aws

Windows 사용 설명서

Amazon FSx for Windows File Server

Amazon FSx for Windows File Server: Windows 사용 설명서

Table of Contents

FSx for Windows File Server란 무엇입니까?

Amazon FSx for Windows File Server는 완전한 네이티브 Windows 파일 시스템이 지원하는 완전관리형 Microsoft Windows 파일 서버를 제공합니다. FSx for Windows File Server는 엔터프라이즈 애플리케이션을 AWS 클라우드로 쉽게 리프트 앤 시프트할 수 있는 기능, 성능 및 호환성을 제공합니다.

Amazon FSx는 Microsoft Windows Server에 구축된 완전관리형 파일 스토리지를 통해 광범위한 엔터프라이즈 Windows 워크로드를 지원합니다. Amazon FSx는 Windows 파일 시스템 기능을 기본적으로 지원하며 네트워크를 통해 파일 스토리지에 액세스할 수 있는 서버 메시지 블록(SMB) 프로토콜도 지원합니다. Amazon FSx는 기본 Windows 호환성, 엔터프라이즈 성능 및 기능, 1밀리초 미만의 일관된 지연 시간을 통해 AWS 클라우드의 엔터프라이즈 애플리케이션에 최적화되어 있습니다.

Windows 개발자와 관리자가 이용 중인 Amazon FSx 상의 파일 스토리지, 코드, 애플리케이션과 도구를 이용하면 어떤 변경도 없이 작업을 계속 진행할 수 있습니다. Amazon FSx에 이상적인 Windows 애플리케이션과 워크로드에는 비즈니스 애플리케이션, 홈 디렉터리, 웹 지원, 콘텐츠 관리, 데이터 분석, 소프트웨어 빌드 설정 및 미디어 처리 워크로드 등이 있습니다.

완전 관리형 서비스인 FSx for Windows File Server는 파일 서버 및 스토리지 볼륨 설정과 프로비저닝을 위한 관리 부담이 없습니다. 또한 Amazon FSx는 Windows 소프트웨어를 최신 상태로 유지하고, 하드웨어 오류를 감지하고 처리하며, 백업을 수행하기도 합니다. 또한 AWS IAM AWS Directory Service for Microsoft Active Directory WorkSpacesAWS Key Management Service, Amazon 등과 같은 다른 AWS 서비스와의 풍부한 통합을 제공합니다. AWS CloudTrail

FSx for Windows File Server 리소스: 파일 시스템, 백업 및 파일 공유

Amazon FSx의 기본 리소스는 파일 시스템과 백업입니다. 파일 시스템은 파일 및 폴더를 저장하고 액세스하는 장소입니다. 파일 시스템은 하나 이상의 Windows 파일 서버와 스토리지 볼륨으로 구성됩니다. 파일 시스템을 생성할 때 스토리지 용량(GiB), SSD IOPS, 처리 용량(MB/s)을 지정합니다. 파일 시스템을 생성한 후 필요에 따라 해당 속성을 수정할 수 있습니다. 자세한 내용은 스토리지 용량 관리, SSD IOPS 관리, 처리량 용량 관리 단원을 참조하세요.

Windows File Server용 FSx file-system-consistent 백업은 내구성이 뛰어나고 증분 백업입니다. Amazon FSx는 파일 시스템 일관성을 보장하기 위해 Microsoft Windows의 볼륨 섀도 복사본 서비스(VSS)를 사용합니다. 파일 시스템을 생성할 때 자동 일일 백업이 기본적으로 활성화되며 언제든지 수동 백업을 추가로 수행할 수도 있습니다. 자세한 정보는 백업 작업을 참조하세요.

Windows 파일 공유는 SMB를 통해 컴퓨팅 인스턴스에 액세스할 수 있도록 하는 파일 시스템 내의 특정 폴더(및 하위 폴더)입니다. 파일 시스템에는 `\share`라는 Windows 파일 공유가 기본으로 제공됩니다. Windows의 공유 폴더 그래픽 사용자 인터페이스(GUI) 도구를 사용하여 원하는 만큼 다른 Windows 파일 공유를 만들고 관리할 수 있습니다. 자세한 정보는 Microsoft Windows 파일 공유 사용을 참조하세요.

파일 공유는 파일 시스템의 DNS 이름 또는 파일 시스템에 연결된 DNS 별칭을 사용하여 액세스합니다. 자세한 정보는 DNS 별칭 관리을 참조하세요.

파일 공유 액세스

Amazon FSx는 SMB 프로토콜(버전 2.0~3.1.1 지원)을 사용하는 컴퓨팅 인스턴스에서 액세스할 수 있습니다. Windows Server 2008 및 Windows 7 이후의 모든 Windows 버전과 최신 버전의 Linux에서 공유에 액세스할 수 있습니다. Amazon FSx 파일 공유를 Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스, 인스턴스, AppStream Amazon 2.0 인스턴스 및 VMware 클라우드 WorkSpaces 온 VM에 매핑할 수 있습니다. AWS

AWS Direct Connect 또는 AWS VPN을 사용하여 온프레미스 컴퓨팅 인스턴스에서 파일 공유에 액세스할 수 있습니다. 파일 시스템과 동일한 VPC, AWS 계정 및 AWS 지역에 있는 파일 공유에 액세스할 수 있을 뿐 아니라 다른 Amazon VPC, 계정 또는 지역에 있는 컴퓨팅 인스턴스의 공유에도 액세스할 수 있습니다. VPC 피어링 또는 전송 게이트웨이를 사용하여 액세스합니다. 자세한 정보는 지원 액세스 방법을 참조하세요.

보안 및 데이터 보호

Amazon FSx는 데이터를 보호하는 데 도움이 되는 여러 수준의 보안 및 규정 준수를 제공합니다. () 에서 AWS Key Management Service 관리하는 키를 사용하여 미사용 데이터 (파일 시스템과 백업 모두)를 자동으로 암호화합니다.AWS KMS전송 중 데이터도 SMB Kerberos 세션 키를 사용하여 자동으로 암호화됩니다. ISO, PCI-DSS 및 SOC 인증을 준수하는 것으로 평가되었으며 HIPAA 인증을 받았습니다.

Amazon FSx는 Windows 액세스 제어 목록(ACL)을 통해 파일 및 폴더 수준의 액세스 제어를 제공합니다. Amazon Virtual Private Cloud(VPC) 보안 그룹을 사용하여 파일 시스템 수준에서 액세스를 제어합니다. 또한 AWS Identity and Access Management (IAM) 액세스 정책을 사용하여 API 수준에서 액세스 제어를 제공합니다. 파일 시스템에 액세스하는 사용자는 Microsoft Active Directory를 통해 인증됩니다. Amazon FSx는 AWS CloudTrail 와 통합되어 API 호출을 모니터링하고 기록하므로 Amazon FSx 리소스에서 사용자가 취한 작업을 볼 수 있습니다.

또한 내구성이 뛰어난 파일 시스템 백업을 매일 자동으로 생성하여 데이터를 보호하고 언제든지 백업을 추가로 수행할 수 있습니다. 자세한 정보는 Amazon FSx의 보안을 참조하세요.

가용성과 내구성

FSx for Windows File Server는 두 가지 수준의 가용성과 내구성을 갖춘 파일 시스템을 제공합니다. 단일 AZ 파일은 구성 요소 장애를 자동으로 감지하고 해결하여 단일 가용 영역(AZ) 내에서 고가용성을 보장합니다. 또한 다중 AZ 파일 시스템은 지역 내 별도의 가용 영역에 대기 파일 서버를 프로비저닝하고 유지함으로써 여러 가용 영역에서 고가용성 및 장애 조치 지원을 제공합니다. AWS 단일 AZ 및 다중 AZ 파일 시스템 배포에 대한 자세한 내용은 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템 섹션을 참조하십시오.

파일 시스템 관리

사용자 지정 PowerShell 원격 관리 명령을 사용하거나 경우에 따라 Windows 네이티브 GUI를 사용하여 Windows File Server 파일 시스템용 FSx를 관리할 수 있습니다. Amazon FSx 파일 시스템 관리에 대한 자세한 내용은 파일 시스템 관리 섹션을 참조하십시오.

가격 및 성능 유연성

FSx for Windows File Server는 솔리드 스테이트 드라이브(SSD) 및 하드 디스크 드라이브(HDD) 스토리지 유형을 제공함으로써 가격 및 성능 유연성을 제공합니다. HDD 스토리지는 홈 디렉터리, 사용자 및 부서별 공유, 콘텐츠 관리 시스템 등 광범위한 워크로드에 맞게 설계되었습니다. SSD 스토리지는 데이터베이스, 미디어 처리 워크로드, 데이터 분석 애플리케이션을 포함하여 성능이 가장 높고 지연 시간에 민감한 워크로드용으로 설계되었습니다.

FSx for Windows File Server를 사용하면 파일 시스템 스토리지, SSD IOPS 및 처리량을 독립적으로 프로비저닝하여 비용과 성능을 적절하게 조합할 수 있습니다. 워크로드의 변경 요구 사항에 맞게 파일 시스템의 스토리지, SSD IOPS 및 처리량 용량을 수정하여 필요한 만큼만 비용을 지불할 수 있습니다. 자세한 정보는 Amazon FSx를 사용한 비용 최적화을 참조하세요.

Amazon FSx 요금

Amazon FSx를 사용하면 하드웨어 또는 소프트웨어 선결제 비용이 없습니다. 최소 약정, 설치 비용 또는 추가 비용 없이 사용한 리소스에 대해서만 비용을 지불하면 됩니다. 서비스와 관련된 요금 및 비용에 대한 내용은 Amazon FSx for Windows File Server 요금을 참조하세요.

가정

Amazon FSx를 사용하려면 지원되는 유형의 환경에서 VMware AWS 클라우드에서 실행되는 Amazon EC2 인스턴스 WorkSpaces , 인스턴스 AppStream , 2.0 인스턴스 또는 VM이 있는 AWS 계정이 필요합니다.

이 안내서에서는 다음과 같은 가정을 합니다.

- Amazon EC2를 사용하는 경우, Amazon EC2를 잘 알고 있다고 가정합니다. Amazon EC2 사용 방법에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하세요.
- 를 사용하는 WorkSpaces 경우 익숙하다고 가정합니다. WorkSpaces 사용 방법에 대한 자세한 내용은 Amazon 사용 WorkSpaces WorkSpaces 설명서를 참조하십시오.
- VMware Cloud AWS on을 사용하는 경우 잘 알고 있는 것으로 간주합니다. 자세한 내용은 AWS의 VMware Cloud 섹션을 참조하세요.
- 당사는 사용자가 Microsoft Active Directory 개념을 잘 알고 있다고 가정합니다.

필수 조건

Amazon FSx 파일 시스템을 생성하려면 다음이 필요합니다.

- Amazon FSx 파일 시스템 및 Amazon EC2 인스턴스를 생성하는 데 필요한 권한이 있는 AWS 계정입니다. 자세한 정보는 설정 AWS 계정을 참조하세요.
- Amazon FSx 파일 시스템과 연결하기 위한 Amazon Virtual Private Cloud(VPC) 에서 Microsoft Windows Server를 실행하는 Amazon EC2 인스턴스. 인스턴스를 생성하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 Windows 인스턴스 시작하기를 참조하십시오.
- Amazon FSx는 Microsoft Active Directory와 함께 작동하여 사용자 인증 및 액세스 제어를 수행합니다. Amazon FSx 파일 시스템을 만드는 과정에 이를 Microsoft Active Directory에 연결합니다. 자세한 정보는 FSx for Windows File Server에서 Microsoft Active Directory 작업을 참조하세요.
- 이 안내서는 Amazon VPC 서비스를 기반으로 하는 VPC의 기본 보안 그룹 규칙을 변경하지 않았다고 가정합니다. 보안 그룹 규칙을 변경한 경우, Amazon EC2 인스턴스에서 Amazon FSx 파일 시스템으로의 네트워크 트래픽을 허용하는 데 필요한 규칙을 추가했는지 확인해야 합니다. 자세한 내용은 Amazon FSx의 보안를 참조하세요.
- AWS Command Line Interface ()AWS CLI를 설치하고 구성하십시오. 지원되는 버전은 1.9.12 이후 버전입니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 AWS CLI의 설치, 업데이트, 제거를 참조하세요.

> **Note**
>
> `aws --version`명령으로 사용 중인 버전을 확인할 수 있습니다. AWS CLI

Amazon FSx for Windows File Server 포럼

Amazon FSx를 사용하는 동안 문제가 발생하는 경우 포럼을 사용하세요.

Amazon FSx를 처음 사용하십니까?

Amazon FSx를 처음 사용한다면, 다음 섹션을 순서대로 읽어보기를 권장합니다.

1. 첫 번째 Amazon FSx 파일 시스템을 만들 준비가 되었으면 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.
2. 성능에 대한 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.
3. Amazon FSx 보안 세부 사항은 Amazon FSx의 보안 섹션을 참조하세요.
4. Amazon FSx API에 대한 자세한 내용은 Amazon FSx API 참조를 참조하세요.

FSx for Windows File Server의 모범 사례

Amazon FSx for Windows File Server를 사용할 때 이 모범 사례를 따를 것이 좋습니다. 아래 링크를 따라가면 논의된 주제에 대해 자세히 알아볼 수 있습니다.

주제

일반 모범 사례

프로덕션으로 이동하기 전에 워크로드 테스트

워크로드를 테스트할 때 프로덕션 환경과 동일한 구성을 가진 스테이징 환경을 사용하는 것이 좋습니다. 예를 들어 동일한 Active Directory(AD) 및 네트워킹 구성, 파일 시스템 크기 및 구성, 그리고 Windows 기능(예: 데이터 중복 제거 및 섀도우 복사본)을 사용합니다. 원하는 프로덕션 트래픽을 시뮬레이션하는 스테이징 환경에서 테스트 워크로드를 실행하면 프로세스를 원활하게 실행할 수 있습니다.

또한 파일 시스템의 가용성 모델을 검토하여 파일 시스템 유지 관리, 처리량 용량 변경, 예상치 못한 서비스 중단과 같은 이벤트 발생 시 해당 파일 시스템 유형의 예상 복구 동작에 맞게 워크로드가 복원되도록 하는 것이 좋습니다. 자세한 내용은 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템 섹션을 참조하세요.

모니터링 계획 생성

파일 시스템 지표를 사용하여 스토리지 및 성능 사용량을 모니터링하고, 사용 패턴을 이해하고, 사용량이 파일 시스템의 스토리지 또는 성능 한도에 가까워지면 알림을 트리거할 수 있습니다. 나머지 애플리케이션 환경과 함께 Amazon FSx 파일 시스템을 모니터링하면 성능에 영향을 미칠 수 있는 모든 문제를 신속하게 디버깅할 수 있습니다.

파일 시스템에 충분한 리소스가 있는지 확인

리소스가 충분하지 않으면 지연 시간이 늘어나고 I/O 요청 대기 시간이 길어질 수 있으며, 이는 파일 시스템이 완전히 또는 부분적으로 사용할 수 없는 것으로 나타날 수 있습니다. 성능 모니터링 방법과, 성

능 경고 및 권장 사항 액세스 방법에 대한 자세한 내용은 Amazon FSx for Windows File Server 모니터링 섹션을 참조하세요.

파일 시스템 정기 백업

정기 백업을 통해 데이터 보존, 비즈니스 및 규정 준수 요구 사항을 충족할 수 있습니다. 파일 시스템에 기본적으로 활성화되어 있는 자동 일일 백업을 사용하고 전체에 걸쳐 AWS 서비스중앙 집중식 백업 솔루션을 사용하는 AWS Backup 것이 좋습니다. AWS Backup 빈도 (예: 하루에 여러 번, 매일 또는 매주) 와 보존 기간을 다르게 하여 추가 백업 계획을 구성할 수 있습니다.

보안 모범 사례

파일 시스템의 보안 및 액세스 제어 기능을 관리하는 이러한 모범 사례를 따르는 것이 좋습니다. 보안 및 규정 준수 목표에 맞는 Amazon FSx 구성에 대한 자세한 내용은 Amazon FSx의 보안 섹션을 참조하세요.

네트워크 보안

파일 시스템과 관련된 ENI를 수정하거나 삭제하지 않습니다.

Amazon FSx 파일 시스템은 파일 시스템과 연결된 Virtual Private Cloud(VPC)에 있는 탄력적 네트워크 인터페이스(ENI)를 통해 액세스합니다. 네트워크 인터페이스를 수정하거나 삭제하면 VPC와 파일 시스템 간의 연결이 영구적으로 손실될 수 있습니다.

보안 그룹 및 네트워크 ACL 활용

보안 그룹 및 네트워크 액세스 제어 목록(ACL)을 사용하여 파일 시스템에 대한 액세스를 제한할 수 있습니다. VPC 보안 그룹의 경우 기본 보안 그룹이 콘솔의 파일 시스템에 이미 추가되었습니다. 파일 시스템을 만드는 서브넷의 보안 그룹과 VPC 네트워크 ACL이 포트를 통한 트래픽을 허용하도록 해야 합니다. 자세한 내용은 Amazon VPC 보안 그룹 섹션을 참조하세요.

Active Directory

Amazon FSx 파일 시스템을 생성할 때는 Microsoft AD 도메인에 조인하여 사용자 인증과 공유/파일/폴더 수준의 액세스 제어 권한 부여를 제공합니다. 사용자는 기존 AD 계정을 사용하여 파일 공유에 연결하고 파일 공유에 포함된 파일 및 폴더에 액세스할 수 있습니다. 또한 기존 보안 ACL 구성을 수정 없이 Amazon FSx로 마이그레이션할 수 있습니다. Amazon FSx는 Active Directory에 대한 두 가지 옵션, 즉 AWS 관리형 Microsoft AD 또는 자체 관리형 Microsoft AD를 제공합니다.

AWS 관리형 Microsoft AD를 사용하는 경우 AD 보안 그룹의 기본 설정을 그대로 두는 것이 좋습니다. 이러한 설정을 수정하는 경우 네트워크 요구 사항을 충족하는 네트워크 구성을 유지해야 합니다. 자세한 내용은 네트워킹 사전 조건 섹션을 참조하세요.

자체 관리형 Microsoft AD를 사용하는 경우 파일 시스템을 구성하기 위한 추가 옵션이 있습니다. 자체 관리형 Microsoft AD와 함께 Amazon FSx를 사용할 때 초기 구성을 위해 다음 모범 사례를 따르는 것이 좋습니다.

- 단일 AD 사이트에 서브넷 할당: AD 환경에 도메인 컨트롤러가 많은 경우 Active Directory 사이트 및 서비스를 사용하여 Amazon FSx 파일 시스템에서 사용하는 서브넷을 가용성과 안정성이 가장 높은 단일 AD 사이트에 할당합니다. VPC 보안 그룹, VPC 네트워크 ACL, DC의 Windows 방화벽 규칙 및 AD 인프라에 있는 기타 네트워크 라우팅 제어가 필요한 포트를 통해 Amazon FSx와의 통신을 허용하도록 해야 합니다. 이렇게 하면 Windows가 할당된 AD 사이트를 사용할 수 없는 경우 다른 DC로 되돌릴 수 있습니다. 자세한 내용은 Amazon VPC를 사용한 파일 시스템 액세스 제어 섹션을 참조하세요.
- 별도의 조직 단위(OU) 사용: 보유하고 있을 수 있는 다른 조직 단위와는 분리된 Amazon FSx 파일 시스템용 OU를 사용합니다.
- 필요한 최소 권한으로 서비스 계정 구성: 필요한 최소 권한으로 Amazon FSx에 제공하는 서비스 계정을 구성하거나 위임합니다. 자세한 내용은 자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항 및 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.
- AD 구성을 지속적으로 확인: Amazon FSx 파일 시스템을 생성하기 전에 AD 구성에 대해 Amazon FSx Active Directory 검증 도구를 실행하여 구성이 Amazon FSx와 함께 사용하기에 유효한지 확인하고 도구에서 노출될 수 있는 경고 및 오류를 검색합니다.

AD 구성 오류로 인한 가용성 손실 방지

Amazon FSx를 자체 관리형 Microsoft AD와 함께 사용하는 경우 파일 시스템을 생성하는 동안뿐만 아니라 지속적인 운영 및 가용성을 위해 유효한 AD 구성을 갖추는 것이 중요합니다. 장애 복구 이벤트, 정기 유지 관리 이벤트 및 처리량 용량 업데이트 작업 중에 Amazon FSx는 파일 서버 리소스를 Active Directory에 다시 조인합니다. 이벤트 중에 AD 구성이 유효하지 않으면 파일 시스템이 잘못 구성됨 상태로 변경되고 사용할 수 없게 될 위험이 있습니다. 가용성 손실을 방지할 수 있는 다음과 같은 몇 가지 방법이 있습니다.

- Amazon FSx를 사용하여 AD 구성을 최신 상태로 유지: 서비스 계정의 암호를 재설정하는 등 변경을 수행하는 경우 이 서비스 계정을 사용하는 모든 파일 시스템의 구성이 업데이트되어야 합니다.

- AD 구성 오류 모니터링: 필요한 경우 파일 시스템의 AD 구성을 재설정할 수 있도록 잘못 구성됨 상태 알림을 직접 설정합니다. Lambda 기반 솔루션을 사용하여 이를 달성하는 예제는 Amazon 및 를 사용하여 Amazon FSx 파일 시스템의 상태 모니터링을 참조하십시오. EventBridge AWS Lambda
- AD 구성을 정기적으로 검증: AD 구성 오류를 사전에 탐지하려면 AD 구성에 대해 Active Directory 검증 도구를 지속적으로 실행하는 것이 좋습니다. 검증 도구를 실행할 때 경고나 오류가 표시되면 파일 시스템이 잘못 구성될 위험이 있다는 의미입니다.
- FSx에서 생성한 컴퓨터 객체의 이동 또는 수정 금지: Amazon FSx는 사용자가 제공한 서비스 계정과 권한을 사용하여 AD에서 컴퓨터 객체를 생성하고 관리합니다. 이러한 컴퓨터 객체를 이동하거나 수정하면 파일 시스템이 잘못 구성될 수 있습니다.

Windows ACL

Amazon FSx에서는 표준 Windows 액세스 제어 목록(ACL)을 사용하여 공유, 파일 및 폴더 수준의 세분화된 액세스 제어를 수행할 수 있습니다. Amazon FSx 파일 시스템은 파일 시스템 데이터에 액세스하는 사용자의 보안 인증 정보를 자동으로 확인하여 이러한 Windows ACL을 적용합니다.

- SYSTEM 사용자의 NTFS ACL 권한 변경 금지: Amazon FSx에서는 시스템 사용자에게 파일 시스템 내 모든 폴더에 대한 전체 제어 NTFS ACL 권한이 있어야 합니다. SYSTEM 사용자에 대한 NTFS ACL 권한을 변경하면 파일 시스템에 액세스할 수 없게 되고 향후 파일 시스템 백업을 사용할 수 없게 될 수 있습니다.

파일 시스템 구성 및 적절한 크기 조정

배포 유형 선택

Amazon FSx는 단일 AZ 및 다중 AZ라는 두 가지 배포 옵션을 제공합니다. 공유 Windows 파일 데이터에 대해 고가용성이 필요한 대부분의 프로덕션 워크로드에는 다중 AZ 파일 시스템을 사용하는 것이 좋습니다. 자세한 내용은 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템 섹션을 참조하세요.

스토리지 유형 선택

SSD 스토리지는 성능 요구 사항이 높고 지연 시간에 민감한 대부분의 프로덕션 워크로드에 적합합니다. 이러한 워크로드의 예로는 데이터베이스, 데이터 분석, 미디어 처리, 비즈니스 애플리케이션 등이 있습니다. 또한 최종 사용자 수가 많거나 I/O 수준이 높거나 작은 파일이 많은 데이터 세트와 관련된 사용 사례에는 SSD를 사용하는 것이 좋습니다. 마지막으로, 섀도우 복사본을 사용할 계획이라면 SSD 스토리지를 사용하는 것이 좋습니다. SSD 스토리지가 있는 파일 시스템에 대해 SSD IOPS를 구성하고 확장할 수 있지만 HDD 스토리지는 안 됩니다.

HDD 스토리지를 사용하기로 결정했다면 파일 시스템을 테스트하여 성능 요구 사항을 충족할 수 있는지 확인합니다. HDD 스토리지는 SSD 스토리지에 비해 비용이 저렴하지만 지연 시간이 길고 디스크 처리량 및 스토리지 단위당 디스크 IOPS 수준이 낮습니다. I/O 요구 사항이 낮은 범용 사용자 공유 및 홈 디렉터리, 데이터가 자주 검색되지 않는 대규모 콘텐츠 관리 시스템(CMS) 또는 대용량 파일 수가 적은 데이터 세트에 적합할 수 있습니다. 자세한 내용은 스토리지 구성 및 성능 섹션을 참조하세요.

Amazon FSx 콘솔 또는 Amazon FSx API를 사용하여 언제든지 스토리지 유형을 HDD에서 SSD로 업그레이드할 수 있습니다. 자세한 내용은 스토리지 유형 관리 섹션을 참조하세요.

처리량 용량 선택

워크로드의 예상 트래픽뿐만 아니라 파일 시스템에서 활성화하려는 기능을 지원하는 데 필요한 추가 성능 리소스를 충족할 수 있도록 충분한 처리량 용량을 갖춘 파일 시스템을 구성합니다. 예를 들어 데이터 중복 제거를 실행하는 경우 선택한 처리량 용량은 보유한 스토리지를 기반으로 중복 제거를 실행할 수 있는 충분한 메모리를 제공해야 합니다. 섀도우 복사본을 사용하는 경우 Windows Server에서 섀도우 복사본을 삭제하지 않도록 처리량 용량을 워크로드에 따라 결정될 것으로 예상되는 값의 3배 이상으로 늘리세요. 자세한 내용은 처리량 용량이 성능에 미치는 영향 섹션을 참조하세요.

스토리지 용량 및 처리량 용량 늘리기

여유 스토리지가 부족하거나 스토리지 요구 사항이 현재 스토리지 한도보다 커질 것으로 예상되는 경우 파일 시스템의 스토리지 용량을 늘립니다. 파일 시스템의 여유 스토리지 용량을 항상 10% 이상 유지하는 것이 좋습니다. 또한 프로세스가 진행되는 동안에는 용량을 늘릴 수 없으므로 스토리지를 확장하기 전에 스토리지 용량을 20% 이상 늘리는 것이 좋습니다. FreeStorage용량 CloudWatch 지표를 사용하여 사용 가능한 무료 스토리지의 양을 모니터링하고 추세를 이해할 수 있습니다. 자세한 정보는 스토리지 용량 관리을 참조하세요.

또한 현재 성능 제한으로 인해 워크로드가 제한되는 경우 파일 시스템의 처리량 용량을 늘려야 합니다. FSx 콘솔의 모니터링 및 성능 페이지를 사용하여 워크로드 수요가 성능 한도에 근접하거나 초과한 시점을 확인하여 파일 시스템이 워크로드에 맞게 충분히 프로비저닝되지 않았는지 확인할 수 있습니다.

스토리지 확장 기간을 최소화하고 쓰기 성능 저하를 방지하려면 스토리지 용량을 늘리기 전에 파일 시스템의 처리량 용량을 늘리고 스토리지 용량 증가가 완료되면 처리량 용량을 다시 조정하는 것이 좋습니다. 대부분의 워크로드는 스토리지를 확장하는 동안 성능에 미치는 영향이 미미하지만, 활성 데이터 세트가 큰 쓰기 중심의 애플리케이션은 쓰기 성능이 일시적으로 최대 절반까지 저하될 수 있습니다.

유휴 기간 동안의 처리량 용량 수정

처리량 용량을 업데이트하면 단일 AZ 파일 시스템의 가용성이 몇 분 동안 중단되고 다중 AZ 파일 시스템의 경우 장애 조치 및 페일백이 발생합니다. 다중 AZ 파일 시스템의 경우 장애 조치 및 페일백 중에

트래픽이 계속 발생하는 경우 이 기간 동안 이루어진 모든 데이터 변경 사항을 파일 서버 간에 동기화해야 합니다. 쓰기가 많고 IOPS가 많은 워크로드의 경우 데이터 동기화 프로세스에 최대 몇 시간이 걸릴 수 있습니다. 이 기간 동안에도 파일 시스템을 계속 사용할 수 있지만 데이터 동기화 기간을 줄이려면 파일 시스템의 부하가 최소화되는 유휴 기간 동안 유지 관리 기간을 예약하고 처리량 용량 업데이트를 수행하는 것이 좋습니다. 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

윈도우 파일 서버용 Amazon FSx 시작하기

다음에서는 Windows File Server용 FSx를 시작하는 방법을 배울 수 있습니다. 이 시작하기 연습에는 다음 단계가 포함됩니다.

1. 계정에 AWS 계정 등록하고 관리 사용자를 생성하십시오.
2. 를 사용하여 AWS 관리되는 Microsoft AD Active Directory를 생성합니다 AWS Directory Service. 파일 시스템 및 컴퓨팅 인스턴스를 Active Directory에 조인합니다.
3. 마이크로소프트 윈도우 서버를 실행하는 Amazon Elastic Compute Cloud 컴퓨팅 인스턴스를 생성합니다. 이 인스턴스를 사용하여 파일 시스템에 액세스합니다.
4. Amazon FSx 콘솔을 사용하여 Windows File Server용 Amazon FSx 파일 시스템을 생성합니다.
5. 파일 시스템을 EC2 인스턴스에 매핑합니다.
6. 파일 시스템에 데이터를 씁니다.
7. 파일 시스템을 백업합니다.
8. 생성한 리소스를 정리하세요.

주제

설정 AWS 계정

Amazon FSx를 처음 사용한다면 먼저 다음 작업을 완료합니다.

1. 가입하여 다음을 수행하십시오. AWS 계정
2. 관리자 액세스 권한이 있는 사용자 생성

가입하여 다음을 수행하십시오. AWS 계정

계정이 없는 경우 다음 단계를 완료하여 계정을 만드세요. AWS 계정

가입하려면 AWS 계정

1. https://portal.aws.amazon.com/billing/signup을 여세요.
2. 온라인 지시 사항을 따르세요.

   등록 절차 중에는 전화를 받고 키패드로 인증 코드를 입력하는 과정이 있습니다.

   에 AWS 계정가입하면 AWS 계정 루트 사용자a가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스 액세스 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 루트 사용자 액세스 권한이 필요한 작업을 수행하는 것입니다.

AWS 가입 절차가 완료된 후 확인 이메일을 보냅니다. 언제든지 https://aws.amazon.com/으로 가서 내 계정(My Account)을 선택하여 현재 계정 활동을 보고 계정을 관리할 수 있습니다.

관리자 액세스 권한이 있는 사용자 생성

등록한 AWS 계정후에는 일상적인 작업에 루트 사용자를 사용하지 않도록 관리 사용자를 보호하고 AWS IAM Identity Center활성화하고 생성하십시오 AWS 계정 루트 사용자.

보안을 유지하세요. AWS 계정 루트 사용자

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

   루트 사용자를 사용하여 로그인하는 데 도움이 필요하면AWS 로그인 사용 설명서의 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 참조하십시오.

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 ID 소스로 사용하는 방법에 대한 자습서는 사용 설명서의 기본값으로 IAM Identity Center 디렉터리사용자 액세스 구성을 참조하십시오. IAM Identity Center 디렉터리 AWS IAM Identity Center

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 사용 설명서의 AWS 액세스 포털에 로그인을 참조하십시오.AWS 로그인

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.

   지침은AWS IAM Identity Center 사용 설명서의 Add groups를 참조하세요.

파일 시스템 생성

Amazon FSx 파일 시스템을 생성하려면 윈도우 아마존 Elastic Compute Cloud (Amazon EC2) 인스턴스와 디렉토리를 생성해야 합니다. AWS Directory Service 아직 설정하지 않았다면 연습 1: 시작을 위한 사전 조건 섹션을 참조하세요.

파일 시스템을 만들려면 (콘솔)

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 FSx for Windows File Server를 선택한 다음 다음을 선택합니다. 파일 시스템 생성 페이지가 표시됩니다.
4. 생성 방법에서 표준 생성을 선택합니다.

파일 시스템 세부 정보

1. 파일 시스템 정보(File system details) 섹션에서 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.
2. 배포 유형으로 다중 AZ 또는 단일 AZ를 선택합니다.

   - 가용 영역을 사용할 수 없어도 되는 파일 시스템을 배포하려면 다중 AZ를 선택합니다. 이 옵션은 SSD 및 HDD 스토리지를 지원합니다.
   - 단일 가용 영역에 배포되는 파일 시스템을 배포하려면 단일 AZ를 선택합니다. 단일 AZ 2는 단일 가용 영역 파일 시스템의 최신 세대이며 SSD 및 HDD 스토리지를 지원합니다.

   자세한 정보는 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템을 참조하세요.
3. 스토리지 유형의 경우 SSD 또는 HDD를 선택할 수 있습니다.

   FSx for Windows File Server는 솔리드 스테이트 드라이브(SSD) 및 하드 디스크 드라이브(HDD) 스토리지 유형을 제공합니다. SSD 스토리지는 데이터베이스, 미디어 처리 워크로드, 데이터 분석 애플리케이션을 포함하여 성능이 가장 높고 지연 시간에 민감한 워크로드용으로 설계되었습니다. HDD 스토리지는 홈 디렉터리, 사용자 및 부서별 파일 공유, 콘텐츠 관리 시스템 등 광범위한 워크로드에 맞게 설계되었습니다. 자세한 정보는 스토리지 유형을 사용한 비용 최적화을 참조하세요.
4. 프로비저닝된 SSD IOPS의 경우 자동 또는 사용자 프로비저닝 모드를 선택할 수 있습니다.

   자동 모드를 선택하면 FSx for Windows File Server가 스토리지 용량 GiB당 3 SSD IOPS를 유지하도록 SSD IOPS를 자동으로 조정합니다. 사용자 프로비저닝 모드를 선택하는 경우 96~400,000 범위의 정수를 입력합니다. 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 유럽(아일랜드), 아시아 태평양(도쿄), 아시아 태평양(싱가포르)에서 SSD IOPS를 80,000 이상으로 확장할 수 있습니다. 자세한 정보는 SSD IOPS 관리을 참조하세요.
5. 스토리지 용량에는 파일 시스템의 스토리지 용량을 GiB 단위로 입력합니다. SSD 스토리지를 사용하는 경우 32~65,536 범위의 정수를 입력합니다. HDD 스토리지를 사용하는 경우 2,000~65,536 범위의 정수를 입력합니다. 파일 시스템을 생성한 후 언제든지 필요에 따라 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.
6. 처리량 용량을 기본 설정으로 유지합니다. 처리량 용량은 파일 시스템을 호스팅하는 파일 서버가 데이터를 제공할 수 있는 지속 속도입니다. 권장 처리량 용량 설정은 선택한 스토리지 용량을 기반으로 합니다. 권장 처리량 용량보다 많은 용량이 필요한 경우 처리량 용량 지정을 선택한 다음 값을 선택합니다. 자세한 정보는 FSx for Windows File Server 성능을 참조하세요.

> **Note**
>
> 파일 액세스 감사를 활성화하려면 처리량 용량을 32MB/s 이상으로 선택해야 합니다. 자세한 정보는 파일 액세스 감사을 참조하세요.

파일 시스템을 생성하고 나서 언제든지 필요에 따라 처리량 용량을 수정할 수 있습니다. 자세한 정보는 처리량 용량 관리을 참조하세요.

네트워크 및 보안

1. 네트워크 및 보안 섹션에서 파일 시스템과 연결할 Amazon VPC를 선택합니다. 이 시작 연습에서는 AWS Directory Service 디렉터리와 Amazon EC2 인스턴스에 대해 선택한 것과 동일한 Amazon VPC를 선택하십시오.
2. VPC 보안 그룹의 경우 기본 Amazon VPC의 기본 보안 그룹이 콘솔의 파일 시스템에 이미 추가되었습니다. 기본 보안 그룹을 사용하지 않는 경우 선택한 보안 그룹이 파일 시스템과 AWS 리전 동일한지 확인하십시오. EC2 인스턴스를 파일 시스템에 연결할 수 있으려면 선택한 보안 그룹에 다음 규칙을 추가해야 합니다.

   a. 다음 포트를 허용하려면 다음 인바운드 및 아웃바운드 규칙을 추가합니다.

규칙	포트
UDP	53, 88, 123, 389, 464
TCP	53, 88, 135, 389, 445, 464, 636, 3268, 3269, 5985, 9389, 49152-65535

   파일 시스템에 액세스하려는 클라이언트 컴퓨팅 인스턴스와 연결된 발신 및 수신 IP 주소 또는 보안 그룹 ID를 추가합니다.

   b. 파일 시스템에 조인하려는 Active Directory로의 모든 트래픽을 허용하려면 아웃바운드 규칙을 추가합니다. 이렇게 하려면 다음 중 한 가지를 수행합니다.

   - AWS 관리형 AD 디렉터리와 연결된 보안 그룹 ID로의 아웃바운드 트래픽을 허용합니다.

- 자체 관리형 Active Directory 도메인 컨트롤러와 연결된 IP 주소로의 모든 아웃바운드 트래픽을 허용합니다.

> **Note**
>
> 경우에 따라 기본 설정에서 보안 그룹의 규칙을 수정했을 수 있습니다. AWS Managed Microsoft AD 그렇다면 이 보안 그룹에 Amazon FSx 파일 시스템으로부터의 트래픽을 허용하는 데 필요한 인바운드 규칙이 있는지 확인합니다. 필수 인바운드 규칙에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD 사전 조건을 참조하세요.

자세한 정보는 Amazon VPC를 사용한 파일 시스템 액세스 제어을 참조하세요.

3. 다중 AZ 파일 시스템에는 각각 고유한 가용 영역과 서브넷에 기본 및 대기 파일 서버가 있습니다. 다중 AZ 파일 시스템을 생성하는 경우 (5단계 참조) 기본 파일 서버의 선호 서브넷 값과 대기 파일 서버의 대기 서브넷 값을 선택합니다.

   단일 AZ 파일 시스템을 생성하는 경우 파일 시스템의 서브넷을 선택하십시오.

윈도우 인증

- Windows 인증의 경우 다음과 같은 옵션을 사용할 수 있습니다.

  에서 AWS 관리하는 Microsoft Active Directory 도메인에 파일 시스템을 가입시키려면 [관리형 Microsoft Active Directory] 를 선택한 다음 목록에서 해당 AWS Directory Service 디렉토리를 선택합니다. AWS자세한 정보는 FSx for Windows File Server에서 Microsoft Active Directory 작업을 참조하세요.

  파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 가입하려면 자체 관리형 Microsoft Active Directory를 선택하고 Active Directory에 대한 다음 세부 정보를 제공하십시오. 자세한 내용은 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용단원을 참조하세요.

  - Active Directory의 정규화된 도메인 이름.

> **Important**
>
> 단일 AZ 2 및 모든 다중 AZ 파일 시스템의 경우 Active Directory 도메인 이름은 47자를 초과할 수 없습니다. 이 제한은 자체 관리형 Active Directory 도메인 AWS Directory Service 이름과 자체 관리형 Active Directory 도메인 이름 모두에 적용됩니다.
> Amazon FSx는 내부 트래픽을 DNS IP 주소로 직접 연결해야 합니다. 인터넷 게이트웨이를 통한 연결은 지원되지 않습니다. 대신 AWS Virtual Private Network, VPC 피어링 또는 연결을 사용하십시오. AWS Direct Connect AWS Transit Gateway

- DNS 서버 IP 주소 - 도메인의 DNS 서버의 IPv4 주소입니다.

> **Note**
>
> DNS 서버에 EDNS(Extension Mechanisms for DNS)가 활성화되어 있어야 합니다. EDNS를 비활성화하면 파일 시스템 생성에 실패할 수 있습니다.

- 서비스 계정 사용자 이름 - 기존 Active Directory에 있는 서비스 계정의 사용자 이름입니다. 도메인 접두사나 접미사를 포함하지 않습니다.
- 서비스 계정 암호 - 서비스 계정의 암호입니다.
- (선택 사항) 조직 단위(OU) - 파일 시스템에 조인하려는 조직 단위의 고유 경로 이름입니다.
- (선택 사항) 위임된 파일 시스템 관리자 그룹 - Active Directory에서 파일 시스템을 관리할 수 있는 그룹의 이름입니다. 기본 그룹은 '도메인 관리자'입니다. 자세한 정보는 Amazon FSx 서비스 계정에 권한 위임 을 참조하세요.

암호화, 감사 및 액세스 (DNS 별칭)

1. 암호화에서는 파일 시스템에 저장된 데이터를 암호화하는 데 사용되는 AWS KMS key 암호화 키를 선택합니다. 키에 ARN을 지정하여 관리하는 기본 aws/fsx (기본값) AWS KMS, 기존 키 또는 고객 관리 키를 선택할 수 있습니다. 자세한 정보는 유휴 데이터 암호화을 참조하세요.
2. 감사 - 선택 사항의 경우 파일 액세스 감사는 기본적으로 비활성화됩니다. 파일 액세스 감사를 활성화 및 구성하는 자세한 내용은 파일 시스템을 만들 때 파일 액세스 감사 활성화(콘솔) 섹션을 참조하세요.
3. 액세스 - 선택 사항의 경우 파일 시스템과 연결할 DNS 별칭을 입력합니다. 각 별칭 이름은 정규화된 도메인 이름(FQDN) 형식으로 지정해야 합니다. 자세한 정보는 DNS 별칭 관리을 참조하세요.

백업 및 유지 관리

자동 일일 백업 및 이 섹션의 설정에 대한 자세한 내용은 을 참조하십시오백업 작업.

1. 일별 자동 백업의 경우 기본적으로 활성화됩니다. Amazon FSx가 파일 시스템을 매일 자동으로 백업하지 않도록 하려면 이 설정을 비활성화할 수 있습니다.
2. 자동 백업이 활성화된 경우 백업 기간이라고 하는 기간 내에 자동 백업이 이루어집니다. 기본 창을 사용하거나 자동 백업 창 시작 시간을 선택할 수 있습니다.
3. 자동 백업 보존 기간의 경우 기본 설정인 30일을 사용하거나 Amazon FSx에서 파일 시스템의 자동 일일 백업을 보존할 기간을 1~90일 사이의 값으로 설정할 수 있습니다. 이 설정은 사용자가 시작한 백업 또는 에서 수행한 백업에는 적용되지 않습니다. AWS Backup
4. 태그 - 선택 사항의 경우 키와 값을 입력하여 태그를 파일 시스템에 추가합니다. 태그는 파일 시스템을 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다. 자세한 정보는 Amazon FSx 리소스 태그 지정을 참조하세요.

   다음을 선택하세요.

구성을 검토하고 생성하십시오.

1. 파일 시스템 생성 페이지에 표시된 파일 시스템 구성을 검토합니다. 참고로 파일 시스템을 만든 후 수정할 수 있는 파일 시스템 설정과 수정할 수 없는 파일 시스템 설정을 확인할 수 있습니다. 파일 시스템 생성을 선택합니다.
2. Amazon FSx가 파일 시스템을 생성한 후 파일 시스템 대시보드의 목록에서 파일 시스템 ID를 선택하여 세부 정보를 확인합니다. [Attach] 를 선택하고 네트워크 및 보안 탭에서 파일 시스템의 DNS 이름을 기록해 둡니다. 공유를 EC2 인스턴스에 매핑하려면 다음 절차에 필요합니다.

파일 공유를 Windows Server를 실행하는 EC2 인스턴스에 매핑합니다.

이제 디렉터리에 연결된 마이크로소프트 윈도우 기반 Amazon EC2 인스턴스에 Amazon FSx 파일 시스템을 마운트할 수 있습니다. AWS Directory Service 파일 공유의 이름은 파일 시스템의 이름과 동일하지 않습니다.

GUI를 사용하여 Amazon EC2 Windows 인스턴스에서 파일 공유 매핑

1. Windows 인스턴스에 파일 공유를 마운트하려면 먼저 EC2 인스턴스를 시작하고 AWS Directory Service for Microsoft Active Directory에 조인해야 합니다. 이 작업을 수행하려면 AWS Directory Service 관리 가이드에서 다음 절차 중 하나를 선택합니다.

   - Windows EC2 인스턴스를 원활하게 조인
   - Windows 인스턴스를 수동으로 조인

2. 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 연결되면 파일 탐색기를 엽니다.
4. 탐색 창에서 네트워크에서 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 네트워크 드라이브 연결을 선택합니다.
5. 드라이브에서 원하는 드라이브 문자를 선택합니다.
6. Amazon FSx에서 할당한 기본 DNS 이름을 사용하거나 선택한 DNS 별칭을 사용하여 파일 시스템을 매핑할 수 있습니다. 이 절차에서는 기본 DNS 이름을 사용하여 파일 공유를 매핑하는 방법을 설명합니다. DNS 별칭을 사용하여 파일 공유를 매핑하려면 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스 섹션을 참조하세요.

   폴더에는 파일 시스템 DNS 이름과 공유 이름을 입력합니다. 기본 Amazon FSx 공유의 이름은 `\share`입니다. DNS 이름은 Amazon FSx 콘솔, https://console.aws.amazon.com/fsx/, Windows 파일 서버 > 네트워크 및 보안 섹션이나 CreateFileSystem 또는 DescribeFileSystems API 명령의 응답에서 찾을 수 있습니다.

   - AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - 자체 관리형 Active Directory에 조인된 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   예를 들어 `\\fs-0123456789abcdef0.ad-domain.com\share`을 입력합니다.
7. 파일 공유를 로그인 시 다시 연결할지 여부를 선택한 다음 마침을 선택합니다.

파일 공유에 데이터 쓰기

이제 파일 공유를 인스턴스에 매핑했으므로 Windows 환경의 다른 디렉터리처럼 파일 공유를 사용할 수 있습니다.

파일 공유에 데이터 작성

1. 메모장 텍스트 편집기를 엽니다.
2. 텍스트 편집기에서 일부 내용을 작성합니다. 예: *Hello, World!*
3. 파일을 파일 공유의 드라이브 문자에 저장합니다.
4. 파일 탐색기를 사용하여 파일 공유로 이동하여 방금 저장한 텍스트 파일을 찾습니다.

파일 시스템 백업

이제 Amazon FSx 파일 시스템과 해당 파일 공유를 사용할 수 있게 되었으므로 백업할 수 있습니다. 기본적으로 일별 백업은 파일 시스템의 30분 백업 기간 동안 자동으로 생성됩니다. 하지만 사용자 시작 백업은 언제든지 생성할 수 있습니다. 백업에는 추가 비용이 발생합니다. 백업 요금에 대한 자세한 내용은 요금을 참조하세요.

콘솔에서 파일 시스템의 백업 생성

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 콘솔 대시보드에서 이 연습을 위해 만든 파일 시스템의 이름을 선택합니다.
3. 파일 시스템의 개요 탭에서 백업 생성을 선택합니다.
4. 열리는 백업 생성 대화 상자에서 백업 이름을 입력합니다. 이 이름은 최대 256개의 유니코드 문자와 공백, 숫자 및 특수 문자 + - =. _ : /를 포함할 수 있습니다.
5. 백업 생성을 선택합니다.
6. 파일 시스템을 복원하거나 백업을 삭제할 수 있도록 모든 백업을 목록으로 표시하려면 백업을 선택합니다.

새 백업을 만들면 생성되는 동안 상태가 생성 중으로 설정됩니다. 몇 분 정도 소요될 수 있습니다. 백업을 사용할 수 있게 되면 상태가 사용 가능으로 변경됩니다.

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

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

   b. 콘솔 대시보드에서 이 연습을 위해 만든 파일 시스템의 이름을 선택합니다.

   c. 작업에서 파일 시스템 삭제를 선택합니다.

   d. 열리는 파일 시스템 삭제 대화 상자에서 최종 백업을 생성할지 여부를 결정합니다. 그럴 경우 최종 백업의 이름을 제공합니다. 자동으로 생성된 백업도 모두 삭제됩니다.

   > **Important**
   >
   > 백업에서 새 파일 시스템을 생성할 수 있습니다. 모범 사례로 최종 백업을 생성할 것이 좋습니다. 일정 시간이 지나도 필요하지 않은 경우 이 백업과 수동으로 만든 다른 백업을 삭제할 수 있습니다.

   e. 파일 시스템 ID 상자에 삭제하려는 파일 시스템의 ID를 입력합니다.

   f. 파일 시스템 삭제를 선택합니다.

   g. 이제 파일 시스템이 삭제되고 대시보드에서 해당 상태가 삭제 중으로 변경됩니다. 파일 시스템이 삭제되면 대시보드에 더 이상 표시되지 않습니다.

   h. 이제 파일 시스템에 대해 수동으로 생성한 백업을 모두 삭제할 수 있습니다. 왼쪽 탐색 창에서 백업을 선택합니다.

   i. 대시보드에서 삭제한 파일 시스템과 동일한 파일 시스템 ID를 가진 백업을 선택하고 백업 삭제를 선택합니다.

   j. 백업 삭제 대화 상자가 열립니다. 선택한 백업 ID의 확인란을 선택한 상태로 두고 백업 삭제를 선택합니다.

   이제 Amazon FSx 파일 시스템 및 관련 자동 백업이 삭제되었습니다.

3. 에서 연습 1: 시작을 위한 사전 조건 이 연습을 위해 AWS Directory Service 디렉터리를 만든 경우 지금 삭제할 수 있습니다. 자세한 내용은 AWS Directory Service 관리 가이드의 디렉터리 삭제를 참조하세요.

Amazon FSx 파일 시스템 상태

Amazon FSx 콘솔, AWS CLI 파일 시스템 설명 또는 API 운영 시스템을 사용하여 Amazon FSx 파일 시스템의 상태를 볼 수 있습니다. DescribeFile

파일 시스템 상태	설명
사용 가능	파일 시스템이 정상 상태이며 접속하여 사용할 수 있습니다.
생성 중	Amazon FSx가 새 파일 시스템을 생성하고 있습니다.
삭제 중	Amazon FSx가 기존 파일 시스템을 삭제하고 있습니다.
업데이트 중	파일 시스템이 고객이 시작한 업데이트를 진행 중입니다.
잘못 구성됨	Active Directory 환경의 변경으로 인해 파일 시스템이 손상된 상태입니다. 파일 시스템이 현재 사용할 수 없거나 가용성이 손실될 위험이 있으며 백업이 실패할 수 있습니다. 가용성 복원에 대한 자세한 내용은 파일 시스템이 잘못 구성된 상태 섹션을 참조하세요.
잘못 구성됨_사용 불가	Active Directory 환경의 변경으로 인해 파일 시스템이 현재 사용할 수 없는 상태입니다. 가용성 복원에 대한 자세한 내용은 파일 시스템이 잘못 구성된 상태 섹션을 참조하세요.
실패함	• 새 파일 시스템을 생성할 때 Amazon FSx가 새 파일 시스템을 생성하지 못했습니다. • 파일 시스템을 사용할 수 없습니다. • 파일 시스템에 오류가 발생하여 Amazon FSx가 복구할 수 없습니다. • Amazon FSx가 백업을 생성할 수 없습니다.

Amazon FSx for Windows File Server가 지원하는 클라이언트, 액세스 방법 및 환경

AWS와 온프레미스 환경 모두에서 지원하는 다양한 클라이언트와 방법으로 Amazon FSx 파일 시스템에 액세스할 수 있습니다.

주제

지원 클라이언트

Amazon FSx는 다양한 컴퓨팅 인스턴스 및 운영 체제에서 파일 시스템에 연결할 수 있도록 지원합니다. 이는 서버 메시지 블록(SMB) 프로토콜 버전 2.0~3.1.1을 통한 액세스를 지원함으로써 가능합니다.

Amazon FSx와 사용할 수 있는 AWS 컴퓨팅 인스턴스는 다음과 같습니다.

- Microsoft Windows, Mac, Amazon Linux 및 Amazon Linux 2 인스턴스를 포함한 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 자세한 내용은 파일 공유 액세스 섹션을 참조하세요.
- Amazon Elastic Container Service(Amazon ECS) 컨테이너. 자세한 내용을 알아보려면 Amazon Elastic Container Service 개발자 안내서의 FSx for Windows File Server 볼륨을 참조하세요.
- WorkSpaces 인스턴스 - 자세한 내용은 Amazon WorkSpaces에서 Using FSx for Windows File Server 사용 AWS 블로그 게시물을 참조하세요.
- Amazon AppStream 2.0 인스턴스 - 자세한 내용은 Amazon AppStream 2.0에서 Amazon FSx 사용 AWS 블로그 게시물을 참조하세요..
- AWS 환경의 VMware Cloud에서 실행되는 VM - 자세한 내용은 AWS 환경의 VMware Cloud에서 환경에서 FSx for Windows File Server를 사용한 파일 저장 및 공유 AWS 블로그 게시물을 참조하세요.

Amazon FSx에서 지원하는 운영 체제는 다음과 같습니다.

- Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.

- Windows Vista, Windows 7, Windows 8, Windows 8.1, Windows 10(WorkSpaces의 Windows 7 및 Windows 10 데스크톱 경험 포함), Windows 11.
- `cifs-utils` 도구를 사용하는 Linux.
- macOS

지원 액세스 방법

Amazon FSx에서는 다음 액세스 방법 및 접근 방식을 사용할 수 있습니다.

기본 DNS 이름을 사용하는 파일 시스템 액세스

FSx for Windows File Server는 모든 파일 시스템의 기본 도메인 이름 시스템(DNS) 이름을 제공합니다. DNS 이름을 사용하여 컴퓨팅 인스턴스의 드라이브 문자를 Amazon FSx 파일 공유에 매핑하면 FSx for Windows File Server 파일 시스템에 액세스할 수 있습니다. 자세한 내용은 Microsoft Windows 파일 공유 사용 섹션을 참조하세요.

> **Important**
>
> Amazon FSx는 Microsoft DNS를 기본 DNS로 사용하는 파일 시스템의 DNS 레코드만 등록합니다. 타사 DNS를 사용하는 경우 Amazon FSx 파일 시스템의 DNS 항목을 수동으로 설정해야 합니다. 파일 시스템에 사용할 올바른 IP 주소를 선택하는 방법에 대한 자세한 내용은 DNS에 사용할 올바른 파일 시스템 IP 주소 획득 섹션을 참조하세요.

DNS 이름은 다음 방법으로 찾습니다.

- Amazon FSx 콘솔에서 파일 시스템을 선택한 다음 세부 정보를 선택합니다. 네트워크 및 보안 섹션에서 DNS 이름을 확인합니다.
- 또한 CreateFileSystem 또는 DescribeFileSystems API 명령의 응답에서 확인할 수 있습니다.

AWS 관리형 Microsoft Active Directory에 연결된 모든 단일 AZ 파일 시스템의 DNS 이름의 형태는 `fs-0123456789abcdef0.`*`ad-dns-domain-name`*과 같습니다.

자체 관리형 Active Directory에 연결된 모든 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 DNS 이름은 `amznfsxaa11bb22.`*`ad-domain`*`.com`과 같습니다.

Kerberos 인증의 DNS 이름 사용

Amazon FSx에서는 전송 중에 Kerberos 기반 인증 및 암호화를 사용하는 것이 좋습니다. Kerberos는 파일 시스템에 액세스하는 클라이언트에게 가장 안전한 인증을 제공합니다. SMB 세션에서 전송 중 데이터의 Kerberos 기반 인증 및 암호화를 활성화하려면 Amazon FSx에서 제공하는 파일 시스템의 DNS 이름을 사용하여 파일 시스템에 액세스합니다.

AWS 관리형 Microsoft Active Directory와 온프레미스 Active Directory 간에 외부 신뢰를 구성한 경우, Kerberos 인증과 함께 Amazon FSx Remote PowerShell을 사용하려면 클라이언트에서 포리스트 검색 순서에 대한 로컬 그룹 정책을 구성해야 합니다. 자세한 내용은 Microsoft 설명서의 Kerberos 포리스트 검색 순서(KFSO) 구성을 참조하세요.

DNS 별칭을 사용한 파일 시스템 액세스

FSx for Windows File Server는 파일 공유에 액세스하는 데 사용할 수 있는 모든 파일 시스템에 DNS 이름을 제공합니다. FSx for Windows File Server 파일 시스템의 별칭을 등록하여 Amazon FSx가 생성하는 기본 DNS 이름 이외의 DNS 이름으로 Amazon FSx에 액세스할 수도 있습니다.

DNS 별칭을 사용하면 Windows 파일 공유 데이터를 Amazon FSx로 이동하고, 기존 DNS 이름을 계속 사용하여 Amazon FSx 데이터에 액세스할 수 있습니다. 또한 DNS 별칭을 사용하면 의미 있는 이름을 사용하여 Amazon FSx 파일 시스템에 연결하는 도구 및 애플리케이션을 보다 쉽게 관리할 수 있습니다. 자세한 내용은 DNS 별칭 관리 섹션을 참조하세요.

Kerberos 인증의 DNS 별칭 사용

Amazon FSx에서는 전송 중에 Kerberos 기반 인증 및 암호화를 사용하는 것이 좋습니다. Kerberos는 파일 시스템에 액세스하는 클라이언트에게 가장 안전한 인증을 제공합니다. DNS 별칭을 사용하여 Amazon FSx에 액세스하는 클라이언트의 Kerberos 인증을 활성화하려면 Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 있는 DNS 별칭에 해당하는 서비스 보안 주체 이름(SPN)을 추가해야 합니다.

선택적으로 Active Directory에서 다음과 같은 그룹 정책 객체(GPO)를 설정하여 DNS 별칭으로 파일 시스템에 액세스하는 클라이언트가 Kerberos 인증 및 암호화를 사용하도록 할 수 있습니다.

- NTLM 제한: 원격 서버로 나가는 NTLM 트래픽 제한 - 이 정책 설정을 사용하면 컴퓨터에서 Windows 운영 체제를 실행하는 원격 서버로 나가는 NTLM 트래픽을 거부하거나 감사할 수 있습니다.
- NTLM 제한: 원격 서버의 NTLM 인증 예외 추가 - 네트워크 보안: NTLM 제한: 원격 서버로 나가는 NTLM 트래픽 정책 설정이 구성된 경우, 이 정책 설정을 사용하여 클라이언트 장치가 NTLM 인증을 사용할 수 있도록 원격 서버 예외 목록을 만들 수 있습니다.

자세한 내용은 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스 섹션을 참조하세요.

FSx for Windows File Server 파일 시스템 및 DFS 네임스페이스 사용

FSx for Windows File Server는 Microsoft 분산 파일 시스템(DFS) 네임스페이스 사용을 지원합니다. DFS 네임스페이스를 사용하여 여러 파일 시스템의 파일 공유를 하나의 공통 폴더 구조(네임스페이스)로 조직하여 전체 파일 데이터세트에 액세스하는 데 사용할 수 있습니다. 링크 대상을 파일 시스템의 DNS 이름으로 구성하고 DFS 네임스페이스의 이름을 사용하여 Amazon FSx 파일 시스템에 액세스할 수 있습니다. 자세한 내용은 DFS 네임스페이스로 여러 파일 시스템 그룹화 섹션을 참조하세요.

지원 환경

파일 시스템과 동일한 VPC에 있는 리소스에서 파일 시스템에 액세스할 수 있습니다. 자세한 정보와 지침은 연습 1: 시작을 위한 사전 조건 섹션을 참조하세요.

또한 온프레미스 리소스와 다른 VPC, AWS 계정, 또는 AWS 리전에 있는 리소스에서 2019년 2월 22일 이후에 생성된 파일 시스템에 액세스할 수 있습니다. 다음 테이블은 지원 환경마다 파일 시스템이 생성된 시기에 따라 Amazon FSx가 클라이언트로부터의 액세스를 지원하는 환경을 보여줍니다.

클라이언트의 위치	2019년 2월 22일 이전에 생성된 파일 시스템에 대한 액세스	2020년 12월 17일 이전에 생성된 파일 시스템에 대한 액세스	2020년 12월 17일 이후에 생성된 파일 시스템에 대한 액세스
파일 시스템이 생성된 서브넷	✓	✓	✓
파일 시스템이 생성된 VPC의 기본 CIDR 블록	✓	✓	✓
파일 시스템이 생성된 VPC의 보조 CIDR		IP 주소가 RFC 1918 프라이빗 IP 주소 범위 내에 있는 클라이언트. • 10.0.0.0/8	IP 주소가 다음 CIDR 블록 범위의 클라이언트: 198.19.0.0/16

클라이언트의 위치	2019년 2월 22일 이전에 생성된 파일 시스템에 대한 액세스	2020년 12월 17일 이전에 생성된 파일 시스템에 대한 액세스	2020년 12월 17일 이후에 생성된 파일 시스템에 대한 액세스
기타 CIDR 또는 피어링된 네트워크		• 172.16.0.0/12 • 192.168.0.0/16	

> **Note**
>
> 프라이빗 IP 주소 범위 밖의 온프레미스에서 2020년 12월 17일 이전에 생성된 파일 시스템에 액세스하려는 경우가 있을 수 있습니다. 이런 경우, 파일 시스템의 백업에서 새 파일 시스템을 생성하세요. 자세한 내용은 백업 작업 섹션을 참조하세요.

아래에서는 온프레미스와 다양한 VPC, AWS 계정 또는 AWS 리전에서 FSx for Windows File Server 파일 시스템에 액세스하는 방법에 대한 정보를 확인할 수 있습니다.

온프레미스 환경에서 FSx for Windows File Server 파일 시스템 액세스

FSx for Windows File Server는 온프레미스 컴퓨팅 인스턴스에서 AWS Direct Connect 또는 AWS VPN을 사용하여 파일 시스템에 액세스하는 것을 지원합니다. FSx for Windows File Server는 AWS Direct Connect를 지원하여 온프레미스 환경에서 전용 네트워크 연결을 통해 파일 시스템에 액세스할 수 있도록 합니다. FSx for Windows File Server는 AWS VPN을 지원하여 온프레미스 장치에서 안전한 프라이빗 터널로 파일 시스템에 액세스할 수 있도록 합니다.

온프레미스 환경을 Amazon FSx 파일 시스템과 연결된 VPC에 연결한 후, DNS 이름 또는 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. VPC 내 컴퓨팅 인스턴스에서와 동일하게 액세스합니다. AWS Direct Connect에 대한 자세한 내용은 AWS Direct Connect 사용 설명서를 참조하세요. AWS VPN 연결 설정에 대한 자세한 내용은 Amazon VPC 사용 설명서의 VPN 연결을 참조하세요.

또한 FSx for Windows File Server는 Amazon FSx File Gateway를 사용하여 온프레미스 컴퓨팅 인스턴스에서 클라우드 내 FSx for Windows File Server 파일 공유에 짧은 지연 시간으로 원활하게 액세스할 수 있도록 지원합니다. 자세한 내용은 Amazon FSx File Gateway 사용 설명서를 참조하세요.

다른 VPC, 계정 또는 AWS 리전에서 FSx for Windows File Server 파일 시스템 액세스

파일 시스템과 연결된 다른 VPC, AWS 계정 또는 AWS 리전의 컴퓨팅 인스턴스에서 FSx for Windows File Server 파일 시스템에 액세스할 수 있습니다. 그러기 위해 VPC 피어링 또는 전송 게이트웨이를 사용할 수 있습니다. VPC 피어링 연결 또는 전송 게이트웨이를 사용하여 VPC를 연결하면 하나의 VPC에 있는 컴퓨팅 인스턴스가 다른 VPC의 Amazon FSx 파일 시스템에 액세스할 수 있습니다. VPC가 다른 계정에 속해 있거나 VPC가 다른 AWS 리전에 있더라도 이런 방식으로 액세스할 수 있습니다.

VPC 피어링 연결은 프라이빗 IPv4 또는 IP 버전 6(IPv6) 주소를 사용하여 두 VPC 간에 트래픽을 라우팅할 수 있게 해주는 두 개의 VPC 사이의 네트워킹 연결입니다. VPC 피어링을 사용하여 동일한 AWS 리전 또는 다른 AWS 리전 간에 VPC를 연결할 수 있습니다. VPC 피어링에 대한 자세한 내용은 Amazon VPC Peering Guide의 VPC 피어링이란?을 참조하세요.

전송 게이트웨이는 VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. 자세한 내용은 Amazon VPC Transit Gateways의 전송 게이트웨이 시작을 참조하세요.

VPC 피어링 또는 트랜짓 게이트웨이 연결을 설정한 후 DNS 이름을 사용하여 파일 시스템에 액세스할 수 있습니다. 연결된 VPC 내 컴퓨팅 인스턴스에서와 동일하게 액세스합니다.

가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템

Amazon FSx for Windows File Server는 단일 AZ 및 다중 AZ라는 두 가지 파일 시스템 배포 유형을 제공합니다. 다음 섹션에서는 워크로드에 적합한 배포 유형을 선택하는 데 도움이 되는 정보를 제공합니다. 서비스의 가용성 SLA(서비스 수준 계약)에 대한 자세한 내용은 Amazon FSx 서비스 수준 계약을 참조하세요.

단일 AZ 파일 시스템은 단일 Windows 파일 서버 인스턴스와, 단일 가용 영역 내의 스토리지 볼륨 세트로 구성됩니다. 단일 AZ 파일 시스템에서는 대부분의 경우 단일 구성 요소의 장애로부터 데이터를 보호하기 위해 데이터가 자동으로 복제됩니다. Amazon FSx는 하드웨어 장애를 지속적으로 모니터링하고 장애 발생 시 자동으로 장애 인프라 구성 요소를 교체하여 복구합니다. 단일 AZ 파일 시스템은 이러한 장애 복구 이벤트 기간 동안과, 파일 시스템에 대해 구성한 유지 관리 기간 내의 계획된 파일 시스템 유지 관리 기간 동안(일반적으로 20분 미만) 오프라인 상태가 됩니다. 단일 AZ 파일 시스템을 사용하는 경우 드물게는 여러 구성 요소 장애 또는 파일 시스템의 일관되지 않은 상태를 초래하는 단일 파일 서버의 비정상 장애로 인해 파일 시스템 장애를 복구할 수 없게 될 수 있으며, 이 경우에는 파일 시스템을 가장 최근의 백업에서 복구할 수 있습니다.

다중 AZ 파일 시스템은 두 개의 AZ(기본 AZ 및 대기 AZ)에 분산된 Windows 파일 서버의 고가용성 클러스터로 구성되며, Windows 서버 장애 조치 클러스터링(WSFC) 기술과 두 AZ 각각에 있는 스토리지 볼륨 세트를 활용합니다. 데이터는 각 개별 AZ 내에서, 그리고 두 AZ 간에 동기적으로 복제됩니다. 단일 AZ 배포에 비해 다중 AZ 배포는 AZ 전체에 데이터를 추가로 복제하여 내구성을 높이고, 대기 AZ로 자동 장애 조치를 수행하여 계획된 시스템 유지 관리 및 예상치 못한 서비스 중단 중에도 가용성을 향상시킵니다. 이렇게 하면 데이터에 계속 액세스할 수 있고 인스턴스 장애 및 AZ 중단으로부터 데이터를 보호하는 데 도움이 됩니다.

단일 AZ 또는 다중 AZ 파일 시스템 배포 선택

다중 AZ 파일 시스템이 제공하는 고가용성 및 내구성 모델을 고려하면 대부분의 프로덕션 워크로드에 다중 AZ 파일 시스템을 사용하는 것이 좋습니다. 단일 AZ 배포는 테스트 및 개발 워크로드, 애플리케이션 계층에 복제가 내장되어 있고 추가 스토리지 수준 중복성이 필요하지 않은 특정 프로덕션 워크로드, 가용성 및 Recovery Point Objective(RPO) 요구 사항이 완화된 프로덕션 워크로드를 위한 비용 효율적인 솔루션으로 설계되었습니다. 가용성 요구 사항이 완화되는 워크로드의 경우 계획된 파일 시스템 유지 관리 또는 예상치 못한 서비스 중단 발생 시 최대 20분 동안 일시적인 가용성 손실이 발생할 수 있으며, RPO 요구 사항이 완화되는 워크로드는 드문 경우이긴 하지만 가장 최근의 백업 이후 데이터 업데이트가 손실되더라도 괜찮습니다.

배포 유형별 기능 지원

다음 표에는 FSx for Windows File Server 파일 시스템 배포 유형이 지원하는 기능이 요약되어 있습니다.

배포 유형	SSD 스토리지	HDD 스토리지	DFS 네임스페이스	DFS 복제	사용자 지정 DNS 이름	CA 공유
단일 AZ 1	✓		✓	✓	✓	
단일 AZ 2	✓	✓	✓		✓	✓*
다중 AZ	✓	✓	✓		✓	✓*

> **Note**
>
> * 단일 AZ 2 파일 시스템에서 지속적으로 사용 가능한(CA) 공유를 생성할 수 있지만 SQL Server HA 배포의 경우 다중 AZ 파일 시스템에서 CA 공유를 사용해야 합니다.

FSx for Windows File Server의 장애 조치 프로세스

다중 AZ 파일 시스템은 다음과 같은 상황이 발생할 경우 기본 파일 서버에서 대기 파일 서버로 자동 장애 조치합니다.

- 가용 영역 중단이 발생합니다.
- 기본 파일 서버를 사용할 수 없게 됩니다.
- 기본 파일 서버가 계획된 유지 관리를 진행합니다.

한 파일 서버에서 다른 파일 서버로 장애 조치하면 새 활성 파일 서버가 자동으로 모든 파일 시스템 읽기 및 쓰기 요청을 처리하기 시작합니다. 기본 서브넷의 리소스를 사용할 수 있게 되면 Amazon FSx는 자동으로 기본 서브넷의 기본 파일 서버로 페일백합니다. 활성 파일 서버에서 장애가 감지된 후 대기 파일 서버가 활성 상태로 승격되기까지 보통 30초 이내에 장애 조치가 완료됩니다. 원래 다중 AZ 구성으로의 페일백도 30초 이내에 완료되며 기본 서브넷의 파일 서버가 완전히 복구된 후에만 발생합니다.

파일 시스템이 페일오버되고 페일백되는 짧은 기간 동안에는 I/O가 일시 중지되고 Amazon CloudWatch 메트릭을 일시적으로 사용할 수 없게 될 수 있습니다.

다중 AZ 파일 시스템의 경우 장애 조치 및 페일백 중에 트래픽이 계속 발생하는 경우 이 기간 동안 이루어진 모든 데이터 변경 사항을 파일 서버 간에 동기화해야 합니다. 쓰기가 많고 IOPS가 많은 워크로드의 경우 이 프로세스에 최대 몇 시간이 걸릴 수 있습니다. 파일 시스템의 부하가 적은 상태에서 애플리케이션에 장애 조치가 미치는 영향을 테스트하는 것이 좋습니다.

Windows 클라이언트에서의 장애 조치 경험

한 파일 서버에서 다른 파일 서버로 장애 조치하면 새 활성 파일 서버가 자동으로 모든 파일 시스템 읽기 및 쓰기 요청을 처리하기 시작합니다. 기본 서브넷의 리소스를 사용할 수 있게 되면 Amazon FSx는 자동으로 기본 서브넷의 기본 파일 서버로 페일백합니다. 파일 시스템의 DNS 이름이 동일하게 유지되기 때문에 Windows 애플리케이션에서는 장애 조치의 영향 없이, 그리고 수동 개입 없이 파일 시스템 작업을 재개할 수 있습니다. 활성 파일 서버에서 장애가 감지된 후 대기 파일 서버가 활성 상태로 승격되기까지 보통 30초 이내에 장애 조치가 완료됩니다. 원래 다중 AZ 구성으로의 페일백도 30초 이내에 완료되며 기본 서브넷의 파일 서버가 완전히 복구된 후에만 발생합니다.

Linux 클라이언트에서의 장애 조치 경험

Linux 클라이언트는 자동 DNS 기반 장애 조치를 지원하지 않습니다. 따라서 장애 조치 중에는 대기 파일 서버에 자동으로 연결되지 않습니다. 다중 AZ 파일 시스템이 기본 서브넷의 파일 서버로 페일백되면 자동으로 파일 시스템 작업이 재개됩니다.

파일 시스템에서 장애 조치 테스트

처리량 용량을 수정하여 다중 AZ 파일 시스템에서 장애 조치를 테스트할 수 있습니다. 파일 시스템의 처리량 용량을 수정하면 Amazon FSx가 파일 시스템의 파일 서버를 교체합니다. Amazon FSx가 기본 서버의 파일 서버를 먼저 대체하는 동안 다중 AZ 파일 시스템은 자동으로 보조 서버로 장애 조치합니다. 그러면 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. 업데이트가 완료되면 파일 시스템이 보조 서버로 장애 조치되고 기본 서버로 페일백됩니다. 파일 시스템의 처리량 용량을 수정하고 요청 진행 상황을 모니터링하는 방법에 대한 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

단일 및 다중 AZ 파일 시스템 리소스 작업

서브넷

VPC를 생성하면 리전의 모든 가용 영역에 적용됩니다. 각 가용 영역은 다른 가용 영역에서 발생한 장애를 격리시킬 수 있도록 서로 분리된 공간이어야 합니다. VPC를 만든 후 각 가용 영역에 하나 이상의 서브넷을 추가할 수 있습니다. 기본 VPC는 각 가용 영역에 서브넷을 가지고 있습니다. 각 서브넷은 단일 가용 영역 내에서만 존재해야 하며, 여러 영역으로 스케일 아웃할 수 없습니다. 단일 AZ Amazon FSx 파일 시스템을 생성할 때는 파일 시스템에 단일 서브넷을 지정합니다. 선택하는 서브넷에 따라 파일 시스템이 생성되는 가용 영역이 정의됩니다.

다중 AZ 파일 시스템을 생성할 때는 2개의 서브넷을 지정하는데, 하나는 기본 파일 서버용이고 다른 하나는 대기 파일 서버용입니다. 선택한 두 서브넷은 같은 지역 내의 서로 다른 가용 영역에 있어야 합니다. AWS

AWS 인-애플리케이션의 경우 지연 시간을 최소화하기 위해 선호하는 파일 서버와 동일한 가용 영역에서 클라이언트를 시작하는 것이 좋습니다.

파일 시스템 탄력적 네트워크 인터페이스

Amazon FSx 파일 시스템을 생성하면 Amazon FSx는 사용자가 파일 시스템과 연결하는 Amazon Virtual Private Cloud(VPC)에 하나 이상의 탄력적 네트워크 인터페이스를 프로비저닝합니다. 네트워크 인터페이스를 통해 클라이언트가 FSx for Windows File Server 파일 시스템과 통신할 수 있습니다. 네트워크 인터페이스는 사용자 계정의 VPC에 속해 있음에도 불구하고 Amazon FSx의 서비스 범위 내에 있는 것으로 간주됩니다. 다중 AZ 파일 시스템에는 각 파일 서버마다 하나씩, 두 개의 탄력적 네트워크 인터페이스가 있습니다. 단일 AZ 파일 시스템에는 하나의 탄력적 네트워크 인터페이스가 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.

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

파일 시스템 배포 유형	서브넷 수	탄력적 네트워크 인터페이스 수	IP 주소 수
단일 AZ 2	1	1	2
단일 AZ 1	1	1	1
다중 AZ	2	2	4

파일 시스템이 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. 인터넷에서 연결할 수 있는 퍼블릭 IP 주소인 탄력적 IP 주소가 파일 시스템의 탄력적 네트워크 인터페이스에 연결되면 Amazon FSx가 이를 자동으로 분리합니다.

Amazon FSx를 사용한 비용 최적화

FSx for Windows File Server는 애플리케이션 요구 사항에 따라 총 소유 비용(TCO)을 최적화하는 데 도움이 되는 여러 기능을 제공합니다. 스토리지 유형(HDD 또는 SSD)을 선택하여 애플리케이션에 필요한 비용과 성능 사이에서 적절한 균형을 맞출 수 있습니다. 스토리지 용량과 별도로 처리량 용량을 선택하여 비용을 최적화할 수 있는 유연성이 있습니다. 또한 데이터 중복 제거를 사용하면 파일 시스템에서 중복 데이터를 제거하여 스토리지 비용을 최적화할 수 있습니다.

주제

스토리지와 처리량을 독립적으로 선택할 수 있는 유연성

FSx for Windows File Server를 사용하면 파일 시스템의 스토리지, SSD IOPS 및 처리량 용량을 독립적으로 구성할 수 있습니다. 이를 통해 비용과 성능을 적절히 조합할 수 있는 유연성을 확보할 수 있습니다. 예를 들어, 사용량이 적은(일반적으로 비활성) 워크로드에 대해서는 비교적 적은 처리량 용량의 대용량 스토리지를 선택하여 불필요한 처리량 비용을 절감할 수 있습니다. 또 다른 예로, 비교적 적은 스토리지 용량에 대해 큰 처리량 용량을 선택할 수 있습니다. 처리량 용량이 높을수록 파일 서버의 캐싱에 사용할 메모리 양도 많아집니다. 파일 서버의 고속 캐싱을 활용하여 활발하게 액세스하는 데이터의 성능을 최적화할 수 있습니다. 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

파일 시스템을 생성한 후 언제든지 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요. 파일 시스템을 생성한 후 언제든지 스토리지 용량과 관계없이 SSD IOPS를 스케일할 수 있습니다. 자세한 내용은 SSD IOPS 관리 섹션을 참조하세요. 언제든지 처리량 용량을 늘리거나 줄일 수 있으므로 변화하는 성능 요구 사항을 유연하게 해결할 수 있습니다. 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

스토리지 비용 최적화

Amazon FSx를 사용하면 다음과 같은 다양한 방법으로 스토리지 비용을 최적화할 수 있습니다.

스토리지 유형을 사용한 비용 최적화

FSx for Windows File Server는 하드 디스크 드라이브(HDD)와 솔리드 스테이트 드라이브(SSD)라는 두 가지 유형의 스토리지를 제공하므로 워크로드 요구 사항에 맞게 비용 및 성능을 최적화할 수 있습니다. HDD 스토리지는 홈 디렉터리, 사용자 및 부서별 공유, 콘텐츠 관리 시스템 등 광범위한 워크로드에 맞게 설계되었습니다. SSD 스토리지는 데이터베이스, 미디어 처리 워크로드, 데이터 분석 애플리케이션을 포함하여 성능이 가장 높고 지연 시간에 민감한 워크로드용으로 설계되었습니다. 요금 정보는 지연 시간 및 Amazon FSx for Windows File Server 요금을 참조하세요.

데이터 중복 제거를 사용한 스토리지 비용 최적화

대규모 데이터 세트에는 종종 데이터가 중복되어 있어 데이터 스토리지 비용이 증가합니다. 예를 들어 사용자 파일 공유에는 여러 사용자가 저장하는 동일한 파일의 사본이 여러 개 있을 수 있습니다. 소프트웨어 개발 공유에는 빌드마다 변경되지 않는 바이너리가 많이 포함될 수 있습니다. 파일 시스템에서 데이터 중복 제거를 활성화하여 데이터 스토리지 비용을 줄일 수 있습니다. 데이터 중복 제거가 활성화되어 있으면 데이터 세트의 중복된 부분을 한 번만 저장하여 중복 데이터를 자동으로 줄이거나 제거합니다. 데이터 중복 제거에 대한 자세한 내용 및 Amazon FSx 파일 시스템에서 데이터 중복 제거를 쉽게 활성화하는 방법에 대한 자세한 내용은 데이터 중복 제거 섹션을 참조하세요.

사용량 및 결제 검토

AWS Billing 대시보드 또는 AWS Cost Explorer를 사용하여 스토리지 용량, 처리량 용량, 백업 및 데이터 전송을 포함한 파일 시스템 사용량을 검토할 수 있습니다. 이러한 도구를 사용하면 리소스 사용량을 검토하고 사용량 유형, 리전 및 기타 관련 기준별로 필터링 및 그룹화할 수 있습니다. 단일 파일 시스템 또는 단일 파일 시스템 백업의 사용량을 보려면 해당 리소스의 태그를 활성화하고 태그 기반 결제 보고를 활성화해야 합니다. 자세한 내용은 AWS Billing 사용 설명서에서 AWS 비용 할당 태그 사용을 참조하세요.

FSx for Windows File Server에서 Microsoft Active Directory 작업

Amazon FSx는 마이크로소프트 액티브 디렉터리와 함께 작동하여 기존 마이크로소프트 윈도우 환경과 통합됩니다. Active Directory는 네트워크상의 개체에 대한 정보를 저장하고 관리자 및 사용자가 해당 정보를 쉽게 찾아 사용할 수 있도록 지원하는 데 사용되는 Microsoft 디렉터리 서비스입니다. 이러한 객체에는 일반적으로 파일 서버, 네트워크 사용자 및 컴퓨터 계정과 같은 공유 리소스가 포함됩니다.

Amazon FSx로 파일 시스템을 생성할 때는 Active Directory 도메인에 조인하여 사용자 인증과 파일 및 폴더 수준의 액세스 제어를 제공합니다. 그러면 사용자는 Active Directory의 기존 사용자 ID를 사용하여 자신을 인증하고 Amazon FSx 파일 시스템에 액세스할 수 있습니다. 또한 사용자는 기존 ID를 사용하여 개별 파일 및 폴더에 대한 액세스를 제어할 수 있습니다. 또한 기존 파일 및 폴더와 이들 항목의 보안 액세스 제어 목록(ACL) 구성을 수정 없이 Amazon FSx로 마이그레이션할 수 있습니다.

Amazon FSx는 Active Directory와 함께 FSx for Windows File Server 파일 시스템을 사용하기 위한 두 가지 옵션, 즉 아마존 FSx를 다음과 함께 사용하기 AWS Directory Service for Microsoft Active Directory 및 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용를 제공합니다.

> **Note**
>
> Amazon FSx는 Microsoft Azure Active Directory 도메인 서비스를 지원하며, 사용자는 Microsoft Azure Active Directory에 조인할 수 있습니다.

파일 시스템에 대해 조인된 Active Directory 구성을 생성한 후에는 다음 속성만 업데이트할 수 있습니다.

- 서비스 사용자 보안 인증
- DNS 서버 IP 주소

파일 시스템을 만든 후에는 가입한 Microsoft AD의 다음 속성을 변경할 수 없습니다.

- DomainName
- OrganizationalUnitDistinguishedName
- FileSystemAdministratorsGroup

하지만 백업에서 새 파일 시스템을 만들고 새 파일 시스템에 대한 Microsoft Active Directory 통합 구성에서 이러한 속성을 변경할 수 있습니다. 자세한 정보는 연습 2: 백업에서 파일 시스템 생성을 참조하세요.

> **Note**
>
> Amazon FSx는 Active Directory Connector 및 Simple Active Directory를 지원하지 않습니다.

Active Directory 구성이 변경되어 파일 시스템에 대한 연결이 중단되는 경우 FSx for Windows File Server가 잘못 구성될 수 있습니다. 파일 시스템을 사용 가능 상태로 되돌리려면 Amazon FSx 콘솔에서 복구 시도 버튼을 선택하거나 Amazon FSx API 또는 콘솔에서 `StartMisconfiguredStateRecovery` 명령을 사용합니다. 자세한 내용은 파일 시스템이 잘못 구성된 상태 섹션을 참조하세요.

주제

- 아마존 FSx를 다음과 함께 사용하기 AWS Directory Service for Microsoft Active Directory
- 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용

아마존 FSx를 다음과 함께 사용하기 AWS Directory Service for Microsoft Active Directory

AWS Directory Service for Microsoft Active Directory (AWS Managed Microsoft AD) 는 클라우드에서 완전히 관리되고 가용성이 높은 실제 Active Directory 디렉터리를 제공합니다. 워크로드 배포에 이러한 Active Directory 디렉터리를 사용할 수 있습니다.

조직에서 ID 및 디바이스를 관리하는 AWS Managed Microsoft AD 데 사용하는 경우 Amazon FSx 파일 시스템을 과 통합하는 것이 좋습니다. AWS Managed Microsoft AD이렇게 하면 Amazon FSx를 사용하여 턴키 솔루션을 얻을 수 있습니다. AWS Managed Microsoft AD AWS 두 서비스의 배포, 운영, 고가용성, 안정성, 보안 및 원활한 통합을 처리하므로 사용자는 자신의 워크로드를 효과적으로 운영하는 데 집중할 수 있습니다.

설정과 함께 Amazon FSx를 사용하려면 Amazon FSx 콘솔을 사용할 수 AWS Managed Microsoft AD 있습니다.AWS 콘솔에서 Windows File Server용 FSx 파일 시스템을 새로 만드는 경우 Windows 인증 섹션에서 관리형 Active Directory를 선택합니다. 사용하려는 특정 디렉터리를 선택할 수도 있습니다. 자세한 내용은 파일 시스템 생성 섹션을 참조하세요.

조직은 자체 관리형 Active Directory 도메인(온프레미스 또는 클라우드에서)에서 ID와 디바이스를 관리할 수 있습니다. 그렇다면 Amazon FSx 파일 시스템을 기존의 자체 관리형 Active Directory 도메인에 직접 가입할 수 있습니다. 자세한 정보는 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용을 참조하세요.

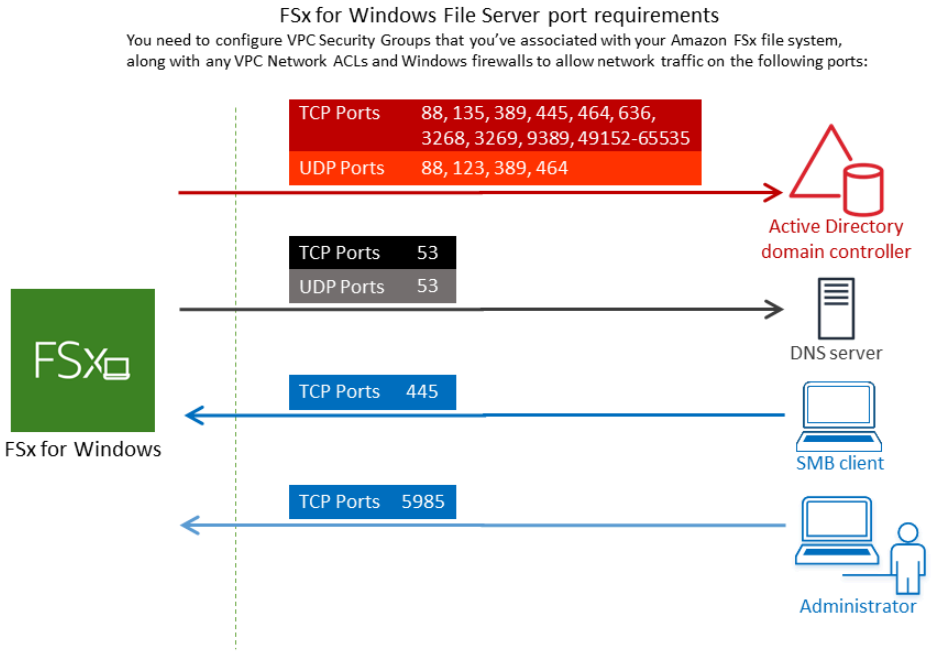
또한 리소스 포리스트 격리 모델을 활용하도록 시스템을 설정할 수도 있습니다. 이 모델에서는 Amazon FSx 파일 시스템을 비롯한 리소스를 사용자가 있는 Active Directory 포리스트와 별도의 Active Directory 포리스트로 분리합니다.

> **Important**
>
> 단일 AZ 2 및 모든 다중 AZ 파일 시스템의 경우 Active Directory 도메인 이름은 47자를 초과할 수 없습니다.

네트워킹 사전 조건

Microsoft 관리형 Active Directory 도메인에 가입된 Windows File Server용 FSx 파일 시스템을 생성하기 AWS 전에 다음 네트워크 구성을 만들고 설정했는지 확인하십시오.

- VPC 보안 그룹의 경우 기본 Amazon VPC의 기본 보안 그룹이 콘솔의 파일 시스템에 이미 추가되었습니다. FSx 파일 시스템을 만드는 서브넷의 보안 그룹과 VPC 네트워크 ACL이 다음 다이어그램에 표시된 방향으로 포트를 통한 트래픽을 허용하는지 확인합니다.



다음 테이블에는 각 포트의 역할이 나와 있습니다.

프로토콜	포트	역할
TCP/UDP	53	도메인 이름 시스템(DNS)
TCP/UDP	88	Kerbe 인증

프로토콜	포트	역할
TCP/UDP	464	암호 변경/설정
TCP/UDP	389	LDAP tweigh Direct Acces Protoc
UDP	123	NTP(N rk Time Protoc

프로토콜	포트	역할
TCP	135	분산 컴퓨팅 환경/엔드포인트 매퍼(DCE/EP MAP)
TCP	445	디렉터리 서비스 SMB 파일 공유

프로토콜	포트	역할
TCP	636	Lightweight Directory Access Protocol over TLS/SSL(LDAPS
TCP	3268	Microsoft 글로벌 카탈로그
TCP	3269	SSL을 통한 Microsoft 글로벌 카탈로그

프로토콜	포트	역할
TCP	5985	WinRM 2.0(Microsoft Windows Remote Management)
TCP	9389	마이크로소프트 AD DS 웹 서비스, PowerShell
TCP	49,152~65,535	RPC 용 임시 포트

> **Important**
>
> 단일 AZ 2 및 모든 다중 AZ 파일 시스템 배포에는 TCP 포트 9389에서 아웃바운드 트래픽을 허용해야 합니다.

> **Note**
>
> VPC 네트워크 ACL을 사용하는 경우 FSx 파일 시스템의 동적 포트(49152~65535)를 통한 아웃바운드 트래픽도 허용해야 합니다.

- Amazon FSx 파일 시스템을 다른 VPC 또는 계정의 AWS 관리형 Microsoft Active Directory에 연결하는 경우, 파일 시스템을 생성하려는 Amazon VPC와 해당 VPC가 연결되어 있는지 확인하십시오. 자세한 정보는 다른 VPC 또는 계정에서 Amazon FSx AWS Managed Microsoft AD 사용하기을 참조하세요.

> **Important**
>
> Amazon VPC 보안 그룹에서는 네트워크 트래픽이 시작되는 방향으로만 포트를 열어야 하지만, VPC 네트워크 ACL에서는 포트가 양방향으로 열려 있어야 합니다.

Amazon FSx 네트워크 검증 도구를 사용하여 Active Directory 도메인 컨트롤러에 대한 연결을 검증합니다.

리소스 포리스트 격리 모델 사용

파일 시스템을 AWS Managed Microsoft AD 설정에 조인합니다. 그런 다음 생성한 도메인과 기존의 자체 관리형 Active AWS Managed Microsoft AD Directory 도메인 간에 단방향 포리스트 신뢰 관계를 설정합니다. Amazon FSx의 Windows 인증에는 관리형 포리스트가 기업 도메인 포리스트를 신뢰하는 단방향 포리스트 트러스트만 필요합니다. AWS

기업 도메인은 신뢰할 수 있는 도메인의 역할을 하고, AWS Directory Service 관리형 도메인은 트러스팅 도메인의 역할을 합니다. 검증된 인증 요청은 도메인 간에 한 방향으로만 전달되며 회사 도메인의 계정이 관리형 도메인에서 공유되는 리소스에 대해 인증합니다. 이 경우 Amazon FSx는 관리형 도메인과만 상호 작용합니다. 그러면 관리형 도메인은 인증 요청을 기업 도메인으로 전달합니다.

Active Directory 구성 테스트

Amazon FSx 파일 시스템을 생성하기 전에 Amazon FSx 네트워크 검증 도구를 사용하여 Active Directory 도메인 컨트롤러에 대한 연결을 검증하는 것이 좋습니다. 자세한 정보는 Active Directory 도메인 컨트롤러에 대한 연결 검증을 참조하세요.

Windows File Server용 FSx를 사용할 AWS Directory Service for Microsoft Active Directory 때 다음과 같은 관련 리소스가 도움이 될 수 있습니다.

- AWS Directory Service 관리 가이드의 AWS Directory Service란?
- AWS Directory Service 관리 가이드에서 AWS 관리형 Active Directory를 생성하십시오.
- AWS Directory Service 관리 안내서의 신뢰 관계 생성 시기
- 연습 1: 시작을 위한 사전 조건

다른 VPC 또는 계정에서 Amazon FSx AWS Managed Microsoft AD 사용하기

VPC 피어링을 사용하여 Windows File Server용 FSx 파일 시스템을 동일한 계정 내의 다른 VPC에 있는 디렉터리에 AWS Managed Microsoft AD 조인할 수 있습니다. 디렉터리 공유를 사용하여 다른 AWS 계정에 있는 AWS Managed Microsoft AD 디렉터리에 파일 시스템을 조인할 수도 있습니다.

> **Note**
>
> 파일 시스템과 AWS 리전 동일한 파일 AWS Managed Microsoft AD 내에서만 하나를 선택할 수 있습니다. 리전 간 VPC 피어링 설정을 사용하려면 자체 관리형 Microsoft Active Directory를 사용해야 합니다. 자세한 정보는 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용을 참조하세요.

파일 시스템을 다른 VPC에 AWS Managed Microsoft AD 있는 VPC에 조인하는 워크플로에는 다음 단계가 포함됩니다.

1. 네트워킹 환경 설정
2. 디렉터리 공유
3. 파일 시스템을 공유 디렉터리에 조인합니다.

자세한 내용은 AWS Directory Service 관리 가이드의 디렉터리 공유를 참조하세요.

네트워킹 환경을 설정하려면 Amazon VPC를 사용하고 AWS Transit Gateway VPC 피어링 연결을 생성할 수 있습니다. 또한 두 VPC 간에 네트워크 트래픽이 허용되도록 해야 합니다.

전송 게이트웨이는 VPC와 온프레미스 네트워크를 상호 연결하는 데 사용할 수 있는 네트워크 전송 허브입니다. VPC 전송 게이트웨이 사용에 대한 자세한 내용은 Amazon VPC Transit Gateway 가이드의 전송 게이트웨이 시작하기 섹션을 참조하세요.

VPC 피어링 연결은 두 VPC 간의 네트워킹 연결입니다. 이러한 연결을 사용하면 프라이빗 Internet Protocol version 4(IPv4) 또는 Internet Protocol version 6(IPv6) 주소를 사용하여 이들 간의 트래픽을 라우팅할 수 있습니다. VPC 피어링을 사용하여 동일한 AWS 지역 내 또는 지역 간에 VPC를 연결할 수 있습니다. AWS VPC 피어링에 대한 자세한 내용은 Amazon VPC 피어링 가이드의 VPC 피어링이란?을 참조하세요.

파일 시스템이 아닌 다른 계정의 AWS Managed Microsoft AD 디렉터리에 파일 시스템을 조인할 때는 또 다른 전제 조건이 있습니다. 또한 Microsoft Active Directory를 다른 계정과 공유해야 합니다. 이렇게 하려면 AWS 관리형 Microsoft Active Directory의 디렉터리 공유 기능을 사용할 수 있습니다. 자세히 알아보려면 AWS Directory Service 관리 가이드의 디렉터리 공유를 참조하세요.

