



# ONTAP용 Amazon FSx 문서

## Amazon FSx for ONTAP

NetApp  
April 01, 2022

# 목차

ONTAP용 Amazon FSx 문서	1
ONTAP용 Amazon FSx의 새로운 기능	2
2022년 2월 27일	2
2021년 10월 31일	2
2021년 10월 4일	2
2021년 9월 2일	2
시작하십시오	4
ONTAP용 Amazon FSx에 대해 자세히 알아보십시오	4
ONTAP용 Amazon FSx를 시작하십시오	5
요구 사항	6
ONTAP용 FSx에 대한 권한을 설정합니다	6
ONTAP용 FSx에 대한 보안 그룹 규칙입니다	7
ONTAP에 Amazon FSx를 사용합니다	14
ONTAP 작업 환경을 위한 Amazon FSx를 생성하고 관리합니다	14
ONTAP용 Amazon FSx의 볼륨을 생성합니다	22
ONTAP용 Amazon FSx의 볼륨을 관리합니다	27
지식 및 지원	29
지원을 위해 등록하십시오	29
도움을 받으십시오	29
법적 고지	30

# ONTAP용 Amazon FSx 문서

# ONTAP용 Amazon FSx의 새로운 기능

ONTAP용 Amazon FSx의 새로운 기능에 대해 알아보십시오.

## 2022년 2월 27일

### IAM 역할을 가정합니다

ONTAP 작업 환경을 위한 FSx를 생성할 때 이제 Cloud Manager가 ONTAP 작업 환경을 위한 FSx를 생성할 것으로 가정할 수 있는 IAM 역할의 ARN을 제공해야 합니다. 이전에는 AWS 액세스 키를 제공해야 했습니다.

["ONTAP용 FSx에 대한 사용 권한을 설정하는 방법에 대해 알아보십시오."](#)

## 2021년 10월 31일

### Cloud Manager API를 사용하여 iSCSI 볼륨을 생성합니다

ONTAP용 FSx용 iSCSI 볼륨은 Cloud Manager API를 사용하여 생성하고 작업 환경에서 관리할 수 있습니다.

### 볼륨을 생성할 때 볼륨 단위를 선택합니다

가능합니다 ["볼륨을 생성할 때 볼륨 단위\(GiB 또는 TiB\)를 선택합니다"](#) FSx for ONTAP에서

## 2021년 10월 4일

### Cloud Manager를 사용하여 CIFS 볼륨을 생성합니다

이제 가능합니다 ["Cloud Manager를 사용하여 ONTAP용 FSx에서 CIFS 볼륨을 생성합니다"](#).

### Cloud Manager를 사용하여 볼륨을 편집합니다

이제 가능합니다 ["Cloud Manager를 사용하여 ONTAP 볼륨의 FSx를 편집합니다"](#).

## 2021년 9월 2일

### ONTAP용 Amazon FSx 지원

- ["ONTAP용 Amazon FSx"](#) 는 고객이 NetApp의 ONTAP 스토리지 운영 체제가 제공하는 파일 시스템을 실행하고 실행할 수 있도록 하는 완전 관리형 서비스입니다. ONTAP용 FSx는 NetApp 고객이 사내에서 사용하는 것과 동일한 기능, 성능 및 관리 기능을 기본 AWS 서비스의 단순성, 민첩성, 보안 및 확장성으로 제공합니다.

["ONTAP용 Amazon FSx에 대해 자세히 알아보십시오."](#)

- Cloud Manager에서 ONTAP 작업 환경에 대한 FSx를 구성할 수 있습니다.

["ONTAP 작업 환경을 위한 Amazon FSx를 생성합니다"](#).

- AWS 및 Cloud Manager의 커넥터를 사용하여 볼륨을 생성 및 관리하고, 데이터를 복제하고, ONTAP용 FSx를 데이터 센스 및 Cloud Sync와 같은 NetApp 클라우드 서비스와 통합할 수 있습니다.

"ONTAP용 Amazon FSx에 대한 클라우드 데이터 센스를 시작해 보십시오".

# 시작하십시오

## ONTAP용 Amazon FSx에 대해 자세히 알아보십시오

"ONTAP용 Amazon FSx"는 고객이 NetApp의 ONTAP 스토리지 운영 체제가 제공하는 파일 시스템을 실행하고 실행할 수 있도록 하는 완전 관리형 서비스입니다. ONTAP용 FSx는 NetApp 고객이 사내에서 사용하는 것과 동일한 기능, 성능 및 관리 기능을 기본 AWS 서비스의 단순성, 민첩성, 보안 및 확장성으로 제공합니다.

### 피처

- 스토리지 디바이스, 소프트웨어 또는 백업을 구성하거나 관리할 필요가 없습니다.
- CIFS, NFSv3, NFSv4.x 및 SMB v2.0-v3.1.1 프로토콜 지원
- 자주 액세스하지 않는(IA) 스토리지 계층을 사용하여 저렴한 비용으로 사실상 제한 없는 데이터 스토리지 용량을 확보할 수 있습니다.
- Oracle RAC를 포함하여 지연 시간에 민감한 애플리케이션에서 실행되도록 인증받았습니다.
- 번들 및 용량제 가격 선택 가능

### 추가 기능은 Cloud Manager에서 제공됩니다

- AWS 및 Cloud Manager의 커넥터를 사용하여 볼륨을 생성 및 관리하고, 데이터를 복제하고, ONTAP용 FSx를 데이터 센스 및 Cloud Sync와 같은 NetApp 클라우드 서비스와 통합할 수 있습니다.
- 클라우드 데이터 센스는 인공 지능(AI) 기반 기술을 사용하여 데이터 컨텍스트를 이해하고 FSx for ONTAP 계정에 상주하는 중요한 데이터를 식별하는 데 도움을 줄 수 있습니다. ["자세한 정보"](#).
- NetApp Cloud Sync를 사용하면 클라우드 또는 사내 타겟으로 데이터 마이그레이션을 자동화할 수 있습니다. ["자세한 정보"](#)

### 비용

ONTAP용 FSx 계정은 Cloud Manager가 아니라 AWS에서 유지 관리됩니다. ["ONTAP용 Amazon FSx 시작 가이드"](#)

AWS에서 커넥터를 사용하는 것과 Cloud Sync 및 데이터 센스와 같은 선택적 데이터 서비스를 사용하는 것과 관련된 추가 비용이 있습니다.

### 지원 지역

["지원되는 아마존 지역을 봅니다."](#)

### 도움말 보기

ONTAP용 Amazon FSx는 AWS 최초의 솔루션입니다. 이 서비스를 사용하는 AWS FSx 파일 시스템, 인프라 또는 AWS 솔루션과 관련된 질문이나 기술 지원 문제가 있는 경우 AWS 콘솔의 Support Center를 사용하여 AWS에 지원 케이스를 접수하십시오. "FSx for ONTAP" 서비스와 적절한 범주를 선택합니다. AWS 지원 케이스를 생성하는 데 필요한 나머지 정보를 제공합니다.

Cloud Manager 또는 Cloud Manager 마이크로 서비스와 관련된 일반적인 질문은 인라인 Cloud Manager 채팅으로

시작할 수 있습니다.

