ONTAP 볼륨 워크로드 보호

NetApp Backup and Recovery

NetApp
March 09, 2026

목차

ONTAP 볼륨 워크로드 보호

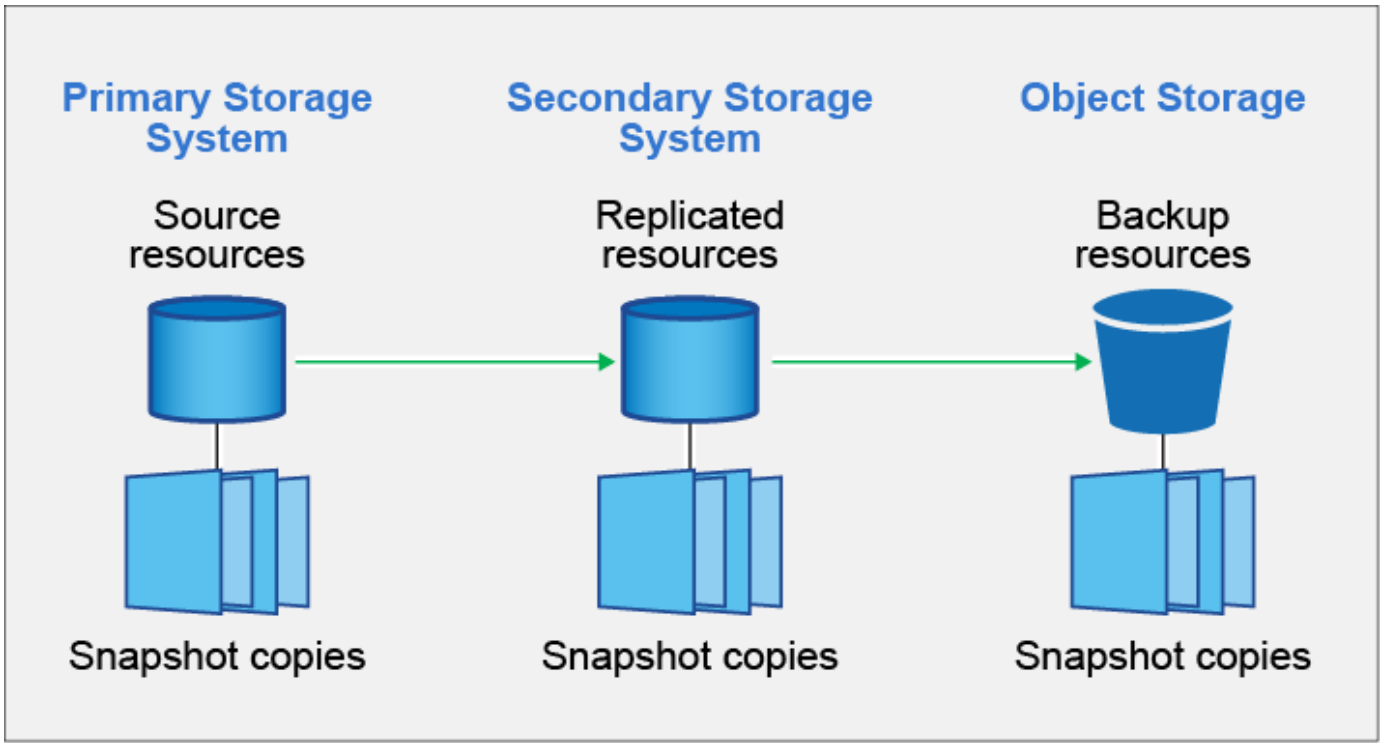
NetApp Backup and Recovery 사용하여 ONTAP 볼륨 데이터를 보호하세요

NetApp Backup and Recovery ONTAP 볼륨 데이터의 보호 및 장기 보관을 위한 백업 및 복원 기능을 제공합니다. 2개의 서로 다른 스토리지 시스템에 소스 데이터의 사본 3개를 두고, 클라우드에 사본 1개를 두는 3-2-1 전략을 구현할 수 있습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

활성화 후 백업 및 복구를 통해 블록 수준의 증분적 영구 백업이 생성되어 다른 ONTAP 클러스터와 클라우드의 개체 스토리지에 저장됩니다. 소스 볼륨 외에도 다음이 제공됩니다.

- 소스 시스템의 볼륨 스냅샷
- 다른 스토리지 시스템에 복제된 볼륨
- 객체 스토리지의 볼륨 백업



NetApp Backup and Recovery NetApp의 SnapMirror 데이터 복제 기술을 활용하여 스냅샷을 생성하고 이를 백업 위치로 전송하여 모든 백업이 완전히 동기화되도록 보장합니다.

3-2-1 접근 방식의 이점은 다음과 같습니다.

- 여러 개의 데이터 사본을 보관하여 내부 및 외부 사이버 보안 위협으로부터 보호합니다.
- 다양한 유형의 미디어를 사용하면 한 유형의 미디어가 실패하더라도 복구하는 데 도움이 됩니다.

- 온사이트 사본에서 빠르게 복원할 수 있으며, 온사이트 사본이 손상된 경우 오프사이트 사본을 사용할 수 있습니다.

필요한 경우 백업 사본에서 전체 볼륨, 폴더 또는 하나 이상의 _파일_을 동일하거나 다른 시스템으로 복원할 수 있습니다.

특징

복제 기능:

- 백업 및 재해 복구를 지원하기 위해 ONTAP 스토리지 시스템 간에 데이터를 복제합니다.
- 높은 가용성으로 DR 환경의 안정성을 확보하세요.
- 두 시스템 간의 사전 공유 키(PSK)를 통해 기본 ONTAP 전송 중 암호화가 설정됩니다.
- 복사된 데이터는 쓰기 가능하고 사용할 준비가 될 때까지 변경할 수 없습니다.
- 전송에 실패하면 복제가 자체적으로 복구됩니다.
- 와 비교했을 때 "NetApp Replication" NetApp Backup and Recovery 의 복제에는 다음과 같은 기능이 포함됩니다.
  - 한 번에 여러 개의 FlexVol 볼륨을 보조 시스템에 복제합니다.
  - UI를 사용하여 복제된 볼륨을 소스 시스템이나 다른 시스템으로 복원합니다.

보다"ONTAP 볼륨에 대한 복제 제한" NetApp Backup and Recovery for ONTAP 볼륨에서 사용할 수 없는 복제 기능 목록은 여기에서 확인하세요.

객체 백업 기능:

- 저렴한 개체 스토리지에 데이터 볼륨의 독립적인 사본을 백업하세요.
- 클러스터의 모든 볼륨에 단일 백업 정책을 적용하거나 고유한 복구 지점 목표가 있는 볼륨에 다른 백업 정책을 할당합니다.
- 클러스터에서 생성되는 모든 향후 볼륨에 적용할 백업 정책을 만듭니다.
- 변경 불가능한 백업 파일을 만들어 보관 기간 동안 잠그고 보호합니다.
- 랜섬웨어 공격 가능성이 있는지 백업 파일을 검사하고 감염된 백업을 자동으로 제거/교체합니다.
- 비용을 절감하기 위해 오래된 백업 파일을 보관 저장소에 계층화합니다.
- 볼륨 백업을 보존하는 동시에 필요 없는 소스 볼륨을 보관할 수 있도록 백업 관계를 삭제합니다.
- 클라우드에서 클라우드로, 온프레미스 시스템에서 퍼블릭 또는 프라이빗 클라우드로 백업합니다.
- 백업 데이터는 저장 중에는 AES-256비트 암호화를 통해 보호되고, 전송 중에는 TLS 1.2 HTTPS 연결을 통해 보호됩니다.
- 클라우드 공급업체의 기본 암호화 키를 사용하는 대신, 고객이 관리하는 자체 키를 사용하여 데이터를 암호화하세요.
- 단일 볼륨에 대해 최대 4,000개의 백업을 지원합니다.

복원 기능:

- 개체 스토리지의 로컬 스냅샷, 복제된 볼륨 또는 백업된 볼륨에서 특정 시점의 데이터를 복원합니다.
- 볼륨, 폴더 또는 개별 파일을 소스 시스템이나 다른 시스템으로 복원합니다.

- 다른 구독/계정을 사용하거나 다른 지역에 있는 시스템으로 데이터를 복원합니다.
- 클라우드 스토리지에서 Cloud Volumes ONTAP 시스템이나 온프레미스 시스템으로 볼륨을 _빠르게 복원_합니다. 가능한 한 빨리 볼륨에 대한 액세스를 제공해야 하는 재해 복구 상황에 적합합니다.
- 원래 ACL을 보존하면서 블록 수준에서 데이터를 복원하여 지정한 위치에 직접 데이터를 배치합니다.
- 개별 폴더와 파일을 쉽게 선택하여 단일 파일을 복원할 수 있도록 파일 카탈로그를 탐색하고 검색합니다.

백업 및 복원 작업을 위한 지원 시스템

NetApp Backup and Recovery ONTAP 시스템과 퍼블릭 및 프라이빗 클라우드 공급업체를 지원합니다.

지원되는 지역

NetApp Backup and Recovery 많은 Amazon Web Services, Microsoft Azure 및 Google Cloud 지역에서 Cloud Volumes ONTAP 통해 지원됩니다.

"글로벌 지역 지도를 사용하여 자세히 알아보세요"

지원되는 백업 대상

NetApp Backup and Recovery 사용하면 다음 소스 시스템의 ONTAP 볼륨을 다음 보조 시스템과 퍼블릭 및 프라이빗 클라우드 공급자의 개체 스토리지로 백업할 수 있습니다. 스냅샷은 소스 시스템에 저장됩니다.

소스 시스템	**2**차 시스템**(**복제**)**	대상 개체 저장소**(**백업**)**
AWS의 Cloud Volumes ONTAP	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	아마존 S3
Azure의 Cloud Volumes ONTAP	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Azure Blob
Google의 Cloud Volumes ONTAP	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	구글 클라우드 스토리지
온프레미스 ONTAP 시스템	Cloud Volumes ONTAP 온프레미스 ONTAP 시스템	Amazon S3 Azure Blob Google Cloud Storage NetApp StorageGRID ONTAP S3

지원되는 복원 대상

보조 시스템(복제된 볼륨) 또는 개체 스토리지(백업 파일)에 있는 백업 파일에서 ONTAP 데이터를 다음 시스템으로 복원할 수 있습니다. 스냅샷은 소스 시스템에 상주하며 동일한 시스템으로만 복원할 수 있습니다.

백업 파일 위치		목적지 시스템
객체 저장소**(**백업**)**	**2**차 시스템**(**복제**)**	
아마존 S3	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
Azure Blob	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP

백업 파일 위치		목적지 시스템
구글 클라우드 스토리지	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
NetApp StorageGRID	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP	온프레미스 ONTAP 시스템
ONTAP S3	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP	온프레미스 ONTAP 시스템

"온프레미스 ONTAP 시스템"에 대한 참조에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

지원되는 볼륨

NetApp Backup and Recovery 다음 유형의 볼륨을 지원합니다.

- FlexVol 읽기-쓰기 볼륨
- FlexGroup 볼륨(ONTAP 9.12.1 이상 필요)
- SnapLock Enterprise 볼륨(ONTAP 9.11.1 이상 필요)
- 온프레미스 볼륨에 대한 SnapLock Compliance (ONTAP 9.14 이상 필요)
- SnapMirror 데이터 보호(DP) 대상 볼륨

NetApp Backup and Recovery FlexCache 볼륨의 백업을 지원하지 않습니다.

섹션을 참조하세요"ONTAP 볼륨에 대한 백업 및 복원 제한 사항" 추가 요구 사항 및 제한 사항에 대해서는.

비용

ONTAP 시스템과 함께 NetApp Backup and Recovery 사용하는 경우 리소스 요금과 서비스 요금이라는 두 가지 유형의 비용이 발생합니다. 두 요금 모두 서비스의 객체 백업 부분에 대한 요금입니다.

스냅샷이나 복제 볼륨을 생성하는 데에는 비용이 들지 않습니다. 스냅샷과 복제 볼륨을 저장하는 데 필요한 디스크 공간 외에는 비용이 들지 않습니다.

자원 요금

리소스 요금은 객체 저장 용량과 클라우드에 백업 파일을 쓰고 읽는 데 대한 비용으로 클라우드 제공자에게 지불됩니다.

- 개체 스토리지에 백업하는 경우 클라우드 공급자에게 개체 스토리지 비용을 지불합니다.

  NetApp Backup and Recovery 소스 볼륨의 스토리지 효율성을 보존하므로 ONTAP 효율성 이후의 데이터(중복 제거 및 압축이 적용된 후의 더 적은 양의 데이터)에 대해 클라우드 공급자 개체 스토리지 비용을 지불합니다.

- 검색 및 복원을 사용하여 데이터를 복원하는 경우 클라우드 공급자가 특정 리소스를 제공하며, 검색 요청으로 스캔된 데이터 양에 따라 TiB당 비용이 발생합니다. (이러한 리소스는 찾아보기 및 복원에 필요하지 않습니다.)
  - AWS에서 "아마존 아테나" 그리고 "AWS 글루" 리소스는 새로운 S3 버킷에 배포됩니다.
  - Azure에서는 "Azure Synapse 작업 영역" 그리고 "Azure 데이터 레이크 스토리지" 귀하의 데이터를 저장하고 분석하기 위해 귀하의 스토리지 계정에 프로비저닝됩니다.

    - Google에서는 새로운 버킷이 배포되고 "Google Cloud BigQuery 서비스" 계정/프로젝트 수준에서 제공됩니다.

- 보관 개체 스토리지로 이동된 백업 파일에서 볼륨 데이터를 복원하려는 경우 클라우드 공급자가 GiB당 추가 검색 요금과 요청당 요금을 부과합니다.
- 볼륨 데이터를 복원하는 과정에서 랜섬웨어에 대한 백업 파일을 스캔할 계획이라면(클라우드 백업에 대해 DataLock 및 랜섬웨어 복원력을 활성화한 경우), 클라우드 공급업체로부터 추가적인 퇴출 비용도 발생합니다.

서비스 요금

서비스 요금은 NetApp 에 지불되며, 여기에는 개체 스토리지에 대한 백업을 _생성_하는 비용과 해당 백업에서 볼륨이나 파일을 _복원_하는 비용이 모두 포함됩니다. ONTAP 볼륨의 소스 논리적 사용 용량(ONTAP 효율성 이전)을 기준으로 개체 스토리지에 백업된 데이터에 대해서만 비용을 지불합니다. 이 용량은 프런트엔드 테라바이트(FETB)라고도 합니다.

백업 서비스 비용은 세 가지 방법으로 지불할 수 있습니다. 첫 번째 옵션은 월 단위로 요금을 지불하고 클라우드 제공업체에 가입하는 것입니다. 두 번째 옵션은 연간 계약을 맺는 것입니다. 세 번째 옵션은 NetApp 에서 직접 라이선스를 구매하는 것입니다.

라이센스

NetApp Backup and Recovery 다음과 같은 소비 모델로 제공됩니다.

- **BYOL**: NetApp 에서 구매한 라이선스로 모든 클라우드 공급자와 함께 사용할 수 있습니다.
- **PAYGO**: 클라우드 공급업체의 마켓플레이스에서 제공하는 시간당 구독입니다.
- 연간: 클라우드 공급업체의 마켓플레이스와 맺은 연간 계약입니다.

백업 라이선스는 개체 스토리지에서 백업하고 복원하는 데만 필요합니다. 스냅샷과 복제 볼륨을 만드는 데는 라이선스가 필요하지 않습니다.

면허증을 직접 가져오세요

BYOL은 기간 기반(1년, 2년 또는 3년)이며 1TiB 단위로 용량을 결정합니다. 예를 들어 1년 동안 일정 기간 동안 NetApp 에 서비스를 사용하고 최대 용량(예: 10TiB)을 지불합니다.

서비스를 활성화하려면 NetApp Console 에 입력하는 일련 번호를 받게 됩니다. 두 가지 제한 중 하나에 도달하면 라이센스를 갱신해야 합니다. 백업 BYOL 라이선스는 NetApp Console 조직 또는 계정과 연결된 모든 소스 시스템에 적용됩니다.

"BYOL 라이선스를 관리하는 방법을 알아보세요".

사용량에 따라 지불하는 구독

NetApp Backup and Recovery 사용량 기반 라이선스를 사용량에 따라 지불하는 모델로 제공합니다. 클라우드 공급업체의 마켓플레이스를 통해 구독한 후, 백업된 데이터에 대해 GiB당 요금을 지불합니다. 선불금은 없습니다. 귀하는 월별 청구서를 통해 클라우드 제공자로부터 요금을 청구받습니다.

"사용량에 따른 요금제 구독을 설정하는 방법을 알아보세요".

PAYGO 구독에 처음 가입하면 30일 무료 체험판을 이용할 수 있습니다.

연간 계약

AWS를 사용하면 1년, 2년 또는 3년 기간의 연간 계약 두 가지를 이용할 수 있습니다.

- Cloud Volumes ONTAP 데이터와 온프레미스 ONTAP 데이터를 백업할 수 있는 "클라우드 백업" 플랜입니다.
- Cloud Volumes ONTAP 과 NetApp Backup and Recovery 번들로 제공하는 "CVO Professional" 플랜입니다. 여기에는 이 라이선스에 따라 청구되는 Cloud Volumes ONTAP 볼륨에 대한 무제한 백업이 포함됩니다(백업 용량은 라이선스에 포함되지 않습니다).

Azure를 사용하면 1년, 2년 또는 3년 기간의 연간 계약 두 가지를 이용할 수 있습니다.

- Cloud Volumes ONTAP 데이터와 온프레미스 ONTAP 데이터를 백업할 수 있는 "클라우드 백업" 플랜입니다.
- Cloud Volumes ONTAP 과 NetApp Backup and Recovery 번들로 제공하는 "CVO Professional" 플랜입니다. 여기에는 이 라이선스에 따라 청구되는 Cloud Volumes ONTAP 볼륨에 대한 무제한 백업이 포함됩니다(백업 용량은 라이선스에 포함되지 않습니다).

GCP를 사용하면 NetApp 에서 비공개 제안을 요청한 다음 NetApp Backup and Recovery 활성화 중에 Google Cloud Marketplace에서 구독할 때 플랜을 선택할 수 있습니다.

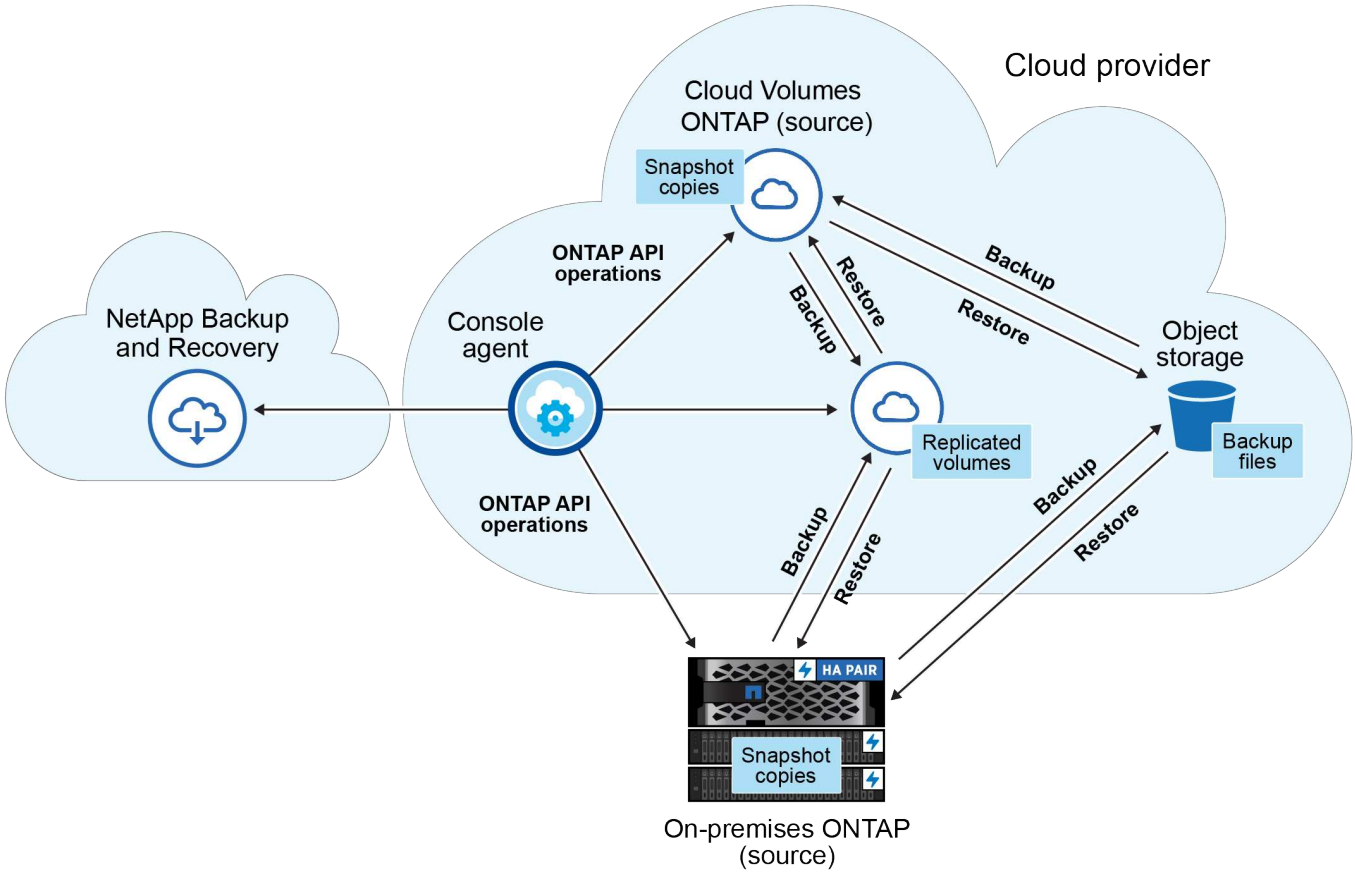
"연간 계약을 설정하는 방법을 알아보세요".

NetApp Backup and Recovery 작동 방식

Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템에서 NetApp Backup and Recovery 활성화하면 해당 서비스가 데이터의 전체 백업을 수행합니다. 최초 백업 이후 모든 추가 백업은 증분식으로, 변경된 블록과 새 블록만 백업됩니다. 이렇게 하면 네트워크 트래픽이 최소화됩니다. 개체 스토리지에 대한 백업은 다음을 기반으로 구축됩니다. "NetApp SnapMirror 클라우드 기술" .

클라우드 백업 파일을 관리하거나 변경하기 위해 클라우드 공급자 환경에서 직접 수행한 모든 작업은 파일을 손상시킬 수 있으며 지원되지 않는 구성으로 이어질 수 있습니다.

다음 이미지는 각 구성 요소 간의 관계를 보여줍니다.



이 다이어그램은 볼륨이 Cloud Volumes ONTAP 시스템에 복제되는 것을 보여주지만, 볼륨은 온프레미스 ONTAP 시스템에도 복제될 수 있습니다.

백업이 있는 위치

백업은 백업 유형에 따라 다른 위치에 저장됩니다.

- _스냅샷_은 소스 시스템의 소스 볼륨에 상주합니다.
- _복제된 볼륨_은 보조 스토리지 시스템(Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템)에 상주합니다.
- _백업 사본_은 콘솔이 클라우드 계정에 생성하는 개체 저장소에 저장됩니다. 클러스터/시스템당 하나의 개체 저장소가 있으며, 콘솔에서는 개체 저장소의 이름을 "netapp-backup-clusteruuid"로 지정합니다. 이 개체 저장소를 삭제하지 마십시오.
  - AWS에서 콘솔을 사용하면 다음이 가능합니다. "Amazon S3 블록 퍼블릭 액세스 기능" S3 버킷에 저장됩니다.
  - Azure에서 콘솔은 Blob 컨테이너에 대한 스토리지 계정이 있는 새 리소스 그룹 또는 기존 리소스 그룹을 사용합니다. 콘솔 "Blob 데이터에 대한 공개 액세스를 차단합니다." 기본적으로.
  - GCP에서 콘솔은 Google Cloud Storage 버킷에 대한 스토리지 계정이 있는 새 프로젝트 또는 기존 프로젝트를 사용합니다.
  - StorageGRID 에서 콘솔은 S3 버킷에 기존 테넌트 계정을 사용합니다.
  - ONTAP S3에서 콘솔은 S3 버킷에 대한 기존 사용자 계정을 사용합니다.

나중에 클러스터의 대상 개체 저장소를 변경하려면 다음이 필요합니다."시스템에 대한 NetApp Backup and Recovery 등록 취소" 그런 다음 새로운 클라우드 공급자 정보를 사용하여 NetApp Backup and Recovery 활성화합니다.

사용자 정의 가능한 백업 일정 및 보존 설정

시스템에 대해 NetApp Backup and Recovery 활성화하면 처음에 선택한 모든 볼륨이 선택한 정책을 사용하여 백업됩니다. 스냅샷, 복제된 볼륨, 백업 파일에 대해 별도의 정책을 선택할 수 있습니다. 서로 다른 복구 지점 목표(RPO)를 가진 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 해당 클러스터에 대한 추가 정책을 만들고 NetApp Backup and Recovery 활성화된 후 해당 정책을 다른 볼륨에 할당할 수 있습니다.

모든 볼륨에 대해 시간별, 일별, 주별, 월별, 연간 백업을 조합하여 선택할 수 있습니다. 개체에 대한 백업의 경우 3개월, 1년, 7년 동안 백업 및 보존을 제공하는 시스템 정의 정책 중 하나를 선택할 수도 있습니다. ONTAP System Manager나 ONTAP CLI를 사용하여 클러스터에서 생성한 백업 보호 정책도 선택 항목으로 나타납니다. 여기에는 사용자 정의 SnapMirror 레이블을 사용하여 생성된 정책이 포함됩니다.

볼륨에 적용된 스냅샷 정책에는 복제 정책과 개체 정책에 사용하는 레이블 중 하나가 있어야 합니다. 일치하는 라벨이 발견되지 않으면 백업 파일이 생성되지 않습니다. 예를 들어, "주간" 복제 볼륨과 백업 파일을 생성하려면 "주간" 스냅샷을 생성하는 스냅샷 정책을 사용해야 합니다.

카테고리 또는 간격에 대한 최대 백업 수에 도달하면 이전 백업이 제거되어 항상 최신 백업을 보유할 수 있습니다(따라서 오래된 백업이 더 이상 공간을 차지하지 않습니다).

데이터 보호 볼륨의 백업 보존 기간은 소스 SnapMirror 관계에서 정의된 기간과 동일합니다. 원하시면 API를 사용하여 이를 변경할 수 있습니다.

백업 파일 보호 설정

클러스터에서 ONTAP 9.11.1 이상을 사용하는 경우 개체 스토리지의 백업을 삭제 및 랜섬웨어 공격으로부터 보호할 수 있습니다. 각 백업 정책은 특정 기간(보존 기간) 동안 백업 파일에 적용할 수 있는 데이터 잠금 및 랜섬웨어 복원력 섹션을 제공합니다.

- _DataLock_은 백업 파일이 수정되거나 삭제되는 것을 방지합니다.
- 랜섬웨어 보호 기능은 백업 파일을 생성할 때와 백업 파일의 데이터를 복원할 때 랜섬웨어 공격의 증거를 찾기 위해 백업 파일을 검사합니다.

예약된 랜섬웨어 보호 검사는 기본적으로 활성화되어 있습니다. 검사 빈도의 기본 설정은 7일입니다. 스캔은 최신 스냅샷에서만 수행됩니다. 예약된 검사는 비용을 절감하기 위해 비활성화할 수 있습니다. 고급 설정 페이지의 옵션을 사용하면 최신 스냅샷에 대한 예약된 랜섬웨어 검사를 활성화하거나 비활성화할 수 있습니다. 이 기능을 활성화하면 기본적으로 매주 검사가 수행됩니다. 일정을 며칠이나 몇 주로 변경하거나 비활성화하여 비용을 절감할 수 있습니다.

백업 보존 기간은 백업 일정 보존 기간과 동일하며, 최대 31일의 버퍼 기간이 추가됩니다. 예를 들어, *5*_개의 사본을 보관하는 _주간 백업의 경우 각 백업 파일은 5주 동안 잠깁니다. *6*_개의 사본을 보관하는 _월별 백업의 경우 각 백업 파일은 6개월 동안 잠깁니다.

현재 백업 대상이 Amazon S3, Azure Blob 또는 NetApp StorageGRID 인 경우에만 지원이 제공됩니다. 향후 릴리스에서는 다른 스토리지 공급자 대상지가 추가될 예정입니다.

자세한 내용은 다음 정보를 참조하세요.

- "DataLock 및 랜섬웨어 보호 작동 방식".
- "고급 설정 페이지에서 랜섬웨어 보호 옵션을 업데이트하는 방법".

백업을 보관 저장소에 계층화하는 경우 DataLock을 활성화할 수 없습니다.

이전 백업 파일을 위한 보관 저장소

특정 클라우드 스토리지를 사용하는 경우, 일정 기간이 지나면 오래된 백업 파일을 비용이 덜 드는 스토리지 클래스/액세스 계층으로 옮길 수 있습니다. 표준 클라우드 저장소에 쓰지 않고도 백업 파일을 즉시 보관 저장소로 보내도록 선택할 수도 있습니다. DataLock을 활성화한 경우 보관 저장소를 사용할 수 없습니다.

- AWS에서 백업은 *Standard* 스토리지 클래스에서 시작하여 30일 후에 *Standard-Infrequent Access* 스토리지 클래스로 전환됩니다.

  클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 NetApp Backup and Recovery UI에서 특정 일수 후에 이전 백업을 *S3 Glacier* 또는 *S3 Glacier Deep Archive* 스토리지로 계층화하여 비용을 더욱 최적화할 수 있습니다. "AWS 보관 스토리지에 대해 자세히 알아보세요".

- Azure에서 백업은 *Cool* 액세스 계층과 연결됩니다.

  클러스터에서 ONTAP 9.10.1 이상을 사용하는 경우 NetApp Backup and Recovery UI에서 특정 일수 후에 이전 백업을 *Azure Archive* 스토리지로 계층화하여 비용을 더욱 최적화할 수 있습니다. "Azure 보관 저장소에 대해 자세히 알아보세요".

- GCP에서 백업은 *Standard* 스토리지 클래스와 연결됩니다.

  클러스터에서 ONTAP 9.12.1 이상을 사용하는 경우 NetApp Backup and Recovery UI에서 특정 기간 후에 이전 백업을 아카이브 스토리지로 계층화하여 비용을 더욱 최적화할 수 있습니다. "Google 보관 저장소에 대해 자세히 알아보세요".

- StorageGRID 에서 백업은 *Standard* 스토리지 클래스와 연결됩니다.

  온프레미스 클러스터에서 ONTAP 9.12.1 이상을 사용하고 StorageGRID 시스템에서 11.4 이상을 사용하는 경우, 특정 일수가 지난 후 이전 백업 파일을 퍼블릭 클라우드 보관 스토리지에 보관할 수 있습니다. 현재 지원되는 스토리지 계층은 AWS S3 Glacier/S3 Glacier Deep Archive 또는 Azure Archive 스토리지 계층입니다. "StorageGRID 에서 백업 파일을 보관하는 방법에 대해 자세히 알아보세요.".

이전 백업 파일을 보관하는 방법에 대한 자세한 내용은 링크:prev-ontap-policy-object-options.html을 참조하세요.

FabricPool 계층화 정책 고려 사항

백업하는 볼륨이 FabricPool 집계에 있고 할당된 계층화 정책이 있는 경우 알아야 할 몇 가지 사항이 있습니다. `none` :

- FabricPool 계층형 볼륨의 첫 번째 백업에는 모든 로컬 데이터와 모든 계층형 데이터(객체 저장소에서)를 읽어야 합니다. 백업 작업은 개체 스토리지에 계층화된 콜드 데이터를 "다시 가열"하지 않습니다.

  이 작업으로 인해 클라우드 공급자로부터 데이터를 읽는 데 드는 비용이 한 번 증가할 수 있습니다.

  - 이후 백업은 증분식으로 이루어지므로 이러한 효과가 없습니다.
  - 볼륨을 처음 생성할 때 계층화 정책이 볼륨에 할당된 경우 이 문제가 발생하지 않습니다.

- 백업을 할당하기 전에 백업의 영향을 고려하십시오. `all` 볼륨에 대한 계층화 정책. 데이터가 즉시 계층화되므로 NetApp Backup and Recovery 로컬 계층이 아닌 클라우드 계층에서 데이터를 읽습니다. 동시 백업 작업은 클라우드 객체 저장소에 대한 네트워크 링크를 공유하므로 네트워크 리소스가 포화 상태가 되면 성능 저하가 발생할 수 있습니다. 이 경우 네트워크 포화 상태를 줄이기 위해 여러 네트워크 인터페이스(LIF)를 사전에 구성하는 것이 좋습니다.

NetApp Backup and Recovery 통해 보호 여정을 계획하세요

NetApp Backup and Recovery 사용하면 소스 볼륨의 복사본을 최대 3개까지 만들어 데이터를 보호할 수 있습니다. 볼륨에서 백업 및 복구를 활성화할 때 선택할 수 있는 옵션이 많으므로 준비할 수 있도록 선택 사항을 검토해야 합니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

다음 옵션을 살펴보겠습니다.

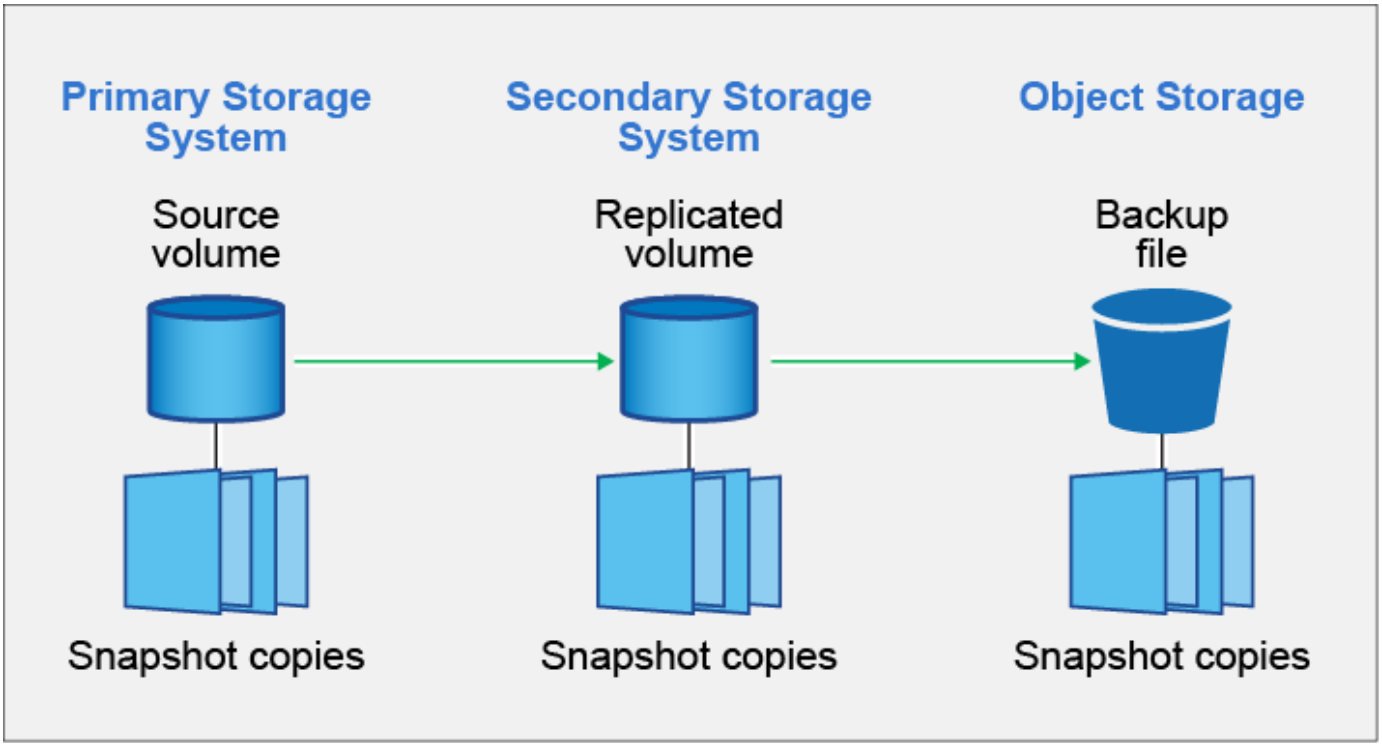
- 스냅샷, 복제 볼륨 및/또는 클라우드 백업 중 어떤 보호 기능을 사용하시겠습니까?
- 어떤 백업 아키텍처를 사용하시겠습니까? 볼륨의 캐스케이드 백업 또는 팬아웃 백업
- 기본 백업 정책을 사용할 것인가, 아니면 사용자 지정 정책을 만들어야 합니까?
- 서비스에서 클라우드 버킷을 생성해 주길 원하시나요, 아니면 작업을 시작하기 전에 개체 스토리지 컨테이너를 만들어 주길 원하시나요?
- 어떤 콘솔 에이전트 배포 모드를 사용하고 있습니까(표준, 제한 또는 개인 모드)?

어떤 보호 기능을 사용하시겠습니까?

사용할 기능을 선택하기 전에 각 기능의 기능과 제공되는 보호 유형에 대한 간단한 설명을 확인해 보세요.

백업 유형	설명
스냅샷	소스 볼륨 내의 볼륨에 대한 읽기 전용, 특정 시점 이미지를 스냅샷으로 생성합니다. 스냅샷을 사용하여 개별 파일을 복구하거나 볼륨의 전체 내용을 복원할 수 있습니다.
복제	다른 ONTAP 스토리지 시스템에 데이터의 보조 사본을 만들고 보조 데이터를 지속적으로 업데이트합니다. 귀하의 데이터는 최신 상태로 유지되며 필요할 때마다 사용할 수 있습니다.
클라우드 백업	보호 및 장기 보관 목적으로 데이터를 클라우드에 백업합니다. 필요한 경우 백업에서 볼륨, 폴더 또는 개별 파일을 동일하거나 다른 시스템으로 복원할 수 있습니다.

스냅샷은 모든 백업 방법의 기반이며, 백업 및 복구 서비스를 사용하려면 필수입니다. 스냅샷은 볼륨의 읽기 전용 특정 시점 이미지입니다. 이미지는 최소한의 저장 공간을 사용하고 마지막 스냅샷이 만들어진 이후 파일의 변경 사항만 기록하므로 성능 오버헤드가 무시할 수 있을 정도입니다. 볼륨에 생성된 스냅샷은 복제된 볼륨과 백업 파일을 소스 볼륨의 변경 사항과 동기화하는 데 사용됩니다(그림 참조).



다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성하고 클라우드에 백업 파일을 생성할 수 있습니다. 아니면 복제된 볼륨이나 백업 파일만 만들 수도 있습니다. 선택은 사용자에게 달려 있습니다.

요약하자면, ONTAP 시스템의 볼륨에 대해 생성할 수 있는 유효한 보호 흐름은 다음과 같습니다.

- 소스 볼륨 → 스냅샷 → 복제된 볼륨 → 백업 파일
- 소스 볼륨 → 스냅샷 → 백업 파일
- 소스 볼륨 → 스냅샷 → 복제된 볼륨

복제된 볼륨이나 백업 파일을 처음 만들 때는 소스 데이터의 전체 사본이 포함됩니다. 이를 _기준선 전송_이라고 합니다. 이후 전송에는 소스 데이터의 차등 사본(스냅샷)만 포함됩니다.

다양한 백업 방법 비교

다음 표는 세 가지 백업 방법을 일반적으로 비교한 것입니다. 일반적으로 개체 스토리지 공간은 온프레미스 디스크 스토리지보다 비용이 저렴하지만, 클라우드에서 데이터를 자주 복원할 것으로 생각된다면 클라우드 공급업체의 이탈 수수료로 인해 절감액이 일부 줄어들 수 있습니다. 클라우드에 있는 백업 파일에서 데이터를 얼마나 자주 복원해야 하는지 파악해야 합니다.

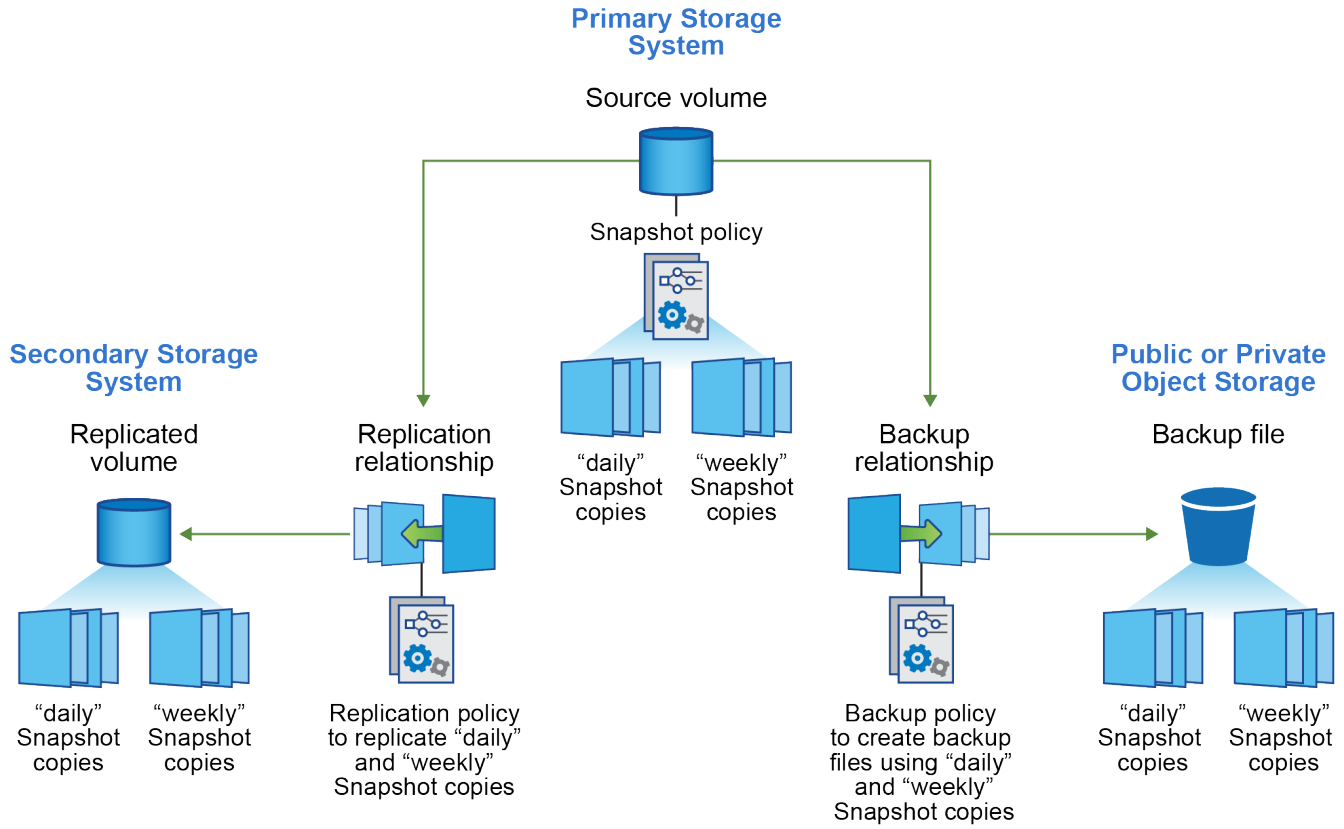
이러한 기준 외에도 클라우드 스토리지는 DataLock 및 랜섬웨어 복원력 기능을 사용하면 추가적인 보안 옵션을 제공하고, 오래된 백업 파일에 대한 보관 스토리지 클래스를 선택하면 추가적으로 비용을 절감할 수 있습니다. "DataLock 및 랜섬웨어 보호와 보관 스토리지 설정에 대해 자세히 알아보세요.".

백업 유형	백업 속도	백업 비용	속도 복원	복구 비용
스냅 사진	높은	낮음(디스크 공간)	높은	낮은
복제	중간	중간(디스크 공간)	중간	중간(네트워크)
클라우드 백업	낮은	낮음(객체 공간)	낮은	높음 (공급자 수수료)

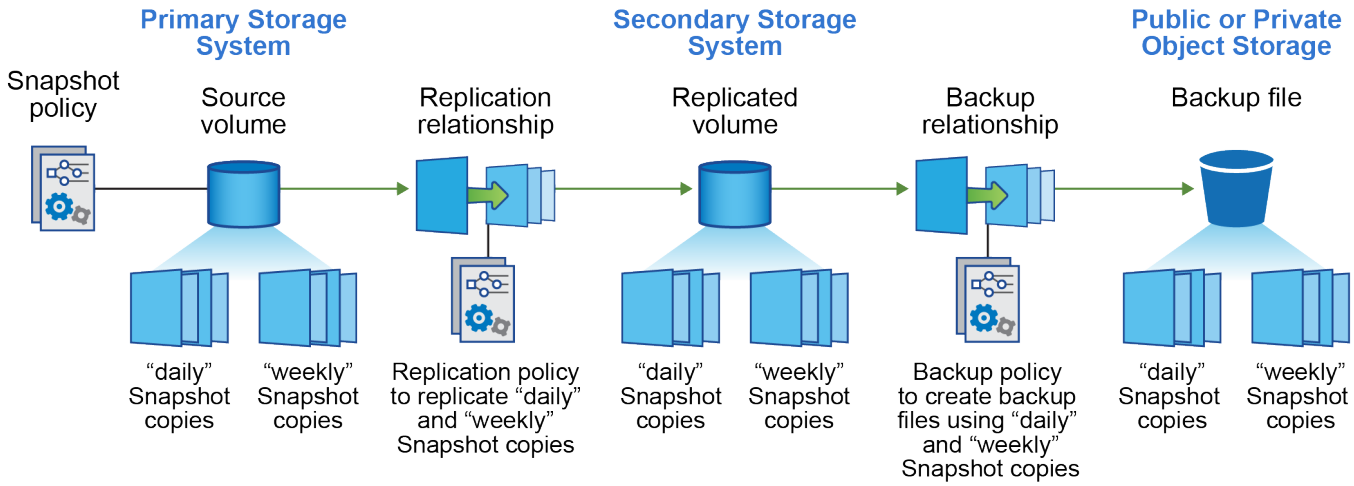
어떤 백업 아키텍처를 사용하시겠습니까?

복제된 볼륨과 백업 파일을 모두 생성할 때 볼륨을 백업하기 위해 팬아웃 또는 캐스케이드 아키텍처를 선택할 수 있습니다.

팬아웃 아키텍처는 스냅샷을 대상 스토리지 시스템과 클라우드의 백업 객체 모두에 독립적으로 전송합니다.



캐스케이드 아키텍처는 스냅샷을 먼저 대상 스토리지 시스템으로 전송한 다음, 해당 시스템이 복사본을 클라우드의 백업 개체로 전송합니다.



다양한 아키텍처 선택 비교

이 표는 팬아웃과 캐스케이드 아키텍처를 비교한 것입니다.

팬아웃	종속
스냅샷을 2개의 서로 다른 시스템으로 전송하기 때문에 소스 시스템에 미치는 성능 영향이 적습니다.	스냅샷을 한 번만 전송하므로 소스 스토리지 시스템의 성능에 미치는 영향이 적습니다.
모든 정책, 네트워킹 및 ONTAP 구성이 소스 시스템에서 수행되므로 설정이 더 쉽습니다.	보조 시스템에서도 일부 네트워킹 및 ONTAP 구성이 필요합니다.

스냅샷, 복제 및 백업에 기본 정책을 사용하시겠습니까?

NetApp 에서 제공하는 기본 정책을 사용하여 백업을 만들 수도 있고, 사용자 정의 정책을 만들 수도 있습니다. 활성화 마법사를 사용하여 볼륨의 백업 및 복구 서비스를 활성화하면 기본 정책과 시스템(Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템)에 이미 있는 다른 정책 중에서 선택할 수 있습니다. 기존 정책과 다른 정책을 사용하려면 활성화 마법사를 시작하기 전이나 사용하는 동안 정책을 만들 수 있습니다.

- 기본 스냅샷 정책은 매시간, 매일, 매주 스냅샷을 생성하여 매시간 6개, 매일 2개, 매주 2개의 스냅샷을 보관합니다.
- 기본 복제 정책은 일일 및 주간 스냅샷을 복제하여 일일 스냅샷 7개와 주간 스냅샷 52개를 보관합니다.
- 기본 백업 정책은 일일 및 주간 스냅샷을 복제하여 일일 스냅샷 7개와 주간 스냅샷 52개를 보관합니다.

복제 또는 백업에 대한 사용자 지정 정책을 생성하는 경우 정책 레이블(예: "매일" 또는 "매주")이 스냅샷 정책이나 복제된 볼륨에 있는 레이블과 일치해야 하며 백업 파일이 생성되지 않습니다.

NetApp Backup and Recovery UI에서 개체 스토리지 정책에 대한 스냅샷, 복제 및 백업을 생성할 수 있습니다. 섹션을 참조하세요"새로운 백업 정책 추가" 자세한 내용은.

