aws

ONTAP 사용 설명서

FSx for ONTAP

FSx for ONTAP: ONTAP 사용 설명서

Table of Contents

Amazon FSx for NetApp ONTAP이란?

Amazon FSx for NetApp ONTAP은 NetApp의 인기 있는 ONTAP 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하는 완전관리형 서비스입니다. FSx for ONTAP은 완전관리형 AWS 서비스의 민첩성, 확장성 및 단순성을 NetApp 파일 시스템의 친숙한 기능, 성능 및 API 작업과 결합합니다.

FSx for ONTAP은 AWS 또는 온프레미스에서 실행되는 Linux, Windows 및 macOS 컴퓨팅 인스턴스에서 광범위하게 액세스할 수 있는 기능이 풍부하고 빠르고 유연한 공유 파일 스토리지를 제공합니다. FSx for ONTAP은 지연 시간이 1밀리초 미만인 고성능 솔리드 스테이트 드라이브(SSD) 스토리지를 제공합니다. FSx for ONTAP을 사용하면 데이터의 극히 일부에 대해서만 SSD 스토리지 비용을 지불하면서 워크로드에 SSD 수준의 성능을 달성할 수 있습니다.

FSx for ONTAP을 사용하면 버튼 클릭 한 번으로 파일의 스냅샷을 생성하고 파일을 복제할 수 있으므로 데이터를 더 쉽게 관리할 수 있습니다. 또한 FSx for ONTAP은 데이터를 보다 저렴하고 탄력적인 스토리지로 자동 계층화하므로 용량을 프로비저닝하거나 관리할 필요가 줄어듭니다.

FSx for ONTAP은 또한 완전관리형 백업과 리전 간 재해 복구 지원을 통해 가용성과 내구성이 뛰어난 스토리지를 제공합니다. 데이터를 보다 쉽게 보호할 수 있도록 FSx for ONTAP은 널리 사용되는 데이터 보안 및 바이러스 백신 애플리케이션을 지원합니다.

온프레미스에서 NetApp ONTAP을 사용하는 고객의 경우 FSx for ONTAP은 애플리케이션 코드 또는 데이터 관리 방법을 변경할 필요 AWS 없이 파일 기반 애플리케이션을 온프레미스에서 로 마이그레이션, 백업 또는 버스트하는 데 이상적인 솔루션입니다.

완전관리형 서비스인 FSx for ONTAP을 사용하면 클라우드에서 안정적이고 성능이 뛰어나며 안전한 공유 파일 스토리지를 쉽게 시작하고 확장할 수 있습니다. FSx for ONTAP을 사용하면 더 이상 다음 사항에 대해 걱정할 필요가 없습니다.

- 파일 서버 및 스토리지 볼륨 설정 및 프로비저닝
- 데이터 복제
- 파일 서버 소프트웨어 설치 및 패치 적용
- 하드웨어 장애 감지 및 해결
- 장애 조치 및 페일백 관리
- 수동 백업 수행

또한 FSx for ONTAP은 (IAM), Amazon WorkSpaces, AWS Key Management Service (AWS KMS) 및와 같은 AWS Identity and Access Management 다른 AWS 서비스와의 풍부한 통합을 제공합니다 AWS CloudTrail.

주제

- FSx for ONTAP의 특징
- 보안 및 데이터 보호
- 모니터링 도구
- FSx for ONTAP 요금
- 의 FSx for ONTAP AWS re:Post
- Amazon FSx를 처음 사용하시나요?

FSx for ONTAP의 특징

FSx for ONTAP을 사용하면 다음과 같은 완전관리형 파일 스토리지 솔루션을 얻을 수 있습니다.

- 단일 네임스페이스에서 페타바이트 규모의 데이터 세트 지원
- 파일 시스템당 최대 초당 수십 기가바이트(GBps)의 처리량 ???
- NFS(Network File System), SMB(Server Message Block), iSCSI(Internet Small Computer Systems Interface) 및 NVMe(Non-Volatile Memory Express) 프로토콜을 사용하여 데이터에 대한 다중 프로토콜 액세스
- 가용성과 내구성이 뛰어난 다중 AZ 및 단일 AZ 배포 옵션
- 액세스 패턴에 따라 자주 액세스하지 않는 데이터를 저렴한 스토리지 계층으로 자동 전환하여 스토리지 비용을 절감하는 자동 데이터 계층화
- 데이터 압축, 중복 제거 및 축소를 통한 스토리지 사용량 감소
- NetApp의 SnapMirror 복제 기능 지원
- NetApp의 온프레미스 캐싱 솔루션 지원: NetApp Global File Cache 및 FlexCache
- 네이티브 AWS 또는 NetApp 도구 및 API 작업을 사용한 액세스 및 관리 지원
  - AWS Management Console, AWS Command Line Interface (AWS CLI) 및 SDKs
  - NetApp ONTAP CLI, REST API 및 BlueXP

보안 및 데이터 보호

공동 책임 모델은와 관련하여 사용됩니다Amazon FSx for NetApp ONTAP의 보안. Amazon FSx는 데이터를 쉽게 보호할 수 있도록 여러 수준의 보안 및 규정 준수를 제공합니다.

FSx for ONTAP은 다음과 같은 데이터 보호, 보안 및 액세스 제어 기능을 지원합니다.

- 를 사용하여 파일 시스템 데이터 및 백업에 대한 저장 데이터 암호화 AWS KMS keys
- 다음을 사용하여 전송 중 데이터 암호화:
  - SMB Kerberos
  - IPSEC
  - Nitro 기반 암호화
- 온디맨드 바이러스 백신 스캔
- Microsoft Active Directory를 사용한 인증 및 권한 부여
- 파일 액세스 감사
- NetAppSnapLock 규정 준수 및 엔터프라이즈 보존 모드를 사용하는 WORM

자세한 내용은 Amazon FSx for NetApp ONTAP의 데이터 보호 및 데이터 보호 섹션을 참조하세요.

또한 Amazon FSx는 내구성이 뛰어난 파일 시스템 백업으로 데이터를 보호합니다. Amazon FSx는 자동 일별 백업을 수행하며 언제든지 추가 백업을 수행할 수 있습니다. 자세한 내용은 데이터 보호 단원을 참조하십시오.

모니터링 도구

모니터링 도구에는 CloudWatch, CloudTrail, ONTAP EMS 이벤트, NetApp Data Infrastructure Insights 및 NetApp Harvest가 포함됩니다.

FSx for ONTAP 요금

다음 범주에 따라 파일 시스템 요금이 청구됩니다.

- SSD 스토리지 용량(월별 GB당)
- GB당 3IOPS를 초과하여 프로비저닝하는 SSD IOPS(월별 IOPS당)
- 처리량 용량(초당 메가바이트당(월별 MBps당)

- 용량 풀 스토리지 사용량(월별 GB당)
- 용량 풀 요청(읽기 및 쓰기당)
- 백업 스토리지 사용량(월별 GB당)

서비스와 연결된 요금 및 비용에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 요금을 참조하세요.

의 FSx for ONTAP AWS re:Post

Amazon FSx를 사용하는 동안 문제가 발생하면 AWS re:Post를 사용하여 FSx for ONTAP 질문에 대한 답변을 얻으세요.

Amazon FSx를 처음 사용하시나요?

Amazon FSx를 처음 사용한다면, 다음 섹션을 순서대로 읽어보는 것이 좋습니다.

1. 를 처음 사용하는 경우 AWS단원FSx for ONTAP 설정을 참조하여를 설정합니다 AWS 계정.
2. 첫 번째 Amazon FSx 파일 시스템을 만들 준비가 되었으면 Amazon FSx for NetApp ONTAP 시작하기의 지침을 따릅니다.
3. 성능에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 성능 섹션을 참조하세요.
4. Amazon FSx 보안 세부 사항은 Amazon FSx for NetApp ONTAP의 보안 섹션을 참조하세요.
5. Amazon FSx API에 대한 자세한 내용은 Amazon FSx API 참조를 참조하세요.

Amazon FSx for NetApp ONTAP 작동 방식

이 주제에서는 NetApp ONTAP영 Amazon FSx 파일 시스템의 주요 기능과 작동 방식을 심층 설명, 중요한 구현 세부 정보 및 단계별 구성 절차가 포함된 섹션으로 연결되는 링크와 함께 소개합니다.

주제

FSx for ONTAP 파일 시스템

파일 시스템은 온프레미스 NetApp ONTAP 클러스터와 유사한 기본 FSx for ONTAP 리소스입니다. 파일 시스템의 솔리드 스테이트 드라이브(SSD) 스토리지 용량 및 처리량 용량을 지정하고 파일 시스템을 생성할 Amazon Virtual Private Cloud(VPC)를 선택합니다. 자세한 내용은 FSx for ONTAP 파일 시스템 관리 단원을 참조하십시오.

파일 시스템에는 구성에 따라 1~12개의 고가용성(HA) 페어가 있을 수 있습니다. HA 페어는 활성 대기 구성의 두 파일 서버로 구성됩니다. 1세대 FSx for ONTAP 파일 시스템과 2세대 Multi-AZ 파일 시스템은 HA 페어 하나를 지원합니다. 2세대 Single-AZ 파일 시스템은 최대 12개의 HA 페어를 지원합니다. 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

스토리지 가상 머신

스토리지 가상 머신(SVM)은 데이터 관리 및 액세스를 위한 자체 관리 및 데이터 액세스 엔드포인트가 있는 격리형 파일 서버입니다. FSx for ONTAP 파일 시스템의 데이터에 액세스할 때 클라이언트와 워크스테이션은 SVM의 엔드포인트 IP 주소를 사용하여 SVM과 인터페이스합니다. 자세한 내용은 SVM 관리 단원을 참조하십시오.

파일 액세스 인증 및 권한 부여를 위해 SVM을 Microsoft Active Directory에 조인할 수 있습니다. 자세한 내용은 FSx for ONTAP에서 Microsoft Active Directory 작업 단원을 참조하십시오.

볼륨

FSx for ONTAP 볼륨은 데이터를 구성하고 그룹화하는 데 사용하는 가상 리소스입니다. 볼륨은 SVM에서 호스팅되는 논리적 컨테이너이며, 볼륨에 저장된 데이터는 파일 시스템의 물리적 스토리지 용량을 사용합니다.

볼륨을 만들 때 볼륨의 크기를 설정하면 데이터가 저장되는 스토리지 계층에 관계없이 볼륨에 저장할 수 있는 실제 데이터의 양이 결정됩니다. RW(읽기-쓰기 가능) 또는 DP(데이터 보호) 중 볼륨 유형을 설정합니다. DP 볼륨은 읽기 전용이며 NetApp SnapMirror 또는 SnapVault 관계에서 대상으로 사용할 수 있습니다.

FSx for ONTAP 볼륨은 씬 프로비저닝되므로 저장된 데이터에 대해서만 스토리지 용량을 소비합니다. 씬 프로비저닝 볼륨의 경우 스토리지 용량은 미리 예약되지 않습니다. 대신 필요에 따라 스토리지가 동적으로 할당됩니다. 볼륨 또는 LUN의 데이터가 삭제되면 여유 공간이 파일 시스템으로 다시 릴리스됩니다. 예를 들어, 10TB의 여유 저장 용량으로 구성된 파일 시스템에서 세 개의 볼륨에 저장된 데이터의 총량이 한 번에 10TB를 초과하지 않는 한 10TB 볼륨을 세 개 만들 수 있습니다. 볼륨에 물리적으로 저장된 데이터의 양은 전체 스토리지 용량 소비에 포함됩니다. 자세한 내용은 FSx for ONTAP 볼륨 관리 단원을 참조하십시오.

스토리지 계층

FSx for ONTAP 파일 시스템에는 기본 스토리지와 용량 풀 스토리지라는 두 개의 스토리지 계층이 있습니다. 기본 스토리지는 데이터 세트의 활성 부분을 위해 특별히 구축되어 프로비저닝된 확장 가능한 고성능 SSD 스토리지입니다. 용량 풀 스토리지는 페타바이트까지 확장할 수 있고 자주 액세스하지 않는 데이터에 맞게 비용을 최적화하는 완전히 탄력적인 스토리지 계층입니다. 볼륨에 데이터를 쓰면 스토리지 계층의 용량이 사용됩니다. 자세한 내용은 FSx for ONTAP 스토리지 계층 단원을 참조하십시오.

데이터 계층화

데이터 계층화는 Amazon FSx for NetApp ONTAP가 SSD와 용량 풀 스토리지 계층 간에 데이터를 자동으로 이동하는 프로세스입니다. 각 볼륨에는 데이터가 비활성화(냉각)될 때 용량 계층으로 이동하는지 여부를 제어하는 계층화 정책이 있습니다. 볼륨의 계층화 정책 냉각 기간은 데이터가 비활성(냉각)되는 시기를 결정합니다. 자세한 내용은 볼륨 데이터 계층화 단원을 참조하십시오.

스토리지 효율성

Amazon FSx for NetApp ONTAP은 ONTAP의 블록 수준 스토리지 효율성 기능인 축소, 압축 및 중복 제거를 지원하여 데이터가 사용하는 스토리지 용량을 줄입니다. 스토리지 효율성 기능을 사용하면 SSD 스토리지, 용량 풀 스토리지 및 백업에서 데이터가 차지하는 공간을 줄일 수 있습니다. 성능 저하 없이 범용 파일 공유 워크로드를 위한 일반적인 스토리지 용량 절감 효과는 SSD 및 용량 풀 스토리지 계층 모두에서 압축, 중복 제거 및 축소를 통해 65%입니다. 자세한 내용은 스토리지 효율성 단원을 참조하십시오.

FSx for ONTAP 파일 시스템에 저장된 데이터 액세스

NFS(v3, v4, v4.1, v4.2) 및 SMB 프로토콜을 통해 여러 Linux, Windows 또는 MacOS 클라이언트에서 FSx for ONTAP 볼륨의 데이터에 동시에 액세스할 수 있습니다. 또한 비휘발성 메모리 익스프레스(NVMe) 및 인터넷 소형 컴퓨터 시스템 인터페이스(iSCSI) 블록 프로토콜을 사용하여 데이터에 액세스할 수 있습니다. 자세한 내용은 FSx for ONTAP 데이터 액세스 단원을 참조하십시오.

FSx for ONTAP 리소스 관리

FSx for ONTAP 파일 시스템과 상호 작용하고 해당 리소스를 관리할 수 있는 방법에는 여러 가지가 있습니다. AWS 및 NetApp ONTAP 관리 도구를 모두 사용하여 FSx for ONTAP 리소스를 관리할 수 있습니다.

- AWS 관리 도구
  - 는 AWS Management Console
  - AWS Command Line Interface (AWS CLI)
  - Amazon FSx API 및 SDK
  - AWS CloudFormation
- NetApp 관리 도구:
  - NetApp BlueXP
  - NetApp ONTAP CLI
  - NetApp ONTAP REST API

자세한 내용은 리소스 관리 단원을 참조하십시오.

Amazon FSx for NetApp ONTAP 시작하기

Amazon FSx for NetApp ONTAP을 사용하여 시작하는 방법을 알아봅니다. 이 시작하기 연습에는 다음 단계가 포함됩니다.

1. 에 가입 AWS 계정 하고 계정에서 관리 사용자를 생성합니다.
2. Amazon FSx 콘솔을 사용하여 Amazon FSx for NetApp ONTAP 파일 시스템을 생성합니다.
3. Amazon EC2 Linux 인스턴스에서 파일 시스템을 마운트합니다.
4. 생성한 리소스를 정리합니다.

주제

FSx for ONTAP 설정

Amazon FSx를 처음 사용한다면 먼저 다음 작업을 완료합니다.

1. 에 가입 AWS 계정
2. 관리자 액세스 권한이 있는 사용자 생성

주제

에 가입 AWS 계정

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 엽니다.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화 또는 텍스트 메시지를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정AWS 계정 루트 사용자이 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 는 가입 프로세스가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 이동하고 내 계정을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

에 가입한 후 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 AWS 계정보호 AWS IAM Identity Center, AWS 계정 루트 사용자활성화 및 생성합니다.

보안 AWS 계정 루트 사용자

1. 루트 사용자를 선택하고 AWS 계정 이메일 주소를 입력하여 계정 소유자AWS Management Console로에 로그인합니다. 다음 페이지에서 비밀번호를 입력합니다.

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 User Guide의 루트 사용자로 로그인을 참조하세요.
2. 루트 사용자의 다중 인증(MFA)을 활성화합니다.

   지침은 IAM 사용 설명서의 AWS 계정 루트 사용자(콘솔)에 대한 가상 MFA 디바이스 활성화를 참조하세요.

관리자 액세스 권한이 있는 사용자 생성

1. IAM Identity Center를 활성화합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 AWS IAM Identity Center설정을 참조하세요.
2. IAM Identity Center에서 사용자에게 관리 액세스 권한을 부여합니다.

를 자격 증명 소스 IAM Identity Center 디렉터리 로 사용하는 방법에 대한 자습서는 사용 AWS IAM Identity Center 설명서의 기본값으로 사용자 액세스 구성을 IAM Identity Center 디렉터리 참조하세요.

관리 액세스 권한이 있는 사용자로 로그인

- IAM IDentity Center 사용자로 로그인하려면 IAM Identity Center 사용자를 생성할 때 이메일 주소로 전송된 로그인 URL을 사용합니다.

  IAM Identity Center 사용자를 사용하여 로그인하는 데 도움이 필요하면 AWS 로그인 사용 설명서의 AWS 액세스 포털에 로그인을 참조하세요.

추가 사용자에게 액세스 권한 할당

1. IAM Identity Center에서 최소 권한 적용 모범 사례를 따르는 권한 세트를 생성합니다.

   지침은AWS IAM Identity Center 사용 설명서의 Create a permission set를 참조하세요.
2. 사용자를 그룹에 할당하고, 그룹에 Single Sign-On 액세스 권한을 할당합니다.

   지침은 AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

다음 단계

FSx for ONTAP 사용을 시작하려면 Amazon FSx for NetApp ONTAP 시작하기를 참조하여 Amazon FSx 리소스 생성 지침을 확인합니다.

Amazon FSx for NetApp ONTAP 파일 시스템 생성

Amazon FSx 콘솔에는 파일 시스템 생성을 위한 두 가지 옵션, 즉 빠른 생성 옵션 및 표준 생성 옵션이 있습니다. 서비스 권장 구성을 통해 Amazon FSx for NetApp ONTAP 파일 시스템을 빠르고 쉽게 생성하려면 빠른 생성 옵션을 사용합니다.

빠른 생성 옵션은 네트워크 파일 시스템(NFS) 프로토콜을 통해 Linux 인스턴스에서 데이터에 액세스할 수 있도록 이 파일 시스템을 구성합니다. 파일 시스템을 생성한 후에는 서버 메시지 블록(SMB) 프로토콜을 통해 Windows 및 MacOS 클라이언트에서 액세스할 수 있도록 Active Directory에 조인된 SVM을 포함하여 필요에 따라 추가 SVM 및 볼륨을 생성할 수 있습니다. 선택한 배포 유형과 생성 시 추가하는 HA 페어 수에 따라 HA(고가용성) 페어를 추가할 수도 있습니다.

표준 생성 옵션을 사용하여 사용자 지정 구성으로 파일 시스템을 생성하고 AWS CLI 및 API를 사용하는 방법에 대한 자세한 내용은 섹션을 참조하세요파일 시스템 만들기.

파일 시스템 생성

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 대시보드에서 파일 시스템 생성을 선택하여 파일 시스템 생성 마법사를 시작합니다.
3. 파일 시스템 유형 선택 페이지에서 Amazon FSx for NetApp ONTAP을 선택한 후 다음을 선택합니다. ONTAP 파일 시스템 생성 페이지가 표시됩니다.
4. 생성 방법으로 빠른 생성을 선택합니다.
5. 빠른 구성 섹션에서 파일 시스템 이름(선택 사항)에 파일 시스템 이름을 입력합니다. 파일 시스템의 이름을 지정하면 파일 시스템을 보다 쉽게 찾고 관리할 수 있습니다. 최대 256개의 유니코드 문자, 공백 및 숫자와 특수 문자 + -(하이픈) = . _(밑줄) : /를 사용할 수 있습니다.
6. 배포 유형으로 다중 AZ 또는 단일 AZ를 선택합니다.

   - 다중 AZ 파일 시스템은 데이터를 복제하고 동일한 AWS 리전내 여러 가용 영역에 걸쳐 장애 조치를 지원합니다.
   - 단일 AZ 파일 시스템은 데이터를 복제하고 단일 가용 영역 내에서 자동 장애 조치를 제공합니다.

   자세한 내용은 가용성, 내구성 및 배포 옵션 단원을 참조하십시오.

   > **Note**
   >
   > 에 사용할 수 있는 최신 세대 FSx for ONTAP 파일 시스템이 기본적으로 선택 AWS 리전됩니다. 표준 생성 옵션을 사용하여 파일 시스템(사용 가능 AWS 리전)의 생성을 지정할 수 있습니다. 자세한 내용은 파일 시스템 만들기 단원을 참조하십시오.

7. SSD 스토리지 용량에는 파일 시스템의 스토리지 용량을 기비바이트(GiB) 단위로 지정합니다. 1,024–1,048,576 범위의 정수를 입력합니다. 자세한 내용은 파일 시스템 생성(콘솔) 단원을 참조하십시오.

   파일 시스템을 생성한 후 언제든지 필요에 따라 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 단원을 참조하십시오.
8. 처리량 용량의 경우 Amazon FSx는 SSD 스토리지를 기반으로 권장 처리량 용량을 자동으로 제공합니다. 파일 시스템의 처리량(배포 유형 및 HA 페어 양에 따라 최대 73,728MBps)을 선택할 수도 있습니다.

9. Virtual Private Cloud(VPC)에는 파일 시스템에 연결할 Amazon VPC를 선택합니다.
10. 스토리지 효율성에 활성화됨을 선택하여 ONTAP 스토리지 효율성 기능(중복 제거, 압축, 축소)을 활성화하거나 비활성화됨을 선택하여 비활성화합니다.
11. (다중 AZ만 해당) 엔드포인트 IP 주소 범위는 파일 시스템에 액세스하기 위한 엔드포인트가 생성될 IP 주소 범위를 지정합니다.

    엔드포인트 IP 주소 범위에 대한 빠른 생성 옵션을 선택합니다.

    - VPC의 할당되지 않은 IP 주소 범위 - Amazon FSx가 VPC의 기본 CIDR 범위에 있는 마지막 64개 IP 주소를 파일 시스템의 엔드포인트 IP 주소 범위로 사용하게 하려면 이 옵션을 선택합니다. 이 옵션을 여러 번 선택하면 이 범위가 여러 파일 시스템에서 공유됩니다.

      > **Note**
      >
      > - 생성하는 각 파일 시스템은 이 범위에서 두 개의 IP 주소를 사용합니다. 하나는 클러스터용이고 다른 하나는 첫 번째 SVM용입니다. 첫 번째 및 마지막 IP 주소도 예약되어 있습니다. SVM이 추가될 때마다 파일 시스템은 다른 IP 주소를 사용합니다. 예를 들어, 10개의 SVM을 호스팅하는 파일 시스템은 11개의 IP 주소를 사용합니다. 추가 파일 시스템도 동일한 방식으로 작동합니다. 초기 IP 주소 2개와, 추가 SVM 하나당 1개를 사용합니다. 동일한 IP 주소 범위를 사용하고 각각 단일 SVM을 사용하는 파일 시스템의 최대 수는 31개입니다.
      > - VPC의 기본 CIDR 범위에 있는 마지막 64개의 IP 주소 중 서브넷에서 사용 중인 주소가 있는 경우 이 옵션은 회색으로 표시됩니다.

    - VPC 외부의 유동 IP 주소 범위 - Amazon FSx가 동일한 VPC 및 라우팅 테이블을 사용하는 다른 파일 시스템에서 아직 사용되지 않은 198.19.x.0/24 주소 범위를 사용하게 하려면 이 옵션을 선택합니다.

    표준 생성 옵션에서 고유한 IP 주소 범위를 지정할 수도 있습니다. 선택한 IP 주소 범위는 서브넷과 겹치지 않고 동일한 VPC 및 라우트 테이블을 가진 다른 파일 시스템에서 이미 사용하고 있지 않다면 VPC의 IP 주소 범위 내부 또는 외부에 위치할 수 있습니다. VPC의 IP 주소 범위 내에 있는 범위를 사용하는 것이 좋습니다.

    > **Note**
    >
    > 사용 중인 모든 라우팅 테이블이 다중 AZ 파일 시스템에 연결되어 있는지 확인합니다. 이렇게 하면 장애 조치 중에 사용할 수 없게 되는 사태를 방지하는 데 도움이 됩니다.

Amazon VPC 라우팅 테이블을 파일 시스템과 연결하는 방법에 대한 자세한 내용은 파일 시스템 업데이트 섹션을 참조하세요.

12. 다음을 선택한 후 ONTAP 파일 시스템 생성 페이지에서 파일 시스템 구성을 검토합니다. 파일 시스템을 생성한 후 수정할 수 있는 파일 시스템 설정을 확인합니다.
13. 파일 시스템 생성을 선택합니다.

빠른 생성은 하나의 SVM(이름이 `fsx`로 지정됨) 및 하나의 볼륨(이름이 `vol1`로 지정됨)으로 구성된 파일 시스템을 생성합니다. 볼륨에는 `/vol1`이라는 정션 경로와, Auto라는 용량 풀 계층화 정책(31일 동안 액세스하지 않은 데이터를 저렴한 용량 풀 스토리지 계층으로 자동 이동)이 있습니다. 기본 스냅샷 정책은 기본 볼륨에 할당됩니다. 파일 시스템 데이터는 기본 서비스 관리형 AWS KMS 키를 사용하여 저장 시 암호화됩니다.

Amazon EC2 Linux 인스턴스에서 파일 시스템 탑재

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 파일 시스템을 마운트할 수 있습니다. 이 절차에서는 Amazon Linux 2를 실행하는 인스턴스를 사용합니다.

Amazon EC2에서 파일 시스템 마운트

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 파일 시스템과 동일한 Virtual Private Cloud(VPC)에 있는 Amazon Linux 2를 실행하는 Amazon EC2 인스턴스를 생성하거나 선택합니다. 인스턴스 시작에 대한 자세한 내용은 Amazon EC2 사용 설명서의 1단계: 인스턴스 시작하기를 참조하세요.
3. Amazon EC2 Linux 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하세요.
4. Secure Shell(SSH)을 사용하는 Amazon EC2 인스턴스에서 터미널을 열고 적절한 보안 인증으로 로그인합니다.
5. 다음 명령을 사용하여 볼륨의 마운트 지점으로 사용할 Amazon EC2 인스턴스에 디렉터리를 생성합니다. 다음 예제에서는 *`mount-point`*를 고유한 정보로 바꿉니다.

```
$ sudo mkdir /mount-point
```

6. 생성한 디렉터리에 Amazon FSx for NetApp ONTAP 파일 시스템을 마운트합니다. 다음 예제와 유사한 `mount` 명령을 사용합니다. 다음 예제에서는 다음의 자리 표시자 값을 고유한 정보로 바꿉니다.

- *nfs_version* - 사용 중인 NFS 버전입니다. FSx for ONTAP은 버전 3, 4.0, 4.1 및 4.2를 지원합니다.
- *nfs-dns-name* - 마운트할 볼륨이 있는 스토리지 가상 머신(SVM)의 NFS DNS 이름입니다. Amazon FSx 콘솔에서 스토리지 가상 머신을 선택한 다음 마운트할 볼륨이 있는 SVM을 선택하면 NFS DNS 이름을 찾을 수 있습니다. NFS DNS 이름은 엔드포인트 패널에서 찾을 수 있습니다.
- *volume-junction-path* - 마운트할 볼륨의 정션 경로입니다. 볼륨 세부 정보 페이지의 요약 패널에 있는 Amazon FSx 콘솔에서 볼륨의 정션 경로를 찾을 수 있습니다.
- *mount-point* - 볼륨의 마운트 지점용으로 EC2 인스턴스에 생성한 디렉터리의 이름입니다.

```
sudo mount -t nfs -o nfsvers=nfs_version nfs-dns-name:/volume-junction-path /mount-point
```

다음 명령에서는 예제 값을 사용합니다.

```
sudo mount -t nfs -o nfsvers=4.1 svm-abcdef1234567890c.fs-012345abcdef6789b.fsx.us-east-2.amazonaws.com:/vol1 /fsxN
```

Amazon EC2 인스턴스에 문제(예: 연결 시간 초과)가 있는 경우 Amazon EC2 사용 설명서의 EC2 인스턴스 문제 해결을 참조하세요.

리소스 정리

이 연습을 마친 후에는 다음 단계에 따라 리소스를 정리하고 AWS 계정을 보호해야 합니다.

리소스를 정리하려면

1. Amazon EC2 콘솔에서 인스턴스를 종료합니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 종료를 참조하세요.
2. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
3. Amazon FSx 콘솔에서 SVM의 루트 볼륨이 아닌 모든 FSx for ONTAP 볼륨을 삭제합니다. 자세한 내용은 볼륨 삭제 단원을 참조하십시오.
4. FSx for ONTAP SVM을 모두 삭제합니다. 자세한 내용은 스토리지 가상 머신 삭제(SVM) 단원을 참조하십시오.

5. Amazon FSx 콘솔에서 파일 시스템을 삭제합니다. 파일 시스템을 삭제하면 모든 자동 백업이 자동으로 삭제됩니다. 그러나 수동으로 생성된 백업은 여전히 삭제해야 합니다. 이 프로세스는 다음 단계로 이루어집니다.

   a. 콘솔 대시보드에서 이 연습을 위해 만든 파일 시스템의 이름을 선택합니다.
   b. 작업에서 파일 시스템 삭제를 선택합니다.
   c. 파일 시스템 삭제 대화 상자에 파일 시스템 ID 상자에서 삭제하려는 파일 시스템의 ID를 입력합니다.
   d. 파일 시스템 삭제를 선택합니다.
   e. Amazon FSx가 파일 시스템을 삭제하는 동안 대시보드에서 해당 상태가 삭제 중으로 변경됩니다. 파일 시스템이 삭제되면 대시보드에 더 이상 표시되지 않습니다. 모든 자동 백업은 파일 시스템과 함께 삭제됩니다.
   f. 이제 파일 시스템에 대해 수동으로 생성한 백업을 모두 삭제할 수 있습니다. 왼쪽 탐색 창에서 백업을 선택합니다.
   g. 대시보드에서 삭제한 파일 시스템과 동일한 파일 시스템 ID를 가진 백업을 선택하고 백업 삭제를 선택합니다. 최종 백업(만든 경우)은 반드시 유지하세요.
   h. 백업 삭제 대화 상자가 열립니다. 삭제할 백업의 ID에 해당하는 확인란을 선택한 다음 백업 삭제를 선택합니다.

   이제 Amazon FSx 파일 시스템 및 모든 관련 자동 백업이 삭제되며, 삭제하기로 선택한 수동 백업도 모두 삭제됩니다.

별 가용성 AWS 리전

Amazon FSx for NetApp ONTAP 파일 시스템은 다음에서 사용할 수 있으며 AWS 리전각 리전에 대해 배포 유형 지원이 표시됩니다.

AWS 리전	단일 AZ 1	다중 AZ 1	단일 AZ 2	다중 AZ 2		
미국 동부(버지니아 북부)	✓	✓	✓	✓		
미국 동부(오하이오)	✓	✓	✓	✓		
미국 서부(캘리포니아 북부)	✓	✓	✓	✓		
미국 서부(오리건)	✓	✓	✓	✓		
AWS GovCloud(미국 동부)	✓	✓				
AWS GovCloud(미국 서부)	✓	✓				
아프리카(케이프타운)	✓	✓				
아시아 태평양(홍콩)	✓	✓				
아시아 태평양(도쿄)	✓	✓	✓	✓		

AWS 리전	단일 AZ 1	다중 AZ 1	단일 AZ 2	다중 AZ 2		
아시아 태평양(서울)	✓	✓				
아시아 태평양(오사카)	✓	✓				
아시아 태평양(뭄바이)	✓	✓	✓	✓		
아시아 태평양(하이데라바드)	✓	✓				
아시아 태평양(싱가포르)	✓	✓	✓	✓		
아시아 태평양(시드니)	✓	✓	✓	✓		
아시아 태평양(자카르타)	✓	✓				
아시아 태평양(멜버른)	✓	✓				
아시아 태평양(말레이시아)	✓	✓				
아시아 태평양(태국)	✓	✓				

AWS 리전	단일 AZ 1	다중 AZ 1	단일 AZ 2	다중 AZ 2		
캐나다(중부)	✓	✓				
캐나다 서부(캘거리)	✓	✓				
유럽(프랑크푸르트)	✓	✓	✓	✓		
유럽(취리히)	✓	✓				
유럽(스톡홀름)	✓	✓	✓	✓		
유럽(밀라노)	✓	✓				
유럽(스페인)	✓	✓				
유럽(아일랜드)	✓	✓	✓	✓		
유럽(런던)	✓	✓				
유럽(파리)	✓	✓				
이스라엘(텔아비브)	✓	✓				
멕시코(중부)	✓	✓				
중동(UAE)	✓	✓				
중동(바레인)	✓	✓				

AWS 리전	단일 AZ 1	다중 AZ 1	단일 AZ 2	다중 AZ 2		
남아메리카(상파울루)	✓	✓				

FSx for ONTAP 데이터 액세스

AWS 클라우드 및 온프레미스 환경 모두에서 지원되는 다양한 클라이언트 및 메서드를 사용하여 Amazon FSx 파일 시스템에 액세스할 수 있습니다.

각 SVM에는 NetApp ONTAP CLI 또는 REST API를 사용하여 데이터에 액세스하거나 SVM을 관리하는 데 사용되는 엔드포인트가 4개 있습니다.

- `Nfs` – Network File System(NFS) 프로토콜을 사용하여 연결하는 경우
- `Smb` – Service Message Block(SMB) 프로토콜을 사용하여 연결하는 경우(SVM이 Active Directory에 조인되어 있거나 워크그룹을 사용하는 경우)
- `Iscsi` - 공유 블록 스토리지 지원을 위해 인터넷 소형 컴퓨터 시스템 인터페이스(iSCSI) 프로토콜을 사용하여 연결하는 경우.
- `Nvme` - 공유 블록 스토리지 지원을 위해 TCP/IP를 통해 비휘발성 메모리 익스프레스(NVMe)를 사용하여 연결하는 데 사용됩니다.
- `Management` – NetApp ONTAP CLI 또는 API 또는 NetApp BlueXP를 사용하여 SVM을 관리하는 경우

> **Note**
>
> iSCSI 프로토콜은 고가용성 페어(HA) 페어가 6개 이하인 모든 파일 시스템에서 사용할 수 있습니다. NVMe/TCP 프로토콜은 HA 페어가 6개 이하인 2세대 파일 시스템에서 사용할 수 있습니다.

주제

- MacOS 클라이언트에서 볼륨 탑재
- Linux용 iSCSI 프로비저닝
- Windows용 iSCSI 프로비저닝
- Linux용 NVMe /TCP 프로비저닝
- Windows용 NVMe /TCP 프로비저닝
- 다른 AWS 서비스를 사용하여 데이터 액세스

지원되는 클라이언트

FSx for ONTAP 파일 시스템은 다양한 컴퓨팅 인스턴스 및 운영 체제에서 데이터에 연결할 수 있도록 지원합니다. 이는 Network File System(NFS) 프로토콜(v3, v4.0, v4.1 및 v4.2), 모든 버전의 Server Message Block(SMB) 프로토콜(2.0, 3.0 및 3.1.1 포함) 및 Internet Small Computer Systems Interface(iSCSI) 프로토콜을 사용한 액세스를 지원함으로써 이루어집니다.

> **Important**
>
> Amazon FSx는 퍼블릭 인터넷에서 파일 시스템에 액세스하는 것을 지원하지 않습니다. Amazon FSx는 인터넷에서 연결할 수 있는 퍼블릭 IP 주소인 탄력적 IP 주소를 자동으로 분리합니다. 이 주소는 파일 시스템의 탄력적 네트워크 인터페이스에 연결됩니다.

FSx for ONTAP에서 사용할 수 있는 AWS 컴퓨팅 인스턴스는 다음과 같습니다.

- NFS 또는 SMB를 지원하는 Linux, Microsoft Windows 및 MacOS를 실행하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 자세한 내용은 Linux 클라이언트에 볼륨 탑재 Microsoft Windows 클라이언트에 볼륨 탑재 및 MacOS 클라이언트에서 볼륨 탑재을 참조하세요.
- Amazon EC2 Windows 및 Linux 인스턴스의 Amazon Elastic Container Service(Amazon ECS) 도커 컨테이너 자세한 내용은 FSx for ONTAP과 함께 Amazon Elastic Container Service 사용 섹션을 참조하세요.
- Amazon Elastic Kubernetes Service – 자세히 알아보려면 Amazon EKS 사용 설명서의 Amazon FSx for NetApp ONTAP CSI 드라이버를 참조하세요.
- Red Hat OpenShift Service on AWS (ROSA) – 자세한 내용은 Red Hat OpenShift Service on 사용 설명서의 Red Hat OpenShift Service on이란 무엇입니까 AWS?를 참조하세요. OpenShift AWS
- Amazon WorkSpaces 인스턴스. 자세한 내용은 FSx for ONTAP과 함께 Amazon WorkSpaces 사용 섹션을 참조하세요.

- Amazon AppStream 2.0 인스턴스.
- AWS Lambda - 자세한 내용은 AWS 블로그 게시물 Amazon FSx를 사용하여 서버리스 워크로드에 대한 SMB 액세스 활성화를 참조하세요.
- AWS 환경의 VMware Cloud에서 실행되는 가상 머신(VMs)입니다. 자세한 내용은 Configure Amazon FSx for NetApp ONTAP as External Storage and VMware Cloud AWS with Amazon FSx for NetApp ONTAP Deployment Guide를 참조하세요.

마운트된 후에는 NFS 및 SMB를 통해 FSx for ONTAP 파일 시스템이 로컬 디렉터리 또는 드라이브 문자로 나타나며, 최대 수천 개의 클라이언트가 동시에 액세스할 수 있는 완전관리형 공유 네트워크 파일 스토리지를 제공합니다. iSCSI LUN은 iSCSI를 통해 마운트되는 경우 블록 디바이스로 액세스할 수 있습니다.

블록 스토리지 프로토콜 사용

Amazon FSx for NetApp ONTAP는 TCP(NVMe/TCP) 블록 스토리지 프로토콜을 통한 iSCSI(인터넷 소형 컴퓨터 시스템 인터페이스) 및 NVMe(비휘발성 메모리 익스프레스)를 지원합니다. 스토리지 영역 네트워크(SAN) 환경에서 스토리지 시스템은 스토리지 대상 디바이스가 있는 대상입니다. iSCSI의 경우 스토리지 대상 디바이스를 논리적 단위(LUNs. NVMe/TCP의 경우 스토리지 대상 디바이스를 네임스페이스라고 합니다.

SVM의 iSCSI 논리적 인터페이스(LIF)를 사용하여 NVMe 및 iSCSI 블록 스토리지 모두에 연결합니다.

iSCSI용 LUNs 생성하고 NVMe용 네임스페이스를 생성하여 스토리지를 구성합니다. 그런 다음 호스트는 iSCSI 또는 TCP 프로토콜을 사용하여 LUNs 및 네임스페이스에 액세스합니다.

iSCSI 및 NVMe/TCP 블록 스토리지 구성에 대한 자세한 내용은 다음을 참조하세요.

- Linux용 iSCSI 프로비저닝
- Windows용 iSCSI 프로비저닝
- Linux용 NVMe /TCP 프로비저닝
- Windows용 NVMe /TCP 프로비저닝

> **Note**
>
> Windows용 NVMe /TCP를 프로비저닝하려면 타사 NVMe 이니시에이터를 사용해야 합니다.

내에서 데이터 액세스 AWS 클라우드

각 Amazon FSx 파일 시스템은 Virtual Private Cloud(VPC)와 연결되어 있습니다. 가용 영역과 관계 없이 파일 시스템 VPC의 어느 곳에서나 FSx for ONTAP 파일 시스템에 액세스할 수 있습니다. 다른 AWS 계정 또는에 있을 수 있는 다른 VPCs에서 파일 시스템에 액세스할 수도 있습니다 AWS 리전. FSx for ONTAP 리소스에 액세스하기 위해서는 다음 섹션에 설명되어 있는 요구 사항 외에도 파일 시스템과 클라이언트 간에 데이터 및 관리 트래픽이 흐를 수 있도록 파일 시스템의 VPC 보안 그룹을 구성해야 합니다. 필수 포트로 보안 그룹을 구성하는 방법에 대한 자세한 내용은 Amazon VPC 보안 그룹 섹션을 참조하세요.

동일 VPC 내에서 데이터 액세스

Amazon FSx for NetApp ONTAP 파일 시스템을 생성할 때는 해당 파일 시스템이 위치한 Amazon VPC를 선택합니다. Amazon FSx for NetApp ONTAP 파일 시스템과 관련된 모든 SVM 및 볼륨도 동일한 VPC에 있습니다. 볼륨을 탑재할 때 파일 시스템과 볼륨을 탑재하는 클라이언트가 동일한 VPC에 있고 클라이언트에 따라 SVM의 DNS 이름 및 볼륨 정션 또는 SMB 공유를 사용할 AWS 계정수 있습니다.

클라이언트와 볼륨이 파일 시스템의 서브넷과 동일한 가용 영역 또는 다중 AZ 파일 시스템의 기본 서브넷에 있는 경우 최적의 성능을 얻을 수 있습니다. 파일 시스템의 서브넷 또는 Amazon FSx 콘솔의 기본 서브넷을 식별하려면 파일 시스템을 선택한 다음 마운트하려는 볼륨이 있는 ONTAP 파일 시스템을 선택합니다. 그러면 서브넷 또는 기본 서브넷 패널에 서브넷 또는 기본 서브넷(다중 AZ)가 표시됩니다.

배포 VPC 외부에서 데이터 액세스

이 섹션에서는 파일 시스템의 배포 VPC 외부 AWS 위치에서 FSx for ONTAP 파일 시스템의 엔드포인트에 액세스하는 방법을 설명합니다.

다중 AZ 파일 시스템의 NFS, SMB 및 ONTAP 관리 엔드포인트에 액세스

Amazon FSx for NetApp ONTAP 다중 AZ 파일 시스템의 NFS, SMB 및 ONTAP 관리 엔드포인트는 유동 인터넷 프로토콜(IP) 주소를 사용하므로 연결된 클라이언트가 장애 조치 이벤트 중에 기본 파일 서버와 대기 파일 서버 간에 원활하게 전환할 수 있습니다. 장애 조치에 대한 자세한 내용은 FSx for ONTAP의 장애 조치 프로세스 섹션을 참조하세요.

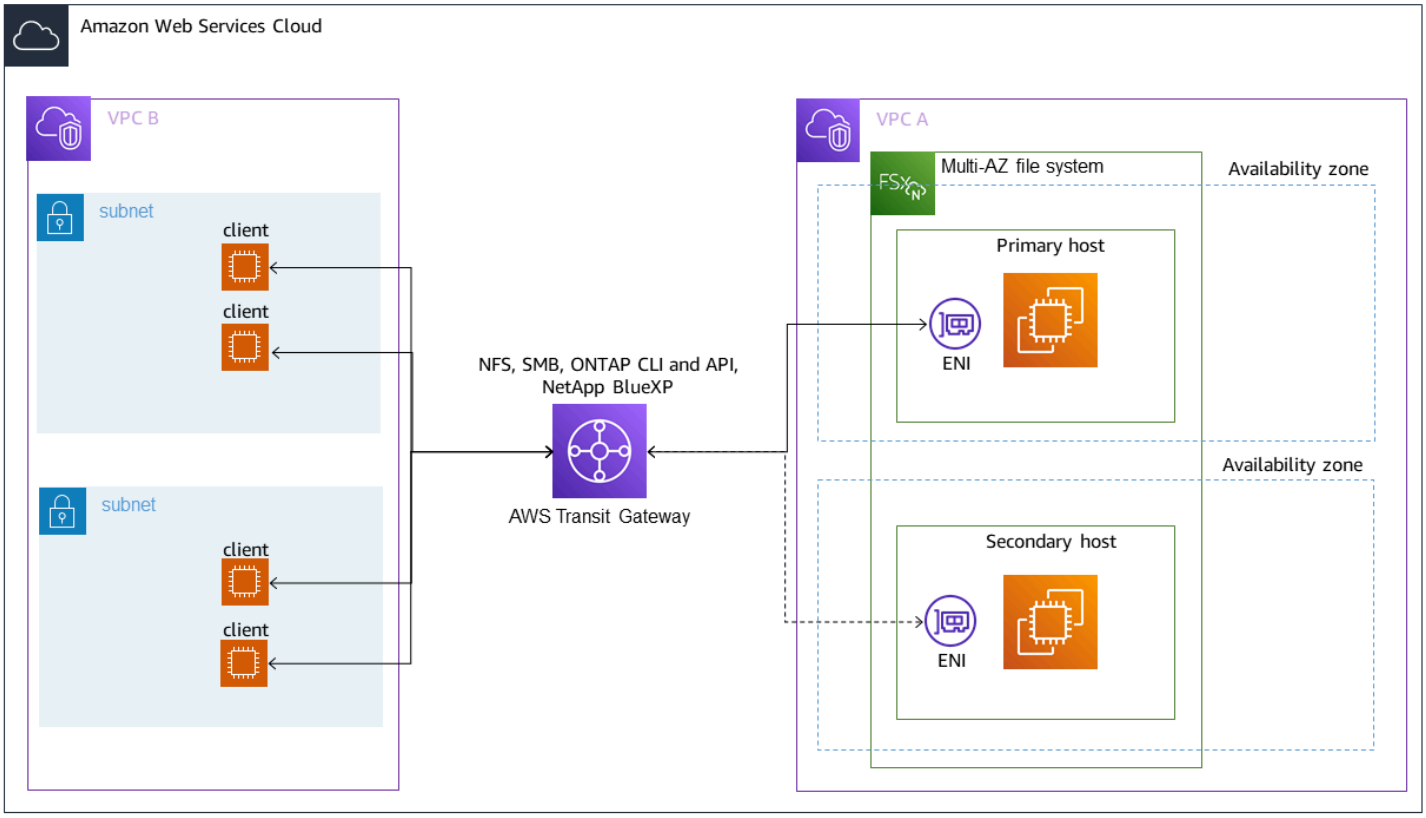
이러한 유동 IP 주소는 파일 시스템에 연결하는 VPC 라우팅 테이블에서 생성되며, 생성 중에 지정할 수 있는 파일 시스템의 `EndpointIpAddressRange` 내에 있습니다. `EndpointIpAddressRange`는 파일 시스템 생성 방법에 따라 다음 주소 범위를 사용합니다.

- 기본적으로 Amazon FSx 콘솔을 사용하여 생성된 다중 AZ 파일 시스템은 파일 시스템의 `EndpointIpAddressRange`에 VPC 기본 CIDR 범위의 마지막 64개 IP 주소를 사용합니다.

- AWS CLI 또는 Amazon FSx API를 사용하여 생성된 다중 AZ 파일 시스템은 `EndpointIpAddressRange` 기본적으로에 대한 주소 블록 내의 IP `198.19.0.0/16` 주소 범위를 사용합니다.
- 표준 생성 옵션을 사용할 때 자체 IP 주소 범위를 지정할 수도 있습니다. 선택한 IP 주소 범위는 서브넷과 겹치지 않고 동일한 VPC 및 라우트 테이블을 가진 다른 파일 시스템에서 이미 사용하고 있지 않다면 VPC의 IP 주소 범위 내부 또는 외부에 위치할 수 있습니다. 이 옵션의 경우 VPC의 IP 주소 범위 내에 있는 범위를 사용하는 것이 좋습니다.

AWS Transit Gateway는 유동 IP 주소로의 라우팅만 지원하며, 이를 전이적 피어링이라고도 합니다. VPC 피어링 AWS Direct Connect, 및 AWS VPN 는 전이적 피어링을 지원하지 않습니다. 따라서 파일 시스템의 VPC 외부에 있는 네트워크에서 이러한 인터페이스에 액세스하려면 Transit Gateway를 사용해야 합니다.

다음 다이어그램은 액세스하는 클라이언트와 다른 VPC에 있는 다중 AZ 파일 시스템에 대한 NFS, SMB 또는 관리 액세스를 위해 Transit Gateway를 사용하는 방법을 보여줍니다.



> **Note**
>
> 사용 중인 모든 라우팅 테이블이 다중 AZ 파일 시스템에 연결되어 있는지 확인합니다. 이렇게 하면 장애 조치 중에 사용할 수 없게 되는 사태를 방지하는 데 도움이 됩니다. Amazon VPC 라우팅 테이블을 파일 시스템과 연결하는 방법에 대한 자세한 내용은 파일 시스템 업데이트 섹션을 참조하세요.

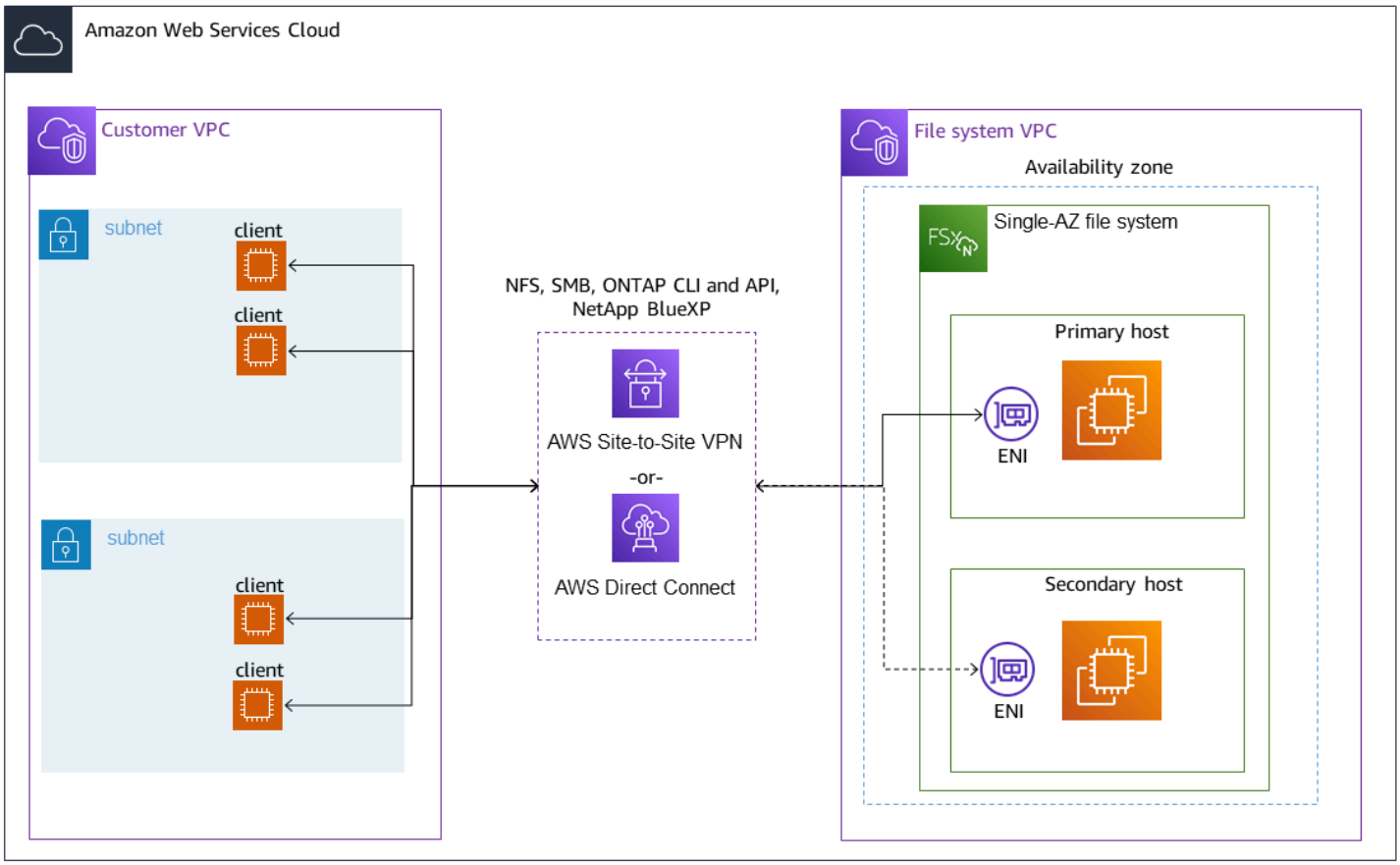
Transit Gateway를 사용하여 FSx for ONTAP 파일 시스템에 액세스해야 하는 경우에 대한 자세한 내용은 Transit Gateway가 필요한 경우 섹션을 참조하세요.

Amazon FSx는 태그 기반 인증을 사용하여 Multi-AZ 파일 시스템의 VPC 라우팅 테이블을 관리합니다. 이러한 라우팅 테이블은 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정됩니다. 를 사용하여 FSx for ONTAP 다중 AZ 파일 시스템을 생성하거나 업데이트할 때는 `Key: AmazonFSx; Value: ManagedByAmazonFSx` 태그를 수동으로 추가하는 것이 AWS CloudFormation 좋습니다.

단일 AZ 파일 시스템의 NFS, SMB 또는 ONTAP CLI 및 API 액세스

NFS 또는 SMB를 통해 FSx for ONTAP 단일 AZ 파일 시스템에 액세스하고 ONTAP CLI 또는 REST API를 사용하여 파일 시스템을 관리하는 데 사용되는 엔드포인트는 활성 파일 서버의 ENI 상의 보조 IP 주소입니다. 보조 IP 주소는 VPC의 CIDR 범위 내에 있으므로 클라이언트는 VPC 피어링 AWS Direct Connect을 사용하거나 필요 AWS VPN 없이 데이터 및 관리 포트에 액세스할 수 있습니다 AWS Transit Gateway.

다음 다이어그램은 AWS VPN 액세스하는 클라이언트와 다른 VPC에 있는 단일 AZ 파일 시스템에 AWS Direct Connect 대한 NFS, SMB 또는 관리 액세스에 또는를 사용하는 방법을 보여줍니다.



Transit Gateway가 필요한 경우

다중 AZ 파일 시스템에 Transit Gateway가 필요한지 여부는 파일 시스템 데이터에 액세스하는 데 사용하는 방법에 따라 다릅니다. 단일 AZ 파일 시스템에는 Transit Gateway가 필요하지 않습니다. 다음 표에서는 다중 AZ 파일 시스템에 액세스하는 데 AWS Transit Gateway 를 사용해야 하는 경우를 설명합니다.

데이터 액세스	Transit Gateway가 필요한 경우
NFS, SMB 또는 NetApp ONTAP REST API, CLI 또는 BlueXP를 통해 FSx에 액세스	다음과 같은 경우에만 해당됩니다. • 피어링된(예: 온프레미스) 네트워크에서 액세스하는 경우 • NetApp FlexCache 또는 Global File Cache 인스턴스를 통해 FSx에 액세스하지 않는 경우
iSCSI를 통한 데이터 액세스	아니요

데이터 액세스	Transit Gateway가 필요한 경우
NVMe를 통한 데이터 액세스	아니요
Active Directory에 SVM 조인	아니요
SnapMirror	아니요
FlexCache 캐싱	아니요
Global File Cache	아니요

배포 VPC 외부에서 NVMe, iSCSI 및 클러스터 간 엔드포인트에 액세스하기

VPC 피어링 또는 AWS Transit Gateway 를 사용하여 파일 시스템의 배포 VPC 외부에서 파일 시스템의 NVMe, iSCSI 및 클러스터 간 엔드포인트에 액세스할 수 있습니다. VPC 피어링을 사용하여 VPC 간에 NVMe, iSCSI 및 클러스터 간 트래픽을 라우팅할 수 있습니다. VPC 피어링 연결은 두 VPC 사이의 네트워킹 연결이며, 프라이빗 IPv4 주소를 사용하여 두 VPC 간에 트래픽을 라우팅하는 데 사용됩니다. VPC 피어링을 사용하여 동일한 내에서 AWS 리전 또는 서로 다른 간에 VPCs를 연결할 수 있습니다 AWS 리전. 자세한 내용은 Amazon VPC 피어링 가이드의 VPC 피어링이란? 섹션을 참조하세요.

온프레미스에서 데이터 액세스

온프레미스에서AWS VPN 및 AWS Direct Connect를 사용하여 FSx for ONTAP 파일 시스템에 액세스할 수 있습니다. 보다 구체적인 사용 사례 지침은 다음 섹션에서 확인할 수 있습니다. 온프레미스에서 다양한 FSx for ONTAP 리소스에 액세스하기 위해서는 아래 나열된 요구 사항 외에도 파일 시스템의 VPC 보안 그룹이 파일 시스템과 클라이언트 간에 데이터 흐름을 허용하는지 확인해야 합니다. 필요한 포트 목록은 Amazon VPC 보안 그룹을 참조하세요.

온프레미스에서 NFS, SMB, ONTAP CLI 및 REST API 엔드포인트에 액세스하기

이 섹션에서는 온프레미스 네트워크에서 FSx for ONTAP 파일 시스템의 NFS, SMB 및 ONTAP 관리 포트에 액세스하는 방법에 대해 설명합니다.

온프레미스에서 Multi-AZ 파일 시스템에 액세스하기

Amazon FSx를 사용하려면 AWS Transit Gateway 온프레미스 네트워크에서 다중 AZ 파일 시스템에 액세스하도록 원격 NetApp Global File Cache 또는 NetApp FlexCache를 사용하거나 구성해야 합니다. Multi-AZ 파일 시스템의 가용성 영역 전반에서 장애 조치를 지원하기 위해 Amazon FSx는 NFS, SMB 및 ONTAP 관리 엔드포인트에 사용되는 인터페이스에 플로팅 IP 주소를 사용합니다.

NFS, SMB 및 관리 엔드포인트는 부동 IP 주소를 사용하기 때문에 온프레미스 네트워크에서 이러한 인터페이스 AWS VPN 에 액세스하려면 AWS Direct Connect 또는와 AWS Transit Gateway 함께를 사용해야 합니다. 이러한 인터페이스에 사용되는 유동 IP 주소는 다중 AZ 파일 시스템을 생성할 때 지정한 `EndpointIpAddressRange` 내에 있습니다. `EndpointIpAddressRange`는 파일 시스템 생성 방법에 따라 다음 주소 범위를 사용합니다.

- 기본적으로 Amazon FSx 콘솔을 사용하여 생성된 다중 AZ 파일 시스템은 파일 시스템의 `EndpointIpAddressRange`에 VPC 기본 CIDR 범위의 마지막 64개 IP 주소를 사용합니다.
- AWS CLI 또는 Amazon FSx API를 사용하여 생성된 다중 AZ 파일 시스템은 `EndpointIpAddressRange` 기본적으로에 대한 주소 블록 내의 IP `198.19.0.0/16` 주소 범위를 사용합니다.
- Amazon FSx 콘솔에서 표준 생성 옵션을 사용할 때 자체 IP 주소 범위를 지정할 수도 있습니다. 선택한 IP 주소 범위는 서브넷과 겹치지 않고 동일한 VPC 및 라우팅 테이블을 가진 다른 파일 시스템에서 아직 사용하지 않는 한 VPC의 IP 주소 범위 내부 또는 외부에 있을 수 있습니다. 이 옵션의 경우 VPC의 IP 주소 범위 내에 있는 범위를 사용하는 것이 좋습니다.

유동 IP 주소는 장애 조치가 필요한 경우 클라이언트를 대기 파일 시스템으로 원활하게 전환할 수 있도록 하는 데 사용됩니다. 자세한 내용은 FSx for ONTAP의 장애 조치 프로세스 섹션을 참조하세요.

> **Important**
>
> Transit Gateway를 사용하여 다중 AZ 파일 시스템에 액세스하려면 라우팅 테이블이 파일 시스템과 연결된 서브넷에 각 Transit Gateway Attachment를 생성해야 합니다.

자세한 내용은 온프레미스에서 Multi-AZ 파일 시스템에 액세스하도록 라우팅 구성 단원을 참조하십시오.

온프레미스에서 단일 AZ 파일 시스템에 액세스

를 사용하여 온프레미스 네트워크에서 데이터에 액세스 AWS Transit Gateway 해야 하는 요구 사항은 단일 AZ 파일 시스템에는 존재하지 않습니다. 단일 AZ 파일 시스템은 단일 서브넷에 배포되며 노드 간 장애 조치를 제공하는 데 유동 IP 주소가 필요하지 않습니다. 대신 단일 AZ 파일 시스템에서 액세스하는 IP 주소는 파일 시스템의 VPC CIDR 범위 내의 보조 IP 주소로 구현되므로 AWS Transit Gateway의 필요 없이 다른 네트워크에서 데이터에 액세스할 수 있습니다.

온프레미스에서 클러스터 간 엔드포인트에 액세스

FSx for ONTAP의 클러스터 간 엔드포인트는 온프레미스 NetApp 배포와 FSx for ONTAP 사이를 포함하여 NetApp ONTAP 파일 시스템 간의 복제 트래픽 전용입니다. 복제 트래픽에는 다양한 파일 시스템에서의 스토리지 가상 머신(SVM) 및 볼륨과 NetApp Global File Cache 간의 SnapMirror, FlexCache, FlexClone 관계가 포함됩니다. 클러스터 간 엔드포인트는 Active Directory 트래픽에도 사용됩니다.

파일 시스템의 클러스터 간 엔드포인트는 FSx for ONTAP 파일 시스템을 생성할 때 제공하는 VPC의 CIDR 범위 내에 있는 IP 주소를 사용하므로 온프레미스와 AWS 클라우드사이의 클러스터 간 트래픽을 라우팅하는 데 Transit Gateway를 사용할 필요가 없습니다. 그러나 온프레미스 클라이언트는 여전히 AWS VPN 또는 AWS Direct Connect 를 사용하여 VPC에 대한 보안 연결을 설정해야 합니다.

자세한 내용은 온프레미스에서 Multi-AZ 파일 시스템에 액세스하도록 라우팅 구성 단원을 참조하십시오.

VPC 외부에서 Multi-AZ 파일 시스템에 액세스하도록 라우팅 구성

VPC의 IP 주소 범위를 벗어나`EndpointIPAddressRange`는가 있는 다중 AZ 파일 시스템이 있는 경우 피어링된 네트워크 또는 온프레미스 네트워크에서 파일 시스템에 액세스하려면에서 추가 라우팅 AWS Transit Gateway 을 설정해야 합니다.

> **Important**
>
> Transit Gateway를 사용하여 다중 AZ 파일 시스템에 액세스하려면 라우팅 테이블이 파일 시스템과 연결된 서브넷에 각 Transit Gateway Attachment를 생성해야 합니다.

> **Note**
>
> VPC의 IP 주소 범위 내에 속하는 EndpointIPAddressRange의 단일 AZ 파일 시스템 또는 다중 AZ 파일 시스템에는 추가 Transit Gateway 구성이 필요하지 않습니다.

를 사용하여 라우팅을 구성하려면 AWS Transit Gateway

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 피어링된 네트워크에서 액세스를 구성할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 네트워크 및 보안에서 엔드포인트 IP 주소 범위를 복사합니다.
4. 이 IP 주소 범위로 향하는 트래픽을 파일 시스템의 VPC로 라우팅하는 Transit Gateway 경로를 추가합니다. 자세한 내용은 Amazon VPC Transit Gateways의 전송 게이트웨이 작업을 참조하세요.
5. 피어링된 네트워크에서 FSx for ONTAP 파일 시스템에 액세스할 수 있는지 확인합니다.

파일 시스템에 라우팅 테이블을 추가하려면 파일 시스템 업데이트 섹션을 참조하세요.

> **Note**
>
> 관리, NFS 및 SMB 엔드포인트의 DNS 레코드는 파일 시스템과 동일한 VPC 내에서만 확인할 수 있습니다. 볼륨을 마운트하거나 다른 네트워크에서 관리 포트에 연결하려면 엔드포인트의 IP 주소를 사용해야 합니다. 이러한 IP 주소는 시간이 지나도 변경되지 않습니다.

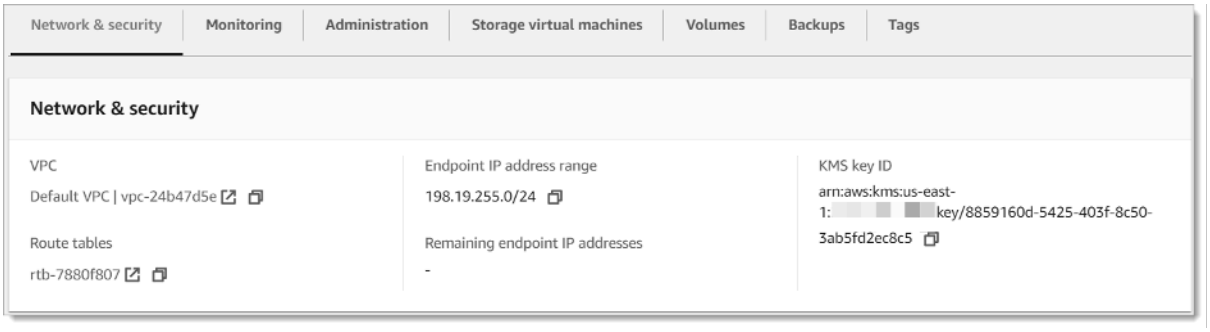
온프레미스에서 Multi-AZ 파일 시스템에 액세스하도록 라우팅 구성

온프레미스에서 다중 AZ 파일 시스템에 AWS Transit Gateway 액세스하도록를 구성하려면

VPC의 CIDR 범위를 벗어나EndpointIPAddressRange는가 있는 다중 AZ 파일 시스템이 있는 경우 피어링된 네트워크 또는 온프레미스 네트워크에서 파일 시스템에 액세스하려면에서 추가 라우팅 AWS Transit Gateway 을 설정해야 합니다.

> **Note**
>
> VPC의 IP 주소 범위 내에 속하는 EndpointIPAddressRange의 단일 AZ 파일 시스템 또는 다중 AZ 파일 시스템에는 추가 Transit Gateway 구성이 필요하지 않습니다.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 피어링된 네트워크에서 액세스를 구성할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 네트워크 및 보안에서 엔드포인트 IP 주소 범위를 복사합니다.



4. 이 IP 주소 범위로 향하는 트래픽을 파일 시스템의 VPC로 라우팅하는 Transit Gateway 경로를 추가합니다. 자세한 내용은 Amazon VPC Transit Gateways 사용 설명서의 전송 게이트웨이 작업을 참조하세요.
5. 피어링된 네트워크에서 FSx for ONTAP 파일 시스템에 액세스할 수 있는지 확인합니다.

> **Important**
>
> Transit Gateway를 사용하여 다중 AZ 파일 시스템에 액세스하려면 라우팅 테이블이 파일 시스템과 연결된 서브넷에 각 Transit Gateway Attachment를 생성해야 합니다. 별도의 Transit Gateway 연결 서브넷이 있는 경우 해당 서브넷의 라우팅 테이블도 Amazon FSx 엔드포인트 주소로 업데이트되도록 Amazon FSx와 연결해야 합니다.

파일 시스템에 라우팅 테이블을 추가하려면 파일 시스템 업데이트 섹션을 참조하세요.

Linux 클라이언트에 볼륨 탑재

Linux 클라이언트와 함께 마운트하려는 볼륨의 보안 스타일 설정은 `UNIX` 또는 `mixed`로 설정하는 것이 좋습니다. 자세한 내용은 FSx for ONTAP 볼륨 관리 단원을 참조하십시오.

> **Note**
>
> 기본적으로 FSx for ONTAP NFS 마운트는 `hard` 마운트입니다. 장애 발생 시 원활한 장애 조치를 위해 기본 `hard` 마운트 옵션을 사용하는 것이 좋습니다.

Linux 클라이언트에 ONTAP 볼륨 마운트

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 파일 시스템과 동일한 VPC에 있는 Amazon Linux 2를 실행하는 Amazon EC2 인스턴스를 생성하거나 선택합니다.

   EC2 Linux 인스턴스 시작에 대한 자세한 내용은 Amazon EC2 사용 설명서의 1단계: 인스턴스 시작하기를 참조하세요.
3. Amazon EC2 Linux 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하세요.
4. Secure Shell(SSH)을 사용하여 EC2 인스턴스에서 터미널을 열고 적절한 보안 인증으로 로그인합니다.
5. 다음과 같이 SVM 볼륨을 마운트할 디렉터리를 EC2 인스턴스에 생성합니다.

   ```
   sudo mkdir /fsx
   ```
6. 다음 명령을 사용하여 생성한 디렉터리에 볼륨을 마운트합니다.

   ```
   sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
   ```

   다음 예제는 샘플 값을 사용합니다.

   ```
   sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
   east-1.amazonaws.com:/vol1 /fsx
   ```

   DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다. DNS 이름을 사용하여 2세대 파일 시스템에 클라이언트를 탑재하는 것이 좋습니다. 클라이언트가 파일 시스템의 고가용성(HA) 페어 간에 균형을 이룰 수 있도록 하기 때문입니다.

   ```
   sudo mount -t nfs 198.51.100.1:/vol1 /fsx
   ```

   > **Note**
   >
   > 2세대 파일 시스템의 경우 병렬 NFS(pNFS) 프로토콜이 기본적으로 활성화되어 있으며 NFS v4.1 이상의 볼륨을 탑재하는 모든 클라이언트에 기본적으로 사용됩니다.

/etc/fstab을 사용하여 인스턴스 재부팅 시 자동으로 마운트

Amazon EC2 Linux 인스턴스가 재부팅될 때 FSx for ONTAP 볼륨을 자동으로 다시 마운트하려면 `/etc/fstab` 파일을 사용합니다. `/etc/fstab` 파일에는 파일 시스템에 대한 정보가 들어 있습니다. 인스턴스 시작 중에 실행되는 `mount -a` 명령은 `/etc/fstab`에 나열된 파일 시스템을 마운트합니다.

> **Note**
>
> FSx for ONTAP 파일 시스템은 Amazon EC2 Mac 인스턴스에서 `/etc/fstab`를 사용하는 자동 마운트를 지원하지 않습니다.

> **Note**
>
> EC2 인스턴스의 `/etc/fstab` 파일을 업데이트하려면 FSx for ONTAP 파일 시스템을 미리 만들어 두어야 합니다. 자세한 내용은 파일 시스템 만들기 섹션을 참조하세요.

EC2 인스턴스의 /etc/fstab 파일 업데이트

1. EC2 인스턴스에 연결합니다.

   - MacOS 또는 Linux를 실행하는 컴퓨터에서 인스턴스에 연결하려면 SSH 명령에 대해 .pem 파일을 지정합니다. 이렇게 하려면 `-i` 옵션 및 프라이빗 키의 경로를 사용합니다.
   - Windows를 실행 중인 컴퓨터에서 인스턴스에 연결하려면 MindTerm 또는 PuTTY를 사용합니다. PuTTY를 사용하려면 설치하고 .pem 파일을 .ppk 파일로 변환합니다.

   자세한 내용은 Amazon EC2 사용 설명서에서 다음 주제를 참조하세요.

   - SSH를 사용하여 Linux 인스턴스에 연결
   - PuTTY를 사용하여 Windows에서 Linux 인스턴스에 연결
2. SVM 볼륨을 마운트하는 데 사용할 로컬 디렉터리를 생성합니다.

   ```
   sudo mkdir /fsx
   ```
3. 원하는 편집기에서 `/etc/fstab` 파일을 엽니다.
4. `/etc/fstab` 파일에 다음 줄을 추가합니다. 각 파라미터 사이에 탭 문자를 삽입합니다. 줄 바꿈 없이 한 줄로 표시되어야 합니다.

```
svm-dns-name:volume-junction-path /fsx nfs nfsvers=version,defaults 0 0
```

볼륨 SVM의 IP 주소를 사용할 수도 있습니다. 마지막 세 파라미터는 NFS 옵션(기본값으로 설정), 파일 시스템 덤핑 및 파일 시스템 검사(이들은 일반적으로 사용되지 않으므로 0으로 설정)를 나타냅니다.

5. 파일 변경 사항을 저장합니다.
6. 이제 다음 명령을 사용하여 파일 공유를 마운트합니다. 다음 번에 시스템을 시작하면 폴더가 자동으로 마운트됩니다.

```
sudo mount /fsx
sudo mount svm-dns-name:volume-junction-path
```

이제 EC2 인스턴스가 다시 시작될 때마다 ONTAP 볼륨을 마운트하도록 구성되었습니다.

Microsoft Windows 클라이언트에 볼륨 탑재

이 섹션에서는 Microsoft Windows 운영 체제를 실행하는 클라이언트를 사용하여 FSx for ONTAP 파일 시스템의 데이터에 액세스하는 방법을 설명합니다. 사용 중인 클라이언트 유형과 관계없이 다음 요구 사항을 검토합니다.

이 절차에서는 클라이언트와 파일 시스템이 동일한 VPC 및 AWS 계정에 있는 것으로 가정합니다. 클라이언트가 온프레미스 또는 다른 VPC, AWS 계정또는에 있는 경우 AWS 리전이 절차에서는 AWS Transit Gateway 또는를 사용하여 전용 네트워크 연결을 설정했거나 AWS Direct Connect 를 사용하여 프라이빗 보안 터널을 설정했다고 가정합니다 AWS Virtual Private Network. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.

SMB 프로토콜을 사용하여 Windows 클라이언트에 볼륨을 연결하는 것이 좋습니다.

사전 조건

Microsoft Windows 클라이언트를 사용하여 ONTAP 스토리지 볼륨에 액세스하려면 다음 사전 조건을 충족해야 합니다.

- 연결하려는 볼륨의 SVM을 조직의 Active Directory에 조인하거나 워크그룹을 사용해야 합니다. Active Directory에 SVM 조인에 대한 자세한 내용은 FSx for ONTAP 스토리지 가상 머신 관리 섹션을 참조하세요. 작업 그룹 사용에 대한 자세한 내용은 섹션을 참조하세요작업 그룹에서 SMB 서버 설정.

- 연결 중인 볼륨의 보안 스타일 설정은 NTFS 또는 mixed입니다. 자세한 내용은 볼륨 보안 스타일 단원을 참조하십시오.

SMB 및 Active Directory를 사용하여 Windows 클라이언트에 볼륨을 마운트하려면 다음과 같이 하세요.

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 파일 시스템과 동일한 VPC에 있고 볼륨의 SVM과 동일한 Microsoft Active Directory에 조인되어 있으며 Microsoft Windows를 실행하는 Amazon EC2 인스턴스를 만들거나 선택합니다.

   인스턴스 시작에 대한 자세한 내용은 Amazon EC2 사용 설명서의 1단계: 인스턴스 시작하기를 참조하세요.

   Active Directory에 SVM 조인에 대한 자세한 내용은 FSx for ONTAP 스토리지 가상 머신 관리 섹션을 참조하세요.
3. Amazon EC2 Windows 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하세요.
4. 명령 프롬프트를 엽니다.
5. 다음 명령을 실행합니다. 다음을 바꿉니다.

   - `Z:`를 사용 가능한 드라이브 문자로 바꿉니다.
   - `DNS_NAME`을 볼륨의 SVM에 대한 SMB 엔드포인트의 DNS 이름 또는 IP 주소로 바꿉니다.
   - `SHARE_NAME`를 SMB 공유의 이름으로 바꿉니다. `C$`는 SVM 네임스페이스의 루트에 있는 기본 SMB 공유이지만, 스토리지를 루트 볼륨에 노출시켜 보안 및 서비스 중단을 일으킬 수 있으므로 마운트하지 않아야 합니다. `C$` 대신 탑재할 SMB 공유 이름을 제공해야 합니다. SMB 공유 생성에 대한 자세한 내용은 SMB 공유 관리 섹션을 참조하세요.

```
net use Z: \\DNS_NAME\SHARE_NAME
```

   다음 예제는 샘플 값을 사용합니다.

```
net use Z: \\corp.example.com\group_share
```

   DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다. DNS 이름을 사용하여 2세대 파일 시스템에 클라이언트를 탑재하는 것이 좋습니다. 클라이언트가 파일 시스템의 고가용성(HA) 페어 간에 균형을 이룰 수 있도록 하기 때문입니다.

```
net use Z: \\198.51.100.5\group_share
```

MacOS 클라이언트에서 볼륨 탑재

이 섹션에서는 MacOS 운영 체제를 실행하는 클라이언트를 사용하여 FSx for ONTAP 파일 시스템의 데이터에 액세스하는 방법을 설명합니다. 사용 중인 클라이언트 유형과 관계없이 다음 요구 사항을 검토합니다.

이 절차에서는 클라이언트와 파일 시스템이 동일한 VPC 및 AWS 계정에 있는 것으로 가정합니다. 클라이언트가 온프레미스 또는 다른 VPC에 있는 경우 AWS 계정 또는 AWS Transit Gateway 를 사용하여 전용 네트워크 연결을 설정 AWS Direct Connect 했거나를 사용하여 프라이빗 보안 터널을 설정 AWS 리전했습니다 AWS Virtual Private Network. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.

SMB 프로토콜을 사용하여 Mac 클라이언트에 볼륨을 연결하는 것이 좋습니다.

SMB를 사용하여 MacOS 클라이언트에 ONTAP 볼륨 마운트

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 파일 시스템과 동일한 VPC에 있는 MacOS를 실행하는 Amazon EC2 Mac 인스턴스를 생성하거나 선택합니다.

   인스턴스 시작에 대한 자세한 내용은 Amazon EC2 사용 설명서의 1단계: 인스턴스 시작하기를 참조하세요.
3. Amazon EC2 Mac 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하세요.
4. Secure Shell(SSH)을 사용하여 EC2 인스턴스에서 터미널을 열고 적절한 보안 인증으로 로그인합니다.
5. 다음과 같이 볼륨을 마운트할 디렉터리를 EC2 인스턴스에 생성합니다.

   ```
   sudo mkdir /fsx
   ```
6. 다음 명령을 사용하여 볼륨을 마운트합니다.

   ```
   sudo mount -t smbfs filesystem-dns-name:/smb-share-name mount-point
   ```

다음 예제는 샘플 값을 사용합니다.

```
sudo mount -t smbfs svm-01234567890abcde2.fs-01234567890abcde5.fsx.us-
east-1.amazonaws.com:/C$ /fsx
```

DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다. DNS 이름을 사용하여 2세대 파일 시스템에 클라이언트를 탑재하는 것이 좋습니다. 클라이언트가 파일 시스템의 고가용성(HA) 페어 간에 균형을 이룰 수 있도록 하기 때문입니다.

```
sudo mount -t smbfs 198.51.100.10:/C$ /fsx
```

C$는 SVM 네임스페이스의 루트를 확인하기 위해 마운트할 수 있는 기본 SMB 공유입니다. SVM에 Server Message Block(SMB)공유를 생성한 경우 C$ 대신 SMB 공유 이름을 제공합니다. SMB 공유 생성에 대한 자세한 내용은 SMB 공유 관리 섹션을 참조하세요.

NFS를 사용하여 MacOS 클라이언트에 ONTAP 볼륨 마운트

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 파일 시스템과 동일한 VPC에 있는 Amazon Linux 2를 실행하는 Amazon EC2 인스턴스를 생성하거나 선택합니다.

   EC2 Linux 인스턴스 시작에 대한 자세한 내용은 Amazon EC2 사용 설명서의 1단계: 인스턴스 시작하기를 참조하세요.
3. Amazon EC2 Linux 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하세요.
4. 인스턴스 시작 중에 사용자 데이터 스크립트를 사용하거나 다음 명령을 실행하여 Linux EC2 인스턴스에 FSx for ONTAP 볼륨을 마운트합니다.

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /mount-
   point
   ```

   다음 예제는 샘플 값을 사용합니다.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다. DNS 이름을 사용하여 2세대 파일 시스템에 클라이언트를 탑재하는 것이 좋습니다. 클라이언트가 파일 시스템의 HA 페어 간에 균형을 이룰 수 있도록 하기 때문입니다.

```
sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
```

5. 생성한 디렉터리에 다음 명령을 사용하여 볼륨을 마운트합니다.

```
sudo mount -t nfs svm-dns-name:/volume-junction-path /fsx
```

다음 예제는 샘플 값을 사용합니다.

```
sudo mount -t nfs svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-
east-1.amazonaws.com:/vol1 /fsx
```

DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다. DNS 이름을 사용하여 2세대 파일 시스템에 클라이언트를 탑재하는 것이 좋습니다. 클라이언트가 파일 시스템의 고가용성(HA) 페어 간에 균형을 이룰 수 있도록 하기 때문입니다.

```
sudo mount -t nfs 198.51.100.1:/vol1 /fsx
```

Linux용 iSCSI 프로비저닝

FSx for ONTAP는 iSCSI 프로토콜을 지원합니다. iSCSI 프로토콜을 사용하여 클라이언트와 파일 시스템 간에 데이터를 전송하려면 Linux 클라이언트와 파일 시스템 모두에서 iSCSI를 프로비저닝해야 합니다. iSCSI 프로토콜은 고가용성 페어(HA)가 6개 이하인 모든 파일 시스템에서 사용할 수 있습니다.

Amazon FSx for NetApp ONTAP에서 iSCSI를 구성하는 세 가지 주요 단계는 다음 절차에서 다룹니다.

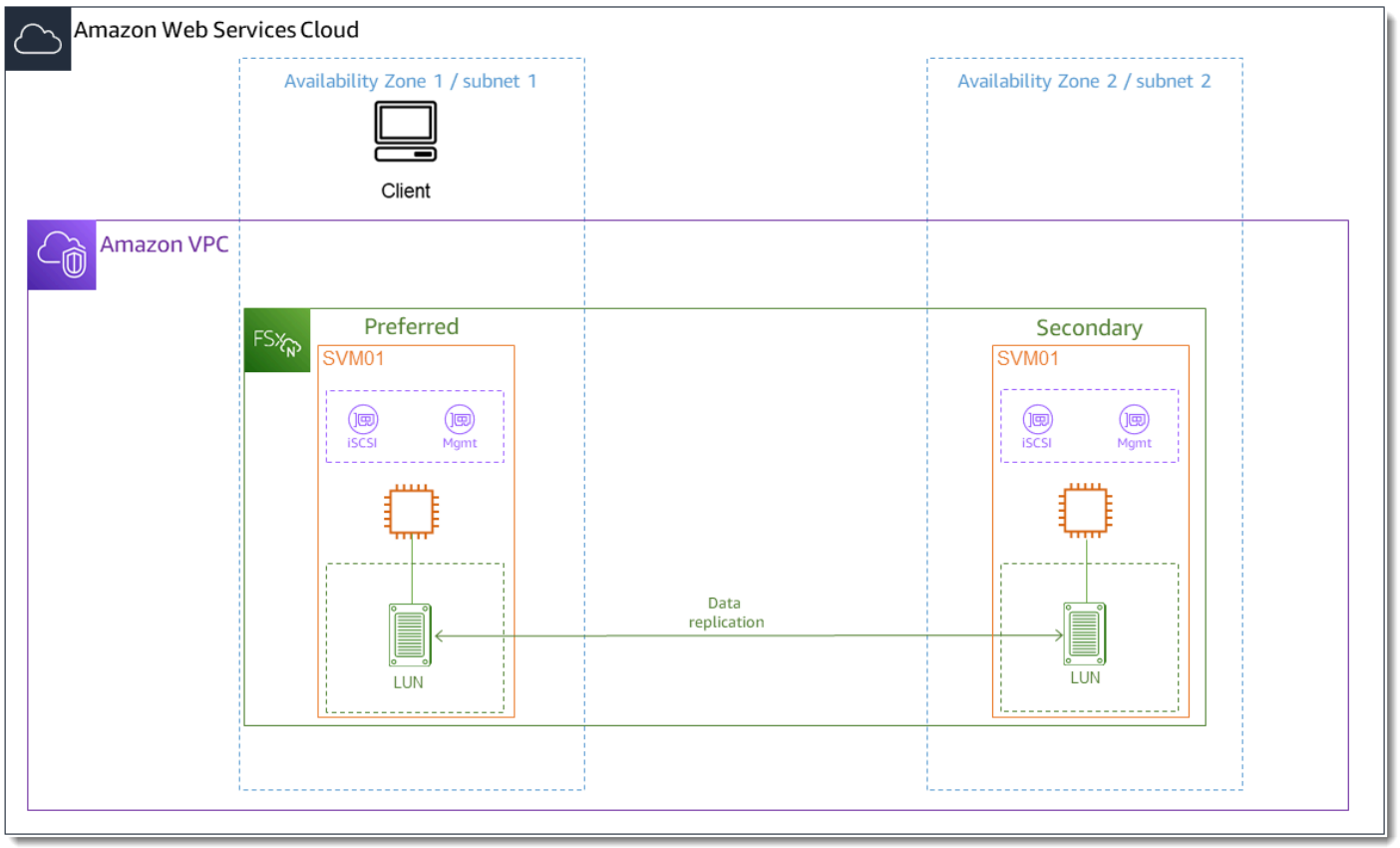
1. Linux 호스트에 iSCSI 클라이언트를 설치하고 구성합니다.
2. 파일 시스템의 SVM에서 iSCSI를 구성합니다.
   - iSCSI 이니시에이터 그룹을 생성합니다.
   - 이니시에이터 그룹을 LUN에 매핑합니다.
3. Linux 클라이언트에 iSCSI LUN 마운트

시작하기 전 준비 사항

iSCSI용 파일 시스템을 구성하는 프로세스를 시작하기 전에 다음 항목을 완료해야 합니다.

- FSx for ONTAP 파일 시스템을 생성합니다. 자세한 내용은 파일 시스템 만들기 단원을 참조하십시오.
- 파일 시스템에서 iSCSI LUN을 생성합니다. 자세한 내용은 iSCSI LUN 생성 단원을 참조하십시오.
- 파일 시스템과 동일한 VPC에서 Amazon Linux 2 AMI(Amazon 머신 이미지)를 실행하는 EC2 인스턴스를 생성합니다. iSCSI를 구성하고 파일 데이터에 액세스할 Linux 호스트입니다.

  이러한 절차의 범위를 벗어나 호스트가 다른 VPC에 있는 경우 VPC 피어링을 사용하거나 다른 VPCs AWS Transit Gateway 에 볼륨의 iSCSI 엔드포인트에 대한 액세스 권한을 부여할 수 있습니다. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.
- Amazon VPC를 사용한 파일 시스템 액세스 제어에 설명된 대로 인바운드 및 아웃바운드 트래픽을 허용하도록 Linux 호스트의 VPC 보안 그룹을 구성합니다.
- ONTAP CLI에 액세스하는 데 사용할 `fsxadmin` 권한이 있는 ONTAP 사용자의 자격 증명을 가져옵니다. 자세한 내용은 ONTAP 사용자 및 역할 단원을 참조하십시오.
- iSCSI용으로 구성하고 FSx for ONTAP 파일 시스템에 액세스하는 데 사용할 Linux 호스트는 동일한 VPC와 AWS 계정에 있습니다.
- 다음 그림과 같이 EC2 인스턴스는 파일 시스템의 기본 서브넷과 동일한 가용 영역에 배치하는 것이 좋습니다.



EC2 인스턴스가 Amazon Linux 2과 다른 Linux AMI를 실행하는 경우 이러한 절차 및 예제에 사용된 일부 유틸리티가 이미 설치되어 있을 수 있으며, 다른 명령을 사용하여 필요한 패키지를 설치할 수 있습니다. 패키지 설치 외에도 이 섹션에 사용된 명령은 다른 EC2 Linux AMI에도 유효합니다.

주제

- Linux 호스트에 iSCSI 설치 및 구성
- FSx for ONTAP 파일 시스템에 iSCSI 구성
- Linux 클라이언트에 iSCSI LUN 마운트

Linux 호스트에 iSCSI 설치 및 구성

iSCSI 클라이언트 설치

1. Linux 디바이스에 `iscsi-initiator-utils` 및 `device-mapper-multipath`가 설치되어 있는지 확인합니다. SSH 클라이언트를 사용하여 Linux 인스턴스에 연결합니다. 자세한 내용은 SSH를 사용하여 Linux 인스턴스에 연결을 참조하세요.

2. 다음 명령을 사용하여 multipath와 iSCSI 클라이언트를 설치하세요. 파일 서버 간에 자동으로 장애 조치하려면 multipath를 설치해야 합니다.

```
~$ sudo yum install -y device-mapper-multipath iscsi-initiator-utils
```

3. multipath를 사용하는 경우 파일 서버 간에 자동으로 장애 조치할 때 응답 속도를 높이려면 /etc/iscsi/iscsid.conf 파일의 대체 제한 시간 값을 기본값인 120 대신 5로 설정합니다.

```
~$ sudo sed -i 's/node.session.timeo.replacement_timeout = .*/
node.session.timeo.replacement_timeout = 5/' /etc/iscsi/iscsid.conf; sudo cat /etc/
iscsi/iscsid.conf | grep node.session.timeo.replacement_timeout
```

4. iSCSI 서비스를 시작합니다.

```
~$ sudo service iscsid start
```

단, Linux 버전에 따라 다음 명령을 대신 사용해야 할 수도 있습니다.

```
~$ sudo systemctl start iscsid
```

5. 다음 명령을 사용하여 에이전트가 실행 중인지 확인합니다.

```
~$ sudo systemctl status iscsid.service
```

시스템이 다음 출력으로 응답합니다.

```
iscsid.service - Open-iSCSI
    Loaded: loaded (/usr/lib/systemd/system/iscsid.service; disabled; vendor
 preset: disabled)
    Active: active (running) since Fri 2021-09-02 00:00:00 UTC; 1min ago
    Docs: man:iscsid(8)
    man:iscsiadm(8)
    Process: 14658 ExecStart=/usr/sbin/iscsid (code=exited, status=0/SUCCESS)
    Main PID: 14660 (iscsid)
    CGroup: /system.slice/iscsid.service
    ##14659 /usr/sbin/iscsid
    ##14660 /usr/sbin/iscsid
```

Linux 클라이언트에 iSCSI 구성

1. 클라이언트가 파일 서버 간에 자동으로 장애 조치할 수 있도록 하려면 다중 경로를 구성해야 합니다. 다음 명령을 사용합니다.

```
~$ sudo mpathconf --enable --with_multipathd y
```

2. 다음 명령을 사용하여 Linux 호스트의 이니시에이터 이름을 확인합니다. 이니시에이터 이름의 위치는 iSCSI 유틸리티에 따라 다릅니다. `iscsi-initiator-utils`를 사용하는 경우 이니시에이터 이름은 `/etc/iscsi/initiatorname.iscsi` 파일에 있습니다.

```
~$ sudo cat /etc/iscsi/initiatorname.iscsi
```

시스템이 이니시에이터 이름으로 응답합니다.

```
InitiatorName=iqn.1994-05.com.redhat:abcdef12345
```

FSx for ONTAP 파일 시스템에 iSCSI 구성

1. 다음 명령을 사용하여 iSCSI LUN을 생성한 FSx for ONTAP 파일 시스템의 NetApp ONTAP CLI에 연결합니다. 자세한 내용은 NetApp ONTAP CLI 사용 섹션을 참조하세요.

```
~$ ssh fsxadmin@your_management_endpoint_ip
```

2. NetApp ONTAP CLI lun igroup create 명령을 사용하여 이니시에이터 그룹(`igroup`)을 생성합니다. 이니시에이터 그룹은 iSCSI LUN에 매핑되며 LUN에 액세스할 수 있는 이니시에이터(클라이언트)를 제어합니다. `host_initiator_name`을 이전 절차에서 검색한 Linux 호스트의 이니시에이터 이름으로 바꿉니다.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype linux
```

이 igroup에 매핑된 LUN을 여러 호스트에서 사용할 수 있도록 하려면 여러 이니시에이터 이름을 쉼표로 구분하여 지정할 수 있습니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 lun igroup 생성을 참조하세요.

3. lun igroup show 명령을 사용하여 `igroup`이 존재하는지 확인합니다.

```
::> lun igroup show
```

시스템이 다음 출력으로 응답합니다.

```
Vserver   Igroup       Protocol OS Type  Initiators
--------- ------------ -------- -------- ------------------------------------
svm_name  igroup_name  iscsi    linux    iqn.1994-05.com.redhat:abcdef12345
```

4. 이 단계에서는 이미 iSCSI LUN을 생성한 것으로 가정합니다. 아직 생성되지 않은 경우 단계별 지침으로 iSCSI LUN 생성 섹션을 참조하여 생성합니다.

   lun mapping create 명령을 사용해서 다음 속성을 지정하여 생성된 LUN과 생성된 igroup 사이의 매핑을 생성합니다.

   - *svm_name* – iSCSI 대상을 제공하는 스토리지 가상 머신의 이름입니다. 호스트는 이 값을 사용하여 LUN에 도달합니다.
   - *vol_name* – LUN을 호스팅하는 볼륨의 이름입니다.
   - *lun_name* – LUN에 할당한 이름입니다.
   - *igroup_name* – 이니시에이터 그룹의 이름입니다.
   - *lun_id* – LUN ID 정수는 LUN 자체가 아니라 매핑에만 해당됩니다. 이는 igroup의 이니시에이터에 의해 사용되며, 이니시에이터가 스토리지에 액세스할 때 논리 유닛 번호로 사용됩니다.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. lun show -path 명령을 사용하여 LUN이 생성되고 온라인 상태이며 매핑되었는지 확인합니다.

```
::> lun show -path /vol/vol_name/lun_name -fields state,mapped,serial-hex
```

시스템이 다음 출력으로 응답합니다.

```
 Vserver    Path                            serial-hex               state    mapped
 --------- ------------------------------- ------------------------ --------
 --------
 svm_name  /vol/vol_name/lun_name          6c5742314e5d52766e796150 online   mapped
```

serial_hex 값(이 예제에서는 6c5742314e5d52766e796150)을 저장하면, 이후 단계에서 이 값을 사용하여 블록 장치에 친숙한 이름을 만들 수 있습니다.

6. network interface show -vserver 명령을 사용하여 iSCSI LUN을 생성한 SVM의 iscsi_1 및 iscsi_2 인터페이스 주소를 검색합니다.

```
::> network interface show -vserver svm_name
```

시스템이 다음 출력으로 응답합니다.

```
            Logical                Status     Network            Current
        Current Is
Vserver     Interface              Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------             ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1                up/up      172.31.0.143/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2                up/up      172.31.21.81/20
 FSxId0123456789abcdef8-02  e0e     true
            nfs_smb_management_1
                                   up/up      198.19.250.177/20
 FSxId0123456789abcdef8-01  e0e     true
3 entries were displayed.
```

이 예제에서 iscsi_1의 IP 주소는 172.31.0.143이고 iscsi_2의 IP 주소는 172.31.21.81입니다.

Linux 클라이언트에 iSCSI LUN 마운트

Linux 클라이언트에 iSCSI LUN을 탑재하는 프로세스는 세 단계로 구성됩니다.

1. 대상 iSCSI 노드 검색
2. iSCSI LUN 분할
3. 클라이언트에 iSCSI LUN 탑재

이는 다음 절차에서 다룹니다.

대상 iSCSI 노드를 검색하려면

1. Linux 클라이언트에서 `iscsi_1`의 IP 주소인 *`iscsi_1_IP`*를 사용하여 대상 iSCSI 노드를 검색하려면 다음 명령을 사용합니다.

```
~$ sudo iscsiadm --mode discovery --op update --type sendtargets --
portal iscsi_1_IP
```

```
172.31.0.143:3260,1029
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
172.31.21.81:3260,1028
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3
```

   이 예제에서 `iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3`은 기본 가용성 영역에 있는 iSCSI LUN의 `target_initiator`에 해당합니다.

2. (선택 사항) iSCSI LUN에 대한 Amazon EC2 단일 클라이언트 최대 5Gbps(~625MBps)보다 높은 처리량을 유도하려면 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Amazon Amazon EC2 인스턴스 네트워크 대역폭에 설명된 절차에 따라 처리량을 높이기 위한 추가 세션을 설정합니다.

   다음 명령은 각 가용 영역에서 ONTAP 노드당 이니시에이터당 8개의 세션을 설정하여 클라이언트가 최대 40Gbps(5,000MBps)의 집계 처리량을 iSCSI LUN으로 구동할 수 있도록 합니다.

```
~$ sudo iscsiadm --mode node -T target_initiator --op update -n
 node.session.nr_sessions -v 8
```

3. 대상 이니시에이터에 로그인합니다. iSCSI LUN이 사용 가능한 디스크로 표시됩니다.

```
~$ sudo iscsiadm --mode node -T target_initiator --login
```

```
Logging in to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] (multiple)
Login to [iface: default, target:
 iqn.1992-08.com.netapp:sn.9cfa2c41207a11ecac390182c38bc256:vs.3, portal:
 172.31.14.66,3260] successful.
```

위 출력은 잘렸습니다. 각 파일 서버의 세션마다 `Logging in` 응답과 `Login successful` 응답이 하나씩 표시되어야 합니다. 노드당 세션이 4개인 경우 응답은 `Logging in` 8개와 `Login successful` 8개입니다.

4. 다음 명령을 사용하여 `dm-multipath`가 여러 정책이 있는 단일 LUN을 표시하여 iSCSI 세션을 식별하고 병합했는지 확인합니다. `active`로 나열된 디바이스와 `enabled`로 나열된 디바이스 수가 같아야 합니다.

```
~$ sudo multipath -ll
```

출력에서 디스크 이름은 `dm-xyz`와 같은 형식으로 지정됩니다. 여기서 `xyz`는 정수입니다. 다른 멀티패스 디스크가 없는 경우 이 값은 `dm-0`입니다.

```
3600a09806c5742314e5d52766e79614f dm-xyz NETAPP  ,LUN C-Mode
size=10G features='4 queue_if_no_path pg_init_retries 50 retain_attached_hw_handle'
 hwhandler='0' wp=rw
|-+- policy='service-time 0' prio=50 status=active
| |- 0:0:0:1 sda     8:0   active ready running
| |- 1:0:0:1 sdc     8:32  active ready running
| |- 3:0:0:1 sdg     8:96  active ready running
| `- 4:0:0:1 sdh     8:112 active ready running
`-+- policy='service-time 0' prio=10 status=enabled
  |- 2:0:0:1 sdb     8:16  active ready running
  |- 7:0:0:1 sdf     8:80  active ready running
  |- 6:0:0:1 sde     8:64  active ready running
  `- 5:0:0:1 sdd     8:48  active ready running
```

이제 블록 디바이스가 Linux 클라이언트에 연결되었습니다. 이는 `/dev/dm-xyz` 경로에 있습니다. 이 경로를 관리 목적으로 사용해서는 안 됩니다. 대신 경로 `/dev/mapper/wwid`에 있는 심볼릭 링크를 사용합니다. 여기서 `wwid`는 디바이스 간에 일관된 LUN의 고유 식별자입니다. 다음 단계에서는 다른 다중 경로 디스크와 구별할 수 있도록 `wwid`에 친숙한 이름을 지정합니다.

블록 디바이스에 표시 이름을 할당하려면

1. `/etc/multipath.conf` 파일에 별칭을 만들어 디바이스에 친숙한 이름을 지정합니다. 이렇게 하려면 선호하는 텍스트 편집기를 사용하여 다음 자리 표시자를 대체하여 파일에 다음 항목을 추가합니다.

   - `serial_hex`를 FSx for ONTAP 파일 시스템에 iSCSI 구성 절차에서 저장한 값으로 바꿉니다.

- 예제에 표시된 대로 `serial_hex` 값에 접두사 `3600a0980`을 추가합니다. 이것은Amazon FSx for NetApp ONTAP이 사용하는 NetApp ONTAP 배포판의 고유한 프리앰블입니다.
- `device_name`을 디바이스에 사용할 친숙한 이름으로 바꿉니다.

```
multipaths {
    multipath {
        wwid 3600a0980serial_hex
        alias device_name
    }
}
```

또는 다음 스크립트를 bash 파일(예: `multipath_alias.sh`)로 복사하여 저장할 수도 있습니다. *serial_hex*(3600a0980 접두사 없이) 및 *device_name*을 해당 일련 번호 및 원하는 친숙한 이름으로 바꾸어 sudo 권한을 사용하여 스크립트를 실행할 수 있습니다. 이 스크립트는 `/etc/multipath.conf` 파일에서 주석이 없는 `multipaths` 섹션을 검색합니다. 해당 항목이 있으면 해당 섹션에 `multipath` 항목이 추가됩니다. 없으면 블록 디바이스에 `multipath` 항목이 있는 새 `multipaths` 섹션이 생성됩니다.

```
#!/bin/bash
SN=serial_hex
ALIAS=device_name
CONF=/etc/multipath.conf
grep -q '^multipaths {' $CONF
UNCOMMENTED=$?
if [ $UNCOMMENTED -eq 0 ]
then
        sed -i '/^multipaths {/a\\tmultipath {\n\t\twwid 3600a0980'"${SN}"'\n\t
\talias '"${ALIAS}"'\n\t}\n' $CONF
else
        printf "multipaths {\n\tmultipath {\n\t\twwid 3600a0980$SN\n\t\talias
 $ALIAS\n\t}\n}" >> $CONF
fi
```

2. `multipathd` 서비스를 다시 시작하여 `/etc/multipathd.conf`의 변경 사항을 적용합니다.

```
~$ systemctl restart multipathd.service
```

LUN 파티션

다음 단계는 fdisk를 사용하여 LUN을 포맷하고 파티셔닝하는 것입니다.

1. 다음 명령을 사용하여 device_name에 대한 경로가 있는지 확인합니다.

```
~$ ls /dev/mapper/device_name
```

```
/dev/device_name
```

2. fdisk를 사용하여 디스크를 파티셔닝합니다. 대화형 프롬프트가 나타날 것입니다. 표시된 순서대로 옵션을 입력합니다. 마지막 섹터보다 작은 값(이 예제에서는 20971519)을 사용하여 여러 파티션을 만들 수 있습니다.

> **Note**
>
> Last sector 값은 iSCSI LUN의 크기(이 예에서는 10GB)에 따라 달라집니다.

```
~$ sudo fdisk /dev/mapper/device_name
```

fsdisk 대화형 프롬프트가 시작됩니다.

```
Welcome to fdisk (util-linux 2.30.2).

Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-20971519, default 2048): 2048
Last sector, +sectors or +size{K,M,G,T,P} (2048-20971519, default
 20971519): 20971519
```

```
Created a new partition 1 of type 'Linux' and of size 512 B.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

w를 입력하면 새 파티션 /dev/mapper/*partition_name*을 사용할 수 있게 됩니다. *partition_name*의 형식은 *<device_name><partition_number>*입니다. 1은 이전 단계의 fdisk 명령에 사용된 파티션 번호로 사용되었습니다.

3. /dev/mapper/*partition_name*을 경로로 사용하여 파일 시스템을 생성합니다.

```
~$ sudo mkfs.ext4 /dev/mapper/partition_name
```

시스템이 다음 출력으로 응답합니다.

```
mke2fs 1.42.9 (28-Dec-2013)
Discarding device blocks: done
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=16 blocks
655360 inodes, 2621184 blocks
131059 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2151677952
80 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
     32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
```

Linux 클라이언트에 LUN 마운트

1. *directory_path* 디렉터리를 파일 시스템의 마운트 지점으로 생성합니다.

```
~$ sudo mkdir /directory_path/mount_point
```

2. 다음 명령을 사용하여 파일 시스템을 마운트합니다.

```
~$ sudo mount -t ext4 /dev/mapper/partition_name /directory_path/mount_point
```

3. (선택 사항) 특정 사용자에게 탑재 디렉터리의 소유권을 부여하려면 *username*를 소유자의 사용자 아이디로 바꿉니다.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (선택 사항) 파일 시스템에서 데이터를 읽고 쓸 수 있는지 확인합니다.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Linux 클라이언트에 iSCSI LUN을 성공적으로 생성하고 마운트했습니다.

Windows용 iSCSI 프로비저닝

FSx for ONTAP는 iSCSI 프로토콜을 지원합니다. iSCSI 프로토콜을 사용하여 클라이언트와 파일 시스템 간에 데이터를 전송하려면 Windows 클라이언트와 SVM 및 볼륨 모두에서 iSCSI를 프로비저닝해야 합니다. iSCSI 프로토콜은 고가용성 페어(HA)가 6개 이하인 모든 파일 시스템에서 사용할 수 있습니다.

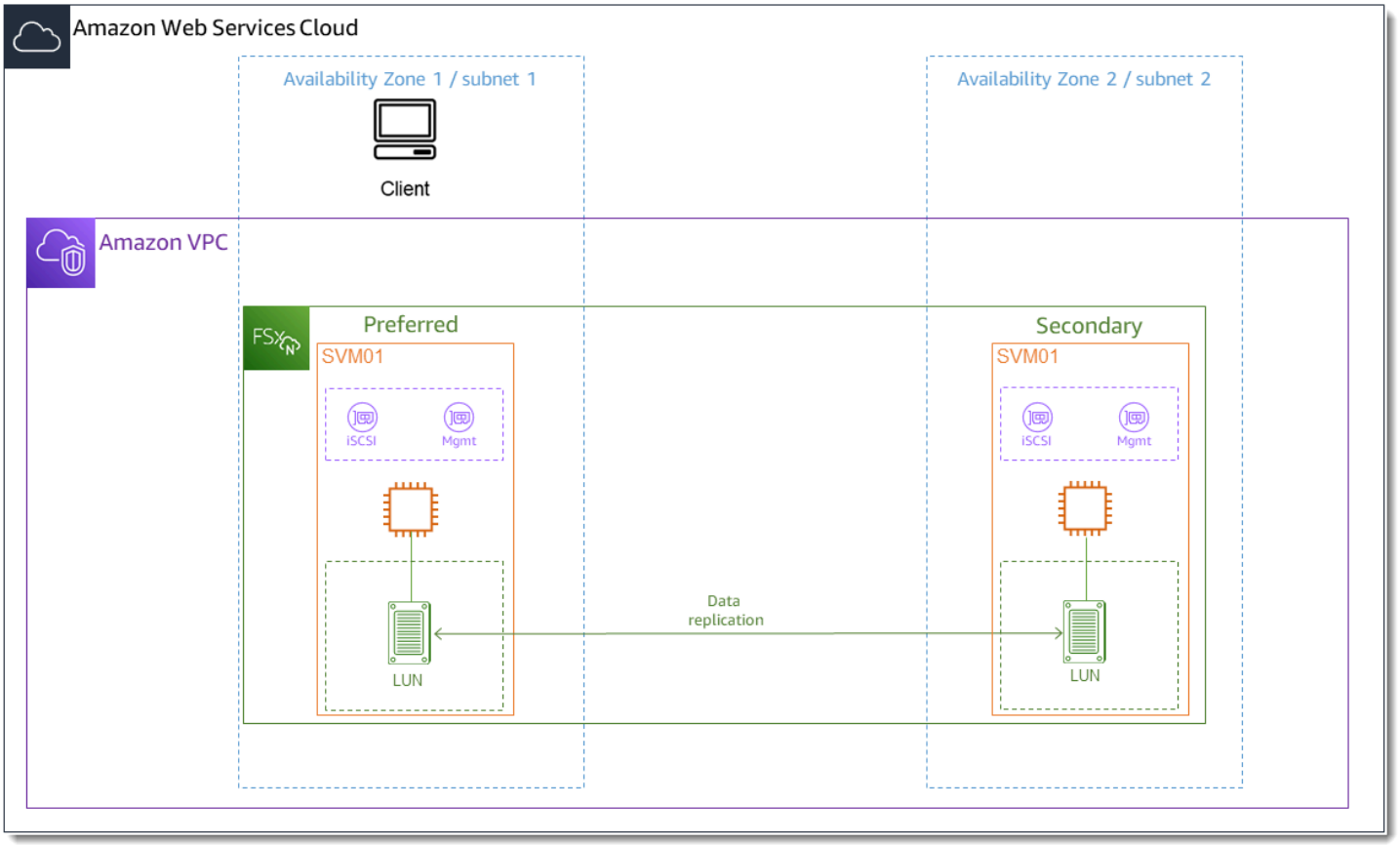
이 절차에 제시된 예제에서는 클라이언트 및 FSx for ONTAP 파일 시스템에 iSCSI 프로토콜을 프로비저닝하고 다음 설정을 사용하는 방법을 보여줍니다.

- Windows 호스트에 마운트되는 iSCSI LUN이 이미 생성되었습니다. 자세한 내용은 iSCSI LUN 생성 섹션을 참조하세요.
- iSCSI LUN을 마운트하는 Microsoft Windows 호스트는 Microsoft Windows Server 2019 Amazon Machine Image(AMI)를 실행하는 Amazon EC2 인스턴스입니다. Amazon VPC를 사용한 파일 시스템 액세스 제어에 설명된 대로 인바운드 및 아웃바운드 트래픽을 허용하도록 구성된 VPC 보안 그룹이 있습니다.

  설정에서 다른 Microsoft Windows AMI를 사용하고 있을 수 있습니다.

- 클라이언트와 파일 시스템이 동일한 VPC 및 AWS 계정에 있습니다. 클라이언트가 다른 VPC에 있는 경우 VPC 피어링 또는 AWS Transit Gateway 를 사용하여 다른 VPCs 액세스 권한을 부여할 수 있습니다. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.

  다음 그림과 같이 EC2 인스턴스는 파일 시스템의 기본 서브넷과 동일한 가용 영역에 배치하는 것이 좋습니다.



주제

- Windows 클라이언트에 iSCSI 구성
- FSx for ONTAP 파일 시스템에 iSCSI 구성
- Windows 클라이언트에 iSCSI LUN 마운트
- iSCSI 구성 검증

Windows 클라이언트에 iSCSI 구성

1. Windows 원격 데스크톱을 사용하여 iSCSI LUN을 마운트하려는 Windows 클라이언트에 연결합니다. 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 RDP를 사용하여 Windows 인스턴스에 연결을 참조하세요.
2. 관리자 권한으로 Windows PowerShell을 엽니다. 다음 명령을 사용하여 Windows 인스턴스에서 iSCSI를 활성화하고 iSCSI 서비스가 자동으로 시작되도록 구성합니다.

```
PS C:\> Start-Service MSiSCSI
PS C:\> Set-Service -Name msiscsi -StartupType Automatic
```

3. Windows 인스턴스의 이니시에이터 이름을 검색합니다. NetApp ONTAP CLI를 사용하여 FSx for ONTAP 파일 시스템에 iSCSI를 구성하는 데 이 값을 사용합니다.

```
PS C:\> (Get-InitiatorPort).NodeAddress
```

시스템이 이니시에이터 포트로 응답합니다.

```
iqn.1991-05.com.microsoft:ec2amaz-abc123d
```

4. 클라이언트가 파일 서버 간에 자동으로 장애 조치하도록 하려면 Windows 인스턴스에 `Multipath-IO`(MPIO)를 설치해야 합니다. 다음 명령을 사용합니다.

```
PS C:\> Install-WindowsFeature Multipath-IO
```

5. `Multipath-IO` 설치가 완료된 후 Windows 인스턴스를 다시 시작합니다. Windows 인스턴스를 열어 두고 다음 섹션에서 iSCSI LUN을 마운트하는 단계를 수행합니다.

FSx for ONTAP 파일 시스템에 iSCSI 구성

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. ONTAP CLI lun igroup create를 사용하여 이니시에이터 그룹을 만들거나 igroup를 만듭니다. 이니시에이터 그룹은 iSCSI LUN에 매핑되며 LUN에 액세스할 수 있는 이니시에이터(클라이언트)를 제어합니다. host_initiator_name을 이전 절차에서 검색한 Windows 호스트의 이니시에이터 이름으로 바꿉니다.

```
::> lun igroup create -vserver svm_name -igroup igroup_name -
initiator host_initiator_name -protocol iscsi -ostype windows
```

이 igroup에 매핑된 LUN을 여러 호스트에서 사용할 수 있도록 하려면 lun igroup create ONTAP CLI 명령을 사용하여 쉼표로 구분된 여러 개의 초기자 이름을 지정할 수 있습니다.

3. lun igroup show ONTAP CLI 명령을 사용하여 igroup이 성공적으로 생성되었는지 확인합니다.

```
::> lun igroup show
```

시스템이 다음 출력으로 응답합니다.

```
Vserver    Igroup        Protocol OS Type  Initiators
---------  ------------  -------- -------- ------------------------------------
svm_name   igroup_name   iscsi    windows  iqn.1994-05.com.windows:abcdef12345
```

igroup을 생성했으면 이제 LUN을 생성하여 igroup에 매핑할 준비가 되었습니다.

4. 이 단계에서는 이미 iSCSI LUN을 생성한 것으로 가정합니다. 아직 생성되지 않은 경우 단계별 지침으로 iSCSI LUN 생성 섹션을 참조하여 생성합니다.

LUN에서 새 igroup으로의 LUN 매핑을 생성합니다.

```
::> lun mapping create -vserver svm_name -path /vol/vol_name/lun_name -
igroup igroup_name -lun-id lun_id
```

5. 다음 명령을 사용하여 LUN이 생성되고 온라인 상태이며 매핑되었는지 확인합니다.

```
::> lun show -path /vol/vol_name/lun_name
Vserver     Path                            State   Mapped   Type     Size
---------   ------------------------------- ------- -------- -------- --------
svm_name    /vol/vol_name/lun_name          online  mapped   windows  10GB
```

이제 Windows 인스턴스에 iSCSI 대상을 추가할 준비가 되었습니다.

6. 다음 명령을 사용하여 SVM의 iscsi_1 및 iscsi_2 인터페이스의 IP 주소를 검색합니다.

```
::> network interface show -vserver svm_name
```

```
            Logical    Status     Network            Current       Current Is
Vserver     Interface  Admin/Oper Address/Mask       Node          Port    Home
----------- ---------- ---------- ------------------ ------------- ------- ----
svm_name
            iscsi_1    up/up      172.31.0.143/20    FSxId0123456789abcdef8-01
                                                                   e0e     true
            iscsi_2    up/up      172.31.21.81/20    FSxId0123456789abcdef8-02
                                                                   e0e     true
            nfs_smb_management_1
                       up/up      198.19.250.177/20  FSxId0123456789abcdef8-01
                                                                   e0e     true
3 entries were displayed.
```

이 예제에서 `iscsi_1`의 IP 주소는 `172.31.0.143`이고 `iscsi_2`의 IP 주소는 `172.31.21.81`입니다.

Windows 클라이언트에 iSCSI LUN 마운트

1. Windows 인스턴스에서 PowerShell 터미널을 관리자 권한으로 엽니다.
2. 다음 작업을 수행하는 `.ps1` 스크립트를 생성합니다.
   - 각 파일 시스템의 iSCSI 인터페이스에 연결합니다.
   - iSCSI용 MPIO를 추가하고 구성합니다.
   - 클라이언트가 최대 40Gbps(5,000MBps)의 집계 처리량을 iSCSI LUN으로 구동할 수 있도록 각 iSCSI 연결에 대해 8개의 세션을 설정합니다. 세션이 8개이면 단일 클라이언트가 최고 수준의 FSx for ONTAP 처리량 용량을 위해 전체 4,000MBps 처리량 용량을 구동할 수 있습니다. 선택적으로 `RecommendedConnectionCount` 변수를 수정하여 세션 수를 더 많거나 더 적은 세션 수로 변경할 수 있습니다(각 세션은 최대 625MBps의 처리량 제공). 자세한 내용은 Windows 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 인스턴스 네트워크 대역폭을 참조하세요.

   다음 명령 세트를 파일에 복사하여 `.psl` 스크립트를 생성합니다.

   - `iscsi_1`과 `iscsi_2`를 이전 단계에서 검색한 IP 주소로 바꿉니다.

- `ec2_ip`를 Windows 인스턴스의 IP 주소로 바꿉니다.

```
Write-Host "Starting iSCSI connection setup..."
     $TargetPortalAddresses = @("iscsi_1","iscsi_2"); $LocaliSCSIAddress = "ec2_ip"
     $RecommendedConnectionCount = 8

     Foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         New-IscsiTargetPortal -TargetPortalAddress $TargetPortalAddress -
TargetPortalPortNumber 3260 -InitiatorPortalAddress $LocaliSCSIAddress
     }

     New-MSDSMSupportedHW -VendorId MSFT2005 -ProductId iSCSIBusType_0x9

     $currentMPIOSettings = Get-MPIOSetting
     if ($currentMPIOSettings.PathVerificationState -ne 'Enabled') {
         Write-Host "Setting MPIO path verification state to Enabled"; Set-
MPIOSetting -NewPathVerificationState Enabled
     } else { Write-Host "MPIO path verification state already Enabled" }

     $portalConnectionCounts = @{}
     foreach ($TargetPortalAddress in $TargetPortalAddresses)
 { $portalConnectionCounts[$TargetPortalAddress] = 0 }

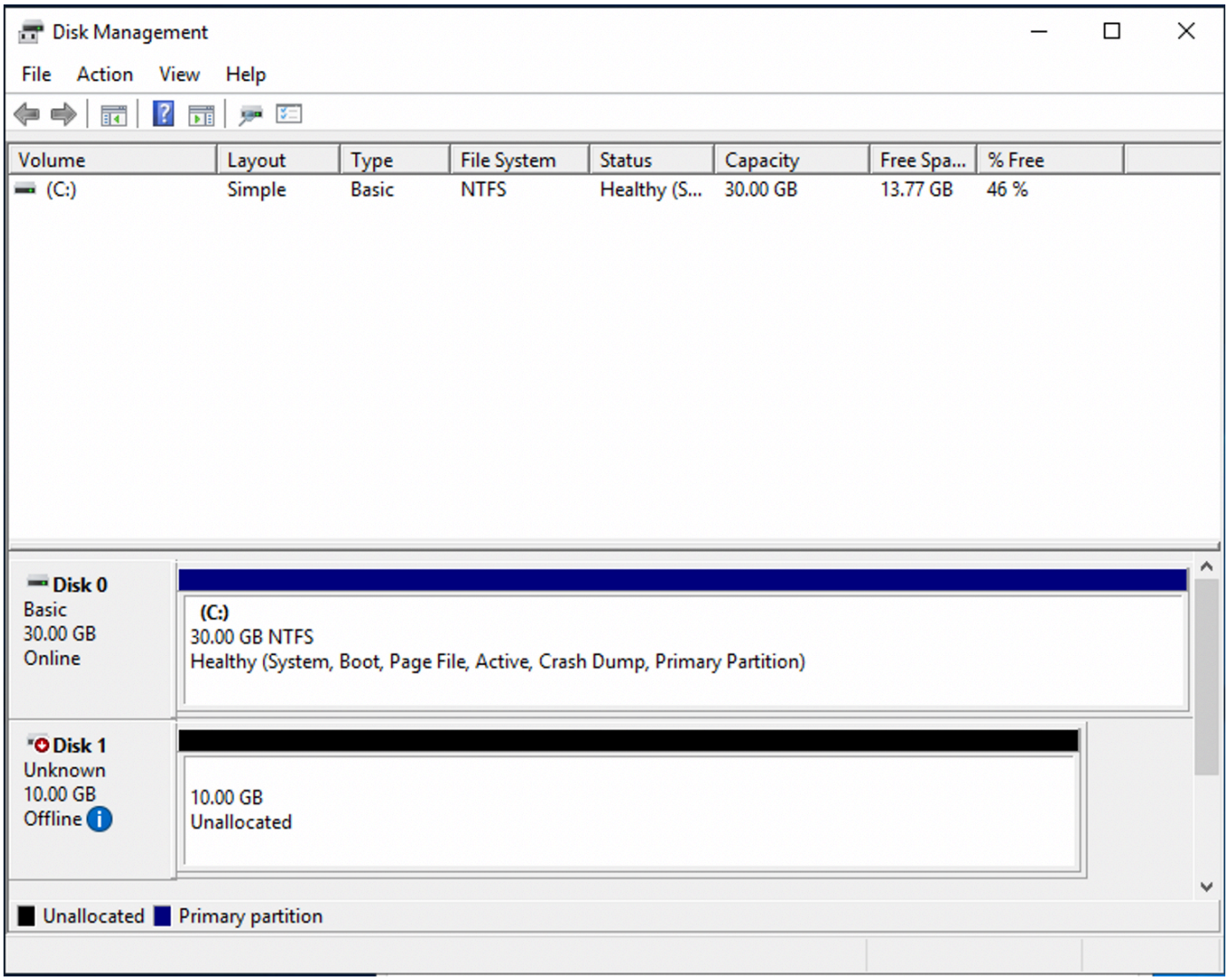
     $sessions = Get-IscsiSession
     if ($sessions) {
         foreach ($session in $sessions) {
             if ($session.IsConnected) {
                 $targetPortal = (Get-IscsiTargetPortal -iSCSISession
 $session).TargetPortalAddress
                 if ($portalConnectionCounts.ContainsKey($targetPortal))
 { $portalConnectionCounts[$targetPortal]++ }
             }
         }
     }

     foreach ($TargetPortalAddress in $TargetPortalAddresses) {
         $existingCount = $portalConnectionCounts[$TargetPortalAddress];
 $remainingConnections = $RecommendedConnectionCount - $existingCount
         Write-Host "Portal $TargetPortalAddress has $existingCount
 existing connections, $remainingConnections remaining (max recommended:
 $RecommendedConnectionCount)"
         if ($remainingConnections -gt 0) {
```

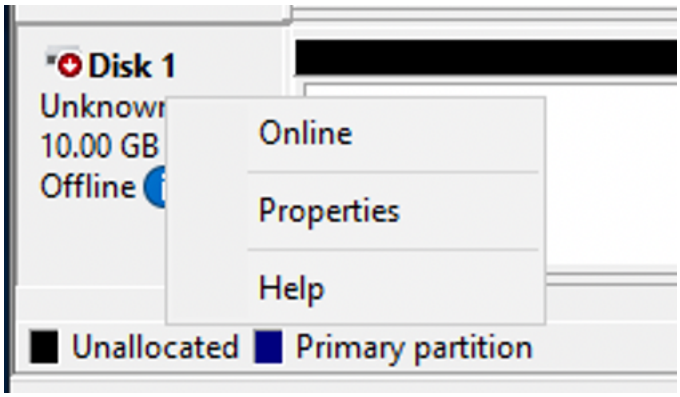
```
            Write-Host "Creating $remainingConnections connections for portal
 $TargetPortalAddress"
            1..$remainingConnections | ForEach-Object {
                Get-IscsiTarget | Connect-IscsiTarget -IsMultipathEnabled $true -
TargetPortalAddress $TargetPortalAddress -InitiatorPortalAddress $LocaliSCSIAddress
 -IsPersistent $true
            }
        } else { Write-Host "Maximum connections (8) reached for portal
 $TargetPortalAddress" }
    }

    Set-MSDSMGlobalDefaultLoadBalancePolicy -Policy RR
```

3. Windows Disk Management 애플리케이션을 시작합니다. Windows Run 대화 상자를 열고 `diskmgmt.msc`를 입력한 후 Enter 키를 누릅니다. Disk Management 애플리케이션이 열립니다.



4. 할당되지 않은 디스크를 찾아봅니다. 이것이 iSCSI LUN입니다. 이 예제에서 Disk 1은 iSCSI 디스크입니다. 오프라인 상태입니다.



Disk 1에 커서를 놓고 마우스 오른쪽 버튼을 클릭한 다음 온라인을 선택하여 볼륨을 온라인 상태로 전환합니다.

> **Note**
>
> 새 볼륨이 자동으로 온라인 상태가 되도록 Storage Area Network(SAN) 정책을 수정할 수 있습니다. 자세한 내용은 Microsoft Windows Server 명령 참조의 SAN 정책을 참조하세요.

5. 디스크를 초기화하려면 커서를 Disk 1 위에 놓고 마우스 오른쪽 버튼을 클릭한 다음 초기화를 선택합니다. 초기화 대화 상자가 표시됩니다. 확인을 선택하여 디스크를 초기화합니다.
6. 일반 절차대로 디스크를 포맷합니다. 포맷이 완료되면 iSCSI 드라이브가 Windows 클라이언트에서 사용 가능한 드라이브로 표시됩니다.

iSCSI 구성 검증

iSCSI 설정이 제대로 구성되었는지 확인하는 스크립트가 제공되었습니다. 스크립트는 세션 수, 노드 배포 및 다중 경로 I/O(MPIO) 상태와 같은 파라미터를 검사합니다. 다음 작업은 스크립트를 설치하고 사용하는 방법을 설명합니다.

iSCSI 구성을 검증하려면

1. Windows PowerShell 창을 엽니다.
2. 다음 명령을 사용하여 스크립트를 다운로드합니다.

```
PS C:\> Invoke-WebRequest "https://docs.aws.amazon.com/fsx/latest/ONTAPGuide/
samples/CheckiSCSI.zip" -OutFile "CheckiSCSI.zip"
```

3. 다음 명령을 사용하여 zip 파일을 확장합니다.

```
PS C:\> Expand-Archive -Path ".\CheckiSCSI.zip" -DestinationPath "./"
```

4. 다음 명령을 사용하여 스크립트를 실행하세요.

```
PS C:\> ./CheckiSCSI.ps1
```

5. 출력을 검토하여 구성의 현재 상태를 이해합니다. 다음 예제에서는 성공적인 iSCSI 구성을 보여줍니다.

```
PS C:\> ./CheckiSCSI.ps1

This script checks the iSCSI configuration on the local instance.
It will provide information about the number of connected sessions, connected file
 servers, and MPIO status.

MPIO is installed on this server.

MPIO Load Balance Policy is set to Round Robin (RR).
Initiator: 'iqn.1991-05.com.microsoft:ec2amaz-d2cebnb'
to Target: 'iqn.1992-08.com.netapp:sn.13266b10e61411ee8bc0c76ad263d613:vs.3'
has 16 total sessions (16 active, 0 non-active)
spread across 2 node(s).
MPIO: Yes
```

Linux용 NVMe /TCP 프로비저닝

FSx for ONTAP는 비휘발성 Memory Express over TCP(NVMe/TCP) 블록 스토리지 프로토콜을 지원합니다. NVMe /TCP를 사용하면 ONTAP CLI를 사용하여 네임스페이스와 하위 시스템을 프로비저닝한 다음 네임스페이스를 하위 시스템에 매핑합니다. 이는 LUNs 프로비저닝하고 iSCSI의 이니시에이터 그룹(igroup)에 매핑하는 방식과 비슷합니다. NVMe /TCP 프로토콜은 고가용성(HA) 페어가 6개 이하인 2세대 파일 시스템에서 사용할 수 있습니다.

> **Note**
>
> FSx for ONTAP 파일 시스템은 iSCSI 및 NVMe/TCP 블록 스토리지 프로토콜 모두에 SVM의 iSCSI 엔드포인트를 사용합니다.

Amazon FSx for NetApp ONTAP에서 NVMe/TCP를 구성하는 세 가지 주요 단계는 다음 절차에서 다룹니다.

1. Linux 호스트에 NVMe 클라이언트를 설치하고 구성합니다.
2. 파일 시스템의 SVM에서 NVMe를 구성합니다.
   - NVMe 네임스페이스를 생성합니다.
   - NVMe 하위 시스템을 생성합니다.
   - 네임스페이스를 하위 시스템에 매핑합니다.
   - 클라이언트 NQN을 하위 시스템에 추가합니다.
3. Linux 클라이언트에 NVMe 디바이스를 탑재합니다.

시작하기 전 준비 사항

NVMe/TCP용 파일 시스템을 구성하는 프로세스를 시작하기 전에 다음 항목을 완료해야 합니다.

- FSx for ONTAP 파일 시스템을 생성합니다. 자세한 내용은 파일 시스템 만들기 단원을 참조하십시오.
- 파일 시스템과 동일한 VPC에서 Red Hat Enterprise Linux(RHEL) 9.3을 실행하는 EC2 인스턴스를 생성합니다. 이는 NVMe를 구성하고 Linux용 NVMe NVMe/TCP를 사용하여 파일 데이터에 액세스할 Linux 호스트입니다.

  이러한 절차의 범위를 벗어나 호스트가 다른 VPC에 있는 경우 VPC 피어링 또는 AWS Transit Gateway 를 사용하여 다른 VPCs에 볼륨의 iSCSI 엔드포인트에 대한 액세스 권한을 부여할 수 있습니다. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.
- Amazon VPC를 사용한 파일 시스템 액세스 제어에 설명된 대로 인바운드 및 아웃바운드 트래픽을 허용하도록 Linux 호스트의 VPC 보안 그룹을 구성합니다.
- ONTAP CLI에 액세스하는 데 사용할 `fsxadmin` 권한이 있는 ONTAP 사용자의 자격 증명을 가져옵니다. 자세한 내용은 ONTAP 사용자 및 역할 단원을 참조하십시오.

- NVMe용으로 구성하고 FSx for ONTAP 파일 시스템에 액세스하는 데 사용할 Linux 호스트는 동일한 VPC와 AWS 계정에 있습니다.
- EC2 인스턴스는 파일 시스템의 기본 서브넷과 동일한 가용성 영역에 있는 것이 좋습니다.

EC2 인스턴스가 RHEL 9.3과 다른 Linux AMI를 실행하는 경우 이러한 절차 및 예제에 사용된 일부 유틸리티가 이미 설치되어 있을 수 있으며, 다른 명령을 사용하여 필요한 패키지를 설치할 수 있습니다. 패키지 설치 외에도 이 섹션에 사용된 명령은 다른 EC2 Linux AMI에도 유효합니다.

주제

Linux 호스트에 NVMe 설치 및 구성

NVMe 클라이언트를 설치하려면

1. SSH 클라이언트를 사용하여 Linux 인스턴스에 연결합니다. 자세한 내용은 SSH를 사용하여 Linux 또는 macOS에서 Linux 인스턴스에 연결을 참조하세요.
2. 다음 명령을 사용하여 `nvme-cli`를 설치합니다.

```
~$ sudo yum install -y nvme-cli
```

3. 호스트에 `nvme-tcp` 모듈을 로드합니다.

```
$ sudo modprobe nvme-tcp
```

4. 다음 명령을 사용하여 Linux 호스트의 NVMe 자격 이름(NQN)을 가져옵니다.

```
$ cat /etc/nvme/hostnqn
nqn.2014-08.org.nvmexpress:uuid:9ed5b327-b9fc-4cf5-97b3-1b5d986345d1
```

다음 단계에서 사용할 응답을 기록합니다.

FSx for ONTAP 파일 시스템에서 NVMe 구성하기

파일 시스템에서 NVMe를 구성하려면

NVMe 디바이스(들)를 생성하려는 FSx for ONTAP 파일 시스템의 NetApp ONTAP CLI에 연결합니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. NVMe 인터페이스에 액세스하는 데 사용하는 새 볼륨을 SVM에 생성합니다.

   ```
   ::> vol create -vserver fsx -volume nvme_vol1 -aggregate aggr1 -size 1t
        [Job 597] Job succeeded: Successful
   ```
3. vserver nvme namespace create NetApp ONTAP CLI 명령을 사용하여 NVMe 네임스페이스 ns_1를 생성합니다. 네임스페이스는 이니시에이터(클라이언트)에 매핑하고 NVMe 디바이스에 액세스할 수 있는 이니시에이터(클라이언트)를 제어합니다.

   ```
   ::> vserver nvme namespace create -vserver fsx -path /vol/nvme_vol1/ns_1 -size 100g
    -ostype linux
   Created a namespace of size 100GB (107374182400).
   ```
4. vserver nvme subsystem create NetApp ONTAP CLI 명령을 사용하여 NVMe 하위 시스템을 생성합니다.

   ```
   ~$ vserver nvme subsystem create -vserver fsx -subsystem sub_1 -ostype linux
   ```
5. 방금 생성한 하위 시스템에 네임스페이스를 매핑합니다.

   ```
   ::> vserver nvme subsystem map add -vserver fsx -subsystem sub_1 -path /vol/
   nvme_vol1/ns_1
   ```
6. 이전에 검색한 NQN을 사용하여 하위 시스템에 클라이언트를 추가합니다.

   ```
   ::> vserver nvme subsystem host add -subsystem sub_1 -host-nqn
    nqn.2014-08.org.nvmexpress:uuid:ec21b083-1860-d690-1f29-44528e4f4e0e -vserver fsx
   ```

이 하위 시스템에 매핑된 장치를 여러 호스트에서 사용할 수 있게 하려면 쉼표로 구분된 목록에 여러 개의 개시자 이름을 지정할 수 있습니다. 자세한 내용은 NetApp ONTAP Docs의 vserver nvme 하위 시스템 호스트 추가를 참조하세요.

7. vserver nvme namespace show 명령을 사용하여 네임스페이스가 존재하는지 확인합니다.

