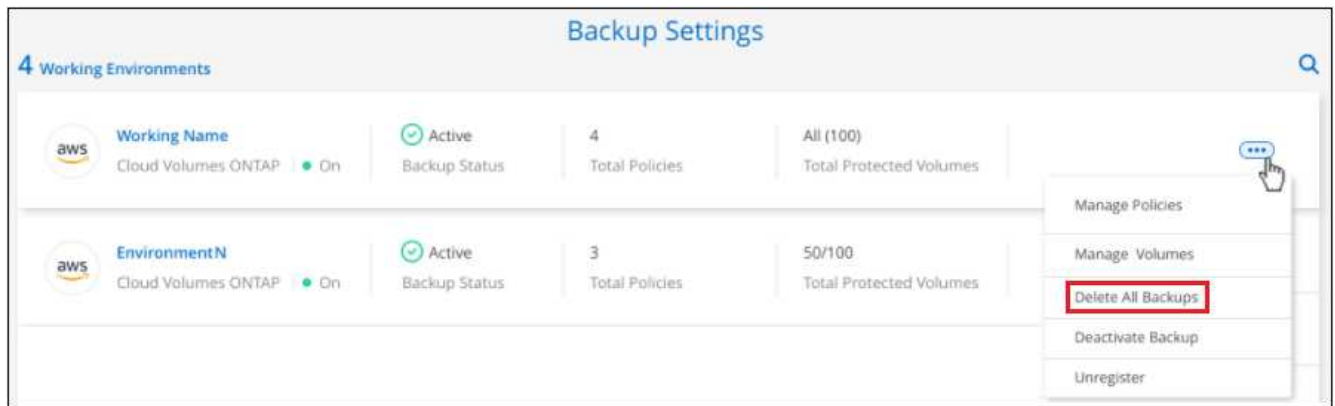
작업 환경의 모든 백업을 삭제해도 이 작업 환경의 볼륨에 대한 향후 백업이 비활성화되지는 않습니다. 작업 환경에서 모든 볼륨의 백업 생성을 중지하려면 백업을 비활성화할 수 있습니다 [참조하십시오](#).

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.

Volumes Restore Applications Virtual Machines Kubernetes Job Monitoring

All Backup Working Environments Backup Settings

1 Working Environments 57 Protected Volumes 15.1 TB Total Backup Capacity

Protected Volumes Status: 57 Healthy Backup Volumes, 0 Failed Backup Volumes

57 Backups

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	Details & Backup List Backup Now Pause Backups
CVO_AWS On	Volume_3 On	SVM_1	May 22 2019, 00:00:00	2,050 Backups	

모든 백업 파일 목록이 표시됩니다.

Source Destination Backup Information

Working Environment: Working Environment N...
 Type: Cloud Volumes ONTAP (HA)
 Provider: AWS
 Volume: Volume Name
 SVM: SVM Name

Cloud Provider: AWS
 Region: us-east-1
 Bucket: netapp-backup
 Account ID: 012345678901234567890

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

2,050 Backups

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.

2,050 Backups

Select Timeframe Actions

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

Delete All Backups
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.

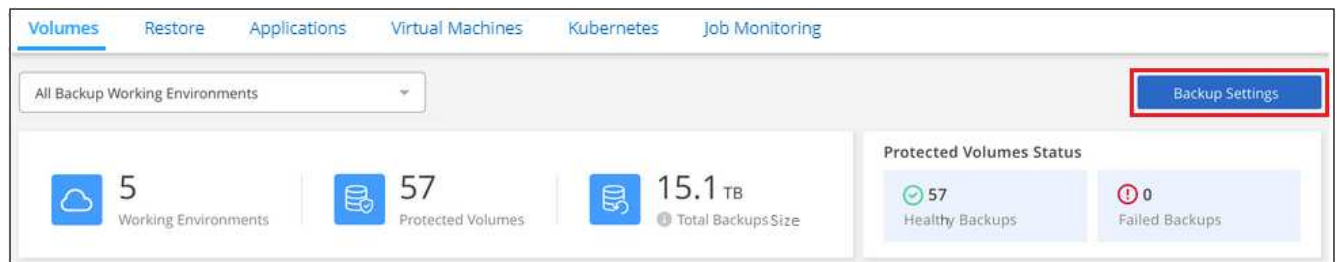
작업 환경에서 **Cloud Backup**을 해제합니다

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.

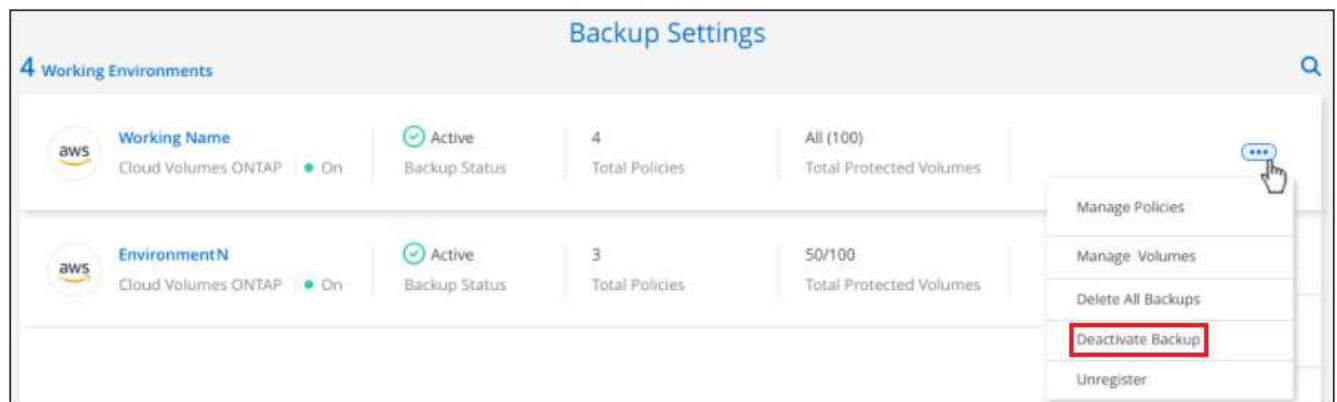
사용자가 비용을 부담하지 않는 한, 클라우드 공급자가 백업 용량에 대한 오브젝트 스토리지 비용에 대해 계속 청구한다는 점에 유의하십시오 **백업을 삭제합니다**.

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.

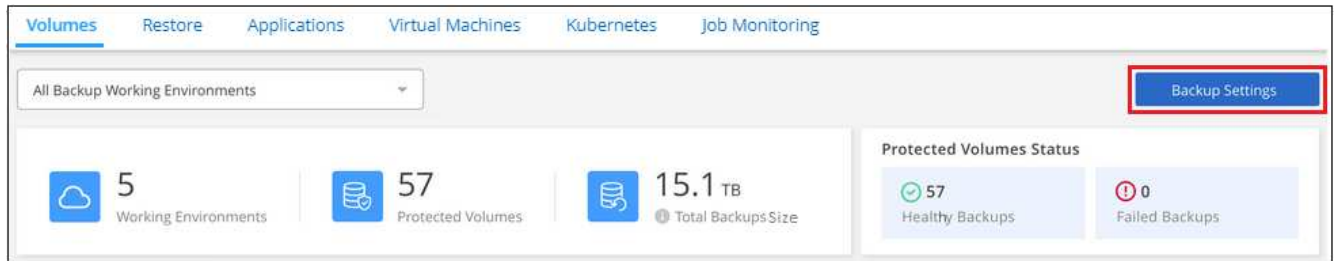
클라우드 백업을 등록 취소하려면 먼저 다음 단계를 순서대로 수행해야 합니다.

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

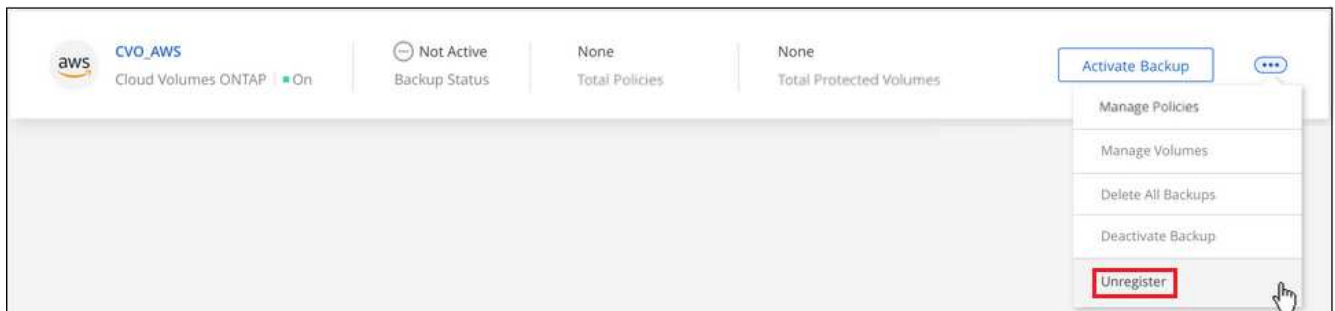
이 두 작업이 완료될 때까지 등록 취소 옵션을 사용할 수 없습니다.

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.

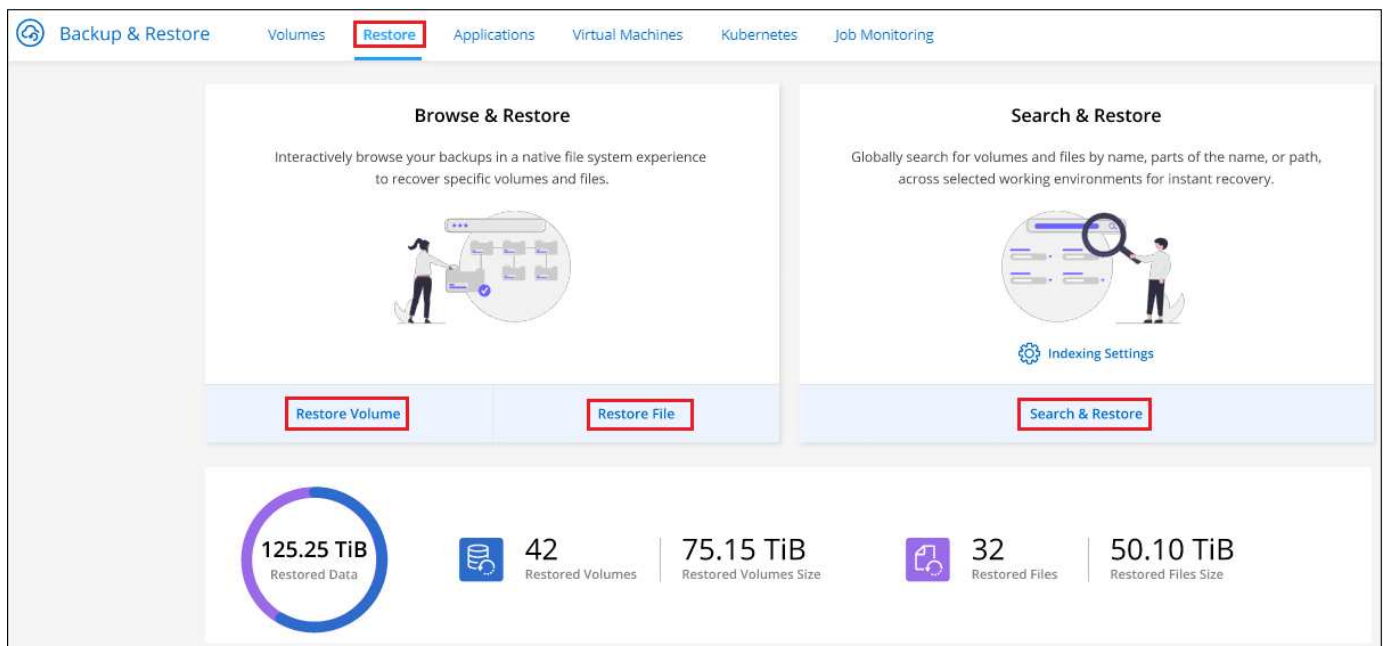
백업 파일에서 운영 시스템으로 데이터를 복원하려면 유효한 Cloud Backup 라이선스가 필요합니다.

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 및 파일 복원은 Amazon S3, Azure Blob, Google Cloud 및 NetApp StorageGRID에 저장된 백업 파일과 함께 작동합니다.	볼륨 및 파일 복원은 Amazon S3 및 Google Cloud에 저장된 백업 파일과 함께 작동합니다
인터넷에 액세스할 수 없는 사이트에서 StorageGRID의 볼륨 및 파일을 복원합니다	어두운 사이트에서는 지원되지 않습니다
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
추가 클라우드 공급자 리소스가 필요하지 않습니다	계정당 필요한 추가 버킷 및 AWS 또는 Google 리소스
추가 클라우드 공급자 비용은 필요하지 않습니다	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 시작)에 있는 경우 복원 작업에 더 많은 시간이 소요되고 비용이 발생합니다. 또한 대상 클러스터에서 ONTAP 9.10.1 이상이 실행되고 있어야 합니다.

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

["Azure 아카이브 스토리지에서 복원에 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 * <code>ifdef::AWS[]</code>

백업 파일 위치	대상 작업 환경	
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	Cloud Volumes ONTAP in AWS on-premises ONTAP system endif::AWS[]ifdef::Azure[]
Azure Blob	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 사내 ONTAP 시스템의 Cloud Volumes ONTAP endif::Azure[]ifdef::GCP[]
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP::GCP []
NetApp StorageGRID를 참조하십시오	사내 ONTAP 시스템	사내 ONTAP 시스템

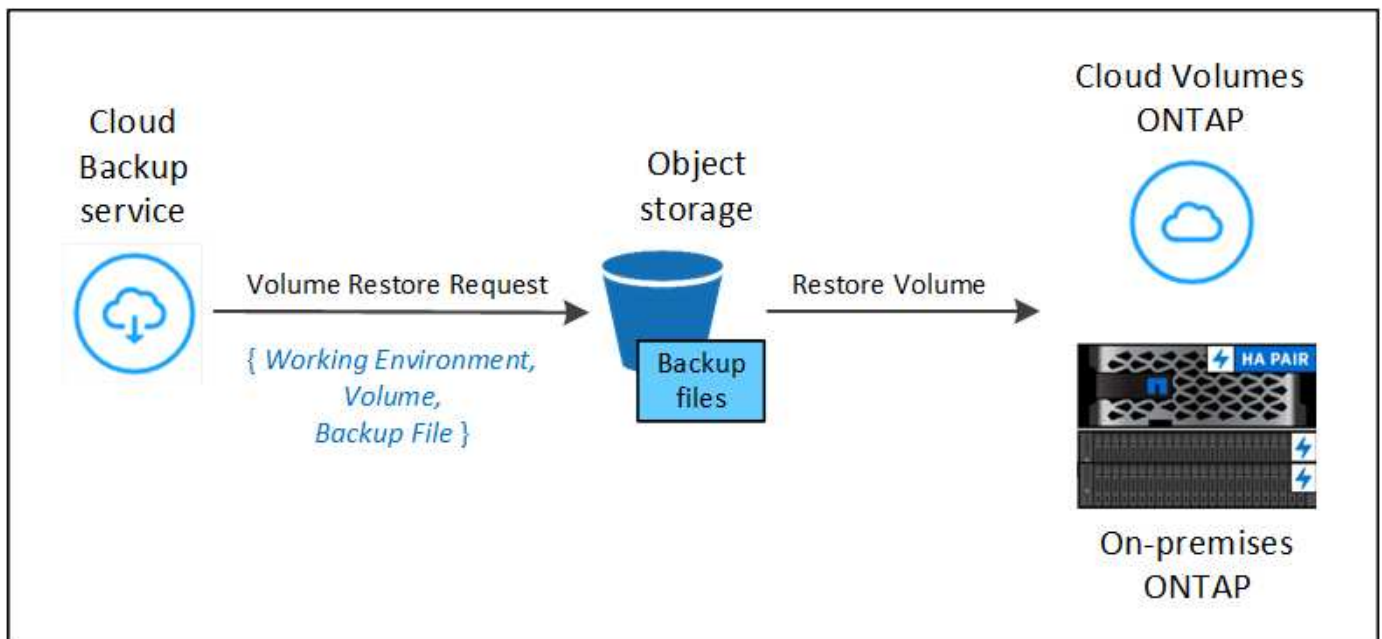
"사내 ONTAP 시스템"을 지칭할 때 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.



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

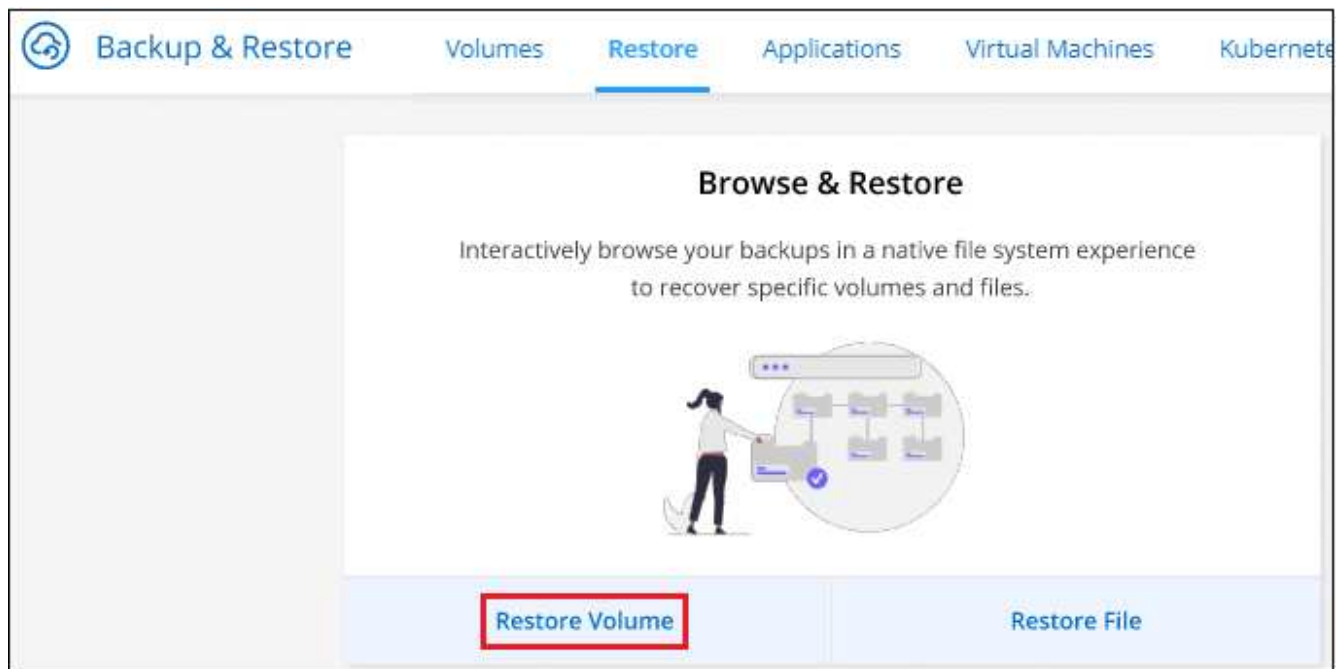
January 2022

 NetApp

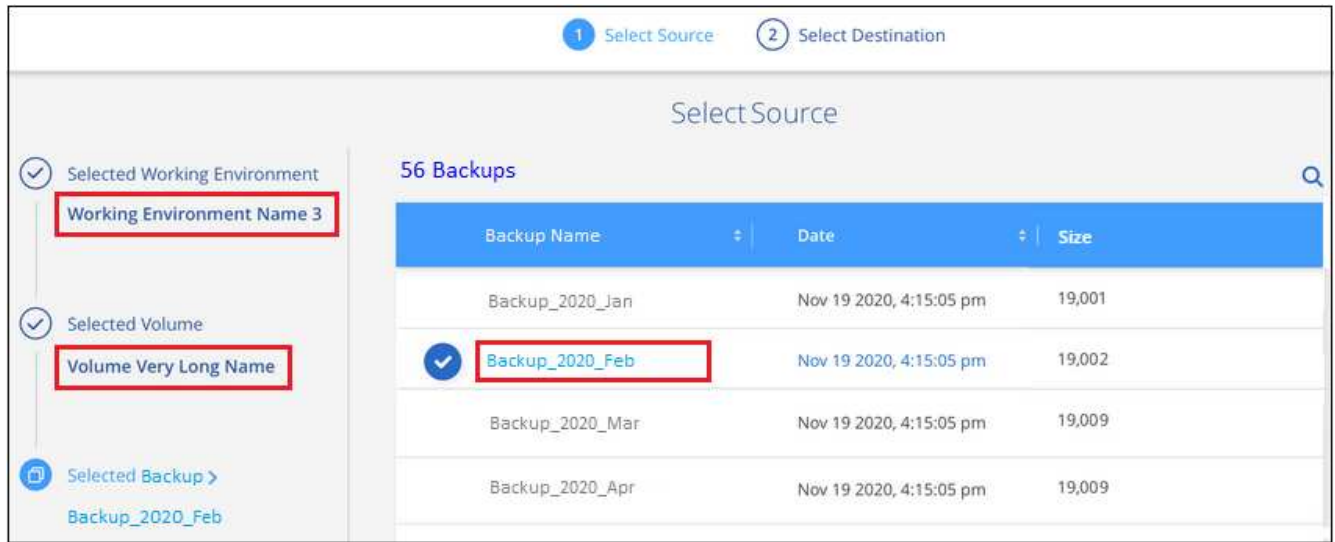


단계

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

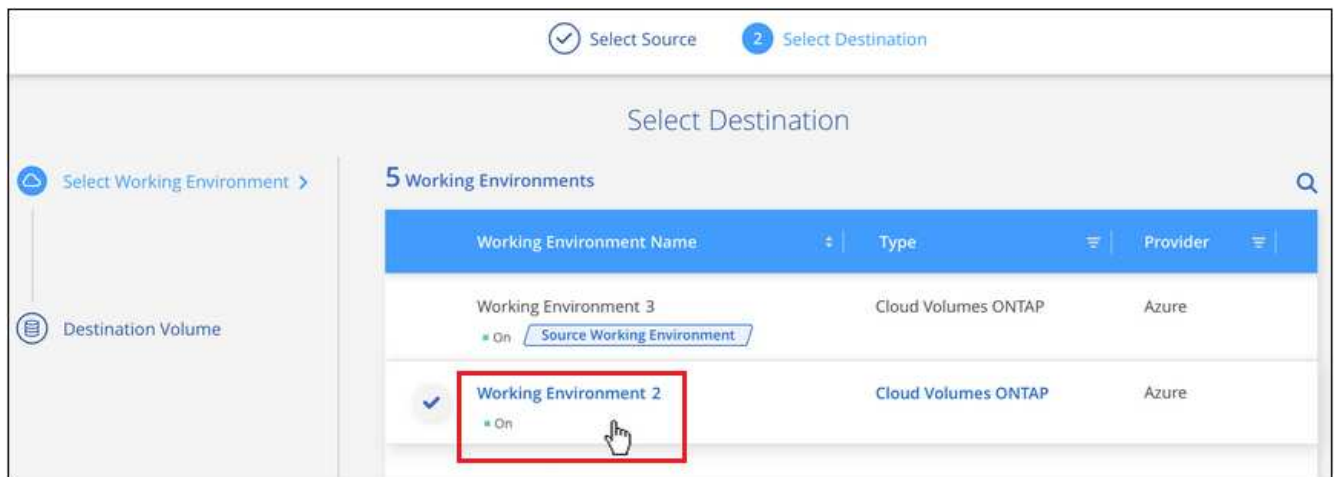


4. Select Source_ 페이지에서 복원하려는 볼륨의 백업 파일로 이동합니다. 복원할 날짜/시간 스탬프가 있는 * Working Environment *, * Volume * 및 * Backup * 파일을 선택합니다.



5. 계속 * 을 클릭합니다.

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



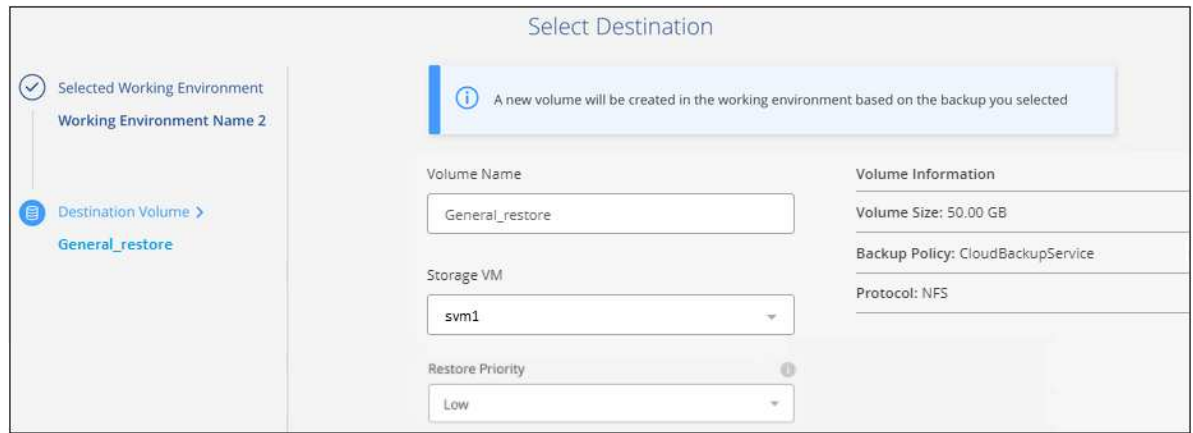
7. 사내 ONTAP 시스템을 선택하고 오브젝트 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 묻는 메시지가 표시됩니다.

◦ 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 복구할 때 StorageGRID 서버의 FQDN과 ONTAP이 StorageGRID와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 객체 스토리지에 액세스하는 데 필요한 액세스 키 및 비밀 키를 선택하고, 대상 볼륨이 상주할 ONTAP 클러스터의 IPspace를 선택합니다.

a. 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.

"AWS 아카이브 스토리지에서 복원하는 방법에 대해 자세히 알아보십시오".

"Azure 아카이브 스토리지에서 복원에 대해 자세히 알아보십시오".

