Amazon S3 File Gateway 사용 설명서

AWS Storage Gateway

API 버전 2013-06-30

AWS Storage Gateway: Amazon S3 File Gateway 사용 설명서

Table of Contents

Amazon S3 File Gateway란 무엇입니까?

Amazon S3 File Gateway – Amazon S3 File Gateway는 Amazon Simple Storage Service(Amazon S3)에 대한 파일 인터페이스를 지원하고 서비스와 가상 소프트웨어 어플라이언스를 결합합니다. 이 조합을 사용하면 NFS(Network File System) 및 SMB(Server Message Block) 같은 업계 표준 파일 프로토콜을 사용하여 Amazon S3에서 객체를 저장하고 검색할 수 있습니다. VMware ESXi, Microsoft Hyper-V 또는 Linux 커널 기반 가상 머신(KVM)에서 실행되는 가상 머신(VM) 또는 선호하는 리셀러로부터 주문하는 하드웨어 어플라이언스로 온프레미스 환경에 게이트웨이를 배포합니다. Storage Gateway VM을의 VMware Cloud에 배포 AWS하거나 Amazon EC2의 AMI로 배포할 수도 있습니다. 이 게이트웨이를 통해 파일 또는 파일 공유 탑재 지점으로 S3 내 객체에 액세스할 수 있습니다. S3 File Gateway를 통해 다음 작업을 할 수 있습니다.

- NFS 버전 3 또는 4.1 프로토콜을 사용하여 파일을 직접 저장하고 가져올 수 있습니다.
- SMB 파일 시스템 버전 2 및 3 프로토콜을 사용하여 파일을 직접 저장하고 가져올 수 있습니다.
- 모든 AWS 클라우드 애플리케이션 또는 서비스에서 Amazon S3의 데이터에 직접 액세스할 수 있습니다.
- 수명 주기 정책, 교차 리전 복제 및 버전 관리를 통해 S3 데이터를 직접 관리할 수 있습니다. S3 File Gateway는 Amazon S3의 파일 시스템 탑재 지점이라고 할 수 있습니다.

S3 File Gateway는 Amazon S3 내 파일 스토리지를 간소화하고 업계 표준 파일 시스템 프로토콜을 통해 기존 애플리케이션에 통합되어 온프레미스 스토리지에 비용 효율적 대안을 제공합니다. 또한 로컬 캐시가 투명하게 이루어지므로 데이터에 액세스할 때 지연 시간이 짧습니다. S3 File Gateway는 송수신 데이터 전송을 관리하고 AWS, 네트워크 정체로부터 애플리케이션을 버퍼링하고, 데이터를 병렬로 최적화 및 스트리밍하고, 대역폭 소비를 관리합니다.

S3 File Gateway는 다음과 같은 다른 AWS 서비스와 통합됩니다.

- AWS Identity and Access Management (IAM)를 사용한 공통 액세스 관리
- AWS Key Management Service (AWS KMS)를 사용한 암호화
- Amazon CloudWatch(CloudWatch)를 사용한 모니터링
- 를 사용한 감사 AWS CloudTrail (CloudTrail)
- AWS Management Console 및 AWS Command Line Interface (AWS CLI)를 사용한 작업
- 비용 및 청구 관리

다음 설명서는 시작하기 섹션에서 모든 게이트웨이에 공통된 설정 정보를 다루고, 각 게이트웨이에 따른 설정을 설명하는 섹션도 제공합니다. 시작하기 섹션에서는 스토리지 게이트웨이를 배포, 활성화 및 구성하는 방법을 설명합니다. 관리 섹션에서는 게이트웨이와 리소스를 관리하는 방법에 대해 설명합니다.

- 에서는 S3 File Gateway를 생성하고 사용하는 방법에 관한 지침을 제공합니다. 또한 파일 공유를 생성하고 드라이브를 Amazon S3 버킷에 매핑하고 Amazon S3로 파일과 폴더를 업로드하는 방법을 설명합니다.

- 에서는 모든 게이트웨이 유형 및 리소스에 관리 작업을 수행하는 방법을 설명합니다.

이 설명서에서는 AWS Management Console을 사용하여 게이트웨이 작업을 수행하는 방법을 주로 설명합니다. 이러한 작업을 프로그래밍 방식으로 수행하려면 AWS Storage Gateway API 참조를 참조하세요.

Amazon S3 File Gateway 작동 방식

S3 File Gateway를 사용하려면 게이트웨이용 VM 이미지를 다운로드하는 것으로 시작합니다. 그런 다음에서 AWS Management Console 또는 Storage Gateway API를 통해 게이트웨이를 활성화합니다. 또한 Amazon EC2 이미지를 사용하여 S3 File Gateway를 생성할 수도 있습니다.

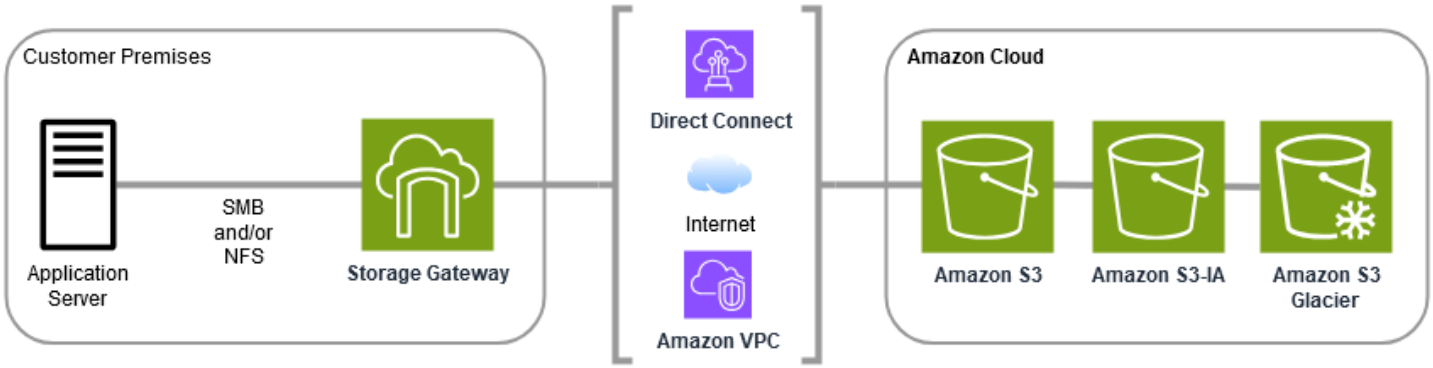
S3 File Gateway가 활성화된 후에는 파일 공유를 생성 및 구성한 후 이 공유를 Amazon S3(Amazon Simple Storage Service) 버킷에 연결합니다. 이렇게 하면 클라이언트에서도 NFS(Network File System) 또는 SMB(Server Message Block) 프로토콜을 사용해 파일 공유에 액세스할 수 있습니다. 파일 공유에 기록된 파일은 Amazon S3의 객체가 되고 키는 경로가 됩니다. 파일과 객체 간에 일대일 매핑이 되어 있고 파일을 변경할 때마다 게이트웨이는 Amazon S3 내부 객체를 비동기 방식으로 업데이트합니다. Amazon S3 버킷에 있는 기존 객체는 파일 시스템에서 파일로 표시되고 키는 경로가 됩니다. 객체는 Amazon S3 서버 측 암호화 키(SSE-S3)로 암호화됩니다. 모든 데이터 전송은 HTTPS를 통해 이루어집니다.

HTTPS 데이터 업로드 요청을 Amazon S3로 전송할 때 File Gateway는 업로드 중인 데이터의 MD5 체크섬으로 Content-MD5 헤더를 채웁니다. 이 헤더를 사용하면 Amazon S3에서 계산한 MD5 체크섬과 File Gateway에서 수신한 값이 일치하지 않는 경우 Amazon S3가 실패를 반환합니다. 이러한 실패가 반환되면 File Gateway가 요청을 다시 보냅니다.

이 서비스는 사용 가능한 대역폭을 더 잘 사용하기 위해 멀티파트 병렬 업로드 또는 바이트 범위 다운로드를 AWS 사용하여 게이트웨이와 간의 데이터 전송을 최적화합니다. 로컬 캐시는 최근에 액세

스한 데이터에 대한 짧은 지연 시간 액세스를 제공하고 데이터 송신 요금을 줄이기 위해 유지됩니다. CloudWatch 지표는 VM의 리소스 사용 및 AWS와의 데이터 전송에 대한 인사이트를 제공합니다. CloudTrail은 모든 API 호출을 추적합니다.

S3 File Gateway 스토리지를 사용할 경우 Amazon S3로의 클라우드 워크로드 수집, 백업 및 아카이브 수행, AWS 클라우드로의 스토리지 데이터 마이그레이션 및 계층화 같은 작업을 수행할 수 있습니다. 다음 다이어그램은 Storage Gateway에 대한 파일 스토리지 배포를 간략하게 보여줍니다.



S3 File Gateway는 Amazon S3에 파일을 업로드할 때 파일을 Amazon S3 객체로 변환합니다. S3 File Gateway와 S3 객체의 파일 공유에 대해 수행되는 파일 작업 간의 상호 작용을 위해서는 파일과 객체 간에 변환할 때 특정 작업을 신중하게 고려해야 합니다.

일반적인 파일 작업은 파일 메타데이터를 변경하여 현재 S3 객체를 삭제하고 새 S3 객체를 생성합니다. 다음 표에는 파일 작업 예제와 S3 객체에 미치는 영향이 나와 있습니다.

파일 작업	S3 객체 영향	스토리지 클래스 영향
파일 이름 바꾸기	기존 S3 객체를 교체하고 각 파일에 대해 새 S3 객체를 생성합니다.	조기 삭제 요금 및 검색 요금이 적용될 수 있습니다.
폴더 이름 변경	기존 S3 객체를 모두 바꾸고 폴더 구조의 각 폴더 및 파일에 대해 새 S3 객체를 생성합니다.	조기 삭제 요금 및 검색 요금이 적용될 수 있습니다.
파일/폴더 권한 변경	기존 S3 객체를 바꾸고 각 파일 또는 폴더에 대해 새 S3 객체를 생성합니다.	조기 삭제 요금 및 검색 요금이 적용될 수 있습니다.

파일 작업	S3 객체 영향	스토리지 클래스 영향
파일/폴더 소유권 변경	기존 S3 객체를 바꾸고 각 파일 또는 폴더에 대해 새 S3 객체를 생성합니다.	조기 삭제 요금 및 검색 요금이 적용될 수 있습니다.
파일에 추가	기존 S3 객체를 교체하고 각 파일에 대해 새 S3 객체를 생성합니다.	조기 삭제 요금 및 검색 요금이 적용될 수 있습니다.

파일이 NFS 또는 SMB 클라이언트에 의해 S3 File Gateway에 기록되면 File Gateway는 파일의 데이터를 Amazon S3에 업로드한 다음 메타데이터(소유권, 타임스탬프 등)를 업로드합니다. 파일 데이터를 업로드하면 S3 객체가 생성되고 파일의 메타데이터를 업로드하면 S3 객체의 메타데이터가 업데이트됩니다. 이 프로세스는 객체의 다른 버전을 생성하여 객체의 두 버전을 생성합니다. S3 버전 관리가 켜져 있으면 두 버전이 모두 저장됩니다.

파일이 Amazon S3에 업로드된 후 NFS 또는 SMB 클라이언트가 S3 File Gateway에서 파일을 수정하면 S3 File Gateway는 전체 파일을 업로드하는 대신 새 데이터 또는 수정된 데이터를 업로드합니다. 파일을 수정하면 새 버전의 S3 객체가 생성됩니다.

S3 File Gateway가 더 큰 파일을 업로드하는 경우 클라이언트가 S3 File Gateway에 쓰기를 완료하기 전에 작은 파일 청크를 업로드해야 할 수 있습니다. 여기에는 캐시 공간 확보 또는 파일 공유에 대한 높은 쓰기 속도가 포함됩니다. 이로 인해 S3 버킷에 여러 버전의 객체가 생성될 수 있습니다.

객체를 다른 스토리지 클래스로 이동하도록 수명 주기 정책을 설정하기 전에 S3 버킷을 모니터링하여 객체의 버전 수를 확인해야 합니다. S3 버킷의 객체에 대한 버전 수를 최소화하려면 이전 버전의 수명 주기 만료를 구성해야 합니다. S3 버킷 간에 동일 리전 복제(SRR) 또는 교차 리전 복제(CRR)를 사용하면 사용되는 스토리지가 증가합니다.

시작하기 AWS Storage Gateway

이 섹션에서는 시작하기에 대한 지침을 제공합니다 AWS. 사용을 시작하려면 AWS 계정이 필요합니다 AWS Storage Gateway. 기존 AWS 계정을 사용하거나 새 계정에 가입할 수 있습니다. 또한 Storage Gateway 작업을 수행하는 데 필요한 관리 권한이 있는 그룹에 속한 AWS 계정의 IAM 사용자가 필요합니다. 적절한 권한이 있는 사용자는 Storage Gateway 콘솔 및 Storage Gateway API에 액세스하여 게이트웨이 배포, 구성 및 유지 관리 작업을 수행할 수 있습니다. 처음 사용하는 경우 Storage Gateway로 작업하기 전에 지원되는 AWS 리전 및 파일 게이트웨이 설정 요구 사항 섹션을 검토하는 것이 좋습니다. https://docs.aws.amazon.com/filegateway/latest/files3/Requirements.html

이 섹션은 다음 주제로 구성되어 있으며, AWS Storage Gateway를 시작하는 방법에 대한 추가 정보를 제공합니다.

주제

- Amazon Web Services 가입 -에 가입 AWS 하고 AWS 계정을 생성하는 방법을 알아봅니다.
- 관리자 권한이 있는 IAM 사용자 생성 - AWS 계정에 대한 관리 권한이 있는 IAM 사용자를 생성하는 방법에 대해 알아봅니다.
- 액세스 AWS Storage Gateway - Storage Gateway 콘솔을 AWS Storage Gateway 통해 또는 AWS SDKs를 사용하여 프로그래밍 방식으로에 액세스하는 방법을 알아봅니다.
- AWS 리전 Storage Gateway를 지원하는 - Storage Gateway에서 게이트웨이를 활성화할 때 데이터를 저장하는 데 사용할 수 있는 AWS 리전을 알아봅니다.

Amazon Web Services 가입

AWS 계정 는 AWS 서비스에 액세스하기 위한 기본 요구 사항입니다. AWS 계정 는 사용자로 생성하는 모든 AWS 리소스의 기본 컨테이너입니다 AWS . AWS 계정 도 AWS 리소스의 기본 보안 경계입니다. 계정에서 생성하는 모든 리소스는 해당 계정에 대한 자격 증명이 있는 사용자가 사용할 수 있습니다. 사용을 시작하려면 먼저에 가입 AWS Storage Gateway해야 합니다 AWS 계정.

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

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

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

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

또한 사용자가 AWS에 액세스할 때 임시 자격 증명을 사용하도록 요구하는 것이 좋습니다. 임시 자격 증명을 제공하기 위해 페더레이션과 AWS IAM Identity Center와 같은 자격 증명 공급자를 사용할 수 있습니다. 회사가 이미 자격 증명 공급자를 사용하는 경우 페더레이션과 함께 사용하여 AWS 계정의 리소스에 대한 액세스를 제공하는 방법을 간소화할 수 있습니다.

관리자 권한이 있는 IAM 사용자 생성

AWS 계정을 생성한 후 다음 단계에 따라 (AWS Identity and Access Management IAM) 사용자를 직접 생성한 다음 관리 권한이 있는 그룹에 해당 사용자를 추가합니다. AWS Identity and Access Management 서비스를 사용하여 Storage Gateway 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 섹션을 참조하세요AWS Storage Gateway의 ID 및 액세스 관리.

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center에서 (권장)	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다. 이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따릅니다.	AWS Command Line Interface 사용 설명서에서 사용하도록 AWS CLI 를 구성 AWS IAM Identity Center하여 프로그래밍 방식 액세스를 구성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
	IAM의 보안 모범 사례를 참조하세요.		
IAM에서 (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 비상 액세스를 위한 IAM 사용자 생성에 나와 있는 지침을 따르세요.	IAM 사용 설명서에 나온 IAM 사용자의 액세스 키 관리를 수행하여 프로그래밍 방식의 액세스를 구성합니다.

> **Warning**
>
> IAM 사용자는 장기 자격 증명을 보유하고 있어 보안 위험이 있습니다. 이 위험을 줄이려면 이러한 사용자에게 작업을 수행하는 데 필요한 권한만 제공하고 더 이상 필요하지 않을 경우 이러한 사용자를 제거하는 것이 좋습니다.

액세스 AWS Storage Gateway

AWS Storage Gateway 콘솔을 사용하여 배포에서 Storage Gateway Hardware Appliance 활성화 또는 제거, 다양한 유형의 게이트웨이 생성, 관리 및 삭제, 파일 공유의 생성, 관리 및 삭제, Storage Gateway 서비스의 다양한 요소의 상태 모니터링 등 다양한 게이트웨이 구성 및 유지 관리 작업을 수행할 수 있습니다. 이 안내서에서는 간편하고 쉽게 사용할 수 있도록 Storage Gateway 콘솔 웹 인터페이스를 사용하여 작업을 수행하는 데 중점을 둡니다. Storage Gateway 콘솔은 웹 브라우저를 통해 액세스할 수 있습니다(https://console.aws.amazon.com/storagegateway/home/).

프로그래밍 방식 접근 방식을 선호하는 경우 AWS Storage Gateway 애플리케이션 프로그래밍 인터페이스(API) 또는 명령줄 인터페이스(CLI)를 사용하여 Storage Gateway 배포에서 리소스를 설정하고 관리할 수 있습니다. Storage Gateway API의 작업, 데이터 유형 및 필수 구문에 대한 자세한 내용은 Storage Gateway API 참조를 참조하세요. Storage Gateway CLI에 대한 자세한 내용은 AWS CLI 명령 참조를 참조하세요.

또한 AWS SDKs를 사용하여 Storage Gateway와 상호 작용하는 애플리케이션을 개발할 수 있습니다. Java, .NET, PHP용 AWS SDK는 기본 Storage Gateway API를 포함하고 있어 프로그래밍 작업을 간소화합니다. SDK 라이브러리 다운로드에 대한 자세한 내용은 AWS 개발자 센터를 참조하세요.

요금에 대한 자세한 정보는 AWS Storage Gateway 요금을 참조하세요.

AWS 리전 Storage Gateway를 지원하는

AWS 리전 는에 여러 가용 영역 AWS 이 있는 세계의 물리적 위치입니다. 가용 영역은 각각 중복 전원, 네트워킹 및 연결을 갖춘 하나 이상의 개별 AWS 데이터 센터로 구성되며 별도의 시설에 보관됩니다. 즉, 각 AWS 리전 는 물리적으로 격리되어 있고 다른 리전과 독립적입니다. 리전에서는 내결함성, 안정성 및 복원성을 지원하고 지연 시간을 줄일 수도 있습니다. AWS 서비스에서 제공하는 복제 기능을 명시적으로 사용하지 않는 한 한 한 리전에서 생성하는 리소스는 다른 리전에 존재하지 않습니다. 예를 들어, Amazon S3와 Amazon EC2 크로스 리전 복제를 지원합니다. 와 같은 일부 서비스에는 리전 리소스 AWS Identity and Access Management가 없습니다. 비즈니스 요구 사항을 충족하는 위치에서 AWS 리소스를 시작할 수 있습니다. 예를 들어 유럽 사용자와 더 가깝거나 법적 요구 사항을 충족하기 위해 유럽의 AWS 리전 에서 어플라이언스를 호스팅 AWS Storage Gateway 하기 위해 Amazon EC2 인스턴스를 시작할 수 있습니다. 는 특정 서비스에서 지원하는 리전 중 사용할 수 있는 리전을 AWS 계정 결정합니다.

- Storage Gateway - 지원되는 AWS 리전 및 Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.
- Storage Gateway Hardware Appliance - 하드웨어 어플라이언스에서 사용할 수 있는 지원되는 리전은 AWS 일반 참조에서 AWS Storage Gateway Hardware Appliance 리전을 참조하세요.

File Gateway 설정 요구 사항

다른 언급이 없을 경우, 다음 요구 사항은 AWS Storage Gateway에서 모든 File Gateway 구성에 공통적으로 적용됩니다. 설정은 이 섹션의 요구 사항을 충족해야 합니다. 게이트웨이를 배포하기 전에 게이트웨이 설정에 적용되는 요구 사항을 검토합니다.

주제

사전 조건

Amazon S3 File Gateway(S3 File Gateway)를 설정하기 전에 다음 사전 조건을 충족해야 합니다.

- Microsoft Active Directory(AD)를 구성하고 필요한 권한이 있는 Active Directory 서비스 계정을 생성합니다. 자세한 내용은 Active Directory 서비스 계정 권한 요구 사항을 참조하세요.
- 게이트웨이와 AWS사이에 충분한 네트워크 대역폭이 있는지 확인합니다. 게이트웨이를 성공적으로 다운로드, 활성화 및 업데이트하려면 최소 100Mbps가 필요합니다.
- AWS 와 게이트웨이를 배포하는 온프레미스 환경 간의 네트워크 트래픽에 사용할 연결을 구성합니다. 퍼블릭 인터넷, 프라이빗 네트워킹, VPN 또는를 사용하여 연결할 수 있습니다 Direct Connect. 게이트웨이가 Amazon Virtual Private Cloud에 대한 프라이빗 연결을 AWS 통해 통신하도록 하려면 게이트웨이를 설정하기 전에 Amazon VPC를 설정합니다.
- 게이트웨이가 Active Directory 도메인 컨트롤러의 이름을 확인할 수 있는지 확인합니다. Active Directory 도메인에서 DHCP를 사용하여 확인을 처리하거나 게이트웨이 로컬 콘솔의 네트워크 구성 설정 메뉴에서 DNS 서버를 수동으로 지정할 수 있습니다.

하드웨어 및 스토리지 요구 사항

다음 섹션에서는 게이트웨이에 필요한 최소 하드웨어 및 스토리지 구성과 필요한 스토리지에 할당할 최소 디스크 공간에 대한 정보를 제공합니다.

File Gateway 성능의 모범 사례에 대한 자세한 내용은 S3 File Gateway에 대한 기본 성능 지침 섹션을 참조하세요.

온프레미스 VM에 대한 하드웨어 요구 사항

게이트웨이를 온프레미스에서 배포하는 경우에는 게이트웨이 가상 머신(VM)을 배포하는 기본 하드웨어가 다음의 최소 리소스를 제공할 수 있도록 해야 합니다.

- VM에 지정한 가상 프로세스 4개
- File Gateway용 16GiB의 예약 RAM
- VM 이미지 및 시스템 데이터 설치용 디스크 공간 80GiB

자세한 내용은 S3 File Gateway 처리량 최대화를 참조하세요. 하드웨어가 게이트웨이 VM의 성능에 미치는 영향에 대한 정보는 파일 공유 할당량 섹션을 참조하세요.

Amazon EC2 인스턴스 유형에 대한 요구 사항

Amazon Elastic Compute Cloud(Amazon EC2)에 게이트웨이를 배포할 경우, 게이트웨이가 작동하려면 인스턴스 크기가 최소한 **`xlarge`**여야 합니다. 하지만 컴퓨팅 최적화 인스턴스 패밀리의 경우 크기가 **`2xlarge`** 이상이 되어야 합니다.

> **Note**
>
> Storage Gateway AMI는 Intel 또는 AMD 프로세서를 사용하는 x86 기반 인스턴스와만 호환됩니다. Graviton 프로세서를 사용하는 ARM 기반 인스턴스는 지원되지 않습니다.

게이트웨이 유형에 대한 권장 인스턴스 유형 중 하나를 사용합니다.

File Gateway 유형에 대한 권장 사항

- 범용 인스턴스 패밀리 – m5, m6 또는 m7 인스턴스 유형. Storage Gateway 프로세서 및 RAM 요구 사항을 충족하려면 xlarge 이상의 인스턴스 크기를 선택합니다.

- 컴퓨팅 최적화 인스턴스 패밀리 – c5, c6, 또는 c7 인스턴스 유형. Storage Gateway 프로세서 및 RAM 요구 사항을 충족하려면 2xlarge 이상의 인스턴스 크기를 선택합니다.
- 메모리 최적화 인스턴스 패밀리 – r5, r6 또는 r7 인스턴스 유형. Storage Gateway 프로세서 및 RAM 요구 사항을 충족하려면 xlarge 이상의 인스턴스 크기를 선택합니다.
- 스토리지 최적화 인스턴스 패밀리 – i3, i4 또는 i7 인스턴스 유형. Storage Gateway 프로세서 및 RAM 요구 사항을 충족하려면 xlarge 이상의 인스턴스 크기를 선택합니다.

> **Note**
>
> 게이트웨이를 Amazon EC2에서 시작하고, 선택한 인스턴스 유형이 임시 스토리지를 지원할 경우 디스크가 자동으로 나열됩니다. Amazon EC2 인스턴스 스토리지에 대한 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 스토리지를 참조하세요.
> 애플리케이션 쓰기는 캐시에 동기 방식으로 저장되지만 내구성이 뛰어난 Amazon S3의 스토리지에는 비동기 방식으로 업로드됩니다. 업로드를 마치기 전에 인스턴스가 중단되어 휘발성 스토리지가 손실될 경우에는 캐시에 저장되어 아직 Amazon Simple Storage Service(Amazon S3)에 작성되지 않은 데이터가 손실될 수 있습니다. 따라서 게이트웨이를 호스팅하고 있는 인스턴스를 중단하려면 먼저 `CachePercentDirty` CloudWatch 지표가 0인지 확인해야 합니다. 휘발성 스토리지에 대한 자세한 내용은 휘발성 스토리지와 EC2 게이트웨이를 함께 사용 섹션을 참조하세요. Storage Gateway의 지표 모니터링에 대한 자세한 내용은 S3 File Gateway 모니터링 섹션을 참조하세요.
> S3 버킷에 객체 수가 500만 개 이상이고 gp2 EBS 볼륨을 사용 중인 경우, 시작 시 게이트웨이가 허용 가능한 성능을 발휘하려면 최소 루트 EBS 볼륨으로 350GiB가 필요합니다. 새로 생성된 Amazon EC2 File Gateway 인스턴스는 기본적으로 gp3 루트 볼륨을 사용하며,이 요구 사항은 없습니다. 볼륨 크기 증가 방법에 대한 자세한 내용은 탄력적 볼륨을 사용하여 EBS 볼륨 수정(콘솔)을 참조하세요.

스토리지 요구 사항

VM에 80GiB 디스크 공간이 필요할 뿐 아니라 게이트웨이에도 추가 디스크가 필요합니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)			
File Gateway	150GiB	64TiB			

> **Note**
>
> 캐시에 대해 하나 이상의 로컬 드라이브를 최대 용량까지 구성할 수 있습니다.
> 기존 게이트웨이에 캐시를 추가할 때 호스트(하이퍼바이저 또는 Amazon EC2 인스턴스)에 새 디스크를 생성하는 것이 중요합니다. 기존 디스크가 이전에 캐시로 할당되었던 경우, 디스크 크기를 변경하지 마십시오.

게이트웨이 할당량에 대한 자세한 내용은 파일 공유 할당량 섹션을 참조하세요.

네트워크 및 방화벽 요구 사항

게이트웨이에서 인터넷, 로컬 네트워크, 도메인 이름 서비스(DNS) 서버, 방화벽, 라우터 등에 액세스할 수 있어야 합니다.

네트워크 대역폭 요구 사항은 게이트웨이가 업로드하고 다운로드하는 데이터 양에 따라 달라집니다. 게이트웨이를 성공적으로 다운로드, 활성화 및 업데이트하려면 최소 100Mbps가 필요합니다. 데이터 전송 패턴에 따라 워크로드 지원에 필요한 대역폭이 결정됩니다.

아래에서 필수 포트에 대한 정보와 방화벽 및 라우터를 통한 액세스를 허용하는 방법에 대한 정보를 얻을 수 있습니다.

> **Note**
>
> 경우에 따라 게이트웨이를 Amazon EC2에 배포하거나 네트워크 보안 정책이 AWS IP 주소 범위를 제한하는 다른 유형의 배포(온프레미스 포함)를 사용할 수 있습니다. 이러한 경우 AWS IP 범위 값이 변경될 때 게이트웨이에 서비스 연결 문제가 발생할 수 있습니다. 사용해야 하는 AWS IP 주소 범위 값은 게이트웨이를 활성화하는 리전의 AWS Amazon 서비스 하위 집합에 있습니다. 현재 IP 범위 값은AWS 일반 참조에서 AWS IP 주소 범위를 참조하세요.

주제

- 포트 요구 사항
- Storage Gateway Hardware Appliance에 대한 네트워킹 및 방화벽 요구 사항
- 방화벽 및 라우터를 통한 AWS Storage Gateway 액세스 허용
- Amazon EC2 게이트웨이 인스턴스에 대한 보안 그룹 구성

포트 요구 사항

S3 File Gateway를 성공적으로 배포하고 작동하려면 네트워크 보안을 통해 특정 포트를 허용해야 합니다. 일부 포트는 모든 게이트웨이에 필요하며, 다른 포트는 NFS 또는 SMB 클라이언트, VPC 엔드포인트 또는 Microsoft Active Directory에 연결할 때와 같은 특정 구성에만 필요합니다.

S3 File Gateway의 경우 도메인 사용자가 SMB(Server Message Block) 파일 공유에 액세스할 수 있게 허용하려면 Microsoft Active Directory만 사용해야 합니다. File Gateway는 유효한 모든 Microsoft Windows 도메인(DNS로 확인 가능)에 조인될 수 있습니다.

Directory Service 를 사용하여 Amazon Web Services 클라우드AWS Managed Microsoft AD에서를 생성할 수도 있습니다. 대부분의 AWS Managed Microsoft AD 배포에서는 VPC에 대한 동적 호스트 구성 프로토콜(DHCP) 서비스를 구성해야 합니다. DHCP 옵션 세트 생성에 대한 자세한 내용은 AWS Directory Service 관리 안내서의 DHCP 옵션 세트 생성을 참조하세요.

다음 표에서는 필요한 포트를 나열하고 참고 열의 조건부 요구 사항을 설명합니다.

S3 File Gateway의 포트 요구 사항

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
웹 브라우저	웹 브라우저	Storage Gateway VM	TCP HTTP	80	✓	✓	✓	Storage Gateway 활성화 키를 가져올 때 로컬 시스템에서 사용합니다. 포트 80은 Storage Gateway 어플라이언스 활성화

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
								중에만 사용됩니다. Storage Gateway VM에 대한 공개 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. Storage Gateway Management Console에서 게이트웨이를 활성화하는 경우,

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
								콘솔에 연결하는 호스트가 게이트웨이의 포트 80에 액세스할 수 있어야 합니다.
웹 브라우저	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	AWS Management Console(기타 모든 작업)
DNS	Storage Gateway VM	DNS(Domain Name Service) 서버	TCP 및 UDP DNS	53	✓	✓	✓	이름 확인을 위해 Storage Gateway VM과 DNS 서버 간 통신에 사용됩니다.

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
NTP	Storage Gateway VM	NTP(Network Time Protocol) 서버	TCP 및 UDP NTP	123	✓	✓	✓	온프레미스 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다. Storage Gateway VM은 다음 NTP 서버를 사용하도록 구성되어 있습니다. • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
								• 3.amazon.pool.ntp.org Note Amazon EC2에서 호스팅되는 게이트웨이에는 필요하지 않습니다.

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
Storage Gateway	Storage Gateway VM	지원 엔드포인트	TCP SSH	22	✓	✓	✓	지원 가게이트웨이에 액세스하여 게이트웨이 문제를 해결할 수 있도록 허용합니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다. 지원 엔드포인트 목록은 지원 엔드포인트를 참조하세요.

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	관리 제어
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	정품 인증용
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	관리 제어 *VPC 엔드포인트를 사용하는 경우에만 필수
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*	컨트롤 플레인 엔드포인트 *VPC 엔드포인트를 사용하는 경우에만 필수

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
VPC	Storage Gateway VM	AWS	TCP HTTPS	1027		✓	✓*	Anon 컨트롤 플레인(활성화용) *VPC 엔드포인트를 사용하는 경우에만 필수
VPC	Storage Gateway VM	AWS	TCP HTTPS	1028		✓	✓*	Proxy 엔드포인트 *VPC 엔드포인트를 사용하는 경우에만 필수
VPC	Storage Gateway VM	AWS	TCP HTTPS	1031		✓	✓*	데이터 영역 *VPC 엔드포인트를 사용하는 경우에만 필수

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
VPC	Storage Gateway VM	AWS	TCP HTTPS	2222		✓	✓*	VPCe에 대한 SSH 지원 채널 *VPC 엔드포인트를 사용할 때 지원 채널을 여는 경우에만 필수
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	관리 제어 *VPC 엔드포인트를 사용하는 경우에만 필수

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
파일 공유 클라이언트	SMB 클라이언트	Storage Gateway VM	TCP 또는 UDP SMBv3	445	✓	✓	✓*	파일 공유 데이터 전송 세션 서비스. Microsoft Windows NT 이상용 포트 137~139를 대체합니다. *SMB에만 필요합니다.
Microsoft Active Directory	Storage Gateway VM	Active Directory 서버	UDP NetBIOS	137	✓	✓	✓*	Name 서비스 *SMBv1에만 필요합니다.
Microsoft Active Directory	Storage Gateway VM	Active Directory 서버	UDP NetBIOS	138	✓	✓	✓*	데이터그램 서비스 *SMBv1에만 필요합니다.

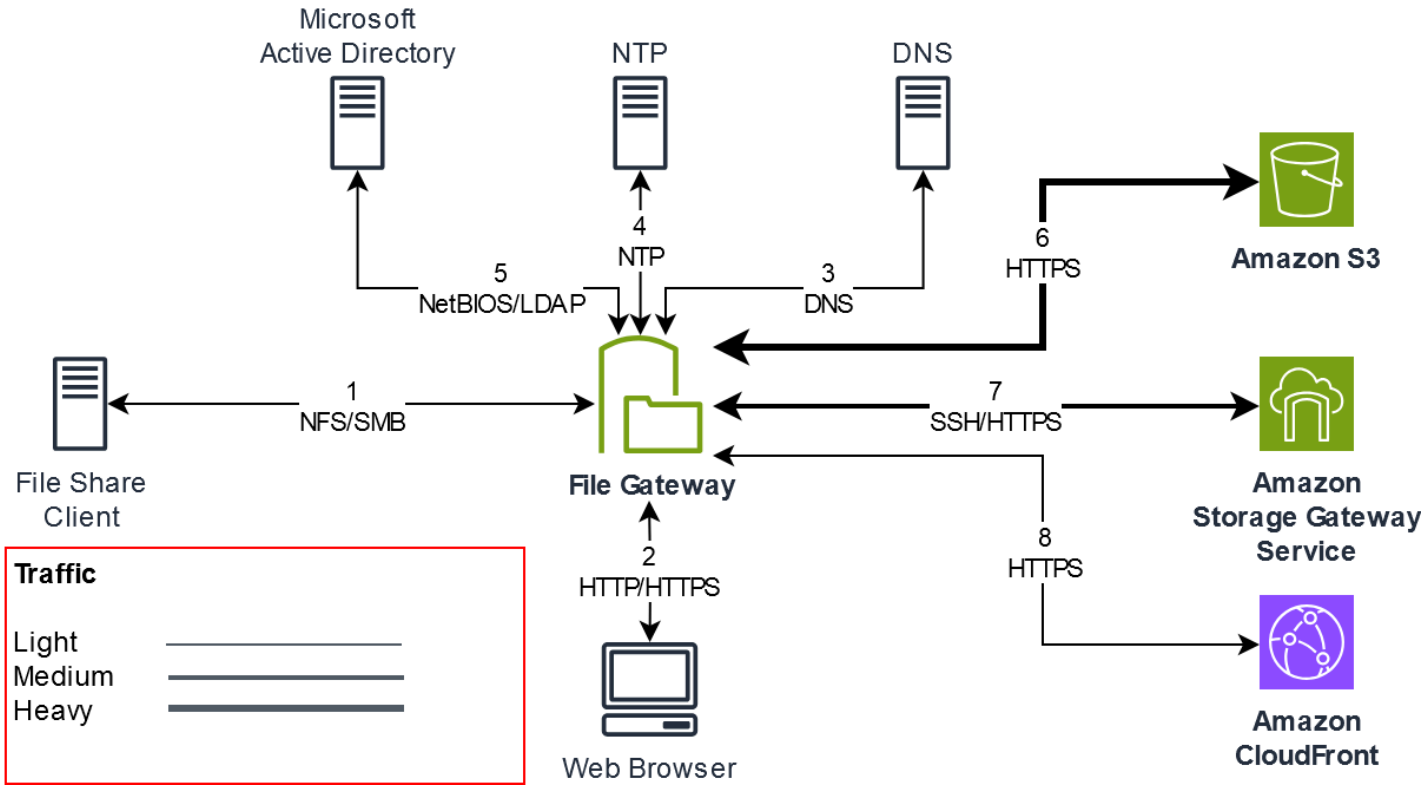
네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
Microsoft Active Directory	Storage Gateway VM	Active Directory 서버	TCP 및 UDP LDAP	389	✓	✓	✓*	DSA(Directory System Agent) 클라이언트 연결 *SMB에만 필요합니다.
Microsoft Active Directory	Storage Gateway VM	Active Directory 서버	TCP 및 UDP Kerberos	88	✓	✓	✓*	Kerberos *SMB에만 필요합니다.
Microsoft Active Directory	Storage Gateway VM	Active Directory 서버	TCP 분산 컴퓨팅 환경/엔드포인트 매퍼 (DCE/EMAP)	135	✓	✓	✓*	RPC *SMB에만 필요합니다.