```
::> vserver nvme namespace show -vserver fsx -instance
Vserver Name: fsx
            Namespace Path: /vol/nvme_vol1/ns_1
                      Size: 100GB
                 Size Used: 90.59GB
                   OS Type: linux
                   Comment:
                Block Size: 4KB
                     State: online
         Space Reservation: false
Space Reservations Honored: false
              Is Read Only: false
             Creation Time: 5/20/2024 17:03:08
            Namespace UUID: c51793c0-8840-4a77-903a-c869186e74e3
                 Vdisk ID: 80d42c6f00000000187cca9
      Restore Inaccessible: false
   Inconsistent Filesystem: false
       Inconsistent Blocks: false
                   NVFail: false
Node Hosting the Namespace: FsxId062e9bb6e05143fcb-01
               Volume Name: nvme_vol1
                Qtree Name:
          Mapped Subsystem: sub_1
            Subsystem UUID: db526ec7-16ca-11ef-a612-d320bd5b74a9
              Namespace ID: 00000001h
              ANA Group ID: 00000001h
              Vserver UUID: 656d410a-1460-11ef-a612-d320bd5b74a9
                Vserver ID: 3
               Volume MSID: 2161388655
               Volume DSID: 1029
                 Aggregate: aggr1
            Aggregate UUID: cfa8e6ee-145f-11ef-a612-d320bd5b74a9
 Namespace Container State: online
       Autodelete Enabled: false
          Application UUID: -
              Application: -
  Has Metadata Provisioned: true
```

```
1 entries were displayed.
```

8. network interface show -vserver 명령을 사용하여 NVMe 디바이스를 생성한 SVM의 블록 스토리지 인터페이스 주소를 검색합니다.

```
::> network interface show -vserver svm_name -data-protocol nvme-tcp
            Logical               Status     Network            Current
        Current Is
Vserver     Interface             Admin/Oper Address/Mask       Node
        Port    Home
----------- ----------            ---------- ------------------ -------------
        ------- ----
svm_name
            iscsi_1               up/up      172.31.16.19/20
 FSxId0123456789abcdef8-01  e0e     true
            iscsi_2               up/up      172.31.26.134/20
 FSxId0123456789abcdef8-02  e0e     true
2 entries were displayed.
```

> **Note**
>
> iscsi_1 LIF는 iSCSI와 NVMe /TCP 모두에 사용됩니다.

이 예제에서 iscsi_1의 IP 주소는 172.31.16.19이고 iscsi_2는 172.31.26.134입니다.

Linux 클라이언트에 NVMe 디바이스 탑재

Linux 클라이언트에 NVMe 디바이스를 탑재하는 프로세스는 세 단계로 구성됩니다.

1. NVMe 노드 검색
2. NVMe 디바이스 파티셔닝
3. 클라이언트에 NVMe 디바이스 탑재

이는 다음 절차에서 다룹니다.

대상 NVMe 노드를 검색하려면

1. Linux 클라이언트에서 다음 명령을 사용하여 대상 NVMe 노드를 검색합니다. *iscsi_1_IP*를 iscsi_1의 IP 주소로 바꾸고 클라이언트의 IP 주소는 *client_IP*로 바꿉니다.

   > **Note**
   >
   > iscsi_1 및 iscsi_2 LIFs는 iSCSI 및 NVMe 스토리지 모두에 사용됩니다.

   ```
   ~$ sudo nvme discover -t tcp -w client_IP -a iscsi_1_IP
   ```

   ```
   Discovery Log Number of Records 4, Generation counter 11
   =====Discovery Log Entry 0======
   trtype:  tcp
   adrfam:  ipv4
   subtype: current discovery subsystem
   treq:    not specified
   portid:  0
   trsvcid: 8009
   subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
   traddr:  172.31.26.134
   eflags:  explicit discovery connections, duplicate discovery information
   sectype: none
   =====Discovery Log Entry 1======
   trtype:  tcp
   adrfam:  ipv4
   subtype: current discovery subsystem
   treq:    not specified
   portid:  1
   trsvcid: 8009
   subnqn:  nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:discovery
   traddr:  172.31.16.19
   eflags:  explicit discovery connections, duplicate discovery information
   sectype: none
   ```

2. (선택 사항) 파일 NVMe 디바이스에 대해 Amazon EC2 단일 클라이언트 최대 5Gbps(~625MBps)보다 높은 처리량을 제공하려면 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 인스턴스 네트워크 대역폭에 설명된 절차에 따라 추가 세션을 설정합니다.

3. 컨트롤러 손실 시간 제한이 1800초 이상인 대상 이니시에이터에 로그인하고, 다시 *iscsi_1_IP*에는 iscsi_1의 IP 주소를, *client_IP*에는 클라이언트의 IP 주소를 사용합니다. NVMe 디바이스는 사용 가능한 디스크로 표시됩니다.

```
~$ sudo nvme connect-all -t tcp -w client_IP -a iscsi_1 -l 1800
```

4. 다음 명령을 사용하여 NVMe 스택이 여러 세션을 식별 및 병합하고 다중 라우팅을 구성했는지 확인합니다. 이 명령은 구성에 성공하면 Y를 반환합니다.

```
~$ cat /sys/module/nvme_core/parameters/multipath
Y
```

5. 다음 명령을 사용하여 사용 가능한 모든 경로에 I/O를 분산하기 위해 각 ONTAP 네임스페이스에 대해 NVMe-oF 설정 model가 NetApp ONTAP Controller로 설정되고 로드 밸런싱 iopolicy가 round-robin로 설정되어 있는지 확인합니다.

```
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/model
Amazon Elastic Block Store
NetApp ONTAP Controller
~$ cat /sys/class/nvme-subsystem/nvme-subsys*/iopolicy
numa
round-robin
```

6. 다음 명령을 사용하여 네임스페이스가 생성되고 호스트에서 올바르게 검색되었는지 확인합니다.

```
~$ sudo nvme list
Node                  Generic               SN                   Model
                        Namespace  Usage                      Format           FW
 Rev
--------------------- --------------------- --------------------
 ---------------------------------------- ---------- --------------------------
 ---------------- --------
/dev/nvme0n1          /dev/ng0n1            vol05955547c003f0580 Amazon Elastic
 Block Store               0x1         25.77  GB /  25.77  GB    512   B +  0 B
 1.0
/dev/nvme2n1          /dev/ng2n1            lWB12JWY/XLKAAAAAAAC NetApp ONTAP
 Controller                0x1        107.37  GB / 107.37  GB      4 KiB +  0 B
 FFFFFFFF
```

출력의 새 디바이스는 /dev/nvme2n1입니다. 이 이름 지정 체계는 Linux 설치에 따라 다를 수 있습니다.

7. 각 경로의 컨트롤러 상태가 라이브이고 올바른 비대칭 네임스페이스 액세스(ANA) 다중 경로 상태가 있는지 확인합니다.

```
~$ nvme list-subsys /dev/nvme2n1
nvme-subsys2 -
 NQN=nqn.1992-08.com.netapp:sn.656d410a146011efa612d320bd5b74a9:subsystem.rhel
               hostnqn=nqn.2014-08.org.nvmexpress:uuid:ec2a70bf-3ab2-6cb0-
f997-8730057ceb24
               iopolicy=round-robin
\
 +- nvme2 tcp
 traddr=172.31.26.134,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live non-optimized
 +- nvme3 tcp
 traddr=172.31.16.19,trsvcid=4420,host_traddr=172.31.25.143,src_addr=172.31.25.143
 live optimized
```

이 예제에서는 NVMe 스택이 파일 시스템의 대체 LIF, `iscsi_2`, 172.31.26.134을 자동으로 검색했습니다.

8. NetApp 플러그인에 각 ONTAP 네임스페이스 디바이스에 대한 올바른 값이 표시되는지 확인합니다.

```
~$ sudo nvme netapp ontapdevices -o column
Device           Vserver                   Namespace Path
           NSID UUID                                   Size
---------------- -------------------------
 ------------------------------------------------- ----
 ------------------------------------ ---------
/dev/nvme2n1     fsx                       /vol/nvme_vol1/ns_1
           1    0441c609-3db1-4b0b-aa83-790d0d448ece   107.37GB
```

디바이스를 분할하려면

1. 다음 명령을 사용하여 device_name nvme2n1의 경로가 있는지 확인합니다.

```
~$ ls /dev/mapper/nvme2n1
/dev/nvme2n1
```

2. fdisk를 사용하여 디스크를 파티셔닝합니다. 대화형 프롬프트가 나타날 것입니다. 표시된 순서대로 옵션을 입력합니다. 마지막 섹터보다 작은 값(이 예제에서는 20971519)을 사용하여 여러 파티션을 만들 수 있습니다.

> **Note**
>
> Last sector 값은 NVMe 디바이스의 크기(이 예제에서는 100GiB)에 따라 달라집니다.

```
~$ sudo fdisk /dev/mapper/nvme2n1
```

fsdisk 대화형 프롬프트가 시작됩니다.

```
Welcome to fdisk (util-linux 2.37.4).
Changes will remain in memory only, until you decide to write them.
Be careful before using the write command.

Device does not contain a recognized partition table.
Created a new DOS disklabel with disk identifier 0x66595cb0.

Command (m for help): n
Partition type
   p primary (0 primary, 0 extended, 4 free)
   e extended (container for logical partitions)
Select (default p): p
Partition number (1-4, default 1): 1
First sector (256-26214399, default 256):
Last sector, +sectors or +size{K,M,G,T,P} (256-26214399, default
 26214399): 20971519

Created a new partition 1 of type 'Linux' and of size 100 GiB.
Command (m for help): w
The partition table has been altered.
Calling ioctl() to re-read partition table.
Syncing disks.
```

w를 입력하면 새 파티션 /dev/nvme2n1을 사용할 수 있게 됩니다. *partition_name*의 형식은 *<device_name><partition_number>*입니다. 1은 이전 단계의 fdisk 명령에 사용된 파티션 번호입니다.

3. /dev/nvme2n1을 경로로 사용하여 파일 시스템을 생성합니다.

```
~$ sudo mkfs.ext4 /dev/nvme2n1
```

시스템이 다음 출력으로 응답합니다.

```
mke2fs 1.46.5 (30-Dec-2021)
Found a dos partition table in /dev/nvme2n1
Proceed anyway? (y,N) y
Creating filesystem with 26214400 4k blocks and 6553600 inodes
Filesystem UUID: 372fb2fd-ae0e-4e74-ac06-3eb3eabd55fb
Superblock backups stored on blocks:
    32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
    4096000, 7962624, 11239424, 20480000, 23887872

Allocating group tables: done
Writing inode tables: done
Creating journal (131072 blocks): done
Writing superblocks and filesystem accounting information: done
```

Linux 클라이언트에 NVMe 장치를 탑재하려면 다음과 같이 하세요.

1. Linux 인스턴스에서 디렉터리 *directory_path*를 파일 시스템의 탑재 지점으로 만듭니다.

```
~$ sudo mkdir /directory_path/mount_point
```

2. 다음 명령을 사용하여 파일 시스템을 마운트합니다.

```
~$ sudo mount -t ext4 /dev/nvme2n1 /directory_path/mount_point
```

3. (선택 사항) 특정 사용자에게 탑재 디렉터리의 소유권을 부여하려면 *username*를 소유자의 사용자 아이디로 바꿉니다.

```
~$ sudo chown username:username /directory_path/mount_point
```

4. (선택 사항) 파일 시스템에서 데이터를 읽고 쓸 수 있는지 확인합니다.

```
~$ echo "Hello world!" > /directory_path/mount_point/HelloWorld.txt
~$ cat directory_path/HelloWorld.txt
Hello world!
```

Linux 클라이언트에 NVMe 장치를 성공적으로 생성하고 탑재했습니다.

Windows용 NVMe /TCP 프로비저닝

FSx for ONTAP는 Windows용 NVMe/TCP(Non-Volatile Memory Express over TCP) 블록 스토리지 프로토콜을 지원합니다. NVMe /TCP를 사용하면 ONTAP CLI를 사용하여 네임스페이스와 하위 시스템을 프로비저닝한 다음 네임스페이스를 하위 시스템에 매핑합니다. 이는 LUNs 프로비저닝하고 iSCSI의 이니시에이터 그룹(igroup)에 매핑하는 방식과 비슷합니다. NVMe /TCP 프로토콜은 고가용성(HA) 페어가 6개 이하인 2세대 파일 시스템에서 사용할 수 있습니다.

Windows 호스트에서 NVMe /TCP를 프로비저닝하려면 원하는 공급업체에서 이니시에이터를 다운로드하고 지침에 따라 설치 및 프로비저닝해야 합니다.

다른 AWS 서비스를 사용하여 데이터 액세스

Amazon EC2 외에도 볼륨과 함께 다른 AWS 서비스를 사용하여 데이터에 액세스할 수 있습니다.

주제

- FSx for ONTAP과 함께 Amazon WorkSpaces 사용
- FSx for ONTAP과 함께 Amazon Elastic Container Service 사용
- FSx for ONTAP에서 Amazon Elastic VMware Service 사용
- FSx for ONTAP과 함께 VMware Cloud 사용

FSx for ONTAP과 함께 Amazon WorkSpaces 사용

FSx for ONTAP을 Amazon WorkSpaces와 함께 사용하여 공유 네트워크 연결 스토리지(NAS)를 제공하거나 Amazon WorkSpaces 계정의 로밍 프로파일을 저장할 수 있습니다. WorkSpaces 인스턴스로 SMB 파일 공유에 연결한 후 사용자는 파일 공유에서 파일을 생성하고 편집할 수 있습니다.

다음 절차는 Amazon WorkSpaces와 함께 Amazon FSx를 사용하여 로밍 프로파일 및 홈 폴더 액세스를 일관되게 제공하고 Windows 및 Linux WorkSpaces 사용자에게 공유 팀 폴더를 제공하는 방법을 보여줍니다. Amazon WorkSpaces를 처음 사용하는 경우 Amazon WorkSpaces 관리 가이드의 WorkSpaces 빠른 설정으로 시작하기 지침에 따라 첫 번째 Amazon WorkSpaces 환경을 생성할 수 있습니다.

주제

- 로밍 프로파일 지원 제공
- 공통 파일에 액세스할 수 있는 공유 폴더 제공

로밍 프로파일 지원 제공

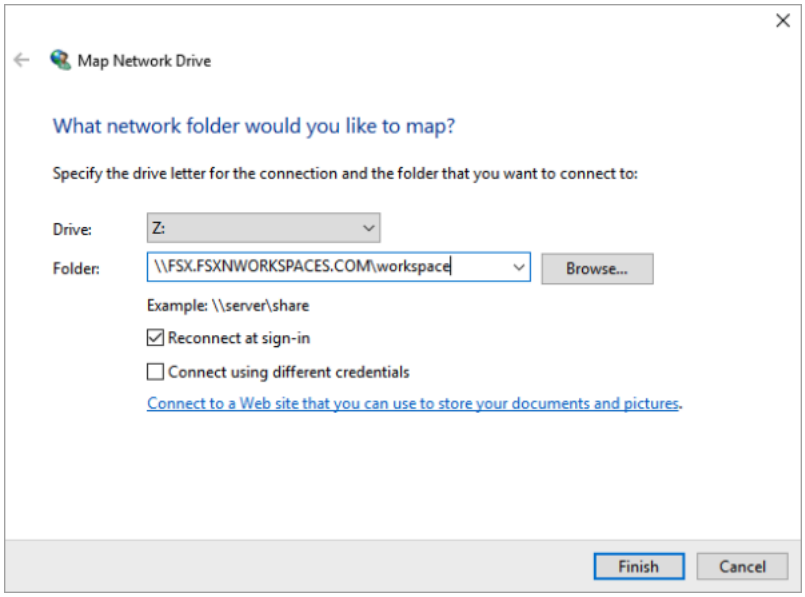
Amazon FSx를 사용하여 조직의 사용자에게 로밍 프로파일 지원을 제공할 수 있습니다. 사용자는 자신의 로밍 프로파일에만 액세스할 수 있는 권한을 갖습니다. 폴더는 Active Directory 그룹 정책을 사용하여 자동으로 연결됩니다. 로밍 프로파일을 사용하면 Amazon FSx 파일 공유에서 로그오프할 때 사용자의 데이터 및 데스크톱 설정이 저장되므로 여러 WorkSpaces 인스턴스 간에 문서와 설정을 공유하고 Amazon FSx 일별 자동 백업을 사용하여 자동으로 백업할 수 있습니다.

1단계: Amazon FSx를 사용하여 도메인 사용자의 프로파일 폴더 위치 생성

1. Amazon FSx 콘솔을 사용하여 FSx for ONTAP 파일 시스템을 생성합니다. 자세한 내용은 파일 시스템 생성(콘솔) 섹션을 참조하세요.

   > **Important**
   >
   > 각 FSx for ONTAP 파일 시스템에는 파일 시스템과 연결된 엔드포인트가 생성되는 엔드포인트 IP 주소 범위가 있습니다. 다중 AZ 파일 시스템의 경우 FSx for ONTAP은 198.19.0.0/16에서 사용되지 않는 기본 IP 주소 범위를 엔드포인트 IP 주소 범위로 선택합니다. Amazon WorkSpaces 관리 가이드의 WorkSpaces의 IP 주소 및 포트 요구 사항에 설명된 대로 이 IP 주소 범위는 WorkSpaces에서 관리 트래픽 범위로도 사용됩니다. 따라서 WorkSpaces에서 다중 AZ FSx for ONTAP 파일 시스템에 액세스하려면 198.19.0.0/16과 겹치지 않는 엔드포인트 IP 주소 범위를 선택해야 합니다.

2. Active Directory에 조인된 스토리지 가상 머신(SVM)이 없는 경우 지금 하나를 생성합니다. 예를 들어 이름이 `fsx`인 SVM을 프로비저닝하고 보안 스타일을 NTFS로 설정할 수 있습니다. 자세한 내용은 스토리지 가상 머신 생성(콘솔) 섹션을 참조하세요.
3. SVM용 볼륨을 생성합니다. 예를 들어, SVM 루트 볼륨의 보안 스타일을 상속하는 `fsx-vol`이라는 이름의 볼륨을 생성할 수 있습니다. 자세한 내용은 FlexVol 볼륨 생성(콘솔) 섹션을 참조하세요.
4. 볼륨에 SMB 공유를 생성합니다. 예를 들어, `fsx-vol`이라는 이름의 볼륨에 `workspace`라는 공유를 생성하고 이 공유에 `profiles`라는 폴더를 생성할 수 있습니다. 자세한 내용은 SMB 공유 관리 섹션을 참조하세요.
5. Windows Server를 실행하는 Amazon EC2 인스턴스 또는 WorkSpaces에서 Amazon FSx SVM에 액세스합니다. 자세한 내용은 FSx for ONTAP 데이터 액세스 섹션을 참조하세요.
6. Windows WorkSpaces 인스턴스에서 공유를 `Z:\`에 매핑합니다.



2단계: FSx for ONTAP 파일 공유를 사용자 계정에 연결

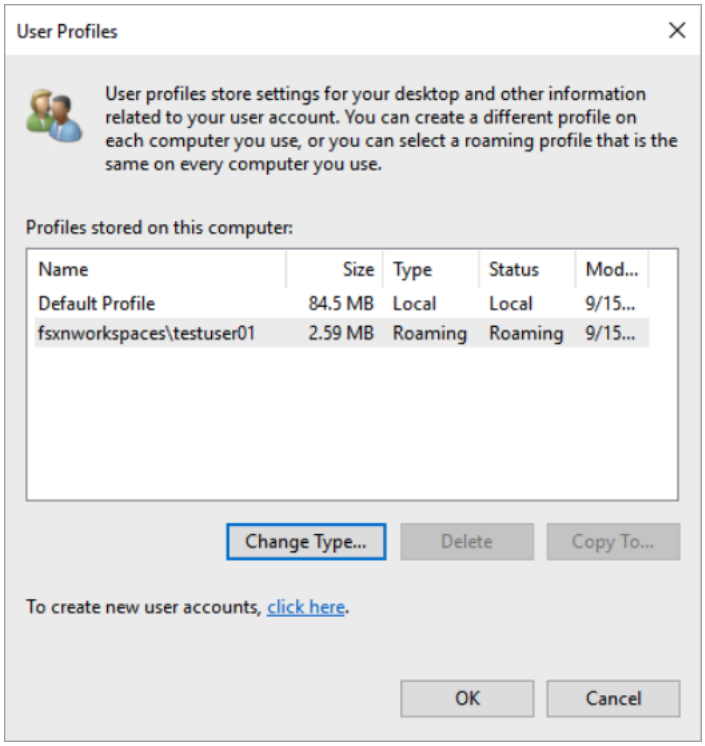
1. 테스트 사용자의 WorkSpace에서 Windows > 시스템 > 고급 시스템 설정을 선택합니다.
2. 시스템 속성에서 고급 탭을 선택하고 사용자 프로파일 섹션에서 설정 버튼을 누릅니다. 로그인한 사용자의 프로파일 유형은 `Local`입니다.
3. WorkSpaces에서 테스트 사용자를 로그아웃합니다.
4. Amazon FSx 파일 시스템에 로밍 프로파일이 위치하도록 테스트 사용자를 설정합니다. 관리자 WorkSpaces에서 PowerShell 콘솔을 열고 다음 예제와 비슷한 명령을 사용합니다(1단계에서 이전에 생성한 `profiles` 폴더 사용).

```
Set-ADUser username -ProfilePath \\filesystem-dns-
name\sharename\foldername\username
```

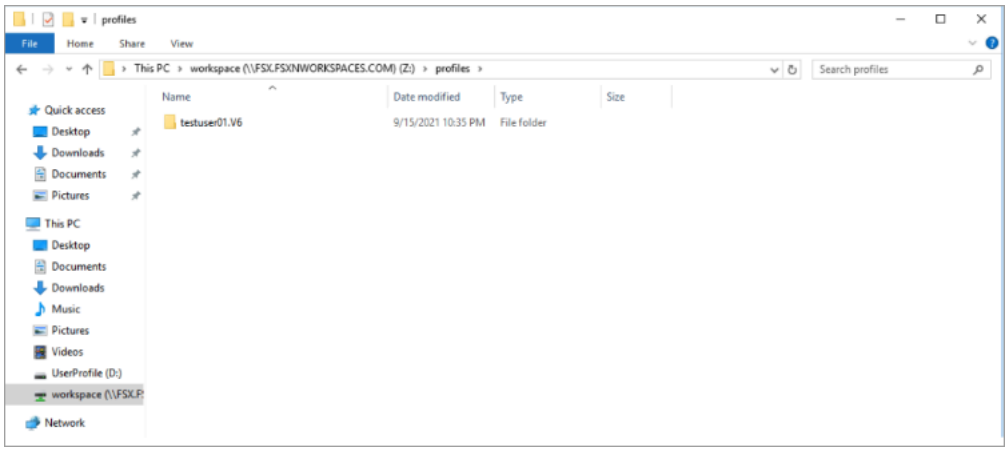
예시:

```
Set-ADUser testuser01 -ProfilePath \\fsx.fsxnworkspaces.com\workspace\profiles
\testuser01
```

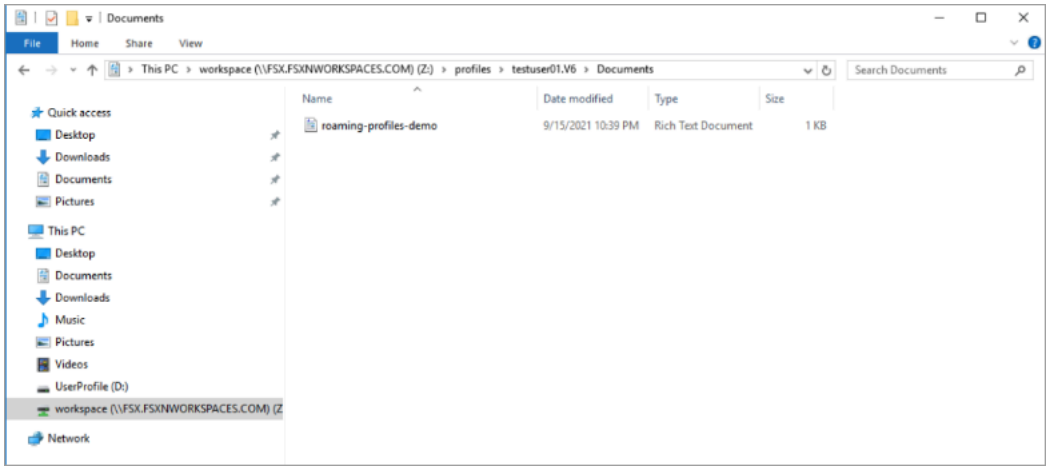
5. 테스트 사용자 WorkSpaces에 로그온합니다.
6. 시스템 속성에서 고급 탭을 선택하고 사용자 프로파일 섹션에서 설정 버튼을 누릅니다. 로그인한 사용자의 프로파일 유형은 `Roaming`입니다.



7. FSx for ONTAP 공유 폴더를 찾아봅니다. `profiles` 폴더에 사용자를 위한 폴더가 있습니다.



8. 테스트 사용자의 `Documents` 폴더에 문서를 생성합니다.
9. WorkSpaces에서 테스트 사용자를 로그아웃합니다.
10. 테스트 사용자로 다시 로그온하고 해당 사용자의 프로파일 저장소를 찾아보면 생성된 문서를 확인할 수 있습니다.



공통 파일에 액세스할 수 있는 공유 폴더 제공

Amazon FSx를 사용하여 조직의 사용자에게 공유 폴더를 제공할 수 있습니다. 공유 폴더는 모든 사용자에게 필요한 데모 파일, 코드 예제, 지침 매뉴얼 등 사용자 커뮤니티에서 사용하는 파일을 저장하는 데 사용할 수 있습니다. 일반적으로 드라이브는 공유 폴더에 매핑되어 있지만 매핑된 드라이브는 문자를 사용하므로 공유할 수 있는 수의 제한이 있습니다. 이 절차를 통해 드라이브 문자 없이 사용할 수 있는 Amazon FSx 공유 폴더를 생성할 수 있으므로 팀에 공유를 보다 유연하게 할당할 수 있습니다.

Linux 및 Windows WorkSpaces에서 플랫폼 간 액세스를 위한 공유 폴더 마운트

1. 작업 표시줄에서 장소 > 서버에 연결을 선택합니다.

   a. 서버에 *`file-system-dns-name`*을 입력합니다.

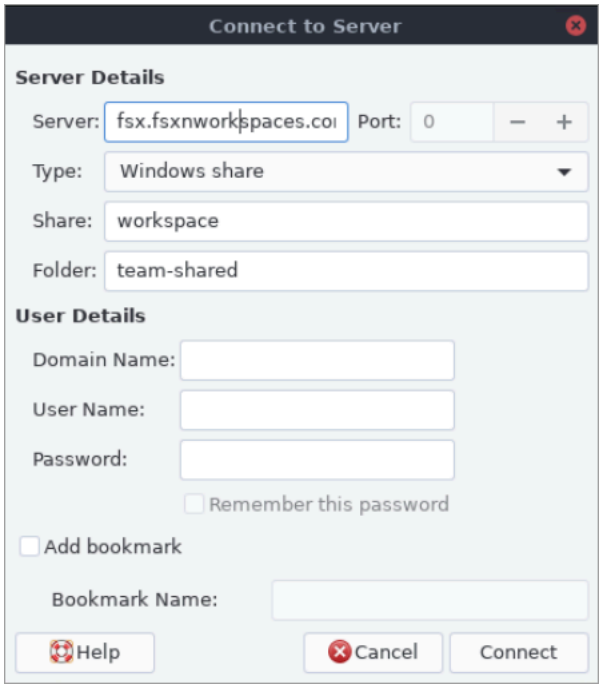
   b. 유형을 `Windows share`로 설정합니다.

   c. 공유를 SMB 공유 이름(예: `workspace`)으로 설정합니다.

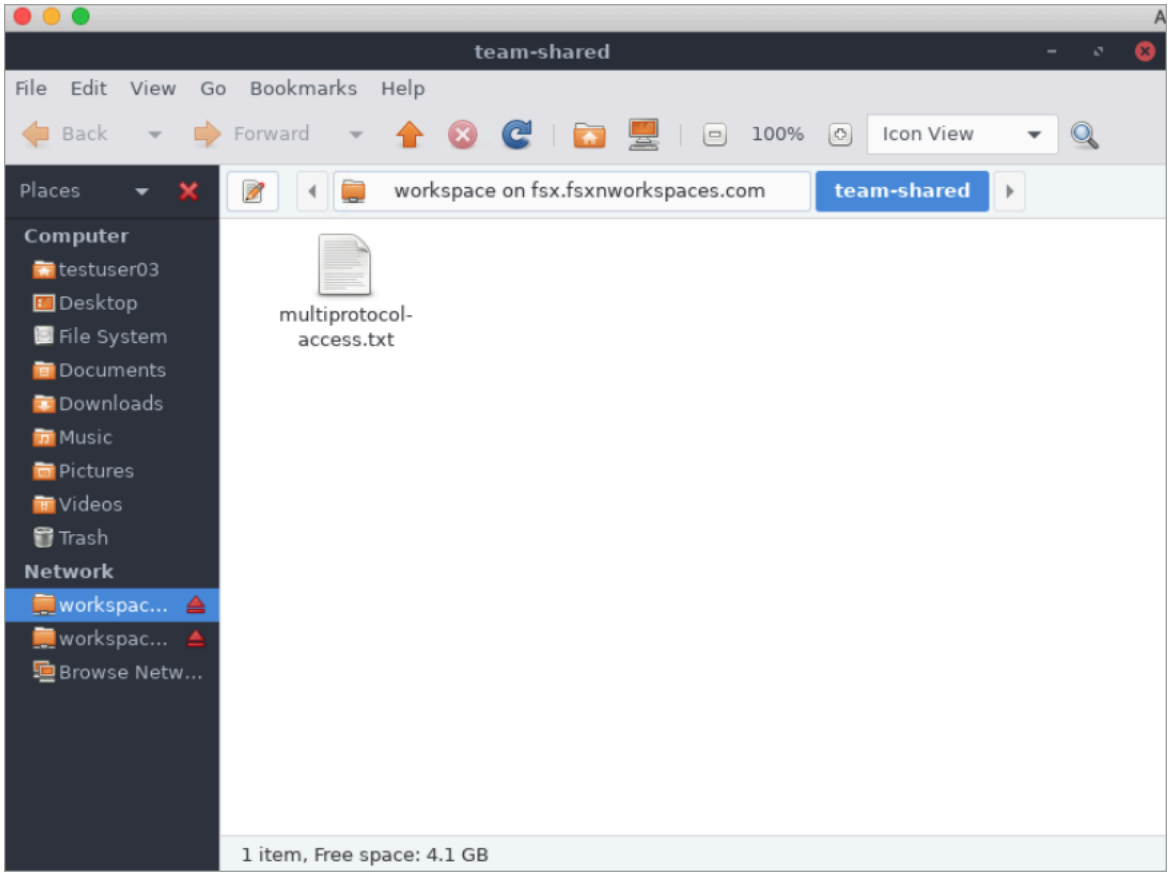
   d. 폴더 를 `/`로 두거나 이름이 지정된 폴더(예: `team-shared`라는 이름의 폴더)로 설정할 수 있습니다.

   e. Linux WorkSpaces가 Amazon FSx 공유와 동일한 도메인에 있으면 Linux WorkSpaces에 사용자 세부 정보를 입력할 필요가 없습니다.

   f. 연결을 선택합니다.



2. 연결이 설정되면 `workspace`라는 이름의 SMB 공유에서 공유 폴더(이 예에서는 이름이 `team-shared`로 지정됨)를 볼 수 있습니다.



FSx for ONTAP과 함께 Amazon Elastic Container Service 사용

Amazon EC2 Linux 또는 Windows 인스턴스에서 Amazon Elastic Container Service(Amazon ECS) 도커 컨테이너로부터 Amazon FSx for NetApp ONTAP 파일 시스템에 액세스할 수 있습니다.

Amazon ECS Linux 컨테이너에서 마운트

1. Linux 컨테이너용 EC2 Linux + 네트워킹 클러스터 템플릿을 사용하여 ECS 클러스터를 생성합니다. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 클러스터 생성을 참조하세요.
2. 다음과 같이 SVM 볼륨을 마운트할 디렉터리를 EC2 인스턴스에 생성합니다.

   ```
   sudo mkdir /fsxontap
   ```

3. 인스턴스 시작 중에 사용자 데이터 스크립트를 사용하거나 다음 명령을 실행하여 Linux EC2 인스턴스에 FSx for ONTAP 볼륨을 마운트합니다.

   ```
   sudo mount -t nfs svm-ip-address:/vol1 /fsxontap
   ```

4. 다음 명령을 사용하여 볼륨을 마운트합니다.

   ```
   sudo mount -t nfs -o nfsvers=NFS_version svm-dns-name:/volume-junction-path /
   fsxontap
   ```

   다음 예제는 샘플 값을 사용합니다.

   ```
   sudo mount -t nfs -o nfsvers=4.1
    svm-01234567890abdef0.fs-01234567890abcdef1.fsx.us-east-1.amazonaws.com:/vol1 /
   fsxontap
   ```

   DNS 이름 대신 SVM의 IP 주소를 사용할 수도 있습니다.

   ```
   sudo mount -t nfs -o nfsvers=4.1 198.51.100.1:/vol1 /fsxontap
   ```

5. Amazon ECS 작업 정의를 생성할 때 JSON 컨테이너 정의에 다음 `volumes` 및 `mountPoints` 컨테이너 속성을 추가합니다. `sourcePath`를 FSx for ONTAP 파일 시스템의 마운트 지점 및 디렉터리로 바꿉니다.

   ```
   {
   ```

```
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

Amazon ECS Windows 컨테이너에서 마운트

1. Windows 컨테이너용 EC2 Windows + 네트워킹 클러스터 템플릿을 사용하여 ECS 클러스터를 생성합니다. 자세한 내용은 Amazon Elastic Container Service 개발자 안내서의 클러스터 생성을 참조하세요.
2. 도메인에 조인된 Windows EC2 인스턴스를 ECS Windows 클러스터에 추가하고 SMB 공유를 매핑합니다.

   Active Directory 도메인에 조인된 ECS에 최적화된 Windows EC2 인스턴스를 시작하고 다음 명령을 실행하여 ECS 에이전트를 초기화합니다.

   ```
   PS C:\Users\user> Initialize-ECSAgent -Cluster windows-fsx-cluster -
   EnableTaskIAMRole
   ```

   다음과 같이 스크립트의 정보를 사용자 데이터 텍스트 필드에 전달할 수도 있습니다.

   ```
   <powershell>
   Initialize-ECSAgent -Cluster windows-fsx-cluster -EnableTaskIAMRole
   </powershell>
   ```

3. SMB 공유를 드라이브에 매핑할 수 있도록 EC2 인스턴스에 SMB 글로벌 매핑을 생성합니다. 아래의 netbios 또는 DNS 이름의 값을 FSx 파일 시스템 및 공유 이름의 값으로 바꿉니다. Linux EC2 인스턴스에 마운트된 NFS 볼륨 vol1은 FSx 파일 시스템에서 CIFS 공유 fsxontap으로 구성되어 있습니다.

```
vserver cifs share show -vserver svm08 -share-name fsxontap


                                    Vserver: svm08
                                      Share: fsxontap
                    CIFS Server NetBIOS Name: FSXONTAPDEMO
                                       Path: /vol1
                             Share Properties: oplocks
                                               browsable
                                               changenotify
                                               show-previous-versions
                           Symlink Properties: symlinks
                    File Mode Creation Mask: -
                Directory Mode Creation Mask: -
                                 Share Comment: -
                                     Share ACL: Everyone / Full Control
               File Attribute Cache Lifetime: -
                                   Volume Name: vol1
                                 Offline Files: manual
               Vscan File-Operations Profile: standard
            Maximum Tree Connections on Share: 4294967295
                   UNIX Group for File Create: -
```

4. 다음 명령을 사용하여 EC2 인스턴스에 SMB 글로벌 매핑을 생성합니다.

```
New-SmbGlobalMapping -RemotePath \\fsxontapdemo.fsxontap.com\fsxontap -LocalPath Z:
```

5. Amazon ECS 작업 정의를 생성할 때 JSON 컨테이너 정의에 다음 `volumes` 및 `mountPoints` 컨테이너 속성을 추가합니다. `sourcePath`를 FSx for ONTAP 파일 시스템의 마운트 지점 및 디렉터리로 바꿉니다.

```
{
    "volumes": [
        {
            "name": "ontap-volume",
            "host": {
                "sourcePath": "mountpoint"
```

```
            }
        }
    ],
    "mountPoints": [
        {
            "containerPath": "containermountpoint",
            "sourceVolume": "ontap-volume"
        }
    ],
    .
    .
    .
}
```

FSx for ONTAP에서 Amazon Elastic VMware Service 사용

FSx for ONTAP을 Amazon Elastic VMware Service(Amazon EVS) 소프트웨어 정의 데이터 센터(SDDCs. 자세한 내용은 Amazon FSx for NetApp ONTAP을 사용하여 고성능 워크로드 실행을 참조하세요. 자세한 지침은 NFS 데이터 스토어로 Amazon FSx for NetApp ONTAP 구성 및 iSCSI 데이터 스토어로 Amazon FSx for NetApp ONTAP 구성을 참조하세요.

FSx for ONTAP과 함께 VMware Cloud 사용

FSx for ONTAP을 AWS 소프트웨어 정의 데이터 센터(SDDC)의 VMware Cloud에 대한 외부 데이터 스토어로 사용할 수 있습니다.SDDCs 자세한 내용은 Configure Amazon FSx for NetApp ONTAP as External Storage and VMware Cloud AWS with Amazon FSx for NetApp ONTAP Deployment Guide를 참조하세요.

가용성, 내구성 및 배포 옵션

Amazon FSx for NetApp ONTAP은 Single-AZ 및 Multi-AZ 배포 유형을 사용합니다. Single-AZ 1, Single-AZ 2, Multi-AZ 1, Multi-AZ 2의 네 가지 옵션 중에서 선택할 수 있습니다. 이 주제에서는 워크로드에 적합한 배포 유형을 선택하는 데 도움이 되도록 각 배포 유형의 가용성 및 내구성 기능을 설명합니다. 서비스의 가용성 SLA(서비스 수준 계약)에 대한 자세한 내용은 Amazon FSx 서비스 수준 계약을 참조하세요.

주제

파일 시스템 배포 유형 선택

Single-AZ 및 Multi-AZ 파일 시스템 배포 유형의 가용성 및 내구성 기능은 다음 섹션에서 설명합니다.

Single-AZ 배포 유형

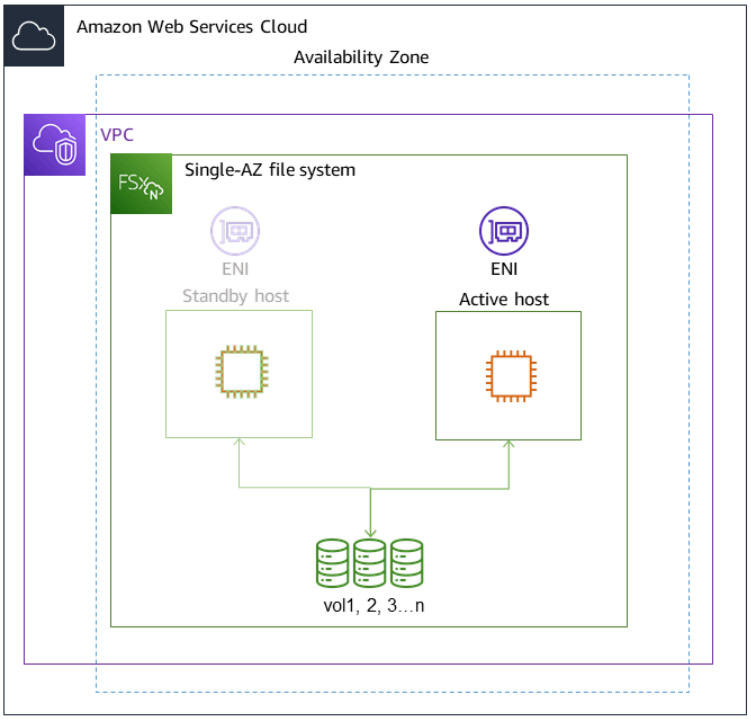
Single-AZ 파일 시스템에 대해 Single-AZ 1과 Single-AZ 2 중에서 선택할 수 있습니다. Single-AZ 1은 고가용성(HA) 페어가 하나 있는 1세대 파일 시스템인 반면, Single-AZ 2는 1~12개의 HA 페어가 있는 2세대 파일 시스템입니다. 자세한 내용은 파일 시스템 생성 선택 단원을 참조하십시오.

Single-AZ 파일 시스템을 생성하면 Amazon FSx는 활성-대기 구성으로 1~12개의 파일 서버 쌍을 자동으로 프로비저닝하며, 각 쌍의 활성 및 대기 파일 서버는 AWS 리전의 단일 가용 영역 내에 있는 별도의 장애 도메인에 위치합니다. 계획된 파일 시스템 유지 관리 또는 활성 파일 서버의 계획되지 않은 서비스 중단 중에 Amazon FSx는 일반적으로 몇 초 이내에 고가용성(HA) 페어를 대기 파일 서버에 자동으로 독립적으로 장애 조치합니다. 장애 조치 중에는 수동 개입 없이 데이터에 계속 액세스할 수 있습니다.

고가용성을 보장하기 위해 Amazon FSx는 하드웨어 장애를 지속적으로 모니터링하고 장애 발생 시 인프라 구성 요소를 자동으로 교체합니다. 높은 내구성을 달성하기 위해 Amazon FSx는 가용 영역 내에 데이터를 자동으로 복제하여 구성 요소 장애로부터 데이터를 보호합니다. 또한 파일 시스템 데이터의 자동 일별 백업을 구성하는 옵션도 있습니다. 이러한 백업은 여러 가용 영역에 저장되어 모든 백업 데이터에 Multi-AZ 복원력을 제공합니다.

Single-AZ 파일 시스템은 Multi-AZ 파일 시스템의 데이터 복원력 모델이 필요하지 않은 사용 사례를 위해 설계되었습니다. 단일 가용 영역 내에서만 데이터를 복제 AWS 리전하여 개발 및 테스트 환경, 온프레미스 또는 다른에 이미 저장된 데이터의 보조 복사본 저장과 같은 사용 사례를 위한 비용 최적화 솔루션을 제공합니다.

다음 다이어그램은 1세대 FSx for ONTAP Single-AZ 파일 시스템의 아키텍처를 보여줍니다.

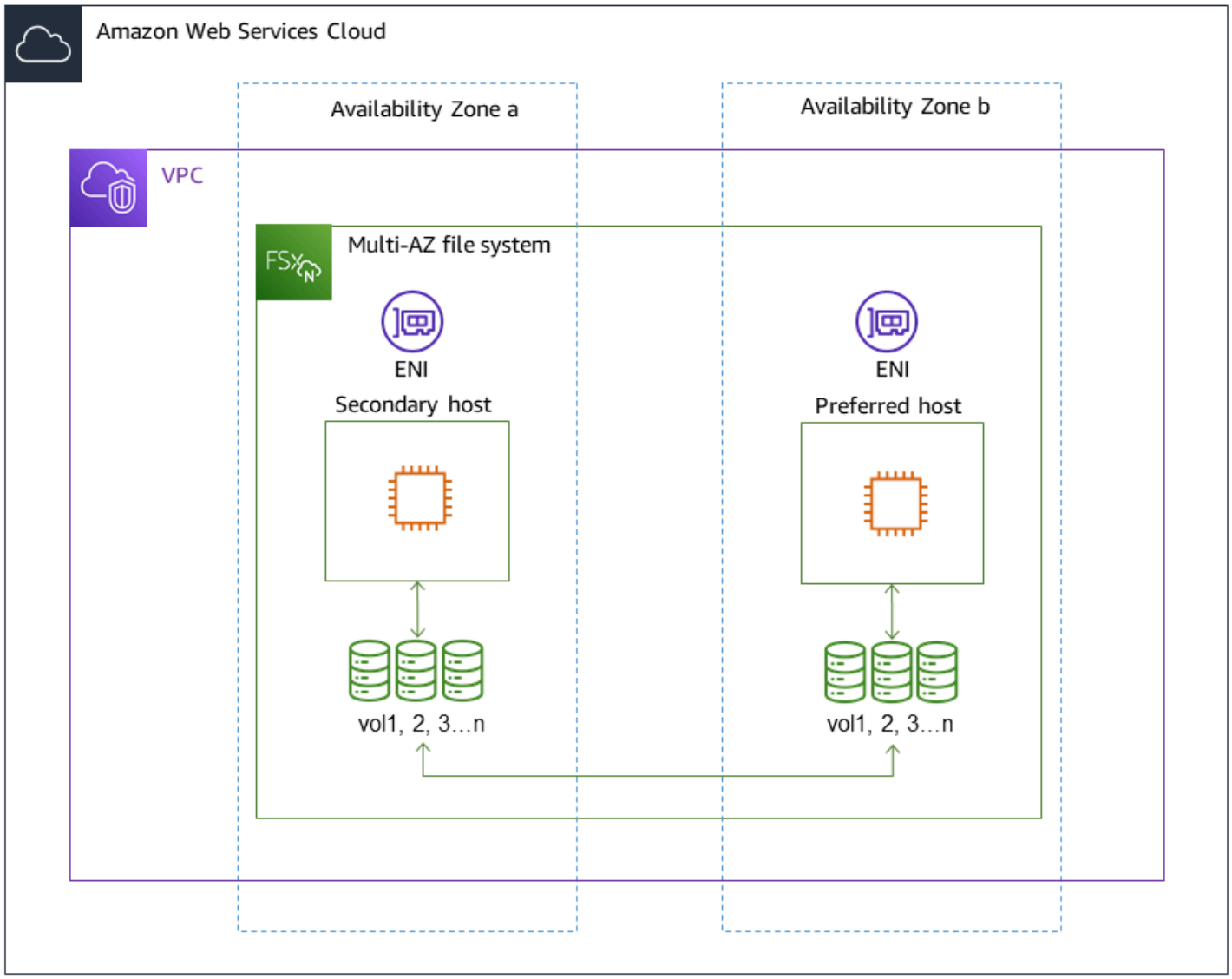


Multi-AZ 배포 유형

Multi-AZ 파일 시스템에 대해 Multi-AZ 1과 Multi-AZ 2 중에서 선택할 수 있습니다. Multi-AZ 1은 1세대 파일 시스템이고 Multi-AZ 2는 2세대 파일 시스템입니다. 두 옵션 모두 하나의 HA 페어가 있습니다. 자세한 내용은 파일 시스템 생성 선택 단원을 참조하십시오.

Multi-AZ 파일 시스템은 Single-AZ 파일 시스템의 가용성 및 내구성 기능을 모두 지원합니다. 또한 가용 영역을 사용할 수 없는 경우에도 데이터에 대한 지속적인 가용성을 제공하도록 설계되었습니다. Multi-AZ 배포에는 단일 HA 쌍의 파일 서버가 있으며, 대기 파일 서버는 동일한 AWS 리전의 활성 파일 서버와 다른 가용성 영역에 배포됩니다. 파일 시스템에 기록된 모든 변경 사항은 가용 영역 전체에서 대기 파일 서버에 동기식으로 복제됩니다.

Multi-AZ 파일 시스템은 공유 ONTAP 파일 데이터에 대한 고가용성이 필요하고 가용 영역 전반에 복제가 내장된 스토리지가 필요한 비즈니스 크리티컬 프로덕션 워크로드와 같은 사용 사례를 위해 설계되었습니다. 다음 다이어그램은 1세대 FSx for ONTAP Multi-AZ 파일 시스템의 아키텍처를 보여줍니다.



파일 시스템 생성 선택

다음 표는 ONTAP 파일 시스템용 1세대 및 2세대 Single-AZ와 Multi-AZ FSx의 차이점을 보여줍니다.

FSx for ONTAP 파일 시스템 생성

차원	1세대	2세대(단일 HA 페어)	2세대(다중 페어)
배포 유형	SINGLE_AZ_1	SINGLE_AZ_2	SINGLE_AZ_2

차원	1세대	2세대(단일 HA 페어)	2세대(다중 페어)
	MULTI_AZ_1	MULTI_AZ_2	
HA 페어	HA 페어 1개		HA 페어 1~12개
SSD 스토리지	최소: 1TiB 최대: 192TiB	최소: 1TiB 최대: 512TiB	최소: 1TiB(HA 페어당) 최대: 1 PiB(총)
SSD IOPS	최소: SSD 의 3 IOPS/GIB 최대: 160,000	최소: SSD 의 3 IOPS/GIB 최대: 200,000	최소: SSD 의 3 IOPS/GIB 최대: 2,400,000(HA 페어당 200,000)
처리량 용량	128MBps, 256MBps, 512MBps, 1,024MBps , 2,048MBps , 4,096MBps	384MBps, 768MBps, 1,536MBps , 3,072MBps , 6,144MBps	1,536MBps(HA 페어당), 3,072MBps(HA 페어당), 6,144MBps (HA 페어당)

> **Note**
>
> 생성 후에는 파일 시스템의 배포 유형을 변경할 수 없습니다. 배포 유형을 변경하려면(예: Single-AZ 1에서 Single-AZ 2로 이동) 데이터를 백업하고 새 파일 시스템에서 복원할 수 있습니다. NetApp SnapMirror, AWS DataSync또는 타사 데이터 복사 도구를 사용하여 데이터를 마이그레이션할 수도 있습니다. 자세한 내용은 NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션 및 AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션 단원을 참조하세요.

FSx for ONTAP의 장애 조치 프로세스

Single-AZ 및 Multi-AZ 파일 시스템은 다음 조건 중 하나라도 발생하면 기본 또는 활성 파일 서버에서 대기 파일 서버로 지정된 HA 쌍을 자동으로 페일오버합니다:

- 기본 또는 활성 파일 서버를 사용할 수 없게 된 경우
- 파일 시스템의 처리량 용량이 변경된 경우

- 기본 또는 활성 파일 서버가 계획된 유지 관리 작업 중인 경우
- 가용 영역 운영 중단 발생(Multi-AZ 파일 시스템만 해당)

> **Note**
>
> HA 페어가 여러 개인 2세대 파일 시스템의 경우 각 HA 페어의 장애 조치 동작은 독립적입니다. 한 HA 페어의 기본 파일 서버를 사용할 수 없는 경우 해당 HA 페어만 대기 파일 서버에 장애 조치됩니다.

한 파일 서버에서 다른 파일 서버로 장애 조치할 때 새 활성 파일 서버는 자동으로 모든 파일 시스템 읽기 및 쓰기 요청을 해당 HA 쌍에 서비스하기 시작합니다. Multi-AZ 파일 시스템의 경우 기본 파일 서버가 완전히 복구되어 사용 가능해지면 Amazon FSx가 자동으로 해당 서버로 페일백되며, 일반적으로 60초 이내에 페일백이 완료됩니다. Single-AZ 및 Multi-AZ 파일 시스템의 경우, 활성 파일 서버에서 장애가 감지된 후 대기 파일 서버가 활성 상태로 승격되기까지 보통 60초 이내에 장애 조치가 완료됩니다. 클라이언트가 NFS 또는 SMB를 통해 데이터에 액세스하는 데 사용하는 엔드포인트 IP 주소는 동일하게 유지되므로 Linux, Windows 및 MacOS 애플리케이션에서 페일오버가 투명하게 이루어져 수동 개입 없이 파일 시스템 작업을 재개합니다.

FSx for ONTAP Single-AZ 및 Multi-AZ 파일 시스템에 연결된 클라이언트에서 장애 조치가 투명하게 수행되도록 하려면 내에서 데이터 액세스 AWS 클라우드 섹션을 참조하세요.

파일 시스템에서 장애 조치 테스트

처리량 용량을 수정하여 파일 시스템에서 장애 조치를 테스트할 수 있습니다. 파일 시스템의 처리량 용량을 수정하면 Amazon FSx가 파일 시스템의 파일 서버를 순차적으로 교체합니다. Amazon FSx가 기본 파일 서버를 먼저 대체하는 동안 파일 시스템은 자동으로 보조 서버로 장애 조치합니다. 업데이트되면 파일 시스템이 자동으로 새 기본 서버로 페일백되고 Amazon FSx가 보조 파일 서버를 대체합니다.

Amazon FSx 콘솔, CLI 및 API에서 처리량 용량 업데이트 요청의 진행 상황을 모니터링할 수 있습니다. 파일 시스템의 처리량 용량을 수정하고 요청 진행 상황을 모니터링하는 방법에 대한 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

네트워크 리소스

이 섹션에서는 Single-AZ 및 Multi-AZ 파일 시스템이 사용하는 네트워크 리소스에 대해 설명합니다.

서브넷

Single-AZ 파일 시스템을 생성할 때는 파일 시스템에 단일 서브넷을 지정합니다. 선택하는 서브넷에 따라 파일 시스템이 생성되는 가용 영역이 정의됩니다. Multi-AZ 파일 시스템을 생성할 때는 2개의 서브넷을 지정하는데, 하나는 기본 파일 서버용이고 다른 하나는 대기 파일 서버용입니다. 선택하는 두 서브넷은 동일한 AWS 리전의 서로 다른 가용 영역에 있어야 합니다. Amazon VPC에 대한 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서의 Amazon VPC?란을 참조하세요.

> **Note**
>
> 지정하는 서브넷과 관계없이 파일 시스템 VPC 내의 모든 서브넷에서 파일 시스템에 액세스할 수 있습니다.

파일 시스템 탄력적 네트워크 인터페이스

Single-AZ 파일 시스템의 경우 Amazon FSx는 파일 시스템에 연결하는 서브넷에 두 개의 탄력적 네트워크 인터페이스(ENI)를 프로비저닝합니다. Multi-AZ 파일 시스템의 경우 Amazon FSx는 파일 시스템에 연결하는 각 서브넷에 하나씩 두 개의 ENI를 프로비저닝합니다. 클라이언트는 탄력적 네트워크 인터페이스를 사용하여 Amazon FSx 파일 시스템과 통신합니다. 네트워크 인터페이스는 사용자 계정의 VPC에 속해 있음에도 불구하고 Amazon FSx의 서비스 범위 내에 있는 것으로 간주됩니다. Multi-AZ 파일 시스템은 플로팅 IP(인터넷 프로토콜) 주소를 사용하므로 연결된 클라이언트는 장애 조치 이벤트 중에 기본 설정 파일 서버와 대기 파일 서버 간에 원활하게 전환할 수 있습니다.

> **Warning**
>
> - 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 수정하거나 삭제해서는 안 됩니다. 네트워크 인터페이스를 수정하거나 삭제하면 VPC와 파일 시스템 간의 연결이 영구적으로 손실될 수 있습니다.
> - 파일 시스템과 연결된 탄력적 네트워크 인터페이스에는 경로가 자동으로 생성되어 기본 VPC 및 서브넷 라우팅 테이블에 추가됩니다. 이러한 경로를 수정하거나 삭제하면 파일 시스템 클라이언트의 연결이 일시적 또는 영구적으로 끊길 수 있습니다.

다음 표에는 각 FSx for ONTAP 파일 시스템 배포 유형에 대한 서브넷, 탄력적 네트워크 인터페이스 및 IP 주소 리소스가 요약되어 있습니다.

	1세대 Single-AZ	2세대 Single-AZ	Multi-AZ
서브넷 수	1	1	2
탄력적 네트워크 인터페이스 수	2	HA 페어당 2개	2
ENI별 IP 주소 수	1 + 파일 시스템의 SVM 수	HA 페어 수 + HA 페어 수에 파일 시스템의 SVMs 수를 곱합니다.	1 + 파일 시스템의 SVM 수
VPC 라우팅 테이블 경로 수	N/A	N/A	1 + 파일 시스템의 SVM 수

파일 시스템 또는 SVM이 생성되면 해당 IP 주소는 파일 시스템이 삭제될 때까지 변경되지 않습니다.

Important

Amazon FSx는 퍼블릭 인터넷에서 파일 시스템에 액세스하거나 퍼블릭 인터넷에 파일 시스템을 노출하는 것을 지원하지 않습니다. Amazon FSx는 인터넷에서 연결할 수 있는 퍼블릭 IP 주소인 탄력적 IP 주소를 자동으로 분리합니다. 이 주소는 파일 시스템의 탄력적 네트워크 인터페이스에 연결됩니다.

Amazon FSx for NetApp ONTAP 성능

다음은 사용 가능한 성능 및 처리량 옵션과 유용한 성능 팁에 대한 설명과 함께 Amazon FSx for NetApp ONTAP 파일 시스템 성능에 대해 소개합니다.

주제

FSx for ONTAP 파일 시스템의 성능 측정 방법

파일 시스템 성능은 지연 시간, 처리량, 초당 I/O 작업 수(IOPS)로 측정됩니다.

지연 시간

Amazon FSx for NetApp ONTAP은 솔리드 스테이트 드라이브(SSD) 스토리지를 사용할 경우 파일 작업 지연 시간이 1밀리초 미만이고 용량 풀 스토리지의 경우 지연 시간이 수십 밀리초입니다. 또한 Amazon FSx는 각 파일 서버에 NVMe(비휘발성 메모리 익스프레스) 드라이브와 인 메모리라는 두 계층의 읽기 캐싱을 제공하므로 가장 자주 읽는 데이터에 액세스할 때 지연 시간을 훨씬 줄일 수 있습니다.

처리량 및 IOPS

각 Amazon FSx 파일 시스템은 최대 수천만 GBps의 처리량과 수백만 IOPS를 제공합니다. 워크로드가 파일 시스템에서 구동할 수 있는 구체적인 처리량 및 IOPS의 양은 파일 시스템의 총 처리량 용량 및 스토리지 용량 구성과 활성 작업 세트의 크기를 비롯한 워크로드의 특성에 따라 달라집니다.

SMB 멀티채널 및 NFS 연결 해제 지원

Amazon FSx를 사용하면 단일 SMB 세션에서 ONTAP과 클라이언트 간에 다중 연결을 제공하도록 SMB 다중 채널을 구성할 수 있습니다. SMB Multichannel은 클라이언트와 서버 간의 여러 네트워크 연

결을 동시에 사용하여 네트워크 대역폭을 집계하여 사용률을 극대화합니다. NetApp ONTAP CLI를 사용하여 SMB 멀티채널을 구성하는 방법에 대한 자세한 내용은 성능 및 이중화를 위한 SMB 멀티채널 구성을 참조하세요.

NFS 클라이언트는 단일 NFS 마운트에 여러 TCP 연결(최대 16개)이 가능하도록 nconnect 마운트 옵션을 사용할 수 있습니다. 이러한 NFS 클라이언트는 라운드 로빈 방식으로 파일 작업을 여러 TCP 연결로 멀티플렉싱하므로 사용 가능한 네트워크 대역폭에서 더 높은 처리량을 얻을 수 있습니다. NFSv3 및 NFSv4.1+에서 nconnect를 지원합니다. Amazon EC2 인스턴스 네트워크 대역폭은 네트워크 흐름 대역폭당 5Gbps의 full duplex 한도를 나타냅니다. nconnect 또는 SMB 다중 채널을 사용하는 다중 네트워크 흐름을 사용하면 이 제한을 극복할 수 있습니다. 사용 중인 클라이언트 버전에서 nconnect가 지원되는지 확인하려면 NFS 클라이언트 설명서를 참조하세요. nconnect에 대한 NetApp ONTAP 지원에 대한 자세한 내용은 ONTAP NFSv4.1 지원을 참조하세요.

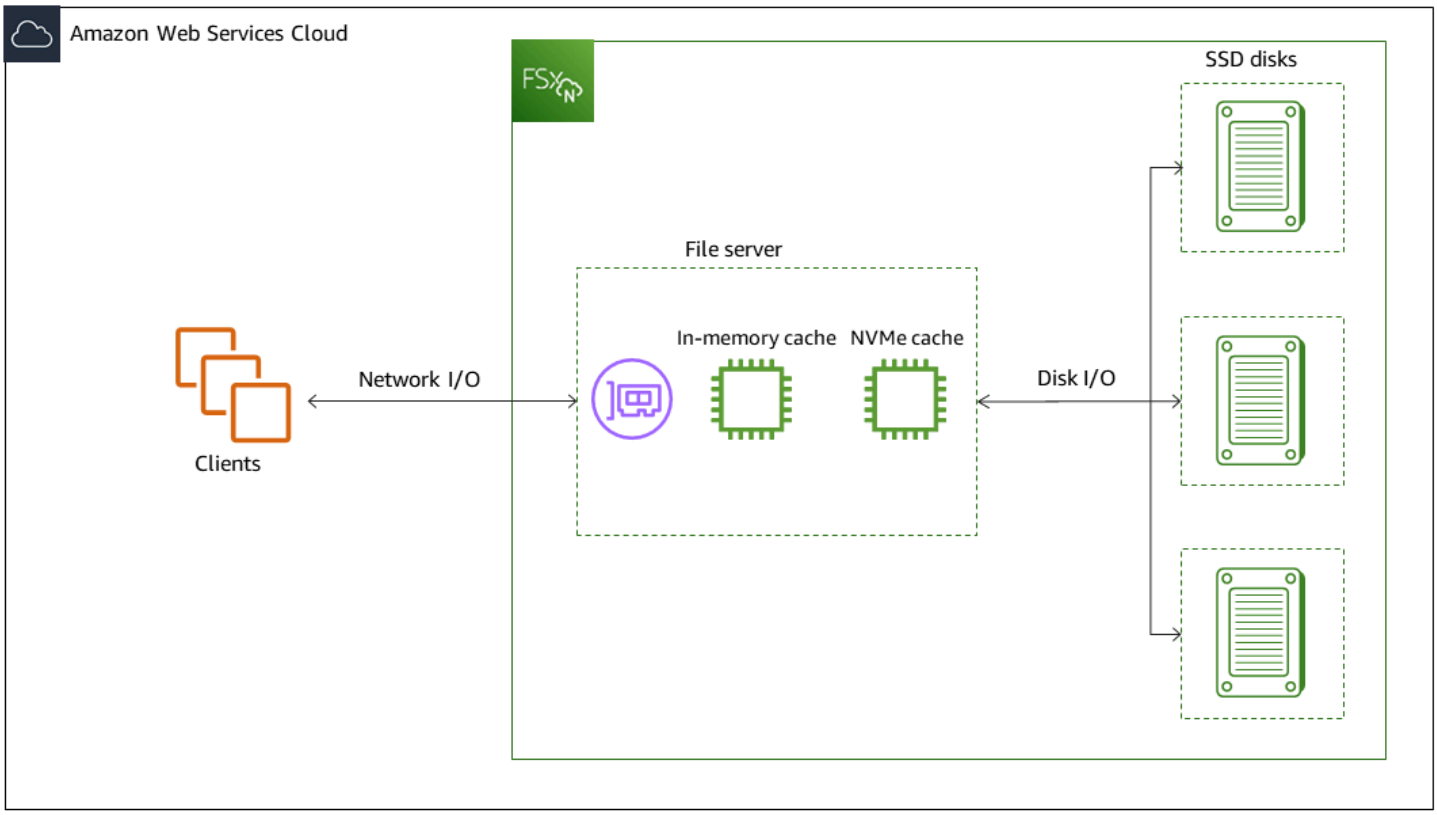
점보 프레임

최대 읽기 또는 쓰기 처리량을 달성하려면 클라이언트 EC2 인스턴스를 포함하여 Amazon FSx 파일 시스템의 데이터 경로에 있는 모든 네트워크 인터페이스에서 점보 프레임을 활성화하는 것이 좋습니다. FSx for ONTAP 파일 시스템의 네트워크 인터페이스에 대한 기본 최대 전송 단위(MTU) 설정은 9,001 바이트입니다.

성능 세부 정보

Amazon FSx 파일 시스템의 아키텍처 구성 요소를 검토하여 Amazon FSx for NetApp ONTAP 성능 모델을 자세히 파악할 수 있습니다. 클라이언트 컴퓨팅 인스턴스는에 있든 AWS 온프레미스에 있든 상관없이 하나 이상의 탄력적 네트워크 인터페이스(ENI)를 통해 파일 시스템에 액세스합니다. 이러한 네트워크 인터페이스는 파일 시스템과 연결하는 Amazon VPC에 있습니다. 각 파일 시스템 ENI 뒤에는 네트워크를 통해 파일 시스템에 액세스하는 클라이언트에 데이터를 제공하는 NetApp ONTAP 파일 서버가 있습니다. Amazon FSx는 각 파일 서버에 고속 인 메모리 캐시와 NVMe 캐시를 제공하여 가장 자주 액세스하는 데이터의 성능을 향상시킵니다. 각 파일 서버에는 파일 시스템 데이터를 호스팅하는 SSD 디스크가 연결되어 있습니다.

다음 다이어그램은 이러한 구성 요소를 보여줍니다.



네트워크 인터페이스, 인 메모리 캐시, NVMe 캐시 및 스토리지 볼륨과 같은 아키텍처 구성 요소에 상응하는 것이 전체 처리량 및 IOPS 성능을 결정하는 Amazon FSx for NetApp ONTAP 파일 시스템의 주요 성능 특성입니다.

- 네트워크 I/O 성능: 클라이언트와 파일 서버 간 요청의 처리량/IOPS(집계)
- 파일 서버의 인 메모리 및 NVMe 캐시 크기: 캐싱에 사용할 수 있는 활성 작업 세트의 크기
- 디스크 I/O 성능: 파일 서버와 스토리지 디스크 간 요청의 처리량 및 IOPS

파일 시스템의 이러한 성능 특성을 결정하는 두 가지 요소가 있는데, 바로 파일 시스템에 대해 구성하는 총 SSD IOPS와 처리량 용량입니다. 처음 두 가지 성능 특성(네트워크 I/O 성능과 인 메모리 및 NVMe 캐시 크기)은 처리량 용량에 의해서만 결정되는 반면, 세 번째인 디스크 I/O 성능은 처리량 용량과 SSD IOPS의 조합에 의해 결정됩니다.

파일 기반 워크로드는 일반적으로 변동이 심하며, 버스트 간 유휴 시간이 길고, 집중적으로 단기간 높은 I/O가 발생하는 것이 특징입니다. 변동이 심한 워크로드를 지원하기 위해 Amazon FSx는 파일 시스템이 연중무휴로 유지할 수 있는 기본 속도 외에도 네트워크 I/O 및 디스크 I/O 작업 모두에 대해 일정 기간 동안 더 빠른 속도로 버스트할 수 있는 기능을 제공합니다. Amazon FSx는 네트워크 I/O 크레딧 메커니즘을 사용하여 평균 사용률을 기준으로 처리량과 IOPS를 할당합니다. 파일 시스템은 처리량과

IOPS 사용량이 기준 한도 미만일 때 크레딧을 적립하고 I/O 작업을 수행할 때 이 크레딧을 사용할 수 있습니다.

> **Note**
>
> iSCSI 및 NVMe/TCP SAN 프로토콜의 경우 순차 읽기 클라이언트 작업은 파일 시스템의 최대 네트워크 I/O 버스트 또는 기준 처리량까지 달성할 수 있습니다.

쓰기 작업은 읽기 작업보다 2배 많은 네트워크 대역폭을 사용합니다. 쓰기 작업은 보조 파일 서버에 복제해야 하므로 한 번의 쓰기 작업으로 네트워크 처리량이 두 배가 됩니다.

배포 유형이 성능에 미치는 영향

FSx for ONTAP를 사용하여 Single-AZ 및 Multi-AZ 파일 시스템을 생성할 수 있습니다. 1세대 파일 시스템(Single-AZ 및 Multi-AZ 모두)과 2세대 Multi-AZ 파일 시스템은 하나의 고가용성(HA) 페어로 구동됩니다. 2세대 Single-AZ 파일 시스템은 최대 12개의 HA 페어로 구동됩니다. 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

FSx for ONTAP 다중 AZ 및 단일 AZ 파일 시스템은 SSD 스토리지를 사용할 경우 일관된 파일 작업에 지연 시간이 1밀리초 미만이고, 용량 풀 스토리지의 경우 지연 시간이 수십 밀리초입니다. 또한 다음 요구 사항을 충족하는 파일 시스템은 NVMe 읽기 캐시를 제공하여 읽기 지연 시간을 줄이고 자주 읽는 데이터의 IOPS를 높입니다.

- Multi-AZ 1 및 Multi-AZ 2 파일 시스템
- 2022년 11월 28일 이후에 생성된, 처리량 용량이 2GBps 이상인 Single-AZ 1 파일 시스템
- 페어당 처리량 용량이 최소 6GBps인 Single-AZ 2 파일 시스템

> **Note**
>
> 2세대 파일 시스템(Single-AZ 2 및 Multi-AZ 2)의 경우 NVMe 캐시를 사용하면 워크로드가 처리량이 높거나 큰 I/O 워크로드의 총 처리량을 줄일 수 있습니다. 처리량이 많은 워크로드가 있는 경우 NVMe 캐시를 비활성화하는 것이 좋습니다. 자세한 내용은 NVMe 캐시 관리 단원을 참조하십시오.

다음 표에는 고가용성(HA) 페어 수 및 가용성과 같은 요인에 따라 파일 시스템이 확장할 수 있는 처리량 용량이 나와 AWS 리전 있습니다.

First-generation file systems

이러한 성능 사양은 1세대 Single-AZ 및 Multi-AZ 파일 시스템에 적용됩니다.

1세대 파일 시스템의 HA 페어당 SSD 스토리지의 최대 처리량

	미국 동부(오하이오) 리전, 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 및 유럽(아일랜드)		FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든 경우	
	읽기 처리량 (MBps)	쓰기 처리량 (MBps)	읽기 처리량 (MBps)	쓰기 처리량 (MBps)
단일 AZ	4,096[1]	1,000	2,048	750
다중 AZ	4,096[1]	1,800	2,048	1,300

> **Note**
>
> [1] 4GBps의 처리량 용량을 프로비저닝하려면 파일 시스템을 최소 5,120GiB의 SSD 스토리지 용량과 160,000 SSD IOPS로 구성해야 합니다.

Second-generation file systems

이러한 성능 사양은 2세대 Single-AZ 및 Multi-AZ 파일 시스템에 적용됩니다. 일반적으로 2세대 파일 시스템은 읽기에 대해 전체 프로비저닝된 용량을 제공하고 쓰기에 대해 프로비저닝된 처리량 용량의 최대 1/3을 제공할 수 있습니다. 이 표에 나열된 6,144MB/s 옵션은 예외입니다.

2세대 파일 시스템의 HA 페어당 SSD 스토리지의 최대 처리량

	읽기 처리량(MBps)	쓰기 처리량(MBps)
단일 AZ	6,144[1]	1,024[1]
다중 AZ	6,144	2,048

> **Note**
>
> HA 페어당 [1]개(최대 12개). 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

스토리지 용량이 성능에 미치는 영향

파일 시스템이 달성할 수 있는 최대 디스크 처리량과 IOPS 수준은 다음의 경우 중 더 낮은 것입니다.

- 파일 시스템에서 선택한 처리량 용량을 기준으로 파일 서버에서 제공하는 디스크 성능 수준
- 파일 시스템에 프로비저닝한 SSD IOPS 수가 제공하는 디스크 성능 수준

기본적으로 파일 시스템의 SSD 스토리지는 최대 다음 수준의 디스크 처리량과 IOPS를 제공합니다.

- 디스크 처리량(스토리지 TiB당 MBps): 768
- 디스크 IOPS(스토리지 TiB당 IOPS): 3,072

처리량 용량이 성능에 미치는 영향

모든 Amazon FSx파일 시스템에는 파일 시스템을 생성할 때 구성하는 처리량 용량이 있습니다. 파일 시스템의 처리량 용량에 따라 네트워크 I/O 성능 수준 또는 파일 시스템을 호스팅하는 각 파일 서버가 네트워크를 통해 파일 데이터를 액세스하는 클라이언트에게 제공할 수 있는 속도가 결정됩니다. 각 파일 서버의 데이터 캐싱을 위한 더 많은 메모리와 NVMe(비휘발성 메모리 익스프레스) 스토리지, 각 파일 서버에서 지원하는 더 높은 수준의 디스크 I/O 성능으로 처리량 용량이 높아집니다.

파일 시스템을 생성할 때 선택적으로 더 높은 수준의 SSD IOPS를 프로비저닝할 수 있습니다. 파일 시스템이 달성할 수 있는 최대 SSD IOPS 수준은 추가 SSD IOPS를 프로비저닝하는 경우에도 파일 시스템의 처리량 용량에 따라 결정됩니다.

다음 표는 처리량 용량에 대한 전체 사양과 기준 및 버스트 수준, 해당 AWS 리전의 파일 서버의 캐싱에 필요한 메모리 양을 보여줍니다.

First-generation Single-AZ file system

이러한 성능 사양은 지정된 AWS 리전에서 2022년 11월 28일 이후에 생성된 1세대 Single-AZ 파일 시스템에 적용됩니다.

파일 시스템의 성능 사양 AWS 리전: 미국 동부(버지니아 북부), 미국 동부(오하이오), 미국 서부(오레곤) 및 유럽(아일랜드)

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 읽기 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트				기준	버스트	기준	버스트
128	188	1,500	x0,000(기본)	16	–	128	1,250	6,000	40,000
256	375	1,500		32	–	256	1,250	12,000	40,000
512	750	1,500	x00,000(기본)	64	–	512	1,250	20,000	40,000
1,024	1,500	–		128	–	1,024	1,250	40,000	–
2,048	3,125	–		256	1,900	2,048	–	80,000	–
4,096	6,250	–		512	5,400	4,096	–	160,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.

이러한 성능 사양은 FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든의 1세대 Single-AZ 파일 시스템에 적용됩니다.

FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든 의 파일 시스템에 대한 성능 사양

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트			기준	버스트	기준	버스트

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
128	150	1,250	x0,000(기본)	16	128	600	6,000	18,750
256	300	1,250		32	256	600	12,000	18,750
512	625	1,250	x00,000(기본)	64	512	600	18,750	–
1,024	1,500	–		128	1,024	–	40,000	–
2,048	3,125	–		256	2,048	–	80,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.

Second-generation Single-AZ file system

이러한 성능 사양은 2세대 Single-AZ 파일 시스템에 적용됩니다.

2세대 Single-AZ 파일 시스템의 성능 사양

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트				기준	버스트	기준	버스트
384**	781	6,250	x00,000(기본)	16	–	384	3,125	12,500	65,000
768**	1,563	6,250		32	–	768	3,125	25,000	65,000
1,536	3,125	6,250		64	–	1,536	3,125	50,000	65,000

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
3,072	6,250	–		128	–	3,072	–	100,000	–
6,144	12,500	–		256	1,900	6,144	–	200,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.
> ** 2세대 Single-AZ 파일 시스템은 384 및 768 처리량 용량을 지원하지만 HA 페어는 하나만 지원합니다. HA 페어를 추가하려면 파일 시스템을 최소 1,536MBps의 처리량 용량으로 구성해야 합니다.

First-generation Multi-AZ file system

이러한 성능 사양은 지정된 AWS 리전에서 2022년 11월 28일 이후에 생성된 1세대 Multi-AZ 파일 시스템에 적용됩니다.

파일 시스템의 성능 사양 AWS 리전: 미국 동부(버지니아 북부), 미국 동부(오하이오), 미국 서부(오레곤) 및 유럽(아일랜드)

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트				기준	버스트	기준	버스트
128	188	1,500	x0,000(기본)	16	238	128	1,250	6,000	40,000
256	375	1,500		32	475	256	1,250	12,000	40,000
512	750	1,500	x00,000(기본)	64	950	512	1,250	20,000	40,000

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
1,024	1,500	–		128	1,900	1,024	1,250	40,000	–
2,048	3,125	–		256	3,800	2,048	–	80,000	–
4,096	6,250	–		512	7,600	4,096	–	160,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.

이러한 성능 사양은 FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든의 1세대 다중 AZ 파일 시스템에 적용됩니다.

FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든의 파일 시스템에 대한 성능 사양

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트				기준	버스트	기준	버스트
128	150	1,250	x0,000(기본)	16	150	128	600	6,000	18,750
256	300	1,250		32	300	256	600	12,000	18,750
512	625	1,250	x00,000(기본)	64	600	512	600	18,750	–
1,024	1,500	–		128	1,200	1,024	–	40,000	–
2,048	3,125	–		256	2,400	2,048	–	80,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.

Second-generation Multi-AZ file systems

이러한 성능 사양은 2세대 Multi-AZ 파일 시스템에 적용됩니다.

2세대 Multi-AZ 파일 시스템의 성능 사양

FSx 처리량 용량 (MBps)	FSx 처리량 용량 (MBps)		네트워크 IOPS	인 메모리 캐싱 (GB)	NVMe 캐싱 (GB)	디스크 처리량 (MBps)		SSD 드라이브 IOPS*	
	기준	버스트				기준	버스트	기준	버스트
384	781	6,250	x00,000(기본)	16	237	384	3,125	12,500	65,000
768	1,563	6,250		32	474	768	3,125	25,000	65,000
1,536	3,125	6,250		64	950	1,536	3,125	50,000	65,000
3,072	6,250	–		128	1,900	3,072	–	100,000	–
6,144	12,500	–		256	3,800	6,144	–	200,000	–

> **Note**
>
> * SSD IOPS는 파일 서버의 인 메모리 캐시 또는 NVMe 캐시에 캐싱되지 않은 데이터에 액세스할 때만 사용됩니다.

예: 스토리지 용량 및 처리량 용량

다음 예제는 스토리지 용량과 처리량 용량이 파일 시스템 성능에 미치는 영향을 보여줍니다.

2TB의 SSD 스토리지 용량과 512MBps의 처리량 용량으로 구성된 1세대 파일 시스템의 처리량 수준은 다음과 같습니다.

- 네트워크 처리량 – 기준 625MBps 및 버스트 1,250MBps(처리량 용량 표 참조)
- 디스크 처리량 – 기준 512MBps 및 버스트 600MBps

따라서 파일 시스템에 액세스하는 워크로드는 파일 서버 인 메모리 캐시 및 NVMe 캐시에 캐싱된 활성 액세스 데이터에 수행되는 파일 작업에 대해 기준 처리량을 최대 625MBps까지, 버스트 처리량을 최대 1,250MBps까지 높일 수 있습니다.

FSx for ONTAP 리소스 관리

AWS Management Console AWS CLI및 ONTAP CLI와 API를 사용하여 FSx for ONTAP 리소스에 대해 다음 관리 작업을 수행할 수 있습니다.

- 파일 시스템, 스토리지 가상 머신(SVM), 볼륨, 백업 및 태그를 만들고, 나열하고, 업데이트하고, 삭제할 수 있습니다.
- 액세스, 관리 계정 및 암호, 암호 요구 사항, SMB 및 iSCSI 프로토콜, 기존 파일 시스템의 탑재 대상에 대한 네트워크 액세스 가능성 관리

주제

스토리지 용량 관리

Amazon FSx for NetApp ONTAP은 파일 시스템의 스토리지 용량을 관리하는 데 사용할 수 있는 다양한 스토리지 관련 기능을 제공합니다.

주제

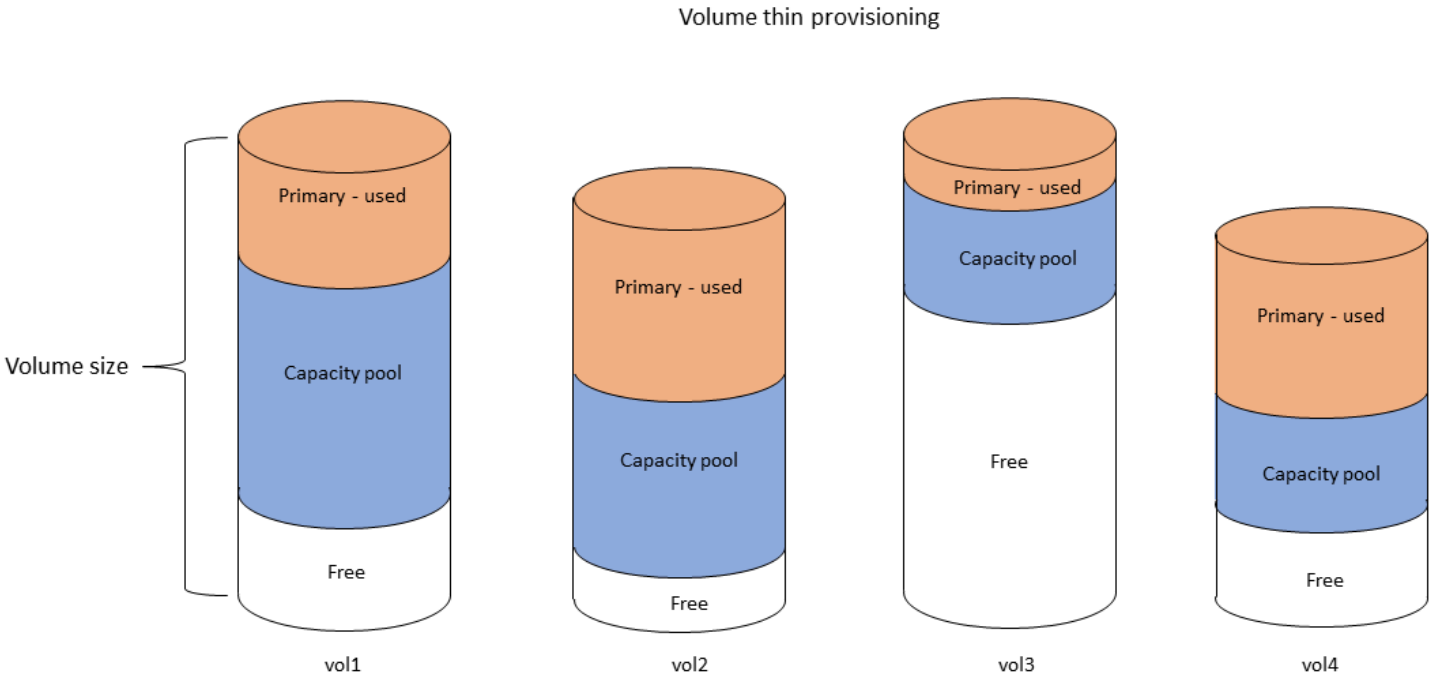
FSx for ONTAP 스토리지 계층

스토리지 계층은 Amazon FSx for NetApp ONTAP 파일 시스템에 대한 물리적 스토리지 미디어입니다. FSx for ONTAP은 다음과 같은 스토리지 계층을 제공합니다.

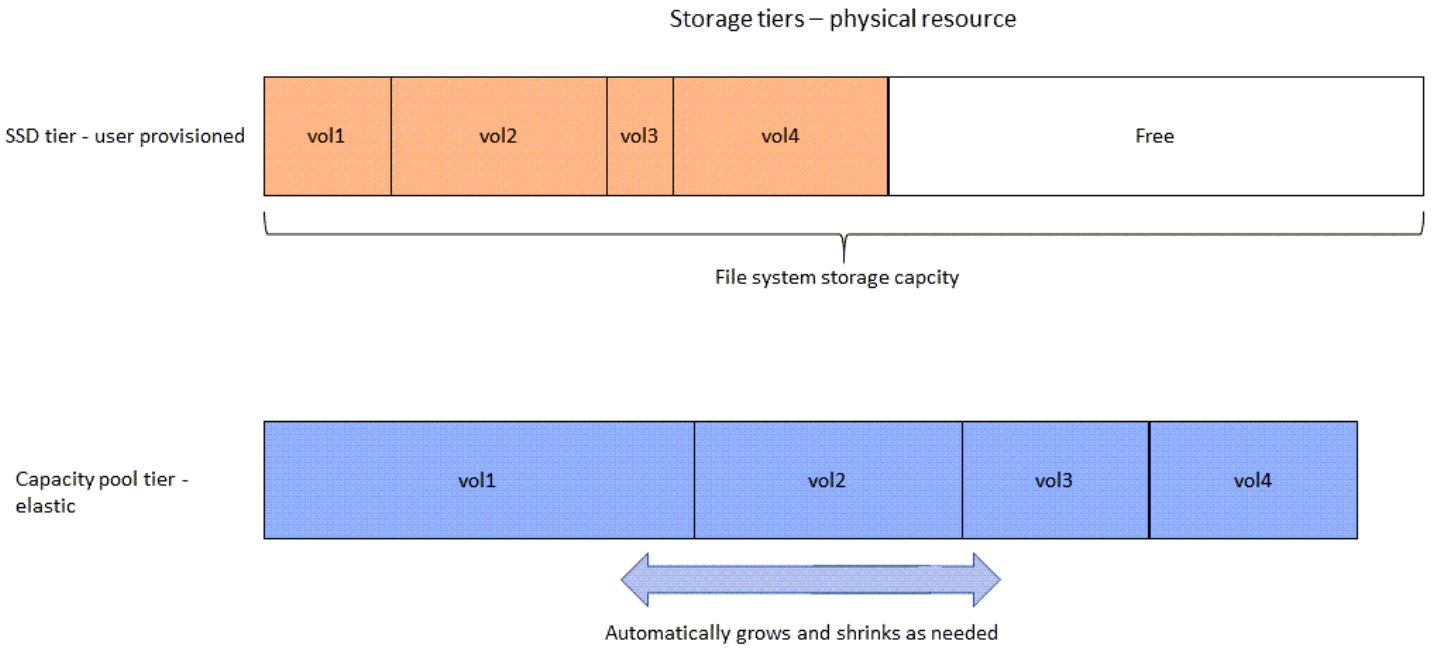
- SSD 계층 - 데이터 세트의 활성 부분을 위해 특별히 구축된 사용자 프로비저닝 고성능 솔리드 스테이트 드라이브(SSD) 스토리지입니다.
- 용량 풀 계층 - 자동으로 페타바이트까지 확장할 수 있고 자주 액세스하지 않는 데이터에 맞게 비용을 최적화하는 완전히 탄력적인 스토리지입니다.

FSx for ONTAP 볼륨은 폴더와 마찬가지로 스토리지 용량을 사용하지 않는 가상 리소스입니다. 저장되어 물리적 스토리지를 사용하는 데이터는 볼륨 내에 있습니다. 볼륨을 생성할 때 크기를 지정하며, 볼륨을 만든 후에 크기를 수정할 수 있습니다. FSx for ONTAP 볼륨은 씬 프로비저닝되며 파일 시스템 스토리지는 미리 예약되지 않습니다. 대신 필요에 따라 SSD 및 용량 풀 스토리지가 동적으로 할당됩니다. 볼륨 수준에서 구성하는 계층화 정책은 SSD 계층에 저장된 데이터가 용량 풀 계층으로 전환되는지 여부 및 시기를 결정합니다.

다음 다이어그램에서는 파일 시스템의 여러 FSx for ONTAP 볼륨에 배치된 데이터의 예제를 보여줍니다.



다음 다이어그램에서는 이전 다이어그램의 4개 볼륨에 있는 데이터가 파일 시스템의 물리적 스토리지 용량을 어떻게 사용하는지 보여줍니다.



파일 시스템의 각 볼륨 요구 사항을 가장 잘 충족하는 계층화 정책을 선택하면 스토리지 비용을 줄일 수 있습니다. 자세한 내용은 볼륨 데이터 계층화 단원을 참조하십시오.

적절한 양의 파일 시스템 SSD 스토리지 선택하기

FSx for ONTAP 파일 시스템의 SSD 스토리지 용량을 선택할 때는 데이터를 저장하는 데 사용할 수 있는 SSD 스토리지의 양에 영향을 미치는 다음 항목을 염두에 두어야 합니다.

- NetApp ONTAP 소프트웨어 오버헤드를 위해 예약된 스토리지 용량.
- 파일 메타데이터
- 최근에 작성된 데이터
- 휴지 기간에 도달하지 않은 데이터이든, 최근에 읽은 데이터를 SSD로 다시 검색했든 상관없이 SSD 스토리지에 저장하려는 파일.

SSD 스토리지 사용 방식

파일 시스템의 SSD 스토리지는 NetApp ONTAP 소프트웨어(오버헤드), 파일 메타데이터 및 데이터의 조합에 사용됩니다.

NetApp ONTAP 소프트웨어 오버헤드

다른 NetApp ONTAP 파일 시스템과 마찬가지로, 파일 시스템의 SSD 스토리지 용량의 최대 16%는 ONTAP 오버헤드용으로 예약되어 있으므로 파일을 저장하는 데 사용할 수 없습니다. ONTAP 오버헤드는 다음과 같이 할당됩니다.

- 11%는 NetApp ONTAP 소프트웨어용으로 예약되어 있습니다. SSD 저장 용량이 30TB(테비바이트)를 초과하는 파일 시스템의 경우 6%가 예약되어 있습니다.
- 5%는 두 파일 시스템의 파일 서버 간에 데이터를 동기화하는 데 필요한 집계 스냅샷에만 사용됩니다.

파일 메타데이터

파일 메타데이터는 일반적으로 파일이 사용하는 스토리지 용량의 3~7%를 차지합니다. 이 비율은 평균 파일 크기(평균 파일 크기가 작을수록 메타데이터가 더 많이 필요함) 및 파일에서 달성한 스토리지 효율성 절감량에 따라 달라집니다. 파일 메타데이터는 스토리지 효율성 절감의 혜택을 받지 못한다는 점에 유의하세요. 다음 지침을 사용하여 파일 시스템의 메타데이터에 사용되는 SSD 스토리지의 양을 추정할 수 있습니다.

평균 파일 크기	메타데이터 크기(파일 데이터의 백분율)
4KB	7%
8KB	3.5%
32KB 이상	1-3%

용량 풀 계층에 저장하려는 파일의 메타데이터에 필요한 SSD 스토리지 용량의 크기를 조정할 때는 용량 풀 계층에 저장하려는 데이터 10GiB당 SSD 스토리지 1GiB의 보수적인 비율을 사용하는 것이 좋습니다.

SSD 계층에 저장된 파일 데이터

활성 데이터 세트와 모든 파일 메타데이터 외에도 파일 시스템에 기록된 모든 데이터는 처음에 SSD 계층에 기록된 후 용량 풀 스토리지 계층으로 이동됩니다. 이는 볼륨의 계층화 정책에 관계없이 적용됩니다. 단, 모든 데이터 계층화 정책으로 구성된 볼륨에서 SnapMirror를 사용할 때 데이터가 용량 풀 스토리지에 직접 기록되는 경우는 예외입니다.

용량 풀 계층의 임의 읽기는 SSD 계층의 사용률이 90% 미만인 한 SSD 계층에 캐시됩니다. 자세한 내용은 볼륨 데이터 계층화 단원을 참조하십시오.

권장 SSD 용량 사용률

SSD 스토리지 계층의 사용률은 지속적으로 80%를 초과하지 않는 것이 좋습니다. 2세대 파일 시스템의 경우, 파일 시스템의 집계 사용률이 지속적으로 80%를 초과하지 않도록 하는 것이 좋습니다. 이러한 권장 사항은 ONTAP에 대한 NetApp의 권장 사항과 일치합니다. 파일 시스템의 SSD 계층은 용량 풀 계층에 대한 스테이징 쓰기 및 용량 풀 계층에서의 임의 읽기에도 사용되므로 액세스 패턴이 갑자기 변경되면 SSD 계층의 사용률이 빠르게 증가할 수 있습니다.

SSD 사용률이 90%이면 용량 풀 계층에서 읽은 데이터가 더 이상 SSD 계층에 캐시되지 않으므로 파일 시스템에 기록되는 새 데이터를 위해 남은 SSD 용량이 보존됩니다. 이로 인해 SSD 계층에서 캐시하여 읽는(파일 시스템의 처리량 용량에 영향을 미칠 수 있음) 대신 용량 풀 계층에서 동일한 데이터를 반복적으로 읽어 용량 풀 스토리지에서 읽을 수 있습니다.

SSD 계층 사용률이 98% 이상이면 모든 계층화 기능이 중지됩니다. 자세한 내용은 계층화 임계값 단원을 참조하십시오.

스토리지 효율성

NetApp ONTAP는 압축, 압축 및 중복 제거를 포함하는 볼륨 수준에서 블록 수준 스토리지 효율성 기능을 제공합니다. 2세대 파일 시스템의 경우, 파일 시스템의 집계 사용률이 지속적으로 65%를 초과하지 않도록 하는 것이 좋습니다. 볼륨 단위로 스토리지 효율성을 활성화할 수 있습니다. 이러한 기능은 데이터가 소비하는 스토리지 용량을 줄여 SSD, 용량 풀 및 백업 스토리지의 스토리지 공간을 적게 소비할 수 있도록 합니다. SSD 스토리지의 데이터에 대해 각 볼륨에서 압축 및 중복 제거를 활성화할 수 있습니다. 데이터를 용량 풀 스토리지로 계층화하면 SSD 스토리지의 압축 및 중복 제거를 통해 절약되는 스토리지가 보존됩니다. 파일 시스템의 스토리지 효율성 구성에 관계없이 백업 데이터에 대해 항상 스토리지 효율성이 활성화됩니다.

다음 표는 일반적인 스토리지 절약의 예를 보여줍니다.

	압축 전용	중복 제거 전용	압축 & 중복 제거
범용 파일 공유	50%	30%	65%
가상 서버 & 데스크톱	55%	70%	70%
데이터베이스 수	65-70%	0%	65-70%

	압축 전용	중복 제거 전용	압축 & 중복 제거
데이터 엔지니어링	55%	30%	75%
지질 데이터	40%	3%	40%

대부분의 워크로드에서 압축 및 중복 제거를 활성화해도 파일 시스템 성능에 부정적인 영향을 미치지 않습니다. 대부분의 워크로드에서 압축은 전반적인 성능을 향상시킵니다. RAM 캐시에서 빠른 읽기 및 쓰기를 제공하기 위해 FSx for ONTAP 파일 서버는 파일 서버와 스토리지 디스크 간에 사용할 수 있는 것보다 프런트엔드 네트워크 인터페이스 카드(NICs)에 더 높은 수준의 네트워크 대역폭을 갖추고 있습니다. 데이터 압축은 파일 서버와 스토리지 디스크 간에 전송되는 데이터의 양을 줄이므로 대부분의 워크로드에서 데이터 압축을 사용하면 전체 파일 시스템 처리 용량이 증가하는 것을 볼 수 있습니다. 데이터 압축과 관련된 처리량 용량 증가는 파일 시스템의 프런트엔드 NIC가 포화 상태가 되면 제한됩니다.

Amazon FSx for NetApp ONTAP은 스냅샷, 씬 프로비저닝 및 FlexClone 볼륨을 포함하여 공간을 절약하는 다른 ONTAP 기능도 지원합니다.

스토리지 효율성 기능은 기본적으로 활성화되어 있지 않습니다. 다음과 같이 활성화할 수 있습니다.

- 파일 시스템을 생성할 때 SVM의 루트 볼륨에서.
- 새 볼륨을 생성할 때.
- 기존 볼륨을 수정할 때.

스토리지 효율성이 활성화된 파일 시스템의 스토리지 절감액을 보려면 스토리지 효율성 절감 모니터링을 참조하세요.

스토리지 효율성 절감액 계산

압축, 중복 제거, 압축, 스냅샷 및 FlexClones로 인한 스토리지 절감 효과를 계산하기 위해 `LogicalDataStored` 및 `StorageUsed` FSx for ONTAP CloudWatch 파일 시스템 지표를 사용할 수 있습니다. 이러한 지표에는 단일 측정기준인 `FileSystemId`가 포함되어 있습니다. 자세한 내용은 파일 시스템 지표 단원을 참조하십시오.

- 스토리지 효율성 절감 효과를 바이트 단위로 계산하려면 지정된 기간 동안의 `StorageUsed` 평균을 구하고 거기에서 동일한 기간 동안의 `LogicalDataStored` 평균을 뺍니다.
- 스토리지 효율성 절감 효과를 총 논리적 데이터 크기의 백분율로 계산하려면 지정된 기간 동안의 `StorageUsed`의 `Average`를 구하고 거기에서 동일한 기간 동안의 `LogicalDataStored`의

Average를 뺍니다. 그런 다음 그 차이를 동일한 기간 동안의 LogicalDataStored의 Average로 나눕니다.

SSD 크기 조정 예제

데이터의 80%가 자주 액세스되지 않는 애플리케이션을 위해 100TiB의 데이터를 저장한다고 가정해 보겠습니다. 이 시나리오에서는 데이터의 80%(80TiB)가 용량 풀 계층으로 자동으로 계층화되고 나머지 20%(20TiB)는 SSD 스토리지에 남아 있습니다. 범용 파일 공유 워크로드의 일반적인 스토리지 효율성 절감 효과인 65%를 기준으로 하면, 이는 7TiB의 데이터에 해당합니다. 80%의 SSD 사용률을 유지하려면 활발하게 액세스하는 20TiB의 데이터에 대해 8.75TiB의 SSD 스토리지 용량이 필요합니다. 다음 계산에서 볼 수 있듯이 프로비저닝하는 SSD 스토리지의 양에는 ONTAP 소프트웨어 스토리지 오버헤드 16%도 고려해야 합니다.

```
ssdNeeded = ssdProvisioned * (1 - 0.16)
8.75 TiB / 0.84 = ssdProvisioned
10.42 TiB = ssdProvisioned
```

따라서 이 예제에서는 최소 10.42TiB의 SSD 스토리지를 프로비저닝해야 합니다. 또한 자주 액세스하지 않는 나머지 80TiB의 데이터에는 28TiB의 용량 풀 스토리지를 사용하게 됩니다.

파일 시스템 스토리지 용량 및 IOPS

FSx for ONTAP 파일 시스템을 생성할 때 SSD 계층의 스토리지 용량을 지정합니다. 2세대 Single-AZ 파일 시스템의 경우 지정한 스토리지 용량은 각 고가용성(HA) 페어의 스토리지 풀 간에 고르게 분산됩니다. 이러한 스토리지 풀을 집계라고 합니다.

프로비저닝하는 SSD 스토리지의 각 GiB에 대해 Amazon FSx는 파일 시스템에 3 SSD IOPS(Input/Output Operations Per Second)를 자동으로 프로비저닝하여, 파일 시스템당 최대 160,000 SSD IOPS를 제공합니다. 2세대 단일 AZ 파일 시스템의 경우, SSD IOPS는 각 파일 시스템의 집계에 균등하게 분산됩니다. GiB당 자동 SSD IOPS 3보다 높게 프로비저닝된 SSD IOPS 수준을 지정할 수 있습니다. FSx for ONTAP 파일 시스템에 프로비저닝할 수 있는 최대 SSD IOPS 수에 대한 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

주제

- 파일 시스템 SSD 스토리지 및 IOPS 업데이트
- 파일 시스템에 대한 스토리지 용량 사용률 알람 만들기
- 스토리지 용량 및 프로비저닝된 IOPS 업데이트

- 스토리지 용량 동적 업데이트
- SSD 스토리지 사용률 모니터링
- 스토리지 효율성 절감 모니터링
- 스토리지 용량 및 IOPS 업데이트 모니터링

파일 시스템 SSD 스토리지 및 IOPS 업데이트

데이터 세트의 활성 부분을 위한 추가 스토리지가 필요한 경우 Amazon FSx for NetApp ONTAP 파일 시스템의 SSD 스토리지 용량을 늘릴 수 있습니다. Amazon FSx 콘솔, Amazon FSx API 또는 AWS Command Line Interface (AWS CLI)를 사용하여 SSD 스토리지 용량을 늘립니다. 자세한 내용은 스토리지 용량 및 프로비저닝된 IOPS 업데이트 단원을 참조하십시오.

Amazon FSx 파일 시스템의 SSD 스토리지 용량을 늘리면 일반적으로 몇 분 내에 새 용량을 사용할 수 있습니다. 새 SSD 스토리지 용량을 사용할 수 있게 된 후에 요금이 청구됩니다. 요금에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 요금을 참조하세요.

스토리지 용량을 늘리면 Amazon FSx는 백그라운드에서 스토리지 최적화 프로세스를 실행하여 데이터를 재조정합니다. 대부분의 파일 시스템에서 스토리지 최적화는 워크로드 성능에 미치는 영향을 최소화하면서 몇 시간이 걸립니다.

Amazon FSx 콘솔, CLI 및 API를 사용하여 언제든지 스토리지 최적화 프로세스의 진행 상황을 추적할 수 있습니다. 자세한 내용은 스토리지 용량 및 IOPS 업데이트 모니터링 단원을 참조하십시오.

고려 사항

다음은 파일 시스템의 SSD 스토리지 용량과 프로비저닝된 IOPS를 수정할 때 고려해야 할 몇 가지 중요한 항목입니다.

- 스토리지 용량 증가만 - 파일 시스템의 SSD 스토리지 용량을 늘릴 수만 있고 스토리지 용량을 줄일 수는 없습니다.
- 저장 용량 최소 증가 - 각 SSD 저장 용량 증가는 파일 시스템의 현재 SSD 저장 용량의 최소 10%에서 파일 시스템 구성에 대한 최대 SSD 저장 용량까지여야 합니다.
- (2세대 단일 AZ 파일 시스템만 해당) 스토리지 용량 분산 - 파일 시스템에 대해 선택한 새 스토리지 용량 또는 SSD IOPS는 각 파일 시스템의 집계에 고르게 분산됩니다.
- 증가 사이 경과 시간 - 파일 시스템에서 SSD 스토리지 용량, 프로비저닝된 IOPS 또는 처리량 용량을 수정한 후에는 동일한 파일 시스템에서 이러한 구성을 다시 수정하려면 6시간 이상 기다려야 합니다. 이를 때로 휴지 기간이라고도 합니다.

- 프로비저닝된 IOPS 모드 - 프로비저닝된 IOPS를 변경하려면 다음 두 IOPS 모드 중 하나를 지정해야 합니다.
  - 자동 모드 - Amazon FSx는 파일 시스템 구성의 최대 SSD IOPS까지, SSD 스토리지 용량 1GB당 프로비저닝된 SSD IOPS 3개를 유지하도록 SSD IOPS를 자동으로 확장합니다.

    > **Note**
    >
    > FSx for ONTAP 파일 시스템에 프로비저닝할 수 있는 최대 SSD IOPS 수에 대한 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

  - 사용자 프로비저닝 모드 - SSD IOPS 수를 지정하며, 이 수는 SSD 스토리지 용량의 GiB당 3 IOPS 이상이어야 합니다. 더 높은 수준의 IOPS를 프로비저닝하기로 선택한 경우 해당 월에 포함된 요금을 초과하여 프로비저닝된 평균 IOPS(IOPS-월로 측정)에 대한 비용을 지불하면 됩니다.

요금에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 요금을 참조하세요.

SSD 스토리지 용량을 늘려야 하는 경우

사용 가능한 SSD 계층 스토리지가 부족한 경우 파일 시스템의 스토리지 용량을 늘리는 것이 좋습니다. 스토리지가 부족하면 데이터 세트의 활성 부분에 비해 SSD 계층 크기가 작다는 의미입니다.

파일 시스템에서 사용 가능한 여유 스토리지의 양을 모니터링하려면 파일 시스템 수준 `StorageCapacity` 및 `StorageUsed` Amazon CloudWatch 지표를 사용합니다. 이 지표에 CloudWatch 경보를 생성하고 특정 임계값 아래로 떨어지면 알림을 받을 수 있습니다. 자세한 내용은 Amazon CloudWatch를 사용한 모니터링 단원을 참조하십시오.

> **Note**
>
> 데이터 계층화, 처리량 조정 및 기타 유지 관리 작업이 제대로 작동하고 추가 데이터에 사용할 수 있는 용량이 확보되도록 SSD 스토리지 용량 사용률의 80%를 초과하지 않는 것이 좋습니다. 2세대 파일 시스템의 경우, 이 권장 사항은 파일 시스템의 모든 집계와 각 개별 집계에 대한 평균 사용률에 모두 적용됩니다.

파일 시스템의 SSD 스토리지 사용 방식과, 파일 메타데이터 및 운영 소프트웨어용으로 예약된 SSD 스토리지의 용량에 대한 자세한 내용은 적절한 양의 파일 시스템 SSD 스토리지 선택하기 섹션을 참조하세요.

파일 시스템에 대한 스토리지 용량 사용률 알람 만들기

평균 SSD 스토리지 용량 사용률은 지속적으로 80%를 초과하지 않는 것이 좋습니다. 가끔 SSD 스토리지 사용률이 80% 이상으로 급증하는 것은 괜찮습니다. 평균 사용률을 80% 미만으로 유지하면 문제 없이 스토리지를 늘릴 수 있는 충분한 용량을 확보할 수 있습니다. 다음 절차는 파일 시스템의 SSD 스토리지 사용률이 80%에 가까워질 때 알려주는 CloudWatch 알람을 만드는 방법을 보여 줍니다.

파일 시스템 스토리지 용량 사용률 알람을 만들려면 다음과 같이 하세요.

`StorageCapacityUtilization` 지표를 사용하여 하나 이상의 FSx for ONTAP 파일 시스템이 스토리지 사용률 임계값에 도달하면 트리거되는 경보를 생성할 수 있습니다.

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 경보 아래의 모든 경보를 선택합니다. 그런 다음 경보 생성을 선택합니다. 경보 생성 마법사에서 지표 선택을 선택합니다.
3. 그래프 탐색기에서 다중 소스 쿼리 탭을 선택합니다.
4. 쿼리 빌더에서 다음을 선택합니다.
   - 네임스페이스에서 AWS/FSx > 세부 파일 시스템 지표를 선택합니다.
   - 지표 이름 에서 MAX(StorageCapacityUtilization)를 선택합니다.
   - 필터링 기준의 경우 ID별로 특정 파일 시스템을 선택적으로 포함하거나 제외할 수 있습니다. 필터 기준을 비워두면 파일 시스템 중 하나가 알람의 저장 용량 사용률 임계값을 초과할 때 알람이 트리거됩니다.
   - 나머지 옵션은 비워 두고 그래프 쿼리를 선택합니다.
5. 지표 선택을 선택하세요. 마법사의 지표 섹션에서 지표에 레이블을 지정합니다. 기간을 5분으로 유지하는 것이 좋습니다.
6. 조건에서 지표가 80보다 크거나 같을 때마다 정적 임계값 유형을 선택합니다.
7. 다음을 선택하여 작업 구성 페이지로 이동합니다.

경보 작업을 구성한다면

설정한 임계값에 도달하면 알람이 트리거되도록 다양한 작업을 구성할 수 있습니다. 이 예에서는 단순 알림 서비스(SNS) 주제를 선택했지만, 다른 작업에 대해서는 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 알람 사용하기에서 확인할 수 있습니다.

1. 알림 섹션에서 알람이 ALARM 상태일 때 알림을 받을 SNS 토픽을 선택합니다. 기존 주제를 선택하거나 새로운 주제를 생성할 수 있습니다. 이메일 주소로 알람 알림을 받으려면 먼저 확인해야 하는 구독 알림을 받게 됩니다.
2. 다음을 선택합니다.

알람을 완료하려면 다음과 같이 하세요.

다음 안내에 따라 CloudWatch 알람을 만드는 과정을 완료하세요.

1. 이름 및 설명 추가 페이지에서 경보에 이름을 지정하고 선택적으로 설명을 지정한 다음 다음을 선택합니다.
2. 미리 보기 및 생성 페이지에서 구성한 모든 항목을 검토한 다음 경보 생성을 선택합니다.

스토리지 용량 및 프로비저닝된 IOPS 업데이트

파일 시스템의 SSD 기반 스토리지를 늘리고 Amazon FSx 콘솔, AWS CLI및 API를 사용하여 프로비저닝된 SSD IOPS의 양을 늘리거나 줄일 수 있습니다.

파일 시스템의 SSD 스토리지 용량 또는 프로비저닝된 IOPS 업데이트(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 열에서 파일 시스템을 선택합니다. 파일 시스템 목록에서, SSD 스토리지 용량 및 SSD IOPS를 업데이트할 FSx for ONTAP을 선택합니다.
3. 작업 > 스토리지 용량 업데이트를 선택합니다. 또는 요약 섹션에서 파일 시스템의 SSD 스토리지 용량 값 옆에 있는 업데이트를 선택합니다.

   SSD 스토리지 용량 및 IOPS 업데이트 대화 상자가 표시됩니다.

Update SSD storage capacity and IOPS

File system ID

fs-01234567890abcdef

Current configuration

SSD storage capacity: 4096 GiB
IOPS mode: Automatic (3 IOPS per GiB of SSD storage)
SSD IOPS: 12288

SSD storage capacity

☑ Modify storage capacity

Input type

◉ Percentage
○ Absolute

Desired % increase

10 %

Minimum 4506 GiB (10% above current); Maximum 1048576 GiB.

Provisioned SSD IOPS

◉ Automatic (3 IOPS per GiB of SSD storage)
○ User-provisioned

Configuration preview

Attribute	Current configuration	New configuration
SSD storage capacity	4,096 GiB (2,048 GiB per HA pair)	4,506 GiB (2,253 GiB per HA pair)
	Mode: Automatic	Mode: Automatic

4. SSD 스토리지 용량을 늘리려면 스토리지 용량 수정을 선택합니다.
5. 입력 유형에서 다음 중 하나를 선택합니다.
   - 새 SSD 스토리지 용량을 현재 값에서 변경된 백분율로 입력하려면 백분율을 선택합니다.
   - 새 값을 GiB로 입력하려면 절대값을 선택합니다.
6. 입력 유형에 따라 원하는 증가율(%) 값을 입력합니다.
   - 백분율에는 증가율 값을 입력합니다. 이 값은 현재 값보다 10% 이상 큰 값이어야 합니다.
   - 절대값에는 새 값을 GiB 단위로 입력합니다(최대 허용 값은 196,608GiB).
7. 프로비저닝된 SSD IOPS에는 파일 시스템의 프로비저닝된 SSD IOPS 수를 수정하는 두 가지 옵션이 있습니다.
   - Amazon FSx에서 SSD IOPS를 자동으로 확장하여 SSD 스토리지 용량 GiB당 프로비저닝된 3 SSD IOPS를 (최대 160,000까지) 유지하도록 하려면 자동을 선택합니다.
   - SSD IOPS 수를 지정하려면 사용자 프로비저닝을 선택합니다. SSD 스토리지 계층 GiB 용량의 3배 이상, 160,000 이하인 절대 IOPS 수를 입력합니다.

   > **Note**
   >
   > FSx for ONTAP 파일 시스템에 프로비저닝할 수 있는 최대 SSD IOPS 수에 대한 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

8. 업데이트를 선택합니다.

   > **Note**
   >
   > 프롬프트 하단에 새 SSD 스토리지 용량과 SSD IOPS에 대한 구성 미리보기가 표시됩니다. 2세대 파일 시스템의 경우 HA 쌍당 값도 표시됩니다.

파일 시스템에 대한 SSD 스토리지 용량 및 프로비저닝된 IOPS 업데이트(CLI)

FSx for ONTAP 파일 시스템의 SSD 스토리지 용량 및 프로비저닝된 IOPS를 업데이트하려면 AWS CLI 명령 update-file-system 또는 동등한 UpdateFileSystem API 작업을 사용합니다. 값으로 다음 파라미터를 설정합니다.

- `--file-system-id`를 업데이트하려는 파일 시스템의 ID로 설정합니다.

- SSD 저장 용량을 늘리려면 `--storage-capacity` 목표 저장 용량 값으로 설정하고, 이 값은 현재 값보다 10% 이상 커야 합니다.
- 프로비저닝된 SSD IOPS를 수정하려면 `--ontap-configuration DiskIopsConfiguration` 속성을 사용합니다. 이 속성에는 `Iops` 및 `Mode`라는 두 개의 파라미터가 있습니다.
  - 프로비저닝된 IOPS 수를 지정하려면 `Iops=number_of_IOPS`(최대 160,000) 및 `Mode=USER_PROVISIONED`를 사용합니다. IOPS 값은 요청된 SSD 스토리지 용량의 3배 이상이어야 합니다. 스토리지 용량을 늘리지 않는 경우 IOPS 값은 현재 SSD 스토리지 용량의 3배 이상이어야 합니다.
  - Amazon FSx에서 SSD IOPS를 자동으로 늘리려면 `Mode=AUTOMATIC`을 사용하고 `Iops` 파라미터를 사용하지 않습니다. Amazon FSx는 프로비저닝된 SSD 스토리지 용량(최대 160,000개)의 GiB당 3 SSD IOPS를 자동으로 유지합니다.

> **Note**
>
> FSx for ONTAP 파일 시스템에 프로비저닝할 수 있는 최대 SSD IOPS 수에 대한 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

다음 예에서는 파일 시스템의 SSD 스토리지를 2000GiB로 늘리고 사용자 프로비저닝된 SSD IOPS의 양을 7000으로 설정합니다.

```
aws fsx update-file-system \
--file-system-id fs-0123456789abcdef0 \
--storage-capacity 2000 \
--ontap-configuration 'DiskIopsConfiguration={Iops=7000,Mode=USER_PROVISIONED}'
```

업데이트 진행 상황을 모니터링하려면 describe-file-systems AWS CLI 명령을 사용합니다. 출력에서 `AdministrativeActions` 섹션을 찾습니다.

자세한 내용은 Amazon FSx for NetApp ONTAP API 참조의 AdministrativeAction을 참조하세요.

스토리지 용량 동적 업데이트

사용한 스토리지 용량이 지정한 임계값을 초과하는 경우 다음 솔루션을 사용하여 FSx for ONTAP 파일 시스템의 SSD 스토리지 용량을 동적으로 늘릴 수 있습니다. 이 AWS CloudFormation 템플릿은 스토리지 용량 임계값,이 임계값을 기반으로 하는 Amazon CloudWatch 경보, 파일 시스템의 스토리지 용량을 늘리는 AWS Lambda 함수를 정의하는 데 필요한 모든 구성 요소를 자동으로 배포합니다.

솔루션은 필요한 모든 구성 요소를 자동으로 배포하고 다음 파라미터를 사용합니다.

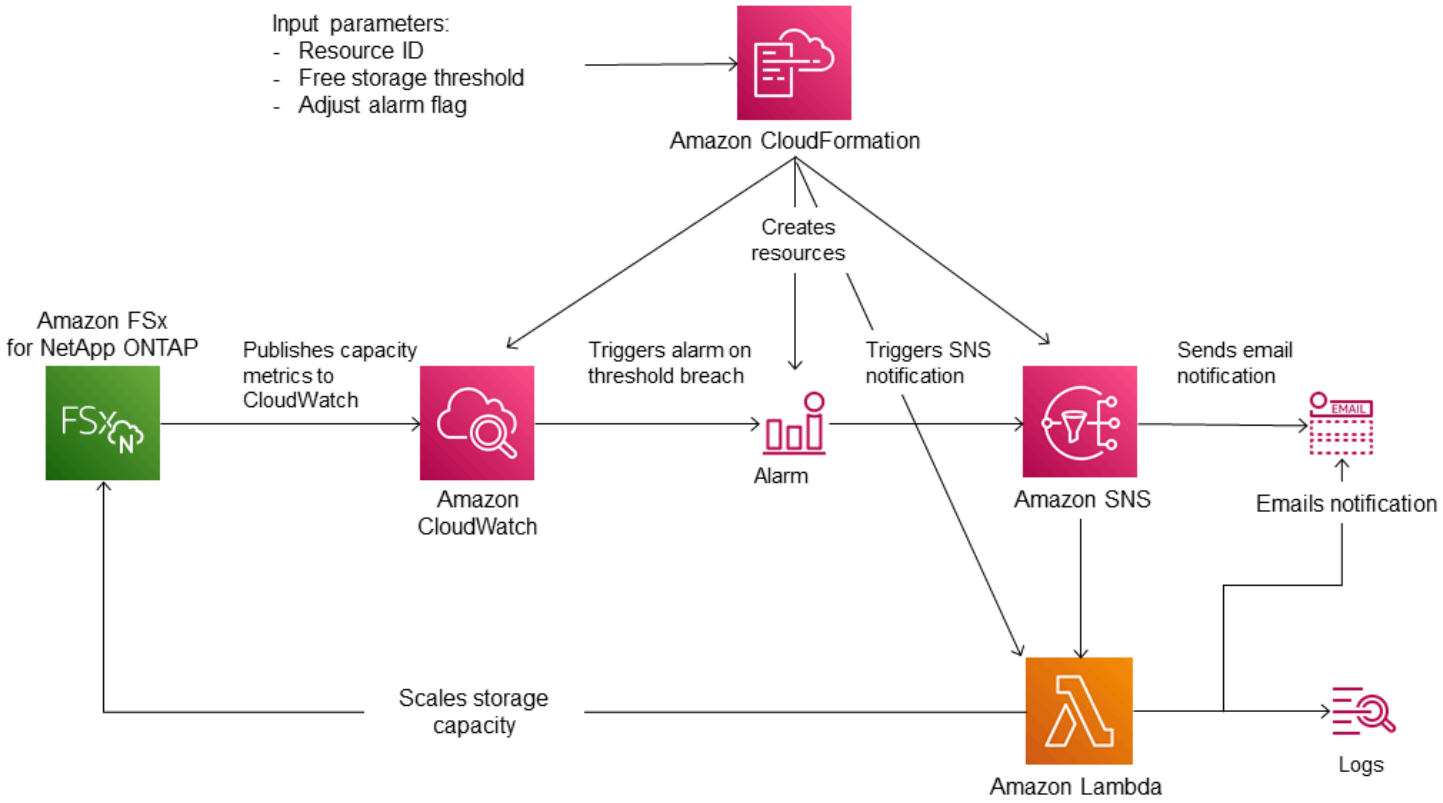
- FSx for ONTAP 파일 시스템 ID.
- 사용 가능한 스토리지 용량 임계값(숫자 값). 이는 CloudWatch 경보가 트리거되는 백분율입니다.
- 스토리지 용량 증가 기준 백분율(%).
- 스케일링 알림을 받는 데 사용되는 이메일 주소.

주제

- 아키텍처 개요
- AWS CloudFormation 템플릿
- 를 사용한 자동 배포 AWS CloudFormation

아키텍처 개요

이 솔루션을 배포하면 AWS 클라우드에 다음과 같은 리소스가 빌드됩니다.



다이어그램은 다음 단계들을 보여줍니다.

1. AWS CloudFormation 템플릿은 CloudWatch 경보, AWS Lambda 함수, Amazon Simple Notification Service(Amazon SNS) 대기열 및 모든 필수 AWS Identity and Access Management (IAM) 역할을

배포합니다. IAM 역할은 Lambda 함수에 Amazon FSx API 작업을 호출할 수 있는 권한을 부여합니다.

2. CloudWatch는 파일 시스템의 사용된 스토리지 용량이 지정된 임계값을 초과하면 경보를 트리거하고 Amazon SNS 대기열에 메시지를 보냅니다. 경보는 파일 시스템의 사용된 용량이 5분 동안 지속적으로 임계값을 초과하는 경우에만 트리거됩니다.
3. 그러면 솔루션이 이 Amazon SNS 주제를 구독하는 Lambda 함수를 트리거합니다.
4. Lambda 함수는 지정된 증가율 값을 기반으로 새 파일 시스템 스토리지 용량을 계산하고 새 파일 시스템 스토리지 용량을 설정합니다.
5. Lambda 함수 작업의 원래 CloudWatch 경보 상태 및 결과는 Amazon SNS 대기열로 전송됩니다.

CloudWatch 경보에 대한 응답으로 수행된 작업에 대한 알림을 받으려면 구독 확인 이메일에 제공된 링크를 따라 Amazon SNS 주제 구독을 확인해야 합니다.

AWS CloudFormation 템플릿

이 솔루션은 AWS CloudFormation 를 사용하여 FSx for ONTAP 파일 시스템의 스토리지 용량을 자동으로 늘리는 데 사용되는 구성 요소 배포를 자동화합니다. 이 솔루션을 사용하려면 FSxOntapDynamicStorageScaling AWS CloudFormation 템플릿을 다운로드합니다.

템플릿은 다음과 같이 설명된 파라미터를 사용합니다. 템플릿 파라미터 및 해당 기본값을 검토하고 파일 시스템의 필요에 맞게 수정합니다.

FileSystemId

기본값이 없습니다. 스토리지 용량을 자동으로 늘리려는 파일 시스템의 ID입니다.

LowFreeDataStorageCapacityThreshold

기본값이 없습니다. 경보를 트리거하고 파일 시스템의 스토리지 용량을 자동으로 늘릴 스토리지 용량 사용 임계값을 지정합니다. 이 임계값은 파일 시스템의 현재 스토리지 용량의 백분율(%)로 지정됩니다. 사용된 스토리지가 이 임계값을 초과하면 파일 시스템은 여유 스토리지 용량이 부족한 것으로 간주됩니다.

EmailAddress

기본값이 없습니다. SNS 구독에 사용할 이메일 주소를 지정하고 스토리지 용량 임계값 알림을 받습니다.

PercentIncrease

기본값은 20%입니다. 스토리지 용량을 늘릴 양을 현재 스토리지 용량의 백분율로 표현하여 지정합니다.

> **Note**
>
> 스토리지 스케일링은 CloudWatch 경보가 ALARM 상태에 진입할 때마다 한 번씩 시도됩니다. 스토리지 스케일링 작업을 시도한 후에도 SSD 스토리지 용량 사용률이 임계값을 초과하면 스토리지 스케일링 작업이 다시 시도되지 않습니다.

MaxFSxSizeinGiB

기본값은 196608입니다. SSD 스토리지에 지원되는 최대 스토리지 용량을 지정합니다.

를 사용한 자동 배포 AWS CloudFormation

다음 절차에서는 FSx for ONTAP 파일 시스템의 스토리지 용량을 자동으로 늘리도록 AWS CloudFormation 스택을 구성하고 배포합니다. 배포하는 데에는 몇 분이 걸립니다. CloudFormation 스택 생성에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 콘솔에서 스택 생성을 참조하세요.

> **Note**
>
> 이 솔루션을 구현하면 연결된 AWS 서비스에 대한 요금이 청구됩니다. 자세한 내용은 해당 서비스에 대한 요금 세부 정보 페이지를 참조하세요.

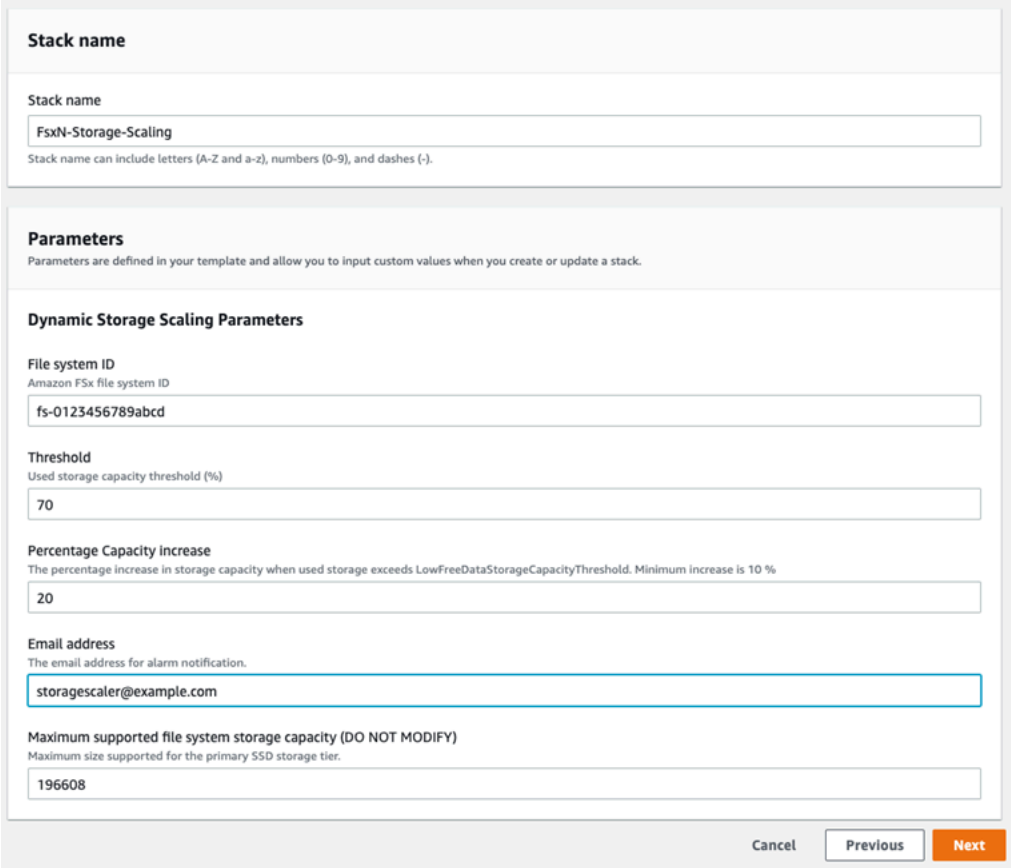
시작하기 전에의 Amazon Virtual Private Cloud(VPC)에서 실행 중인 Amazon FSx 파일 시스템의 ID가 있어야 합니다 AWS 계정. Amazon FSx 리소스 생성에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 시작하기 섹션을 참조하세요.

자동 스토리지 용량 증가 솔루션 스택 시작

1. FSxOntapDynamicStorageScaling AWS CloudFormation 템플릿을 다운로드합니다.

> **Note**
>
> Amazon FSx는 현재 특정 AWS 리전에서만 사용할 수 있습니다. Amazon FSx를 사용할 수 있는 AWS 리전에서이 솔루션을 시작해야 합니다. 자세한 내용은 AWS 일반 참조의 Amazon FSx 엔드포인트 및 할당량을 참조하세요.

2. AWS CloudFormation 콘솔에서 스택 생성 > 새 리소스 사용을 선택합니다.
3. 템플릿이 준비됨을 선택합니다. 템플릿 지정 섹션에서 템플릿 파일 업로드를 선택하고 다운로드한 템플릿을 업로드합니다.
4. 스택 세부 정보 지정에 자동 스토리지 용량 증가 솔루션의 값을 입력합니다.



5. 스택 이름을 입력합니다.
6. 파라미터의 경우 템플릿의 파라미터를 검토하고 파일 시스템의 필요에 맞게 수정합니다. 그런 다음 다음을 선택합니다.

> **Note**
>
> 이 CloudFormation 템플릿으로 스케일링을 시도할 때 이메일 알림을 받으려면 템플릿을 배포한 후 수신한 SNS 구독 이메일을 확인합니다.

7. 사용자 지정 솔루션에 대해 원하는 옵션 설정을 입력하고 다음을 선택합니다.
8. 검토에서 솔루션 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스를 생성한다는 것을 확인하는 확인란을 선택해야 합니다.
9. 생성을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 몇 분 후에 CREATE_COMPLETE 상태를 확인할 수 있습니다.

스택 업데이트

스택이 생성된 후, 동일한 템플릿을 사용하고 파라미터에 새 값을 제공하여 스택을 업데이트할 수 있습니다. 자세한 내용은 AWS CloudFormation 사용 설명서의 직접 스택 업데이트를 참조하세요.

SSD 스토리지 사용률 모니터링

다양한 AWS 및 NetApp 도구를 사용하여 파일 시스템의 SSD 스토리지 용량 사용률을 모니터링할 수 있습니다. Amazon CloudWatch를 사용하면 스토리지 용량 사용률을 모니터링하여 스토리지 용량 사용률이 사용자 지정 가능한 임계값에 도달하면 알림을 보내는 경보를 설정할 수 있습니다.

> **Note**
>
> SSD 스토리지 계층의 스토리지 용량 사용률은 80%를 초과하지 않는 것이 좋습니다. 그러면 계층화가 제대로 작동하고 새 데이터에 대한 오버헤드를 제공합니다. SSD 스토리지 계층의 스토리지 용량 사용률이 지속적으로 80%를 넘으면 SSD 스토리지 계층의 용량을 늘릴 수 있습니다. 자세한 내용은 파일 시스템 SSD 스토리지 및 IOPS 업데이트 단원을 참조하십시오.

Amazon FSx 콘솔에서 파일 시스템의 사용 가능한 SSD 스토리지와 전체 스토리지 분포를 볼 수 있습니다. 사용 가능한 기본 스토리지 용량 그래프는 파일 시스템에서 사용 가능한 SSD 기반 스토리지 용량을 시간 경과에 따라 보여줍니다. 스토리지 분포 그래프는 파일 시스템의 전체 스토리지 용량이 현재 세 가지 범주에 걸쳐 어떻게 분포되어 있는지를 보여줍니다.

- 용량 풀 계층

- SSD 계층 - 사용 가능
- SSD 계층 - 사용됨

다음 절차를 AWS Management Console사용하여에서 파일 시스템의 SSD 스토리지 용량 사용률을 모니터링할 수 있습니다.

파일 시스템 사용 가능한 SSD 계층 스토리지 용량 모니터링하기(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 열에서 파일 시스템을 선택한 다음 스토리지 용량 정보를 보려는 ONTAP 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지가 표시됩니다.
3. 두 번째 패널에서 모니터링 및 성능 탭을 선택한 다음 스토리지를 선택합니다. 사용가능한 기본 스토리지 용량 및 집계 그래프당 스토리지 용량 사용률이 표시됩니다.

스토리지 효율성 절감 모니터링

활성화하면 Amazon FSx 콘솔, Amazon CloudWatch 콘솔 및 ONTAP CLI에서 절감되고 있는 스토리지 용량을 확인할 수 있습니다.

스토리지 효율성 절감액 보기 (콘솔)

FSx for ONTAP 파일 시스템의 Amazon FSx 콘솔에 표시된 스토리지 효율성 절감 효과에는 FlexClones 및 스냅샷으로 인한 절감이 포함됩니다.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 목록에서 스토리지 효율성 절감 효과를 확인할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 파일 시스템 세부 정보 페이지의 두 번째 패널에 있는 모니터링 및 성능 탭에서 요약을 선택합니다.
4. 스토리지 효율성 절감 효과 차트는 절감되고 있는 공간을 논리적 데이터 크기의 백분율 및 물리적 바이트 단위로 보여줍니다.

스토리지 효율성 절감액 보기 (ONTAP CLI)

ONTAP CLI를 사용하여 `storage aggregate show-efficiency` 명령을 실행하면 스냅샷 및 FlexClones의 영향 없이 축소, 압축 및 중복 제거만으로 스토리지 효율성 절감 효과를 확인할 수 있습니다. 자세한 내용은 NetApp ONTAP 설명서 센터에서 스토리지 집계 표시 효율성을 참조하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 이 storage aggregate show-efficiency 명령은 모든 집계의 저장소 효율성에 대한 정보를 표시합니다. 스토리지 효율성은 네 가지 수준으로 표시됩니다.

   - 합계
   - Aggregate
   - Volume
   - 스냅샷 및 FlexClone 볼륨

   ```
   ::*> aggr show-efficiency

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Efficiency Ratio:  3.29:1
   Total Storage Efficiency Ratio:         4.29:1
   Aggregate: aggr2
        Node: node1

   Total Data Reduction Efficiency Ratio:  4.50:1
   Total Storage Efficiency Ratio:         5.49:1

   cluster::*> aggr show-efficiency -details

   Aggregate: aggr1
        Node: node1

   Total Data Reduction Ratio:                    2.39:1
   Total Storage Efficiency Ratio:                4.29:1

   Aggregate level Storage Efficiency
   (Aggregate Deduplication and Data Compaction): 1.00:1
   ```

```
Volume Deduplication Efficiency:                5.03:1
Compression Efficiency:                         1.00:1

Snapshot Volume Storage Efficiency:             8.81:1
FlexClone Volume Storage Efficiency:            1.00:1
Number of Efficiency Disabled Volumes:          1

Aggregate: aggr2
     Node: node1
Total Data Reduction Ratio:                     2.39:1
Total Storage Efficiency Ratio:                 4.29:1

Aggregate level Storage Efficiency
(Aggregate Deduplication and Data Compaction): 1.00:1
Volume Deduplication Efficiency:                5.03:1
Compression Efficiency:                         1.00:1

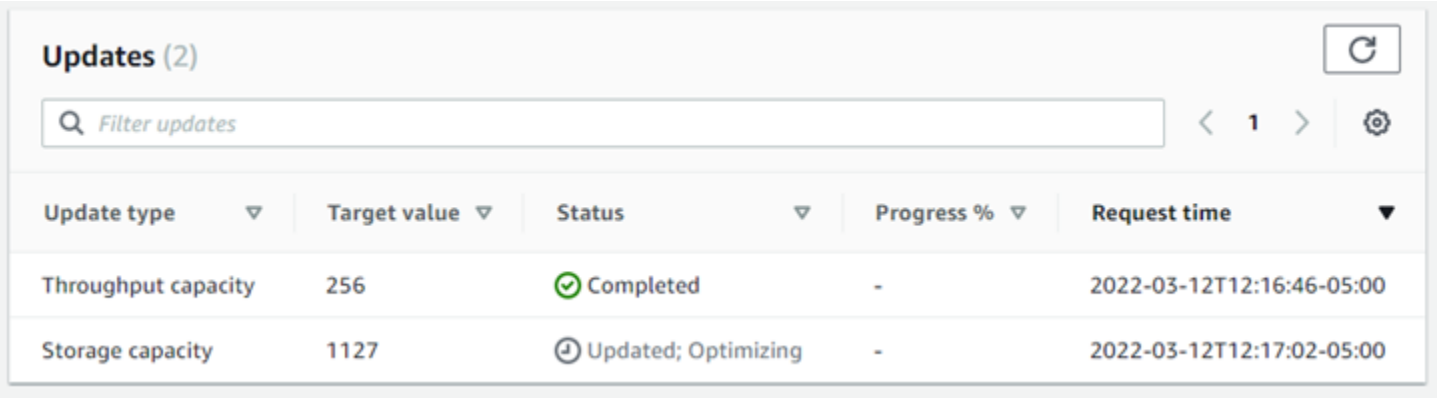
Snapshot Volume Storage Efficiency:             8.81:1
FlexClone Volume Storage Efficiency:            1.00:1
Number of Efficiency Disabled Volumes:          1
```

스토리지 용량 및 IOPS 업데이트 모니터링

Amazon FSx 콘솔, CLI 및 API를 사용하여 SSD 스토리지 용량 및 IOPS 업데이트의 진행 상황을 모니터링할 수 있습니다.