1. 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

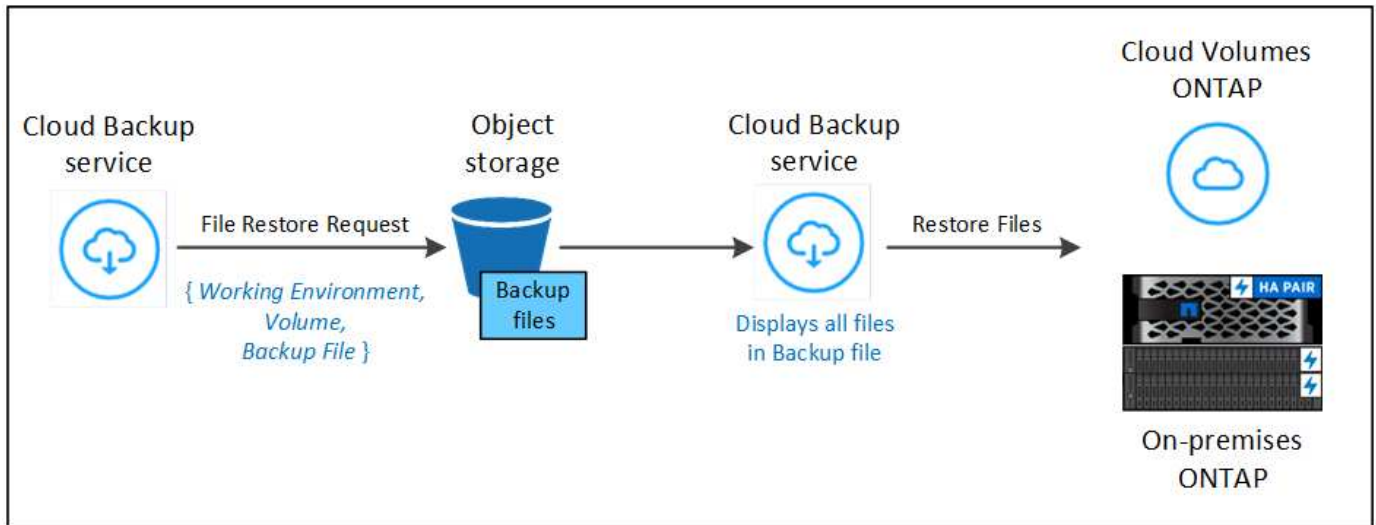
- 파일 복원 작업을 수행하려면 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템에서 ONTAP 버전이 9.6 이상이어야 합니다.
- AWS 교차 계정 복원에는 AWS 콘솔에서 수동으로 수행해야 합니다. AWS 항목을 참조하십시오 ["교차 계정 버킷"](#)

권한 부여"를 참조하십시오.

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. 클라우드 백업은 선택한 백업 파일 내에 있는 폴더와 파일을 표시합니다.
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 복원됩니다.



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

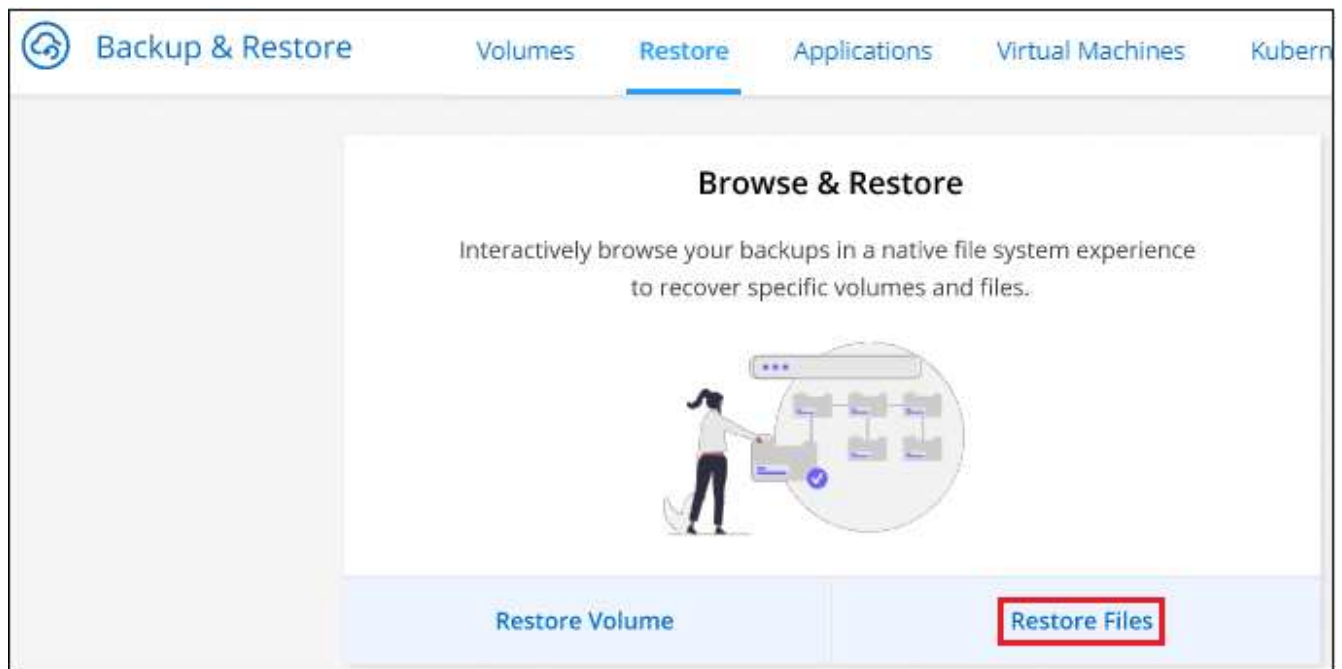
January 2022

 NetApp

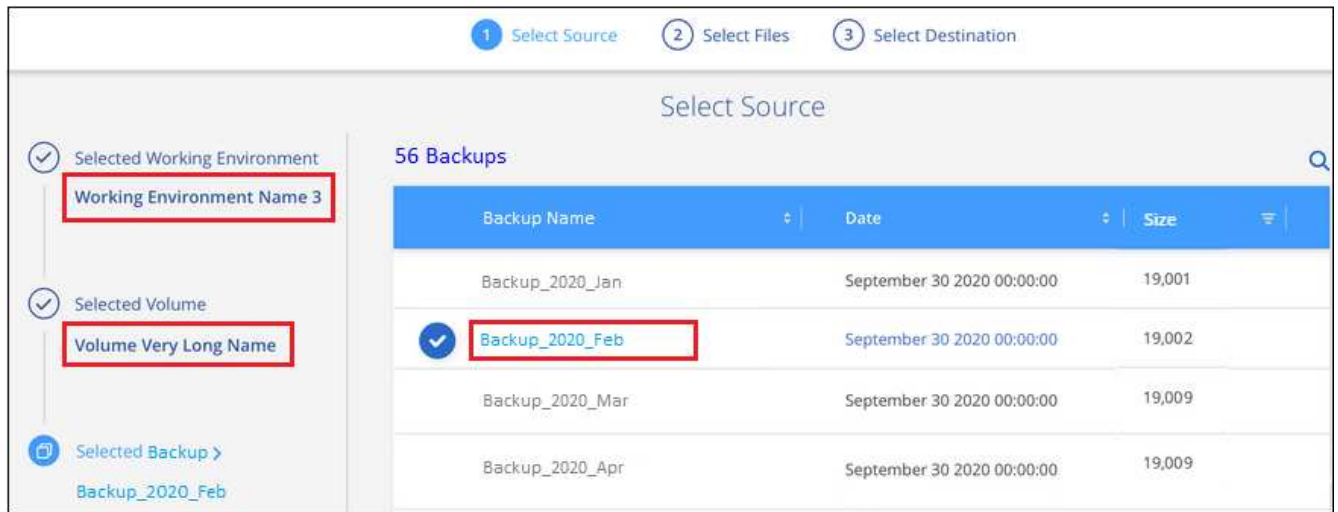


단계

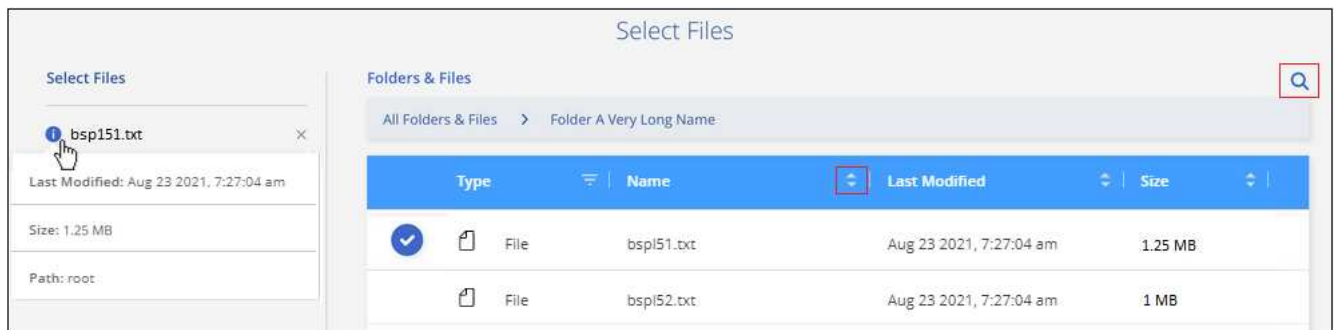
1. 백업 및 복원 * 서비스를 선택합니다.
2. Restore * 탭을 클릭하면 Restore Dashboard가 표시됩니다.
3. Browse & Restore _ 섹션에서 * Restore Files * 를 클릭합니다.



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 볼륨 백업의 폴더 및 파일 목록이 표시됩니다.

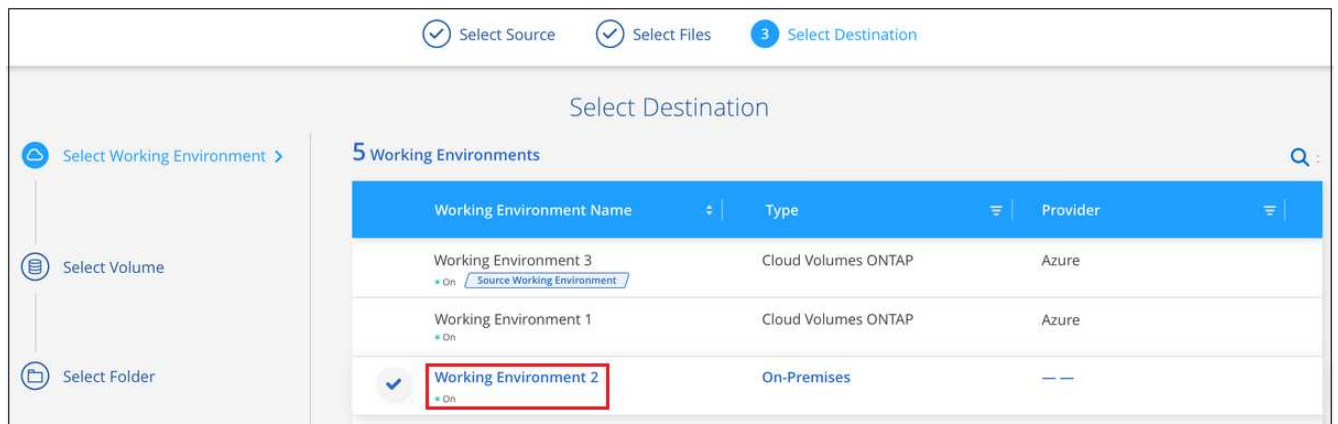


6. Select Files_page(파일 선택_페이지)에서 복원하려는 파일을 선택하고 * Continue *(계속 *)를 클릭합니다. 파일을 찾는 데 도움이 되는 방법은 다음과 같습니다.

- 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.

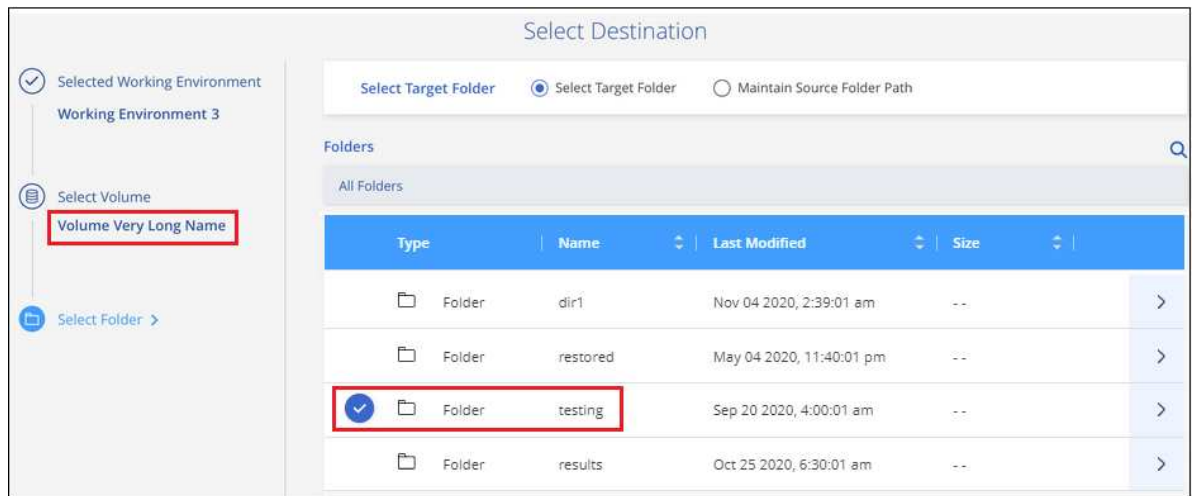
파일을 선택하면 이미 선택한 파일을 볼 수 있도록 페이지 왼쪽에 추가됩니다. 필요한 경우 파일 이름 옆의 * x * 를 클릭하여 이 목록에서 파일을 제거할 수 있습니다.

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.
 - Google 클라우드 스토리지에서 복원할 때 대상 볼륨이 있는 ONTAP 클러스터에 IPspace를 입력하고 오브젝트 스토리지에 액세스하는 데 필요한 액세스 키 및 비밀 키를 입력합니다.
 - StorageGRID에서 복구할 때 StorageGRID 서버의 FQDN과 ONTAP이 StorageGRID과의 HTTPS 통신에 사용해야 하는 포트를 입력하고, 오브젝트 스토리지에 액세스하는 데 필요한 액세스 키 및 비밀 키, 대상 볼륨이 있는 ONTAP 클러스터의 IPspace를 입력합니다.
 - a. 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.
 - a. 복원 * 을 클릭하면 복원 작업의 진행률을 검토할 수 있도록 복원 대시보드로 돌아갑니다. 또한 * Job Monitor * 탭을 클릭하여 복원 진행률을 확인할 수도 있습니다.

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 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 * <code>ifdef::AWS[]</code>
Amazon S3	Cloud Volumes ONTAP를 사내의 AWS ONTAP 시스템에 설치하고	<code>Cloud Volumes ONTAP in AWS on-premises ONTAP system</code> <code>endif::AWS[]ifdef::Azure[]</code>

백업 파일 위치	대상 작업 환경	
Azure Blob	현재 지원되지 않습니다	endif::Azure []ifdef::GCP []
Google 클라우드 스토리지	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP	Google 사내 ONTAP 시스템의 Cloud Volumes ONTAP::GCP []
NetApp StorageGRID를 참조하십시오	현재 지원되지 않습니다	

"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.

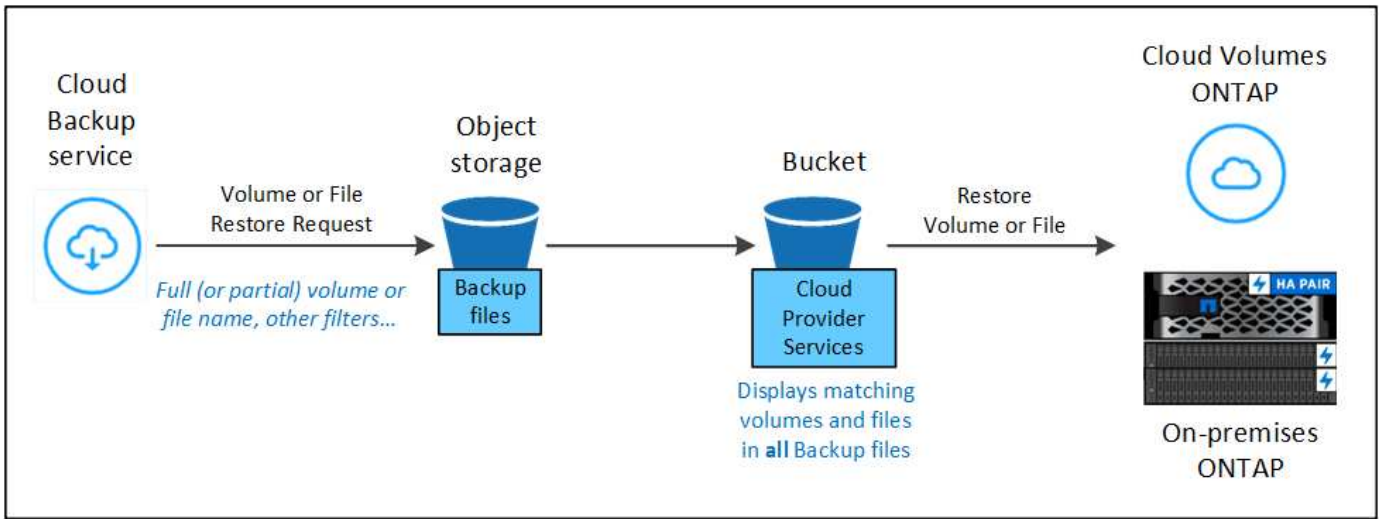
- 검색 및 복원을 사용하려면 볼륨이나 파일을 복원할 각 소스 작업 환경에서 "인덱싱"을 활성화해야 합니다. 따라서 인덱싱된 카탈로그를 통해 모든 볼륨의 백업 파일을 추적할 수 있습니다.
- 볼륨 백업에서 볼륨이나 파일을 복원하려면 **Search & Restore** 아래에서 * 검색 및 복원 * 을 클릭합니다.
- 볼륨 또는 파일의 검색 기준을 전체 또는 일부 볼륨 이름, 전체 파일 이름, 크기 범위, 생성 날짜 범위, 기타 검색 필터로 입력하고 * 검색 * 을 클릭합니다.

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

- 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 v3을 활성화하고 다음 작업을 수행합니다.

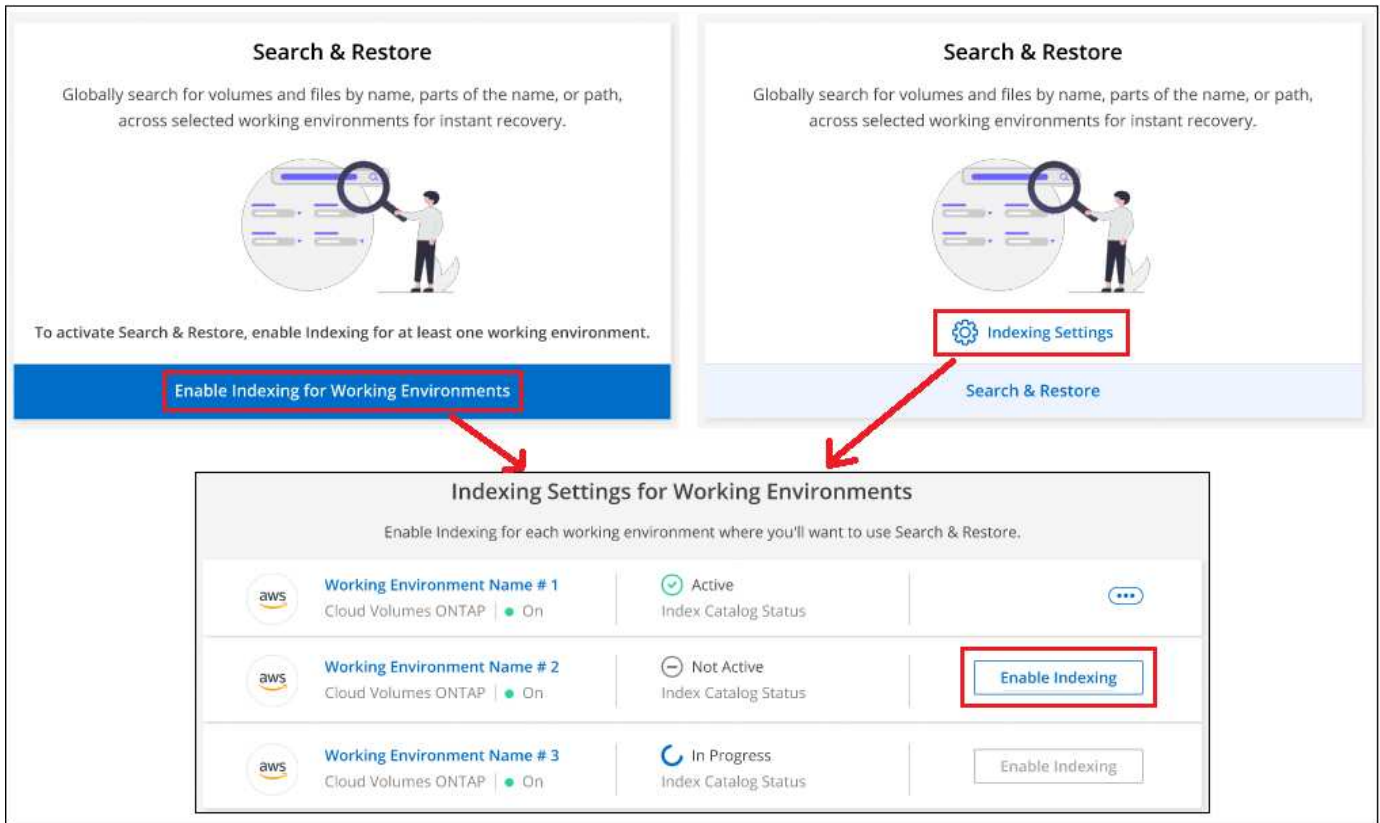
- AWS에 저장된 백업의 경우 새로운 S3 버킷과 을 프로비저닝합니다 "아마존 Athena 대화형 쿼리 서비스" 및 "AWS Glue 서버리스 데이터 통합 서비스".
- Google Cloud에 저장된 백업의 경우 IT 부서는 새로운 버킷과 을 프로비저닝합니다 "Google Cloud BigQuery 서비스" 계정/프로젝트 수준에서 프로비저닝됩니다.

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

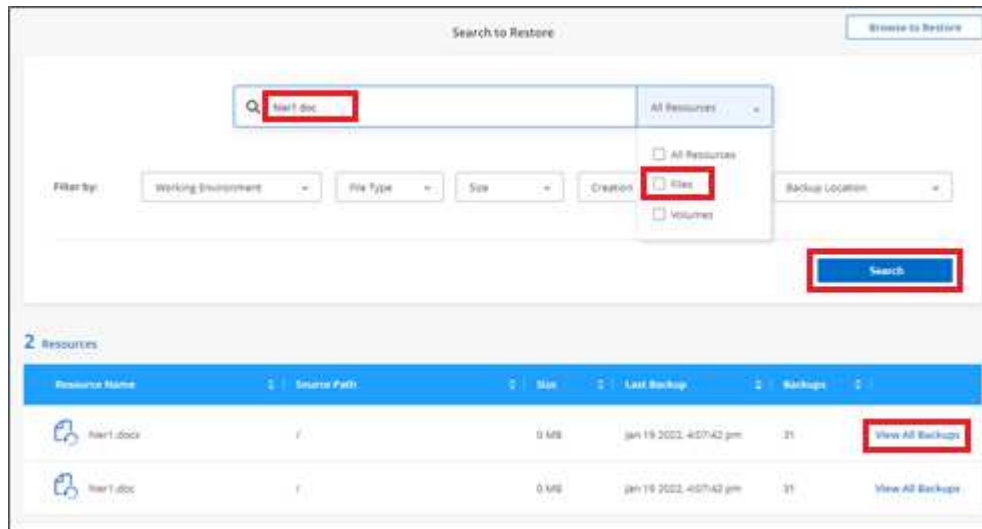
먼저 해 **작업 환경에 대한 인덱싱 기능을 활성화했습니다**, 검색 및 복원을 사용하여 볼륨이나 파일을 복원할 수 있습니다. 이를 통해 광범위한 필터를 사용하여 모든 백업 파일에서 복원하려는 정확한 파일 또는 볼륨을 찾을 수 있습니다.

단계

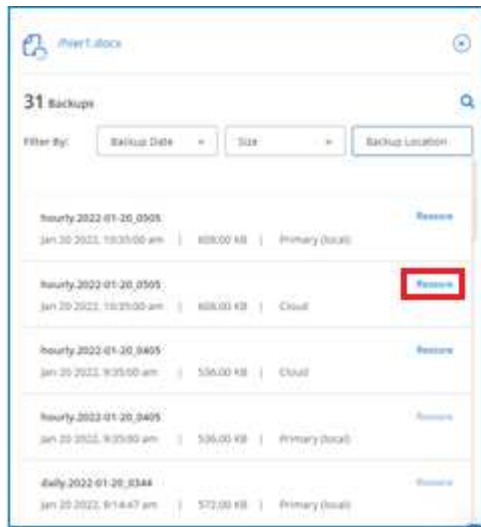
1. 백업 및 복원 * 서비스를 선택합니다.
2. Restore * 탭을 클릭하면 Restore Dashboard가 표시됩니다.
3. Search & Restore _ 섹션에서 * Search & Restore * 를 클릭합니다.



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.

Kubernetes 데이터 백업 및 복원

Cloud Backup을 사용하여 Kubernetes 클러스터 데이터를 보호합니다

Cloud Backup은 Kubernetes 클러스터 데이터의 보호 및 장기 아카이브를 위한 백업 및 복원 기능을 제공합니다. 백업은 자동으로 생성되어 퍼블릭 또는 프라이빗 클라우드 계정의 오브젝트 저장소에 저장됩니다.

필요한 경우 백업에서 전체 `_volume_`을 동일하거나 다른 작업 환경으로 복원할 수 있습니다.