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
파일 공유 클라이언트	NFS 클라이언트	Storage Gateway VM	TCP 또는 UDP 데이터 NFSv3	111	✓	✓	✓*	파일 공유 데이터 전송 (NFS v3에만 해당) *NFS에만 필요합니다.
파일 공유 클라이언트	NFS 클라이언트	Storage Gateway VM	TCP 또는 UDP NFS	2049	✓	✓	✓*	파일 공유 데이터 전송 *NFS v3 및 v4에만 필요합니다.
파일 공유 클라이언트	NFS 클라이언트	Storage Gateway VM	TCP 또는 UDP NFSv3	20048	✓	✓	✓*	파일 공유 데이터 전송 *NFSv3에만 필수

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
파일 공유 클라이언트	NFS 클라이언트	Storage Gateway VM	TCP 또는 UDP NFSv3	8750	✓	✓	✓*	파일 공유 할당량 *NFSv3에만 필수
파일 공유 클라이언트	SMB 클라이언트	Storage Gateway VM	TCP 또는 UDP SMBv2	139	✓	✓	✓*	파일 공유 데이터 전송 세션 서비스 *SMB에만 필요합니다

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
Amazon S3	Storage Gateway VM	Amazon S3 서비스 엔드포인트	TCP HTTPS	443	✓	✓	✓	Storage Gateway VM에서 AWS 서비스 엔드포인트로의 통신용입니다. 서비스 엔드포인트에 대한 자세한 내용은 방화벽 및 라우터를 통한 Allowing AWS Storage Gateway 액세스를 참조하세요.

다음 그림은 기본 S3 File Gateway 배포를 위한 네트워크 트래픽 흐름을 보여줍니다.



Storage Gateway Hardware Appliance에 대한 네트워킹 및 방화벽 요구 사항

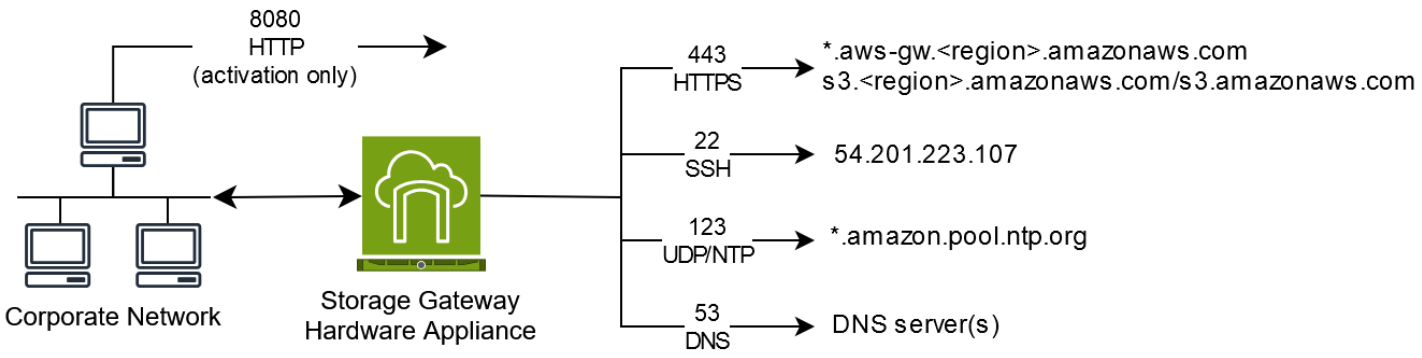
각 Storage Gateway Hardware Appliance에는 다음과 같은 네트워크 서비스가 필요합니다.

- 인터넷 액세스 - 서버의 모든 네트워크 인터페이스를 통해 인터넷에 상시 접속할 수 있는 네트워크 연결입니다.
- DNS 서비스 - 하드웨어 어플라이언스와 DNS 서버 간의 통신을 위한 DNS 서비스입니다.
- 시간 동기화 - 자동으로 구성된 Amazon NTP 시간 서비스에 연결할 수 있어야 합니다.
- IP 주소 - 할당된 DHCP 또는 고정 IPv4 주소입니다. IPv6 주소는 할당할 수 없습니다.

Dell PowerEdge R640 서버 후면에는 5개의 물리적 네트워크 포트가 있습니다. 서버 뒷면을 보고 왼쪽부터 오른쪽 순서로 이 포트는 다음과 같습니다.

1. iDRAC
2. em1
3. em2
4. em3
5. em4

iDRAC 포트는 원격 서버 관리에 사용할 수 있습니다.



하드웨어 어플라이언스를 작동하려면 다음 포트가 필요합니다.

프로토콜	포트	Direction	소스	Destination	사용법
SSH	22	아웃바운드	하드웨어 어플라이언스	`54.201.223.107`	지원 채널
DNS	53	아웃바운드	하드웨어 어플라이언스	DNS 서버	이름 확인
UDP/NTP	123	아웃바운드	하드웨어 어플라이언스	`*.amazon.pool.ntp.org`	시간 동기화
HTTPS	443	아웃바운드	하드웨어 어플라이언스	`*.amazonaws.com`	데이터 전송
HTTP	8080	인바운드	AWS	하드웨어 어플라이언스	활성화(잠시 동안)

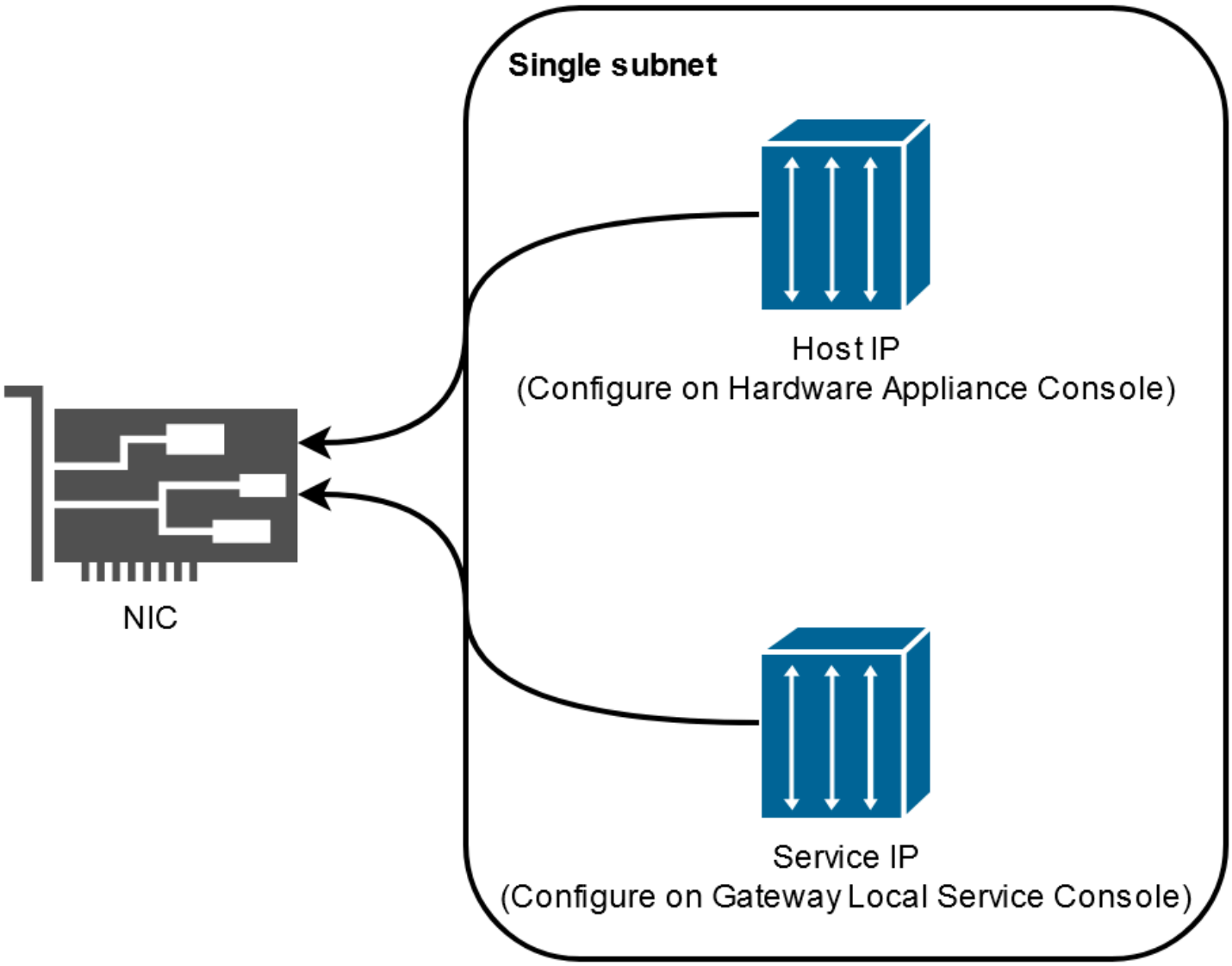
하드웨어 어플라이언스는 설계상 다음과 같은 네트워크 및 방화벽 설정이 필요합니다.

- 하드웨어 콘솔에서 연결된 모든 네트워크 인터페이스를 구성합니다.
- 각 네트워크 인터페이스는 고유한 서브넷에 있어야 합니다.
- 연결된 모든 네트워크 인터페이스에 위의 그림에 나와 있는 엔드포인트에 대한 아웃바운드 액세스를 제공합니다.

- 하드웨어 어플라이언스를 지원하는 네트워크 인터페이스를 한 개 이상 구성합니다. 자세한 내용은 하드웨어 어플라이언스 네트워크 파라미터 구성 단원을 참조하십시오.

> **Note**
>
> 서버 뒷면과 포트가 나와 있는 그림을 보려면 하드웨어 어플라이언스를 물리적으로 설치하기 섹션을 참조하세요.

동일한 네트워크 인터페이스(NIC)의 모든 IP 주소는 게이트웨이용이든 호스트용이든 상관없이 동일한 서브넷에 있어야 합니다. 다음 그림은 주소 지정 체계를 보여 줍니다.



하드웨어 어플라이언스 활성화 및 구성에 대한 자세한 내용은 AWS Storage Gateway 하드웨어 어플라이언스 사용 섹션을 참조하세요.

방화벽 및 라우터를 통한 AWS Storage Gateway 액세스 허용

게이트웨이와 통신하려면 다음 Storage Gateway 서비스 엔드포인트에 액세스해야 합니다 AWS. 게이트웨이 설정 중에 네트워크 환경에 따라 게이트웨이의 엔드포인트 유형을 선택합니다. 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다.

> **Note**
>
> Storage Gateway가 연결 및 데이터 송수신에 사용하도록 프라이빗 VPC 엔드포인트 AWS 를 구성하는 경우 게이트웨이는 퍼블릭 인터넷에 액세스할 필요가 없습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하세요.

> **Important**
>
> 다음 엔드포인트 예제의 *region*을와 같은 게이트웨이의 올바른 AWS 리전 문자열로 바꿉니다us-west-2.
> *amzn-s3-demo-bucket*을 배포에서 Amazon S3 버킷의 실제 이름으로 바꿉니다. *amzn-s3-demo-bucket* 대신 별표(*)를 사용하여 방화벽 규칙에 와일드카드 항목을 생성할 수도 있습니다. 그러면 모든 버킷 이름에 대한 서비스 엔드포인트가 나열됩니다.
> 게이트웨이가 미국 또는 캐나다 AWS 리전 에 배포되어 있고 FIPS(Federal Information Processing Standard) 준수 엔드포인트 연결이 필요한 경우 *s3*를 로 바꿉니다s3-fips.

엔드포인트 유형

표준 엔드포인트

이러한 엔드포인트는 게이트웨이 어플라이언스와 간의 IPv4 트래픽을 지원합니다 AWS.

head-bucket 작업을 위해 모든 게이트웨이에는 다음과 같은 서비스 엔드포인트가 필요합니다.

```
bucket-name.s3.region.amazonaws.com:443
```

다음의 서비스 엔드포인트는 제어 경로(anon-cp, client-cp, proxy-app) 및 데이터 경로(dp-1) 작업을 위한 모든 게이트웨이에 필요합니다.

```
anon-cp.storagegateway.region.amazonaws.com:443
client-cp.storagegateway.region.amazonaws.com:443
proxy-app.storagegateway.region.amazonaws.com:443
dp-1.storagegateway.region.amazonaws.com:443
```

다음 게이트웨이 서비스 엔드포인트는 API 호출에 필요합니다.

```
storagegateway.region.amazonaws.com:443
```

다음 예제는 미국 서부(오리건) 리전(us-west-2)의 게이트웨이 서비스 엔드포인트입니다.

```
storagegateway.us-west-2.amazonaws.com:443
```

듀얼 스택 엔드포인트

이러한 엔드포인트는 게이트웨이 어플라이언스와 AWS간의 IPv4 및 IPv6 트래픽을 지원합니다.

head-bucket 작업을 위해 모든 게이트웨이에는 다음과 같은 듀얼 스택 서비스 엔드포인트가 필요합니다.

```
bucket-name.s3.dualstack.region.amazonaws.com:443
```

제어 경로(활성화, 컨트롤 플레인, 프록시) 및 데이터 경로(데이터플레인) 작업을 위해서는 모든 게이트웨이에 다음과 같은 듀얼 스택 서비스 엔드포인트가 필요합니다.

```
activation-storagegateway.region.api.aws:443
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
```

다음 게이트웨이 듀얼 스택 서비스 엔드포인트는 API 호출에 필요합니다.

```
storagegateway.region.api.aws:443
```

다음 예제는 미국 서부(오리건) 리전(us-west-2)의 게이트웨이 듀얼 스택 서비스 엔드포인트입니다.

```
storagegateway.us-west-2.api.aws:443
```

Amazon S3 서비스 엔드포인트

Amazon S3 File Gateway를 Amazon S3 서비스에 연결하려면 다음 세 가지 유형의 엔드포인트가 필요합니다.

Amazon S3 엔드포인트 서비스

> **Note**
>
> 이 엔드포인트의 경우에만 FIPS 호환 배포를 위해 `s3`를 `s3-fips`로 바꾸지 마십시오.

```
s3.amazonaws.com
```

Amazon S3 리전 엔드포인트

```
s3.region.amazonaws.com (Standard)
s3.dualstack.region.amazonaws.com (Dual-stack)
```

다음 예제는 미국 동부(오하이오) 리전(`us-east-2`)의 Amazon S3 리전 엔드포인트를 보여줍니다.

```
s3.us-east-2.amazonaws.com
s3.dualstack.us-east-2.amazonaws.com
```

다음 예제는 미국 서부(캘리포니아 북부) 리전(`us-west-1`)의 표준 및 듀얼 스택 FIPS 호환 Amazon S3 리전 엔드포인트를 보여줍니다.

```
s3-fips.us-west-1.amazonaws.com
s3-fips.dualstack.us-west-1.amazonaws.com
```

다음 예제는 AWS GovCloud (US) 리전에서 사용하는 표준 및 듀얼 스택 Amazon S3 리전 엔드포인트를 보여줍니다.

```
s3-fips.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS))
s3-fips.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS))
s3.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Standard))
s3.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Standard))
s3-fips.dualstack.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (FIPS
 dual-stack))
```

```
s3-fips.dualstack.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (FIPS
 dual-stack))
s3.dualstack.us-gov-east-1.amazonaws.com (AWS GovCloud (US-East) Region (Dual-stack))
s3.dualstack.us-gov-west-1.amazonaws.com (AWS GovCloud (US-West) Region (Dual-stack))
```

> **Note**
>
> 게이트웨이가 Amazon S3 버킷 AWS 리전 의 위치를 확인할 수 없는 경우이 서비스 엔드포인트는 기본적으로 로 설정됩니다`s3.us-east-1.amazonaws.com`. AWS 리전 게이트웨이가 활성화되고 Amazon S3 버킷이 위치한 외에도 미국 동부(버지니아 북부) 리전(`us-east-1`)에 대한 액세스를 허용하는 것이 좋습니다.

Amazon S3 버킷 엔드포인트

```
bucket-name.s3.region.amazonaws.com (Standard)
bucket-name.s3.dualstack.region.amazonaws.com (Dual-stack)
```

다음 예제는 미국 동부(오하이오) 리전(`us-east-2`)에서 이름이 *amzn-s3-demo-bucket*인 버킷의 표준 및 듀얼 스택 Amazon S3 버킷 엔드포인트를 보여줍니다.

```
amzn-s3-demo-bucket.s3.us-east-2.amazonaws.com (Standard)
amzn-s3-demo-bucket.s3.dualstack.us-east-2.amazonaws.com (Dual-stack)
```

다음 예제는 AWS GovCloud(미국 동부) 리전()*amzn-s3-demo-bucket1*에서 이름이 인 버킷에 대한 표준 및 듀얼 스택 FIPS 호환 Amazon S3 버킷 엔드포인트를 보여줍니다`us-gov-east-1`.

```
amzn-s3-demo-bucket1.s3-fips.us-gov-east-1.amazonaws.com (FIPS)
amzn-s3-demo-bucket1.s3-fips.dualstack.us-gov-east-1.amazonaws.com (FIPS dual-stack)
```

Storage Gateway 및 Amazon S3 서비스 엔드포인트 외에도 Storage Gateway VM에 다음 NTP 서버에 대한 네트워크 액세스도 필요합니다.

```
time.aws.com
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
```

```
3.amazon.pool.ntp.org
```

지원되는 엔드포인트 AWS 리전 및 서비스 엔드포인트에 대한 자세한 내용은의 Storage Gateway를 참조하세요AWS 일반 참조.

Amazon EC2 게이트웨이 인스턴스에 대한 보안 그룹 구성

에서 AWS Storage Gateway보안 그룹은 Amazon EC2 게이트웨이 인스턴스에 대한 트래픽을 제어합니다. 보안 그룹을 구성할 때는 다음을 수행하는 것이 좋습니다.

- 보안 그룹은 외부 인터넷에서 들어오는 연결을 허용해서는 안 됩니다. 게이트웨이 보안 그룹 내 인스턴스만 게이트웨이와 통신할 수 있도록 허용해야 합니다.

  인스턴스가 보안 그룹 외부에서 게이트웨이에 연결해야 하는 경우에는 포트 80(활성화용)에 대해서만 연결을 허용하는 것이 좋습니다.
- 게이트웨이 보안 그룹 외부에 있는 Amazon EC2 호스트에서 게이트웨이를 활성화하려면 호스트의 IP 주소에서 포트 80으로 들어오는 접속을 허용합니다. 활성화 호스트의 IP 주소를 확인할 수 없는 경우에는 포트 80을 열어 게이트웨이를 활성화하고 활성화가 완료되면 포트 80에 대한 액세스를 종료하는 방법을 사용할 수 있습니다.
- 문제 해결을 지원 위해를 사용하는 경우에만 포트 22 액세스를 허용합니다. 자세한 내용은 Amazon EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우 단원을 참조하십시오.

게이트웨이 용도로 개방하는 포트에 대한 자세한 내용은 포트 요구 사항 섹션을 참조하세요.

지원되는 하이퍼바이저 및 호스트 요구 사항

Storage Gateway를 온프레미스에서 가상 머신(VM) 어플라이언스 또는 물리적 하드웨어 어플라이언스로 실행하거나에서 Amazon EC2 인스턴스 AWS 로 실행할 수 있습니다.

> **Note**
>
> File Gateway 2.x, Volume Gateway 3.x 및 Tape Gateway 3.x에는 보안 부팅이 비활성화된 UEFI 부팅 모드(loader_secure=no)가 필요합니다. xml 파일은 각 qcow 다운로드와 함께 빠른 설정 구성으로 제공됩니다.

Storage Gateway에서 지원하는 하이퍼바이저 버전 및 호스트는 다음과 같습니다.

- VMware ESXi 하이퍼바이저(버전 7.0 또는 8.0) - 이 설정의 경우 호스트에 연결하기 위한 VMware vSphere 클라이언트도 필요합니다.
- Microsoft Hyper-V Hypervisor(2019, 2022 또는 2025) – 이 설정의 경우 호스트에 연결하려면 Microsoft Windows 클라이언트 컴퓨터에서 Microsoft Hyper-V Manager를 사용해야 합니다.
- Linux 커널 기반 가상 머신(KVM) - 무료 오픈 소스 가상화 기술입니다. KVM은 Linux 버전 2.6.20 이상의 모든 버전에 포함되어 있습니다. Storage Gateway는 CentOS/RHEL 7.7, RHEL 8.6 Ubuntu 16.04 LTS 및 Ubuntu 18.04 LTS 배포판에 대해 테스트 및 지원됩니다. 다른 최신 Linux 배포판이 작동하지만 기능이나 성능이 보장되지는 않습니다. KVM 환경이 이미 가동되고 있고 KVM 작동 방식에 익숙하다면 이 옵션을 사용하는 것이 좋습니다. 제안된 부팅 구성은 제공된 aws-storage-gateway.xml 파일을 참조하세요. File Gateway 2.x, Volume Gateway 3.x 및 Tape Gateway 3.x에는 보안 부팅이 비활성화된 UEFI 부팅 모드(loader_secure=no)가 필요합니다.
- 버전 10.0.1.1부터 시작하는 Nutanix AHV(Acropolis Hypervisor) - Nutanix 하이퍼 컨버지드 인프라(HCI) 솔루션에 통합된 KVM 기반 가상화 플랫폼입니다.
- Amazon EC2 인스턴스 - Storage Gateway는 게이트웨이 VM 이미지를 포함하는 Amazon Machine Image(AMI)를 제공합니다. Amazon EC2에 게이트웨이를 배포하는 방법에 대한 자세한 내용은 S3 File Gateway용 기본 Amazon EC2 호스트 배포 섹션을 참조하세요.
- Storage Gateway Hardware Appliance - Storage Gateway는 제한된 가상 머신 인프라 위치에 대한 온프레미스 배포 옵션으로 물리적 하드웨어 어플라이언스를 제공합니다.

> **Note**
>
> Storage Gateway는 다른 게이트웨이 VM의 스냅샷 또는 복제본에서 생성된 VM이나 Amazon EC2 AMI에서 게이트웨이를 복구하는 기능을 지원하지 않습니다. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 새로운 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다. 자세한 내용은 가상 머신이 예기치 않게 종료된 상황에서 복구하기 단원을 참조하십시오. Storage Gateway는 동적 메모리 및 가상 메모리 벌루닝(ballooning)을 지원하지 않습니다.

File Gateway에 지원되는 NFS 및 SMB 클라이언트

File Gateway는 다음 클라이언트를 지원합니다.

운영 체제 버전	커널 버전	지원되는 프로토콜
Amazon Linux 2023	6.1 LTS	NFSv4.1, NFSv3

운영 체제 버전	커널 버전	지원되는 프로토콜
Amazon Linux 2	5.10 LTS	NFSv4.1, NFSv3
RHEL 9	5.14	NFSv4.1, NFSv3
RHEL 8.10	4.18	NFSv4.1, NFSv3
SUSE 15	6.4	NFSv4.1, NFSv3
Ubuntu 24.04 LTS	6.8 LTS	NFSv4.1, NFSv3
Ubuntu 22.04 LTS	5.15 LTS	NFSv4.1, NFSv3
Microsoft Windows Server 2025		SMBv2, SMBv3, NFSv3
Microsoft Windows Server 2022		SMBv2, SMBv3, NFSv3
Microsoft Windows 11		SMBv2, SMBv3, NFSv3
Microsoft Windows 10		SMBv2, SMBv3, NFSv3

> **Note**
>
> SMB(Server Message Block) 암호화에는 SMB v3 언어를 지원하는 클라이언트가 필요합니다.

File Gateway에 지원되는 파일 시스템 작업

NFS 또는 SMB 클라이언트는 파일에 대해 쓰기, 읽기, 삭제 및 자르기 작업을 할 수 있습니다. 클라이언트는 쓰기를에 보내 AWS Storage Gateway면 로컬 캐시에 동기적으로 씁니다. 그런 다음 최적의 전송 방법을 통해 Amazon S3에 비동기 방식으로 작성합니다. 읽기 작업은 처음에 로컬 캐시를 통해 이루어집니다. 데이터를 사용할 수 없는 경우, S3를 통해 연속 읽기 캐시로 가져옵니다.

쓰기 및 읽기는 변경되거나 요청된 부분만 게이트웨이를 통해 전송되는 방법으로 최적화됩니다. 삭제는 Amazon S3에서 객체를 제거합니다. 디렉터리는 Amazon S3 콘솔과 동일한 구문을 사용하여 S3의 폴더 객체로 관리됩니다.

GET, PUT, UPDATE 및 DELETE 같은 HTTP 작업들은 파일 공유에서 파일을 수정할 수 있습니다. 이들 작업은 자동 만들기, 읽기, 업데이트 및 삭제(CRUD) 기능을 따릅니다.

게이트웨이의 로컬 디스크 관리

게이트웨이 가상 머신(VM)은 버퍼링 및 스토리지에 온프레미스로 할당하는 로컬 디스크를 사용합니다. Amazon EC2 인스턴스에서 생성된 File Gateway는 Amazon EBS 볼륨을 로컬 디스크로 사용합니다. 게이트웨이에 할당하려는 디스크의 개수 및 크기는 사용자가 직접 결정합니다. 게이트웨이는 최근에 액세스한 데이터에 대한 액세스 지연 시간을 줄이기 위해 할당한 캐시 스토리지를 사용합니다. 캐시 스토리지는 Amazon S3로 업로드 보류 중인 데이터를 위한 온프레미스 내구성 저장소 역할을 합니다. File Gateway에는 캐시로 사용할 150 GiB 디스크가 한 개 이상 필요합니다. 게이트웨이의 초기 구성 및 배포 후 워크로드 수요가 증가함에 따라 캐시 스토리지용 디스크를 더 추가할 수 있습니다. 이 섹션에는 로컬 디스크 관리와 관련된 개념과 절차를 설명하는 다음 주제가 포함되어 있습니다.

주제

- 로컬 디스크 스토리지 용량 결정 - File Gateway에 할당할 로컬 캐시 디스크의 수와 크기를 결정하는 방법을 알아봅니다.
- 추가 캐시 스토리지 구성 - 애플리케이션 요구 사항에 따라 File Gateway의 캐시 스토리지 용량을 늘리는 방법을 알아봅니다.
- 휘발성 스토리지와 EC2 게이트웨이를 함께 사용 - File Gateway에서 임시 디스크 스토리지를 사용할 때 데이터 손실을 방지하는 방법을 알아봅니다.

로컬 디스크 스토리지 용량 결정

S3 File Gateway를 배포할 때 할당할 캐시 디스크의 양을 고려합니다. S3 File Gateway는 가장 최근에 사용되지 않은 알고리즘을 사용하여 캐시에서 데이터를 자동으로 제거합니다. S3 File Gateway의 캐시는 해당 게이트웨이의 모든 파일 공유 간에 공유됩니다. 활성 공유가 여러 개인 경우 한 공유의 사용률이 높으면 다른 공유가 액세스할 수 있는 캐시 리소스의 양에 영향을 주어 성능에 영향을 미칠 수 있다는 점에 유의해야 합니다.

특정 워크로드에 필요한 캐시 디스크의 양을 결정할 때는 항상 게이트웨이에 캐시 디스크를 추가할 수 있지만(S3 File Gateway의 현재 할당량까지) 해당 게이트웨이의 캐시를 줄일 수는 없다는 점에 유의해야 합니다. 데이터세트에 대한 기본 분석을 수행하여 적절한 양의 캐시 디스크를 결정할 수 있지만, 로컬에 저장해야 하는 '핫' 데이터 양과 클라우드에 계층화할 수 있는 '콜드' 데이터 양을 정확히 결정할 수 있는 방법은 없습니다. 워크로드는 시간이 지남에 따라 변경되며, S3 File Gateway는 소비할 수 있는

리소스의 양과 관련된 유연성과 탄력성을 제공합니다. 캐시 양은 항상 늘릴 수 있으므로 필요에 따라 작게 시작하여 늘리는 것이 가장 비용 효율적인 접근 방식인 경우가 많습니다.

게이트웨이 설정 중에 150GiB의 초기 근사치를 사용하여 캐시 스토리지용 디스크를 프로비저닝할 수 있습니다. 이후에는 Amazon CloudWatch 운영 지표를 사용하여 캐시 스토리지 사용량을 모니터링하고 콘솔을 사용하여 필요에 따라 추가 스토리지를 프로비저닝할 수 있습니다. 측정치 사용 및 경보 설정에 대한 정보는 성능 및 최적화 섹션을 참조하세요.

> **Note**
>
> 기본 물리 스토리지 리소스는 VMware에서 데이터 스토어로 표시됩니다. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 로컬 디스크를 프로비저닝하는 경우(예: 캐시 스토리지 용도), 가상 디스크를 동일한 데이터 스토어에 VM으로 저장하거나 다른 데이터 스토어에 저장하는 옵션을 선택할 수 있습니다.
> 데이터 스토어가 한 개 이상인 경우에는 캐시 스토리지에 데이터 스토어 한 개를 선택할 것을 적극 권장합니다. 오직 기본 물리 디스크 한 개의 지원을 받는 데이터 스토어는 캐시 스토리지를 모두 지원하는 데 사용되는 경우 성능이 떨어질 수 있습니다. 이는 백업이 RAID1 같이 성능이 비교적 떨어지는 RAID 구성일 때도 마찬가지입니다.

추가 캐시 스토리지 구성

애플리케이션 요구 사항이 변화함에 따라 게이트웨이의 캐시 스토리지 용량을 늘릴 수 있습니다. 기능을 중단하거나 다운타임을 유발하지 않고 게이트웨이에 스토리지 용량을 추가할 수 있습니다. 스토리지를 추가할 때는 게이트웨이 VM이 켜져 있어야 합니다.

> **Important**
>
> 기존 게이트웨이에 캐시를 추가할 경우, 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에 새 디스크를 생성해야 합니다. 캐시로 이미 할당된 기존 디스크의 크기는 제거하거나 변경하지 마세요.

게이트웨이에 대한 추가 캐시 스토리지를 구성하려면

1. 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에서 새 디스크를 하나 이상 프로비저닝합니다. 하이퍼바이저에서 디스크를 프로비저닝하는 방법에 대한 자세한 내용은 해당 하이퍼바이저의 설명서를 참조하세요. Amazon EC2 인스턴스에 대한 Amazon EBS 볼륨 프로비저닝에

대한 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 Amazon EBS 볼륨을 참조하세요. 다음 단계에서는 이 디스크를 캐시 스토리지로 구성합니다.

2. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
3. 탐색 창에서 게이트웨이를 선택합니다.
4. 게이트웨이를 검색하고 목록에서 선택합니다.
5. 작업 메뉴에서 캐시 스토리지 구성을 선택합니다.
6. 캐시 스토리지 구성 섹션에서 프로비저닝한 디스크를 지정합니다. 디스크가 표시되지 않으면 새로 고침 아이콘을 선택하여 목록을 새로 고칩니다. 각 디스크에 대해 할당 대상 드롭다운 메뉴에서 캐시를 선택합니다.

   > **Note**
   >
   > 캐시는 File Gateway에서 디스크를 할당하는 데 사용할 수 있는 유일한 옵션입니다.

7. 변경 사항 저장을 선택하여 구성 설정을 저장합니다.

휘발성 스토리지와 EC2 게이트웨이를 함께 사용

이 섹션에서는 휘발성 디스크를 게이트웨이의 캐시 스토리지로 선택할 때 데이터 손실을 방지하기 위해 수행해야 하는 단계에 대해 설명합니다.

휘발성 디스크는 Amazon EC2 인스턴스에 임시 블록 스토리지를 제공합니다. 휘발성 디스크는 게이트웨이의 캐시 스토리지의 데이터와 같이 빈번히 바뀌는 데이터를 임시로 저장하는 데 이상적입니다. 게이트웨이를 Amazon EC2 Amazon Machine Image로 시작하고, 선택한 인스턴스 유형이 임시 스토리지를 지원할 경우 휘발성 디스크가 자동으로 나열됩니다. 디스크 중 하나를 선택하여 게이트웨이의 캐시 데이터를 저장할 수 있습니다. 자세한 내용을 알아보려면 Amazon EC2 사용 설명서의 Amazon EC2 인스턴스 저장소를 참조하세요.

애플리케이션이 게이트웨이에 쓰는 데이터는 임시 디스크의 캐시에 동기식으로 저장된 다음 Amazon S3의 내구성 있는 스토리지에 비동기식으로 업로드됩니다. 데이터가 임시 스토리지에 기록된 후 비동기 업로드가 발생하기 전에 Amazon EC2 인스턴스가 중지되면 Amazon S3에 아직 업로드되지 않은 모든 데이터가 손실될 수 있습니다. 게이트웨이를 호스팅하는 EC2 인스턴스를 다시 시작하거나 중지하기 전에 단계에 따라 이러한 데이터 손실을 방지할 수 있습니다.

> **Important**
>
> 휘발성 스토리지를 사용하는 Amazon EC2 게이트웨이를 중지했다가 다시 시작하면 게이트웨이가 영구적으로 오프라인 상태가 됩니다. 이는 물리적 스토리지 디스크가 대체되기 때문에 발생합니다. 이 문제에 대한 해결 방법은 없습니다. 유일한 해결 방법은 게이트웨이를 삭제하고 새 EC2 인스턴스에서 새 게이트웨이를 활성화하는 것입니다.

이 다음 절차의 단계는 File Gateway에 특정합니다.

휘발성 디스크를 사용하는 File Gateway의 데이터 손실을 방지하려면

1. Amazon S3에 쓰고 있는 프로세스를 모두 중지하십시오.
2. CloudWatch Events의 알림 수신을 구독하십시오. 자세한 내용은 파일 작업에 대한 알림 받기 단원을 참조하세요.
3. 임시 스토리지가 손실될 때까지 작성된 데이터가 Amazon S3에 내구성 있게 저장될 때 알림을 받으려면 NotifyWhenUploaded API를 호출합니다.
4. API가 완료할 때까지 대기한 후 알림 id를 받으십시오.

