



# **NetApp ONTAP용 Amazon FSx를 사용합니다**

## Amazon FSx for NetApp ONTAP

NetApp  
February 17, 2026

# 목차

NetApp ONTAP용 Amazon FSx를 사용합니다.	1
NetApp Workload Factory에서 FSx for ONTAP 으로 비용 절감을 살펴보세요	1
계산기 옵션	1
맞춤화를 통한 절감 효과를 살펴보십시오.	1
감지된 스토리지 환경의 비용 절감에 대해 알아보십시오.	3
FSx for ONTAP 파일 시스템 배포	6
NetApp Workload Factory 에서 리소스 비용을 추적하세요.	6
링크를 사용하십시오	7
NetApp Workload Factory 링크에 대해 알아보세요	7
Lambda 링크를 사용하여 FSx for ONTAP 파일 시스템에 연결합니다	9
워크로드 팩토리 링크 관리	15
Workload Factory에서 캐시 볼륨을 검색합니다.	18
볼륨 관리	19
Workload Factory에서 ONTAP 볼륨에 대한 FSx 생성	19
FSx for ONTAP 파일 시스템 데이터에 액세스합니다.	24
블록 스토리지 리소스 생성	25
NetApp Workload Factory에서 파일 시스템용 이니시에이터 그룹을 생성합니다	25
NetApp Workload Factory 에서 파일 시스템용 블록 장치를 생성합니다.	26
FSx for ONTAP 파일 시스템용 스토리지 VM을 생성합니다.	28
스토리지 VM을 생성합니다.	28
데이터 보호	29
NetApp Workload Factory의 데이터 보호 유형	29
스냅샷을 사용하세요	31
백업을 개체 스토리지에 사용	34
복제를 사용하세요	36
AI를 활용한 NetApp 자율형 랜섬웨어 보호로 데이터를 보호하세요	41
NetApp Workload Factory에서 볼륨 복제	45
NetApp Workload Factory에서 온프레미스 ONTAP 클러스터 데이터 사용	45
사이버 볼트로 데이터를 보호하세요	49

# NetApp ONTAP용 Amazon FSx를 사용합니다

## NetApp Workload Factory에서 FSx for ONTAP 으로 비용 절감을 살펴보세요

Amazon EBS(Elastic Block Store), EFS(Elastic File System) 및 FSx for Windows 파일 서버를 FSx for NetApp ONTAP과 비교하여 사용하는 스토리지 워크로드의 절감 효과에 대해 알아보십시오.

NetApp Workload Factory에는 Amazon 스토리지 환경과 FSx for ONTAP 비교하는 스토리지 절감 계산기가 포함되어 있습니다. AWS 자격 증명을 제공하거나 제공하지 않고도 절감 효과를 알아볼 수 있으며, 스토리지 환경에 맞게 구성 설정을 사용자 지정할 수 있습니다. AWS 자격 증명을 제공하면 예를 들어 Amazon Elastic Block Store의 인스턴스를 하나 이상 선택하고 Workload Factory에서 자동으로 비교를 수행할 수 있습니다. 계산기는 수동이든 자동이든 귀하의 보관 요구 사항에 가장 낮은 비용을 제공하는 보관 서비스를 찾아줍니다.

스토리지 계산기에서 가장 비용 효율적인 스토리지가 FSx for ONTAP 이라고 판단하는 경우 FSx for ONTAP 구성을 만들거나 저장하고 Codebox를 사용하여 Workload Factory에 부여한 권한에 관계없이 Infrastructure-as-Code 템플릿을 생성할 수 있습니다.

### 계산기 옵션

시스템과 FSx for ONTAP 간의 비용 비교를 위해 Amazon 스토리지 환경을 위한 커스터마이징 및 자동 감지 기능을 제공하는 두 가지 계산기 옵션을 사용할 수 있습니다.

사용자 정의를 통한 절감 탐색: 활용 사례, 지역, 볼륨 또는 파일 시스템 수, 스토리지 양, 스냅샷 빈도, 스냅샷당 변경된 양, 프로비저닝된 IOPS, 처리량 등을 포함한 스토리지 환경에 대한 구성 설정을 제공합니다.

감지된 스토리지 환경에 대한 절감 효과를 살펴보세요. Workload Factory는 기존 AWS 스토리지 환경에 연결하여 세부 정보를 계산기에 입력하여 자동으로 비교합니다. 자동 모드를 사용하려면 자동화 권한을 부여해야 합니다. 사용 사례는 변경할 수 있지만, 다른 모든 세부 사항은 계산에서 자동으로 결정됩니다.


또한 계산기 분석의 정확도를 개선할 수 ["AWS 자격 증명을 추가합니다"](#) 있습니다. 기존 리소스를 기준으로 절감 비율 계산 \* 을 선택합니다. 자격 증명 추가 페이지로 리디렉션됩니다. 자격 증명을 추가한 후 FSx for ONTAP와 비교할 기존 리소스를 선택하고 \* 절감 효과 탐색 \* 을 선택합니다.

### 맞춤화를 통한 절감 효과를 살펴보세요

저장소 선택에 해당하는 탭 아래의 단계를 따릅니다.

## Amazon EBS(Elastic Block Store)

### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 절약 내용 살펴보기\*를 선택한 다음 \*Amazon Elastic Block Store(EBS) 탭을 선택합니다.
4. Storage Savings Calculator에서 다음 세부 정보를 제공합니다.
  - a. \* 사용 사례 \*: 필수. 드롭다운 메뉴에서 사용 사례를 선택합니다. 선택한 사용 사례에 따라 비교할 FSx for ONTAP 파일 시스템의 특성이 결정됩니다.
  - b. \* 지역 \*: 선택 요소입니다. 드롭다운 메뉴에서 EBS 구성 지역을 선택합니다.
  - c. \*EBS 볼륨 유형 선택 \*: 선택 사항. 구성에 사용되는 EBS 볼륨 유형을 선택합니다.
  - d. \* 볼륨 수 \*: 선택 사항. EBS 구성에 볼륨 수를 입력합니다.
  - e. \* 볼륨당 스토리지 용량(TiB) \*: 선택 사항. 볼륨당 스토리지 용량을 TiB 단위로 입력합니다.
  - f. \* 스냅샷 주파수 \*: 선택 사항. EBS 구성에 대한 스냅샷 빈도를 선택합니다.
  - g. \* 스냅샷당 변경된 양(GiB) \*: 선택 사항. 스냅샷 스토리지 전용입니다. 스냅샷당 변경된 용량을 GiB 단위로 입력합니다.
  - h. \* 볼륨당 프로비저닝된 IOPS \*: 선택 사항. GP3, io1 및 io2 볼륨의 경우 볼륨당 프로비저닝된 IOPS를 입력합니다.
  - i. \* 처리량(MiB/s) \*: 선택 요소입니다. GP3 볼륨에만 해당됩니다. 볼륨당 MiB/s 단위로 처리량을 입력합니다.

## Amazon FSx for Windows 파일 서버


### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 절약 내용 살펴보기\*를 선택한 다음 \*Amazon Elastic Block Store(EBS) 탭을 선택합니다.
4. Storage Savings Calculator에서 다음 세부 정보를 제공합니다.
  - a. \* 사용 사례 \*: 필수. 드롭다운 메뉴에서 사용 사례를 선택합니다. 선택한 사용 사례에 따라 비교할 FSx for ONTAP 파일 시스템의 특성이 결정됩니다.
  - b. \* 지역 \*: 선택 요소입니다. 드롭다운 메뉴에서 Windows용 FSx 파일 서버 구성 지역을 선택합니다.
  - c. \* 배포 유형 \*: 선택 요소입니다. Single Availability Zone \* 또는 \* Multiple Availability Zone \* 을 선택합니다.
  - d. \* 스토리지 유형 \*: SSD 스토리지 유형이 기본적으로 선택됩니다.
  - e. \* 스토리지 용량(TiB) \*: 선택 사항. 구성에 대한 스토리지 용량을 입력합니다.
  - f. \* 중복 제거 절약(%) \*: 선택 사항. 중복제거를 통해 예상되는 용량 절감 비율을 입력합니다.
  - g. \* 스냅샷 주파수 \*: 선택 사항. 구성에 대한 스냅샷 빈도를 선택합니다.

- h. \* 스냅샷당 변경된 양(GiB) \*: 선택 사항. 스냅샷 스토리지 전용입니다. 스냅샷당 변경된 용량을 GiB 단위로 입력합니다.
- i. \* 프로비저닝된 SSD IOPS \*: 선택 사항. 프로비저닝된 SSD IOPS를 입력합니다.
- j. \* 처리량(MiB/s) \*: 선택 요소입니다. MiB/s 단위로 처리량을 입력합니다

### Amazon Elastic File System(EFS)

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 절약 내용 살펴보기\*를 선택한 다음 \*Amazon Elastic Block Store(EBS) 탭을 선택합니다.
4. Storage Savings Calculator에서 다음 세부 정보를 제공합니다.
  - a. \* 사용 사례 \*: 필수. 드롭다운 메뉴에서 사용 사례를 선택합니다. 선택한 사용 사례에 따라 비교할 FSx for ONTAP 파일 시스템의 특성이 결정됩니다.
  - b. \* 지역 \*: 선택 요소입니다. 드롭다운 메뉴에서 Windows용 FSx 파일 서버 구성 지역을 선택합니다.
  - c. \* 파일 시스템 유형 \*: 선택 사항. Regional \* 또는 \* one zone \* 을 선택합니다.
  - d. \* 스토리지 용량(TiB) \*: 선택 사항. EFS 구성의 저장 용량을 입력합니다.
  - e. \* 자주 액세스하는 데이터(%) \*: 선택 요소입니다. 자주 액세스하는 데이터의 비율을 입력합니다.
  - f. \* 처리량 모드 \*: 선택 사항. provisioned throughput \* 또는 \* Elastic throughput \* 을 선택합니다.
  - g. \* 처리량(MiB/s) \*: 선택 요소입니다. MiB/s 단위로 처리량을 입력합니다

스토리지 시스템 구성에 대한 세부 정보를 제공한 후 페이지에 제공된 계산 및 권장 사항을 검토합니다.

또한 페이지 하단으로 스크롤하여 다음 중 하나를 선택하여 보고서를 봅니다.

- \* PDF 내보내기 \*
- \* 이메일로 보내기 \*
- \* 계산 보기 \*

FSx for ONTAP으로 전환하려면 의 지침을 [FSx for ONTAP 파일 시스템 배포](#)따릅니다.

## 감지된 스토리지 환경의 비용 절감에 대해 알아보십시오

시작하기 전에

Workload Factory가 AWS 계정에서 Amazon Elastic Block Store(EBS), Elastic File System(EFS) 및 FSx for Windows File Server 스토리지 환경을 감지하려면 다음을 확인하세요."[view, planning 및 analysis 권한 부여](#)" 귀하의 AWS 계정에서.




이 계산기 옵션은 EBS 스냅샷 및 FSx for Windows File Server 새도 복사본에 대한 계산을 지원하지 않습니다. 사용자 지정을 통해 비용 절감을 도모할 때 EBS 및 FSx for Windows File Server 스냅샷 세부 정보를 제공할 수 있습니다.

저장소 선택에 해당하는 탭 아래의 단계를 따릅니다.


## Amazon EBS(Elastic Block Store)

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 절약 내용 살펴보기\*를 선택한 다음 \*Amazon Elastic Block Store(EBS) 탭을 선택합니다.
4. EBS(Elastic Block Store) \* 탭에서 FSx for ONTAP와 비교할 인스턴스를 선택하고 \* Explore Savings \* 를 선택합니다.
5. Storage Savings Calculator가 나타납니다. 다음 스토리지 시스템 특성은 선택한 인스턴스를 기반으로 미리 채워집니다.
  - a. \* 사용 사례 \*: 구성에 대한 사용 사례. 필요한 경우 사용 사례를 변경할 수 있습니다.
  - b. \* Selected volumes \*: EBS 구성의 볼륨 수입니다
  - c. \* 총 스토리지 용량(TiB) \*: 볼륨당 스토리지 용량(TiB)입니다
  - d. \* 총 프로비저닝 IOPS \*: GP3, io1 및 io2 볼륨의 경우
  - e. \* 총 처리량(MiB/s) \*: GP3 볼륨에만 해당


## Amazon FSx for Windows 파일 서버

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 절약 사항 살펴보기\*를 선택한 다음 \* Amazon FSx for Windows File Server 탭을 선택합니다.
4. Amazon FSx for Windows 파일 서버 \* 탭에서 FSx for ONTAP와 비교할 인스턴스를 선택하고 \* 절감 효과 탐색 \* 을 선택합니다.
5. Storage Savings Calculator가 나타납니다. 다음 스토리지 시스템 특성은 선택한 인스턴스의 배포 유형에 따라 미리 채워집니다.
  - a. \* 사용 사례 \*: 구성에 대한 사용 사례. 필요한 경우 사용 사례를 변경할 수 있습니다.
  - b. 선택된 파일 시스템
  - c. \* 총 저장 용량(TiB) \*
  - d. \* 프로비저닝된 SSD IOPS \*
  - e. \* 처리량(MiB/s) \*

## Amazon Elastic File System(EFS)

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 스토리지 메뉴에서 절약 효과 살펴보기\*를 선택한 다음 \*Amazon Elastic File System(EFS) 탭을

선택합니다.

4. Elastic File System(EFS) \* 탭에서 FSx for ONTAP와 비교할 인스턴스를 선택하고 \* Explore Savings \* 를 선택합니다.
5. Storage Savings Calculator가 나타납니다. 다음 스토리지 시스템 특성은 선택한 인스턴스를 기반으로 미리 채워집니다.
  - a. \* 사용 사례 \*: 구성에 대한 사용 사례. 필요한 경우 사용 사례를 변경할 수 있습니다.
  - b. \* 전체 파일 시스템 \*
  - c. \* 총 저장 용량(TiB) \*
  - d. \* 총 프로비저닝 처리량(MiB/s) \*
  - e. \* 총 탄성 처리량 - 읽기(GiB) \*
  - f. \* 총 탄력적 처리량 - 쓰기(GiB) \*

스토리지 시스템 구성에 대한 세부 정보를 제공한 후 페이지에 제공된 계산 및 권장 사항을 검토합니다.

또한 페이지 하단으로 스크롤하여 다음 중 하나를 선택하여 보고서를 봅니다.

- \* PDF 내보내기 \*
- \* 이메일로 보내기 \*
- \* 계산 보기 \*

## FSx for ONTAP 파일 시스템 배포

ONTAP용 FSx로 전환하여 비용을 절감하려면 \* 생성 \* 을 선택하여 ONTAP용 FSx 파일 시스템 생성 마법사에서 직접 파일 시스템을 생성하거나 \* 저장 \* 을 선택하여 나중에 권장되는 구성을 저장하십시오.

### 배포 방법

자동화 모드에서는 Workload Factory에서 직접 FSx for ONTAP 파일 시스템을 배포할 수 있습니다. Codebox 창에서 내용을 복사한 후 Codebox 방법 중 하나를 사용하여 시스템을 배포할 수도 있습니다.

\_basic\_mode에서는 코드박스 창에서 콘텐츠를 복사하고 코드박스 방법 중 하나를 사용하여 FSx for ONTAP 파일 시스템을 배포할 수 있습니다.

## NetApp Workload Factory 에서 리소스 비용을 추적하세요

NetApp Workload Factory 사용하면 FSx for ONTAP 파일 시스템 비용과 사용량을 통합된 보기로 추적할 수 있습니다. 비용 데이터는 예산을 관리하고 리소스를 효과적으로 최적화하는 데 도움이 됩니다. AWS Cost Explorer는 비용 데이터를 제공합니다.

### 이 작업에 대해

FSx for ONTAP 파일 시스템 리소스에 대한 비용 및 사용 데이터는 다음 권한을 사용하여 AWS Cost Explorer에서 추출됩니다.

- `ce:GetCostAndUsage`




- `ce:GetTags`

시작하기 전에

"[view, planning, and analysis](#) 권한 정책으로 자격 증명 부여" Workload Factory에서 ONTAP 비용에 대한 FSx를 추적합니다.

단계

1. 중 하나를 사용하여 "콘솔 환경" 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*비용\*을 선택합니다.
4. 비용 페이지에서 다음을 제공하여 FSx for ONTAP 리소스에 대한 비용 및 용량 데이터를 필터링합니다.
  - a. **AWS** 계정: 비용 데이터를 보려는 계정을 선택하세요.
  - b. 자격 증명: 보기, 계획 및 분석 권한이 있는 자격 증명을 선택합니다.
  - c. 지역: 비용 데이터를 보려는 AWS 지역을 선택하세요.
  - d. 비용 데이터 범위: 비용 데이터를 볼 시간 범위를 선택하세요.
5. FSx for ONTAP 리소스에 대한 \*비용 세부정보\*를 확인하세요.

## 링크를 사용하십시오

### NetApp Workload Factory 링크에 대해 알아보세요

NetApp Workload Factory 링크는 Workload Factory 계정과 하나 이상의 FSx for ONTAP 파일 시스템 간에 신뢰 관계와 연결을 생성합니다. 이를 통해 Amazon FSx for ONTAP API를 통해서는 사용할 수 없는 특정 파일 시스템 기능을 ONTAP REST API 호출에서 직접 모니터링하고 관리할 수 있습니다.

Workload Factory를 시작하는 데는 링크가 필요하지 않지만, 어떤 경우에는 모든 Workload Factory 기능과 워크로드 기능을 잠금 해제하려면 링크를 만들어야 합니다.

링크가 유익한 이유

링크는 Workload Factory가 Amazon FSx for ONTAP API를 통해 기본적으로 사용할 수 없는 작업을 수행할 수 있게 해주기 때문에 유용합니다. 링크를 통해 고급 ONTAP 기능과 자동화가 가능해져 FSx for ONTAP 파일 시스템 관리가 향상됩니다.

링크를 사용하면 다음과 같은 이점이 있습니다.

- 이 링크를 통해 NetApp 콘솔은 ONTAP 명령을 FSx for ONTAP 파일 시스템으로 직접 전송할 수 있으며, 이를 통해 AWS에서 기본적으로 제공하는 것보다 더 고급 ONTAP 기능을 사용할 수 있습니다.
- 링크는 AWS Lambda를 활용하여 이벤트에 응답하여 코드를 실행합니다. 이러한 서버리스 접근 방식은 VPC에서 실행 중인 인스턴스의 종속성을 제거합니다.

## 링크 작동 방법

링크 활용 AWS Lambda. Lambda는 이벤트에 대한 응답으로 코드를 실행하고 해당 코드에 필요한 컴퓨팅 리소스를 자동으로 관리합니다. 생성하는 링크는 NetApp 계정의 일부이며 AWS 계정과 연결됩니다.