Active Directory 도메인 컨트롤러에 대한 연결 검증

Active Directory에 조인할 FSx for Windows File Server 파일 시스템을 생성하기 전에 Amazon FSx Active Directory 검증 도구를 사용하여 Active Directory 도메인에 대한 연결을 검증하는 것이 좋습니다. Windows File Server용 FSx를 관리형 Microsoft Active Directory와 함께 사용하든 자체 관리형 Active Directory AWS 구성과 함께 사용하든 관계없이 이 테스트를 사용할 수 있습니다. 도메인 컨트롤러 네트워크 연결 테스트 (Test-FSxADControllerConnection) 는 도메인의 모든 도메인 컨트롤러에 대해 전체 네트워크 연결 검사를 실행하지는 않습니다. 대신 이 테스트를 사용하여 특정 도메인 컨트롤러 세트에 대해 네트워크 연결 검증을 실행합니다.

Active Directory 도메인 컨트롤러에 대한 연결 검증

1. FSx for Windows File Server 파일 시스템에 사용할 동일한 Amazon VPC 보안 그룹 및 동일한 서브넷에서 Amazon EC2 Windows 인스턴스를 시작합니다. 다중 AZ 배포 유형의 경우 기본 활성 파일 서버의 서브넷을 사용합니다.
2. EC2 Windows 인스턴스를 Active Directory에 조인합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Windows 인스턴스 수동 조인을 참조하세요.
3. EC2 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

4. EC2 인스턴스에서 Windows PowerShell 창 (관리자 권한으로 실행 사용) 을 엽니다.

   Windows용 필수 Active Directory PowerShell 모듈이 설치되어 있는지 테스트하려면 다음 테스트 명령을 사용하십시오.

```
PS C:\> Import-Module ActiveDirectory
```

   테스트 명령이 오류를 반환하면 다음 명령을 사용하여 모듈을 설치합니다.

```
PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
```

5. 다음 명령을 사용하여 네트워크 검증 도구를 다운로드합니다.

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

6. 다음 명령을 사용하여 zip 파일을 확장합니다.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. AmazonFSxADValidation 모듈을 현재 세션에 추가합니다.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. Active Directory 도메인 컨트롤러 IP 주소 값을 설정하고 다음 명령을 사용하여 연결 테스트를 실행합니다.

```
$ADControllerIp = '10.0.75.243'
$Result = Test-FSxADControllerConnection -ADControllerIp $ADControllerIp
```

9. 다음 예제는 테스트 출력을 검색하여 성공적인 연결 테스트 결과를 보여주는 것입니다.

```
PS C:\AmazonFSxADValidation> $Result

Name                           Value
----                           -----
TcpDetails                     {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
```

```
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         True


PS C:\AmazonFSxADValidation> $Result.TcpDetails

Port Result    Description
---- ------    -----------
  88 Listening Kerberos authentication
 135 Listening DCE / EPMAP (End Point Mapper)
 389 Listening Lightweight Directory Access Protocol (LDAP)
 445 Listening Directory Services SMB file sharing
 464 Listening Kerberos Change/Set password
 636 Listening Lightweight Directory Access Protocol over TLS/SSL (LDAPS)
3268 Listening Microsoft Global Catalog
3269 Listening Microsoft Global Catalog over SSL
9389 Listening Microsoft AD DS Web Services, PowerShell
```

다음 예제는 테스트를 실행하여 실패한 결과를 보여주는 것입니다.

```
PS C:\AmazonFSxADValidation> $Result = Test-FSxADControllerConnection -
ADControllerIp $ADControllerIp
WARNING: TCP 9389 failed to connect. Required for Microsoft AD DS Web Services,
 PowerShell.
Verify security group and firewall settings on both client and directory
 controller.
WARNING: 1 ports failed to connect to 10.0.75.243. Check pre-requisites in
https://docs.aws.amazon.com/fsx/latest/WindowsGuide/self-managed-AD.html#self-
manage-prereqs

PS C:\AmazonFSxADValidation> $Result

Name                            Value
----                            -----
TcpDetails                      {@{Port=88; Result=Listening; Description=Kerberos
 authentication}, @{Port=135; Resul...
Server                          10.0.75.243
UdpDetails                      {@{Port=88; Result=Timed Out; Description=Kerberos
 authentication}, @{Port=123; Resul...
Success                         False
FailedTcpPorts                  {9389}
```

```
PS C:\AmazonFSxADValidation> $Result.FailedTcpPorts
9389
```

```
Windows socket error code mapping

https://msdn.microsoft.com/en-us/library/ms740668.aspx
```

자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용

조직이 자체 관리형 Active Directory 온프레미스 또는 클라우드에서 ID 및 디바이스를 관리하는 경우 Amazon FSx 파일 시스템을 기존의 자체 관리형 Active Directory 도메인에 직접 조인할 수 있습니다. 에서 Amazon FSx를 사용하려면 Amazon FSx AWS Managed Microsoft AD콘솔을 사용하면 됩니다. 콘솔에서 새 FSx for Windows File Server파일 시스템을 생성할 때는 Windows 인증에서 자체 관리형 Microsoft Active Directory를 선택합니다. 다음 자체 관리형 Active Directory 세부 정보를 제공합니다.

- 자체 관리형 디렉터리의 정규화된 도메인 이름

> **Note**
>
> 도메인 이름은 단일 레이블 도메인(SLD) 형식일 수 없습니다. Amazon FSx는 현재 SLD 도메인을 지원하지 않습니다.

> **Note**
>
> 단일 AZ 2 및 다중 AZ 파일 시스템의 경우, Active Directory 도메인 이름은 47자를 초과할 수 없습니다.

- 도메인의 DNS 서버 IP 주소

  DNS 서버 IP 주소, Active Directory 도메인 컨트롤러 IP 주소 및 클라이언트 네트워크는 다음 요구 사항을 충족해야 합니다.

2020년 12월 17일 이전에 생성된 파일 시스템의 경우	2020년 12월 17일 이후에 생성된 파일 시스템의 경우
IP 주소는 RFC 1918 프라이빗 IP 주소 범위 내에 있어야 합니다. • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 주소는 다음을 제외한 모든 범위에 속할 수 있습니다. • 해당 AWS 지역의 Amazon Web Services 소유 IP 주소와 충돌하는 IP 주소 지역별 AWS 소유 IP 주소 목록은 AWS IP 주소 범위를 참조하십시오. • 다음 CIDR 블록 범위의 IP 주소: 198.19.0.0/16

> **Note**
>
> Active Directory 도메인 컨트롤러는 쓰기가 가능해야 합니다.

- Amazon FSx가 파일 시스템을 Active Directory 도메인에 조인하는 데 사용할 Active Directory 도메인에 있는 서비스 계정의 사용자 이름 및 암호
- (선택 사항) 파일 시스템을 조인하려는 도메인의 조직 구성 단위(OU)
- (선택 사항) 파일 시스템에서 관리 작업을 수행할 권한을 위임하는 도메인 그룹. 예를 들어 도메인 그룹은 Windows 파일 공유를 관리하고, 파일 시스템의 루트 폴더에 있는 액세스 제어 목록(ACL)을 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.

> **Note**
>
> 제공하는 도메인 그룹 이름은 Active Directory에서 고유해야 합니다. Windows File Server용 FSx는 다음과 같은 상황에서는 도메인 그룹을 만들지 않습니다.
>
> - 지정한 이름을 가진 그룹이 이미 있는 경우
> - 이름을 지정하지 않고 Active Directory에 “도메인 관리자”라는 이름의 그룹이 이미 존재하는 경우

자세한 정보는 Amazon FSx 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인을 참조하세요.

> **Important**
>
> Amazon FSx는 Microsoft DNS를 기본 DNS 서비스로 사용하는 경우에만 파일 시스템의 DNS 레코드를 등록합니다. 타사 DNS를 사용하는 경우 파일 시스템을 생성한 후 Amazon FSx 파일 시스템의 DNS 항목을 수동으로 설정해야 합니다.

파일 시스템을 자체 관리형 Active Directory에 직접 조인하면 FSx for Windows File Server가 동일한 Active Directory 포리스트(도메인, 사용자 및 컴퓨터를 포함하는 Active Directory 구성의 최상위 논리 컨테이너)에 있고, 사용자 및 기존 리소스(기존 파일 서버 포함)와 동일한 Active Directory 도메인에 있습니다.

> **Note**
>
> Amazon FSx 파일 시스템을 비롯한 리소스를 사용자가 있는 Active Directory 포리스트와 별도의 Active Directory 포리스트로 분리할 수 있습니다. 이렇게 하려면 파일 시스템을 관리형 Active Directory에 가입시키고 생성한 AWS 관리형 Active Directory와 기존의 자체 AWS 관리형 Active Directory 간에 단방향 포리스트 신뢰 관계를 설정하십시오.

주제

- 자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항
- FSx for Windows File Server 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인하는 모범 사례
- Active Directory 구성 검증
- Amazon FSx 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인
- DNS에 사용할 올바른 파일 시스템 IP 주소 획득
- 자체 관리형 Active Directory 구성 업데이트

자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항

자체 관리형 Microsoft Active Directory 도메인에 연결된 Amazon FSx 파일 시스템을 생성하기 전에 다음 사전 요구 사항을 검토합니다.

주제

온프레미스 구성

Amazon FSx 파일 시스템을 조인할 수 있는 온프레미스 또는 기타 자체 관리형 Microsoft Active Directory가 있어야 합니다. 온프레미스 Active Directory 구성이 다음과 같아야 합니다.

- Active Directory 도메인 컨트롤러의 도메인 기능 수준은 Windows Server 2008 R2 이상입니다.
- DNS 서버 IP 주소 및 Active Directory 도메인 컨트롤러 IP 주소는 파일 시스템이 생성된 시기에 따라 다음과 같습니다.

2020년 12월 17일 이전에 생성된 파일 시스템의 경우	2020년 12월 17일 이후에 생성된 파일 시스템의 경우
IP 주소는 RFC 1918 프라이빗 IP 주소 범위 내에 있어야 합니다. • 10.0.0.0/8 • 172.16.0.0/12 • 192.168.0.0/16	IP 주소는 다음을 제외한 모든 범위에 속할 수 있습니다. • 해당 AWS 지역의 Amazon Web Services 소유 IP 주소와 충돌하는 IP 주소 지역별 AWS 소유 IP 주소 목록은 AWS IP 주소 범위를 참조하십시오. • 다음 CIDR 블록 범위의 IP 주소: 198.19.0.0/16

프라이빗 IP 주소 범위 밖의 2020년 12월 17일 이전에 생성된 FSx for Windows File Server 파일 시스템에 액세스해야 하는 경우, 파일 시스템의 백업을 복원하여 새 파일 시스템을 생성할 수 있습니다. 자세한 정보는 백업 작업을 참조하세요.

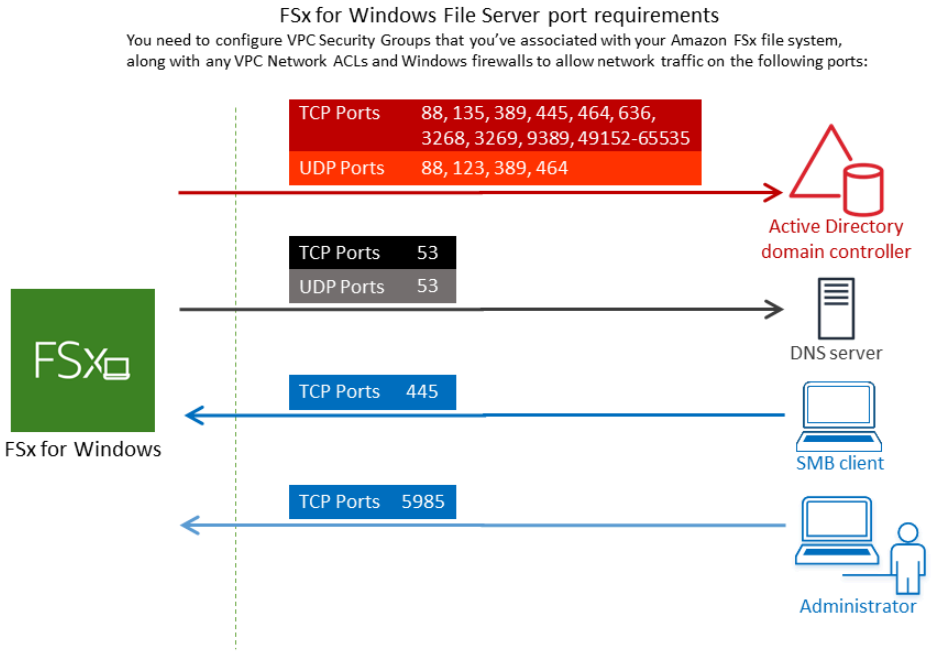
- 도메인 이름 단일 레이블 도메인(SLD) 형식이 아닙니다. Amazon FSx는 현재 SLD 도메인을 지원하지 않습니다.
- 단일 AZ 2 및 모든 다중 AZ 파일 시스템의 경우 Active Directory 도메인 이름은 47자를 초과할 수 없습니다.
- Microsoft Active Directory 사이트가 정의되어 있는 경우에는 Amazon FSx 파일 시스템과 연결된 VPC의 서브넷이 Microsoft Active Directory 사이트에 정의되어 있도록 하고 VPC의 서브넷과 다른 사이트의 서브넷 간에 충돌이 존재하지 않도록 해야 합니다.
- Active Directory 도메인 컨트롤러와 Amazon FSx 간의 ICMP 트래픽을 허용하려면 방화벽에 규칙을 추가해야 할 수 있습니다.

네트워크 구성

이 섹션에서는 파일 시스템을 자체 관리형 Active Directory에 연결하는 데 필요한 네트워크 구성을 설명합니다.

파일 시스템을 자체 관리형 Active Directory에 연결하기 전에 Amazon FSx Active Directory 검증 도구를 사용하여 네트워크 설정을 테스트하는 것이 좋습니다.

- 파일 시스템을 생성하려는 Amazon VPC와 자체 관리형 Active Directory 간에 연결성이 있어야 합니다. AWS Direct Connect, AWS Virtual Private Network, VPC 피어링 또는 를 사용하여 이 연결을 설정할 수 있습니다. AWS Transit Gateway
- VPC 보안 그룹의 경우 기본 Amazon VPC의 기본 보안 그룹이 콘솔의 파일 시스템에 추가되어 있어야 합니다. FSx 파일 시스템을 만드는 서브넷의 보안 그룹과 VPC 네트워크 ACL이 다음 다이어그램에 표시된 방향으로 포트를 통한 트래픽을 허용하는지 확인합니다.



다음 테이블에는 각 포트의 역할이 나와 있습니다.

프로토콜	포트	역할
TCP/UDP	53	도메인 이름 시스템(DNS)
TCP/UDP	88	Kerberos 인증
TCP/UDP	464	암호 변경/설정
TCP/UDP	389	LDAP(Lightweight Directory Access Protocol)
UDP	123	NTP(Network Time Protocol)
TCP	135	분산 컴퓨팅 환경/엔드포인트 매퍼(DCE/EPMAP)
TCP	445	디렉터리 서비스 SMB 파일 공유
TCP	636	Lightweight Directory Access Protocol over TLS/SSL(LDAPS)

프로토콜	포트	역할
TCP	3268	Microsoft 글로벌 카탈로그
TCP	3269	SSL을 통한 Microsoft 글로벌 카탈로그
TCP	5985	WinRM 2.0(Microsoft Windows Remote Management)
TCP	9389	마이크로소프트 액티브 디렉터리 DS 웹 서비스, PowerShell
TCP	49,152~65,535	RPC용 임시 포트

이러한 트래픽 규칙이 각 Active Directory 도메인 컨트롤러, DNS 서버 및 FSx 클라이언트, FSx 관리자에 적용되는 방화벽에도 반영되는지 확인하세요.

Important

단일 AZ 2 및 다중 AZ 파일 시스템 배포에는 TCP 포트 9389에서 아웃바운드 트래픽을 허용해야 합니다.

Note

VPC 네트워크 ACL을 사용하는 경우 FSx 파일 시스템의 동적 포트(49152~65535)를 통한 아웃바운드 트래픽도 허용해야 합니다.

Important

Amazon VPC 보안 그룹에서는 네트워크 트래픽이 시작되는 방향으로만 포트를 열어야 하지만, 대부분의 Windows 방화벽과 VPC 네트워크 ACL에서는 포트가 양방향으로 열려 있어야 합니다.

서비스 계정 권한

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.

서비스 계정은 파일 시스템에 조인하려는 OU에서 최소한 다음 권한을 위임받아야 합니다.

- 암호 재설정 기능
- 계정의 데이터 읽기 및 쓰기 제한 기능
- 검증된 DNS 호스트 이름 쓰기 기능
- 검증된 서비스 보안 주체 이름 쓰기 기능
- 컴퓨터 객체의 생성 및 삭제 기능(위임 가능)
- 검증된 계정 제한 사항의 읽기 및 쓰기 기능
- 권한 수정 기능

이는 컴퓨터 객체를 Active Directory에 조인하는 데 필요한 최소 권한 집합을 나타냅니다. 자세한 내용은 Microsoft Windows Server 설명서의 오류: 제어를 위임받은 관리자가 아닌 사용자가 컴퓨터를 도메인 컨트롤러에 조인하려고 하면 액세스가 거부됨 항목을 참조하세요.

올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

Amazon FSx를 사용하려면 Amazon FSx 파일 시스템의 수명 주기 동안 유효한 서비스 계정이 필요합니다. Amazon FSx는 파일 시스템을 완벽하게 관리할 수 있어야 하며, 서비스 계정을 사용하여 Active Directory 도메인에 가입을 취소했다가 다시 가입해야 하는 작업을 수행할 수 있어야 합니다. 이러한 작업에는 장애가 발생한 파일 서버 교체 또는 Windows Server 소프트웨어 패치 적용이 포함됩니다. 반드시 Amazon FSx를 사용하여 서비스 계정 자격 증명을 포함한 Active Directory 구성을 업데이트해야 합니다. 자세한 정보는 Active Directory 구성을 최신 상태로 유지을 참조하세요.

Amazon FSx는 Active Directory 환경의 모든 도메인 컨트롤러에 연결해야 합니다. 도메인 컨트롤러가 여러 개 있는 경우 모든 도메인 컨트롤러가 위의 요구 사항을 충족하는지 확인하고, 서비스 계정 변경 사항이 모든 도메인 컨트롤러에 전파되는지 확인하세요.

Amazon FSx Active Directory 검증 도구를 사용하여 여러 도메인 컨트롤러의 연결성 테스트 등 Active Directory 구성을 검증할 수 있습니다. 연결이 필요한 도메인 컨트롤러의 수를 제한하기 위해 온프레미

스 도메인 컨트롤러와 AWS Managed Microsoft AD사이에 신뢰 관계를 구축할 수도 있습니다. 자세한 정보는 리소스 포리스트 격리 모델 사용을 참조하세요.

> **Important**
>
> 파일 시스템이 생성된 후 Amazon FSx가 OU에 생성한 컴퓨터 객체를 옮기지 마세요. 이렇게 하면 파일 시스템 구성이 잘못될 수 있습니다.

FSx for Windows File Server 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인하는 모범 사례

Amazon FSx for Windows File Server 파일 시스템을 자체 관리형 Microsoft Active Directory에 조인할 때는 다음과 같은 모범 사례를 사용하는 것이 좋습니다.

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 파일 시스템을 도메인에 조인하려면 서비스 계정에 권한이 위임되었는지 확인해야 합니다. 도메인 관리자 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 Amazon FSx 파일 시스템을 도메인에 가입시키는 데 필요한 권한만 위임하는 방법을 보여줍니다.

Active Directory 사용자 및 컴퓨터 MMC 스냅인의 위임 제어 또는 고급 기능을 사용하여 이러한 권한을 할당합니다.

Active Directory에 가입되어 있고 스냅인이 설치된 컴퓨터에서 다음 절차 중 하나를 수행하십시오. Active Directory User and Computers MMC

위임 제어를 사용하여 서비스 계정 또는 그룹에 사용 권한을 할당하려면

1. Active Directory 도메인의 도메인 관리자로 시스템에 로그인합니다.
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 Amazon FSx 서비스 계정 또는 그룹의 이름을 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. 다음을 선택합니다.
10. 권한에서 다음을 선택합니다.

    - 암호 재설정
    - 읽기 및 쓰기 계정 제한
    - DNS 호스트 이름에 대한 검증된 쓰기
    - 서비스 보안 주체 이름에 대한 검증된 쓰기
11. 다음을 선택한 후 완료를 선택합니다.
12. Active Directory User and Computers MMC 스냅인을 닫습니다.

고급 기능을 사용하여 권한을 할당하려면

1. Active Directory 도메인의 도메인 관리자로 시스템에 로그인합니다.
2. Active Directory User and Computers MMC 스냅인을 엽니다.
3. 메뉴 표시줄에서 보기를 선택하고 고급 기능이 활성화되어 있는지 확인합니다(고급 기능이 활성화된 경우 고급 기능 옆에 체크 표시가 나타남).
4. 작업창에서 도메인 노드를 확장합니다.
5. 수정하려는 OU에 대한 컨텍스트 메뉴를 찾아 마우스 오른쪽 클릭으로 연 다음 속성을 선택합니다.
6. OU 속성 창에서 보안 탭을 선택합니다.
7. 보안 탭에서 고급을 선택합니다. 그런 다음 추가를 선택합니다.
8. 권한 항목 페이지에서 보안 주체 선택을 선택하고 Amazon FSx 서비스 계정 또는 그룹의 이름을 입력합니다. 적용 대상:에서 하위 컴퓨터 개체를 선택합니다. 다음이 선택되었는지 확인합니다.

    - 권한 수정
    - 컴퓨터 객체 생성
    - 컴퓨터 객체 삭제
9. 적용을 선택한 다음 확인을 선택합니다.

10. Active Directory User and Computers MMC 스냅인을 닫습니다.

> **Important**
>
> 파일 시스템이 생성된 후 Amazon FSx가 OU에서 생성한 컴퓨터 객체를 이동하지 않습니다. 이렇게 하면 파일 시스템이 잘못 구성될 수 있습니다. 새 서비스 계정으로 파일 시스템을 업데이트하는 경우 파일 시스템과 연결된 기존 컴퓨터 객체에 대한 전체 제어 권한이 새 서비스 계정에 있는지 확인합니다.

Active Directory 구성을 최신 상태로 유지

Amazon FSx 파일 시스템을 중단 없이 지속적으로 사용할 수 있도록 하려면 자체 관리형 Active Directory 설정을 변경할 때마다 파일 시스템의 Active Directory 구성을 업데이트해야 합니다.

예를 들어 Active Directory에서 시간 기반 암호 재설정 정책을 사용하는 경우 암호가 재설정되는 즉시 Amazon FSx로 서비스 계정 암호를 업데이트해야 합니다. 마찬가지로 Active Directory 도메인의 DNS 서버 IP 주소가 변경되는 경우 변경이 발생하는 즉시 Amazon FSx로 DNS 서버 IP 주소를 업데이트합니다. 자세한 설명은 자체 관리형 Active Directory 구성 업데이트 섹션을 참조하세요.

Amazon FSx 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트하면 업데이트가 적용되는 동안 파일 시스템의 상태가 사용 가능에서 업데이트 중으로 전환됩니다. 업데이트가 적용된 후 상태가 다시 사용 가능으로 전환되는지 확인합니다. 업데이트를 완료하는 데 몇 분 정도 걸릴 수 있습니다. 자세한 설명은 자체 관리형 Active Directory 업데이트 모니터링 섹션을 참조하세요.

업데이트된 자체 관리형 Active Directory 구성에 문제가 있는 경우 파일 시스템 상태가 잘못 구성됨으로 전환됩니다. 이 상태에는 콘솔, API 및 CLI의 파일 시스템 설명 옆에 오류 메시지와 권장 수정 조치가 표시됩니다. 권장 수정 조치를 취한 후 파일 시스템 상태가 최종적으로 사용 가능으로 변경되는지 확인합니다.

자체 관리형 Active Directory 구성 오류 문제를 해결하는 방법에 대한 자세한 내용은 파일 시스템이 잘못 구성된 상태 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 Active Directory 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 제어 단원을 참조하십시오.

Active Directory 구성 검증

Active Directory에 조인할 FSx for Windows File Server 파일 시스템을 생성하기 전에 Amazon FSx Active Directory 검증 도구를 사용하여 Active Directory 구성을 검증하는 것이 좋습니다. Active Directory 구성을 성공적으로 검증하려면 아웃바운드 인터넷 연결이 필요합니다.

Active Directory 구성 검증

1. FSx for Windows File Server 파일 시스템에 사용할 동일한 Amazon VPC 보안 그룹 및 동일한 서브넷에서 Amazon EC2 Windows 인스턴스를 시작합니다. EC2 인스턴스에 필요한 `AmazonEC2ReadOnlyAccess` IAM 권한이 있는지 확인하세요. IAM 정책 시뮬레이터를 사용하여 EC2 인스턴스 역할 권한을 검증할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM 정책 시뮬레이터로 IAM 정책 테스트를 참조하세요.
2. EC2 Windows 인스턴스를 Active Directory에 조인합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 Windows 인스턴스 수동 조인을 참조하세요.
3. EC2 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
4. EC2 인스턴스에서 Windows PowerShell 창 (관리자 권한으로 실행 사용) 을 엽니다.

   Windows용 필수 Active Directory PowerShell 모듈이 설치되어 있는지 테스트하려면 다음 테스트 명령을 사용하십시오.

   ```
   PS C:\> Import-Module ActiveDirectory
   ```

   테스트 명령이 오류를 반환하면 다음 명령을 사용하여 모듈을 설치합니다.

   ```
   PS C:\> Install-WindowsFeature RSAT-AD-PowerShell
   ```

5. 다음 명령을 사용하여 네트워크 검증 도구를 다운로드합니다.

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

6. 다음 명령을 사용하여 zip 파일을 확장합니다.

```
PS C:\> Expand-Archive -Path "AmazonFSxADValidation.zip"
```

7. AmazonFSxADValidation 모듈을 현재 세션에 추가합니다.

```
PS C:\> Import-Module .\AmazonFSxADValidation
```

8. 다음 명령에 필요한 변수를 넣어 설정합니다.

   - Active Directory 도메인 이름(*DOMAINNAME.COM*)
   - 다음 옵션 중 하나를 사용하여 서비스 계정 암호용 $Credential 객체를 준비합니다.
     - 대화형 방식으로 보안 인증 객체를 생성하려면 다음 명령을 사용합니다.

       ```
       $Credential = Get-Credential
       ```

     - AWS Secrets Manager 리소스를 사용하여 자격 증명 개체를 생성하려면 다음 명령을 사용합니다.

       ```
       $Secret = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
        $AdminSecret).SecretString
       $Credential = (New-Object PSCredential($Secret.UserName,(ConvertTo-SecureString
        $Secret.Password -AsPlainText -Force)))
       ```

   - DNS 서버 IP 주소(*IP_ADDRESS_1*, *IP_ADDRESS_2*)
   - Amazon FSx 파일 시스템을 생성하려는 서브넷의 서브넷 ID(예: *SUBNET_1*, *SUBNET_2*, 예시: subnet-04431191671ac0d19).

```
PS C:\>
$FSxADValidationArgs = @{
    # DNS root of ActiveDirectory domain
    DomainDNSRoot = 'DOMAINNAME.COM'

    # IP v4 addresses of DNS servers
```

```
    DnsIpAddresses = @('IP_ADDRESS_1', 'IP_ADDRESS_2')

    # Subnet IDs for Amazon FSx file server(s)
    SubnetIds = @('SUBNET_1', 'SUBNET_2')

    Credential = $Credential
}
```

9. (선택 사항) 유효성 검사 도구를 실행하기 전에 포함된 README.md 파일의 지침에 따라 조직 구성 단위 DomainControllersMaxCount, 위임된 관리자 그룹을 설정하고 서비스 계정 권한 검증을 활성화합니다.

> **Note**
>
> 운영 체제가 영어가 아닌 경우 Domain Admins 그룹 이름이 다릅니다. 예를 들어, 프랑스 OS 버전에서 그룹 이름은 Administrateurs du domaine입니다. 값을 지정하지 않으면 기본 Domain Admins 그룹 이름이 사용되고 파일 시스템 생성이 실패합니다.

10. 이 명령을 사용하여 유효성 검사 도구를 실행합니다.

```
PS C:\> $Result = Test-FSxADConfiguration @FSxADValidationArgs
```

11. 다음은 테스트에 성공한 결과의 예입니다.

```
Test 1 - Validate EC2 Subnets ...
...
Test 17 - Validate 'Delete Computer Objects' permission ...

Test computer object amznfsxtestd53f deleted!
...
SUCCESS - All tests passed! Please proceed to creating an Amazon FSx file system.
 For your convenience, SelfManagedActiveDirectoryConfiguration of result can be
 used directly in CreateFileSystemWindowsConfiguration for New-FSXFileSystem
PS C:\AmazonFSxADValidation> $Result.Failures.Count
0
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

다음은 테스트에 오류가 발생한 결과의 예입니다.

```
Test 1 - Validate EC2 Subnets ...
```

```
...
Test 7 - Validate that provided EC2 Subnets belong to a single AD Site ...

Name          DistinguishedName
     Site
----          -----------------
     ----
10.0.0.0/19   CN=10.0.0.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local   CN=SiteB,CN=Sites,CN=Configu...
10.0.128.0/19 CN=10.0.128.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local CN=Default-First-Site-Name,C...
10.0.64.0/19  CN=10.0.64.0/19,CN=Subnets,CN=Sites,CN=Configuration,DC=test-
ad,DC=local  CN=SiteB,CN=Sites,CN=Configu...



Best match for EC2 subnet subnet-092f4caca69e360e7 is AD site CN=Default-First-
Site-Name,CN=Sites,CN=Configuration,DC=te
st-ad,DC=local
Best match for EC2 subnet subnet-04431191671ac0d19 is AD site
 CN=SiteB,CN=Sites,CN=Configuration,DC=test-ad,DC=local
WARNING: EC2 subnets subnet-092f4caca69e360e7 subnet-04431191671ac0d19 matched to
 different AD sites! Make sure they
are in a single AD site.
...
9 of 16 tests skipped.
FAILURE - Tests failed. Please see error details below:

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}



Please address all errors and warnings above prior to re-running validation to
 confirm fix.
PS C:\AmazonFSxADValidation> $Result.Failures.Count
1
PS C:\AmazonFSxADValidation> $Result.Failures

Name                           Value
----                           -----
SubnetsInSeparateAdSites       {subnet-04431191671ac0d19, subnet-092f4caca69e360e7}
```

```
PS C:\AmazonFSxADValidation> $Result.Warnings.Count
0
```

유효성 검사 도구를 실행할 때 경고 또는 오류가 발생하는 경우, 유효성 검사 도구 패키지(TROUBLESHOOTING.md) 및 Amazon FSx 문제 해결 섹션에 포함된 문제 해결 안내서를 참조하세요.

Amazon FSx 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인

Windows File Server 파일 시스템에 대한 새 FSx를 생성할 때 자체 관리형 Microsoft Active Directory 도메인에 조인하도록 Microsoft Active Directory 통합을 구성할 수 있습니다. 이렇게 하려면 Microsoft Active Directory에 대한 다음 정보를 제공합니다.

- 온프레미스 Microsoft Active Directory 디렉터리의 정규화된 도메인 이름.

> **Note**
>
> Amazon FSx는 현재 단일 레이블 도메인(SLD) 도메인을 지원하지 않습니다.

- 도메인의 DNS 서버의 IP 주소.
- 온프레미스 Microsoft Active Directory 도메인의 서비스 계정에 대한 자격 증명. Amazon FSx는 이러한 보안 인증 정보를 사용하여 자체 관리형 Active Directory에 조인합니다.

선택적으로 다음을 지정할 수도 있습니다.

- Amazon FSx 파일 시스템을 조인하려는 도메인 내의 특정 조직 단위(OU).
- 멤버에게 Amazon FSx 파일 시스템에 대한 관리 권한이 부여된 도메인 그룹의 이름.

> **Note**
>
> 제공하는 도메인 그룹 이름은 Active Directory에서 고유해야 합니다. Windows File Server용 FSx는 다음과 같은 상황에서는 도메인 그룹을 만들지 않습니다.
>
> - 지정한 이름을 가진 그룹이 이미 있는 경우

- 이름을 지정하지 않고 Active Directory에 “도메인 관리자”라는 이름의 그룹이 이미 존재하는 경우

이 정보를 지정하면 Amazon FSx는 사용자가 제공한 서비스 계정을 사용하여 자체 관리형 Active Directory 도메인에 새 파일 시스템을 조인합니다.

Important

Amazon FSx는 파일 시스템을 조인하려는 Active Directory 도메인이 Microsoft DNS를 기본 DNS로 사용하는 경우에만 파일 시스템에 대한 DNS 레코드를 등록합니다. 서드 파티 DNS를 사용하는 경우 파일 시스템을 생성한 후 Amazon FSx 파일 시스템에 대한 DNS 항목을 수동으로 설정해야 합니다. 파일 시스템에 사용할 올바른 IP 주소를 선택하는 방법에 대한 자세한 내용은 DNS에 사용할 올바른 파일 시스템 IP 주소 획득 섹션을 참조하세요.

시작하기 전 준비 사항

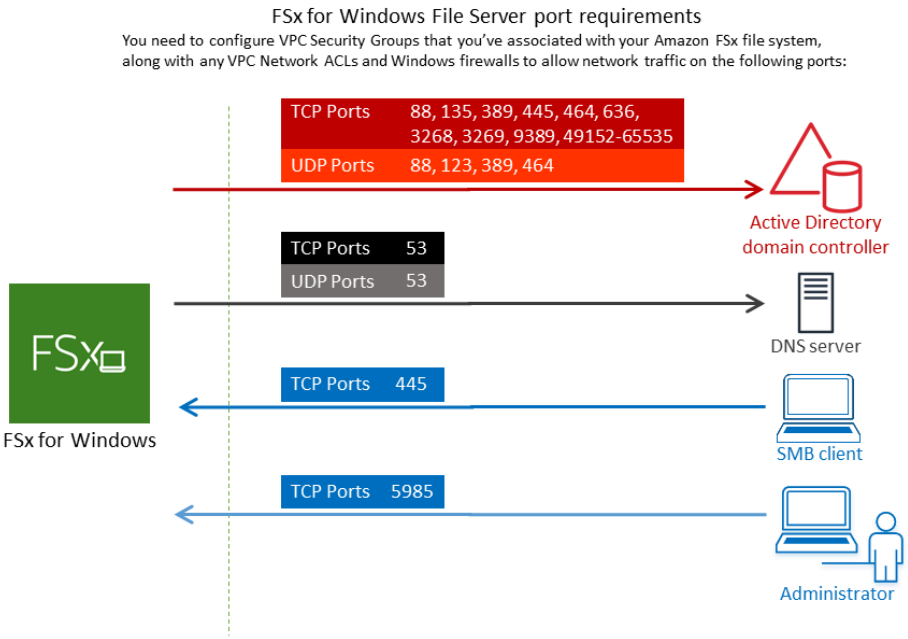
자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용에서 설명한 자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항을 완료했는지 확인합니다.

자체 관리형 Active Directory에 조인된 FSx for Windows File Server 파일 시스템 생성(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 대시보드에서 파일 시스템 생성을 선택하여 파일 시스템 생성 마법사를 시작합니다.
3. FSx for Windows File Server를 선택한 후 다음을 선택합니다. 파일 시스템 생성 페이지가 표시됩니다.
4. 파일 시스템의 이름을 제공합니다. 최대 256개의 유니코드 문자, 공백 및 숫자와 특수 문자 + - = . _ : /를 사용할 수 있습니다.
5. 스토리지 용량에는 파일 시스템의 스토리지 용량을 GiB 단위로 입력합니다. SSD 스토리지를 사용하는 경우 32~65,536 범위의 정수를 입력합니다. HDD 스토리지를 사용하는 경우 2,000~65,536 범위의 정수를 입력합니다. 파일 시스템을 생성한 후 언제든지 필요에 따라 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.
6. 처리량 용량을 기본 설정으로 유지합니다. 처리량 용량은 파일 시스템을 호스팅하는 파일 서버가 데이터를 제공할 수 있는 지속 속도입니다. 권장 처리량 용량 설정은 선택한 스토리지 용량을 기반으로 합니다. 권장 처리량 용량보다 많은 용량이 필요한 경우 처리량 용량 지정을 선택한 다음 값을 선택합니다. 자세한 설명은 FSx for Windows File Server 성능 섹션을 참조하세요.

파일 시스템을 생성하고 나서 언제든지 필요에 따라 처리량 용량을 수정할 수 있습니다. 자세한 설명은 처리량 용량 관리 섹션을 참조하세요.

7. 파일 시스템과 연결할 VPC를 선택합니다. 이 시작하기 연습에서는 AWS Directory Service 디렉터리 및 Amazon EC2 인스턴스와 동일한 VPC를 선택하십시오.
8. 가용 영역 및 서브넷에서 원하는 값을 선택합니다.
9. VPC 보안 그룹의 경우 기본 Amazon VPC의 기본 보안 그룹이 콘솔의 파일 시스템에 이미 추가되었습니다. FSx 파일 시스템을 만드는 서브넷의 보안 그룹과 VPC 네트워크 ACL이 다음 다이어그램에 표시된 방향으로 포트를 통한 트래픽을 허용하는지 확인합니다.



다음 테이블에는 각 포트의 역할이 나와 있습니다.

프로토콜	포트	역할
TCP/UDP	53	도메인 이름

프로토콜	포트	역할
		시스템 (DNS)
TCP/UDP	88	Kerbe 인증
TCP/UDP	464	암호 변경/ 설정
TCP/UDP	389	LDAP tweigh Direct Acces Protoc
UDP	123	NTP(N rk Time Protoc

프로토콜	포트	역할
TCP	135	분산 컴퓨팅 환경/엔드포인트 매퍼(DCE/EP MAP)
TCP	445	디렉터리 서비스 SMB 파일 공유

프로토콜	포트	역할
TCP	636	Lightweight Directory Access Protocol over TLS/SSL(LDAPS
TCP	3268	Microsoft 글로벌 카탈로그
TCP	3269	SSL을 통한 Microsoft 글로벌 카탈로그

프로토콜	포트	역할
TCP	5985	WinRM 2.0(Microsoft Windows Remote Management)
TCP	9389	마이크로소프트 액티브 디렉터리 DS 웹 서비스, PowerI

프로토콜	포트	역할
TCP	49152 - 65535	RPC용 임시 포트

Important

단일 AZ 2 및 모든 다중 AZ 파일 시스템 배포에는 TCP 포트 9389에서 아웃바운드 트래픽을 허용해야 합니다.

Note

VPC 네트워크 ACL을 사용하는 경우 FSx 파일 시스템의 동적 포트(49152~65535)를 통한 아웃바운드 트래픽도 허용해야 합니다.

- 아웃바운드 규칙은 자체 관리형 Microsoft Active Directory 도메인의 DNS 서버 및 도메인 컨트롤러와 연결된 IP 주소로 들어오는 모든 트래픽을 허용합니다. 자세한 내용은 Active Directory 통신을 위한 방화벽 구성에 대한 Microsoft 설명서를 참조하세요.
- 이러한 트래픽 규칙이 각 Active Directory 도메인 컨트롤러, DNS 서버, FSx 클라이언트, FSx 관리자에 적용되는 방화벽에도 반영되는지 확인합니다.

Note

Microsoft Active Directory 사이트가 정의되어 있는 경우에는 Amazon FSx 파일 시스템과 연결된 VPC의 서브넷이 Microsoft Active Directory 사이트에 정의되어 있도록 하고 VPC의 서브넷과 다른 사이트의 서브넷 간에 충돌이 존재하지 않도록 해야 합니다. Active Directory Sites and Services MMC 스냅인을 사용하여 이러한 설정을 보고 변경할 수 있습니다.

> **Important**
>
> Amazon VPC 보안 그룹에서는 네트워크 트래픽이 시작되는 방향으로만 포트를 열어야 하지만, 대부분의 Windows 방화벽과 VPC 네트워크 ACL에서는 포트가 양방향으로 열려 있어야 합니다.

10. Windows 인증에서 자체 관리형 Microsoft Active Directory를 선택합니다.
11. 자체 관리형 Microsoft Active Directory 디렉터리의 정규화된 도메인 이름에 값을 입력합니다.

> **Note**
>
> 도메인 이름은 단일 레이블 도메인(SLD) 형식일 수 없습니다. Amazon FSx는 현재 SLD 도메인을 지원하지 않습니다.

> **Important**
>
> 단일 AZ 2 및 모든 다중 AZ 파일 시스템의 경우 Active Directory 도메인 이름은 47자를 초과할 수 없습니다.

12. 자체 관리형 Microsoft Active Directory 디렉터리의 조직 단위에 값을 입력합니다.

> **Note**
>
> 제공한 서비스 계정에 여기서 지정하는 OU 또는 기본 OU(지정하지 않은 경우)에 위임된 권한이 있는지 확인합니다.

13. 자체 관리형 Microsoft Active Directory 디렉터리의 DNS 서버 IP 주소 값을 하나 이상 두 개 이하로 입력합니다.
14. 자체 관리형 Active Directory 도메인의 계정에 대한 서비스 계정 사용자 이름의 문자열 값(예: `ServiceAcct`)을 입력합니다. Amazon FSx는 이 사용자 이름을 사용하여 Microsoft Active Directory 도메인에 조인합니다.

> **Important**
>
> 서비스 계정 사용자 이름을 입력할 때 도메인 접두사(`corp.com\ServiceAcct`) 또는 도메인 접미사(`ServiceAcct@corp.com`)를 포함하지 않습니다.
> 서비스 계정 사용자 이름(`CN=ServiceAcct,OU=example,DC=corp,DC=com`)을 입력할 때 고유 이름(DN)을 사용하지 않습니다.

15. 자체 관리형 Active Directory 도메인의 계정에 대한 서비스 계정 암호의 값을 입력합니다. Amazon FSx는 이 암호를 사용하여 Microsoft Active Directory 도메인에 조인합니다.
16. 암호 확인에서 암호를 다시 입력하여 확인합니다.
17. 위임된 파일 시스템 관리자 그룹에서 `Domain Admins` 그룹 또는 사용자 지정 위임 파일 시스템 관리자 그룹(생성한 경우)을 지정합니다. 지정하는 그룹에는 파일 시스템에서 관리 작업을 수행할 수 있는 위임된 권한이 있어야 합니다. 값을 입력하지 않으면 Amazon FSx가 기본 제공 `Domain Admins` 그룹을 사용합니다. Amazon FSx는 내장 컨테이너에 위치 (사용자가 지정하는 그룹 또는 사용자 지정 그룹) 를 지원하지 않는다는 점에 유의하십시오. `Delegated file system administrators group Domain Admins`

> **Important**
>
> 위임 파일 시스템 관리자 그룹을 제공하지 않는 경우 Amazon FSx는 기본적으로 Active Directory 도메인의 기본 제공 `Domain Admins` 그룹을 사용하려고 시도합니다. 이 기본 제공 그룹의 이름이 변경되었거나 도메인 관리에 다른 그룹을 사용하는 경우 여기에 해당 그룹 이름을 입력해야 합니다.

> **Important**
>
> 그룹 이름 파라미터를 제공할 때 도메인 접두사 (corp.com\ FSxAdmins) 또는 도메인 접미사 (F SxAdmins @corp .com) 를 포함하지 마십시오.
> 그룹에 DN(고유 이름)을 사용하지 않습니다. 고유 이름의 예로는 CN=F, OU=예제, DC=Corp, SxAdmins DC=com이 있습니다.

자체 관리형 Active Directory에 조인된 FSx for Windows File Server 파일 시스템 생성(AWS CLI)

다음 예제에서는 `us-east-2` 가용 영역에 `SelfManagedActiveDirectoryConfiguration`이 있는 FSx for Windows File Server 파일 시스템을 생성합니다.

```
aws fsx --region us-east-2 \
create-file-system \
--file-system-type WINDOWS \
--storage-capacity 300 \
--security-group-ids security-group-id \
--subnet-ids subnet-id\
--windows-configuration
 SelfManagedActiveDirectoryConfiguration='{DomainName="corp.example.com", \
OrganizationalUnitDistinguishedName="OU=FileSystems,DC=corp,DC=example,DC=com",FileSystemAdmini
 \
UserName="FSxService",Password="password", \
   DnsIps=["10.0.1.18"]}',ThroughputCapacity=8
```

> **Important**
>
> 파일 시스템이 생성된 후 Amazon FSx가 OU에서 생성한 컴퓨터 객체를 이동하지 않습니다. 이렇게 하면 파일 시스템이 잘못 구성될 수 있습니다.

DNS에 사용할 올바른 파일 시스템 IP 주소 획득

Amazon FSx는 Microsoft DNS를 기본 DNS 서비스로 사용하는 경우에만 파일 시스템의 DNS 레코드를 등록합니다. 타사 DNS를 사용하는 경우 Amazon FSx 파일 시스템의 DNS 항목을 수동으로 설정해야 합니다. 이 섹션에서는 DNS에 파일 시스템을 수동으로 추가해야 하는 경우에 올바른 파일 시스템 IP 주소 획득 방법을 설명합니다. 파일 시스템이 생성되면 해당 IP 주소는 파일 시스템이 삭제될 때까지 변경되지 않습니다.

DNS A 항목에 사용할 파일 시스템 IP 주소 획득 방법

1. https://console.aws.amazon.com/fsx/ 에서 IP 주소를 획득할 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 표시합니다.
2. 네트워크 및 보안 탭에서 다음 중 하나를 수행하세요.

   - 단일 AZ 1 파일 시스템의 경우:

  - 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2 콘솔에서 네트워크 인터페이스 페이지를 엽니다.
  - 사용할 단일 AZ 1 파일 시스템의 IP 주소는 기본 프라이빗 IPv4 IP 열에 표시됩니다.
- 단일 AZ 2 또는 다중 AZ 파일 시스템의 경우:
  - 기본 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2 콘솔에서 네트워크 인터페이스 페이지를 엽니다.
  - 사용할 기본 서브넷의 IP 주소는 보조 프라이빗 IPv4 IP 열에 표시됩니다.
  - Amazon FSx 대기 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2 콘솔에서 네트워크 인터페이스 페이지를 엽니다.
  - 사용할 대기 서브넷의 IP 주소는 보조 프라이빗 IPv4 IP 열에 표시됩니다.

> **Note**
>
> 단일 AZ 2 또는 다중 AZ 파일 시스템에 대한 Windows 원격 PowerShell 엔드포인트의 DNS 항목을 설정해야 하는 경우 기본 서브넷의 Elastic Network 인터페이스용 기본 프라이빗 IPv4 주소를 사용해야 합니다. 자세한 정보는 아마존 FSx CLI를 사용하는 방법 PowerShell을 참조하세요.

자체 관리형 Active Directory 구성 업데이트

Amazon FSx API를 사용하거나 파일 시스템의 자체 관리형 Active Directory 구성의 서비스 계정 사용자 이름 및 암호와 DNS 서버 IP 주소를 업데이트할 수 있습니다. AWS Management Console AWS CLI AWS Management Console, CLI 및 API를 사용하여 언제든지 자체 관리형 Active Directory 구성 업데이트의 진행 상황을 추적할 수 있습니다. 자세한 정보는 자체 관리형 Active Directory 업데이트 모니터링을 참조하세요.

자체 관리형 Active Directory 구성 업데이트(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 자체 관리형 Active Directory 구성을 업데이트하려는 Windows 파일 시스템을 선택합니다.
3. 네트워크 및 보안 탭에서 업데이트하려는 Active Directory 속성에 따라 DNS 서버 IP 주소 또는 서비스 계정 사용자 이름의 업데이트를 선택합니다.
4. 나타나는 대화 상자에 새 DNS 서버 IP 주소 또는 새 서비스 계정 보안 인증 정보를 입력합니다.

5. 업데이트를 선택하여 Active Directory 구성 업데이트를 시작합니다.

   AWS Management Console 또는 를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. AWS CLI

자체 관리형 Active Directory 구성 업데이트(CLI)

- Windows File Server용 FSx 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트하려면 update-file-system 명령을 사용합니다. AWS CLI 다음 파라미터를 설정합니다.
  - `--file-system-id` 업데이트하려는 파일 시스템 ID.
  - `UserName` 자체 관리형 Active Directory 서비스 계정의 새 사용자 이름.
  - `Password` 자체 관리형 Active Directory 서비스 계정의 새 암호.
  - `DnsIps` 자체 관리형 Active Directory DNS 서버의 IP 주소

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
  --windows-configuration
 'SelfManagedActiveDirectoryConfiguration={UserName=username,Password=password,\
    DnsIps=[192.0.2.0,192.0.2.24]}'
```

   업데이트 작업이 성공하면 서비스가 HTTP 200 응답을 다시 전송합니다. 응답의 `AdminstrativeActions` 개체는 요청과 해당 상태를 설명합니다.

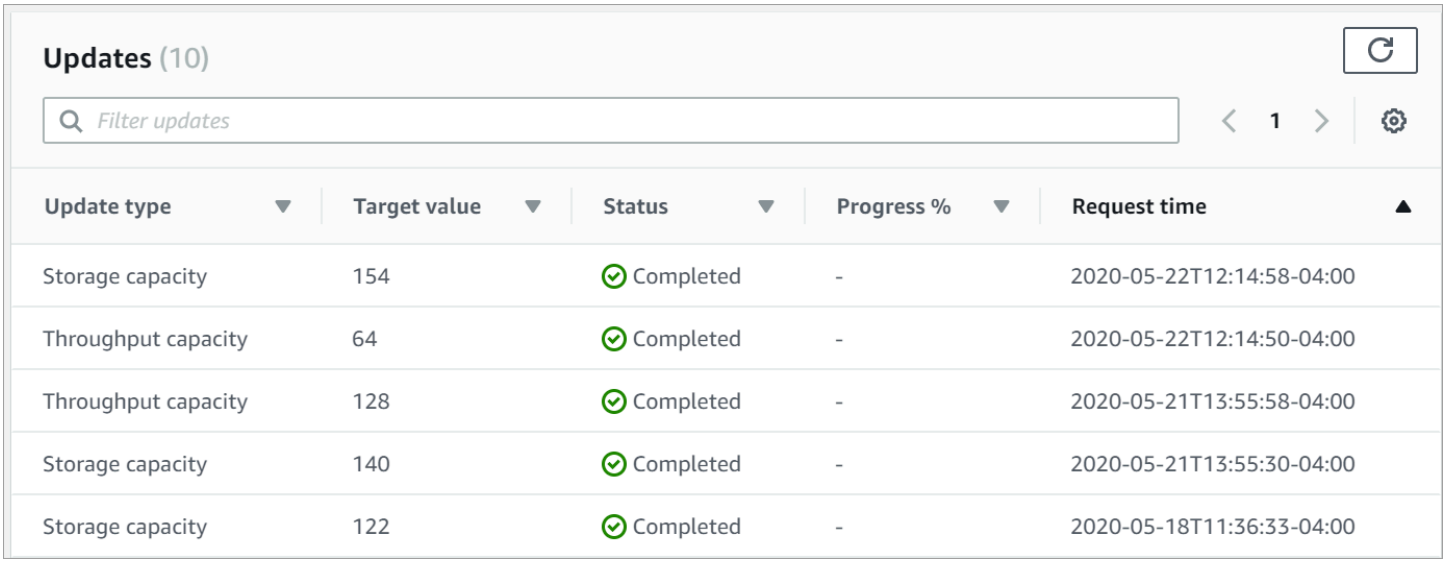
자체 관리형 Active Directory 업데이트 모니터링

파일 시스템의 자체 관리형 Active Directory 구성을 업데이트하면 업데이트가 적용되는 동안 파일 시스템의 상태가 사용 가능에서 업데이트 중으로 전환됩니다. 업데이트가 완료되면 상태가 다시 사용 가능으로 전환됩니다. 업데이트를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

다음 섹션에 설명된 API 또는 를 사용하여 자체 관리형 Active Directory 구성 업데이트의 진행 상황을 모니터링할 수 있습니다. AWS Management Console AWS CLI

콘솔에서 업데이트 모니터링

파일 시스템 세부 정보 창의 업데이트 탭에서 각 업데이트 유형에 대한 최신 업데이트 10개를 볼 수 있습니다.



자체 관리형 Active Directory 업데이트의 경우, 다음 정보를 볼 수 있습니다.

업데이트 유형

지원되는 유형은 다음과 같습니다.

- DNS 서버 IP 주소
- 서비스 계정 보안 인증 정보

대상 값

파일 시스템에서 업데이트할 원하는 값. 서비스 계정 보안 인증 정보 업데이트의 경우, 사용자 이름만 표시되며 서비스 계정 암호는 이 필드에 절대 포함되지 않습니다.

상태

현재 업데이트 상태. 자체 관리형 Active Directory 업데이트에서 가능한 값은 다음과 같습니다.

- 보류 중 – Amazon FSx가 업데이트 요청을 받았지만 처리를 시작하지 않았습니다.
- 진행 중 – Amazon FSx에서 업데이트 요청을 처리하고 있습니다.
- 완료 - 파일 시스템 업데이트가 성공적으로 완료되었습니다.
- 실패 - 파일 시스템 업데이트에 실패했습니다. 실패의 세부 정보를 보려면 물음표(?)를 선택하세요.

진행 %

파일 시스템 업데이트 진행률을 완료율로 표시합니다.

요청 시간

Amazon FSx가 업데이트 작업 요청을 받은 시간입니다.

및 API를 사용하여 업데이트를 모니터링합니다 AWS CLI .

describe-file-systems AWS CLI 명령과 시스템 API 작업을 사용하여 진행 중인 파일 시스템 업데이트 요청을 보고 모니터링할 수 있습니다. DescribeFile `AdministrativeActions` 배열에 각 관리 작업 유형에 대한 가장 최근의 업데이트 작업 10개가 나열됩니다.

다음 예는 describe-file-systems CLI 명령의 응답에서 발췌한 자체 관리형 Active Directory 파일 시스템 업데이트 두 개를 보여줍니다.

```
{
    "OwnerId": "111122223333",
    .
    .
    .
    "StorageCapacity": 1000,
    "AdministrativeActions": [
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1581694766.757,
            "Status": "PENDING",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                        "UserName": "serviceUser",
                    }
                }
            }
        },
        {
            "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
            "RequestTime": 1619032957.759,
            "Status": "FAILED",
            "TargetFileSystemValues": {
                "WindowsConfiguration": {
                    "SelfManagedActiveDirectoryConfiguration": {
                    "DnsIps": [
                            "10.0.138.161"
                        ]
                    }
                }
            },
            "FailureDetails": {
```

```
                    "Message": "Failure details message."
                }
            }
        ],
    .
    .
    .
```

Microsoft Windows 파일 공유 사용

Microsoft Windows 파일 공유는 파일 시스템의 특정 폴더입니다. 여기에는 서버 메시지 블록(SMB) 프로토콜을 사용하여 컴퓨팅 인스턴스가 액세스할 수 있도록 하는 해당 폴더의 하위 폴더가 포함됩니다. 파일 시스템에는 `share`라는 Windows 파일 공유가 기본으로 제공됩니다. 공유 폴더라는 Windows 그래픽 사용자 인터페이스(GUI) 도구를 사용하여 원하는 만큼 다른 Windows 파일 공유를 만들고 관리할 수 있습니다.

파일 공유 액세스

파일 공유에 액세스하려면 Windows Map Network Drive 기능을 사용하여 컴퓨팅 인스턴스의 드라이브 문자를 Amazon FSx 파일 공유에 매핑합니다. 파일 공유를 컴퓨팅 인스턴스의 드라이브에 매핑하는 프로세스는 Linux에서는 파일 공유를 마운트한다고 합니다. 매핑 프로세스는 컴퓨팅 인스턴스의 유형과 운영 체제에 따라 다릅니다. 파일 공유가 매핑되면 애플리케이션과 사용자가 로컬 파일 및 폴더인 것처럼 파일 공유의 파일 및 폴더에 액세스할 수 있습니다.

다음은 지원되는 여러 컴퓨팅 인스턴스에 파일 공유를 매핑하는 절차입니다.

주제

- Amazon EC2 Windows 인스턴스에서 파일 공유 매핑
- Amazon EC2 Mac 인스턴스에 파일 공유 마운트
- Amazon EC2 Linux 인스턴스에 파일 공유 마운트
- Active Directory에 조인되지 않은 Amazon Linux EC2 인스턴스에 파일 공유 자동 마운트

Amazon EC2 Windows 인스턴스에서 파일 공유 매핑

Windows 파일 탐색기 또는 명령 프롬프트를 사용하여 EC2 Windows 인스턴스의 파일 공유를 매핑할 수 있습니다.

Amazon EC2 Windows 인스턴스(콘솔)에서 파일 공유 매핑

1. EC2 인스턴스를 시작하고 이를 Amazon FSx 파일 시스템이 조인된 Microsoft Active Directory에 연결합니다. 이를 수행하려면 AWS Directory Service 관리 가이드에서 다음 절차 중 하나를 선택합니다.

   - Windows EC2 인스턴스를 원활하게 조인
   - Windows 인스턴스를 수동으로 조인

2. EC2 Windows 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 연결되면 파일 탐색기를 엽니다.
4. 탐색 창에서 네트워크에서 컨텍스트(오른쪽 클릭) 메뉴를 열고 맵 네트워크 드라이브를 선택합니다.
5. 드라이브인 경우, 드라이브 문자를 선택합니다.
6. 폴더에는 파일 시스템의 DNS 이름 또는 파일 시스템과 관련된 DNS 별칭과 공유 이름을 입력합니다.

> **Important**
>
> DNS 이름 대신 IP 주소를 사용하면 다중 AZ 파일 시스템의 장애 조치 프로세스 중에 사용할 수 없게 될 수 있습니다. 또한 다중 AZ 및 단일 AZ 파일 시스템의 Kerberos 기반 인증에는 DNS 이름 또는 관련 DNS 별칭이 필요합니다.

Amazon FSx 콘솔에서 Windows File Server, 네트워크 및 보안을 선택하여 파일 시스템의 DNS 이름과 모든 관련 DNS 별칭을 찾을 수 있습니다. 또는 CreateFile시스템 또는 DescribeFile시스템 API 작업의 응답에서 해당 정보를 찾을 수도 있습니다. DNS 별칭 사용에 대한 자세한 내용은 DNS 별칭 관리 섹션을 참조하세요.

- AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
fs-0123456789abcdef0.ad-domain.com
```

- 자체 관리형 Active Directory에 연결된 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
amznfsxaa11bb22.ad-domain.com
```

예를 들어, 단일 AZ 파일 시스템의 DNS 이름을 사용하려면 폴더에 다음을 입력합니다.

```
\\fs-0123456789abcdef0.ad-domain.com\share
```

다중 AZ 파일 시스템의 DNS 이름을 사용하려면 폴더에 다음을 입력합니다.

```
\\famznfsxaa11bb22.ad-domain.com\share
```

파일 시스템과 연결된 DNS 별칭을 사용하려면 폴더에 다음을 입력합니다.

```
\\fqdn-dns-alias\share
```

7. 로그인 시 파일 공유를 다시 연결할지 여부를 나타내는 로그인 시 재연결 옵션을 선택한 다음 마침을 선택합니다.

Amazon EC2 Windows 인스턴스(명령 프롬프트)에서 파일 공유 매핑

1. EC2 인스턴스를 시작하고 이를 Amazon FSx 파일 시스템이 조인된 Microsoft Active Directory에 연결합니다. 이를 수행하려면 AWS Directory Service 관리 가이드에서 다음 절차 중 하나를 선택합니다.
   - Windows EC2 인스턴스를 원활하게 조인
   - Windows 인스턴스를 수동으로 조인
2. AWS Managed Microsoft AD 디렉터리의 사용자로 EC2 Windows 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 연결되면 명령 프롬프트 창을 엽니다.
4. 선택한 드라이브 문자, 파일 시스템의 DNS 이름, 공유 이름을 사용하여 파일 공유를 마운트합니다. Amazon FSx 콘솔에서 Windows File Server, 네트워크 및 보안을 선택하여 DNS 이름을 찾을 수 있습니다. `CreateFileSystem` 또는 `DescribeFileSystems` API 작업의 응답에서도 찾을 수 있습니다.
   - AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

     ```
     fs-0123456789abcdef0.ad-domain.com
     ```

   - 자체 관리형 Active Directory에 연결된 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

     ```
     amznfsxaa11bb22.ad-domain.com
     ```

   다음은 파일 공유 마운트 명령의 예시입니다.

```
$ net use H: \\amzfsxaa11bb22.ad-domain.com\share /persistent:yes
```

`net use`명령 대신 지원되는 PowerShell 명령을 사용하여 파일 공유를 마운트할 수도 있습니다.

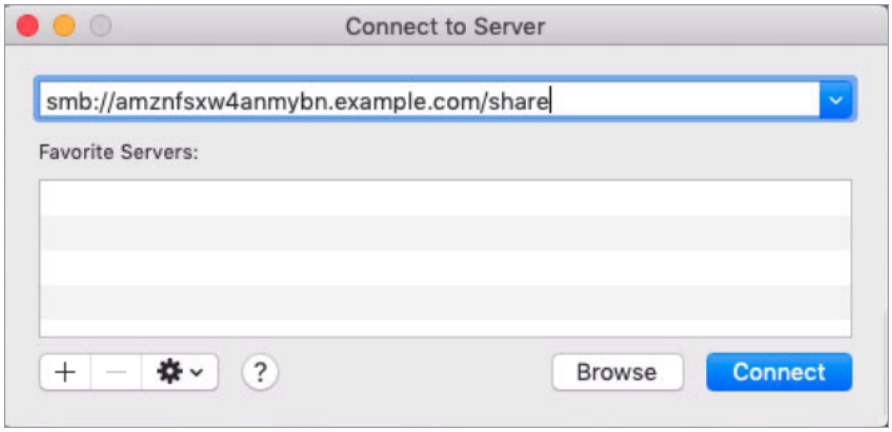
Amazon EC2 Mac 인스턴스에 파일 공유 마운트

Active Directory에 조인되거나 조인되지 않은 Amazon EC2 Mac 인스턴스에 파일 공유를 마운트할 수 있습니다. 인스턴스가 Active Directory에 조인되어 있지 않은 경우, Active Directory 도메인의 DNS 이름 서버를 포함하도록 인스턴스가 있는 Amazon Virtual Private Cloud(VPC) 에 설정된 DHCP 옵션을 업데이트해야 합니다. 그런 다음 인스턴스를 다시 시작합니다.

Amazon EC2 Mac 인스턴스에 파일 공유 마운트(GUI)

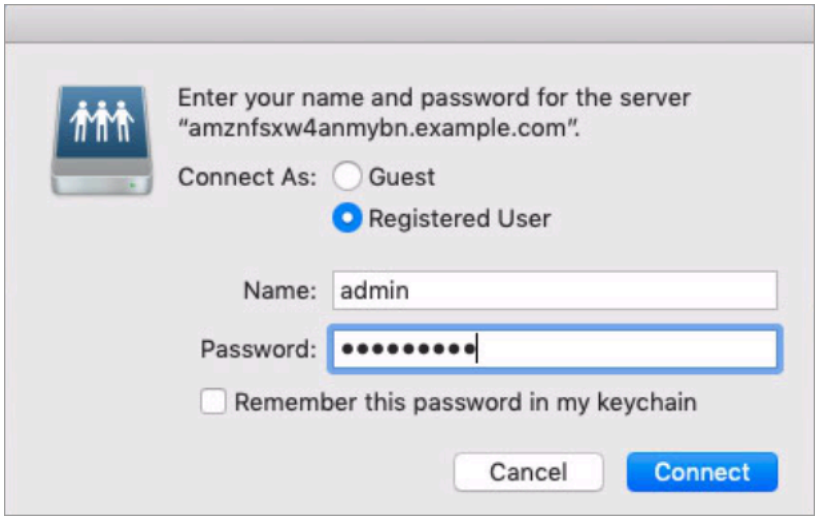
1. EC2 Mac 인스턴스를 시작합니다. 이렇게 하려면 Amazon EC2 사용 설명서에서 다음 절차 중 하나를 선택하십시오.
   - 콘솔을 사용하여 Mac 인스턴스 시작
   - 를 사용하여 Mac 인스턴스를 시작합니다. AWS CLI
2. 가상 네트워크 컴퓨팅(VNC)을 사용하여 EC2 Mac 인스턴스에 연결할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 VNC를 사용한 인스턴스 연결을 참조하십시오.
3. EC2 Mac 인스턴스에서 다음과 같이 Amazon FSx 파일 공유에 연결합니다.
   a. Finder를 열고, Go를 선택한 다음 서버에 연결을 선택합니다.
   b. 서버에 연결 대화 상자에 파일 시스템의 DNS 이름 또는 파일 시스템과 관련된 DNS 별칭과 공유 이름을 입력합니다. 그런 다음 연결을 선택합니다.

      Amazon FSx 콘솔에서 Windows File Server, 네트워크 및 보안을 선택하여 파일 시스템의 DNS 이름과 모든 관련 DNS 별칭을 찾을 수 있습니다. 또는 CreateFile시스템 또는 DescribeFile시스템 API 작업의 응답에서 해당 정보를 찾을 수도 있습니다. DNS 별칭 사용에 대한 자세한 내용은 DNS 별칭 관리 섹션을 참조하세요.



c. 다음 화면에서 연결을 선택하여 계속합니다.

d. 다음 예제와 같이 Amazon FSx 서비스 계정에 대한 Microsoft Active Directory(AD) 보안 인증 정보를 입력합니다. 그런 다음 연결을 선택합니다.



e. 연결에 성공하면 Finder 창의 위치에서 Amazon FSx 공유를 볼 수 있습니다.

Amazon EC2 Mac 인스턴스에 파일 공유 마운트(명령줄)

1. EC2 Mac 인스턴스를 시작합니다. 이렇게 하려면 Amazon EC2 사용 설명서에서 다음 절차 중 하나를 선택하십시오.
   - 콘솔을 사용하여 Mac 인스턴스 시작
   - 를 사용하여 Mac 인스턴스를 시작합니다. AWS CLI
2. 가상 네트워크 컴퓨팅(VNC)을 사용하여 EC2 Mac 인스턴스에 연결할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 VNC를 사용한 인스턴스 연결을 참조하십시오.
3. 다음 명령을 사용하여 파일 공유를 마운트합니다.

```
mount_smbfs //file_system_dns_name/file_share mount_point
```

Amazon FSx 콘솔에서 Windows 파일 서버, 네트워크 및 보안을 선택하여 DNS 이름을 찾을 수 있습니다. `CreateFileSystem` 또는 `DescribeFileSystems` API 작업의 응답에서도 찾을 수 있습니다.

- AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

  ```
  fs-0123456789abcdef0.ad-domain.com
  ```

- 자체 관리형 Active Directory에 연결된 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

  ```
  amznfsxaa11bb22.ad-domain.com
  ```

이 절차에서 사용되는 마운트 명령은 지정된 시점에서 다음을 수행합니다.

- *//file_system_dns_name/file_share* - 마운트할 파일 시스템의 DNS 이름과 공유를 지정합니다.
- *mount_point* - 파일 시스템을 마운트하려는 EC2 인스턴스의 디렉터리입니다.

Amazon EC2 Linux 인스턴스에 파일 공유 마운트

Active Directory에 조인되거나 조인되지 않은 Amazon EC2 Linux 인스턴스에 FSx for Windows File Server 파일 공유를 마운트할 수 있습니다.

> **Note**
>
> - 다음 명령은 SMB 프로토콜, 캐싱, 읽기 및 쓰기 버퍼 크기와 같은 파라미터를 지정하는 예입니다. Linux `cifs` 명령의 파라미터 선택과 사용된 Linux 커널 버전은 클라이언트와 Amazon FSx 파일 시스템 간의 네트워크 작업 처리량과 지연 시간에 영향을 미칠 수 있습니다. 자세한 내용은 사용 중인 리눅스 환경의 `cifs` 설명서를 참조하세요.

- Linux 클라이언트는 자동 DNS 기반 장애 조치를 지원하지 않습니다. 자세한 정보는 Linux 클라이언트에서의 장애 조치 경험을 참조하세요.

Active Directory에 연결된 Amazon EC2 Linux 인스턴스에 파일 공유 마운트

1. 실행 중인 EC2 Linux 인스턴스를 Microsoft Active Directory에 아직 조인하지 않은 경우 AWS Directory Service 관리 안내서의 Linux 인스턴스 수동 조인을 참조하세요.
2. EC2 Linux 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하십시오.
3. 다음 명령을 실행하여 `cifs-utils` 패키지를 설치합니다. 이 패키지는 Linux에서 Amazon FSx와 같은 네트워크 파일 시스템을 마운트하는 데 사용됩니다.

```
$ sudo yum install cifs-utils
```

4. 마운트 포인트 디렉터리 **/mnt/fsx**를 생성합니다. 여기에 Amazon FSx 파일 시스템을 마운트할 수 있습니다.

```
$ sudo mkdir -p /mnt/fsx
```

5. 다음 명령을 사용하여 kerberos로 인증합니다.

```
$ kinit
```

6. 다음 명령을 사용하여 파일 공유를 마운트합니다.

```
$ sudo mount -t cifs //file_system_dns_name/file_share mount_point --verbose -o
 vers=SMB_version,sec=krb5,cruid=ad_user,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=no
file-server-Ip
```

Amazon FSx 콘솔에서 Windows 파일 서버, 네트워크 및 보안을 선택하여 DNS 이름을 찾을 수 있습니다. `CreateFileSystem` 또는 `DescribeFileSystems` API 작업의 응답에서도 찾을 수 있습니다.

- AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
fs-0123456789abcdef0.ad-domain.com
```

- 자체 관리형 Active Directory에 연결된 단일 AZ 파일 시스템 및 다중 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
amznfsxaa11bb22.ad-domain.com
```

*CIFSMaxBufSize*의 값을 커널에서 허용하는 최대 값으로 바꿉니다. 최대 값을 알기 위해 다음 명령을 실행합니다.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

출력이 최대 버퍼 크기가 130048임을 보여줍니다.

7. Common Internet File System(CIFS) 유형의 파일 시스템만 반환하는 다음 명령을 실행하여 파일 시스템이 마운트되었는지 확인합니다.

```
$ mount -l -t cifs
//fs-0123456789abcdef0/share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=krb5,cache=cache_mode,username=user1@CORP.NETWORK.COM,ui
```

이 절차에서 사용되는 마운트 명령은 지정된 시점에서 다음을 수행합니다.

- *//file_system_dns_name/file_share* - 마운트할 파일 시스템의 DNS 이름과 공유를 지정합니다.
- *mount_point* - 파일 시스템을 마운트하려는 EC2 인스턴스의 디렉터리입니다.
- `-t cifs vers=`*SMB_version* - 파일 시스템 유형을 CIFS 및 SMB 프로토콜 버전으로 지정합니다. Amazon FSx for Windows File Server는 SMB 버전 2.0~3.1.1을 지원합니다.
- `sec=krb5` - 인증에 Kerberos 버전 5를 사용하도록 지정합니다.
- `cache=`*cache_mode* - 캐시 모드를 설정합니다. CIFS 캐시 옵션은 성능에 영향을 미칠 수 있으므로 커널 및 워크로드에 가장 적합한 설정을 테스트하고 Linux 설명서를 검토해야 합니다. `loose` 옵션은 프로토콜 의미 체계가 느슨하여 데이터 불일치가 발생할 수 있으므로 `strict` 또는 none 옵션을 권장합니다.
- `cruid=`*ad_user* - 보안 인증 정보 캐시 소유자의 uid를 AD 디렉터리 관리자에게 설정합니다.
- */mnt/fsx* - EC2 인스턴스에서 Amazon FSx 파일 공유의 마운트 지점을 지정합니다.

- `rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize` - 읽기 및 쓰기 버퍼 크기를 CIFS 프로토콜에서 허용하는 최대값으로 지정합니다. *CIFSMaxBufSize*의 값을 커널에서 허용하는 최대 값으로 바꿉니다. 다음 명령을 실행하여 CIFSMaxBufSize의 값을 결정합니다.

  ```
  $ modinfo cifs | grep CIFSMaxBufSize
  parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
   16384 Range: 8192 to 130048 (uint)
  ```

  출력이 최대 버퍼 크기가 130048임을 보여줍니다.

- `ip=preferred-file-server-Ip` - 대상 IP 주소를 파일 시스템의 기본 파일 서버의 대상 IP 주소로 설정합니다.

  다음과 같이 파일 시스템의 기본 파일 서버 IP 주소를 획득할 수 있습니다.

  - Amazon FSx 콘솔을 사용하여 파일 시스템 세부 정보 페이지의 네트워크 및 보안 탭.
  - `describe-file-systems`CLI 명령 또는 이에 상응하는 DescribeFile시스템 API 명령에 대한 응답으로

Active Directory에 연결된 Amazon EC2 Linux 인스턴스에 파일 공유 마운트

다음 절차는 Active Directory(AD)에 조인되지 않은 Amazon EC2 Linux 인스턴스에 Amazon FSx 파일 공유를 마운트합니다. AD에 조인되지 않은 EC2 Linux 인스턴스의 경우, 프라이빗 IP 주소를 사용하여 FSx for Windows File Server 파일 공유만 마운트할 수 있습니다. Amazon FSx 콘솔을 사용하여 네트워크 및 보안 탭에 있는 기본 파일 서버 IP 주소에서 파일 시스템의 프라이빗 IP 주소를 가져올 수 있습니다.

예제에서는 NTLM 인증을 사용합니다. FSx for Windows File Server 파일 시스템이 조인된 Microsoft Active Directory 도메인의 구성원인 사용자로 파일 시스템을 마운트합니다. 사용자 계정의 보안 인증 정보는 EC2 인스턴스에서 생성한 `creds.txt` 텍스트 파일로 제공됩니다. 이 파일에는 사용자의 사용자 이름, 암호 및 도메인이 들어 있습니다.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Amazon Linux EC2 인스턴스의 시작 및 구성

1. Amazon EC2 콘솔을 사용하여 Amazon Linux EC2 인스턴스를 시작합니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하십시오.
2. Amazon Linux EC2 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하십시오.
3. 다음 명령을 실행하여 `cifs-utils` 패키지를 설치합니다. 이 패키지는 Linux에서 Amazon FSx와 같은 네트워크 파일 시스템을 마운트하는 데 사용됩니다.

```
$ sudo yum install cifs-utils
```

4. Amazon FSx 파일 시스템을 마운트할 **`/mnt/fsxx`** 마운트 포인트를 생성합니다.

```
$ sudo mkdir -p /mnt/fsx
```

5. 이전에 표시된 형식을 사용하여 `/home/ec2-user` 디렉터리에 `creds.txt` 보안 인증 파일을 생성합니다.
6. 다음 명령을 실행하여 사용자(소유자)만 파일을 읽고 쓸 수 있도록 `creds.txt` 파일 권한을 설정합니다.

```
$ chmod 700 creds.txt
```

파일 시스템 마운트

1. Active Directory에 조인하지 않은 파일 공유를 프라이빗 IP 주소를 사용하여 마운트합니다. Amazon FSx 콘솔을 사용하여 네트워크 및 보안 탭에 있는 기본 파일 서버 IP 주소에서 파일 시스템의 프라이빗 IP 주소를 가져올 수 있습니다.
2. 다음 명령을 사용하여 파일 시스템을 마운트합니다.

```
$ sudo mount -t cifs //file-system-IP-address/file_share /mnt/fsx
 --verbose -o vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

*`CIFSMaxBufSize`*의 값을 커널에서 허용하는 최대 값으로 바꿉니다. 최대 값을 알기 위해 다음 명령을 실행합니다.

```
$ modinfo cifs | grep CIFSMaxBufSize
```

```
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

출력이 최대 버퍼 크기가 130048임을 보여줍니다.

3. CIFS 파일 시스템만 반환하는 다음 명령을 실행하여 파일 시스템이 마운트되었는지 확인합니다.

```
$ mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_mode,username=user1,domain=CORP.EXA
```

이 절차에서 사용되는 마운트 명령은 지정된 시점에서 다음을 수행합니다.

- *//file-system-IP-address/file_share* - 마운트하는 파일 시스템의 IP 주소와 공유를 지정합니다.
- `-t cifs vers=`*SMB_version* - 파일 시스템 유형을 CIFS 및 SMB 프로토콜 버전으로 지정합니다. Amazon FSx for Windows File Server는 SMB 버전 2.0~3.1.1을 지원합니다.
- `sec=ntlmsspi` - 인증에 NT LAN Manager Security Support Provider Interface(NTLMSSPI)를 사용하도록 지정합니다.
- `cache=`*cache_mode* - 캐시 모드를 설정합니다. CIFS 캐시 옵션은 성능에 영향을 미칠 수 있으므로 커널 및 워크로드에 가장 적합한 설정을 테스트하고 Linux 설명서를 검토해야 합니다. `loose` 옵션은 프로토콜 의미 체계가 느슨하여 데이터 불일치가 발생할 수 있으므로 `strict` 또는 none 옵션을 권장합니다.
- `cred=/home/ec2-user/creds.txt` - 사용자 보안 인증 정보를 가져올 위치를 지정합니다.
- */mnt/fsx* - EC2 인스턴스에서 Amazon FSx 파일 공유의 마운트 지점을 지정합니다.
- `rsize=`*CIFSMaxBufSize*`,wsize=`*CIFSMaxBufSize* - 읽기 및 쓰기 버퍼 크기를 CIFS 프로토콜에서 허용하는 최대값으로 지정합니다. *CIFSMaxBufSize*의 값을 커널에서 허용하는 최대 값으로 바꿉니다. 다음 명령을 실행하여 `CIFSMaxBufSize`의 값을 결정합니다.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

Active Directory에 조인되지 않은 Amazon Linux EC2 인스턴스에 파일 공유 자동 마운트

FSx for Windows File Server 파일 공유는 마운트된 Amazon EC2 Linux 인스턴스가 재부팅될 때마다 자동으로 마운트할 수 있습니다. 자동으로 마운트하려면 EC2 인스턴스의 `/etc/fstab` 파일에 항목을 추가하세요. `/etc/fstab` 파일에는 파일 시스템에 대한 정보가 들어 있습니다. 인스턴스 시작 중에 실행되는 mount -a 명령은 `/etc/fstab` 파일에 나열된 파일 시스템을 마운트합니다.

Active Directory에 조인되지 않은 Amazon EC2 Linux 인스턴스의 경우, 프라이빗 IP 주소를 사용하여 FSx for Windows File Server 파일 공유만 마운트할 수 있습니다. Amazon FSx 콘솔을 사용하여 네트워크 및 보안 탭에 있는 기본 파일 서버 IP 주소에서 파일 시스템의 프라이빗 IP 주소를 가져올 수 있습니다.

다음 절차는 Microsoft NTLM 인증을 사용합니다. FSx for Windows File Server 파일 시스템이 조인된 Microsoft Active Directory 도메인의 구성원인 사용자로 파일 시스템을 마운트합니다. 사용자 계정의 보안 인증 정보는 `creds.txt` 텍스트 파일에 제공됩니다. 이 파일에는 사용자의 사용자 이름, 암호 및 도메인이 들어 있습니다.

```
$ cat creds.txt
username=user1
password=Password123
domain=EXAMPLE.COM
```

Active Directory에 조인되지 않은 Amazon Linux EC2 인스턴스에 파일 공유 자동 마운트

Amazon Linux EC2 인스턴스의 시작 및 구성

1. Amazon EC2 콘솔을 사용하여 Amazon Linux EC2 인스턴스를 시작합니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 시작을 참조하십시오.
2. 인스턴스에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Linux 인스턴스에 연결을 참조하십시오.
3. 다음 명령을 실행하여 `cifs-utils` 패키지를 설치합니다. 이 패키지는 Linux에서 Amazon FSx와 같은 네트워크 파일 시스템을 마운트하는 데 사용됩니다.

   ```
   $ sudo yum install cifs-utils
   ```

4. `/mnt/fsx` 디렉터리를 만듭니다. 여기에 Amazon FSx 파일 시스템을 마운트할 수 있습니다.

```
$ sudo mkdir /mnt/fsx
```

5. /home/ec2-user 디렉터리에 creds.txt 보안 인증 정보 파일을 생성합니다.
6. 다음 명령을 실행하여 사용자(소유자)만 파일을 읽을 수 있도록 파일 권한을 설정합니다.

```
$ sudo chmod 700 creds.txt
```

파일 시스템 자동 마운트

1. Active Directory에 조인하지 않은 파일 공유를 프라이빗 IP 주소를 사용하여 자동으로 마운트합니다. Amazon FSx 콘솔을 사용하여 네트워크 및 보안 탭에 있는 기본 파일 서버 IP 주소에서 파일 시스템의 프라이빗 IP 주소를 가져올 수 있습니다.
2. 프라이빗 IP 주소를 사용하여 파일 공유를 자동으로 마운트하려면 /etc/fstab 파일에 다음 줄을 추가하십시오.

```
//file-system-IP-address/file_share /mnt/fsx cifs
 vers=SMB_version,sec=ntlmsspi,cred=/home/ec2-user/
creds.txt,rsize=CIFSMaxBufSize,wsize=CIFSMaxBufSize,cache=none
```

*CIFSMaxBufSize*의 값을 커널에서 허용하는 최대 값으로 바꿉니다. 최대 값을 알기 위해 다음 명령을 실행합니다.

```
$ modinfo cifs | grep CIFSMaxBufSize
parm:           CIFSMaxBufSize:Network buffer size (not including header). Default:
 16384 Range: 8192 to 130048 (uint)
```

출력이 최대 버퍼 크기가 130048임을 보여줍니다.

3. 'all' 및 'verbose' 옵션과 함께 'fake '옵션을 사용하여 mount 명령을 실행함으로써 fstab 항목을 테스트합니다.

```
$ sudo mount -fav
home/ec2-user/fsx      : successfully mounted
```

4. 파일 공유를 마운트하려면 Amazon EC2 인스턴스를 재부팅합니다.
5. 인스턴스를 다시 사용할 수 있게 되면 다음 명령을 실행하여 파일 시스템이 마운트되었는지 확인합니다.

```
$ sudo mount -l -t cifs
//file-system-IP-address/file_share on /mnt/fsx type cifs
 (rw,relatime,vers=SMB_version,sec=ntlmsspi,cache=cache_code,username=user1,domain=CORP.EXA
```

이 절차에서 /etc/fstab 파일에 추가된 행은 지정된 시점에서 다음 작업을 수행합니다.

- *//file-system-IP-address/file_share* - 마운트하는 Amazon FSx 파일 시스템의 IP 주소와 공유를 지정합니다.
- /mnt/fsx - EC2 인스턴스에서 Amazon FSx 파일 시스템의 마운트 지점을 지정합니다.
- cifs vers=*SMB_version* - 파일 시스템 유형을 CIFS 및 SMB 프로토콜 버전으로 지정합니다. Amazon FSx for Windows File Server는 SMB 버전 2.0~3.1.1을 지원합니다.
- sec=ntlmsspi - NTLM 챌린지 응답 인증에 NT LAN Manager Security Support Provider Interface(NTLMSSPI)를 사용하도록 지정합니다.
- cache=*cache_mode* - 캐시 모드를 설정합니다. CIFS 캐시 옵션은 성능에 영향을 미칠 수 있으므로 커널 및 워크로드에 가장 적합한 설정을 테스트하고 Linux 설명서를 검토해야 합니다. loose 옵션은 프로토콜 의미 체계가 느슨하여 데이터 불일치가 발생할 수 있으므로 strict 또는 none 옵션을 권장합니다.
- cred=/home/ec2-user/creds.txt - 사용자 보안 인증 정보를 가져올 위치를 지정합니다.
- _netdev - 운영 체제에 파일 시스템을 네트워크 액세스를 요구하는 장치에 위치시키라고 명령합니다. 해당 옵션은 클라이언트에서 네트워크 서비스가 활성화되기 전에 인스턴스가 파일 시스템을 마운트하는 것을 방지합니다.
- 0 - 0이 아닌 값이면 파일 시스템을 dump까지 백업해야 함을 나타냅니다. Amazon FSx의 경우 이 값은 0이 되어야 합니다.
- 0 - 부팅 시 fsck가 파일 시스템을 검사하는 순서를 지정합니다. Amazon FSx 파일 시스템의 경우 이 값을 0으로 하여 시작 시 fsck가 실행되지 않도록 해야 합니다.

기존 파일 스토리지를 Amazon FSx로 마이그레이션

FSx for Windows File Server는 엔터프라이즈 애플리케이션을 Amazon Web Services Cloud로 쉽게 리프트 앤 시프트할 수 있는 기능, 성능 및 호환성을 제공합니다. FSx for Windows File Server로 마이그레이션하는 프로세스에는 다음 단계가 포함됩니다.

1. FSx for Windows File Server로 파일을 마이그레이션합니다. 자세한 정보는 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션을 참조하세요.
2. 파일 공유 구성을 FSx for Windows File Server로 마이그레이션합니다. 자세한 정보는 파일 공유 구성을 Amazon FSx로 마이그레이션을 참조하세요.
3. 기존 DNS 이름을 Amazon FSx 파일 시스템의 DNS 별칭으로 연결합니다. 자세한 내용은 DNS 별칭을 Amazon FSx와 연결을 참조하세요.
4. FSx for Windows File Server로 전환 자세한 정보는 Amazon FSx로 전환을 참조하세요.

프로세스의 각 단계에 대한 세부 정보는 다음 섹션에서 확인할 수 있습니다.

주제

- 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션
- 파일 공유 구성을 Amazon FSx로 마이그레이션
- DNS 구성을 Amazon FSx로 마이그레이션
- Amazon FSx로 전환

기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션

기존 파일을 FSx for Windows File Server 파일 시스템으로 마이그레이션하려면 스토리지 서비스와의 대량 데이터 복제를 간소화, 자동화 및 가속화하도록 설계된 온라인 데이터 전송 서비스를 사용하는 AWS DataSync것이 좋습니다. AWS DataSync 인터넷을 통해 데이터를 복사하거나 AWS Direct Connect완전 관리형 서비스이므로 DataSync 애플리케이션을 수정하거나 스크립트를 개발하거나 인프라를 관리할 필요가 거의 없습니다. 자세한 정보는 AWS DataSync를 사용하여 기존 파일을 FSx for Windows File Server로 마이그레이션을 참조하세요.

대체 솔루션으로는 Microsoft Windows용 명령줄 디렉터리 및 파일 복제 명령 집합인 Robust File Copy 또는 Robocopy를 사용할 수 있습니다. Robocopy를 사용하여 파일 스토리지를 FSx for Windows File Server로 마이그레이션하는 방법에 대한 자세한 절차는 Robocopy를 사용하여 기존 파일을 FSx for Windows File Server로 마이그레이션 섹션을 참조하세요.

기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션하는 모범 사례

대량의 데이터를 FSx for Windows File Server로 최대한 빨리 마이그레이션하려면 솔리드 스테이트 드라이브(SSD) 스토리지로 구성된 Amazon FSx 파일 시스템을 사용합니다. 마이그레이션이 완료된 후 애플리케이션에 가장 적합한 솔루션인 경우 하드 디스크 드라이브(HDD) 스토리지를 사용하여 Amazon FSx 파일 시스템으로 데이터를 이동할 수 있습니다.

SDD 스토리지를 사용하는 Amazon FSx 파일 시스템에서 HDD 스토리지로 데이터를 이동하려면 다음 단계를 수행합니다. (HDD 파일 시스템의 스토리지 용량은 최소 2TB이며 백업에서 복원할 때는 스토리지 용량을 변경할 수 없습니다.)

1. SSD 파일 시스템을 백업합니다. 자세한 정보는 사용자 시작 백업 생성을 참조하세요.
2. HDD 스토리지를 사용하는 파일 시스템에 백업을 복원합니다. 자세한 정보는 백업 복원을 참조하세요.

AWS DataSync를 사용하여 기존 파일을 FSx for Windows File Server로 마이그레이션

Windows File Server 파일 시스템용 FSx 간에 데이터를 전송하는 AWS DataSync 데 사용하는 것이 좋습니다. DataSync 인터넷 또는 기타 AWS 스토리지 서비스를 통해 온프레미스 스토리지 시스템과 다른 스토리지 서비스 간에 데이터를 이동 및 복제하는 작업을 간소화, 자동화 및 가속화하는 데이터 전송 서비스입니다. AWS Direct Connect DataSync 소유권, 타임스탬프, 액세스 권한 등의 파일 시스템 데이터와 메타데이터를 전송할 수 있습니다.

DataSync NTFS ACL (액세스 제어 목록) 복사를 지원하고, 관리자가 사용자의 파일 액세스 시도에 대한 감사 로깅을 제어하는 데 사용하는 파일 감사 제어 정보 (NTFS 시스템 액세스 제어 목록 (SACL) 라고도 하는 파일 감사 제어 정보 복사도 지원합니다.

를 DataSync 사용하여 두 FSx for Windows File Server 파일 시스템 간에 파일을 전송할 수 있으며 다른 또는 계정의 파일 시스템으로 데이터를 이동할 수도 있습니다. AWS 리전 AWS Windows File Server 파일 시스템용 DataSync FSx와 함께 사용하여 다른 작업을 수행할 수 있습니다. 예를 들어, 일회성 데이터 마이그레이션을 수행하고, 분산 워크로드를 위해 주기적으로 데이터를 수집하며, 복제를 예약하여 데이터를 보호 및 복구할 수 있습니다.

에서 AWS DataSync Windows File Server용 FSx의 위치는 Windows 파일 서버용 FSx의 엔드포인트입니다. FSx for Windows File Server의 위치와 다른 파일 시스템의 위치 간에 파일을 전송할 수 있습니다. 자세한 내용은 AWS DataSync 사용 설명서의 여러 위치 간의 작업을 참조하세요.

DataSync SMB (서버 메시지 블록) 프로토콜을 사용하여 Windows File Server용 FSx에 액세스합니다. 콘솔 또는 콘솔에서 구성한 사용자 이름과 암호로 인증합니다. AWS DataSync AWS CLI

필수 조건

Windows File Server용 Amazon FSx 설정으로 데이터를 마이그레이션하려면 요구 사항을 충족하는 서버와 네트워크가 DataSync 필요합니다. 자세한 내용은 DataSync AWS DataSync 사용 설명서의 요구 사항을 참조하십시오.

대규모 데이터 마이그레이션 또는 여러 개의 작은 파일이 포함된 마이그레이션을 수행하는 경우 SSD 스토리지 유형의 Amazon FSx 파일 시스템을 사용하는 것이 좋습니다. 이는 DataSync 작업에 파일 메타데이터 스캔이 포함되므로 HDD 파일 시스템의 디스크 IOPS 한도가 소진되어 장기간 실행되는 마이그레이션이 발생하고 파일 시스템 성능에 영향을 미칠 수 있기 때문입니다. 자세한 내용은 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션하는 모범 사례 섹션을 참조하세요.

데이터세트가 대부분 작은 파일로 구성되어 있고 파일 수가 수백만 개에 달하거나 단일 DataSync 작업보다 사용 가능한 네트워크 대역폭이 더 많은 경우 스케일 아웃 아키텍처를 통해 데이터 전송을 가속화할 수도 있습니다. 자세한 내용은 AWS DataSync 스케일 아웃 아키텍처로 데이터 전송을 가속화하는 방법을 참조하세요.

FSx 성능 지표를 사용하여 파일 시스템의 디스크 I/O 사용률을 모니터링할 수 있습니다.

를 사용하여 파일을 마이그레이션하는 기본 단계 DataSync

를 사용하여 DataSync 원본 위치에서 대상 위치로 파일을 전송하려면 다음 기본 단계를 따르세요.

- 사용자 환경에서 에이전트를 다운로드하여 배포하고 활성화합니다.
- 소스 및 대상 위치를 생성하고 구성합니다.
- 작업을 생성하고 구성합니다.
- 작업을 실행하여 소스에서 대상으로 파일 전송.

기존 온프레미스 파일 시스템에서 Windows File Server용 FSx로 파일을 전송하는 방법을 알아보려면 사용 설명서의 자체 관리형 AWS스토리지와 (과) 간의 데이터 전송, 중소기업용 위치 생성및 Windows File Server용 Amazon FSx 위치 생성을 참조하십시오.AWS DataSync

기존 클라우드 내 파일 시스템에서 FSx for Windows File Server로 파일을 전송하는 방법을 알아보려면 AWS DataSync 사용 설명서의 에이전트를 Amazon EC2 인스턴스로 배포를 참조하세요.

두 Amazon FSx 파일 시스템 간 마이그레이션

를 DataSync 사용하여 두 Amazon FSx 파일 시스템 간에 데이터를 마이그레이션할 수 있습니다. 이는 기존 파일 시스템에서 구성이 다른 새 파일 시스템으로(예: 단일 AZ에서 다중 AZ 구성으로) 워크로드를 이동해야 하는 경우에 유용할 수 있습니다. 또한 두 파일 시스템 간에 워크로드를 DataSync 분할하는 데 사용할 수 있습니다.

다음은 마이그레이션 프로세스의 샘플 개요입니다.

1. 소스 및 대상 파일 시스템의 DataSync 위치를 생성합니다. 소스와 대상은 동일한 Active Directory(AD) 도메인에 속하거나 도메인 간에 AD 신뢰 관계가 있어야 한다는 점에 유의하세요.
2. 소스에서 대상으로 데이터를 전송하는 DataSync 작업을 생성하고 구성합니다. 작업을 일회성 인스턴스로 실행하거나, 구성한 일정에 따라 작업이 자동으로 실행되도록 설정할 수 있습니다.
3. 작업이 완료되면 대상 파일 시스템의 데이터가 소스의 정확한 사본이 됩니다. 단, 작업을 완료하려면 소스 파일 시스템에서 쓰기 활동이나 파일 업데이트를 일시 중지해야 합니다. 그런 다음 대상 파일 시스템으로 전환하고 소스 파일 시스템을 삭제할 수 있습니다.

프로덕션 파일 시스템에서 마이그레이션하기 전에 최근 백업에서 복원된 파일 시스템에서 마이그레이션 프로세스를 테스트할 수 있습니다. 이를 통해 데이터 전송 프로세스에 걸리는 시간을 예측하고 DataSync 오류를 미리 해결할 수 있습니다.

컷오버 시간을 최소화하기 위해 소스 파일 시스템에서 대상 파일 시스템으로 대부분의 데이터를 이동하는 DataSync 작업을 미리 실행할 수 있습니다. 소스 파일 시스템으로 향하는 트래픽을 중지한 후에는 최종 작업 전송을 실행하여 트래픽이 중단된 이후 새로 업데이트된 데이터를 동기화한 다음 대상 파일 시스템으로 전환할 수 있습니다.

특정 디렉터리에서만 실행하거나 특정 경로를 포함 또는 제외하도록 DataSync 작업을 구성할 수 있습니다. 이는 여러 작업을 병렬로 실행하거나 데이터의 일부를 마이그레이션하려는 경우에 유용할 수 있습니다.