   알림 id가 동일한 CloudWatch 이벤트를 수신합니다.
5. 파일 공유에 대한 `CachePercentDirty` 지표가 0인지 확인하십시오. 이를 통해 모든 데이터가에 씌어졌음을 확인합니다. 파일 공유 지표 지표에 대한 자세한 내용은 파일 공유 지표 이해 섹션을 참조하세요.
6. 이제 데이터 손실의 위험 없이 File Gateway를 다시 시작하거나 중지할 수 있습니다.

AWS Storage Gateway 하드웨어 어플라이언스 사용

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

AWS Storage Gateway 하드웨어 어플라이언스는 검증된 서버 구성에 Storage Gateway 소프트웨어가 사전 설치된 물리적 하드웨어 어플라이언스입니다. AWS Storage Gateway 콘솔의 하드웨어 어플라이언스 개요 페이지에서 배포의 하드웨어 어플라이언스를 관리할 수 있습니다.

하드웨어 어플라이언스는 고성능 1U 서버로, 데이터 센터 또는 회사 방화벽 내 온프레미스에 배포할 수 있습니다. 하드웨어 어플라이언스를 구매하고 활성화하면 활성화 프로세스를 통해 하드웨어 어플라이언스가 AWS 계정과 연결됩니다. 활성화 후에는 하드웨어 어플라이언스가 콘솔의 하드웨어 어플라이언스 개요 페이지에 표시됩니다. 하드웨어 어플라이언스를 S3 File Gateway, FSx File Gateway, Tape Gateway, 또는 Volume Gateway 유형으로 구성할 수 있습니다. 이러한 게이트웨이 유형을 하드웨어 어플라이언스에 배포하는 절차는 가상 플랫폼에서의 절차와 동일합니다.

활성화 및 사용에 AWS Storage Gateway 하드웨어 어플라이언스를 사용할 수 AWS 리전 있는 지원되는 목록은의 AWS Storage Gateway 하드웨어 어플라이언스 리전을 참조하세요AWS 일반 참조.

다음 섹션에서는 AWS Storage Gateway 하드웨어 어플라이언스를 설정, 랙 마운트, 전원 공급, 구성, 활성화, 시작, 사용 및 삭제하는 방법에 대한 지침을 확인할 수 있습니다.

주제

- 하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거
- AWS Storage Gateway 하드웨어 어플라이언스 삭제

AWS Storage Gateway 하드웨어 어플라이언스 설정

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

Storage Gateway 하드웨어 어플라이언스를 받은 후 하드웨어 어플라이언스 로컬 콘솔을 사용하여 에 상시 연결을 제공하고 어플라이언스를 AWS 활성화하도록 네트워킹을 구성합니다. 활성화는 어플라이언스를 활성화 프로세스 중에 사용되는 AWS 계정과 연결합니다. 어플라이언스가 활성화되면 Storage Gateway 콘솔에서 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway를 시작할 수 있습니다.

하드웨어 어플라이언스를 설치하고 구성하려면

1. 어플라이언스를 랙 마운팅하고 전원과 네트워크 연결을 가동합니다. 자세한 내용은 하드웨어 어플라이언스를 물리적으로 설치하기 단원을 참조하십시오.
2. 하드웨어 어플라이언스(호스트)의 인터넷 프로토콜 버전 4(IPv4) 주소를 설정합니다. 자세한 내용은 하드웨어 어플라이언스 네트워크 파라미터 구성 단원을 참조하십시오.
3. 선택한 AWS 리전의 콘솔 하드웨어 어플라이언스 개요 페이지에서 하드웨어 어플라이언스를 활성화합니다. 자세한 내용은 AWS Storage Gateway 하드웨어 어플라이언스 활성화 단원을 참조하십시오.
4. 하드웨어 어플라이언스에 게이트웨이를 생성합니다. 자세한 내용은 게이트웨이 생성 단원을 참조하십시오.

   VMware ESXi, Microsoft Hyper-V, Linux 커널 기반 가상 머신(KVM) 또는 Amazon EC2에서 게이트웨이를 설정하는 것과 동일한 방식으로 하드웨어 어플라이언스에서 게이트웨이를 설정합니다.

사용 가능한 캐시 스토리지 증가

하드웨어 어플라이언스의 사용 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있습니다. 이렇게 하면의 데이터에 대한 짧은 지연 시간 액세스를 위한 더 큰 캐시가 제공됩니다 AWS. 5TB 모델을 주문한 경우 1.92TB SSD(Solid State Drive)를 5개 구입하여 사용 가능한 스토리지를 12TB로 늘릴 수 있습니다.

그런 다음 하드웨어 어플라이언스를 활성화하기 전에 하드웨어 어플라이언스에 추가할 수 있습니다. 하드웨어 어플라이언스를 이미 활성화한 상태에서 어플라이언스의 사용 가능한 스토리지를 12TB로 늘리려면 다음을 수행합니다.

1. 하드웨어 어플라이언스를 초기 설정으로 재설정합니다. 이 작업을 수행하는 방법에 대한 지침은 AWS Support에 문의하십시오.
2. 1.92TB SSD 5개를 어플라이언스에 추가합니다.

네트워크 인터페이스 카드 옵션

주문한 어플라이언스 모델에 따라 10G-Base-T RJ45 구리 또는 10G DA/SFP+ 네트워크 카드가 함께 제공될 수 있습니다.

- 10G-Base-T NIC 구성:
  - 10G의 경우 CAT6 케이블, 1G의 경우 CAT5(e) 사용
- 10G DA/SFP+ NIC 구성:
  - Twinax 구리 직접 연결 케이블(최대 5m) 사용
  - Dell/Intel 호환 SFP+ 광 모듈(SR 또는 LR)
  - 1G-Base-T 또는 10G-Base-T용 SFP/SFP+ 구리 트랜시버

하드웨어 어플라이언스를 물리적으로 설치하기

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

해당 애플라이언스는 1U 폼 팩터이며 표준 국제 전기기술위원회(IEC) 규격의 19인치 랙에 맞게 설계되었습니다.

사전 조건

하드웨어 어플라이언스를 설치하려면 다음 구성 요소가 필요합니다.

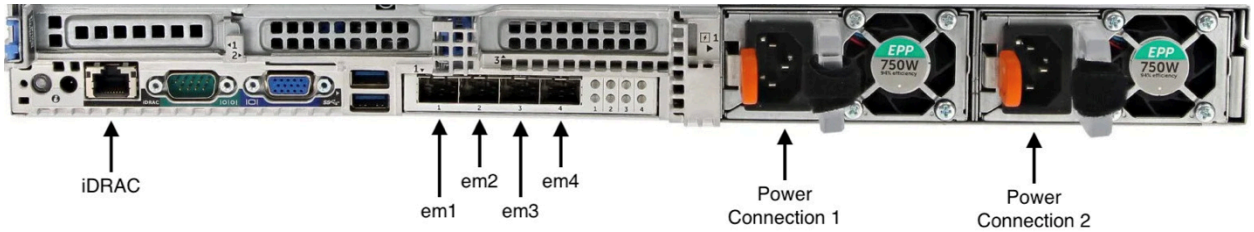
- 전원 케이블: 1개 필요, 2개 권장.
- 지원되는 네트워크 케이블(하드웨어 어플라이언스에 포함된 네트워크 인터페이스 카드(NIC)에 따라 다름). Twinax Copper DAC, SFP+ 광 모듈(Intel 호환) 또는 SFP - Base-T 구리 트랜시버.
- 키보드 및 모니터 또는 키보드, 비디오, 마우스(KVM) 스위치 솔루션.

> **Note**
>
> 다음 절차를 수행하기 전에 Storage Gateway Hardware Appliance에 대한 네트워킹 및 방화벽 요구 사항에 설명된 대로 Storage Gateway Hardware Appliance에 대한 요구 사항을 모두 충족하는지 확인하세요.

하드웨어 어플라이언스를 물리적으로 설치하려면

1. 하드웨어 어플라이언스의 상자를 개봉하고 상자에 포함된 지침에 따라 서버를 랙에 장착합니다.

   다음 이미지는 전원, 이더넷, 모니터, USB 키보드 및 iDRAC 연결용 포트가 있는 하드웨어 어플라이언스의 뒷면을 보여줍니다.
   네트워크 및 전원 커넥터 레이블이 표시된 하드웨어 어플라이언스 1 후면입니다.

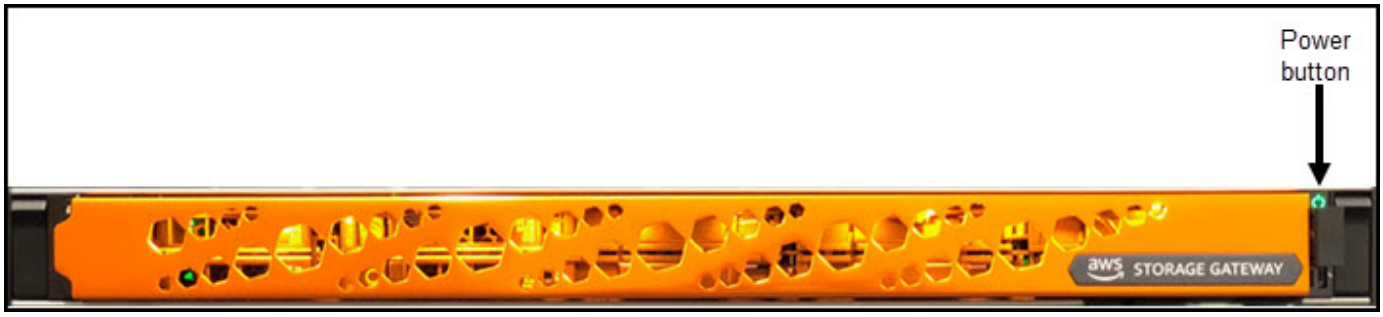
   네트워크 및 전원 커넥터 레이블이 표시된 하드웨어 어플라이언스 1 후면입니다.

2. 2개의 전원 공급 장치 각각에 전원을 연결합니다. 하나의 전원 연결만 사용할 수도 있지만, 중복성을 위해 두 전원 공급 장치에 모두 연결할 것을 권장합니다.

3. 이더넷 케이블을 em1 포트에 연결하여 상시 인터넷 연결을 제공합니다. em1 포트는 뒷면에 있는 4개의 물리 네트워크 포트 중 첫 번째(왼쪽에서 오른쪽으로)입니다.

> **Note**
>
> 하드웨어 어플라이언스는 VLAN 트렁킹을 지원하지 않습니다. 하드웨어 어플라이언스를 연결할 스위치 포트를 비트렁크 VLAN 포트로 설정합니다.

4. 키보드 및 모니터를 연결합니다.
5. 다음 이미지와 같이 앞면 패널에 있는 전원 버튼을 눌러 서버를 켭니다.
   전원 버튼 레이블이 표시된 하드웨어 어플라이언스 전면입니다.



전원 버튼 레이블이 표시된 하드웨어 어플라이언스 전면입니다.

다음 단계

[하드웨어 어플라이언스 콘솔 액세스]

하드웨어 어플라이언스 콘솔 액세스

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

하드웨어 어플라이언스의 전원을 켜면 하드웨어 어플라이언스 콘솔이 모니터에 표시됩니다. 하드웨어 어플라이언스 콘솔은 관리자 암호를 설정하고, 초기 네트워크 파라미터를 구성하고, 지원 채널을 여는 데 사용할 수 AWS 있는 별 사용자 인터페이스를 제공합니다 AWS.

하드웨어 어플라이언스 콘솔로 작업하려면 키보드를 사용하여 텍스트를 입력하고, Up, Down, Right, Left Arrow 키를 사용하여 화면을 표시된 방향으로 이동합니다. Tab 키를 사용하여 화면 상의 항목에 따라 앞으로 이동합니다. 일부 설정에서 Shift+Tab 키를 눌러 순차적으로 뒤로 이동할 수 있습니다. Enter 키를 사용하여 선택 사항을 저장하거나 화면에 있는 버튼을 선택합니다.

하드웨어 어플라이언스 콘솔이 처음 나타나면 시작 페이지가 표시되고 콘솔에 액세스하기 전에 관리자 사용자 계정의 암호를 설정하라는 메시지가 표시됩니다.

관리자 암호를 설정하려면

- 로그인 암호 설정 프롬프트에서 다음을 수행합니다.

  a. 암호 설정에서 암호를 입력하고 Down arrow 키를 누릅니다.
  b. 확인에서 암호를 재입력하고 암호 저장을 선택합니다.

암호를 설정하면 하드웨어 콘솔 홈 페이지가 나타납니다. 홈 페이지에는 em1, em2, em3, em4 네트워크 인터페이스에 대한 네트워크 정보가 표시되며, 다음과 같은 메뉴 옵션이 있습니다.

- 네트워크 구성
- 서비스 콘솔 열기
- 암호 변경
- 로그아웃
- 지원 콘솔 열기

다음 단계

하드웨어 어플라이언스 네트워크 파라미터 구성

하드웨어 어플라이언스 네트워크 파라미터 구성

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

하드웨어 어플라이언스가 부팅되고 하드웨어 어플라이언스 콘솔 액세스에 설명된 대로 하드웨어 콘솔에서 관리자 사용자 암호를 설정한 후 다음 절차에 따라 하드웨어 어플라이언스가 AWS에 연결할 수 있도록 네트워크 파라미터를 구성합니다.

네트워크 주소를 설정하려면

1. 홈 페이지에서 네트워크 구성을 선택한 다음 `Enter` 키를 누릅니다. 네트워크 구성 페이지가 나타납니다. 네트워크 구성 페이지에 하드웨어 어플라이언스의 4개의 네트워크 인터페이스 각각에 대한 IP 및 DNS 정보가 표시되며, 각 인터페이스에 대해 DHCP 또는 정적 주소를 구성하는 메뉴 옵션이 포함되어 있습니다.
2. em1 인터페이스의 경우 다음 중 하나를 수행합니다:

   - DHCP(Dynamic Host Configuration Protocol) 서버에서 물리적 네트워크 포트에 할당한 IPv4 주소를 사용하려면 DHCP를 선택하고 `Enter` 키를 누릅니다.

     이 주소는 나중에 활성화 단계에서 사용할 수 있도록 기록해 둡니다.

   - 정적 IPv4 주소를 구성하려면 정적을 선택하고 `Enter` 키를 누릅니다.

     em1 네트워크 인터페이스의 유효한 IP 주소, 서브넷 마스크, 게이트웨이, DNS 서버 주소를 입력합니다.

     완료되었으면 저장을 선택한 다음 `Enter` 키를 눌러 구성을 저장합니다.

> **Note**
>
> 이 절차를 사용하여 em1 외에 다른 네트워크 인터페이스도 구성할 수 있습니다. 다른 인터페이스를 구성하는 경우 요구 사항에 나열된 AWS 엔드포인트에 대해 동일한 상시 연결을 제공해야 합니다.
> 하드웨어 어플라이언스 또는 Storage Gateway에서는 네트워크 본딩 및 LACP(Link Aggregation Control Protocol)를 지원하지 않습니다.
> 동일한 서브넷에 여러 개의 네트워크 인터페이스를 구성하는 것은 라우팅 문제를 일으킬 수 있으므로 권장하지 않습니다.

하드웨어 콘솔에서 로그아웃하려면

1. 뒤로를 선택하고 `Enter` 키를 눌러 홈 페이지로 돌아갑니다.
2. 로그아웃을 선택하고 `Enter` 키를 눌러 시작 페이지로 돌아갑니다.

다음 단계

AWS Storage Gateway 하드웨어 어플라이언스 활성화

AWS Storage Gateway 하드웨어 어플라이언스 활성화

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

IP 주소를 구성한 후 AWS Storage Gateway 콘솔의 하드웨어 페이지에이 IP 주소를 입력하여 하드웨어 어플라이언스를 활성화합니다. 활성화 프로세스를 통해 기기가 AWS 계정에 등록됩니다.

지원되는 중 하나에서 하드웨어 어플라이언스를 활성화하도록 선택할 수 있습니다 AWS 리전. 지원되는 목록은의 Storage Gateway 하드웨어 어플라이언스 리전을 AWS 리전참조하세요AWS 일반 참조.

AWS Storage Gateway 하드웨어 어플라이언스를 활성화하려면

1. AWS Storage Gateway 관리 콘솔을 열고 난 다음 하드웨어를 활성화하는 데 사용할 계정 보안 인증 정보로 로그인합니다.

   > **Note**
   >
   > 활성화를 위해서는 다음이 충족되어야 합니다.
   >
   > - 브라우저가 하드웨어 어플라이언스와 동일한 네트워크에 있어야 합니다.
   > - 방화벽이 인바운드 트래픽에 대해 어플라이언스에 포트 8080에서 HTTP에 액세스하도록 허용해야 합니다.

2. 페이지 왼쪽의 탐색 메뉴에서 하드웨어를 선택합니다.
3. 어플라이언스 활성화를 선택합니다.
4. IP 주소에서 하드웨어 어플라이언스용으로 구성한 IP 주소를 입력한 다음 연결을 선택합니다.

   IP 주소 구성에 대한 자세한 내용은 네트워크 파라미터 구성 섹션을 참조하세요.

5. 이름에서 하드웨어 어플라이언스의 이름을 입력합니다. 이름은 최대 255자 길이이며 스플래시 문자를 포함할 수 없습니다.
6. 하드웨어 어플라이언스 시간대에서 게이트웨이에 대한 대부분의 워크로드가 생성되는 현지 시간대를 입력하고 다음을 선택합니다.

   시간대는 하드웨어 업데이트가 수행되는 시간을 제어하며, 오전 2시가 기본 업데이트 예정 시간으로 사용됩니다. 시간대를 올바르게 설정하면 기본적으로 현지 근무일 시간 외에 업데이트가 이루어집니다.
7. 하드웨어 어플라이언스 세부 정보 섹션에서 활성화 파라미터를 검토하십시오. 필요한 경우 이전을 선택하여 돌아가서 변경할 수 있습니다. 그렇지 않으면 활성화를 선택하여 활성화를 완료하십시오.

하드웨어 어플라이언스가 성공적으로 활성화되었음을 나타내는 배너가 하드웨어 어플라이언스 개요 페이지에 나타납니다.

이제 어플라이언스가 계정에 연결됩니다. 다음 단계는 새 어플라이언스에서 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway를 구성하고 시작하는 것입니다.

다음 단계

하드웨어 어플라이언스에서 게이트웨이 생성

하드웨어 어플라이언스에서 게이트웨이 생성

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

배포의 모든 AWS Storage Gateway Hardware Appliance에서 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway를 생성할 수 있습니다.

하드웨어 어플라이언스에서 게이트웨이를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/storagegateway/home Storage Gateway 콘솔을 엽니다.
2. 게이트웨이 생성에 설명된 절차에 따라 배포하려는 Storage Gateway 유형을 설정, 연결 및 구성합니다.

Storage Gateway 콘솔에서 게이트웨이 생성이 완료되면 Storage Gateway 소프트웨어가 하드웨어 어플라이언스에 자동으로 설치되기 시작합니다. DHCP(Dynamic Host Configuration Protocol)를 사용하는 경우 게이트웨이가 콘솔에 온라인 상태로 표시되는 데 5~10분 정도 걸릴 수 있습니다. 설치된 게이트웨이에 정적 IP 주소를 할당하려면 게이트웨이에 대한 IP 주소 구성을 참조하세요.

설치된 게이트웨이에 고정 IP 주소를 할당하려면 어플라이언스에서 사용할 수 있도록 게이트웨이의 네트워크 인터페이스를 구성합니다.

다음 단계

하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성

하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

하드웨어 어플라이언스를 활성화하기 전에 물리적 네트워크 인터페이스에 IP 주소를 할당했습니다. 이제 어플라이언스를 활성화하고 Storage Gateway를 시작했으므로 하드웨어 어플라이언스에서 실행되는 Storage Gateway 가상 머신에 다른 IP 주소를 할당해야 합니다. 하드웨어 어플라이언스에 설치된 게이트웨이에 고정 IP 주소를 할당하려면 게이트웨이 로컬 콘솔에서 해당 게이트웨이의 IP 주소를 구성합니다. 애플리케이션(예: NFS 또는 SMB 클라이언트)이 IP 주소에 연결됩니다. 게이트웨이 로컬 콘솔은 서비스 콘솔 열기 옵션을 사용하여 하드웨어 어플라이언스 콘솔에서 액세스할 수 있습니다.

애플리케이션에서 작동하도록 어플라이언스에서 IP 주소를 구성하려면

1. 하드웨어 콘솔에서 서비스 콘솔 열기를 선택한 다음 `Enter` 키를 눌러 게이트웨이 로컬 콘솔의 로그인 페이지를 엽니다.
2. AWS Storage Gateway 로컬 콘솔 로그인 페이지에 네트워크 구성 및 기타 설정을 변경하기 위해 로그인하라는 메시지가 표시됩니다.

   기본 계정은 `admin`이고 기본 암호는 `password`입니다.

   > **Note**
   >
   > AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 게이트웨이 콘솔에 해당하는 번호를 입력한 다음 `passwd` 명령을 실행하여 기본 암호를 변경하는 것이 좋습니다. 명령을 실행하는 방법에 대한 정보는 로컬 콘솔에서 Storage Gateway 명령 실행 섹션을 참조하세요. Storage Gateway 콘솔에서 암호를 설정할 수도 있습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정 단원을 참조하십시오.

3. AWS 어플라이언스 활성화 - 구성 페이지에는 다음 메뉴 옵션이 포함되어 있습니다.

   - HTTP/SOCKS 프록시 구성
   - 네트워크 구성
   - 네트워크 연결 테스트
   - 시스템 리소스 점검 조회
   - 시스템 시간 관리
   - 라이선스 정보
   - 명령 프롬프트

   > **Note**
   >
   > 일부 옵션은 특정 게이트웨이 유형 또는 호스트 플랫폼에만 표시됩니다.

   해당 숫자를 입력하여 네트워크 구성 페이지로 이동합니다.
4. 게이트웨이 IP 주소를 구성하려면 다음 중 하나를 수행합니다.

- DHCP(Dynamic Host Configuration Protocol) 서버에서 할당한 IP 주소를 사용하려면 DHCP 구성에 해당하는 숫자를 입력한 후 다음 페이지에 유효한 DHCP 구성 정보를 입력합니다.
- 정적 IP 주소를 할당하려면 정적 IP 구성에 해당하는 숫자를 입력한 후 다음 페이지에 유효한 IP 주소 및 DNS 정보를 입력합니다.

> **Note**
>
> 여기서 지정한 IP 주소는 하드웨어 어플라이언스 활성화 중에 사용된 IP 주소와 동일한 서브넷에 있어야 합니다.

게이트웨이 로컬 콘솔을 종료하려면

- `Crtl+]`(닫는 대괄호) 키를 누릅니다. 하드웨어 콘솔이 표시됩니다.

> **Note**
>
> 키 입력을 통해서만 게이트웨이 로컬 콘솔을 종료할 수 있습니다.

하드웨어 어플라이언스가 활성화되고 구성되면 콘솔에 어플라이언스가 나타납니다. 이제 Storage Gateway 콘솔에서 게이트웨이에 대한 설정 및 구성 절차를 계속 진행할 수 있습니다. 지침은 Amazon S3 File Gateway 구성 섹션을 참조하세요.

하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

하드웨어 어플라이언스에 배포한 특정 Storage Gateway가 더 이상 필요하지 않은 경우 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거할 수 있습니다. 게이트웨이 소프트웨어를 제거한 후 새

게이트웨이를 배포하거나 Storage Gateway 콘솔에서 하드웨어 어플라이언스 자체를 삭제할 수 있습니다. 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거하려면 다음 절차를 수행합니다.

하드웨어 어플라이언스에서 게이트웨이를 제거하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 콘솔 페이지 왼쪽의 탐색 창에서 하드웨어를 선택한 다음 게이트웨이 소프트웨어를 제거할 어플라이언스의 하드웨어 어플라이언스 이름을 선택합니다.
3. 작업 드롭다운 메뉴에서 게이트웨이 제거를 선택합니다.

   확인 대화 상자가 표시됩니다.
4. 지정된 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거할 것인지 확인한 다음 확인 상자에 `remove`라는 단어를 입력합니다.
5. 제거를 선택하여 게이트웨이 소프트웨어를 영구적으로 제거합니다.

> **Note**
>
> 게이트웨이 소프트웨어를 제거한 후에는 작업을 취소할 수 없습니다. 특정 게이트웨이 유형의 경우 삭제 시 데이터 특히, 캐시된 데이터를 잃을 수 있습니다. 게이트웨이 삭제에 대한 자세한 내용은 게이트웨이 삭제 및 연결된 리소스 제거 섹션을 참조하세요.

게이트웨이를 제거해도 콘솔에서 하드웨어 어플라이언스가 삭제되지는 않습니다. 하드웨어 어플라이언스는 향후 게이트웨이 배포를 위해 남아 있습니다.

AWS Storage Gateway 하드웨어 어플라이언스 삭제

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

이미 활성화한 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 필요하지 않은 경우 AWS 계정에서 어플라이언스를 완전히 삭제할 수 있습니다.

> **Note**
>
> 어플라이언스를 다른 AWS 계정으로 이동하려면 먼저 다음 절차에 따라 어플라이언스를 삭제한 다음 게이트웨이의 지원 채널을 열고 지원 에 문의하여 소프트 재설정을 수행해야 AWS 리전합니다. 자세한 내용은 온프레미스에서 호스팅되는 게이트웨이 문제를 해결하는 데 도움이 되는 지원 액세스 켜기온프레미스.

하드웨어 어플라이언스를 삭제하려면

1. 하드웨어 어플라이언스에 게이트웨이를 설치한 경우, 먼저 게이트웨이를 제거해야 어플라이언스를 삭제할 수 있습니다. 하드웨어 어플라이언스에서 게이트웨이를 제거하는 방법은 하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거 섹션을 참조하세요.
2. Storage Gateway 콘솔의 하드웨어 페이지에서 삭제할 하드웨어 어플라이언스를 선택합니다.
3. 작업에서 어플라이언스 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.
4. 지정된 하드웨어 어플라이언스를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

   하드웨어 어플라이언스를 삭제할 경우 어플라이언스에 설치된 게이트웨이와 연결된 모든 리소스가 삭제됩니다. 그러나 하드웨어 어플라이언스 자체의 데이터는 삭제되지 않습니다.

게이트웨이 생성

이 페이지의 개요 섹션에서는 Storage Gateway 생성 프로세스의 작동 방식에 대한 개괄적인 개요를 제공합니다. Storage Gateway 콘솔을 사용하여 특정 유형의 게이트웨이를 생성하는 단계별 절차는 다음 주제를 참조하세요.

- Amazon S3 File Gateway 생성 및 활성화
- Amazon FSx File Gateway 생성 및 활성화
- Tape Gateway 생성 및 활성화
- Volume Gateway 생성 및 활성화

개요 - 게이트웨이 활성화

게이트웨이 활성화에는 게이트웨이 설정, 연결 AWS, 설정 검토 및 활성화가 포함됩니다.

게이트웨이 설정

Storage Gateway를 설정하려면 먼저 생성할 게이트웨이 유형과 게이트웨이 가상 어플라이언스를 실행할 호스트 플랫폼을 선택합니다. 그런 다음 원하는 플랫폼용 게이트웨이 가상 어플라이언스 템플릿을 다운로드하여 온프레미스 환경에 배포합니다. Storage Gateway를 선호하는 리셀러로부터 주문하는 물리적 하드웨어 어플라이언스 또는 AWS 클라우드 환경의 Amazon EC2 인스턴스로 배포할 수도 있습니다. 게이트웨이 어플라이언스를 배포할 때 가상화 호스트에 로컬 물리적 디스크 공간을 할당합니다.

에 연결 AWS

다음 단계는 게이트웨이를 AWS에 연결하는 것입니다. 이렇게 하려면 먼저 게이트웨이 가상 어플라이언스와 클라우드의 서비스 간의 통신에 사용할 AWS 서비스 엔드포인트 유형을 선택합니다. 이 엔드포인트는 퍼블릭 인터넷에서 액세스할 수도 있고, 사용자가 네트워크 보안 구성을 완전히 제어할 수 있도록 Amazon VPC 내에서만 액세스할 수도 있습니다. 그런 다음 게이트웨이의 IP 주소 또는 정품 인증 키를 지정합니다. 이 정보는 게이트웨이 어플라이언스의 로컬 콘솔에 연결하여 얻을 수 있습니다.

검토 및 활성화

이제 선택한 게이트웨이 및 연결 옵션을 검토하고 필요한 경우 변경할 수 있습니다. 모든 설정이 원하는 대로 완료되었으면 게이트웨이를 활성화하면 됩니다. 활성화된 게이트웨이를 사용하기 전에 몇 가지 추가 설정을 구성하고 스토리지 리소스를 생성해야 합니다.

개요 - 게이트웨이 구성

Storage Gateway를 활성화한 후에는 몇 가지 추가 구성을 수행해야 합니다. 이 단계에서는 게이트웨이 호스트 플랫폼에서 프로비저닝한 물리적 스토리지를 게이트웨이 어플라이언스에서 캐시 또는 업로드 버퍼로 사용하도록 할당합니다. 그런 다음 Amazon CloudWatch Logs 및 CloudWatch 경보를 사용하여 게이트웨이의 상태를 모니터링하는 데 도움이 되는 설정을 구성하고, 필요한 경우 게이트웨이를 식별하는 데 도움이 되는 태그를 추가합니다. 활성화되고 구성된 게이트웨이를 사용하기 전에 먼저 스토리지 리소스를 생성해야 합니다.

개요 - 스토리지 리소스

Storage Gateway를 활성화하고 구성한 후에는 사용할 클라우드 스토리지 리소스를 생성해야 합니다. 생성한 게이트웨이 유형에 따라 Storage Gateway 콘솔을 사용하여 연결할 볼륨, 테이프 또는 Amazon S3 또는 Amazon FSx 파일 공유를 생성합니다. 각 게이트웨이 유형은 해당 리소스를 사용하여 관련 유형의 네트워크 스토리지 인프라를 에뮬레이션하고 여기에 기록한 데이터를 AWS 클라우드로 전송합니다.

Amazon S3 File Gateway 생성 및 활성화

이 섹션에서는 AWS Storage Gateway에서 File Gateway를 생성, 배포 및 활성화하는 방법에 대한 지침을 얻을 수 있습니다.

주제

- Amazon S3 File Gateway 설정
- Amazon S3 File Gateway를에 연결 AWS
- 설정 검토 및 Amazon S3 File Gateway 활성화
- Amazon S3 File Gateway 구성

Amazon S3 File Gateway 설정

새 S3 File Gateway를 설정하려면

1. https://console.aws.amazon.com/storagegateway/home/ AWS Management Console 를 열고 게이트웨이를 생성할 AWS 리전 를 선택합니다.
2. 게이트웨이 생성을 선택하여 게이트웨이 설정 페이지를 엽니다.

3. 게이트웨이 설정 섹션에서 다음을 수행합니다.

   a. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 게이트웨이가 생성된 후 이 이름으로 검색하면 AWS Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 찾을 수 있습니다.

   b. 게이트웨이 표준 시간대에서 게이트웨이를 배포하려는 전 세계 지역의 현지 시간대를 선택합니다.

4. 게이트웨이 옵션 섹션의 게이트웨이 유형에서 Amazon S3 File Gateway를 선택합니다.

5. 플랫폼 옵션 섹션에서 다음을 수행합니다.

   a. 호스트 플랫폼에서 게이트웨이를 배포할 플랫폼을 선택합니다. 그런 다음 Storage Gateway 콘솔 페이지에 표시된 플랫폼별 지침에 따라 호스트 플랫폼을 설정합니다. 다음 옵션 중에서 선택할 수 있습니다.

      - VMware ESXi - VMware ESXi를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
      - Microsoft Hyper-V - Microsoft Hyper-V를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
      - Linux KVM - Linux 커널 기반 가상 머신(KVM)을 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다. 제안된 부팅 구성은 제공된 aws-storage-gateway.xml 파일을 참조하세요. File Gateway 2.x, Volume Gateway 3.x 및 Tape Gateway 3.x에는 보안 부팅이 비활성화된 UEFI 부팅 모드(loader_secure=no)가 필요합니다.
      - Nutanix AHV - Linux 커널 기반 가상 머신(KVM)을 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다. 동일한 이미지가 Linux KVM 및 Nutanix AHV 하이퍼바이저 환경 모두에서 작동합니다.
      - Amazon EC2 - 게이트웨이를 호스팅할 Amazon EC2 인스턴스를 구성하고 시작합니다.
      - 하드웨어 어플라이언스 -에서 전용 물리적 하드웨어 어플라이언스를 주문 AWS 하여 게이트웨이를 호스팅합니다.

   b. 게이트웨이 설정 확인의 확인란을 선택하여 선택한 호스트 플랫폼에 대한 배포 단계를 수행했는지 확인합니다. 하드웨어 어플라이언스 호스트 플랫폼에는 이 단계가 해당되지 않습니다.

6. 게이트웨이가 설정되었으므로 게이트웨이를 연결하고 통신할 방법을 선택해야 합니다 AWS. 다음을 선택하여 계속 진행합니다.

Amazon S3 File Gateway를에 연결 AWS

새 S3 파일 게이트웨이를에 연결하려면 AWS

1. Amazon S3 File Gateway 설정에 설명된 절차를 아직 완료하지 않은 경우 해당 절차를 완료합니다. 완료되면 다음을 선택하여 AWS Storage Gateway 콘솔에서에 연결 AWS 페이지를 엽니다.
2. 게이트웨이 연결 옵션 섹션의 연결 옵션에서 AWS에 대한 게이트웨이를 식별하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

   - IP 주소 - 해당 필드에 게이트웨이의 IP 주소를 입력합니다. 이 IP 주소는 공용이거나 현재 네트워크 내에서 액세스할 수 있어야 하며 웹 브라우저에서 연결할 수 있어야 합니다.

     게이트웨이 IP 주소는 하이퍼바이저 클라이언트에서 게이트웨이의 로컬 콘솔에 로그인하거나 Amazon EC2 인스턴스 세부 정보 페이지에서 복사하여 얻을 수 있습니다. 자세한 내용은 게이트웨이 IP 주소 가져오기 단원을 참조하십시오.
   - 정품 인증 키 - 해당 필드에 게이트웨이의 정품 인증 키를 입력합니다. 게이트웨이의 로컬 콘솔을 사용하여 정품 인증 키를 생성할 수 있습니다. 게이트웨이의 IP 주소를 사용할 수 없는 경우 이 옵션을 선택합니다.
3. 엔드포인트 옵션 섹션에서 다음과 같이 실행합니다.

   a. 서비스 엔드포인트에서 게이트웨이가 통신하는 데 사용할 엔드포인트 유형을 선택합니다 AWS. 다음 옵션 중에서 선택할 수 있습니다.

      - 퍼블릭 액세스 - 게이트웨이는 퍼블릭 인터넷을 AWS 통해와 통신합니다. 이 옵션을 선택하는 경우 FIPS 준수 엔드포인트 확인란을 사용하여 연결이 연방 정보 처리 표준(FIPS)을 준수해야 하는지 여부를 지정합니다.

        > **Note**
        >
        > 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-2 검증 암호화 모듈이 필요한 경우 FIPS 준수 엔드포인트를 사용합니다. 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.
        > FIPS 서비스 엔드포인트는 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

      - VPC 호스팅 - 게이트웨이는 Virtual Private Cloud(VPC)와의 프라이빗 연결을 AWS 통해와 통신하므로 네트워크 설정을 제어할 수 있습니다. 이 옵션을 선택하는 경우 드롭다운 목록

에서 VPC 엔드포인트 ID를 선택하여 기존 VPC 엔드포인트를 지정해야 합니다. VPC 엔드포인트 도메인 이름 시스템(DNS) 이름 또는 IP 주소를 제공할 수도 있습니다.

> **Note**
>
> 게이트웨이를 생성하는 데 현재 사용 중인 계정 외의 AWS 계정 에 속하는 VPC 엔드포인트를 지정하려면 해당 DNS 이름 또는 IP 주소를 제공해야 합니다.

b. IP 버전에서 게이트웨이가 AWS와 통신하는 데 사용할 프로토콜 버전 및 엔드포인트를 선택합니다.