링크를 만든 후에는 하나 이상의 FSx for ONTAP 파일 시스템과 연결할 수 있습니다. 각 파일 시스템은 동일한 NetApp 계정에 있는 하나의 링크에만 연결할 수 있습니다. NetApp 계정이 여러 개인 경우 단일 파일 시스템을 다른 NetApp 계정 아래의 추가 링크에 연결할 수 있습니다.

Workload Factory에서 Storage 워크로드의 링크를 만들고 연결합니다.

Workload Factory 자격 증명 서비스에 저장된 자격 증명이나 AWS Secrets Manager에 저장된 자격 증명을 사용하여 링크를 인증할 수 있습니다. 워크로드 팩토리는 인증 모드 변경을 지원하지 않습니다.

## 비용

Lambda가 수행하는 각 거래에는 요금이 부과됩니다. Lambda는 두 시스템 간의 프록시 역할을 하므로 Lambda가 파일 시스템의 ONTAP REST API에 요청을 보낼 때와 Workload Factory에 응답을 다시 보낼 때 요금이 발생합니다.

["AWS Lambda 사용과 관련된 비용에 대해 자세히 알아보십시오"](#)

## 링크가 필요한 경우

워크로드 팩토리에는 일부 정보를 표시하고 일부 작업을 수행하기 위한 링크가 필요합니다. 링크가 필요한 작업을 수행하려고 하지만 FSx for ONTAP 파일 시스템과 링크를 연결하지 않은 경우 Workload Factory는 해당 작업에 링크가 필요하다는 알림을 보냅니다.

링크가 필요한 기능은 다음과 같습니다.

- 사전 예방적 유지 관리, 안정성 및 비용 성능 최적화를 위한 FSx for ONTAP 파일 시스템 구성의 잘 설계된 상태
- ONTAP EMS 이벤트 모니터링 및 알림
- NetApp 자율형 랜섬웨어 보호(ARP/AI)
- FSx for ONTAP 파일 시스템 전반의 향상된 전체적인 용량 관찰 기능
- 볼륨 및 스토리지 VM 데이터 복제, 관리 및 모니터링
- SMB/CIFS 공유 및 NFS 내보내기 정책 프로비저닝 및 관리
- FSx for ONTAP 파일 시스템에서 iSCSI 볼륨 관리
- 사용자 정의 보호 SLA에 대한 스냅샷 정책 생성 및 관리
- 자동 용량 관리를 위한 Inode 관리 향상
- 탄력적 확장을 위한 볼륨 자동 증가
- 즉각적이고 즉각적인 데이터 복제를 위한 복제본 생성 및 관리
- ONTAP 버전과 같은 ONTAP에서 직접 추가 메트릭 표시

의 방법을 ["FSx for ONTAP 파일 시스템에 링크 연결"](#)알아보십시오.

## Lambda 링크를 사용하여 FSx for ONTAP 파일 시스템에 연결합니다

고급 ONTAP 관리 작업을 수행하려면 Workload Factory 계정과 하나 이상의 FSx for ONTAP 파일 시스템 간의 연결을 설정합니다. 여기에는 새 람다 링크와 기존 람다 링크를 연결하고, 링크를 인증하는 작업이 포함됩니다. 링크 연결을 사용하면 Amazon FSx for ONTAP API를 통해서만 사용할 수 없는 특정 기능을 FSx for ONTAP 파일 시스템에서 직접 모니터링하고 관리할 수 있습니다.

"링크에 대해 자세히 알아보세요"..

이 작업에 대해

Link는 AWS Lambda를 활용하여 이벤트에 대한 응답으로 코드를 실행하고 해당 코드에 필요한 컴퓨팅 리소스를 자동으로 관리합니다. 생성하는 링크는 NetApp 계정의 일부이며 AWS 계정과 연결됩니다.

FSx for ONTAP 파일 시스템을 정의할 때 계정에 링크를 만들 수 있습니다. 해당 링크는 해당 파일 시스템에 사용되며, 다른 FSx for ONTAP 파일 시스템에도 사용될 수 있습니다. 나중에 파일 시스템에 대한 링크를 연결할 수도 있습니다.

링크에는 인증이 필요합니다. Workload Factory 자격 증명 서비스에 저장된 자격 증명이나 AWS Secrets Manager에 저장된 자격 증명을 사용하여 링크를 인증할 수 있습니다. 링크당 하나의 인증 방법만 지원됩니다. 예를 들어 AWS Secrets Manager를 사용하여 링크 인증을 선택한 경우 나중에 인증 방법을 변경할 수 없습니다.



콘솔 에이전트를 사용하는 경우 AWS Secrets Manager는 지원되지 않습니다.

새 링크를 연결합니다

새 링크를 연결하면 링크 생성 및 연결이 포함됩니다.

이 워크플로에서 링크를 만드는 데는 자동 또는 수동의 두 가지 옵션이 있습니다. AWS 계정에서 AWS CloudFormation 스택을 실행하여 링크를 생성해야 합니다.

- 자동: Workload Factory를 통해 자동 등록 링크를 생성합니다. 자동으로 생성된 링크에는 Workload Factory 자동화를 위한 토큰이 필요하며 CloudFormation 코드는 수명이 짧습니다. 최대 6시간 동안만 사용할 수 있습니다.
- 수동: Codebox에서 CloudFormation이나 Terraform을 사용하여 수동 등록 링크를 만듭니다. 코드가 지속되면 작업을 완료할 수 있는 시간이 더 늘어납니다. 이 기능은 보안 및 DevOps와 같이 링크 생성을 완료하는 데 필요한 권한을 먼저 부여해야 하는 여러 팀과 작업할 때 유용합니다.

시작하기 전에

- 사용할 링크 만들기 옵션을 고려해야 합니다.
- Workload Factory에는 최소한 하나의 FSx for ONTAP 파일 시스템이 있어야 합니다. ONTAP 파일 시스템용 FSx를 검색하려면 ONTAP 인스턴스용 FSx에 대한 권한이 있는 AWS 계정이 있어야 합니다. "[Workload Factory에 자격 증명 추가](#)" 저장소 관리에 대한 보기, 계획 및 분석 권한이 있습니다.
- FSx for ONTAP 파일 시스템에 연결된 보안 그룹에서 링크 연결을 위해 다음 포트가 열려 있어야 합니다.
  - Workload Factory 콘솔의 경우: 포트 443(HTTPS)
  - ONTAP 긴급 관리 시스템(EMS) 이벤트 분석을 위한 CloudShell 및 FSx의 경우: 포트 22(SSH)
- 해당 링크는 다음 엔드포인트에 연결할 수 있어야 합니다. <https://api.workloads.netapp.com>. 웹 기반 콘솔은 이 엔드포인트에 연결하여 Workload Factory API와 상호 작용함으로써 FSx for ONTAP 워크로드를 관리하고 운영합니다.


- CloudFormation 스택을 사용하여 링크를 추가할 때 AWS 계정에 다음 권한이 있어야 합니다.

```
"cloudformation:GetTemplateSummary",  
"cloudformation:CreateStack",  
"cloudformation>DeleteStack",  
"cloudformation:DescribeStacks",  
"cloudformation:ListStacks",  
"cloudformation:DescribeStackEvents",  
"cloudformation:ListStackResources",  
"ec2:DescribeSubnets",  
"ec2:DescribeSecurityGroups",  
"ec2:DescribeVpcs",  
"iam:ListRoles",  
"iam:GetRolePolicy",  
"iam:GetRole",  
"iam>DeleteRolePolicy",  
"iam:CreateRole",  
"iam:DetachRolePolicy",  
"iam:PassRole",  
"iam:PutRolePolicy",  
"iam>DeleteRole",  
"iam:AttachRolePolicy",  
"lambda:AddPermission",  
"lambda:RemovePermission",  
"lambda:InvokeFunction",  
"lambda:GetFunction",  
"lambda:CreateFunction",  
"lambda>DeleteFunction",  
"lambda:TagResource",  
"codestar-connections:GetSyncConfiguration",  
"ecr:BatchGetImage",  
"ecr:GetDownloadUrlForLayer"
```

자동으로 만듭니다

CloudFormation을 사용하여 Workload Factory 내에서 링크를 자동으로 생성하고 등록합니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 링크를 연결할 파일 시스템의 작업 메뉴를 선택한 다음 \*링크 연결\*을 선택합니다.
5. 연결 링크 대화 상자에서 \* 새 링크 만들기 \* 를 선택하고 \* 계속 \* 을 선택합니다.
6. 링크 만들기 페이지에서 다음을 제공합니다.

- a. \* 링크 이름 \*: 이 링크에 사용할 이름을 입력하십시오. 이름은 계정 내에서 고유해야 합니다.
- b. **AWS Secrets Manager**: 선택 사항. Workload Factory가 AWS Secrets Manager에서 FSx for ONTAP 액세스 자격 증명을 가져올 수 있도록 허용합니다.

링크 배포 스택은 Lambda 권한 정책에 다음 기본 비밀 관리자 ARN 정규식을 자동으로 추가합니다.

```
arn:aws:secretsmanager:<link_deployment_region>:<link_deployment_account_id>:secret:FSxSecret* .
```

기본 사용 권한에 맞춰 암호를 만들거나 링크 정책에 대한 사용자 지정 사용 권한을 할당할 수 있습니다.

- AWS Secrets Manager로 VPC 전용 엔드포인트 구성 \* 은 기본적으로 비활성화됩니다. 이 옵션을 선택하면 VPC 개인 엔드포인트를 로컬로 저장하는 대신 VPC 전용 엔드포인트를 사용하여 암호를 저장합니다.
- c. 링크 권한: 링크 권한에 대해 다음 옵션 중 하나를 선택하세요.
    - 자동: AWS CloudFormation 코드가 Lambda 권한 정책과 실행 역할을 자동으로 생성하도록 이 옵션을 선택합니다.
    - 사용자 제공: 지정된 Lambda 실행 역할과 연결된 정책을 Lambda 링크에 할당하려면 이 옵션을 선택합니다. 권한 정책에는 다음 권한이 필요합니다. `secretsmanager:GetSecretValue` AWS Secrets Manager를 활성화한 경우에만 권한이 필요합니다.

```
"ec2:CreateNetworkInterface",  
"ec2:DescribeNetworkInterfaces",  
"ec2:DeleteNetworkInterface",  
"ec2:AssignPrivateIpAddresses",  
"ec2:UnassignPrivateIpAddresses",  
"secretsmanager:GetSecretValue"
```

텍스트 상자에 Lambda 실행 역할 ARN을 입력합니다.

- d. \* 태그 \*: 필요에 따라 이 링크에 연결할 태그를 추가하여 리소스를 보다 쉽게 분류할 수 있습니다. 예를 들어, FSx for ONTAP 파일 시스템에서 이 링크를 사용 중인 것으로 식별하는 태그를 추가할 수 있습니다.

Workload Factory는 FSx for ONTAP 파일 시스템을 기반으로 AWS 계정, 위치 및 보안 그룹을 자동으로

검색합니다.

7. Create \* 를 선택합니다.

CloudFormation으로 리디렉션 대화 상자가 나타나고 AWS CloudFormation 서비스에서 링크를 만드는 방법이 설명되어 있습니다.

8. AWS 관리 콘솔을 열고 이 FSx for ONTAP 파일 시스템에 대한 AWS 계정에 로그인하려면 \* 계속 \* 을 선택하십시오.
9. 빠른 스택 만들기 페이지의 기능 에서 \* AWS CloudFormation이 IAM 리소스를 생성할 수 있음을 확인합니다 \* 를 선택합니다.

CloudFormation 템플릿을 시작하면 Lambda에게 세 가지 권한이 부여됩니다. 워크로드 팩토리에서는 링크를 사용할 때 이러한 권한을 사용합니다.

```
"lambda:InvokeFunction",  
"lambda:GetFunction",  
"lambda:UpdateFunctionCode"
```

10. Create stack \* 을 선택한 다음 \* Continue \* 를 선택합니다.

이벤트 페이지에서 링크 생성 상태를 모니터링할 수 있습니다. 이 작업에는 5분 이상 걸리지 않습니다.

11. Workload Factory 인터페이스로 돌아가면 링크가 FSx for ONTAP 파일 시스템과 연결되어 있는 것을 볼 수 있습니다.

수동으로 만듭니다

Codebox의 두 가지 Infrastructure-as-Code(IaC) 도구인 CloudFormation 또는 Terraform을 사용하여 링크를 만들 수 있습니다. 이 옵션을 사용하면 AWS CloudFormation에서 링크의 ARN을 추출하여 여기에 보고할 수 있습니다. Workload Factory가 수동으로 링크를 등록해 줍니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 링크를 연결할 파일 시스템의 작업 메뉴를 선택한 다음 \*링크 연결\*을 선택합니다.
5. 연결 링크 대화 상자에서 \* 새 링크 만들기 \* 를 선택하고 \* 계속 \* 을 선택합니다.
6. 링크 생성 페이지에서 코드박스에서 CloudFormation 또는 Terraform을 선택한 후 다음을 제공합니다.
  - a. \* 링크 이름 \*: 이 링크에 사용할 이름을 입력하십시오. 이름은 계정 내에서 고유해야 합니다.
  - b. **AWS Secrets Manager**: 선택 사항. Workload Factory가 AWS Secrets Manager에서 FSx for ONTAP 액세스 자격 증명을 가져올 수 있도록 허용합니다.

링크 배포 스택은 Lambda 권한 정책에 다음 기본 비밀 관리자 ARN 정규식을 자동으로 추가합니다.

```
arn:aws:secretsmanager:<link_deployment_region>:<link_deployment_account_id>:secret:FSxSecret*.
```

기본 사용 권한에 맞춰 암호를 만들거나 링크 정책에 대한 사용자 지정 사용 권한을 할당할 수 있습니다.

- AWS Secrets Manager로 VPC 전용 엔드포인트 구성 \* 은 기본적으로 비활성화됩니다. 이 옵션을 선택하면 VPC 개인 엔드포인트를 로컬로 저장하는 대신 VPC 전용 엔드포인트를 사용하여 암호를 저장합니다.

c. 링크 권한: 링크 권한에 대해 다음 옵션 중 하나를 선택하세요.

- 자동: AWS CloudFormation 코드가 Lambda 권한 정책과 실행 역할을 자동으로 생성하도록 이 옵션을 선택합니다.
- 사용자 제공: 지정된 Lambda 실행 역할과 연결된 정책을 Lambda 링크에 할당하려면 이 옵션을 선택합니다. 권한 정책에는 다음 권한이 필요합니다. `secretsmanager:GetSecretValue` AWS Secrets Manager를 활성화한 경우에만 권한이 필요합니다.

```
"ec2:CreateNetworkInterface",  
"ec2:DescribeNetworkInterfaces",  
"ec2:DeleteNetworkInterface",  
"ec2:AssignPrivateIpAddresses",  
"ec2:UnassignPrivateIpAddresses",  
"secretsmanager:GetSecretValue"
```

텍스트 상자에 Lambda 실행 역할 ARN을 입력합니다.

- d. \* 태그 \*: 필요에 따라 이 링크에 연결할 태그를 추가하여 리소스를 보다 쉽게 분류할 수 있습니다. 예를 들어, FSx for ONTAP 파일 시스템에서 이 링크를 사용 중인 것으로 식별하는 태그를 추가할 수 있습니다.
- e. 링크 등록: 링크 등록 방법에 대한 지침을 보려면 CloudFormation 또는 Terraform을 선택하고 지침을 따르세요.

CloudFormation 템플릿을 시작하면 Lambda에게 세 가지 권한이 부여됩니다. 워크로드 팩토리에서는 링크를 사용할 때 이러한 권한을 사용합니다.

```
"lambda:InvokeFunction",  
"lambda:GetFunction",  
"lambda:UpdateFunctionCode"
```

+ 스택을 성공적으로 만든 후 텍스트 상자에 Lambda ARN을 붙여 넣습니다.

- a. Workload Factory는 FSx for ONTAP 파일 시스템을 기반으로 AWS 계정, 위치 및 보안 그룹을 자동으로 검색합니다.

7. Create \* 를 선택합니다.

이벤트 페이지에서 링크 생성 상태를 모니터링할 수 있습니다. 이 작업에는 5분 이상 걸리지 않습니다.


8. Workload Factory 인터페이스로 돌아가면 링크가 FSx for ONTAP 파일 시스템과 연결되어 있는 것을 볼 수 있습니다.

워크로드 팩토리는 링크를 FSx for ONTAP 파일 시스템과 연결합니다. 고급 ONTAP 작업을 수행할 수 있습니다.

기존 링크를 **FSx for ONTAP** 파일 시스템에 연결합니다

링크를 생성한 후 하나 이상의 FSx for ONTAP 파일 시스템에 연결합니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 링크를 연결할 파일 시스템의 작업 메뉴를 선택한 다음 \*링크 연결\*을 선택합니다.
5. 연결 링크 페이지에서 \* 기존 링크 연결 \* 을 선택하고 링크를 선택한 다음 \* 계속 \* 을 선택합니다.
6. 인증 모드를 선택합니다.
  - 워크로드 팩토리: 암호를 두 번 입력합니다.
  - AWS Secrets Manager: 비밀 ARN을 입력합니다.

\_filesystemID\_는 선택 사항이지만, 비밀 ARN에 다음과 같은 키 유효 쌍이 포함되어 있는지 확인하세요.

- filesystemID = FSx\_filesystem\_id (선택 사항)
- 사용자 = FSx\_user
- password=user\_password입니다



AWS Secrets Manager를 인증하려면 사용자가 필요합니다. 이 사용자는 귀하가 제공한 \_FSx\_user\_ 이거나 FSx for ONTAP 파일 시스템에서 생성된 다른 사용자입니다. 기본 사용자는 fsxadmin 사용자를 제공하지 않는 경우.

7. Apply \* 를 선택합니다.

결과

이 링크는 FSx for ONTAP 파일 시스템에 연결됩니다. 고급 ONTAP 작업을 수행할 수 있습니다.

## AWS Secrets Manager 링크 인증 관련 문제 해결

문제

링크에 암호를 검색할 권한이 없습니다.

- 해결 \*: 링크가 활성화된 후 권한을 추가합니다. AWS 콘솔에 로그인하고 Lambda 링크를 찾은 다음 첨부된 권한 정책을 편집합니다.

문제

암호를 찾을 수 없습니다.

- 해상도 \*: 올바른 비밀 ARN을 제공합니다.



## 문제

암호가 올바른 형식이 아닙니다.

- 해상도 \*: AWS 비밀 관리자로 이동하여 형식을 편집합니다.

비밀에는 다음 키 유효 쌍이 포함되어야 합니다.