스토리지 및 IOPS 업데이트를 모니터링하려면 (콘솔)

FSx for ONTAP 파일 시스템에 대한 파일 시스템 세부 정보 페이지의 업데이트 탭에서 각 업데이트 유형에 대한 최신 업데이트 10개를 볼 수 있습니다.



SSD 스토리지 용량 및 IOPS 업데이트에서 다음 정보를 볼 수 있습니다.

업데이트 유형

지원되는 유형은 스토리지 용량, 모드, IOPS입니다. 모든 스토리지 용량 및 IOPS 스케일링 요청의 모드 및 IOPS 값이 나열됩니다.

대상 값

파일 시스템의 SSD 스토리지 용량 또는 IOPS를 업데이트하기 위해 지정한 값입니다.

상태

업데이트의 현재 상태입니다. 가능한 값은 다음과 같습니다.

- 보류 중 – Amazon FSx가 업데이트 요청을 받았지만 처리를 시작하지 않았습니다.
- 진행 중 – Amazon FSx에서 업데이트 요청을 처리하고 있습니다.
- 업데이트 후 최적화 중 - Amazon FSx가 파일 시스템의 스토리지 용량을 늘렸습니다. 이제 스토리지 최적화 프로세스가 백그라운드에서 데이터를 재조정하고 있습니다.
- 완료 - 업데이트가 완료되었습니다.
- 실패 - 업데이트 요청이 실패했습니다. 세부 정보를 보려면 물음표(?)를 선택합니다.

진행률(%)

스토리지 최적화 프로세스의 진행률을 완료율로 표시합니다.

요청 시간

Amazon FSx가 업데이트 작업 요청을 받은 시간입니다.

스토리지 및 IOPS 업데이트 모니터링 (CLI)

describe-file-systems AWS CLI 명령과 DescribeFileSystems API 작업을 사용하여 파일 시스템 SSD 스토리지 용량 증가 요청을 보고 모니터링할 수 있습니다. `AdministrativeActions` 배열에 각 관리 작업 유형에 대한 가장 최근의 업데이트 작업 10개가 나열됩니다. 파일 시스템의 스토리지 용량을 늘리면 `FILE_SYSTEM_UPDATE` 및 `STORAGE_OPTIMIZATION`이라는 두 개의 `AdministrativeActions` 작업이 생성됩니다.

다음 예제는 `describe-file-systems` CLI 명령의 응답 발췌문을 보여줍니다. 파일 시스템에는 SSD 스토리지 용량을 2000GiB로 늘리고 프로비저닝된 SSD IOPS를 7000으로 늘리기 위한 관리 작업이 보류 중입니다.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
```

```
        "RequestTime": 1586797629.095,
        "Status": "PENDING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
             }
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "RequestTime": 1586797629.095,
        "Status": "PENDING"
    }
]
```

Amazon FSx는 FILE_SYSTEM_UPDATE 작업을 먼저 처리하여 더 큰 새 스토리지 디스크를 파일 시스템에 추가합니다. 파일 시스템에서 새 스토리지를 사용할 수 있게 되면 FILE_SYSTEM_UPDATE 상태가 UPDATED_OPTIMIZING으로 변경됩니다. 스토리지 용량은 더 큰 새로운 값을 보여주며, Amazon FSx는 STORAGE_OPTIMIZATION 관리 작업을 처리하기 시작합니다. 이 작업은 describe-file-systems CLI 명령의 다음 응답 발췌문에 나와 있습니다.

ProgressPercent 속성은 스토리지 최적화 프로세스의 진행 상황을 표시합니다. 스토리지 최적화 프로세스가 완료되면 FILE_SYSTEM_UPDATE 작업 상태가 COMPLETED로 변경되고 STORAGE_OPTIMIZATION 작업이 더 이상 표시되지 않습니다.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586799169.445,
        "Status": "UPDATED_OPTIMIZING",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
```

```
        }
    },
    {
        "AdministrativeActionType": "STORAGE_OPTIMIZATION",
        "ProgressPercent": 41,
        "RequestTime": 1586799169.445,
        "Status": "IN_PROGRESS"
    }
]
```

스토리지 용량 또는 IOPS 업데이트 요청이 실패하면 다음 예제와 같이 `FILE_SYSTEM_UPDATE` 작업 상태가 `FAILED`로 변경됩니다. `FailureDetails` 속성은 실패에 대한 정보를 제공합니다.

```
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1586373915.697,
        "Status": "FAILED",
        "TargetFileSystemValues": {
            "StorageCapacity": 2000,
            "OntapConfiguration": {
                "DiskIopsConfiguration": {
                    "Mode": "USER_PROVISIONED",
                    "Iops": 7000
                }
            }
        },
        "FailureDetails": {
            "Message": "failure-message"
        }
    }
]
```

볼륨 스토리지 용량

FSx for ONTAP 볼륨은 데이터를 그룹화하고, 데이터 저장 방식을 결정하고, 데이터에 대한 액세스 유형을 결정하는 데 사용하는 가상 리소스입니다. 폴더와 같은 볼륨은 파일 시스템 스토리지 용량 자체를 사용하지 않습니다. 볼륨에 저장된 데이터만 SSD 스토리지를 사용하며, 볼륨의 계층화 정책에 따라 용량 풀 스토리지를 사용합니다. 볼륨을 생성할 때 볼륨 크기를 설정하고 나중에 크기를 변경할 수 있습니다. AWS Management Console AWS CLI 및 API와 ONTAP CLI를 사용하여 FSx for ONTAP 볼륨의 스토리지 용량을 모니터링하고 관리할 수 있습니다.

주제

볼륨 데이터 계층화

Amazon FSx for NetApp ONTAP 파일 시스템에는 기본 스토리지와 용량 풀 스토리지라는 두 개의 스토리지 계층이 있습니다. 기본 스토리지는 데이터 세트의 활성 부분을 위해 특별히 구축되어 프로비저닝된 확장 가능한 고성능 SSD 스토리지입니다. 용량 풀 스토리지는 페타바이트까지 확장할 수 있고 자주 액세스하지 않는 데이터에 맞게 비용을 최적화하는 완전히 탄력적인 스토리지 계층입니다.

각 볼륨의 데이터는 볼륨의 계층화 정책, 냉각 기간 및 임계값 설정에 따라 자동으로 용량 풀 스토리지 계층으로 계층화됩니다. 다음 섹션에서는 ONTAP 볼륨 계층화 정책과 데이터가 용량 풀에 계층화되는 시점을 결정하는 데 사용되는 임계값에 대해 설명합니다.

> **Note**
>
> FSx for ONTAP는 SnapLock 유형에 관계없이 모든 SnapLock 볼륨의 용량 풀에 대한 계층화 데이터를 지원합니다. 자세한 내용은 SnapLock 작동 방법 단원을 참조하십시오.

볼륨 계층화 정책

파일 시스템의 각 볼륨에 대한 계층화 정책을 선택하여 FSx for ONTAP 파일 시스템의 스토리지 계층을 사용하는 방법을 결정합니다. 볼륨을 생성할 때 계층화 정책을 선택하면 Amazon FSx 콘솔, AWS CLI API 또는 NetApp 관리 도구를 사용하여 언제든지 수정할 수 있습니다. 다음 정책 중 하나를 선택하여 용량 풀 스토리지 계층으로 이동할 데이터(있는 경우)를 결정할 수 있습니다.

> **Note**
>
> 계층화를 통해 파일 데이터와 스냅샷 데이터를 용량 풀 계층으로 이동할 수 있습니다. 하지만 파일 메타데이터는 항상 SSD 계층에 남아 있습니다. 자세한 내용은 SSD 스토리지 사용 방식 단원을 참조하십시오.

- 자동 - 이 정책은 모든 콜드 데이터(사용자 데이터 및 스냅샷)를 용량 풀 계층으로 이동합니다. 데이터 휴지율은 정책의 휴지 기간에 따라 결정되고, 이 기간은 기본적으로 31일이며 2~183일 사이의 값으로 구성할 수 있습니다. (일반적인 파일 액세스에서처럼) 기본 콜드 데이터 블록을 무작위로 읽으면 핫 데이터 블록이 되어 기본 스토리지 계층에 기록됩니다. 콜드 데이터 블록을 순차적으로 읽을 때(예: 바이러스 백신 스캔) 콜드 데이터 블록은 콜드 상태로 유지되며 용량 풀 스토리지 계층에 남습니다. 이는 Amazon FSx 콘솔을 사용하여 볼륨을 생성할 때의 기본 정책입니다.
- 스냅샷 전용 - 이 정책은 스냅샷 데이터만 용량 풀 스토리지 계층으로 이동합니다. 스냅샷이 용량 풀 계층으로 이동되는 빈도는 정책의 휴지 기간에 따라 결정되고, 휴지 기간은 기본적으로 2일로 설정되며 2~183일 사이의 값으로 구성할 수 있습니다. 콜드 스냅샷 데이터를 읽으면 핫 스냅샷 데이터가 되어 기본 스토리지 계층에 기록됩니다. 이는 AWS CLI Amazon FSx API 또는 NetApp ONTAP CLI를 사용하여 볼륨을 생성할 때의 기본 정책입니다.
- 모두 - 이 정책은 모든 사용자 데이터와 스냅샷 데이터를 콜드 데이터로 표시하고 용량 풀 계층에 저장합니다. 데이터 블록을 읽어도 콜드 상태로 유지되며 기본 스토리지 계층에 기록되지 않습니다. 모두 계층화 정책이 적용된 볼륨에 데이터가 기록되더라도 처음에는 여전히 SSD 스토리지 계층에 기록되며 백그라운드 프로세스를 통해 용량 풀 계층으로 이동됩니다. 이미 데이터가 포함된 볼륨에 모두 정책이 적용되는 경우 기존 데이터는 SSD에서 용량 풀로 계층화됩니다. 하지만 파일 메타데이터는 항상 SSD 계층에 남아 있습니다.
- 없음 - 이 정책은 볼륨의 모든 데이터를 기본 스토리지 계층에 보관하고 용량 풀 스토리지로 이동하는 것을 방지합니다. 다른 정책을 사용한 후 볼륨을이 정책으로 설정하면 용량 풀 스토리지에 있던 볼륨의 기존 데이터(스냅샷 포함)가 백그라운드 프로세스에 의해 SSD 스토리지로 이동합니다. 이 데이터 마이그레이션은 SSD 사용률이 90% 미만이고 클라우드 검색 정책이 `promote` 또는 로 설정된 경우에만 발생합니다`on-read`. 이 백그라운드 프로세스는 의도적으로 데이터를 읽어 속도를 높일 수 있습니다. 자세한 내용은 클라우드 검색 정책 단원을 참조하십시오.

볼륨의 계층화 정책 설정 또는 수정에 대한 자세한 내용은 등급 정책 업데이트하기 섹션을 참조하세요.

용량 풀 스토리지에 장기간 저장하려는 데이터를 마이그레이션할 때는 볼륨에 자동 계층화 정책을 사용하는 것이 모범 사례입니다. 자동 계층화를 사용하면 데이터가 용량 풀 계층으로 이동하기 전에 최소 2일(볼륨의 냉각 기간 기준) 동안 SSD 스토리지 계층에 데이터가 저장됩니다. ONTAP는 SSD 스토리지 계층에 저장된 데이터에 대해 사후 처리 중복 제거를 주기적으로 실행하며, 볼륨의 데이터 변경 속도에 따라 자동으로 빈도를 조정합니다(속도가 높을수록 사후 처리 중복 제거 작업이 더 자주 트리거됩니다).

기본적으로 프로세스 후 압축은 파일 시스템의 진행 중인 워크로드에 미칠 수 있는 성능 영향으로 인해 ONTAP에서 비활성화됩니다. 포스트 프로세스 압축을 활성화하기 전에 워크로드 성능에 미치는 영향을 평가해야 합니다. 프로세스 후 압축을 활성화하려면 ONTAP CLI에서 진단 권한 수준을 가정하고 다음 명령을 실행합니다.

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-
name -is-enabled true
```

ONTAP는 최소 14일 동안 SSD 스토리지에 보관된 데이터에 대해 프로세스 후 압축을 실행합니다. 짧은 기간 후에 데이터에 액세스할 가능성이 낮은 워크로드의 경우, 후처리 압축 설정을 수정하여 후처리 압축을 더 빨리 실행할 수 있습니다. 예를 들어 5일 동안 액세스하지 않은 데이터에 후처리 압축 절감을 적용하려면 다음 ONTAP CLI 명령을 실행합니다.

```
::> volume efficiency inactive-data-compression modify -vserver svm-name -volume vol-
name -threshold-days 5 -threshold-days-min 2 -threshold-days-max 14
```

명령에 대한 자세한 내용은 볼륨 효율성 비활성-데이터 압축 수정하기를 참조하세요.

SSD 스토리지의 데이터 전송 속도가 더 빠르기 때문에 데이터를 SSD에 보관하면 생성하는 볼륨 백업의 전송 속도를 극대화할 수 있습니다.

계층화 휴지 기간

볼륨의 계층화 휴지 기간은 SSD 계층의 데이터가 콜드 상태로 표시되는 데 걸리는 시간을 설정합니다. 휴지 기간은 `Auto` 및 `Snapshot-only` 계층화 정책에 적용됩니다. 휴지 기간을 2~183일 범위의 값으로 설정할 수 있습니다. 휴지 기간 설정에 대한 자세한 내용은 최소 휴지 일수 업데이트 섹션을 참조하세요.

데이터는 휴지 기간이 만료된 후 24~48시간 후에 계층화됩니다. 계층화는 네트워크 리소스를 사용하는 백그라운드 프로세스이며 클라이언트 측 요청보다 우선 순위가 낮습니다. 클라이언트 측 요청이 진행 중인 경우 계층화 활동이 제한됩니다.

클라우드 검색 정책

볼륨의 클라우드 검색 정책은 용량 풀 계층에서 읽은 데이터를 SSD 계층으로 승격할 수 있는 시기를 지정하는 조건을 설정합니다. 클라우드 검색 정책이 `Default` 이외의 것으로 설정된 경우 이 정책은 볼륨 계층화 정책의 검색 동작보다 우선합니다. 볼륨은 다음 클라우드 검색 정책 중 하나를 포함할 수 있습니다.

- 기본값 - 이 정책은 볼륨의 기본 계층화 정책을 기반으로 계층화된 데이터를 검색합니다. 이는 모든 볼륨에 대한 기본 클라우드 검색 정책입니다.
- 검색 안 함 - 이 정책은 읽기가 순차적인지 무작위인지와 관계없이 계층화된 데이터를 검색하지 않습니다. 이는 볼륨의 계층화 정책을 모두로 설정하는 것과 비슷하지만 자동, 스냅샷 전용 등의 다른 정책과 함께 사용하여 데이터를 즉시 계층화하는 대신 최소 휴지 기간에 따라 데이터를 계층화할 수 있다는 점이 다릅니다.
- 읽는 중 - 이 정책은 모든 클라이언트 기반 데이터 읽기에 대해 계층화된 데이터를 검색합니다. 모두 계층화 정책을 사용할 때는 이 정책이 적용되지 않습니다.
- 승격 - 이 정책은 용량 풀에 있는 모든 볼륨 데이터를 SSD 계층으로 검색할 수 있도록 표시합니다. 데이터는 다음에 일별 백그라운드 계층화 스캐너를 실행할 때 표시됩니다. 이 정책은 자주 실행되지 않는 주기적 워크로드가 있지만 실행 시 SSD 계층 성능이 필요한 애플리케이션에 유용합니다. 모두 계층화 정책을 사용할 때는 이 정책이 적용되지 않습니다.

볼륨의 클라우드 검색 정책 설정에 대한 자세한 내용은 볼륨의 클라우드 검색 정책 업데이트 섹션을 참조하세요.

계층화 임계값

파일 시스템의 SSD 스토리지 용량 사용률에 따라 ONTAP이 모든 볼륨의 계층화 동작을 관리하는 방식이 결정됩니다. 파일 시스템의 SSD 스토리지 용량 사용량을 기반으로 다음 임계값은 설명된 대로 계층화 동작을 설정합니다. 볼륨의 SSD 스토리지 계층의 용량 사용률을 모니터링하는 방법에 대한 자세한 내용은 볼륨 스토리지 용량 모니터링 섹션을 참조하세요.

> **Note**
>
> SSD 스토리지 계층의 스토리지 용량 사용률은 80%를 초과하지 않는 것이 좋습니다. 2세대 파일 시스템의 경우, 이 권장 사항은 파일 시스템의 모든 집계에 대한 총 평균 사용률과 각 개별 집계에 대한 사용률 모두에 적용됩니다. 그러면 계층화가 제대로 작동하고 새 데이터에 대한 오버헤드를 제공합니다. SSD 스토리지 계층의 스토리지 용량 사용률이 지속적으로 80%를 넘

으면 SSD 스토리지 계층의 용량을 늘릴 수 있습니다. 자세한 내용은 파일 시스템 SSD 스토리지 및 IOPS 업데이트 단원을 참조하십시오.

FSx for ONTAP은 다음 스토리지 용량 임계값을 사용하여 볼륨의 계층화를 관리합니다.

- SSD 스토리지 계층 사용률 50% 이하 - 이 임계값에서 SSD 스토리지 계층은 사용률이 낮은 것으로 간주되며 모두 계층화 정책을 사용하는 볼륨만 데이터가 용량 풀 스토리지 계층으로 이동됩니다. 자동 및 스냅샷 전용 정책이 적용된 볼륨은 이 임계값에서 데이터를 계층화하지 않습니다.
- SSD 스토리지 계층 사용률 50% 초과 - 자동 및 스냅샷 전용 계층화 정책이 적용된 볼륨은 계층화 최소 휴지 일수 설정을 기준으로 데이터를 계층화합니다. 기본 설정은 31일입니다.
- SSD 스토리지 계층 사용률 90% 이상 - 이 임계값에서 Amazon FSx는 SSD 스토리지 계층의 공간 보존을 우선시합니다. 자동 및 스냅샷 전용 정책을 사용하여 볼륨을 읽을 때 용량 풀 계층의 콜드 데이터는 더 이상 SSD 스토리지 계층으로 이동되지 않습니다.
- SSD 스토리지 계층 사용률 98% 이상 - SSD 스토리지 계층 사용률이 98% 이상이면 모든 계층화 기능이 중지됩니다. 스토리지 계층에서 계속 읽을 수는 있지만 계층에 기록할 수는 없습니다.

스냅샷 및 볼륨 스토리지 용량

스냅샷은 특정 시점의 Amazon FSx for NetApp ONTAP 볼륨의 읽기 전용 이미지입니다. 스냅샷은 볼륨의 파일을 실수로 삭제하거나 수정하지 못하도록 보호합니다. 스냅샷을 사용하면 사용자가 이전 스냅샷에서 개별 파일 또는 폴더를 쉽게 보고 복원할 수 있습니다.

스냅샷은 파일 시스템의 데이터와 함께 저장되므로 파일 시스템의 스토리지 용량을 사용합니다. 하지만 스냅샷은 마지막 스냅샷 이후 파일의 변경된 부분에 대해서만 스토리지 용량을 사용합니다. 스냅샷은 파일 시스템 볼륨의 백업에 포함되지 않습니다.

스냅샷은 기본 스냅샷 정책을 사용하여 볼륨에서 기본적으로 활성화됩니다. 스냅샷은 볼륨 루트의 `.snapshot` 디렉터리에 저장됩니다. 스냅샷의 볼륨 스토리지 용량을 다음과 같은 방법으로 관리할 수 있습니다.

- 스냅샷 정책 - 내장형 스냅샷 정책을 선택하거나, ONTAP CLI 또는 REST API에서 생성한 사용자 지정 정책을 선택합니다.
- 스냅샷 수동 삭제 - 스냅샷을 수동으로 삭제하여 스토리지 용량을 재확보합니다.
- 스냅샷 자동 삭제 정책 생성 - 기본 스냅샷 정책보다 더 많은 스냅샷을 삭제하는 정책을 생성합니다.
- 자동 스냅샷 끄기 - 자동 스냅샷을 끄면 스토리지 용량을 절약할 수 있습니다.

자세한 내용은 스냅샷으로 데이터 보호 단원을 참조하십시오.

볼륨 파일 용량

Amazon FSx for NetApp ONTAP 볼륨에는 파일 이름, 마지막 액세스 시간, 권한, 크기와 같은 파일 메타데이터를 저장하고 데이터 블록에 대한 포인터 역할을 하는 데 사용되는 파일 포인터가 있습니다. 이러한 파일 포인터를 inode라고 하고, 각 볼륨은 inode 수만큼 유한한 용량을 가지며, 이를 볼륨 파일 용량이라고 합니다. 볼륨이 부족하거나 사용 가능한 파일(inode)을 모두 사용하면 해당 볼륨에 추가 데이터를 기록할 수 없습니다.

볼륨에 포함할 수 있는 파일 시스템 객체(파일, 디렉터리, 스냅샷 복사본)의 수는 볼륨에 있는 inode 수에 따라 결정됩니다. 볼륨의 인노드 수는 볼륨의 스토리지 용량(및 FlexGroup 볼륨의 볼륨 구성 요소 수)에 따라 증가합니다. 기본적으로 스토리지 용량이 648기가바이트 이상인 FlexVol 볼륨(또는 FlexGroup 구성 요소)의 이노드 수는 모두 21,251,126개로 동일합니다. 648GiB보다 큰 볼륨을 생성하고 21,251,126개 이상의 inode를 포함하려는 경우 최대 inode(파일) 수를 수동으로 늘려야 합니다. 볼륨의 최대 파일 수를 보는 방법에 대한 자세한 내용은 볼륨의 파일 용량 모니터링을 참조하세요.

볼륨의 기본 inode 수는 볼륨 스토리지 용량 32KiB당 1개의 inode이며, 볼륨 크기는 최대 648GiB입니다. 1GiB 볼륨의 경우:

Volume_size_in_bytes × (파일 1개 ÷ inode_size_in_bytes) = maximum_number_of_files

1,073,741,824바이트 × (파일 1개 ÷ 32,768바이트) = 32,768개 파일

볼륨에 포함할 수 있는 최대 inode 수를 스토리지 용량 4KiB당 최대 1개의 inode까지 늘릴 수 있습니다. 1GiB 볼륨의 경우 이렇게 하면 최대 inode 또는 파일 수가 32,768개에서 262,144개로 늘어납니다.

1,073,741,824바이트 × (파일 1개 ÷ 4096바이트) = 262,144개 파일

FSx for ONTAP 볼륨에는 최대 20억 개의 inode가 있을 수 있습니다.

볼륨에 저장할 수 있는 최대 파일 수를 변경하는 방법에 대한 자세한 내용은 볼륨의 최대 파일 수 업데이트하기을 참조하세요.

스토리지 효율성 관리

FSx for ONTAP 볼륨에서 스토리지 효율성을 활성화하면 스토리지 사용률을 최적화하고 스토리지 비용을 절감하며 파일 시스템의 성능을 전반적으로 개선할 수 있습니다.

ONTAP는 파일을 4KB(KiB) 데이터 블록으로 구성합니다. 스토리지 효율성은 개별 파일 수준에서가 아닌 데이터 블록 수준에서 발생합니다. 스토리지 효율성이 활성화되면 ONTAP는 중복 데이터를 제거하

고, 데이터 크기를 압축하고, 최적의 디스크 사용을 위해 데이터 레이아웃을 재구성하는 데이터 감소 기술을 조합하여 사용합니다.

스토리지 효율성은 두 가지 방식으로 적용합니다. 데이터 인라인(데이터가 디스크에 기록되기 전, 메모리에 저장)에 적용되어 즉각적인 스토리지 절감 효과를 제공합니다. 또한 주기적인 효율화 작업을 통해 SSD 스토리지 계층의 백그라운드 데이터(데이터가 디스크에 기록된 후)에도 적용되어 시간이 지남에 따라 스토리지 사용률을 최적화합니다. 백그라운드 스토리지의 효율성은 용량 풀에 계층화된 데이터에 대해서는 실행되지 않습니다. 그러나 데이터가 SSD에 있는 동안 저장 공간을 절약한 경우, 데이터가 용량 풀로 계층화될 때 이러한 절약 효과가 보존됩니다.

> **Note**
>
> ONTAP는 데이터 보호(DP) 볼륨에서 스토리지 효율성 활성화를 지원하지 않습니다. 그러나 데이터를 대상 DP 볼륨에 복제하면 소스 RW(읽기-쓰기 가능) 볼륨에서 달성된 스토리지 절감 효과가 유지됩니다.

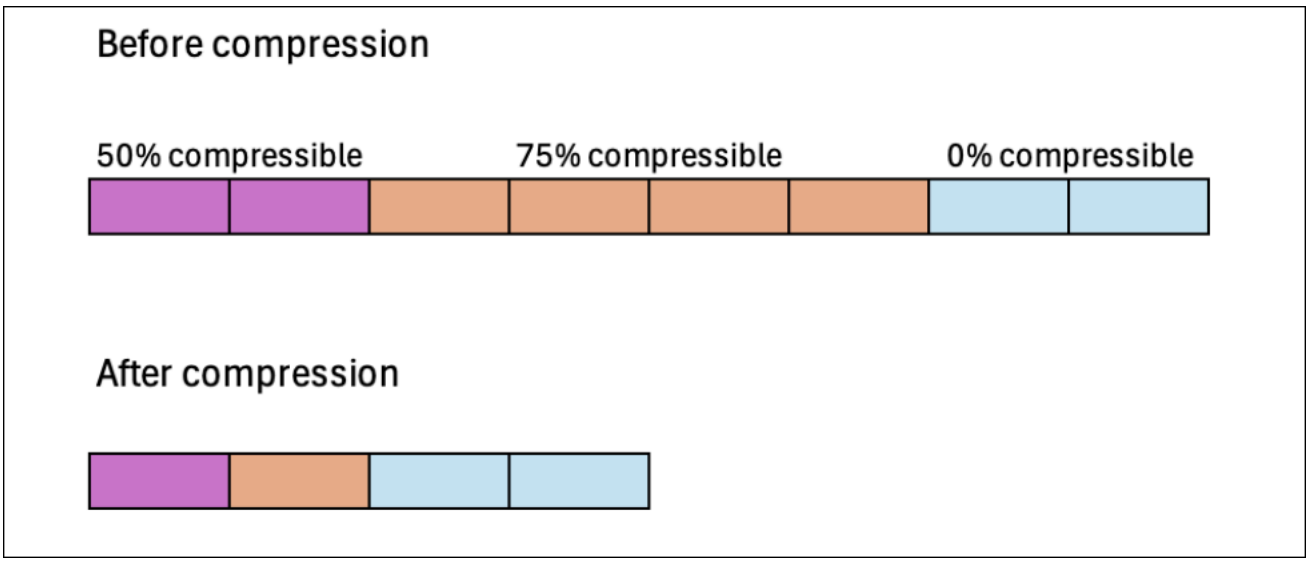
데이터 블록 압축

압축 그룹은 단일 블록으로 함께 관리 및 압축되는 데이터의 논리적 그룹입니다. 는 데이터 블록을 압축 그룹으로 ONTAP는 자동으로 묶어 디스크에서 소비되는 공간을 줄입니다. 성능 및 스토리지 사용률을 최적화하기 위해 ONTAP는 액세스 패턴을 기반으로 데이터에 적용되는 압축 정도를 조정하여 데이터 관리에 대한 균형 잡힌 접근 방식을 제공합니다.

기본적으로 데이터는 볼륨에 데이터를 쓸 때 최적의 성능을 보장하기 위해 8KB 압축 그룹을 사용하여 인라인으로 압축합니다. 선택적으로 볼륨에서 비활성 데이터 압축을 활성화하여 데이터에 더 무거운 압축을 적용하여 SSD에서 데이터를 추가로 압축될 수 있습니다. 비활성 데이터 압축은 콜드 데이터에 32KB 압축 그룹을 사용하여 스토리지를 추가로 절감됩니다. 자세한 내용은 NetApp ONTAP Documentation Center의 `volume efficiency inactive-data-compression modify` 명령을 참조하십시오.

> **Note**
>
> 비활성 데이터 압축은 CPU와 디스크 IOPS를 추가로 소모하며 리소스 집약적인 작업이 될 수 있습니다. 이 기능을 활성화하기 전에 비활성 데이터 압축을 실행하는 것이 워크로드에 미치는 성능 영향을 평가하는 것이 좋습니다.

다음 이미지는 데이터 블록을 압축하여 얻을 수 있는 스토리지 절감 효과를 보여줍니다.



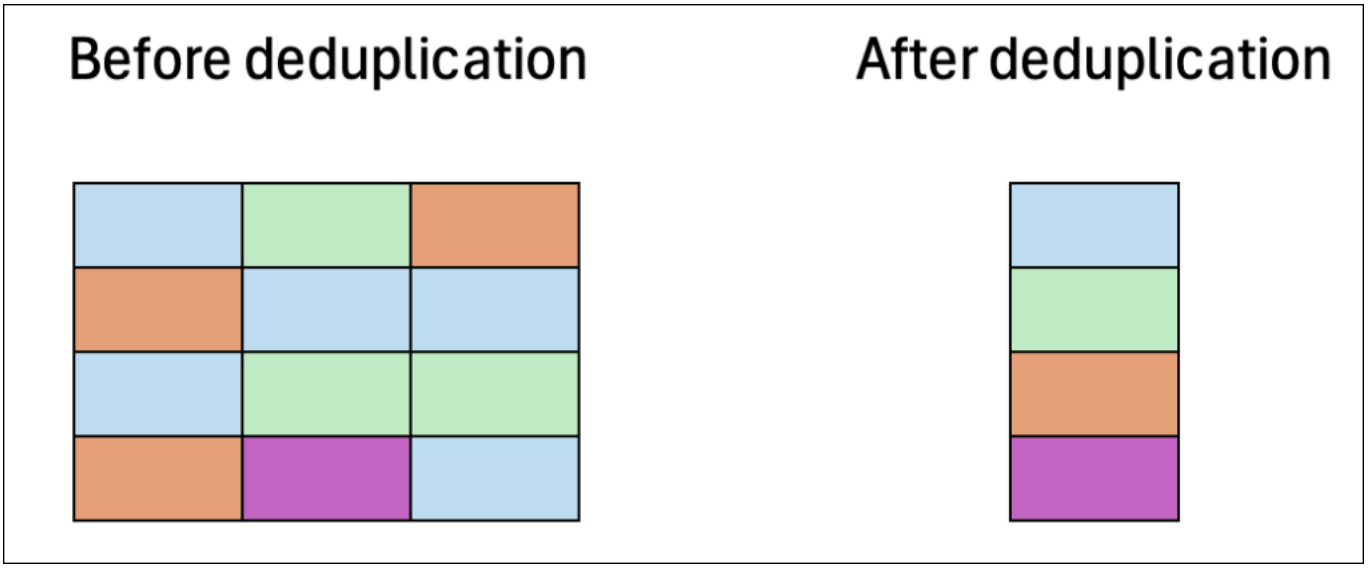
데이터 블록 중복 제거

ONTAP는 중복 데이터 블록을 감지하고 제거하여 데이터의 중복을 줄입니다. 중복된 블록은 공유 고유 블록에 대한 참조로 대체됩니다.

기본적으로 데이터는 디스크에 기록되기 전에 스토리지 공간을 줄이기 위해 인라인으로 중복 제거됩니다. 또한 ONTAP는 지정된 간격으로 백그라운드 중복 제거 스캐너를 실행하여 디스크에 기록된 후 중복 데이터를 식별하고 제거합니다. 이러한 예약된 스캔 중에 ONTAP는 변경 로그를 처리하여 아직 중복 제거되지 않은 마지막 스캔 이후의 새 데이터 블록 또는 수정된 데이터 블록을 식별합니다. 중복이 발견되면 ONTAP는 복제된 블록의 단일 복사본을 가리키도록 메타데이터를 업데이트하고 중복 블록을 회수할 준비가 된 여유 공간으로 표시합니다.

> **Note**
>
> ONTAP는 한 번에 4KB의 입력되는 쓰기에 중복 제거를 적용하므로 크기가 4KB 미만인 쓰기로 워크로드를 실행할 때 중복 제거 비용 절감이 줄어들 수 있습니다.
> FSx for ONTAP는 교차 볼륨 중복 제거를 지원하지 않습니다.

다음 이미지는 중복 제거를 통해 얻을 수 있는 스토리지 절감 효과를 보여줍니다.



데이터 블록 압축

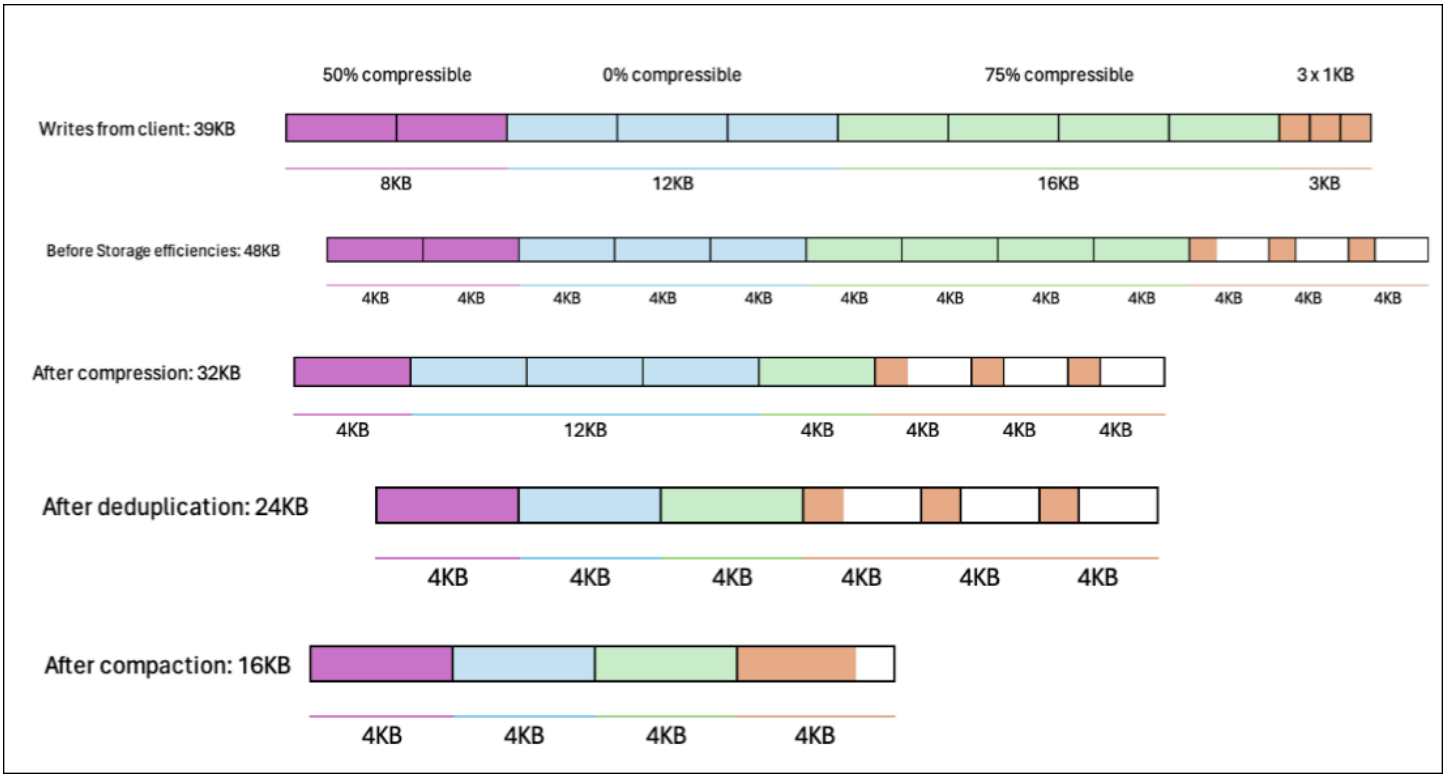
ONTAP는 각각 4KB 미만의 부분적으로 채워진 데이터 블록을 보다 효율적으로 활용되는 4KB 블록으로 통합합니다.

기본적으로 데이터는 인라인으로 압축되어 디스크에 기록될 때 데이터의 레이아웃을 최적화하여 스토리지 오버헤드를 최소화하고 조각화를 줄이며 읽기 성능을 향상시킵니다.

다음 이미지는 압축을 통해 얻을 수 있는 저장 공간 절약 효과를 보여줍니다.

예제: 스토리지 효율성

다음 이미지는 데이터에 스토리지 효율성을 적용하는 방법을 보여줍니다.



자동 크기 조정 사용

볼륨 자동 크기 조정으로 사용 공간 임계값에 도달하면 볼륨이 지정된 크기까지 자동으로 커지도록 합니다. `volume autosize` ONTAP CLI 명령을 사용하여 (FSx for ONTAP의 기본 볼륨 유형인) FlexVol 볼륨 유형에 대해 이 작업을 수행할 수 있습니다.

볼륨 자동 크기 조정 활성화(ONTAP CLI)

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. 표시된 대로 `volume autosize` 명령을 사용하여 다음 값을 바꿉니다.

   - *`svm_name`*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *`vol_name`*을 크기를 조정할 볼륨의 이름으로 바꿉니다.

- *grow_threshold*를 볼륨 크기가 (최대 *max_size* 값까지) 자동으로 증가하는 사용된 공간 백분율 값(예: 90)으로 바꿉니다.
- *max_size*를 볼륨을 늘릴 수 있는 최대 크기로 바꿉니다. *integer*[KB|MB|GB|TB|PB] 형식(예: 300TB)을 사용합니다. 최대 크기는 300TB입니다. 기본값은 볼륨 크기의 120%입니다.
- *min_size*를 볼륨을 축소할 최소 크기로 바꿉니다. *max_size*와 동일한 형식을 사용합니다.
- *shrink_threshold*를 볼륨 크기가 자동으로 축소되는 사용된 공간 백분율로 바꿉니다.

```
::> volume autosize -vserver svm_name -volume vol_name -mode grow_shrink -
grow-threshold-percent grow_threshold -maximum-size max_size -shrink-threshold-
percent shrink_threshold -minimum-size min_size
```

3. 현재 Autosize 설정을 표시하려면 다음 명령을 실행합니다. *svm_name* 및 *vol_name*을 사용자 정보로 바꿉니다.

```
::> volume autosize -vserver svm_name -volume vol_name
```

클라우드 쓰기 모드 활성화

기존 볼륨에 대한 클라우드 쓰기 모드를 활성화 또는 비활성화하려면 `volume modify` ONTAP CLI 명령을 사용합니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume modify` 섹션을 참조하세요.

클라우드 쓰기 모드를 설정하기 위한 전제 조건은 다음과 같습니다.

- 볼륨은 기존 볼륨이야 합니다. 이 기능은 기존 볼륨에서만 활성화할 수 있습니다.
- 볼륨은 읽기-쓰기 (RW) 볼륨이어야 합니다.
- 볼륨에 모든 계층화 정책이 있어야 합니다. 볼륨의 계층화 정책을 수정하는 방법에 대한 자세한 내용은 등급 정책 업데이트하기를 참조하세요.

클라우드 쓰기 모드는 마이그레이션과 같이 NFS 프로토콜을 사용하여 대량의 데이터를 파일 시스템으로 전송하는 경우에 유용합니다.

볼륨의 클라우드 쓰기 모드 설정하기(ONTAP CLI)

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.

2. 다음 명령을 사용하여 ONTAP CLI 고급 모드로 들어갑니다.

   ```
   FSx::> set -privilege advanced
   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 다음 명령을 사용하여 다음 값을 대체하여 볼륨의 클라우드 쓰기 모드를 설정합니다.

   - *svm_name*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *vol_name*를 클라우드 쓰기 모드를 설정할 볼륨의 이름으로 바꿉니다.
   - 볼륨에서 클라우드 쓰기 모드를 활성화하려면 *vol_cw_mode*를 `true`로 바꾸고, 비활성화하려면 `false`로 바꾸세요.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -is-cloud-write-
   enabled vol_cw_mode
   ```

   요청이 성공하면 시스템이 다음과 같이 응답합니다.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

스토리지 용량 업데이트

AWS Management Console AWS CLI 및 API와 ONTAP CLI를 사용하여 볼륨 크기를 수동으로 늘리거나 줄여 볼륨 스토리지 용량을 관리할 수 있습니다. 또한 볼륨 자동 크기 조정을 활성화하여 특정 스토리지 용량 사용 임계값에 도달하면 볼륨 크기가 자동으로 증가하거나 축소되도록 할 수 있습니다. ONTAP CLI를 사용하여 볼륨 자동 크기 조정을 관리합니다.

볼륨의 저장 용량을 변경하려면(콘솔) 다음과 같이 하세요.

- Amazon FSx 콘솔 AWS CLI및 API를 사용하여 볼륨의 스토리지 용량을 늘리거나 줄일 수 있습니다. 자세한 내용은 볼륨 업데이트 단원을 참조하십시오.

ONTAP CLI를 사용하여 `volume modify` 명령을 통해 볼륨의 스토리지 용량을 수정할 수도 있습니다.

볼륨 크기 수정하기 (ONTAP CLI)

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. 볼륨의 스토리지 용량을 수정하려면 volume modify ONTAP CLI 명령을 사용합니다. 다음 값 대신 데이터를 사용하여 다음 명령을 실행합니다:

   - *`svm_name`*을 볼륨이 생성되는 스토리지 가상 머신(SVM)의 이름으로 바꿉니다.
   - *`vol_name`*을 크기를 조정할 볼륨의 이름으로 바꿉니다.
   - *`vol_size`*를 *`integer`*`[KB|MB|GB|TB|PB]` 형식의 새 볼륨 크기로 바꿉니다(예: 볼륨 크기를 100GB로 늘리려면 `100GB`).

   ```
   ::> volume modify -vserver svm_name -volume vol_name -size vol_size
   ```

등급 정책 업데이트하기

AWS Management Console AWS CLI 및 API와 ONTAP CLI를 사용하여 볼륨의 계층화 정책을 수정할 수 있습니다.

볼륨의 데이터 계층화 정책 수정(콘솔)

다음 절차에 따라 AWS Management Console을 사용하여 볼륨의 데이터 계층화 정책을 수정합니다.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.

2. 왼쪽 탐색 창에서 볼륨을 선택한 다음 데이터 계층화 정책을 수정할 ONTAP 볼륨을 선택합니다.
3. 작업 드롭다운 메뉴에서 볼륨 업데이트를 선택합니다. 볼륨 업데이트 창이 표시됩니다.
4. 용량 풀 계층화 정책에서 볼륨의 새 정책을 선택합니다. 자세한 내용은 볼륨 계층화 정책 단원을 참조하십시오.
5. 업데이트를 선택하여 새 정책을 볼륨에 적용합니다.

볼륨의 계층화 정책(CLI)을 설정하려면 다음과 같이 하세요.

- update-volume CLI 명령을 사용하여 볼륨의 계층화 정책을 수정합니다(UpdateVolume은 동일한 Amazon FSx API 작업입니다). 다음 CLI 명령 예제는 볼륨의 데이터 계층화 정책을 SNAPSHOT_ONLY로 설정합니다.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
```

요청이 성공한 경우 시스템은 볼륨 설명으로 응답합니다.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 2,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
```

```
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

볼륨의 데이터 계층화 정책 수정(ONTAP CLI)

`volume modify` ONTAP CLI 명령을 사용하여 볼륨의 계층화 정책을 설정합니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume modify` 섹션을 참조하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.

2. 다음 명령을 사용하여 ONTAP CLI 고급 모드로 들어갑니다.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 다음 명령을 사용하여 볼륨 데이터 계층화 정책을 수정하고 다음 값을 바꿉니다.

   - *`svm_name`*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *`vol_name`*을 데이터 계층화 정책을 설정할 볼륨의 이름으로 바꿉니다.
   - *`tiering_policy`*를 원하는 정책으로 바꿉니다. 유효한 값은 `snapshot-only`, `auto`, `all` 또는 none입니다. 자세한 내용은 볼륨 계층화 정책 단원을 참조하십시오.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-
   policy tiering_policy
   ```

최소 휴지 일수 업데이트

볼륨의 최소 휴지 일수는 웜 데이터와 콜드 데이터를 결정하는 데 사용되는 임계값을 설정합니다. AWS CLI 및 API와 ONTAP CLI를 사용하여 볼륨의 최소 냉각 일수를 설정할 수 있습니다.

볼륨의 최소 휴지 일수 설정(CLI)

- update-volume CLI 명령(Amazon FSx API의 UpdateVolume 작업과 동일함)을 사용하여 볼륨 구성을 수정합니다. 다음 CLI 명령 예제에서는 볼륨의 `CoolingPeriod`를 104일로 설정합니다.

```
aws fsx update-volume \
    --volume-id fsxvol-abcde0123456789f
    --ontap-configuration TieringPolicy={Name=SNAPSHOT_ONLY}
aws fsx update-volume --volume-id fsvol-006530558c14224ac --ontap-configuration
 TieringPolicy={CoolingPeriod=104}
```

요청이 성공한 경우 시스템은 볼륨 설명으로 응답합니다.

```
{
    "Volume": {
        "CreationTime": "2021-10-05T14:27:44.332000-04:00",
        "FileSystemId": "fs-abcde0123456789f",
        "Lifecycle": "CREATED",
        "Name": "vol1",
        "OntapConfiguration": {
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "UNIX",
            "SizeInMegabytes": 1048576,
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abc0123de456789f",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "CoolingPeriod": 104,
                "Name": "SNAPSHOT_ONLY"
            },
            "UUID": "aaaa1111-bb22-cc33-dd44-abcde01234f5",
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcde0123456789f/fsvol-abc012def3456789a",
```

```
        "VolumeId": "fsvol-abc012def3456789a",
        "VolumeType": "ONTAP"
    }
}
```

볼륨의 최소 휴지 일수 설정(ONTAP CLI)

`volume modify` ONTAP CLI 명령을 사용하여 기존 볼륨의 최소 휴지 일수를 설정합니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume modify` 섹션을 참조하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.
2. 다음 명령을 사용하여 ONTAP CLI 고급 모드로 들어갑니다.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```
3. 다음 명령을 사용하여 볼륨의 계층화 최소 휴지 일수를 변경하고 다음 값을 바꿉니다.

   - *`svm_name`*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *`vol_name`*을 휴지 일수를 설정할 볼륨의 이름으로 바꿉니다.
   - *`cooling_days`*를 원하는 값(2~183 사이의 정수)으로 바꿉니다.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -tiering-minimum-cooling-
   days cooling_days
   ```

   요청이 성공하면 시스템이 다음과 같이 응답합니다.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

볼륨의 클라우드 검색 정책 업데이트

`volume modify` ONTAP CLI 명령을 사용하여 기존 볼륨에 대한 클라우드 검색 정책을 설정합니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume modify` 섹션을 참조하세요.

볼륨의 클라우드 검색 정책 설정(ONTAP CLI)

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.

2. 다음 명령을 사용하여 ONTAP CLI 고급 모드로 들어갑니다.

   ```
   FSx::> set adv

   Warning: These advanced commands are potentially dangerous; use them only when
        directed to do so by NetApp personnel.
   Do you want to continue? {y|n}: y
   ```

3. 다음 명령을 사용하여 볼륨의 클라우드 검색 정책을 설정하고 다음 값을 바꿉니다.

   - *svm_name*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *vol_name*을 클라우드 검색 정책을 설정할 볼륨의 이름으로 바꿉니다.
   - *retrieval_policy*를 원하는 값(`default`, `on-read`, `never`, `promote`)으로 바꿉니다.

   ```
   FSx::> volume modify -vserver svm_name -volume vol_name -cloud-retrieval-
   policy retrieval_policy
   ```

   요청이 성공하면 시스템이 다음과 같이 응답합니다.

   ```
   Volume modify successful on volume vol_name of Vserver svm_name.
   ```

볼륨의 최대 파일 수 업데이트하기

사용 가능한 inode 또는 파일 포인터 수가 모두 소모되면 FSx for ONTAP 볼륨의 파일 용량이 부족해질 수 있습니다.

볼륨의 최대 파일 수를 늘리려면(ONTAP CLI) 다음과 같이 하세요.

`volume modify` ONTAP CLI 명령을 사용하여 볼륨의 최대 파일 수를 늘릴 수 있습니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume modify`를 참조하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 사용 사례에 따라 다음 중 하나를 수행합니다. *svm_name* 및 *vol_name*을 사용자의 값으로 바꿉니다.

   - 항상 최대 파일(inode) 수를 사용할 수 있도록 볼륨을 구성하려면 다음을 수행합니다.

     1. 다음 명령을 사용하여 ONTAP CLI의 고급 모드로 들어갑니다.

        ```
        ::> set adv
        ```

     2. 이 명령을 실행하면 다음과 같은 출력이 표시됩니다. 계속하려면 y를 입력합니다.

        ```
        Warning: These advanced commands are potentially dangerous; use them only
         when
        directed to do so by NetApp personnel.
        Do you want to continue? {y|n}: y
        ```

     3. 항상 볼륨에 있는 최대 파일 수를 사용하려면 다음 명령을 입력합니다.

        ```
        ::> volume modify -vserver svm_name -volume vol_name -files-set-maximum true
        ```

   - *max_number_files* = (current_size_of_volume) × (1 file ÷ 4 KiB)를 사용해 볼륨에 허용된 총 파일 수(최대 20억 개)를 수동으로 지정하려면 다음 명령을 사용합니다.

```
::> volume modify -vserver svm_name -volume vol_name -files max_number_files
```

볼륨 스토리지 용량 모니터링

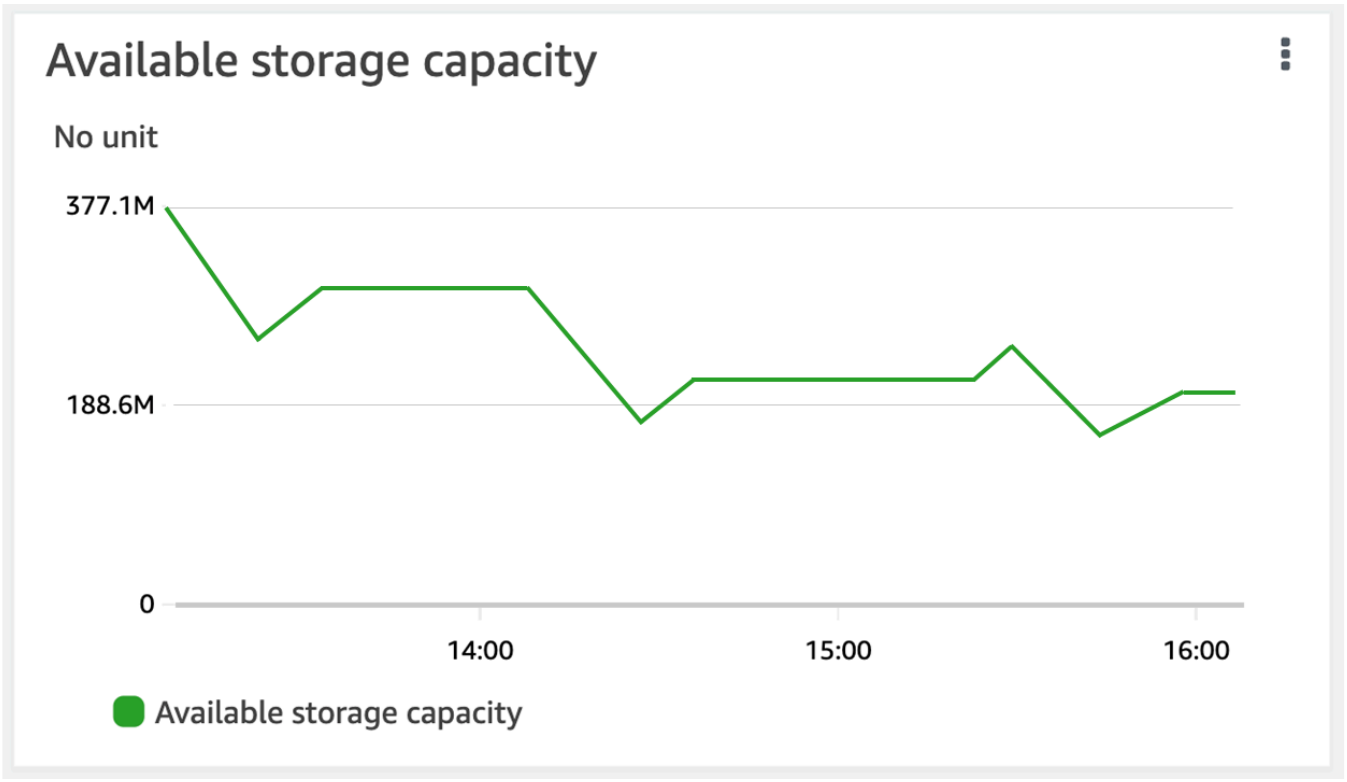
볼륨의 사용 가능한 스토리지와의 스토리지 배포 AWS Management Console AWS CLI및 NetApp ONTAP CLI를 볼 수 있습니다.

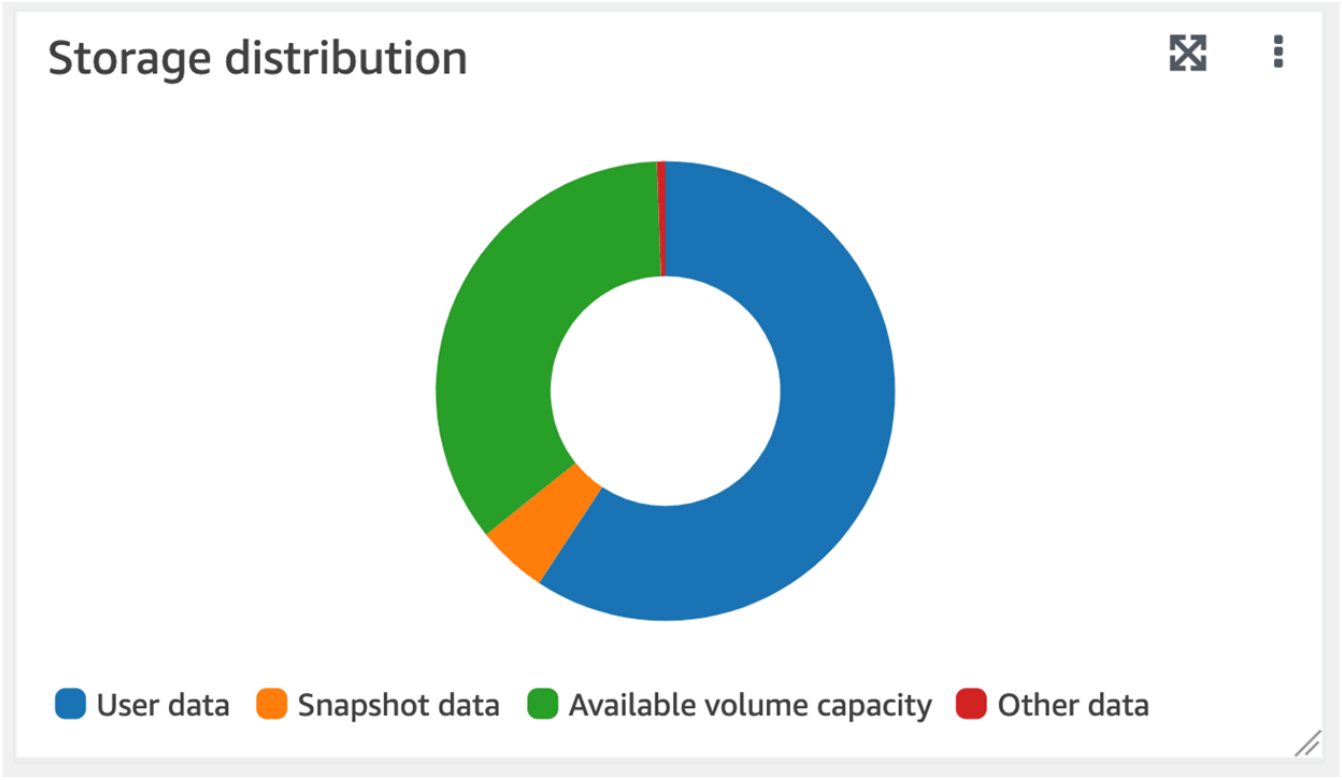
볼륨의 저장 용량을 모니터링하려면 (콘솔) 다음과 같이 하세요.

사용 가능한 스토리지 그래프는 볼륨의 여유 스토리지 용량을 시간 경과에 따라 보여줍니다. 스토리지 분포 그래프는 볼륨의 스토리지 용량이 현재 4가지 범주에 걸쳐 어떻게 분포되어 있는지를 보여줍니다.

- 사용자 데이터
- 스냅샷 데이터
- 사용 가능한 볼륨 용량
- 기타 데이터

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 열에서 볼륨을 선택한 다음 스토리지 용량 정보를 보려는 ONTAP 볼륨을 선택합니다. 볼륨 세부 정보 페이지가 표시됩니다.
3. 두 번째 패널에서 모니터링 탭을 선택합니다. 사용 가능한 스토리지 및 스토리지 분포 그래프가 여러 다른 그래프와 함께 표시됩니다.


Available storage capacity
No unit
377.1M
188.6M
0
14:00
15:00
16:00
Available storage capacity


Storage distribution
User data
Snapshot data
Available volume capacity
Other data

볼륨의 스토리지 용량 모니터링하기 (ONTAP CLI)

`volume show-space` ONTAP CLI 명령을 사용하여 볼륨의 저장 용량이 어떻게 사용되고 있는지 모니터링할 수 있습니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 `volume show-space`를 참조하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 다음 명령을 실행하여 볼륨의 스토리지 용량 사용량을 확인하고 다음 값을 바꿉니다.

   - *`svm_name`*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
   - *`vol_name`*을 데이터 계층화 정책을 설정할 볼륨의 이름으로 바꿉니다.

   ```
   ::> volume show-space -vserver svm_name -volume vol_name
   ```

   이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다.

   ```
   Vserver : svm_name
   Volume  : vol_name
   Feature                                     Used      Used%
   --------------------------------     ----------     ------
   User Data                                  140KB         0%
   Filesystem Metadata                      164.4MB         1%
   Inodes                                   10.28MB         0%
   Snapshot Reserve                         563.2MB         5%
   Deduplication                               12KB         0%
   Snapshot Spill                            9.31GB        85%
   Performance Metadata                       668KB         0%

   Total Used                               10.03GB        91%

   Total Physical Used                      10.03GB        91%
   ```

이 명령의 출력에는 다양한 유형의 데이터가 이 볼륨에서 차지하는 물리적 공간의 양이 표시됩니다. 또한 각 데이터 유형이 사용하는 총 볼륨 용량의 백분율도 표시됩니다. 이 예시에서는 `Snapshot Spill` 및 `Snapshot Reserve`가 볼륨 용량의 총 90%를 사용합니다.

`Snapshot Reserve`는 스냅샷 복사본을 저장하기 위해 예약된 디스크 공간의 양을 보여줍니다. 스냅샷 복사본 스토리지가 예약 공간을 초과하면 파일 시스템으로 침범되며 이 양은 `Snapshot Spill` 아래에 나와 있습니다.

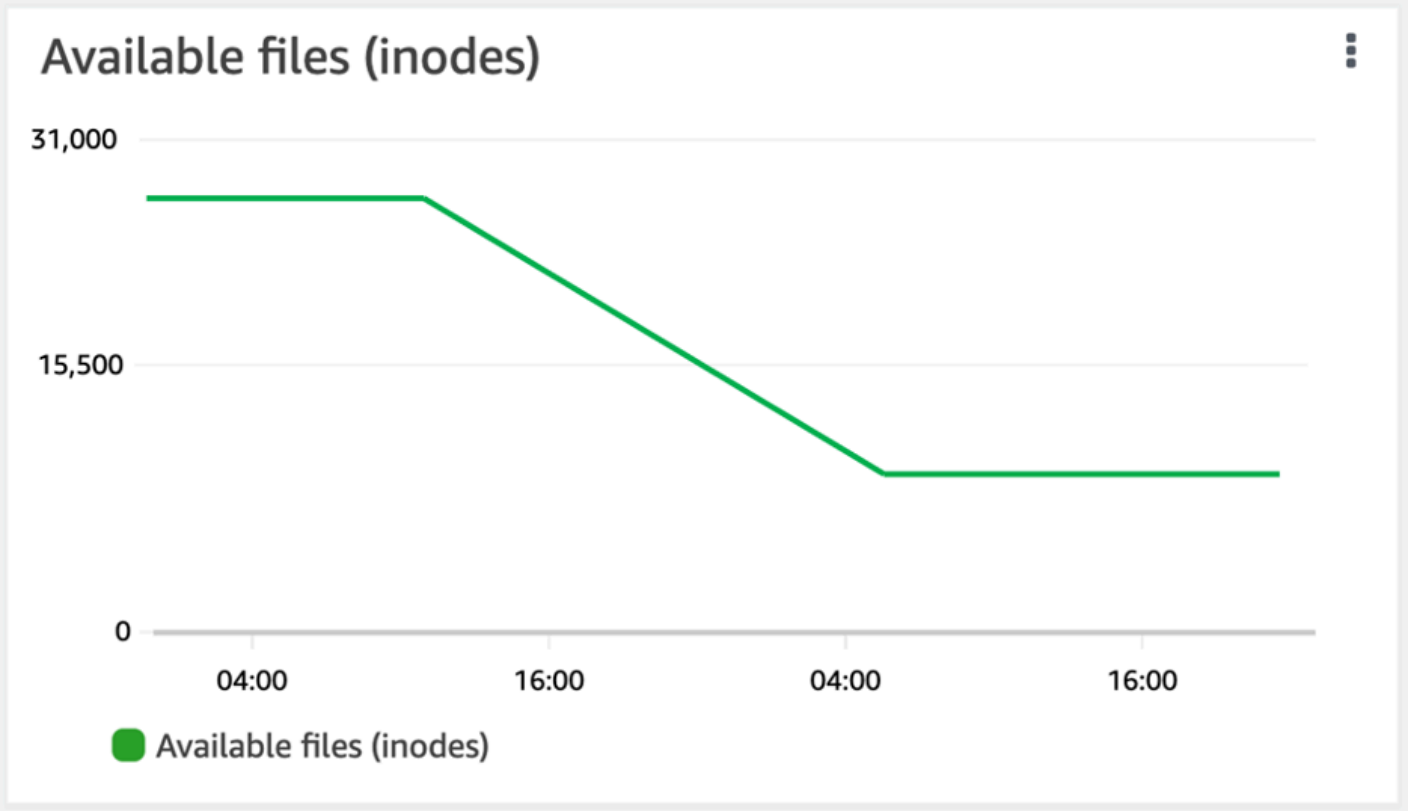
사용 가능한 공간의 양을 늘리려면 다음 절차와 같이 볼륨 크기를 늘리거나 사용하지 않는 스냅샷을 삭제하면 됩니다.

FlexVol 볼륨 유형(FSx for ONTAP 볼륨의 기본 볼륨 유형)의 경우 볼륨 자동 크기 조정을 활성화할 수도 있습니다. 자동 크기 조정을 활성화하면 특정 임계값에 도달하는 경우 볼륨 크기가 자동으로 증가합니다. 자동 스냅샷을 비활성화할 수도 있습니다. 이 두 기능 모두 다음 섹션에 설명되어 있습니다.

볼륨의 파일 용량 모니터링

다음 방법 중 하나를 사용하여 허용되는 최대 파일 수 및 볼륨에서 이미 사용된 파일 수를 볼 수 있습니다.

- CloudWatch 볼륨 지표 `FilesCapacity` 및 `FilesUsed`.
- Amazon FSx 콘솔에서, 볼륨의 모니터링 탭에서 사용 가능한 파일(inode) 차트로 이동합니다. 다음 이미지는 시간이 지남에 따라 감소하는 볼륨의 사용 가능한 파일(inode)을 보여줍니다.



FSx for ONTAP 파일 시스템 관리

파일 시스템은 온프레미스 ONTAP 클러스터와 유사한 기본 Amazon FSx 리소스입니다. 파일 시스템의 솔리드 스테이트 드라이브(SSD) 스토리지 용량 및 처리량 용량을 지정하고 파일 시스템을 생성할 Virtual Private Cloud(VPC)를 선택합니다. 각 파일 시스템에는 관리 엔드포인트가 있으며, 이 엔드포인트를 사용하여 ONTAP CLI 또는 REST API로 리소스 및 데이터를 관리할 수 있습니다.

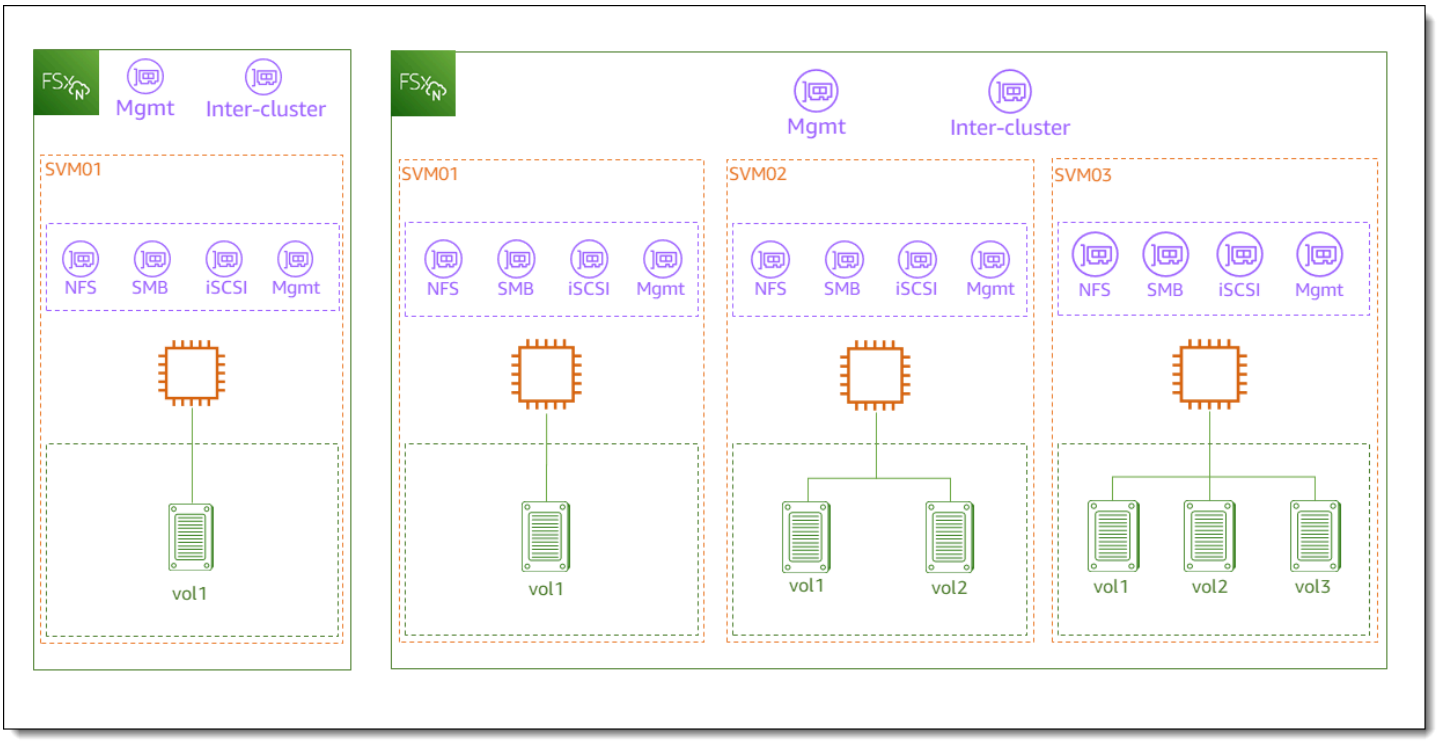
파일 시스템 리소스

Amazon FSx for NetApp ONTAP 파일 시스템은 다음과 같은 기본 리소스로 구성되어 있습니다.

- 파일 시스템 자체의 물리적 하드웨어(파일 서버 및 스토리지 미디어 포함).
- 스토리지 가상 머신(SVM)을 호스팅하는 하나 이상의 고가용성(HA) 파일 서버 쌍입니다. 1세대 파일 시스템과 Multi-AZ 2세대 파일 시스템에는 HA 페어가 하나 있고 2세대 Single-AZ 파일 시스템에는 최대 12개의 HA 페어가 있습니다. 각 HA 페어에는 집계라는 스토리지 풀이 있습니다. 모든 HA 페어의 집계 모음은 SSD 스토리지 계층을 구성합니다.
- 파일 시스템 볼륨을 호스팅하고 자체 자격 증명 및 액세스 관리 기능을 갖춘 하나 이상의 SVM.

- 데이터를 가상으로 구성하고 클라이언트가 마운트하는 하나 이상의 볼륨.

다음 이미지는 하나의 HA 쌍이 있는 1세대 FSx for ONTAP 파일 시스템의 아키텍처와 기본 리소스 간의 관계를 보여줍니다. 왼쪽의 FSx for ONTAP 파일 시스템은 하나의 SVM 및 하나의 볼륨으로 구성된 가장 단순한 파일 시스템입니다. 오른쪽의 파일 시스템에는 여러 SVM이 있으며 일부 SVM에는 여러 볼륨이 있습니다. 파일 시스템과 SVM에는 각각 여러 관리 엔드포인트가 있으며, SVM에는 데이터 액세스 엔드포인트도 있습니다.



FSx for ONTAP 파일 시스템을 생성할 때는 다음 속성을 정의합니다.

- 배포 유형 - 파일 시스템의 배포 유형(Multi-AZ 또는 Single-AZ). Single-AZ 파일 시스템은 데이터를 복제하고 단일 가용 영역 내에서 자동 장애 조치를 제공합니다. 1세대 Single-AZ 파일 시스템은 HA 페어 하나를 지원합니다. 2세대 Single-AZ 파일 시스템은 최대 12개의 HA 페어를 지원합니다. Multi-AZ 파일 시스템은 데이터를 복제하고 동일한 AWS 리전내 여러 가용 영역에 걸쳐 장애 조치를 지원하여 복원력을 강화합니다. 1세대 및 2세대 Multi-AZ 파일 시스템 모두 하나의 HA 페어를 지원합니다.

> **Note**
>
> 생성 후에는 파일 시스템의 배포 유형을 변경할 수 없습니다. 배포 유형을 변경하려면(예: Single-AZ 1에서 Single-AZ 2로 이동) 데이터를 백업하고 새 파일 시스템에서 복원할 수 있

습니다. NetApp SnapMirror, AWS DataSync또는 타사 데이터 복사 도구를 사용하여 데이터를 마이그레이션할 수도 있습니다. 자세한 내용은 NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션 및 AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션 섹션을 참조하세요.

- 스토리지 용량 - 1세대 파일 시스템의 경우 최대 192테비바이트(TiB), 2세대 Multi-AZ 파일 시스템의 경우 512TiB, 2세대 Single-AZ 파일 시스템의 경우 1페비바이트(PiB)의 SSD 스토리지 용량입니다.
- SSD IOPS - 기본적으로 각 기가바이트의 SSD 스토리지에는 3개의 SSD IOPS(파일 시스템 구성에서 지원하는 최대 개수까지)가 포함됩니다. 필요에 따라 SSD IOPS를 추가로 프로비저닝할 수도 있습니다.
- 처리량 용량 - 파일 서버가 데이터를 제공할 수 있는 지속 속도입니다.
- 네트워킹 - 파일 시스템이 생성하는 관리 및 데이터 액세스 엔드포인트의 VPC와 서브넷입니다. Multi-AZ 파일 시스템의 경우 IP 주소 범위와 라우팅 테이블도 정의합니다.
- 암호화 - 저장된 파일 시스템 데이터를 암호화하는 데 사용되는 AWS Key Management Service (AWS KMS) 키입니다.
- 관리 액세스 - `fsxadmin` 사용자의 암호를 지정할 수 있습니다. 이 사용자는 NetApp ONTAP CLI 및 REST API를 사용하여 파일 시스템을 관리할 수 있습니다.

NetApp ONTAP CLI 또는 REST API를 사용하여 FSx for ONTAP 파일 시스템을 관리할 수 있습니다. 또한 Amazon FSx 파일 시스템과 다른 ONTAP 배포(다른 Amazon FSx 파일 시스템 포함) 간에 SnapMirror 또는 SnapVault 관계를 설정할 수 있습니다. 각 FSx for ONTAP 파일 시스템에는 NetApp 애플리케이션에 대한 액세스를 제공하는 다음과 같은 파일 시스템 엔드포인트가 있습니다.

- 관리(Management) - Secure Shell(SSH)을 통해 NetApp ONTAP CLI에 액세스하거나 파일 시스템에 NetApp ONTAP REST API를 사용하려면 이 엔드포인트를 사용합니다.
- 인터클러스터(Intercluster) - NetApp SnapMirror를 사용하여 복제를 설정하거나 NetApp FlexCache를 사용하여 캐싱을 설정할 때 이 엔드포인트를 사용합니다.

자세한 내용은 NetApp 애플리케이션을 사용하여 FSx for ONTAP 관리 및 를 사용하여 데이터 복제 NetApp SnapMirror 섹션을 참조하세요.

파일 시스템 만들기

이 섹션에서는 Amazon FSx 콘솔 AWS CLI또는 Amazon FSx FSx API를 사용하여 FSx for ONTAP 파일 시스템을 생성하는 방법을 설명합니다. 소유한 Virtual Private Cloud(VPC) 또는 다른가 공유 AWS

계정 한 VPC에서 파일 시스템을 생성할 수 있습니다. 참가자인 VPC에서 Multi-AZ 파일 시스템을 생성할 때 고려해야 할 사항이 있습니다. 이러한 고려 사항은 이 주제에서 설명합니다.

기본적으로 Amazon FSx 콘솔에서 새 파일 시스템을 생성하면 Amazon FSx는 단일 스토리지 가상 머신(SVM)과 하나의 볼륨으로 파일 시스템을 자동으로 생성하여 NFS(네트워크 파일 시스템) 프로토콜을 통해 Linux 인스턴스의 데이터에 빠르게 액세스할 수 있습니다. 파일 시스템을 생성할 때 선택적으로 SVM을 Active Directory에 조인하면 Windows 및 MacOS 클라이언트에서 서버 메시지 블록(SMB) 프로토콜을 통해 액세스할 수 있습니다. 파일 시스템을 생성한 후 필요에 따라 추가 SVM 및 볼륨을 생성할 수 있습니다.

파일 시스템 생성(콘솔)

이 절차에서는 표준 생성 옵션을 사용하여 필요에 맞게 사용자 지정하는 구성으로 FSx for ONTAP을 생성합니다. 빠른 생성 옵션을 사용하여 기본 구성 파라미터 세트를 통해 파일 시스템을 빠르게 생성하는 방법에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 파일 시스템 생성 섹션을 참조하세요.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 대시보드에서 파일 시스템 생성을 선택합니다.
3. 파일 시스템 유형 선택 페이지의 파일 시스템 옵션에서 Amazon FSx for NetApp ONTAP를 선택한 후 다음을 선택합니다.
4. 생성 방법 섹션에서 표준 생성을 선택합니다.
5. 파일 시스템 세부 정보 섹션에서 다음 정보를 입력합니다.

   - 파일 시스템 이름 - 선택 사항에 파일 시스템의 이름을 입력합니다. 파일 시스템의 이름을 지정하면 파일 시스템을 보다 쉽게 찾고 관리할 수 있습니다. 최대 256개의 유니코드 문자, 공백 및 숫자와 특수 문자 + - = . _ : /를 사용할 수 있습니다.
   - 배포 유형에서 Multi-AZ 2, Single-AZ 2, Multi-AZ 1 또는 Single-AZ 1을 선택합니다.
     - Multi-AZ 파일 시스템은 데이터를 복제하고 동일한 AWS 리전내 여러 가용 영역에 걸쳐 장애 조치를 지원합니다. Multi-AZ 1은 1세대 FSx for ONTAP 파일 시스템입니다. Multi-AZ 2는 2세대 파일 시스템입니다. 둘 다 고가용성(HA) 페어 하나를 지원합니다.
     - Single-AZ 파일 시스템은 데이터를 복제하고 단일 가용 영역 내에서 자동 장애 조치를 제공합니다. Single-AZ 1은 HA 페어 하나를 지원하는 1세대 FSx for ONTAP 파일 시스템입니다. Single-AZ 2는 최대 12개의 HA 페어를 지원하는 2세대 파일 시스템입니다. 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

     배포 유형에 대한 자세한 내용은 가용성, 내구성 및 배포 옵션 섹션을 참조하세요.

> **Note**
>
> 생성 후에는 파일 시스템의 배포 유형을 변경할 수 없습니다. 배포 유형을 변경하려면(예: Single-AZ 1에서 Single-AZ 2로 이동) 데이터를 백업하고 새 파일 시스템에서 복원할 수 있습니다. NetApp SnapMirror, AWS DataSync또는 타사 데이터 복사 도구를 사용하여 데이터를 마이그레이션할 수도 있습니다. 자세한 내용은 NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션 및 AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션 섹션을 참조하세요.

- SSD 스토리지 용량에는 파일 시스템의 스토리지 용량을 기비바이트(GiB) 단위로 입력합니다. 1,024~1,048,576GiB(최대 1페비바이트[PiB]) 범위의 정수를 입력합니다.

  파일 시스템을 생성한 후 언제든지 필요에 따라 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 단원을 참조하십시오.

- 프로비저닝된 SSD IOPS의 경우 파일 시스템의 IOPS 수를 프로비저닝하는 두 가지 옵션이 있습니다.
  - Amazon FSx가 SSD 스토리지의 GiB당 3 IOPS를 자동으로 프로비저닝하도록 하려면 자동(기본값)을 선택합니다.
  - IOPS 수를 지정하려면 사용자 프로비저닝을 선택합니다. 파일 시스템당 최대 200,000 SSD IOPS를 프로비저닝할 수 있습니다.

  > **Note**
  >
  > 파일 시스템을 생성한 후 프로비저닝된 SSD IOPS를 늘릴 수 있습니다. 파일 시스템이 달성할 수 있는 최대 SSD IOPS 수준은 추가 SSD IOPS를 프로비저닝하는 경우에도 파일 시스템의 처리량 용량에 따라 결정된다는 점을 기억하세요. 자세한 내용은 처리량 용량이 성능에 미치는 영향 및 스토리지 용량 관리 섹션을 참조하세요.

- 처리량 용량의 경우 처리량 용량을 초당 메가바이트(MBps) 단위로 결정하는 두 가지 옵션이 있습니다.
  - Amazon FSx가 선택한 스토리지 용량 양에 따라 처리량 용량을 자동으로 선택하도록 하려면 권장 처리량 용량을 선택합니다.
  - 처리량 용량 양을 지정하려면 처리량 용량 지정을 선택합니다. 이 옵션을 선택하면 처리량 용량 드롭다운이 나타나고 선택한 배포 유형에 따라 채워집니다. HA 페어 수(최대 12개)를 선택할 수도 있습니다. 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

처리량 용량은 파일 시스템을 호스팅하는 파일 서버가 데이터를 제공할 수 있는 지속 속도입니다. 자세한 내용은 Amazon FSx for NetApp ONTAP 성능 단원을 참조하십시오.

6. 네트워킹 섹션에서 다음 정보를 입력합니다.

- Virtual Private Cloud(VPC)의 경우 파일 시스템에 연결할 VPC를 선택합니다.
- VPC 보안 그룹의 경우, 파일 시스템의 네트워크 인터페이스와 연결할 보안 그룹을 선택할 수 있습니다. 지정하지 않으면 Amazon FSx가 VPC의 기본 보안 그룹을 파일 시스템과 연결합니다.
- 파일 서버의 서브넷을 지정합니다. Multi-AZ 파일 시스템을 생성하는 경우 대기 파일 서버의 대기 서브넷도 선택합니다.
- (Multi-AZ만 해당) VPC 라우팅 테이블의 경우 파일 시스템의 엔드포인트를 생성할 VPC 라우팅 테이블을 지정합니다. 클라이언트가 있는 서브넷과 연결된 모든 VPC 라우팅 테이블을 선택합니다. 기본적으로 Amazon FSx는 VPC의 기본 라우팅 테이블을 선택합니다. 자세한 내용은 배포 VPC 외부에서 데이터 액세스 단원을 참조하십시오.

> **Note**
>
> Amazon FSx는 태그 기반 인증을 사용하여 Multi-AZ 파일 시스템에 대한 이러한 라우팅 테이블을 관리합니다. 이러한 라우팅 테이블은 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정됩니다. 를 사용하여 FSx for ONTAP 다중 AZ 파일 시스템을 생성할 때는 `Key: AmazonFSx; Value: ManagedByAmazonFSx` 태그를 수동으로 추가하는 것이 AWS CloudFormation 좋습니다.

- (Multi-AZ만 해당) 엔드포인트 IP 주소 범위는 파일 시스템에 액세스하기 위한 엔드포인트가 생성될 IP 주소 범위를 지정합니다.

  엔드포인트 IP 주소 범위에는 다음과 같은 세 가지 옵션이 있습니다.

  - VPC의 할당되지 않은 IP 주소 범위 - Amazon FSx는 파일 시스템의 엔드포인트 IP 주소 범위로 사용할 VPC의 기본 CIDR 범위에서 마지막 64개 IP 주소를 선택합니다. 이 옵션을 여러 번 선택하면 이 범위가 여러 파일 시스템에서 공유됩니다.

  > **Note**
  >
  > VPC의 기본 CIDR 범위에 있는 마지막 64개의 IP 주소 중 서브넷에서 사용 중인 주소가 있는 경우 이 옵션은 회색으로 표시됩니다. 이 경우에도 IP 주소 범위 입력 옵션을 선택하여 VPC 내 주소 범위(즉, 기본 CIDR 범위의 끝에 있지 않은 범위 또는 VPC의 보조 CIDR에 있는 범위)를 선택할 수 있습니다.

- 기본 서브넷에 파일 서버의 서브넷을 지정합니다. Multi-AZ 파일 시스템을 생성하는 경우 대기 파일 서버의 대기 서브넷도 선택합니다.
- (Multi-AZ만 해당) VPC 라우팅 테이블의 경우 파일 시스템의 엔드포인트를 생성할 VPC 라우팅 테이블을 지정합니다. 클라이언트가 있는 서브넷과 연결된 모든 VPC 라우팅 테이블을 선택합니다. 기본적으로 Amazon FSx는 VPC의 기본 라우팅 테이블을 선택합니다.
- (Multi-AZ만 해당) 엔드포인트 IP 주소 범위는 파일 시스템에 액세스하기 위한 엔드포인트가 생성될 IP 주소 범위를 지정합니다.

  엔드포인트 IP 주소 범위에는 다음과 같은 세 가지 옵션이 있습니다.

  - VPC의 할당되지 않은 IP 주소 범위 - Amazon FSx는 파일 시스템의 엔드포인트 IP 주소 범위로 사용할 VPC의 기본 CIDR 범위에서 마지막 64개 IP 주소를 선택합니다. 이 옵션을 여러 번 선택하면 이 범위가 여러 파일 시스템에서 공유됩니다.

    > **Note**
    >
    > VPC의 기본 CIDR 범위에 있는 마지막 64개의 IP 주소 중 서브넷에서 사용 중인 주소가 있는 경우 이 옵션은 회색으로 표시됩니다. 이 경우에도 IP 주소 범위 입력 옵션을 선택하여 VPC 내 주소 범위(즉, 기본 CIDR 범위의 끝에 있지 않은 범위 또는 VPC의 보조 CIDR에 있는 범위)를 선택할 수 있습니다.

  - VPC 외부의 유동 IP 주소 범위 - Amazon FSx는 동일한 VPC와 라우팅 테이블을 사용하는 다른 파일 시스템에서 아직 사용되지 않은 198.19.x.0/24 주소 범위를 선택합니다.
  - IP 주소 범위 입력 - 원하는 CIDR 범위를 제공할 수 있습니다. 선택한 IP 주소 범위는 서브넷과 겹치지 않는 한 VPC의 IP 주소 범위 내부 또는 외부에 있을 수 있습니다.

    > **Note**
    >
    > 다음 CIDR 범위에 속하는 범위는 FSx for ONTAP과 호환되지 않으므로 선택하지 않습니다.
    >
    > - 0.0.0.0/8
    > - 127.0.0.0/8
    > - 198.19.0.0/20
    > - 224.0.0.0/4
    > - 240.0.0.0/4
    > - 255.255.255.255/32

7. 암호화 섹션의 암호화 키에서 파일 시스템의 저장 데이터를 보호하는 AWS Key Management Service (AWS KMS) 암호화 키를 선택합니다.
8. 파일 시스템 관리 암호에는 `fsxadmin` 사용자의 보안 암호를 입력합니다. 암호를 확인합니다.

   `fsxadmin` 사용자는 ONTAP CLI 및 REST API를 사용하여 파일 시스템을 관리할 수 있습니다. `fsxadmin` 사용자에 대한 자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.
9. 기본 스토리지 가상 머신 구성 섹션에 다음 정보를 입력합니다.

   - 스토리지 가상 머신 이름 필드에 스토리지 가상 머신의 이름을 입력합니다. 밑줄(_) 특수 문자를 포함해 최대 47자의 영숫자를 사용할 수 있습니다.
   - SVM 관리 암호의 경우 선택적으로 암호 지정을 선택하고 SVM의 `vsadmin` 사용자 암호를 제공할 수 있습니다. `vsadmin` 사용자를 사용하여 ONTAP CLI 또는 REST API를 사용해 SVM을 관리할 수 있습니다. `vsadmin` 사용자에 대한 자세한 내용은 ONTAP CLI로 SVM 관리하기 섹션을 참조하세요.

     암호 지정 안 함(기본값)을 선택한 경우에도 파일 시스템의 `fsxadmin` 사용자를 사용하여 ONTAP CLI 또는 REST API를 사용해 파일 시스템을 관리할 수 있지만 SVM의 `vsadmin` 사용자를 사용하여 동일한 작업을 수행할 수는 없습니다.
   - 볼륨 보안 스타일에서 볼륨에 대해 Unix(Linux)와 NTFS 중에서 선택합니다. 자세한 내용은 볼륨 보안 스타일 단원을 참조하십시오.
   - Active Directory 섹션에서 Active Directory를 SVM에 조인할 수 있습니다. 자세한 내용은 FSx for ONTAP에서 Microsoft Active Directory 작업 단원을 참조하십시오.

     SVM을 Active Directory에 조인하지 않으려면 Active Directory 조인 안 함을 선택합니다.

     SVM을 자체 관리형 Active Directory 도메인에 조인하려면 Active Directory 조인을 선택하고 Active Directory에 대한 다음 세부 정보를 제공합니다.

     - SVM에 대해 생성할 Active Directory 컴퓨터 객체의 NetBIOS 이름. NetBIOS 이름은 15자를 초과할 수 없습니다.
     - Active Directory의 정규화된 도메인 이름. 도메인 이름은 255자를 초과할 수 없습니다.
     - DNS 서버 IP 주소 - 도메인에 대한 도메인 이름 시스템(DNS)의 IPv4 주소입니다.
     - 서비스 계정 사용자 이름 - 기존 Active Directory에 있는 서비스 계정의 사용자 이름입니다. 도메인 접두사나 접미사를 포함하지 않습니다.
     - 서비스 계정 암호 - 서비스 계정의 암호입니다.
     - 암호 확인 - 서비스 계정의 암호입니다.

- (선택 사항) 조직 단위(OU) - 파일 시스템에 조인하려는 조직 단위의 고유 경로 이름입니다.
- 위임된 파일 시스템 관리자 그룹 - Active Directory에서 파일 시스템을 관리할 수 있는 그룹의 이름입니다.

  를 사용하는 경우 AWS 위임된 FSx 관리자 AWS Managed Microsoft AD AWS , 위임된 관리자 또는 OU에 위임된 권한이 있는 사용자 지정 그룹과 같은 그룹을 지정해야 합니다.

  자체 관리형 AD에 조인하는 경우 AD에 있는 그룹의 이름을 사용합니다. 기본 그룹은 `Domain Admins`입니다.

10. 기본 볼륨 구성 섹션에서 파일 시스템으로 만든 기본 볼륨에 대해 다음 정보를 입력합니다.

- 볼륨 이름 필드에 볼륨의 이름을 입력합니다. 최대 203자의 영숫자 또는 밑줄 (_) 문자를 사용할 수 있습니다.
- (HA 페어가 한 개 있는 파일 시스템만 해당) 볼륨 스타일에서 FlexVol 또는 FlexGroup를 선택합니다. FlexVol 볼륨은 최대 300테비바이트(TiB) 크기의 범용 볼륨입니다. FlexGroup 볼륨은 고성능 워크로드를 위한 것이며 최대 20 PiB 크기의 볼륨일 수 있습니다.
- 볼륨 크기는 FlexVol 볼륨의 경우 20–314,572,800 메비바이트(MiB) 범위의 정수를 입력하거나, FlexGroup 볼륨의 경우 HA 쌍당 800기가바이트(GiB)~2,400TiB 범위의 정수를 입력합니다. 예를 들어 HA 페어가 12개인 파일 시스템의 최소 볼륨 크기는 9,600GiB이고 최대 크기는 20,480TiB.
- 볼륨 유형의 경우 읽기 및 쓰기가 가능한 볼륨을 생성하려면 읽기-쓰기(RW)를 선택하고 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용할 수 있는 읽기 전용 볼륨을 생성하려면 데이터 보호(DP)를 선택합니다. 자세한 내용은 볼륨 유형 단원을 참조하십시오.
- 정션 경로에는 파일 시스템 내에서 볼륨을 마운트할 위치를 입력합니다. 이름 앞에 슬래시가 있어야 합니다(예: `/vol3`).
- 스토리지 효율성의 경우 ONTAP 스토리지 효율성 기능(중복 제거 및 압축)을 활성화하려면 활성화를 선택합니다. 자세한 내용은 스토리지 효율성 섹션을 참조하세요.
- 스냅샷 정책에서 볼륨의 스냅샷 정책을 선택합니다. 스냅샷 정책에 대한 자세한 내용은 스냅샷 정책 섹션을 참조하세요.

  사용자 지정 정책을 선택하는 경우 custom-policy 필드에 정책 이름을 지정해야 합니다. 사용자 지정 정책은 SVM 또는 파일 시스템에 이미 있어야 합니다. ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요.

11. 기본 볼륨 스토리지 계층화 섹션에서 용량 풀 계층화 정책에는 볼륨의 스토리지 풀 계층화 정책을 자동(기본값), 스냅샷만, 모두, 없음 중에서 선택합니다. 용량 풀 계층화 정책에 대한 자세한 내용은 볼륨 계층화 정책 섹션을 참조하세요.

    계층화 정책 휴지 기간에서 스토리지 계층화를 `Auto` 및 `Snapshot-only` 정책 중 하나로 설정한 경우 유효한 값은 2~183일입니다. 볼륨의 계층화 정책 휴지 기간은 액세스되지 않은 데이터가 콜드 상태로 표시되고 용량 풀 스토리지로 이동되기까지의 일수를 정의합니다.

12. 기본 볼륨 SnapLock 구성 섹션의 SnapLock 구성에서 활성화와 비활성화 중 하나를 선택합니다. SnapLock 컴플라이언스 볼륨 또는 SnapLock 엔터프라이즈 볼륨 구성에 대한 자세한 내용은 SnapLock 규정 준수 이해 및 SnapLock 엔터프라이즈 이해를 참조하세요. SnapLock에 대한 자세한 정보는 SnapLock로 데이터 보호 섹션을 참조하세요.

13. 백업 및 유지 관리 - 선택 사항에서 다음 옵션을 설정할 수 있습니다.

    - 일별 자동 백업의 경우 자동 일별 백업의 활성화를 선택합니다. 이 옵션은 기본적으로 활성화되어 있습니다.
    - 일별 자동 백업 기간에는 하루 중 일별 자동 백업 기간을 시작할 시간을 협정 세계시(UTC) 단위로 설정합니다. 기간은 지정 시각에서 시작하여 30분입니다. 이 기간은 주별 유지 관리 백업 기간과 겹칠 수 없습니다.
    - 자동 백업 보존 기간의 경우 자동 백업을 보존할 기간을 1~90일로 설정합니다.
    - 주별 유지 관리 기간에는 유지 관리 기간을 주중 시각을 설정합니다. 1일차는 월요일, 2일차는 화요일 등입니다. 백업 기간은 지정 시각에서 시작하여 30분입니다. 이 기간은 일별 자동 백업 기간과 겹칠 수 없습니다.

14. 태그 - 옵션의 경우 키와 값을 입력하여 태그를 파일 시스템에 추가합니다. 태그는 파일 시스템을 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.

    다음을 선택합니다.

15. 파일 시스템 생성 페이지에 표시된 파일 시스템 구성을 검토합니다. 참조할 수 있도록 파일 시스템을 생성한 후 수정할 수 있는 파일 시스템 설정을 확인합니다.

16. 파일 시스템 생성을 선택합니다.

파일 시스템 생성(CLI)

- FSx for ONTAP 파일 시스템을 생성하려면 다음 예제와 같이 create-file-system CLI 명령(또는 이에 상응하는 CreateFileSystem API 작업)을 사용합니다.

> **Note**
>
> 생성 후에는 파일 시스템의 배포 유형을 변경할 수 없습니다. 배포 유형을 변경하려면(예: Single-AZ 1에서 Single-AZ 2로 이동) 데이터를 백업하고 새 파일 시스템에서 복원할 수 있습니다. NetApp SnapMirror, AWS DataSync또는 타사 데이터 복사 도구를 사용하여 데이터를 마이그레이션할 수도 있습니다. 자세한 내용은 NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션 및 AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션 섹션을 참조하세요.

```
aws fsx create-file-system \
    --file-system-type ONTAP \
    --storage-capacity 1024 \
    --storage-type SSD \
    --security-group-ids security-group-id \

    --subnet-ids subnet-abcdef1234567890b subnet-abcdef1234567890c \
    --ontap-configuration DeploymentType=MULTI_AZ_1,
        ThroughputCapacity=512,PreferredSubnetId=subnet-abcdef1234567890b
```

파일 시스템을 만든 후 Amazon FSx에서는 다음 예제에서처럼 파일 시스템 설명을 JSON 형식으로 반환합니다.

```
{
  "FileSystem": {
    "OwnerId": "111122223333",
    "CreationTime": 1625066825.306,
    "FileSystemId": "fs-0123456789abcdef0",
    "FileSystemType": "ONTAP",
    "Lifecycle": "CREATING",
    "StorageCapacity": 1024,
    "StorageType": "SSD",
    "VpcId": "vpc-11223344556677aab",
    "SubnetIds": [
      "subnet-abcdef1234567890b",
      "subnet-abcdef1234567890c"
    ],
    "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJalrXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
```

```
    "ResourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/
fs-0123456789abcdef0",
    "Tags": [],
    "OntapConfiguration": {
      "DeploymentType": "MULTI_AZ_HA_1",
      "EndpointIpAddressRange": "198.19.0.0/24",
      "Endpoints": {
        "Management": {
          "DnsName": "management.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        },
        "Intercluster": {
          "DnsName": "intercluster.fs-0123456789abcdef0.fsx.us-east-1.amazonaws.com"
        }
      },
      "DiskIopsConfiguration": {
                "Mode": "AUTOMATIC",
                "Iops": 3072
      },
      "PreferredSubnetId": "subnet-abcdef1234567890b",
      "RouteTableIds": [
        "rtb-abcdef1234567890e",
        "rtb-abcd1234ef567890b"
      ],
      "ThroughputCapacity": 512,
      "WeeklyMaintenanceStartTime": "4:10:00"
    }
  }
}
```

> **Note**
>
> 콘솔에서 파일 시스템을 만드는 과정과 달리, `create-file-system` CLI 명령과 `CreateFileSystem` API 작업은 기본 SVM이나 볼륨을 만들지 않습니다. SVM을 생성하려면 스토리지 가상 머신 생성(SVM) 섹션을 참조하고, 볼륨을 생성하려면 볼륨 생성 섹션을 참조하세요.

공유 서브넷에서 FSx for ONTAP 파일 시스템 만들기

VPC 공유를 사용하면 여러 AWS 계정 가 공유된 중앙 관리형 Virtual Private Cloud(VPCs. 이 모델에서 VPC(소유자)를 소유한 계정은 하나 이상의 서브넷을 동일한 조직에 속한 다른 계정(참가자)과 공유합니다 AWS Organizations.

참가자 계정은 소유자 계정이 공유한 VPC 서브넷에서 FSx for ONTAP Single-AZ 및 Multi-AZ 파일 시스템을 생성할 수 있습니다. 참가자 계정이 Multi-AZ 파일 시스템을 생성하려면 소유자 계정도 Amazon FSx에 참가자 계정을 대신하여 공유 서브넷의 라우팅 테이블을 수정할 수 있는 권한을 부여해야 합니다. 자세한 내용은 Multi-AZ 파일 시스템에 대한 공유 VPC 지원 관리 단원을 참조하십시오.

> **Note**
>
> 참가자 계정은 참가자 파일 시스템의 VPC 내 CIDR과 겹치는 후속 VPC 서브넷이 생성되지 않도록 VPC 소유자와 조율할 책임이 있습니다. 서브넷이 겹치면 파일 시스템으로의 트래픽이 중단될 수 있습니다.

공유 서브넷 요구 사항 및 고려 사항

FSx for ONTAP 파일 시스템을 공유 VPC 서브넷에 생성할 경우 다음 사항에 유의하세요.

- VPC 서브넷의 소유자는 참가자 계정과 서브넷을 공유해야만 해당 계정이 해당 서브넷에 FSx for ONTAP 파일 시스템을 생성할 수 있습니다.
- 참여자는 VPC의 기본 보안 그룹을 사용하여 리소스를 시작할 수 없습니다. 보안 그룹은 소유자에게 속해 있기 때문입니다. 또한 참여자 계정은 소유자 또는 다른 참여자가 소유한 보안 그룹을 사용하여 리소스를 시작할 수 없습니다.
- 공유 서브넷에서는 참여자와 소유자가 각 계정 내의 보안 그룹을 별도로 제어합니다. 소유자 계정은 참가자가 만든 보안 그룹을 볼 수 있지만 해당 그룹에 대해 어떤 작업도 수행할 수 없습니다. 소유자 계정에서 보안 그룹을 제거하거나 수정하고자 하는 경우 보안 그룹을 생성한 참가자가 조치를 취해야 합니다.
- 참가자 계정은 소유자 계정이 공유한 서브넷에서 Single-AZ 파일 시스템 및 관련 리소스를 확인, 생성, 수정 및 삭제할 수 있습니다.
- 참가자 계정은 소유자 계정이 공유한 서브넷에서 Multi-AZ 파일 시스템 및 관련 리소스를 생성, 보기, 수정 및 삭제할 수 있습니다. 또한 소유자 계정은 참가자 계정을 대신하여 공유 서브넷의 라우팅 테이블을 수정할 수 있는 Amazon FSx 서비스 권한도 부여해야 합니다. 자세한 내용은 Multi-AZ 파일 시스템에 대한 공유 VPC 지원 관리 섹션을 참조하세요.
- 공유 VPC 소유자는 참가자가 공유 서브넷에서 만든 리소스를 보거나 수정하거나 삭제할 수 없습니다. 여기에 더해 계정마다 액세스 권한이 다른 VPC 리소스가 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 소유자 및 참여자에 대한 책임 및 권한을 참조하세요.

자세한 내용은 Amazon VPC 사용 설명서의 다른 계정과 VPC 공유를 참조하세요.

VPC 서브넷을 공유하는 경우

공유 서브넷에서 FSx for ONTAP 파일 시스템을 생성할 참가자 계정과 서브넷을 공유할 때는 다음을 수행해야 합니다.

- VPC 소유자는를 사용하여 VPCs 및 서브넷을 다른와 AWS Resource Access Manager 안전하게 공유해야 합니다 AWS 계정. 자세한 내용은 AWS Resource Access Manager 사용 설명서의 AWS 리소스 공유를 참조하세요.
- VPC 소유자는 참가자 계정과 하나 이상의 VPCs를 공유해야 합니다. 자세한 내용은 Amazon 가상 사설 클라우드 사용 설명서에서 다른 계정과 VPC 공유를 참조하세요.
- 참가자 계정이 FSx for ONTAP Multi-AZ 파일 시스템을 생성하려면 VPC 소유자는 참가자 계정을 대신하여 공유 서브넷에서 라우팅 테이블을 생성하고 수정할 수 있는 Amazon FSx 서비스 권한도 부여해야 합니다. 이는 FSx for ONTAP Multi-AZ 파일 시스템이 부동 IP 주소를 사용하므로 연결된 클라이언트가 장애 조치 이벤트 중에 기본 파일 서버와 대기 파일 서버 간에 원활하게 전환할 수 있기 때문입니다. 장애 조치 이벤트가 발생하면 Amazon FSx는 현재 활성 파일 서버를 가리키도록 파일 시스템과 연결된 모든 라우팅 테이블의 모든 경로를 업데이트합니다.

Multi-AZ 파일 시스템에 대한 공유 VPC 지원 관리

소유자 계정은 다음 섹션에 설명된 대로 소유자가 AWS Management Console AWS CLI및 API를 사용하여 참가자와 공유한 VPC 서브넷에서 참가자 계정이 다중 AZ FSx for ONTAP 파일 시스템을 생성할 수 있는지 여부를 관리할 수 있습니다.

Multi-AZ 파일 시스템의 VPC 공유를 관리하려면(콘솔)

https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.

1. 탐색 창에서 설정을 선택합니다.
2. 설정 페이지에서 Multi-AZ 공유 VPC 설정을 찾습니다.
    - 공유하는 VPC 서브넷에서 Multi-AZ 파일 시스템에 대한 VPC 공유를 활성화하려면 참가자 계정에서 라우팅 테이블 업데이트 활성화를 선택합니다.
    - 소유한 모든 VPC에서 Multi-AZ 파일 시스템에 대한 VPCs 비활성화하려면 참가자 계정에서 라우팅 테이블 업데이트 비활성화를 선택합니다. 확인 화면이 표시됩니다.

> **Important**
>
> 이 기능을 비활성화하기 전에 공유 VPC에서 참가자가 생성한 Multi-AZ 파일 시스템을 삭제하는 것이 좋습니다. 기능이 비활성화되면 이러한 파일 시스템은 `MISCONFIGURED` 상태가 되고 사용할 수 없게 될 위험이 있습니다.

3. **`confirm`**를 입력하고 확인을 선택하여 기능을 비활성화합니다.

Multi-AZ 파일 시스템의 VPC 공유를 관리하려면(AWS CLI)

1. Multi-AZ VPC 공유의 현재 설정을 보려면 다음과 같이 describe-shared-vpc-configuration CLI 명령 또는 이에 상응하는 DescribeSharedVpcConfiguration API 명령을 사용합니다.

```
$ aws fsx describe-shared-vpc-configuration
```

서비스는 다음과 같이 성공적인 요청에 응답합니다.

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

2. Multi-AZ 공유 VPC 구성을 관리하려면 update-shared-vpc-configuration CLI 명령 또는 동등한 UpdateSharedVpcConfiguration API 명령을 사용합니다. 다음 예제에서는 Multi-AZ 파일 시스템에 대한 VPC 공유를 활성화합니다.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-
participant-accounts true
```

서비스는 다음과 같이 성공적인 요청에 응답합니다.

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "true"
}
```

3. 기능을 비활성화하려면 다음 예제와 같이 `EnableFsxRouteTableUpdatesFromParticipantAccounts`를 `false`로 설정합니다.

```
$ aws fsx update-shared-vpc-configuration --enable-fsx-route-table-updates-from-
participant-accounts false
```

서비스는 다음과 같이 성공적인 요청에 응답합니다.

```
{
    "EnableFsxRouteTableUpdatesFromParticipantAccounts": "false"
}
```

파일 시스템 업데이트

이 주제에서는 업데이트할 수 있는 기존 파일 시스템의 속성을 설명하고 Amazon FSx 콘솔 및 CLI를 사용하여 업데이트할 수 있는 절차를 제공합니다. Amazon FSx 콘솔 AWS CLI및 API를 사용하여 다음 FSx for ONTAP 파일 시스템 속성을 업데이트할 수 있습니다.

- 자동 일별 백업. 자동 일별 백업을 켜거나 끄고, 백업 기간과 백업 보존 기간을 수정합니다. 자세한 내용은 자동 일별 백업. 단원을 참조하십시오.
- 주별 유지 관리 기간. Amazon FSx가 파일 시스템 유지 관리 및 업데이트를 수행하는 요일과 시간을 설정합니다. 자세한 내용은 Amazon FSx 유지 관리 기간을 통한 성능 최적화 단원을 참조하십시오.
- 파일 시스템 관리 암호. 파일 시스템의 `fsxadmin` 사용자의 암호를 변경합니다. `fsxadmin` 사용자는 ONTAP CLI 및 REST API를 사용하여 파일 시스템을 관리할 수 있습니다. `fsxadmin` 사용자에 대한 자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.
- Amazon VPC 라우팅 테이블. Multi-AZ FSx for ONTAP 파일 시스템을 사용하는 경우 NFS 또는 SMB를 통해 데이터에 액세스하는 데 사용하는 엔드포인트와, ONTAP CLI, API 및 BlueXP에 액세스하는 관리 엔드포인트는 파일 시스템과 연결하는 Amazon VPC 라우팅 테이블의 유동 IP 주소를 사용합니다. 새로 생성한 라우팅 테이블을 기존의 Multi-AZ 파일 시스템과 연결하여 네트워크가 발전하더라도 데이터에 액세스할 수 있는 클라이언트를 구성할 수 있습니다. 파일 시스템에서 기존 라우팅 테이블을 분리(제거)할 수도 있습니다.

> **Note**
>
> Amazon FSx는 태그 기반 인증을 사용하여 Multi-AZ 파일 시스템의 VPC 라우팅 테이블을 관리합니다. 이러한 라우팅 테이블은 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정됩니다. 를 사용하여 FSx for ONTAP 다

중 AZ 파일 시스템을 생성하거나 업데이트할 때는 `Key: AmazonFSx; Value: ManagedByAmazonFSx` 태그를 수동으로 추가하는 것이 AWS CloudFormation 좋습니다.

파일 시스템 업데이트(콘솔)

다음 절차에서는 AWS Management Console를 사용하여 기존 FSx for ONTAP 파일 시스템을 업데이트하는 방법에 대한 지침을 제공합니다.

자동 일별 백업 업데이트

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 페이지의 두 번째 패널에서 백업 탭을 선택합니다.
4. 업데이트를 선택합니다.
5. 이 파일 시스템의 자동 일별 백업 설정을 수정합니다.
6. 저장을 선택하여 변경 사항을 저장합니다.

주별 유지 관리 기간 업데이트

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 페이지의 두 번째 패널에서 관리 탭을 선택합니다.
4. 유지 관리 창에서 업데이트를 선택합니다.
5. 이 파일 시스템의 주별 유지 관리 기간이 발생하는 시기를 수정합니다.
6. 저장을 선택하여 변경 사항을 저장합니다.

파일 시스템 관리 암호 변경

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 관리 탭을 선택합니다.

4. ONTAP 관리 창의 ONTAP 관리자 암호에서 업데이트를 선택합니다.
5. ONTAP 관리자 자격 증명 업데이트 대화 상자의 ONTAP 관리 암호 필드에 새 암호를 입력합니다.
6. 암호 확인 필드를 사용하여 암호를 확인합니다.
7. 자격 증명 업데이트를 선택하여 변경 사항을 저장합니다.

> **Note**
>
> 새 암호가 암호 요구 사항을 충족하지 않는다는 오류가 발생하면 `security login role config show` ONTAP CLI 명령을 사용하여 파일 시스템의 암호 요구 사항 설정을 볼 수 있습니다. 암호 설정을 변경하는 방법에 대한 지침을 비롯한 자세한 내용은 fsxadmin 계정 암호 업데이트 실패했습니다.을 참조하세요.

Multi-AZ 파일 시스템에서 VPC 경로 테이블 업데이트하기

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 작업에는 라우팅 테이블 관리를 선택합니다. 이 옵션은 Multi-AZ 파일 시스템에서만 사용할 수 있습니다.
4. 라우팅 테이블 관리 대화 상자에서 다음 중 하나를 수행합니다.
   - 새 VPC 라우팅 테이블을 연결하려면 새 라우팅 테이블 연결 드롭다운 목록에서 라우팅 테이블을 선택한 후 연결을 선택합니다.
   - 기존 VPC 라우팅 테이블을 연결 해제하려면 현재 라우팅 테이블 창에서 라우팅 테이블을 선택한 후 연결 해제를 선택합니다.
5. 닫기를 선택하세요.

파일 시스템 업데이트(CLI)

다음 절차에서는 AWS CLI를 사용하여 기존 FSx for ONTAP 파일 시스템을 업데이트하는 방법을 보여줍니다.

1. FSx for ONTAP 파일 시스템 구성을 업데이트하려면 다음 예제에서와 같이 update-file-system CLI 명령(또는 이에 상응하는 UpdateFileSystem API 작업)을 사용합니다.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration
 AutomaticBackupRetentionDays=30,DailyAutomaticBackupStartTime=01:00, \
      WeeklyMaintenanceStartTime=1:01:30,AddRouteTableIds=rtb-0123abcd, \
      FsxAdminPassword=new-fsx-admin-password
```

2. 자동 일일 백업을 비활성화하려면 AutomaticBackupRetentionDays 속성을 0으로 설정합니다.

```
aws fsx update-file-system \
    --file-system-id fs-0123456789abcdef0 \
    --ontap-configuration AutomaticBackupRetentionDays=0
```

고가용성(HA) 페어 관리

각 FSx for ONTAP 파일 시스템은 액티브 스탠바이 구성에서 하나 이상의 고가용성(HA) 파일 서버 페어로 구동됩니다. 이 구성에는 트래픽을 적극적으로 처리하는 기본 파일 서버와 활성 서버를 사용할 수 없는 경우 인계하는 보조 파일 서버가 있습니다. 1세대 FSx for ONTAP 파일 시스템은 최대 4GBps의 처리량 용량과 160,000 SSD IOPs. 2세대 FSx for ONTAP Multi-AZ 파일 시스템은 하나의 HA 페어로도 구동되며 최대 6GBps의 처리량 용량과 200,000 SSD IOPS를 제공합니다. 2세대 FSx for ONTAP Single-AZ 파일 시스템은 최대 12개의 HA 페어로 구동되며, 최대 72GBps의 처리량 용량과 2,400,000 SSD IOPS(HA 페어당 6GBps의 처리량 용량과 200,000 SSD IOPS)를 제공할 수 있습니다.

Amazon FSx 콘솔에서 파일 시스템을 생성할 때 Amazon FSx는 원하는 SSD 스토리지를 기반으로 사용해야 하는 HA 페어 수를 권장합니다. 워크로드 및 성능 요구 사항에 따라 HA 페어 수를 수동으로 선택할 수도 있습니다. 파일 시스템 요구 사항이 최대 6GBps의 처리량 용량과 200,000 SSD IOPs를 충족하는 경우 단일 HA 페어를 사용하고 워크로드에 더 높은 수준의 성능 확장성이 필요한 경우 여러 HA 페어를 사용하는 것이 좋습니다.

각 HA 페어에는 논리적 물리적 디스크 집합인 하나의 집계가 있습니다.

> **Note**
>
> 2세대 Single-AZ 파일 시스템에 HA 페어를 추가할 수 있습니다. 자세한 내용은 고가용성(HA) 페어 추가 단원을 참조하십시오. 그렇지 않으면를 사용하거나 백업에서 새 파일 시스템으로 데

이터를 복원SnapMirror AWS DataSync하여 파일 시스템(다른 HA 페어 사용) 간에 데이터를 마이그레이션할 수 있습니다.

고가용성(HA) 페어 추가

FSx for ONTAP 파일 시스템은 하나 이상의 HA 쌍의 파일 서버로 구성됩니다. 1세대 파일 시스템과 2세대 Multi-AZ 파일 시스템은 HA 페어 하나를 지원하는 반면 2세대 Single-AZ 파일 시스템은 최대 12개의 HA 페어를 지원합니다. 2세대 Single-AZ 파일 시스템을 생성한 후 HA 페어를 더 추가할 수도 있습니다(최대 12개). HA 페어를 추가하는 것은 방해가 되지 않으며 일반적으로 완료하는 데 몇 분밖에 걸리지 않습니다.

파일 시스템에 HA 페어를 추가할 때 다음 사항을 고려하세요.

- 파일 시스템에 HA 페어를 추가하면 자체 스토리지(또는 집계)가 있는 새 파일 서버가 도입됩니다. 새 HA 페어는 파일 시스템의 기존 HA 페어와 처리량 및 스토리지 용량이 동일합니다. 예를 들어 파일 시스템에 총 12GBps의 처리량 용량과 2테비바이트(TiB)의 SSD 스토리지를 포함하는 HA 페어가 2개 있다고 가정해 보겠습니다. 새 HA 페어를 하나 추가하면 파일 시스템에 18GBps의 처리량 용량과 3TiB의 SSD 스토리지가 제공됩니다.
- 새 HA 페어의 추가 성능을 활용하려면 기존 볼륨의 일부를 새 HA 페어로 이동하고 클라이언트를 다시 탑재하여 연결해야 합니다. 자세한 내용은 HA 페어 간에 워크로드 밸런싱 단원을 참조하십시오.
- HA 페어를 추가할 때 또는 HA 페어 추가 업데이트가 진행되는 동안에는 파일 시스템의 처리량 용량, SSD 스토리지 용량 또는 프로비저닝된 SSD IOPS를 수정할 수 없습니다.
- HA 페어를 추가한 후에는 제거할 수 없습니다. 일시적으로 더 많은 성능이 필요한 경우 파일 시스템의 처리량 용량을 조정하는 것이 좋습니다(파일 시스템이 처리량 용량이 가장 크지 않다고 가정). 이렇게 하면 파일 시스템의 기존 HA 페어의 처리량 용량이 증가합니다.
- 2세대 파일 시스템의 HA 페어를 1개에서 2개 이상으로 늘리려면 파일 시스템에 최대 5개의 SVMS가 있을 수 있습니다.
- iSCSI 프로토콜은 고가용성 페어(HA 페어)가 6개 이하인 파일 시스템에서 사용할 수 있습니다. NVMe/TCP 프로토콜은 HA 페어가 6개 이하인 2세대 파일 시스템에서 사용할 수 있습니다. 자세한 내용은 FSx for ONTAP 데이터 액세스 단원을 참조하십시오.
- 파일 시스템에 새 HA 페어를 추가하면 새 파일 시스템 노드에 대해 NVMe 캐시가 기본적으로 활성화됩니다. 처리량이 많은 워크로드에는 비활성화하는 것이 좋습니다. 자세한 내용은 NVMe 캐시 관리 단원을 참조하십시오.

HA 페어를 추가하려면

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트할 FSx for ONTAP 파일 시스템을 선택합니다.
3. 요약 패널의 HA 페어 수에서 업데이트를 선택합니다.
4. HA 페어 드롭다운에서 파일 시스템에 추가할 HA 페어 수를 선택합니다.
5. 업데이트 버튼을 선택합니다.

HA 페어를 추가한 후에는 I/O가 파일 시스템의 HA 페어에 고르게 분산되도록 기존 데이터의 균형을 재조정하는 것이 중요합니다. 자세한 내용은 HA 페어 간에 워크로드 밸런싱 단원을 참조하십시오.

HA 페어 간에 워크로드 밸런싱

HA(고가용성) 페어가 여러 개 있는 파일 시스템이 있는 경우 각 HA 페어에 처리량과 스토리지가 분산됩니다. FSx for ONTAP는 파일 시스템에 기록될 때 자동으로 파일의 균형을 맞추지만 HA 페어를 추가하면 워크로드 데이터와 I/O가 더 이상 균형을 이루지 않습니다. 또한 드문 경우지만 워크로드 데이터 또는 I/O가 파일 시스템의 기존 HA 페어에서 불균형해질 수 있으며, 이는 워크로드의 전체 성능에 영향을 미칠 수 있습니다. 워크로드가 불균형한 경우 각 파일 시스템의 HA 페어(및 그에 상응하는 파일 서버 및 집계, 즉 프라이머리 스토리지 계층을 구성하는 스토리지 풀) 간에 워크로드를 재조정할 수 있습니다.

주제

- 기본 스토리지 사용률 균형
- 파일 서버 및 디스크 성능 사용률 불균형
- CloudWatch 차원을 ONTAP CLI 및 REST API 리소스에 매핑
- 클라이언트 리밸런싱
- 볼륨 재조정

기본 스토리지 사용률 균형

파일 시스템의 기본 스토리지 용량은 집계라고 하는 스토리지 풀의 각 HA 페어 간에 균등하게 분할됩니다. 각 HA 페어에는 하나의 집계가 있습니다. 기본 스토리지 계층의 평균 사용률을 80% 이하로 유지하는 것이 좋습니다. HA 페어가 여러 개인 파일 시스템의 경우 모든 집계에 대해 평균 사용률을 최대 80%까지 유지하는 것이 좋습니다.

80%의 사용률을 유지하면 새 수신 데이터를 위한 여유 공간이 확보되고 유지 관리 작업에 대한 양호한 오버헤드가 유지되어 집계의 여유 공간을 일시적으로 확보할 수 있습니다.

집계가 불균형한 경우 파일 시스템의 기본 스토리지 용량을 늘리거나(각 집계의 스토리지 용량을 늘리는 것에 상응) 집계 간에 볼륨을 이동할 수 있습니다. 자세한 내용은 집계 간 볼륨 이동 단원을 참조하십시오.

파일 서버 및 디스크 성능 사용률 불균형

파일 시스템의 총 성능 기능(예: 네트워크 처리량, 파일 서버-디스크 처리량 및 IOPS, 디스크 IOPS)은 파일 시스템의 HA 페어 간에 균등하게 분할됩니다. 모든 성능 제한에 대해 평균 사용률을 지속적으로 50% 미만으로 유지하는 것이 좋습니다(최대 최대 사용률은 80% 미만). 이는 모든 HA 페어에서 파일 시스템의 파일 서버 리소스를 전체적으로 사용하는 것뿐만 아니라 파일당 서버 기준으로도 적용됩니다.

파일 서버 성능 사용률이 불균형하고 워크로드가 불균형한 파일 서버의 사용률이 80%를 초과하는 경우 ONTAP CLI 및 REST API를 사용하여 성능 불균형의 원인을 추가로 진단하고 수정할 수 있습니다. 다음은 가능한 불균형 지표와 추가 진단을 위한 다음 단계 표입니다.

파일 시스템의	해당되는 조치
파일 서버 디스크 처리량 또는 파일 서버 디스크 IOPS 불균형	HA 페어의 하위 집합(액세스되는 데이터의 양이 너무 많은 볼륨의 하위 집합)에서 I/O 핫스팟이 발생할 수 있으며, 이로 인해 HA 페어의 하위 집합에 대해 병목 현상이 발생하기 때문에 워크로드의 전체 성능이 제한될 수 있습니다. 활용도가 높은 각 파일 서버에 대해 가장 많이 사용되는 볼륨을 확인하여 집계 내에서 활동이 가장 높은 볼륨을 확인합니다. 이 절차에 대한 자세한 정보는 볼륨 재조정 단원을 참조하세요.
네트워크 처리량이 불균형하지만 파일 서버 디스크 처리량, 파일 서버 디스크 IOPS 또는 디스크 IOPS가 불균형하지 않음	데이터는 HA 페어 간에 균등하게 분산되지만 클라이언트는 그렇지 않습니다. 다른 것보다 네트워크 처리량 사용률이 더 높은 파일 서버의 경우 각 파일 서버의 최상위 클라이언트를 확인한 다음 해당 클라이언트에서 볼륨을 탑재재 해제하고 다른 HA 페어에서 다른 엔드포인트를 사용하여 다시 탑재재하여 해당 클라이언트의 균형을 조정합니다. 이 절차에 대한 자세한 정보는 클라이언트 리밸런싱 단원을 참조하세요.

CloudWatch 차원을 ONTAP CLI 및 REST API 리소스에 매핑

2세대 파일 시스템에는 `FileServer` 또는 `Aggregate` 차원이 있는 Amazon CloudWatch 지표가 있습니다. 불균형 사례를 추가로 진단하려면 이러한 차원 값을 ONTAP CLI 또는 REST API의 특정 파일 서버(또는 노드) 및 집계에 매핑해야 합니다.

- 파일 서버의 경우 각 파일 서버 이름은 ONTAP의 파일 서버(또는 노드) 이름(예: `FsxId01234567890abcdef-01`)에 매핑됩니다. 홀수 번호의 파일 서버는 선호하는 파일 서버(즉, 파일 시스템이 보조 파일 서버로 장애 조치되지 않은 한 트래픽을 서비스함)이고, 짝수 번호의 파일 서버는 보조 파일 서버(즉, 파트너를 사용할 수 없는 경우에만 트래픽을 서비스함)입니다. 따라서 보조 파일 서버는 일반적으로 선호하는 파일 서버보다 사용률이 낮습니다.
- 집계의 경우 각 집계 이름은 ONTAP의 집계에 매핑됩니다(예: `aggr1`). 모든 HA 페어에는 하나의 집계가 있는데, 즉, 집계 `aggr1`는 HA 페어의 파일 서버 `FsxId01234567890abcdef-01`(활성 파일 서버)와 `FsxId01234567890abcdef-02`(보조 파일 서버)가 공유하고, 집계 `aggr2`는 파일 서버 `FsxId01234567890abcdef-03`와 `FsxId01234567890abcdef-04`가 공유하는 식입니다.

ONTAP CLI를 사용하여 모든 집계와 파일 서버 간의 매핑을 볼 수 있습니다.

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 스토리지 집계 표시 명령을 사용하여 `-fields node` 파라미터를 지정합니다.

   ```
   ::> storage aggregate show -fields node
   aggregate                      node
   ------------------------------ -------------------------
   aggr1                          FsxId01234567890abcdef-01
   aggr2                          FsxId01234567890abcdef-03
   aggr3                          FsxId01234567890abcdef-05
   aggr4                          FsxId01234567890abcdef-07
   aggr5                          FsxId01234567890abcdef-09
   aggr6                          FsxId01234567890abcdef-11
   6 entries were displayed.
   ```

클라이언트 리밸런싱

HA 페어를 추가한 후 또는 파일 서버 간에 I/O 불균형이 발생하는 경우(특히 네트워크 처리량 사용률에 따라) 클라이언트를 재조정할 수 있습니다. HA 페어를 추가한 후 클라이언트의 리밸런싱을 수행하는 경우 클라이언트 재탑재로 건너뛸 수 있습니다. 그렇지 않으면 먼저 이동하려는 트래픽이 많은 클라이언트를 식별하여 워크로드 I/O의 균형을 재조정해야 합니다.

파일 서버(특히 네트워크 처리량 사용률) 간에 I/O 불균형이 발생하는 경우 I/O 클라이언트가 높을 수 있습니다. 트래픽이 많은 클라이언트를 식별하려면 ONTAP CLI를 사용합니다.

트래픽이 많은 클라이언트 식별

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 트래픽이 가장 높은 클라이언트를 보려면 통계 상위 클라이언트 show ONTAP CLI 명령을 사용합니다. 선택적으로 -node 파라미터를 지정하여 특정 파일 서버의 최상위 클라이언트만 볼 수 있습니다. 특정 파일 서버의 불균형을 진단하는 경우 -node 파라미터를 사용하고 node_name를 파일 서버의 이름으로 바꿉니다(예: FsxId01234567890abcdef-01).

   선택적으로 -interval 파라미터를 추가하여 각 보고서가 출력되기 전에 측정할 간격(초)을 제공할 수 있습니다. 간격을 늘리면(예: 최대 300초) 각 볼륨으로 구동되는 트래픽 양에 대한 장기 샘플이 제공됩니다. 기본값은 5(초)입니다.

   ```
   ::> statistics top client show -node FsxId01234567890abcdef-01 [-interval [5,300]]
   ```

   출력에서 최상위 클라이언트는 IP 주소 및 포트별로 표시됩니다.

   ```
                                                    *Total     Total
              Client   Vserver          Node           Ops     (Bps)
   ------------------ --------- ------------------------ ------ ---------
    172.17.236.53:938 svm01     FsxId01234567890abcdef-01   2143 140443648
   172.17.236.160:898 svm02     FsxId01234567890abcdef-01    812  53215232
   ```

클라이언트 재탑재

- 클라이언트를 다른 HA 페어로 리밸런싱할 수 있습니다. 이렇게 하려면 클라이언트에서 볼륨을 탑재재 해제하고 SVM의 NFS/SMB 엔드포인트의 DNS 이름을 사용하여 다시 탑재재합니다. 그러면 무작위 HA 페어에 해당하는 무작위 엔드포인트가 반환됩니다.

  DNS 이름을 재사용하는 것이 좋지만 지정된 클라이언트 탑재재에 대해 명시적으로 HA 페어를 선택할 수 있는 옵션이 있습니다. 클라이언트를 다른 엔드포인트에 탑재하고 있는지 확인하기 위해 트래픽이 많은 파일 서버에 해당하는 것과 다른 엔드포인트 IP 주소를 대신 지정할 수 있습니다. 다음 명령을 실행하면 됩니다.

  ```
  ::> network interface show -vserver svm_name -lif nfs_smb_management* -fields
   address,curr-node
  vserver   lif                  address      curr-node
  --------- -------------------- ------------ -------------------------
  svm01 nfs_smb_management_1 172.31.15.89 FsxId01234567890abcdef-01
  svm01 nfs_smb_management_3 172.31.8.112 FsxId01234567890abcdef-03
  2 entries were displayed.
  ```

  `statistics top client show` 명령의 예제 출력에 따르면 클라이언트 `172.17.236.53`는 `FsxId01234567890abcdef-01`로 높은 트래픽을 유도하고 있습니다. `network interface show` 명령의 출력은 이 주소 `172.31.15.89`임을 나타냅니다. 다른 엔드포인트에 탑재하려면 다른 주소를 선택합니다(이 예제에서는 `FsxId01234567890abcdef-03`에 해당하는 유일한 다른 주소는 `172.31.8.112`입니다).

볼륨 재조정

볼륨 또는 집계에 I/O 불균형이 발생하는 경우 볼륨을 재조정하여 볼륨 전체에 I/O 트래픽을 재분배할 수 있습니다.

> **Note**
>
> 집계에 스토리지 사용률 불균형이 발생하는 경우 높은 사용률이 I/O 불균형과 결합되지 않는 한 일반적으로 성능에 영향을 주지 않습니다. 스토리지 사용률의 균형을 맞추기 위해 집계 간에 볼륨을 이동할 수 있지만 성능에 영향을 미치는 경우에만 볼륨을 이동하는 것이 좋습니다. 이동 볼륨은 이동을 고려 중인 각 볼륨에 I/O를 구동하지 않으면 성능에 부정적인 영향을 미칠 수 있습니다.

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 통계 볼륨 show ONTAP CLI 명령을 사용하여 다음과 같은 변경 사항과 함께 지정된 집계의 최고 트래픽 볼륨을 확인합니다.

   - *aggregate_name*을 aggregate의 이름으로 바꿉니다(예: aggr1).
   - 선택적으로 -interval 파라미터를 추가하여 각 보고서가 출력되기 전에 측정할 간격(초)을 제공할 수 있습니다. 간격을 늘리면(예: 최대 300초) 각 볼륨으로 구동되는 트래픽 양에 대한 장기 샘플이 제공됩니다. 기본값은 5(초)입니다.

```
::> statistics volume show -aggregate aggregate_name -sort-key total_ops [-interval
 [5,300]]
```

   선택한 간격에 따라 데이터를 표시하는 데 최대 5분이 걸릴 수 있습니다. 명령은 각 집계로 구동되는 트래픽 양과 함께 집계의 모든 볼륨을 표시합니다.