Cloud Manager 또는 내의 마이크로 서비스와 관련된 기술 지원 문제의 경우 Cloud Manager 계정 레벨 일련 번호를 사용하여 NetApp 지원 티켓을 열 수 있습니다. 지원을 활성화하려면 Cloud Manager 일련 번호를 등록해야 합니다.

## 제한 사항

- Cloud Manager는 온프레미스 또는 Cloud Volumes ONTAP에서 ONTAP용 FSx로 데이터를 복제할 수 있습니다.
- 이때 ONTAP CLI, ONTAP API 또는 Cloud Manager API를 사용하여 iSCSI 볼륨을 생성할 수 있습니다.

## ONTAP용 Amazon FSx를 시작하십시오

몇 가지 단계를 통해 ONTAP용 Amazon FSx를 시작해 보십시오.

몇 단계만 거치면 ONTAP용 FSx를 시작할 수 있습니다.

볼륨을 추가하기 전에 ONTAP 작업 환경을 위한 Amazon FSx를 생성해야 합니다. 이 작업을 수행해야 합니다 ["Cloud Manager SaaS가 역할을 맡을 수 있도록 IAM 역할을 설정합니다"](#).

가 있어야 합니다 ["AWS용 커넥터"](#) ONTAP 작업 환경을 위한 FSx를 열려면 볼륨을 생성하거나 다른 작업을 수행합니다. Connector가 필요한 경우 Cloud Manager에서 아직 추가되지 않은 경우 이를 묻습니다.

Cloud Manager를 사용하여 ONTAP 볼륨용 FSx를 생성할 수 있습니다.

Cloud Manager를 사용하여 볼륨을 관리하고 복제, Cloud Sync, 데이터 센스와 같은 추가 서비스를 구성합니다.

### 관련 링크

- ["Cloud Manager에서 커넥터 생성"](#)
- ["AWS Marketplace에서 커넥터 실행"](#)
- ["Linux 호스트에 Connector 소프트웨어 설치"](#)

# 요구 사항

## ONTAP용 FSx에 대한 권한을 설정합니다

ONTAP 작업 환경을 위한 Amazon FSx를 생성 또는 관리하려면 Cloud Manager에 ONTAP 작업 환경을 위한 FSx를 생성하는 데 필요한 권한을 제공하는 IAM 역할의 ARN을 제공하여 AWS 자격 증명을 Cloud Manager에 추가해야 합니다.

### IAM 역할을 설정합니다

Cloud Manager SaaS가 역할을 맡을 수 있도록 IAM 역할을 설정합니다.

단계

1. 대상 계정에서 IAM 콘솔로 이동합니다.
2. 액세스 관리에서 \* 역할 > 역할 만들기 \* 를 클릭하고 단계를 따라 역할을 만듭니다.

다음을 수행하십시오.