대상 파일 시스템에 소스 파일 시스템의 DNS 이름과 동일한 DNS 별칭을 만들 수 있습니다. 이렇게 하면 최종 사용자와 애플리케이션이 소스 파일 시스템의 DNS 이름을 사용하여 파일 데이터에 계속 액세스할 수 있습니다. DNS 별칭 설정 방법에 대한 자세한 내용은 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스 섹션을 참조하세요.

이러한 유형의 마이그레이션을 수행할 때는 다음을 권장합니다.

- 파일 시스템 백업, 주별 유지 관리 기간 및 `Data Deduplication` 작업을 피하도록 마이그레이션 일정을 잡습니다. 특히 계획된 마이그레이션과 일치하는 경우 `Data Deduplication GarbageCollection` 작업을 비활성화하는 것이 좋습니다.
- 소스 및 대상 파일 시스템 모두에 SSD 스토리지 유형을 사용합니다. 백업에서 복원하여 HDD와 SSD 스토리지 유형 간에 전환할 수 있습니다. 자세한 내용은 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션 섹션을 참조하세요.
- 전송해야 하는 데이터 양에 충분한 처리량 용량을 갖도록 소스 및 대상 파일 시스템을 구성합니다. DataSync 작업 프로세스 중에 소스 및 대상 파일 시스템의 성능 사용률을 모니터링하십시오. 자세한 내용은 Amazon을 통한 지표 모니터링 CloudWatch 섹션을 참조하세요.
- 진행 중인 작업의 진행 상황을 이해하는 데 도움이 되도록 DataSync 모니터링을 설정하십시오. 오류가 발생할 경우 Amazon Logs 그룹에 DataSync CloudWatch 로그를 전송하여 작업을 디버깅하는 데 도움을 받을 수도 있습니다.

Robocopy를 사용하여 기존 파일을 FSx for Windows File Server로 마이그레이션

Microsoft Windows Server를 기반으로 구축된 Amazon FSx for Windows File Server를 사용하면 기존 데이터 세트를 Amazon FSx 파일 시스템으로 완전히 마이그레이션할 수 있습니다. 각 파일의 데이터를 마이그레이션할 수 있습니다. 또한 속성, 타임스탬프, 액세스 제어 목록(ACL), 소유자 정보, 감사 정보를 비롯한 모든 관련 파일 메타데이터를 마이그레이션할 수 있습니다. Amazon FSx는 이러한 전체 마이그레이션 지원을 통해 이러한 파일 데이터 세트를 사용하는 Windows 기반 워크로드 및 애플리케이션을 Amazon Web Services Cloud로 이전할 수 있도록 지원합니다.

다음 주제를 기존 파일 데이터를 복사하는 프로세스의 지침으로 사용합니다. 이 복사를 수행하면 온프레미스 데이터 센터 또는 Amazon EC2의 자체 관리형 파일 서버의 모든 파일 메타데이터를 보존하게 됩니다.

사전 조건

시작하기 전에 다음을 수행했는지 확인합니다.

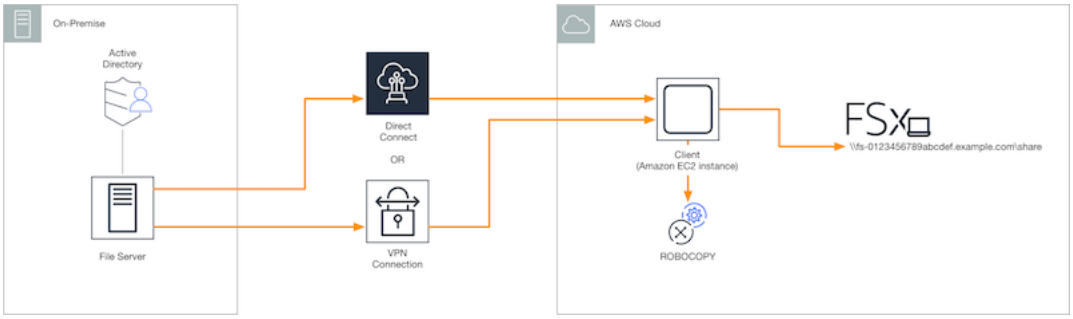
- 온프레미스 Active Directory와 Amazon FSx 파일 시스템을 만들려는 VPC 간에 네트워크 연결(AWS Direct Connect 또는 VPN 사용) 을 설정합니다.
- Active Directory에는 컴퓨터를 도메인에 조인할 수 있는 권한이 위임된 서비스 계정을 만듭니다. 자세한 내용은 AWS Directory Service 관리 가이드의 서비스 계정에 권한 위임을 참조하세요.
- 자체 관리형(온프레미스) Microsoft AD 디렉터리에 조인된 Amazon FSx 파일 시스템을 생성합니다.

- Amazon FSx로 전송하려는 기존 파일이 포함된 파일 공유 (예: 온프레미스 또는 내부 `\\Source\Share` AWS) 의 위치 (예:) 를 기록해 둡니다.
- 기존 파일이 전송될 Amazon FSx 파일 시스템의 파일 공유 위치(예: `\\Target\Share`)를 기록해 둡니다.

다음 표에는 세 가지 마이그레이션 사용자 액세스 모델에 대한 소스 및 대상 파일 시스템 접근성 요구 사항이 요약되어 있습니다.

마이그레이션 사용자 액세스 모델	소스 파일 시스템 접근성 요구 사항	대상 FSx 파일 서버 접근성 요구 사항
직접 읽기/쓰기 권한 모델	사용자는 마이그레이션 할 파일 및 폴더에 대해 최소 읽기 권한(NTFS ACL)을 가지고 있어야 합니다.	사용자는 마이그레이션 할 파일 및 폴더에 대해 최소 쓰기 권한(NTFS ACL)을 가지고 있어야 합니다.
액세스 권한을 재정의하는 백업/복원 권한 모델	사용자는 온-프레미스 Active Directory의 백업 운영자 그룹의 구성원이어야 하며 /b 플래그와 함께 사용해야 합니다. RoboCopy	사용자는 Amazon FSx 파일 시스템 관리자 그룹*의 구성원이어야 하며 /b 플래그와 함께 사용해야 합니다. RoboCopy
액세스 권한을 재정의하는 도메인 관리자 (전체) 권한 모델	사용자는 온프레미스 Active Directory의 도메인 관리자 그룹의 구성원이어야 합니다.	사용자는 Amazon FSx 파일 시스템 관리자 그룹*의 구성원이어야 하며 /b 플래그를 다음과 같이 사용해야 합니다. RoboCopy

> **Note**
>
> * AWS 관리형 Microsoft AD에 가입된 파일 시스템의 경우 Amazon FSx 파일 시스템 관리자 그룹은 AWS 위임 FSx 관리자입니다. 자체 관리형 Microsoft AD에서 Amazon FSx 파일 시스템 관리자 그룹은 파일 시스템을 생성할 때 관리를 위해 지정한 도메인 관리자 또는 사용자 지정 그룹입니다.



Robocopy를 사용하여 기존 파일을 Amazon FSx로 마이그레이션하는 방법

다음 절차를 사용하여 기존 파일을 Amazon FSx로 마이그레이션할 수 있습니다.

Robocopy를 사용하여 기존 파일을 Amazon FSx로 마이그레이션

1. Amazon FSx 파일 시스템과 동일한 Amazon VPC에서 Windows Server 2016 Amazon EC2 인스턴스를 시작합니다.
2. Amazon EC2 인스턴스에 연결합니다. 자세한 내용은 Windows 인스턴스용 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하세요.
3. 명령 프롬프트를 열고 다음과 같이 기존 파일 서버 (온-프레미스 또는 내부 AWS) 의 소스 파일 공유를 드라이브 문자 (예: *Y*:) 에 매핑합니다. 이 과정에서 온프레미스 Active Directory의 도메인 관리자 그룹 구성원에 대한 보안 인증 정보를 제공합니다.

```
C:\>net use Y: \\fileserver1.mydata.com\localdata /user:mydata.com\Administrator
Enter the password for 'fileserver1.mydata.com': _

Drive Y: is now connected to \\fileserver1.mydata.com\localdata.

The command completed successfully.
```

4. 다음과 같이 Amazon FSx 파일 시스템의 대상 파일 공유를 Amazon EC2 인스턴스의 다른 드라이브 문자(예: *Z*:)에 매핑합니다. 이 과정에서 온프레미스 Active Directory의 도메인 관리자 그룹과 Amazon FSx 파일 시스템의 관리자 그룹에 속하는 사용자 계정에 대한 보안 인증 정보를 제공합니다. AWS 관리형 Microsoft AD에 가입된 파일 시스템의 경우 해당 그룹은 다음과 같습니다 **`AWS Delegated FSx Administrators`**. 자체 관리형 Microsoft AD에서 해당 그룹은 파일 시스템을 생성할 때 관리를 위해 지정한 **`Domain Admins`** 또는 사용자 지정 그룹입니다.

   자세한 내용은 사전 조건의 소스 및 대상 파일 시스템 접근성 요구 사항 표를 참조하세요.

```
C:\>net use Z: \\amznfsxabcdef1.mydata.com\share /user:mydata.com\Administrator
```

```
Enter the password for 'amznfsxabcdef1.mydata.com': _

Drive Z: is now connected to \\amznfsxabcdef1.mydata.com\share.

The command completed successfully.
```

5. 컨텍스트 메뉴에서 관리자 권한으로 실행을 선택합니다. 관리자 PowerShell 권한으로 명령 프롬프트 또는 Windows를 열고 다음 Robocopy 명령을 실행하여 소스 공유에서 대상 공유로 파일을 복사합니다.

   ROBOCOPY 명령은 데이터 전송 프로세스를 제어할 수 있는 여러 옵션이 있는 유연한 파일 전송 유틸리티입니다. 이 ROBOCOPY 명령 프로세스로 인해 소스 공유의 모든 파일 및 디렉터리가 Amazon FSx 대상 공유로 복사됩니다. 복사본에는 파일 및 폴더 NTFS ACL, 속성, 타임스탬프, 소유자 정보 및 감사 정보가 보존됩니다.

   ```
   robocopy Y:\ Z:\ /copy:DATSOU /secfix /e /b /MT:8
   ```

   앞의 예제 명령에서는 다음 요소와 옵션을 사용합니다.

   - Y - 온프레미스 Active Directory 포리스트 mydata.com에 있는 소스 공유를 나타냅니다.
   - Z - Amazon FSx의 대상 공유 \\amznfsxabcdef1.mydata.com\share를 나타냅니다.
   - /copy - 복사할 다음 파일 속성을 지정합니다.
     - D - 데이터
     - A - 속성
     - T - 타임스탬프
     - S - NTFS ACL
     - O - 소유자 정보
     - U - 감사 정보.
   - /secfix - 모든 파일, 심지어 건너뛰는 파일까지 파일 보안을 수정합니다.
   - /e - 빈 디렉터리를 포함한 하위 디렉터리를 복사합니다.
   - /b - NTFS ACL이 현재 사용자에 대한 권한을 거부하는 경우에도 Windows의 백업 및 복원 권한을 사용하여 파일을 복사합니다.
   - /MT:8 - 멀티스레드 복사를 수행하는 데 사용할 스레드 수를 지정합니다.

> **Note**
>
> 연결이 느리거나 불안정한 상태에서 큰 파일을 복사하는 경우 /b 옵션 대신 /zb 옵션을 robocopy와 함께 사용하여 재시작 가능 모드를 활성화할 수 있습니다. 재시작 가능 모드를 사용하면 대용량 파일의 전송이 중단되는 경우 전체 파일을 처음부터 다시 복사하지 않고 전송 중간에 후속 Robocopy 작업을 재개할 수 있습니다. 재시작 가능 모드를 활성화하면 데이터 전송 속도를 줄일 수 있습니다.

파일 공유 구성을 Amazon FSx로 마이그레이션

다음 절차를 사용하여 기존 파일 공유 설정을 Amazon FSx로 마이그레이션할 수 있습니다. 이 절차에서 소스 파일 서버는 Amazon FSx로의 마이그레이션 대상이 되는 파일 공유 구성을 가진 파일 서버입니다.

> **Note**
>
> 파일 공유 구성을 마이그레이션하기 전에 먼저 파일을 Amazon FSx로 마이그레이션하세요. 자세한 정보는 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션을 참조하세요.

기존 파일 공유를 FSx for Windows File Server로 마이그레이션

1. 소스 파일 서버의 컨텍스트 메뉴에서 관리자 권한으로 실행을 선택합니다. 관리자 PowerShell 권한으로 Windows를 엽니다.
2. 에서 다음 명령을 `SmbShares.xml` 실행하여 소스 파일 서버의 파일 공유를 이름이 지정된 파일로 내보냅니다 PowerShell. 이 예제에서 F:를 파일 공유를 내보내는 파일 서버의 드라이브 문자로 바꿉니다.

   ```
   $shareFolder = Get-SmbShare -Special $false | ? { $_.Path -like “F:\*” }
   $shareFolder | Export-Clixml -Path F:\SmbShares.xml
   ```

3. Amazon FSx 파일 시스템이 D:\share에 있으므로 F:(사용자의 드라이브 문자)에 대한 모든 참조를 D:\share로 대체하여 `SmbShares.xml` 파일을 편집합니다.
4. 기존 파일 공유 구성을 FSx for Windows File Server로 가져옵니다. 대상 Amazon FSx 파일 시스템 및 소스 파일 서버에 액세스할 수 있는 클라이언트에서 저장된 파일 공유 구성을 복사합니다. 그런 다음, 다음 명령을 사용하여 변수로 가져옵니다.

```
$shares = Import-Clixml -Path F:\SmbShares.xml
```

5. 다음 옵션 중 하나를 사용하여 FSx for Windows File Server 파일 서버에서 파일 공유를 생성하는 데 필요한 보안 인증 객체를 준비합니다.

   대화형 방식으로 보안 인증 객체를 생성하려면 다음 명령을 사용합니다.

   ```
   $credential = Get-Credential
   ```

   AWS Secrets Manager 리소스를 사용하여 자격 증명 개체를 생성하려면 다음 명령을 사용합니다.

   ```
   $credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
    $AdminSecret).SecretString
   $FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
   SecureString $credential.Password -AsPlainText -Force)))
   ```

6. 다음 스크립트를 사용하여 파일 공유 구성을 Amazon FSx 파일 서버로 마이그레이션합니다.

   ```
   $FSxAcceptedParameters = ("ContinuouslyAvailable", "Description",
    "ConcurrentUserLimit", "CATimeout", "FolderEnumerationMode", "CachingMode",
    "FullAccess", "ChangeAccess", "ReadAccess", "NoAccess", "SecurityDescriptor",
    "Path", "Name", "EncryptData")
   ForEach ($item in $shares) {
       $param = @{};
       Foreach ($property in $item.psObject.properties) {
           if ($property.Name -In $FSxAcceptedParameters) {
               $param[$property.Name] = $property.Value
           }
       }
       Invoke-Command -ConfigurationName FSxRemoteAdmin -ComputerName
    amznfsxxxxxxxxx.corp.com -ErrorVariable errmsg -ScriptBlock { New-FSxSmbShare -
   Credential $Using:credential @Using:param }
   }
   ```

DNS 구성을 Amazon FSx로 마이그레이션

FSx for Windows File Server는 파일 시스템의 데이터에 액세스하는 데 사용할 수 있는 모든 파일 시스템에 기본 도메인 이름 시스템(DNS) 이름을 제공합니다. 또한 대체 DNS 이름을 Amazon FSx 파일 시스템의 DNS 별칭으로 구성하여 원하는 DNS 이름을 사용하여 파일 시스템에 액세스할 수 있습니다.

DNS 별칭을 사용하면 온프레미스에서 Amazon FSx로 파일 시스템 스토리지를 마이그레이션할 때 기존 DNS 이름을 사용하여 Amazon FSx에 저장된 데이터에 계속 액세스할 수 있습니다. 이렇게 하면 Amazon FSx로 마이그레이션할 때 DNS 이름을 사용하는 도구 또는 애플리케이션을 업데이트할 필요가 없습니다. 새 파일 시스템을 생성하고 백업에서 새 파일 시스템을 생성할 때 기존 FSx for Windows File Server 파일 시스템에 DNS 별칭을 연결할 수 있습니다. 언제든지 한 번에 파일 시스템에 최대 50개의 DNS 별칭을 연결할 수 있습니다. 자세한 정보는 DNS 별칭 관리을 참조하세요.

별칭 이름은 다음 요구 사항을 충족해야 합니다.

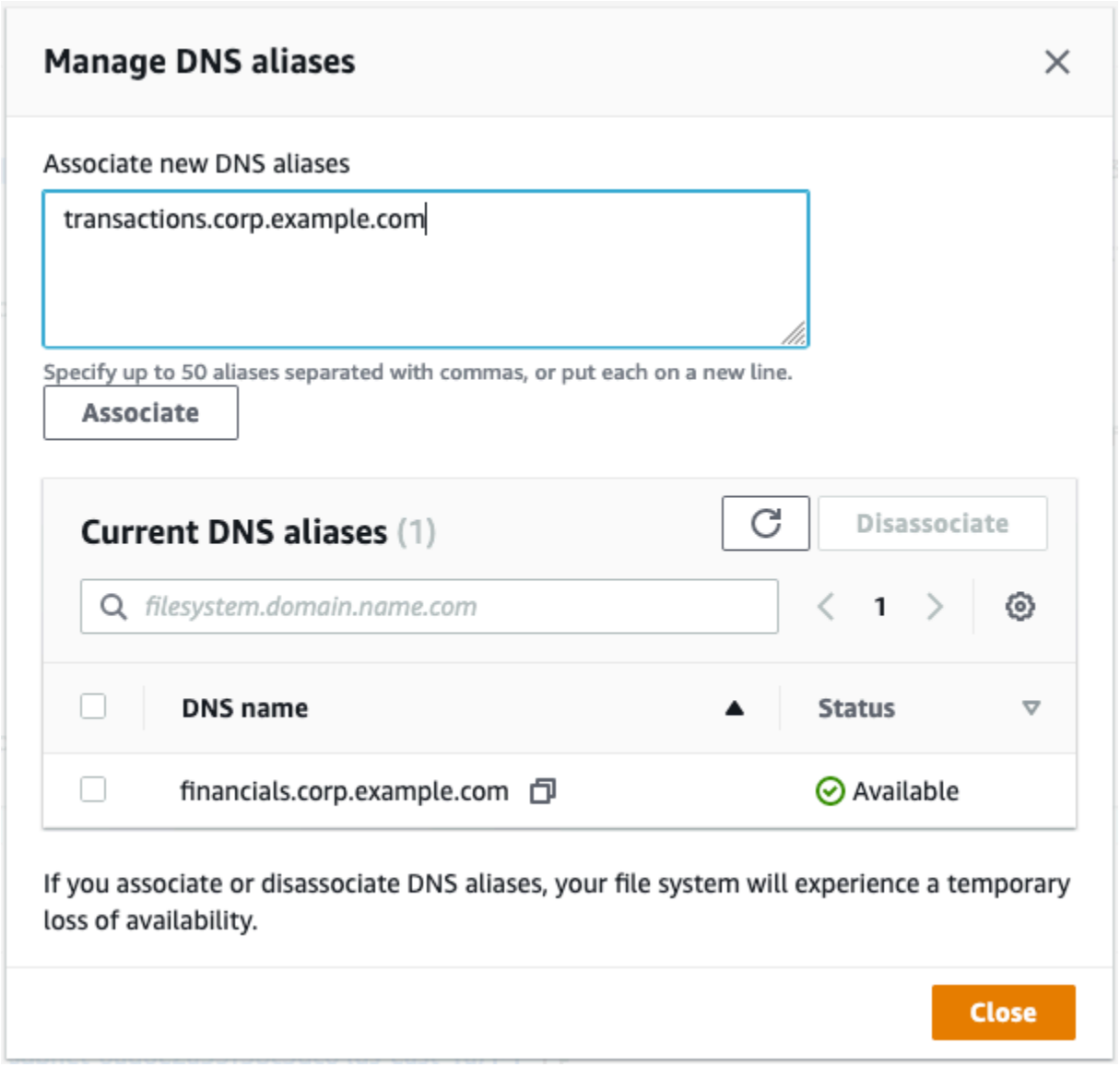
- 정규화된 도메인 이름(FQDN)(예: `accounting.example.com`) 형식으로 지정해야 합니다.
- 영숫자 및 하이픈(-)을 포함할 수 있습니다.
- 하이픈으로 시작되거나 끝날 수 없습니다.
- 숫자로 시작될 수 있습니다.

DNS 별칭 이름의 경우 Amazon FSx는 영문자가 지정된 방법(대문자, 소문자 또는 이스케이프 코드)과 관계없이 영문자를 소문자(a~z)로 저장합니다.

다음 절차는 Amazon FSx 콘솔, CLI 및 API를 사용하여 기존 FSx for Windows File Server 파일 시스템에 DNS 별칭을 연결하는 방법을 설명합니다. 백업에서의 새 파일 시스템을 포함하여 새 파일 시스템을 생성할 때 DNS 별칭을 연결하는 방법에 대한 자세한 내용은 DNS 별칭을 파일 시스템에 연결 섹션을 참조하세요.

DNS 별칭을 기존 파일 시스템과 연결(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 DNS 별칭과 연결할 Windows 파일 시스템을 선택합니다.
3. 네트워크 및 보안 탭에서 DNS 별칭의 관리를 선택하여 DNS 별칭 관리 대화 상자를 엽니다.



4. 새 별칭 연결 상자에서, 연결하려는 DNS 별칭을 입력합니다.
5. 연결을 선택하여 파일 시스템에 별칭을 추가합니다.

   현재 별칭 목록에서 연결한 별칭의 상태를 모니터링할 수 있습니다. 상태가 사용 가능으로 표시되면 별칭이 파일 시스템과 연결됩니다(이 프로세스에는 최대 2.5분이 소요될 수 있음).

DNS 별칭을 기존 파일 시스템과 연결(CLI)

- `associate-file-system-aliases`CLI 명령 또는 AssociateFileSystemAliasesAPI 작업을 사용하여 DNS 별칭을 기존 파일 시스템에 연결합니다.

  다음 CLI 요청은 별칭 두 개를 지정된 파일 시스템과 연결합니다.

```
aws fsx associate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com transfers.corp.example.com
```

응답은 Amazon FSx가 파일 시스템과 연결하는 별칭의 상태를 보여줍니다.

```
{
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": CREATING
          },
          {
              "Name": "transfers.corp.example.com",
              "Lifecycle": CREATING
          }
      ]
  }
```

연결 중인 별칭의 상태를 모니터링하려면 `describe-file-system-aliases` CLI 명령(DescribeFileSystemAliases동일한 API 작업) 을 사용합니다. `Lifecycle`의 별칭 값이 '사용 가능'이면 이를 사용하여 파일 시스템에 액세스할 수 있습니다(이 프로세스에는 최대 2.5분이 소요될 수 있음).

Amazon FSx로 전환

FSx for Windows File Server 파일 시스템으로 전환하려면 다음 단계를 수행합니다.

- 전환을 준비합니다.
  - 원래 파일 시스템에서 SMB 클라이언트의 연결을 일시적으로 끊습니다.
  - 최종 파일 및 파일 공유 구성 동기화를 수행합니다.
- Amazon FSx 파일 시스템의 서비스 보안 주체 이름(SPN)을 구성합니다.
- Amazon FSx 파일 시스템을 가리키도록 DNS CNAME 레코드를 업데이트합니다.

각 단계를 수행하는 절차는 다음 섹션에 나와 있습니다.

주제

Amazon FSx로 전환하기 위한 준비

Amazon FSx 파일 시스템으로 전환을 준비하기 위해 다음을 수행해야 합니다.

- 원본 파일 시스템에 기록하는 모든 클라이언트의 연결을 끊습니다.
- 또는 Robocopy를 사용하여 AWS DataSync 최종 파일 동기화를 수행합니다. 자세한 정보는 기존 파일 스토리지를 FSx for Windows File Server로 마이그레이션을 참조하세요.
- 최종 파일 및 공유 구성 동기화를 수행합니다. 자세한 정보는 파일 공유 구성을 Amazon FSx로 마이그레이션을 참조하세요.

Kerberos 인증에 대한 SPN 구성

Amazon FSx에서 Kerberos 기반 인증 및 전송 중 암호화를 사용하는 것이 좋습니다. Kerberos는 파일 시스템에 액세스하는 클라이언트에게 가장 안전한 인증을 제공합니다. DNS 별칭을 사용하여 Amazon FSx에 액세스하는 클라이언트에 대해 Kerberos 인증을 활성화하려면 Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에서 DNS 별칭에 해당하는 서비스 보안 주체 이름(SPN)을 추가해야 합니다.

Kerberos 인증에는 두 개의 필수 SPN이 있습니다.

```
HOST/alias
HOST/alias.domain
```

예를 들어 별칭이 `finance.domain.com`인 경우 두 개의 필수 SPN은 다음과 같습니다.

```
HOST/finance
HOST/finance.domain.com
```

SPN은 한 번에 하나의 Active Directory 컴퓨터 객체와만 연결할 수 있습니다. 원본 파일 시스템의 Active Directory 컴퓨터 객체에 대해 구성된 DNS 이름의 기존 SPN이 있는 경우 Amazon FSx 파일 시스템용 SPN을 생성하기 전에 해당 SPN을 삭제해야 합니다.

다음 절차는 기존 SPN을 찾고, 삭제하고, Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체를 위한 새 SPN을 생성하는 방법을 설명합니다.

필수 PowerShell Active Directory 모듈을 설치하려면

1. Amazon FSx 파일 시스템이 조인되어 있는 Active Directory에 조인된 Windows 인스턴스에 로그온합니다.
2. 관리자 PowerShell 권한으로 엽니다.
3. 다음 명령을 사용하여 PowerShell 액티브 디렉터리 모듈을 설치합니다.

```
Install-WindowsFeature RSAT-AD-PowerShell
```

원본 파일 시스템의 Active Directory 컴퓨터 개체에서 기존 DNS 별칭 SPN을 찾아 삭제

1. 다음 명령을 사용하여 기존 SPN을 모두 찾습니다. *alias_fqdn*를 DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템과 연결한 DNS 별칭으로 바꿉니다.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 다음 예제 스크립트를 사용하여 이전 단계에서 반환된 기존 HOST SPN을 삭제합니다.

   - *alias_fqdn*을 DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템과 연결한 전체 DNS 별칭으로 바꿉니다.
   - *file_system_DNS_name*을 원본 파일 시스템의 DNS 이름으로 바꿉니다.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템과 연결한 각 DNS 별칭에 대해 이 단계를 반복합니다.

Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 SPN 설정

1. 다음 명령을 실행하여 Amazon FSx 파일 시스템의 새 SPN을 설정합니다.

   - *file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 DNS 이름으로 바꿉니다.

     Amazon FSx 콘솔에서 파일 시스템의 DNS 이름을 찾으려면 파일 시스템을 선택하여 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지의 네트워크 및 보안 창을 선택합니다. DescribeFile시스템 API 작업의 응답으로 DNS 이름을 가져올 수도 있습니다.
   - *alias_fqdn*을 DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템과 연결한 전체 DNS 별칭으로 바꿉니다.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> DNS 별칭에 대한 SPN이 원본 파일 시스템의 컴퓨터 객체의 AD에 있는 경우 Amazon FSx 파일 시스템에 대한 SPN 설정이 실패합니다. 기존 SPN 검색 및 삭제에 대한 자세한 내용은 원본 파일 시스템의 Active Directory 컴퓨터 개체에서 기존 DNS 별칭 SPN을 찾아 삭제 섹션을 참조하세요.

2. 다음 예제 스크립트를 사용하여 DNS 별칭에 대해 새 SPN이 구성되었는지 확인합니다. 응답에 두 개의 호스트 SPN인 HOST/*alias* 및 HOST/*alias_fqdn*이 포함되어 있는지 확인합니다.

*file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 DNS 이름으로 바꿉니다. Amazon FSx 콘솔에서 파일 시스템의 DNS 이름을 찾으려면 파일 시스템을 선택하고 파일 시스템을 선택한 다음 파일 시스템 세부 정보 페이지의 네트워크 및 보안 창을 선택합니다.

DescribeFile시스템 API 작업에 대한 응답으로 DNS 이름을 가져올 수도 있습니다.

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템과 연결한 각 DNS 별칭에 대해 이전 단계를 반복합니다.

> **Note**
>
> Active Directory에서 다음과 같은 그룹 정책 객체(GPO)를 설정하여 DNS 별칭으로 파일 시스템에 연결하는 클라이언트가 Kerberos 인증 및 전송 중 암호화를 사용하도록 할 수 있습니다.
>
> - NTLM 제한: 원격 서버로 나가는 NTLM 트래픽
> - NTLM 제한: NTLM 인증을 위한 원격 서버 예외 추가
>
> 자세한 내용은 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스의 GPO를 사용하여 Kerberos 인증 적용 섹션을 참조하세요.

Amazon FSx 파일 시스템의 DNS CNAME 레코드 업데이트

파일 시스템에 맞게 SPN을 적절히 구성한 후에는 원본 파일 시스템으로 확인된 각 DNS 레코드를 Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 레코드로 교체하여 Amazon FSx로 전환할 수 있습니다.

필수 PowerShell cmdlet을 설치하려면

1. Amazon FSx 파일 시스템이 DNS 관리 권한을 가진 그룹의 구성원인 사용자 AWS (AWS 관리형 Microsoft Active Directory의 위임 도메인 이름 시스템 관리자, 자체 관리형 Active Directory에서

DNS 관리 권한을 위임한 도메인 관리자 또는 사용자가 자체 관리형 Active Directory에서 DNS 관리 권한을 위임한 다른 그룹) 의 구성원인 사용자로 가입된 Active Directory에 가입된 Windows 인스턴스에 로그온합니다.

자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

2. 관리자 PowerShell 권한으로 엽니다.
3. 이 절차의 지침을 수행하려면 PowerShell DNS 서버 모듈이 필요합니다. 다음 명령을 사용하여 설치합니다.

```
Install-WindowsFeature RSAT-DNS-Server
```

기존 DNS CNAME 레코드 업데이트

1. 다음 스크립트는 *alias_fqdn*에 대한 기존 DNS CNAME 레코드를 Amazon FSx 파일 시스템의 컴퓨터 객체로 업데이트합니다. 찾지 못했다면 Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 별칭 *alias_fqdn*에 대한 새 DNS CNAME 레코드를 생성합니다.

   스크립트를 실행하려면 다음과 같이 하세요.

   - *alias_fqdn*을 파일 시스템에 연결한 DNS 별칭으로 바꿉니다.
   - *file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 기본 DNS 이름으로 바꿉니다.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name)[0]

Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName
 $DnsServerComputerName -HostNameAlias $FSxDnsName -ZoneName $ZoneName
```

2. DNS 구성을 Amazon FSx로 마이그레이션에서 파일 시스템에 연결한 각 DNS 별칭에 대해 이전 단계를 반복합니다.

FSx for Windows File Server에서의 Microsoft SQL Server 사용

고가용성(HA) Microsoft SQL Server는 일반적으로 Windows Server 장애 조치 클러스터(WSFC)의 여러 데이터베이스 노드에 배포되며, 각 노드는 공유 파일 스토리지에 액세스할 수 있습니다. FSx for Windows File Server를 고가용성(HA) Microsoft SQL Server 배포를 위한 공유 스토리지로 사용할 수 있으며, 활성 데이터 파일을 위한 스토리지와 SMB 파일 공유 감시 두 가지 방법이 있습니다.

> **Note**
>
> 현재 Amazon FSx는 Microsoft SQL Server IFI(인스턴트 파일 초기화) 기능을 지원하지 않습니다.

SQL 서버에는 SSD 스토리지 사용을 권장합니다. SSD 스토리지는 데이터베이스를 포함한 성능이 가장 높고 지연 시간에 민감한 워크로드용으로 설계되었습니다.

Amazon FSx를 사용하여 SQL Server 고가용성 배포의 복잡성과 비용을 줄이는 방법에 대한 자세한 내용은 AWS 스토리지 블로그의 다음 게시물을 참조하십시오.

- Amazon FSx for Windows File Server를 사용하여 Microsoft SQL Server 배포 단순화
- AWS에서의 고가용성 SQL Server 배포를 위한 비용 최적화
- AWS 실행 마법사와 Amazon FSx를 사용한 SQL Server Always On 배포 간소화

Amazon FSx for Active SQL Server 데이터 파일 사용

Microsoft SQL Server는 SMB 파일 공유를 활성 데이터 파일의 스토리지 옵션으로 배포할 수 있습니다. Amazon FSx는 지속적으로 사용 가능한(CA) 파일 공유를 지원하여 SQL Server 데이터베이스용 공유 스토리지 제공에 최적화되었습니다. 이러한 파일 공유는 공유 파일 데이터에 중단 없이 액세스해야 하는 SQL Server와 같은 애플리케이션을 위해 설계되었습니다. 단일 AZ 2 파일 시스템에서도 CA 공유를 생성할 수 있지만, HA 여부 관계없이 모든 SQL Server 배포에는 다중 AZ 파일 시스템에서 CA 공유를 사용해야 합니다.

지속적으로 사용 가능한 공유 만들기

PowerShell에서 원격 관리용 Amazon FSx CLI를 사용하여 지속적으로 사용 가능한(CA) 공유를 생성할 수 있습니다. `-ContinuouslyAvailable` 옵션을 `$True`로 설정한 상태에서 `New-FSxSmbShare` 명령을 사용하여 공유를 지속적으로 사용 가능한 공유로 지정합니다. 새 CA 공유 생성에 대한 자세한 내용은 지속적으로 사용 가능한 (CA) 공유 생성 섹션을 참조하세요.

SMB 타임아웃 설정 구성

FSx for Windows File Server의 장애 조치 프로세스 섹션에 설명된 대로 다중 AZ의 장애 조치 및 페일백으로 I/O 일시 중지가 발생할 수 있지만 일반적으로 30초 이내에 완료됩니다. SQL Server 응용 프로그램은 구성 방식에 따라 시간 초과 설정에 대한 민감도가 다를 수 있습니다.

SMB 클라이언트 구성 세션 제한 시간을 조정하여 애플리케이션이 다중 AZ 파일 시스템 장애 조치에 대한 복원력을 갖도록 할 수 있습니다. 자동 장애 조치 및 페일백을 시작하는 파일 시스템의 처리량 용량을 업데이트하여 장애 조치 중 애플리케이션의 동작을 테스트할 수 있습니다.

Amazon FSx를 이용한 SMB 파일 공유 감시

Windows Server 장애 조치 클러스터 배포 시 일반적으로 클러스터 리소스의 쿼럼을 유지하기 위해 SMB 파일 공유 감시를 배포합니다. 파일 공유 감시에는 쿼럼 정보를 위한 소량의 저장소만 필요합니다. Amazon FSx 파일 시스템은 Windows 서버 장애 조치 클러스터 배포를 위한 SMB 파일 공유 감시로 사용할 수 있습니다.

Amazon Kendra와 함께 FSx for Windows File Server 사용

Amazon Kendra는 매우 정확하고 지능적인 검색 서비스입니다. FSx for Windows File Server 파일 시스템은 Amazon Kendra의 데이터 소스로 사용하여 파일 시스템에 저장된 문서에 포함된 정보를 인덱싱하고 검색할 수 있습니다.

- Amazon Kendra에 대한 자세한 내용은 Amazon Kendra 개발자 안내서의 Amazon Kendra란 무엇인가요? 섹션을 참조하세요.
- 파일 시스템을 Amazon Kendra 데이터 소스로 추가하는 방법에 대한 자세한 내용은 Amazon Kendra 개발자 안내서의 Amazon FSx 데이터 소스 시작하기(콘솔)를 참조하세요.
- Amazon Kendra에 대한 개요 정보는 Amazon Kendra 웹사이트를 참조하세요.
- Amazon Kendra를 사용하여 파일 시스템을 검색하는 방법에 대한 자세한 내용은 AWS 기계 학습 블로그의 Amazon FSx for Windows File Server용 Amazon Kendra 커넥터를 사용하여 Windows 파일 시스템의 비정형 데이터를 안전하게 검색하기를 참조하세요.

파일 시스템 성능

FSx for Windows File Server 파일 시스템을 데이터 소스로 추가하면 Amazon Kendra는 파일 시스템의 파일 및 폴더를 정기적인 동기화 빈도로 크롤링하여 검색 인덱스를 생성하고 유지합니다. (통합을 설정할 때 동기화 빈도를 선택할 수 있습니다.) Amazon Kendra의 이 파일 액세스 활동은 파일 시스템에 액세스하는 자체 워크로드의 활동과 마찬가지로 파일 시스템 리소스를 사용합니다.

파일 시스템이 워크로드 성능에 영향을 미치지 않도록 충분한 리소스로 구성되어 있는지 확인합니다. 특히 많은 수의 파일을 인덱싱할 계획이라면 스토리지 볼륨에 액세스해야 하는 요청에 대해 더 높은 최대 처리량과 IOPS 수준을 제공하는 SSD 스토리지 유형의 파일 시스템을 사용하는 것이 좋습니다.

Amazon FSx 성능 모델에 대한 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

백업, 섀도우 복사본, 예약 복제를 통한 데이터 보호

Amazon FSx는 파일 시스템의 데이터를 자동으로 복제하여 높은 내구성을 보장하는 것 외에도 파일 시스템에 저장된 데이터를 추가로 보호할 수 있는 다음과 같은 옵션을 제공합니다.

- 네이티브 Amazon FSx 백업은 Amazon FSx 내의 백업 보존 및 규정 준수 요구 사항을 지원합니다.
- AWS Backup Amazon FSx 파일 시스템의 백업은 클라우드와 온프레미스의 서비스 AWS 전반에 걸친 중앙 집중식 자동 백업 솔루션의 일부입니다.
- Windows 섀도우 복사본을 사용하면 파일을 이전 버전으로 복원하여 파일 변경을 쉽게 취소하고 파일 버전을 비교할 수 있습니다.
- AWS DataSync Amazon FSx 파일 시스템을 보조 파일 시스템으로 예약 복제하면 데이터 보호 및 복구가 가능합니다.

주제

백업 작업

Amazon FSx를 사용하면 백업의 내구성이 뛰어나고 file-system-consistent 점진적으로 백업할 수 있습니다. 각 백업에는 새 파일 시스템을 생성하는 데 필요한 모든 정보가 포함되어 있어 파일 시스템의 point-in-time 스냅샷을 효과적으로 복원합니다. Amazon FSx는 파일 시스템 일관성을 보장하기 위해 Microsoft Windows의 볼륨 섀도 복사본 서비스(VSS)를 사용합니다. Amazon FSx는 높은 내구성을 보장하기 위해 Amazon Simple Storage Service(Amazon S3)에 백업을 저장합니다.

Amazon FSx 백업은 자동 일일 백업 또는 사용자가 시작한 백업에 관계없이 증분식입니다. 가장 최근의 백업 이후 파일 시스템에서 변경된 데이터만 저장됨을 의미합니다. 그러면 백업을 만드는 데 필요한 시간이 최소화되며 데이터를 복제하지 않으므로 스토리지 비용이 절약됩니다.

백업 프로세스 중 특정 시점에서 스토리지 I/O가 보통 몇 초 정도 잠시 중단될 수 있습니다. VSS 서비스는 I/O를 재개하기 전에 캐시된 모든 쓰기를 디스크로 플러시해야 하므로, 워크로드에 초당 쓰기 작업량(`DataWriteOperations`)이 많으면 일시 중지 시간이 더 길어질 수 있습니다. 대부분의 최종 사용자와 애플리케이션의 I/O 일시 중지는 짧게 발생합니다. 응용 프로그램은 구성 방식에 따라 시간 초과 설정에 대한 민감도가 다를 수 있습니다.

정기적으로 파일 시스템의 백업을 생성하는 것은 Amazon FSx for Windows File Server의 파일 시스템 복제를 보완하는 모범 사례입니다. Amazon FSx 백업은 백업 보존 및 규정 준수 요구 사항을 지원하는 데 도움이 됩니다. Amazon FSx 백업 작업은 백업 생성, 백업 복사, 백업의 파일 시스템 복원, 백업 삭제와 관계없이 쉽습니다. 단일 파일 시스템 백업의 사용량을 보려면 해당 백업의 태그를 활성화하고 태그 기반 결제 보고를 활성화해야 합니다.

주제

자동 일일 백업 작업

기본적으로 Amazon FSx는 파일 시스템을 매일 자동으로 백업합니다. 자동 일일 백업은 파일 시스템을 생성할 때 설정한 일일 백업 기간 중에 발생합니다. 일일 백업 기간을 선택할 때는 하루 중 편리한 시간을 선택하는 것이 좋습니다. 파일 시스템을 사용하는 애플리케이션의 정상 작동 시간을 벗어나는 것이 이상적입니다.

자동 일일 백업은 보존 기간이라고 하는 특정 기간 동안 보관됩니다. Amazon FSx 콘솔에서 파일 시스템을 생성할 때 자동 일일 백업의 기본 보존 기간은 30일입니다. 기본 보존 기간은 Amazon FSx API 및 CLI에서 다릅니다. 백업 보존 기간은 0~90일로 설정할 수 있습니다. 보존 기간을 0일로 설정하면 자동 일일 백업이 꺼집니다. 파일 시스템이 삭제되면 자동 일일 백업도 삭제됩니다.

> **Note**
>
> 보존 기간을 0일로 설정하면 파일 시스템이 자동으로 백업되지 않습니다. 어떤 수준이든 중요 기능이 관련된 파일 시스템에 대해서는 자동 일일 백업을 사용하는 것이 좋습니다.

AWS SDK AWS CLI 또는 둘 중 하나를 사용하여 파일 시스템의 백업 기간과 백업 보존 기간을 변경할 수 있습니다. `UpdateFileSystem` API 작업 또는 `update-file-system` CLI 명령을 사용합니다. 자세한 설명은 연습 3: 기존 파일 시스템 업데이트 섹션을 참조하세요.

사용자 시작 백업 작업

Amazon FSx로 파일 시스템을 언제든지 수동으로 백업할 수 있습니다. Amazon FSx 콘솔, API 또는 AWS Command Line Interface () 를 사용하여 이 작업을 수행할 수 있습니다.AWS CLI사용자가 시작한 Amazon FSx 파일 시스템 백업은 절대 만료되지 않으며, 원하는 시간만큼 유지할 수 있습니다. 사용자가 시작한 백업은 백업된 파일 시스템을 삭제한 후에도 보존됩니다. 사용자가 시작한 백업은 Amazon FSx 콘솔, API 또는 CLI를 사용해야만 삭제할 수 있습니다. Amazon FSx는 사용자 시작 백업을 자동으로 삭제하지 않습니다. 자세한 설명은 백업 삭제 섹션을 참조하세요.

파일 시스템이 수정되고 있을 때(처리량 용량 업데이트, 파일 시스템 유지 관리 등) 백업을 시작하는 경우, 백업 요청은 대기열에 있다가 수정 작업이 완료되면 재개됩니다.

사용자 시작 백업 생성

다음 절차는 Amazon FSx 콘솔에서 기존 파일 시스템의 사용자 시작 백업을 생성하는 방법을 안내합니다.

파일 시스템의 사용자 시작 백업 생성

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 콘솔 대시보드에서 백업하려는 파일 시스템의 이름을 선택합니다.
3. 작업에서 백업 생성을 선택합니다.
4. 열리는 백업 생성 대화 상자에서 백업 이름을 입력합니다. 백업 이름은 문자, 공백, 숫자 및 특수 문자 + - = _:/를 포함한 최대 256자의 유니코드 문자입니다.
5. 백업 생성을 선택합니다.

이제 파일 시스템 백업을 생성했습니다. 왼쪽 탐색 메뉴에서 백업을 선택하여 Amazon FSx 콘솔의 모든 백업 테이블을 확인할 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.

아마존 AWS Backup FSx와 함께 사용

AWS Backup Amazon FSx 파일 시스템을 백업하여 데이터를 보호하는 간단하고 비용 효율적인 방법입니다. AWS Backup 는 백업의 생성, 복사, 복원 및 삭제를 단순화하는 동시에 향상된 보고 및 감사를

제공하도록 설계된 통합 백업 서비스입니다. AWS Backup 법률, 규정 및 전문 규정 준수를 위한 중앙 집중식 백업 전략을 보다 쉽게 개발할 수 있습니다. AWS Backup 또한 다음을 수행할 수 있는 중앙 위치를 제공하여 AWS 스토리지 볼륨, 데이터베이스 및 파일 시스템을 더 간단하게 보호할 수 있습니다.

- 백업하려는 AWS 리소스를 구성하고 감사하십시오.
- 백업 예약을 자동화합니다.
- 보존 정책을 설정합니다.
- AWS 지역 간 및 AWS 계정 간에 백업을 복사합니다.
- 최근의 모든 백업, 복사 및 복원 활동을 모니터링합니다.

AWS Backup Amazon FSx의 내장된 백업 기능을 사용합니다. AWS Backup 콘솔에서 생성한 백업은 Amazon FSx 콘솔을 통해 생성된 백업과 동일한 수준의 파일 시스템 일관성과 성능, 동일한 복원 옵션을 제공합니다. 에서 생성된 AWS Backup 백업은 사용자가 생성한 다른 Amazon FSx 백업에 비해 사용자 시작 또는 자동 백업에 비해 증분 백업입니다.

를 AWS Backup 사용하여 이러한 백업을 관리하면 무제한 보존 옵션과 1시간마다 예약 백업을 생성할 수 있는 기능과 같은 추가 기능을 이용할 수 있습니다. 또한 소스 파일 시스템이 AWS Backup 삭제된 후에도 변경할 수 없는 백업을 보존합니다. 이렇게 하면 실수로 삭제되거나 악의적으로 삭제되는 것을 방지할 수 있습니다.

에서 수행한 AWS Backup 백업은 사용자가 시작한 백업으로 간주되며 Amazon FSx의 사용자 시작 백업 할당량에 포함됩니다. Amazon FSx 콘솔, CLI 및 AWS Backup API에서 만든 백업을 보고 복원할 수 있습니다. 하지만 Amazon FSx 콘솔, CLI 또는 AWS Backup API에서 만든 백업은 삭제할 수 없습니다. Amazon FSx 파일 시스템을 AWS Backup 백업하는 데 사용하는 방법에 대한 자세한 내용은 개발자 안내서의 Amazon FSx 파일 시스템 사용을 참조하십시오.AWS Backup

백업 복사

Amazon FSx를 사용하여 AWS 동일한 계정 내의 백업을 AWS 다른 지역 (지역 간 사본) 또는 동일한 지역 내 (지역 내 사본) 에 AWS 수동으로 복사할 수 있습니다. 동일한 파티션 내에서만 지역 간 사본을 만들 수 있습니다. AWS Amazon FSx 콘솔 또는 API를 사용하여 사용자가 시작한 백업 사본을 생성할 수 있습니다. AWS CLI사용자 시작 백업 사본에는 다음과 같이 `USER_INITIATED` 유형이 있습니다.

또한 를 사용하여 AWS 지역 간 및 계정 간에 백업을 AWS Backup 복사할 수 있습니다. AWS AWS Backup 정책 기반 백업 계획을 위한 중앙 인터페이스를 제공하는 완전 관리형 백업 관리 서비스입니다. 교차 계정 관리를 사용하면, 백업 정책을 사용하여 조직 내의 계정 전체에 걸쳐 백업 계획을 자동으로 적용할 수 있습니다.

크로스 리전 백업 복사본은 크로스 리전 재해 복구에 특히 유용합니다. 백업을 만들어 다른 AWS 지역으로 복사하면 주 지역에 재해가 발생할 경우 다른 AWS AWS 지역의 백업 및 복구 가용성을 신속하게 복원할 수 있습니다. 백업 복사본을 사용하여 파일 데이터세트를 다른 AWS 지역이나 같은 AWS 지역 내에 복제할 수도 있습니다. Amazon FSx 콘솔 또는 Amazon FSx API를 사용하여 동일한 AWS 계정 (지역 간 또는 지역 내) 내에서 백업 사본을 만들 수 있습니다. AWS CLI또한 AWS Backup으로 온디맨드 또는 정책 기반으로 백업 복사를 수행하는 데에도 사용할 수 있습니다.

계정 간 백업 복사는 격리된 계정에 백업을 복사할 때 규정 준수 요구 사항을 충족하는 데 유용합니다. 또한 우발적 또는 악의적인 백업 삭제, 자격 증명 손실 또는 키 손상을 방지하는 데 도움이 되는 추가 데이터 보호 계층을 제공합니다. AWS KMS 교차 계정 백업은 팬인(여러 기본 계정의 백업을 하나의 격리된 백업 사본 계정으로 복사) 및 팬아웃(하나의 기본 계정에서 여러 격리된 백업 사본 계정으로 백업 복사)을 지원합니다.

지원 부서와 AWS Backup 함께 AWS Organizations 사용하면 계정 간 백업 복사본을 만들 수 있습니다. 계정 간 복사본의 계정 한도는 정책에 따라 AWS Organizations 정의됩니다. 계정 간 백업 복사본을 만드는 AWS Backup 데 사용하는 방법에 대한 자세한 내용은 AWS Backup 개발자 안내서의 백업 복사본 만들기를 참조하세요. AWS 계정

백업 사본 제한 사항

다음은 백업을 복사할 때 적용되는 몇몇 제한 사항입니다.

- 지역 간 백업 복사본은 두 상업 AWS 지역 간, 중국 (베이징) 과 중국 (닝샤) 지역 간, (미국 동부) 및 AWS GovCloud AWS GovCloud (미국 서부) 지역 간에만 지원되며 해당 지역 간에는 지원되지 않습니다.
- 크로스 리전 백업 복사본은 옵트인 리전에서 지원되지 않습니다.
- 모든 지역 내에서 지역 내 백업 복사본을 만들 수 있습니다. AWS
- 원본 백업이 `AVAILABLE` 상태여야만 복사할 수 있습니다.
- 복사 중인 소스 백업은 삭제할 수 없습니다. 대상 백업을 사용할 수 있게 되는 시점과 소스 백업을 삭제할 수 있는 시점 사이에는 약간의 지연이 있을 수 있습니다. 소스 백업을 다시 삭제하려고 할 때는 지연을 염두에 두어야 합니다.
- 계정당 단일 대상 AWS 지역으로 최대 5개의 백업 사본 요청을 진행할 수 있습니다.

크로스 리전 백업 복사본 권한

IAM 정책 설명을 사용하여 백업 복사 작업을 수행할 권한을 부여합니다. 소스 AWS 리전과 통신하여 리전 간 백업 사본을 요청하려면 요청자 (IAM 역할 또는 IAM 사용자) 가 소스 백업 및 소스 리전에 액세스할 수 있어야 합니다. AWS

정책을 사용하여 백업 복사 작업에 대한 `CopyBackup` 작업 권한을 부여합니다. 다음 예제와 같이 정책의 `Action` 필드에서 작업을 지정하고, 정책의 `Resource` 필드에서 리소스 값을 지정합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "fsx:CopyBackup",
            "Resource": "arn:aws:fsx:*:111111111111:backup/*"
        }
    ]
}
```

IAM 정책에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 정책 및 권한을 참조하세요.

전체 및 증분 복사

원본 백업과 다른 대상 AWS 지역 또는 대상 AWS 계정에 백업을 복사하는 경우 동일한 KMS 키를 사용하여 백업의 원본 및 대상 복사본을 모두 암호화하더라도 첫 번째 복사본은 전체 백업 사본입니다.

해당 지역에서 이전에 복사한 백업을 모두 삭제하지 않고 동일한 키를 사용한 경우 첫 번째 백업 복사본 이후 동일한 AWS 계정 내의 동일한 대상 지역에 대한 모든 후속 백업 사본은 증분 복사본이 됩니다. AWS KMS 두 조건 중 하나라도 충족되지 않은 상태에서 복사 작업을 수행하면 증분이 아닌 전체 백업 사본이 생성됩니다.

콘솔을 사용하여 동일한 계정(크로스 리전 또는 리전 내) 내에서 백업 복사

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 탐색 창에서 백업을 선택합니다.
3. 백업 테이블에서 복사할 백업을 선택한 다음 백업 복사를 선택합니다.
4. 설정 섹션에서 다음을 수행합니다.

- 대상 지역 목록에서 백업을 복사할 대상 AWS 지역을 선택합니다. 대상은 다른 지역에 있을 수도 있고 (AWS 지역 간 복사) 같은 지역 내에 있을 수도 있고 (AWS 지역 내 복사) 내에 있을 수도 있습니다.
- (선택 사항) 소스 백업에서 대상 백업으로 태그를 복사하려면 태그 복사를 선택합니다. 6단계에서 태그 복사를 선택하고 태그도 추가하면 모든 태그가 병합됩니다.

5. 암호화에서는 복사한 백업을 암호화하는 데 사용할 AWS KMS 암호화 키를 선택합니다.
6. 태그 - 선택 사항의 경우 키와 값을 입력하여 태그를 복사된 백업에 추가합니다. 여기에 태그를 추가하고 4단계에서 태그 복사를 선택하면 모든 태그가 병합됩니다.
7. 백업 복사를 선택합니다.

백업은 동일한 AWS 계정 내에서 선택한 AWS 지역에 복사됩니다.

CLI를 사용하여 동일한 계정(크로스 리전 또는 리전 내) 내에서 백업 복사

- `copy-backup`CLI 명령 또는 CopyBackupAPI 작업을 사용하여 리전 또는 AWS 리전 내에서 동일한 AWS 계정 내에서 백업을 복사합니다. AWS

  다음 명령은 `us-east-1` 리전에서 ID가 `backup-0abc123456789cba7`인 백업을 복사합니다.

  ```
  aws fsx copy-backup \
    --source-backup-id backup-0abc123456789cba7 \
    --source-region us-east-1
  ```

  응답에는 복사된 백업의 설명이 표시됩니다.

  Amazon FSx 콘솔에서 또는 CLI 명령 또는 API 작업을 사용하여 `describe-backups` 프로그래밍 방식으로 백업을 볼 수 있습니다. DescribeBackups

백업 복원

사용 가능한 백업을 사용하여 새 파일 시스템을 생성하여 다른 파일 시스템의 point-in-time 스냅샷을 효과적으로 복원할 수 있습니다. 콘솔 또는 AWS SDK 중 하나를 사용하여 백업을 복원할 수 있습니다. AWS CLI백업을 새 파일 시스템으로 복원하는 데는 새 파일 시스템을 만드는 시간과 동일한 시간이 걸립니다. 백업에서 복원된 데이터는 파일 시스템에 지연 로드되고, 로딩되는 동안 지연 시간이 약간 더 길어집니다.

사용자가 복원된 파일 시스템에 계속 액세스할 수 있도록 하려면 복원된 파일 시스템과 연결된 Active Directory 도메인이 원래 파일 시스템의 Active Directory 도메인과 동일한지, 또는 원래 파일 시스템의 AD 도메인이 신뢰하는지 확인하세요. Microsoft Active Directory에 대한 자세한 내용은 FSx for Windows File Server에서 Microsoft Active Directory 작업 섹션을 참조하세요.

다음 절차는 콘솔을 사용하여 백업을 복원하고 새 파일 시스템을 만드는 방법을 안내합니다.

> **Note**
>
> 백업은 배포 유형과 스토리지 용량이 원본과 같은 파일 시스템에만 복원할 수 있습니다. 복원된 파일 시스템이 사용할 수 있는 상태가 되면 파일 시스템의 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.

백업에서 파일 시스템 복원

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 콘솔 대시보드의 왼쪽 탐색 메뉴에서 백업을 선택합니다.
3. 백업 테이블에서 복원할 백업을 선택한 다음 백업 복원을 선택합니다.

   그러면 파일 시스템 생성 마법사가 열립니다. 생성 마법사는 배포 유형과 스토리지 용량이 이미 설정되어 있고 변경할 수 없다는 점을 제외하면 표준 파일 시스템 생성 마법사와 동일합니다. 하지만 처리량 용량, 관련 VPC, 기타 설정, 스토리지 유형은 변경할 수 있습니다. 스토리지 유형은 기본적으로 SSD로 설정되지만, 다음 조건에서는 HDD로 변경할 수 있습니다.

   - 파일 시스템 배포 유형은 다중 AZ 또는 단일 AZ 2입니다.
   - 스토리지 용량이 2,000GiB 이상.
4. 새 파일 시스템을 생성할 때와 마찬가지로 마법사를 완료합니다.
5. 검토 및 생성을 선택합니다.
6. Amazon FSx 파일 시스템의 선택한 설정을 검토한 다음 파일 시스템 생성을 선택합니다.

백업에서 복원하여 이제 새 파일 시스템이 생성됩니다. 파일 시스템이 `AVAILABLE` 상태로 변경되면 정상적으로 사용할 수 있습니다.

백업 삭제

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. 유형이AWS 백업인 에서 수행한 AWS Backup백업은 Amazon FSx 콘솔, CLI 또는 API에서 삭제할 수 없습니다.

백업 삭제

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. 열린 백업 삭제 대화 상자에서 백업 ID가 삭제하려는 백업을 식별하는지 확인합니다.
5. 삭제할 백업의 확인란이 선택되어 있는지 확인합니다.
6. 백업 삭제를 선택합니다.

이제 백업과 포함된 모든 데이터가 영구적으로 삭제되어 복구할 수 없습니다.

백업 크기

백업 크기는 프로비저닝된 총 스토리지 용량이 아닌 파일 시스템의 사용된 스토리지를 사용하여 결정됩니다. 백업 크기는 사용된 스토리지 용량과 파일 시스템의 데이터 변동량에 따라 달라집니다. 파일 시스템의 스토리지 볼륨 전체에 데이터가 분산되는 방식과 변경 빈도에 따라 총 백업 사용량은 사용된 스토리지 용량보다 크거나 작을 수 있습니다. 백업을 삭제하면 해당 백업의 고유한 데이터만 제거됩니다. Amazon FSx를 사용하면 중복 제거 및 압축으로 인한 스토리지 효율성 확보 효과가 기본 SSD/HDD 스토리지뿐만 아니라 백업에도 적용됩니다.

안정적이고 증분적인 백업을 제공하기 file-system-consistent 위해 Amazon FSx는 블록 수준에서 데이터를 백업합니다. 파일 시스템의 스토리지 볼륨에 있는 데이터는 데이터를 쓰거나 덮어쓴 패턴에 따라 여러 블록에 걸쳐 저장될 수 있습니다. 따라서 총 백업 사용량이 파일 시스템에 있는 파일 및 디렉토리의 정확한 크기와 일치하지 않을 수 있습니다.

전체 백업 사용량 및 비용은 대시보드 또는 에서 확인할 수 있습니다. AWS Billing AWS Cost Management Console개별 파일 시스템 백업의 크기와 비용을 계산하려면 개별 백업에 태그를 지정하고 태그 기반 결제 보고를 활성화하면 됩니다.

섀도우 복사본으로 데이터 보호

Microsoft Windows 섀도우 복사본은 특정 시점의 Windows 파일 시스템 스냅샷입니다. 섀도 복사본을 활성화하면 사용자는 네트워크에 저장된 삭제되거나 변경된 파일을 신속하게 복구하고 파일 버전을 비교할 수 있습니다. 스토리지 관리자는 Windows PowerShell 명령을 사용하여 섀도우 복제본이 주기적으로 생성되도록 쉽게 스케줄을 지정할 수 있습니다.

섀도 복사본은 파일 시스템의 데이터와 함께 저장되며 파일의 변경된 부분에 대해서만 파일 시스템 스토리지 용량을 소비합니다. 파일 시스템에 저장된 모든 섀도 복사본은 파일 시스템 백업에 포함됩니다.

> **Note**
>
> FSx for Windows File Server에서는 기본적으로 섀도우 복사본이 활성화되지 않습니다. 섀도 복사본을 사용하여 파일 시스템의 데이터를 보호하려면 섀도 복사본을 활성화하고 파일 시스템에 섀도 복사본 일정을 설정해야 합니다. 자세한 정보는 기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다.을 참조하세요.

> **Warning**
>
> 섀도우 복사본은 백업을 대체할 수 없습니다. 섀도우 복사본을 활성화한 경우 정기적인 백업을 계속 수행해야 합니다.

주제

- 섀도우 복사본 일정 삭제
- 섀도우 복사본 생성
- 기존 섀도우 복사본 보기
- 섀도우 복사본 삭제

섀도우 복사본 사용 모범 사례

파일 시스템의 섀도우 복사본을 사용하면 최종 사용자가 Windows 파일 탐색기의 이전 스냅샷에서 개별 파일 또는 폴더를 보고 복원할 수 있습니다. Amazon FSx는 Microsoft Windows Server에서 제공하는 섀도우 복사본 기능을 사용합니다. 섀도우 복사본의 경우 다음 모범 사례를 사용합니다.

- 파일 시스템에 충분한 성능 리소스가 있는지 확인: Microsoft Windows는 설계상 가장 최근의 섀도 복제본 시점 이후의 변경 내용을 기록하는 copy-on-write 방법을 사용하며, 이 copy-on-write 활동으로 인해 모든 파일 쓰기 작업에 대해 최대 세 번의 I/O 작업이 발생할 수 있습니다.
- SSD 스토리지 사용 및 처리량 용량 증가: Windows에서 섀도우 복사본을 유지하려면 높은 수준의 I/O 성능이 필요하므로 SSD 스토리지를 사용하고 예상 워크로드의 최대 3배까지 처리량 용량을 늘리는 것이 좋습니다. 이렇게 하면 파일 시스템에 충분한 리소스가 확보되어 원치 않는 섀도우 복사본 삭제와 같은 문제를 방지할 수 있습니다.
- 필요한 섀도우 복사본 수만 유지: 섀도우 복사본이 많은 경우(예: 가장 최근의 섀도우 복사본 64개 이상) 또는 단일 파일 시스템에서 많은 양의 스토리지(TB 규모)를 차지하는 섀도우 복사본이 있는 경우 장애 조치 및 페일백 등의 프로세스에 시간이 더 걸릴 수 있습니다. 이는 FSx for Windows에서 섀도우 복사본 스토리지에서 일관성 검사를 실행해야 하기 때문입니다. 또한 Windows용 FSx가 섀도우 복사본을 유지 관리하면서 작업을 copy-on-write 수행해야 하기 때문에 I/O 작업 지연 시간이 길어질 수 있습니다. 섀도우 복사본으로 인한 가용성 및 성능 영향을 최소화하려면 사용하지 않는 섀도우 복사본을 수동으로 삭제하거나 파일 시스템에서 오래된 섀도우 복사본을 자동으로 삭제하도록 스크립트를 구성합니다.

> **Note**
>
> 다중 AZ 파일 시스템의 장애 조치 이벤트 중에 FSx for Windows는 새 활성 파일 서버가 온라인 상태가 되기 전에 파일 시스템의 섀도우 복사본 스토리지를 스캔해야 하는 정합성 검사를 실행합니다. 일관성 검사 기간은 파일 시스템의 섀도우 복사본 수 및 사용된 스토리지와 관련이 있습니다. 지연된 장애 조치 및 페일백 이벤트를 방지하려면 파일 시스템에 64개 미만의 섀도우 복사본을 유지하고 아래 단계에 따라 가장 오래된 섀도우 복사본을 정기적으로 모니터링하여 삭제하는 것이 좋습니다.

섀도우 복사본 설정

Amazon FSx에서 정의한 Windows PowerShell 명령을 사용하여 파일 시스템에서 주기적인 섀도 복사를 활성화하고 스케줄링할 수 있습니다. 다음은 Windows File Server용 FSx 파일 시스템에서 섀도 복제본을 구성할 때의 세 가지 기본 설정입니다.

- 섀도 복사본이 파일 시스템에서 사용할 수 있는 최대 스토리지 용량 설정
- (선택 사항) 파일 시스템에 저장할 수 있는 섀도 복사본의 최대 수를 설정합니다. 기본값은 20입니다.
- (선택 사항) 섀도 복제본을 생성하는 시간 및 간격 (예: 매일, 매주, 매월) 을 정의하는 스케줄 설정

언제든지 파일 시스템당 최대 500개의 섀도 복사본을 저장할 수 있지만 가용성과 성능을 보장하기 위해 항상 64개 미만의 섀도 복사본을 유지하는 것이 좋습니다. 이 한도에 도달하면 다음에 생성하는 섀도우 복사본이 가장 오래된 섀도우 복사본을 대체합니다. 마찬가지로 섀도우 복사본 최대 저장 용량에 도달하면 가장 오래된 섀도우 복사본 중 하나 이상이 삭제되어 다음 섀도우 복사본을 위한 충분한 저장 공간을 확보합니다.

기본 Amazon FSx 설정을 사용하여 주기적인 섀도우 복사본을 신속하게 활성화하고 스케줄링하는 방법에 대한 자세한 내용은 기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다. 섹션을 참조하세요.

섀도우 복사본 스토리지 할당 고려 사항

섀도우 복사본은 마지막 섀도우 복사본 이후에 이루어진 파일 변경 사항의 블록 수준 복사본입니다. 전체 파일은 복사되지 않고 변경 내용만 복사됩니다. 따라서 이전 버전의 파일은 일반적으로 현재 파일만큼 많은 저장 공간을 차지하지 않습니다. 변경에 사용되는 볼륨 공간은 워크로드에 따라 달라질 수 있습니다. 파일이 수정될 때 섀도우 복사본이 사용하는 스토리지 공간은 워크로드에 따라 달라집니다. 섀도우 복사본에 할당할 스토리지 공간을 결정할 때는 워크로드의 파일 시스템 사용 패턴을 고려해야 합니다.

섀도우 복사본을 활성화하면 섀도우 복사본이 파일 시스템에서 사용할 수 있는 최대 스토리지 양을 지정할 수 있습니다. 기본 제한은 파일 시스템의 10%입니다. 사용자가 파일을 자주 추가하거나 수정하는 경우 제한을 늘리는 것이 좋습니다. 제한을 너무 작게 설정하면 가장 오래된 섀도우 복사본이 사용자가 예상하는 것보다 더 자주 삭제될 수 있습니다.

섀도우 복사본 스토리지를 언바운드(`Set-FsxShadowStorage -Maxsize "UNBOUNDED"`)로 설정할 수 있습니다. 그러나 무제한 구성으로 인해 많은 수의 섀도우 복사본이 파일 시스템 스토리지를 소비하게 될 수 있습니다. 이로 인해 워크로드를 위한 스토리지 용량이 충분하지 않을 수 있습니다. 무제

한 스토리지를 설정하는 경우 섀도우 복사본 한도에 도달했을 때 스토리지 용량을 확장해야 합니다. 섀도우 복사본 스토리지를 특정 크기로 구성하거나 제한되지 않은 스토리지로 구성하는 방법에 대한 자세한 내용은 섀도 복사본 스토리지의 최대 용량 설정 섹션을 참조하세요.

섀도우 복사본을 활성화한 후 섀도우 복사본이 소비하는 스토리지 공간을 모니터링할 수 있습니다. 자세한 정보는 섀도우 복사본 스토리지 보기을 참조하세요.

섀도 복사본의 최대 수를 설정할 때의 고려 사항

섀도 복사본을 활성화하면 파일 시스템에 저장되는 섀도 복사본의 최대 수를 지정할 수 있습니다. 기본 제한은 20개이며, 섀도 복사본으로 인한 가용성 및 성능 영향을 최소화하기 위해 Microsoft는 섀도 복사본의 최대 수를 64개 미만으로 구성할 것을 권장합니다. Windows에서 섀도 복사본을 유지 관리하려면 높은 수준의 I/O 성능이 필요하므로 SSD 스토리지를 사용하고 처리 용량을 예상 워크로드의 최대 3배까지 늘리는 것이 좋습니다. 이렇게 하면 파일 시스템에 충분한 리소스가 확보되어 원치 않는 섀도우 복사본 삭제와 같은 문제를 방지할 수 있습니다.

섀도 복사본의 최대 수를 500개까지 설정할 수 있습니다. 그러나 단일 파일 시스템에서 많은 양의 스토리지 (TB 규모) 를 차지하는 섀도 복사본 또는 섀도 복사본이 많은 경우 페일오버 및 페일백 등의 프로세스가 예상보다 오래 걸릴 수 있습니다. 이는 Windows에서 섀도 복사본 저장소에 대해 일관성 검사를 실행해야 하기 때문입니다. 또한 Windows에서 섀도우 복사본을 유지 관리하면서 작업을 수행해야 copy-on-write 하기 때문에 I/O 작업 지연 시간이 길어질 수 있습니다.

섀도우 복사본에 대한 파일 시스템 권장 사항

다음은 섀도우 복사본을 사용하기 위한 파일 시스템 권장 사항입니다.

- 파일 시스템의 워크로드 요구 사항에 맞는 충분한 성능 용량을 프로비저닝해야 합니다. Amazon FSx는 Microsoft Windows Server에서 제공하는 섀도우 복사본 기능을 제공합니다. Microsoft Windows는 설계상 가장 최근의 섀도 복제본 시점 이후의 변경 내용을 기록하는 copy-on-write 방법을 사용하며, 이 copy-on-write 작업으로 인해 모든 파일 쓰기 작업에 대해 최대 세 번의 I/O 작업이 발생할 수 있습니다. Windows가 초당 들어오는 I/O 작업 속도를 따라가지 못하면 를 통해 섀도 복사본을 더 이상 유지할 수 없으므로 모든 섀도 복사본이 삭제될 수 copy-on-write 있습니다. 따라서 파일 시스템의 워크로드 요구 사항에 맞게 충분한 I/O 성능 용량을 프로비저닝하는 것이 중요합니다(파일 서버 I/O 성능을 결정하는 처리 용량 차원과 스토리지 I/O 성능을 결정하는 스토리지 유형 및 용량 모두).
- Windows가 섀도우 복사본을 유지 관리하는 데 더 높은 I/O 성능을 소비하고 HDD 스토리지가 I/O 작업에 더 낮은 성능 용량을 제공한다는 점을 고려하면 일반적으로 섀도우 복사본을 활성화할 때는 HDD 스토리지 대신 SSD 스토리지로 구성된 파일 시스템을 사용하는 것이 좋습니다.

- 파일 시스템에 구성된 최대 섀도우 복사본 스토리지 용량 외에 최소 320MB의 여유 공간이 있어야 합니다(MaxSpace). 예를 들어 섀도우 복사본에 5GB MaxSpace를 할당한 경우 파일 시스템에는 5GB MaxSpace 외에 항상 320MB 이상의 여유 공간이 있어야 합니다.

> **Warning**
>
> 섀도우 복사본 일정을 구성할 때는 데이터를 마이그레이션하거나 데이터 중복 제거 작업이 실행되도록 예약할 때 섀도우 복사본을 예약하지 않도록 하십시오. 파일 시스템이 유휴 상태일 것으로 예상될 때 섀도우 복사본 일정을 만들어야 합니다. 섀도우 복사본 일정을 사용자 지정하는 방법은 사용자 지정 섀도우 복사본 일정 생성 섹션을 참조하세요.

기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다.

기본 섀도 복사본 저장소 설정 및 일정을 사용하여 파일 시스템에 섀도 복사본을 빠르게 설정할 수 있습니다. 기본 섀도 복사본 저장소 설정을 사용하면 섀도 복사본이 파일 시스템 스토리지 용량의 최대 10% 를 차지할 수 있습니다. 파일 시스템의 스토리지 용량을 늘려도 현재 할당된 섀도 복사본 스토리지의 양은 비슷하게 증가하지 않습니다.

기본 스케줄은 매주 월요일, 화요일, 수요일, 목요일, 금요일 오전 7시와 오후 12시(UTC)에 섀도우 복사본을 자동으로 생성합니다.

섀도우 복사본 스토리지의 기본 수준 설정

1. 파일 시스템과 네트워크로 연결된 Windows 컴퓨팅 인스턴스에 연결합니다.
2. 파일 시스템 관리자 그룹의 구성원으로 Windows 컴퓨팅 인스턴스에 로그인합니다. 에서 AWS Managed Microsoft AD해당 그룹은 AWS 위임된 FSx 관리자입니다. 자체 관리형 Microsoft AD에서 해당 그룹은 파일 시스템을 생성할 때 관리를 위해 지정한 도메인 관리자 또는 사용자 지정 그룹입니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 다음 명령을 사용하여 섀도우 스토리지의 기본 용량을 설정합니다. 관리하려는 파일 시스템의 Windows 원격 *FSxFileSystem-Remote-PowerShell-Endpoint* PowerShell 엔드포인트로 대체하십시오. Amazon FSx 콘솔, 파일 시스템 세부 정보 화면의 네트워크 및 보안 섹션 또는 API 작업의 DescribeFileSystem 응답에서 Windows Remote PowerShell 엔드포인트를 찾을 수 있습니다.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowStorage -Default}
```

그 응답은 다음과 같습니다.

```
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 10737418240                  20
```

기본 섀도 복사 일정을 설정하려면

1. 파일 시스템과 네트워크로 연결된 Windows 컴퓨팅 인스턴스에 연결합니다.
2. 파일 시스템 관리자 그룹의 구성원으로 Windows 컴퓨팅 인스턴스에 로그인합니다. 에서 AWS Managed Microsoft AD해당 그룹은 AWS 위임된 FSx 관리자입니다. 자체 관리형 Microsoft AD에서 해당 그룹은 파일 시스템을 생성할 때 관리를 위해 지정한 도메인 관리자 또는 사용자 지정 그룹입니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 다음 명령을 사용하여 기본 섀도우 복사 일정을 설정합니다.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName FSxFileSystem-Remote-
PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {Set-
FsxShadowCopySchedule -Default}
```

응답에는 현재 설정된 기본 일정이 표시됩니다.

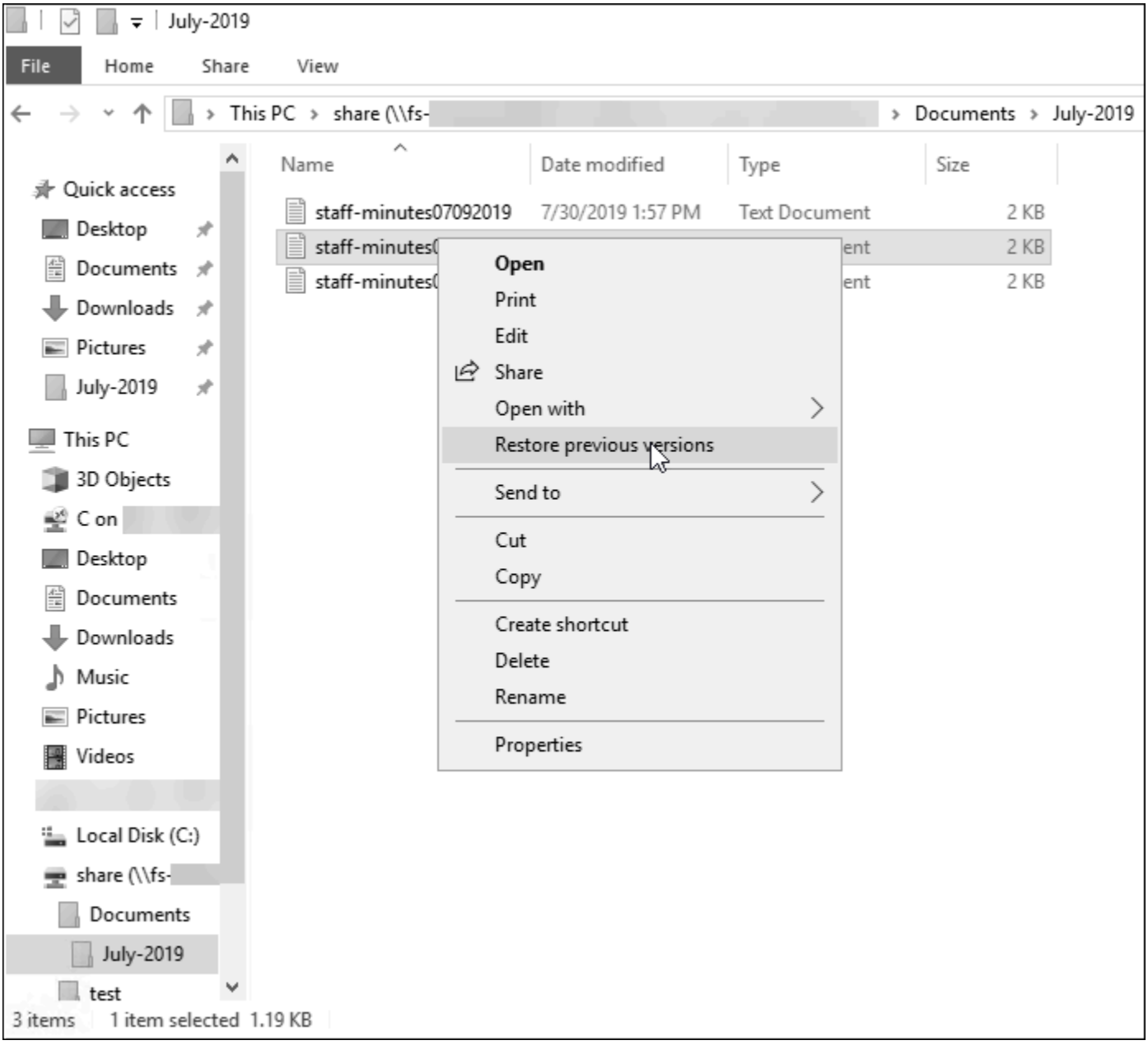
```
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday              1
```

추가 옵션 및 사용자 지정 섀도우 복사본 일정 생성에 대한 자세한 내용은 사용자 지정 섀도우 복사본 일정 생성 섹션을 참조하세요.

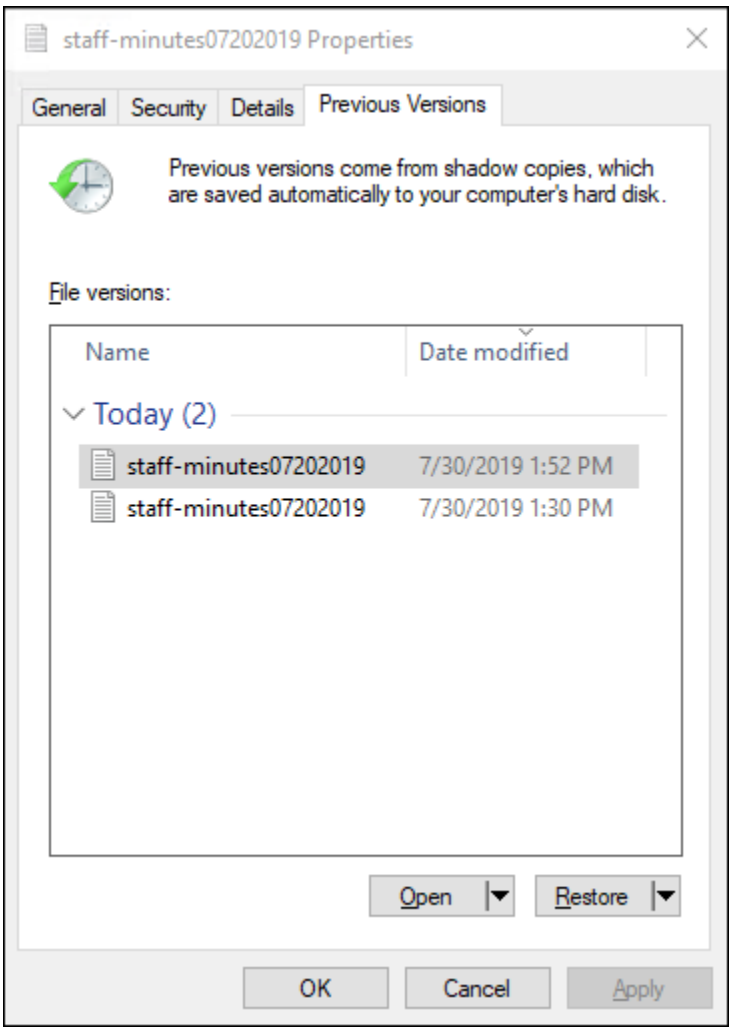
개별 파일 및 폴더 복원

Amazon FSx 파일 시스템에서 섀도 복사본을 구성하면 사용자가 개별 파일 또는 폴더의 이전 버전을 신속하게 복원하고 삭제된 파일을 복구할 수 있습니다.

사용자는 익숙한 Windows 파일 탐색기 인터페이스를 사용하여 파일을 이전 버전으로 복원할 수 있습니다. 파일을 복원하려면 복원할 파일을 선택한 다음 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴에서 이전 버전 복원을 선택하세요.



그러면 사용자는 이전 버전 목록에서 이전 버전을 보고 복원할 수 있습니다.



섀도 복사본 스토리지의 최대 용량 설정

`Set-FsxShadowStorage`사용자 지정 PowerShell 명령을 사용하여 파일 시스템에서 섀도 복사본이 사용할 수 있는 최대 스토리지 양을 정의합니다. `-Maxsize`또는 `-Default` 매개 변수를 사용하여 섀도 복사본을 늘릴 수 있는 최대 크기를 지정할 수 있습니다. 를 사용하면 파일 시스템 스토리지 용량의 최대 10% 가 `Default` 설정됩니다. `-Maxsize`및 `-Default` 매개 변수는 동일한 명령에 지정할 수 없습니다.

`-Maxsize`를 사용하여 다음과 같이 섀도우 복사본 스토리지를 정의할 수 있습니다.

- 바이트 단위: `Set-FsxShadowStorage -Maxsize 2500000000`
- 킬로바이트, 메가바이트, 기가바이트 또는 기타 단위: `Set-FsxShadowStorage -Maxsize (2500MB)` 또는 `Set-FsxShadowStorage -Maxsize (2.5GB)`
- 전체 스토리지의 백분율: `Set-FsxShadowStorage -Maxsize "20%"`

- 무제한: `Set-FsxShadowStorage -Maxsize "UNBOUNDED"`

`-Default`를 사용하여 파일 시스템의 최대 10%를 사용하도록 섀도우 스토리지를 설정하려면 `Set-FsxShadowStorage -Default`로 설정합니다. 기본 옵션 사용에 대한 자세한 내용은 기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다. 섹션을 참조하세요.

FSx for Windows File Server 파일 시스템에서 섀도우 복사본 스토리지 용량 설정

1. 파일 시스템 관리자 그룹의 구성원인 사용자로 파일 시스템과 네트워크 연결이 가능한 컴퓨팅 인스턴스에 연결합니다. 에서 AWS Managed Microsoft AD해당 그룹은 AWS 위임된 FSx 관리자입니다. 자체 관리형 Microsoft AD에서 해당 그룹은 파일 시스템을 생성할 때 관리를 위해 지정한 도메인 관리자 또는 사용자 지정 그룹입니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
2. 컴퓨팅 인스턴스에서 Windows PowerShell 창을 엽니다.
3. 다음 명령을 사용하여 Amazon FSx 파일 시스템에서 원격 PowerShell 세션을 엽니다. 관리하려는 파일 시스템의 Windows 원격 *FSxFileSystem-Remote-PowerShell-Endpoint* PowerShell 엔드포인트로 대체하십시오. Amazon FSx 콘솔, 파일 시스템 세부 정보 화면의 네트워크 및 보안 섹션 또는 API 작업의 `DescribeFileSystem` 응답에서 Windows Remote PowerShell 엔드포인트를 찾을 수 있습니다.

```
PS C:\Users\delegateadmin> enter-pssession -computername FSxFileSystem-Remote-
PowerShell-Endpoint -configurationname fsxremoteadmin
```

4. 다음 명령을 사용하여 파일 시스템에 섀도우 복사본 스토리지가 이미 구성되어 있지 않은지 확인합니다.

```
[fs-1234567890abcef12]: PS>Get-FsxShadowStorage
No Fsx Shadow Storage Configured
```

5. 옵션을 사용하여 섀도우 스토리지의 양을 볼륨의 10% 로 설정하고 섀도 복사본의 최대 수를 20개로 설정합니다. `-Default`

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage -Default
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
             0         0 32530536858                  20
```

Set-FSxShadowStorage명령을 -MaxShadowCopyNumber 매개 변수와 함께 사용하고 1~500 사이의 값을 지정하여 파일 시스템에 허용되는 최대 섀도 복사본 수를 제한할 수 있습니다. 기본적으로 최대 섀도우 복제본 수는 활성 워크로드에 대해 Microsoft에서 권장하는 대로 20개로 설정됩니다.

섀도우 복사본 스토리지 보기

파일 시스템의 원격 PowerShell 세션에서 Get-FsxShadowStorage 명령을 사용하여 파일 시스템의 섀도우 복사본이 현재 사용하고 있는 스토리지의 양을 볼 수 있습니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-1234567890abcef12]: PS>PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- ------------------
             0         0 10737418240                 20
```

출력에는 다음과 같이 섀도우 스토리지 구성이 표시됩니다.

- AllocatedSpace— 현재 섀도 복사본에 할당된 파일 시스템의 스토리지 크기 (바이트). 처음에 이 값은 0입니다.
- UsedSpace— 섀도우 복사본에서 현재 사용하고 있는 스토리지 양 (바이트) 처음에 이 값은 0입니다.
- MaxSpace— 섀도우 스토리지를 확장할 수 있는 최대 스토리지 크기 (바이트). Set-FsxShadowStorage 명령을 사용하여 섀도우 복사본 스토리지에 설정하는 값입니다.
- MaxShadowCopyNumber— 파일 시스템에서 보유할 수 있는 최대 섀도 복사본 수는 1~500개입니다.

크기가 구성된 섀도 복사본 최대 스토리지 양 (MaxSpace) 에 도달하거나 섀도 복사본 수가 구성된 최대 섀도 복사본 수 (MaxShadowCopyNumber) 에 도달하면 다음으로 생성하는 섀도 복사본이 가장 오래된 섀도 복사본을 대체합니다. UsedSpace 가장 오래된 섀도우 복사본을 잃지 않으려면 섀도우 복사본 스토리지를 모니터링하여 새 섀도우 복사본을 저장할 충분한 저장 공간이 있는지 확인합니다. 공간이 더 필요한 경우 기존 섀도우 복사본을 삭제하거나 최대 섀도우 복사본 스토리지 양을 늘릴 수 있습니다.

> **Note**
>
> 섀도 복제본을 자동 또는 수동으로 생성할 때는 스토리지 제한으로 구성한 섀도 복사본 스토리지의 양이 사용됩니다. 섀도 복사본은 시간이 지남에 따라 크기가 커지며 CloudWatch `FreeStorageCapacity` 지표에 표시된 사용 가능한 스토리지 공간을 구성된 최대 섀도 복사본 스토리지 양까지 활용합니다 (`MaxSpace`).

섀도우 복사본 스토리지, 일정 및 모든 섀도우 복사본 삭제

기존의 모든 섀도우 복사본을 포함한 섀도우 복사본 구성을 섀도우 복사본 일정과 함께 삭제할 수 있습니다. 동시에 파일 시스템에서 섀도우 복사본 스토리지를 확보할 수 있습니다.

이렇게 하려면 파일 시스템의 원격 PowerShell 세션에 `Remove-FsxShadowStorage` 명령을 입력합니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowStorage

Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FsxShadowStorage" on target "Removing all Shadow
 Copies, Shadow Copy Schedule, and Shadow Storage".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
FSx Shadow Storage Configuration
Removing Shadow Copy Schedule
Removing Shadow Copies
All shadow copies removed.
Removing Shadow Storage
Shadow Storage removed successfully.
```

사용자 지정 섀도우 복사본 일정 생성

섀도우 복사본 일정은 Microsoft Windows의 예약 작업 트리거를 사용하여 섀도우 복사본이 자동으로 생성되는 시기를 지정합니다. 섀도우 복사본 일정에는 트리거가 여러 개 있을 수 있으므로 일정을 유연하게 조정할 수 있습니다. 섀도우 복사본 일정은 한 번에 하나만 존재할 수 있습니다. 섀도우 복사본 일정을 생성하려면 먼저 섀도우 복사본 스토리지의 양을 설정해야 합니다.

파일 시스템에서 `Set-FsxShadowCopySchedule` 명령을 실행하면 기존 섀도우 복사본 일정을 모두 덮어씁니다. 클라이언트 컴퓨터가 UTC 시간대에 있는 경우 Windows 시간대 및 `-TimezoneId` 옵션

을 사용하여 트리거의 시간대를 지정할 수도 있습니다. Windows 시간대 목록을 보려면 Microsoft의 기본 시간대 설명서를 참조하거나 Windows 명령 프롬프트에서 `tzutil /l`를 실행하세요. Windows 작업 트리거에 대한 자세한 내용은 Microsoft Windows 개발자 센터 설명서의 작업 트리거를 참조하세요.

`-Default` 옵션을 사용하여 기본 섀도우 복사본 일정을 빠르게 설정할 수도 있습니다. 자세한 내용은 기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다. 섹션을 참조하세요.

사용자 지정 섀도우 복사본 일정 생성

1. Windows 예약 작업 트리거 세트를 생성하여 섀도우 복사본 일정에서 섀도우 복사본을 생성하는 시기를 정의합니다. 로컬 PowerShell 컴퓨터의 a에서 `new-scheduledTaskTrigger` 명령을 사용하여 여러 트리거를 설정합니다.

   다음 예제에서는 매주 월요일~금요일, 오전 6시, 오후 6시(UTC)에 섀도우 복사본을 생성하는 사용자 지정 섀도우 복사본 일정을 생성합니다. 만든 Windows 예약 작업 트리거에서 시간대를 지정하지 않는 한, 기본적으로 시간은 UTC로 표시됩니다.

   ```
   PS C:\Users\delegateadmin> $trigger1 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 06:00
   PS C:\Users\delegateadmin> $trigger2 = new-scheduledTaskTrigger -weekly -DaysOfWeek
    Monday,Tuesday,Wednesday,Thursday,Friday -at 18:00
   ```

2. `invoke-command`를 사용하여 `scriptblock` 명령을 실행합니다. 이렇게 하면 방금 만든 `new-scheduledTaskTrigger` 값으로 섀도우 복사본 일정을 설정하는 스크립트가 작성됩니다. 관리하려는 파일 시스템의 Windows 원격 *`FSxFileSystem-Remote-PowerShell-Endpoint`* PowerShell 엔드포인트로 바꾸십시오. Amazon FSx 콘솔, 파일 시스템 세부 정보 화면의 네트워크 및 보안 섹션 또는 API 작업의 `DescribeFileSystem` 응답에서 Windows Remote PowerShell 엔드포인트를 찾을 수 있습니다.

   ```
   PS C:\Users\delegateadmin> invoke-command -ComputerName FSxFileSystem-Remote-
   PowerShell-Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {
   ```

3. >> 프롬프트에 다음 줄을 입력하여 `set-fsxshadowcopyschedule` 명령을 사용하여 섀도우 복사본 일정을 설정합니다.

   ```
   >> set-fsxshadowcopyschedule -scheduledtasktriggers $Using:trigger1,$Using:trigger2
    -Confirm:$false }
   ```

   응답에는 파일 시스템에 구성한 섀도우 복사본 일정이 표시됩니다.

```
FSx Shadow Copy Schedule


Start Time:    : 2019-07-16T06:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcde1

Start Time:    : 2019-07-16T18:00:00+00:00
Days of Week   : Monday,Tuesday,Wednesday,Thursday,Friday
WeeksInterval  : 1
PSComputerName : fs-0123456789abcdef1
RunspaceId     : 12345678-90ab-cdef-1234-567890abcdef
```

섀도우 복사본 일정 보기

파일 시스템의 기존 섀도 복사 일정을 보려면 파일 시스템의 원격 PowerShell 세션에서 다음 명령을 입력합니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-0123456789abcdef1]PS> Get-FsxShadowCopySchedule
FSx Shadow Copy Schedule

Start Time                Days of week                              WeeksInterval
----------                ------------                              -------------
2019-07-16T07:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
2019-07-16T12:00:00+00:00 Monday,Tuesday,Wednesday,Thursday,Friday             1
```

섀도우 복사본 일정 삭제

파일 시스템의 기존 섀도 복제본 일정을 삭제하려면 파일 시스템의 원격 PowerShell 세션에서 다음 명령을 입력합니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopySchedule

Confirm
Are you sure you want to perform this action?
```

```
Performing the operation "Remove-FsxShadowCopySchedule" on target "Removing FSx Shadow
 Copy Schedule".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y"): Y
[fs-0123456789abcdef1]PS>
```

섀도우 복사본 생성

섀도 복제본을 수동으로 생성하려면 파일 시스템의 원격 PowerShell 세션에 다음 명령을 입력합니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-0123456789abcdef1]PS>New-FsxShadowCopy

Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} taken successfully
```

기존 섀도우 복사본 보기

파일 시스템에 있는 기존 섀도 복사본 세트를 보려면 파일 시스템의 원격 PowerShell 세션에서 다음 명령을 입력합니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

```
[fs-0123456789abcdef1]PS>Get-FsxShadowCopies
FSx Shadow Copies: 2 total

Shadow Copy ID                          Creation Time
--------------                          -----------------
{ABCDEF12-3456-7890-ABCD-EF1234567890} 6/17/2019 7:11:09 AM
{FEDCBA21-6543-0987-0987-EF3214567892} 6/19/2019 11:24:19 AM
```

섀도우 복사본 삭제

파일 시스템의 원격 PowerShell 세션에서 `Remove-FsxShadowCopies` 명령을 사용하여 파일 시스템에 있는 기존 섀도 복사본을 하나 이상 삭제할 수 있습니다. 파일 시스템에서 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오아마존 FSx CLI를 사용하는 방법 PowerShell.

다음과 같은 필수 옵션 중 하나를 사용하여 삭제할 섀도우 복사본을 지정합니다.

- `-Oldest`는 가장 오래된 섀도우 복사본을 삭제합니다.
- `-All`은 기존 섀도우 복사본을 모두 삭제합니다.

- -ShadowCopyId는 ID별로 특정 섀도우 복사본을 삭제합니다.

명령에 하나의 옵션만 사용할 수 있습니다. 삭제할 섀도우 복사본을 지정하지 않거나, 섀도우 복사본 ID를 여러 개 지정하거나, 잘못된 섀도우 복사본 ID를 지정한 경우 오류가 발생합니다.

파일 시스템에서 가장 오래된 섀도 복제본을 삭제하려면 파일 시스템의 원격 PowerShell 세션에 다음 명령을 입력합니다.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -Oldest
Confirm
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing oldest shadow
 copy".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y": Y
Shadow Copy {ABCDEF12-3456-7890-ABCD-EF1234567890} deleted
```

파일 시스템에서 특정 섀도 복사본을 삭제하려면 파일 시스템의 원격 PowerShell 세션에 다음 명령을 입력합니다.