```
                           *Total Read Write Other      Read Write Latency
    Volume Vserver Aggregate    Ops  Ops   Ops   Ops     (Bps) (Bps)    (us)
---------- ------- --------- ------ ---- ----- ----- --------- ----- -------
vol1__0007    svm1     aggr1   4078 4078     0     0 267255808     0    1092
vol1__0005    svm1     aggr1   4078 4078     0     0 267255808     0    1086
vol1__0003    svm1     aggr1   4077 4077     0     0 267223040     0    1086
vol1__0001    svm1     aggr1   4077 4077     0     0 267239424     0    1087
vol1__0008    svm1     aggr2   2314 2314     0     0 151650304     0    1112
vol1__0006    svm1     aggr2   2144 2144     0     0 140509184     0    1104
vol1__0002    svm1     aggr2   2183 2183     0     0 143065088     0    1106
vol1__0004    svm1     aggr2   2183 2183     0     0 143065088     0    1103
```

   볼륨 통계는 구성 요소별로 표시됩니다(예: vol1__0015는 FlexGroup vol1의 15번째 구성 요소). 예시 출력에서 aggr1의 구성 요소가 aggr2의 구성 요소보다 활용도가 높다는 것을 알 수 있습니다. 집계 간 트래픽의 균형을 맞추기 위해 트래픽이 더 균등하게 분산되도록 구성 볼륨을 집계 간에 이동할 수 있습니다.

3. 새 HA 페어를 추가한 경우 기존 볼륨을 새 집계로 이동해야 합니다. 자세한 내용은 집계 간 볼륨 이동 단원을 참조하십시오.

NVMe 캐시 관리

NVMe 캐시는 2세대 파일 시스템에서 기본적으로 활성화됩니다. 2세대 파일 시스템에 처리량이 많은 워크로드가 있는 경우 NVMe 캐시를 비활성화하여 성능을 개선할 수 있습니다. 다음 절차에서는 파일 시스템의 NVMe 캐시를 활성화, 비활성화 및 검증하는 방법을 설명합니다.

NVMe 캐시를 관리하려면

1. SSH를 ONTAP 파일 시스템에 입력합니다. 자세한 내용은 the section called “NetApp ONTAP CLI 사용” 단원을 참조하십시오.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. system node external-cache modify ONTAP CLI 명령을 사용합니다. NVMe 캐시를 활성화하려면 **true**를 선택하고 비활성화하려면 **false**를 선택합니다.

   ```
   ::> system node external-cache modify -node * -is-enabled [true|false]
   ```

3. system node external-cache show ONTAP CLI 명령을 사용하여 NVMe 캐시가 활성화 또는 비활성화되었는지 확인합니다.

   ```
   ::> system node external-cache show -node * -fields is-enabled
   ```

NVMe 캐시는 노드별로 활성화 또는 비활성화됩니다. 파일 시스템에 새 고가용성(HA) 페어를 추가하면 각 새 노드의 기본 동작은 새 파일 시스템 노드와 동일합니다. 따라서 기존 노드에 비활성화되어 있더라도 파일 시스템의 새 노드에 대해 NVMe 캐시가 활성화됩니다. 자세한 내용은 고가용성(HA) 페어 추가 단원을 참조하십시오.

파일 시스템 세부 정보 모니터링

Amazon FSx 콘솔, 및 API AWS CLI와 지원되는SDK를 사용하여 FSx for ONTAP 파일 시스템에 대한 자세한 구성 정보를 볼 수 있습니다. AWS SDKs

자세한 파일 시스템 정보를 보려면:

- 콘솔 사용 - 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 봅니다. 요약 패널에는 파일 시스템의 ID, 수명 주기 상태, 배포 유형, SSD 스토리지 용량, 처리량 용량, 프로비저닝된 IOPS, 가용 영역, 생성 시간이 표시됩니다.

다음 탭은 수정할 수 있는 속성에 대한 자세한 구성 정보와 편집을 제공합니다.

- 네트워크 및 보안
- 모니터링 및 성능 - 생성한 CloudWatch 경보와 다음 범주에 대한 지표 및 경고를 표시합니다.
  - 요약 - 파일 시스템 활동 지표에 대한 상위 수준 요약
  - 파일 시스템 스토리지 용량
  - 파일 서버 및 디스크 성능

  자세한 내용은 Amazon CloudWatch를 사용한 모니터링 단원을 참조하십시오.
- 관리 - 다음 파일 시스템 관리 정보를 표시합니다.
  - 파일 시스템 관리 및 클러스터 간 엔드포인트의 DNS 이름과 IP 주소입니다.
  - ONTAP 관리자 사용자 아이디입니다.
  - ONTAP 관리자 암호를 업데이트하는 옵션입니다.
- 파일 시스템의 SVMs 목록
- 파일 시스템의 볼륨 목록
- 백업 설정 - 파일 시스템의 자동 일일 백업 설정을 변경합니다.
- 업데이트 - 파일 시스템 구성에 대한 사용자 시작 업데이트의 상태를 표시합니다.
- 태그 - Key:Value 페어 태그를 보고, 편집하고, 추가하고, 제거합니다.

- CLI 또는 API 사용 - describe-file-systems CLI 명령 또는 DescribeFileSystems API 작업을 사용합니다.

FSx for ONTAP 파일 시스템 상태

Amazon FSx 콘솔, AWS CLI 명령 describe-file-systems 또는 API 작업 DescribeFileSystems를 사용하여 Amazon FSx 파일 시스템의 상태를 볼 수 있습니다.

파일 시스템 상태	설명
사용 가능	파일 시스템이 성공적으로 생성되어 사용할 수 있습니다.
생성 중	Amazon FSx가 새 파일 시스템을 생성하고 있습니다.

파일 시스템 상태	설명
삭제 중	Amazon FSx가 기존 파일 시스템을 삭제하고 있습니다.
잘못 구성됨	파일 시스템이 잘못 구성되었지만 복구 가능한 상태입니다.
실패함	1. 파일 시스템에 오류가 발생하여 Amazon FSx가 복구할 수 없습니다. 2. 새 파일 시스템을 생성할 때 Amazon FSx가 새 파일 시스템을 생성하지 못했습니다.

파일 시스템 삭제

Amazon FSx 콘솔, AWS CLI및 Amazon FSx API 및 SDK를 사용하여 FSx for ONTAP 파일 시스템을 삭제할 수 있습니다. SDKs

파일 시스템을 삭제하려면 다음을 수행합니다.

- 콘솔 사용 - 리소스 정리에 설명된 절차를 따릅니다.
- CLI 또는 API 사용 - 먼저 파일 시스템에서 모든 볼륨과 SVM을 삭제합니다. 그런 다음 delete-file-system CLI 명령 또는 DeleteFileSystem API 작업을 사용합니다.

FSx for ONTAP 스토리지 가상 머신 관리

FSx for ONTAP에서 볼륨은 스토리지 가상 머신(SVM)이라는 가상 파일 서버에서 호스팅됩니다. SVM은 데이터 관리 및 액세스를 위한 자체 관리자 보안 인증과 엔드포인트가 있는 격리형 파일 서버입니다. FSx for ONTAP의 데이터에 액세스하면 클라이언트와 워크스테이션이 SVM의 엔드포인트(IP 주소)를 사용하여 SVM에서 호스팅하는 볼륨, SMB 공유 또는 iSCSI LUN을 마운트합니다.

Amazon FSx는 AWS Management Console을 사용하여 파일 시스템을 생성할 때 파일 시스템에 기본 SVM을 자동으로 생성합니다. 콘솔 AWS CLI또는 Amazon FSx API 및 SDK를 사용하여 언제든지 파일 시스템에 추가 SVMs을 생성할 수 있습니다. SDKs ONTAP CLI 또는 REST API를 사용하여 SVM을 생성할 수 없습니다.

파일 액세스 인증 및 권한 부여를 위해 SVM을 Microsoft Active Directory에 조인할 수 있습니다. 자세한 내용은 FSx for ONTAP에서 Microsoft Active Directory 작업 섹션을 참조하세요.

파일 시스템당 최대 SVM 수

다음 표에는 파일 시스템에 생성할 수 있는 최대 SVM 수가 나와 있습니다. 최대 SVM 수는 프로비저닝된 처리량 용량(MBps)에 따라 달라집니다.

고가용성(HA) 페어	처리량 용량(MBps)	파일 시스템당 최대 SVM 수
HA 페어 1개	128	6
	256	6
	384	6
	512	14
	768	14
	1,024	14
	1,536	14
	2,048	24
	3,072	14
	4,096	24
	6,144	24
HA 페어 2~12개	임의	5

주제

- 스토리지 가상 머신 생성(SVM)
- 스토리지 가상 머신(SVM) 업데이트
- 파일 액세스 감사
- 작업 그룹에서 SMB 서버 설정

- 스토리지 가상 머신(SVM) 구성 세부 정보 모니터링
- 스토리지 가상 머신 삭제(SVM)

스토리지 가상 머신 생성(SVM)

AWS Management Console AWS CLI및 API를 사용하여 FSx for ONTAP SVM을 생성할 수 있습니다.

파일 시스템에 대해 생성할 수 있는 최대 SVM 수는 파일 시스템의 배포 유형과 프로비저닝된 처리량 용량에 따라 달라집니다. 자세한 내용은 파일 시스템당 최대 SVM 수 단원을 참조하십시오.

SVM 속성

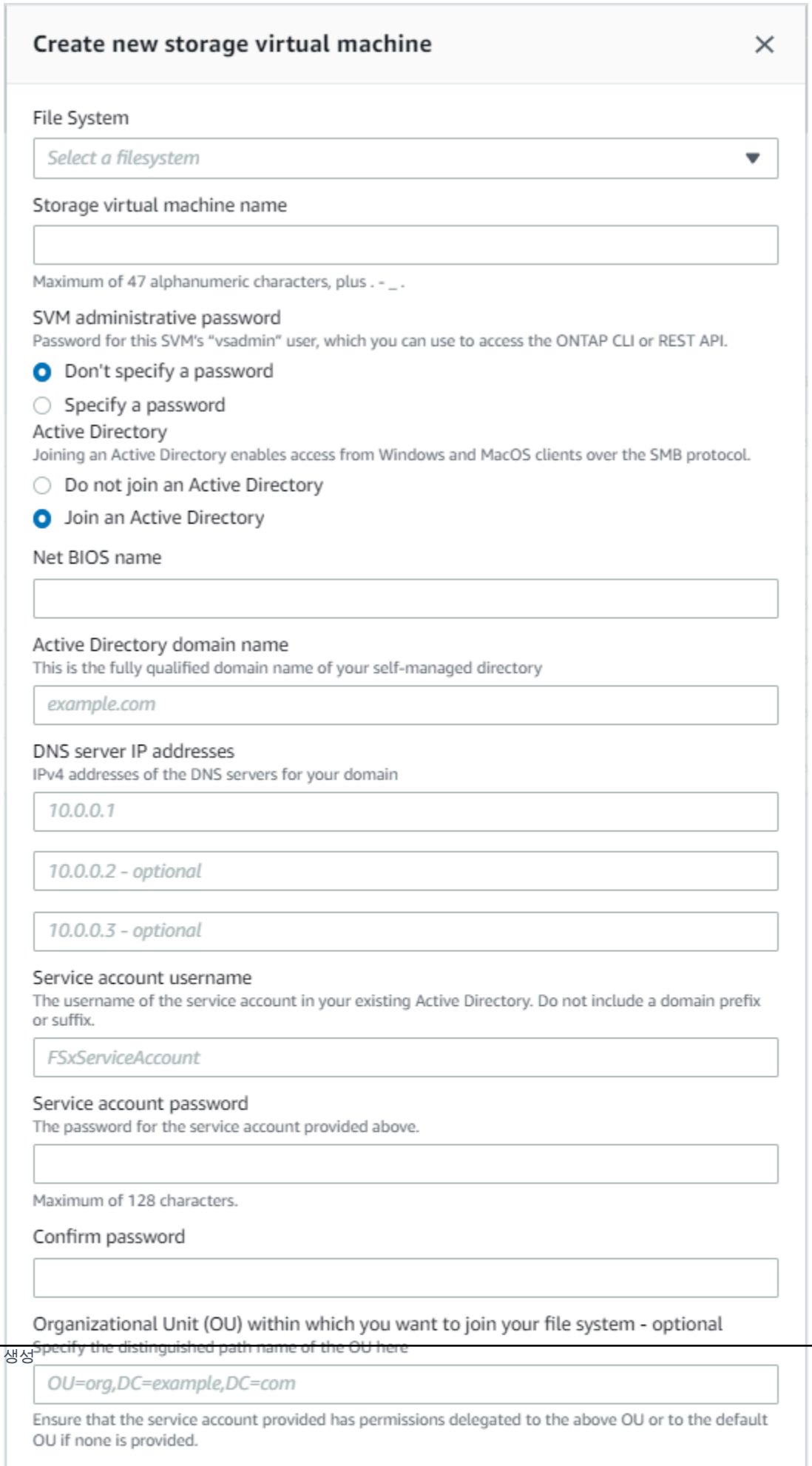
SVM을 생성할 때 다음 속성을 정의합니다.

- SVM이 속한 FSx for ONTAP 파일 시스템.
- Microsoft Active Directory(AD) 구성 — 선택적으로 SVM을 자체 관리형 AD에 조인하여 Windows 및 MacOS 클라이언트의 인증 및 액세스 제어를 수행할 수 있습니다. 자세한 내용은 FSx for ONTAP에서 Microsoft Active Directory 작업 단원을 참조하십시오.
- 루트 볼륨 보안 스타일 - SVM 내의 데이터에 액세스하는 데 사용하는 클라이언트 유형에 맞게 루트 볼륨 보안 스타일(Unix 또는 NTFS)을 설정합니다. 자세한 내용은 볼륨 보안 스타일 단원을 참조하십시오.
- SVM 관리자 암호 – 선택적으로 SVM `vsadmin` 사용자의 암호를 설정할 수 있습니다. 자세한 내용은 ONTAP CLI로 SVM 관리하기 섹션을 참조하세요.

스토리지 가상 머신 생성(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 스토리지 가상 머신을 선택합니다.
3. 새 스토리지 가상 머신 생성을 선택합니다.

   새 스토리지 가상 머신 생성 대화 상자가 표시됩니다.


Create new storage virtual machine
File System
Select a filesystem
Storage virtual machine name
Maximum of 47 alphanumeric characters, plus . - _ .
SVM administrative password
Password for this SVM's "vsadmin" user, which you can use to access the ONTAP CLI or REST API.
Don't specify a password
Specify a password
Active Directory
Joining an Active Directory enables access from Windows and MacOS clients over the SMB protocol.
Do not join an Active Directory
Join an Active Directory
Net BIOS name
Active Directory domain name
This is the fully qualified domain name of your self-managed directory
example.com
DNS server IP addresses
IPv4 addresses of the DNS servers for your domain
10.0.0.1
10.0.0.2 - optional
10.0.0.3 - optional
Service account username
The username of the service account in your existing Active Directory. Do not include a domain prefix or suffix.
FSxServiceAccount
Service account password
The password for the service account provided above.
Maximum of 128 characters.
Confirm password
Organizational Unit (OU) within which you want to join your file system - optional
Specify the distinguished path name of the OU here
OU=org,DC=example,DC=com
Ensure that the service account provided has permissions delegated to the above OU or to the default OU if none is provided.

4. 파일 시스템에서, 스토리지 가상 머신을 생성할 파일 시스템을 선택합니다.
5. 스토리지 가상 머신 이름 필드에 스토리지 가상 머신의 이름을 입력합니다. 밑줄(_) 특수 문자를 포함해 최대 47자의 영숫자를 사용할 수 있습니다.
6. SVM 관리자 암호의 경우 선택적으로 암호 지정을 선택하고 이 SVM의 `vsadmin` 사용자의 암호를 입력할 수 있습니다. `vsadmin` 사용자를 사용하여 ONTAP CLI 또는 REST API를 사용해 SVM을 관리할 수 있습니다. `vsadmin` 사용자에 대한 자세한 내용은 ONTAP CLI로 SVM 관리하기 섹션을 참조하세요.

   암호 지정 안 함(기본값)을 선택한 경우에도 파일 시스템의 `fsxadmin` 사용자를 사용하여 ONTAP CLI 또는 REST API를 사용해 파일 시스템을 관리할 수 있지만 SVM의 `vsadmin` 사용자를 사용하여 동일한 작업을 수행할 수는 없습니다.
7. Active Directory의 경우 다음과 같은 옵션을 사용할 수 있습니다.

   - 파일 시스템을 Active Directory(AD)에 조인하지 않을 경우 Active Directory에 조인 안 함을 선택합니다.
   - SVM을 자체 관리형 AD 도메인에 조인하려면 Active Directory 조인을 선택하고 AD에 대해 다음과 같은 세부 정보를 입력합니다. 자세한 내용은 SVM을 자체 관리형 Microsoft Active Directory에 조인하기 위한 사전 조건 섹션을 참조하세요.
     - SVM에 대해 생성할 Active Directory 컴퓨터 객체의 NetBIOS 이름. NetBIOS 이름은 15자를 초과할 수 없습니다. Active Directory에서 이 SVM의 이름입니다.
     - Active Directory의 정규화된 도메인 이름(FQDN). FQDN은 255자를 초과할 수 없습니다.
     - DNS 서버 IP 주소 - 도메인의 DNS 서버의 IPv4 주소입니다.
     - 서비스 계정 사용자 이름 - 기존 Active Directory에 있는 서비스 계정의 사용자 이름입니다. 도메인 접두사나 접미사를 포함하지 않습니다. `EXAMPLE\ADMIN`의 경우 `ADMIN`을 사용합니다.
     - 서비스 계정 암호 - 서비스 계정의 암호입니다.
     - 암호 확인 - 서비스 계정의 암호입니다.
     - (선택 사항) 조직 단위(OU) – 파일 시스템에 조인하려는 조직 단위의 고유 경로 이름입니다.
     - 위임된 파일 시스템 관리자 그룹 - AD에서 파일 시스템을 관리할 수 있는 그룹의 이름입니다.

       를 사용하는 경우 AWS 위임된 FSx 관리자 AWS Managed Microsoft AD, AWS 위임된 관리자 또는 OU에 위임된 권한이 있는 사용자 지정 그룹과 같은 그룹을 지정해야 합니다.

       자체 관리형 AD에 조인하는 경우 AD에 있는 그룹의 이름을 사용합니다. 기본 그룹은 `Domain Admins`입니다.

8. SVM 루트 볼륨 보안 스타일의 경우 데이터에 액세스하는 클라이언트 유형에 따라 SVM의 보안 스타일을 선택합니다. 주로 Linux 클라이언트를 사용하여 데이터에 액세스하는 경우 Unix(Linux)를 선택하고, 주로 Windows 클라이언트를 사용하여 데이터에 액세스하는 경우 NTFS를 선택합니다. 자세한 내용은 볼륨 보안 스타일 섹션을 참조하세요.
9. 확인을 선택하여 스토리지 가상 머신을 생성합니다.

스토리지 가상 머신 창의 상태 열에 있는 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다. 상태가 생성됨이면 스토리지 가상 머신을 사용할 준비가 된 것입니다.

스토리지 가상 머신 생성(CLI)

- FSx for ONTAP 스토리지 가상 머신(SVM)을 생성하려면 다음 예제와 같이 create-storage-virtual-machine CLI 명령(또는 이에 상응하는 CreateStorageVirtualMachine API 작업)을 사용합니다.

```
aws fsx create-storage-virtual-machine \
    --file-system-id fs-0123456789abcdef0 \
    --name svm1 \
    --svm-admin-password password \
    --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAd
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

스토리지 가상 머신을 생성한 후 Amazon FSx는 다음 예제와 같이 JSON 형식으로 설명을 반환합니다.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
```

```
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
  }
}
```

스토리지 가상 머신(SVM) 업데이트

Amazon FSx 콘솔 AWS CLI및 Amazon FSx FSx API를 사용하여 다음 스토리지 가상 머신(SVM) 구성 속성을 업데이트할 수 있습니다.

- SVM 관리자 계정 암호.
- SVM Active Directory(AD) 구성 - SVM을 AD에 조인하거나, 이미 AD에 조인한 SVM의 AD 구성을 수정할 수 있습니다. 자세한 내용은 SVM Active Directory 구성 관리 섹션을 참조하세요.

SVM 관리자 계정 보안 인증 업데이트(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 다음과 같이 업데이트할 SVM을 선택합니다.
   - 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 SVM을 업데이트할 ONTAP 파일 시스템을 선택합니다.
   - 스토리지 가상 머신 탭을 선택합니다.

     또는
   - 현재의 AWS 계정 에서 사용할 수 있는 모든 SVMs 목록을 표시하려면 ONTAP을 AWS 리전확장하고 스토리지 가상 머신을 선택합니다.
3. 업데이트할 스토리지 가상 머신을 선택합니다.
4. 작업 > 관리자 암호 업데이트를 선택합니다. SVM 관리자 보안 인증 업데이트 창이 표시됩니다.
5. `vsadmin` 사용자의 새 암호를 입력하고 확인합니다.
6. 보안 인증 업데이트를 선택하여 새 암호를 저장합니다.

SVM 관리자 계정 보안 인증 업데이트(CLI)

- FSx for ONTAP SVM의 구성을 업데이트하려면 다음 예제와 같이 update-storage-virtual machine CLI 명령(또는 이에 상응하는 UpdateStorageVirtualMachine API 작업)을 사용합니다.

```
aws fsx update-storage-virtual-machine \
--storage-virtual-machine-id svm-abcdef01234567890 \
--svm-admin-password new-svm-password \
```

스토리지 가상 머신을 생성한 후 Amazon FSx는 다음 예제와 같이 JSON 형식으로 설명을 반환합니다.

```
{
  "StorageVirtualMachine": {
    "CreationTime": 1625066825.306,
    "Endpoints": {
```

```
      "Management": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef01234567890.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATING",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef01234567890",
    "StorageVirtualMachineId": "svm-abcdef01234567890",
    "Subtype": "default",
    "Tags": [],
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
```

```
  }
}
```

파일 액세스 감사

Amazon FSx for NetApp ONTAP은 스토리지 가상 머신(SVM)의 파일 및 디렉터리에 대한 최종 사용자 액세스 감사를 지원합니다.

주제

- 파일 액세스 감사 개요
- 파일 액세스 감사 설정 작업 개요

파일 액세스 감사 개요

파일 액세스 감사를 사용하면 정의한 감사 정책을 기반으로 개별 파일 및 디렉터리에 대한 최종 사용자 액세스를 기록할 수 있습니다. 파일 액세스 감사는 시스템 보안을 개선하고 시스템 데이터에 대한 무단 액세스 위험을 줄이는 데 도움이 될 수 있습니다. 파일 액세스 감사를 통해 조직은 데이터 보호 요구 사항을 지속적으로 준수하고 잠재적 위협을 조기에 식별하며 데이터 침해 위험을 줄일 수 있습니다.

Amazon FSx는 파일 및 디렉터리 액세스에서 성공한 시도(예: 충분한 권한을 가진 사용자가 파일에 성공적으로 액세스하는 경우), 실패한 시도 또는 두 가지 모두에 대한 로깅을 지원합니다. 파일 액세스 감사를 언제든지 비활성화할 수도 있습니다.

기본적으로 감사 이벤트 로그는 Microsoft Event Viewer를 사용하여 볼 수 있는 EVTX 파일 형식으로 저장됩니다.

감사할 수 있는 SMB 액세스 이벤트

다음 표에는 감사할 수 있는 SMB 파일 및 폴더 액세스 이벤트가 나열되어 있습니다.

이벤트 ID(EVT/EVTX)	이벤트	설명	범주
560/4656	객체 열기/객체 생성	OBJECT ACCESS: 객체(파일 또는 디렉터리) 열기	파일 액세스
563/4659	삭제할 의도로 객체 열기	OBJECT ACCESS: 삭제할 의도로 객체(파일	파일 액세스

이벤트 ID(EVT/EVTX)	이벤트	설명	범주
		또는 디렉터리)에 대한 처리가 요청됨	
564/4660	객체 삭제	OBJECT ACCESS: 객체(파일 또는 디렉터리) 삭제 ONTAP은 Windows 클라이언트가 객체(파일 또는 디렉터리)를 삭제하려고 시도할 때 이 이벤트를 생성함	파일 액세스

이벤트 ID(EVT/EVTX)	이벤트	설명	범주
567/4663	객체 읽기/객체 쓰기/객체 속성 가져오기/객체 속성 설정	OBJECT ACCESS: 객체 액세스 시도(읽기, 쓰기, 속성 가져오기, 속성 설정) Note 이 이벤트의 경우 ONTAP은 객체에 대한 첫 번째 SMB 읽기 및 첫 번째 SMB 쓰기 작업(성공 또는 실패)만 감사합니다. 이를 통해 단일 클라이언트가 객체를 열고 동일한 객체에 대해 여러 번 연속적으로 읽기 또는 쓰기 작업을 수행할 때 ONTAP에서 과도한 로그 항목이 생성되는 것을 방지할 수 있습니다.	파일 액세스

이벤트 ID(EVT/EVTX)	이벤트	설명	범주
해당 사항 없음/4664	하드 링크	OBJECT ACCESS: 하드 링크를 생성하려고 시도함	파일 액세스
해당 사항 없음/해당 사항 없음 ONTAP 이벤트 ID 9999	객체 이름 변경	OBJECT ACCESS: 객체 이름이 변경되었습니다. 이는 ONTAP 이벤트입니다. 현재 Windows에서는 단일 이벤트로 지원되지 않습니다.	파일 액세스
해당 사항 없음/해당 사항 없음 ONTAP 이벤트 ID 9998	객체 연결 해제	OBJECT ACCESS: 객체 연결이 해제되었습니다. 이는 ONTAP 이벤트입니다. 현재 Windows에서는 단일 이벤트로 지원되지 않습니다.	파일 액세스

감사할 수 있는 NFS 액세스 이벤트

다음의 NFS 파일 및 폴더 액세스 이벤트를 감사할 수 있습니다.

- READ
- OPEN
- CLOSE
- READDIR
- WRITE
- SETATTR
- CREATE
- LINK
- OPENATTR

- REMOVE
- GETATTR
- VERIFY
- NVERIFY
- RENAME

파일 액세스 감사 설정 작업 개요

파일 액세스 감사를 위해 FSx for ONTAP을 설정하려면 다음과 같은 고급 작업이 필요합니다.

1. 파일 액세스 감사 요구 사항 및 고려 사항을 숙지합니다.
2. 특정 SVM에 감사 구성을 생성합니다.
3. 해당 SVM에서 감사를 활성화합니다.
4. 파일 및 디렉터리에 감사 정책을 구성합니다.
5. FSx for ONTAP에서 감사 이벤트 로그를 내보낸 후 감사 이벤트 로그를 확인합니다.

작업 세부 정보는 다음 절차에 나와 있습니다.

파일 액세스 감사를 활성화하려는 파일 시스템의 다른 SVM에 대해 작업을 반복합니다.

감사 요구 사항

SVM에서 감사를 구성 및 활성화하려면 먼저 다음 요구 사항 및 고려 사항을 이해해야 합니다.

- NFS 감사는 u 유형으로 지정된 액세스 제어 항목(ACE) 감사를 지원하며, 이는 객체에 대한 액세스를 시도할 때 감사 로그 항목을 생성합니다. NFS 감사의 경우 모드 비트와 감사 ACE 간에 매핑이 없습니다. ACL을 모드 비트로 변환할 때 감사 ACE는 건너뛰게 됩니다. 모드 비트를 ACL을 변환할 때 감사 ACE는 생성되지 않습니다.
- 감사는 스테이징 볼륨에 사용 가능한 공간이 있는지에 따라 달라집니다. (스테이징 볼륨은 EVTX 또는 XML 파일 형식으로 변환하기 전에 감사 기록이 저장되는 개별 노드의 중간 바이너리 파일인 스테이징 파일을 저장하기 위해 ONTAP에서 만든 전용 볼륨입니다.) 감사된 볼륨이 포함된 집계에 스테이징 볼륨을 위한 충분한 공간이 있는지 확인해야 합니다.
- 감사는 변환된 감사 이벤트 로그가 저장되는 디렉터리가 포함된 볼륨에 사용 가능한 공간이 있는지에 따라 달라집니다. 이벤트 로그를 저장하는 데 사용되는 볼륨에 충분한 공간이 있는지 확인해야 합니다. 감사 구성을 만들 때 `-rotate-limit` 파라미터를 사용하여 감사 디렉터리에 유지할 감사 로

그 수를 지정할 수 있으며, 이를 통해 볼륨에 감사 로그에 사용할 수 있는 공간이 충분하도록 할 수 있습니다.

SVM에 감사 구성 생성

파일 및 디렉터리 이벤트 감사를 시작하려면 먼저 스토리지 가상 머신(SVM)에 감사 구성을 생성해야 합니다. 감사 구성을 생성한 후에는 SVM에서 활성화해야 합니다.

`vserver audit create` 명령을 사용하여 감사 구성을 생성하기 전에 로그 대상으로 사용할 디렉터리를 생성하고 디렉터리에 심볼 링크가 없는지 확인합니다. `-destination` 파라미터를 사용하여 대상 디렉터리를 지정합니다.

다음과 같이 로그 크기나 일정에 따라 감사 로그를 로테이션시키는 감사 구성을 만들 수 있습니다.

- 로그 크기에 따라 감사 로그를 로테이션하려면 다음 명령을 사용합니다.

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}] [-
rotate-limit integer] [-rotate-size {integer[KB|MB|GB|TB|PB]}]
```

다음 예제에서는 크기 기반 로테이션을 통해 파일 작업과 CIFS(SMB) 로그온 및 로그오프 이벤트(기본값)를 감사하는 `svm1`이라는 SVM에 대한 감사 구성을 생성합니다. 로그 형식은 EVTX(기본값)이고 로그는 `/audit_log` 디렉터리에 저장되며 한 번에 하나의 로그 파일(최대 200MB의 크기)을 갖게 됩니다.

```
vserver audit create -vserver svm1 -destination /audit_log -rotate-size 200MB
```

- 일정에 따라 감사 로그를 로테이션하려면 다음 명령을 사용합니다.

```
vserver audit create -vserver svm_name -destination path [-format {xml|evtx}]
        [-rotate-limit integer] [-rotate-schedule-month chron_month]
        [-rotate-schedule-dayofweek chron_dayofweek] [-rotate-schedule-
day chron_dayofmonth]
        [-rotate-schedule-hour chron_hour] [-rotate-schedule-minute chron_minute]
```

시간 기반 감사 로그 로테이션을 구성하는 경우 `-rotate-schedule-minute` 파라미터가 필요합니다.

다음 예제에서는 시간 기반 로테이션을 통해 `svm2`라는 SVM에 대한 감사 구성을 생성합니다. 로그 형식은 EVTX(기본값)이며 감사 로그는 매월 모든 요일의 오후 12시 30분에 로테이션됩니다.

```
vserver audit create -vserver svm2 -destination /audit_log -rotate-size 200MB  -
rotate-schedule-month all -rotate-schedule-dayofweek all -rotate-schedule-hour 12 -
rotate-schedule-minute 30
```

`-format` 파라미터를 사용하여 감사 로그를 변환된 EVTX 형식(기본값)으로 생성할지 또는 XML 파일 형식으로 생성할지 지정할 수 있습니다. EVTX 형식을 사용하면 Microsoft 이벤트 뷰어로 로그 파일을 볼 수 있습니다.

기본적으로, 감사할 이벤트 범주는 파일 액세스 이벤트(SMB 및 NFS 모두), CIFS(SMB) 로그온 및 로그오프 이벤트, 권한 부여 정책 변경 이벤트입니다. 다음 형식의 `-events` 파라미터를 사용하여 로깅할 이벤트를 보다 잘 제어할 수 있습니다.

```
-events {file-ops|cifs-logon-logoff|cap-staging|file-share|audit-policy-change|user-
account|authorization-policy-change|security-group}
```

예를 들어 `-events file-share`를 사용하면 파일 공유 이벤트를 감사할 수 있습니다.

`vserver audit create` 명령에 대한 자세한 내용은 감사 구성 생성을 참조하세요.

SVM에서 감사 활성화

감사 구성을 설정한 후에는 SVM에서 감사를 활성화해야 합니다. 이렇게 하려면 다음 명령을 사용합니다.

```
vserver audit enable -vserver svm_name
```

예를 들어, 다음 명령을 사용하여 `svm1`이라는 SVM에 대한 감사를 활성화합니다.

```
vserver audit enable -vserver svm1
```

액세스 감사는 언제든지 비활성화할 수 있습니다. 예를 들어, 다음 명령을 사용하여 `svm4`라는 SVM에 대한 감사를 비활성화합니다.

```
vserver audit disable -vserver svm4
```

감사를 비활성화했을 때 SVM에서 감사 구성이 삭제되지는 않으므로 언제든지 해당 SVM에서 감사를 재활성화할 수 있습니다.

파일 및 폴더 감사 정책 구성

사용자 액세스 시도에 대해 감사할 파일 및 폴더에 감사 정책을 구성해야 합니다. 성공한 액세스 시도 및 실패한 액세스 시도 모두 모니터링하도록 감사 정책을 구성할 수 있습니다.

SMB 및 NFS 감사 정책을 모두 구성할 수 있습니다. SMB 및 NFS 감사 정책은 볼륨의 보안 스타일에 따라 구성 요구 사항과 감사 기능이 다릅니다.

NTFS 보안 스타일 파일 및 디렉터리에 대한 감사 정책

Windows 보안 탭 또는 ONTAP CLI를 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

NTFS 감사 정책 구성(Windows 보안 탭)

NTFS 보안 설명자와 연결된 NTFS SACL에 항목을 추가하여 NTFS 감사 정책을 구성합니다. 그러면 보안 설명자가 NTFS 파일 및 디렉터리에 적용됩니다. 이러한 작업은 Windows GUI에서 자동으로 처리됩니다. 보안 설명자에는 파일 및 폴더 액세스 권한을 적용하기 위한 임의 액세스 제어 목록(DACL), 파일 및 폴더 감사를 위한 SACL 또는 SACL과 DACL 모두를 포함할 수 있습니다.

1. Windows 탐색기의 도구 메뉴에서 네트워크 드라이브 연결을 선택합니다.
2. 네트워크 드라이브 연결 상자에서 다음 작업을 수행합니다.
   a. 드라이브 문자를 선택합니다.
   b. 폴더 상자에서, 감사할 데이터가 있는 공유가 포함된 SMB(CIFS) 서버 이름 및 공유 이름을 입력합니다.
   c. 마침을 클릭합니다.

   선택한 드라이브가 마운트되고 바로 사용할 수 있으며 Windows 탐색기 창에 공유에 포함된 파일 및 폴더가 표시됩니다.
3. 감사 액세스를 활성화할 파일 또는 디렉터리를 선택합니다.
4. 파일 또는 디렉터리를 마우스 오른쪽 버튼으로 클릭하고 속성을 선택합니다.
5. 보안 탭을 선택합니다.
6. 고급을 클릭합니다.
7. 감사 탭을 선택합니다.
8. 원하는 작업을 수행합니다.

다음을 수행하려는 경우	수행 방법
새 사용자 또는 그룹에 대한 감사 설정	1. 추가를 선택합니다. 2. 선택할 객체 이름 입력 상자에서, 추가하려는 사용자 또는 그룹의 이름을 입력합니다. 3. 확인을 선택합니다.
사용자 또는 그룹에서 감사 제거	1. 선택할 객체 이름 입력 상자에서, 제거하려는 사용자 또는 그룹을 선택합니다. 2. 제거를 선택합니다. 3. 확인을 선택합니다. 4. 이 절차의 나머지 단계는 건너뜁니다.
사용자 또는 그룹에 대한 감사 변경	1. 선택할 객체 이름 입력 상자에서, 변경하려는 사용자 또는 그룹을 선택합니다. 2. 편집을 선택합니다. 3. 확인을 선택합니다.

사용자 또는 그룹에 대한 감사를 설정하거나 기존 사용자 또는 그룹에 대한 감사를 변경하는 경우 **##**에 대한 감사 항목 상자가 열립니다.

9. 적용 대상 상자에서, 이 감사 항목을 적용할 방법을 선택합니다.

   단일 파일에 감사를 설정하는 경우 이 객체로만 기본 설정되기 때문에 적용 대상 상자가 활성화되지 않습니다.

10. 액세스 상자에서, 감사할 대상 및 성공한 이벤트, 실패한 이벤트 또는 둘 다를 감사할지 여부를 선택합니다.

    - 성공한 이벤트를 감사하려면 성공 상자를 선택합니다.
    - 실패한 이벤트를 감사하려면 실패 상자를 선택합니다.

    보안 요구 사항을 충족하기 위해 모니터링해야 하는 작업을 선택합니다. 이러한 감사 가능 이벤트에 대한 자세한 내용은 Windows 설명서를 참조하세요. 다음 이벤트를 감사할 수 있습니다.

- 전체 제어
- 폴더 트래버스/파일 실행
- 폴더 나열/데이터 읽기
- 속성 읽기
- 확장 속성 읽기
- 파일 생성/데이터 쓰기
- 폴더 생성/데이터 추가
- 속성 쓰기
- 확장 속성 쓰기
- 하위 폴더 및 파일 삭제
- 삭제
- 권한 읽기
- 권한 변경
- 소유권 취득

11. 감사 설정이 원본 컨테이너의 후속 파일 및 폴더에 전파되지 않도록 하려면 이 감사 항목을 이 컨테이너 내의 객체 및/또는 컨테이너에만 적용 상자를 선택합니다.
12. 적용을 선택합니다.
13. 감사 항목을 추가, 제거, 편집한 후 확인을 선택합니다.

    ##에 대한 감사 항목 상자가 닫힙니다.
14. 감사 상자에서 이 폴더의 상속 설정을 선택합니다. 보안 요구 사항을 충족하는 감사 이벤트를 제공하는 최소 수준만 선택합니다.

    다음 중 하나를 선택할 수 있습니다.

    - 이 객체의 부모로부터 상속 가능한 감사 항목 포함 상자를 선택합니다.
    - 모든 하위 항목에 있는 기존의 상속 가능한 감사 항목을 모두 이 객체의 상속 가능한 감사 항목으로 바꾸기 상자를 선택합니다.
    - 두 상자를 모두 선택합니다.
    - 어느 상자도 선택하지 않습니다.

단일 파일에 SACL을 설정하는 경우 감사 상자에 모든 하위 항목에 있는 기존의 상속 가능한 감사 항목을 모두 이 객체의 상속 가능한 감사 항목으로 바꾸기 상자가 표시되지 않습니다.

15. 확인을 선택합니다.

NTFS 감사 정책 구성(ONTAP CLI)

ONTAP CLI를 사용하면 Windows 클라이언트의 SMB 공유를 사용하여 데이터에 연결할 필요 없이 NTFS 감사 정책을 구성할 수 있습니다.

- vserver 보안 파일 디렉터리 ntfs sacl add 명령 패밀리를 사용하여 NTFS 감사 정책을 구성할 수 있습니다.

예를 들어 다음 명령은 라는 SVM에 p1 대해 라는 보안 정책을 생성합니다vs0.

```
vserver security file-directory policy create -policy-name p1 -vserver vs0
```

그런 다음 다음 명령은 vs0 SVM에 p1 보안 정책을 적용합니다.

```
vserver security file-directory apply -vserver vs0 -policy-name p1
```

UNIX 보안 스타일 파일 및 디렉터리에 대한 감사 정책

NFS v4.x 액세스 제어 목록(ACL)에 감사 액세스 제어 표현식(ACE)을 추가하여 UNIX 보안 스타일 파일 및 디렉터리에 대한 감사를 구성합니다. 그러면 보안을 위해 특정 NFS 파일 및 디렉터리 액세스 이벤트를 모니터링할 수 있습니다.

> **Note**
>
> NFS v4.x의 경우 임의 및 시스템 ACE가 모두 동일한 ACL에 저장됩니다. 따라서 기존 ACL에 감사 ACE를 추가할 때는 기존 ACL이 덮어써져서 손실되지 않도록 주의해야 합니다. 기존 ACL에 감사 ACE를 추가하는 순서는 중요하지 않습니다.

UNIX 감사 정책 구성

1. nfs4_getfacl 또는 이에 상응하는 명령을 사용하여 파일 또는 디렉터리의 기존 ACL을 검색합니다.

2. 원하는 감사 ACE를 추가합니다.
3. `nfs4_setfacl` 또는 이에 상응하는 명령을 사용하여 파일 또는 디렉터리에 업데이트된 ACL을 적용합니다.

   이 예제에서는 `-a` 옵션을 사용하여 `testuser`라는 사용자에게 `file1`이라는 파일에 대한 읽기 권한을 부여합니다.

   ```
   nfs4_setfacl -a "A::testuser@example.com:R" file1
   ```

감사 이벤트 로그 보기

EVTX 또는 XML 파일 형식으로 저장된 감사 이벤트 로그를 볼 수 있습니다.

- EVTX 파일 형식 - Microsoft 이벤트 뷰어를 사용하여 변환된 EVTX 감사 이벤트 로그를 저장된 파일로 열 수 있습니다.

  이벤트 뷰어를 사용하여 이벤트 로그를 볼 때 사용할 수 있는 두 가지 옵션은 다음과 같습니다.
  - 일반 보기: 모든 이벤트에 공통적인 정보가 이벤트 레코드에 표시됩니다. 이벤트 레코드의 이벤트별 데이터는 표시되지 않습니다. 세부 보기를 사용하여 이벤트별 데이터를 표시할 수 있습니다.
  - 세부 보기: 친숙한 보기와 XML 보기를 사용할 수 있습니다. 친숙한 보기와 XML 보기에는 모든 이벤트에 공통적인 정보와 이벤트 레코드의 이벤트별 데이터가 모두 표시됩니다.
- XML 파일 형식 - XML 파일 형식을 지원하는 서드 파티 애플리케이션에서 XML 감사 이벤트 로그를 보고 처리할 수 있습니다. XML 스키마와, XML 필드 정의에 대한 정보가 있는 경우 XML 보기 도구를 사용하여 감사 로그를 볼 수 있습니다.

작업 그룹에서 SMB 서버 설정

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 SVM을 Microsoft Active Directory에 조인하는 대신 작업 그룹에서 서버 메시지 블록(SMB) 서버를 구성할 수 있습니다. 작업 그룹은 SMB 프로토콜을 사용하고 로컬 계정 및 그룹만 있는 peer-to-peer 네트워크입니다.

SMB 서버를 작업 그룹의 멤버로 설정하는 프로세스는 다음과 같이 구성됩니다.

- 스토리지 가상 머신(SVM)에서 SMB 서버 생성.
- 로컬 사용자 및 그룹 생성.
- 로컬 사용자 또는 그룹을 작업 그룹의 구성원으로 추가합니다.

작업 그룹 모드의 SMB 서버는 다음 SMB 기능을 지원하지 않습니다.

- SMB3 감시 프로토콜
- SMB3 CA 공유
- SQL over SMB
- 폴더 리디렉션
- 로밍 프로파일
- 그룹 정책 객체(GPO)
- 볼륨 스냅샷 서비스(VSS)

또한 작업 그룹 모드의 SMB 서버는 NTLM 인증만 지원하고 Kerberos 인증을 지원하지 않습니다.

다음 절차에서는 작업 그룹의 SVM에 SMB 서버를 설정하고, 로컬 계정을 생성하고, 이러한 계정을 작업 그룹 멤버십에 추가하는 프로세스를 안내합니다. 파일 시스템 또는 SVM 관리 인터페이스의 NetApp ONTAP CLI를 사용하여 이러한 절차를 구현합니다. 자세한 내용은 NetApp ONTAP CLI 사용 단원을 참조하십시오.

주제

- 작업 그룹에서 SMB 서버 생성
- SMB 서버에서 로컬 사용자 계정 생성
- SMB 서버에서 로컬 그룹 생성
- 로컬 그룹에 로컬 사용자 추가

작업 그룹에서 SMB 서버 생성

vserver cifs create ONTAP CLI 명령을 사용하여 SVM에서 SMB 서버를 생성하고 해당 서버가 속한 작업 그룹을 지정할 수 있습니다.

시작하기 전 준비 사항

데이터를 제공하는 데 사용하는 SVM 및 볼륨(및 인터페이스)은 SMB 프로토콜을 허용하도록 구성되어야 합니다.

LIFs는 SVM에 구성된 DNS 서버에 연결할 수 있어야 합니다. 파일 시스템에 CIFS 라이선스가 필요할 수 있지만 SMB 서버를 인증에만 사용할 경우에는 CIFS 라이선스가 필요하지 않습니다.

작업 그룹에서 SMB 서버를 생성하려면

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 작업 그룹에서 SMB 서버를 생성합니다.

   ```
   FSxIdabcde123456::> vserver cifs create -vserver vserver_name -cifs-
   server cifs_server_name -workgroup workgroup_name [-comment workgroup_description]
   ```

   다음 명령은 작업 그룹 smb_server01에 SMB 서버를 생성합니다workgroup01.

   ```
   FSxIdabcde123456::> vserver cifs create -vserver svm1 -cifs-server SMB_SERVER01 -
   workgroup workgroup01
   ```

   SVM의 관리 포트에 연결된 경우를 지정할 필요가 없습니다-vserver.

3. vserver cifs show 명령을 사용하여 SMB 서버 구성을 확인합니다.

   다음 예제에서 명령 출력은 이름이 인 SMB 서버가 작업 그룹의 SVMsvm1에 생성smb_server01되었음을 보여줍니다workgroup01.

   ```
   FSxIdabcde123456::> vserver cifs show -vserver svm1

                                           Vserver: svm1
                        CIFS Server NetBIOS Name: SMB_SERVER01
                    NetBIOS Domain/Workgroup Name: workgroup01
                     Fully Qualified Domain Name: -
                             Organizational Unit: -
   Default Site Used by LIFs Without Site Membership: -
                                   Workgroup Name: workgroup01
                              Authentication Style: workgroup
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
   ```

SMB 서버에서 로컬 사용자 계정 생성

SMB 연결을 통해 SVM에 포함된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 사용자 계정을 생성할 수 있습니다. SMB 세션을 생성할 때 로컬 사용자 계정을 인증에 사용할 수도 있습니다. 로컬 사용자 기능은 SVM이 생성될 때 기본적으로 활성화됩니다. 로컬 사용자 계정을 생성할 때 사용자 이름을 지정하고 계정을 연결할 SVM을 지정해야 합니다.

SMB 서버에서 로컬 사용자 계정을 생성하려면

1. vserver cifs users-and-groups local-user create ONTAP CLI 명령을 사용하여 로컬 사용자를 생성합니다.

   ```
   vserver cifs users-and-groups local-user create -vserver svm_name -user-
   name user_name optional_parameters
   ```

   다음과 같은 선택적 파라미터가 유용할 수 있습니다.

   - `-full-name` - 사용자의 전체 이름입니다.
   - `-description` - 로컬 사용자에 대한 설명입니다.
   - `-is-account-disabled {true|false}` - 사용자 계정의 활성화 또는 비활성화 여부를 지정합니다. 이 파라미터를 지정하지 않으면 기본값은 사용자 계정을 활성화하는 것입니다.

   명령은 로컬 사용자의 암호를 묻는 메시지를 표시합니다.
2. 로컬 사용자의 암호를 입력한 다음 암호를 확인합니다.
3. 사용자가 성공적으로 생성되었는지 확인합니다.

   ```
   vserver cifs users-and-groups local-user show -vserver svm_name
   ```

다음 예제에서는 SVM `SMB_SERVER01\sue`과 `Sue Chang`연결된 전체 이름이 인 로컬 사용자를 생성합니다`svm1`.

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user create -vserver svm1
 -user-name SMB_SERVER01\sue -full-name "Sue Chang"

Enter the password:
Confirm the password:
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-user show
Vserver  User Name                  Full Name  Description
-------- -------------------------- ---------- -------------
svm1     SMB_SERVER01\Administrator            Built-in administrator account
svm1     SMB_SERVER01\sue           Sue Chang
```

SMB 서버에서 로컬 그룹 생성

SMB 연결을 통해 SVM과 연결된 데이터에 대한 액세스를 승인하는 데 사용할 수 있는 로컬 그룹을 생성할 수 있습니다. 그룹 구성원이 보유한 사용자 권한 또는 기능을 정의하는 권한을 할당할 수도 있습니다.

로컬 그룹 기능은 SVM이 생성될 때 기본적으로 활성화됩니다. 로컬 그룹을 생성할 때 그룹의 이름을 지정하고 그룹을 연결할 SVM을 지정해야 합니다. 로컬 도메인 이름을 사용하거나 사용하지 않고 그룹 이름을 지정할 수 있으며, 선택적으로 로컬 그룹에 대한 설명을 지정할 수 있습니다. 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.

SMB 서버에서 로컬 그룹을 생성하려면

1. vserver cifs users-and-groups local-group create ONTAP CLI 명령을 사용하여 로컬 그룹을 생성합니다.

   ```
   vserver cifs users-and-groups local-group create -vserver svm_name -group-
   name group_name [-description local_group_description
   ```

   로컬 그룹에 대한 설명을 포함하는 것이 유용합니다.
2. 그룹이 성공적으로 생성되었는지 확인합니다.

   ```
   vserver cifs users-and-groups local-group show -vserver svm_name
   ```

다음 예제에서는 SVM과 SMB_SERVER01\engineering 연결된 로컬 그룹을 생성합니다svm1.

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group create -vserver svm1 -
group-name SMB_SERVER01\engineering
```

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group show -vserver svm1

Vserver          Group Name                  Description
```

```
---------------- ---------------------------- ----------------------------
svm1             BUILTIN\Administrators       Built-in Administrators group
svm1             BUILTIN\Backup Operators     Backup Operators group
svm1             BUILTIN\Guests               Built-in Guests group
svm1             BUILTIN\Power Users          Restricted administrative privileges
svm1             BUILTIN\Users                All users
svm1             SMB_SERVER01\engineering
```

로컬 그룹에 로컬 사용자 추가

로컬 또는 도메인 사용자를 추가 및 제거하거나 도메인 그룹을 추가 및 제거하여 로컬 그룹 멤버십을 관리할 수 있습니다. 이는 그룹에 배치된 액세스 제어를 기반으로 데이터에 대한 액세스를 제어하거나 사용자에게 해당 그룹과 연결된 권한을 부여하려는 경우에 유용합니다. 로컬 사용자, 도메인 사용자 또는 도메인 그룹이 그룹의 멤버십을 기반으로 액세스 권한 또는 권한을 더 이상 갖지 않도록 하려면 그룹에서 멤버를 제거할 수 있습니다.

로컬 그룹에 멤버를 추가할 때는 다음 사항에 유의하세요.

- 특별한 모든 사람 그룹에 사용자를 추가할 수 없습니다.
- 로컬 그룹을 다른 로컬 그룹에 추가할 수 없습니다.
- 도메인 사용자 또는 그룹을 로컬 그룹에 추가하려면가 이름을 SID로 확인할 수 있어야 ONTAP 합니다.

로컬 그룹에서 멤버를 제거할 때는 다음 사항에 유의하세요.

- 특별한 모든 사람 그룹에서 멤버를 제거할 수 없습니다.
- 로컬 그룹에서 멤버를 제거하려면가 해당 이름을 SID로 확인할 수 있어야 ONTAP 합니다.

이 절차에 사용되는 명령을 실행하려면 `fsxadmin` 역할이 있어야 합니다. 자세한 내용은 ONTAP 사용자 및 역할 단원을 참조하십시오.

로컬 그룹 멤버십을 관리하려면

- vserver cifs users-and-groups local-group add-members 및 vserver cifs users-and-groups local-group remove-members ONTAP CLI 명령을 사용하여 멤버를 그룹에 추가하거나 그룹에서 제거합니다.

  - 작업 그룹에 멤버를 추가하려면:

```
vserver cifs users-and-groups local-group add-members -vserver svm_name -group-
name group_name -member-names name[,...]
```

지정된 로컬 그룹에 추가할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정할 수 있습니다.

- 작업 그룹의 구성원을 보려면:

```
vserver cifs users-and-groups local-group show-members -vserver svm_name -group-
name group_name
```

- 작업 그룹에서 멤버를 제거하려면:

```
vserver cifs users-and-groups local-group remove-members -vserver svm_name -
group-name group_name -member-names name[,...]
```

지정된 로컬 그룹에서 제거할 로컬 사용자, 도메인 사용자 또는 도메인 그룹의 쉼표로 구분된 목록을 지정할 수 있습니다.

다음 예시에서는 SMB_SERVER01\engineering SVM SMB_SERVER01\sue의 로컬 그룹에 로컬 사용자를 추가합니다svm1.

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group add-members -vserver svm1
 -group-name SMB_SERVER01\engineering -member-names SMB_SERVER01\sue
```

다음 예시에서는 SMB_SERVER01\engineering SVM의 로컬 그룹에서 로컬 사용자 SMB_SERVER01\sue 및 SMB_SERVER01\james를 제거합니다svm1.

```
FSxIdabcde123456::> vserver cifs users-and-groups local-group remove-
members -vserver svm1 -group-name SMB_SERVER01\engineering -member-names
 SMB_SERVER01\sue,SMB_SERVER01\james
```

다음 예시에서는 로컬 그룹의 멤버를 나열합니다SMB_SERVER01\engineering.

```
FsxIdabcdef01234::> vserver cifs users-and-groups local-group show-members -
vserver svm_name -group-name group_name

           Vserver: svm1
      Domain Name: SMB_SERVER01
```

```
        Group Name: SMB_SERVER01\engineering
      Member Name: SMB_SERVER01\anita
                   SMB_SERVER01\james
                   SMB_SERVER01\liang
```

스토리지 가상 머신(SVM) 구성 세부 정보 모니터링

Amazon FSx 콘솔 AWS CLI, 및 Amazon FSx FSx API를 사용하여 현재 파일 시스템에 있는 FSx for ONTAP 스토리지 가상 머신을 볼 수 있습니다.

파일 시스템의 스토리지 가상 머신을 보려면 다음 작업을 수행합니다.

- 콘솔 사용 - 파일 시스템을 선택하여 해당 파일 시스템의 세부 정보 페이지를 봅니다. 파일 시스템의 모든 스토리지 가상 머신을 나열하려면 스토리지 가상 머신 탭을 선택한 다음 보려는 스토리지 가상 머신을 선택합니다.
- CLI 또는 API 사용 – describe-storage-virtual-machines CLI 명령 또는 DescribeStorageVirtualMachines API 작업을 사용합니다.

  AWS 리전의 해당 계정에 있는 모든 SVM에 대한 전체 설명 목록이 시스템 응답으로 제시됩니다.

스토리지 가상 머신 삭제(SVM)

Amazon FSx 콘솔, AWS CLI및 API를 사용해야만 FSx for ONTAP SVM을 삭제할 수 있습니다. SVM을 삭제하려면 먼저 SVM에 연결된 루트가 아닌 모든 볼륨을 삭제해야 합니다.

> **Important**
>
> NetApp ONTAP CLI 또는 API를 사용하여 SVM을 삭제할 수 없습니다.

> **Note**
>
> 스토리지 가상 머신을 삭제하기 전에 SVM의 데이터에 액세스하는 애플리케이션이 없는지, SVM에 연결된 루트가 아닌 모든 볼륨을 삭제했는지 확인해야 합니다.

스토리지 가상 머신 삭제(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.

2. 다음과 같이 삭제하려는 SVM을 선택합니다.

   - 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 SVM을 삭제할 ONTAP 파일 시스템을 선택합니다.
   - 스토리지 가상 머신 탭을 선택합니다.

     또는

   - 사용 가능한 모든 SVM 목록을 표시하려면 ONTAP을 확장하고 스토리지 가상 머신을 선택합니다.

   목록에서 삭제하려는 SVM을 선택합니다.
3. 볼륨 탭에서 SVM에 연결된 볼륨 목록을 확인합니다. SVM에 연결된 루트가 아닌 볼륨이 있는 경우 SVM을 삭제하기 전에 이를 먼저 삭제해야 합니다. 자세한 내용은 볼륨 삭제 섹션을 참조하세요.
4. 작업메뉴에서 스토리지 가상 머신 삭제를 선택합니다.
5. 삭제 확인 대화 상자에서 스토리지 가상 머신 삭제를 선택합니다.

스토리지 가상 머신 삭제(CLI)

- FSx for ONTAP 스토리지 가상 머신을 삭제하려면 다음 예제와 같이 delete-storage-virtual-machine CLI 명령(또는 이에 상응하는 DeleteStorageVirtualMachine API 작업)을 사용합니다.

```
aws fsx delete-storage-virtual-machine --storage-virtual-machine-id svm-
abcdef0123456789d
```

FSx for ONTAP 볼륨 관리

FSx for ONTAP 파일 시스템의 각 스토리지 가상 머신(SVM)은 볼륨을 하나 이상 가질 수 있습니다. 볼륨은 파일, 디렉터리 또는 iSCSI 논리적 스토리지 유닛(LUN)을 위한 격리된 데이터 컨테이너입니다. 볼륨은 씬 프로비저닝되므로 볼륨에 저장된 데이터에 대해서만 스토리지 용량을 사용합니다.

iSCSI LUN(공유 블록 스토리지)을 생성하여 네트워크 파일 시스템(NFS) 프로토콜, 서버 메시지 블록(SMB) 프로토콜 또는 인터넷 소형 컴퓨터 시스템 인터페이스(iSCSI) 프로토콜을 통해 Linux, Windows 또는 MacOS 클라이언트에서 볼륨에 액세스할 수 있습니다. FSx for ONTAP은 동일한 볼륨에 대한 다중 프로토콜 액세스(동시 NFS 및 SMB 액세스)도 지원합니다.

AWS Management Console, Amazon FSx API 또는 NetApp BlueXP를 사용하여 볼륨 AWS CLI을 생성할 수 있습니다. 또한 파일 시스템 또는 SVM의 관리 엔드포인트에서도 NetApp ONTAP CLI 또는 REST API를 사용하여 볼륨을 생성, 업데이트 및 삭제할 수 있습니다.

> **Note**
>
> HA 쌍당 500개의 볼륨을 생성할 수 있으며, 모든 HA 쌍에 걸쳐 최대 1,000개의 볼륨을 생성할 수 있습니다. FlexGroup 구성 볼륨은 이 제한에 포함됩니다. 기본적으로 FlexGroup마다 집계당 8개의 구성 볼륨이 있습니다.

볼륨을 생성할 때 다음 속성을 정의합니다.

- 볼륨 스타일 - 볼륨 스타일은 FlexVol 또는 FlexGroup일 수 있습니다.
- 볼륨 이름 - 볼륨의 이름입니다.
- 볼륨 유형 - 볼륨 유형은 읽기-쓰기(RW) 또는 데이터 보호(DP)일 수 있습니다. DP 볼륨은 읽기 전용이며 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용됩니다.
- 볼륨 크기 - 스토리지 계층과 관계없이 볼륨이 저장할 수 있는 최대 데이터 양입니다.
- 정션 경로 - SVM의 네임스페이스에서 볼륨이 마운트되는 위치입니다.
- 스토리지 효율성 - 데이터 압축, 압축, 중복 제거 등의 스토리지 효율성 기능을 통해 일반적인 파일 공유 워크로드에서 일반적으로 65%의 스토리지를 절약할 수 있습니다.
- 볼륨 보안 스타일(Unix 또는 NTFS) - 사용자에게 권한을 부여할 때 볼륨의 데이터 액세스에 어떤 유형의 권한이 사용되는지 결정합니다.
- 데이터 계층화 - 계층화 정책은 비용 효율적인 용량 풀 계층에 어떤 데이터를 저장할지 정의합니다.
- 계층화 정책 냉각 기간 - 데이터가 콜드로 표시되고 용량 풀 스토리지로 이동되는 시기를 정의합니다.
- 스냅샷 정책 - 스냅샷 정책은 시스템에서 볼륨에 대한 스냅샷을 생성하는 방법을 정의합니다. 사전 정의된 세 가지 정책 중에서 선택하거나 ONTAP CLI 또는 REST API를 사용하여 생성한 사용자 지정 정책을 사용할 수 있습니다.
- 백업에 태그 복사 – Amazon FSx는 이 옵션을 사용하여 볼륨의 모든 태그를 백업으로 자동 복사합니다. AWS CLI 또는 Amazon FSx API를 사용하여이 옵션을 설정할 수 있습니다.

주제

- 볼륨 스타일
- 볼륨 유형

볼륨 스타일

FSx for ONTAP은 다양한 용도로 사용할 수 있는 두가지 스타일의 볼륨을 제공합니다. Amazon FSx 콘솔, AWS CLI및 Amazon FSx API를 사용하여 FlexVol 또는 FlexGroup 볼륨을 생성할 수 있습니다.

- FlexVol 볼륨은 고가용성(HA) 페어 1개가 있는 파일 시스템에 가장 간단한 환경을 제공하므로 HA 페어 1개가 있는 1세대 파일 시스템 및 2세대 파일 시스템의 기본 볼륨 스타일입니다. FlexVol 볼륨의 최소 크기는 20메비바이트(MiB)이고 최대 크기는 314,572,800MiB 입니다.
- FlexGroup 볼륨은 여러 구성 FlexVol 볼륨으로 구성되므로 HA 페어가 여러 개인 파일 시스템의 FlexVol 볼륨보다 더 높은 성능과 스토리지 확장성을 제공할 수 있습니다. FlexGroup 볼륨은 HA 페어가 두 개 이상인 2세대 파일 시스템의 기본 볼륨 스타일입니다. FlexGroup 볼륨의 최소 크기는 구성 요소당 100기가비바이트(GiB)이고 최대 크기는 20페비바이트(PiB)입니다.

ONTAP CLI를 사용하여 FlexVol 스타일의 볼륨을 FlexGroup 스타일로 변환하면 단일 구성 요소로 FlexGroup를 만들 수 있습니다. 그러나 AWS DataSync 를 사용하여 FlexVol 볼륨과 새 FlexGroup 볼륨 간에 데이터를 이동하여 FlexGroup's 데이터가 구성 요소에 고르게 분산되도록 하는 것이 좋습니다. 자세한 내용은 FlexGroup 구성 요소 단원을 참조하십시오.

> **Note**
>
> ONTAP CLI를 사용하여 FlexVol 볼륨을 FlexGroup 볼륨으로 변환하려면 변환하기 전에 FlexVol 볼륨의 백업을 모두 삭제해야 합니다. ONTAP는 변환 과정에서 자동으로 데이터 밸런스를 재조정하지 않으므로 FlexGroup 구성 요소 간에 데이터 밸런스가 불균형할 수 있습니다.

FlexGroup 구성 요소

FlexGroup 볼륨은 FlexVol 볼륨인 구성 요소로 구성됩니다. 기본적으로 FSx for ONTAP는 HA 페어당 FlexGroup 볼륨에 8개의 구성 요소를 할당합니다.

FlexGroup 볼륨을 생성하면 볼륨의 크기가 구성 요소 간에 균등하게 분할됩니다. 예를 들어, 8개의 구성 요소로 800기가바이트(GB) FlexGroup 볼륨을 생성하는 경우 각 구성 요소의 크기는 100GB입니다. FlexGroup 볼륨의 크기는 100GB에서 20 PiB 사이일 수 있지만 총 크기는 구성 요소의 크기에 따라 달라집니다. 각 구성 요소의 최소 크기는 100GB이고 최대 크기는 300TiB 입니다. 예를 들어 구성 요소가 8개인 FlexGroup 볼륨의 최소 크기는 800GB이고 최대 크기는 20 PiB 입니다.

ONTAP는 구성 요소에 걸쳐 파일 수준에서 데이터를 배포합니다. FlexGroup 볼륨의 각 구성 요소에 최대 20억 개의 파일을 저장할 수 있습니다.

FlexGroup 볼륨 크기를 업데이트하면 새 크기가 기존 구성 요소 간에 균등하게 분산됩니다.

ONTAP CLI 또는 REST API를 사용하여 FlexGroup 볼륨에 구성 요소를 더 추가할 수도 있습니다. 그러나 추가 스토리지 용량이 필요하고 모든 구성 요소가 이미 최대 크기(구성 요소당 300TiB)인 경우에만 그렇게 하는 것이 좋습니다. 구성 요소를 추가하면 구성 요소 간에 데이터와 I/O가 불균형해질 수 있습니다. 구성 요소가 균형을 이룰 때까지 쓰기 처리량이 균형잡힌 FlexGroup 볼륨보다 5~10% 낮을 수 있습니다. 새 데이터가 FlexGroup 볼륨에 기록되면 ONTAP는 구성 요소가 균형을 이룰 때까지 새 구성 요소 간에 배포하는 것을 우선으로 합니다. 새 구성 요소를 추가하는 경우 집계당 8개를 초과하지 않는 짝수를 선택하는 것이 좋습니다.

> **Note**
>
> 새 구성 요소를 추가하면 기존 스냅샷이 부분 스냅샷이 되므로 FlexGroup 볼륨을 이전 상태로 완전히 복원하는 데 사용할 수 없습니다. 새 구성 요소가 아직 존재하지 않았기 때문에 이전 스냅샷은 FlexGroup 볼륨의 전체 시점 이미지를 제공할 수 없습니다. 그러나 부분 스냅샷을 사용하여 개별 파일 및 디렉터리를 복원하거나, 새 볼륨을 생성하거나, SnapMirror로 복제할 수 있습니다.

볼륨 유형

FSx for ONTAP은 Amazon FSx 콘솔 AWS CLI, 및 Amazon FSx FSx API를 사용하여 생성할 수 있는 두 가지 유형의 볼륨을 제공합니다.

- 대부분의 경우 읽기-쓰기(RW) 볼륨이 사용됩니다. 이름에서 알 수 있듯이 읽기-쓰기가 가능합니다.
- 데이터 보호(DP) 볼륨은 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용하는 읽기 전용 볼륨입니다. 단일 볼륨의 데이터를 마이그레이션하거나 보호하려면 DP 볼륨을 사용해야 합니다.

FlexVol 및 FlexGroup볼륨은 RW 또는 DP일 수 있습니다.

> **Note**
>
> 볼륨 생성 후에는 볼륨 유형을 업데이트할 수 없습니다.

볼륨 보안 스타일

FSx for ONTAP 볼륨을 생성할 때 Unix와 NTFS라는 두 가지 보안 스타일 중에서 선택할 수 있습니다. 각 보안 스타일은 데이터에 대한 권한 처리 방식에 서로 다른 영향을 미칩니다. 목적에 적합한 보안 스타일을 선택하려면 다양한 영향을 이해해야 합니다.

보안 스타일이 데이터에 액세스할 수 있거나 액세스할 수 없는 클라이언트 유형을 결정하지 않는다는 점을 이해하는 것이 중요합니다. 보안 스타일은 FSx for ONTAP가 데이터 액세스를 제어하는 데 사용하는 권한 유형과 이러한 권한을 수정할 수 있는 클라이언트 유형만 결정합니다.

볼륨의 보안 스타일을 결정하는 데 사용하는 두 가지 요소는 파일 시스템을 관리하는 관리자 유형과 볼륨의 데이터에 액세스하는 사용자 또는 서비스 유형입니다.

Amazon FSx 콘솔, CLI 및 API에서 볼륨을 생성할 때 보안 스타일은 자동으로 루트 볼륨의 보안 스타일로 설정됩니다. AWS CLI 또는 API를 사용하여 볼륨의 보안 스타일을 수정할 수 있습니다. 볼륨을 생성한 후에 이 설정을 수정할 수 있습니다. 자세한 내용은 볼륨 업데이트 섹션을 참조하세요.

볼륨에 보안 스타일을 구성할 때는 사용 권한 관리와 관련된 문제가 발생하지 않도록 환경 요구 사항을 고려하여 최상의 보안 스타일을 선택합니다. 보안 스타일은 데이터에 액세스할 수 있는 클라이언트 유형을 결정하지 않는다는 점에 유의하세요. 보안 스타일은 데이터 액세스를 허용하는 데 사용되는 권한과 이러한 권한을 수정할 수 있는 클라이언트 유형을 결정합니다. 다음은 볼륨에 어떤 보안 스타일을 선택할지 결정하는 데 도움이 될 수 있는 고려 사항입니다.

- Unix(Linux) – UNIX 관리자가 파일 시스템을 관리하고, 대다수의 사용자가 NFS 클라이언트이고, 데이터에 액세스하는 애플리케이션이 UNIX 사용자를 서비스 계정으로 사용하는 경우 이 보안 스타일을 선택합니다. Linux 클라이언트만 Unix 보안 스타일로 권한을 수정할 수 있으며, 파일 및 디렉터리에 사용되는 권한 유형은 모드 비트 또는 NFS v4.x ACL입니다.
- NTFS – Windows 관리자가 파일 시스템을 관리하고, 대다수의 사용자가 SMB 클라이언트이고, 데이터에 액세스하는 애플리케이션이 Windows 사용자를 서비스 계정으로 사용하는 경우 이 보안 스타일을 선택합니다. 볼륨에 Windows 액세스가 필요한 경우 NTFS 보안 스타일을 사용하는 것이 좋습니다. Windows 클라이언트만 NTFS 보안 스타일로 권한을 수정할 수 있으며 파일 및 디렉터리에 사용되는 권한 유형은 NTFS ACL입니다.

볼륨 생성

ONTAP 명령줄 인터페이스(CLI) 및 REST API 외에도 Amazon FSx FSx 콘솔 AWS CLI, 및 Amazon FSx API를 사용하여 FSx for NetApp ONTAP FlexVol 또는 FlexGroup 볼륨을 생성할 수 있습니다.

FlexVol 볼륨 생성(콘솔)

> **Note**
> 볼륨의 보안 스타일이 루트 볼륨의 보안 스타일로 자동 설정됩니다.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 볼륨을 선택합니다.
3. 볼륨 생성을 선택합니다.
4. 파일 시스템 유형에서 Amazon FSx for NetApp ONTAP를 선택합니다.
5. 파일 시스템 세부 정보 섹션에서 다음 정보를 입력합니다.
   - 파일 시스템에서, 볼륨을 생성할 파일 시스템을 선택합니다.
   - 스토리지 가상 머신에서, 볼륨을 생성할 스토리지 가상 머신(SVM)을 선택합니다.
6. 볼륨 스타일 섹션에서 FlexVol을 선택합니다
7. 볼륨 세부 정보 섹션에서 다음 정보를 입력합니다.
   - 볼륨 이름 필드에 볼륨의 이름을 입력합니다. 최대 203자의 영숫자 또는 밑줄 (_) 문자를 사용할 수 있습니다.
   - 볼륨 크기에는 20~314572800 범위의 정수를 입력하여 크기를 메비바이트(MiB) 단위로 지정합니다.
   - 볼륨 유형의 경우 읽기 및 쓰기가 가능한 볼륨을 생성하려면 읽기-쓰기(RW)를 선택하고 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용할 수 있는 읽기 전용 볼륨을 생성하려면 데이터 보호(DP)를 선택합니다. 자세한 내용은 볼륨 유형 단원을 참조하십시오.
   - 정션 경로에는 파일 시스템 내에서 볼륨을 마운트할 위치를 입력합니다. 이름 앞에 슬래시가 있어야 합니다(예: `/vol3`).
   - 스토리지 효율성의 경우, 이 볼륨에서 ONTAP 스토리지 효율 기능(중복 제거, 압축 및 압축)을 활성화하려면 사용을 선택합니다. 자세한 내용은 스토리지 효율성 단원을 참조하십시오.
   - 볼륨 보안 스타일에서 볼륨에 대해 Unix(Linux)와 NTFS 중에서 선택합니다. 자세한 내용은 볼륨 보안 스타일 단원을 참조하십시오.

- 스냅샷 정책에서 볼륨의 스냅샷 정책을 선택합니다. 스냅샷 정책에 대한 자세한 내용은 스냅샷 정책 섹션을 참조하세요.

  사용자 지정 정책을 선택하는 경우 custom-policy 필드에 정책 이름을 지정해야 합니다. 사용자 지정 정책은 SVM 또는 파일 시스템에 이미 있어야 합니다. ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요.

8. 스토리지 계층화 섹션에서 다음 정보를 입력합니다.

   - 용량 풀 계층화 정책의 경우 볼륨에 대한 스토리지 풀 계층화 정책을 자동(기본값), 스냅샷만, 모두 또는 없음 중에서 선택합니다. 자세한 내용은 볼륨 계층화 정책 단원을 참조하십시오.
   - 자동 또는 스냅샷 전용을 선택하는 경우 계층화 정책 냉각 기간을 설정하여 액세스하지 않은 데이터가 콜드 상태로 표시되어 용량 풀 스토리지로 이동되기까지의 일수를 정의할 수 있습니다. 2 ~ 183일 사이의 값을 입력할 수 있습니다. 기본 설정은 31일입니다.

9. 고급 섹션의 SnapLock 구성에는 활성화됨과 비활성화됨 중에서 선택합니다. SnapLock 컴플라이언스 볼륨 또는 SnapLock 엔터프라이즈 볼륨 구성에 대한 자세한 내용은 SnapLock 규정 준수 이해 및 SnapLock 엔터프라이즈 이해를 참조하세요. SnapLock에 대한 자세한 정보는 SnapLock로 데이터 보호을 참조하세요.
10. 확인을 선택하여 볼륨을 생성합니다.

파일 시스템 세부 정보 페이지에 있는 볼륨 창의 상태 열에서 업데이트 진행 상황을 모니터링할 수 있습니다. 볼륨 상태가 생성됨이면 볼륨을 사용할 준비가 된 것입니다.

FlexGroup 볼륨 생성(콘솔)

> **Note**
>
> Amazon FSx 콘솔을 사용하여 여러 HA 페어가 있는 파일 시스템의 FlexGroup 볼륨만 생성할 수 있습니다. HA 페어가 여러 개인 파일 시스템의 FlexVol 볼륨을 생성하려면 AWS CLI, Amazon FSx API 또는 NetApp 관리 도구를 사용합니다.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 볼륨을 선택합니다.
3. 볼륨 생성을 선택합니다.
4. 파일 시스템 유형에서 Amazon FSx for NetApp ONTAP를 선택합니다.

5. 파일 시스템 세부 정보 섹션에서 다음 정보를 입력합니다.

   - 파일 시스템에서, 볼륨을 생성할 파일 시스템을 선택합니다.
   - 스토리지 가상 머신에서, 볼륨을 생성할 스토리지 가상 머신(SVM)을 선택합니다.

6. 볼륨 스타일 섹션에서 FlexGroup 선택합니다.

7. 볼륨 세부 정보 섹션에서 다음 정보를 입력합니다.

   - 볼륨 이름 필드에 볼륨의 이름을 입력합니다. 최대 203자의 영숫자 또는 밑줄 (_) 문자를 사용할 수 있습니다.
   - 볼륨 크기에 HA 페어당 800기가비바이트(GiB)~2,400테비바이트(TiB) 범위의 정수를 입력합니다. 예를 들어 고가용성(HA) 페어가 12개인 파일 시스템의 최소 볼륨 크기는 9,600GiB이고 최대 크기는 20,480TiB.
   - 볼륨 유형의 경우 읽기 및 쓰기가 가능한 볼륨을 생성하려면 읽기-쓰기(RW)를 선택하고 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용할 수 있는 읽기 전용 볼륨을 생성하려면 데이터 보호(DP)를 선택합니다. 자세한 내용은 볼륨 유형 단원을 참조하십시오.
   - 정션 경로에는 파일 시스템 내에서 볼륨을 마운트할 위치를 입력합니다. 이름 앞에 슬래시가 있어야 합니다(예: `/vol3`).
   - 스토리지 효율성의 경우 ONTAP 스토리지 효율성 기능(중복 제거 및 압축)을 활성화하려면 활성화를 선택합니다. 자세한 내용은 스토리지 효율성 단원을 참조하십시오.
   - 볼륨 보안 스타일에서 볼륨에 대해 Unix(Linux)와 NTFS 중에서 선택합니다. 자세한 내용은 볼륨 보안 스타일 단원을 참조하십시오.

     > **Note**
     >
     > 볼륨의 보안 스타일이 루트 볼륨의 보안 스타일로 자동 설정됩니다.

   - 스냅샷 정책에서 볼륨의 스냅샷 정책을 선택합니다. 스냅샷 정책에 대한 자세한 내용은 스냅샷 정책 섹션을 참조하세요.

     사용자 지정 정책을 선택하는 경우 custom-policy 필드에 정책 이름을 지정해야 합니다. 사용자 지정 정책은 SVM 또는 파일 시스템에 이미 있어야 합니다. ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요.

8. 스토리지 계층화 섹션에서 다음 정보를 입력합니다.

- 용량 풀 계층화 정책의 경우 볼륨에 대한 스토리지 풀 계층화 정책을 자동(기본값), 스냅샷만, 모두 또는 없음 중에서 선택합니다. 자세한 내용은 볼륨 계층화 정책 단원을 참조하십시오.
- 자동 또는 스냅샷 전용을 선택하는 경우 계층화 정책 냉각 기간을 설정하여 액세스하지 않은 데이터가 콜드 상태로 표시되어 용량 풀 스토리지로 이동되기까지의 일수를 정의할 수 있습니다. 2~183일 사이의 값을 입력할 수 있습니다. 기본 설정은 31일입니다.

9. 고급 섹션의 SnapLock 구성에는 활성화됨과 비활성화됨 중에서 선택합니다. SnapLock 컴플라이언스 볼륨 또는 SnapLock 엔터프라이즈 볼륨 구성에 대한 자세한 내용은 SnapLock 규정 준수 이해 및 SnapLock 엔터프라이즈 이해를 참조하세요. SnapLock에 대한 자세한 정보는 SnapLock로 데이터 보호을 참조하세요.
10. 확인을 선택하여 볼륨을 생성합니다.

파일 시스템 세부 정보 페이지에 있는 볼륨 창의 상태 열에서 업데이트 진행 상황을 모니터링할 수 있습니다. 볼륨 상태가 생성됨이면 볼륨을 사용할 준비가 된 것입니다.

볼륨 생성(CLI)

- 다음 예제와 같이 create-volume CLI 명령(또는 이에 상응하는 CreateVolume API 작업)을 사용하여 FSx for ONTAP 볼륨을 생성합니다.

```
aws fsx create-volume \
    --volume-type ONTAP \
    --name vol1 \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/
vol1,SecurityStyle=NTFS, \
          SizeInMegabytes=1024,SnapshotPolicy=default, \
          StorageVirtualMachineId=svm-abcdef0123456789a,OntapVolumeType=RW, \
          StorageEfficiencyEnabled=true
```

Amazon FSx는 볼륨 생성 후 다음 예제와 같이 JSON 형식으로 설명을 반환합니다.

```
{
    "Volume": {
        "CreationTime": "2022-08-12T13:03:37.625000-04:00",
        "FileSystemId": "fs-abcdef0123456789c",
        "Lifecycle": "CREATING",
        "Name": "vol1",
        "OntapConfiguration": {
            "CopyTagsToBackups": true,
```

```
            "FlexCacheEndpointType": "NONE",
            "JunctionPath": "/vol1",
            "SecurityStyle": "NTFS",
            "SizeInMegabytes": 1024,
            "SnapshotPolicy": "default",
            "StorageEfficiencyEnabled": true,
            "StorageVirtualMachineId": "svm-abcdef0123456789a",
            "StorageVirtualMachineRoot": false,
            "TieringPolicy": {
                "Name": "NONE"
            },
            "OntapVolumeType": "RW"
        },
        "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-abcdef0123456789c/
fsvol-abcdef0123456789b",
        "VolumeId": "fsvol-abcdef0123456789b",
        "VolumeType": "ONTAP"


    }
}
```


볼륨의 백업을 새 볼륨으로 복원하여 새 볼륨을 생성할 수도 있습니다. 자세한 내용은 백업을 새 볼륨으로 복원 단원을 참조하십시오.

볼륨 업데이트

ONTAP 명령줄 인터페이스(CLI) 및 REST API 외에도 Amazon FSx 콘솔 AWS CLI, 및 Amazon FSx API를 사용하여 FSx for NetApp ONTAP 볼륨의 구성을 업데이트할 수 있습니다. 기존 FSx for ONTAP 볼륨의 다음 속성을 수정할 수 있습니다.

- 볼륨 이름
- 정션 경로
- 볼륨 크기
- 스토리지 효율성
- 용량 풀 계층화 정책
- 볼륨 보안 스타일
- 스냅샷 정책
- 계층화 정책 휴지 기간

- 백업에 태그 복사(AWS CLI 및 Amazon FSx API 사용)

자세한 내용은 FSx for ONTAP 볼륨 관리 단원을 참조하십시오.

볼륨 구성 업데이트(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 볼륨을 업데이트할 ONTAP 파일 시스템을 선택합니다.
3. 볼륨 탭을 선택합니다.
4. 업데이트할 볼륨을 선택합니다.
5. 작업에서 볼륨 업데이트를 선택합니다.

   볼륨 업데이트 대화 상자가 볼륨의 현재 설정과 함께 표시됩니다.
6. 정션 경로에는 파일 시스템 내에서 볼륨을 마운트할 기존 위치를 입력합니다. `/vol15`와 같이 이름 앞에 슬래시가 있어야 합니다.
7. 볼륨 크기의 경우 Amazon FSx 콘솔에 지정된 범위 내에서 볼륨 크기를 늘리거나 줄일 수 있습니다. FlexVol 볼륨의 경우 최대 크기는 300TiB 입니다. FlexGroup 볼륨의 경우, 최대 크기는 300TiB에 FlexGroup의 총 구성 볼륨 수를 곱한 값으로 최대 20PiB까지 가능합니다.
8. 스토리지 효율성의 경우, 볼륨에서 ONTAP 스토리지 효율 기능(중복 제거, 압축, 압축)을 활성화하려면 사용을 선택하고, 사용하지 않으려면 비활성화를 선택합니다.
9. 용량 풀 계층화 정책에는 볼륨의 새 스토리지 풀 계층화 정책을 자동(기본값), 스냅샷만, 모두, 없음 중에서 선택합니다. 용량 풀 계층화 정책에 대한 자세한 내용은 볼륨 계층화 정책 섹션을 참조하세요.
10. 볼륨 보안 스타일에는 Unix(Linux), NTFS 또는 혼합 중 하나를 선택합니다. 볼륨의 보안 스타일에 따라 다중 프로토콜 액세스에 대한 기본 설정이 NTFS 또는 ACL로 기본 설정됩니다. 혼합 모드는 다중 프로토콜 액세스에는 필요하지 않으며 고급 사용자에게만 권장됩니다.
11. 스냅샷 정책에서 볼륨의 스냅샷 정책을 선택합니다. 스냅샷 정책에 대한 자세한 내용은 스냅샷 정책 섹션을 참조하세요.

    사용자 지정 정책을 선택하는 경우 custom-policy 필드에 정책 이름을 지정해야 합니다. 사용자 지정 정책은 SVM 또는 파일 시스템에 이미 있어야 합니다. ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요.

12. 계층화 정책 휴지 기간에 유효한 값은 2~183일입니다. 볼륨의 계층화 정책 휴지 기간은 액세스되지 않은 데이터가 콜드 상태로 표시되고 용량 풀 스토리지로 이동되기까지의 일수를 정의합니다. 이 설정은 `Auto` 및 `Snapshot-only` 정책에만 영향을 줍니다.
13. 업데이트를 선택하여 볼륨을 업데이트합니다.

볼륨의 구성 업데이트(CLI)

- FSx for ONTAP 볼륨의 구성을 업데이트하려면 다음 예제와 같이 update-volume CLI 명령(또는 이에 상응하는 UpdateVolume API 작업)을 사용합니다.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=default-1weekly, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

FlexGroup 볼륨 확장

ONTAP CLI의 `volume expand` 명령을 사용하여 FlexGroup 볼륨에 구성 볼륨을 추가할 수 있습니다. 이는 FlexGroup 볼륨의 균형을 유지하기 때문에 파일 시스템에 고가용성(HA) 페어를 추가한 후 모범 사례입니다.

FlexGroup 볼륨을 확장하기 전에 다음 사항을 고려하세요.

- FlexGroup's를 구성하는 모든 볼륨의 스토리지 용량은 동일합니다. 추가 구성 요소로 FlexGroup 볼륨을 확장하면 각 구성 요소는 기존 구성 요소와 크기가 동일합니다. 따라서 구성 요소를 추가하기 전에 각 집계에 사용 가능한 충분한 공간이 있는지 확인합니다.
- AWS 에서는 각 볼륨에 대해 집계당 8개의 구성 FlexGroup 볼륨을 유지할 것을 권장합니다. 집계당 8개의 구성 볼륨은 FlexGroup 볼륨의 병렬 처리를 극대화하고 워크로드에 가장 최적의 성능을 제공합니다. 일반적으로 HA 페어를 추가하는 경우에만 추가 구성 요소로 FlexGroup 볼륨을 확장하는 것이 좋습니다. 이는 집계당 8개의 구성 요소를 유지하기 위해 구성 요소를 추가해야 하는 유일한 시나리오입니다.
- FlexGroup 볼륨이 SnapMirror 관계에 있는 경우 소스 볼륨과 대상 FlexGroup 볼륨 모두 동일한 수의 구성 요소를 가져야 합니다. 그렇지 않으면 SnapMirror 전송이 실패합니다. SnapMirror는 구성 요소 수준에서 작동하고 각 개별 구성 요소 간에 데이터를 전송합니다. 따라서 FlexGroup 볼륨을 추가

구성 볼륨과 함께 확장하는 경우, 이 볼륨과 SnapMirror 관계에 있는 볼륨도 수동으로 확장해야 합니다.

- 추가 구성 요소로 FlexGroup 볼륨을 확장하면 기존 스냅샷 복사본이 모두 '부분' 복사본이 됩니다. 부분 복사본은 복원할 수 없지만 찾아보고 개별 파일을 복원할 수 있습니다. 또한 이로 인해 Amazon FSx 백업, AWS 백업 또는 SnapMirror 관계에 대한 증분성이 손실됩니다.
- 구성 볼륨을 추가한 후에는 제거할 수 없습니다.

FlexGroup 볼륨 구성 요소 추가

ONTAP CLI를 사용하여 FlexGroup 볼륨에 구성 볼륨을 추가할 수 있습니다.

FlexGroup 볼륨 구성 요소를 추가하려면

1. NetApp ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 볼륨 확장 ONTAP CLI 명령을 사용하여 추가 구성 요소로 FlexGroup 볼륨을 확장합니다. 다음 값을 교체합니다.

   - `svm_name`를 FlexGroup 볼륨을 호스팅하는 스토리지 가상 머신(SVM)의 이름(예: `svm1`)으로 대체합니다.
   - `vol_name`를 확장하려는 FlexGroup 볼륨의 이름(예: `vol1`)과 함께 입력합니다.
   - 쉼표로 구분된 집계 목록과 함께 FlexGroup 구성 볼륨을 추가할 `aggregates`를 입력합니다. 예를 들어 `aggr1` 단일 집계 또는 여러 집계의 `aggr1,aggr2` 경우.
   - `constituent_per_aggregate`에 지정된 각 `aggregates`에 추가할 추가 구성 요소의 수를 입력합니다. FlexGroup를 볼륨에 상주하는 집계에 걸쳐 균형 잡힌 구성 요소 수가 있는지 확인하기 위해 충분한 구성 요소만 추가해야 합니다.

   ```
   ::> volume expand -vserver svm_name -volume vol_name -aggr-list aggregates -aggr-
   list-multiplier constituents_per_aggregate
   ```

> **Important**
>
> FlexGroup 구성 요소를 추가한 후에는 제거할 수 없으므로 이전 명령을 실행하기 전에 입력을 확인하세요.

집계 간 볼륨 이동

파일 시스템에 고가용성(HA) 페어를 추가할 때는 볼륨을 새 집계로 이동하여 기존 데이터의 균형을 재조정해야 합니다. 집계 간에 볼륨을 이동하려면 ONTAP CLI에서 `volume move` 명령을 사용할 수 있습니다.

`volume move` 명령을 사용하기 전에 다음 사항을 고려하세요.

- `volume move` 명령을 사용하면 파일 시스템의 네트워크 및 디스크 리소스를 사용하기 때문에 성능에 영향을 미칠 수 있습니다. 따라서 활동이 적은 기간에는 집계 간에 볼륨을 이동하는 것이 좋습니다. 또는 볼륨을 이동하는 동안 파일 시스템의 네트워크 처리량 사용률 및 디스크 처리량 사용률을 50% 이하로 줄일 수 있습니다.
- 파일 시스템에 미치는 성능 영향을 줄이려면 한 번에 두 HA 페어와 집계 간에 단일 볼륨을 이동하는 것이 좋습니다. 예를 들어 파일 시스템에 HA 페어가 4개 있는 경우 한 번에 두 개의 볼륨을 이동하는 것이 좋습니다(볼륨 이동이 동일한 HA 페어에서 오거나 향하지 않는 것으로 가정). ONTAP는 한 번에 각 HA 페어에서 최대 8개의 볼륨을 이동할 수 있도록 지원하지만, 더 많은 볼륨을 동시에 이동하면 클라이언트 I/O와 진행 중인 볼륨 이동의 성능이 모두 저하됩니다.
- 영향을 받는 볼륨의 SSD 계층에 저장된 모든 데이터는 물리적으로 다른 파일 서버의 다른 디스크 세트로 이동합니다. 이 작업은 백그라운드에서 수행되며 시간이 걸립니다. 전송에 걸리는 시간은 파일 시스템의 처리량 용량과 파일 시스템의 활동량에 따라 달라집니다. 그러나 볼륨 이동은 제한될 수 있습니다. 자세한 내용은 볼륨 이동 제한 단원을 참조하십시오.
- HA 페어가 동일한 용량 풀 스토리지를 공유하기 때문에 용량 계층에 저장된 모든 데이터는 물리적으로 이동되지 않습니다. 따라서 대부분의 데이터가 계층화된 볼륨을 이동하는 속도가 빨라집니다. 파일 메타데이터는 항상 SSD 계층에 저장된다는 점에 유의하세요. 자세한 내용은 볼륨 데이터 계층화 단원을 참조하십시오.

볼륨 이동 단계

볼륨 이동 작업에는 복제 단계와 전환 단계의 두 단계가 있습니다. 복제 단계에서 기존 데이터는 볼륨의 새 집계에 복제됩니다. 전환 단계에서 ONTAP는 볼륨의 새 집계로 최종 빠른 전송을 시도합니다. 여기에는 전송 단계 중에 작성된 모든 데이터를 전송하고 새 트래픽을 볼륨의 새 집계로 리디렉션하는 작

업이 포함됩니다. 기본적으로 컷오버 기간은 30초이며 볼륨에 대한 모든 I/O를 중지합니다. ONTAP가 전환 기간 동안 이러한 단계를 모두 수행할 수 없는 경우 실패합니다. 기본적으로 ONTAP는 3회 연속으로 축소를 시도합니다. 세 번의 연속 시도가 모두 실패하면 ONTAP는 성공할 때까지 1시간에 한 번 재시도합니다. 전환 단계가 시작되기 전에 볼륨에 대한 I/O 트래픽을 줄이거나 일시 중지하여 전환 단계가 성공하도록 파일 시스템의 부하를 줄일 수 있습니다.

시작 볼륨 이동

볼륨 이동을 시작하려면

1. NetApp ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. 볼륨 이동 시작 ONTAP CLI 명령을 실행합니다. 다음 값을 교체합니다.

   - `vserver_name`에 이동하려는 볼륨을 호스팅하는 SVM의 이름을 입력합니다.
   - `volume_name`를 볼륨의 구성 요소 이름(예: `vol1__0001`)
   - `aggregate_name`를 볼륨의 대상 집계 이름과 함께 입력합니다.
   - `-enforce-network-throttling` 볼륨 이동의 총 처리량을 제한합니다. 이는 선택 사항입니다.

   ```
   ::> volume move start -vserver svm_name -volume volume_name --destination-
   aggregate aggregate_name -foreground false
   [Job 1] Job is queued: Move "vol1__0001" in Vserver "svm01" to aggregate "aggr1".
    Use the "volume move show -vserver svm01 -volume vol1__0001" command to view the
    status of this operation.
   ```

> **Important**
>
> 이동 볼륨은 소스 및 대상 파일 서버의 네트워크 및 디스크 리소스를 사용합니다. 따라서 진행 중인 볼륨 이동이 워크로드의 성능에 영향을 미칠 수 있습니다. 또한 볼륨 이동의 전환 단계에서 볼륨에 대한 I/O 트래픽이 일시적으로 일시 중지됩니다.

볼륨 이동 모니터링

볼륨 이동을 모니터링하려면

- 볼륨 이동 작업의 상태를 확인하려면 `volume move show` ONTAP CLI 명령을 사용합니다.

```
::> volume move show -vserver svm_name -volume volume_name

Vserver Name: svm01
Volume Name: vol1__0001
Actual Completion Time: -
Bytes Remaining: 1.00TB
Specified Action For Cutover: retry_on_failure
Specified Cutover Time Window: 30
Destination Aggregate: aggr2
Destination Node: FsxId01234567890abcdef-03
Detailed Status: Transferring data: 12.23GB sent.
Percentage Complete: 1%
Move Phase: replicating
Prior Issues Encountered: -
Estimated Remaining Duration: 00:40:25
Replication Throughput: 434.3MB/s
Duration of Move: 00:00:27
Source Aggregate: aggr1
Source Node: FsxId01234567890abcdef-01
Move State: healthy
```

명령 출력은 이동을 완료하는 데 걸리는 예상 시간을 보여줍니다. 완료되면 `Move phase`에 `completed` 상태가 표시됩니다.

균형 잡힌 FlexGroup 볼륨 유지

워크로드가 최적의 성능을 발휘하려면 FlexGroup 볼륨이 모든 집계에 걸쳐 있어야 하고 집계당 구성 볼륨의 수가 짝수여야 합니다. 집계당 8개의 구성 요소를 사용하는 것이 좋습니다. FlexGroup 볼륨 리밸런싱 시 다음 시나리오를 고려하세요.

- 기존 집계 간에 FlexGroup 구성 요소 이동: FlexGroup's 구성 요소 볼륨을 균형이 잡힌 FlexGroup의 다른 집계로 이동하는 경우, 활용도가 낮은 다른 구성 요소를 원래 집계로 이동해야 합니다. 이렇게 하면 FlexGroup에 집계당 구성 요소가 짝수로 표시됩니다.

HA 쌍을 추가한 후 FlexGroup 구성 요소를 새 집계로 이동: HA 쌍을 추가한 후 FlexGroup's 구성 볼륨을 새 집계로 이동하는 경우, 구성 요소가 손실된 집계에서 추가 구성 요소로 FlexGroup를 확장해야 합니다. 이렇게 하면 FlexGroup에 집계당 구성 요소가 짝수로 표시됩니다. 자세한 내용은 the section called “FlexGroup 볼륨 확장” 단원을 참조하십시오.

볼륨 이동 제한

파일 시스템에서 볼륨 이동의 대역폭을 제한하려면 작업을 시작할 때 `-enforce-network-throttling` 옵션을 추가할 수 있습니다.

> **Note**
>
> 이 옵션을 사용하면 파일 시스템의 수신 SnapMirror 복제 데이터 전송에 영향을 미칩니다. 파일 시스템의 복제 옵션을 설정한 후에는 볼 수 없으므로 파일 시스템의 복제 옵션을 구성하는 방법을 추적합니다.

볼륨 이동을 제한하려면

1. 스로틀은 전역 복제 스로틀을 사용합니다. 전역 복제 스로틀을 설정하려면 ONTAP CLI에서 다음 명령을 사용합니다.

   ```
   ::> options -option-name replication.throttle.enable on
   ```

2. 복제에 사용할 수 있는 최대 총 대역폭을 지정하고 다음 옵션을 대체합니다.

   - 모든 복제(SnapMirror 및 볼륨 이동 포함)에 사용할 최대 원하는 처리량(초당 킬로바이트)을 `kbs_throttle`로 설정합니다.

   ```
   ::> options -option-name replication.throttle.incoming.max_kbs kbs_throttle
   ::> options -option-name replication.throttle.outgoing.max_kbs kbs_throttle
   ```

볼륨 모니터링

Amazon FSx 콘솔, 및 Amazon FSx API AWS CLI및 SDKs.

파일 시스템에서 볼륨 모니터링

- 콘솔 사용 - 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 봅니다. 볼륨 탭을 선택하여 파일 시스템의 모든 볼륨을 나열한 다음 보려는 볼륨을 선택합니다.
- CLI 또는 API 사용 - describe-volumes CLI 명령 또는 DescribeVolumes API 작업을 사용합니다.

```
$ aws fsx describe-volumes
{
    "Volumes": [
        {
            "CreationTime": "2024-03-04T20:17:44+00:00",
            "FileSystemId": "fs-abcdef0123a0bb087",
            "Lifecycle": "CREATED",
            "Name": "SVM8_ext_root",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
                "JunctionPath": "/",
                "SecurityStyle": "NTFS",
                "SizeInMegabytes": 1024,
                "StorageEfficiencyEnabled": false,
                "StorageVirtualMachineId": "svm-01234567890abcdef",
                "StorageVirtualMachineRoot": true,
                "TieringPolicy": {
                    "Name": "NONE"
                },
                "UUID": "42ce3de0-da64-11ee-a22d-7f7cdfb8d381",
                "OntapVolumeType": "RW",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
                "VolumeStyle": "FLEXVOL",
                "AggregateConfiguration": {
                    "Aggregates": [
                        "aggr1"
                    ]
                },
                "SizeInBytes": 1073741824
            },
            "ResourceARN": "arn:aws:fsx:us-east-2:111122223333:volume/fs-
abcdef0123a0bb087/fsvol-abcdef0123456789a",
            "VolumeId": "fsvol-abcdef0123456789a",
            "VolumeType": "ONTAP"
        }
    ]
```

```
}
```

오프라인 볼륨 보기

소스 볼륨이 오프라인일 때는 볼륨 백업을 생성하거나 삭제할 수 없습니다. `volume show` ONTAP CLI 명령을 사용하여 볼륨의 현재 상태를 확인할 수 있습니다.

```
volume show -vserver svm-name
```

파일 시스템의 ONTAP CLI에 액세스하는 방법에 대한 자세한 내용은 NetApp ONTAP CLI 사용을 참조하세요.

```
FsxIdabc12345::> volume show -vserver vs1
Vserver   Volume       Aggregate    State      Type       Size  Available Used%
--------- ------------ ------------ ---------- ---- ---------- ---------- -----
vs1       vol1         aggr1        online     RW          2GB      1.9GB    5%
vs1       vol1_dr      aggr0_dp     online     DP        200GB    160.0GB   20%
vs1       vol2         aggr0        online     RW        150GB    110.3GB   26%
vs1       vol2_dr      aggr0_dp     online     DP        150GB    110.3GB   26%
vs1       vol3         aggr1        online     RW        150GB    120.0GB   20%
vs1       vol3_dr      aggr1_dp     online     DP        150GB    120.0GB   20%
vs1       vol4         aggr1        online     RW        200GB    159.8GB   20%
7 entries were displayed.
```

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

볼륨 삭제

ONTAP 명령줄 인터페이스(CLI) 및 REST API 외에도 Amazon FSx FSx 콘솔 AWS CLI, 및 Amazon FSx API를 사용하여 FSx for NetApp ONTAP 볼륨을 삭제할 수 있습니다.

볼륨을 삭제하기 전에 삭제하려는 볼륨의 데이터에 액세스하는 애플리케이션이 없는지 확인합니다.

> **Important**
>
> 볼륨에 Amazon FSx 백업이 활성화된 경우에만 Amazon FSx 콘솔, API 또는 CLI를 사용하여 볼륨을 삭제할 수 있습니다.

최종 볼륨 백업 수행

Amazon FSx 콘솔을 사용하여 볼륨을 삭제하면 볼륨의 최종 백업을 수행할 수 있습니다. 가장 좋은 방법은 최종 백업을 선택하는 것입니다. 일정 시간이 지나도 필요하지 않은 경우 이 백업과 수동으로 만든 다른 볼륨 백업을 삭제할 수 있습니다. `delete-volume` CLI 명령을 사용하여 볼륨을 삭제하면 Amazon FSx는 기본적으로 최종 백업을 수행합니다.

볼륨 백업에 대한 자세한 내용은 섹션을 참조하세요볼륨 백업으로 데이터 보호.

볼륨 삭제(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 볼륨을 삭제할 ONTAP 파일 시스템을 선택합니다.
3. 볼륨 탭을 선택합니다.
4. 삭제하려는 볼륨을 선택합니다.
5. 작업에서 볼륨 삭제를 선택합니다.
6. (SnapLock Enterprise 볼륨만 해당) SnapLock Enterprise Retention을 우회하려면 예를 선택합니다.
7. 확인 대화 상자의 최종 백업 생성의 경우 다음 두 가지 옵션이 있습니다.
   - 볼륨의 최종 백업을 수행하려면 예를 선택합니다. 최종 백업의 이름이 표시됩니다.
   - 볼륨의 최종 백업을 원하지 않으면 아니요를 선택합니다. 볼륨이 삭제되면 자동 백업을 더 이상 사용할 수 없음을 확인하라는 메시지가 표시됩니다.
8. 삭제 확인 필드에 delete를 입력하여 볼륨 삭제를 확인합니다.
9. 볼륨 삭제를 선택합니다.

볼륨 삭제(CLI)

- FSx for ONTAP 볼륨을 삭제하려면 다음 예제와 같이 delete-volume CLI 명령(또는 이에 상응하는 DeleteVolume API 작업)을 사용합니다.

```
aws fsx delete-volume --volume-id fsvol-1234567890abcde
```

SnapLock 볼륨 삭제

이 섹션에서는 SnapLock 볼륨을 삭제하는 방법을 설명합니다.

SnapLock 규정 준수 볼륨은 볼륨 내의 모든 WORM(Write Once Read Many 파일의 보존 기간이 만료되면 삭제할 수 있습니다.

> **Note**
>
> SnapLock Enterprise 또는 Compliance 볼륨 AWS 계정 이 포함된를 닫으면 FSx for ONTAP은 90일 동안 계정을 일시 중지 AWS 하고 데이터는 그대로 둡니다. 이 90일 동안 계정을 다시 열지 않으면는 보존 설정에 관계없이 SnapLock 볼륨의 데이터를 포함한 데이터를 AWS 삭제합니다.

필요한 권한이 있는 경우 언제든지 SnapLock 엔터프라이즈 볼륨을 삭제할 수 있습니다. ONTAP CLI를 사용하여 SnapLock 엔터프라이즈 볼륨을 삭제하려면 `fsxadmin` 역할이 있어야 합니다. 자세한 내용은 파일 시스템 관리자 역할 및 사용자 단원을 참조하십시오.

Amazon FSx 콘솔, CLI 또는 Amazon FSx API를 사용하여 활성 보존 정책이 있는 WORM 데이터가 포함된 SnapLock 엔터프라이즈 볼륨을 삭제하려면 `fsx:BypassSnapLockEnterpriseRetention` IAM 권한이 있어야 합니다.

> **Warning**
>
> SnapLock 감사 로그 볼륨의 최소 보존 기간은 6개월입니다. 이 보존 기간이 만료되기 전까지는 볼륨이 SnapLock 엔터프라이즈 모드에서 생성된 경우에도 SnapLock 감사 로그 볼륨, 스토리지 가상 머신(SVM) 또는 SVM에 연결된 파일 시스템을 삭제할 수 없습니다. 자세한 내용은 SnapLock 감사 로그 볼륨 단원을 참조하십시오.

iSCSI LUN 생성

이 프로세스에서는 NetApp ONTAP CLI lun create 명령을 사용하여 Amazon FSx for NetApp ONTAP 파일 시스템에 iSCSI LUN을 생성하는 방법을 설명합니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 lun create를 참조하세요.

> **Note**
>
> iSCSI 프로토콜은 HA 페어가 6개를 초과하는 파일 시스템에서는 지원되지 않습니다.

이 프로세스에서는 파일 시스템에 이미 볼륨이 생성되어 있다고 가정합니다. 자세한 내용은 볼륨 생성 단원을 참조하십시오.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. lun create NetApp CLI 명령을 사용하여 LUN을 생성하고 다음 값을 바꿉니다.

   - ***svm_name*** – iSCSI 대상을 제공하는 스토리지 가상 머신(SVM)의 이름입니다. 호스트는 이 값을 사용하여 LUN에 도달합니다.
   - ***vol_name*** – LUN을 호스팅하는 볼륨의 이름입니다.
   - ***lun_name*** – LUN에 할당하려는 이름입니다.
   - ***size***- LUN의 크기(바이트)입니다. 생성할 수 있는 최대 LUN 크기는 128TB입니다.

     > **Note**
     >
     > LUN 크기보다 5% 이상 큰 볼륨을 사용하는 것이 좋습니다. 이 여유 공간은 볼륨 스냅샷 용도의 공간입니다.

   - ***ostype*** - 호스트의 운영 체제(`windows_2008` 또는 `linux`)입니다. 모든 Windows 버전에는 `windows_2008`을 사용할 수 있으며, 이를 통해 운영 체제에 적합한 블록 오프셋이 LUN에 지정되고 성능이 최적화됩니다.

> **Note**
>
> LUN에서 공간 할당을 활성화하는 것이 좋습니다. 공간 할당을 활성화하면 LUN의 용량이 부족할 경우 ONTAP이 호스트에 알릴 수 있고 LUN에서 데이터가 삭제되면 공간을 재확보할 수 있습니다.

자세한 내용은 NetApp ONTAP 설명서의 lun create 섹션을 참조하세요.

```
> lun create -vserver svm_name -path /vol/vol_name/lun_name -size size -
ostype ostype -space-allocation enabled
```

```
Created a LUN of size 10g (10737418240)
```

3. LUN이 생성되고 온라인 상태이며 매핑되었는지 확인합니다.

```
> lun show
```

시스템이 다음 출력으로 응답합니다.

```
Vserver   Path                            State   Mapped   Type         Size
--------- ------------------------------- ------- -------- ------------ --------
svm_name
          /vol/vol_name/lun_name          online  unmapped windows_2008 10GB
```

다음 단계

이제 iSCSI LUN을 생성했으므로 iSCSI LUN을 블록 스토리지로 사용하는 프로세스의 다음 단계는 LUN을 igroup에 매핑하는 것입니다. 자세한 내용은 Linux용 iSCSI 프로비저닝 또는 Windows용 iSCSI 프로비저닝을 참조하세요.

Amazon FSx 유지 관리 기간을 통한 성능 최적화

완전관리형 서비스인 FSx for ONTAP은 파일 시스템에 대한 유지 관리 및 업데이트를 정기적으로 수행합니다. 이 유지 관리는 대부분의 워크로드에 영향을 미치지 않습니다. 성능에 민감한 워크로드의 경우, 드물게는 유지 관리가 수행될 때 성능에 일시적인 영향(60초 미만)을 미칠 수 있습니다. Amazon

FSx를 사용하면 유지 관리 기간을 통해 이러한 잠재적 유지 관리 활동이 발생하는 시기를 제어할 수 있습니다.

패치 적용은 드물게 발생하며 일반적인 빈도는 몇 주에 한 번입니다. 패치가 발생하면 각 파일 시스템의 파일 서버에 한 번에 하나씩 패치가 적용되고 각 파일 서버에 패치가 적용되려면 일반적으로 최대 1시간이 걸립니다. 파일 서버가 HA 페어 내에 패치되기 전에 파일 시스템은 파일 서버의 HA 파트너에게 자동으로 장애 조치되므로 해당 HA 페어를 향하는 모든 I/O에 대해 잠시(60초 미만) I/O 일시 중지가 발생할 수 있습니다. 그러면 파일 시스템이 장애 복구되어 또 다른 짧은(60초 미만) I/O 일시 중지가 발생할 수 있습니다. 파일 시스템을 만드는 동안 유지 관리 창 시작 시간을 선택합니다. 창을 선택하지 않으면 창이 자동으로 할당됩니다.

> **Important**
>
> 파일 시스템을 성공적으로 패치할 수 있도록 FSx for ONTAP은 패치 적용 프로세스 기간 동안 오프라인 볼륨을 모두 온라인 상태로 전환합니다. Amazon FSx가 온라인으로 다시 가져오는 모든 볼륨은 클라이언트가 액세스할 수 없습니다.

FSx for ONTAP을 사용하면 워크로드 및 운영 요구 사항에 맞게 유지 관리 기간을 조정할 수 있습니다. 유지 관리 기간이 14일에 한 번 이상 발생한다면 필요한 만큼 자주 유지 관리 기간을 이동할 수 있습니다. 패치가 릴리스되고 14일 이내에 유지보수 기간이 발생하지 않는 경우, FSx for ONTAP는 파일 시스템의 보안과 안정성을 보장하기 위해 유지보수를 진행합니다.

> **Note**
>
> 유지 관리 작업 중 데이터 무결성을 보장하기 위해 FSx for ONTAP은 유지 관리가 시작되기 전에 모든 기회 잠금을 닫고 파일 시스템을 호스팅하는 기본 스토리지 볼륨에 대한 보류 중인 쓰기 작업을 완료합니다.

Amazon FSx Management Console, AWS CLI AWS API 또는 AWS SDKs 중 하나를 사용하여 파일 시스템의 유지 관리 기간을 변경할 수 있습니다.

주별 유지 관리 기간 변경(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 열에서 파일 시스템을 선택합니다.

3. 주별 유지 관리 기간을 변경하려는 파일 시스템을 선택합니다. 요약 파일 시스템 세부 정보 페이지가 표시됩니다.
4. 관리를 선택하면 파일 시스템 관리 설정 패널이 표시됩니다.
5. 업데이트를 선택하면 유지 관리 기간 변경 창이 표시됩니다.
6. 주별 유지 관리 기간을 시작하려는 새 날짜와 시간을 입력합니다.
7. 저장을 선택하여 변경 사항을 저장합니다. 새 유지 관리 시작 시간이 파일 시스템 관리 설정 패널에 표시됩니다.

update-file system CLI 명령을 사용하여 주별 유지 관리 기간을 변경하려면 파일 시스템 업데이트(CLI) 섹션을 참조하세요.

처리량 용량 관리

FSx for ONTAP은 파일 시스템을 생성할 때 처리량 용량을 구성합니다. 언제든지 파일 시스템의 처리량 용량을 수정할 수 있습니다. 파일 시스템의 최대 처리량 용량을 달성하려면 특정 구성이 필요하다는 점에 유의하세요. 예를 들어, 1세대 파일 시스템에 4GBps의 처리량 용량을 프로비저닝하려면 파일 시스템에 최소 5,120GiB의 SSD 스토리지 용량과 160,000 SSD IOPS의 구성이 필요합니다. 자세한 내용은 처리량 용량이 성능에 미치는 영향 단원을 참조하십시오.

처리량 용량은 파일 시스템을 호스팅하는 파일 서버의 파일 데이터 서비스 제공 속도를 결정하는 요소 중 하나입니다. 처리량 용량이 높을수록 네트워크, 초당 디스크 읽기 I/O 작업 수(IOPS) 및 파일 서버의 데이터 캐싱 용량이 높아집니다. 자세한 내용은 성능 단원을 참조하십시오.

파일 시스템의 처리량 용량을 수정하면 Amazon FSx가 파일 시스템을 구동하는 파일 서버를 교체합니다. 단일 AZ 및 다중 AZ 파일 시스템 모두 이 프로세스 중에 자동 장애 조치 및 페일백이 발생하며, 완료하는 데 일반적으로 몇 분 정도 걸립니다. 장애 조치 및 페일백 프로세스는 NFS(네트워크 파일 공유), SMB(서버 메시지 블록) 및 iSCSI(인터넷 소형 컴퓨터 시스템 인터페이스) 클라이언트에서 투명하게 진행되므로 중단이나 수동 개입 없이 워크로드를 계속 실행할 수 있습니다. 새 처리량 용량을 파일 시스템에서 사용할 수 있게 되면 요금이 청구됩니다.

> **Note**
>
> 유지 관리 작업 중 데이터 무결성을 보장하기 위해 FSx for ONTAP은 유지 관리가 시작되기 전에 모든 기회 잠금을 닫고 파일 시스템을 호스팅하는 기본 스토리지 볼륨에 대한 보류 중인 쓰기 작업을 완료합니다. 예약된 파일 시스템 유지 관리 기간 중에는 시스템 수정(예: 처리량 용량 수정)이 지연될 수 있습니다. 시스템 유지 관리로 인해 이러한 변경 사항은 처리될 때까지 대기

열에 추가될 수 있습니다. 자세한 내용은 the section called “유지 관리 기간 업데이트” 단원을 참조하십시오.

주제

처리량 용량을 수정해야 하는 경우

Amazon FSx는 Amazon CloudWatch와 통합되므로 파일 시스템의 지속적인 처리량 사용 수준을 모니터링할 수 있습니다. 파일 시스템을 통해 구동할 수 있는 처리량 및 IOPS 성능은 파일 시스템의 처리량 용량뿐 아니라 특정 워크로드의 특성에 따라 달라집니다. 일반적으로 워크로드의 읽기 처리량과 워크로드의 쓰기 처리량의 두 배를 지원할 수 있는 충분한 처리량 용량을 프로비저닝해야 합니다. CloudWatch 지표를 사용하여 성능 개선을 위해 변경해야 할 측정기준을 결정할 수 있습니다. 자세한 내용은 the section called “Amazon FSx 콘솔에서 모니터링” 단원을 참조하십시오.

동시 요청 처리 방법

1세대 파일 시스템의 경우, SSD 스토리지 용량 및 프로비저닝된 IOPS 업데이트 워크플로우가 시작되기 직전 또는 진행 중에도 처리량 용량 업데이트를 요청할 수 있습니다. Amazon FSx가 두 요청을 처리하는 순서는 다음과 같습니다.

- SSD/IOPS 업데이트와 처리량 용량 업데이트를 동시에 제출하면 두 요청이 모두 수락됩니다. SSD/IOPS 업데이트는 처리량 용량 업데이트 전에 우선 순위가 지정됩니다.
- SSD/IOPS 업데이트가 진행 중인 동안 처리량 용량 업데이트를 제출하면 처리량 용량 업데이트 요청이 수락되고 SSD/IOPS 업데이트 이후에 발생하도록 대기열에 추가됩니다. 처리량 용량 업데이트는 SSD/IOPS가 업데이트된(새 값이 사용 가능하게 된) 후 및 최적화 단계에서 시작됩니다. 이 작업은 일반적으로 10분 정도 걸립니다.
- 처리량 용량 업데이트가 진행 중인 동안 SSD/IOPS 업데이트를 제출하면 SSD/IOPS 스토리지 업데이트 요청이 수락되어 처리량 용량 업데이트가 완료된(새 처리량 용량이 사용 가능하게 된) 후 시작되도록 대기열에 추가됩니다. 이 작업은 일반적으로 20분 정도 걸립니다.

2세대 파일 시스템에 대한 처리량 용량 업데이트를 요청할 때는 다음 사항을 고려하세요.

- 2세대 파일 시스템의 처리량 용량을 업데이트하려면 최소 6시간을 기다려야 합니다.
- 처리량 용량 휴지 기간은 SSD/IOPS 크기 조정과 공유됩니다.
- 처리량 용량 조정 및 SSD/IOPS 조정은 이 진행 중인 동안에는 시뮬레이션 방식으로 수행하거나 대기열에 넣을 수 없습니다.
- 처리량 용량 조정 또는 SSD/IOPS 조정이 진행 중인 동안에는 또는 와 함께 고가용성(HA) 페어를 추가할 수 없습니다. 그러나 HA 페어를 추가해도 SSD/IOPS 조정 및 처리량 용량 조정과 휴지 시간이 공유되지 않습니다. 자세한 내용은 고가용성(HA) 페어 추가 단원을 참조하십시오.

SSD 스토리지 및 프로비저닝된 IOPS 업데이트에 대한 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.

처리량 용량 업데이트

Amazon FSx 콘솔, AWS Command Line Interface (AWS CLI) 또는 Amazon FSx API를 사용하여 파일 시스템의 처리량 용량을 수정할 수 있습니다.

> **Note**
>
> 2세대 파일 시스템의 처리량 용량을 업데이트하려면 최소 6시간을 기다려야 합니다.

파일 시스템의 처리량 용량 수정(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 처리량 용량을 늘리려는 ONTAP 파일 시스템을 선택합니다.
3. 작업에서 처리량 용량 업데이트를 선택합니다. 또는 요약 패널에서 파일 시스템의 처리량 용량 옆에 있는 업데이트를 선택합니다.
4. 목록에서 처리량 용량의 새 값을 선택합니다.
5. 업데이트를 선택하여 처리량 용량 업데이트를 시작합니다.
6. 업데이트 탭의 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다.

   Amazon FSx 콘솔, AWS CLI및 API를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 처리량 용량 변화 모니터링 단원을 참조하십시오.

파일 시스템의 처리량 용량 수정(CLI)

파일 시스템의 처리량 용량을 수정하려면 update-file-system AWS CLI 명령을 사용합니다. 다음 파라미터를 설정합니다.

- `--file-system-id`를 업데이트하려는 파일 시스템의 ID로 설정합니다.
- `ThroughputCapacity`를 파일 시스템을 업데이트하려는 적정 값으로 설정합니다.

Amazon FSx 콘솔, AWS CLI및 API를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 처리량 용량 변화 모니터링 단원을 참조하십시오.

처리량 용량 변화 모니터링

Amazon FSx 콘솔, API 및 AWS CLI를 사용하여 처리량 용량 수정 진행 상황을 모니터링할 수 있습니다.

콘솔에서 처리량 용량 변화 모니터링

파일 시스템 세부 정보 창의 업데이트 탭에서 각 업데이트 작업 유형에 대한 가장 최근의 업데이트 작업 10개를 볼 수 있습니다.

처리량 용량 업데이트 작업에서 다음 정보를 볼 수 있습니다.

업데이트 유형

지원되는 유형은 처리량 용량, 스토리지 용량, 스토리지 최적화입니다.

대상 값

파일 시스템의 처리량 용량을 변경할 적정 값입니다.

상태

업데이트의 현재 상태입니다. 처리량 용량 업데이트에 사용할 수 있는 값은 다음과 같습니다.

- 보류 중 – Amazon FSx가 업데이트 요청을 받았지만 처리를 시작하지 않았습니다.
- 진행 중 – Amazon FSx에서 업데이트 요청을 처리하고 있습니다.
- 완료됨 – 처리량 용량 업데이트가 완료되었습니다.
- 실패 - 처리량 용량 업데이트에 실패했습니다. 처리량 업데이트가 실패한 자세한 이유를 보려면 물음표(?)를 선택합니다.

요청 시간

Amazon FSx가 업데이트 요청을 받은 시간입니다.

AWS CLI 및 API를 사용하여 변경 사항 모니터링

describe-file-systems CLI 명령과 DescribeFileSystems API 작업을 사용하여 파일 시스템 처리량 용량 수정 요청을 보고 모니터링할 수 있습니다. `AdministrativeActions` 배열에 각 관리 작업 유형에 대한 가장 최근의 업데이트 작업 10개가 나열됩니다. 파일 시스템의 처리량 용량을 수정하면 `FILE_SYSTEM_UPDATE` 관리 작업이 생성됩니다.

다음 예제는 `describe-file-systems` CLI 명령의 응답 발췌문을 보여줍니다. 파일 시스템의 처리량 용량은 128MBps이고 목표 처리량 용량은 256MBps입니다.

```
.
.
.
    "ThroughputCapacity": 128,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Amazon FSx가 작업을 처리하면 상태가 `COMPLETED`로 변경됩니다. 그러면 파일 시스템에서 새 처리량 용량을 사용할 수 있으며 `ThroughputCapacity` 속성에 표시됩니다. 이는 describe-file-systems CLI 명령의 다음 응답 발췌문에 나와 있습니다.

```
.
.
.
    "ThroughputCapacity": 256,
"AdministrativeActions": [
    {
```

```
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "COMPLETED",
        "TargetFileSystemValues": {
          "OntapConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

처리량 용량 수정에 실패하면 상태가 FAILED로 변경되고 FailureDetails 속성이 실패에 대한 정보를 제공합니다.

SMB 공유 관리

Amazon FSx 파일 시스템에서 SMB 파일 공유를 관리하기 위해 Microsoft Windows 공유 폴더 GUI를 사용할 수 있습니다. 공유 폴더 GUI는 스토리지 가상 머신(SVM)의 모든 공유 폴더를 관리할 수 있는 중앙 위치를 제공합니다. 다음 절차에서는 파일 공유를 생성, 업데이트 및 제거하는 방법을 자세히 설명합니다.

> **Note**
>
> NetApp 시스템 관리자를 사용하여 SMB 파일 공유를 관리할 수도 있습니다. 자세한 내용은 BlueXP와 함께 NetApp 시스템 관리자 사용 단원을 참조하십시오.

Amazon FSx 파일 시스템에 공유 폴더 연결

1. Amazon EC2 인스턴스를 시작하고 이를 Amazon FSx 파일 시스템이 조인된 Microsoft Active Directory에 연결합니다. 이렇게 하려면 AWS Directory Service 관리 가이드에서 다음 절차 중 하나를 선택합니다.
   - Windows EC2 인스턴스를 원활하게 조인
   - Windows 인스턴스를 수동으로 조인
2. 파일 시스템 관리자 그룹의 구성원인 사용자로 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하세요.
3. 시작 메뉴를 열고 관리자 권한으로 실행을 사용하여 fsmgmt.msc를 실행합니다. 이렇게 하면 공유 폴더 GUI 도구가 열립니다.

4. 작업에서 다른 컴퓨터에 연결을 선택합니다.
5. 다른 컴퓨터의 경우 스토리지 가상 머신(SVM)의 DNS 이름(예: **`netbios_name.corp.example.com`**)을 입력합니다.

   Amazon FSx 콘솔에서 SVM의 DNS 이름을 찾으려면 스토리지 가상 머신을 선택하고 SVM을 선택한 후 SMB DNS 이름을 찾을 때까지 엔드포인트 섹션을 아래로 스크롤합니다. 또한 DescribeStorageVirtualMachines API 작업의 응답에서 DNS 이름을 가져올 수도 있습니다.
6. 확인을 선택합니다. 그러면 Amazon FSx 파일 시스템 항목이 공유 폴더 도구 목록에 표시됩니다.

이제 공유 폴더가 Amazon FSx 파일 시스템에 연결되었으므로 다음 작업을 통해 파일 시스템에서 Windows 파일 공유를 관리할 수 있습니다.

> **Note**
>
> 루트 볼륨이 아닌 다른 볼륨에 SMB 공유를 배치하는 것이 좋습니다.

- 새 파일 공유 생성 - 공유 폴더 도구의 왼쪽 창에서 공유를 선택하여 Amazon FSx 파일 시스템의 활성 공유를 확인합니다. 볼륨은 볼륨 생성 중에 선택한 경로에 마운트된 것으로 표시됩니다. 새 공유를 선택하고 공유 폴더 생성 마법사를 완료합니다.

  새 파일 공유를 생성하기 전에 로컬 폴더를 생성해야 합니다. 이는 다음과 같이 수행할 수 있습니다.

  - 공유 폴더 도구 사용: 로컬 폴더 경로를 지정할 때 찾아보기를 선택하고 새 폴더 만들기를 선택하여 로컬 폴더를 생성합니다.
  - 명령줄 사용:

    ```
    New-Item -Type Directory -Path \\netbios_name.corp.example.com\C
    $volume_path\MyNewFolder
    ```
- 파일 공유 수정 - 공유 폴더 도구의 오른쪽 창에서 수정할 파일 공유의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 속성을 선택합니다. 속성을 수정하고 확인을 선택합니다.
- 파일 공유 제거 - 공유 폴더 도구의 오른쪽 창에서 제거할 파일 공유의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 공유 중지를 선택합니다.

> **Note**
>
> GUI에서 파일 공유 제거는 Amazon FSx 파일 시스템의 DNS 이름을 사용하여 fsmgmt.msc에 연결한 경우에만 가능합니다. 파일 시스템의 IP 주소 또는 DNS 별칭을 사용하여 연결한 경우 공유 중지 옵션이 작동하지 않아 파일 공유가 제거되지 않습니다.

NetApp 애플리케이션을 사용하여 FSx for ONTAP 관리

AWS Management Console AWS CLI및 AWS API와 SDKs 외에도 다음과 같은 NetApp 관리 도구 및 애플리케이션을 사용하여 FSx for ONTAP 리소스를 관리할 수도 있습니다.

주제

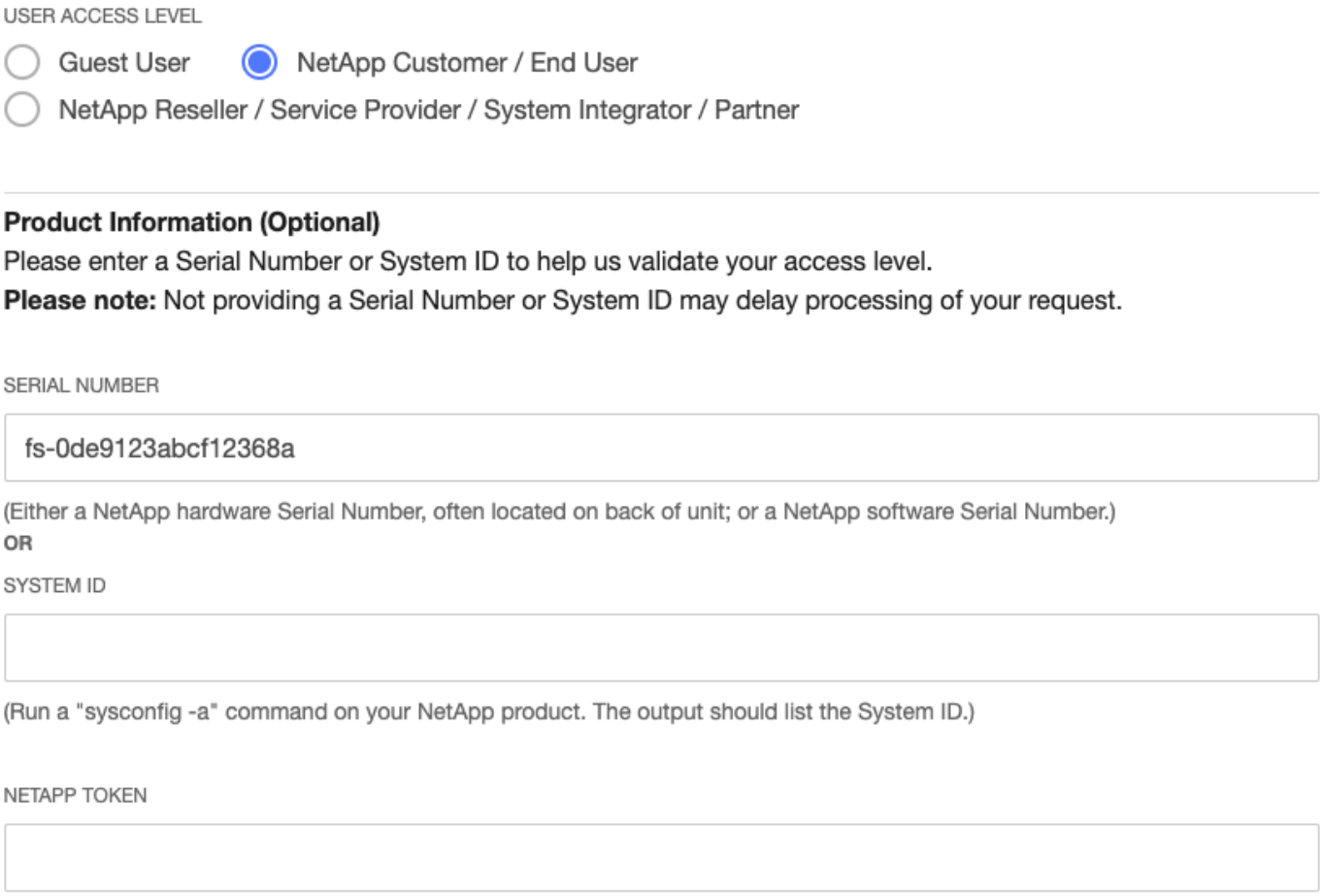
- NetApp 계정 가입
- NetApp BlueXP 사용하기
- NetApp ONTAP CLI 사용
- ONTAP REST API 사용

> **Important**
>
> Amazon FSx는 일관성을 보장하기 위해 ONTAP과 주기적으로 동기화합니다. NetApp 애플리케이션을 사용하여 볼륨을 생성하거나 수정하는 경우 이러한 변경 사항이 AWS Management Console AWS CLI API 및 SDKs.

NetApp 계정 가입

BlueXP, SnapCenter 및 ONTAP 바이러스 백신 커넥터와 같은 일부 NetApp 소프트웨어를 다운로드하려면 NetApp 계정이 있어야 합니다. NetApp 계정에 가입하려면 다음 단계를 수행합니다.

1. NetApp 사용자 등록 페이지로 이동하여 새 NetApp 사용자 계정을 등록합니다.
2. 정보를 양식에 작성합니다. NetApp 고객/최종 사용자 액세스 수준을 선택해야 합니다. 일련 번호 필드에서 FSx for ONTAP 파일 시스템의 파일 시스템 ID를 복사하여 붙여넣습니다. 다음 예제를 참조하세요.



등록 후 기대할 수 있는 사항

기존 NetApp 제품을 보유한 고객은 영업일 기준 1일 이내에 고객 수준 액세스 권한으로 NSS 계정을 레벨업할 수 있습니다. NetApp을 처음 사용하는 고객은 NSS 계정을 고객 수준 액세스 권한으로 레벨업하는 것 외에도 표준 비즈니스 관행에 따라 온보딩됩니다. 파일 시스템 ID를 제공하면 이 프로세스를 신속하게 처리할 수 있습니다. mysupport.netapp.com에 로그인하고 시작 페이지로 이동하여 NSS 계정의 상태를 확인할 수 있습니다. 계정의 액세스 수준은 고객 액세스여야 합니다.

NetApp BlueXP 사용하기

NetApp BlueXP는 온프레미스 및 클라우드 환경 전반에서 스토리지 및 데이터 서비스의 관리 경험을 단순화하는 통합 컨트롤 플레인입니다. BlueXP는 AWS 및 온프레미스에서 ONTAP 배포를 관리, 모니터링 및 자동화할 수 있는 중앙 집중식 사용자 인터페이스를 제공합니다. 자세한 내용은 NetApp BlueXP 설명서 및 Amazon FSx for NetApp ONTAP용 NetApp BlueXP 설명서를 참조하세요.

> **Note**
>
> NetApp BlueXP는 고가용성(HA) 페어가 두 개 이상인 2세대 파일 시스템에서는 지원되지 않습니다.

BlueXP와 함께 NetApp 시스템 관리자 사용

BlueXP에서 직접 System Manager를 사용하여 Amazon FSx for NetApp ONTAP 파일 시스템을 관리할 수 있습니다. BlueXP를 사용하면 익숙한 동일한 System Manager 인터페이스를 사용하여 단일 제어 영역에서 하이브리드 멀티 클라우드 인프라를 관리할 수 있습니다. BlueXP의 다른 기능에 대한 액세스 권한도 있습니다. 자세한 내용은 NetApp ONTAP 설명서의 시스템 관리자와 BlueXP 통합 항목을 참조하세요.

> **Note**
>
> NetApp System Manager는 HA 페어가 두 개 이상인 2세대 파일 시스템에서는 지원되지 않습니다.

NetApp ONTAP CLI 사용

NetApp ONTAP CLI를 사용하여 Amazon FSx for NetApp ONTAP 리소스를 관리할 수 있습니다. 파일 시스템(NetApp ONTAP 클러스터와 유사) 수준 및 SVM 수준에서 리소스를 관리할 수 있습니다.

ONTAP CLI를 사용한 파일 시스템 관리

NetApp ONTAP 클러스터에서 CLI 명령을 실행하는 것과 마찬가지로 FSx for ONTAP 파일 시스템에서 ONTAP CLI 명령을 실행할 수 있습니다. 파일 시스템의 관리 엔드포인트에 대한 보안 쉘(SSH) 연결을 설정하고 `fsxadmin` 사용자 이름과 암호로 로그인하여 파일 시스템의 ONTAP CLI에 액세스합니다. 사용자 지정 생성 흐름 또는를 사용하여 파일 시스템을 생성할 때 `fsxadmin` 암호를 설정할 수 있습니다 AWS CLI. 빠른 생성 옵션을 사용하여 파일 시스템을 생성한 경우 `fsxadmin` 암호가 설정되지 않았으므로 ONTAP CLI에 로그인하려면 암호를 설정해야 합니다. 파일 시스템의 `fsxadmin`, 암호 설정에 대한 자세한 내용은 섹션을 참조하세요파일 시스템 업데이트. Amazon FSx 콘솔의 FSx FSx for ONTAP 파일 시스템 세부 정보 페이지의 관리 탭에서 파일 시스템 관리 엔드포인트의 DNS 이름과 IP 주소를 찾을 수 있습니다.

SSH를 사용하여 파일 시스템의 관리 엔드포인트에 연결하려면 먼저 FSx for ONTAP 파일 시스템과 동일한 VPC의 EC2 인스턴스에 로그인합니다. EC2 인스턴스에 로그인한 후에는 다음 예제와 같이

fsxadmin 사용자 및 암호를 사용하여 파일 시스템의 관리 엔드포인트 IP 주소 또는 DNS 이름에 SSH를 추가합니다.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

샘플 값이 있는 SSH 명령:

```
ec2user $ ssh fsxadmin@198.51.100.0
```

관리 엔드포인트 DNS 이름을 사용하는 SSH 명령:

```
ec2user $ ssh fsxadmin@file-system-management-endpoint-dns-name
```

샘플 DNS 이름을 사용하는 SSH 명령:

```
ec2user $ ssh fsxadmin@management.fs-0abcdef123456789.fsx.us-east-2.aws.com
  Password: fsxadmin_password

This is your first recorded login.
FsxId0abcdef123456789::>
```

fsxadmin에서 사용할 수 있는 ONTAP CLI 명령의 범위

fsxadmin의 관리 보기는 파일 시스템의 모든 SVMs과 볼륨을 포함하는 파일 시스템 수준에 있습니다. fsxadmin 역할은 ONTAP 클러스터 관리자의 역할을 수행합니다. Amazon FSx for NetApp ONTAP 파일 시스템은 완전히 관리되므로 fsxadmin 역할은 사용 가능한 ONTAP CLI 명령의 하위 집합을 실행할 수 있습니다.

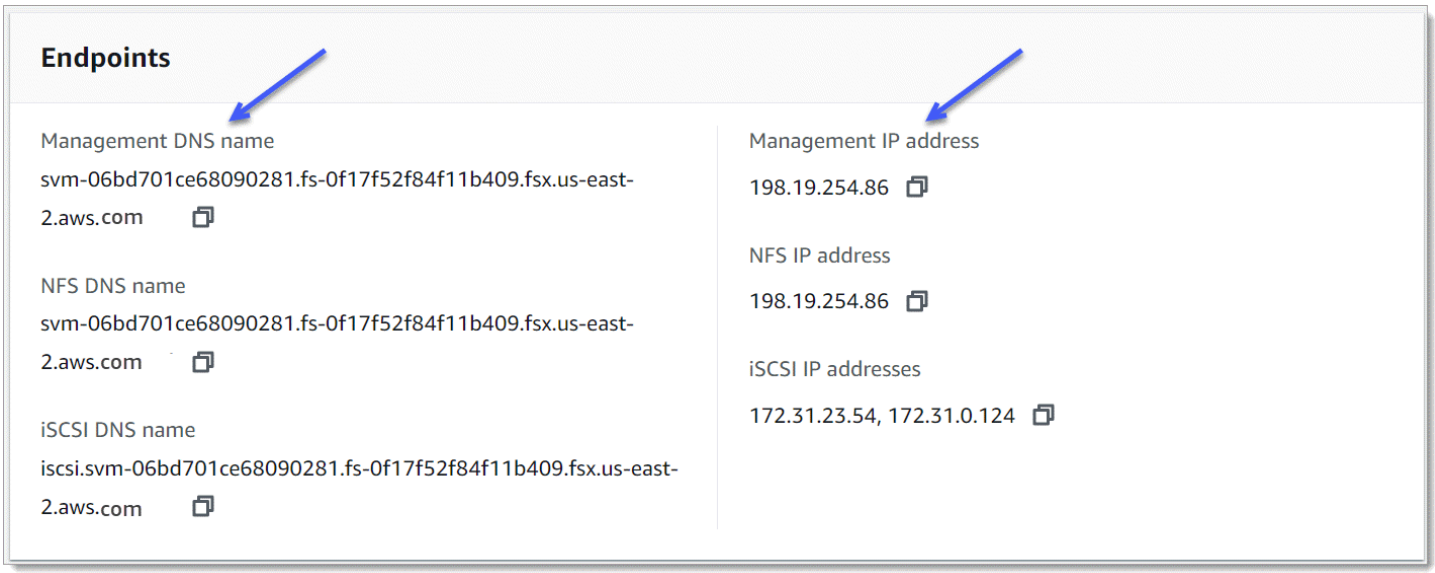
fsxadmin가 실행할 수 있는 명령 목록을 보려면 다음 security login role show ONTAP CLI 명령을 사용하세요.

```
FsxId0abc123def456::> security login role show -role fsxadmin -access !none
           Role          Command/                                  Access
Vserver    Name          Directory                        Query    Level
---------- ------------- --------- ---------------------------------- --------
FsxId0abcdef123456789
           fsxadmin      application                                 all
                         cluster application-record                  all
                         cluster date show                           readonly
                         cluster ha modify                           readonly
                         cluster ha show                             readonly
```

```
                        cluster identity modify                        readonly
                        cluster identity show                          readonly
                        cluster log-forwarding           -port !55555 all
                        cluster modify                                 readonly
                        cluster peer                                   all
                        cluster show                                   readonly
                        cluster statistics show                        readonly
                        cluster time-service ntp server create         readonly
                        cluster time-service ntp server delete         readonly
                        cluster time-service ntp server modify         readonly
                        cluster time-service ntp server show           readonly
                        debug network tcpdump       -ipspace !Cluster all
                        debug san lun                                  all
                        df         -vserver !FsxId* -vserver !Cluster readonly
                        echo                                           all
                        event catalog show                             readonly
                        event config                                   all
.
.
.
378 entries were displayed.
```

ONTAP CLI로 SVM 관리하기

vsadmin 사용자 이름과 암호를 사용하여 SVM의 관리 엔드포인트에 대한 보안 쉘(SSH) 연결을 설정하여 SVM의 ONTAP CLI에 액세스할 수 있습니다. 다음 그림과 같이 Amazon FSx 콘솔의 스토리지 가상 머신 세부 정보 페이지의 엔드포인트 패널에서 SVM의 관리 엔드포인트 DNS 이름과 IP 주소를 찾을 수 있습니다.