- filesystemID = FSx\_filesystem\_id입니다
- 사용자 이름 = FSx\_user
- password=user\_password입니다

## 문제

암호에 파일 시스템 인증을 위한 유효한 ONTAP 자격 증명이 포함되어 있지 않습니다.

- 해결 방법 \*: AWS 비밀 관리자에서 FSx for ONTAP 파일 시스템을 인증할 수 있는 자격 증명을 제공합니다.

## 워크로드 팩토리 링크 관리

Workload Factory 계정과 연결된 링크를 관리하세요. FSx for ONTAP 파일 시스템과 연결된 링크를 보고, 링크 인증에 사용되는 비밀번호를 제공하고, Workload Factory 콘솔에서 링크를 제거할 수 있습니다.

"링크에 대해 자세히 알아보세요" 링크를 만들고 연결하세요" 또는.

계정과 연결된 링크를 봅니다

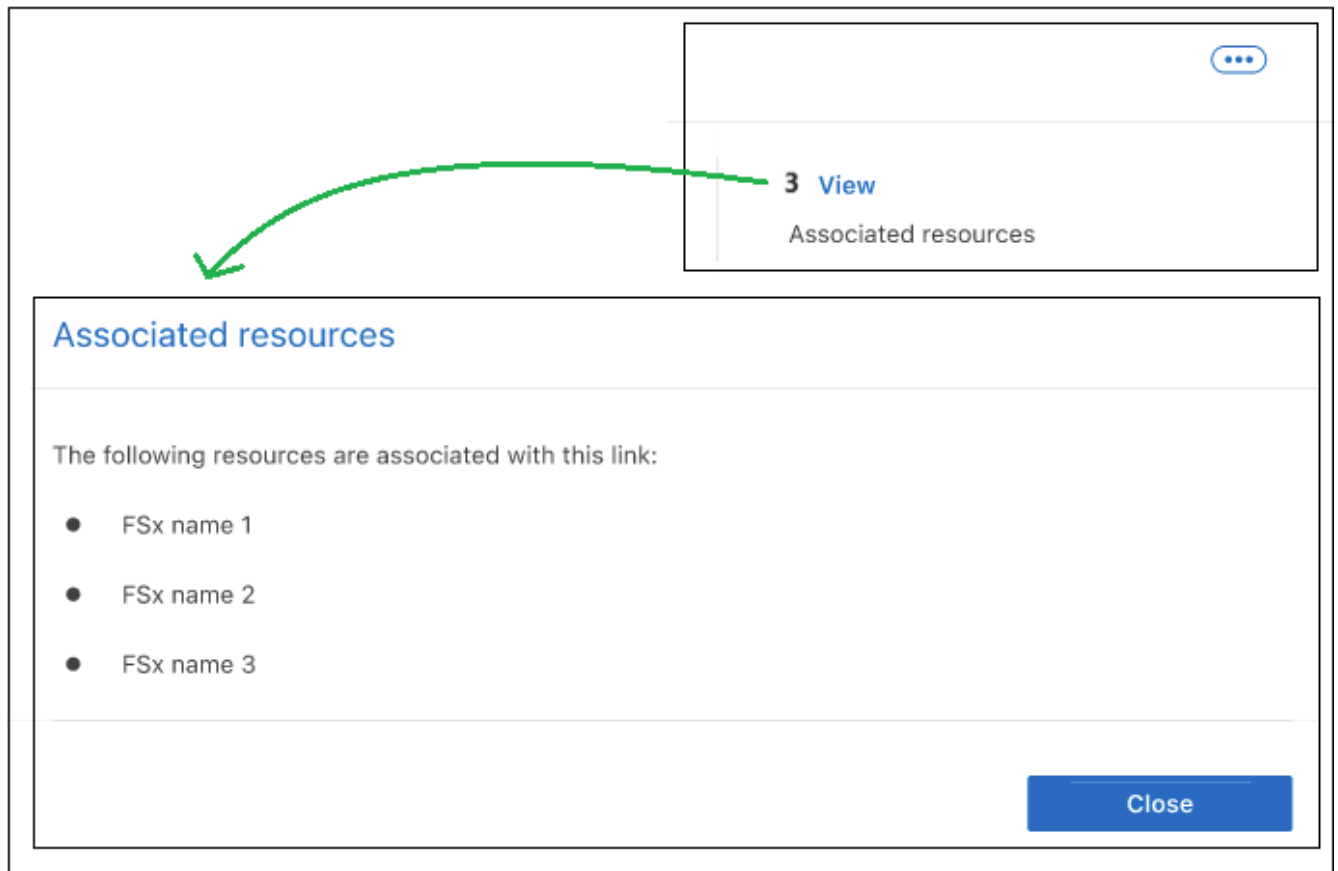
현재 계정과 연결된 링크를 볼 수 있습니다.

## 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 저장소 메뉴에서 \*관리\*를 선택한 다음 \*링크\*를 선택합니다.

기존 링크는 링크 페이지에 나타납니다.

3. 링크와 연결된 FSx for ONTAP 파일 시스템을 보려면 관련 리소스 섹션에서 \* 보기 \* 버튼을 선택합니다.



4. 링크에 대한 ARN(아마존 리소스 이름)이 필요한 경우 ARN 필드 옆에 있는 \_copy\_icon을 선택할 수 있습니다.

링크를 편집합니다

Workload Factory 인터페이스에서는 링크를 편집할 수 없습니다. 링크를 변경해야 하는 경우 새 링크를 만든 다음 해당 링크를 파일 시스템에 연결해야 합니다.



AWS 콘솔을 사용하여 Lambda 네트워크 구성(예: VPC, 서브넷 및 보안 그룹)을 편집할 수 있으며 변경 사항은 링크 관리 UI에 반영됩니다. 그러나 이러한 변경으로 인해 Lambda와 ONTAP 간 연결 문제가 발생할 수 있으며 권장되지 않습니다.

링크를 인증합니다


FSx for ONTAP 파일 시스템에 링크를 연결하려면 Workload Factory 자격 증명에 대한 관리자 사용자 암호나 AWS Secrets Manager 암호 ARN을 제공합니다.

콘솔 에이전트를 사용하는 경우 AWS Secrets Manager는 지원되지 않습니다.



링크당 하나의 인증 방법만 지원됩니다. 예를 들어, AWS Secrets Manager로 링크 인증을 선택한 경우 나중에 인증 방법을 변경할 수 없습니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.

- 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
- \*FSx for ONTAP\*에서 링크를 연결할 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
- 파일 시스템 개요에서 \* 링크 인증 \* 을 선택합니다.
- 인증 링크 페이지에서 인증 모드를 선택합니다.
  - 워크로드 팩토리: 암호를 두 번 입력합니다.
  - AWS Secrets Manager: 비밀 ARN을 입력합니다.
- Apply \* 를 선택합니다.


#### 결과

링크가 인증되고 고급 ONTAP 작업을 수행할 수 있습니다

링크 인증을 위한 암호를 업데이트합니다

관리자 암호가 유효하지 않으면 암호를 업데이트하여 ONTAP용 FSx 파일 시스템에 연결합니다.

#### 단계

- 중 하나를 사용하여 "콘솔 환경"로그인합니다.
- 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
- 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
- \*FSx for ONTAP\*에서 링크를 연결할 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
- 파일 시스템 개요에서 \* Update password \* 를 선택합니다.
- 인증 링크 페이지에서 새 암호를 두 번 입력합니다.
- Apply \* 를 선택합니다.

#### 결과


암호가 업데이트되고 링크가 이제 FSx for ONTAP 파일 시스템에 연결됩니다.

링크를 제거합니다

사용자 환경에서 더 이상 사용하지 않는 링크를 제거할 수 있습니다. FSx for ONTAP 파일 시스템 또는 링크를 사용하는 기타 리소스는 링크가 제거된 후 특정 기능을 사용할 수 없습니다.

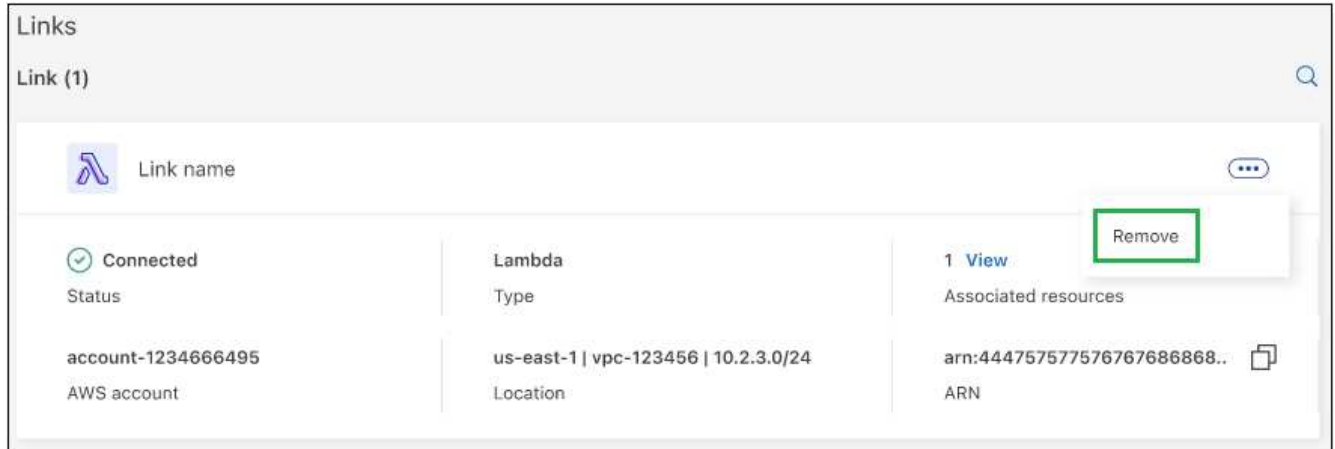
링크는 Workload Factory에서만 삭제되고 AWS 환경에서는 삭제되지 않습니다. Workload Factory에서 링크를 제거한 후 AWS 계정에서 Lambda 함수를 삭제해야 합니다.

#### 단계

- 중 하나를 사용하여 "콘솔 환경"로그인합니다.
- 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
- 저장소 메뉴에서 \*관리\*를 선택한 다음 \*링크\*를 선택합니다.

기존 링크는 링크 페이지에 나타납니다.

4. 링크 페이지에서 제거할 링크의 작업 메뉴를 선택한 다음 \*제거\*를 선택합니다.



5. 확실하면 \* 제거 \* 를 다시 선택하십시오.

AWS 설명서를 참조하십시오 ["Lambda 함수를 삭제합니다"](#).

## Workload Factory에서 캐시 볼륨을 검색합니다.

NetApp Workload Factory 콘솔을 벗어나지 않고도 캐시 관계와 연관된 캐시 볼륨을 검색하고 볼 수 있습니다. 캐시 관계는 ONTAP FlexCache 관계라고도 합니다. Workload Factory는 NetApp ONTAP의 원격 캐싱 기능인 FlexCache 기술을 사용하여 기존 캐시 관계를 검색합니다. FlexCache는 데이터 액세스를 가속화하고, WAN 지연 시간과 대역폭을 줄이고, 특히 클라이언트가 동일한 데이터에 반복적으로 액세스해야 하는 읽기 중심 워크로드의 비용을 줄여줍니다.

["FlexCache 사용하여 데이터를 복제하는 방법에 대해 자세히 알아보세요."](#)

이 작업에 대해

캐시 관계를 발견하려면 링크 연결이 필요합니다.


두 ONTAP 시스템(예: FSx for ONTAP 파일 시스템 하나와 Cloud Volumes ONTAP 시스템 하나)의 볼륨 간에 캐시 관계가 존재할 수 있습니다. 캐시 관계는 볼륨 간에 단일 FSx for ONTAP 파일 시스템 내에서도 존재할 수 있습니다.

시작하기 전에

시작하기 전에 다음 사항을 고려하세요.

- 파일 시스템의 캐시 관계를 알아보려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) . 링크가 연결되면 이 작업으로 돌아갑니다.
- 기존 캐시 관계가 있어야 합니다.

단계

1. 중 하나를 사용하여 ["콘솔 환경"](#)로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.

3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. **FSx for ONTAP\***에서 \*캐시 관계 탭을 선택합니다.
5. 캐시 볼륨이 표에 표시됩니다. 표에는 각 캐시 볼륨에 대한 다음 정보가 포함되어 있습니다.
  - 원본 클러스터: FlexCache 관계의 원점 또는 소스 클러스터입니다.
  - 원본 볼륨: FlexCache 관계의 원본 또는 소스 볼륨입니다.
  - 원본 저장소 **VM**: 볼륨의 원본 또는 소스 저장소 VM입니다.
  - 캐시 볼륨: FlexCache 관계의 캐시 또는 대상 볼륨입니다.
  - 캐시 스토리지 **VM**: 볼륨의 캐시 또는 대상 스토리지 VM입니다.
  - 상태: FlexCache 관계의 상태입니다.
  - 캐시의 사용 가능한 저장 공간: 캐시 볼륨에서 사용 가능한 저장 공간의 양입니다.
  - 캐시 파일 시스템: 캐시 볼륨의 파일 시스템입니다.
  - 쓰기 모드: FlexCache 관계의 쓰기 모드입니다.
  - **DR** 캐시: FlexCache 관계가 재해 복구(DR) 캐시인지 여부를 나타냅니다.
  - 내보내기 정책: 캐시 볼륨의 내보내기 정책입니다.

관련 정보

["캐시 볼륨 관리"](#)

## 볼륨 관리

### Workload Factory에서 ONTAP 볼륨에 대한 FSx 생성

FSx for ONTAP 파일 시스템을 설정한 후 Workload Factory에서 FSx for ONTAP 볼륨을 생성하여 데이터를 그룹화하기 위한 가상 리소스로 사용합니다.

이 작업에 대해

FSx for ONTAP 볼륨은 데이터를 가상으로 그룹화하고, 데이터가 저장되는 방식을 결정하고, 데이터에 대한 액세스 유형을 결정합니다. 볼륨은 파일 시스템 스토리지 용량을 소비하지 않습니다. 볼륨에 저장된 데이터는 주로 SSD 스토리지를 사용합니다. 볼륨의 계층화 정책에 따라 데이터가 용량 풀 스토리지를 사용할 수도 있습니다. 볼륨을 만들 때 볼륨 크기를 설정하고 나중에 크기를 변경할 수 있습니다.

다음 프로토콜을 볼륨에 사용할 수 있습니다.

- SMB/CIFS: Windows 운영 체제용 파일 저장 프로토콜
- NFS: Unix 운영 체제용 파일 스토리지 프로토콜입니다
- iSCSI: 블록 스토리지 프로토콜

S3 엔드포인트는 FSx for ONTAP 볼륨에 연결될 수 있습니다. S3 액세스 포인트를 사용하면 AWS S3 API를 통해 SMB/CIFS 또는 NFS 볼륨에 있는 파일 데이터에 액세스할 수 있습니다. 이를 통해 S3 액세스 포인트를 지원하는 AWS 서비스의 GenAI, ML 및 분석과 기존 데이터를 통합할 수 있습니다.

## 변경 불가능한 파일

이 기능은 SnapLock 이라고도 하며 기본적으로 비활성화되어 있습니다. 변경 불가능한 파일을 활성화하면 일정 기간 동안 데이터 삭제나 덮어쓰기가 방지됩니다. 이 기능을 활성화하는 것은 볼륨을 생성하는 동안에만 가능합니다. 해당 기능을 활성화한 후에는 비활성화할 수 없습니다. 이는 FSx for ONTAP 의 프리미엄 기능으로, 추가 요금이 부과됩니다. 자세한 내용은 다음을 참조하세요. "[SnapLock 작동 방법](#)" Amazon FSx for NetApp ONTAP 설명서.

- 보존 모드: *Enterprise* 또는 *\_Compliance\_* 의 두 가지 보존 모드 중에서 선택할 수 있습니다.
  - *Enterprise\_mode*, 변경 불가능한 파일 또는 SnapLock에서 관리자는 보존 기간 동안 파일을 삭제할 수 있습니다.
  - *Compliance\_mode*에서는 보존 기간이 만료되기 전에 WORM 파일을 삭제할 수 없습니다. 마찬가지로 볼륨 내의 모든 파일에 대한 보존 기간이 만료될 때까지 변경 불가능한 볼륨을 삭제할 수 없습니다.
- 보관 기간: 보관 기간에는 *\_보관 정책\_* 과 *\_보관 기간\_* 의 두 가지 설정이 있습니다. *\_보존 정책\_* 은 변경 불가능한 WORM 상태에서 파일을 보관하는 기간을 정의합니다. 고유한 보존 정책을 지정하거나 기본 보존 정책(지정되지 않음)인 30년을 사용할 수 있습니다. 최소 및 최대 *\_보관 기간\_* 은 파일 잠금에 허용되는 시간 범위를 정의합니다.



보존 기간이 만료된 후에도 WORM 파일을 수정할 수 없습니다. WORM 보호만 삭제하거나 새 보존 기간을 설정하여 WORM 보호를 다시 설정할 수 있습니다.

- 자동 커밋: 자동 커밋 기능을 활성화할 수 있습니다. 자동 커밋 기능은 파일이 자동 커밋 기간 동안 변경되지 않으면 SnapLock 볼륨에서 해당 파일을 WORM 상태로 커밋합니다. 자동 커밋 기능은 기본적으로 비활성화되어 있습니다. 자동 커밋하려는 파일이 SnapLock 볼륨에 있는지 확인해야 합니다.
- 권한 있는 삭제: SnapLock 관리자는 SnapLock Enterprise 볼륨에서 권한 있는 삭제를 커서 파일의 보존 기간이 만료되기 전에 파일을 삭제할 수 있습니다. 이 기능은 기본적으로 비활성화되어 있습니다.
- 볼륨 추가 모드: WORM으로 보호된 파일의 기존 데이터를 수정할 수 없습니다. 그러나 변경 불가능한 파일을 사용하면 WORM 추가 가능 파일을 사용하여 기존 데이터에 대한 보호를 유지할 수 있습니다. 예를 들어, 점진적으로 데이터를 쓰는 동안 로그 파일을 생성하거나 오디오 또는 비디오 스트리밍 데이터를 보존할 수 있습니다. "[볼륨 추가 모드에 대해 자세히 알아보십시오](#)" Amazon FSx for NetApp ONTAP 설명서.

## 시작하기 전에

볼륨을 생성하기 전에 다음 사전 요구 사항을 검토하십시오.

- Workload Factory 콘솔에 FSx for ONTAP 파일 시스템이 있어야 합니다.
- 스토리지 VM이 있어야 합니다.
- 프로토콜 액세스의 경우 다음을 수행합니다.
  - 볼륨에 대한 액세스를 구성하려면 링크를 연결해야 합니다. "[기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요](#)".. 링크가 연결되면 이 작업으로 돌아갑니다.
  - SMB/CIFS, NFS 또는 iSCSI 중 선택한 프로토콜에 대한 액세스를 구성해야 합니다.