> **Note**
>
> 게이트웨이의 IP 주소는 여기에 지정한 IP 버전과 일치해야 합니다. 듀얼 스택 엔드포인트는 IPv4 및 IPv6 연결을 수락하지만 선택한 IP 버전을 통해서만 게이트웨이와 통신합니다.

4. 게이트웨이를 연결할 방법을 선택했으므로 게이트웨이를 활성화 AWS해야 합니다. 다음을 선택하여 계속 진행합니다.

설정 검토 및 Amazon S3 File Gateway 활성화

설정을 검토하고 새 S3 File Gateway를 활성화하려면

1. 다음 주제에 설명된 절차를 아직 완료하지 않은 경우 완료합니다.

   - Amazon S3 File Gateway 설정
   - Amazon S3 File Gateway를에 연결 AWS

   완료했으면 다음을 선택하여 AWS Storage Gateway 콘솔에서 검토 및 활성화 페이지를 엽니다.

2. 페이지에서 각 섹션의 초기 게이트웨이 세부 정보를 검토합니다.
3. 섹션에 오류가 있는 경우 편집을 선택하여 해당 설정 페이지로 돌아가서 변경합니다.

> **Important**
>
> 게이트웨이가 활성화된 후에는 게이트웨이 옵션 또는 연결 설정을 수정할 수 없습니다.

4. 게이트웨이를 활성화했으므로 로컬 스토리지 디스크를 할당하고 로깅을 구성하기 위한 최초 구성을 수행해야 합니다. 다음을 선택하여 계속 진행합니다.

Amazon S3 File Gateway 구성

새 S3 File Gateway에서 최초 구성을 수행하려면

1. 다음 주제에 설명된 절차를 아직 완료하지 않은 경우 완료합니다.

   - Amazon S3 File Gateway 설정
   - Amazon S3 File Gateway를에 연결 AWS
   - 설정 검토 및 Amazon S3 File Gateway 활성화

   완료했으면 다음을 선택하여 AWS Storage Gateway 콘솔에서 게이트웨이 구성 페이지를 엽니다.
2. 스토리지 구성 섹션에서 드롭다운 목록을 사용하여 최소 150기가바이트(GiB) 용량의 로컬 디스크를 하나 이상 캐시에 할당합니다. 이 섹션에 나열된 로컬 디스크는 호스트 플랫폼에서 프로비저닝한 물리적 스토리지에 해당합니다.
3. CloudWatch 로그 그룹 섹션에서 게이트웨이의 상태를 모니터링하기 위해 Amazon CloudWatch Logs를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

   - 새 로그 그룹 생성 - 게이트웨이를 모니터링할 새 로그 그룹을 설정합니다.
   - 기존 로그 그룹 사용 - 해당 드롭다운 목록에서 기존 로그 그룹을 선택합니다.
   - 로깅 비활성화 - 게이트웨이를 모니터링하는 데 Amazon CloudWatch Logs를 사용하지 않습니다.

   > **Note**
   >
   > Storage Gateway 상태 로그를 수신하려면 로그 그룹 리소스 정책에 다음 권한이 있어야 합니다. ## ### ##을 배포에 대한 특정 로그 그룹 resourceArn 정보로 바꿉니다.

   ```
   "Sid": "AWSLogDeliveryWrite20150319",
         "Effect": "Allow",
         "Principal": {
           "Service": [
             "delivery.logs.amazonaws.com"
           ]
   ```

```
        },
        "Action": [
          "logs:CreateLogStream",
          "logs:PutLogEvents"
        ],
        "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-
stream:*"
```

'Resource' 요소는 개별 로그 그룹에 명시적으로 권한을 적용하려는 경우에만 필요합니다.

4. CloudWatch 경보 섹션에서 게이트웨이 지표가 정의된 한도를 벗어날 때 알리도록 Amazon CloudWatch 경보를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

   - Storage Gateway의 권장 경보 생성 - 게이트웨이 생성 시 모든 권장 CloudWatch 경보를 자동으로 생성합니다. 권장 경보에 대한 자세한 내용은 CloudWatch 경보 이해를 참조하세요.

     Note

     이 기능을 사용하려면 CloudWatch 정책 권한이 필요합니다. 이 권한은 사전 구성된 Storage Gateway 전체 액세스 정책의 일부로 자동 부여되지 않습니다. 권장 CloudWatch 경보를 생성하기 전에 보안 정책이 다음 권한을 부여하는지 확인하세요.

     - `cloudwatch:PutMetricAlarm` - 경보 생성
     - `cloudwatch:DisableAlarmActions` - 경보 작업 끄기
     - `cloudwatch:EnableAlarmActions` - 경보 작업 켜기
     - `cloudwatch:DeleteAlarms` - 경보 삭제

   - 사용자 지정 경보 생성 - 게이트웨이 지표에 대해 알리도록 새 CloudWatch 경보를 구성합니다. 경보 생성을 선택하여 Amazon CloudWatch 콘솔에서 지표를 정의하고 경보 작업을 지정합니다. 지침은 Amazon CloudWatch 사용 설명서에서 Amazon CloudWatch 경보 사용을 참조하세요.
   - 경보 없음 - 게이트웨이 지표에 대한 CloudWatch 알림을 수신하지 않습니다.

5. (선택 사항) 태그 섹션에서 새 태그 추가를 선택한 다음 대소문자를 구분하여 키-값 페어를 입력하면 AWS Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 검색하고 필터링하는 데 도움이 됩니다. 이 단계를 반복하여 필요한 만큼 태그를 추가합니다.

6. (선택 사항) VMware 고가용성 구성 확인 섹션에서 게이트웨이가 VMware 고가용성(HA) 클러스터의 일부인 VMware 호스트에 배포된 경우 VMware HA 확인을 선택하여 HA 구성이 제대로 작동하는지 테스트합니다.

> **Note**
>
> 이 섹션은 VMware 호스트 플랫폼에서 실행 중인 게이트웨이에만 표시됩니다. 게이트웨이 구성 프로세스를 완료하는 데는 이 단계가 필요하지 않습니다. 게이트웨이의 HA 구성은 언제든지 테스트할 수 있습니다. 확인에는 몇 분 정도 걸리며 Storage Gateway 가상 머신(VM)을 재부팅합니다.

7. 구성을 선택하여 게이트웨이 생성을 완료합니다.

   새 게이트웨이의 상태를 확인하려면 AWS Storage Gateway 의 게이트웨이 개요 페이지에서 해당 게이트웨이를 검색합니다.

게이트웨이를 생성했으므로 게이트웨이에서 사용할 파일 공유를 생성해야 합니다. 관련 지침은 파일 공유 생성을 참조하세요.

Virtual Private Cloud(VPC)에서 게이트웨이 활성화

온프레미스 게이트웨이 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 이 연결을 사용하여 게이트웨이를 활성화하고 퍼블릭 인터넷을 통해 통신하지 않고 AWS 스토리지 서비스로 데이터를 전송하도록 구성할 수 있습니다. Amazon VPC 서비스를 사용하면 사용자 지정 Virtual Private Cloud(VPC)에서 프라이빗 네트워크 인터페이스 엔드포인트를 포함한 AWS 리소스를 시작할 수 있습니다. VPC를 통해 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서에서 Amazon VPC란 무엇인가요?를 참조하세요.

VPC에서 게이트웨이를 활성화하려면 Amazon VPC 콘솔을 사용하여 Storage Gateway용 VPC 엔드포인트를 생성하고 VPC 엔드포인트 ID를 가져온 다음, 게이트웨이를 생성하고 활성화할 때 이 VPC 엔드포인트 ID를 지정하세요. 자세한 내용은 Amazon S3 File Gateway를에 연결 AWS.

VPC를 통해 데이터를 전송하도록 S3 File Gateway를 구성하려면 Amazon S3에 대해 별도의 VPC 엔드포인트를 생성한 다음 게이트웨이에 대한 파일 공유를 생성할 때 이 VPC 엔드포인트를 지정해야 합니다.

> **Note**
>
> Storage Gateway용 VPC 엔드포인트를 생성하는 리전과 동일한 리전에서 게이트웨이를 활성화해야 하며, 파일 공유용으로 구성하는 Amazon S3 스토리지는 Amazon S3용 VPC 엔드포인트를 생성하는 리전과 동일한 리전에 있어야 합니다.

Storage Gateway용 VPC 엔드포인트 생성

여기 나온 지침에 따라 VPC 엔드포인트를 생성합니다. Storage Gateway용 VPC 엔드포인트가 이미 있는 경우 이를 사용할 수 있습니다.

Storage Gateway용 VPC 엔드포인트를 생성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/vpc/ Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택하고 엔드포인트 생성을 선택합니다.
3. 엔드포인트 생성 페이지에서 AWS 서비스를 서비스 범주로 선택합니다.
4. 서비스 이름에서 `com.amazonaws.`*`region`*`.storagegateway`를 선택합니다. 예: `com.amazonaws.us-east-2.storagegateway`.
5. VPC에서 VPC를 선택하고 해당 가용 영역 및 서브넷을 기록합니다.
6. DNS 이름 활성화가 선택되지 않았는지 확인합니다.
7. 보안 그룹에서 VPC에 사용할 보안 그룹을 선택합니다. 기본 보안 그룹을 적용할 수 있습니다. 다음 모든 TCP 포트가 보안 그룹에서 허용되는지 확인합니다.
   - TCP 443
   - TCP 1026
   - TCP 1027
   - TCP 1028
   - TCP 1031
   - TCP 2222
8. 엔드포인트 생성을 선택합니다. 엔드포인트의 초기 상태는 대기 중입니다. 엔드포인트가 생성되면 방금 생성한 VPC 엔드포인트의 ID를 기록합니다.
9. 엔드포인트가 생성되면 엔드포인트를 선택한 다음 새 VPC 엔드포인트를 선택합니다.

10. 선택한 스토리지 게이트웨이 엔드포인트의 세부 정보 탭의 DNS 이름에서 가용 영역을 지정하지 않은 첫 번째 DNS 이름을 사용합니다. DNS 이름은 다음 예와 비슷해야 합니다. `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

VPC 엔드포인트가 있으므로 게이트웨이를 생성하고 활성화할 수 있습니다. 자세한 내용은 Amazon S3 File Gateway 생성 및 활성화를 참조하세요.

활성화 키 가져오기에 대한 자세한 내용은 게이트웨이의 활성화 키 가져오기를 참조하세요.

> **Important**
>
> VPC를 통해 데이터를 전송하도록 S3 File Gateway를 구성하려면 Amazon S3에 대해 별도의 VPC 엔드포인트를 생성한 다음 게이트웨이에 대한 파일 공유를 생성할 때 이 VPC 엔드포인트를 지정해야 합니다.
> 이렇게 하려면 위와 동일한 단계를 따르되 서비스 이름에 대해 `com.amazonaws.region.s3`를 선택한 다음 서브넷/보안 그룹 대신 S3 엔드포인트를 연결할 라우팅 테이블을 선택합니다. 지침은 게이트웨이 엔드포인트 생성을 참조하세요.

파일 공유 생성

이 섹션에서는 NFS(Network File System) 또는 SMB(Server Message Block) 프로토콜을 사용하여 액세스할 수 있는 파일 공유를 만드는 방법에 대한 지침을 찾을 수 있습니다.

NFS 공유를 생성하면 기본적으로 NFS 서버에 대한 액세스 권한을 가진 사람이라면 누구나 NFS 파일 공유에 액세스할 수 있습니다. IP 주소에 따라 클라이언트로 액세스를 제한할 수 있습니다.

SMB 파일 공유를 생성할 때 다음 세 가지 인증 모드 중 하나를 사용할 수 있습니다.

- Microsoft Active Directory(AD) 액세스 권한을 사용한 파일 공유. 인증된 모든 Microsoft AD 사용자가 이 파일 공유 유형에 대해 액세스 권한을 얻게 됩니다.
- 제한된 액세스 권한을 사용한 SMB 파일 공유. 사용자가 지정한 특정 도메인 사용자 및 그룹만 액세스가 허용됩니다(허용 목록을 통해). 사용자와 그룹의 액세스가 거부될 수도 있습니다(거부 목록을 통해).
- 게스트 액세스 권한을 사용한 SMB 파일 공유. 게스트 암호를 입력하는 사용자는 누구나 이 파일 공유에 대한 액세스 권한을 얻게 됩니다.

> **Note**
>
> NFS 파일 공유를 위해 게이트웨이를 통해 내보내진 파일 공유는 POSIX 권한을 지원합니다. SMB 파일 공유를 위해 ACL(액세스 제어 목록)을 사용하여 파일 공유의 파일 및 폴더에 대한 권한을 관리할 수 있습니다. 자세한 내용은 Windows ACL을 사용하여 SMB 파일 공유 액세스 제한 단원을 참조하십시오.

하나의 File Gateway는 유형이 다른 파일 공유를 하나 이상 호스팅할 수 있습니다. File Gateway 하나에 다수의 NFS 및 SMB 파일 공유를 가질 수 있습니다.

> **Important**
>
> 파일 공유를 생성하려면 파일 게이트웨이에서 AWS Security Token Service ()를 활성화해야 합니다AWS STS. 파일 게이트웨이를 생성하는 AWS 리전 에서 AWS STS 가 활성화되지 않은 경우 활성화합니다. 활성화 방법에 대한 자세한 내용은 AWS Identity and Access Management 사용 설명서의 AWS 리전 AWS Security Token Service 에서 활성화 및 비활성화를 AWS STS참조하세요.

주제

게이트웨이 데이터를 업로드할 때 예상치 못한 비용 방지

NFS 클라이언트가 파일을 File Gateway에 쓰면 File Gateway는 파일의 데이터를 Amazon S3에 업로드한 다음 메타데이터를 업로드합니다. 파일 데이터를 업로드하면 S3 객체가 생성되고 파일의 메타데이터를 업로드하면 S3 객체의 메타데이터가 업데이트됩니다. 이 프로세스는 객체의 추가 버전을 생성합니다. S3 버전 관리가 켜져 있으면 두 버전이 모두 저장됩니다.

File Gateway에 저장된 파일의 메타데이터를 변경하면 새 S3 객체가 생성되어 기존 S3 객체를 대체합니다. 이 동작은 파일을 편집해도 새 파일이 생성되지 않는 파일 시스템에서 파일을 편집하는 것과 다릅니다. 각 파일 작업이 Amazon S3 스토리지와 상호 작용하는 방식을 이해할 수 있도록 AWS Storage Gateway와 함께 사용할 모든 파일 작업을 테스트합니다.

File Gateway에서 데이터를 업로드할 때 Amazon S3에서 S3 버전 관리 및 리전 간 복제(CRR) 사용을 신중하게 고려하세요. S3 버전 관리가 켜져 있을 때 파일 게이트웨이에서 Amazon S3로 파일을 업로드하면 일반적으로 둘 이상의 S3 객체 버전이 생성됩니다.

여러 단계로 수행되는 파일 업로드와 같은 대용량 파일 및 파일 쓰기 패턴과 관련된 특정 워크플로는 저장된 S3 객체 버전의 수를 늘릴 수 있습니다. File Gateway 캐시가 높은 파일 쓰기 속도로 인해 공간을 확보해야 하는 경우 여러 S3 객체 버전이 생성될 수 있습니다. 이러한 시나리오는 S3 버전 관리가 켜져 있는 경우 S3 스토리지를 늘리고 CRR과 관련된 전송 비용을 높입니다. 각 파일 작업이 Amazon S3 스토리지와 상호 작용하는 방식을 이해할 수 있도록 Storage Gateway와 함께 사용할 모든 파일 작업을 테스트합니다.

Rsync 유틸리티를 File Gateway와 함께 사용하면 캐시에 임시 파일이 생성되고 Amazon S3에 임시 S3 객체가 생성됩니다. 이 경우 S3 Standard-Infrequent Access(S3 Standard-IA) 스토리지 클래스에서 조기 삭제 요금이 발생합니다.

Amazon S3에서 File Gateway에 저장된 객체 암호화

S3 File Gateway는 Amazon S3에 저장하는 데이터에 대해 다음과 같은 서버 측 암호화 방법을 지원합니다.

- SSE-S3 - 기본적으로 Amazon S3 버킷에 업로드되는 모든 새 객체는 Amazon S3 관리형 키를 통한 서버 측 암호화를 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 관리형 키로 서버 측 암호화 사용을 참조하세요.
- SSE-KMS - AWS Key Management Service (AWS KMS) 관리형 키를 사용한 서버 측 암호화를 사용하도록 파일 공유를 구성할 수 있습니다. AWS KMS 는 안전하고 가용성이 높은 하드웨어와 소프트웨어를 결합하여 클라우드에 맞게 조정된 키 관리 시스템을 제공하는 서비스입니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS Key Management Service란 무엇입니까?를 참조하세요.
- DSSE-KMS - AWS KMS 키를 사용한 이중 계층 서버 측 암호화는 객체가 Amazon S3에 업로드될 때 객체에 두 계층의 암호화를 적용합니다. 이는 다중 계층 암호화에 대한 규정 준수 표준을 충족하는 데 도움이 됩니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 이중 계층 서버 측 암호화 사용을 참조하세요.

> **Note**
>
> DSSE-KMS 및 AWS KMS 키 사용에는 추가 요금이 부과됩니다. 자세한 내용은 AWS KMS 요금을 참조하십시오.

Storage Gateway 콘솔 또는 Storage Gateway API를 사용하여 새 파일 공유를 생성할 때 암호화 방법을 지정할 수 있습니다. 콘솔 절차는 사용자 지정 구성으로 NFS 파일 공유 생성 또는 사용자 지정 구성으로 SMB 파일 공유 생성 섹션을 참조하세요. 해당 API 명령에 대한 자세한 내용은 AWS Storage Gateway API 참조의 CreateNFSFileShare 또는 CreateSMBFileShare를 참조하세요.

Storage Gateway 콘솔 또는 Storage Gateway API를 사용하여 기존 파일 공유의 암호화 설정을 업데이트할 수도 있습니다. 콘솔 절차는 기존 파일 공유의 서버 측 암호화 방법 변경 섹션을 참조하세요. 해당 API 명령에 대한 자세한 내용은 AWS Storage Gateway API 참조의 UpdateNFSFileShare 또는 UpdateSMBFileShare를 참조하세요.

> **Note**
>
> 암호화 방법을 업데이트한 후 게이트웨이는 Amazon S3에서 생성하는 모든 새 객체와 향후 업데이트하거나 수정하는 모든 저장된 객체에 대해 새 방법을 사용합니다. 기존 Amazon S3 객체는 게이트웨이에 의해 업데이트되거나 수정된 경우에만 새 암호화 방법을 수신합니다.

> **Important**
>
> 파일 공유가 데이터를 저장하는 Amazon S3 버킷과 동일한 암호화 유형을 사용하는지 확인하세요.
> 암호화에 SSE-KMS 또는 DSSE-KMS를 사용하도록 File Gateway를 구성하는 경우 파일 공유와 연결된 IAM 역할에 `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt*`, `kms:GenerateDataKey` 및 `kms:DescribeKey` 권한을 수동으로 추가해야 합니다. 자세한 내용은 Storage Gateway에 대한 자격 증명 기반 정책(IAM 정책) 사용을 참조하세요.

NFS 파일 공유 생성

NFS(Network File System) 프로토콜은 Unix 기반 시스템을 위한 상태 저장 파일 공유 프로토콜입니다. NFS 지원 클라이언트와 NFS 서버가 통신하면 클라이언트는 원격 프로시저 호출(RPC)을 사용하여 서버에서 파일 또는 디렉터리를 요청합니다. 서버는 파일 또는 디렉터리를 사용할 수 있고 클라이언트에 필요한 액세스 권한이 있는지 확인합니다. 그런 다음 서버는 클라이언트에 파일 또는 디렉터리를 원격으로 탑재하고 가상 연결을 통해 액세스를 공유합니다. 클라이언트 작업의 경우 NFS는 로컬 파일에 액세스하는 것과 유사한 원격 서버 파일을 사용합니다.

> **Note**
>
> NFS 프로토콜은 사용자당 최대 16개의 그룹을 지원합니다. 사용자가 16개 이상의 그룹에 속한 경우 NFS 파일 공유를 마운트하는 데 문제가 있을 수 있습니다. 탑재 문제를 방지하려면 사용자가 NFS 파일 공유에 액세스할 때 16개 이하의 그룹에 속해야 합니다.

다음 주제에서는 File Gateway에 대한 NFS 파일 공유를 생성하는 다양한 방법을 설명합니다.

목차

기본 구성을 사용하여 NFS 파일 공유 생성

이 섹션에서는 미리 구성된 기본 설정을 사용하여 새 NFS(Network File System) 파일 공유를 생성하는 방법을 설명합니다. 이 방법을 기본 배포, 개인용, 테스트에 사용하거나 나중에 편집하고 사용자 지정

하려는 여러 파일 공유를 빠르게 배포하는 방법으로 사용합니다. 이 절차를 사용하여 생성하는 파일 공유의 기본 설정 목록은 NFS 파일 공유의 기본 구성 설정을 참조하세요. 보다 세분화된 제어가 필요하거나 파일 공유에 고급 설정을 사용하려면 사용자 지정 구성을 사용하여 NFS 파일 공유 생성을 참조하세요.

> **Note**
>
> 가상 프라이빗 클라우드(VPC)를 통해 파일 공유를 Amazon S3에 연결해야 하는 경우 사용자 지정 구성 절차를 따라야 합니다. 파일 공유를 생성한 후에는 파일 공유에 대한 VPC 설정을 편집할 수 없습니다.

> **Important**
>
> File Gateway에서 데이터를 업로드할 때 S3 버전 관리, 교차 리전 복제 또는 Rsync 유틸리티를 사용하면 상당한 비용에 영향을 미칠 수 있습니다. 자세한 내용은 File Gateway에서 데이터를 업로드할 때 예상치 못한 비용 방지를 참조하세요.

기본 구성을 사용하여 NFS 파일 공유를 생성하려면:

1. https://console.aws.amazon.com/storagegateway/home/ AWS Storage Gateway 콘솔을 열고 왼쪽 탐색 창에서 파일 공유를 선택합니다.
2. 파일 공유 생성을 선택합니다.
3. 게이트웨이의 경우 목록에서 Amazon S3 File Gateway를 선택합니다.
4. 파일 공유 프로토콜에서 NFS를 선택합니다.
5. S3 버킷에서 다음 중 한 가지를 실행합니다.
   - 드롭다운 목록에서 계정의 기존 Amazon S3 버킷을 선택합니다.
   - 드롭다운 목록에서 다른 계정의 버킷을 선택한 다음 교차 계정 버킷 이름에 버킷 이름을 입력합니다.
   - 새 S3 버킷 생성을 선택한 다음 새 버킷의 Amazon S3 엔드포인트가 AWS 리전 있는 을 선택하고 고유한 S3 버킷 이름을 입력합니다. 완료했으면 S3 버킷 생성을 선택합니다.

     새 버킷을 생성하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서에서 S3 버킷을 생성하려면 어떻게 해야 합니까?를 참조하세요.

> **Note**
>
> S3 File Gateway는 버킷 이름에 마침표(.)가 있는 Amazon S3 버킷을 지원하지 않습니다. 버킷 이름이 Amazon S3의 버킷 이름 지정 규칙을 준수하는지 확인합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

6. 기본 구성의 설정을 검토한 다음 파일 공유 생성을 선택하여 기본 구성을 사용하여 새 NFS 파일 공유를 생성합니다.

NFS 파일 공유가 생성되면 파일 공유의 세부 정보 탭에 있는 AWS Storage Gateway 콘솔에서 해당 구성 설정을 볼 수 있습니다. 파일 공유 탑재에 대한 자세한 내용은 클라이언트에 NFS 파일 공유 탑재를 참조하세요.

NFS 파일 공유의 기본 구성 설정

다음 설정은 기본 구성을 사용하여 생성하는 모든 새 NFS 파일 공유에 적용됩니다. 파일 공유를 생성한 후 AWS Storage Gateway 콘솔의 파일 공유 페이지에서 파일 공유를 선택하여 해당 구성에 대한 세부 정보를 볼 수 있습니다.

> **Important**
>
> 기본 NFS 파일 공유 구성은 버킷이 다른 AWS 계정에서 소유한 경우에도 파일 공유에 매핑된 S3 버킷의 소유자에게 전체 파일 제어 및 액세스 권한을 제공합니다. 파일 공유를 사용하여 또 다른 계정이 소유한 버킷의 객체에 액세스하는 방법에 대한 자세한 내용은 교차 계정 액세스에서 파일 공유 사용 섹션을 참조하세요.

설정	기본값	참고
Amazon S3 위치	파일 공유는 Amazon S3 버킷에 직접 연결되며 버킷과 이름이 동일합니다. 이 버킷은 게이트웨이에서 파일을 저장하거나 가져올 때 사용됩니다.	이름에는 접두사가 포함되지 않습니다.

설정	기본값	참고
AWS S3용 PrivateLink	파일 공유는 가상 프라이빗 클라우드(VPC)의 인터페이스 엔드포인트를 통해 Amazon S3에 연결되지 않습니다.	
파일 업로드 알림	꺼짐	
새 객체에 대한 스토리지 클래스	Amazon S3 Standard	자주 액세스하는 객체 데이터를 지리적으로 떨어져 있는 여러 가용 영역에 저장합니다. Amazon S3 Standard 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 자주 액세스하는 객체의 스토리지 클래스를 참조하세요.
암호화(Encryption)	S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화	S3 File Gateway가 업로드, 업데이트 또는 수정하는 모든 Amazon S3 객체는 기본적으로 Amazon S3 관리형 키를 사용한 서버 측 암호화로 암호화됩니다.

설정	기본값	참고
객체 메타데이터	MIME 유형 추측	이렇게 하면 Storage Gateway가 파일 확장명을 기반으로 업로드된 객체의 MIME(Multipurpose Internet Mail Extension) 유형을 추측할 수 있습니다. 이 옵션을 사용하려면 파일 공유와 연결된 Amazon S3 버킷에 대한 액세스 제어 목록(ACL)이 켜져 있어야 합니다. ACL이 꺼져 있으면 파일 공유는 Amazon S3 버킷에 액세스할 수 없으며 무기한으로 사용 불가 상태로 유지됩니다.
요청자 지불 활성화	꺼짐	자세한 내용은 요청자 지불 버킷을 참조하세요.
감사 로그	꺼짐	Amazon CloudWatch 그룹에 대한 로깅은 기본적으로 꺼져 있습니다.

설정	기본값	참고
S3 버킷에 대한 액세스	새 IAM 역할 생성	기본 옵션을 사용하면 File Gateway가 사용자를 대신하여 새로운 IAM 역할과 액세스 정책을 만들 수 있습니다. 모든 NFS 클라이언트에 대한 액세스가 허용됩니다. 지원되는 NFS 클라이언트에 대한 자세한 내용은 File Gateway에 지원되는 NFS 및 SMB 클라이언트 섹션을 참조하세요.
탑재 옵션	• 스쿼시 레벨 - 루트 스쿼시 • 다음으로 내보내기 - 읽기-쓰기	Squash 레벨의 기본값은 원격 superuser(루트)에 대한 액세스는 사용자 식별자(UID)(65534) 및 그룹 식별자(GID)(65534)에 매핑됨을 의미합니다.
파일 메타데이터 기본값	• 디렉터리 권한 – 0777 • 파일 권한 – 0666 • 사용자 식별자(UID) – 65534 • 그룹 식별자(GID) – 65534	

사용자 지정 구성으로 NFS 파일 공유 생성

다음 절차에 따라 사용자 지정 구성으로 NFS(Network File System) 파일 공유를 생성합니다. 기본 구성 설정을 사용하여 NFS 파일 공유를 생성하려면 기본 구성을 사용하여 NFS 파일 공유 생성을 참조하세요.

> **Important**
>
> File Gateway에서 데이터를 업로드할 때 S3 버전 관리, 교차 리전 복제 또는 Rsync 유틸리티를 사용하면 상당한 비용에 영향을 미칠 수 있습니다. 자세한 내용은 File Gateway에서 데이터를 업로드할 때 예상치 못한 비용 방지를 참조하세요.

사용자 지정 설정을 사용하여 NFS 파일 공유를 생성하려면

1. https://console.aws.amazon.com/storagegateway/home/ AWS Storage Gateway 콘솔을 열고 왼쪽 탐색 창에서 파일 공유를 선택합니다.
2. 파일 공유 생성을 선택합니다.
3. 구성 사용자 지정을 선택합니다. 지금은 이 페이지의 다른 필드를 무시할 수 있습니다. 후속 단계에서 게이트웨이, 프로토콜 및 스토리지 설정을 구성하라는 메시지가 표시됩니다.
4. 게이트웨이의 경우 드롭다운 목록에서에 대한 새 파일 공유의 Amazon S3 File Gateway를 선택합니다.
5. CloudWatch 로그 그룹의 경우 드롭다운 목록에서 다음 중 하나를 선택합니다.

   - 이 파일 공유에 대한 로깅을 끄려면 로깅 비활성화를 선택합니다.
   - 이 파일 공유에 대한 새 로그 그룹을 자동으로 생성하려면 Storage Gateway에서 생성을 선택합니다.
   - 이 파일 공유에 대한 상태 및 리소스 알림을 기존 로그 그룹에 보내려면 목록에서 원하는 그룹을 선택합니다.

   감사 로그에 대한 자세한 내용은 S3 File Gateway 감사 로그 이해를 참조하세요.
6. (선택 사항) 태그 - 선택 사항에서 새 태그 추가를 선택한 다음 파일 공유에 대한 키와 값을 입력합니다.

   태그는 Storage Gateway 리소스를 분류하는 데 도움이 되는 대/소문자를 구분하는 키-값 페어입니다. 태그를 추가하면 파일 공유를 더 쉽게 필터링하고 검색할 수 있습니다. 이 단계를 반복하여 최대 50개의 태그를 추가할 수 있습니다.

   마친 후에는 다음을 선택합니다.
7. S3 버킷의 경우 다음 중 하나를 수행하여 파일 공유가 파일을 저장하고 검색할 위치를 지정합니다.

   - 파일 공유를 Amazon Web Services 계정의 기존 S3 버킷에 직접 연결하려면 드롭다운 목록에서 버킷 이름을 선택합니다.
   - 파일 공유를 생성하는 데 사용하는 계정이 아닌 Amazon Web Services 계정이 소유한 기존 S3 버킷에 연결하려면 드롭다운 목록에서 다른 계정의 버킷을 선택한 다음 교차 계정 버킷 이름을 입력합니다.
   - 파일 공유를 새 S3 버킷에 연결하려면 새 S3 버킷 생성을 선택한 다음 새 버킷의 Amazon S3 엔드포인트가 있는 리전을 선택하고 고유한 S3 버킷 이름을 입력합니다. 완료했으면 S3 버킷 생

성을 선택합니다. 새 버킷 생성에 대한 자세한 내용은 Amazon S3 사용 설명서의 S3 버킷을 생성하려면 어떻게 해야 합니까?를 참조하세요.

- 액세스 포인트 이름을 사용하여 파일 공유를 S3 버킷에 연결하려면 드롭다운 목록에서 Amazon S3 액세스 포인트 이름을 선택한 다음 액세스 포인트 이름을 입력합니다. 새 액세스 포인트를 생성해야 하는 경우 S3 액세스 포인트 생성을 선택할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트 생성을 참조하세요. 액세스 포인트에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리 및 액세스 포인트에 대한 액세스 제어 위임을 참조하세요.
- 액세스 포인트 별칭을 사용하여 파일 공유를 S3 버킷에 연결하려면 드롭다운 목록에서 Amazon S3 액세스 포인트 별칭을 선택한 다음 액세스 포인트 별칭을 입력합니다. 새 액세스 포인트를 생성해야 하는 경우 S3 액세스 포인트 생성을 선택할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트 생성을 참조하세요. 액세스 포인트 별칭에 대한 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트에 버킷 스타일 별칭 사용을 참조하세요.

> **Note**
>
> 각 파일 공유는 하나의 S3 버킷에만 연결할 수 있지만 여러 파일 공유는 동일한 버킷에 연결할 수 있습니다. 둘 이상의 파일 공유를 동일한 버킷에 연결하는 경우 읽기/쓰기 충돌을 방지하기 위해 중복되지 않는 고유한 S3 버킷 접두사를 사용하도록 각 파일 공유를 구성해야 합니다.
>
> S3 File Gateway는 버킷 이름에 마침표(.)가 있는 Amazon S3 버킷을 지원하지 않습니다. 버킷 이름이 Amazon S3의 버킷 이름 지정 규칙을 준수하는지 확인합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

8. (선택 사항) S3 버킷 접두사에 Amazon S3에서 생성하는 객체에 적용할 파일 공유의 접두사를 입력합니다. 접두사는 기존 파일 구조의 디렉터리와 마찬가지로 S3에서 데이터를 구성하는 방법입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.

> **Note**
>
> - 둘 이상의 파일 공유를 동일한 버킷에 연결하는 경우 읽기/쓰기 충돌을 방지하기 위해 중복되지 않는 고유한 접두사를 사용하도록 각 파일 공유를 구성해야 합니다.
> - 접두사는 슬래시(/)로 끝나야 합니다.
> - 파일 공유가 생성된 후에는 접두사를 수정하거나 삭제할 수 없습니다.

9. 리전의 경우 드롭다운 목록에서 버킷 AWS 리전 의 S3 엔드포인트가 있는를 선택합니다. 이 필드는 S3 버킷에 대한 다른 계정의 액세스 포인트 또는 버킷을 지정하는 경우에만 나타납니다.
10. 새 객체의 스토리지 클래스의 경우 드롭다운 목록에서 스토리지 클래스를 선택합니다. 스토리지 클래스에 대한 자세한 내용은 File Gateway와 함께 스토리지 클래스 사용을 참조하세요.
11. IAM 역할에서 다음 중 하나를 수행하여 파일 공유에 대한 IAM 역할을 구성합니다.

    - 파일 공유가 제대로 작동하는 데 필요한 권한이 있는 새 IAM 역할을 자동으로 생성하려면 드롭다운 목록에서 Storage Gateway에서 생성을 선택합니다.
    - 기존 IAM 역할을 사용하려면 드롭다운 목록에서 역할 이름을 선택합니다.
    - 새 IAM 역할을 만들려면 새 역할 생성을 선택합니다. 자세한 지침은 AWS Identity and Access Management 사용 설명서의 AWS 서비스에 권한을 위임할 역할 생성을 참조하세요.

    IAM 역할이 파일 공유와 S3 버킷 간의 액세스를 제어하는 방법에 대한 자세한 내용은 Amazon S3 버킷에 대한 액세스 권한 부여를 참조하세요.
12. 프라이빗 링크의 경우 Virtual Private Cloud(VPC)의 프라이빗 엔드포인트를 AWS 사용하여와 통신하도록 파일 공유를 구성해야 하는 경우에만 다음을 수행합니다. 그렇지 않은 경우 이 단계를 건너뜁니다. 자세한 내용은 AWS PrivateLink 안내서의 PrivateLink란 AWS 무엇입니까?를 참조하세요.

    a. VPC 엔드포인트 사용을 선택합니다.

    b. VPC 엔드포인트 식별 기준에 대해 다음 중 하나를 수행하십시오.

        - VPC 엔드포인트 ID를 선택한 다음 VPC 엔드포인트 드롭다운 목록에서 사용할 엔드포인트를 선택합니다.
        - DNS 이름을 선택한 다음 사용하려는 엔드포인트의 DNS 이름을 입력합니다.
13. 암호화에서 파일 공유가 Amazon S3에 저장하는 데이터에 사용할 서버 측 암호화 유형을 선택합니다.

    - Amazon S3(SSE-S3)로 관리되는 서버 측 암호화를 사용하려면 S3 관리형 키(SSE-S3)를 선택합니다.

      자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 관리형 키로 서버 측 암호화 사용을 참조하세요.
    - AWS Key Management Service(SSE-KMS)로 관리되는 서버 측 암호화를 사용하려면 KMS 관리형 키(SSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS

키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS Key Management Service란 무엇입니까?를 AWS KMS참조하세요.