SSH를 사용하여 SVM의 관리 엔드포인트에 연결하려면 vsadmin 사용자 이름과 암호를 사용할 수 있습니다. SVM이 생성될 때 vsadmin 사용자의 암호를 설정하지 않은 경우 언제든지 vsadmin 암호를 설정할 수 있습니다. 자세한 내용은 스토리지 가상 머신(SVM) 업데이트 단원을 참조하십시오. 관리 엔드포인트 IP 주소 또는 DNS 이름을 사용하여 파일 시스템과 동일한 VPC에 있는 클라이언트에서 SVM으로 SSH를 설정할 수 있습니다.

```
ssh vsadmin@svm-management-endpoint-ip-address
```

샘플 값이 있는 명령:

```
ssh vsadmin@198.51.100.10
```

관리 엔드포인트 DNS 이름을 사용하는 SSH 명령:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

샘플 DNS 이름을 사용하는 SSH 명령:

```
ssh vsadmin@management.svm-abcdef01234567892fs-0abcdef123456789.fsx.us-east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxId0abcdef123456789::>
```

Amazon FSx for NetApp ONTAP은 NetApp ONTAP CLI 명령을 지원합니다.

NetApp ONTAP CLI 명령에 대한 전체 참조는 ONTAP 명령: 매뉴얼 페이지 참조를 참조하세요.

ONTAP REST API 사용

fsxadmin 자격 증명을 사용하여 ONTAP REST API를 사용하여 FSx for ONTAP 파일 시스템에 액세스할 때는 다음 중 하나를 수행합니다.

- TLS 검증을 비활성화합니다.

  Or

- AWS 인증 기관(CAs) 신뢰 - 각 리전의 CAs에 대한 인증서 번들은 다음 URLs

- 퍼블릭용 https://fsx-aws-certificates.s3.amazonaws.com/bundle-*aws-region*.pem AWS 리전
- https://fsx-aws-us-gov-certificates.s3.us-gov-west-1.amazonaws.com/bundle-*aws-region*.pem for AWS GovCloud 리전
- AWS 중국 리전의 경우 https://fsx-aws-cn-certificates.s3.cn-north-1.amazonaws.com.cn/bundle-*aws-region*.pem

NetApp ONTAP REST API 명령에 대한 전체 참조는 NetApp ONTAP REST API 온라인 참조를 참조하세요.

Amazon FSx 리소스 태그 지정

파일 시스템 및 기타 Amazon FSx 리소스 관리를 돕기 위해 태그 형식으로 각 리소스에 고유한 메타데이터를 할당할 수 있습니다. 태그를 사용하면 용도, 소유자 또는 환경 등 다양한 방식으로 AWS 리소스를 분류할 수 있습니다. 이 분류는 동일 유형의 리소스가 많을 때 유용합니다. 지정한 태그에 따라 특정 리소스를 빠르게 식별할 수 있습니다. 이 주제에서는 태그를 설명하고 태그를 생성하는 방법을 보여줍니다.

주제

태그 기본 사항

태그는 AWS 리소스에 할당하는 레이블입니다. 각 태그는 다음과 같이 사용자가 정의하는 두 부분으로 구성됩니다.

- 태그 키(예: `CostCenter`, `Environment` 또는 `Project`). 태그 키는 대/소문자를 구별합니다.
- 태그 값(예: `111122223333` 또는 `Production`). 태그 키처럼 태그 값은 대/소문자를 구별합니다. 태그 값은 선택 사항입니다.

태그를 사용하여 용도, 소유자 또는 환경별로 AWS 리소스를 다양한 방식으로 분류할 수 있습니다. 예를 들어, 계정의 Amazon FSx 파일 시스템에 대해 각 인스턴스의 소유자나 스택 수준을 추적하는 데 도움이 되는 태그 세트를 정의할 수 있습니다.

각 리소스 유형에 대한 요건을 충족하는 태그 키 세트를 고안하는 것이 좋습니다. 일관된 태그 키 세트를 사용하면 리소스를 보다 쉽게 관리할 수 있습니다. 추가하는 태그에 따라 리소스를 검색하고 필터링할 수 있습니다. 효과적인 리소스 태그 지정 전략을 구현하는 방법에 대한 자세한 내용은의 AWS 리소스 태그 지정을 참조하세요AWS 일반 참조.

유의해야 할 몇 가지 태그 지정 동작은 다음과 같습니다.

- 태그는 Amazon FSx에는 의미가 없으며 엄격하게 문자열로 해석됩니다.
- 태그가 리소스에 자동으로 할당되는 것은 아닙니다.
- 태그 키와 값을 편집할 수 있으며 언제든지 리소스에서 태그를 제거할 수 있습니다.
- 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 `null`로 설정할 수는 없습니다.
- 해당 리소스에 대해 키가 기존 태그와 동일한 태그를 추가하는 경우 새 값이 이전 값을 덮어씁니다.
- 리소스를 삭제하면 리소스 태그도 삭제됩니다.
- Amazon FSx API, AWS Command Line Interface (AWS CLI) 또는 AWS SDK를 사용하는 경우 다음을 수행할 수 있습니다.
  - `TagResource` API 작업을 사용하여 기존 리소스에 태그를 적용할 수 있습니다.
  - 일부 리소스 생성 작업에서 리소스 생성 시 리소스에 태그를 지정할 수 있습니다. 생성 시 리소스에 태그를 지정하면 리소스 생성 후 사용자 지정 태그 지정 스크립트를 실행할 필요가 없습니다.

    리소스 생성 도중 태그를 적용할 수 없는 경우 Amazon FSx는 리소스 생성 프로세스를 롤백합니다. 이 동작은 태그를 사용하여 리소스가 생성되거나 아예 리소스가 생성되지 않도록 하고 언제든 태그가 지정되지 않은 리소스가 남지 않게 합니다.

    > **Note**
    >
    > 사용자가 생성 시 리소스에 태그를 지정하려면 특정 AWS Identity and Access Management (IAM) 권한이 필요합니다. 자세한 내용은 생성 시 리소스 태그 지정에 대한 권한 부여 단원을 참조하십시오.

리소스 태그 지정

계정에 존재하는 Amazon FSx 리소스에 태그를 지정할 수 있습니다. Amazon FSx 콘솔을 사용하는 경우, 관련 리소스 화면에서 태그 탭을 사용하여 리소스에 태그를 적용할 수 있습니다. 리소스를 생성할 때 이름 키를 값과 함께 적용할 수 있으며, 새 파일 시스템을 생성할 때 원하는 태그를 적용할 수 있습니다. 그러나 콘솔이 이름 키에 따라 리소스를 조직할 수 있지만 이 키는 Amazon FSx 서비스에 대한 의미가 없습니다.

생성 시 태그 지정을 지원하는 Amazon FSx API 작업에 IAM 정책의 태그 기반 리소스 수준 권한을 적용하여 생성 시 리소스에 태그를 지정할 수 있는 사용자와 그룹을 세밀하게 제어할 수 있습니다. 정책에 이러한 권한을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

- 리소스는 생성 시점부터 적절하게 보호됩니다.
- 리소스에 태그가 즉시 적용되기 때문에 태그를 기반으로 리소스 사용을 제어하는 리소스 수준 권한이 즉시 발효됩니다.
- 이에 따라 더욱 정확한 리소스 추적 및 보고가 가능합니다.
- 새 리소스에서 태그 지정 사용을 적용하고 리소스에서 어떤 태그 키와 값이 설정되는지 제어할 수 있습니다.

IAM 정책에서 `TagResource` 및 `UntagResource` Amazon FSx API 작업에 리소스 수준 권한을 적용하여 기존 리소스에서 어떤 태그 키와 값이 설정되는지 제어할 수도 있습니다.

생성 시 Amazon FSx 리소스에 태그를 지정하는 데 필요한 권한에 대한 자세한 내용은 생성 시 리소스 태그 지정에 대한 권한 부여 섹션을 참조하세요.

IAM 정책에서 태그를 사용하여 Amazon FSx에 대한 액세스를 제한하는 방법에 대한 자세한 내용은 태그를 사용하여 Amazon FSx 리소스에 대한 액세스 제어 섹션을 참조하세요.

결제를 위한 리소스 태그 지정에 대한 자세한 내용은 AWS Billing 사용 설명서에서 비용 할당 태그 사용을 참조하세요.

백업에 태그 복사

Amazon FSx API에서 볼륨을 생성하거나 업데이트할 때가 볼륨에서 백업`CopyTagsToBackups`으로 태그를 자동으로 복사하도록 할 AWS CLI수 있습니다.

> **Note**
>
> 사용자 시작 백업을 생성할 때 태그를 지정하는 경우(Amazon FSx 콘솔을 사용하여 백업을 생성할 때 이름 태그 포함), CopyTagsToBackups를 활성화한 경우에도 볼륨에서 태그가 복사되지 않습니다.

백업에 대한 자세한 내용은 볼륨 백업으로 데이터 보호 섹션을 참조하세요. CopyTagsToBackups 활성화에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 사용 설명서의 볼륨 생성(CLI) 및 볼륨의 구성 업데이트(CLI) 또는Amazon FSx for NetApp ONTAP API 참조의 CreateVolume 및 UpdateVolume을 참조하세요.

태그 제한

태그에 적용되는 기본 제한은 다음과 같습니다.

- 리소스당 최대 태그 수는 50개입니다.
- 키의 최대 길이는 UTF-8 형식의 유니코드 문자 128자입니다.
- 값의 최대 길이는 UTF-8 형식의 유니코드 문자 256자입니다.
- 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 숫자 및 공백과 다음 문자들입니다. + -(하이픈) = . _(밑줄) : / @.
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 값만 가질 수 있습니다.
- 태그 키와 값은 대소문자를 구분합니다.
- aws: 접두사는 AWS 사용을 위해 예약되어 있습니다. 태그에 이 접두사가 있는 태그 키가 있는 경우 태그의 키 또는 값을 편집하거나 삭제할 수 없습니다. aws: 접두사가 지정된 태그는 리소스당 태그 수 제한에 포함되지 않습니다.

태그에만 기초하여 리소스를 삭제할 수 없습니다. 리소스 식별자를 지정해야 합니다. 예를 들어 DeleteMe라는 태그 키로 태그를 지정한 파일 시스템을 삭제하려면 해당 파일 시스템 리소스 식별자(예: fs-1234567890abcdef0)를 지정하여 DeleteFileSystem 작업을 사용해야 합니다.

퍼블릭 또는 공유 리소스에 태그를 지정할 때 할당하는 태그는 에서만 사용할 수 AWS 계정있으며 다른 AWS 계정 태그는 해당 태그에 액세스할 수 없습니다. 공유 리소스에 대한 태그 기반 액세스 제어를 위해 각는 리소스에 대한 액세스를 제어하기 위해 자체 태그 세트를 할당 AWS 계정 해야 합니다.

권한 및 태그 지정

생성 시 Amazon FSx 리소스에 태그를 지정하는 데 필요한 권한에 대한 자세한 내용은 생성 시 리소스 태그 지정에 대한 권한 부여 섹션을 참조하세요.

IAM 정책에서 태그를 사용하여 Amazon FSx에 대한 액세스를 제한하는 방법에 대한 자세한 내용은 태그를 사용하여 Amazon FSx 리소스에 대한 액세스 제어 섹션을 참조하세요.

데이터 보호

Amazon FSx를 사용하면 파일 시스템의 데이터를 자동으로 복제하여 높은 내구성을 보장하는 것 외에도 데이터를 추가로 보호하는 데 사용할 수 있는 다음과 같은 옵션도 있습니다.

- Amazon FSx 내에서 백업 보존 및 규정 준수 요구 사항을 지원하는 기본 Amazon FSx 볼륨 백업입니다.
- AWS Backup 를 사용하여 여러에서 중앙 관리형 자동 백업 및 보존 전략을 구현합니다 AWS 서비스.
- 파일을 이전 버전으로 복원하여 사용자가 원치 않는 파일 변경을 쉽게 취소할 수 있게 해주는 스냅샷입니다.
- SnapLock를 사용하여 지정된 보존 기간 동안 파일 수정 또는 삭제를 방지하기 위해 WORM(Write One, Read Many) 스토리지 볼륨을 한 번 생성합니다.
- FlexCache 볼륨은 대부분 변경되지 않는 데이터를 사용하여 읽기 작업이 많은 워크로드에 스토리지 효율적이고 비용 효율적인 고성능 데이터 복제를 제공합니다.
- SnapMirror를 사용하여 데이터 보호 및 재해 복구를 위해 두 번째 파일 시스템으로 예약된 자동 파일 시스템 복제를 생성합니다.

주제

볼륨 백업으로 데이터 보호

FSx for ONTAP를 사용하면 파일 시스템의 볼륨을 매일 자동 백업하고 사용자가 직접 백업을 수행하여 데이터를 보호할 수 있습니다. 볼륨을 정기적으로 백업하는 것은 데이터 보존 및 규정 준수 요구 사항을 지원하는 데 도움이 되는 모범 사례입니다. 백업이 저장된 AWS 리전 동일한에 있는 액세스 권한이 있는 기존 FSx for ONTAP 파일 시스템으로 볼륨 백업을 복원할 수 있습니다. Amazon FSx 백업을 사용하면 볼륨의 백업을 쉽게 생성, 보기, 복원 및 삭제할 수 있습니다.

Amazon FSx는 읽기-쓰기(RW)의 `OntapVolumeType`로 ONTAP 볼륨 백업을 지원합니다.

> **Note**
>
> Amazon FSx는 FlexCache 및에 대한 데이터 보호(DP) 볼륨, 로드 공유 미러(LSM) 볼륨 또는 대상 볼륨 백업을 지원하지 않습니다SnapMirror.

주제

백업 작동 방식

모든 Amazon FSx 백업(자동 일일 백업 및 사용자 시작 백업)은 증분식이므로 이전 백업이 완료된 이후의 데이터 변경 사항만 저장합니다. 이렇게 하면 백업을 생성하는 데 필요한 시간과 각 백업에서 사용하는 스토리지 양이 모두 최소화됩니다. 증분 백업은 중복 데이터를 저장하지 않음으로써 스토리지 비용을 최적화합니다. FSx for ONTAP 백업은 볼륨당이며 각 백업에는 하나의 특정 볼륨의 데이터만 포함됩니다. Amazon FSx 백업은 높은 내구성을 달성하기 위해 여러 가용 영역에 중복 저장됩니다.

Amazon FSx 백업은 특정 시점의 읽기 전용 볼륨 이미지인 스냅샷을 사용하여 백업 간 증분성을 유지합니다. 백업을 수행할 때마다 Amazon FSx는 먼저 볼륨의 스냅샷을 생성합니다. 백업 스냅샷은 볼륨

에 저장되며 볼륨의 스토리지 공간을 사용합니다. 그러면 Amazon FSx는 이 스냅샷을 이전 백업 스냅샷(있는 경우)과 비교하여 변경된 데이터만 백업에 복사합니다.

이전 백업 스냅샷이 없는 경우 가장 최근 백업 스냅샷의 전체 콘텐츠가 백업에 복사됩니다. 최신 백업 스냅샷을 성공적으로 생성한 후 Amazon FSx는 이전 백업 스냅샷을 삭제합니다. 최신 백업에 사용된 스냅샷은 프로세스가 반복되면 다음 백업이 생성될 때까지 볼륨에 남아 있습니다. 백업 스토리지 비용을 최적화하기 위해 ONTAP는 백업에서 볼륨의 스토리지 효율성 절감을 유지합니다.

백업을 삭제하면 해당 백업에 고유한 데이터만 삭제됩니다. 각 Amazon FSx 백업에는 백업의 새 볼륨을 생성하는 데 필요한 모든 정보가 포함되어 있어 볼륨의 특정 시점 스냅샷을 효과적으로 복원합니다.

볼륨당 AWS 계정 및 볼륨당 저장할 수 있는 백업 수에는 제한이 있습니다. 자세한 내용은 늘릴 수 있는 할당량 및 각 파일 시스템의 리소스 할당량 섹션을 참조하세요.

스토리지 요구 사항

볼륨과 파일 시스템에는 백업 스냅샷을 저장할 수 있는 충분한 SSD 스토리지 용량이 있어야 합니다. 백업 스냅샷을 찍을 때 스냅샷에 사용되는 추가 스토리지 용량으로 인해 볼륨이 98%의 SSD 스토리지 사용률을 초과할 수 없습니다. 이 경우 백업이 실패합니다. 언제든지 볼륨 또는 파일 시스템의 SSD 스토리지를 늘려 백업이 중단되지 않도록 할 수 있습니다.

자동 일별 백업.

파일 시스템을 생성하면 파일 시스템의 볼륨에 대해 자동 일일 백업이 기본적으로 활성화됩니다. 언제든지 기존 파일 시스템에 대한 자동 일일 백업을 활성화하거나 비활성화할 수 있습니다. 모든 볼륨에 대한 자동 일일 백업은 파일 시스템의 일일 백업 기간 동안 발생하며, 파일 시스템을 생성할 때 자동으로 설정됩니다. 언제든지 일일 백업 기간을 수정할 수 있습니다. 최적의 백업 성능을 위해 클라이언트와 애플리케이션이 볼륨의 데이터에 액세스할 때 정상 운영 시간을 벗어나는 일일 백업 기간을 선택하는 것이 좋습니다.

콘솔을 사용하여 파일 시스템을 생성할 때 또는 언제든지 자동 일일 백업의 보존 기간을 1~90일의 값으로 설정할 수 있습니다. 기본 일일 자동 백업 보존 기간은 30일입니다. Amazon FSx는 보존 기간이 만료되면 자동 일일 백업을 삭제합니다. AWS CLI 및 API를 사용하여 보존 기간을 0~90일의 값으로 설정할 수 있습니다. 0으로 설정하면 자동 일일 백업이 꺼집니다.

자동 일일 백업, 일일 백업 기간 및 백업 보존 기간은 파일 시스템 설정으로, 파일 시스템의 모든 볼륨에 적용됩니다. Amazon FSx 콘솔, AWS CLI또는 API를 사용하여 이러한 설정을 변경할 수 있습니다. 자세한 내용은 파일 시스템 업데이트 단원을 참조하십시오.

볼륨이 오프라인 상태인 경우 볼륨 백업(자동 일일 백업 또는 사용자 시작 백업)을 생성할 수 없습니다. 자세한 내용은 오프라인 볼륨 보기 단원을 참조하십시오.

> **Note**
>
> 자동 일일 백업의 최대 보존 기간은 90일이지만를 사용하여 생성된 백업을 포함하여 사용자가 생성한 사용자 시작 백업 AWS Backup은 사용자가 AWS Backup 삭제하지 않는 한 영구적으로 보존됩니다.

Amazon FSx 콘솔, CLI 및 API를 사용하여 자동 일일 백업을 수동으로 삭제할 수 있습니다. 볼륨을 삭제하면 해당 볼륨에 대한 자동 일일 백업도 삭제됩니다. Amazon FSx는 볼륨을 삭제하기 전에 볼륨의 최종 백업을 생성하는 옵션을 제공합니다. 최종 백업은 삭제하지 않는 한 영구적으로 유지됩니다.

사용자 시작 백업

Amazon FSx를 사용하면 , AWS Management Console AWS CLI및 API를 사용하여 언제든지 파일 시스템 볼륨의 백업을 수동으로 수행할 수 있습니다. 사용자가 시작한 백업은 볼륨에 대해 생성되었을 수 있고 삭제하지 않는 한 영구적으로 보존되는 다른 백업에 비해 증분식입니다. 사용자가 시작한 백업은 백업이 생성된 볼륨이나 파일 시스템을 삭제한 후에도 유지됩니다. Amazon FSx 콘솔, API 또는 CLI를 사용해야만 사용자 시작 백업 삭제를 할 수 있습니다. Amazon FSx는 사용자 시작 백업을 자동으로 삭제하지 않습니다.

사용자 시작 백업을 생성하는 방법에 대한 지침은 사용자 시작 백업 생성을 참조하세요.

백업에 태그 복사

CLI 또는 API를 사용하여 볼륨을 만들거나 업데이트할 때 백업으로 볼륨의 모든 태그를 자동으로 복사하도록 `CopyTagsToBackups`를 활성화할 수 있습니다. 그러나 콘솔을 사용할 때 백업 이름 지정을 포함하여 사용자 시작 백업을 생성하는 동안 태그를 추가하는 경우 Amazon FSx는 `CopyTagsToBackups`이 활성화된 경우에도 볼륨에서 태그를 복사하지 않습니다.

Amazon FSx AWS Backup 에서 사용

AWS Backup 는 Amazon FSx for NetApp ONTAP 볼륨을 백업하여 데이터를 보호하는 간단하고 비용 효율적인 방법입니다. AWS Backup 는 백업의 생성, 복원 및 삭제를 간소화하는 동시에 향상된 보고 및 감사를 제공하도록 설계된 통합 백업 서비스입니다. AWS Backup 를 사용하면 법률, 규제 및 전문 규정 준수를 위한 중앙 집중식 백업 전략을 더 쉽게 개발할 수 있습니다. 또한 다음을 수행할 수 있는 중

앙 위치를 제공하여 AWS 스토리지 볼륨, 데이터베이스 및 파일 시스템을 더 간단하게 보호할 수 있습니다.

- 백업하려는 AWS 리소스를 구성하고 감사합니다.
- 백업 예약을 자동화합니다.
- 보존 정책을 설정합니다.
- 최근의 모든 백업, 복사 및 복원 활동을 모니터링합니다.

AWS Backup 는 Amazon FSx의 기본 제공 백업 기능을 사용합니다. AWS Backup 콘솔을 사용하여 생성된 백업은 파일 시스템 일관성 및 성능이 동일하고, 볼륨에서 가져온 다른 Amazon FSx 사용자 시작 백업에 비해 증분적이며, Amazon FSx 콘솔을 사용하여 만든 백업과 동일한 복원 옵션을 제공합니다. AWS Backup 를 사용하여 이러한 백업을 관리하면 1시간마다 예약 백업을 생성할 수 있는 기능 등 추가 기능이 제공됩니다. 백업 저장소에 백업을 저장하여 백업이 의도치 않거나 악의적으로 삭제되지 않도록 보호하기 위해 추가 방어 계층을 추가할 수 있습니다.

에서 생성한 백업 AWS Backup 은 사용자가 시작한 백업으로 간주되며 Amazon FSx에 대한 사용자 시작 백업 할당량에 포함됩니다. 자세한 내용은 늘릴 수 있는 할당량 단원을 참조하십시오. Amazon FSx 콘솔, CLI 및 API를 AWS Backup 사용하여 생성된 백업을 보고 복원할 수 있습니다. 그러나 Amazon FSx 콘솔, CLI 또는 API AWS Backup 에서가 생성한 백업은 삭제할 수 없습니다. 자세한 내용은 AWS Backup 개발자 안내서의 시작하기 AWS Backup를 참조하세요.

AWS Backup 는 오프라인 볼륨을 백업할 수 없습니다.

태그를 사용하여 백업 계획에서 보호되는 FSx for ONTAP 리소스를 선택할 수 있습니다. 이러한 태그는 파일 시스템 수준 전체가 아닌 볼륨 수준에서 적용해야 합니다. 자세한 내용은 AWS Backup 개발자 안내서의 백업 계획에 리소스 할당을 참조하세요.

백업을 새 볼륨으로 복원

볼륨 백업을 백업이 저장된 AWS 리전 와 동일한 파일 시스템의 새 볼륨으로 복원할 수 있습니다. 백업과 다른에 있는 파일 시스템으로 백업을 복원할 AWS 리전 수 없습니다.

2세대 FSx for ONTAP 파일 시스템에서 백업을 복원할 때 클라이언트는 복원되는 동안 볼륨에서 데이터를 탑하고 읽을 수 있습니다. 클라이언트는 복원 중인 볼륨을 탑재하고 Amazon FSx가 모든 메타데이터를 새 볼륨에 로드하고 볼륨이 CREATED의 수명 주기 상태를 보고하면 파일 데이터를 읽을 수 있습니다. Amazon FSx 콘솔의 볼륨 세부 정보 페이지와 describe-volumes CLI 명령의 응답에서 볼륨의 수명 주기 상태를 찾을 수 있습니다.

백업에서 복원되는 동안 볼륨에서 데이터를 읽을 때 데이터가 아직 볼륨에 다운로드되지 않은 경우 첫 번째 액세스에 대해 최대 10밀리초의 읽기 지연 시간이 발생합니다. 이러한 읽기는 SSD 계층에 캐시되며 후속 읽기에 대해 밀리초 미만의 읽기 지연 시간을 예상할 수 있습니다.

Amazon FSx가 읽기 전용 액세스에 볼륨을 사용할 수 있도록 하는 데 걸리는 시간은 백업에 저장된 파일 메타데이터의 양에 비례합니다. 파일 메타데이터는 일반적으로 데이터 세트의 평균 파일 크기에 따라 전체 백업 데이터의 1~7%를 소비합니다(작은 파일 데이터 세트는 대용량 파일 데이터 세트보다 더 많은 메타데이터를 소비함).

FlexGroup 볼륨 백업을 원래 파일 시스템과 고가용성(HA) 페어 수가 다른 파일 시스템으로 복원하면 Amazon FSx는 구성 요소가 균등하게 분산되도록 구성 요소 볼륨을 추가합니다.

> **Note**
>
> Amazon FSx는 1세대 파일 시스템의 볼륨 또는 볼륨에 대한 백업에서 SnapLock 볼륨이 복원되는 동안 데이터에 대한 읽기 액세스를 지원하지 않습니다. 이러한 백업을 복원하면 복원 프로세스가 완료되면 볼륨을 사용하여 데이터를 탑재하고 액세스할 수 있으며 모든 메타데이터와 데이터가 새 볼륨에 로드됩니다.

백업을 복원할 때 모든 데이터는 처음에 SSD 스토리지 계층에 기록됩니다. 복원이 진행되는 동안 데이터는 복원되는 볼륨의 계층화 정책에 따라 용량 풀 스토리지로 계층화됩니다. 데이터가 SSD 계층에 처음 기록되므로 파일 시스템에 SSD 스토리지 공간이 부족하면 Amazon FSx가 복원 프로세스를 일시 중지합니다. 복원은 프로세스를 계속할 수 있는 충분한 SSD 공간이 확보되는 즉시 자동으로 재개됩니다. 복원된 볼륨의 계층화 정책이 `All`인 경우 주기적 백그라운드 프로세스는 데이터를 용량 풀로 계층화합니다. 복원된 볼륨의 계층화 정책이 `Snapshot Only` 또는 `Auto`인 경우 파일 시스템의 SSD 사용률이 50%보다 크면 데이터가 용량 풀로 계층화되고 냉각 속도는 계층화 정책의 냉각 기간에 따라 결정됩니다.

2세대 파일 시스템의 새 볼륨에 백업을 복원할 때 워크로드에 밀리초 미만의 읽기 대기 시간이 지속적으로 필요한 경우, 복원을 시작할 때 볼륨의 계층화 정책을 None로 설정한 다음 모든 데이터가 볼륨에 완전히 다운로드될 때까지 기다렸다가 액세스하는 것이 좋습니다. 모든 데이터는 SSD 스토리지에 로드된 후 액세스하려고 하므로 데이터에 대한 지연 시간이 짧은 일관된 액세스가 가능합니다.

백업을 새 볼륨으로 복원하는 방법에 대한 단계별 지침은 백업을 새 볼륨으로 복원을 참조하세요.

2세대 파일 시스템에서는 전체 복원 작업이 완료될 때까지 기다릴 필요 없이 백업에서 데이터 하위 집합만 복원할 수도 있습니다. 백업 데이터의 하위 집합만 복원하면 데이터가 실수로 삭제, 수정 또는 손

상된 경우 작업을 더 빠르게 재개할 수 있습니다. 자세한 내용은 데이터 하위 집합 복원 단원을 참조하십시오.

AWS Management Console AWS CLI및 API의 2세대 파일 시스템에서 백업을 복원할 때 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 백업 복원 시 진행 상황 모니터링 단원을 참조하십시오.

> **Note**
>
> - 볼륨 스냅샷을 생성하거나 복제, SnapMirror 복제 및 백업에서 복원되는 볼륨의 백업 생성과 같은 스냅샷 기반 작업을 수행할 수 없습니다.
> - 복원된 볼륨은 항상 원래 볼륨과 동일한 볼륨 스타일을 갖습니다. 복원할 때는 볼륨 스타일을 변경할 수 없습니다.

백업 및 복원 성능

다양한 요인이 백업 및 복원 작업의 성능에 영향을 미칠 수 있습니다. 백업 및 복원 작업은 백그라운드 프로세스이므로 클라이언트 IO 작업에 비해 우선 순위가 낮습니다. 클라이언트 IO 작업에는 NFS, CIFS, iSCSI 데이터 및 메타데이터 읽기 및 쓰기가 포함됩니다. 모든 백그라운드 프로세스는 파일 시스템의 처리 용량 중 사용하지 않는 부분만 사용하며, 백업의 크기와 파일 시스템의 미사용 처리 용량에 따라 완료하는 데 몇 분에서 몇 시간까지 걸릴 수 있습니다.

백업 및 복원 성능에 영향을 미치는 다른 요인에는 데이터가 저장되는 스토리지 계층과 데이터 세트 프로파일이 포함됩니다. 대부분의 데이터가 SSD 스토리지에 있는 경우 볼륨의 첫 번째 백업을 생성하는 것이 좋습니다. 대부분 작은 파일을 포함하는 데이터 세트는 일반적으로 대부분 큰 파일을 포함하는 비슷한 크기의 데이터 세트에 비해 성능이 떨어집니다. 이는 많은 수의 작은 파일을 처리하면 더 적은 수의 큰 파일을 처리하는 것보다 더 많은 CPU 주기와 네트워크 오버헤드를 소비하기 때문입니다.

일반적으로 SSD 스토리지 계층에 저장된 데이터를 백업할 때 다음과 같은 백업 속도를 예상할 수 있습니다.

- 대부분 대용량 파일이 포함된 여러 동시 백업에서 750MBps.
- 대부분 작은 파일을 포함하는 여러 동시 백업에서 100MBps.

일반적으로 다음과 같은 복원 속도를 예상할 수 있습니다.

- 대부분 대용량 파일을 포함하는 여러 동시 복원에서 250MBps.
- 대부분 작은 파일을 포함하는 여러 동시 복원에서 100MBps.

SnapLock 볼륨 백업

추가 데이터 보호를 위해 SnapLock 볼륨을 백업할 수 있습니다. SnapLock 볼륨을 복원할 때 볼륨의 원래 설정(예: 기본 보존, 최소 보존, 최대 보존)이 유지됩니다. Write once, read many(WORM) 설정 및 법적 보존도 유지됩니다.

> **Note**
>
> SnapLock FlexGroup 볼륨은 백업할 수 없습니다.

SnapLock 볼륨의 백업을 SnapLock 또는 비 SnapLock 볼륨으로 복원할 수 있습니다. 그러나 비 SnapLock 볼륨의 백업을 SnapLock 볼륨으로 복원할 수는 없습니다.

자세한 내용은 SnapLock 작동 방법 단원을 참조하십시오.

사용자 시작 백업 생성

다음 절차에서는 사용자가 시작한 볼륨 백업을 생성하는 방법을 설명합니다.

볼륨이 오프라인인 경우 볼륨 백업을 생성할 수 없습니다. 자세한 내용은 오프라인 볼륨 보기 단원을 참조하십시오.

사용자 시작 백업을 생성하려면(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 볼륨을 백업할 ONTAP 파일 시스템을 선택합니다.
3. 볼륨 탭을 선택합니다.
4. 백업할 볼륨을 선택합니다.
5. 작업에서 백업 생성을 선택합니다.
6. 열리는 백업 생성 대화 상자에서 백업 이름을 입력합니다. 백업 이름은 문자, 공백, 숫자 및 특수 문자 + - = _:/를 포함한 최대 256자의 유니코드 문자입니다.
7. 백업 생성을 선택합니다.

이제 파일 시스템 볼륨 중 하나의 백업이 생성되었습니다. 왼쪽 탐색에서 백업을 선택하면 Amazon FSx 콘솔에서 모든 백업을 볼 수 있습니다. 백업에 지정한 이름을 검색할 수 있으며, 테이블은 일치하는 결과만 표시하도록 필터링됩니다.

이 절차에서 설명한 대로 만든 사용자 시작 백업은 `USER_INITIATED` 유형이 되며 완전히 사용할 수 있을 때까지는 `CREATING` 상태가 됩니다.

백업을 새 볼륨으로 복원

다음 절차에서는 AWS Management Console 및를 사용하여 FSx for ONTAP 백업을 새 볼륨으로 복원하는 방법을 설명합니다 AWS CLI. 볼륨을 2세대 파일 시스템으로 복원할 때 AWS Management Console AWS CLI및 API를 사용하여 진행 상황을 모니터링할 수 있습니다.

볼륨 백업을 새 볼륨으로 복원하려면(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 탐색 창에서 백업을 선택한 다음 복원하려는 FSx for ONTAP 볼륨 백업을 선택합니다.
3. 오른쪽 상단 작업 메뉴에서 백업 복원을 선택합니다. 백업에서 볼륨 생성 페이지가 나타납니다.
4. 드롭다운 메뉴에서 백업을 복원할 FSx for ONTAP File 시스템 및 스토리지 가상 머신을 선택합니다.
5. 오른쪽 상단 작업 메뉴에서 백업 복원을 선택합니다. 백업에서 볼륨 생성 페이지가 나타납니다.
6. 드롭다운 메뉴에서 백업을 복원할 FSx for ONTAP File 시스템 및 스토리지 가상 머신을 선택합니다.
7. 볼륨 세부 정보 아래에는 몇 가지 선택 사항이 있습니다. 먼저 볼륨 이름을 입력합니다. 최대 203자의 영숫자 또는 밑줄 (_) 문자를 사용할 수 있습니다.
8. 볼륨 크기에는 20~314572800 범위의 정수를 입력하여 크기를 메비바이트(MiB) 단위로 지정합니다.
9. 볼륨 유형의 경우 읽기 및 쓰기가 가능한 볼륨을 생성하려면 읽기-쓰기(RW)를 선택하고 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용할 수 있는 읽기 전용 볼륨을 생성하려면 데이터 보호(DP)를 선택합니다. 자세한 내용은 볼륨 유형 단원을 참조하십시오.
10. 정션 경로에는 파일 시스템 내에서 볼륨을 마운트할 위치를 입력합니다. 이름 앞에 슬래시가 있어야 합니다(예: `/vol3`).
11. 스토리지 효율성의 경우 활성화를 선택하여 ONTAP 스토리지 효율 기능(중복 제거, 압축 및 압축)을 활성화합니다. 자세한 내용은 스토리지 효율성 단원을 참조하십시오.
12. 볼륨 보안 스타일에는 Unix(Linux), NTFS 또는 혼합 중 하나를 선택합니다. 볼륨의 보안 스타일에 따라 다중 프로토콜 액세스에 대한 기본 설정이 NTFS 또는 ACL로 기본 설정됩니다. 혼합 모드는 다중 프로토콜 액세스에는 필요하지 않으며 고급 사용자에게만 권장됩니다.
13. 스냅샷 정책에서 볼륨의 스냅샷 정책을 선택합니다. 스냅샷 정책에 대한 자세한 내용은 스냅샷 정책 섹션을 참조하세요.

사용자 지정 정책을 선택하는 경우 custom-policy 필드에 정책 이름을 지정해야 합니다. 사용자 지정 정책은 SVM 또는 파일 시스템에 이미 있어야 합니다. ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요.

14. 계층화 정책 휴지 기간에 유효한 값은 2~183일입니다. 볼륨의 계층화 정책 휴지 기간은 액세스되지 않은 데이터가 콜드 상태로 표시되고 용량 풀 스토리지로 이동되기까지의 일수를 정의합니다. 이 설정은 `Auto` 및 `Snapshot-only` 정책에만 영향을 줍니다.
15. 고급 섹션의 SnapLock 구성에서 기본 비활성화 설정을 그대로 두거나 활성화를 선택하여 SnapLock 볼륨을 구성할 수 있습니다. SnapLock 컴플라이언스 볼륨 또는 SnapLock 엔터프라이즈 볼륨 구성에 대한 자세한 내용은 SnapLock 규정 준수 이해 및 SnapLock 엔터프라이즈 이해를 참조하세요. SnapLock에 대한 자세한 정보는 SnapLock로 데이터 보호 섹션을 참조하세요.
16. 확인을 선택하여 볼륨을 생성합니다.
17. 백업을 2세대 파일 시스템으로 복원하는 경우 볼륨 페이지의 업데이트 탭에서 백업 복원 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 백업 복원 시 진행 상황 모니터링 단원을 참조하십시오.

백업을 새 볼륨으로 복원하려면(CLI) 다음과 같이 하세요.

create-volume-from-backup CLI 명령 또는 동등한 CreateVolumeFromBackup API 명령을 사용하여 볼륨 백업을 새 볼륨으로 복원합니다.

- ```
  $ aws fsx create-volume-from-backup --backup-id backup-08e6fc1133fff3532 \
        --name demo --ontap-configuration JunctionPath=/demo,SizeInMegabytes=100000,\
        StorageVirtualMachineId=svm-0f04a9c7c27e1908b,TieringPolicy={Name=ALL}
  ```

  백업을 2세대 파일 시스템으로 복원하기 위한 성공적인 복원 요청에 대한 시스템 응답은 다음과 같습니다. 응답에는 요청에 대한 상태 및 진행률 정보를 제공하는 "AdministrativeActions" 객체가 포함됩니다.

  ```
  {
        "Volume": {
            "CreationTime": 1692721488.428,
            "FileSystemId": "fs-07ab735385276ed60",
            "Lifecycle": "CREATING",
            "Name": "demo",
            "OntapConfiguration": {
                "FlexCacheEndpointType": "NONE",
  ```
  ```

```
                "JunctionPath": "/demo",
                "SizeInMegabytes": 100000,
                "StorageEfficiencyEnabled": true,
                "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
                "StorageVirtualMachineRoot": false,
                "TieringPolicy": {
                    "Name": "ALL"
                },
                "OntapVolumeType": "DP",
                "SnapshotPolicy": "default",
                "CopyTagsToBackups": false,
            },
            "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
            "VolumeId": "fsvol-0b6ec764c9c5f654a",
            "VolumeType": "ONTAP",
  --->      "AdministrativeActions": [
                {
                    "AdministrativeActionType": "DOWNLOAD_DATA_FROM_BACKUP",
                    "RequestTime": 1685729972.069,
                    "Status": "PENDING"
                }
            ]                   <----
        }
    }
```

백업을 1세대 파일 시스템으로 복원하기 위한 성공적인 요청에 대한 시스템 응답은 다음과 같습니다.

```
{
      "Volume": {
          "CreationTime": 1692721488.428,
          "FileSystemId": "fs-07ab735385276ed60",
          "Lifecycle": "CREATING",
          "Name": "demo",
          "OntapConfiguration": {
              "FlexCacheEndpointType": "NONE",
              "JunctionPath": "/demo",
              "SizeInMegabytes": 100000,
              "StorageEfficiencyEnabled": true,
              "StorageVirtualMachineId": "svm-0f04a9c7c27e1908b",
              "StorageVirtualMachineRoot": false,
              "TieringPolicy": {
```

```
                "Name": "ALL"
            },
            "OntapVolumeType": "DP",
            "SnapshotPolicy": "default",
            "CopyTagsToBackups": false,
        },
        "ResourceARN": "arn:aws:fsx:us-east-1:752825163408:volume/
fs-07ab735385276ed60/fsvol-0b6ec764c9c5f654a",
        "VolumeId": "fsvol-0b6ec764c9c5f654a",
        "VolumeType": "ONTAP",
    }
}
```

볼륨을 2세대 파일 시스템으로 복원할 때 AWS Management Console AWS CLI및 API를 사용하여 진행 상황을 모니터링할 수 있습니다.

데이터 하위 집합 복원

전체 백업 데이터 세트가 완전히 복원될 때까지 기다릴 필요 없이 2세대 파일 시스템의 새 볼륨으로 복원되는 동안 백업에서 데이터 하위 집합을 복원할 수 있습니다.

다음 절차에서는 백업을 복원할 때 데이터 하위 집합을 복구해야 하고 전체 복원이 완료될 때까지 기다릴 수 없는 경우 취해야 할 단계를 나열합니다.

백업을 복원하는 동안 데이터 하위 집합을 복원하려면

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 백업 페이지에서 복원하려는 데이터의 버전이 포함된 백업을 찾습니다.
3. 오른쪽 상단 작업 메뉴에서 백업 복원을 선택합니다. 백업에서 볼륨 생성 페이지가 나타납니다.
4. 드롭다운 메뉴에서 백업을 복원할 FSx for ONTAP File 시스템 및 스토리지 가상 머신을 선택합니다.
5. 볼륨 세부 정보에서 필요에 맞게 볼륨을 구성합니다.
6. 확인을 선택하여 볼륨을 생성합니다.
7. 백업 복원 진행 상황을 모니터링합니다.
8. CREATED의 수명 주기 상태를 보고할 때 복원되는 볼륨을 탑재합니다.
9. 복사해야 하는 볼륨에서 데이터의 하위 집합을 찾습니다.
10. 애플리케이션을 사용하여 기존 볼륨에 데이터를 복사합니다.

11. 백업에서 필요한 데이터를 대상 위치로 복사한 후에는 복원 중인 볼륨이 완료되기 전에 삭제하여 파일 시스템 리소스의 사용률을 최적화할 수 있습니다.

백업 복원 시 진행 상황 모니터링

AWS Management Console AWS CLI및 API에서 볼륨 백업을 2세대 파일 시스템으로 복원할 때 진행 상황을 모니터링할 수 있습니다. 모든 Amazon FSx 관리 작업과 마찬가지로 작업이 완료된 후 30일 동안 콘솔, CLI 및 API에서 백업 복원 상태를 사용할 수 있습니다.

백업 복원 시 진행 상황을 모니터링하려면(콘솔)

https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.

1. 왼쪽 탐색 메뉴에서 볼륨을 선택합니다.
2. 백업을 복원할 볼륨을 선택합니다.
3. 업데이트 탭을 선택합니다.
4. 백업 복원 업데이트 유형은 다음 정보를 제공합니다.

    - PENDING은 파일 메타데이터가 볼륨에 다운로드되고 있음을 나타냅니다. 볼륨의 수명 주기 상태는 CREATING입니다.
    - IN_PROGRESS는 볼륨을 사용할 수 있고 클라이언트가 데이터에 대한 읽기 전용 액세스 권한으로 볼륨을 탑재할 수 있음을 나타냅니다. 진행률 %는 볼륨에 다운로드된 데이터의 백분율을 보여줍니다.
    - 완료됨은 모든 데이터가 볼륨에 다운로드되었고 백업 복원이 완료되었음을 나타냅니다. 이제 클라이언트에 읽기-쓰기 액세스 권한이 있습니다. `RW` 볼륨의 경우, 이 시점에서 볼륨의 유형이 `DP`에서 `RW`로 변경됩니다.

백업 복원 시 진행 상황을 모니터링하려면(CLI)

- 2세대 FSx for ONTAP 파일 시스템에서 백업을 새 볼륨으로 복원할 때 `describe-volumes` CLI 명령을 사용하여 복원 진행 상황을 모니터링할 수 있습니다.

    백업을 2세대 파일 시스템으로 복원할 때 응답에는 데이터 다운로드 프로세스에 대한 상태 정보를 제공하는 `AdministrativeActions` 객체가 포함됩니다. .

    ```
    $ aws fsx describe-volumes
    {
        “Volumes”: [
    ```

```
        {
            “CreationTime”: 1691686114.674,
            “FileSystemId”: fs-029ff92192bd4d375,
            “LifeCycle”: “CREATING”,
            “Name”: vol1,
            “OntapConfiguration”: {
                   “FlexCacheEndpointType”: “NONE”,
                   “JunctionPath”: “/vol1”,
                   “SizeInMegabytes”: 100000,
                   “StorageEfficiencyEnabled”: true,
                   “StorageVirtualMachineId”: “svm-0ed1d714019426ca9”,
                   “StorageVirtualMachineRoot”: false,
                   “TieringPolicy”: {
                    “Name”: “ALL”
                   },
                   “OntapVolumeType”: “DP”,
                   “SnapshotPolicy”: “default”,
                   “CopyTagsToBackups”: false,
                  },
                  “ResourceARN”: “arn:aws:fsx:us-east-1:630831496844:volume/
fs-08ac75f715c6aec76/fsvol-094c015af930790fa”,
                  “VolumeId”: “fsvol-094c015af930790fa”,
                  “VolumeType”: “ONTAP”,
                  “AdministrativeActions”: [
                         {
                          “AdministrativeActionType”: “DOWNLOAD_DATA_FROM_BACKUP”,
                          “RequestTime”: 1685729972.069,
                          “Status”: “PENDING”
                         }
                  ]
    }
```

Amazon FSx가 복원된 볼륨에 모든 파일 메타데이터를 로드하면 이러한 필드에 다음 값이 표시됩니다.

- `"LifeCycle": "CREATED"` – 볼륨을 탑재할 준비가 되었음을 나타냅니다.
- `"OntapVolumeType": "DP"` – 파일 데이터를 다운로드하는 동안 볼륨이 읽기 전용임을 나타냅니다.
- `"ProgressPercent` - 볼륨에 로드되는 파일 데이터의 백분율을 표시합니다.
- `"Status": "IN_PROGRESS"` - 볼륨에 파일 데이터 다운로드가 진행 중입니다.

복원 프로세스의 이 단계에서는 복원 중인 백업의 모든 데이터에 대한 읽기 전용 액세스 권한으로 볼륨을 탑재할 수 있습니다.

Amazon FSx가 모든 파일 데이터를 새 볼륨으로 다운로드를 완료하면 RW 볼륨인 경우 클라이언트는 전체 읽기-쓰기 액세스 권한을 갖습니다. 표시기의 값은 다음과 같습니다.

- `"LifeCycle": "CREATED"` – 변경되지 않음
- `"OntapVolumeType": "RW"` – 클라이언트에 전체 읽기-쓰기 액세스 권한이 있음을 나타냅니다.
- `"Status": "COMPLETED"` – 복원이 완료되었음을 나타냅니다.

복원 프로세스가 실패하면 `AdminstrativeAction > Status`의 값은 `FAILED`입니다. `FailureDetails` 객체에 오류 메시지가 제공됩니다. 자세한 내용은 Amazon FSx API 레퍼런스에서 AdministrativeActionFailureDetails를 참조하세요.

백업 삭제

Amazon FSx 콘솔, Amazon FSx API 또는 AWS Command Line Interface (AWS CLI)를 사용하여 볼륨의 자동 일일 백업과 사용자 시작 백업FSx 모두 삭제할 수 있습니다. 백업 삭제는 영구적이고 복구할 수 없는 작업입니다. 삭제된 백업의 모든 데이터도 삭제됩니다. 나중에 해당 백업이 다시 필요하지 않을 것이라는 확신이 들지 않으면 백업을 삭제하지 마세요. 소스 볼륨이 오프라인인 경우 백업을 삭제할 수 없습니다.

볼륨이 모든 FSx for ONTAP 파일 시스템의 백업에서 복원되는 동안 볼륨을 삭제할 수 있습니다. 복원 중에 볼륨을 삭제하면 진행 중인 복원 작업이 효과적으로 취소됩니다.

> **Note**
>
> Amazon FSx는 볼륨의 다른 모든 백업이 삭제되지 않는 한 ONTAP 볼륨의 가장 최근 `AVAILABLE` 백업을 삭제하는 기능을 지원하지 않습니다.

를 사용하여 생성된 백업을 삭제하려면 AWS Backup 개발자 안내서의 백업 삭제를 AWS Backup참조하세요.

백업 삭제(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 콘솔 대시보드의 왼쪽 탐색 메뉴에서 백업을 선택합니다.
3. 백업 테이블에서 삭제하려는 백업을 선택한 다음 백업 삭제를 선택합니다.
4. 백업 삭제 대화 상자가 열리면 표시된 백업의 ID가 삭제하려는 백업인지 확인합니다.
5. 삭제할 백업의 확인란이 선택되어 있는지 확인합니다.
6. 백업 삭제를 선택합니다.

이제 백업과 포함된 모든 데이터가 영구적으로 삭제되어 복구할 수 없습니다.

백업 삭제(CLI)

- 다음 예와 같이 delete-backup CLI 명령 또는 이와 동등한 DeleteBackup API 작업을 사용하여 FSx for ONTAP 볼륨 백업을 삭제할 수 있습니다.

```
$ aws fsx delete-backup --backup-id backup-a0123456789abcdef
```

시스템 응답에는 삭제 중인 백업의 ID와 값이 DELETED인 수명 주기 상태가 포함되며, 이는 요청이 성공했음을 나타냅니다.

```
{
    "BackupId": "backup-a0123456789abcdef",
    "Lifecycle": "DELETED"
}
```

스냅샷으로 데이터 보호

스냅샷은 특정 시점의 Amazon FSx for NetApp ONTAP 볼륨의 읽기 전용 이미지입니다. 스냅샷은 볼륨의 파일을 실수로 삭제하거나 수정하지 못하도록 보호합니다. 스냅샷을 사용하면 사용자가 이전 스냅샷에서 개별 파일 또는 폴더를 쉽게 보고 복원하여 변경 사항을 실행 취소하고, 삭제된 콘텐츠를 복구하고, 파일 버전을 비교할 수 있습니다.

스냅샷에는 파일 시스템의 SSD 스토리지 용량을 사용하는 마지막 스냅샷 이후 변경된 데이터가 포함됩니다. 스냅샷은 볼륨 백업에 포함되지 않습니다. 스냅샷은 `default` 스냅샷 정책을 사용하여 볼륨에서 기본적으로 활성화됩니다. 스냅샷은 볼륨 루트의 `.snapshot` 디렉터리에 저장됩니다. 언제든지 볼

륨당 최대 1,023개의 스냅샷을 저장할 수 있습니다. 이 한도에 도달하면 볼륨의 새 스냅샷을 생성하기 전에 기존 스냅샷을 삭제해야 합니다.

주제

- 스냅샷 정책
- 스냅샷에서 파일 복원
- 공통 스냅샷 보기
- 볼륨의 스냅샷 예약 업데이트
- 자동 스냅샷 비활성화
- 스냅샷 삭제
- 스냅샷 삭제
- 스냅샷 예약

스냅샷 정책

스냅샷 정책은 시스템에서 볼륨에 대한 스냅샷을 생성하는 방법을 정의합니다. 정책은 스냅샷을 생성할 시기, 보존할 복사본 수 및 이름 지정 방법을 지정합니다. FSx for ONTAP에는 다음과 같은 세 가지 기본 제공 스냅샷 정책이 있습니다.

- `default`
- `default-1weekly`
- `none`

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

이 `default` 정책은 다음 일정에 따라 스냅샷을 자동으로 생성하며, 새 복사본을 위한 공간을 확보하기 위해 가장 오래된 스냅샷 복사본이 삭제됩니다.

- 매시 5분에 최대 6개의 시간별 스냅샷이 생성됩니다.
- 월요일부터 토요일까지 자정 10분 후 최대 2개의 일별 스냅샷이 생성됩니다.
- 매주 일요일 자정 15분 후 최대 2개의 주별 스냅샷이 생성됩니다.

> **Note**
>
> 스냅샷 시간은 파일 시스템의 시간대로 설정됩니다. 즉, 기본적으로 협정 세계시(UTC)로 설정됩니다. `timezone -timezone time_zone` ONTAP CLI 명령을 사용하여 FSx for ONTAP 파일 시스템의 시간대를 설정할 수 있습니다. ONTAP CLI 액세스에 대한 자세한 내용은 섹션을 참조하세요NetApp ONTAP CLI 사용.

`default-1weekly` 정책은 주간 일정에서 하나의 스냅샷만 유지한다는 점을 제외하면 `default` 정책과 동일합니다.

none 정책은 스냅샷을 생성하지 않습니다. 자동 스냅샷이 생성되지 않도록 볼륨에 이 정책을 할당할 수 있습니다.

ONTAP CLI 또는 REST API를 사용하여 사용자 지정 스냅샷 정책을 생성할 수도 있습니다. 자세한 내용은 NetApp ONTAP 제품 설명서의 스냅샷 정책 생성을 참조하세요. Amazon FSx 콘솔 AWS CLI, 또는 Amazon FSx API에서 볼륨을 생성하거나 업데이트하는 동안 스냅샷 정책을 선택할 수 있습니다. 자세한 내용은 볼륨 생성 및 볼륨 업데이트 섹션을 참조하세요.

스냅샷에서 파일 복원

Amazon FSx 파일 시스템의 스냅샷을 사용하면 개별 파일 또는 폴더의 이전 버전을 빠르게 복원할 수 있습니다.

Linux 및 macOS 클라이언트를 사용하는 경우 볼륨 루트의 `.snapshot` 디렉터리에서 스냅샷을 볼 수 있습니다. Windows 클라이언트를 사용하는 경우, 파일이나 폴더를 마우스 오른쪽 버튼으로 클릭하면 Windows 탐색기의 `Previous Versions` 탭에서 스냅샷을 볼 수 있습니다.

스냅샷에서 파일 복원(Linux 및 MacOS 클라이언트)

1. 원본 파일이 여전히 존재하고 스냅샷의 파일로 덮어쓰지 않으려면 Linux 또는 MacOS 클라이언트를 사용하여 원본 파일의 이름을 바꾸거나 파일을 다른 디렉터리로 이동하세요.
2. `.snapshot` 디렉터리에서 복원하려는 파일 버전이 들어 있는 스냅샷을 찾으세요.
3. `.snapshot` 디렉터리의 파일을 파일이 원래 있던 디렉터리로 복사합니다.

스냅샷에서 파일 복원(Windows 클라이언트)

Windows 클라이언트 사용자는 익숙한 Windows 파일 탐색기 인터페이스를 사용하여 파일을 이전 버전으로 복원할 수 있습니다.

1. 파일을 복원하려면 사용자가 복원할 파일을 선택한 다음 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴에서 이전 버전 복원을 선택합니다.
2. 그러면 사용자는 이전 버전 목록에서 이전 버전을 보고 복원할 수 있습니다.

스냅샷의 데이터는 읽기 전용입니다. 이전 버전 탭에 나열된 파일 및 폴더를 수정하려면 수정하려는 파일 및 폴더의 사본을 쓰기 가능한 위치에 저장하고 사본을 수정해야 합니다.

공통 스냅샷 보기

공통 스냅샷은 백업 간의 증분성을 유지하는 데 사용됩니다. 이 절차에서는 볼륨에서 일반적인 스냅샷을 식별하는 방법을 설명합니다.

볼륨의 공통 스냅샷을 보려면

- 볼륨의 공통 스냅샷을 확인하려면 volume snapshot show ONTAP CLI 명령을 사용합니다.

```
volume snapshot show -volume volume-name
```

출력에서 공통 스냅샷의 이름은 다음 예시와 같이 backup-*id* 형식이며, 여기서 *id*는 17자리 영숫자 문자열입니다.

```
FsxIdabc12345::> volume snapshot show -volume test_vol
                                  ---Blocks---
Vserver Volume    Snapshot                    Size     Total% Used%
-------- -------- --------------------------- -------- ------ -----
dest-svm test_vol
                  snap1                        144KB    0%     3%
                  snap2                        832KB    0%    16%
         --->     backup-abcdef0123456789a    4.87MB    0%    53% <---
                  weekly.2024-05-26_0015      5.02MB    0%    54%
                  weekly.2024-06-02_0015      2.22MB    0%    34%
                  daily.2024-06-04_0010        284KB    0%     6%
                  daily.2024-06-05_0010       4.29MB    0%    50%
                  hourly.2024-06-05_0705       168KB    0%     4%
8 entries were displayed.
```

> **Important**
>
> 볼륨의 공통 스냅샷은 백업 간의 증분성을 유지하는 데 사용되므로 삭제하지 마세요. 볼륨의 공통 스냅샷을 삭제하면 다음 백업이 증분 백업 대신 볼륨의 전체 백업이 됩니다.

볼륨의 스냅샷 예약 업데이트

다음 절차에 설명된 NetApp ONTAP CLI 또는 API를 사용하여 볼륨의 스냅샷 예약량을 변경할 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. volume modify ONTAP CII 명령을 사용하여 스냅샷 복사 예약에 사용되는 디스크 공간의 백분율을 변경합니다. 다음 자리 표시자 값을 데이터로 바꿉니다.

   - *svm_name* - SVM 이름을 사용합니다.
   - *vol_name* - 볼륨 이름을 사용합니다.
   - *percent* - 스냅샷 복사본에 예약하려는 디스크 공간의 백분율입니다.

   ```
   ::> volume modify -vserver svm_name -volume vol_name -percent-snapshot-
   space percent
   ```

   다음 예제에서는 vol1에 대한 스냅샷 예약이 볼륨 스토리지 용량의 25%로 변경됩니다.

   ```
   ::> volume modify -vserver vs0 -volume vol1 -percent-snapshot-space 25
   ```

자동 스냅샷 비활성화

자동 스냅샷은 FSx for ONTAP 파일 시스템의 볼륨에 대한 기본 스냅샷 정책에 의해 활성화됩니다. 데이터의 스냅샷이 필요하지 않은 경우(예: 테스트 데이터를 사용하는 경우) 다음 절차에 설명된 대로 볼

륨의 스냅샷 정책을 및 API와 CLI를 사용하여 로 설정하여 스냅샷을 비활성화할 수 있습니다. none AWS Management Console AWS CLI ONTAP

자동 스냅샷을 비활성화하려면(AWS 콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 볼륨을 업데이트할 ONTAP 파일 시스템을 선택합니다.
3. 볼륨 탭을 선택합니다.
4. 업데이트할 볼륨을 선택합니다.
5. 작업에서 볼륨 업데이트를 선택합니다.

   볼륨 업데이트 대화 상자가 볼륨의 현재 설정과 함께 표시됩니다.
6. 스냅샷 정책의 경우 없음을 선택합니다.
7. 업데이트를 선택하여 볼륨을 업데이트합니다.

자동 스냅샷을 비활성화하려면(AWS CLI)

- 다음 예제와 none같이 update-volume AWS CLI 명령(또는 동등한 UpdateVolume API 명령)을 사용하여를 SnapshotPolicy로 설정합니다.

```
aws fsx update-volume \
    --volume-id fsvol-1234567890abcdefa \
    --name new_vol \
    --ontap-configuration CopyTagsToBackups=true,JunctionPath=/new_vol, \
           SizeInMegabytes=2048,SnapshotPolicy=none, \
           StorageEfficiencyEnabled=true, \
           TieringPolicy=all
```

자동 스냅샷을 비활성화하려면(ONTAP CLI)

볼륨의 스냅샷 정책을 설정하여 none 기본 정책을 사용하여 자동 스냅샷을 끕니다.

1. volume snapshot policy show ONTAP CLI 명령을 사용하여 none 정책을 표시합니다.

```
::> snapshot policy show -policy none

Vserver: FsxIdabcdef01234567892
                          Number of Is
```

```
Policy Name                  Schedules Enabled Comment
---------------------------- --------- ------- ---------------------------------
none                                 0 false   Policy for no automatic snapshots.
    Schedule                  Count     Prefix                 SnapMirror Label
    ------------------------ -----     ---------------------- ------------------
    -                             -     -                      -
```

2. volume modify ONTAP CII 명령을 사용하여 볼륨의 스냅샷 정책을 none로 설정하여 자동 스냅샷을 비활성화합니다. 다음 자리 표시자 값을 데이터로 바꿉니다.

   - *svm_name* - SVM 이름을 사용합니다.
   - *vol_name* - 볼륨 이름을 사용합니다.

   계속할지 묻는 메시지가 표시되면 **y**를 입력합니다.

```
::> volume modify -vserver svm_name -volume vol_name -snapshot-policy none

Warning: You are changing the Snapshot policy on volume "vol_name" to "none".
 Snapshot copies on this volume
         that do not match any of the prefixes of the new Snapshot policy will not
 be deleted. However, when
         the new Snapshot policy takes effect, depending on the new retention
 count, any existing Snapshot copies
         that continue to use the same prefixes might be deleted. See the 'volume
 modify' man page for more information.
Do you want to continue? {y|n}: y
Volume modify successful on volume vol_name of Vserver svm_name.
```

스냅샷 삭제

스냅샷은 마지막 스냅샷 이후 변경된 볼륨의 데이터에 대해서만 스토리지 용량을 소비합니다. 이러한 이유로 워크로드가 데이터를 빠르게 쓰는 경우 오래된 데이터의 스냅샷이 볼륨의 스토리지 용량을 상당 부분 차지할 수 있습니다.

예를 들어 volume show-space ONTAP CLI 명령 출력에는 140KB의 User Data가 표시됩니다. 하지만 사용자 데이터가 삭제되기 전에는 볼륨이 9.8GB의 User Data였습니다. 볼륨에서 파일을 삭제했더라도 스냅샷은 여전히 이전 사용자 데이터를 참조할 수 있습니다. 이 때문에 이전 예제에서 Snapshot Reserve 및 Snapshot Spill은 볼륨에 사용자 데이터가 거의 없더라도 총 9.8GB의 공간을 차지합니다.

볼륨에서 공간을 확보하려면 더 이상 필요하지 않은 이전 스냅샷을 삭제하면 됩니다. 스냅샷은 증분 형이므로 스냅샷을 삭제할 때 스냅샷 크기와 동일한 스토리지 양을 회수하지 않습니다. 볼륨 스냅샷 컴퓨팅 재생 가능 -vserver ONTAP CII 명령을 사용하고 데이터를 사용하여 *svm_name* , *vol_name* , *snapshot_name*를 대체하여 스냅샷을 삭제할 때 재생할 수 있는 스토리지 양을 확인할 수 있습니다.

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

스냅샷 자동 삭제 정책을 만들거나 수동으로 스냅샷 삭제를 통해 스냅샷을 삭제할 수 있습니다. 스냅샷을 삭제하면 스냅샷에 저장된 변경된 데이터가 삭제됩니다.

스냅샷 삭제

volume snapshot delete ONTAP CLI 명령을 사용하여 스냅샷을 수동으로 삭제하고 다음 자리 표시자 값을 데이터로 바꿉니다.

- *svm_name*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
- *vol_name*을 볼륨의 이름으로 바꿉니다.
- *snapshot_name*을 스냅샷의 이름으로 바꿉니다. 이 명령은 *snapshot_name*에 와일드카드 문자(*)를 지원합니다. 따라서 예를 들어 hourly*를 사용하여 모든 시간별 스냅샷을 삭제할 수 있습니다.

> **Important**
>
> Amazon FSx 백업을 활성화한 경우 Amazon FSx는 각 볼륨의 최신 Amazon FSx 백업에 대한 스냅샷을 보관합니다. 이러한 스냅샷은 백업 간 증가분을 유지하는 데 사용되며 이 방법을 사용하여 삭제해서는 안 됩니다. 자세한 내용은 공통 스냅샷 보기 단원을 참조하십시오.

```
FsxIdabcdef01234567892::> volume snapshot delete -vserver svm_name -volume vol_name -
snapshot snapshot_name
```

스냅샷 자동 삭제 정책 생성

볼륨의 사용 가능한 공간이 부족할 때 스냅샷을 자동으로 삭제하도록 정책을 생성할 수 있습니다. 볼륨 스냅샷 자동 삭제 수정 ONTAP CLI 명령을 사용하여 볼륨에 대한 자동 삭제 정책을 설정합니다.

이 명령을 사용할 때 데이터를 사용하여 다음 자리 표시자 값을 바꿉니다.

- *svm_name*을 볼륨이 생성되는 SVM의 이름으로 바꿉니다.
- *vol_name*을 볼륨의 이름으로 바꿉니다.

`-trigger`에 다음 값 중 하나를 할당하세요.

- `volume` – 스냅샷이 삭제되는 임계값을 총 사용 볼륨 용량 임계값과 일치하도록 하려는 경우에 `volume`을 사용합니다. 스냅샷 삭제를 유발하는 사용 볼륨 용량 임계값은 볼륨 크기에 따라 결정되며, 임계값은 사용 용량의 85~98%로 조정됩니다. 볼륨이 작을수록 임계값이 작고, 볼륨이 클수록 임계값이 큽니다.
- `snap_reserve` – 스냅샷 예약에 보관할 수 있는 항목을 기준으로 스냅샷을 삭제하려는 경우에 `snap_reserve`를 사용합니다.

```
::> volume snapshot autodelete modify -vserver svm_name -volume vol_name -enabled true
 -trigger [volume|snap_reserve]
```

자세한 내용은 NetApp ONTAP 설명서 센터의 volume snapshot autodelete modify 명령을 참조하세요.

스냅샷 예약

스냅샷 복사본 예약은 스냅샷 복사본을 저장하기 위한 볼륨 스토리지 용량의 특정 비율을 기본값인 5%로 설정합니다. 스냅샷 복사본 예약에는 볼륨 백업을 포함하여 스냅샷 복사본에 할당된 충분한 공간이 있어야 합니다. 스냅샷 복사본이 스냅샷 예약 공간을 초과하는 경우 파일 시스템을 사용하기 위한 스토리지 용량을 복구하려면 활성 파일 시스템에서 기존 스냅샷 복사본을 삭제해야 합니다. 스냅샷 복사본에 할당된 디스크 공간의 백분율을 수정할 수도 있습니다.

스냅샷이 스냅샷 예약의 100% 이상을 소비할 때마다 기본 SSD 스토리지 공간을 차지하기 시작합니다. 이 프로세스를 스냅샷 유출이라고 합니다. 스냅샷이 활성 파일 시스템 공간을 계속 차지하면 파일 시스템이 가득 찰 위험이 있습니다. 스냅샷 유출로 인해 파일 시스템이 가득 차면 충분한 스냅샷을 삭제한 후에만 파일을 생성할 수 있습니다.

스냅샷 예약의 스냅샷에 충분한 디스크 공간을 사용할 수 있는 경우 기본 SSD 계층에서 파일을 삭제하면 새 파일의 디스크 공간이 확보되고 해당 파일을 참조하는 스냅샷 복사본은 스냅샷 복사 예약의 공간만 사용합니다.

스냅샷이 예약된 양(스냅샷 예약)보다 더 많은 디스크 공간을 소비하지 못하도록 할 방법이 없으므로 기본 SSD 계층에 새 파일을 생성하거나 기존 파일을 수정할 수 있는 공간이 항상 있도록 스냅샷에 충분한 디스크 공간을 예약하는 것이 중요합니다.

디스크가 가득 찼을 때 스냅샷이 생성되면 새로 생성된 스냅샷에서도 해당 데이터를 모두 참조하므로 기본 SSD 계층에서 파일을 삭제해도 여유 공간이 생성되지 않습니다. 파일을 생성하거나 업데이트하기 위해 스토리지를 확보하려면 스냅샷을 삭제해야 합니다.

NetApp ONTAP CLI를 사용하여 볼륨에 대한 스냅샷 예약 양을 수정할 수 있습니다. 자세한 내용은 볼륨의 스냅샷 예약 업데이트 단원을 참조하십시오.

자율 랜섬웨어 보호를 통한 데이터 보호

Autonomous Ransomware Protection(ARP)은 Windows 또는 Linux 클라이언트가 손상될 경우 랜섬웨어 및 맬웨어 공격으로부터 데이터를 모니터링하고 보호하는 NetApp ONTAP AI 기반 기능입니다. ARP는 기계 학습을 사용하여 FSx for ONTAP 파일 시스템에 익숙해져 비정상적인 활동을 사전에 탐지합니다. ARP는 Amazon FSx for NetApp ONTAP을 사용할 수 AWS 리전 있는 모든의 모든 신규 및 기존 FSx for ONTAP 파일 시스템에서 사용할 수 있습니다.

ARP 작동 방식

ONTAP CLI 또는 REST API를 사용하여 SVM의 모든 새 볼륨에서 볼륨별로 또는 기본적으로 ARP를 활성화할 수 있습니다. ARP 활성화에 대한 자세한 내용은 섹션을 참조하세요자율 랜섬웨어 보호 활성화.

ARP는 학습 및 활성이라는 두 가지 모드로 작동합니다. FSx for ONTAP 볼륨에 대해 ARP를 처음 활성화하면 학습 모드에서 실행됩니다. 학습 모드에서 ARP는 워크로드 액세스 패턴을 분석합니다. 는 볼륨의 워크로드를 기반으로 최적의 학습 기간을 ONTAP 자동으로 결정하며, 최대 30일이 걸릴 수 있습니다. 완료되면 ARP가 활성 모드로 전환됩니다. 활성 모드에서 ARP는 볼륨에서 수신되는 데이터와 활동을 모니터링하여 잠재적 랜섬웨어 및 맬웨어 공격을 식별합니다. 자세한 내용은 ARP가 찾는 것 단원을 참조하십시오. ARP가 비정상적인 활동을 감지하면 스냅샷ONTAP이 자동으로 생성되어 잠재적 공격 시점에 최대한 가깝게 데이터를 복구할 수 있습니다. 스냅샷의 접두사는 `Anti_ransomware_backup`이므로 쉽게 식별할 수 있습니다. 공격 확률이 보통인 것으로 확인되면 ONTAP에서 검토할 이벤트 관리 시스템(EMS) 메시지를 생성합니다. 자세한 내용은 ARP로 의심되는 공격에 대응하는 방법 및 자율 랜섬웨어 보호에 대한 EMS 알림 이해 섹션을 참조하세요.

ARP의 성능 오버헤드는 대부분의 워크로드에서 최소화됩니다. 볼륨에 읽기 집약적인 워크로드가 있는 경우는 파일 시스템당 이러한 볼륨을 150개 이하로 보호할 것을 NetApp 권장합니다. 이 수를 초

과하면 해당 워크로드의 IOPS가 최대 4% 감소할 수 있습니다. 볼륨에 쓰기 집약적인 워크로드가 있는 경우는 파일 시스템당 이러한 볼륨을 60개 이하로 보호할 것을 NetApp 권장합니다. 그렇지 않으면 해당 워크로드의 IOPS가 최대 10% 감소할 수 있습니다. 성능에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 성능 섹션을 참조하세요.

FSx for ONTAP 파일 시스템에서 ARP를 활성화하는 데 드는 추가 비용은 없습니다.

ARP가 찾는 것

ARP는 Windows 또는 Linux 클라이언트가 손상되었다는 신호를 찾습니다. ARP가 FSx for ONTAP 볼륨에 대해 알아보고 활성 모드로 전환하면 볼륨에서 다음 유형의 활동을 찾습니다.

- 파일의 데이터 무작위성 차이를 의미하는 엔트로피의 변경.
- 파일 확장자 유형이 변경되면 새 확장자가 일반적으로 사용되는 확장자 유형과 일치하지 않습니다. 기본값은 볼륨에서 이전에 관찰되지 않은 파일 확장자가 있는 파일 20개입니다.
- 파일 IOPS의 변경으로, 암호화된 데이터로 인해 비정상적인 볼륨 활동이 급증하는 것을 의미합니다.

필요한 경우 볼륨에 대한 랜섬웨어 탐지 파라미터를 수정할 수 있습니다. 예를 들어 볼륨이 여러 유형의 파일 확장자를 호스팅하는 경우입니다. 자세한 내용은 NetApp 설명서 센터의 Manage ONTAP Autonomous Ransomware Protection attack detection parameters를 참조하세요.

> **Note**
>
> ARP는 자격 증명이 있는 비인증 관리자가 FSx for ONTAP 파일 시스템에 액세스하는 것을 방지하지 않습니다.는 AWS BackupONTAP 스냅샷 및를 포함한 계층화된 보안 접근 방식을 AWS 권장합니다SnapLock.

ARP로 의심되는 공격에 대응하는 방법

ARP가 공격을 탐지하면 복구 시점으로 사용할 수 있는 스냅샷이 생성됩니다. 스냅샷이 잠겨 있으므로 일반적인 방법으로 삭제할 수 없습니다. 공격의 심각도에 따라 영향을 받는 볼륨, 공격 확률 및 공격 타임라인을 보여주는 EMS 알림도 생성됩니다. 볼륨에서 새 스냅샷 생성 또는 새 파일 확장자 관찰에 대한 알림을 받으려면 이러한 알림을 보내도록 ARP를 구성할 수 있습니다. 자세한 내용은 NetApp 설명서 센터에서 ARP 알림 구성을 참조하세요.

보고서를 생성하여 의심되는 공격에 대한 자세한 정보를 볼 수 있습니다. 보고서를 검토한 후 거짓 긍ONTAP정 또는 의심되는 공격으로 인해 알림이 생성되었는지 알 수 있습니다. 알림에 의심스러운 공

격으로 레이블을 지정하는 경우 공격 범위를 확인한 다음 ARP 생성 스냅샷에서 데이터를 복구해야 합니다. 공격에 거짓 긍정으로 레이블을 지정하면 ARP 생성 스냅샷이 자동으로 삭제됩니다. 자세한 내용은 자율 랜섬웨어 보호 알림에 대응 단원을 참조하십시오.

ONTAP CLI 및 REST API에서 파일 시스템의 EMS 메시지와 볼륨 상태를 모니터링하는 것이 좋습니다. ARP용 EMS 메시지에 대한 자세한 내용은 섹션을 참조하세요자율 랜섬웨어 보호에 대한 EMS 알림 이해.

주제

- 자율 랜섬웨어 보호 활성화
- 자율 랜섬웨어 보호 알림에 대응
- 자율 랜섬웨어 보호에 대한 EMS 알림 이해

자율 랜섬웨어 보호 활성화

다음 절차에서는 ONTAP CLI를 사용하여 학습 모드 및 활성 모드에서 자율 랜섬웨어 보호(ARP)를 활성화하는 방법과 ARP가 활성화되었는지 확인하는 방법을 설명합니다. ARP에 대한 자세한 내용은 섹션을 참조하세요ARP 작동 방식.

학습 모드에서 ARP 활성화

ONTAP CLI를 사용하여 기존 볼륨에서 학습 모드에서 ARP를 활성화하려면

- 다음 명령을 실행합니다. *vol_name* 및 *svm_name*을 자신의 정보로 바꿉니다.

```
security anti-ransomware volume dry-run -volume vol_name -vserver svm_name
```

이 명령security anti-ransomware volume dry-run에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

> **Note**
>
> 학습 모드는 새로 작성된 데이터에만 적용됩니다. 기존 데이터는 스캔되거나 분석되지 않습니다. 일반적인 데이터 트래픽 동작은 볼륨에서 ARP가 활성화된 후 작성된 새 데이터를 기반으로 결정됩니다.

ONTAP CLI를 사용하여 새 볼륨에서 학습 모드에서 ARP를 활성화하려면

- 다음 명령을 실행합니다. *vol_name*, *svm_name*, *size* 및 */path_name*을 정보로 바꿉니다.

```
volume create -volume vol_name -vserver svm_name -aggregate aggr_name -size size -
anti-ransomware-state dry-run -junction-path /path_name
```

이 명령volume create에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

활성 모드에서 ARP 활성화

ONTAP CLI를 사용하여 기존 볼륨에서 활성 모드에서 ARP를 활성화하려면

- 다음 명령을 실행합니다. *vol_name* 및 *svm_name*을 자신의 정보로 바꿉니다.

```
security anti-ransomware volume enable -volume vol_name -vserver svm_name
```

이 명령security anti-ransomware volume enable에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

> **Note**
>
> 활성 모드로 변환하기 전에 볼륨을 최소 30일 동안 학습 모드로 유지하는 것이 좋습니다. ARP는 최적의 학습 기간을 자동으로 결정하고 준비가 되면 학습 모드에서 전환합니다. 이 프로세스는 30일 이내에 발생할 수 있습니다.

SVM 수준에서 기본적으로 ARP 활성화

ONTAP CLI를 사용하여 기존 SVM에서 기본적으로 ARP를 활성화하려면

- 다음 명령을 실행합니다. *svm_name*을 사용자의 정보로 바꿉니다.

```
vserver modify -vserver svm_name -anti-ransomware-default-volume-state dry-run
```

이 명령vserver modify에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

ARP 상태 확인

ONTAP CLI를 사용하여 ARP의 상태를 확인하려면

- 다음 명령을 실행합니다.

```
security anti-ransomware volume show
```

이 명령security anti-ransomware volume show에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

워크로드 이벤트가 많을 것으로 예상되는 경우 ARP를 일시적으로 일시 중지(다시 시작)할 수 있습니다. 자세한 내용은 NetApp 설명서 센터의 분석에서 워크로드 이벤트를 제외하려면 ONTAP 자율 랜섬웨어 보호 일시 중지를 참조하세요.

자율 랜섬웨어 보호 알림에 대응

다음 절차에서는 ONTAP CLI를 사용하여 자율 랜섬웨어 보호(ARP) 알림을 보고, 공격 보고서를 생성하고, 보고서에 대한 조치를 취하는 방법을 설명합니다. ARP가 공격을 탐지하고 대응하는 방법에 대한 자세한 내용은 ARP가 찾는 것 및 섹션을 참조하세요ARP로 의심되는 공격에 대응하는 방법.

ARP 알림 보기

ONTAP CLI를 사용하여 볼륨에 대한 ARP 알림을 보려면

- 다음 명령을 실행합니다. *svm_name* 및 *vol_name*을 자신의 정보로 바꿉니다.

```
security anti-ransomware volume show -vserver svm_name -volume vol_name
```

명령을 실행하면 다음 예제와 유사한 출력이 표시됩니다.

```
Vserver Name: fsx
Volume Name: vol1
State: enabled
Attack Probability: moderate
Attack Timeline: 9/14/2021 01:03:23
Number of Attacks: 1
```

이 명령security anti-ransomware volume show에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

ARP 보고서 생성

ONTAP CLI를 사용하여 ARP 보고서를 생성하려면

- 다음 명령을 실행합니다. *vol_name* 및 */file_location/*을 자신의 정보로 바꿉니다. 보고서를 생성한 후 클라이언트 시스템에서 볼 수 있습니다.

```
security anti-ransomware volume attack generate-report -volume vol_name -dest-
path /file_location/
```

이 명령security anti-ransomware volume attack generate-report에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

ARP 보고서에 대한 작업 수행

ONTAP CLI를 사용하여 ARP 보고서의 거짓 긍정 공격에 대한 조치를 취하려면

- 다음 명령을 실행합니다. *svm_name*, *vol_name* 및 *[## ###]#* 사용자 고유의 정보로 바꿉니다.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive true
```

이 명령security anti-ransomware volume attack clear-suspect에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

> **Note**
>
> 알림을 거짓 긍정으로 표시하면 랜섬웨어 프로필이 업데이트됩니다. 이렇게 하면 해당 특정 시나리오에 대한 알림을 다시 받지 않습니다.

ONTAP CLI를 사용하여 ARP 보고서의 잠재적 공격에 대한 조치를 취하려면

- 다음 명령을 실행합니다. *svm_name*, *vol_name* 및 *[## ###]#* 사용자 고유의 정보로 바꿉니다.

```
security anti-ransomware volume attack clear-suspect -vserver svm_name -
volume vol_name [extension identifiers] -false-positive false
```

이 명령security anti-ransomware volume attack clear-suspect에 대한 자세한 내용은 NetApp 설명서 센터의 섹션을 참조하세요.

자율 랜섬웨어 보호에 대한 EMS 알림 이해

NetApp ONTAP's 이벤트 관리 시스템(EMS)을 사용하여 잠재적 공격을 포함하여 ARP와 관련된 이벤트를 모니터링할 수 있습니다. ARP 및 공격을 탐지하는 방법에 대한 자세한 내용은 ARP 작동 방식 및 섹션을 참조하세요ARP가 찾는 것.

다음 표에는 ARP와 관련된 모든 알림이 포함되어 있습니다. EMS에 대한 자세한 내용은 섹션을 참조하세요FSx for ONTAP EMS 이벤트 모니터링.

EMS 메시지 이름	EMS 메시지 설명
arw.analytics.ext.report	이 메시지는 랜섬웨어 방지 분석이 볼륨에 대한 의심스러운 파일 확장자 보고서를 생성하거나 업데이트할 때 발생합니다.
arw.analytics.high.entropy	이 메시지는 높은 엔트로피 데이터 로그 메시지 수(랜섬웨어 탐지 및 분석 관련)가 볼륨에 대해 사전 정의된 임계값을 초과할 때 발생합니다.
arw.analytics.probability	이 메시지는 랜섬웨어 방지 공격 확률이 볼륨lowhigh에서에서 로 변경된 경우에 발생합니다.
arw.analytics.report	이 메시지는 볼륨에 대한 랜섬웨어 방지 분석 보고서가 생성되거나 업데이트될 때 발생합니다.
arw.analytics.suspects	이 메시지는 랜섬웨어 방지 분석에 의해 생성된 용의자 목록이 추가 조사가 필요한 지점까지 증가할 때 발생합니다.
arw.auto.switch.enabled	이 메시지는 학습 기간, 파일 생성, 파일 쓰기 및 파일 확장자 검색 활동과 같은 다양한 조건이 충

EMS 메시지 이름	EMS 메시지 설명
	족된 후 랜섬웨어 방지가 학습 모드에서 활성화로 자동 전환된 경우에 발생합니다.
arw.new.file.extn.seen	이 메시지는 랜섬웨어 방지가 활성화된 볼륨에서 새 파일 확장명이 관찰될 때 발생합니다. 목적은 관찰된 확장에 대해 사용자에게 즉시 알려 적시에 조사할 수 있도록 하는 것입니다.
arw.snapshot.created	이 메시지는 랜섬웨어 방지가 활성화된 볼륨에서 새 ARP 스냅샷이 생성될 때 발생합니다. 또한 스냅샷이 생성된 이유에 대한 정보를 제공합니다.
arw.volume.state	이 메시지는 볼륨의 랜섬웨어 방지 상태가 변경될 때 발생합니다.
arw.vserver.state	이 메시지는 SVM의 랜섬웨어 방지 상태가 변경될 때 발생합니다.

SnapLock로 데이터 보호

SnapLock은 파일을 지정된 보존 기간 동안 수정이나 삭제를 방지하는 WORM(Write Once Read Many 상태로 전환하여 보호할 수 있도록 하는 기능입니다. SnapLock을 사용하여 규정을 준수하고, 비즈니스 크리티컬 데이터를 랜섬웨어 공격으로부터 보호하고, 변경 또는 삭제로부터 데이터를 보호하는 추가 계층을 제공할 수 있습니다.

Amazon FSx for NetApp ONTAP은 SnapLock을 통해 규정 준수 및 엔터프라이즈 보존 모드를 지원합니다. 자세한 내용은 SnapLock 규정 준수 이해 및 SnapLock 엔터프라이즈 이해 섹션을 참조하세요.

2023년 7월 13일 또는 그 이후에 생성된 FSx for ONTAP 파일 시스템에서 SnapLock 볼륨을 생성할 수 있습니다. 기존 파일 시스템은 향후 주별 유지 관리 기간 동안 SnapLock 지원을 받게 됩니다.

주제

- SnapLock 작동 방법
- SnapLock 규정 준수 이해
- SnapLock 엔터프라이즈 이해

- SnapLock 보존 기간 이해
- 파일을 WORM 상태로 커밋

SnapLock 작동 방법

SnapLock은 파일의 삭제, 변경 또는 이름 변경을 방지하여 규제 및 거버넌스 목적을 충족하는 데 도움이 될 수 있습니다. SnapLock 볼륨을 생성할 때 파일을 WORM(Write Once Read Many 스토리지로 커밋하고 데이터의 보존 기간을 설정합니다. 파일은 지우거나 쓸 수 없는 상태로 지정된 기간 동안 또는 무기한으로 저장할 수 있습니다.

> **Important**
>
> 볼륨을 만들 때 SnapLock 설정을 사용할지 여부를 지정해야 합니다. SnapLock이 아닌 볼륨은 생성 후 SnapLock 볼륨으로 변환할 수 없습니다.

보존 모드

SnapLock은 규정 준수와 엔터프라이즈라는 두 가지 보존 모드가 있습니다. Amazon FSx for NetApp ONTAP은 이 두 가지를 모두 지원합니다. 사용 사례가 다르고 일부 기능이 다르지만 둘 다 WORM 모델을 사용하여 데이터를 수정하거나 삭제하지 못하도록 보호합니다. 다음 표에는 이러한 보존 모드 간의 몇 가지 유사점과 차이점이 설명되어 있습니다.

SnapLock 기능	SnapLock 규정 준수 이해	SnapLock 엔터프라이즈 이해
설명	규정 준수 볼륨에서 WORM으로 전환된 파일은 보존 기간이 만료될 때까지 삭제할 수 없습니다.	권한 있는 사용자는 엔터프라이즈 볼륨에서 WORM으로 전환된 파일을 보존 기간이 만료되기 전에 권한이 필요한 삭제를 사용하여 삭제할 수 있습니다.
사용 사례	• SEC 규칙 17a-4(f), FINRA 규칙 4511 및 CFTC 규정 1.31과 같은 정부 또는 산업별 규정 준수.	• 조직의 데이터 무결성 및 내부 규정 준수 개선. • SnapLock 규정 준수를 사용하기 전에 보존 설정 테스트.

SnapLock 기능	SnapLock 규정 준수 이해	SnapLock 엔터프라이즈 이해
	• 랜섬웨어 공격으로부터 보호.	
자동 커밋	예	예
이벤트 기반 보존(EBR)[1]	예	예
법적 보존[1]	예	아니요
권한 있는 삭제 사용	아니요	예
볼륨 추가 모드	예	예
SnapLock 감사 로그 볼륨	예	예

Note

[1]EBR 및 법적 보존 작업은 ONTAP CLI 및 REST API에서 지원됩니다.

Note

FSx for ONTAP는 SnapLock 유형에 관계없이 모든 SnapLock 볼륨의 용량 풀에 대한 계층화 데이터를 지원합니다. 자세한 내용은 볼륨 데이터 계층화 단원을 참조하십시오.

SnapLock 관리자

SnapLock 볼륨에서 특정 작업을 수행하려면 SnapLock 관리자 권한이 있어야 합니다. SnapLock 관리자 권한은 ONTAP CLI의 `vsadmin-snaplock` 역할에 정의되어 있습니다. SnapLock 관리자 역할을 가진 스토리지 가상 머신(SVM) 관리자 계정을 생성하려면 클러스터 관리자여야 합니다.

ONTAP CLI에서 `vsadmin-snaplock` 역할을 사용하여 다음 작업을 수행할 수 있습니다.

- 사용자 계정, 로컬 암호 및 키 정보 관리
- 볼륨 관리(이동 볼륨 제외)
- 할당량, Qtree, 스냅샷 복사본, 파일 관리

- 권한이 필요한 삭제 및 법적 보존을 포함한 SnapLock 작업 수행
- Network File System(NFS) 및 Server Message Block(SMB) 프로토콜 구성
- 도메인 이름 시스템(DNS), 경량 디렉터리 액세스 프로토콜(LDAP) 및 네트워크 정보 서비스(NIS) 서비스 구성
- 작업 모니터링

다음 절차는 ONTAP CLI에서 SnapLock 관리자를 생성하는 방법을 자세히 설명합니다. 이 작업을 수행하려면 Secure Shell Protocol(SSH)과 같은 보안 연결에서 클러스터 관리자로 로그인해야 합니다.

ONTAP CLI에서 vsadmin-snaplock 역할을 사용하여 SVM 관리자 계정 생성

- 다음 명령을 실행합니다. *SVM_name* 및 *SnapLockAdmin*을 사용자의 정보로 바꿉니다.

```
cluster1::> security login create -vserver SVM_name -user-or-group-
name SnapLockAdmin -application ssh -authentication-method password -role vsadmin-
snaplock
```

자세한 내용은 ONTAP 사용자 및 역할 단원을 참조하십시오.

SnapLock 감사 로그 볼륨

SnapLock 감사 로그 볼륨에는 SnapLock 감사 로그가 포함되어 있습니다. 감사 로그에는 SnapLock 관리자가 생성된 시간, 권한이 필요한 삭제 작업이 실행된 시간 또는 파일에 법적 보존이 적용된 시기와 같은 이벤트의 타임스탬프가 포함됩니다. SnapLock 감사 로그 볼륨은 지울 수 없는 이벤트 기록입니다.

다음 작업을 수행하려면 SnapLock 볼륨과 동일한 SVM에 SnapLock 감사 로그 볼륨을 생성해야 합니다.

- SnapLock 엔터프라이즈 볼륨에서 권한이 필요한 삭제 켜기 또는 끄기
- SnapLock 규정 준수 볼륨의 파일에 법적 보존 적용

> ⚠ Warning
>
> - SnapLock 감사 로그 볼륨의 최소 보존 기간은 6개월입니다. 이 보존 기간이 만료되기 전까지는 볼륨이 SnapLock 엔터프라이즈 모드에서 생성된 경우에도 SnapLock 감사 로그 볼륨과 관련 SVM 및 파일 시스템을 삭제할 수 없습니다.

- 권한 있는 삭제를 사용하여 파일을 삭제하고 해당 보존 기간이 볼륨의 보존 기간보다 긴 경우 감사 로그 볼륨이 파일의 보존 기간을 상속합니다. 예를 들어 보존 기간이 10개월인 파일을 권한이 필요한 삭제를 사용하여 삭제하고 감사 로그 볼륨의 보존 기간이 6개월인 경우 감사 로그 볼륨의 보존 기간은 10개월로 연장됩니다.

SVM에는 활성 SnapLock 감사 로그 볼륨이 하나만 있을 수 있지만 SVM의 여러 SnapLock 볼륨에서 공유할 수 있습니다. SnapLock 감사 로그 볼륨을 성공적으로 마운트하려면 정션 경로를 `/snaplock_audit_log`로 설정합니다. 감사 로그 볼륨이 아닌 볼륨을 비롯한 다른 볼륨은 이 정션 경로를 사용할 수 없습니다.

감사 로그 볼륨의 루트 아래에 있는 `/snaplock_log` 디렉터리에서 SnapLock 감사 로그를 찾을 수 있습니다. 권한이 필요한 삭제 작업은 `privdel_log` 하위 디렉터리에 기록됩니다. 법적 보존 시작 및 종료 작업이 `/snaplock_log/legal_hold_logs/`에 로그인되었습니다. 다른 모든 로그는 `system_log` 하위 디렉터리에 저장됩니다.

Amazon FSx 콘솔, , AWS CLI Amazon FSx API, ONTAP CLI 및 REST API를 사용하여 SnapLock 감사 로그 볼륨을 생성할 수 있습니다.

> **Note**
>
> 데이터 보호(DP) 볼륨은 SnapLock 감사 로그 볼륨으로 사용할 수 없습니다.

Amazon FSx API로 SnapLock 감사 로그 볼륨을 켜려면 `CreateSnaplockConfiguration`에서 `AuditLogVolume`을 사용합니다. Amazon FSx 콘솔의 감사 로그 볼륨에서 활성화를 선택합니다. 정션 경로가 `/snaplock_audit_log`로 설정되어 있는지 확인합니다.

SnapLock 볼륨의 데이터에 액세스

NFS 및 SMB와 같은 오픈 파일 프로토콜을 사용하여 SnapLock 볼륨의 데이터에 액세스할 수 있습니다. SnapLock 볼륨에 데이터를 쓰거나 WORM으로 보호되는 데이터를 읽어도 성능에 미치는 영향은 없습니다.

NFS 및 SMB를 사용하여 SnapLock 볼륨 간에 파일을 복사할 수 있지만 대상 SnapLock 볼륨에 WORM 속성이 유지되지는 않습니다. 파일이 수정되거나 삭제되지 않도록 하려면 복사한 파일을 WORM에 다시 커밋해야 합니다. 자세한 내용은 파일을 WORM 상태로 커밋 섹션을 참조하세요.

SnapMirror를 사용하여 SnapLock 데이터를 복제할 수도 있지만 소스 볼륨과 대상 볼륨은 보존 모드가 동일한 SnapLock 볼륨이어야 합니다(예: 둘 다 규정 준수 또는 엔터프라이즈여야 함).

SnapLock 규정 준수 이해

이 섹션에서는 SnapLock 규정 준수 보존 모드의 사용 사례 및 고려 사항을 설명합니다.

다음 사용 사례에서 규정 준수 보존 모드를 선택할 수 있습니다.

- SnapLock 규정 준수를 사용하여 SEC 규칙 17a-4(f), FINRA 규칙 4511 및 CFTC 규정 1.31과 같은 정부 또는 산업별 의무 사항을 준수할 수 있습니다. Amazon FSx for NetApp ONTAP의 SnapLock 규정 준수는 Cohasset Associates에 의해 이러한 의무 사항 및 규정에 대해 평가되었습니다. 자세한 내용은Compliance Assessment Report for Amazon FSx for NetApp ONTAP에 대한 규정 준수 평가 보고서를 참조하세요.
- SnapLock 규정 준수를 사용하여 랜섬웨어 공격에 대응하기 위한 포괄적인 데이터 보호 전략을 보완하거나 강화할 수 있습니다.

다음은 SnapLock 규정 준수 보존 모드에 대해 고려해야 할 몇 가지 중요한 항목입니다.

- SnapLock 규정 준수 볼륨에서 파일이 WORM(Write Once Read Many 상태로 전환된 후에는 보존 기간이 만료되기 전에 파일을 삭제할 수 없습니다.
- SnapLock 규정 준수 볼륨은 볼륨에 있는 모든 WORM 파일의 보존 기간이 만료되고 해당 볼륨에서 WORM 파일이 삭제된 경우에만 삭제할 수 있습니다.
- SnapLock 규정 준수 볼륨을 만든 후에는 이름을 바꿀 수 없습니다.
- SnapMirror를 사용하여 WORM 파일을 복제할 수 있지만 소스 볼륨과 대상 볼륨의 보존 모드가 동일해야 합니다(예: 둘 다 규정 준수여야 함).
- SnapLock 규정 준수 볼륨은 SnapLock 엔터프라이즈 볼륨으로 변환할 수 없으며 그 반대의 경우도 마찬가지입니다.

SnapLock 엔터프라이즈 이해

이 섹션에서는 SnapLock 엔터프라이즈 보존 모드의 사용 사례 및 고려 사항에 대해 설명합니다.

다음 사용 사례에 맞게 SnapLock 엔터프라이즈 보존 모드를 선택할 수 있습니다.

- SnapLock 엔터프라이즈를 사용하여 특정 사용자에게만 파일 삭제 권한을 부여할 수 있습니다.
- SnapLock 엔터프라이즈를 사용하여 조직의 데이터 무결성과 내부 규정 준수를 개선할 수 있습니다.
- SnapLock 규정 준수를 사용하기 전에 SnapLock 엔터프라이즈를 사용하여 보존 설정을 테스트할 수 있습니다.

다음은 SnapLock 엔터프라이즈 보존 모드에 대해 고려해야 할 몇 가지 중요한 항목입니다.

- SnapMirror를 사용하여 WORM 파일을 복제할 수 있지만 소스 볼륨과 대상 볼륨의 보존 모드가 동일해야 합니다(예: 둘 다 엔터프라이즈여야 함).
- SnapLock 볼륨은 엔터프라이즈에서 규정 준수로 또는 규정 준수에서 엔터프라이즈로 변환할 수 없습니다.
- SnapLock 엔터프라이즈는 법적 보존을 지원하지 않습니다.

권한 있는 삭제 사용

SnapLock 엔터프라이즈와 SnapLock 규정 준수의 주요 차이점 중 하나는 SnapLock 관리자가 SnapLock 엔터프라이즈 볼륨에서 권한이 필요한 삭제를 켜서 파일의 보존 기간이 만료되기 전에 파일을 삭제하도록 허용할 수 있다는 것입니다. SnapLock 관리자는 활성 보존 정책이 적용된 SnapLock 엔터프라이즈 볼륨에서 파일을 삭제할 수 있는 유일한 사용자입니다. 자세한 내용은 SnapLock 관리자 단원을 참조하십시오.

Amazon FSx 콘솔, , Amazon FSx AWS CLI FSx API, ONTAP CLI 및 REST API를 사용하여 권한 있는 삭제를 켜거나 끌 수 있습니다. 권한이 필요한 삭제를 켜려면 먼저 SnapLock 볼륨과 동일한 SVM에 SnapLock 감사 로그 볼륨을 생성해야 합니다. 자세한 내용은 SnapLock 감사 로그 볼륨 섹션을 참조하세요.

Amazon FSx API를 사용하여 권한이 필요한 삭제를 켜려면 `CreateSnaplockConfiguration`의 `PrivilegedDelete`를 사용합니다. Amazon FSx 콘솔의 권한 있는 삭제에서 활성화를 선택합니다.

> **Note**
>
> 보존 기간이 만료된 WORM(Write Once Read Many 파일에는 권한이 필요한 삭제 명령을 실행할 수 없습니다. 보존 기간이 만료된 후에는 일반 삭제 작업을 실행할 수 있습니다.

권한이 필요한 삭제를 영구적으로 끄도록 선택할 수 있지만 이 작업은 되돌릴 수 없습니다. 권한이 필요한 삭제가 영구적으로 꺼진 경우 SnapLock 엔터프라이즈 볼륨과 연결된 SnapLock 감사 로그 볼륨이 없어도 됩니다.

Amazon FSx API를 사용하여 권한이 필요한 삭제를 끄려면 `CreateSnaplockConfiguration`의 `PrivilegedDelete`를 사용합니다. Amazon FSx 콘솔의 권한 있는 삭제에서 영구적으로 비활성화를 선택합니다.

SnapLock 엔터프라이즈 모드 우회

Amazon FSx 콘솔 또는 Amazon FSx API를 사용하는 경우 활성 보존 정책이 적용되는 WORM 파일이 포함된 SnapLock 엔터프라이즈 볼륨을 삭제하려면 IAM `fsx:BypassSnapLockEnterpriseRetention` 권한이 있어야 합니다.

자세한 내용은 SnapLock 볼륨 삭제 단원을 참조하십시오.

SnapLock 보존 기간 이해

SnapLock 볼륨을 생성할 때 볼륨의 기본 보존 기간을 설정하거나, WORM(Write Once Read Many 파일에 대한 보존 기간을 명시적으로 설정할 수 있습니다. 보존 기간 중에는 WORM 보호 파일을 삭제하거나 수정할 수 없습니다. 보존 기간은 보존 기간을 계산하는 데 사용됩니다. 예를 들어, 2023년 7월 14일 자정에 파일을 WORM으로 전환하고 보존 기간을 5년으로 설정하면 보존 기간은 2028년 7월 14일 자정까지가 됩니다.

WORM에 대한 자세한 내용은 파일을 WORM 상태로 커밋 섹션을 참조하세요.

보존 기간 정책

보존 기간은 다음 파라미터에 할당한 값에 따라 결정됩니다.

- 기본 보존 – 보존 기간을 명시하지 않은 경우 WORM 파일에 할당되는 기본 보존 기간입니다.
- 최소 보존 – WORM 파일에 할당할 수 있는 가장 짧은 보존 기간입니다.
- 최대 보존 – WORM 파일에 할당할 수 있는 가장 긴 보존 기간입니다.

> **Note**
>
> 보존 기간이 만료된 후에도 WORM 파일은 수정할 수 없습니다. 파일을 삭제하거나 새 보존 기간을 설정하여 WORM 보호를 다시 켜는 것만 가능합니다.

여러 시간 단위를 사용하여 보존 기간을 지정할 수 있습니다. 다음 표에는 지원되는 지정 범위가 표시되어 있습니다.

유형	값	설명
초	0 - 65,535	

유형	값	설명
분	0 - 65,535	
시간	0 - 24	
일	0 - 365	
개월	0 -12	
년	0 - 100	
무제한	-	파일을 영구 보존합니다. 기본 보존, 최대 보존 및 최소 보존에 사용할 수 있습니다.
지정되지 않음[1]	-	보존 기간을 설정할 때까지 파일을 보존합니다. 기본 보존에만 사용할 수 있습니다.

> **Note**
>
> [1]파일을 보존 기간이 지정되지 않은 WORM으로 전환하면 SnapLock 볼륨에 대해 구성된 최소 보존 기간이 지정됩니다. WORM 보호 파일을 절대 보존 기간으로 전환하는 경우 새 보존 기간은 이전에 파일에 설정한 최소 기간보다 길어야 합니다.

보존 기간 만료

WORM 파일의 보존 기간이 만료된 후에는 파일을 삭제하거나 새 보존 기간을 설정하여 WORM 보호를 재활성화할 수 있습니다. WORM 파일은 보존 기간이 만료된 후 자동으로 삭제되지 않습니다. 보존 기간이 만료된 후에도 WORM 파일의 내용을 수정할 수 없습니다.

SnapLock 볼륨 보존 기간 설정

Amazon FSx 콘솔, AWS CLI, Amazon FSx API 및 ONTAP CLI와 REST API를 사용하여 SnapLock 볼륨의 보존 기간을 설정할 수 있습니다.

Amazon FSx API로 보존 기간을 설정하려면 `SnaplockRetentionPeriod` 구성을 사용합니다. Amazon FSx 콘솔에서 보존 기간에 기본 보존, 최소 보존 및 최대 보존에 대한 값을 입력합니다. 그런 다음 각각에 해당하는 단위를 선택합니다.

파일을 WORM 상태로 커밋

이 섹션에서는 파일을 WORM(Write Once Read Many 상태로 전환하는 방법에 대해 설명합니다. 또한 WORM 보호 파일에 데이터를 증분 방식으로 쓰는 방법인 볼륨 추가 모드에 대해서도 설명합니다.

자동 커밋

파일이 지정된 기간 동안 수정되지 않은 경우 자동 커밋을 사용하여 파일을 WORM으로 전환할 수 있습니다. Amazon FSx 콘솔, , AWS CLI Amazon FSx API, ONTAP CLI 및 REST API를 사용하여 자동 커밋을 켤 수 있습니다.

자동 커밋 기간을 5분에서 10년 사이로 지정할 수 있습니다. 다음 표에는 지원되는 지정 범위가 표시되어 있습니다.

단위	값
분	5 - 65,535
시간	1 - 65,535
일	1 - 3,650
개월	1 - 120
년	1 - 10

Amazon FSx API를 사용하여 자동 커밋을 켜려면 `CreateSnaplockConfiguration`에서 `AutocommitPeriod`를 사용합니다. Amazon FSx 콘솔의 Autocommit에서 활성화 를 선택합니다. 그리고, 자동 커밋 기간에 값을 입력하고 해당 자동 커밋 단위를 선택합니다.

5분~10년 범위의 값을 지정할 수 있습니다.

볼륨 추가 모드

WORM 보호 파일의 기존 데이터는 수정할 수 없습니다. 하지만 SnapLock을 통해 WORM 추가 가능 파일을 사용하여 기존 데이터에 대한 보호를 유지할 수 있습니다. 예를 들어, 데이터를 점진적으로 기록하면서 로그 파일을 생성하거나 오디오 또는 비디오 스트리밍 데이터를 보존할 수 있습니다. Amazon FSx 콘솔, , Amazon AWS CLI FSx API, ONTAP CLI 및 REST API를 사용하여 볼륨 추가 모드를 켜거나 끌 수 있습니다.

볼륨 추가 모드 업데이트 요구 사항

- SnapLock 볼륨을 마운트 해제해야 합니다.
- SnapLock 볼륨에는 스냅샷 복사본과 사용자 데이터가 없어야 합니다.

Amazon FSx API로 볼륨 추가 모드를 켜려면 `CreateSnaplockConfiguration`의 `VolumeAppendModeEnabled`를 사용합니다. Amazon FSx 콘솔의 볼륨 추가 모드에서 활성화를 선택합니다.

이벤트 기반 보존(EBR)

이벤트 기반 보존(EBR)을 사용하여 관련 보존 기간과 함께 사용자 지정 정책을 만들 수 있습니다. 예를 들어, 지정된 경로의 모든 파일을 WORM으로 전환하고 `snaplock event-retention policy create` 및 `snaplock event-retention apply` 명령을 사용하여 보존 기간을 1년으로 설정할 수 있습니다. EBR을 사용할 때 볼륨, 디렉터리 또는 파일을 지정해야 합니다. EBR 정책을 만들 때 선택한 보존 기간은 지정된 경로의 모든 파일에 적용됩니다.

EBR은 ONTAP CLI 및 REST API에서 지원됩니다.

> **Note**
>
> ONTAP은 FlexGroup 볼륨에 대한 EBR을 지원하지 않습니다.

다음 절차는 EBR 정책을 생성, 적용, 수정 및 삭제하는 방법을 설명합니다. ONTAP CLI에서 이러한 작업을 완료하려면 `vsadmin-snaplock` 역할을 보유한 SnapLock 관리자여야 합니다. 자세한 내용은 SnapLock 관리자 단원을 참조하십시오.

ONTAP CLI에서 EBR 정책 생성

ONTAP CLI에서 EBR 정책을 생성하려면

- 다음 명령을 실행합니다. *p1*과 *"10#"*을 자체 정보로 바꿉니다.

```
vs1::> snaplock event-retention policy create -name p1 -retention-period "10 years"
```

ONTAP CLI에서 EBR 정책 적용

ONTAP CLI에서 EBR 정책을 적용하려면

- 다음 명령을 실행합니다. *p1*과 *slc*를 자체 정보로 바꿉니다. EBR 정책의 특정 경로를 지정하려는 경우 슬래시(/) 뒤에 경로를 추가할 수 있습니다. 그렇지 않으면 이 명령은 EBR 정책을 볼륨의 모든 파일에 적용합니다.

```
vs1::> snaplock event-retention apply -policy-name p1 -volume slc -path /
```

ONTAP CLI에서 EBR 정책 수정

ONTAP CLI에서 EBR 정책을 수정하려면

- 다음 명령을 실행합니다. *p1*과 *"5#"*을 자체 정보로 바꿉니다.

```
vs1::> snaplock event-retention policy modify -name p1 -retention-period "5 years"
```

ONTAP CLI에서 EBR 정책 삭제

ONTAP CLI에서 EBR 정책을 삭제하려면

- 다음 명령을 실행합니다. *p1*을 사용자의 정보로 바꿉니다.

```
vs1::> snaplock event-retention policy delete -name p1
```

NetApp 설명서 센터의 관련 명령:

- snaplock event-retention abort

- snaplock event-retention show-vservers
- snaplock event-retention show
- snaplock event-retention policy show

법적 보존

법적 보존을 사용하여 WORM 파일을 무기한으로 보존할 수 있습니다. 법적 보존은 일반적으로 소송 목적으로 사용됩니다. 법적 보존 대상인 WORM 파일은 법적 보존이 해제될 때까지 삭제할 수 없습니다.

법적 보존은 ONTAP CLI 및 REST API에서 지원됩니다.

> **Note**
>
> ONTAP은 FlexGroup 볼륨에 대한 법적 보존을 지원하지 않습니다.

다음 절차에서는 법적 보존을 시작하고 종료하는 방법을 설명합니다. ONTAP CLI에서 이러한 작업을 완료하려면 `vsadmin-snaplock` 역할을 보유한 SnapLock 관리자여야 합니다. 자세한 내용은 SnapLock 관리자 단원을 참조하십시오.

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 파일에 대한 법적 보존 시작

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 파일에 법적 보존을 시작하려면

- 다음 명령을 실행합니다. *litigation1*, *slc_vol1* 및 *file1*을 자체 정보로 바꿉니다.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 모든 파일에 대한 법적 보존 시작

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 모든 파일에 대해 법적 보존을 시작하려면

- 다음 명령을 실행합니다. *litigation1* 및 *slc_vol1*을 자체 정보로 바꿉니다.

```
vs1::> snaplock legal-hold begin -litigation-name litigation1 -volume slc_vol1 -
path /
```

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 파일에 대한 법적 보존 종료

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 파일에 대한 법적 보존을 종료하려면

- 다음 명령을 실행합니다. *litigation1*, *slc_vol1* 및 *file1*을 자체 정보로 바꿉니다.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /file1
```

> **Note**
>
> 법적 보존을 실행할 때는 `snaplock legal-hold show` 명령으로 `-operation-status`를 모니터링하여 실패하지 않도록 하는 것이 좋습니다.

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 모든 파일에 대한 법적 보존 종료

ONTAP CLI를 사용하여 SnapLock 규정 준수 볼륨의 모든 파일에 대한 법적 보존을 종료하려면

- 다음 명령을 실행합니다. *litigation1* 및 *slc_vol1*을 자체 정보로 바꿉니다.

```
vs1::> snaplock legal-hold end -litigation-name litigation1 -volume slc_vol1 -
path /
```

> **Note**
>
> 법적 보존을 실행할 때는 `snaplock legal-hold show` 명령으로 `-operation-status`를 모니터링하여 실패하지 않도록 하는 것이 좋습니다.

NetApp 설명서 센터의 관련 명령:

- snaplock legal-hold abort
- snaplock legal-hold dump-files
- snaplock legal-hold dump-litigations
- snaplock legal-hold show

를 사용하여 데이터 복제 FlexCache

FlexCache는 클라이언트에 데이터 세트를 더 가깝게 만들어 액세스 성능을 개선하고 비용을 절감하는 NetApp ONTAP's 원격 캐싱 기능입니다. 파일 배포를 간소화하고 WAN 비용을 절감합니다. FlexCache 볼륨을 생성하면 처음에는 오리진 파일 시스템의 메타데이터만 복사합니다. 이 접근 방식은 전체 데이터 복사보다 빠르고 공간 효율적이며 스토리지 용량의 일부만 소비합니다.

FlexCache 작동 방법

FlexCache 볼륨은 오리진 볼륨에 저장된 데이터에 대한 액세스를 제공하는 희소하게 채워진 캐시입니다. 캐시는 선택적으로 다른 원격 파일 시스템에 위치할 수 있습니다. 원본 볼륨에서 모든 데이터를 복사하는 대신 필요에 따라 데이터를 FlexCache 복사합니다. 원본 데이터를 변경하려면 캐시를 새로 고쳐야 하므로 FlexCache 볼륨은 자주 변경되지 않는 읽기 집약적인 워크플로에 가장 적합합니다.

다음 구성에서 FSx for ONTAP과 FlexCache 함께를 사용할 수 있습니다.

오리진 볼륨	FlexCache volume
온프레미스 NetApp ONTAP	FSx for ONTAP
FSx for ONTAP	온프레미스 NetApp ONTAP
FSx for ONTAP	FSx for ONTAP

FlexCache 쓰기 모드

FlexCache 볼륨은 쓰기 작업에 대해 라이트 어라운드 모드와 라이트백 모드의 두 가지 작업 모드를 지원합니다.

기본 모드인 라이트 어라운드 모드에서는 쓰기가 캐시에서 오리진 볼륨으로 전달됩니다. 데이터가 오리진 볼륨의 스토리지에 커밋되고 오리진이 캐시에 대한 쓰기를 다시 승인할 때까지 쓰기 작업은 클라이언트에 승인되지 않습니다. 각 쓰기는 캐시와 오리진 간에 네트워크를 통과해야 하므로이 모드는 쓰기-백 모드보다 지연 시간이 더 깁니다.

ONTAP 9.15.1에 도입된 라이트백 모드에서는 쓰기가 캐시 위치의 스토리지에 커밋되고 클라이언트에 즉시 승인됩니다. 그런 다음 데이터가 오리진 볼륨에 비동기식으로 기록됩니다. 이 모드를 사용하면 로컬에 가까운 속도로 쓰기를 수행할 수 있으므로 분산 워크로드의 성능이 크게 향상될 수 있습니다.

지연 시간이 짧은 캐시 쓰기가 필요한 쓰기 작업이 많은 워크로드에는 라이트백 모드를 사용합니다. 지연 시간에 민감하지 않은 읽기 작업이 많은 워크로드 또는 오리진 파일 시스템의 FlexCache 오리진 볼륨이 10개를 초과하는 경우 라이트 어라운드 모드를 사용합니다.

FlexCache 볼륨 생성 개요

FlexCache 볼륨 생성은 다음 단계로 구성됩니다.

- 소스 및 대상 논리적 인터페이스(LIFs) 수집
- 오리진과 캐시 파일 시스템 간에 클러스터 피어링 설정
- 스토리지 가상 머신(SVM) 피어링 관계 생성
- FlexCache 볼륨을 생성하고 쓰기 모드를 선택합니다.
- 클라이언트에 FlexCache 볼륨 탑재

자세한 지침은 FlexCache 생성 섹션을 참조하세요.

FlexCache 생성

다음 절차에 따라 Amazon FSx for NetApp ONTAP 파일 시스템에서 온프레미스 NetApp ONTAP 클러스터에 있는 오리진 FlexCache 볼륨의 지원을 받는 볼륨을 생성합니다.

ONTAP CLI 사용

ONTAP CLI를 사용하여 FSx for ONTAP 파일 시스템에서 FlexCache 구성을 생성하고 관리합니다.

이 절차의 명령은 클러스터, SVM 및 볼륨에 대해 다음 별칭을 사용합니다.

- `Cache_ID` - 캐시 클러스터의 ID(FSxIdabcdef1234567890a 형식)
- `Origin_ID` - 오리진 클러스터의 ID
- `CacheSVM` - 캐시 SVM 이름
- `OriginSVM` - 오리진 SVM 이름
- `OriginVol` - 오리진 볼륨 이름
- `CacheVol` - FlexCache 볼륨 이름

이 섹션의 절차에서는 다음 NetApp ONTAP CLI 명령을 사용합니다.

- `network interfaces show`
- `cluster peer` 명령
- `volume flexcache create`

사전 조건

다음 섹션의 절차를 사용하기 전에 다음 사전 조건을 충족했는지 확인하세요.

- 소스 및 대상 파일 시스템은 동일한 VPC에 연결되거나 Amazon VPC, AWS Transit Gateway AWS Direct Connect또는를 사용하여 피어링된 네트워크에 있습니다 AWS VPN. 자세한 내용은 Amazon VPC 피어링 가이드의 내에서 데이터 액세스 AWS 클라우드 및 VPC 피어링이란 무엇입니까?를 참조하세요. https://docs.aws.amazon.com/vpc/latest/peering/what-is-vpc-peering.html
- FSx for ONTAP 파일 시스템의 VPC 보안 그룹에는 클러스터 간 엔드포인트(LIFs.
- SVM을 사용하여 대상 FSx for ONTAP 파일 시스템을 생성했지만 FlexCache로 사용할 볼륨을 생성하지 않았습니다. 자세한 내용은 파일 시스템 만들기 단원을 참조하십시오.

소스 및 대상 클러스터 간 LIF 기록

1. 대상 클러스터인 FSx for ONTAP 파일 시스템의 경우:

   a. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.

   b. 파일 시스템을 선택한 다음 대상 클러스터인 FSx for ONTAP 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 엽니다.

   c. 관리에서 클러스터 간 엔드포인트 - IP 주소를 찾고 값을 기록합니다.

   > **Note**
   >
   > 스케일 아웃 파일 시스템의 경우 각 고가용성(HA) 페어에 대해 클러스터 간 엔드포인트 IP 주소 2개가 있습니다.

2. 온프레미스 소스 클러스터의 경우 다음 ONTAP CLI 명령을 사용하여 클러스터 간 LIF IP 주소를 검색합니다.

```
Origin::> network interface show -role intercluster
Logical                         Network
Vserver     Interface  Status   Address/Mask
```

```
----------- ---------- -------    ------------
OriginSVM
            inter_1     up/up    10.0.0.36/24
            inter_2     up/up    10.0.1.69/24
```

3. inter_1 및 inter_2 IP 주소를 저장합니다. OriginSVM 별칭에서는 origin_inter_1 및 로, 별origin_inter_2CacheSVM칭에서는 cache_inter_1 및 로 참조됩니다.cache_inter_2

오리진과 캐시 간에 클러스터 피어링 설정

cluster peer create ONTAP CLI 명령을 사용하여 Cache 및 클러스터에서 Source 클러스터 피어 관계를 설정합니다. 소스 및 대상 클러스터 간 LIF 기록 절차에서 이전에 저장한 클러스터 간 IP 주소를 제공합니다. 메시지가 표시되면 Origin 클러스터에서 클러스터 피어링을 설정할 때 입력해야 *cluster-peer-passphrase* 하는를 생성하라는 메시지가 표시됩니다.

1. 클러스터(FSx for ONTAP 파일 시스템)에서 Cache 클러스터 피어링을 설정합니다.

   a. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

   b. 다음 명령을 사용하여 생성한 암호를 기록합니다. 스케일 아웃 파일 시스템의 경우 각 HA 페어에 대한 inter_1 및 inter_2 IP 주소를 제공합니다.

   ```
   FSx-Cache::> cluster peer create -address-family ipv4 -peer-
   addrs origin_inter_1,origin_inter_2

   Enter the passphrase: cluster-peer-passphrase
   Confirm the passphrase: cluster-peer-passphrase
   Notice: Now use the same passphrase in the "cluster peer create" command in the
    other cluster.
   ```

2. 다음 명령을 사용하여 source (온프레미스) 클러스터에서 클러스터 피어링을 설정합니다. 인증하려면 이전 단계에서 생성한 암호를 입력해야 합니다. 스케일 아웃 파일 시스템의 경우 각 HA 페어의 클러스터 간 IP 주소를 제공해야 합니다.

```
Origin::> cluster peer create -address-family ipv4 -peer-
addrs cache_inter_1,cache_inter_2

Enter the passphrase: cluster-peer-passphrase
Confirm the passphrase: cluster-peer-passphrase
```

3. source 클러스터에서 다음 명령을 사용하여 클러스터 피어링이 성공적으로 설정되었는지 확인합니다. 출력에서 Availability를 Available로 설정해야 합니다.

```
Origin::> cluster peer show

Peer Cluster Name     Availability    Authentication
-------------------   -------------   --------------
Cache_ID              Available       ok
```

출력에가 표시되지 않으면 source 및 cache 클러스터에서 이전 단계를 Available반복합니다.

스토리지 가상 머신(SVM) 피어링 구성

클러스터 피어링을 성공적으로 설정한 후 다음 단계는 vserver peer 명령을 사용하여 캐시 클러스터(Cache)에 SVM 피어링 관계를 생성하는 것입니다. 다음 절차에 사용되는 추가 별칭은 다음과 같습니다.

- *CacheLocalName* - cache SVM에서 SVM 피어링을 구성할 때 origin SVM을 식별하는 데 사용되는 이름입니다.
- *OriginLocalName* - origin SVM에서 SVM 피어링을 구성할 때 cache SVM을 식별하는 데 사용되는 이름입니다.

1. cache SVM에서 다음 명령을 사용하여 SVM 피어링 관계를 생성합니다.

```
FSx-Cache::> vserver peer create -vserver CacheSVM -peer-vserver OriginSVM -peer-
cluster Origin_ID -local-name OriginLocalName -application flexcache
```

2. 소스 클러스터에서 다음 명령을 사용하여 SVM 피어링 관계를 수락합니다.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

3. 소스 클러스터에서 피어링 관계를 수락합니다.

```
Origin::> vserver peer accept -vserver OriginSVM -peer-vserver CacheSVM -local-
name CacheLocalName
```

4. 다음 명령을 사용하여 SVM 피어링이 성공했는지 확인합니다. 응답peered에서를 로 설정해야 `Peer State` 합니다.

```
Origin::> vserver peer show

Vserver      Peer Vserver    Peer State    Peering Cluster    Remote Applications

------------ --------------- ------------- ------------------
 ------------------------
OriginSVM    CacheSVM        peered        FSx-Cache          flexcache
```

FlexCache 볼륨 생성

SVM 피어링 관계를 성공적으로 생성한 후 다음 단계는 캐시 SVM에서 FlexCache 볼륨을 생성하는 것입니다. FlexCache 볼륨은 여야 합니다FlexGroup. FlexCache 볼륨에 대한 작업 모드도 선택합니다. 자세한 내용은 FlexCache 쓰기 모드 단원을 참조하십시오.

1. 캐시 클러스터에서 다음 ONTAP CLI 명령을 사용하여 FlexCache 볼륨을 생성합니다. 이 예제에서는 *CacheVol*이라는 2TB FlexCache 볼륨을 생성합니다.

   - 라이트어라운드 FlexCache 볼륨을 생성하려면 다음 명령을 사용합니다.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1
   ```

   - 라이트백 FlexCache 볼륨을 생성하려면 다음 명령을 사용합니다.

   ```
   FSx-Cache::> volume flexcache create -vserver CacheSVM -size 2t -volume CacheVol
    -origin-volume OriginVol -origin-vserver OriginSVM -junction-path /flexcache -
   aggr-list aggr1 -is-writeback-enabled true
   ```

> **Note**
>
> volume flexcache config modify -is-writeback-enabled {true|false} 명령을 사용하여 쓰기 모드를 수정할 수 있습니다. 이 명령을 사용하기 전에 set -privilege advanced 명령을 사용하여 ONTAP CLI 고급 모드로 전환해야 합니다.

2. FlexCache 볼륨과 오리진 볼륨 간의 FlexCache 관계를 확인합니다.

   - FlexCache 라이트 어라운드 볼륨의 경우 출력은 다음 예제와 비슷합니다.

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
-------   ----------  -------  --------------  -------------  --------------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
```

   - FlexCache 라이트백 볼륨의 경우 출력은 다음 예제와 비슷합니다.

```
FSx-Cache::> volume flexcache show

Vserver   Volume      Size     Origin-Vserver  Origin-Volume  Origin-Cluster
 Writeback
-------   ----------  -------  --------------  -------------  --------------
 ---------
CacheSVM  CacheVol    2TB      OriginSVM       OriginVol      Origin
 true
```

FlexCache 볼륨 탑재

FlexCache 볼륨이 AVAILABLE 상태가 되면 NFSv3, NFSv4 및 SMB 클라이언트가 볼륨을 탑재할 수 있습니다. 이 탑재되면 클라이언트FlexCache는 온프레미스 오리진 볼륨의 전체 데이터 세트에 액세스할 수 있습니다.

- 탑재 지점을 생성하고 FlexCache를 탑재하려면 클라이언트에서 다음 명령을 실행합니다.