```
[fs-0123456789abcdef1]PS>Remove-FsxShadowCopies -ShadowCopyId "{ABCDEF12-3456-7890-
ABCD-EF1234567890}"
Are you sure you want to perform this action?
Performing the operation "Remove-FSxShadowCopies" on target "Removing shadow copy
 {ABCDEF12-3456-7890-ABCD-EF1234567890}".
[Y] Yes [A] Yes to All [N] No [L] No to All [?] Help (Default is "Y":>Y
Shadow Copy \\AMZNFSXABCDE123\root\cimv2:Wind32_ShadowCopy.ID{ABCDEF12-3456-7890-ABCD-
EF1234567890}".ID deleted.
```

파일 시스템에서 가장 오래된 섀도 복사본을 특정 개수만큼 삭제하려면 남기고 싶은 섀도 복사본 -MaxShadowCopyNumber 수로 매개 변수를 업데이트하십시오. 그러나 이 변경 사항은 시스템에서 초과 섀도 복사본을 자동으로 삭제하는 다음 섀도 복사본 스냅샷을 만든 후에만 적용됩니다. 파일 시스템의 원격 PowerShell 세션에서 다음 명령을 사용하십시오.

```
[fs-1234567890abcef12]: PS>Get-fsxshadowstorage
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace MaxSpace    MaxShadowCopyNumber
-------------- --------- ----------- -------------------
     556679168  21659648 10737418240                  50
```

```
[fs-1234567890abcef12]: PS>Set-FsxShadowStorage  -MaxShadowCopyNumber 5
Validation
You have 50 shadow copies. Older versions of shadow copies will be deleted, keeping 5
 latest shadow copies on your file system.
Do you want to continue?
[Y] Yes  [N] No  [?] Help (default is "N"): y
FSx Shadow Storage Configuration

AllocatedSpace UsedSpace    MaxSpace MaxShadowCopyNumber
-------------- ---------    -------- -------------------
     556679168  21659648 10737418240                   5
```

를 사용한 예약 복제 AWS DataSync

를 사용하여 Windows File Server용 FSx 파일 시스템을 보조 파일 시스템으로 정기적으로 AWS DataSync 복제하도록 스케줄링할 수 있습니다. 이 기능은 리전 내 배포와 크로스 리전 배포 모두에 사용할 수 있습니다. 자세한 내용은 이 가이드의 설명서와 사용 설명서의 AWS 스토리지 서비스 간 데이터 전송을 참조하십시오AWS DataSync를 사용하여 기존 파일을 FSx for Windows File Server로 마이그레이션.AWS DataSync

파일 시스템 관리

이 장에서는 원격 PowerShell 관리를 위해 Amazon FSx CLI에 액세스하는 방법과 사용 가능한 파일 시스템 관리 작업을 수행하는 방법을 설명합니다. Microsoft Windows 고유의 그래픽 사용자 인터페이스(GUI) 를 사용하여 일부 관리 작업을 수행할 수도 있습니다.

주제

아마존 FSx CLI를 사용하는 방법 PowerShell

원격 PowerShell 관리용 Amazon FSx CLI를 사용하면 파일 시스템 관리자 그룹의 사용자가 파일 시스템을 관리할 수 있습니다. FSx for Windows File Server 파일 시스템에서 원격 PowerShell 세션을 시작하려면 먼저 다음 사전 요구 사항을 충족해야 합니다.

- Windows File Server용 FSx 파일 시스템과 네트워크로 연결된 Windows 컴퓨팅 인스턴스에 연결할 수 있어야 합니다.
- 파일 시스템 관리자 그룹의 구성원으로 Windows 컴퓨팅 인스턴스에 로그인합니다. 를 사용하는 AWS Managed Microsoft AD경우 이는 AWS 위임된 FSx 관리자 그룹입니다. 자체 관리형 Microsoft

Active Directory를 사용하는 경우 이는 파일 시스템을 만들 때 관리하도록 지정한 도메인 관리자 그룹 또는 사용자 지정 그룹입니다. 자세한 정보는 자체 관리형 Active Directory 모범 사례을 참조하세요.

- 파일 시스템의 VPC 보안 그룹 인바운드 규칙은 포트 5985에서의 트래픽을 허용합니다.

원격 PowerShell 관리를 위한 Amazon FSx CLI는 다음과 같은 보안 기능을 사용합니다.

- 사용자 자격 증명은 Kerberos 인증을 사용하여 인증됩니다.
- 연결된 클라이언트와 파일 시스템 간의 관리 세션 통신은 Kerberos를 사용하여 암호화됩니다.

Amazon FSx 파일 시스템에서 원격 관리 CLI 명령을 실행할 수 있는 두 가지 옵션이 있습니다.

- 장기 실행 원격 PowerShell 세션을 설정하고 세션 내에서 명령을 실행할 수 있습니다.
- 장기 실행 원격 PowerShell 세션을 설정하지 않고도 `Invoke-Command` 를 사용하여 단일 명령 또는 단일 명령 블록을 실행할 수 있습니다.

변수를 설정하여 원격 관리 명령에 매개 변수로 전달하려면 를 사용해야 `Invoke-Command` 합니다.

> **Note**
>
> 다중 AZ 파일 시스템의 경우, 파일 시스템이 기본 파일 서버를 사용하는 동안에는 원격 관리용 Amazon FSx CLI만 사용할 수 있습니다. 자세한 정보는 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템을 참조하세요.

리모컨을 사용할 때는 파일 시스템의 Windows 원격 PowerShell 엔드포인트를 사용해야 합니다. PowerShell 를 AWS Management Console사용하면 파일 시스템 세부 정보 페이지의 네트워크 및 보안 탭에서 엔드포인트를 찾을 수 있습니다. AWS CLI `describe-file-systems`명령을 사용하면 응답에 `RemoteAdministrationEndpoint` 속성이 반환됩니다. 원격 관리 엔드포인트는 형식을 `amznfsxctlyaa1k.`*`ActiveDirectory-DNS-name`* 사용합니다 (예`amznfsxctlyaa1k.corp.example.com`:

`Get-Command`cmdlet을 사용하여 에서 사용할 수 있는 cmdlet, 함수 및 별칭에 대한 정보를 가져올 수 있습니다. PowerShell 자세한 내용은 Microsoft Get-Command 설명서를 참조하세요.

또한 다음 구문을 사용하여 cmdlet을 사용하여 파일 `Invoke-Command` 시스템의 명령에 대해 원격 관리 PowerShell CLI용 Amazon FSx CLI를 실행할 수 있습니다.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName
 amznfsxctlyaa1k.corp.example.com -ConfigurationName FSxRemoteAdmin -scriptblock { fsx-
command}
```

Windows File Server용 FSx 파일 시스템에서 수명이 긴 원격 PowerShell 세션을 시작하는 방법에 대한 지침은 을 참조하십시오. 아마존 PowerShell FSx 원격 세션 시작

아마존 PowerShell FSx 원격 세션 시작

이 항목에서는 Windows File Server용 FSx 파일 서버에서 수명이 긴 원격 PowerShell 세션을 시작하기 위한 지침을 제공합니다.

파일 시스템에서 원격 PowerShell 세션을 시작하려면

1. 파일 시스템을 생성할 때 선택한 위임된 FSx Administrators Group의 구성원인 사용자로 파일 시스템에 네트워크로 연결된 컴퓨팅 인스턴스에 연결합니다.
2. 컴퓨팅 인스턴스에서 Windows PowerShell 창을 엽니다.
3. 에서 다음 PowerShell 명령을 입력하여 Amazon FSx 파일 시스템에서 수명이 긴 원격 세션을 엽니다. 관리하려는 파일 시스템의 Windows 원격 *Remote-PowerShell-Endpoint* PowerShell 엔드포인트로 대체하십시오. `FsxRemoteAdmin`을 세션 구성 이름으로 사용합니다.

   ```
   PS C:\Users\delegateadmin> enter-pssession -ComputerName Remote-PowerShell-Endpoint
    -ConfigurationName FsxRemoteAdmin
   [fs-0123456789abcdef0]: PS>
   ```

   인스턴스가 Amazon FSx Active Directory 도메인에 속하지 않는 경우 팝업에 사용자 자격 증명을 입력하라는 메시지가 표시됩니다. FSx 관리자 그룹 구성원인 사용자의 자격 증명을 입력합니다. 인스턴스가 도메인에 조인된 경우 보안 인증을 요청하지 않습니다.

DNS 별칭 관리

FSx for Windows File Server는 파일 시스템의 데이터에 액세스하는 데 사용할 수 있는 모든 파일 시스템에 기본 도메인 이름 시스템(DNS) 이름을 제공합니다. 선택한 DNS 별칭을 사용하여 파일 시스템에 액세스할 수도 있습니다. DNS 별칭을 사용하면 도구나 애플리케이션을 업데이트할 필요 없이 온프레미스에서 Amazon FSx로 파일 시스템 스토리지를 마이그레이션할 때 기존 DNS 이름을 사용하여 Amazon FSx에 저장된 데이터에 계속 액세스할 수 있습니다. 자세한 정보는 기존 파일 스토리지를 Amazon FSx로 마이그레이션을 참조하세요.

> **Note**
>
> DNS 별칭에 대한 지원은 2020년 11월 9일 오후 12시(동부 표준시) 이후에 생성된 FSx for Windows File Server 파일 시스템에서 사용할 수 있습니다. 2020년 11월 9일 오후 12시(동부 표준시) 이전에 생성된 파일 시스템에서 DNS 별칭을 사용하려면 다음과 같이 하세요.
>
> 1. 기존 파일 시스템을 백업합니다. 자세한 정보는 사용자 시작 백업 작업을 참조하세요.
> 2. 백업을 새 파일 시스템으로 복원합니다. 자세한 정보는 백업 복원을 참조하세요.
>
> 새 파일 시스템을 사용할 수 있게 되면 이 섹션에 제공된 정보를 사용하여 DNS 별칭을 사용하여 해당 파일 시스템에 액세스할 수 있습니다.

> **Note**
>
> 여기에 제시된 정보는 사용자가 전적으로 Active Directory 내에서 작업하고 외부 DNS 공급자를 사용하지 않는 것을 가정합니다. 서드 파티 DNS 공급자는 예기치 않은 동작을 발생시킬 수 있습니다.
> Amazon FSx는 파일 시스템에 조인하려는 AD 도메인이 Microsoft DNS를 기본 DNS로 사용하는 경우에만 파일 시스템에 대한 DNS 레코드를 등록합니다. 서드 파티 DNS를 사용하는 경우 파일 시스템을 생성한 후 Amazon FSx 파일 시스템에 대한 DNS 항목을 수동으로 설정해야 합니다. 파일 시스템에 사용할 올바른 IP 주소를 선택하는 방법에 대한 자세한 내용은 DNS에 사용할 올바른 파일 시스템 IP 주소 획득 섹션을 참조하세요.

새 파일 시스템을 생성하고 백업에서 새 파일 시스템을 생성할 때 기존 FSx for Windows File Server 파일 시스템에 DNS 별칭을 연결할 수 있습니다. 언제든지 한 번에 파일 시스템에 최대 50개의 DNS 별칭을 연결할 수 있습니다.

DNS 별칭을 파일 시스템에 연결하는 것 외에도 클라이언트가 DNS 별칭을 사용하여 파일 시스템에 연결하려면 다음 작업도 수행해야 합니다.

- Kerberos 인증 및 암호화를 위한 서비스 보안 주체 이름(SPN)을 구성합니다.
- Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 별칭에 대한 DNS CNAME 레코드를 구성합니다.

자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

Windows File Server용 FSx 파일 시스템의 DNS 별칭 이름은 다음 요구 사항을 충족해야 합니다.

- 정규화된 도메인 이름(FQDN) 형식으로 지정해야 합니다.
- 영숫자 및 하이픈(-)을 포함할 수 있습니다.
- 하이픈으로 시작되거나 끝날 수 없습니다.
- 숫자로 시작될 수 있습니다.

DNS 별칭 이름의 경우 Amazon FSx는 영문자가 지정된 방법(대문자, 소문자 또는 이스케이프 코드)과 관계없이 영문자를 소문자(a~z)로 저장합니다.

파일 시스템과 이미 연결되어 있는 별칭을 연결하려고 해도 아무 효과가 없습니다. 파일 시스템과 연결되지 않은 파일 시스템에서 별칭을 연결 해제하려고 하면 Amazon FSx는 잘못된 요청 오류로 응답합니다.

> **Note**
>
> Amazon FSx가 파일 시스템에서 별칭을 추가하거나 제거하면 연결된 클라이언트의 연결이 일시적으로 끊기고 자동으로 파일 시스템에 다시 연결됩니다. 연결이 끊겼을 때 연속적으로 사용할 수 없는(비CA) 공유를 매핑하는 클라이언트가 열었던 모든 파일을 클라이언트가 다시 열어야 합니다.

주제

DNS 별칭 상태

DNS 별칭은 다음 상태 값 중 하나를 가질 수 있습니다.

- 사용 가능 - DNS 별칭이 Amazon FSx 파일 시스템과 연결되어 있습니다.
- 생성 중 - Amazon FSx가 DNS 별칭을 생성하고 이를 파일 시스템과 연결하고 있습니다.

- 삭제 중 - Amazon FSx가 파일 시스템에서 DNS 별칭을 연결 해제하여 삭제하고 있습니다.
- 생성 실패 - Amazon FSx가 DNS 별칭을 파일 시스템과 연결할 수 없습니다.
- 삭제 실패 - Amazon FSx가 DNS 별칭을 파일 시스템에서 연결 해제할 수 없습니다.

Kerberos 인증의 DNS 별칭 사용

Amazon FSx에서는 전송 중에 Kerberos 기반 인증 및 암호화를 사용하는 것이 좋습니다. Kerberos는 파일 시스템에 액세스하는 클라이언트에게 가장 안전한 인증을 제공합니다. DNS 별칭을 사용하여 Amazon FSx 파일 시스템에 액세스하는 클라이언트에 대해 Kerberos 인증을 활성화하려면 파일 시스템의 Active Directory 컴퓨터 객체에 있는 DNS 별칭에 해당하는 SPN (서비스 사용자 이름) 을 구성해야 합니다.

Active Directory의 컴퓨터 객체에 있는 다른 파일 시스템에 할당한 DNS 별칭으로 SPN을 구성한 경우 파일 시스템의 컴퓨터 객체에 SPN을 추가하기 전에 먼저 해당 SPN을 제거해야 합니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

파일 시스템 및 백업의 DNS 별칭 보기

Amazon FSx 콘솔, AWS CLI 및 API를 사용하여 현재 파일 시스템 및 백업과 연결된 DNS 별칭을 확인할 수 있습니다. 이 주제에서는 파일 시스템 및 백업의 DNS 별칭을 보는 방법에 대한 지침을 제공합니다.

파일 시스템과 연결된 DNS 별칭을 보려면

- 콘솔 사용 - 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 봅니다. 네트워크 및 보안 탭을 선택하여 DNS 별칭을 봅니다.
- CLI 또는 API 사용 - `describe-file-system-aliases` CLI 명령 또는 API 작업을 사용합니다. DescribeFileSystemAliases

백업과 관련된 DNS 별칭을 보려면

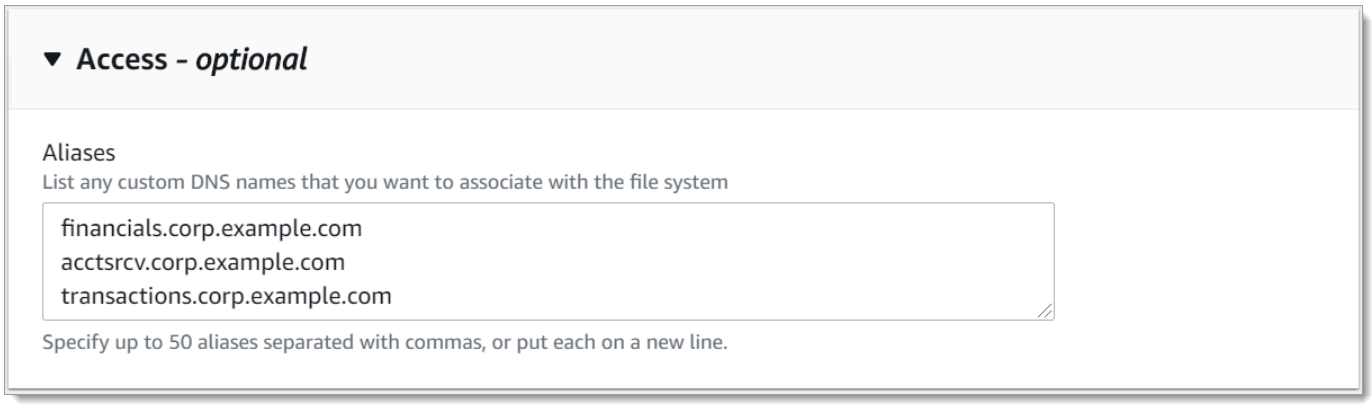
- 콘솔 사용 - 탐색 창에서 백업을 선택한 다음 보려는 백업을 선택합니다. 요약 창에서 DNS 별칭 필드를 봅니다.
- CLI 또는 API 사용 - `describe-backups` CLI 명령 또는 API 작업을 사용합니다. DescribeBackups

DNS 별칭을 파일 시스템에 연결

이 항목에서는 Windows File Server용 새 FSx 파일 시스템을 처음부터 생성하거나, 및 API를 AWS Management Console사용하여 AWS CLI백업에서 파일 시스템을 생성할 때 DNS 별칭을 연결하는 방법에 대해 설명합니다.

새 파일 시스템을 생성할 때 DNS 별칭을 연결하려면 (콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 시작하기 섹션의 파일 시스템 생성 섹션에 설명된 새 파일 시스템 생성 절차를 따릅니다.
3. 파일 시스템 생성 마법사의 액세스 - 선택 사항 섹션에서 파일 시스템과 연결할 DNS 별칭을 입력합니다.



4. 파일 시스템이 사용 가능 상태가 되면 서비스 보안 주체 이름(SPN)을 구성하고 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성하여 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

새 Amazon FSx 파일 시스템을 생성할 때 DNS 별칭 연결(CLI)

1. 새 파일 시스템을 생성할 때는 CreateFileSystemAPI 작업에 Alias 속성을 사용하여 DNS 별칭을 새 파일 시스템에 연결합니다.

```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 2000 \
  --storage-type SSD \
  --subnet-ids subnet-123456 \
  --windows-configuration Aliases=[financials.corp.example.com,accts-
rcv.corp.example.com]
```

2. 파일 시스템이 사용 가능 상태가 되면 서비스 보안 주체 이름(SPN)을 구성하고 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성하여 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

백업을 복원할 때 DNS 별칭을 추가하거나 제거하려면 (CLI)

1. 기존 파일 시스템의 백업에서 새 파일 시스템을 생성할 때 다음과 같이 CreateFileSystemFromBackupAPI 작업에 Aliases 속성을 사용할 수 있습니다.

   - 백업과 연결된 모든 별칭은 기본적으로 새 파일 시스템과 연결됩니다.
   - 백업의 별칭을 보존하지 않고 파일 시스템을 만들려면 빈 세트가 있는 `Aliases` 속성을 사용합니다.

     추가 DNS 별칭을 연결하려면 `Aliases` 속성을 사용하고 백업과 연결된 원래 별칭 및 연결하려는 새 별칭을 모두 포함합니다.

   다음 CLI 명령은 두 개의 별칭을 Amazon FSx가 백업에서 생성하는 파일 시스템과 연결합니다.

   ```
   aws fsx create-file-system-from-backup \
     --backup-id backup-0123456789abcdef0
     --storage-capacity 2000 \
     --storage-type HDD \
     --subnet-ids subnet-123456 \
     --windows-configuration Aliases=[transactions.corp.example.com,accts-
   rcv.corp.example.com]
   ```

2. 파일 시스템이 사용 가능 상태가 되면 서비스 보안 주체 이름(SPN)을 구성하고 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성하여 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

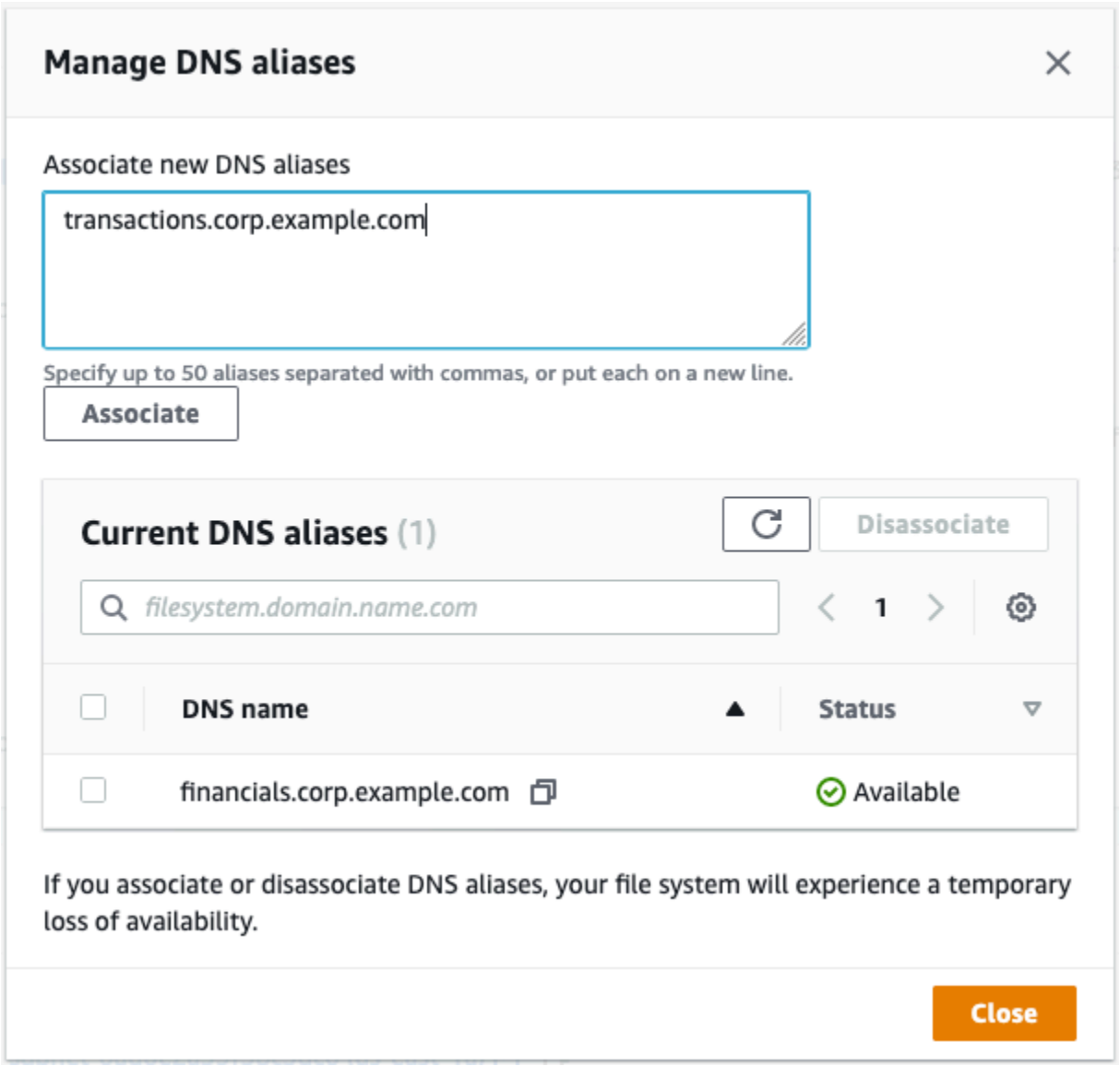
기존 파일 시스템의 DNS 별칭 관리

이 항목에서는 AWS Management Console 및 AWS CLI 를 사용하여 기존 파일 시스템에 별칭을 추가 및 제거하는 방법에 대해 설명합니다.

파일 시스템 DNS 별칭을 관리하려면 (콘솔)

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

2. 파일 시스템으로 이동하여 DNS 별칭을 관리할 Windows 파일 시스템을 선택합니다.
3. 네트워크 및 보안 탭에서 DNS 별칭의 관리를 선택하여 DNS 별칭 관리 대화 상자를 표시합니다.



- DNS 별칭 연결 방법 - 새 별칭 연결 상자에서, 연결하려는 DNS 별칭을 입력합니다. Associate(연결)를 선택합니다.
- DNS 별칭 연결 해제 방법 - 현재 별칭 목록에서, 연결을 해제할 별칭을 선택합니다. 연결 해제를 선택합니다.

현재 별칭 목록에서 관리한 별칭의 상태를 모니터링할 수 있습니다. 목록의 새로 고침을 수행하여 상태를 업데이트합니다. 별칭이 파일 시스템과 연결되거나 연결 해제되는 데 최대 2.5분이 소요됩니다.

4. 별칭이 사용 가능 상태가 되면 서비스 보안 주체 이름(SPN)을 구성하고 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성하여 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

DNS 별칭을 기존 파일 시스템 (CLI) 에 연결하는 방법

1. `associate-file-system-aliases`CLI 명령 또는 AssociateFileSystemAliasesAPI 작업을 사용하여 DNS 별칭을 기존 파일 시스템에 연결합니다.

   다음 CLI 요청은 별칭 두 개를 지정된 파일 시스템과 연결합니다.

   ```
   aws fsx associate-file-system-aliases \
     --file-system-id fs-0123456789abcdef0 \
     --aliases financials.corp.example.com transfers.corp.example.com
   ```

   응답은 Amazon FSx가 파일 시스템과 연결하는 별칭의 상태를 보여줍니다.

   ```
   {
       "Aliases": [
           {
               "Name": "financials.corp.example.com",
               "Lifecycle": CREATING
           },
           {
               "Name": "transfers.corp.example.com",
               "Lifecycle": CREATING
           }
       ]
   }
   ```

2. `describe-file-system-aliases`CLI 명령 (DescribeFileSystemAliases동일한 API 작업) 을 사용하여 연결 중인 별칭의 상태를 모니터링할 수 있습니다.

3. `Lifecycle`이 '사용 가능' 값을 가지게 되면(처리에 2.5분 소요) 서비스 보안 주체 이름(SPN)을 구성하고 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성하여 DNS 별칭을 사용하여 파일 시스템에 액세스할 수 있습니다. 자세한 정보는 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스을 참조하세요.

파일 시스템에서 DNS 별칭을 분리하려면 (CLI)

- `disassociate-file-system-aliases`CLI 명령 또는 DisassociateFileSystemAliasesAPI 작업을 사용하여 기존 파일 시스템에서 DNS 별칭을 분리합니다.

  다음 명령은 파일 시스템에서 별칭 하나를 연결 해제합니다.

  ```
  aws fsx disassociate-file-system-aliases \
    --file-system-id fs-0123456789abcdef0 \
    --aliases financials.corp.example.com
  ```

  응답은 Amazon FSx가 파일 시스템에서 연결 해제하는 별칭의 상태를 보여줍니다.

  ```
  {
      "Aliases": [
          {
              "Name": "financials.corp.example.com",
              "Lifecycle": DELETING
          }
      ]
  }
  ```

  `describe-file-system-aliases`CLI 명령 (DescribeFileSystemAliases동일한 API 작업) 을 사용하여 별칭의 상태를 모니터링합니다. 별칭을 삭제하는 데 최대 2.5분이 소요됩니다.

Windows File Server 파일 시스템용 FSx의 파일 공유 관리

이 항목에서는 다음 작업을 수행하여 파일 공유를 관리하는 방법에 대해 설명합니다.

- 새 파일 공유 생성
- 기존 파일 공유를 수정합니다.
- 기존 파일 공유 제거

Windows 네이티브 공유 폴더 GUI와 Amazon FSx CLI를 사용하여 Windows 파일 서버용 FSx 파일 시스템의 파일 공유를 관리하는 원격 관리를 수행할 PowerShell 수 있습니다. 다른 파일 시스템에 있는 공유의 컨텍스트 메뉴를 처음 열 때 공유 폴더 GUI(fsmgmt.msc)를 사용하면 지연이 발생할 수 있습니다. 이러한 지연을 방지하려면 여러 파일 시스템에 있는 파일 PowerShell 공유를 관리하는 데 사용하십시오.

Windows에서 지원하는 모든 파일 시스템에는 파일 및 디렉터리 이름에 대한 규칙과 제한이 있다는 점에 유의해야 합니다. 데이터를 성공적으로 만들고 액세스할 수 있으려면 이러한 Windows 지침에 따라 파일 및 디렉터리의 이름을 지정해야 합니다. 자세한 내용은 이름 지정 규칙을 참조하세요.

> **Warning**
>
> Amazon FSx에서는 SMB 파일 공유를 생성하는 모든 폴더에 대해 시스템 사용자에게 전체 제어 NTFS ACL 권한이 있어야 합니다. 폴더에서 이 사용자의 NTFS ACL 권한을 변경하면 파일 공유에 액세스할 수 없게 될 수 있으므로 변경하지 않습니다.

공유 폴더 GUI를 통한 파일 공유 관리

Amazon FSx 파일 시스템에서 파일 공유를 관리하기 위해 공유 폴더 GUI를 사용할 수 있습니다. 공유 폴더 GUI는 Windows 서버의 모든 공유 폴더를 관리할 수 있는 중앙 위치를 제공합니다. 다음 절차에서는 파일 공유를 관리하는 방법을 설명합니다.

FSx for Windows File Server 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. AWS 관리형 Microsoft Active Directory에서는 이 그룹을 AWS 위임 FSx 관리자라고 합니다. 자체 관리형 Microsoft Active Directory에서는 이 그룹을 도메인 관리자 또는 생성 시 제공한 관리자 그룹의 사용자 지정 이름이라고 합니다. 자세한 내용은 Windows 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Windows 인스턴스에 연결을 참조하세요.
3. 시작 메뉴를 열고 관리자 권한으로 실행 을 사용하여 fsmgmt.msc를 실행합니다. 이렇게 하면 공유 폴더 GUI 도구가 열립니다.
4. 작업에서 다른 컴퓨터에 연결을 선택합니다.
5. 다른 컴퓨터에 Amazon FSx 파일 시스템의 도메인 이름 시스템(DNS) 이름(예: **`amznfsxabcd0123.corp.example.com`**)을 입력합니다.

Amazon FSx 콘솔에서 파일 시스템의 DNS 이름을 찾으려면 파일 시스템을 선택하고 원하는 파일 시스템을 선택한 다음 파일 시스템 세부 정보 페이지의 네트워크 및 보안 섹션을 확인합니다. DescribeFile시스템 API 작업에 대한 응답으로 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 파일 시스템에서 Windows 파일 공유를 관리할 수 있습니다. 기본 공유의 이름은 \share입니다. 그렇게 하려면 다음 작업을 수행합니다.

- 새 파일 공유 생성 - 공유 폴더 도구의 왼쪽 창에서 공유를 선택하여 Amazon FSx 파일 시스템의 활성 공유를 확인합니다. 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 '찾아보기'를 클릭하고 '새 폴더 만들기'를 클릭하여 로컬 폴더를 생성합니다.
  - 명령줄 사용:

  ```
  New-Item -Type Directory -Path \\amznfsxabcd0123.corp.example.com\D$\share
  \MyNewShare
  ```

- 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**
>
> 단일 AZ 2 및 다중 AZ 파일 시스템의 경우, Amazon FSx 파일 시스템의 DNS 이름을 사용하여 fsmgmt.msc에 연결하는 경우에만 공유 폴더 GUI 도구를 사용하여 파일 공유를 제거하거나 파일 공유를 수정(권한, 사용자 제한 및 기타 속성 업데이트 포함)할 수 있습니다. 공유 폴더 GUI 도구는 파일 시스템의 IP 주소 또는 DNS 별칭 이름을 사용하여 연결하는 경우 이러한 작업을 지원하지 않습니다.

> **Note**
>
> fsmgmt.msc 공유 폴더 GUI 도구를 사용하여 여러 FSx 파일 시스템에 있는 공유에 액세스하는 경우, 다른 파일 시스템에 있는 공유에 대한 파일 공유 컨텍스트 메뉴를 처음 열 때 지연이 발생할 수 있습니다. 이러한 지연을 방지하기 위해 아래 PowerShell 설명된 방법을 사용하여 파일 공유를 관리할 수 있습니다.

파일 공유 관리: PowerShell

에 대한 사용자 지정 원격 관리 명령을 사용하여 파일 공유를 관리할 수 있습니다. PowerShell 다음 명령을 사용하면 이러한 작업을 보다 쉽게 자동화할 수 있습니다.

- 기존 파일 서버의 파일 공유를 Amazon FSx로 마이그레이션
- 재해 복구를 위한 AWS 지역 간 파일 공유 동기화
- 팀 파일 공유 프로비저닝과 같은 진행 중인 워크플로를 위한 파일 공유의 프로그래밍 방식 관리

에서 원격 관리를 위해 Amazon FSx CLI를 사용하는 방법을 알아보려면 을 참조하십시오. PowerShell 아마존 FSx CLI를 사용하는 방법 PowerShell

다음 표에는 Windows File Server 파일 시스템용 FSx에서 파일 공유를 관리하는 데 사용할 수 있는 Amazon FSx CLI PowerShell 원격 관리 명령이 나와 있습니다.

공유 관리 명령	설명
New-FSxSmbShare	새 파일 공유를 생성합니다.
Remove-FSxSmbShare	파일 공유를 제거합니다.
Get-FSxSmbShare	기존 파일 공유를 검색합니다.
Set-FSxSmbShare	공유의 속성을 설정합니다.
Get-FSxSmbShareAccess	공유의 액세스 제어 목록(ACL)을 검색합니다.
Grant-FSxSmbShareAccess	수탁자의 액세스 제어 항목(ACE)을 공유의 보안 설명자에 추가합니다.

공유 관리 명령	설명
Revoke-FSxSmbShareAccess	공유의 보안 설명자에서 수탁자의 허용 ACE를 모두 제거합니다.
Block-FSxSmbShareAccess	수탁자의 거부 ACE를 공유의 보안 설명자에 추가합니다.
Unblock-FSxSmbShareAccess	공유의 보안 설명자에서 수탁자의 거부 ACE를 모두 제거합니다.

각 명령의 온라인 도움말은 모든 명령 옵션에 대한 참조를 제공합니다. 이 도움말에 액세스하려면 `-?`(예: `New-FSxSmbShare -?`)와 함께 명령을 실행합니다.

New-F Share에 자격 증명 전달 SxSmb

자격 증명을 SxSmbShare New-F에 전달하면 매번 자격 증명을 다시 입력할 필요 없이 New-F를 루프에서 실행하여 수백 또는 수천 개의 공유를 생성할 수 있습니다.

다음 옵션 중 하나를 사용하여 FSx for Windows File Server 파일 서버에서 파일 공유를 생성하는 데 필요한 보안 인증 객체를 준비합니다.

- 대화형 방식으로 보안 인증 객체를 생성하려면 다음 명령을 사용합니다.

```
$credential = Get-Credential
```

- AWS Secrets Manager 리소스를 사용하여 자격 증명 개체를 생성하려면 다음 명령을 사용합니다.

```
$credential = ConvertFrom-Json -InputObject (Get-SECSecretValue -SecretId
 $AdminSecret).SecretString
$FSxAdminUserCredential = (New-Object PSCredential($credential.UserName,(ConvertTo-
SecureString $credential.Password -AsPlainText -Force)))
```

지속적으로 사용 가능한 (CA) 공유 생성

원격 관리용 Amazon FSx CLI를 사용하여 지속적으로 사용 가능한 (CA) 공유를 생성할 수 있습니다. PowerShell FSx for Windows File Server 다중 AZ 파일 시스템에서 생성된 CA 공유는 내구성이 뛰어나고 가용성이 높습니다. Amazon FSx 단일 AZ 파일 시스템은 단일 노드 클러스터에 구축됩니다. 따라서 단일 AZ 파일 시스템에서 생성된 CA 공유는 내구성이 높지만 가용성이 높지는 않습니다. `-ContinuouslyAvailable` 옵션을 `$True`로 설정한 상태에서 `New-FSxSmbShare` 명령을 사용하여 공유를 지속적으로 사용 가능한 공유로 지정합니다. 다음은 CA 공유를 생성하는 명령 예제입니다.

```
New-FSxSmbShare -Name "New CA Share" -Path "D:\share\new-share" -Description "CA share"
 -ContinuouslyAvailable $True
```

`Set-FSxSmbShare` 명령을 사용하여 기존 파일 공유의 `-ContinuouslyAvailable` 옵션을 수정할 수 있습니다.

기존 파일 공유를 계속 사용할 수 있는지 확인하십시오.

다음 명령을 사용하여 기존 파일 공유의 연속 사용 가능 속성 값을 볼 수 있습니다.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { get-fsxsmbshare -name share_name }
```

CA가 활성화된 경우 출력에는 다음 줄이 포함됩니다.

```
[...]
ContinuouslyAvailable : True
[...]
```

CA가 활성화되지 않은 경우 출력에는 다음 줄이 포함됩니다.

```
[...]
ContinuouslyAvailable : False
[...]
```

기존 파일 공유에서 연속 사용 가능을 활성화하려면 다음 명령을 사용합니다.

```
Invoke-Command -ComputerName powershell_endpoint -ConfigurationName FSxRemoteAdmin -
scriptblock { set-fsxsmbshare -name share_name -ContinuouslyAvailable $True}
```

파일 액세스 감사

Windows File Server용 Amazon FSx File Server는 파일, 폴더 및 파일 공유에 대한 최종 사용자 액세스 감사를 지원합니다. 파일 시스템의 감사 이벤트 로그를 다양한 기능을 제공하는 다른 AWS 서비스에 전송하도록 선택할 수 있습니다. 여기에는 로그의 쿼리, 처리, 저장 및 보관, 알림 발행, 보안 및 규정 준수 목표를 더욱 향상시키기 위한 트리거 조치가 포함됩니다.

파일 액세스 감사를 사용하여 액세스 패턴에 대한 인사이트를 얻고 최종 사용자 활동에 대한 보안 알림을 구현하는 방법에 대한 자세한 내용은 파일 스토리지 액세스 패턴 인사이트 및 최종 사용자 활동에 대한 보안 알림 구현을 참조하세요.

파일 액세스 감사를 사용하면 정의된 감사 제어를 기반으로 개별 파일, 폴더 및 파일 공유에 대한 최종 사용자 액세스를 기록할 수 있습니다. 감사 제어는 NTFS 시스템 액세스 제어 목록(SACL)이라고도 합니다. 기존 파일 데이터에 감사 제어를 이미 설정한 경우, 새 Amazon FSx for Windows File Server 파일 시스템을 생성하고 데이터를 마이그레이션하여 파일 액세스 감사를 활용할 수 있습니다.

Amazon FSx는 파일, 폴더 및 파일 공유 액세스에 대해 다음과 같은 Windows 감사 이벤트를 지원합니다.

- 파일 액세스의 경우, 모두, 폴더 트래버스/파일 실행, 폴더 나열/데이터 읽기, 속성 읽기, 파일 생성/데이터 쓰기, 폴더 생성/데이터 추가, 속성 쓰기, 하위 폴더 및 파일 삭제, 삭제, 읽기 권한, 변경 권한, 소유권 가져오기 옵션을 지원합니다.
- 파일 공유 액세스의 경우, 파일 공유 연결을 지원합니다.

Amazon FSx는 파일, 폴더 및 파일 공유 액세스에서 성공한 시도(예: 충분한 권한을 가진 사용자가 파일 또는 파일 공유에 성공적으로 액세스하는 경우), 실패한 시도 또는 두 가지 모두에 대한 로깅을 지원합니다.

액세스 감사를 파일 및 폴더에만 적용할지, 파일 공유에만 적용할지, 아니면 둘 다에 대해 감사할지 구성할 수 있습니다. 또한 로깅할 액세스 유형(성공한 시도만, 실패한 시도만 또는 둘 다)을 구성할 수 있습니다. 파일 액세스 감사를 언제든지 비활성화할 수도 있습니다.

> **Note**
>
> 파일 액세스 감사는 활성화된 시점부터 최종 사용자 액세스 데이터만 기록합니다. 즉, 파일 액세스 감사에서는 파일 액세스 감사가 활성화되기 전에 발생한 최종 사용자 파일, 폴더 및 파일 공유 액세스 활동에 대한 감사 이벤트 로그를 생성하지 않습니다.

지원되는 액세스 감사 이벤트의 최대 비율은 초당 5,000개 이벤트입니다. 액세스 감사 이벤트는 각 파일 읽기 및 쓰기 작업에 대해 생성되지 않고 파일 메타데이터 작업마다(예: 사용자가 파일을 만들거나 열거나 삭제할 때) 한 번씩 생성됩니다.

주제

- 파일 액세스 감사 관리

감사 이벤트 로그 대상

파일 액세스 감사를 활성화할 때는 Amazon FSx가 감사 AWS 이벤트 로그를 전송할 서비스를 구성해야 합니다. 감사 이벤트 로그는 로그 로그 그룹의 Amazon CloudWatch Logs 로그 스트림 또는 Amazon Data Firehose 전송 스트림으로 보낼 수 있습니다. CloudWatch 감사 이벤트 로그 대상은 Windows File Server용 Amazon FSx 파일 시스템을 생성할 때 또는 기존 파일 시스템을 업데이트한 후 언제든지 선택할 수 있습니다. 자세한 정보는 파일 액세스 감사 관리을 참조하세요.

다음은 어떤 감사 이벤트 로그 대상을 선택할지 결정하는 데 도움이 될 수 있는 몇 가지 권장 사항입니다.

- Amazon CloudWatch 콘솔에서 감사 이벤트 CloudWatch 로그를 저장, 확인 및 검색하고, Logs Insights를 사용하여 로그에 대한 쿼리를 실행하고, CloudWatch 경보 또는 Lambda 함수를 트리거하려면 [CloudWatch Logs] 를 선택합니다.
- 추가 분석을 위해 Amazon S3의 스토리지, Amazon Redshift의 데이터베이스, OpenSearch Amazon 서비스 또는 파트너 솔루션 (예: Splunk 또는 Datadog) 으로 이벤트를 지속적으로 AWS 스트리밍하려면 Firehose를 선택하십시오.

기본적으로 Amazon FSx는 계정에 CloudWatch 기본 로그 로그 그룹을 생성하여 감사 이벤트 로그 대상으로 사용합니다. 사용자 지정 로그 CloudWatch 로그 그룹을 사용하거나 Firehose를 감사 이벤트 로그 대상으로 사용하려는 경우 감사 이벤트 로그 대상의 이름 및 위치에 대한 요구 사항은 다음과 같습니다.

- 로그 CloudWatch 로그 그룹의 이름은 `/aws/fsx/` 접두사로 시작해야 합니다. 콘솔에서 파일 시스템을 생성하거나 업데이트할 때 기존 CloudWatch 로그 로그 그룹이 없는 경우, Amazon FSx는 로그 로그 그룹에 기본 로그 스트림을 생성하고 사용할 수 있습니다. CloudWatch `/aws/fsx/windows` 기본 로그 그룹을 사용하지 않으려는 경우 콘솔에서 파일 시스템을 생성하거나 업데이트할 때 구성 UI를 사용하여 CloudWatch 로그 로그 그룹을 생성할 수 있습니다.
- Firehose 전송 스트림의 이름은 접두사로 시작해야 합니다. `aws-fsx-` 기존 Firehose 전송 스트림이 없는 경우 콘솔에서 파일 시스템을 만들거나 업데이트할 때 전송 스트림을 만들 수 있습니다.
- Firehose 전송 스트림을 `Direct PUT` 소스로 사용하도록 구성해야 합니다. 기존 Kinesis 데이터 스트림은 전송 스트림의 데이터 소스로 사용할 수 없습니다.
- 대상 (로그 CloudWatch 로그 그룹 또는 Firehose 전송 스트림) 은 Amazon FSx 파일 시스템과 AWS 계정 동일한 AWS 파티션에 있어야 합니다. AWS 리전

감사 이벤트 로그 대상은 언제든지 변경할 수 있습니다 (예: CloudWatch Logs에서 Firehose로). 이렇게 하면 새 감사 이벤트 로그가 새 대상으로만 전송됩니다.

최선의 감사 이벤트 로그 전송

일반적으로 감사 이벤트 로그 레코드는 몇 분 안에 대상에 전달되지만 때로는 더 오래 걸릴 수도 있습니다. 아주 드문 경우지만 감사 이벤트 로그 기록이 누락될 수 있습니다. 사용 사례에 특정 의미 체계 (예: 누락된 감사 이벤트가 없는지 확인)가 필요한 경우 워크플로를 설계할 때 누락된 이벤트를 고려하는 것이 좋습니다. 파일 시스템의 파일 및 폴더 구조를 검사하여 누락된 이벤트가 있는지 감사할 수 있습니다.

감사 제어 마이그레이션

기존 파일 데이터에 감사 제어(SACL)가 이미 설정되어 있는 경우, Amazon FSx 파일 시스템을 생성하고 데이터를 새 파일 시스템으로 마이그레이션할 수 있습니다. 데이터 및 관련 SACL을 Amazon FSx 파일 시스템으로 전송하는 AWS DataSync 데 사용하는 것이 좋습니다. 대체 솔루션으로는 Robocopy(Robust File Copy)를 사용할 수 있습니다. 자세한 정보는 기존 파일 스토리지를 Amazon FSx로 마이그레이션을 참조하세요.

감사 로그 보기

Amazon FSx에서 감사 이벤트 로그를 생성하기 시작한 후에 감사 이벤트 로그를 볼 수 있습니다. 로그를 보는 위치 및 방법은 감사 이벤트 로그 대상에 따라 다릅니다.

- CloudWatch 콘솔로 이동하여 감사 이벤트 로그가 전송되는 로그 그룹과 로그 스트림을 선택하면 로그 CloudWatch 로그를 볼 수 있습니다. 자세한 내용은 Amazon Logs 사용 설명서의 CloudWatch Logs로 전송된 CloudWatch 로그 데이터 보기를 참조하십시오.

  CloudWatch Logs Insights를 사용하여 대화형 방식으로 로그 데이터를 검색하고 분석할 수 있습니다. 자세한 내용은 Amazon Logs 사용 설명서의 CloudWatch Logs Insights를 사용한 CloudWatch 로그 데이터 분석을 참조하십시오.

  또한 감사 이벤트 로그를 Amazon S3로 내보낼 수 있습니다. 자세한 내용은 Amazon Logs 사용 설명서의 Amazon S3로 CloudWatch 로그 데이터 내보내기를 참조하십시오.
- Firehose에서는 감사 이벤트 로그를 볼 수 없습니다. 하지만 로그를 읽을 수 있는 대상으로 전달하도록 Firehose를 구성할 수 있습니다. 대상에는 Amazon S3, Amazon Redshift, Amazon OpenSearch Service와 Splunk 및 Datadog와 같은 파트너 솔루션이 포함됩니다. 자세한 내용은 Amazon Data Firehose 개발자 안내서의 대상 선택을 참조하십시오.

감사 이벤트 필드

이 섹션에서는 감사 이벤트 로그의 정보에 대한 설명과, 감사 이벤트의 예제를 제공합니다.

다음은 Windows 감사 이벤트의 주요 필드에 대한 설명입니다.

- EventID는 Microsoft가 정의한 Windows 이벤트 로그 이벤트 ID를 나타냅니다. 파일 시스템 이벤트 및 파일 공유 이벤트에 대한 자세한 내용은 Microsoft 설명서를 참조하세요.
- SubjectUserName액세스를 수행하는 사용자를 말합니다.
- ObjectName액세스한 대상 파일, 폴더 또는 파일 공유를 나타냅니다.
- ShareName파일 공유 액세스를 위해 생성된 이벤트에 사용할 수 있습니다. 예를 들어, 네트워크 공유 객체에 액세스할 때 `EventID 5140`이 생성됩니다.
- IpAddress파일 공유 이벤트에 대한 이벤트를 시작한 클라이언트를 나타냅니다.
- Keywords(사용 가능한 경우)는 파일 액세스의 성공 또는 실패 여부를 나타냅니다. 성공한 액세스의 경우 값은 `0x8020000000000000`입니다. 실패한 액세스의 경우 값은 `0x8010000000000000`입니다.
- TimeCreated SystemTime이벤트가 시스템에서 생성되고 <YYYY-MM-DDThh:mm:ss.s>Z 형식으로 표시된 시간을 나타냅니다.
- 컴퓨터는 파일 시스템 Windows 원격 PowerShell 엔드포인트의 DNS 이름을 말하며 파일 시스템을 식별하는 데 사용할 수 있습니다.
- AccessMask, 사용 가능한 경우 수행된 파일 액세스 유형 (예: WriteData) 을 나타냅니다. ReadData
- AccessList객체에 대한 요청 또는 부여된 액세스 권한을 나타냅니다. 자세한 내용은 아래 표와 Microsoft 설명서(예: 이벤트 4556)를 참조하세요.

액세스 유형	액세스 마스크	값
데이터 읽기 또는 디렉터리 나열	0x1	%%4416
데이터 쓰기 또는 파일 추가	0x2	%%4417
데이터 추가 또는 하위 디렉터리 추가	0x4	%%4418
확장 속성 읽기	0x8	%%4419

액세스 유형	액세스 마스크	값
확장 속성 쓰기	0x10	%%4420
실행/트래버스	0x20	%%4421
하위 삭제	0x40	%%4422
속성 읽기	0x80	%%4423
속성 쓰기	0x100	%%4424
삭제	0x10000	%%1537
ACL 읽기	0x20000	%%1538
ACL 쓰기	0x40000	%%1539
소유자 쓰기	0x80000	%%1540
동기화	0x100000	%%1541
액세스 보안 ACL	0x1000000	%%1542

다음은 몇 가지 주요 이벤트와 예제입니다. XML은 가독성을 위해 형식이 지정되어 있습니다.

객체 삭제 시 이벤트 ID 4660이 로깅됩니다.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4660</EventID><Version>0</Version><Level>0</Level>
<Task>12800</Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-05-18T04:51:56.916563800Z'/>
<EventRecordID>315452</EventRecordID><Correlation/>
<Execution ProcessID='4' ThreadID='5636'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x50932f71</Data><Data Name='ObjectServer'>Security</Data>
```

```
<Data Name='HandleId'>0x12e0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data></EventData></
Event>
```

파일 삭제 요청 시 이벤트 ID 4659가 로깅됩니다.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4659</EventID><Version>0</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-0603T19:18:09.951551200Z'/>
<EventRecordID>308888</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5540'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device\HarddiskVolume8\shar
\event.txt</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1537
    %%4423
    </Data><Data Name='AccessMask'>0x10080</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='ProcessId'>0x4</Data></EventData></Event>
```

객체에 특정 작업이 수행되면 이벤트 ID 4663이 로깅됩니다. 다음은 파일에서 데이터를 읽는 예제입니다(AccessList %%4416에서 해석 가능).

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663< /EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:10:13.887145400Z'/>
<EventRecordID>308831</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='6916'/>
```

```
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData>< Data
 Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113< /Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0x101c</Data><Data Name='AccessList'>%%4416
    </Data>
<Data Name='AccessMask'>0x1</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data>
</EventData></Event>
```

다음은 파일에서 데이터를 읽고 추가하는 예제입니다(AccessList %%4417에서 해석 가능).

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4663</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:12:16.813827100Z'/>
<EventRecordID>308838</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='5828'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\event.txt</Data>
<Data Name='HandleId'>0xa38</Data><Data Name='AccessList'>%%4417
    </Data><Data Name='AccessMask'>0x2</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data><Data Name='ResourceAttributes'>S:AI</Data></
EventData></Event>
```

이벤트 ID 4656은 객체에 대해 특정 액세스가 요청되었음을 나타냅니다. 다음 예제에서는 키워드 값에서 볼 수 있듯이 읽기 요청이 ObjectName “permtest”로 시작되었지만 실패한 시도였습니다. 0x8010000000000000

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4656</EventID><Version>1</Version><Level>0</Level><Task>12800</
Task><Opcode>0</Opcode>
<Keywords>0x8010000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:22:55.113783500Z'/>
<EventRecordID>308919</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='4924'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</
Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0x0</Data><Data
 Name='TransactionId'>{00000000-0000-0000-0000-000000000000}</Data>
<Data Name='AccessList'>%%1541
    %%4416
    %%4423
    </Data><Data Name='AccessReason'>%%1541: %%1805
    %%4416: %%1805
    %%4423: %%1811 D:(A;OICI;0x1301bf;;;AU)
    </Data><Data Name='AccessMask'>0x100081</Data><Data Name='PrivilegeList'>-</Data>
<Data Name='RestrictedSidCount'>0</Data><Data Name='ProcessId'>0x4</Data><Data
 Name='ProcessName'></Data>
<Data Name='ResourceAttributes'>-</Data></EventData></Event>
```

객체에 대한 권한이 변경되면 이벤트 ID 4670이 로깅됩니다. 다음 예에서는 사용자 “admin”이 “permtest”의 권한을 수정하여 “ ObjectName S-1-5-21-658495921-4185342820-3824891517-1113" SID에 권한을 추가했음을 보여줍니다. 권한을 해석하는 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하세요.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>4670</EventID><Version>0</Version><Level>0</Level>
<Task>13570</Task><Opcode>0</Opcode><Keywords>0x8020000000000000</Keywords>
<TimeCreated SystemTime='2021-06-03T19:39:47.537129500Z'/><EventRecordID>308992</
EventRecordID>
```

```
<Correlation/><Execution ProcessID='4' ThreadID='2776'/><Channel>Security</Channel>
<Computer>amznfsxgyzohmw8.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-1113</Data>
<Data Name='SubjectUserName'>Admin</Data><Data Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2a9a603f</Data><Data Name='ObjectServer'>Security</Data>
<Data Name='ObjectType'>File</Data><Data Name='ObjectName'>\Device
\HarddiskVolume8\share\permtest</Data>
<Data Name='HandleId'>0xcc8</Data>
<Data Name='OldSd'>D:PAI(A;OICI;FA;;;SY)
(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-2622)</Data>
<Data Name='NewSd'>D:PARAI(A;OICI;FA;;;S-1-5-21-658495921-4185342820-3824891517-1113)
(A;OICI;FA;;;SY)(A;OICI;FA;;;
S-1-5-21-658495921-4185342820-3824891517-2622)</Data><Data Name='ProcessId'>0x4</Data>
<Data Name='ProcessName'></Data></EventData></Event>
```

이벤트 ID 5140은 파일 공유에 액세스할 때마다 로깅됩니다.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5140</EventID><Version>1</Version><Level>0</Level><Task>12808</
Task><Opcode>0</Opcode>
<Keywords>0x8020000000000000</Keywords><TimeCreated
 SystemTime='2021-06-03T19:32:07.535208200Z'/>
<EventRecordID>308947</EventRecordID><Correlation/><Execution ProcessID='4'
 ThreadID='3120'/>
<Channel>Security</Channel><Computer>amznfsxgyzohmw8.example.com</Computer><Security/
></System>
<EventData><Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-2620</
Data>
<Data Name='SubjectUserName'>EC2AMAZ-1GP4HMN$</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x2d4ca529</Data><Data Name='ObjectType'>File</Data><Data
 Name='IpAddress'>172.45.6.789</Data>
<Data Name='IpPort'>49730</Data><Data Name='ShareName'>\\AMZNFSXCYDKLDZZ\share</Data>
<Data Name='ShareLocalPath'>\??\D:\share</Data><Data Name='AccessMask'>0x1</Data><Data
 Name='AccessList'>%%4416
    </Data></EventData></Event>
```

파일 공유 수준에서 액세스가 거부되면 이벤트 ID 5145가 로깅됩니다. 다음 예는 ShareName “demoshare01"에 대한 액세스가 거부되었음을 보여줍니다.

```
<Event xmlns='http://schemas.microsoft.com/win/2004/08/events/event'><System>
```

```
<Provider Name='Microsoft-Windows-Security-Auditing' Guid='{54849625-5478-4994-
A5BA-3E3B0328C30D}'/>
<EventID>5145</EventID><Version>0</Version><Level>0</Level>
<Task>12811</Task><Opcode>0</Opcode><Keywords>0x8010000000000000</Keywords>
<TimeCreated SystemTime='2021-05-19T22:30:40.485188700Z'/><EventRecordID>282939</
EventRecordID>
<Correlation/><Execution ProcessID='4' ThreadID='344'/><Channel>Security</Channel>
<Computer>amznfsxtmn9autz.example.com</Computer><Security/></System><EventData>
<Data Name='SubjectUserSid'>S-1-5-21-658495921-4185342820-3824891517-
1113</Data><Data Name='SubjectUserName'>Admin</Data><Data
 Name='SubjectDomainName'>example</Data>
<Data Name='SubjectLogonId'>0x95b3fb7</Data><Data Name='ObjectType'>File</Data>
<Data Name='IpAddress'>172.31.7.112</Data><Data Name='IpPort'>59979</Data>
<Data Name='ShareName'>\\AMZNFSXDPNTE0DC\demoshare01</Data><Data Name='ShareLocalPath'>
\??\D:\demoshare01</Data>
<Data Name='RelativeTargetName'>Desktop.ini</Data><Data Name='AccessMask'>0x120089</
Data>
<Data Name='AccessList'>%%1538 %%1541 %%4416 %%4419 %%4423 </Data><Data
 Name='AccessReason'>%%1538:
%%1804 %%1541: %%1805 %%4416: %%1805 %%4419: %%1805 %%4423: %%1805 </Data></
EventData></Event>
```

CloudWatch Logs Insights를 사용하여 로그 데이터를 검색하는 경우 다음 예와 같이 이벤트 필드에서 쿼리를 실행할 수 있습니다.

- 특정 이벤트 ID 쿼리:

```
fields @message
   | filter @message like /4660/
```

- 특정 파일 이름과 일치하는 모든 이벤트 쿼리:

```
fields @message
   | filter @message like /event.txt/
```

CloudWatch Logs Insights 쿼리 언어에 대한 자세한 내용은 Amazon Logs 사용 설명서의 Logs Insights를 사용한 CloudWatch CloudWatch 로그 데이터 분석을 참조하십시오.

파일 및 폴더 감사 제어 설정

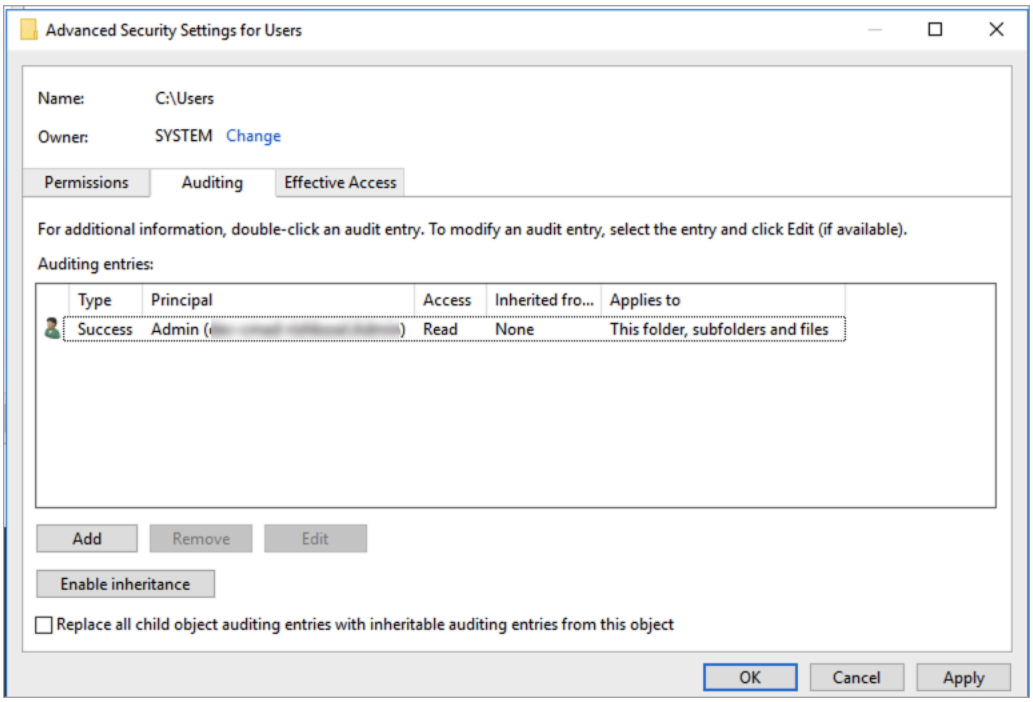
사용자 액세스 시도에 대해 감사할 파일 및 폴더에 감사 제어를 설정해야 합니다. 감사 제어는 NTFS 시스템 액세스 제어 목록(SACL)이라고도 합니다.

Windows 네이티브 GUI 인터페이스를 사용하거나 Windows 명령을 사용하여 프로그래밍 방식으로 감사 제어를 구성합니다. PowerShell 상속을 활성화한 경우 일반적으로 액세스를 로깅하려는 최상위 폴더에만 감사 제어를 설정해야 합니다.

Windows GUI를 사용하여 감사 액세스 설정

GUI를 사용하여 파일 및 폴더에 감사 제어를 설정하려면 Windows 파일 탐색기를 사용합니다. 지정된 파일 또는 폴더에서 Windows 파일 탐색기를 열고 속성 > 보안 > 고급 > 감사 탭을 선택합니다.

다음 감사 제어 예제는 폴더의 성공 이벤트를 감사합니다. Windows 이벤트 로그 항목은 관리자 사용자가 해당 핸들을 성공적으로 열어서 읽을 때마다 생성됩니다.



유형 필드에는 감사하려는 작업이 표시됩니다. 성공한 시도를 감사하려면 이 필드를 성공으로 설정하고, 실패한 시도를 감사하려면 실패로 설정하고, 성공한 시도와 실패한 시도를 모두 감사하려면 모두로 설정합니다.

감사 항목 필드에 대한 자세한 내용은 Microsoft 설명서의 파일 또는 폴더에 기본 감사 정책 적용을 참조하세요.

명령을 사용하여 감사 액세스 설정 PowerShell

Microsoft Windows `Set-Acl` 명령을 사용하여 모든 파일 또는 폴더에 감사 SACL을 설정할 수 있습니다. 이 명령에 대한 자세한 내용은 Microsoft Set-Acl 설명서를 참조하세요.

다음은 일련의 PowerShell 명령과 변수를 사용하여 성공적인 시도에 대한 감사 액세스를 설정하는 예제입니다. 이 예제 명령을 파일 시스템의 요구 사항에 맞게 조정할 수 있습니다.

```
$path = "C:\Users\TestUser\Desktop\DemoTest\"

$ACL = Get-Acl $path

$ACL | Format-List

$AuditUser = "TESTDOMAIN\TestUser"

$AuditRules = "FullControl"

$InheritType = "ContainerInherit,ObjectInherit"

$AuditType = "Success"

$AccessRule = New-Object System.Security.AccessControl.FileSystemAuditRule($AuditUser,
$AuditRules,$InheritType,"None",$AuditType)

$ACL.SetAuditRule($AccessRule)

$ACL | Set-Acl $path

Get-Acl $path -Audit | Format-List
```

파일 액세스 감사 관리

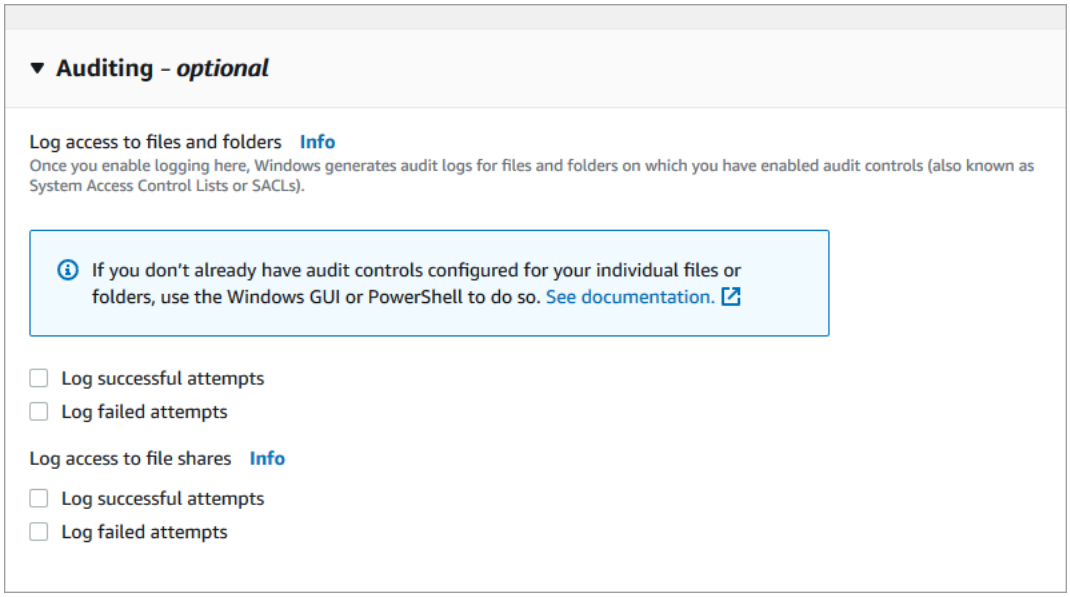
새로운 Amazon FSx for Windows File Server 파일 시스템을 만들 때 파일 액세스 감사를 활성화할 수 있습니다. Amazon FSx 콘솔에서 파일 시스템을 생성하면 파일 액세스 감사가 기본적으로 비활성화됩니다.

파일 액세스 감사가 활성화된 기존 파일 시스템에서는 파일 및 파일 공유 액세스에 대한 액세스 시도 유형 및 감사 이벤트 로그 대상 변경을 포함하여 파일 액세스 감사 설정을 변경할 수 있습니다. Amazon FSx 콘솔 AWS CLI또는 API를 사용하여 이러한 작업을 수행할 수 있습니다.

> **Note**
>
> 파일 액세스 감사는 처리량 용량이 32MB/s 이상인 Amazon FSx for Windows File Server 파일 시스템에서만 지원됩니다. 파일 액세스 감사가 활성화된 경우 처리량 용량이 32MB/s 미만인 파일 시스템을 생성하거나 업데이트할 수 없습니다. 파일 시스템을 생성하고 나서 언제든지 필요에 따라 처리량 용량을 수정할 수 있습니다. 자세한 정보는 처리량 용량 관리을 참조하세요.

파일 시스템을 만들 때 파일 액세스 감사 활성화(콘솔)

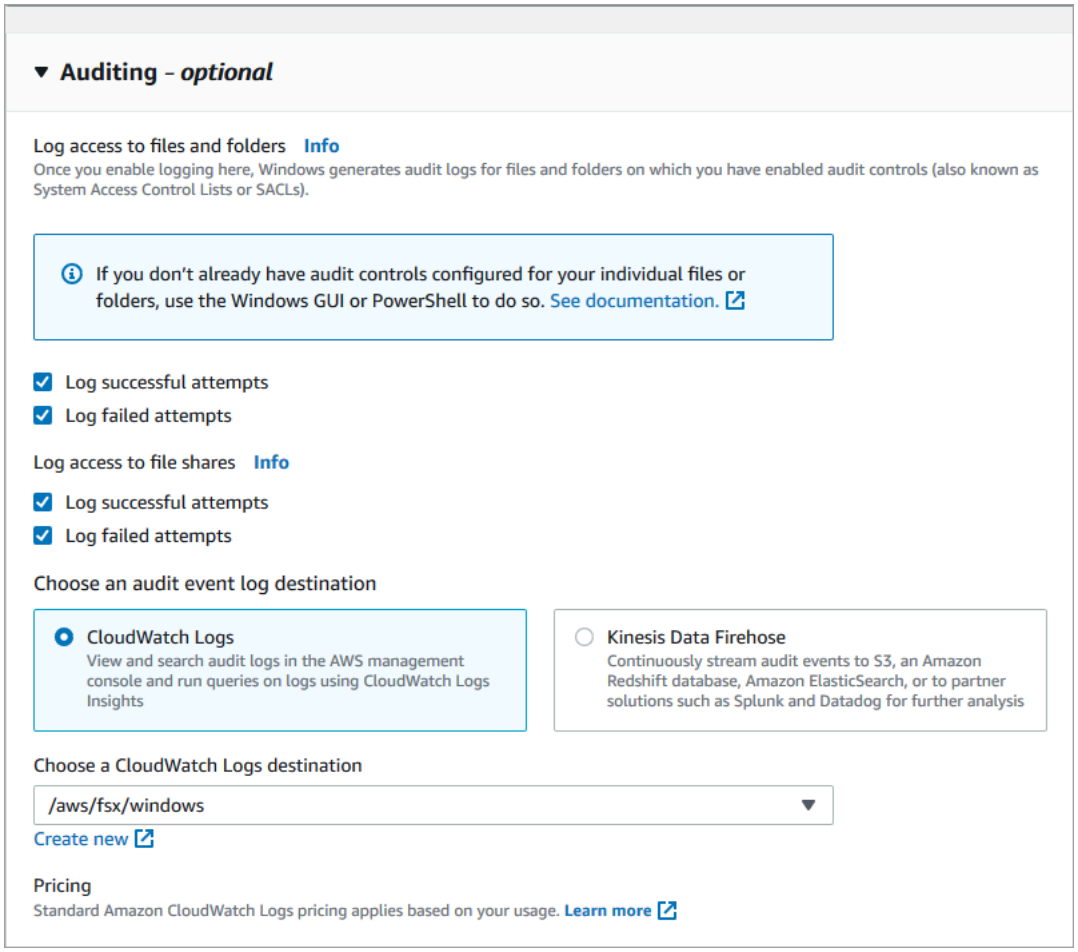
1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 시작하기 섹션의 파일 시스템 생성 섹션에 설명된 새 파일 시스템 생성 절차를 따릅니다.
3. 감사 - 선택 사항 섹션을 엽니다. 파일 액세스 감사는 기본적으로 비활성화되어 있습니다.



4. 파일 액세스 감사를 활성화하고 구성하려면 다음과 같이 합니다.

   - 파일 및 폴더에 대한 액세스 로깅에서 성공 및 실패 시도의 로깅을 선택합니다. 선택하지 않으면 파일 및 폴더에 대한 로깅이 비활성화됩니다.
   - 파일 공유에 대한 액세스 로깅에서 성공 및 실패 시도의 로깅을 선택합니다. 선택하지 않으면 파일 공유에 대한 로깅이 비활성화됩니다.
   - 감사 이벤트 로그 대상 선택에서 CloudWatch Logs 또는 Firehose를 선택합니다. 그런 다음 기존 로그 또는 전송 스트림을 선택하거나, 새로 생성합니다. CloudWatch 로그의 경우, Amazon FSx는 로그 로그 그룹에서 CloudWatch 기본 로그 스트림을 생성하고 사용할 수 있습니다. `/aws/fsx/windows`

다음은 파일, 폴더 및 파일 공유에 대한 최종 사용자의 성공 및 실패 액세스를 감사하는 파일 액세스 감사 구성의 예제입니다. 감사 이벤트 로그는 기본 로그 CloudWatch `/aws/fsx/windows` 로그 그룹 대상으로 전송됩니다.



5. 파일 시스템 생성 마법사의 다음 섹션으로 계속 진행합니다.

파일 시스템이 사용 가능 상태이면 파일 액세스 감사 기능이 활성화됩니다.

파일 시스템을 만들 때 파일 액세스 감사 활성화(CLI)

1. 새 파일 시스템을 생성할 때 CreateFileSystemAPI 작업과 함께 `AuditLogConfiguration` 속성을 사용하여 새 파일 시스템에 대한 파일 액세스 감사를 활성화하십시오.

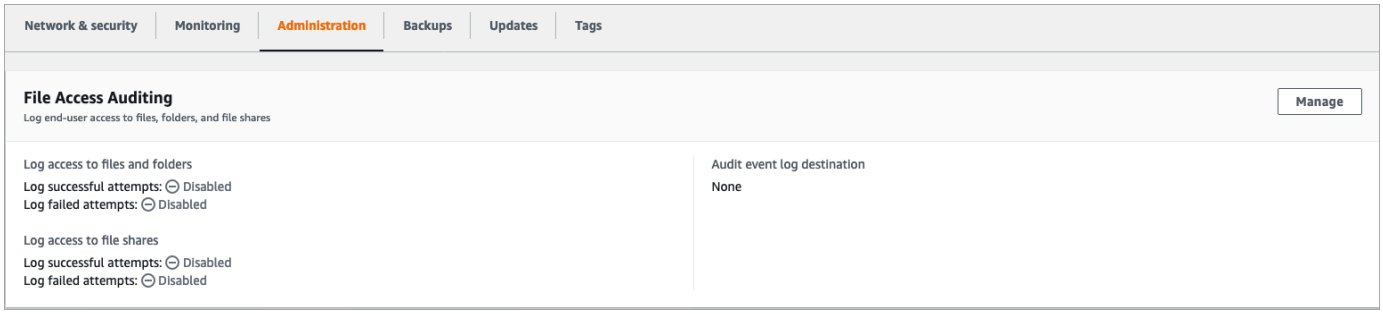
```
aws fsx create-file-system \
  --file-system-type WINDOWS \
  --storage-capacity 300 \
  --subnet-ids subnet-123456 \
```

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    FileShareAccessAuditLogLevel="SUCCESS_AND_FAILURE", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

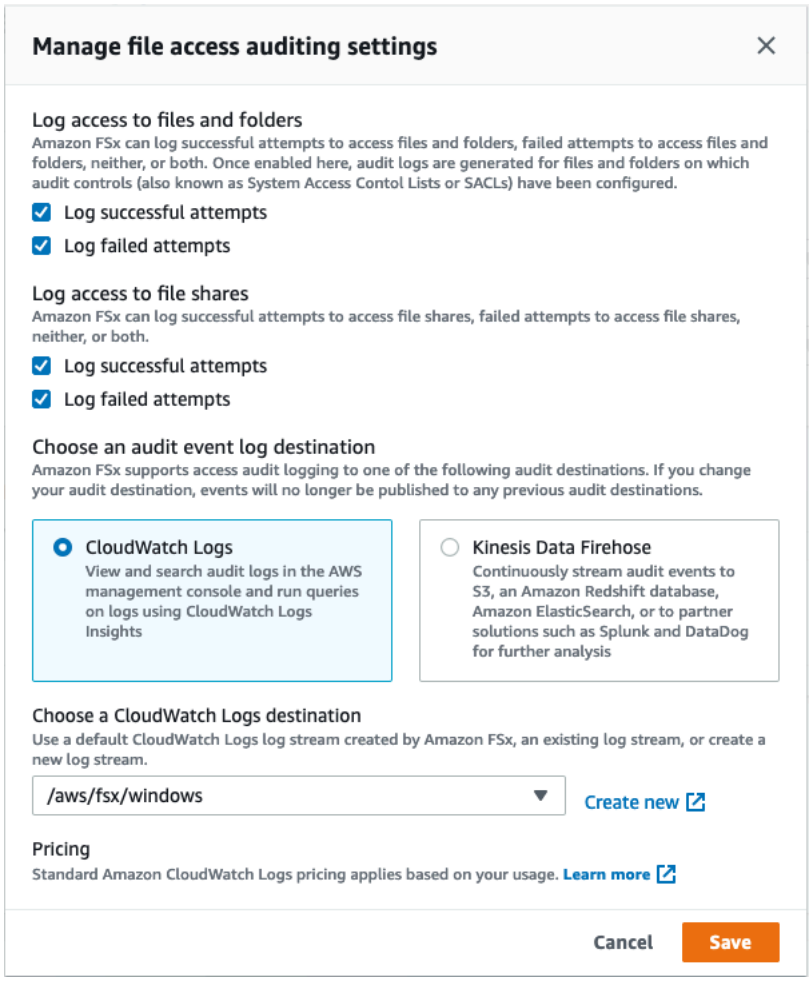
2. 파일 시스템이 사용 가능 상태이면 파일 액세스 감사 기능이 활성화됩니다.

파일 액세스 감사 구성 변경(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 파일 액세스 감사를 관리할 Windows 파일 시스템을 선택합니다.
3. 관리 탭을 선택합니다.
4. 파일 액세스 감사 패널에서 관리를 선택합니다.



5. 파일 액세스 감사 설정 관리 대화 상자에서 원하는 설정을 변경합니다.



- 파일 및 폴더에 대한 액세스 로깅에서 성공 및 실패 시도의 로깅을 선택합니다. 선택하지 않으면 파일 및 폴더에 대한 로깅이 비활성화됩니다.
- 파일 공유에 대한 액세스 로깅에서 성공 및 실패 시도의 로깅을 선택합니다. 선택하지 않으면 파일 공유에 대한 로깅이 비활성화됩니다.
- 감사 이벤트 로그 대상 선택에서 CloudWatch Logs 또는 Firehose를 선택합니다. 그런 다음 기존 로그 또는 전송 스트림을 선택하거나, 새로 생성합니다.

6. 저장을 선택합니다.

파일 액세스 감사 구성 변경(CLI)

- update-file-system CLI 명령 또는 이에 상응하는 UpdateFileSystem API 작업을 사용합니다.

```
aws fsx update-file-system \
  --file-system-id fs-0123456789abcdef0 \
```

```
  --windows-configuration
 AuditLogConfiguration='{FileAccessAuditLogLevel="SUCCESS_ONLY", \
    FileShareAccessAuditLogLevel="FAILURE_ONLY", \
    AuditLogDestination="arn:aws:logs:us-east-1:123456789012:log-group:/aws/fsx/my-
customer-log-group"}'
```

사용자 세션 및 열린 파일

이제 공유 폴더 도구를 사용하여 FSx for Windows File Server 파일 시스템에서 연결된 사용자 세션과 열린 파일을 모니터링할 수 있습니다. 공유 폴더 도구를 사용하면 파일 시스템에 누가 연결되어 있는지, 어떤 파일을 누가 열었는지와 함께 중앙에서 모니터링할 수 있습니다. 이 도구를 사용하여 다음을 수행할 수 있습니다.

- 잠긴 파일에 대한 액세스 복원.
- 사용자 세션 연결을 해제하여 해당 사용자가 연 모든 파일 닫기.

Windows 네이티브 공유 폴더 GUI 도구와 원격 관리를 위한 Amazon FSx CLI를 사용하여 Windows용 FSx 파일 시스템에서 PowerShell 사용자 세션을 관리하고 파일을 열 수 있습니다.

GUI를 사용하여 사용자 및 세션 관리

다음 절차는 Microsoft Windows 공유 폴더 도구를 사용하여 Amazon FSx 파일 시스템에서 사용자 세션을 관리하고 파일을 여는 방법을 자세히 설명합니다.

공유 폴더 도구 시작하기

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.

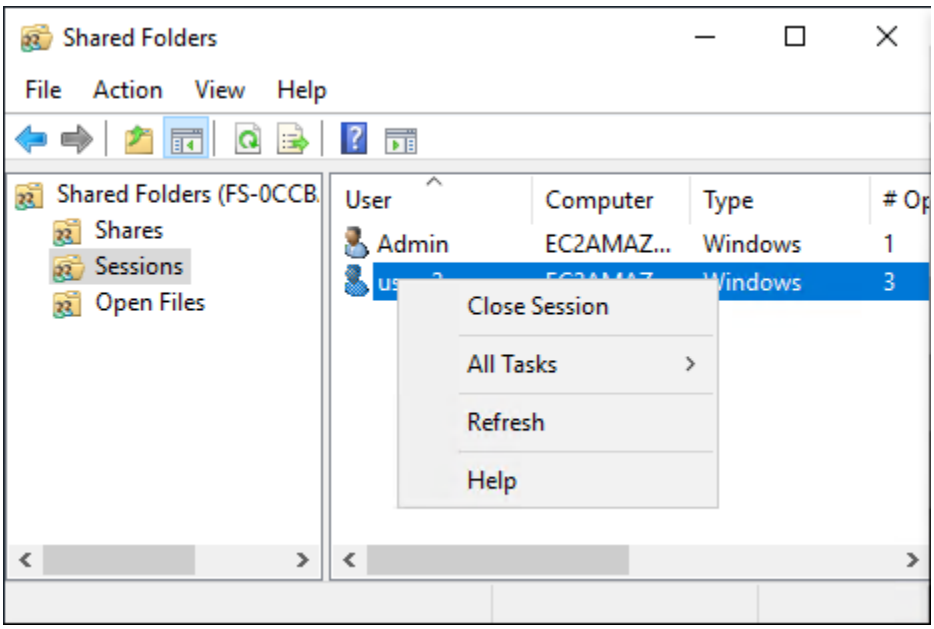
   - Windows EC2 인스턴스를 원활하게 조인
   - Windows 인스턴스를 수동으로 조인

2. 파일 시스템 관리자 그룹의 구성원인 사용자로 인스턴스에 연결합니다. AWS 관리형 Microsoft Active Directory에서는 이 그룹을 AWS 위임 FSx 관리자라고 합니다. 자체 관리형 Microsoft Active Directory에서는 이 그룹을 도메인 관리자 또는 생성 시 제공한 관리자 그룹의 사용자 지정 이름이라고 합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

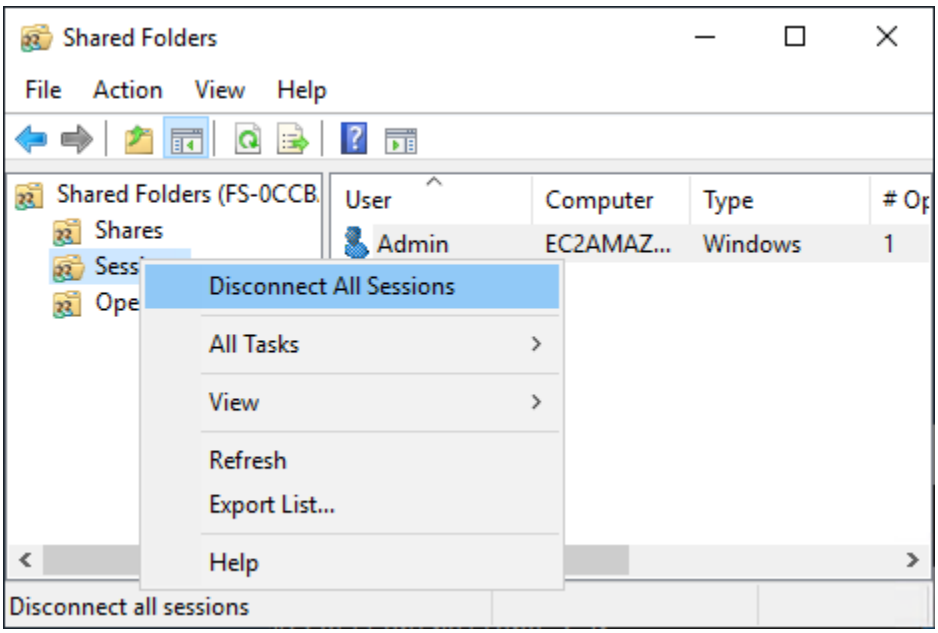
3. 시작 메뉴를 열고 `Run As Administrator`를 사용하여 fsmgmt.msc를 실행합니다. 이렇게 하면 공유 폴더 GUI 도구가 열립니다.
4. 작업에서 다른 컴퓨터에 연결을 선택합니다.
5. 다른 컴퓨터에 Amazon FSx 파일 시스템의 DNS 이름(예: `fs-01234567890123456.ad-domain.com`)을 입력합니다.
6. 확인을 선택합니다. 그러면 Amazon FSx 파일 시스템 항목이 공유 폴더 도구 목록에 표시됩니다.

사용자 세션 (GUI) 을 관리하려면

공유 폴더 도구에서 세션을 선택하여 FSx for Windows File Server 파일 시스템에 연결된 모든 사용자 세션을 확인합니다. 사용자 또는 애플리케이션이 Amazon FSx 파일 시스템의 파일 공유에 액세스하는 경우 이 스냅인은 해당 세션을 보여줍니다. 세션의 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) 세션 닫기를 선택하여 세션 연결을 해제할 수 있습니다.

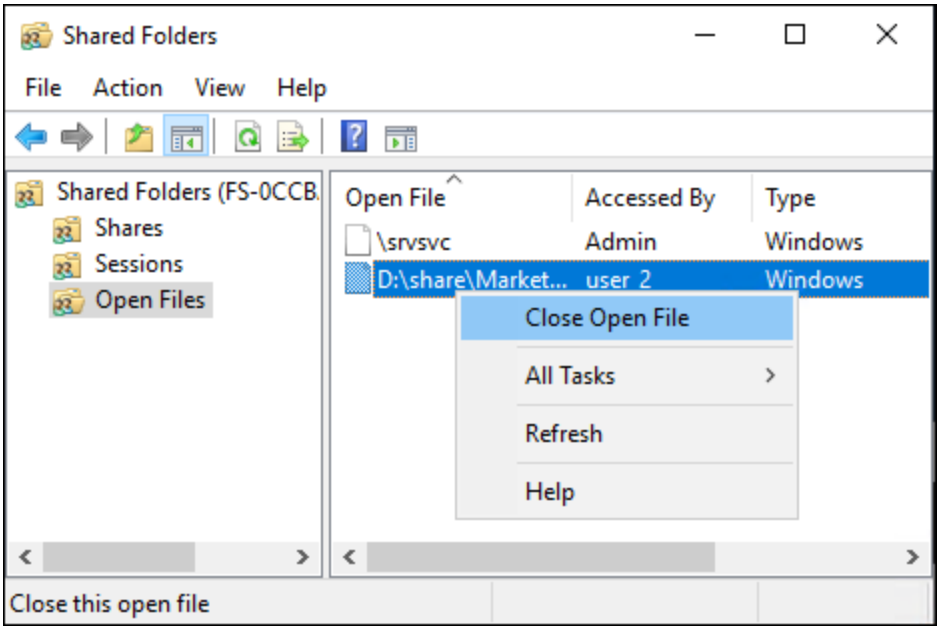


열려 있는 모든 세션의 연결을 해제하려면 세션의 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) 모든 세션 연결 해제를 선택한 후 작업을 확인합니다.

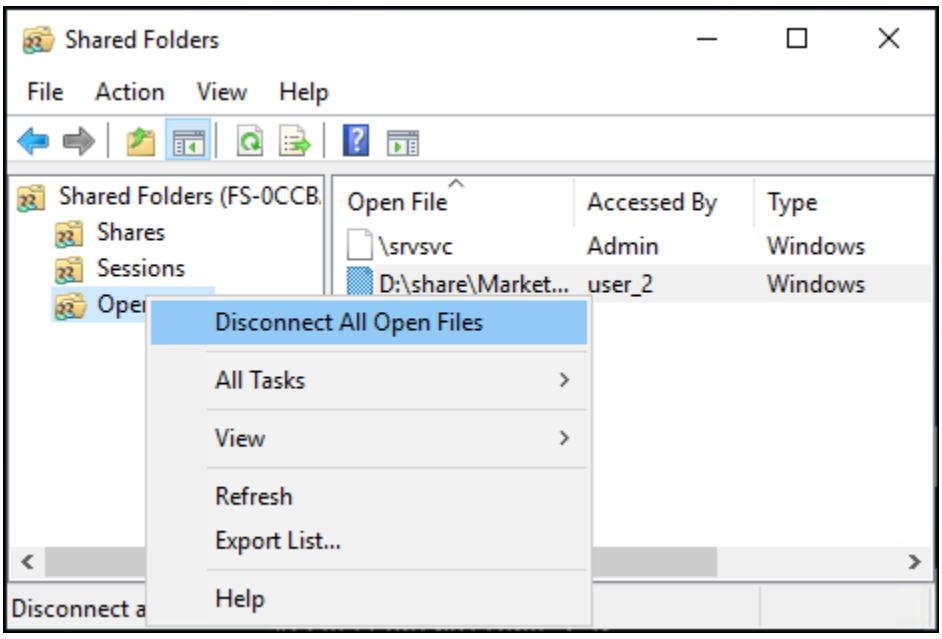


열린 파일 (GUI) 관리하기

공유 폴더 도구에서 열린 파일을 선택하여 시스템에서 현재 열려 있는 모든 파일을 확인합니다. 이 뷰에는 파일이나 폴더를 연 사용자도 표시됩니다. 이 정보는 다른 사용자가 특정 파일을 열 수 없는 이유를 추적하는 데 유용할 수 있습니다. 목록에 있는 파일 항목의 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) 열린 파일 닫기를 선택하여 사용자가 열어 놓은 파일을 모두 닫을 수 있습니다.



파일 시스템에서 열려 있는 모든 파일의 연결을 끊으려면 열린 파일의 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) 열린 파일 모두 연결 해제를 선택한 다음 작업을 확인합니다.



사용자 세션을 관리하고 파일을 여는 PowerShell 데 사용

원격 관리용 Amazon FSx CLI를 사용하여 파일 시스템에서 활성 사용자 세션을 관리하고 파일을 열 수 있습니다. PowerShell 이 CLI를 사용하는 방법을 알아보려면 아마존 FSx CLI를 사용하는 방법 PowerShell 섹션을 참조하세요.

다음은 사용자 세션 및 열린 파일 관리에 사용할 수 있는 명령입니다.

Command	설명
Get-FSxSmbSession	파일 시스템과 관련 클라이언트 간에 현재 설정된 Server Message Block(SMB) 세션에 대한 정보를 검색합니다.
Close-FSxSmbSession	SMB 세션을 종료합니다.
Get-FSxSmbOpenFile	파일 시스템에 연결된 클라이언트에 대해 열려 있는 파일에 대한 정보를 검색합니다.
Close-FSxSmbOpenFile	SMB 서버의 클라이언트 중 하나에 대해 열려 있는 파일을 닫습니다.

각 명령의 온라인 도움말은 모든 명령 옵션에 대한 참조를 제공합니다. 이 도움말에 액세스하려면 -?(예: Get-FSxSmbSession -?)와 함께 명령을 실행합니다.

데이터 중복 제거

FSx는 Microsoft 데이터 중복 제거를 사용하여 중복 데이터를 식별하고 제거할 수 있도록 지원합니다. 대규모 데이터 세트에는 종종 데이터가 중복되어 있어 데이터 스토리지 비용이 증가합니다. 예를 들어 사용자 파일 공유에는 여러 사용자가 저장하는 동일한 파일의 사본 또는 버전이 여러 개 있을 수 있습니다. 소프트웨어 개발 공유에는 빌드마다 변경되지 않는 바이너리가 많이 남아 있을 수 있습니다.

파일 시스템에서 데이터 중복 제거를 활성화하여 데이터 스토리지 비용을 줄일 수 있습니다. 데이터 중복 제거가 데이터 세트의 중복된 부분을 한 번만 저장하여 중복 데이터를 자동으로 줄이거나 제거합니다. 데이터 중복 제거를 사용하면 기본적으로 데이터 압축이 활성화되며, 중복 제거 후 데이터를 압축하여 데이터 스토리지의 양을 더욱 줄일 수 있습니다. 데이터 중복 제거는 파일 시스템을 지속적으로 자동 스캔하고 최적화하는 백그라운드 프로세스로 실행되며 사용자와 연결된 클라이언트에 영향을 미치지 않습니다.

데이터 중복 제거로 얻을 수 있는 스토리지 절감 효과는 파일 간 중복 양 등의 데이터 세트 특성에 따라 달라집니다. 범용 파일 공유의 경우 일반적으로 평균 50%~60%가 절감됩니다. 공유 내에서 사용자 문서의 경우 30%~50%, 소프트웨어 개발 데이터 세트의 경우 70%~80%가 절감됩니다. 아래 설명된 `Measure-FSxDedupFileMetadata` 명령을 사용하여 잠재적 중복 제거 절감 효과를 측정할 수 있습니다.

특정 스토리지 요구 사항에 맞게 데이터 중복 제거를 사용자 지정할 수도 있습니다. 예를 들어 특정 파일 유형에서만 중복 제거가 실행되도록 구성하거나 사용자 지정 작업 일정을 만들 수 있습니다. 중복 제거 작업은 파일 서버 리소스를 소비할 수 있으므로 아래 설명된 `Get-FSxDedupStatus` 명령을 사용하여 중복 제거 작업의 상태를 모니터링하는 것이 좋습니다.

데이터 중복 제거에 대한 자세한 내용은 Microsoft의 데이터 중복 제거 이해 설명서를 참조하세요.

> **Note**
>
> 데이터 중복 제거 사용 모범 사례에 대한 모범 사례를 참조하세요. 데이터 중복 제거 작업을 성공적으로 실행하는 데 문제가 발생하는 경우 데이터 중복 제거 문제 해결 섹션을 참조하세요.

> **Warning**
>
> 데이터 중복 제거와 함께 특정 Robocopy 명령을 실행하는 것은 권장되지 않습니다. 이러한 명령은 Chunk Store의 데이터 무결성에 영향을 줄 수 있기 때문입니다. 자세한 내용은 Microsoft 데이터 중복 제거 상호 운용성 설명서를 참조하세요.

데이터 중복 제거 사용 모범 사례

다음은 데이터 중복 제거 사용에 대한 모범 사례입니다.

- 파일 시스템이 유휴 상태일 때 데이터 중복 제거 작업이 실행되도록 예약: 기본 일정에는 토요일 2:45 UTC의 주별 `GarbageCollection` 작업이 포함됩니다. 파일 시스템에 많은 양의 데이터 변동이 있는 경우 완료하는 데 몇 시간이 걸릴 수 있습니다. 이 시간이 워크로드에 적합하지 않은 경우 파일 시스템의 트래픽이 적을 것으로 예상되는 시간에 이 작업이 실행되도록 예약하세요.
- 데이터 중복 제거를 완료할 수 있도록 충분한 처리량 용량 구성: 처리량 용량이 높을수록 메모리 수준이 높아집니다. Microsoft는 데이터 중복 제거를 실행하기 위해 논리 데이터 1TB당 1GB의 메모리를 사용하는 것이 좋습니다. Amazon FSx 성능 테이블을 사용하여 파일 시스템의 처리량 용량 관련 메모리를 확인하여 메모리 리소스가 데이터 크기에 충분하도록 합니다.
- 특정 스토리지 요구 사항을 충족하고 성능 요구 사항을 줄일 수 있도록 데이터 중복 제거 설정 사용자 지정: 특정 파일 유형 또는 폴더에서 실행하도록 최적화를 제한하거나 최적화를 위한 최소 파일 크기 및 기간을 설정할 수 있습니다. 자세한 내용은 데이터 중복 제거 섹션을 참조하세요.

데이터 중복 제거 관리

원격 관리를 위한 Amazon FSx CLI를 사용하여 파일 시스템의 데이터 중복 제거를 관리할 수 있습니다. PowerShell 이 CLI를 사용하는 방법을 알아보려면 아마존 FSx CLI를 사용하는 방법 PowerShell 섹션을 참조하세요.

다음은 데이터 중복 제거에 사용할 수 있는 명령입니다.

데이터 중복 제거 명령	설명
Enable-FSxDedup	파일 공유에서 데이터 중복 제거를 활성화합니다. 데이터 중복 제거를 활성화하면 중복 제거 후 데이터 압축이 기본적으로 활성화됩니다.
Disable-FSxDedup	파일 공유에서 데이터 중복 제거를 비활성화합니다.
Get-FSxDedupConfiguration	최적화를 위한 최소 파일 크기 및 보존 기간, 압축 설정, 제외된 파일 유형 및 폴더를 비롯한 중복 제거 구성 정보를 검색합니다.
Set-FSxDedupConfiguration	최적화를 위한 최소 파일 크기 및 보존 기간, 압축 설정, 제외된 파일 유형 및 폴더를 비롯한 중복 제거 구성 설정을 변경합니다.