## 볼륨을 생성합니다

코드상자에서 사용할 수 있는 REST API, CloudFormation 및 Terraform 도구를 사용하여 볼륨을 생성할 수 있습니다. "[자동화를 위해 Codebox를 사용하는 방법을 알아보십시오](#)"..



Codebox에서 Terraform을 사용할 때 복사하거나 다운로드하는 코드는 숨겨지고 암호가 숨겨집니다.  
fsxadmin vsadmin 코드를 실행할 때 암호를 다시 입력해야 합니다.

## 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 볼륨을 생성하려는 파일 시스템의 작업 메뉴를 선택하고 \*볼륨 생성\*을 선택합니다.
5. 볼륨 생성 페이지의 일반 세부 정보 아래에서 다음 세부 정보를 제공합니다.

- a. \* 볼륨 이름 \*: 볼륨의 이름을 입력합니다.
- b. \* 스토리지 VM 이름 \*: 필요에 따라 스토리지 VM 이름을 입력합니다.
- c. \* 볼륨 스타일 \*: \* FlexVol \* 또는 \* FlexGroup \* 볼륨을 선택합니다.

FlexVol 볼륨 스타일이 기본적으로 선택되어 있습니다.

FlexGroup 볼륨 크기는 구성 요소의 수에 따라 달라지며 구성 요소당 100GiB가 필요합니다.

- a. \* 볼륨 크기 \*: 볼륨 크기 및 단위를 입력합니다.

선택적으로 볼륨 자동 확장을 활성화합니다. 이 옵션은 볼륨 액세스 유형으로 \* 파일 액세스 \* 를 선택한 경우 사용할 수 있습니다.

- b. 볼륨 자동 증가: 선택적으로 볼륨 자동 증가 기능을 활성화하여 볼륨 용량이 최대 크기에 도달할 때까지 자동으로 확장되도록 할 수 있습니다. 이 기능은 데이터 사용량 증가에 대응하여 중단 없는 운영을 보장합니다.

최대 볼륨 증가 크기와 단위를 지정하세요. 현재 볼륨 크기보다 작은 최대 증가 크기를 설정할 수 없습니다.

- c. \* 태그 \*: 선택적으로 최대 50개의 태그를 추가할 수 있습니다.

6. Access(연결된 링크가 있는 파일 시스템에만 해당)에서 다음 세부 정보를 제공합니다.

- a. \* 액세스 유형 \*: \* 파일 액세스 \* 또는 \* 액세스 차단 \* 을 선택합니다. 볼륨 액세스를 구성하는 추가 필드는 선택에 따라 다릅니다.

- \* 파일 액세스 \*: SMB/CIFS, NFS 또는 이중(SMB/NFS) 프로토콜을 사용하여 권한 있는 여러 사용자와 장치가 볼륨에 액세스할 수 있습니다.

볼륨에 대한 파일 액세스를 설정하려면 다음 필드를 완료하십시오.

- b. \* NFS 내보내기 정책 \*: NFS 액세스를 제공하기 위해 다음 세부 정보를 제공합니다.

- i. \* 액세스 제어 \*: 드롭다운 메뉴에서 \* 사용자 지정 내보내기 정책 \*, \* 기존 내보내기 정책 \* 또는 \* 볼륨에 대한 액세스 없음 \* 을 선택합니다.

- ii. \* 수출 정책 이름 \*:

사용자 지정 내보내기 정책을 선택한 경우 드롭다운 메뉴에서 기존 정책 이름을 선택합니다.

기존 익스포트 정책을 선택한 경우 새 정책 이름을 입력합니다.

- i. \* 수출 정책 규칙 추가 \*: 필요에 따라 사용자 지정 수출 정책의 경우 수출 정책 규칙을 정책에 추가할 수 있습니다.

c. **SMB/CIFS** 공유: 다음을 제공하세요.

- i. 이름: 액세스를 제공하려면 SMB/CIFS 공유 이름을 입력하세요.
- ii. \* 권한 \*: 모든 권한, 읽기/쓰기, 읽기 또는 권한 없음 을 선택한 다음 세미콜론(;)으로 구분된 사용자 또는 그룹을 입력합니다. 사용자 또는 그룹은 대소문자를 구분하며 사용자 도메인은 "domain\username" 형식을 사용하여 포함되어야 합니다.

d. \* 보안 스타일 \*: 이중 프로토콜 볼륨의 경우 UNIX 또는 NTFS 보안 스타일을 선택합니다. UNIX는 이중 프로토콜 볼륨의 기본 보안 스타일입니다. 이 컨텍스트에서 사용자 매핑에 대한 자세한 지침은 AWS 블로그 문서를 ["Amazon FSx for NetApp ONTAP으로 멀티프로토콜 워크로드를 지원합니다"](#) 참조하십시오.

- \* 블록 액세스 \*: 중요한 비즈니스 응용 프로그램을 실행하는 호스트가 iSCSI 프로토콜을 사용하여 볼륨에 액세스할 수 있습니다. 파일 시스템 스케일아웃 구축에 HA 쌍 6개 이하가 있는 경우에만 블록 액세스를 사용할 수 있습니다.

볼륨에 대한 블록 액세스를 설정하려면 다음 필드를 완료하십시오.

A. \* iSCSI 구성 \*: 볼륨에 대한 블록 액세스를 위해 iSCSI를 구성하려면 다음 세부 정보를 제공하십시오.

- I. 새 이니시에이터 그룹 생성 \* 또는 \* 기존 이니시에이터 그룹 매핑 \* 을 선택합니다.
- II. 드롭다운 메뉴에서 \* 호스트 운영 체제 \* 를 선택합니다.
- III. 새 이니시에이터 그룹에 대해 \* 이니시에이터 그룹 이름 \* 을 입력합니다.
- IV. 호스트 이니시에이터 에서 IQN(iSCSI 정규화된 이름) 호스트 이니시에이터를 하나 이상 추가합니다.

e. **S3 액세스 포인트**: 선택적으로 AWS S3 API를 통해 NFS 또는 SMB/CIFS 볼륨에 있는 FSx for ONTAP 파일 시스템 데이터에 액세스하기 위해 S3 액세스 포인트를 연결합니다. 파일 접근 유형만 지원됩니다. 다음 세부 정보를 제공합니다.

- **S3 액세스 포인트 이름**: S3 액세스 포인트의 이름을 입력하세요.
- **사용자**: 볼륨에 액세스할 수 있는 기존 사용자를 선택하거나 새 사용자를 만듭니다.
- **사용자 유형**: 사용자 유형으로 **UNIX** 또는 \*Windows\*를 선택합니다.
- **네트워크 구성**: 인터넷 또는 \*Virtual private cloud (VPC)\*를 선택하십시오. 선택한 네트워크 유형에 따라 액세스 포인트가 인터넷에서 접근 가능한지 또는 특정 VPC로 제한되는지가 결정됩니다.
- **메타데이터 활성화**: 메타데이터를 활성화하면 S3 액세스 포인트에서 액세스할 수 있는 모든 객체가 포함된 S3 테이블이 생성되며, 이를 감사, 거버넌스, 자동화, 분석 및 최적화에 사용할 수 있습니다. 메타데이터를 활성화하면 추가 AWS 비용이 발생합니다. 자세한 내용은 ["Amazon S3 가격 책정 문서"](#)(를) 참조하십시오.

f. **S3 액세스 포인트 태그**: 필요에 따라 최대 50개의 태그를 추가하거나 태그를 제거할 수 있습니다.

7. **효율성 및 보호** 아래에 다음 세부 정보를 제공합니다.

a. **저장소 효율성**: 기본적으로 활성화되어 있습니다. 기능을 비활성화하려면 선택하세요.

ONTAP은 중복 제거 및 압축 기능을 사용하여 스토리지 효율성을 달성합니다. 중복 제거는 중복되는 데이터 블록을 제거합니다. 데이터 압축: 데이터 블록을 압축하여 필요한 물리적 스토리지의 양을 줄입니다.

b. \* **스냅샷 정책** \*: 스냅샷 정책을 선택하여 스냅샷의 빈도와 보존을 지정합니다.



다음은 AWS의 기본 정책입니다. 기존 스냅샷 정책을 표시하려면 다음을 수행해야 합니다. ["링크를 연결합니다"](#).

#### default

이 정책은 다음 스케줄에 따라 스냅샷을 자동으로 생성하고 가장 오래된 스냅샷 복사본은 새 복제본을 위한 공간을 확보하기 위해 삭제합니다.

- 시간당 최대 6개의 스냅샷이 해당 시간 이후 5분 동안 촬영되었습니다.
- 월요일부터 토요일까지 자정 이후 10분에 최대 2개의 일일 스냅샷을 촬영합니다.
- 매주 일요일 자정 이후 15분에 최대 2개의 주간 스냅샷이 촬영됩니다.



스냅샷 시간은 기본적으로 UTC(협정 세계시)로 설정된 파일 시스템의 시간대를 기준으로 합니다. 시간대 변경에 대한 자세한 내용은 NetApp 지원 설명서의 ["시스템 시간대 표시 및 설정"](#) 참조하십시오.

#### default-1weekly

이 정책은 주간 스케줄에서 스냅샷을 하나만 보존한다는 점을 제외하고 정책과 동일한 방식으로 default 작동합니다.

#### none

이 정책은 스냅샷을 촬영하지 않습니다. 이 정책을 볼륨에 할당하여 자동 스냅샷이 생성되지 않도록 할 수 있습니다.

c. \* Tiering policy \*: 볼륨에 저장된 데이터에 대한 계층화 정책을 선택합니다.

Workload Factory 콘솔을 사용하여 볼륨을 생성할 때 기본 티어링 정책은 `_균형(자동)_`입니다. 볼륨 티어링 정책에 대한 자세한 내용은 다음을 참조하십시오. ["볼륨 스토리지 용량"](#) AWS FSx for NetApp ONTAP 설명서에 나와 있습니다. 참고로 Workload Factory 콘솔에서는 계층화 정책에 대해 사용 사례 기반 이름을 사용하며, ONTAP 계층화 정책 이름은 괄호 안에 FSx로 표시됩니다.

d. 변경 불가능한 파일: 변경 불가능한 파일 기능을 활성화하면 이 볼륨의 파일이 변경 불가능한 WORM(한 번 쓰고 여러 번 읽음) 상태로 영구적으로 커밋됩니다. 다음 세부 정보를 제공하세요.

i. SnapLock\*에서 제공하는 \* 변경 불가능한 파일을 활성화하려면 선택합니다.

ii. 동의하고 계속하려면 상자를 선택합니다.

iii. 활성화 \* 를 선택합니다.

iv. \* 보존 모드 \*: \* Enterprise \* 또는 \* Compliance \* 모드를 선택합니다.

v. \* 보존 기간 \*:

▪ 보존 정책 선택:

▪ \* Unspecified \*: 보존 정책을 30년으로 설정합니다.

▪ \* 기간 지정 \*: 자신의 보존 정책을 설정할 초, 분, 시간, 일, 월 또는 연도 수를 입력합니다.

▪ 최소 및 최대 보존 기간 선택:

▪ \* 최소 \*: 최소 보존 기간을 설정할 초, 분, 시간, 일, 개월 또는 연도 수를 입력합니다.

▪ \* 최대 \*: 최대 보존 기간을 설정할 초, 분, 시간, 일, 개월 또는 연도 수를 입력합니다.

- vi. **autocomit**: 자동 커밋을 비활성화하거나 활성화합니다. 자동 커밋을 설정한 경우 자동 커밋 시간을 설정합니다.
- vii. **특권 삭제**: 비활성화 또는 활성화. 권한 있는 삭제를 활성화하면 SnapLock 관리자가 보존 기간이 만료되기 전에 파일을 삭제할 수 있습니다.
- viii. **\* 볼륨 추가 모드 \***: 비활성화 또는 활성화. WORM 파일에 새 콘텐츠를 추가할 수 있습니다.
- e. **ARP/AI**: AI를 탑재한 NetApp 자율형 랜섬웨어 보호(ARP/AI)는 링크가 파일 시스템에 연결된 경우 기본적으로 활성화됩니다. "[ARP/AI에 대해 자세히 알아보세요](#)".. 계속하려면 설명을 수락하십시오.

해당 기능을 사용할 수 없는 경우, 다음 중 하나의 이유가 있습니다.

- 링크는 파일 시스템과 연관되지 않습니다. "[기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요](#)".. 링크가 연결되면 이 작업으로 돌아갑니다.
- 변경 불가능한 파일이 있는 볼륨과 iSCSI 및 NVMe 프로토콜이 있는 볼륨은 ARP/AI에서 지원되지 않습니다.
- 파일 시스템에는 이미 ARP/AI 정책이 있습니다.

8. 고급 구성에서 다음을 제공합니다.

- a. **\* Junction path \***: 볼륨이 마운트되는 스토리지 VM 네임스페이스의 위치를 입력합니다. 기본 접합 경로는 ``/<volume-name>``입니다.
- b. **\* aggregates list \***: FlexGroup 볼륨에만 해당됩니다. 애그리게이트를 추가하거나 제거합니다. 최소 애그리게이트 수는 1개입니다.
- c. **\* 구성 요소 수 \***: FlexGroup 볼륨에만 해당됩니다. 애그리게이트당 구성요소 수를 입력합니다. 구성요소당 100GiB가 필요합니다.

9. Create \* 를 선택합니다.

관련 정보

- "[Workload Factory에서 볼륨 용량 조정](#)"
- "[Workload Factory에서 볼륨 계층화 정책 변경](#)"
- "[Workload Factory에서 S3 액세스 포인트 관리](#)"

## FSx for ONTAP 파일 시스템 데이터에 액세스합니다

온프레미스에서 NAS 클라이언트의 볼륨을 마운트하고 SAN 클라이언트용 iSCSI LUN을 마운트하여 FSx for ONTAP 파일 시스템에 액세스할 수 있습니다.

"[데이터 액세스](#)" Amazon FSx for NetApp ONTAP 설명서에서 참조용 데이터에 액세스하는 방법에 대한 항목을 제공합니다.


NetApp Workload Factory에서 볼륨의 마운트 지점을 가져올 수도 있습니다.

### NetApp Workload Factory에서 볼륨의 마운트 지점 가져오기

CIFS 공유 또는 NFS 클라이언트에서 공유를 마운트하기 위한 볼륨의 마운트 지점을 가져옵니다.

단계

1. 중 하나를 사용하여 "[콘솔 환경](#)"로그인합니다.

2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. \*FSx for ONTAP\*에서 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
4. 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.
5. 볼륨 탭에서 볼륨에 대한 작업 메뉴를 선택한 다음, \*기본 작업\*을 선택하고, \*마운트 명령 보기\*를 선택합니다.
6. Mount 명령 대화 상자에서 \* Copy \* 를 선택하여 NFS 마운트 지점 또는 CIFS 공유에 대한 명령을 복사합니다. 복사한 명령을 터미널에 입력합니다.
7. 닫기 \* 를 선택합니다.

#### NAS 클라이언트에 연결합니다

- ["Linux 클라이언트에서 볼륨을 마운트합니다"](#)
- ["Windows 클라이언트에 볼륨을 마운트합니다"](#)
- ["macOS 클라이언트에 볼륨을 마운트합니다"](#)

#### SAN 클라이언트에 연결합니다

- ["Linux 클라이언트에 iSCSI LUN을 마운트합니다"](#)
- ["Windows 클라이언트에 iSCSI LUN을 마운트합니다"](#)

## 블록 스토리지 리소스 생성

### NetApp Workload Factory에서 파일 시스템용 이니시에이터 그룹을 생성합니다

NetApp Workload Factory를 사용하여 이니시에이터 그룹을 생성하고 SAN 블록 장치에 대한 호스트 액세스를 관리하세요.

#### 이 작업에 대해

이니시에이터 그룹(igroup)은 블록 장치(LUN)를 해당 장치에 접근할 수 있는 컴퓨팅 리소스에 연결합니다. 볼륨에 대한 접근이 광범위하게 허용되고 사용자 권한으로 접근을 제어하는 NFS 또는 CIFS와 달리, 블록 스토리지 권한은 시스템 수준에서 작동합니다. 일반적으로 한 번에 하나의 시스템만 블록 장치에 접근할 수 있습니다.

igroup은 블록 스토리지에 대한 권한 계층 역할을 합니다. 서버가 스토리지 시스템에 연결되면 iSCSI 인증 호스트 이니시에이터(IQN)를 사용하여 자신을 식별합니다. 해당 IQN이 하나 이상의 igroup에 속하면 서버는 해당 igroup과 연결된 모든 LUN에 액세스할 수 있게 됩니다. iSCSI가 제대로 작동하려면 igroup과 iSCSI 호스트 연결이 모두 필요합니다.

#### 시작하기 전에

igroup을 생성하려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크를 연결한 후, 이 작업으로 돌아오십시오.

#### 단계

1. 중 하나를 사용하여 ["콘솔 환경"](#)로 로그인합니다.
2. 저장소 타일에서 \*저장소로 이동\*을 선택합니다.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.

4. **FSx for ONTAP\***에서 **\*장치 차단** 탭을 선택합니다.
5. 리소스 유형 **\*Create initiator group\***을 선택한 다음 **\*Create igroup\***을 선택합니다.
6. 이니시에이터 그룹 생성 대화 상자에서 다음을 수행합니다.
  - **igroup name**: 이니시에이터 그룹의 이름을 입력합니다.
  - **igroup 설명**: (선택 사항) 이니시에이터 그룹에 대한 설명을 입력하십시오.
  - 스토리지 **VM** 이름: 이니시에이터 그룹의 스토리지 VM을 선택합니다.
  - 블록 디바이스 이름: 이니시에이터 그룹과 연결할 블록 디바이스를 하나 이상 선택합니다. 나열된 블록 디바이스는 아직 호스트 이니시에이터에 매핑되지 않은 디바이스입니다.
  - 운영 체제 유형: 운영 체제 유형으로 Linux, VMware 또는 Windows를 선택합니다.
  - 호스트 이니시에이터: 이니시에이터 그룹에 하나 이상의 iSCSI 적격(IQN) 호스트 이니시에이터를 추가합니다.
7. Create \* 를 선택합니다.

관련 정보

["FSx for ONTAP 파일 시스템의 igroup을 관리합니다."](#)

**NetApp Workload Factory** 에서 파일 시스템용 블록 장치를 생성합니다.

사업 부문(LOB) 애플리케이션 요구 사항을 지원하는 블록 장치를 생성합니다.