- 신뢰할 수 있는 엔터티 유형 \* 에서 \* AWS 계정 \* 을 선택합니다.
- 다른 AWS 계정 \* 을 선택하고 Cloud Manager SaaS:952013314444의 ID를 입력합니다
- 다음 권한이 포함된 정책을 만듭니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "VisualEditor0",
      "Effect": "Allow",
      "Action": [
        "fsx:*",
        "ec2:Describe*",
        "ec2:CreateTags",
        "kms:Describe*",
        "kms:List*",
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*"
    }
  ]
}
```

3. 다음 단계에서 Cloud Manager에 붙여넣을 수 있도록 IAM 역할의 역할 ARN을 복사합니다.

이제 IAM 역할에 필요한 권한이 있습니다.



## 자격 증명을 추가합니다

필요한 권한을 IAM 역할에 제공한 후 ARN 역할을 Cloud Manager에 추가합니다.

방금 IAM 역할을 생성한 경우 사용할 수 있을 때까지 몇 분 정도 걸릴 수 있습니다. 몇 분 후에 Cloud Manager에 자격 증명을 추가합니다.

단계

1. Cloud Manager 콘솔의 오른쪽 위에서 설정 아이콘을 클릭하고 \* 자격 증명 \* 을 선택합니다.



2. 자격 증명 추가 \* 를 클릭하고 마법사의 단계를 따릅니다.
  - a. \* 자격 증명 위치 \*: \* Amazon Web Services > Cloud Manager \* 를 선택합니다.
  - b. \* 자격 증명 정의 \*: IAM 역할의 ARN(Amazon Resource Name)을 제공합니다.
  - c. \* 검토 \*: 새 자격 증명에 대한 세부 정보를 확인하고 \* 추가 \* 를 클릭합니다.

이제 ONTAP 작업 환경에 대한 FSx를 생성할 때 자격 증명을 사용할 수 있습니다.

## 관련 링크

- ["AWS 자격 증명 및 권한"](#)
- ["Cloud Manager의 AWS 자격 증명 관리"](#)

## ONTAP용 FSx에 대한 보안 그룹 규칙입니다

Cloud Manager는 Cloud Manager 및 FSx for ONTAP가 성공적으로 운영하는 데 필요한 인바운드 및 아웃바운드 규칙을 포함하는 AWS 보안 그룹을 생성합니다. 테스트 목적으로 또는 자체 포트를 사용해야 하는 경우 포트를 참조할 수 있습니다.

### ONTAP의 FSx 규칙

ONTAP용 FSx 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

#### 인바운드 규칙

미리 정의된 보안 그룹의 인바운드 규칙 소스는 0.0.0.0/0입니다.

프로토콜	포트	목적
모든 ICMP	모두	인스턴스에 Ping을 수행 중입니다
HTTP	80	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTP 액세스
HTTPS	443	클러스터 관리 LIF의 IP 주소를 사용하여 System Manager 웹 콘솔에 대한 HTTPS 액세스

프로토콜	포트	목적
SSH를 클릭합니 다	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 SSH를 액세스할 수 있습니다
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션입니다
TCP	161-162	단순한 네트워크 관리 프로토콜
TCP	445	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049	NFS 서버 데몬
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 데몬
TCP	4046	NFS에 대한 네트워크 상태 모니터
TCP	10000입 니다	NDMP를 사용한 백업
TCP	11104	SnapMirror에 대한 인터클러스터 통신 세션의 관리
TCP	11105	인터클러스터 LIF를 사용하여 SnapMirror 데이터 전송
UDP입니 다	111	NFS에 대한 원격 프로시저 호출
UDP입니 다	161-162	단순한 네트워크 관리 프로토콜
UDP입니 다	635	NFS 마운트
UDP입니 다	2049	NFS 서버 데몬
UDP입니 다	4045	NFS 잠금 데몬
UDP입니 다	4046	NFS에 대한 네트워크 상태 모니터
UDP입니 다	4049	NFS rquotad 프로토콜

## 아웃바운드 규칙

ONTAP용 FSx에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

## 기본 아웃바운드 규칙

ONTAP용 FSx에 대해 미리 정의된 보안 그룹에는 다음과 같은 아웃바운드 규칙이 포함됩니다.

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

#### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 ONTAP용 FSx의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스는 ONTAP 시스템용 FSx의 인터페이스(IP 주소)입니다.

서비스	프로토콜	포트	출처	목적지	목적
Active Directory 를 클릭합니 다	TCP	88	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니 다	138	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	노드 관리 LIF	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	노드 관리 LIF	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	노드 관리 LIF	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니 다	464	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	노드 관리 LIF	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	TCP	88	데이터 LIF(NFS, CIFS, iSCSI)	Active Directory 포리스트입니다	Kerberos V 인증