데이터 중복 제거 명령	설명
Get-FSxDedupStatus	중복 제거 상태를 검색하고, 파일 시스템의 최적화 절감 및 상태, 시간 및 파일 시스템의 마지막 작업에 대한 완료 상태를 설명하는 읽기 전용 속성을 포함합니다.
Get-FSxDedupMetadata	중복 제거 최적화 메타데이터를 검색합니다.
Update-FSxDedupStatus	업데이트된 데이터 중복 제거 절감 정보를 계산하고 검색합니다.
Measure-FSxDedupFileMetadata	폴더 그룹을 삭제할 경우 파일 시스템에서 확보할 수 있는 잠재적 스토리지 공간을 측정하고 검색합니다. 파일에는 다른 폴더와 공유되는 청크가 있는 경우가 많으며, 데이터 중복 제거 엔진이 고유하고 삭제될 청크를 계산합니다.
Get-FSxDedupSchedule	현재 정의된 중복 제거 일정을 검색합니다.
New-FSxDedupSchedule	데이터 중복 제거 일정을 만들고 사용자 지정합니다.
Set-FSxDedupSchedule	기존 데이터 중복 제거 일정의 구성 설정을 변경합니다.
Remove-FSxDedupSchedule	중복 제거 일정을 삭제합니다.
Get-FSxDedupJob	현재 실행 중이거나 대기 중인 모든 중복 제거 작업의 상태 및 정보를 가져옵니다.
Stop-FSxDedupJob	하나 이상의 지정된 데이터 중복 제거 작업을 취소합니다.

각 명령의 온라인 도움말은 모든 명령 옵션에 대한 참조를 제공합니다. 이 도움말에 액세스하려면 -?(예: Enable-FSxDedup -?)와 함께 명령을 실행합니다.

데이터 중복 제거 활성화

다음과 같이 `Enable-FSxDedup` 명령을 사용하여 Amazon FSx for Windows File Server 파일 공유에서 데이터 중복 제거를 활성화합니다.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {Enable-FsxDedup }
```

데이터 중복 제거를 활성화하면 기본 일정과 구성이 생성됩니다. 아래 명령을 사용하여 일정과 구성을 생성, 수정 및 제거할 수 있습니다.

Disable-FSxDedup 명령을 사용하여 파일 시스템에서 데이터 중복 제거를 완전히 비활성화할 수 있습니다.

데이터 중복 제거 일정 생성

대부분의 경우 기본 일정이 잘 작동하지만 다음과 같이 New-FsxDedupSchedule 명령을 사용하여 새 중복 제거 일정을 만들 수 있습니다. 데이터 중복 제거 일정은 UTC 시간을 사용합니다.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
New-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days Mon,Wed,Sat -
Start 08:00 -DurationHours 7
}
```

이 명령은 월요일, 수요일, 토요일에 실행되는 CustomOptimization이라는 이름의 일정을 생성하여 매일 오전 8시(UTC)에 작업을 시작하고 최대 지속 시간은 7시간이며, 그 이후에도 작업이 계속 실행 중이면 중지됩니다.

단, 사용자 지정 중복 제거 작업 일정을 새로 생성해도 기존 기본 일정이 재정의되거나 제거되지는 않습니다. 사용자 지정 중복 제거 작업을 생성하기 전에, 기본 작업이 필요하지 않은 경우 기본 작업을 비활성화할 수 있습니다.

다음과 같이 Set-FsxDedupSchedule 명령을 사용하여 기본 중복 제거 일정을 비활성화할 수 있습니다.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com
 -ConfigurationName FSxRemoteAdmin -ScriptBlock {Set-FSxDedupSchedule -Name
 “BackgroundOptimization” -Enabled $false}
```

Remove-FSxDedupSchedule -Name "ScheduleName" 명령을 사용하여 중복 제거 일정을 제거할 수 있습니다. 기본 BackgroundOptimization 중복 제거 일정은 수정하거나 제거할 수 없으며 대신 비활성화해야 합니다.

데이터 중복 제거 일정 수정

다음과 같이 Set-FsxDedupSchedule 명령을 사용하여 기존 중복 제거 일정을 수정할 수 있습니다.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FSxRemoteAdmin -ScriptBlock {
Set-FSxDedupSchedule -Name "CustomOptimization" -Type Optimization -Days
 Mon,Tues,Wed,Sat -Start 09:00 -DurationHours 9
}
```

이 명령은 월요일, 수요일, 토요일에 실행되는 기존 CustomOptimization 일정을 수정하여 매일 오전 9시(UTC)에 작업을 시작하고 최대 지속 시간은 9시간이며, 그 이후에도 작업이 계속 실행 중이면 중지됩니다.

설정을 최적화하기 전에 최소 파일 보존 기간을 수정하려면 Set-FSxDedupConfiguration 명령을 사용합니다.

절감된 공간의 양 보기

데이터 중복 제거를 실행하여 절감한 디스크 공간의 양을 보려면 다음과 같이 Get-FSxDedupStatus 명령을 사용합니다.

```
PS C:\Users\Admin> Invoke-Command -ComputerName amznfsxzzzzzzzz.corp.example.com -
ConfigurationName FsxRemoteAdmin -ScriptBlock {
Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate

OptimizedFilesCount OptimizedFilesSize SavedSpace OptimizedFilesSavingsRate
------------------- ------------------ ---------- -------------------------
              12587           31163594   25944826                        83
```

> **Note**
>
> 다음 파라미터에 대한 명령 응답에 표시된 값은 신뢰할 수 없으므로 Capacity,,, 및 값을 사용해서는 안 됩니다. FreeSpace UsedSpace UnoptimizedSize SavingsRate

데이터 중복 제거 문제 해결

다음 섹션에 설명된 것처럼 데이터 중복 제거 문제의 잠재적 원인은 여러 가지가 있습니다.

주제

- 데이터 중복 제거 작동하지 않음
- 중복 제거 값이 예기치 않게 0으로 설정됨

- 파일을 삭제한 후 파일 시스템의 여유 공간이 확보되지 않음

데이터 중복 제거 작동하지 않음

데이터 중복 제거 설명서의 지침에 따라 `Get-FSxDedupStatus` 명령을 실행하여 가장 최근의 중복 제거 작업의 완료 상태를 확인합니다. 하나 이상의 작업이 실패하는 경우, 파일 시스템에서 사용 가능한 스토리지 용량이 증가하지 않을 수 있습니다.

데이터 중복 제거 작업이 실패하는 가장 일반적인 이유는 메모리가 부족하기 때문입니다.

- Microsoft는 논리적 데이터 1TB당 1GB(또는 최소 300MB+논리 데이터 1TB당 50MB)의 메모리를 최적으로 사용할 것을 권장합니다. Amazon FSx 성능 테이블을 사용하여 파일 시스템의 처리량 용량 관련 메모리를 확인해 메모리 리소스가 데이터 크기에 충분하도록 합니다.
- 중복 제거 작업은 Windows 권장 기본값인 25% 메모리 할당으로 구성됩니다. 즉, 32GB 메모리가 있는 파일 시스템에서는 8GB를 중복 제거에 사용할 수 있습니다. 메모리 할당은 `Set-FSxDedupSchedule` 명령을 `-Memory` 파라미터와 함께 사용하여 구성할 수 있지만 추가 메모리를 사용하면 파일 시스템 성능에 영향을 미칠 수 있습니다.
- 중복 제거 작업 구성을 수정하여 메모리 요구량을 더 줄일 수 있습니다. 예를 들어, 최적화를 특정 파일 유형 또는 폴더에서 실행하도록 제한하거나, 최적화를 위한 최소 파일 크기 및 기간을 설정할 수 있습니다. 또한 파일 시스템의 부하가 최소인 유휴 기간에 데이터 중복 제거 작업이 실행되도록 구성하는 것을 권장합니다.

데이터 중복 제거 작업을 완료하는 데 시간이 충분하지 않은 경우에도 오류가 발생할 수 있습니다. 데이터 중복 제거 일정 수정 섹션에 설명된 대로 작업의 최대 지속시간을 변경해야 할 수도 있습니다.

중복 제거 작업이 실패하는 기간이 길고, 이 기간 동안 파일 시스템의 데이터가 변경된 경우, 후속 데이터 중복 제거 작업을 처음 성공적으로 완료하려면 더 많은 리소스가 필요할 수 있습니다.

중복 제거 값이 예기치 않게 0으로 설정됨

데이터 중복 제거를 구성한 파일 시스템에서 `SavedSpace` 및 `OptimizedFilesSavingsRate` 값이 예기치 않게 0이 됩니다.

이는 스토리지 최적화 프로세스 중에 파일 시스템의 스토리지 용량을 늘릴 때 발생할 수 있습니다. 파일 시스템의 스토리지 용량을 늘리면, Amazon FSx는 스토리지 최적화 프로세스 중에 기존 데이터 중복 제거 작업을 취소하고 기존 디스크의 데이터를 더 큰 새 디스크로 마이그레이션합니다. Amazon FSx는 스토리지 최적화 작업이 완료되면 파일 시스템에서 데이터 중복 제거를 재개합니다. 스토리지 용량 증가 및 스토리지 최적화에 대한 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.

파일을 삭제한 후 파일 시스템의 여유 공간이 확보되지 않음

데이터 중복 제거를 통해 공간을 절약한 데이터가 삭제된 경우, 가비지 수집 작업이 실행될 때까지 파일 시스템에서 실제로 공간이 확보되지 않는 것은 데이터 중복 제거의 예상된 동작입니다.

많은 파일을 삭제한 후 바로 가비지 수집 작업을 실행하도록 일정을 설정하는 것이 도움이 될 수 있습니다. 가비지 수집 작업이 끝난 후, 가비지 수집 일정을 이전 설정으로 되돌릴 수 있습니다. 이렇게 하면 즉시 삭제된 공간을 빠르게 확인할 수 있습니다.

다음 절차로 5분 내에 가비지 수집 작업이 실행되도록 설정하세요.

1. `Get-FSxDedupStatus` 명령을 사용하여 데이터 중복 제거가 활성화되었는지 확인합니다. 명령 및 예상되는 출력에 대한 자세한 내용은 절감된 공간의 양 보기 섹션을 참조하세요.
2. 다음에 따라 5분 후에 가비지 수집 작업이 실행되도록 설정하세요.

```
$FiveMinutesFromNowUTC = ((get-date).AddMinutes(5)).ToUniversalTime()
$DayOfWeek = $FiveMinutesFromNowUTC.DayOfWeek
$Time = $FiveMinutesFromNowUTC.ToString("HH:mm")

Invoke-Command -ComputerName ${RPS_ENDPOINT} -ConfigurationName FSxRemoteAdmin -
ScriptBlock {
    Set-FSxDedupSchedule -Name "WeeklyGarbageCollection" -Days $Using:DayOfWeek -
Start $Using:Time -DurationHours 9
}
```

3. 가비지 수집 작업을 실행하여 공간을 확보한 후, 일정을 원래대로 다시 설정합니다.

스토리지 할당량

파일 시스템에서 사용자 스토리지 할당량을 구성하여 사용자가 사용할 수 있는 데이터 스토리지의 양을 제한할 수 있습니다. 할당량을 설정한 후에는 할당량 상태를 추적하여 사용량을 모니터링하고 사용자가 할당량을 초과한 시점을 확인할 수 있습니다.

할당량에 도달한 사용자가 스토리지 공간에 쓰지 못하도록 하여 할당량을 적용할 수도 있습니다. 할당량을 적용하면 할당량을 초과하는 사용자에게 “디스크 공간 부족” 오류 메시지가 표시됩니다.

할당량 설정에 다음과 같은 임계값을 설정할 수 있습니다.

- 경고 - 사용자 또는 그룹이 할당량 한도에 도달했는지 여부를 추적하는 데 사용되며, 추적에만 해당됩니다.

- 한도 - 사용자 또는 그룹의 스토리지 할당량 한도입니다.

파일 시스템에 액세스하는 새 사용자에게 적용되는 기본 할당량과 특정 사용자 또는 그룹에 적용되는 할당량을 구성할 수 있습니다. 또한 각 사용자 또는 그룹이 사용하고 있는 스토리지의 양과 할당량을 초과하고 있는지 여부에 대한 보고서를 볼 수 있습니다.

사용자 수준의 스토리지 사용량은 파일 소유권을 기준으로 추적됩니다. 스토리지 사용량은 파일이 차지하는 실제 물리적 스토리지 공간이 아닌 논리적 파일 크기를 사용하여 계산됩니다. 사용자 스토리지 할당량은 데이터가 파일에 기록될 때 추적됩니다.

여러 사용자에 대한 할당량을 업데이트하려면 각 사용자에 대해 업데이트 명령을 한 번씩 실행하거나, 사용자를 그룹으로 구성하고 해당 그룹의 할당량을 업데이트해야 합니다.

사용자 스토리지 할당량 관리

원격 관리를 위한 Amazon FSx CLI를 사용하여 파일 시스템의 사용자 스토리지 할당량을 관리할 수 있습니다. PowerShell 이 CLI를 사용하는 방법을 알아보려면 아마존 FSx CLI를 사용하는 방법 PowerShell 섹션을 참조하세요.

다음은 사용자 스토리지 할당량을 관리하는 데 사용할 수 있는 명령입니다.

사용자 스토리지 할당량 명령	설명
Enable-FSxUserQuotas	사용자 스토리지 할당량을 추적하거나 적용하거나 둘 다 시작합니다.
Disable-FSxUserQuotas	사용자 스토리지 할당량 추적 및 적용을 중지합니다.
Get-FSxUserQuotaSettings	파일 시스템의 현재 사용자 스토리지 할당량 설정을 검색합니다.
Get-FSxUserQuotaEntries	파일 시스템의 개별 사용자 및 그룹에 대한 현재 사용자 스토리지 할당량 항목을 검색합니다.
Set-FSxUserQuotas	개별 사용자 또는 그룹의 사용자 스토리지 할당량을 설정합니다. 할당량 값은 바이트 단위로 지정됩니다.

각 명령의 온라인 도움말은 모든 명령 옵션에 대한 참조를 제공합니다. 이 도움말에 액세스하려면 -?(예: Enable-FSxUserQuotas -?)와 함께 명령을 실행합니다.

전송 중 암호화 관리

일련의 사용자 지정 PowerShell 명령을 사용하여 Windows File Server용 FSx 파일 시스템과 클라이언트 간에 전송되는 데이터의 암호화를 제어할 수 있습니다. SMB 암호화를 지원하는 클라이언트로만 파일 시스템 액세스를 제한하여 항상 암호화되도록 data-in-transit 할 수 있습니다. 암호화에 대한 적용 기능이 설정된 경우 SMB 3.0 암호화를 지원하지 않는 클라이언트에서 파일 시스템에 액세스하는 사용자는 암호화가 설정된 파일 공유에 액세스할 수 없습니다. data-in-transit

파일 서버 수준이 아닌 파일 공유 수준에서 암호화를 제어할 수도 있습니다. data-in-transit 민감한 데이터가 포함된 일부 파일 공유에 전송 중 암호화를 적용하고 모든 사용자가 일부 다른 파일 공유에 액세스하도록 허용하려는 경우 파일 공유 수준 암호화 제어를 통해 동일한 파일 시스템에서 암호화된 파일 공유와 암호화되지 않은 파일 공유를 혼합하여 사용할 수 있습니다. 서버 전체 암호화는 공유 수준 암호화보다 우선합니다. 글로벌 암호화가 활성화된 경우 특정 공유에 대한 암호화를 선택적으로 비활성화할 수 없습니다.

원격 관리를 위한 Amazon FSx CLI를 사용하여 파일 시스템에서 사용자 전송 중 암호화를 관리할 수 있습니다. PowerShell 이 CLI를 사용하는 방법을 알아보려면 아마존 FSx CLI를 사용하는 방법 PowerShell 섹션을 참조하세요.

다음은 파일 시스템에서 사용자 전송 중 암호화를 관리하는 데 사용할 수 있는 명령입니다.

전송 중 암호화 명령	설명
Get-FSxSmbServerConfiguration	Server Message Block(SMB) 서버 구성을 검색합니다.
Set-FSxSmbServerConfiguration	이 명령에는 전송 중 암호화를 구성하는 두 가지 옵션이 있습니다. • `-EncryptData $True\|$False` — 전송 중 데이터 암호화를 `True` 활성화하려면 이 매개 변수를 로 설정합니다. 전송 중 데이터 암호화를 `False` 끄려면 이 매개 변수를 로 설정하십시오. • `-RejectUnencryptedAccess $True\|$False` — 암호화를 지원하지 않는 클라이언트가 파일 시스템에 액세스하는 것을 허용하지 `True` 않으려면 이 매개 변수를 로 설정합니다. 암호화를 지원하지 않는 클라이언트가 파일 시스템에 액세스할 수 있도록 `False` 하려면 이 매개 변수를 로 설정하십시오.

각 명령의 온라인 도움말은 모든 명령 옵션에 대한 참조를 제공합니다. 이 도움말에 액세스하려면 -?(예: Get-FSxSmbServerConfiguration -?)와 함께 명령을 실행합니다.

스토리지 구성 관리

파일 시스템의 스토리지 구성에는 스토리지 용량, 스토리지 유형, SSD IOPS가 포함됩니다. 파일 시스템 생성 도중 및 이후에 이러한 리소스를 처리량 용량과 함께 구성하여 워크로드에 대해 원하는 성능 수준을 달성할 수 있습니다. 자세한 내용은 다음 항목을 참조하세요.

주제

- 스토리지 용량 관리
- 스토리지 유형 관리
- SSD IOPS 관리

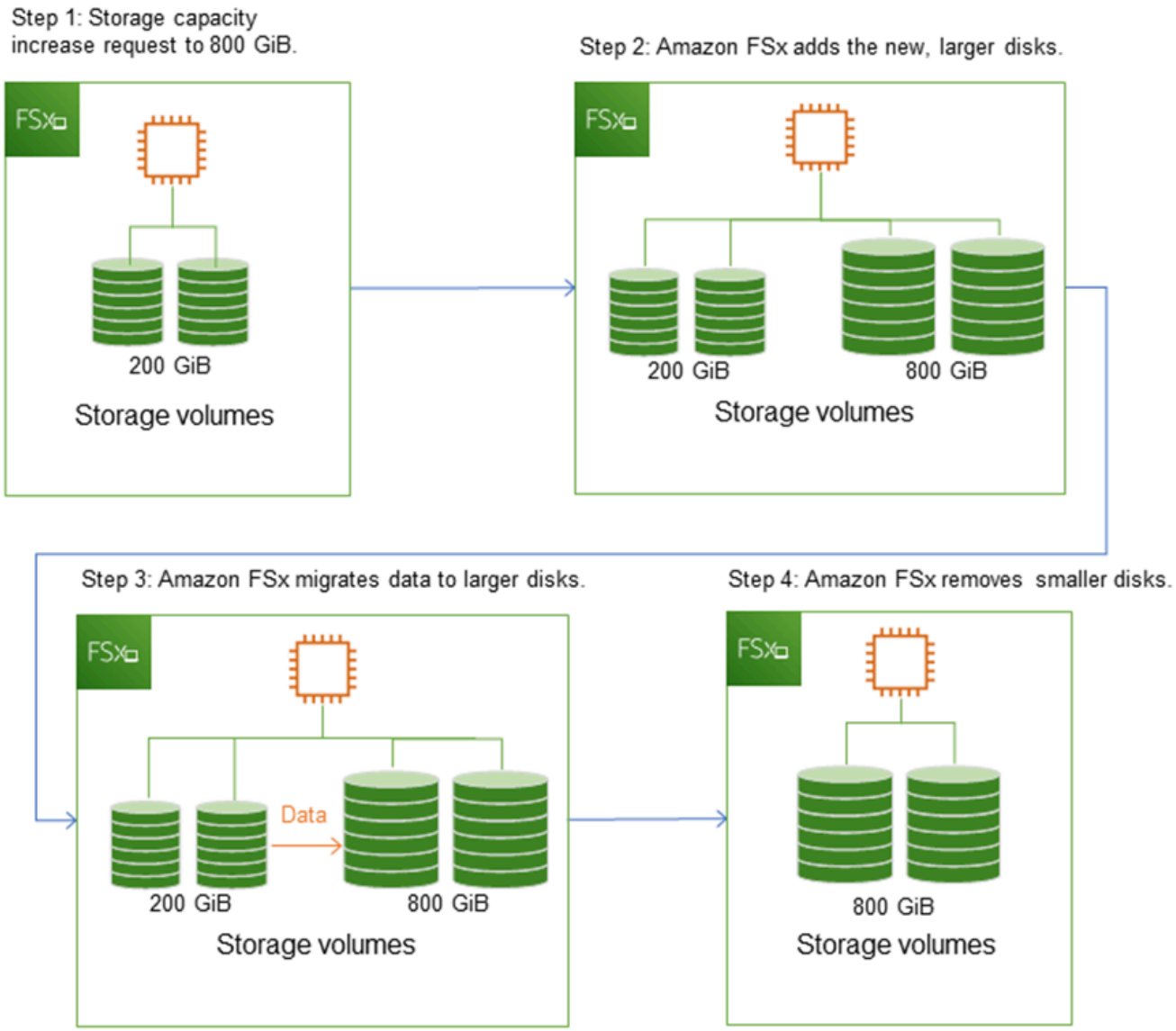
스토리지 용량 관리

FSx for Windows File Server 파일 시스템에 구성된 스토리지 용량을 필요에 따라 늘릴 수 있습니다. 이는 Amazon FSx 콘솔, Amazon FSx API 또는 AWS Command Line Interface(AWS CLI)를 사용하여 수행할 수 있습니다. 파일 시스템의 스토리지 용량을 늘릴 수만 있고 스토리지 용량을 줄일 수는 없습니다.

> **Note**
>
> 2019년 6월 23일 이전에 생성된 파일 시스템이나 2019년 6월 23일 이전에 생성된 파일 시스템에 속하는 백업에서 복원된 파일 시스템의 스토리지 용량은 늘릴 수 없습니다.

Amazon FSx 파일 시스템의 스토리지 용량을 늘리면 Amazon FSx는 파일 시스템에 더 큰 새 디스크 세트를 백그라운드에서 추가합니다. 그런 다음 Amazon FSx는 백그라운드에서 스토리지 최적화 프로세스를 실행하여 이전 디스크의 데이터를 새 디스크로 투명하게 마이그레이션합니다. 스토리지 최적화에는 몇 시간에서 며칠이 소요될 수 있으며, 워크로드 성능에 미치는 영향은 미미합니다. 이전 스토리지 볼륨과 새 스토리지 볼륨이 모두 파일 시스템 수준 백업에 포함되기 때문에 이 최적화 중에는 백업 사용량이 일시적으로 더 높아집니다. Amazon FSx가 스토리지 스케일링 활동 중에도 성공적으로 백업을 생성하고 백업에서 복원할 수 있도록 두 스토리지 볼륨 세트가 모두 포함되어 있습니다. 이전 스토리지 볼륨이 더 이상 백업 기록에 포함되지 않으면 백업 사용량이 이전 기준 수준으로 되돌아갑니다. 새 스토리지 용량을 사용할 수 있게 되면 새 스토리지 용량에 대해서만 요금이 청구됩니다.

다음 그림은 Amazon FSx가 파일 시스템의 스토리지 용량을 늘릴 때 사용하는 프로세스의 네 가지 주요 단계를 보여줍니다.



Amazon FSx 콘솔, CLI 또는 API를 사용하여 언제든지 스토리지 최적화, SSD 스토리지 용량 증가 또는 SSD IOPS 업데이트의 진행 상황을 추적할 수 있습니다. 자세한 내용은 스토리지 용량 증가 모니터링 섹션을 참조하세요.

주제

스토리지 용량을 늘릴 때 알아야 할 중요 사항

스토리지 용량을 늘릴 때 고려해야 할 몇 가지 중요한 항목은 다음과 같습니다.

- 증가만 - 파일 시스템의 스토리지 용량을 늘릴 수만 있고 스토리지 용량을 줄일 수는 없습니다.
- 최소 증가 - 각 스토리지 용량 증가는 파일 시스템의 현재 스토리지 용량의 최소 10%(최대 허용 값인 65,536GiB까지)여야 합니다.
- 최소 처리량 용량 - 스토리지 용량을 늘리려면 파일 시스템의 최소 처리량 용량이 16MB/s여야 합니다. 스토리지 최적화 단계는 처리량이 많은 프로세스이기 때문입니다.
- 증가 사이 경과 시간 - 마지막 증가 요청 후 6시간 또는 스토리지 최적화 프로세스가 완료될 때까지(둘 중 더 긴 시간이 경과할 때까지) 파일 시스템의 스토리지 용량을 추가로 늘릴 수 없습니다. 스토리지 최적화를 완료하는 데 몇 시간에서 며칠까지 걸릴 수 있습니다. 스토리지 최적화를 완료하는 데 걸리는 시간을 최소화하려면 스토리지 용량을 늘리기 전에 파일 시스템의 처리량 용량을 늘리고(스토리지 스케일링이 완료된 후 처리량 용량을 다시 스케일 다운할 수 있음), 파일 시스템의 트래픽이 최소일 때는 스토리지 용량을 늘리는 것이 좋습니다.

> **Note**
>
> 특정 파일 시스템 이벤트는 디스크 I/O 성능 리소스를 사용할 수 있습니다. 예를 들면 스토리지 용량 스케일링의 최적화 단계에서 디스크 처리량이 증가하여 잠재적으로 성능 경고가 발생할 수 있습니다. 자세한 내용은 성능 경고 및 권장 사항 섹션을 참조하세요.

스토리지 용량을 늘려야 하는 경우

여유 스토리지 용량이 부족할 경우 파일 시스템의 스토리지 용량을 늘립니다. 파일 시스템에서 사용 가능한 여유 스토리지의 양을 모니터링하려면 `FreeStorageCapacity` CloudWatch 지표를 사용합니

다. 이 지표에 Amazon CloudWatch 경보를 생성하면 지표가 특정 임계값 아래로 떨어질 때 알림을 받을 수 있습니다. 자세한 내용은 Amazon을 통한 지표 모니터링 CloudWatch 섹션을 참조하세요.

파일 시스템의 여유 스토리지 용량을 항상 10% 이상 유지하는 것이 좋습니다. 스토리지 용량을 모두 사용하면 성능이 저하되고 데이터 불일치가 발생할 수 있습니다.

여유 스토리지 용량이 사용자가 지정하여 정의된 임계값 아래로 떨어질 때 파일 시스템의 스토리지 용량을 자동으로 늘릴 수 있습니다. AWS에서 개발된 사용자 지정 AWS CloudFormation 템플릿을 사용하여 자동화된 솔루션을 구현하는 데 필요한 모든 구성 요소를 배포합니다. 자세한 내용은 스토리지 용량 동적 증가 섹션을 참조하세요.

스토리지 용량 증가 및 파일 시스템 성능

새 스토리지 용량을 사용할 수 있게 된 후 Amazon FSx가 백그라운드에서 스토리지 최적화 프로세스를 실행하는 동안 대부분의 워크로드가 겪는 성능 영향은 미미합니다. 대규모 활성 데이터 세트를 포함하는 쓰기 중심의 애플리케이션은 쓰기 성능이 일시적으로 최대 절반까지 저하될 수 있습니다. 이러한 경우에는 스토리지 용량을 늘리기 전에 먼저 파일 시스템의 처리량 용량을 늘릴 수 있습니다. 이렇게 하면 애플리케이션의 성능 요구 사항에 맞게 동일한 수준의 처리량을 계속 제공할 수 있습니다. 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

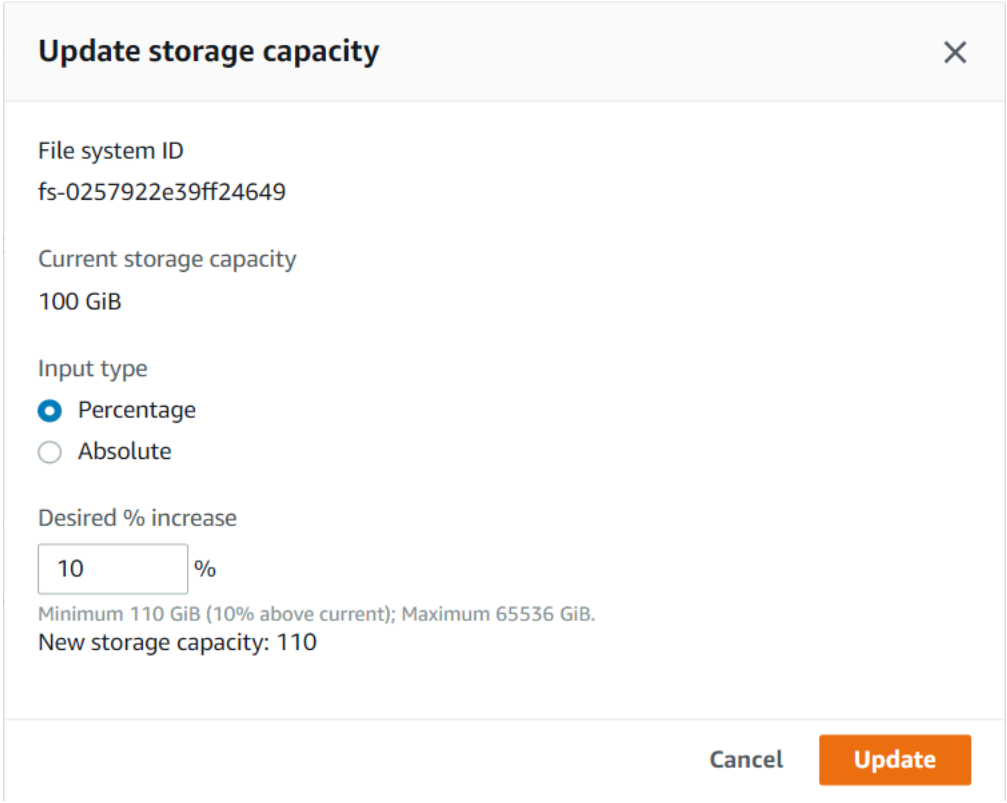
스토리지 용량을 늘리는 방법

Amazon FSx 콘솔, AWS CLI 또는 Amazon FSx API를 사용하여 파일 시스템의 스토리지 용량을 늘릴 수 있습니다.

파일 시스템의 스토리지 용량 증가(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 스토리지 용량을 늘리려는 Windows 파일 시스템을 선택합니다.
3. 작업에서 스토리지 업데이트를 선택합니다. 또는 요약 패널에서 파일 시스템의 스토리지 용량 옆에 있는 업데이트를 선택합니다.

   스토리지 용량 업데이트 창이 표시됩니다.



4. 입력 유형에서 백분율을 선택하여 현재 값에서 변경된 백분율로 새 스토리지 용량을 입력하거나 절대를 선택하여 GiB 단위로 새 값을 입력합니다.
5. 원하는 스토리지 용량을 입력합니다.

> **Note**
>
> 원하는 용량 값은 현재 값보다 10% 이상 커야 합니다(최대 값은 65,536GiB).

6. 업데이트를 선택하여 스토리지 용량 업데이트를 시작합니다.
7. 업데이트 탭의 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다.

파일 시스템의 스토리지 용량 증가(CLI)

FSx for Windows File Server 파일 시스템의 스토리지 용량을 늘리려면 update-file-system AWS CLI 명령을 사용합니다. 다음 파라미터를 설정합니다.

- `--file-system-id`를 업데이트하려는 파일 시스템의 ID로 설정합니다.
- `--storage-capacity`를 현재 값보다 10% 이상 큰 값으로 설정합니다.

AWS CLI 명령 describe-file-systems를 사용하여 업데이트 진행률을 모니터링할 수 있습니다. 출력에서 `administrative-actions`를 찾습니다.

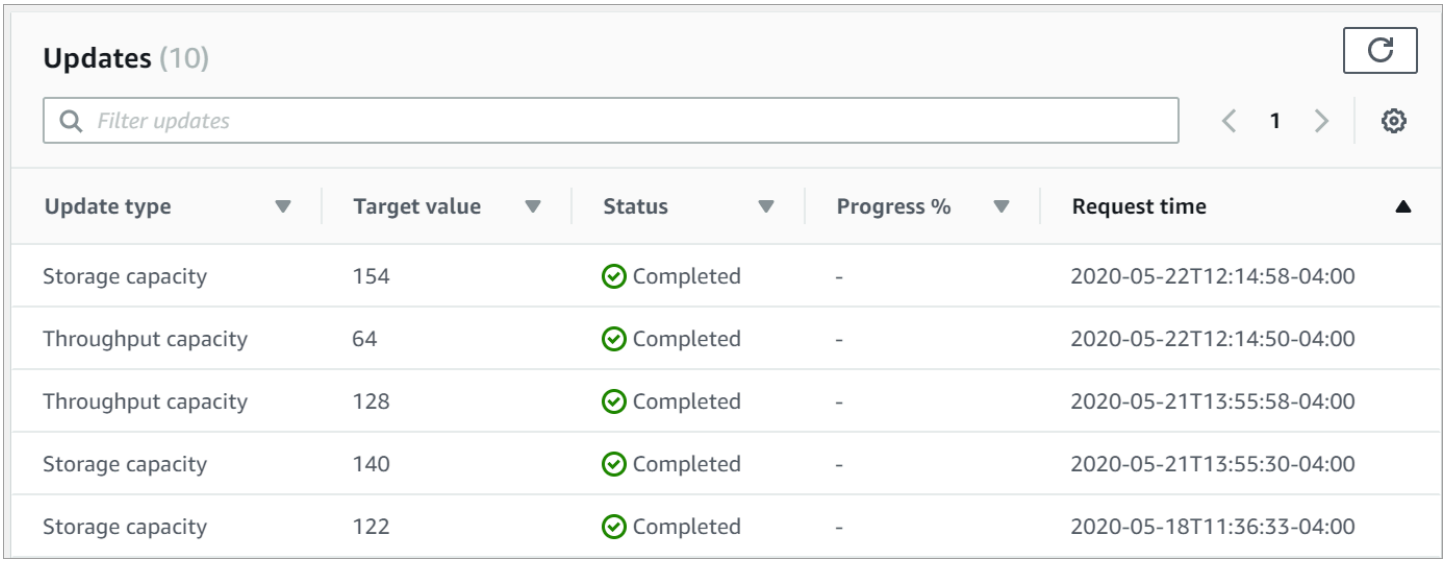
자세한 내용은 AdministrativeAction을 참조하세요.

스토리지 용량 증가 모니터링

Amazon FSx 콘솔, API 및 AWS CLI를 사용하여 스토리지 용량 증가 진행 상황을 모니터링할 수 있습니다.

콘솔에서 증가 모니터링

파일 시스템 세부 정보 창의 업데이트 탭에서 각 업데이트 유형에 대한 가장 최근의 업데이트 10개를 볼 수 있습니다.



스토리지 용량 업데이트에서 다음 정보를 볼 수 있습니다.

업데이트 유형

가능한 값은 스토리지 용량입니다.

대상 값

파일 시스템의 스토리지 용량을 업데이트하려는 적정 값입니다.

상태

업데이트의 현재 상태입니다. 스토리지 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.

- 업데이트 후 최적화 중 - Amazon FSx가 파일 시스템의 스토리지 용량을 늘렸습니다. 스토리지 최적화 프로세스가 이제 파일 시스템 데이터를 더 큰 새 디스크로 옮기고 있습니다.
- 완료 - 스토리지 용량 증가가 완료되었습니다.
- 실패 - 스토리지 용량 증가에 실패했습니다. 스토리지 업데이트가 실패한 자세한 이유를 보려면 ?를 선택합니다.

진행률(%)

스토리지 최적화 프로세스의 진행률을 완료율로 표시합니다.

요청 시간

Amazon FSx가 업데이트 작업 요청을 받은 시간입니다.

AWS CLI 및 API를 사용한 증가 모니터링

describe-file-systems AWS CLI 명령과 DescribeFileSystems API 작업을 사용하여 파일 시스템 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 시스템의 스토리지 용량은 300GB이며, 스토리지 용량을 1000GB로 늘리기 위한 관리 작업이 보류 중입니다.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                     "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                     "RequestTime": 1581694764.757,
                     "Status": "PENDING",
                     "TargetFileSystemValues": {
                         "StorageCapacity": 1000
                     }
                },
```

```
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "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. 이는 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.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 1000,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "RequestTime": 1581694764.757,
                    "Status": "UPDATED_OPTIMIZING",
                    "TargetFileSystemValues": {
                        "StorageCapacity": 1000
                }
                },
                {
                    "AdministrativeActionType": "STORAGE_OPTIMIZATION",
                    "RequestTime": 1581694764.757,
                    "Status": "IN_PROGRESS",
                    "ProgressPercent": 50,
                }
            ]
```

스토리지 용량 증가에 실패하면 FILE_SYSTEM_UPDATE 작업 상태가 FAILED로 변경됩니다. 이 FailureDetails 속성은 다음 예제와 같이 실패에 대한 정보를 제공합니다.

```
{
    "FileSystems": [
        {
            "OwnerId": "111122223333",
            .
            .
            .
            "StorageCapacity": 300,
            "AdministrativeActions": [
                {
                    "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
                    "FailureDetails": {
                        "Message": "string"
                    },
                    "RequestTime": 1581694764.757,
                    "Status": "FAILED",
                    "TargetFileSystemValues":
                        "StorageCapacity": 1000
                }
            ]
```

실패 작업에 대한 문제 해결 방법은 스토리지 또는 처리량 용량 업데이트 실패 섹션을 참조하세요.

FSx for Windows File Server 파일 시스템의 스토리지 용량 동적 증가

여유 스토리지 용량이 사용자가 지정하여 정의된 임계값 아래로 떨어질 경우 다음 솔루션을 사용하여 FSx for Windows File Server 파일 시스템의 스토리지 용량을 동적으로 늘릴 수 있습니다. 이 AWS CloudFormation 템플릿은 여유 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.

이 솔루션은 필요한 모든 구성 요소를 자동으로 배포하고 다음 파라미터를 사용합니다.

- 파일 시스템 ID
- 여유 스토리지 용량 임계값(숫자 값)
- 측정 단위(백분율 [기본값] 또는 GiB)
- 스토리지 용량 증가 기준 백분율(%)
- SNS 구독을 위한 이메일 주소

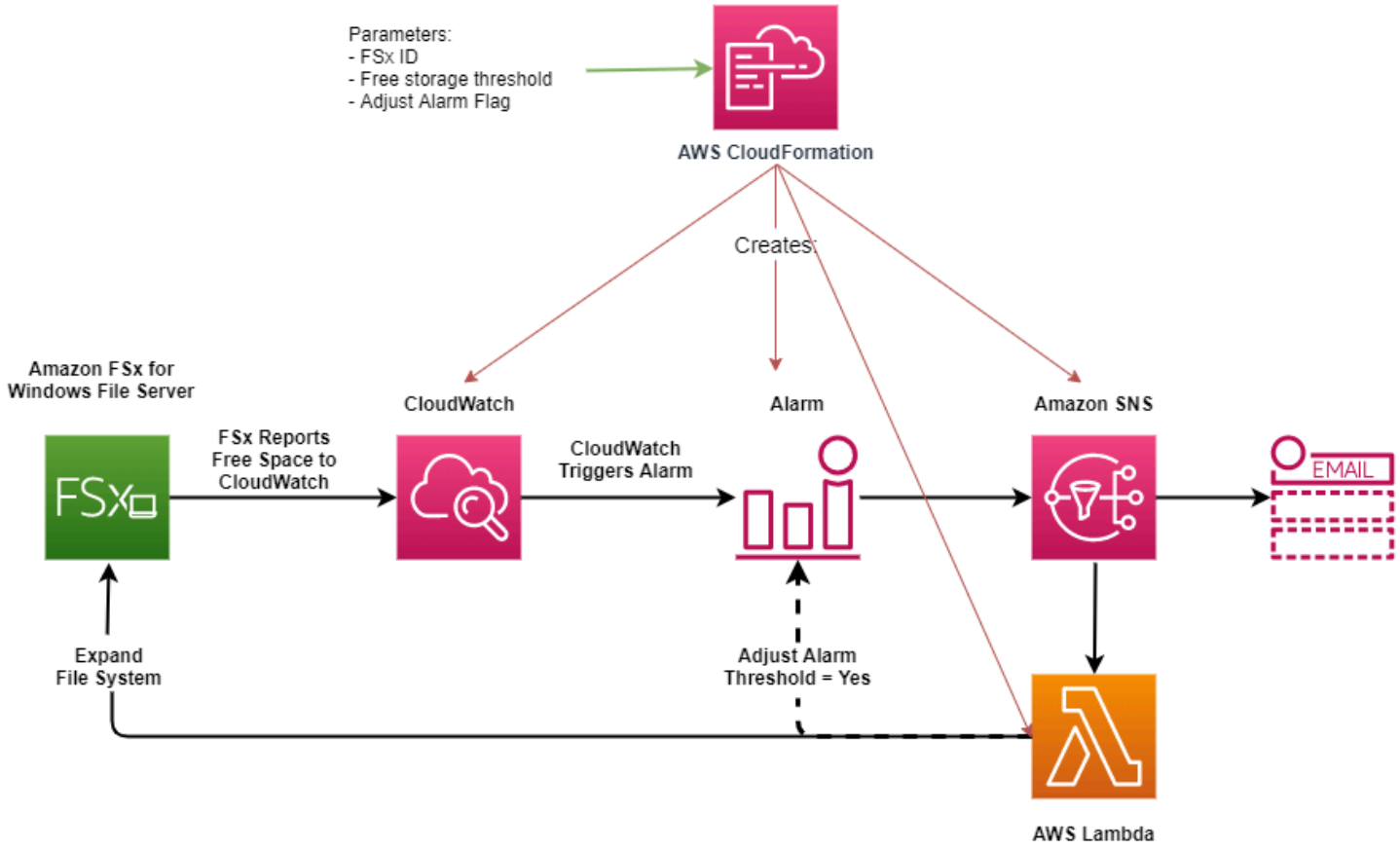
- 경보 임계값 조정(예/아니요)

주제

- 아키텍처 개요
- AWS CloudFormation 템플릿
- AWS CloudFormation을 사용하여 배포 자동화

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(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 여유 스토리지 용량이 지정된 임계값 아래로 떨어지면 경보를 트리거하고 Amazon SNS 대기열에 메시지를 보냅니다.

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 함수는 파일 시스템의 새 스토리지 용량의 지정된 비율과 같도록 여유 스토리지 용량 임계값을 선택적으로 조정할 수 있습니다.
6. 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 FSx for Windows File Server 파일 시스템의 스토리지 용량을 자동으로 늘리는 데 사용되는 구성 요소를 자동으로 배포하는 데 AWS CloudFormation을 사용합니다. 이 솔루션을 사용하려면 IncreaseFSxSize 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 늘리는 기준이 되는 초기 여유 스토리지 용량 임계값을 지정합니다. 이 임계값은 GiB 단위로 지정하거나 파일 시스템의 현재 스토리지 용량의 백분율(%)로 지정합니다. CloudFormation 템플릿은 백분율로 표시될 때 CloudWatch 경보 설정과 일치하도록 GiB로 다시 계산됩니다.

LowFreeDataStorageCapacityThresholdUnit

기본값은 %입니다. `LowFreeDataStorageCapacityThreshold`의 단위를 GiB로 지정하거나 현재 스토리지 용량의 백분율로 지정합니다.

AlarmModificationNotification

기본값은 Yes입니다. Yes로 설정하면 초기 `LowFreeDataStorageCapacityThreshold`가 후속 경보 임계값의 `PercentIncrease` 값에 비례하여 증가합니다.

예를 들어 `PercentIncrease`가 20으로 설정되고 AlarmModificationNotification이 Yes로 설정된 경우 GiB에 지정된 사용 가능한 여유 공간 임계값(`LowFreeDataStorageCapacityThreshold`)은 후속 스토리지 용량 증가 이벤트에 대해 20% 증가합니다.

EmailAddress

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

PercentIncrease

기본값이 없습니다. 스토리지 용량을 늘릴 양을 현재 스토리지 용량의 백분율로 표현하여 지정합니다.

AWS CloudFormation을 사용하여 배포 자동화

다음 절차는 FSx for Windows File Server 파일 시스템의 스토리지 용량을 자동으로 늘리도록 AWS CloudFormation 스택을 구성하고 배포합니다. 배포에는 약 5분이 소요됩니다.

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

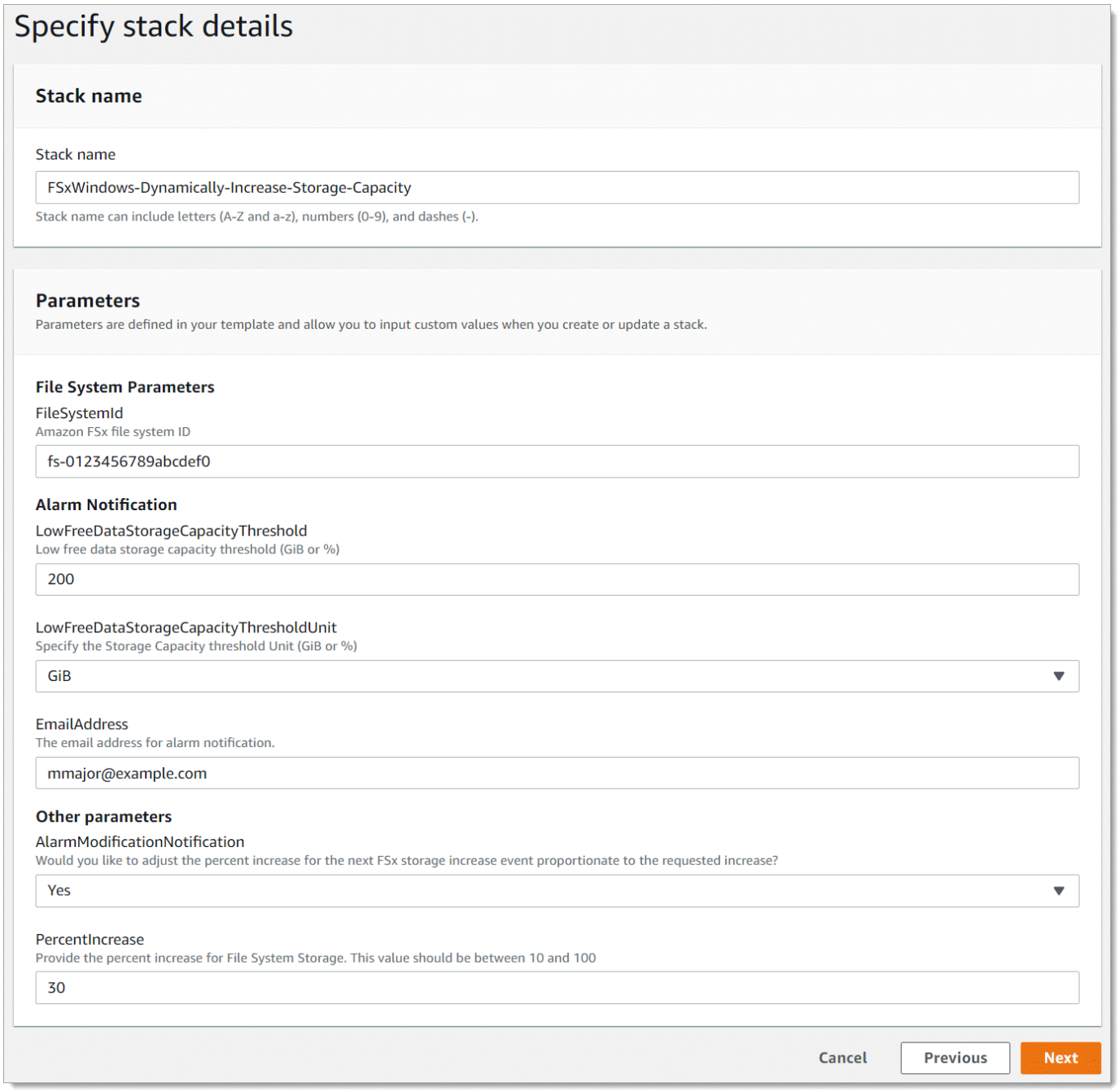
시작하기 전에 AWS 계정에 Amazon Virtual Private Cloud(VPC)에서 실행되는 Amazon FSx 파일 시스템의 ID가 있어야 합니다. Amazon FSx 리소스 생성에 대한 자세한 내용은 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.

자동 스토리지 용량 증가 솔루션 스택 시작

1. IncreaseFSxSize AWS CloudFormation 템플릿을 다운로드합니다. CloudFormation 스택 생성에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 AWS CloudFormation 콘솔에서 스택 생성을 참조하세요.

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

2. 스택 세부 정보 지정에 자동 스토리지 용량 증가 솔루션의 값을 입력합니다.



3. 스택 이름을 입력합니다.
4. 파라미터의 경우 템플릿의 파라미터를 검토하고 파일 시스템의 필요에 맞게 수정합니다. 이후 다음을 선택합니다.
5. 사용자 지정 솔루션에 대해 원하는 옵션 설정을 입력하고 다음을 선택합니다.
6. 검토에서 솔루션 설정을 검토하고 확인합니다. 템플릿이 IAM 리소스를 생성한다는 것을 확인하는 확인란을 선택해야 합니다.

7. 생성을 선택하여 스택을 배포합니다.

AWS CloudFormation 콘솔의 상태 열에서 스택의 상태를 볼 수 있습니다. 약 5분 후에 생성_완료라는 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.

스토리지 유형 관리

FSx for Windows File Server는 솔리드 스테이트 드라이브(SSD) 및 마그네틱 하드 디스크 드라이브(HDD) 스토리지 유형을 제공합니다. SSD 스토리지는 데이터베이스, 미디어 처리 워크로드, 데이터 분석 애플리케이션을 포함하여 성능이 가장 높고 지연 시간에 민감한 워크로드용으로 설계되었습니다. HDD 스토리지는 홈 디렉터리, 사용자 및 부서별 파일 공유, 콘텐츠 관리 시스템 등 광범위한 워크로드에 맞게 설계되었습니다.

Amazon FSx 콘솔 또는 Amazon FSx API를 사용하여 파일 시스템 스토리지 유형을 HDD에서 SSD로 변경할 수 있습니다. 파일 시스템 스토리지 유형을 SSD에서 HDD로 변경할 수 없습니다. 마지막 업데이트가 요청된 후 6시간이 지나거나 스토리지 최적화 프로세스가 완료될 때까지(둘 중 시간이 더 오래 걸리는 경우) 파일 시스템 구성을 다시 업데이트할 수 없다는 점에 유의하세요. 스토리지 최적화를 완료하는 데 몇 시간에서 며칠까지 걸릴 수 있습니다. 이 시간을 최소화하려면 파일 시스템의 트래픽이 최소일 때 스토리지 유형을 업데이트하는 것이 좋습니다.

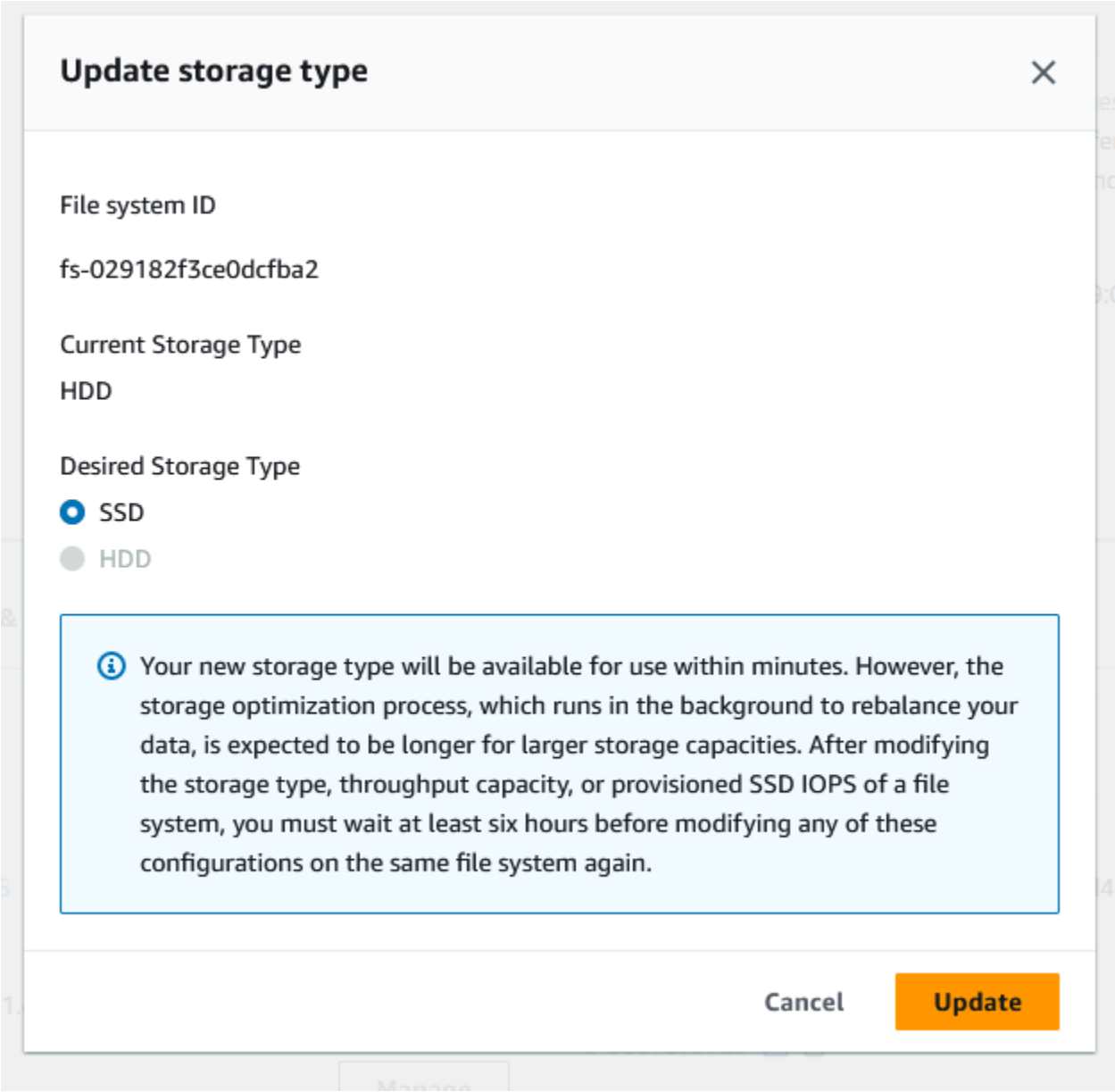
사용 가능한 백업을 복원하여 새 파일 시스템을 만들고 새 스토리지 유형을 선택하여 파일 시스템 스토리지 유형을 HDD에서 SSD로 변경할 수도 있습니다. 자세한 내용은 백업 복원 섹션을 참조하세요.

스토리지 유형을 업데이트하는 방법

Amazon FSx 콘솔, AWS CLI 또는 Amazon FSx API를 사용하여 파일 시스템의 스토리지 유형을 업데이트할 수 있습니다.

파일 시스템의 스토리지 유형 업데이트(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 스토리지 유형을 업데이트할 Windows 파일 시스템을 선택합니다.
3. 작업에서 스토리지 유형 업데이트를 선택합니다. 또는 요약 패널에서 HDD 옆의 업데이트 버튼을 선택합니다. 스토리지 유형 업데이트 창이 표시됩니다.



4. 원하는 스토리지 유형에서 SSD를 선택합니다. 업데이트를 선택하여 스토리지 유형 업데이트를 시작합니다.
5. 업데이트 탭의 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다.

파일 시스템의 스토리지 유형 업데이트(CLI)

FSx for Windows File Server 파일 시스템의 스토리지 유형을 업데이트하려면 AWS CLI 명령 update-file-system을 사용합니다. 다음 파라미터를 설정합니다.

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

- `--storage-type`을 SSD로 설정합니다. SSD 스토리지 유형에서 HDD 스토리지 유형으로는 전환할 수 없습니다.

AWS CLI 명령 describe-file-systems를 사용하여 업데이트 진행률을 모니터링할 수 있습니다. 출력에서 `administrative-actions`를 찾습니다.

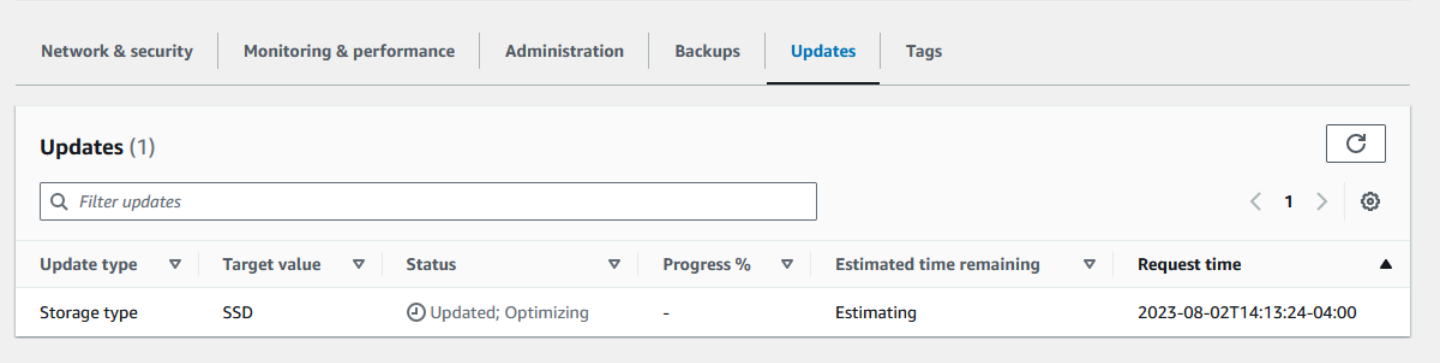
자세한 내용은 AdministrativeAction을 참조하세요.

스토리지 유형 업데이트 모니터링

Amazon FSx 콘솔, API 및 AWS CLI를 사용하여 스토리지 유형 업데이트 진행 상황을 모니터링할 수 있습니다.

콘솔에서 업데이트 모니터링

파일 시스템 세부 정보 창의 업데이트 탭에서 각 업데이트 유형에 대한 가장 최근의 업데이트 10개를 볼 수 있습니다.



스토리지 유형 업데이트에서 다음 정보를 볼 수 있습니다.

업데이트 유형

가능한 값은 스토리지 유형입니다.

대상 값

SSD

상태

업데이트의 현재 상태입니다. 스토리지 유형 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.

- 업데이트 후 최적화 중 - 워크로드의 쓰기 작업에 SSD 스토리지 성능을 사용할 수 있습니다. 업데이트는 업데이트 후 최적화 중 상태로 전환되며, 이 상태는 일반적으로 몇 시간 동안 지속되어 이 기간 동안 워크로드의 읽기 작업은 HDD와 SSD 수준 사이의 성능을 유지합니다. 업데이트 작업이 완료되면 새 SSD 성능을 읽기와 쓰기 모두에 사용할 수 있습니다.
- 완료 - 스토리지 유형 업데이트가 완료되었습니다.
- 실패 - 스토리지 유형 업데이트에 실패했습니다. 세부 정보를 보려면 물음표(?)를 선택합니다.

진행률(%)

스토리지 최적화 프로세스의 진행률을 완료율로 표시합니다.

요청 시간

Amazon FSx가 업데이트 작업 요청을 받은 시간입니다.

AWS CLI 및 API를 사용하여 업데이트 모니터링

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

SSD IOPS 관리

SSD 스토리지 볼륨에서 IOPS를 스토리지 용량과 관계없이 선택하고 확장할 수 있습니다. 프로비저닝할 수 있는 최대 SSD IOPS는 파일 시스템용으로 선택한 스토리지 용량과 처리량 용량에 따라 달라집니다. 처리량 용량이 지원하는 한도 이상으로 SSD IOPS를 늘리려는 경우 요청된 SSD IOPS 수준을 지원하도록 처리량 용량을 늘려야 할 수 있습니다. 자세한 내용은 FSx for Windows File Server 성능 및 처리량 용량 관리 섹션을 참조하세요.

주제

- SSD IOPS를 업데이트할 때 알아두어야 할 중요 사항
- SSD IOPS 업데이트 방법
- 프로비저닝된 SSD IOPS 업데이트 모니터링

SSD IOPS를 업데이트할 때 알아두어야 할 중요 사항

SSD IOPS를 업데이트할 때 고려해야 할 몇 가지 중요한 항목은 다음과 같습니다.

- 파일 시스템에 프로비저닝된 SSD IOPS의 양을 지정하려면 두 IOPS 모드 중 하나를 선택해야 합니다.
  - 자동 — Amazon FSx는 스토리지 용량 GiB당 3 SSD IOPS를 유지하도록 SSD IOPS를 자동으로 확장하여 파일 시스템당 최대 40만 SSD IOPS를 유지합니다.
  - 사용자 프로비저닝 — SSD IOPS 수를 96~400,000 범위 내에서 지정합니다. Amazon FSx가 사용 가능한 모든 AWS 리전에서 스토리지 용량 GiB당 3~50 IOPS 사이의 수를 지정하거나, 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 유럽(아일랜드), 아시아 태평양(도쿄) 및 아시아 태평양(싱가포르)에서 스토리지 용량 GiB당 3~500 IOPS 사이의 수를 지정합니다. SSD IOPS의 양이 GiB당 3 IOPS 이상이 아닌 경우 요청이 실패합니다. 프로비저닝된 SSD IOPS 수준이 더 높은 경우 파일 시스템별로 GiB당 3 IOPS를 초과하는 평균 IOPS에 대한 비용을 지불합니다.
- 스토리지 용량 업데이트 - 스토리지 용량을 늘리고 새 용량에 사용자가 프로비저닝한 SSD IOPS 수준보다 높은 수준의 SSD IOPS가 필요한 경우, Amazon FSx는 자동으로 파일 시스템을 자동 모드로 전환합니다.
- 처리량 용량 업데이트 - 처리량 용량을 늘리고 새 처리량 용량이 지원하는 최대 SSD IOPS가 사용자가 프로비저닝한 SSD IOPS 수준보다 높을 경우, Amazon FSx는 자동으로 파일 시스템을 자동 모드로 전환합니다.
- 증가 사이 경과 시간 - 마지막 증가 요청 후 6시간 또는 스토리지 최적화 프로세스가 완료될 때까지(둘 중 더 긴 시간이 경과할 때까지) 파일 시스템에서 SSD IOPS를 추가로 늘리거나, 처리량 용량을 늘리거나, 스토리지 유형을 업데이트할 수 없습니다. 스토리지 최적화를 완료하는 데 몇 시간에서 며칠까지 걸릴 수 있습니다. 스토리지 최적화를 완료하는 데 걸리는 시간을 최소화하려면 파일 시스템의 트래픽이 최소일 때 SSD IOPS를 조정하는 것이 좋습니다.

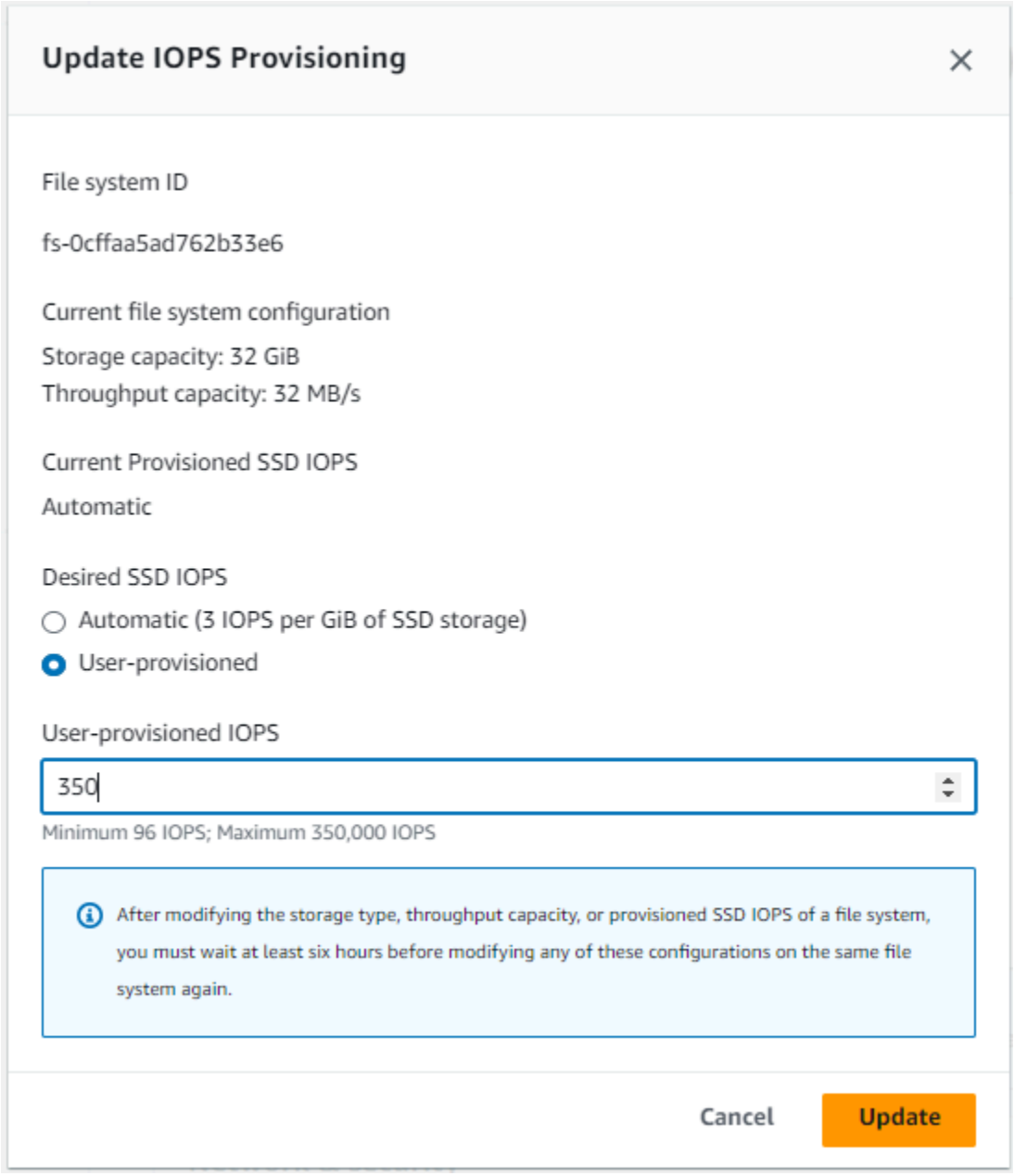
> **Note**
>
> 4,608MBps 이상의 처리량 용량 수준은 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 유럽(아일랜드), 아시아 태평양(도쿄) 및 아시아 태평양(싱가포르)의 AWS 리전에서만 지원됩니다.

SSD IOPS 업데이트 방법

Amazon FSx 콘솔, AWS CLI 또는 Amazon FSx API를 사용하여 파일 시스템의 SSD IOPS를 업데이트할 수 있습니다.

파일 시스템의 SSD IOPS 업데이트 방법(콘솔)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템으로 이동하여 SSD IOPS를 업데이트할 Windows 파일 시스템을 선택합니다.
3. 작업에서 SSD IOPS 업데이트를 선택합니다. 또는 요약 패널에서 프로비저닝된 SSD IOPS 옆의 업데이트 버튼을 선택합니다. IOPS 프로비저닝 업데이트 창이 열립니다.



4. 모드에서 자동 또는 사용자 프로비저닝을 선택합니다. 자동을 선택하면 Amazon FSx는 파일 시스템의 스토리지 용량 GiB당 3개의 SSD IOPS를 자동으로 프로비저닝합니다. 사용자 프로비저닝을 선택하는 경우 96~400,000 범위의 정수를 입력합니다.

5. 업데이트를 선택하여 프로비저닝된 SSD IOPS 업데이트를 시작합니다.
6. 업데이트 탭의 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다.

파일 시스템의 SSD IOPS 업데이트 방법(CLI)

FSx for Windows File Server 파일 시스템의 SSD IOPS를 업데이트하려면 `--windows-configuration DiskIopsConfiguration` 속성을 사용합니다. 이 속성에는 `Iops` 및 `Mode`라는 두 개의 파라미터가 있습니다.

- SSD IOPS 수를 지정하려면 지원되는 지역에서 최대 `Iops=`*`number_of_IOPS`* 400,000을 사용하십시오. AWS `Mode=USER_PROVISIONED`
- Amazon FSx에서 SSD IOPS를 자동으로 늘리도록 하려면 `Mode=AUTOMATIC`을 사용하고 `Iops` 파라미터를 사용하지 않습니다. Amazon FSx는 파일 시스템의 스토리지 용량 GiB당 3개의 SSD IOPS를 자동으로 유지하며, 지원되는 지역에서는 최대 40만 IOPS를 유지합니다. AWS

명령을 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. AWS CLI describe-file-systems 출력에서 `administrative-actions`를 찾습니다.

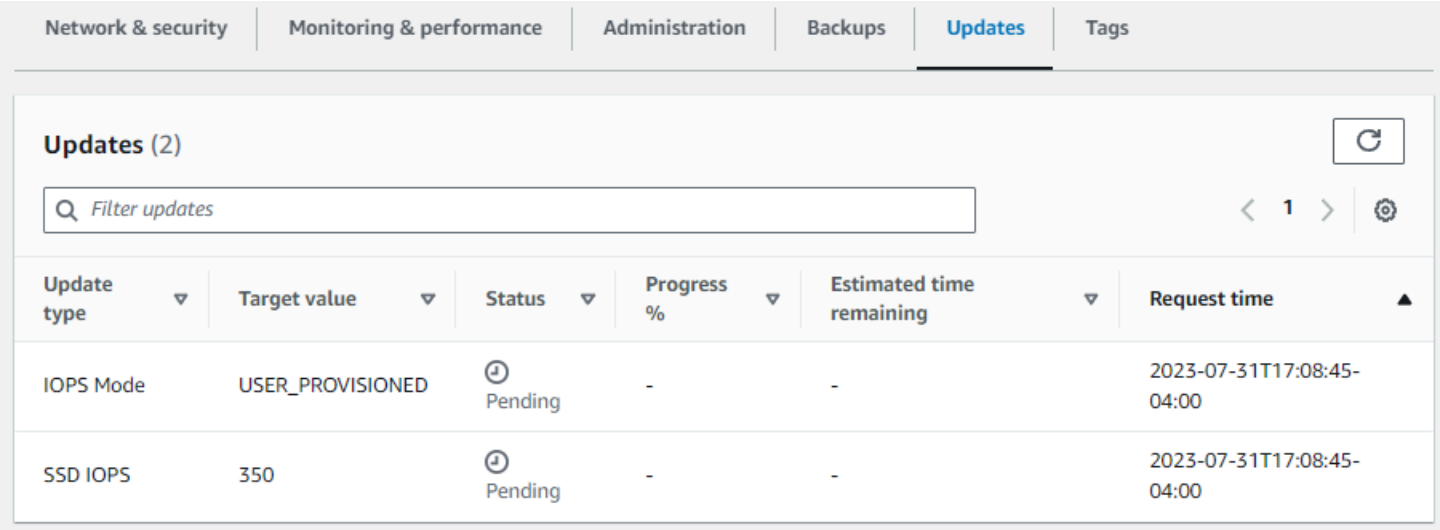
자세한 내용은 을 참조하십시오 AdministrativeAction.

프로비저닝된 SSD IOPS 업데이트 모니터링

Amazon FSx 콘솔, AWS CLI 또는 API를 사용하여 프로비저닝된 SSD IOPS 업데이트 진행 상황을 모니터링할 수 있습니다.

콘솔에서 업데이트 모니터링

파일 시스템 세부 정보 창의 업데이트 탭에서 각 업데이트 유형에 대한 최신 업데이트 10개를 볼 수 있습니다.



프로비저닝된 SSD IOPS 업데이트의 경우 다음 정보를 볼 수 있습니다.

업데이트 유형

가능한 값은 IOPS 모드와 SSD IOPS입니다.

대상 값

파일 시스템의 IOPS 모드 및 SSD IOPS를 업데이트하는 데 필요한 값입니다.

상태

업데이트의 현재 상태입니다. SSD IOPS 업데이트에 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 - 워크로드의 쓰기 작업에 새 IOPS 수준을 사용할 수 있습니다. 업데이트는 업데이트 후 최적화 중 상태로 전환되며, 이 상태는 일반적으로 몇 시간 동안 지속되어 이 기간 동안 워크로드의 읽기 작업은 이전 수준과 새 수준 사이의 IOPS 성능을 유지합니다. 업데이트 작업이 완료되면 새 IOPS 수준을 읽기와 쓰기 모두에 사용할 수 있습니다.
- 완료 - SSD IOPS 업데이트가 완료되었습니다.
- 실패 - SSD IOPS 업데이트에 실패했습니다. 스토리지 업데이트가 실패한 자세한 이유를 보려면 ?를 선택합니다.

진행률(%)

스토리지 최적화 프로세스의 진행률을 완료율로 표시합니다.

요청 시간

Amazon FSx가 업데이트 작업 요청을 받은 시간입니다.

AWS CLI 및 API를 사용하여 업데이트 모니터링

describe-file-systemsAWS CLI명령과 DescribeFileSystemsAPI 작업을 사용하여 파일 시스템 SSD IOPS 업데이트 요청을 보고 모니터링할 수 있습니다. `AdministrativeActions` 배열에 각 관리 작업 유형에 대한 가장 최근의 업데이트 작업 10개가 나열됩니다. 파일 시스템의 SSD IOPS를 늘리면 `FILE_SYSTEM_UPDATE`와 `IOPS_OPTIMIZATION`이라는 두 개의 `AdministrativeActions` 작업이 생성됩니다.

처리량 용량 관리

모든 FSx for Windows File Server 파일 시스템에는 파일 시스템을 생성할 때 구성된 처리량 용량이 있습니다. 언제든지 필요할 때마다 파일 시스템의 처리량 용량을 수정할 수 있습니다. 처리량 용량은 파일 시스템을 호스팅하는 파일 서버의 파일 데이터 서비스 제공 속도를 결정하는 요소 중 하나입니다. 처리량 용량이 높을수록 초당 I/O 작업 수(IOPS) 및 파일 서버의 데이터 캐싱을 위한 메모리 용량 또한 많아집니다. 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

파일 시스템의 처리량 용량을 수정하면 Amazon FSx가 파일 시스템의 파일 서버를 백그라운드에서 교체합니다. 다중 AZ 파일 시스템의 경우 Amazon FSx가 기본 파일 서버와 보조 파일 서버를 교체하는 동안 자동 장애 조치 및 페일백이 발생합니다. 단일 AZ 시스템의 경우 처리량 용량 스케일링 중에 몇 분 동안 파일 시스템을 사용할 수 없게 됩니다. 새 처리량 용량을 파일 시스템에서 사용할 수 있게 되면 요금이 청구됩니다.

> **Note**
>
> 백엔드의 파일 시스템 유지 관리 작업 중에는 시스템 수정(예: 처리량 용량 수정)이 지연될 수 있습니다. 유지 관리로 인해 이러한 변경 사항은 다음에 처리될 때까지 대기열에 추가될 수 있습니다.

주제

- 처리량 용량을 수정해야 하는 경우
- 처리량 용량을 수정하는 방법
- 처리량 용량 변화 모니터링

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 성능(처리량 및 IOPS)은 파일 시스템의 처리량 용량, 스토리지 용량, 스토리지 유형뿐 아니라 특정 워크로드의 특성에 따라 달라집니다. CloudWatch 지표를 사용하여 성능 개선을 위해 변경해야 할 측정기준을 결정할 수 있습니다. 자세한 내용은 Amazon을 통한 지표 모니터링 CloudWatch 섹션을 참조하세요.

다중 AZ 파일 시스템의 경우 처리량 용량 스케일링을 통해 Amazon FSx가 기본 파일 서버와 보조 파일 서버를 교체하는 동안 자동 장애 조치 및 페일백이 발생합니다. 처리량 용량 스케일링 중에 또는 파일 시스템 유지 관리 및 예상치 못한 서비스 중단 중에 발생하는 파일 서버 교체 중에는 나머지 파일 서버가 파일 시스템으로 향하는 모든 지속적인 트래픽을 처리합니다. 교체된 파일 서버가 다시 온라인 상태가 되면 FSx for Windows는 재동기화 작업을 실행하여 데이터가 새로 교체된 파일 서버에 다시 동기화되도록 합니다.

FSx for Windows는 이러한 재동기화 활동이 애플리케이션과 사용자에게 미치는 영향을 최소화하도록 설계되었습니다. 하지만 재동기화 프로세스에는 데이터를 큰 블록 단위로 동기화하는 작업이 포함됩니다. 즉, 일부만 업데이트되더라도 큰 데이터 블록의 동기화가 필요할 수 있습니다. 따라서 재동기화 양은 데이터 변동량뿐만 아니라 파일 시스템의 데이터 변동 특성에 따라서도 달라집니다. 워크로드에 쓰기 작업이 많고 IOPS가 많은 경우 데이터 동기화 프로세스에 시간이 더 오래 걸리고 추가 성능 리소스가 필요할 수 있습니다.

이 기간 동안에도 파일 시스템을 계속 사용할 수 있지만 데이터 동기화 기간을 줄이려면 파일 시스템의 부하가 최소화되는 유휴 기간 동안 처리량 용량을 수정하는 것이 좋습니다. 또한 데이터 동기화 기간을 줄이려면 워크로드 외에 동기화 작업을 실행할 수 있는 충분한 처리량 용량이 파일 시스템에 있는지 확인하는 것이 좋습니다. 마지막으로, 파일 시스템의 부하가 적은 상태에서 장애 조치가 미치는 영향을 테스트하는 것이 좋습니다.

처리량 용량을 수정하는 방법

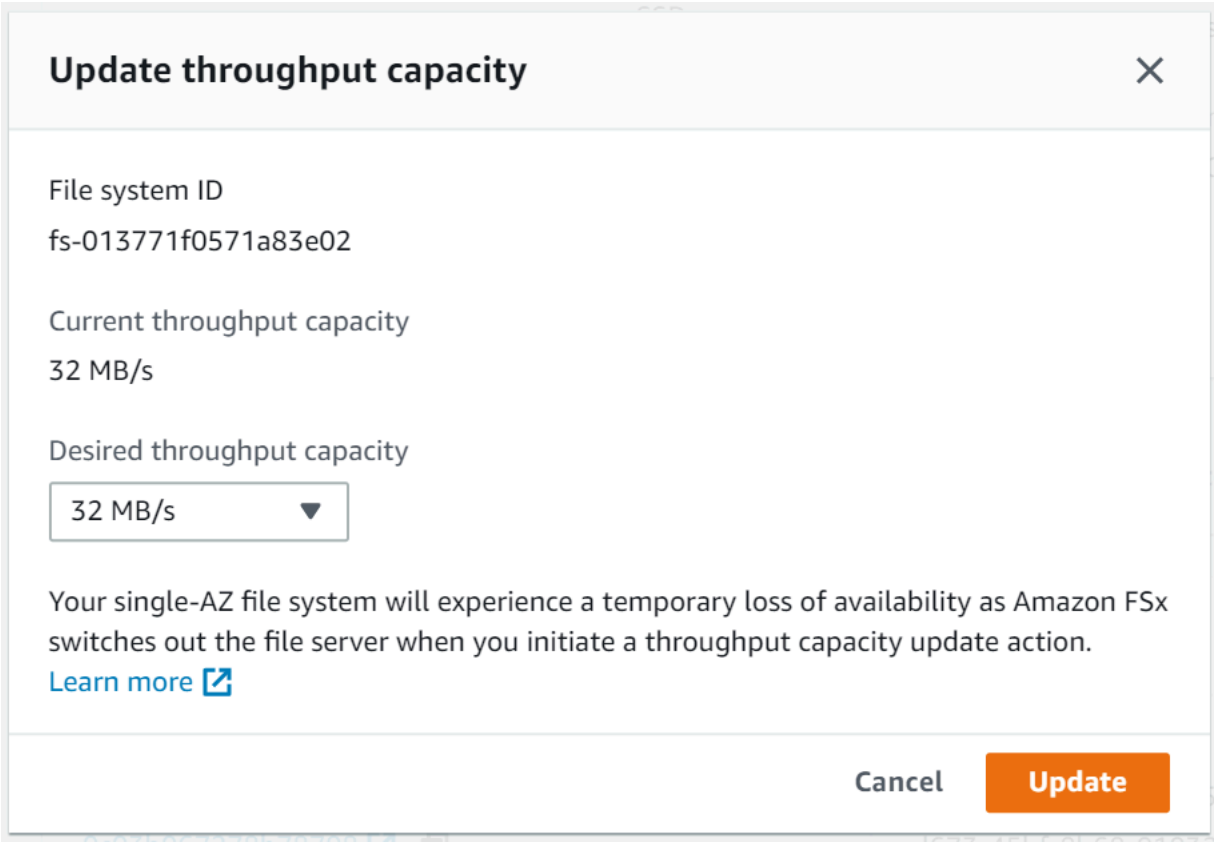
Amazon FSx 콘솔, AWS Command Line Interface(AWS CLI) 또는 Amazon FSx API를 사용하여 파일 시스템의 처리량 용량을 수정할 수 있습니다.

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 Windows 파일 시스템을 선택합니다.
3. 작업에서 처리량 업데이트를 선택합니다. 또는 요약 패널에서 파일 시스템의 처리량 용량 옆에 있는 업데이트를 선택합니다.

처리량 용량 업데이트 창이 표시됩니다.

4. 목록에서 처리량 용량의 새 값을 선택합니다.



5. 업데이트를 선택하여 처리량 용량 업데이트를 시작합니다.

> **Note**
>
> 다중 AZ 파일 시스템은 처리량 스케일링 업데이트 시 장애 조치 및 페일백되며 완전히 사용할 수 있습니다. 단일 AZ 파일 시스템은 업데이트 중에 매우 짧은 기간 동안 사용할 수 없게 됩니다.

6. 업데이트 탭의 파일 시스템 세부 정보 페이지에서 업데이트 진행 상황을 모니터링할 수 있습니다.

Amazon FSx 콘솔, AWS CLI 및 API를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 처리량 용량 변화 모니터링 섹션을 참조하세요.

파일 시스템의 처리량 용량 수정(CLI)

파일 시스템의 처리량 용량을 수정하려면 AWS CLI 명령 update-file-system을 사용합니다. 다음 파라미터를 설정합니다.

- `--file-system-id`를 업데이트하려는 파일 시스템의 ID로 설정합니다.
- `ThroughputCapacity`를 파일 시스템을 업데이트하려는 적정 값으로 설정합니다.

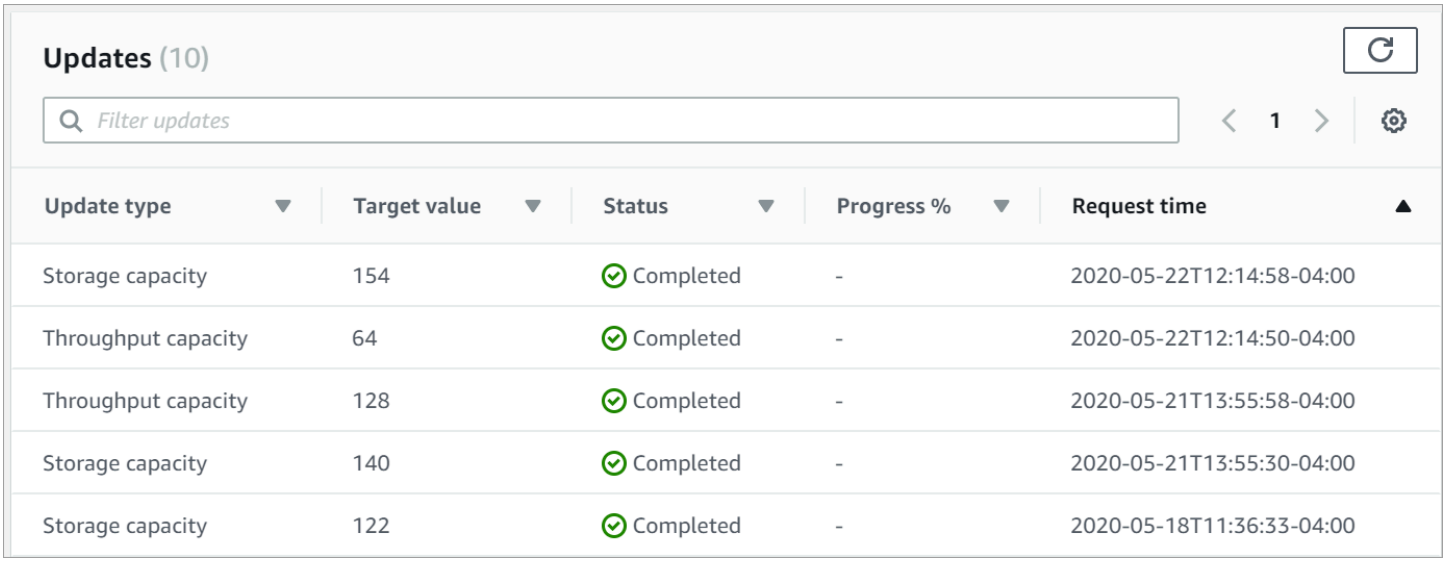
Amazon FSx 콘솔, AWS CLI 및 API를 사용하여 업데이트 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 처리량 용량 변화 모니터링 섹션을 참조하세요.

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

가능한 값은 처리량 용량입니다.

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.
- 업데이트 후 최적화 중 - Amazon FSx가 파일 시스템의 네트워크 I/O, CPU 및 메모리 리소스를 업데이트했습니다. 새로운 디스크 I/O 성능 수준을 쓰기 작업에 사용할 수 있습니다. 파일 시스템이 더 이상 이 상태가 아닐 때까지 읽기 작업에서는 이전 수준과 새 수준 사이의 디스크 I/O 성능을 확인할 수 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 8MB/s이고 목표 처리량 용량은 256MB/s입니다.

```
.
.
.
    "ThroughputCapacity": 8,
"AdministrativeActions": [
    {
        "AdministrativeActionType": "FILE_SYSTEM_UPDATE",
        "RequestTime": 1581694764.757,
        "Status": "PENDING",
        "TargetFileSystemValues": {
```

```
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

Amazon FSx가 작업 처리를 완료하면 상태가 COMPLETED로 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": {
          "WindowsConfiguration": {
            "ThroughputCapacity": 256
          }
        }
    }
]
```

처리량 용량 수정에 실패하면 상태가 FAILED로 변경되고 FailureDetails 속성이 실패에 대한 정보를 제공합니다. 실패 작업에 대한 문제 해결 방법은 스토리지 또는 처리량 용량 업데이트 실패 섹션을 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 환경을 기준으로 하는 등 AWS 리소스를 다양한 방식으로 분류할 수 있습니다. 이 기능은 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 사용자가 정의하는 키와 선택적 값으로 구성됩니다.

태그를 사용하면 용도, 소유자 또는 환경을 기준으로 하는 등 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 내용은 AWS 백서 태그 지정 모범 사례를 참조하세요.

태그는 Amazon FSx에는 의미가 없으며 엄격하게 문자열로 해석됩니다. 또한 태그는 리소스에 자동으로 배정되지 않습니다. 태그 키와 값을 편집할 수 있으며 언제든지 리소스에서 태그를 제거할 수 있습니다. 태그의 값을 빈 문자열로 설정할 수 있지만 태그의 값을 Null로 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 CLI 또는 AWS SDK를 사용하는 경우 `TagResource` API 작업을 사용하여 기존 리소스에 태그를 적용할 수 있습니다. 또한 일부 리소스 생성 작업에서는 리소스 생성 시 리소스의 태그를 지정할 수 있습니다. 리소스 생성 도중 태그를 적용할 수 없는 경우, 리소스 생성 프로세스가 롤백됩니다. 이는 태그를 사용하여 리소스가 생성되거나 아예 리소스가 생성되지 않도록 하고 언제든 태그 지정되지 않은 리소스가 남지 않게 합니다. 생성 시 리소스에 태그를 지정하면 리소스 생성 후 사용자 지정 태그 지정 스크립트를 실행할 필요가 없습니다. 사용자가 생성 시 리소스 태그를 지정할 수 있도록 하는 방법에 대한 자세한 내용은 생성 시 리소스 태그 지정에 대한 권한 부여 섹션을 참조하세요.

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 Name 키를 값과 함께 적용할 수 있으며, 새 파일 시스템을 생성할 때 원하는 태그를 적용할 수 있습

니다. 콘솔은 Name 태그에 따라 리소스를 조직할 수 있지만 이 태그는 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. 리소스를 생성하면 태그가 즉시 적용되기 때문에 생성 단계부터 리소스를 적절하게 보호할 수 있습니다. 따라서 태그를 기반으로 리소스 사용을 제어하는 리소스 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.

결제를 위한 리소스 태그 지정에 대한 자세한 내용은 AWS Billing 사용 설명서에서 비용 할당 태그 사용을 참조하세요.

태그 제한

태그에 적용되는 기본 제한은 다음과 같습니다.

- 리소스당 최대 태그 수 – 50개
- 각 리소스에 대해 각 태그 키는 고유하며 하나의 값만 가질 수 있습니다.
- 최대 키 길이 - UTF-8 형식의 유니코드 문자 128자
- 최대 값 길이 - UTF-8 형식의 유니코드 문자 256자
- Amazon FSx 태그에서 허용되는 문자는 UTF-8로 표현할 수 있는 문자, 숫자 및 공백과 특수 문자 + - = . _ : / @입니다.
- 태그 키와 값은 대/소문자를 구분합니다.
- `aws:` 접두사는 AWS용으로 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 `DeleteMe`라는 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 경우 할당하는 태그는 사용자의 AWS 계정에만 사용할 수 있으며 다른 AWS 계정은 해당 태그에 액세스할 수 없습니다. 공유 리소스에 대한 태그 기반 액세스 제어의 경우 각 AWS 계정은 리소스에 대한 액세스를 제어하기 위해 자체 태그 세트를 할당해야 합니다.

권한 및 태그

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.

Amazon FSx 유지 관리 기간 작업

Amazon FSx for Windows File Server는 관리하는 Microsoft Windows Server 소프트웨어에 대해 정기적인 소프트웨어 패치 적용을 수행합니다. 유지 관리 기간을 통해 소프트웨어 패치 적용이 발생하는 요일 및 시간을 제어할 수 있습니다. 파일 시스템 생성 중에 유지 관리 기간을 선택합니다. 원하는 시간이 없는 경우 30분의 기본 기간이 지정됩니다.

FSx for Windows File Server를 사용하면 워크로드 및 운영 요구 사항에 맞게 유지 관리 기간을 조정할 수 있습니다. 유지 관리 기간이 14일에 한 번 이상으로 예약되어 있는 경우, 필요에 따라 유지 관리 기간을 수시로 이동할 수 있습니다. 패치가 릴리스되고 14일 이내에 유지 관리 기간을 예약하지 않은 경우 FSx for Windows File Server는 파일 시스템의 보안 및 안정성을 보장하기 위해 파일 시스템에 대한 유지 관리를 진행합니다.

패치 적용이 진행 중인 동안에는 단일 AZ 파일 시스템을 사용할 수 없게 될 수 있으며, 일반적으로 그 기간은 20분 미만입니다. 다중 AZ 파일 시스템은 계속 사용할 수 있으며 기본 파일 서버와 대기 파일 서버 간에 자동으로 장애 조치 및 페일백됩니다. 자세한 내용은 FSx for Windows File Server의 장애 조치 프로세스 섹션을 참조하세요. 다중 AZ 파일 시스템에 대한 패치 적용에는 장애 조치와 페일백이 포함되므로 이 시간 동안 파일 시스템으로 향하는 모든 트래픽은 기본 파일 서버와 대기 파일 서버 간에 동기화되어야 합니다. 패치 적용 시간을 줄이려면 파일 시스템의 부하가 최소인 유휴 기간에 유지 관리 기간을 예약하는 것이 좋습니다.

> **Note**
>
> 유지 관리 작업 중 데이터 무결성을 보장하기 위해 Amazon FSx for Windows File Server는 유지 관리가 시작되기 전에 파일 시스템을 호스팅하는 기본 스토리지 볼륨에 대한 보류 중인 쓰기 작업을 모두 완료합니다.

Amazon FSx 관리 콘솔, AWS CLI, AWS, API 또는 AWS SDK 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. 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 관리 설정 패널에 표시됩니다.

update-file system CLI 명령을 사용하여 주별 유지 관리 기간을 변경하려면 연습 3: 기존 파일 시스템 업데이트 섹션을 참조하세요.

Amazon FSx 파일 시스템 관리 모범 사례

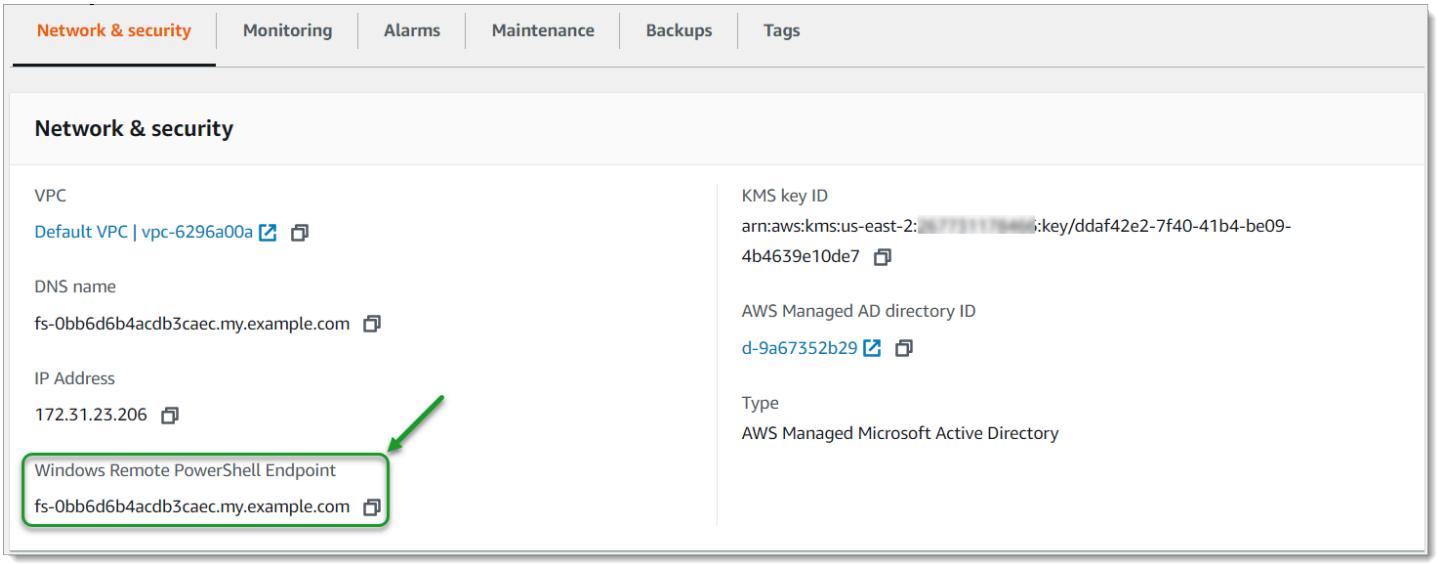
Amazon FSx는 파일 시스템 관리에 대한 모범 사례를 구현하는 데 도움이 되는 다음과 같은 여러 기능을 제공합니다.

- 스토리지 사용 최적화
- 최종 사용자가 파일 및 폴더를 이전 버전으로 복구할 수 있도록 지원
- 연결된 모든 클라이언트에 암호화 적용

명령에 대해 다음 Amazon FSx CLI를 사용하여 파일 시스템에 PowerShell 이러한 모범 사례를 신속하게 구현하십시오.

이러한 명령을 실행하려면 파일 시스템의 Windows 원격 PowerShell 엔드포인트를 알아야 합니다. 이 엔드포인트를 찾으려면 다음 단계를 따라하세요.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템을 선택합니다. 네트워크 및 보안 탭에서 다음과 같이 Windows 원격 PowerShell 엔드포인트를 찾습니다.



자세한 내용은 파일 시스템 관리 및 아마존 FSx CLI를 사용하는 방법 PowerShell 섹션을 참조하세요.

주제

- 일회성 관리 설정 작업
- 파일 시스템을 모니터링하기 위한 지속적인 관리 작업

일회성 관리 설정 작업

다음은 파일 시스템에 한 번 빠르게 설정할 수 있는 작업입니다.

스토리지 사용량 관리

다음 명령을 사용하여 파일 시스템 스토리지 사용량을 관리합니다.

- 기본 일정에 따라 데이터 중복 제거를 활성화하려면 다음 명령을 실행합니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FsxDedup }
```

선택적으로, 최소 파일 보존 기간 없이 다음 명령을 사용하여 파일이 생성된 직후 파일에서 데이터 중복 제거 작업을 실행할 수 있습니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FSxDedupConfiguration -MinimumFileAgeDays 0 }
```

자세한 내용은 데이터 중복 제거 섹션을 참조하세요.

- 다음 명령을 사용하여 "추적" 모드에서 사용자 스토리지 할당량을 활성화할 수 있습니다. 이 모드는 보고 목적으로만 사용되며 적용을 위한 것이 아닙니다.