피처

백업 기능:

- 영구 볼륨의 독립적인 복사본을 저비용 오브젝트 스토리지로 백업합니다.
- 클러스터의 모든 볼륨에 단일 백업 정책을 적용하거나 고유한 복구 지점 목표가 있는 볼륨에 다른 백업 정책을 할당합니다.
- 사용 중인 AES-256비트 암호화 유틸 및 TLS 1.2 HTTPS 연결로 백업 데이터를 보호합니다.
- 단일 볼륨에 대해 최대 4,000개의 백업을 지원합니다.

복원 기능:

- 특정 시점에서 데이터 복원
- 소스 시스템 또는 다른 시스템으로 볼륨을 복구합니다.
- 블록 수준에서 데이터를 복원하여 원래 ACL을 보존하면서 데이터를 사용자가 지정한 위치에 직접 배치합니다.

지원되는 Kubernetes 작업 환경 및 오브젝트 스토리지 공급자

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

소스 작업 환경	백업 파일 대상 <code>ifdef::AWS[]</code>
AWS의 Kubernetes 클러스터	Amazon S3 엔디프::AWS[] <code>ifdef::Azure[]</code>
Azure의 Kubernetes 클러스터	Azure Blob 엔디프::Azure [] <code>ifdef::GCP[]</code>
Google의 Kubernetes 클러스터	Google Cloud 스토리지 엔디프::GCP[]

Kubernetes 백업 파일에서 다음 작업 환경으로 볼륨을 복원할 수 있습니다.

백업 파일 위치	대상 작업 환경 <code>ifdef::AWS[]</code>
Amazon S3	AWS 엔디프::AWS[] <code>ifdef::Azure[]</code> 의 Kubernetes 클러스터
Azure Blob	Azure 엔디프의 Kubernetes 클러스터::Azure [] <code>ifdef::GCP[]</code>
Google 클라우드 스토리지	Google 엔디프의 Kubernetes 클러스터::GCP[]

비용

Cloud Backup을 사용하는 경우 리소스 요금과 서비스 요금이라는 두 가지 유형의 비용이 있습니다.

- 리소스 비용 *

클라우드 공급자의 오브젝트 스토리지 용량에 대한 리소스 요금이 부과됩니다. 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.

- 서비스 요금 *

서비스 비용은 NetApp에 지불되며 해당 백업에서 _create_backups와 to_restore_volumes에 대한 두 가지 비용이 모두 포함됩니다. 오브젝트 스토리지에 백업된 볼륨의 소스 논리적 사용 용량(_Before_ONTAP 효율성)을 사용하여 계산한, 보호되는 데이터에 대해서만 비용을 지불합니다. 이 용량을 FETB(Front-End Terabytes)라고도 합니다.

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

라이선싱

Cloud Backup은 PAYGO(Pay As You Go) 및 BYOL(Bring Your Own License)의 두 가지 라이선스 옵션으로 제공됩니다. 라이선스가 없는 경우 30일 무료 평가판을 사용할 수 있습니다.

무료 평가판

30일 무료 평가판을 사용하는 경우 남은 무료 평가판 사용 일수에 대한 알림이 표시됩니다. 무료 평가판이 끝나면 백업이 생성되지 않습니다. 서비스를 계속 사용하려면 서비스에 가입하거나 라이선스를 구입해야 합니다.

서비스가 비활성화되면 백업 파일이 삭제되지 않습니다. 백업을 삭제하지 않을 경우 클라우드 공급자가 백업 용량에 대한 오브젝트 스토리지 비용을 계속 청구합니다.

용량제 구독

Cloud Backup은 용량제 모델로 소비 기반 라이선스를 제공합니다. 클라우드 공급자의 마켓플레이스를 통해 구독한 후에는 백업되는 데이터의 GB당 비용을 지불하며, 이러한 데이터를 미리 지불할 필요가 없습니다. 클라우드 공급자가 월별 요금을 청구합니다.

무료 평가판을 가지고 있거나 BYOL(Bring Your Own License)을 사용하는 경우에도 가입해야 합니다.

- 구독하면 무료 평가판이 종료된 후에도 서비스가 중단되지 않습니다.

평가판이 종료되면 백업하는 데이터의 양에 따라 매시간 요금이 부과됩니다.

- BYOL 라이선스에서 허용하는 것보다 더 많은 데이터를 백업하는 경우 용량제 가입형 모델을 통해 데이터 백업을 계속 수행할 수 있습니다.

예를 들어, 10TB BYOL 라이선스가 있는 경우 PAYGO 구독을 통해 10TB 이상의 모든 용량이 청구됩니다.

무료 평가판 사용 중 또는 BYOL 라이선스를 초과하지 않은 경우 용량제 구독을 통해 비용을 지불할 필요가 없습니다.

"선불 종량제 구독을 설정하는 방법을 알아보십시오".

각자 보유한 라이선스를 가지고 오시기 바랍니다

BYOL은 기간 기반(12, 24 또는 36개월) _ 및 _ 용량 기반(1TB 증분) 1년, 최대 용량(10TB)을 위해 서비스 사용 비용을 NetApp에 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".

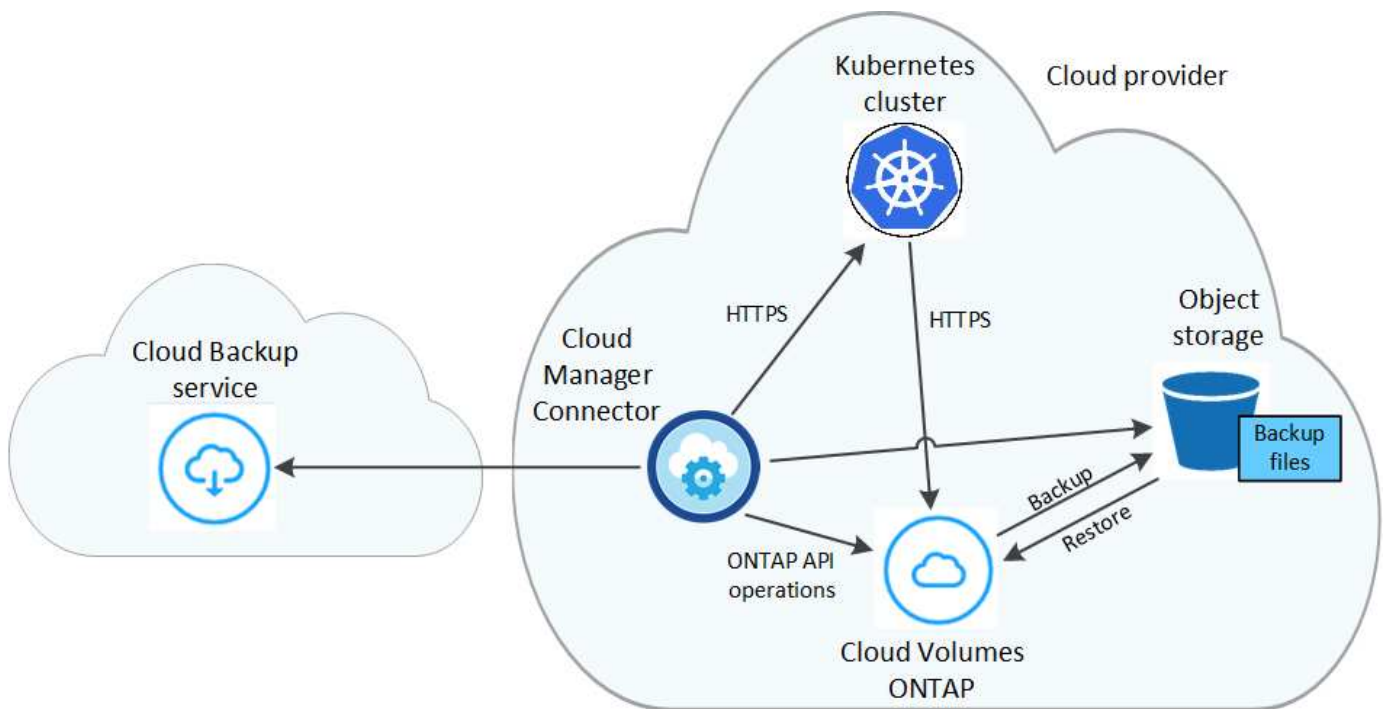
Cloud Backup의 작동 방식

Kubernetes 시스템에서 Cloud Backup을 활성화하면 서비스가 데이터의 전체 백업을 수행합니다. 초기 백업 후에는 모든 추가 백업이 증분 백업되므로 변경된 블록과 새 블록만 백업됩니다. 이렇게 하면 네트워크 트래픽이 최소로 유지됩니다.



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.



지원되는 스토리지 클래스 또는 액세스 계층

- AWS에서는 백업이 _Standard_storage 클래스에서 시작되고 30일 후에 _Standard - Infrequent Access_storage 클래스로 전환됩니다.
- Azure에서 백업은 _Cool_access 계층과 연결됩니다.

- GCP에서 백업은 기본적으로 `_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.

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

지원되는 볼륨

Cloud Backup은 PVS(Persistent Volume)를 지원합니다.

제한 사항

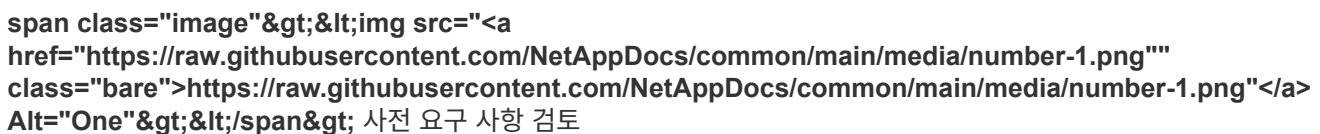
- 정책에 할당된 볼륨이 없을 때 백업 정책을 생성하거나 편집할 때 유지되는 백업 수는 최대 1018개가 될 수 있습니다. 이 문제를 해결하려면 정책을 생성할 백업 수를 줄일 수 있습니다. 그런 다음 정책에 볼륨을 할당한 후 정책을 편집하여 최대 4000개의 백업을 생성할 수 있습니다.
- 지금 백업 * 버튼을 사용한 임시 볼륨 백업은 Kubernetes 볼륨에서 지원되지 않습니다.

Kubernetes 영구 볼륨 데이터를 Amazon S3에 백업

몇 가지 단계를 완료하여 EKS Kubernetes 클러스터의 영구 볼륨에서 Amazon S3 스토리지로 데이터 백업을 시작하십시오.

빠른 시작

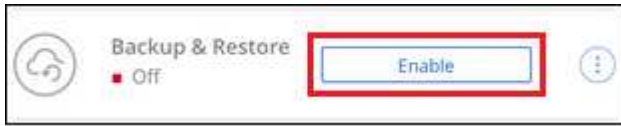
다음 단계를 따라 빠르게 시작하거나 나머지 섹션으로 스크롤하여 자세한 내용을 확인하십시오.

 `span class="image"><img src="https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png" Alt="One"` 사전 요구 사항 검토

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다.
 - Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다.
 - 백업하려는 영구 체적을 생성하는 데 사용되는 모든 PVC는 "snapshotPolicy(스냅샷 정책)"를 "default(기본값)"로 설정해야 합니다.
 - 클러스터는 백엔드 스토리지를 위해 AWS에서 Cloud Volumes ONTAP를 사용해야 합니다.
 - Cloud Volumes ONTAP 시스템에서 ONTAP 9.7P5 이상을 실행해야 합니다.
- 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".

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 * 활성화 * 를 클릭한 다음 설정 마법사를 따릅니다.



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.

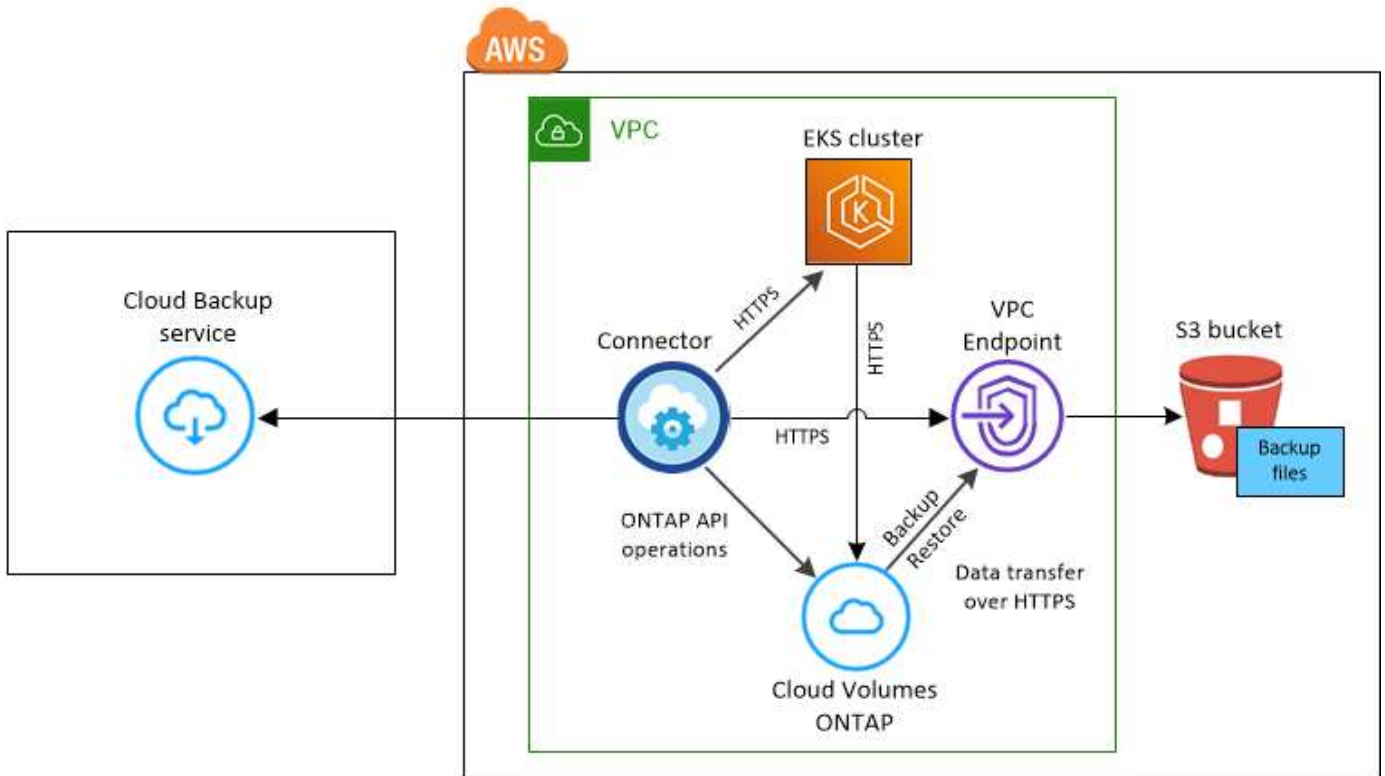
A screenshot of a 'Define Policy' wizard. The title 'Define Policy' is at the top. Below it, the section 'Policy - Retention & Schedule' is active. It contains four rows of options: 'Hourly' (unchecked), 'Daily' (checked), 'Weekly' (unchecked), and 'Monthly' (unchecked). Each row has a 'Number of backups to retain' label and a corresponding numeric input field with up/down arrows. The values are 24, 30, 52, and 12 respectively. At the bottom, there is a section for 'S3 Bucket' with a note: 'Cloud Manager will create the S3 bucket after you complete the wizard'.

Select Volumes 페이지에서 백업할 볼륨을 식별합니다. S3 버킷은 Cloud Volumes ONTAP 시스템과 동일한 AWS 계정 및 지역에 자동으로 생성되며 백업 파일은 여기에 저장됩니다.

요구 사항

Kubernetes 영구 볼륨을 S3에 백업하기 전에 다음 요구사항을 읽고 지원되는 구성이 있는지 확인합니다.

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



VPC 엔드포인트가 선택 사항입니다.

Kubernetes 클러스터 요구사항

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다. "[Kubernetes 클러스터를 검색하는 방법을 알아보십시오](#)".
- Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다. 을 참조하십시오 "[Trident 설치 방법](#)" 또는 "[Trident 버전을 업그레이드하는 방법](#)".
- 클러스터는 백엔드 스토리지를 위해 AWS에서 Cloud Volumes ONTAP를 사용해야 합니다.
- Cloud Volumes ONTAP 시스템은 Kubernetes 클러스터와 같은 AWS 지역에 있어야 하며 ONTAP 9.7P5 이상을 실행해야 합니다(ONTAP 9.8P11 이상 권장).

사내 위치의 Kubernetes 클러스터는 지원되지 않습니다. Cloud Volumes ONTAP 시스템을 사용하는 클라우드 구축 환경의 Kubernetes 클러스터만 지원됩니다.

- 백업하려는 영구 볼륨을 생성하는 데 사용되는 모든 영구 볼륨 클레임 객체에는 "snapshotPolicy"가 "default"로 설정되어 있어야 합니다.

주석 아래에 '스냅샷 정책'을 추가하여 개별 PVC에 대해 이 작업을 수행할 수 있습니다.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver

```

backend.json 파일의 기본값 아래에 'shapshotPolicy' 필드를 추가하여 특정 백엔드 스토리지와 관련된 모든 PVC에 대해 이 작업을 수행할 수 있습니다.

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

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 백업 권한이 필요합니다

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

다음은 정책의 특정 S3 사용 권한입니다.

```
{
  "Sid": "backupPolicy",
  "Effect": "Allow",
  "Action": [
    "s3:DeleteBucket",
    "s3:GetLifecycleConfiguration",
    "s3:PutLifecycleConfiguration",
    "s3:PutBucketTagging",
    "s3:ListBucketVersions",
    "s3:GetObject",
    "s3:DeleteObject",
    "s3:ListBucket",
    "s3:ListAllMyBuckets",
    "s3:GetBucketTagging",
    "s3:GetBucketLocation",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicy",
    "s3:PutBucketPublicAccessBlock"
  ],
  "Resource": [
    "arn:aws:s3:::netapp-backup-*"
  ]
},
```


클라우드 백업 활성화

Kubernetes 작업 환경에서 Cloud Backup을 바로 사용할 수 있습니다.

단계

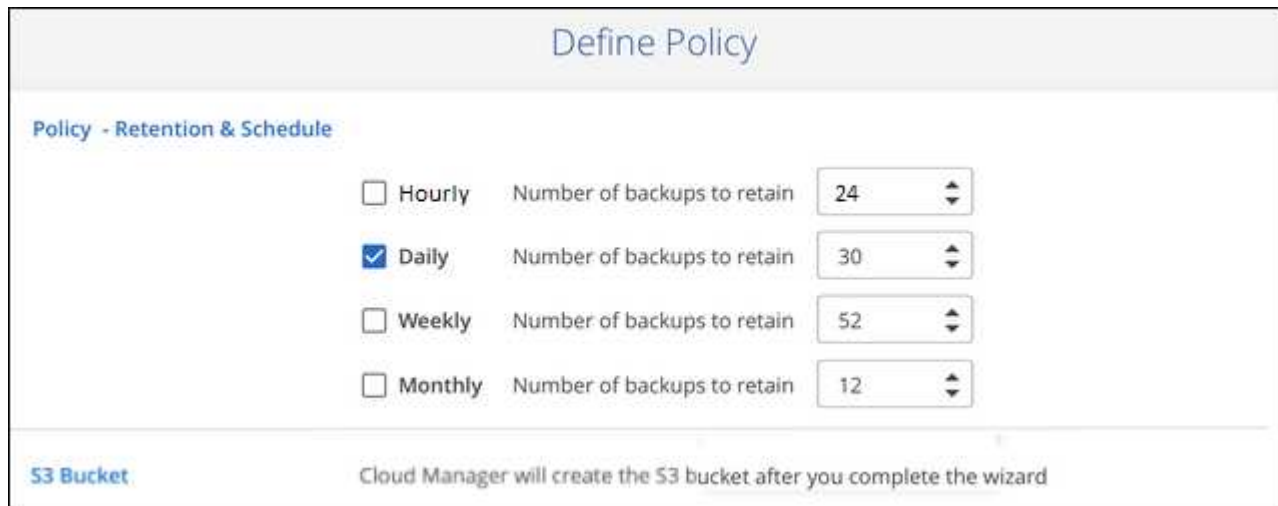
1. 작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 * 활성화 * 를 클릭합니다.

백업에 대한 Amazon S3 대상이 Canvas에서 작업 환경으로 존재하는 경우 Kubernetes 클러스터를 Amazon S3 작업 환경으로 끌어서 설정 마법사를 시작할 수 있습니다.



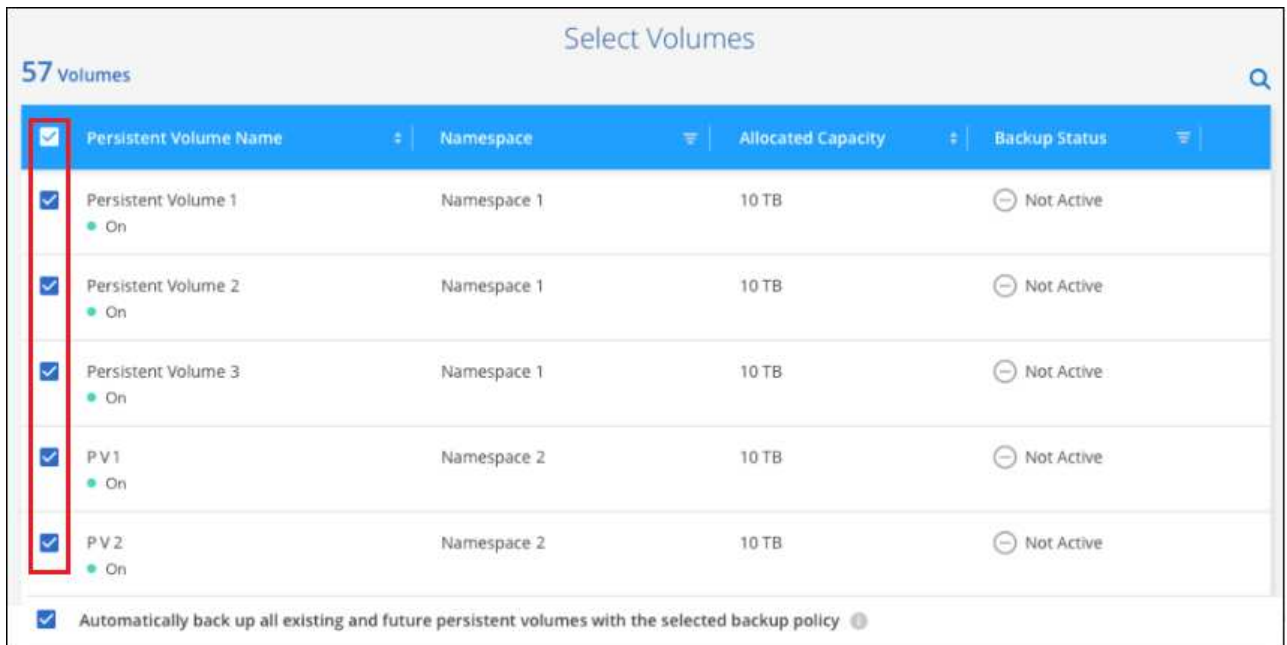
2. 백업 정책 세부 정보를 입력하고 * 다음 * 을 클릭합니다.

백업 스케줄을 정의하고 유지할 백업 수를 선택할 수 있습니다.



3. 백업할 영구 볼륨을 선택합니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume_1)를 클릭합니다.



4. 현재 및 향후 모든 볼륨에서 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 Cloud Volumes ONTAP 시스템과 동일한 AWS 계정 및 지역에 자동으로 생성되며 백업 파일은 여기에 저장됩니다.

Kubernetes 대시보드가 표시되므로 백업 상태를 모니터링할 수 있습니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨을 복원합니다" 같은 지역(AWS)의 동일한 또는 다른 Kubernetes 클러스터에서 새 볼륨으로.

Kubernetes 영구 볼륨 데이터를 Azure Blob 스토리지에 백업

몇 가지 단계를 완료하여 AKS Kubernetes 클러스터의 영구 볼륨에서 Azure Blob 스토리지로 데이터 백업을 시작하십시오.

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" & 사진 요구 사항 검토

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다.
 - Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다.
 - 백업하려는 영구 체적을 생성하는 데 사용되는 모든 PVC는 "snapshotPolicy(스냅샷 정책)"를 "default(기본값)"로 설정해야 합니다.
 - 클러스터는 '백엔드 스토리지'를 위해 Azure에서 Cloud Volumes ONTAP를 사용해야 합니다.

- Cloud Volumes ONTAP 시스템에서 ONTAP 9.7P5 이상을 실행해야 합니다.
- 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

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 * 활성화 * 를 클릭한 다음 설정 마법사를 따릅니다.



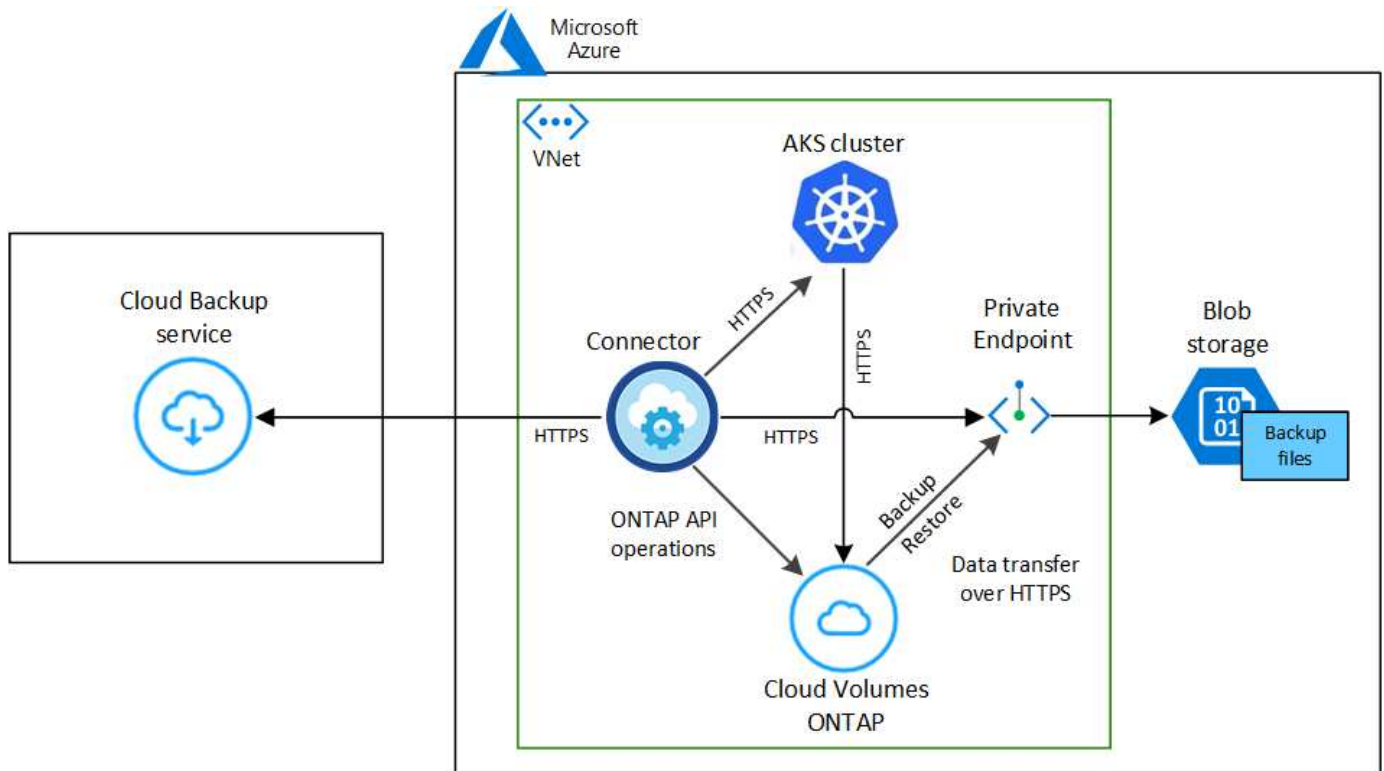
기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

Select Volumes 페이지에서 백업할 볼륨을 식별합니다. 백업 파일은 Cloud Volumes ONTAP 시스템과 동일한 Azure 가입 및 지역을 사용하는 Blob 컨테이너에 저장됩니다.

요구 사항

Kubernetes 영구 볼륨을 Blob 스토리지에 백업하기 전에 다음 요구사항을 읽고 지원되는 구성이 있는지 확인합니다.

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



개별 엔드포인트가 선택 사항입니다.

Kubernetes 클러스터 요구사항

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다. "[Kubernetes 클러스터를 검색하는 방법을 알아보십시오](#)".
- Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다. 을 참조하십시오 "[Trident 설치 방법](#)" 또는 "[Trident 버전을 업그레이드하는 방법](#)".
- 클러스터는 '백엔드 스토리지'를 위해 Azure에서 Cloud Volumes ONTAP를 사용해야 합니다.
- Cloud Volumes ONTAP 시스템은 Kubernetes 클러스터와 같은 Azure 지역에 있어야 하며 ONTAP 9.7P5 이상을 실행해야 합니다(ONTAP 9.8P11 이상 권장).

사내 위치의 Kubernetes 클러스터는 지원되지 않습니다. Cloud Volumes ONTAP 시스템을 사용하는 클라우드 구축 환경의 Kubernetes 클러스터만 지원됩니다.

- 백업하려는 영구 볼륨을 생성하는 데 사용되는 모든 영구 볼륨 클레임 객체에는 "snapshotPolicy"가 "default"로 설정되어 있어야 합니다.

주석 아래에 '스냅샷 정책'을 추가하여 개별 PVC에 대해 이 작업을 수행할 수 있습니다.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver

```

backend.json 파일의 기본값 아래에 'shapshotPolicy' 필드를 추가하여 특정 백엔드 스토리지와 관련된 모든 PVC에 대해 이 작업을 수행할 수 있습니다.