NetApp Backup and Recovery 사용하여 사용자 정의 정책을 만드는 것 외에도 System Manager나 ONTAP 명령줄 인터페이스(CLI)를 사용할 수 있습니다.

- "System Manager 또는 ONTAP CLI를 사용하여 스냅샷 정책을 만듭니다."
- "System Manager 또는 ONTAP CLI를 사용하여 복제 정책을 만듭니다."

참고: 시스템 관리자를 사용하는 경우 복제 정책의 정책 유형으로 비동기*를 선택하고, 개체 백업 정책의 경우 *비동기 및 *클라우드에 백업*을 선택합니다.

사용자 지정 정책을 만드는 경우 도움이 될 수 있는 몇 가지 ONTAP CLI 명령 샘플을 소개합니다. *admin* vserver(저장소 VM)를 사용해야 한다는 점에 유의하세요. `<vserver_name>` 이러한 명령에서.

정책 설명	명령
간단한 스냅샷 정책	`snapshot policy create -policy WeeklySnapshotPolicy -enabled true -schedule1 weekly -count1 10 -vserver ClusterA -snapmirror-label1 weekly`
클라우드로의 간단한 백업	`snapmirror policy create -policy <policy_name> -transfer -priority normal -vserver <vserver_name> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

정책 설명	명령
DataLock 및 랜섬웨어 보호 기능을 갖춘 클라우드 백업	`snapmirror policy create -policy CloudBackupService-Enterprise -snapshot-lock-mode enterprise -vserver <vserver_name>` `snapmirror policy add-rule -policy CloudBackupService-Enterprise -retention-period 30days`
보관 스토리지 클래스를 사용한 클라우드 백업	`snapmirror policy create -vserver <vserver_name> -policy <policy_name> -archive-after-days <days> -create -snapshot-on-source false -type vault` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`
다른 스토리지 시스템으로의 간단한 복제	`snapmirror policy create -policy <policy_name> -type async-mirror -vserver <vserver_name>` `snapmirror policy add-rule -policy <policy_name> -vserver <vserver_name> -snapmirror-label <snapmirror_label> -keep`

클라우드 관계에 대한 백업에는 볼트 정책만 사용할 수 있습니다.

내 보험은 어디에 있나요?

백업 정책은 사용하려는 백업 아키텍처(팬아웃 또는 캐스케이딩)에 따라 다른 위치에 있습니다. 복제 정책과 백업 정책은 동일한 방식으로 설계되지 않았습니다. 복제는 두 개의 ONTAP 스토리지 시스템을 쌍으로 구성하고 개체에 대한 백업은 스토리지 공급자를 대상으로 사용하기 때문입니다.

- 스냅샷 정책은 항상 기본 스토리지 시스템에 있습니다.
- 복제 정책은 항상 보조 스토리지 시스템에 있습니다.
- 개체 백업 정책은 소스 볼륨이 있는 시스템에서 생성됩니다. 이는 팬아웃 구성의 기본 클러스터이고, 계단식 구성의 보조 클러스터입니다.

이러한 차이점은 표에 나와 있습니다.

아키텍처	스냅샷 정책	복제 정책	백업 정책
팬아웃	주요한	반성	주요한
종속	주요한	반성	반성

따라서 계단식 아키텍처를 사용할 때 사용자 지정 정책을 만들 계획이라면 복제 볼륨이 생성될 보조 시스템에서 복제 및 개체 정책에 대한 백업을 만들어야 합니다. 팬아웃 아키텍처를 사용할 때 사용자 지정 정책을 만들 계획이라면 복제 볼륨이 생성될 보조 시스템에서 복제 정책을 만들고 기본 시스템에서 개체 정책으로 백업을 만들어야 합니다.

모든 ONTAP 시스템에 존재하는 기본 정책을 사용한다면 아무런 문제가 없습니다.

자체 객체 스토리지 컨테이너를 만들고 싶습니까?

시스템의 개체 스토리지에 백업 파일을 만들면 기본적으로 백업 및 복구 서비스는 사용자가 구성한 개체 스토리지 계정에 백업 파일에 대한 컨테이너(버킷 또는 스토리지 계정)를 만듭니다. AWS 또는 GCP 버킷의 이름은 기본적으로

"netapp-backup-<uuid>"로 지정됩니다. Azure Blob 저장소 계정의 이름은 "netappbackup<uuid>"입니다.

특정 접두사를 사용하거나 특수 속성을 지정하려면 개체 공급자 계정에서 직접 컨테이너를 만들 수 있습니다. 자체 컨테이너를 만들려면 활성화 마법사를 시작하기 전에 컨테이너를 만들어야 합니다. NetApp Backup and Recovery 모든 버킷을 사용하고 버킷을 공유할 수 있습니다. 백업 활성화 마법사는 선택한 계정과 자격 증명에 대해 프로비저닝된 컨테이너를 자동으로 검색하므로 사용할 컨테이너를 선택할 수 있습니다.

콘솔이나 클라우드 공급자를 통해 버킷을 만들 수 있습니다.

- "콘솔에서 Amazon S3 버킷 만들기"
- "콘솔에서 Azure Blob 저장소 계정 만들기"
- "콘솔에서 Google Cloud Storage 버킷 만들기"

"netapp-backup-xxxxxx"가 아닌 다른 버킷 접두사를 사용하려는 경우 콘솔 에이전트 IAM 역할에 대한 S3 권한을 수정해야 합니다.

고급 버킷 설정

이전 백업 파일을 보관 저장소로 이동하거나 DataLock 및 랜섬웨어 보호 기능을 활성화하여 백업 파일을 잠그고 랜섬웨어가 있는지 검사하려는 경우 특정 구성 설정을 사용하여 컨테이너를 만들어야 합니다.

- 현재 클러스터에서 ONTAP 9.10.1 이상의 소프트웨어를 사용하는 경우 AWS S3 스토리지에서 자체 버킷의 보관 스토리지가 지원됩니다. 기본적으로 백업은 S3 *Standard* 스토리지 클래스에서 시작됩니다. 적절한 수명 주기 규칙으로 버킷을 생성했는지 확인하세요.
  - 30일 후에 버킷 전체 범위의 객체를 S3 _Standard-IA_로 이동합니다.
  - "smc_push_to_archive: true" 태그가 있는 객체를 *Glacier Flexible Retrieval*(이전 S3 Glacier)로 이동합니다.
- 클러스터에서 ONTAP 9.11.1 이상 소프트웨어를 사용하는 경우 AWS 스토리지에서 DataLock 및 랜섬웨어 보호가 지원되고, ONTAP 9.12.1 이상 소프트웨어를 사용하는 경우 Azure 스토리지에서 DataLock 및 랜섬웨어 보호가 지원됩니다.
  - AWS의 경우 30일 보존 기간을 사용하여 버킷에서 개체 잠금을 활성화해야 합니다.
  - Azure의 경우 버전 수준 불변성 지원이 포함된 저장소 클래스를 만들어야 합니다.

어떤 콘솔 에이전트 배포 모드를 사용하고 있습니까?

이미 콘솔을 사용하여 저장소를 관리하고 있다면 콘솔 에이전트가 이미 설치되어 있습니다. NetApp Backup and Recovery 와 동일한 콘솔 에이전트를 사용할 계획이라면 준비가 완료된 것입니다. 다른 콘솔 에이전트를 사용해야 하는 경우 백업 및 복구 구현을 시작하기 전에 해당 에이전트를 설치해야 합니다.

NetApp Console 비즈니스 및 보안 요구 사항을 충족하는 방식으로 콘솔을 사용할 수 있도록 다양한 배포 모드를 제공합니다. _표준 모드_는 콘솔 SaaS 계층을 활용하여 모든 기능을 제공하는 반면, _제한 모드_와 _개인 모드_는 연결 제한이 있는 조직에서 사용할 수 있습니다.

"NetApp Console 배포 모드에 대해 자세히 알아보세요".

인터넷 연결이 완벽하게 가능한 사이트 지원

NetApp Backup and Recovery 완전한 인터넷 연결(표준 모드 또는 SaaS 모드라고도 함)이 있는 사이트에서 사용하는 경우 콘솔에서 관리하는 모든 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템에 복제된 볼륨을 만들 수

있으며, 지원되는 모든 클라우드 공급자의 개체 스토리지에 백업 파일을 만들 수 있습니다. "지원되는 백업 대상의 전체 목록을 확인하세요.".

유효한 콘솔 에이전트 위치 목록을 보려면 백업 파일을 만들려는 클라우드 공급자의 다음 백업 절차 중 하나를 참조하세요. 콘솔 에이전트를 Linux 시스템에 수동으로 설치하거나 특정 클라우드 공급자에 배포해야 하는 몇 가지 제한 사항이 있습니다.

- "Cloud Volumes ONTAP 데이터를 Amazon S3에 백업합니다."
- "Cloud Volumes ONTAP 데이터를 Azure Blob에 백업"
- "Cloud Volumes ONTAP 데이터를 Google Cloud에 백업"
- "온프레미스 ONTAP 데이터를 Amazon S3에 백업"
- "온-프레미스 ONTAP 데이터를 Azure Blob에 백업"
- "온프레미스 ONTAP 데이터를 Google Cloud에 백업"
- "온프레미스 ONTAP 데이터를 StorageGRID 에 백업"
- "온프레미스 ONTAP ONTAP S3로 백업"

인터넷 연결이 제한된 사이트 지원

NetApp Backup and Recovery 인터넷 연결이 제한된 사이트(제한 모드라고도 함)에서 볼륨 데이터를 백업하는 데 사용할 수 있습니다. 이 경우 대상 클라우드 지역에 콘솔 에이전트를 배포해야 합니다.

- AWS 상업 지역에 설치된 온프레미스 ONTAP 시스템이나 Cloud Volumes ONTAP 시스템의 데이터를 Amazon S3에 백업할 수 있습니다. "Cloud Volumes ONTAP 데이터를 Amazon S3에 백업합니다.".
- Azure 상용 지역에 설치된 온-프레미스 ONTAP 시스템 또는 Cloud Volumes ONTAP 시스템의 데이터를 Azure Blob에 백업할 수 있습니다. "Cloud Volumes ONTAP 데이터를 Azure Blob에 백업".

인터넷 연결이 없는 사이트 지원

NetApp Backup and Recovery 인터넷 연결이 없는 사이트(개인 모드 또는 다크 사이트라고도 함)에서 볼륨 데이터를 백업하는 데 사용할 수 있습니다. 이 경우, 동일한 사이트의 Linux 호스트에 콘솔 에이전트를 배포해야 합니다.

> BlueXP 개인 모드(레거시 BlueXP 인터페이스)는 일반적으로 인터넷 연결이 없고 AWS Secret Cloud, AWS Top Secret Cloud, Azure IL6를 포함하는 보안 클라우드 지역이 있는 온프레미스 환경에서 사용됩니다. NetApp 기존 BlueXP 인터페이스를 통해 이러한 환경을 계속 지원합니다. 레거시 BlueXP 인터페이스의 개인 모드 설명서는 다음을 참조하세요. "BlueXP 개인 모드에 대한 PDF 문서" .

- 로컬 온프레미스 ONTAP 시스템의 데이터를 로컬 NetApp StorageGRID 시스템으로 백업할 수 있습니다. "온프레미스 ONTAP 데이터를 StorageGRID 에 백업".
- 로컬 온프레미스 ONTAP 시스템의 데이터를 S3 개체 스토리지에 대해 구성된 로컬 온프레미스 ONTAP 시스템이나 Cloud Volumes ONTAP 시스템으로 백업할 수 있습니다. "온프레미스 ONTAP 데이터를 ONTAP S3에 백업".

NetApp Backup and Recovery 사용하여 ONTAP 볼륨에 대한 백업 정책 관리

NetApp Backup and Recovery 사용하면 NetApp 에서 제공하는 기본 백업 정책을 사용하여

백업을 만들거나 사용자 지정 정책을 만들 수 있습니다. 정책은 백업 빈도, 백업 시간, 보관되는 백업 파일 수를 관리합니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

활성화 마법사를 사용하여 볼륨의 백업 및 복구 서비스를 활성화하면 기본 정책과 시스템(Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템)에 이미 있는 다른 정책 중에서 선택할 수 있습니다. 기존 정책과 다른 정책을 사용하려면 활성화 마법사를 사용하기 전이나 사용하는 동안 정책을 만들 수 있습니다.

제공된 기본 백업 정책에 대해 알아보려면 다음을 참조하세요."보호 여정을 계획하세요" .

NetApp Backup and Recovery ONTAP 데이터에 대한 스냅샷, 복제, 개체 스토리지 백업의 세 가지 유형의 백업을 제공합니다. 해당 정책은 사용하는 아키텍처와 백업 유형에 따라 서로 다른 위치에 있습니다.

아키텍처	스냅샷 정책 저장 위치	복제 정책 저장 위치	개체 정책 저장 위치로 백업
팬아웃	주요한	반성	주요한
종속	주요한	반성	반성

환경, 기본 설정, 보호 유형에 따라 다음 도구를 사용하여 백업 정책을 만듭니다.

- NetApp Console UI
- 시스템 관리자 UI
- ONTAP CLI

시스템 관리자를 사용하는 경우 복제 정책의 정책 유형으로 *비동기*를 선택하고, 개체 백업 정책의 경우 *비동기*와 *클라우드에 백업*을 선택합니다.

시스템에 대한 정책 보기

1. 콘솔 UI에서 볼륨 > *백업 설정*을 선택합니다.
2. 백업 설정 페이지에서 시스템을 선택하고 *작업*을 선택합니다. ••• 아이콘을 클릭하고 *정책 관리*를 선택하세요.

   정책 관리 페이지가 나타납니다. 스냅샷 정책은 기본적으로 표시됩니다.

3. 시스템에 있는 다른 정책을 보려면 복제 정책 또는 *백업 정책*을 선택하세요. 기존 정책을 백업 계획에 사용할 수 있다면 준비가 완료된 것입니다. 다른 특성을 가진 정책이 필요한 경우 이 페이지에서 새로운 정책을 만들 수 있습니다.

정책 생성

스냅샷, 복제 및 개체 스토리지에 대한 백업을 관리하는 정책을 만들 수 있습니다.

- 스냅샷을 시작하기 전에 스냅샷 정책을 만듭니다.
- 복제를 시작하기 전에 복제 정책을 만듭니다.
- 백업을 시작하기 전에 개체 저장소에 대한 백업 정책을 만듭니다.

스냅샷을 시작하기 전에 스냅샷 정책을 만듭니다.

3-2-1 전략의 일부에는 기본 스토리지 시스템의 볼륨 스냅샷을 만드는 것이 포함됩니다.

정책 생성 프로세스에는 일정과 보존 기간을 나타내는 스냅샷 및 SnapMirror 레이블을 식별하는 작업이 포함됩니다. 미리 정의된 라벨을 사용하거나 직접 라벨을 만들 수 있습니다.

단계

1. 콘솔 UI에서 볼륨 > *백업 설정*을 선택합니다.
2. 백업 설정 페이지에서 시스템을 선택하고 *작업*을 선택합니다. ••• 아이콘을 클릭하고 *정책 관리*를 선택하세요.

   정책 관리 페이지가 나타납니다.

3. 정책 페이지에서 정책 만들기 > *스냅샷 정책 만들기*를 선택합니다.
4. 정책 이름을 지정합니다.
5. 스냅샷 일정을 선택하세요. 최대 5개의 라벨을 사용할 수 있습니다. 또는 일정을 만들어 보세요.
6. 일정을 만들기로 선택한 경우:
   a. 매시간, 매일, 매주, 매월 또는 매년 빈도를 선택하세요.
   b. 일정과 보존 기간을 나타내는 스냅샷 레이블을 지정합니다.
   c. 스냅샷을 언제, 얼마나 자주 찍을지 입력하세요.
   d. 보존: 보관할 스냅샷 수를 입력합니다.
7. *만들기*를 선택하세요.

계단식 아키텍처를 사용한 스냅샷 정책 예

이 예제에서는 두 개의 클러스터로 스냅샷 정책을 만듭니다.

1. 클러스터 1:
   a. 정책 페이지에서 클러스터 1을 선택합니다.
   b. 복제 및 개체 백업 정책 섹션을 무시합니다.
   c. 스냅샷 정책을 생성합니다.
2. 클러스터 2:
   a. 정책 페이지에서 클러스터 2를 선택합니다.
   b. 스냅샷 정책 섹션을 무시하세요.
   c. 개체 정책에 대한 복제 및 백업을 구성합니다.

복제를 시작하기 전에 복제 정책을 만듭니다.

3-2-1 전략에는 다른 스토리지 시스템에 볼륨을 복제하는 것이 포함될 수 있습니다. 복제 정책은 보조 스토리지 시스템에 있습니다.

단계

1. 정책 페이지에서 정책 만들기 > *복제 정책 만들기*를 선택합니다.

2. 정책 세부 정보 섹션에서 정책 이름을 지정합니다.
3. 각 레이블의 보존 기간을 나타내는 SnapMirror 레이블(최대 5개)을 지정합니다.
4. 환승 일정을 지정하세요.
5. *만들기*를 선택하세요.

백업을 시작하기 전에 개체 저장소에 대한 백업 정책을 만듭니다.

3-2-1 전략에는 볼륨을 개체 스토리지에 백업하는 것이 포함될 수 있습니다.

이 저장 정책은 백업 아키텍처에 따라 다른 저장 시스템 위치에 있습니다.

- 팬아웃: 기본 저장 시스템
- 캐스케이딩: 보조 저장 시스템

단계

1. 정책 관리 페이지에서 정책 만들기 > *백업 정책 만들기*를 선택합니다.
2. 정책 세부 정보 섹션에서 정책 이름을 지정합니다.
3. 각 레이블의 보존 기간을 나타내는 SnapMirror 레이블(최대 5개)을 지정합니다.
4. 전송 일정과 백업 보관 시기 등의 설정을 지정합니다.
5. (선택 사항) 특정 기간이 지난 후 오래된 백업 파일을 비용이 덜 드는 스토리지 클래스 또는 액세스 계층으로 이동하려면 보관 옵션을 선택하고 데이터가 보관되기까지 경과해야 하는 일수를 지정합니다. 백업 파일을 보관 저장소로 직접 보내려면 "보관 후 일수"에 *0*을 입력하세요.

   "보관 저장소 설정에 대해 자세히 알아보세요".

6. (선택 사항) 백업이 수정되거나 삭제되는 것을 방지하려면 **DataLock** 및 랜섬웨어 보호 옵션을 선택하세요.

   클러스터에서 ONTAP 9.11.1 이상을 사용하는 경우 *DataLock* 및 _랜섬웨어 보호_를 구성하여 백업이 삭제되지 않도록 보호할 수 있습니다.

   "사용 가능한 DataLock 설정에 대해 자세히 알아보세요.".

7. *만들기*를 선택하세요.

정책 편집

사용자 정의 스냅샷, 복제 또는 백업 정책을 편집할 수 있습니다.

백업 정책을 변경하면 해당 정책을 사용하는 모든 볼륨에 영향을 미칩니다.

단계

1. 정책 관리 페이지에서 정책을 선택하고 *작업*을 선택합니다. ••• 아이콘을 클릭하고 *정책 편집*을 선택하세요.

   복제 및 백업 정책의 프로세스는 동일합니다.

2. 정책 편집 페이지에서 변경 사항을 적용합니다.

3. *저장*을 선택하세요.

정책 삭제

볼륨과 연결되지 않은 정책은 삭제할 수 있습니다.

볼륨에 연결된 정책이 있고 해당 정책을 삭제하려면 먼저 볼륨에서 해당 정책을 제거해야 합니다.

단계

1. 정책 관리 페이지에서 정책을 선택하고 *작업*을 선택합니다. ••• 아이콘을 클릭하고 *스냅샷 정책 삭제*를 선택합니다.
2. *삭제*를 선택하세요.

더 많은 정보를 찾아보세요

System Manager 또는 ONTAP CLI를 사용하여 정책을 만드는 방법에 대한 지침은 다음을 참조하세요.

"시스템 관리자를 사용하여 스냅샷 정책 만들기" "ONTAP CLI를 사용하여 스냅샷 정책 만들기" "System Manager를 사용하여 복제 정책 만들기" "ONTAP CLI를 사용하여 복제 정책 생성" "System Manager를 사용하여 개체 스토리지 정책에 대한 백업을 만듭니다." "ONTAP CLI를 사용하여 개체 스토리지 정책에 대한 백업을 만듭니다."

NetApp Backup and Recovery 의 개체 백업 정책 옵션

NetApp Backup and Recovery 사용하면 온프레미스 ONTAP 및 Cloud Volumes ONTAP 시스템에 대한 다양한 설정으로 백업 정책을 만들 수 있습니다.

이러한 정책 설정은 개체 저장소 백업에만 적용됩니다. 이러한 설정은 스냅샷이나 복제 정책에 영향을 미치지 않습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

백업 일정 옵션

NetApp Backup and Recovery 사용하면 각 시스템(클러스터)에 대해 고유한 일정을 적용하여 여러 백업 정책을 만들 수 있습니다. 서로 다른 복구 지점 목표(RPO)를 가진 볼륨에 서로 다른 백업 정책을 할당할 수 있습니다.

각 백업 정책에는 백업 파일에 적용할 수 있는 레이블 및 보존 섹션이 제공됩니다. 볼륨에 적용된 스냅샷 정책은 NetApp Backup and Recovery 에서 인식하는 정책 중 하나여야 하며, 그렇지 않으면 백업 파일이 생성되지 않습니다.

일정에는 레이블과 보존 값의 두 부분이 있습니다.

- *레이블*은 볼륨에서 백업 파일이 생성(또는 업데이트)되는 빈도를 정의합니다. 다음 유형의 라벨 중에서 선택할 수 있습니다.
  - 시간별, 일별, 주별, 월별, 연간 기간 중 하나 또는 여러 기간을 조합하여 선택할 수 있습니다.
  - 3개월, 1년 또는 7년 동안 백업 및 보존을 제공하는 시스템 정의 정책 중 하나를 선택할 수 있습니다.
  - ONTAP System Manager나 ONTAP CLI를 사용하여 클러스터에서 사용자 정의 백업 보호 정책을 만든 경우

해당 정책 중 하나를 선택할 수 있습니다.

- 보존 값은 각 레이블(기간)에 대해 얼마나 많은 백업 파일을 보존할지 정의합니다. 카테고리나 간격에서 백업의 최대 수에 도달하면 오래된 백업이 제거되어 항상 최신 백업을 보유할 수 있습니다. 또한, 오래된 백업이 클라우드에서 더 이상 공간을 차지하지 않으므로 저장 비용도 절약됩니다.

예를 들어, 7개의 주간 백업과 12개의 월간 백업을 생성하는 백업 정책을 생성한다고 가정해 보겠습니다.

- 매주, 매월 볼륨에 대한 백업 파일이 생성됩니다.
- 8주차에 첫 번째 주간 백업이 제거되고 8주차의 새로운 주간 백업이 추가됩니다(최대 7개의 주간 백업 유지)
- 13번째 달에 첫 번째 월별 백업이 제거되고 13번째 달의 새로운 월별 백업이 추가됩니다(최대 12개의 월별 백업 유지)

연간 백업은 개체 스토리지로 전송된 후 소스 시스템에서 자동으로 삭제됩니다. 이러한 기본 동작은 시스템의 고급 설정 페이지에서 변경할 수 있습니다.

DataLock 및 랜섬웨어 보호 옵션

NetApp Backup and Recovery 볼륨 백업에 대한 DataLock 및 랜섬웨어 보호를 지원합니다. 이러한 기능을 사용하면 백업 파일을 잠그고 검사하여 백업 파일에 랜섬웨어가 있는지 감지할 수 있습니다. 이는 클러스터의 볼륨 백업에 대한 추가 보호가 필요할 때 백업 정책에서 정의할 수 있는 선택적 설정입니다.

이 두 가지 기능은 모두 백업 파일을 보호하여 랜섬웨어 공격 시도가 발생할 경우 항상 유효한 백업 파일에서 데이터를 복구할 수 있도록 합니다. 백업을 잠그고 일정 기간 동안 보관해야 하는 특정 규정 요구 사항을 충족하는 데도 도움이 됩니다. DataLock 및 랜섬웨어 복원력 옵션이 활성화되면 NetApp Backup and Recovery 활성화의 일부로 프로비저닝된 클라우드 버킷에서 개체 잠금 및 개체 버전 관리가 활성화됩니다.

이 기능은 소스 볼륨에 대한 보호 기능을 제공하지 않으며, 해당 소스 볼륨의 백업에만 보호 기능을 제공합니다. 일부를 사용하세요 "ONTAP 에서 제공하는 랜섬웨어 방지 보호" 소스 볼륨을 보호하세요.

- DataLock 및 랜섬웨어 보호 기능을 사용하려는 경우 첫 번째 백업 정책을 만들고 해당 클러스터에 대한 NetApp Backup and Recovery 활성화할 때 이를 활성화할 수 있습니다. 나중에 NetApp Backup and Recovery 고급 설정을 사용하여 랜섬웨어 검사를 활성화하거나 비활성화할 수 있습니다.
- 볼륨 데이터를 복원할 때 콘솔이 백업 파일에서 랜섬웨어를 검사하면 백업 파일의 내용에 액세스하기 위해 클라우드 공급자로부터 추가 퇴장 비용이 발생합니다.

DataLock이란 무엇입니까**?**

이 기능을 사용하면 SnapMirror 통해 클라우드에 복제된 클라우드 스냅샷을 잠글 수 있으며, 랜섬웨어 공격을 감지하고 객체 저장소에서 스냅샷의 일관된 복사본을 복구할 수 있습니다. 이 기능은 AWS, Azure, Google Cloud Platform 및 StorageGRID 에서 지원됩니다.

DataLock은 백업 파일이 일정 기간 동안 수정되거나 삭제되는 것을 방지합니다. 이를 _변경 불가능한 저장소_라고도 합니다. 이 기능은 "객체 잠금"을 위해 객체 스토리지 공급자의 기술을 사용합니다.

클라우드 제공자는 스냅샷 보존 기간을 기준으로 계산되는 보존 기간(RUD)을 사용합니다. 스냅샷 보존 기간은 백업 정책에 정의된 레이블과 보존 횟수를 기준으로 계산됩니다.

최소 스냅샷 보존 기간은 30일입니다. 이것이 어떻게 작동하는지 몇 가지 예를 살펴보겠습니다.

- 일일 라벨을 선택하고 보존 횟수를 20으로 설정하면 스냅샷 보존 기간은 20일이며, 최소값은 30일로 기본 설정됩니다.
- 주간 라벨을 선택하고 보존 횟수를 4로 설정하면 스냅샷 보존 기간은 28일이며, 최소값은 30일로 기본 설정됩니다.
- 월별 라벨을 선택하고 보존 횟수를 3으로 설정하면 스냅샷 보존 기간은 90일입니다.
- 연간 라벨을 선택하고 보존 횟수를 1로 설정하면 스냅샷 보존 기간은 365일이 됩니다.

보유기간**(RUD)**은 무엇이고**,** 어떻게 계산하나요**?**

보존 기간(RUD)은 스냅샷 보존 기간을 기준으로 결정됩니다. 보존 기간은 스냅샷 보존 기간과 버퍼를 합산하여 계산됩니다.

- 버퍼는 전송 시간 버퍼(3일) + 비용 최적화 버퍼(28일)로 총 31일이 됩니다.
- 최소 보존 기간은 30일 + 31일 버퍼 = 61일입니다.

다음은 몇 가지 예입니다.

- 12개의 보존 기간이 있는 월별 백업 일정을 만들면 백업은 삭제(다음 백업 파일로 대체)되기 전에 12개월(31일 추가) 동안 잠깁니다.
- 매일 30회, 매주 7회, 매월 12회의 백업을 생성하는 백업 정책을 만들면 3개의 잠긴 보존 기간이 있습니다.
  - "30일" 백업은 61일 동안 보관됩니다(30일 + 31일 버퍼).
  - "7주" 백업은 11주(7주 + 31일) 동안 보관됩니다.
  - "12개월" 백업은 12개월(31일 추가) 동안 보관됩니다.
- 24개의 보존 기간을 갖는 시간별 백업 일정을 생성하면 백업이 24시간 동안 잠겨 있다고 생각할 수 있습니다. 하지만 최소 기간인 30일보다 짧으므로 각 백업은 61일(30일 + 버퍼 기간 31일) 동안 잠겨 보관됩니다.

> DataLock 보존 기간이 만료되면 이전 백업은 삭제되지만, 백업 정책 보존 기간이 만료되면 삭제되지 않습니다.

DataLock 보존 설정은 백업 정책의 정책 보존 설정을 재정의합니다. 백업 파일이 더 오랜 기간 동안 개체 저장소에 저장되므로 저장 비용에 영향을 미칠 수 있습니다.

DataLock 및 랜섬웨어 보호 활성화

정책을 생성할 때 DataLock 및 랜섬웨어 보호 기능을 활성화할 수 있습니다. 정책이 생성된 후에는 이 기능을 활성화, 수정 또는 비활성화할 수 없습니다.

1. 정책을 생성할 때 **DataLock** 및 랜섬웨어 복원력 섹션을 확장합니다.
2. 다음 중 하나를 선택하세요.
   - 없음: DataLock 보호 및 랜섬웨어 복원력이 비활성화되었습니다.
   - 잠금 해제: DataLock 보호 및 랜섬웨어 복원력이 활성화되었습니다. 특정 권한이 있는 사용자는 보존 기간 동안 보호된 백업 파일을 덮어쓰거나 삭제할 수 있습니다.
   - 잠김: DataLock 보호 및 랜섬웨어 복원력이 활성화되었습니다. 보존 기간 동안 사용자는 보호된 백업 파일을 덮어쓰거나 삭제할 수 없습니다. 이는 규정을 완벽하게 준수하는 것입니다.

참조하다"고급 설정 페이지에서 랜섬웨어 보호 옵션을 업데이트하는 방법" .

랜섬웨어 보호란 무엇입니까**?**

랜섬웨어 보호 기능은 백업 파일을 검사하여 랜섬웨어 공격의 증거를 찾습니다. 랜섬웨어 공격 탐지는 체크섬 비교를 통해 수행됩니다. 이전 백업 파일이 아닌 새로운 백업 파일에서 잠재적인 랜섬웨어가 확인되면, 해당 새로운 백업 파일은 랜섬웨어 공격의 흔적이 없는 가장 최근의 백업 파일로 대체됩니다. (랜섬웨어 공격을 받은 것으로 확인된 파일은 교체된 후 1일 후에 삭제됩니다.)

스캔은 다음과 같은 상황에서 발생합니다.

- 클라우드 백업 객체에 대한 검사는 클라우드 객체 스토리지로 전송된 직후에 시작됩니다. 백업 파일이 클라우드 저장소에 처음 기록될 때 스캔이 수행되지 않고, 다음 백업 파일이 기록될 때 스캔이 수행됩니다.
- 랜섬웨어 검사는 복원 프로세스에 백업을 선택하면 시작될 수 있습니다.
- 언제든지 필요에 따라 스캔을 수행할 수 있습니다.

회수 과정은 어떻게 진행되나요**?**

랜섬웨어 공격이 감지되면 서비스는 Active Data Console 에이전트 Integrity Checker REST API를 사용하여 복구 프로세스를 시작합니다. 데이터 객체의 가장 오래된 버전이 진실의 원천이며 복구 프로세스의 일부로 현재 버전으로 만들어집니다.

이것이 어떻게 작동하는지 살펴보겠습니다.

- 랜섬웨어 공격이 발생하면 서비스는 버킷에 있는 객체를 덮어쓰거나 삭제하려고 시도합니다.
- 클라우드 스토리지는 버전 관리가 가능하므로 백업 개체의 새 버전이 자동으로 생성됩니다. 버전 관리가 켜진 상태에서 객체를 삭제하면 삭제된 것으로 표시되지만 여전히 검색할 수 있습니다. 객체를 덮어쓰면 이전 버전이 저장되고 표시됩니다.
- 랜섬웨어 검사가 시작되면 두 개체 버전에 대한 체크섬이 검증되고 비교됩니다. 체크섬이 일치하지 않으면 잠재적인 랜섬웨어가 감지된 것입니다.
- 복구 과정에는 마지막으로 알려진 양호한 사본으로 되돌리는 작업이 포함됩니다.

지원되는 시스템 및 개체 스토리지 공급자

다음 퍼블릭 및 프라이빗 클라우드 공급자의 개체 스토리지를 사용하는 경우 다음 시스템의 ONTAP 볼륨에서 DataLock 및 랜섬웨어 보호를 활성화할 수 있습니다.

소스 시스템	백업 파일 저장 위치
AWS의 Cloud Volumes ONTAP	아마존 S3
Azure의 Cloud Volumes ONTAP	Azure Blob
Google Cloud의 Cloud Volumes ONTAP	구글 클라우드
온프레미스 ONTAP 시스템	Amazon S3 Azure Blob Google Cloud NetApp StorageGRID

요구 사항

- AWS의 경우:
  - 클러스터는 ONTAP 9.11.1 이상을 실행해야 합니다.

- 콘솔 에이전트는 클라우드나 사내에 배포될 수 있습니다.
- 다음 S3 권한은 콘솔 에이전트에 권한을 제공하는 IAM 역할의 일부여야 합니다. 이들은 리소스 "arn:aws:s3:::netapp-backup-*"의 "backupS3Policy" 섹션에 있습니다.

  AWS S3 권한

  - s3:GetObjectVersionTagging
  - s3:GetBucketObjectLockConfiguration
  - s3:GetObjectVersionAcl
  - s3:PutObjectTagging
  - s3:객체 삭제
  - s3:객체태깅 삭제
  - s3:객체 보존 가져오기
  - s3:DeleteObjectVersionTagging
  - s3:객체 넣기
  - s3:객체 가져오기
  - s3:PutBucketObjectLock구성
  - s3:수명주기구성 가져오기
  - s3:버킷태깅 가져오기
  - s3:객체 버전 삭제
  - s3:리스트버킷버전
  - s3:리스트버킷
  - s3:PutBucket태깅
  - s3:객체태깅 가져오기
  - s3:PutBucketVersioning
  - s3:PutObjectVersionTagging
  - s3:버킷 버전 가져오기
  - s3:GetBucketAcl
  - s3:바이패스거버넌스보존
  - s3:객체 보존 넣기
  - s3:버킷 위치 가져오기
  - s3:객체 버전 가져오기

  "필요한 권한을 복사하여 붙여넣을 수 있는 정책에 대한 전체 JSON 형식을 확인하세요.".

- Azure의 경우:
  - 클러스터는 ONTAP 9.12.1 이상을 실행해야 합니다.

    - 콘솔 에이전트는 클라우드나 사내에 배포될 수 있습니다.
- Google Cloud의 경우:
    - 클러스터는 ONTAP 9.17.1 이상을 실행해야 합니다.
    - 콘솔 에이전트는 클라우드나 사내에 배포될 수 있습니다.
- StorageGRID 의 경우:
    - 클러스터는 ONTAP 9.11.1 이상을 실행해야 합니다.
    - StorageGRID 시스템은 11.6.0.3 이상을 실행해야 합니다.
    - 콘솔 에이전트는 귀하의 구내에 배포되어야 합니다(인터넷 접속이 가능한 사이트나 불가능한 사이트에 설치 가능)
    - 다음 S3 권한은 콘솔 에이전트에 권한을 제공하는 IAM 역할의 일부여야 합니다.

StorageGRID S3 권한

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:객체 삭제
- s3:객체태깅 삭제
- s3:객체 보존 가져오기
- s3:DeleteObjectVersionTagging
- s3:객체 넣기
- s3:객체 가져오기
- s3:PutBucketObjectLock구성
- s3:수명주기구성 가져오기
- s3:버킷태깅 가져오기
- s3:객체 버전 삭제
- s3:리스트버킷버전
- s3:리스트버킷
- s3:PutBucket태깅
- s3:객체태깅 가져오기
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:버킷 버전 가져오기
- s3:GetBucketAcl
- s3:객체 보존 넣기
- s3:버킷 위치 가져오기
- s3:객체 버전 가져오기

제한

- 백업 정책에서 보관 저장소를 구성한 경우 DataLock 및 랜섬웨어 보호 기능을 사용할 수 없습니다.
- NetApp Backup and Recovery 활성화할 때 선택하는 DataLock 옵션은 해당 클러스터의 모든 백업 정책에 사용해야 합니다.
- 단일 클러스터에서 여러 DataLock 모드를 사용할 수 없습니다.
- DataLock을 활성화하면 모든 볼륨 백업이 잠깁니다. 단일 클러스터에 대해 잠긴 볼륨 백업과 잠기지 않은 볼륨 백업을 혼합할 수 없습니다.
- DataLock 및 랜섬웨어 보호는 DataLock 및 랜섬웨어 보호가 활성화된 백업 정책을 사용하여 새 볼륨 백업에

적용할 수 있습니다. 나중에 고급 설정 옵션을 사용하여 이러한 기능을 활성화하거나 비활성화할 수 있습니다.

- FlexGroup 볼륨은 ONTAP 9.13.1 이상을 사용할 때만 DataLock 및 랜섬웨어 보호 기능을 사용할 수 있습니다.

DataLock 비용을 완화하는 방법에 대한 팁

DataLock 기능을 활성화한 상태에서 랜섬웨어 검사 기능을 활성화하거나 비활성화할 수 있습니다. 추가 요금을 피하려면 예약된 랜섬웨어 검사를 비활성화할 수 있습니다. 이를 통해 보안 설정을 사용자 정의하고 클라우드 제공업체로부터 비용이 발생하는 것을 방지할 수 있습니다.

예약된 랜섬웨어 검사가 비활성화된 경우에도 필요할 때 주문형 검사를 수행할 수 있습니다.

다양한 수준의 보호를 선택할 수 있습니다.

- 랜섬웨어 검사 없는 **DataLock**: 거버넌스 또는 규정 준수 모드에 있는 대상 저장소의 백업 데이터를 보호합니다.
  - 거버넌스 모드: 관리자가 보호된 데이터를 덮어쓰거나 삭제할 수 있는 유연성을 제공합니다.
  - 준수 모드: 보존 기간이 만료될 때까지 완전한 삭제 불가성을 제공합니다. 이는 엄격하게 규제되는 환경의 가장 엄격한 데이터 보안 요구 사항을 충족하는 데 도움이 됩니다. 데이터는 수명 주기 동안 덮어쓰거나 수정될 수 없으므로 백업 사본에 대한 가장 강력한 수준의 보호가 제공됩니다.

    Microsoft Azure는 대신 잠금 및 잠금 해제 모드를 사용합니다.

- 랜섬웨어 검사 기능이 있는 **DataLock**: 데이터에 대한 보안을 한층 더 강화합니다. 이 기능은 백업 사본을 변경하려는 시도를 감지하는 데 도움이 됩니다. 어떠한 시도가 이루어지면 데이터의 새로운 버전이 신중하게 생성됩니다. 검사 빈도는 1, 2, 3, 4, 5, 6, 7일로 변경할 수 있습니다. 검사 주기를 7일로 설정하면 비용이 상당히 줄어듭니다.

DataLock 비용을 완화하기 위한 추가 팁은 다음을 참조하세요.https://community.netapp.com/t5/Tech-ONTAP-Blogs/Understanding-NetApp-Backup-and-Recovery-DataLock-and-Ransomware-Feature-TCO/ba-p/453475[]

또한 DataLock과 관련된 비용에 대한 견적은 다음을 방문하여 얻을 수 있습니다. "NetApp Backup and Recovery 총소유비용(TCO) 계산기" .

보관 저장 옵션

AWS, Azure 또는 Google 클라우드 스토리지를 사용하는 경우 특정 기간이 지나면 오래된 백업 파일을 비용이 덜 드는 보관 스토리지 클래스 또는 액세스 계층으로 옮길 수 있습니다. 표준 클라우드 저장소에 쓰지 않고도 백업 파일을 즉시 보관 저장소로 보내도록 선택할 수도 있습니다. 백업 파일을 보관 저장소로 직접 보내려면 "보관 후 일수"에 *0*을 입력하세요. 이 기능은 클라우드 백업 데이터에 거의 액세스할 필요가 없는 사용자나 테이프 백업 솔루션을 교체하는 사용자에게 특히 유용할 수 있습니다.

보관 계층의 데이터는 필요할 때 즉시 액세스할 수 없으며 검색 비용이 더 많이 들기 때문에 백업 파일을 보관하기로 결정하기 전에 백업 파일에서 데이터를 복원해야 하는 빈도를 고려해야 합니다.

- 모든 데이터 블록을 보관 클라우드 스토리지로 보내도록 "0"을 선택하더라도 메타데이터 블록은 항상 표준 클라우드 스토리지에 기록됩니다.
- DataLock을 활성화한 경우 보관 저장소를 사용할 수 없습니다.
- *0*일(즉시 보관)을 선택한 후에는 보관 정책을 변경할 수 없습니다.

각 백업 정책은 백업 파일에 적용할 수 있는 보관 정책 섹션을 제공합니다.

- AWS에서 백업은 *Standard* 스토리지 클래스에서 시작하여 30일 후에 *Standard-Infrequent Access* 스토리지 클래스로 전환됩니다.

  클러스터가 ONTAP 9.10.1 이상을 사용하는 경우 이전 백업을 *S3 Glacier* 또는 *S3 Glacier Deep Archive* 스토리지로 계층화할 수 있습니다. "AWS 보관 스토리지에 대해 자세히 알아보세요".

  - NetApp Backup and Recovery 활성화할 때 첫 번째 백업 정책에서 보관 계층을 선택하지 않으면 _S3 Glacier_가 향후 정책에 대한 유일한 보관 옵션이 됩니다.
  - 첫 번째 백업 정책에서 *S3 Glacier_*를 선택하면 해당 클러스터의 향후 백업 정책에 대해 *_S3 Glacier Deep Archive* 계층으로 변경할 수 있습니다.
  - 첫 번째 백업 정책에서 _S3 Glacier Deep Archive_를 선택하면 해당 계층은 해당 클러스터의 향후 백업 정책에 사용할 수 있는 유일한 아카이브 계층이 됩니다.
- Azure에서 백업은 *Cool* 액세스 계층과 연결됩니다.

  클러스터가 ONTAP 9.10.1 이상을 사용하는 경우 이전 백업을 *Azure Archive* 저장소로 계층화할 수 있습니다. "Azure 보관 저장소에 대해 자세히 알아보세요".

- GCP에서 백업은 *Standard* 스토리지 클래스와 연결됩니다.

  온프레미스 클러스터에서 ONTAP 9.12.1 이상을 사용하는 경우, NetApp Backup and Recovery UI에서 특정 기간 후에 이전 백업을 아카이브 스토리지로 계층화하여 비용을 더욱 최적화할 수 있습니다. "Google 보관 저장소에 대해 자세히 알아보세요".

- StorageGRID 에서 백업은 *Standard* 스토리지 클래스와 연결됩니다.

  온프레미스 클러스터에서 ONTAP 9.12.1 이상을 사용하고 StorageGRID 시스템에서 11.4 이상을 사용하는 경우 이전 백업 파일을 퍼블릭 클라우드 보관 스토리지에 보관할 수 있습니다.

  - AWS의 경우, AWS *S3 Glacier* 또는 *S3 Glacier Deep Archive* 스토리지로 백업을 계층화할 수 있습니다. "AWS 보관 스토리지에 대해 자세히 알아보세요".
  - Azure의 경우, 오래된 백업을 Azure Archive 스토리지로 계층화할 수 있습니다. "Azure 보관 저장소에 대해 자세히 알아보세요".

NetApp Backup and Recovery 고급 설정에서 개체 스토리지 백업 옵션 관리

고급 설정 페이지를 사용하여 각 ONTAP 시스템에 대해 NetApp Backup and Recovery 활성화할 때 설정한 클러스터 수준의 개체 스토리지 백업 설정을 변경할 수 있습니다. "기본" 백업 설정으로 적용되는 일부 설정을 수정할 수도 있습니다. 여기에는 백업의 개체 스토리지 전송 속도 변경, 과거 스냅샷을 백업 파일로 내보낼지 여부, 시스템에 대한 랜섬웨어 검사를 활성화 또는 비활성화하는 것이 포함됩니다.

이러한 설정은 백업-객체 저장소에만 사용할 수 있습니다. 이러한 설정은 스냅샷이나 복제 설정에 영향을 미치지 않습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

고급 설정 페이지에서 다음 옵션을 변경할 수 있습니다.

- ONTAP 시스템이 객체 스토리지에 액세스할 수 있도록 하는 스토리지 키 변경
- 객체 스토리지에 연결된 ONTAP IPspace 변경
- 최대 전송 속도 옵션을 사용하여 객체 스토리지에 백업을 업로드하는 데 할당되는 네트워크 대역폭을 변경합니다.
- 과거 스냅샷을 백업 파일로 내보내고 향후 볼륨의 초기 기준 백업 파일에 포함할지 여부를 변경합니다.
- "연간" 스냅샷이 소스 시스템에서 제거되는지 여부 변경
- 예약된 검사를 포함하여 시스템에 대한 랜섬웨어 검사 활성화 또는 비활성화

클러스터 수준 백업 설정 보기

클러스터 수준 시스템 설정과 각 시스템의 공급자 설정을 볼 수 있습니다.

단계

1. 콘솔 메뉴에서 *보호 > 백업 및 복구*를 선택합니다.
2. 볼륨 탭에서 *백업 설정*을 선택합니다.
3. _백업 설정 페이지_에서 다음을 선택하세요. ••• 시스템의 경우 *고급 설정 구성 > 시스템 설정*을 선택하여 시스템 설정을 보고, *고급 설정 구성 > 공급자 설정*을 선택하여 공급자 설정을 볼 수 있습니다.

   결과 페이지에는 해당 시스템의 현재 설정이 표시됩니다. 공급자 설정을 볼 때 표시되는 공급자 설정은 페이지 상단에서 선택한 버킷과 관련된 설정입니다.

참고로, 일부 옵션은 소스 클러스터의 ONTAP 버전과 백업이 저장되는 클라우드 공급자 대상에 따라 사용 불가능할 수 있습니다.

백업을 개체 스토리지에 업로드하는 데 사용 가능한 네트워크 대역폭을 변경합니다.

시스템에 대해 NetApp Backup and Recovery 활성화하면 기본적으로 ONTAP 무제한의 대역폭을 사용하여 시스템 볼륨의 백업 데이터를 개체 스토리지로 전송할 수 있습니다. 백업 트래픽이 일반 사용자 작업 부하에 영향을 미치는 경우 고급 설정 페이지에서 최대 전송 속도 옵션을 사용하여 전송 중에 사용되는 네트워크 대역폭 양을 조절할 수 있습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 클릭하세요. ••• 시스템의 경우 *고급 설정 구성 > 시스템 설정*을 선택하십시오.
3. 고급 설정 페이지에서 최대 전송 속도 섹션을 확장합니다.
4. 최대 전송 속도로 1~1,000Mbps 사이의 값을 선택하세요.
5. 제한됨 라디오 버튼을 선택하고 사용 가능한 최대 대역폭을 입력하거나, *무제한*을 선택하여 제한이 없음을 나타냅니다.
6. *적용*을 선택하세요.

이 설정은 시스템의 볼륨에 대해 구성될 수 있는 다른 복제 관계에 할당된 대역폭에는 영향을 미치지 않습니다.

과거 스냅샷을 백업 파일로 내보낼지 여부를 변경합니다.

이 시스템에서 사용하는 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 볼륨에 대한 로컬 스냅샷이 있는 경우 해당 기록 스냅샷을 백업 파일로 개체 스토리지에 내보낼 수 있습니다. 이를 통해 이전 스냅샷을 기준 백업 사본으로 이동하여 클라우드에서 백업을 초기화할 수 있습니다.

이 옵션은 새 읽기/쓰기 볼륨의 새 백업 파일에만 적용되며, 데이터 보호(DP) 볼륨에서는 지원되지 않습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 클릭하세요. ••• 시스템의 경우 *고급 설정 구성 > 시스템 설정*을 선택하십시오.
3. 고급 설정 페이지에서 기존 스냅샷 복사본 내보내기 섹션을 확장합니다.
4. 기존 스냅샷을 내보낼지 여부를 선택하세요.
5. *적용*을 선택하세요.

"연간" 스냅샷이 소스 시스템에서 제거되는지 여부를 변경합니다.

볼륨의 백업 정책에 대해 "연간" 백업 레이블을 선택하면 생성되는 스냅샷의 크기가 매우 커집니다. 기본적으로 이러한 연간 스냅샷은 개체 스토리지로 전송된 후 소스 시스템에서 자동으로 삭제됩니다. 연간 스냅샷 삭제 섹션에서 이 기본 동작을 변경할 수 있습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 클릭하세요. ••• 시스템의 경우 *고급 설정 구성 > 시스템 설정*을 선택하십시오.
3. 고급 설정 페이지에서 연간 스냅샷 삭제 섹션을 확장합니다.
4. 소스 시스템에서 연간 스냅샷을 유지하려면 *비활성화*를 선택합니다.
5. *적용*을 선택하세요.

랜섬웨어 검사 활성화 또는 비활성화

랜섬웨어 보호 검사는 기본적으로 활성화되어 있습니다. 검사 빈도의 기본 설정은 7일입니다. 스캔은 최신 스냅샷에서만 수행됩니다.