이 작업에 대해

NetApp Workload Factory 의 블록 장치에는 FlexVol 볼륨만 지원됩니다. iSCSI 프로토콜을 사용하여 블록 장치를 생성할 수 있습니다.

블록 크기는 사용 가능한 FlexVol volume 크기보다 작아야 합니다.

시작하기 전에

- 차단 장치를 생성하려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크를 연결한 후 이 작업으로 돌아오세요.

단계

1. 중 하나를 사용하여 **"콘솔 환경"**로그인합니다.
2. 저장소 타일에서 **\*저장소로 이동\***을 선택합니다.
3. 저장소 메뉴에서 **\*FSx for ONTAP\***를 선택합니다.
4. **FSx for ONTAP\***에서 **\*장치 차단** 탭을 선택합니다.
5. **\*블록 장치 생성\***을 선택하세요.
6. **\*볼륨 세부 정보\***에서 다음을 수행하십시오.
  - a. 권명: 다음 옵션 중 하나를 선택하십시오.
    - 새 볼륨을 생성하고 볼륨 이름을 입력하십시오.
    - 기존 볼륨을 선택하세요.
  - b. 저장소 **VM**: 저장소 VM을 선택하세요.

- c. 볼륨 스타일: 기본 볼륨 스타일은 \* FlexVol\*입니다.
- d. 용량: 용량을 입력하고 단위를 선택하세요. FlexVol volume 당 최대 크기는 100TiB입니다.
- e. 볼륨 자동 증가: 선택적으로 볼륨 자동 증가 기능을 활성화하면 볼륨이 용량에 도달했을 때 자동으로 크기가 증가합니다. 최대 성장 크기는 300 TiB입니다.
- f. 태그: 선택적으로 태그를 추가하여 차단 장치를 정리하고 분류할 수 있습니다.

7. \*차단 장치 세부 정보\*에서 다음을 수행하십시오.

- a. 차단 장치 이름: 차단 장치의 이름을 입력하십시오.
- b. 블록 장치 크기: 블록 장치의 크기를 입력하고 단위를 선택하십시오. 블록 장치 크기는 사용 가능한 볼륨 크기보다 작아야 합니다.

8. \*액세스\*에서 다음을 수행하십시오.

- a. **iSCSI** 구성: 다음 옵션 중 하나를 선택하십시오.
  - 새 이니시에이터 그룹 생성: 호스트 운영 체제, 이니시에이터 그룹 이름을 제공하고 하나 이상의 iSCSI 정규화 이름(IQN) 호스트 이니시에이터를 추가합니다.
  - 기존 이니시에이터 그룹 매핑: 기존 이니시에이터 그룹을 선택하고 호스트 운영 체제를 제공한 다음 하나 이상의 iSCSI 정규화된 이름(IQN) 호스트 이니시에이터를 선택합니다.

9. 효율성 및 보호 항목에서 다음을 수행하십시오.

- a. 저장소 효율성: 기본적으로 활성화되어 있습니다. 기능을 비활성화하려면 선택하세요.

ONTAP은 중복 제거 및 압축 기능을 사용하여 스토리지 효율성을 달성합니다. 중복 제거는 중복되는 데이터 블록을 제거합니다. 데이터 압축: 데이터 블록을 압축하여 필요한 물리적 스토리지의 양을 줄입니다.

- b. \* 스냅샷 정책 \*: 스냅샷 정책을 선택하여 스냅샷의 빈도와 보존을 지정합니다.

다음은 AWS의 기본 정책입니다. 기존 스냅샷 정책을 표시하려면 다음을 수행해야 합니다. xref:./"링크를 연결합니다".

#### default

이 정책은 다음 스케줄에 따라 스냅샷을 자동으로 생성하고 가장 오래된 스냅샷 복사본은 새 복제본을 위한 공간을 확보하기 위해 삭제합니다.

- 시간당 최대 6개의 스냅샷이 해당 시간 이후 5분 동안 촬영되었습니다.
- 월요일부터 토요일까지 자정 이후 10분에 최대 2개의 일일 스냅샷을 촬영합니다.
- 매주 일요일 자정 이후 15분에 최대 2개의 주간 스냅샷이 촬영됩니다.



스냅샷 시간은 기본적으로 UTC(협정 세계시)로 설정된 파일 시스템의 시간대를 기준으로 합니다. 시간대 변경에 대한 자세한 내용은 NetApp 지원 설명서의 을 "시스템 시간대 표시 및 설정" 참조하십시오.

#### default-1weekly

이 정책은 주간 스케줄에서 스냅샷을 하나만 보존한다는 점을 제외하고 정책과 동일한 방식으로 default 작동합니다.

none

이 정책은 스냅샷을 촬영하지 않습니다. 이 정책을 볼륨에 할당하여 자동 스냅샷이 생성되지 않도록 할 수 있습니다.

c. \* Tiering policy \*: 볼륨에 저장된 데이터에 대한 계층화 정책을 선택합니다.

Workload Factory 콘솔을 사용하여 볼륨을 생성할 때 기본 티어링 정책은 \_균형(자동)\_입니다. 볼륨 티어링 정책에 대한 자세한 내용은 다음을 참조하십시오. "[볼륨 스토리지 용량](#)" AWS FSx for NetApp ONTAP 설명서에 나와 있습니다. 참고로 Workload Factory 콘솔에서는 계층화 정책에 대해 사용 사례 기반 이름을 사용하며, ONTAP 계층화 정책 이름은 괄호 안에 FSx로 표시됩니다.

d. **ARP/AI**: AI를 탑재한 NetApp 자율형 랜섬웨어 보호(ARP/AI)는 링크가 파일 시스템에 연결된 경우 기본적으로 활성화됩니다. "[ARP/AI에 대해 자세히 알아보세요](#)".. 계속하려면 설명을 수락하십시오.

해당 기능을 사용할 수 없는 경우, 다음 중 하나의 이유가 있습니다.

- 링크는 파일 시스템과 연관되지 않습니다. "[기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요](#)".. 링크가 연결되면 이 작업으로 돌아갑니다.
- 변경 불가능한 파일이 포함된 볼륨과 NVMe 프로토콜을 사용하는 볼륨은 ARP/AI를 지원하지 않습니다.
- 파일 시스템에는 이미 ARP/AI 정책이 있습니다.

10. Create \* 를 선택합니다.

관련 정보

["FSx for ONTAP 파일 시스템의 블록 장치 관리"](#)

## FSx for ONTAP 파일 시스템용 스토리지 VM을 생성합니다

NetApp Workload Factory에서 워크로드에 대한 스토리지 및 데이터 서비스에 가상으로 액세스하기 위해 FSx for ONTAP 파일 시스템에 대한 스토리지 VM(SVM)을 만듭니다.

이 작업에 대해

스토리지 VM은 Workload Factory Storage의 각 워크로드에서 데이터에 액세스하는 데 사용할 수 있는 격리된 파일 서버입니다. 각 SVM에는 데이터 관리 및 액세스를 위한 자체 관리 자격 증명과 엔드포인트가 있습니다.

SVM을 사용하면 FSx for ONTAP에서 데이터에 액세스할 때 클라이언트와 워크스테이션이 SVM의 엔드포인트(IP 주소)를 사용하여 SVM에서 호스팅하는 볼륨, CIFS/SMB 공유 또는 iSCSI LUN을 마운트합니다.

시작하기 전에

파일 시스템당 지원되는 스토리지 VM 수를 확인합니다. 파일 시스템당 최대 SVM 수는 AWS 설명서의 ["FSx for ONTAP 스토리지 가상 머신 관리"](#) .


### 스토리지 VM을 생성합니다

Workload Factory 콘솔에서 스토리지 VM을 생성할 수 있습니다. Codebox에서 제공하는 다음 도구도 사용할 수 있습니다: REST API, CloudFormation, Terraform. "[자동화를 위해 Codebox를 사용하는 방법을 알아보십시오](#)" .



Codebox에서 Terraform을 사용할 때 복사하거나 다운로드하는 코드는 숨겨지고 암호가 숨겨집니다. fsxadmin vsadmin 코드를 실행할 때 암호를 다시 입력해야 합니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요의 스토리지 VM에서 \*스토리지 VM 생성\*을 선택합니다.
6. 스토리지 VM 생성 페이지의 스토리지 VM 구성에서 다음 정보를 제공하십시오.
  - a. \* 이름 \*: 스토리지 VM의 이름을 입력합니다.
  - b. \* 스토리지 VM 자격 증명 \*: 이 스토리지 VM 사용자의 암호를 vsadmin 제공하거나 파일 시스템의 fsxadmin 사용자 자격 증명을 사용합니다.
  - c. \* 루트 볼륨 보안 스타일 \*: 데이터에 액세스하는 클라이언트 유형(UNIX(Linux 클라이언트), NTFS(Windows 클라이언트) 또는 혼합)에 따라 루트 볼륨 보안 스타일을 선택합니다.
  - d. \* 태그 \*: 선택적으로 최대 50개의 태그를 추가할 수 있습니다.
7. Create \* 를 선택합니다.

## 데이터 보호

### NetApp Workload Factory의 데이터 보호 유형

FSx for ONTAP 데이터 보호를 위해 스냅샷, AI를 활용한 NetApp Autonomous Ransomware Protection, 복제 및 백업을 지원합니다. 불가피한 상황에 대비하고 데이터를 보호하려면 다양한 데이터 보호 유형을 조합하여 사용하는 것이 좋습니다.

#### 데이터 보호 유형

워크로드의 데이터 보호를 통해 언제든지 데이터 손실로부터 복구할 수 있습니다. 사용할 기능을 선택하기 전에 데이터 보호 유형에 대해 알아보십시오.

#### 스냅샷 수

스냅샷은 소스 볼륨 내에 있는 볼륨의 읽기 전용 시점 이미지를 스냅샷 복사본으로 생성합니다. 스냅샷 복사본을 사용하여 개별 파일을 복구하거나 볼륨의 전체 내용을 복원할 수 있습니다. 스냅샷은 모든 백업 방법의 기초입니다. 볼륨에 생성된 스냅샷 복사본은 복제된 볼륨 및 백업 파일을 소스 볼륨에 대한 변경 내용과 동기화된 상태로 유지하는 데 사용됩니다.

#### AI를 활용한 NetApp 자율형 랜섬웨어 보호

AI(ARP/AI)를 탑재한 NetApp Autonomous Ransomware Protection은 NAS(NFS/SMB) 환경에서 워크로드 분석을 사용하여 랜섬웨어 공격일 수 있는 비정상적인 활동을 감지하고 경고합니다. 공격이 의심되는 경우 ARP/AI는 예약된 스냅샷에서 제공하는 기존 보호 기능 외에도 변경 불가능한 새로운 스냅샷을 생성합니다.

#### 복제

복제를 통해 다른 FSx for ONTAP 파일 시스템에 데이터의 보조 복사본이 생성되고 2차 데이터가 지속적으로 업데이트됩니다. 데이터는 최신 상태로 유지되고 재해 복구와 같이 필요할 때 언제든지 사용할 수 있는 상태로 유지됩니다.

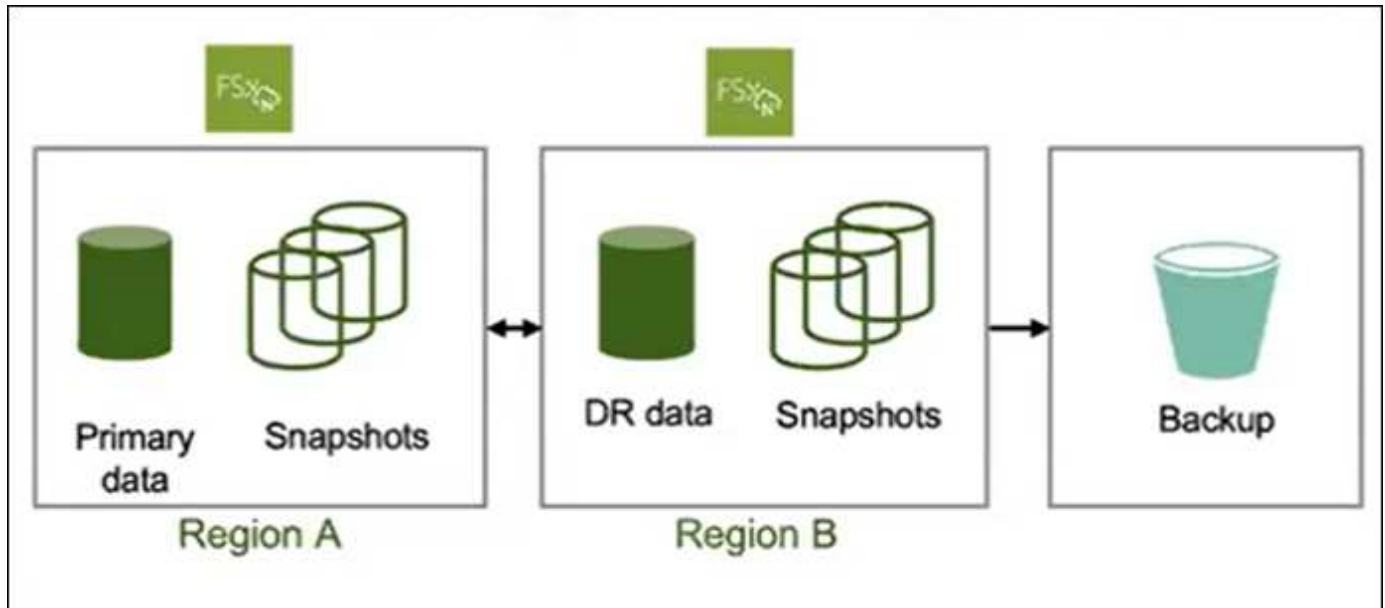


복제된 볼륨을 다른 FSx for ONTAP 파일 시스템에 생성하고 클라우드에 백업 파일을 생성하도록 선택할 수 있습니다. 또는 복제된 볼륨이나 백업 파일을 생성하도록 선택할 수 있습니다.

## 백업

보호 및 장기 보존을 위해 클라우드에 데이터 백업을 생성할 수 있습니다. 필요한 경우 백업에서 볼륨, 폴더 또는 개별 파일을 동일하거나 다른 작업 파일 시스템으로 복원할 수 있습니다.

다음 다이어그램은 스냅샷, 영역 간 복제, 오브젝트 스토리지에 백업을 사용하는 FSx for ONTAP 스토리지의 데이터 보호를 시각적으로 보여줍니다.



워크로드 데이터를 보호하는 모범 사례를 소개합니다

FSx for ONTAP은 선택한 복구 시점 및 시간 목표를 달성하기 위해 결합할 수 있는 여러 데이터 보호 옵션을 제공합니다. 최상의 보호를 위해 볼륨 스냅샷과 볼륨 백업을 모두 사용하는 것이 좋습니다.

RPO(복구 지점 목표)는 데이터의 최신 복사본이 얼마나 자주 복사되는지에 따라 보장되는지 설명합니다. 복구 시간 목표(RTO)는 데이터를 복원하는 데 걸리는 시간을 정의합니다.

스냅샷으로 워크로드 데이터를 보호합니다

스냅샷은 스케줄에 따라 생성된 볼륨의 가상 시점 버전입니다. 표준 파일 시스템 명령을 사용하여 스냅샷에 액세스할 수 있습니다. 스냅샷은 1시간 만에 RPO를 제공합니다. RTO는 복원할 데이터 양에 따라 달라지며 주로 볼륨 처리량 제한에 의해 제한됩니다. 또한 스냅샷을 사용하면 특정 파일 및 디렉토리를 복구할 수 있으므로 RTO가 훨씬 감소합니다. 스냅샷은 볼륨의 변경 사항에 대해서만 추가 볼륨 공간을 사용합니다.

**AI를 활용한 NetApp Autonomous Ransomware Protection으로 워크로드 데이터를 보호하세요**

AI(ARP/AI)를 탑재한 NetApp 자율형 랜섬웨어 보호 기능은 바이러스 백신 소프트웨어가 침입을 감지하지 못한 경우 중요한 추가 방어 계층 역할을 합니다. ARP/AI 정책을 설정하면 모든 스토리지 VM과 모든 기존 볼륨, 새로 생성된 볼륨에 대해 해당 정책이 활성화됩니다. ARP/AI를 활성화하면 모든 볼륨과 스토리지 VM을 감지하고 보호합니다. 파일 확장자가 비정상적으로 표시되는 경우 알림을 평가해야 합니다.



## 볼륨 복제로 워크로드 데이터 보호

볼륨 복제는 다른 지역에 있는 모든 스냅샷을 포함하여 볼륨의 최신 데이터의 복사본을 생성합니다. 볼륨 백업에서 전체 볼륨 복원 작업에 대해 몇 시간 분량의 RTO를 사용할 수 없는 경우 볼륨 복제를 수행하는 것이 좋습니다. 볼륨 복제를 사용하면 다른 지역에서 최신 데이터를 사용할 수 있지만 다른 지역의 볼륨을 사용하도록 클라이언트를 조정해야 합니다.

## 백업을 통해 워크로드 데이터 보호

볼륨 백업은 볼륨의 독립적인 시점 복사본을 제공합니다. 이러한 파일은 이전 백업을 저장하고 데이터에 대한 필요한 두 번째 복사본을 제공하는 데 사용할 수 있습니다. 매일, 매주 및 매월 백업 스케줄을 사용하면 RPO를 하루 기준으로 시작할 수 있습니다. 볼륨 백업은 전체로만 복원할 수 있습니다. 백업(RTO)에서 볼륨을 생성하는 데는 백업 크기에 따라 몇 시간에서 며칠까지 걸릴 수 있습니다.

## 워크로드 데이터 보호를 위한 권장 사항

워크로드 데이터를 보호하기 위해 다음 권장 사항을 고려하십시오.

- 재해 복구를 위해 볼륨 복제를 사용하세요. 애플리케이션에 낮은 RTO가 필요한 경우 볼륨 복제를 사용하여 데이터를 다른 지역으로 복제하는 것을 고려하세요.
- 스냅샷과 함께 볼륨 백업 사용: 두 기능을 함께 사용하면 스냅샷에서 파일을 복원하고 백업을 사용하여 볼륨이 손실되는 경우 전체 복원을 수행할 수 있습니다.
- 볼륨 백업 정책 정의: 백업 정책이 백업 기간 및 빈도에 대한 회사의 요구 사항을 충족하는지 확인합니다. 각 볼륨에 대해 최소 2개의 일일 백업을 유지하는 것이 좋습니다.
- 스냅샷 스케줄 정의: 이전 스냅샷을 사용하여 데이터를 복구할 가능성이 낮습니다. 기존 스냅샷을 추가 스냅샷 용량에 대한 비용과 비교하여 줄어드는 수익을 고려하여 스냅샷 스케줄을 정의하는 것이 좋습니다.
- 랜섬웨어 공격으로부터 데이터를 보호하기 위해 파일 시스템이나 개별 볼륨에 ARP/AI 정책을 활성화하여 보호 계층을 추가하세요.