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

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](#)".

클라우드 백업 활성화

Kubernetes 작업 환경에서 Cloud Backup을 바로 사용할 수 있습니다.

단계

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

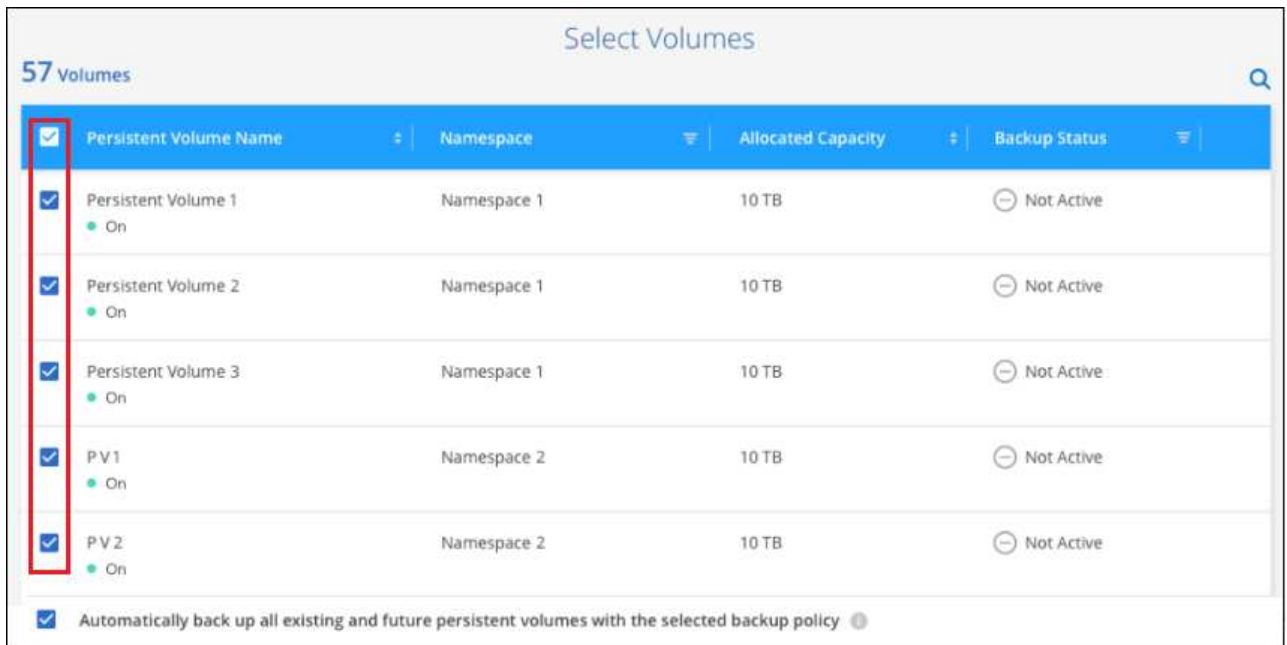


2. 백업 정책 세부 정보를 입력하고 * 다음 * 을 클릭합니다.

백업 스케줄을 정의하고 유지할 백업 수를 선택할 수 있습니다.

3. 백업할 영구 볼륨을 선택합니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume_1)를 클릭합니다.



4. 현재 및 향후 모든 볼륨에서 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.

백업 파일은 Cloud Volumes ONTAP 시스템과 동일한 Azure 가입 및 지역을 사용하는 Blob 컨테이너에 저장됩니다.

Kubernetes 대시보드가 표시되므로 백업 상태를 모니터링할 수 있습니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨을 복원합니다" Azure(동일한 지역)의 동일한 또는 다른 Kubernetes 클러스터에서 새 볼륨으로.

Kubernetes 영구 볼륨 데이터를 Google Cloud 스토리지에 백업

몇 가지 단계를 완료하여 GKE Kubernetes 클러스터의 영구 볼륨에서 Google Cloud 스토리지로 데이터 백업을 시작하십시오.

빠른 시작

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

<https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png>
 사전 요구 사항 검토

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다.
 - Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다.
 - 백업하려는 영구 체적을 생성하는 데 사용되는 모든 PVC는 "snapshotPolicy(스냅샷 정책)"를 "default(기본값)"로 설정해야 합니다.
 - 클러스터는 해당 백엔드 스토리지에 대해 GCP에서 Cloud Volumes ONTAP를 사용해야 합니다.

- Cloud Volumes ONTAP 시스템에서 ONTAP 9.7P5 이상을 실행해야 합니다.
- 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

작업 환경을 선택하고 오른쪽 패널에서 백업 및 복원 서비스 옆에 있는 * 활성화 * 를 클릭한 다음 설정 마법사를 따릅니다.



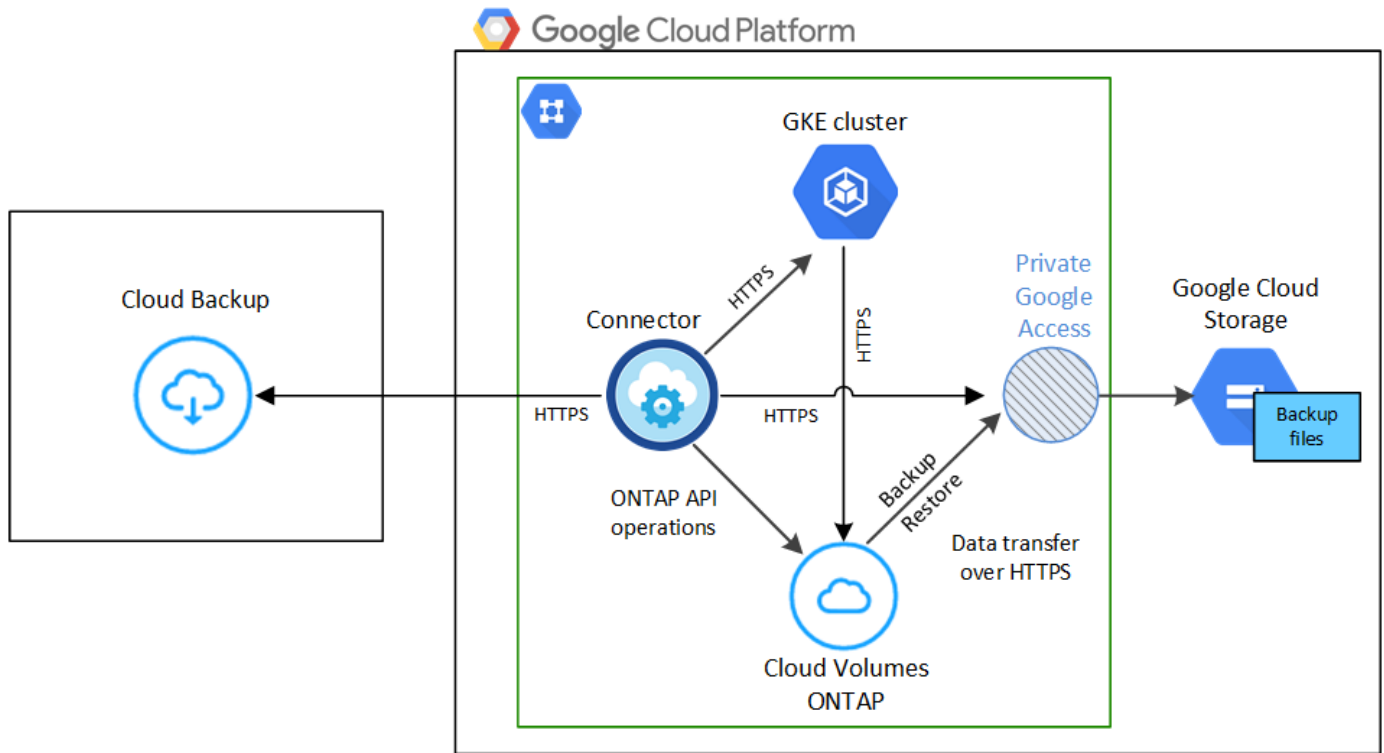
기본 정책은 매일 볼륨을 백업하고 각 볼륨의 최근 30개 백업 복사본을 유지합니다. 시간별, 일별, 주별 또는 월별 백업으로 변경하거나 더 많은 옵션을 제공하는 시스템 정의 정책 중 하나를 선택합니다. 보존할 백업 복사본의 수를 변경할 수도 있습니다.

Select Volumes 페이지에서 백업할 볼륨을 식별합니다. 백업 파일은 Cloud Volumes ONTAP 시스템과 동일한 GCP 구독 및 지역을 사용하는 Google Cloud Storage 버킷에 저장됩니다.

요구 사항

Kubernetes 영구 볼륨을 Google Cloud 스토리지에 백업하기 전에 다음 요구사항을 읽고 지원되는 구성이 있는지 확인합니다.

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



개별 엔드포인트가 선택 사항입니다.

Kubernetes 클러스터 요구사항

- Kubernetes 클러스터를 Cloud Manager 작업 환경으로 발견했습니다. "[Kubernetes 클러스터를 검색하는 방법을 알아보십시오](#)".
- Trident는 클러스터에 설치해야 하며 Trident 버전은 21.1 이상이어야 합니다. 을 참조하십시오 "[Trident 설치 방법](#)" 또는 "[Trident 버전을 업그레이드하는 방법](#)".
- 클러스터는 해당 백엔드 스토리지에 대해 GCP에서 Cloud Volumes ONTAP를 사용해야 합니다.
- Cloud Volumes ONTAP 시스템은 Kubernetes 클러스터와 같은 GCP 지역에 있어야 하며 ONTAP 9.7P5 이상을 실행해야 합니다(ONTAP 9.8P11 이상 권장).

사내 위치의 Kubernetes 클러스터는 지원되지 않습니다. Cloud Volumes ONTAP 시스템을 사용하는 클라우드 구축 환경의 Kubernetes 클러스터만 지원됩니다.

- 백업하려는 영구 볼륨을 생성하는 데 사용되는 모든 영구 볼륨 클레임 객체에는 "snapshotPolicy"가 "default"로 설정되어 있어야 합니다.

주석 아래에 '스냅샷 정책'을 추가하여 개별 PVC에 대해 이 작업을 수행할 수 있습니다.

```

kind: PersistentVolumeClaim
apiVersion: v1
metadata:
  name: full
  annotations:
    trident.netapp.io/snapshotPolicy: "default"
spec:
  accessModes:
    - ReadWriteMany
  resources:
    requests:
      storage: 1000Mi
  storageClassName: silver

```

backend.json 파일의 기본값 아래에 'shapshotPolicy' 필드를 추가하여 특정 백엔드 스토리지와 관련된 모든 PVC에 대해 이 작업을 수행할 수 있습니다.

```

apiVersion: trident.netapp.io/v1
kind: TridentBackendConfig
metadata:
  name: backend-tbc-ontap-nas-advanced
spec:
  version: 1
  storageDriverName: ontap-nas
  managementLIF: 10.0.0.1
  dataLIF: 10.0.0.2
  backendName: tbc-ontap-nas-advanced
  svm: trident_svm
  credentials:
    name: backend-tbc-ontap-nas-advanced-secret
  limitAggregateUsage: 80%
  limitVolumeSize: 50Gi
  nfsMountOptions: nfsvers=4
  defaults:
    spaceReserve: volume
    exportPolicy: myk8scluster
    snapshotPolicy: default
    snapshotReserve: '10'
    deletionPolicy: retain

```

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 가 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](#)".

클라우드 백업 활성화

Kubernetes 작업 환경에서 Cloud Backup을 바로 사용할 수 있습니다.

단계

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



2. 백업 정책 세부 정보를 입력하고 * 다음 * 을 클릭합니다.

백업 스케줄을 정의하고 유지할 백업 수를 선택할 수 있습니다.



3. 백업할 영구 볼륨을 선택합니다.

- 모든 볼륨을 백업하려면 제목 행(☒ Volume Name)를 클릭합니다.
- 개별 볼륨을 백업하려면 각 볼륨에 대한 확인란을 선택합니다(☒ Volume_1)를 클릭합니다.



4. 현재 및 향후 모든 볼륨에서 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.

백업 파일은 Cloud Volumes ONTAP 시스템과 동일한 GCP 구독 및 지역을 사용하는 Google Cloud Storage 버킷에 저장됩니다.

Kubernetes 대시보드가 표시되므로 백업 상태를 모니터링할 수 있습니다.

가능합니다 "볼륨에 대한 백업을 시작 및 중지하거나 백업 일정을 변경합니다". 또한 가능합니다 "백업 파일에서 전체 볼륨을 복원합니다" GCP(동일한 지역)의 동일한 또는 다른 Kubernetes 클러스터의 새 볼륨으로.

Kubernetes 시스템 백업 관리

백업 일정을 변경하고, 볼륨 백업을 활성화/비활성화하고, 백업을 삭제하는 등 Kubernetes 시스템의 백업을 관리할 수 있습니다.



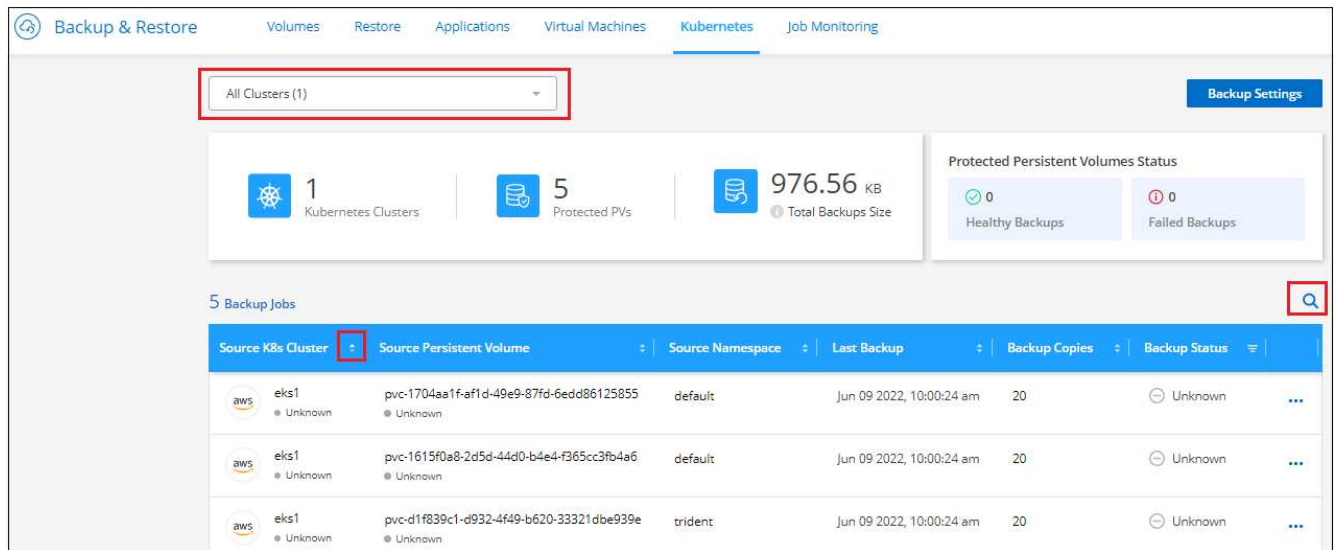
클라우드 공급자 환경에서 직접 백업 파일을 관리하거나 변경하지 마십시오. 이로 인해 파일이 손상되어 지원되지 않는 구성이 발생할 수 있습니다.

백업 중인 볼륨 보기

Cloud Backup에서 현재 백업 중인 모든 볼륨의 목록을 볼 수 있습니다.

단계

1. 백업 및 복원 * 서비스를 클릭합니다.
2. Kubernetes * 탭을 클릭하여 Kubernetes 시스템의 영구 볼륨 목록을 확인하십시오.



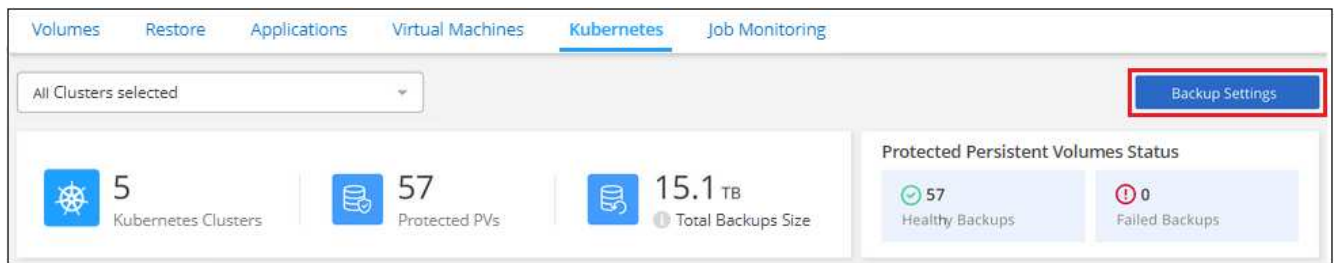
특정 클러스터에서 특정 볼륨을 찾는 경우 클러스터 및 볼륨별로 목록을 세분화하거나 검색 필터를 사용할 수 있습니다.

볼륨 백업 활성화 및 비활성화

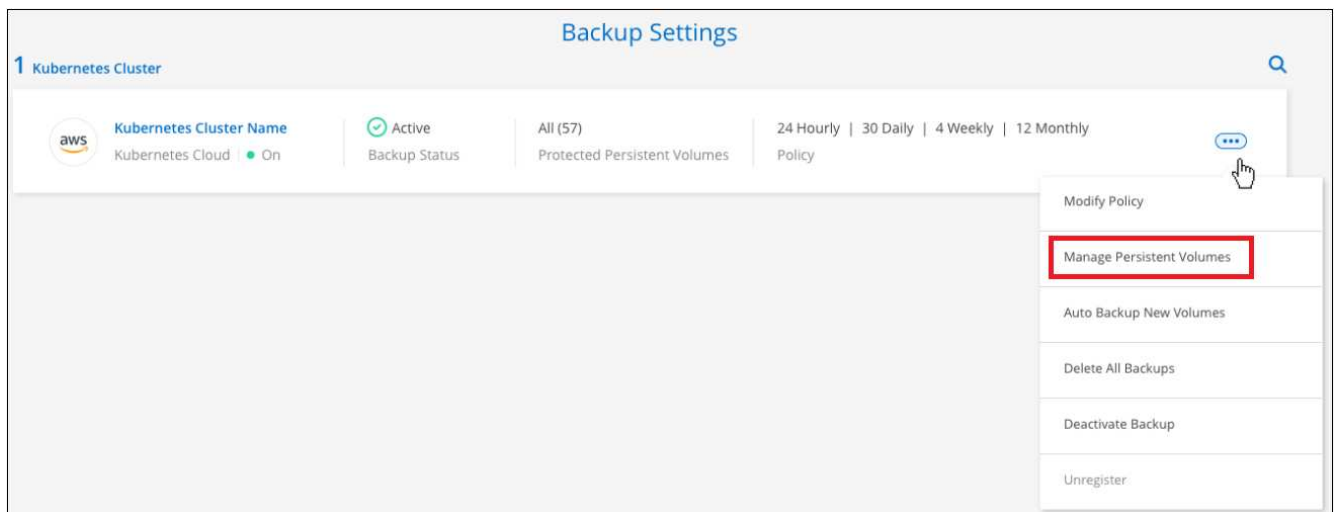
해당 볼륨의 백업 복사본이 필요하지 않고 백업 저장 비용을 지불하지 않으려는 경우 볼륨 백업을 중지할 수 있습니다. 현재 백업 중이 아닌 경우 백업 목록에 새 볼륨을 추가할 수도 있습니다.

단계

1. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.



2. 백업 설정 페이지에서 _ 을(를) 클릭합니다 ... Kubernetes 클러스터의 경우 * 영구 볼륨 관리 * 를 선택합니다.



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

Manage Volumes
Working Environment: CVO_Eng

60 Volumes

Search | **Activate** | Deactivate | Change Policy

<input type="checkbox"/>	Volume Name	Volume Type	SVM Name	Used Capacity	Policy	Backup Status	Modified
<input checked="" type="checkbox"/>	Volume_1 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input type="checkbox"/>	Volume_2 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input checked="" type="checkbox"/>	Volume_3 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	
<input type="checkbox"/>	Volume_4 On	RW	SVM_1	20.25 TiB	30 Daily, 13 Weekly, 3 Monthly, 1 Yearly	Active	

1 - 50 of 500 < 1 >

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. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.

Volumes | Restore | Applications | Virtual Machines | **Kubernetes** | Job Monitoring

All Clusters selected

Backup Settings

5
Kubernetes Clusters

57
Protected PVs

15.1 TB
Total Backups Size

Protected Persistent Volumes Status

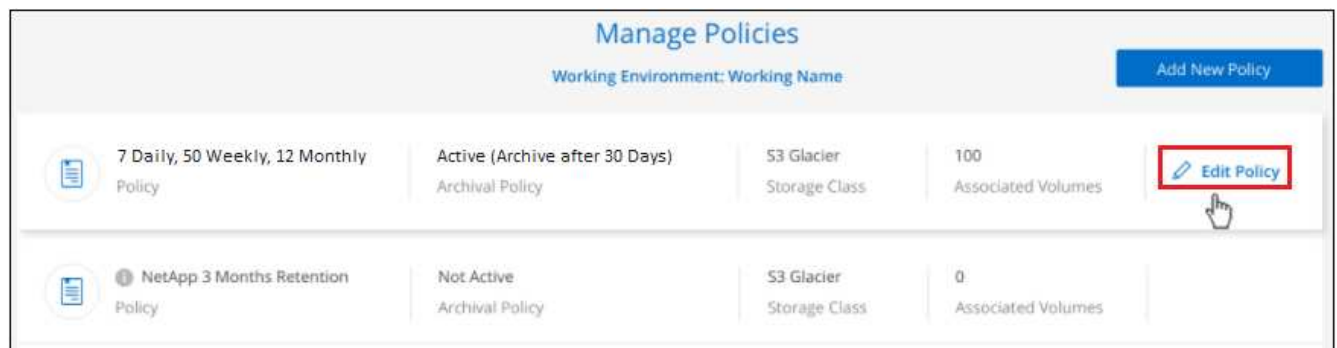
57
Healthy Backups

0
Failed Backups

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.



새 볼륨에 할당할 백업 정책 설정

Kubernetes 클러스터에서 Cloud Backup을 처음 활성화할 때 새로 생성된 볼륨에 백업 정책을 자동으로 할당하는 옵션을 선택하지 않은 경우, 나중에 *Backup Settings* 페이지에서 이 옵션을 선택할 수 있습니다. 새로 생성된 볼륨에 백업 정책을 할당하면 모든 데이터가 보호됩니다.