DataLock 및 랜섬웨어 복원력 옵션에 대한 자세한 내용은 다음을 참조하세요."DataLock 및 랜섬웨어 복원력 옵션" .

일정을 며칠이나 몇 주로 변경하거나 비활성화하여 비용을 절감할 수 있습니다.

랜섬웨어 검사를 활성화하면 클라우드 제공업체에 따라 추가 요금이 부과됩니다.

예약된 랜섬웨어 검사가 비활성화된 경우에도 주문형 검사를 수행할 수 있으며 복원 작업 중에도 검사가 계속 진행됩니다.

참조하다"정책 관리" 랜섬웨어 탐지를 구현하는 정책 관리에 대한 자세한 내용은 다음을 참조하세요.

시스템에 대한 랜섬웨어 검사를 활성화 또는 비활성화합니다.

클러스터에 대한 랜섬웨어 검사를 활성화 또는 비활성화할 수 있습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 클릭하세요. ••• 시스템의 경우 *고급 설정 구성 > 시스템 설정*을 선택하십시오.
3. 다음 페이지에서 랜섬웨어 검사 섹션을 펼치십시오.
4. 랜섬웨어 검사를 활성화하거나 비활성화합니다.
5. *예약된 랜섬웨어 검사*를 선택하세요.
6. 선택적으로, 기본 스캔 주기를 매주 또는 며칠 또는 몇 주로 변경할 수 있습니다.
7. 검사를 실행할 빈도를 일 또는 주 단위로 설정합니다.
8. *적용*을 선택하세요.

공급자에 대한 랜섬웨어 검사를 활성화 또는 비활성화합니다.

공급자 설정 페이지를 사용하여 공급자 수준에서 랜섬웨어 검사를 활성화 또는 비활성화할 수 있습니다. 이 페이지의 설정은 페이지 상단에서 선택한 버킷과 관련이 있습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 다음을 클릭하세요. ••• 시스템에서 *고급 설정 구성 > 공급자 설정*을 선택합니다.
3. 결과 페이지 상단에서 설정을 변경해야 하는 버킷을 선택하십시오.
4. 랜섬웨어 검사 섹션을 펼치세요.
5. 랜섬웨어 검사를 활성화하거나 비활성화합니다.
6. *예약된 랜섬웨어 검사*를 선택하세요.
7. 선택적으로, 기본 스캔 주기를 매주 또는 며칠 또는 몇 주로 변경할 수 있습니다.
8. 검사를 실행할 빈도를 일 또는 주 단위로 설정합니다.
9. *적용*을 선택하세요.

NetApp Backup and Recovery 사용하여 Cloud Volumes ONTAP 데이터를 Amazon S3에 백업합니다.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 Cloud Volumes ONTAP 시스템에서 Amazon S3로 볼륨 데이터 백업을 시작하세요.

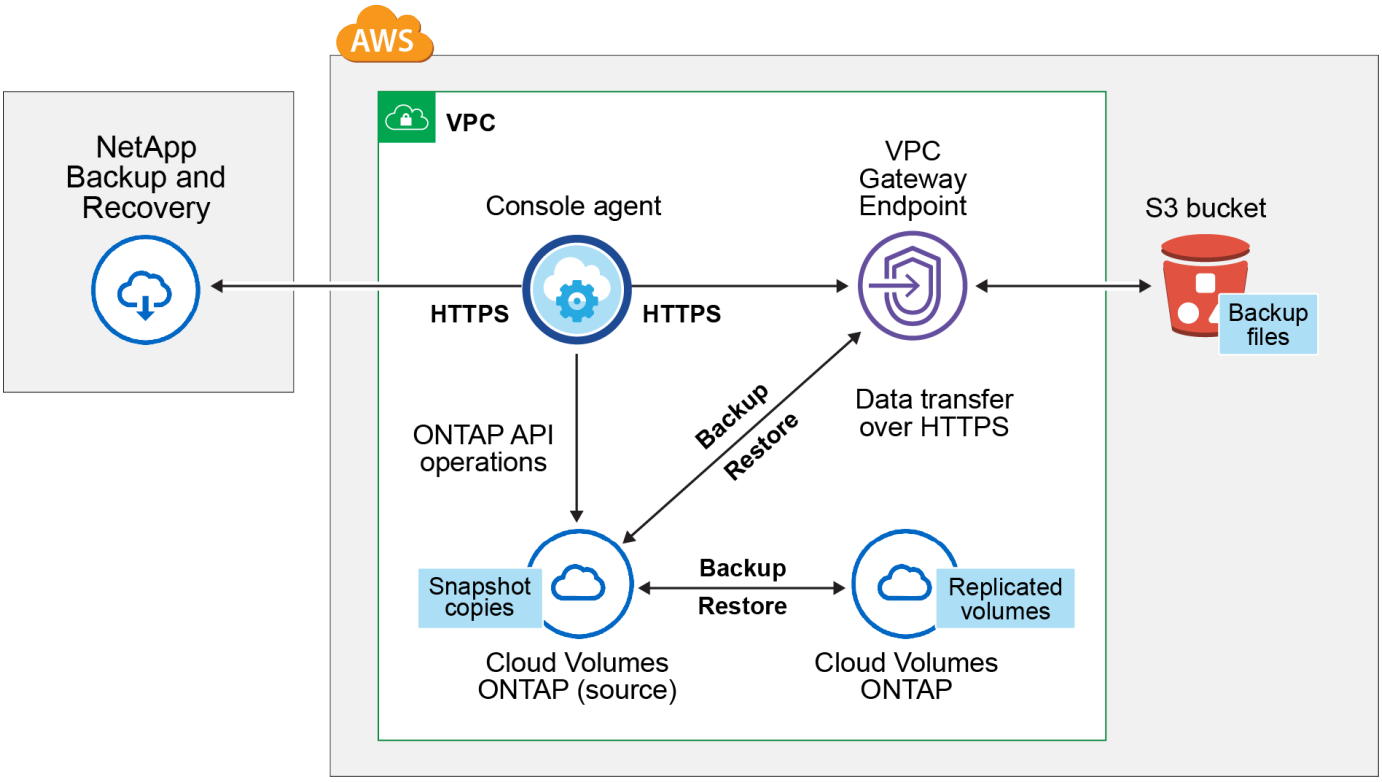
NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

구성에 대한 지원을 확인하세요

S3에 볼륨 백업을 시작하기 전에 지원되는 구성이 있는지 확인하려면 다음 요구 사항을 읽어보세요.

다음 이미지는 각 구성 요소와 구성 요소 간에 준비해야 할 연결을 보여줍니다.

선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.



VPC 게이트웨이 엔드포인트는 이미 VPC에 존재해야 합니다. "게이트웨이 엔드포인트에 대해 자세히 알아보세요" .

지원되는 **ONTAP** 버전

최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.

데이터 암호화를 위한 고객 관리 키 사용에 필요한 정보

기본 Amazon S3 암호화 키를 사용하는 대신, 활성화 마법사에서 데이터 암호화를 위한 고객 관리 키를 직접 선택할 수 있습니다. 이 경우에는 암호화 관리 키가 이미 설정되어 있어야 합니다. "자신의 키를 사용하는 방법을 확인하세요" .

라이센스 요구 사항 확인

NetApp Backup and Recovery PAYGO 라이선스의 경우 AWS Marketplace에서 Cloud Volumes ONTAP 및 NetApp Backup and Recovery 배포할 수 있는 콘솔 구독을 이용할 수 있습니다. 당신은 필요합니다 "이 NetApp Console 구독을 구독하세요" NetApp Backup and Recovery 활성화하기 전에. NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다.

Cloud Volumes ONTAP 데이터와 온프레미스 ONTAP 데이터를 모두 백업할 수 있는 연간 계약의 경우 다음에서 구독해야 합니다. "AWS Marketplace 페이지" 그런 다음 "구독을 AWS 자격 증명과 연결합니다." .

Cloud Volumes ONTAP 과 NetApp Backup and Recovery 묶을 수 있는 연간 계약의 경우 Cloud Volumes ONTAP

시스템을 생성할 때 연간 계약을 설정해야 합니다. 이 옵션을 사용하면 온프레미스 데이터를 백업할 수 없습니다.

NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요". 콘솔 에이전트와 Cloud Volumes ONTAP 시스템이 다크 사이트에 배포되는 경우 BYOL 라이선스를 사용해야 합니다.

백업이 저장될 저장 공간에 대한 AWS 계정이 필요합니다.

콘솔 에이전트를 준비하세요

콘솔 에이전트는 전체 또는 제한된 인터넷 액세스("표준" 또는 "제한" 모드)가 가능한 AWS 지역에 설치해야 합니다. "자세한 내용은 NetApp Console 배포 모드를 참조하세요." .

- "콘솔 에이전트에 대해 알아보세요"
- "AWS에 표준 모드(전체 인터넷 액세스)로 콘솔 에이전트 배포"
- "제한 모드(아웃바운드 액세스 제한)로 콘솔 에이전트 설치"

콘솔 에이전트에 대한 권한을 확인하거나 추가합니다.

콘솔에 권한을 제공하는 IAM 역할에는 최신 S3 권한이 포함되어야 합니다. "콘솔 정책" . 정책에 이러한 모든 권한이 포함되어 있지 않으면 다음을 참조하세요. "AWS 설명서: IAM 정책 편집" .

해당 정책의 구체적인 권한은 다음과 같습니다.

```
{
  "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:PutBucketPolicy",
    "s3:PutBucketOwnershipControls",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutEncryptionConfiguration",
    "s3:GetObjectVersionTagging",
    "s3:GetBucketObjectLockConfiguration",
    "s3:GetObjectVersionAcl",
    "s3:PutObjectTagging",
    "s3:DeleteObjectTagging",
    "s3:GetObjectRetention",
    "s3:DeleteObjectVersionTagging",
    "s3:PutBucketObjectLockConfiguration",
    "s3:DeleteObjectVersion",
    "s3:GetObjectTagging",
    "s3:PutBucketVersioning",
    "s3:PutObjectVersionTagging",
    "s3:GetBucketVersioning",
    "s3:BypassGovernanceRetention",
    "s3:PutObjectRetention",
    "s3:GetObjectVersion",
    "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-*"
        ]
    }
```

AWS 중국 리전에서 백업을 생성할 때 IAM 정책의 모든 *Resource* 섹션 아래에 있는 AWS 리소스 이름 "arn"을 "aws"에서 "aws-cn"으로 변경해야 합니다. 예를 들어, `arn:aws-cn:s3:::netapp-backup-*` .

필수 **AWS Cloud Volumes ONTAP** 권한

Cloud Volumes ONTAP 시스템에서 ONTAP 9.12.1 이상 소프트웨어를 실행하는 경우 해당 시스템에 권한을 제공하는 IAM 역할에는 최신 버전의 NetApp Backup and Recovery 위한 새로운 S3 권한 세트가 포함되어야 합니다. "Cloud Volumes ONTAP 정책" .

콘솔 버전 3.9.23 이상을 사용하여 Cloud Volumes ONTAP 시스템을 만든 경우 이러한 권한은 이미 IAM 역할의 일부여야 합니다. 그렇지 않으면 누락된 권한을 추가해야 합니다.

지원되는 **AWS** 지역

NetApp Backup and Recovery AWS GovCloud 지역을 포함한 모든 AWS 지역에서 지원됩니다.

다른 **AWS** 계정에서 백업을 생성하기 위한 필수 설정

기본적으로 백업은 Cloud Volumes ONTAP 시스템에 사용된 계정과 동일한 계정을 사용하여 생성됩니다. 백업에 다른 AWS 계정을 사용하려면 다음을 수행해야 합니다.

- "s3:PutBucketPolicy" 및 "s3:PutBucketOwnershipControls" 권한이 콘솔 에이전트에 권한을 제공하는 IAM 역할의 일부인지 확인하세요.
- 콘솔에 대상 AWS 계정 자격 증명을 추가합니다. "이 작업을 수행하는 방법을 확인하세요" .
- 두 번째 계정의 사용자 자격 증명에 다음 권한을 추가합니다.

```
"athena:StartQueryExecution",
"athena:GetQueryResults",
"athena:GetQueryExecution",
"glue:GetDatabase",
"glue:GetTable",
"glue:CreateTable",
"glue:CreateDatabase",
"glue:GetPartitions",
"glue:BatchCreatePartition",
"glue:BatchDeletePartition"
```

나만의 버킷을 만들어보세요

기본적으로 서비스는 사용자를 위해 버킷을 생성합니다. 자신의 버킷을 사용하려면 백업 활성화 마법사를 시작하기 전에 버킷을 만든 다음 마법사에서 해당 버킷을 선택하면 됩니다.

"나만의 버킷을 만드는 방법에 대해 자세히 알아보세요".

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.
- 서로 다른 서브넷에 있는 두 개의 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 서브넷을 함께 라우팅해야 합니다(이는 기본 설정입니다).

Cloud Volumes ONTAP 에서 **NetApp Backup and Recovery** 활성화

NetApp Backup and Recovery 활성화하는 것은 쉽습니다. 단계는 기존 Cloud Volumes ONTAP 시스템이 있는지 아니면 새 시스템이 있는지에 따라 약간씩 다릅니다.

새 시스템에서 **NetApp Backup and Recovery** 활성화

NetApp Backup and Recovery 시스템 마법사에서 기본적으로 활성화되어 있습니다. 해당 옵션을 활성화해 두세요.

보다 "AWS에서 Cloud Volumes ONTAP 출시" Cloud Volumes ONTAP 시스템을 만드는 데 필요한 요구 사항과 세부 정보를 확인하세요.

단계

1. 콘솔의 시스템 페이지에서 *시스템 추가*를 선택하고, 클라우드 공급자를 선택한 다음 *새로 추가*를 선택합니다. * Cloud Volumes ONTAP 만들기*를 선택합니다.
2. 클라우드 공급자로 *Amazon Web Services*를 선택한 다음 단일 노드 또는 HA 시스템을 선택합니다.
3. 세부 정보 및 자격 증명 페이지를 작성하세요.
4. 서비스 페이지에서 서비스를 활성화한 상태로 두고 *계속*을 선택합니다.
5. 마법사의 페이지를 완료하여 시스템을 배포합니다.

결과

시스템에서 NetApp Backup and Recovery 활성화되어 있습니다. 이러한 Cloud Volumes ONTAP 시스템에서 볼륨을 생성한 후 NetApp Backup and Recovery 실행하세요."보호하려는 각 볼륨에서 백업을 활성화합니다." .

기존 시스템에서 **NetApp Backup and Recovery** 활성화

콘솔에서 언제든지 기존 시스템에서 NetApp Backup and Recovery 활성화할 수 있습니다.

단계

1. 콘솔의 시스템 페이지에서 클러스터를 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화*를 선택합니다.

   백업을 위한 Amazon S3 대상이 시스템 페이지에 클러스터로 존재하는 경우, 클러스터를 Amazon S3 시스템으로 끌어서 놓으면 설정 마법사가 시작됩니다.

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

   - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

     백업을 위한 AWS 대상이 콘솔의 시스템 페이지에 시스템으로 존재하는 경우 ONTAP 클러스터를 AWS 개체 스토리지로 끌어올 수 있습니다.

◦ 백업 및 복구 메뉴에서 *볼륨*을 선택하세요. 볼륨 탭에서 *작업*을 선택합니다. ••• 아이콘 옵션을 선택하고 (복제 또는 객체 스토리지 백업이 이미 활성화되지 않은) 단일 볼륨에 대해 *3-2-1 보호 활성화*를 선택합니다.

마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
   ◦ 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
   ◦ 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
   ◦ 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
   ◦ 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
   ◦ 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
   - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
   - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
   - 백업: 볼륨을 객체 스토리지에 백업합니다. 기존 버킷을 선택하거나 새 버킷을 구성할 때 클러스터당 최대 6개의 버킷에 볼륨을 백업할 수 있습니다.
2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   - 계단식: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 보조 스토리지에서 개체 스토리지로 흐릅니다.
   - 팬아웃: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

     이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새 정책을 만듭니다.

   스냅샷을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

   정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

   a. 정책의 이름을 입력하세요.
   b. 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
   c. *만들기*를 선택하세요.
4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 스토리지 VM을 선택하십시오. 선택적으로 복제된 볼륨 이름에 추가될 대상 애그리게이트 또는 애그리게이트들을 선택하고 접두사 또는 접미사를 지정할 수 있습니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새로 만듭니다.

     사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     i. 정책의 이름을 입력하세요.
     ii. 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     iii. *만들기*를 선택하세요.
5. 백업: 다음 옵션을 설정하세요.
   - 공급자: *Amazon Web Services*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보와 백업이 저장될 지역을 입력하세요.

     백업을 저장하는 데 사용되는 AWS 계정을 입력하세요. 이는 Cloud Volumes ONTAP 시스템이 있는 계정과 다를 수 있습니다.

     백업에 다른 AWS 계정을 사용하려면 콘솔에서 대상 AWS 계정 자격 증명을 추가하고 콘솔에 권한을 제공하는

IAM 역할에 "s3:PutBucketPolicy" 및 "s3:PutBucketOwnershipControls" 권한을 추가해야 합니다.

백업이 저장될 지역을 선택하세요. 이는 Cloud Volumes ONTAP 시스템이 있는 지역과 다른 지역일 수 있습니다.

새로운 버킷을 만들거나 기존 버킷을 선택하세요.

- 암호화: 새 버킷을 생성한 경우 공급자로부터 받은 암호화 키 정보를 입력하십시오. 데이터 암호화를 관리할 때 기본 AWS 암호화 키를 사용할지, 아니면 AWS 계정에서 직접 관리하는 고객 키를 사용할지 선택하세요. ("자신의 암호화 키를 사용하는 방법을 확인하세요").

  고객이 직접 관리하는 키를 사용하기로 선택한 경우 키 보관소와 키 정보를 입력하세요.

  기존 버킷을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

- 네트워킹: 이 공급자에 대한 네트워킹 옵션을 구성합니다.
- 백업 정책: 기존의 백업-객체 스토리지 정책을 선택하거나 새로 만듭니다.

  백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

  정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

  i. 정책의 이름을 입력하세요.

  ii. 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.

  iii. 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .

  iv. *만들기*를 선택하세요.

- 기존 스냅샷 내보내기: 이 시스템의 볼륨에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 로컬 스냅샷이 있는 경우 이 추가 메시지가 표시됩니다. 볼륨을 가장 완벽하게 보호하기 위해 모든 과거 스냅샷을 백업 파일로 객체 스토리지에 복사하려면 이 확인란을 선택하십시오.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 *로컬 스냅샷, 복제 및 백업에서 일치하지 않는 레이블을 자동으로 수정*할 수 있습니다. 이렇게 하면 스냅샷, 복제 및 백업 정책의 레이블과 일치하는 레이블이 지정된 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 스토리지 시스템 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 저장소 볼륨과 동기화됩니다.

입력한 S3 액세스 키와 비밀 키로 지정된 서비스 계정에 S3 버킷이 생성되고, 백업 파일이 해당 버킷에 저장됩니다.

볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 사용하여 Cloud Volumes ONTAP 데이터를 Azure Blob 스토리지에 백업합니다.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 Cloud Volumes ONTAP 시스템에서 Azure Blob 스토리지로 볼륨 데이터를 백업하세요.

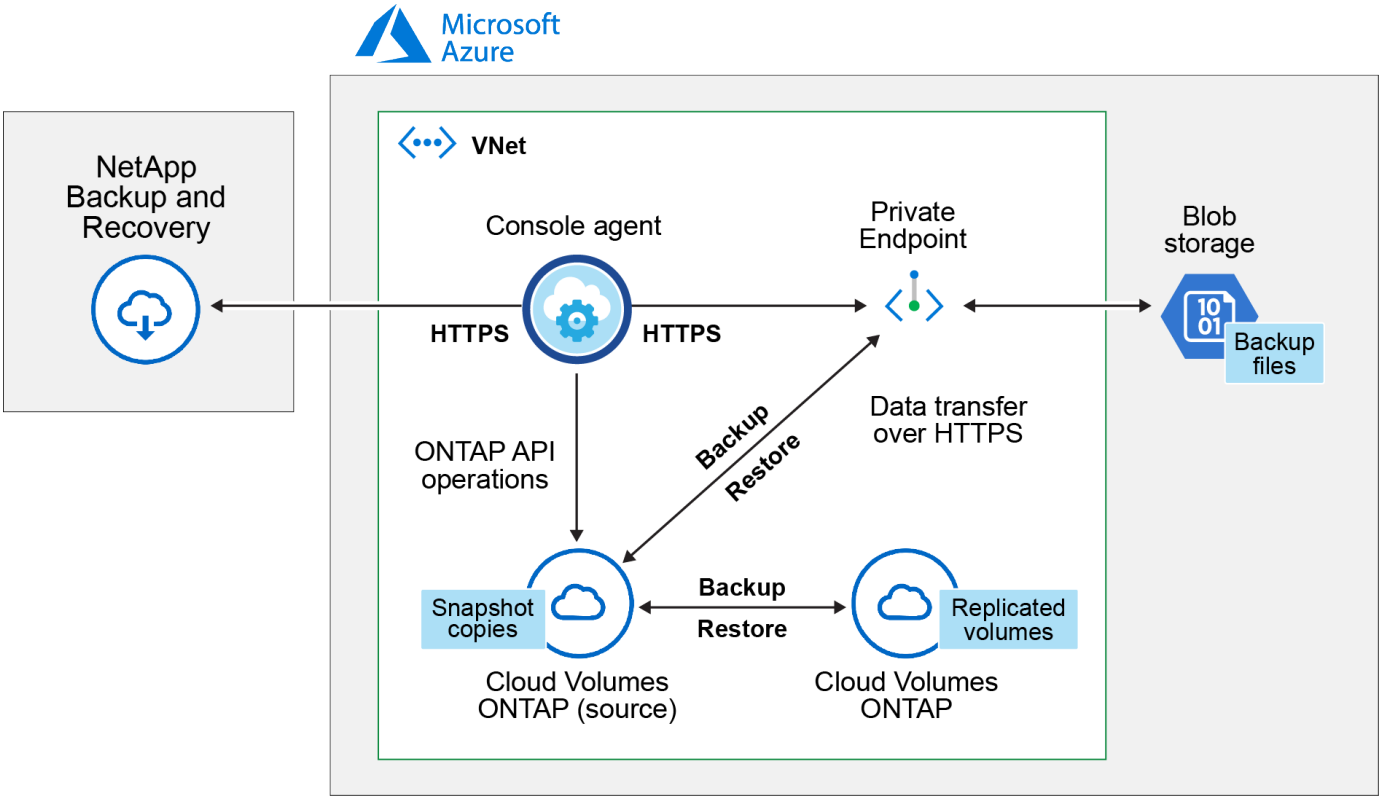
NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

구성에 대한 지원을 확인하세요

Azure Blob 저장소에 볼륨을 백업하기 전에 지원되는 구성이 있는지 확인하려면 다음 요구 사항을 읽어보세요.

다음 이미지는 각 구성 요소와 구성 요소 간에 준비해야 할 연결을 보여줍니다.

선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.



지원되는 **ONTAP** 버전

최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.

지원되는 **Azure** 지역

NetApp Backup and Recovery Azure Government 지역을 포함한 모든 Azure 지역에서 지원됩니다.

기본적으로 NetApp Backup and Recovery 비용 최적화를 위해 로컬 중복성(LRS)을 사용하여 Blob 컨테이너를 프로비저닝합니다. NetApp Backup and Recovery 활성화한 후 데이터가 서로 다른 영역 간에 복제되도록 하려면 이 설정을 영역 중복성(ZRS)으로 변경할 수 있습니다. Microsoft 지침을 참조하세요. "저장소 계정 복제 방식 변경" .

다른 **Azure** 구독에서 백업을 만드는 데 필요한 설정

기본적으로 백업은 Cloud Volumes ONTAP 시스템에 사용된 것과 동일한 구독을 사용하여 생성됩니다.

라이센스 요구 사항 확인

NetApp Backup and Recovery PAYGO 라이선싱의 경우 NetApp Backup and Recovery 활성화하기 전에 Azure Marketplace를 통해 구독해야 합니다. NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다. "시스템 마법사의 세부 정보 및 자격 증명 페이지에서 구독할 수 있습니다." .

NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요". 콘솔 에이전트와 Cloud Volumes ONTAP 시스템이 다크 사이트("비공개 모드")에 배포되는 경우 BYOL 라이선스를 사용해야 합니다.

백업이 저장될 저장 공간에 대한 Microsoft Azure 구독이 필요합니다.

콘솔 에이전트를 준비하세요

콘솔 에이전트는 전체 또는 제한된 인터넷 액세스("표준" 또는 "제한" 모드)가 가능한 Azure 지역에 설치할 수 있습니다.

"자세한 내용은 NetApp Console 배포 모드를 참조하세요." .

- "콘솔 에이전트에 대해 알아보세요"
- "Azure에서 표준 모드(전체 인터넷 액세스)로 콘솔 에이전트 배포"
- "제한 모드(아웃바운드 액세스 제한)로 콘솔 에이전트 설치"

콘솔 에이전트에 대한 권한을 확인하거나 추가합니다.

NetApp Backup and Recovery 검색 및 복원 기능을 사용하려면 콘솔 에이전트 역할에 대한 특정 권한이 있어야 Azure Synapse Workspace 및 Data Lake Storage 계정에 액세스할 수 있습니다. 아래의 권한을 확인하고, 정책을 수정해야 하는 경우 단계에 따라 진행하세요.

시작하기 전에

- 구독을 통해 Azure Synapse Analytics 리소스 공급자("Microsoft.Synapse")를 등록해야 합니다. "구독을 위해 이 리소스 공급자를 등록하는 방법을 확인하세요." . 리소스 공급자를 등록하려면 구독 소유자 또는 *기여자*여야 합니다.
- 콘솔 에이전트와 Azure Synapse SQL 서비스 간 통신을 위해서는 포트 1433이 열려 있어야 합니다.

단계

1. 콘솔 에이전트 가상 머신에 할당된 역할을 식별합니다.
   a. Azure Portal에서 가상 머신 서비스를 엽니다.
   b. 콘솔 에이전트 가상 머신을 선택합니다.
   c. 설정에서 *ID*를 선택합니다.
   d. *Azure 역할 할당*을 선택합니다.
   e. 콘솔 에이전트 가상 머신에 할당된 사용자 지정 역할을 기록해 둡니다.
2. 사용자 지정 역할 업데이트:
   a. Azure Portal에서 Azure 구독을 엽니다.
   b. *액세스 제어(IAM) > 역할*을 선택합니다.
   c. 사용자 지정 역할에 대한 줄임표(...)를 선택한 다음 *편집*을 선택합니다.
   d. *JSON*을 선택하고 다음 권한을 추가합니다.

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"정책에 대한 전체 JSON 형식 보기"

e. *검토 + 업데이트*를 선택한 다음 *업데이트*를 선택합니다.

데이터 암호화를 위한 고객 관리 키 사용에 필요한 정보

기본 Microsoft 관리 암호화 키를 사용하는 대신, 활성화 마법사에서 고객이 관리하는 키를 사용하여 데이터를 암호화할 수 있습니다. 이 경우 Azure 구독, Key Vault 이름 및 키가 필요합니다. "자신의 키를 사용하는 방법을 확인하세요" .

NetApp Backup and Recovery *Azure* 액세스 정책, *Azure* 역할 기반 액세스 제어(Azure RBAC) 권한 모델 및 관리형 하드웨어 보안 모델(HSM)을 지원합니다(참조 "Azure Key Vault 관리형 HSM이란 무엇인가요?").

Azure Blob 저장소 계정 만들기

기본적으로 이 서비스는 사용자를 위한 스토리지 계정을 생성합니다. 자신의 스토리지 계정을 사용하려면 백업 활성화 마법사를 시작하기 전에 계정을 만든 다음 마법사에서 해당 스토리지 계정을 선택하면 됩니다.

"나만의 스토리지 계정 생성에 대해 자세히 알아보세요".

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.
- 서로 다른 서브넷에 있는 두 개의 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 서브넷을 함께 라우팅해야 합니다(이는 기본 설정입니다).

Cloud Volumes ONTAP 에서 **NetApp Backup and Recovery** 활성화

NetApp Backup and Recovery 활성화하는 것은 쉽습니다. 단계는 기존 Cloud Volumes ONTAP 시스템이 있는지 아니면 새 시스템이 있는지에 따라 약간씩 다릅니다.

새 시스템에서 **NetApp Backup and Recovery** 활성화

NetApp Backup and Recovery 시스템 마법사에서 기본적으로 활성화되어 있습니다. 해당 옵션을 활성화해 두세요.

보다 "Azure에서 Cloud Volumes ONTAP 시작" Cloud Volumes ONTAP 시스템을 만드는 데 필요한 요구 사항과 세부 정보를 확인하세요.

리소스 그룹의 이름을 선택하려면 Cloud Volumes ONTAP 배포할 때 NetApp Backup and Recovery *비활성화*하세요.

단계

1. 콘솔의 시스템 페이지에서 *시스템 추가*를 선택하고, 클라우드 공급자를 선택한 다음 *새로 추가*를 선택합니다. * Cloud Volumes ONTAP 만들기*를 선택합니다.
2. 클라우드 공급자로 *Microsoft Azure*를 선택한 다음 단일 노드 또는 HA 시스템을 선택합니다.
3. Azure 자격 증명 정의 페이지에서 자격 증명 이름, 클라이언트 ID, 클라이언트 비밀번호, 디렉터리 ID를 입력하고 *계속*을 선택합니다.
4. 세부 정보 및 자격 증명 페이지를 작성하고 Azure Marketplace 구독이 있는지 확인한 후 *계속*을 선택합니다.
5. 서비스 페이지에서 서비스를 활성화한 상태로 두고 *계속*을 선택합니다.
6. 마법사의 페이지를 완료하여 시스템을 배포합니다.

결과

시스템에서 NetApp Backup and Recovery 활성화되어 있습니다. 이러한 Cloud Volumes ONTAP 시스템에서 볼륨을 생성한 후 NetApp Backup and Recovery 실행하세요."보호하려는 각 볼륨에서 백업을 활성화합니다." .

기존 시스템에서 **NetApp Backup and Recovery** 활성화

언제든지 시스템에서 직접 NetApp Backup and Recovery 활성화하세요.

단계

1. 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화*를 선택합니다.

   백업을 위한 Azure Blob 대상이 콘솔의 시스템 페이지에 시스템으로 존재하는 경우, 클러스터를 Azure Blob 시스템으로 끌어서 놓으면 설치 마법사를 시작할 수 있습니다.

2. 마법사의 페이지를 완료하여 NetApp Backup and Recovery 배포합니다.
3. 백업을 시작하려면 다음을 계속하세요.ONTAP 볼륨에서 백업 활성화 .

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

   ◦ 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

백업을 위한 Azure 대상이 시스템 페이지에 시스템으로 존재하는 경우 ONTAP 클러스터를 Azure Blob 개체 스토리지로 끌어다 놓을 수 있습니다.

- 백업 및 복구 막대에서 *볼륨*을 선택합니다. 볼륨 탭에서 *작업*을 선택하세요. ••• 아이콘을 클릭하고 단일 볼륨(이미 복제나 개체 스토리지 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
   - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
   - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 백업 정책.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
   - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
   - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다. (FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다.) 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
   - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
   - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
   - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
   - 백업: 볼륨을 개체 스토리지에 백업합니다.
2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   - 계단식: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 보조 스토리지에서 개체 스토리지로 흐릅니다.
   - 팬아웃: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

   이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새로 만듭니다.

   스냅샷을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

   정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
   - 정책의 이름을 입력하세요.
   - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
   - *만들기*를 선택하세요.
4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새로 만듭니다.

     복제를 활성화하기 전에 사용자 지정 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.
5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: *Microsoft Azure*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보를 입력하세요.

     백업이 저장될 지역을 입력하세요. 이는 Cloud Volumes ONTAP 시스템이 있는 지역과 다른 지역일 수

있습니다.

새로운 저장 계정을 만들거나 기존 계정을 선택하세요.

백업을 저장하는 데 사용되는 Azure 구독을 입력하세요. 이는 Cloud Volumes ONTAP 시스템이 있는 구독과 다를 수 있습니다.

Blob 컨테이너를 관리하는 자체 리소스 그룹을 만들거나 리소스 그룹 유형과 그룹을 선택하세요.

백업 파일이 수정되거나 삭제되는 것을 방지하려면 30일 보존 기간을 설정하고 변경 불가능한 저장소를 활성화하여 저장소 계정을 생성했는지 확인하세요.

- 암호화 키: 새 Azure Storage 계정을 만든 경우 공급자로부터 받은 암호화 키 정보를 입력합니다. 기본 Azure 암호화 키를 사용할지 아니면 Azure 계정에서 고객이 관리하는 키를 선택하여 데이터 암호화를 관리할지 선택하세요.

  고객이 직접 관리하는 키를 사용하기로 선택한 경우 키 보관소와 키 정보를 입력하세요. "자신의 열쇠를 사용하는 방법을 알아보세요" .

  기존 Microsoft 저장소 계정을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

- 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다. 개인 엔드포인트는 기본적으로 비활성화되어 있습니다.

  i. 백업하려는 볼륨이 있는 ONTAP 클러스터의 IP 공간입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.

  ii. 선택적으로, 이전에 구성한 Azure 개인 엔드포인트를 사용할지 여부를 선택합니다. "Azure 개인 엔드포인트 사용에 대해 알아보세요" .

- 백업 정책: 기존의 개체 저장소 백업 정책을 선택합니다.

  백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

  정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

  - 정책의 이름을 입력하세요.
  - 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .
  - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
  - *만들기*를 선택하세요.

- 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 저장소 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 볼륨과 동기화됩니다.

입력한 리소스 그룹에 Blob 스토리지 컨테이너가 생성되고, 백업 파일이 여기에 저장됩니다.

기본적으로 NetApp Backup and Recovery 비용 최적화를 위해 로컬 중복성(LRS)을 사용하여 Blob 컨테이너를 프로비저닝합니다. 서로 다른 영역 간에 데이터가 복제되도록 하려면 이 설정을 영역 중복성(ZRS)으로 변경할 수 있습니다. Microsoft 지침을 참조하세요. "저장소 계정 복제 방식 변경" .

볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

다음은 무엇인가요?

- 당신은 할 수 있습니다"백업 파일과 백업 정책을 관리하세요" . 여기에는 백업 시작 및 중지, 백업 삭제, 백업 일정 추가 및 변경 등이 포함됩니다.
- 당신은 할 수 있습니다"클러스터 수준 백업 설정 관리" . 여기에는 ONTAP 클라우드 스토리지에 액세스하는 데 사용하는 스토리지 키 변경, 개체 스토리지에 백업을 업로드하는 데 사용할 수 있는 네트워크 대역폭 변경, 향후 볼륨에 대한 자동 백업 설정 변경 등이 포함됩니다.
- 당신도 할 수 있습니다"백업 파일에서 볼륨, 폴더 또는 개별 파일 복원" AWS의 Cloud Volumes ONTAP 시스템이나 온프레미스 ONTAP 시스템으로.

NetApp Backup and Recovery 사용하여 Cloud Volumes ONTAP 데이터를 Google Cloud Storage에 백업하세요.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 Cloud Volumes ONTAP 시스템에서 Google Cloud Storage로 볼륨 데이터를 백업하세요.

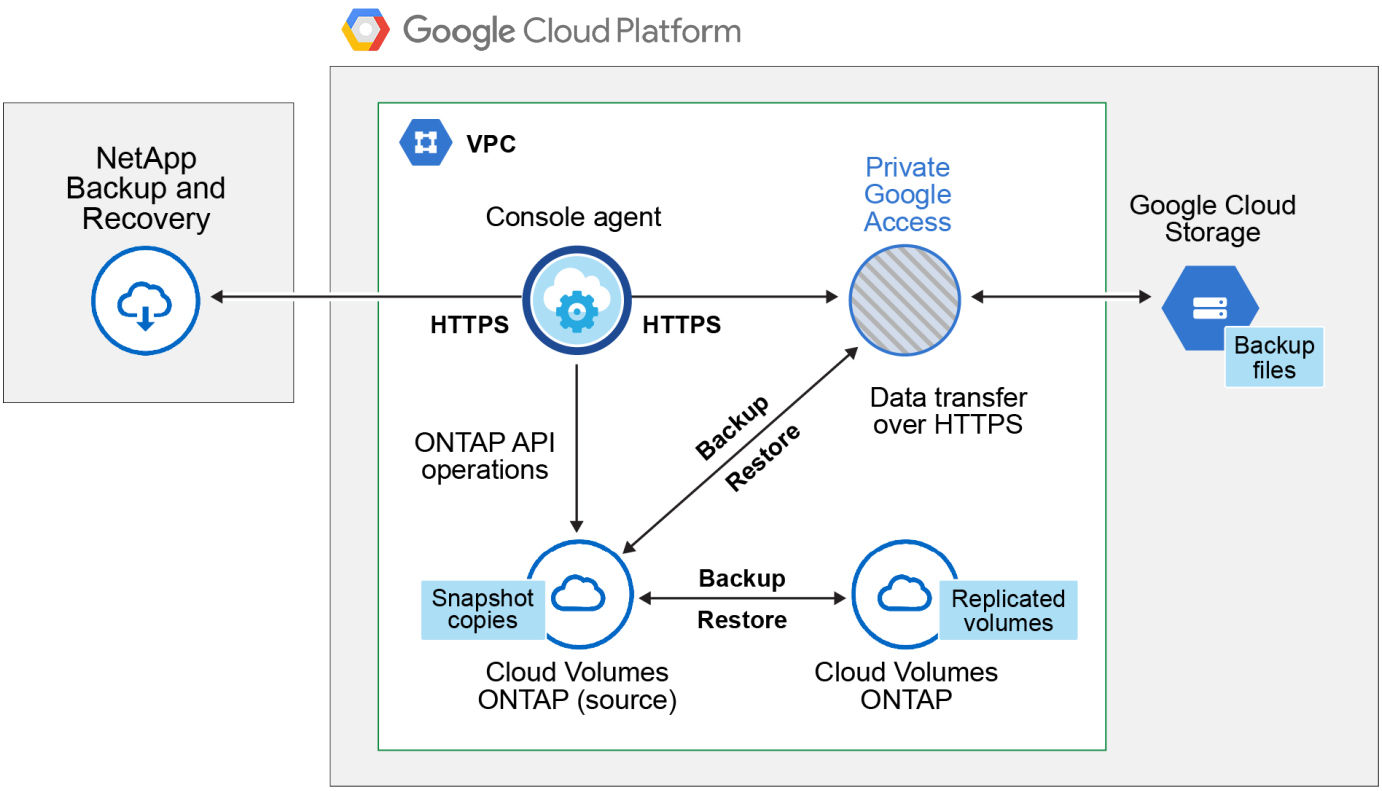
NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

구성에 대한 지원을 확인하세요

Google Cloud Storage에 볼륨을 백업하기 전에 지원되는 구성이 있는지 확인하려면 다음 요구 사항을 읽어보세요.

다음 이미지는 각 구성 요소와 구성 요소 간에 준비해야 할 연결을 보여줍니다.

선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.



지원되는 **ONTAP** 버전

최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.

지원되는 **GCP** 지역

NetApp Backup and Recovery 모든 GCP 지역에서 지원됩니다.

GCP 서비스 계정

Google Cloud 프로젝트에 사용자 지정 역할이 있는 서비스 계정이 있어야 합니다. "서비스 계정을 만드는 방법을 알아보세요" .

NetApp Backup and Recovery Google Cloud Storage 버킷에 액세스할 수 있도록 하는 서비스 계정에는 더 이상 스토리지 관리자 역할이 필요하지 않습니다.

라이센스 요구 사항 확인

NetApp Backup and Recovery PAYGO 라이선스의 경우, Google Marketplace에서 Cloud Volumes ONTAP 및 NetApp Backup and Recovery 배포할 수 있는 콘솔 구독을 이용할 수 있습니다. 당신은 필요합니다 "이 콘솔 구독을 구독하세요" NetApp Backup and Recovery 활성화하기 전에. NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다. "시스템 마법사의 세부 정보 및 자격 증명 페이지에서 구독할 수 있습니다." .

NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요".

백업이 저장될 저장 공간에 대한 Google 구독이 필요합니다.

콘솔 에이전트를 준비하세요

콘솔 에이전트는 인터넷 접속이 가능한 Google 지역에 설치해야 합니다.

- "콘솔 에이전트에 대해 알아보세요"
- "Google Cloud에 콘솔 에이전트 배포"

콘솔 에이전트에 대한 권한을 확인하거나 추가합니다.

NetApp Backup and Recovery "검색 및 복원" 기능을 사용하려면 콘솔 에이전트 역할에 대한 특정 권한이 있어야 Google Cloud BigQuery 서비스에 액세스할 수 있습니다. 아래의 권한을 확인하고, 정책을 수정해야 하는 경우 단계에 따라 진행하세요.