	UDP입니 다	137	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니 다	138	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	TCP	139	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP 및 UDP	389	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	UDP입니 다	464	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos 키 관리
	TCP	749	데이터 LIF(NFS, CIFS)	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
S3로 백업	TCP	5010	인터클러스터 LIF	엔드포인트 백업 또는 복원	S3로 백업 기능의 백업 및 복원 작업

서비스	프로토콜	포트	출처	목적지	목적
클러스터	모든 교통 정보	모든 교통 정보	모든 LIF가 하나의 노드에 있습니다	다른 노드의 모든 LIF	인터클러스터 통신(Cloud Volumes ONTAP HA에만 해당)
	TCP	3000입니다	노드 관리 LIF	HA 중재자	ZAPI 호출(Cloud Volumes ONTAP HA 전용)
	ICMP	1	노드 관리 LIF	HA 중재자	활성 상태 유지(Cloud Volumes ONTAP HA만 해당)
DHCP를 선택합니다	UDP입니다	68	노드 관리 LIF	DHCP를 선택합니다	처음으로 설정하는 DHCP 클라이언트
DHCPs	UDP입니다	67	노드 관리 LIF	DHCP를 선택합니다	DHCP 서버
DNS	UDP입니다	53	노드 관리 LIF 및 데이터 LIF(NFS, CIFS)	DNS	DNS
NDMP	TCP	1860-18699	노드 관리 LIF	대상 서버	NDMP 복제
SMTP	TCP	25	노드 관리 LIF	메일 서버	AutoSupport에 사용할 수 있는 SMTP 경고
SNMP를 선택합니다	TCP	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	161	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	TCP	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
	UDP입니다	162	노드 관리 LIF	서버 모니터링	SNMP 트랩으로 모니터링
SnapMirror를 참조하십시오	TCP	11104	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror에 대한 인터클러스터 통신 세션의 관리
	TCP	11105	인터클러스터 LIF	ONTAP 인터클러스터 LIF	SnapMirror 데이터 전송
Syslog를 클릭합니다	UDP입니다	514	노드 관리 LIF	Syslog 서버	Syslog 메시지를 전달합니다

## 커넥터 규칙

Connector의 보안 그룹에는 인바운드 및 아웃바운드 규칙이 모두 필요합니다.

### 인바운드 규칙

프로토콜	포트	목적
SSH를 클릭합니 다	22	커넥터 호스트에 대한 SSH 액세스를 제공합니다
HTTP	80	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTP 액세스를 제공하고 Cloud Data Sense에서 연결을 제공합니다
HTTPS	443	클라이언트 웹 브라우저에서 로컬 사용자 인터페이스로 HTTPS 액세스를 제공합니다
TCP	3128	AWS 네트워크에서 NAT 또는 프록시를 사용하지 않는 경우 인터넷 액세스가 가능한 클라우드 데이터 감지 인스턴스를 제공합니다

## 아웃바운드 규칙

Connector에 대해 미리 정의된 보안 그룹은 모든 아웃바운드 트래픽을 엽니다. 허용 가능한 경우 기본 아웃바운드 규칙을 따릅니다. 더 엄격한 규칙이 필요한 경우 고급 아웃바운드 규칙을 사용합니다.

### 기본 아웃바운드 규칙

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

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

### 고급 아웃바운드 규칙

아웃바운드 트래픽에 대해 엄격한 규칙이 필요한 경우 다음 정보를 사용하여 Connector의 아웃바운드 통신에 필요한 포트만 열 수 있습니다.



소스 IP 주소는 커넥터 호스트입니다.

서비스	프로토콜	포트	목적지	목적
Active Directory를 클릭합니다	TCP	88	Active Directory 포리스트입니다	Kerberos V 인증
	TCP	139	Active Directory 포리스트입니다	NetBIOS 서비스 세션입니다
	TCP	389	Active Directory 포리스트입니다	LDAP를 지원합니다
	TCP	445	Active Directory 포리스트입니다	Microsoft SMB/CIFS over TCP 및 NetBIOS 프레임
	TCP	464	Active Directory 포리스트입니다	Kerberos V 변경 및 암호 설정(set_change)
	TCP	749	Active Directory 포리스트입니다	Active Directory Kerberos V 변경 및 암호 설정(RPCSEC_GSS)
	UDP입니다	137	Active Directory 포리스트입니다	NetBIOS 이름 서비스입니다
	UDP입니다	138	Active Directory 포리스트입니다	NetBIOS 데이터그램 서비스
	UDP입니다	464	Active Directory 포리스트입니다	Kerberos 키 관리
API 호출 및 AutoSupport	HTTPS	443	아웃바운드 인터넷 및 ONTAP 클러스터 관리 LIF	API는 AWS 및 ONTAP를 호출하고 AutoSupport 메시지를 NetApp에 보냅니다
API 호출	TCP	3000입니다	ONTAP HA 중재자	ONTAP HA 중재인과의 커뮤니케이션
	TCP	8088	S3로 백업	API에서 S3로 백업을 호출합니다
DNS	UDP입니다	53	DNS	Cloud Manager에서 DNS Resolve에 사용됩니다
클라우드 데이터 감지	HTTP	80	클라우드 데이터 감지 인스턴스	Cloud Volumes ONTAP에 대한 클라우드 데이터 감지

# ONTAP에 Amazon FSx를 사용합니다

## ONTAP 작업 환경을 위한 Amazon FSx를 생성하고 관리합니다

Cloud Manager를 사용하면 ONTAP 작업 환경의 FSx를 생성하고 관리하여 볼륨 및 추가 데이터 서비스를 추가하고 관리할 수 있습니다.