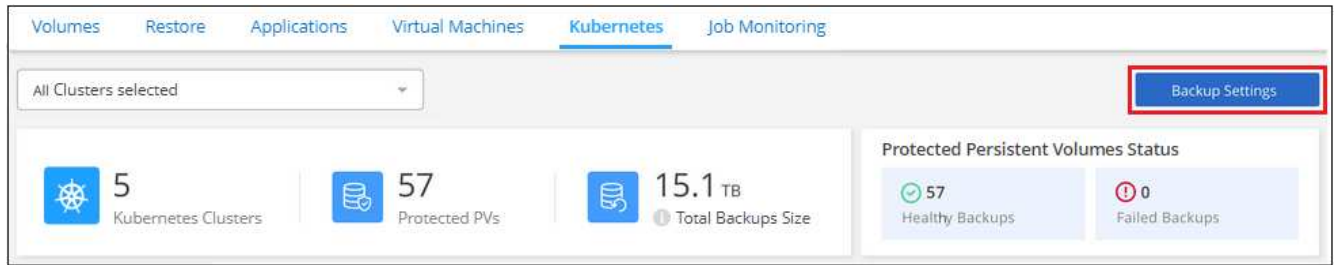
볼륨에 적용할 정책이 이미 있어야 합니다. [작업 환경에 대한 새 백업 정책을 추가하는 방법에 대해 알아봅니다.](#)

새로 생성된 볼륨이 자동으로 백업되지 않도록 이 설정을 비활성화할 수도 있습니다. 이 경우 나중에 백업하려는 특정

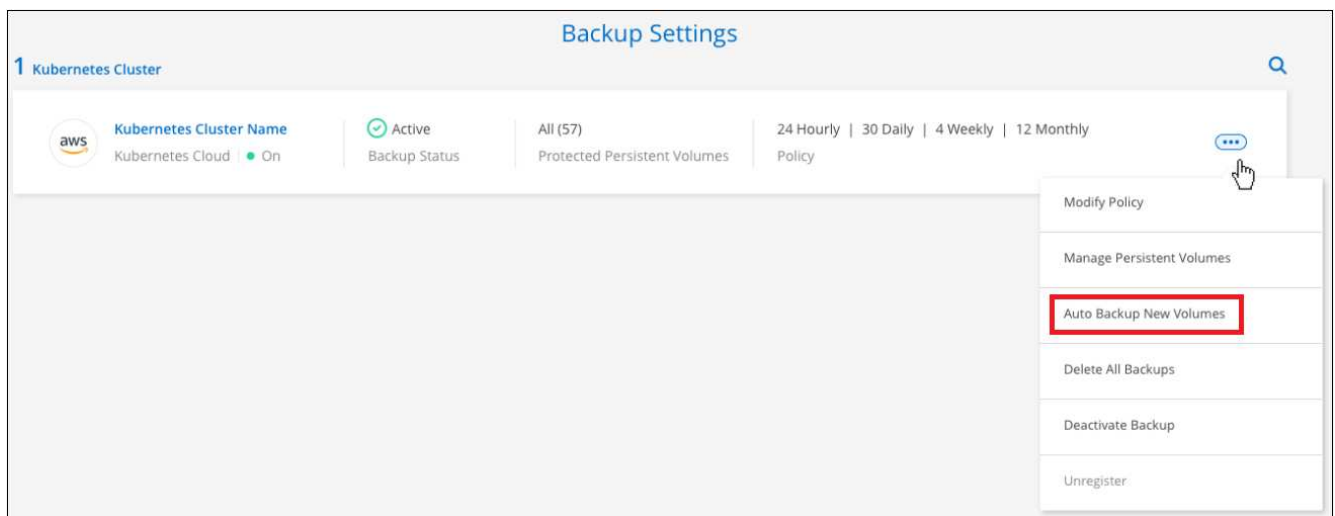
볼륨에 대해 백업을 수동으로 설정해야 합니다.

단계

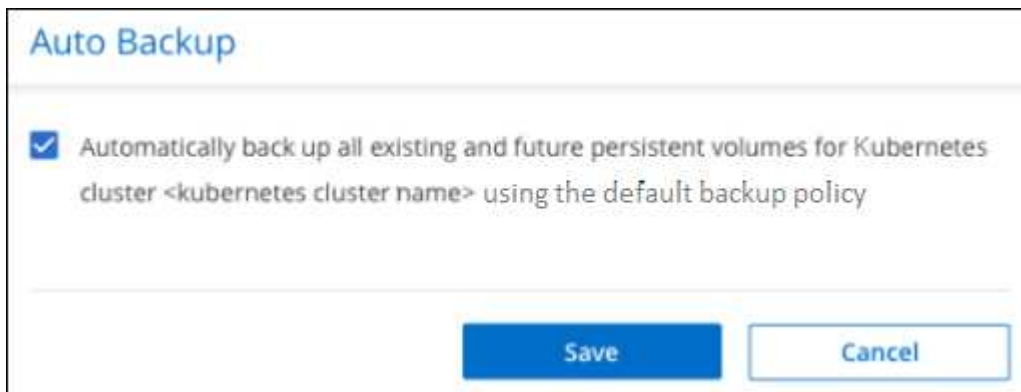
1. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.



2. 백업 설정 페이지에서 _을(를) 클릭합니다 ... 볼륨이 있는 Kubernetes 클러스터의 경우 * Auto Backup New Volumes * 를 선택합니다.



3. "Automatically back up future persistent volumes..." 확인란을 선택하고 새 볼륨에 적용할 백업 정책을 선택한 다음 * Save * 를 클릭합니다.



이제 이 백업 정책이 이 Kubernetes 클러스터에서 생성된 모든 새 볼륨에 적용됩니다.

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. Kubernetes * 탭에서 를 클릭합니다 ... 소스 볼륨에 대해 * Details & Backup List * 를 선택합니다.

Backup & Restore Volumes Restore Applications Virtual Machines **Kubernetes** Job Monitoring

All Kubernetes Clusters Backup Settings

1 Kubernetes Clusters 57 Protected PVs 15.1 TB Total Backups Size

Protected Persistent Volumes Status
57 Healthy Backup 0 Failed Backup

57 Backups

Source Kubernetes Cluster	Source Persistent Volume	Source Namespace	Last Backup	Backups	Backup Status
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Backups	Active
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	
Kubernetes_Cloud_AWS	Source Persistent Volume	Source Namespace	May 22 2019, 00:00:00	2,050 Snapshot	

Details & Backup List
Backup Now
Pause Backups

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

Source Destination Backup Information

Kubernetes Cluster: eks1 Cloud Provider: AWS Relationship Status: enabled

Type: EKS Bucket: netapp-backup-vsa5twmc9ae Last Backup: Dec 07 2021, 2:20:30 pm

Provider: AWS Region: us-west-1 Lag Duration: 1 hour

Persistent Volume: pvc-05881c70-cf5f-4edc-8537... Account ID: 123456789012 Backups: 2

Namespace: default Backup Policy: 24 hourly | 30 daily | 52 weekly

2 Backups

Backup Name	Date	Size
daily.dem-163887957011628bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:19:30 pm	9.77 KB
daily.dem-163887963015128bef197-34b5-11ec-8916-5b2669f1987a	Dec 07 2021, 2:20:30 pm	9.77 KB

Restore

백업을 삭제하는 중입니다

Cloud Backup을 사용하면 단일 백업 파일을 삭제하거나, 볼륨에 대한 모든 백업을 삭제하거나, Kubernetes 클러스터의 모든 볼륨에 대한 모든 백업을 삭제할 수 있습니다. 백업이 더 이상 필요하지 않거나 소스 볼륨을 삭제하고 모든 백업을 제거하려는 경우 모든 백업을 삭제할 수 있습니다.



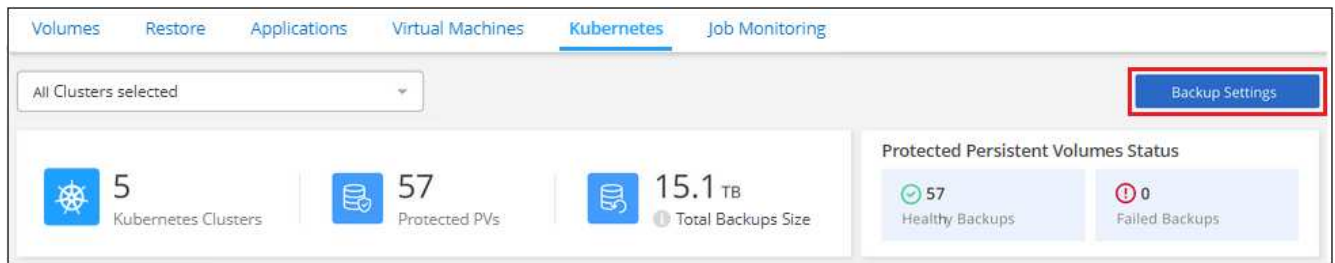
백업이 있는 작업 환경 또는 클러스터를 삭제하려면 * 시스템을 삭제하기 전에 * 백업을 삭제해야 합니다. Cloud Backup은 시스템을 삭제할 때 백업을 자동으로 삭제하지 않으며, 시스템이 삭제된 후 백업을 삭제할 수 있도록 UI에 현재 지원이 없습니다. 나머지 백업에 대한 오브젝트 스토리지 비용은 계속해서 청구됩니다.

작업 환경의 모든 백업 파일을 삭제하는 중입니다

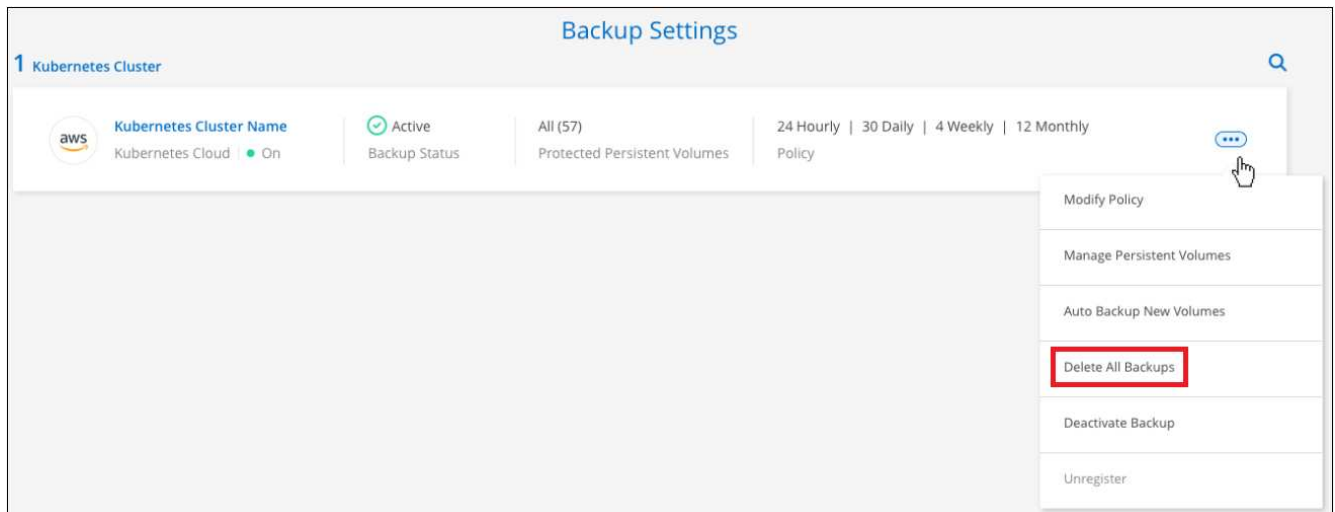
작업 환경의 모든 백업을 삭제해도 이 작업 환경의 볼륨에 대한 향후 백업이 비활성화되지는 않습니다. 작업 환경에서 모든 볼륨의 백업 생성을 중지하려면 백업을 비활성화할 수 있습니다 [참조하십시오](#).

단계

1. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.



2. 을 클릭합니다 ... 모든 백업을 삭제할 Kubernetes 클러스터의 경우 * Delete all backups * 를 선택합니다.



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

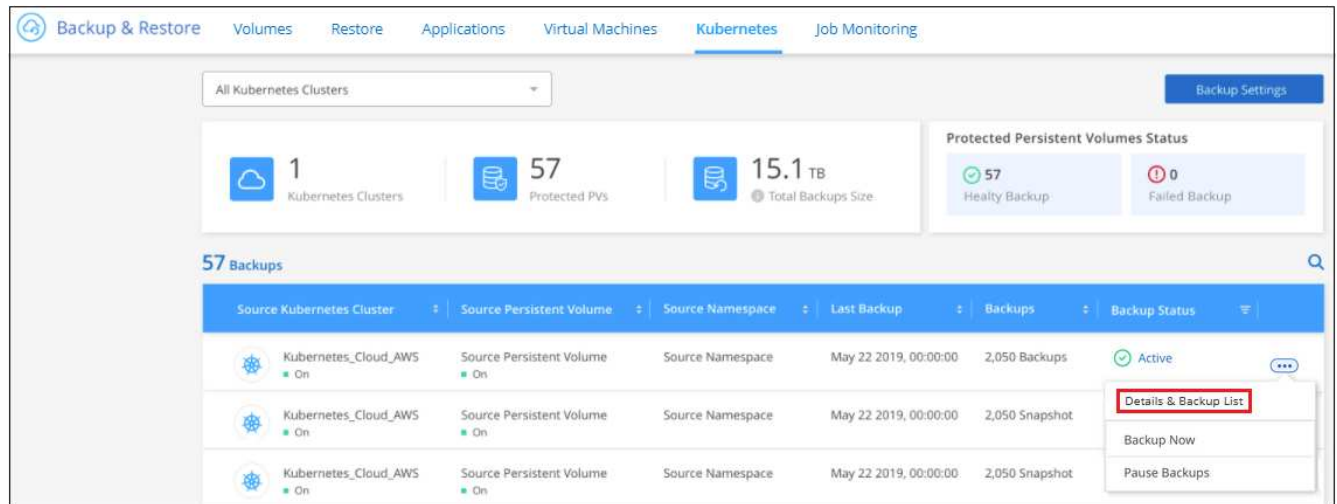
볼륨에 대한 모든 백업 파일을 삭제하는 중입니다

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

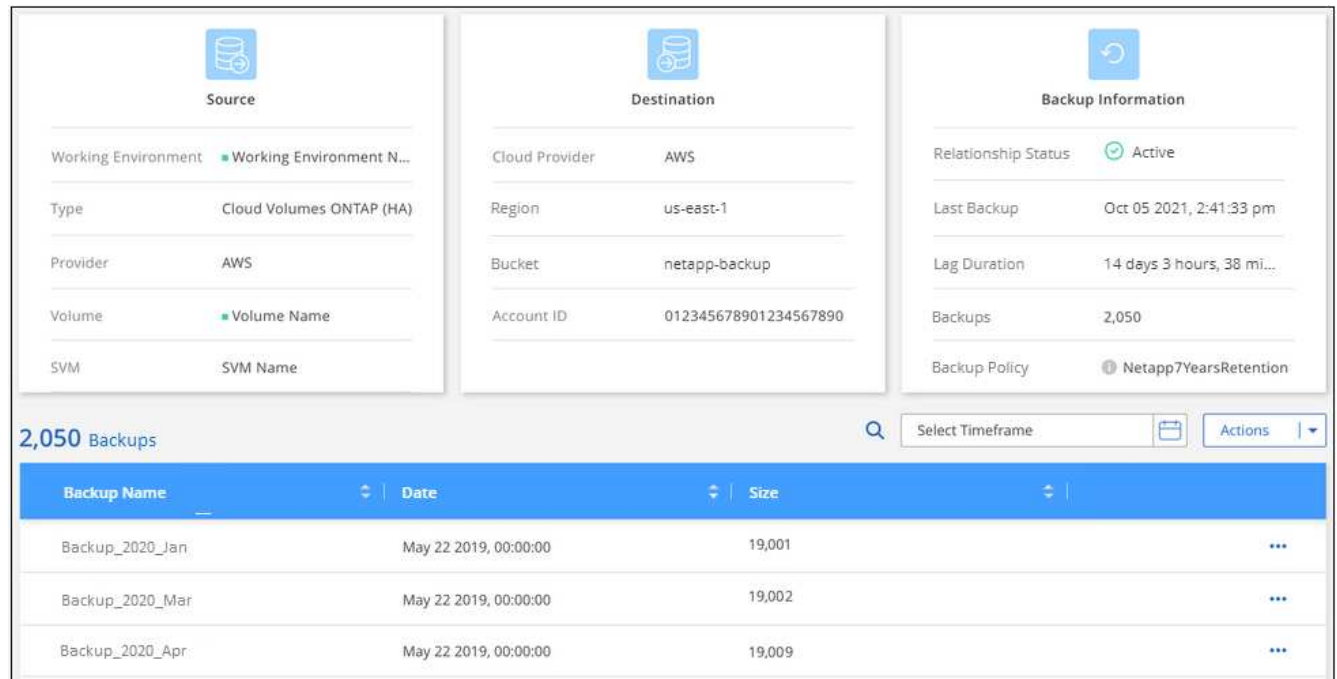
가능합니다 볼륨에 대한 백업을 다시 시작합니다 언제든지 백업 관리 페이지에서 수행할 수 있습니다.

단계

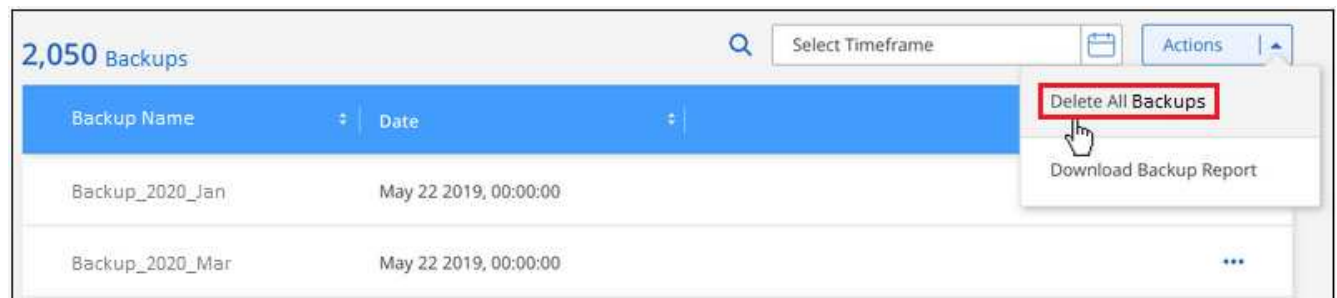
1. Kubernetes * 탭에서 를 클릭합니다 ... 소스 볼륨에 대해 * Details & Backup List * 를 선택합니다.



모든 백업 파일 목록이 표시됩니다.



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



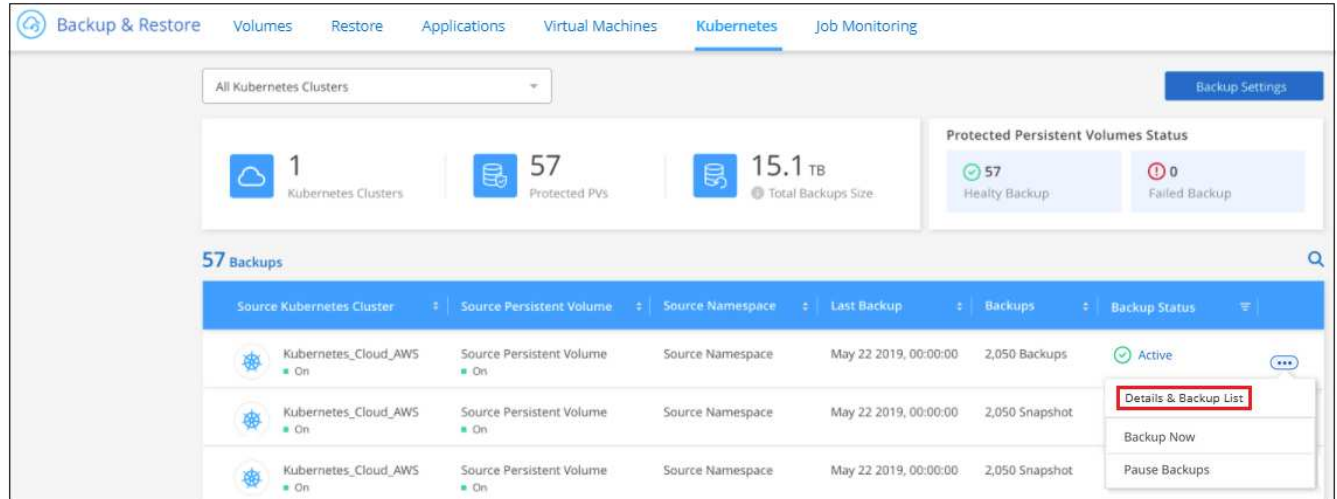
3. 확인 대화 상자에서 볼륨 이름을 입력하고 * 삭제 * 를 클릭합니다.

볼륨에 대한 단일 백업 파일 삭제

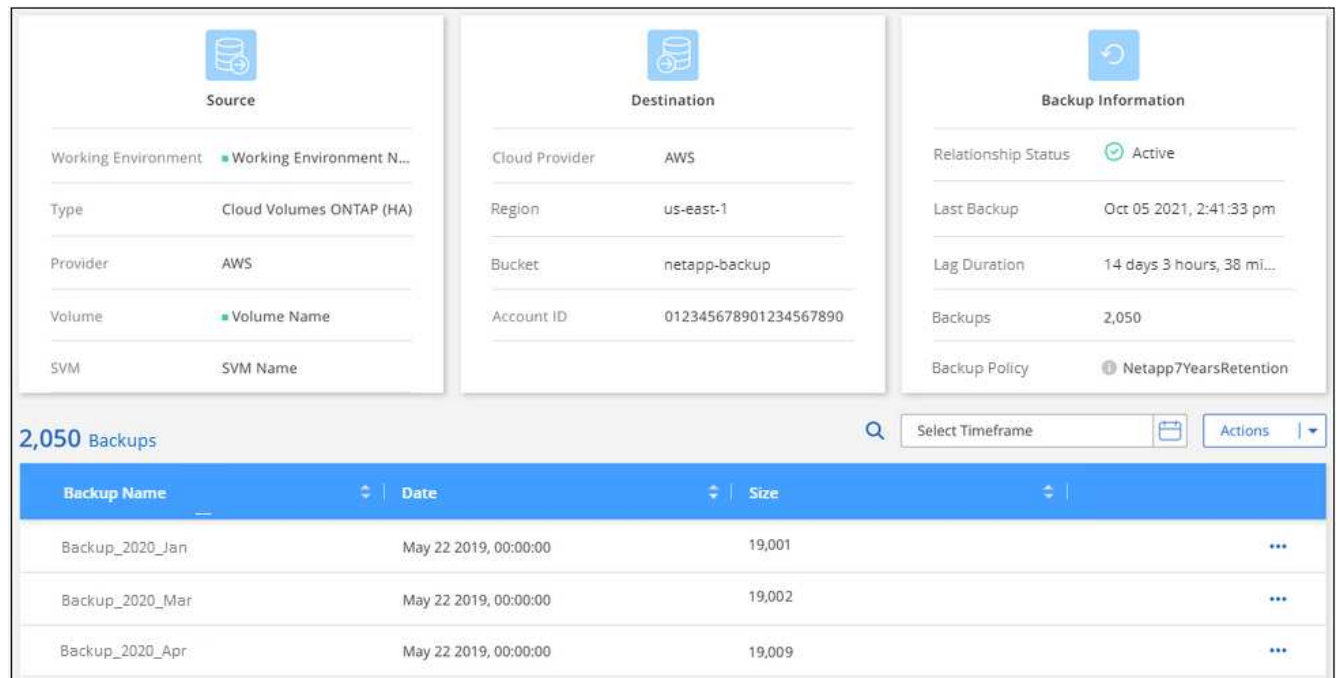
단일 백업 파일을 삭제할 수 있습니다. 이 기능은 ONTAP 9.8 이상의 시스템에서 볼륨 백업을 생성한 경우에만 사용할 수 있습니다.

단계

1. Kubernetes * 탭에서 를 클릭합니다 ... 소스 볼륨에 대해 * Details & Backup List * 를 선택합니다.



모든 백업 파일 목록이 표시됩니다.



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



3. 확인 대화 상자에서 * 삭제 * 를 클릭합니다.

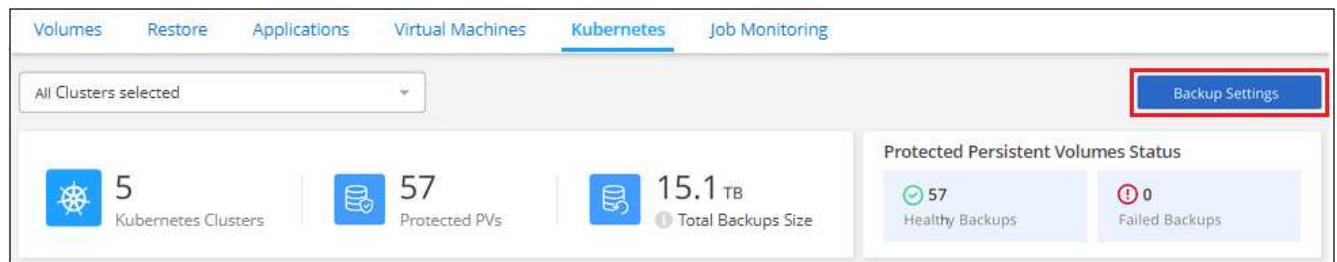
작업 환경에서 Cloud Backup을 해제합니다

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.