단계

1. 에서 "구글 클라우드 콘솔" 역할 페이지로 이동합니다.
2. 페이지 상단의 드롭다운 목록을 사용하여 편집하려는 역할이 포함된 프로젝트나 조직을 선택합니다.
3. 사용자 지정 역할을 선택하세요.
4. 역할의 권한을 업데이트하려면 *역할 편집*을 선택하세요.
5. *권한 추가*를 선택하여 역할에 다음과 같은 새로운 권한을 추가합니다.

```
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. 편집한 역할을 저장하려면 *업데이트*를 선택하세요.

고객 관리 암호화 키**(CMEK)** 사용에 필요한 정보

기본 Google 관리 암호화 키 대신 고객이 관리하는 키를 사용하여 데이터를 암호화할 수 있습니다. 지역 간 키와 프로젝트 간 키가 모두 지원되므로 CMEK 키의 프로젝트와 다른 버킷의 프로젝트를 선택할 수 있습니다. 고객이 직접 관리하는 키를 사용하려는 경우:

- 활성화 마법사에 이 정보를 추가하려면 키 링과 키 이름이 필요합니다. "고객 관리 암호화 키에 대해 자세히 알아보세요" .
- 콘솔 에이전트 역할에 다음과 같은 필수 권한이 포함되어 있는지 확인해야 합니다.

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 프로젝트에서 Google "Cloud Key Management Service(KMS)" API가 활성화되어 있는지 확인해야 합니다. 를 참조하십시오 "Google Cloud 문서: API 활성화" 자세한 내용은.

CMEK 고려 사항**:**

- HSM(하드웨어 지원)과 소프트웨어 생성 키가 모두 지원됩니다.
- 새로 생성한 Cloud KMS 키나 가져온 Cloud KMS 키가 모두 지원됩니다.
- 지역 키만 지원되고, 글로벌 키는 지원되지 않습니다.
- 현재는 "대칭 암호화/복호화" 목적만 지원됩니다.
- 스토리지 계정과 연결된 서비스 에이전트에는 NetApp Backup and Recovery 에서 "CryptoKey 암호화/복호화(roles/cloudkms.cryptoKeyEncrypterDecrypter)" IAM 역할이 할당됩니다.

나만의 버킷을 만들어보세요

기본적으로 서비스는 사용자를 위해 버킷을 생성합니다. 자신의 버킷을 사용하려면 백업 활성화 마법사를 시작하기 전에 버킷을 만든 다음 마법사에서 해당 버킷을 선택하면 됩니다.

"나만의 버킷을 만드는 방법에 대해 자세히 알아보세요".

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.
- 서로 다른 서브넷에 있는 두 개의 Cloud Volumes ONTAP 시스템 간에 데이터를 복제하려면 서브넷을 함께 라우팅해야 합니다(이는 기본 설정입니다).

Cloud Volumes ONTAP 에서 NetApp Backup and Recovery 활성화

NetApp Backup and Recovery 활성화하는 단계는 기존 Cloud Volumes ONTAP 시스템이 있는지 아니면 새 시스템이 있는지에 따라 약간 다릅니다.

새 시스템에서 **NetApp Backup and Recovery** 활성화

시스템 마법사를 완료하여 새로운 Cloud Volumes ONTAP 시스템을 만들면 NetApp Backup and Recovery 활성화할 수 있습니다.

서비스 계정이 이미 구성되어 있어야 합니다. Cloud Volumes ONTAP 시스템을 생성할 때 서비스 계정을 선택하지 않으면 시스템을 끄고 GCP 콘솔에서 Cloud Volumes ONTAP 에 서비스 계정을 추가해야 합니다.

보다 "GCP에서 Cloud Volumes ONTAP 출시" Cloud Volumes ONTAP 시스템을 만드는 데 필요한 요구 사항과 세부 정보를 확인하세요.

단계

1. 콘솔의 시스템 페이지에서 *시스템 추가*를 선택하고, 클라우드 공급자를 선택한 다음 *새로 추가*를 선택합니다. * Cloud Volumes ONTAP 만들기*를 선택합니다.
2. 위치 선택: *Google Cloud Platform*을 선택하세요.
3. 유형 선택: * Cloud Volumes ONTAP*(단일 노드 또는 고가용성)을 선택합니다.
4. 세부 정보 및 자격 증명: 다음 정보를 입력하세요.
   a. *프로젝트 편집*을 클릭하고, 사용하려는 프로젝트가 기본 프로젝트(콘솔 에이전트가 있는 프로젝트)와 다른 경우 새 프로젝트를 선택합니다.
   b. 클러스터 이름을 지정합니다.
   c. 서비스 계정 스위치를 활성화하고 미리 정의된 스토리지 관리자 역할이 있는 서비스 계정을 선택합니다. 이는 백업과 계층화를 활성화하는 데 필요합니다.
   d. 자격 증명을 지정하세요.

      GCP Marketplace 구독이 활성화되어 있는지 확인하세요.

5. 서비스: NetApp Backup and Recovery 활성화한 상태로 두고 *계속*을 클릭합니다.
6. 시스템을 배포하려면 마법사의 페이지를 완료하세요. "GCP에서 Cloud Volumes ONTAP 출시" .

결과

시스템에서 NetApp Backup and Recovery 활성화되어 있습니다. 이러한 Cloud Volumes ONTAP 시스템에서 볼륨을 생성한 후 NetApp Backup and Recovery 실행하세요."보호하려는 각 볼륨에서 백업을 활성화합니다." .

기존 시스템에서 **NetApp Backup and Recovery** 활성화

언제든지 시스템에서 직접 NetApp Backup and Recovery 활성화할 수 있습니다.

단계

1. 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화*를 선택합니다.

   백업을 위한 Google Cloud Storage 대상이 콘솔의 시스템 페이지에 시스템으로 존재하는 경우, 클러스터를 Google Cloud Storage 시스템으로 끌어서 놓으면 설정 마법사가 시작됩니다.

Google Cloud Storage를 백업 대상으로 준비하세요

Google Cloud Storage를 백업 대상으로 준비하려면 다음 단계를 따르세요.

- 권한을 설정합니다.
- (선택 사항) 나만의 버킷을 만드세요. (원하시면 서비스에서 버킷을 만들어드립니다.)
- (선택 사항) 데이터 암호화를 위한 고객 관리 키 설정

권한 설정

사용자 지정 역할을 사용하여 특정 권한이 있는 서비스 계정에 대한 저장소 액세스 키를 제공해야 합니다. 서비스 계정을 사용하면 NetApp Backup and Recovery 백업을 저장하는 데 사용되는 Cloud Storage 버킷을 인증하고 액세스할 수 있습니다. Google Cloud Storage에서 누가 요청하는지 알 수 있도록 키가 필요합니다.

단계

1. 에서 "구글 클라우드 콘솔" 역할 페이지로 이동합니다.
2. "새로운 역할 만들기"다음 권한이 필요합니다.

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloud 콘솔에서 "서비스 계정 페이지로 이동" .
4. 클라우드 프로젝트를 선택하세요.
5. *서비스 계정 만들기*를 선택하고 필요한 정보를 제공합니다.
   a. 서비스 계정 세부 정보: 이름과 설명을 입력하세요.
   b. 이 서비스 계정에 프로젝트에 대한 액세스 권한 부여: 방금 만든 사용자 지정 역할을 선택합니다.
   c. *완료*를 선택하세요.
6. 로 가다 "GCP 스토리지 설정" 서비스 계정에 대한 액세스 키를 생성합니다.
   a. 프로젝트를 선택하고 *상호운용성*을 선택하세요. 아직 선택하지 않았다면 *상호 운용성 액세스 활성화*를 선택하세요.
   b. *서비스 계정용 액세스 키*에서 *서비스 계정용 키 만들기*를 선택하고 방금 만든 서비스 계정을 선택한 다음 *키 만들기*를 클릭합니다.

      나중에 백업 서비스를 구성할 때 NetApp Backup and Recovery 에 키를 입력해야 합니다.

나만의 버킷을 만들어보세요

기본적으로 서비스는 사용자를 위해 버킷을 생성합니다. 또는, 사용자 고유의 버킷을 사용하려면 백업 활성화 마법사를 시작하기 전에 버킷을 만든 다음 마법사에서 해당 버킷을 선택하면 됩니다.

"나만의 버킷을 만드는 방법에 대해 자세히 알아보세요".

데이터 암호화를 위한 고객 관리 암호화 키**(CMEK)** 설정

기본 Google 관리 암호화 키 대신 고객이 관리하는 키를 사용하여 데이터를 암호화할 수 있습니다. 지역 간 키와 프로젝트 간 키가 모두 지원되므로 CMEK 키의 프로젝트와 다른 버킷의 프로젝트를 선택할 수 있습니다.

고객이 직접 관리하는 키를 사용하려는 경우:

- 활성화 마법사에 이 정보를 추가하려면 키 링과 키 이름이 필요합니다. "고객 관리 암호화 키에 대해 자세히 알아보세요" .
- 콘솔 에이전트 역할에 다음과 같은 필수 권한이 포함되어 있는지 확인해야 합니다.

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 프로젝트에서 Google "Cloud Key Management Service(KMS)" API가 활성화되어 있는지 확인해야 합니다. 를 참조하십시오 "Google Cloud 문서: API 활성화" 자세한 내용은.

CMEK 고려 사항**:**

- HSM(하드웨어 지원)과 소프트웨어 생성 키가 모두 지원됩니다.
- 새로 생성한 Cloud KMS 키나 가져온 Cloud KMS 키가 모두 지원됩니다.
- 지역 키만 지원되고 글로벌 키는 지원되지 않습니다.
- 현재는 "대칭 암호화/복호화" 목적만 지원됩니다.
- 스토리지 계정과 연결된 서비스 에이전트에는 NetApp Backup and Recovery 에서 "CryptoKey 암호화/복호화(roles/cloudkms.cryptoKeyEncrypterDecrypter)" IAM 역할이 할당됩니다.

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.
   - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

     백업을 위한 GCP 대상이 콘솔의 시스템 페이지에 시스템으로 존재하는 경우 ONTAP 클러스터를 GCP 개체 스토리지로 끌어다 놓을 수 있습니다.
   - 백업 및 복구 막대에서 *볼륨*을 선택합니다. 볼륨 탭에서 *작업*을 선택하세요. ••• 아이콘을 클릭하고 단일

볼륨(이미 복제나 개체 스토리지 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
   - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
   - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
   - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
   - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
   - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
   - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
   - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
   - 백업: 볼륨을 개체 스토리지에 백업합니다.
2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   - 계단식: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 보조 스토리지에서 개체 스토리지로 흐릅니다.
   - 팬아웃: 정보는 기본 스토리지 시스템에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

     이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새로 만듭니다.

   백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

   정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
   - 정책의 이름을 입력하세요.
   - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
   - 백업-객체 정책의 경우 Datalock 및 랜섬웨어 복원력을 구성합니다. Datalock 및 Ransomware Resilience에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .
   - *만들기*를 선택하세요.
4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새로 만듭니다.

     복제를 활성화하기 전에 사용자 지정 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.
5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: *Google Cloud*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보와 백업이 저장될 지역을 입력하세요.

     새로운 버킷을 만들거나 기존 버킷을 선택하세요.

◦ 암호화 키: 새 Google 버킷을 만든 경우 공급업체에서 제공한 암호화 키 정보를 입력하세요. 데이터 암호화를 관리하기 위해 기본 Google Cloud 암호화 키를 사용할지, 아니면 Google 계정에서 고객이 관리하는 키를 선택할지 선택하세요.

고객이 직접 관리하는 키를 사용하기로 선택한 경우 키 보관소와 키 정보를 입력하세요.

기존 Google Cloud 버킷을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

◦ 백업 정책: 기존의 백업-객체 스토리지 정책을 선택하거나 새로 만듭니다.

백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

- 정책의 이름을 입력하세요.
- 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
- *만들기*를 선택하세요.

◦ 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 스토리지 시스템 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 스토리지 시스템 볼륨과 동기화됩니다.

입력한 Google 액세스 키와 비밀 키로 지정된 서비스 계정에 Google Cloud Storage 버킷이 생성되고, 백업 파일이 해당 버킷에 저장됩니다.

백업은 기본적으로 *Standard* 스토리지 클래스와 연결됩니다. 비용이 저렴한 *Nearline*, *Coldline* 또는 *Archive* 스토리지 클래스를 사용할 수 있습니다. 하지만 NetApp Backup and Recovery UI가 아닌 Google을 통해 스토리지 클래스를 구성합니다. Google 주제를 참조하세요 "버킷의 기본 스토리지 클래스 변경" 자세한 내용은.

볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

다음은 무엇인가요?

- 당신은 할 수 있습니다"백업 파일과 백업 정책을 관리하세요" . 여기에는 백업 시작 및 중지, 백업 삭제, 백업 일정 추가 및 변경 등이 포함됩니다.
- 당신은 할 수 있습니다"클러스터 수준 백업 설정 관리" . 여기에는 ONTAP 클라우드 스토리지에 액세스하는 데 사용하는 스토리지 키 변경, 개체 스토리지에 백업을 업로드하는 데 사용할 수 있는 네트워크 대역폭 변경, 향후 볼륨에 대한 자동 백업 설정 변경 등이 포함됩니다.
- 당신도 할 수 있습니다"백업 파일에서 볼륨, 폴더 또는 개별 파일 복원" AWS의 Cloud Volumes ONTAP 시스템이나 온프레미스 ONTAP 시스템으로.

NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 데이터를 Amazon S3에 백업하세요.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 온프레미스 ONTAP 시스템의 볼륨 데이터를 보조 스토리지 시스템과 Amazon S3 클라우드 스토리지로 백업하세요.

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

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

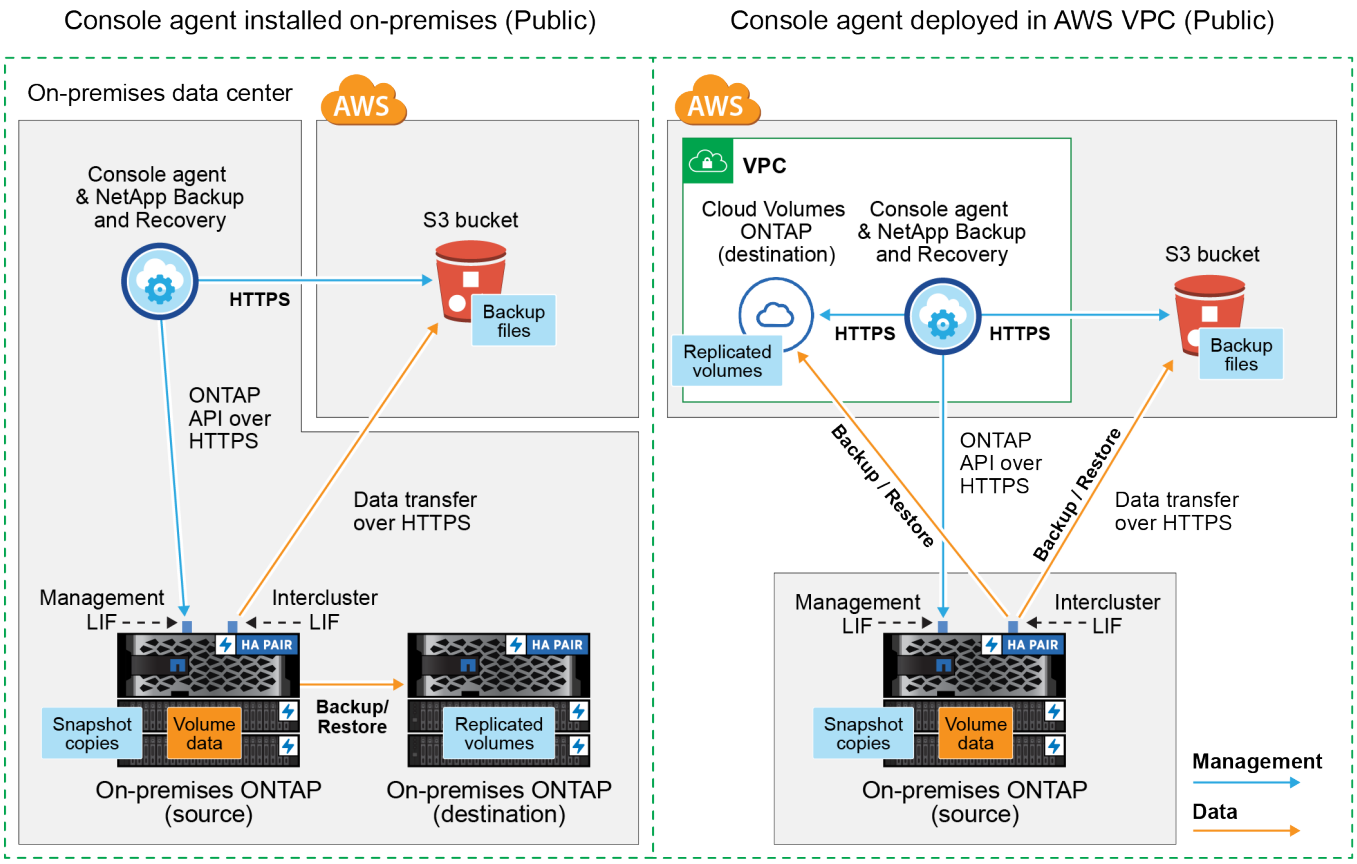
연결 방법을 식별하세요

온프레미스 ONTAP 시스템에서 AWS S3로 백업을 구성할 때 두 가지 연결 방법 중 어떤 것을 사용할지 선택하세요.

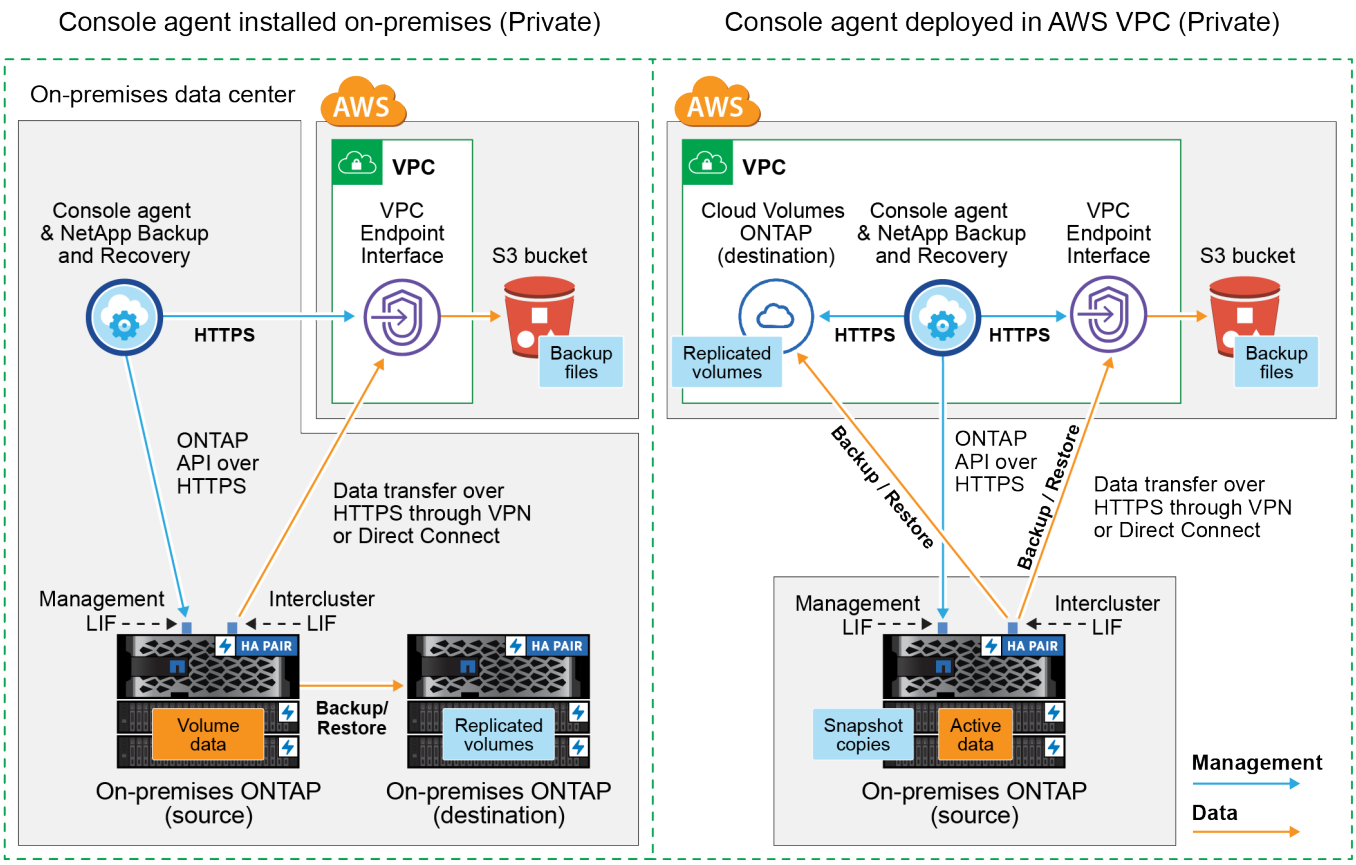
- 공개 연결 - 공개 S3 엔드포인트를 사용하여 ONTAP 시스템을 AWS S3에 직접 연결합니다.
- 개인 연결 - VPN 또는 AWS Direct Connect를 사용하고 개인 IP 주소를 사용하는 VPC 엔드포인트 인터페이스를 통해 트래픽을 라우팅합니다.

선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.

다음 다이어그램은 공개 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 사내에 설치한 콘솔 에이전트나 AWS VPC에 배포한 콘솔 에이전트를 사용할 수 있습니다.



다음 다이어그램은 개인 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 사내에 설치한 콘솔 에이전트나 AWS VPC에 배포한 콘솔 에이전트를 사용할 수 있습니다.



콘솔 에이전트를 준비하세요

콘솔 에이전트는 NetApp Console 기능을 위한 주요 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 콘솔 에이전트가 필요합니다.

콘솔 에이전트 만들기 또는 전환

AWS VPC나 사내에 콘솔 에이전트가 이미 배포되어 있다면 준비가 완료된 것입니다.

그렇지 않은 경우 해당 위치 중 하나에 콘솔 에이전트를 만들어 ONTAP 데이터를 AWS S3 스토리지에 백업해야 합니다. 다른 클라우드 공급자에 배포된 콘솔 에이전트를 사용할 수 없습니다.

- "콘솔 에이전트에 대해 알아보세요"
- "AWS에 콘솔 에이전트 설치"
- "귀하의 구내에 콘솔 에이전트를 설치하세요"
- "AWS GovCloud 지역에 콘솔 에이전트 설치"

  NetApp Backup and Recovery 콘솔 에이전트가 클라우드에 배포된 경우에만 GovCloud 지역에서 지원되며, 사내에 설치된 경우에는 지원되지 않습니다. 또한 AWS Marketplace에서 콘솔 에이전트를 배포해야 합니다. NetApp Console SaaS 웹사이트에서는 정부 지역에 콘솔 에이전트를 배포할 수 없습니다.

콘솔 에이전트 네트워킹 요구 사항 준비

다음 네트워킹 요구 사항이 충족되는지 확인하세요.

- 콘솔 에이전트가 설치된 네트워크에서 다음 연결이 허용되는지 확인하세요.
  - NetApp Backup and Recovery 와 S3 개체 스토리지에 대한 포트 443을 통한 HTTPS 연결("엔드포인트 목록을 확인하세요")
  - ONTAP 클러스터 관리 LIF에 대한 포트 443을 통한 HTTPS 연결
  - AWS 및 AWS GovCloud 배포에는 추가적인 인바운드 및 아웃바운드 보안 그룹 규칙이 필요합니다. 보다 "AWS의 콘솔 에이전트에 대한 규칙" 자세한 내용은.
- ONTAP 클러스터에서 VPC로 Direct Connect 또는 VPN 연결이 있고 콘솔 에이전트와 S3 간의 통신을 AWS 내부 네트워크(비공개 연결)에 유지하려는 경우 S3에 대한 VPC 엔드포인트 인터페이스를 활성화해야 합니다. VPC 엔드포인트 인터페이스를 사용하여 개인 연결을 위한 시스템 구성.

라이센스 요구 사항 확인

AWS와 NetApp Console 모두에 대한 라이선스 요구 사항을 확인해야 합니다.

- 클러스터에 대한 NetApp Backup and Recovery 활성화하려면 먼저 AWS에서 제공하는 PAYGO(Pay-as-you-go) NetApp Console 마켓플레이스에 가입하거나 NetApp 에서 NetApp Backup and Recovery BYOL 라이선스를 구매하여 활성화해야 합니다. 이러한 라이선스는 귀하의 계정에 적용되며 여러 시스템에서 사용할 수 있습니다.
  - NetApp Backup and Recovery PAYGO 라이선싱의 경우 구독이 필요합니다. "AWS Marketplace에서 제공하는 NetApp Console" . NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다.
  - NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다.
- 백업이 저장될 개체 스토리지 공간에 대한 AWS 구독이 필요합니다.

지원 지역

AWS GovCloud 지역을 포함한 모든 지역의 온프레미스 시스템에서 Amazon S3로 백업을 생성할 수 있습니다. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

ONTAP 클러스터 준비

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템을 준비합니다.

ONTAP 클러스터를 준비하는 단계는 다음과 같습니다.

- NetApp Console 에서 ONTAP 시스템을 찾아보세요
- ONTAP 시스템 요구 사항 확인
- 개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인
- 볼륨 복제를 위한 ONTAP 네트워킹 요구 사항 확인

NetApp Console 에서 ONTAP 시스템을 찾아보세요

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템 모두 NetApp Console 시스템 페이지에서 사용할 수 있어야 합니다.

클러스터를 추가하려면 클러스터 관리 IP 주소와 관리자 사용자 계정의 비밀번호를 알아야 합니다. "클러스터를 검색하는 방법을 알아보세요".

ONTAP 시스템 요구 사항 확인

ONTAP 시스템이 다음 요구 사항을 충족하는지 확인하세요.

- 최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됨).

  참고: NetApp Backup and Recovery 사용하는 경우 "하이브리드 클라우드 번들"은 필요하지 않습니다.

  방법을 배우십시오 "클러스터 라이선스 관리" .
- 시간과 시간대가 올바르게 설정되었습니다. 방법을 배우십시오 "클러스터 시간 구성" .
- 데이터를 복제하는 경우 소스 및 대상 시스템이 호환되는 ONTAP 버전을 실행하는지 확인하세요.

  "SnapMirror 관계에 대한 호환 ONTAP 버전 보기".

개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인

개체 스토리지에 연결하는 시스템에서 다음 요구 사항을 구성해야 합니다.

- 팬아웃 백업 아키텍처의 경우 기본 시스템에서 다음 설정을 구성합니다.
- 계단식 백업 아키텍처의 경우 보조 시스템에서 다음 설정을 구성합니다.

다음과 같은 ONTAP 클러스터 네트워킹 요구 사항이 필요합니다.

- 클러스터에는 콘솔 에이전트에서 클러스터 관리 LIF로의 인바운드 HTTPS 연결이 필요합니다.
- 백업하려는 볼륨을 호스팅하는 각 ONTAP 노드에는 클러스터 간 LIF가 필요합니다. 이러한 클러스터 간 LIF는 개체 저장소에 액세스할 수 있어야 합니다.

  클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 Amazon S3 스토리지로 포트 443을 통해 아웃바운드 HTTPS 연결을 시작합니다. ONTAP 개체 스토리지에서 데이터를 읽고 씁니다. 개체 스토리지는 결코 시작하지 않고 단지 응답만 합니다.

- 클러스터 간 LIF는 ONTAP 개체 스토리지에 연결하는 데 사용해야 하는 _IPspace_와 연결되어야 합니다. "IPspaces에 대해 자세히 알아보세요" .

  NetApp Backup and Recovery 설정하면 사용할 IP 공간을 입력하라는 메시지가 표시됩니다. 이러한 LIF가 연결된 IP 공간을 선택해야 합니다. 이는 "기본" IP 공간일 수도 있고 사용자가 만든 사용자 지정 IP 공간일 수도 있습니다.

  "기본"이 아닌 다른 IP 공간을 사용하는 경우 개체 스토리지에 액세스하려면 정적 경로를 만들어야 할 수도 있습니다.

  IPspace 내의 모든 클러스터 간 LIF는 개체 저장소에 액세스할 수 있어야 합니다. 현재 IP 공간에 대해 이를 구성할 수 없는 경우 모든 클러스터 간 LIF가 개체 저장소에 액세스할 수 있는 전용 IP 공간을 만들어야 합니다.

- 볼륨이 위치한 스토리지 VM에 대해 DNS 서버가 구성되어야 합니다. 방법을 확인하세요 "SVM에 대한 DNS 서비스 구성" .
- 필요한 경우 방화벽 규칙을 업데이트하여 ONTAP 에서 개체 스토리지로의 NetApp Backup and Recovery 연결이 포트 443을 통해 허용되고 스토리지 VM에서 DNS 서버로의 이름 확인 트래픽이 포트 53(TCP/UDP)을 통해 허용되도록 합니다.

- AWS에서 S3 연결을 위해 Private VPC Interface Endpoint를 사용하는 경우 HTTPS/443을 사용하려면 S3 엔드포인트 인증서를 ONTAP 클러스터에 로드해야 합니다. VPC 엔드포인트 인터페이스를 사용하여 개인 연결을 위한 시스템 구성.
- ONTAP 클러스터에 S3 버킷에 액세스할 수 있는 권한이 있는지 확인하세요.

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.

Amazon S3를 백업 대상으로 준비하세요

Amazon S3를 백업 대상으로 준비하려면 다음 단계를 따르세요.

- S3 권한을 설정합니다.
- (선택 사항) 나만의 S3 버킷을 만듭니다. (원하시면 서비스에서 버킷을 만들어드립니다.)
- (선택 사항) 데이터 암호화를 위해 고객 관리 AWS 키를 설정합니다.
- (선택 사항) VPC 엔드포인트 인터페이스를 사용하여 개인 연결을 위해 시스템을 구성합니다.

S3 권한 설정

두 가지 권한 세트를 구성해야 합니다.

- 콘솔 에이전트가 S3 버킷을 생성하고 관리할 수 있는 권한입니다.
- 온프레미스 ONTAP 클러스터가 S3 버킷에서 데이터를 읽고 쓸 수 있는 권한입니다.

단계

1. 콘솔 에이전트에 필요한 권한이 있는지 확인하세요. 자세한 내용은 다음을 참조하세요. "NetApp Console 정책 권한" .

> AWS 중국 리전에서 백업을 생성할 때 IAM 정책의 모든 *Resource* 섹션 아래에 있는 AWS 리소스 이름 "arn"을 "aws"에서 "aws-cn"으로 변경해야 합니다. 예를 들어, `arn:aws-cn:s3:::netapp-backup-*` .

2. 서비스를 활성화하면 백업 마법사가 액세스 키와 비밀 키를 입력하라는 메시지를 표시합니다. 이러한 자격 증명은 ONTAP 클러스터에 전달되어 ONTAP S3 버킷에 데이터를 백업하고 복원할 수 있도록 합니다. 이를 위해서는 다음 권한이 있는 IAM 사용자를 만들어야 합니다.

   를 참조하세요 "AWS 설명서: IAM 사용자에게 권한을 위임하는 역할 생성" .

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

나만의 버킷을 만들어보세요

기본적으로 서비스는 사용자를 위해 버킷을 생성합니다. 또는, 사용자 고유의 버킷을 사용하려면 백업 활성화 마법사를 시작하기 전에 버킷을 만든 다음 마법사에서 해당 버킷을 선택하면 됩니다.

"나만의 버킷을 만드는 방법에 대해 자세히 알아보세요".

자체 버킷을 생성하는 경우 버킷 이름으로 "netapp-backup"을 사용해야 합니다. 사용자 정의 이름을 사용해야 하는 경우 다음을 편집하세요. `ontapcloud-instance-policy-netapp-backup` 기존 CVO에 대한 IAMRole을 추가하고 다음 JSON 블록을 S3 권한에 추가합니다. `Statement` 정렬. 포함해야 합니다 `"Resource": "arn:aws:s3:::*"` 그리고 버킷과 연관되어야 하는 모든 필수 권한을 할당합니다.

```
[
  {
    "Effect": "Allow",
    "Action": [
      "s3:ListBucket",
      "s3:GetBucketLocation"
    ],
    "Resource": "arn:aws:s3:::*"
  },
  {
    "Effect": "Allow",
    "Action": [
      "s3:GetObject",
      "s3:PutObject",
      "s3:DeleteObject",
      "s3:ListAllMyBuckets",
      "s3:PutObjectTagging",
      "s3:GetObjectTagging",
      "s3:RestoreObject",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetObjectRetention",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutObjectRetention"
    ],
    "Resource": "arn:aws:s3:::*"
  }
]
```

데이터 암호화를 위한 고객 관리 **AWS** 키 설정

온프레미스 클러스터와 S3 버킷 간에 전달되는 데이터를 암호화하기 위해 기본 Amazon S3 암호화 키를 사용하려는 경우, 기본 설치에서 해당 유형의 암호화가 사용되므로 모든 준비가 완료된 것입니다.

대신 기본 키를 사용하는 대신 고객이 관리하는 키를 사용하여 데이터를 암호화하려는 경우 NetApp Backup and Recovery 마법사를 시작하기 전에 암호화 관리 키를 미리 설정해야 합니다.

"Cloud Volumes ONTAP 에서 자체 Amazon 암호화 키를 사용하는 방법을 참조하세요.".

"NetApp Backup and Recovery 에서 자체 Amazon 암호화 키를 사용하는 방법을 참조하세요.".

VPC 엔드포인트 인터페이스를 사용하여 개인 연결을 위한 시스템 구성

표준 공용 인터넷 연결을 사용하려는 경우 모든 권한은 콘솔 에이전트에 의해 설정되므로 그 외에는 아무것도 할 필요가 없습니다.

온프레미스 데이터 센터에서 VPC로 인터넷을 통해 보다 안전한 연결을 원하는 경우 백업 활성화 마법사에서 AWS PrivateLink 연결을 선택하는 옵션이 있습니다. 개인 IP 주소를 사용하는 VPC 엔드포인트 인터페이스를 통해 온프레미스 시스템에 연결하기 위해 VPN이나 AWS Direct Connect를 사용하려는 경우 필요합니다.

단계

1. Amazon VPC 콘솔이나 명령줄을 사용하여 인터페이스 엔드포인트 구성을 만듭니다. "Amazon S3에 AWS PrivateLink를 사용하는 방법에 대한 자세한 내용을 참조하세요." .
2. 콘솔 에이전트와 연결된 보안 그룹 구성을 수정합니다. 정책을 "전체 액세스"에서 "사용자 지정"으로 변경해야 합니다.백업 정책에서 S3 권한을 추가합니다. 앞서 보여준 것처럼.

   개인 엔드포인트와 통신하기 위해 포트 80(HTTP)을 사용한다면 준비가 완료된 것입니다. 이제 클러스터에서 NetApp Backup and Recovery 활성화할 수 있습니다.

   개인 엔드포인트와 통신하기 위해 포트 443(HTTPS)을 사용하는 경우 다음 4단계에 표시된 대로 VPC S3 엔드포인트에서 인증서를 복사하여 ONTAP 클러스터에 추가해야 합니다.

3. AWS 콘솔에서 엔드포인트의 DNS 이름을 얻습니다.
4. VPC S3 엔드포인트에서 인증서를 가져옵니다. 당신은 이것을 이렇게 합니다 "콘솔 에이전트를 호스팅하는 VM에 로그인" 다음 명령을 실행합니다. 엔드포인트의 DNS 이름을 입력할 때 "*"를 "bucket"으로 바꿔서 처음에 추가합니다.

   ```
   openssl s_client -connect bucket.vpce-0ff5c15df7e00fbab-yxs7lt8v.s3.us-west-2.vpce.amazonaws.com:443 -showcerts
   ```

5. 이 명령의 출력에서 S3 인증서에 대한 데이터를 복사합니다(BEGIN / END CERTIFICATE 태그를 포함하여 그 사이의 모든 데이터).

```
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 로그인하고 다음 명령을 사용하여 복사한 인증서를 적용합니다(사용자의 스토리지 VM 이름으로 대체).

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

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

   - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

     백업을 위한 Amazon S3 대상이 콘솔의 시스템 페이지에 시스템으로 존재하는 경우 ONTAP 클러스터를 Amazon S3 개체 스토리지로 끌어다 놓을 수 있습니다.

   - 백업 및 복구 표시줄에서 *볼륨*을 선택합니다. 볼륨 탭에서 *작업*을 선택하세요. ••• 아이콘을 클릭하고 단일 볼륨(이미 복제나 개체 스토리지 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

   마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
    - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
    - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
    - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
    - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
    - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.

- 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
- 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
- 백업: 볼륨을 개체 스토리지에 백업합니다.

2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   - 계단식: 정보는 기본 저장소에서 보조 저장소로, 보조 저장소에서 객체 저장소로 흐릅니다.
   - 팬아웃: 정보는 기본 스토리지에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

   이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .

3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 정책을 만듭니다.

   스냅샷을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

4. 정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
   - 정책의 이름을 입력하세요.
   - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .
   - *만들기*를 선택하세요.

5. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 정책을 만듭니다.

     복제를 활성화하기 전에 사용자 지정 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.

6. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: *Amazon Web Services*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보와 백업이 저장될 AWS 지역을 입력합니다.

     액세스 키와 비밀 키는 ONTAP 클러스터에 S3 버킷에 대한 액세스 권한을 부여하기 위해 생성한 IAM 사용자를 위한 것입니다.

   - 버킷: 기존 S3 버킷을 선택하거나 새 버킷을 만듭니다. 참조하다 "S3 버킷 추가" .
   - 암호화 키: 새 S3 버킷을 생성한 경우 공급자로부터 받은 암호화 키 정보를 입력하세요. 데이터 암호화를 관리하기 위해 기본 Amazon S3 암호화 키를 사용할지, 아니면 AWS 계정에서 고객이 관리하는 키를 선택할지 선택하세요.

기존 버킷을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

- 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다. 개인 엔드포인트는 기본적으로 비활성화되어 있습니다.
  i. 백업하려는 볼륨이 있는 ONTAP 클러스터의 IP 공간입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.
  ii. 선택적으로, 이전에 구성한 AWS PrivateLink를 사용할지 여부를 선택합니다. "Amazon S3에 AWS PrivateLink를 사용하는 방법에 대한 자세한 내용을 확인하세요." .
- 백업 정책: 기존 백업 정책을 선택하거나 정책을 만듭니다.

백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

- 정책의 이름을 입력하세요.
- 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
- *만들기*를 선택하세요.

- 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

7. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 저장소 볼륨과 동기화됩니다.

S3 액세스 키와 비밀 키를 입력한 서비스 계정에 S3 버킷이 생성되고, 백업 파일은 해당 계정에 저장됩니다. 볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 사용하여 온-프레미스 ONTAP 데이터를 Azure Blob 스토리지에 백업

온프레미스 ONTAP 시스템의 볼륨 데이터를 보조 스토리지 시스템과 Azure Blob 스토리지로 백업하려면 NetApp Backup and Recovery 에서 몇 가지 단계를 완료하세요.

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

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

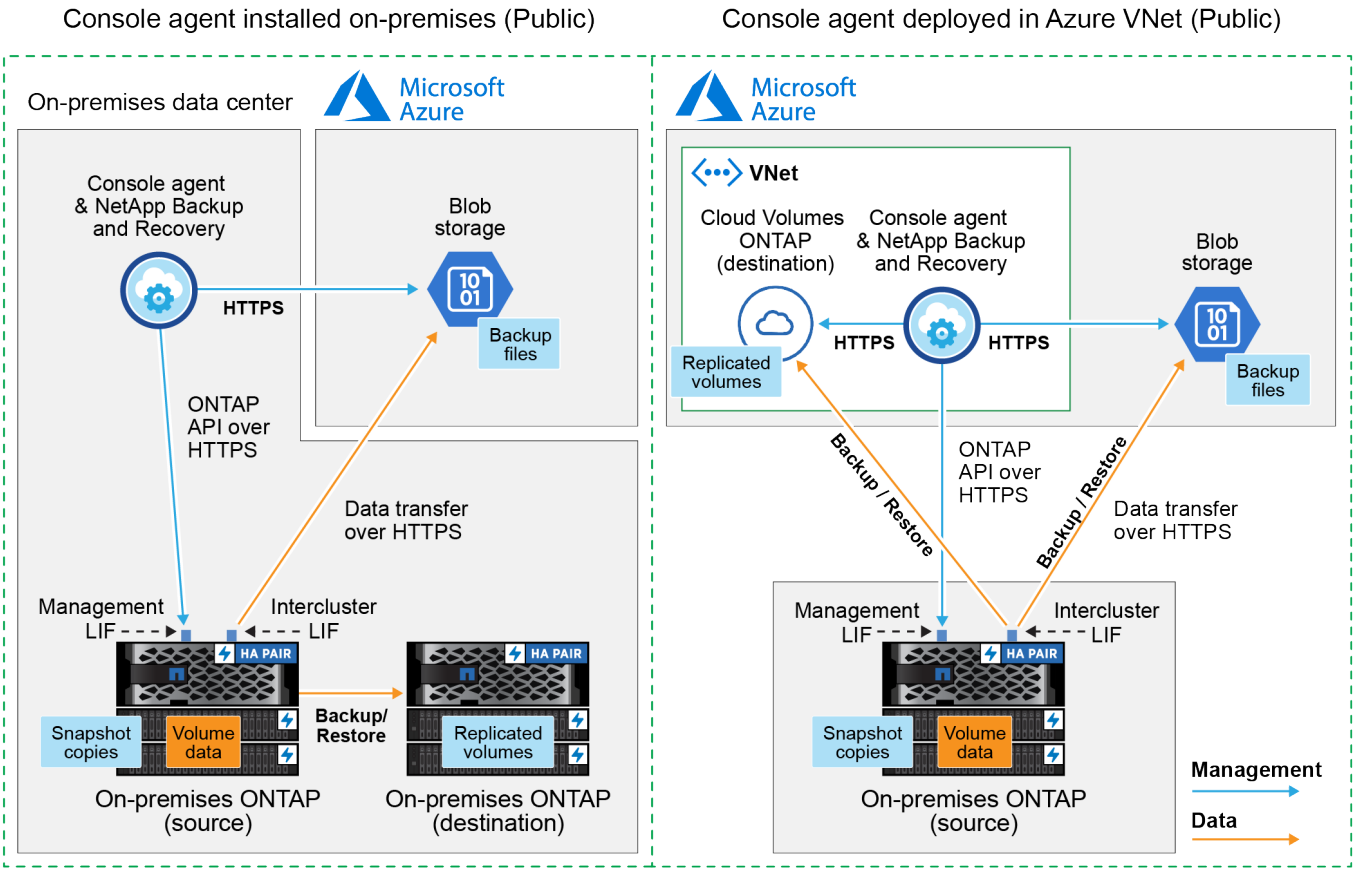
연결 방법을 식별하세요

온-프레미스 ONTAP 시스템에서 Azure Blob으로 백업을 구성할 때 두 가지 연결 방법 중 어떤 것을 사용할지 선택하세요.

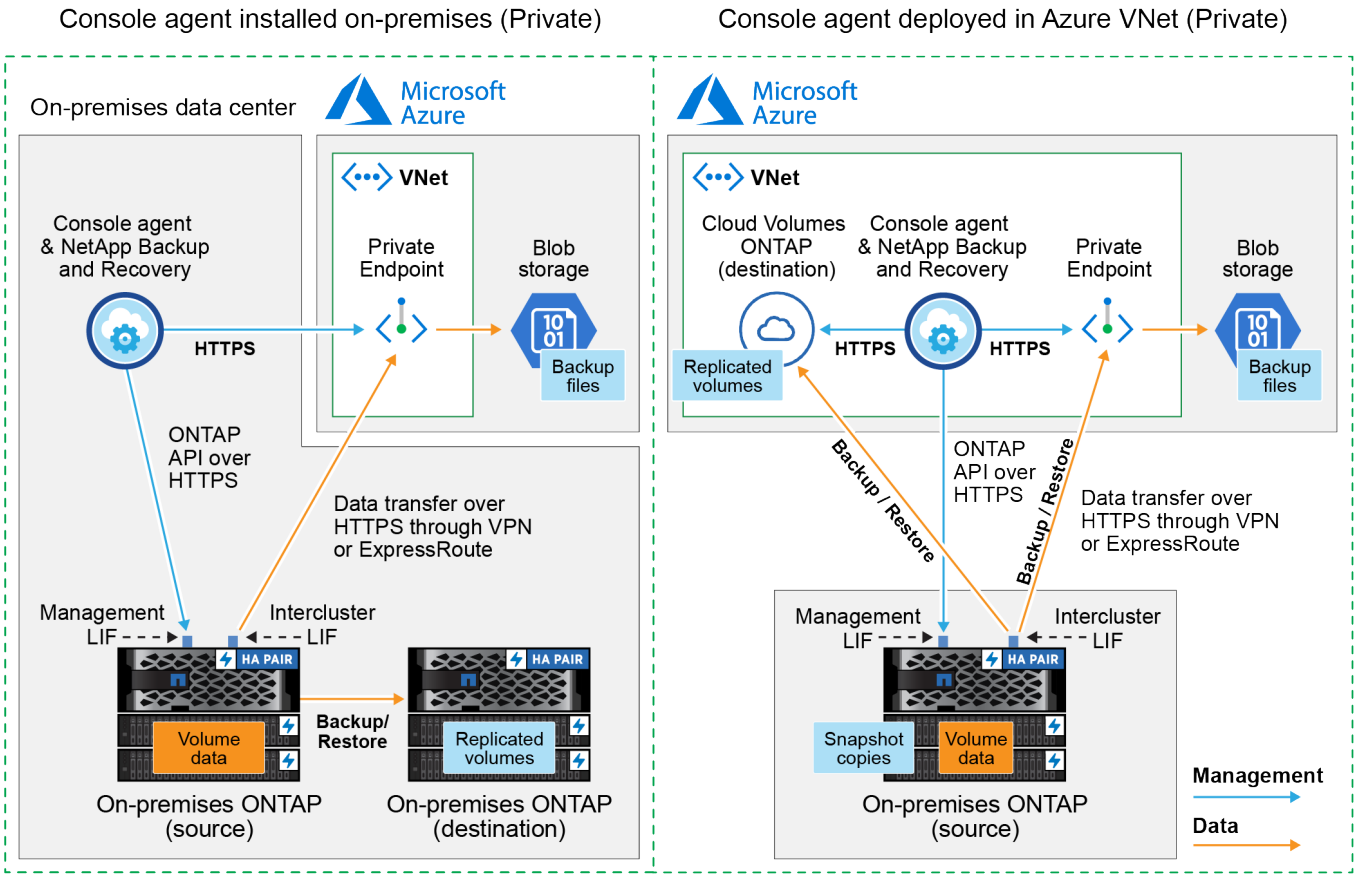
- 공개 연결 - 공개 Azure 엔드포인트를 사용하여 ONTAP 시스템을 Azure Blob 저장소에 직접 연결합니다.
- 개인 연결 - VPN이나 ExpressRoute를 사용하고 개인 IP 주소를 사용하는 VNet 개인 엔드포인트를 통해 트래픽을 라우팅합니다.

선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.

다음 다이어그램은 공개 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 온프레미스에 설치한 콘솔 에이전트나 Azure VNet에 배포한 콘솔 에이전트를 사용할 수 있습니다.



다음 다이어그램은 개인 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 온프레미스에 설치한 콘솔 에이전트나 Azure VNet에 배포한 콘솔 에이전트를 사용할 수 있습니다.



콘솔 에이전트를 준비하세요

콘솔 에이전트는 NetApp Console 기능을 위한 주요 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 콘솔 에이전트가 필요합니다.

콘솔 에이전트 만들기 또는 전환

Azure VNet이나 온프레미스에 콘솔 에이전트가 이미 배포되어 있다면 준비가 완료된 것입니다.

그렇지 않은 경우 해당 위치 중 하나에 콘솔 에이전트를 만들어 ONTAP 데이터를 Azure Blob 저장소에 백업해야 합니다. 다른 클라우드 공급자에 배포된 콘솔 에이전트를 사용할 수 없습니다.

- "콘솔 에이전트에 대해 알아보세요"
- "Azure에 콘솔 에이전트 설치"
- "귀하의 구내에 콘솔 에이전트를 설치하세요"
- "Azure Government 지역에 콘솔 에이전트 설치"

  NetApp Backup and Recovery 콘솔 에이전트가 클라우드에 배포된 경우에만 Azure Government 지역에서 지원되며, 사내에 설치된 경우에는 지원되지 않습니다. 또한 Azure Marketplace에서 콘솔 에이전트를 배포해야 합니다. 콘솔 SaaS 웹사이트에서 정부 지역에 콘솔 에이전트를 배포할 수 없습니다.

콘솔 에이전트를 위한 네트워킹 준비

콘솔 에이전트에 필요한 네트워크 연결이 있는지 확인하세요.

단계

1. 콘솔 에이전트가 설치된 네트워크에서 다음 연결이 허용되는지 확인하세요.
   - NetApp Backup and Recovery 와 Blob 개체 스토리지에 대한 포트 443을 통한 HTTPS 연결("엔드포인트 목록을 확인하세요")
   - ONTAP 클러스터 관리 LIF에 대한 포트 443을 통한 HTTPS 연결
   - NetApp Backup and Recovery 검색 및 복원 기능이 작동하려면 콘솔 에이전트와 Azure Synapse SQL 서비스 간 통신을 위해 포트 1433이 열려 있어야 합니다.
   - Azure 및 Azure Government 배포에는 추가 인바운드 보안 그룹 규칙이 필요합니다. 보다 "Azure의 콘솔 에이전트에 대한 규칙" 자세한 내용은.
2. Azure 저장소에 대한 VNet 개인 엔드포인트를 활성화합니다. ONTAP 클러스터에서 VNet으로 ExpressRoute 또는 VPN 연결이 있고 콘솔 에이전트와 Blob 스토리지 간 통신을 가상 사설망(비공개 연결)에 유지하려는 경우 이 작업이 필요합니다.

콘솔 에이전트에 대한 권한을 확인하거나 추가합니다.

NetApp Backup and Recovery 검색 및 복원 기능을 사용하려면 콘솔 에이전트 역할에 대한 특정 권한이 있어야 Azure Synapse Workspace 및 Data Lake Storage 계정에 액세스할 수 있습니다. 아래의 권한을 확인하고, 정책을 수정해야 하는 경우 단계에 따라 진행하세요.

시작하기 전에

구독을 통해 Azure Synapse Analytics 리소스 공급자("Microsoft.Synapse")를 등록해야 합니다. "구독을 위해 이 리소스 공급자를 등록하는 방법을 확인하세요." . 리소스 공급자를 등록하려면 구독 소유자 또는 *기여자*여야 합니다.

단계

1. 콘솔 에이전트 가상 머신에 할당된 역할을 식별합니다.
   a. Azure Portal에서 가상 머신 서비스를 엽니다.
   b. 콘솔 에이전트 가상 머신을 선택합니다.
   c. *설정*에서 *ID*를 선택하세요.
   d. *Azure 역할 할당*을 선택합니다.
   e. 콘솔 에이전트 가상 머신에 할당된 사용자 지정 역할을 기록해 둡니다.
2. 사용자 지정 역할 업데이트:
   a. Azure Portal에서 Azure 구독을 엽니다.
   b. *액세스 제어(IAM) > 역할*을 선택합니다.
   c. 사용자 지정 역할에 대한 줄임표(...)를 선택한 다음 *편집*을 선택합니다.
   d. *JSON*을 선택하고 다음 권한을 추가합니다.

```
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/write",
"Microsoft.Storage/storageAccounts/blobServices/containers/read",
"Microsoft.Storage/storageAccounts/listAccountSas/action",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Resources/subscriptions/resourceGroups/read",
"Microsoft.Resources/subscriptions/resourcegroups/resources/read"
,
"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Authorization/locks/*",
"Microsoft.Network/privateEndpoints/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",
"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
"Microsoft.Synapse/workspaces/write",
"Microsoft.Synapse/workspaces/read",
"Microsoft.Synapse/workspaces/delete",
"Microsoft.Synapse/register/action",
"Microsoft.Synapse/checkNameAvailability/action",
"Microsoft.Synapse/workspaces/operationStatuses/read",
"Microsoft.Synapse/workspaces/firewallRules/read",
"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
"Microsoft.Synapse/workspaces/operationResults/read",
"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/
action"
```

"정책에 대한 전체 JSON 형식 보기"

e. *검토 + 업데이트*를 선택한 다음 *업데이트*를 선택합니다.

라이센스 요구 사항 확인

Azure와 콘솔 모두에 대한 라이선스 요구 사항을 확인해야 합니다.

- 클러스터에 대한 NetApp Backup and Recovery 활성화하려면 먼저 Azure에서 PAYGO(Pay-as-you-go) 콘솔 마켓플레이스 상품을 구독하거나 NetApp 에서 NetApp Backup and Recovery BYOL 라이선스를 구매하여 활성화해야 합니다. 이러한 라이선스는 귀하의 계정에 적용되며 여러 시스템에서 사용할 수 있습니다.
  - NetApp Backup and Recovery PAYGO 라이선싱의 경우 구독이 필요합니다. "Azure Marketplace에서 제공하는 NetApp Console" . NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다.
  - NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요".
- 백업이 저장될 개체 스토리지 공간에 대한 Azure 구독이 필요합니다.

지원 지역

Azure Government 지역을 포함한 모든 지역의 온-프레미스 시스템에서 Azure Blob으로 백업을 만들 수 있습니다. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

ONTAP 클러스터 준비

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템을 준비합니다.

ONTAP 클러스터를 준비하는 단계는 다음과 같습니다.

- NetApp Console 에서 ONTAP 시스템을 찾아보세요
- ONTAP 시스템 요구 사항 확인
- 개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인
- 볼륨 복제를 위한 ONTAP 네트워킹 요구 사항 확인

NetApp Console 에서 ONTAP 시스템을 찾아보세요

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템 모두 NetApp Console 시스템 페이지에서 사용할 수 있어야 합니다.

클러스터를 추가하려면 클러스터 관리 IP 주소와 관리자 사용자 계정의 비밀번호를 알아야 합니다. "클러스터를 검색하는 방법을 알아보세요".

ONTAP 시스템 요구 사항 확인

ONTAP 시스템이 다음 요구 사항을 충족하는지 확인하세요.

- 최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됨).

  참고: NetApp Backup and Recovery 사용하는 경우 "하이브리드 클라우드 번들"은 필요하지 않습니다.

  방법을 배우십시오 "클러스터 라이선스 관리" .

- 시간과 시간대가 올바르게 설정되었습니다. 방법을 배우십시오 "클러스터 시간 구성" .
- 데이터를 복제하는 경우 소스 및 대상 시스템이 호환되는 ONTAP 버전을 실행하는지 확인하세요.

  "SnapMirror 관계에 대한 호환 ONTAP 버전 보기".

개체 스토리지에 데이터를 백업하기 위한 **ONTAP** 네트워킹 요구 사항 확인

개체 스토리지에 연결하는 시스템에서 다음 요구 사항을 구성해야 합니다.

- 팬아웃 백업 아키텍처의 경우 기본 시스템에서 다음 설정을 구성합니다.
- 계단식 백업 아키텍처의 경우 보조 시스템에서 다음 설정을 구성합니다.

다음과 같은 ONTAP 클러스터 네트워킹 요구 사항이 필요합니다.

- ONTAP 클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 Azure Blob 저장소로 포트 443을 통해 HTTPS 연결을 시작합니다.

  ONTAP 객체 스토리지에서 데이터를 읽고 씁니다. 객체 스토리지는 결코 시작되지 않고, 단지 응답만 합니다.

- ONTAP 콘솔 에이전트에서 클러스터 관리 LIF로의 인바운드 연결이 필요합니다. 콘솔 에이전트는 Azure VNet에 상주할 수 있습니다.
- 백업하려는 볼륨을 호스팅하는 각 ONTAP 노드에는 클러스터 간 LIF가 필요합니다. LIF는 ONTAP 개체 스토리지에 연결하는 데 사용해야 하는 _IPspace_와 연결되어야 합니다. "IPspaces에 대해 자세히 알아보세요" .

  NetApp Backup and Recovery 설정하면 사용할 IP 공간을 입력하라는 메시지가 표시됩니다. 각 LIF가 연결된 IP 공간을 선택해야 합니다. 이는 "기본" IP 공간일 수도 있고 사용자가 만든 사용자 지정 IP 공간일 수도 있습니다.

- 노드와 클러스터 간 LIF는 객체 저장소에 액세스할 수 있습니다.
- 볼륨이 위치한 스토리지 VM에 대한 DNS 서버가 구성되었습니다. 방법을 확인하세요 "SVM에 대한 DNS 서비스 구성" .
- 기본 IP 공간과 다른 IP 공간을 사용하는 경우 개체 스토리지에 액세스하려면 정적 경로를 만들어야 할 수도 있습니다.
- 필요한 경우 방화벽 규칙을 업데이트하여 ONTAP 에서 개체 스토리지로의 NetApp Backup and Recovery 서비스 연결이 포트 443을 통해 허용되고 스토리지 VM에서 DNS 서버로의 이름 확인 트래픽이 포트 53(TCP/UDP)을 통해 허용되도록 합니다.

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.