## 스냅샷을 사용하세요

### FSx for ONTAP 볼륨의 수동 스냅샷을 생성합니다

NetApp Workload Factory에서 FSx for ONTAP 볼륨의 수동 스냅샷을 만듭니다. 스냅샷은 볼륨 콘텐츠의 특정 시점 버전입니다.

스냅샷은 볼륨의 리소스로, 수정된 데이터에 대해서만 공간을 소비하는 데이터를 즉시 캡처합니다. 데이터는 시간이 지남에 따라 변경되기 때문에 일반적으로 스냅샷은 오래될수록 더 많은 공간을 사용합니다.

FSx for ONTAP 볼륨은 Just-in-time copy-on-write를 사용하므로 스냅샷에서 수정되지 않은 파일이 볼륨의 용량을 소비하지 않습니다.




스냅샷은 데이터의 복사본이 아닙니다. 데이터 복사본을 만들려면 FSx for ONTAP 백업 또는 볼륨 복제 기능을 사용하는 것이 좋습니다.

## 시작하기 전에

볼륨의 수동 스냅샷을 생성하려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크가 연결되면 이 작업으로 돌아갑니다.

## 단계

1. 중 하나를 사용하여 "콘솔 환경"로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 스냅샷을 생성할 볼륨이 포함된 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \*Volumes\* 탭을 선택합니다.
6. 볼륨 탭에서 스냅샷으로 보호할 볼륨에 대한 작업 메뉴를 선택합니다.
7. \*데이터 보호 작업\*을 선택한 다음 \*스냅샷 관리\*를 선택합니다.
8. 스냅샷 관리 페이지에서 \*스냅샷 만들기\*를 선택합니다.
9. 스냅샷 만들기 대화 상자에서 다음을 수행합니다.
  - a. 스냅샷 이름 필드에 스냅샷 이름을 입력합니다.
  - b. 선택적으로, 라벨을 선택하거나 새 라벨을 만들 수 있습니다.
  - c. 보존 기간 \* 을 시간, 일, 월 또는 년 수로 설정합니다.
  - d. 선택 사항: 스냅샷이 보존 기간 동안 삭제되는 것을 방지하려면 스냅샷을 변경 불가능하게 설정합니다.  
  
변경 불가능한 스냅샷에 대한 설명을 수락합니다.
10. Create \* 를 선택합니다.

**Workload Factory**에서 스토리지 VM에 대한 스냅샷 정책을 만듭니다.

Workload Factory의 스토리지 VM에 대한 사용자 지정 스냅샷 정책을 만들어 스냅샷 생성 및 보존을 관리합니다. 스냅샷 정책은 시스템이 스토리지 VM에 대한 스냅샷을 생성하는 방법을 정의합니다. FSx for ONTAP 파일 시스템의 스토리지 VM에 대한 스냅샷 정책을 생성할 수 있습니다. 여러 스토리지 VM에서 정책을 공유할 수도 있습니다.

## 이 작업에 대해

FSx for ONTAP에 대한 내장된 세 가지 스냅샷 정책과 다른 사용자 지정 스냅샷 정책을 생성할 수 있습니다.

- default
- default-1weekly
- none

기본적으로 모든 볼륨은 파일 시스템의 default 스냅샷 정책에 연결됩니다. 대부분의 워크로드에 이 정책을 사용하는 것이 좋습니다.


정책을 사용자 정의하면 스냅샷을 생성할 시기, 보존할 복제본 수 및 이름 지정 방법을 지정할 수 있습니다.

## 시작하기 전에

- 스냅샷 정책을 생성한 후에는 스토리지 VM과의 연결을 수정할 수 없지만 언제든지 볼륨에서 정책을 추가하거나 제거할 수 있습니다.

- 스냅샷을 사용하기 전에 스냅샷 용량에 대해 다음 사항을 고려하십시오.
  - 대부분의 데이터 세트의 경우 20%의 추가 용량으로 스냅샷을 최대 4주 동안 보관할 수 있습니다. 데이터가 오래되면 복원에 사용할 가능성이 줄어듭니다.
  - 스냅샷의 모든 데이터를 덮어쓰면 볼륨 용량이 상당히 많이 소모되며, 이는 볼륨 용량 할당에 영향을 미칩니다.
- 사용자 정의 스냅샷 정책을 만들려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#).. 링크가 연결되면 이 작업으로 돌아갑니다.

## 단계

1. 중 하나를 사용하여 **"콘솔 환경"**로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \* Storage VMS \* 탭을 선택합니다.
6. 저장소 **VM** 탭에서 예약된 스냅샷으로 보호할 볼륨에 대한 작업 메뉴를 선택한 다음, \*고급 작업\*을 선택하고, \*스냅샷 정책 관리\*를 선택합니다.
7. 스냅샷 정책 관리 페이지에서 \* 스냅샷 정책 생성 \* 을 선택합니다.
8. 스냅샷 정책 이름 \* 필드에 스냅샷 정책의 이름을 입력합니다.
9. 필요한 경우 스냅샷 정책에 대한 설명을 입력합니다.
10. Policy schedule and copies \* 아래에서 스냅샷을 생성할 시기를 선택합니다. 예를 들어, 매 분 또는 매시간.  
  
둘 이상의 주파수를 선택할 수 있습니다.
11. 사본 수 \* 에 보관할 매수를 입력합니다.  
  
최대 인쇄 매수는 1,023매입니다.
12. 선택 사항: \* 명명 규칙 \* 에서 정책에 \* 접두사 \* 를 입력합니다.
13. \* 보존 레이블 \* 이 자동으로 채워집니다.  
  
이 레이블은 소스에서 타겟 파일 시스템으로의 복제에 지정된 스냅샷만 선택하는 데 사용되는 SnapMirror 또는 복제 레이블을 나타냅니다.
14. 선택 사항: 필요한 모든 스케줄에 대해 \* 변경 불가능한 스냅샷 \* 을 활성화하고, 각 스케줄에 대해 \* 보존 기간 \* 을 설정하고, 계속하려면 문을 수락합니다.  
  
변경 불가능한 스냅샷을 활성화하면 이 스냅샷 정책의 모든 스냅샷이 잠기므로 보존 기간 동안 스냅샷이 삭제되지 않습니다.
15. \* 스토리지 VM 간에 공유 \*: 기본적으로 활성화됩니다. 설정된 경우 스냅샷 정책은 파일 시스템의 모든 스토리지 VM에서 공유됩니다. 단일 스토리지 VM에 대한 스냅샷 정책을 생성하려면 비활성화하십시오.
16. Create \* 를 선택합니다.

## Workload Factory의 스냅샷에서 볼륨 복원

Workload Factory에서는 스냅샷의 데이터를 기존 볼륨이나 새 볼륨으로 복원할 수 있습니다. 복원 작업을 통해 볼륨에 삭제되거나 손상된 파일이 있는 경우 특정 시점으로 복구할 수 있습니다.

이 작업에 대해

스냅샷의 데이터를 기존 볼륨이나 새 볼륨으로 복원할 수 있습니다.


스냅샷에서 새 볼륨을 생성하면 볼륨 크기에 관계없이 몇 초 내에 전체 볼륨의 복사본이 생성됩니다. 새로 생성된 복사본은 새로운 볼륨을 나타냅니다.

시작하기 전에

스냅샷에서 볼륨을 생성하기 전에 다음과 같은 제한 사항을 고려하십시오.

- 볼륨의 기존 스냅샷 복사본이 있는 경우에만 스냅샷에서 볼륨을 복원할 수 있습니다.
- 권한 모델 변경: 이 작업을 사용하여 NAS(Network-Attached Storage) 프로토콜 유형을 전환하는 경우 보안 스타일이 제공하는 권한 모델도 전환할 수 있습니다. 파일 액세스 권한 문제가 발생할 수 있습니다. 이 문제는 권한 설정에 NAS 클라이언트 도구를 사용하여 관리자 액세스 권한으로만 수동으로 해결할 수 있습니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \*Volumes\* 탭을 선택합니다.
6. 볼륨 탭에서 스냅샷에서 복원할 볼륨에 대한 작업 메뉴를 선택합니다.
7. \*데이터 보호 작업\*을 선택한 다음 \*스냅샷 관리\*를 선택합니다.
8. 스냅샷 관리 페이지에서 복원할 스냅샷의 작업 메뉴를 선택한 다음, \*복원\*을 선택합니다.
9. 스냅샷에서 볼륨 복원 대화 상자에서 다음 옵션 중에서 선택하세요.

- \*새 볼륨으로 복원\*을 선택합니다.

복원된 볼륨 이름 \* 필드에 복원할 볼륨의 고유한 이름을 입력합니다.

- 스냅샷의 데이터를 기존 볼륨으로 복원합니다. 이 작업은 스냅샷 생성 시간 이후에 수정된 모든 데이터를 영구적으로 삭제합니다.

계속하려면 설명을 수락하십시오.

10. Restore \* 를 선택합니다.

백업을 개체 스토리지에 사용

**NetApp Workload Factory**에서 볼륨의 수동 백업을 만듭니다.

**NetApp Workload Factory**에서 정기적으로 예약된 백업 외에 볼륨의 수동 백업을 만듭니다.

이 작업에 대해


FSx for ONTAP 백업은 볼륨별로 수행되므로 각 백업에는 특정 볼륨의 데이터만 포함됩니다.

FSx for ONTAP 백업은 증분 백업이므로 최신 백업 후에 변경된 볼륨의 데이터만 저장됩니다. 따라서 백업을 생성하는데 필요한 시간과 백업에 필요한 스토리지를 최소화하여 데이터 중복을 방지함으로써 스토리지 비용을 절감할 수 있습니다.

시작하기 전에

볼륨을 백업하려면 볼륨과 파일 시스템 모두에 백업 스냅샷을 저장할 수 있는 충분한 SSD 저장 용량이 있어야 합니다. 백업 스냅샷을 생성할 때 스냅샷에 사용된 추가 스토리지 용량으로 인해 볼륨이 SSD 스토리지 사용률을 98%로 초과할 수 없습니다. 이 경우 백업이 실패합니다.

단계


1. 중 하나를 사용하여 **"콘솔 환경"**로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.
6. 볼륨 탭에서 백업할 볼륨에 대한 작업 메뉴를 선택합니다.
7. 데이터 보호 작업 \*, \* ONTAP용 FSx 백업 \* 을 선택한 다음 \* 수동 백업 \* 을 선택합니다.
8. 수동 백업 대화 상자에서 백업 이름을 입력합니다.
9. 백업 \* 을 선택합니다.

**NetApp Workload Factory**에서 백업으로부터 볼륨 복원

**NetApp Workload Factory**에서는 AWS 계정의 FSx for ONTAP 파일 시스템으로 백업의 볼륨을 복원할 수 있습니다.

워크로드 팩토리얼은 복원에 필요한 충분한 용량이 있는지 확인하고 그렇지 않은 경우 SSD 스토리지 계층 용량을 자동으로 추가할 수 있습니다.

단계

1. 중 하나를 사용하여 **"콘솔 환경"**로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 볼륨이 있는 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.
6. 볼륨 탭에서 백업에서 복원할 볼륨에 대한 작업 메뉴를 선택합니다.

7. 데이터 보호 작업 \*, \* ONTAP용 FSx 백업 \* 을 선택한 다음 \* 백업에서 복원 \* 을 선택합니다.

8. 백업에서 복원 대화 상자에서 다음을 제공합니다.

- a. \* 대상 파일 시스템 \* : 드롭다운 메뉴에서 대상 파일 시스템을 선택합니다.
- b. \* 대상 스토리지 VM \* : 드롭다운 메뉴에서 대상 스토리지 VM을 선택합니다.
- c. \* 백업 이름 \* : 드롭다운 메뉴에서 백업 이름을 선택합니다.
- d. \* 복원된 볼륨 이름 \* : 복원된 볼륨 이름을 입력합니다.

9. 복구 작업에 사용할 파일 시스템 용량을 확인합니다.

파일 시스템 용량이 제한된 경우 다음과 같은 문제가 발생할 수 있습니다.

- 복원을 통해 사용된 용량이 지정한 임계값을 초과할 수 있습니다. 복구 작업을 완료할 수 있습니다. 고려하다 "SSD 스토리지 계층 용량을 수동으로 추가" 또는 Workload Factory에서 SSD 스토리지 계층 용량을 자동으로 추가하도록 선택합니다.
- 복원에는 추가 SSD 용량이 필요합니다. 계속하려면 Workload Factory에서 SSD 스토리지 계층 용량을 자동으로 추가하도록 선택해야 합니다.

10. Restore \* 를 선택합니다.

## 복제를 사용하세요

NetApp Workload Factory에서 FSx for ONTAP으로 데이터를 복제

예기치 못한 재해 발생 시 데이터 손실을 방지하려면 NetApp Workload Factory에서 FSx for ONTAP 파일 시스템에 대한 복제 관계를 생성하십시오. 두 FSx for ONTAP 파일 시스템 간 또는 온프레미스 ONTAP 시스템과 FSx for ONTAP 파일 시스템 간에 데이터를 복제할 수 있습니다.

스토리지 VM 마이그레이션을 위해서는 복제 관계를 생성한 직후에 컷오버 작업을 완료해야 합니다.

이 작업에 대해

복제는 재해가 해당 지역에 영향을 미칠 경우 데이터를 보호하며, 마이그레이션 목적으로도 사용할 수 있습니다.

타겟 파일 시스템의 복제된 볼륨은 데이터 보호(DP) 볼륨이며 다음과 같은 명명 형식을 {OriginalVolumeName}\_copy 따릅니다.

불변 파일이 포함된 소스 볼륨을 복제하면 소스 볼륨의 보존 기간이 종료될 때까지 타겟 볼륨과 파일 시스템이 잠긴 상태로 유지됩니다. 불변 파일 기능은 FSx for ONTAP 파일 시스템에 대해 "볼륨을 생성하다"할 때 사용할 수 있습니다.



- iSCSI 또는 NVMe 프로토콜을 사용하는 블록 볼륨의 경우 복제가 지원되지 않습니다.
- 소스(읽기/쓰기) 볼륨 1개 또는 데이터 보호(DP) 볼륨을 복제할 수 있습니다. 계단식 복제는 지원되지만 세 번째 홉은 지원되지 않습니다. 에 대해 자세히 "계단식 복제"알아보십시오.

## 마이그레이션 사용 사례

마이그레이션 사용 사례를 선택할 때 단일 스토리지 VM에 대해 스토리지 VM 데이터와 구성 설정을 복제하도록 선택적으로 선택할 수 있습니다. 데이터와 구성 설정을 동시에 마이그레이션할 경우 지난 24시간 이내에 볼륨에 대한 마지막 복제가 완료되었는지 확인하십시오. 이 기능을 사용하려면 동일한 스토리지 VM에 있는 모든 볼륨을 선택해야

합니다. 모든 볼륨의 계층화 정책은 기본적으로 소스 볼륨의 계층화 정책으로 설정되며, 이는 마이그레이션 사용 사례에 권장됩니다.

Workload Factory는 다음 스토리지 시스템 간의 마이그레이션 복제를 지원합니다.

- 온프레미스 ONTAP 시스템 및 FSx for ONTAP 파일 시스템
- Cloud Volumes ONTAP 및 FSx for ONTAP 파일 시스템
- FSx for ONTAP 및 FSx for ONTAP 파일 시스템
  - 1세대에서 1세대로
  - 1세대에서 2세대로
  - 2세대에서 2세대로

스토리지 VM 데이터 및 구성 설정을 마이그레이션하려면 두 가지 작업을 완료해야 합니다.

1. [복제 관계를 생성합니다](#) 사용 사례로 \*Migration\*을 선택하고 \*Replicate storage VM configuration\*을 선택합니다.
2. [마이그레이션 사용 사례를 위한 컷오버 복제](#) 소스 파일 시스템의 데이터 및 구성 설정을 타겟 FSx for ONTAP 파일 시스템으로 영구적으로 마이그레이션합니다.

복제 관계를 생성합니다


두 FSx for ONTAP 파일 시스템 간 또는 온프레미스 ONTAP 시스템과 FSx for ONTAP 파일 시스템 간에 데이터를 복제합니다.

시작하기 전에

시작하기 전에 다음 요구 사항을 검토하십시오.

- 복제 관계에서 타겟으로 사용할 FSx for ONTAP 파일 시스템이 하나 있어야 합니다.
- 복제 관계에 사용하는 FSx for ONTAP 파일 시스템에는 연결된 링크가 있어야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크를 연결한 후, 이 작업으로 돌아오십시오.
- 온프레미스 ONTAP 시스템에서 FSx for ONTAP 파일 시스템으로 복제하려면 온프레미스 ONTAP 시스템을 검색했는지 확인하십시오.
- 볼륨 상태가 사용 가능, 생성됨 또는 잘못 구성됨 이외의 상태이거나 ONTAP 버전이 호환되지 않는 경우 복제가 지원되지 않습니다.
- 마이그레이션 사용 사례의 경우 스토리지 VM 데이터 및 구성 설정과의 복제 관계를 생성하기 전에 볼륨에 대한 마지막 복제가 지난 24시간 이내에 완료되었는지 확인하십시오.

단계

1. 중 하나를 사용하여 ["콘솔 환경"](#) 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 복제할 볼륨이 포함된 파일 시스템을 선택합니다.
5. 파일 시스템의 모든 볼륨을 복제하거나 선택한 볼륨을 복제합니다.
  - 파일 시스템의 모든 볼륨을 복제하려면 파일 시스템 개요에서 \*Replicate data \*를 선택합니다.

- 선택한 볼륨을 복제하려면 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.

Volumes 테이블에서 하나 이상의 볼륨을 선택한 다음 \* Replicate data \* 를 선택합니다.

## 6. 데이터 복제 페이지의 복제 타겟에서 다음을 제공합니다.

- 사용 사례: 복제에 대한 다음 사용 사례 중 하나를 선택하세요. 선택한 사용 사례에 따라 Workload Factory는 모범 사례에 따라 권장 값으로 양식을 채웁니다. 권장되는 값을 수락하거나 양식을 작성하면서 변경할 수 있습니다.

- 마이그레이션: 데이터를 대상 FSx for ONTAP 파일 시스템으로 전송합니다

스토리지 **VM** 구성 복제: 선택적으로 단일 스토리지 VM의 스토리지 VM 데이터 및 구성 설정을 복제하도록 선택합니다. 데이터와 구성 설정을 동시에 마이그레이션할 경우 지난 24시간 이내에 볼륨에 대한 마지막 복제가 완료되었는지 확인하십시오. 이 기능을 사용하려면 동일한 스토리지 VM에 있는 모든 볼륨을 선택해야 합니다. 모든 볼륨의 계층화 정책은 기본적으로 소스 볼륨의 계층화 정책으로 설정되며, 이는 마이그레이션 사용 사례에 권장됩니다.