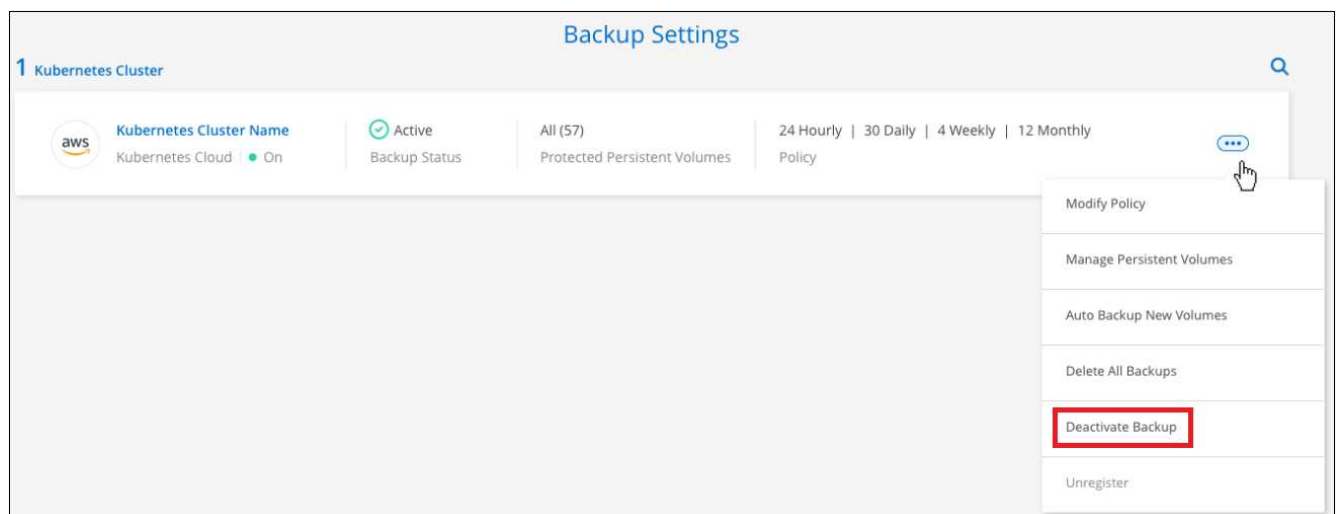
사용자가 비용을 부담하지 않는 한, 클라우드 공급자가 백업 용량에 대한 오브젝트 스토리지 비용에 대해 계속 청구한다는 점에 유의하십시오 **백업을 삭제합니다**.

단계

1. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.



2. 백업 설정 페이지에서 _ 을(를) 클릭합니다 ... 작업 환경 또는 Kubernetes 클러스터의 경우 백업을 비활성화하고 * 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 Kubernetes 클러스터를 삭제할 계획이고 백업 서비스를 취소하려는 경우에 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.

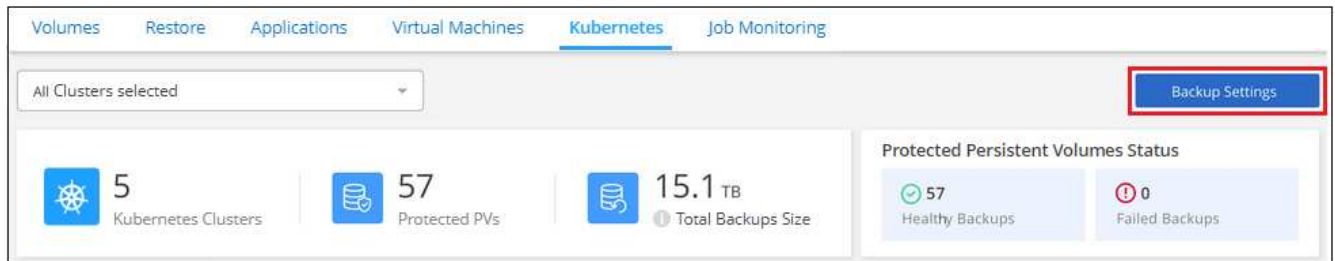
클라우드 백업을 등록 취소하려면 먼저 다음 단계를 순서대로 수행해야 합니다.

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

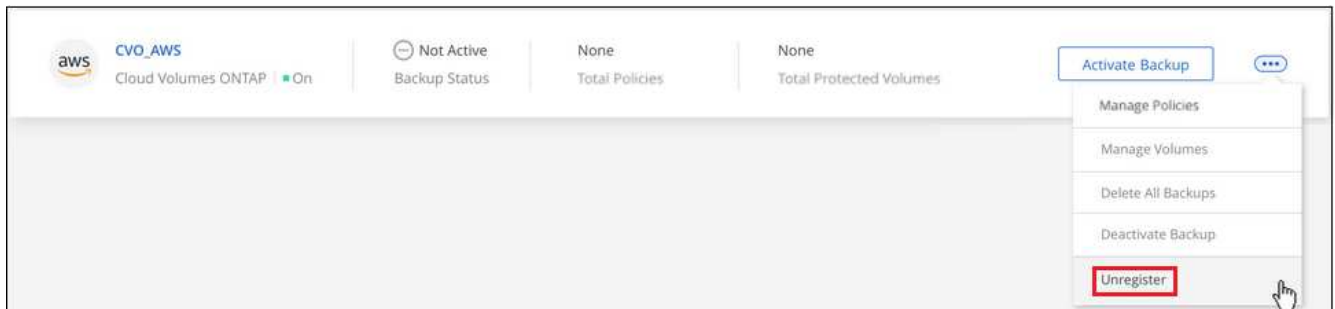
이 두 작업이 완료될 때까지 등록 취소 옵션을 사용할 수 없습니다.

단계

1. Kubernetes * 탭에서 * 백업 설정 * 을 선택합니다.



2. 백업 설정 페이지에서 _을(를) 클릭합니다 ... 백업 서비스의 등록을 취소하려는 Kubernetes 클러스터의 경우 * 등록 취소 * 를 선택합니다.



3. 확인 대화 상자에서 * 등록 취소 * 를 클릭합니다.

백업 파일에서 **Kubernetes** 데이터를 복원하는 중입니다

백업은 클라우드 계정의 오브젝트 저장소에 저장되므로 특정 시점에서 데이터를 복원할 수 있습니다. 저장된 백업 파일에서 전체 Kubernetes 영구 볼륨을 복원할 수 있습니다.

영구 볼륨(새 볼륨)을 동일한 작업 환경 또는 동일한 클라우드 계정을 사용하는 다른 작업 환경에 복원할 수 있습니다.

지원되는 작업 환경 및 오브젝트 스토리지 공급자

Kubernetes 백업 파일에서 다음 작업 환경으로 볼륨을 복원할 수 있습니다.

백업 파일 위치	대상 작업 환경 ifdef::AWS[]
Amazon S3	AWS endif::AWS[]ifdef::Azure[]의 Kubernetes 클러스터
Azure Blob	Azure endif의 Kubernetes 클러스터::Azure []ifdef::GCP[]
Google 클라우드 스토리지	Google endif의 Kubernetes 클러스터::GCP[]

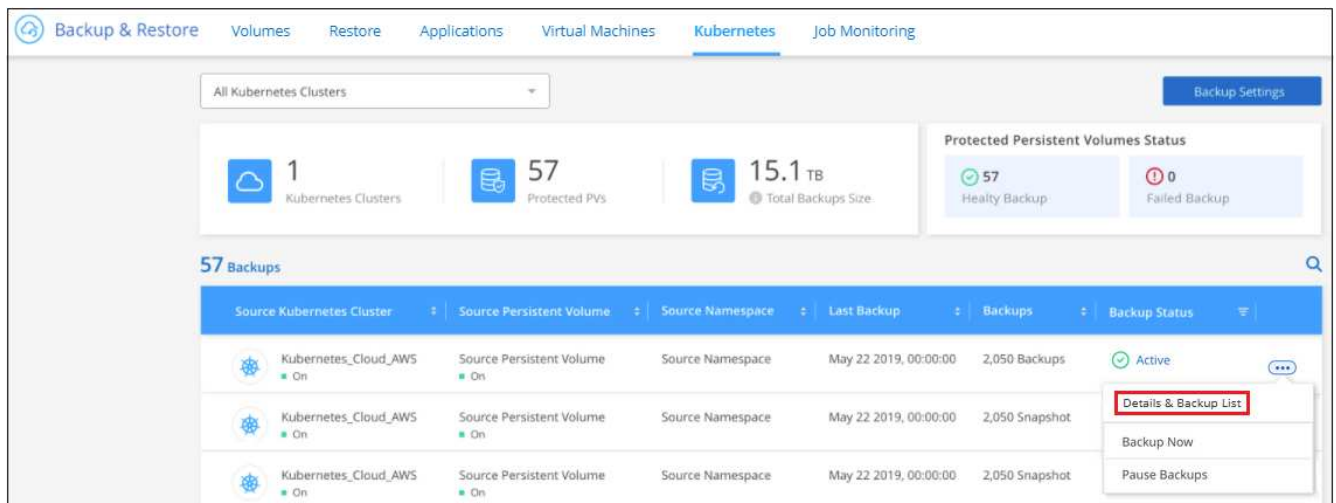
Kubernetes 백업 파일에서 볼륨 복원

백업 파일에서 영구 볼륨을 복구할 때 Cloud Manager는 백업의 데이터를 사용하여 `_new_volume`을 생성합니다. 동일한 Kubernetes 클러스터의 볼륨이나 소스 Kubernetes 클러스터와 같은 클라우드 계정에 있는 다른 Kubernetes 클러스터로 데이터를 복원할 수 있습니다.

시작하기 전에 복원하려는 볼륨의 이름과 새로 복구된 볼륨을 생성하는 데 사용할 백업 파일의 날짜를 알아야 합니다.

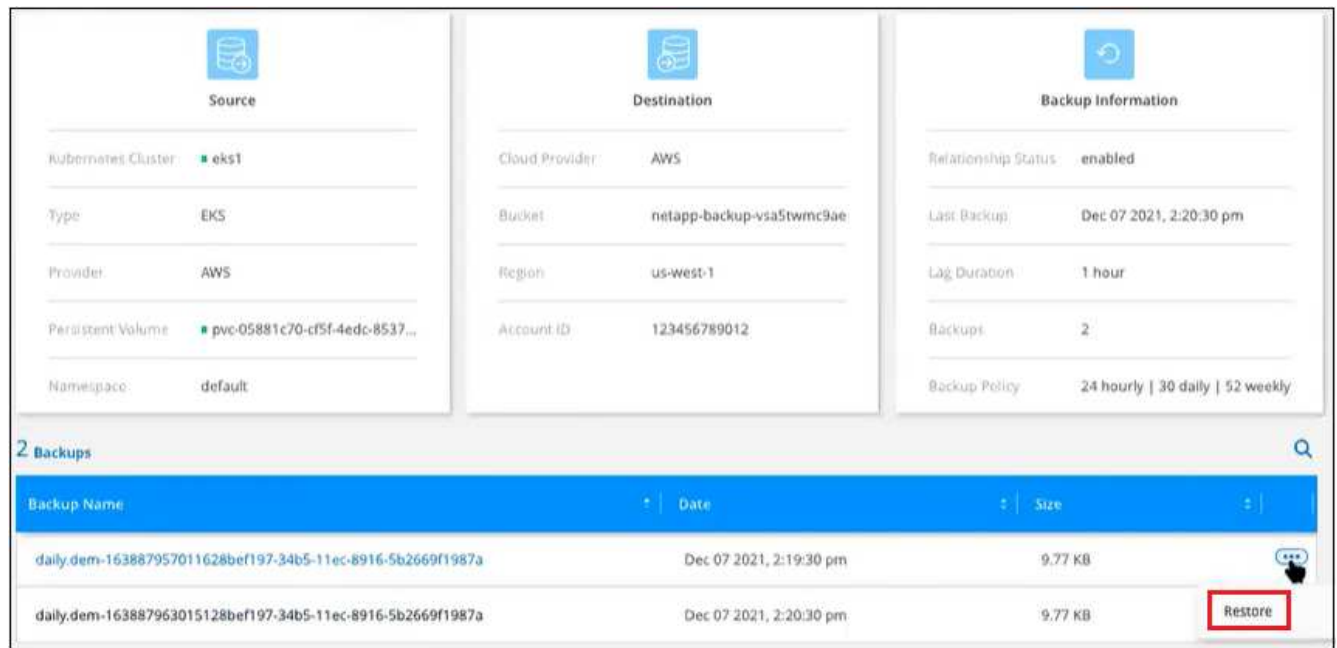
단계

1. 백업 및 복원 * 서비스를 선택합니다.
2. Kubernetes * 탭을 클릭하면 Kubernetes 대시보드가 표시됩니다.



3. 복원하려는 볼륨을 찾은 후 을 클릭합니다 ...를 클릭한 다음 * 세부 정보 및 백업 목록 * 을 클릭합니다.

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



4. 날짜/시간 스탬프를 기준으로 복원하려는 특정 백업 파일을 찾은 후 을 클릭합니다 ..., * 복원 * 을 차례로 클릭합니다.
5. Select Destination_ 페이지에서 볼륨을 복구할 _Kubernetes 클러스터 _, _ 네임스페이스 _, _ 스토리지 클래스 _ 및 새 _ 영구 볼륨 이름 _ 을(를) 선택합니다.

Select Destination

Select Kubernetes Cluster:

eks1

Namespace

default

Storage Class

basic

PVC Name

pvc-05881c70-cf5f-4edc-8537-a0a5ce36f9a1-restore

Cancel

Restore

6. 복원 * 을 클릭하면 복원 작업의 진행률을 검토할 수 있도록 Kubernetes 대시보드로 돌아갑니다.

Cloud Manager는 선택한 백업을 기반으로 Kubernetes 클러스터에 새 볼륨을 생성합니다. 가능합니다 "이 새 볼륨에 대한 백업 설정을 관리합니다" 필요에 따라.

사내 애플리케이션 데이터를 백업 및 복원합니다

온프레미스 애플리케이션 데이터를 보호합니다

Cloud Backup for Applications를 Cloud Manager 및 사내 SnapCenter와 통합하여 사내 ONTAP에서 클라우드로 애플리케이션 정합성을 보장하는 스냅샷을 백업할 수 있습니다. 필요한 경우 클라우드에서 사내 SnapCenter 서버로 복원할 수 있습니다.

Oracle 및 Microsoft SQL 애플리케이션 데이터를 사내 ONTAP 시스템에서 다음 클라우드 공급자로 백업할 수 있습니다.

- Amazon Web Services에서 직접 지원합니다
- Microsoft Azure를 참조하십시오



SnapCenter 소프트웨어 4.6을 사용해야 합니다.

Cloud Backup for Applications에 대한 자세한 내용은 다음을 참조하십시오.

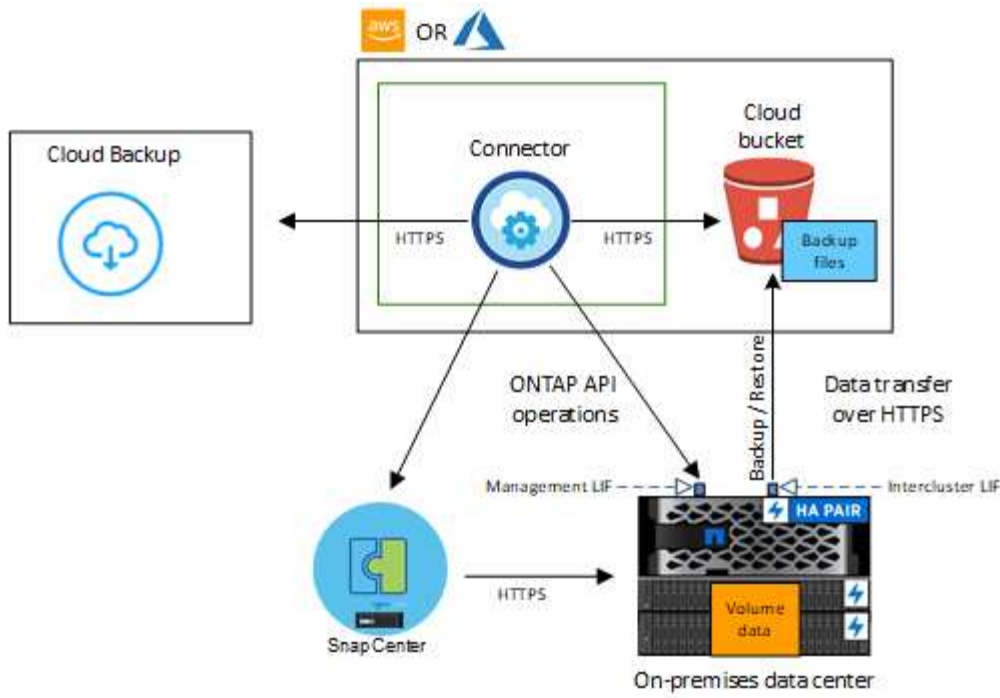
- ["클라우드 백업 및 SnapCenter를 통한 애플리케이션 인식 백업"](#)
- ["애플리케이션을 위한 클라우드 백업"](#)

요구 사항

애플리케이션 데이터를 클라우드 서비스에 백업하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인합니다.

- ONTAP 9.8 이상
- Cloud Manager 3.9
- SnapCenter 서버 4.6
- SnapCenter 서버에서 응용 프로그램당 하나 이상의 백업을 사용할 수 있어야 합니다
- SnapCenter에서 Cloud Manager의 클라우드 백업 애플리케이션 정책과 레이블 또는 레이블이 없는 일별, 주별 또는 월별 정책 하나 이상

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



보호 정책

Cloud Backup for Applications에 정의된 정책 중 하나를 사용하여 애플리케이션 데이터를 클라우드에 백업해야 합니다.



사용자 지정 정책은 지원되지 않습니다.

정책 이름	라벨	보존 값
1년 일일 LTR	매일	366
5년 일일 LTR	매일	1830
7년 주간 LTR	매주	370
10년 월간 LTR	매월	120

이러한 정책의 레이블 및 보존 값은 정책이 애플리케이션과 연결될 때까지 REST API를 사용하여 수정할 수 있습니다. 하나의 정책만 응용 프로그램에 연결할 수 있고 한 번 연결된 경우에는 연결을 해제할 수 없습니다.

클라우드 백업 for Applications 정책 외에도, 애플리케이션 데이터를 클라우드에 백업하려면 적어도 하나의 SnapCenter 정책도 필요합니다.

사내 애플리케이션 데이터를 클라우드에 백업

Cloud Backup for Applications를 Cloud Manager 및 사내 SnapCenter와 통합하여 ONTAP에서 클라우드로 애플리케이션 데이터를 백업할 수 있습니다.

SnapCenter 서버를 등록합니다

SnapCenter 서버 4.6이 실행 중인 호스트는 SnapCenterAdmin 역할을 가진 사용자만 등록할 수 있습니다. 여러 SnapCenter 서버 호스트를 등록할 수 있지만, 일단 등록하면 SnapCenter 서버 호스트를 제거할 수 없습니다.

• 단계 *

1. Cloud Manager UI에서 * 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * SnapCenter 서버 * 를 클릭합니다.
3. SnapCenter 서버 등록 * 을 클릭합니다.
4. 다음 세부 정보를 지정합니다.
 - a. SnapCenter 서버 필드에서 SnapCenter 서버 호스트의 FQDN 또는 IP 주소를 지정합니다.
 - b. 포트 필드에서 SnapCenter 서버가 실행 중인 포트 번호를 지정합니다.

SnapCenter 서버와 클라우드 응용 프로그램 백업 간에 통신이 이루어지게 하려면 포트가 열려 있어야 합니다.

- c. 태그 필드에서 SnapCenter 서버에 태그를 지정할 사이트 이름, 도시 이름 또는 사용자 지정 이름을 지정합니다.

태그는 쉼표로 구분됩니다.

- d. 사용자 이름 및 암호 필드에서 SnapCenterAdmin 역할을 가진 사용자의 자격 증명을 지정합니다.

5. Register * 를 클릭합니다.

• 완료 후 *

등록된 SnapCenter 서버 호스트를 사용하여 보호되는 모든 응용 프로그램을 보려면 * 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.



SQL Server 데이터베이스의 경우 Application Name 옆에 _application_name(호스트 이름)_format으로 이름이 표시됩니다. 이름을 _application_name(호스트 이름)_format으로 입력하여 검색하면 SQL Server 데이터베이스 세부 정보가 표시되지 않습니다.

지원되는 응용 프로그램 및 해당 구성은 다음과 같습니다.

- Oracle 데이터베이스: 최소 1일, 주별 또는 월별 스케줄을 사용하여 생성된 전체 백업(데이터 + 로그)
- Microsoft SQL Server 데이터베이스:
 - 독립 실행형, 파일오버 클러스터 인스턴스, 가용성 그룹
 - 최소 1개의 일일, 주별 또는 월별 스케줄을 사용하여 생성된 전체 백업입니다

다음 Oracle 및 SQL Server 데이터베이스는 표시되지 않습니다.

- 백업이 없는 데이터베이스입니다
- 주문형 또는 시간별 정책만 있는 데이터베이스
- RDM 또는 VMDK에 상주하는 데이터베이스입니다

애플리케이션 데이터를 백업합니다

단일 정책을 사용하여 하나 이상의 애플리케이션을 클라우드에 동시에 보호할 수 있습니다. 기본 사전 스캔 정책만 할당하여 애플리케이션을 보호할 수 있습니다.



Cloud Manager GUI를 사용하는 경우 한 번에 하나의 애플리케이션만 보호할 수 있습니다. 그러나 REST API를 사용하는 경우 여러 애플리케이션을 동시에 보호할 수 있습니다.

SQL Server 인스턴스를 보호하는 경우 해당 인스턴스에 있는 해당 데이터베이스의 모든 볼륨에 대해 클라우드 보호가 구성됩니다. SQL Server 가용성 그룹을 보호하는 경우 해당 가용성 그룹에 있는 데이터베이스의 모든 볼륨에 대해 클라우드 보호가 구성됩니다. 그러나 백업 기본 설정에 따라 해당 볼륨에서 스냅샷이 복사됩니다.

• 단계 *

1. Cloud Manager UI에서 * 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 을 클릭합니다 ... 응용 프로그램에 해당하는 을 클릭하고 * 백업 활성화 * 를 클릭합니다.
3. 작업 환경을 추가합니다.

애플리케이션이 실행되고 있는 SVM을 호스팅하는 ONTAP 클러스터를 구성합니다. 애플리케이션 중 하나에 대한 작업 환경을 추가한 후 동일한 ONTAP 클러스터에 있는 다른 모든 애플리케이션에 다시 사용할 수 있습니다.

- a. SVM을 선택하고 작업 환경 추가를 클릭합니다.
- b. 작업 환경 추가 마법사에서 다음을 수행합니다.
 - i. ONTAP 클러스터의 IP 주소를 지정합니다.
 - ii. 관리자 자격 증명을 지정합니다.

Cloud Backup for Applications는 클러스터 관리자만 지원합니다.

- c. 작업 환경 추가 * 를 클릭합니다.



작업 환경 세부 정보가 업데이트될 때까지 진행해서는 안 됩니다. 작업 환경 세부 정보를 업데이트하는 데 최대 30분이 걸릴 수 있습니다. 30분 후 마법사를 닫고 1단계에서 다시 시도하여 작업 환경 세부 정보를 확인해야 합니다. 작업 환경 세부 정보가 업데이트되지 않은 경우 다시 시도한 후 올바른 작업 환경을 추가했는지 확인하십시오.

4. 클라우드 공급자를 선택하고 구성합니다.

Amazon Web Services를 구성합니다

- a. AWS 계정을 지정합니다.
- b. AWS 액세스 키 필드에서 키를 지정합니다.
- c. AWS 암호 키 필드에 암호를 지정합니다.
- d. 백업을 생성할 영역을 선택합니다.
- e. 작업 환경으로 추가된 ONTAP 클러스터의 IP 주소를 지정합니다.

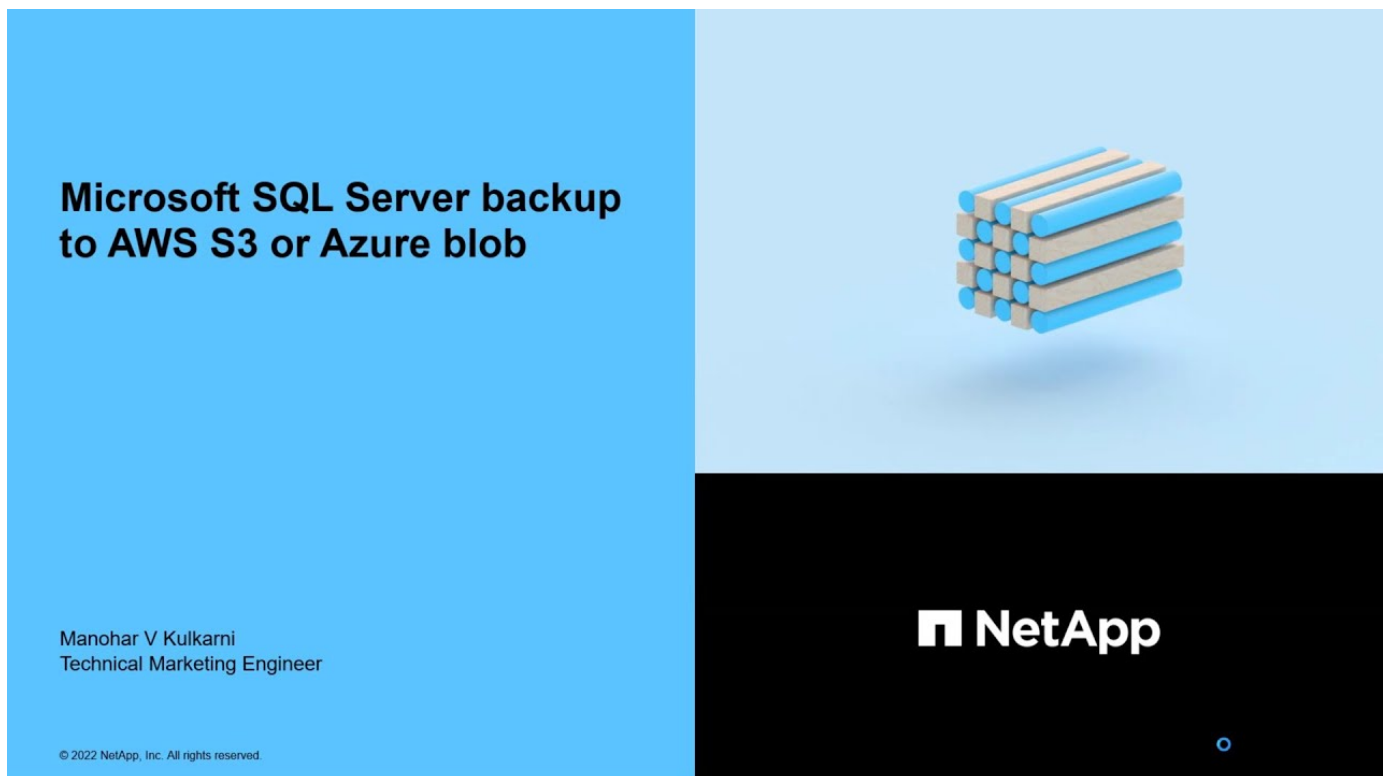
Microsoft Azure를 구성합니다

- a. Azure 구독 ID를 지정합니다.
- b. 백업을 생성할 영역을 선택합니다.
- c. 새 자원 그룹을 만들거나 기존 자원 그룹을 사용합니다.
- d. 작업 환경으로 추가된 ONTAP 클러스터의 IP 주소를 지정합니다.