Azure Blob을 백업 대상으로 준비

1. 기본 Microsoft 관리 암호화 키를 사용하는 대신, 활성화 마법사에서 사용자 지정 관리 키를 사용하여 데이터를 암호화할 수 있습니다. 이 경우 Azure 구독, Key Vault 이름 및 키가 필요합니다. "자신의 열쇠를 사용하는 방법을 알아보세요" .

   백업 및 복구는 권한 모델로 *Azure* 액세스 정책_을 지원합니다. _*Azure* 역할 기반 액세스 제어 (Azure RBAC) 권한 모델은 현재 지원되지 않습니다.

2. 온프레미스 데이터 센터에서 VNet으로 공용 인터넷을 통해 보다 안전하게 연결하려면 활성화 마법사에서 Azure 개인 엔드포인트를 구성하는 옵션이 있습니다. 이 경우 해당 연결에 대한 VNet과 서브넷을 알아야 합니다. "개인 엔드포인트 사용에 대한 세부 정보를 참조하세요." .

Azure Blob 저장소 계정 만들기

기본적으로 이 서비스는 사용자를 위한 스토리지 계정을 생성합니다. 자신의 스토리지 계정을 사용하려면 백업 활성화 마법사를 시작하기 전에 계정을 만든 다음 마법사에서 해당 스토리지 계정을 선택하면 됩니다.

"나만의 스토리지 계정 생성에 대해 자세히 알아보세요".

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

   - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 서비스 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

     백업을 위한 Azure 대상이 콘솔의 시스템 페이지에 있는 경우 ONTAP 클러스터를 Azure Blob 개체 스토리지로 끌어다 놓을 수 있습니다.

   - 백업 및 복구 표시줄에서 *볼륨*을 선택합니다. 볼륨 탭에서 *작업*을 선택하세요. ••• 아이콘을 클릭하고 단일 볼륨(이미 복제나 개체 스토리지 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
   - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
   - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
   - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
   - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
   - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

  선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
   - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
   - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
   - 백업: 볼륨을 개체 스토리지에 백업합니다.
2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   - 계단식: 정보는 기본 저장소에서 보조 저장소로, 보조 저장소에서 개체 저장소로 흐릅니다.
   - 팬아웃: 정보는 기본 스토리지에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

     이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새 정책을 만듭니다.

   스냅샷을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

   정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
   - 정책의 이름을 입력하세요.
   - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
   - *만들기*를 선택하세요.
4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새 복제 정책을 만듭니다.

     복제를 활성화하기 전에 사용자 지정 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.
     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.
5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: *Microsoft Azure*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보와 백업이 저장될 지역을 입력하세요.

     새로운 저장 계정을 만들거나 기존 계정을 선택하세요.

     Blob 컨테이너를 관리하는 자체 리소스 그룹을 만들거나 리소스 그룹 유형과 그룹을 선택하세요.

     백업 파일이 수정되거나 삭제되는 것을 방지하려면 30일 보존 기간을 설정하고 변경 불가능한 저장소를 활성화하여 저장소 계정을 생성했는지 확인하세요.

추가적인 비용 최적화를 위해 이전 백업 파일을 Azure Archive Storage에 계층화하려면 스토리지 계정에 적절한 수명 주기 규칙이 있는지 확인하세요.

*자체 버킷 사용*을 선택하는 경우 백업 대상으로 생성하는 컨테이너의 이름이 Azure 스토리지 계정의 이름과 동일한지 확인하십시오.

- 암호화 키: 새 Azure Storage 계정을 만든 경우 공급자로부터 받은 암호화 키 정보를 입력합니다. 기본 Azure 암호화 키를 사용할지 아니면 Azure 계정에서 고객이 관리하는 키를 선택하여 데이터 암호화를 관리할지 선택하세요.

  고객이 직접 관리하는 키를 사용하기로 선택한 경우 키 보관소와 키 정보를 입력하세요.

  기존 Microsoft 저장소 계정을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

- 네트워킹: IP 공간을 선택하고 개인 엔드포인트를 사용할지 여부를 선택합니다. 개인 엔드포인트는 기본적으로 비활성화되어 있습니다.

  i. 백업하려는 볼륨이 있는 ONTAP 클러스터의 IP 공간입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.

  ii. 선택적으로, 이전에 구성한 Azure 개인 엔드포인트를 사용할지 여부를 선택합니다. "Azure 개인 엔드포인트 사용에 대해 알아보세요" .

- 백업 정책: 기존의 개체 스토리지 백업 정책을 선택하거나 새 정책을 만듭니다.

  백업을 활성화하기 전에 사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

  정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

  - 정책의 이름을 입력하세요.
  - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
  - 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .
  - *만들기*를 선택하세요.

- 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면

복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.

3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 스토리지 시스템 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 볼륨과 동기화됩니다.

입력한 리소스 그룹에 Blob 스토리지 계정이 생성되고 백업 파일이 해당 계정에 저장됩니다. 볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 데이터를 Google Cloud Storage에 백업하세요.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 온프레미스 기본 ONTAP 시스템의 볼륨 데이터를 보조 스토리지 시스템과 Google Cloud Storage로 백업하세요.

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

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

연결 방법을 식별하세요

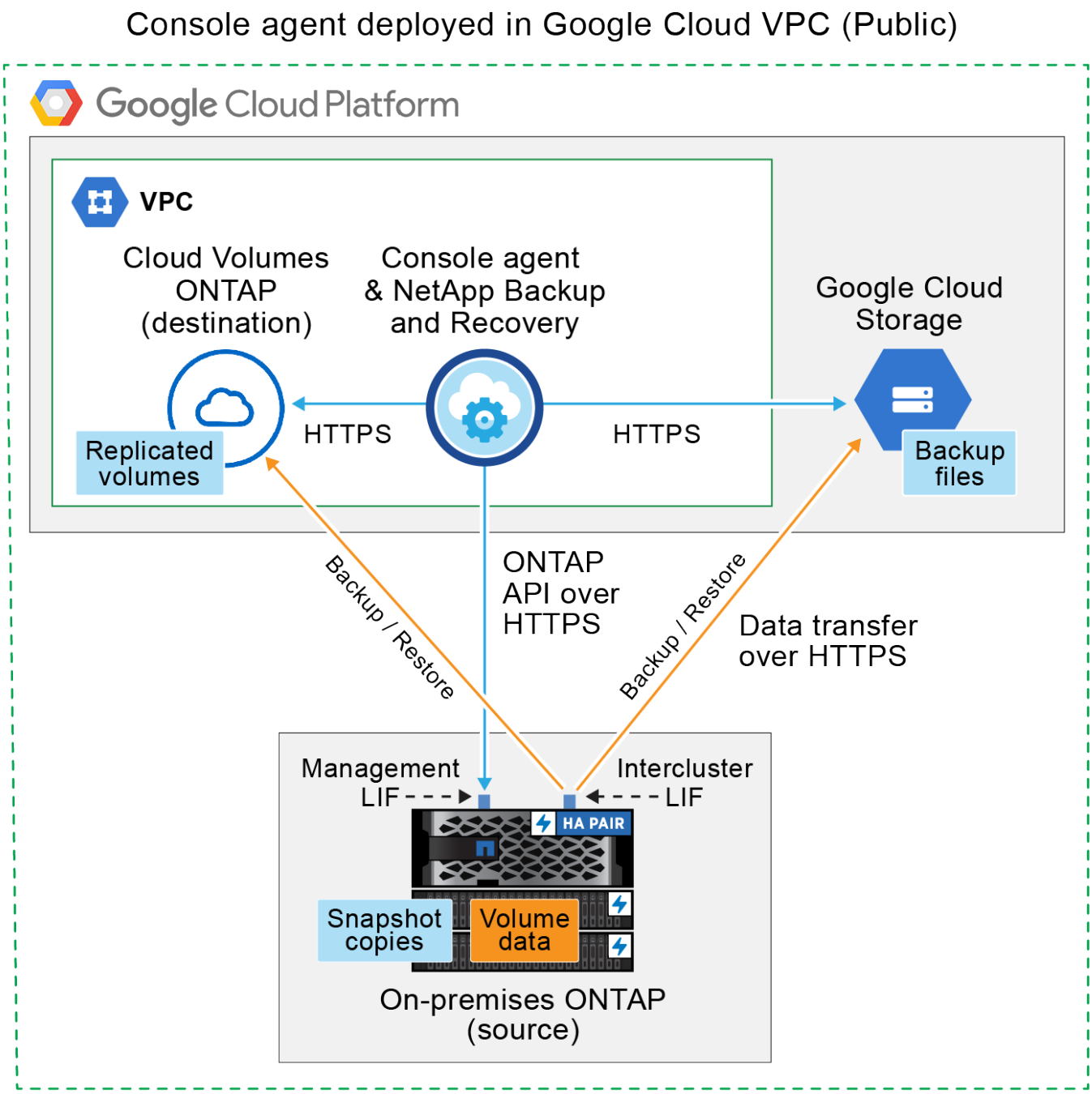
온프레미스 ONTAP 시스템에서 Google Cloud Storage로 백업을 구성할 때 두 가지 연결 방법 중 어떤 것을 사용할지 선택하세요.

- 공개 연결 - 공개 Google 엔드포인트를 사용하여 ONTAP 시스템을 Google Cloud Storage에 직접 연결합니다.
- 개인 연결 - VPN이나 Google Cloud Interconnect를 사용하고 개인 IP 주소를 사용하는 개인 Google 액세스 인터페이스를 통해 트래픽을 라우팅합니다.

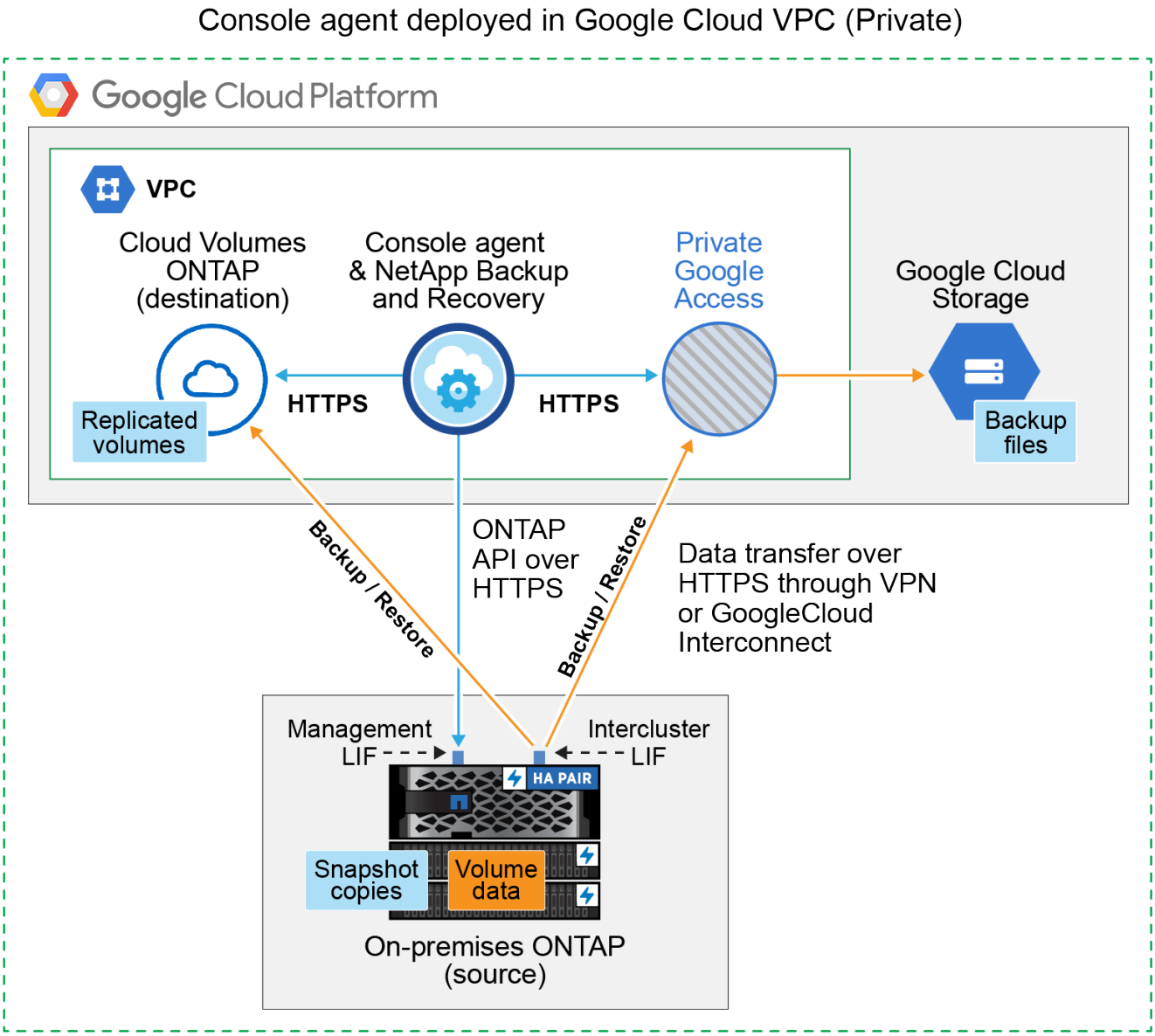
선택적으로, 공용 또는 개인 연결을 사용하여 복제된 볼륨의 보조 ONTAP 시스템에 연결할 수도 있습니다.

다음 다이어그램은 공개 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 콘솔 에이전트는 Google Cloud

Platform VPC에 배포되어야 합니다.



다음 다이어그램은 개인 연결 방법과 구성 요소 간에 준비해야 하는 연결을 보여줍니다. 콘솔 에이전트는 Google Cloud Platform VPC에 배포되어야 합니다.



콘솔 에이전트를 준비하세요

콘솔 에이전트는 콘솔 기능을 위한 주요 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 콘솔 에이전트가 필요합니다.

콘솔 에이전트 만들기 또는 전환

Google Cloud Platform VPC에 이미 콘솔 에이전트가 배포되어 있다면 준비가 완료된 것입니다.

그렇지 않은 경우 해당 위치에 콘솔 에이전트를 만들어 ONTAP 데이터를 Google Cloud Storage에 백업해야 합니다. 다른 클라우드 공급자나 온프레미스에 배포된 콘솔 에이전트는 사용할 수 없습니다.

- "콘솔 에이전트에 대해 알아보세요"
- "GCP에 콘솔 에이전트 설치"

콘솔 에이전트를 위한 네트워킹 준비

콘솔 에이전트에 필요한 네트워크 연결이 있는지 확인하세요.

단계

1. 콘솔 에이전트가 설치된 네트워크에서 다음 연결이 허용되는지 확인하세요.
   - 포트 443을 통해 NetApp Backup and Recovery 와 Google Cloud Storage에 HTTPS 연결("엔드포인트 목록을 확인하세요")
   - ONTAP 클러스터 관리 LIF에 대한 포트 443을 통한 HTTPS 연결
2. 콘솔 에이전트를 배포할 서브넷에서 Private Google Access(또는 Private Service Connect)를 활성화합니다. "비공개 Google 액세스" 또는 "프라이빗 서비스 커넥트" ONTAP 클러스터에서 VPC로 직접 연결되어 있고 콘솔 에이전트와 Google Cloud Storage 간 통신을 가상 사설망(비공개 연결)에 유지하려는 경우 필요합니다.

   이러한 비공개 액세스 옵션을 설정하려면 Google 지침을 따르세요. DNS 서버가 다음을 가리키도록 구성되었는지 확인하세요. `www.googleapis.com` 그리고 `storage.googleapis.com` 올바른 내부(개인) IP 주소로.

콘솔 에이전트에 대한 권한을 확인하거나 추가합니다.

NetApp Backup and Recovery "검색 및 복원" 기능을 사용하려면 콘솔 에이전트 역할에 대한 특정 권한이 있어야 Google Cloud BigQuery 서비스에 액세스할 수 있습니다. 아래 권한을 검토하고, 정책을 수정해야 하는 경우 단계에 따라 진행하세요.

단계

1. 에서 "구글 클라우드 콘솔" 역할 페이지로 이동합니다.
2. 페이지 상단의 드롭다운 목록을 사용하여 편집하려는 역할이 포함된 프로젝트나 조직을 선택합니다.
3. 사용자 지정 역할을 선택하세요.
4. 역할의 권한을 업데이트하려면 *역할 편집*을 선택하세요.
5. *권한 추가*를 선택하여 역할에 다음과 같은 새로운 권한을 추가합니다.

```
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. 편집한 역할을 저장하려면 *업데이트*를 선택하세요.

라이센스 요구 사항 확인

- 클러스터에 대한 NetApp Backup and Recovery 활성화하려면 먼저 Google에서 제공하는 PAYGO(Pay-as-you-go) 콘솔 마켓플레이스에 가입하거나 NetApp 에서 NetApp Backup and Recovery BYOL 라이선스를 구매하여 활성화해야 합니다. 이러한 라이선스는 귀하의 계정에 적용되며 여러 시스템에서 사용할 수 있습니다.
  - NetApp Backup and Recovery PAYGO 라이선싱의 경우 구독이 필요합니다. "Google Marketplace에서 제공하는 NetApp Console" . NetApp Backup and Recovery 대한 청구는 이 구독을 통해 이루어집니다.
  - NetApp Backup and Recovery BYOL 라이선스의 경우, 라이선스 기간과 용량 동안 서비스를 사용할 수 있도록 하는 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요".
- 백업이 저장될 개체 저장 공간에 대한 Google 구독이 필요합니다.

지원 지역

모든 지역의 온프레미스 시스템에서 Google Cloud Storage로 백업을 생성할 수 있습니다. 서비스를 설정할 때 백업을 저장할 지역을 지정합니다.

ONTAP 클러스터 준비

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템을 준비합니다.

ONTAP 클러스터를 준비하는 단계는 다음과 같습니다.

- NetApp Console 에서 ONTAP 시스템을 찾아보세요
- ONTAP 시스템 요구 사항 확인
- 개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인
- 볼륨 복제를 위한 ONTAP 네트워킹 요구 사항 확인

NetApp Console 에서 ONTAP 시스템을 찾아보세요

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템 모두 NetApp Console 시스템 페이지에서 사용할 수 있어야 합니다.

클러스터를 추가하려면 클러스터 관리 IP 주소와 관리자 사용자 계정의 비밀번호를 알아야 합니다. "클러스터를 검색하는 방법을 알아보세요".

ONTAP 시스템 요구 사항 확인

ONTAP 시스템이 다음 요구 사항을 충족하는지 확인하세요.

- 최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됨).

  참고: NetApp Backup and Recovery 사용하는 경우 "하이브리드 클라우드 번들"은 필요하지 않습니다.

  방법을 배우십시오 "클러스터 라이선스 관리" .
- 시간과 시간대가 올바르게 설정되었습니다. 방법을 배우십시오 "클러스터 시간 구성" .
- 데이터를 복제하는 경우 소스 및 대상 시스템이 호환되는 ONTAP 버전을 실행하는지 확인하세요.

"SnapMirror 관계에 대한 호환 ONTAP 버전 보기".

개체 스토리지에 데이터를 백업하기 위한 **ONTAP** 네트워킹 요구 사항 확인

개체 스토리지에 연결하는 시스템에서 다음 요구 사항을 구성해야 합니다.

- 팬아웃 백업 아키텍처의 경우 기본 시스템에서 다음 설정을 구성합니다.
- 계단식 백업 아키텍처의 경우 보조 시스템에서 다음 설정을 구성합니다.

다음과 같은 ONTAP 클러스터 네트워킹 요구 사항이 필요합니다.

- ONTAP 클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 포트 443을 통해 Google Cloud Storage로 HTTPS 연결을 시작합니다.

  ONTAP 객체 스토리지에서 데이터를 읽고 씁니다. 객체 스토리지는 결코 시작되지 않고, 단지 응답만 합니다.

- ONTAP 콘솔 에이전트에서 클러스터 관리 LIF로의 인바운드 연결이 필요합니다. 콘솔 에이전트는 Google Cloud Platform VPC에 상주할 수 있습니다.
- 백업하려는 볼륨을 호스팅하는 각 ONTAP 노드에는 클러스터 간 LIF가 필요합니다. LIF는 ONTAP 개체 스토리지에 연결하는 데 사용해야 하는 _IPspace_와 연결되어야 합니다. "IPspaces에 대해 자세히 알아보세요" .

  NetApp Backup and Recovery 설정하면 사용할 IP 공간을 입력하라는 메시지가 표시됩니다. 각 LIF가 연결된 IP 공간을 선택해야 합니다. 이는 "기본" IP 공간일 수도 있고 사용자가 만든 사용자 지정 IP 공간일 수도 있습니다.

- 노드의 클러스터 간 LIF는 객체 저장소에 액세스할 수 있습니다.
- 볼륨이 위치한 스토리지 VM에 대한 DNS 서버가 구성되었습니다. 방법을 확인하세요 "SVM에 대한 DNS 서비스 구성" .

  Private Google Access 또는 Private Service Connect를 사용하는 경우 DNS 서버가 다음을 가리키도록 구성되었는지 확인하세요. `storage.googleapis.com` 올바른 내부(개인) IP 주소로.

- 기본 IP 공간과 다른 IP 공간을 사용하는 경우 개체 스토리지에 액세스하려면 정적 경로를 만들어야 할 수도 있습니다.
- 필요한 경우 방화벽 규칙을 업데이트하여 ONTAP 에서 포트 443을 통해 개체 스토리지로 NetApp Backup and Recovery 연결을 허용하고, 스토리지 VM에서 포트 53(TCP/UDP)을 통해 DNS 서버로 이름 확인 트래픽을 허용합니다.

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.

Google Cloud Storage를 백업 대상으로 준비하세요

Google Cloud Storage를 백업 대상으로 준비하려면 다음 단계를 따르세요.

- 권한을 설정합니다.
- (선택 사항) 나만의 버킷을 만드세요. (원하시면 서비스에서 버킷을 만들어드립니다.)
- (선택 사항) 데이터 암호화를 위한 고객 관리 키 설정

권한 설정

사용자 지정 역할을 사용하여 특정 권한이 있는 서비스 계정에 대한 저장소 액세스 키를 제공해야 합니다. 서비스 계정을 사용하면 NetApp Backup and Recovery 백업을 저장하는 데 사용되는 Cloud Storage 버킷을 인증하고 액세스할 수 있습니다. Google Cloud Storage에서 누가 요청하는지 알 수 있도록 키가 필요합니다.

단계

1. 에서 "구글 클라우드 콘솔" 역할 페이지로 이동합니다.
2. "새로운 역할 만들기"다음 권한이 필요합니다.

```
storage.buckets.create
storage.buckets.delete
storage.buckets.get
storage.buckets.list
storage.buckets.update
storage.buckets.getIamPolicy
storage.multipartUploads.create
storage.objects.create
storage.objects.delete
storage.objects.get
storage.objects.list
storage.objects.update
```

3. Google Cloud 콘솔에서 "서비스 계정 페이지로 이동" .
4. 클라우드 프로젝트를 선택하세요.
5. *서비스 계정 만들기*를 선택하고 필요한 정보를 제공합니다.
   a. 서비스 계정 세부 정보: 이름과 설명을 입력하세요.
   b. 이 서비스 계정에 프로젝트에 대한 액세스 권한 부여: 방금 만든 사용자 지정 역할을 선택합니다.
   c. *완료*를 선택하세요.
6. 로 가다 "GCP 스토리지 설정" 서비스 계정에 대한 액세스 키를 생성합니다.

a. 프로젝트를 선택하고 *상호운용성*을 선택하세요. 아직 선택하지 않았다면 *상호 운용성 액세스 활성화*를 선택하세요.

b. *서비스 계정용 액세스 키*에서 *서비스 계정용 키 만들기*를 선택하고 방금 만든 서비스 계정을 선택한 다음 *키 만들기*를 클릭합니다.

   나중에 백업 서비스를 구성할 때 NetApp Backup and Recovery 에 키를 입력해야 합니다.

나만의 버킷을 만들어보세요

기본적으로 서비스는 사용자를 위해 버킷을 생성합니다. 또는, 사용자 고유의 버킷을 사용하려면 백업 활성화 마법사를 시작하기 전에 버킷을 만든 다음 마법사에서 해당 버킷을 선택하면 됩니다.

"나만의 버킷을 만드는 방법에 대해 자세히 알아보세요".

데이터 암호화를 위한 고객 관리 암호화 키**(CMEK)** 설정

기본 Google 관리 암호화 키 대신 고객이 관리하는 키를 사용하여 데이터를 암호화할 수 있습니다. 지역 간 키와 프로젝트 간 키가 모두 지원되므로 CMEK 키의 프로젝트와 다른 버킷의 프로젝트를 선택할 수 있습니다.

고객이 직접 관리하는 키를 사용하려는 경우:

- 활성화 마법사에 이 정보를 추가하려면 키 링과 키 이름이 필요합니다. "고객 관리 암호화 키에 대해 자세히 알아보세요" .
- 콘솔 에이전트 역할에 다음과 같은 필수 권한이 포함되어 있는지 확인해야 합니다.