- AWS Key Management Service(DSSE-KMS)로 관리되는 이중 계층 서버 측 암호화를 사용하려면 AWS Key Management Service 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS 키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

  DSSE-KMS에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 이중 계층 서버 측 암호화 사용을 참조하세요.

  > **Note**
  >
  > DSSE-KMS 및 AWS KMS 키 사용에는 추가 요금이 부과됩니다. 자세한 내용은 AWS KMS 요금을 참조하십시오.
  > 목록에 없는 별칭이 있는 AWS KMS 키를 지정하거나 다른 AWS 계정의 AWS KMS 키를 사용하려면를 사용해야 합니다 AWS Command Line Interface. 비대칭 KMS 키는 지원되지 않습니다. 자세한 내용을 알아보려면 AWS Storage Gateway API 참조의 CreateNFSFileShare를 참조하세요.

> **Important**
>
> 파일 공유가 데이터를 저장하는 Amazon S3 버킷과 동일한 암호화 유형을 사용하는지 확인하세요.

14. MIME 유형 추측에서 미디어 MIME 유형 추측을 선택하여 Storage Gateway가 파일 확장명을 기반으로 업로드된 객체의 미디어 유형을 추측할 수 있도록 합니다.
15. 파일 공유 이름에 파일 공유의 이름을 입력합니다.

    > **Note**
    >
    > 유효한 NFS 파일 공유 이름에는 `a-z`, `A-Z`, `0-9`, `-`, `.` 및 `_` 문자만 포함될 수 있습니다.

16. 게이트웨이가 Amazon S3에 파일을 성공적으로 업로드할 때 CloudWatch 로그 이벤트를 기록하도록 하려면 업로드 이벤트에서 게이트웨이에 의해 파일이 성공적으로 업로드되면 이벤트 로깅을

선택합니다. 알림 지연은 최근 클라이언트 쓰기 작업과 `ObjectUploaded` 로그 알림 생성 사이의 최소 지연을 제어합니다. 클라이언트는 짧은 시간 동안 파일에 소규모 쓰기 작업을 많이 수행할 수 있으므로 동일한 파일에 대해 여러 개의 알림이 빠르게 연속해서 생성되지 않도록 이 파라미터를 최대한 길게 설정하는 것이 좋습니다. 자세한 내용은 파일 업로드 알림 받기를 참조하세요.

> **Note**
>
> 이 설정은 객체가 S3에 업로드되는 타이밍에 영향을 주지 않으며 알림 타이밍에만 영향을 줍니다.
> 이 설정은 알림이 전송되는 정확한 시간을 지정하기 위한 것이 아닙니다. 경우에 따라 게이트웨이가 알림을 생성하고 전송하는 데 지정된 지연 시간보다 오래 걸릴 수 있습니다.

마친 후에는 다음을 선택합니다.

17.

18. 파일 공유 프로토콜에서 NFS를 선택합니다.

19. 클라이언트 액세스의 경우 다음 중 하나를 수행하여 파일 공유에 액세스할 수 있는 NFS 클라이언트를 지정합니다.

    - 모든 수신 클라이언트 연결을 수락하려면 모든 NFS 클라이언트를 선택합니다.
    - 특정 IP 주소에서만 수신 클라이언트 연결을 수락하려면 특정 NFS 클라이언트를 선택한 다음 클라이언트 추가를 선택합니다. 허용된 클라이언트에서 연결을 수락할 유효한 IP 주소 또는 CIDR 블록을 지정합니다. 추가 IP 주소를 지정해야 하는 경우 다른 클라이언트 추가를 선택합니다.

    > **Note**
    >
    > 특정 NFS 클라이언트 옵션을 사용하여 파일 공유에 대한 액세스를 제한하도록 구성하는 것이 좋습니다. 그렇지 않으면 네트워크 상의 모든 클라이언트가 파일 공유에 마운트될 수 있습니다.

20. 액세스 유형에서 다음 중 하나를 선택합니다.

    - 클라이언트가 파일 공유에서 파일을 읽고 쓸 수 있도록 허용하려면 읽기/쓰기를 선택합니다.
    - 클라이언트가 파일을 읽지만 파일 공유에 쓰지 않도록 허용하려면 읽기 전용을 선택합니다.

> **Note**
>
> Microsoft Windows 클라이언트에 탑재된 파일 공유의 경우, 읽기 전용을 선택하면 예상하지 못한 오류가 발생하여 폴더를 생성할 수 없다는 메시지가 표시될 수도 있습니다. 이 메시지는 무시해도 됩니다.

21. 액세스 수준에서 다음 중 하나를 선택합니다.

    - Root squash (default)(Root Squash(기본값)) 원격 superuser(root)에 대한 액세스가 UID(65534) 및 GID(65534)로 매핑됩니다.
    - All squash(모든 Squash): 모든 사용자 액세스가 사용자 ID(UID)(65534) 및 그룹 ID(65534)로 매핑됩니다.
    - No root squash(Root Squash 없음) 원격 superuser(root)는 root로서 액세스를 받습니다.

22. (선택 사항) S3에서 자동 캐시 새로 고침의 경우 캐시 새로 고침 간격 설정을 선택한 다음 TTL(Time To Live)을 사용하여 파일 공유의 캐시를 새로 고치는 시간을 분 또는 일 단위로 설정합니다. TTL은 마지막 새로 고침 이후 경과한 시간입니다. TTL 간격이 경과한 후 디렉터리에 액세스하면 File Gateway가 Amazon S3 버킷에서 해당 디렉터리의 콘텐츠를 새로 고칩니다.

    > **Note**
    >
    > 이 값을 30분 미만으로 설정하면 대량의 Amazon S3 객체가 자주 생성되거나 삭제되는 경우 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.

23. 게이트웨이가 S3 버킷에서 검색한 기존 객체에 파일 메타데이터(Unix 권한 포함)를 적용하도록 하려면 파일 메타데이터 기본값에서 게이트웨이에서 생성하거나 수정하지 않은 S3 객체의 기본 메타데이터 변경을 선택합니다. 해당 필드에 적용할 디렉터리 권한, 파일 권한, 사용자 ID 및 그룹 ID를 지정합니다.

24. 파일 소유권 및 권한에서 S3 버킷을 소유한 계정이 파일 공유에 의해 버킷에 기록된 모든 객체를 완전히 제어하도록 하려면 읽기, 쓰기, 편집 및 삭제 권한을 포함하여 게이트웨이에서 생성된 파일의 전체 소유권 부여를 선택합니다. AWS S3

    마친 후에는 다음을 선택합니다.

25. 파일 공유 구성을 검토합니다. 변경하려는 섹션의 설정을 수정하려면 편집을 선택합니다. 마친 후에는 Create(생성)를 선택합니다.

NFS 파일 공유가 생성되면 파일 공유의 세부 정보 탭에 있는 AWS Storage Gateway 콘솔에서 해당 구성 설정을 볼 수 있습니다. 파일 공유를 탑재하는 지침은 클라이언트에 NFS 파일 공유 탑재를 참조하세요.

SMB 파일 공유 생성

SMB(Server Message Block) 프로토콜은 Microsoft Windows 제품군에 깊이 통합되어 있으며 Windows 운영 체제의 기본 파일 공유 프로토콜로 남아 있습니다. 클라이언트-서버 통신 프로세스는 개략적인 수준에서 보면 NFS와 유사하지만 일부 세부 정보 및 운영 메커니즘에는 차이가 있습니다. 예를 들어 SMB에서는 파일 시스템이 로컬 SMB 클라이언트에 탑재되지 않습니다. 대신 SMB 서버에서 호스팅되는 네트워크 공유는 네트워크 경로를 통해 액세스됩니다.

이 섹션의 주제에서는 File Gateway에 대한 SMB 파일 공유를 생성하는 다양한 방법을 설명합니다.

목차

기본 구성을 사용하여 SMB 파일 공유 생성

이 섹션에서는 미리 구성된 기본 설정을 사용하여 새 SMB(Server Message Block) 파일 공유를 생성하는 방법을 설명합니다. 이 방법을 기본 배포, 개인용, 테스트에 사용하거나 나중에 편집하고 사용자 지정하려는 여러 파일 공유를 빠르게 배포하는 방법으로 사용합니다. 이 절차를 사용하여 생성하는 파일 공유의 기본 설정 목록은 SMB 파일 공유의 기본 구성 설정을 참조하세요. 보다 세분화된 제어가 필요하거나 파일 공유에 고급 설정을 사용하려면 사용자 지정 구성을 사용하여 SMB 파일 공유 생성을 참조하세요.

> **Note**
>
> 가상 프라이빗 클라우드(VPC)를 통해 파일 공유를 Amazon S3에 연결해야 하는 경우 사용자 지정 구성 절차를 따라야 합니다. 파일 공유를 생성한 후에는 파일 공유에 대한 VPC 설정을 편집할 수 없습니다.

> **Important**
>
> File Gateway에서 데이터를 업로드할 때 S3 버전 관리, 교차 리전 복제 또는 Rsync 유틸리티를 사용하면 상당한 비용에 영향을 미칠 수 있습니다. 자세한 내용은 File Gateway에서 데이터를 업로드할 때 예상치 못한 비용 방지를 참조하세요.

사전 조건

파일 공유를 생성하기 전에 다음을 수행합니다.

- File Gateway의 SMB 보안 설정을 구성합니다. 지침은 게이트웨이의 보안 수준 설정을 참조하세요.
- 또한 인증을 위해 Microsoft Active Directory 또는 게스트 액세스를 구성합니다. 지침은 Active Directory를 사용하여 사용자 인증 또는 파일 공유에 대한 게스트 액세스 제공을 참조하세요.
- 보안 그룹에서 필요한 포트가 열려 있는지 확인합니다. 자세한 내용은 포트 요구 사항을 참조하세요.

기본 구성을 사용하여 SMB 파일 공유를 생성하려면:

1. https://console.aws.amazon.com/storagegateway/home/ AWS Storage Gateway 콘솔을 열고 왼쪽 탐색 창에서 파일 공유를 선택합니다.
2. 파일 공유 생성을 선택합니다.
3. 게이트웨이의 경우 드롭다운 목록에서 Amazon S3 File Gateway를 선택합니다.
4. 파일 공유 프로토콜에서 SMB를 선택합니다.
5. S3 버킷에서 다음 중 한 가지를 실행합니다.
   - 드롭다운 목록에서 계정의 기존 Amazon S3 버킷을 선택합니다.
   - 드롭다운 목록에서 다른 계정의 버킷을 선택한 다음 교차 계정 버킷 이름에 버킷 이름을 입력합니다.
   - 새 S3 버킷 생성을 선택한 다음 새 버킷의 Amazon S3 엔드포인트가 AWS 리전 있는 을 선택하고 고유한 S3 버킷 이름을 입력합니다. 완료했으면 S3 버킷 생성을 선택합니다.

     새 버킷을 생성하는 방법에 대한 자세한 내용은 Amazon S3 사용 설명서에서 S3 버킷을 생성하려면 어떻게 해야 합니까?를 참조하세요.

> **Note**
>
> S3 File Gateway는 버킷 이름에 마침표(.)가 있는 Amazon S3 버킷을 지원하지 않습니다. 버킷 이름이 Amazon S3의 버킷 이름 지정 규칙을 준수하는지 확인합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

6. 사용자 인증 드롭다운 목록에서 사용할 인증 방법을 선택합니다.

   - 회사 Microsoft Active Directory AWS Managed Microsoft AD 를 사용하거나 SMB 파일 공유에 대한 사용자 액세스를 인증하려면 Active Directory를 선택합니다. 이 방법을 사용하려면 게이트웨이를 도메인에 조인해야 합니다. 자세한 내용은 Active Directory를 사용하여 사용자 인증을 참조하세요.

     > **Note**
     >
     > Amazon EC2 게이트웨이와 AWS Managed Microsoft AD 함께를 사용하려면와 동일한 VPC에서 Amazon EC2 인스턴스를 생성하고 AWS Managed Microsoft AD, Amazon EC2 인스턴스에 `_workspaceMembers` 보안 그룹을 추가하고,의 관리자 자격 증명을 사용하여 AD 도메인에 조인해야 합니다 AWS Managed Microsoft AD.
     > 에 대한 자세한 내용은 AWS Directory Service 관리 안내서를 AWS Managed Microsoft AD참조하세요.
     > Amazon EC2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하세요.

     조인 상태가 게이트웨이가 이미 Active Directory 도메인에 조인되었음을 나타내는 경우 다음 단계로 진행합니다. 그렇지 않으면 다음을 수행하세요.

     1. 구성을 선택합니다.
     2. 도메인에 게이트웨이가 조인할 Active Directory 도메인의 이름을 입력합니다.
     3. 게이트웨이가 도메인에 조인하는 데 사용할 사용자 이름과 암호를 입력합니다.
     4. (선택 사항) 조직 단위(OU)에 Active Directory가 새 컴퓨터 객체에 사용하는 지정된 OU를 입력합니다.
     5. (선택 사항) 도메인 컨트롤러(DC)에 게이트웨이가 Active Directory에 연결할 DC의 이름을 입력합니다. DNS가 DC를 자동으로 선택할 수 있도록 이 필드를 비워 둘 수 있습니다.
     6. Active Directory 조인을 선택합니다.

> **Note**
>
> 도메인에 조인하면 게이트웨이 ID를 계정 이름(예: SGW-1234ADE)으로 사용하여 기본 컨테이너(조직 단위가 아님)에 Active Directory 계정이 생성됩니다. 이 계정의 이름은 사용자 지정할 수 없습니다.
>
> Active Directory 환경에서 도메인 조인 프로세스를 용이하게 하기 위해 계정을 사전 준비해야 하는 경우 이 계정을 미리 생성해야 합니다.
>
> Active Directory 환경에 새 컴퓨터 객체에 대해 지정된 OU가 있는 경우 도메인을 조인할 때 해당 OU를 지정해야 합니다.

- 구성한 게스트 암호를 제공하는 모든 사용자에게 암호로 보호되는 액세스 권한을 부여하려면 게스트 액세스를 선택합니다. 이 방법을 사용하기 위해 File Gateway가 Microsoft Active Directory 도메인의 일부일 필요는 없습니다. 구성을 선택하여 게스트 암호를 지정한 다음 저장을 선택합니다.

7. 기본 구성의 설정을 검토한 다음 파일 공유 생성을 선택하여 기본 구성을 사용하여 새 SMB 파일 공유를 생성합니다.

SMB 파일 공유가 생성되면 파일 공유의 세부 정보 탭에 있는 AWS Storage Gateway 콘솔에서 해당 구성 설정을 볼 수 있습니다. 파일 공유 탑재에 대한 자세한 내용은 클라이언트에 SMB 파일 공유 탑재를 참조하세요.

SMB 파일 공유의 기본 구성 설정

다음 설정은 기본 구성을 사용하여 생성하는 모든 새 SMB 파일 공유에 적용됩니다. 파일 공유를 생성한 후 AWS Storage Gateway 콘솔의 파일 공유 페이지에서 파일 공유를 선택하여 해당 구성에 대한 세부 정보를 볼 수 있습니다.

> **Important**
>
> 기본 SMB 파일 공유 구성은 버킷이 다른 Amazon Web Services 계정에서 소유한 경우에도 파일 공유에 매핑된 S3 버킷의 소유자에게 전체 파일 제어 및 액세스 권한을 제공합니다. 파일 공유를 사용하여 다른 계정이 소유한 버킷의 객체에 액세스하는 방법에 대한 자세한 내용은 교차 계정 액세스를 위한 파일 공유 사용을 참조하세요.

설정	기본값	참고
Amazon S3 위치	파일 공유는 Amazon S3 버킷에 직접 연결되며 버킷과 이름이 동일합니다. 이 버킷은 게이트웨이에서 파일을 저장하거나 가져올 때 사용됩니다.	이름에는 접두사가 포함되지 않습니다.
AWS S3용 PrivateLink	파일 공유는 가상 프라이빗 클라우드(VPC)의 인터페이스 엔드포인트를 통해 Amazon S3에 연결되지 않습니다.	
파일 업로드 알림	꺼짐	
새 객체에 대한 스토리지 클래스	Amazon S3 Standard	자주 액세스하는 객체 데이터를 지리적으로 떨어져 있는 여러 가용 영역에 저장합니다. Amazon S3 Standard 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 자주 액세스하는 객체의 스토리지 클래스를 참조하세요.
암호화(Encryption)	S3 관리형 키(SSE-S3)를 사용한 서버 측 암호화	S3 File Gateway가 업로드, 업데이트 또는 수정하는 모든 Amazon S3 객체는 기본적으로 Amazon S3 관리형 키를 사용한 서버 측 암호화로 암호화됩니다.
객체 메타데이터	MIME 유형 추측	이렇게 하면 Storage Gateway가 파일 확장명을 기반으로 업로드된 객체의 MIME(Multipurpose Internet Mail

설정	기본값	참고
		Extension) 유형을 추측할 수 있습니다. 이 옵션을 사용하려면 파일 공유와 연결된 Amazon S3 버킷에 대한 액세스 제어 목록(ACL)이 켜져 있어야 합니다. ACL이 꺼져 있으면 파일 공유는 Amazon S3 버킷에 액세스할 수 없으며 무기한으로 사용 불가 상태로 유지됩니다.
액세스 기반 열거	활성화되지 않음	디렉터리 열거 중 파일 공유의 파일 및 폴더는 모든 사용자에게 표시됩니다. 액세스 기반 열거는 SMB 파일 공유의 액세스 제어 목록(ACL)을 기반으로 해당 공유의 파일 및 폴더 열거를 필터링하는 시스템입니다.
요청자 지불 활성화	꺼짐	자세한 내용은 요청자 지불 버킷을 참조하세요.
기회 잠금	켜짐	이를 통해 파일 공유는 기회 잠금을 사용하여 파일 버퍼링 전략을 최적화할 수 있습니다. 대부분의 경우 기회 잠금을 활성화하면 성능이 향상되며, 특히 Windows 컨텍스트 메뉴와 관련하여 성능이 향상됩니다.
감사 로그	꺼짐	Amazon CloudWatch 그룹에 대한 로깅은 기본적으로 꺼져 있습니다.

설정	기본값	참고
대/소문자 구분 강제 적용	꺼짐	이 설정을 통해 클라이언트가 대/소문자 구분을 제어할 수 있습니다.
S3 버킷에 대한 액세스	새 IAM 역할 생성	기본 옵션을 사용하면 File Gateway가 사용자를 대신하여 새로운 IAM 역할과 액세스 정책을 만들 수 있습니다.

사용자 지정 구성으로 SMB 파일 공유 생성

다음 절차에 따라 사용자 지정 구성으로 SMB(Server Message Block) 파일 공유를 생성합니다. 기본 구성 설정을 사용하여 SMB 파일 공유를 생성하려면 기본 구성을 사용하여 SMB 파일 공유 생성을 참조하세요을 참조하세요.

> **Important**
>
> File Gateway에서 데이터를 업로드할 때 S3 버전 관리, 교차 리전 복제 또는 Rsync 유틸리티를 사용하면 상당한 비용에 영향을 미칠 수 있습니다. 자세한 내용은 File Gateway에서 데이터를 업로드할 때 예상치 못한 비용 방지를 참조하세요.

사전 조건

파일 공유를 생성하기 전에 다음을 수행합니다.

- File Gateway의 SMB 보안 설정을 구성합니다. 지침은 게이트웨이의 보안 수준 설정을 참조하세요.
- 또한 인증을 위해 Microsoft Active Directory 또는 게스트 액세스를 구성합니다. 지침은 Active Directory를 사용하여 사용자 인증 또는 파일 공유에 대한 게스트 액세스 제공을 참조하세요.
- 보안 그룹에서 필요한 포트가 열려 있는지 확인합니다. 자세한 내용은 포트 요구 사항을 참조하세요.

사용자 지정 설정을 사용하여 SMB 파일 공유를 생성하려면

1. https://console.aws.amazon.com/storagegateway/home/ AWS Storage Gateway 콘솔을 열고 왼쪽 탐색 창에서 파일 공유를 선택합니다.
2. 파일 공유 생성을 선택합니다.
3. 구성 사용자 지정을 선택합니다. 지금은 이 페이지의 다른 필드를 무시할 수 있습니다. 후속 단계에서 게이트웨이, 프로토콜 및 스토리지 설정을 구성하라는 메시지가 표시됩니다.
4. 게이트웨이의 경우 드롭다운 목록에서 Amazon S3 File Gateway를 선택합니다.
5. CloudWatch 로그 그룹의 경우 드롭다운 목록에서 다음 중 하나를 선택합니다.

   - 이 파일 공유에 대한 로깅을 끄려면 로깅 비활성화를 선택합니다.
   - 이 파일 공유에 대한 새 로그 그룹을 자동으로 생성하려면 Storage Gateway에서 생성을 선택합니다.
   - 이 파일 공유에 대한 상태 및 리소스 알림을 기존 로그 그룹에 보내려면 목록에서 원하는 그룹을 선택합니다.

   감사 로그에 대한 자세한 내용은 S3 File Gateway 감사 로그 이해를 참조하세요.
6. (선택 사항) 태그 - 선택 사항에서 새 태그 추가를 선택한 다음 파일 공유에 대한 키와 값을 입력합니다. 태그는 Storage Gateway 리소스를 분류하는 데 도움이 되는 대/소문자를 구분하는 키-값 페어입니다. 태그를 추가하면 파일 공유를 더 쉽게 필터링하고 검색할 수 있습니다. 이 단계를 반복하여 최대 50개의 태그를 추가할 수 있습니다.

   마친 후에는 다음을 선택합니다.
7. S3 버킷의 경우 다음 중 하나를 수행하여 파일을 저장하고 검색할 위치를 지정합니다.

   - 파일 공유를 Amazon Web Services 계정의 기존 S3 버킷에 직접 연결하려면 드롭다운 목록에서 버킷 이름을 선택합니다.
   - 파일 공유를 생성하는 데 사용하는 계정이 아닌 Amazon Web Services 계정이 소유한 기존 S3 버킷에 파일 공유를 연결하려면 드롭다운 목록에서 다른 계정의 버킷을 선택한 다음 교차 계정 버킷 이름을 입력합니다.
   - 파일 공유를 새 S3 버킷에 연결하려면 새 S3 버킷 생성을 선택한 다음 새 버킷의 Amazon S3 엔드포인트가 있는 리전을 선택하고 고유한 S3 버킷 이름을 입력합니다. 완료했으면 S3 버킷 생성을 선택합니다. 새 버킷 생성에 대한 자세한 내용은 Amazon S3 사용 설명서의 S3 버킷을 생성하려면 어떻게 해야 합니까?를 참조하세요.

- 액세스 포인트 이름을 사용하여 파일 공유를 S3 버킷에 연결하려면 드롭다운 목록에서 Amazon S3 액세스 포인트 이름을 선택한 다음 액세스 포인트 이름을 입력합니다. 새 액세스 포인트를 생성해야 하는 경우 S3 액세스 포인트 생성을 선택할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트 생성을 참조하세요. 액세스 포인트에 대한 자세한 내용은 Amazon S3 사용 설명서의 Amazon S3 액세스 포인트를 사용한 데이터 액세스 관리 및 액세스 포인트에 대한 액세스 제어 위임을 참조하세요.
- 액세스 포인트 별칭을 사용하여 파일 공유를 S3 버킷에 연결하려면 드롭다운 목록에서 Amazon S3 액세스 포인트 별칭을 선택한 다음 액세스 포인트 별칭을 입력합니다. 새 액세스 포인트를 생성해야 하는 경우 S3 액세스 포인트 생성을 선택할 수 있습니다. 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트 생성을 참조하세요. 액세스 포인트 별칭에 대한 자세한 내용은 Amazon S3 사용 설명서의 액세스 포인트에 버킷 스타일 별칭 사용을 참조하세요.

> **Note**
>
> 각 파일 공유는 하나의 S3 버킷에만 연결할 수 있지만 여러 파일 공유는 동일한 버킷에 연결할 수 있습니다. 둘 이상의 파일 공유를 동일한 버킷에 연결하는 경우 읽기/쓰기 충돌을 방지하기 위해 중복되지 않는 고유한 S3 버킷 접두사를 사용하도록 각 파일 공유를 구성해야 합니다.
>
> S3 File Gateway는 버킷 이름에 마침표(.)가 있는 Amazon S3 버킷을 지원하지 않습니다. 버킷 이름이 Amazon S3의 버킷 이름 지정 규칙을 준수하는지 확인합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 버킷 이름 지정 규칙을 참조하세요.

8. (선택 사항) S3 버킷 접두사에 Amazon S3에서 생성하는 객체에 적용할 파일 공유의 접두사를 입력합니다. 접두사는 기존 파일 구조의 디렉터리와 마찬가지로 S3에서 데이터를 구성하는 방법입니다. 자세한 내용은 Amazon S3 사용 설명서의 접두사를 사용하여 객체 구성하기를 참조하세요.

> **Note**
>
> - 둘 이상의 파일 공유를 동일한 버킷에 연결하는 경우 읽기/쓰기 충돌을 방지하기 위해 중복되지 않는 고유한 접두사를 사용하도록 각 파일 공유를 구성해야 합니다.
> - 접두사는 슬래시(/)로 끝나야 합니다.
> - 파일 공유가 생성된 후에는 접두사를 수정하거나 삭제할 수 없습니다.

9. 리전의 경우 드롭다운 목록에서 버킷 AWS 리전 의 S3 엔드포인트가 있는를 선택합니다. 이 필드는 S3 버킷에 대한 다른 계정의 액세스 포인트 또는 버킷을 지정하는 경우에만 나타납니다.

10. 새 객체의 스토리지 클래스의 경우 드롭다운 목록에서 스토리지 클래스를 선택합니다. 스토리지 클래스에 대한 자세한 내용은 File Gateway와 함께 스토리지 클래스 사용을 참조하세요.
11. IAM 역할에서 다음 중 하나를 수행하여 파일 공유에 대한 IAM 역할을 구성합니다.

    - 파일 공유가 제대로 작동하는 데 필요한 권한이 있는 새 IAM 역할을 자동으로 생성하려면 드롭다운 목록에서 Storage Gateway에서 생성을 선택합니다.
    - 기존 IAM 역할을 사용하려면 드롭다운 목록에서 역할 이름을 선택합니다.
    - 새 IAM 역할을 만들려면 새 역할 생성을 선택합니다. 자세한 지침은 AWS Identity and Access Management 사용 설명서의 AWS 서비스에 권한을 위임할 역할 생성을 참조하세요.

    IAM 역할이 파일 공유와 S3 버킷 간의 액세스를 제어하는 방법에 대한 자세한 내용은 Amazon S3 버킷에 대한 액세스 권한 부여를 참조하세요.
12. 프라이빗 링크의 경우 Virtual Private Cloud(VPC)의 프라이빗 엔드포인트를 AWS 사용하여와 통신하도록 파일 공유를 구성해야 하는 경우에만 다음을 수행합니다. 그렇지 않은 경우 이 단계를 건너뜁니다. 자세한 내용은 AWS PrivateLink 안내서의 PrivateLink란 AWS 무엇입니까?를 참조하세요.

    a. VPC 엔드포인트 사용을 선택합니다.

    b. VPC 엔드포인트 식별 기준에 대해 다음 중 하나를 수행하십시오.

        - VPC 엔드포인트 ID를 선택한 다음 VPC 엔드포인트 드롭다운 목록에서 사용할 엔드포인트를 선택합니다.
        - DNS 이름을 선택한 다음 사용하려는 엔드포인트의 DNS 이름을 입력합니다.
13. 암호화의 경우 File Gateway가 Amazon S3에 저장하는 객체를 암호화하는 데 사용할 암호화 키 유형을 선택합니다.

    - Amazon S3(SSE-S3)로 관리되는 서버 측 암호화를 사용하려면 S3 관리형 키(SSE-S3)를 선택합니다.

      자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 관리형 키로 서버 측 암호화 사용을 참조하세요.
    - AWS Key Management Service(SSE-KMS)로 관리되는 서버 측 암호화를 사용하려면 KMS 관리형 키(SSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS 키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS Key Management Service란 무엇입니까?를 AWS KMS참조하세요.

- AWS Key Management Service(DSSE-KMS)로 관리되는 이중 계층 서버 측 암호화를 사용하려면 AWS Key Management Service 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS 키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

  DSSE-KMS에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 이중 계층 서버 측 암호화 사용을 참조하세요.

  > **Note**
  >
  > DSSE-KMS 및 AWS KMS 키 사용에는 추가 요금이 부과됩니다. 자세한 내용은 AWS KMS 요금을 참조하십시오.
  > 목록에 없는 별칭이 있는 AWS KMS 키를 지정하거나 다른 AWS 계정의 AWS KMS 키를 사용하려면를 사용해야 합니다 AWS Command Line Interface. 비대칭 KMS 키는 지원되지 않습니다. 자세한 내용을 알아보려면 AWS Storage Gateway API 참조의 CreateSMBFileShare를 참조하세요.

> **Important**
>
> 파일 공유가 데이터를 저장하는 Amazon S3 버킷과 동일한 암호화 유형을 사용하는지 확인하세요.

14. MIME 유형 추측에서 미디어 MIME 유형 추측을 선택하여 Storage Gateway가 파일 확장명을 기반으로 업로드된 객체의 MIME(Multipurpose Internet Mail Extension) 유형을 추측할 수 있도록 합니다.
15. 파일 공유 이름에 파일 공유의 이름을 입력합니다.

    > **Note**
    >
    > 유효한 SMB 파일 공유 이름에는 [,],#,;,<,>,:,",\,/,|,?,*,+ 또는 ASCII 제어 문자 1-31이 포함될 수 없습니다.

16. 게이트웨이가 Amazon S3에 파일을 성공적으로 업로드할 때 CloudWatch 로그 이벤트를 기록하도록 하려면 업로드 이벤트에서 게이트웨이에 의해 파일이 성공적으로 업로드되면 이벤트 로깅을

선택합니다. 알림 지연은 최근 클라이언트 쓰기 작업과 `ObjectUploaded` 로그 알림 생성 사이의 지연을 제어합니다. 클라이언트는 짧은 시간 동안 파일에 소규모 쓰기 작업을 많이 수행할 수 있으므로 동일한 파일에 대해 여러 개의 알림이 빠르게 연속해서 생성되지 않도록 이 파라미터를 최대한 길게 설정하는 것이 좋습니다. 자세한 내용은 파일 업로드 알림 받기를 참조하세요.

> **Note**
>
> 이 설정은 객체가 S3에 업로드되는 타이밍에 영향을 주지 않으며 알림 타이밍에만 영향을 줍니다.
> 이 설정은 알림이 전송되는 정확한 시간을 지정하기 위한 것이 아닙니다. 경우에 따라 게이트웨이가 알림을 생성하고 전송하는 데 지정된 지연 시간보다 오래 걸릴 수 있습니다.

마친 후에는 다음을 선택합니다.

17. 파일 공유 프로토콜에서 SMB를 선택합니다.
18. 사용자 인증의 경우 드롭다운 목록에서 사용할 인증 방법을 선택합니다.

- 회사 Microsoft Active Directory AWS Managed Microsoft AD 를 사용하거나 SMB 파일 공유에 대한 사용자 액세스를 인증하려면 Active Directory를 선택합니다. 이 방법을 사용하려면 게이트웨이를 도메인에 조인해야 합니다. 자세한 내용은 Active Directory를 사용하여 사용자 인증을 참조하세요.

> **Note**
>
> Amazon EC2 게이트웨이와 AWS Managed Microsoft AD 함께를 사용하려면와 동일한 VPC에서 Amazon EC2 인스턴스를 생성하고 AWS Managed Microsoft AD, Amazon EC2 인스턴스에 `_workspaceMembers` 보안 그룹을 추가하고,의 관리자 자격 증명을 사용하여 AD 도메인에 조인해야 합니다 AWS Managed Microsoft AD.
> 에 대한 자세한 내용은 AWS Directory Service 관리 안내서를 AWS Managed Microsoft AD참조하세요.
> Amazon EC2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하세요.

조인 상태가 게이트웨이가 이미 Active Directory 도메인에 조인되었음을 나타내는 경우 다음 단계로 진행합니다. 그렇지 않으면 다음을 수행하세요.

1. 구성을 선택합니다.

2. 도메인에 게이트웨이가 조인할 Active Directory 도메인의 이름을 입력합니다.
3. 게이트웨이가 도메인에 조인하는 데 사용할 사용자 이름과 암호를 입력합니다.
4. (선택 사항) 조직 단위(OU)에 Active Directory가 새 컴퓨터 객체에 사용하는 지정된 OU를 입력합니다.
5. (선택 사항) 도메인 컨트롤러(DC)에 게이트웨이가 Active Directory에 연결할 DC의 이름을 입력합니다. DNS가 DC를 자동으로 선택할 수 있도록 이 필드를 비워 둘 수 있습니다.
6. Active Directory 조인을 선택합니다.

> **Note**
>
> 도메인에 조인하면 게이트웨이의 게이트웨이 ID를 계정 이름(예: SGW-1234ADE)으로 사용하여 기본 컨테이너(조직 단위가 아님)에 Active Directory 계정이 생성됩니다. 이 계정의 이름은 사용자 지정할 수 없습니다.
> Active Directory 환경에서 도메인 조인 프로세스를 용이하게 하기 위해 계정을 사전 준비해야 하는 경우 이 계정을 미리 생성해야 합니다.
> Active Directory 환경에 새 컴퓨터 객체에 대해 지정된 OU가 있는 경우 도메인을 조인할 때 해당 OU를 지정해야 합니다.

- 구성한 게스트 암호를 제공하는 모든 사용자에게 암호로 보호되는 액세스 권한을 부여하려면 게스트 액세스를 선택합니다. 이 방법을 사용하기 위해 File Gateway가 Microsoft Active Directory 도메인의 일부일 필요는 없습니다. 구성을 선택하여 게스트 암호를 지정한 다음 저장을 선택합니다.

19. 사용자 액세스의 경우 다음 중 하나를 수행하여 파일 공유에 액세스할 수 있는 SMB 클라이언트를 지정합니다.

    - Active Directory를 통해 성공적으로 인증한 모든 사용자에게 액세스 권한을 부여하려면 모든 AD 인증 사용자를 선택합니다.
    - 특정 사용자 또는 그룹에 대한 액세스를 허용하거나 거부하려면 특정 AD 인증 사용자 또는 그룹을 선택한 후 다음을 수행합니다.
        - 허용된 사용자 및 그룹의 경우 허용된 사용자 추가 또는 허용된 그룹 추가를 선택하고 파일 공유 액세스를 허용할 Active Directory 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 허용합니다.
        - 거부된 사용자 및 그룹의 경우 거부된 사용자 추가 또는 거부된 그룹 추가를 선택하고 파일 공유 액세스를 거부할 Active Directory 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 거부합니다.

> **Note**
>
> 사용자 및 그룹 파일 공유 액세스 섹션은 사용자 인증이 Active Directory로 설정된 경우에만 나타납니다.
> 사용자 또는 그룹을 지정할 때 도메인을 포함하지 마십시오. 도메인 이름에는 게이트웨이가 조인되는 특정 Active Directory의 게이트웨이 멤버십이 내재되어 있습니다.

20. (선택 사항) 관리 사용자에 Active Directory 사용자 및 그룹이 포함된 쉼표로 구분된 목록을 입력합니다. 관리 사용자는 파일 공유의 모든 파일 및 폴더에 대한 액세스 제어 목록(ACL)을 업데이트할 수 있는 권한을 받습니다. 그룹에는 @ 문자가 접두사로 붙어야 합니다(예: `@group1`).
21. 액세스 유형에서 다음 중 하나를 선택합니다.
    - 클라이언트가 파일 공유에서 파일을 읽고 쓸 수 있도록 허용하려면 읽기/쓰기를 선택합니다.
    - 클라이언트가 파일을 읽지만 파일 공유에 쓰지 않도록 허용하려면 읽기 전용을 선택합니다.