```
$ sudo mkdir -p /fsx/CacheVol
$ sudo mount -t nfs management.fs-01d2f606463087f6d.fsx.us-east-1.amazonaws.com:/
CacheVol /fsx/CacheVol
```

를 사용하여 데이터 복제 NetApp SnapMirror

NetApp SnapMirror를 사용하여 두 번째 파일 시스템으로 또는 두 번째 파일 시스템에서 FSx for ONTAP 파일 시스템의 주기적 복제를 예약할 수 있습니다. 이 기능은 리전 내 배포와 크로스 리전 배포 모두에 사용할 수 있습니다.

NetApp SnapMirror는 데이터를 고속으로 복제하므로 두 Amazon FSx 파일 ONTAP 시스템 간에 복제 AWS하든 온프레미스에서 로 복제하든 관계없이 시스템 간에 높은 데이터 가용성과 빠른 데이터 복제를 얻을 수 있습니다 AWS. RPO(복구 지점 목표), RTO(복구 시간 목표) 및 성능 고려 사항에 따라 간격을 신중하게 선택해야 하지만 복제 빈도를 5분까지 예약할 수 있습니다.

NetApp 스토리지 시스템에 데이터를 복제하고 보조 데이터를 지속적으로 업데이트하면 데이터가 최신 상태로 유지되고 필요할 때마다 사용할 수 있습니다. 외부 복제 서버가 필요하지 않습니다. 를 사용하여 데이터를 복제NetApp SnapMirror하는 방법에 대한 자세한 내용은 NetApp BlueXP 설명서의 복제 서비스에 대해 알아보기를 참조하세요.

NetApp ONTAP CLI 및 REST API 외에도 Amazon FSx 콘솔, AWS CLI및 Amazon FSx API를 NetApp SnapMirror 사용하기 위한 데이터 보호(DP) 대상 볼륨을 생성할 수 있습니다. Amazon FSx 콘솔을 사용하여 대상 볼륨을 생성하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요볼륨 생성.

NetApp BlueXP 또는 ONTAP CLI를 사용하여 파일 시스템의 복제를 예약할 수 있습니다.

> **Note**
>
> SnapMirror 복제에는 볼륨 레벨 SnapMirror와 SVM 재해 복구(SVMDR)라는 두 가지 유형이 있습니다. FSx for ONTAP에서는 볼륨 수준 SnapMirror 복제만 지원됩니다. Synchronous SnapMirror를 포함한 StrictSync는 지원되지 않습니다.

NetApp BlueXP를 사용하여 복제 예약

NetApp BlueXP를 사용하여 FSx for ONTAP 파일 시스템에서 SnapMirror로 복제를 설정할 수 있습니다. 자세한 내용은 NetApp BlueXP 설명서의 시스템 간 데이터 복제를 참조하세요.

ONTAP CLI를 사용하여 복제 예약

ONTAP CLI를 사용하여 예약된 볼륨 복제를 구성할 수 있습니다. 자세한 내용은 NetApp ONTAP 설명서 센터의 SnapMirror 볼륨 복제 관리를 참조하세요.

AWS FSx for ONTAP에 대한 결제 및 사용 보고서

AWS 는 FSx for ONTAP에 대한 두 가지 사용 보고서를 제공합니다.

- AWS 결제 보고서는 FSx for ONTAP을 포함하여 사용 중인 모든 활동에 대한 AWS 서비스 상위 수준 보기입니다.
- AWS 사용 보고서는 특정 서비스에 대한 활동을 시간, 일 또는 월별로 집계한 요약입니다. 또한 FSx for ONTAP 사용량을 그래픽으로 표현하는 사용 차트도 포함되어 있습니다.

> **Note**
>
> 다른 것과 마찬가지로 AWS 서비스 FSx for ONTAP는 사용한 만큼만 요금을 청구합니다. 자세한 내용은 Amazon FSx for NetApp ONTAP 요금을 참조하세요.

FSx for ONTAP에 대한 AWS 결제 보고서 보기

AWS 결제 및 비용 관리 콘솔의 청구서 페이지에서 서비스별로 나열된 AWS 사용량 및 요금 요약을 볼 수 있습니다.

AWS 결제 보고서를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/costmanagement/ AWS 결제 및 비용 관리 콘솔을 엽니다.
2. 탐색 창에서 청구서(Bills)를 선택합니다.
3. 결제 기간(예: 2024년 8월)을 선택합니다.
4. Amazon FSx 요금을 보려면 서비스별 요금 탭에서 서비스별 필터 텍스트 필드에 FSx를 입력한 다음 FSx를 확장하여 요금을 확인합니다 AWS 리전.

   FSx for ONTAP 파일 시스템에 대한 요금은 보고서의 Amazon FSx CreateFileSystem:ONTAP 항목 아래에 표시됩니다.
5. CSV 형식으로 세부 결제 보고서를 다운로드하려면 청구서 페이지 상단에서 CSV로 모두 다운로드를 선택합니다.

AWS 청구서에 대한 자세한 내용은 AWS Billing 사용 설명서의 청구서 보기를 참조하세요.

결제 보고서에는 FSx for ONTAP 파일 시스템에 적용되는 다음과 같은 사용 유형이 포함됩니다.

First generation FSx for ONTAP file systems

요금 유형	단위	설명	
ONTAP 단일 AZ SSD 스토리지	GB-월	1세대 Single-AZ ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양	
ONTAP 다중 AZ SSD 스토리지	GB-월	1세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양	
ONTAP 단일 AZ 처리량 용량	MBps-월	1세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량	
ONTAP 다중 AZ 처리량 용량	MBps-월	1세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량	
프로비저닝된 ONTAP 단일 AZ SSD IOPS	IOPS-월	1세대 Single-AZ FSx for ONTAP 파일 시스템에서 프로비저닝된 SSD IOPS의 양	
프로비저닝된 ONTAP 다중 AZ SSD IOPS	IOPS-월	1세대 Multi-AZ FSx for ONTAP 파일 시스템에서 프로비저닝된 SSD IOPS의 양	

Second generation FSx for ONTAP file systems

요금 유형	단위	설명	
ONTAP Single-AZ-2 SSD 스토리지	GB-월	2세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양	

요금 유형	단위	설명	
ONTAP Multi-AZ-2 SSD 스토리지	GB-월	2세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양	
ONTAP Single-AZ-2 처리량 용량	MBps-월	2세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량	
ONTAP Multi-AZ-2 처리량 용량	MBps-월	2세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량	
프로비저닝된 ONTAP Single-AZ-2 SSD IOPS	IOPS-월	2세대 Single-AZ FSx for ONTAP 파일 시스템에서 프로비저닝된 SSD IOPS의 양	
프로비저닝된 ONTAP Multi-AZ-2 SSD IOPS	IOPS-월	2세대 Multi-AZ FSx for ONTAP 파일 시스템에서 프로비저닝된 SSD IOPS의 양	

All FSx for ONTAP filesystems

요금 유형	단위	설명	
ONTAP 표준 용량 풀 스토리지	GB-월	FSx for ONTAP 파일 시스템에서 사용하는 용량 풀 스토리지의 양입니다.	
ONTAP 백업 스토리지	GB-월	백업에 사용되는 스토리지 용량	
SnapLock 사용	GB-월	SnapLock 볼륨에서 사용하는 스토리지 용량	

요금 유형	단위	설명	
ONTAP 표준 용량 풀 스토리지에 대한 읽기 요청	운영	FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 읽기 요청 수	
ONTAP 표준 용량 풀 스토리지에 요청 쓰기	운영	FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 쓰기 요청 수	

FSx for ONTAP AWS 사용 보고서 보기

AWS 는 결제 보고서보다 더 자세한 FSx 사용 보고서를 제공합니다. 사용량 보고서는 시간, 일 또는 월별 집계 사용량 데이터를 제공하며 리전 및 사용량 유형별로 작업을 나열합니다.

AWS 사용 보고서를 보려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/costmanagement/ AWS 결제 및 비용 관리 콘솔을 엽니다.
2. 탐색 창에서 Cost Explorer를 선택합니다.
3. 보고서 파라미터 섹션에서 보고서의 날짜 범위 및 세부 수준을 선택합니다.
4. 그룹화 기준 > 차원을 서비스로 설정한 상태로 둡니다.
5. 필터 > 서비스에서를 선택합니다. FSx
6. 사용 유형을 선택합니다. FSx for ONTAP 사용 유형 목록은이 절차에 따라 표를 참조하세요.
7. 보고서에 대해 추가 필터를 선택합니다.
8. 보고서 세부 정보를 파일로 다운로드하려면 CSV로 다운로드를 선택합니다.

다음 표에는 ONTAP 파일 시스템의 사용 데이터를 보기 위해 보고서를 필터링하는 데 사용할 수 있는 FSx for ONTAP 사용 유형이 나열되어 있습니다. Cost Explorer 사용에 대한 자세한 내용은 AWS Cost Management 사용 설명서의 를 사용하여 비용 및 사용량 분석을 참조하세요 AWS Cost Explorer.

First generation FSx for ONTAP file systems

사용 유형	단위	설명
region-Storage.SAZ_2N:SSD	GB-월	1세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양입니다.
region-Storage.MAZ:SSD	GB-월	1세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양입니다.
region-ThroughputCapacity.SAZ_2N	MiBps-Mo	1세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량입니다.
region-ThroughputCapacity.MAZ	MiBps-Mo	1세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량입니다.
region-ProvisionedSSDIOPS.SAZ_2N	IOPS-Mo	1세대 Single-AZ FSx for ONTAP 파일 시스템에서 SSD 스토리지의 GiB당 3 IOPS 이상으로 프로비저닝된 SSD IOPS의 양입니다.
region-ProvisionedSSDIOPS.MAZ	IOPS-Mo	1세대 Multi-AZ FSx for ONTAP 파일 시스템에서 SSD 스토리지의 GiB당 3 IOPS 이상으로 프로비저닝된 SSD IOPS의 양입니다.

Second generation FSx for ONTAP file systems

사용 유형	단위	설명
region-Storage.SAZ_2N2:SSD	GB-월	2세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양입니다.

사용 유형	단위	설명
region-Storage.MAZ2:SSD	GB-월	2세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 SSD 스토리지의 양입니다.
region-ThroughputCapacity.SAZ_2N2	MiBps-Mo	2세대 Single-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량입니다.
region-ThroughputCapacity.MAZ2	MiBps-Mo	2세대 Multi-AZ FSx for ONTAP 파일 시스템에 프로비저닝된 처리량 용량입니다.
region-ProvisionedSSDIOPS.SAZ_2N2	IOPS-Mo	2세대 Single-AZ FSx for ONTAP 파일 시스템에서 SSD 스토리지의 GiB당 3 IOPS 이상으로 프로비저닝된 SSD IOPS의 양입니다.
region-ProvisionedSSDIOPS.MAZ2	IOPS-Mo	2세대 Multi-AZ FSx for ONTAP 파일 시스템에서 SSD 스토리지의 GiB당 3 IOPS 이상으로 프로비저닝된 SSD IOPS의 양입니다.

All FSx for ONTAP file systems

사용 유형	단위	설명
region-Storage.SAZ_2N:CPoolStd	GB-Mo	1세대 또는 2세대 Single-AZ FSx for ONTAP 파일 시스템에 사용되는 표준 용량 풀 스토리지의 양입니다.
region-Storage.MAZ:CPoolStd	GB-Mo	1세대 또는 2세대 Multi-AZ FSx for ONTAP 파일 시스템에 사용되는 표준 용량 풀 스토리지의 양입니다.

사용 유형	단위	설명
region-BackupUsage	GB-월	백업에 사용되는 스토리지 용량입니다.
region-SnaplockUsage	GB-월	SnapLock 볼륨에서 사용하는 스토리지 용량입니다.
region-Requests.SAZ_2N:CPoolStdRd	운영	단일 AZ FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 읽기 요청 수입니다.
region-Requests.SAZ_2N:CPoolStdWr	운영	단일 AZ FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 쓰기 요청 수입니다.
region-Requests.MAZ:CPoolStdRd	운영	다중 AZ FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 읽기 요청 수입니다.
region-Requests.MAZ:CPoolStdWr	운영	다중 AZ FSx for ONTAP 파일 시스템의 표준 용량 풀 스토리지에 대한 쓰기 요청 수입니다.

Amazon FSx for NetApp ONTAP 모니터링

다음 서비스 및 도구를 사용하여 Amazon FSx for NetApp ONTAP 사용량 및 활동을 모니터링할 수 있습니다.

- Amazon CloudWatch – FSx for ONTAP에서 원시 데이터를 자동으로 수집하여 읽기 가능한 지표로 처리하는 Amazon CloudWatch를 사용하여 파일 시스템을 모니터링할 수 있습니다. 이러한 통계는 15개월간 기록되므로 기록 정보를 확인하고 파일 시스템이 어떻게 실행되고 있는지 파악할 수 있습니다. 또한 지정된 기간 동안 지표를 기반으로 경보를 설정하고 지정한 임계값을 기준으로 지표 값에 따라 하나 이상의 작업을 수행할 수 있습니다.
- ONTAP EMS 이벤트 - ONTAP의 이벤트 관리 시스템(EMS)에서 생성된 이벤트를 사용하여 FSx for ONTAP 파일 시스템을 모니터링할 수 있습니다. EMS 이벤트는 iSCSI LUN 생성 또는 볼륨 자동 크기 조정과 같이 파일 시스템에서 발생하는 상황에 대한 알림입니다.
- NetApp Data Infrastructure Insights - NetApp Data Infrastructure Insights 서비스를 사용하여 FSx for ONTAP 파일 시스템의 구성, 용량 및 성능 지표를 모니터링할 수 있습니다. 지표 조건에 따라 알림을 생성할 수도 있습니다.
- NetApp Harvest 및 NetApp Grafana – NetApp Harvest와 NetApp Grafana를 사용하여 FSx for ONTAP 파일 시스템을 모니터링할 수 있습니다. NetApp Harvest는 FSx for ONTAP 파일 시스템에서 성능, 용량 및 하드웨어 지표를 수집하여 ONTAP 파일 시스템을 모니터링합니다. Grafana는 수집된 Harvest 지표를 표시할 수 있는 대시보드를 제공합니다.
- AWS CloudTrail - AWS CloudTrail 를 사용하여 Amazon FSx에 대한 모든 API 호출을 이벤트로 캡처할 수 있습니다. 이러한 이벤트는 Amazon FSx의 사용자, 역할 또는 AWS 서비스에 의해 수행된 작업의 레코드를 제공합니다.

주제

Amazon CloudWatch를 사용한 모니터링

Amazon FSx for NetApp ONTAP에서 원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 파일 시스템을 모니터링할 수 있습니다. 이러한 통계는 15개월 간 기록되므로 기록 정보를 확인하고 파일 시스템이 어떻게 실행되고 있는지 파악할 수 있습니다. FSx for ONTAP 지표 데이터는 기본적으로 1분마다 CloudWatch에 자동 전송됩니다. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch란 무엇인가요?를 참조하세요.

> **Note**
>
> 기본적으로 FSx for ONTAP은 1분 간격으로 CloudWatch에 지표 데이터를 전송합니다. 단, 5분 간격으로 전송되는 다음 지표는 예외입니다.
>
> - `FileServerDiskThroughputBalance`
> - `FileServerDiskIopsBalance`

FSx for ONTAP에 대한 CloudWatch 지표는 각 지표를 쿼리하는 데 사용되는 측정기준에 따라 정의되는 네 가지 범주로 구성됩니다. 측정기준에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 측정기준 섹션을 참조하세요.

- 파일 시스템 지표: 파일 시스템 수준 성능 및 스토리지 용량 지표.
- 파일 서버 지표: 파일 서버 수준 지표입니다.
- 세부 파일 시스템 집계 지표: 집계당 세부 파일 시스템 지표입니다.
- 세부 파일 시스템 지표: 스토리지 계층(SSD 및 용량 풀)별 파일 시스템 수준 스토리지 지표.
- 볼륨 지표: 볼륨별 성능 및 스토리지 용량 지표.
- 세부 볼륨 지표: 스토리지 계층 또는 데이터 유형(사용자, 스냅샷 또는 기타)에 따른 볼륨별 스토리지 용량 지표.

FSx for ONTAP에 대한 모든 CloudWatch 지표는 CloudWatch의 `AWS/FSx` 네임스페이스에 게시됩니다.

주제

- CloudWatch 지표 액세스
- Amazon FSx 콘솔에서 모니터링

- 파일 시스템 지표
- 2세대 파일 시스템 지표
- 볼륨 지표

CloudWatch 지표 액세스

다음과 같은 방법으로 Amazon FSx에 대한 Amazon CloudWatch 지표를 확인할 수 있습니다.

- Amazon FSx 콘솔
- Amazon CloudWatch 콘솔
- CloudWatch용 AWS Command Line Interface (AWS CLI)
- CloudWatch API

다음 절차는 Amazon FSx 콘솔을 사용하여 파일 시스템의 CloudWatch 지표를 보는 방법을 설명합니다.

Amazon FSx 콘솔을 사용하여 파일 시스템에 대한 CloudWatch 지표 확인

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 확인하려는 파일 시스템을 선택합니다.
3. 요약 페이지의 두 번째 패널에서 모니터링 및 성능을 선택하여 파일 시스템 지표에 대한 그래프를 확인합니다.

모니터링 및 성능 패널에는 네 개의 탭이 있습니다.

- 요약(기본 탭)을 선택하면 활성 경고, CloudWatch 경보 및 파일 시스템 활동에 대한 그래프가 표시됩니다.
- 스토리지를 선택하면 용량 및 사용률 지표가 표시됩니다.
- 성능을 선택하면 파일 서버 및 스토리지 성능 지표가 표시됩니다.
- CloudWatch 경보를 선택하면 파일 시스템에 구성된 모든 경보의 그래프가 표시됩니다.

다음 절차는 Amazon FSx 콘솔을 사용하여 볼륨의 CloudWatch 지표를 보는 방법을 설명합니다.

Amazon FSx 콘솔을 사용하여 볼륨에 대한 CloudWatch 지표 확인

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 볼륨을 선택한 다음 확인하려는 볼륨을 선택합니다.
3. 요약 페이지의 두 번째 패널에서 모니터링(기본 탭)을 선택하여 볼륨 지표에 대한 그래프를 확인합니다.

다음 절차는 Amazon CloudWatch 콘솔을 사용하여 파일 시스템의 CloudWatch 지표를 보는 방법을 설명합니다.

Amazon CloudWatch 콘솔을 사용한 지표 확인

1. 파일 시스템의 요약 페이지의 두 번째 패널에서 모니터링 및 성능을 선택하여 파일 시스템 지표에 대한 그래프를 확인합니다.
2. Amazon CloudWatch 콘솔에서 보려는 그래프 오른쪽 상단에 있는 작업 메뉴에서 지표에서 보기를 선택합니다. 그러면 Amazon CloudWatch 콘솔에 지표 페이지가 열립니다.

다음 절차는 Amazon CloudWatch 콘솔의 대시보드에 FSx for ONTAP 파일 시스템 지표를 추가하는 방법을 설명합니다.

Amazon CloudWatch 콘솔에 지표 추가

1. Amazon FSx 콘솔의 모니터링 및 성능 패널에서 지표 세트(요약, 스토리지 또는 성능)를 선택합니다.
2. 패널 오른쪽 상단에서 대시보드에 추가를 선택합니다. 그러면 Amazon CloudWatch 콘솔이 열립니다.
3. 목록에서 기존 CloudWatch 대시보드를 선택하거나 새 대시보드를 생성합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 Amazon CloudWatch 대시보드 사용을 참조하세요.

다음 절차는 AWS CLI를 사용하여 파일 시스템 지표에 액세스하는 방법을 설명합니다.

에서 지표에 액세스하려면 AWS CLI

- CloudWatch list-metrics CLI 명령을 `--namespace "AWS/FSx"` 파라미터와 함께 사용합니다. 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

다음 절차는 CloudWatch API를 사용하여 파일 시스템 지표에 액세스하는 방법을 설명합니다.

CloudWatch API에서 지표에 액세스

- GetMetricStatistics API 작업을 호출합니다. 자세한 내용은 Amazon CloudWatch API 참조를 참조하세요.

Amazon FSx 콘솔에서 모니터링

Amazon FSx에서 보고하는 CloudWatch 지표는 FSx for ONTAP 파일 시스템 및 볼륨에 대한 중요한 정보를 제공합니다.

주제

Amazon FSx 콘솔에서 파일 시스템 지표 모니터링

Amazon FSx 콘솔의 파일 시스템 대시보드에서 모니터링 및 성능 패널을 사용하여 다음 표에 설명된 지표를 볼 수 있습니다. 자세한 내용은 CloudWatch 지표 액세스 섹션을 참조하세요.

모니터링 및 성능	방법	차트	관련 지표
요약	...파일 시스템에서 사용 가능한 스토리지 용량을 어떻게 확인하나요?	사용 가능한 기본 스토리지 용량(바이트)	`StorageCapacity {SSD} - StorageUsed {SSD}`
	...파일 시스템의 총 클라이언트 처리량을 어떻게 확인하나요?	총 클라이언트 처리량(바이트/초)	합계(`DataReadBytes +DataWriteBytes`)/기간(초)

모니터링 및 성능	방법	차트	관련 지표
	...파일 시스템의 총 클라이언트 IOPS를 어떻게 확인하나요?	총 클라이언트 IOPS(초당 작업 수)	합계(DataReadOperations +DataWriteOperations +MetadataOperations)/기간(초)
	...파일 시스템의 읽기, 쓰기 및 메타데이터 작업에 대한 평균 지연 시간을 어떻게 확인하나요?	평균 지연 시간(ms/작업)	평균 읽기 지연 시간: DataReadOperationTime *1,000/DataReadOperations 평균 쓰기 지연 시간: DataWriteOperationTime *1,000/DataWriteOperations 평균 메타데이터 지연 시간: MetadataOperationTime * 1,000/MetadataOperations
	...파일 시스템에서 사용된 스토리지 용량과 사용 가능한 스토리지 용량의 분포를 어떻게 확인하나요?	스토리지 배포	사용 가능한 기본 계층: StorageCapacity {SSD}~StorageUsed {SSD} 사용된 기본 계층: StorageUsed {SSD} 사용된 용량 풀: StorageUsed {StandardCapacityPool }

모니터링 및 성능	방법	차트	관련 지표
	...스토리지 효율성(압축, 중복 제거, 축소)으로 인한 절감 효과를 어떻게 확인하나요?	스토리지 효율성 절감	StorageEfficiencySavings
스토리지	...사용 가능한 기본 스토리지 용량을 어떻게 확인하나요?	사용 가능한 기본 스토리지 용량(바이트)	StorageCapacity {SSD} - StorageUsed {SSD}
	...파일 시스템에 사용된 기본 스토리지의 비율을 어떻게 확인하나요?	기본 스토리지 용량 사용률(백분율)	StorageUsed {SSD}*100/StorageCapacity {SSD}
	...파일 시스템이 네트워크 처리량 한도에 근접하고 있는지 어떻게 확인하나요?	네트워크 처리량 - 사용률(백분율)	NetworkThroughputUtilization
파일 서버 성능	...파일 시스템이 디스크 처리량 한도에 근접하고 있는지 어떻게 확인하나요?	디스크 처리량 - 사용률(백분율)	FileServerDiskThroughputUtilization
	...파일 시스템이 디스크 처리량에 대해 허용된 버스트 크레딧을 모두 사용했는지 어떻게 확인하나요?	디스크 처리량 - 버스트 밸런스(백분율)	FileServerDiskThroughputBalance

모니터링 및 성능	방법	차트	관련 지표
	...파일 시스템이 파일 서버의 SSD IOPS 한도에 근접하고 있는지 어떻게 확인하나요?	디스크 IOPS - 사용률(백분율)	`FileServerDiskIopsUtilization`
	...파일 시스템이 파일 서버의 디스크 SSD IOPS에 대해 허용한 버스트 크레딧을 모두 사용했는지 어떻게 확인하나요?	디스크 IOPS - 버스트 밸런스(백분율)	`FileServerDiskIopsBalance`
	...파일 시스템 CPU의 평균 사용률을 어떻게 확인하나요?	CPU 사용률(백분율)	`CPUUtilization`
	...워크로드가 파일 시스템의 RAM 및 NVMe 읽기 캐시를 효율적으로 사용하고 있는지 어떻게 확인하나요?	캐시 적중률(백분율)	`FileServerCacheHitRatio`
디스크 성능	...파일 시스템이 현재 프로비저닝된 SSD IOPS 용량에 근접하고 있는지 어떻게 확인하나요?	디스크 IOPS - 사용률(SSD)(백분율)	`DiskIopsUtilization`

> **Note**
>
> 네트워크 사용률, CPU 사용률, SSD IOPS 사용률 등 모든 성능 관련 측정기준의 평균 처리량 용량 사용률을 50% 미만으로 유지하는 것이 좋습니다. 이렇게 하면 예상치 못한 워크로드 스파이크는 물론 백그라운드 스토리지 작업(예: 스토리지 동기화, 데이터 계층화 또는 백업)에 필요한 예비 처리량 용량을 충분히 확보할 수 있습니다.

Amazon FSx 콘솔에서 볼륨 지표 모니터링

Amazon FSx 콘솔에서 볼륨의 대시보드에 있는 모니터링 패널을 보고 추가 성능 지표를 확인할 수 있습니다. 자세한 내용은 CloudWatch 지표 액세스 섹션을 참조하세요.

모니터링	방법	차트	관련 지표
	...볼륨의 사용 가능한 스토리지 용량을 어떻게 확인하나요?	사용 가능한 스토리지 용량	`StorageCapacity`
	...볼륨의 총 클라이언트 처리량을 어떻게 확인하나요?	총 클라이언트 처리량(바이트/초)	합계(`DataReadBytes +DataWriteBytes `)/기간(초)
	...볼륨의 총 클라이언트 IOPS를 어떻게 확인하나요?	총 클라이언트 IOPS(초당 작업 수)	합계(`DataReadOperations +DataWriteOperations +MetadataOperations `)/기간(초)
	...용량 풀 계층에서 들어오고 나가는 읽기 및 쓰기 작업 수를 어떻게 확인하나요?	용량 풀 IOPS(작업/초)	읽기 작업: `CapacityPoolReadOperations` 쓰기 작업: `CapacityPoolWriteOperations`
	...볼륨의 읽기, 쓰기 및 메타데이터 작업에 대한 평균 지연 시간을 어떻게 확인하나요?	평균 지연 시간(ms/작업)	평균 읽기 지연 시간: `DataReadOperationTime *1,000/DataReadOperations` 평균 쓰기 지연 시간: `DataWriteOperationTime *1,000/DataWriteOperations`

모니터링	방법	차트	관련 지표
			평균 메타데이터 지연 시간: `MetadataOperationTime *1,000/MetadataOperations`
	...볼륨에서 사용할 수 있는 파일 또는 아이노드의 양을 어떻게 확인하나요?	사용 가능한 파일(아이노드)	`FilesCapacity - FilesUsed`
	...볼륨에서 사용된 스토리지 용량과 사용 가능한 스토리지 용량의 분포를 어떻게 확인하나요?	스토리지 배포	`StorageCapacity - StorageUsed`

성능 경고 및 권장 사항

FSx for ONTAP은 CloudWatch 지표 중 하나가 연속된 여러 데이터 포인트에 대해 미리 정해진 임계값에 도달하거나 이를 초과할 때마다 CloudWatch 지표에 대한 경고를 표시합니다. 이러한 경고는 파일 시스템 성능을 최적화하는 데 사용할 수 있는 실행 가능한 권장 사항을 제공합니다.

모니터링 및 성능 대시보드의 여러 영역에서 경고에 액세스할 수 있습니다. 모든 활성 또는 최신 Amazon FSx 성능 경고와 경보 상태인 파일 시스템에 대해 구성된 모든 CloudWatch 경보가 요약 섹션의 모니터링 및 성능 패널에 표시됩니다. 이 경고는 지표 그래프가 표시되는 대시보드 섹션에도 표시됩니다.

모든 Amazon FSx 지표에 대해 CloudWatch 경보를 생성할 수 있습니다. 자세한 내용은 Amazon FSx를 모니터링하여 Amazon CloudWatch 경보 생성 섹션을 참조하세요.

성능 경고를 사용하면 파일 시스템 성능을 개선할 수 있습니다.

Amazon FSx는 파일 시스템 성능을 최적화하는 데 사용할 수 있는 실행 가능한 권장 사항을 제공합니다. 이러한 권장 사항은 잠재적인 성능 병목 현상을 해결할 수 있는 방법을 설명합니다. 활동이 계속될 것으로 예상되거나 이로 인해 파일 시스템 성능이 저하되는 경우 권장 조치를 취할 수 있습니다. 경고를 트리거한 지표에 따라 다음 표에 설명된 대로 파일 시스템의 처리량 용량 또는 스토리지 용량을 늘려 경고를 해결할 수 있습니다.

대시보드 섹션	이 지표에 대한 경고가 있는 경우	조치
스토리지	기본 스토리지 용량 사용률	파일 시스템이 아직 최대 SSD 스토리지 용량에 도달하지 않은 경우 파일 시스템의 기본 스토리지 용량을 늘리세요. 자세한 내용은 스토리지 용량 및 프로비저닝된 IOPS 업데이트 단원을 참조하십시오. 파일 시스템에 HA 페어가 여러 개 있고 파일 시스템 집계(기본 스토리지 계층을 구성하는 스토리지 풀)의 하위 집합에 대해서만 기본 스토리지 용량 사용률이 더 높은 경우, 기본 스토리지 용량 사용률이 파일 시스템 전체에 더 균등하게 분산되도록 워크로드를 재조정할 수도 있습니다. 워크로드 리밸런싱에 대한 자세한 내용은 HA 페어 간에 워크로드 밸런싱을 참조하세요.
파일 서버 성능	네트워크 처리량 디스크 처리량 디스크 IOPS CPU 사용률	파일 시스템이 아직 최대 처리량 용량에 도달하지 않은 경우 파일 시스템의 처리량 용량을 늘리세요. 처리량 용량 업데이트에 대한 자세한 내용은 처리량 용량 업데이트를 참조하세요. 파일 시스템에 HA 페어가 여러 개 있고 파일 서버의 하위 집합에 대해서만 사용률이 높은 경우 워크로드를 재조정하여 각 파일 시스템의 HA 페어의 성능 기능을 보다 균등하게 활용할 수 있습니다. 워크로드 리밸런싱에 대한 자세한 내용은 HA 페어 간에 워크로드 밸런싱을 참조하세요.
디스크 성능	디스크 IOPS	파일 시스템이 파일 시스템의 현재 처리량 용량에 대한 최대 SSD IOPS에 아직 도달하지 않은 경우 SSD IOPS를 늘립니다. 파일 시스템의 프로비저닝된 IOPS 업데이트에 대한 자세한 내용은 스토리지 용량 및 프로비저닝된 IOPS 업데이트을 참조하세요. 파일 시스템에 HA 페어가 여러 개 있고 디스크 IOPS 사용률이 파일 시스템 집계의 하위 집합(기본 스토리지 계층을 구성하는 스토리지 풀)에 대해서만 더 높은 경우, 파일 시스템 전체에서 디스크 IOPS가 더 균등하게 활용

대시보드 섹션	이 지표에 대한 경고가 있는 경우	조치
		되도록 워크로드를 재조정할 수도 있습니다. 워크로드 리밸런싱에 대한 자세한 내용은 HA 페어 간에 워크로드 밸런싱을 참조하세요.

파일 시스템 성능에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 성능 섹션을 참조하세요.

Amazon FSx를 모니터링하여 Amazon CloudWatch 경보 생성

경보 때문에 상태가 변경되면 Amazon Simple Notification Service(Amazon SNS) 메시지를 보내는 CloudWatch 경보를 생성할 수 있습니다. 경보는 지정한 기간 동안 단일 지표를 감시합니다. 필요한 경우 경보는 기간 수에 대해 지정된 임계값과 지표 값을 비교하여 하나 이상의 작업을 수행합니다. 이 작업은 Amazon SNS 주제 또는 Auto Scaling 정책에 전송되는 알림입니다.

경보는 지속적인 상태 변경에 대해서만 작업을 호출합니다. CloudWatch 경보는 특정 상태에 있다는 이유만으로는 작업을 호출하지 않습니다. 상태가 변경되고 지정한 기간 동안 유지되어야 합니다. Amazon FSx 콘솔 또는 Amazon CloudWatch 콘솔에서 경보를 생성할 수 있습니다.

다음 절차에서는 Amazon FSx 콘솔, AWS Command Line Interface (AWS CLI) 및 API를 사용하여 경보를 생성하는 방법을 설명합니다.

Amazon FSx 콘솔을 사용한 경보 설정

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 파일 시스템을 선택한 다음 경보를 생성할 파일 시스템을 선택합니다.
3. 요약 페이지의 두 번째 패널에서 모니터링 및 성능 선택합니다.
4. CloudWatch 경보 탭을 선택합니다.
5. CloudWatch 경보 생성을 선택합니다. 그러면 CloudWatch 콘솔로 리디렉션됩니다.
6. 지표 선택을 선택합니다.
7. 지표 섹션에서 FSx를 선택합니다.
8. 지표 범주 선택:

   - 파일 시스템 지표
   - 세부 파일 시스템 지표
   - 볼륨 지표

- 세부 볼륨 지표

9. 경보를 설정하려는 지표를 선택한 다음, 지표 선택을 선택합니다.
10. 조건 섹션에서 경보에 적용할 조건을 선택한 후 다음을 선택합니다.

> **Note**
>
> 파일 시스템 유지 관리 중에는 지표가 게시되지 않을 수 있습니다. 불필요하고 오해의 소지가 있는 경보 조건 변경을 방지하고 누락된 데이터 포인트에 대해 복원력을 갖도록 경보를 구성하려면 Amazon CloudWatch 사용 설명서의 CloudWatch 경보가 누락된 데이터를 처리하는 방법 구성을 참조하세요.

11. 경보 상태가 작업을 시작할 때 CloudWatch에서 이메일 또는 Amazon SNS 알림을 보내도록 하려면 경보 상태 트리거에 경보 상태를 선택합니다.

    다음 SNS 주제로 알림 전송에서 옵션을 선택합니다. 주제 생성을 선택한 경우 새 이메일 구독 목록에 대한 이름 및 이메일 주소를 설정할 수 있습니다. 이 목록은 향후 경보를 위해 필드에 저장되고 표시됩니다. 다음을 선택합니다.

> **Note**
>
> 새 Amazon SNS 주제를 생성하기 위해 주제 생성을 사용할 경우 이메일 주소는 알림을 받기 전에 검증되어야 합니다. 이메일은 경보가 경보 상태에 입력될 때만 전송됩니다. 이러한 경보 상태 변경이 이메일이 검증되기 전에 발생할 경우에는 알림을 받지 못합니다.

12. 경보 이름 및 경보 설명 필드를 입력한 후 다음을 선택합니다.
13. 미리 보기 및 생성 페이지에서 생성하려는 경보를 검토한 다음 경보 생성을 선택합니다.

CloudWatch 콘솔을 사용하여 경보를 설정하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. Amazon FSx 콘솔을 사용하여 경보를 설정하려면 6단계부터 시작하여 절차를 따릅니다.

를 사용하여 경보를 설정하려면 AWS CLI

- put-metric-alarm CLI 명령을 호출합니다. 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

CloudWatch API를 사용하여 경보 설정

- PutMetricalAlarm API 작업을 호출합니다. 자세한 내용은 Amazon CloudWatch API 참조를 참조하세요.

파일 시스템 지표

Amazon FSx for NetApp ONTAP 파일 시스템 지표는 파일 시스템 지표 또는 세부 파일 시스템 지표로 분류됩니다.

- 파일 시스템 지표는 단일 측정기준인 `FileSystemId`를 가지는 단일 파일 시스템에 대한 총 성능 및 스토리지 지표입니다. 이 지표는 파일 시스템의 네트워크 성능과 스토리지 용량 사용량을 측정합니다.
- 세부 파일 시스템 지표는 파일 시스템의 스토리지 용량과 각 스토리지 계층(예: SSD 스토리지 및 용량 풀 스토리지)에서 사용된 스토리지를 측정합니다. 각 지표에는 `FileSystemId`, `StorageTier` 및 `DataType` 측정기준이 포함되어 있습니다.

Amazon FSx가 이러한 지표에 대한 데이터 포인트를 CloudWatch 에 게시하는 경우에 대한 다음 사항에 유의하세요.

- 사용률 지표(`NetworkThroughputUtilization`과 같이 이름이 사용률로 끝나는 모든 지표)의 경우 모든 활성 파일 서버 또는 집계에 대해 각 기간마다 데이터 포인트가 방출됩니다. 예를 들어 Amazon FSx는 `FileServerDiskIopsUtilization`의 경우 활성 파일 서버당 1분 단위 지표를, `DiskIopsUtilization`의 경우 집계당 1분 단위 지표를 내보냅니다.
- 다른 모든 지표의 경우 각 기간마다 단일 데이터 포인트가 방출되며, 이는 모든 활성 파일 서버(예: `DataReadBytes` 파일 서버 지표) 또는 모든 집계(예: `DiskReadBytes` 스토리지 지표)에 대한 지표의 총 값에 해당합니다.

주제

네트워크 I/O 지표

이러한 모든 지표는 하나의 측정기준인 FileSystemId를 가집니다.

지표	설명
NetworkThroughputUtilization	파일 시스템에 대한 네트워크 처리량 사용률입니다. Average 통계는 지정된 기간 동안 파일 시스템의 평균 네트워크 처리량 사용률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 가장 낮은 네트워크 처리량 사용률입니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 가장 높은 네트워크 처리량 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
NetworkSentBytes	파일 시스템에서 전송한 바이트 수(네트워크 I/O)입니다. Sum 통계는 파일 시스템에서 지정된 기간 동안 전송된 총 바이트 수입니다. 통계를 위해 전송된 처리량(바이트/초)을 계산하려면 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
NetworkReceivedBytes	파일 시스템에서 수신한 바이트 수(네트워크 I/O)입니다. Sum 통계는 파일 시스템에서 지정된 기간 동안 수신한 총 바이트 수입니다.

지표	설명
	통계를 위해 수신한 처리량(바이트/초)을 계산하려면 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
DataReadBytes	클라이언트가 파일 시스템으로 읽기에서 발생한 바이트 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 읽기 작업과 연결된 총 바이트 수입니다. 일정 기간 평균 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
DataWriteBytes	파일 시스템에 대한 클라이언트의 쓰기 작업으로 발생한 바이트 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 쓰기 작업과 연결된 총 바이트 수입니다. 일정 기간 평균 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum

지표	설명
DataReadOperations	파일 시스템에 대한 클라이언트의 읽기 작업으로 발생한 읽기 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 발생한 총 I/O 작업 수입니다. 일정 기간 초당 평균 읽기 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum
DataWriteOperations	파일 시스템에 대한 클라이언트의 쓰기 작업으로 발생한 쓰기 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 발생한 총 I/O 작업 수입니다. 일정 기간 초당 평균 쓰기 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum
MetadataOperations	파일 시스템에 대한 클라이언트의 메타데이터 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 발생한 총 I/O 작업 수입니다. 일정 기간 초당 평균 메타데이터 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum

지표	설명
DataReadOperationTime	파일 시스템의 데이터에 액세스하는 클라이언트의 읽기 작업(네트워크 I/O)을 위해 파일 시스템에서 소요된 총 시간의 합계입니다. Sum 통계는 지정된 기간 동안 읽기 작업에 소요된 총 시간(초)입니다. 일정 기간의 평균 읽기 지연 시간을 계산하려면 Sum 통계를 동일한 기간 동안의 DataReadOperations 지표의 Sum으로 나눕니다. 단위: 초 유효한 통계: Sum
DataWriteOperationTime	파일 시스템의 데이터에 액세스하는 클라이언트의 쓰기 작업(네트워크 I/O)을 수행하기 위해 파일 시스템 내에서 소요된 총 시간의 합계입니다. Sum 통계는 지정된 기간 동안 쓰기 작업에 소요된 총 시간(초)입니다. 일정 기간의 평균 쓰기 지연 시간을 계산하려면 Sum 통계를 동일한 기간 동안의 DataWriteOperations 지표의 Sum으로 나눕니다. 단위: 초 유효한 통계: Sum

지표	설명
CapacityPoolReadBytes	파일 시스템의 용량 풀 계층에서 읽은 바이트 수(네트워크 I/O)입니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 파일 시스템의 용량 풀 계층에서 읽은 총 바이트 수입니다. 용량 풀의 초당 바이트 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 바이트 유효한 통계: Sum
CapacityPoolReadOperations	파일 시스템의 용량 풀 계층에서 발생한 읽기 작업 수(네트워크 I/O)입니다. 이는 용량 풀 읽기 요청으로 변환됩니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 파일 시스템의 용량 풀 계층에서 발생한 총 읽기 작업 수입니다. 용량 풀의 초당 요청 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 개 유효한 통계: Sum

지표	설명
CapacityPoolWriteBytes	파일 시스템의 용량 풀 계층에 쓴 바이트 수(네트워크 I/O)입니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 파일 시스템의 용량 풀 계층에 쓴 총 바이트 수입니다. 용량 풀의 초당 바이트 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 바이트 유효한 통계: Sum
CapacityPoolWriteOperations	파일 시스템의 용량 풀 계층에 발생한 쓰기 작업 수(네트워크 I/O)입니다. 이는 쓰기 요청으로 변환됩니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 파일 시스템의 용량 풀 계층에 대한 총 쓰기 작업 수입니다. 용량 풀의 초당 요청 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 개 유효한 통계: Sum

파일 서버 지표

이러한 모든 지표는 하나의 측정기준인 FileSystemId를 가집니다.

지표	설명
CPUUtilization	파일 시스템의 CPU 리소스 사용률입니다. Average 통계는 지정된 기간 동안 파일 시스템의 평균 CPU 사용률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 가장 낮은 CPU 사용률입니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 가장 높은 CPU 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerDiskThroughputUtilization	파일 서버와 기본 계층 간의 디스크 처리량(처리량 용량에 따라 결정된 프로비저닝된 한도의 백분율)입니다. Average 통계는 지정된 기간 동안 서버 디스크 처리량의 평균 사용률입니다. Minimum 통계는 지정된 기간 동안 서버 디스크 처리량의 가장 낮은 사용률입니다. Maximum 통계는 지정된 기간 동안 서버 디스크 처리량의 가장 높은 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerDiskThroughputBalance	파일 서버와 기본 계층 간의 디스크 처리량에 사용할 수 있는 버스트 크레딧의 비율입니다. 이는 처리량 용량이 512MBps 미만인 프로비저닝된 파일 시스템에 유효합니다.

지표	설명
	Average 통계는 지정된 기간 동안 사용할 수 있는 평균 버스트 밸런스입니다. Minimum 통계는 지정된 기간 동안 사용할 수 있는 최소 버스트 밸런스입니다. Maximum 통계는 지정된 기간 동안 사용할 수 있는 최대 버스트 밸런스입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerDiskIopsBalance	파일 서버와 기본 계층 간의 디스크 IOPS에 사용할 수 있는 버스트 크레딧의 비율입니다. 이는 처리량 용량이 512MBps 미만인 프로비저닝된 파일 시스템에 유효합니다. Average 통계는 지정된 기간 동안 사용할 수 있는 평균 버스트 밸런스입니다. Minimum 통계는 지정된 기간 동안 사용할 수 있는 최소 버스트 밸런스입니다. Maximum 통계는 지정된 기간 동안 사용할 수 있는 최대 버스트 밸런스입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum

지표	설명
FileServerDiskIopsUtilization	파일 서버의 사용 가능한 디스크 IOPS 용량의 IOPS 사용률입니다. Average 통계는 지정된 기간 동안 파일 시스템의 평균 디스크 IOPS 사용률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 최소 디스크 IOPS 사용률입니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 최대 디스크 IOPS 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerCacheHitRatio	파일 시스템의 RAM 및 NVMe 캐시에 있는 데이터에서 처리한 모든 읽기 요청의 비율입니다. 비율이 높을수록 파일 시스템의 읽기 캐시에서 더 많은 읽기를 처리한다는 의미입니다. 단위: 백분율 Average 통계는 지정된 기간 동안 파일 시스템의 평균 캐시 적중률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 가장 낮은 캐시 적중률입니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 가장 높은 캐시 적중률입니다. 유효한 통계: Average, Minimum 및 Maximum

디스크 I/O 지표

이러한 모든 지표는 하나의 측정기준인 FileSystemId를 가집니다.

지표	설명
DiskReadBytes	파일 시스템의 기본 계층에 대한 디스크 읽기의 바이트 수(디스크 I/O)입니다. Sum 통계는 파일 시스템에서 지정된 기간 동안 읽은 총 바이트 수입니다. 통계를 위해 읽기 디스크 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
DiskWriteBytes	파일 시스템의 기본 계층에 대한 모든 디스크 쓰기에서 발생한 바이트 수(디스크 I/O)입니다. Sum 통계는 파일 시스템에서 지정된 기간 동안 쓴 총 바이트 수입니다. 통계를 위해 쓰기 디스크 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
DiskIopsUtilization	파일 서버와 스토리지 볼륨 간의 디스크 IOPS(기본 계층의 프로비저닝된 디스크 IOPS 한도의 백분율)입니다. Average 통계는 지정된 기간 동안 파일 시스템의 평균 디스크 IOPS 사용률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 최소 디스크 IOPS 사용률입니다.

지표	설명
	Maximum 통계는 지정된 기간 동안 파일 시스템의 최대 디스크 IOPS 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
DiskReadOperations	파일 시스템의 기본 계층에서 발생한 읽기 작업 수(디스크 I/O)입니다. Sum 통계는 지정된 기간 동안 기본 계층에서 발생한 총 읽기 작업 수입니다. 단위: 개 유효한 통계: Sum
DiskWriteOperations	파일 시스템의 기본 계층에 대한 쓰기 작업 수(디스크 I/O)입니다. Sum 통계는 지정된 기간 동안 기본 계층에 대한 총 쓰기 작업 수입니다. 단위: 개 유효한 통계: Sum

스토리지 용량 지표

이러한 모든 지표는 하나의 측정기준인 FileSystemId를 가집니다.

지표	설명
StorageEfficiencySavings	스토리지 효율성 기능(압축, 중복 제거, 축소)을 통해 절약된 바이트입니다. Average 통계는 지정된 기간 동안의 평균 스토리지 효율성 절감 효과입니다. 스토리지 효율

지표	설명
	성 절감 효과를 1분 동안 저장된 모든 데이터의 백분율로 계산하려면 StorageUsed 에 대한 Sum 통계를 사용하여 StorageEfficiencySavings 를 StorageEfficiencySavings 및 StorageUsed 파일 시스템 지표의 합계로 나눕니다. Minimum 통계는 지정된 기간 동안의 최소 스토리지 효율성 절감 효과입니다. Maximum 통계는 지정된 기간 동안의 최대 스토리지 효율성 절감 효과입니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum
StorageUsed	기본(SSD) 계층과 용량 풀 계층 모두에서 파일 시스템에 저장된 물리적 데이터의 총량입니다. 이 지표에는 데이터 압축 및 중복 제거와 같은 스토리지 효율성 기능을 통한 절감 효과가 포함됩니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum

지표	설명
LogicalDataStored	SSD 계층과 용량 풀 계층을 모두 고려하여 파일 시스템에 저장된 논리적 데이터의 총량입니다. 이 지표에는 스냅샷과 FlexClones의 총 논리적 크기가 포함되지만 압축, 축소 및 중복 제거를 통해 달성한 스토리지 효율성 절감 효과는 포함되지 않습니다. 스토리지 효율성 절감 효과를 바이트 단위로 계산하려면 지정된 기간 동안 StorageUsed 의 Average를 구하고 그 값을 같은 기간 LogicalDataStored 의 Average에서 뺍니다. 스토리지 효율성 절감 효과를 총 논리적 데이터 크기의 백분율로 계산하려면 지정된 기간 동안의 StorageUsed 의 Average를 구하고 거기에서 동일한 기간 동안의 LogicalDataStored 의 Average를 뺍니다. 그런 다음 그 차이를 동일한 기간 동안의 LogicalDataStored 의 Average로 나눕니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum

세부 파일 시스템 지표

세부 파일 시스템 지표는 각 스토리지 계층에 대한 세부 스토리지 사용률 지표입니다. 세부 파일 시스템 지표는 모두 FileSystemId, StorageTier 및 DataType 측정기준을 가지고 있습니다.

- StorageTier 측정기준은 지표가 측정하는 스토리지 계층을 나타내며 가능한 값은 SSD 및 StandardCapacityPool입니다.
- DataType 측정기준은 지표가 측정하는 데이터 유형을 나타내며 가능한 값은 All입니다.

주어진 지표와 측정기준 키-값 페어의 고유한 조합마다 행이 있으며, 해당 조합의 측정 결과에 대한 설명이 있습니다.

지표	설명
StorageCapacityUtilization	각 파일 시스템의 집계에 대한 스토리지 용량 사용률입니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Average 통계는 지정된 기간 동안 파일 시스템의 성능 계층에 대한 평균 스토리지 용량 사용률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 성능 계층에 대한 스토리지 용량 사용률이 가장 낮습니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 성능 계층에 대한 스토리지 용량 사용률이 가장 높습니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
StorageCapacity	기본(SSD) 계층의 총 스토리지 용량입니다. 단위: 바이트 유효한 통계: Maximum
StorageUsed	스토리지 계층별로 사용된 물리적 스토리지 용량(바이트)입니다. 이 값에는 데이터 압축 및 중복 제거와 같은 스토리지 효율성 기능을 통한 절감 효과가 포함됩니다. StorageTier 의 유효한 측정기준 값은 이 지표가 측정하는 스토리지 계층에 해당하는 SSD와 StandardCapacityPool 입니다. 또한 이 지표의 경우 DataType 측정기준의 값은 All이어야 합니다.

지표	설명
	Average, Minimum 및 Maximum 통계는 지정된 기간 동안의 계층별 스토리지 사용량(바이트)입니다. 기본(SSD) 스토리지 계층의 스토리지 용량 사용률을 계산하려면 StorageTier 측정기준이 SSD와 동일한 상태에서 이러한 통계를 같은 기간의 Maximum StorageCapacity 로 나눕니다. 기본(SSD) 스토리지 계층의 무료 스토리지 용량(바이트)을 계산하려면 StorageTier 측정기준이 SSD와 동일한 상태에서 같은 기간의 Maximum StorageCapacity 에서 이러한 통계를 뺍니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum

2세대 파일 시스템 지표

2세대 FSx for ONTAP 파일 시스템에는 다음 지표가 제공됩니다. 지표의 경우 각 HA 페어 및 각 집계(스토리지 사용률 지표의 경우)에 대해 데이터 포인트가 생성됩니다.

> **Note**
>
> HA 페어가 여러 개인 파일 시스템이 있는 경우 단일 HA 페어 파일 시스템 지표와 볼륨 지표를 사용할 수도 있습니다.

주제

- 네트워크 I/O 지표
- 파일 서버 지표
- 디스크 I/O 지표

- 세부 파일 시스템 지표

네트워크 I/O 지표

이들 지표는 모두 FileSystemId와 FileServer라는 두 측정기준을 가집니다.

- FileSystemId - 파일 시스템의 AWS 리소스 ID입니다.
- FileServer – ONTAP(예: FsxId01234567890abcdef-01)의 파일 서버(또는 노드) 이름입니다. 홀수 번호의 파일 서버는 선호하는 파일 서버(즉, 파일 시스템이 보조 파일 서버로 장애 조치되지 않은 한 트래픽을 서비스함)이고, 짝수 번호의 파일 서버는 보조 파일 서버(즉, 파트너를 사용할 수 없는 경우에만 트래픽을 서비스함)입니다. 따라서 보조 파일 서버는 일반적으로 선호하는 파일 서버보다 사용률이 낮습니다.

지표	설명
NetworkThroughputUtilization	네트워크 처리량 사용률은 파일 시스템에 사용 가능한 네트워크 처리량의 백분율입니다. 이 지표는 파일 시스템에 대한 한 HA 쌍의 네트워크 처리량 용량의 백분율로 NetworkSentBytes 및 NetworkReceivedBytes 의 최대값에 해당합니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Average 통계는 지정된 기간 동안 지정된 파일 서버의 평균 네트워크 처리량 사용률입니다. Minimum 통계는 지정된 기간 동안 분당 지정된 파일 서버의 가장 낮은 네트워크 처리량 사용률입니다. Maximum 통계는 지정된 기간 동안 분당 지정된 파일 서버의 가장 높은 네트워크 처리량 사용률입니다. 단위: 백분율

지표	설명
	유효한 통계: Average, Minimum 및 Maximum
NetworkSentBytes	파일 시스템에서 전송한 바이트 수(네트워크 IO)입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 파일 서버에서 네트워크를 통해 전송한 총 바이트 수입니다. Average 통계는 지정된 기간 동안 지정된 파일 서버에서 네트워크를 통해 전송한 평균 바이트 수입니다. Minimum 통계는 지정된 기간 동안 지정된 파일 서버에서 네트워크를 통해 전송한 가장 낮은 바이트 수입니다. Maximum 통계는 지정된 기간 동안 지정된 파일 서버에서 네트워크를 통해 전송한 가장 높은 바이트 수입니다. 통계를 위해 전송된 처리량(바이트/초)을 계산하려면 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum, Average, Minimum 및 Maximum

지표	설명
NetworkReceivedBytes	파일 시스템에서 수신한 바이트 수(네트워크 IO)입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 파일 서버에서 네트워크를 통해 수신한 총 바이트 수입니다. Average 통계는 지정된 기간 동안 지정된 파일 서버가 분당 네트워크를 통해 수신하는 평균 바이트 수입니다. Minimum 통계는 지정된 기간 동안 지정된 파일 서버가 분당 네트워크를 통해 수신하는 가장 낮은 바이트 수입니다. Maximum 통계는 지정된 기간 동안 지정된 파일 서버가 분당 네트워크를 통해 수신하는 가장 높은 바이트 수입니다. 통계의 수신 처리량(초당 바이트 수)을 계산하려면 해당 통계를 해당 기간의 초로 나눕니다. 단위: 바이트 유효한 통계: Sum, Average, Minimum 및 Maximum

파일 서버 지표

이들 지표는 모두 FileSystemId와 FileServer라는 두 측정기준을 가집니다.

지표	설명
CPUUtilization	파일 시스템의 CPU 리소스 사용률입니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Average 통계는 지정된 기간 동안 파일 시스템의 평균 CPU 사용률입니다. Minimum 통계는 지정된 기간 동안 지정된 집계의 CPU 사용률이 가장 낮습니다. Maximum 통계는 지정된 기간 동안 지정된 집계의 CPU 사용률이 가장 높습니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerDiskThroughputUtilization	파일 서버와 집계 간의 디스크 처리량으로, 처리량 용량에 따라 결정되는 프로비저닝된 제한의 백분율입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 이 지표는 파일 시스템의 HA 페어 하나에 대한 파일 서버의 디스크 처리량 용량의 백분율로 DiskReadBytes 및 DiskWriteBytes 의 합계와 동일합니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Average 통계는 지정된 기간 동안 지정된 파일 서버의 평균 파일 서버 디스크 처리량 사용률입니다. Minimum 통계는 지정된 기간 동안 지정된 파일 서버의 가장 낮은 파일 서버 디스크 처리량 사용률입니다.

지표	설명
	Maximum 통계는 지정된 기간 동안 지정된 파일 서버의 가장 높은 파일 서버 디스크 처리량 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
FileServerDiskIopsUtilization	파일 서버의 사용 가능한 디스크 IOPS 용량 중 사용률(디스크 IOPS 제한의 백분율)입니다. 이는 프로비저닝된 디스크 IOPS가 아니라 파일 서버가 처리할 수 있는 최대치를 벗어난 디스크 IOPS의 사용률이라는 점에서 DiskIopsUtilization 와 다릅니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. Average 통계는 지정된 기간 동안 지정된 파일 서버의 평균 디스크 IOPS 사용률입니다. Minimum 파일 서버는 지정된 기간 동안 지정된 집계의 디스크 IOPS 사용률이 가장 낮습니다. Maximum 통계는 지정된 기간 동안 지정된 집계의 디스크 IOPS 사용률이 가장 높습니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum

지표	설명
FileServerCacheHitRatio	각 HA 페어(예: HA 페어의 활성 파일 서버)에 대한 파일 시스템의 RAM 또는 NVMe 캐시에 있는 데이터에서 제공되는 모든 읽기 요청의 백분율입니다. 백분율이 높을수록 캐시된 읽기 대 총 읽기의 비율이 높음을 나타냅니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함한 모든 I/O가 고려됩니다. 각 파일 시스템의 파일 서버에 대해 분당 하나의 지표가 생성됩니다. 단위: 백분율 Average 통계는 지정된 기간 동안 파일 시스템의 HA 페어 중 하나에 대한 평균 캐시 적중률입니다. Minimum 통계는 지정된 기간 동안 파일 시스템의 HA 페어 중 하나에 대한 캐시 적중률이 가장 낮습니다. Maximum 통계는 지정된 기간 동안 파일 시스템의 HA 페어 중 하나에 대한 캐시 적중률이 가장 높습니다. 유효한 통계: Average, Minimum 및 Maximum

디스크 I/O 지표

이들 지표는 모두 FileSystemId와 Aggregate라는 두 측정기준을 가집니다.

- FileSystemId - 파일 시스템의 AWS 리소스 ID입니다.
- Aggregate – 파일 시스템의 성능 계층은 집계 라는 여러 스토리지 풀로 구성됩니다. 각 HA 페어에는 하나의 집계가 있습니다. 예를 들어, 집계 aggr1는 파일 서버 FsxId01234567890abcdef-01(활성 파일 서버)와 파일 서버 FsxId01234567890abcdef-02(보조 파일 서버)에 HA 쌍으로 매핑됩니다.

지표	설명
DiskReadBytes	이 집계에서 읽은 모든 디스크의 바이트 수(디스크 IO)입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 집계에서 분당 읽는 총 바이트 수입니다. Average 통계는 지정된 기간 동안 지정된 집계에서 분당 읽는 평균 바이트 수입니다. Minimum 통계는 지정된 기간 동안 지정된 집계에서 분당 읽는 가장 낮은 바이트 수입니다. Maximum 통계는 지정된 기간 동안 지정된 집계에서 분당 읽는 가장 높은 바이트 수입니다. 통계에 대한 디스크 읽기 처리량(초당 바이트)을 계산하려면 해당 통계를 기간(초)으로 나눕니다. 단위: 바이트 유효한 통계: Sum, Average, Minimum 및 Maximum
DiskWriteBytes	이 집계에 쓰는 디스크의 바이트 수(디스크 IO)입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 집계에 기록된 총 바이트 수입니다. Average 통계는 지정된 기간 동안 분당 지정된 집계에 기록된 평균 바이트 수입니다.

지표	설명
	Minimum 통계는 지정된 기간 동안 분당 지정된 집계에 기록된 가장 낮은 바이트 수입니다. Maximum 통계는 지정된 기간 동안 분당 지정된 집계에 기록된 가장 높은 바이트 수입니다. 통계를 위해 쓰기 디스크 처리량(바이트/초)을 계산하려면 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum, Average, Minimum 및 Maximum

지표	설명
DiskIopsUtilization	집계의 디스크 IOPS 한도(즉, 파일 시스템의 총 IOPS를 파일 시스템의 HA 페어 수로 나눈 값)의 백분율로 나타낸 하나의 집계의 디스크 IOPS 사용률입니다. 이는 파일 서버에서 지원하는 최대 디스크 IOPS(즉, HA 쌍당 구성된 처리량 용량에 따라 결정되는)가 아니라 프로비저닝된 IOPS 한도에 대한 프로비저닝된 디스크 IOPS의 사용률이라는 점에서 FileServerDiskIops Utilization 와 다릅니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Average 통계는 지정된 기간 동안 지정된 집계의 평균 디스크 IOPS 사용률입니다. Minimum 통계는 지정된 기간 동안 지정된 집계의 디스크 IOPS 사용률이 가장 낮습니다. Maximum 통계는 지정된 기간 동안 지정된 집계에 대한 디스크 IOPS 사용률이 가장 높습니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum

지표	설명
DiskReadOperations	이 집계에 대한 읽기 작업(디스크 IO) 수입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 집계에 의해 수행되는 총 읽기 작업 수입니다. Average 통계는 지정된 기간 동안 지정된 집계에 의해 분당 수행되는 평균 읽기 작업 수입니다. Minimum 통계는 지정된 기간 동안 지정된 집계에 의해 분당 수행되는 가장 낮은 읽기 작업 수입니다. Maximum 통계는 지정된 기간 동안 지정된 집계에 의해 분당 수행되는 가장 많은 읽기 작업 수입니다. 기간 동안의 평균 디스크 IOPS를 계산하려면 Average 통계를 사용하고 결과를 60(초)으로 나눕니다. 단위: 개 유효한 통계: Sum, Average, Minimum 및 Maximum

지표	설명
DiskWriteOperations	이 집계에 대한 쓰기 작업(디스크 IO) 수입니다. 백그라운드 작업(예: SnapMirror , 계층화 및 백업)을 포함하여 모든 트래픽이 이 지표에서 고려됩니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Sum 통계는 지정된 기간 동안 지정된 집계에 의해 수행되는 총 쓰기 작업 수입니다. Average 통계는 지정된 기간 동안 지정된 집계에 의해 분당 수행되는 평균 쓰기 작업 수입니다. 기간 동안의 평균 디스크 IOPS를 계산하려면 Average 통계를 사용하고 결과를 60(초)으로 나눕니다. 단위: 개 유효한 통계: Sum 및 Average

세부 파일 시스템 지표

세부 파일 시스템 지표는 각 스토리지 계층에 대한 세부 스토리지 사용률 지표입니다. 자세한 파일 시스템 지표에는 FileSystemId, StorageTier, 및 DataType차원 또는 FileSystemId, StorageTier, DataType 및 Aggregate 차원이 있습니다.

- Aggregate 차원이 제공되지 않으면 지표는 전체 파일 시스템에 대한 것입니다. StorageUsed 및 StorageCapacity 지표에는 파일 시스템의 총 소비 스토리지(스토리지 계층당) 및 총 스토리지 용량(SSD 계층의 경우)에 해당하는 분당 단일 데이터 포인트가 있습니다. 한편 StorageCapacityUtilization 지표는 각 집계에 대해 분당 하나의 지표를 내보냅니다.
- Aggregate 차원이 제공되면 지표는 각 집계에 대한 것입니다.

차원의 의미는 다음과 같습니다.

- FileSystemId - 파일 시스템의 AWS 리소스 ID입니다.

- Aggregate – 파일 시스템의 성능 계층은 집계 라는 여러 스토리지 풀로 구성됩니다. 각 HA 페어에는 하나의 집계가 있습니다. 예를 들어, 집계 aggr1는 파일 서버 FsxId01234567890abcdef-01(활성 파일 서버)와 파일 서버 FsxId01234567890abcdef-02(보조 파일 서버)에 HA 쌍으로 매핑됩니다.
- StorageTier - 지표가 측정하는 스토리지 계층을 나타내며, 가능한 값은 SSD와 StandardCapacityPool입니다.
- DataType - 지표가 측정하는 데이터의 유형을 나타내며, 가능한 값은 All입니다.

주어진 지표와 측정기준 키-값 페어의 고유한 조합마다 행이 있으며, 해당 조합의 측정 결과에 대한 설명이 있습니다.

지표	설명
StorageCapacityUtilization	지정된 파일 시스템 집계의 스토리지 용량 사용률입니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Average 통계는 지정된 기간 동안 지정된 집계의 평균 스토리지 용량 사용률입니다. Minimum 통계는 지정된 기간 동안 지정된 집계의 최소 스토리지 용량 사용률입니다. Maximum 통계는 지정된 기간 동안 지정된 집계의 최대 스토리지 용량 사용률입니다. 단위: 백분율 유효한 통계: Average, Minimum 및 Maximum
StorageCapacity	지정된 파일 시스템 집계의 스토리지 용량입니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Average 통계는 지정된 기간 동안 지정된 집계의 평균 스토리지 용량입니다.

지표	설명
	Minimum 통계는 지정된 기간 동안 지정된 집계의 최소 스토리지 용량입니다. Maximum 통계는 지정된 기간 동안 지정된 집계의 최대 스토리지 용량입니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum
StorageUsed	스토리지 계층별로 사용된 물리적 스토리지 용량(바이트)입니다. 이 값에는 데이터 압축 및 중복 제거와 같은 스토리지 효율성 기능을 통한 절감 효과가 포함됩니다. StorageTier 의 유효한 측정기준 값은 이 지표가 측정하는 스토리지 계층에 해당하는 SSD와 StandardCapacityPool 입니다. 파일 시스템의 각 집계에 대해 매분 하나의 메트릭이 생성됩니다. Average 통계는 지정된 스토리지 계층에서 지정된 기간 동안 지정된 집계에 의해 소비되는 물리적 스토리지 용량의 평균량입니다. Minimum 통계는 지정된 기간 동안 지정된 집계가 지정된 스토리지 계층에서 소비하는 물리적 스토리지 용량의 최소량입니다. Maximum 통계는 지정된 기간 동안 지정된 스토리지 계층에서 지정된 집계에 의해 소비되는 물리적 스토리지 용량의 최대량입니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum

볼륨 지표

Amazon FSx for NetApp ONTAP 파일 시스템에는 데이터를 저장하는 볼륨이 하나 이상 있을 수 있습니다. 이러한 각 볼륨에는 볼륨 지표 또는 세부 볼륨 지표로 분류된 CloudWatch 지표 세트가 있습니다.

- 볼륨 지표는 `FileSystemId`와 `VolumeId` 두 측정기준을 가지는 볼륨별 성능 및 스토리지 지표입니다. `FileSystemId`는 볼륨이 속한 파일 시스템에 매핑됩니다.
- 세부 볼륨 지표는 `StorageTier` 측정기준을 가지는(`SSD`와 `StandardCapacityPool` 값 가능) 계층별 스토리지 사용량과 `DataType` 측정기준을 가지는(`User`, `Snapshot`, `Other` 값 가능) 데이터 유형별 스토리지 사용량을 측정한 스토리지 계층별 지표입니다. 이러한 지표는 `FileSystemId`, `VolumeId`, `StorageTier` 및 `DataType` 측정기준을 가집니다.

주제

네트워크 I/O 지표

이들 지표는 모두 `FileSystemId`와 `VolumeId`라는 두 측정기준을 가집니다.

지표	설명
`DataReadBytes`	클라이언트가 볼륨에서 읽은 바이트 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안 읽기 작업과 연결된 총 바이트 수입니다. 일정 기간 평균 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
`DataWriteBytes`	클라이언트가 볼륨에 쓴 바이트 수(네트워크 I/O)입니다.

지표	설명
	Sum 통계는 지정된 기간 동안 쓰기 작업과 연결된 총 바이트 수입니다. 일정 기간 평균 처리량(바이트/초)을 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 바이트 유효한 통계: Sum
DataReadOperations	볼륨에 대한 클라이언트의 읽기 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안의 총 읽기 작업 수입니다. 일정 기간 초당 평균 읽기 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum
DataWriteOperations	볼륨에 대한 클라이언트의 쓰기 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안의 총 쓰기 작업 수입니다. 일정 기간 초당 평균 쓰기 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum

지표	설명
MetadataOperations	클라이언트가 볼륨에 수행한 메타데이터 작업의 I/O 작업 수(네트워크 I/O)입니다. Sum 통계는 지정된 기간 동안의 총 메타데이터 작업 수입니다. 일정 기간 초당 평균 메타데이터 작업 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나누면 됩니다. 단위: 개 유효한 통계: Sum
DataReadOperationTime	볼륨 내에서 해당 볼륨의 데이터에 액세스하는 클라이언트의 읽기 작업(네트워크 I/O)에 소요된 총 시간의 합계입니다. Sum 통계는 지정된 기간 동안 읽기 작업에 소요된 총 시간(초)입니다. 일정 기간의 평균 읽기 지연 시간을 계산하려면 Sum 통계를 동일한 기간 동안의 DataReadOperations 지표의 Sum으로 나눕니다. 단위: 초 유효한 통계: Sum

지표	설명
DataWriteOperationTime	볼륨 내에서 해당 볼륨의 데이터에 액세스하는 클라이언트의 쓰기 작업(네트워크 I/O)에 소요된 총 시간의 합계입니다. Sum 통계는 지정된 기간 동안 쓰기 작업에 소요된 총 시간(초)입니다. 일정 기간의 평균 쓰기 지연 시간을 계산하려면 Sum 통계를 동일한 기간 동안의 DataWriteOperations 지표의 Sum으로 나눕니다. 단위: 초 유효한 통계: Sum
MetadataOperationTime	볼륨 내에서 해당 볼륨의 데이터에 액세스하는 클라이언트의 메타데이터 작업(네트워크 I/O)에 소요된 총 시간의 합계입니다. Sum 통계는 지정된 기간 동안 읽기 작업에 소요된 총 시간(초)입니다. 일정 기간의 평균 지연 시간을 계산하려면 Sum 통계를 동일한 기간 동안의 MetadataOperations 의 Sum으로 나눕니다. 단위: 초 유효한 통계: Sum

지표	설명
CapacityPoolReadBytes	볼륨의 용량 풀 계층에서 읽은 바이트 수(네트워크 I/O)입니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 볼륨의 용량 풀 계층에서 읽은 총 바이트 수입니다. 용량 풀의 초당 바이트 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 바이트 유효한 통계: Sum
CapacityPoolReadOperations	볼륨 용량 풀 계층의 읽기 작업 수(네트워크 I/O)입니다. 이는 용량 풀 읽기 요청으로 변환됩니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 볼륨의 용량 풀 계층에서 발생한 총 읽기 작업 수입니다. 용량 풀의 초당 요청 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 개 유효한 통계: Sum

지표	설명
CapacityPoolWriteBytes	볼륨의 용량 풀 계층에 쓴 바이트 수(네트워크 I/O)입니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 볼륨의 용량 풀 계층에 쓴 총 바이트 수입니다. 용량 풀의 초당 바이트 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 바이트 유효한 통계: Sum
CapacityPoolWriteOperations	볼륨의 용량 풀 계층에 발생한 쓰기 작업 수(네트워크 I/O)입니다. 이는 쓰기 요청으로 변환됩니다. 데이터 무결성을 보장하기 위해 ONTAP은 쓰기 작업을 수행한 후 즉시 용량 풀에서 읽기 작업을 수행합니다. Sum 통계는 지정된 기간 동안 볼륨의 용량 풀 계층에 대한 총 쓰기 작업 수입니다. 용량 풀의 초당 요청 수를 계산하려면 Sum 통계를 초 단위의 해당 기간으로 나눕니다. 단위: 개 유효한 통계: Sum

스토리지 용량 지표

이들 지표는 모두 FileSystemId와 VolumeId라는 두 측정기준을 가집니다.

지표	설명
StorageCapacity	바이트 단위의 볼륨 크기. 단위: 바이트 유효한 통계: Maximum
StorageUsed	볼륨의 사용된 논리적 스토리지 용량. 단위: 바이트 유효한 통계: Average
StorageCapacityUtilization	볼륨의 스토리지 용량 사용률입니다. 단위: 백분율 유효한 통계: Average
FilesUsed	볼륨에서 사용된 파일(파일 또는 아이노드 수). 단위: 개 유효한 통계: Average
FilesCapacity	볼륨에 생성할 수 있는 총 아이노드 수. 단위: 개 유효한 통계: Maximum

세부 볼륨 지표

세부 볼륨 지표는 볼륨 지표보다 더 많은 측정기준을 가지고 있으므로 데이터를 더 세밀하게 측정할 수 있습니다. 모든 세부 볼륨 지표는 FileSystemId, VolumeId, StorageTier 및 DataType 측정기준을 가집니다.

- StorageTier 측정기준은 지표가 측정하는 스토리지 계층을 나타내며 가능한 값은 All, SSD 및 StandardCapacityPool입니다.

- DataType 측정기준은 지표가 측정하는 데이터 유형을 나타내며 가능한 값은 All, User, Snapshot 및 Other입니다.

다음 표는 StorageUsed 지표가 나열된 측정기준에 대해 측정하는 내용을 정의합니다.

지표	설명
StorageUsed	사용된 논리적 공간의 양(바이트) 이 지표는 이 지표에 사용된 측정기준에 따라 다양한 유형의 공간 사용을 측정합니다. StorageTier 를 SSD 또는 StandardCapacityPool 로 설정하고 DataType을 All로 설정하는 경우 이 지표는 SSD 및 용량 풀 계층에서 각각 이 볼륨의 논리적 공간 사용량을 측정합니다. DataType 측정기준을 User, Snapshot 또는 Other로 설정하고 StorageTier 를 All로 설정하는 경우 이 지표는 각 데이터 유형에 대한 논리적 공간 사용량을 측정합니다. Snapshot 데이터 사용에는 기본적으로 볼륨 크기의 5%인 스냅샷 예약이 포함됩니다. 단위: 바이트 유효한 통계: Average, Minimum 및 Maximum
StorageCapacityUtilization	볼륨에서 사용된 물리적 디스크 공간의 비율입니다. 단위: 백분율 유효한 통계: Maximum

FSx for ONTAP EMS 이벤트 모니터링

NetApp ONTAP의 네이티브 이벤트 관리 시스템(EMS)을 사용하여 FSx for ONTAP 파일 시스템 이벤트를 모니터링할 수 있습니다. NetApp ONTAP CLI를 사용하여 이러한 이벤트를 볼 수 있습니다.

주제

EMS 이벤트 개요

EMS 이벤트는 미리 정의된 조건이 FSx for ONTAP 파일 시스템에서 발생하면 자동으로 생성되는 알림입니다. 이러한 알림은 스토리지 가상 머신(SVM) 인증 문제 또는 전체 볼륨과 같은 더 큰 문제로 이어질 수 있는 문제를 예방하거나 수정할 수 있도록 지속적으로 정보를 제공합니다.

기본적으로 이벤트는 이벤트 관리 시스템 로그에 기록됩니다. EMS를 사용하면 사용자 암호 변경, FlexGroup 내 구성 요소가 최대 용량에 가까워진 경우, Logical Unit Number(LUN)를 수동으로 온라인 또는 오프라인으로 전환한 경우 또는 볼륨의 자동 크기 조정과 같은 이벤트를 모니터링할 수 있습니다.

ONTAP EMS 이벤트에 대한 자세한 내용은 NetApp ONTAP 설명서 센터의 ONTAP EMS 참조를 참조하세요. 이벤트 범주를 표시하려면 문서의 왼쪽 탐색 창을 사용합니다.

> **Note**
>
> FSx for ONTAP 파일 시스템에는 일부 ONTAP EMS 메시지만 사용할 수 있습니다. 사용 가능한 ONTAP EMS 메시지 목록을 보려면 NetApp ONTAP CLI 이벤트 카탈로그 표시 명령을 사용합니다.

EMS 이벤트 설명에는 이벤트 이름, 심각도, 가능한 원인, 로그 메시지, 대응 방법을 결정하는 데 도움이 되는 해결 조치가 포함됩니다. 예를 들어, wafl.vol.autoSize.fail 이벤트는 볼륨의 자동 크기 조정이 실패할 때 발생합니다. 이벤트 설명에 따르면 수정 조치는 자동 크기 조정을 설정하는 동안 볼륨의 최대 크기를 늘리는 것입니다.

EMS 이벤트 보기

이벤트 로그의 내용을 표시하려면 NetApp ONTAP CLI 이벤트 로그 show 명령을 사용합니다. 이 명령은 파일 시스템에 `fsxadmin` 역할이 있는 경우 사용할 수 있습니다. 명령 구문은 다음과 같습니다.

```
event log show [event_options]
```

가장 최근 이벤트가 먼저 나열됩니다. 기본적으로 이 명령은 다음 정보가 포함된 EMERGENCY, ALERT, 및 ERROR 심각도 수준 이벤트를 표시합니다.

- 시간 - 이벤트 시간입니다.
- 노드 - 이벤트가 발생한 노드입니다.
- 심각도 - 이벤트의 심각도 수준입니다. NOTICE, INFORMATIONAL 또는 DEBUG 심각도 수준 이벤트를 표시하려면 -severity 옵션을 사용합니다.
- 이벤트 - 이벤트 이름 및 메시지입니다.

이벤트에 대한 자세한 정보를 표시하려면 다음 표에 나열된 이벤트 옵션 중 하나 이상을 사용합니다.

이벤트 옵션	설명
-detail	추가 이벤트 정보를 표시합니다.
-detailtime	역순으로 자세한 이벤트 정보를 표시합니다.
-instance	모든 필드에 대한 세부 정보를 표시합니다.
-node *nodename*|local	지정한 노드의 이벤트 목록을 표시합니다. 이 옵션을 -seqnum과 함께 사용하면 자세한 정보를 표시할 수 있습니다.
-seqnum *sequence_number*	시퀀스에서 이 번호와 일치하는 이벤트를 선택합니다. -node와 함께 사용하면 자세한 정보를 표시할 수 있습니다.
-time *MM/DD/YYYY HH:MM:SS*	이 특정 시간에 발생한 이벤트를 선택합니다. MM/DD/YYYY HH:MM:SS [+- HH:MM] 형식을 사용합니다. 두 시간 문 사이에

이벤트 옵션	설명

	`..` 연산자를 사용하여 시간 범위를 지정할 수 있습니다.
	`event log show -time "04/17/2023 05:55:00".."04/17/2023 06:10:00"`
	비교 시간 값은 명령을 실행할 때의 현재 시간을 기준으로 합니다. 다음 예제에서는 최근 1분 내에 발생한 이벤트만 표시하는 방법을 보여줍니다.
	`event log show -time >1m`
	이 옵션의 월 및 날짜 필드는 0으로 채워지지 않습니다. 이러한 필드는 한 자리 숫자일 수 있습니다(예:`4/1/2023 06:45:00`).

이벤트 옵션	설명
`-severity` *sev_level*	*sev_level* 값과 일치하는 이벤트를 선택합니다. 이 값은 다음 중 하나여야 합니다. • EMERGENCY - 중단 • ALERT - 단일 장애 지점 • ERROR - 성능 저하 • NOTICE - 정보 • INFORMATIONAL - 정보 • DEBUG - 디버그 정보 모든 이벤트를 표시하려면 다음과 같이 심각도를 지정합니다. `event log show -severity <=DEBUG`

이벤트 옵션	설명
-ems-severity *ems_sev_level*	*ems_sev_level* 값과 일치하는 이벤트를 선택합니다. 이 값은 다음 중 하나여야 합니다. • NODE_FAULT - 데이터 손상이 감지되었거나 노드가 클라이언트 서비스를 제공할 수 없습니다. • SVC_FAULT - 일시적인 서비스 손실(일반적으로 일시적인 소프트웨어 장애)이 감지됩니다. • NODE_ERROR - 즉시 치명적이지 않은 하드웨어 오류가 감지됩니다. • SVC_ERROR - 즉시 치명적이지 않은 소프트웨어 오류가 감지됩니다. • WARNING - 장애를 나타내지 않는 높은 우선 순위의 메시지입니다. • NOTICE - 장애를 나타내지 않는 보통 우선 순위의 메시지입니다. • INFO - 장애를 나타내지 않는 낮은 우선 순위의 메시지입니다. • DEBUG - 디버깅 메시지입니다. • VAR - 런타임에 선택되는 다양한 심각도를 가진 메시지입니다.

이벤트 옵션	설명
	모든 이벤트를 표시하려면 다음과 같이 심각도를 지정합니다. `event log show -ems-severity <=DEBUG`
`-source` *text*	*text* 값과 일치하는 이벤트를 선택합니다. 소스는 일반적으로 소프트웨어 모듈입니다.
`-message-name` *message_name*	*message_name* 값과 일치하는 이벤트를 선택합니다. 메시지 이름은 설명적이므로 메시지 이름별로 출력을 필터링하면 특정 유형의 메시지가 표시됩니다.
`-event` *text*	*text* 값과 일치하는 이벤트를 선택합니다. event 필드에는 파라미터를 비롯한 이벤트의 전체 텍스트가 포함됩니다.
`-kernel-generation-num` *integer*	*integer* 값과 일치하는 이벤트를 선택합니다. 커널에서 오는 이벤트에만 커널 생성 번호가 있습니다.
`-kernel-sequence-num` *integer*	*integer* 값과 일치하는 이벤트를 선택합니다. 커널에서 오는 이벤트에만 커널 시퀀스 번호가 있습니다.

이벤트 옵션	설명
`-action` *text*	*text* 값과 일치하는 이벤트를 선택합니다. action 필드는 상황을 해결하기 위해 취해야 하는 수정 조치(있는 경우)를 설명합니다.
`-description` *text*	*text* 값과 일치하는 이벤트를 선택합니다. description 필드는 이벤트가 발생한 이유와 그 의미를 설명합니다.
`-filter-name` *filter_name*	*filter_name* 값과 일치하는 이벤트를 선택합니다. 기존 필터에 의해 포함된 이벤트 중 이 값과 일치하는 이벤트만 표시됩니다.
`-fields` *fieldname* `,...`	지정된 필드도 명령 출력에 포함됨을 나타냅니다. `-fields ?`를 사용하여 지정하려는 필드를 선택할 수 있습니다.

EMS 이벤트 보기

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. `event log show` 명령을 사용하여 이벤트 로그의 내용을 표시합니다.

```
::> event log show
Time                 Node          Severity      Event
-------------------- ------------- ------------- -------------------------
```

```
6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
 received on node node1, port e0a.
6/30/2023 13:54:19  node1         NOTICE        vifmgr.portup: A link up event was
 received on node node1, port e0d.
```

`event log show` 명령에 의해 반환되는 EMS 이벤트에 대한 자세한 내용은 NetApp ONTAP 설명서 센터의 ONTAP EMS 참조를 참조하세요.

Syslog 서버로 EMS 이벤트 전달

알림을 Syslog 서버에 전달하도록 EMS 이벤트를 구성할 수 있습니다. EMS 이벤트 전달은 파일 시스템을 실시간으로 모니터링하여 다양한 문제의 근본 원인을 파악하고 격리하는 데 사용됩니다. 환경에 이벤트 알림을 위한 Syslog 서버가 아직 포함되어 있지 않은 경우 먼저 서버를 생성해야 합니다. Syslog 서버 이름을 확인하려면 파일 시스템에 DNS를 구성해야 합니다.

> **Note**
>
> Syslog 대상은 파일 시스템에서 사용하는 기본 서브넷에 있어야 합니다.

알림을 Syslog 서버로 전달하도록 EMS 이벤트를 구성하려면

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 이벤트 알림 대상 생성 명령을 사용하여 다음 속성을 지정하여 `syslog` 유형의 이벤트 알림 대상을 생성합니다.

   - *`dest_name`* - 생성할 알림 대상의 이름입니다(예: `syslog-ems`). 이벤트 알림 대상 이름은 2~64자여야 합니다. 유효한 문자는 A-Z, a-z, 0-9, '_' 및 '-'와 같은 ASCII 문자입니다. 이름은 A-Z, a-z 또는 0-9로 시작하고 끝나야 합니다.
   - *`syslog_name`* - Syslog 메시지가 전송되는 Syslog 서버 호스트 이름 또는 IP 주소입니다.
   - *`transport_protocol`* – 이벤트를 보내는 데 사용되는 프로토콜.
     - `udp-unencrypted` - 보안이 없는 사용자 Datagram 프로토콜입니다. 이것이 기본 프로토콜입니다.
     - `tcp-unencrypted` - 보안이 없는 전송 제어 프로토콜.

- `tcp-encrypted` – 전송 계층 보안(TLS)을 사용하는 전송 제어 프로토콜. 이 옵션을 지정하면 FSx for ONTAP는 인증서를 검증하여 대상 호스트의 ID를 확인합니다.

- *`port_number`* - Syslog 메시지가 전송되는 Syslog 서버 포트입니다. 기본값 `syslog-port` 파라미터는 `syslog-transport` 파라미터 설정에 따라 달라집니다. `syslog-transport`가 `tcp-encrypted`로 설정된 경우 `syslog-port` 기본값은 `6514`입니다. `syslog-transport`가 `tcp-unencrypted`로 설정된 경우 `syslog-port`는 기본값 `601`를 갖습니다. 그렇지 않으면 기본 포트가 `514`로 설정됩니다.

```
::> event notification destination create -name dest_name -syslog syslog_name -
syslog-transport transport_protocol -syslog-port port_number
```

3. 이벤트 알림 생성 명령을 사용하여 이벤트 필터에 의해 정의된 이벤트 세트에 대해 다음 속성을 지정하여 이전 단계에서 생성된 알림 대상으로 새 알림을 생성합니다.

   - *`node_name`* - 이벤트 필터의 이름입니다. 이벤트 필터에 포함된 이벤트는 `-destinations` 파라미터에 지정된 대상으로 전달됩니다.
   - *`dest_name`* - 이벤트 알림이 전송되는 기존 알림 대상의 이름입니다.

```
::> event notification create -filter-name filter_name -destinations dest_name
```

4. TCP를 *`transport_protocol`*로 선택한 경우 `event notification destination check` 명령을 사용하여 테스트 메시지를 생성하고 설정이 작동하는지 확인할 수 있습니다. 명령으로 다음 속성을 지정합니다.

   - *`node_name`* - 노드의 이름(예: `FsxId07353f551e6b557b4-01`)입니다.
   - *`dest_name`* - 이벤트 알림이 전송되는 기존 알림 대상의 이름입니다.

```
::> set diag
::*> event notification destination check -node node_name -destination-
name dest_name
```

데이터 인프라 인사이트를 사용한 모니터링

NetApp Data Infrastructure Insights(이전 Cloud Insights)는 다른 NetApp 스토리지 솔루션과 함께 Amazon FSx for NetApp ONTAP 파일 시스템을 모니터링하는 데 사용할 수 있는 NetApp 서비스입니

다. Data Infrastructure Insights를 사용하면 시간 경과에 따른 구성, 용량 및 성능 지표를 모니터링하여 워크로드의 추세를 이해하고 향후 성능 및 스토리지 용량 요구 사항을 계획할 수 있습니다. 또한 기존 워크플로 및 생산성 도구와 통합할 수 있는 지표 조건을 기반으로 알림을 생성할 수 있습니다.

> **Note**
>
> 데이터 인프라 인사이트는 HA 페어가 두 개 이상인 2세대 파일 시스템에서는 지원되지 않습니다.

Data Infrastructure Insights는 다음을 제공합니다.

- 광범위한 지표 및 로그 – 구성, 용량 및 성능 지표를 수집합니다. 사전 정의된 대시보드, 알림 및 보고서를 통해 워크로드의 동향을 파악할 수 있습니다.
- 사용자 분석 및 랜섬웨어 보호 – Cloud Secure 및 ONTAP 스냅샷을 사용하면 사용자 오류 및 랜섬웨어 사고를 감사, 탐지, 중지 및 복구할 수 있습니다.
- SnapMirror 보고 – SnapMirror 관계를 이해하고 복제 문제에 대한 알림을 설정할 수 있습니다.
- 용량 계획 – 온프레미스 워크로드의 리소스 요구 사항을 이해하면 워크로드를 보다 효율적인 FSx for ONTAP 구성으로 마이그레이션하는 데 도움이 됩니다. 또한 이러한 인사이트를 사용하여 FSx for ONTAP 배포에 더 많은 성능 또는 용량이 필요한 시기를 계획할 수 있습니다.

자세한 내용은 NetApp ONTAP 제품 설명서의 Data Infrastructure Insights 설명서를 참조하세요.

Harvest 및 Grafana를 사용하여 FSx for ONTAP 파일 시스템 모니터링

NetApp Harvest는 ONTAP 시스템에서 성능 및 용량 지표를 수집하기 위한 오픈 소스 도구이며 FSx for ONTAP와 호환됩니다. 오픈 소스 모니터링 솔루션에 Harvest를 Grafana와 함께 사용할 수 있습니다.

Harvest 및 Grafana 시작하기

다음 섹션에서는 FSx for ONTAP 파일 시스템의 성능과 스토리지 용량 사용률을 측정하도록 Harvest 및 Grafana를 설정하고 구성하는 방법을 자세히 설명합니다.

Harvest 및를 사용하여 Amazon FSx for NetApp ONTAP 파일 시스템을 모니터링할 수 있습니다 Grafana.는 FSx for ONTAP 파일 시스템에서 성능, 용량 및 하드웨어 지표를 수집하여 ONTAP 데이터

센터를 NetApp Harvest 모니터링합니다. Grafana는 수집된 Harvest 지표를 표시할 수 있는 대시보드를 제공합니다.

지원되는 Harvest 대시보드

Amazon FSx for NetApp ONTAP은 온프레미스와 다른 지표 세트를 노출합니다NetApp ONTAP. 따라서 로 태그가 지정된 다음과 같은 out-of-the-box Harvest 대시보드만 `fsx` 현재 FSx for ONTAP에서 사용할 수 있습니다. 이러한 대시보드의 일부 패널에는 지원되지 않는 정보가 누락될 수 있습니다.

- 수확: 메타데이터
- ONTAP: cDOT
- ONTAP: 클러스터
- ONTAP: 규정 준수
- ONTAP: 데이터 센터
- ONTAP: 데이터 보호 스냅샷
- ONTAP: LUN
- ONTAP: 노드
- ONTAP: Qtree
- ONTAP: 보안
- ONTAP: SnapMirror
- ONTAP: SVM
- ONTAP: 볼륨

다음 Harvest 대시보드는 FSx for ONTAP에서 지원되지만 에서는 기본적으로 활성화되지 않습니다 Harvest.

- ONTAP: FlexCache
- ONTAP: FlexGroup
- ONTAP: NFS 클라이언트
- ONTAP: NFSv4 Storepool Monitors
- ONTAP: NFS 문제 해결
- ONTAP: SMB
- ONTAP: 워크로드

지원되지 않는 Harvest 대시보드

다음 Harvest 대시보드는 FSx for ONTAP에서 지원되지 않습니다.

- ONTAP: 집계
- ONTAP: 디스크
- ONTAP: 외부 서비스 작업
- ONTAP: File Systems Analytics(FSA)
- ONTAP: 상태
- ONTAP: MetroCluster
- ONTAP: 전원
- ONTAP: 선반
- ONTAP: S3 객체 스토어

AWS CloudFormation 템플릿

시작하려면 Harvest 및 Grafana를 실행하는 Amazon EC2 인스턴스를 자동으로 시작하는 AWS CloudFormation 템플릿을 배포할 수 있습니다. AWS CloudFormation 템플릿에 대한 입력으로이 배포의 일부로 추가될 파일 시스템의 `fsxadmin` 사용자 및 Amazon FSx 관리 엔드포인트를 지정합니다. 배포가 완료되면 Grafana 대시보드에 로그인하여 파일 시스템을 모니터링할 수 있습니다.

이 솔루션은 AWS CloudFormation 를 사용하여 Harvest 및 Grafana 솔루션의 배포를 자동화합니다. 이 템플릿은 Amazon EC2 Linux 인스턴스를 생성하고 Harvest 및 Grafana 소프트웨어를 설치합니다. 이 솔루션을 사용하려면 fsx-ontap-harvest-grafana.template AWS CloudFormation 템플릿을 다운로드합니다.

> **Note**
>
> 이 솔루션을 구현하면 연결된 AWS 서비스에 대한 요금이 청구됩니다. 자세한 내용은 해당 서비스에 대한 요금 세부 정보 페이지를 참조하세요.

Amazon EC2 인스턴스 유형

템플릿을 구성할 때 Amazon EC2 인스턴스 유형을 제공합니다. NetApp의 인스턴스 크기 권장 사항은 모니터링하는 파일 시스템의 수와, 수집하기로 선택한 지표의 수에 따라 달라집니다. 기본 구성을 사용하면 모니터링하는 파일 시스템 10개 각각에 대해 NetApp은 다음을 권장합니다.

- CPU: 코어 2개
- 메모리: 1GB
- 디스크: 500MB(주로 로그 파일에 사용됨)

다음은 몇 가지 샘플 구성과, 선택할 수 있는 `t3` 인스턴스 유형입니다.

파일 시스템	CPU	디스크	인스턴스 유형
10개 미만	코어 2개	500MB	`t3.micro`
10~40	코어 4개	1000MB	`t3.xlarge`
40+	코어 8개	2000MB	`t3.2xlarge`

Amazon EC2 인스턴스 유형에 대한 자세한 내용은 Amazon EC2 사용 설명서의 범용 인스턴스를 참조하세요.

인스턴스 포트 규칙

Amazon EC2 인스턴스를 설정할 때 Amazon EC2 Harvest 및 Grafana 인스턴스가 속해 있는 보안 그룹의 인바운드 트래픽을 위해 포트 3000과 9090이 열려 있도록 해야 합니다. 시작된 인스턴스는 HTTPS를 통해 엔드포인트에 연결되므로 DNS를 위해 포트 53 TCP/UDP가 필요한 엔드포인트를 해결해야 합니다. 또한 엔드포인트에 도달하려면 HTTPS 및 인터넷 액세스를 위한 포트 443 TCP가 필요합니다.

배포 절차

다음은 Harvest 및 Grafana 솔루션을 구성하고 배포하는 절차입니다. 배포에는 약 5분이 소요됩니다. 시작하기 전에 AWS 계정의 Amazon Virtual Private Cloud(Amazon VPC)에서 실행되는 FSx for ONTAP 파일 시스템과 아래에 나열된 템플릿의 파라미터 정보가 있어야 합니다. 파일 시스템 생성에 대한 자세한 내용은 파일 시스템 만들기 섹션을 참조하세요.

Harvest 및 Grafana 솔루션 스택 시작

1. fsx-ontap-harvest-grafana.template AWS CloudFormation 템플릿을 다운로드합니다. AWS CloudFormation 스택 생성에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 콘솔에서 스택 생성을 참조하세요.

   > **Note**
   >
   > 기본적으로이 템플릿은 미국 동부(버지니아 북부) AWS 리전에서 시작됩니다. Amazon FSx를 사용할 수 AWS 리전 있는에서이 솔루션을 시작해야 합니다. 자세한 내용은 AWS 일반 참조의 Amazon FSx 엔드포인트 및 할당량을 참조하세요.

2. 파라미터의 경우 템플릿의 파라미터를 검토하고 파일 시스템의 필요에 맞게 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

파라미터	Default	설명
InstanceType	`t3.micro`	Amazon EC2 인스턴스 유형 `t3` 인스턴스 유형은 다음과 같습니다. • `t3.micro` • `t3.small` • `t3.medium` • `t3.large` • `t3.xlarge` • `t3.2xlarge` 이 파라미터에 허용된 Amazon EC2 인스턴스 유형 값의 전체 목록은 fsx-ontap-harvest-grafana.template을 참조하세요.

파라미터	Default	설명
KeyPair	기본값 없음	Amazon EC2 인스턴스에 액세스하는 데 사용되는 키 페어입니다.
SecurityGroup	기본값 없음	Harvest 및 Grafana 인스턴스의 보안 그룹 ID입니다. 인바운드 포트 3000 및 9090과 포트 53 및 443이 Grafana 대시보드에 액세스하는 데 사용하려는 클라이언트에서 열려 있는지 확인합니다.
서브넷 유형	기본값 없음	서브넷 유형으로 `public` 또는 `private`을 지정합니다. 인터넷에 연결되어야 하는 리소스에는 `public` 서브넷을 사용하고, 인터넷에 연결되지 않는 리소스에는 프라이빗 서브넷을 사용합니다. 자세한 내용은 Amazon VPC 사용 설명서의 서브넷 크기를 참조하세요.
서브넷	기본값 없음	Amazon FSx for NetApp ONTAP 파일 시스템의 기본 서브넷과 동일한 서브넷을 지정합니다. Amazon FSx 콘솔의 FSx for ONTAP 파일 시스템 세부 정보 페이지의 네트워크 및 보안 탭에서 파일 시스템의 기본 서브넷 ID를 찾을 수 있습니다.

파라미터	Default	설명
LatestLinuxAmiId	`/aws/service/ami-amazon-linux-latest/amzn2-ami-hvm-x86_64-gp2`	주어진 AWS 리전에서 Amazon Linux 2 AMI의 최신 버전입니다.
FSxEndPoint	기본값 없음	파일 시스템의 관리 엔드포인트 IP 주소입니다. Amazon FSx 콘솔의 FSx for ONTAP 파일 시스템 세부 정보 페이지의 관리 탭에서 파일 시스템의 관리 엔드포인트 IP 주소를 찾을 수 있습니다.
SecretName	기본값 없음	AWS Secrets Manager 파일 시스템 `fsxadmin` 사용자의 암호가 포함된 보안 암호 이름입니다. 파일 시스템을 생성할 때 제공한 암호입니다.

3. 다음을 선택합니다.
4. 옵션에서 다음을 선택합니다.
5. 검토에서 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스를 생성한다는 것을 확인하는 확인란을 선택해야 합니다.
6. 생성을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 5분 후에 CREATE_COMPLETE 상태를 확인할 수 있습니다.

Grafana에 로그인

배포가 완료되면 브라우저를 사용하여 Amazon EC2 인스턴스의 IP 및 포트 3000에서 Grafana 대시보드에 로그인합니다.

```
http://EC2_instance_IP:3000
```

메시지가 표시되면 Grafana 기본 사용자 이름(admin)과 암호(pass)를 사용합니다. 로그인하는 즉시 암호를 변경하는 것이 좋습니다.

자세한 내용은 GitHub의 NetApp Harvest 페이지를 참조하세요.

Harvest 및 Grafana 문제 해결

Harvest 및 Grafana 대시보드에 언급된 데이터가 누락되거나 FSx for ONTAP를 사용하여 Harvest 및 Grafana를 설정하는 데 문제가 있는 경우 다음 주제에 잠재적 솔루션이 있는지 확인하세요.

주제

- SVM 및 볼륨 대시보드가 비어 있음
- 제한 시간 이후에 롤백되는 CloudFormation 스택

SVM 및 볼륨 대시보드가 비어 있음

AWS CloudFormation 스택이 성공적으로 배포되어 Grafana에 문의할 수 있지만 SVM 및 볼륨 대시보드가 비어 있는 경우 다음 절차를 사용하여 환경 문제를 해결합니다. Harvest 및 Grafana가 배포된 Amazon EC2 인스턴스에 대한 SSH 액세스 권한이 필요합니다.

1. Harvest 및 Grafana 클라이언트가 실행 중인 Amazon EC2 인스턴스에 대한 SSH입니다.

```
[~]$ ssh ec2-user@ec2_ip_address
```

2. 다음 명령을 사용하여 harvest.yml 파일을 열고.

   - FSx for ONTAP 인스턴스에 대한 항목이 Cluster-2로 생성되었는지 확인합니다.
   - 사용자 이름과 암호의 항목이 fsxadmin 보안 인증 정보와 일치하는지 확인합니다.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /home/ec2-user/harvest_install/harvest/
harvest.yml
```

3. 암호 필드가 비어 있는 경우 다음과 같이 편집기에서 파일을 열고 fsxadmin 암호로 업데이트합니다.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo vi /home/ec2-user/harvest_install/harvest/
harvest.yml
```

4. 향후 배포를 위해 `fsxadmin` 사용자 보안 인증 정보가 Secrets Manager에 다음 형식으로 저장되어 있는지 확인하고 *`fsxadmin_password`*를 암호로 바꿉니다.

```
{"username" : "fsxadmin", "password" : "fsxadmin_password"}
```

제한 시간 이후에 롤백되는 CloudFormation 스택

CloudFormation 스택을 성공적으로 배포할 수 없고 오류가 있는 상태로 롤백되는 경우 다음 절차를 사용하여 문제를 해결합니다. CloudFormation 스택에서 배포한 EC2 인스턴스에 대한 SSH 액세스 권한이 필요합니다.

1. 자동 롤백이 비활성화되어 있는지 확인하여 CloudFormation 스택을 재배포합니다.
2. Harvest 및 Grafana 클라이언트가 실행 중인 Amazon EC2 인스턴스에 대한 SSH입니다.

```
[~]$ ssh ec2-user@ec2_ip_address
```

3. 다음 명령을 사용하여 도커 컨테이너가 성공적으로 시작되었는지 확인합니다.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo docker ps
```

응답에는 다음과 같이 5개의 컨테이너가 표시됩니다.

```
CONTAINER ID   IMAGE                     COMMAND                  CREATED
 STATUS                           PORTS                     NAMES
6b9b3f2085ef   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago
 Restarting (1) 20 seconds ago                              harvest_cluster-2
3cf3e3623fde   rahulguptajss/harvest   "bin/poller --config…"   8 minutes ago   Up
 About a minute                                             harvest_cluster-1
708f3b7ef6f8   grafana/grafana         "/run.sh"                8 minutes ago   Up
 8 minutes                   0.0.0.0:3000->3000/tcp   harvest_grafana
0febee61cab7   prom/alertmanager       "/bin/alertmanager -…"   8
 minutes ago   Up 8 minutes                    0.0.0.0:9093->9093/tcp
 harvest_prometheus_alertmanager
1706d8cd5a0c   prom/prometheus         "/bin/prometheus --c…"   8 minutes ago   Up
 8 minutes                   0.0.0.0:9090->9090/tcp   harvest_prometheus
```

4. 도커 컨테이너가 실행되지 않는 경우 다음과 같이 `/var/log/cloud-init-output.log` 파일에서 실패 여부를 확인합니다.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo cat /var/log/cloud-init-output.log
     PLAY [Manage Harvest]
 ***********************************************************

TASK [Gathering Facts] ***************************************************
ok: [localhost]

TASK [Verify images] *****************************************************
failed: [localhost] (item=prom/prometheus) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/prometheus",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}
failed: [localhost] (item=prom/alertmanager) => {"ansible_loop_var": "item",
 "changed": false, "item": "prom/alertmanage
r", "msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104,
'Connection reset by peer'))"}
failed: [localhost] (item=rahulguptajss/harvest) => {"ansible_loop_var": "item",
 "changed": false, "item": "rahulguptajs
s/harvest", "msg": "Error connecting: Error while fetching server API version:
 ('Connection aborted.', ConnectionResetEr
ror(104, 'Connection reset by peer'))"}
failed: [localhost] (item=grafana/grafana) => {"ansible_loop_var": "item",
 "changed": false, "item": "grafana/grafana",
"msg": "Error connecting: Error while fetching server API version: ('Connection
 aborted.', ConnectionResetError(104, 'Co
nnection reset by peer'))"}

PLAY RECAP ***************************************************************
localhost                  : ok=1    changed=0    unreachable=0    failed=1
 skipped=0    rescued=0    ignored=0
```

5. 장애가 발생하면 다음 명령을 실행하여 Harvest 및 Grafana 컨테이너를 배포합니다.

```
[ec2-user@ip-ec2_ip_address ~]$ sudo su
     [ec2-user@ip-ec2_ip_address ~]$ cd /home/ec2-user/harvest_install
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml
     [ec2-user@ip-ec2_ip_address ~]$ /usr/local/bin/ansible-playbook
 manage_harvest.yml --tags api
```

6. sudo docker ps를 실행하고 Harvest 및 Grafana URL에 연결하여 컨테이너가 성공적으로 시작되었는지 확인합니다.

를 사용하여 FSx for ONTAP API 호출 모니터링 AWS CloudTrail

Amazon FSx는 Amazon FSx에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Amazon FSx for NetApp ONTAP에 대한 모든 Amazon FSx API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Amazon FSx 콘솔로부터의 호출과 Amazon FSx API 작업에 대한 코드 호출이 포함됩니다.

추적을 생성하면 Amazon FSx 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 트레일을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집하는 정보를 사용하여 Amazon FSx에 어떤 요청이 이루어졌는지 확인할 수 있습니다. 또한 어떤 IP 주소에서 요청했는지, 누가 언제 요청했는지 등의 추가 세부 정보도 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Amazon FSx 정보

AWS 계정을 생성할 때 계정에서 CloudTrail이 활성화됩니다. Amazon FSx에서 API 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amazon FSx에 대한 이벤트를 포함하여 AWS 계정의 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 추적을 생성하면 추적이 모든 AWS 리전에 적용됩니다. 추적은 AWS 파티션의 모든 AWS 리전에서 이벤트를 로깅하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은AWS CloudTrail 사용 설명서에서 다음 주제를 참조하세요.

- 에 대한 추적 생성 AWS 계정
- AWS CloudTrail Logs와의 서비스 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Amazon FSx API 호출은 CloudTrail에서 로깅합니다. 예를 들어, `CreateFileSystem` 및 `TagResource` 작업에 대한 호출은 CloudTrail 로그 파일의 항목을 생성합니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 자격 증명을 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부.

자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail userIdentity 요소를 참조하세요.

Amazon FSx 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예는 콘솔에서 파일 시스템의 태그를 만든 경우 `TagResource` 작업을 실행하는 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": “111122223333”,
        "arn": "arn:aws:sts::111122223333:root”,
        "accountId": “111122223333”,
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE”,
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T22:36:07Z"
            }
        }
    },
    "eventTime": "2018-11-14T22:36:07Z",
    "eventSource": "fsx.amazonaws.com",
```

```
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": “192.0.2.0”,
    "userAgent": “console.amazonaws.com”,
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789”
    },
    "responseElements": null,
    "requestID": “aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51”,
    "eventID": “bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p”,
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": “111122223333”
}
```

다음 예는 콘솔에서 파일 시스템의 태그를 삭제할 경우 진행되는 UntagResource 작업에 대한 CloudTrail 로그 항목을 보여줍니다.

```
{
    "eventVersion": "1.05",
    "userIdentity": {
        "type": “Root”,
        "principalId": "111122223333",
        "arn": "arn:aws:sts::111122223333:root",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "attributes": {
                "mfaAuthenticated": "false",
                "creationDate": "2018-11-14T23:40:54Z"
            }
        }
    },
    "eventTime": "2018-11-14T23:40:54Z",
    "eventSource": "fsx.amazonaws.com",
    "eventName": "UntagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "console.amazonaws.com",
    "requestParameters": {
        "resourceARN": "arn:aws:fsx:us-east-1:111122223333:file-system/fs-
ab12cd34ef56gh789"
```

```
    },
    "responseElements": null,
    "requestID": "aEXAMPLE-abcd-1234-56ef-b4cEXAMPLE51",
    "eventID": "bEXAMPLE-gl12-3f5h-3sh4-ab6EXAMPLE9p",
    "eventType": "AwsApiCall",
    "apiVersion": "2018-03-01",
    "recipientAccountId": "111122223333"
}
```

FSx for ONTAP에서 Microsoft Active Directory 작업

Amazon FSx는 Microsoft Active Directory와 페더레이션되어 기존 환경에 통합됩니다. Active Directory는 네트워크상의 객체에 대한 정보를 저장하고 관리자 및 사용자가 해당 정보를 찾아 사용할 수 있도록 지원하는 데 사용되는 Microsoft 디렉터리 서비스입니다. 이러한 객체에는 일반적으로 파일 서버, 네트워크 사용자 및 컴퓨터 계정과 같은 공유 리소스가 포함됩니다.

선택적으로 FSx for ONTAP 스토리지 가상 머신(SVM)을 Active Directory 도메인에 조인하여 사용자 인증과 파일 및 폴더 수준의 액세스 제어를 제공할 수 있습니다. 그러면 서버 메시지 블록(SMB) 클라이언트가 Active Directory의 기존 사용자 ID를 사용하여 자신을 인증하고 SVM 볼륨에 액세스할 수 있습니다. 사용자는 기존 ID를 사용하여 개별 파일 및 폴더에 대한 액세스를 제어할 수 있습니다. 또한 기존 파일 및 폴더와 해당 보안 액세스 제어 목록(ACL) 구성을 수정 없이 Amazon FSx로 마이그레이션할 수 있습니다.

Microsoft Active Directory 도메인 인프라를 사용할 수 없는 경우 SVM을 Microsoft Active Directory에 조인하는 대신 SVM의 작업 그룹에서 서버 메시지 블록(SMB) 서버를 구성할 수 있습니다. 자세한 내용은 작업 그룹에서 SMB 서버 설정 단원을 참조하십시오.

Amazon FSx for NetApp ONTAP을 Active Directory에 조인하는 경우 파일 시스템의 SVM을 Active Directory에 독립적으로 조인합니다. 즉, Active Directory에 조인된 일부 SVM 및 그렇지 않은 SVM이 포함된 파일 시스템을 사용할 수 있습니다.

SVM을 Active Directory에 조인한 후 다음의 Active Directory 구성 속성을 업데이트할 수 있습니다.

- DNS 서버 IP 주소
- 자체 관리형 Active Directory 서비스 계정 사용자 이름 및 암호

주제

- SVM을 자체 관리형 Microsoft Active Directory에 조인하기 위한 사전 조건
- Active Directory 작업의 모범 사례
- SVMs Microsoft Active Directory에 조인하는 방법
- SVM Active Directory 구성 관리

SVM을 자체 관리형 Microsoft Active Directory에 조인하기 위한 사전 조건

FSx for ONTAP SVM을 자체 관리형 Microsoft Active Directory 도메인에 조인하기 전에 Active Directory 및 네트워크가 다음 섹션에 설명된 요구 사항을 충족하는지 확인합니다.

주제

온프레미스 Active Directory 요구 사항

SVM에 조인할 수 있는 온프레미스 또는 기타 자체 관리형 Microsoft Active Directory가 이미 있어야 합니다. 이 Active Directory의 구성은 다음과 같아야 합니다.

- Active Directory 도메인 컨트롤러의 도메인 기능 수준은 Windows Server 2000 이상입니다.
- Active Directory는 단일 레이블 도메인(SLD) 형식이 아닌 도메인 이름을 사용합니다. Amazon FSx는 현재 SLD 도메인을 지원하지 않습니다.
- Active Directory 사이트가 정의되어 있는 경우에는 FSx for ONTAP 파일 시스템과 연결된 VPC의 서브넷이 동일한 Active Directory 사이트에 정의되어 있도록 하고 VPC 서브넷과 Active Directory 사이트의 서브넷 간에 충돌이 존재하지 않도록 해야 합니다.

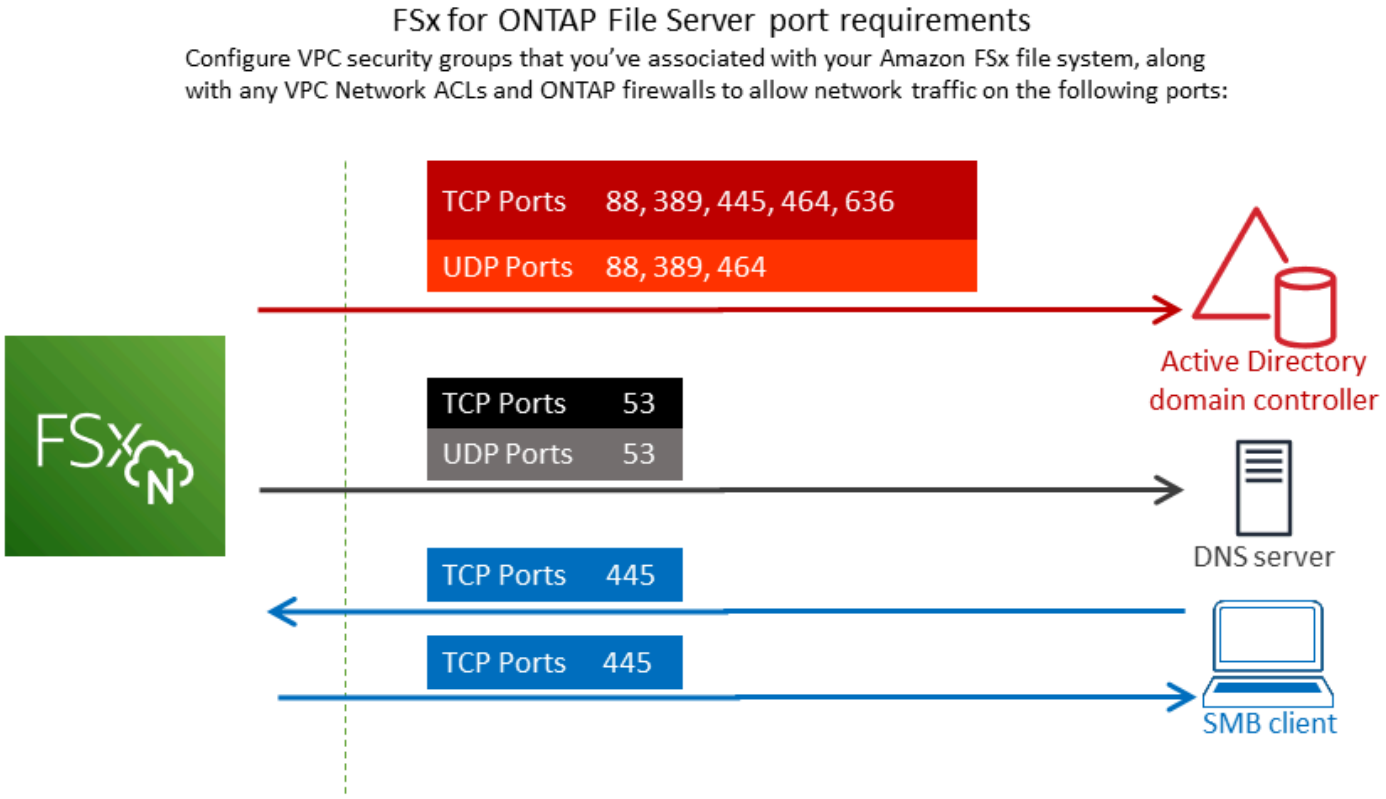
> **Note**
>
> 를 사용하는 경우 AWS Directory Service FSx for ONTAP은 SVMs Simple Active Directory에 조인하는 것을 지원하지 않습니다.

네트워크 구성 요구 사항

다음 네트워크 구성이 준비되었고 관련 정보를 사용할 수 있는지 확인합니다.

> **Important**
>
> SVM이 Active Directory에 조인하려면 이 주제에 설명된 포트가 모든 Active Directory 도메인 컨트롤러와 SVM의 iSCSI IP 주소(iscsi_1 및 iscsi_2 논리 인터페이스(LIF)) 간의 트래픽을 허용하는지 확인해야 합니다.

- DNS 서버 및 Active Directory 도메인 컨트롤러 IP 주소입니다.
- AWS Direct Connect, AWS VPN 또는 AWS Transit Gateway를 사용하는, 파일 시스템이 생성될 Amazon VPC와 자체 관리형 Active Directory 간의 연결.
- 파일 시스템이 생성될 서브넷의 보안 그룹 및 VPC 네트워크 ACL이 다음 다이어그램에 표시된 방향으로 포트를 통한 트래픽을 허용해야 합니다.



다음 표에서는 각 포트의 역할을 설명합니다.

프로토콜	포트	역할
TCP/UDP	53	도메인 이름 시스템(DNS)

프로토콜	포트	역할
TCP/UDP	88	Kerberos 인증
TCP/UDP	389	Lightweight Directory Access Protocol(LDAP)
TCP	445	디렉터리 서비스 SMB 파일 공유
TCP/UDP	464	암호 변경/설정
TCP	636	Lightweight Directory Access Protocol over TLS/SSL(LDAPS)

- 이러한 트래픽 규칙이 각 Active Directory 도메인 컨트롤러, DNS 서버 및 FSx 클라이언트, FSx 관리자에 적용되는 방화벽에도 반영되는지 확인하세요.

> **Important**
>
> Amazon VPC 보안 그룹에서는 네트워크 트래픽이 시작되는 방향으로만 포트를 열어야 하지만, 대부분의 Windows 방화벽과 VPC 네트워크 ACL에서는 포트가 양방향으로 열려 있어야 합니다.

Active Directory 서비스 계정 요구 사항

자체 관리형 Microsoft Active Directory에는 컴퓨터를 도메인에 조인할 수 있는 권한이 위임된 서비스 계정이 있어야 합니다. 서비스 계정은 특정 작업을 수행할 권한이 위임된 자체 관리형 Active Directory의 사용자 계정입니다.

최소한 SVM에 조인하려는 OU에서 서비스 계정에 다음 권한을 위임해야 합니다.

- 암호 재설정 기능
- 계정의 데이터 읽기 및 쓰기 제한 기능
- 컴퓨터 객체에 `msDS-SupportedEncryptionTypes` 속성을 설정하는 기능
- 검증된 DNS 호스트 이름 쓰기 기능
- 검증된 서비스 보안 주체 이름 쓰기 기능
- 컴퓨터 객체를 생성하고 삭제할 수 있는 기능
- 계정 제한 사항을 읽고 쓸 수 있는 검증된 기능

이는 컴퓨터 객체를 Active Directory에 조인하는 데 필요한 최소 권한 집합을 나타냅니다. 자세한 내용은 Windows Server 설명서의 오류: 제어를 위임받은 관리자가 아닌 사용자가 컴퓨터를 도메인 컨트롤러에 조인하려고 하면 액세스가 거부됨 항목을 참조하세요.

올바른 권한으로 서비스 계정을 생성하는 방법에 대해 자세히 알아보려면 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

> **Important**
>
> Amazon FSx를 사용하려면 Amazon FSx 파일 시스템의 수명 주기 동안 유효한 서비스 계정이 필요합니다. Amazon FSx는 파일 시스템을 완벽하게 관리하고 리소스를 Active Directory 도메인에 조인 해제했다가 다시 조인하는 데 필요한 작업을 수행할 수 있어야 합니다. 이러한 작업에는 장애가 발생한 파일 시스템 또는 SVM 교체 또는 NetApp ONTAP 소프트웨어 패치가 포함됩니다. 서비스 계정 자격 증명을 포함하여 Amazon FSx를 통해 Active Directory 구성 정보를 최신 상태로 유지하세요. 자세한 내용은 Amazon FSx를 사용하여 Active Directory 구성을 최신 상태로 유지을 참조하십시오.

AWS 및 FSx for ONTAP을 처음 사용하는 경우 Active Directory 통합을 시작하기 전에 초기 설정 단계를 완료해야 합니다. 자세한 내용은 FSx for ONTAP 설정 단원을 참조하십시오.

> **Important**
>
> SVM이 생성된 후 Amazon FSx가 OU에서 생성한 컴퓨터 객체를 이동하거나 SVM이 조인된 상태에서 Active Directory를 삭제하지 않습니다. 그러면 SVM이 잘못 구성될 수 있습니다.

Active Directory 작업의 모범 사례

다음은 Amazon FSx for NetApp ONTAP SVM을 자체 관리형 Microsoft Active Directory에 조인할 때 고려해야 할 몇 가지 제안 및 지침입니다. 이는 모범 사례로 권장되지만 필수 사항은 아닙니다.

Amazon FSx 서비스 계정에 권한 위임

Amazon FSx에 제공하는 서비스 계정을 필요한 최소 권한으로 구성해야 합니다. 또한 조직 단위(OU)를 다른 도메인 컨트롤러 문제와 분리합니다.

Amazon FSx SVM을 도메인에 조인하려면 서비스 계정에 권한이 위임되었는지 확인해야 합니다. Domain Admins 그룹의 구성원은 이 작업을 수행할 수 있는 충분한 권한을 가지고 있습니다. 그러나

이 작업에 필요한 최소 권한만을 가진 서비스 계정을 사용하는 것이 모범 사례입니다. 다음 절차는 FSx for ONTAP SVM을 도메인에 조인하는 데 필요한 권한만 위임하는 방법을 보여줍니다.

이 절차는 디렉터리에 조인되고 Active Directory User and Computers MMC 스냅인이 설치된 머신에서 수행합니다.

Microsoft Active Directory 도메인의 서비스 계정을 생성하려면

1. Microsoft Active Directory 도메인의 도메인 관리자로 로그인했는지 확인합니다.
2. Active Directory User and Computers MMC 스냅인을 엽니다.
3. 작업 창에서 도메인 노드를 확장합니다.
4. 수정하려는 OU에 대한 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 찾아 연 다음 제어 위임을 선택합니다.
5. 제어 위임 마법사 페이지에서 다음을 선택합니다.
6. 추가를 선택하여 선택된 사용자 및 그룹에 특정 사용자 또는 특정 그룹을 추가한 후 다음을 선택합니다.
7. 위임할 작업 페이지에서 위임할 사용자 지정 작업 만들기를 선택하고 다음을 선택합니다.
8. 폴더의 다음 객체만을 선택한 후 컴퓨터 객체를 선택합니다.
9. 이 폴더에서 선택한 객체 생성을 선택한 후 이 폴더에서 선택한 객체 삭제를 선택합니다. 그런 다음 다음을 선택합니다.
10. 이러한 권한 표시에서 일반 및 속성별 이 선택되어 있는지 확인합니다.
11. 권한에서 다음을 선택합니다.
    - 암호 재설정
    - 읽기 및 쓰기 계정 제한
    - DNS 호스트 이름에 대한 검증된 쓰기
    - 서비스 보안 주체 이름에 대한 검증된 쓰기
    - msDS -SupportedEncryptionTypes 쓰기
12. 다음을 선택한 후 완료를 선택합니다.
13. Active Directory User and Computers MMC 스냅인을 닫습니다.

> **Important**
>
> SVM이 생성된 후 Amazon FSx가 OU에 생성한 컴퓨터 객체를 이동하지 않습니다. 그러면 SVM이 잘못 구성될 수 있습니다.

Amazon FSx를 사용하여 Active Directory 구성을 최신 상태로 유지

Amazon FSx SVM을 중단 없이 사용할 수 있도록 하려면 자체 관리형 AD 설정을 변경할 때 SVM의 자체 관리형 Active Directory(AD) 구성을 업데이트합니다.

예를 들어 AD가 시간 기반 암호 재설정 정책을 사용한다고 가정합니다. 이 경우 암호가 재설정되는 즉시 Amazon FSx로 서비스 계정 암호를 업데이트해야 합니다. 이렇게 하려면 Amazon FSx 콘솔, Amazon FSx API 또는를 사용합니다 AWS CLI. 마찬가지로 Active Directory 도메인의 DNS 서버 IP 주소가 변경되는 경우 변경이 발생하는 즉시 Amazon FSx로 DNS 서버 IP 주소를 업데이트합니다.

업데이트된 자체 관리형 Active Directory 구성에 문제가 있는 경우 SVM 상태가 잘못 구성됨으로 전환됩니다. 이 상태에는 콘솔, API 및 CLI의 SVM 설명 옆에 오류 메시지와 권장 조치가 표시됩니다. SVM의 AD 구성에 문제가 발생하는 경우 구성 속성에 대해 권장되는 수정 조치를 취해야 합니다. 문제가 해결되면 SVM의 상태가 생성됨으로 변경되는지 확인합니다.

자세한 내용은 AWS Management ConsoleAWS CLI및 API를 사용하여 기존 SVM Active Directory 구성 업데이트 및 ONTAP CLI를 사용하여 Active Directory 구성 수정 섹션을 참조하세요.

보안 그룹을 사용하여 VPC 내 트래픽 제한

Virtual Private Cloud(VPC)에서 네트워크 트래픽을 제한하기 위해 VPC에 최소 권한 원칙을 구현할 수 있습니다. 다시 말해, 권한을 필요한 최소 권한으로 제한할 수 있습니다. 이렇게 하려면 보안 그룹 규칙을 사용합니다. 자세한 내용은 Amazon VPC 보안 그룹 섹션을 참조하세요.

파일 시스템의 네트워크 인터페이스에 대한 아웃바운드 보안 그룹 규칙 생성

보안을 강화하려면 아웃바운드 트래픽 규칙을 사용하여 보안 그룹을 구성하는 것이 좋습니다. 이러한 규칙은 아웃바운드 트래픽을 자체 관리형 AD 도메인 컨트롤러에만 허용하거나 서브넷 또는 보안 그룹 내에서만 허용해야 합니다. Amazon FSx 파일 시스템의 탄력적 네트워크 인터페이스와 연결된 VPC에 이 보안 그룹을 적용합니다. 자세한 내용은 Amazon VPC를 사용한 파일 시스템 액세스 제어을 참조하십시오.

SVMs Microsoft Active Directory에 조인하는 방법

조직은 온프레미스든 클라우드든 상관없이 Active Directory를 사용하여 ID와 디바이스를 관리할 수 있습니다. FSx for ONTAP을 사용하면 다음과 같은 방법으로 SVM을 기존 Active Directory 도메인에 직접 조인할 수 있습니다.

- 생성 시 Active Directory에 새 SVMs 조인:
  - Amazon FSx 콘솔의 표준 생성 옵션을 사용하여 새 FSx for ONTAP 파일 시스템을 생성하면 기본 SVM을 자체 관리형 Active Directory에 조인할 수 있습니다. 자세한 내용은 파일 시스템 생성(콘솔) 단원을 참조하십시오.
  - Amazon FSx 콘솔 AWS CLI또는 Amazon FSx API를 사용하여 기존 FSx for ONTAP 파일 시스템에 새 SVM을 생성합니다. 자세한 내용은 스토리지 가상 머신 생성(SVM) 단원을 참조하십시오.
- 기존 SVM을 Active Directory에 가입.
  - AWS Management Console AWS CLI및 API를 사용하여 SVM을 Active Directory에 조인하고, 초기 조인 시도가 실패한 경우 SVM을 Active Directory에 다시 조인합니다. 이미 Active Directory에 조인된 SVM의 일부 Active Directory 구성 속성을 업데이트할 수도 있습니다. 자세한 내용은 SVM Active Directory 구성 관리 단원을 참조하십시오.
  - NetApp ONTAP CLI 및 REST API를 사용하여 SVM을 Active Directory에 조인, 조인 재시도, 조인 해제하는 구성을 관리합니다. 자세한 내용은 NetApp CLI를 사용하여 SVM Active Directory 구성 업데이트 단원을 참조하십시오.

> **Important**
>
> - Amazon FSx는 Microsoft DNS를 기본 DNS 서비스로 사용하는 경우에만 SVM에 대한 DNS 레코드를 등록합니다. 서드 파티 DNS를 사용하는 경우 Amazon FSx SVM을 생성한 후 수동으로 DNS 항목을 설정해야 합니다.
> - 를 사용하는 경우 AWS 위임된 FSx 관리자, AWS 위임된 관리자 또는 OU에 위임된 권한이 있는 사용자 지정 그룹과 같은 그룹을 지정해야 AWS Managed Microsoft AD합니다.

FSx for ONTAP SVM을 자체 관리형 Active Directory에 직접 조인하는 경우 SVM은 동일한 Active Directory 포리스트(도메인, 사용자, 컴퓨터를 포함하는 Active Directory 구성의 최상위 논리적 컨테이너)와 사용자 및 기존 리소스(기존 파일 서버 포함)와 동일한 Active Directory 도메인에 있습니다.

SVM을 Active Directory에 조인할 때 필요한 정보

선택한 API 작업과 관계없이 SVM을 Active Directory에 조인할 때는 Active Directory에 대해 다음 정보를 제공해야 합니다.

- SVM에 대해 생성할 Active Directory 컴퓨터 객체의 NetBIOS 이름. Active Directory의 SVM 이름이며 Active Directory 내에서 고유해야 합니다. 홈 도메인의 NetBIOS 이름을 사용하지 않습니다. NetBIOS 이름은 15자를 초과할 수 없습니다.
- Active Directory의 정규화된 도메인 이름(FQDN). FQDN은 255자를 초과할 수 없습니다.

> **Note**
>
> FQDN은 단일 레이블 도메인(SLD) 형식일 수 없습니다. Amazon FSx는 현재 SLD 도메인을 지원하지 않습니다.

- 도메인의 DNS 서버 또는 도메인 호스트의 IP 주소 최대 3개.

  DNS 서버 IP 주소 및 Active Directory 도메인 컨트롤러 IP 주소는 다음을 제외한 모든 IP 주소 범위에 속할 수 있습니다.

  - 해당 AWS 리전에서 Amazon Web Service가 소유한 IP 주소와 충돌하는 IP 주소입니다. 리전별 AWS IP 주소 목록은 AWS IP 주소 범위를 참조하세요.
  - 다음 CIDR 블록 범위의 IP 주소: 198.19.0.0/16
- SVM을 Active Directory 도메인에 조인할 때 Amazon FSx용 Active Directory 도메인의 서비스 계정에 대한 사용자 이름 및 암호입니다. 서비스 계정 요구 사항에 대한 자세한 내용은 Active Directory 서비스 계정 요구 사항 섹션을 참조하세요.
- (선택 사항) SVM에 조인하는 도메인의 조직 단위(OU)입니다.

> **Note**
>
> SVM을 AWS Directory Service Active Directory에 조인하는 경우 관련 디렉터리 객체에 대해가 AWS Directory Service 생성하는 기본 OU 내에 있는 OU를 제공해야 합니다 AWS. 이는가 Active Directory의 기본 `Computers` OU에 대한 액세스를 제공하지 AWS Directory Service 않기 때문입니다. 예를 들어 Active Directory 도메인이 `example.com`인 경우 `OU=Computers,OU=example,DC=example,DC=com` OU를 지정할 수 있습니다.

- (선택 사항) 파일 시스템에서 관리 작업을 수행할 권한을 위임하는 도메인 그룹. 예를 들어 이 도메인 그룹은 Windows SMB 파일 공유를 관리하고 파일 및 폴더의 소유권을 가져오는 등의 작업을 수행할

수 있습니다. 이 그룹을 지정하지 않으면 Amazon FSx는 기본적으로 Active Directory 도메인의 도메인 관리 그룹에 이 권한을 위임합니다.

SVM Active Directory 구성 관리

이 섹션에서는 AWS Management Console, AWS CLI FSx API 및 ONTAP CLI를 사용하여 다음을 수행하는 방법을 설명합니다.

- 기존 SVM을 Active Directory에 가입하기
- 기존 SVM Active Directory 구성 수정
- Active Directory에서 SVMs 제거

Active Directory에서 SVM을 제거하려면 NetApp ONTAP CLI를 사용해야 합니다.

주제

- AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인
- AWS Management ConsoleAWS CLI및 API를 사용하여 기존 SVM Active Directory 구성 업데이트
- NetApp CLI를 사용하여 SVM Active Directory 구성 업데이트

AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인

기존 SVM을 Active Directory에 조인하려면 다음 절차를 따릅니다. 이 절차에서는 SVM이 아직 Active Directory에 조인하지 않았습니다.

Active Directory(AWS Management Console)에 SVM 조인

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 다음과 같이 Active Directory에 조인할 SVM을 선택합니다.
   - 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트하려는 SVM이 있는 ONTAP 파일 시스템을 선택합니다.
   - 스토리지 가상 머신 탭을 선택합니다.

     또는

- 사용 가능한 모든 SVM 목록을 표시하려면 왼쪽 탐색 창에서 ONTAP을 확장하고 스토리지 가상 머신을 선택합니다. 의 계정에 SVMs 목록이 AWS 리전 표시됩니다.

  목록에서 Active Directory에 조인할 SVM을 선택합니다.

3. SVM 요약 패널의 오른쪽 상단에서 작업 > Active Directory 조인/업데이트를 선택합니다. Active Directory에 SVM 연결 창이 표시됩니다.
4. SVM에 조인하려는 Active Directory에 대해 다음 정보를 입력합니다.

   - SVM에 대해 생성할 Active Directory 컴퓨터 객체의 NetBIOS 이름. Active Directory의 SVM 이름이며 Active Directory 내에서 고유해야 합니다. 홈 도메인의 NetBIOS 이름을 사용하지 않습니다. NetBIOS 이름은 15자를 초과할 수 없습니다.
   - Active Directory의 정규화된 도메인 이름(FQDN). 도메인 이름은 255자를 초과할 수 없습니다.
   - DNS 서버 IP 주소 - 도메인의 DNS 서버의 IPv4 주소입니다.
   - 서비스 계정 사용자 이름 - 기존 Active Directory에 있는 서비스 계정의 사용자 이름입니다. 도메인 접두사나 접미사를 포함하지 않습니다. 예를 들어 `EXAMPLE\ADMIN`에는 `ADMIN`만 사용합니다.
   - 서비스 계정 암호 - 서비스 계정의 암호입니다.
   - 암호 확인 - 서비스 계정의 암호입니다.
   - (선택 사항) 조직 단위(OU) - SVM에 조인할 조직 단위의 고유 경로 이름입니다.
   - 위임된 파일 시스템 관리자 그룹 - Active Directory에서 파일 시스템을 관리할 수 있는 그룹의 이름입니다.

     를 사용하는 경우 AWS 위임된 FSx 관리자 AWS Managed Microsoft AD, AWS 위임된 관리자 또는 OU에 위임된 권한이 있는 사용자 지정 그룹과 같은 그룹을 지정해야 합니다.

     자체 관리형 Active Directory에 조인하는 경우 Active Directory에 있는 그룹의 이름을 사용합니다. 기본 그룹은 `Domain Admins`입니다.
5. 제공한 구성을 사용하여 SVM을 Active Directory에 조인하려면 Active Directory 조인을 선택합니다.

SVM을 Active Directory에 조인하려면(AWS CLI)

- FSx for ONTAP SVM을 Active Directory에 조인하려면 다음 예제와 같이 update-storage-virtual machine CLI 명령(또는 이에 상응하는 UpdateStorageVirtualMachine API 작업)을 사용합니다.

```
aws fsx update-storage-virtual-machine \
  --storage-virtual-machine-id svm-abcdef0123456789a\
  --active-directory-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
    OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",
\
    FileSystemAdministratorsGroup="FSxAdmins",UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}',NetBiosName=amznfsx12345
```

스토리지 가상 머신을 생성한 후 Amazon FSx는 다음 예제와 같이 JSON 형식으로 설명을 반환합니다.

```
{
  "StorageVirtualMachine": {
    "ActiveDirectoryConfiguration": {
      "NetBiosName": "amznfsx12345",
      "SelfManagedActiveDirectoryConfiguration": {
        "UserName": "Admin",
        "DnsIps": [
          "10.0.1.3",
          "10.0.91.97"
        ],
        "OrganizationalUnitDistinguishedName": "OU=Computers,OU=customer-
ad,DC=customer-ad,DC=example,DC=com",
        "DomainName": "customer-ad.example.com"
      }
    }
    "CreationTime": 1625066825.306,
    "Endpoints": {
      "Management": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Nfs": {
        "DnsName": "svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.4"]
      },
      "Smb": {
        "DnsName": "amznfsx12345",
```

```
        "IpAddressses": ["198.19.0.4"]
      },
      "SmbWindowsInterVpc": {
        "IpAddressses": ["198.19.0.5", "198.19.0.6"]
      },
      "Iscsi": {
        "DnsName": "iscsi.svm-abcdef0123456789a.fs-0123456789abcdef0.fsx.us-
east-1.amazonaws.com",
        "IpAddressses": ["198.19.0.7", "198.19.0.8"]
      }
    },
    "FileSystemId": "fs-0123456789abcdef0",
    "Lifecycle": "CREATED",
    "Name": "vol1",
    "ResourceARN": "arn:aws:fsx:us-east-1:123456789012:storage-virtual-machine/
fs-0123456789abcdef0/svm-abcdef0123456789a",
    "StorageVirtualMachineId": "svm-abcdef0123456789a",
    "Subtype": "default",
    "Tags": [],

  }
}
```


AWS Management ConsoleAWS CLI및 API를 사용하여 기존 SVM Active Directory 구성 업데이트

다음 절차를 사용하여 이미 Active Directory에 조인된 SVM의 Active Directory 구성을 업데이트합니다.

SVM Active Directory 구성(AWS Management Console)을 업데이트하려면

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 다음과 같이 업데이트할 SVM을 선택합니다.
   - 왼쪽 탐색 창에서 파일 시스템을 선택한 후 업데이트하려는 SVM이 있는 ONTAP 파일 시스템을 선택합니다.
   - 스토리지 가상 머신 탭을 선택합니다.

     또는
   - 사용 가능한 모든 SVM 목록을 표시하려면 왼쪽 탐색 창에서 ONTAP을 확장하고 스토리지 가상 머신을 선택합니다.

목록에서 업데이트할 SVM을 선택합니다.

3. SVM 요약 패널에서 작업 > Active Directory 조인/업데이트를 선택합니다. SVM Active Directory 구성 업데이트 창이 표시됩니다.
4. 이 창에서 다음과 같은 Active Directory 구성 속성을 업데이트할 수 있습니다.
   - DNS 서버 IP 주소 - 도메인의 DNS 서버의 IPv4 주소입니다.
   - 서비스 계정 사용자 이름 - 기존 Active Directory에 있는 서비스 계정의 사용자 이름입니다. 도메인 접두사나 접미사를 포함하지 않습니다. `EXAMPLE\ADMIN`에는 `ADMIN`을 사용합니다.
   - 서비스 계정 암호 - Active Directory 서비스 계정의 암호입니다.
5. 업데이트를 입력한 후 Active Directory 업데이트를 선택하여 변경합니다.

다음 절차를 사용하여 이미 Active Directory에 조인된 SVM의 Active Directory 구성을 업데이트합니다.

SVM Active Directory 구성(AWS CLI)을 업데이트하려면

- AWS CLI 또는 API를 사용하여 SVM의 Active Directory 구성을 업데이트하려면 다음 예제와 같이 update-storage-virtual-machine CLI 명령(또는 동등한 UpdateStorageVirtualMachine API 작업)을 사용합니다.

```
aws fsx update-storage-virtual-machine \
    --storage-virtual-machine-id svm-abcdef0123456789a\
    --active-directory-configuration \
    SelfManagedActiveDirectoryConfiguration='{UserName="FSxService",\
    Password="password", \
    DnsIps=["10.0.1.18"]}'
```

NetApp CLI를 사용하여 SVM Active Directory 구성 업데이트

NetApp ONTAP CLI를 사용하여 SVM을 Active Directory에 조인 및 조인 해제하고 기존 SVM Active Directory 구성을 수정할 수 있습니다.

ONTAP CLI를 사용하여 SVM을 Active Directory에 가입하기

다음 절차의 설명에 따라 ONTAP CLI를 사용하여 기존 SVM을 Active Directory에 조인할 수 있습니다. SVM이 이미 Active Directory에 조인된 경우에도 이 작업을 수행할 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 전체 디렉터리 DNS 이름(corp.example.com) 및 하나 이상의 DNS 서버 IP 주소를 제공하여 Active Directory용 DNS 항목을 생성합니다.

```
::>vserver services name-service dns create -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1, dns_ip_2
```

   DNS 서버에 대한 연결을 확인하려면 다음 명령을 실행합니다. *svm_name*을 사용자의 정보로 바꿉니다.

```
FsxId0ae30e5b7f1a50b6a::>vserver services name-service dns check -vserver svm_name

                            Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svm_name      172.31.14.245   up           Response time (msec): 0
svm_name      172.31.25.207   up           Response time (msec): 1
2 entries were displayed.
```

3. SVM을 Active Directory에 조인하려면 다음 명령을 실행합니다. Active Directory에 아직 존재하지 않는 computer_name을 지정하고 -domain의 디렉터리 DNS 이름을 제공해야 한다는 점에 유의하세요. -OU의 경우 SVM이 조인할 OU 및 전체 DNS 이름을 DC 형식으로 입력합니다.

```
::>vserver cifs create -vserver svm_name -cifs-server computer_name -
domain corp.example.com -OU OU=Computers,OU=example,DC=corp,DC=example,DC=com
```

   Active Directory 연결 상태를 확인하려면 다음 명령을 실행합니다.

```
::>vserver cifs check -vserver svm_name

             Vserver : svm_name
                   Cifs NetBIOS Name : svm_netBIOS_name
                         Cifs Status : Running
```

```
                                  Site : Default-First-Site-Name
Node Name       DC Server Name  DC Server IP    Status   Status Details
--------------- --------------  --------------- ------   --------------
FsxId0ae30e5b7f1a50b6a-01
                corp.example.com
                                172.31.14.245   up       Response time (msec): 5
FsxId0ae30e5b7f1a50b6a-02
                corp.example.com
                                172.31.14.245   up       Response time (msec): 20
2 entries were displayed.
```

4. 이 조인 후에 공유에 액세스할 수 없는 경우 공유에 액세스하는 데 사용하는 계정에 권한이 있는지 확인합니다. 예를 들어 AWS 관리형 Active Directory에서 기본 `Admin` 계정(위임된 관리자)을 사용하는 경우 ONTAP에서 다음 명령을 실행해야 합니다. `netbios_domain`은 Active Directory의 도메인 이름(`corp.example.com`의 경우 여기서 사용되는 `netbios_domain`은 `example`임)과 일치합니다.

```
FsxId0123456789a::>vserver cifs users-and-groups local-group add-members -vserver
 svm_name -group-name BUILTIN\Administrators -member-names netbios_domain\admin
```

ONTAP CLI를 사용하여 Active Directory 구성 수정

ONTAP CLI를 사용하여 기존 Active Directory 구성을 수정할 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 다음 명령을 실행하여 SVM의 CIFS 서버를 일시적으로 가동 중지합니다.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Active Directory의 DNS 항목을 수정해야 하는 경우 다음 명령을 실행합니다.

```
::>vserver services name-service dns modify -vserver svm_name -
domains corp.example.com -name-servers dns_ip_1,dns_ip_2
```

`vserver services name-service dns check -vserver svm_name` 명령을 사용하여 Active Directory의 DNS 서버에 대한 연결 상태를 확인할 수 있습니다.

```
::>vserver services name-service dns check -vserver svm_name
                              Name Server
Vserver       Name Server     Status       Status Details
------------- --------------- ------------ --------------------------
svmciad       dns_ip_1        up           Response time (msec): 1
svmciad       dns_ip_2        up           Response time (msec): 1
2 entries were displayed.
```

4. Active Directory 구성 자체를 수정해야 하는 경우 다음 명령에서 기존 필드를 변경할 수 있습니다.

   - SVM의 NetBIOS(시스템 계정) 이름을 수정하려는 경우 *computer_name*을 변경.
   - 도메인 이름을 수정하려는 경우 *domain_name*을 변경. 이는 이 섹션의 3단계에 기록된 DNS 도메인 항목(`corp.example.com`)과 일치해야 합니다.
   - OU(`OU=Computers,OU=example,DC=corp,DC=example,DC=com`)를 수정하려는 경우 `organizational_unit`을 변경.