### ONTAP 작업 환경을 위한 Amazon FSx를 생성합니다

첫 번째 단계는 ONTAP 작업 환경에 대한 FSx를 생성하는 것입니다. AWS 관리 콘솔에서 ONTAP용 FSx 파일 시스템을 이미 생성한 경우를 사용할 수 있습니다 ["Cloud Manager를 사용하여 IT에 대해 알아보십시오"](#).

Cloud Manager에서 ONTAP 작업 환경을 위한 FSx를 생성하기 전에 다음이 필요합니다.

- ONTAP 작업 환경을 위한 FSx를 생성하는 데 필요한 권한을 클라우드 관리자에게 제공하는 IAM 역할의 ARN 을 참조하십시오 ["Cloud Manager에 AWS 자격 증명 추가"](#) 를 참조하십시오.
- ONTAP용 FSx 인스턴스를 생성할 지역 및 VPN 정보

단계

1. Cloud Manager에서 새 작업 환경을 추가하고 \* Amazon Web Services \* 위치를 선택한 후 \* 다음 \* 을 클릭합니다.
2. ONTAP \* 용 \* 아마존 FSx 를 선택하고 \* 다음 \* 을 클릭합니다.

The screenshot shows the 'Add Working Environment' wizard in AWS Cloud Manager. The 'Choose a Location' section has four options: Microsoft Azure, Amazon Web Services (selected), Google Cloud Platform, and On-Premises. The 'Choose Type' section has four options: Cloud Volumes ONTAP (Single Node), Cloud Volumes ONTAP HA (High Availability), Amazon FSx for ONTAP (High Availability) (selected), and Kubernetes Cluster (Managed). A 'Next' button is at the bottom.

3. Cloud Manager에서 ONTAP에 대한 FSx를 인증합니다.
  - a. 계정에 ONTAP용 FSx에 대한 올바른 AWS 권한이 있는 기존 IAM 역할이 있는 경우 드롭다운에서 해당 역할을 선택합니다.



## FSx for ONTAP Authentication

Select the credentials that provides Cloud Manager with the permissions that it needs to manage FSx for ONTAP.

Credentials Name

mjulia ▼

---

To add a new set of credential, go to the [Credentials Page](#).

- b. 계정에 IAM 역할이 없는 경우 \* 자격 증명 페이지 \* 를 클릭하고 마법사의 단계에 따라 ONTAP 자격 증명을 위한 FSx를 사용하여 AWS IAM 역할에 대한 ARN을 추가합니다. 을 참조하십시오 ["Cloud Manager에 AWS 자격 증명 추가"](#) 를 참조하십시오.

## FSx for ONTAP Authentication

To provide the required AWS permissions, Cloud Manager needs the ARN of an IAM role in your account that it can assume.

- 1** | Go to [Credentials Page](#).
- 2 | Click [Add Credentials](#).
- 3 | Select [AWS > Cloud Manager](#).
- 4 | Enter the required information.
- 5 | Restart this wizard.

4. ONTAP용 FSx 인스턴스에 대한 정보를 제공합니다.
- a. 사용할 작업 환경 이름을 입력합니다.
  - b. 또는 더하기 기호를 클릭하고 태그 이름과 값을 입력하여 태그를 만들 수도 있습니다.
  - c. 사용할 ONTAP 클러스터 암호를 입력하고 확인합니다.
  - d. SVM 사용자에게 대해 동일한 암호를 사용하거나 다른 암호를 설정하는 옵션을 선택합니다.

e. 다음 \* 을 클릭합니다.

Add FSx for ONTAP

Details and Credentials

**Details**

Working Environment Name ⓘ  
myfsxenvironment

**Tags** *Optional*  
[Add Tags](#)

**Credentials**

User Name  
fsxadmin

ONTAP Cluster Password  
.....

Confirm ONTAP Cluster Password  
.....

☒ Use the same password for SVM user (vsadmin)

Previous Next

5. 지역 및 VPC 정보 제공:

- 각 노드가 전용 가용성 영역에 있도록 적어도 두 개의 가용성 영역에 서브넷이 있는 영역 및 VPC를 선택합니다.
- 기본 보안 그룹을 수락하거나 다른 보안 그룹을 선택합니다. ["AWS 보안 그룹"](#) 인바운드 및 아웃바운드 트래픽을 제어합니다. 이러한 항목은 AWS 관리자가 구성하며 에 연결됩니다 ["AWS의 탄력적인 네트워크 인터페이스\(ENI\)"](#).
- 각 노드에 대한 가용성 영역 및 서브넷을 선택합니다.
- 다음 \* 을 클릭합니다.

Add FSx for ONTAP

Region and VPC

Region: us-east-2 | US East (Ohio) VPC: VPC4QA - 10.0.0.0/16 Security Group: Default security group

**Node 1**

Availability Zone: us-east-2b Subnet: 10.0.4.0/24

**Node 2**

Availability Zone: us-east-2c Subnet: 10.0.3.0/24

Previous Next

6. CIDR Range\_Empty를 그대로 두고 \* Next \* 를 클릭하여 사용 가능한 범위를 자동으로 설정합니다. 선택적으로 를 사용할 수 있습니다 ["AWS Transit Gateway를 참조하십시오"](#) 범위를 수동으로 구성합니다.

Add FSx for ONTAP
Floating IP

Floating IP addresses are required for cluster and SVM access and for NFS and CIFS data access.