```
$QuotaLimit = Quota limit in bytes
$QuotaWarningLimit = Quota warning threshold in bytes
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Enable-FSxUserQuotas -Track -DefaultLimit
 $Using:QuotaLimit -DefaultWarningLimit $Using:QuotaWarningLimit }
```

자세한 내용은 스토리지 할당량 섹션을 참조하세요.

섀도우 복사본을 활성화하여 최종 사용자가 파일 및 폴더를 이전 버전으로 복구할 수 있도록 지원

다음과 같이 기본 일정(평일 오전 7시와 정오)에 따라 섀도우 복제본을 활성화합니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowStorage -Default }

Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxShadowCopySchedule -Default -Confirm:$False}
```

자세한 정보는 기본 저장소 및 스케줄을 사용하도록 섀도 복사본을 구성합니다.을 참조하세요.

전송 중 암호화 적용

다음 명령은 파일 시스템에 연결하는 클라이언트에 대해 암호화를 적용합니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Set-FsxSmbServerConfiguration -EncryptData $True -
RejectUnencryptedAccess $True -Confirm:$False}
```

열려 있는 모든 세션을 닫고 암호화를 사용하여 현재 연결된 클라이언트가 다시 연결되도록 할 수 있습니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbSession -Confirm:$False}
```

자세한 내용은 전송 중 암호화 관리 및 사용자 세션 및 열린 파일 섹션을 참조하세요.

파일 시스템을 모니터링하기 위한 지속적인 관리 작업

다음과 같은 지속적인 작업을 통해 파일 시스템의 디스크 사용량, 사용자 할당량 및 열린 파일을 모니터링할 수 있습니다.

데이터 중복 제거 상태 모니터링

다음과 같이 파일 시스템에서 달성한 절감률을 포함하여 중복 제거 상태를 모니터링합니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -
ConfigurationName FsxRemoteAdmin -ScriptBlock { Get-FSxDedupStatus } | select
 OptimizedFilesCount,OptimizedFilesSize,SavedSpace,OptimizedFilesSavingsRate
```

사용자 수준 스토리지 사용량 모니터링

사용 중인 공간, 한도 및 경고 임계값 위반 여부 등 현재 사용자 스토리지 할당량 항목에 대한 보고서를 받아봅니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxUserQuotaEntries }
```

열린 파일 모니터링 및 닫기

열려 있는 파일을 찾고 닫아 열린 파일을 관리합니다. 다음 명령을 사용하여 열린 파일이 있는지 확인합니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Get-FSxSmbOpenFile}
```

다음 명령을 사용하여 열린 파일을 닫습니다.

```
Invoke-Command -ComputerName $FSxWindowsRemotePowerShellEndpoint -ConfigurationName
 FSxRemoteAdmin -ScriptBlock { Close-FSxSmbOpenFile -Confirm:$false}
```

DFS 네임스페이스로 여러 파일 시스템 그룹화

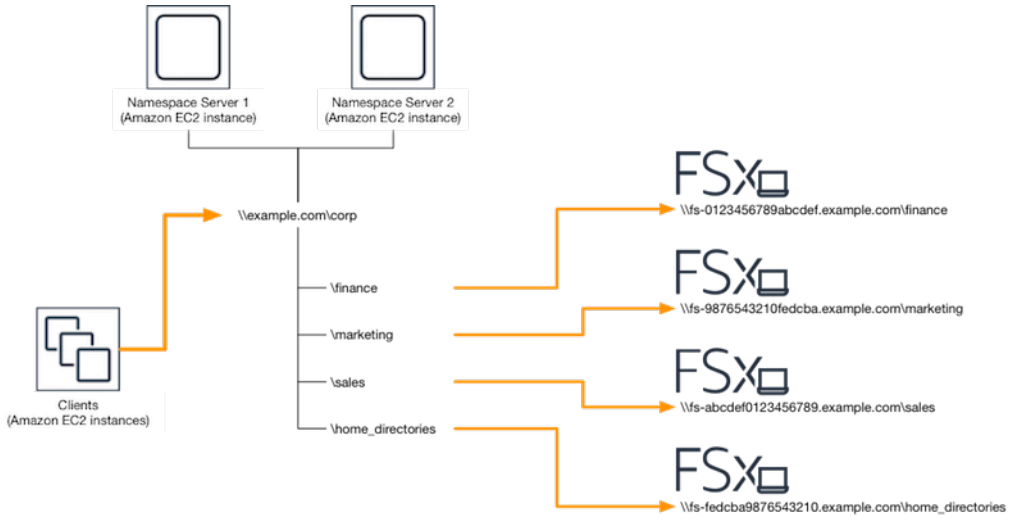
Amazon FSx for Windows File Server는 Microsoft의 분산 파일 시스템(DFS) 네임스페이스 사용을 지원합니다. DFS 네임스페이스를 사용하여 여러 파일 시스템의 파일 공유를 하나의 공통 폴더 구조(네임스페이스)로 그룹화하여 전체 파일 데이터 세트에 액세스하는 데 사용할 수 있습니다. DFS 네임스페이스를 사용하면 여러 파일 시스템에서 파일 공유에 대한 액세스를 구성하고 통합할 수 있습니다. 또한 DFS 네임스페이스는 대용량 파일 데이터 세트에 대해 각 파일 시스템이 지원하는 용량(64TB)을 초과하여 최대 수백 페타바이트까지 파일 데이터 스토리지를 확장하는 데 도움이 될 수 있습니다.

여러 파일 시스템을 그룹화하기 위한 DFS 네임스페이스 설정

DFS 네임스페이스를 사용하여 여러 파일 시스템을 단일 네임스페이스로 그룹화할 수 있습니다. 다음 예제에서는 도메인 기반 네임스페이스(example.com\corp)가 두 개의 네임스페이스 서버에 생성되어 여러 Amazon FSx 파일 시스템(재무, 마케팅, 영업, 홈 디렉터리)에 저장된 파일 공유를 통합합니다. 이렇게 하면 사용자가 공통 네임스페이스를 사용하여 파일 공유에 액세스할 수 있습니다. 따라서 파일 공유를 호스팅하는 각 파일 시스템에 대해 파일 시스템 DNS 이름을 지정할 필요가 없습니다.

> **Note**
>
> Amazon FSx는 DFS 공유 경로의 루트에 추가할 수 없습니다.

다음 단계는 두 네임스페이스 서버에 단일 네임스페이스(example.com\corp)를 생성하는 방법을 안내합니다. 또한 네임스페이스 아래에 4개의 파일 공유를 설정하여 각 파일 공유를 별도의 Amazon FSx 파일 시스템에 호스팅된 공유로 투명하게 리디렉션합니다.



여러 파일 시스템을 공통 DFS 네임스페이스로 그룹화

1. 아직 DFS 네임스페이스 서버를 실행하고 있지 않은 경우 Setup-DFSN-servers.template 템플릿을 사용하여 가용성이 높은 DFS 네임스페이스 서버 쌍을 시작할 수 있습니다. AWS CloudFormation 스택 생성에 대한 자세한 내용은 사용 설명서의 콘솔에서 스택 생성을 참조하십시오. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. AWS 위임 관리자 그룹의 사용자로 이전 단계에서 시작한 DFS 네임스페이스 서버 중 하나에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. DFS 관리 콘솔을 열어 액세스합니다. 시작 메뉴를 열고 dfsmgmt.msc를 실행합니다. 그러면 DFS 관리 GUI 도구가 열립니다.
4. 작업 , 새 네임스페이스 순으로 선택하고 서버용으로 시작한 첫 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력한 후 다음을 선택합니다.
5. 이름에는 만들려는 네임스페이스(예: corp)를 입력합니다.
6. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정합니다. 다음을 선택합니다.
7. 기본 도메인 기반 네임스페이스 옵션을 선택한 상태로 두고 Windows Server 2008 모드 활성화 옵션을 선택한 상태로 두고 다음을 선택합니다.

   > **Note**
   >
   > Windows Server 2008 모드는 네임스페이스에 사용할 수 있는 최신 옵션입니다.

8. 네임스페이스 설정을 검토한 다음 생성을 선택합니다.
9. 탐색 표시줄의 네임스페이스에서 새로 만든 네임스페이스를 선택한 상태에서 작업, 네임스페이스 서버 추가 순으로 선택합니다.
10. 네임스페이스 서버용으로 시작한 두 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력합니다.
11. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정한 다음 확인을 선택합니다.
12. 방금 만든 네임스페이스의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 폴더를 선택한 다음 폴더 이름(예: 이름에 `finance`)을 입력하고 확인을 선택합니다.
13. 폴더 대상 경로에 DFS 네임스페이스 폴더가 가리킬 파일 공유의 DNS 이름을 UNC 형식으로 입력하고(예: `\\fs-0123456789abcdef0.example.com\finance`) 확인을 선택합니다.
14. 공유가 존재하지 않는 경우:

    a. 예를 선택하여 생성합니다.

    b. 공유 생성 대화 상자에서 탐색을 선택합니다.

    c. 기존 폴더를 선택하거나 D$에서 새 폴더를 만든 다음 확인을 선택합니다.

d. 적절한 공유 권한을 설정하고 확인을 선택합니다.

15. 새 폴더 대화 상자에서 확인을 선택합니다. 네임스페이스 아래에 새 폴더가 생성됩니다.
16. 동일한 네임스페이스에서 공유하려는 다른 폴더에 대해 마지막 네 단계를 반복합니다.

Amazon FSx for Windows File Server 모니터링

모니터링은 Amazon FSx 및 솔루션의 안정성, 가용성 및 성능을 유지하는 데 있어 중요한 부분입니다. AWS 다중 지점 장애가 발생할 경우 이를 보다 쉽게 디버깅할 수 있도록 AWS 솔루션의 모든 부분에서 모니터링 데이터를 수집해야 합니다. 하지만 Amazon FSx 모니터링을 시작하기 전에 다음 질문에 대한 답변을 포함하는 모니터링 계획을 수립해야 합니다.

- 모니터링의 목표
- 모니터링할 리소스
- 이러한 리소스를 모니터링하는 빈도
- 사용할 모니터링 도구
- 모니터링 작업을 수행할 사람
- 문제 발생 시 알려야 할 대상

FSx for Windows File Server의 로깅 및 모니터링에 대한 자세한 내용은 다음 주제를 참조하세요.

주제

- 모니터링 도구
- Amazon을 통한 지표 모니터링 CloudWatch
- AWS CloudTrail을 사용하여 Amazon FSx for Windows File Server API 호출 로깅

모니터링 도구

AWS Amazon FSx를 모니터링하는 데 사용할 수 있는 다양한 도구를 제공합니다. 이들 도구 중에는 모니터링을 자동으로 수행하도록 구성할 수 있는 도구도 있지만, 수동 작업이 필요한 도구도 있습니다. 모니터링 작업은 최대한 자동화하는 것이 좋습니다.

자동 모니터링 도구

다음과 같은 자동 모니터링 도구를 사용하여 Amazon FSx를 관찰하고 문제 발생 시 보고할 수 있습니다.

- Amazon CloudWatch Alarms — 지정한 기간 동안 단일 지표를 관찰하고 일정 기간 동안 지정된 임계값을 기준으로 지표의 값을 기준으로 하나 이상의 작업을 수행합니다. 작업은 아마존 심플 알

림 서비스 (Amazon SNS) 주제 또는 Amazon EC2 Auto Scaling 정책으로 전송되는 알림입니다. CloudWatch 경보가 특정 상태에 있다는 이유만으로 경보가 작업을 호출하는 것은 아닙니다. 상태가 변경되고 지정된 기간 동안 유지되어야 합니다. 자세한 정보는 Amazon을 통한 지표 모니터링 CloudWatch을 참조하세요.

- Amazon CloudWatch Logs — AWS CloudTrail 또는 다른 소스에서 로그 파일을 모니터링, 저장 및 액세스합니다. 자세한 내용은 Amazon CloudWatch Logs란 무엇입니까? 를 참조하십시오. Amazon CloudWatch Logs 사용 설명서에서 확인할 수 있습니다.
- AWS CloudTrail 로그 모니터링 — 계정 간에 로그 파일을 공유하고, CloudTrail 로그 파일을 CloudWatch Logs로 전송하여 실시간으로 모니터링하고, Java로 로그 처리 애플리케이션을 작성하고, 전송 후 로그 파일이 변경되지 않았는지 확인합니다 CloudTrail. 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 로그 파일 작업을 참조하십시오.

수동 모니터링 도구

Amazon FSx 모니터링의 또 다른 중요한 부분은 Amazon 경보에서 다루지 않는 항목을 수동으로 모니터링하는 것입니다. CloudWatch Amazon FSx CloudWatch 및 AWS 기타 콘솔 at-a-glance 대시보드는 환경 상태를 보여줍니다. AWS

Amazon FSx 콘솔의 모니터링 및 성능 대시보드는 다음을 보여줍니다.

- Windows File Server용 최신 FSx 경고 및 경보 CloudWatch
- 파일 시스템 활동 요약을 보여주는 그래프
- 파일 시스템 스토리지 용량 및 사용률 그래프
- 파일 서버 및 스토리지 볼륨 성능 그래프
- CloudWatch 알람

CloudWatch 홈 페이지에는 다음이 표시됩니다.

- 현재 경보 및 상태
- 경보 및 리소스 그래프
- 서비스 상태

또한 다음을 CloudWatch 사용하여 수행할 수 있습니다.

- 사용자 지정 대시보드를 만들어 사용하는 서비스 모니터링

- 지표 데이터를 그래프로 작성하여 문제를 해결하고 추세 파악
- 모든 AWS 리소스 메트릭을 검색하고 찾아보십시오.
- 문제에 대해 알려주는 경보 생성 및 편집

Amazon FSx 모니터링 및 성능 대시보드에 대한 자세한 내용은 FSx for Windows File Server 지표를 사용하는 방법 섹션을 참조하세요.

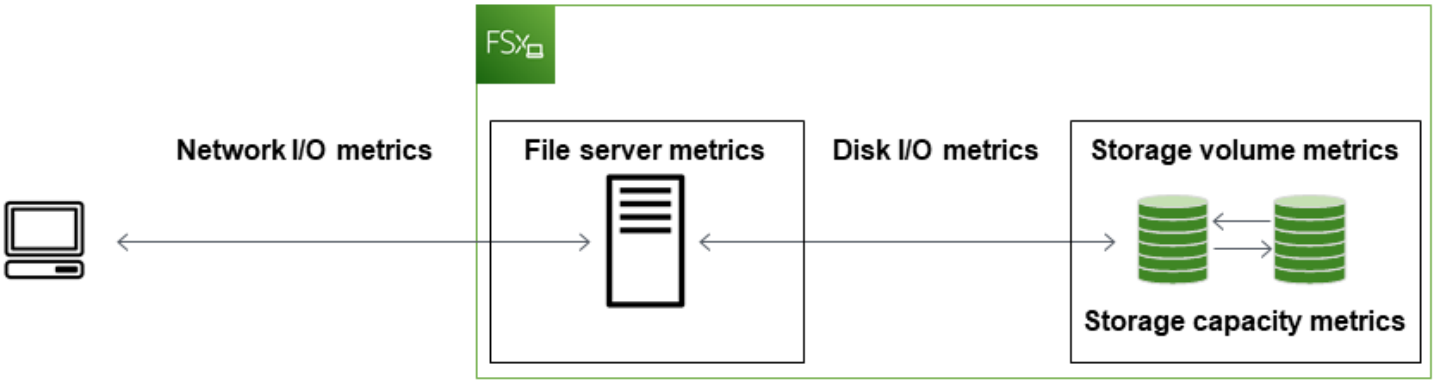
Amazon을 통한 지표 모니터링 CloudWatch

Windows File Server용 FSx의 원시 데이터를 수집하여 거의 실시간으로 읽을 수 있는 지표로 처리하는 CloudWatch Amazon을 사용하여 Windows File Server용 FSx 파일 시스템을 모니터링할 수 있습니다. 이러한 통계는 15개월간 유지되므로 기록 정보를 보고 웹 애플리케이션이나 파일 시스템이 어떻게 실행되고 있는지 전체적으로 파악할 수 있습니다.

Windows용 FSx File CloudWatch Server는 다음 도메인에 메트릭을 게시합니다.

- 네트워크 I/O 지표는 파일 시스템에 액세스하는 클라이언트와 파일 서버 간의 활동을 측정합니다.
- 파일 서버 지표는 네트워크 처리량 사용률, 파일 서버 CPU 및 메모리, 파일 서버 디스크 처리량 및 IOPS 사용률을 측정합니다.
- 디스크 I/O 지표는 파일 서버와 스토리지 볼륨 간의 활동을 측정합니다.
- 스토리지 볼륨 지표는 HDD 스토리지 볼륨의 디스크 처리량 사용률과 SSD 스토리지 볼륨의 IOPS 사용률을 측정합니다.
- 스토리지 용량 지표는 데이터 중복 제거로 인한 스토리지 절감을 포함하여 스토리지 사용량을 측정합니다.

다음 다이어그램은 FSx for Windows File Server 파일 시스템, 해당 구성 요소 및 지표 도메인을 보여줍니다.



기본적으로 Windows File Server용 Amazon FSx는 1분 간격으로 메트릭 CloudWatch 데이터를 전송하지만, 5분 간격으로 전송되는 다음과 같은 예외가 있습니다.

- `FileServerDiskThroughputBalance`
- `FileServerDiskIopsBalance`

에 대한 CloudWatch 자세한 내용은 Amazon이란 무엇입니까 CloudWatch? 를 참조하십시오. Amazon CloudWatch 사용 설명서에서 확인할 수 있습니다.

파일 시스템 유지 관리 또는 인프라 구성 요소 교체 중에는 단일 AZ 파일 시스템에 대한 지표가 게시되지 않고, 기본 파일 서버와 보조 파일 서버 간의 장애 조치 및 페일백 중에는 다중 AZ 파일 시스템에 대한 지표가 게시되지 않을 수 있습니다.

일부 Amazon CloudWatch FSx 지표는 원시 바이트로 보고됩니다. 바이트는 단위의 십진수나 이진수에 반올림되지 않습니다.

주제

지표 및 측정기준

Windows용 FSx File Server는 모든 파일 시스템의 Amazon에 있는 네임스페이스에 CloudWatch 다음과 같은 `AWS/FSx` 메트릭을 게시합니다.

- `DataReadBytes`
- `DataWriteBytes`
- `DataReadOperations`
- `DataWriteOperations`
- `MetadataOperations`
- `FreeStorageCapacity`

Windows File Server용 FSx는 처리 용량이 32Mbps 이상인 파일 시스템을 위해 다음에 AWS/FSx 설명된 메트릭을 CloudWatch Amazon의 네임스페이스에 게시합니다.

주제

FSx for Windows 네트워크 I/O 지표

AWS/FSx 네임스페이스에는 다음 네트워크 I/O 지표가 포함되어 있습니다.

지표	설명
DataReadBytes	파일 시스템에 액세스하는 클라이언트의 읽기 작업에 대한 바이트 수입니다. 단위: 바이트 유효한 통계: Sum
DataWriteBytes	파일 시스템에 액세스하는 클라이언트의 쓰기 작업에 대한 바이트 수입니다. 단위: 바이트 유효한 통계: Sum
DataReadOperations	파일 시스템에 액세스하는 클라이언트의 읽기 작업 수입니다. 단위: 개 유효한 통계: Sum
DataWriteOperations	파일 시스템에 액세스하는 클라이언트의 쓰기 작업 수입니다.

지표	설명
	단위: 개 유효한 통계: Sum
MetadataOperations	파일 시스템에 액세스하는 클라이언트의 메타데이터 작업 수입니다. 단위: 개 유효한 통계: Sum
ClientConnections	클라이언트와 파일 서버 간의 활성 연결 수입니다. 단위: 개

FSx for Windows File Server 지표

AWS/FSx 네임스페이스에는 다음과 같은 파일 서버 지표가 포함되어 있습니다.

지표	설명
NetworkThroughputUtilization	파일 시스템에 액세스하는 클라이언트의 네트워크 처리량(프로비저닝된 한도 대비 백분율)입니다. 단위: 백분율
CPUUtilization	파일 서버의 CPU 리소스 사용률입니다. 단위: 백분율
MemoryUtilization	파일 서버의 메모리 리소스 사용률입니다. 단위: 백분율
FileServerDiskThroughputUtilization	파일 서버와 스토리지 볼륨 간의 디스크 처리량(처리량 용량에 따라 결정된 프로비저닝된 한도의 백분율)입니다. 단위: 백분율

지표	설명
FileServerDiskThroughputBalance	파일 서버와 스토리지 볼륨 간의 디스크 처리량에 사용할 수 있는 버스트 크레딧의 비율입니다. 처리량 용량이 256MBps 이하로 프로비저닝된 파일 시스템에 유효합니다. 단위: 백분율
FileServerDiskIopsUtilization	파일 서버와 스토리지 볼륨 간의 디스크 IOPS(처리량 용량에 따라 결정된 프로비저닝된 한도의 백분율)입니다. 단위: 백분율
FileServerDiskIopsBalance	파일 서버와 스토리지 볼륨 간의 디스크 IOPS에 사용할 수 있는 버스트 크레딧의 비율입니다. 처리량 용량이 256MBps 이하로 프로비저닝된 파일 시스템에 유효합니다. 단위: 백분율

FSx for Windows 디스크 I/O 지표

AWS/FSx 네임스페이스에는 다음 디스크 I/O 지표가 포함되어 있습니다.

지표	설명
DiskReadBytes	스토리지 볼륨에 액세스하는 읽기 작업의 바이트 수입니다. 단위: 바이트 유효 통계: Sum
DiskWriteBytes	스토리지 볼륨에 액세스하는 쓰기 작업의 바이트 수입니다. 단위: 바이트 유효 통계: Sum

지표	설명
DiskReadOperations	스토리지 볼륨에 액세스하는 파일 서버의 읽기 작업 수입니다. 단위: 개 유효한 통계: Sum
DiskWriteOperations	스토리지 볼륨에 액세스하는 파일 서버의 쓰기 작업 수입니다. 단위: 개 유효한 통계: Sum

FSx for Windows File 볼륨 지표

AWS/FSx 네임스페이스에는 다음 스토리지 볼륨 지표가 포함되어 있습니다.

지표	설명
DiskThroughputUtilization	(HDD만 해당) 파일 서버와 스토리지 볼륨 간의 디스크 처리량(스토리지 볼륨에 따라 결정된 프로비저닝된 한도의 백분율)입니다. 단위: 백분율
DiskThroughputBalance	(HDD만 해당) 스토리지 볼륨의 디스크 처리량에 사용할 수 있는 버스트 크레딧의 비율입니다. 단위: 백분율
DiskIopsUtilization	(SSD만 해당) 파일 서버와 스토리지 볼륨 간의 디스크 IOPS(스토리지 볼륨에 따라 결정된 프로비저닝된 IOPS 한도의 백분율)입니다. 단위: 백분율

FSx for Windows 스토리지 용량 지표

AWS/FSx 네임스페이스에는 다음 스토리지 용량 지표가 포함되어 있습니다.

지표	설명
FreeStorageCapacity	사용 가능한 스토리지 용량 크기입니다. 단위: 바이트 유효한 통계: Average, Minimum
StorageCapacityUtilization	사용된 물리적 스토리지 용량(총 스토리지 용량의 백분율)입니다. 단위: 백분율
DeduplicationSavedStorage	데이터 중복 제거(활성화된 경우)를 통해 절감되는 스토리지 공간의 양입니다. 단위: 바이트

FSx for Windows File 측정기준

FSx for Windows File Server 지표는 FSx 네임스페이스를 사용하며 단일 측정기준인 FileSystemId에 대한 지표를 제공합니다. 명령 또는 API 명령을 사용하여 파일 시스템의 ID를 찾을 수 있습니다 describe-file-systems AWS CLI . DescribeFileSystems 파일 시스템 ID는 *fs-0123456789abcdef0*의 형식을 사용합니다.

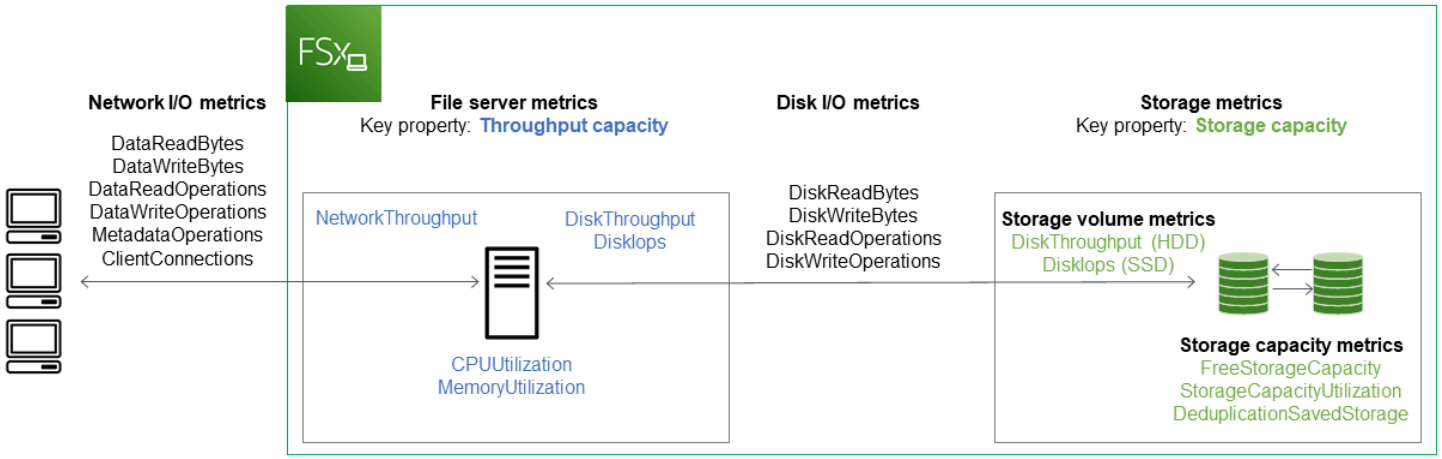
FSx for Windows File Server 지표를 사용하는 방법

각 Amazon FSx 파일 시스템에는 다음과 같은 두 가지 기본 아키텍처 구성 요소가 있습니다.

- 파일 시스템에 액세스하는 클라이언트에 데이터를 제공하는 파일 서버.
- 파일 시스템의 데이터를 호스팅하는 스토리지 볼륨.

FSx for Windows File Server는 파일 시스템의 파일 서버 및 스토리지 볼륨에 대한 성능 및 리소스 사용률을 추적하는 CloudWatch 지표를 보고합니다. 다음 다이어그램은 아키텍처 구성 요소가 포함된 Amazon FSx 파일 시스템과 모니터링에 사용할 수 있는 성능 및 CloudWatch 리소스 지표를 보여줍니

다. 지표 세트에 표시된 주요 속성은 해당 지표의 용량을 결정하는 파일 시스템 속성입니다. 해당 속성을 조정하면 해당 지표 세트에 대한 파일 시스템의 성능이 수정됩니다.



Amazon FSx 콘솔의 모니터링 및 성능 패널을 사용하여 다음 표에 설명된 Windows CloudWatch File Server용 FSx 측정치를 볼 수 있습니다.

모니터링 및 성능 패널	방법	차트	관련 지표
요약	...파일 시스템의 총 IOPS를 어떻게 확인하나요?	총 IOPS	합계(DataReadOperations +DataWriteOperations +MetadataOperations)/기간(초)
	...파일 시스템의 총 처리량을 어떻게 확인하나요?	총 처리량	합계(DataReadBytes +DataWriteBytes)/기간(초)
	...파일 시스템에서 사용 가능한 스토리지 용량을 어떻게 확인하나요?	사용 가능한 스토리지 용량	FreeStorageCapacity
	...클라이언트와 파일 서버 간에 설정된 연결 수를 어떻게 확인하나요?	클라이언트 연결	ClientConnections

모니터링 및 성능 패널	방법	차트	관련 지표
스토리지	...물리적 디스크 공간 사용량(파일 시스템의 총 스토리지 용량의 백분율)을 어떻게 확인하나요?	스토리지 용량 사용률	StorageCapacityUtilization
	...데이터 중복 제거로 절감되는 물리적 디스크 공간의 양을 어떻게 확인하나요?	데이터 중복 제거를 통해 절감된 스토리지	DeduplicationSavedStorage
성능 - 파일 서버	...파일 시스템에 액세스하는 클라이언트의 네트워크 처리량(프로비저닝된 한도 대비 백분율)을 어떻게 확인하나요?	네트워크 처리량 사용률	NetworkThroughputUtilization
	...파일 서버와 스토리지 볼륨 간의 디스크 처리량(처리량 용량에 따라 결정된 프로비저닝된 한도의 백분율)을 어떻게 확인하나요?	디스크 처리량 사용률	FileServerDiskThroughputUtilization
	...파일 서버와 스토리지 볼륨 간의 디스크 처리량에 사용할 수 있는 버스트 크레딧의 비율을 어떻게 확인하나요?	디스크 처리량 버스트 밸런스	FileServerDiskThroughputBalance
	...파일 서버와 스토리지 볼륨 간의 디스크 IOPS 양(처리량 용량에 따라 결정된 프로비저닝된 한도의 백분율)을 어떻게 확인하나요?	디스크 IOPS 사용률	FileServerDiskIopsUtilization
	...파일 서버와 스토리지 볼륨 간의 디스크 IOPS에 사용할 수 있는 버스트 크레딧의 비율을 어떻게 확인하나요?	디스크 IOPS 버스트 밸런스	FileServerDiskIopsBalance

모니터링 및 성능 패널	방법	차트	관련 지표
	...파일 서버의 CPU 사용률을 어떻게 확인하나요?	CPU 사용률	`CPUUtilization`
	...파일 서버의 메모리 사용률을 어떻게 확인하나요?	메모리 사용률	`MemoryUtilization`
성능 - 스토리지 볼륨	...스토리지 볼륨에 액세스하는 작업의 처리량(HDD 스토리지 용량에 따라 결정된 프로비저닝된 한도의 백분율)을 어떻게 확인하나요?	디스크 처리량 사용률(HDD)	`DiskThroughputUtilization`
	...HDD 스토리지 볼륨에 액세스하는 작업의 처리량에 사용할 수 있는 버스트 크레딧의 비율을 어떻게 확인하나요?	디스크 처리량 버스트 밸런스(HDD)	`DiskThroughputBalance`
	...스토리지 볼륨에 액세스하는 작업의 IOPS(SSD 스토리지 용량에 따라 결정된 프로비저닝된 한도의 백분율)을 어떻게 확인하나요?	디스크 IOPS 사용률(SSD)	`DiskIopsUtilization`

> **Note**
>
> 예상치 못한 워크로드 스파이크는 물론 백그라운드 Windows 스토리지 작업(예: 스토리지 동기화, 중복 제거 또는 섀도우 복사본)에 대비해 충분한 예비 처리량 용량을 확보하려면 평균 처리량 용량 사용률을 50% 미만으로 유지하는 것이 좋습니다.

성능 경고 및 권장 사항

FSx for Windows는 처리량 용량이 32MBps 이상으로 구성된 파일 시스템에 대한 성능 경고를 제공합니다. Amazon FSx는 이러한 지표 중 하나가 연속된 여러 데이터 포인트에 대해 미리 정해진 임계값에

도달하거나 초과할 때마다 지표 세트에 대한 경고를 표시합니다. CloudWatch 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 ALARM 상태인 파일 시스템에 대해 구성된 CloudWatch 모든 경보는 요약 섹션의 모니터링 및 성능 패널에 표시됩니다. 이 경고는 지표 그래프가 표시되는 대시보드 섹션에도 표시됩니다.

모든 Amazon FSx CloudWatch 지표에 대해 경보를 생성할 수 있습니다. 자세한 정보는 Amazon FSx를 모니터링하기 위한 CloudWatch 알람 생성을 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.

이 지표에 대한 경고가 있는 경우	조치
네트워크 처리량 - 사용률	처리량 용량 늘리기
파일 서버 > 디스크 IOPS – 사용률	
파일 서버 > 디스크 처리량 - 사용률	
파일 서버 > 디스크 IOPS – 버스트 밸런스	
파일 서버 > 디스크 처리량 – 버스트 밸런스	
스토리지 용량 사용률	스토리지 용량 늘리기
스토리지 볼륨 > 디스크 처리량 - 사용률(HDD)	스토리지 용량을 늘리거나 SDD 스토리지 유형으로 전환
스토리지 볼륨 > 디스크 처리량 - 버스트 밸런스(HDD)	
스토리지 볼륨 > 디스크 IOPS – 사용률 (SSD)	SSD IOPS 늘리기

> **Note**
>
> 특정 파일 시스템 이벤트는 디스크 I/O 성능 리소스를 사용하므로 잠재적으로 성능 경고를 트리거할 수 있습니다. 예:
>
> - 스토리지 용량 증가 및 파일 시스템 성능에 설명된 대로 스토리지 용량 확장의 최적화 단계에서 디스크 처리량이 증가할 수 있습니다.
> - 다중 AZ 파일 시스템의 경우 처리량 용량 확장, 하드웨어 교체 또는 가용 영역 중단과 같은 이벤트로 인해 자동 장애 조치 및 페일백 이벤트가 발생합니다. 이 기간 동안 발생하는 모든 데이터 변경 사항은 기본 및 보조 파일 서버 간에 동기화되어야 하며, Windows Server는 디스크 I/O 리소스를 소비할 수 있는 데이터 동기화 작업을 실행합니다. 자세한 정보는 처리량 용량 관리을 참조하세요.

파일 시스템 성능에 대한 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

FSx for Windows File Server 지표 액세스

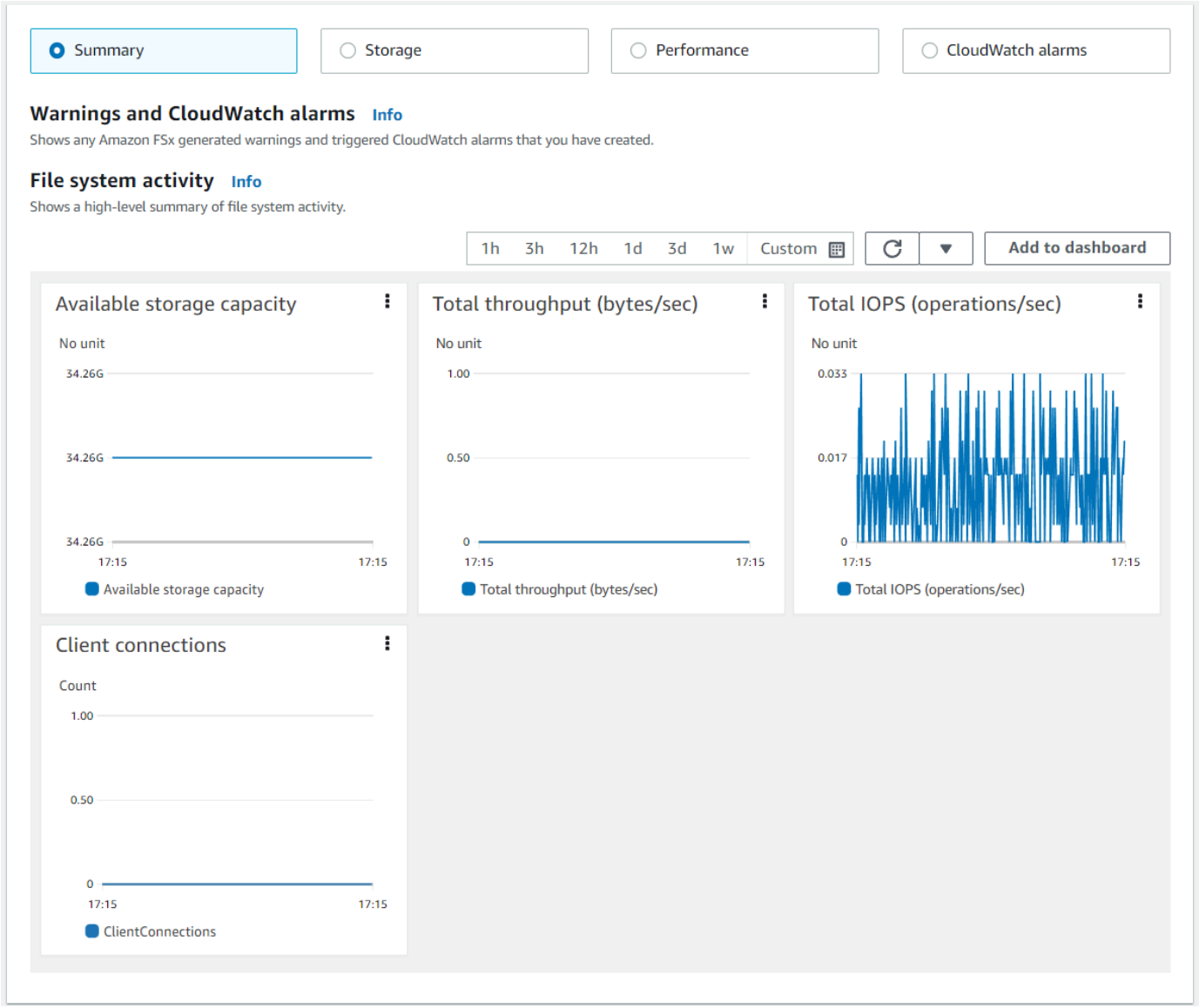
다음과 같은 방법으로 Amazon FSx 지표를 CloudWatch 볼 수 있습니다.

- Amazon FSx 콘솔.
- 콘솔 CloudWatch .
- CloudWatch CLI (명령줄 인터페이스)
- CloudWatch API.

다음의 절차는 다양한 도구를 사용하여 파일 시스템의 지표에 액세스하는 방법을 설명합니다.

Amazon FSx 콘솔을 사용하여 파일 시스템 지표 확인

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 파일 시스템 세부 정보 페이지를 표시하려면 탐색 창에서 파일 시스템을 선택합니다.
3. 표시할 지표가 있는 파일 시스템을 선택합니다.
4. 파일 시스템의 지표에 대한 그래프를 보려면 두 번째 패널에서 모니터링 및 성능을 선택합니다.

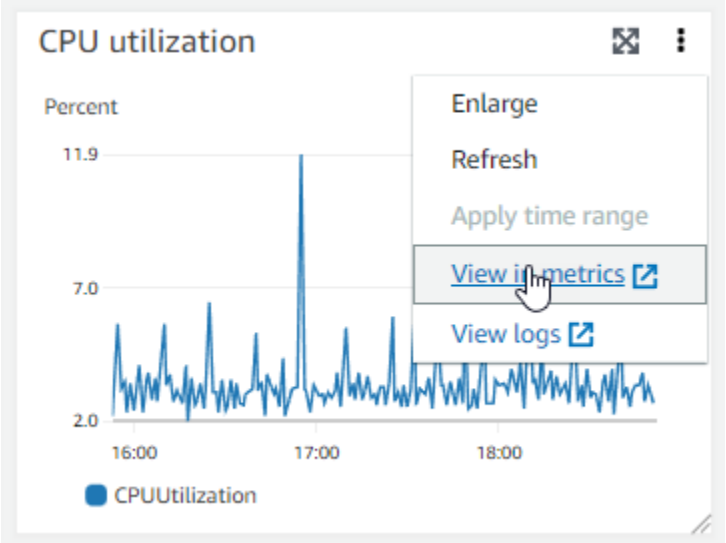


- 요약 지표는 기본적으로 표시되며, 파일 시스템 활동 지표와 함께 모든 활성 경고 및 CloudWatch 경보를 표시합니다.
- 스토리지를 선택하면 용량 및 사용률 지표가 표시됩니다.
- 성능을 선택하면 파일 서버 및 스토리지 성능 지표가 표시됩니다.
- 파일 시스템에 구성된 모든 경보의 그래프를 보려면 CloudWatch 경보를 선택합니다.

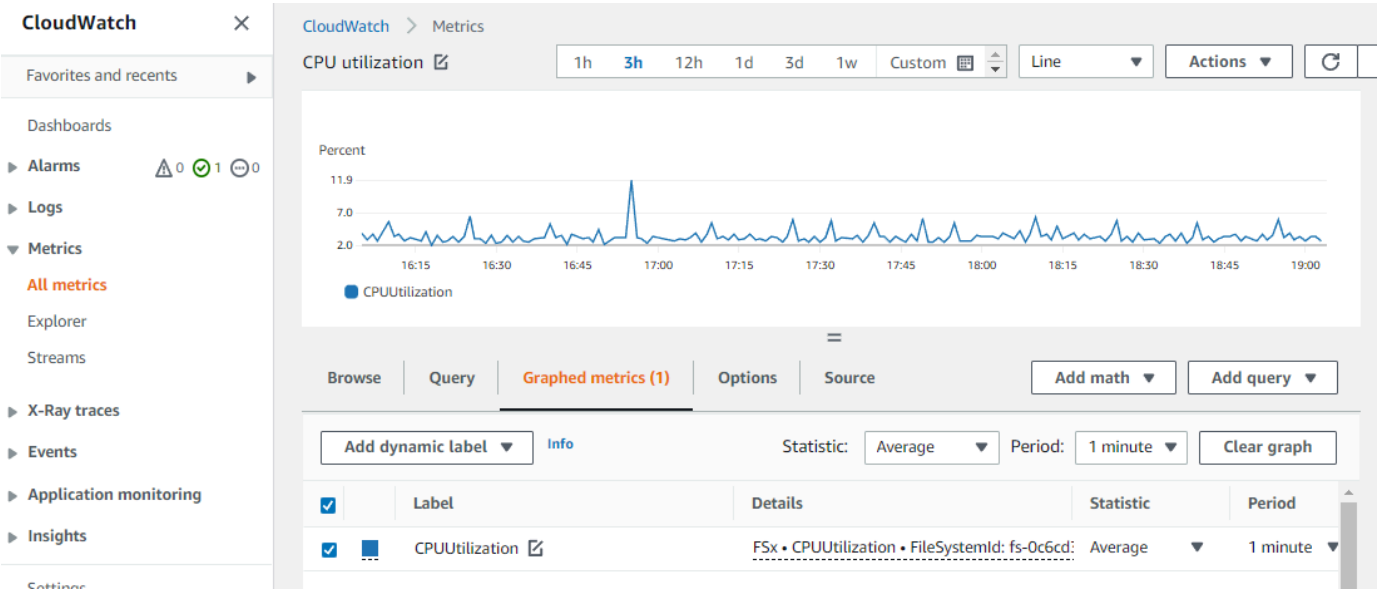
자세한 내용은 FSx for Windows File Server 지표를 사용하는 방법단원을 참조하세요.

콘솔에서 지표를 보려면 CloudWatch

1. Amazon 콘솔의 지표 페이지에서 파일 시스템 지표를 보려면 Amazon FSx CloudWatch 콘솔의 모니터링 및 성능 패널에 있는 지표로 이동하십시오.
2. 다음 이미지와 같이 지표 그래프의 오른쪽 상단에 있는 작업 메뉴에서 지표에서 보기를 선택합니다.



그러면 CloudWatch 콘솔에 지표 페이지가 열리고 다음 이미지와 같이 지표 그래프가 표시됩니다.



대시보드에 메트릭을 추가하려면 CloudWatch

1. 콘솔의 대시보드에 Windows용 FSx 파일 시스템 지표 세트를 추가하려면 Amazon FSx 콘솔의 모니터링 및 성능 패널에서 CloudWatch 지표 집합 (요약, 스토리지 또는 성능) 을 선택합니다.
2. 패널 오른쪽 상단에서 대시보드에 추가를 선택하면 콘솔이 열립니다. CloudWatch
3. 목록에서 기존 CloudWatch 대시보드를 선택하거나 새 대시보드를 생성합니다. 자세한 내용은 Amazon 사용 설명서의 Amazon CloudWatch 대시보드 사용을 참조하십시오. CloudWatch

에서 지표에 액세스하려면 AWS CLI

- `list-metrics` 명령과 `--namespace "AWS/FSx"` 네임스페이스를 사용합니다. 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

CloudWatch API 사용

CloudWatch API에서 지표에 액세스하려면

- `GetMetricStatistics`을 호출합니다. 자세한 내용은 Amazon CloudWatch API 레퍼런스를 참조하십시오.

Amazon FSx를 모니터링하기 위한 CloudWatch 알람 생성

CloudWatch 경보 상태가 변경될 때 Amazon SNS 메시지를 보내는 경보를 생성할 수 있습니다. 경보는 지정한 기간에 단일 지표를 감시하고 여러 기간에 지정된 임계값에 대한 지표 값을 기준으로 작업을 하나 이상 수행합니다. 이 작업은 Amazon SNS 주제 또는 Auto Scaling 정책으로 전송되는 알림입니다.

경보는 지속적인 상태 변경에 대한 조치만 호출합니다. CloudWatch 경보는 단순히 특정 상태에 있다는 이유만으로 작업을 호출하지 않습니다. 상태가 변경되고 지정된 기간 동안 유지되어야 합니다. Amazon FSx 콘솔 또는 콘솔에서 경보를 생성할 수 있습니다. CloudWatch

다음 절차에서는 콘솔, AWS CLI및 API를 사용하여 Amazon FSx 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. 작업 메뉴를 선택하고 세부 정보 보기를 선택합니다.

4. 요약 페이지에서 모니터링 및 성능을 선택합니다.
5. 알람을 선택합니다CloudWatch .
6. CloudWatch 알람 만들기를 선택합니다. 그러면 CloudWatch 콘솔로 리디렉션됩니다.
7. 지표 선택을 선택하고 다음을 선택합니다.
8. 지표 섹션에서 FSx를 선택합니다.
9. 파일 시스템 지표를 선택하고 경보를 설정하려는 지표를 선택한 다음, 지표 선택을 선택합니다.
10. 조건 섹션에서 경보에 적용할 조건을 선택한 후 다음을 선택합니다.

> **Note**
>
> 파일 시스템 유지 관리 중에는 단일 AZ 파일 시스템에 대한 지표가 게시되지 않고, 기본 파일 서버와 보조 파일 서버 간의 장애 조치 및 페일백 중에는 다중 AZ 파일 시스템에 대한 지표가 게시되지 않을 수 있습니다. 불필요하고 오해의 소지가 있는 경보 조건 변경을 방지하고 누락된 데이터 포인트에 대해 복원력을 갖도록 경보를 구성하려면 Amazon User Guide의 CloudWatch 경보가 누락된 데이터를 처리하는 방법 구성을 참조하십시오. CloudWatch

11. 경보 상태가 작업을 트리거할 때 이메일이나 SNS 알림을 CloudWatch 보내려면 이 경보 상태일 때마다 경보 상태를 선택하십시오.

    SNS 주제 선택에서 기존 SNS 주제를 선택합니다. 주제 생성을 선택한 경우 새 이메일 구독 목록에 대한 명칭 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. 지표에 대한 이름, 설명, 항상 값을 입력하고 다음을 선택합니다.
13. 미리 보기 및 생성 페이지에서 생성하려는 경보를 검토한 다음 경보 생성을 선택합니다.

콘솔을 사용하여 알람을 설정하려면 CloudWatch

1. https://console.aws.amazon.com/cloudwatch/ 에서 AWS Management Console 로그인하고 CloudWatch 콘솔을 엽니다.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. FSx 지표를 선택하고 Amazon FSx 지표를 스크롤하여 경보를 생성할 지표를 찾습니다. 이 대화 상자에서 Amazon FSx 지표만 표시하려면 파일 시스템의 파일 시스템 ID를 검색합니다. 경보를 생성할 지표를 선택하고 다음을 선택합니다.
4. 지표에 대한 Name, Description, Whenever 값을 입력합니다.
5. 경보 상태에 도달했을 때 이메일을 CloudWatch 보내려면 이 경보가 발생할 때마다 [State is ALARM] 을 선택합니다. 다음 주소로 알림 전송에서 기존 SNS 주제를 선택합니다. 주제 생성을 선택한 경우 새 이메일 구독 목록에 대한 명칭 및 이메일 주소를 설정할 수 있습니다. 이 목록은 향후 경보를 위해 필드에 저장되고 표시됩니다.

   > **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.

6. 이제 경보 미리 보기 영역에서 생성할 경보를 미리 볼 수 있습니다. 경보 생성을 선택합니다.

를 사용하여 알람을 설정하려면 AWS CLI

- `put-metric-alarm`을 호출합니다. 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

CloudWatch API를 사용하여 알람을 설정하려면

- `PutMetricAlarm`을 호출합니다. 자세한 내용은 Amazon CloudWatch API 레퍼런스를 참조하십시오.

AWS CloudTrail을 사용하여 Amazon FSx for Windows File Server API 호출 로깅

Amazon FSx for Windows File Server는 Amazon FSx에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 레코드를 제공하는 서비스인 AWS CloudTrail과 통합됩니다. CloudTrail은 Amazon FSx

에 대한 모든 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. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Amazon FSx에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Amazon FSx 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Amazon FSx에서 활동이 수행되면 해당 활동은 이벤트 기록에서 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 CloudTrail 이벤트 기록을 사용하여 이벤트 보기를 참조하세요.

Amazon FSx의 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에 대한 Amazon SNS 알림 구성
- 여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기

모든 Amazon FSx 작업은 CloudTrail에서 로깅되며 Amazon FSx API 참조에 설명되어 있습니다. 예를 들어 `CreateFileSystem`, `CreateBackup`, `TagResource` 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 보안 인증 정보로 했는지
- 역할 또는 페더레이션 사용자에 대한 임시 보안 인증 정보를 사용하여 요청이 생성되었는지 여부.

- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 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 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 콘솔에서 파일 시스템의 태그를 만든 경우 `TagResource` 작업의 실행과 관련된 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 예제는 콘솔에서 파일 시스템의 태그를 삭제한 경우 UntagResource 작업의 실행과 관련된 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 Windows File Server 성능

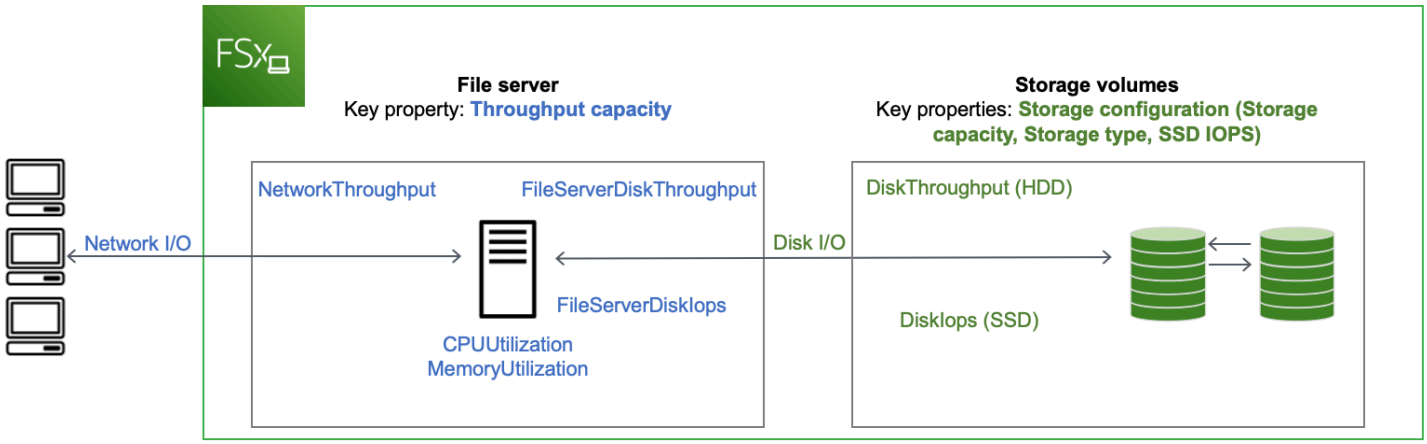
FSx for Windows File Server는 다양한 성능 요구 사항을 충족하는 파일 시스템 구성 옵션을 제공합니다. 다음은 사용 가능한 성능 구성 옵션과 유용한 성능 팁에 대한 설명과 함께 Amazon FSx 파일 시스템 성능에 대해 소개합니다.

주제

파일 시스템 성능

각 FSx for Windows File Server 파일 시스템은 클라이언트가 통신하는 Windows 파일 서버와 파일 서버에 연결된 스토리지 볼륨 또는 디스크 세트로 구성됩니다. 각 파일 서버는 고속 인 메모리 캐시를 사용하여 가장 자주 액세스하는 데이터의 성능을 향상시킵니다.

다음 다이어그램은 FSx for Windows File Server 파일 시스템에서 데이터에 액세스하는 방법을 보여줍니다.



클라이언트가 인 메모리 캐시에 저장된 데이터에 액세스하면 해당 데이터는 요청한 클라이언트에 네트워크 I/O로 직접 제공됩니다. 파일 서버는 디스크에서 데이터를 읽거나 디스크에 쓸 필요가 없습니다. 이 데이터 액세스의 성능은 네트워크 I/O 제한과 메모리 내 캐시의 크기에 따라 결정됩니다.

클라이언트가 캐시에 없는 데이터에 액세스하면 파일 서버는 이 데이터를 디스크 I/O로 디스크에서 읽거나 디스크에 씁니다. 그런 다음 데이터는 파일 서버에서 클라이언트에 네트워크 I/O로 제공됩니다. 이 데이터 액세스 성능은 네트워크 I/O 제한과 디스크 I/O 제한에 따라 결정됩니다.

네트워크 I/O 성능과 파일 서버 인 메모리 캐시는 파일 시스템의 처리량 용량에 따라 결정됩니다. 디스크 I/O 성능은 처리량 용량과 스토리지 구성의 조합에 따라 결정됩니다. 처리량과 IOPS 수준으로 구성되는 파일 시스템이 달성할 수 있는 최대 디스크 I/O 성능은 다음의 경우 중 더 낮은 것입니다.

- 파일 시스템에서 선택한 처리량 용량을 기준으로 파일 서버에서 제공하는 디스크 I/O 성능 수준
- 스토리지 구성에서 제공하는 디스크 I/O 성능 수준 (파일 시스템에 대해 선택한 스토리지 용량, 스토리지 유형, SSD IOPS 수준).

추가 성능 고려 사항

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

지연 시간

FSx for Windows File Server 파일 서버는 활발하게 액세스하는 데이터에 대한 지연 시간이 일관되게 1밀리초 미만으로 유지되도록 고속 인 메모리 캐시를 사용합니다. 인 메모리 캐시에 없는 데이터, 즉 기본 스토리지 볼륨에서 I/O를 수행하여 처리해야 하는 파일 작업의 경우 Amazon FSx는 솔리드 스테이트 드라이브(SSD) 스토리지의 경우 1밀리초 미만의 파일 작업 지연 시간을 제공하고 하드 디스크 드라이브(HDD) 스토리지의 경우 수 밀리초의 지연 시간을 제공합니다.

처리량 및 IOPS

Amazon FSx 파일 시스템은 AWS 리전 Amazon FSx를 사용할 수 있는 모든 지역에서 최대 2Gb/s 및 80,000 IOPS를 제공하며, 미국 동부 (버지니아 북부), 미국 서부 (오레곤), 미국 동부 (오하이오), 유럽 (아일랜드), 아시아 태평양 (도쿄) 및 아시아 태평양 (싱가포르) 에서 12GB/s의 처리량과 400,000 IOPS를 제공합니다. 워크로드가 파일 시스템에서 구동할 수 있는 구체적인 처리량 및 IOPS의 양은 파일 시스템의 처리량 용량, 스토리지 용량 및 스토리지 유형과 활성 작업 세트의 크기를 비롯한 워크로드의 특성에 따라 달라집니다.

단일 클라이언트 성능

Amazon FSx를 사용하면 파일 시스템에 액세스하는 단일 클라이언트에서 파일 시스템의 전체 처리량과 IOPS 수준을 얻을 수 있습니다. Amazon FSx는 SMB 멀티채널을 지원합니다. 이 기능을 사용하면 파일 시스템에 액세스하는 단일 클라이언트에 대해 최대 몇 GB/s의 처리량과 수십만 IOPS를 제공할 수 있습니다. SMB Multichannel은 클라이언트와 서버 간의 여러 네트워크 연결을 동시에 사용하여 네트워크 대역폭을 집계하여 사용률을 극대화합니다. Windows에서 지원하는 SMB 연결 수에는 이론적인 제한이 있지만 이 제한은 수백만 개에 달하며 사실상 SMB 연결 수에는 제한이 없습니다.

버스트 성능

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 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.

처리량 용량이 성능에 미치는 영향

처리량 용량은 다음 범주의 파일 시스템 성능을 결정합니다.

- 네트워크 I/O - 파일 서버가 파일 서버에 액세스하는 클라이언트에 파일 데이터를 제공할 수 있는 속도입니다.
- 파일 서버 CPU 및 메모리 - 파일 데이터를 제공하고 데이터 중복 제거 및 섀도우 복사본과 같은 백그라운드 작업을 수행하는 데 사용할 수 있는 리소스입니다.
- 디스크 I/O - 파일 서버가 파일 서버와 스토리지 볼륨 간의 I/O를 지원할 수 있는 속도입니다.

다음 표에는 각 프로비저닝된 처리량 용량 구성으로 구동할 수 있는 최대 네트워크 I/O 수준(처리량 및 IOPS) 및 디스크 I/O(처리량 및 IOPS)와, 데이터 중복 제거 및 섀도우 복사본과 같은 백그라운드 활동 캐싱 및 지원에 사용할 수 있는 메모리 양에 대한 세부 정보가 표시되어 있습니다. Amazon FSx API 또는 CLI를 사용할 때 초당 32메가바이트 (MBps) 미만의 처리 용량 수준을 선택할 수 있지만, 이러한 수준은 프로덕션 워크로드가 아닌 테스트 및 개발 워크로드를 위한 것임을 명심하십시오.

> **Note**
>
> 4,608MBps 이상의 처리량 용량 수준은 미국 동부(버지니아 북부), 미국 서부(오레곤), 미국 동부(오하이오), 유럽(아일랜드), 아시아 태평양(도쿄) 및 아시아 태평양(싱가포르) 리전에서만 지원됩니다.

네트워크 I/O 및 메모리

FSx 처리 용량 (초당 메가바이트)	네트워크 처리량 (초당 메가바이트)		네트워크 IOPS	메모리(GB)
	기준	버스트(하루에 몇 분간)		
32	32	600	수천	4
64	64	600	수만	8
128	150	1,250		8
256	300	1,250	수십만	16
512	600	1,250		32
1,024	1,500	–		72
2,048	3,125	–		144
4,608	9,375	–	수백만	192
6,144	12,500	–		256
9,216	18,750	–		384
12,288	21,250	–		512

디스크 I/O

FSx 처리 용량 (초당 메가바이트)	디스크 처리량 (초당 메가바이트)		디스크 IOPS	
	기준	버스트(하루 30분 간)	기준	버스트(하루 30분 간)
32	32	260	2K	12K
64	64	350	4K	16K
128	128	600	6K	20K
256	256	600	1만	20K
512	512	–	20K	–
1,024	1,024	–	40K	–
2,048	2,048	–	80K	–
4,608	4,608	–	15만	–
6,144	6,144	–	20만	–
9,216	9,216 [1]	–	300K [1]	–
12,288	12,288 [1]	–	400K [1]	–

> **Note**
>
> [1] 처리 용량이 9,216 또는 12,288MBps인 다중 AZ 파일 시스템을 사용하는 경우 성능은 쓰기 트래픽의 경우에만 9,000MBps 및 262,500 IOPS로 제한됩니다. 그렇지 않으면 모든 다중 AZ 파일 시스템의 읽기 트래픽, 모든 단일 AZ 파일 시스템의 읽기 및 쓰기 트래픽, 기타 모든 처리량 용량 수준의 경우 파일 시스템이 표에 나와 있는 성능 한도까지 지원합니다.

적절한 수준의 처리량 용량 선택

Amazon Web Services 관리 콘솔을 사용하여 파일 시스템을 생성하면 Amazon FSx는 구성한 스토리지 용량에 따라 파일 시스템의 권장 처리량 용량 수준을 자동으로 선택합니다. 권장 처리량 용량은 대부분의 워크로드에 충분해야 하지만 권장 사항을 재정의하고 애플리케이션 요구 사항에 맞게 특정 처리량 용량을 선택할 수 있습니다. 예를 들어 파일 시스템으로 1GBps의 트래픽을 전송해야 하는 워크로드의 경우 최소 1,024MBps의 처리량 용량을 선택해야 합니다.

또한 구성할 처리량 수준을 결정할 때는 파일 시스템에서 활성화하려는 기능을 고려해야 합니다. 예를 들어 섀도우 복사본을 사용 설정하면 파일 서버가 사용 가능한 I/O 성능 용량으로 섀도우 복사본을 유지할 수 있도록 처리량 용량을 예상 워크로드의 최대 3배까지 늘려야 할 수 있습니다. 데이터 중복 제거를 사용 설정하는 경우 파일 시스템의 처리량 용량과 관련된 메모리 양을 결정하고 이 메모리 양이 데이터 크기에 충분하도록 해야 합니다.

생성 후 언제든지 처리량 용량을 늘리거나 줄일 수 있습니다. 자세한 내용은 처리량 용량 관리 섹션을 참조하세요.

Amazon FSx 콘솔의 모니터링 및 성능 > 성능 탭을 보면 파일 서버 성능 리소스의 워크로드 사용률을 모니터링하고 선택할 처리량 용량에 대한 권장 사항을 얻을 수 있습니다. 사전 프로덕션 환경에서 테스트하여 선택한 구성이 워크로드의 성능 요구 사항을 충족하는지 확인하는 것이 좋습니다. 다중 AZ 파일 시스템의 경우 파일 시스템 유지 관리, 처리량 용량 변경 및 예상치 못한 서비스 중단 중에 발생하는 장애 조치 프로세스가 워크로드에 미치는 영향을 테스트하고, 이러한 이벤트가 발생하는 동안 성능에 영향을 미치지 않도록 충분한 처리량 용량을 프로비저닝했는지 확인하는 것이 좋습니다. 자세한 내용은 FSx for Windows File Server 지표 액세스 섹션을 참조하세요.

스토리지 구성이 성능에 미치는 영향

파일 시스템의 스토리지 용량, 스토리지 유형 및 SSD IOPS 수준은 모두 파일 시스템의 디스크 I/O 성능에 영향을 미칩니다. 워크로드에 원하는 성능 수준을 제공하도록 이러한 리소스를 구성할 수 있습니다.

언제든지 스토리지 용량을 늘리고 SSD IOPS를 확장할 수 있습니다. 자세한 내용은 스토리지 용량 관리 및 SSD IOPS 관리 섹션을 참조하세요. 파일 시스템을 HDD 스토리지 유형에서 SSD 스토리지 유형으로 업그레이드할 수도 있습니다. 자세한 내용은 스토리지 유형 관리 섹션을 참조하세요.

파일 시스템은 다음과 같은 기본 수준의 디스크 처리량과 IOPS를 제공합니다.

스토리지 유형	디스크 처리량 (스토리지 TiB당 MBps)	디스크 IOPS(스토리지 TiB당 IOPS)
SSD	750	3,000*
HDD	기준 12, 버스트 80(파일 시스템당 최대 1Gb/s)	기준 12, 버스트 80

> **Note**
>
> *SSD 스토리지 유형의 파일 시스템의 경우 스토리지의 GiB당 최대 500 IOPS, 파일 시스템당 400,000 IOPS의 최대 비율까지 추가 IOPS를 프로비저닝할 수 있습니다.

HDD 버스트 성능

HDD 스토리지 볼륨의 경우 Amazon FSx는 성능 측정에 버스트 버킷 모델을 사용합니다. 볼륨 크기에 따라 볼륨의 기준 처리량, 즉 볼륨이 처리량 크레딧을 누적하는 속도가 결정됩니다. 볼륨 크기는 볼륨의 버스트 처리량, 즉 사용 가능한 크레딧을 소비할 수 있는 속도도 결정합니다. 볼륨이 클수록 기본 및 버스트 처리량이 높습니다. 볼륨에 크레딧이 많을수록 버스트 수준에서 더 오랫동안 I/O를 구동할 수 있습니다.

HDD 스토리지 볼륨의 사용 가능 처리량은 다음 수식으로 표현됩니다.

```
(Volume size) × (Credit accumulation rate per TiB) = Throughput
```

1TiB HDD 볼륨의 경우 버스트 처리량은 80MiB/s로 제한되고, 버킷의 크레딧은 12MiB/s 속도로 채워지며, 최대 1TiB에 해당하는 크레딧을 보유할 수 있습니다.

예: 스토리지 용량 및 처리량 용량

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

2TiB의 HDD 스토리지 용량과 32MBps의 처리량 용량으로 구성된 파일 시스템의 처리량 수준은 다음과 같습니다.

- 네트워크 처리량 – 기준 32MBps 및 버스트 600MBps(처리량 용량 표 참조)

- 디스크 처리량 – 기준 24MBps 및 버스트 160MBps로, 다음 중 더 낮은 수치입니다.
  - 파일 시스템의 처리량 용량을 기준으로 파일 서버가 지원하는 기준 32MBps 및 버스트 260MBps의 디스크 처리량 수준
  - 스토리지 유형 및 용량에 따라 스토리지 볼륨이 지원하는 기준 24MBps(TB당 12MBps* 2TiB) 및 버스트 160MBps(TiB당 80MBps * 2TiB)의 디스크 처리량 수준

따라서 파일 시스템에 액세스하는 워크로드는 파일 서버 인 메모리 캐시에 캐싱된 활성 액세스 데이터에 수행되는 파일 작업에 대해 기준 처리량을 최대 32MBps까지, 버스트 처리량을 최대 600MBps까지 높일 수 있습니다. 그리고 예를 들어 캐시 누락으로 인해 디스크까지 이동해야 하는 파일 작업의 경우 최대 기준 24MBps 및 버스트 160MBps의 처리량을 제공합니다.

메트릭을 CloudWatch 사용한 성능 측정

CloudWatch Amazon을 사용하여 파일 시스템의 처리량과 IOPS를 측정하고 모니터링할 수 있습니다. 자세한 정보는 Amazon을 통한 지표 모니터링 CloudWatch을 참조하세요.

성능 문제 해결

일반적인 성능 문제를 해결하는 데 도움이 필요하면 파일 시스템 성능 문제 해결 섹션을 참조하세요.

Amazon FSx 연습

다양한 프로세스를 안내하는 여러가지 작업 중심 연습이 다음에 나와 있습니다.

주제

연습 1: 시작을 위한 사전 조건

연습을 시작하기 전에 Microsoft Windows 기반 Amazon EC2 인스턴스가 AWS Directory Service 디렉터리에 연결되어 있어야 합니다. 또한 Windows 원격 데스크톱 프로토콜을 통해 디렉터리의 관리자 사용자로 인스턴스에 로그인해야 합니다. 다음 연습에서 필수 사전 작업의 수행 방법을 소개합니다.

주제

1단계: Active Directory 설정

Amazon FSx를 사용하면 Windows 기반 워크로드용 완전 관리형 파일 스토리지를 운영할 수 있습니다. 마찬가지로 AWS Directory Service는 워크로드 배포에 사용할 완전 관리형 디렉터리를 제공합니다. EC2 인스턴스를 사용하는 가상 사설 클라우드(VPC)의 AWS에서 기존 기업 AD 도메인을 실행하는 경우 사용자 기반 인증 및 액세스 제어를 활성화할 수 있습니다. 이를 위해 AWS 관리형 Microsoft AD와 회사 도메인 간에 신뢰 관계를 설정해야 합니다. Amazon FSx에서 Windows 인증은 AWS 관리형 포리스트가 기업 도메인 포리스트를 신뢰하는 단방향 포리스트 트러스트만 필요합니다.

기업 도메인은 신뢰할 수 있는 도메인의 역할을 하고, AWS Directory Service 관리형 도메인은 신뢰하는 도메인의 역할을 합니다. 검증된 인증 요청은 도메인 간에 한 방향으로만 전달되며 회사 도메인의 계정이 관리형 도메인에서 공유되는 리소스에 대해 인증합니다. 이 경우 Amazon FSx는 관리형 도메인과만 상호 작용합니다. 그러면 관리형 도메인은 인증 요청을 기업 도메인으로 전달합니다.

> **Note**
>
> 또한 Amazon FSx에서 신뢰할 수 있는 도메인에 대한 외부 신뢰 유형을 사용할 수 있습니다.

Active Directory 보안 그룹은 Amazon FSx 파일 시스템의 보안 그룹으로부터의 인바운드 액세스를 활성화해야 합니다.

Microsoft AD용 AWS 디렉터리 서비스 생성

- AWS 관리형 Microsoft AD 디렉터리가 아직 없는 경우 AWS Directory Service를 사용하여 생성합니다. 자세한 내용은 AWS Directory Service 관리 안내서의 AWS 관리형 Microsoft AD 디렉터리 생성을 참조하세요.

  > **Important**
  >
  > 관리자 사용자에게 할당한 암호를 기억하세요. 이후 시작 연습에서 필요합니다. 암호를 잊은 경우, 새로운 AWS Directory Service 디렉터리 및 관리자 사용자를 사용하여 연습의 단계를 반복해야 합니다.

- 기존 AD가 있는 경우, AWS 관리형 Microsoft AD와 기존 AD 간에 신뢰 관계를 생성하세요. 자세한 내용은 AWS Directory Service 관리 안내서의 신뢰 관계를 생성해야 하는 경우를 참조하세요.

2단계: Amazon EC2 콘솔에서 Windows 인스턴스 시작

다음 절차의 설명에 따라 AWS Management Console을 사용하여 Windows 인스턴스를 시작할 수 있습니다. 첫 번째 인스턴스를 빠르게 시작하도록 돕기 위한 것이므로 가능한 모든 옵션을 다루지는 않습니다. 고급 옵션에 대한 자세한 내용은 인스턴스 시작 섹션을 참조하세요.

인스턴스 시작

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 콘솔 대시보드에서 인스턴스 시작을 선택합니다.

3. Amazon Machine Image(AMI) 선택 페이지에 인스턴스에 대한 템플릿 역할을 하는 Amazon Machine Image(AMI)라는 기본 구성 목록이 표시됩니다. Windows Server 2016 Base 또는 Windows Server 2012 R2 Base용 AMI를 선택합니다. 해당되는 AMI는 "프리 티어 사용 가능"으로 표시됩니다.
4. 인스턴스 유형 선택 페이지에서 인스턴스의 하드웨어 구성을 선택할 수 있습니다. 기본으로 선택된 `t2.micro` 유형을 선택합니다. 프리 티어에 적격인 인스턴스 유형입니다.
5. 검토 후 시작을 선택하여 마법사가 다른 구성 설정을 완료하게 합니다.
6. 검토 후 시작 페이지의 보안 그룹에서 마법사가 보안 그룹을 만들고 선택했음을 확인합니다. 이 보안 그룹을 사용하거나, 다음 단계를 이용하여 설정을 시작할 때 만든 보안 그룹을 선택합니다.

   a. 보안 그룹 편집을 선택합니다.

   b. 보안 그룹 구성 페이지에서 기존 보안 그룹 선택이 선택되어 있는지 확인합니다.

   c. 기존 보안 그룹 목록에서 보안 그룹을 선택한 다음 검토 후 시작을 선택합니다.
7. 인스턴스 시작 검토 페이지에서 시작을 선택합니다.
8. 키 페어에 대한 메시지가 나타나면 기존 키 페어 선택을 선택한 다음 설치할 때 생성한 키 페어를 선택합니다.

   또는 키 페어를 새로 만들 수 있습니다. 새 키 페어 생성을 선택하고 키 페어 이름을 입력한 다음 키 페어 다운로드를 선택합니다. 이때가 사용자가 프라이빗 키 파일을 저장할 수 있는 유일한 기회이므로 반드시 다운로드하세요. 프라이빗 키 파일을 안전한 장소에 저장합니다. 인스턴스를 시작할 때 키 페어의 이름을 제공하고, 인스턴스에 연결할 때마다 해당 프라이빗 키를 제공해야 합니다.

   > **Warning**
   >
   > 키 페어 없이 계속 옵션을 선택하지 마세요. 키 페어 없이 인스턴스를 시작하면 인스턴스에 연결할 수 없습니다.

   준비되면 승인 확인란을 선택한 다음 인스턴스 시작을 선택합니다.
9. 확인 페이지에서 인스턴스가 실행 중인지 확인할 수 있습니다. 인스턴스 보기를 선택하여 확인 페이지를 닫고 콘솔로 돌아갑니다.
10. 인스턴스 화면에서 시작 상태를 볼 수 있습니다. 인스턴스를 시작하는 데 약간 시간이 걸립니다. 인스턴스를 시작할 때 초기 상태는 `pending`입니다. 인스턴스가 시작된 후에는 상태가 `running`으로 바뀌고 퍼블릭 DNS 이름을 받습니다. (퍼블릭 DNS(IPv4) 열이 숨겨져 있는 경우 페이지 오른쪽 상단 모서리에 있는 열 표시/숨기기(기어 모양 아이콘)를 선택한 다음 퍼블릭 DNS(IPv4)를 선택합니다.)

11. 연결할 수 있도록 인스턴스가 준비될 때까지 몇 분 정도 걸릴 수 있습니다. 인스턴스가 상태 확인을 통과했는지 확인하세요. 상태 검사 열에서 이 정보를 볼 수 있습니다.

> **Important**
>
> 인스턴스를 시작할 때 생성된 보안 그룹의 ID를 기록해 두세요. Amazon FSx 파일 시스템을 생성할 때 필요합니다.

이제 인스턴스가 시작되면 인스턴스에 연결할 수 있습니다.

3단계: 인스턴스에 연결

Windows 인스턴스에 연결하려면 최초 관리자 암호를 검색한 다음 원격 데스크톱을 사용하여 인스턴스에 연결할 때 이 암호를 지정해야 합니다.

관리자 계정의 이름은 운영 체제의 언어에 따라 다릅니다. 예를 들어 영어는 Administrator, 프랑스어는 Administrateur, 포르투갈어는 Administrador입니다. 자세한 내용은 Microsoft TechNet Wiki의 Localized Names for Administrator Account in Windows를 참조하세요.

인스턴스를 도메인에 조인한 경우 AWS Directory Service에서 정의한 도메인 자격 증명을 사용하여 인스턴스에 연결할 수 있습니다. 원격 데스크톱 로그인 화면에서는 로컬 컴퓨터 이름과 생성된 비밀번호를 사용하지 마세요. 대신 관리자의 정식 사용자 이름과 계정의 암호를 사용하세요. 예를 들면, **`corp.example.com\Admin`**입니다.

Windows Server 운영 체제(OS) 라이선스는 관리 목적으로 두 개의 동시 원격 연결을 허용합니다. Windows 인스턴스 가격에는 Windows Server 라이선스가 포함됩니다. 2개를 초과하는 동시 원격 연결이 필요할 경우, 원격 데스크톱 서비스(RDS) 라이선스를 구매해야 합니다. 제3의 연결을 시도하면 오류가 발생합니다. 자세한 내용은 동시 원격 연결 허용 수 섹션을 참조하세요.

RDP 클라이언트로 Windows 인스턴스 연결

1. Amazon EC2 콘솔에서 인스턴스를 선택한 다음 연결을 선택합니다.
2. 인스턴스에 연결 대화 상자에서 암호 가져오기를 선택합니다(인스턴스가 시작된 후 몇 분 정도 지나야 암호를 사용할 수 있음).
3. 찾아보기를 선택하고 인스턴스를 시작할 때 생성한 프라이빗 키 파일을 탐색합니다. 파일을 선택하고 열기를 클릭하여 파일의 전체 내용을 콘텐츠 필드로 복사합니다.

4. 암호 해독을 선택합니다. 콘솔에서는 인스턴스 연결 대화 상자에 해당 인스턴스에 대한 기본 관리자 암호가 표시되어 이전에 표시된 암호 가져오기에 대한 링크가 실제 암호로 바뀝니다.
5. 기본 관리자 암호를 기록하거나 클립보드로 복사합니다. 이 암호는 인스턴스에 연결하는 데 필요합니다.
6. 원격 데스크톱 파일 다운로드를 선택합니다. 브라우저에서 .rdp 파일을 열거나 저장하라는 메시지가 표시됩니다. 어떤 옵션이든 좋습니다. 마쳤으면 닫기를 선택하여 인스턴스 연결 대화 상자를 닫습니다.

   - .rdp 파일을 연 경우에는 원격 데스크톱 연결 대화 상자가 나타납니다.
   - .rdp 파일을 저장한 경우에는, 다운로드 디렉터리로 이동해 .rdp 파일을 열면 대화 상자가 표시됩니다.
7. 원격 연결 게시자를 알 수 없다는 경고를 받을 수도 있습니다. 계속해서 인스턴스에 연결할 수 있습니다.
8. 관련 메시지가 표시되면 운영 체제 관리자 계정과 이전에 기록하거나 복사한 암호를 사용하여 인스턴스에 로그인합니다. 원격 데스크톱 연결에 관리자 계정이 이미 설정되어 있는 경우에는 다른 계정 사용 옵션을 선택해 사용자 이름과 암호를 수동으로 입력해야 할 수도 있습니다.

   > **Note**
   >
   > 때로는 콘텐츠를 복사하고 붙여 넣으면 데이터가 손상될 수 있습니다. 로그인할 때 "Password Failed" 오류가 발생하면 암호를 수동으로 입력해 보세요.
9. 자체 서명된 인증서의 특성으로 인해, 보안 인증서를 인증할 수 없다는 경고 메시지가 나타날 수도 있습니다. 다음 단계에 따라 원격 컴퓨터의 자격 증명을 확인하거나, 인증서를 신뢰할 경우에는 단순히 예 또는 계속을 선택하여 계속 진행합니다.

   a. Windows PC에서 [Remote Desktop Connection]을 사용 중이라면 [View certificate]을 선택합니다. Mac에서 [Microsoft Remote Desktop]을 사용 중이라면 [Show Certificate]을 선택합니다.

   b. 세부 정보 탭을 선택하고 Windows PC에서는 지문 항목, Mac에서는 SHA1 지문 항목이 나타날 때까지 아래로 스크롤합니다. 이것은 원격 컴퓨터의 보안 인증서에 대한 고유한 식별자입니다.

   c. Amazon EC2 콘솔에서 인스턴스를 선택하고 [작업(Actions)]을 선택한 다음 [시스템 로그 가져오기(Get System Log)]를 선택합니다.

   d. 시스템 로그 출력에서 `RDPCERTIFICATE-THUMBPRINT`라는 항목을 확인합니다. 이 값이 인증서의 지문과 일치한다면 원격 컴퓨터의 자격 증명을 확인한 것입니다.

e. Windows PC에서 Remote Desktop Connection을 사용 중이라면 [Certificate] 대화 상자로 돌아가서 [OK]를 선택합니다. Mac에서 [Microsoft Remote Desktop]을 사용 중이라면 [Verify Certificate]으로 돌아가서 [Continue]를 선택합니다.

f. [Windows] 원격 데스크톱 연결 창에서 예를 선택하여 인스턴스에 연결합니다.

이제 인스턴스에 연결했으므로 인스턴스를 AWS Directory Service 디렉터리에 조인할 수 있습니다.

4단계: 인스턴스를 AWS Directory Service 디렉터리에 조인

다음 절차에서는 기존 Amazon EC2 Windows 인스턴스를 AWS Directory Service 디렉터리에 수동으로 조인하는 방법을 보여줍니다.

AWS Directory Service 디렉터리에 Windows 인스턴스 조인

1. 원격 데스크톱 프로토콜 클라이언트를 사용해 인스턴스를 연결합니다.
2. 인스턴스에서 TCP/IPv4 속성 대화 상자를 엽니다.

   a. 네트워크 연결 대화 상자를 엽니다.

   > **Tip**
   >
   > 인스턴스의 명령 프롬프트에서 다음을 실행하여 네트워크 연결 대화 상자를 직접 열 수 있습니다.
   >
   > ```
   > %SystemRoot%\system32\control.exe ncpa.cpl
   > ```

   b. 활성화된 네트워크 연결에 대한 컨텍스트 메뉴를 열고(마우스 오른쪽 버튼 클릭) 속성을 선택합니다.

   c. 연결 속성 대화 상자에서 인터넷 프로토콜 버전 4를 엽니다(더블 클릭).
3. 다음 DNS 서버 주소 사용을 선택하고 선호 DNS 서버 및 대체 DNS 서버 주소를 AWS Directory Service에서 제공하는 DNS 서버의 IP 주소로 변경하고 확인을 선택하십시오.
4. 인스턴스에 대한 시스템 속성 대화 상자를 열고 컴퓨터 이름 탭을 선택한 다음, 변경을 선택합니다.

> **Tip**
>
> 인스턴스의 명령 프롬프트에서 다음을 실행하여 시스템 속성 대화 상자를 직접 열 수 있습니다.
>
> ```
> %SystemRoot%\system32\control.exe sysdm.cpl
> ```

5. 멤버 필드에서 도메인을 선택하고 AWS Directory Service 디렉터리의 정규화된 이름을 입력한 후 확인을 선택합니다.
6. 도메인 관리자의 이름과 암호를 묻는 메시지가 표시되면 관리자 계정의 사용자 이름과 암호를 입력합니다.

> **Note**
>
> 도메인의 정규화된 이름이나 NetBios 이름을 입력하고 백슬래시(\)를 붙이고 사용자 이름, 이 경우는 관리자를 추가할 수 있습니다. 예를 들어, corp.example.com\admin 또는 corp \admin입니다.

7. 도메인에 온 것을 환영하는 메시지를 받은 후에 인스턴스를 재시작해야 변경 사항이 적용됩니다.
8. RDP를 통해 인스턴스에 다시 연결하고 AWS Directory Service 디렉터리의 관리자 사용자의 사용자 이름과 암호를 사용하여 인스턴스에 로그인합니다.

이제 인스턴스가 도메인에 가입되었으므로 Amazon FSx 파일 시스템을 생성할 준비가 되었습니다. 시작 연습의 다른 작업을 계속 완료할 수 있습니다. 자세한 내용은 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.

연습 2: 백업에서 파일 시스템 생성

Amazon FSx를 사용하면 백업에서 파일 시스템을 생성할 수 있습니다. 이때 새로 생성한 파일 시스템의 사용 사례에 더 적합하도록 다음 요소를 변경할 수 있습니다.

- 스토리지 유형
- 처리량 용량
- VPC
- 가용 영역

- 서브넷
- VPC 보안 그룹
- Active Directory 구성
- AWS KMS 암호화 키
- 일일 자동 백업 시작 시간
- 주간 유지 관리 기간

다음 절차는 백업에서 새 파일 시스템을 생성하는 과정을 안내합니다. 파일 시스템을 만들려면 먼저 기존 백업이 있어야 합니다. 자세한 정보는 백업 작업 섹션을 참조하세요.

기존 백업에서 파일 시스템 생성

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 여세요.
2. 오른쪽 탐색 목록에서 백업을 선택합니다.
3. 대시보드의 테이블에서 새 파일 시스템 생성에 사용할 백업을 선택합니다.

   > **Note**
   >
   > 백업은 원본과 스토리지 용량이 같은 파일 시스템에만 복원할 수 있습니다. 복원된 파일 시스템이 사용할 수 있는 상태가 되면 파일 시스템의 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리 섹션을 참조하세요.

4. 백업 복원을 선택합니다. 그러면 파일 시스템 생성 마법사가 시작됩니다.
5. 새 파일 시스템에서 변경하려는 설정을 선택합니다. 스토리지 유형은 기본적으로 SSD로 설정되지만, 다음 조건에서는 HDD로 변경할 수 있습니다.
   - 파일 시스템 배포 유형은 다중 AZ 또는 단일 AZ 2입니다.
   - 스토리지 용량은 2,000GiB 이상입니다.
6. 파일 시스템을 생성하기 전에 요약 검토를 선택하여 설정을 검토하세요.
7. 파일 시스템 생성을 선택합니다.

기존 백업에서 새 파일 시스템을 성공적으로 생성했습니다.

연습 3: 기존 파일 시스템 업데이트

연습 절차에 따라 세 가지 요소를 업데이트할 수 있습니다. 파일 시스템의 다른 업데이트할 수 있는 모든 요소는 콘솔에서 업데이트할 수 있습니다. 이 절차에서는 로컬 컴퓨터에 AWS CLI를 설치하고 구성한 것으로 가정합니다. 자세한 내용은 AWS Command Line Interface 사용 설명서의 설치 및 구성 섹션을 참조하세요.

- AutomaticBackupRetentionDays - 파일 시스템의 자동 백업을 유지하는 일수.
- DailyAutomaticBackupStartTime - UTC(협정 세계시)로 나타낸 하루 중 자동 백업 기간을 시작하는 시각. 백업 기간은 지정 시각에서 시작하여 30분입니다. 백업 기간은 주간 유지 보수 기간과 겹칠 수 없습니다.
- WeeklyMaintenanceStartTime – 유지 관리 기간을 시작하려는 주중 시각. 1일이 월요일, 2일이 화요일 순서입니다. 백업 기간은 지정 시각에서 시작하여 30분입니다. 주중 유지 관리 기간은 일일 자동 백업 기간과 겹칠 수 없습니다.

다음 절차는 AWS CLI를 사용하여 파일 시스템을 업데이트하는 방법을 설명합니다.

파일 시스템의 자동 백업 보존 기간 업데이트

1. 로컬 컴퓨터에서 명령 프롬프트 또는 터미널을 엽니다.
2. 다음 명령을 실행하여 파일 시스템 ID를 사용자 파일 시스템의 ID로 바꾸고 원하는 자동 백업 보존 기간 일수를 바꿉니다.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration AutomaticBackupRetentionDays=30
```

파일 시스템의 일일 백업 기간 업데이트

1. 로컬 컴퓨터에서 명령 프롬프트 또는 터미널을 엽니다.
2. 다음 명령을 실행하여 파일 시스템 ID를 사용자 파일 시스템의 ID로 바꾸고 백업 기간을 시작하려는 시간으로 바꿉니다.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration DailyAutomaticBackupStartTime=01:00
```

파일 시스템의 주간 유지 관리 기간 업데이트

1. 로컬 컴퓨터에서 명령 프롬프트 또는 터미널을 엽니다.
2. 다음 명령을 실행하여 파일 시스템 ID를 파일 시스템의 ID로 바꾸고 기간을 시작하려는 날짜 및 시간으로 바꿉니다.