    > **Note**
    >
    > Microsoft Windows 클라이언트에 탑재된 파일 공유의 경우, 읽기 전용을 선택하면 예상하지 못한 오류가 발생하여 폴더를 생성할 수 없다는 메시지가 표시될 수도 있습니다. 이 메시지는 무시해도 됩니다.

22. 파일 및 디렉터리 액세스 제어에서 다음 중 하나를 선택합니다.
    - SMB 파일 공유의 파일 및 폴더에 대한 세분화된 권한을 설정하려면 Windows 액세스 제어 목록을 선택합니다. 자세한 내용은 Microsoft Windows ACL를 사용하여 SMB 파일 공유에 대한 액세스 제어를 참조하세요.
    - POSIX 권한을 사용해 SMB 파일 공유를 통해 저장된 파일 및 디렉터리에 대한 액세스를 제어하려면 POSIX 권한을 선택합니다.
23. 액세스 기반 열거의 경우 다음 중 하나를 수행합니다.
    - 공유의 파일과 폴더를 읽기 액세스 권한이 있는 사용자에게만 표시하려면 사용자에게 권한이 없는 파일 및 디렉터리 숨기기를 선택합니다.
    - 디렉터리 열거 중에 공유의 파일과 폴더를 모든 사용자에게 표시하려면 확인란을 선택하지 마십시오.

> **Note**
>
> 액세스 기반 열거는 SMB 파일 공유의 액세스 제어 목록(ACL)을 기반으로 해당 공유의 파일 및 폴더 열거를 필터링하는 시스템입니다.

24. 파일 액세스 옵션에서 다음 중 하나를 선택합니다.

    - 기회 잠금을 사용하여 파일 공유의 파일 버퍼링 전략을 최적화하려면 기회 잠금을 선택합니다. 대부분의 경우 기회 잠금을 활성화하면 특히 Windows 컨텍스트 메뉴와 관련하여 성능이 향상됩니다.
    - SMB 클라이언트가 아닌 게이트웨이가 파일 이름 대/소문자 구분을 제어할 수 있도록 하려면 대/소문자 구분 강제 적용을 선택합니다.
    - 두 설정을 모두 비활성화하려면 둘 다 없음을 선택합니다.

> **Note**
>
> 파일 액세스 충돌을 방지하기 위해 이러한 설정은 상호 배타적이며 동시에 활성화할 수 없습니다.

25. (선택 사항) S3에서 자동 캐시 새로 고침의 경우 캐시 새로 고침 간격 설정을 선택한 다음 TTL(Time To Live)을 사용하여 파일 공유의 캐시를 새로 고치는 시간을 분 또는 일 단위로 설정합니다. TTL은 마지막 새로 고침 이후 경과한 시간입니다. TTL 간격이 경과한 후 디렉터리에 액세스하면 File Gateway가 Amazon S3 버킷에서 해당 디렉터리의 콘텐츠를 새로 고칩니다.

> **Note**
>
> 이 값을 30분 미만으로 설정하면 대량의 Amazon S3 객체가 자주 생성되거나 삭제되는 경우 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.

26. 파일 소유권 및 권한에서 S3 버킷을 소유한 계정이 파일 공유에 의해 버킷에 기록된 모든 객체를 완전히 제어하도록 하려면 읽기, 쓰기, 편집 및 삭제 권한을 포함하여 게이트웨이에서 생성된 파일의 전체 소유권 부여를 선택합니다. AWS S3

    마친 후에는 다음을 선택합니다.

27. 파일 공유 구성을 검토합니다. 변경하려는 섹션의 설정을 수정하려면 편집을 선택합니다. 마친 후에는 Create(생성)를 선택합니다.

SMB 파일 공유가 생성되면 파일 공유의 세부 정보 탭에 있는 AWS Storage Gateway 콘솔에서 해당 구성 설정을 볼 수 있습니다. 파일 공유를 탑재하는 지침은 클라이언트에 SMB 파일 공유 탑재를 참조하세요.

파일 공유 탑재 및 사용

이 섹션의 주제에서는 클라이언트에 파일 공유를 탑재하고, 파일 공유를 사용하고, File Gateway를 테스트하고, 테스트 목적으로 생성할 수 있는 게이트웨이, Amazon EC2 인스턴스 또는 온프레미스 VMs과 같이 더 이상 필요하지 않은 리소스를 정리하는 방법에 대한 지침을 제공합니다. 지원되는 NFS(Network File System) 및 SMB(Service Message Block) 클라인언트에 대한 자세한 내용은 File Gateway에 지원되는 NFS 및 SMB 클라이언트 섹션을 참조하세요.

> **Note**
>
> AWS Management Console 또한는 파일 공유를 탑재하는 데 사용할 수 있는 예제 명령을 제공합니다.

주제

- 클라이언트에 NFS 파일 공유 탑재 - 이제 클라이언트의 드라이브에 NFS 파일 공유를 탑재하고 Amazon S3 버킷에 이를 매핑하는 방법을 알아봅니다.
- 클라이언트에 SMB 파일 공유 탑재 - 이제 SMB 파일 공유를 탑재하고 클라이언트에 액세스할 수 있는 드라이브에 매핑하는 방법을 알아봅니다.
- 기존 객체가 있는 버킷에서 파일 공유 사용 - NFS 또는 SMB를 사용해 File Gateway 밖에서 객체가 생성된 Amazon S3 버킷에서 파일 공유를 내보내는 방법을 알아봅니다.
- S3 File Gateway 테스트 - 매핑된 드라이브에 파일과 폴더를 복사하고 Amazon S3 버킷에 자동으로 표시되는지 확인하여 게이트웨이를 테스트하는 방법을 알아봅니다.

클라이언트에 NFS 파일 공유 탑재

다음 절차에 따라 클라이언트의 드라이브에 NFS 파일 공유를 탑재하고 Amazon S3 버킷에 이를 매핑합니다.

파일 공유를 탑재하고 Amazon S3 버킷에 매핑하려면

1. Microsoft Windows 클라이언트를 사용하는 경우 SMB 파일 공유를 생성하고 Windows 클라이언트에 이미 설치된 SMB 클라이언트를 사용하여 액세스하는 것이 좋습니다. NFS를 사용하는 경우 Windows에서 NFS용 서비스를 켭니다.
2. 다음과 같이 NFS 파일 공유를 탑재합니다.

- Linux 클라이언트의 경우, 명령 프롬프트에서 다음 명령을 입력합니다.

  ```
  sudo mount -t nfs -o nolock,hard [GatewayVMIPAddress]:/[FileShareName]
  [ClientMountPath]
  ```

- Windows 클라이언트의 경우, 명령 프롬프트에서 cmd.exe 명령을 입력합니다.

  ```
  mount -o nolock -o mtype=hard [GatewayVMIPAddress]:/[FileShareName]
  [WindowsDriveLetter]
  ```

예를 들어 Windows 클라이언트에서 VM의 IP 주소가 123.123.1.2이고 파일 공유 이름이 `test-fileshare`라고 가정합니다. 또한 드라이브 T로 매핑하려 한다고 가정해 보겠습니다. 이 경우 명령은 다음과 같습니다.

```
mount -o nolock -o mtype=hard 123.123.1.2:/test-fileshare T:
```

> **Note**
>
> 파일 공유를 탑재할 때 다음 사항에 유의하십시오.
>
> - 기본적으로 Windows는 NFS 공유에 소프트 탑재를 사용합니다. 연결 문제가 있으면 소프트 탑재는 더 쉽게 시간 초과됩니다. 하드 탑재가 더 안전하고 데이터를 더 잘 보존하므로 중요한 워크로드에는 하드 탑재를 사용하는 것이 좋습니다. 하드 마운트를 사용하려면 명령에서 `-o mtype=hard` 스위치를 사용해야 합니다.
> - S3 File Gateway는 NFS 파일 잠금을 지원하지 않습니다. NFS 파일 공유를 탑재할 때는 항상 `-o nolock` 옵션을 사용하여 파일 잠금을 끕니다.
> - 폴더와 객체가 Amazon S3 버킷에 존재하고 이름이 서로 같은 경우가 있을 수 있습니다. 이 경우 객체 이름에 후행 슬래시가 포함되지 않으면 File Gateway에서는 폴더만 볼 수 있습니다. 예를 들어 버킷에 `test` 또는 `test/`라는 객체와 `test/test1`이라는 폴더가 포함되어 있는 경우, File Gateway에서는 `test/` 및 `test/test1`만 보입니다.
> - 클라이언트를 재부팅한 후 파일 공유를 다시 탑재해야 할 수 있습니다.
> - Windows 클라이언트를 사용하는 경우 옵션 없이 `mount` 명령을 실행하여 탑재 후 `mount` 옵션을 검사합니다. 응답에서 제공한 최신 옵션을 사용하여 파일 공유가 탑재되었는지 확인해야 합니다. 또한 캐시된 이전 항목을 사용하지 않고 있음을 확인해야 합니다. 이는 지우기까지 최소 60초가 소요됩니다.

다음 단계

S3 File Gateway 테스트

클라이언트에 SMB 파일 공유 탑재

다음 절차에 따라 SMB 파일 공유를 탑재하고 클라이언트에 액세스할 수 있는 드라이브에 매핑합니다. 콘솔의 File Gateway 섹션에는 SMB 클라이언트에서 지원되는 탑재 명령이 표시됩니다. 이어서 몇 가지 사용해볼 만한 추가 옵션들도 있습니다.

다음을 포함해 몇 가지 방법을 사용하여 SMB 파일 공유를 탑재할 수 있습니다.

- 명령 프롬프트(`cmdkey` 및 `net use`) - 명령 프롬프트를 사용하여 파일 공유를 탑재합니다. `cmdkey`를 사용하여 자격 증명을 저장한 다음 `net use`를 사용하여 드라이브를 탑재하고 시스템 재부팅 간에 연결을 유지하려면 `/persistent:yes` 및 `/savecred` 스위치를 포함합니다. 사용하는 특정 명령은 Microsoft Active Directory(AD) 액세스 또는 게스트 사용자 액세스를 위해 드라이브를 탑재할지 여부에 따라 달라집니다. 예제는 아래에 있습니다.
- 파일 탐색기(맵 네트워크 드라이브) - Windows 파일 탐색기를 사용하여 파일 공유를 탑재합니다. 시스템 재부팅 간에 연결을 유지할지 여부를 지정하고 네트워크 자격 증명을 묻는 메시지를 표시하도록 설정을 구성합니다.
- PowerShell 스크립트 - 사용자 지정 PowerShell 스크립트를 생성하여 파일 공유를 탑재합니다. 스크립트에서 지정하는 파라미터에 따라 시스템 재부팅 전반에 걸쳐 연결이 지속될 수 있으며, 탑재된 동안 운영 체제에 공유가 표시되거나 표시되지 않을 수 있습니다.

> **Note**
>
> Microsoft AD 사용자는 로컬 시스템에 파일 공유를 탑재하기 전에 SMB 파일 공유에 대한 액세스 권한을 가지고 있는지 관리자에게 확인합니다.
> 게스트 사용자라면 파일 공유 탑재를 시도하기 앞서 게스트 사용자 암호를 가지고 있는지 확인합니다.

명령 프롬프트를 사용해 Microsoft AD 사용자를 위한 SMB 파일 공유를 탑재하려면:

1. 파일 공유를 사용자의 시스템에 탑재하기 전에 Microsoft AD 사용자에게 SMB 파일 공유에 필요한 권한이 있는지 확인합니다.
2. 명령 프롬프트에 다음을 입력하여 파일 공유를 탑재합니다.

```
net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
persistent:yes
```

명령 프롬프트를 사용하여 특정 로그인 자격 증명 조합으로 SMB 파일 공유를 탑재하려면:

1. 시스템에 파일 공유를 탑재하기 전에 사용자가 SMB 파일 공유에 대한 액세스 권한을 가지고 있는지 확인합니다.
2. 명령 프롬프트에 다음을 입력하여 Windows Credential Manager에 사용자 자격 증명을 저장합니다.

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\UserName /pass:Password
   ```
3. 명령 프롬프트에 다음을 입력하여 파일 공유를 탑재합니다.

   ```
   net use WindowsDriveLetter: \\GatewayIPAddress\FileShareName /
   persistent:yes /savecred
   ```

명령 프롬프트를 사용해 게스트 사용자를 위한 SMB 파일 공유를 탑재하려면:

1. 파일 공유를 탑재하기 앞서 게스트 사용자 암호를 가지고 있는지 확인합니다.
2. 명령 프롬프트에 다음을 입력하여 Windows Credential Manager에 게스트 자격 증명을 저장합니다.

   ```
   cmdkey /add:GatewayIPAddress /user:DomainName\smbguest /pass:Password
   ```
3. 명령 프롬프트에서 다음을 입력합니다.

   ```
   net use WindowsDriveLetter: \\$GatewayIPAddress\$Path /user:$Gateway
   ID\smbguest /persistent:yes /savecred
   ```

> **Note**
>
> 파일 공유를 탑재할 때 다음 사항에 유의하십시오.
>
> - 폴더와 객체가 Amazon S3 버킷에 존재하고 이름이 서로 같은 경우가 있을 수 있습니다. 이 경우 객체 이름에 후행 슬래시가 포함되지 않으면 File Gateway에서는 폴더만 볼 수 있습니다. 예를 들어 버킷에 `test` 또는 `test/`라는 객체와 `test/test1`이라는 폴더가 포함되어 있는 경우, File Gateway에서는 `test/` 및 `test/test1`만 보입니다.

- 사용자 자격 증명을 저장하고 시스템 재시작 후에도 유지되도록 파일 공유 연결을 구성하지 않는 한 클라이언트 시스템을 다시 시작할 때마다 파일 공유를 다시 마운트해야 할 수 있습니다.

Windows File Explorer를 사용하여 SMB 파일 공유를 탑재하려면

1. Windows 키를 누르고 Windows 검색 상자에 **`File Explorer`**를 입력하거나 **`Win+E`**를 누릅니다.
2. 탐색 창에서 내 PC를 선택합니다. 그런 다음 컴퓨터 탭에서 네트워크 드라이브 매핑을 선택합니다.
3. 네트워크 드라이브 매핑 대화 상자에서 드라이브의 드라이브 문자를 선택합니다.
4. 폴더에서 **`\\[File Gateway IP]\[SMB File Share Name]`**을 입력하거나 찾아보기를 선택하고 대화 상자에서 SMB 파일 공유를 선택합니다.
5. (선택 사항) 재부팅 이후에 탑재 지점이 지속되기를 원하는 경우에는 가입 시 재연결을 선택합니다.
6. (선택 사항) 사용자가 Microsoft AD 로그인 또는 게스트 계정 사용자 암호를 입력하도록 하고 싶은 경우에는 다른 자격 증명을 사용해 연결(Connect using different credentials)를 선택합니다.
7. 완료(Finish)를 선택하여 탑재 지점을 완료합니다.

> **Note**
>
> 점(`.`) 문자로 시작하는 모든 파일 또는 디렉터리는 Windows에서 숨김으로 표시됩니다. 이러한 파일 및 디렉터리를 표시하려면 Windows File Explorer의 보기 탭에서 숨겨진 항목 확인란을 선택해야 합니다.

Storage Gateway Management Console에서 파일 공유 설정을 편집하고 허용/거부되는 사용자 및 그룹을 편집하며 게스트 액세스 암호를 변경할 수 있습니다. 또한 파일 공유의 캐시에 저장된 데이터를 새로 고치고 이 콘솔에서 파일 공유를 삭제할 수도 있습니다.

SMB 파일 공유의 속성을 수정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 파일 공유를 선택합니다.
3. 파일 공유 페이지에서 수정하려는 SMB 파일 공유 옆의 확인란을 선택합니다.

4. 작업에서 원하는 작업을 선택합니다.

   - 파일 공유 설정 편집을 선택해 공유 액세스를 수정합니다.
   - 허용/거부된 사용자 편집(Edit allowed/denied users)을 선택해 사용자 및 그룹을 추가 또는 삭제한 다음, 허용된 사용자(Allowed Users), 거부된 사용자(Denied Users), 허용된 그룹(Allowed Groups) 및 거부된 그룹(Denied Groups) 상자에 허용/거부된 사용자 및 그룹을 입력합니다. 새 액세스 권한을 생성하려면 항목 추가 버튼을, 액세스 권한을 제거하려면 (X)를 사용합니다.

   > **Note**
   >
   > 그룹에는 @ 문자 접두사가 붙어야 합니다. 허용 가능한 형식은 다음과 같습니다. `DOMAIN\User1`, `user1`, `@group1` 및 `@DOMAIN\group1`.

5. 작업을 마쳤으면 저장을 선택합니다.

   허용된 사용자 및 그룹을 입력할 때 허용 목록을 생성합니다. 허용 목록을 생성하지 않으면 인증된 모든 Microsoft AD 사용자가 SMB 파일 공유에 액세스할 수 있습니다. 거부로 표시된 모든 사용자 및 그룹은 거부 목록에 추가되어 SMB 파일 공유에 액세스할 수 없게 됩니다. 사용자나 그룹이 거부 목록과 허용 목록에 모두 올라와 있는 경우에는 거부 목록이 우선 적용됩니다.

   SMB 파일 공유에서 액세스 제어 목록(ACL)을 켤 수 있습니다. ACL을 켜는 방법은 Windows ACL을 사용하여 SMB 파일 공유 액세스 제한 섹션을 참조하세요.

다음 단계

S3 File Gateway 테스트

기존 객체가 있는 버킷에서 파일 공유 사용

NFS 또는 SMB를 사용해 File Gateway 밖에서 객체가 생성된 Amazon S3 버킷에서 파일 공유를 내보낼 수 있습니다. 게이트웨이 밖에서 생성된 버킷의 객체들은 파일 시스템 클라이언트가 액세스할 때 NFS 또는 SMB 파일 시스템에서 파일로 표시됩니다. 파일 공유에는 표준 POSIX(Portable Operating System Interface) 액세스 및 권한이 사용됩니다. 파일을 Amazon S3 버킷에 다시 작성할 때는 파일이 부여하는 속성과 액세스 권한을 갖게 됩니다.

객체는 언제든지 S3 버킷에 업로드할 수 있습니다. 파일 공유에서 이렇게 새로 추가된 객체를 파일로 표시하려면 S3 버킷 새로 고침을 수행해야 합니다. 자세한 내용은 the section called “Amazon S3 버킷 객체 새로 고침” 단원을 참조하십시오.

> **Note**
>
> Amazon S3 버킷 1개에 작성자가 복수인 것은 바람직하지 않습니다. 그렇다면 "Amazon S3 버킷에 여러 라이터를 둘 수 있나요?" 섹션을 꼭 읽어보세요. Storage Gateway FAQ의 "Amazon S3 버킷에 작성자가 여러 개 있을 수 있나요?" 섹션을 읽어야 합니다.

NFS를 통해 액세스한 객체에 메타데이터 기본값을 할당하려면 Amazon S3 File Gateway 관리 섹션에서 메타데이터 기본값 편집을 참조하세요.

SMB에서는 객체가 이미 채워진 Amazon S3 버킷에서 Microsoft AD 또는 게스트 액세스 권한을 사용해 공유를 내보낼 수 있습니다. SMB 파일 공유를 통해 내보낸 객체는 바로 위에 있는 상위 디렉터리에서 POSIX 소유권과 권한을 상속합니다. 객체가 루트 폴더 아래 있을 경우에는 루트 액세스 제어 목록(ACL)이 상속됩니다. 루트 ACL의 경우 소유자는 `smbguest`이고, 파일 권한은 `666`이고, 디렉터리는 `777`입니다. 이는 인증된 액세스(Microsoft AD 및 게스트) 모두에게 적용됩니다.

S3 File Gateway 테스트

다음 절차에 따라 매핑된 드라이브에 파일과 폴더를 복사하고 Amazon S3 버킷에 자동으로 나타나는지 확인하여 게이트웨이를 테스트합니다.

Windows 클라이언트에서 Amazon S3로 파일을 업로드하려면

1. Windows 클라이언트에서 파일 공유를 탑재한 드라이브로 이동합니다. 드라이브 이름 앞에 S3 버킷 이름이 옵니다.
2. 파일 또는 폴더 하나를 드라이브에 복사합니다.
3. Amazon S3 Management Console에서 매핑된 버킷으로 이동합니다. 지정한 Amazon S3 버킷에 복사한 파일과 폴더가 보여야 합니다.

   AWS Storage Gateway 관리 콘솔의 파일 공유 탭에서 생성한 파일 공유를 볼 수 있습니다.

NFS 또는 SMB 클라이언트는 파일에 대해 쓰기, 읽기, 삭제, 이름 바꾸기 및 자르기 작업을 할 수 있습니다.

> **Note**
>
> File Gateway는 파일 공유에 대한 하드 또는 심볼 링크를 지원하지 않습니다.

S3에서 File Gateway가 작동하는 방식에 대한 다음 사항에 유의하십시오.

- 읽은 데이터는 연속 읽기 캐시에서 제공됩니다. 다시 말해서 데이터를 사용할 수 없으면 S3에서 가져와서 캐시에 추가합니다.
- 작성한 데이터는 다시 쓰기 캐시를 사용하여 최적화된 멀티파트 업로드를 통해 S3로 전송됩니다.
- 읽은 데이터 및 작성한 데이터는 요청을 받거나 변경된 부분만 네트워크를 통해 전송되도록 최적화됩니다.
- 삭제는 S3에서 객체를 제거합니다.
- 디렉터리는 Amazon S3 콘솔과 동일한 구문을 사용하여 S3의 폴더 객체로 관리됩니다. 빈 디렉터리의 이름을 바꿀 수 있습니다.
- 재귀적 파일 시스템 작업 성능(예: `ls -l`)은 버킷에 있는 객체의 수에 따라 달라집니다.

Amazon S3 File Gateway 관리

이 섹션의 주제에서는 Amazon S3 File Gateway 리소스를 관리하는 방법에 대한 정보를 제공합니다. 게이트웨이 관리에는 게이트웨이에 파일 공유 및 Amazon S3 버킷에 액세스할 수 있는 권한 부여, 게이트웨이 및 파일 공유에 대한 정보 및 설정 편집, 파일 공유 삭제, 캐시된 객체 새로 고침, 게이트웨이 및 파일 공유에 대한 운영 상태 표시기 이해가 포함됩니다.

주제

- 기본 게이트웨이 정보 편집 - Storage Gateway 콘솔을 사용하여 게이트웨이 이름, 시간대, CloudWatch 로그 그룹 등 기존 게이트웨이의 기본 정보를 편집하는 방법에 대해 알아봅니다.
- 액세스 및 권한 부여 - IAM 역할을 사용하여 게이트웨이에 Amazon S3 버킷 및 Amazon VPC 엔드포인트에 대한 액세스 권한을 제공하고, 특정 보안 문제를 방지하고, AWS 계정 간 버킷에 파일 공유를 연결하는 방법을 알아봅니다.
- 파일 공유 삭제 - Storage Gateway 콘솔을 사용하여 파일 공유를 삭제하는 방법에 대해 알아봅니다.
- 게이트웨이 SMB 설정 편집 - 게이트웨이의 SMB 파일 공유에 대한 보안 전략, Active Directory 인증, 게스트 액세스, 로컬 그룹 권한 및 파일 공유 가시성을 제어하는 게이트웨이 수준 SMB 설정을 편집하는 방법을 알아봅니다.
- SMB 파일 공유 설정 편집 - 설정을 편집하여 SMB 파일 공유의 이름, 로깅, 캐시 새로 고침, 스토리지 클래스, 파일 내보내기 등을 구성하는 방법을 알아봅니다.
- SMB 파일 공유 액세스 제한 - 허용되거나 거부된 사용자 또는 그룹을 추가하여 SMB 파일 공유에 대한 액세스를 제한하는 방법을 알아봅니다.
- NFS 파일 공유 설정 편집 - 설정을 편집하여 NFS 파일 공유의 이름, 로깅, 캐시 새로 고침, 스토리지 클래스, 파일 내보내기 등을 구성하는 방법을 알아봅니다.
- NFS 파일 공유 메타데이터 기본값 편집 - NFS 파일 공유의 파일 및 폴더에 대한 Unix 권한을 포함하는 기본 메타데이터 값을 편집하는 방법을 알아봅니다.
- NFS 파일 공유 액세스 제한 - NFS 파일 공유의 특정 IP 주소 또는 IP 범위에서 클라이언트에 대한 액세스를 제한하는 방법을 알아봅니다.
- Amazon S3 버킷 객체 새로 고침 - 파일 공유의 S3 버킷 객체 캐시를 새로 고치고 캐시를 자동으로 새로 고치도록 일정을 구성하는 방법을 알아봅니다.
- S3 Object Lock 사용 - Amazon S3 File Gateway가 S3 Object Lock 기능과 작동하는 방식에 대해 알아봅니다.
- 파일 공유 상태 - 파일 공유 상태를 보고 해석하는 방법을 알아봅니다.
- 게이트웨이 상태 - 게이트웨이 상태를 보고 해석하는 방법을 알아봅니다.

- Amazon S3 File Gateway의 대역폭 관리 - 게이트웨이에서 사용하는 네트워크 대역폭의 양을 제어하기 AWS 위해 게이트웨이의 업로드 처리량을 로 제한하는 방법을 알아봅니다.

S3 File Gateway의 기본 정보 편집

Storage Gateway 콘솔을 사용하여 게이트웨이 이름, 시간대, CloudWatch 로그 그룹 등 기존 게이트웨이의 기본 정보를 편집할 수 있습니다.

기존 게이트웨이의 기본 정보를 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 기본 정보를 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 게이트웨이 정보 편집을 선택합니다.
4. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 이 이름으로 검색하면 Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 찾을 수 있습니다.

   > **Note**
   >
   > 게이트웨이 이름은 2~255자여야 하며 슬래시(\ 또는 /)를 포함할 수 없습니다. 게이트웨이 이름을 변경하면 게이트웨이 모니터링을 위해 설정된 모든 CloudWatch 경보의 연결이 끊어집니다. 경보를 다시 연결하려면 CloudWatch 콘솔에서 각 경보의 GatewayName을 업데이트합니다.

5. 게이트웨이 표준 시간대에서 게이트웨이를 배포하려는 전 세계 지역의 현지 시간대를 선택합니다.
6. 로그 그룹 설정 방법 선택에서 게이트웨이의 상태를 모니터링하기 위해 Amazon CloudWatch Logs를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
   - 새 로그 그룹 생성 - 게이트웨이를 모니터링할 새 로그 그룹을 설정합니다.
   - 기존 로그 그룹 사용 - 해당 드롭다운 목록에서 기존 로그 그룹을 선택합니다.
   - 로깅 비활성화 - 게이트웨이를 모니터링하는 데 Amazon CloudWatch Logs를 사용하지 않습니다.
7. 변경하려는 설정 수정을 마쳤으면 변경 사항 저장을 선택합니다.

파일 공유 및 버킷에 대한 액세스 및 권한 부여

S3 File Gateway가 활성화되고 실행된 후 추가 파일 공유를 추가하고 게이트웨이 및 파일 공유 AWS 계정 와 다른의 버킷을 포함하여 Amazon S3 버킷에 대한 액세스 권한을 부여할 수 있습니다. 다음 섹션에서는 IAM 역할을 사용하여 게이트웨이에 Amazon S3 버킷 및 VPC 엔드포인트에 대한 액세스 권한을 제공하고, 특정 보안 문제를 방지하고, AWS 계정의 버킷에 파일 공유를 연결하는 방법을 설명합니다.

파일 공유를 새로 생성하는 방법에 대한 자세한 내용은 파일 공유 생성 섹션을 참조하세요.

이 섹션에는 파일 공유 및 Amazon S3 버킷에 대한 액세스 및 권한을 부여하는 방법에 대한 추가 정보를 제공하는 다음 주제가 포함되어 있습니다.

주제

- Amazon S3 버킷에 액세스할 수 있는 권한 부여 - File Gateway에 Amazon S3 버킷에 파일을 업로드하고 버킷에 연결하는 데 사용하는 모든 액세스 포인트 또는 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트에서 작업을 수행할 수 있는 액세스 권한을 부여하는 방법을 알아봅니다.
- 교차 서비스 혼동된 대리인 방지 - 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요하는 일반적인 보안 문제를 방지하는 방법을 알아보세요.
- 교차 계정 액세스에서 파일 공유 사용 - Amazon Web Services 계정 및 해당 계정의 사용자에게 다른 Amazon Web Services 계정에 속한 리소스에 액세스할 수 있는 액세스 권한을 부여하는 방법을 알아봅니다.

Amazon S3 버킷에 액세스할 수 있는 권한 부여

파일 공유를 생성할 때 File Gateway는 Amazon S3 버킷에 파일을 업로드하고 버킷에 연결하는 데 사용하는 액세스 포인트 또는 가상 프라이빗 클라우드(VPC) 엔드포인트에서 작업을 수행할 수 있는 액세스 권한이 필요합니다. 이 액세스 권한을 부여하기 위해 File Gateway는이 액세스 권한을 부여하는 IAM 정책과 연결된 AWS Identity and Access Management (IAM) 역할을 수임합니다.

이 역할에는 IAM 정책과 이 정책에 대한 보안 토큰 서비스 신뢰(STS) 관계가 필요합니다. 이 정책에 따라 역할이 실행할 수 있는 작업이 결정됩니다. 또한 S3 버킷 및 연결된 액세스 포인트 또는 VPC 엔드포인트에는 IAM 역할이 액세스할 수 있도록 허용하는 액세스 정책이 있어야 합니다.

역할 및 액세스 정책을 직접 생성하거나 File Gateway에서 대신 생성할 수 있습니다. File Gateway에서 이러한 정책을 대신 생성한 경우 해당 정책에는 S3 작업 목록이 포함됩니다. 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 역할을 만들어 AWS 서비스에 권한 위임을 참조하세요.

다음 예는 File Gateway가 IAM 역할을 수임하도록 허용하는 신뢰 정책입니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Important

Storage Gateway는 `iam:PassRole` 정책 작업을 사용하여 전달된 기존 서비스 역할을 수임할 수 있지만 `iam:PassedToService` 컨텍스트 키를 사용하여 작업을 특정 서비스로 제한하는 IAM 정책은 지원하지 않습니다.
자세한 내용은AWS Identity and Access Management 사용 설명서에서 다음 주제를 참조하세요.

- IAM: 특정 AWS 서비스에 IAM 역할 전달
- 사용자에게 AWS 서비스에 역할을 전달할 수 있는 권한 부여
- IAM에 사용 가능한 키

File Gateway에서 사용자 대신 정책을 생성하도록 하지 않으려는 경우 정책을 직접 생성하여 파일 공유에 연결합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 파일 공유 생성 섹션을 참조하세요.

다음 예제 정책은 File Gateway에서 정책에 나열된 모든 Amazon S3 작업을 수행하도록 허용합니다. 설명문의 첫 번째 부분은 S3 버킷 `amzn-s3-demo-bucket`에 대해 나열된 모든 작업을 수행하도록 허용합니다. 두 번째 부분은 `amzn-s3-demo-bucket`의 모든 객체에 대해 나열된 작업을 허용합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:GetAccelerateConfiguration",
                "s3:GetBucketLocation",
                "s3:GetBucketVersioning",
                "s3:ListBucket",
                "s3:ListBucketVersions",
                "s3:ListBucketMultipartUploads"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
            "Effect": "Allow"
        },
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/*",
            "Effect": "Allow"
        }
    ]
}
```

다음 예제 정책은 이전 정책과 유사하지만 File Gateway가 액세스 포인트를 통해 버킷에 액세스하는 데 필요한 작업을 수행하도록 허용합니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:GetObject",
                "s3:GetObjectAcl",
                "s3:GetObjectVersion",
                "s3:ListMultipartUploadParts",
                "s3:PutObject",
                "s3:PutObjectAcl"
            ],
            "Resource": "arn:aws:s3:us-east-1:111122223333:accesspoint/
TestAccessPointName/*",
            "Effect": "Allow"
        }
    ]
}
```

> **Note**
>
> VPC 엔드포인트를 통해 파일 공유를 S3 버킷에 연결해야 하는 경우 AWS PrivateLink 사용 설명서의 Amazon S3에 대한 엔드포인트 정책을 참조하세요.

> **Note**
>
> 암호화된 버킷의 경우 파일 공유는 대상 S3 버킷 계정의 키를 사용해야 합니다.

> **Note**
>
> File Gateway가 암호화에 SSE-KMS 또는 DSSE-KMS를 사용하는 경우 파일 공유와 연결된 IAM 역할에 kms:Encrypt, kms:Decrypt, kms:ReEncrypt*, kms:GenerateDataKey 및

kms:DescribeKey 권한이 포함되어 있는지 확인합니다. 자세한 내용은 Storage Gateway에 대한 자격 증명 기반 정책(IAM 정책) 사용을 참조하세요.

교차 서비스 혼동된 대리인 방지

혼동된 대리자 문제는 작업을 수행할 권한이 없는 엔터티가 권한이 더 많은 엔터티에게 작업을 수행하도록 강요할 수 있는 보안 문제입니다. 에서 AWS교차 서비스 가장은 혼동된 대리자 문제를 초래할 수 있습니다. 교차 서비스 가장은 한 서비스(직접 호출하는 서비스)가 다른 서비스(직접 호출되는 서비스)를 직접 호출할 때 발생할 수 있습니다. 직접 호출하는 서비스는 다른 고객의 리소스에 대해 액세스 권한이 없는 방식으로 작동하게 권한을 사용하도록 조작될 수 있습니다. 이를 방지하기 위해 AWS 에서는 계정의 리소스에 대한 액세스 권한이 부여된 서비스 위탁자를 사용하여 모든 서비스에 대한 데이터를 보호하는 데 도움이 되는 도구를 제공합니다.

리소스 정책에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 리소스에 다른 서비스를 AWS Storage Gateway 제공하는 권한을 제한하는 것이 좋습니다. 두 전역 조건 컨텍스트 키를 모두 사용하는 경우 `aws:SourceAccount` 값과 `aws:SourceArn` 값의 계정은 동일한 정책 문에서 사용할 경우 동일한 계정 ID를 사용해야 합니다.

`aws:SourceArn`의 값은 파일 공유가 연결된 Storage Gateway의 ARN이어야 합니다.

혼동된 대리인 문제로부터 보호하는 가장 효과적인 방법은 리소스의 전체 ARN이 포함된 `aws:SourceArn`글로벌 조건 컨텍스트 키를 사용하는 것입니다. 리소스의 전체 ARN을 모를 경우 또는 여러 리소스를 지정하는 경우, ARN의 알 수 없는 부분에 대해 와일드카드(*)를 포함한 `aws:SourceArn`전역 조건 컨텍스트 키를 사용합니다. 예제: `arn:aws:servicename::123456789012:*`.

다음 예는 Storage Gateway에서 `aws:SourceArn` 및 `aws:SourceAccount` 전역 조건 컨텍스트 키를 사용하여 혼동된 대리자 문제를 방지하는 방법을 보여줍니다.

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
       "Sid": "ConfusedDeputyPreventionExamplePolicy",
       "Effect": "Allow",
       "Principal": {
         "Service": "storagegateway.amazonaws.com"
```

```
        },
        "Action": "sts:AssumeRole",
        "Condition": {
          "StringEquals": {
            "aws:SourceAccount": "444455556666"
          },
          "ArnLike": {
           "aws:SourceArn": "arn:aws:storagegateway:us-
east-1:444455556666:gateway/sgw-123456DA"
         }
       }
     }
   ]
}
```

교차 계정 액세스에서 파일 공유 사용

교차 계정 액세스란 Amazon Web Services 계정과 해당 계정의 사용자에게 다른 Amazon Web Services 계정에 속한 리소스에 대한 액세스 권한이 부여되는 경우를 말합니다. File Gateway에서 한 Amazon Web Services 계정의 파일 공유를 사용하여 다른 Amazon Web Services 계정에 속한 Amazon S3 버킷의 객체에 액세스할 수 있습니다.