Floating IPs can migrate between HA nodes if failures occur. To access the data from outside the VPC, you can set up an [AWS transit gateway](#).

CIDR Range

Optional

Example: 10.10.10.10/24

**Notice:** You must specify a CIDR block that is outside of the CIDR blocks for all VPCs in the selected AWS region.

Previous

Next

7. 부동 IP 주소에 대한 라우트가 포함된 라우팅 테이블을 선택합니다. VPC(기본 경로 테이블)에 있는 서브넷에 대한 경로 테이블이 하나만 있는 경우 Cloud Manager는 해당 경로 테이블에 부동 IP 주소를 자동으로 추가합니다. 계속하려면 \* 다음 \* 을 클릭합니다.

Add FSx for ONTAP
Route Tables

Select the route tables that should include routes to the floating IP addresses. This enables client access to volumes. Clients associated with unselected route tables won't have access to volumes.

[Learn More](#)

2 Route table

<input type="checkbox"/>	Name	Main	ID	Associate with Subnets	Tags	
<input checked="" type="checkbox"/>	VPC4QA	Yes	rtb-0880ec9d aeb55d630	2 Subnets	2	⌵
<input type="checkbox"/>	No tag name	No	rtb-0e0c7d9e a4cf05d66	1 Subnet	1	⌵

**Notice:** The main route table is the default for the VPC

Previous

Next

8. 기본 AWS 마스터 키를 수락하거나 \* 키 변경 \* 을 클릭하여 다른 AWS CMK(Customer Master Key)를 선택합니다. CMK에 대한 자세한 내용은 을 참조하십시오 ["AWS KMS 설정"](#). 계속하려면 \* 다음 \* 을 클릭합니다.

Add FSx for ONTAP
Data Encryption

AWS Managed Encryption

AWS is responsible for data encryption and decryption operations. Key management is handled by AWS key management services.

---

Default Master Key: aws/fsx [Change Key](#)

Previous

Next

## 9. 스토리지 구성:

- 처리량, 용량 및 단위를 선택합니다.
- 선택적으로 IOPS 값을 지정할 수 있습니다. IOPS 값을 지정하지 않으면 Cloud Manager가 입력된 총 용량의 GiB당 3 IOPS를 기준으로 기본값을 설정합니다. 예를 들어, 총 용량에 대해 2000GiB를 입력하고 IOPS 값이 없으면 유효 IOPS 값은 6000으로 설정됩니다.

최소 요구 사항을 충족하지 않는 IOPS 값을 지정하면 작업 환경을 추가할 때 오류가 발생합니다.



Failed to create FSx for ONTAP systems [Show Less](#) ^

Invalid SSD IOPS provided: 400 IOPS. Amazon FSx does not support provisioning fewer than 3 IOPS per GB of SSD storage capacity on a ONTAP file system.

- 다음 \* 을 클릭합니다

Add FSx for ONTAP
Storage Configuration

SSD Disk Properties

Throughput

512 MBps

Capacity

3

Unit

TiB

IOPS Value

400

Optional ⓘ

Notice: The current version of FSx does not allow changing the capacity after creation. Also, note that the capacity drives the cost of the service.

Previous

Next

10. 구성을 검토합니다.

- 탭을 클릭하여 ONTAP 속성, 공급자 속성 및 네트워킹 구성을 검토합니다.
- 설정을 변경하려면 \* Previous \* (이전 \*)를 클릭합니다.
- 설정을 적용하고 작업 환경을 만들려면 \* 추가 \* 를 클릭합니다.

Review

**myfsxenvironment**  
FSx for ONTAP | HA | Multiple AZs

Overview

ONTAP Properties
Provider Properties
Networking

HA Deployment Model
Multiple Availability Zone

Capacity
3 TiB

Throughput
512 MBps

Previous

Add

클라우드 관리자는 Canvas 페이지에 ONTAP용 FSx 구성을 표시합니다.



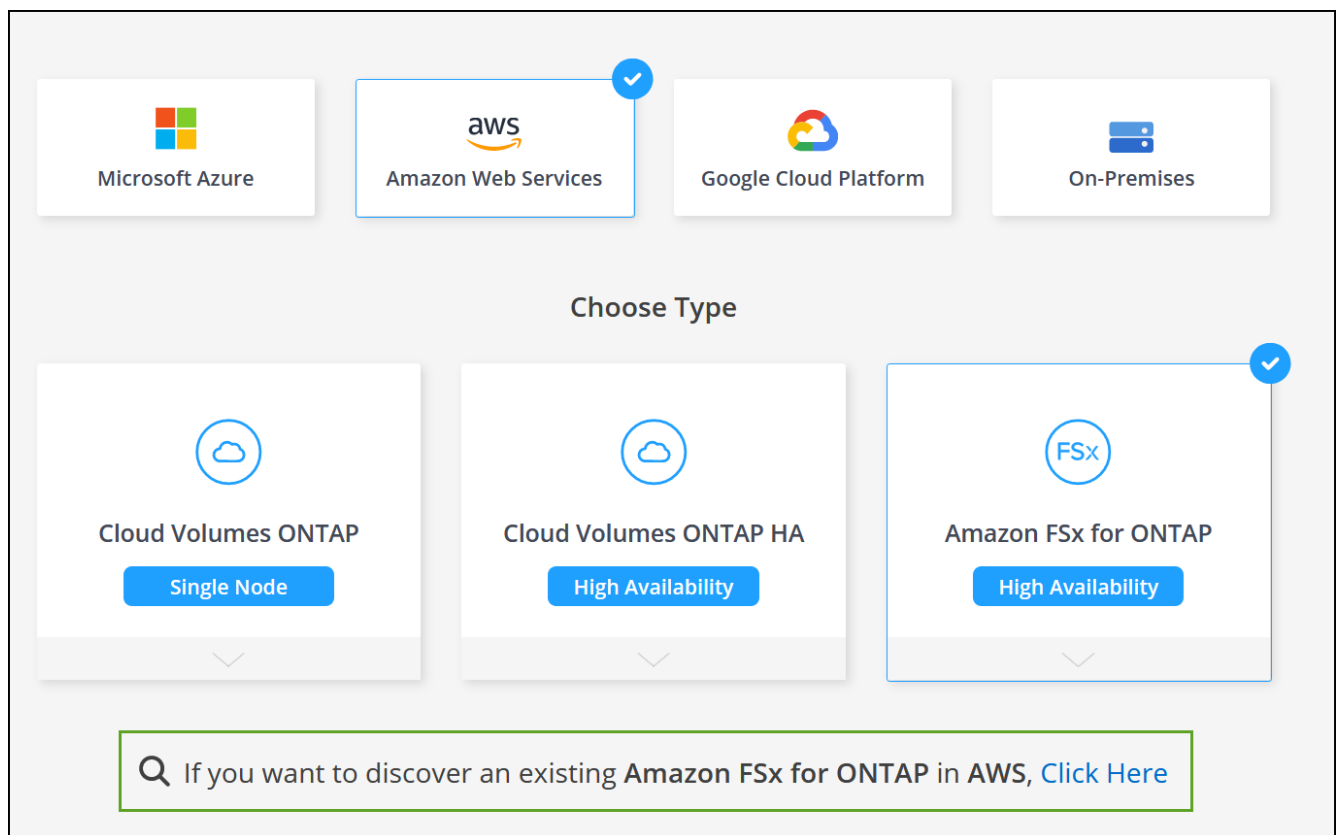
이제 Cloud Manager를 사용하여 ONTAP 작업 환경의 FSx에 볼륨을 추가할 수 있습니다.

## ONTAP 파일 시스템용 기존 FSx를 검색합니다

AWS 관리 콘솔을 사용하여 ONTAP용 FSx 파일 시스템을 생성했거나 이전에 제거한 작업 환경을 복구하려는 경우 Cloud Manager를 사용하여 검색할 수 있습니다.

단계

1. Cloud Manager에서 \* 작업 환경 추가 \* 를 클릭하고 \* Amazon Web Services \* 를 선택합니다.
2. ONTAP \* 용 \* 아마존 FSx 를 선택하고 \* 여기를 클릭 \* 을 클릭합니다.



3. 기존 자격 증명을 선택하거나 새 자격 증명을 생성합니다. 다음 \* 을 클릭합니다.
4. 추가할 AWS 지역과 작업 환경을 선택합니다.



5. 추가 \* 를 클릭합니다.

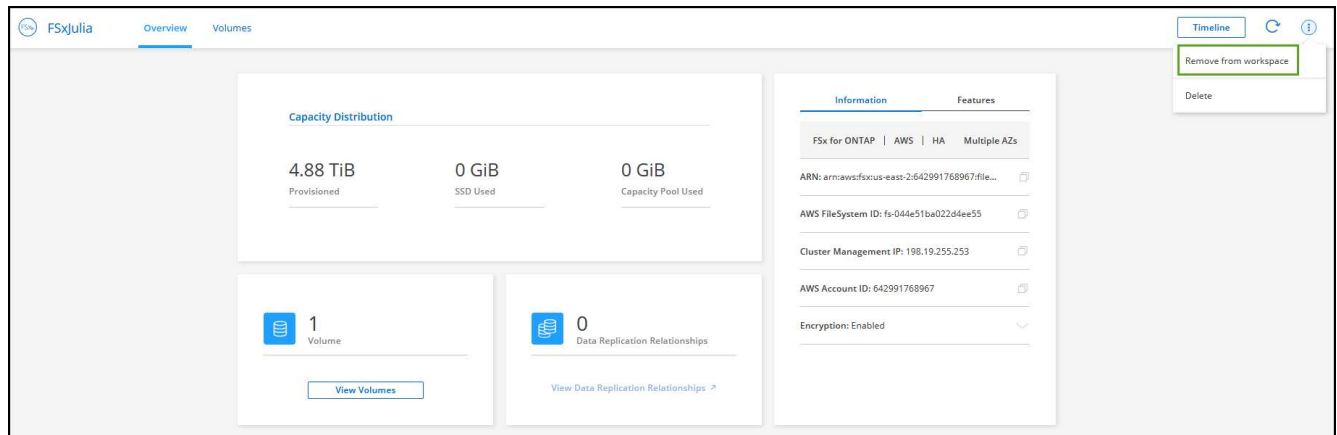
ONTAP 파일 시스템에 대해 검색된 FSx가 클라우드 관리자에 표시됩니다.