```
aws fsx update-file-system --file-system-id fs-0123456789abcdef0 --windows-
configuration WeeklyMaintenanceStartTime=1:01:30
```

연습 4: Amazon AppStream 2.0과 함께 Amazon FSx 사용

Amazon FSx for Windows File Server는 서버 메시지 블록(SMB) 프로토콜을 지원하여 Amazon EC2, AWS 내 VMware Cloud, Amazon WorkSpaces, Amazon AppStream 2.0 인스턴스에서 파일 시스템에 액세스할 수 있도록 지원합니다. AppStream 2.0은 완전 관리형 애플리케이션 스트리밍 서비스입니다. AppStream 2.0에서 데스크톱 애플리케이션을 중앙에서 관리하고 모든 컴퓨터의 브라우저에 안전하게 제공할 수 있습니다. AppStream 2.0에 대한 자세한 내용은 Amazon AppStream 2.0 관리 안내서를 참조하세요. Amazon AppStream 2.0 이미지 및 플릿의 관리를 간소화하는 방법에 대한 지침은 AWS 블로그 게시물 사용자 지정 AppStream 2.0 Windows 이미지 자동 생성을 참조하세요.

이 연습을 두 가지 사용 사례에 대해 AppStream 2.0과 함께 Amazon FSx를 사용하는 방법을 안내하는 지침으로 사용하세요. 각 사용자에게 개인용 영구 스토리지를 제공하고 사용자 간에 공통 파일에 액세스할 수 있는 공유 폴더를 제공할 수 있습니다.

각 사용자에게 개인용 영구 스토리지 제공

Amazon FSx를 사용하여 AppStream 2.0 스트리밍 세션에서 조직의 모든 사용자에게 고유한 스토리지 드라이브를 제공할 수 있습니다. 사용자는 자신의 폴더에만 액세스할 수 있는 권한을 갖습니다. 스트리밍 세션 시작 시 드라이브가 자동으로 마운트되며 드라이브에 추가 또는 업데이트된 파일은 스트리밍 세션 간에 자동으로 유지됩니다.

이 작업을 완료하려면 세 가지 절차를 수행해야 합니다.

Amazon FSx를 사용하여 도메인 사용자를 위한 홈 폴더 생성

1. Amazon FSx 파일 시스템 생성 자세한 내용은 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.
2. 파일 시스템을 사용할 수 있게 되면 Amazon FSx 파일 시스템 내에 모든 도메인 AppStream 2.0 사용자를 위한 폴더를 생성합니다. 다음 예제에서는 사용자의 도메인 사용자 이름을 해당 폴더의 이

름으로 사용합니다. 이렇게 하면 Windows 환경 변수 `%username%`을 사용하여 쉽게 매핑할 파일 공유의 UNC 이름을 만들 수 있습니다.

3. 각 폴더를 공유 폴더로 공유하세요. 자세한 내용은 Windows File Server 파일 시스템용 FSx의 파일 공유 관리 섹션을 참조하세요.

도메인에 조인된 AppStream 2.0 이미지 빌더 시작

1. https://console.aws.amazon.com/appstream2로 AppStream 2.0 콘솔에 로그인합니다.
2. 탐색 메뉴에서 디렉토리 구성을 선택하고 디렉토리 구성 객체를 생성합니다. 자세한 내용은 Amazon AppStream 2.0 관리 안내서의 Active Directory와 함께 AppStream 2.0 사용을 참조하세요.
3. 이미지, 이미지 빌더를 선택하고 새 이미지 빌더를 시작합니다.
4. 이미지 빌더를 Active Directory 도메인에 조인하려면 이미지 빌더 시작 마법사에서 이전에 만든 디렉터리 구성의 개체를 선택합니다.
5. Amazon FSx 파일 시스템과 동일한 VPC에서 이미지 빌더를 시작합니다. Amazon FSx 파일 시스템이 연결되어 있는 동일한 AWS Managed Microsoft AD 디렉터리에 이미지 빌더를 연결해야 합니다. 이미지 빌더와 연결하는 VPC 보안 그룹은 Amazon FSx 파일 시스템에 대한 액세스를 허용해야 합니다.
6. 이미지 빌더를 사용할 수 있게 되면 이미지 빌더에 연결하고 도메인 관리자 계정을 사용하여 로그인합니다.
7. 애플리케이션을 설치합니다.

Amazon FSx 파일 공유를 AppStream2.0에 연결

1. 이미지 빌더에서 다음 명령으로 배치 스크립트를 생성하고 알려진 파일 위치(예: C:\Scripts\map - fs.bat)에 저장합니다. 다음 예제에서는 S:를 드라이브 문자로 사용하여 Amazon FSx 파일 시스템의 공유 폴더를 매핑합니다. 이 스크립트에서 Amazon FSx 파일 시스템의 DNS 이름 또는 파일 시스템과 연결된 DNS 별칭을 사용합니다. DNS 별칭은 Amazon FSx 콘솔의 파일 시스템 세부 정보 보기에서 확인할 수 있습니다.

   파일 시스템의 DNS 이름을 사용하는 경우

```
@echo off
net use S: /delete
net use S: \\file-system-DNS-name\users\%username%
```

파일 시스템과 연결된 DNS 별칭을 사용하는 경우

```
@echo off
net use S: /delete
net use S: \\fqdn-DNS-alias\users\%username%
```

2. PowerShell 프롬프트를 열고 `gpedit.msc` 명령을 실행합니다.
3. 사용자 구성에서 Windows 설정을 선택한 다음 로그온을 선택합니다.
4. 이 절차의 첫 번째 단계에서 생성한 배치 스크립트로 이동하여 스크립트를 선택합니다.
5. 컴퓨터 구성에서 Windows 관리 템플릿, 시스템, 그룹 정책을 차례로 선택합니다.
6. 로그온 스크립트 지연 구성 정책을 선택합니다. 정책을 활성화하고 시간 지연을 `0`로 줄이십시오. 이 설정은 사용자가 스트리밍 세션을 시작할 때 사용자 로그온 스크립트가 즉시 실행되도록 하는 데 도움이 됩니다.
7. 이미지를 생성하여 AppStream 2.0 플릿에 할당합니다. 또한 이미지 빌더에 사용한 것과 동일한 Active Directory 도메인에 AppStream 2.0 플릿을 조인해야 합니다. Amazon FSx 파일 시스템이 사용하는 동일한 VPC에서 플릿을 시작합니다. 플릿과 연결하는 VPC 보안 그룹은 Amazon FSx 파일 시스템에 대한 액세스를 제공해야 합니다.
8. SAML SSO를 사용하여 스트리밍 세션을 시작합니다. Active Directory에 조인된 플릿에 연결하려면 SAML 공급자를 사용하여 Single Sign-On 페더레이션을 구성하세요. 자세한 내용은 Amazon AppStream 2.0 관리 안내서의 AppStream 2.0에 SAML 2.0을 사용하여 Single Sign-On 액세스를 참조하세요.
9. Amazon FSx 파일 공유는 스트리밍 세션 내의 S: 드라이브 문자에 매핑됩니다.

사용자 간 공유 폴더 제공

Amazon FSx를 사용하여 조직의 사용자에게 공유 폴더를 제공할 수 있습니다. 공유 폴더를 사용하여 모든 사용자에게 필요한 공통 파일(예: 데모 파일, 코드 예제, 지침 매뉴얼 등)을 관리할 수 있습니다.

이 작업을 완료하려면 세 가지 절차를 수행해야 합니다.

Amazon FSx를 사용하여 공유 폴더 생성

1. Amazon FSx 파일 시스템 생성 자세한 내용은 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.
2. 모든 Amazon FSx 파일 시스템에는 기본적으로 *file-system-DNS-name*\share, 또는 DNS 별칭을 사용하는 경우 *fqdn-DNS-alias*\share를 주소로 사용하여 액세스할 수 있는 공유 폴더가

포함되어 있습니다. 기본 공유를 사용하거나 다른 공유 폴더를 생성할 수 있습니다. 자세한 내용은 Windows File Server 파일 시스템용 FSx의 파일 공유 관리 섹션을 참조하세요.

AppStream 2.0 이미지 빌더 시작

1. AppStream 2.0 콘솔에서 새 이미지 빌더를 시작하거나 기존 이미지 빌더에 연결합니다. Amazon FSx 파일 시스템이 사용하는 동일한 VPC에서 이미지 빌더를 시작합니다. 이미지 빌더와 연결하는 VPC 보안 그룹은 Amazon FSx 파일 시스템에 대한 액세스를 허용해야 합니다.
2. 이미지 빌더를 사용할 수 있게 되면 관리자 사용자로 이미지 빌더에 연결합니다.
3. 관리자 권한으로 애플리케이션을 설치하거나 업데이트하세요.

AppStream 2.0에 공유 폴더 연결

1. 이전 절차에서 설명한 대로 배치 스크립트를 생성하여 사용자가 스트리밍 세션을 시작할 때마다 공유 폴더를 자동으로 마운트합니다. 스크립트를 완료하려면 파일 시스템의 DNS 이름 또는 파일 시스템과 연결된 DNS 별칭(Amazon FSx Console의 파일 시스템 세부 정보 보기에서 확인 가능)과 공유 폴더에 액세스하기 위한 보안 인증 정보가 필요합니다.

   파일 시스템의 DNS 이름을 사용하는 경우

   ```
   @echo off
   net use S: /delete
   net use S: \\file-system-DNS-name\share /user:username password
   ```

   파일 시스템과 연결된 DNS 별칭을 사용하는 경우

   ```
   @echo off
   net use S: /delete
   net use S: \\fqdn-DNS-alias\share /user:username password
   ```

2. 그룹 정책을 생성하여 사용자가 로그온할 때마다 배치 스크립트를 실행하세요. 이전 섹션의 설명한 지침을 따를 수 있습니다.
3. 이미지를 생성하여 플릿에 할당합니다.
4. 스트리밍 세션을 시작합니다. 이제 공유 폴더가 드라이브 문자에 자동으로 매핑되는 것을 볼 수 있을 것입니다.

연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스

FSx for Windows File Server는 파일 시스템의 데이터에 액세스하는 데 사용할 수 있는 모든 파일 시스템에 기본 도메인 이름 시스템(DNS) 이름을 제공합니다. 선택한 DNS 별칭을 사용하여 파일 시스템에 액세스할 수도 있습니다. DNS 별칭을 사용하면 도구나 애플리케이션을 업데이트할 필요 없이 온프레미스에서 Amazon FSx로 파일 시스템 스토리지를 마이그레이션할 때 기존 DNS 이름을 사용하여 Amazon FSx에 저장된 데이터에 계속 액세스할 수 있습니다. 언제든지 한 번에 파일 시스템에 최대 50개의 DNS 별칭을 연결할 수 있습니다.

DNS 별칭을 사용하여 Amazon FSx 파일 시스템에 액세스하려면 다음 세 단계를 수행해야 합니다.

1. DNS 별칭을 Amazon FSx 파일 시스템에 연결합니다.
2. 파일 시스템 컴퓨터 객체의 서비스 보안 주체 이름(SPN)을 구성합니다. (DNS 별칭을 사용하여 파일 시스템에 액세스할 때 Kerberos 인증을 받는 데 필요합니다.)
3. 파일 시스템 및 DNS 별칭에 대한 DNS CNAME 레코드를 업데이트하거나 생성합니다.

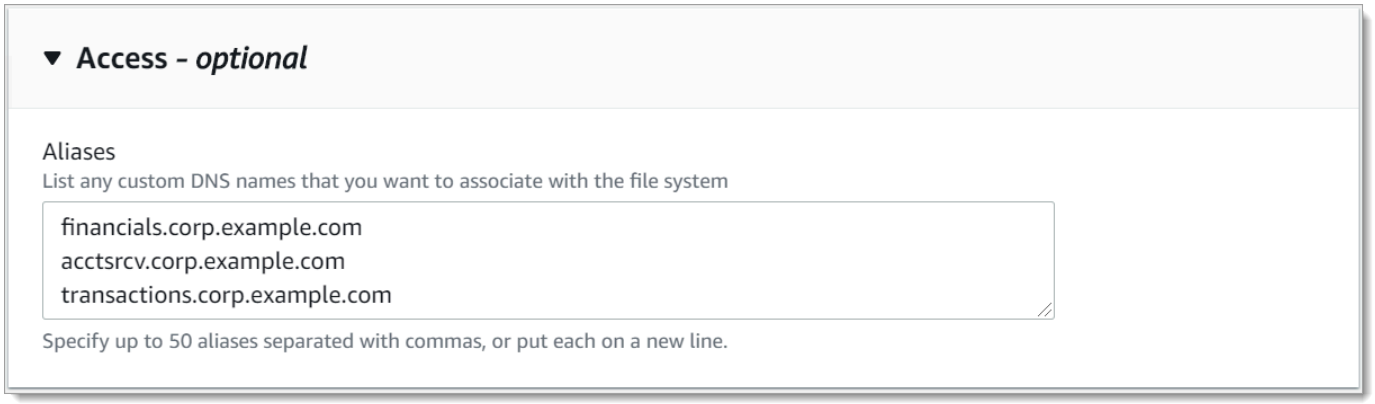
주제

1단계: DNS 별칭을 Amazon FSx 파일 시스템에 연결

Amazon FSx 콘솔, CLI, 및 API를 사용하여 새 파일 시스템을 생성하고 백업에서 새 파일 시스템을 생성할 때 기존 FSx for Windows File Server 파일 시스템에 DNS 별칭을 연결할 수 있습니다. 다른 도메인 이름으로 별칭을 생성하는 경우, 상위 도메인을 포함한 전체 이름을 입력하여 별칭을 연결합니다.

이 절차는 Amazon FSx 콘솔을 사용하여 새 파일 시스템을 생성할 때 DNS 별칭 연결 방법을 설명합니다. DNS 별칭을 기존 파일 시스템에 연결하는 방법과 CLI 및 API 사용에 대한 자세한 내용은 DNS 별칭 관리 섹션을 참조하세요.

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 시작하기 섹션의 파일 시스템 생성 섹션에 설명된 새 파일 시스템 생성 절차를 따릅니다.
3. 파일 시스템 생성 마법사의 액세스 - 옵션 섹션에서 파일 시스템에 연결할 DNS 별칭을 입력합니다.



DNS 별칭을 지정할 때는 다음 지침을 따르세요.

- 정규화된 도메인 이름(FQDN) *hostname.domain* 형식으로 예를 들어 `accounting.example.com`이어야 합니다.
- 영숫자 및 하이픈(-)을 포함할 수 있습니다.
- 하이픈으로 시작되거나 끝날 수 없습니다.
- 숫자로 시작될 수 있습니다.

DNS 별칭 이름의 경우 Amazon FSx는 영문자가 지정된 방법(대문자, 소문자 또는 이스케이프 코드)과 관계없이 영문자를 소문자(a~z)로 저장합니다.

4. 유지 관리 기본 설정을 원하는 대로 변경합니다.
5. 태그 - 선택 사항 섹션에서 필요한 태그를 추가하고 다음을 선택합니다.
6. 파일 시스템 생성 페이지에 표시된 파일 시스템 구성을 검토합니다. 파일 시스템 생성을 선택해 파일 시스템을 생성합니다.

   새 파일 시스템을 사용할 수 있게 되면 2단계를 계속합니다.

2단계: Kerberos의 서비스 보안 주체 이름(SPN) 구성

Amazon FSx에서는 전송 중에 Kerberos 기반 인증 및 암호화를 사용하는 것이 좋습니다. Kerberos는 파일 시스템에 액세스하는 클라이언트에게 가장 안전한 인증을 제공합니다.

DNS 별칭을 사용하여 Amazon FSx에 액세스하는 클라이언트의 Kerberos 인증을 활성화하려면 Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 있는 DNS 별칭에 해당하는 서비스 보안 주체 이름(SPN)을 추가해야 합니다. SPN은 한 번에 하나의 Active Directory 컴퓨터 개체와만 연결할

수 있습니다. 원래 파일 시스템의 Active Directory 컴퓨터 객체에 대해 구성된 DNS 이름의 기존 SPN이 있으면 해당 SPN을 삭제해야 합니다.

케르베로스 인증에는 두 개의 SPN이 필요합니다.

```
HOST/alias
HOST/alias.domain
```

별칭이 `finance.domain.com`인 경우, 두 개의 필수 SPN은 다음과 같습니다.

```
HOST/finance
HOST/finance.domain.com
```

> **Note**
>
> Amazon FSx 파일 시스템의 Active Directory(AD) 컴퓨터 객체에 대한 새 호스트 SPN을 생성하기 전에 Active Directory 컴퓨터 객체의 DNS 별칭에 해당하는 기존 HOST SPN을 삭제해야 합니다. DNS 별칭의 SPN이 AD에 있는 경우, Amazon FSx 파일 시스템의 SPN 설정 시도는 실패합니다.

다음 절차는 다음 일을 하는 방법을 설명합니다.

- 원본 파일 시스템의 Active Directory 컴퓨터 객체에서 기존 DNS 별칭 SPN을 찾습니다.
- SPN을 찾으면 삭제합니다.
- Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 새 DNS 별칭 SPN을 생성합니다.

필수 PowerShell Active Directory 모듈을 설치하려면

1. Amazon FSx 파일 시스템이 조인되고 Active Directory에 조인된 Windows 인스턴스에 로그온합니다.
2. 관리자 PowerShell 권한으로 엽니다.
3. 다음 명령을 사용하여 PowerShell 액티브 디렉터리 모듈을 설치합니다.

   ```
   Install-WindowsFeature RSAT-AD-PowerShell
   ```

원본 파일 시스템의 Active Directory 컴퓨터 개체에서 기존 DNS 별칭 SPN을 찾아 삭제

1. 다음 명령을 사용하여 기존 SPN을 모두 찾습니다. 1단계에서 파일 시스템에 연결한 *alias_fqdn*을 DNS 별칭으로 바꿉니다.

```
## Find SPNs for original file system's AD computer object
$ALIAS = "alias_fqdn"
SetSPN /Q ("HOST/" + $ALIAS)
SetSPN /Q ("HOST/" + $ALIAS.Split(".")[0])
```

2. 다음 예제 스크립트를 사용하여 이전 단계에서 반환된 기존 HOST SPN을 삭제합니다.

   - 1단계에서 파일 시스템에 연결한 *alias_fqdn*을 전체 DNS 별칭으로 바꿉니다.
   - *file_system_DNS_name*을 원래 파일 시스템의 DNS 이름으로 바꿉니다.

```
## Delete SPNs for original file system's AD computer object
$Alias = "alias_fqdn"
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})

SetSPN /D ("HOST/" + ${Alias}) ${FSxAdComputer}.Name
SetSPN /D ("HOST/" + ${Alias}.Split(".")[0]) ${FSxAdComputer}.Name
```

3. 1단계에서 파일 시스템에 연결한 각 DNS 별칭에 대해 이전 단계를 반복합니다.

Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 SPN 설정

1. 다음 명령을 실행하여 Amazon FSx 파일 시스템의 새 SPN을 설정합니다.

   - *file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 DNS 이름으로 대체합니다.

     Amazon FSx 콘솔에서 파일 시스템의 DNS 이름을 찾으려면 파일 시스템을 선택하고 파일 시스템을 선택한 다음 파일 시스템 세부 정보 페이지의 네트워크 및 보안 창을 선택합니다.

     DescribeFile시스템 API 작업의 응답으로 DNS 이름을 가져올 수도 있습니다.
   - 1단계에서 파일 시스템에 연결한 *alias_fqdn*을 전체 DNS 별칭으로 바꿉니다.

```
## Set SPNs for FSx file system AD computer object
$FSxDnsName = "file_system_DNS_name"
$Alias = "alias_fqdn"
$FileSystemHost = (Resolve-DnsName $FSxDnsName | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity $FileSystemHost)

##Use one of the following commands, not both:
Set-AdComputer -Identity $FSxAdComputer -Add @{"msDS-
AdditionalDnsHostname"="$Alias"}
##Or
SetSpn /S ("HOST/" + $Alias.Split('.')[0]) $FSxAdComputer.Name
SetSpn /S ("HOST/" + $Alias) $FSxAdComputer.Name
```

> **Note**
>
> DNS 별칭에 대한 SPN이 원본 파일 시스템 컴퓨터 객체의 AD에 있는 경우 Amazon FSx 파일 시스템에 대한 SPN 설정이 실패합니다. 기존 SPN 검색 및 삭제에 대한 자세한 내용은 원본 파일 시스템의 Active Directory 컴퓨터 개체에서 기존 DNS 별칭 SPN을 찾아 삭제 섹션을 참조하세요.

2. 다음 예제 스크립트를 사용하여 새 SPN이 DNS 별칭에 맞게 구성되었는지 확인합니다. 이 절차의 앞부분에서 설명한 대로 응답에 두 개의 HOST SPN HOST/*alias*, HOST/*alias_fqdn*이 포함되어 있는지 확인합니다.

   *file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 DNS 이름으로 대체합니다. Amazon FSx 콘솔에서 파일 시스템의 DNS 이름을 찾으려면 파일 시스템을 선택하고 파일 시스템을 선택한 다음 파일 시스템 세부 정보 페이지의 네트워크 및 보안 창을 선택합니다.

   DescribeFile시스템 API 작업에 대한 응답으로 DNS 이름을 가져올 수도 있습니다.

```
## Verify SPNs on FSx file system AD computer object
$FileSystemDnsName = "file_system_dns_name"
$FileSystemHost = (Resolve-DnsName ${FileSystemDnsName} | Where Type -eq 'A')
[0].Name.Split(".")[0]
$FSxAdComputer = (Get-AdComputer -Identity ${FileSystemHost})
SetSpn /L ${FSxAdComputer}.Name
```

3. 1단계에서 파일 시스템에 연결한 각 DNS 별칭에 대해 이전 단계를 반복합니다.

Amazon FSx 파일 시스템에 연결할 때 클라이언트가 Kerberos 인증 및 암호화를 사용하도록 강제하는 방법에 대한 자세한 내용은 GPO를 사용하여 Kerberos 인증 적용 섹션을 참조하세요.

3단계: 파일 시스템의 DNS CNAME 레코드 업데이트 또는 생성

파일 시스템에 맞게 SPN을 적절히 구성한 후에는 원래 파일 시스템으로 확인된 각 DNS 레코드를 Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 레코드로 교체하여 Amazon FSx로 전환할 수 있습니다.

이 섹션에 제시된 명령을 실행하려면 `dnsserver` 및 `activedirectory` Windows 모듈이 필요합니다.

필수 PowerShell cmdlet을 설치하려면

1. Amazon FSx 파일 시스템이 DNS 관리 권한을 가진 그룹 AWSAWS (관리형 Active Directory의 위임 도메인 이름 시스템 관리자, 자체 관리형 Active AWS Directory에서 DNS 관리 권한을 위임한 도메인 관리자 또는 다른 그룹) 의 구성원인 사용자로 가입된 Active Directory에 가입된 Windows 인스턴스에 로그온합니다.

   자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
2. 관리자 PowerShell 권한으로 엽니다.
3. 이 절차의 지침을 수행하려면 PowerShell DNS 서버 모듈이 필요합니다. 다음 명령을 사용하여 모듈을 설치합니다.

   ```
   Install-WindowsFeature RSAT-DNS-Server
   ```

Amazon FSx 파일 시스템의 사용자 지정 DNS 이름 업데이트 또는 생성

1. DNS 관리 권한이 있는 그룹 (관리형 Active Directory의 AWS 위임 도메인 이름 시스템 관리자, 자체 AWS 관리형 Active Directory에서 DNS 관리 권한을 위임한 도메인 관리자 또는 다른 그룹) 의 구성원인 사용자로 Amazon EC2 인스턴스에 연결합니다.

   자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
2. 명령 프롬프트에서 다음 스크립트를 실행합니다. 이 스크립트는 기존 DNS CNAME 레코드를 Amazon FSx 파일 시스템으로 마이그레이션합니다. 찾지 못했다면 Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 별칭 *alias_fqdn*에 대한 새 DNS CNAME 레코드를 생성합니다.

다음과 같이 스크립트를 실행합니다.

- *alias_fqdn*을 파일 시스템에 연결한 DNS 별칭으로 바꿉니다.
- *file_system_DNS_name*을 Amazon FSx가 파일 시스템에 할당한 DNS 이름으로 대체합니다.

```
$Alias="alias_fqdn"
$FSxDnsName="file_system_dns_name"
$AliasHost=$Alias.Split('.')[0]
$ZoneName=((Get-WmiObject Win32_ComputerSystem).Domain)
$DnsServerComputerName = (Resolve-DnsName $ZoneName -Type NS | Where Type -eq 'A' |
 Select -ExpandProperty Name) | Select -First 1
foreach ($computer in $DnsServerComputerName)
{
Add-DnsServerResourceRecordCName -Name $AliasHost -ComputerName $computer -
HostNameAlias $FSxDnsName -ZoneName $ZoneName
}
```

3. 1단계에서 파일 시스템에 연결한 각 DNS 별칭에 대해 이전 단계를 반복합니다.

DNS 별칭을 사용하여 Amazon FSx 파일 시스템에 DNS CNAME 값을 추가한 것입니다. 이제 DNS 별칭을 사용하여 데이터에 액세스할 수 있습니다.

> **Note**
>
> 이전에 다른 파일 시스템을 가리키던 Amazon FSx 파일 시스템을 가리키도록 DNS CNAME 레코드를 업데이트하면 클라이언트가 잠시 동안 파일 시스템에 연결하지 못할 수 있습니다. 클라이언트 DNS 캐시가 새로 고쳐지면 DNS 별칭을 사용하여 연결할 수 있어야 합니다. 자세한 정보는 DNS 별칭으로 파일 시스템 액세스 불가을 참조하세요.

GPO를 사용하여 Kerberos 인증 적용

Active Directory에서 다음과 같은 그룹 정책 객체(GPO)를 설정하여 파일 시스템에 액세스할 때 Kerberos 인증 및 암호화를 사용하도록 강제할 수 있습니다.

- NTLM 제한: 원격 서버로 나가는 NTLM 트래픽 제한 - 이 정책 설정을 사용하면 컴퓨터에서 Windows 운영 체제를 실행하는 원격 서버로 나가는 NTLM 트래픽을 거부하거나 감사할 수 있습니다.

- NTLM 제한: 원격 서버의 NTLM 인증 예외 추가 - 네트워크 보안: NTLM 제한: 원격 서버로 나가는 NTLM 트래픽 정책 설정이 구성된 경우, 이 정책 설정을 사용하여 클라이언트 장치가 NTLM 인증을 사용할 수 있도록 원격 서버 예외 목록을 만들 수 있습니다.

1. Amazon FSx 파일 시스템이 조인되고 Active Directory에 관리자로 조인된 Windows 인스턴스에 로그온합니다. 자체 관리형 Active Directory를 구성하는 경우, Active Directory에 다음 단계를 직접 적용합니다.
2. 시작을 선택하고, 관리 도구를 선택한 다음 그룹 정책 관리를 선택합니다.
3. 그룹 정책 객체를 선택합니다.
4. 그룹 정책 객체가 없으면 새로 생성합니다.
5. 기존 네트워크 보안: NTLM 제한: 원격 서버로 나가는 NTLM 트래픽 정책을 찾습니다. (기존 정책이 없는 경우, 새 정책을 생성합니다.) 로컬 보안 설정 탭에서 컨텍스트 메뉴(오른쪽 클릭)를 열고 속성을 선택합니다.
6. 모두 거부를 선택합니다.
7. 적용을 선택하여 보안 설정을 저장합니다.
8. 클라이언트의 특정 원격 서버에 대한 NTLM 연결 예외를 설정하려면 네트워크 보안: NTLM 제한: 원격 서버 예외 추가를 찾으세요.

   컨텍스트 메뉴(오른쪽 클릭)를 열고 로컬 보안 설정 탭에서 속성을 선택합니다.
9. 예외 목록에 추가할 서버의 이름을 입력합니다.
10. 적용을 선택하여 보안 설정을 저장합니다.

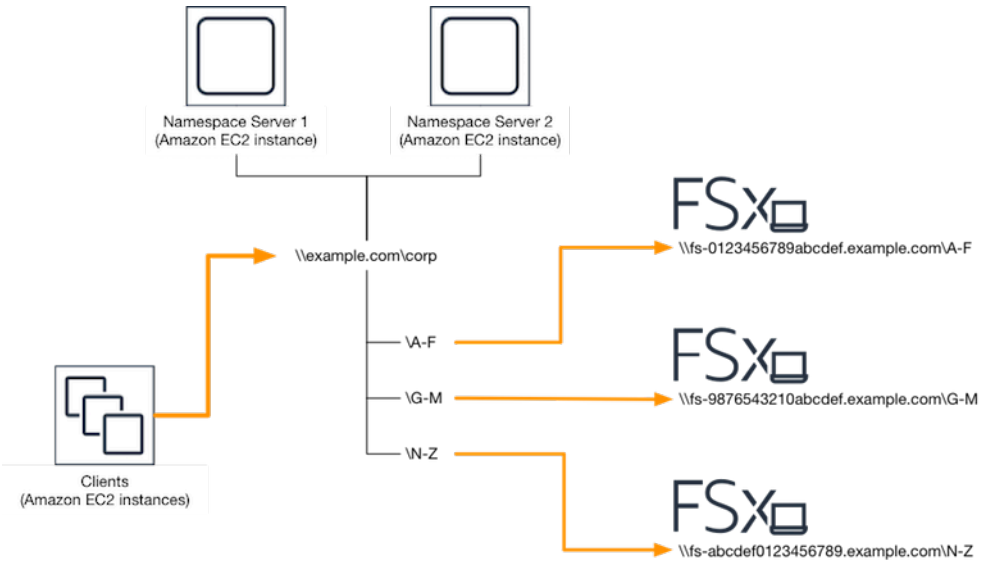
연습 6: 샤드를 통한 스케일 아웃

Amazon FSx for Windows File Server는 Microsoft 분산 파일 시스템(DFS) 사용을 지원합니다. DFS 네임스페이스를 사용하면 파일 데이터를 여러 Amazon FSx 파일 시스템에 분산하여 I/O 집약적인 워크로드를 처리하도록 성능(읽기 및 쓰기 모두)을 확장할 수 있습니다. 동시에 공통 네임스페이스를 사용하여 애플리케이션에 통합된 뷰를 제공할 수도 있습니다. 이 솔루션에는 파일 데이터를 더 작은 데이터 세트 또는 샤드로 나누어 여러 파일 시스템에 저장하는 작업이 포함됩니다. 여러 인스턴스에서 데이터에 액세스하는 애플리케이션은 이러한 샤드에 대한 읽기 및 쓰기를 병렬로 수행하여 높은 수준의 성능을 달성할 수 있습니다.

워크로드에 파일 데이터에 대한 균일하게 분산된 읽기, 쓰기 액세스가 필요한 경우(예: 컴퓨팅 인스턴스의 각 하위 집합이 파일 데이터의 다른 부분에 액세스하는 경우) 이 솔루션을 사용할 수 있습니다.

스케일 아웃 성능을 위한 DFS 네임스페이스 설정

다음 절차는 Amazon FSx에서 스케일 아웃 성능을 위한 DFS 솔루션을 생성하는 과정을 안내합니다. 이 예시에서는 *corp* 네임스페이스에 저장된 데이터를 알파벳순으로 분할합니다. 데이터 파일 'A~F', 'G~M', 'N~Z'는 모두 서로 다른 파일 공유에 저장됩니다. 데이터 유형, I/O 크기 및 I/O 액세스 패턴에 따라 여러 파일 공유에서 데이터를 가장 잘 분할하는 방법을 결정해야 합니다. 사용하려는 모든 파일 공유에 I/O를 균등하게 분배하는 샤드 규칙을 선택하세요. 각 네임스페이스는 최대 50,000개의 파일 공유와 총 수백 페타바이트의 스토리지 용량을 지원한다는 점에 유의하세요.



스케일 아웃 성능을 위한 DFS 네임스페이스 설정

1. 아직 DFS 네임스페이스 서버를 실행하지 않은 경우 Setup-DFSN-servers.template 템플릿을 사용하여 가용성이 높은 DFS 네임스페이스 서버 쌍을 시작할 수 있습니다. AWS CloudFormation 스택 생성에 대한 자세한 내용은 사용 설명서의 콘솔에서 스택 생성을 참조하십시오. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. AWS 위임 관리자 그룹의 사용자로 이전 단계에서 시작한 DFS 네임스페이스 서버 중 하나에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. DFS 관리 콘솔를 열어 액세스합니다. 시작 메뉴를 열고 dfsmgmt.msc를 실행합니다. 그러면 DFS 관리 GUI 도구가 열립니다.
4. 작업 , 새 네임스페이스 순으로 선택하고 서버용으로 시작한 첫 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력한 후 다음을 선택합니다.
5. 이름에는 만들려는 네임스페이스(예: corp)를 입력합니다.
6. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정합니다. 다음을 선택합니다.

7. 기본 도메인 기반 네임스페이스 옵션을 선택한 상태로 두고 Windows Server 2008 모드 활성화 옵션을 선택한 상태로 두고 다음을 선택합니다.

> **Note**
>
> Windows Server 2008 모드는 네임스페이스에 사용할 수 있는 최신 옵션입니다.

8. 네임스페이스 설정을 검토한 다음 생성을 선택합니다.
9. 탐색 표시줄의 네임스페이스에서 새로 만든 네임스페이스를 선택한 상태에서 작업, 네임스페이스 서버 추가 순으로 선택합니다.
10. 네임스페이스 서버용으로 시작한 두 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력합니다.
11. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정한 다음 확인을 선택합니다.
12. 방금 만든 네임스페이스의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 새 폴더 를 선택한 다음 첫 번째 샤드의 폴더 이름(예: `A-F`에 Name)을 입력하고 추가를 선택합니다.
13. 폴더 대상 경로에 이 샤드를 호스팅하는 파일 공유의 DNS 이름(예: `\\fs-0123456789abcdef0.example.com\A-F`)을 UNC 형식으로 입력하고 확인을 선택합니다.
14. 샤드가 존재하지 않는 경우
    a. 예를 선택하여 생성합니다.
    b. 공유 생성 대화 상자에서 탐색을 선택합니다.
    c. 기존 폴더를 선택하거나 D$에서 새 폴더를 만든 다음 확인을 선택합니다.
    d. 적절한 공유 권한을 설정하고 확인을 선택합니다.
15. 이제 샤드에 대한 폴더 대상이 추가된 상태에서 확인을 선택합니다.
16. 동일한 네임스페이스에서 추가하려는 다른 샤드에 대해 마지막 네 단계를 반복합니다.

연습 7: 백업을 다른 AWS 리전에 복사

Amazon FSx를 사용하면 동일 AWS 계정 내의 기존 백업을 다른 AWS 리전(크로스 리전 백업 사본) 또는 동일 AWS 리전(리전 내 백업 사본)으로 복사할 수 있습니다.

다음 절차는 동일 AWS 계정 내에서 백업 사본을 생성하는 과정을 안내합니다. 이 백업 사본을 생성하려면 먼저 기존 백업이 있어야 합니다. 자세한 내용은 백업 작업 섹션을 참조하세요.

기존 백업을 동일한 AWS 계정 내에 복사(크로스 리전 또는 리전 내)

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 탐색 창에서 백업을 선택합니다.
3. 백업 테이블에서, 복사하려는 백업을 선택합니다.
4. 백업 복사를 선택합니다. 이렇게 하면 백업 복사 마법사가 열립니다.
5. 대상 리전 목록에서 백업을 복사할 대상 AWS 리전을 선택합니다. 대상은 다른 AWS 리전에 있을 수도 있고 동일한 AWS 리전 내에 있을 수도 있습니다.
6. (선택 사항) 소스 백업에서 대상 백업으로 태그를 복사하려면 태그 복사를 선택합니다. 8단계에서 태그 복사를 선택하고 태그도 추가하면 모든 태그가 병합됩니다.
7. 암호화의 경우 복사된 백업을 암호화하는 데 사용할 AWS KMS 암호화 키를 선택합니다.
8. 태그 - 선택 사항의 경우 키와 값을 입력하여 태그를 복사된 백업에 추가합니다. 6단계에서 태그 복사를 선택하고 태그도 추가하면 모든 태그가 병합됩니다.
9. 백업 복사를 선택합니다.

이제 동일한 AWS 계정에서 다른 AWS 리전으로 또는 동일 AWS 리전 내에서 백업을 복사했습니다.

Amazon FSx의 보안

클라우드 AWS 보안은 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드 보안 — AWS Amazon Web AWS Services 클라우드에서 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 서드 파티 감사원은 정기적으로 AWS 규정 준수 프로그램의 일환으로 보안 효과를 테스트하고 검증합니다. Amazon FSx for Windows File Server에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 제공 범위 내AWS 서비스를 참조하세요.
- 클라우드에서의 보안 — 귀하의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는Amazon FSx for Windows File Server를 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 Windows용 Amazon FSx File Server 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

Amazon FSx의 데이터 암호화

Amazon FSx for Windows File Server는 전송 중 데이터 암호화와 유휴 데이터 암호화라는 두 가지 파일 시스템 암호화를 지원합니다. 전송 중 데이터의 암호화는 SMB 프로토콜 3.0 이상을 지원하는 컴퓨

팅 인스턴스에 매핑된 파일 공유에서 지원됩니다. Amazon FSx 파일 시스템을 생성할 때 저장 데이터 암호화가 자동으로 활성화됩니다. Amazon FSx는 애플리케이션을 수정할 필요 없이 파일 시스템에 액세스할 때 SMB 암호화를 사용하여 전송 중 데이터를 자동으로 암호화합니다.

암호화를 사용해야 하는 경우

조직이 유휴 상태의 데이터 및 메타데이터 암호화를 요구하는 기업 정책이나 규제 정책을 준수해야 하는 경우 전송 중 데이터 암호화를 사용하여 파일 시스템을 마운트하는 암호화된 파일 시스템을 생성하는 것이 좋습니다.

Amazon FSx for Windows File Server의 암호화에 대한 자세한 내용은 다음의 관련 주제를 참조하세요.

- Amazon FSx for Windows File Server 파일 시스템 생성
- IAM 사용 설명서의 Amazon FSx에 사용되는 작업, 리소스 및 조건 키

주제

- 유휴 데이터 암호화
- 전송 중 데이터 암호화

유휴 데이터 암호화

모든 Amazon FSx 파일 시스템은 유휴 상태에서 AWS Key Management Service (AWS KMS)를 사용하여 관리되는 키로 암호화됩니다. 데이터는 파일 시스템에 기록되기 전에 자동으로 암호화되고 읽기 중에 자동으로 복호화됩니다. 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 연방 정보 처리 표준 (FIPS) 140-2에서 승인한 암호화 알고리즘을 사용합니다. 이 인프라는 미국 국립 표준 기술 연구소(NIST) 800-57 표준의 권장 사항에 부합됩니다.

아마존 FSx가 사용하는 방법 AWS KMS

Amazon FSx는 키 관리를 위해 와 통합됩니다. AWS KMS Amazon FSx는 AWS KMS key 를 사용하여 파일 시스템을 암호화합니다. 사용자는 파일 시스템(데이터 및 메타데이터 모두)을 암호화하고 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.

- AWS 관리형 키 – 기본 KMS 키로 무료로 사용할 수 있습니다.
- 고객 관리형 키 – 여러 사용자나 서비스에 대한 키 정책 및 권한을 구성할 수 있는 가장 유연한 KMS 키입니다. 고객 관리 키 생성에 대한 자세한 내용은 개발자 안내서의 키 생성을 참조하십시오. AWS Key Management Service

고객 관리형 키를 데이터 암호화 및 암호화 해제의 KMS 키로 사용하면 키 교체를 활성화할 수 있습니다. 키 교체를 활성화하면 AWS KMS 가 매년 1회 키를 자동 교체합니다. 또한 고객 관리형 키를 사용하면 KMS 키에 대한 액세스를 비활성화, 재활성화, 삭제, 취소하는 시기를 선택할 수 있습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 회전을 AWS KMS keys 참조하십시오.

유휴 파일 시스템의 암호화 및 암호화 해제는 투명하게 처리됩니다. 하지만 Amazon FSx 전용 AWS 계정 ID는 작업과 관련된 로그에 AWS CloudTrail 표시됩니다. AWS KMS

에 대한 아마존 FSx 주요 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 암호화된 저장 파일 시스템에 대해 Amazon FSx가 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 암호화 해제합니다. 사이퍼텍스트는 이전에 암호화한 일반 텍스트입니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms: ReEncrypt — (선택 사항) 클라이언트 측 데이터의 일반 텍스트를 노출하지 않고 새 KMS 키로 서버 측 데이터를 암호화합니다. 먼저 데이터를 복호화한 후 다시 암호화합니다. 이 권한은 기본 키 정책에 포함되어 있습니다.
- kms: GenerateData KeyWithout 일반 텍스트 — (필수) KMS 키로 암호화된 데이터 암호화 키를 반환합니다. 이 권한은 kms: Key*의 기본 키 정책에 포함됩니다. GenerateData
- kms: CreateGrant - (필수) 누가 어떤 조건에서 키를 사용할 수 있는지 지정하는 권한 부여를 키에 추가합니다. 이런 권한 부여는 키 정책을 대체하는 권한 메커니즘입니다. 권한 부여에 대한 자세한 내

용은 AWS Key Management Service 개발자 안내서의 권한 부여 사용을 참조하세요. 이 권한은 기본 키 정책에 포함되어 있습니다.

- kms: DescribeKey — (필수) 지정된 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

전송 중 데이터의 암호화는 SMB 프로토콜 3.0 이상을 지원하는 컴퓨팅 인스턴스에 매핑된 파일 공유에서 지원됩니다. 여기에는 Windows Server 2012와 Windows 8 이후 모든 Windows 버전과 Samba 클라이언트 버전 4.2 이상이 설치된 모든 Linux 클라이언트가 포함됩니다. Amazon FSx for Windows File Server는 애플리케이션을 수정할 필요 없이 파일 시스템에 액세스할 때 SMB 암호화를 사용하여 전송 중 데이터를 자동으로 암호화합니다.

SMB 암호화는 AES-128-GCM 또는 AES-128-CCM(클라이언트가 SMB 3.1.1을 지원하는 경우 GCM 변형 선택)을 암호화 알고리즘으로 사용하며 SMB Kerberos 세션 키를 사용한 서명을 통해 데이터 무결성을 제공합니다. AES-128-GCM 사용하면 성능이 향상됩니다. 예를 들어, 암호화된 SMB 연결을 통해 대용량 파일을 복제할 때 성능이 최대 2배 향상됩니다.

상시 암호화에 대한 규정 준수 요구 사항을 충족하기 위해 data-in-transit SMB 암호화를 지원하는 클라이언트에 대한 액세스만 허용하도록 파일 시스템 액세스를 제한할 수 있습니다. 또한 파일 공유별 또는 전체 파일 시스템에 대한 전송 중 암호화를 활성화하거나 비활성화할 수 있습니다. 이렇게 하면 동일한 파일 시스템에서 암호화된 파일 공유와 암호화되지 않은 파일 공유를 혼합하여 사용할 수 있습니다. 파일 시스템 관리에 encryption-in-transit 대한 자세한 내용은 을 참조하십시오. 전송 중 암호화 관리

Windows ACL을 사용한 파일 및 폴더 수준 액세스 제어

Amazon FSx for Windows File Server는 Microsoft Active Directory를 통해 SMB(Server Message Block) 프로토콜을 통한 ID 기반 인증을 지원합니다. Active Directory는 네트워크상의 개체에 대한 정보를 저장하고 관리자와 사용자가 이 정보를 쉽게 찾고 사용할 수 있도록 하는 Microsoft 디렉터리 서비스입니다. 이러한 개체에는 일반적으로 파일 서버, 네트워크 사용자 및 컴퓨터 계정과 같은 공유 리소스가 포함됩니다. Amazon FSx의 Active Directory 지원에 대한 자세한 내용은 FSx for Windows File Server에서 Microsoft Active Directory 작업 섹션을 참조하세요.

도메인에 연결된 컴퓨팅 인스턴스는 Active Directory 보안 인증 정보를 사용하여 Amazon FSx 파일 공유에 액세스할 수 있습니다. 파일 및 폴더 수준의 세분화된 액세스 제어를 위해 표준 Windows 액세스 제어 목록(ACL)을 사용합니다. Amazon FSx 파일 시스템은 파일 시스템 데이터에 액세스하는 사용자의 보안 인증 정보를 자동으로 확인하여 Windows ACL을 적용합니다.

모든 Amazon FSx 파일 시스템에는 기본 Windows 파일 공유가 `share`로 함께 제공됩니다. 해당 공유 폴더의 Windows ACL은 도메인 사용자에게 읽기/쓰기 액세스를 허용하도록 구성되어 있습니다. 또한 파일 시스템에서 관리 작업을 수행하도록 위임된 Active Directory의 위임된 관리자 그룹에 대한 모든 권한을 부여합니다. 파일 시스템을 AWS 관리형 Microsoft AD와 통합하는 경우 이 그룹은 AWS 위임 FSx 관리자입니다. 파일 시스템을 자체 관리형 Microsoft AD 설정과 통합하는 경우, 이 그룹은 도메인 관리자가 될 수 있습니다. 또는 파일 시스템을 생성할 때 지정한 사용자 지정 위임형 관리자 그룹이 될 수도 있습니다. ACL을 변경하려면 위임된 관리자 그룹의 구성원인 사용자로 공유를 매핑할 수 있습니다.

> **Warning**
>
> Amazon FSx에서는 시스템 사용자에게 파일 시스템 내 모든 폴더에 대한 전체 제어 NTFS ACL 권한이 있어야 합니다. 폴더에서 이 사용자의 NTFS ACL 권한을 변경하지 마세요. 이렇게 하면 파일 공유에 액세스할 수 없게 되고 파일 시스템 백업을 사용할 수 없게 될 수 있습니다.

관련 링크

- AWS 디렉터리 서비스란? AWS Directory Service 관리 가이드에서
- AWS Directory Service 관리 가이드에서 AWS 관리되는 Microsoft AD 디렉터리를 만드세요.
- AWS Directory Service 관리 안내서의 신뢰 관계 생성 시기.
- 연습 1: 시작을 위한 사전 조건.

Amazon VPC를 사용한 파일 시스템 액세스 제어

탄력적 네트워크 인터페이스를 통해 Amazon FSx 파일 시스템에 액세스합니다. 이 네트워크 인터페이스는 파일 시스템에 연결하는 Amazon Virtual Private Cloud(VPC) 서비스를 기반으로 하는 Virtual Private Cloud(VPC)에 있습니다. Domain Name Service(DNS) 이름을 통해 Amazon FSx 파일 시스템에 연결합니다. DNS 이름은 VPC의 파일 시스템 탄력적 네트워크 인터페이스의 프라이빗 IP 주소에 매

핑됩니다. 연결된 VPC 내의 리소스, AWS Direct Connect 또는 VPN을 통해 연결된 VPC와 연결된 리소스 또는 피어링된 VPC 내의 리소스만 파일 시스템의 네트워크 인터페이스에 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.

Windows File Server용 FSx는 VPC 공유를 지원합니다. VPC 공유를 사용하면 다른 계정이 소유한 VPC의 공유 서브넷에 있는 리소스를 보고, 만들고, 수정하고, 삭제할 수 있습니다. AWS 자세한 내용은 Amazon VPC 사용 설명서의 공유 VPC 작업을 참조하세요.

Amazon VPC 보안 그룹

VPC 내에서 파일 시스템의 탄력적 네트워크 인터페이스를 통과하는 네트워크 트래픽을 추가로 제어하려면 보안 그룹을 사용하여 파일 시스템에 대한 액세스를 제한합니다. 보안 그룹은 관련 네트워크 인터페이스로 들어오고 나가는 트래픽을 제어하는 상태 저장 방화벽입니다. 이 경우, 관련 리소스는 파일 시스템의 네트워크 인터페이스입니다.

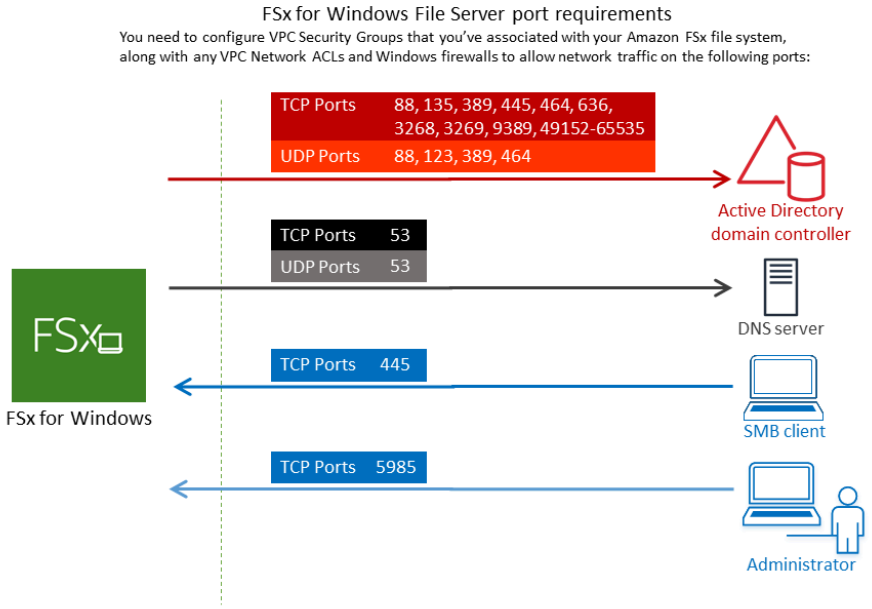
보안 그룹을 사용하여 Amazon FSx 파일 시스템에 대한 액세스를 제어하려면 인바운드 및 아웃바운드 규칙을 추가합니다. 인바운드 규칙은 들어오는 트래픽을 제어하고 아웃바운드 규칙은 파일 시스템에서 나가는 트래픽을 제어합니다. Amazon FSx 파일 시스템의 파일 공유를 지원되는 컴퓨팅 인스턴스의 폴더에 매핑하려면 보안 그룹에 올바른 네트워크 트래픽 규칙이 있는지 확인합니다.

보안 그룹 규칙에 대한 자세한 내용은 Amazon EC2 사용 설명서의 보안 그룹 규칙을 참조하십시오.

Amazon FSx에 대한 보안 그룹을 생성하는 방법

1. https://console.aws.amazon.com/ec2 에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 보안 그룹을 선택합니다.
3. 보안 그룹 생성을 선택합니다.
4. 보안 그룹의 이름과 설명을 지정합니다.
5. VPC의에서는 파일 시스템과 연결된 Amazon VPC를 선택하여 해당 VPC 내에 보안 그룹을 생성합니다.
6. 다음 포트에서 아웃바운드 네트워크 트래픽을 허용하려면 다음 규칙을 추가합니다.

a. VPC 보안 그룹의 경우 기본 Amazon VPC의 기본 보안 그룹이 콘솔의 파일 시스템에 이미 추가되었습니다. FSx 파일 시스템을 만드는 서브넷의 보안 그룹과 VPC 네트워크 ACL이 다음 다이어그램에 표시된 방향으로 포트를 통한 트래픽을 허용하는지 확인합니다.



다음 테이블에는 각 포트의 역할이 나와 있습니다.

프로토콜	포트	역할
TCP/UDP	53	도메인 이름 시스템(DNS)
TCP/UDP	88	Kerberos 인증
TCP/UDP	464	암호 변경/설정
TCP/UDP	389	LDAP(Lightweight Directory Access Protocol)
UDP	123	NTP(Network Time Protocol)
TCP	135	분산 컴퓨팅 환경/엔드포인트 매퍼(DCE/EPMAP)
TCP	445	디렉터리 서비스 SMB 파일 공유

프로토콜	포트	역할
TCP	636	Lightweight Directory Access Protocol over TLS/SSL(LDAPS)
TCP	3268	Microsoft 글로벌 카탈로그
TCP	3269	SSL을 통한 Microsoft 글로벌 카탈로그
TCP	5985	WinRM 2.0(Microsoft Windows Remote Management)
TCP	9389	마이크로소프트 AD DS 웹 서비스, PowerShell
TCP	49,152~65,535	RPC용 임시 포트

> **Important**
>
> 단일 AZ 2 및 모든 다중 AZ 파일 시스템 배포에는 TCP 포트 9389에서 아웃바운드 트래픽을 허용해야 합니다.

b. 이러한 트래픽 규칙이 각 AD 도메인 컨트롤러, DNS 서버 및 FSx 클라이언트, FSx 관리자에 적용되는 방화벽에도 반영되는지 확인합니다.

> **Important**
>
> Amazon VPC 보안 그룹에서는 네트워크 트래픽이 시작되는 방향으로만 포트를 열어야 하지만, 대부분의 Windows 방화벽과 VPC 네트워크 ACL에서는 포트가 양방향으로 열려 있어야 합니다.

> **Note**
>
> Microsoft Active Directory 사이트가 정의되어 있는 경우에는 Amazon FSx 파일 시스템과 연결된 VPC의 서브넷이 Microsoft Active Directory 사이트에 정의되어 있도록 하고 VPC의 서브넷과 다른 사이트의 서브넷 간에 충돌이 존재하지 않도록 해야 합니다. Active

Directory 사이트 및 서비스 MMC 스냅인을 사용하여 이러한 설정을 보고 변경할 수 있습니다.

> **Note**
>
> 경우에 따라 기본 설정에서 AWS Managed Microsoft AD 보안 그룹의 규칙을 수정할 수도 있습니다. 그렇다면 이 보안 그룹에 Amazon FSx 파일 시스템으로부터의 트래픽을 허용하는 데 필요한 인바운드 규칙이 있는지 확인합니다. 필수 인바운드 규칙에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 AWS Managed Microsoft AD 사전 요구 사항을 참조하세요.

이제 보안 그룹을 만들었으니 Amazon FSx 파일 시스템의 탄력적 네트워크 인터페이스와 연결할 수 있습니다.

Amazon FSx 파일 시스템과 보안 그룹의 연결

1. https://console.aws.amazon.com/fsx/에서 Amazon FSx 콘솔을 엽니다.
2. 대시보드에서 세부 정보를 보려면 파일 시스템을 선택합니다.
3. 네트워크 및 보안 탭을 선택하고 파일 시스템의 네트워크 인터페이스(예: ENI-01234567890123456)를 선택합니다. 단일 AZ 파일 시스템의 경우, 단일 네트워크 인터페이스 하나가 표시됩니다. 다중 AZ 파일 시스템의 경우, 기본 서브넷의 네트워크 인터페이스와 대기 서브넷의 네트워크 인터페이스가 각각 하나씩 표시됩니다.
4. 각 네트워크 인터페이스에 대해 네트워크 인터페이스를 선택하고 작업에서 보안 그룹 변경을 선택합니다.
5. 보안 그룹 변경 대화 상자에서 사용할 보안 그룹을 선택하고 저장을 선택합니다.

파일 시스템에 대한 액세스 허용 해제

모든 클라이언트에서 파일 시스템에 대한 네트워크 액세스에 대한 허용을 일시적으로 해제하려면 파일 시스템의 탄력적 네트워크 인터페이스와 연결된 모든 보안 그룹을 제거하고 인바운드 또는 아웃바운드 규칙이 없는 그룹으로 바꾸면 됩니다.

Amazon VPC 네트워크 ACL

VPC 내 파일 시스템에 대한 액세스를 보호하는 또 다른 방법은 네트워크 액세스 제어 목록(네트워크 ACL)을 설정하는 것입니다. 네트워크 ACL은 보안 그룹과는 별개이지만, VPC의 리소스에 추가 보안 계층을 추가하기 위한 비슷한 기능이 있습니다. 네트워크 ACL에 대한 자세한 내용은 Amazon VPC 사용 설명서의 네트워크 ACL을 참조하세요.

Amazon FSx for Windows File Server를 위한 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 은 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM 관리자는 어떤 사용자가 Amazon FSx 리소스를 사용할 수 있도록 인증(로그인)되고 권한이 부여(권한 있음)될 수 있는지 제어합니다. IAM은 추가 AWS 서비스 비용 없이 사용할 수 있습니다.

주제

고객

사용 방법 AWS Identity and Access Management (IAM) 은 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 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. Amazon FSx의 기능에 액세스할 수 없다면 Amazon FSx for Windows File Server를 위한 ID 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 IAM을 사용하는 방법에 대해 자세히 알아보려면 IAM과 함께 Amazon FSx for Windows File Server를 사용하는 방법 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 Windows File Server의 자격 증명 기반 정책 예제 섹션을 참조하세요.

보안 인증 정보를 통한 인증

인증은 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM 사용자로 인증 (로그인 AWS) 하거나 IAM 역할을 맡아 인증 (로그인) 해야 합니다. AWS 계정 루트 사용자

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAM ID 센터) 사용자, 회사의 싱글 사인온 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션형 ID로 로그인할 때 관리자가 이전에 IAM 역할을 사용하여 ID 페더레이션을 설정했습니다. 페더레이션을 사용하여 액세스하는 경우 AWS 간접적으로 역할을 맡게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 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 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS API 요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, AWS 계정의 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 것을 권장합니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 다중 인증 및 IAM 사용 설명서의 AWS에서 다중 인증(MFA) 사용을 참조하세요.

AWS 계정 루트 사용자

계정을 AWS 계정 만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않

을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 이를 사용하여 루트 사용자만 수행할 수 있는 작업을 수행하세요. 루트 사용자로 로그인해야 하는 태스크의 전체 목록은 IAM 사용자 안내서의 루트 사용자 보안 인증이 필요한 태스크를 참조하세요.

페더레이션 ID

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS Directory Service 페더레이션 ID에 AWS 계정 액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center을 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. AWS 계정 IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서에서 IAM Identity Center란 무엇입니까?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 사용자 또는 애플리케이션에 대한 특정 권한을 AWS 계정 가진 사용자 내 자격 증명입니다. 가능하다면 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신, 임시 보안 인증 정보를 사용하는 것이 좋습니다. 하지만 IAM 사용자의 장기 보안 인증 정보가 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 보안 인증입니다. 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 보안 인증을 가지고 있지만, 역할은 임시 자격 증명만 제공합니다. 자세한 정보는 IAM 사용 설명서의 IAM 사용자를 만들어야 하는 경우(역할이 아님)를 참조하세요.

IAM 역할

IAM 역할은 특정 권한을 가진 사용자 AWS 계정 내의 자격 증명입니다. IAM 사용자와 유사하지만, 특정 개인과 연결되지 않습니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역

할을 맡을 수 있습니다. AWS CLI 또는 AWS API 작업을 호출하거나 사용자 지정 URL을 사용하여 역할을 수임할 수 있습니다. 역할 사용 방법에 대한 자세한 정보는 IAM 사용 설명서의 IAM 역할 사용을 참조하세요.

임시 보안 인증이 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션형 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션형 ID가 인증되면 이 ID는 역할과 연결되며 역할에 의해 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 타사 자격 증명 공급자의 역할 만들기 부분을 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 아이덴티티가 액세스할 수 있는 항목을 통제하기 위해 IAM Identity Center는 권한 세트를 IAM의 역할과 연관짓습니다. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 IAM 역할을 맡아 특정 작업에 대한 다양한 권한을 임시로 받을 수 있습니다.
- 크로스 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 AWS 서비스 경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 크로스 계정 액세스를 위한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.
- 서비스 간 액세스 — 일부는 다른 AWS 서비스 기능을 AWS 서비스 사용합니다. 예를 들어 서비스에서 직접적으로 호출을 수행하면 일반적으로 해당 서비스는 Amazon EC2에서 애플리케이션을 실행하거나 Amazon S3에 객체를 저장합니다. 서비스는 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이를 수행할 수 있습니다.
  - 순방향 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 경우 보안 AWS 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 AWS 서비스 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 태스크를 수행하기 위해 맡는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하세요.
  - 서비스 연결 역할 — 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은

사용자에게 AWS 계정 표시되며 해당 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 API 요청을 AWS CLI 하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 생성합니다. 인스턴스 프로파일에는 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.

IAM 역할을 사용할지 또는 IAM 사용자를 사용할지를 알아보려면 IAM 사용 설명서의 IAM 역할(사용자 대신)을 생성하는 경우를 참조하세요.

정책을 사용한 액세스 관리

정책을 생성하고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되는지 또는 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 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, 사용자와 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 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 AWS API에서 역할 정보를 가져올 수 있습니다.

보안 인증 기반 정책

보안 인증 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 보안 인증에 연결할 수 있는 JSON 권한 정책 설명서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정 관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책과 인라인 정책의 선택을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예는 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 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. IAM의 AWS 관리형 정책은 리소스 기반 정책에 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 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ACL을 지원하는 서비스의 예로는 아마존 S3와 아마존 VPC가 있습니다. AWS WAF ACL에 대해 자세히 알아보려면 Amazon Simple Storage Service 개발자 안내서의 액세스 제어 목록(ACL) 개요를 참조하세요.

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 타입에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 – 권한 경계는 자격 증명 기반 정책에 따라 IAM 엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 엔터티에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 엔터티의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 보안 주체로 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 엔터티에 대한 권한 경계를 참조하세요.

- 서비스 제어 정책 (SCP) - SCP는 조직 또는 조직 단위 (OU) 에 대한 최대 권한을 지정하는 JSON 정책입니다. AWS Organizations AWS Organizations 사업체가 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직에서 모든 기능을 활성화할 경우 서비스 통제 정책(SCP)을 임의의 또는 모든 계정에 적용할 수 있습니다. SCP는 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 제한합니다. AWS 계정 루트 사용자 조직 및 SCP에 대한 자세한 정보는 AWS Organizations 사용 설명서의 SCP 작동 방식을 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 보안 인증 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 타입

여러 정책 타입이 요청에 적용되는 경우 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하십시오.

IAM과 함께 Amazon FSx for Windows File Server를 사용하는 방법

IAM을 사용하여 Amazon FSx에 대한 액세스를 관리하기 전에 Amazon FSx에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

IAM은 Amazon FSx for Windows File Server와 함께 사용할 수 있는 특성을 가지고 있습니다.

IAM 특성	FSx 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACL	아니요

IAM 특성	FSx 지원
ABAC(정책의 태그)	예
임시 보안 인증	예
포워드 액세스 세션	예
서비스 역할	아니요
서비스 링크 역할	예

FSx 및 AWS 기타 서비스가 대부분의 IAM 기능과 어떻게 작동하는지 자세히 알아보려면 IAM 사용 설명서의 IAM과 함께 작동하는 서비스를 AWS 참조하십시오.

FSx에 대한 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 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성을 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. ID 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용하는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

FSx에 대한 자격 증명 기반 정책 예제

Amazon FSx 자격 증명 기반 정책 예제를 보려면 Amazon FSx for Windows File Server의 자격 증명 기반 정책 예제 섹션을 참조하세요.

FSx 내 리소스 기반 정책

리소스 기반 정책 지원	아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예는 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 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

크로스 계정 액세스를 활성화하려는 경우 전체 계정이나 다른 계정의 IAM 엔터티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 신뢰 관계 설정의 절반밖에 되지 않는다는 것을 유념하세요. 보안 주체와 리소스가 다른 AWS 계정 경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 개체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스 권한을 부여하는 경우 추가 ID 기반 정책이 필요하지 않습니다. 자세한 정보는 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

FSx 정책 작업

정책 작업 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.

JSON 정책의 `Action` 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 API 작업이 없는 권한 전용 작업 같은 몇 가지 예외도 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

FSx 작업 목록을 보려면 서비스 승인 참조의 Amazon FSx for Windows File Server에서 정의한 작업을 참조하세요.

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 Windows File Server의 자격 증명 기반 정책 예제 섹션을 참조하세요.

FSx 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. 명령문에는 `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 이 작업을 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 FSx for Windows File Server에서 정의한 리소스를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면 Amazon FSx for Windows File Server에서 정의한 작업을 참조하세요.

Amazon FSx 자격 증명 기반 정책 예제를 보려면 Amazon FSx for Windows File Server의 자격 증명 기반 정책 예제 섹션을 참조하세요.

FSx 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. 같음이나 미만 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 은(는) 논리적 `AND` 작업을 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명령문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리표시자 변수를 사용할 수도 있습니다. 예를 들어, IAM 사용자에게 IAM 사용자 이름으로 태그가 지정된 경우에만 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하세요.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM 사용 AWS 설명서의 글로벌 조건 컨텍스트 키를 참조하십시오.

FSx 조건 키 목록을 보려면 서비스 승인 참조의 Amazon FSx for Windows File Server에 사용되는 조건 키를 참조하세요. 조건 키를 사용할 수 있는 작업과 리소스를 알아보려면 Amazon FSx for Windows File Server에서 정의한 작업을 참조하세요.

Amazon FSx 자격 증명 기반 정책 예제를 보려면 Amazon FSx for Windows File Server의 자격 증명 기반 정책 예제 섹션을 참조하세요.

FSx의 ACL

ACL 지원	아니요

액세스 제어 목록(ACL)은 리소스에 액세스할 권한이 있는 보안 주체(계정 구성원, 사용자 또는 역할)를 제어합니다. ACL은 JSON 정책 설명서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

ABAC을 통한 FSx

ABAC 지원(정책의 태그)	예

ABAC(속성 기반 액세스 제어)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM 개체 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. ABAC의 첫 번째 단계로 엔터티 및 리소스에 태그를 지정합니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로운 상황에 도움이 됩니다.

태그를 기반으로 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 정보는 IAM 사용 설명서의 ABAC란 무엇인가요?를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 ABAC(속성 기반 액세스 제어) 사용을 참조하세요.

FSx에서 임시 자격 증명 사용

임시 보안 인증 지원	예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 방법을 AWS 서비스 비롯한 추가 정보는 IAM 사용 설명서의 IAM과 AWS 서비스 연동되는 내용을 참조하십시오.

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하면 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 SSO (Single Sign-On) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 정보는 IAM 사용 설명서의 역할로 전환(콘솔)을 참조하세요.

또는 API를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS CLI . AWS 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS 있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 정보는 IAM의 임시 보안 보안 인증 섹션을 참조하세요.

FSx용 포워드 액세스 세션

전달 액세스 세션(FAS) 지원	예

IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS 경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS는 전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS 요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

FSx에 대한 서비스 역할

서비스 역할 지원	아니요

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 IAM role(IAM 역할)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 역할을 생성하여 AWS 서비스에게 권한 위임을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 FSx 기능이 중단될 수 있습니다. FSx에서 관련 지침을 제공하는 경우에만 서비스 역할을 편집하세요.

FSx에 대한 서비스 연결 역할

서비스 링크 역할 지원	예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. AWS 서비스 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 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 Windows File Server의 자격 증명 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 생성을 참조하세요.

각 리소스 유형에 대한 ARN 형식을 포함하여 FSx에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 인증 참조에서 Amazon FSx for Windows File Server에 대한 작업, 리소스 및 조건 키를 참조하세요.

주제

- 정책 모범 사례
- 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. 자격 증명 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책으로 시작하고 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 에서 사용할 수 있습니다. AWS 계정 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 정보는 IAM 사용 설명서의 AWS managed policies(관리형 정책) 또는 AWS managed policies for job functions(직무에 대한 관리형 정책)를 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 태스크를 설정하는 경우 태스크를 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 least-privilege permissions(최소 권한)으로 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.
- Use conditions in IAM policies to further restrict access(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 정책 조건을 생성할 수 있습니다. 예를 AWS 서비스 들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation 있습니다. 자세한 정보는 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.

- IAM Access Analyzer를 통해 IAM 정책을 검증하여 안전하고 기능적인 권한 보장 – IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 신규 및 기존 정책을 검증합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 권장 사항을 제공하여 안전하고 기능적인 정책을 생성하도록 돕습니다. 자세한 정보는 IAM 사용 설명서의 IAM Access Analyzer 정책 검증을 참조하세요.
- 멀티 팩터 인증 (MFA) 필요 - IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 AWS 계정 MFA를 활성화하십시오. API 작업을 호출할 때 MFA를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 정보는 IAM 사용 설명서의 Configuring MFA-protected API access(MFA 보호 API 액세스 구성)를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

FSx 콘솔 사용

Amazon FSx for Windows File Server 콘솔에 액세스하려면 최소한의 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 Amazon FSx 리소스를 나열하고 세부 정보를 볼 수 있어야 합니다. AWS 계정 최소 필수 권한보다 더 제한적인 ID 기반 정책을 만들면 콘솔이 해당 정책에 연결된 개체(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 API만 호출하는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다. AWS 그 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 FSx 콘솔을 계속 사용할 수 있도록 하려면 FSx 관리형 정책도 `AmazonFSxConsoleReadOnlyAccess` AWS 엔티티에 연결하십시오. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예는 IAM 사용자가 자신의 사용자 보안 인증에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 API를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함됩니다. AWS CLI AWS

```
{
    "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": "*"
        }
    ]
}
```

AWS 아마존 FSx에 대한 관리형 정책

AWS 관리형 정책은 에서 생성하고 관리하는 독립형 정책입니다. AWS AWS 관리형 정책은 많은 일반 사용 사례에 대한 권한을 제공하도록 설계되었으므로 사용자, 그룹 및 역할에 권한을 할당하기 시작할 수 있습니다.

AWS 관리형 정책은 모든 AWS 고객이 사용할 수 있으므로 특정 사용 사례에 대해 최소 권한 권한을 부여하지 않을 수도 있다는 점에 유의하세요. 사용 사례에 고유한 고객 관리형 정책을 정의하여 권한을 줄이는 것이 좋습니다.

관리형 정책에 정의된 권한은 변경할 수 없습니다. AWS AWS 관리형 정책에 정의된 권한을 업데이트하는 경우 AWS 해당 업데이트는 정책이 연결된 모든 주체 ID (사용자, 그룹, 역할) 에 영향을 미칩니다. AWS 새 API 작업이 시작되거나 기존 서비스에 새 AWS 서비스 API 작업을 사용할 수 있게 되면 AWS 관리형 정책을 업데이트할 가능성이 가장 높습니다.

자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책을 참조하십시오.

AmazonF SxServiceRolePolicy

Amazon FSx가 사용자를 대신하여 리소스를 AWS 관리할 수 있도록 허용합니다. 자세한 내용은 Amazon FSx에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

AWS 관리형 정책: AmazonF SxDeleteServiceLinkedRoleAccess

`AmazonFSxDeleteServiceLinkedRoleAccess`를 IAM 엔터티에 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 설명은 Amazon FSx에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

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 정책에 대한 권한을 보려면 AWS 관리형 정책 참조 SxDeleteServiceLinkedRoleAccess 가이드의 AmazonF를 참조하십시오.

AWS 관리형 정책: AmazonF SxFullAccess

Amazon F를 IAM SxFullAccess 엔티티에 연결할 수 있습니다. Amazon FSx는 사용자를 대신하여 Amazon FSx가 작업을 수행할 수 있도록 허용하는 서비스 역할에도 이 정책을 연결합니다.

Amazon FSx에 대한 전체 액세스 권한 및 관련 서비스에 대한 액세스를 제공합니다. AWS

권한 세부 정보

이 정책에는 다음 권한이 포함되어 있습니다.

- `fsx` - 보안 주체가 `BypassSnaplockEnterpriseRetention`을 제외한 모든 Amazon FSx 작업을 수행할 수 있습니다.
- `ds`— 주도자가 디렉터리에 대한 정보를 볼 수 있습니다. AWS Directory Service
- `ec2`

  - 주도자가 지정된 조건에서 태그를 생성할 수 있습니다.
  - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대한 향상된 보안 그룹 검증을 제공합니다.
- `iam` - 보안 주체가 사용자를 대신하여 Amazon FSx 서비스 연결 역할을 생성할 수 있습니다. 이는 Amazon FSx가 사용자를 대신하여 리소스를 AWS 관리할 수 있도록 하기 위해 필요합니다.
- `logs` - 보안 주체가 로그 그룹, 로그 스트림을 생성하고, 로그 스트림에 이벤트를 기록할 수 있습니다. 이는 사용자가 감사 액세스 로그를 로그로 전송하여 FSx for Windows File Server 파일 시스템 액세스를 모니터링할 수 있도록 하기 위해 필요합니다. CloudWatch
- `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.

이 정책에 대한 권한을 보려면 관리형 정책 참조 SxFullAccess 가이드의 AWS AmazonF를 참조하십시오.

AWS 관리형 정책: AmazonF SxConsoleFullAccess

`AmazonFSxConsoleFullAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Amazon FSx에 대한 전체 액세스 및 를 통한 AWS 관련 서비스 액세스를 허용하는 관리자 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 디렉터리에 대한 정보를 나열할 수 있습니다. AWS Directory Service
- `ec2`
  - 보안 주체가 라우팅 테이블에 태그를 생성하고, 네트워크 인터페이스, 라우팅 테이블, 보안 그룹, 서브넷 및 Amazon FSx 파일 시스템과 연결된 VPC를 나열할 수 있습니다.
  - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대한 향상된 보안 그룹 검증을 제공합니다.
- `kms`— 보안 주체가 키의 별칭을 나열할 수 있도록 허용합니다. AWS Key Management Service

- `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 정책에 대한 권한을 보려면 관리형 정책 참조 안내서의 AmazonF를 SxConsoleFullAccess 참조하십시오. AWS

AWS 관리형 정책: AmazonF SxConsoleReadOnlyAccess

`AmazonFSxConsoleReadOnlyAccess` 정책을 IAM 보안 인증에 연결할 수 있습니다.

이 정책은 Amazon FSx 및 AWS 관련 서비스에 읽기 전용 권한을 부여하여 사용자가 에서 이러한 서비스에 대한 정보를 볼 수 있도록 합니다. 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 관리 콘솔의 AWS Directory Service 디렉터리에 대한 정보를 볼 수 있습니다.
- `ec2`
  - 보안 주체가 Amazon FSx 관리 콘솔에서 Amazon FSx 파일 시스템과 연결된 네트워크 인터페이스, 보안 그룹, 서브넷 및 VPC를 볼 수 있습니다.
  - VPC와 함께 사용할 수 있는 모든 보안 그룹에 대한 향상된 보안 그룹 검증을 제공합니다.
- `kms`— 보안 주체가 Amazon FSx 관리 콘솔에서 AWS Key Management Service 키의 별칭을 볼 수 있습니다.
- `log`— 보안 주체가 요청한 계정과 관련된 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`— 주체가 요청하는 계정과 관련된 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 정책에 대한 권한을 보려면 관리형 정책 참조 SxConsoleReadOnlyAccess 가이드의 AWS AmazonF를 참조하십시오.

AWS 관리형 정책: AmazonF SxReadOnlyAccess

`AmazonFSxReadOnlyAccess` 정책을 IAM 자격 증명에 연결할 수 있습니다.

이 정책은 Amazon FSx에 대한 읽기 전용 액세스를 허용하는 권한을 부여합니다.

- `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 대한 향상된 보안 그룹 검증을 제공합니다.

이 정책에 대한 권한을 보려면 AWS 관리형 정책 참조 SxReadOnlyAccess 가이드의 AmazonF를 참조하십시오.

관리형 정책에 대한 Amazon FSx 업데이트 AWS

이 서비스가 변경 사항을 추적하기 시작한 이후 Amazon FSx의 AWS 관리형 정책 업데이트에 대한 세부 정보를 확인하십시오. 이 페이지의 변경 사항에 대한 자동 알림을 받아보려면 Amazon FSx 문서 이력 페이지에서 RSS 피드를 구독하세요.

변경 사항	설명	날짜
AmazonF SxServiceRolePolicy — 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있는 새로운 권한을 `ec2:GetSecurityGroupsForVpc` 추가했습니다.	2024년 1월 9일
AmazonF — 기존 정책에 SxReadOnlyAccess 대한 업데이트	Amazon FSx는 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있는 새로운 권한을 `ec2:GetSe`	2024년 1월 9일

변경 사항	설명	날짜
	curityGroupsForVpc 추가했습니다.	
AmazonF — 기존 정책에 SxConsoleReadOnlyAccess 대한 업데이트	Amazon FSx는 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있는 새로운 권한을 ec2:GetSecurityGroupsForVpc 추가했습니다.	2024년 1월 9일
AmazonF — 기존 정책에 SxFullAccess 대한 업데이트	Amazon FSx는 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있는 새로운 권한을 ec2:GetSecurityGroupsForVpc 추가했습니다.	2024년 1월 9일
AmazonF — 기존 정책에 SxConsoleFullAccess 대한 업데이트	Amazon FSx는 보안 주체가 VPC와 함께 사용할 수 있는 모든 보안 그룹에 대해 향상된 보안 그룹 검증을 제공할 수 있는 새로운 권한을 ec2:GetSecurityGroupsForVpc 추가했습니다.	2024년 1월 9일
AmazonF — 기존 정책에 SxFullAccess 대한 업데이트	Amazon FSx는 사용자가 OpenZFS용 FSX에 대해 지역 간 및 계정 간 데이터 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 12월 20일

변경 사항	설명	날짜
SxConsoleFullAccesssAmazonF — 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 OpenZFS용 FSX에 대해 지역 간 및 계정 간 데이터 복제를 수행할 수 있는 새로운 권한을 추가했습니다.	2023년 12월 20일
SxFullAccessAmazonF — 기존 정책에 대한 업데이트	Amazon FSx는 사용자가 OpenZFS 파일 시스템용 FSX용 볼륨의 온디맨드 복제를 수행할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 11월 26일
AmazonF — 기존 정책에 대한 업데이트 SxConsoleFullAccess	Amazon FSx는 사용자가 OpenZFS 파일 시스템용 FSX용 볼륨의 온디맨드 복제를 수행할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 11월 26일
AmazonF — 기존 정책에 대한 업데이트 SxFullAccess	Amazon FSx는 사용자가 ONTAP 다중 AZ 파일 시스템용 FSx에 대한 공유 VPC 지원을 보고, 활성화하고, 비활성화할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 11월 14일
AmazonF — 기존 정책에 대한 업데이트 SxConsoleFullAccess	Amazon FSx는 사용자가 ONTAP 다중 AZ 파일 시스템용 FSx에 대한 공유 VPC 지원을 보고, 활성화하고, 비활성화할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 11월 14일

변경 사항	설명	날짜
AmazonF — 기존 정책에 대한 업데이트 SxFullAccess	Amazon FSx가 FSx for OpenZFS 다중 AZ 파일 시스템의 네트워크 구성을 관리할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 8월 9일
AWS 관리형 정책: AmazonF SxServiceRolePolicy — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 네임스페이스에 지표를 게시하도록 `cloudwatch:PutMetricData` 기존 권한을 수정했습니다. CloudWatch `AWS/FSx`	2023년 7월 24일
AmazonF — 기존 정책에 대한 업데이트 SxFullAccess	Amazon FSx의 `fsx:*` 권한을 제거하고 특정 `fsx` 작업을 추가하도록 정책을 업데이트했습니다.	2023년 7월 13일
AmazonF SxConsole FullAccess — 기존 정책에 대한 업데이트	Amazon FSx의 `fsx:*` 권한을 제거하고 특정 `fsx` 작업을 추가하도록 정책을 업데이트했습니다.	2023년 7월 13일
AmazonF SxFullAccess — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 FSx for OpenZFS 다중 AZ 파일 시스템의 네트워크 구성을 관리할 수 있도록 하는 새로운 권한을 추가했습니다.	2023년 5월 31일
AmazonF SxConsole ReadOnlyAccess — 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

변경 사항	설명	날짜
AmazonF SxConsole FullAccess — 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
AmazonF — 정책 추적 시작 SxReadOnlyAccess	이 정책은 모든 Amazon FSx 리소스 및 이와 관련된 모든 태그에 대한 읽기 전용 액세스 권한을 부여합니다.	2022년 2월 4일
AmazonF — 추적 정책 시작 SxDeleteServiceLinkedRoleAccess	이 정책은 Amazon FSx가 Amazon S3 액세스에 대한 서비스 연결 역할을 삭제할 수 있도록 허용하는 관리자 권한을 부여합니다.	2022년 1월 7일
AmazonF SxServiceRolePolicy — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 ONTAP 파일 시스템용 Amazon FSx의 네트워크 구성을 관리할 수 있도록 하는 새로운 권한을 추가했습니다. NetApp	2021년 9월 2일
AmazonF — 기존 정책에 대한 업데이트 SxFullAccess	Amazon FSx가 EC2 라우팅 테이블에서 범위를 좁힌 호출에 대한 태그를 생성할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일
AmazonF SxConsole FullAccess — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 ONTAP 다중 AZ 파일 시스템용 Amazon FSx를 생성할 수 있도록 하는 새로운 권한을 추가했습니다. NetApp	2021년 9월 2일

변경 사항	설명	날짜
SxConsoleFullAcces sAmazonF — 기존 정책에 대한 업데이트	Amazon FSx가 EC2 라우팅 테이블에서 범위를 좁힌 호출에 대한 태그를 생성할 수 있도록 하는 새로운 권한을 추가했습니다.	2021년 9월 2일
AmazonF SxServiceRolePolicy — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 로그 로그 스트림을 설명하고 이에 쓸 수 있도록 새 권한을 추가했습니다. CloudWatch 이는 사용자가 로그를 사용하여 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다. CloudWatch	2021년 6월 8일
AmazonF SxServiceRolePolicy — 기존 정책에 대한 업데이트	Amazon FSx는 Amazon FSx가 Amazon Data Firehose 전송 스트림을 설명하고 이에 쓸 수 있도록 새 권한을 추가했습니다. 이는 사용자가 Amazon Data Firehose를 사용하여 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonF SxFullAccess — 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 로그 로그 그룹, 로그 스트림을 설명하고 CloudWatch 생성하고 로그 스트림에 이벤트를 쓸 수 있도록 하는 새로운 권한을 추가했습니다. 이는 주도자가 로그를 사용하여 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다. CloudWatch	2021년 6월 8일
AmazonF — 기존 정책에 대한 업데이트 SxFullAccess	Amazon FSx는 보안 주체가 Amazon Data Firehose에 레코드를 설명하고 기록할 수 있는 새로운 권한을 추가했습니다. 이는 사용자가 Amazon Data Firehose를 사용하여 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 볼 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonF SxConsole FullAccess — 기존 정책에 대한 업데이트	Amazon FSx는 보안 주체가 요청한 계정과 관련된 CloudWatch Amazon Logs 로그 그룹을 설명할 수 있는 새로운 권한을 추가했습니다. 이는 주도자가 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사를 구성할 때 기존 CloudWatch 로그 로그 그룹을 선택할 수 있도록 하기 위해 필요합니다.	2021년 6월 8일
AmazonF — 기존 정책에 SxConsoleFullAccess 대한 업데이트	Amazon FSx는 보안 주체가 요청한 계정과 관련된 Amazon Data Firehose 전송 스트림을 설명할 수 있는 새로운 권한을 추가했습니다. 이는 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사를 구성할 때 보안 주체가 기존 Firehose 전송 스트림을 선택할 수 있도록 하기 위해 필요합니다.	2021년 6월 8일

변경 사항	설명	날짜
AmazonF — 기존 정책에 대한 업데이트 SxConsole ReadOnlyAccess	Amazon FSx는 보안 주체가 요청한 계정과 관련된 CloudWatch Amazon Logs 로그 그룹을 설명할 수 있는 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
AmazonF — 기존 정책에 대한 업데이트 SxConsole ReadOnlyAccess	Amazon FSx는 보안 주체가 요청한 계정과 관련된 Amazon Data Firehose 전송 스트림을 설명할 수 있는 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 관리형 정책의 변경 사항을 추적하기 시작했습니다. AWS	2021년 6월 8일

Amazon FSx for Windows File Server를 위한 ID 및 액세스 문제 해결

다음 정보를 사용하여 Amazon FSx 및 IAM으로 작업할 때 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- FSx에서 작업을 수행할 권한이 없음

- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 FSx 리소스에 액세스할 AWS 계정 수 있도록 허용하고 싶습니다.

FSx에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 수신되면, 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 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 보안 인증을 제공한 사용자입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

iam:PassRole 작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 Amazon FSx에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 서비스에서는 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 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 보안 인증을 제공한 사용자입니다.

외부 사용자가 내 FSx 리소스에 액세스할 AWS 계정 수 있도록 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 제어 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 IAM과 함께 Amazon FSx for Windows File Server를 사용하는 방법 섹션을 참조하세요.
- 소유하고 AWS 계정 있는 모든 리소스에 대한 액세스를 제공하는 방법을 알아보려면 IAM 사용 설명서의 다른 AWS 계정 IAM 사용자에게 액세스 권한 제공을 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사 AWS 계정AWS 계정 소유에 대한 액세스 제공을 참조하십시오.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스를 위한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM 역할과 리소스 기반 정책의 차이를 참조하세요.

Amazon FSx에서 태그 사용

태그를 사용하여 Amazon FSx 리소스에 대한 액세스를 제어하고 속성 기반 액세스 제어(ABAC)를 구현할 수 있습니다. 생성 중에 Amazon FSx 리소스에 태그를 적용하려면 사용자에게 특정 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. 리소스 태그를 사용하여 속성 기반 액세스 제어(ABAC)를 구현할 수도 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS의 ABAC란?을 참조하세요.

사용자가 생성 시 리소스에 태그를 지정할 수 있으려면 리소스를 생성하는 작업을 사용할 권한이 있어야 합니다(예: `fsx:CreateFileSystem` 또는 `fsx:CreateBackup`). 리소스 생성 작업에서 태그가 지정되면 Amazon은 `fsx:TagResource` 작업에서 추가 권한 부여를 수행해 사용자에게 태그를 생성할 권한이 있는지 확인합니다. 따라서 사용자는 `fsx:TagResource` 작업을 사용할 명시적 권한도 가지고 있어야 합니다.

다음 예는 사용자가 특정 시스템에서 파일 시스템을 생성하고 파일 시스템을 생성하는 동안 파일 시스템에 태그를 적용할 수 있도록 허용하는 정책을 보여줍니다. AWS 계정

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
         "fsx:CreateFileSystem",
         "fsx:TagResource"
      ],
      "Resource": "arn:aws:fsx:region:account-id:file-system/*"
    }
  ]
}
```

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 사용하

여 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 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 제어하기 위해 태그를 기반으로 하는 (IAM) AWS Identity and Access Management 정책을 사용할 수 있습니다. 두 가지 방법으로 제어할 수 있습니다.

1. Amazon FSx 리소스의 태그를 기반으로 해당 리소스에 대한 액세스를 제어합니다.
2. IAM 요청 조건에 어떤 태그가 전달될 수 있는지를 제어합니다.

태그를 사용하여 AWS 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 태그를 사용한 액세스 제어를 참조하십시오. 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 있는지 제어하기 위해 해당 리소스의 태그를 사용할 수 있습니다. 예를 들어, 리소스에 있는 태그의 키-값 페어를 기반으로 해당 리소스에서 특정 API 작업을 허용하거나 거부할 수 있습니다.

Example 정책 - 특정 태그를 제공하는 경우에 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 정책 - 특정 태그가 있는 Amazon FSx 파일 시스템의 백업만 생성

이 정책을 통해 사용자는 key=Department, value=Finance 키 값 쌍으로 태그가 지정된 파일 시스템의 백업만 생성할 수 있으며, 백업은 Deparment=Finance 태그를 사용하여 생성됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateBackup"
            ],
            "Resource": "arn:aws:fsx:region:account-id:file-system/*",
            "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 정책 - 특정 태그가 있는 백업에서 특정 태그가 포함된 파일 시스템 생성

이 정책을 통해 사용자는 Department=Finance 태그가 지정된 백업에서만 Department=Finance 태그가 지정된 파일 시스템을 생성할 수 있습니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "fsx:CreateFileSystemFromBackup",
                "fsx:TagResource"
            ],
            "Resource": "arn:aws:fsx:region:account-id:backup/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/Department": "Finance"
                }
            }
        }
    ]
}
```

Example 정책 - 특정 태그가 있는 파일 시스템 삭제

이 정책을 통해 사용자는 Department=Finance 태그가 지정된 파일 시스템만 삭제할 수 있습니다. 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"
                }
            }
        }
    ]
}
```

Amazon FSx에 대해 서비스 연결 역할 사용

Windows용 Amazon FSx 파일 AWS Identity and Access Management 서버는 (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 서비스를 호출하는 데 필요한 모든 권한을 포함합니다. AWS

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 엔터티에 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 작업하는 AWS 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 `AWSServiceRoleForAmazonFSx`라는 서비스 연결 역할을 사용합니다. 이 역할은 VPC의 파일 시스템을 위한 탄력적 네트워크 인터페이스를 생성합니다.

역할 권한 정책에 따라 Amazon FSx는 모든 해당 리소스에 대해 다음 작업을 완료할 수 있습니다. AWS

AmazonF를 IAM SxServiceRolePolicy 엔티티에 연결할 수 없습니다. 이 정책은 FSx가 사용자를 대신하여 리소스를 관리할 수 있도록 하는 서비스 연결 역할에 연결됩니다. AWS 자세한 설명은 Amazon FSx에 대해 서비스 연결 역할 사용 섹션을 참조하세요.

이 정책에 대한 업데이트는 다음을 참조하십시오. AmazonF SxServiceRolePolicy

이 정책은 FSx가 사용자를 대신하여 리소스를 AWS 관리할 수 있는 관리자 권한을 부여합니다.

권한 세부 정보

AmazonF SxServiceRolePolicy 역할 권한은 AmazonF 관리형 정책에 의해 정의됩니다. SxServiceRolePolicy AWS SxServiceRolePolicy AmazonF에는 다음과 같은 권한이 있습니다.

> **Note**
>
> SxServiceRolePolicy AmazonF는 모든 Amazon FSx 파일 시스템 유형에서 사용됩니다. 나열된 권한 중 일부는 Windows용 FSx에 적용되지 않을 수 있습니다.

- ds— FSx가 디렉토리의 응용 프로그램을 보고, 승인하고, 권한 부여를 취소할 수 있습니다. AWS Directory Service
- ec2 - FSx 에서 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 대한 향상된 보안 그룹 검증을 제공합니다.
  - 권한이 AWS 부여된 사용자가 네트워크 인터페이스에서 특정 작업을 수행할 수 있는 권한을 생성합니다.
- cloudwatch— FSx가 /FSx 네임스페이스 아래에 AWS 메트릭 데이터 포인트를 CloudWatch 게시할 수 있습니다.
- route53 - FSx에서 Amazon VPC를 프라이빗 호스팅 영역과 연결할 수 있도록 허용합니다.
- logs— FSx가 로그 로그 스트림을 설명하고 쓸 수 CloudWatch 있도록 합니다. 이는 사용자가 Windows File Server용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 로그 스트림으로 보낼 수 있도록 CloudWatch 하기 위한 것입니다.

- `firehose`— FSx가 Amazon Data Firehose 전송 스트림을 설명하고 이에 쓸 수 있도록 허용합니다. 이를 통해 사용자는 Windows용 FSx 파일 시스템에 대한 파일 액세스 감사 로그를 Amazon Data Firehose 전송 스트림에 게시할 수 있습니다.

```
{
    "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"
                }
            }
        },
        {
            "Sid": "PutCloudWatchLogs",
            "Effect": "Allow",
            "Action": [
                "logs:DescribeLogGroups",
                "logs:DescribeLogStreams",
                "logs:PutLogEvents"
            ],
            "Resource": "arn:aws:logs:*:*:log-group:/aws/fsx/*"
        },
        {
            "Sid": "ManageAuditLogs",
            "Effect": "Allow",
            "Action": [
                "firehose:DescribeDeliveryStream",
                "firehose:PutRecord",
                "firehose:PutRecordBatch"
            ],
            "Resource": "arn:aws:firehose:*:*:deliverystream/aws-fsx-*"
        }
    ]
}
```

이 정책에 대한 모든 업데이트는 관리형 정책에 대한 Amazon FSx 업데이트 AWS에 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 링크 역할 권한을 참조하세요.

Amazon FSx에 대한 서비스 연결 역할 생성

서비스 링크 역할은 수동으로 생성할 필요가 없습니다. IAM CLI 또는 IAM API에서 파일 시스템을 생성하면 Amazon FSx가 서비스 연결 역할을 자동으로 생성합니다. AWS Management Console

> **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 FSx에서는 서비스 연결 역할을 편집하도록 허용하지 않습니다. 서비스 링크 역할을 생성한 후에는 다양한 개체가 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 없어야 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 링크 역할을 삭제하려면

IAM 콘솔, IAM CLI 또는 IAM API를 사용하여 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 참조하십시오.

Amazon FSx for Windows File Server의 규정 준수 확인

특정 규정 준수 프로그램의 범위 내에 AWS 서비스 있는지 알아보려면AWS 서비스 규정 준수 프로그램의AWS 서비스 범위별, 규정 참조하여 관심 있는 규정 준수 프로그램을 선택하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

사용 시 규정 준수 AWS 서비스 책임은 데이터의 민감도, 회사의 규정 준수 목표, 관련 법률 및 규정에 따라 결정됩니다. AWS 규정 준수에 도움이 되는 다음 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 AWS 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- Amazon Web Services의 HIPAA 보안 및 규정 준수를 위한 설계 — 이 백서에서는 기업이 HIPAA 적격 애플리케이션을 만드는 AWS 데 사용할 수 있는 방법을 설명합니다.

  > **Note**
  >
  > 모든 AWS 서비스 사람이 HIPAA 자격을 갖춘 것은 아닙니다. 자세한 내용은 HIPAA 적격 서비스 참조를 참조하십시오.

- AWS 규정 준수 리소스AWS — 이 워크북 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS 고객 규정 준수 가이드 — 규정 준수의 관점에서 공동 책임 모델을 이해하십시오. 이 가이드에서는 보안을 유지하기 위한 모범 사례를 AWS 서비스 요약하고 여러 프레임워크 (미국 표준 기술 연구소 (NIST), 결제 카드 산업 보안 표준 위원회 (PCI), 국제 표준화기구 (ISO) 등) 에서 보안 제어에 대한 지침을 매핑합니다.
- 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— 이를 AWS 서비스 통해 내부 AWS보안 상태를 포괄적으로 파악할 수 있습니다. Security Hub는 보안 제어를 사용하여 AWS 리소스를 평가하고 보안 업계 표준 및 모범 사례에

대한 규정 준수를 확인합니다. 지원되는 서비스 및 제어 목록은 Security Hub 제어 참조를 참조하십시오.

- Amazon GuardDuty — 환경에 의심스럽고 악의적인 활동이 있는지 AWS 계정모니터링하여 워크로드, 컨테이너 및 데이터에 대한 잠재적 위협을 AWS 서비스 탐지합니다. GuardDuty 특정 규정 준수 프레임워크에서 요구하는 침입 탐지 요구 사항을 충족하여 PCI DSS와 같은 다양한 규정 준수 요구 사항을 해결하는 데 도움이 될 수 있습니다.
- AWS Audit Manager— 이를 AWS 서비스 통해 AWS 사용량을 지속적으로 감사하여 위험을 관리하고 규정 및 업계 표준을 준수하는 방법을 단순화할 수 있습니다.

Amazon FSx for Windows File Server 및 인터페이스 VPC 엔드포인트

인터페이스 VPC 엔드포인트를 사용하도록 Amazon FSx를 구성하여 VPC의 보안 상태를 향상시킬 수 있습니다. 인터페이스 VPC 엔드포인트는 인터넷 게이트웨이, NAT 디바이스, VPN 연결 또는 AWS Direct Connect 연결 없이 비공개로 Amazon FSx API에 액세스할 수 있도록 지원하는 AWS PrivateLink 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 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 File Server 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. VPC는 두 개의 서로 다른 AWS 리전에 있을 수도 있습니다.

피어링된 VPC 간의 트래픽은 AWS 네트워크에 유지되며 공용 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(AWS CLI)를 사용하여 Amazon FSx API에 대한 VPC 엔드포인트를 생성할 수 있습니다. 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.

중국의 AWS 리전을 제외하고, 엔드포인트에 프라이빗 DNS를 활성화한 경우 AWS 리전에 대한 기본 DNS 이름(예:`fsx.us-east-1.amazonaws.com`)을 사용하여 VPC 엔드포인트를 통해 Amazon FSx에 API 요청을 수행할 수 있습니다. 중국(베이징) 및 중국(닝샤) AWS 리전의 경우 각각 `fsx-api.cn-north-1.amazonaws.com.cn` 및 `fsx-api.cn-northwest-1.amazonaws.com.cn`을 사용하여 VPC 엔드포인트를 통해 API 요청을 수행할 수 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 추가로 제어하기 위해 VPC 엔드포인트에 AWS Identity and Access Management(IAM) 정책을 선택적으로 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.

할당량

다음에서는 Amazon FSx for Windows File Server 작업 시 할당량에 대해 알아봅니다.

주제

늘릴 수 있는 할당량

다음은 AWS 리전별로 각 AWS 계정에 대해 늘릴 수 있는 Amazon FSx for Windows File Server의 할당량입니다.

Resource	기본값	설명
Windows 파일 시스템	100	이 계정에서 생성할 수 있는 Amazon FSx for Windows Server 파일 시스템의 최대 수입니다.
Windows 처리량 용량	10240	이 계정의 모든 Amazon FSx for Windows 파일 시스템에 허용된 총 처리량 용량(MBps)입니다.
Windows HDD 스토리지 용량	524288	이 계정의 모든 Amazon FSx for Windows File Server 파일 시스템에 허용된 최대 HDD 스토리지 용량(GiB)입니다.
Windows SSD 스토리지 용량	524288	이 계정의 모든 Amazon FSx for Windows File Server 파일 시스템에 허용된 최대 SSD 스토리지 용량(GiB)입니다.

Resource	기본값	설명
Windows 총 SSD IOPS	500,000	이 계정의 모든 Amazon FSx for Windows File Server 파일 시스템에 허용된 총 SSD IOPS 양입니다.
Windows 백업	500	이 계정에서 보유할 수 있는 모든 Amazon FSx for Windows File Server 파일 시스템의 최대 사용자 시작 백업 수입니다.

할당량 증가 요청

1. Service Quotas 콘솔을 엽니다.
2. 탐색 창에서 AWS 서비스를 선택합니다.
3. Amazon FSx를 선택합니다.
4. 할당량을 선택합니다.
5. 할당량 증가 요청을 선택한 다음, 지침에 따라 할당량 증가를 요청합니다.
6. 할당량 요청 상태를 보려면 콘솔 탐색 창에서 할당량 요청 기록을 선택합니다.

자세한 내용은Service Quotas 사용 설명서의 할당량 증가 요청을 참조하세요.

각 파일 시스템의 리소스 할당량

다음은 AWS 리전의 각 파일 시스템에 대한 Amazon FSx for Windows File Server 리소스 할당량입니다.

Resource	파일 시스템당 한도
최대 태그 수	50
자동 백업의 최대 보존 기간	90일
계정당 단일 대상 리전으로 진행 중인 최대 백업 복사 요청 수입니다.	5

Resource	파일 시스템당 한도
최소 스토리지 용량, SSD 파일 시스템	32GiB
최소 스토리지 용량, HDD 파일 시스템	2,000GiB
최대 스토리지 용량, SSD 및 HDD	64TiB
최소 SSD IOPS	96
최대 SSD IOPS	400,000
최소 처리량 용량	8MBps
최대 처리량 용량	12,288MBps
최대 파일 공유 개수	100,000건

추가 고려 사항

또한 다음 사항에 유의하세요.

- 최대 125개의 Amazon FSx 파일 시스템에서 각 AWS Key Management Service(AWS KMS) 키를 사용할 수 있습니다.
- 파일 시스템을 생성할 수 있는 AWS 리전 목록의 경우 AWS 일반 참조의 Amazon FSx 엔드포인트 및 할당량을 참조하세요.
- Virtual Private Cloud(VPC)에 있는 Amazon EC2 인스턴스의 파일 공유를 도메인 이름 서비스(DNS) 이름과 매핑합니다.

Microsoft Windows 전용 할당량

자세한 내용은 Microsoft Windows 개발자 센터의 NTFS 제한을 참조하세요.

Amazon FSx 문제 해결

다음 섹션의 내용으로 Amazon FSx 관련 문제를 해결할 수 있습니다.

Amazon FSx를 사용하는 동안 다음 목록에 없는 문제가 발생하는 경우, Amazon FSx 포럼에 질문해 보세요.

주제

파일 시스템 액세스 불가

파일 시스템에 액세스할 수 없는 잠재적 원인은 여러 가지가 있으며, 원인마다 해결 방법이 다릅니다.

주제

- DNS 별칭으로 파일 시스템 액세스 불가
- IP 주소를 사용하여 파일 시스템 액세스 불가

수정 또는 삭제된 파일 시스템 탄력적 네트워크 인터페이스

파일 시스템의 탄력적 네트워크 인터페이스를 수정하거나 삭제해서는 안 됩니다. 네트워크 인터페이스를 수정하거나 삭제하면 VPC와 파일 시스템 간의 연결이 영구적으로 손실될 수 있습니다. 새 파일 시스템을 생성하고, Amazon FSx 탄력적 네트워크 인터페이스를 수정하거나 삭제하지 마세요. 자세한 정보는 Amazon VPC를 사용한 파일 시스템 액세스 제어을 참조하세요.

파일 시스템 탄력적 네트워크 인터페이스에 연결된 탄력적 IP 주소 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 정보는 Amazon FSx for Windows File Server가 지원하는 클라이언트, 액세스 방법 및 환경을 참조하세요.

파일 시스템 보안 그룹에는 필요한 인바운드 또는 아웃바운드 규칙이 없습니다.