- 핫 재해 복구: 중요한 워크로드에 대한고가용성 및 신속한 재해 복구를 보장합니다

- 콜드 또는 아카이브 재해 복구:

- 콜드 재해 복구: 더 긴 RTO(복구 시간 목표) 및 RPO(복구 시점 개체)를 사용하여 비용을 절감합니다
- 아카이브: 장기 스토리지 및 규정 준수를 위해 데이터 복제

- 기타

또한 사용 사례를 선택하여 복제 정책 또는 ONTAP(SnapMirror policy)를 결정합니다. 복제 정책을 설명하는 데 사용되는 용어는 에서 가져온 "[ONTAP 9 설명서](#)" 것입니다.

- 마이그레이션 및 기타 의 경우 복제 정책을 `_MirrorAllSnapshots_`라고 합니다. `_MirrorAllSnapshots_`은(는) 모든 스냅샷과 최신 활성 파일 시스템을 미러링하기 위한 비동기 정책입니다.
- 핫, 콜드 또는 아카이브 재해 복구의 경우 복제 정책을 `_MirrorAndVault_`라고 합니다. `_MirrorAndVault_`는 최신 활성 파일 시스템과 일별 및 주별 스냅샷을 미러링하기 위한 비동기 및 볼트 정책입니다.

모든 활용 사례에서 장기 보존을 위해 스냅샷을 활성화하면 기본 복제 정책은 `_MirrorAndVault_`입니다.

- \* FSx for ONTAP 파일 시스템 \*: 대상 FSx for ONTAP 파일 시스템에 대한 자격 증명, 지역 및 FSx for ONTAP 파일 시스템 이름을 선택합니다.
- \* 스토리지 VM 이름 \*: 드롭다운 메뉴에서 스토리지 VM을 선택합니다. 선택한 스토리지 VM은 이 복제 관계에서 선택한 모든 볼륨의 대상입니다.
- \* 볼륨 이름 \*: 대상 볼륨 이름은 다음 형식으로 자동으로 `{OriginalVolumeName}_copy` 생성됩니다. 자동 생성된 볼륨 이름을 사용하거나 다른 볼륨 이름을 입력할 수 있습니다.
- \* Tiering policy \*: 타겟 볼륨에 저장된 데이터에 대한 계층화 정책을 선택합니다. 계층화 정책은 기본적으로 선택한 활용 사례에 대해 권장되는 계층화 정책으로 설정됩니다.

Workload Factory 콘솔을 사용하여 볼륨을 생성할 때 기본 계층화 정책은 `_균형(자동)_`입니다. 볼륨 계층화 정책에 대한 자세한 내용은 다음을 참조하세요. "[볼륨 스토리지 용량](#)" AWS FSx for NetApp ONTAP 문서. Workload Factory는 계층화 정책에 대해 Workload Factory 콘솔에서 사용 사례 기반 이름을 사용하고 FSx



for ONTAP 계층화 정책 이름을 괄호 안에 포함합니다.

마이그레이션 사용 사례를 선택한 경우 Workload Factory는 소스 볼륨의 계층화 정책을 대상 볼륨으로 자동으로 복사합니다. 계층화 정책을 복사하려면 선택을 취소하고 복제를 위해 선택한 볼륨에 적용되는 계층화 정책을 선택합니다.

- a. \* 최대 전송 속도 \*: \* 제한 \* 을 선택하고 최대 전송 제한(MB/s)을 입력합니다 또는 \* 무제한 \* 을 선택합니다.

제한이 없으면 네트워크 및 애플리케이션 성능이 저하될 수 있습니다. 또는 중요한 워크로드(예: 재해 복구에 주로 사용되는 워크로드)에 FSx for ONTAP 파일 시스템에 대해 무제한 전송 속도를 사용하는 것이 좋습니다.

## 7. Replication settings(복제 설정) 에서 다음을 제공합니다.

- a. \* 복제 간격 \*: 소스 볼륨에서 타겟 볼륨으로 스냅샷이 전송되는 빈도를 선택합니다.
- b. 장기 보존: 장기 보존을 위해 스냅샷을 선택적으로 사용할 수 있습니다. 장기 보존을 통해 전체 사이트 장애가 발생하더라도 비즈니스 서비스를 계속 운영할 수 있으므로, 보조 복사본을 사용하여 애플리케이션을 투명하게 페일오버할 수 있습니다.

장기 보존이 없는 복제는 *MirrorAllSnapshots* 정책을 사용합니다. 장기 보존을 활성화하면 복제에 *MirrorAndVault* 정책이 할당됩니다.

장기 보존을 사용하도록 설정한 경우 기존 정책을 선택하거나 새 정책을 생성하여 복제할 스냅샷 및 유지할 스냅샷 수를 정의합니다.



장기간 보존을 위해서는 소스 및 타겟 레이블이 일치해야 합니다. 원하는 경우 워크로드 공장에서 누락된 레이블을 생성할 수 있습니다.

- \* 기존 정책 선택 \*: 드롭다운 메뉴에서 기존 정책을 선택합니다.
  - 새 정책 만들기: \*정책 이름\*을 입력하세요.
- c. 변경 불가능한 스냅샷: 선택 사항. 보존 기간 동안 이 정책에서 생성한 스냅샷이 삭제되지 않도록 하려면 \* 변경 불가능한 스냅샷 활성화 \* 를 선택합니다.
- 보존 기간 \* 을 시간, 일, 월 또는 년 수로 설정합니다.
  - \* Snapshot policies \*: 표에서 스냅샷 정책 빈도와 유지할 복제본 수를 선택합니다. 두 개 이상의 스냅샷 정책을 선택할 수 있습니다.
- d. **S3 액세스 포인트**: 선택적으로 AWS S3 API를 통해 NFS 또는 SMB/CIFS 볼륨에 있는 FSx for ONTAP 파일 시스템 데이터에 액세스하기 위해 S3 액세스 포인트를 연결합니다. 파일 접근 유형만 지원됩니다. 다음 세부 정보를 제공합니다.
- **S3 액세스 포인트 이름**: S3 액세스 포인트의 이름을 입력하세요.
  - 사용자: 볼륨에 액세스할 수 있는 기존 사용자를 선택하거나 새 사용자를 만듭니다.
  - 사용자 유형: 사용자 유형으로 **UNIX** 또는 \*Windows\*를 선택합니다.
  - 네트워크 구성: 인터넷 또는 \*Virtual private cloud (VPC)\*를 선택하십시오. 선택한 네트워크 유형에 따라 액세스 포인트가 인터넷에서 접근 가능한지 또는 특정 VPC로 제한되는지가 결정됩니다.
  - 메타데이터 활성화: 메타데이터를 활성화하면 S3 액세스 포인트에서 액세스할 수 있는 모든 객체가 포함된 S3 테이블이 생성되며, 이를 감사, 거버넌스, 자동화, 분석 및 최적화에 사용할 수 있습니다. 메타데이터를 활성화하면 추가 AWS 비용이 발생합니다. 자세한 내용은 "[Amazon S3 가격 책정 문서](#)"(를) 참조하십시오.
- e. **S3 액세스 포인트 태그**: 선택적으로 최대 50개의 태그를 추가할 수 있습니다.

## 8. Create \* 를 선택합니다.

### 결과

복제 관계는 대상 FSx for ONTAP 파일 시스템의 \* 복제 관계 \* 탭에 표시됩니다.

마이그레이션을 위해 복제 관계를 생성한 경우 스토리지 VM 데이터 및 구성 설정을 타겟 FSx for ONTAP 파일 시스템으로 마이그레이션하려면 모든 볼륨과 해당 스토리지 VM을 컷오버해야 합니다.

### 마이그레이션 사용 사례를 위한 컷오버 복제


마이그레이션 사용 사례를 위한 복제 관계를 생성한 후에는 스토리지 VM 데이터 및 구성 설정을 타겟 FSx for ONTAP 파일 시스템으로 마이그레이션하려면 컷오버 복제를 수행해야 합니다. 컷오버 복제는 소스 파일 시스템에서 타겟 FSx for ONTAP 파일 시스템으로 데이터 및 스토리지 VM 구성 설정을 영구적으로 마이그레이션합니다. 컷오버 과정에서 데이터는 마지막으로 복제됩니다. 시스템은 컷오버가 완료되면 소스 볼륨을 삭제합니다. 이 작업은 되돌릴 수 없습니다.

### 시작하기 전에

시작하기 전에 다음 요구 사항을 검토하십시오.

- 복제를 전환하기 전에 스토리지 VM에 대한 모든 클라이언트 액세스를 중지하십시오.
- 복제를 전환하기 전에 모든 소스 볼륨에서 데이터가 제공되지 않는지 확인하십시오.
- 복제 전환을 수행하기 전에 소스 볼륨과 타겟 볼륨 간의 데이터 동기화가 완료되었는지 확인하십시오.
- 복제 관계에 사용하는 FSx for ONTAP 파일 시스템에는 연결된 링크가 있어야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크를 연결한 후, 이 작업으로 돌아오십시오.

### 단계

1. 중 하나를 사용하여 ["콘솔 환경"](#) 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 복제할 볼륨이 포함된 파일 시스템을 선택합니다.
5. 복제 관계 탭을 선택합니다.
6. 복제 관계 테이블에서 전환할 복제 관계를 선택한 다음 \*복제 전환\*을 선택합니다.
7. Cut over replication 대화 상자의 정보를 검토한 다음 \_cut over\_를 입력하여 확인합니다.
8. \*Cut over\*를 선택하세요.

### 결과

전환이 완료되면 소스 볼륨이 삭제되고 타겟 볼륨은 읽기/쓰기 가능 상태가 됩니다. 전환 후 타겟 볼륨에 대해 ["계층화 정책을 수정합니다"](#)할 수 있습니다.

### NetApp Workload Factory에서 복제 관계 초기화

NetApp Workload Factory의 스냅샷과 모든 데이터 블록을 전송하기 위해 소스 볼륨과 대상 볼륨 간의 복제 관계를 초기화합니다.


### 이 작업에 대해

초기화는 소스 볼륨의 스냅샷을 만든 다음 해당 스냅샷과 해당 스냅샷이 참조하는 모든 데이터 블록을 타겟 볼륨으로 전송합니다.

시작하기 전에

이 작업을 완료하도록 선택할 때를 고려하십시오. 초기화에는 시간이 오래 걸릴 수 있습니다. 사용량이 적은 시간에 기준 전송을 실행할 수 있습니다.

단계

1. 중 하나를 사용하여 "콘솔 환경"로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 업데이트할 파일 시스템의 작업 메뉴를 선택한 다음 \*관리\*를 선택합니다.
5. 파일 시스템 개요에서 \*복제 관계\* 탭을 선택합니다.
6. 복제 관계 탭에서 초기화할 복제 관계의 작업 메뉴를 선택합니다.
7. Initialize \* 를 선택합니다.
8. 관계 초기화 대화 상자에서 \* 초기화 \* 를 선택합니다.

## AI를 활용한 NetApp 자율형 랜섬웨어 보호로 데이터를 보호하세요

AI(ARP/AI)를 탑재한 NetApp Autonomous Ransomware Protection으로 데이터를 보호하세요. 이 기능은 NAS(NFS/SMB) 환경에서 워크로드 분석을 사용하여 랜섬웨어 공격일 수 있는 비정상적인 활동을 감지하고 경고합니다. 공격이 의심되는 경우 ARP/AI는 데이터를 복원할 수 있는 변경 불가능한 새로운 스냅샷을 생성합니다.

이 작업에 대해

ARP/AI를 사용하여 공격자가 몸값을 지불할 때까지 데이터를 숨기는 서비스 거부 공격으로부터 보호합니다. ARP/AI는 다음을 기반으로 실시간 랜섬웨어 감지 기능을 제공합니다.

- 들어오는 데이터를 암호화된 데이터 또는 일반 텍스트로 식별합니다.
- 다음을 감지하는 분석:
  - **Entropy**: 파일에 있는 데이터의 임의 정도를 평가합니다
  - 파일 확장명 형식: 일반 확장명 형식에 맞지 않는 확장자입니다
  - 파일 **IOPS**: 데이터 암호화를 통한 비정상적인 볼륨 활동의 급증

ARP/AI는 소수의 파일만 암호화된 후 대부분의 랜섬웨어 공격이 확산되는 것을 감지하고, 자동으로 조치를 취해 데이터를 보호하며, 의심되는 공격이 발생했을 때 경고를 보냅니다.

ARP/AI 기능은 Amazon FSx for NetApp ONTAP 에서 실행되는 ONTAP 버전에 따라 자동으로 업데이트되므로 수동으로 업데이트할 필요가 없습니다.

학습 및 활성화 모드

ARP/AI는 먼저 \_학습 모드\_에서 작동한 후 자동으로 \_활성 모드\_로 전환됩니다.

- 학습 모드: ARP/AI를 활성화하면 \_학습 모드\_로 실행됩니다. 학습 모드에서 FSx for ONTAP 파일 시스템은

엔트로피, 파일 확장자 유형, 파일 IOPS 등의 분석 영역을 기반으로 알림 프로필을 개발합니다. 파일 시스템이 워크로드 특성을 평가하기에 충분한 시간 동안 ARP/AI를 학습 모드로 실행한 후, Workload Factory는 자동으로 ARP/AI를 **\_활성 모드\_**로 전환하고 데이터 보호를 시작합니다.

- **활성 모드:** ARP/AI가 **\_활성 모드\_**로 전환된 후, FSx for ONTAP은 위협이 감지되면 데이터를 보호하기 위해 ARP/AI 스냅샷을 생성합니다.

활성 모드에서 파일 확장자가 비정상적으로 플래그되는 경우 경고를 평가해야 합니다. 경고를 통해 데이터를 보호하거나 경고를 거짓 긍정으로 표시할 수 있습니다. 경고를 false positive로 표시하면 경고 프로필이 업데이트됩니다. 예를 들어, 새 파일 확장자에 의해 경고가 트리거되고 이 경고를 false positive로 표시하면 다음에 파일 확장명이 관찰될 때 알림이 수신되지 않습니다.

블록 장치를 포함하는 FlexVol 볼륨은 ARP/AI를 활성 모드로 시작합니다.

지원되지 않는 구성입니다

다음 구성은 ARP/AI 사용을 지원하지 않습니다.

- iSCSI 볼륨
- NVMe 볼륨

파일 시스템 또는 볼륨에 대해 **ARP/AI** 활성화

파일 시스템에 ARP/AI를 활성화하면 모든 기존 NAS와 새로 생성된 NAS(NFS/SMB) 볼륨에 대한 보호가 자동으로 추가됩니다. 개별 볼륨에 대해 ARP/AI를 활성화할 수도 있습니다.


ARP/AI를 활성화한 후 공격이 발생하고 공격이 실제라고 확인되면 Workload Factory는 4시간마다 최대 6개의 스냅샷을 생성하는 스냅샷 정책을 자동으로 설정합니다. 각 스냅샷은 2~5일 동안 잠금됩니다.

시작하기 전에

파일 시스템이나 볼륨에 대해 ARP/AI를 활성화하려면 링크를 연결해야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#) 링크가 연결되면 이 작업으로 돌아갑니다.


## 파일 시스템에 **ARP/AI** 활성화

### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 파일 시스템의 작업 메뉴를 선택하여 ARP/AI를 활성화한 다음 \*관리\*를 선택합니다.
5. 정보에서 자율 랜섬웨어 보호 옆에 있는 연필 아이콘을 선택하세요. 마우스를 자율 랜섬웨어 보호 행 위에 올려놓으면 화살표 옆에 연필 아이콘이 나타납니다.
6. AI(ARP/AI)를 통한 NetApp 자율형 랜섬웨어 보호 페이지에서 다음을 수행합니다.
  - a. 기능을 활성화하거나 비활성화합니다.
  - b. 자동 스냅샷 생성: 보관할 스냅샷의 최대 개수와 스냅샷을 찍는 간격을 선택합니다. 기본값은 4시간마다 6개의 스냅샷을 찍는 것입니다.
  - c. 변경 불가능한 스냅샷: 기본 보존 기간(시간)과 변경 불가능한 스냅샷을 보존할 최대 일수를 선택합니다. 이 옵션을 활성화하면 지정된 보존 기간이 끝날 때까지 스냅샷을 삭제하거나 수정할 수 없습니다.
  - d. 탐지: 선택적으로 다음 매개변수 중 하나를 선택하여 자동으로 이상을 스캔하고 감지합니다.
7. 계속하려면 설명을 수락하십시오.
8. 적용 \* 을 선택하여 변경 사항을 저장합니다.

## 볼륨에 대해 **ARP/AI** 활성화


### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 파일 시스템의 작업 메뉴를 선택하여 ARP/AI를 활성화한 다음 \*관리\*를 선택합니다.
5. 볼륨 탭에서 볼륨의 작업 메뉴를 선택하여 ARP/AI를 활성화한 다음, \*데이터 보호 작업\*을 선택하고, \*ARP/AI 관리\*를 선택합니다.
6. ARP/AI 관리 대화 상자에서 다음을 수행합니다.
  - a. 기능을 활성화하거나 비활성화합니다.
  - b. 탐지: 선택적으로 다음 매개변수 중 하나를 선택하여 자동으로 이상을 스캔하고 감지합니다.
7. 계속하려면 설명을 수락하십시오.
8. 적용 \* 을 선택하여 변경 사항을 저장합니다.

## 랜섬웨어 공격을 검증합니다

공격이 거짓 경보 또는 진정한 랜섬웨어 사고인지 확인합니다.

### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 랜섬웨어 공격을 검증할 파일 시스템을 선택합니다.
5. 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.
6. Autonomous Ransomware Protection 타일에서 \* Analyze Attacks \* 를 선택합니다.
7. 공격 이벤트 보고서를 다운로드하여 손상된 파일이나 폴더가 있는지 검토한 다음 공격이 발생했는지 여부를 결정합니다.
8. 공격이 발생하지 않은 경우 표의 볼륨에 대해 \* False alarm \* 을 선택한 다음 \* Close \* 를 선택합니다
9. 공격이 발생한 경우 표의 볼륨에 대해 \* Real attack \* 을 선택합니다. 손상된 볼륨 데이터 복원 대화 상자가 열립니다. 즉시 로 진행하거나 \* Close \* 를 선택하고 나중에 복구 프로세스를 완료할 수 [데이터를 복구합니다](#)있습니다.