5. 정책 할당 페이지에서 정책을 선택하고 * 다음 * 을 클릭합니다.

6. 세부 정보를 검토하고 * 백업 활성화 * 를 클릭합니다.

다음 비디오에서는 데이터베이스 보호에 대한 간단한 단계별 안내를 보여 줍니다.



애플리케이션 보호 관리

정책과 백업을 볼 수 있습니다. 데이터베이스, 정책 또는 리소스 그룹의 변경에 따라 Cloud Manager UI에서 업데이트를 새로 고칠 수 있습니다.

정책을 봅니다

사전 구성된 기본 정책을 모두 볼 수 있습니다. 각 정책에 대해 연결된 모든 Cloud Backup for Applications 정책과 모든 관련 애플리케이션이 나열됩니다.

1. 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * 정책 * 을 클릭합니다.
3. 세부 정보를 보려는 정책에 해당하는 * 세부 정보 보기 * 를 클릭합니다.

연결된 Cloud Backup for Applications 정책과 모든 애플리케이션이 나열됩니다.



Cloud Backup for Applications 정책은 삭제할 수 없습니다.

Get-SmResources SnapCenter cmdlet을 실행하여 클라우드 확장 SnapCenter 정책을 볼 수도 있습니다. cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 Get-Help command_name을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)".

클라우드에서 백업 보기

Cloud Manager UI에서 클라우드의 백업을 볼 수 있습니다.

1. 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 을 클릭합니다 ... 해당 응용 프로그램에 대해 * 세부 정보 보기 * 를 클릭합니다.



백업이 나열되는 데 걸리는 시간은 ONTAP의 기본 복제 일정(최대 1시간) 및 Cloud Manager(최대 6시간)에 따라 다릅니다.

- Oracle 데이터베이스의 경우 데이터 및 로그 백업, 각 백업에 대한 SCN 번호, 각 백업에 대한 종료 날짜가 모두 나열됩니다. 데이터 백업만 선택하고 데이터베이스를 온-프레미스 SnapCenter 서버로 복원할 수 있습니다.
- Microsoft SQL Server 데이터베이스의 경우 각 백업의 전체 백업과 종료 날짜만 나열됩니다. 백업을 선택하고 데이터베이스를 온-프레미스 SnapCenter 서버로 복원할 수 있습니다.
- Microsoft SQL Server 인스턴스의 경우 백업이 표시되지 않고 해당 인스턴스 아래에 있는 데이터베이스만 나열됩니다.



클라우드 보호를 설정하기 전에 생성된 백업은 복구에 표시되지 않습니다.

Get-SmBackup SnapCenter cmdlet을 실행하여 이러한 백업을 볼 수도 있습니다. cmdlet과 함께 사용할 수 있는 매개 변수와 이에 대한 설명은 Get-Help command_name을 실행하여 얻을 수 있습니다. 또는 을 참조할 수도 있습니다 "[SnapCenter 소프트웨어 cmdlet 참조 가이드](#)".

데이터베이스 레이아웃 변경

데이터베이스에 볼륨이 추가되면 SnapCenter 서버는 정책 및 일정에 따라 새 볼륨에 스냅샷에 자동으로 레이블을 지정합니다. 이러한 새 볼륨에는 개체 저장소 끝점이 없으며 다음 단계를 실행하여 새로 고쳐야 합니다.

1. 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * SnapCenter 서버 * 를 클릭합니다.

3. 을 클릭합니다 ... 응용 프로그램을 호스팅하는 SnapCenter 서버에 해당하는 을 클릭하고 * 새로 고침 * 을 클릭합니다.

새 볼륨이 검색됩니다.

4. 을 클릭합니다 ... 새 볼륨에 대한 클라우드 보호를 활성화하려면 응용 프로그램에 해당하는 * 보호 새로 고침 * 을 클릭합니다.

클라우드 서비스를 구성한 후 애플리케이션에서 스토리지 볼륨을 제거하면 새 백업의 경우 SnapCenter Server는 애플리케이션이 상주하는 스냅샷에 대해서만 레이블을 지정합니다. 제거된 볼륨을 다른 응용 프로그램에서 사용하지 않는 경우 개체 저장소 관계를 수동으로 삭제해야 합니다. 애플리케이션 인벤토리를 업데이트하면 애플리케이션의 현재 스토리지 레이아웃이 포함됩니다.

정책 또는 리소스 그룹 변경

SnapCenter 정책 또는 리소스 그룹이 변경된 경우 보호 기능을 새로 고쳐야 합니다.

1. 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 을 클릭합니다 ... 응용 프로그램에 해당하는 을 클릭하고 * 보호 새로 고침 * 을 클릭합니다.

작업을 모니터링합니다

모든 클라우드 백업 작업에 대한 작업이 생성됩니다. 각 작업의 일부로 수행되는 모든 작업과 모든 하위 작업을 모니터링할 수 있습니다.

1. 백업 및 복원 * > * 작업 모니터링 * 을 클릭합니다.

작업을 시작하면 작업이 시작되었다는 창이 나타납니다. 링크를 클릭하여 작업을 모니터링할 수 있습니다.

2. 각 하위 작업의 하위 작업 및 상태를 보려면 기본 작업을 클릭합니다.

CA 인증서를 구성합니다

CA 인증서가 있는 경우 루트 CA 인증서를 커넥터 컴퓨터에 수동으로 복사해야 합니다.

그러나 CA 인증서가 없는 경우에는 CA 인증서를 구성하지 않고 계속 진행할 수 있습니다.

• 단계 *

1. Docker 에이전트에서 액세스할 수 있는 볼륨에 인증서를 복사합니다.

- "cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_certs"
- "chmod 777 sc_certs"

2. RootCA 인증서 파일을 커넥터 컴퓨터의 위 폴더로 복사합니다.

```
'cp<path on  
connector>/<filename>/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_certs'
```

3. Docker 에이전트에서 액세스할 수 있는 볼륨에 CRL 파일을 복사합니다.

- "cd /var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/mkdir sc_CRL"

- "chmod 777 sc_CRL"

4. CRL 파일을 커넥터 시스템의 위 폴더에 복사합니다.

```
'cp<path on connector>/<filename>/var/lib/docker/volumes/cloudmanager_snapcenter_volume/_data/sc_CRL'
```

5. 인증서와 CRL 파일을 복사한 후 Cloud Backup for Apps 서비스를 다시 시작합니다.

- 'SUDO Docker Exec cloudmanager_snapcenter SED-I's/skipSCCertValidation: true/skipSCCertValidation: false/g'/opt/NetApp/cloudmanager-snapcenter-agent/config/config.yml'
- 'SUDO Docker restart cloudmanager_snapcenter'를 선택합니다

애플리케이션 데이터를 복원합니다

Oracle 데이터베이스를 복원합니다

Oracle 데이터베이스는 동일한 SnapCenter 서버 호스트, 동일한 SVM 또는 동일한 데이터베이스 호스트에만 복원할 수 있습니다. RAC 데이터베이스의 경우 백업이 생성된 사내 노드에 데이터가 복구됩니다.

제어 파일 복원이 있는 전체 데이터베이스만 지원됩니다. 아카이브 로그가 AFS에 없는 경우 복구에 필요한 아카이브 로그가 포함된 위치를 지정해야 합니다.

• 단계 *

1. Cloud Manager UI에서 * 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 필터 기준 * 필드에서 필터 * 유형 * 을 선택하고 드롭다운에서 * Oracle * 을 선택합니다.
3. 복원하려는 데이터베이스에 해당하는 * View Details * 를 클릭하고 * Restore * 를 클릭합니다.
4. 복원 유형 페이지에서 다음 작업을 수행합니다.
 - a. 전체 데이터베이스와 함께 제어 파일을 복원하려면 * 제어 파일 * 을 선택합니다.
 - b. 복원 및 복구에 필요한 경우 * 데이터베이스 상태 변경 * 을 선택하여 복원 및 복구 작업을 수행하는 데 필요한 상태로 데이터베이스의 상태를 변경합니다.

상위 데이터베이스에서 하위 데이터베이스까지의 다양한 상태는 열기, 마운트, 시작 및 종료입니다. 데이터베이스가 더 높은 상태에 있지만 복원 작업을 수행하려면 상태를 더 낮은 상태로 변경해야 하는 경우 이 확인란을 선택해야 합니다. 데이터베이스가 더 낮은 상태에 있지만 복원 작업을 수행하려면 상태를 더 높은 상태로 변경해야 하는 경우 확인란을 선택하지 않아도 데이터베이스 상태가 자동으로 변경됩니다.

데이터베이스가 열려 있는 상태이고 복구를 위해 데이터베이스가 마운트된 상태여야 하는 경우 이 확인란을 선택한 경우에만 데이터베이스 상태가 변경됩니다.

1. 복구 범위 페이지에서 다음 작업을 수행합니다.
 - a. 복구 범위를 지정합니다.

만약...	수행할 작업...
마지막 트랜잭션으로 복구하려고 합니다	모든 로그 * 를 선택합니다.

만약...	수행할 작업...
특정 SCN(시스템 변경 번호)으로 복구하려는 경우	SCN(시스템 변경 번호) * 까지 * 를 선택합니다.
특정 데이터 및 시간으로 복구하려는 경우	날짜 및 시간 * 을 선택합니다. 데이터베이스 호스트의 표준 시간대의 날짜 및 시간을 지정해야 합니다.
복구하기를 원하지 않습니다	No recovery * 를 선택합니다.
외부 아카이브 로그 위치를 지정하려는 경우	아카이브 로그가 AFS에 없는 경우 복구에 필요한 아카이브 로그가 포함된 위치를 지정해야 합니다.

b. 복구 후 데이터베이스를 열려면 이 확인란을 선택합니다.

RAC 설정에서는 복구에 사용되는 RAC 인스턴스만 복구 후 열립니다.

2. 세부 정보를 검토하고 * Restore * 를 클릭합니다.


SQL Server 데이터베이스를 복원합니다

SQL Server 데이터베이스를 동일한 호스트 또는 대체 호스트로 복원할 수 있습니다. 로그 백업 복구 및 가용성 그룹의 재시딩은 지원되지 않습니다.

• 단계 *

1. Cloud Manager UI에서 * 백업 및 복원 * > * 응용 프로그램 * 을 클릭합니다.
2. 필터 기준 * 필드에서 필터 * 유형 * 을 선택하고 드롭다운에서 * SQL * 을 선택합니다.
3. 사용 가능한 모든 백업을 보려면 * 세부 정보 보기 * 를 클릭합니다.
4. 백업을 선택하고 * 복원 * 을 클릭합니다.
5. 데이터베이스 파일을 복원할 위치를 선택합니다.

옵션을 선택합니다	설명
백업을 생성한 동일한 호스트에 데이터베이스를 복구합니다	백업을 수행한 동일한 SQL Server에 데이터베이스를 복원하려면 이 옵션을 선택합니다.

옵션을 선택합니다	설명
데이터베이스를 대체 호스트로 복구합니다	<p>백업을 수행하는 동일한 호스트 또는 다른 호스트에 있는 다른 SQL Server로 데이터베이스를 복구하려는 경우 이 옵션을 선택합니다.</p> <p>호스트 이름을 선택하고 데이터베이스 이름(선택 사항)을 입력한 다음 인스턴스를 선택하고 복구 경로를 지정합니다.</p> <div style="display: flex; align-items: center;">  <div> <p>대체 경로에 제공된 파일 확장자는 원본 데이터베이스 파일의 파일 확장명과 동일해야 합니다.</p> </div> </div> <p>Restore Scope 페이지에 * Restore the database to an alternate host * 옵션이 표시되지 않으면 브라우저를 지웁니다.</p>

6. 사전 복원 옵션 * 페이지에서 다음 옵션 중 하나를 선택합니다.

- 같은 이름으로 데이터베이스를 복원하려면 * 복원 중에 같은 이름으로 데이터베이스 덮어쓰기 * 를 선택합니다.
- 데이터베이스를 복원하고 기존 복제 설정을 유지하려면 * SQL 데이터베이스 복제 설정 유지 * 를 선택합니다.

7. 사후 복원 옵션 * 페이지에서 추가 트랜잭션 로그를 복원하기 위한 데이터베이스 상태를 지정하려면 다음 옵션 중 하나를 선택합니다.

- 지금 필요한 모든 백업을 복원하는 경우 * 작동 가능하나 * 를 선택합니다.

이는 기본 동작으로, 커밋되지 않은 트랜잭션을 롤백하여 데이터베이스를 사용할 수 있도록 합니다. 백업을 생성할 때까지 추가 트랜잭션 로그를 복원할 수 없습니다.

- 커밋되지 않은 트랜잭션을 롤백하지 않고 데이터베이스를 비작동 상태로 두려면 * 비작동, 사용 가능 * 을 선택합니다.

추가 트랜잭션 로그를 복원할 수 있습니다. 데이터베이스가 복구될 때까지 데이터베이스를 사용할 수 없습니다.

- 데이터베이스를 읽기 전용 모드로 전환하려면 * 읽기 전용 모드 및 사용 가능 * 을 선택합니다.

이 옵션은 커밋되지 않은 트랜잭션을 수행하지 않지만 복구 효과를 되돌릴 수 있도록 실행 취소된 작업을 대기 파일에 저장합니다.

Undo directory(디렉터리 실행 취소) 옵션이 활성화된 경우 더 많은 트랜잭션 로그가 복원됩니다. 트랜잭션 로그의 복원 작업이 실패한 경우 변경 내용을 롤백할 수 있습니다. 자세한 내용은 SQL Server 설명서를 참조하십시오.

1. 세부 정보를 검토하고 * Restore * 를 클릭합니다.

가상 머신 데이터 백업 및 복원

가상 시스템 데이터 보호

SnapCenter Plug-in for VMware vSphere를 Cloud Manager와 통합하면 가상 머신의 데이터를 보호할 수 있습니다. 데이터 저장소를 클라우드에 백업하고 VMware vSphere용 사내 SnapCenter 플러그인으로 가상 머신을 간편하게 복원할 수 있습니다.

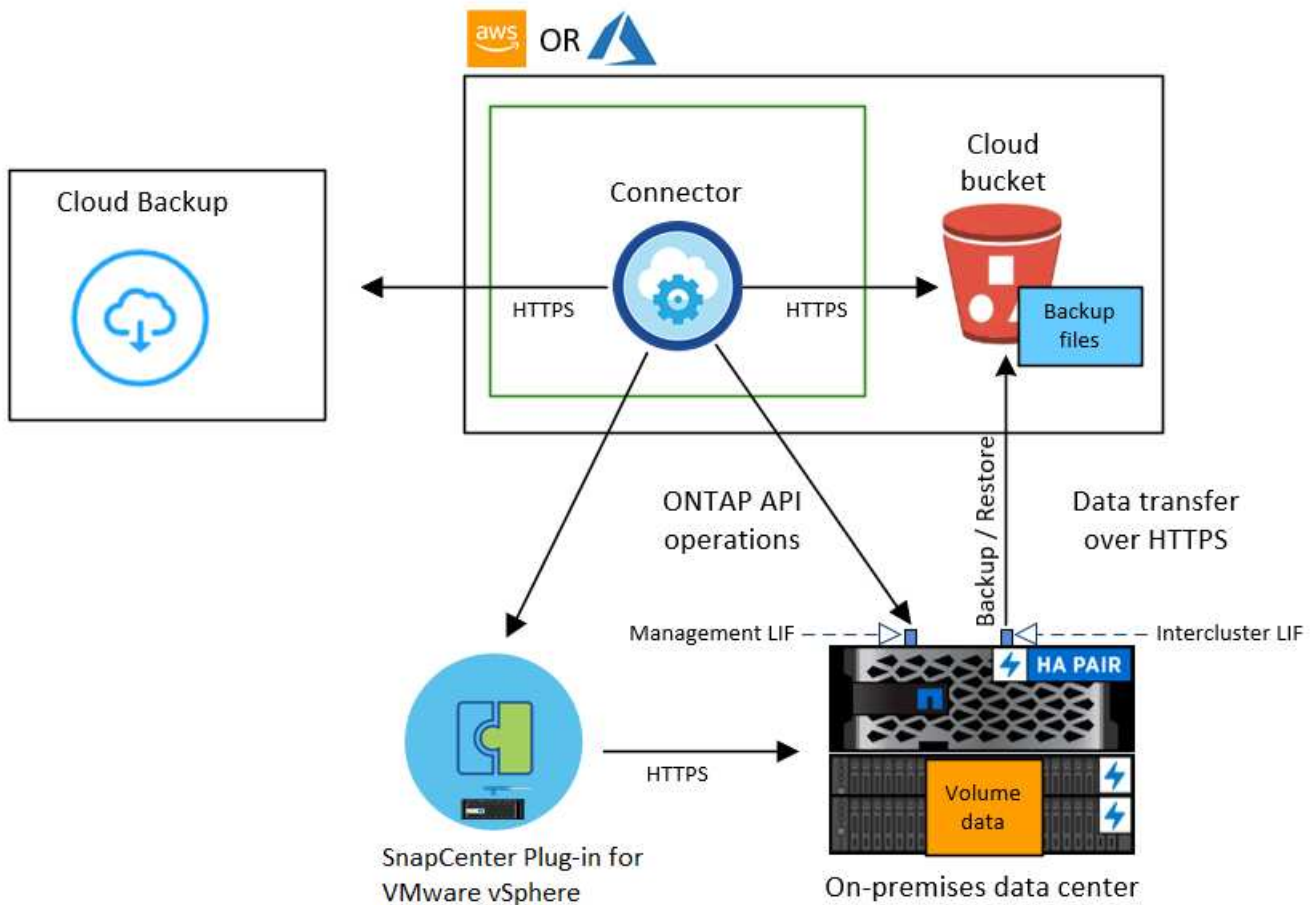
데이터 저장소를 Amazon Web Services S3 또는 Microsoft Azure Blob에 백업할 수 있습니다.

요구 사항

클라우드 서비스에 데이터 저장소 및 가상 머신 백업을 시작하기 전에 다음 요구 사항을 읽고 지원되는 구성이 있는지 확인하십시오.

- VMware vSphere 4.6P1 이상용 SnapCenter 플러그인
- ONTAP 9.8 이상
- Cloud Manager 3.9 이상
- VMware vSphere 4.6P1용 SnapCenter 플러그인에서 하나 이상의 백업을 수행해야 합니다.
- SnapCenter Plug-in for VMware vSphere에서 Cloud Manager의 Cloud Backup for Virtual Machines 정책에 대한 레이블 또는 레이블이 없는 상태로 최소 1일, 매주 또는 매월 정책을 구현합니다.
- 사전 구성된 정책의 경우 VMware vSphere 및 클라우드용 SnapCenter 플러그인의 데이터 저장소에 대한 스케줄 계층이 동일해야 합니다.
- FlexGroup 볼륨 백업 및 복구는 지원되지 않으므로 데이터 저장소에 FlexGroup 볼륨이 없는지 확인합니다.
- 암호화된 볼륨 복원이 지원되지 않으므로 암호화된 볼륨이 없는지 확인합니다.
- 필요한 리소스 그룹에서 " *_Recent *"를 비활성화합니다. 리소스 그룹에 대해 " *_Recent *"를 설정한 경우 해당 리소스 그룹의 백업을 클라우드의 데이터 보호에 사용할 수 없으며 이후에 복구 작업에 사용할 수 없습니다.
- 가상 머신이 복구될 대상 데이터 저장소에 VMDK, VMX, VMSD 등과 같은 모든 가상 머신 파일의 복제본을 수용할 수 있는 공간이 충분한지 확인합니다.
- 대상 데이터 저장소에 이전 복원 작업 실패의 restore_xxx_xxxxxx_filename 형식으로 오래된 가상 머신 파일이 없는지 확인합니다. 복구 작업을 트리거하기 전에 오래된 파일을 삭제해야 합니다.

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



보호 정책

Cloud Backup for Virtual Machines에 정의된 정책 중 하나를 사용하여 데이터 저장소를 클라우드에 백업해야 합니다.



사용자 지정 정책은 지원되지 않습니다.

Cloud Manager에서 * Backup & Restore * > * Virtual Machines * > * Policies * 를 클릭하여 기본 정책을 볼 수 있습니다.

정책 이름	라벨	보존 값
1년 일일 LTR	매일	366
5년 일일 LTR	매일	1830
7년 주간 LTR	매주	370
10년 월간 LTR	매월	120

데이터 저장소를 클라우드에 백업합니다

SnapCenter Plug-in for VMware vSphere를 Cloud Manager와 통합하여 데이터 저장소를 클라우드에 백업할 수 있습니다. VM 관리자는 이를 통해 스토리지 효율성을 위해 데이터를 쉽고 빠르게 백업 및 아카이브하고 클라우드 전환을 가속화할 수 있습니다.



를 모두 충족했는지 확인합니다 "요구 사항" 클라우드에 데이터 저장소를 백업하기 전에.

VMware vSphere용 SnapCenter 플러그인을 등록합니다

Cloud Manager에서 VMware vSphere용 SnapCenter 플러그인을 등록하여 데이터 저장소와 가상 머신을 Cloud Manager에 표시해야 합니다. 관리 액세스 권한이 있는 사용자만 VMware vSphere용 SnapCenter 플러그인을 등록할 수 있습니다.



VMware vSphere용 SnapCenter 플러그인을 여러 개 등록할 수 있습니다. 그러나 일단 등록하면 VMware vSphere용 SnapCenter 플러그인을 제거할 수 없습니다.

단계

1. Cloud Manager UI에서 * 백업 및 복원 * > * 가상 머신 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * SnapCenter Plug-in for VMware vSphere * 를 클릭합니다.
3. VMware vSphere * 용 SnapCenter 플러그인 등록 을 클릭합니다.
4. 다음 세부 정보를 지정합니다.
 - a. VMware vSphere용 SnapCenter 플러그인 필드에서 VMware vSphere용 SnapCenter 플러그인의 FQDN 또는 IP 주소를 지정합니다.
 - b. 포트 필드에서 VMware vSphere용 SnapCenter 플러그인이 실행되고 있는 포트 번호를 지정합니다.

VMware vSphere용 SnapCenter 플러그인과 애플리케이션용 클라우드 백업 간에 통신이 가능하도록 포트가 열려 있는지 확인해야 합니다.
 - c. 사용자 이름 및 암호 필드에서 관리자 역할을 가진 사용자의 자격 증명을 지정합니다.
5. Register * 를 클릭합니다.
 - 완료 후 *

등록된 VMware vSphere용 SnapCenter 플러그인을 사용하여 보호할 수 있는 모든 데이터 저장소와 가상 머신을 보려면 * 백업 및 복원 > 가상 머신 * 을 클릭합니다.

데이터 저장소를 백업합니다

단일 정책을 사용하여 하나 이상의 데이터 저장소를 클라우드에 동시에 백업할 수 있습니다. 기본 정책만 데이터 저장소에 할당할 수 있습니다.

단계

1. Cloud Manager UI에서 * 백업 및 복원 * > * 가상 머신 * 을 클릭합니다.
2. 을 클릭합니다 ... 백업하려는 데이터 저장소에 대해 * Activate Backup * 를 클릭합니다.

3. 작업 환경을 추가합니다.

Cloud Manager에서 검색할 ONTAP 클러스터를 구성하여 데이터 저장소를 백업합니다. 데이터 저장소 중 하나에 작업 환경을 추가한 후 동일한 ONTAP 클러스터에 상주하는 다른 모든 데이터 저장소에 다시 사용할 수 있습니다.

- a. SVM에 해당하는 * 작업 환경 추가 * 를 클릭합니다.
- b. 작업 환경 추가 마법사에서 다음을 수행합니다.
 - i. ONTAP 클러스터의 IP 주소를 지정합니다.
 - ii. ONTAP 클러스터 사용자의 자격 증명을 지정합니다.
- c. 작업 환경 추가 * 를 클릭합니다.

4. 클라우드 공급자를 선택하고 구성합니다.

Amazon Web Services를 구성합니다

- a. AWS 계정을 지정합니다.
- b. AWS 액세스 키 필드에서 데이터 암호화에 대한 키를 지정합니다.
- c. AWS 암호 키 필드에서 데이터 암호화에 대한 암호를 지정합니다.
- d. 백업을 생성할 영역을 선택합니다.
- e. 작업 환경으로 추가된 ONTAP 클러스터의 IP 주소를 지정합니다.

Microsoft Azure를 구성합니다

- a. Azure 구독 ID를 지정합니다.
- b. 백업을 생성할 영역을 선택합니다.
- c. 새 자원 그룹을 만들거나 기존 자원 그룹을 사용합니다.
- d. 작업 환경으로 추가된 ONTAP 클러스터의 IP 주소를 지정합니다.

5. 정책 할당 페이지에서 정책을 선택하고 * 다음 * 을 클릭합니다.

6. 세부 정보를 검토하고 * 백업 활성화 * 를 클릭합니다.

가상 시스템 보호 관리

데이터를 백업 및 복원하기 전에 정책, 데이터 저장소 및 가상 시스템을 볼 수 있습니다. 데이터베이스, 정책 또는 리소스 그룹의 변경에 따라 Cloud Manager UI에서 업데이트를 새로 고칠 수 있습니다.