## 작업 영역에서 **ONTAP**용 **FSx**를 제거합니다

ONTAP 계정 또는 볼륨에 대한 FSx를 삭제하지 않고 Cloud Manager에서 ONTAP용 FSx를 제거할 수 있습니다. ONTAP 작업 환경용 FSx를 언제든지 Cloud Manager에 다시 추가할 수 있습니다.

단계

1. 작업 환경을 엽니다. AWS에 커넥터가 없는 경우 프롬프트 화면이 표시됩니다. 이 문제를 무시하고 작업 환경 제거를 계속할 수 있습니다.
2. 페이지 오른쪽 상단에서 작업 메뉴를 선택하고 \* 작업 영역에서 제거 \* 를 클릭합니다.



3. Cloud Manager에서 ONTAP용 FSx를 제거하려면 \* 제거 \* 를 클릭합니다.

## ONTAP 작업 환경의 **FSx**를 삭제합니다

Cloud Manager에서 ONTAP용 FSx를 삭제할 수 있습니다.

시작하기 전에

- 반드시 해야 합니다 "모든 볼륨을 삭제합니다" 파일 시스템과 연결되어 있습니다.



볼륨을 제거 또는 삭제하려면 AWS의 활성 커넥터가 필요합니다.

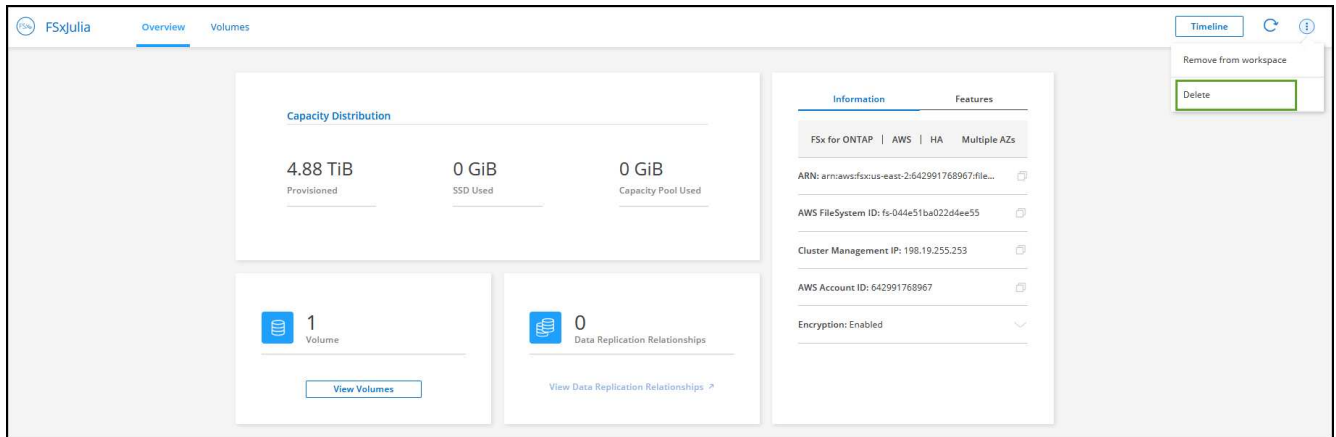
- 오류가 발생한 볼륨이 있는 작업 환경은 삭제할 수 없습니다. ONTAP 파일 시스템용 FSx를 삭제하기 전에 AWS 관리 콘솔 또는 CLI를 사용하여 실패한 볼륨을 삭제해야 합니다.



이 작업을 수행하면 작업 환경과 관련된 모든 리소스가 삭제됩니다. 이 작업은 실행 취소할 수 없습니다.

단계

1. 작업 환경을 엽니다. AWS에 커넥터가 없는 경우 프롬프트 화면이 표시됩니다. 이 작업을 무시하고 작업 환경 삭제를 계속할 수 있습니다.
2. 페이지 오른쪽 상단에서 작업 메뉴를 선택하고 \* 삭제 \* 를 클릭합니다.



3. 작업 환경의 이름을 입력하고 \* 삭제 \* 를 클릭합니다.

## ONTAP용 Amazon FSx의 볼륨을 생성합니다

작업 환경을 설정한 후 ONTAP 볼륨용 FSx를 생성하고 마운트할 수 있습니다.

### 볼륨 생성

Cloud Manager의 ONTAP 작업 환경을 위한 FSx에서 NFS 및 CIFS 볼륨을 생성하고 관리할 수 있습니다. ONTAP CLI를 사용하여 생성된 NFS 및 CIFS 볼륨은 ONTAP 작업 환경의 FSx에도 표시됩니다.

ONTAP CLI, ONTAP API 또는 Cloud Manager API를 사용하여 iSCSI 볼륨을 생성하고 FSx for ONTAP 작업 환경에서 Cloud Manager를 사용하여 관리할 수 있습니다.

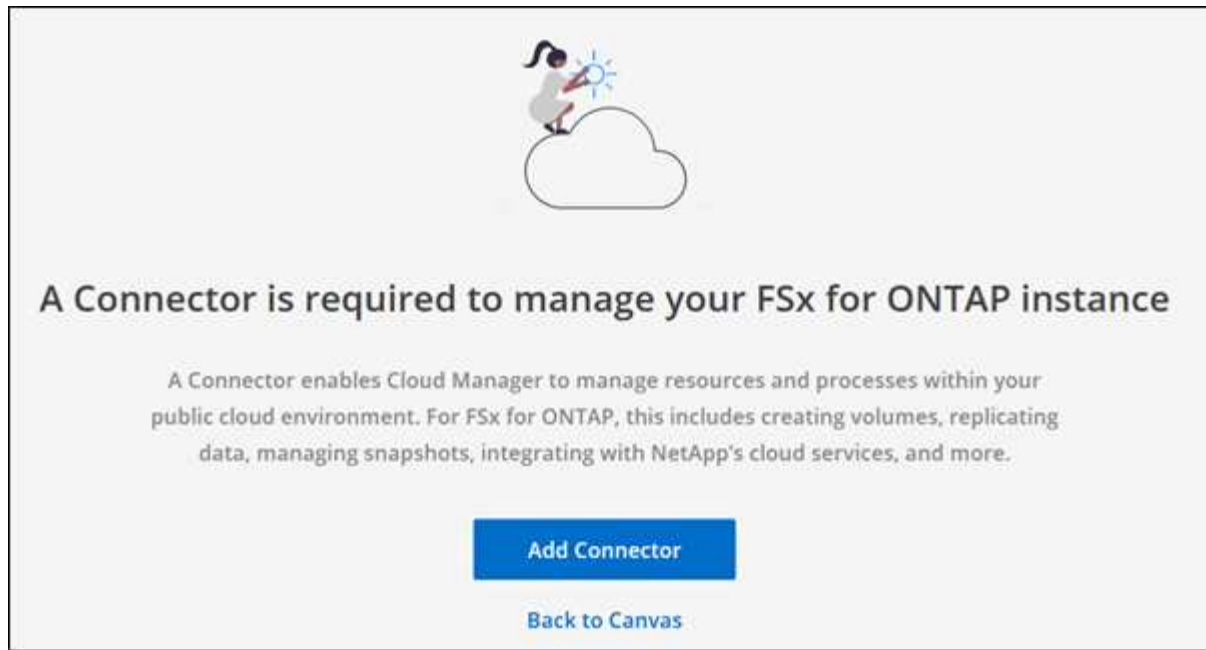
필요한 사항:

- 활성 ["커넥터를 사용하여 AWS에 연결합니다"](#).
- SMB를 사용하려면 DNS 및 Active Directory를 설정해야 합니다. DNS 및 Active Directory 네트워크 구성에 대한 자세한 내용은 ["AWS: 자체 관리되는 Microsoft AD를 사용하기 위한 사전 요구 사항"](#)을 참조하십시오.

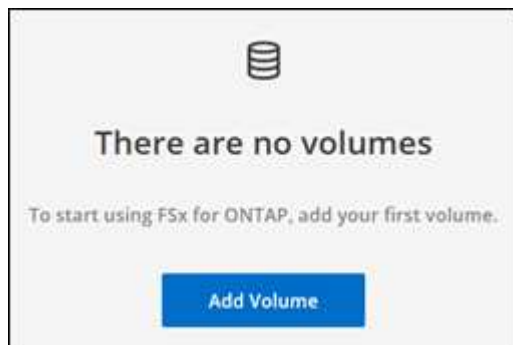
단계

1. ONTAP 작업 환경을 위한 FSx를 엽니다.
2. 커넥터가 활성화되어 있지 않으면 커넥터를 추가하라는 메시지가 표시됩니다.





3. 볼륨 \* 탭을 클릭합니다
4. 볼륨 추가 \* 를 클릭합니다.



5. \* 볼륨 세부 정보 및 보호 \*:
  - a. 새 볼륨의 이름을 입력합니다.
  - b. SVM(Storage VM) 필드는 작업 환경의 이름을 기준으로 SVM을 자동으로 채웁니다.
  - c. 볼륨 크기를 입력하고 단위(GiB 또는 TiB)를 선택합니다. 볼륨 크기는 사용량에 따라 증가합니다.
  - d. 스냅샷 정책을 선택합니다. 기본적으로 스냅샷은 매시간(마지막 6개 복사본 유지), 매일(마지막 2개 복사본 유지) 및 매주(마지막 2개 복사본 유지) 생성됩니다.
  - e. 다음 \* 을 클릭합니다.

1 Details and Protection   2 Protocol   3 Usage Profile & Tiering Policy   4 Review

### Volume Details & Protection

Volume Name i

Storage VM (SVM)

Volume Size i  Unit i

Snapshot Policy

default policy i

TiB

GiB

6. \* 프로토콜 \*: NFS 또는 CIFS 볼륨 프로토콜을 선택합니다.

a. NFS의 경우:

- 액세스 제어 정책을 선택합니다.
- NFS 버전을 선택합니다.
- 사용자 지정 내보내기 정책을 선택합니다. 유효한 값 기준에 대한 정보 아이콘을 클릭합니다.

1 Details & Protection   2 Protocol   3 Usage Profile & Tiering Policy   4 Review

### Volume Protocol

Select the volume's protocol: ☒ NFS Protocol ☐ CIFS Protocol

Access Control

Select NFS Version ☒ NFSv3 ☒ NFSv4

Custom Export Policy i

b. CIFS의 경우:

- 공유 이름을 입력합니다.
- 세미콜론으로 구분된 사용자 또는 그룹을 입력합니다.
- 볼륨에 대한 사용 권한 수준을 선택합니다.

✓ Details & Protection

2 Protocol

3 Usage Profile & Tiering Policy

4 Review

Volume Protocol

Select the volume's protocol:

☐ NFS Protocol
☒ CIFS Protocol

Share Name

<Volume name>\_share

Users/Groups

Everyone;

Permissions

Full Control



이 작업 환경의 첫 번째 CIFS 볼륨인 경우 \_Active Directory\_ 또는 \_Workgroup\_setup을 사용하여 CIFS 연결을 구성하라는 메시지가 표시됩니다.

- Active Directory 설정을 선택한 경우 다음 구성 정보를 제공해야 합니다.

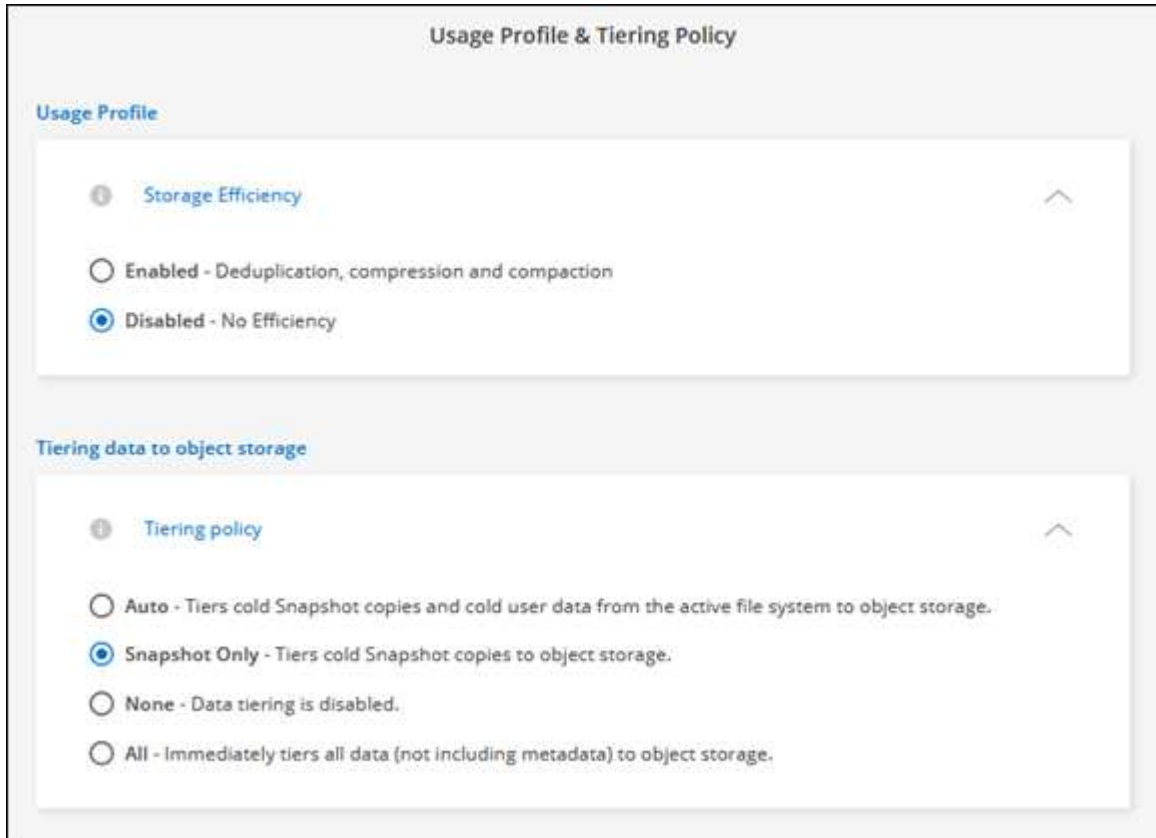
필드에 입력합니다	설명
DNS 기본 IP 주소입니다	CIFS 서버에 대한 이름 확인을 제공하는 DNS 서버의 IP 주소입니다. 나열된 DNS 서버에는 CIFS 서버가 연결할 도메인의 Active Directory LDAP 서버 및 도메인 컨트롤러를 찾는 데 필요한 서비스 위치 레코드(SRV)가 포함되어 있어야 합니다.