#### 랜섬웨어 공격 후 데이터 복구

공격이 의심되면 시스템은 해당 시점의 볼륨 스냅샷을 찍고 해당 복사본을 잠급니다. 나중에 공격이 확인되면 ARP/AI 스냅샷을 사용하여 영향을 받은 파일이나 전체 볼륨을 복원할 수 있습니다.

잠긴 스냅샷은 보존 기간이 끝날 때까지 삭제할 수 없습니다. 그러나 나중에 이 공격을 가양성 공격으로 표시하기로 결정하면 잠긴 복사본이 삭제됩니다.

영향을 받는 파일과 공격 시간을 알면 전체 볼륨을 스냅샷 중 하나로 되돌리는 대신 다양한 스냅샷에서 영향을 받는 파일을 선택적으로 복구할 수 있습니다.

#### 단계

1. 중 하나를 사용하여 "콘솔 환경"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*FSx for ONTAP\*를 선택합니다.
4. \*FSx for ONTAP\*에서 데이터를 복구할 파일 시스템을 선택합니다.
5. 파일 시스템 개요에서 \* Volumes \* 탭을 선택합니다.
6. Autonomous Ransomware Protection 타일에서 \* Analyze Attacks \* 를 선택합니다.
7. 공격이 발생한 경우 표의 볼륨에 대해 \* Real attack \* 을 선택합니다.
8. 손상된 볼륨 데이터 복원 대화 상자에서 지침에 따라 파일 수준 또는 볼륨 수준에서 복원합니다. 대부분의 경우 전체 볼륨이 아닌 파일을 복원합니다.
9. 복원을 완료한 후 \* 닫기 \* 를 선택합니다.

#### 결과

손상된 데이터가 복원되었습니다.

## NetApp Workload Factory에서 볼륨 복제

테스트를 위해 NetApp Workload Factory에서 볼륨을 복제하여 원래 볼륨의 읽기/쓰기 볼륨을 만듭니다.

클론은 데이터의 현재 시점 상태를 반영합니다. 또한 클론을 사용하면 운영 데이터에 대한 액세스 권한을 부여하지 않고 추가 사용자에게 데이터에 대한 액세스 권한을 부여할 수 있습니다.


이 작업에 대해

볼륨 클로닝은 FlexClone 볼륨에만 지원됩니다.

볼륨의 클론이 생성되면 상위 볼륨의 스냅샷을 참조하여 쓰기 가능한 볼륨이 생성됩니다. 클론은 몇 초 내에 생성됩니다. 클론 복제된 데이터는 볼륨 클론에 상주하지 않고 상위 볼륨에 상주합니다. 클론 생성 후 볼륨에 기록되는 모든 새 데이터는 클론에 상주합니다.

복제된 볼륨에 상위 볼륨의 모든 데이터와 생성 후 클론에 추가된 새 데이터가 포함되도록 하려면 상위 볼륨에서 이 작업을 수행해야 **"클론을 분할합니다"** 합니다. 또한 상위 볼륨에 클론이 있는 경우 해당 볼륨을 삭제할 수 없습니다. 상위 볼륨을 삭제하려면 먼저 클론을 분할해야 합니다.

단계

1. 중 하나를 사용하여 **"콘솔 환경"** 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 **\*저장소\***를 선택하세요.
3. 저장소 메뉴에서 **\*FSx for ONTAP\***를 선택합니다.
4. **\*FSx for ONTAP\***에서 복제할 볼륨이 포함된 FSx for ONTAP 파일 시스템의 작업 메뉴를 선택한 다음 **\*관리\***를 선택합니다.
5. 파일 시스템의 개요 탭에서 **\* Volumes \*** 탭을 선택합니다.
6. 볼륨 탭에서 복제할 볼륨의 작업 메뉴를 선택합니다.
7. Data protection actions \* 를 선택한 다음 **\* Clone volume \*** 을 선택합니다.
8. 클론 볼륨 대화 상자에서 볼륨 클론의 이름을 입력합니다.
9. 클론 \* 을 선택합니다.

## NetApp Workload Factory에서 온프레미스 ONTAP 클러스터 데이터 사용

NetApp Workload Factory에서 온프레미스 ONTAP 데이터를 검색하고 복제하여 AI 지식 기반을 강화하는 데 사용할 수 있습니다.

이 작업에 대해

온프레미스 ONTAP 클러스터의 데이터를 사용하려면 먼저 온프레미스 ONTAP 클러스터를 검색해야 합니다. 온프레미스 ONTAP 클러스터를 검색한 후에는 다음 사용 사례에 해당 데이터를 사용할 수 있습니다.

사용 사례

GenAI 워크로드의 주요 사용 사례는 이 일련의 작업에 중점을 두고 있습니다.

- **\* GenAI 워크로드 \*:** 온프레미스-ONTAP 볼륨 데이터를 FSx for ONTAP 파일 시스템에 복제하여 데이터를 사용할 수 **"AI 지식 기반을 보강합니다"** 있습니다.

- \* 클라우드로 백업 및 마이그레이션 \*: 온프레미스 ONTAP 볼륨 데이터를 FSx for ONTAP 파일 시스템으로 복제하는 경우 클라우드에서 백업으로 사용할 수 있습니다.
- \* 데이터 계층화 \*: 복제 후 드물게 액세스되는 온프레미스 ONTAP 볼륨 데이터를 SSD 스토리지 계층에서 용량 풀 스토리지 계층으로 계층화할 수 있습니다.

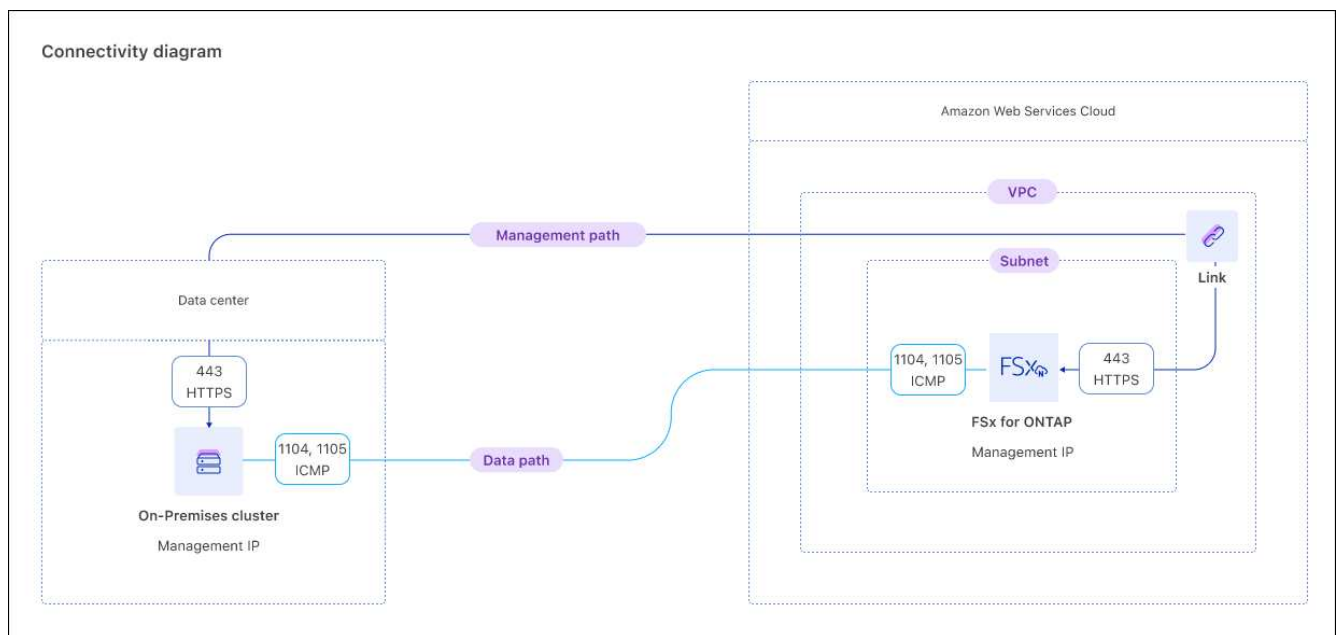
사내 **ONTAP** 클러스터를 검색합니다

NetApp Workload Factory에서 온프레미스 ONTAP 클러스터를 검색하여 Amazon FSx for NetApp ONTAP 파일 시스템에 데이터를 복제할 수 있습니다.


시작하기 전에

시작하기 전에 다음 사항이 있는지 확인하십시오.

- 복제용 FSx for ONTAP 파일 시스템
- 검색된 온-프레미스 클러스터와 연결할 연결된 링크 링크가 없는 경우 이 작업을 수행해야 **"새로 만듭니다"**합니다.
- 필요한 권한이 있는 ONTAP 사용자 자격 증명입니다.
- 온프레미스 ONTAP 버전 9.8 이상
- 다음 다이어그램에 표시된 연결.



단계

1. 중 하나를 사용하여 **"콘솔 환경"**로 로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 온-프레미스 ONTAP \* 탭을 선택합니다.
4. Discover \* 를 선택합니다.
5. 필수 구성 요소를 검토하고 \* Next \* 를 선택합니다.
6. ONTAP 온프레미스 검색 페이지의 \* 클러스터 구성 \* 에 다음을 제공합니다.



- a. 링크: 링크를 선택하세요. 이 링크는 온프레미스 클러스터와 연결되어 클러스터와 Workload Factory 간의 연결을 생성합니다.

링크를 만들지 않은 경우 지침에 따라 이 작업으로 돌아가서 링크를 선택합니다.

- b. \* 클러스터 IP 주소 \*: 복제할 온-프레미스 ONTAP 클러스터의 IP 주소를 제공합니다.
- c. \* ONTAP credentials \*: 온-프레미스 ONTAP 클러스터의 ONTAP 자격 증명을 입력합니다. 사용자에게 필요한 권한이 있는지 확인합니다.

7. 검색 프로세스를 시작하려면 \* 검색 \* 을 선택합니다.

## 결과

온프레미스 ONTAP 클러스터가 검색되어 \* 온프레미스 ONTAP \* 탭에 표시됩니다.

이제 온프레미스 ONTAP 클러스터와 의 데이터를 볼 수 있습니다.[데이터를 FSx for ONTAP 파일 시스템에 복제합니다](#)


온프레미스 **ONTAP** 클러스터에서 볼륨 데이터를 복제합니다

온프레미스 ONTAP 클러스터의 볼륨 데이터를 FSx for ONTAP 파일 시스템으로 복제합니다. 복제 후에는 데이터를 사용하여 AI 지식 기반을 강화할 수 있습니다.

## 시작하기 전에

- 볼륨 데이터를 복제하려면 온프레미스 ONTAP 클러스터를 검색해야 합니다.
- 복제 대상으로 사용할 수 있는 FSx for ONTAP 파일 시스템이 있어야 합니다.
- 온프레미스 ONTAP 클러스터와 복제 관계에 사용하는 FSx for ONTAP 파일 시스템 모두에 연결된 링크가 있어야 합니다. ["기존 링크를 연결하는 방법이나 새 링크를 만들고 연결하는 방법을 알아보세요."](#).. 링크가 연결되면 이 작업으로 돌아갑니다.

## 단계

1. 중 하나를 사용하여 ["콘솔 환경"](#)로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.
3. 저장소 메뉴에서 \*온프레미스 ONTAP\*을 선택합니다.
4. 스토리지 VM별로 볼륨을 찾으려면 드롭다운에서 \* 스토리지 VM \* 을 선택합니다.
5. 복제할 볼륨을 하나 이상 선택한 다음 \* Replicate \* 를 선택합니다.
6. 복제 생성 페이지의 복제 타겟에서 다음을 제공합니다.
  - a. \* FSx for ONTAP 파일 시스템 \*: 대상 FSx for ONTAP 파일 시스템에 대한 자격 증명, 지역 및 FSx for ONTAP 파일 시스템 이름을 선택합니다.
  - b. \* 스토리지 VM 이름 \*: 드롭다운 메뉴에서 스토리지 VM을 선택합니다.
  - c. \* 볼륨 이름 \*: 대상 볼륨 이름은 다음 형식으로 자동으로 `{OriginalVolumeName}\_copy` 생성됩니다. 자동 생성된 볼륨 이름을 사용하거나 다른 볼륨 이름을 입력할 수 있습니다.
  - d. \* 데이터 계층화 \*: 타겟 볼륨에 저장된 데이터에 대한 계층화 정책을 선택합니다.
    - 자동: Workload Factory FSx for ONTAP 사용자 인터페이스를 사용하여 볼륨을 생성할 때의 기본 계층화 정책입니다. 사용자 데이터와 스냅샷을 포함한 모든 쿨드 데이터를 특정 기간 동안의 용량 풀 스토리지 계층으로 계층화합니다.

- \* 스냅샷 전용 \*: 스냅샷 데이터만 용량 풀 스토리지 계층에 계층화합니다.
- \* 없음 \*: 모든 볼륨의 데이터를 기본 스토리지 계층에 보관합니다.
- \* ALL \*: 모든 사용자 데이터와 스냅샷 데이터를 콜드 데이터로 표시하고 용량 풀 스토리지 계층에 저장합니다.

일부 계층화 정책에는 볼륨의 사용자 데이터가 "콜드"로 간주되고 용량 풀 스토리지 계층으로 이동하려면 볼륨의 사용자 데이터가 비활성 상태로 유지되어야 하는 시간을 설정하는 관련 최소 냉각 기간 또는 *cooling days* 이 있습니다. 냉각 기간은 데이터가 디스크에 기록될 때 시작됩니다.

볼륨 계층화 정책에 대한 자세한 내용은 AWS FSx for NetApp ONTAP 설명서 를 "[볼륨 스토리지 용량](#)" 참조하십시오.

- a. \* 최대 전송 속도 \*: \* 제한 \* 을 선택하고 MiB/s 단위의 최대 전송 한도를 입력하십시오 또는 \* 무제한 \* 을 선택합니다.

제한이 없으면 네트워크 및 애플리케이션 성능이 저하될 수 있습니다. 또는 중요한 워크로드(예: 재해 복구에 주로 사용되는 워크로드)에 FSx for ONTAP 파일 시스템에 대해 무제한 전송 속도를 사용하는 것이 좋습니다.

## 7. Replication settings(복제 설정) 에서 다음을 제공합니다.

- a. \* 복제 간격 \*: 소스 볼륨에서 타겟 볼륨으로 스냅샷이 전송되는 빈도를 선택합니다.
- b. 장기 보존: 장기 보존을 위해 스냅샷을 선택적으로 사용할 수 있습니다.

장기 보존을 사용하도록 설정한 경우 기존 정책을 선택하거나 새 정책을 생성하여 복제할 스냅샷 및 유지할 스냅샷 수를 정의합니다.

- 기존 정책의 경우 \* 기존 정책 선택 \* 을 선택한 다음 드롭다운 메뉴에서 기존 정책을 선택합니다.
- 새 정책의 경우 \* 새 정책 생성 \* 을 선택하고 다음을 제공합니다.
  - \* 정책 이름 \*: 정책 이름을 입력하십시오.
  - \* Snapshot policies \*: 표에서 스냅샷 정책 빈도와 유지할 복제본 수를 선택합니다. 두 개 이상의 스냅샷 정책을 선택할 수 있습니다.

## 8. Create \* 를 선택합니다.

결과

복제 관계는 대상 FSx for ONTAP 파일 시스템의 \* 복제 관계 \* 탭에 표시됩니다.


## NetApp Workload Factory에서 온프레미스 ONTAP 클러스터 제거

필요한 경우 NetApp Workload Factory에서 온프레미스 ONTAP 클러스터를 제거합니다.

시작하기 전에

온-프레미스 ONTAP 클러스터의 모든 볼륨을 선택한 후 클러스터를 제거해야 "[기존 복제 관계를 모두 삭제합니다](#)" 분리된 관계가 남아 있지 않습니다.

단계

1. 중 하나를 사용하여 "[콘솔 환경](#)"로그인합니다.
2. 메뉴를 선택하세요  그런 다음 \*저장소\*를 선택하세요.

3. 저장소 메뉴에서 \*온프레미스 ONTAP\*을 선택합니다.
4. 제거할 온프레미스 ONTAP 클러스터를 선택합니다.
5. 작업 메뉴를 선택하고 \*Workload Factory에서 제거\*를 선택합니다.

#### 결과

온프레미스 ONTAP 클러스터가 NetApp Workload Factory에서 제거되었습니다.

## 사이버 볼트로 데이터를 보호하세요

사이버 볼트 볼륨은 데이터의 백업 사본을 저장하는 데 사용되는 격리된 안전한 저장 위치로, 랜섬웨어 공격 및 기타 사이버 위협으로부터 데이터를 보호합니다. 볼트 생성의 일부로 사이버 볼트 볼륨을 생성하고, 모든 클라이언트 프로토콜을 비활성화하고, 소스 볼륨과 사이버 볼트 볼륨 간의 복제 관계를 설정하고, 사이버 볼트 볼륨에 변경 불가능한 스냅샷을 생성합니다.

#### 사이버 볼트란 무엇인가요?

사이버 볼트는 주요 IT 인프라와 분리된 격리된 환경에 중요한 데이터를 저장하는 특정 데이터 보호 기술입니다.

사이버 볼트는 악성 소프트웨어, 랜섬웨어 또는 내부 위협 등 주요 네트워크에 영향을 미치는 위협으로부터 면역이 있는 "공기 차단" 방식의 변경 불가능하고 삭제 불가능한 데이터 저장소입니다. 변경 불가능하고 지울 수 없는 스냅샷을 통해 사이버 볼트를 구현할 수 있습니다.

기존 방식을 사용하는 에어 갭 백업에는 공간을 만들고 1차 및 2차 미디어를 물리적으로 분리하는 작업이 포함됩니다. 미디어를 다른 곳으로 옮기거나 연결을 끊으면 악의적인 행위자가 데이터에 액세스할 수 없습니다. 이렇게 하면 데이터는 보호되지만 복구 시간이 더 느려질 수 있습니다.

#### ONTAP 사이버 볼트용 FSx

Amazon FSx for NetApp ONTAP 사이버 볼트 소스 및 대상으로 지원됩니다.

#### 구현

Workload Factory는 사이버 볼트 아키텍처를 만드는 데 도움을 제공합니다. NetApp 에 연락하여 사이버 볼트 구현에 대한 관심을 표명하면 NetApp 전문가가 연락하여 요구 사항에 대해 논의합니다.

시작하려면 [ng-FSx-CyberVault@netapp.com](mailto:ng-FSx-CyberVault@netapp.com)으로 이메일을 보내세요.

#### 관련 정보

사이버 볼트와 이 아키텍처를 설정하는 방법에 대한 자세한 내용은 다음을 참조하세요. ["ONTAP 사이버 볼트 문서"](#).

## 저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

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

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

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

## 상표 정보

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