Amazon VPC 보안 그룹에 지정된 인바운드 규칙을 검토하고 파일 시스템 관련 보안 그룹에 해당하는 인바운드 규칙이 있는지 확인하세요.

컴퓨팅 인스턴스의 보안 그룹에는 필요한 아웃바운드 규칙이 없습니다.

Amazon VPC 보안 그룹에 지정된 아웃바운드 규칙을 검토하고 컴퓨팅 인스턴스 관련 보안 그룹에 해당하는 아웃바운드 규칙이 있는지 확인하세요.

컴퓨팅 인스턴스가 Active Directory에 조인되지 않음

컴퓨팅 인스턴스가 다음 두 가지 유형의 Active Directory 중 하나에 제대로 조인되지 않을 수 있습니다.

- 파일 시스템이 가입된 AWS Managed Microsoft AD 디렉터리입니다.
- AWS Managed Microsoft AD 디렉터리와 단방향 포리스트 신뢰 관계가 설정된 Microsoft Active Directory 디렉터리입니다.

컴퓨팅 인스턴스가 두 가지 유형의 디렉터리 중 하나에 연결되어 있는지 확인합니다. 한 가지 유형은 파일 시스템이 가입된 AWS Managed Microsoft AD 디렉토리입니다. 다른 유형은 디렉터리와 단방향

포리스트 트러스트 관계가 설정된 Microsoft Active AWS Managed Microsoft AD Directory 디렉터리입니다. 자세한 정보는 아마존 FSx를 다음과 함께 사용하기 AWS Directory Service for Microsoft Active Directory을 참조하세요.

파일 공유가 존재하지 않음

액세스하려는 Microsoft Windows 파일 공유가 존재하지 않습니다.

기존 파일 공유를 사용하는 경우, 파일 시스템 DNS 이름과 공유 이름을 올바르게 지정해야 합니다. 파일 공유를 관리하려면 Windows File Server 파일 시스템용 FSx의 파일 공유 관리 섹션을 참조하세요.

Active Directory 사용자의 필수 권한 없음

파일 공유에 액세스하는 Active Directory 사용자에게 필요한 액세스 권한이 없습니다.

파일 공유에 대한 액세스 권한과 공유 폴더에 대한 Windows 액세스 제어 목록(ACL) 이 해당 폴더에 액세스하려는 Active Directory 사용자에게 액세스를 허용하는지 확인합니다.

전체 제어 허용 NTFS ACL 권한 없음

SYSTEM 사용자에게 공유한 폴더에 대한 전체 제어 허용 NTFS ACL 권한이 없으면 해당 공유에 액세스할 수 없게 되고 해당 시점부터 생성된 파일 시스템 백업을 사용하지 못할 수 있습니다.

영향을 받은 파일 공유는 다시 생성해야 합니다. 자세한 정보는 Windows File Server 파일 시스템용 FSx의 파일 공유 관리을 참조하세요. 폴더 또는 공유를 다시 생성한 후, 컴퓨팅 인스턴스의 Windows 파일 공유를 매핑하여 사용할 수 있습니다.

온프레미스 클라이언트를 사용하여 파일 시스템 액세스 불가

온프레미스에서는 또는 VPN을 사용하여 Amazon FSx 파일 시스템을 AWS Direct Connect 사용하고 있으며, 온프레미스 클라이언트에는 비사설 IP 주소 범위를 사용하고 있습니다.

Amazon FSx는 2020년 12월 17일 이후에 생성된 파일 시스템에서 프라이빗 IP 주소가 아닌 IP 주소를 사용하는 온프레미스 클라이언트에서의 액세스만 지원합니다.

프라이빗 IP 주소 범위 밖의 2020년 12월 17일 이전에 생성된 FSx for Windows File Server 파일 시스템에 액세스해야 하는 경우, 파일 시스템의 백업을 복원하여 새 파일 시스템을 생성할 수 있습니다. 자세한 정보는 백업 작업을 참조하세요.

DNS에 등록되지 않은 새 파일 시스템

자체 관리형 Active Directory에 조인된 파일 시스템의 경우, Amazon FSx는 고객 네트워크가 Microsoft DNS를 사용하지 않으면 파일 시스템 DNS를 생성할 때 등록하지 않았습니다.

Microsoft DNS 대신 타사 DNS 서비스를 사용하는 네트워크인 경우, Amazon FSx는 DNS에 파일 시스템을 등록하지 않습니다. Amazon FSx 파일 시스템의 DNS A 항목을 수동으로 설정해야 합니다. 단일 AZ 1 파일 시스템은 DNS A 항목을 하나 추가해야 하고, 단일 AZ 2 및 다중 AZ 파일 시스템은 DNS A 항목을 2개 추가해야 합니다. 다음 절차를 사용하여 DNS A 항목을 수동으로 추가할 때 사용할 파일 시스템 IP 주소 또는 주소를 획득합니다.

1. https://console.aws.amazon.com/fsx/ 에서 IP 주소를 획득할 파일 시스템을 선택하여 파일 시스템 세부 정보 페이지를 표시합니다.
2. 네트워크 및 보안 탭에서 다음 중 하나를 수행하세요.

   - 단일 AZ 1 파일 시스템의 경우:
     - 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2에서 네트워크 인터페이스 페이지를 엽니다.
     - 사용할 단일 AZ 1 파일 시스템의 IP 주소는 기본 프라이빗 IPv4 IP 열에 표시됩니다.
   - 단일 AZ 2 또는 다중 AZ 파일 시스템의 경우:
     - 기본 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2에서 네트워크 인터페이스 페이지를 엽니다.
     - 사용할 기본 서브넷의 IP 주소는 보조 프라이빗 IPv4 IP 열에 표시됩니다.
     - Amazon FSx 대기 서브넷 패널의 네트워크 인터페이스 아래에 표시된 탄력적 네트워크 인터페이스를 선택하여 Amazon EC2 콘솔에서 네트워크 인터페이스 페이지를 엽니다.
     - 사용할 대기 서브넷의 IP 주소는 보조 프라이빗 IPv4 IP 열에 표시됩니다.

DNS 별칭으로 파일 시스템 액세스 불가

DNS 별칭을 사용하여 파일 시스템에 액세스할 수 없는 경우, 다음 절차를 사용하여 문제를 해결합니다.

1. 다음 단계 중 하나를 수행하여 별칭이 파일 시스템에 연결되어 있는지 확인하세요.

   a. Amazon FSx 콘솔 사용 — 액세스하려는 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지의 네트워크 및 보안 탭에 DNS 별칭이 표시됩니다.

b. CLI 또는 API 사용 - **`describe-file-system-aliases`**CLI 명령 또는 DescribeFileSystemAliasesAPI 작업을 사용하여 현재 파일 시스템에 연결된 별칭을 검색합니다.

2. DNS 별칭이 목록에 없는 경우, 해당 별칭을 파일 시스템에 연결해야 합니다. 자세한 정보는 기존 파일 시스템의 DNS 별칭 관리을 참조하세요.
3. DNS 별칭이 파일 시스템과 연결된 경우, 다음 필수 항목을 구성했는지 확인하세요.

   - Amazon FSx 파일 시스템의 Active Directory 컴퓨터 객체에 DNS 별칭에 대해 생성된 서비스 보안 주체 이름(SPN).

     자세한 정보는 2단계: Kerberos의 서비스 보안 주체 이름(SPN) 구성을 참조하세요.
   - Amazon FSx 파일 시스템의 기본 DNS 이름으로 확인되는 DNS 별칭에 대해 생성된 DNS CNAME 레코드.

     자세한 정보는 3단계: 파일 시스템의 DNS CNAME 레코드 업데이트 또는 생성을 참조하세요.
4. 유효한 SPN과 DNS CNAME 레코드가 있다면, 클라이언트의 DNS에 올바른 파일 시스템으로 확인되는 DNS CNAME 레코드가 있는지 확인하세요.

   a. `nslookup`을 실행하여 레코드가 존재하고, 해당 레코드가 파일 시스템의 기본 DNS 이름으로 확인되는지 확인합니다.

   b. DNS CNAME이 다른 파일 시스템으로 확인되면 클라이언트의 DNS 캐시가 새로 고쳐질 때까지 기다린 다음 CNAME 레코드를 다시 확인합니다. 다음 명령을 사용하여 클라이언트의 DNS 캐시를 비우면 프로세스를 가속화할 수 있습니다.

   ```
   ipconfig /flushdns
   ```
5. DNS CNAME 레코드가 Amazon FSx 파일 시스템의 기본 DNS로 확인되고, 클라이언트가 여전히 파일 시스템에 액세스할 수 없는 경우, 추가 문제 해결 단계를 확인하기 위해 파일 시스템 액세스 불가 섹션을 참조하세요.

IP 주소를 사용하여 파일 시스템 액세스 불가

IP 주소를 사용하여 파일 시스템에 액세스할 수 없는 경우, DNS 이름 또는 연결된 DNS 별칭을 대신 사용해 보세요.

Amazon FSx 콘솔에서 Windows File Server, 네트워크 및 보안을 선택하여 파일 시스템의 DNS 이름과 모든 관련 DNS 별칭을 찾을 수 있습니다. 또는 API 작업의 응답에서 찾을 CreateFileSystem수도

DescribeFileSystems있습니다. DNS 별칭 사용에 대한 자세한 내용은 DNS 별칭 관리 섹션을 참조하세요.

- AWS 관리형 Microsoft Active Directory에 연결된 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
fs-0123456789abcdef0.ad-domain.com
```

- 자체 관리형 Active Directory에 연결된 모든 다중 AZ 파일 시스템 및 단일 AZ 파일 시스템의 경우 DNS 이름은 다음과 같습니다.

```
amznfsxaa11bb22.ad-domain.com
```

새 Amazon FSx 파일 시스템 생성 실패

다음 섹션에 설명된 것처럼 파일 시스템 생성 요청이 실패하는 잠재적 원인은 여러 가지가 있습니다.

주제

- AWS 관리형 Microsoft Active Directory에 조인된 파일 시스템 문제 해결
- 자체 관리형 Active Directory에 연결된 파일 시스템을 만들면 실패합니다.

AWS 관리형 Microsoft Active Directory에 조인된 파일 시스템 문제 해결

다음 섹션은 자체 관리형 Active Directory에 조인되는 FSx for Windows File Server 파일 시스템을 생성할 때 발생한 문제를 해결하는 데 도움이 됩니다.

잘못 구성된 VPC 보안 그룹 및 네트워크 ACL

VPC 보안 그룹과 네트워크 ACL이 권장 보안 그룹 구성을 사용하고 있는지 확인합니다. 자세한 내용은 보안 그룹 생성을 참조하십시오.

자체 관리형 Active Directory에 연결된 파일 시스템을 만들면 실패합니다.

주제

- 중복된 파일 시스템 관리자 그룹 이름
- DNS 서버 또는 도메인 컨트롤러에 연결할 수 없습니다.
- 잘못된 서비스 계정 자격 증명

- 서비스 계정 권한이 충분하지 않습니다.
- 서비스 계정 용량 초과
- Amazon FSx는 조직 단위 (OU) 에 액세스할 수 없습니다.
- 서비스 계정은 관리자 그룹에 접근할 수 없습니다.
- Amazon FSx의 도메인 연결이 끊어졌습니다.
- 서비스 계정에 올바른 권한이 없습니다.
- 생성 매개변수에 사용되는 유니코드 문자

중복된 파일 시스템 관리자 그룹 이름

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
File system creation failed. Amazon FSx is unable to apply your Microsoft Active
 Directory configuration with the
specified file system administrators group. Please ensure that your Active Directory
 does not contain multiple domain
groups with the name: domain_group.
```

도메인에 이름이 같은 관리자 그룹이 여러 개 있기 때문에 Amazon FSx는 파일 시스템을 생성하지 않았습니다.

그룹 이름을 지정하지 않으면 Amazon FSx는 기본값인 “Domain Admins”를 관리자 그룹으로 사용하려고 시도합니다. 기본 “Domain Admins” 이름을 사용하는 그룹이 둘 이상인 경우 요청이 실패합니다.

다음 단계를 사용하여 문제를 해결하십시오.

1. 파일 시스템을 자체 관리형 Active Directory에 가입하기 위한 사전 요구 사항을 검토하십시오.
2. Amazon FSx Active Directory 검증 도구를 사용하여 자체 관리형 Active Directory에 연결된 Windows File Server용 FSx 파일 시스템을 생성하기 전에 자체 관리형 Active Directory 구성을 검증하십시오.
3. OR를 사용하여 새 파일 시스템을 생성하십시오. AWS Management Console AWS CLI자세한 정보는 Amazon FSx 파일 시스템을 자체 관리형 Microsoft Active Directory 도메인에 조인을 참조하세요.
4. 자체 관리형 Active Directory의 도메인에서 고유한 파일 시스템 관리자 그룹 이름을 제공하십시오.

DNS 서버 또는 도메인 컨트롤러에 연결할 수 없습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx can't reach the DNS servers provided or the domain controllers for your
 self-managed directory in Microsoft Active Directory.
File system creation failed. Amazon FSx is unable to communicate with your Microsoft
 Active Directory domain controllers.
This is because Amazon FSx can't reach the DNS servers provided or domain controllers
 for your domain.
To fix this problem, delete your file system and create a new one with valid DNS
 servers and networking configuration that allows
traffic from the file system to the domain controller.
```

다음 단계에 따라 문제를 해결합니다.

1. Amazon FSx 파일 시스템을 생성하는 서브넷과 자체 관리형 Active Directory 간에 네트워크 연결 및 라우팅을 설정하기 위한 사전 요건을 따랐는지 확인하세요. 자세한 정보는 자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항을 참조하세요.

   Amazon FSx Active Directory 검증 도구를 사용하여 네트워크 설정을 테스트하고 확인하세요.

   > **Note**
   >
   > Microsoft Active Directory 사이트가 다수 정의되어 있는 경우에는 Amazon FSx 파일 시스템과 연결된 VPC의 서브넷이 Microsoft Active Directory 사이트에 정의되어 있도록 하고 VPC의 서브넷과 다른 사이트의 서브넷 간에 IP가 충돌하지 않도록 해야 합니다. Active Directory 사이트 및 서비스 MMC 스냅인을 사용하여 이러한 설정을 보고 변경할 수 있습니다.

2. Amazon FSx 파일 시스템에 연결한 VPC 보안 그룹을 VPC 네트워크 ACL과 함께 모든 포트에서 아웃바운드 네트워크 트래픽을 허용하도록 구성했는지 확인하세요.

   > **Note**
   >
   > 최소 권한을 구현하려는 경우, Active Directory 도메인 컨트롤러와의 통신에 필요한 특정 포트로의 아웃바운드 트래픽만 허용할 수 있습니다. 자세한 내용은 Microsoft Active Directory 설명서를 참조하세요.

3. Microsoft Windows 파일 서버 또는 네트워크 관리 속성의 값에 Latin-1이 아닌 문자가 포함되어 있지 않은지 확인합니다. 예를 들어, 파일 시스템 관리자 그룹의 이름으로 `Domänen-Admins`를 사용하면 파일 시스템 생성이 실패합니다.
4. Active Directory 도메인의 DNS 서버 및 도메인 컨트롤러가 활성 상태이고 제공된 도메인에 대한 요청에 응답하는지 확인합니다.
5. Active Directory 도메인의 기능 수준이 Windows Server 2008 R2 이상인지 확인합니다.
6. Active Directory 도메인의 도메인 컨트롤러에 있는 방화벽 규칙이 Amazon FSx 파일 시스템으로부터의 트래픽을 허용하는지 확인합니다. 자세한 내용은 Microsoft Active Directory 설명서를 참조하세요.

잘못된 서비스 계정 자격 증명

자체 관리형 Active Directory에 연결된 파일 시스템을 만들면 실패하고 다음 오류 메시지가 표시됩니다.

```
Amazon FSx is unable to establish a connection with your Microsoft Active Directory
 domain controllers
because the service account credentials provided are invalid. To fix this problem,
 delete your file
system and create a new one using a valid service account.
```

다음 단계에 따라 문제를 해결합니다.

1. 자체 관리형 Active Directory 구성의 `ServiceAcct`와 같이 서비스 계정 사용자 이름을 입력할 때 사용자 이름만 입력하고 있는지 확인합니다.

   > **Important**
   >
   > 서비스 계정 사용자 이름을 입력할 때 도메인 접두사(`corp.com\ServiceAcct`) 또는 도메인 접미사(`ServiceAcct@corp.com`)를 포함하지 않습니다.
   > 서비스 계정 사용자 이름 (CN=ServiceAcct, OU=Example, DC=corp, DC=com) 을 입력할 때는 DN (고유 이름) 을 사용하지 마십시오.

2. 제공한 서비스 계정이 Active Directory 도메인에 있는지 확인하세요.
3. 제공한 서비스 계정에 필요한 권한을 위임했는지 확인하세요. 서비스 계정은 파일 시스템에 조인하려는 도메인의 OU에서 컴퓨터 개체를 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

올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

서비스 계정 권한이 충분하지 않습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx is unable to establish a connection with your
Microsoft Active Directory domain controllers. This is because the service account
 provided does not
have permission to join the file system to the domain with the specified organizational
 unit.
To fix this problem, delete your file system and create a new one using a service
 account with
permission to join the file system to the domain with the specified organizational
 unit.
```

다음 절차에 따라 문제를 해결합니다.

- 제공한 서비스 계정에 필요한 권한을 위임했는지 확인하세요. 서비스 계정은 파일 시스템에 조인하려는 도메인의 OU에서 컴퓨터 개체를 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

  올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

서비스 계정 용량 초과

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx can't establish a connection with your Microsoft Active Directory
domain controllers. This is because the service account provided has reached the
maximum number of computers that it can join to the domain. To fix this problem,
delete your file system and create a new one, supplying a service account that
is able to join new computers to the domain.
```

문제를 해결하려면 제공한 서비스 계정이 도메인에 조인할 수 있는 최대 컴퓨터 수에 도달했는지 확인합니다. 최대 한도에 도달한 경우 올바른 권한을 가진 새 서비스 계정을 생성합니다. 새 서비스 계정을 사용하여 새 파일 시스템을 생성합니다. 자세한 정보는 Amazon FSx 서비스 계정에 권한 위임 을 참조하세요.

Amazon FSx는 조직 단위 (OU) 에 액세스할 수 없습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx can't establish a connection with your Microsoft Active Directory domain
 controller(s).
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, delete your file system and
 create a new one specifying an
organizational unit to which the service account can join the file system.
```

다음 단계에 따라 문제를 해결합니다.

1. 제공한 OU가 Active Directory 도메인에 있는지 확인하세요.
2. 제공한 서비스 계정에 필요한 권한을 위임했는지 확인하세요. 서비스 계정은 파일 시스템에 조인하려는 도메인의 OU에서 컴퓨터 개체를 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 개체 생성 및 삭제 위임받음
- 검증된 계정 제한 사항의 읽기 및 쓰기 기능

올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

서비스 계정은 관리자 그룹에 접근할 수 없습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. This is
 because the file system
administrators group you provided either doesn't exist or isn't accessible to the
 service account you
provided. To fix this problem, delete your file system and create a new one specifying
 a file
system administrators group in the domain that is accessible to the service account
provided.
```

다음 단계에 따라 문제를 해결합니다.

1. 그룹 이름만 관리자 그룹 파라미터의 문자열로 제공해야 합니다.

   > **Important**
   >
   > 그룹 이름 파라미터를 제공할 때 도메인 접두사(`corp.com\FSxAdmins`) 또는 도메인 접미사(`FSxAdmins@corp.com`)를 포함하지 않습니다.
   > 그룹에 고유 이름(DN)을 사용하지 않습니다. 고유 이름의 예로는 CN=FSxAdmins, OU=Example, DC=Corp, DC=com 등이 있습니다.

2. 제공된 관리자 그룹이 파일 시스템에 조인하려는 Active Directory 도메인과 동일한 Active Directory 도메인에 존재하는지 확인하세요
3. 관리자 그룹 파라미터를 제공하지 않은 경우, Amazon FSx는 Active Directory 도메인의 `Builtin Domain Admins` 그룹을 사용하려고 시도합니다. 그룹의 이름이 변경되었거나 도메인 관리에 다른 그룹을 사용하는 경우 여기에 해당 그룹 이름을 입력해야 합니다.

Amazon FSx의 도메인 연결이 끊어졌습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
Amazon FSx is unable to apply your Microsoft Active Directory configuration. To fix
 this problem, delete your file system and create a new one
meeting the pre-requisites described in the Amazon FSx user guide.
```

파일 시스템을 생성할 때, Amazon FSx는 Active Directory 도메인의 DNS 서버 및 도메인 컨트롤러에 도달하여 파일 시스템을 Active Directory 도메인에 성공적으로 조인할 수 있었습니다. 하지만 파일 시스템 생성을 완료하는 동안 Amazon FSx가 도메인과의 연결이 끊어졌거나 도메인 구성원 자격을 잃었습니다. 다음 단계에 따라 문제를 해결합니다.

1. Amazon FSx 파일 시스템과 Active Directory 간에 네트워크 연결이 계속 유지되도록 합니다. 또한 라우팅 규칙, VPC 보안 그룹 규칙, VPC 네트워크 ACL, 도메인 컨트롤러 방화벽 규칙을 사용하여 둘 사이의 네트워크 트래픽이 계속 허용되도록 합니다.
2. Active Directory 도메인의 파일 시스템에 대해 Amazon FSx이 생성한 컴퓨터 객체가 여전히 활성 상태이고, 삭제되거나 조작되지 않았는지 확인합니다.

서비스 계정에 올바른 권한이 없습니다.

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
File system creation failed. Amazon FSx is unable to establish a connection with your
 Microsoft Active Directory domain controller(s).
This is because the service account provided does not have permission to join the file
 system to the domain with the specified
organizational unit (OU). To fix this problem, delete your file system and create a new
 one using a service account with permission
to create computer objects and reset passwords within the specified organizational
 unit.
```

제공한 서비스 계정에 필요한 권한을 위임했는지 확인하세요. 다음 단계에 따라 문제를 해결합니다.

서비스 계정에는 최소한 다음 권한이 있어야 합니다.

- 파일 시스템을 조인하려는 OU에서 컴퓨터 객체를 생성하고 삭제할 수 있는 권한을 위임받음

- 파일 시스템이 조인하려는 OU에는 다음과 같은 권한이 있어야 합니다.
  - 암호 재설정 기능
  - 계정의 데이터 읽기 및 쓰기 제한 기능
  - 검증된 DNS 호스트 이름 쓰기 기능
  - 검증된 서비스 보안 주체 이름 쓰기 기능
  - 컴퓨터 객체의 생성 및 삭제 기능(위임 가능)
  - 검증된 계정 제한 사항의 읽기 및 쓰기 기능
  - 권한 수정 기능

  올바른 권한이 있는 서비스 계정을 생성하는 방법에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.

생성 매개변수에 사용되는 유니코드 문자

자체 관리형 Active Directory에 조인된 파일 시스템을 만들면 작업이 실패하고 다음과 같은 오류 메시지가 표시됩니다.

```
File system creation failed. Amazon FSx is unable to create a file system within the
 specified
Microsoft Active Directory. To fix this problem, please delete your file system and
 create a new one
meeting the pre-requisites described in the FSx for ONTAP User Guide.
```

Amazon FSx는 유니코드 문자를 지원하지 않습니다. 생성 파라미터에 액센트 부호와 같은 유니코드 문자가 없는지 확인합니다. 비워두면 기본값이 자동으로 입력되는 파라미터도 확인합니다. 해당 Active Directory 기본값에도 유니코드 문자가 포함되어 있지 않은지 확인합니다.

Amazon FSx를 사용하는 동안 여기에 나열되지 않은 문제가 발생하는 경우, Amazon FSx 포럼에 질문하거나 Amazon Web Services 지원 부서에 문의하십시오.

파일 시스템이 잘못 구성된 상태

Active Directory 환경의 변화로 인해 FSx for Windows File Server 파일 시스템이 잘못 구성된 상태가 될 수 있습니다. 파일 시스템이 잘못 구성된 상태이면 현재 사용할 수 없거나 가용성이 손실될 위험이 있으며 백업이 실패할 수 있습니다.

잘못 구성된 상태에는 Amazon FSx 콘솔, API 또는 AWS CLI를 사용하여 액세스할 수 있는 오류 메시지와 권장 수정 조치가 포함됩니다. 수정 조치를 취한 후, 파일 시스템이 최종적으로 `Available` 상태로 변경되는지 확인하세요. 변경을 완료하는 데 몇 분이 걸릴 수 있습니다.

파일 시스템이 잘못 구성된 상태가 될 수 있는 이유는 다음과 같습니다.

- DNS 서버 IP 주소가 더 이상 유효하지 않습니다.
- 서비스 계정 보안 인증 정보가 더 이상 유효하지 않거나 필요한 권한이 없습니다.
- 유효하지 않은 VPC 보안 그룹, VPC 네트워크 ACL 또는 라우팅 테이블 구성 또는 도메인 컨트롤러 방화벽 설정 등의 네트워크 연결 문제로 인해 Active Directory 도메인 컨트롤러에 연결할 수 없습니다.

(Active Directory 요구 사항의 전체 목록은 자체 관리형 Microsoft Active Directory를 사용하기 위한 사전 요구 사항 섹션을 참조하세요. Amazon FSx Active Directory 검증 도구를 사용하여 Active Directory 환경이 요구 사항을 충족하도록 적절하게 구성되어 있는지 확인할 수도 있습니다.)

일부 문제는 해결하려면 파일 시스템의 Active Directory 구성에서 DNS 서버 IP 주소를 변경하거나, 서비스 계정 사용자 이름 또는 암호를 변경하는 등 하나 이상의 매개 변수를 직접 업데이트해야 합니다. 이러한 경우 수정 조치에는 반드시 Amazon FSx 콘솔 AWS CLI 또는 API를 사용하거나 필수 구성 파라미터를 업데이트해야 합니다.

다른 문제에서는 도메인 컨트롤러 방화벽 설정 또는 VPC 보안 그룹 변경과 같은 Active Directory 구성 파라미터를 변경할 필요가 없을 수도 있습니다. 하지만 이러한 경우, 파일 시스템을 `Available` 상태로 만들려면 추가 조치를 취해야 합니다. Active Directory 환경이 제대로 구성되었는지 확인한 후, Amazon FSx 콘솔에서 잘못 구성된 상태 옆에 있는 복구 시도 버튼을 선택하거나 Amazon FSx 콘솔, API, 또는 AWS CLI에서 `StartMisconfiguredStateRecovery` 명령을 사용하세요.

주제

- 잘못 구성된 파일 시스템: Amazon FSx가 도메인의 DNS 서버 또는 도메인 컨트롤러에 연결할 수 없습니다.
- 잘못 구성된 파일 시스템: 서비스 계정 보안 인증 정보가 유효하지 않음
- 잘못 구성된 파일 시스템: 제공된 서비스 계정에 파일 시스템을 도메인에 조인할 권한이 없음
- 잘못 구성된 파일 시스템: 서비스 계정이 더 이상 컴퓨터를 도메인에 조인할 수 없음
- 잘못 구성된 파일 시스템: 서비스 계정이 OU에 액세스할 수 없음

잘못 구성된 파일 시스템: Amazon FSx가 도메인의 DNS 서버 또는 도메인 컨트롤러에 연결할 수 없습니다.

Amazon FSx가 Microsoft Active Directory 도메인 컨트롤러 또는 여러 컨트롤러와 통신할 수 없는 경우 파일 시스템은 `Misconfigured` 상태가 됩니다.

이러한 상황을 해결하려면 다음 작업을 시도해 보세요.

1. 네트워크 구성이 파일 시스템에서 도메인 컨트롤러로의 트래픽을 허용하는지 확인합니다.
2. Amazon FSx Active Directory 검증 도구를 사용하여 자체 관리형 Active Directory의 네트워크 설정을 테스트하고 확인하세요. 자세한 정보는 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용을 참조하세요.
3. Amazon FSx 콘솔에서 파일 시스템의 자체 관리형 Active Directory 구성을 검토하세요.
4. Amazon FSx 콘솔을 사용하여 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트할 수 있습니다.

   a. 탐색 창에서 파일 시스템을 선택하고 업데이트할 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지가 나타납니다.

   b. 파일 시스템 세부 정보 페이지의 네트워킹 및 보안 탭에서 업데이트를 선택합니다.

   Amazon FSx `update-file-system` CLI 명령 또는 API 작업을 사용할 수도 있습니다. UpdateFileSystem

잘못 구성된 파일 시스템: 서비스 계정 보안 인증 정보가 유효하지 않음

Amazon FSx가 Microsoft Active Directory 도메인 컨트롤러 또는 여러 컨트롤러와 연결을 설정할 수 없습니다. 제공된 서비스 계정 보안 인증 정보가 유효하지 않기 때문입니다. 자세한 정보는 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용을 참조하세요.

잘못된 구성을 해결하려면 다음을 수행합니다.

1. 올바른 서비스 계정을 사용하고 있는지 확인하고, 해당 계정의 올바른 보안 인증 정보를 사용하고 있는지 확인합니다.
2. 그런 다음 Amazon FSx 콘솔을 사용하여 올바른 서비스 계정 또는 계정 보안 인증 정보로 파일 시스템 구성을 업데이트합니다.

   a. 탐색 창에서 파일 시스템을 선택하고 업데이트할 잘못 구성된 파일 시스템을 선택합니다.

b. 파일 시스템 세부 정보 페이지의 네트워킹 및 보안 탭에서 업데이트를 선택합니다.

Amazon FSx API 작업 `update-file-system`을 사용할 수도 있습니다. 자세한 내용은 Amazon FSx API UpdateFileSystem레퍼런스의 을 참조하십시오.

잘못 구성된 파일 시스템: 제공된 서비스 계정에 파일 시스템을 도메인에 조인할 권한이 없음

Amazon FSx가 Microsoft Active Directory 도메인 컨트롤러와 연결을 설정할 수 없습니다. 이는 제공된 서비스 계정에 파일 시스템을 지정된 OU가 있는 도메인에 조인할 권한이 없기 때문입니다.

잘못된 구성을 해결하려면 다음을 수행합니다.

1. Amazon FSx 서비스 계정에 필요한 권한을 추가하거나 필요한 권한을 가진 새 서비스 계정을 생성합니다. 해당 작업에 대한 자세한 내용은 Amazon FSx 서비스 계정에 권한 위임 섹션을 참조하세요.
2. 그런 다음 새 서비스 계정 보안 인증 정보로 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트합니다. Amazon FSx 콘솔을 사용하여 구성을 업데이트할 수 있습니다.

   a. 탐색 창에서 파일 시스템을 선택하고 업데이트할 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지가 나타납니다.
   b. 파일 시스템 세부 정보 페이지의 네트워킹 및 보안 탭에서 업데이트를 선택합니다.

   Amazon FSx API 작업 `update-file-system`을 사용할 수도 있습니다. 자세한 내용은 Amazon FSx API UpdateFileSystem레퍼런스의 을 참조하십시오.

잘못 구성된 파일 시스템: 서비스 계정이 더 이상 컴퓨터를 도메인에 조인할 수 없음

Amazon FSx가 Microsoft Active Directory 도메인 컨트롤러와 연결을 설정할 수 없습니다. 이 때 원인은 제공한 서비스 계정이 도메인에 조인할 수 있는 최대 컴퓨터 수에 도달했기 때문입니다.

잘못된 구성을 해결하려면 다음을 수행합니다.

1. 다른 서비스 계정을 식별하거나, 새 컴퓨터를 도메인에 조인할 수 있는 새 서비스 계정을 만드세요.

2. 그런 다음 Amazon FSx 콘솔을 사용하여 새 서비스 계정 보안 인증 정보로 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트합니다.

   a. 탐색 창에서 파일 시스템을 선택하고 업데이트할 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지가 나타납니다.
   b. 파일 시스템 세부 정보 페이지의 네트워킹 및 보안 탭에서 업데이트를 선택합니다.

   Amazon FSx API 작업 `update-file-system`을 사용할 수도 있습니다. 자세한 내용은 Amazon FSx API UpdateFileSystem레퍼런스의 을 참조하십시오.

잘못 구성된 파일 시스템: 서비스 계정이 OU에 액세스할 수 없음

제공된 서비스 계정에 지정된 OU에 대한 액세스 권한이 없기 때문에 Amazon FSx가 Microsoft Active Directory 도메인 컨트롤러에 대한 연결을 설정할 수 없습니다.

잘못된 구성을 해결하려면 다음을 수행합니다.

1. 다른 서비스 계정을 식별하거나 OU에 액세스할 수 있는 새 서비스 계정을 만드세요.
2. 그런 다음 새 서비스 계정 보안 인증 정보로 파일 시스템의 자체 관리형 Active Directory 구성을 업데이트합니다.

   a. 탐색 창에서 파일 시스템을 선택하고 업데이트할 파일 시스템을 선택합니다. 파일 시스템 세부 정보 페이지가 나타납니다.
   b. 파일 시스템 세부 정보 페이지의 네트워킹 및 보안 탭에서 업데이트를 선택합니다.

   Amazon FSx API 작업 `update-file-system`을 사용할 수도 있습니다. 자세한 내용은 Amazon FSx API UpdateFileSystem레퍼런스의 을 참조하십시오.

FSx for Windows File Server에서 원격 PowerShell을 사용하여 문제 해결

사용자 지정 원격 관리 명령을 사용하여 Windows File Server 파일 시스템용 FSx를 관리할 수 있습니다. PowerShell

주제

- New-F SxSmbShare 명령이 단방향 신뢰로 인해 실패합니다.

- Remote를 사용하여 파일 시스템에 액세스할 수 없습니다. PowerShell

New-F SxSmbShare 명령이 단방향 신뢰로 인해 실패합니다.

Amazon FSx는 단방향 트러스트가 있고 사용자가 상주하는 도메인이 Amazon FSx 파일 시스템과 연결된 도메인을 신뢰하도록 구성되지 않은 경우 명령 실행을 `New-FSxSmbShare` PowerShell 지원하지 않습니다.

다음 방법 중 하나를 사용하여 상황을 해결할 수 있습니다.

- `New-FSxSmbShare` 명령을 실행하는 사용자는 FSx 파일 시스템과 동일한 도메인에 있어야 합니다.
- fsmgmt.msc GUI를 사용하여 파일 시스템에 공유를 생성할 수 있습니다. 자세한 정보는 공유 폴더 GUI를 통한 파일 공유 관리을 참조하세요.

Remote를 사용하여 파일 시스템에 액세스할 수 없습니다. PowerShell

Remote를 사용하여 파일 시스템에 연결할 수 없는 원인에는 여러 가지가 PowerShell 있으며, 각 원인마다 해결 방법이 다릅니다.

먼저 Windows 원격 PowerShell 엔드포인트에 성공적으로 연결할 수 있는지 확인하기 위해 기본 연결 테스트를 실행할 수도 있습니다. 예를 들어, `test-netconnection endpoint -port 5985` 명령을 실행할 수 있습니다.

파일 시스템의 보안 그룹에는 원격 연결을 허용하는 데 필요한 인바운드 규칙이 없습니다. PowerShell

원격 세션을 설정하려면 파일 시스템의 보안 그룹에 포트 5985의 트래픽을 허용하는 인바운드 규칙이 있어야 합니다. PowerShell 자세한 정보는 Amazon VPC 보안 그룹을 참조하세요.

AWS 관리되는 Microsoft Active Directory와 온-프레미스 Active Directory 간에 외부 트러스트가 구성되어 있습니다.

Kerberos 인증과 함께 Amazon FSx PowerShell Remote를 사용하려면 클라이언트에서 포리스트 검색 순서에 대한 로컬 그룹 정책을 구성해야 합니다. 자세한 내용은 Microsoft 설명서의 Kerberos 포리스트 검색 순서(KFSO) 구성을 참조하세요.

원격 세션을 시작하려고 할 때 언어 현지화 오류가 발생합니다. PowerShell

명령에 `-SessionOption` 옵션으로 `-SessionOption (New-PSSessionOption -uiCulture "en-US")`를 추가해야 합니다.

다음은 파일 시스템에서 원격 PowerShell 세션을 시작할 `-SessionOption` 때 사용하는 두 가지 예입니다.

```
PS C:\Users\delegateadmin> Invoke-Command -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FSxRemoteAdmin -scriptblock {fsx-command} -SessionOption
 (New-PSSessionOption -uiCulture "en-US")
```

```
PS C:\Users\delegateadmin> Enter-Pssession -ComputerName Windows Remote PowerShell
 Endpoint -ConfigurationName FsxRemoteAdmin -SessionOption (New-PSSessionOption -
uiCulture "en-US")
```

다중 AZ 또는 단일 AZ 2 파일 시스템에서 DFS-R 구성 불가

Microsoft 분산 파일 시스템 복제(DFS-R)는 다중 AZ 및 단일 AZ 2 파일 시스템에서 지원되지 않습니다.

다중 AZ 파일 시스템은 기본적으로 여러 액세스 영역에 걸쳐 중복되도록 구성됩니다. 다중 AZ 배포 유형을 사용하면 여러 가용 영역에서 고가용성을 확보할 수 있습니다. 자세한 정보는 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템을 참조하세요.

스토리지 또는 처리량 용량 업데이트 실패

파일 시스템 스토리지 및 처리량 용량 업데이트 요청이 실패할 수 있는 잠재적 원인은 여러 가지가 있으며, 각 원인마다 해결 방법이 다릅니다.

Amazon FSx가 파일 시스템의 KMS 암호화 키에 액세스할 수 없어 스토리지 용량 증가 실패

Amazon FSx가 파일 시스템의 AWS Key Management Service (AWS KMS) 암호화 키에 액세스할 수 없어서 스토리지 용량 증가 요청이 실패했습니다.

관리 작업을 실행하려면 Amazon FSx가 AWS KMS 키에 액세스할 수 있는지 확인해야 합니다. 다음 정보를 사용하여 키 액세스 문제를 해결합니다.

- KMS 키가 삭제된 경우, 새 KMS 키를 사용하여 백업에서 새 파일 시스템을 생성해야 합니다. 자세한 정보는 연습 2: 백업에서 파일 시스템 생성을 참조하세요. 새 파일 시스템을 사용할 수 있게 되면 요청을 재시도합니다.
- KMS 키가 비활성화된 경우 다시 활성화한 다음 스토리지 용량 증가 요청을 다시 시도하세요. 자세한 내용은 AWS Key Management Service 개발자 안내서의 키 활성화 및 비활성화를 참조하세요.
- KMS 키가 삭제 보류 중이어서 유효하지 않은 경우, 새 KMS 키를 사용하여 백업에서 새 파일 시스템을 생성해야 합니다. 새 파일 시스템을 사용할 수 있게 되면 요청을 재시도합니다. 자세한 정보는 연습 2: 백업에서 파일 시스템 생성을 참조하세요.
- 키가 가져오기 보류 중이어서 키가 유효하지 않은 경우, 가져오기가 완료될 때까지 기다린 다음 스토리지 증가 요청을 다시 시도해야 합니다.
- 키의 권한 한도를 초과한 경우, 키에 대한 권한 부여 횟수 증가를 요청해야 합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서에서 리소스 할당량을 참조하세요. 할당량 증가가 허용되면 스토리지 증가 요청을 다시 시도하세요.

자체 관리형 Active Directory가 잘못 구성되어 스토리지 또는 처리량 용량 업데이트 실패

파일 시스템의 자체 관리형 Active Directory가 잘못 구성된 상태여서 스토리지 용량 또는 처리량 용량 업데이트 요청이 실패했습니다.

특정한 잘못 구성된 상태를 해결하려면 파일 시스템이 잘못 구성된 상태 섹션을 참조하세요.

처리량 용량이 충분하지 않아 스토리지 용량 증가 실패

파일 시스템의 처리량 용량이 8MB/s로 설정되었기 때문에 스토리지 용량 증가 요청이 실패했습니다.

파일 시스템의 처리량 용량을 최소 16MB/s로 늘린 다음 요청을 다시 시도하세요. 자세한 정보는 처리량 용량 관리을 참조하세요.

처리량 용량의 8MB/s 업데이트 실패

파일 시스템의 처리량 용량을 8MB/s로 수정하라는 요청이 실패했습니다.

스토리지 용량 증가 요청이 보류 중 또는 진행 중일 때 발생할 수 있습니다. 스토리지 용량을 늘리려면 최소 16MB/s의 처리량이 필요합니다. 스토리지 용량 증가 요청이 완료되면 처리량 용량 수정 요청을 다시 시도하세요.

백업 복원 중 스토리지 유형의 HDD로의 전환 실패

백업에서 파일 시스템을 생성하는 작업이 실패하고 다음 오류 메시지가 표시됩니다.

```
Switching storage type to HDD while creating a file system from backup
backup_id is not supported because a storage scaling activity was still
under way on the source file system to increase storage capacity from less
than 2000 GiB when the backup backup_id was taken, and the minimum storage
capacity for HDD storage is 2000 GiB.
```

이 문제는 백업을 복원할 때 스토리지 유형을 SSD에서 HDD로 변경할 때 발생합니다. 기존 파일 시스템에서 스토리지 용량 증가가 진행 중일 때 복원 중인 백업이 수행되었으므로 백업 복원이 실패합니다. 증가 요청 이전 파일 시스템의 SSD 스토리지 용량이 HDD 파일 시스템을 생성하는 데 필요한 최소 스토리지 용량인 2000GiB 미만이었습니다.

다음 절차를 사용하여 문제를 해결합니다.

1. 스토리지 용량 증가 요청이 완료되고 파일 시스템에 최소 2000GiB의 SSD 스토리지 용량이 생길 때까지 기다립니다. 자세한 정보는 스토리지 용량 증가 모니터링을 참조하세요.
2. 파일 시스템의 사용자 시작 백업을 사용합니다. 자세한 정보는 사용자 시작 백업 작업을 참조하세요.
3. 사용자 시작 백업을 HDD 스토리지를 사용하는 새 파일 시스템으로 복원합니다. 자세한 정보는 백업 복원을 참조하세요.

섀도우 복사본 문제 해결

다음 섹션에 설명된 것처럼 섀도우 복사본이 누락되거나 액세스할 수 없는 잠재적 원인은 여러 가지가 있습니다.

주제

- 가장 오래된 섀도우 복사본 누락
- 모든 섀도우 복사본 누락
- 최근에 복원되거나 업데이트된 파일 시스템에서 Amazon FSx 백업 생성 또는 섀도우 복사본 액세스 불가

가장 오래된 섀도우 복사본 누락

가장 오래된 섀도우 복사본은 다음 상황에서 삭제됩니다.

- 500개의 섀도우 복사본이 있을 때, 섀도우 복사본에 할당된 스토리지 볼륨의 남은 공간에 관계없이 다음 섀도우 복사본이 가장 오래된 섀도우 복사본을 대체합니다.
- 구성된 최대 섀도우 복사본 저장 용량에 도달하면 섀도우 복사본이 500개 미만이더라도 가장 오래된 섀도우 복사본 하나 이상이 다음 섀도우 복사본으로 대체됩니다.

두 결과 모두 예상된 동작입니다. 섀도우 복사본에 할당된 스토리지가 충분하지 않은 경우, 할당 스토리지를 늘리는 것을 고려하세요.

모든 섀도우 복사본 누락

파일 시스템의 I/O 성능 용량이 충분하지 않으면(예를 들어, HDD 스토리지가 사용 중이거나, HDD 스토리지의 버스트 용량이 부족하여) Windows Server가 사용할 수 있는 I/O 성능 용량으로 섀도우 복사본을 유지할 수 없어 Windows Server에서 모든 섀도우 복사본이 삭제될 수 있습니다. 이 문제를 방지하려면 다음 권장 사항을 고려하세요.

- HDD 스토리지를 사용하는 경우 Amazon FSx 콘솔 또는 Amazon FSx API를 사용하여 SSD 스토리지를 사용하도록 전환하십시오. 자세한 정보는 스토리지 유형 관리을 참조하세요.
- 파일 시스템의 처리량 용량을 예상 워크로드의 3배로 증가시키세요.
- 파일 시스템에 구성된 최대 섀도 복사본 스토리지 용량 외에 최소 320MB의 여유 공간이 있어야 합니다.
- 파일 시스템이 유휴 상태일 것으로 예상될 때 섀도우 복사본 일정을 만드세요.

자세한 정보는 섀도우 복사본에 대한 파일 시스템 권장 사항을 참조하세요.

최근에 복원되거나 업데이트된 파일 시스템에서 Amazon FSx 백업 생성 또는 섀도우 복사본 액세스 불가

이는 예상된 동작입니다. Amazon FSx는 최근에 복원된 파일 시스템에 섀도우 복사본 상태를 재구축하며, 재구축하는 동안에는 섀도우 복사본 또는 백업에 대한 액세스를 허용하지 않습니다.

파일 시스템 성능 문제 해결

파일 시스템 성능은 파일 시스템으로 이동하는 트래픽, 파일 시스템 프로비저닝 방법, 활성화된 데이터 중복 제거 또는 섀도우 복사본과 같은 기능 등 여러 요인에 따라 달라집니다. 파일 시스템 성능 이해에 대한 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

주제

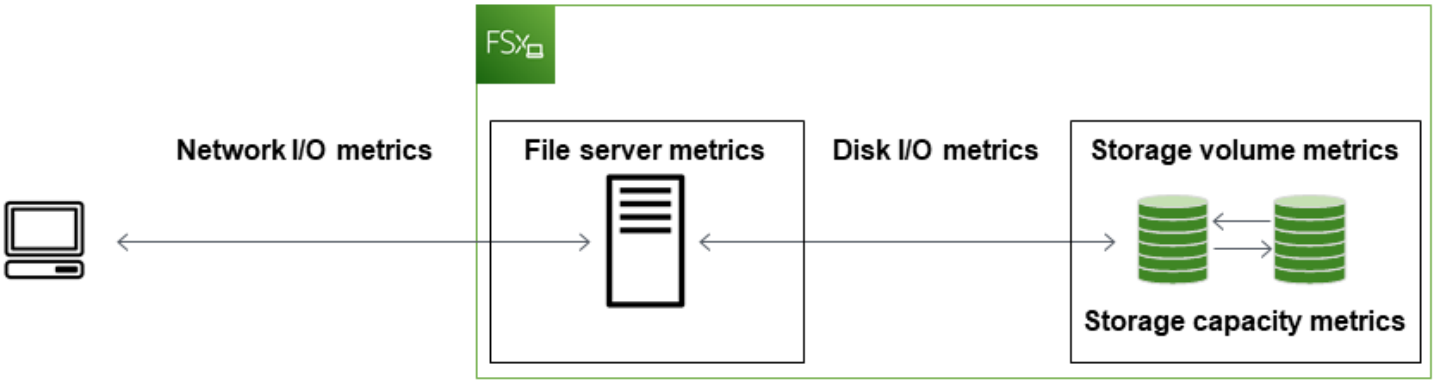
- 파일 시스템의 처리량 및 IOPS 한도는 어떻게 결정하나요?
- 네트워크 I/O와 디스크 I/O의 차이는 무엇인가요? 네트워크 I/O가 디스크 I/O와 다른 이유는 무엇인가요?
- 네트워크 I/O가 낮은데도 CPU 또는 메모리 사용량이 높은 이유는 무엇인가요?
- 버스팅은 무엇인가요? 파일 시스템에서 사용하는 버스팅의 양은 얼마인가요? 버스트 크레딧이 소진되면 어떻게 되나요?
- 모니터링 및 성능 페이지에 경고가 표시됩니다. 파일 시스템 구성을 변경해야 하나요?
- 지표가 일시적으로 누락되었는데 걱정해야 하나요?

파일 시스템의 처리량 및 IOPS 한도는 어떻게 결정하나요?

파일 시스템의 처리량과 IOPS 제한을 보려면 프로비저닝 처리량 용량에 따른 성능 수준을 보여주는 테이블을 참조하세요.

네트워크 I/O와 디스크 I/O의 차이는 무엇인가요? 네트워크 I/O가 디스크 I/O와 다른 이유는 무엇인가요?

Amazon FSx 파일 시스템은 파일 시스템에 액세스하는 클라이언트에게 네트워크를 통해 데이터를 제공하는 하나 이상의 파일 서버를 포함합니다. 이것이 네트워크 I/O입니다. 파일 서버에 가장 자주 액세스하는 데이터의 성능을 향상하기 위한 빠른 인 메모리 캐시가 있습니다. 또한 파일 서버는 파일 시스템 데이터를 호스팅하는 스토리지 볼륨으로 트래픽을 유도합니다. 이것이 디스크 I/O입니다. 다음 다이어그램은 Amazon FSx 파일 시스템의 네트워크 I/O 및 디스크 I/O를 보여줍니다.



자세한 정보는 Amazon을 통한 지표 모니터링 CloudWatch을 참조하세요.

네트워크 I/O가 낮은데도 CPU 또는 메모리 사용량이 높은 이유는 무엇인가요?

파일 서버 CPU 및 메모리 사용량은 구동 중인 네트워크 트래픽뿐만 아니라 파일 시스템에서 활성화한 기능에 따라 달라집니다. 해당 기능을 구성 및 스케줄링 방법이 CPU 및 메모리 사용량에 영향을 미칠 수 있습니다.

진행 중인 데이터 중복 제거 작업은 메모리를 소비할 수 있습니다. 중복 제거 작업 구성을 수정하여 메모리 요구량을 줄일 수 있습니다. 예를 들어, 최적화를 특정 파일 유형 또는 폴더에서 실행하도록 제한하거나, 최적화를 위한 최소 파일 크기 및 기간을 설정할 수 있습니다. 또한 파일 시스템의 부하가 최소인 유휴 기간에 데이터 중복 제거 작업이 실행되도록 구성하는 것을 권장합니다. 자세한 정보는 데이터 중복 제거을 참조하세요.

액세스 기반 열거를 활성화한 경우, 최종 사용자가 파일 공유를 보거나 나열할 때, 또는 스토리지 규모 조정 작업의 최적화 단계에서 CPU 사용량이 높아질 수 있습니다. 자세한 내용은 Microsoft 스토리지 설명서에서 네임스페이스에서 액세스 기반 열거 활성화를 참조하세요.

버스팅은 무엇인가요? 파일 시스템에서 사용하는 버스팅의 양은 얼마인가요? 버스트 크레딧이 소진되면 어떻게 되나요?

파일 기반 워크로드는 일반적으로 변동이 심하며, 버스트 간 유휴 시간이 있고, 집중적으로 단기간 높은 I/O가 발생하는 것이 특징입니다. 이런 유형의 워크로드를 지원하기 위해 Amazon FSx는 파일 시스템이 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 사용량을 기준으로 처리량과 IOPS를 할당합니다. 파일 시스템은 처리량과 IOPS 사용량이 기준 제한 미만일 때 크레딧을 적립하고, 기준 제

한을 넘는(최대 버스트 제한까지) 버스트 시 필요에 따라 크레딧을 사용할 수 있습니다. 파일 시스템의 버스트 제한 및 기간에 대한 자세한 내용은 FSx for Windows File Server 성능 섹션을 참조하세요.

모니터링 및 성능 페이지에 경고가 표시됩니다. 파일 시스템 구성을 변경해야 하나요?

모니터링 및 성능 페이지에는 파일 시스템 구성 방식에 따라 최근 워크로드 수요가 결정된 리소스 제한에 근접하거나 초과했을 때를 나타내는 경고가 있습니다. 권장 조치를 취하지 않으면 워크로드에 맞게 파일 시스템이 제대로 프로비저닝되지 않을 수 있지만, 반드시 구성을 변경해야 하는 것은 아닙니다.

경고를 일으킨 워크로드가 비정상적이어서 계속될 것으로 예상되지 않는 경우에는 아무 조치 없이 향후 사용량을 면밀히 모니터링하는 것이 안전할 수 있습니다. 그러나 경고를 일으킨 워크로드가 일반적이고 계속 또는 더 심해질 것으로 예상되는 경우, 권장 조치에 따라 파일 서버 성능을 높이거나(처리량 용량을 늘리거나, 스토리지 용량을 늘리거나, HDD에서 SSD 스토리지로 전환) 스토리지 볼륨 성능을 높이는 것을 권장합니다.

> **Note**
>
> 특정 파일 시스템 이벤트는 디스크 I/O 성능 리소스를 소비하여 잠재적으로 성능 경고를 유발할 수 있습니다. 예:
>
> - 스토리지 용량 증가 및 파일 시스템 성능에 설명된 대로 스토리지 용량 확장의 최적화 단계에서 디스크 처리량이 증가할 수 있습니다.
> - 다중 AZ 파일 시스템의 경우 처리량 용량 확장, 하드웨어 교체 또는 가용 영역 중단과 같은 이벤트로 인해 자동 장애 조치 및 페일백 이벤트가 발생합니다. 이 기간 동안 발생하는 모든 데이터 변경 사항은 기본 및 보조 파일 서버 간에 동기화되어야 하며, Windows Server는 디스크 I/O 리소스를 소비할 수 있는 데이터 동기화 작업을 실행합니다. 자세한 정보는 처리량 용량 관리을 참조하세요.

지표가 일시적으로 누락되었는데 걱정해야 하나요?

파일 시스템 유지 관리, 인프라 구성 요소 교체, 가용 영역을 사용할 수 없는 경우, 단일 AZ 파일 시스템을 사용할 수 없게 됩니다. 이 기간에는 지표를 사용할 수 없습니다.

다중 AZ 배포에서 Amazon FSx는 자동으로 서로 다른 가용 영역에 예비 파일 서버를 프로비저닝하고 유지합니다. Amazon FSx는 파일 시스템 유지 관리 또는 예상치 못한 서비스 중단 시 보조 파일 서버로 자동 장애 조치를 수행하여 수동으로 개입하지 않고 데이터에 계속 액세스할 수 있습니다. 파일 시스템이 장애 조치되고 페일백되는 짧은 기간 동안에는 지표를 일시적으로 사용할 수 없게 될 수 있습니다.

추가 정보

이 섹션에서는 지원되지만 사용 중단된 Amazon FSx 기능에 대한 참조를 제공합니다.

주제

사용자 지정 백업 일정 설정

파일 시스템에 대한 사용자 지정 백업 일정을 설정하는 AWS Backup 데 사용하는 것이 좋습니다. 여기에 제공된 정보는 백업을 사용할 때보다 더 자주 백업을 예약해야 하는 경우 AWS Backup참조용입니다.

활성화된 경우 Amazon FSx for Windows File Server는 일별 백업 기간 동안 하루에 한 번 파일 시스템을 자동으로 백업합니다. Amazon FSx는 이러한 자동 백업에 대해 사용자가 지정한 보존 기간을 적용합니다. 또한 사용자 시작 백업을 지원하므로 언제든지 백업할 수 있습니다.

다음에서 사용자 지정 백업 예약을 배포하기 위한 리소스 및 구성을 찾을 수 있습니다. 사용자 지정 백업 예약은 사용자가 정의한 사용자 지정 일정에 따라 Amazon FSx 파일 시스템에서 사용자 시작 백업을 수행합니다. 6시간에 한 번, 일주일에 한 번 등을 예로 들 수 있습니다. 또한 이 스크립트는 지정된 보존 기간보다 오래된 백업을 삭제하도록 구성합니다.

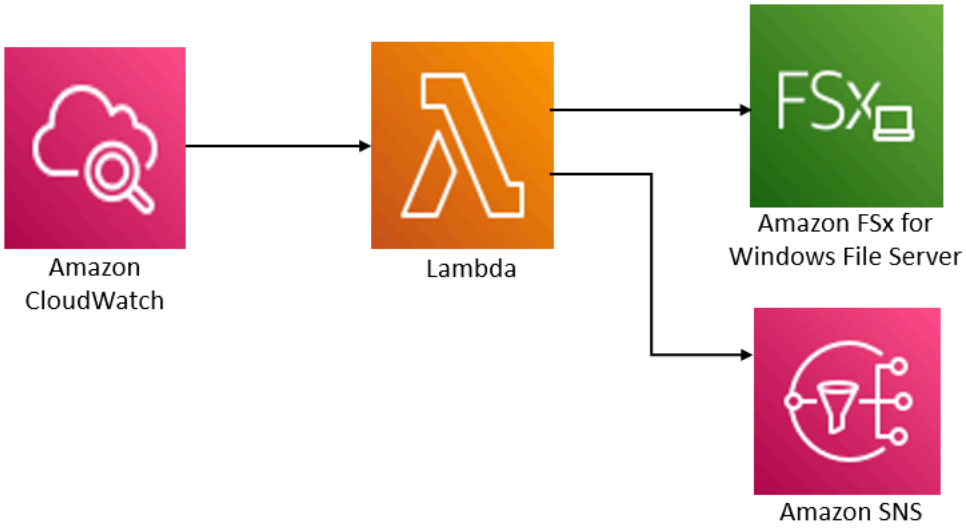
솔루션은 필요한 모든 구성 요소를 자동으로 배포하고 다음 파라미터를 사용합니다.

- 파일 시스템.
- 백업 수행을 위한 CRON 일정 패턴
- 백업 보존 기간(일 단위)
- 백업 이름 태그

CRON 스케줄 패턴에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 규칙에 대한 스케줄 표현식을 참조하십시오.

아키텍처 개요

이 솔루션을 배포하면 AWS 클라우드에 다음과 같은 리소스가 빌드됩니다.



이 솔루션은 다음 작업을 수행합니다.

1. AWS CloudFormation 템플릿은 CloudWatch 이벤트, Lambda 함수, Amazon SNS 대기열 및 IAM 역할을 배포합니다. IAM 역할은 Lambda 함수에 Amazon FSx API 작업을 호출할 수 있는 권한을 부여합니다.
2. CloudWatch 이벤트는 초기 배포 시 사용자가 CRON 패턴으로 정의한 일정에 따라 실행됩니다. 이 이벤트는 Amazon FSx `CreateBackup` API 작업을 호출하여 백업을 시작하는 솔루션의 백업 관리자 Lambda 함수를 호출합니다.
3. 백업 관리자는 `DescribeBackups`를 사용하여 지정된 파일 시스템에 대해 사용자가 시작한 기존 백업 목록을 검색합니다. 그런 다음 초기 배포 시 지정한 보존 기간보다 오래된 백업을 삭제합니다.
4. 초기 배포 중에 알림을 받는 옵션을 선택하면 백업 관리자가 백업 성공 시 Amazon SNS 대기열에 알림 메시지를 보냅니다. 장애 발생 시 항상 알림이 전송됩니다.

AWS CloudFormation 템플릿

이 솔루션은 Amazon FSx 사용자 지정 백업 예약 솔루션의 배포를 자동화하는 AWS CloudFormation 데 사용합니다. 이 솔루션을 사용하려면 fsx-scheduled-backup.template 템플릿을 다운로드하십시오. AWS CloudFormation

배포 자동화

다음 절차는 이 사용자 지정 백업 예약 솔루션을 구성하고 배포합니다. 배포에는 약 5분이 소요됩니다. 시작하기 전에 계정에 아마존 가상 사설 클라우드 (Amazon VPC) 에서 실행되는 Amazon FSx 파일 시스템의 ID가 있어야 합니다. AWS 리소스 생성에 대한 자세한 내용은 윈도우 파일 서버용 Amazon FSx 시작하기 섹션을 참조하세요.

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

사용자 지정 백업 솔루션 스택 시작

1. AWS CloudFormation fsx-scheduled-backup.template 템플릿을 다운로드하십시오. 스택 생성에 대한 자세한 내용은 사용 설명서의 콘솔에서 AWS CloudFormation 스택 생성을 참조하십시오. AWS CloudFormationAWS CloudFormation

   > **Note**
   >
   > 기본적으로 이 템플릿은 미국 동부 (버지니아 북부) AWS 지역에서 시작됩니다. Amazon FSx는 현재 특정 지역에서만 사용할 수 있습니다. AWS 리전 Amazon FSx를 사용할 수 있는 AWS 리전에서 이 솔루션을 시작해야 합니다. 자세한 내용은 AWS 일반 참조의 AWS 리전 및 엔드포인트의 Amazon FSx 섹션을 참조하세요.

2. 파라미터의 경우 템플릿의 파라미터를 검토하고 파일 시스템의 필요에 맞게 수정합니다. 이 솔루션은 다음과 같은 기본값을 사용합니다.

파라미터	기본값	설명
Amazon FSx 파일 시스템 ID	기본값 없음	백업하려는 파일 시스템의 파일 시스템 ID
백업을 위한 CRON 일정 패턴.	0 0/4 * *? *	CloudWatch 이벤트 실행 일정, 새 백업 트리거, 보존 기간 외 이전 백업 삭제
백업 보존 기간(일)	30	사용자 시작 백업을 보존할 일수입니다. Lambda 함수는 이 일수보다 오래된 사용자 시작 백업을 삭제합니다.

파라미터	기본값	설명
백업 이름	사용자 예약 백업	Amazon FSx 관리 콘솔의 백업 이름 열에 표시되는 이러한 백업의 이름입니다.
백업 알림	예	백업이 시작되었을 때 알림을 받을지 여부를 선택합니다. 오류가 있는 경우 항상 알림이 전송됩니다.
이메일 주소	기본값 없음	SNS 알림을 구독하기 위한 이메일 주소

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 스택 상태를 볼 수 있습니다. 약 5분 후에 생성_완료 상태를 확인할 수 있습니다.

추가 옵션

이 솔루션으로 생성된 Lambda 함수를 사용하여 둘 이상의 Amazon FSx 파일 시스템에 대한 사용자 지정 예약 백업을 수행할 수 있습니다. 파일 시스템 ID는 이벤트에 대한 입력 JSON의 Amazon FSx 함수에 전달됩니다. CloudWatch Lambda 함수에 전달되는 기본 JSON은 다음과 같습니다. 여기서 `SuccessNotification` 및 값은 `FileSystemId` 스택을 시작할 때 지정된 파라미터에서 전달됩니다. AWS CloudFormation

```
{
 "start-backup": "true",
 "purge-backups": "true",
 "filesystem-id": "${FileSystemId}",
 "notify_on_success": "${SuccessNotification}"
}
```

추가 Amazon FSx 파일 시스템의 백업을 예약하려면 다른 이벤트 규칙을 CloudWatch 생성하십시오. 이렇게 하려면 이 솔루션에서 생성한 Lambda 함수를 대상으로 하는 일정 이벤트 소스를 사용합니다. 입력 구성에서 상수(JSON 텍스트)를 선택합니다. JSON 입력의 경우 `${FileSystemId}` 대신 백업할 Amazon FSx 파일 시스템의 파일 시스템 ID로 대체하면 됩니다. 또한 위의 JSON에서 `${SuccessNotification}` 대신 `Yes` 또는 `No`를 사용할 수 있습니다.

수동으로 생성한 추가 CloudWatch 이벤트 규칙은 Amazon FSx 사용자 지정 예약 백업 솔루션 스택의 일부가 아닙니다. AWS CloudFormation 따라서 스택을 삭제해도 해당 스택은 제거되지 않습니다.

Microsoft Distributed File System 복제 사용

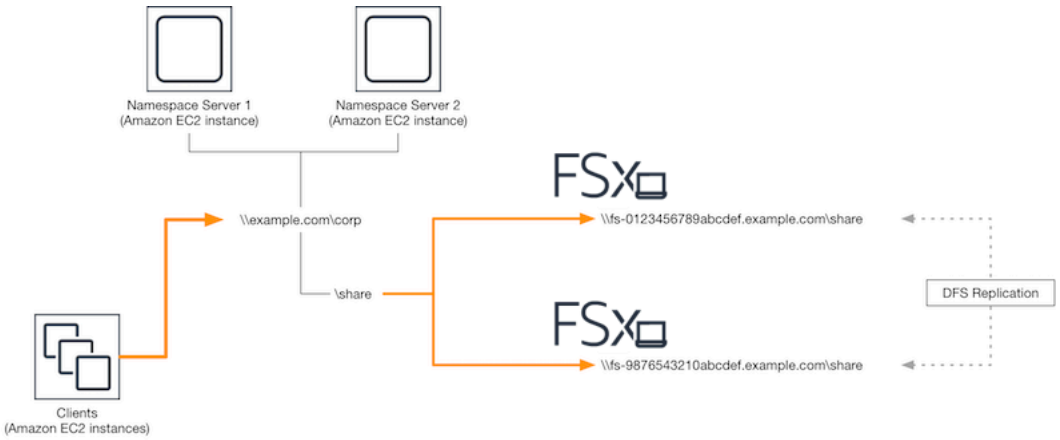
> **Note**
>
> FSx for Windows File Server의 고가용성을 구현하려면 Amazon FSx 다중 AZ를 사용하는 것이 좋습니다. Amazon FSx 다중 AZ에 대한 자세한 내용은 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템 섹션을 참조하세요.

Amazon FSx는 Microsoft Distributed File System(DFS)을 통해 여러 가용 영역(AZ)에 파일 시스템을 배포하여 다중 AZ 가용성과 내구성을 확보할 수 있도록 지원합니다. DFS 복제를 사용하면 두 파일 시스템 간에 데이터를 자동으로 복제할 수 있습니다. DFS 네임스페이스를 사용하면 한 파일 시스템을 기본 파일 시스템으로 구성하고 다른 파일 시스템을 대기 파일 시스템으로 구성할 수 있으며, 기본 파일 시스템이 응답하지 않을 경우 대기 시스템으로 자동 장애 조치를 수행할 수 있습니다.

DFS 복제를 사용하기 전에 다음 단계를 수행합니다.

- Amazon FSx 시작하기의 Step 8에 설명된 대로 보안 그룹을 설정합니다.
- 지역 내의 서로 다른 AZ에 두 개의 Amazon FSx 파일 시스템을 생성합니다. AWS 파일 시스템 만들기에 대한 자세한 내용은 파일 공유에 데이터 쓰기 섹션을 참조하세요.
- 두 파일 시스템이 동일한 AWS Directory Service for Microsoft Active Directory에 있어야 합니다.
- 파일 시스템이 생성되면 추후 사용을 위해 파일 시스템 ID를 기록해 둡니다.

다음 주제에서는 Amazon FSx를 사용하여 AZ 간에 DFS 복제 및 DFS 네임스페이스 장애 조치를 설정하고 사용하는 방법에 대해 설명합니다.



DFS 복제 설정

DFS 복제를 사용하면 두 Amazon FSx 파일 시스템 간에 데이터를 자동으로 복제할 수 있습니다. 이 복제는 양방향으로 이루어지므로 한 파일 시스템에 쓸 수 있고 변경 내용은 다른 파일 시스템에 복제됩니다.

> **Important**
>
> FSx for Windows File Server 파일 시스템에서 DFS 복제를 구성하는 데 Microsoft Windows 관리 도구(dfsmgmt.msc)의 DFS 관리 UI를 사용할 수 없습니다.

DFS 복제 설정(스크립트 작성)

1. 인스턴스를 시작하고 Amazon FSx 파일 시스템에 조인한 Microsoft Active Directory에 인스턴스를 연결하여 DFS 관리 프로세스를 시작합니다. 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 Active Directory 사용자로 인스턴스에 연결합니다. AWS 관리형 AD에서는 이 그룹을 AWS 위임된 FSx 관리자라고 합니다. 자체 관리형 Microsoft AD에서는 이 그룹을 도메인 관리자 또는 생성 시 제공한 관리자 그룹의 사용자 지정 이름이라고 합니다.

   또한 이 사용자는 DFS 관리 권한이 위임된 그룹의 구성원이어야 합니다. AWS 관리형 AD에서는 이 그룹을 AWS 위임 분산 파일 시스템 관리자라고 합니다. 자체 관리형 AD에서 이 사용자는 도메인 관리자 또는 DFS 관리 권한을 위임받은 다른 그룹의 구성원이어야 합니다.

자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.

3. FSX-DFSR-Setup.ps1 스크립트를 PowerShell 다운로드하십시오.
4. 시작 메뉴를 열고 입력합니다. PowerShell 목록에서 Windows를 선택합니다 PowerShell.
5. 지정된 다음 매개 변수를 사용하여 PowerShell 스크립트를 실행하여 두 파일 시스템 간에 DFS 복제를 설정합니다.

   - DFS 복제 그룹 및 폴더의 이름
   - 파일 시스템에 복제하려는 폴더의 로컬 경로(예: Amazon FSx 파일 시스템에 포함된 기본 공유의 경우 `D:\share`)
   - 사전 필수 단계에서 생성한 기본 및 대기 Amazon FSx 파일 시스템의 DNS 이름

   Example

   ```
   FSx-DFSr-Setup.ps1 -group Group -folder Folder -path ContentPath -
   primary FSxFileSystem1-DNS-Name -standby FSxFileSystem2-DNS-Name
   ```

DFS 복제 설정(단계별)

1. 인스턴스를 시작하고 Amazon FSx 파일 시스템에 조인한 Microsoft Active Directory에 인스턴스를 연결하여 DFS 관리 프로세스를 시작합니다. 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 Active Directory 사용자로 인스턴스에 연결합니다. AWS 관리형 AD에서는 이 그룹을 AWS 위임된 FSx 관리자라고 합니다. 자체 관리형 Microsoft AD에서는 이 그룹을 도메인 관리자 또는 생성 시 제공한 관리자 그룹의 사용자 지정 이름이라고 합니다.

   또한 이 사용자는 DFS 관리 권한이 위임된 그룹의 구성원이어야 합니다. AWS 관리형 AD에서는 이 그룹을 AWS 위임 분산 파일 시스템 관리자라고 합니다. 자체 관리형 AD에서 이 사용자는 도메인 관리자 또는 DFS 관리 권한을 위임받은 다른 그룹의 구성원이어야 합니다.

   자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 시작 메뉴를 열고 를 입력합니다 PowerShell. 목록에서 Windows를 선택합니다 PowerShell.
4. 아직 DFS 관리 도구가 설치되어 있지 않다면 다음과 같은 명령으로 인스턴스에 설치합니다.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

5. PowerShell 프롬프트에서 다음 명령을 사용하여 DFS 복제 그룹 및 폴더를 생성합니다.

```
$Group = "Name of the DFS Replication group"
$Folder = "Name of the DFS Replication folder"

New-DfsReplicationGroup -GroupName $Group
New-DfsReplicatedFolder -GroupName $Group -FolderName $Folder
```

6. 다음 명령을 사용하여 각 파일 시스템과 연결된 Active Directory 컴퓨터 이름을 확인합니다.

```
$Primary = "DNS name of the primary FSx file system"
$Standby = "DNS name of the standby FSx file system"

$C1 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Primary'").Name
$C2 = (Get-ADObject -Filter "objectClass -eq 'Computer' -and ServicePrincipalName -
eq 'HOST/$Standby'").Name
```

7. 다음 명령을 사용하여 생성한 DFS 복제 그룹의 구성원으로 파일 시스템을 추가합니다.

```
Add-DfsrMember -GroupName $Group -ComputerName $C1
Add-DfsrMember -GroupName $Group -ComputerName $C2
```

8. 다음 명령을 사용하여 각 파일 시스템의 로컬 경로(예: `D:\share`)를 DFS 복제 그룹에 추가합니다. 이 절차에서는 *file system 1*이 기본 구성원 역할을 합니다. 즉, 해당 내용이 처음에 다른 파일 시스템에 동기화됩니다.

```
$ContentPath1 = "Local path to the folder you want to replicate on file system 1"
$ContentPath2 = "Local path to the folder you want to replicate on file system 2"

Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath1
 -ComputerName $C1 -PrimaryMember $True
Set-DfsrMembership -GroupName $Group -FolderName $Folder -ContentPath $ContentPath2
 -ComputerName $C2 -PrimaryMember $False
```

9. 다음 명령을 사용하여 파일 시스템 간 연결을 추가합니다.

```
Add-DfsrConnection -GroupName $Group -SourceComputerName $C1 -
DestinationComputerName $C2
```

몇 분 안에 두 파일 시스템 모두 `ContentPath`가 지정된 이전 항목의 내용을 동기화하기 시작할 것입니다.

장애 조치를 위한 DFS 네임스페이스 설정

DFS 네임스페이스를 사용하여 한 파일 시스템을 기본 파일 시스템으로 취급하고 다른 파일 시스템을 대기 파일 시스템으로 취급할 수 있습니다. 이렇게 하면 기본 파일 시스템이 응답하지 않는 경우 대기 파일 시스템으로 자동 장애 조치를 구성할 수 있습니다. DFS 네임스페이스를 사용하면 여러 서버의 공유 폴더를 단일 네임스페이스로 그룹화하여 단일 폴더 경로를 통해 여러 서버에 파일을 저장할 수 있습니다. DFS 네임스페이스는 DFS 네임스페이스 서버에서 관리되어 DFS 네임스페이스 폴더를 매핑하는 컴퓨팅 인스턴스를 적절한 파일 서버로 보냅니다.

장애 조치를 위한 DFS 네임스페이스 설정(UI)

1. 아직 DFS 네임스페이스 서버를 실행하고 있지 않은 경우 Setup-DFSN-servers.template 템플릿을 사용하여 가용성이 높은 DFS 네임스페이스 서버 한 쌍을 시작하십시오. AWS CloudFormation 스택 생성에 대한 자세한 내용은 사용 설명서의 콘솔에서 스택 생성을 참조하십시오. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. AWS 위임된 관리자 그룹의 사용자로 이전 단계에서 실행한 DFS 네임스페이스 서버 중 하나에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. DFS 관리 콘솔을 엽니다. 시작 메뉴를 열고 `dfsmgmt.msc`를 실행합니다. 그러면 DFS 관리 GUI 도구가 열립니다.
4. 작업에서 새 네임스페이스를 선택하고 서버용으로 시작한 첫 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력한 후 다음을 선택합니다.
5. 이름에는 만들려는 네임스페이스(예: **`corp`**)를 입력합니다.
6. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정합니다. 다음을 선택합니다.
7. 기본 도메인 기반 네임스페이스 옵션을 선택한 상태로 두고 Windows Server 2008 모드 사용 옵션을 선택한 상태로 두고 다음을 선택합니다.

   > **Note**
   >
   > Windows Server 2008 모드는 네임스페이스에 사용할 수 있는 최신 옵션입니다.

8. 네임스페이스 설정을 검토한 다음 생성을 선택합니다.
9. 탐색 표시줄의 네임스페이스에서 새로 만든 네임스페이스를 선택한 상태에서 작업, 네임스페이스 서버 추가 순으로 선택합니다.

10. 네임 스페이스 서버에는 시작한 두 번째 DFS 네임스페이스 서버의 컴퓨터 이름을 입력합니다.
11. 설정 편집을 선택하고 요구 사항에 따라 적절한 권한을 설정한 다음 확인을 선택합니다.
12. 추가를 선택하고 폴더 대상 경로에 기본 Amazon FSx 파일 시스템에 있는 파일 공유의 UNC 이름(예: *fs-0123456789abcdef0*.example.com*share*)을 입력한 다음 확인을 선택합니다.
13. 추가를 선택하고 폴더 대상 경로에 대기 Amazon FSx 파일 시스템에 있는 파일 공유의 UNC 이름(예: *fs-fedbca9876543210f*.example.com*share*)을 입력한 다음 확인을 선택합니다.
14. 새 폴더 창에서 확인을 선택합니다. 네임스페이스 아래에 두 개의 폴더 대상이 있는 새 폴더가 생성됩니다.
15. 네임스페이스에 추가할 각 파일 공유에 대해 마지막 세 단계를 반복합니다.

장애 조치를 위한 DFS 네임스페이스 설정하기 () PowerShell

1. 아직 DFS 네임스페이스 서버를 실행하고 있지 않은 경우 Setup-DFSN-servers.template 템플릿을 사용하여 가용성이 높은 DFS 네임스페이스 서버 한 쌍을 시작하십시오. AWS CloudFormation 스택 생성에 대한 자세한 내용은 사용 설명서의 콘솔에서 스택 생성을 참조하십시오. AWS CloudFormation AWS CloudFormation AWS CloudFormation
2. AWS 위임 관리자 그룹의 사용자로 이전 단계에서 시작한 DFS 네임스페이스 서버 중 하나에 연결합니다. 자세한 내용은 Amazon EC2 사용 설명서의 Windows 인스턴스에 연결을 참조하십시오.
3. 시작 메뉴를 열고 를 입력합니다 PowerShell. Windows가 경기 목록에 PowerShell 나타납니다.
4. PowerShellWindows용 컨텍스트 메뉴 (마우스 오른쪽 버튼 클릭) 를 열고 [관리자 권한으로 실행]을 선택합니다.
5. 아직 DFS 관리 도구가 설치되어 있지 않다면 다음과 같은 명령으로 인스턴스에 설치합니다.

```
Install-WindowsFeature RSAT-DFS-Mgmt-Con
```

6. 기존 DFS 네임스페이스가 아직 없는 경우 다음 명령을 사용하여 새 DFS 네임스페이스를 만들 수 있습니다. PowerShell

```
$NSS1 = computer name of the 1st DFS Namespace server
$NSS2 = computer name of the 2nd DFS Namespace server

$DNSRoot = fully qualified Active Directory domain name (e.g. mydomain.com)
$Namespace = Namespace name you want to use
$Folder = Folder path you want to use within the Namespace
$FS1FolderTarget = Share path to Folder Target on File System 1
$FS2FolderTarget = Share path to Folder Target on File System 2
```

```
$NSS1,$NSS2 | ForEach-Object { Invoke-Command -ComputerName $_ -ScriptBlock { mkdir
 “C:\DFS\${using:Namespace}”;
New-SmbShare -Name ${using:Namespace} -Path “C:\DFS\${using:Namespace}” } }

New-DfsnRoot -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS1}.${DNSRoot}\
${Namespace}" -Type DomainV2
New-DfsnRootTarget -Path "\\${DNSRoot}\${Namespace}" -TargetPath "\\${NSS2}.
${DNSRoot}\${Namespace}"
```

7. DFS 네임스페이스 내에 폴더를 만들려면 다음 명령을 사용할 수 있습니다. PowerShell 이렇게 하면 기본적으로 폴더에 액세스하는 컴퓨팅 인스턴스를 기본 Amazon FSx 파일 시스템으로 보내는 폴더가 생성됩니다.

```
$FS1 = DNS name of primary FSx file system
New-DfsnFolder -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\${FS1}\
${FS1FolderTarget}” -EnableTargetFailback $True -ReferralPriorityClass GlobalHigh
```

8. 대기 Amazon FSx 파일 시스템을 동일한 DFS 네임스페이스 폴더에 추가합니다. 폴더에 액세스하는 컴퓨팅 인스턴스는 기본 Amazon FSx 파일 시스템에 연결할 수 없는 경우 이 파일 시스템으로 돌아갑니다.

```
$FS2 = DNS name of secondary FSx file system
New-DfsnFolderTarget -Path “\\${DNSRoot}\${Namespace}\${Folder}" -TargetPath “\\
${FS2}\${FS2FolderTarget}”
```

이제 앞에서 지정한 DFS 네임스페이스 폴더의 원격 경로를 사용하여 컴퓨팅 인스턴스에서 데이터에 액세스할 수 있습니다. 이렇게 하면 컴퓨팅 인스턴스를 기본 Amazon FSx 파일 시스템으로(기본 파일 시스템이 응답하지 않는 경우 대기 파일 시스템으로) 보냅니다.

예를 들어, 시작 메뉴를 열고 `PowerShell`을 입력합니다. 목록에서 `Windows PowerShell`을 선택하고 다음 명령을 실행합니다.

```
net use Z: \\${DNSRoot}\${Namespace}\${Folder} /persistent:yes
```

Maintenance Windows 및 FSx 다중 AZ 작업

다중 AZ 파일 시스템 배포의 고가용성을 보장하려면 다중 AZ 배포에서 두 Amazon FSx 파일 시스템에 대해 중복되지 않는 유지 관리 기간을 선택하는 것이 좋습니다. 이렇게 하면 시스템 유지 관리 기간 동안 애플리케이션과 사용자가 파일 데이터를 계속 사용할 수 있습니다.

> **Note**
>
> 파일 시스템으로 들어오고 나가는 DFS 복제 트래픽을 허용하려면 Amazon VPC 보안 그룹에 설명된 대로 VPC 보안 그룹 인바운드 및 아웃바운드 규칙을 추가해야 합니다.

문서 이력

- API 버전: 2018년 3월 1일
- 최신 설명서 업데이트: 2024년 1월 17일

아래 표에 Amazon FSx Windows 사용 설명서의 주요 변경 사항이 설명되어 있습니다. 설명서 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하시면 됩니다.

변경 사항	설명	날짜
처리 용량이 4GB/s 이상인 파일 시스템에서 더 높은 수준의 IOPS에 대한 지원이 추가되었습니다.	Windows File Server용 FSx는 처리 용량이 4GB/s 이상인 파일 시스템의 경우 최대 IOPS를 130K에서 150K로, 처리 용량이 6GB/s 이상인 파일 시스템의 경우 175K에서 20K로, 처리 용량이 9GB/s 이상인 파일 시스템의 경우 26만 IOPS에서 30만, 처리 용량이 12GB/s인 파일 시스템의 경우 350K에서 400K로 늘리고 있습니다. 또는 그 이상. 자세한 내용은 FSx for Windows File Server 성능을 참조하세요.	2024년 1월 17일
Amazon FSx는 AmazonF, AmazonF, SxFullAccess AmazonF, AmazonF 및 SxConsoleFullAccess AmazonF 관리형 정책을 업데이트했습니다. SxReadOnlyAccess SxConsole ReadOnlyAccess SxService RolePolicy AWS	Amazon FSx는 AmazonF, AmazonF, SxFullAccess AmazonF, SxConsole FullAccess AmazonF 및 AmazonF SxReadOnlyAccess 정책을 업데이트하여 권한을 추가했습니다. SxConsole ReadOnlyAccess SxService RolePolicy `ec2:GetSecurityGroupsForVpc` 자세한 내용은 관리형 정책에	2024년 1월 9일

	대한 Amazon FSx 업데이트를 AWS 참조하십시오.	
Amazon FSx는 AmazonF 및 SxFullAccess AmazonF 관리형 정책을 업데이트했습니다. SxConsoleFullAccess AWS	Amazon FSx는 SxFullAccess AmazonF 및 SxConsoleFullAccess AmazonF 정책을 업데이트하여 작업을 추가했습니다. `ManageCrossAccountDataReplication` 자세한 내용은 관리형 정책에 대한 Amazon FSx 업데이트를 AWS 참조하십시오.	2023년 12월 20일
Amazon FSx는 AmazonF 및 SxFullAccess AmazonF 관리형 정책을 업데이트했습니다. SxConsoleFullAccess AWS	Amazon FSx는 SxFullAccess AmazonF 및 SxConsoleFullAccess AmazonF 정책을 업데이트하여 권한을 추가했습니다. `fsx:CopySnapshotAndUpdateVolume` 자세한 내용은 관리형 정책에 대한 Amazon FSx 업데이트를 AWS 참조하십시오.	2023년 11월 26일
Amazon FSx는 AmazonF 및 SxFullAccess AmazonF 관리형 정책을 업데이트했습니다. SxConsoleFullAccess AWS	Amazon FSx는 AmazonF 및 SxFullAccess AmazonF 정책을 업데이트하여 및 권한을 SxConsoleFullAccess 추가했습니다. `fsx:DescribeSharedVPCConfiguration` `fsx:UpdateSharedVPCConfiguration` 자세한 내용은 관리형 정책에 대한 Amazon FSx 업데이트를 AWS 참조하십시오.	2023년 11월 14일

파일 시스템 스토리지 유형 업데이트 지원 추가	FSx for Windows File Server 파일 시스템은 이제 HDD 스토리지 유형에서 SSD 스토리지 유형으로의 업데이트를 지원합니다. 자세한 내용은 스토리지 유형 관리를 참조하세요.	2023년 8월 9일
최대 처리량 용량 증대를 위한 지원 추가	FSx for Windows File Server 파일 시스템은 이제 최대 12GBps의 처리량 용량을 지원합니다. 자세한 내용은 FSx for Windows File Server 성능을 참조하세요.	2023년 8월 9일
SSD IOPS 프로비저닝에 대한 지원 추가	FSx for Windows File Server 파일 시스템은 이제 스토리지 용량과 관계없이 최대 350,000 IOPS까지 SSD IOPS 프로비저닝을 지원합니다. 자세한 내용은 SSD IOPS 관리를 참조하세요.	2023년 8월 9일
Amazon FSx는 AmazonF 관리형 정책을 업데이트했습니다. SxServiceRolePolicy AWS	Amazon FSx가 `cloudwatch:PutMetricData` AmazonF의 권한을 업데이트했습니다. SxServiceRolePolicy 자세한 내용은 Amazon F를 참조하십시오. SxServiceRolePolicy	2023년 7월 24일
Amazon FSx는 AmazonF 관리형 정책을 업데이트했습니다. SxFullAccess AWS	Amazon FSx는 SxFullAccess AmazonF 정책을 업데이트하여 권한을 제거하고 특정 작업을 추가했습니다`fsx:*`. `fsx` 자세한 내용은 AmazonF 정책을 참조하십시오. SxFullAccess	2023년 7월 13일

Amazon FSx는 AmazonF 관리형 정책을 업데이트했습니다. SxConsoleFullAccess AWS	Amazon FSx는 SxConsole FullAccess AmazonF 정책을 업데이트하여 권한을 제거하고 특정 작업을 추가했습니다`fsx:*`. `fsx` 자세한 내용은 AmazonF 정책을 참조하십시오. SxConsoleFullAccess	2023년 7월 13일
Windows File Server용 Amazon FSx에 대한 새로운 CloudWatch 메트릭에 대한 지원이 추가되었습니다.	FSx for Windows File CloudWatch Server는 이제 파일 서버 및 스토리지 볼륨 성능과 용량 사용량을 모니터링하는 추가 메트릭을 제공합니다. 자세한 내용은 지표 및 측정기준을 참조하세요.	2022년 9월 22일
파일 시스템 성능 경고에 대한 지원 추가	Amazon FSx는 이제 지표 세트 CloudWatch 중 하나라도 이러한 지표에 대해 미리 정해진 임계값에 도달하거나 이를 초과할 경우 성능 및 모니터링 창에 경고를 표시합니다. 또한 각 경고는 파일 시스템 성능 개선을 위한 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 성능 경고 및 권장 사항을 참조하세요.	2022년 9월 22일

향상된 파일 시스템 성능 모니터링에 대한 지원 추가	FSx for Windows File Server 파일 시스템용 Amazon FSx 콘솔 파일 시스템 모니터링 대시보드에는 새로운 요약, 스토리지 및 성능 섹션이 포함되어 있습니다. 이 섹션에는 향상된 성능 모니터링을 제공하는 새로운 CloudWatch 지표의 그래프가 표시됩니다. 자세한 내용은 메트릭 모니터링을 참조하십시오 CloudWatch.	2022년 9월 22일
AWS PrivateLink 인터페이스 VPC 엔드포인트에 대한 지원이 추가되었습니다.	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
Amazon Kendra에 대한 지원 추가	이제 FSx for Windows File Server 파일 시스템을 Amazon Kendra의 데이터 소스로 사용하여 파일 시스템에 저장된 문서에 포함된 정보를 인덱싱하고 검색할 수 있습니다. 자세한 내용은 Amazon Kendra와 함께 FSx for Windows File Server 사용을 참조하세요.	2022년 3월 26일

파일 액세스 감사에 대한 지원 추가	이제 파일, 폴더 및 파일 공유에 대한 최종 사용자 액세스 감사를 활성화할 수 있습니다. 감사 이벤트 로그를 Amazon Logs 또는 Amazon CloudWatch Data Firehose 서비스에 전송하도록 선택할 수 있습니다. 자세한 내용은 파일 액세스 감사를 참조하세요.	2021년 6월 8일
백업 복사에 대한 지원 추가	이제 Amazon FSx를 사용하여 동일한 계정 내의 백업을 AWS 리전 다른 계정에 복사 (지역 간 사본) 하거나 AWS 동일한 계정 내 (지역 내 사본) 에 AWS 리전 복사할 수 있습니다. 자세한 내용은 백업 복사를 참조하세요.	2021년 4월 12일
파일 시스템의 스토리지 용량 자동 증가	AWS자체 개발한 사용자 지정 가능 AWS CloudFormation 템플릿을 사용하면 용량이 지정한 임계값에 도달하면 파일 시스템의 스토리지 용량을 자동으로 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 동적 증가 섹션을 참조하세요.	2021년 2월 17일

프라이빗이 아닌 IP 주소를 사용한 클라이언트 액세스에 대한 지원 추가	프라이빗이 아닌 IP 주소를 사용하는 온프레미스 클라이언트를 사용하여 FSx for Windows File Server 파일 시스템에 액세스할 수 있습니다. 자세한 내용은 지원되는 환경을 참조하세요. 프라이빗이 아닌 IP 주소를 사용하는 DNS 서버 및 AD 도메인 컨트롤러를 사용하여 FSx for Windows File Server 파일 시스템을 자체 관리형 Microsoft Active Directory에 조인할 수 있습니다. 자세한 내용은 자체 관리형 Microsoft Active Directory와 함께 Amazon FSx 사용을 참조하세요.	2020년 12월 17일
DNS 별칭 사용에 대한 지원 추가	이제 파일 시스템의 데이터에 액세스하는 데 사용할 수 있는 DNS 별칭을 FSx for Windows File Server 파일 시스템과 연결할 수 있습니다. 자세한 내용은 DNS 별칭 관리 및 연습 5: DNS 별칭을 사용하여 파일 시스템에 액세스를 참조하세요.	2020년 11월 9일
Amazon Elastic Container Service에 대한 지원 추가	이제 Amazon ECS와 함께 FSx for Windows File Server를 사용할 수 있습니다. 자세한 내용은 지원되는 클라이언트를 참조하세요.	2020년 11월 9일

Amazon FSx는 이제 다음과 통합되었습니다. AWS Backup	이제 기본 Amazon FSx 백업을 사용하는 AWS Backup 것 외에도 FSx 파일 시스템을 백업 및 복원하는 데 사용할 수 있습니다. 자세한 내용은 Amazon FSx에서 AWS Backup 사용을 참조하세요.	2020년 11월 9일
처리량 용량 확장에 대한 지원 추가	이제 처리량 요구 사항이 증가함에 따라 기존 FSx for Windows File Server 파일 시스템의 처리량 용량을 수정할 수 있습니다. 자세한 내용은 처리량 용량 관리를 참조하세요.	2020년 6월 1일
스토리지 용량 확장에 대한 지원 추가	이제 스토리지 요구 사항이 증가함에 따라 기존 FSx for Windows File Server 파일 시스템의 스토리지 용량을 늘릴 수 있습니다. 자세한 내용은 스토리지 용량 관리를 참조하세요.	2020년 6월 1일
하드 디스크 드라이브(HDD) 스토리지에 대한 지원 추가	FSx for Windows File Server를 사용할 때 HDD 스토리지는 가격 및 성능 유연성을 제공합니다. 자세한 내용은 Amazon FSx를 사용한 비용 최적화를 참조하세요.	2020년 3월 26일
를 사용하여 파일 전송에 대한 지원이 추가되었습니다. AWS DataSync	이제 Windows File Server용 FSx와 파일을 주고 받는 AWS DataSync 데 사용할 수 있습니다. 자세한 내용은 Windows File Server를 사용하여 Amazon FSx로 파일 마이그레이션을 참조하십시오. AWS DataSync	2020년 2월 4일

FSx for Windows File Server에서 추가 Windows 파일 시스템 관리 작업 지원 시작	이제 원격 관리용 Amazon FSx CLI를 사용하여 파일 공유에 대한 파일 공유, 데이터 중복 제거, 스토리지 할당량, 전송 중 암호화를 관리하고 관리할 수 있습니다. PowerShell 자세한 내용은 파일 시스템 관리를 참조하세요.	2019년 11월 20일
FSx for Windows File Server에서 네이티브 다중 AZ 지원 시작	FSx for Windows File Server용 다중 AZ 배포를 사용하면 여러 가용 영역(AZ)에 걸쳐 있는 고가용성의 파일 시스템을 보다 쉽게 만들 수 있습니다. 자세한 내용은 가용성 및 내구성: 단일 AZ 및 다중 AZ 파일 시스템을 참조하세요.	2019년 11월 20일
FSx for Windows File Server에서 사용자 세션 및 열린 파일 관리 지원 시작	이제 Microsoft Windows 고유의 공유 폴더 도구를 사용하여 FSx for Windows File Server 파일 시스템에서 사용자 세션과 열린 파일을 관리할 수 있습니다. 자세한 내용은 사용자 세션 및 열린 파일 관리를 참조하세요.	2019년 10월 17일
Amazon FSx에서 Microsoft Windows 섀도우 복사본 지원 시작	이제 FSx for Windows File Server 파일 시스템에 Windows 섀도우 복사본을 구성할 수 있습니다. 섀도우 복사본을 사용하면 파일을 이전 버전으로 복원하여 파일 변경 취소 및 파일 버전 비교를 쉽게 수행할 수 있습니다. 자세한 내용은 섀도우 복사본 작업을 참조하세요.	2019년 7월 31일

Amazon FSx에서 공유 Microsoft Active Directory 지원 시작	이제 Windows File Server 용 FSx 파일 AWS Managed Microsoft AD 시스템을 다른 VPC에 있거나 파일 시스템이 아닌 다른 디렉터리에 조인할 수 있습니다. AWS 계정 자세한 내용은 Active Directory 지원을 참조하세요.	2019년 6월 25일
Amazon FSx에서 향상된 Microsoft Active Directory 지원 시작	이제 FSx for Windows File Server 파일 시스템을 온프레미스 또는 클라우드의 자체 관리형 Microsoft Active Directory 도메인에 조인할 수 있습니다. 자세한 내용은 Active Directory 지원을 참조하세요.	2019년 6월 24일
Amazon FSx의 SOC 인증 준수	Amazon FSx는 SOC 인증을 준수하는 것으로 평가되었습니다. 자세한 내용은 보안 및 데이터 보호를 참조하세요.	2019년 5월 16일
VPN 및 리전 간 VPC 피어링 연결 지원에 관한 AWS Direct Connect 설명 추가	2019년 2월 22일 이후에 생성된 Amazon FSx 파일 시스템은 VPN 및 지역 간 VPC 피어링을 AWS Direct Connect 사용하여 액세스할 수 있습니다. 자세한 내용은 지원되는 액세스 방법을 참조하세요.	2019년 2월 25일
AWS Direct Connect, VPN 및 리전 간 VPC 피어링 연결 지원 추가	이제 온프레미스 리소스와, Amazon VPC 또는 AWS 계정의 리소스에서 Amazon FSx for Windows File Server 파일 시스템에 액세스할 수 있습니다. 자세한 내용은 지원되는 액세스 방법을 참조하세요.	2019년 2월 22일

이제 Amazon FSx 정식 출시	Amazon FSx for Windows File Server는 완전한 네이티브 Windows 파일 시스템이 지원하는 완전 관리형 Microsoft Windows 파일 서버를 제공합니다. Amazon FSx for Windows File Server는 엔터프라이즈 애플리케이션을 AWS로 쉽게 리프트 앤 시프트할 수 있는 기능, 성능 및 호환성을 제공합니다.	2018년 11월 28일

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.