한 Amazon Web Services 계정이 소유한 파일 공유를 사용하여 다른 Amazon Web Services 계정의 S3 버킷에 액세스하려면

1. S3 버킷 소유자가 액세스해야 하는 S3 버킷 및 해당 버킷의 객체에 대한 액세스 권한을 Amazon Web Services 계정에 부여해야 합니다. 이 액세스 권한을 부여하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 예제 2: 버킷 소유자가 교차 계정 버킷 권한 부여를 참조하세요. 필요한 권한 목록은 Amazon S3 버킷에 액세스할 수 있는 권한 부여 섹션을 참조하세요.
2. 파일 공유에서 S3 버킷에 액세스하기 위해 사용하는 IAM 역할에 `s3:GetObjectAcl` 및 `s3:PutObjectAcl` 등과 같은 작업에 대한 권한이 포함되어 있어야 합니다. 또한 IAM 역할에 계정이 해당 IAM 역할을 할 수 있도록 허용하는 신뢰 정책이 포함되어 있어야 합니다. 이러한 신뢰 정책의 예제는 Amazon S3 버킷에 액세스할 수 있는 권한 부여 섹션을 참조하세요.

   파일 공유가 S3 버킷에 액세스하기 위해 기존 역할을 사용하는 경우에는 반드시 `s3:GetObjectAc` 및 `s3:PutObjectAcl` 작업에 대한 권한이 포함되어 있어야 합니다. 또한 계정이 이 역할을 수임할 수 있도록 허용하는 신뢰 정책이 필요합니다. 이러한 신뢰 정책의 예제는 Amazon S3 버킷에 액세스할 수 있는 권한 부여 섹션을 참조하세요.

3. https://console.aws.amazon.com/storagegateway/home에서 파일 공유를 생성하거나 파일 공유 설정을 편집할 때 S3 버킷 소유자가 액세스할 수 있는 게이트웨이 파일을 선택합니다.

교차 계정 액세스를 위해 파일 공유를 생성 또는 업데이트하고 온프레미스에서 파일 공유를 탑재한 경우 설정을 테스트하는 것이 가장 좋습니다. 이를 위해 디렉터리 콘텐츠를 나열하거나 테스트 파일을 작성하고 파일이 S3 버킷에 객체로 표시되는지 확인할 수 있습니다.

> **Important**
>
> 파일 공유에서 사용하는 계정에 교차 계정 액세스 권한을 부여할 수 있도록 정책이 올바르게 설정되어 있는지 확인합니다. 올바르게 선택되어 있지 않는 경우 온프레미스 애플리케이션을 통한 파일 업데이트 내용이 작업 중인 Amazon S3 버킷에 전파되지 않습니다.

리소스

액세스 정책 및 액세스 제어 목록에 대한 자세한 내용은 다음 항목을 참조하세요.

Amazon Simple Storage Service 사용 설명서의 사용 가능한 액세스 정책 옵션 사용 지침

Amazon Simple Storage Service 사용 설명서의 액세스 제어 목록(ACL) 개요

파일 공유 삭제

파일 공유가 필요 없으면 Storage Gateway 콘솔에서 삭제할 수 있습니다. 파일 공유를 삭제하면 파일 공유가 매핑되는 Amazon S3 버킷에서 게이트웨이가 연결 해제됩니다. 그러나 S3 버킷과 그 콘텐츠는 삭제되지 않습니다.

게이트웨이가 S3 버킷으로 데이터를 업로드하는 도중 파일 공유를 삭제할 경우 삭제 프로세스는 모든 데이터가 업로드된 이후에 완료됩니다. 파일 공유는 데이터가 완전히 업로드될 때까지 DELETING 상태를 유지합니다.

데이터가 완전히 업로드될 때까지 기다리지 않으려는 경우 이 주제의 뒷부분에 나오는 파일 공유를 강제로 삭제하려면 절차를 참조하세요.

파일 공유를 삭제하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.

2. 파일 공유를 선택한 다음 삭제할 파일 공유를 하나 이상 선택합니다.
3. 작업에서 파일 공유 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.
4. 지정된 파일 공유를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

경우에 따라 파일 공유를 삭제하기 전에 네트워크 파일 시스템(NFS) 파일 공유에 있는 파일에 쓴 모든 데이터를 업로드할 때까지 기다리지 않을 수도 있습니다. 예를 들어, 아직 업로드되지 않은 데이터를 의도적으로 삭제하거나, 파일 공유를 지원하는 Amazon S3 버킷이 이미 삭제되어 지정된 데이터를 더 이상 업로드할 수 없는 경우가 있습니다.

이러한 경우 AWS Management Console 또는 `DeleteFileShare` API 작업을 사용하여 파일 공유를 강제로 삭제할 수 있습니다. 이 작업을 실행하면 데이터 업로드 프로세스가 중지됩니다. 파일 공유는 FORCE_DELETING 상태로 바뀝니다. Storage Gateway 콘솔에서 파일 공유를 강제로 삭제하려면 다음 절차를 참조하세요.

파일 공유를 강제로 삭제하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유 목록 페이지에서 위 절차에서 삭제 플래그를 지정한 파일 공유를 선택하여 세부 정보를 확인합니다. 몇 초 후 세부 정보 탭에 삭제 알림 메시지가 나타납니다.
3. 세부 정보 탭에 표시되는 메시지에서 강제로 삭제할 파일 공유의 ID를 확인하고 확인란을 선택한 후 지금 강제 삭제를 선택합니다.

> **Note**
>
> 강제 삭제 작업은 실행 취소할 수 없습니다.
> 파일 공유를 강제로 삭제하면 다중 파트 업로드에서 부분적으로 전송된 파일이 Amazon S3에 남아 스토리지 요금이 발생할 수 있습니다. 이러한 파일 부분을 자동으로 삭제하도록 Amazon S3 버킷 수명 주기 규칙을 구성하는 것이 좋습니다. 자세한 내용은 모범 사례: 멀티파트 업로드 관리를 참조하세요.

DeleteFileShare API 작업을 사용하여 파일 공유를 강제로 삭제할 수도 있습니다. API를 사용하여 파일 공유를 삭제하려면 `storagegateway:DeleteFileShare` IAM 정책 권한이 필요합니다.

게이트웨이에 대한 SMB 설정 편집

게이트웨이 수준 SMB 설정을 사용하면 게이트웨이의 SMB 파일 공유에 대한 보안 전략, Active Directory 인증, 게스트 액세스, 로컬 그룹 권한 및 파일 공유 가시성을 구성할 수 있습니다.

게이트웨이 수준 SMB 설정을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 SMB 설정을 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 편집할 설정을 선택합니다.

이 섹션에는 게이트웨이의 각 개별 SMB 설정 구성과 관련된 추가 정보와 절차를 제공하는 다음 주제가 포함되어 있습니다.

주제

- 게이트웨이 보안 수준 설정 - SMB(Server Message Block) 서명 및 암호화와 같은 연결 요구 사항을 지정하도록 보안 수준을 설정하는 방법과 SMB 버전 1 클라이언트로부터의 연결을 허용할지 여부를 알아봅니다.
- Active Directory 인증 구성 - SMB 파일 공유에 대한 사용자 인증 액세스를 위해 회사 Active Directory 또는 AWS 관리형 Microsoft AD를 구성하는 방법을 알아봅니다.
- 게스트 액세스 권한 제공 - 올바른 게스트 계정 사용자 이름과 암호를 제공하는 모든 사용자의 게스트 액세스를 허용하도록 게이트웨이를 구성하는 방법을 알아봅니다.
- 로컬 그룹 구성 - Active Directory 사용자에게 특수 파일 공유 권한을 부여하도록 로컬 그룹을 구성하는 방법을 알아봅니다.
- 파일 공유 표시 여부 설정 - 사용자에게 공유를 나열할 때 게이트웨이의 공유가 표시되는지 여부를 지정하는 방법을 알아봅니다.

게이트웨이의 보안 수준 설정

S3 File Gateway를 사용하여 게이트웨이의 보안 수준을 지정할 수 있습니다. 이러한 보안 수준을 지정하면 게이트웨이에서 SMB(Server Message Block) 서명 또는 SMB 암호화가 필요한지 여부와 SMB 버전 1을 활성화하고 싶은지 여부를 설정할 수 있습니다.

보안 수준을 구성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.

2. 게이트웨이를 선택한 다음 SMB 설정을 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 SMB 보안 설정을 선택합니다.
4. Security level(보안 수준)에서 다음 중 하나를 선택합니다.

> **Note**
>
> AWS API를 사용하여이 설정을 구성하는 방법에 대한 자세한 내용은 API 참조의 UpdateSMBSecurityStrategy를 AWS Storage Gateway 참조하세요.
> 보안 수준이 높아지면 게이트웨이 성능에 영향을 미칠 수 있습니다.

- AES256 암호화 적용 - 이 옵션을 선택하면 S3 File Gateway는 256비트 AES 암호화 알고리즘을 사용하는 SMBv3 클라이언트로부터의 연결만 허용합니다. 128비트 알고리즘은 허용되지 않습니다. 이 옵션은 민감한 데이터를 처리하는 환경에서 사용하는 것이 좋습니다. Microsoft Windows의 모든 현재 SMB 클라이언트에서 작동합니다.
- 암호화 적용 - 이 옵션을 선택하면 S3 File Gateway에서 암호화가 켜진 SMBv3 클라이언트의 연결만 허용합니다. 256비트 알고리즘과 128비트 알고리즘이 모두 허용됩니다. 이 옵션은 민감한 데이터를 처리하는 환경에서 사용하는 것이 좋습니다. Microsoft Windows의 모든 현재 SMB 클라이언트에서 작동합니다.
- 서명 적용 – 이 옵션을 선택하면 S3 File Gateway가 서명이 활성화된 SMBv2 또는 SMBv3 클라이언트에서의 연결만 허용합니다. 이 옵션은 Microsoft Windows의 모든 현재 SMB 클라이언트에서 작동합니다.
- 클라이언트 협상 – 이 옵션을 선택하면 클라이언트가 협상한 내용에 따라 요청이 설정됩니다. 환경의 서로 다른 클라이언트에서 호환성을 극대화하고 싶을 때 이 옵션을 사용할 것을 권장합니다.

> **Note**
>
> 2019년 6월 20일 전에 활성화된 게이트웨이의 경우, 기본 보안 수준이 Client negotiated(클라이언트 협상)입니다.
> 2019년 6월 20일자로 활성화된 게이트웨이의 경우, 기본 보안 수준이 Enforce encryption(암호화 적용)입니다.

5. 저장을 선택합니다.

Active Directory를 사용하여 사용자 인증

회사 Active Directory를 사용하거나 SMB 파일 공유 AWS Managed Microsoft AD 에 대한 사용자 인증 액세스를 위해 Microsoft AD 도메인 자격 증명으로 게이트웨이의 SMB 설정을 편집합니다. 이렇게 하면 게이트웨이가 Active Directory 도메인에 조인하고 도메인의 멤버들이 SMB 파일 공유에 액세스할 수 있습니다.

> **Note**
>
> 를 사용하여에서 호스팅 Active Directory 도메인 서비스를 생성할 Directory Service수 있습니다 AWS 클라우드.
> Amazon EC2 게이트웨이와 AWS Managed Microsoft AD 함께를 사용하려면와 동일한 VPC에서 Amazon EC2 인스턴스를 생성하고 AWS Managed Microsoft AD, Amazon EC2 인스턴스에 _workspaceMembers 보안 그룹을 추가하고,의 관리자 자격 증명을 사용하여 AD 도메인에 가입해야 합니다 AWS Managed Microsoft AD.
> 에 대한 자세한 내용은 AWS Directory Service 관리 안내서를 AWS Managed Microsoft AD참조하세요.
> Amazon EC2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 설명서를 참조하세요.

SMB 파일 공유에서 액세스 제어 목록(ACL)을 활성화할 수도 있습니다. ACL을 활성화하는 방법에 대한 자세한 내용은 Windows ACL을 사용하여 SMB 파일 공유 액세스 제한 섹션을 참조하세요.

Active Directory 인증을 활성화하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 SMB 설정을 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 Active Directory 설정을 선택합니다.
4. 도메인 이름에 게이트웨이가 조인할 Active Directory 도메인의 이름을 입력합니다.

> **Note**
>
> 게이트웨이가 도메인에 조인한 적이 없는 경우Active Directory 상태는 분리 완료로 표시됩니다.
> Active Directory 서비스 계정에는 필요한 권한이 있어야 합니다. 자세한 내용은 Active Directory 서비스 계정 권한 요구 사항을 참조하세요.

도메인에 조인하면 게이트웨이의 게이트웨이 ID를 계정 이름(예: SGW-1234ADE)으로 사용하여 기본 컴퓨터 컨테이너(OU 아님)에 Active Directory 컴퓨터 계정이 생성됩니다. 이 계정의 이름은 사용자 지정할 수 없습니다.
Active Directory 환경에서 도메인 조인 프로세스를 용이하게 하기 위해 계정을 사전 준비해야 하는 경우 이 계정을 미리 생성해야 합니다.
Active Directory 환경에 새 컴퓨터 객체에 대해 지정된 OU가 있는 경우 도메인을 조인할 때 해당 OU를 지정해야 합니다.
게이트웨이에서 Active Directory 디렉터리를 조인할 수 없는 경우에는 JoinDomain API 작업을 사용하여 디렉터리의 IP 주소로 조인해보십시오.

5. 도메인 사용자 및 도메인 암호에 게이트웨이가 도메인에 조인하는 데 사용할 Active Directory 서비스 계정의 자격 증명을 입력합니다.
6. (선택 사항) 조직 단위(OU)에 Active Directory가 새 컴퓨터 객체에 사용하는 지정된 OU를 입력합니다.
7. (선택 사항) 도메인 컨트롤러(DC)에 게이트웨이가 Active Directory에 연결할 하나 이상의 DC 이름을 입력합니다. 여러 DC를 쉼표로 구분된 목록으로 입력할 수 있습니다. DNS가 DC를 자동으로 선택할 수 있도록 이 필드를 비워 둘 수 있습니다.
8. 변경 사항 저장을 선택합니다.

특정 AD 사용자 및 그룹으로 파일 공유 액세스를 제한하려면

1. Storage Gateway 콘솔에서 액세스를 제한하려는 파일 공유를 선택합니다.
2. 작업 드롭다운 메뉴에서 파일 공유 액세스 설정 편집을 선택합니다.
3. 사용자 및 그룹 파일 공유 액세스 섹션에서 설정을 선택합니다.

   허용된 사용자 및 그룹에서 허용된 사용자 추가 또는 허용된 그룹 추가를 선택하고 파일 공유 액세스를 허용할 AD 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 허용합니다.

   거부된 사용자 및 그룹에서 거부된 사용자 추가 또는 거부된 그룹 추가를 선택하고 파일 공유 액세스를 거부할 AD 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 거부합니다.

   > **Note**
   >
   > 사용자 및 그룹 파일 공유 액세스 섹션은 Active Directory가 선택된 경우에만 나타납니다.

그룹에는 @ 문자 접두사가 붙어야 합니다. 허용 가능한 형식은 다음과 같습니다. `DOMAIN\User1`, `user1`, `@group1` 및 `@DOMAIN\group1`.
허용 및 거부된 사용자 및 그룹 목록을 구성하면 Windows ACL은 해당 목록을 재정의하는 액세스 권한을 부여하지 않습니다.
허용 및 거부된 사용자 및 그룹 목록은 ACL보다 먼저 평가되며 파일 공유를 탑재하거나 액세스할 수 있는 사용자를 제어합니다. 허용 목록에 사용자 또는 그룹이 있는 경우 해당 목록은 활성으로 간주되며 해당 사용자만 파일 공유를 탑재할 수 있습니다.
사용자가 파일 공유를 탑재한 후 ACL은 사용자가 액세스할 수 있는 특정 파일 또는 폴더를 제어하는 보다 세분화된 보호를 제공합니다. 자세한 내용은 새 SMB 파일 공유에서 Windows ACL 활성화를 참조하세요.

4. 항목 추가를 마치면 저장을 선택하십시오.

파일 공유에 대한 게스트 액세스 권한 제공

올바른 게스트 계정 사용자 이름과 암호를 제공할 수 있는 모든 사용자에게 게스트 액세스를 허용하도록 S3 File Gateway를 구성할 수 있습니다. 이 방법이 사용자가 File Gateway에 액세스할 수 있는 유일한 방법이 되도록 하려면 게이트웨이를 Microsoft Active Directory 도메인에 조인할 필요가 없습니다. 이 게스트 액세스 방법을 사용하여 Active Directory 도메인의 멤버인 S3 File Gateway에서 파일 공유를 생성할 수도 있습니다.

게스트 액세스 권한 인증 방법을 사용하도록 파일 공유를 구성하면 게스트 액세스 사용자 이름은 `smbguest`입니다. 게스트 액세스 권한을 사용하여 파일 공유를 생성하려면 먼저 `smbguest` 사용자에 대한 기본 암호를 변경해야 합니다.

다음 절차에 따라 게스트 사용자 `smbguest`의 암호를 변경할 수 있습니다.

게스트 액세스 암호를 변경하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 콘솔 페이지 왼쪽의 탐색 창에서 게이트웨이를 선택한 다음 게스트 액세스 권한을 제공할 게이트웨이의 이름을 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 게스트 액세스 설정을 선택합니다.
4. 게스트 암호에 설정하려는 게스트 액세스 암호를 입력한 다음 변경 사항 저장을 선택합니다.

게이트웨이의 로컬 그룹을 구성하려면

로컬 그룹 설정을 사용하면 게이트웨이의 SMB 파일 공유에 대한 특별한 권한을 Active Directory 사용자 또는 그룹에 부여할 수 있습니다.

로컬 그룹 설정을 사용하여 게이트웨이 관리자 권한을 할당할 수 있습니다. 게이트웨이 관리자는 공유 폴더 Microsoft Management Console 스냅인을 사용하여 열려 있고 잠긴 파일을 강제로 닫을 수 있습니다.

> **Note**
>
> 게이트웨이를 Active Directory 도메인에 조인하려면 먼저 하나 이상의 게이트웨이 관리자 사용자 또는 그룹을 추가해야 합니다.

게이트웨이 관리자를 할당하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 SMB 설정을 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 로컬 그룹 설정을 선택합니다.
4. 로컬 그룹 설정 섹션에서 설정을 선택합니다. 이 섹션은 Active Directory를 사용하는 파일 공유에만 표시됩니다.

   게이트웨이 관리자의 경우 로컬 게이트웨이 관리자 권한을 부여하려는 Active Directory 사용자 및 그룹을 추가합니다. 도메인 이름을 포함하여 줄 당 하나의 사용자 또는 그룹을 추가합니다. 예를 들어 **`corp\Domain Admins`**입니다. 줄을 더 생성하려면 새 게이트웨이 관리자 추가를 선택합니다.

   > **Note**
   >
   > 게이트웨이 관리자를 편집하면 모든 SMB 파일 공유의 연결이 해제되었다가 다시 연결됩니다.

5. 변경 사항 저장을 선택한 다음 계속을 선택하여 표시되는 경고 메시지를 확인합니다.

파일 공유 표시 여부 설정

파일 공유 표시 여부는 사용자에게 공유를 나열할 때 게이트웨이의 공유를 표시할지 여부를 제어합니다(예: 네트워크 보기 또는 찾아보기 목록). 게이트웨이의 파일 공유가 표시되면 클라이언트가 게이트웨이 IP 주소 또는 DNS 이름을 알고 있는 경우 파일 브라우저를 사용하여 공유를 쉽게 검색할 수 있습니다. 파일 공유가 표시되지 않으면 클라이언트는 게이트웨이 IP 또는 DNS 이름 외에도 파일 공유 이름을 알아야 공유를 검색할 수 있습니다.

> **Note**
>
> 이 설정은 배포의 파일 공유에 대한 액세스를 보호하는 효과적인 방법이 아닙니다. 보안을 위해 특정 사용자 및 그룹에 대한 액세스를 제한하도록 권한을 구성하는 것이 좋습니다. 지침은 SMB 파일 공유에 대한 사용자 및 그룹 액세스 제한을 참조하세요.

파일 공유 표시 여부를 설정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 SMB 설정을 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 SMB 설정 편집을 선택한 다음 파일 공유 표시 여부 설정을 선택합니다.
4. 게이트웨이가 사용자에게 공유를 나열할 때 이 게이트웨이의 공유를 표시하려면 표시 여부 상태 확인란을 선택합니다. 게이트웨이가 사용자에게 공유를 나열할 때 이 게이트웨이의 공유가 표시되지 않도록 하려면 이 확인란을 선택 취소한 상태로 둡니다.

SMB 파일 공유에 대한 설정 편집

기존 SMB 파일 공유에 대해 다음 설정을 편집할 수 있습니다.

- 파일 공유 이름 - 파일 공유의 이름을 선택합니다.
- 감사 로그 - 감사 로그를 켜거나 끕니다.
- 기존 로그 그룹 목록 - 감사 로그에 대한 기존 로그 그룹을 선택합니다.
- 비게이트웨이 파일 캐시 새로 고침 시간 - 파일 공유의 캐시를 새로 고칠 간격을 지정합니다.

> **Note**
>
> 이 값을 30분 미만으로 설정하면 대량의 Amazon S3 객체가 자주 생성되거나 삭제되는 경우 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.

- 이벤트 업로드 설정 시간 - 클라이언트가 `ObjectUploaded` 알림을 생성하기 전에 파일에 쓴 마지막 시점 이후 대기할 시간(초)을 지정합니다.
- 새 객체의 스토리지 클래스 - Amazon S3 버킷에 생성한 새 객체에 사용할 스토리지 클래스를 선택합니다.
- MIME 유형 추측 - Storage Gateway가 파일 확장자를 기반으로 하여 업로드되는 객체의 MIME 유형을 추측하도록 할지 선택합니다.
- S3 버킷 소유자가 액세스할 수 있는 게이트웨이 파일 - 게이트웨이의 파일을 파일 공유에 연결된 Amazon S3 버킷을 소유한 AWS 계정에 액세스할 수 있도록 할지 여부를 선택합니다.
- 요청자 지불 활성화 - 버킷 소유자가 아닌 파일 공유에서 데이터를 읽거나 요청하는 계정에 액세스 요금을 지불하도록 요구할지 여부를 선택합니다.
- 다음으로 내보내기 - 파일을 읽기-쓰기 또는 읽기 전용 상태로 내보낼지 여부를 선택합니다.
- 제어하는 파일 및 디렉터리 액세스 - Windows ACL 또는 POSIX 권한을 사용하여 파일 및 디렉터리 액세스를 제어할지 여부를 선택합니다.
- 기회 잠금(oplock) - 파일 공유가 기회 잠금을 사용하여 파일 버퍼링 전략을 최적화하도록 허용할지 여부를 선택합니다.
- 대/소문자 구분 강제 적용 - 클라이언트 또는 게이트웨이가 파일 및 디렉터리 이름에 대한 대/소문자 구분을 제어할지 여부를 선택합니다.

> **Note**
>
> 파일 공유에 현재 강제 대/소문자 구분이 활성화된 경우 비활성화하면 이름이 동일하지만 대/소문자가 다른 파일(예: file.txt, File.txt)에 액세스할 수 없게 될 수 있습니다. 대/소문자를 구분하지 않는 클라이언트는 버전 하나만 액세스할 수 있습니다.

- 파일 및 디렉터리에 대한 액세스 기반 열거 - 디렉터리 열거 중에 공유의 파일 및 폴더를 모든 사용자에게 표시할지 아니면 읽기 액세스 권한이 있는 사용자에게만 표시할지 선택합니다.

> **Note**
>
> 새 버킷 또는 액세스 포인트를 가리키도록 기존 파일 공유를 편집하거나 VPC 엔드포인트 설정을 수정할 수 없습니다. 새 파일 공유를 생성할 때만 이러한 설정을 구성할 수 있습니다.

파일 공유 설정을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 후 업데이트할 파일 공유를 선택하십시오.
3. 작업에서 파일 공유 설정 편집을 선택합니다.
4. 변경하려는 설정을 모두 변경합니다.
5. 저장을 선택합니다.

SMB 파일 공유에 대한 사용자 및 그룹 액세스 제한

파일 공유에 대한 액세스를 제한하려면 허용되거나 거부된 사용자 또는 그룹을 추가하는 것이 좋습니다. 그렇지 않으면 인증된 모든 사용자가 파일 공유를 사용할 수 있습니다.

SMB 액세스 설정을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 후 편집할 SMB 파일 공유를 선택합니다.
3. 작업에서 액세스 공유 설정 편집을 선택합니다.
4. 사용자 및 그룹 파일 공유 액세스 섹션에서 설정을 선택합니다.

   허용된 사용자 및 그룹에서 허용된 사용자 추가 또는 허용된 그룹 추가를 선택하고 파일 공유 액세스를 허용할 AD 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 허용합니다. 허용된 사용자 및 그룹 목록에 없는 모든 사용자는 액세스가 거부됩니다.

   거부된 사용자 및 그룹에서 거부된 사용자 추가 또는 거부된 그룹 추가를 선택하고 파일 공유 액세스를 거부할 AD 사용자 또는 그룹을 입력합니다. 이 프로세스를 반복하여 필요한 만큼 사용자 및 그룹을 거부합니다. 허용된 사용자 및 그룹 목록이 비어 있는 경우 거부된 사용자 및 그룹 목록에 있는 사용자를 제외한 모든 사용자에게 액세스 권한이 부여됩니다.

> **Note**
>
> AD 사용자 또는 그룹 이름만 입력합니다. 도메인 이름에는 게이트웨이가 조인되는 특정 AD의 게이트웨이 멤버십이 내재되어 있습니다.
> 허용된/거부된 사용자 또는 그룹을 지정하지 않으면 모든 인증된 AD 사용자가 파일 공유를 내보낼 수 있습니다.

기존 파일 공유의 서버 측 암호화 방법 변경

다음 절차에서는 Storage Gateway 콘솔을 사용하여 기존 NFS 또는 SMB 파일 공유의 서버 측 암호화 방법을 변경하는 방법을 설명합니다. Storage Gateway API를 사용하여 이 작업을 수행하려면 AWS Storage Gateway API 참조의 UpdateNFSFileShare 또는 UpdateSMBFileShare를 참조하세요.

> **Note**
>
> 암호화 방법을 업데이트하면 업데이트 후 Amazon S3 버킷에 저장된 기존 객체에 새 방법이 적용됩니다.
> 암호화에 SSE-KMS를 사용하도록 File Gateway를 구성하는 경우 파일 공유와 연결된 IAM 역할에 `kms:Encrypt`, `kms:Decrypt`, `kms:ReEncrypt*`, `kms:GenerateDataKey` 및 `kms:DescribeKey` 권한을 수동으로 추가해야 합니다. 자세한 내용은 Storage Gateway에 대한 자격 증명 기반 정책(IAM 정책) 사용을 참조하세요.

NFS 또는 SMB 파일 공유의 서버 측 암호화 방법을 변경하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 다음 암호화 방법을 변경할 파일 공유를 선택합니다.
3. 작업에서 파일 공유 암호화 편집을 선택합니다.
4. 암호화에서 Amazon S3의 저장 파일에 사용할 암호화 유형을 선택합니다.

   - Amazon S3(SSE-S3)로 관리되는 서버 측 암호화를 사용하려면 S3 관리형 키(SSE-S3)를 선택합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 Amazon S3 관리형 키로 서버 측 암호화 사용을 참조하세요.
   - AWS Key Management Service(SSE-KMS)로 관리되는 서버 측 암호화를 사용하려면 KMS 관리형 키(SSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS

키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

에 대한 자세한 내용은 AWS Key Management Service 개발자 안내서의 AWS Key Management Service란 무엇입니까?를 AWS KMS참조하세요.

- AWS Key Management Service(DSSE-KMS)로 관리되는 이중 계층 서버 측 암호화를 사용하려면 AWS Key Management Service 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)를 선택합니다. 기본 KMS 키에서 기존 AWS KMS 키를 선택하거나 새 KMS 키 생성을 선택하여 AWS Key Management Service(AWS KMS) 콘솔에서 새 KMS 키를 생성합니다.

  DSSE-KMS에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 AWS KMS 키를 사용한 이중 계층 서버 측 암호화 사용을 참조하세요.

  > **Note**
  >
  > DSSE-KMS 및 AWS KMS 키 사용에는 추가 요금이 부과됩니다. 자세한 내용은 AWS KMS 요금을 참조하십시오.
  > 목록에 없는 별칭이 있는 AWS KMS 키를 지정하거나 다른 AWS 계정의 AWS KMS 키를 사용하려면를 사용해야 합니다 AWS Command Line Interface. 비대칭 KMS 키는 지원되지 않습니다. 자세한 내용을 알아보려면 AWS Storage Gateway API 참조의 CreateSMBFileShare를 참조하세요.

5. 완료되었으면 변경 사항 저장을 선택합니다.

NFS 파일 공유에 대한 설정 편집

기존 NFS 파일 공유를 생성한 후 다음 절차에 따라 설정을 편집합니다.

> **Note**
>
> 새 버킷 또는 액세스 포인트를 가리키도록 기존 파일 공유를 편집하거나 VPC 엔드포인트 설정을 수정할 수 없습니다. 새 파일 공유를 생성할 때만 이러한 설정을 구성할 수 있습니다.

파일 공유 설정을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 후 업데이트할 파일 공유를 선택하십시오.

3. 작업에서 파일 공유 설정 편집을 선택합니다.
4. 파일 공유 이름에 파일 공유의 이름을 입력합니다.
5. 감사 로그에서 다음 중 하나를 선택합니다.

   - 이 파일 공유에 대한 새 로그 그룹을 생성하려면 새 로그 그룹 생성을 선택합니다.
   - 이 파일 공유에 대한 상태 및 리소스 알림을 기존 로그 그룹에 보내려면 기존 로그 그룹 사용을 선택한 다음 목록에서 원하는 그룹을 선택합니다.
   - 이 파일 공유에 대한 로깅을 끄려면 로깅 비활성화를 선택합니다.

   감사 로그에 대한 자세한 내용은 S3 File Gateway 감사 로그 이해를 참조하세요.
6. 비게이트웨이 파일 캐시 새로 고침 시간에서 새로 고침 간격 설정을 선택한 다음 TTL(Time To Live)을 사용하여 파일 공유의 캐시를 새로 고치는 시간을 분 또는 일 단위로 설정합니다. TTL은 마지막 새로 고침 이후 경과한 시간입니다. TTL 간격이 경과한 후 디렉터리에 액세스하면 File Gateway가 Amazon S3 버킷에서 해당 디렉터리의 콘텐츠를 새로 고칩니다.

   > **Note**
   >
   > 이 값을 30분 미만으로 설정하면 대량의 Amazon S3 객체가 자주 생성되거나 삭제되는 경우 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.
7. 이벤트 업로드 설정 시간에서 설정 시간 설정을 선택한 다음 설정 시간을 초 단위로 입력합니다. 설정 시간은 최근 클라이언트 쓰기 작업과 `ObjectUploaded` 로그 알림 생성 사이의 최소 지연을 제어합니다. 클라이언트는 짧은 시간 동안 파일에 소규모 쓰기 작업을 많이 수행할 수 있으므로 동일한 파일에 대해 여러 개의 알림이 빠르게 연속해서 생성되지 않도록 이 파라미터를 최대한 길게 설정하는 것이 좋습니다. 자세한 내용은 파일 업로드 알림 받기를 참조하세요.
8. 새 객체의 스토리지 클래스의 경우 드롭다운 목록에서 스토리지 클래스를 선택합니다. 스토리지 클래스에 대한 자세한 내용은 File Gateway와 함께 스토리지 클래스 사용을 참조하세요.
9. 객체 메타데이터에서 다음을 수행합니다.

   a. Storage Gateway가 파일 확장명을 기반으로 업로드된 객체의 미디어 유형을 추측하도록 허용하려면 MIME 유형 추측을 선택합니다.

   b. S3 버킷을 소유한 계정이 읽기, 쓰기, 편집 및 삭제 권한을 포함하여 게이트웨이에서 생성한 파일의 전체 소유권을 갖도록 하려면 S3 버킷 소유자가 액세스할 수 있는 게이트웨이 파일을 선택합니다. AWS S3

10. 버킷 소유자가 아닌 파일 요청자가 데이터 요청 비용을 지불하고 S3 버킷에서 다운로드하도록 하려면 요청자 지불 활성화를 선택합니다.
11.
12. 액세스 수준에서 다음 중 하나를 선택합니다.

    - Root squash (default)(Root Squash(기본값)) 원격 superuser(root)에 대한 액세스가 UID(65534) 및 GID(65534)로 매핑됩니다.
    - All squash(모든 Squash): 모든 사용자 액세스가 사용자 ID(UID)(65534) 및 그룹 ID(65534)로 매핑됩니다.
    - No root squash(Root Squash 없음) 원격 superuser(root)는 root로서 액세스를 받습니다.
13. 다른 이름으로 내보내기에서 다음 중 하나를 선택합니다.

    - 클라이언트가 파일 공유에서 파일을 읽고 쓸 수 있도록 허용하려면 읽기/쓰기를 선택합니다.
    - 클라이언트가 파일을 읽지만 파일 공유에 쓰지 않도록 허용하려면 읽기 전용을 선택합니다.

    > **Note**
    >
    > Microsoft Windows 클라이언트에 탑재된 파일 공유의 경우, 읽기 전용을 선택하면 예상하지 못한 오류가 발생하여 폴더를 생성할 수 없다는 메시지가 표시될 수도 있습니다. 이 메시지는 무시해도 됩니다.

14. 설정 편집을 완료한 후 변경사항 저장을 선택합니다.

NFS 파일 공유에서 메타데이터 기본값 편집

버킷의 파일 또는 디렉터리에 대한 메타데이터 값을 설정하지 않으면 S3 File Gateway가 기본 메타데이터 값을 설정합니다. 이러한 값에는 파일 및 폴더에 대한 Unix 권한이 포함됩니다. Storage Gateway 콘솔에서 메타데이터 기본값을 편집할 수 있습니다.

S3 File Gateway가 Amazon S3에 파일 및 폴더를 저장하면 Unix 파일 권한은 객체 메타데이터에 저장됩니다. S3 File Gateway가 S3 File Gateway에서 저장하지 않은 객체를 발견하면 이러한 객체에는 기본 Unix 파일 권한이 할당됩니다. 다음 표에서 기본 Unix 권한을 확인할 수 있습니다.

Metadata	설명
디렉터리 권한	"nnnn" 형식의 Unix 디렉터리 모드. 예를 들어 "0666"은 파일 공유 내 모든 디렉터리의 액세스 모드를 나타냅니다. 기본값은 0777입니다.
파일 권한	"nnnn" 형식의 Unix 파일 모드. 예를 들어 "0666"은 파일 공유 내 파일 모드를 나타냅니다. 기본값은 0666입니다.
사용자 ID	파일 공유 내 파일에 대한 기본 소유자 ID. 기본값은 65534입니다.
그룹 ID입니다.	파일 공유의 기본 그룹 ID. 기본값은 65534입니다.

메타데이터 기본값을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 후 업데이트할 파일 공유를 선택하십시오.
3. 작업에서 파일 메타데이터 기본값 편집을 선택하십시오.
4. 파일 메타데이터 기본값 편집 대화 상자에서 메타데이터 정보를 입력하고 저장을 선택하십시오.

NFS 파일 공유에 대한 클라이언트 액세스 제한

NFS 파일 공유에 연결할 수 있는 NFS 클라이언트의 특정 클라이언트 IP 주소 또는 CIDR 블록 범위 목록을 정의하려면 NFS 클라이언트 액세스 설정을 편집하는 것이 좋습니다. 액세스를 제한하지 않으면 네트워크의 모든 클라이언트가 파일 공유에 마운트할 수 있습니다.

NFS 파일 공유에 대한 클라이언트 액세스를 제한하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 콘솔 페이지 왼쪽의 탐색 창에서 파일 공유를 선택한 다음 편집하려는 NFS 파일 공유의 파일 공유 ID를 선택합니다.
3. 작업 드롭다운 메뉴에서 파일 공유 액세스 설정 편집을 선택합니다.