   이 디바이스를 Active Directory에 연결하는 데 사용한 Active Directory 보안 인증을 다시 입력해야 합니다.

   ```
   ::>vserver cifs modify -vserver svm_name -cifs-server computer_name -
   domain domain_name -OU organizational_unit
   ```

   `vserver cifs check -vserver svm_name` 명령을 사용하여 Active Directory 연결의 연결 상태를 확인할 수 있습니다.

5. Active Directory 및 DNS 구성 수정을 완료하면 다음 명령을 실행하여 CIFS 서버의 가동을 재개합니다.

   ```
   ::>vserver cifs modify -vserver svm_name -status-admin up
   ```

NetApp ONTAP CLI를 사용하여 SVM에서 Active Directory 조인 해제

NetApp ONTAP CLI를 사용하여 아래 단계에 따라 Active Directory에서 SVM을 조인 해제할 수도 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 다음 명령을 실행하여 Active Directory에서 디바이스 조인을 해제한 CIFS 서버를 삭제합니다. ONTAP에서 SVM의 시스템 계정을 삭제하도록 하려면 원래 SVM을 Active Directory에 조인하는 데 사용한 보안 인증을 제공합니다.

```
FsxId0123456789a::>vserver cifs modify -vserver svm_name -status-admin down
```

3. Active Directory의 DNS 항목을 수정해야 하는 경우 다음 명령을 실행합니다.

```
FsxId0123456789a::vserver cifs delete -vserver svm_name

In order to delete an Active Directory machine account for the CIFS server, you
 must supply the name and password of a Windows account with
sufficient privileges to remove computers from the "CORP.ADEXAMPLE.COM" domain.

Enter the user name: user_name

Enter the password:

Warning: There are one or more shares associated with this CIFS server
         Do you really want to delete this CIFS server and all its shares? {y|n}: y
```

4. 다음 명령을 실행하여 Active Directory용 DNS 서버를 삭제합니다.

```
::vserver services name-service dns delete -vserver svm_name
```

   다음과 같이 ns-switch로 구성된 dns를 제거해야 한다는 경고 메시지가 표시되고 이 디바이스를 Active Directory에 다시 조인할 계획이 없는 경우 ns-switch 항목을 제거할 수 있습니다.

```
Warning: "DNS" is present as one of the sources in one or more ns-switch databases
 but no valid DNS configuration was found for Vserver
         "svm_name". Remove "DNS" from ns-switch using the "vserver services name-
service ns-switch" command. Configuring "DNS" as a source
```

```
          in the ns-switch setting when there is no valid configuration can cause
 protocol access issues.
```

5. (선택 사항) 다음 명령을 실행하여 dns에 대한 ns-switch 항목을 제거합니다. 소스 순서를 확인한 다음 나열된 다른 소스만 sources에 포함되도록 수정하여 hosts 데이터베이스의 dns 항목을 제거합니다. 이 예제에서 유일한 다른 소스는 files입니다.

```
::>vserver services name-service ns-switch show -vserver svm_name -database hosts

                    Vserver: svm_name
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

6. (선택 사항) 데이터베이스 호스트의 sources가 files만 포함하도록 수정하여 dns 항목을 제거합니다.

```
::>vserver services name-service ns-switch modify -vserver svm_name -database hosts
 -sources files
```

Amazon FSx for NetApp ONTAP으로 마이그레이션

다음 섹션에서는 기존 NetApp ONTAP 파일 시스템을 Amazon FSx for NetApp ONTAP으로 마이그레이션하는 방법에 대한 정보를 제공합니다.

> **Note**
>
> `All` 계층화 정책을 사용하여 데이터를 용량 풀 계층으로 마이그레이션하려는 경우 파일 메타데이터는 항상 SSD 계층에 저장되며 모든 새 사용자 데이터는 먼저 SSD 계층에 기록된다는 점에 유념하세요. 데이터가 SSD 계층에 기록되면 백그라운드 계층화 프로세스가 데이터를 용량 풀 스토리지 계층으로 이동하기 시작하지만 계층화 프로세스는 즉시 이루어지지 않으며 네트워크 리소스를 사용합니다. 사용자 데이터를 용량 풀 스토리지 계층으로 이동하기 전에 사용자 데이터를 위한 버퍼로서 파일 메타데이터(사용자 데이터 크기의 3%~7%)를 고려하여 SSD 계층 크기를 조정해야 합니다. SSD 계층의 사용률은 80%를 초과하지 않는 것이 좋습니다. 데이터를 마이그레이션하는 동안 CloudWatch 파일 시스템 지표를 사용하여 SSD 계층을 모니터링하여 계층화 프로세스가 데이터를 용량 풀 스토리지로 이동할 수 있는 것보다 더 빠르게 채워지지 않는지 확인합니다.

주제

- NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션
- AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션

NetApp SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션

NetApp SnapMirror를 사용하여 NetApp ONTAP 파일 시스템을 Amazon FSx for NetApp ONTAP으로 마이그레이션할 수 있습니다.

NetApp SnapMirror는 두 ONTAP 파일 시스템 간에 블록 수준 복제를 사용하여 지정된 소스 볼륨에서 대상 볼륨으로 데이터를 복제합니다. SnapMirror를 사용하여 온프레미스 NetApp ONTAP 파일 시스템을 FSx for ONTAP으로 마이그레이션하는 것이 좋습니다. NetApp SnapMirror의 블록 레벨 복제는 다음과 같은 파일 시스템에서도 빠르고 효율적입니다.

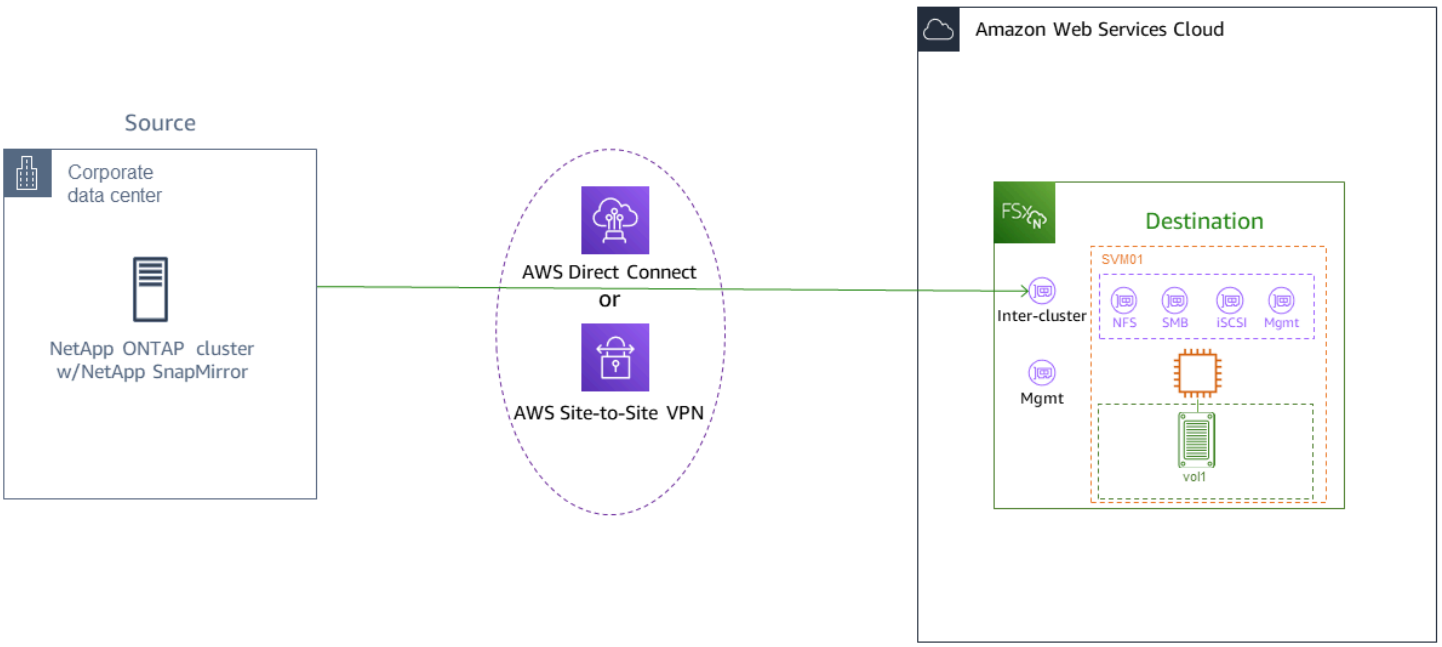
- 복잡한 디렉터리 구조
- 5천만 개 이상의 파일

- 매우 작은 파일 크기(킬로바이트 정도)

SnapMirror를 사용하여 FSx for ONTAP으로 마이그레이션하면 중복 제거 및 압축된 데이터가 해당 상태로 유지되므로 전송 시간이 단축되고 마이그레이션에 필요한 대역폭이 줄어듭니다. 소스 ONTAP 볼륨에 있는 스냅샷은 대상 볼륨으로 마이그레이션될 때 보존됩니다. 온프레미스 NetApp ONTAP 파일 시스템을 FSx for ONTAP으로 마이그레이션하려면 다음과 같은 높은 수준의 작업이 필요합니다.

1. Amazon FSx에서 대상 볼륨 생성.
2. 소스 및 대상 논리 인터페이스(LIF) 수집.
3. 소스 파일 시스템과 대상 파일 시스템 간에 클러스터 피어링 설정.
4. SVM 피어링 관계 생성.
5. SnapMirror 관계 생성.
6. 업데이트된 대상 클러스터 유지 관리.
7. FSx for ONTAP 파일 시스템으로 전환.

다음 다이어그램은 이 섹션에 설명된 마이그레이션 시나리오를 보여줍니다.



주제

- 시작하기 전 준비 사항
- 대상 볼륨 생성
- 소스 및 대상 클러스터 간 LIF 기록

- 소스 및 대상 간에 클러스터 피어링 설정
- SVM 피어링 관계 생성
- SnapMirror 관계 생성
- FSx for ONTAP 파일 시스템으로 데이터 전송
- Amazon FSx로 전환

시작하기 전 준비 사항

다음 섹션에 설명된 절차를 사용하기 전에 다음 사전 조건을 충족해야 합니다.

- FSx for ONTAP은 데이터 계층화, 스토리지 효율성, 백업 등의 백그라운드 작업보다 클라이언트 트래픽에 우선 순위를 둡니다. 데이터를 마이그레이션할 때는 일반적으로 SSD 계층의 용량을 모니터링하여 사용률이 80%를 초과하지 않도록 하는 것이 좋습니다. CloudWatch 파일 시스템 지표를 사용하여 SSD 계층의 사용률을 모니터링할 수 있습니다. 자세한 내용은 볼륨 지표 섹션을 참조하세요.
- 데이터를 마이그레이션할 때 대상 볼륨의 데이터 계층화 정책을 `All`로 설정하면 모든 파일 메타데이터가 기본 SSD 스토리지 계층에 저장됩니다. 파일 메타데이터는 볼륨의 데이터 계층화 정책과 관계없이 항상 SSD 기반 기본 계층에 저장됩니다. 기본 계층과 용량 풀 계층 스토리지 용량의 비율을 1:10으로 가정하는 것이 좋습니다.
- 소스 및 대상 파일 시스템은 동일한 VPC에 연결되거나 Amazon VPC 피어링, Transit Gateway AWS Direct Connect 또는를 사용하여 피어링되는 네트워크에 있습니다 AWS VPN. 자세한 내용은 Amazon VPC 피어링 가이드의 내에서 데이터 액세스 AWS 클라우드와 VPC 피어링이란? 섹션을 참조하세요.
- ONTAP용 FSx 파일 시스템의 VPC 보안 그룹에는 클러스터 간 엔드포인트(LIF)용 포트 443, 10000, 11104 및 11105에서 ICMP와 TCP를 허용하는 인바운드 및 아웃바운드 규칙이 있습니다.
- SnapMirror 데이터 보호 관계를 생성하기 전에 소스 볼륨과 대상 볼륨이 호환되는 NetApp ONTAP 버전을 실행하고 있는지 확인합니다. 자세한 내용은 NetApp의 ONTAP 사용자 설명서에서 SnapMirror 관계에 대한 호환 가능한 ONTAP 버전을 참조하세요. 여기에 제시된 절차는 온프레미스 NetApp ONTAP 파일 시스템을 소스로 사용합니다.
- 온프레미스 (소스) NetApp ONTAP 파일 시스템에는 SnapMirror 라이센스가 포함되어 있습니다.
- SVM을 사용하여 대상 FSx for ONTAP 파일 시스템을 생성했지만 대상 볼륨은 생성하지 않았습니다. 자세한 내용은 파일 시스템 만들기 섹션을 참조하세요.

이 절차의 명령은 다음 클러스터, SVM 및 볼륨 별칭을 사용합니다.

- *`FSx-Dest`* – 대상(FSx) 클러스터의 ID(FSxIdabcdef1234567890a 형식).

- *OnPrem-Source* – 소스 클러스터의 ID.
- *DestSVM* – 대상 SVM 이름.
- *SourceSVM* – 소스 SVM 이름.
- 소스 볼륨 이름과 대상 볼륨 이름 모두 `vol1`입니다.

> **Note**
>
> FSx for ONTAP 파일 시스템은 모든 ONTAP CLI 명령에서 클러스터라고 합니다.

이 섹션의 절차에서는 다음과 같은 NetApp ONTAP CLI 명령을 사용합니다.

- volume create 명령
- cluster 명령
- vserver peer 명령
- snapmirror 명령

NetApp ONTAP CLI를 사용하여 FSx for ONTAP 파일 시스템에서 SnapMirror 구성을 생성하고 관리합니다. 자세한 내용은 NetApp ONTAP CLI 사용 섹션을 참조하세요.

대상 볼륨 생성

NetApp ONTAP CLI 및 REST API 외에도 Amazon FSx 콘솔 AWS CLI, 및 Amazon FSx API를 사용하여 데이터 보호(DP) 대상 볼륨을 생성할 수 있습니다. Amazon FSx 콘솔을 사용하여 대상 볼륨을 생성하는 방법에 대한 자세한 내용은 섹션을 AWS CLI참조하세요볼륨 생성.

> **Note**
>
> ONTAP는 대상 볼륨의 계층화 정책이 인 경우 대상 DP 볼륨의 소스에서 달성된 프로세스 후 압축 절감을 보존하지 않습니다`All`. 프로세스 후 압축 절감을 유지하려면 대상 볼륨 계층화 정책을 `Auto` 로 설정하고 대상 파일 시스템에서 inactive-data-compression을 활성화하여 대상에서 프로세스 후 압축 절감을 다시 적용해야 합니다.

다음 절차에서는 NetApp ONTAP CLI를 사용하여 FSx for ONTAP 파일 시스템의 대상 볼륨을 생성합니다. 파일 시스템의 관리 포트의 `fsxadmin` 암호와 IP 주소 또는 DNS 이름이 필요합니다.

1. 파일 시스템을 생성할 때 설정한 사용자 fsxadmin과 암호를 사용하여 대상 파일 시스템과의 SSH 세션을 설정합니다.

```
ssh fsxadmin@file-system-management-endpoint-ip-address
```

2. 대상 클러스터에 최소한 소스 볼륨 스토리지 용량과 같은 스토리지 용량을 가진 볼륨을 생성합니다. -type DP를 사용하여 SnapMirror 관계의 대상으로 지정합니다.

   데이터 계층화를 사용하려는 경우 -tiering-policy를 all로 설정하는 것이 좋습니다. 이렇게 하면 데이터가 용량 풀 스토리지로 즉시 전송되고 SSD 계층의 용량이 부족해지는 것을 방지할 수 있습니다. 마이그레이션 후에는 -tiering-policy를 auto로 전환할 수 있습니다.

> **Note**
>
> 파일 메타데이터는 볼륨의 데이터 계층화 정책과 관계없이 항상 SSD 기반 기본 계층에 저장됩니다.

```
FSx-Dest::> vol create -vserver DestSVM -volume vol1 -aggregate aggr1 -size 1g -
type DP -tiering-policy all
```

소스 및 대상 클러스터 간 LIF 기록

SnapMirror는 각각 고유한 IP 주소를 가진 클러스터 간 논리 인터페이스(LIF)를 사용하여 소스 및 대상 클러스터 간의 데이터 전송을 용이하게 합니다.

1. 대상 FSx for ONTAP 파일 시스템의 경우 파일 시스템 세부 정보 페이지의 관리 탭으로 이동하여 Amazon FSx 콘솔에서 클러스터 간 엔드포인트 - IP 주소를 검색할 수 있습니다.
2. 소스 NetApp ONTAP 클러스터에서는 ONTAP CLI를 사용하여 클러스터 간 LIF IP 주소를 검색합니다. 다음 명령을 실행합니다.

```
OnPrem-Source::> network interface show -role intercluster

Logical                         Network
Vserver     Interface  Status  Address/Mask
----------- ---------- ------- ------------
FSx-Dest
             inter_1    up/up  10.0.0.36/24
```

```
            inter_2     up/up   10.0.1.69/24
```

> **Note**
>
> 2세대 Single-AZ 파일 시스템의 경우 각 고가용성(HA) 페어에 대해 클러스터 간 IP 주소가 두 개 있습니다. 나중에 사용할 수 있도록 이 값을 저장합니다.

`inter_1` 및 `inter_2` IP 주소를 저장합니다. 이들은 `FSx-Dest`에서는 `dest_inter_1`과 `dest_inter_2`로, `OnPrem-Source`에 대해서는 `source_inter_1`과 `source_inter_2`로 참조됩니다.

소스 및 대상 간에 클러스터 피어링 설정

클러스터 간 IP 주소를 제공하여 대상 클러스터에서 클러스터 피어 관계를 설정합니다. 또한 소스 클러스터에서 클러스터 피어링을 설정할 때 필요한 암호를 생성해야 합니다.

1. 다음 명령을 사용하여 대상 클러스터에서 피어링을 설정합니다. 2세대 Single-AZ 파일 시스템의 경우 각 클러스터 간 IP 주소를 제공해야 합니다.

```
FSx-Dest::> cluster peer create -address-family ipv4 -peer-
addrs source_inter_1,source_inter_2

Enter the passphrase:
Confirm the passphrase:
Notice: Now use the same passphrase in the "cluster peer create" command in the
 other cluster.
```

2. 다음으로, 소스 클러스터에서 클러스터 피어 관계를 설정합니다. 인증을 위해 앞서 생성한 암호를 입력해야 합니다. 2세대 Single-AZ 파일 시스템의 경우 각 클러스터 간 IP 주소를 제공해야 합니다.

```
OnPrem-Source::> cluster peer create -address-family ipv4 -peer-
addrs dest_inter_1,dest_inter_2

Enter the passphrase:
Confirm the passphrase:
```

3. 소스 클러스터에서 다음 명령을 사용하여 피어링이 성공했는지 확인합니다. 출력에서 `Availability`를 `Available`로 설정해야 합니다.

```
OnPrem-Source::> cluster peer show

Peer Cluster Name  Availability   Authentication
-----------------  -------------- --------------
FSx-Dest           Available      ok
```

SVM 피어링 관계 생성

클러스터 피어링이 설정되면 다음 단계는 SVM을 피어링하는 것입니다. `vserver peer` 명령을 사용하여 대상 클러스터(FSx-Dest)에서 SVM 피어링 관계를 생성합니다. 다음 명령에 사용되는 추가 별칭은 다음과 같습니다.

- `DestLocalName` – 소스 SVM에서 SVM 피어링을 구성할 때 대상 SVM을 식별하는 데 사용되는 이름입니다.
- `SourceLocalName` – 대상 SVM에서 SVM 피어링을 구성할 때 소스 SVM을 식별하는 데 사용되는 이름입니다.

1. 다음 명령을 사용하여 소스 SVM과 대상 SVM 간에 SVM 피어링 관계를 생성합니다.

```
FSx-Dest::> vserver peer create -vserver DestSVM -peer-vserver SourceSVM -peer-
cluster OnPrem-Source -applications snapmirror -local-name SourceLocalName

 Info: [Job 207] 'vserver peer create' job queued
```

2. 다음과 같이 소스 클러스터에서 피어링 관계를 수락합니다.

```
OnPrem-Source::> vserver peer accept -vserver SourceSVM -peer-vserver DestSVM -
local-name DestLocalName

 Info: [Job 211] 'vserver peer accept' job queued
```

3. 다음 명령을 사용하여 SVM 피어링 상태를 확인합니다. `Peer State`는 응답에서 `peered`로 설정해야 합니다.

```
OnPrem-Source::> vserver peer show
```

```
        Peer     Peer   Peer     Peering       Remote
Vserver Vserver  State  Cluster  Applications  Vserver
------- -------- ------ -------- ------------- ---------
svm01   destsvm1 peered FSx-Dest snapmirror    svm01
```

SnapMirror 관계 생성

소스 SVM 및 대상 SVM을 피어링했으므로 다음 단계는 대상 클러스터에서 SnapMirror 관계를 생성하고 초기화하는 것입니다.

> **Note**
>
> SnapMirror 관계를 생성하고 초기화하면 관계가 끊어질 때까지 대상 볼륨은 읽기 전용 상태가 됩니다.

- `snapmirror create` 명령을 사용하여 대상 클러스터에 SnapMirror 관계를 생성합니다. `snapmirror create` 명령은 대상 SVM에서 사용해야 합니다.

  선택적으로 SnapMirror 관계에 최대 대역폭(KB/s)을 설정하기 위해 `-throttle`을 사용할 수 있습니다.

```
FSx-Dest::> snapmirror create -source-path SourceLocalName:vol1 -destination-
path DestSVM:vol1 -vserver DestSVM -throttle unlimited

 Operation succeeded: snapmirror create for the relationship with destination
 "DestSVM:vol1".
```

FSx for ONTAP 파일 시스템으로 데이터 전송

이제 SnapMirror 관계를 생성했으므로 대상 파일 시스템으로 데이터를 전송할 수 있습니다.

1. 대상 파일 시스템에서 다음 명령을 실행하여 대상 파일 시스템으로 데이터를 전송할 수 있습니다.

   > **Note**
   >
   > 이 명령을 실행하면 SnapMirror가 소스 볼륨에서 대상 볼륨으로 데이터 스냅샷을 전송하기 시작합니다.

```
FSx-Dest::> snapmirror initialize -destination-path DestSVM:vol1 -source-
path SourceLocalName:vol1
```

2. 현재 사용 중인 데이터를 마이그레이션하는 경우 대상 클러스터를 업데이트하여 소스 클러스터와 동기화된 상태를 유지해야 합니다. 대상 클러스터를 일회성으로 업데이트하려면 다음 명령을 실행합니다.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

3. 마이그레이션을 완료하고 클라이언트를 FSx for ONTAP으로 이동하기 전에 시간별 또는 일별 업데이트를 예약할 수도 있습니다. `snapmirror modify` 명령을 사용하여 SnapMirror 업데이트 일정을 설정할 수 있습니다.

```
FSx-Dest::> snapmirror modify -destination-path DestSVM:vol1 -schedule hourly
```

Amazon FSx로 전환

FSx for ONTAP 파일 시스템으로 전환을 준비하기 위해 다음을 수행합니다.

- 소스 클러스터에 쓰는 모든 클라이언트를 연결 해제합니다.
- 전환 시 데이터 손실이 없도록 최종 SnapMirror 전송을 수행합니다.
- SnapMirror 관계를 끊습니다.
- FSx for ONTAP 파일 시스템에 모든 클라이언트를 연결합니다.

1. 소스 클러스터의 모든 데이터가 FSx for ONTAP 파일 시스템으로 전송되도록 하려면 최종 Snapmirror 전송을 수행합니다.

```
FSx-Dest::> snapmirror update -destination-path DestSVM:vol1
```

2. `Mirror State`가 `Snapmirrored`로, `Relationship Status`가 `Idle`로 설정되어 있는지 확인하여 데이터 마이그레이션이 완료되었는지 확인합니다. 또한 대상 볼륨으로의 마지막 전송이 발생한 시간을 보여주는 `Last Transfer End Timestamp` 날짜가 예상과 같은지 확인해야 합니다.
3. 다음 명령을 실행하여 SnapMirror 상태를 표시합니다.

```
FSx-Dest::> snapmirror show -fields state,status,last-transfer-end-timestamp

Source     Destination   Mirror        Relationship Last Transfer End
Path       Path          State         Status       Timestamp
---------- -----------   ----------    -------      ---------------
Svm01:vol1 svm02:DestVol Snapmirrored  Idle         09/02 09:02:21
```

4. `snapmirror quiesce` 명령을 사용하여 향후 SnapMirror 전송을 비활성화합니다.

```
FSx-Dest::> snapmirror quiesce -destination-path DestSVM:vol1
```

5. `snapmirror show`를 사용하여 `Relationship Status`가 `Quiesced`로 변경되었는지 확인합니다.

```
FSx-Dest::> snapmirror show

Source            Destination   Mirror        Relationship
Path              Path          State         Status
-----------       ------------  ------------- --------
sourcesvm1:vol1   svm01:DestVol Snapmirrored  Quiesced
```

6. 마이그레이션 중에는 대상 볼륨이 읽기 전용입니다. 읽기/쓰기를 활성화하려면 SnapMirror 관계를 끊고 FSx for ONTAP 파일 시스템으로 전환해야 합니다. 다음 명령을 사용하여 SnapMirror 관계를 끊습니다.

```
FSx-Dest::> snapmirror break -destination-path DestSVM:vol1

Operation succeeded: snapmirror break for destination "DestSVM:vol1".
```

7. SnapMirror 복제가 완료되고 SnapMirror 관계가 끊어지면 볼륨을 마운트하여 데이터를 사용할 수 있도록 할 수 있습니다.

```
FSx-Dest::> vol mount -vserver fsx -volume vol1 -junction-path /vol1
```

이제 소스 볼륨의 데이터가 대상 볼륨으로 완전히 마이그레이션된 상태에서 볼륨을 사용할 수 있습니다. 볼륨에 대해 클라이언트가 읽고 쓸 수도 있습니다. 이전에 이 볼륨의 `tiering-policy`를 `all`로 설정한 경우 `auto` 또는 `snapshot-only`로 변경할 수 있으며 액세스 패턴에 따라 스토리지 계층 간에 데이터가 자동으로 전환됩니다. 클라이언트와 애플리케이션에서 이 데이터에 액세스할 수 있도록 하려면 FSx for ONTAP 데이터 액세스 섹션을 참조하세요.

AWS DataSync를 사용하여 FSx for ONTAP으로 마이그레이션

AWS DataSync 를 사용하여 FSx for ONTAP 파일 시스템과 FSx for Lustre, FSx for OpenZFS, FSx FSx for Windows File Server, Amazon EFS, Amazon S3 및 온프레미스 파일러를 포함한 비 ONTAP 파일 시스템 간에 데이터를 전송하는 것이 좋습니다. FSx for ONTAP과 NetApp ONTAP 간에 파일을 전송하는 경우 NetApp SnapMirror를 사용하는 것이 좋습니다. AWS DataSync 는 인터넷 또는를 통해 자체 관리형 스토리지 시스템과 AWS 스토리지 서비스 간의 데이터 이동 및 복제를 간소화, 자동화 및 가속화하는 데이터 전송 서비스입니다 AWS Direct Connect. DataSync는 소유권, 타임스탬프, 액세스 권한과 같은 파일 시스템 데이터 및 메타데이터를 전송할 수 있습니다.

DataSync를 사용하여 두 FSx for ONTAP 파일 시스템 간에 파일을 전송하고 데이터를 다른 AWS 리전 또는 AWS 계정의 파일 시스템으로 이동할 수도 있습니다. FSx for ONTAP 파일 시스템들과의 DataSync를 다른 작업에 사용할 수도 있습니다. 예를 들어, 일회성 데이터 마이그레이션을 수행하고, 분산 워크로드를 위해 주기적으로 데이터를 수집하며, 복제를 예약하여 데이터를 보호 및 복구할 수 있습니다.

DataSync에서 위치는 FSx for ONTAP 파일 시스템의 엔드포인트입니다. 특정 전송 시나리오에 대한 자세한 내용은 AWS DataSync 사용 설명서의 위치 작업 섹션을 참조하세요.

> **Note**
>
> `All` 계층화 정책을 사용하여 데이터를 용량 풀 계층으로 마이그레이션하려는 경우 파일 메타데이터는 항상 SSD 계층에 저장되며 모든 새 사용자 데이터는 먼저 SSD 계층에 기록된다는 점에 유념하세요. 데이터가 SSD 계층에 기록되면 백그라운드 계층화 프로세스가 데이터를 용량 풀 스토리지 계층으로 이동하기 시작하지만 계층화 프로세스는 즉시 이루어지지 않으며 네트워크 리소스를 사용합니다. 사용자 데이터를 용량 풀 스토리지 계층으로 이동하기 전에 사용자 데이터를 위한 버퍼로서 파일 메타데이터(사용자 데이터 크기의 3%~7%)를 고려하여 SSD 계층 크기를 조정해야 합니다. SSD 사용률은 80% 를 초과하지 않는 것이 좋습니다.
> 데이터를 마이그레이션하는 동안 CloudWatch 파일 시스템 지표를 사용하여 SSD 계층을 모니터링하여 계층화 프로세스가 데이터를 용량 풀 스토리지로 이동할 수 있는 것보다 더 빠르게 채워지지 않는지 확인합니다. 또한 DataSync 전송을 계층화 속도보다 낮은 속도로 조절하여 SSD 계층 사용률이 80% 를 초과하지 않도록 할 수 있습니다. 예를 들어 처리량 용량이 512MBps 이상인 파일 시스템의 경우 일반적으로 200MBps 제한은 데이터 전송 속도와 데이터 계층화 속도의 균형을 맞춥니다.

사전 조건

FSx for ONTAP 설정으로 데이터를 마이그레이션하려면 서버와 네트워크가 DataSync 요구 사항을 충족해야 합니다. 자세히 알아보려면 AWS DataSync 사용 설명서의 DataSync 요구 사항을 참조하세요.

DataSync를 사용하여 파일을 마이그레이션하는 기본 단계

DataSync를 사용하여 소스에서 대상으로 파일을 전송하는 기본 단계는 다음과 같습니다.

- 환경에 에이전트를 다운로드하여 배포하고 활성화합니다(호출하는 경우 필요하지 않음 AWS 서비스).
- 소스 및 대상 위치 생성.
- 작업 생성.
- 작업을 실행하여 소스에서 대상으로 파일 전송.

자세한 내용은 AWS DataSync 사용 설명서에서 다음 주제를 참조하세요.

- 자체 관리형 스토리지와 간의 데이터 전송 AWS
- Amazon FSx for NetApp ONTAP을 위한 위치 생성

Amazon FSx for NetApp ONTAP의 보안

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다 AWS 클라우드. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. Amazon FSx for NetApp ONTAP에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 AWS 프로그램 제공 범위 내 서비스규정 준수 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 사용자는 데이터의 민감도, 회사 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Amazon FSx를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Amazon FSx를 구성하는 방법을 보여줍니다. 또한 Amazon FSx 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- Amazon FSx for NetApp ONTAP의 데이터 보호
- Amazon FSx for NetApp ONTAP의 ID 및 액세스 관리
- AWS Amazon FSx for OpenZFS에 대한 관리형 정책
- Amazon VPC를 사용한 파일 시스템 액세스 제어
- Amazon FSx for NetApp ONTAP에 대한 규정 준수 확인
- Amazon FSx for NetApp ONTAP 및 인터페이스 VPC 엔드포인트(AWS PrivateLink)
- Amazon FSx for NetApp ONTAP의 복원력
- Amazon FSx for NetApp ONTAP의 인프라 보안
- FSx for ONTAP과 함께 NetApp ONTAP Vscan 사용
- ONTAP 사용자 및 역할

Amazon FSx for NetApp ONTAP의 데이터 보호

AWS 공동 책임 모델 Amazon FSx for NetApp ONTAP의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Amazon FSx 또는 기타 AWS 서비스 에서 콘솔, API AWS CLI또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 보안 인증 정보를 URL에 포함시켜서는 안 됩니다.

FSx for ONTAP의 데이터 암호화

Amazon FSx for NetApp ONTAP은 저장 데이터의 암호화와 전송 중 데이터의 암호화를 지원합니다. Amazon FSx 파일 시스템을 생성할 때 저장 데이터 암호화가 자동으로 활성화됩니다. Amazon FSx for NetApp ONTAP은 Active Directory 또는 Lightweight Directory Access Protocol(LDAP)을 사용하는 도메인에 조인된 스토리지 가상 머신(SVM)의 데이터에 액세스하는 경우 NFS 및 SMB 프로토콜을 통한 Kerberos 기반 전송 중 암호화를 지원합니다.

암호화를 사용해야 하는 경우

저장 데이터 및 저장 메타데이터의 암호화를 요구하는 기업 또는 규제 정책이 조직에 적용되는 경우 저장 데이터는 자동으로 암호화됩니다. 또한 전송 중 데이터 암호화를 사용해 파일 시스템을 마운트하여 전송 중 데이터 암호화를 활성화하는 것이 좋습니다.

Amazon FSx for NetApp ONTAP를 사용한 데이터 암호화에 대한 자세한 내용은 저장 데이터의 암호화 및 전송 중 데이터 암호화을 참조하세요.

저장 데이터의 암호화

모든 Amazon FSx for NetApp ONTAP 파일 시스템 및 백업은 ()를 사용하여 AWS Key Management Service 관리되는 키로 저장 시 암호화됩니다AWS KMS. 데이터는 파일 시스템에 기록되기 전에 자동으로 암호화되고 읽기 중에 자동으로 복호화됩니다. 모든 백업은 생성 시 자동으로 암호화되며 백업이 새 볼륨으로 복원될 때 자동으로 해독됩니다. Amazon FSx는 해당 프로세스를 투명하게 처리하기 때문에 애플리케이션을 수정할 필요가 없습니다.

Amazon FSx는 유휴 Amazon FSx 데이터 및 메타데이터 암호화에 업계 표준인 AES-256 암호화 알고리즘을 사용합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 암호화 기초를 참조하세요.

> **Note**
>
> AWS 키 관리 인프라는 FIPS(Federal Information Processing Standards) 140-2 승인 암호화 알고리즘을 사용합니다. 이 인프라는 미국 국립 표준 기술 연구소(NIST) 800-57 표준의 권장 사항에 부합됩니다.

Amazon FSx의 사용 방식 AWS KMS

Amazon FSx는 키 관리를 AWS KMS 위해와 통합됩니다. Amazon FSx는 KMS 키를 사용하여 파일 시스템 및 볼륨 백업을 암호화합니다. 파일 시스템 및 볼륨 백업(데이터 및 메타데이터 모두)을 암호화하

고 해독하는 데 사용되는 KMS 키를 선택합니다. KMS 키에 대한 권한을 활성화, 비활성화, 취소할 수 있습니다. KMS 키는 다음 두 가지 유형 중 하나가 될 수 있습니다.

- AWS관리형 KMS 키 – 기본 KMS 키이며, 무료로 사용할 수 있습니다.
- 고객 관리형 KMS 키 – 여러 사용자나 서비스에 대한 키 정책 및 권한을 구성할 수 있는 가장 유연한 KMS 키입니다. KMS 키 생성에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 생성을 참조하세요.

> **Important**
>
> Amazon FSx는 대칭 암호화 KMS 키만 승인합니다. Amazon FSx에서는 비대칭 KMS 키를 사용할 수 없습니다.

고객 관리형 KMS 키를 데이터 암호화 및 복호화의 KMS 키로 사용하면 키 교체를 활성화할 수 있습니다. 키 교체를 활성화하면 AWS KMS 가 매년 1회 키를 자동 교체합니다. 또한 고객 관리형 KMS 키를 사용하면 언제든지 KMS 키에 대한 액세스를 비활성화, 재활성화, 삭제, 취소하는 시기를 선택할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS KMS keys교체 및 키 활성화 및 비활성화를 참조하세요.

에 대한 Amazon FSx 키 정책 AWS KMS

키 정책은 KMS 키에 대한 액세스를 제어하는 기본 방법입니다. 키 정책에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS KMS의 키 정책 사용을 참조하세요. 다음 목록은 유휴 시 암호화된 파일 시스템 및 백업에 대해 Amazon FSx에서 지원하는 모든 AWS KMS관련 권한을 설명합니다.

- kms:Encrypt – (선택 사항) 일반 텍스트를 사이퍼텍스트로 암호화합니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms:Decrypt – (필수 사항) 사이퍼텍스트를 복호화합니다. 사이퍼텍스트는 이전에 암호화한 일반 텍스트입니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms:ReEncrypt – (선택 사항) 클라이언트 측 데이터의 일반 텍스트를 노출 AWS KMS key하지 않고 새 로 서버 측의 데이터를 암호화합니다. 먼저 데이터를 복호화한 후 다시 암호화합니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms:GenerateDataKeyWithoutPlaintext – (필수 사항) KMS 키로 암호화된 데이터 암호화 키를 반환합니다. 이 권한은 kms:GenerateDataKey* 아래 기본 키 정책에 포함되어 있습니다.

- kms:CreateGrant – (필수 사항)특정 조건 하에 키를 사용할 수 있는 사람을 지정할 수 있도록 키에 권한을 추가합니다. 이런 권한 부여는 키 정책을 대체하는 권한 메커니즘입니다. 권한 부여에 대한 자세한 내용은AWS Key Management Service 개발자 안내서의 권한 부여 사용을 참조하세요. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms:DescribeKey – (필수 사항) 지정한 KMS 키에 대한 세부 정보를 제공합니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms:ListAliases – (선택 사항) 계정의 모든 키 별칭을 나열합니다. 콘솔을 사용해 암호화된 파일 시스템을 생성하는 경우, 이 권한이 KMS 키 목록을 채웁니다. 최상의 사용자 경험을 제공하기 위해 이 권한을 사용하는 것이 좋습니다. 이 권한은 기본 키 정책에 포함되어 있습니다.

전송 중 데이터 암호화

이 항목에서는 파일 데이터가 FSx for ONTAP 파일 시스템과 연결된 클라이언트 간에 전송되는 동안 파일 데이터를 암호화하는 데 사용할 수 있는 다양한 옵션에 대해 설명합니다. 또한 워크플로에 가장 적합한 암호화 방법을 선택하는 데 도움이 되는 지침도 제공합니다.

AWS 글로벌 네트워크를 AWS 리전 통해 흐르는 모든 데이터는 AWS 보안 시설을 떠나기 전에 물리적 계층에서 자동으로 암호화됩니다. 가용 영역 간 트래픽은 모두 암호화됩니다. 이 섹션에 나열된 암호화 계층을 비롯한 추가 암호화 계층은 추가적인 보호 기능을 제공할 수 있습니다. 에서 사용 AWS 리전가능한 영역 및 인스턴스 간 데이터 흐름에 대한 보호를 AWS 제공하는 방법에 대한 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 전송 중 암호화를 참조하세요.

Amazon FSx for NetApp ONTAP은 FSx for ONTAP 파일 시스템 및 연결된 클라이언트 간에 전송 중 데이터를 암호화하기 위해 다음과 같은 방법을 지원합니다.

- 지원되는 Amazon EC2 Linux 및 Windows 인스턴스 유형에서 실행되는 지원되는 모든 프로토콜 및 클라이언트에 대한 자동 Nitro 기반 암호화.
- NFS 및 SMB 프로토콜을 통한 Kerberos 기반 암호화.
- NFS, iSCSI, SMB 프로토콜을 통한 IPsec 기반 암호화

전송 중 데이터를 암호화하는 데 지원되는 모든 방법은 엔터프라이즈 수준의 암호화를 제공하는 업계 표준 AES-256 암호화 알고리즘을 사용합니다.

주제

- 전송 중 데이터를 암호화하기 위한 방법 선택
- AWS Nitro System을 사용하여 전송 중 데이터 암호화

- Kerberos 기반 암호화를 사용하여 전송 중 데이터 암호화
- IPsec 암호화로 전송 중 데이터 암호화
- 전송 중인 데이터의 SMB 암호화 활성화
- PSK 인증을 사용하여 IPsec 구성
- 인증서 인증을 사용하여 IPsec 구성

전송 중 데이터를 암호화하기 위한 방법 선택

이 섹션에서는 지원되는 전송 중 암호화 방법 중 해당 워크플로에 가장 적합한 방법을 결정하는 데 도움이 되는 정보를 제공합니다. 이후의 섹션에 자세히 설명된 지원 옵션을 살펴보면서 이 섹션을 다시 참조하세요.

FSx for ONTAP 파일 시스템 및 연결된 클라이언트 간에 전송 중 데이터를 암호화하는 방법을 선택할 때는 몇 가지 요소를 고려해야 합니다. 이러한 요소에는 다음이 포함됩니다.

- FSx for ONTAP 파일 시스템이 실행 중인 AWS 리전 입니다.
- 클라이언트가 실행되는 인스턴스 유형.
- 파일 시스템에 액세스하는 클라이언트의 위치.
- 네트워크 성능 요구 사항.
- 암호화하려는 데이터 프로토콜.
- Microsoft Active Directory를 사용 중인 경우.

AWS 리전

AWS 리전 파일 시스템이 실행 중인에 따라 Amazon Nitro 기반 암호화를 사용할 수 있는지 여부가 결정됩니다. 자세한 내용은 AWS Nitro System을 사용하여 전송 중 데이터 암호화 단원을 참조하십시오.

클라이언트 인스턴스 유형

파일 시스템에 액세스하는 클라이언트가 지원되는 Amazon EC2 Mac, Linux 또는 Windows 인스턴스 유형에서 실행 중이고 워크플로가 Nitro 기반 암호화를 사용하기 위한 기타 모든 요구 사항을 충족하는 경우 Amazon Nitro 기반 암호화를 사용할 수 있습니다. Kerberos 또는 IPsec 암호화를 사용하기 위한 클라이언트 인스턴스 유형 요구 사항은 없습니다.

클라이언트 위치

파일 시스템 위치와 관련하여 데이터에 액세스하는 클라이언트의 위치는 사용할 수 있는 전송 중 암호화 방법에 영향을 줍니다. 클라이언트와 파일 시스템이 동일한 VPC에 있는 경우 지원되는 모든 암호화 방법을 사용할 수 있습니다. 트래픽이 전송 게이트웨이 같은 가상 네트워크 디바이스 또는 서비스를 통과하지 않는 한, 클라이언트 및 파일 시스템이 피어링된 VPC에 있는 경우에도 마찬가지입니다. 클라이언트가 동일하거나 피어링된 VPC에 있지 않거나 트래픽이 가상 네트워크 디바이스 또는 서비스를 통과하는 경우에는 Nitro 기반 암호화를 사용할 수 없습니다.

네트워크 성능

Amazon Nitro 기반 암호화를 사용해도 네트워크 성능에는 영향을 미치지 않습니다. 이는 지원되는 Amazon EC2 인스턴스가 기본 Nitro 시스템 하드웨어의 오프로드 기능을 활용하여 인스턴스 간 전송 중 트래픽을 자동으로 암호화하기 때문입니다.

Kerberos 또는 IPsec 암호화를 사용하면 네트워크 성능에 영향을 미칩니다. 이는 두 암호화 방법 모두 소프트웨어 기반이므로 클라이언트와 서버가 컴퓨팅 리소스를 사용하여 전송 중인 트래픽을 암호화 및 복호화해야 하기 때문입니다.

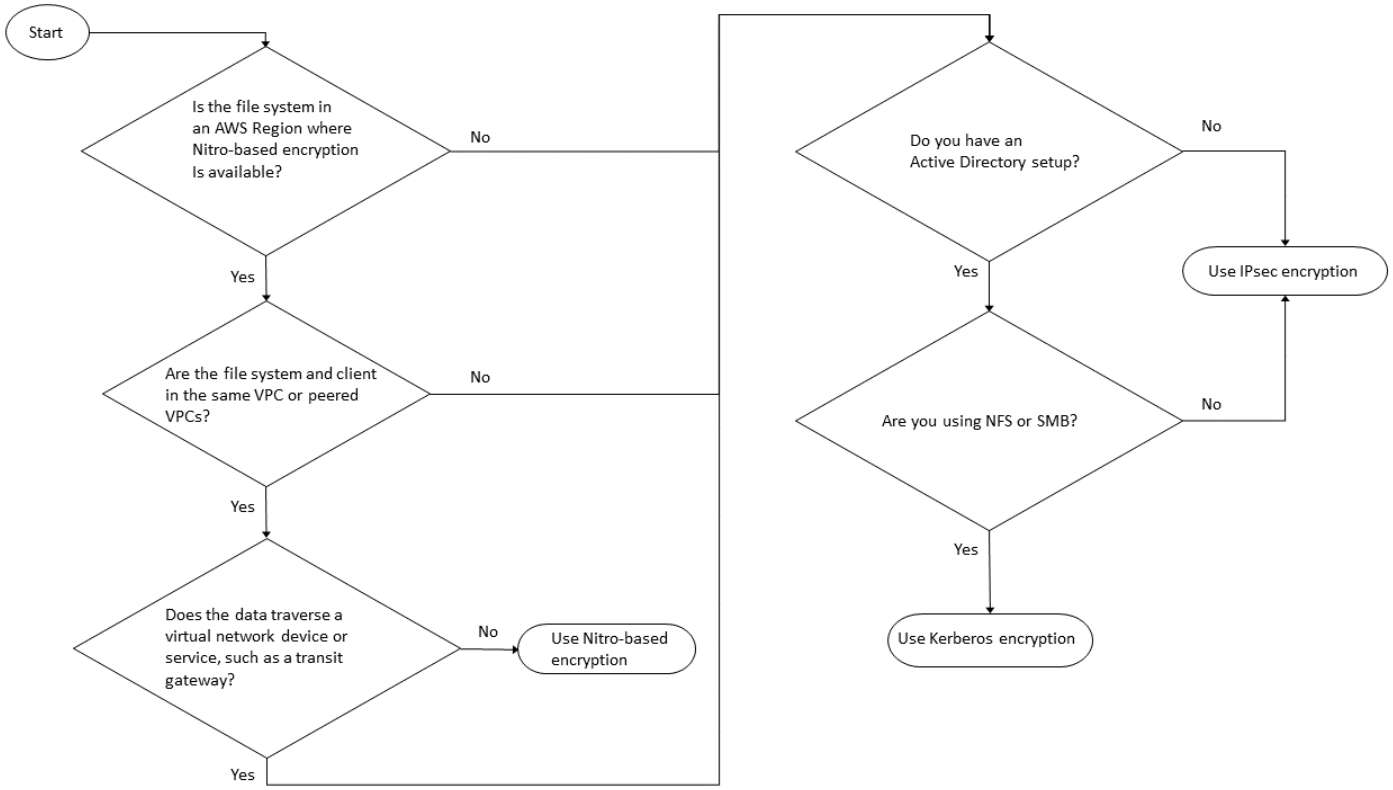
데이터 프로토콜

지원되는 모든 프로토콜(NFS, SMB, iSCSI)에서 Amazon Nitro 기반 암호화 및 IPsec 암호화를 사용할 수 있습니다. (Active Directory를 사용하는 경우) NFS 및 SMB 프로토콜을 통해 Kerberos 암호화를 사용할 수 있습니다.

Active Directory

Microsoft Kerberos Active Directory를 사용하는 경우 NFS 및 SMB 프로토콜을 통해 Kerberos 암호화를 사용할 수 있습니다.

다음 다이어그램을 통해 사용할 전송 중 암호화 방법을 쉽게 결정할 수 있습니다.



IPsec 암호화는 워크플로에 다음 조건이 모두 적용되는 경우 사용할 수 있는 유일한 옵션입니다.

- NFS, SMB 또는 iSCSI 프로토콜을 사용하고 있습니다.
- 워크플로에서 Amazon Nitro 기반 암호화 사용을 지원하지 않습니다.
- Microsoft Active Directory 도메인을 사용하고 있지 않습니다.

AWS Nitro System을 사용하여 전송 중 데이터 암호화

Nitro 기반 암호화를 사용하면 파일 시스템에 액세스하는 클라이언트가 FSx for ONTAP에서 사용할 수 AWS 리전 있는의 지원되는 Amazon EC2 Linux 또는 Windows 인스턴스 유형에서 실행될 때 전송 중 데이터가 자동으로 암호화됩니다.

Amazon Nitro 기반 암호화를 사용해도 네트워크 성능에는 영향을 미치지 않습니다. 이는 지원되는 Amazon EC2 인스턴스가 기본 Nitro 시스템 하드웨어의 오프로드 기능을 활용하여 인스턴스 간 전송 중 트래픽을 자동으로 암호화하기 때문입니다.

지원되는 클라이언트 인스턴스 유형이 동일한 AWS 리전 및 동일한 VPC에 있거나 파일 시스템의 VPC와 피어링된 VPC에 있는 경우 Nitro 기반 암호화가 자동으로 활성화됩니다. 또한 클라이언트가 피어링된 VPC에 있는 경우 Nitro 기반 암호화가 자동으로 활성화되기 위해 데이터가 가상 네트워크 디바이

스 또는 서비스(예: 전송 게이트웨이)를 통과할 수 없습니다. Nitro 기반 암호화에 대한 자세한 내용은 Linux 또는 Windows 인스턴스 유형의 Amazon EC2 사용 설명서에 있는 전송 중 암호화를 참조하세요.

다음 표에서는 Nitro 기반 암호화를 사용할 수 AWS 리전 있는에 대해 자세히 설명합니다.

Nitro 기반 암호화 지원

생성	배포 유형	AWS 리전
1세대 파일 시스템[1]	Single-AZ 1 Multi-AZ 1	미국 동부(버지니아 북부), 미국 동부(오하이오), 미국 서부(오리건), 유럽(아일랜드)
2세대 파일 시스템	Single-AZ 2 Multi-AZ 2	미국 동부(버지니아 북부), 미국 동부(오하이오), 미국 서부(캘리포니아 북부), 미국 서부(오리건), 유럽(프랑크푸르트), 유럽(아일랜드), 아시아 태평양(시드니)

[1] 2022년 11월 28일 이후에 생성된 1세대 파일 시스템은 나열된 AWS 리전에서 Nitro 기반 전송 중 암호화를 지원합니다.

FSx for ONTAP을 사용할 수 AWS 리전 있는에 대한 자세한 내용은 Amazon FSx for NetApp ONTAP 요금을 참조하세요.

FSx for ONTAP 파일 시스템의 성능 사양에 대한 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

Kerberos 기반 암호화를 사용하여 전송 중 데이터 암호화

Microsoft Active Directory를 사용하는 경우, NFS 및 SMB 프로토콜을 통해 Kerberos 기반 암호화를 사용하여 Microsoft Active Directory에 조인된 SVM의 하위 볼륨에 대해 전송 중인 데이터를 암호화할 수 있습니다.

Kerberos를 사용하여 NFS를 통해 전송 중 데이터 암호화

Kerberos를 사용한 전송 중 데이터의 암호화는 NFSv3 및 NFSv4 프로토콜에서 지원됩니다. NFS 프로토콜에 Kerberos를 사용하여 전송 중 암호화를 활성화하려면 NetApp ONTAP 설명서 센터에서 NFS와 함께 Kerberos 사용을 통한 보안 강화를 참조하세요.

Kerberos를 사용하여 SMB를 통해 전송 중 데이터 암호화

SMB 프로토콜을 통한 전송 중 데이터의 암호화는 SMB 프로토콜 3.0 이상을 지원하는 컴퓨팅 인스턴스에 매핑된 파일 공유에서 지원됩니다. 여기에는 Microsoft Windows Server 2012 이상 버전과 Microsoft Windows 8 이상 버전의 모든 Microsoft Windows 버전이 포함됩니다. 활성화된 경우 FSx for ONTAP은 애플리케이션을 수정할 필요 없이 파일 시스템에 액세스할 때 SMB 암호화를 사용하여 전송 중 데이터를 자동으로 암호화합니다.

FSx for ONTAP SMB는 클라이언트 세션 요청에 따라 결정되는 128비트 및 256비트 암호화를 지원합니다. 다양한 암호화 수준에 대한 설명은 NetApp ONTAP 설명서 센터의 CLI로 SMB 관리의 SMB 서버 최소 인증 보안 수준 설정 섹션을 참조하세요.

> **Note**
>
> 클라이언트가 암호화 알고리즘을 결정합니다. NTLM 인증과 Kerberos 인증 모두 128비트 및 256비트 암호화로 작동합니다. FSx for ONTAP SMB 서버는 모든 표준 Windows 클라이언트 요청을 수락하며 Microsoft 그룹 정책 또는 레지스트리 설정을 통해 세분화된 제어를 처리합니다.

ONTAP CLI를 사용하여 FSx for ONTAP SVM 및 볼륨에 대한 전송 중 암호화 설정을 관리합니다. NetApp ONTAP CLI에 액세스하려면 ONTAP CLI로 SVM 관리하기에 설명된 대로 전송 중 암호화 설정을 수행하는 SVM에 SSH 세션을 설정합니다.

SVM 또는 볼륨에서 SMB 암호화를 활성화하는 방법에 대한 지침은 전송 중인 데이터의 SMB 암호화 활성화을 참조하세요.

IPsec 암호화로 전송 중 데이터 암호화

FSx for ONTAP은 전송 모드에서 IPsec 프로토콜을 사용하여 전송 중에 데이터를 지속적으로 보호하고 암호화할 수 있도록 지원합니다. IPsec은 지원되는 모든 IP 트래픽(NFS, iSCSI, SMB 프로토콜)에 대해 클라이언트와 FSx for ONTAP 파일 시스템 간의 전송 중 데이터에 대한 엔드 투 엔드 암호화를 제공합니다. IPsec 암호화를 사용하면 IPsec을 활성화하도록 구성된 FSx for ONTAP과, 데이터에 액세스하는 연결된 클라이언트에서 실행되는 IPsec 클라이언트 간에 IPsec 터널을 설정합니다.

Nitro 기반 암호화를 지원하지 않는 클라이언트에서 데이터에 액세스할 때, 그리고 클라이언트와 SVM이 Kerberos 기반 암호화에 필요한 Active Directory에 조인되어 있지 않은 경우 IPsec을 사용하여 NFS, SMB, iSCSI 프로토콜을 통해 전송 중 데이터를 암호화하는 것이 좋습니다. IPsec 암호화는 iSCSI 클라이언트가 Nitro 기반 암호화를 지원하지 않는 경우 iSCSI 트래픽을 위해 전송 중 데이터를 암호화하는 데 사용할 수 있는 유일한 옵션입니다.

IPsec 인증의 경우 사전 공유 키(PSK) 또는 인증서를 사용할 수 있습니다. PSK를 사용하는 경우 사용하는 IPsec 클라이언트는 PSK를 사용하여 인터넷 키 교환 버전 2(IKEv2)를 지원해야 합니다. FSx for ONTAP와 클라이언트 모두에서 IPsec 암호화를 구성하는 높은 수준의 단계는 다음과 같습니다.

1. 파일 시스템에서 IPsec 활성화 및 구성
2. 클라이언트에 IPsec 설치 및 구성
3. 다중 클라이언트 액세스를 위한 IPsec 구성

PSK를 사용하여 IPsec을 구성하는 방법에 대한 자세한 내용은 NetApp ONTAP 문서 센터에서 유선 암호화를 통한 IP 보안(IPsec) 구성을 참조하세요.

인증서를 사용하여 IPsec을 구성하는 방법에 대한 자세한 내용은 인증서 인증을 사용하여 IPsec 구성를 참조하세요.

전송 중인 데이터의 SMB 암호화 활성화

기본적으로 SVM을 생성하면 SMB 암호화가 해제됩니다. 개별 공유에 필요한 SMB 암호화를 활성화하거나 SVM에서 활성화하여 해당 SVM의 모든 공유에 대해 SMB 암호화를 활성화할 수 있습니다.

> **Note**
>
> SVM 또는 공유에 필요한 SMB 암호화가 활성화된 경우 암호화를 지원하지 않는 SMB 클라이언트는 해당 SVM 또는 공유에 연결할 수 없습니다.

SVM에서 수신되는 SMB 트래픽에 SMB 암호화 요구

NetApp ONTAP CLI를 사용하여 SVM에서 SMB 암호화를 요구하려면 다음 절차를 사용합니다.

1. SSH를 사용하여 SVM 관리 엔드포인트에 연결하려면 SVM을 생성할 때 설정한 사용자 이름 `vsadmin` 및 vsadmin 암호를 사용합니다. vsadmin 암호를 설정하지 않은 경우 사용자 이름 `fsxadmin` 및 fsxadmin 암호를 사용합니다. 관리 엔드포인트 IP 주소 또는 DNS 이름을 사용하여 파일 시스템과 동일한 VPC에 있는 클라이언트에서 SVM으로 SSH를 설정할 수 있습니다.

   ```
   ssh vsadmin@svm-management-endpoint-ip-address
   ```

   샘플 값이 있는 명령:

```
ssh vsadmin@198.51.100.10
```

관리 엔드포인트 DNS 이름을 사용하는 SSH 명령:

```
ssh vsadmin@svm-management-endpoint-dns-name
```

샘플 DNS 이름을 사용하는 SSH 명령:

```
ssh vsadmin@management.svm-abcdef01234567892fs-08fc3405e03933af0.fsx.us-
east-2.aws.com
```

```
Password: vsadmin-password

This is your first recorded login.
FsxIdabcdef01234567892::>
```

2. 다음 vserver cifs security modify NetApp ONTAP CLI 명령을 사용하여 SVM으로 수신되는 SMB 트래픽에 대해 SMB 암호화를 요구합니다.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required true
```

3. 수신되는 SMB 트래픽에 대해 SMB 암호화를 요구하지 않으려면 다음 명령을 사용합니다.

```
vserver cifs security modify -vserver vserver_name -is-smb-encryption-required
 false
```

4. SVM의 현재 `is-smb-encryption-required` 설정을 보려면 다음 vserver cifs security show NetApp ONTAP CLI 명령을 사용합니다.

```
vserver cifs security show -vserver vs1 -fields is-smb-encryption-required

vserver  is-smb-encryption-required
-------- -------------------------
vs1      true
```

SVM에서 SMB 암호화를 관리하는 방법에 대한 자세한 내용은 NetApp ONTAP 설명서 센터의 SMB를 통한 데이터 전송을 위한 SMB 서버의 필수 SMB 암호화 구성을 참조하세요.

볼륨에서 SMB 암호화 활성화

NetApp ONTAP CLI를 사용하여 공유에서 SMB 암호화를 활성화하려면 다음 절차를 사용합니다.

1. ONTAP CLI로 SVM 관리하기에 설명된 대로 SVM의 관리 엔드포인트에 대한 Secure Shell(SSH) 연결을 설정합니다.
2. 다음 NetApp ONTAP CLI 명령을 사용하여 새 SMB 공유를 생성하고 이 공유에 액세스할 때 SMB 암호화를 요구합니다.

   ```
   vserver cifs share create -vserver vserver_name -share-name share_name -
   path share_path -share-properties encrypt-data
   ```

   자세한 내용은 NetApp ONTAP CLI 명령 매뉴얼 페이지에서 vserver cifs share create 섹션을 참조하세요.
3. 기존 SMB 공유에서 SMB 암호화를 요구하려면 다음 명령을 사용합니다.

   ```
   vserver cifs share properties add -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   자세한 내용은 NetApp ONTAP CLI 명령 매뉴얼 페이지에서 vserver cifs share create 섹션을 참조하세요.
4. 기존 SMB 공유에서 SMB 암호화를 해제하려면 다음 명령을 사용합니다.

   ```
   vserver cifs share properties remove -vserver vserver_name -share-name share_name -
   share-properties encrypt-data
   ```

   자세한 내용은 NetApp ONTAP CLI 명령 매뉴얼 페이지에서 vserver cifs share properties remove 섹션을 참조하세요.
5. SMB 공유의 현재 `is-smb-encryption-required` 설정을 보려면 다음 NetApp ONTAP CLI 명령을 사용합니다.

   ```
   vserver cifs share properties show -vserver vserver_name -share-name share_name -
   fields share-properties
   ```

   명령에서 반환된 속성 중 하나가 `encrypt-data` 속성인 경우 해당 속성은 이 공유에 액세스할 때 SMB 암호화를 사용해야 한다고 지정합니다.

자세한 내용은 NetApp ONTAP CLI 명령 매뉴얼 페이지에서 `vserver cifs share properties show` 섹션을 참조하세요.

PSK 인증을 사용하여 IPsec 구성

인증에 PSK를 사용하는 경우 FSx for ONTAP 및 클라이언트 모두에서 IPsec 암호화를 구성하는 단계는 다음과 같습니다.

1. 파일 시스템에서 IPsec 활성화 및 구성
2. 클라이언트에 IPsec 설치 및 구성
3. 다중 클라이언트 액세스를 위한 IPsec 구성

PSK를 사용하여 IPsec을 구성하는 방법에 대한 자세한 내용은 NetApp ONTAP 설명서 센터의 유선 암호화를 통한 IP 보안(IPsec) 구성을 참조하세요.

인증서 인증을 사용하여 IPsec 구성

다음 항목에서는 FSx for ONTAP 파일 시스템과 Libreswan IPsec을 실행하는 클라이언트에서 인증서 인증을 사용하여 IPsec 암호화를 구성하는 방법에 대해 설명합니다. 이 솔루션은 AWS Certificate Manager 및 AWS Private Certificate Authority 를 사용하여 프라이빗 인증 기관을 생성하고 인증서를 생성합니다.

FSx for ONTAP 파일 시스템 및 연결된 클라이언트에 대해 인증서 인증을 사용하여 IPsec 암호화를 구성하는 높은 수준의 단계는 다음과 같습니다.

1. 인증서 발급을 위한 인증 기관 준비
2. 파일 시스템 및 클라이언트용 CA 인증서 생성 및 내보내기
3. 클라이언트 인스턴스에 인증서 설치 및 IPsec 구성
4. 파일 시스템에 인증서 설치 및 IPsec 구성
5. 보안 정책 데이터베이스(SPD) 정의
6. 다중 클라이언트 액세스를 위한 IPsec 구성

CA 인증서 생성 및 설치

인증서 인증의 경우 FSx for ONTAP 파일 시스템과, 파일 시스템의 데이터에 액세스할 클라이언트에서 인증 기관의 인증서를 생성하고 설치해야 합니다. 다음 예제에서는 AWS Private Certificate Authority

를 사용하여 프라이빗 인증 기관을 설정하고 파일 시스템 및 클라이언트에 설치할 인증서를 생성합니다. 를 사용하면 조직의 내부 사용을 위해 루트 및 하위 인증 기관(CAs)의 완전히 AWS 호스팅된 계층 구조를 생성할 AWS Private Certificate Authority수 있습니다. 이 프로세스에는 다음의 다섯 단계가 있습니다.

1. 를 사용하여 사설 인증 기관(CA) 생성 AWS Private CA
2. 프라이빗 CA에 루트 인증서 발급 및 설치
3. 파일 시스템 및 클라이언트에 AWS Certificate Manager 대해에서 프라이빗 인증서 요청
4. 파일 시스템 및 클라이언트용 인증서를 내보냅니다.

자세한 내용은 AWS Private Certificate Authority 사용 설명서의 Private CA 관리를 참조하세요.

루트 프라이빗 CA 생성

1. CA를 생성할 때 제공하는 파일에 CA 구성을 지정해야 합니다. 다음 명령은 Nano 텍스트 편집기를 사용하여 다음 정보를 지정하는 `ca_config.txt` 파일을 생성합니다.

   - 알고리즘의 이름
   - CA가 서명하는 데 사용하는 서명 알고리즘
   - X.500 주체 정보

   ```
   $ > nano ca_config.txt
   ```

   텍스트 편집기가 표시됩니다.

2. CA 사양으로 파일을 편집합니다.

   ```
   {
      "KeyAlgorithm":"RSA_2048",
      "SigningAlgorithm":"SHA256WITHRSA",
      "Subject":{
         "Country":"US",
         "Organization":"Example Corp",
         "OrganizationalUnit":"Sales",
         "State":"WA",
         "Locality":"Seattle",
         "CommonName":"*.ec2.internal"
      }
   ```

```
}
```

3. 파일을 저장한 후 닫고 텍스트 편집기를 종료합니다. 자세한 내용은 AWS Private Certificate Authority 사용 설명서의 CA 생성 절차를 참조하세요.
4. create-certificate-authority AWS Private CA CLI 명령을 사용하여 프라이빗 CA를 생성합니다.

```
~/home > aws acm-pca create-certificate-authority \
     --certificate-authority-configuration file://ca_config.txt \
     --certificate-authority-type "ROOT" \
     --idempotency-token 01234567 --region aws-region
```

이 명령이 제대로 실행되면 CA의 Amazon 리소스 이름(ARN)을 출력합니다.

```
{
   "CertificateAuthorityArn": "arn:aws:acm-pca:aws-region:111122223333:certificate-
authority/12345678-1234-1234-1234-123456789012"
}
```

프라이빗 루트 CA에 대한 인증서 생성 및 설치(AWS CLI)

1. get-certificate-authority-csr AWS CLI 명령을 사용하여 인증서 서명 요청(CSR)을 생성합니다.

```
$ aws acm-pca get-certificate-authority-csr \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --output text \
     --endpoint https://acm-pca.aws-region.amazonaws.com \
     --region eu-west-1 > ca.csr
```

base64 형식으로 인코딩된 PEM 파일인 결과 파일 `ca.csr`은 다음과 같이 표시됩니다.

```
-----BEGIN CERTIFICATE-----
 MIICiTCCAfICCQD6m7oRw0uXOjANBgkqhkiG9w0BAQUFADCBiDELMAkGA1UEBhMC
 VVMxCzAJBgNVBAgTAldBMRAwDgYDVQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6
 b24xFDASBgNVBAsTC0lBTSBDb25zb2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAd
 BgkqhkiG9w0BCQEWEG5vb25lQGFtYXpvbi5jb20wHhcNMTEwNDI1MjA0NTIxWhcN
 MTIwNDI0MjA0NTIxWjCBiDELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAldBMRAwDgYD
 VQQHEwdTZWF0dGxlMQ8wDQYDVQQKEwZBbWF6b24xFDASBgNVBAsTC0lBTSBDb25z
 b2xlMRIwEAYDVQQDEwlUZXN0Q2lsYWMxHzAdBgkqhkiG9w0BCQEWEG5vb25lQGFt
```

```
YXpvbi5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBAMaK0dn+a4GmWIWJ
21uUSfwfEvySWtC2XADZ4nB+BLYgVIk60CpiwsZ3G93vUEIO3IyNoH/f0wYK8m9T
rDHudUZg3qX4waLG5M43q7Wgc/MbQITxOUSQv7c7ugFFDzQGBzZswY6786m86gpE
Ibb3OhjZnzcvQAaRHhdlQWIMm2nrAgMBAAEwDQYJKoZIhvcNAQEFBQADgYEAtCu4
nUhVVxYUntneD9+h8Mg9q6q+auNKyExzyLwaxlAoo7TJHidbtS4J5iNmZgXL0Fkb
FFBjvSfpJIlJ00zbhNYS5f6GuoEDmFJl0ZxBHjJnyp378OD8uTs7fLvjx79LjSTb
NYiytVbZPQUQ5Yaxu2jXnimvw3rrszlaEXAMPLE=
-----END CERTIFICATE-----
```

자세한 내용은 AWS Private Certificate Authority 사용 설명서의 루트 CA 인증서 설치를 참조하세요.

2. issue-certificate AWS CLI 명령을 사용하여 프라이빗 CA에서 루트 인증서를 발급하고 설치합니다.

```
$ aws acm-pca issue-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --csr file://ca.csr \
     --signing-algorithm SHA256WITHRSA \
     --template-arn arn:aws:acm-pca:::template/RootCACertificate/V1 \
     --validity Value=3650,Type=DAYS --region aws-region
```

3. get-certificate AWS CLI 명령을 사용하여 루트 인증서를 다운로드합니다.

```
$ aws acm-pca get-certificate \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
    --certificate-arn arn:aws:acm-pca:aws-region:486768734100:certificate-
authority/12345678-1234-1234-1234-123456789012/certificate/
abcdef0123456789abcdef0123456789 \
    --output text --region aws-region > rootCA.pem
```

4. import-certificate-authority-certificate AWS CLI 명령을 사용하여 프라이빗 CA에 루트 인증서를 설치합니다.

```
$ aws acm-pca import-certificate-authority-certificate \
     --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012 \
     --certificate file://rootCA.pem --region aws-region
```

파일 시스템 및 클라이언트 인증서 생성 및 내보내기

1. request-certificate AWS CLI 명령을 사용하여 파일 시스템 및 클라이언트에서 사용할 AWS Certificate Manager 인증서를 요청합니다.

```
$ aws acm request-certificate \
    --domain-name *.ec2.internal \
    --idempotency-token 12345 \
    --region aws-region \
    --certificate-authority-arn arn:aws:acm-pca:aws-
region:111122223333:certificate-authority/12345678-1234-1234-1234-123456789012
```

   요청이 성공하면 발급한 인증서의 ARN이 반환됩니다.

2. 보안을 위해 프라이빗 키를 내보낼 때 프라이빗 키에 암호를 할당해야 합니다. 암호를 생성하여 `passphrase.txt`라는 이름의 파일에 저장

3. export-certificate AWS CLI 명령을 사용하여 이전에 발급된 프라이빗 인증서를 내보냅니다. 내보낸 파일에는 인증서, 인증서 체인, 인증서에 내장된 퍼블릭 키와 관련된 암호화된 프라이빗 2048비트 RSA 키가 포함됩니다. 보안을 위해 프라이빗 키를 내보낼 때 프라이빗 키에 암호를 할당해야 합니다. 다음은 Linux EC2 인스턴스의 예제입니다.

```
$ aws acm export-certificate \
     --certificate-arn arn:aws:acm:aws-
region:111122223333:certificate/12345678-1234-1234-1234-123456789012 \
     --passphrase $(cat passphrase.txt | base64) --region aws-region >
 exported_cert.json
```

4. 다음 `jq` 명령을 사용하여 JSON 응답에서 프라이빗 키와 인증서를 추출합니다.

```
$ passphrase=$(cat passphrase.txt | base64)
cat exported_cert.json | jq -r .PrivateKey > prv.key

cat exported_cert.json | jq -r .Certificate > cert.pem
```

5. 다음 `openssl` 명령을 사용하여 JSON 응답에서 프라이빗 키를 복호화합니다. 명령을 입력하고 나면 암호를 입력하라는 메시지가 표시됩니다.

```
$ openssl rsa -in prv.key -passin pass:$passphrase -out decrypted.key
```

Amazon Linux 2 클라이언트에 Libreswan IPsec 설치 및 구성

다음 섹션에서는 Amazon Linux 2를 실행하는 Amazon EC2 인스턴스에서 Libreswan IPsec을 설치하고 구성하기 위한 지침을 제공합니다.

Libreswan 설치 및 구성

1. SSH를 사용하여 EC2 인스턴스에 연결합니다. 이 작업을 수행하는 방법에 대한 구체적인 지침은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 SSH 클라이언트를 사용하여 Linux 인스턴스에 연결을 참조하세요.
2. `libreswan`을 설치하려면 다음 명령을 실행합니다.

   ```
   $ sudo yum install libreswan
   ```

3. (선택 사항) 이후 단계에서 IPsec을 확인할 때 이러한 설정이 없으면 이러한 속성에 플래그가 지정될 수 있습니다. 먼저 이러한 설정을 사용하지 않고 설정을 테스트해 보는 것이 좋습니다. 연결에 문제가 있는 경우 이 단계로 돌아가서 다음과 같이 변경합니다.

   설치가 완료되면 선호하는 텍스트 편집기를 사용하여 `/etc/sysctl.conf` 파일에 다음 항목을 추가합니다.

   ```
   net.ipv4.ip_forward=1
   net.ipv4.conf.all.accept_redirects = 0
   net.ipv4.conf.all.secure_redirects = 0
   net.ipv4.conf.all.send_redirects = 0
   net.ipv4.conf.default.accept_redirects = 0
   net.ipv4.conf.default.send_redirects = 0
   net.ipv4.conf.lo.accept_redirects = 0
   net.ipv4.conf.lo.send_redirects = 0
   net.ipv4.conf.all.rp_filter = 0
   net.ipv4.conf.default.rp_filter = 0
   net.ipv4.conf.eth0.rp_filter = 0
   ```

   파일을 저장하고 텍스트 편집기를 종료합니다.

4. 변경 사항을 적용합니다.

   ```
   $ sudo sysctl -p
   ```

5. IPsec 구성을 확인합니다.

```
$ sudo ipsec verify
```

설치한 Libreswan 버전이 실행 중인지 확인합니다.

6. IPsec NSS 데이터베이스를 초기화합니다.

```
$ sudo ipsec checknss
```

클라이언트에 인증서 설치

1. 클라이언트용으로 생성한 인증서를 EC2 인스턴스의 작업 디렉터리에 복사합니다. 사용자
2. 이전에 생성한 인증서를 libreswan과 호환 가능한 형식으로 내보냅니다.

```
$ openssl pkcs12 -export -in cert.pem -inkey decrypted.key \
    -certfile rootCA.pem -out certkey.p12 -name fsx
```

3. 포맷이 변경된 키를 가져오고, 메시지가 표시되면 암호를 입력합니다.

```
$ sudo ipsec import certkey.p12
```

4. 선호하는 텍스트 편집기를 사용하여 IPsec 구성 파일을 생성합니다.

```
$ sudo cat /etc/ipsec.d/nfs.conf
```

다음 항목을 구성 파일에 추가합니다.

```
conn fsxn
    authby=rsasig
    left=172.31.77.6
    right=198.19.254.13
    auto=start
    type=transport
    ikev2=insist
    keyexchange=ike
    ike=aes256-sha2_384;dh20
    esp=aes_gcm_c256
    leftcert=fsx
    leftrsasigkey=%cert
    leftid=%fromcert
```

```
    rightid=%fromcert
    rightrsasigkey=%cert
```

파일 시스템에서 IPsec을 구성한 후 클라이언트에서 IPsec을 시작합니다.

파일 시스템에서 IPsec 구성

이 섹션에서는 FSx for ONTAP 파일 시스템에 인증서를 설치하고 IPsec을 구성하는 방법에 대한 지침을 제공합니다.

파일 시스템에 인증서 설치

1. 루트 인증서(`rootCA.pem`)), 클라이언트 인증서(`cert.pem`) 및 복호화된 키(`decrypted.key`) 파일을 파일 시스템에 복사합니다. 인증서의 암호를 알아야 합니다.
2. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
3. (파일 시스템이 아니라) 클라이언트에서 cat를 사용하여 `rootCA.pem`, `cert.pem`, `decrypted.key` 파일의 내용을 나열하여 다음 단계에서 메시지가 표시되면 각 파일의 출력을 복사하여 붙여넣을 수 있습니다.

   ```
   $ > cat cert.pem
   ```

   인증서 내용을 복사합니다.
4. (ONTAP 자체 서명 루트 CA의 경우처럼) ONTAP 측 CA 및 클라이언트 측 CA를 포함하여 상호 인증 중에 사용되는 모든 CA 인증서를 ONTAP 인증서 관리에 설치해야 합니다.

   `security certificate install` NetApp CLI 명령을 사용하여 다음과 같이 클라이언트 인증서를 설치합니다.

   ```
   FSxID123:: > security certificate install -vserver dr -type client -cert-name
    ipsec-client-cert
   ```

```
Please enter Certificate: Press <Enter> when done
```

이전에 복사한 `cert.pem` 파일의 내용을 붙여넣고 Enter 키를 누릅니다.

```
Please enter Private Key: Press <Enter> when done
```

`decrypted.key` 파일의 내용을 붙여넣고 Enter 키를 누릅니다.

```
Do you want to continue entering root and/or intermediate certificates {y|n}:
```

n을 입력하여 클라이언트 인증서 입력을 완료합니다.

5. SVM에서 사용할 인증서를 생성하고 설치합니다. 이 인증서의 발급자 CA가 이미 ONTAP에 설치되어 있고 IPsec에 추가되어 있어야 합니다.

   다음 명령을 사용하여 루트 인증서를 설치합니다.

```
FSxID123:: > security certificate install -vserver dr -type server-ca -cert-name
 ipsec-ca-cert
```

```
Please enter Certificate: Press <Enter> when done
```

`rootCA.pem` 파일의 내용을 붙여넣고 Enter 키를 누릅니다.

6. 인증 중에 설치된 CA가 IPsec CA 검색 경로 내에 있는지 확인하려면 “security ipsec ca-certificate add” 명령을 사용하여 ONTAP 인증서 관리 CA를 IPsec 모듈에 추가합니다.

   다음 명령을 입력하여 루트 인증서를 추가합니다.

```
FSxID123:: > security ipsec ca-certificate add -vserver dr -ca-certs ipsec-ca-cert
```

7. 다음 명령을 입력하여 보안 정책 데이터베이스(SPD)에 필요한 IPsec 정책을 생성합니다.

```
security ipsec policy create -vserver dr -name policy-name -local-ip-
subnets 198.19.254.13/32 -remote-ip-subnets 172.31.0.0/16 -auth-method PKI -action
 ESP_TRA -cipher-suite SUITEB_GCM256 -cert-name ipsec-client-cert -local-identity
 "CN=*.ec2.internal" -remote-identity "CN=*.ec2.internal"
```

8. 다음 명령을 사용하여 확인할 파일 시스템에 대한 IPsec 정책을 표시합니다.

```
FSxID123:: > security ipsec policy show -vserver dr -instance

                                 Vserver: dr
                             Policy Name: promise
                          Local IP Subnets: 198.19.254.13/32
                         Remote IP Subnets: 172.31.0.0/16
                               Local Ports: 0-0
                              Remote Ports: 0-0
                                 Protocols: any
                                    Action: ESP_TRA
                              Cipher Suite: SUITEB_GCM256
        IKE Security Association Lifetime: 86400
      IPsec Security Association Lifetime: 28800
IPsec Security Association Lifetime (bytes): 0
                        Is Policy Enabled: true
                           Local Identity: CN=*.ec2.internal
                          Remote Identity: CN=*.ec2.internal
                   Authentication Method: PKI
          Certificate for Local Identity: ipsec-client-cert
```

클라이언트에서 IPsec 시작

이제 FSx for ONTAP 파일 시스템 및 클라이언트 모두에 IPsec이 구성되었으므로 클라이언트에서 IPsec을 시작할 수 있습니다.

1. SSH를 사용하여 클라이언트 시스템에 연결합니다.
2. IPsec을 시작합니다.

```
$ sudo ipsec start
```

3. IPsec의 상태를 확인합니다.

```
$ sudo ipsec status
```

4. 파일 시스템에 볼륨을 마운트합니다.

```
$ sudo mount -t nfs 198.19.254.13:/benchmark /home/ec2-user/acm/dr
```

5. FSx for ONTAP 파일 시스템에 암호화된 연결을 표시하여 IPsec 설정을 확인합니다.

```
FSxID123:: > security ipsec show-ikesa -node FsxId123
FsxId08ac16c7ec2781a58::> security ipsec show-ikesa -node FsxId08ac16c7ec2781a58-01
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ---------------- -----------
dr          policy-name
                   198.19.254.13   172.31.77.6     551c55de57fe8976 ESTABLISHED
fsx         policy-name
                   198.19.254.38   172.31.65.193   4fd3f22c993e60c5 ESTABLISHED
2 entries were displayed.
```

다중 클라이언트에 대한 IPsec 설정

소수의 클라이언트가 IPsec을 활용해야 하는 경우 각 클라이언트에 대해 단일 SPD 항목을 사용하는 것으로 충분합니다. 그러나 수백 또는 수천 개의 클라이언트가 IPsec을 활용해야 하는 경우에는 IPsec 다중 클라이언트 구성을 사용하는 것이 좋습니다.

FSx for ONTAP은 IPsec이 활성화된 상태에서 여러 네트워크의 여러 클라이언트를 단일 SVM IP 주소에 연결할 수 있도록 지원합니다. 다음 절차에 설명된 `subnet` 구성 또는 `Allow all clients` 구성을 사용하여 이 작업을 수행할 수 있습니다.

서브넷 구성을 사용하여 여러 클라이언트에 IPsec 구성

특정 서브넷(예: 192.168.134.0/24)의 모든 클라이언트가 단일 SPD 정책 항목을 사용하여 단일 SVM IP 주소에 연결할 수 있도록 하려면 `remote-ip-subnets`를 서브넷 형식으로 지정해야 합니다. 또한 올바른 클라이언트측 자격 증명으로 `remote-identity` 필드를 지정해야 합니다.

> **Important**
>
> 인증서 인증을 사용하는 경우 각 클라이언트는 고유한 인증서 또는 공유 인증서를 사용하여 인증할 수 있습니다. FSx for ONTAP IPsec은 로컬 신뢰 저장소에 설치된 CA를 기반으로 인증서의 유효성을 확인합니다. FSx for ONTAP에서는 인증서 취소 목록(CRL) 검사도 지원합니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 다음과 같이 `security ipsec policy create` NetApp ONTAP CLI 명령을 사용하여 *##* 값을 특정 값으로 바꿉니다.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
  -remote-identity client_side_identity
```

모든 클라이언트 구성 허용을 사용하여 여러 클라이언트에 IPsec 구성

소스 IP 주소와 관계없이 모든 클라이언트가 SVM IPsec 지원 IP 주소에 연결할 수 있도록 하려면 `remote-ip-subnets` 필드를 지정할 때 `0.0.0.0/0` 와일드카드를 사용합니다.

또한 올바른 클라이언트측 자격 증명으로 `remote-identity` 필드를 지정해야 합니다. 인증서 인증의 경우 `ANYTHING`을 입력할 수 있습니다.

또한 0.0.0.0/0 와일드카드를 사용하는 경우 사용할 특정 로컬 또는 원격 포트 번호를 구성해야 합니다. NFS 포트 2049를 예로 들 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. 다음과 같이 `security ipsec policy create` NetApp ONTAP CLI 명령을 사용하여 *##* 값을 특정 값으로 바꿉니다.

```
FsxId123456::> security ipsec policy create -vserver svm_name -name policy_name \
  -local-ip-subnets 192.168.134.34/32 -remote-ip-subnets 0.0.0.0/0 \
  -local-ports 2049 -protocols tcp -auth-method PSK \
  -cert-name my_nfs_server_cert -local-identity ontap_side_identity \
```

```
-local-ports 2049 -remote-identity client_side_identity
```

Amazon FSx for NetApp ONTAP의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 어떤 사용자가 Amazon FSx 리소스를 사용할 수 있도록 인증(로그인)되고 권한이 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 Amazon FSx에서 수행하는 작업에 따라 다릅니다.

서비스 사용자 – Amazon FSx 서비스를 사용하여 작업을 수행하는 경우 필요한 보안 인증 정보와 권한을 관리자가 제공합니다. 더 많은 Amazon FSx 기능을 사용하여 작업을 수행한다면 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방법을 이해하면 관리자에게 올바른 권한을 요청하는 데 도움이 됩니다. Amazon FSx의 기능에 액세스할 수 없다면 Amazon FSx for NetApp ONTAP 자격 증명 및 액세스 문제 해결 섹션을 참조하세요.

서비스 관리자 – 회사에서 Amazon FSx 리소스를 책임지고 있다면 Amazon FSx에 대한 완전한 액세스 권한이 있을 것입니다. 서비스 관리자는 서비스 사용자가 액세스해야 하는 Amazon FSx 기능과 리소스를 결정합니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 IAM의 기본 개념을 이해해 두세요. 회사가 Amazon FSx에서 IAM

을 사용하는 방법에 대해 자세히 알아보려면 Amazon FSx for NetApp ONTAP 및 IAM의 작동 방식 섹션을 참조하세요.

IAM 관리자 - IAM 관리자라면 Amazon FSx에 대한 액세스 관리 정책 작성 방법을 자세히 알고 싶을 수도 있습니다. IAM에서 사용할 수 있는 Amazon FSx ID 기반 정책의 예제를 확인하려면 Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제 섹션을 참조하세요.

보안 인증 정보를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. IAM 사용자 또는 AWS 계정 루트 사용자 IAM 역할을 수임하여 로 인증(로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 자격 증명 AWS 으로에 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의에 로그인하는 방법을 AWS참조하세요. AWS 계정

AWS 프로그래밍 방식으로에 액세스하는 경우는 자격 증명을 사용하여 요청에 암호화 방식으로 서명할 수 있는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 요청에 직접 서명하는 자세한 방법은 IAM 사용 설명서에서 API 요청용AWS Signature Version 4를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어는 멀티 팩터 인증(MFA)을 사용하여 계정의 보안을 강화할 것을 AWS 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 다중 인증 및 IAM 사용 설명서에서 IAM의AWS 다중 인증을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 계정의 모든 AWS 서비스 및 리소스에 대한 전체 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는 데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명을 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 전체 작업 목록은 IAM 사용 설명서의 루트 사용자 보안 인증이 필요한 작업을 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스 에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, AWS Directory Service, Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스 에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명에 액세스할 때 역할을 AWS 계정수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을(를) 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 모든 및 애플리케이션에서 사용할 수 있도록 자체 ID 소스의 사용자 AWS 계정 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇인가요?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. 가능하면 암호 및 액세스 키와 같은 장기 자격 증명이 있는 IAM 사용자를 생성하는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 자격 증명이 필요한 특정 사용 사례가 있는 경우, 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 장기 보안 인증이 필요한 사용 사례의 경우, 정기적으로 액세스 키 교체를 참조하세요.

IAM 그룹은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어, IAMAdmins라는 그룹이 있고 이 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 자격 증명을 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서에서 IAM 사용자 사용 사례를 참조하세요.

IAM 역할

IAM 역할은 특정 권한이 AWS 계정 있는 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 에서 IAM 역할을 일시적으로 수임하려면 사용자에서 IAM 역할(콘솔)로 전환할 AWS Management Console수 있습니다. https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_use_switch-role-console.html 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 AWS

CLI 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 관련 역할에 대한 자세한 내용은 IAM 사용 설명서의 Create a role for a third-party identity provider (federation)를 참조하세요. IAM Identity Center를 사용하는 경우, 권한 집합을 구성합니다. 인증 후 ID가 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 집합을 IAM의 역할과 연관짓습니다. 권한 집합에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 집합을 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 수임하여 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 사용자(신뢰할 수 있는 보안 주체)가 내 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 교차 계정 리소스 액세스를 참조하세요.
- 교차 서비스 액세스 - 일부는 다른에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어, 서비스에서 호출하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 직접적으로 호출하는 위탁자의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여에서 작업을 수행하는 경우 AWS보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 Create a role to delegate permissions to an AWS 서비스를 참조하세요.
  - 서비스 연결 역할 - 서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에

표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

- Amazon EC2에서 실행되는 애플리케이션 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로필에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 보안 인증을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결 AWS 될 때 권한을 정의하는의 객체입니다.는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조와 콘텐츠에 대한 자세한 정보는 IAM 사용 설명서의 JSON 정책 개요를 참조하세요.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자 및 역할에는 어떠한 권한도 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하기 위해 사용하는 방법과 상관없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책이 있는 사용자는 AWS Management Console AWS CLI, 또는 API에서 역할 정보를 가져올 수 있습니다 AWS .

ID 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은의 여러 사용자, 그룹 및 역할에 연결할 수 있는

독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 위탁자가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 위탁자를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는가 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACL)

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

Amazon S3 AWS WAF및 Amazon VPC는 ACLs. ACL에 관한 자세한 내용은 Amazon Simple Storage Service 개발자 가이드의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 ID 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 ID 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 정보는 IAM 사용 설명서의 IAM 엔티티에 대한 권한 경계를 참조하세요.
- 서비스 제어 정책(SCPs) - SCPs는의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 JSON 정책입니다 AWS Organizations. AWS Organizations 는 AWS 계정 비즈니스가 소유한 여러를 그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직에서 모든 기능을 활성화할 경우, 서비스 제어 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각각을 포함하여 멤버 계정의 엔

터티에 대한 권한을 제한합니다 AWS 계정 루트 사용자. 조직 및 SCP에 대한 자세한 내용은 AWS Organizations 사용 설명서에서 Service control policies을 참조하세요.

- 리소스 제어 정책(RCP) - RCP는 소유한 각 리소스에 연결된 IAM 정책을 업데이트하지 않고 계정의 리소스에 대해 사용 가능한 최대 권한을 설정하는 데 사용할 수 있는 JSON 정책입니다. RCP는 멤버 계정의 리소스에 대한 권한을 제한하며 조직에 속하는지 여부에 AWS 계정 루트 사용자관계없이를 포함한 자격 증명에 대한 유효 권한에 영향을 미칠 수 있습니다. RCP를 AWS 서비스 지원하는 목록을 포함하여 조직 및 RCPs에 대한 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCPs)을 참조하세요.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 ID 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 정보는 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

Amazon FSx for NetApp ONTAP 및 IAM의 작동 방식

IAM을 사용하여 Amazon FSx에 대한 액세스를 관리하기 전에 Amazon FSx에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

Amazon FSx for NetApp ONTAP에서 사용할 수 있는 IAM 기능

IAM 기능	Amazon FSx 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키	예

IAM 기능	Amazon FSx 지원
ACLs	아니요
ABAC(정책의 태그)	예
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	아니요
서비스 링크 역할	예

Amazon FSx 및 기타 AWS 서비스에서 대부분의 IAM 기능을 사용하는 방법을 전체적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

Amazon FSx의 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 위탁자가 연결된 사용자 또는 역할에 적용되므로 위탁자를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

Amazon FSx의 자격 증명 기반 정책 예

Amazon FSx 자격 증명 기반 정책 예제를 보려면 Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon FSx 내의 리소스 기반 정책

리소스 기반 정책 지원: 아니요

Amazon FSx의 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 위탁자가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

Amazon FSx 작업 목록을 보려면 서비스 승인 참조의 Amazon FSx에서 정의한 작업을 참조하세요.

Amazon FSx의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
fsx
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "fsx:action1",
      "fsx:action2"
         ]
```

Amazon FSx 자격 증명 기반 정책 예제를 보려면 Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon FSx의 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 문에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을

사용하여 리소스를 지정합니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

Amazon FSx 리소스 유형 및 해당 ARN의 목록을 보려면 서비스 권한 부여 참조에서 Amazon FSx에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon FSx에서 정의한 작업을 참조하세요.

Amazon FSx ID 기반 정책 예제를 보려면 Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon FSx의 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 `OR` 작업을 사용하여 조건을 AWS 평가합니다. 문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 는 전역 조건 키와 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

Amazon FSx 조건 키 목록을 보려면 서비스 승인 참조의 Amazon FSx에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon FSx에서 정의한 작업을 참조하세요.

Amazon FSx ID 기반 정책 예제를 보려면 Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제 섹션을 참조하세요.

Amazon FSx의 액세스 제어 목록(ACL)

ACL 지원: 아니요

Amazon FSx를 사용한 속성 기반 액세스 제어(ABAC)

ABAC 지원(정책의 태그): 예

속성 기반 액세스 제어(ABAC)는 속성에 근거하여 권한을 정의하는 권한 부여 전략입니다. 에서는 AWS이러한 속성을 태그라고 합니다. IAM 엔터티(사용자 또는 역할) 및 많은 AWS 리소스에 태그를 연결할 수 있습니다. ABAC의 첫 번째 단계로 개체 및 리소스에 태그를 지정합니다. 그런 다음 위탁자의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

Amazon FSx 리소스 태그 지정에 대한 자세한 내용은 Amazon FSx 리소스 태그 지정 섹션을 참조하세요.

리소스의 태그를 기반으로 리소스에 대한 액세스를 제한하는 자격 증명 기반 정책의 예제는 태그를 사용하여 Amazon FSx 리소스에 대한 액세스 제어 섹션에서 확인할 수 있습니다.

Amazon FSx에서 임시 보안 인증 사용

임시 자격 증명 지원: 예

일부 AWS 서비스 는 임시 자격 증명을 사용하여 로그인할 때 작동하지 않습니다. 임시 자격 증명으로 AWS 서비스 작업하는를 비롯한 추가 정보는 AWS 서비스 IAM 사용 설명서의 IAM으로 작업하는 섹션을 참조하세요.

사용자 이름과 암호를 제외한 방법을 AWS Management Console 사용하여에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 SSO(Single Sign-On) 링크를 AWS 사용하여에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 자격 증명을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 사용자에서 IAM 역할로 전환(콘솔)을 참조하세요.

AWS CLI 또는 AWS API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 access AWS. AWS recommends에 액세스할 수 있습니다. 자세한 정보는 IAM의 임시 보안 자격 증명 섹션을 참조하세요.

Amazon FSx에 대한 액세스 세션 전달

전달 액세스 세션(FAS) 지원: 예

IAM 사용자 또는 역할을 사용하여에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우, 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 완료하기 위해 다른 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 수신할 때만 이루어집니다. 이 경우, 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

Amazon FSx의 서비스 역할

서비스 역할 지원: 아니요

Amazon FSx의 서비스 연결 역할

서비스 링크 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 링크 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

Amazon FSx 서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 Amazon FSx에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

Amazon FSx for NetApp ONTAP의 ID 기반 정책 예제

기본적으로 사용자 및 역할은 Amazon FSx 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 AWS API를 사용하여 작업을 수행할 수 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다. 그런 다음 관리자가 IAM 정책을 역할에 추가하고, 사용자가 역할을 맡을 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 Amazon FSx에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Amazon FSx에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- Amazon FSx 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책에 따라 계정에서 사용자가 Amazon FSx 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정

책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.
- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정켭니다. API 작업을 직접 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

Amazon FSx 콘솔 사용

Amazon FSx for NetApp ONTAP 콘솔에 액세스하려면 최소한의 권한 세트가 있어야 합니다. 이러한 권한은에서 Amazon FSx 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 Amazon FSx 콘솔을 계속 사용할 수 있도록 하려면 `AmazonFSxConsoleReadOnlyAccess` AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

`AmazonFSxConsoleReadOnlyAccess` 및 기타 Amazon FSx 관리 서비스 정책은 AWS Amazon FSx for OpenZFS에 대한 관리형 정책 섹션에서 확인할 수 있습니다.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Amazon FSx for NetApp ONTAP 자격 증명 및 액세스 문제 해결

다음 정보를 사용하여 Amazon FSx 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- Amazon FSx에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행할 권한이 없음
- 내 외부의 사람이 내 Amazon FSx 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

Amazon FSx에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 fsx:*GetWidget* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 fsx:GetWidget on resource: my-example-widget
```

이 경우, fsx:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행할 권한이 없음

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Amazon FSx에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 Amazon FSx에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 Amazon FSx 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- Amazon FSx에서 이러한 기능을 지원하는지 여부를 알아보려면 Amazon FSx for NetApp ONTAP 및 IAM의 작동 방식 섹션을 참조하세요.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 리소스에 대한 액세스 권한을 타사에 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정 소유에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

Amazon FSx에 대해 서비스 연결 역할 사용

Amazon FSx는 AWS Identity and Access Management (IAM) 서비스 연결 역할을 사용합니다. 서비스 연결 역할은 Amazon FSx에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Amazon FSx에서 사전 정의하며 서비스가 사용자를 대신하여 다른 AWS 서비스를 호출하는 데 필요한 모든 권한을 포함합니다.

필요한 권한을 수동으로 추가할 필요가 없으므로 서비스 연결 역할로 Amazon FSx를 더 쉽게 설정할 수 있습니다. Amazon FSx에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Amazon FSx만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며 이 권한 정책은 다른 IAM 엔티티에 연결할 수 없습니다.

먼저 관련 리소스를 삭제한 후에만 서비스 연결 역할을 삭제할 수 있습니다. 이렇게 하면 리소스에 대한 액세스 권한을 실수로 삭제할 수 없기 때문에 Amazon FSx 리소스가 보호됩니다.

서비스 연결 역할을 지원하는 기타 서비스에 대해 자세히 알아보려면 IAM으로 작업하는AWS 서비스를 참조하여 서비스 연결 역할 열이 예인 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Amazon FSx에 대한 서비스 연결 역할 권한

Amazon FSx는 AWSServiceRoleForAmazonFSx라는 서비스 연결 역할을 사용합니다. 이 역할은 VPC의 파일 시스템을 위한 탄력적 네트워크 인터페이스를 생성하고 CloudWatch에 파일 시스템 및 볼륨 지표를 게시하는 등 사용자 계정에서 특정 작업을 수행합니다.

이 정책에 대한 업데이트는 AmazonFSxServiceRolePolicy을 참조하세요.

권한 세부 정보

권한 세부 정보

AWSServiceRoleForAmazonFSx 역할 권한은 AmazonFSxServiceRolePolicy AWS 관리형 정책에 의해 정의됩니다. AWSServiceRoleForAmazonFSx에는 다음과 같은 권한이 있습니다.

> **Note**
>
> AWSServiceRoleForAmazonFSx는 모든 Amazon FSx 파일 시스템 유형에서 사용되며, 나열된 권한 중 일부는 FSx for ONTAP에 적용할 수 없습니다.

- ds - Amazon FSx가 AWS Directory Service 디렉터리에서 애플리케이션을 보고, 권한을 부여하고, 권한을 부여하지 않도록 허용합니다.
- ec2 - Amazon FSx에서 다음 작업을 수행하도록 허용합니다.
  - Amazon FSx 파일 시스템과 연결된 네트워크 인터페이스를 확인하고, 생성하고, 연결을 해제합니다.
  - Amazon FSx 파일 시스템과 연결된 하나 이상의 탄력적 IP 주소를 확인합니다.
  - Amazon FSx 파일 시스템과 연결된 Amazon VPC, 보안 그룹 및 서브넷을 확인합니다.
  - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공합니다.
  - AWS권한이 부여된 사용자가 네트워크 인터페이스에서 특정 작업을 수행할 수 있는 권한을 생성합니다.
- cloudwatch - Amazon FSx가 지표 데이터 포인트를 AWS/FSx 네임스페이스 아래의 CloudWatch에 게시하도록 허용합니다.
- route53 - Amazon FSx에서 Amazon VPC를 프라이빗 호스팅 영역과 연결할 수 있도록 허용합니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CreateFileSystem",
            "Effect": "Allow",
            "Action": [
                "ds:AuthorizeApplication",
                "ds:GetAuthorizedApplicationDetails",
                "ds:UnauthorizeApplication",
                "ec2:CreateNetworkInterface",
                "ec2:CreateNetworkInterfacePermission",
                "ec2:DeleteNetworkInterface",
                "ec2:DescribeAddresses",
                "ec2:DescribeDhcpOptions",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeSubnets",
                "ec2:DescribeVPCs",
                "ec2:DisassociateAddress",
                "ec2:GetSecurityGroupsForVpc",
                "route53:AssociateVPCWithHostedZone"
            ],
            "Resource": "*"
        },
        {
            "Sid": "PutMetrics",
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": [
                "*"
            ],
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": "AWS/FSx"
                }
            }
        },

        {
            "Sid": "TagResourceNetworkInterface",
            "Effect": "Allow",
```

```
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": "AmazonFSx.FileSystemId"
                }
            }
        },
        {
            "Sid": "ManageNetworkInterface",
            "Effect": "Allow",
            "Action": [
                "ec2:AssignPrivateIpAddresses",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:UnassignPrivateIpAddresses"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:network-interface/*"
            ],
            "Condition": {
                "Null": {
                    "aws:ResourceTag/AmazonFSx.FileSystemId": "false"
                }
            }
        },
        {
            "Sid": "ManageRouteTable",
            "Effect": "Allow",
            "Action": [
                "ec2:CreateRoute",
                "ec2:ReplaceRoute",
                "ec2:DeleteRoute"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:route-table/*"
            ],
            "Condition": {
```

```
                "StringEquals": {
                    "aws:ResourceTag/AmazonFSx": "ManagedByAmazonFSx"
                }
            }
        }
    ]
}
```

이 정책에 대한 모든 업데이트는 AWS 관리형 정책에 대한 Amazon FSx 업데이트에 설명되어 있습니다.

IAM 엔터티(사용자, 그룹, 역할 등)가 서비스 연결 역할을 생성하고 편집하거나 삭제할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 권한 섹션을 참조하세요.

Amazon FSx에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. AWS Management Console, IAM CLI 또는 IAM API에서 파일 시스템을 생성하면 Amazon FSx가 서비스 연결 역할을 생성합니다.

> **Important**
>
> 이러한 서비스 연결 역할은 해당 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 자세한 내용은 내 IAM 계정에 표시되는 새 역할을 참조하세요.

이 서비스 연결 역할을 삭제했다가 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. 파일 시스템을 생성할 때 Amazon FSx에서는 서비스 연결 역할을 다시 생성합니다.

Amazon FSx에 대한 서비스 연결 역할 편집

Amazon FSx는 AWSServiceRoleForAmazonFSx 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 연결 역할을 생성한 후에는 다양한 엔터티가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 편집을 참조하세요.

Amazon FSx에 대한 서비스 연결 역할 삭제

서비스 연결 역할이 필요한 기능 또는 서비스가 더 이상 필요 없는 경우에는 해당 역할을 삭제할 것이 좋습니다. 따라서 적극적으로 모니터링하거나 유지하지 않는 미사용 엔터티가 없도록 합니다. 그러나 서비스 연결 역할을 수동으로 삭제하려면 먼저 모든 파일 시스템 및 백업을 삭제해야 합니다.

> **Note**
>
> 리소스를 삭제하려고 할 때 Amazon FSx 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

IAM을 사용하여 수동으로 서비스 연결 역할을 삭제하려면 다음을 수행하세요.

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 AWSServiceRoleForAmazonFSx 서비스 연결 역할을 삭제합니다. 자세한 내용은 IAM 사용 설명서의 서비스 연결 역할 삭제 섹션을 참조하세요.

Amazon FSx 서비스 연결 역할을 지원하는 리전

Amazon FSx는 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원합니다. 자세한 내용은 AWS 리전 및 엔드포인트 섹션을 참조하세요.

Amazon FSx에서 태그 사용

태그를 사용하여 Amazon FSx 리소스에 대한 액세스를 제어하고 ABAC(속성 기반 액세스 제어)를 구현할 수 있습니다. 생성 중에 Amazon FSx 리소스에 태그를 적용하려면 사용자에게 AWS Identity and Access Management (IAM) 권한이 있어야 합니다.

생성 시 리소스 태그 지정에 대한 권한 부여

일부 리소스 생성 Amazon FSx API 작업에서는 리소스를 생성할 때 태그를 지정할 수 있습니다. 이러한 리소스 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 구현할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 ABAC란 무엇입니까 AWS?를 참조하세요.

사용자가 생성 시 리소스에 태그를 지정할 수 있으려면 리소스를 생성하는 작업을 사용할 권한이 있어야 합니다(예: `fsx:CreateFileSystem`, `fsx:CreateStorageVirtualMachine` 또는 `fsx:CreateVolume`). 리소스 생성 작업에서 태그가 지정되면 IAM은 `fsx:TagResource` 작업에서 추가 권한 부여를 수행하여 사용자에게 태그를 생성할 권한이 있는지 확인합니다. 따라서 사용자는 `fsx:TagResource` 작업을 사용할 명시적 권한도 가지고 있어야 합니다.

다음 예제 정책은 사용자가 파일 시스템과 스토리지 가상 머신(SVMs)을 생성하고 특정에서 생성하는 동안 태그를 적용할 수 있도록 허용합니다 AWS 계정.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:CreateStorageVirtualMachine",
         "fsx:TagResource"
      ],
      "Resource": [
         "arn:aws:fsx:region:account-id:file-system/*",
         "arn:aws:fsx:region:account-id:file-system/*/storage-virtual-machine/*"
      ]
    }
  ]
}
```

마찬가지로 다음 정책은 사용자가 특정 파일 시스템에 백업을 생성하고 백업 생성 도중 백업에 임의의 태그를 적용하는 것을 허용합니다.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateBackup"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/file-system-id*"
    },
    {
      "Effect": "Allow",
      "Action": [
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:backup/*"
    }
  ]
}
```

`fsx:TagResource` 작업은 리소스 생성 작업 도중 태그가 적용되는 경우에만 평가됩니다. 따라서 리소스를 생성할 권한이 있는 사용자(태그 지정 조건은 없다고 가정)는 요청에서 태그가 지정되지 않은 경우, `fsx:TagResource` 작업을 사용할 권한이 필요하지 않습니다. 하지만 사용자가 태그를 사용하여 리소스 생성을 시도하는 경우, 사용자에게 `fsx:TagResource` 작업을 사용할 권한이 없다면 요청은 실패합니다.

Amazon FSx 리소스 태그 지정에 대한 자세한 내용은 Amazon FSx 리소스 태그 지정 섹션을 참조하세요. 태그를 사용하여 Amazon FSx 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 태그를 사용하여 Amazon FSx 리소스에 대한 액세스 제어 섹션을 참조하세요.

태그를 사용하여 Amazon FSx 리소스에 대한 액세스 제어

Amazon FSx 리소스 및 작업에 대한 액세스를 제어하려면 태그를 기반으로 IAM 정책을 사용할 수 있습니다. 두 가지 방법으로 제어할 수 있습니다.

- Amazon FSx 리소스의 태그를 기반으로 리소스에 대한 액세스를 제어할 수 있습니다.
- IAM 요청 조건에 어떤 태그가 전달될 수 있는지를 제어할 수 있습니다.

태그를 사용하여 AWS 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 태그를 사용하여 액세스 제어를 참조하세요. 생성 시 Amazon FSx 리소스 태그 지정에 대한 자세한 내용은 생성 시 리소스 태그 지정에 대한 권한 부여 섹션을 참조하세요. 리소스 태그 지정에 대한 자세한 내용은 Amazon FSx 리소스 태그 지정 섹션을 참조하세요.

리소스의 태그를 기반으로 액세스 제어

사용자나 역할이 Amazon FSx 리소스에서 어떤 작업을 수행할 수 있는지를 제어하기 위해 리소스의 태그를 사용할 수 있습니다. 예를 들어, 파일 시스템 리소스에 있는 태그의 키-값 페어를 기반으로 해당 리소스에서 특정 API 작업을 허용하거나 거부할 수 있습니다.

Example 예제 정책 - 특정 태그를 사용하는 경우에만 파일 시스템 생성

이 정책을 통해 사용자가 특정 태그 키-값 페어(이 예제에서는 `key=Department`, `value=Finance`)로 태그를 지정하는 경우에만 파일 시스템을 생성할 수 있습니다.

```
{
    "Effect": "Allow",
    "Action": [
        "fsx:CreateFileSystem",
        "fsx:TagResource"
    ],
```

```
    "Resource": "arn:aws:fsx:region:account-id:file-system/*",
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/Department": "Finance"
        }
    }
}
```

Example 예제 정책 - 특정 태그가 있는 Amazon FSx for NetApp ONTAP 볼륨의 백업만 생성

이 정책을 통해 사용자는 키-값 페어 key=Department, value=Finance로 태그가 지정된 FSx for ONTAP 볼륨에 대한 백업만 생성할 수 있습니다. 백업은 Department=Finance 태그를 사용하여 생성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource",
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
```

```
    ]
}
```

Example 예제 정책 - 특정 태그가 있는 백업에서 특정 태그가 포함된 볼륨 생성

이 정책을 통해 사용자는 Department=Finance 태그가 지정된 백업에서만 Department=Finance 태그가 지정된 볼륨을 생성할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateVolumeFromBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 예제 정책 - 특정 태그가 있는 파일 시스템 삭제

이 정책은 사용자가 Department=Finance 태그가 지정된 파일 시스템만 삭제하도록 허용합니다. 최종 백업을 생성하는 경우 Department=Finance 태그를 지정해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteFileSystem"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 예제 정책 - 특정 태그가 있는 볼륨 삭제

이 정책을 통해 사용자는 Department=Finance 태그가 지정된 볼륨만 삭제할 수 있습니다. 최종 백업을 생성하는 경우 Department=Finance 태그를 지정해야 합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:DeleteVolume"
            ],
```

```
            "Resource": "arn:aws:fsx:region:account-id:volume/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:RequestTag/Department": "Finance"
                }
            }
        }
    ]
}
```

AWS Amazon FSx for OpenZFS에 대한 관리형 정책

AWS 관리형 정책은에서 생성하고 관리하는 독립 실행형 정책입니다 AWS. AWS 관리형 정책은 사용자, 그룹 및 역할에 권한 할당을 시작할 수 있도록 많은 일반적인 사용 사례에 대한 권한을 제공하도록 설계되었습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한을 부여하지 않을 수 있습니다. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

AWS 관리형 정책에 정의된 권한은 변경할 수 없습니다. 가 관리형 정책에 정의된 권한을 AWS 업데이트하는 AWS 경우 업데이트는 정책이 연결된 모든 보안 주체 자격 증명(사용자, 그룹 및 역할)에 영향을 미칩니다. AWS AWS 서비스 는 새가 시작되거나 기존 서비스에 새 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하세요.

AmazonFSxServiceRolePolicy

Amazon FSx가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 허용합니다. 자세한 내용은 Amazon FSx에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

AWS 관리형 정책: AmazonFSxDeleteServiceLinkedRoleAccess

AmazonFSxDeleteServiceLinkedRoleAccess를 IAM 엔티티에 연결할 수 없습니다. 이 정책은 서비스에 연결되어 있으며 해당 서비스에 대한 서비스 연결 역할에서만 사용됩니다. 이 정책은 연결, 분리, 수정 또는 삭제할 수 없습니다. 자세한 내용은 Amazon FSx에 대해 서비스 연결 역할 사용 단원을 참조하십시오.

이 정책은 Amazon FSx가 Amazon FSx for Lustre에서만 사용하는 Amazon S3 액세스에 대한 서비스 연결 역할을 삭제할 수 있도록 허용하는 관리자 권한을 부여합니다.

권한 세부 정보

이 정책에는 Amazon FSx가 Amazon S3 액세스를 위한 FSx 서비스 연결 역할에 대한 삭제 상태를 보고, 삭제하고, 볼 수 있도록 허용하는 iam 권한이 포함되어 있습니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조 안내서의 AmazonFSxDeleteServiceLinkedRoleAccess를 참조하세요.

AWS 관리형 정책: AmazonFSxFullAccess

AmazonFSxFullAccess를 IAM 엔터티에 연결할 수 있습니다. Amazon FSx는 사용자를 대신하여 Amazon FSx가 작업을 수행할 수 있도록 허용하는 서비스 역할에도 이 정책을 연결합니다.

Amazon FSx에 대한 전체 액세스 권한과 관련 AWS 서비스에 대한 액세스를 제공합니다.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- fsx - 보안 주체가 BypassSnaplockEnterpriseRetention을 제외한 모든 Amazon FSx 작업을 수행할 수 있습니다.
- ds - 보안 주체가 AWS Directory Service 디렉터리에 대한 정보를 볼 수 있도록 허용합니다.
- ec2
  - 보안 주체가 지정된 조건에서 태그를 생성할 수 있습니다.
  - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공합니다.
- iam - 보안 주체가 사용자를 대신하여 Amazon FSx 서비스 연결 역할을 생성할 수 있습니다. 이는 Amazon FSx가 사용자를 대신하여 AWS 리소스를 관리할 수 있도록 하기 위해 필요합니다.
- firehose - 보안 주체가 Amazon Data Firehose에 레코드를 쓸 수 있습니다. 이는 사용자가 Firehose에 감사 액세스 로그를 전송하여 FSx for Windows File Server 파일 시스템 액세스를 모니터링할 수 있도록 하기 위해 필요합니다.

- `logs` - 보안 주체가 로그 그룹, 로그 스트림을 생성하고, 로그 스트림에 이벤트를 기록할 수 있습니다. 이는 사용자가 CloudWatch Logs에 감사 액세스 로그를 전송하여 FSx for Windows File Server 파일 시스템 액세스를 모니터링할 수 있도록 하기 위해 필요합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조 안내서의 AmazonFSxFullAccess를 참조하세요.

AWS 관리형 정책: AmazonFSxConsoleFullAccess

`AmazonFSxConsoleFullAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은를 통해 Amazon FSx에 대한 전체 액세스 및 관련 AWS 서비스에 대한 액세스를 허용하는 관리 권한을 부여합니다 AWS Management Console.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `fsx` - 보안 주체가 Amazon FSx 관리 콘솔에서 `BypassSnaplockEnterpriseRetention`을 제외한 모든 작업을 수행할 수 있습니다.
- `cloudwatch` - 보안 주체가 Amazon FSx 관리 콘솔에서 CloudWatch 경보 및 지표를 볼 수 있습니다.
- `ds` - 보안 주체가 AWS Directory Service 디렉터리에 대한 정보를 나열할 수 있도록 허용합니다.
- `ec2`
  - 보안 주체가 라우팅 테이블에 태그를 생성하고, 네트워크 인터페이스, 라우팅 테이블, 보안 그룹, 서브넷 및 Amazon FSx 파일 시스템과 연결된 VPC를 나열할 수 있습니다.
  - 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있도록 허용합니다.
  - 보안 주체가 Amazon FSx 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 볼 수 있도록 허용합니다.
- `kms` - 보안 주체가 AWS Key Management Service 키의 별칭을 나열할 수 있도록 허용합니다.
- `s3` - 보안 주체가 Amazon S3 버킷의 일부 또는 모든 객체를 나열할 수 있습니다(최대 1000개).
- `iam` - Amazon FSx가 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 서비스 연결 역할을 생성할 권한을 부여합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조 안내서의 AmazonFSxConsoleFullAccess를 참조하세요.

AWS 관리형 정책: AmazonFSxConsoleReadOnlyAccess

`AmazonFSxConsoleReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 사용자가에서 이러한 AWS 서비스에 대한 정보를 볼 수 있도록 Amazon FSx 및 관련 서비스에 읽기 전용 권한을 부여합니다 AWS Management Console.

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `fsx`- 보안 주체가 Amazon FSx 관리 콘솔에서 모든 태그를 비롯하여 Amazon FSx 파일 시스템에 대한 정보를 볼 수 있습니다.
- `cloudwatch` - 보안 주체가 Amazon FSx 관리 콘솔에서 CloudWatch 경보 및 지표를 볼 수 있습니다.
- `ds` - 보안 주체가 Amazon FSx Management Console에서 AWS Directory Service 디렉터리에 대한 정보를 볼 수 있도록 허용합니다.
- `ec2`
  - 보안 주체가 Amazon FSx 관리 콘솔에서 Amazon FSx 파일 시스템과 연결된 네트워크 인터페이스, 보안 그룹, 서브넷 및 VPC를 볼 수 있습니다.
  - 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있도록 허용합니다.
  - 보안 주체가 Amazon FSx 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 볼 수 있도록 허용합니다.
- `kms` - 보안 주체가 Amazon FSx Management Console에서 AWS Key Management Service 키의 별칭을 볼 수 있도록 허용합니다.
- `log` - 보안 주체가 요청을 하는 계정과 연결된 Amazon CloudWatch Logs 로그 그룹을 설명할 수 있습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 기존 파일 액세스 감사 구성을 볼 수 있도록 하기 위해 필요합니다.
- `firehose` - 보안 주체가 요청하는 계정과 연결된 Amazon Data Firehose 전송 스트림을 설명할 수 있습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 기존 파일 액세스 감사 구성을 볼 수 있도록 하기 위해 필요합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조 안내서의 AmazonFSxConsoleReadOnlyAccess를 참조하세요.

AWS 관리형 정책: AmazonFSxReadOnlyAccess

`AmazonFSxReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

- `fsx`- 보안 주체가 Amazon FSx 관리 콘솔에서 모든 태그를 비롯하여 Amazon FSx 파일 시스템에 대한 정보를 볼 수 있습니다.
- `ec2` - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공합니다.

이 정책의 권한을 보려면 AWS 관리형 정책 참조 안내서의 AmazonFSxReadOnlyAccess를 참조하세요.

AWS 관리형 정책에 대한 Amazon FSx 업데이트

이 서비스가 이러한 변경 사항을 추적하기 시작한 이후부터 Amazon FSx의 AWS 관리형 정책 업데이트에 대한 세부 정보를 봅니다. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Amazon FSx Amazon FSx for NetApp ONTAP의 문서 기록 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 S3를 생성하여 FSx 볼륨에 연결할 수 `fsx:CreateAndAttachS3AccessPoint` 있는 새 권한을 추가했습니다.	2025년 4월 14일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 의에 있는 모든 S3를 나열할 수 `fsx:DescribeS3AccessPointAttachments` 있는 새 권한을 추가했습니다 AWS 계정 . AWS 리전	2025년 4월 14일

변경 사항	설명	날짜
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 기존 S3를 수정할 수 `fsx:UpdateS3AccessPointAttachments` 있는 새 권한을 추가했습니다.	2025년 4월 14일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 S3를 삭제할 수 `fsx:DetachAndDeleteS3AccessPoint` 있는 새 권한을 추가했습니다.	2025년 4월 14일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 S3를 생성하여 FSx 볼륨에 연결할 수 `fsx:CreateAndAttachS3AccessPoint` 있는 새 권한을 추가했습니다.	2025년 4월 14일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 의에 있는 모든 S3를 나열할 수 `fsx:DescribeS3AccessPointAttachments` 있는 새 권한을 추가했습니다 AWS 계정 . AWS 리전	2025년 4월 14일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 기존 S3를 수정할 수 `fsx:UpdateS3AccessPointAttachments` 있는 새 권한을 추가했습니다.	2025년 4월 14일

변경 사항	설명	날짜
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 S3를 삭제할 수 `fsx:DetachAndDeleteS3AccessPoint` 있는 새 권한을 추가했습니다.	2025년 4월 14일
AmazonFSxConsoleReadOnlyAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체`ec2:DescribeNetworkInterfaces` 가 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 볼 수 있는 새로운 권한을 추가했습니다.	2025년 2월 25일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체`ec2:DescribeNetworkInterfaces` 가 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 볼 수 있는 새로운 권한을 추가했습니다.	2025년 2월 7일
AmazonFSxServiceRolePolicy - 기존 정책에 대한 업데이트	Amazon FSx에 새로운 권한인 `ec2:GetSecurityGroupsForVpc` 가 추가되어 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 유효성 검사를 제공할 수 있습니다.	2024년 1월 9일
AmazonFSxReadOnlyAccess – 기존 정책에 대한 업데이트	Amazon FSx에 새로운 권한인 `ec2:GetSecurityGroupsForVpc` 가 추가되어 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 유효성 검사를 제공할 수 있습니다.	2024년 1월 9일

변경 사항	설명	날짜
AmazonFSxConsoleReadOnlyAccess - 기존 정책에 대한 업데이트	Amazon FSx에 새로운 권한인 `ec2:GetSecurityGroupsForVpc` 가 추가되어 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 유효성 검사를 제공할 수 있습니다.	2024년 1월 9일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에 새로운 권한인 `ec2:GetSecurityGroupsForVpc` 가 추가되어 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 유효성 검사를 제공할 수 있습니다.	2024년 1월 9일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에 새로운 권한인 `ec2:GetSecurityGroupsForVpc` 가 추가되어 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 유효성 검사를 제공할 수 있습니다.	2024년 1월 9일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 OpenZFS용 FSx 파일 시스템에 대해 리전 간 및 계정 간 데이터 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 12월 20일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 OpenZFS용 FSx 파일 시스템에 대해 리전 간 및 계정 간 데이터 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 12월 20일

변경 사항	설명	날짜
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 FSx for OpenZFS 파일 시스템에 대한 볼륨의 온디맨드 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 11월 26일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 FSx for OpenZFS 파일 시스템에 대한 볼륨의 온디맨드 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 11월 26일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 ONTAP Multi-AZ용 FSx 파일 시스템에 대한 공유 VPC 지원을 보고, 활성화하고, 비활성화할 수 있는 새로운 권한을 추가했습니다.	2023년 11월 14일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 ONTAP Multi-AZ용 FSx 파일 시스템에 대한 공유 VPC 지원을 보고, 활성화하고, 비활성화할 수 있는 새로운 권한을 추가했습니다.	2023년 11월 14일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx가 FSx for OpenZFS 다중 AZ 파일 시스템의 네트워크 구성을 관리할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 8월 9일

변경 사항	설명	날짜
AWS 관리형 정책: AmazonFSxServiceRolePolicy – 기존 정책 업데이트	Amazon FSx가 CloudWatch 지표를 AWS/FSx 네임스페이스에 게시하도록 기존 cloudwatch:PutMetricData 권한을 수정했습니다.	2023년 7월 24일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx의 fsx:* 권한을 제거하고 특정 fsx 작업을 추가하도록 정책을 업데이트했습니다.	2023년 7월 13일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx의 fsx:* 권한을 제거하고 특정 fsx 작업을 추가하도록 정책을 업데이트했습니다.	2023년 7월 13일
AmazonFSxConsoleReadOnlyAccess - 기존 정책에 대한 업데이트	사용자가 Amazon FSx 콘솔에서 FSx for Windows File Server 파일 시스템에 대한 향상된 성능 지표와 권장 조치를 볼 수 있도록 하는 새로운 권한을 추가했습니다.	2022년 9월 21일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	사용자가 Amazon FSx 콘솔에서 FSx for Windows File Server 파일 시스템에 대한 향상된 성능 지표와 권장 조치를 볼 수 있도록 하는 새로운 권한을 추가했습니다.	2022년 9월 21일
AmazonFSxReadOnlyAccess - 정책 추적 시작	이 정책은 모든 Amazon FSx 리소스 및 이와 관련된 모든 태그에 대한 읽기 전용 액세스 권한을 부여합니다.	2022년 2월 4일

변경 사항	설명	날짜
AmazonFSxDeleteServiceLinkedRoleAccess - 정책 추적 시작	이 정책은 Amazon FSx가 Amazon S3 액세스에 대한 서비스 연결 역할을 삭제할 수 있도록 허용하는 관리자 권한을 부여합니다.	2022년 1월 7일
AmazonFSxServiceRolePolicy - 기존 정책에 대한 업데이트	Amazon FSx가 Amazon FSx for NetApp ONTAP 파일 시스템의 네트워크 구성을 관리할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx가 EC2 라우팅 테이블에서 범위를 좁힌 호출에 대한 태그를 생성할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx가 Amazon FSx for NetApp ONTAP 파일 시스템을 생성할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx가 EC2 라우팅 테이블에서 범위를 좁힌 호출에 대한 태그를 생성할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일

변경 사항	설명	날짜
AmazonFSxServiceRolePolicy - 기존 정책에 대한 업데이트	Amazon FSx가 CloudWatch Logs 로그 스트림을 설명하고 이에 쓸 수 있도록 하는 새 권한을 추가했습니다. 이는 사용자가 CloudWatch Logs를 사용하여 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
AmazonFSxServiceRolePolicy - 기존 정책에 대한 업데이트	Amazon FSx가 Amazon Data Firehose 전송 스트림을 설명하고 이에 쓸 수 있도록 하는 새 권한을 추가했습니다. 이는 사용자가 Amazon Data Firehose를 사용하여 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 CloudWatch Logs 로그 그룹, 로그 스트림을 설명하고 생성하고, 로그 스트림에 이벤트를 쓸 수 있도록 하는 새로운 권한을 추가했습니다. 이는 보안 주체가 CloudWatch Logs를 사용하여 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
AmazonFSxFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 Amazon Data Firehose에 레코드를 설명하고 기록할 수 있도록 하는 새로운 권한을 추가했습니다. 이는 사용자가 Amazon Data Firehose를 사용하여 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 요청을 하는 계정과 연결된 Amazon CloudWatch Logs 로그 그룹을 설명할 수 있도록 하는 새로운 권한을 추가했습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사를 구성할 때 기존 CloudWatch Logs 로그 그룹을 선택할 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
AmazonFSxConsoleFullAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 요청한 계정과 관련된 Amazon Data Firehose 전송 스트림을 설명할 수 있도록 하는 새로운 권한을 추가했습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 파일 액세스 감사를 구성할 때 기존 Firehose 전송 스트림을 선택할 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonFSxConsoleReadOnlyAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 요청을 하는 계정과 연결된 Amazon CloudWatch Logs 로그 그룹을 설명할 수 있도록 하는 새로운 권한을 추가했습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 기존 파일 액세스 감사 구성을 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
AmazonFSxConsoleReadOnlyAccess - 기존 정책에 대한 업데이트	Amazon FSx에서 보안 주체가 요청한 계정과 관련된 Amazon Data Firehose 전송 스트림을 설명할 수 있도록 하는 새로운 권한을 추가했습니다. 이는 보안 주체가 FSx for Windows File Server 파일 시스템에 대한 기존 파일 액세스 감사 구성을 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
Amazon FSx에서 변경 사항 추적 시작	Amazon FSx는 AWS 관리형 정책에 대한 변경 사항 추적을 시작했습니다.	2021년 6월 8일

Amazon VPC를 사용한 파일 시스템 액세스 제어

액세스 유형에 따라 엔드포인트 중 하나의 DNS 이름 또는 IP 주소를 사용하여 Amazon FSx for NetApp ONTAP 파일 시스템 및 SVM에 액세스합니다. DNS 이름은 VPC에 있는 파일 시스템 또는 SVM의 탄력적 네트워크 인터페이스의 프라이빗 IP 주소에 매핑됩니다. 연결된 VPC 내의 리소스 또는 AWS Direct Connect 또는 VPN을 통해 연결된 VPC와 연결된 리소스만 NFS, SMB 또는 iSCSI 프로토

콜을 통해 파일 시스템의 데이터에 액세스할 수 있습니다. 자세한 내용은 Amazon VPC 사용 설명서의 Amazon VPC란 무엇인가요?를 참조하세요.

> ⚠ Warning
>
> 파일 시스템과 연결된 탄력적 네트워크 인터페이스를 수정하거나 삭제해서는 안 됩니다. 네트워크 인터페이스를 수정하거나 삭제하면 VPC와 파일 시스템 간의 연결이 영구적으로 손실될 수 있습니다.

Amazon VPC 보안 그룹

보안 그룹은 FSx for ONTAP 파일 시스템에 대해 수신 및 발신 트래픽을 제어하는 가상 방화벽 역할을 합니다. 인바운드 규칙은 파일 시스템에 들어오는 트래픽을 제어하고 아웃바운드 규칙은 파일 시스템에서 나가는 트래픽을 제어합니다. 파일 시스템을 생성할 때 파일 시스템이 생성될 VPC를 지정하면 해당 VPC의 기본 보안 그룹이 적용됩니다. 연결된 파일 시스템 및 SVM에서 트래픽을 주고 받을 수 있도록 하는 규칙을 각 보안 그룹에 추가할 수 있습니다. 언제든지 보안 그룹에 대한 규칙을 수정할 수 있습니다. 새 규칙 및 수정된 규칙은 보안 그룹에 연결된 모든 리소스에 자동으로 적용됩니다. Amazon FSx는 트래픽이 리소스에 도달하도록 허용할지 여부를 결정할 때 리소스와 연결된 모든 보안 그룹에서 모든 규칙을 평가합니다.

보안 그룹을 사용하여 Amazon FSx 파일 시스템에 대한 액세스를 제어하려면 인바운드 및 아웃바운드 규칙을 추가합니다. 인바운드 규칙은 들어오는 트래픽을 제어하고 아웃바운드 규칙은 파일 시스템에서 나가는 트래픽을 제어합니다. Amazon FSx 파일 시스템의 파일 공유를 지원되는 컴퓨팅 인스턴스의 폴더에 매핑하려면 보안 그룹에 올바른 네트워크 트래픽 규칙이 있는지 확인합니다.

보안 그룹에 대한 자세한 내용은 Amazon EC2 사용 설명서의 보안 그룹 규칙을 참조하세요.

VPC 보안 그룹 생성

Amazon FSx에 대한 보안 그룹 생성

1. https://console.aws.amazon.com/ec2 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 보안 그룹을 선택합니다.
3. 보안 그룹 생성을 선택합니다.
4. 보안 그룹의 이름과 설명을 지정합니다.
5. VPC의 경우 파일 시스템과 연결된 Amazon VPC를 선택하여 해당 VPC 내에 보안 그룹을 생성합니다.

6. 아웃바운드 규칙의 경우 모든 포트의 모든 트래픽을 허용합니다.
7. 다음 규칙을 보안 그룹의 인바운드 포트에 추가합니다. 소스 필드에서 사용자 지정을 선택하고 다음을 포함하여 FSx for ONTAP 파일 시스템에 액세스해야 하는 인스턴스와 연결된 보안 그룹 또는 IP 주소 범위를 입력해야 합니다.

   - NFS, SMB 또는 iSCSI를 통해 파일 시스템의 데이터에 액세스하는 Linux, Windows 및/또는 MacOS 클라이언트.
   - 파일 시스템에 피어링할 모든 ONTAP 파일 시스템/클러스터(예: SnapMirror, SnapVault 또는 FlexCache 사용).
   - ONTAP REST API, CLI 또는 ZAPI에 액세스하는 데 사용할 모든 클라이언트(예: Harvest/Grafana 인스턴스, NetApp Connector 또는 NetApp BlueXP).

프로토콜	포트	역할
모든 ICMP	모두	인스턴스에 Ping 실행
SSH	22	클러스터 관리 LIF 또는 노드 관리 LIF의 IP 주소에 대한 SSH 액세스
TCP	111	NFS에 대한 원격 프로시저 호출
TCP	135	CIFS에 대한 원격 프로시저 호출
TCP	139	CIFS에 대한 NetBIOS 서비스 세션
TCP	161-162	Simple Network Management Protocol(SNMP)
TCP	443	클러스터 관리 LIF 또는 SVM 관리 LIF의 IP 주소에 대한 ONTAP REST API 액세스
TCP	445	NetBIOS 프레이밍을 사용하는 TCP를 통한 Microsoft SMB/CIFS
TCP	635	NFS 마운트
TCP	749	Kerberos
TCP	2049	NFS 서버 대몬(daemon)

프로토콜	포트	역할
TCP	3260	iSCSI 데이터 LIF를 통한 iSCSI 액세스
TCP	4045	NFS 잠금 대몬(daemon)
TCP	4046	NFS에 대한 네트워크 상태 모니터
TCP	10000	네트워크 데이터 관리 프로토콜(NDMP) 및 NetApp SnapMirror 인터클러스터 통신
TCP	11104	NetApp SnapMirror 인터클러스터 통신 관리
TCP	11105	인터클러스터 LIF를 사용한 SnapMirror 데이터 전송
UDP	111	NFS에 대한 원격 프로시저 호출
UDP	135	CIFS에 대한 원격 프로시저 호출
UDP	137	CIFS에 대한 NetBIOS 이름 확인
UDP	139	CIFS에 대한 NetBIOS 서비스 세션
UDP	161-162	Simple Network Management Protocol(SNMP)
UDP	635	NFS 마운트
UDP	2049	NFS 서버 대몬(daemon)
UDP	4045	NFS 잠금 대몬(daemon)
UDP	4046	NFS에 대한 네트워크 상태 모니터
UDP	4049	NFS 할당량 프로토콜

8. 파일 시스템의 탄력적 네트워크 인터페이스에 보안 그룹을 추가합니다.

파일 시스템에 대한 액세스 허용 해제

모든 클라이언트에서 파일 시스템에 대한 네트워크 액세스 허용을 일시적으로 해제하려면 파일 시스템의 탄력적 네트워크 인터페이스와 연결된 모든 보안 그룹을 제거하고 인바운드 또는 아웃바운드 규칙이 없는 그룹으로 바꾸면 됩니다.

Amazon FSx for NetApp ONTAP에 대한 규정 준수 확인

AWS 서비스 가 특정 규정 준수 프로그램의 범위 내에 있는지 알아보려면 AWS 서비스 규정 준수 프로그램 제공 범위 섹션을 참조하고 관심 있는 규정 준수 프로그램을 선택합니다. 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 에서 보고서 다운로드 AWS Artifact에서 .

사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 AWS 서비스 결정됩니다.는 규정 준수를 지원하기 위해 다음 리소스를 AWS 제공합니다.

- 보안 규정 준수 및 거버넌스 - 이러한 솔루션 구현 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수 기능을 배포하는 단계를 제공합니다.
- HIPAA 적격 서비스 참조 - HIPAA 적격 서비스가 나열되어 있습니다. 모두 HIPAA 자격이 AWS 서비스 있는 것은 아닙니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 - 규정 준수의 관점에서 공동 책임 모델을 이해합니다. 이 가이드에는 여러 프레임워크(미국 국립표준기술연구소(NIST), 결제 카드 산업 보안 표준 위원회(PCI), 국제표준화기구(ISO) 포함)의 보안 제어에 대한 지침을 보호하고 AWS 서비스 매핑하는 모범 사례가 요약되어 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub - 내 보안 상태에 대한 포괄적인 보기를 AWS 서비스 제공합니다 AWS. Security Hub는 보안 컨트롤을 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에 대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하세요.
- Amazon GuardDuty - 의심스러운 악의적인 활동이 있는지 환경을 모니터링하여 사용자, AWS 계정 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty는 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 따르는 데 도움을 줄 수 있습니다.
- AWS Audit Manager - 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험과 규정 및 업계 표준 준수를 관리하는 방법을 간소화할 수 있습니다.

Amazon FSx for NetApp ONTAP 및 인터페이스 VPC 엔드포인트 (AWS PrivateLink)

인터페이스 VPC 엔드포인트를 사용하도록 Amazon FSx를 구성하여 VPC의 보안 상태를 향상시킬 수 있습니다. 인터페이스 VPC 엔드포인트는 인터넷 게이트웨이AWS PrivateLink, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 Amazon FSx APIs에 비공개로 액세스할 수 있는 기술로 구동됩니다. VPC의 인스턴스는 Amazon FSx API와 통신하는 데 퍼블릭 IP 주소를 필요로 하지 않습니다. VPC와 Amazon FSx 간의 트래픽은 AWS 네트워크를 벗어나지 않습니다.

각 인터페이스 VPC 엔드포인트는 서브넷에서 하나 이상의 탄력적 네트워크 인터페이스로 표현됩니다. 네트워크 인터페이스는 트래픽에 대한 진입점 역할을 하는 프라이빗 IP 주소를 Amazon FSx API에 제공합니다. Amazon FSx는 IPv4 및 듀얼 스택(IPv4 및 IPv6) IP 주소 유형으로 구성된 VPC 엔드포인트를 지원합니다. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트 생성을 참조하세요.

Amazon FSx 인터페이스 VPC 엔드포인트에 대한 고려 사항

Amazon FSx에 대한 인터페이스 VPC 엔드포인트를 설정하기 전에 Amazon VPC 사용 설명서에서 인터페이스 VPC 엔드포인트 속성 및 제한 사항을 검토해야 합니다.

VPC에서 모든 Amazon FSx API 작업을 호출할 수 있습니다. 예를 들어 VPC 내에서 CreateFileSystem API를 호출하여 FSx for Windows 파일 시스템을 생성할 수 있습니다. Amazon FSx API의 전체 목록은 Amazon FSx API 참조의 작업을 참조하세요.

VPC 피어링 고려 사항

VPC 피어링을 사용하여 인터페이스 VPC 엔드포인트가 있는 VPC에 다른 VPC를 연결할 수 있습니다. VPC 피어링은 두 VPC 간의 네트워킹 연결입니다. 사용자의 자체 두 VPC 간에 또는 다른 AWS 계정의 VPC와 VPC 피어링 연결을 설정할 수 있습니다. VPCs는 두 가지 다른에 있을 수도 있습니다 AWS 리전.

피어링된 VPCs 간의 트래픽은 AWS 네트워크에 남아 있으며 퍼블릭 인터넷을 통과하지 않습니다. VPC가 피어링되면 두 VPC의 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 같은 리소스는 VPC 중 하나에서 생성된 인터페이스 VPC 엔드포인트를 통해 Amazon FSx API에 액세스할 수 있습니다.

Amazon FSx API에 대한 인터페이스 VPC 엔드포인트 생성

Amazon VPC 콘솔 또는 AWS Command Line Interface ()를 사용하여 Amazon FSx API에 대한 VPC 엔드포인트를 생성할 수 있습니다AWS CLI. 자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트 생성을 참조하세요.

Amazon FSx에 대한 인터페이스 VPC 엔드포인트를 생성하려면 다음 중 하나를 사용합니다.

- **`com.amazonaws.region.fsx`** - Amazon FSx API 작업을 위한 엔드포인트를 생성합니다.
- **`com.amazonaws.region.fsx-fips`** - Federal Information Processing Standard(FIPS) 140-2를 준수하는 Amazon FSx API에 대한 엔드포인트를 생성합니다.

프라이빗 DNS 옵션을 사용하려면 VPC의 `enableDnsHostnames` 및 `enableDnsSupport` 속성을 설정해야 합니다. 자세한 내용은 Amazon VPC 사용 설명서의 VPC에 대한 DNS 지원 보기 및 업데이트를 참조하세요.

중국을 제외하고 엔드포인트 AWS 리전 에 대해 프라이빗 DNS를 활성화한 경우와 AWS 리전같은 에 대한 기본 DNS 이름을 사용하여 VPC 엔드포인트를 사용하여 Amazon FSx에 API 요청을 할 수 있습니다`fsx.us-east-1.amazonaws.com`. 중국(베이징) 및 중국(닝샤)의 경우 `fsx-api.cn-northwest-1.amazonaws.com.cn`각각 `fsx-api.cn-north-1.amazonaws.com.cn` 및를 사용하여 VPC 엔드포인트로 API 요청을 수행할 AWS 리전수 있습니다.

자세한 내용은 Amazon VPC 사용 설명서의 인터페이스 VPC 엔드포인트를 통해 서비스 액세스를 참조하세요.

Amazon FSx에 대한 VPC 엔드포인트 정책 생성

Amazon FSx API에 대한 액세스를 제어하기 위해 VPC 엔드포인트에 AWS Identity and Access Management (IAM) 정책을 연결할 수 있습니다. 이 정책은 다음을 지정합니다.

- 작업을 수행할 수 있는 보안 주체.
- 수행할 수 있는 작업.
- 작업을 수행할 수 있는 리소스.

자세한 내용은 Amazon VPC 사용 설명서의 VPC 엔드포인트를 통해 서비스에 대한 액세스 제어를 참조하세요.

Amazon FSx for NetApp ONTAP의 복원력

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.는 물리적으로 분리되고 격리된 여러 가용 영역을 AWS 리전 제공하며,이 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹과 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 Amazon FSx는 데이터 복원력 및 백업 요구 사항을 지원하는 몇 가지 기능을 제공합니다.

백업 및 복원

Amazon FSx는 Amazon FSx for NetApp ONTAP 파일 시스템에서 볼륨의 자동 백업을 생성하고 저장합니다. Amazon FSx는 Amazon FSx for NetApp ONTAP 파일 시스템의 백업 기간 중 볼륨의 자동 백업을 생성합니다. Amazon FSx는 사용자가 지정한 백업 보존 기간에 따라 볼륨의 자동 백업을 저장합니다. 사용자 시작 백업을 생성하여 수동으로 볼륨을 백업할 수도 있습니다. 백업이 원본으로 지정된 상태에서 새 볼륨을 생성하여 언제든지 볼륨 백업을 복원할 수 있습니다.

자세한 내용은 볼륨 백업으로 데이터 보호 단원을 참조하십시오.

스냅샷

Amazon FSx는 Amazon FSx for NetApp ONTAP 볼륨의 스냅샷 복사본을 생성합니다. 스냅샷은 최종 사용자가 볼륨의 파일을 실수로 삭제하거나 수정하지 못하도록 보호합니다. 자세한 내용은 스냅샷으로 데이터 보호 단원을 참조하십시오.

가용 영역

Amazon FSx for NetApp ONTAP 파일 시스템은 서버 장애가 발생하더라도 데이터에 대한 지속적인 가용성을 제공하도록 설계되었습니다. 각 파일 시스템은 각각 자체 스토리지가 있는 하나 이상의 가용 영역에 있는 두 개의 파일 서버로 구동됩니다. Amazon FSx는 데이터를 자동으로 복제하여 구성 요소 장애로부터 데이터를 보호하고, 하드웨어 장애를 지속적으로 모니터링하며, 장애 발생 시 인프라 구성 요소를 자동으로 교체합니다. 파일 시스템은 필요에 따라 (일반적으로 60초 이내에) 자동으로 장애 조치 및 페일백하고, 클라이언트는 파일 시스템을 사용하여 자동으로 장애 조치 및 페일백합니다.

다중 AZ 파일 시스템

Amazon FSx for NetApp ONTAP 파일 시스템은 AWS 가용 영역 전체에서 가용성과 내구성이 뛰어나며 가용 영역을 사용할 수 없는 경우에도 데이터에 대한 지속적인 가용성을 제공하도록 설계되었습니다.

자세한 내용은 가용성, 내구성 및 배포 옵션 단원을 참조하십시오.

단일 AZ 파일 시스템

Amazon FSx for NetApp ONTAP 파일 시스템은 단일 AWS 가용 영역 내에서 가용성과 내구성이 뛰어나며 개별 파일 서버 또는 디스크 오류가 발생한 경우에도 가용 영역 내에서 지속적인 가용성을 제공하도록 설계되었습니다.

자세한 내용은 가용성, 내구성 및 배포 옵션 단원을 참조하십시오.

Amazon FSx for NetApp ONTAP의 인프라 보안

관리형 서비스인 Amazon FSx for NetApp ONTAP은 AWS 글로벌 네트워크 보안으로 보호됩니다. AWS 보안 서비스 및가 인프라를 AWS 보호하는 방법에 대한 자세한 내용은 AWS 클라우드 보안을 참조하세요. 인프라 보안 모범 사례를 사용하여 AWS 환경을 설계하려면 보안 원칙 AWS Well-Architected Framework의 인프라 보호를 참조하세요.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Amazon FSx에 액세스합니다. 고객은 다음을 지원해야 합니다.

- Transport Layer Security(TLS) TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- DHE(Ephemeral Diffie-Hellman) 또는 ECDHE(Elliptic Curve Ephemeral Diffie-Hellman)와 같은 완전 전송 보안(PFS)이 포함된 암호 제품군 Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 보안 암호 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 통해 임시 보안 인증 정보를 생성하여 요청에 서명할 수 있습니다.

FSx for ONTAP과 함께 NetApp ONTAP Vscan 사용

NetApp ONTAP's Vscan 기능을 사용하여 지원되는 타사 바이러스 백신 소프트웨어를 실행할 수 있습니다. 자세한 내용은 지원되는 각 솔루션에 대한 다음 리소스를 참조하세요.

- Deep Instinct – Vscan 파트너 솔루션 및 Deep Instinct 설명서[1]
- SentinelOne - Vscan 파트너 솔루션 및 SentinelOne Singularity 클라우드 데이터 보안
- Symantec – Vscan 파트너 솔루션 및 Symantec 보호 엔진
- Trellix(이전 McAfee) - Vscan 파트너 솔루션 및 Trellix 제품 문서
- Trend Micro – Vscan 파트너 솔루션

> **Note**
>
> [1] 설명서를 보려면 Deep Instinct의 포털에 로그인해야 합니다.

ONTAP 사용자 및 역할

NetApp ONTAP에는 강력하고 확장 가능한 역할 기반 액세스 제어(RBAC) 기능이 포함되어 있습니다. ONTAP 역할은 ONTAP CLI 및 REST API를 사용할 때 사용자 기능과 권한을 정의합니다. 각 역할은 서로 다른 수준의 관리 기능과 권한을 정의합니다. ONTAP REST API 및 CLI를 사용할 때 FSx for ONTAP 리소스에 대한 액세스를 제어할 목적으로 사용자에게 역할을 할당합니다. FSx for ONTAP 파일 시스템 사용자와 스토리지 가상 머신(SVM) 사용자에 대해 별도로 사용할 수 있는 ONTAP 역할이 있습니다.

ONTAP요 FSx 파일 시스템을 생성하면 파일 시스템 수준과 SVM 수준에서 기본 ONTAP 사용자가 생성됩니다. 추가 파일 시스템과 SVM 사용자를 생성할 수 있으며 조직의 요구 사항을 충족하는 추가 SVM 역할을 생성할 수 있습니다. 이 장에서는 ONTAP 사용자와 역할에 대해 설명하고 추가 사용자 및 SVM 역할을 만드는 자세한 절차를 설명합니다.

파일 시스템 관리자 역할 및 사용자

기본 ONTAP 파일 시스템 사용자는 `fsxadmin` 역할이 할당된 `fsxadmin`입니다. 파일 시스템 사용자에게 할당할 수 있는 사전 정의된 역할은 다음 두 가지가 있습니다.

- **`fsxadmin`** - 이 역할을 가진 관리자는 ONTAP 시스템에서 무제한 권한을 갖습니다. FSx for ONTAP 파일 시스템에서 사용할 수 있는 모든 파일 시스템 및 SVM 수준 리소스를 구성할 수 있습니다.
- **`fsxadmin-readonly`**- 이 역할을 가진 관리자는 파일 시스템 수준에서 모든 내용을 볼 수 있지만 변경할 수는 없습니다.

  이 역할은 사용 가능한 모든 리소스와 해당 속성에 대한 읽기 전용 액세스 권한이 있지만 변경할 수 없으므로 NetApp Harvest와 같은 모니터링 애플리케이션과 함께 사용하기에 적합합니다.

추가 파일 시스템 사용자를 생성하고 `fsxadmin` 또는 `fsxadmin-readonly` 역할을 할당할 수 있습니다. 새 역할을 만들거나 기존 역할을 수정할 수 없습니다. 자세한 내용은 파일 시스템 및 SVM 관리를 위한 새 ONTAP 사용자 만들기 단원을 참조하십시오.

다음 표에서는 파일 시스템 관리자 역할이 ONTAP CLI 및 REST API 명령 및 명령 디렉터리에 대해 갖는 액세스 권한 수준에 대해 설명합니다.

역할 이름	액세스 수준	다음 명령 또는 명령 디렉터리로
`fsxadmin`	모두	FSx for ONTAP에서 사용 가능한 모든 명령 디렉터리
`fsxadmin-readonly`	모두	`security login password` 본인의 사용자 계정 로컬 암호 및 키 정보 관리 전용
	없음	`security`
	읽기 전용	FSx for ONTAP에서 사용 가능한 다른 모든 명령 디렉터리

SVM 관리자 역할 및 사용자

각 SVM에는 별도의 인증 도메인이 있으며 자체 관리자가 독립적으로 관리할 수 있습니다. 파일 시스템의 각 SVM에 대해 기본 사용자는 기본적으로 `vsadmin` 역할이 할당된 vsadmin입니다. 이 `vsadmin` 역할 외에도 SVM 사용자에게 할당할 수 있는 범위가 지정된 권한을 제공하는 다른 사전 정의된 SVM 역할이 있습니다. 조직의 요구 사항에 맞는 액세스 제어 수준을 제공하는 사용자 지정 역할을 만들 수도 있습니다.

SVM 관리자의 사전 정의된 역할과 기능은 다음과 같습니다.

역할 이름	기능
`vsadmin`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • 볼륨 관리(볼륨 이동 제외)

역할 이름	기능
	• 할당량, Qtree, 스냅샷 복사본, 파일 관리 • LUN 관리 • SnapLock 작업 수행(권한 있는 삭제 제외) • 프로토콜 구성: NFS, SMB 및 iSCSI • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링 • SVM의 상태 모니터링
`vsadmin-volume`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • 볼륨 관리(볼륨 이동 포함) • 할당량, Qtree, 스냅샷 복사본, 파일 관리 • LUN 관리 • 프로토콜 구성: NFS, SMB 및 iSCSI • 서비스 구성: DNS, LDAP 및 NIS • 네트워크 인터페이스 모니터링 • SVM의 상태 모니터링
`vsadmin-protocol`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • LUN 관리 • 프로토콜 구성: NFS, SMB 및 iSCSI • 서비스 구성: DNS, LDAP 및 NIS • 네트워크 인터페이스 모니터링 • SVM의 상태 모니터링
`vsadmin-backup`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • NDMP 작업 관리 • 복원된 볼륨을 읽기/쓰기로 설정 • SnapMirror 관계 및 스냅샷 복사본 관리 • 볼륨 및 네트워크 정보 보기

역할 이름	기능
`vsadmin-snaplock`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • 볼륨 관리(볼륨 이동 제외) • 할당량, Qtree, 스냅샷 복사본, 파일 관리 • SnapLock 작업 수행(권한 있는 삭제 포함) • 프로토콜 구성: NFS 및 SMB • 서비스 구성: DNS, LDAP 및 NIS • 작업 모니터링 • 네트워크 연결 및 네트워크 인터페이스 모니터링
`vsadmin-readonly`	• 사용자 계정, 로컬 암호 및 키 정보 관리 • SVM의 상태 모니터링 • 네트워크 인터페이스 모니터링 • 볼륨 및 LUN 보기 • 서비스 및 프로토콜 보기

새 SVM 역할을 만드는 방법에 대한 자세한 내용은 SVM 역할 생성를 참조하세요.

Active Directory를 사용하여 ONTAP 사용자 인증

FSx for ONTAP 파일 시스템 및 SVM에 대한 Windows Active Directory 도메인 사용자의 액세스를 인증할 수 있습니다. Active Directory 계정에서 파일 시스템에 액세스하려면 다음 작업을 수행해야 합니다:

- SVM에 대한 Active Directory 도메인 컨트롤러 액세스를 구성해야 합니다.

  Active Directory 도메인 컨트롤러 액세스를 위한 게이트웨이 또는 터널로 구성하는 데 사용하는 SVM은 CIFS가 사용 설정되어 있거나 Active Directory에 가입되어 있거나 둘 다에 가입되어 있어야 합니다. CIFS를 활성화하지 않고 터널 SVM만 Active Directory에 조인하는 경우 SVM이 Active Directory에 조인되어 있는지 확인합니다. 자세한 내용은 SVMs Microsoft Active Directory에 조인하는 방법 단원을 참조하십시오.
- 파일 시스템에 액세스하려면 Active Directory 도메인 사용자 계정을 활성화해야 합니다.

ONTAP CLI 또는 REST API에 액세스하는 Windows 도메인 사용자에 대해 암호 인증 또는 SSH 퍼블릭 키 인증을 사용할 수 있습니다.

파일 시스템 및 SVM 관리자에 대한 Active Directory 인증을 구성하는 방법을 설명하는 절차는 ONTAP 사용자에 대한 Active Directory 인증 구성을 참조하세요.

파일 시스템 및 SVM 관리를 위한 새 ONTAP 사용자 만들기

각 ONTAP 사용자는 SVM 또는 파일 시스템과 연결됩니다. `fsxadmin` 역할을 가진 파일 시스템 사용자는 `security login create` ONTAP CLI 명령을 사용하여 새 SVM 역할 및 사용자를 생성할 수 있습니다.

`security login create` 명령은 관리 유틸리티에 대한 로그인 방법을 생성합니다. 로그인 방법은 사용자 이름, 애플리케이션(액세스 방법), 인증 방법으로 구성됩니다. 사용자 이름은 여러 애플리케이션에 연결할 수 있습니다. 선택적으로 액세스 제어 역할 이름을 포함할 수 있습니다. Active Directory, LDAP 또는 NIS 그룹 이름을 사용하는 경우 로그인 방법을 통해 지정된 그룹에 속한 사용자에게 액세스 권한을 부여합니다. 사용자가 보안 로그인 테이블에 프로비저닝된 여러 그룹의 구성원인 경우에는 개별 그룹에 대해 권한이 부여된 명령의 통합 목록에 액세스할 수 있습니다.

새 ONTAP 사용자를 생성하는 방법에 대한 자세한 내용은 ONTAP 사용자 생성을 참조하세요.

주제

- ONTAP 사용자 생성
- SVM 역할 생성
- ONTAP 사용자에 대한 Active Directory 인증 구성
- 퍼블릭 키 인증 구성
- 파일 시스템 및 SVM 역할에 대한 비밀번호 요구 사항 업데이트하기
- fsxadmin 계정 암호 업데이트 실패했습니다.

ONTAP 사용자 생성

새 SVM 또는 파일 시스템 사용자 생성하기(ONTAP CLI)

해당 `fsxadmin` 역할이 있는 파일 시스템 사용자만 새 SVM 및 파일 시스템 사용자를 만들 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