```
cloudkms.cryptoKeys.get
cloudkms.cryptoKeys.getIamPolicy
cloudkms.cryptoKeys.list
cloudkms.cryptoKeys.setIamPolicy
cloudkms.keyRings.get
cloudkms.keyRings.getIamPolicy
cloudkms.keyRings.list
cloudkms.keyRings.setIamPolicy
```

- 프로젝트에서 Google "Cloud Key Management Service(KMS)" API가 활성화되어 있는지 확인해야 합니다. 를 참조하십시오 "Google Cloud 문서: API 활성화" 자세한 내용은.

CMEK 고려 사항**:**

- HSM(하드웨어 지원)과 소프트웨어 생성 키가 모두 지원됩니다.
- 새로 생성한 Cloud KMS 키나 가져온 Cloud KMS 키가 모두 지원됩니다.
- 지역 키만 지원되고 글로벌 키는 지원되지 않습니다.
- 현재는 "대칭 암호화/복호화" 목적만 지원됩니다.
- 스토리지 계정과 연결된 서비스 에이전트에는 NetApp Backup and Recovery 에서 "CryptoKey 암호화/복호화(roles/cloudkms.cryptoKeyEncrypterDecrypter)" IAM 역할이 할당됩니다.

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

    - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

      백업을 위한 Google Cloud Storage 대상이 콘솔의 시스템 페이지에 있는 경우 ONTAP 클러스터를 Google Cloud 개체 스토리지로 끌어다 놓을 수 있습니다.

    - 백업 및 복구 표시줄에서 *볼륨*을 선택합니다. 볼륨 탭에서 *작업*을 선택하세요. ••• 아이콘을 클릭하고 단일 볼륨(이미 복제나 개체 스토리지 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

    마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.

    - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
    - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
    - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
    - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
    - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
    - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
    - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
    - 백업: 볼륨을 개체 스토리지에 백업합니다.
2. 아키텍처: 복제 및 백업을 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
    - 계단식: 정보는 기본 저장소에서 보조 저장소로, 보조 저장소에서 개체 저장소로 흐릅니다.
    - 팬아웃: 정보는 기본 스토리지에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

    이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새 정책을 만듭니다.

사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

- 정책의 이름을 입력하세요.
- 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
- *만들기*를 선택하세요.

4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새 복제 정책을 만듭니다.

     사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.
5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: *Google Cloud*를 선택하세요.
   - 공급자 설정: 공급자 세부 정보와 백업이 저장될 지역을 입력하세요.

     새로운 버킷을 만들거나 이미 만든 버킷을 선택하세요.

     추가적인 비용 최적화를 위해 이전 백업 파일을 Google Cloud Archive 스토리지에 계층화하려면 버킷에 적절한 수명 주기 규칙이 있는지 확인하세요.

     Google Cloud 액세스 키와 비밀 키를 입력하세요.
   - 암호화 키: 새로운 Google Cloud Storage 계정을 만든 경우 공급업체에서 제공한 암호화 키 정보를 입력하세요. 데이터 암호화를 관리하기 위해 기본 Google Cloud 암호화 키를 사용할지, 아니면 Google Cloud 계정에서 고객이 관리하는 키를 선택할지 선택하세요.

     기존 Google Cloud 스토리지 계정을 선택한 경우 암호화 정보가 이미 제공되므로 지금 입력할 필요가 없습니다.

     고객이 직접 관리하는 키를 사용하려면 키 링과 키 이름을 입력하세요. "고객 관리 암호화 키에 대해 자세히 알아보세요" .
   - 네트워킹: IP 공간을 선택하세요.

     백업하려는 볼륨이 있는 ONTAP 클러스터의 IP 공간입니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다.
   - 백업 정책: 기존의 개체 스토리지 백업 정책을 선택하거나 새 정책을 만듭니다.

     사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.

        - *만들기*를 선택하세요.
    - 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.
6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준 전송에는 기본 스토리지 시스템 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 스토리지 시스템 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 소스 볼륨과 동기화됩니다.

입력한 Google 액세스 키와 비밀 키로 지정된 서비스 계정에 Google Cloud Storage 버킷이 자동으로 생성되고, 백업 파일이 해당 버킷에 저장됩니다. 볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 데이터를 ONTAP S3에 백업

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 기본 온프레미스 ONTAP 시스템에서 볼륨 데이터 백업을 시작하세요. 백업을 보조 ONTAP 스토리지 시스템(복제된 볼륨)이나 S3 서버로 구성된 ONTAP 시스템의 버킷(백업 파일) 또는 둘 다에 보낼 수 있습니다.

기본 온프레미스 ONTAP 시스템은 FAS, AFF 또는 ONTAP Select 시스템이 될 수 있습니다. 보조 ONTAP 시스템은 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템이 될 수 있습니다. 개체 저장소는 온프레미스 ONTAP

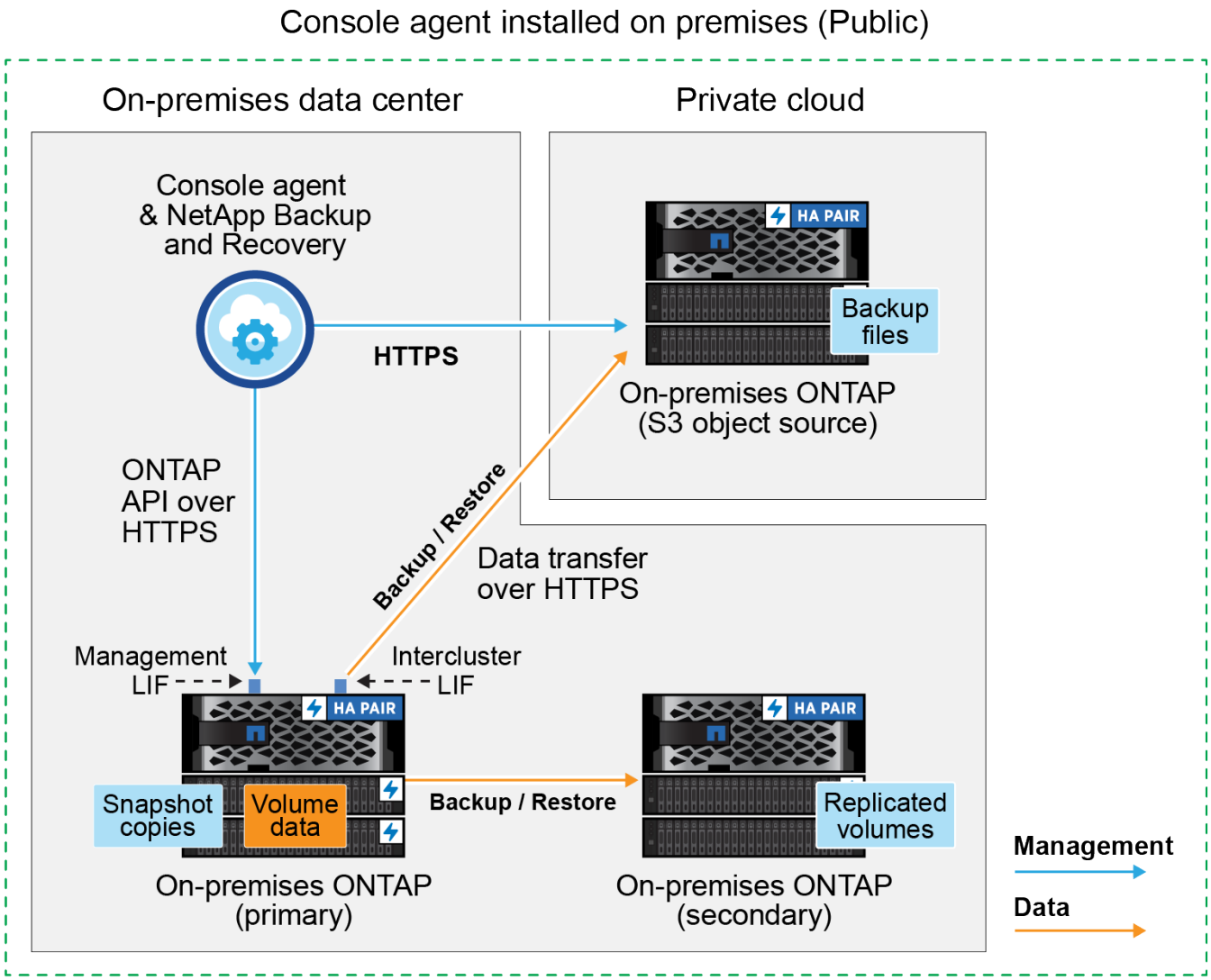
시스템이나 S3(Simple Storage Service) 개체 저장소 서버를 활성화한 Cloud Volumes ONTAP 시스템에 있을 수 있습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

연결 방법을 식별하세요

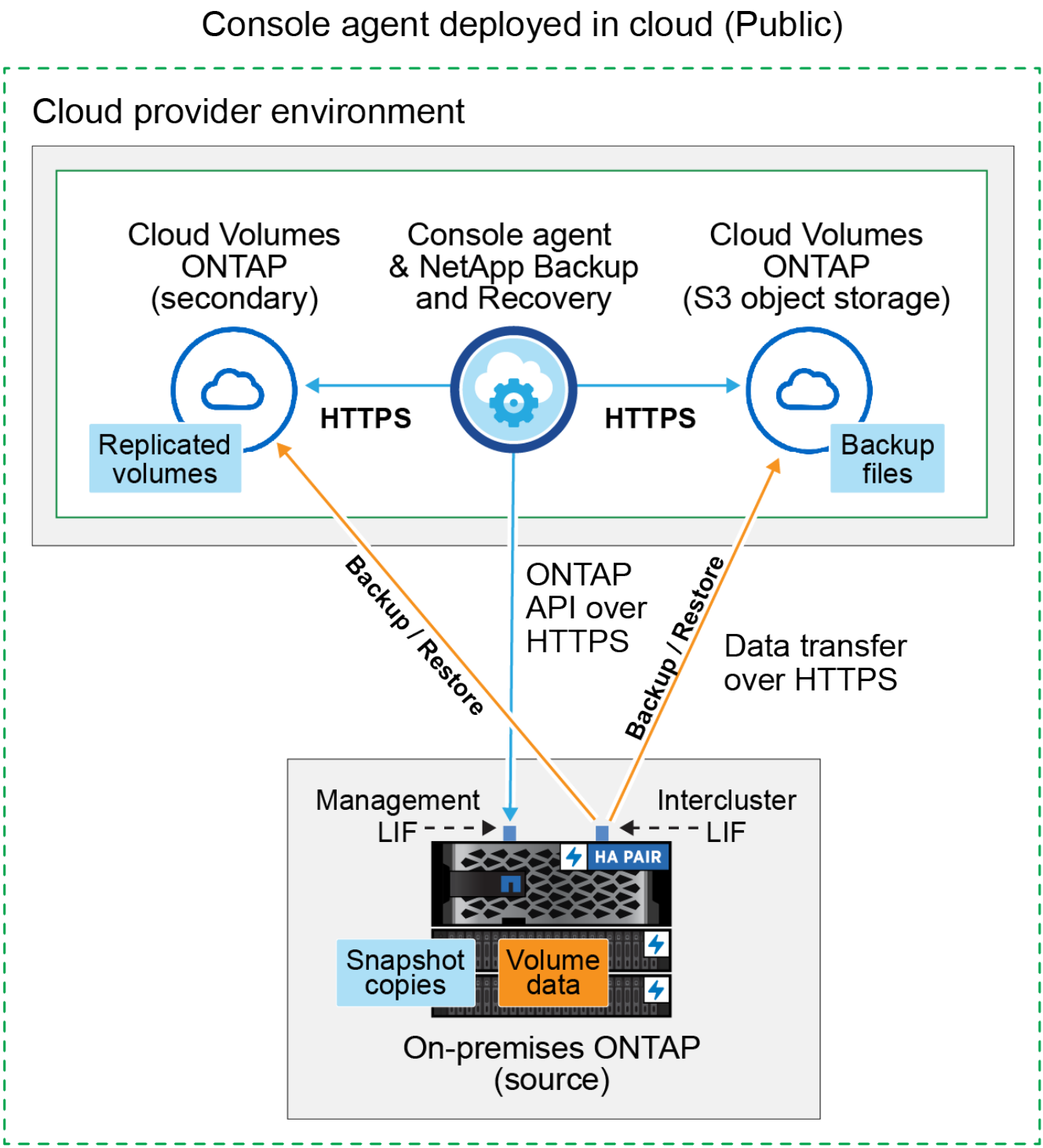
ONTAP 시스템의 S3 버킷에 백업을 생성할 수 있는 구성은 다양합니다. 아래에 두 가지 시나리오가 나와 있습니다.

다음 이미지는 S3에 대해 구성된 온프레미스 ONTAP 시스템에 기본 온프레미스 ONTAP 시스템을 백업할 때의 각 구성 요소와 이들 간에 준비해야 하는 연결을 보여줍니다. 또한 볼륨을 복제하기 위해 동일한 온프레미스 위치에 있는 보조 ONTAP 시스템에 대한 연결을 보여줍니다.



콘솔 에이전트와 기본 온프레미스 ONTAP 시스템이 인터넷 접속이 불가능한 온프레미스 위치에 설치된 경우("개인" 모드 배포), ONTAP S3 시스템은 동일한 온프레미스 데이터 센터에 있어야 합니다.

다음 이미지는 S3에 대해 구성된 Cloud Volumes ONTAP 시스템에 기본 온프레미스 ONTAP 시스템을 백업할 때의 각 구성 요소와 이들 간에 준비해야 하는 연결을 보여줍니다. 또한 동일한 클라우드 공급자 환경의 보조 Cloud Volumes ONTAP 시스템에 연결하여 볼륨을 복제하는 모습도 보여줍니다.



이 시나리오에서는 콘솔 에이전트는 Cloud Volumes ONTAP 시스템이 배포된 동일한 클라우드 공급자 환경에 배포되어야 합니다.

콘솔 에이전트를 준비하세요

콘솔 에이전트는 콘솔 기능을 위한 주요 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 콘솔 에이전트가 필요합니다.

콘솔 에이전트 만들기 또는 전환

ONTAP S3에 데이터를 백업하는 경우, 사내 또는 클라우드에서 콘솔 에이전트를 사용할 수 있어야 합니다. 새로운 콘솔 에이전트를 설치하거나 현재 선택된 콘솔 에이전트가 이러한 위치 중 하나에 있는지 확인해야 합니다. 온프레미스 콘솔 에이전트는 인터넷 접속이 가능한 사이트나 불가능한 사이트에 설치할 수 있습니다.

- "콘솔 에이전트에 대해 알아보세요"
- "클라우드 환경에 콘솔 에이전트를 설치하세요"
- "인터넷 접속이 가능한 Linux 호스트에 콘솔 에이전트 설치"
- "인터넷 접속이 없는 Linux 호스트에 콘솔 에이전트 설치"
- "콘솔 에이전트 간 전환"

콘솔 에이전트 네트워킹 요구 사항 준비

콘솔 에이전트가 설치된 네트워크에서 다음 연결이 허용되는지 확인하세요.

- ONTAP S3 서버에 대한 포트 443을 통한 HTTPS 연결
- 포트 443을 통한 소스 ONTAP 클러스터 관리 LIF에 대한 HTTPS 연결
- 포트 443을 통한 NetApp Backup and Recovery 로의 아웃바운드 인터넷 연결(콘솔 에이전트가 "다크" 사이트에 설치된 경우 필요하지 않음)

개인 모드(다크 사이트) 고려 사항

NetApp Backup and Recovery 기능은 콘솔 에이전트에 내장되어 있습니다. 개인 모드로 설치하는 경우 새로운 기능을 사용하려면 콘솔 에이전트 소프트웨어를 주기적으로 업데이트해야 합니다. 확인하다"NetApp Backup and Recovery의 새로운 기능" NetApp Backup and Recovery 각 릴리스에서 새로운 기능을 확인하세요. 새로운 기능을 사용하려면 다음 단계를 따르세요. "콘솔 에이전트 소프트웨어 업그레이드" .

표준 SaaS 환경에서 NetApp Backup and Recovery 사용하면 NetApp Backup and Recovery 구성 데이터가 클라우드에 백업됩니다. 인터넷 접속이 없는 사이트에서 NetApp Backup and Recovery 사용하는 경우 NetApp Backup and Recovery 구성 데이터는 백업이 저장되는 ONTAP S3 버킷에 백업됩니다.

라이센스 요구 사항 확인

클러스터에 대한 NetApp Backup and Recovery 활성화하려면 먼저 NetApp 에서 NetApp Backup and Recovery BYOL 라이선스를 구매하고 활성화해야 합니다. 라이선스는 개체 스토리지에 대한 백업 및 복원을 위한 것이며, 스냅샷이나 복제 볼륨을 생성하는 데는 라이선스가 필요하지 않습니다. 이 라이선스는 해당 계정에 대한 것이며 여러 시스템에서 사용할 수 있습니다.

라이선스 기간과 용량에 맞춰 서비스를 사용하려면 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요".

ONTAP S3에 파일을 백업하는 경우 PAYGO 라이선싱이 지원되지 않습니다.

ONTAP 클러스터 준비

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템을 준비합니다.

ONTAP 클러스터를 준비하는 단계는 다음과 같습니다.

- NetApp Console 에서 ONTAP 시스템을 찾아보세요
- ONTAP 시스템 요구 사항 확인
- 개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인
- 볼륨 복제를 위한 ONTAP 네트워킹 요구 사항 확인

NetApp Console 에서 **ONTAP** 시스템을 찾아보세요

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템 모두 NetApp Console 시스템 페이지에서 사용할 수 있어야 합니다.

클러스터를 추가하려면 클러스터 관리 IP 주소와 관리자 사용자 계정의 비밀번호를 알아야 합니다. "클러스터를 검색하는 방법을 알아보세요".

ONTAP 시스템 요구 사항 확인

ONTAP 시스템이 다음 요구 사항을 충족하는지 확인하세요.

- 최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됨).

  참고: NetApp Backup and Recovery 사용하는 경우 "하이브리드 클라우드 번들"은 필요하지 않습니다.

  방법을 배우십시오 "클러스터 라이선스 관리" .
- 시간과 시간대가 올바르게 설정되었습니다. 방법을 배우십시오 "클러스터 시간 구성" .
- 데이터를 복제하는 경우 소스 및 대상 시스템이 호환되는 ONTAP 버전을 실행하는지 확인하세요.

  "SnapMirror 관계에 대한 호환 ONTAP 버전 보기".

개체 스토리지에 데이터를 백업하기 위한 **ONTAP** 네트워킹 요구 사항 확인

개체 스토리지에 연결하는 시스템에서 다음 요구 사항이 충족되는지 확인해야 합니다.

- 팬아웃 백업 아키텍처를 사용하는 경우 설정은 기본 스토리지 시스템에서 구성해야 합니다.
- 계단식 백업 아키텍처를 사용하는 경우 설정은 보조 스토리지 시스템에서 구성해야 합니다.

  "백업 아키텍처 유형에 대해 자세히 알아보세요".

다음과 같은 ONTAP 클러스터 네트워킹 요구 사항이 필요합니다.

- ONTAP 클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 ONTAP S3 서버로 사용자가 지정한 포트를 통해 HTTPS 연결을 시작합니다. 포트는 백업 설정 중에 구성할 수 있습니다.

  ONTAP 객체 스토리지에서 데이터를 읽고 씁니다. 객체 스토리지는 결코 시작되지 않고, 단지 응답만 합니다.
- ONTAP 콘솔 에이전트에서 클러스터 관리 LIF로의 인바운드 연결이 필요합니다.
- 백업하려는 볼륨을 호스팅하는 각 ONTAP 노드에는 클러스터 간 LIF가 필요합니다. LIF는 ONTAP 개체

스토리지에 연결하는 데 사용해야 하는 _IPspace_와 연결되어야 합니다. "IPspaces에 대해 자세히 알아보세요" .

NetApp Backup and Recovery 설정하면 사용할 IP 공간을 입력하라는 메시지가 표시됩니다. 각 LIF가 연결된 IP 공간을 선택해야 합니다. 이는 "기본" IP 공간일 수도 있고 사용자가 만든 사용자 지정 IP 공간일 수도 있습니다.

- 노드의 클러스터 간 LIF는 개체 저장소에 액세스할 수 있습니다(콘솔 에이전트가 "다크" 사이트에 설치된 경우에는 필요하지 않음).
- 볼륨이 위치한 스토리지 VM에 대한 DNS 서버가 구성되었습니다. 방법을 확인하세요 "SVM에 대한 DNS 서비스 구성" .
- 기본 IP 공간과 다른 IP 공간을 사용하는 경우 개체 스토리지에 액세스하려면 정적 경로를 만들어야 할 수도 있습니다.
- 필요한 경우 방화벽 규칙을 업데이트하여 ONTAP 에서 개체 스토리지로의 NetApp Backup and Recovery 서비스 연결을 지정한 포트(일반적으로 포트 443)를 통해 허용하고, 스토리지 VM에서 DNS 서버로의 이름 확인 트래픽을 포트 53(TCP/UDP)을 통해 허용합니다.

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.

ONTAP S3를 백업 대상으로 준비하세요

개체 스토리지 백업에 사용할 ONTAP 클러스터에서 S3(Simple Storage Service) 개체 스토리지 서버를 활성화해야 합니다. 를 참조하십시오 "ONTAP S3 문서" 자세한 내용은.

참고**:** 이 클러스터를 콘솔 시스템 페이지에 추가할 수 있지만, S3 개체 스토리지 서버로 식별되지 않으며, 이 S3 시스템에 소스 시스템을 끌어서 놓아 백업 활성화를 시작할 수 없습니다.

이 ONTAP 시스템은 다음 요구 사항을 충족해야 합니다.

지원되는 **ONTAP** 버전

온프레미스 ONTAP 시스템에는 ONTAP 9.8 이상이 필요합니다. Cloud Volumes ONTAP 시스템에는 ONTAP 9.9.1 이상이 필요합니다.

S3 자격 증명

ONTAP S3 스토리지에 대한 액세스를 제어하려면 S3 사용자를 생성해야 합니다. "자세한 내용은 ONTAP S3 문서를 참조하세요." .

ONTAP S3에 대한 백업을 설정하면 백업 마법사가 사용자 계정에 대한 S3 액세스 키와 비밀 키를 입력하라는 메시지를 표시합니다. 사용자 계정을 통해 NetApp Backup and Recovery ONTAP S3 버킷을 인증하고 백업을 저장하는 데 사용되는 버킷에 액세스할 수 있습니다. ONTAP S3에서 누가 요청하는지 알 수 있도록 키가 필요합니다.

이러한 액세스 키는 다음 권한이 있는 사용자와 연결되어야 합니다.

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

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 및 정책 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.
   - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.
   - 백업 및 복구 표시줄에서 볼륨*을 선택합니다. 볼륨 탭에서 *작업(...) 옵션을 선택하고 단일 볼륨(복제 또는 개체 저장소로의 백업이 아직 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

   마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.
   - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.

◦ 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 스냅샷 정책, 복제 정책, 개체 정책에 대한 백업 중 하나 이상을 갖춘 볼륨입니다.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
   ◦ 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
   ◦ 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
   ◦ 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 구성해야 합니다.

- 보호 옵션: 로컬 스냅샷, 복제, 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 구현할지 여부
- 아키텍처: 팬아웃 또는 계단식 백업 아키텍처를 사용할지 여부
- 로컬 스냅샷 정책
- 복제 대상 및 정책
- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
   ◦ 로컬 스냅샷: 로컬 스냅샷을 생성합니다.
   ◦ 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
   ◦ 백업: S3에 대해 구성된 ONTAP 시스템의 버킷에 볼륨을 백업합니다.
2. 아키텍처: 복제와 백업을 모두 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
   ◦ 계단식: 백업 데이터는 기본 시스템에서 보조 시스템으로 흐르고, 보조 시스템에서 개체 스토리지로 흐릅니다.

- 팬아웃: 백업 데이터는 기본 시스템에서 보조 시스템으로 흐르고, 기본 시스템에서 개체 스토리지로 흐릅니다.

  이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .

3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새 정책을 만듭니다.

   스냅샷을 활성화하기 전에 사용자 정의 정책을 만들려면 시스템 관리자 또는 ONTAP CLI를 사용할 수 있습니다. `snapmirror policy create` 명령. 참조하다 .

   백업 및 복구를 사용하여 사용자 지정 정책을 만들려면 다음을 참조하세요."정책 만들기" .

   정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

   - 정책의 이름을 입력하세요.
   - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
   - *만들기*를 선택하세요.

4. 복제: *복제*를 선택한 경우 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 대상 집계(FlexGroup 볼륨의 집계)와 복제된 볼륨 이름에 추가할 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새 복제 정책을 만듭니다.

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.

5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: * ONTAP S3*를 선택하세요.
   - 공급자 설정: S3 서버 FQDN 세부 정보, 포트, 사용자의 액세스 키와 비밀 키를 입력합니다.

     액세스 키와 비밀 키는 ONTAP 클러스터에 S3 버킷에 대한 액세스 권한을 부여하기 위해 생성한 사용자를 위한 것입니다.

   - 네트워킹: 백업하려는 볼륨이 있는 소스 ONTAP 클러스터의 IP 공간을 선택합니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다(콘솔 에이전트가 "다크" 사이트에 설치된 경우에는 필요하지 않음).

     올바른 IP 공간을 선택하면 NetApp Backup and Recovery ONTAP 에서 ONTAP S3 개체 스토리지로의 연결을 설정할 수 있습니다.

   - 백업 정책: 기존 백업 정책을 선택하거나 새 백업 정책을 만듭니다.

     System Manager나 ONTAP CLI를 사용하여 정책을 만들 수 있습니다. ONTAP CLI를 사용하여 사용자 정의 정책을 생성하려면 `snapmirror policy create` 명령, 참조 .

백업 및 복구를 사용하여 사용자 지정 정책을 만들려면 다음을 참조하세요."정책 만들기" .

정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

- 정책의 이름을 입력하세요.
- 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
- 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .
- *만들기*를 선택하세요.

◦ 기존 스냅샷을 백업 파일로 개체 스토리지로 내보내기: 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 이 시스템의 볼륨에 대한 로컬 스냅샷이 있는 경우 이 추가 메시지가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다. 정책이 일치하지 않으면 백업이 생성되지 않습니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준선 전송에는 소스 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 저장소 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 저장소 볼륨과 동기화됩니다.

입력한 S3 액세스 키와 비밀 키로 지정된 서비스 계정에 S3 버킷이 생성되고, 백업 파일이 해당 버킷에 저장됩니다.

볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 사용하여 온프레미스 ONTAP 데이터를 StorageGRID 에 백업합니다.

NetApp Backup and Recovery 에서 몇 가지 단계를 완료하여 온프레미스 기본 ONTAP 시스템의 볼륨 데이터를 보조 스토리지 시스템과 NetApp StorageGRID 시스템의 개체 스토리지로 백업을 시작하세요.

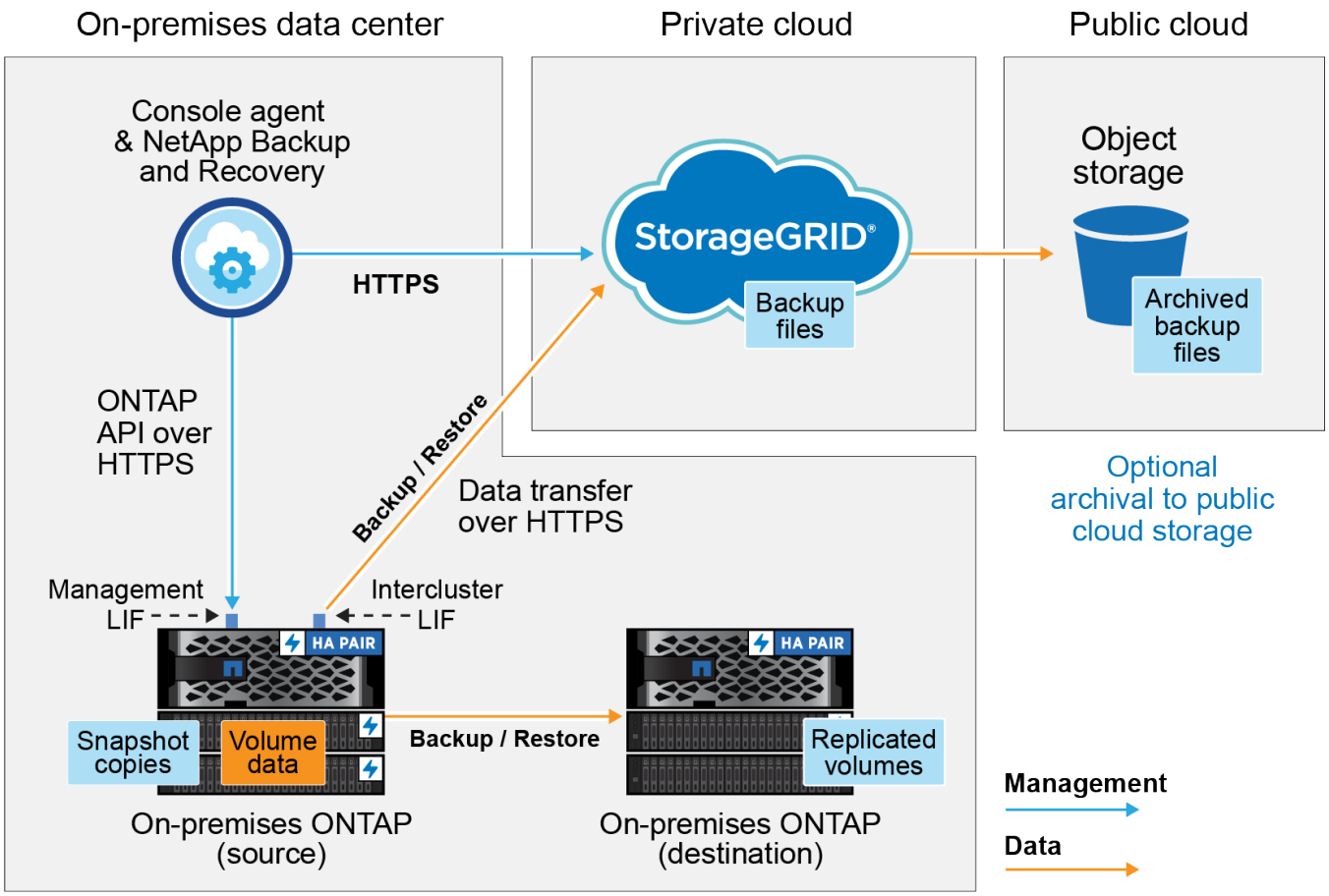
"온프레미스 ONTAP 시스템"에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

연결 방법을 식별하세요

다음 이미지는 온프레미스 ONTAP 시스템을 StorageGRID 에 백업할 때 필요한 각 구성 요소와 이들 간에 준비해야 하는 연결을 보여줍니다.

선택적으로 동일한 온프레미스 위치에 있는 보조 ONTAP 시스템에 연결하여 볼륨을 복제할 수 있습니다.



콘솔 에이전트와 온프레미스 ONTAP 시스템이 인터넷 접속이 불가능한 온프레미스 위치(다크 사이트)에 설치된 경우, StorageGRID 시스템은 동일한 온프레미스 데이터 센터에 위치해야 합니다. 다크 사이트 구성에서는 이전 백업 파일을 퍼블릭 클라우드에 보관하는 기능이 지원되지 않습니다.

콘솔 에이전트를 준비하세요

콘솔 에이전트는 콘솔 기능을 위한 주요 소프트웨어입니다. ONTAP 데이터를 백업하고 복원하려면 콘솔 에이전트가 필요합니다.

콘솔 에이전트 만들기 또는 전환

StorageGRID 에 데이터를 백업하는 경우, 사내에서 콘솔 에이전트를 사용할 수 있어야 합니다. 새로운 콘솔 에이전트를 설치하거나 현재 선택된 콘솔 에이전트가 온프레미스에 있는지 확인해야 합니다. 콘솔 에이전트는 인터넷 접속이 가능한 사이트나 불가능한 사이트에 설치할 수 있습니다.

- "콘솔 에이전트에 대해 알아보세요"
- "인터넷 접속이 가능한 Linux 호스트에 콘솔 에이전트 설치"
- "인터넷 접속이 없는 Linux 호스트에 콘솔 에이전트 설치"
- "콘솔 에이전트 간 전환"

콘솔 에이전트 네트워킹 요구 사항 준비

콘솔 에이전트가 설치된 네트워크에서 다음 연결이 허용되는지 확인하세요.

- StorageGRID Gateway 노드에 대한 포트 443을 통한 HTTPS 연결
- ONTAP 클러스터 관리 LIF에 대한 포트 443을 통한 HTTPS 연결
- 포트 443을 통한 NetApp Backup and Recovery 로의 아웃바운드 인터넷 연결(콘솔 에이전트가 "다크" 사이트에 설치된 경우 필요하지 않음)

개인 모드(다크 사이트) 고려 사항

- NetApp Backup and Recovery 기능은 콘솔 에이전트에 내장되어 있습니다. 개인 모드로 설치하는 경우 새로운 기능을 사용하려면 콘솔 에이전트 소프트웨어를 주기적으로 업데이트해야 합니다. 확인하다"NetApp Backup and Recovery 의 새로운 기능" NetApp Backup and Recovery 각 릴리스에서 새로운 기능을 확인하세요. 새로운 기능을 사용하려면 다음 단계를 따르세요. "콘솔 에이전트 소프트웨어 업그레이드" .

  스냅샷과 복제된 볼륨을 예약하고 생성하는 기능, 개체 스토리지에 대한 백업을 생성하는 기능이 포함된 새로운 버전의 NetApp Backup and Recovery 사용하려면 콘솔 에이전트 버전 3.9.31 이상을 사용해야 합니다. 따라서 모든 백업을 관리하려면 이 최신 릴리스를 사용하는 것이 좋습니다.

- SaaS 환경에서 NetApp Backup and Recovery 사용하면 NetApp Backup and Recovery 구성 데이터가 클라우드에 백업됩니다. 인터넷 접속이 없는 사이트에서 NetApp Backup and Recovery 사용하는 경우 NetApp Backup and Recovery 구성 데이터는 백업이 저장되는 StorageGRID 버킷에 백업됩니다.

라이센스 요구 사항 확인

클러스터에 대한 NetApp Backup and Recovery 활성화하려면 먼저 NetApp 에서 NetApp Backup and Recovery BYOL 라이선스를 구매하고 활성화해야 합니다. 이 라이선스는 해당 계정에 대한 것이며 여러 시스템에서 사용할 수 있습니다.

라이선스 기간과 용량에 맞춰 서비스를 사용하려면 NetApp 의 일련 번호가 필요합니다. "BYOL 라이선스를 관리하는 방법을 알아보세요".

StorageGRID 에 파일을 백업하는 경우 PAYGO 라이선싱이 지원되지 않습니다.

ONTAP 클러스터 준비

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템을 준비합니다.

ONTAP 클러스터를 준비하는 단계는 다음과 같습니다.

- NetApp Console 에서 ONTAP 시스템을 찾아보세요
- ONTAP 시스템 요구 사항 확인
- 개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인
- 볼륨 복제를 위한 ONTAP 네트워킹 요구 사항 확인

NetApp Console 에서 ONTAP 시스템을 찾아보세요

소스 온프레미스 ONTAP 시스템과 보조 온프레미스 ONTAP 또는 Cloud Volumes ONTAP 시스템 모두 NetApp Console 시스템 페이지에서 사용할 수 있어야 합니다.

클러스터를 추가하려면 클러스터 관리 IP 주소와 관리자 사용자 계정의 비밀번호를 알아야 합니다. "클러스터를 검색하는 방법을 알아보세요".

ONTAP 시스템 요구 사항 확인

ONTAP 시스템이 다음 요구 사항을 충족하는지 확인하세요.

- 최소 ONTAP 9.8; ONTAP 9.8P13 이상을 권장합니다.
- SnapMirror 라이선스(프리미엄 번들 또는 데이터 보호 번들의 일부로 포함됨).

  참고: NetApp Backup and Recovery 사용하는 경우 "하이브리드 클라우드 번들"은 필요하지 않습니다.

  방법을 배우십시오 "클러스터 라이선스 관리" .
- 시간과 시간대가 올바르게 설정되었습니다. 방법을 배우십시오 "클러스터 시간 구성" .
- 데이터를 복제하는 경우 소스 및 대상 시스템이 호환되는 ONTAP 버전을 실행하는지 확인하세요.

  "SnapMirror 관계에 대한 호환 ONTAP 버전 보기".

개체 스토리지에 데이터를 백업하기 위한 ONTAP 네트워킹 요구 사항 확인

개체 스토리지에 연결하는 시스템에서 다음 요구 사항을 구성해야 합니다.

- 팬아웃 백업 아키텍처를 사용하는 경우 기본 스토리지 시스템에서 다음 설정을 구성해야 합니다.
- 계단식 백업 아키텍처를 사용하는 경우 보조 스토리지 시스템에서 다음 설정을 구성해야 합니다.

다음과 같은 ONTAP 클러스터 네트워킹 요구 사항이 필요합니다.

- ONTAP 클러스터는 백업 및 복원 작업을 위해 클러스터 간 LIF에서 StorageGRID 게이트웨이 노드로 사용자가 지정한 포트를 통해 HTTPS 연결을 시작합니다. 포트는 백업 설정 중에 구성할 수 있습니다.

ONTAP 객체 스토리지에서 데이터를 읽고 씁니다. 객체 스토리지는 결코 시작되지 않고, 단지 응답만 합니다.

- ONTAP 콘솔 에이전트에서 클러스터 관리 LIF로의 인바운드 연결이 필요합니다. 콘솔 에이전트는 귀하의 구내에 상주해야 합니다.
- 백업하려는 볼륨을 호스팅하는 각 ONTAP 노드에는 클러스터 간 LIF가 필요합니다. LIF는 ONTAP 개체 스토리지에 연결하는 데 사용해야 하는 _IPspace_와 연결되어야 합니다. "IPspaces에 대해 자세히 알아보세요" .

  NetApp Backup and Recovery 설정하면 사용할 IP 공간을 입력하라는 메시지가 표시됩니다. 각 LIF가 연결된 IP 공간을 선택해야 합니다. 이는 "기본" IP 공간일 수도 있고 사용자가 만든 사용자 지정 IP 공간일 수도 있습니다.

- 노드의 클러스터 간 LIF는 개체 저장소에 액세스할 수 있습니다(콘솔 에이전트가 "다크" 사이트에 설치된 경우에는 필요하지 않음).
- 볼륨이 위치한 스토리지 VM에 대한 DNS 서버가 구성되었습니다. 방법을 확인하세요 "SVM에 대한 DNS 서비스 구성" .
- 기본 IP 공간과 다른 IP 공간을 사용하는 경우 개체 스토리지에 액세스하려면 정적 경로를 만들어야 할 수도 있습니다.
- 필요한 경우 방화벽 규칙을 업데이트하여 ONTAP 에서 개체 스토리지로의 NetApp Backup and Recovery 서비스 연결을 지정한 포트(일반적으로 포트 443)를 통해 허용하고, 스토리지 VM에서 DNS 서버로의 이름 확인 트래픽을 포트 53(TCP/UDP)을 통해 허용합니다.

볼륨 복제를 위한 **ONTAP** 네트워킹 요구 사항 확인

NetApp Backup and Recovery 사용하여 보조 ONTAP 시스템에 복제된 볼륨을 생성하려는 경우 소스 및 대상 시스템이 다음 네트워킹 요구 사항을 충족하는지 확인하세요.

온프레미스 **ONTAP** 네트워킹 요구 사항

- 클러스터가 온프레미스에 있는 경우 회사 네트워크에서 클라우드 공급자의 가상 네트워크로 연결되어야 합니다. 이는 일반적으로 VPN 연결입니다.
- ONTAP 클러스터는 추가적인 서브넷, 포트, 방화벽 및 클러스터 요구 사항을 충족해야 합니다.

  Cloud Volumes ONTAP 또는 온프레미스 시스템에 복제할 수 있으므로 온프레미스 ONTAP 시스템에 대한 피어링 요구 사항을 검토하세요. "ONTAP 설명서에서 클러스터 피어링에 대한 필수 구성 요소 보기" .

Cloud Volumes ONTAP 네트워킹 요구 사항

- 인스턴스의 보안 그룹에는 필수 인바운드 및 아웃바운드 규칙이 포함되어야 합니다. 구체적으로는 ICMP 및 포트 11104와 11105에 대한 규칙이 포함됩니다. 이러한 규칙은 미리 정의된 보안 그룹에 포함됩니다.

StorageGRID 백업 대상으로 준비하세요

StorageGRID 다음 요구 사항을 충족해야 합니다. 를 참조하십시오 "StorageGRID 문서" 자세한 내용은.

StorageGRID 의 DataLock 및 Ransomware Resilience 요구 사항에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 옵션" .

지원되는 **StorageGRID** 버전

StorageGRID 10.3 이상이 지원됩니다.

백업에 DataLock 및 Ransomware Resilience를 사용하려면 StorageGRID 시스템에서 11.6.0.3 이상 버전을 실행해야 합니다.

이전 백업을 클라우드 보관 스토리지로 계층화하려면 StorageGRID 시스템에서 11.3 이상 버전을 실행해야 합니다. 또한, StorageGRID 시스템은 콘솔의 시스템 페이지에서 검색되어야 합니다.

사용자 보관 저장소를 사용하려면 관리자 노드 IP 액세스가 필요합니다.

게이트웨이 IP 액세스는 항상 필요합니다.

S3 자격 증명

StorageGRID 스토리지에 대한 액세스를 제어하려면 S3 테넌트 계정을 만들어야 합니다. "자세한 내용은 StorageGRID 문서를 참조하세요." .

StorageGRID 에 대한 백업을 설정하면 백업 마법사가 테넌트 계정에 대한 S3 액세스 키와 비밀 키를 입력하라는 메시지를 표시합니다. 테넌트 계정을 통해 NetApp Backup and Recovery 인증을 받고 백업을 저장하는 데 사용되는 StorageGRID 버킷에 액세스할 수 있습니다. StorageGRID 요청을 하는 사람이 누구인지 알 수 있도록 키가 필요합니다.

이러한 액세스 키는 다음 권한이 있는 사용자와 연결되어야 합니다.

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

객체 버전 관리

객체 저장소 버킷에서 StorageGRID 객체 버전 관리를 수동으로 활성화해서는 안 됩니다.

이전 백업 파일을 퍼블릭 클라우드 스토리지에 보관할 준비를 하세요.

오래된 백업 파일을 보관 저장소에 계층화하면 필요하지 않은 백업에 저렴한 스토리지 클래스를 사용하여 비용을 절감할 수 있습니다. StorageGRID 는 보관 저장소를 제공하지 않는 온프레미스(프라이빗 클라우드) 솔루션이지만, 오래된 백업 파일을 퍼블릭 클라우드 보관 저장소로 옮길 수 있습니다. 이런 방식으로 사용하면 클라우드 스토리지에 계층화된 데이터나 클라우드 스토리지에서 복원된 데이터는 StorageGRID 와 클라우드 스토리지 사이를 이동합니다. 콘솔은 이 데이터 전송에 관여하지 않습니다.

현재 지원을 통해 AWS *S3 Glacier*/*S3 Glacier Deep Archive* 또는 *Azure Archive* 스토리지에 백업을 보관할 수 있습니다.

- ONTAP 요구 사항*
- 클러스터는 ONTAP 9.12.1 이상을 사용해야 합니다.
- StorageGRID 요구 사항*
- StorageGRID 는 11.4 이상을 사용해야 합니다.
- 귀하의 StorageGRID 다음과 같아야 합니다. "콘솔에서 발견되어 사용 가능" .

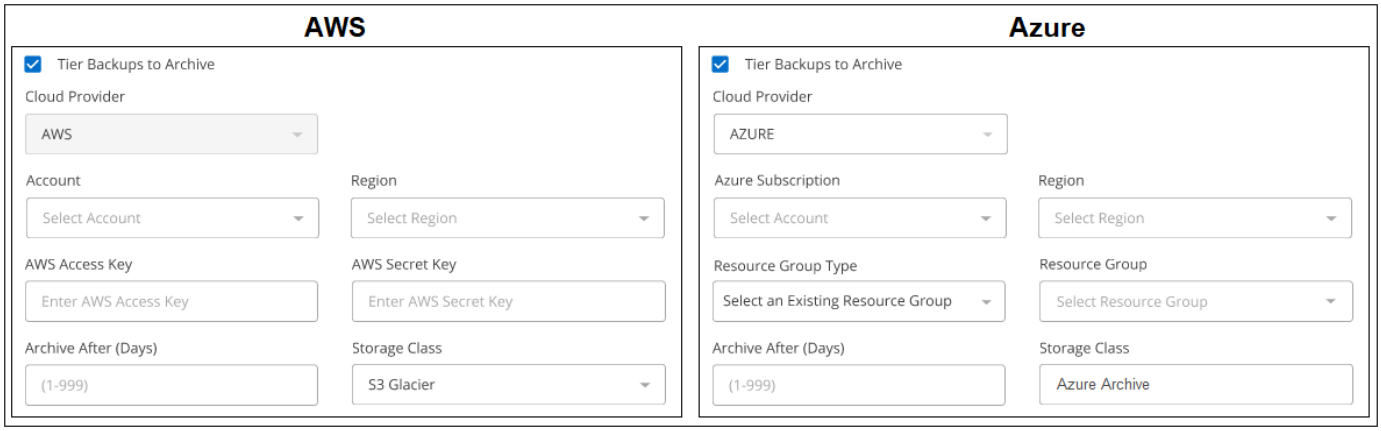
Amazon S3 요구 사항

- 보관된 백업이 저장될 저장 공간에 대한 Amazon S3 계정에 가입해야 합니다.
- AWS S3 Glacier 또는 S3 Glacier Deep Archive 스토리지에 대한 백업을 계층화할 수 있습니다. "AWS 보관 계층에 대해 자세히 알아보세요".
- StorageGRID 버킷에 대한 전체 제어 액세스 권한을 가져야 합니다.(`s3:*`); 그러나 이것이 가능하지 않은 경우 버킷 정책은 StorageGRID 에 다음과 같은 S3 권한을 부여해야 합니다.
  - `s3:AbortMultipartUpload`
  - `s3:DeleteObject`
  - `s3:GetObject`
  - `s3:ListBucket`
  - `s3:ListBucketMultipartUploads`
  - `s3:ListMultipartUploadParts`
  - `s3:PutObject`
  - `s3:RestoreObject`

Azure Blob 요구 사항

- 보관된 백업이 저장될 저장 공간에 대한 Azure 구독에 가입해야 합니다.
- 활성화 마법사를 사용하면 기존 리소스 그룹을 사용하여 백업을 저장할 Blob 컨테이너를 관리하거나 새 리소스 그룹을 만들 수 있습니다.

클러스터의 백업 정책에 대한 보관 설정을 정의할 때 클라우드 공급자 자격 증명을 입력하고 사용하려는 스토리지 클래스를 선택합니다. NetApp Backup and Recovery 클러스터에 대한 백업을 활성화하면 클라우드 버킷을 생성합니다. AWS 및 Azure 보관 저장소에 필요한 정보는 아래와 같습니다.



선택한 보관 정책 설정에 따라 StorageGRID 에서 정보 수명 주기 관리(ILM) 정책이 생성되고 해당 설정이 "규칙"으로 추가됩니다.

- 기존에 활성 ILM 정책이 있는 경우 데이터를 보관 계층으로 이동하기 위해 ILM 정책에 새 규칙이 추가됩니다.
- "제안됨" 상태의 기존 ILM 정책이 있는 경우, 새로운 ILM 정책을 만들고 활성화할 수 없습니다. "StorageGRID ILM 정책 및 규칙에 대해 자세히 알아보세요." .

ONTAP 볼륨에서 백업 활성화

언제든지 온프레미스 시스템에서 직접 백업을 활성화하세요.

마법사가 다음의 주요 단계를 안내합니다.

- 백업할 볼륨을 선택하세요
- 백업 전략 정의
- 선택 사항을 검토하세요

당신도 할 수 있습니다API 명령 표시 검토 단계에서 코드를 복사하여 향후 시스템에 대한 백업 활성화를 자동화할 수 있습니다.

마법사 시작

단계

1. 다음 방법 중 하나를 사용하여 백업 및 복구 활성화 마법사에 액세스하세요.

    - 콘솔의 시스템 페이지에서 시스템을 선택하고 오른쪽 패널의 백업 및 복구 옆에 있는 *활성화 > 백업 볼륨*을 선택합니다.

      백업 대상이 콘솔의 시스템 페이지에 있는 시스템으로 존재하는 경우 ONTAP 클러스터를 개체 스토리지로 끌어다 놓을 수 있습니다.

    - 백업 및 복구 표시줄에서 볼륨*을 선택합니다. 볼륨 탭에서 *작업(...) 옵션을 선택하고 단일 볼륨(이미 복제나 개체 저장소로의 백업이 활성화되지 않은 볼륨)에 대해 *백업 활성화*를 선택합니다.

   마법사의 소개 페이지에는 로컬 스냅샷, 복제, 백업을 포함한 보호 옵션이 표시됩니다. 이 단계에서 두 번째 옵션을 선택한 경우, 하나의 볼륨이 선택된 상태로 백업 전략 정의 페이지가 나타납니다.

2. 다음 옵션을 계속 진행하세요.

    - 이미 콘솔 에이전트가 있다면 준비가 완료된 것입니다. *다음*을 선택하세요.
    - 아직 콘솔 에이전트가 없으면 콘솔 에이전트 추가 옵션이 나타납니다. 참조하다콘솔 에이전트를 준비하세요 .

백업할 볼륨을 선택하세요

보호할 볼륨을 선택하세요. 보호된 볼륨은 다음 중 하나 이상을 갖춘 볼륨입니다. 스냅샷 정책, 복제 정책, 개체 정책으로의 백업.

FlexVol 또는 FlexGroup 볼륨을 보호하도록 선택할 수 있습니다. 그러나 시스템 백업을 활성화할 때 이러한 볼륨을 혼합하여 선택할 수는 없습니다. 방법을 확인하세요"시스템의 추가 볼륨에 대한 백업을 활성화합니다." (FlexVol 또는 FlexGroup) 초기 볼륨에 대한 백업을 구성한 후.

- 한 번에 하나의 FlexGroup 볼륨에서만 백업을 활성화할 수 있습니다.
- 선택한 볼륨에는 동일한 SnapLock 설정이 있어야 합니다. 모든 볼륨에는 SnapLock Enterprise 활성화되어 있어야 하거나 SnapLock 비활성화되어 있어야 합니다.

단계

선택한 볼륨에 이미 스냅샷이나 복제 정책이 적용된 경우 나중에 선택하는 정책이 기존 정책을 덮어씁니다.

1. 볼륨 선택 페이지에서 보호하려는 볼륨을 선택합니다.
    - 선택적으로, 특정 볼륨 유형, 스타일 등을 갖춘 볼륨만 표시하도록 행을 필터링하여 선택을 더 쉽게 할 수 있습니다.
    - 첫 번째 볼륨을 선택한 후에는 모든 FlexVol 볼륨을 선택할 수 있습니다(FlexGroup 볼륨은 한 번에 하나씩만 선택할 수 있습니다). 기존의 모든 FlexVol 볼륨을 백업하려면 먼저 볼륨 하나를 선택한 다음 제목 행의 상자를 선택합니다.
    - 개별 볼륨을 백업하려면 각 볼륨의 상자를 선택하세요.
2. *다음*을 선택하세요.

백업 전략 정의

백업 전략을 정의하려면 다음 옵션을 설정해야 합니다.

- 로컬 스냅샷, 복제 및 개체 스토리지 백업 등 백업 옵션 중 하나 또는 전부를 원하는지 여부
- 아키텍처
- 로컬 스냅샷 정책
- 복제 대상 및 정책

선택한 볼륨에 이 단계에서 선택한 정책과 다른 스냅샷 및 복제 정책이 있는 경우 기존 정책이 덮어쓰여집니다.

- 개체 스토리지 정보(공급자, 암호화, 네트워킹, 백업 정책 및 내보내기 옵션)에 대한 백업입니다.

단계

1. 백업 전략 정의 페이지에서 다음 중 하나 또는 모두를 선택하세요. 기본적으로 세 가지 모두 선택되어 있습니다.
    - 로컬 스냅샷: 개체 스토리지에 복제나 백업을 수행하는 경우 로컬 스냅샷을 만들어야 합니다.
    - 복제: 다른 ONTAP 스토리지 시스템에 복제된 볼륨을 생성합니다.
    - 백업: 볼륨을 개체 스토리지에 백업합니다.
2. 아키텍처: 복제와 백업을 모두 선택한 경우 다음 정보 흐름 중 하나를 선택하세요.
    - 계단식: 정보는 기본 스토리지에서 보조 스토리지로 흐르고, 보조 스토리지에서 개체 스토리지로 흐릅니다.
    - 팬아웃: 정보는 기본 스토리지에서 보조 스토리지로, 기본 스토리지에서 개체 스토리지로 흐릅니다.

    이러한 아키텍처에 대한 자세한 내용은 다음을 참조하세요."보호 여정을 계획하세요" .
3. 로컬 스냅샷: 기존 스냅샷 정책을 선택하거나 새 정책을 만듭니다.

사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

    - 정책의 이름을 입력하세요.
    - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
    - *만들기*를 선택하세요.

4. 복제: 다음 옵션을 설정합니다.
   - 복제 대상: 대상 시스템과 SVM을 선택합니다. 선택적으로 복제된 볼륨 이름에 추가될 대상 집계 또는 집계와 접두사 또는 접미사를 선택합니다.
   - 복제 정책: 기존 복제 정책을 선택하거나 새로 만듭니다.

     사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - *만들기*를 선택하세요.
5. 개체로 백업: *백업*을 선택한 경우 다음 옵션을 설정합니다.
   - 공급자: * StorageGRID*를 선택하세요.
   - 공급자 설정: 공급자 게이트웨이 노드 FQDN 세부 정보, 포트, 액세스 키 및 비밀 키를 입력합니다.

     액세스 키와 비밀 키는 ONTAP 클러스터에 버킷에 대한 액세스 권한을 부여하기 위해 생성한 IAM 사용자를 위한 것입니다.
   - 네트워킹: 백업하려는 볼륨이 있는 ONTAP 클러스터의 IP 공간을 선택합니다. 이 IP공간의 클러스터 간 LIF에는 아웃바운드 인터넷 액세스가 있어야 합니다(콘솔 에이전트가 "다크" 사이트에 설치된 경우에는 필요하지 않음).

     올바른 IP 공간을 선택하면 NetApp Backup and Recovery ONTAP 에서 StorageGRID 개체 스토리지로의 연결을 설정할 수 있습니다.
   - 백업 정책: 기존의 개체 스토리지 백업 정책을 선택하거나 새로 만듭니다.

     사용자 정의 정책을 생성하려면 다음을 참조하세요."정책 만들기" .

     정책을 만들려면 *새 정책 만들기*를 선택하고 다음을 수행하세요.

     - 정책의 이름을 입력하세요.
     - 일반적으로 서로 다른 빈도로 최대 5개의 일정을 선택하세요.
     - 개체 백업 정책의 경우 DataLock 및 랜섬웨어 복원력 설정을 지정합니다. DataLock 및 랜섬웨어 복원력에 대한 자세한 내용은 다음을 참조하세요."개체 백업 정책 설정" .

       클러스터에서 ONTAP 9.11.1 이상을 사용하는 경우 _DataLock 및 랜섬웨어 복원력_을 구성하여 백업을 삭제 및 랜섬웨어 공격으로부터 보호할 수 있습니다. _DataLock_은 백업 파일이 수정되거나 삭제되는 것을 방지하고, _Ransomware Resilience_는 백업 파일을 검사하여 백업 파일에서 랜섬웨어 공격의 증거를 찾습니다.
     - *만들기*를 선택하세요.

     클러스터에서 ONTAP 9.12.1 이상을 사용하고 StorageGRID 시스템에서 11.4 이상을 사용하는 경우, 특정 일수가 지난 후 이전 백업을 퍼블릭 클라우드 보관 계층으로 계층화하도록 선택할 수 있습니다. 현재 지원되는 스토리지 계층은 AWS S3 Glacier/S3 Glacier Deep Archive 또는 Azure Archive 스토리지 계층입니다. 이

기능을 위해 시스템을 구성하는 방법을 확인하세요..

- 퍼블릭 클라우드에 대한 계층형 백업: 계층형 백업을 수행할 클라우드 공급자를 선택하고 공급자 세부 정보를 입력합니다.

  새로운 StorageGRID 클러스터를 선택하거나 생성합니다. 콘솔에서 검색할 수 있도록 StorageGRID 클러스터를 만드는 방법에 대한 자세한 내용은 다음을 참조하세요. "StorageGRID 문서" .

- 기존 스냅샷을 백업 사본으로 개체 스토리지로 내보내기: 이 시스템의 볼륨에 대한 로컬 스냅샷이 이 시스템에 대해 방금 선택한 백업 일정 레이블(예: 매일, 매주 등)과 일치하는 경우 이 추가 프롬프트가 표시됩니다. 볼륨에 대한 가장 완벽한 보호를 보장하기 위해 모든 이전 스냅샷을 백업 파일로 개체 스토리지에 복사하려면 이 상자를 선택하세요.

6. *다음*을 선택하세요.

선택 사항을 검토하세요

이는 귀하의 선택 사항을 검토하고 필요한 경우 조정할 수 있는 기회입니다.

단계

1. 검토 페이지에서 선택 사항을 검토하세요.
2. 선택적으로 스냅샷 정책 레이블을 복제 및 백업 정책 레이블과 자동으로 동기화 확인란을 선택합니다. 이렇게 하면 복제 및 백업 정책의 레이블과 일치하는 레이블이 있는 스냅샷이 생성됩니다.
3. *백업 활성화*를 선택하세요.

결과

NetApp Backup and Recovery 볼륨의 초기 백업을 시작합니다. 복제된 볼륨과 백업 파일의 기준선 전송에는 소스 데이터의 전체 사본이 포함됩니다. 이후 전송에는 스냅샷에 포함된 기본 저장소 데이터의 차등 사본이 포함됩니다.

대상 클러스터에 복제된 볼륨이 생성되어 기본 저장소 볼륨과 동기화됩니다.

입력한 S3 액세스 키와 비밀 키로 지정된 서비스 계정에 S3 버킷이 생성되고, 백업 파일이 해당 버킷에 저장됩니다.

볼륨 백업 대시보드가 표시되어 백업 상태를 모니터링할 수 있습니다.

다음을 사용하여 백업 및 복원 작업의 상태를 모니터링할 수도 있습니다."작업 모니터링 페이지" .

API 명령 표시

백업 및 복구 활성화 마법사에서 사용되는 API 명령을 표시하고 선택적으로 복사할 수 있습니다. 향후 시스템에서 백업 활성화를 자동화하려면 이 작업을 수행하는 것이 좋습니다.

단계

1. 백업 및 복구 활성화 마법사에서 *API 요청 보기*를 선택합니다.
2. 명령을 클립보드에 복사하려면 복사 아이콘을 선택하세요.

NetApp Backup and Recovery 에서 SnapMirror 사용하여 볼륨을 Cloud Resync로 마이그레이션

NetApp Backup and Recovery 의 SnapMirror to Cloud Resync 기능은 NetApp 환경에서 볼륨 마이그레이션 중에 데이터 보호와 연속성을 간소화합니다. SnapMirror Logical Replication(LRSE)을 사용하여 볼륨을 온프레미스 NetApp 배포에서 다른 배포로 또는 Cloud Volumes ONTAP 과 같은 클라우드 기반 솔루션으로 마이그레이션하는 경우 SnapMirror to Cloud Resync를 통해 기존 클라우드 백업이 손상되지 않고 작동 상태를 유지하도록 보장합니다.

이 기능을 사용하면 재기준화 프로세스가 필요 없으며 마이그레이션 후에도 백업을 계속할 수 있습니다. 이 기능은 FlexVol과 FlexGroup을 모두 지원하여 워크로드 마이그레이션 시나리오에서 유용하며 ONTAP 버전 9.16.1부터 사용할 수 있습니다.

이 기능은 2025년 5월에 출시된 NetApp Backup and Recovery 버전 4.0.3부터 사용할 수 있습니다.

SnapMirror to Cloud Resync는 여러 환경 간에 백업 연속성을 유지하므로 하이브리드 및 멀티 클라우드 설정에서 데이터를 더 쉽게 관리할 수 있습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

시작하기 전에

다음 전제 조건이 충족되었는지 확인하세요.

- 대상 ONTAP 클러스터는 ONTAP 버전 9.16.1 이상을 실행해야 합니다.
- 이전 Source ONTAP 클러스터는 NetApp Backup and Recovery 사용하여 보호해야 합니다.
- SnapMirror to Cloud Resync 기능은 2025년 5월에 출시된 NetApp Backup and Recovery 버전 4.0.3부터 사용할 수 있습니다.
- 개체 저장소의 최신 백업이 이전 소스, 새 소스 및 개체 저장소의 공통 스냅샷인지 확인하세요. 개체 저장소에 백업된 최신 스냅샷보다 오래된 일반 스냅샷을 사용하지 마세요.
- 재동기화 작업을 시작하기 전에 이전 ONTAP 클러스터에서 사용된 스냅샷 정책과 SnapMirror 정책을 모두 새 ONTAP 클러스터에서 만들어야 합니다. 재동기화 프로세스에서 정책을 사용하는 경우 해당 정책도 만들어야 합니다. Resync 작업은 정책을 생성하지 않습니다.
- 마이그레이션 볼륨 SnapMirror 관계에 적용되는 SnapMirror 정책에 클라우드 관계에 사용되는 것과 동일한 레이블이 포함되어 있는지 확인하세요. 문제를 방지하려면 볼륨과 모든 스냅샷의 정확한 미러를 관리하는 정책을 사용하세요.

SVM-Migrate, SVM-DR 또는 Head Swap 방법을 사용하여 마이그레이션한 후 SnapMirror 에서 Cloud Resync로 다시 동기화하는 기능은 현재 지원되지 않습니다.

NetApp Backup and Recovery SnapMirror to Cloud Resync 작동 방식

기술적 업데이트를 완료하거나 한 ONTAP 클러스터에서 다른 ONTAP 클러스터로 볼륨을 마이그레이션하는 경우 백업이 중단 없이 계속 작동하는 것이 중요합니다. NetApp Backup and Recovery SnapMirror to Cloud Resync는 볼륨 마이그레이션 후에도 클라우드 백업이 일관성을 유지하도록 보장하여 이를 지원합니다.

예를 들면 다음과 같습니다.

Vol1a라는 온프레미스 볼륨이 있다고 가정해 보겠습니다. 이 볼륨에는 S1, S2, S3의 세 개의 스냅샷이 있습니다. 이러한 스냅샷은 복원 지점입니다. Vol1은 SnapMirror to Cloud(SM-C)를 사용하여 클라우드에 백업되지만, 객체 저장소에는 S1과 S2만 있습니다.

이제 Vol1을 다른 ONTAP 클러스터로 마이그레이션하려고 합니다. 이를 위해 Vol1b라는 새로운 클라우드 볼륨에 대한 SnapMirror 논리적 복제(LRSE) 관계를 생성합니다. 이렇게 하면 세 개의 스냅샷(S1, S2, S3)이 모두 Vol1a에서 Vol1b로 전송됩니다.

마이그레이션이 완료되면 다음과 같은 설정이 적용됩니다.

- 원래 SM-C 관계(Vol1a → Object store)가 삭제됩니다.
- LRSE 관계(Vol1a → Vol1b)도 삭제됩니다.
- Vol1b가 이제 활성 볼륨이 되었습니다.

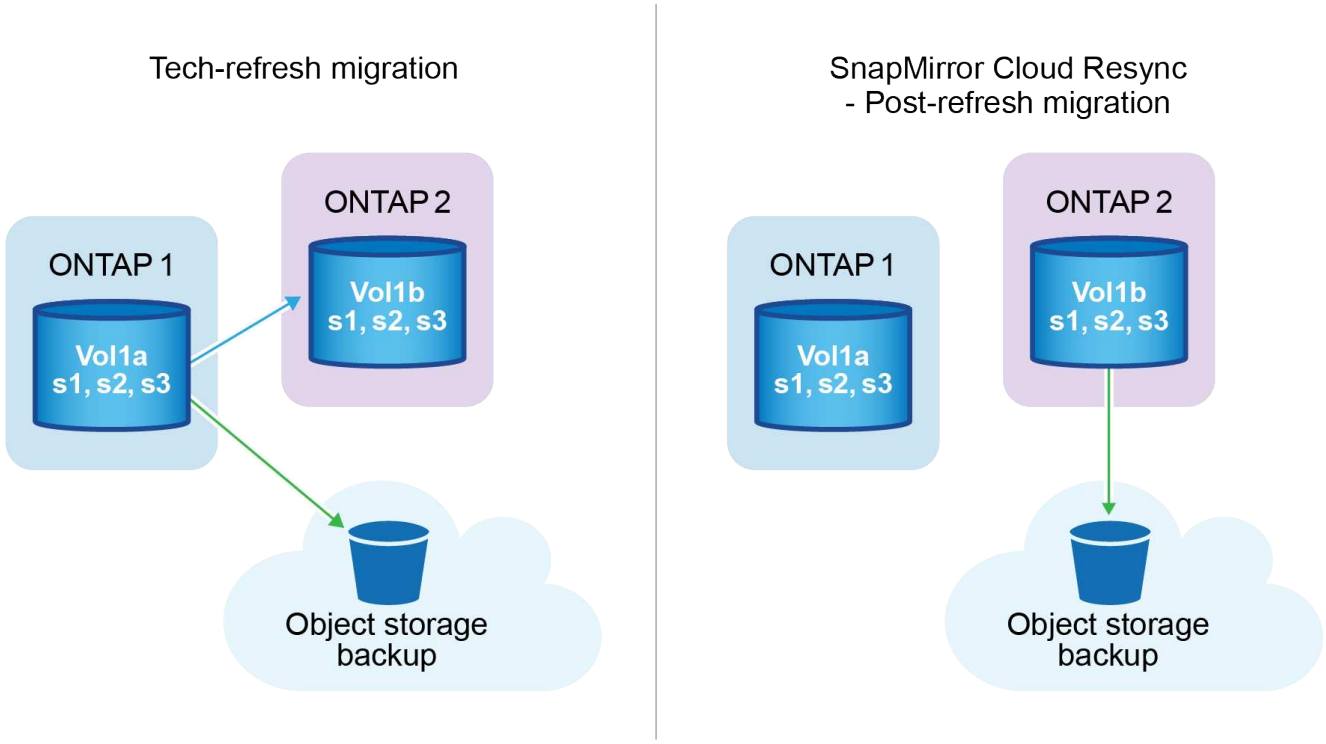
이 시점에서 Vol1b를 동일한 클라우드 엔드포인트로 계속 백업하려고 합니다. 하지만 처음부터 전체 백업을 시작하는 대신(시간과 리소스가 필요함) SnapMirror 사용하여 Cloud Resync를 수행합니다.

재동기화는 다음과 같이 작동합니다.

- 시스템은 Vol1a와 Object store 간의 공통 스냅샷을 확인합니다. 이 경우 둘 다 S2를 갖습니다.
- 이러한 공유 스냅샷으로 인해 시스템은 S2와 S3 간에 증분 변경 사항만 전송하면 됩니다.

즉, S2 이후에 추가된 새 데이터만 개체 저장소로 전송되고 전체 볼륨은 전송되지 않습니다.

이 프로세스를 통해 중복 백업을 방지하고, 대역폭을 절약하며, 마이그레이션 후에도 백업을 계속 실행할 수 있습니다.



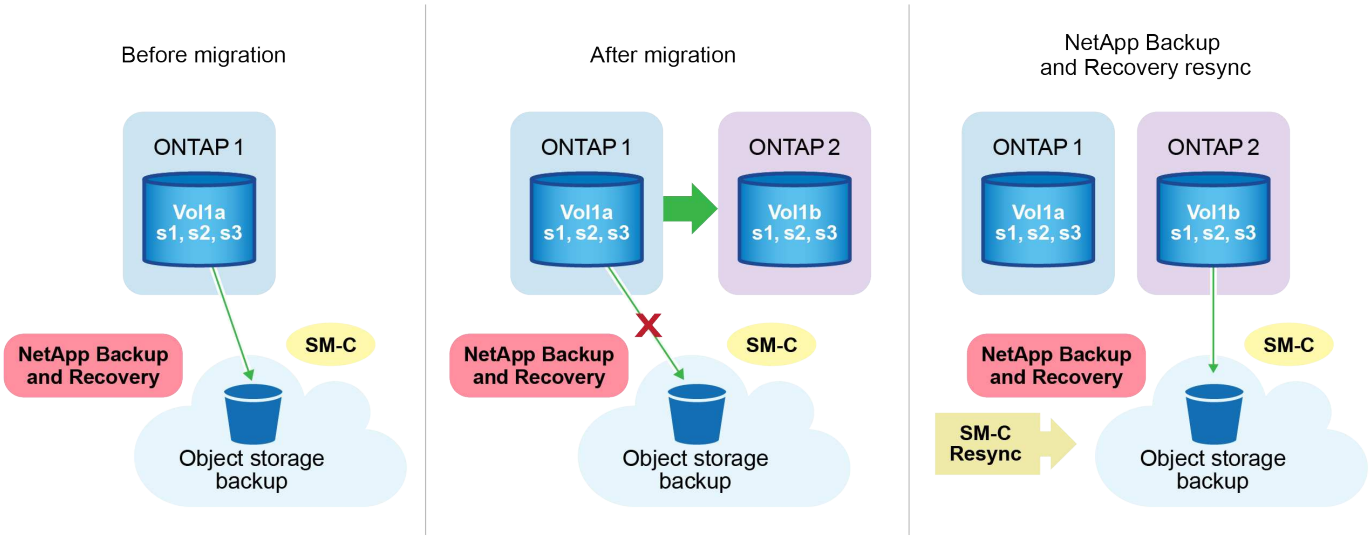
시술 노트

- NetApp Backup and Recovery 사용하여 마이그레이션 및 기술 업데이트가 수행되지 않습니다. 이러한 작업은 전문 서비스 팀이나 자격을 갖춘 보관 관리자가 수행해야 합니다.
- NetApp 마이그레이션 팀은 볼륨 이동을 돕기 위해 소스 및 대상 ONTAP 클러스터 간에 SnapMirror 관계를 만듭니다.
- 기술 업데이트 중 마이그레이션이 SnapMirror 기반 마이그레이션을 기반으로 수행되는지 확인하세요.

SnapMirror 사용하여 볼륨을 Cloud Resync로 마이그레이션하는 방법

SnapMirror 사용하여 볼륨을 Cloud Resync로 마이그레이션하는 작업에는 다음과 같은 주요 단계가 포함되며, 각 단계에 대한 자세한 내용은 아래에서 설명합니다.

- 마이그레이션 전 체크리스트를 따르세요: 마이그레이션을 시작하기 전에 NetApp Tech Refresh 팀은 데이터 손실을 방지하고 원활한 마이그레이션 프로세스를 보장하기 위해 다음 전제 조건이 충족되는지 확인합니다.
- 마이그레이션 후 체크리스트를 따르세요: 마이그레이션 후 NetApp 기술 업데이트 팀은 다음 단계가 완료되어 보호가 확립되고 재동기화를 준비합니다.
- * SnapMirror 에서 클라우드 재동기화 수행*: 마이그레이션 후 NetApp 기술 업데이트 팀은 SnapMirror 에서 클라우드 재동기화 작업을 수행하여 새로 마이그레이션된 볼륨에서 클라우드 백업을 재개합니다.



이주 전 체크리스트를 따르세요

마이그레이션 전에 NetApp Tech Refresh 팀은 데이터 손실을 방지하고 원활한 프로세스를 보장하기 위해 이러한 필수 조건을 확인합니다.

1. 마이그레이션할 모든 볼륨이 NetApp Backup and Recovery 사용하여 보호되는지 확인하세요.
2. 볼륨 인스턴스 UUID를 기록합니다. 마이그레이션을 시작하기 전에 모든 볼륨의 인스턴스 UUID를 기록해 두세요. 이러한 식별자는 나중에 매핑 및 재동기화 작업에 매우 중요합니다.
3. SnapMirror 관계를 삭제하기 전에 최신 상태를 보존하기 위해 각 볼륨의 최종 스냅샷을 찍습니다.
4. SnapMirror 정책을 문서화합니다. 각 볼륨의 관계에 현재 연결된 SnapMirror 정책을 기록합니다. 이 작업은 나중에 SnapMirror 와 Cloud Resync 프로세스 중에 필요합니다.

5. 개체 저장소와 SnapMirror Cloud 관계를 삭제합니다.
6. 볼륨을 새 대상 ONTAP 클러스터로 마이그레이션하려면 새 ONTAP 클러스터와 표준 SnapMirror 관계를 만듭니다.

이주 후 체크리스트를 따르세요

마이그레이션 후 NetApp 기술 업데이트 팀은 다음 단계가 완료되어 보호가 확립되고 재동기화를 준비합니다.

1. 대상 ONTAP 클러스터에 있는 모든 마이그레이션된 볼륨의 새 볼륨 인스턴스 UUID를 기록합니다.
2. 이전 ONTAP 클러스터에서 사용 가능했던 모든 필수 SnapMirror 정책이 새 ONTAP 클러스터에서 올바르게 구성되었는지 확인합니다.
3. 콘솔의 시스템 페이지에서 새로운 ONTAP 클러스터를 시스템으로 추가합니다.

> 볼륨 ID가 아닌 볼륨 인스턴스 UUID를 사용해야 합니다. 볼륨 인스턴스 UUID는 마이그레이션 전체에서 일관되게 유지되는 고유 식별자인 반면, 볼륨 ID는 마이그레이션 후에 변경될 수 있습니다.

SnapMirror 클라우드 재동기화로 수행

마이그레이션 후 NetApp Tech Refresh 팀은 SnapMirror to Cloud Resync 작업을 수행하여 새로 마이그레이션된 볼륨에서 클라우드 백업을 재개합니다.

1. 콘솔의 시스템 페이지에서 새로운 ONTAP 클러스터를 시스템으로 추가합니다.
2. NetApp Backup and Recovery 볼륨 페이지를 확인하여 이전 소스 시스템 세부 정보를 사용할 수 있는지 확인하세요.
3. NetApp Backup and Recovery 볼륨 페이지에서 *백업 설정*을 선택합니다.
   - 백업 설정 페이지에서 *모두 보기*를 선택합니다.
   - 새로운 소스 오른쪽에 있는 작업… 메뉴에서 *백업 재동기화*를 선택합니다.
4. Resync 시스템 페이지에서 다음을 수행합니다.
   a. 새로운 소스 시스템: 볼륨이 마이그레이션된 새로운 ONTAP 클러스터를 입력합니다.
   b. 기존 대상 개체 저장소: 이전 소스 시스템의 백업이 포함된 대상 개체 저장소를 선택합니다.
5. *CSV 템플릿 다운로드*를 선택하여 Resync 세부 정보 Excel 시트를 다운로드하세요. 이 시트를 사용하여 마이그레이션할 볼륨의 세부 정보를 입력하세요. CSV 파일에 다음 세부 정보를 입력하세요.
   - 소스 클러스터의 이전 볼륨 인스턴스 UUID
   - 대상 클러스터의 새 볼륨 인스턴스 UUID
   - 새로운 관계에 적용될 SnapMirror 정책입니다.
6. *볼륨 매핑 세부 정보 업로드*에서 *업로드*를 선택하여 작성된 CSV 시트를 NetApp Backup and Recovery UI에 업로드합니다.

> 볼륨 ID가 아닌 볼륨 인스턴스 UUID를 사용해야 합니다. 볼륨 인스턴스 UUID는 마이그레이션 전체에서 일관되게 유지되는 고유 식별자인 반면, 볼륨 ID는 마이그레이션 후에 변경될 수 있습니다.

7. 재동기화 작업에 필요한 공급자 및 네트워크 구성 정보를 입력하세요.

8. *제출*을 선택하여 검증 과정을 시작하세요.

   NetApp Backup and Recovery 재동기화를 위해 선택된 각 볼륨이 최신 스냅샷이고 적어도 하나의 공통 스냅샷이 있는지 확인합니다. 이렇게 하면 볼륨이 SnapMirror to Cloud Resync 작업에 준비됩니다.

9. 새로운 소스 볼륨 이름과 각 볼륨의 재동기화 상태를 포함한 검증 결과를 검토합니다.
10. 볼륨 적합성을 확인하세요. 시스템은 볼륨이 재동기화에 적합한지 확인합니다. 볼륨이 적합하지 않은 경우 최신 스냅샷이 아니거나 공통 스냅샷을 찾을 수 없음을 의미합니다.

    볼륨이 SnapMirror to Cloud Resync 작업에 적합한 상태를 유지하도록 하려면 사전 마이그레이션 단계에서 SnapMirror 관계를 삭제하기 전에 각 볼륨의 최종 스냅샷을 찍습니다. 이렇게 하면 최신 데이터 상태가 보존됩니다.

11. 재동기화 작업을 시작하려면 *재동기화*를 선택하세요. 시스템은 최신의 공통 스냅샷을 사용하여 증분 변경 사항만 전송하여 백업 연속성을 보장합니다.
12. 작업 모니터 페이지에서 재동기화 프로세스를 모니터링합니다.

다크 사이트에서 **NetApp Backup and Recovery** 구성 데이터 복원

인터넷 접속이 불가능한 사이트(개인 모드)에서 NetApp Backup and Recovery 사용하는 경우, NetApp Backup and Recovery 구성 데이터는 백업이 저장되는 StorageGRID 또는 ONTAP S3 버킷에 백업됩니다. 콘솔 에이전트 호스트 시스템에 문제가 있는 경우 새로운 콘솔 에이전트를 배포하고 중요한 NetApp Backup and Recovery 데이터를 복원할 수 있습니다.

이 절차는 ONTAP 볼륨 데이터에만 적용됩니다.

클라우드 공급업체나 인터넷에 연결된 자체 호스트에 콘솔 에이전트를 배포하여 SaaS 환경에서 NetApp Backup and Recovery 사용하면 시스템이 클라우드에 있는 모든 중요한 구성 데이터를 백업하고 보호합니다. 콘솔 에이전트에 문제가 있는 경우 새 콘솔 에이전트를 만들고 시스템을 추가하세요. 백업 세부정보가 자동으로 복원됩니다.

백업되는 데이터에는 두 가지 유형이 있습니다.

- NetApp Backup and Recovery 데이터베이스 - 모든 볼륨, 백업 파일, 백업 정책 및 구성 정보 목록이 포함되어 있습니다.
- 색인된 카탈로그 파일 - 볼륨 데이터를 복원할 때 검색을 매우 빠르고 효율적으로 수행할 수 있는 검색 및 복원 기능에 사용되는 자세한 색인이 포함되어 있습니다.

이 데이터는 하루에 한 번 자정에 백업되며, 각 파일의 최대 7개 사본이 보관됩니다. 콘솔 에이전트가 여러 온프레미스 ONTAP 시스템을 관리하는 경우 NetApp Backup and Recovery 파일은 먼저 활성화된 시스템의 버킷에 저장됩니다.

NetApp Backup and Recovery 데이터베이스나 인덱싱된 카탈로그 파일에는 볼륨 데이터가 포함되지 않습니다.

NetApp Backup and Recovery 데이터를 새 콘솔 에이전트로 복원

온프레미스 콘솔 에이전트가 작동을 멈추면 새 콘솔 에이전트를 설치한 다음 NetApp Backup and Recovery 데이터를 새 콘솔 에이전트로 복원해야 합니다.

NetApp Backup and Recovery 시스템을 작동 상태로 되돌리려면 다음 작업을 수행해야 합니다.

- 새 콘솔 에이전트 설치
- NetApp Backup and Recovery 데이터베이스 복원
- 인덱싱된 카탈로그 파일 복원
- 온프레미스 ONTAP 시스템과 StorageGRID 시스템을 모두 NetApp Console UI로 다시 검색하세요.

시스템이 제대로 작동하는지 확인한 후 새로운 백업 파일을 만드세요.

필요한 것

백업 파일이 저장되어 있는 StorageGRID 또는 ONTAP S3 버킷에서 최신 데이터베이스 및 인덱스 백업에 액세스해야 합니다.

- NetApp Backup and Recovery MySQL 데이터베이스 파일

  이 파일은 버킷의 다음 위치에 있습니다. `netapp-backup-<GUID>/mysql_backup/` , 그리고 그것은 이름이 붙습니다 `CBS_DB_Backup_<day>_<month>_<year>.sql` .

- 색인된 카탈로그 백업 zip 파일

  이 파일은 버킷의 다음 위치에 있습니다. `netapp-backup-<GUID>/catalog_backup/` , 그리고 그것은 이름이 붙습니다 `Indexed_Catalog_DB_Backup_<db_name>_<day>_<month>_<year>.zip` .

새로운 온프레미스 **Linux** 호스트에 새 콘솔 에이전트 설치

새로운 콘솔 에이전트를 설치할 때 원래 에이전트와 동일한 소프트웨어 버전을 다운로드하세요. NetApp Backup and Recovery 데이터베이스가 변경되면 최신 소프트웨어 버전이 이전 데이터베이스 백업과 작동하지 않을 수 있습니다. 당신은 할 수 있습니다 "백업 데이터베이스를 복원한 후 콘솔 에이전트 소프트웨어를 최신 버전으로 업그레이드합니다." .

1. "새로운 온프레미스 Linux 호스트에 콘솔 에이전트 설치"
2. 방금 만든 관리자 사용자 자격 증명을 사용하여 콘솔에 로그인합니다.

NetApp Backup and Recovery 데이터베이스 복원

1. 백업 위치에서 MySQL 백업을 새 콘솔 에이전트 호스트로 복사합니다. 아래에서는 "CBS_DB_Backup_23_05_2023.sql"이라는 예제 파일 이름을 사용하겠습니다.
2. Docker 또는 Podman 컨테이너를 사용하는지에 따라 다음 명령 중 하나를 사용하여 백업을 MySQL Docker 컨테이너에 복사합니다.