연결할 Active Directory 도메인입니다	CIFS 서버를 연결할 AD(Active Directory) 도메인의 FQDN입니다.
도메인에 가입하도록 승인된 자격 증명입니다	AD 도메인 내의 지정된 OU(조직 구성 단위)에 컴퓨터를 추가할 수 있는 충분한 권한이 있는 Windows 계정의 이름 및 암호입니다.
CIFS 서버 NetBIOS 이름입니다	AD 도메인에서 고유한 CIFS 서버 이름입니다.
조직 구성 단위	CIFS 서버와 연결할 AD 도메인 내의 조직 단위입니다. 기본값은 CN=Computers입니다.
DNS 도메인	SVM(스토리지 가상 머신)용 DNS 도메인 대부분의 경우 도메인은 AD 도메인과 동일합니다.
NTP 서버	Active Directory DNS를 사용하여 NTP 서버를 구성하려면 * NTP 서버 구성 활성화 * 를 선택합니다. 다른 주소를 사용하여 NTP 서버를 구성해야 하는 경우 API를 사용해야 합니다. 를 참조하십시오 <a href="#">"Cloud Manager 자동화 문서"</a> 를 참조하십시오.

- 워크그룹 설정을 선택한 경우 CIFS용으로 구성된 워크그룹의 서버 및 워크그룹 이름을 입력합니다.

a. 다음 \* 을 클릭합니다.

7. \* 사용 프로필 및 계층화 \*:

- a. 기본적으로 \* 스토리지 효율성 \* 은 사용되지 않습니다. 이 설정을 변경하여 중복제거 및 압축을 활성화할 수 있습니다.
- b. 기본적으로 \* 계층화 정책 \* 은 \* 스냅샷 전용 \* 으로 설정됩니다. 필요에 따라 다른 계층화 정책을 선택할 수 있습니다.
- c. 다음 \* 을 클릭합니다.



8. \* 검토 \*: 볼륨 구성을 검토합니다. Previous \* (이전 \*)를 클릭하여 설정을 변경하거나 \* Add \* (추가 \*)를 클릭하여 볼륨을 만듭니다.

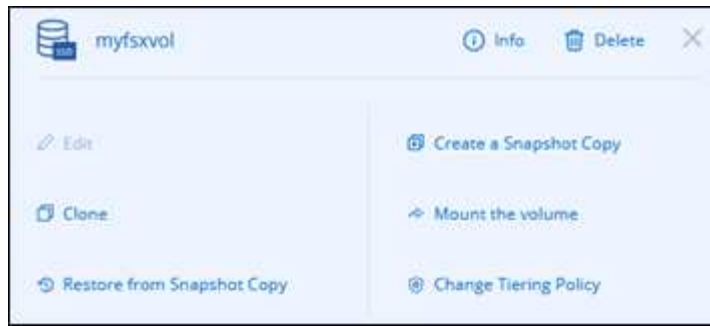
새 볼륨이 작업 환경에 추가됩니다.

## 볼륨을 마운트합니다

Cloud Manager 내에서 마운트 지침에 액세스하여 볼륨을 호스트에 마운트할 수 있습니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 \* 볼륨 마운트 \* 를 선택합니다.



3. 지침에 따라 볼륨을 마운트합니다.

## ONTAP용 Amazon FSx의 볼륨을 관리합니다

Cloud Manager를 사용하여 볼륨, 클론, 스냅샷을 관리하고 ONTAP용 FSx의 계층화 정책을 변경할 수 있습니다.

### 볼륨을 편집합니다

볼륨을 생성한 후에는 언제든지 수정할 수 있습니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 \* 편집 \* 을 선택합니다.
  - a. NFS의 경우 크기와 태그를 수정할 수 있습니다.
  - b. CIFS의 경우 필요에 따라 공유 이름, 사용자, 권한 및 스냅샷 정책을 수정할 수 있습니다.
3. 적용 \* 을 클릭합니다.

### 클론 볼륨

볼륨을 생성한 후 새 스냅샷으로부터 새 읽기-쓰기 볼륨을 생성할 수 있습니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 \* 클론 \* 을 선택합니다.
3. 복제된 볼륨의 이름을 입력합니다.
4. 클론 \* 을 클릭합니다.

### 스냅샷 복사본을 관리합니다

Snapshot 복사본은 볼륨의 시점 복사본을 제공합니다. 스냅샷 복사본을 생성하고 데이터를 새 볼륨으로 복원합니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 사용 가능한 옵션 중 하나를 선택하여 스냅샷 복사본을 관리합니다.

- \* 스냅샷 복사본 생성 \*
- \* 스냅샷 복사본에서 복원 \*

3. 프롬프트에 따라 선택한 작업을 완료합니다.

## 계층화 정책을 변경합니다

볼륨에 대한 계층화 정책을 변경합니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 \* 계층화 정책 변경 \* 을 선택합니다.
3. 새 볼륨 계층화 정책을 선택하고 \* Change \* 를 클릭합니다.

## 데이터 복제 및 동기화

Cloud Manager를 사용하여 스토리지 환경 간에 데이터를 복제할 수 있습니다. ONTAP 복제에 대해 FSx를 구성하려면 [참조하십시오 "시스템 간 데이터 복제"](#).

Cloud Manager에서 Cloud Sync를 사용하여 동기화 관계를 생성할 수 있습니다. 동기화 관계를 구성하려면 [참조하십시오 "동기화 관계를 생성합니다"](#).

## 볼륨을 삭제합니다

더 이상 필요하지 않은 볼륨을 삭제합니다.

Cloud Manager를 사용하여 SnapMirror 관계의 이전 부분이었던 볼륨을 삭제할 수 없습니다. SnapMirror 볼륨은 AWS 관리 콘솔 또는 CLI를 사용하여 삭제해야 합니다.

단계

1. 작업 환경을 엽니다.
2. 볼륨 메뉴를 열고 \* 삭제 \* 를 선택합니다.
3. 작업 환경 이름을 입력하고 볼륨 삭제를 확인합니다. Cloud Manager에서 볼륨이 완전히 제거되기까지 최대 1시간이 걸릴 수 있습니다.



복제된 볼륨을 삭제하려고 하면 오류가 발생합니다.

## 지식 및 지원

지원을 위해 등록하십시오



도움을 받으십시오



# 법적 고지

""

""

- "Cloud Manager 3.9에 대한 고지 사항"
- "Cloud Backup에 대한 알림"
- "Cloud Sync에 대한 고지 사항"
- "Cloud Tiering에 관한 고지 사항"
- "클라우드 데이터 센스에 대한 고지 사항"



## Copyright Information

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

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

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

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

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

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

## Trademark Information

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