```
[~]$ ssh fsxadmin@management_endpoint_ip
```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.

2. `security login create` ONTAP CLI 명령을 사용하여 FSx for ONTAP 파일 시스템 또는 SVM에서 새 사용자 계정을 생성합니다.

   예제에서 플레이스홀더에 대한 데이터를 삽입하여 다음과 같은 필수 속성을 정의합니다:

   - `-vserver` - 새 SVM 역할 또는 사용자를 생성할 SVM의 이름을 지정합니다. 파일 시스템 역할 또는 사용자를 만드는 경우에는 SVM을 지정하지 마세요.
   - `-user-or-group-name` - 로그인 방법의 사용자 이름 또는 Active Directory 그룹 이름을 지정합니다. Active Directory 그룹 이름은 `domain` 인증 방법, `ontapi` 및 `ssh` 애플리케이션을 통해서만 지정할 수 있습니다.
   - `-application` - 로그인 방법의 적용을 지정합니다. 가능한 값으로는 http, ontapi, ssh 등이 있습니다.
   - `-authentication-method` - 로그인을 위한 인증 방법을 지정합니다. 가능한 값은 다음을 포함합니다.
     - 도메인 - Active Directory 인증에 사용
     - 암호 - 암호 인증에 사용
     - 퍼블릭 키 - 퍼블릭 키 인증용 사용자
   - `-role` - 로그인 방법에 대한 액세스 제어 역할 이름을 지정합니다. 파일 시스템 수준에서 지정할 수 있는 유일한 역할은 `fsxadmin`입니다.

   (선택 사항) 다음 매개변수 중 하나 이상을 명령과 함께 사용할 수도 있습니다.

   - `[-comment]` - 사용자 계정에 대한 표기법이나 주석을 포함할 때 사용합니다. 예를 들어 **`Guest account`**입니다. 최대 길이는 128자입니다.
   - `[-second-authentication-method {none|publickey|password|nsswitch}]` - 2단계 인증 방법을 지정합니다. 다음 메타데이터를 지정할 수 있습니다.
     - 암호 - 암호 인증에 사용
     - 퍼블릭 키 - 퍼블릭 키 인증에 사용

- nsswitch - NIS 또는 LDAP 인증에 사용
- none - 지정하지 않을 경우 기본값입니다.

```
Fsx0123456::> security login create -vserver vserver_name -user-or-group-
name user_or_group_name -application login_application -authentication-
method auth_method -role role_or_account_name
```

다음 명령은 로그인 시 암호가 포함된 SSH를 사용하여 fsxadmin-readonly 역할이 할당된 새 파일 시스템 사용자 new_fsxadmin를 생성합니다. 메시지가 표시되면 사용자 암호를 입력합니다.

```
Fsx0123456::> security login create -user-or-group-name new_fsxadmin -application
 ssh -authentication-method password -role fsxadmin-readonly

Please enter a password for user 'new_fsxadmin':
Please enter it again:

Fsx0123456::>
```

3. 다음 명령은 암호가 있는 SSH를 사용하여 로그인하도록 구성된 vsadmin_readonly 역할을 가진 새 SVM 사용자 new_vsadmin를 fsx SVM에 생성합니다. 메시지가 표시되면 사용자 암호를 입력합니다.

```
Fsx0123456::> security login create -vserver fsx  -user-or-group-name new_vsadmin -
application ssh -authentication-method password -role vsadmin-readonly

Please enter a password for user 'new_vsadmin':
Please enter it again:

Fsx0123456::>
```

4. 다음 명령은 NetApp Harvest 애플리케이션에서 성능 및 용량 지표를 수집하는 데 사용할 새 읽기 전용 파일 시스템 사용자 harvest2-user를 생성합니다. 자세한 내용은 Harvest 및 Grafana를 사용하여 FSx for ONTAP 파일 시스템 모니터링 단원을 참조하십시오.

```
Fsx0123456::> security login create -user-or-group-name harvest2-user -application
 ssh -role fsxadmin-readonly -authentication-method password
```

모든 파일 시스템 및 SVM 사용자에 대한 정보를 보려면 다음과 같이 하세요.

- 다음 명령을 사용하여 파일 시스템 및 SVM에 대한 모든 로그인 정보를 볼 수 있습니다.

```
Fsx0123456::> security login show

Vserver: Fsx0123456
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
autosupport    console     password      autosupport      no     none
fsxadmin       http        password      fsxadmin         no     none
fsxadmin       ontapi      password      fsxadmin         no     none
fsxadmin       ssh         password      fsxadmin         no     none
fsxadmin       ssh         publickey     fsxadmin         -      none
new_fsxadmin   ssh         password      fsxadmin-readonly
                                                        no     none

Vserver: fsx
                                                                 Second
User/Group                Authentication                 Acct    Authentication
Name           Application Method        Role Name        Locked Method
-------------- ----------- ------------- ---------------- ------ --------------
new_vsadmin    ssh         password      vsadmin-readonly no     none
vsadmin        http        password      vsadmin          yes    none
vsadmin        ontapi      password      vsadmin          yes    none
vsadmin        ssh         password      vsadmin          yes    none
10 entries were displayed.

Fsx0123456::>
```

SVM 역할 생성

생성하는 각 SVM에는 미리 정의된 `vsadmin` 역할이 할당된 기본 SVM 관리자가 있습니다. 사전 정의된 SVM 역할 세트 외에도 새 SVM 역할을 생성할 수 있습니다. SVM에 새 역할을 만들어야 하는 경우 `security login role create` ONTAP CLI 명령을 사용하세요. 이 명령은 `fsxadmin` 역할을 가진 파일 시스템 관리자가 사용할 수 있습니다.

새 SVM 역할 생성하기(ONTAP CLI)

1. security login role create ONTAP CLI 명령을 사용하여 새 SVM 역할을 만들 수 있습니다:

```
Fsx0123456::> security login role create -vserver vs1.example.com -role vol_role -
cmddirname volume
```

2. 명령에서 다음 필수 파라미터를 지정합니다.

- -vserver SVM의 이름
- -role - 역할의 이름입니다.
- -cmddirname - 역할이 액세스 권한을 부여하는 명령 또는 명령 디렉터리입니다. 명령 하위 디렉터리 이름은 큰따옴표로 묶여 있습니다. 예를 들어 "volume snapshot"입니다. 모든 명령 디렉터리를 지정하려면 DEFAULT를 입력합니다.

3. (선택 사항) 명령에 다음 파라미터 중 하나를 추가할 수도 있습니다.

- -vserver - 해당 역할과 연결되는 SVM의 이름입니다.
- -access - 역할의 액세스 수준입니다. 명령 디렉터리의 경우 여기에는 다음이 포함됩니다.
  - none - 명령 디렉터리의 명령에 대한 액세스를 거부합니다. 이는 사용자 지정 역할의 기본값입니다.
  - readonly - 명령 디렉터리 및 해당 하위 디렉터리의 표시 명령에 대한 액세스 권한을 부여합니다.
  - all - 명령 디렉터리 및 해당 하위 디렉터리의 모든 명령에 대한 액세스 권한을 부여합니다. 내장 함수 명령에 대한 액세스를 허용하거나 거부하려면 명령 디렉터리를 지정해야 합니다.

  비내장 함수 명령(create, modify, delete, show로 끝나지 않는 명령)의 경우:
  - none - 명령 디렉터리의 명령에 대한 액세스를 거부합니다. 이는 사용자 지정 역할의 기본값입니다.
  - readonly - 해당 사항 없음. 사용 금지.
  - all - 명령에 대한 액세스 권한을 부여합니다.
- -query - 액세스 수준을 필터링하는 데 사용되는 쿼리 객체입니다. 이 객체는 명령 또는 명령 디렉터리의 명령에 유효한 옵션 형식으로 지정됩니다. 쿼리 객체는 큰따옴표로 묶습니다.

4. security login role create 명령을 실행합니다.

다음 명령은 vs1.example.com V서버에 대해 “admin”이라는 액세스 제어 역할을 만듭니다. 역할은 “볼륨” 명령에 대한 모든 액세스 권한이 있지만 “aggr0” 집계 내에서만 액세스할 수 있습니다.

```
Fsx0123456::>security login role create -role admin -cmddirname volume -query "-
aggr aggr0" -access all -vserver vs1.example.com
```

ONTAP 사용자에 대한 Active Directory 인증 구성

ONTAP CLI를 사용하여 ONTAP 파일 시스템 및 SVM 사용자에 대한 Active Directory 인증 사용을 구성합니다.

이 절차의 명령을 사용하려면 `fsxadmin` 역할을 가진 파일 시스템 관리자여야 합니다.

ONTAP 사용자에 대한 Active Directory 인증 설정하기(ONTAP CLI)

이 절차의 명령은 해당 `fsxadmin` 역할이 있는 파일 시스템 사용자가 사용할 수 있습니다.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. 그림과 같은 `security login domain-tunnel create` 명령을 사용하여 Windows Active Directory 사용자를 인증하기 위한 도메인 터널을 설정합니다. *svm_name*을 도메인 터널에 사용 중인 SVM의 이름으로 바꿉니다.

   ```
   FsxId0123456::> security login domain-tunnel create -vserver svm_name
   ```
3. `security login create` 이 명령을 사용하여 파일 시스템에 액세스할 Active Directory 도메인 사용자 계정을 만들 수 있습니다.

   명령에서 다음 필수 파라미터를 지정합니다.

   - `-vserver` – CIFS로 구성되고 Active Directory에 가입된 SVM의 이름입니다. 이는 Active Directory 도메인 사용자를 파일 시스템에 인증하기 위한 터널로 사용되며 새 역할 또는 사용자가 생성됩니다.

- `-user-or-group-name` - 로그인 방법의 사용자 이름 또는 Active Directory 그룹 이름입니다. Active Directory 그룹 이름은 `domain` 인증 방법, `ontapi` 및 `ssh` 애플리케이션을 통해서만 지정할 수 있습니다.
- `-application` - 로그인 방법의 애플리케이션입니다. 가능한 값으로는 http, ontapi, ssh 등이 있습니다.
- `-authentication-method` - 로그인에 사용되는 인증 방법입니다. 가능한 값은 다음을 포함합니다.
  - 도메인 - Active Directory 인증에 사용
  - 암호 - 암호 인증용
  - 퍼블릭 키 - 퍼블릭 키 인증용
- `-role` - 로그인 방법에 대한 액세스 제어 역할 이름입니다. 파일 시스템 수준에서 지정할 수 있는 유일한 역할은 `-role fsxadmin`입니다.

다음 예제에서는 `filesystem1` 파일 시스템에 대한 Active Directory 도메인 사용자 계정 `CORP\Admin`을 생성합니다.

```
FSxId012345::> security login create -vserver filesystem1 -username CORP\Admin -
application ssh -authmethod domain -role fsxadmin
```

다음 예제에서는 퍼블릭 키 인증을 사용하여 `CORP\Admin`의 사용자 계정을 생성합니다.

```
FsxId0123456ab::> security login create -user-or-group-name "CORP\Admin" -
application ssh -authentication-method publickey -role fsxadmin
Warning: To use public-key authentication, you must create a public key for user
 "CORP\Admin".
```

다음 명령을 사용하여 `CORP\Admin` 사용자에 대한 공개 키를 만듭니다:

```
FsxId0123456ab::> security login publickey create -username "CORP
\Admin" -publickey "ecdsa-sha2-nistp256 SECRET_STRING_HERE_IS_REDACTED=
 cwaltham@b0be837a91bf.ant.amazon.com"
```

Active Directory 자격 증명으로 SSH를 사용하여 파일 시스템에 로그인하려면 다음과 같이 하세요.

- 다음 예제에서는 `-application` 유형으로 `ssh`를 선택한 경우 Active Directory 보안 인증을 사용하여 파일 시스템에 SSH를 설정하는 방법을 보여줍니다. `username`은 계정을 만들 때 입력한 도메인 이름과 사용자 이름을 백슬래시로 구분하고 따옴표로 묶은 `"domain-name\user-name"` 형식입니다.

  ```
  Fsx0123456::> ssh "CORP\user"@management.fs-abcdef01234567892.fsx.us-east-2.aws.com
  ```

  암호를 입력하라는 메시지가 표시되면 Active Directory 사용자 암호를 사용합니다.

퍼블릭 키 인증 구성

SSH 퍼블릭 키 인증을 활성화하려면 먼저 SSH 키를 생성해서 `security login publickey create` 명령을 사용해 관리자 계정에 연결시켜야 합니다. 그러면 계정이 SVM에 액세스할 수 있습니다. `security login publickey create` 명령은 다음 파라미터를 허용합니다.

파라미터	설명
`-vserver` (선택 사항)	계정에서 액세스하는 SVM의 이름. 파일 시스템 사용자에 대해 SSH 퍼블릭 키 인증을 구성하는 경우 `-versver`를 포함하지 마세요.
`-username`	계정의 사용자 이름. 기본값인 `admin`은 클러스터 관리자의 기본 이름입니다.
`-index`	퍼블릭 키의 인덱스 번호. 키가 해당 계정에 대해 생성된 첫 번째 키인 경우 기본값은 0입니다. 그렇지 않으면 기본값은 계정의 기존 인덱스 번호 중 가장 높은 번호보다 1이 높은 숫자입니다.
`-publickey`	OpenSSH 퍼블릭 키. 이 키는 큰따옴표로 묶습니다.
`-role`	계정에 할당된 액세스 제어 역할.
`-comment` (선택 사항)	퍼블릭 키에 대한 설명 텍스트. 이 텍스트는 큰따옴표로 묶습니다.

다음 예제에서는 퍼블릭 키를 SVM svm01의 SVM 관리자 계정인 svmadmin과 연결합니다. 퍼블릭 키에는 인덱스 번호 5가 할당됩니다.

```
Fsx0123456::> security login publickey create -vserver svm01 -username svmadmin
 -index 5 -publickey "ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAspH64CYbUsDQCdW22JnK6J/
vU9upnKzd2zAk9C1f7YaWRUAFNs2Qe5lUmQ3ldi8AD0Vfbr5T6HZPCixNAIzaFciDy7hgnmdj9eNGedGr/
JNrftQbLD1hZybX
+72DpQB0tYWBhe6eDJ1oPLobZBGfMlPXh8VjeU44i7W4+s0hG0E=tsmith@publickey.example.com"
```

> **Important**
>
> 이 작업을 수행하려면 SVM 또는 파일 시스템 관리자여야 합니다.

파일 시스템 및 SVM 역할에 대한 비밀번호 요구 사항 업데이트하기

security login role config modify ONTAP CLI 명령을 사용하여 파일 시스템 또는 SVM 역할에 대한 비밀번호 요구 사항을 업데이트할 수 있습니다. 이 명령은 fsxadmin 역할이 있는 시스템 관리자 계정을 파일링하는 경우에만 사용할 수 있습니다. 암호 요구 사항을 수정할 때 변경으로 영향을 받는 역할을 가진 기존 사용자가 있는 경우 시스템에서 경고합니다.

다음 예제에서는 fsx SVM에 vsadmin-readonly 역할이 있는 사용자의 최소 길이 암호 요구 사항을 12글자로 수정합니다. 이 예제에는 이 역할을 가진 기존 사용자가 있습니다.

```
FsxId0123456::> security login role config modify -role vsadmin-readonly -vserver fsx -
passwd-minlength 12
```

기존 사용자로 인해 시스템에 다음과 같은 경고가 표시됩니다.

```
Warning: User accounts with this role exist. Modifications to the username/password
 restrictions on this role could result in non-compliant user
         accounts.
Do you want to continue? {y|n}:

FsxId0123456::>
```

fsxadmin 계정 암호 업데이트 실패했습니다.

fsxadmin 사용자의 비밀번호를 업데이트할 때 파일 시스템에 설정된 비밀번호 요건을 충족하지 않으면 오류가 발생할 수 있습니다. security login role config show ONTAP CLI 또는 REST API 명령을 사용하여 비밀번호 요구 사항을 확인할 수 있습니다.

파일 시스템 또는 SVM 역할에 대한 비밀번호 요구 사항을 보려면 다음과 같이 하세요.

1. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *management_endpoint_ip*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 단원을 참조하십시오.
2. security login role config show 명령은 파일 시스템 또는 SVM 역할에 대한 암호 요구 사항을 반환합니다.

   ```
   FsxId0123456::> security login role config show -role fsxadmin -
   fields password_requirement_fields
   ```

   -fields 매개변수에는 다음 중 일부 또는 전부를 지정합니다:

   - passwd-minlength - 암호의 최소 길이.
   - passwd-min-special-chars - 암호의 최소 특수 문자 수.
   - passwd-min-lowercase-chars - 암호의 최소 소문자 수.
   - passwd-min-uppercase-chars - 암호의 최소 대문자 수.
   - passwd-min-digits - 암호의 최소 자릿수.
   - passwd-alphanum - 영숫자 문자의 포함 또는 제외에 대한 정보.
   - passwd-expiry-time - 암호 만료 시간.
   - passwd-expiry-warn-time - 암호 만료 경고 시간.
3. 다음 명령을 실행하여 모든 암호 요구 사항을 확인합니다:

   ```
   FsxId0123456::> security login role config show -role fsxadmin -fields passwd-
   minlength, passwd-min-special-chars, passwd-min-lowercase-chars, passwd-min-
   digits, passwd-alphanum, passwd-expiry-time, passwd-expiry-warn-time, passwd-min-
   uppercase-chars
   ```

```
vserver                role     passwd-minlength passwd-alphanum passwd-min-
special-chars passwd-expiry-time passwd-min-lowercase-chars passwd-min-uppercase-
chars passwd-min-digits passwd-expiry-warn-time
---------------------- -------- ---------------- ---------------
 ------------------------ ------------------ --------------------------
 -------------------------- ----------------- ----------------------
FsxId0123456           fsxadmin 3                enabled         0
       unlimited          0                         0                         0
               unlimited
```

할당량

다음에서는 Amazon FSx for NetApp ONTAP 작업 시 할당량에 대해 알아봅니다.

주제

늘릴 수 있는 할당량

다음은 늘릴 수 AWS 리전있는 각 AWS 계정에 대한 Amazon FSx for NetApp ONTAP 할당량입니다.

리소스	Default	설명
ONTAP 파일 시스템	100	이 계정에서 생성할 수 있는 Amazon FSx for NetApp ONTAP 파일 시스템의 최대 수입니다.
ONTAP SSD 스토리지 용량	524,288	이 계정에서 보유할 수 있는 모든 Amazon FSx for NetApp ONTAP 파일 시스템의 최대 SSD 스토리지 용량(GiB)입니다.
ONTAP 처리량 용량	10,240	이 계정에서 보유할 수 있는 모든 Amazon FSx for NetApp ONTAP 파일 시스템의 최대 처리량 용량(MBps)입니다.
ONTAP SSD IOPS	1,000,000	이 계정에서 보유할 수 있는 모든 Amazon FSx for NetApp ONTAP 파일 시스템의 최대 SSD IOPS 양입니다.
ONTAP 백업	10,000개	AWS 계정에 포함할 수 있는 모든 Amazon FSx for NetApp

리소스	Default	설명
		ONTAP 파일 시스템에 대한 사용자 시작 볼륨 백업의 최대 개수입니다.

할당량 증가 요청

1. AWS Support 페이지를 열고 필요 시 로그인을 한 다음 사례 생성을 선택합니다.
2. 사례 생성에서 계정 및 결제 지원을 선택합니다.
3. 사례 세부 정보 패널에 다음과 같이 입력합니다.
   - 유형에서 계정을 선택합니다.
   - 범주에서 기타 계정 문제를 선택합니다.
   - 제목에 **`Amazon FSx for NetApp ONTAP service limit increase request`**를 입력합니다.
   - 다음을 포함하여 요청에 대한 자세한 설명을 입력합니다.
     - 증가를 원하는 FSx 할당량과 원하는 증가 값(알고 있는 경우).
     - 할당량 증가를 원하는 이유.
     - 증가를 요청하는 각 파일 시스템의 파일 시스템 ID 및 리전.
4. 원하는 연락처 옵션을 제공하고 제출을 선택합니다.

각 파일 시스템의 리소스 할당량

다음 표에는 AWS 리전의 각 파일 시스템에 대한 Amazon FSx for NetApp ONTAP 리소스의 할당량이 나와 있습니다.

리소스	파일 시스템당 한도
최소 SSD 스토리지 용량	고가용성(HA) 페어당 1,024GiB
최대 SSD 스토리지 용량	• 2세대 Single-AZ 파일 시스템: HA 페어당 512TiB, 최대 1PiB • 2세대 Multi-AZ 파일 시스템: 512TiB

리소스	파일 시스템당 한도
	• 1세대 파일 시스템: 192TiB
최대 SSD IOPS	2세대 파일 시스템: • Single-AZ의 경우 HA 페어당 200,000개(최대 12개 페어) • Multi-AZ의 경우 총 200,000 1세대 파일 시스템: • 미국 동부(오하이오) 지역, 미국 동부(버지니아 북부) 지역, 미국 서부(오리건) 지역 및 유럽(아일랜드)의 160,000명 • FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든에서 80,000
최소 처리량 용량	• 2세대 파일 시스템(HA 페어 1개): 384MBps • 2세대 파일 시스템(2개 이상의 HA 페어): HA 페어당 1,536MBps • 1세대 파일 시스템: 128MBps

리소스	파일 시스템당 한도
최대 처리량 용량	2세대 파일 시스템: • Single-AZ의 경우 73,728MBps [1] • Multi-AZ의 경우 6,144MBps 1세대 파일 시스템: • 미국 동부(오하이오) 지역, 미국 동부(노스버지니아) 지역, 미국 서부(오리건) 지역 및 유럽(아일랜드)에서 4,096MBps[2] • FSx for ONTAP을 사용할 수 AWS 리전 있는 다른 모든에서 2,048MBps
최대 볼륨 수	• 2세대 파일 시스템(HA 페어 1개): 500 • 2세대 파일 시스템(2개 이상의 HA 페어): 1,000개 • 1세대 파일 시스템: 500
최대 스냅샷 수	볼륨당 1,023개[3]
최대 백업 수	볼륨당 4,091개[4]

리소스	파일 시스템당 한도
최대 SVM 수	HA 페어가 한 개 있는 2세대 파일 시스템: • 6(처리량 용량 384MBps) • 6(처리량 용량 768MBps) • 14(처리량 용량 1,536MBps) • 14(처리량 용량 3,072MBps) • 24(처리량 용량 6,144MBps) HA 페어가 2~12개인 2세대 파일 시스템: • 5 1세대 파일 시스템: • 6(128MBps 처리량 용량) • 6(256MBps 처리량 용량) • 14(512MBps 처리량 용량) • 14(1,024MBps 처리량 용량) • 24(2,048MBps 처리량 용량) • 24(4,096MBps 처리량 용량)
최대 태그 수	50
자동 백업의 최대 보존 기간	90일
사용자 시작 백업의 최대 보존 기간	보존 제한 없음
파일 시스템당 지원되는 최대 경로 수	50[5]
파일 서버당 최대 클라이언트 연결 수[6]	100,000건

Note

[1] HA 페어가 12개(HA 페어당 6,144MBps)인 2세대 Single-AZ 파일 시스템에서. 자세한 내용은 고가용성(HA) 페어 관리 단원을 참조하십시오.

[2] 4GBps의 처리량 용량을 프로비저닝하려면 FSx for ONTAP 1세대 파일 시스템에서 지원되는 AWS 리전에 최대 SSD IOPS(160,000)와 최소 5,120 GiB의 SSD 스토리지 용량을 구성해야 합니다. 4,096MBps의 처리량 용량을 AWS 리전 지원하는에 대한 자세한 내용은 섹션을 참조하세요처리량 용량이 성능에 미치는 영향.

[3] 언제든지 볼륨당 최대 1,023개의 스냅샷을 저장할 수 있습니다. 이 한도에 도달하면 볼륨의 새 스냅샷을 생성하기 전에 기존 스냅샷을 삭제해야 합니다.

[4] 언제든지 볼륨당 최대 4,091개의 백업을 저장할 수 있습니다. 이 한도에 도달하면 볼륨의 새 백업을 생성하기 전에 기존 백업을 삭제해야 합니다.

[5] 언제든지 파일 시스템당 최대 50개의 경로를 구성할 수 있습니다. 이 한도에 도달하면 새 경로를 구성하기 전에 기존 경로를 삭제해야 합니다. 파일 시스템이 보유한 라우팅 수는 파일 시스템이 보유한 SVMs 수와 해당 시스템과 연결된 라우팅 테이블 수에 따라 결정됩니다. (1 + 파일 시스템의 SVMs 수) * (파일 시스템과 연결된 라우팅 테이블) 방정식을 사용하여 파일 시스템에 대한 기존 라우팅 수를 확인할 수 있습니다.

[6] 클라이언트 연결은 지정된 파일 서버에 대한 단일 TCP 연결로 정의됩니다. 파일 시스템에는 HA 페어당 하나의 활성 파일 서버가 있습니다. 클라이언트는 파일 서버에 여러 TCP 연결을 가질 수 있습니다. 예를 들어 클라이언트가 다중 경로를 사용하는 경우입니다.

Amazon FSx for NetApp ONTAP 문제 해결

다음 섹션을 사용하여 FSx for ONTAP 파일 시스템의 문제를 해결합니다.

주제

파일 시스템이 **MISCONFIGURED** 상태임

파일 시스템의 `MISCONFIGURED` 상태에는 다음과 같이 여러 가지 잠재적인 원인이 있으며, 각 원인에는 고유한 해결 방법이 있습니다.

주제

VPC 소유자 계정이 Multi-AZ VPC 공유를 비활성화했습니다.

공유 VPC 서브넷 AWS 계정 에서 참가자가 생성한 다중 AZ 파일 시스템은 다음 이유 중 하나로 `MISCONFIGURED` 상태가 됩니다.

- VPC 서브넷을 공유한 소유자 계정은 FSx for ONTAP 파일 시스템에 대한 Multi-AZ VPC 공유 지원을 비활성화했습니다.
- 소유자 계정이 VPC 서브넷 공유를 중지했습니다.

소유자 계정이 VPC 서브넷 공유를 중지한 경우 해당 파일 시스템의 콘솔에 다음 메시지가 표시됩니다.

```
The vpc ID vpc-012345abcde does not exist
```

문제를 해결하려면 VPC 서브넷을 공유한 소유자 계정에 문의해야 합니다. 자세한 내용은 공유 서브넷에서 FSx for ONTAP 파일 시스템 만들기을 참조하세요.

Multi-AZ 파일 시스템에서 새 SVM을 생성할 수 없습니다.

공유 VPC AWS 계정 의 참가자가 생성한 다중 AZ 파일 시스템의 경우 다음 이유 중 하나로 인해 새 SVM을 생성할 수 없습니다.

- VPC 서브넷을 공유한 소유자 계정은 FSx for ONTAP 파일 시스템에 대한 Multi-AZ VPC 공유 지원을 비활성화했습니다.
- 소유자 계정이 VPC 서브넷 공유를 중지했습니다.

문제를 해결하려면 VPC 서브넷을 공유한 소유자 계정에 문의해야 합니다. 자세한 내용은 공유 서브넷에서 FSx for ONTAP 파일 시스템 만들기을 참조하세요.

파일 시스템의 SSD 스토리지 계층이 90% 이상 찼습니다.

단일 AZ 또는 다중 AZ 파일 시스템의 SSD 스토리지 계층이 현재 90% 이상 가득 찼습니다. SSD 스토리지 계층의 사용률은 지속적으로 80%를 초과하지 않는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에 SSD 스토리지 계층의 공간을 확보하지 않으면 FSx for ONTAP은 패치 작업 기간 동안 파일 시스템의 처리량을 일시적으로 제한합니다. 이는 백그라운드 유지 관리 프로세스가 적절한 기간 내에 완료될 수 있도록 하기 위해 수행됩니다. 이를 방지하려면 SSD 스토리지 계층의 사용률을 90% 미만으로 줄이세요. SSD 사용률을 다음과 같은 여러 가지 방법으로 줄일 수 있습니다.

- 파일 시스템의 SSD 스토리지 용량 증가.
- 불필요한 데이터를 삭제합니다.
- 불필요한 볼륨 스냅샷을 삭제합니다.

자세한 내용은 스토리지 용량 관리 단원을 참조하십시오.

파일 시스템 액세스 불가

이 섹션에서는 파일 시스템에 액세스할 수 없는 것과 관련된 문제와 해결 방법을 설명합니다.

주제

다중 AZ 파일 시스템에 라우팅 테이블 태그가 없습니다.

Amazon FSx는 태그 기반 인증을 사용하여 Multi-AZ 파일 시스템의 VPC 라우팅 테이블을 관리합니다. 파일 시스템과 연결된 하나 이상의 라우팅 테이블에 현재 이러한 라우팅 테이블 태그가 누락되어 있습니다. 이러한 라우팅 테이블은 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정됩니다. 다음 유지 관리 기간 전에 이러한 태그를 수동으로 추가하지 않으면 태그가 누락된 라우팅 테이블과 연결된 서브넷의 모든 클라이언트는 패치 작업 기간 동안 파일 시스템에 대한 액세스 권한을 일시적으로 잃게 됩니다. 이를 방지하려면 누락된 라우팅 테이블 태그를 수동으로 추가하십시오.

자세한 내용은 파일 시스템 업데이트 단원을 참조하십시오.

파일 시스템에 50개 이상의 경로가 있습니다.

현재 파일 시스템에는 50개 이상의 경로가 연결되어 있습니다. 파일 시스템의 다음 예약된 유지 관리 기간 전에 이러한 경로 중 일부를 제거하지 않으면 장애 조치 프로세스가 평소보다 오래 걸릴 수 있습니다. 이를 방지하려면 경로 수를 50개 미만으로 줄이세요. 다음은 파일 시스템과 연결된 경로 수를 줄이기 위해 수행할 수 있는 단계입니다.

- 초과 경로 삭제

- 파일 시스템과 연결된 SVMs 수 줄이기
- 파일 시스템과 연결된 라우팅 테이블 수 줄이기

자세한 내용은 파일 시스템 업데이트 및 스토리지 가상 머신 삭제(SVM) 섹션을 참조하세요.

파일 시스템에 하나 이상의 파일 서버에 대한 경로가 없습니다.

파일 시스템에 현재 하나 이상의 파일 서버에 대한 경로가 누락되어 있고 기존 라우팅 테이블에 새 라우팅 테이블 항목을 추가할 공간이 충분하지 않습니다. 파일 시스템의 예약된 다음 유지 관리 기간 전에 누락된 경로를 추가하지 않으면 패치 작업 기간 동안 연결된 모든 클라이언트의 연결이 끊어집니다. 이를 방지하려면 누락된 경로를 추가하십시오.

자세한 내용은 파일 시스템 업데이트 및 할당량 섹션을 참조하세요.

파일 시스템의 탄력적 네트워크 인터페이스가 수정 또는 삭제됨

파일 시스템의 탄력적 네트워크 인터페이스 중 어떤 것도 수정하거나 삭제해서는 안 됩니다. 네트워크 인터페이스를 수정하거나 삭제하면 Virtual Private Cloud(VPC)와 파일 시스템 간의 연결이 영구적으로 손실될 수 있습니다. 새 파일 시스템을 생성하고, Amazon FSx 네트워크 인터페이스를 수정하거나 삭제하지 않습니다. 자세한 내용은 Amazon VPC를 사용한 파일 시스템 액세스 제어 섹션을 참조하세요.

파일 시스템의 탄력적 네트워크 인터페이스에 연결된 탄력적 IP 주소가 삭제됨

Amazon FSx는 퍼블릭 인터넷에서 파일 시스템에 액세스하는 것을 지원하지 않습니다. Amazon FSx는 인터넷에서 연결할 수 있는 퍼블릭 IP 주소인 탄력적 IP 주소를 자동으로 분리합니다. 이 주소는 파일 시스템의 탄력적 네트워크 인터페이스에 연결됩니다. 자세한 내용은 지원되는 클라이언트 단원을 참조하십시오.

파일 시스템의 VPC 보안 그룹에 필요한 인바운드 규칙이 없음

Amazon VPC 보안 그룹에 지정된 인바운드 규칙을 검토하고 파일 시스템 관련 보안 그룹에 해당 인바운드 규칙이 포함되도록 해야 합니다.

컴퓨팅 인스턴스의 VPC 보안 그룹에는 필요한 아웃바운드 규칙이 없습니다.

Amazon VPC 보안 그룹에 지정된 아웃바운드 규칙을 검토하고 컴퓨팅 인스턴스 관련 보안 그룹에 해당 아웃바운드 규칙이 포함되도록 해야 합니다.

컴퓨팅 인스턴스의 서브넷이 파일 시스템과 연결된 라우팅 테이블을 사용하지 않음

FSx for ONTAP은 VPC 라우팅 테이블의 파일 시스템에 액세스하기 위한 엔드포인트를 생성합니다. 클라이언트가 있는 서브넷과 연결된 모든 VPC 라우팅 테이블을 사용하도록 파일 시스템을 구성하는 것이 좋습니다. 기본적으로 Amazon FSx는 VPC의 기본 라우팅 테이블을 사용합니다. 파일 시스템을 생성할 때 Amazon FSx가 사용할 하나 이상의 라우팅 테이블을 선택적으로 지정할 수 있습니다.

파일 시스템의 클러스터 간 엔드포인트에 ping을 수행할 수 있지만 파일 시스템의 관리 엔드포인트에 ping을 수행할 수 없는 경우(자세한 내용은 파일 시스템 리소스 섹션 참조), 클라이언트가 파일 시스템의 라우팅 테이블 중 하나와 연결된 서브넷에 있지 않을 가능성이 높습니다. 파일 시스템에 액세스하려면 파일 시스템의 라우팅 테이블 중 하나를 클라이언트의 서브넷에 연결합니다. 파일 시스템의 Amazon VPC 라우팅 테이블 업데이트에 대한 자세한 내용은 파일 시스템 업데이트 섹션을 참조하세요.

Amazon FSx는를 사용하여 생성된 다중 AZ 파일 시스템의 라우팅 테이블을 업데이트할 수 없습니다. AWS CloudFormation

Amazon FSx는 태그 기반 인증을 사용하여 Multi-AZ 파일 시스템의 VPC 라우팅 테이블을 관리합니다. 이러한 라우팅 테이블은 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정됩니다. 를 사용하여 FSx for ONTAP 다중 AZ 파일 시스템을 생성하거나 업데이트할 때는 `Key: AmazonFSx; Value: ManagedByAmazonFSx` 태그를 수동으로 추가하는 것이 AWS CloudFormation 좋습니다.

Multi-AZ 파일 시스템에 연결할 수 없는 경우 파일 시스템과 연결된 VPC 라우팅 테이블에 `Key: AmazonFSx; Value: ManagedByAmazonFSx`로 태그가 지정되었는지 확인합니다. 그렇지 않은 경우 Amazon FSx는 장애 조치 이벤트가 발생할 때 관리 및 데이터 포트의 부동 IP 주소를 활성 파일 서버로 라우팅하도록 이러한 라우팅 테이블을 업데이트할 수 없습니다. 파일 시스템의 Amazon VPC 라우팅 테이블 업데이트에 대한 자세한 내용은 파일 시스템 업데이트 섹션을 참조하세요.

다른 VPC에 있는 클라이언트에서 iSCSI를 통해 파일 시스템에 액세스할 수 없음

다른 VPC에 있는 클라이언트에서 Internet Small Computer Systems Interface(iSCSI) 프로토콜을 통해 파일 시스템에 액세스하려면 Amazon VPC 피어링을 구성하거나 파일 시스템과 연결된 VPC와 클라이언트가 있는 VPC 간에 AWS Transit Gateway 를 구성하면 됩니다. 자세한 내용은 Amazon Virtual Private Cloud 설명서의 VPC 피어링 연결 생성 및 수락을 참조하세요.

소유 계정이 VPC 서브넷 공유를 중지했습니다.

공유된 VPC 서브넷에서 파일 시스템을 생성한 경우 소유 계정이 VPC 서브넷 공유를 중지했을 수 있습니다.

소유자 계정이 VPC 서브넷 공유를 중지한 경우 해당 파일 시스템의 콘솔에 다음 메시지가 표시됩니다.

```
The vpc ID vpc-012345abcde does not exist
```

소유 계정에 문의하여 서브넷을 다시 공유할 수 있도록 해야 합니다.

다른 VPC 또는 온프레미스의 클라이언트에서 NFS, SMB, ONTAP CLI 또는 ONTAP REST API를 통해 파일 시스템에 액세스할 수 없음

다른 VPC 또는 온프레미스의 클라이언트에서 NFS(Network File System), SMB(Server Message Block) 또는 NetApp ONTAP CLI 및 REST API를 통해 파일 시스템에 액세스하려면 파일 시스템과 연결된 VPC와 클라이언트가 있는 네트워크 AWS Transit Gateway 간에 라우팅을 구성해야 합니다. 자세한 내용은 FSx for ONTAP 데이터 액세스 단원을 참조하십시오.

스토리지 가상 머신(SVM)이 **MISCONFIGURED** 상태임

다음과 같이 스토리지 가상 머신이 MISCONFIGURED 상태가 되는 여러 가지 잠재적 원인이 있으며, 각각 자체 해상도를 갖습니다.

SVM에 오프라인 볼륨이 있음

파일 시스템에는 오프라인 상태의 볼륨이 포함되어 있습니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인 상태로 전환하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인 상태로 전환합니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 volume online ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 -vserver 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

SVM에 iSCSI LUN 또는 NVMe/TCP 네임스페이스가 있는 오프라인 볼륨이 있음

파일 시스템에는 제한된 상태의 볼륨이 포함되어 있습니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인 상태로 전환하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인 상태로 전환합니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

스토리지 가상 머신(SVM)을 Active Directory에 조인할 수 없음

SVM을 Active Directory(AD)에 조인할 수 없는 경우 먼저 SVMs Microsoft Active Directory에 조인하는 방법 섹션을 검토합니다. SVM을 Active Directory에 조인하지 못하게 하는 일반적인 문제는 다음 섹션에 나열되어 있으며 각 상황에서 생성되는 오류 메시지도 나와 있습니다.

주제

- SVM NetBIOS 이름은 홈 도메인의 NetBIOS 이름과 동일합니다.
- SVM이 이미 다른 Active Directory에 조인되어 있음
- SVM의 NetBIOS 이름이 이미 사용 중이기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음
- Amazon FSx가 Active Directory 도메인 컨트롤러와 통신할 수 없음
- 포트 요구 사항 또는 서비스 계정 권한이 충족되지 않아 Amazon FSx가 Active Directory에 연결할 수 없음
- 서비스 계정 보안 인증이 유효하지 않기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음
- 서비스 계정 보안 인증이 충분하지 않기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음
- Amazon FSx가 Active Directory DNS 서버 또는 도메인 컨트롤러와 통신할 수 없음
- 잘못된 Active Directory 도메인 이름 때문에 Amazon FSx가 Active Directory와 통신할 수 없음

- 서비스 계정이 SVM Active Directory 구성에 지정된 관리자 그룹에 액세스할 수 없음
- 지정된 조직 단위가 존재하지 않거나 액세스할 수 없어 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음

SVM NetBIOS 이름은 홈 도메인의 NetBIOS 이름과 동일합니다.

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory. This is because the server name you specified is the NetBIOS name of the home domain. To fix this problem, choose a NetBIOS name for your SVM that is different from the NetBIOS name of the home domain. Then reattempt to join your SVM to your Active Directory.

이 문제를 해결하려면 AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다. SVM에 Active Directory 홈 도메인의 NetBIOS 이름과 다른 NetBIOS 이름을 사용해야 합니다.

SVM이 이미 다른 Active Directory에 조인되어 있음

Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection to your Active Directory. This is because the SVM is already joined to a domain. To join this SVM to a different domain, you can use the ONTAP CLI or REST API to unjoin this SVM from Active Directory. Then reattempt to join your SVM to a different Active Directory.

이 문제를 해결하려면 다음과 같이 실행합니다.

1. NetApp ONTAP CLI를 사용하여 현재 Active Directory에서 SVM의 조인을 해제합니다. 자세한 내용은 NetApp ONTAP CLI를 사용하여 SVM에서 Active Directory 조인 해제 섹션을 참조하세요.
2. AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 새 AD에 다시 조인해 봅니다.

SVM의 NetBIOS 이름이 이미 사용 중이기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음

자체 관리형 AD에 조인된 SVM을 생성하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory. This is because the NetBIOS (computer) name you specified is already in-use in your Active Directory. To fix this problem, pick a NetBIOS name for your SVM that is not in use in your Active Directory., specifying a NetBIOS (computer) Then reattempt to join your SVM to your Active Directory.

이 문제를 해결하려면 AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다. SVM에는 고유하고 Active Directory에서 아직 사용되고 있지 않은 NetBIOS 이름을 사용해야 합니다.

Amazon FSx가 Active Directory 도메인 컨트롤러와 통신할 수 없음

자체 관리형 AD에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to communicate with your Active Directory. To fix this problem, ensure that network traffic is allowed between Amazon FSx and your domain controllers. Then reattempt to join your SVM to your Active Directory.

이 문제를 해결하려면 다음과 같이 실행합니다.

1. 네트워크 구성 요구 사항에 설명된 요구 사항을 검토하고 Amazon FSx와 AD 간의 네트워크 통신이 가능하도록 필요한 사항을 변경합니다.
2. Amazon FSx가 AD와 통신할 수 있게 되면 AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다.

포트 요구 사항 또는 서비스 계정 권한이 충족되지 않아 Amazon FSx가 Active Directory에 연결할 수 없음

자체 관리형 AD에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory. This is due to either the port requirements for your Active Directory not being met, or the service account provided not having permissions to join the storage virtual machine to the domain with the specified organization unit. To fix this problem, update your storage virtual machine's Active Directory configuration after resolving any permissions issues with ports and service accounts, as recommended in the Amazon FSx user guide.

이 문제를 해결하려면 다음과 같이 실행합니다.

1. 네트워크 구성 요구 사항에 설명된 요구 사항을 검토하고 네트워킹 요구 사항을 충족하도록 필요한 사항을 변경하고 필요한 포트에서 통신이 활성화되도록 해야 합니다.
2. Active Directory 서비스 계정 요구 사항에 설명된 서비스 계정 요구 사항을 검토합니다. 서비스 계정에 지정된 조직 단위를 사용하여 SVM을 AD 도메인에 조인하는 데 필요한 위임된 권한이 있도록 해야 합니다.
3. 포트 권한 또는 서비스 계정을 변경한 후에는 AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다.

서비스 계정 보안 인증이 유효하지 않기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory domain controller(s) because the service account credentials provided are invalid. To fix this problem, update your storage virtual machine's Active Directory configuration with a valid service account.

이 문제를 해결하려면 AWS Management ConsoleAWS CLI및 API를 사용하여 기존 SVM Active Directory 구성 업데이트에 설명된 절차를 사용하여 SVM의 서비스 계정 보안 인증 정보를 업데이트합니다. 서비스 계정 사용자 이름을 입력할 때는 사용자 이름(예: `ServiceAcct`)만 포함하고 도메인 접두사(예:`corp.com\ServiceAcct`) 또는 도메인 접미사(예: `ServiceAcct@corp.com`)는 포함하지 않아야 합니다. 서비스 계정 사용자 이름(예: `CN=ServiceAcct,OU=example,DC=corp,DC=com`)을 입력할 때 고유 이름(DN)을 사용하지 않습니다.

서비스 계정 보안 인증이 충분하지 않기 때문에 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory domain controller(s). 이는 Active Directory에 대한 충족되지 않은 포트 요구 사항 또는 제공된 서비스 계정에 지정된 조직 단위를 사용하여 스토리지 가상 머신을 도메인에 조인할 권한이 없기 때문입니다.

이 문제를 해결하려면 제공한 서비스 계정에 필요한 권한을 위임해야 합니다. 서비스 계정은 파일 시스템에 조인하려는 도메인의 OU에서 컴퓨터 객체를 만들고 삭제할 수 있어야 합니다. 또한 서비스 계정에는 최소한 다음 작업을 수행할 수 있는 권한이 있어야 합니다.

- 암호 재설정

- 계정의 데이터 읽기 및 쓰기 제한
- 검증된 DNS 호스트 이름 쓰기 기능
- 검증된 서비스 보안 주체 이름 쓰기 기능
- 컴퓨터 객체를 생성하고 삭제할 수 있는 기능
- 계정 제한 사항을 읽고 쓸 수 있는 검증된 기능

올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Active Directory 서비스 계정 요구 사항 및 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

Amazon FSx가 Active Directory DNS 서버 또는 도메인 컨트롤러와 통신할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to communicate with your Active Directory. This is because Amazon FSx can't reach the DNS servers provided or domain controllers for your domain. To fix this problem, update your storage virtual machine's Active Directory configuration with valid DNS servers and a networking configuration that allows traffic to flow from the storage virtual machine to the domain controller.

이 문제를 해결하려면 다음 절차에 따릅니다.

1. 지리적 제한이나 방화벽으로 인해 Active Directory의 일부 도메인 컨트롤러에만 연결할 수 있는 경우 기본 도메인 컨트롤러를 추가할 수 있습니다. Amazon FSx는 이 옵션을 사용하여 기본 도메인 컨트롤러에 연락을 시도합니다. 다음과 같이 `vserver cifs domain preferred-dc add` NetApp ONTAP CLI 명령을 사용하여 기본 도메인 컨트롤러를 추가합니다.

   a. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.

   b. 다음 명령을 입력합니다. 여기서

   - `-vserver vserver_name`은 스토리지 가상 머신(SVM) 이름을 지정합니다.

- `-domain domain_name`은 지정된 도메인 컨트롤러가 속한 도메인의 정규화된 Active Directory 이름(FQDN)을 지정합니다.
- `-preferred-dc IP_address,…` 는 기본 도메인 컨트롤러의 하나 이상의 IP 주소를 원하는 순서에 따라 쉼표로 구분된 목록으로 지정합니다.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vserver_name -
domain domain_name -preferred-dc IP_address, …+
```

다음 명령은 SVM vs1의 SMB 서버가 cifs.lab.example.com 도메인에 대한 외부 액세스를 관리하는 데 사용하는 기본 도메인 컨트롤러 목록에 도메인 컨트롤러 172.17.102.25 및 172.17.102.24를 추가합니다.

```
FsxId123456789::> vserver cifs domain preferred-dc add -vserver vs1 -domain
 cifs.lab.example.com -preferred-dc 172.17.102.25,172.17.102.24
```

2. DNS를 사용하여 도메인 컨트롤러를 확인할 수 있는지 확인합니다. `vserver services access-check dns forward-lookup` NetApp ONTAP CLI 명령을 사용하여 지정된 DNS 서버의 조회 또는 vserver의 DNS 구성을 기반으로 호스트 이름의 IP 주소를 반환합니다.

   a. ONTAP CLI에 액세스하려면 다음 명령을 실행하여 Amazon FSx for NetApp ONTAP 파일 시스템 또는 SVM의 관리 포트에 SSH 세션을 설정합니다. *`management_endpoint_ip`*를 파일 시스템의 관리 포트의 IP 주소로 바꿉니다.

   ```
   [~]$ ssh fsxadmin@management_endpoint_ip
   ```

   자세한 내용은 ONTAP CLI를 사용한 파일 시스템 관리 섹션을 참조하세요.

   b. 다음 명령을 사용하여 ONTAP CLI 고급 모드로 들어갑니다.

   ```
   FsxId123456789::> set adv
   ```

   c. 다음 명령을 입력합니다. 여기서

   - `-vserver vserver_name`은 스토리지 가상 머신(SVM) 이름을 지정합니다.
   - `-hostname host_name`은 DNS 서버에서 조회할 호스트 이름을 지정합니다.
   - `-node node_name` 은 명령이 실행되는 노드의 이름을 지정합니다.

- `-lookup-type`은 DNS 서버에서 조회할 IP 주소 유형을 지정합니다. 기본값은 `all`입니다.

```
FsxId123456789::> vserver services access-check dns forward-lookup \
-vserver vserver_name -node node_name \
-domains domain_name -name-servers dns_server_ip_address \
-hostname host_name
```

3. SVM을 AD에 연결할 때 필요한 정보를 검토합니다.
4. SVM을 AD에 조인할 때의 네트워킹 요구 사항을 검토합니다.
5. 네트워크 구성 요구 사항에 설명된 절차를 사용하여 AD DNS 서버의 올바른 IP 주소를 사용하여 SVM의 AD 구성을 업데이트합니다.

잘못된 Active Directory 도메인 이름 때문에 Amazon FSx가 Active Directory와 통신할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx has detected the provided FQDN is invalid. To fix this problem, update your storage virtual machine's Active Directory configuration with an FQDN that adheres to configuration requirements.

이 문제를 해결하려면 다음 절차에 따릅니다.

1. SVM을 Active Directory에 조인할 때 필요한 정보에 설명된 온프레미스 Active Directory 이름 요구 사항을 검토하고 조인하려는 AD가 해당 요구 사항을 준수하도록 해야 합니다.
2. AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다. AD 도메인의 FQDN에 올바른 형식을 사용해야 합니다.

서비스 계정이 SVM Active Directory 구성에 지정된 관리자 그룹에 액세스할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to apply your Active Directory configuration. This is because the administrators group you provided either doesn't exist or isn't accessible to the service account you provided.

To fix this problem, ensure that your networking configuration allows traffic from the SVM to your Active Directory's domain controller(s) and DNS servers. Then update your SVM's Active Directory configuration, providing your Active Directory's DNS servers and, specifying an administrators group in the domain that is accessible to the service account provided.

이 문제를 해결하려면 다음과 같이 실행합니다.

1. SVM에서 관리 작업을 수행하기 위한 도메인 그룹 제공에 대한 정보를 검토합니다. AD 도메인 관리자 그룹의 올바른 이름을 사용하고 있어야 합니다.
2. AWS Management ConsoleAWS CLI 및 API를 사용하여 Active Directory에 SVMs 조인에 설명된 절차에 따라 SVM을 AD에 다시 조인해 봅니다.

지정된 조직 단위가 존재하지 않거나 액세스할 수 없어 Amazon FSx가 Active Directory 도메인 컨트롤러에 연결할 수 없음

자체 관리형 Active Directory에 SVM을 조인하는 데 실패하고 다음과 같은 오류 메시지가 표시됩니다.

Amazon FSx is unable to establish a connection with your Active Directory. This is because the organizational unit you specified either doesn't exist or isn't accessible to the service account provided. To fix this problem, update your storage virtual machine's Active Directory configuration, specifying an organizational unit to which the service account has permissions to join.

이 문제를 해결하려면 다음과 같이 실행합니다.

1. SVM을 AD에 조인하기 위한 사전 조건을 검토합니다.
2. SVM을 AD에 조인할 때 필요한 정보를 검토합니다.
3. 올바른 조직 단위와 함께 이 절차를 사용하여 SVM을 AD에 다시 조인해 봅니다.

스토리지 가상 머신 또는 볼륨을 삭제할 수 없음

각 FSx for ONTAP 파일 시스템은 하나 이상의 스토리지 가상 머신(SVM)을 포함할 수 있으며 각 SVM은 하나 이상의 볼륨을 포함할 수 있습니다. 리소스를 삭제할 때는 먼저 해당 하위 항목이 모두 삭제되어 있어야 합니다. 예를 들어, SVM을 삭제하기 전에 먼저 SVM에서 루트가 아닌 모든 볼륨을 삭제해야 합니다.

> **Important**
>
> Amazon FSx 콘솔, API 및 CLI를 사용해서만 스토리지 가상 머신을 삭제할 수 있습니다. 볼륨에 Amazon FSx 백업이 활성화된 경우에만 Amazon FSx 콘솔, API 또는 CLI를 사용하여 볼륨을 삭제할 수 있습니다.

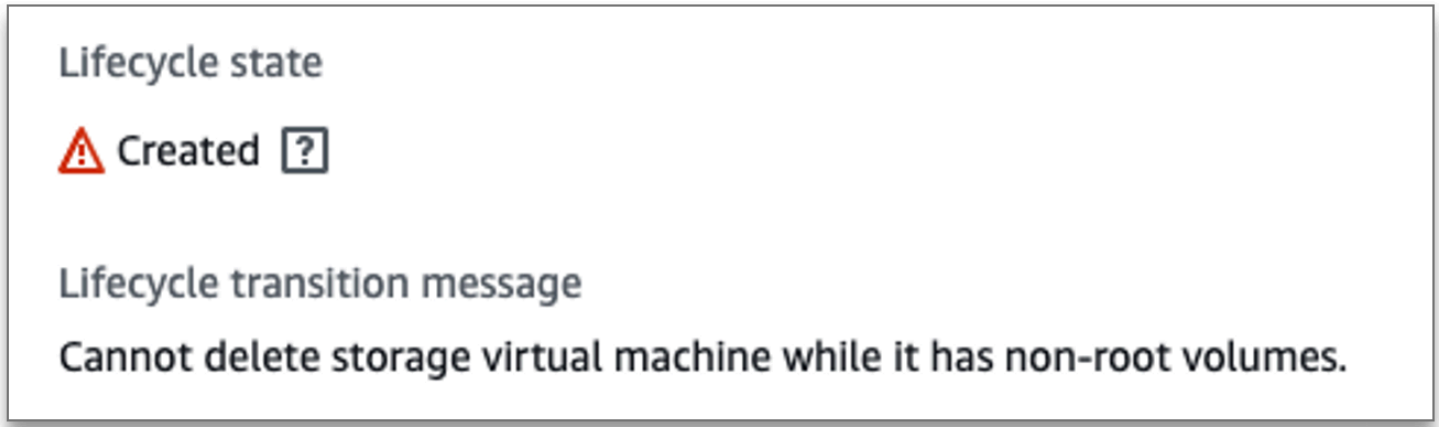
데이터 및 구성을 보호하기 위해 Amazon FSx는 특정 상황에서 SVM 및 볼륨 삭제를 방지합니다. SVM 또는 볼륨을 삭제하려고 하는데 삭제 요청이 성공하지 못하면 Amazon FSx는 AWS 콘솔, AWS Command Line Interface (AWS CLI) 및 API에서 리소스가 삭제되지 않은 이유에 대한 정보를 제공합니다. 삭제 실패 원인을 해결한 후 삭제 요청을 재시도할 수 있습니다.

주제

실패한 삭제 식별

Amazon FSx SVM 또는 볼륨을 삭제하면 일반적으로 리소스가 Amazon FSx 콘솔, CLI 및 API에서 사라지기까지 최대 몇 분 동안 리소스의 `Lifecycle` 상태가 `DELETING`으로 전환됩니다.

리소스를 삭제하려고 할 때 `Lifecycle` 상태가 `DELETING`으로 전환되었다가 다시 `CREATED`로 되돌아오는 경우, 이 동작은 리소스가 성공적으로 삭제되지 않았음을 나타냅니다. 이 경우 Amazon FSx는 콘솔의 `CREATED` 수명 주기 상태 옆에 알림 아이콘을 보고합니다. 알림 아이콘을 선택하면 다음 예제와 같이 삭제 실패 이유가 표시됩니다.



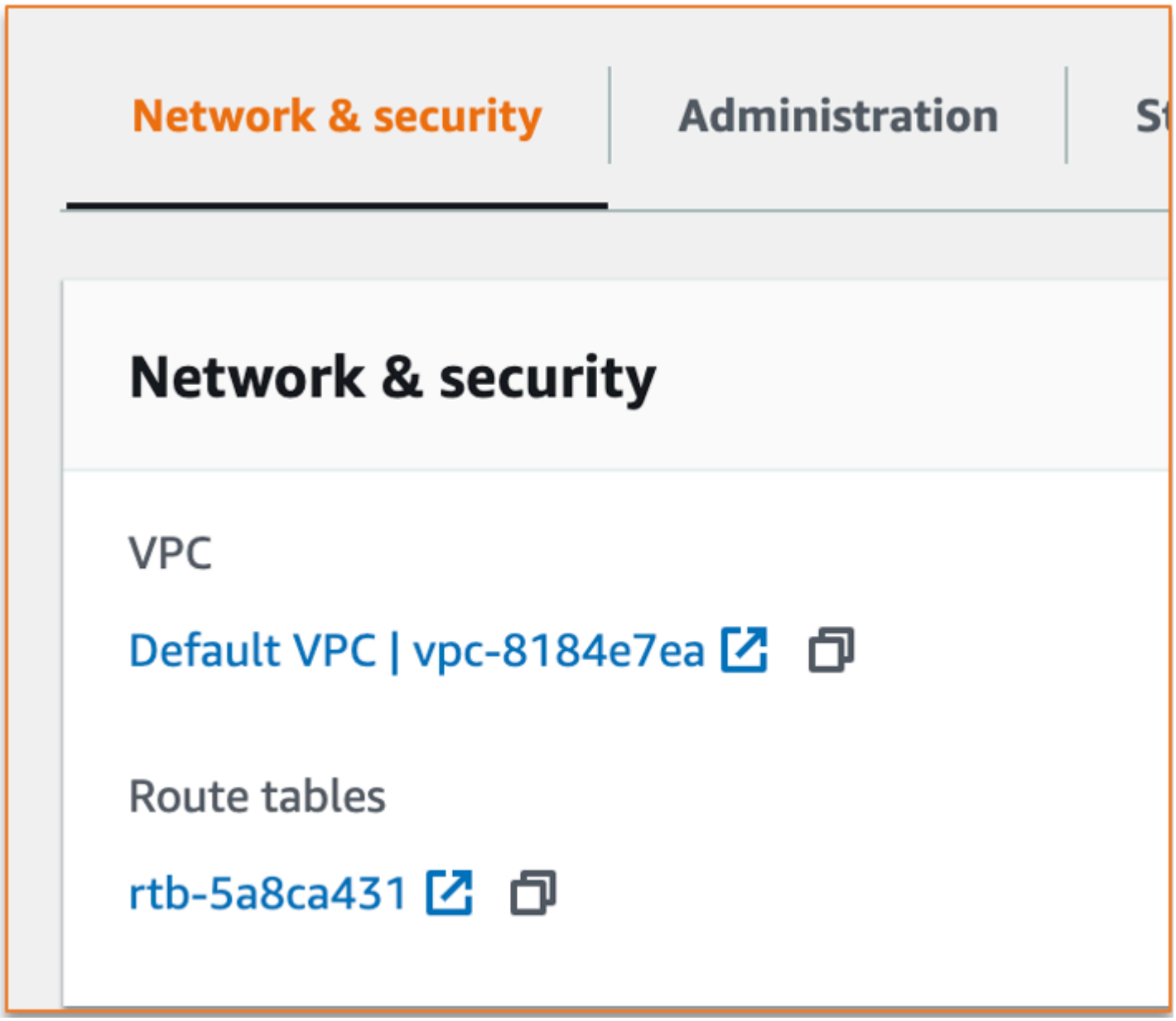
Amazon FSx가 SVM 및 볼륨 삭제를 방지하는 가장 일반적인 이유가 이러한 문제를 해결하는 방법에 대한 단계별 지침과 함께 다음 섹션에 나와 있습니다.

SVM 삭제: 라우팅 테이블에 액세스할 수 없음

각 FSx for ONTAP 파일 시스템은 하나 이상의 라우팅 테이블 항목을 생성하여 가용 영역 전체에서 자동 장애 조치 및 페일백을 제공합니다. 기본적으로 이러한 라우팅 테이블 항목은 VPC의 기본 라우팅 테이블에 생성됩니다. 선택적으로 FSx for ONTAP 인터페이스가 생성될 수 있는 기본이 아닌 라우팅 테이블을 하나 이상 지정할 수 있습니다. Amazon FSx는 파일 시스템과 연결된 각 라우팅 테이블에 `AmazonFSx` 태그를 지정하며, 이 태그를 제거하면 Amazon FSx가 리소스를 삭제하지 못하게 됩니다. 이 상황이 발생하면 다음과 같은 `LifecycleTransitionReason`이 표시됩니다.

```
Amazon FSx is unable to complete the requested storage virtual machine
operation because of an inability to access one or more of the route tables
associated with your file system. Please contact ##.
```

Amazon FSx 콘솔에서 파일 시스템의 요약 페이지로 이동하면 네트워크 및 보안 탭에서 파일 시스템의 라우팅 테이블을 찾을 수 있습니다.



라우팅 테이블 링크를 선택하면 라우팅 테이블로 이동합니다. 다음으로, 파일 시스템과 연결된 각 라우팅 테이블에 다음 키-값 페어로 태그가 지정되어 있는지 확인합니다.

```
Key: AmazonFSx
Value: ManagedByAmazonFSx
```

이 태그가 없는 경우 태그를 다시 생성한 다음 SVM을 다시 삭제해 봅니다.

SVM 삭제: 피어 관계

피어 관계에 속하는 SVM 또는 볼륨을 삭제하려는 경우 SVM 또는 볼륨을 삭제하기 전에 먼저 피어 관계를 삭제해야 합니다. 이 요구 사항은 피어링된 SVM이 비정상 상태가 되는 것을 방지합니다. 피어 관계로 인해 SVM을 삭제할 수 없는 경우 다음 `LifecycleTransitionReason`이 표시됩니다.

Amazon FSx is unable to delete the storage virtual machine because it is part of a SVM peer or transition peer relationship. Please delete the relationship and retry.

ONTAP CLI를 통해 SVM 피어 관계를 삭제할 수 있습니다. ONTAP CLI에 액세스하려면 ONTAP CLI를 사용한 파일 시스템 관리의 단계를 따릅니다. ONTAP CLI를 사용하여 다음 단계를 수행합니다.

1. 다음 명령을 사용하여 SVM 피어 관계를 점검합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

   ```
   FsxId123456789::> vserver peer show -vserver svm_name
   ```

   이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다.

   ```
               Peer        Peer                            Peering        Remote
   Vserver     Vserver     State        Peer Cluster       Applications   Vserver
   ----------- ----------- ------------ ----------------- -------------- ---------
   svm_name    test2       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   svm_name    test3       peered       FsxId02d81fef0d84734b6
                                                          snapmirror     fsxDest
   2 entries were displayed.
   ```

2. 다음 명령을 사용하여 각 SVM 피어 관계를 삭제합니다. *svm_name* 및 *remote_svm_name*을 사용자의 실제 값으로 바꿉니다.

```
FsxId123456789abcdef::> vserver peer delete -vserver svm_name -peer-
vserver remote_svm_name
```

이 명령이 제대로 실행되면 다음과 같은 출력이 표시됩니다.

```
Info: 'vserver peer delete' command is successful.
```

SVM 또는 볼륨 삭제: SnapMirror

피어 관계를 먼저 삭제하지 않으면 피어 관계가 있는 SVM을 삭제할 수 없는 것처럼(SVM 삭제: 피어 관계 참조), SnapMirror 관계를 먼저 삭제하지 않으면 SnapMirror 관계가 있는 SVM을 삭제할 수 없습니다. SnapMirror 관계를 삭제하려면 ONTAP CLI를 사용하여 SnapMirror 관계의 대상이 되는 파일 시스템에서 다음 단계를 수행합니다. ONTAP CLI에 액세스하려면 ONTAP CLI를 사용한 파일 시스템 관리의 단계를 따릅니다.

> **Note**
>
> Amazon FSx 백업은 SnapMirror를 사용하여 파일 시스템 볼륨의 특정 시점의 증분 백업을 생성합니다. ONTAP CLI에서 백업에 대한 이 SnapMirror 관계를 삭제할 수 없습니다. 하지만 AWS CLI, API 또는 콘솔을 통해 볼륨을 삭제하면 이 관계가 자동으로 삭제됩니다.

1. 다음 명령을 사용하여 대상 파일 시스템의 SnapMirror 관계를 나열합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

   ```
   FsxId123456789abcdef::> snapmirror show -vserver svm_name
   ```

   이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다.

   ```
   Source            Destination    Mirror  Relationship   Total             Last
   Path        Type  Path           State   Status         Progress  Healthy Updated
   ----------- ---- ------------    ------- -------------- --------- ------- --------
   sourceSvm:sourceVol
               XDP  destSvm:destVol Snapmirrored
                                       Idle           -         true    -
   ```

2. 대상 파일 시스템에서 다음 명령을 실행하여 SnapMirror 관계를 삭제합니다.

```
FsxId123456789abcdef::> snapmirror release -destination-path destSvm:destVol -
source-path sourceSvm:sourceVol -force true
```

SVM 삭제: Kerberos 지원 LIF

Kerberos가 활성화된 논리 인터페이스(LIF)가 있는 SVM을 삭제하려는 경우 SVM을 삭제하기 전에 먼저 해당 LIF에서 Kerberos를 비활성화해야 합니다.

ONTAP CLI를 통해 LIF에서 Kerberos를 비활성화할 수 있습니다. ONTAP CLI에 액세스하려면 ONTAP CLI를 사용한 파일 시스템 관리의 단계를 따릅니다.

1. 다음 명령을 사용하여 ONTAP CLI에서 진단 모드로 들어갑니다.

   ```
   FsxId123456789abcdef::> set diag
   ```

   계속할지 묻는 메시지가 표시되면 **y**를 입력합니다.

   ```
   Warning: These diagnostic commands are for use by NetApp personnel only.
   Do you want to continue? {y|n}: y
   ```

2. 어떤 인터페이스에 Kerberos가 활성화되어 있는지 확인합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

   ```
   FsxId123456789abcdef::> kerberos interface show -vserver svm_name
   ```

   이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다.

   ```
   (vserver nfs kerberos interface show)
                  Logical
   Vserver        Interface     Address         Kerberos SPN
   -------------- ------------- --------------- -------- ----------------------
   svm_name       nfs_smb_management_1
                                10.19.153.48    enabled
   5 entries were displayed.
   ```

3. 다음 명령을 사용하여 Kerberos LIF를 비활성화합니다. *svm_name*을 SVM의 이름으로 바꿉니다. 이 SVM을 Active Directory에 조인하는 데 사용한 Active Directory 사용자 이름과 암호를 제공해야 합니다.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1
```

이 명령이 제대로 실행되면 다음과 같은 출력이 표시됩니다. 이 SVM을 Active Directory에 조인하는 데 사용한 Active Directory 사용자 이름과 암호를 제공합니다. 계속할지 묻는 메시지가 표시되면 **y**를 입력합니다.

```
(vserver nfs kerberos interface disable)
Username: admin
Password: *************

Warning: This command deletes the service principal name from the machine account
 on the KDC.
Do you want to continue? {y|n}: y

Disabled Kerberos on LIF "nfs_smb_management_1" in Vserver "svm_name".
```

4. 다음 명령을 사용하여 SVM에서 Kerberos가 비활성화되었는지 확인합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

```
FsxId123456789abcdef::> kerberos interface show -vserver svm_name
```

이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다.

```
(vserver nfs kerberos interface show)
               Logical
Vserver        Interface     Address         Kerberos SPN
-------------- ------------- --------------- -------- ----------------------
svm_name       nfs_smb_management_1
                             10.19.153.48    disabled
5 entries were displayed.
```

5. 인터페이스가 로 표시되면 AWS CLI`disabled`, API 또는 콘솔을 통해 SVM을 다시 삭제해 보십시오.

이전 명령을 사용하여 LIF를 삭제할 수 없는 경우 다음 명령을 사용하여 Kerberos LIF를 강제 삭제할 수 있습니다. *svm_name*을 SVM의 이름으로 바꿉니다.

> **Important**
>
> 다음 명령을 실행하면 Active Directory에서 SVM의 컴퓨터 객체가 분리될 수 있습니다.

```
FsxId123456789abcdef::> kerberos interface disable -vserver svm_name -lif
 nfs_smb_management_1 -force true
```

이 명령이 제대로 실행되면 다음과 비슷한 출력이 표시됩니다. 계속할지 묻는 메시지가 표시되면 **y**를 입력합니다.

```
(vserver nfs kerberos interface disable)

Warning: Kerberos configuration for LIF "nfs_smb_management_1" in Vserver
 "svm_name" will be deleted.
The corresponding account on the KDC will not be deleted. Do you want to continue?
 {y|n}: y
```

SVM 삭제: 기타 이유

FSx for ONTAP SVM은 Active Directory에 조인할 때 Active Directory에 컴퓨터 객체를 생성합니다. 경우에 따라 ONTAP CLI를 사용하여 Active Directory에서 SVM의 조인을 수동으로 해제할 수도 있습니다. ONTAP CLI에 액세스하려면 ONTAP CLI를 사용한 파일 시스템 관리의 단계를 따르고 `fsxadmin` 보안 인증 정보를 사용하여 파일 시스템 수준에서 ONTAP CLI에 로그인합니다. ONTAP CLI를 사용하여 다음 단계를 수행하여 Active Directory에서 SVM의 연결을 해제합니다.

> **Important**
>
> 이 절차를 수행하면 Active Directory에서 SVM의 컴퓨터 객체가 분리될 수 있습니다.

1. 다음 명령을 사용하여 ONTAP CLI의 고급 모드로 들어갑니다.

```
FsxId123456789abcdef::> set adv
```

이 명령을 실행하면 다음과 같은 출력이 표시됩니다. 계속하려면 **y**를 입력합니다.

```
Warning: These advanced commands are potentially dangerous; use them only when
      directed to do so by NetApp personnel.
      Do you want to continue? {y|n}: y
```

2. 다음 명령을 사용하여 Active Directory의 DNS를 삭제합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update record
 delete -vserver svm_name -lif nfs_smb_management_1
```

> **Note**
>
> DNS 레코드가 이미 삭제되었거나 DNS 서버에 연결할 수 없는 경우 이 명령은 실패합니다. 이 문제가 발생하면 다음 단계를 계속 진행합니다.

3. 다음 명령을 사용하여 DNS를 비활성화합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

```
FsxId123456789abcdef::> vserver services name-service dns dynamic-update modify -
vserver svm_name -is-enabled false -use-secure false
```

이 명령이 제대로 실행되면 다음과 같은 출력이 표시됩니다.

```
Warning: DNS updates for Vserver "svm_name" are now disabled.
     Any LIFs that are subsequently modified or deleted
     can result in a stale DNS entry on the DNS server,
     even when DNS updates are enabled again.
```

4. Active Directory에서 디바이스의 조인을 해제합니다. *svm_name*을 SVM의 이름으로 바꿉니다.

```
FsxId123456789abcdef::> vserver cifs delete -vserver svm_name
```

이 명령을 실행하면 다음과 같은 출력이 표시됩니다. 여기서 *CORP.EXAMPLE.COM*은 도메인 이름으로 바뀝니다. 메시지가 표시되면 사용자 이름과 암호를 입력합니다. 서버를 삭제할지 묻는 메시지가 표시되면 **y**를 입력합니다.

```
In order to delete an Active Directory machine account for the CIFS server,
you must supply the name and password of a Windows account with sufficient
privileges to remove computers from the "CORP.EXAMPLE.COM" domain.
```

```
Enter the user name: admin
Enter the password:
Warning: There are one or more shares associated with this CIFS server
     Do you really want to delete this CIFS server and all its shares? {y|n}: y
Warning: Unable to delete the Active Directory computer account for this CIFS
 server.
     Do you want to continue with CIFS server deletion anyway? {y|n}: y
```

볼륨 삭제: FlexCache 관계

먼저 캐시 관계를 삭제하지 않으면 FlexCache 관계의 원본 볼륨인 볼륨을 삭제할 수 없습니다. FlexCache 관계가 있는 볼륨을 확인하려면 ONTAP CLI를 사용할 수 있습니다. ONTAP CLI에 액세스하려면 ONTAP CLI를 사용한 파일 시스템 관리의 단계를 따릅니다.

1. 다음 명령을 사용하여 FlexCache 관계를 점검합니다.

```
FsxId123456789abcdef::> volume flexcache origin show-caches
```

2. 다음 명령을 사용하여 모드 캐시 관계를 삭제합니다. *dest_svm_name* 및 *dest_vol_name*을 사용자의 실제 값으로 바꿉니다.

```
FsxId123456789abcdef::> volume flexcache delete -vserver dest_svm_name -
volume dest_vol_name
```

3. 캐시 관계를 삭제한 후 AWS CLI, API 또는 콘솔을 통해 SVM을 다시 삭제해 봅니다.

볼륨이 **MISCONFIGURED** 상태임

다음 주제에 설명된 대로 ONTAP 볼륨이 MISCONFIGURED 상태가 되는 잠재적 원인은 여러 가지가 있습니다.

볼륨이 98% 이상 찼습니다.

파일 시스템에는 현재 98%를 초과하는 볼륨이 포함되어 있습니다. 볼륨 사용률은 지속적으로 95%를 초과하지 않는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에 볼륨의 공간을 확보하지 않으면 Amazon FSx는 볼륨에 대한 기회 잠금을 비활성화하여 기존 'oplocks'를 차단합니다. Amazon FSx는 패치 적용 프로세스가 완료된 후 볼륨에서 oplock을 다시 활성화합니다. 이를 방지하려면 볼륨의 스토리지 용량 사용률을 98% 미만으로 줄이세요. 이를 달성하는 몇 가지 방법은 다음과 같습니다.

- 볼륨 크기를 늘립니다.
- 불필요한 데이터 삭제.
- 불필요한 스냅샷 삭제.

자세한 정보는 스토리지 용량 업데이트 및 스냅샷 삭제 섹션을 참조하세요.

오프라인 볼륨에 iSCSI LUN 또는 NVMe/TCP 네임스페이스가 있음

파일 시스템은 현재 오프라인 상태인 볼륨을 호스팅하며, 해당 볼륨에는 iSCSI LUN, NVMe/TCP 네임스페이스 또는 둘 다 포함됩니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인 상태로 전환하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인 상태로 전환합니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

오프라인 볼륨이 FlexCache 오리진임

파일 시스템에는 오프라인 상태의 FlexCache 오리진 볼륨이 포함되어 있습니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인 상태로 전환하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인 상태로 전환합니다. 이 시간 동안 캐시 볼륨의 데이터와 함께 FlexCache 오리진 볼륨에 데이터가 다시 기록될 수 있습니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

오프라인 볼륨이 SnapMirror 관계의 일부임

파일 시스템은 현재 오프라인 상태인 볼륨을 호스팅하며 해당 볼륨은 SnapMirror 소스 또는 대상입니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인화하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인화하고 SnapMirror 관계를 일시 중지합니다. 이 시간 동안 SnapMirror 소스 볼륨의 데이터를 사용하여 SnapMirror 대상 볼륨에 데이터가 기록될 수 있습니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

제한된 볼륨에 iSCSI LUN 또는 NVMe/TCP 네임스페이스 포함

파일 시스템은 현재 제한된 상태의 볼륨을 호스팅하며, 해당 볼륨에는 iSCSI LUN, NVMe/TCP 네임스페이스 또는 둘 다 포함됩니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인화하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인화합니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

제한된 볼륨이 FlexCache 오리진입니다.

파일 시스템에는 제한된 상태의 FlexCache 오리진 볼륨이 포함되어 있습니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에이 볼륨을 온라인화하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인화합니다. 이 시간 동안 캐시 볼륨의 데이터와 함께 FlexCache 오리진 볼륨에 데이터가 다시 기록될 수 있습니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

제한된 볼륨은 SnapMirror 관계의 일부입니다.

파일 시스템은 현재 제한된 상태의 볼륨을 호스팅하며 해당 볼륨은 SnapMirror 소스 또는 대상입니다. 볼륨을 지속적으로 온라인 상태로 유지하는 것이 좋습니다. 파일 시스템의 다음 유지 관리 기간 전에 이 볼륨을 온라인화하지 않으면 Amazon FSx는 패치 작업 기간 동안이 볼륨을 일시적으로 온라인화하고 SnapMirror 관계를 일시 중지합니다. 이 시간 동안 SnapMirror 소스 볼륨의 데이터를 사용하여 SnapMirror 대상 볼륨에 데이터가 기록될 수 있습니다. 이를 방지하려면 온라인으로 하거나 볼륨을 삭제하십시오.

오프라인 볼륨을 다시 온라인 상태로 전환하려면 다음 예제와 같이 `volume online` ONTAP CLI 명령을 사용합니다. SVM(Vserver)이 하나만 있는 경우 `-vserver` 파라미터를 지정할 필요가 없습니다.

```
FsxID-abcdef123456::> volume online -volume volume_name -vserver svm_name

Volume 'vs1:vol1' is now online.
```

볼륨의 스토리지 용량이 부족합니다.

볼륨 공간이 부족한 경우 여기에 표시된 절차를 사용하여 상황을 진단하고 해결할 수 있습니다.

주제

- 볼륨 스토리지 용량이 어떻게 사용되고 있는지 확인
- 볼륨의 스토리지 용량 늘리기
- 볼륨 자동 크기 조정 사용
- 파일 시스템의 기본 스토리지가 가득 참
- 스냅샷 삭제
- 볼륨의 최대 파일 용량 늘리기

볼륨 스토리지 용량이 어떻게 사용되고 있는지 확인

`volume show-space` NetApp ONTAP CLI 명령을 사용하여 볼륨의 스토리지 용량이 어떻게 사용되고 있는지 확인할 수 있습니다. 이 정보는 볼륨 스토리지 용량을 재확보하거나 보존하는 방법을 결정하는 데 도움이 될 수 있습니다. 자세한 내용은 볼륨의 저장 용량을 모니터링하려면 (콘솔) 다음과 같이 하세요. 섹션을 참조하세요.

볼륨의 스토리지 용량 늘리기

Amazon FSx 콘솔 AWS CLI및 Amazon FSx API를 사용하여 볼륨의 스토리지 용량을 늘릴 수 있습니다. 용량을 늘려 볼륨을 업데이트하는 방법에 대한 자세한 내용은 볼륨 업데이트 섹션을 참조하세요.

또는 `volume modify` NetApp ONTAP CLI 명령을 사용하여 볼륨의 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 볼륨의 저장 용량을 변경하려면(콘솔) 다음과 같이 하세요. 섹션을 참조하세요.

볼륨 자동 크기 조정 사용

볼륨 자동 크기 조정 기능을 사용하면 볼륨이 지정된 양만큼 또는 사용된 공간 임계값에 도달할 때 지정된 크기로 자동 증가하도록 할 수 있습니다. `volume autosize` NetApp ONTAP CLI 명령을 사용하여 FSx for ONTAP의 기본 볼륨 유형인 FlexVol 볼륨 유형에 대해 이 작업을 수행할 수 있습니다. 자세한 내용은 자동 크기 조정 사용 섹션을 참조하세요.

파일 시스템의 기본 스토리지가 가득 참

FSx for ONTAP 파일 시스템의 기본 스토리지가 가득 차면 볼륨에 사용 가능한 스토리지 용량이 충분하다고 표시되더라도 파일 시스템의 볼륨에 더 이상 데이터를 추가할 수 없습니다. Amazon FSx 콘솔의 파일 시스템 세부 정보 페이지에 있는 모니터링 및 성능 탭에서 사용 가능한 기본 스토리지 용량을 확인할 수 있습니다. 자세한 내용은 SSD 스토리지 사용률 모니터링 섹션을 참조하세요.

이 문제를 해결하기 위해 파일 시스템의 기본 스토리지 계층 크기를 늘릴 수 있습니다. 자세한 내용은 파일 시스템 SSD 스토리지 및 IOPS 업데이트 섹션을 참조하세요.

스냅샷 삭제

스냅샷은 기본 스냅샷 정책을 사용하여 볼륨에서 기본적으로 활성화됩니다. 스냅샷은 볼륨 루트의 `.snapshot` 디렉터리에 저장됩니다. 스냅샷과 관련된 볼륨 스토리지 용량을 다음과 같은 방법으로 관리할 수 있습니다.

- 스냅샷 수동 삭제 - 스냅샷을 수동으로 삭제하여 스토리지 용량을 재확보합니다.

- 스냅샷 자동 삭제 정책 생성 - 기본 스냅샷 정책보다 더 적극적으로 스냅샷을 삭제하는 정책을 생성합니다.
- 자동 스냅샷 끄기 - 자동 스냅샷을 끄면 스토리지 용량을 절약할 수 있습니다.

스냅샷을 삭제할 때 삭제하려는 스냅샷 크기와 동일한 스토리지 양을 회수하지 않습니다. 볼륨 스냅샷 컴퓨팅 회수 가능 -vserver ONTAP CLI 명령을 사용하고 데이터를 사용하여 *svm_name*, *vol_name* 및 *snapshot_name*을 대체하여 스냅샷을 삭제할 때 회수할 수 있는 스토리지 양을 확인할 수 있습니다.

```
fsid8970abc52::> volume snapshot compute-reclaimable -vserver svm_name -volume vol_name
 -snapshot snapshot_name
A total of 667648 bytes can be reclaimed.
```

스냅샷을 삭제하고 스냅샷 정책을 관리하여 스토리지 용량을 절약하는 방법에 대한 자세한 내용은 스냅샷 삭제 섹션을 참조하세요.

볼륨의 최대 파일 용량 늘리기

사용 가능한 아이노드, 즉 파일 포인터 수가 모두 소모되면 FSx for ONTAP 볼륨의 파일 용량이 부족해질 수 있습니다. 기본적으로 볼륨에서 사용 가능한 아이노드 수는 볼륨 크기 32KiB당 1개입니다. 자세한 내용은 볼륨 파일 용량 단원을 참조하십시오.

볼륨의 아이노드 수는 볼륨의 스토리지 용량에 비례하여 최대 648GiB까지 증가합니다. 기본적으로 스토리지 용량이 648GiB 이상인 볼륨의 아이노드 수는 모두 21,251,126개로 동일합니다. 볼륨의 최대 파일 용량을 보려면 볼륨의 파일 용량 모니터링 섹션을 참조하세요.

648GiB보다 큰 볼륨을 생성하고 21,251,126개 이상의 아이노드를 포함하려는 경우 볼륨의 최대 파일 수를 수동으로 늘려야 합니다. 볼륨의 스토리지 용량이 부족한 경우 최대 파일 용량을 확인할 수 있습니다. 파일 용량이 거의 다 되었으면 수동으로 늘릴 수 있습니다. 자세한 내용은 볼륨의 최대 파일 수를 늘리려면(ONTAP CLI) 다음과 같이 하세요. 단원을 참조하십시오.

볼륨 용량이 부족하여 백업이 실패합니다.

볼륨의 자동 일일 백업은 다음 메시지와 함께 실패합니다.

```
Amazon FSx could not create a backup of your volume because the backup snapshot was
 deleted.
```

볼륨에 사용 가능한 스토리지 용량이 충분하지 않아 자동 일일 백업이 실패합니다. 이 조건을 완화하려면 볼륨의 스토리지 용량을 확보해야 합니다. 상황에 따라 다음 옵션 중 하나 이상을 사용하여 이 작업을 수행할 수 있습니다.

- 볼륨의 스토리지 용량 증가
- 볼륨의 스냅샷 예약 증가
- 스냅샷 자동 삭제 비활성화
- ONTAP CLI를 사용하여 백업 스냅샷을 삭제하지 마세요.

네트워크 문제 해결

네트워크 문제가 발생하는 경우 여기에 표시된 절차를 사용하여 문제를 진단할 수 있습니다.

패킷 추적을 캡처하려는 경우

패킷 추적은 레이어를 통해 목적지까지의 패킷 경로를 확인하는 프로세스입니다. 다음 NetApp ONTAP CLI 명령을 사용하여 패킷 추적 프로세스를 제어합니다.

- network tcpdump start – 패킷 추적 시작
- network tcpdump show - 현재 실행 중인 패킷 추적 표시
- network tcpdump stop – 실행 중인 패킷 추적 중지

이 명령은 파일 시스템에서 `fsxadmin` 역할을 담당하는 사용자가 사용할 수 있습니다.

파일 시스템에서 패킷 추적 캡처

1. 파일 시스템의 NetApp ONTAP CLI에 SSH를 설정하려면 Amazon FSx for NetApp ONTAP 사용 설명서의 NetApp ONTAP CLI 사용 섹션에 설명된 단계를 따릅니다.

   ```
   ssh fsxadmin@file-system-management-endpoint-ip-address
   ```

2. 다음 명령을 사용하여 ONTAP CLI에 진단 권한 수준을 입력합니다.

   ```
   ::> set diag
   ```

   계속할지 묻는 메시지가 표시되면 y를 입력합니다.

```
Warning: These diagnostic commands are for use by NetApp personnel only.
Do you want to continue? {y|n}: y
```

3. 파일 시스템에서 패킷 추적을 저장할 위치를 식별합니다. 볼륨은 온라인 상태여야 하며 유효한 정션 경로가 있는 네임스페이스에 마운트되어야 합니다. 다음 명령을 사용하여 해당 기준을 충족하는 볼륨이 있는지 점검합니다.

```
::*> volume show -junction-path !- -fields junction-path
vserver volume    junction-path
------- --------- -------------
fsx     test_vol1 /test_vol1
fsx     test_vol2 /test_vol2
fsx     test_vol2 /test_vol3
```

4. 최소한의 필수 인수를 사용하여 추적을 시작합니다. 다음을 바꿉니다.

   - *node_name*을 노드의 이름으로 바꿉니다(예: FsxId01234567890abcdef-01).
   - *svm_name*을 스토리지 가상 머신의 이름으로 바꿉니다(예: fsx).
   - *junction_path_name*을 볼륨의 이름으로 바꿉니다(예: test-vol1).

```
::*> debug network tcpdump start -node node_name -ipspace Default -pass-through "-i
 e0e -w /clus/svm_name/junction_path_name"
Info: Started network trace on interface "e0e"
Warning: Snapshots should be disabled on the tcpdump destination volume while
 packet traces are occurring. Use the
"volume modify -snapshot-policy none -vserver fsx -volume test_vol1" command to
 disable Snapshots on the
tcpdump destination volume.
```

> **Important**
>
> 패킷 추적은 e0e 인터페이스와 Default IP 공간에서만 캡처할 수 있습니다. FSx for ONTAP에서는 모든 네트워크 트래픽이 e0e 인터페이스를 사용합니다.

패킷 추적을 사용할 때는 다음 사항에 유의하세요.

- 패킷 추적을 시작할 때 추적 파일을 저장할 위치의 경로를 /clus/*svm_name*/*junction-path-name* 경로 이름형식으로 포함해야 합니다.
- 필요에 따라 패킷 추적의 파일 이름을 제공합니다. filter_name을 지정하지 않으면 *node-name_port-name _yyyymmdd_hhmmss*.trc 형식으로 자동으로 생성됩니다.
- 롤링 추적이 지정된 경우 filter_name에는 교체 시퀀스의 위치를 나타내는 숫자가 접미사로 붙습니다.
- ONTAP CLI는 다음과 같은 선택적 -pass-through 인수도 허용합니다.

```
-B, --buffer-size=<KiB>
-c <number_of_packets>
-C <file_size-mB>
-F <filter_expression_filename>
-G <rotate_seconds>
--time-stamp-precision {micro|nano}
-Q, --direction {in|out|inout}
-s, --snapshot-length=<bytes>
-U, --packet-buffered
-W <rotate_file_count>
<filter-expression>
```

- 필터 표현식에 대한 자세한 내용은 pcap-filter(7) 매뉴얼 페이지를 참조하세요.

5. 진행 중인 추적을 봅니다.

```
::*> debug network tcpdump show
Node                      IPspace  Port     Filename
------------------------  -------- -------- --------
FsxId123456789abcdef-01  Default  e0e      /clus/fsx/test_vol1/
FsxId123456789abcdef-01_e0e_20230605_181451.trc
```

6. 추적을 중지합니다.

```
::*> debug network tcpdump stop -node FsxId123456789abcdef-01 -ipspace Default -
port e0e
Info: Stopped network trace on interface "e0e"
```

7. 관리자 권한 수준으로 돌아갑니다.

```
::*> set -priv admin
::>
```

8. 패킷 추적에 액세스합니다.

   패킷 추적은 debug network tcpdump start 명령을 사용하여 지정한 볼륨에 저장되며 해당 볼륨에 해당하는 NFS 내보내기 또는 SMB 공유를 통해 액세스할 수 있습니다.

패킷 추적 캡처에 대한 자세한 내용은의 ONTAP 9.10+에서 디버그 네트워크 덤프를 사용하는 방법을 참조하세요NetApp Knowledge Base.

Amazon FSx for NetApp ONTAP의 문서 기록

- API 버전: 2018년 3월 1일
- 최종 설명서 업데이트: 2025년 6월 9일

아래 표에 Amazon FSx NetApp ONTAP 사용 설명서의 주요 변경 사항이 설명되어 있습니다. 설명서 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
FSx for ONTAP에서 Amazon Elastic VMware Service 지원	이제 FSx for ONTAP을 Amazon EVS의 외부 데이터 스토어로 사용할 수 있습니다. 자세한 내용은 FSx for ONTAP에서 Amazon Elastic VMware Service 사용을 참조하세요.	2025년 6월 9일
추가 AWS 리전 지원 추가	이제 아시아 태평양(도쿄) 및 아시아 태평양(뭄바이)에서 2세대(다중 AZ 2 및 단일 AZ 2) FSx for ONTAP 파일 시스템을 사용할 수 있습니다. 자세한 내용은 가용성 기준을 AWS 리전 참조하세요.	2025년 6월 2일
FlexCache 라이트백 모드에 대한 지원 추가	이제 FSx for ONTAP 볼륨이 FlexCache 쓰기-백 모드를 지원합니다. 자세한 내용은 를 사용하여 데이터 복제를 참조하세요FlexCache.	2025년 5월 28일
Amazon FSx에서 AmazonFSxFullAccess AWS 관리형 정책 업데이트	AmazonFSxFullAccess 관리형 정책이 `fsx:CreateAndAttachS3AccessPoint` , `fsx:DescribeS3AccessPointAt`	2025년 5월 28일

	tachments fsx:UpdateS3AccessPointAttachments, 및 fsx:DetachAndDeleteS3AccessPoint 권한을 추가하도록 업데이트되었습니다.	
Amazon FSx에서 AmazonFSxConsoleFullAccess AWS 관리형 정책 업데이트	AmazonFSxConsoleFullAccess 관리형 정책이 fsx:CreateAndAttachS3AccessPoint , fsx:DescribeS3AccessPointAttachments fsx:UpdateS3AccessPointAttachments, 및 fsx:DetachAndDeleteS3AccessPoint 권한을 추가하도록 업데이트되었습니다.	2025년 5월 28일
추가 AWS 리전 지원 추가	이제 아시아 태평양(태국) 및 멕시코(중부)에서 FSx for ONTAP 파일 시스템을 사용할 수 있습니다. 자세한 내용은 가용성 기준을 AWS 리전 참조하세요.	2025년 5월 8일
이제 자율 랜섬웨어 보호(ARP)가 지원됩니다.	랜섬웨어 및 맬웨어 공격을 모니터링하고 보호하는 NetApp AI 기반 기능인 ARP가 이제 FSx for ONTAP에서 지원됩니다. 자세한 내용은 자율 랜섬웨어 보호를 통한 데이터 보호를 참조하세요.	2025년 4월 7일

FSx for ONTAP 사용 설명서의 새 주제에서는 작업 그룹에서 SMB 서버를 설정하는 방법을 설명합니다.	작업 그룹에서 SMB 서버를 설정하는 방법은 SVM을 Microsoft Active Directory에 조인하는 대신 SVM의 작업 그룹에서 SMB 서버를 설정하는 방법을 설명합니다.	2025년 3월 4일
Amazon FSx에서 AmazonFSxConsoleReadOnlyAccess AWS 관리형 정책 업데이트	Amazon FSx는 `ec2:DescribeNetworkInterfaces` 권한을 추가하도록 AmazonFSxConsoleReadOnlyAccess 정책을 업데이트했습니다. 자세한 내용은 AmazonFSxConsoleReadOnlyAccess 정책을 참조하세요.	2025년 2월 25일
이제 추가 Harvest 대시보드가 지원됩니다.	이제 기본적으로 활성화되지 않은 Harvest 대시보드를 포함하여 FSx for ONTAP에서 추가 대시보드를 지원합니다. FSx for ONTAP에서 지원하지 않는 대시보드 목록도 추가되었습니다. 자세한 내용은 Harvest 및 Grafana를 사용하여 FSx for ONTAP 파일 시스템 모니터링을 참조하세요.	2025년 2월 18일
FSx for ONTAP 사용 설명서에 새로운 FSx for ONTAP 결제 및 사용 보고 주제 추가	AWS FSx for ONTAP에 대한 결제 및 사용 보고 주제에서는 AWS 결제 및 비용 관리 콘솔에서 FSx for ONTAP 파일 시스템에 대한 사용 보고서 결제에 액세스하는 방법을 설명합니다. 또한 두 보고서 모두에서 FSx for ONTAP과 관련된 모든 사용 유형을 제공합니다.	2025년 2월 13일

Amazon FSx용 듀얼 스택 VPC 인터페이스 엔드포인트에 대한 지원 추가	이제 IPv4 및 IPv6 IP 주소와 DNS 이름을 모두 사용하여 Amazon FSx용 듀얼 스택 VPC 인터페이스 엔드포인트를 생성할 수 있습니다. 자세한 내용은 FSx for ONTAP 및 인터페이스 VPC 엔드포인트를 참조하세요.	2025년 2월 7일
듀얼 스택 API 엔드포인트에 대한 지원 추가	파일 시스템을 생성하고 관리하기 위한 Amazon FSx 서비스 API에는 새로운 듀얼 스택 엔드포인트가 있습니다. 자세한 내용은 Amazon FSx API 참조의 API 엔드포인트를 참조하세요.	2025년 2월 7일
Amazon FSx에서 AmazonFSxConsoleFullAccess AWS 관리형 정책 업데이트	Amazon FSx는 `ec2:DescribeNetworkInterfaces` 권한을 추가하도록 AmazonFSxConsoleFullAccess 정책을 업데이트했습니다. 자세한 내용은 AmazonFSxConsoleFullAccess 정책을 참조하세요.	2025년 2월 7일
새 주제 게시,를 사용하여 데이터 복제 FlexCache	FlexCache를 사용하여 온프레미스 ONTAP 파일 시스템의 데이터를 FSx for ONTAP 파일 시스템에 복제하는 방법을 설명하는 새 주제가 게시되었습니다. 자세한 내용은 FlexCache로 데이터 복제를 참조하세요.	2024년 12월 19일

2세대 파일 시스템에 대한 지원 추가	이제 2세대 Single-AZ 및 Multi-AZ 파일 시스템을 생성할 수 있습니다. 단일 고가용성(HA) 페어는 이제 최대 6GBps의 처리량 용량과 200,000 SSD IOPS를 제공합니다. 자세한 내용은 고가용성(HA) 쌍을 참조하세요.	2024년 7월 9일
백업에서 복원되는 동안 볼륨에서 데이터를 읽기 위한 지원이 추가되었습니다.	이제 2세대 파일 시스템의 백업에서 복원되는 동안 파일 데이터에 대한 읽기 전용 액세스 권한으로 볼륨을 탑재할 수 있습니다. 자세한 내용은 백업을 새 볼륨으로 복원하기를 참조하세요.	2024년 7월 9일
2세대 파일 시스템의 처리량 용량 조정에 대한 지원이 추가되었습니다.	이제 생성 후 2세대 파일 시스템의 처리량 용량을 조정할 수 있습니다. 자세한 내용은 처리량 용량 관리를 참조하세요.	2024년 7월 9일
2세대 Single-AZ 파일 시스템에 HA 페어 추가 지원 추가	이제 생성 후 2세대 Single-AZ 파일 시스템에 HA 페어를 추가할 수 있습니다. 2세대 Single-AZ 파일 시스템에는 총 12개의 HA 페어가 있을 수 있습니다. 자세한 내용은 고가용성(HA) 쌍 추가하기를 참조하세요.	2024년 7월 9일
TCP를 통한 비휘발성 Memory Express(NVMe/TCP) 프로토콜에 대한 지원이 추가되었습니다.	이제 Amazon FSx for NetApp ONTAP 파일 시스템에서 데이터 전송에 NVMe /TCP 프로토콜을 사용할 수 있습니다. 자세한 내용은 블록 스토리지 프로토콜 사용을 참조하세요.	2024년 7월 9일

파일 시스템 관리 사용자의 `fsxadmin-readonly` 역할에 대한 지원이 추가되었습니다.	이제 ONTAP 파일 시스템 관리 사용자가 이 `fsxadmin-readonly` 역할을 사용할 수 있으며 NetApp Harvest와 같은 파일 시스템 모니터링 애플리케이션에 사용할 수 있습니다. 자세한 내용은 파일 시스템 관리자 역할 및 사용자을 참조하세요.	2024년 4월 30일
Windows 도메인 관리 사용자를 위한 SSH 퍼블릭 키 인증에 대한 지원이 추가되었습니다.	이제 Active Directory 도메인 파일 시스템 및 SVM 사용자와 함께 SSH 퍼블릭 키 인증을 사용할 수 있습니다. 자세한 내용은 ONTAP 사용자를 위한 Active Directory 인증 구성을 참조하세요.	2024년 4월 30일
스케일 아웃 파일 시스템에서 12개의 HA 페어에 대한 지원이 추가되었습니다.	Amazon FSx for NetApp ONTAP는 스케일 아웃 파일 시스템에서 12개의 HA 페어에 대한 지원을 추가했습니다. HA 페어가 12개인 파일 시스템은 12개의 고가용성(HA) 페어에서 최대 72GBps의 처리량 용량과 2,400,000 SSD IOPS를 제공할 수 있습니다. 자세한 내용은 고가용성(HA) 페어 및 Amazon FSx for NetApp ONTAP 성능을 참조하세요.	2024년 3월 4일
클라우드 쓰기 모드에 대한 지원이 추가되었습니다.	Amazon FSx for NetApp ONTAP는 볼륨에 대한 클라우드 쓰기 모드에 대한 지원을 추가했습니다. 자세한 내용은 볼륨에서 클라우드 쓰기 모드 활성화를 참조하세요.	2024년 2월 6일

를 사용하여 FlexGroup 볼륨 백업에 대한 지원 추가 AWS Backup	이제 AWS Backup 를 사용하여 FSx for ONTAP 파일 시스템에서 FlexGroup 볼륨을 백업하고 복원할 수 있습니다. 자세한 내용은 Amazon FSx AWS Backup 에서 사용을 참조하세요.	2024년 1월 11일
Amazon FSx에서 AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonFSxReadOnlyAccess, AmazonFSxConsoleReadOnlyAccess 및 AmazonFSx ServiceRolePolicy AWS 관리형 정책 업데이트	Amazon FSx는 AmazonFSx FullAccess, AmazonFSx ConsoleFullAccess, AmazonFSxReadOnlyAccess, AmazonFSxConsoleReadOnlyAccess 및 AmazonFSx ServiceRolePolicy 정책을 업데이트하여 `ec2:GetSecurityGroupsForVpc` 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon FSx 업데이트를 참조하세요.	2024년 1월 9일
Amazon FSx에서 AmazonFSx FullAccess 및 AmazonFSx ConsoleFullAccess AWS 관리형 정책 업데이트	Amazon FSx는 `ManageCrossAccountDataReplication` 작업을 추가하기 위해 AmazonFSxFullAccess 및 AmazonFSxConsoleFullAccess 정책을 업데이트했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon FSx 업데이트를 참조하세요.	2023년 12월 20일

스케일 아웃 지표에 대한 지원이 추가되었습니다.	ONTAP용 FSx는 이제 여러 HA 페어가 있는 파일 시스템에 대한 Amazon CloudWatch 지표를 제공합니다. 자세한 내용은 스케일 아웃 파일 시스템 지표를 참조하세요.	2023년 11월 26일
스케일 아웃 파일 시스템에 대한 지원 추가	Amazon FSx for NetApp ONTAP는 6개의 고가용성(HA) 페어에서 최대 36GBps의 처리량 용량과 1,200,000 SSD IOPS를 제공할 수 있는 스케일 아웃 파일 시스템에 대한 지원을 추가했습니다. 자세한 내용은 고가용성(HA) 페어 및 Amazon FSx for NetApp ONTAP 성능을 참조하세요.	2023년 11월 26일
FlexGroup 볼륨에 대한 지원이 추가되었습니다.	Amazon FSx for NetApp ONTAP에서 FlexGroup 볼륨에 대한 지원을 추가했습니다. 자세한 내용은 볼륨 스타일을 참조하세요.	2023년 11월 26일
Multi-AZ 파일 시스템에 대한 공유 VPC 지원 추가	이제 참여자 계정은 공유된 VPC에서 멀티 AZ 파일 시스템을 만들 수 있습니다. 소유자 계정은 Amazon FSx 콘솔, CLI 및 API에서 이 기능을 관리할 수 있습니다. 자세한 내용은 공유 서브넷에서 ONTAP용 FSx 파일 시스템 만들기를 참조하십시오.	2023년 11월 26일

Amazon FSx에서 AmazonFSx FullAccess 및 AmazonFSx ConsoleFullAccess AWS 관리형 정책 업데이트	Amazon FSx는 `fsx:CopySnapshotAndUpdateVolume` 권한을 추가하기 위해 AmazonFSxFullAccess 및 AmazonFSxConsoleFullAccess 정책을 업데이트했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon FSx 업데이트를 참조하세요.	2023년 11월 26일
Amazon FSx에서 AmazonFSx FullAccess 및 AmazonFSx ConsoleFullAccess AWS 관리형 정책 업데이트	Amazon FSx는 AmazonFSx FullAccess 및 AmazonFSx ConsoleFullAccess 정책을 업데이트하여 `fsx:DescribeSharedVPCConfiguration` 및 `fsx:UpdateSharedVPCConfiguration` 권한을 추가했습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon FSx 업데이트를 참조하세요.	2023년 11월 14일
추가 ONTAP 역할 및 사용자 생성을 위한 지원 추가	이제 Amazon FSx for NetApp ONTAP에서 추가 ONTAP 역할 및 사용자를 생성하여 ONTAP CLI 및 REST API를 사용할 때 사용자 기능과 권한을 정의할 수 있습니다. 자세한 내용은 Amazon FSx for NetApp ONTAP의 역할 및 사용자를 참조하세요.	2023년 9월 6일

추가 CloudWatch 지표 및 향상된 모니터링 대시보드에 대한 지원 추가	이제 FSx for ONTAP은 파일 시스템 활동에 대한 가시성을 높이기 위해 추가 성능 지표 및 향상된 모니터링 대시보드를 제공합니다. 자세한 내용은 CloudWatch를 사용한 모니터링을 참조하세요.	2023년 8월 17일
Amazon FSx에서 AmazonFSx ServiceRolePolicy AWS 관리형 정책 업데이트	Amazon FSx에서 AmazonFSx ServiceRolePolicy의 `cloudwatch:PutMetricData` 권한이 업데이트되었습니다. 자세한 내용은 AWS 관리형 정책에 대한 Amazon FSx 업데이트를 참조하세요.	2023년 7월 24일
NetApp 시스템 관리자를 직접 사용하기 위한 지원 추가	System Manager를 사용하여 NetApp BlueXP에서 직접 FSx for ONTAP 파일 시스템을 관리할 수 있습니다. 자세한 내용은 BlueXP와 함께 NetApp 시스템 관리자 사용을 참조하세요.	2023년 7월 13일
EMS 이벤트 모니터링에 대한 지원 추가	NetApp ONTAP의 네이티브 Events Management System (EMS)을 사용하여 FSx for ONTAP 파일 시스템을 모니터링할 수 있습니다. NetApp ONTAP CLI를 사용하여 EMS 이벤트를 볼 수 있습니다. 자세한 내용은 FSx for ONTAP EMS 이벤트 모니터링을 참조하세요.	2023년 7월 13일

SnapLock에 대한 지원 추가	이제 FSx for ONTAP에서 SnapLock 볼륨을 지원합니다. SnapLock을 사용하면 파일을 지정된 보존 기간 동안 수정이나 삭제를 방지하는 write once, read many(WORM) 상태로 전환하여 보호할 수 있습니다. FSx for ONTAP에서 SnapLock을 통해 규정 준수 및 엔터프라이즈 보존 모드를 지원합니다. 자세한 내용은 SnapLock 작업을 참조하세요.	2023년 7월 13일
전송 중 데이터의 IPsec 암호화 지원 추가	이제 FSx for ONTAP에서 IPsec 암호화를 사용하여 파일 시스템과 연결된 클라이언트 간에 전송 중 데이터를 암호화할 수 있도록 지원합니다. 자세한 내용은 PSK 인증을 사용하여 IPsec 구성 및 인증서 인증을 사용하여 IPsec 구성을 참조하세요.	2023년 7월 13일
최대 볼륨 크기가 증가됨	FSx for ONTAP이 볼륨의 최대 크기를 100TB에서 300TB로 업데이트했습니다. 자세한 내용은 볼륨 자동 크기 조정 켜기를 참조하세요.	2023년 7월 13일
Amazon FSx에서 AmazonFSx FullAccess AWS 관리형 정책 업데이트	Amazon FSx의 `fsx:*` 권한을 제거하고 특정 `fsx` 작업을 추가하도록 AmazonFSx FullAccess 정책을 업데이트했습니다. 자세한 내용은 AmazonFSxFullAccess 정책을 참조하세요.	2023년 7월 13일

Amazon FSx에서 AmazonFSx ConsoleFullAccess AWS 관리형 정책 업데이트	Amazon FSx의 `fsx:*` 권한을 제거하고 특정 `fsx` 작업을 추가하도록 AmazonFSx ConsoleFullAccess 정책을 업데이트했습니다. 자세한 내용은 AmazonFSxConsoleFullAccess 정책을 참조하세요.	2023년 7월 13일
기존 스토리지 가상 머신을 Active Directory에 조인하기 위한 지원 추가	AWS Management Console AWS CLI 및 API를 사용하여 기존 스토리지 가상 머신을 Active Directory에 조인할 수 있습니다. 자세한 내용은 SVM을 Active Directory에 조인을 참조하세요.	2023년 6월 13일
단일 AZ 파일 시스템에 NVMe 읽기 캐시에 대한 지원 추가	이제 미국 동부(오하이오) 리전, 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 및 유럽(아일랜드)에서는 2022년 11월 28일 이후에 생성된 2GBps 이상의 처리량 용량을 가진 단일 AZ 파일 시스템에 대해 NVMe 읽기 캐시를 지원합니다. 자세한 내용은 배포 유형이 성능에 미치는 영향을 참조하세요.	2022년 11월 28일
VPC 내 IP 주소 범위를 사용하여 다중 AZ 파일 시스템을 생성하기 위한 지원 추가	이제 VPC의 IP 주소 범위 내에 있는 엔드포인트를 지정하여 다중 AZ FSx for ONTAP 파일 시스템을 생성할 수 있습니다. 자세한 내용은 FSx for ONTAP 파일 시스템 생성을 참조하세요.	2022년 11월 28일

다중 AZ 파일 시스템에서 VPC 라우팅 테이블을 업데이트하기 위한 지원 추가	이제 새 VPC 라우팅 테이블을 기존의 다중 AZ FSx for ONTAP 파일 시스템에 연결(추가)하거나 기존의 다중 AZ FSx for ONTAP 파일 시스템에서 기존의 VPC 라우팅 테이블의 연결을 해제(제거)할 수 있습니다. 자세한 내용은 파일 시스템 업데이트를 참조하세요.	2022년 11월 28일
AWS Nitro System을 사용한 전송 중 데이터 암호화 지원 추가	미국 동부(오하이오) 리전, 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 및 유럽(아일랜드)에서는 지원되는 Amazon EC2 인스턴스에서 액세스할 때 전송 중 데이터가 자동으로 암호화됩니다. 자세한 내용은 AWS Nitro 시스템을 사용하여 전송 중인 데이터 암호화를 참조하세요.	2022년 11월 28일
DP 볼륨 생성에 대한 지원 추가	이제 Amazon FSx 콘솔 AWS CLI또는 Amazon FSx API를 사용하여 DP(데이터 보호) 볼륨을 생성할 수 있습니다. 단일 볼륨의 데이터를 마이그레이션하거나 보호하려는 경우 DP 볼륨을 NetApp SnapMirror 또는 SnapVault 관계의 대상으로 사용할 수 있습니다. 자세한 내용은 볼륨 유형을 참조하세요.	2022년 11월 28일

백업에 볼륨 태그 복사에 대한 지원 추가	이제 AWS CLI 또는 Amazon FSx API에서 CopyTagsToBackups 를 활성화하여 볼륨의 태그를 백업으로 자동 복사할 수 있습니다. 자세한 내용은 백업에 태그 복사를 참조하세요.	2022년 11월 28일
스냅샷 정책 선택에 대한 지원 추가	이제 Amazon FSx 콘솔 또는 Amazon FSx API를 사용하여 볼륨을 생성하거나 업데이트할 때 세 가지 기본 제공 스냅샷 정책 중에서 선택할 수 AWS CLI FSx. ONTAP CLI 또는 REST API에서 만든 사용자 지정 스냅샷 정책을 선택할 수도 있습니다. 자세한 내용은 스냅샷 정책을 참조하세요.	2022년 11월 28일
추가 파일 시스템 처리량 용량 옵션에 대한 지원 추가	이제 FSx for ONTAP은 미국 동부(오하이오) 리전, 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 및 유럽(아일랜드)에서 2022년 11월 28일 이후에 생성된 파일 시스템에 대해 4,096MBps의 처리량 용량을 지원합니다. 자세한 내용은 처리량 용량이 성능에 미치는 영향을 참조하세요.	2022년 11월 28일

추가 SSD IOPS에 대한 지원 추가	이제 FSx for ONTAP은 미국 동부(오하이오) 리전, 미국 동부(버지니아 북부) 리전, 미국 서부(오레곤) 리전 및 유럽(아일랜드)에서 2022년 11월 28일 이후에 생성된 파일 시스템에 대해 160,000 SSD IOPS를 지원합니다. 자세한 내용은 처리량 용량이 성능에 미치는 영향을 참조하세요.	2022년 11월 28일
에서 VMware Cloud의 외부 데이터 스토어로 FSx for ONTAP 사용 지원 추가 AWS	FSx for ONTAP을 AWS 소프트웨어 정의 데이터 센터(SDDC)의 VMware Cloud에 대한 외부 데이터 스토어로 사용할 수 있습니다.SDDCs 이 추가 지원은 AWS 워크로드 기반 VMware Cloud의 컴퓨팅 리소스와 독립적으로 스토리지를 확장하거나 축소할 수 있는 유연성을 제공합니다. 자세한 내용은 FSx for ONTAP과 함께 VMware Cloud 사용을 참조하세요.	2022년 8월 30일
파일 시스템의 스토리지 용량 자동 증가	AWS사용한 SSD 스토리지 용량이 지정한 임계값을 초과하면 미리 개발된 사용자 지정 AWS CloudFormation 템플릿을 사용하여 파일 시스템의 스토리지 용량을 자동으로 늘릴 수 있습니다. 자세한 내용은 SSD 스토리지 용량 동적 증가를 참조하세요.	2022년 6월 3일

이제 Amazon FSx가와 통합되었습니다. AWS Backup	이제 AWS Backup 를 사용하여 네이티브 Amazon FSx 백업 외에도 FSx 파일 시스템을 백업하고 복원할 수 있습니다. 자세한 내용은 Amazon FSx AWS Backup 에서 사용을 참조하세요.	2022년 5월 18일
단일 가용 영역 ONTAP 파일 시스템 배포에 대한 지원 추가	단일 가용 영역(AZ) 내에서 고가용성과 내구성을 제공하도록 설계된 단일 AZ FSx for ONTAP 파일 시스템을 생성할 수 있습니다. 자세한 내용은 파일 시스템 배포 선택을 참조하세요.	2022년 4월 13일
AWS PrivateLink 인터페이스 VPC 엔드포인트에 대한 지원 추가	이제 인터넷을 통해 트래픽을 보내지 않고 인터페이스 VPC 엔드포인트를 사용하여 VPC에서 Amazon FSx API에 액세스할 수 있습니다. 자세한 내용은 Amazon FSx 및 인터페이스 VPC 엔드포인트를 참조하세요.	2022년 4월 5일
기존 ONTAP 파일 시스템의 처리량 용량 수정에 대한 지원 추가	이제 기존 ONTAP 파일 시스템에서 사용할 수 있는 처리량 용량을 수정할 수 있습니다. 자세한 내용은 처리량 용량 관리를 참조하세요.	2022년 3월 30일

SSD 스토리지 용량 및 프로비저닝된 IOPS 크기 조정에 대한 지원 추가	이제 스토리지 및 IOPS 요구 사항이 증가함에 따라 기존 FSx for ONTAP 파일 시스템에 대한 SSD 스토리지 용량 및 프로비저닝된 IOPS를 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 및 프로비저닝된 IOPS 관리를 참조하세요.	2022년 1월 25일
Amazon CloudWatch 지표에 대한 지원 추가	FSx for ONTAP에서 원시 데이터를 수집하여 읽기 가능하며 실시간에 가까운 지표로 처리하는 Amazon CloudWatch를 통해 파일 시스템을 모니터링할 수 있습니다. 자세한 내용은 Amazon CloudWatch를 사용한 모니터링을 참조하세요.	2022년 1월 19일
추가 파일 시스템 처리량 용량 옵션에 대한 지원 추가	FSx for ONTAP은 이제 파일 시스템 처리량에 대해 128MBps 및 256MBps 옵션을 지원합니다. 자세한 내용은 처리량 용량이 성능에 미치는 영향을 참조하세요.	2021년 11월 30일
이제 Amazon FSx for NetApp ONTAP이 정식 출시됨	FSx for ONTAP은 NetApp의 ONTAP 파일 시스템에 구축된 매우 안정적이고 확장 가능하며 성능이 뛰어나고 기능이 풍부한 파일 스토리지를 제공하는 완전 관리형 서비스입니다. NetApp 파일 시스템의 친숙한 기능, 성능, 기능 및 APIs에 완전 관리형 AWS 서비스의 민첩성, 확장성 및 단순성을 제공합니다.	2021년 9월 2일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.