```
docker cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

```
podman cp CBS_DB_Backup_23_05_2023.sql ds_mysql_1:/.
```

3. Docker 또는 Podman 컨테이너를 사용하는지에 따라 다음 명령 중 하나를 사용하여 MySQL 컨테이너 셸을 입력합니다.

```
docker exec -it ds_mysql_1 sh
```

```
podman exec -it ds_mysql_1 sh
```

4. 컨테이너 셸에서 "env"를 배포합니다.
5. MySQL DB 비밀번호가 필요하므로 "MYSQL_ROOT_PASSWORD" 키 값을 복사합니다.
6. 다음 명령을 사용하여 NetApp Backup and Recovery MySQL DB를 복원합니다.

```
mysql -u root -p cloud_backup < CBS_DB_Backup_23_05_2023.sql
```

7. 다음 SQL 명령을 사용하여 NetApp Backup and Recovery MySQL DB가 올바르게 복원되었는지 확인하세요.

```
mysql -u root -p cloud_backup
```

8. 비밀번호를 입력하세요.

```
mysql> show tables;
mysql> select * from volume;
```

9. 표시된 볼륨이 원래 환경에 있던 볼륨과 동일한지 확인하세요.

인덱싱된 카탈로그 파일 복원

1. 백업 위치에서 Indexed Catalog 백업 zip 파일(예시 파일 이름 "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip"을 사용함)을 "/opt/application/netapp/cbs" 폴더에 있는 새 콘솔 에이전트 호스트로 복사합니다.
2. 다음 명령을 사용하여 "Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip" 파일의 압축을 풉니다.

```
unzip Indexed_Catalog_DB_Backup_catalogdb1_23_05_2023.zip -d catalogdb1
```

3. **ls** 명령을 실행하여 "catalogdb1" 폴더가 생성되었고 그 아래에 "changes"와 "snapshots"라는 하위 폴더가 있는지 확인합니다.

ONTAP 클러스터와 **StorageGRID** 시스템을 알아보세요

1. "온프레미스 ONTAP 시스템을 모두 알아보세요"이전 환경에서 사용 가능했던 기능입니다. 여기에는 S3 서버로 사용한 ONTAP 시스템이 포함됩니다.
2. "StorageGRID 시스템을 알아보세요".

StorageGRID 환경 세부 정보 설정

원래 콘솔 에이전트 설정에서 설정된 대로 ONTAP 시스템과 연결된 StorageGRID 시스템의 세부 정보를 추가합니다. "NetApp Console API" .

다음 정보는 NetApp Console 3.9.xx부터 시작하는 개인 모드 설치에 적용됩니다. 이전 버전의 경우 다음 절차를 따르세요. "DarkSite 클라우드 백업: MySQL 및 인덱스 카탈로그 백업 및 복원" .

StorageGRID 에 데이터를 백업하는 각 시스템에 대해 이러한 단계를 수행해야 합니다.

1. 다음 oauth/token API를 사용하여 권한 부여 토큰을 추출합니다.

```
curl 'http://10.193.192.202/oauth/token' -X POST -H 'Accept:
application/json' -H 'Accept-Language: en-US,en;q=0.5' -H 'Accept-
Encoding: gzip, deflate' -H 'Content-Type: application/json' -d '
{"username":"admin@netapp.com","password":"Netapp@123","grant_type":"pas
sword"}
> '
```

   IP 주소, 사용자 이름, 비밀번호는 사용자 지정 값이지만 계정 이름은 그렇지 않습니다. 계정 이름은 항상 "account-DARKSITE1"입니다. 또한, 사용자 이름은 이메일 형식의 이름을 사용해야 합니다.

   이 API는 다음과 같은 응답을 반환합니다. 아래와 같이 인증 토큰을 검색할 수 있습니다.

```
{"expires_in":21600,"access_token":"eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIs
ImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vY
XBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0cDovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uY
W1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQubmV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ld
GFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwcm9maWxlIiwiaWF0IjoxNjcyNzM2MDIzLCJle
HAiOjE2NzI3NTc2MjMsImlzcyI6Imh0dHA6Ly9vY2NtYXV0aDo4NDIwLyJ9CJtRpRDY23Pok
yLg1if67bmgnMcYxdCvBOY-ZUYWzhrWbbY_hqUH4T-
114v_pNDsPyNDyWqHaKizThdjjHYHxm56vTz_Vdn4NqjaBDPwN9KAnC6Z88WA1cJ4WRQqj5y
kODNDmrv5At_f9HHp0-xVMyHqywZ4nNFalMvAh4xESc5jfoKOZc-
IOQdWm4F4LHpMzs4qFzCYthTuSKLYtqSTUrZB81-o-ipvrOqSo1iwIeHXZJJV-
UsWun9daNgiYd_wX-4WWJViGEnDzzwOKfUoUoe1Fg3ch--7JFkFl-
rrXDOjk1sUMumN3WHV9usp1PgBE5HAcJPrEBm0ValSZcUbiA"}
```

2. 테넌시/외부/리소스 API를 사용하여 시스템 ID와 X-Agent-Id를 추출합니다.

```
curl -X GET
http://10.193.192.202/tenancy/external/resource?account=account-
DARKSITE1 -H 'accept: application/json' -H 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw'
```

이 API는 다음과 같은 응답을 반환합니다. "resourceIdentifier" 아래의 값은 _WorkingEnvironment Id_를 나타내고 "agentId" 아래의 값은 _x-agent-id_를 나타냅니다.

```
[{"resourceIdentifier":"OnPremWorkingEnvironment-
pMtZND0M","resourceType":"ON_PREM","agentId":"vB_1xShPpBtUosjD7wfBlLIhqD
gIPA0wclients","resourceClass":"ON_PREM","name":"CBSFAS8300-01-
02","metadata":"{\"clusterUuid\": \"2cb6cb4b-dc07-11ec-9114-
d039ea931e09\"}","workspaceIds":["workspace2wKYjTy9"],"agentIds":["vB_1x
ShPpBtUosjD7wfBlLIhqDgIPA0wclients"]}]
```

3. StorageGRID 시스템에 연결된 시스템의 세부 정보로 NetApp Backup and Recovery 데이터베이스를 업데이트합니다. 아래와 같이 StorageGRID 의 정규화된 도메인 이름, 액세스 키, 스토리지 키를 입력해야 합니다.

```
curl -X POST 'http://10.193.192.202/account/account-
DARKSITE1/providers/cloudmanager_cbs/api/v1/sg/credentials/working-
environment/OnPremWorkingEnvironment-pMtZND0M' \
> --header 'authorization: Bearer
eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCIsImtpZCI6IjJlMGFiZjRiIn0eyJzdWIiOiJvY
2NtYXV0aHwxIiwiYXVkIjpbImh0dHBzOi8vYXBpLmNsb3VkLm5ldGFwcC5jb20iXSwiaHR0c
DovL2Nsb3VkLm5ldGFwcC5jb20vZnVsbF9uYW1lIjoiYWRtaW4iLCJodHRwOi8vY2xvdWQub
mV0YXBwLmNvbS9lbWFpbCI6ImFkbWluQG5ldGFwcC5jb20iLCJzY29wZSI6Im9wZW5pZCBwc
m9maWxlIiwiaWF0IjoxNjcyNzIyNzEzLCJleHAiOjE2NzI3NDQzMTMsImlzcyI6Imh0dHA6L
y9vY2NtYXV0aDo4NDIwLyJ9X_cQF8xttD0-S7sU2uph2cdu_kN-
fLWpdJJX98HODwPpVUitLcxV28_sQhuopjWobozPelNISf7KvMqcoXc5kLDyX-
yE0fH9gr4XgkdswjWcNvw2rRkFzjHpWrETgfqAMkZcAukV4DHuxogHWh6-
DggB1NgPZT8A_szHinud5W0HJ9c4AaT0zC-
sp81GaqMahPf0KcFVyjbBL4krOewgKHGFo_7ma_4mF39B1LCj7Vc2XvUd0wCaJvDMjwp19-
KbZqmmBX9vDnYp7SSxC1hHJRDStcFgJLdJHtowweNH2829KsjEGBTTcBdO8SvIDtctNH_GAx
wSgMT3zUfwaOimPw' \
> --header 'x-agent-id: vB_1xShPpBtUosjD7wfBlLIhqDgIPA0wclients' \
> -d '
> { "storage-server" : "sr630ip15.rtp.eng.netapp.com:10443", "access-
key": "2ZMYOAVAS5E70MCNH9", "secret-password":
"uk/6ikd4LjlXQOFnzSzP/T0zR4ZQlG0w1xgWsB" }'
```

NetApp Backup and Recovery 설정 확인

1. 각 ONTAP 시스템을 선택하고 오른쪽 패널의 백업 및 복구 서비스 옆에 있는 *백업 보기*를 클릭합니다.

   볼륨에 대해 생성된 모든 백업이 표시되어야 합니다.

2. 복원 대시보드의 검색 및 복원 섹션에서 *인덱싱 설정*을 클릭합니다.

   이전에 색인 카탈로그 기능이 활성화된 시스템은 계속 활성화된 상태로 유지되는지 확인하세요.

3. 검색 및 복원 페이지에서 몇 가지 카탈로그 검색을 실행하여 인덱싱된 카탈로그 복원이 성공적으로 완료되었는지 확인합니다.

NetApp Backup and Recovery 사용하여 ONTAP 시스템의 백업을 관리하세요

NetApp Backup and Recovery 사용하면 백업 일정 변경, 볼륨 백업 활성화/비활성화, 백업 일시 중지, 백업 삭제, 백업 강제 삭제 등을 통해 Cloud Volumes ONTAP 및 온프레미스 ONTAP 시스템의 백업을 관리할 수 있습니다. 여기에는 스냅샷, 복제된 볼륨, 개체 스토리지의 백업 파일을 포함한 모든 유형의 백업이 포함됩니다. NetApp Backup and Recovery 의 등록을 취소할 수도 있습니다.

스토리지 시스템이나 클라우드 공급자 환경에서 직접 백업 파일을 관리하거나 변경하지 마세요. 이렇게 하면 파일이 손상될 수 있으며 지원되지 않는 구성이 발생할 수 있습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

시스템의 볼륨 백업 상태 보기

볼륨 백업 대시보드에서 현재 백업 중인 모든 볼륨 목록을 볼 수 있습니다. 여기에는 스냅샷, 복제된 볼륨, 개체 스토리지의 백업 파일을 포함한 모든 유형의 백업이 포함됩니다. 현재 백업되지 않은 시스템의 볼륨도 볼 수 있습니다.

단계

1. 콘솔 메뉴에서 *보호 > 백업 및 복구*를 선택합니다.
2. 볼륨 메뉴를 선택하면 Cloud Volumes ONTAP 및 온프레미스 ONTAP 시스템의 백업된 볼륨 목록을 볼 수 있습니다.
3. 특정 시스템의 특정 볼륨을 찾는 경우 시스템과 볼륨별로 목록을 구체화할 수 있습니다. 검색 필터를 사용할 수도 있고, 볼륨 스타일(FlexVol 또는 FlexGroup), 볼륨 유형 등을 기준으로 열을 정렬할 수도 있습니다.

   추가 열(집계, 보안 스타일(Windows 또는 UNIX), 스냅샷 정책, 복제 정책, 백업 정책)을 표시하려면 더하기 기호를 선택합니다.

4. "기존 보호" 열에서 보호 옵션의 상태를 검토하세요. 3개의 아이콘은 "로컬 스냅샷", "복제된 볼륨", "개체 스토리지의 백업"을 의미합니다.

   각 아이콘은 해당 백업 유형이 활성화되면 불이 켜지고, 비활성화되면 회색으로 표시됩니다. 각 아이콘 위에 마우스 커서를 올리면 사용 중인 백업 정책과 각 백업 유형에 대한 기타 관련 정보를 확인할 수 있습니다.

시스템의 추가 볼륨에 대한 백업 활성화

NetApp Backup and Recovery 처음 활성화할 때 시스템의 일부 볼륨에서만 백업을 활성화한 경우 나중에 추가 볼륨에서 백업을 활성화할 수 있습니다.

단계

1. 볼륨 탭에서 백업을 활성화할 볼륨을 선택하고 작업 메뉴를 선택합니다. ••• 해당 행의 맨 끝에서 *3-2-1 보호 활성화*를 선택하십시오.
2. 백업 전략 정의 페이지에서 백업 아키텍처를 선택한 다음 로컬 스냅샷, 복제된 볼륨, 백업 파일에 대한 정책과 기타 세부 정보를 정의합니다. 이 시스템에서 활성화한 초기 볼륨의 백업 옵션에 대한 세부 정보를 확인하세요. 그런 다음 *다음*을 선택하세요.
3. 이 볼륨의 백업 설정을 검토한 다음 *백업 활성화*를 선택합니다.

기존 볼륨에 할당된 백업 설정 변경

정책이 할당된 기존 볼륨에 할당된 백업 정책을 변경할 수 있습니다. 로컬 스냅샷, 복제된 볼륨 및 백업 파일에 대한 정책을 변경할 수 있습니다. 볼륨에 적용하려는 새로운 스냅샷, 복제 또는 백업 정책은 이미 존재해야 합니다.

단일 볼륨의 백업 설정 편집

단계

1. 볼륨 메뉴에서 정책 설정을 수정하려는 볼륨을 찾고, [작업] 메뉴를 선택합니다. ••• 해당 행의 맨 끝에서 *백업 전략 편집*을 선택합니다.
2. 백업 전략 편집 페이지에서 로컬 스냅샷, 복제된 볼륨 및 백업 파일에 대한 기존 백업 정책을 변경하고 *다음*을 선택합니다.

   이 클러스터에 대해 NetApp Backup and Recovery 활성화할 때 초기 백업 정책에서 클라우드 백업에 대해 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우 DataLock으로 구성된 다른 정책만 표시됩니다. NetApp Backup and Recovery 활성화할 때 _DataLock 및 랜섬웨어 복원력_을 활성화하지 않은 경우 DataLock이 구성되지 않은 다른 클라우드 백업 정책만 표시됩니다.

3. 이 볼륨의 백업 설정을 검토한 다음 *백업 활성화*를 선택합니다.

여러 볼륨의 백업 설정 편집

여러 볼륨에서 동일한 백업 설정을 사용하려면 여러 볼륨에서 동시에 백업 설정을 활성화하거나 편집할 수 있습니다. 백업 설정이 없는 볼륨, 스냅샷 설정만 있는 볼륨, 클라우드 백업 설정만 있는 볼륨 등을 선택하고 다양한 백업 설정으로 모든 볼륨에 대량 변경을 적용할 수 있습니다.

여러 볼륨으로 작업할 때 모든 볼륨은 다음과 같은 공통적인 특성을 가져야 합니다.

- 같은 시스템
- 동일한 스타일(FlexVol 또는 FlexGroup 볼륨)
- 동일한 유형(읽기-쓰기 또는 데이터 보호 볼륨)

백업용으로 활성화된 볼륨이 5개 이상인 경우 NetApp Backup and Recovery 한 번에 5개의 볼륨만 초기화합니다. 이 작업이 완료되면 모든 볼륨이 초기화될 때까지 5개씩 그룹으로 나누어 계속 진행됩니다.

단계

1. 볼륨 탭에서 볼륨이 있는 시스템별로 필터링합니다.
2. 백업 설정을 관리할 모든 볼륨을 선택합니다.
3. 구성하려는 백업 작업 유형에 따라 대량 작업 메뉴에서 버튼을 클릭합니다.

백업 작업...	이 버튼을 선택하세요...
스냅샷 백업 설정 관리	로컬 스냅샷 관리
복제 백업 설정 관리	복제 관리
클라우드 백업 설정 관리	백업 관리
다양한 유형의 백업 설정을 관리합니다. 이 옵션을 사용하면 백업 아키텍처도 변경할 수 있습니다.	백업 및 복구 관리

4. 나타나는 백업 페이지에서 로컬 스냅샷, 복제된 볼륨 또는 백업 파일에 대한 기존 백업 정책을 변경하고 *저장*을 선택합니다.

   이 클러스터에 대해 NetApp Backup and Recovery 활성화할 때 초기 백업 정책에서 클라우드 백업에 대해 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우 DataLock으로 구성된 다른 정책만 표시됩니다. NetApp

Backup and Recovery 활성화할 때 _DataLock 및 랜섬웨어 복원력_을 활성화하지 않은 경우 DataLock이 구성되지 않은 다른 클라우드 백업 정책만 표시됩니다.

언제든지 수동 볼륨 백업을 생성합니다.

언제든지 주문형 백업을 만들어 볼륨의 현재 상태를 캡처할 수 있습니다. 이 기능은 볼륨에 매우 중요한 변경 사항이 적용되었고 해당 데이터를 보호하기 위해 다음에 예약된 백업을 기다리고 싶지 않은 경우에 유용할 수 있습니다. 이 기능을 사용하면 현재 백업되지 않고 있는 볼륨에 대한 백업을 생성하여 현재 상태를 캡처할 수도 있습니다.

볼륨의 객체 저장소에 임시 스냅샷 또는 백업을 생성할 수 있습니다. 임시 복제 볼륨을 생성할 수 없습니다.

백업 이름에는 타임스탬프가 포함되어 있으므로 다른 예약된 백업과 주문형 백업을 구별할 수 있습니다.

이 클러스터에 대해 NetApp Backup and Recovery 활성화할 때 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우, 주문형 백업도 DataLock으로 구성되고 보존 기간은 30일이 됩니다. 임시 백업에는 랜섬웨어 검사가 지원되지 않습니다. "DataLock 및 랜섬웨어 보호에 대해 자세히 알아보세요".

임시 백업을 생성하면 소스 볼륨에 스냅샷이 생성됩니다. 이 스냅샷은 일반 스냅샷 일정에 포함되지 않으므로 회전하지 않습니다. 백업이 완료되면 소스 볼륨에서 이 스냅샷을 수동으로 삭제할 수 있습니다. 이를 통해 이 스냅샷과 관련된 블록을 해제할 수 있습니다. 스냅샷의 이름은 다음으로 시작합니다. `cbs-snapshot-adhoc-` . "ONTAP CLI를 사용하여 스냅샷을 삭제하는 방법을 알아보세요." .

데이터 보호 볼륨에서는 주문형 볼륨 백업이 지원되지 않습니다.

단계

1. 볼륨 탭에서 다음을 선택하세요.••• 볼륨에 대해 백업 > *임시 백업 만들기*를 선택합니다.

백업이 생성될 때까지 해당 볼륨의 백업 상태 열은 "진행 중"으로 표시됩니다.

각 볼륨에 대한 백업 목록 보기

각 볼륨에 존재하는 모든 백업 파일 목록을 볼 수 있습니다. 이 페이지에는 소스 볼륨, 대상 위치, 마지막으로 수행된 백업, 현재 백업 정책, 백업 파일 크기 등의 백업 세부 정보가 표시됩니다.

단계

1. 볼륨 탭에서 다음을 선택하세요.••• 소스 볼륨의 경우 *볼륨 세부 정보 보기*를 선택합니다.

   볼륨에 대한 세부 정보와 스냅샷 목록이 표시됩니다.

2. 각 백업 유형에 대한 모든 백업 파일 목록을 보려면 스냅샷, 복제 또는 *백업*을 선택하세요.

개체 스토리지의 볼륨 백업에 대한 랜섬웨어 검사 실행

NetApp Backup and Recovery 백업을 개체 파일로 생성할 때와 백업 파일의 데이터를 복원할 때 랜섬웨어 공격의 증거를 찾기 위해 백업 파일을 검사합니다. 언제든지 주문형 검사를 실행하여 개체 스토리지에서 특정 백업 파일의 사용 가능성을 확인할 수도 있습니다. 특정 볼륨에서 랜섬웨어 문제가 발생했고 해당 볼륨의 백업이 영향을 받지 않았는지 확인하려는 경우 이 기능이 유용할 수 있습니다.

이 기능은 볼륨 백업이 ONTAP 9.11.1 이상이 설치된 시스템에서 생성되고, 백업-개체 정책에서 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우에만 사용할 수 있습니다.

단계

1. 볼륨 탭에서 다음을 선택하세요.••• 소스 볼륨의 경우 *볼륨 세부 정보 보기*를 선택합니다.

   해당 볼륨에 대한 세부 정보가 표시됩니다.

2. *백업*을 선택하면 개체 스토리지에 있는 백업 파일 목록을 볼 수 있습니다.
3. 선택하다••• 랜섬웨어를 검사하려는 볼륨 백업 파일에 대해 *랜섬웨어 검사*를 클릭합니다.

   랜섬웨어 복원력 열은 검사가 진행 중임을 보여줍니다.

소스 볼륨과의 복제 관계 관리

두 시스템 간에 데이터 복제를 설정한 후에는 데이터 복제 관계를 관리할 수 있습니다.

단계

1. 볼륨 탭에서 다음을 선택하세요.••• 소스 볼륨에 대해 복제 옵션을 선택합니다. 사용 가능한 모든 옵션을 볼 수 있습니다.
2. 수행할 복제 작업을 선택하세요.

   다음 표에서는 사용 가능한 작업을 설명합니다.

행동	설명
뷰 복제	볼륨 관계에 대한 세부 정보를 표시합니다. 전송 정보, 마지막 전송 정보, 볼륨에 대한 세부 정보, 관계에 할당된 보호 정책에 대한 정보 등이 표시됩니다.
복제 업데이트	소스 볼륨과 동기화할 대상 볼륨을 업데이트하기 위해 증분 전송을 시작합니다.
복제 일시 중지	대상 볼륨을 업데이트하기 위해 스냅샷의 증분 전송을 일시 중지합니다. 증분 업데이트를 다시 시작하려면 나중에 다시 시작할 수 있습니다.
복제 중단	소스 볼륨과 대상 볼륨 간의 관계를 끊고, 데이터 액세스를 위해 대상 볼륨을 활성화하여 읽기-쓰기가 가능하도록 합니다. 이 옵션은 일반적으로 데이터 손상, 실수로 삭제 또는 오프라인 상태와 같은 이벤트로 인해 소스 볼륨이 데이터를 제공할 수 없을 때 사용됩니다.https://docs.netapp.com/us-en/ontap-sm-classic/volume-disaster-recovery/index.html["ONTAP 설명서에서 데이터 액세스를 위한 대상 볼륨을 구성하고 소스 볼륨을 다시 활성화하는 방법을 알아보세요."^]
복제 중단	이 볼륨을 대상 시스템에 백업하는 기능을 비활성화하고 볼륨을 복원하는 기능도 비활성화합니다. 기존 백업은 삭제되지 않습니다. 이렇게 해도 소스 볼륨과 대상 볼륨 간의 데이터 보호 관계는 삭제되지 않습니다.
역방향 재동기화	소스 볼륨과 대상 볼륨의 역할을 바꿉니다. 원본 볼륨의 내용은 대상 볼륨의 내용으로 덮어쓰여집니다. 이 기능은 오프라인 상태가 된 소스 볼륨을 다시 활성화할 때 유용합니다. 마지막 데이터 복제와 소스 볼륨이 비활성화된 시간 사이에 원본 소스 볼륨에 기록된 모든 데이터는 보존되지 않습니다.
관계 삭제	소스 볼륨과 대상 볼륨 간의 데이터 보호 관계를 삭제합니다. 즉, 볼륨 간에 데이터 복제가 더 이상 발생하지 않습니다. 이 작업은 데이터 액세스를 위한 대상 볼륨을 활성화하지 않습니다. 즉, 읽기/쓰기가 가능하지 않습니다. 이 작업을 수행하면 시스템 간에 다른 데이터 보호 관계가 없는 경우 클러스터 피어 관계와 스토리지 VM(SVM) 피어 관계도 삭제됩니다.

결과

작업을 선택하면 콘솔에서 관계가 업데이트됩니다.

기존 클라우드 백업 정책 편집

현재 시스템의 볼륨에 적용된 백업 정책의 속성을 변경할 수 있습니다. 백업 정책을 변경하면 해당 정책을 사용하는 모든 기존 볼륨에 영향을 미칩니다.

- 이 클러스터에 대해 NetApp Backup and Recovery 활성화할 때 초기 정책에서 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우, 편집하는 모든 정책은 동일한 DataLock 설정(거버넌스 또는 규정 준수)으로 구성되어야 합니다. NetApp Backup and Recovery 활성화할 때 _DataLock 및 랜섬웨어 복원력_을 활성화하지 않은 경우 지금 DataLock을 활성화할 수 없습니다.
- AWS에서 백업을 생성할 때 NetApp Backup and Recovery 활성화할 때 첫 번째 백업 정책에서 *S3 Glacier* 또는 _S3 Glacier Deep Archive_를 선택한 경우, 백업 정책을 편집할 때 해당 계층은 사용 가능한 유일한 아카이브 계층이 됩니다. 첫 번째 백업 정책에서 보관 계층을 선택하지 않은 경우 정책을 편집할 때 _S3 Glacier_가 유일한 보관 옵션이 됩니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. 백업 설정 페이지에서 다음을 선택하세요.••• 정책 설정을 변경하려는 시스템의 경우 *정책 관리*를 선택합니다.
3. 정책 관리 페이지에서 해당 시스템에서 변경하려는 백업 정책에 대해 *편집*을 선택합니다.
4. 정책 편집 페이지에서 아래쪽 화살표를 선택하여 레이블 및 보존 섹션을 확장하여 일정 및/또는 백업 보존을 변경하고 *저장*을 선택합니다.

   클러스터에서 ONTAP 9.10.1 이상을 실행하는 경우 특정 일수가 지난 후 보관 저장소에 대한 백업 계층화를 활성화하거나 비활성화하는 옵션도 있습니다.

   "AWS 보관 스토리지 사용에 대해 자세히 알아보세요". "Azure 보관 저장소 사용에 대해 자세히 알아보세요". "Google 보관 저장소 사용에 대해 자세히 알아보세요". (ONTAP 9.12.1이 필요합니다.)

   참고로, 아카이브 저장소로 계층화된 백업 파일은 백업 계층화를 중지하더라도 해당 계층에 그대로 남아 있으며, 자동으로 표준 계층으로 다시 이동되지 않습니다. 표준 티어에는 새로운 볼륨 백업만 저장됩니다.

새로운 클라우드 백업 정책 추가

시스템에 대해 NetApp Backup and Recovery 활성화하면 처음에 선택한 모든 볼륨이 정의한 기본 백업 정책을 사용하여 백업됩니다. 서로 다른 복구 지점 목표(RPO)를 가진 특정 볼륨에 서로 다른 백업 정책을 할당하려는 경우 해당 클러스터에 대한 추가 정책을 만들고 해당 정책을 다른 볼륨에 할당할 수 있습니다.

시스템의 특정 볼륨에 새로운 백업 정책을 적용하려면 먼저 시스템에 백업 정책을 추가해야 합니다. 그럼 당신은 할 수 있습니다해당 시스템의 볼륨에 정책을 적용합니다. .

- 이 클러스터에 대해 NetApp Backup and Recovery 활성화할 때 초기 정책에서 _DataLock 및 랜섬웨어 복원력_을 활성화한 경우, 추가로 생성하는 모든 정책은 동일한 DataLock 설정(거버넌스 또는 규정 준수)으로 구성되어야 합니다. NetApp Backup and Recovery 활성화할 때 _DataLock 및 랜섬웨어 복원력_을 활성화하지 않은 경우 DataLock을 사용하는 새 정책을 만들 수 없습니다.
- AWS에서 백업을 생성할 때 NetApp Backup and Recovery 활성화할 때 첫 번째 백업 정책에서 *S3 Glacier* 또는 _S3 Glacier Deep Archive_를 선택한 경우 해당 계층은 해당 클러스터의 향후 백업 정책에 사용할 수 있는 유일한 아카이브 계층이 됩니다. 첫 번째 백업 정책에서 보관 계층을 선택하지 않은 경우, _S3 Glacier_가 향후 정책에 대한 유일한 보관 옵션이 됩니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. 백업 설정 페이지에서 다음을 선택하세요.••• 새 정책을 추가하려는 시스템에 대해 *정책 관리*를 선택합니다.
3. 정책 관리 페이지에서 *새 정책 추가*를 선택합니다.
4. 새 정책 추가 페이지에서 아래쪽 화살표를 선택하여 레이블 및 보존 섹션을 확장하여 일정 및 백업 보존을 정의하고 *저장*을 선택합니다.

   클러스터에서 ONTAP 9.10.1 이상을 실행하는 경우 특정 일수가 지난 후 보관 저장소에 대한 백업 계층화를 활성화하거나 비활성화하는 옵션도 있습니다.

   "AWS 보관 스토리지 사용에 대해 자세히 알아보세요". "Azure 보관 저장소 사용에 대해 자세히 알아보세요". "Google 보관 저장소 사용에 대해 자세히 알아보세요". (ONTAP 9.12.1이 필요합니다.)

백업 삭제

NetApp Backup and Recovery 사용하면 단일 백업 파일을 삭제하거나, 볼륨에 대한 모든 백업을 삭제하거나, 시스템의 모든 볼륨에 대한 모든 백업을 삭제할 수 있습니다. 더 이상 백업이 필요하지 않은 경우 또는 소스 볼륨을 삭제하고 모든 백업을 제거하려는 경우 모든 백업을 삭제할 수 있습니다.

DataLock 및 랜섬웨어 보호 기능을 사용하여 잠근 백업 파일은 삭제할 수 없습니다. 하나 이상의 잠긴 백업 파일을 선택한 경우 UI에서 "삭제" 옵션을 사용할 수 없습니다.

백업이 있는 시스템이나 클러스터를 삭제하려는 경우 시스템을 삭제하기 전에 백업을 삭제해야 합니다. NetApp Backup and Recovery 시스템을 삭제할 때 자동으로 백업을 삭제하지 않으며, 현재 UI에서는 시스템이 삭제된 후 백업을 삭제하는 기능을 지원하지 않습니다. 남은 백업에 대해서는 계속해서 개체 스토리지 비용이 청구됩니다.

시스템의 모든 백업 파일을 삭제합니다.

시스템의 개체 스토리지에 있는 모든 백업을 삭제해도 해당 시스템의 볼륨에 대한 향후 백업은 비활성화되지 않습니다. 시스템의 모든 볼륨에 대한 백업 생성을 중지하려면 백업을 비활성화할 수 있습니다.여기에 설명된 대로 .

이 작업은 스냅샷이나 복제된 볼륨에는 영향을 미치지 않습니다. 이러한 유형의 백업 파일은 삭제되지 않습니다.

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. 선택하다••• 모든 백업을 삭제하려는 시스템의 경우 *모든 백업 삭제*를 선택합니다.
3. 확인 대화 상자에서 시스템 이름을 입력합니다.

4. *고급 설정*을 선택하세요.
5. 백업 강제 삭제: 모든 백업을 강제로 삭제할지 여부를 표시합니다.

   극단적인 경우에는 NetApp Backup and Recovery 더 이상 백업에 액세스하지 못하도록 설정해야 할 수도 있습니다. 예를 들어, 서비스가 더 이상 백업 버킷에 액세스할 수 없거나 백업이 DataLock으로 보호되지만 더 이상 필요하지 않은 경우 이런 일이 발생할 수 있습니다. 이전에는 직접 삭제할 수 없었고 NetApp 지원팀에 문의해야 했습니다. 이 릴리스에서는 볼륨 및 시스템 수준에서 백업을 강제로 삭제하는 옵션을 사용할 수 있습니다.

   이 옵션은 신중하게 사용하고 극단적인 정리가 필요한 경우에만 사용하세요. NetApp Backup and Recovery 개체 스토리지에서 백업이 삭제되지 않더라도 더 이상 이러한 백업에 액세스할 수 없습니다. 클라우드 제공업체에 가서 수동으로 백업을 삭제해야 합니다.

6. *삭제*를 선택하세요.

볼륨에 대한 모든 백업 파일 삭제

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

단계

1. 볼륨 탭에서 다음을 클릭합니다.••• 소스 볼륨의 경우 *세부 정보 및 백업 목록*을 선택합니다.

   모든 백업 파일 목록이 표시됩니다.

2. 작업 > *모든 백업 삭제*를 선택합니다.
3. 볼륨 이름을 입력하세요.
4. *고급 설정*을 선택하세요.
5. 백업 강제 삭제: 모든 백업을 강제로 삭제할지 여부를 표시합니다.

   극단적인 경우에는 NetApp Backup and Recovery 더 이상 백업에 액세스하지 못하도록 설정해야 할 수도 있습니다. 예를 들어, 서비스가 더 이상 백업 버킷에 액세스할 수 없거나 백업이 DataLock으로 보호되지만 더 이상 필요하지 않은 경우 이런 일이 발생할 수 있습니다. 이전에는 직접 삭제할 수 없었고 NetApp 지원팀에 문의해야 했습니다. 이 릴리스에서는 볼륨 및 시스템 수준에서 백업을 강제로 삭제하는 옵션을 사용할 수 있습니다.

   이 옵션은 신중하게 사용하고 극단적인 정리가 필요한 경우에만 사용하세요. NetApp Backup and Recovery 개체 스토리지에서 백업이 삭제되지 않더라도 더 이상 이러한 백업에 액세스할 수 없습니다. 클라우드 제공업체에 가서 수동으로 백업을 삭제해야 합니다.

6. *삭제*를 선택하세요.

볼륨에 대한 단일 백업 파일 삭제

더 이상 필요하지 않으면 단일 백업 파일을 삭제할 수 있습니다. 여기에는 볼륨 스냅샷의 단일 백업이나 개체 스토리지의 백업을 삭제하는 것이 포함됩니다.

복제된 볼륨(데이터 보호 볼륨)은 삭제할 수 없습니다.

단계

1. 볼륨 탭에서 다음을 선택하세요.••• 소스 볼륨의 경우 *볼륨 세부 정보 보기*를 선택합니다.

볼륨에 대한 세부 정보가 표시되고, 스냅샷, 복제 또는 *백업*을 선택하면 해당 볼륨의 모든 백업 파일 목록을 볼 수 있습니다. 기본적으로 사용 가능한 스냅샷이 표시됩니다.

2. 삭제하려는 백업 파일 유형을 보려면 스냅샷 또는 *백업*을 선택하세요.
3. 선택하다... 삭제하려는 볼륨 백업 파일에 대해 *삭제*를 선택합니다.
4. 확인 대화 상자에서 *삭제*를 선택합니다.

볼륨 백업 관계 삭제

볼륨의 백업 관계를 삭제하면 새 백업 파일 생성을 중지하고 소스 볼륨을 삭제하지만 기존 백업 파일은 모두 보존하려는 경우 보관 메커니즘이 제공됩니다. 이렇게 하면 나중에 필요할 경우 소스 스토리지 시스템의 공간을 비우는 동시에 백업 파일에서 볼륨을 복원할 수 있습니다.

반드시 소스 볼륨을 삭제할 필요는 없습니다. 볼륨의 백업 관계를 삭제하고 소스 볼륨을 유지할 수 있습니다. 이 경우 나중에 볼륨의 백업을 "활성화"할 수 있습니다. 이 경우에도 원본 기준 백업 사본이 계속 사용됩니다. 새로운 기준 백업 사본이 생성되어 클라우드로 내보내지지 않습니다. 백업 관계를 다시 활성화하면 볼륨에 기본 백업 정책이 할당됩니다.

이 기능은 시스템에서 ONTAP 9.12.1 이상을 실행하는 경우에만 사용할 수 있습니다.

NetApp Backup and Recovery 사용자 인터페이스에서 소스 볼륨을 삭제할 수 없습니다. 하지만 콘솔 시스템 페이지에서 볼륨 세부 정보 페이지를 열 수 있습니다. "거기에서 볼륨을 삭제하세요" .

관계가 삭제되면 개별 볼륨 백업 파일을 삭제할 수 없습니다. 하지만 볼륨에 대한 모든 백업을 삭제할 수는 있습니다.

단계

1. 볼륨 탭에서 다음을 선택하세요... 소스 볼륨의 경우 백업 > *관계 삭제*를 선택합니다.

시스템에 대한 **NetApp Backup and Recovery** 비활성화

시스템의 NetApp Backup and Recovery 비활성화하면 시스템의 각 볼륨 백업이 비활성화되고 볼륨을 복원하는 기능도 비활성화됩니다. 기존 백업은 삭제되지 않습니다. 이렇게 하면 시스템에서 백업 서비스가 등록 해제되는 것은 아닙니다. 기본적으로 모든 백업 및 복원 활동을 일정 기간 동안 일시 중지할 수 있습니다.

백업에 사용되는 용량에 대한 개체 스토리지 비용은 클라우드 공급자가 계속 청구합니다.백업을 삭제하다 .

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 다음을 선택하세요... 백업을 비활성화하려는 시스템의 경우 *백업 비활성화*를 선택하세요.
3. 확인 대화 상자에서 *비활성화*를 선택합니다.

백업이 비활성화되어 있는 동안 해당 시스템에는 백업 활성화 버튼이 나타납니다. 해당 시스템의 백업 기능을 다시 활성화하려면 이 버튼을 선택하면 됩니다.

시스템에 대한 **NetApp Backup and Recovery** 등록 취소

더 이상 백업 기능을 사용하지 않고 해당 시스템에서 백업에 대한 요금이 청구되는 것을 원하지 않는 경우 해당 시스템의

NetApp Backup and Recovery 등록을 취소할 수 있습니다. 일반적으로 이 기능은 시스템을 삭제할 계획이고 백업 서비스를 취소하려는 경우에 사용됩니다.

클러스터 백업이 저장되는 대상 개체 저장소를 변경하려는 경우에도 이 기능을 사용할 수 있습니다. 시스템의 NetApp Backup and Recovery 등록을 취소한 후, 새로운 클라우드 공급자 정보를 사용하여 해당 클러스터에 대해 NetApp Backup and Recovery 활성화할 수 있습니다.

NetApp Backup and Recovery 등록 취소하려면 다음 단계를 순서대로 수행해야 합니다.

- 시스템에 대한 NetApp Backup and Recovery 비활성화
- 해당 시스템의 모든 백업을 삭제합니다.

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

단계

1. 볼륨 탭에서 *백업 설정*을 선택합니다.
2. _백업 설정 페이지_에서 다음을 선택하세요.••• 백업 서비스를 등록 취소하려는 시스템의 경우 *등록 취소*를 선택하세요.
3. 확인 대화 상자에서 *등록 취소*를 선택하세요.

ONTAP 백업에서 복원

NetApp Backup and Recovery 사용하여 백업 파일에서 ONTAP 데이터 복원

ONTAP 볼륨 데이터의 백업은 복제된 볼륨이나 개체 스토리지에 스냅샷으로 저장됩니다. 이러한 위치 중 어느 곳에서든 특정 시점의 데이터를 복원할 수 있습니다. NetApp Backup and Recovery 사용하면 필요에 따라 전체 볼륨, 폴더 또는 개별 파일을 복원할 수 있습니다.

NetApp Backup and Recovery 워크로드로 전환하려면 다음을 참조하세요."다양한 NetApp Backup and Recovery 워크로드로 전환" .

- *볼륨*을 (새로운 볼륨으로) 원래 시스템, 동일한 클라우드 계정을 사용하는 다른 시스템 또는 온프레미스 ONTAP 시스템에 복원할 수 있습니다.
- *폴더*를 원래 시스템의 볼륨, 동일한 클라우드 계정을 사용하는 다른 시스템의 볼륨 또는 온프레미스 ONTAP 시스템의 볼륨으로 복원할 수 있습니다.
- *파일*을 원래 시스템의 볼륨, 동일한 클라우드 계정을 사용하는 다른 시스템의 볼륨 또는 온프레미스 ONTAP 시스템의 볼륨으로 복원할 수 있습니다.

프로덕션 시스템에 데이터를 복원하려면 유효한 NetApp Backup and Recovery 라이선스가 필요합니다.

요약하자면, ONTAP 시스템에 볼륨 데이터를 복원하는 데 사용할 수 있는 유효한 흐름은 다음과 같습니다.

- 백업 파일 → 복원된 볼륨
- 복제된 볼륨 → 복원된 볼륨
- 스냅샷 → 복원된 볼륨

복원 작업이 완료되지 않으면 작업 모니터에 "실패"가 표시될 때까지 기다린 후 복원 작업을 다시 시도하세요.

ONTAP 데이터 복원과 관련된 제한 사항은 다음을 참조하세요."ONTAP 볼륨에 대한 백업 및 복원 제한 사항" .

복원 대시보드

복원 대시보드를 사용하여 볼륨, 폴더 및 파일 복원 작업을 수행합니다. 복원 대시보드에 액세스하려면 콘솔 메뉴에서 백업 및 복구*를 선택한 다음 *복원 탭을 선택합니다. 또한 선택할 수도 있습니다 > 서비스 패널의 백업 및 복구 서비스에서 복원 대시보드 보기

NetApp Backup and Recovery 적어도 하나의 시스템에 대해 이미 활성화되어 있어야 하며 초기 백업 파일이 있어야 합니다.