정책을 봅니다

사전 구성된 기본 정책을 모두 볼 수 있습니다. 각 정책에 대해 세부 정보를 볼 때 연결된 모든 Cloud Backup for Virtual Machines 정책과 연결된 모든 가상 머신이 나열됩니다.

1. 백업 및 복원 > 가상 시스템 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * 정책 * 을 클릭합니다.

3. 세부 정보를 보려는 정책에 해당하는 * 세부 정보 보기 * 를 클릭합니다.

관련 Cloud Backup for Virtual Machines 정책과 모든 가상 머신이 나열됩니다.

데이터 저장소 및 가상 머신을 봅니다

등록된 VMware vSphere용 SnapCenter 플러그인을 사용하여 보호되는 데이터 저장소 및 가상 머신이 표시됩니다.

- 이 작업에 대한 정보 *
- NFS 데이터 저장소만 표시됩니다.
- SnapCenter Plug-in for VMware vSphere에서 하나 이상의 백업이 성공한 데이터 저장소만 표시됩니다.

단계

1. Cloud Manager UI에서 * 백업 및 복원 * > * 가상 머신 * > * 설정 * > * SnapCenter Plug-in for VMware vSphere * 를 클릭합니다.
2. 데이터 저장소 및 가상 머신을 보려는 VMware vSphere용 SnapCenter 플러그인을 클릭합니다.

VMware vSphere용 SnapCenter 플러그인을 편집합니다

Cloud Manager에서 VMware vSphere용 SnapCenter 플러그인의 세부 정보를 편집할 수 있습니다

단계

1. Cloud Manager UI에서 * 백업 및 복원 * > * 가상 머신 * > * 설정 * > * SnapCenter Plug-in for VMware vSphere * 를 클릭합니다.
2. 을 클릭하고 * 편집 * 을 선택합니다
3. 필요에 따라 세부 정보를 수정합니다
4. 저장 * 을 클릭합니다.

보호 상태를 새로 고칩니다

새 볼륨이 데이터베이스에 추가되거나 정책 또는 리소스 그룹이 변경된 경우 보호 기능을 새로 고쳐야 합니다.

1. 백업 및 복원 > 가상 시스템 * 을 클릭합니다.
2. 설정 * 드롭다운에서 * SnapCenter Plug-in for VMware vSphere * 를 클릭합니다.
3. 을 클릭합니다 ... 가상 머신을 호스팅하는 VMware vSphere용 SnapCenter 플러그인에 해당하는 * Refresh * 를 클릭합니다.

새로운 변경 사항이 검색됩니다.

4. 을 클릭합니다 ... 데이터 저장소에 해당하는 * Refresh Protection * 을 클릭하여 변경 사항에 대한 클라우드 보호를 활성화합니다.

작업을 모니터링합니다

모든 클라우드 백업 작업에 대한 작업이 생성됩니다. 각 작업의 일부로 수행되는 모든 작업과 모든 하위 작업을 모니터링할 수 있습니다.

1. 백업 및 복원 > 작업 모니터링 * 을 클릭합니다.

작업을 시작하면 작업이 시작되었다는 창이 나타납니다. 링크를 클릭하여 작업을 모니터링할 수 있습니다.

2. 각 하위 작업의 하위 작업 및 상태를 보려면 기본 작업을 클릭합니다.

클라우드에서 가상 머신을 복구합니다

클라우드에서 가상 머신을 사내 vCenter로 복구할 수 있습니다. 백업이 수행된 위치와 정확히 동일한 위치로 복구됩니다. 다른 대체 위치에 백업을 복원할 수 없습니다. 데이터 저장소 또는 VM 보기에서 가상 머신을 복구할 수 있습니다.



데이터 저장소 간에 확장되는 가상 시스템은 복구할 수 없습니다.

를 모두 충족했는지 확인합니다 "요구 사항" 가상 머신을 클라우드에서 복구하기 전에

단계

1. Cloud Manager에서 * 백업 및 복원 * > * 가상 머신 * > * SnapCenter Plug-in for VMware vSphere * 를 클릭하고 가상 머신을 복구할 VMware vSphere * 용 SnapCenter 플러그인을 선택합니다.



소스 가상 머신이 다른 위치(vMotion)로 이동되고 사용자가 Cloud Manager에서 해당 가상 머신의 복구를 트리거하면 가상 머신이 백업이 수행된 원래 소스 위치로 복구됩니다.

1. 데이터 저장소에서 복구하려면 다음을 따르십시오.

- 을 클릭합니다 ... 복원하려는 데이터 저장소에 해당하는 * View Details * 를 클릭합니다.
- 복원하려는 백업에 해당하는 * 복원 * 을 클릭합니다.
- 백업에서 복원할 가상 머신을 선택하고 * Next * 를 클릭합니다.
- 세부 정보를 검토하고 * Restore * 를 클릭합니다.

2. 가상 시스템에서 복구하려면 다음을 따르십시오.

- 을 클릭합니다 ... 복원하려는 가상 머신에 해당하는 을 클릭하고 * Restore * 를 클릭합니다.
- 가상 컴퓨터를 복원할 백업을 선택하고 * 다음 * 을 클릭합니다.
- 세부 정보를 검토하고 * Restore * 를 클릭합니다.

백업이 수행된 위치와 동일한 위치로 VM이 복구됩니다.

클라우드 백업 API

웹 UI를 통해 사용할 수 있는 Cloud Backup 기능은 RESTful API를 통해서도 사용할 수 있습니다.

Cloud Backup Service에는 8개의 끝점 범주가 정의되어 있습니다.

- 백업
- 카탈로그
- 클라우드
- 있습니다
- 라이선스
- 복원
- 단일 파일 레벨 복원(SFR)
- 작업 환경

시작하기

Cloud Backup API를 시작하려면 사용자 토큰, Cloud Central 계정 ID 및 Cloud Connector ID를 얻어야 합니다.

API 호출을 할 때 권한 부여 헤더에 사용자 토큰을 추가하고 x-agent-id 헤더에 클라우드 커넥터 ID를 추가합니다. API에서 Cloud Central 계정 ID를 사용해야 합니다.

단계

1. NetApp Cloud Central에서 사용자 토큰을 얻습니다.

다음 링크에서 새로 고침 토큰을 생성해야 합니다. <https://services.cloud.netapp.com/refresh-token/>. 새로 고침 토큰은 사용자 토큰을 생성하는 데 사용할 영숫자 문자열입니다.

```
curl --location --request POST 'https://netapp-cloud-account.auth0.com/oauth/token?=' \
--header 'Content-Type: application/json' \
-d '{
  "grant_type": "refresh token",
  "refresh_token": "JxaVHn9cGkX92aPVCkhat3zxxxxxwsC9qMl_pLHkZtsVA",
  "client_id": "Mu0V1ywgYteI6w1MbD15fKfVIUrNXGWC"
}'
```

2. NetApp Cloud Central 계정 ID를 받습니다.

```
GET 'https://cloudmanager.cloud.netapp.com/tenancy/account' -H
'authority: cloudmanager.cloud.netapp.com'
Header:
-H 'accept: application/json'
-H 'accept-language: en-GB,en;q=0.9'
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR.....
```

이 API는 다음과 같은 응답을 반환합니다. [0].[accountPublicId] * 에서 출력을 구문 분석하여 계정 ID를 검색할 수 있습니다.

```
[{"accountPublicId":"account-
i6vJXvZW","accountName":"rashidn","isSaas":true,"isGov":false,"isPrivate
PreviewEnabled":false,"is3rdPartyServicesEnabled":false,"accountSerial":
"96064469711530003565","userRole":"Role-1"}].....
```

3. Cloud Manager 커넥터 ID가 포함된 x-agent-id를 얻습니다.

```
GET curl 'https://api.services.cloud.netapp.com/occm/list-occms/account-
OOnAR4ZS?excludeStandalone=true&source=saas' \
Header:
-H 'authority: api.services.cloud.netapp.com' \
-H 'accept: application/json' \
-H 'accept-language: en-GB,en;q=0.9' \
-H 'authorization: Bearer eyJhbGciOiJSUzI1NiIsInR5.....
```

이 API는 다음과 같은 응답을 반환합니다. occm.[0].[agent].[AGENTID] * 의 출력을 구문 분석하여 에이전트 ID를 검색할 수 있습니다.


```
{
  "occms": [
    {
      "account": "account-OOnAR4ZS",
      "accountName": "cbs",
      "occm": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Z",
      "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Z",
      "status": "ready",
      "occmName": "cbsgcpdevcntsg-asia",
      "primaryCallbackUri": "http://34.93.197.21",
      "manualOverrideUris": [],
      "automaticCallbackUris": [
        "http://34.93.197.21",
        "http://34.93.197.21/occmui",
        "https://34.93.197.21",
        "https://34.93.197.21/occmui",
        "http://10.138.0.16",
        "http://10.138.0.16/occmui",
        "https://10.138.0.16",
        "https://10.138.0.16/occmui",
        "http://localhost",
        "http://localhost/occmui",
        "http://localhost:1337",
        "http://localhost:1337/occmui",
        "https://localhost",
        "https://localhost/occmui",
        "https://localhost:1337",
        "https://localhost:1337/occmui"
      ],
      "createDate": "1652120369286",
      "agent": {
        "useDockerInfra": true,
        "network": "default",
        "name": "cbsgcpdevcntsg-asia",
        "agentId": "imEdsEW4HyYTFbt8ZcNKTKDF05jMie6Zclients",
        "provider": "gcp",
        "systemId": "a3aa3578-bfee-4d16-9e10-"
      }
    }
  ]
}
```

API 사용 예

다음 예에서는 Azure 클라우드의 East-US-2 영역에서 일별, 시간별, 주별 레이블이 설정되고 보관 기간이 180일로 설정된 새 정책을 사용하여 작업 환경에서 백업을 활성화하는 API 호출을 보여 줍니다. 이 옵션은 작업 환경에서만 백업을 활성화하지만 볼륨은 백업되지 않습니다. ""자동 백업 사용": true를 선택하면 시스템에 이미 있는 모든 볼륨이 백업되고 이후 볼륨이 추가됩니다.

Cloud Central 계정 ID "account-DpTFcxN3", Cloud Manager Connector ID "iZwFFeVCZjWnzGlw8RgD0QNaNZvpP7IClients" 및 사용자 토큰 "BEARER UJHbGciOiJSUzSUI1NiSXinSXinS4UCJUCJUCJUXYUXUXUXUXUXYUXYUXYUXYUXYUX4CJUXYUX4CJUXYUC4UXUXYUXYUXYUXYUXYUXYUXYUXYUXYUXYUX4CJUXY"

```

curl --location --request POST
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v3/backup/working-
environment/VsaWorkingEnvironment-99hPYEgk' \
--header 'x-agent-id: iZwFFeVCZjWnzGlw8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Iks5rSx1PVFUzUWpZek1E...y6nyhBjwk
eMwHc4ValobjUmju2x0xUH48g' \
--data-raw '{
  "provider": "AZURE",
  "backup-policy": {
    "archive-after-days": 180,
    "rule": [
      {
        "label": "hourly",
        "retention": "2"
      },
      {
        "label": "daily",
        "retention": "30"
      },
      {
        "label": "weekly",
        "retention": "52"
      }
    ]
  },
  "ip-space": "Default",
  "region": "eastus2",
  "azure": {
    "resource-group": "rn-test-backup-rg",
    "subscription": "3beb4dd0-25d4-464f-9bb0-303d7cf5c0c2"
  }
}'

```

응답은 모니터링할 수 있는 작업 ID입니다.

```

{
  "job-id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a"
}

```

응답을 모니터링합니다.

```
curl --location --request GET
'https://cloudmanager.cloud.netapp.com/account/account-
DpTFcxN3/providers/cloudmanager_cbs/api/v1/job/1b34b6f6-8f43-40fb-9a52-
485b0dfe893a' \
--header 'x-agent-id: iZwFFeVCZjWnzG1w8RgD0QQNANZvpP7Iclients' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6Ikp5rSXlPVFUzUWpZek1E...hE9ss2Nub
K6wZRHUdSaORI7JvcOorUhJ8srqdiUiW6MvuGIFAQIh668of2M3dLbhVDBe8BBMtsa939UGnJx
7Qz6Eg'
```

응답.

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "PENDING",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

"상태"가 "완료됨"이 될 때까지 모니터링합니다.

```
{
  "job": [
    {
      "id": "1b34b6f6-8f43-40fb-9a52-485b0dfe893a",
      "type": "backup-working-environment",
      "status": "COMPLETED",
      "error": "",
      "time": 1651852160000
    }
  ]
}
```

토큰이 만료되면 어떻게 해야 하나요?

NetApp Cloud Central의 사용자 토큰에 만료일이 있습니다. 토큰을 새로 고치려면 1단계에서 API를 다시 호출해야 합니다.

API 응답에는 토큰이 만료되는 시점을 나타내는 "expires_in" 필드가 포함됩니다.

API 참조입니다

각 Cloud Backup API에 대한 문서는 에서 확인할 수 있습니다 <https://docs.netapp.com/us-en/cloud-manager-automation/cbs/overview.html>.

참조하십시오

AWS S3 아카이브 스토리지 클래스 및 복원 검색 시간

Cloud Backup은 2개의 S3 아카이브 스토리지 클래스와 대부분의 영역을 지원합니다.

Cloud Backup에 지원되는 S3 아카이브 스토리지 클래스

백업 파일이 처음 생성되면 S3_Standard_Storage에 저장됩니다. 이 계층은 자주 액세스하지 않는 데이터를 저장하는 데 최적화되어 있지만 이를 즉시 액세스할 수도 있습니다. 30일 후에 백업이 S3_Standard - Infrequent Access_storage 클래스로 전환되어 비용이 절감됩니다.

소스 클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 추가 비용 최적화를 위해 일정 일(일반적으로 30일 이상) 후에 백업을 S3 Glacier 또는 S3 Glacier Deep Archive_storage로 계층화하도록 선택할 수 있습니다. 이러한 계층의 데이터는 필요할 때 즉시 액세스할 수 없으며 검색 비용을 더 높여야 하기 때문에 이러한 아카이브 백업 파일에서 데이터를 복원해야 하는 빈도를 고려해야 합니다. 에 대한 섹션을 참조하십시오 [아카이브 스토리지에서 데이터 복원](#).

이러한 유형의 수명주기 규칙을 사용하여 Cloud Backup을 구성할 때는 AWS 계정에서 버킷을 설정할 때 수명주기 규칙을 구성하지 않아야 합니다.

["S3 스토리지 클래스에 대해 알아보십시오"](#).

아카이브 스토리지에서 데이터 복원

오래된 백업 파일을 아카이브 스토리지에 저장하는 것은 Standard 또는 Standard-IA 스토리지에 비해 훨씬 저렴하지만, 복원 작업을 위해 아카이브 스토리지에 있는 백업 파일의 데이터에 액세스하는 데 시간이 더 오래 걸리고 비용이 더 많이 듭니다.

Amazon S3 Glacier 및 Amazon S3 Glacier Deep Archive에서 데이터를 복원하는 데 비용이 얼마나 드나요?

Amazon S3 Glacier에서 데이터를 검색할 때 3가지 복원 우선순위를 선택할 수 있으며, Amazon S3 Glacier Deep Archive에서 데이터를 검색할 경우 2가지 복원 우선순위를 선택할 수 있습니다. S3 Glacier Deep Archive 비용 미만 S3 Glacier:

아카이브 계층	복구 우선 순위 및 비용		
	* 높음 *	* 표준 *	* 낮음 *
* S3 빙하 *	신속한 검색, 높은 비용	검색 속도 감소, 비용 절감	가장 느린 검색, 가장 낮은 비용
* S3 Glacier Deep Archive *		빠른 검색, 높은 비용	검색 속도 감소, 비용 최소화

각 방법은 GB당 검색 비용과 요청당 수수료를 다르게 합니다. AWS 지역별 S3 Glacier 가격 에 대한 자세한 내용은 [참조하십시오 "Amazon S3 가격 페이지"](#).

Amazon S3 Glacier에 보관된 개체를 복원하는 데 시간이 얼마나 걸립니까?

총 복원 시간을 구성하는 두 가지 부분이 있습니다.

- * 검색 시간 *: 아카이브에서 백업 파일을 검색하여 표준 저장소에 저장하는 시간입니다. 이를 "재수화" 시간이라고도 합니다. 검색 시간은 선택한 복원 우선 순위에 따라 다릅니다.

아카이브 계층	복구 우선 순위 및 검색 시간		
	* 높음 *	* 표준 *	* 낮음 *
* S3 빙하 *	3-5분	3-5시간	5-12시간
* S3 Glacier Deep Archive *		12시간	48시간

- * 복원 시간 *: 표준 저장소의 백업 파일에서 데이터를 복원하는 시간입니다. 이 시간은 아카이브 계층을 사용하지 않을 때 표준 스토리지에서 직접 수행하는 일반적인 복원 작업과 다르지 않습니다.

Amazon S3 Glacier 및 S3 Glacier Deep Archive 검색 옵션에 대한 자세한 내용은 을 참조하십시오 ["이러한 스토리지 클래스에 대한 Amazon FAQ가 있습니다"](#).

Azure 아카이브 계층 및 복원 검색 시간

Cloud Backup은 하나의 Azure 아카이브 액세스 계층 및 대부분의 영역을 지원합니다.

Cloud Backup에 지원되는 Azure Blob 액세스 계층

백업 파일이 처음 생성될 때는 _Cool_access 계층에 저장됩니다. 이 계층은 자주 액세스하지 않는 데이터를 저장하는 데 최적화되어 있지만 필요할 때 즉시 액세스할 수 있습니다.

소스 클러스터에서 ONTAP 9.10.1 이상이 실행 중인 경우 추가 비용 최적화를 위해 일정 일(일반적으로 30일 이상) 후에 _Cool_to_Azure Archive_storage에서 백업을 계층화하도록 선택할 수 있습니다. 이 계층의 데이터는 필요할 때 즉시 액세스할 수 없으며 검색 비용을 더 높여야 하기 때문에 이러한 아카이브 백업 파일에서 데이터를 복원해야 하는 빈도를 고려해야 합니다. 에 대한 다음 섹션을 참조하십시오 [아카이브 스토리지에서 데이터 복원](#).

이러한 유형의 수명 주기 규칙으로 Cloud Backup을 구성할 때는 Azure 계정에서 컨테이너를 설정할 때 수명 주기 규칙을 구성하지 않아야 합니다.

["Azure Blob 액세스 계층에 대해 알아보십시오"](#).

아카이브 스토리지에서 데이터 복원

오래된 백업 파일을 아카이브 스토리지에 저장하는 것은 Cool 스토리지보다 훨씬 저렴하지만, 복원 작업을 위해 Azure Archive의 백업 파일에서 데이터에 액세스하는 데 더 많은 시간이 걸리고 비용이 더 많이 듭니다.

Azure Archive에서 데이터를 복원하는 데 비용이 얼마나 드는가?

Azure Archive에서 데이터를 검색할 때 선택할 수 있는 두 가지 복원 우선 순위가 있습니다.

- * 높음 *: 가장 빠른 검색, 높은 비용
- * 표준 *: 검색 속도 감소, 비용 절감

각 방법은 GB당 검색 비용과 요청당 수수료를 다르게 합니다. Azure 지역별 Azure Archive에 대한 자세한 가격을 보려면 를 방문하십시오 ["Azure 가격 책정 페이지입니다"](#).

Azure Archive에 보관된 데이터를 복원하는 데 시간이 얼마나 걸립니까?

복원 시간을 구성하는 두 가지 부분이 있습니다.

- * 검색 시간 *: Azure Archive에서 보관된 백업 파일을 검색하여 Cool storage에 저장하는 시간입니다. 이를

"재수화" 시간이라고도 합니다. 검색 시간은 선택한 복원 우선 순위에 따라 다릅니다.

- * 높음 *: 1시간 미만
- * 표준 *: 15시간 미만
- * 복원 시간 *: Cool storage의 백업 파일에서 데이터를 복원하는 시간입니다. 이 시간은 보관 계층을 사용하지 않을 때 Cool 스토리지에서 직접 수행하는 일반적인 복원 작업과 다르지 않습니다.

Azure Archive 검색 옵션에 대한 자세한 내용은 [이 Azure FAQ를 참조하십시오](#).

지식 및 지원

지원을 위해 등록하십시오

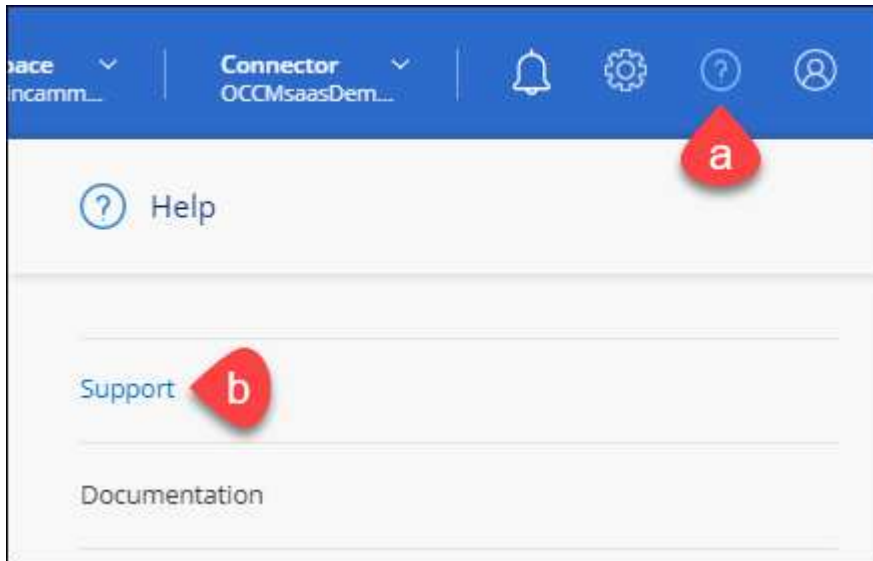
NetApp 기술 지원으로 지원 케이스를 생성하기 전에 NetApp Support 사이트 계정을 Cloud Manager에 추가한 다음 지원을 위해 등록해야 합니다.

NSS 계정을 추가합니다

지원 대시보드를 이용하면 모든 NetApp Support 사이트 계정을 단일 위치에서 추가 및 관리할 수 있습니다.

단계

1. 아직 NetApp Support 사이트 계정이 없는 경우 **"1인 등록"**.
2. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 * 지원 * 을 선택합니다.



3. NSS 관리 > NSS 계정 추가 * 를 클릭합니다.
4. 메시지가 표시되면 * 계속 * 을 클릭하여 Microsoft 로그인 페이지로 리디렉션됩니다.

NetApp은 Microsoft Azure Active Directory를 지원 및 라이선싱과 관련된 인증 서비스의 ID 공급자로 사용합니다.

5. 로그인 페이지에서 인증 프로세스를 수행할 수 있도록 NetApp Support 사이트의 등록 이메일 주소와 암호를 제공합니다.

이 작업을 수행하면 Cloud Manager에서 NSS 계정을 사용할 수 있습니다.

참고 계정은 고객 수준 계정이어야 합니다(게스트 또는 임시 계정이 아님).

계정을 등록하여 지원을 받을 수 있습니다

지원 등록은 지원 대시보드의 Cloud Manager에서 가능합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 상단에서 도움말 아이콘을 클릭하고 * 지원 * 을 선택합니다.



2. Resources * 탭에서 * Register for Support * 를 클릭합니다.
3. 등록할 NSS 자격 증명을 선택한 다음 * 등록 * 을 클릭합니다.

도움을 받으십시오

NetApp은 다양한 방법으로 Cloud Manager 및 클라우드 서비스를 지원합니다. 기술 자료(KB) 기사 및 커뮤니티 포럼과 같은 광범위한 무료 셀프 지원 옵션이 24x7 제공됩니다. 지원 등록에는 웹 티켓팅을 통한 원격 기술 지원이 포함됩니다.

자체 지원

이 옵션은 하루 24시간, 주 7일 동안 무료로 사용할 수 있습니다.

- "기술 자료"

Cloud Manager 기술 자료를 검색하여 문제를 해결할 수 있는 유용한 문서를 찾습니다.

- "커뮤니티"

Cloud Manager 커뮤니티에 가입하여 진행 중인 토론을 팔로우하거나 새 토론을 만들어보십시오.

- 문서화

현재 보고 있는 Cloud Manager 문서입니다.

- <mailto:ng-cloudmanager-feedback@netapp.com> [피드백 이메일]

저희는 귀하의 의견을 소중하게 생각합니다. 클라우드 관리자 개선에 도움이 되는 피드백을 제출해 주십시오.

NetApp 지원

위의 자체 지원 옵션 외에도 NetApp 지원 엔지니어와 협력하여 지원을 활성화한 이후의 모든 문제를 해결할 수 있습니다.

단계

1. Cloud Manager에서 * 도움말 > 지원 * 을 클릭합니다.
2. 기술 지원 아래에서 사용 가능한 옵션 중 하나를 선택합니다.
 - a. NetApp 기술 지원을 위한 전화 번호를 찾으려면 * 문의하다
 - b. 문제 열기 * 를 클릭하고 옵션 중 하나를 선택한 다음 * 보내기 * 를 클릭합니다.

NetApp 담당자가 귀하의 케이스를 검토하고 곧 다시 귀하에 연락을 드릴 것입니다.

법적 고지

법적 고지 사항은 저작권 선언, 상표, 특허 등에 대한 액세스를 제공합니다.

저작권

<http://www.netapp.com/us/legal/copyright.aspx>

상표

NetApp, NetApp 로고, NetApp 상표 페이지에 나열된 마크는 NetApp Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

특허

NetApp 소유 특허 목록은 다음 사이트에서 확인할 수 있습니다.

<https://www.netapp.com/us/media/patents-page.pdf>

개인 정보 보호 정책

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

오픈 소스

통지 파일은 NetApp 소프트웨어에 사용된 타사의 저작권 및 라이선스에 대한 정보를 제공합니다.

- ["Cloud Manager 3.9에 대한 고지 사항"](#)
- ["Cloud Backup에 대한 알림"](#)
- ["단일 파일 복원에 대한 고지 사항"](#)

저작권 정보

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

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

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

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

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

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

상표 정보

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