복원 대시보드는 백업 파일에서 데이터를 복원하는 두 가지 방법을 제공합니다. *찾아보기 및 복원*과 *검색 및 복원*입니다.

Browse & Restore와 **Search & Restore** 비교

넓은 의미에서, _찾아보기 및 복원_은 지난주나 지난달의 특정 볼륨, 폴더 또는 파일을 복원해야 할 때 일반적으로 더 나은 방법입니다. 파일의 이름과 위치, 마지막으로 좋은 상태였던 날짜를 알고 있을 때 더욱 그렇습니다. _검색 및 복원_은 볼륨, 폴더 또는 파일을 복원해야 하지만 정확한 이름이나 해당 볼륨이 있는 볼륨, 마지막으로 양호한 상태였던 날짜를 기억하지 못하는 경우에 일반적으로 더 좋습니다.

이 표는 두 가지 방법의 특징을 비교한 것입니다.

찾아보기 및 복원	검색 및 복원
폴더 스타일 구조를 탐색하여 단일 백업 파일 내의 볼륨, 폴더 또는 파일을 찾습니다.	*모든 백업 파일*에서 볼륨 이름 일부 또는 전체, 폴더/파일 이름 일부 또는 전체, 크기 범위 및 추가 검색 필터를 사용하여 볼륨, 폴더 또는 파일을 검색합니다.
파일이 삭제되거나 이름이 변경되고 사용자가 원래 파일 이름을 모르는 경우 파일 복구를 처리하지 않습니다.	새로 생성/삭제/이름이 변경된 디렉토리와 새로 생성/삭제/이름이 변경된 파일을 처리합니다.
빠른 복원이 지원됩니다.	빠른 복원은 지원되지 않습니다.

이 표는 백업 파일이 있는 위치를 기준으로 유효한 복원 작업 목록을 제공합니다.

백업 유형	찾아보기 및 복원			검색 및 복원		
	볼륨 복원	파일 복원	폴더 복원	볼륨 복원	파일 복원	폴더 복원
스냅샷	예	아니요	아니요	예	예	예
복제된 볼륨	예	아니요	아니요	예	예	예
백업 파일	예	예	예	예	예	예

두 가지 복원 방법을 사용하기 전에 리소스 요구 사항을 충족하도록 환경을 구성하세요. 자세한 내용은 다음 섹션을 참조하세요.

사용하려는 복원 작업 유형에 대한 요구 사항과 복원 단계를 확인하세요.

- "찾아보기 및 복원을 사용하여 볼륨 복원"
- "찾아보기 및 복원을 사용하여 폴더 및 파일 복원"
- "검색 및 복원을 사용하여 볼륨, 폴더 및 파일 복원"

검색 및 복원을 사용하여 **ONTAP** 백업에서 복원

검색 및 복원을 사용하면 ONTAP 백업 파일에서 볼륨, 폴더 또는 파일을 복구할 수 있습니다. 검색 및 복원을 사용하면 정확한 시스템, 볼륨 또는 파일 이름이 없어도 모든 백업(로컬 스냅샷, 복제된 볼륨, 개체 스토리지 포함)을 검색할 수 있습니다.

로컬 스냅샷이나 복제된 볼륨에서 복원하는 것이 일반적으로 개체 스토리지에서 복원하는 것보다 빠르고 비용이 저렴합니다.

전체 볼륨을 복원할 때 NetApp Backup and Recovery 백업 데이터를 사용하여 새 볼륨을 만듭니다. 원래 시스템, 동일한 클라우드 계정 내의 다른 시스템 또는 온프레미스 ONTAP 시스템으로 복원할 수 있습니다. 폴더와 파일은 원래 위치, 동일한 시스템의 다른 볼륨, 동일한 클라우드 계정의 다른 시스템 또는 온프레미스 시스템으로 복원할 수 있습니다.

복원 기능은 ONTAP 버전에 따라 다릅니다.

- 폴더**:** ONTAP 9.13.0 이상을 사용하면 모든 파일과 하위 폴더가 포함된 폴더를 복원할 수 있습니다. 이전 버전에서는 폴더 내의 파일만 복원할 수 있습니다.
- 보관 저장소**:** 보관 저장소(ONTAP 9.10.1 이상에서 사용 가능)에서 복원하는 경우 속도가 느리고 추가 비용이 발생할 수 있습니다.
- 목적지 클러스터 요구 사항**:**
  - 볼륨 복원: ONTAP 9.10.1 이상
  - 파일 복원: ONTAP 9.11.1 이상
  - Google Archive 및 StorageGRID: ONTAP 9.12.1 이상
  - 폴더 복원: ONTAP 9.13.1 이상

"AWS 보관 스토리지에서 복원하는 방법에 대해 자세히 알아보세요.". "Azure 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". "Google 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.".

- 개체 스토리지의 백업 파일에 DataLock 및 랜섬웨어 보호 기능이 구성된 경우, ONTAP 버전이 9.13.1 이상인 경우에만 폴더 수준 복원이 지원됩니다. 이전 버전의 ONTAP 사용하는 경우 백업 파일에서 전체 볼륨을 복원한 다음 필요한 폴더와 파일에 액세스할 수 있습니다.
- 개체 스토리지의 백업 파일이 보관 스토리지에 있는 경우, ONTAP 버전이 9.13.1 이상인 경우에만 폴더 수준 복원이 지원됩니다. 이전 버전의 ONTAP 사용하는 경우 보관되지 않은 최신 백업 파일에서 폴더를 복원하거나 보관된 백업에서 전체 볼륨을 복원한 다음 필요한 폴더와 파일에 액세스할 수 있습니다.
- Azure 보관 저장소에서 StorageGRID 시스템으로 데이터를 복원하는 경우 "높음" 복원 우선 순위는 지원되지 않습니다.
- 현재 ONTAP S3 개체 스토리지의 볼륨에서는 폴더 복원이 지원되지 않습니다.

시작하기 전에 복원하려는 볼륨이나 파일의 이름이나 위치를 어느 정도 알고 있어야 합니다.

검색 및 복원 지원 시스템 및 개체 스토리지 공급자

보조 시스템(복제된 볼륨) 또는 개체 스토리지(백업 파일)에 있는 백업 파일에서 ONTAP 데이터를 다음 시스템으로 복원할 수 있습니다. 스냅샷은 소스 시스템에 저장되며 동일한 시스템으로만 복원할 수 있습니다.

참고**:** 모든 유형의 백업 파일에서 볼륨과 파일을 복원할 수 있지만, 현재는 개체 스토리지의 백업 파일에서만 폴더를 복원할 수 있습니다.

백업 파일 위치		목적지 시스템
객체 저장소(백업)	2차 시스템(복제)	
아마존 S3	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
Azure Blob	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
구글 클라우드 스토리지	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
NetApp StorageGRID	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP	온프레미스 ONTAP 시스템
ONTAP S3	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP	온프레미스 ONTAP 시스템

검색 및 복원의 경우 콘솔 에이전트를 다음 위치에 설치할 수 있습니다.

- Amazon S3의 경우 콘솔 에이전트는 AWS 또는 사내에 배포될 수 있습니다.
- Azure Blob의 경우 콘솔 에이전트는 Azure 또는 사내에 배포될 수 있습니다.
- Google Cloud Storage의 경우 콘솔 에이전트는 Google Cloud Platform VPC에 배포되어야 합니다.
- StorageGRID 의 경우 콘솔 에이전트는 인터넷 접속 여부와 관계없이 사내에 배포되어야 합니다.
- ONTAP S3의 경우 콘솔 에이전트는 인터넷 접속 여부와 관계없이 사내 또는 클라우드 공급자 환경에 배포될 수 있습니다.

"온프레미스 ONTAP 시스템"에 대한 참조에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

검색 및 복원 필수 조건

검색 및 복원을 활성화하기 전에 환경이 다음 요구 사항을 충족하는지 확인하세요.

- 클러스터 요구 사항:
  - ONTAP 버전은 9.8 이상이어야 합니다.
  - 볼륨이 있는 스토리지 VM(SVM)에는 구성된 데이터 LIF가 있어야 합니다.
  - 볼륨에서 NFS를 활성화해야 합니다(NFS와 SMB/CIFS 볼륨 모두 지원됨).
  - SVM에서 SnapDiff RPC 서버를 활성화해야 합니다. 시스템에서 인덱싱을 활성화하면 콘솔에서 자동으로 이 작업이 수행됩니다. (SnapDiff는 스냅샷 간의 파일 및 디렉토리 차이점을 빠르게 식별하는 기술입니다.)

- NetApp 검색 및 복원의 복원력을 높이기 위해 콘솔 에이전트에 별도의 볼륨을 마운트할 것을 권장합니다. 지침은 다음을 참조하세요.카탈로그를 다시 인덱싱하려면 볼륨을 마운트하세요. .

레거시 검색 및 복원 필수 구성 요소(인덱싱된 카탈로그 **v1** 사용)

레거시 인덱싱을 사용할 때 검색 및 복원에 대한 요구 사항은 다음과 같습니다.

- AWS 요구 사항:
  - 콘솔에 권한을 제공하는 사용자 역할에 특정 Amazon Athena, AWS Glue 및 AWS S3 권한을 추가해야 합니다. "모든 권한이 올바르게 구성되었는지 확인하세요.".

    과거에 구성한 콘솔 에이전트와 함께 NetApp Backup and Recovery 이미 사용하고 있는 경우 지금 콘솔 사용자 역할에 Athena 및 Glue 권한을 추가해야 합니다. 검색 및 복원에 필요합니다.

- Azure 요구 사항:
  - 구독을 통해 Azure Synapse Analytics 리소스 공급자("Microsoft.Synapse")를 등록해야 합니다. "구독을 위해 이 리소스 공급자를 등록하는 방법을 확인하세요." . 리소스 공급자를 등록하려면 구독 소유자 또는 *기여자*여야 합니다.
  - 콘솔에 권한을 제공하는 사용자 역할에 특정 Azure Synapse Workspace 및 Data Lake Storage 계정 권한을 추가해야 합니다. "모든 권한이 올바르게 구성되었는지 확인하세요.".

    이전에 구성한 콘솔 에이전트와 함께 NetApp Backup and Recovery 이미 사용하고 있는 경우 지금 콘솔 사용자 역할에 Azure Synapse Workspace 및 Data Lake Storage 계정 권한을 추가해야 합니다. 검색 및 복원에 필요합니다.

  - 콘솔 에이전트는 인터넷과의 HTTP 통신을 위해 프록시 서버 없이 구성되어야 합니다. 콘솔 에이전트에 대해 HTTP 프록시 서버를 구성한 경우 검색 및 복원 기능을 사용할 수 없습니다.
- Google Cloud 요구 사항:
  - NetApp Console 권한을 제공하는 사용자 역할에 특정 Google BigQuery 권한을 추가해야 합니다. "모든 권한이 올바르게 구성되었는지 확인하세요.".

    과거에 구성한 콘솔 에이전트와 함께 NetApp Backup and Recovery 이미 사용하고 있는 경우 지금 콘솔 사용자 역할에 BigQuery 권한을 추가해야 합니다. 검색 및 복원에 필요합니다.

- StorageGRID 및 ONTAP S3 요구 사항:

  구성에 따라 검색 및 복원이 구현되는 방법은 2가지가 있습니다.

  - 계정에 클라우드 공급자 자격 증명이 없으면 인덱싱된 카탈로그 정보는 콘솔 에이전트에 저장됩니다.

    Indexed Catalog v2에 대한 자세한 내용은 아래 섹션의 Indexed Catalog를 활성화하는 방법을 참조하세요.

  - 개인(다크) 사이트에서 콘솔 에이전트를 사용하는 경우 인덱싱된 카탈로그 정보는 콘솔 에이전트에 저장됩니다(콘솔 에이전트 버전 3.9.25 이상 필요).
  - 만약 당신이 가지고 있다면 "AWS 자격 증명" 또는 "Azure 자격 증명" 계정에서 색인된 카탈로그는 클라우드 제공자에 저장됩니다. 이는 클라우드에 배포된 콘솔 에이전트와 마찬가지입니다. (두 자격 증명이 모두 있는 경우 기본적으로 AWS가 선택됩니다.)

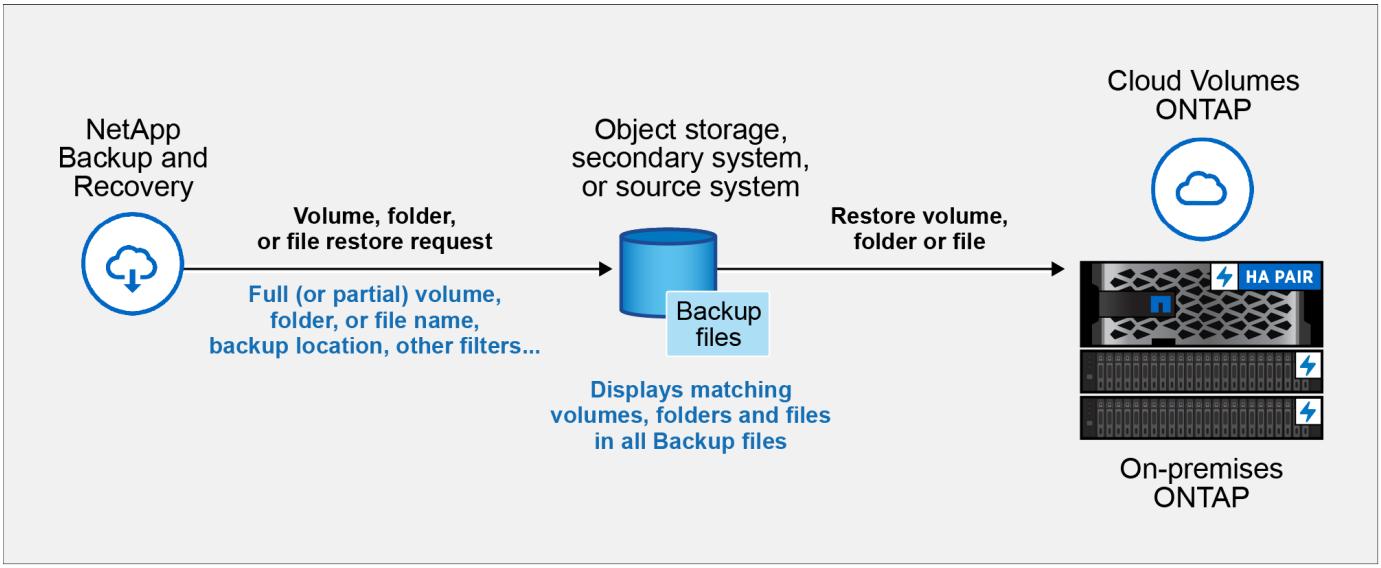
    온프레미스 콘솔 에이전트를 사용하는 경우에도 콘솔 에이전트 권한과 클라우드 공급자 리소스 모두에 대한 클라우드 공급자 요구 사항을 충족해야 합니다. 이 구현을 사용하는 경우 위의 AWS 및 Azure 요구 사항을 참조하세요.

검색 및 복원 프로세스

과정은 다음과 같습니다.

1. 검색 및 복원을 사용하려면 먼저 볼륨 데이터를 복원하려는 각 소스 시스템에서 "인덱싱"을 활성화해야 합니다. 이를 통해 색인된 카탈로그는 모든 볼륨의 백업 파일을 추적할 수 있습니다.
2. 볼륨 백업에서 볼륨이나 파일을 복원하려면 _검색 및 복원_에서 *검색 및 복원*을 선택합니다.
3. 볼륨, 폴더 또는 파일에 대한 검색 기준을 부분 또는 전체 볼륨 이름, 부분 또는 전체 파일 이름, 백업 위치, 크기 범위, 생성 날짜 범위, 기타 검색 필터로 입력하고 *검색*을 선택합니다.

   검색 결과 페이지에는 검색 기준과 일치하는 파일이나 볼륨이 있는 모든 위치가 표시됩니다.
4. 볼륨이나 파일을 복원할 위치에 대해 *모든 백업 보기*를 선택한 다음, 사용하려는 실제 백업 파일에서 *복원*을 선택합니다.
5. 볼륨, 폴더 또는 파일을 복원할 위치를 선택하고 *복원*을 선택합니다.
6. 볼륨, 폴더 또는 파일이 복원됩니다.



일부 이름만 알면 NetApp Backup and Recovery 검색 결과와 일치하는 모든 백업 파일을 검색합니다.

각 시스템에 대해 색인된 카탈로그를 활성화합니다.

검색 및 복원을 사용하려면 먼저 볼륨이나 파일을 복원할 각 소스 시스템에서 "인덱싱"을 활성화해야 합니다. 이를 통해 색인 카탈로그는 모든 볼륨과 모든 백업 파일을 추적하여 검색을 매우 빠르고 효율적으로 수행할 수 있습니다.

색인 카탈로그는 시스템의 모든 볼륨과 백업 파일에 대한 메타데이터를 저장하는 데이터베이스입니다. 이는 검색 및 복원 기능에서 복원하려는 데이터가 포함된 백업 파일을 빠르게 찾는 데 사용됩니다.

색인된 카탈로그 기능

NetApp Backup and Recovery 인덱싱된 카탈로그를 사용할 때 별도의 버킷을 프로비저닝하지 않습니다. 대신 AWS, Azure, Google Cloud Platform, StorageGRID 또는 ONTAP S3에 저장된 백업의 경우 서비스는 콘솔 에이전트 또는 클라우드 공급자 환경에서 공간을 프로비저닝합니다.

색인 카탈로그는 다음을 지원합니다.

- 3분 이내에 글로벌 검색 효율성 향상
- 최대 50억 개의 파일
- 클러스터당 최대 5000개의 볼륨
- 볼륨당 최대 100K 스냅샷
- 기준 색인에 걸리는 최대 시간은 7일 미만입니다. 실제 시간은 환경에 따라 달라집니다.

시스템에 대한 인덱싱을 활성화하는 단계**:**

시스템에서 인덱싱이 이미 활성화된 경우 다음 섹션으로 이동하여 데이터를 복원하세요.

먼저 카탈로그 파일을 보관할 별도의 볼륨을 마운트해야 합니다. 이렇게 하면 스냅샷을 보관하는 파일의 크기가 너무 커져도 데이터 손실을 방지할 수 있습니다. 이는 모든 클러스터에 필요한 것은 아닙니다. 사용자 환경의 모든 클러스터에서 원하는 볼륨을 마운트할 수 있습니다. 이렇게 하지 않으면 인덱싱이 제대로 작동하지 않을 수 있습니다.

장착된 볼륨의 경우 다음 크기 조정 지침을 사용하세요.

- NetApp NFS 볼륨 사용
- 300MB/s 디스크 처리량의 권장 AFF 스토리지입니다. 처리량이 낮아지면 검색 및 기타 작업에 영향을 미칩니다.
- 카탈로그 백업 zip 파일 외에도 카탈로그 메타데이터를 보호하기 위해 NetApp 스냅샷을 활성화합니다.
- 10억 개의 파일당 50GB
- 카탈로그 데이터를 위한 20GB, zip 파일 생성 및 임시 파일을 위한 추가 공간

카탈로그를 다시 인덱싱하기 위해 볼륨을 마운트하는 단계

1. 볼륨을 마운트합니다 `/opt/application/netapp/cbs` 다음 명령을 입력하여 다음을 수행합니다.
    - `volume name` 카탈로그 파일이 저장될 클러스터의 볼륨입니다.
    - `/opt/application/netapp/cbs` 마운트되는 경로입니다

    ```
    mount <cluster IP address>:/<volume name> /opt/application/netapp/cbs
    ```

    예:

```
mount 10.192.24.17:/CATALOG_SCALE_234 /opt/application/netapp/cbs
```

인덱스를 활성화하는 단계

1. 다음 중 하나를 수행하세요.
    - 시스템이 인덱싱되지 않은 경우, 복원 대시보드의 _검색 및 복원_에서 *시스템 인덱싱 사용*을 선택합니다.
    - 하나 이상의 시스템이 이미 인덱싱된 경우, 복원 대시보드의 _검색 및 복원_에서 *인덱싱 설정*을 선택하세요.
2. 시스템에 대해 *인덱싱 사용*을 선택합니다.

결과

모든 서비스가 제공되고 색인 카탈로그가 활성화되면 시스템이 "활성"으로 표시됩니다.

시스템의 볼륨 크기와 3개 백업 위치의 백업 파일 수에 따라 초기 인덱싱 프로세스는 최대 1시간이 걸릴 수 있습니다. 그 후에는 점진적인 변경 사항을 매시간 투명하게 업데이트하여 최신 상태를 유지합니다.

검색 및 복원을 사용하여 볼륨, 폴더 및 파일 복원

당신이 가지고 후시스템에 인덱싱이 활성화되었습니다. 검색 및 복원을 사용하여 볼륨, 폴더 및 파일을 복원할 수 있습니다. 이를 통해 광범위한 필터를 사용하여 모든 백업 파일에서 복원하려는 정확한 파일이나 볼륨을 찾을 수 있습니다.

단계

1. 콘솔 메뉴에서 *보호 > 백업 및 복구*를 선택합니다.
2. 복원 탭을 선택하면 복원 대시보드가 표시됩니다.
3. 검색 및 복원 섹션에서 *검색 및 복원*을 선택합니다.
4. 검색 및 복원 섹션에서 *검색 및 복원*을 선택합니다.
5. 검색 및 복원 페이지에서:
   a. _검색 창_에 볼륨 이름 전체 또는 일부, 폴더 이름 또는 파일 이름을 입력합니다.
   b. 리소스 유형을 선택하세요: 볼륨, 파일, 폴더, 모두.
   c. 필터 기준 영역에서 필터 기준을 선택합니다. 예를 들어, 데이터가 있는 시스템과 파일 형식(예: .JPEG 파일)을 선택할 수 있습니다. 또는 개체 스토리지에서 사용 가능한 스냅샷이나 백업 파일 내에서만 결과를 검색하려는 경우 백업 위치 유형을 선택할 수 있습니다.
6. *검색*을 선택하면 검색 결과 영역에 검색 조건과 일치하는 파일, 폴더 또는 볼륨이 있는 모든 리소스가 표시됩니다.
7. 복원하려는 데이터가 있는 리소스를 찾은 다음 *모든 백업 보기*를 선택하면 일치하는 볼륨, 폴더 또는 파일이 포함된 모든 백업 파일이 표시됩니다.
8. 데이터를 복원하는 데 사용할 백업 파일을 찾아 *복원*을 선택합니다.

   검색 결과에는 검색 대상 파일이 포함된 로컬 볼륨 스냅샷과 원격 복제 볼륨이 식별됩니다. 클라우드 백업 파일, 스냅샷 또는 복제된 볼륨에서 복원하도록 선택할 수 있습니다.

9. 볼륨, 폴더 또는 파일을 복원할 대상 위치를 선택하고 *복원*을 선택합니다.
   - 볼륨의 경우 원래 대상 시스템을 선택하거나 대체 시스템을 선택할 수 있습니다. FlexGroup 볼륨을 복원할 때는 여러 개의 집계를 선택해야 합니다.
   - 폴더의 경우 원래 위치로 복원할 수도 있고 시스템, 볼륨, 폴더 등의 대체 위치를 선택할 수도 있습니다.
   - 파일의 경우 원래 위치로 복원할 수도 있고 시스템, 볼륨, 폴더 등의 대체 위치를 선택할 수도 있습니다. 원래 위치를 선택할 때, 소스 파일을 덮어쓸지 아니면 새 파일을 만들지 선택할 수 있습니다.

     온프레미스 ONTAP 시스템을 선택하고 개체 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 입력하라는 메시지가 표시됩니다.

     - Amazon S3에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택하고, ONTAP 클러스터에 S3 버킷에 대한 액세스 권한을 부여하기 위해 생성한 사용자의 액세스 키와 비밀 키를 입력하고, 선택적으로 안전한 데이터 전송을 위해 개인 VPC 엔드포인트를 선택합니다. "이러한 요구 사항에 대한 세부 정보를 확인하세요".
     - Azure Blob에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택하고, 필요에 따라 VNet 및 서브넷을 선택하여 안전한 데이터 전송을 위한 개인 엔드포인트를 선택합니다. "이러한 요구 사항에 대한 세부 정보를 확인하세요".

- Google Cloud Storage에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택하고, 개체 스토리지에 액세스하기 위한 액세스 키와 비밀 키를 선택합니다. "이러한 요구 사항에 대한 세부 정보를 확인하세요".
- StorageGRID 에서 복원할 때 StorageGRID 서버의 FQDN과 ONTAP StorageGRID 와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 입력하고, 대상 볼륨이 있는 ONTAP 클러스터의 IP 공간을 입력합니다. "이러한 요구 사항에 대한 세부 정보를 확인하세요".
- ONTAP S3에서 복원할 때 ONTAP S3 서버의 FQDN과 ONTAP ONTAP S3와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 선택하고, 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택합니다. "이러한 요구 사항에 대한 세부 정보를 확인하세요".

결과

볼륨, 폴더 또는 파일이 복원되고 복원 대시보드로 돌아와서 복원 작업의 진행 상황을 검토할 수 있습니다. 작업 모니터링 탭을 선택하여 복원 진행 상황을 확인할 수도 있습니다. 보다"작업 모니터 페이지" .

Browse & Restore를 사용하여 ONTAP 데이터 복원

NetApp Backup and Recovery 사용하여 찾아보기 및 복원 기능을 사용하여 ONTAP 데이터를 복원하세요. 복원하기 전에 소스 볼륨 이름, 소스 시스템 및 SVM, 백업 파일 날짜를 기록해 두세요. 스냅샷, 복제된 볼륨 또는 개체 스토리지에 저장된 백업에서 ONTAP 데이터를 복원할 수 있습니다.

복원 기능은 ONTAP 버전에 따라 다릅니다.

- 폴더: ONTAP 9.13.0 이상을 사용하면 모든 파일과 하위 폴더가 포함된 폴더를 복원할 수 있습니다. 이전 버전에서는 폴더 내의 파일만 복원할 수 있습니다.
- 보관 저장소: 보관 저장소(ONTAP 9.10.1 이상에서 사용 가능)에서 복원하는 경우 속도가 느리고 추가 비용이 발생할 수 있습니다.
- 목적지 클러스터 요구 사항:
  - 볼륨 복원: ONTAP 9.10.1 이상
  - 파일 복원: ONTAP 9.11.1 이상
  - Google Archive 및 StorageGRID: ONTAP 9.12.1 이상
  - 폴더 복원: ONTAP 9.13.1 이상

"AWS 보관 스토리지에서 복원하는 방법에 대해 자세히 알아보세요.". "Azure 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". "Google 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.".

Azure 보관 저장소에서 StorageGRID 시스템으로 데이터를 복원하는 경우 높은 우선순위는 지원되지 않습니다.

지원되는 시스템 및 개체 스토리지 공급자를 찾아보고 복원합니다.

보조 시스템(복제된 볼륨) 또는 개체 스토리지(백업 파일)에 있는 백업 파일에서 ONTAP 데이터를 다음 시스템으로 복원할 수 있습니다. 스냅샷은 소스 시스템에 저장되며 동일한 시스템으로만 복원할 수 있습니다.

참고: 모든 유형의 백업 파일에서 볼륨을 복원할 수 있지만, 현재 개체 스토리지의 백업 파일에서만 폴더나 개별 파일을 복원할 수 있습니다.

객체 저장소에서(백업)	기본(스냅샷)에서	2차 시스템(복제)에서	목적지 시스템
아마존 S3	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	AWS 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Azure Blob
Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	Azure 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	구글 클라우드 스토리지	Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP
Google 온프레미스 ONTAP 시스템의 Cloud Volumes ONTAP	NetApp StorageGRID	온프레미스 ONTAP 시스템	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP
온프레미스 ONTAP 시스템으로	ONTAP S3	온프레미스 ONTAP 시스템	온프레미스 ONTAP 시스템 Cloud Volumes ONTAP

찾아보기 및 복원의 경우 콘솔 에이전트를 다음 위치에 설치할 수 있습니다.

- Amazon S3의 경우 콘솔 에이전트는 AWS 또는 사내에 배포될 수 있습니다.
- Azure Blob의 경우 콘솔 에이전트는 Azure 또는 사내에 배포될 수 있습니다.
- Google Cloud Storage의 경우 콘솔 에이전트는 Google Cloud Platform VPC에 배포되어야 합니다.
- StorageGRID 의 경우 콘솔 에이전트는 인터넷 접속 여부와 관계없이 사내에 배포되어야 합니다.
- ONTAP S3의 경우 콘솔 에이전트는 인터넷 접속 여부와 관계없이 사내 또는 클라우드 공급자 환경에 배포될 수 있습니다.

"온프레미스 ONTAP 시스템"에 대한 참조에는 FAS, AFF 및 ONTAP Select 시스템이 포함됩니다.

시스템의 ONTAP 버전이 9.13.1 미만이면 백업 파일이 DataLock & Ransomware로 구성된 경우 폴더나 파일을 복원할 수 없습니다. 이 경우 백업 파일에서 전체 볼륨을 복원한 다음 필요한 파일에 액세스할 수 있습니다.

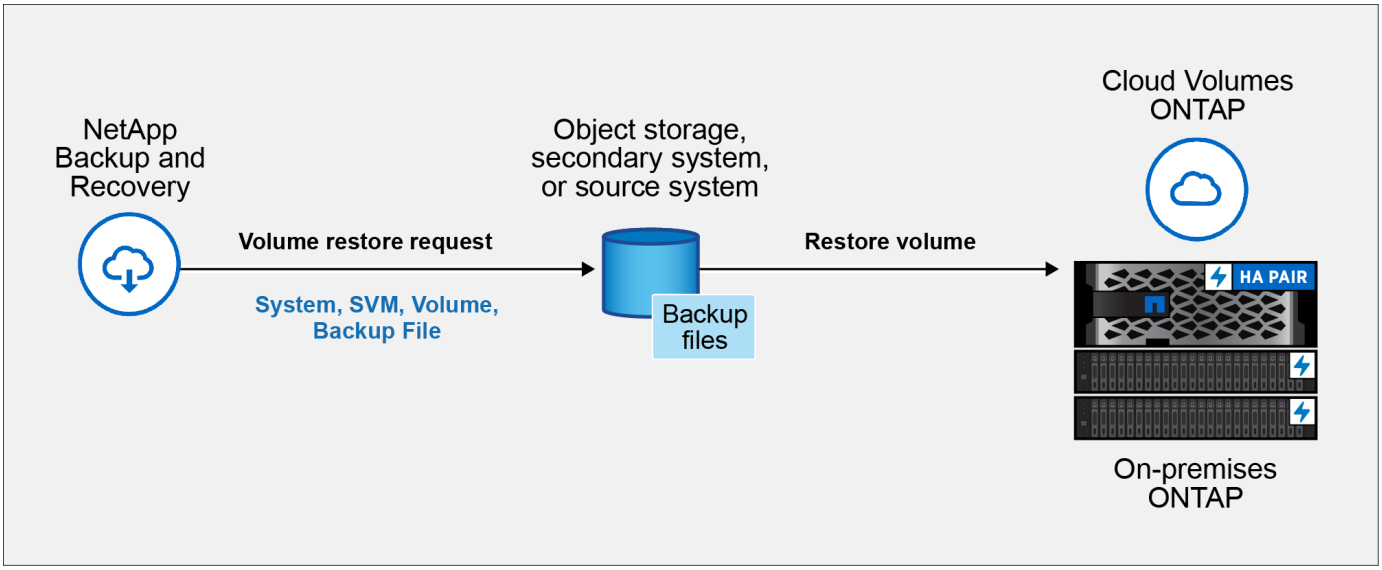
찾아보기 및 복원을 사용하여 볼륨 복원

백업 파일에서 볼륨을 복원하면 NetApp Backup and Recovery 백업의 데이터를 사용하여 새로운 볼륨을 만듭니다. 개체 스토리지에서 백업을 사용하면 원본 시스템의 볼륨, 소스 시스템과 동일한 클라우드 계정에 있는 다른 시스템 또는 온프레미스 ONTAP 시스템에 데이터를 복원할 수 있습니다.

ONTAP 9.13.0 이상을 사용하여 Cloud Volumes ONTAP 시스템에 클라우드 백업을 복원하거나 ONTAP 9.14.1을 실행하는 온프레미스 ONTAP 시스템에 클라우드 백업을 복원하는 경우 빠른 복원 작업을 수행할 수 있는 옵션이 제공됩니다. 빠른 복원은 가능한 한 빨리 볼륨에 대한 액세스를 제공해야 하는 재해 복구 상황에 이상적입니다. 빠른 복원은 전체 백업 파일을 복원하는 대신 백업 파일의 메타데이터를 볼륨으로 복원합니다. 빠른 복원은 성능이나 지연 시간에 민감한 애플리케이션에는 권장되지 않으며, 보관된 저장소의 백업에서는 지원되지 않습니다.

클라우드 백업이 생성된 소스 시스템에서 ONTAP 9.12.1 이상이 실행되고 있는 경우에만 FlexGroup 볼륨에 대한 빠른 복원이 지원됩니다. SnapLock 볼륨은 소스 시스템에서 ONTAP 9.11.0 이상을 실행하는 경우에만 지원됩니다.

복제된 볼륨에서 복원할 경우 볼륨을 원래 시스템이나 Cloud Volumes ONTAP 또는 온프레미스 ONTAP 시스템으로 복원할 수 있습니다.



볼륨을 복원하려면 소스 시스템 이름, 스토리지 VM, 볼륨 이름 및 백업 파일 날짜가 필요합니다.

단계

1. 콘솔 메뉴에서 *보호 > 백업 및 복구*를 선택합니다.
2. 복원 탭을 선택하면 복원 대시보드가 표시됩니다.
3. 찾아보기 및 복원 섹션에서 *볼륨 복원*을 선택합니다.
4. 소스 선택 페이지에서 복원하려는 볼륨의 백업 파일로 이동합니다. 복원하려는 날짜/시간 스탬프가 있는 시스템, 볼륨, 백업 파일을 선택합니다.

   위치 열은 백업 파일(스냅샷)이 로컬(소스 시스템의 스냅샷), 보조(보조 ONTAP 시스템의 복제된 볼륨), 개체 스토리지(개체 스토리지의 백업 파일)인지 여부를 보여줍니다. 복원할 파일을 선택하세요.

5. *다음*을 선택하세요.

   개체 스토리지에서 백업 파일을 선택하고 해당 백업에 대해 랜섬웨어 복원력이 활성화된 경우(백업 정책에서 DataLock 및 랜섬웨어 복원력을 활성화한 경우), 데이터를 복원하기 전에 백업 파일에 대한 추가 랜섬웨어 검사를 실행하라는 메시지가 표시됩니다. 랜섬웨어가 있는지 백업 파일을 검사하는 것이 좋습니다. (백업 파일의 내용에 접근하려면 클라우드 제공업체로부터 추가 퇴장 비용이 발생합니다.)

6. 대상 선택 페이지에서 볼륨을 복원할 *시스템*을 선택합니다.
7. 개체 스토리지에서 백업 파일을 복원할 때 온프레미스 ONTAP 시스템을 선택하고 개체 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 입력하라는 메시지가 표시됩니다.
   - Amazon S3에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택하고, ONTAP 클러스터에 S3 버킷에 대한 액세스 권한을 부여하기 위해 생성한 사용자의 액세스 키와 비밀 키를 입력하고, 선택적으로 안전한 데이터 전송을 위해 개인 VPC 엔드포인트를 선택합니다.
   - Azure Blob에서 복원할 때 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택하고, 개체 스토리지에 액세스할 Azure 구독을 선택하고, 선택적으로 VNet 및 서브넷을 선택하여 안전한 데이터 전송을 위한 개인 엔드포인트를 선택합니다.
   - Google Cloud Storage에서 복원할 때 Google Cloud Project와 개체 스토리지에 액세스할 액세스 키 및 비밀

키, 백업이 저장된 지역, 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택합니다.

- StorageGRID 에서 복원할 때 StorageGRID 서버의 FQDN과 ONTAP StorageGRID 와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 선택하고, 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택합니다.
- ONTAP S3에서 복원할 때 ONTAP S3 서버의 FQDN과 ONTAP ONTAP S3와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 선택하고, 대상 볼륨이 상주할 ONTAP 클러스터의 IP 공간을 선택합니다.

8. 복원된 볼륨에 사용할 이름을 입력하고 볼륨이 상주할 저장소 VM과 집계를 선택합니다. FlexGroup 볼륨을 복원할 때는 여러 개의 집계를 선택해야 합니다. 기본적으로 *<source_volume_name>_restore*가 볼륨 이름으로 사용됩니다.

   ONTAP 9.13.0 이상을 사용하여 Cloud Volumes ONTAP 시스템이나 ONTAP 9.14.1을 실행하는 온프레미스 ONTAP 시스템으로 개체 스토리지에서 백업을 복원하는 경우 빠른 복원 작업을 수행할 수 있는 옵션이 제공됩니다.

   그리고 보관 스토리지 계층(ONTAP 9.10.1부터 사용 가능)에 있는 백업 파일에서 볼륨을 복원하는 경우 복원 우선순위를 선택할 수 있습니다.

   "AWS 보관 스토리지에서 복원하는 방법에 대해 자세히 알아보세요.". "Azure 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". "Google 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". Google 보관함 저장 계층의 백업 파일은 거의 즉시 복원되며 복원 우선 순위가 필요하지 않습니다.

9. *다음*을 선택하여 일반 복원 또는 빠른 복원 프로세스를 수행할지 여부를 선택합니다.
   - 일반 복원: 높은 성능이 필요한 볼륨에 일반 복원을 사용합니다. 복원 프로세스가 완료될 때까지 볼륨을 사용할 수 없습니다.
   - 빠른 복원: 복원된 볼륨과 데이터는 즉시 사용할 수 있습니다. 높은 성능이 필요한 볼륨에서는 이 기능을 사용하지 마세요. 빠른 복원 프로세스 중에는 데이터에 대한 액세스가 평소보다 느릴 수 있습니다.
10. *복원*을 선택하면 복원 대시보드로 돌아가서 복원 작업의 진행 상황을 검토할 수 있습니다.

결과

NetApp Backup and Recovery 선택한 백업을 기반으로 새 볼륨을 생성합니다.

보관 저장소에 있는 백업 파일에서 볼륨을 복원하는 작업은 보관 계층과 복원 우선순위에 따라 몇 분에서 몇 시간이 걸릴 수 있습니다. 작업 모니터링 탭을 선택하면 복원 진행 상황을 볼 수 있습니다.

찾아보기 및 복원을 사용하여 폴더 및 파일 복원

ONTAP 볼륨 백업에서 몇 개의 파일만 복원해야 하는 경우 전체 볼륨을 복원하는 대신 폴더나 개별 파일만 복원하도록 선택할 수 있습니다. 원래 시스템의 기존 볼륨이나 동일한 클라우드 계정을 사용하는 다른 시스템으로 폴더와 파일을 복원할 수 있습니다. 온프레미스 ONTAP 시스템의 볼륨으로 폴더와 파일을 복원할 수도 있습니다.

지금은 개체 스토리지의 백업 파일에서만 폴더나 개별 파일을 복원할 수 있습니다. 현재 로컬 스냅샷이나 보조 시스템(복제된 볼륨)에 있는 백업 파일에서 파일과 폴더를 복원하는 것은 지원되지 않습니다.

여러 파일을 선택하면 동일한 대상 볼륨에 복원됩니다. 파일을 다른 볼륨으로 복원하려면 프로세스를 여러 번 실행하세요.

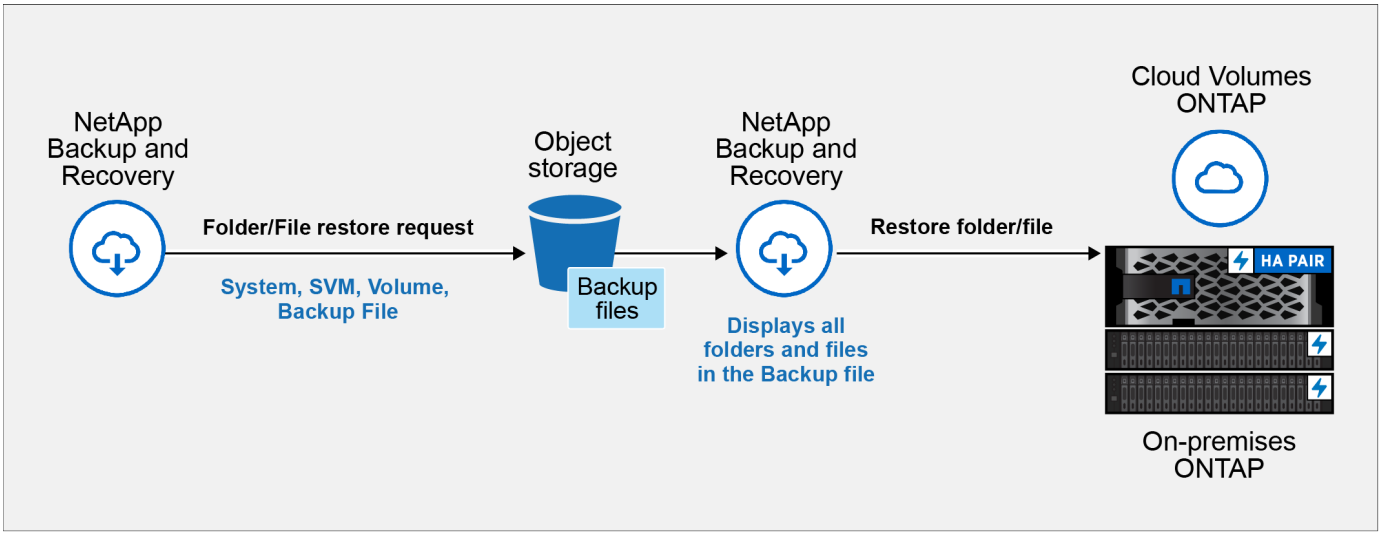
ONTAP 9.13.0 이상을 사용하면 폴더와 그 안의 모든 파일 및 하위 폴더를 복원할 수 있습니다. 9.13.0 이전 버전의 ONTAP 사용하는 경우 해당 폴더의 파일만 복원되고 하위 폴더나 하위 폴더의 파일은 복원되지 않습니다.

- 백업 파일이 DataLock 및 랜섬웨어 보호 기능으로 구성된 경우, ONTAP 버전이 9.13.1 이상인 경우에만 폴더 수준 복원이 지원됩니다. 이전 버전의 ONTAP 사용하는 경우 백업 파일에서 전체 볼륨을 복원한 다음 필요한 폴더와 파일에 액세스할 수 있습니다.
- 백업 파일이 보관 저장소에 있는 경우 ONTAP 버전이 9.13.1 이상인 경우에만 폴더 수준 복원이 지원됩니다. 이전 버전의 ONTAP 사용하는 경우 보관되지 않은 최신 백업 파일에서 폴더를 복원하거나 보관된 백업에서 전체 볼륨을 복원한 다음 필요한 폴더와 파일에 액세스할 수 있습니다.
- ONTAP 9.15.1에서는 "찾아보기 및 복원" 옵션을 사용하여 FlexGroup 폴더를 복원할 수 있습니다.

  다음에서 설명하는 특수 플래그를 사용하여 테스트할 수 있습니다. "NetApp Backup and Recovery 2024년 7월 릴리스 블로그" .

폴더 및 파일 복원

ONTAP 볼륨 백업에서 볼륨으로 폴더나 파일을 복원하려면 다음 단계를 따르세요. 폴더나 파일을 복원하는 데 사용할 볼륨의 이름과 백업 파일의 날짜를 알아야 합니다. 이 기능은 라이브 브라우징을 사용하여 각 백업 파일 내의 디렉토리와 파일 목록을 볼 수 있습니다.



시작하기 전에

- 파일 복원 작업을 수행하려면 ONTAP 버전이 9.6 이상이어야 합니다.
- 폴더 복원 작업을 수행하려면 ONTAP 버전이 9.11.1 이상이어야 합니다. 데이터가 보관 저장소에 있거나 백업 파일에 DataLock 및 랜섬웨어 보호 기능이 있는 경우 ONTAP 버전 9.13.1이 필요합니다.
- 찾아보기 및 복원 옵션을 사용하여 FlexGroup 디렉토리를 복원하려면 ONTAP 버전이 9.15.1 p2 이상이어야 합니다.

단계

1. 콘솔 메뉴에서 *보호 > 백업 및 복구*를 선택합니다.
2. 복원 탭을 선택하면 복원 대시보드가 표시됩니다.
3. 찾아보기 및 복원 섹션에서 *파일 또는 폴더 복원*을 선택합니다.
4. 소스 선택 페이지에서 복원하려는 폴더나 파일이 포함된 볼륨의 백업 파일로 이동합니다. 파일을 복원할 날짜/시간 스탬프가 있는 시스템, 볼륨, *백업*을 선택합니다.
5. *다음*을 선택하면 볼륨 백업의 폴더와 파일 목록이 표시됩니다.

보관 저장소 계층에 있는 백업 파일에서 폴더나 파일을 복원하는 경우 복원 우선순위를 선택할 수 있습니다.

"AWS 보관 스토리지에서 복원하는 방법에 대해 자세히 알아보세요.". "Azure 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". "Google 보관 저장소에서 복원하는 방법에 대해 자세히 알아보세요.". Google 보관함 저장 계층의 백업 파일은 거의 즉시 복원되며 복원 우선 순위가 필요하지 않습니다.

백업 파일에 대해 랜섬웨어 복원력이 활성화된 경우(백업 정책에서 DataLock 및 랜섬웨어 복원력을 활성화한 경우) 데이터를 복원하기 전에 백업 파일에 대한 추가 랜섬웨어 검사를 실행하라는 메시지가 표시됩니다. 랜섬웨어가 있는지 백업 파일을 검사하는 것이 좋습니다. (백업 파일의 내용에 접근하려면 클라우드 제공업체로부터 추가 퇴장 비용이 발생합니다.)

6. 항목 선택 페이지에서 복원하려는 폴더나 파일을 선택하고 *계속*을 선택합니다. 해당 항목을 찾는 데 도움이 되는 내용:
   - 폴더나 파일 이름이 보이면 선택할 수 있습니다.
   - 검색 아이콘을 선택하고 폴더나 파일 이름을 입력하면 해당 항목으로 바로 이동할 수 있습니다.
   - 행 끝에 있는 아래쪽 화살표를 사용하여 폴더의 하위 수준으로 이동하여 특정 파일을 찾을 수 있습니다.

     파일을 선택하면 해당 파일이 페이지 왼쪽에 추가되어 이미 선택한 파일을 볼 수 있습니다. 필요한 경우 파일 이름 옆에 있는 *x*를 선택하여 이 목록에서 파일을 제거할 수 있습니다.

7. 대상 선택 페이지에서 항목을 복원할 *시스템*을 선택합니다.

   온프레미스 클러스터를 선택하고 개체 스토리지에 대한 클러스터 연결을 아직 구성하지 않은 경우 추가 정보를 입력하라는 메시지가 표시됩니다.

   - Amazon S3에서 복원할 때 대상 볼륨이 있는 ONTAP 클러스터의 IP 공간과 개체 스토리지에 액세스하는 데 필요한 AWS 액세스 키와 비밀 키를 입력합니다. 클러스터에 연결하기 위해 개인 링크 구성을 선택할 수도 있습니다.
   - Azure Blob에서 복원하는 경우 대상 볼륨이 있는 ONTAP 클러스터의 IP 공간을 입력합니다. 클러스터에 연결하기 위해 개인 엔드포인트 구성을 선택할 수도 있습니다.
   - Google Cloud Storage에서 복원하는 경우 대상 볼륨이 있는 ONTAP 클러스터의 IP 공간과 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 입력합니다.
   - StorageGRID 에서 복원할 때 StorageGRID 서버의 FQDN과 ONTAP StorageGRID 와 HTTPS 통신에 사용해야 하는 포트를 입력하고, 개체 스토리지에 액세스하는 데 필요한 액세스 키와 비밀 키를 입력하고, 대상 볼륨이 있는 ONTAP 클러스터의 IP 공간을 입력합니다.

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

   폴더와 파일을 복원할 때 위치에 대한 몇 가지 옵션이 있습니다.

   - 위에 표시된 대로 *대상 폴더 선택*을 선택한 경우:
     - 원하는 폴더를 선택할 수 있습니다.
     - 폴더 위에 마우스를 올려놓고 행의 끝을 클릭하면 하위 폴더로 드릴다운한 다음 폴더를 선택할 수 있습니다.
   - 소스 폴더/파일이 있던 위치와 동일한 대상 시스템 및 볼륨을 선택한 경우, *소스 폴더 경로 유지 관리*를 선택하면 해당 폴더 또는 파일을 소스 구조에 있던 폴더로 복원할 수 있습니다. 모든 동일한 폴더와 하위 폴더가 이미 존재해야 하며, 폴더는 생성되지 않습니다. 파일을 원래 위치로 복원할 때 원본 파일을 덮어쓸지 아니면 새 파일을 만들지 선택할 수 있습니다.

9. 복원 대시보드로 돌아가서 복원 작업의 진행 상황을 검토하려면 *복원*을 선택하세요.