객체 액세스 섹션에는 현재 NFS 파일 공유에 연결할 수 있는 IP 주소 및 CIDR 블록 목록이 표시됩니다. 현재 액세스가 제한되지 않은 경우 0.0.0.0/0 CIDR 블록의 허용된 클라이언트 아래에 가능한 모든 IPv4 주소의 연결이 허용됨을 나타내는 항목이 표시됩니다.

4. 허용된 클라이언트의 0.0.0.0/0 CIDR 블록 오른쪽에 있는 제거를 선택합니다.
5. 클라이언트 추가를 선택한 다음 허용하려는 클라이언트의 CIDR 표기법으로 IP 주소 또는 주소 범위를 제공합니다.
6. 필요에 따라 IP 주소 또는 범위를 더 추가하려면 이전 단계를 반복합니다. 실수하거나 액세스를 취소해야 하는 경우 목록에서 삭제하려는 IP 주소 또는 범위의 오른쪽에 있는 제거를 선택할 수 있습니다.
7. 완료되었으면 변경 사항 저장을 선택합니다.

Amazon S3 버킷 객체 새로 고침

NFS/SMB 클라이언트가 파일 시스템 작업을 수행할 때 게이트웨이가 파일 공유와 연결된 Amazon S3 객체 캐시 내 객체의 인벤토리를 유지합니다. 게이트웨이가 이 캐시된 인벤토리를 사용하여 Amazon S3 요청의 지연 시간 및 빈도를 줄입니다. 이 작업은 S3 File Gateway 캐시 스토리지로 파일을 가져오지 않습니다. Amazon S3 객체 캐시의 객체 인벤토리 변경 사항을 반영하도록 캐시된 인벤토리만 업데이트합니다.

파일 공유의 S3 버킷 객체 캐시를 새로 고치려면 다음 목록에서 사용 사례에 가장 적합한 방법을 선택한 다음 아래 해당 절차를 완료합니다.

> **Note**
>
> 사용하는 방법에 관계없이 디렉터리를 처음 나열하면 초기화되어 게이트웨이가 Amazon S3에서 디렉터리의 메타 데이터 콘텐츠를 나열합니다. 디렉터리를 초기화하는 데 필요한 시간은 해당 디렉터리의 항목 수에 비례합니다.

주제

- Storage Gateway 콘솔을 사용하여 자동 캐시 새로 고침 일정 구성
- Amazon CloudWatch 규칙과 AWS Lambda 함께를 사용하여 자동 캐시 새로 고침 일정 구성
- Storage Gateway 콘솔을 사용하여 수동 캐시 새로 고침 수행
- Storage Gateway API를 사용하여 수동 캐시 새로 고침 수행

Storage Gateway 콘솔을 사용하여 자동 캐시 새로 고침 일정 구성

다음 절차에서는 지정한 TTL(Time To Live) 값을 기반으로 자동 캐시 새로 고침 일정을 구성합니다. TTL 기반 캐시 새로 고침 일정을 구성하기 전에 다음 사항을 고려하세요.

- TTL은 지정된 디렉터리의 마지막 캐시 새로 고침 이후 시간으로 측정됩니다.
- TTL 기반 캐시 새로 고침은 지정된 TTL 기간이 만료된 후 지정된 디렉터리에 액세스하는 경우에만 발생합니다.
- 새로 고침은 비반복적입니다. 액세스 중인 특정 디렉터리에서만 발생합니다.
- 새로 고침은 TTL 만료 이후 동기화되지 않은 디렉터리에 대해서만 Amazon S3 API 비용이 발생합니다.
  - 디렉터리는 NFS 또는 SMB 활동으로 액세스하는 경우에만 동기화됩니다.
  - 동기화는 지정한 TTL 기간보다 더 자주 발생하지 않습니다.
- TTL 기반 캐시 새로 고침 구성은 게이트웨이와 Amazon S3 버킷 간의 워크플로 외부에서 Amazon S3 버킷의 콘텐츠를 직접 자주 업데이트하는 경우에만 권장됩니다.
- 게이트웨이가 디렉터리의 내용을 새로 고치는 동안 만료된 TTL이 있는 디렉터리에 액세스하는 NFS 및 SMB 작업이 차단됩니다.

> **Note**
>
> 캐시 새로 고침은 디렉터리 액세스 작업을 차단할 수 있으므로 배포에 유용한 가장 긴 TTL 기간을 구성하는 것이 좋습니다.

Storage Gateway 콘솔을 사용하여 자동 캐시 새로 고침 일정을 구성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택합니다.
3. 새로 고침 일정을 구성할 파일 공유를 선택합니다.
4. 작업에서 파일 공유 설정 편집을 선택합니다.
5. 이후 S3에서 자동 캐시 새로 고침의 경우 확인란을 선택하고 TTL(Time To Live)을 사용하여 파일 공유의 캐시를 새로 고치는 시간을 일, 시간 및 분으로 설정합니다. TTL은 마지막 새로 고침 이후 디렉터리에 액세스할 때 File Gateway가 Amazon S3 버킷에서 해당 디렉터리의 콘텐츠를 처음으로 새로 고칠 때까지의 시간입니다.
6. 변경 사항 저장을 선택합니다.

Amazon CloudWatch 규칙과 AWS Lambda 함께를 사용하여 자동 캐시 새로 고침 일정 구성

Amazon CloudWatch 규칙과 AWS Lambda 함께를 사용하여 자동 캐시 새로 고침 일정을 구성하려면

1. S3 File Gateway에서 사용하는 S3 버킷을 식별합니다.
2. 이벤트 섹션이 비어 있는지 확인합니다. 나중에 자동으로 채워집니다.
3. IAM 역할을 생성하고 Lambda `lambda.amazonaws.com`에 대한 신뢰 관계를 허용합니다.
4. 다음 정책을 추가합니다.

   JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "StorageGatewayPermissions",
            "Effect": "Allow",
            "Action": "storagegateway:RefreshCache",
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchLogsPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogStream",
                "logs:CreateLogGroup",
                "logs:PutLogEvents"
            ],
            "Resource": "*"
        }
    ]
}
```

5. Lambda 콘솔을 사용하여 Lambda 함수를 생성합니다.
6. Lambda 작업에 다음 함수를 사용합니다.

```
import json
import boto3
client = boto3.client('storagegateway')
```

```
def lambda_handler(event, context):
    print(event)
    response = client.refresh_cache(
        FileShareARN='arn:aws:storagegateway:ap-southeast-2:672406474878:share/
share-E51FBS9C'
    )
    print(response)
    return 'Your FileShare cache has been refreshed'
```

7. 실행 역할에 대해 생성한 IAM 역할을 선택합니다.
8. 선택 사항: Amazon S3에 대한 트리거를 추가하고 ObjectCreated 또는 ObjectRemoved 이벤트를 선택합니다.

> **Note**
>
> RefreshCache는 다른 프로세스를 시작하기 전에 한 프로세스를 완료해야 합니다. 버킷에 많은 객체를 생성하거나 삭제하면 성능이 저하될 수 있습니다. 따라서 S3 트리거를 사용하지 않는 것이 좋습니다. 대신 다음에 설명된 Amazon CloudWatch 규칙을 사용합니다.

9. CloudWatch 콘솔에서 CloudWatch 규칙을 생성하고 일정을 추가합니다. 일반적으로 고정 속도는 30분으로 하는 것이 좋습니다. 그러나 대형 S3 버킷에는 1~2시간을 사용할 수 있습니다.
10. CloudWatch 이벤트에 대한 새 트리거를 추가하고 방금 생성한 규칙을 선택합니다.
11. Lambda 구성을 저장합니다. 테스트를 선택합니다.
12. S3 PUT을 선택하고 요구 사항에 맞게 테스트를 사용자 지정합니다.
13. 테스트가 성공해야 합니다. 그렇지 않은 경우 요구 사항에 맞게 JSON을 수정하고 다시 테스트합니다.
14. Amazon S3 콘솔을 열고 생성한 이벤트와 Lambda 함수 ARN이 있는지 확인합니다.
15. Amazon S3 콘솔 또는 AWS CLI를 사용하여 객체를 S3 버킷에 업로드합니다.

CloudWatch 콘솔은 다음과 유사한 CloudWatch 출력을 생성합니다.

```
{
    u'Records': [
        {u'eventVersion': u'2.0', u'eventTime': u'2018-09-10T01:03:59.217Z',
 u'requestParameters': {u'sourceIPAddress': u'MY-IP-ADDRESS'},
        u's3': {u'configurationId': u'95a51e1c-999f-485a-b994-9f830f84769f',
 u'object': {u'sequencer': u'00549CC2BF34D47AED', u'key': u'new/filename.jpeg'},
```

```
        u'bucket': {u'arn': u'arn:aws:s3:::amzn-s3-demo-bucket', u'name':
 u'MY-GATEWAY-NAME', u'ownerIdentity': {u'principalId': u'A3OKNBZ72HVPP9'}},
 u's3SchemaVersion': u'1.0'},
        u'responseElements': {u'x-amz-id-2':
 u'76tiugjhvjfyriugiug87t890nefevbck0iA3rPU9I/s4NY9uXwtRL75tCyxasgsdgfsq+IhvAg5M=',
 u'x-amz-request-id': u'651C2D4101D31593'},
        u'awsRegion': u'MY-REGION', u'eventName': u'ObjectCreated:PUT',
 u'userIdentity': {u'principalId': u'AWS:AROAI5LQR5JHFHDFHDFHJ:MY-USERNAME'},
 u'eventSource': u'aws:s3'}
    ]
}
```

Lambda 호출은 다음과 유사한 출력을 제공합니다.

```
{
    u'FileShareARN': u'arn:aws:storagegateway:REGION:ACCOUNT-ID:share/MY-SHARE-
ID',
        'ResponseMetadata': {'RetryAttempts': 0, 'HTTPStatusCode': 200,
 'RequestId': '6663236a-b495-11e8-946a-bf44f413b71f',
            'HTTPHeaders': {'x-amzn-requestid': '6663236a-b495-11e8-946a-
bf44f413b71f', 'date': 'Mon, 10 Sep 2018 01:03:59 GMT',
                'content-length': '90', 'content-type': 'application/x-amz-
json-1.1'
        }
    }
}
```

클라이언트에 탑재된 NFS 공유에는 이 업데이트가 반영됩니다.

> **Note**
>
> 수백만 개의 객체가 있는 대용량 버킷에서 대용량 객체 생성 또는 삭제를 업데이트하는 캐시의 경우 업데이트에 몇 시간이 걸릴 수 있습니다.

16. Amazon S3 콘솔 또는 AWS CLI를 사용하여 해당 객체를 수동으로 삭제합니다.
17. 클라이언트에 탑재된 NFS 공유를 확인합니다. 객체가 사라졌는지 확인합니다(캐시가 새로 고쳐졌기 때문).
18. CloudWatch 로그를 확인하여 `ObjectRemoved:Delete` 이벤트를 사용한 삭제 로그를 확인합니다.

```
{
    u'account': u'MY-ACCOUNT-ID', u'region': u'MY-REGION', u'detail': {}, u'detail-
type': u'Scheduled Event', u'source': u'aws.events',
    u'version': u'0', u'time': u'2018-09-10T03:42:06Z', u'id':
 u'6468ef77-4db8-0200-82f0-04e16a8c2bdb',
    u'resources': [u'arn:aws:events:REGION:MY-ACCOUNT-ID:rule/FGw-RefreshCache-CW']
}
```

> **Note**
>
> cron 작업 또는 예약된 작업의 경우 CloudWatch 로그 이벤트는 `u'detail-type': u'Scheduled Event'`입니다.

Storage Gateway 콘솔을 사용하여 수동 캐시 새로 고침 수행

Storage Gateway 콘솔을 사용하여 수동 캐시 새로 고침을 수행하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 파일 공유를 선택한 다음 새로 고침을 수행할 파일 공유를 선택합니다.
3. 작업에서 캐시 새로 고침을 선택하십시오.

   새로 고침 프로세스에 걸리는 시간은 게이트웨이에 캐시된 객체의 수와 S3 버킷에 추가되거나 S3 버킷에서 제거된 객체의 수에 따라 달라집니다.

Storage Gateway API를 사용하여 수동 캐시 새로 고침 수행

다음 절차에서는 Storage Gateway API를 사용하여 수동 캐시 새로 고침을 수행합니다. API 기반 캐시 새로 고침을 수행하기 전에 다음 사항을 고려하세요.

- 재귀 또는 비재귀 새로 고침을 지정할 수 있습니다.
- 재귀 새로 고침은 리소스 집약적이고 비용이 많이 듭니다.
- 새로 고침은 요청에서 인수로 전달하는 디렉터리에만 Amazon S3 API 비용이 발생하고, 재귀 새로 고침을 지정하는 경우 해당 디렉터리의 하위 항목에만 비용이 발생합니다.
- 새로 고침은 게이트웨이를 사용하는 동안 다른 작업과 동시에 실행됩니다.

  - NFS 및 SMB 작업은 일반적으로 작업에서 액세스하는 디렉터리에 대해 새로 고침이 활성화되지 않는 한 새로 고침 중에 차단되지 않습니다.
  - 게이트웨이는 현재 캐시 콘텐츠가 오래된 것인지 확인할 수 없으며 최신성과 관계없이 NFS 및 SMB 작업에 현재 콘텐츠를 사용합니다.
  - 캐시 새로 고침은 게이트웨이 가상 하드웨어 리소스를 활용하므로 새로 고침이 진행되는 동안 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.
- API 기반 캐시 새로 고침은 게이트웨이와 Amazon S3 버킷 간의 워크플로 외부에서 Amazon S3 버킷의 콘텐츠를 직접 업데이트하는 경우에만 권장됩니다.

> **Note**
>
> 게이트웨이 워크플로 외부에서 Amazon S3 콘텐츠를 업데이트하는 특정 디렉터리를 알고 있는 경우 API 기반 새로 고침 요청에 이러한 디렉터리를 지정하여 Amazon S3 API 비용과 게이트웨이 성능 영향을 줄이는 것이 좋습니다.

Storage Gateway API를 사용하여 수동 캐시 새로 고침을 수행하려면

- HTTP POST 요청을 보내 Storage Gateway API를 통해 원하는 파라미터로 `RefreshCache` 작업을 호출합니다. 자세한 내용은 AWS Storage Gateway API 참조에서 RefreshCache를 참조하세요.

> **Note**
>
> `RefreshCache` 요청을 전송하면 캐시 새로 고침 작업만 시작됩니다. 캐시 새로 고침이 완료되었다고 해서 반드시 파일 새로 고침이 완료되었음을 의미하지는 않습니다. 게이트웨이 파일 공유에서 새 파일을 확인하기 전에 파일 새로 고침 작업이 완료되었는지 확인하려면 `refresh-complete` 알림을 사용하십시오. 이렇게 하려면 Amazon CloudWatch 이벤트를 통해 알림을 받도록 구독하면 됩니다. 자세한 내용은 파일 작업에 대한 알림 받기 단원을 참조하십시오.

Amazon S3 File Gateway에 S3 Object Lock 사용

Amazon S3 File Gateway는 Amazon S3 Object Lock이 켜진 S3 버킷에 대한 액세스를 지원합니다. Amazon S3 Object Lock을 사용하면 "Write Once Read Many(WORM)" 모델을 사용하여 객체를 저장

할 수 있습니다. Amazon S3 Object Lock을 사용하면, S3 버킷의 객체를 삭제하거나 덮어쓰지 못하게 할 수 있습니다. Amazon S3 Object Lock은 객체 버전 관리 기능과 연동하여 데이터를 보호합니다.

Amazon S3 Object Lock을 활성화할 경우에도 객체를 수정할 수는 있습니다. 예를 들어 S3 File Gateway의 파일 공유를 통해 객체에 쓰거나 객체를 삭제하거나 객체 이름을 변경할 수 있습니다. 이러한 방식으로 객체를 수정할 경우 S3 File Gateway는 이전 버전(잠긴 개체)에 영향을 주지 않고 새 버전의 객체를 저장합니다.

예를 들어 S3 File Gateway NFS 또는 SMB 인터페이스를 사용하여 파일을 삭제할 때 해당 S3 객체가 잠긴 경우, 게이트웨이는 S3 삭제 마커를 객체의 다음 버전으로 배치하고 원래 객체 버전을 그대로 유지합니다. 마찬가지로, S3 File Gateway가 잠긴 객체의 내용이나 메타데이터를 수정하는 경우, 객체의 새 버전은 변경 사항과 함께 업로드되지만 객체의 원래 잠금 버전은 변경되지 않은 상태로 유지됩니다.

Amazon S3 3 Object Lock 기능에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 S3 Object Lock을 사용하여 객체 잠금을 참조하세요.

파일 공유 상태 이해

파일 공유의 상태를 확인하여 파일 공유의 상태를 한눈에 볼 수 있습니다. 상태가 파일 공유가 정상적으로 작동하고 있음을 나타내는 경우 사용자는 아무런 조치를 취할 필요가 없습니다. 상태가 문제가 있음을 나타내는 경우 조사하여 조치가 필요한지 여부를 확인할 수 있습니다.

Storage Gateway 콘솔의 상태 열에서 파일 공유의 상태를 볼 수 있습니다. 제대로 작동하는 파일 공유에는 AVAILABLE 상태가 표시됩니다. 대부분의 경우 이 상태가 되어야 합니다.

다음 표에서는 파일 공유 상태, 파일 공유의 의미 및 조치가 필요한지 여부를 설명합니다.

Status	의미
AVAILABLE	파일 공유가 적절히 구성되어 사용할 수 있습니다. 제대로 작동하는 파일 공유의 표준 상태입니다.
CREATING	파일 공유가 아직 완전히 생성되지 않았으므로 사용할 준비가 되지 않았습니다. CREATING 상태는 일시적입니다. 아무 조치도 필요하지 않습니다. 파일 공유가이 상태에서 멈춘 경우 게이트웨이 VM이 연결을 끊었기 때문일 수 있습니다 AWS.

Status	의미
업데이트 중	파일 공유 구성이 현재 업데이트 중입니다. 업데이트 중 상태는 과도기적인 상태입니다. 아무 조치도 필요하지 않습니다. 파일 공유가이 상태에서 멈춘 경우 게이트웨이 VM이 연결을 끊었기 때문일 수 있습니다 AWS.
DELETING	파일 공유를 삭제하고 있습니다. 모든 데이터가 업로드될 때까지 파일 공유는 삭제되지 않습니다 AWS. DELETING 상태는 일시적이므로 아무 조치도 취할 필요가 없습니다.
FORCE_DELETING	파일 공유를 강제로 삭제하고 있습니다. 파일 공유는 즉시 삭제되고 데이터는에 업로드되지 않습니다 AWS. FORCE_DELETING 상태는 일시적이므로 아무 조치도 취할 필요가 없습니다.
UNAVAILABLE	파일 공유가 비정상 상태입니다. 조치가 필요합니다. 몇 가지 가능한 원인으로는 역할 정책 오류 또는 존재하지 않는 Amazon S3 버킷에 대한 매핑이 있습니다. 비정상 상태를 유발한 문제가 해결되면 파일 공유는 다시 AVAILABLE 상태가 됩니다.

게이트웨이 상태 이해

AWS Storage Gateway 배포의 각 게이트웨이에는 게이트웨이의 상태를 한눈에 알려주는 연결된 상태가 있습니다. 대부분의 경우 그 상태는 게이트웨이가 정상적으로 작동하고 있으므로 아무 조치도 취할 필요가 없음을 알려줍니다. 어떤 경우에는 상태를 통해 조치가 필요한 또는 필요 없는 문제가 있음을 나타냅니다.

Storage Gateway 콘솔의 게이트웨이 페이지에서 배포의 각 게이트웨이 상태를 확인할 수 있습니다. 게이트웨이 상태가 게이트웨이 이름 옆의 상태 열에 나타납니다. 정상적으로 작동하는 게이트웨이의 상태는 `RUNNING`입니다.

다음 표에는 각 게이트웨이 상태에 대한 설명과 해당 상태를 기반으로 조치를 취해야 하는지 여부가 나와 있습니다. 사용 중인 모든 경우 또는 거의 대부분의 경우에 게이트웨이는 `RUNNING` 상태여야 합니다.

Status	의미
`RUNNING`	게이트웨이가 적절히 구성되어 사용할 수 있습니다.

Status	의미
OFFLINE	다음 중 하나 이상의 이유로 게이트웨이가 OFFLINE 상태일 수 있습니다. • 게이트웨이가 Storage Gateway 서비스 엔드포인트에 연결할 수 없습니다. • 게이트웨이가 예기치 않게 종료되었습니다. • 게이트웨이에 연결 해제되었거나 수정되었거나 실패한 연결된 캐시 디스크가 있습니다.

Amazon S3 File Gateway의 대역폭 관리

게이트웨이의 업로드 처리량을 로 제한 AWS 하여 게이트웨이가 사용하는 네트워크 대역폭의 양을 제어할 수 있습니다. 기본적으로 활성화된 게이트웨이는 속도 제한이 없습니다.

AWS Management Console, AWS 소프트웨어 개발 키트(SDK) 또는 AWS Storage Gateway API를 사용하여 bandwidth-rate-limit 일정을 구성할 수 있습니다(AWS Storage Gateway API 참조의 UpdateBandwidthRateLimitSchedule 참조). 대역폭 속도 제한 일정을 사용하는 경우 하루 또는 일주일 내내 제한이 자동으로 변경되도록 구성할 수 있습니다. 자세한 내용은 Storage Gateway 콘솔을 사용하여 게이트웨이의 대역폭 속도 제한 일정을 보고 편집할 수 있습니다. 단원을 참조하십시오.

Storage Gateway 콘솔의 모니터링 탭 또는 Amazon CloudWatch에서 CloudBytesUploaded 지표를 사용하여 Storage Gateway의 업로드 처리량을 모니터링할 수 있습니다.

> **Note**
>
> 대역폭 속도 제한은 Storage Gateway 파일 업로드에만 적용됩니다. 다른 게이트웨이 작업은 영향을 받지 않습니다.
> 대역폭 속도 제한은 업로드되는 모든 파일의 초당 평균 처리량을 밸런싱하는 방식으로 작동합니다. 업로드가 특정 마이크로초 또는 밀리초 동안 대역폭 속도 제한을 잠시 초과할 수는 있지만, 장기간에 걸쳐 큰 폭의 스파이크가 발생하지는 않습니다.
> 현재는 대역폭 속도 제한 및 일정 구성이 Amazon FSx File Gateway 유형에서 지원되지 않습니다.

주제

- Storage Gateway 콘솔을 사용하여 게이트웨이의 대역폭 속도 제한 일정을 보고 편집할 수 있습니다.
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for .NET
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS Tools for Windows PowerShell

Storage Gateway 콘솔을 사용하여 게이트웨이의 대역폭 속도 제한 일정을 보고 편집할 수 있습니다.

이 섹션에서는 게이트웨이의 대역폭 속도 제한 일정을 보고 편집하는 방법을 설명합니다.

대역폭 속도 제한 일정을 보고 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 왼쪽 탐색 창에서 게이트웨이를 선택한 다음 관리할 게이트웨이를 선택합니다.
3. 작업에서 대역폭 속도 제한 일정 편집을 선택합니다.

   게이트웨이의 현재 대역폭 속도 제한 일정이 대역폭 속도 제한 일정 편집 페이지에 표시됩니다. 기본적으로 새 게이트웨이에는 정의된 대역폭 속도 제한이 없습니다.
4. (선택 사항) 새 대역폭 속도 제한 추가를 선택하여 구성 가능한 새 간격을 일정에 추가합니다. 추가한 간격에 대해 다음 정보를 입력합니다.

   - 업로드 속도 - 업로드 속도 제한을 초당 메가비트(Mbps) 단위로 입력합니다. 최소값은 100Mbps입니다.
   - 요일 - 간격을 적용할 요일을 선택합니다. 평일(월요일~금요일), 주말(토요일 및 일요일), 매주 요일 또는 매주 특정 요일에 간격을 적용할 수 있습니다. 대역폭 속도 제한을 모든 날짜 및 항상 균일하게 지속적으로 적용하려면 일정 없음을 선택합니다.
   - 시작 시간 - 게이트웨이의 UTC 기준 시간대와 HH:MM 형식을 사용하여 대역폭 간격의 시작 시간을 입력합니다.

     > **Note**
     >
     > 여기에 지정한 시간이 시작되면 대역폭 속도 제한 간격이 시작됩니다.

   - 종료 시간 - 게이트웨이의 GMT 기준 시간대와 HH:MM 형식을 사용하여 대역폭 간격의 종료 시간을 입력합니다.

> **Important**
>
> 여기에 지정된 시간이 끝나면 대역폭 속도 제한 간격이 종료됩니다. 한 시간이 지나면 종료되는 간격을 예약하려면 **59**를 입력합니다.
> 간격 사이에 중단 없이 시간 시작 시점에 전환되는 연속적인 간격을 예약하려면 첫 번째 간격의 종료 분에 **59**를 입력합니다. 다음 간격의 시작 분에는 **00**을 입력합니다.

5. (선택 사항) 대역폭 속도 제한 일정이 완료될 때까지 원하는 대로 이전 단계를 반복합니다. 일정에서 일정 간격을 삭제해야 하는 경우 제거를 선택합니다.

> **Important**
>
> 대역폭 속도 제한 간격은 겹칠 수 없습니다. 간격의 시작 시간은 이전 간격의 종료 시간 이후, 다음 간격의 시작 시간 이전이어야 합니다.

6. 작업을 마쳤으면 변경 사항 저장을 선택합니다.

를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java

대역폭 속도 제한을 프로그래밍 방식으로 업데이트하면 일정 기간 동안 예약된 작업을 사용하는 등의 방법으로 자동으로 제한을 조정할 수 있습니다. 다음 예시는 AWS SDK for Java를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예시 코드를 사용하려면 Java 콘솔 애플리케이션을 실행하는 방법을 잘 알아야 합니다. 자세한 내용은AWS SDK for Java 개발자 안내서에서 시작하기를 참조하세요.

Example:를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java

다음 Java 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN), 업로드 한도를 제공해야 합니다. Storage Gateway에서 사용할 수 있는 AWS 서비스 엔드포인트 목록은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
```

```
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleRequest;
   import com.amazonaws.services.storagegateway.model.
UpdateBandwidthRateLimitScheduleReturn;

   import java.util.Arrays;
   import java.util.Collections;
   import java.util.List;

   public class UpdateBandwidthExample {

       public static AWSStorageGatewayClient sgClient;

       // The gatewayARN
       public static String gatewayARN = "*** provide gateway ARN ***";

       // The endpoint
       static String serviceURL = "https://storagegateway.us-east-1.amazonaws.com";

       // Rates
       static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum 100
Megabits/second

       public static void main(String[] args) throws IOException {

           // Create a Storage Gateway client
           sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
           sgClient.setEndpoint(serviceURL);

           UpdateBandwidth(gatewayARN, uploadRate, null); // download rate not
supported by S3 File Gateways

       }

       private static void UpdateBandwidth(String gatewayArn, long uploadRate, long
downloadRate) {
           try
           {
               BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
               BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
```

```
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                    .withGatewayARN(gatewayArn)
                    .with
BandwidthRateLimitIntervals(Collections.singletonList(noScheduleInterval));

                UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);

                String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.getGatewayARN();
                System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
                System.out.println("Upload bandwidth limit = " + uploadRate + " bits
per second");
            }
            catch (AmazonClientException ex)
            {
                System.err.println("Error updating gateway bandwith.\n" +
ex.toString());
            }
        }
    }
```

를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for .NET

대역폭 속도 제한을 프로그래밍 방식으로 업데이트하면 일정 기간 동안 예약된 작업을 사용하는 등의 방법으로 자동으로 제한을 조정할 수 있습니다. 다음 예제에서는 .NET용 AWS 소프트웨어 개발 키트(SDK)를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예시 코드를 사용하려면 .NET 콘솔 애플리케이션을 실행하는 방법을 잘 알아야 합니다. 자세한 내용은AWS SDK for .NET 개발자 안내서에서 시작하기를 참조하세요.

Example:를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for .NET

다음 C# 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN), 업로드 한도를 제공해야 합니다. Storage Gateway에서 사용할 수 있는 AWS 서비스 엔드포인트 목록은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

```
    using System;
    using System.Collections.Generic;
    using System.Linq;
    using System.Text;
    using Amazon.StorageGateway;
    using Amazon.StorageGateway.Model;

    namespace AWSStorageGateway
    {
        class UpdateBandwidthExample
        {
            static AmazonStorageGatewayClient sgClient;
            static AmazonStorageGatewayConfig sgConfig;

            // The gatewayARN
            public static String gatewayARN = "*** provide gateway ARN ***";

            // The endpoint
            static String serviceURL = "https://storagegateway.us-
east-1.amazonaws.com";

            // Rates
            static long uploadRate = 100 * 1024 * 1024;  // Bits per second, minimum
 100 Megabits/second

            public static void Main(string[] args)
            {
                // Create a Storage Gateway client
                sgConfig = new AmazonStorageGatewayConfig();
                sgConfig.ServiceURL = serviceURL;
                sgClient = new AmazonStorageGatewayClient(sgConfig);

                UpdateBandwidth(gatewayARN, uploadRate, null);

                Console.WriteLine("\nTo continue, press Enter.");
                Console.Read();
```

```
            }

            public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
            {
                try
                {
                   BandwidthRateLimit bandwidthRateLimit = new
BandwidthRateLimit(downloadRate, uploadRate);
                    BandwidthRateLimitInterval noScheduleInterval = new
BandwidthRateLimitInterval()
                    .withBandwidthRateLimit(bandwidthRateLimit)
                    .withDaysOfWeek(Arrays.asList(1, 2, 3, 4, 5, 6, 0))
                    .withStartHourOfDay(0)
                    .withStartMinuteOfHour(0)
                    .withEndHourOfDay(23)
                    .withEndMinuteOfHour(59);
                  List <BandwidthRateLimitInterval> bandwidthRateLimitIntervals = new
List<BandwidthRateLimitInterval>();
                  bandwidthRateLimitIntervals.Add(noScheduleInterval);
                  UpdateBandwidthRateLimitScheduleRequest
updateBandwidthRateLimitScheduleRequest =
                    new UpdateBandwidthRateLimitScheduleRequest()
                       .withGatewayARN(gatewayARN)
                       .with BandwidthRateLimitIntervals(bandwidthRateLimitIntervals);

                    UpdateBandwidthRateLimitScheduleReturn
updateBandwidthRateLimitScheuduleResponse =
sgClient.UpdateBandwidthRateLimitSchedule(updateBandwidthRateLimitScheduleRequest);
                    String returnGatewayARN =
updateBandwidthRateLimitScheuduleResponse.GatewayARN;
                    Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                    Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits
per second");
                }
                catch (AmazonStorageGatewayException ex)
                {
                    Console.WriteLine("Error updating gateway bandwith.\n" +
ex.ToString());
                }
            }
        }
```

```
    }
```

를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS Tools for Windows PowerShell

대역폭 속도 제한을 프로그래밍 방식으로 업데이트하면 일정 기간 동안 예약된 작업을 사용하는 등의 방법으로 자동으로 제한을 조정할 수 있습니다. 다음 예시는 AWS Tools for Windows PowerShell를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예시 코드를 사용하려면 PowerShell 스크립트를 실행하는 방법을 잘 알아야 합니다. 자세한 내용은 AWS Tools for PowerShell 사용 설명서에서 시작하기를 참조하세요.

Example:를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS Tools for Windows PowerShell

다음 PowerShell 스크립트 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 스크립트를 사용하려면 게이트웨이 Amazon 리소스 이름(ARN) 및 업로드 한도를 제공해야 합니다.

```
    <#
    .DESCRIPTION
        Update Gateway bandwidth limits schedule

    .NOTES
        PREREQUISITES:
        1) AWS Tools for PowerShell from https://aws.amazon.com/powershell/
        2) Credentials and region stored in session using Initialize-AWSDefault.
        For more info, see https://docs.aws.amazon.com/powershell/latest/userguide/
specifying-your-aws-credentials.html


    .EXAMPLE
        powershell.exe .\SG_UpdateBandwidth.ps1
    #>

    $UploadBandwidthRate = 100 * 1024 * 1024
    $gatewayARN = "*** provide gateway ARN ***"

    $bandwidthRateLimitInterval = New-Object
 Amazon.StorageGateway.Model.BandwidthRateLimitInterval
    $bandwidthRateLimitInterval.StartHourOfDay = 0
    $bandwidthRateLimitInterval.StartMinuteOfHour = 0
    $bandwidthRateLimitInterval.EndHourOfDay = 23
    $bandwidthRateLimitInterval.EndMinuteOfHour = 59
    $bandwidthRateLimitInterval.DaysOfWeek = 0,1,2,3,4,5,6
```

```
   $bandwidthRateLimitInterval.AverageUploadRateLimitInBitsPerSec =
$UploadBandwidthRate

   #Update Bandwidth Rate Limits
   Update-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN `
                                       -BandwidthRateLimitInterval
@($bandwidthRateLimitInterval)

   $schedule =  Get-SGBandwidthRateLimitSchedule -GatewayARN $gatewayARN

   Write-Output("`nGateway: " + $gatewayARN);
   Write-Output("`nNew bandwidth throttle schedule: " +
$schedule.BandwidthRateLimitIntervals.AverageUploadRateLimitInBitsPerSec)
```

Storage Gateway 모니터링

이 섹션의 주제에서는 게이트웨이와 관련된 리소스 모니터링하는 것을 포함하여 Amazon CloudWatch를 사용하여 게이트웨이를 모니터링하는 방법에 대해 설명합니다. Storage Gateway 콘솔을 사용하여 게이트웨이에 대한 지표와 경보를 볼 수 있습니다. 예를 들어 읽기 및 쓰기 작업에 사용된 바이트 수, 읽기 및 쓰기 작업에 소요된 시간, AWS 클라우드에서 데이터를 검색하는 데 걸린 시간을 볼 수 있습니다. 지표를 사용하여 게이트웨이의 상태를 추적하고 하나 이상의 지표가 정의한 임계값 범위를 벗어나는 경우 이를 알리도록 경보를 설정할 수 있습니다.

Storage Gateway는 추가 요금 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이 지표를 사용하여 기록 정보에 액세스하고 게이트웨이가 어떻게 실행되고 있는지 더 잘 파악할 수 있습니다. 또한 Storage Gateway는 고해상도 경보를 제외한 CloudWatch 경보를 추가 비용 없이 제공합니다. CloudWatch 요금에 대한 자세한 내용은 Amazon CloudWatch 요금을 참조하세요. CloudWatch에 대한 자세한 정보는 Amazon CloudWatch 사용 설명서를 참조하세요.

주제

- CloudWatch 경보 이해 - 경보 상태 및 권장 구성을 포함하여 CloudWatch 경보에 대한 기본 정보를 알아봅니다.
- 권장 CloudWatch 경보 생성 - 초기 File Gateway 설정 프로세스의 일부로 모든 권장 CloudWatch 경보를 빠르게 자동으로 구성하는 방법을 알아봅니다.
- 사용자 지정 CloudWatch 경보 생성 - 특정 평가 기준을 사용하여 특정 지표를 모니터링하여 경보 상태를 트리거하고 알림을 전송하는 사용자 지정 CloudWatch 경보를 생성하는 방법을 알아봅니다.
- S3 File Gateway 모니터링 - CloudWatch 로그 및 감사 로그를 보고 게이트웨이에서 보고하는 특정 게이트웨이 및 파일 공유파일 시스템 지표에 대한 정보를 찾는 방법을 알아봅니다.

CloudWatch 경보 이해

CloudWatch 경보는 지표와 표현식을 기반으로 게이트웨이에 대한 정보를 모니터링합니다. Storage Gateway 콘솔에서 게이트웨이에 대한 CloudWatch 경보를 추가하고 상태를 확인할 수 있습니다. S3 File Gateway를 모니터링하는 데 사용되는 지표에 대한 자세한 내용은 게이트웨이 지표 이해 및 파일 공유 지표 이해를 참조하세요. 각 경보마다 ALARM 상태 활성화 조건을 지정합니다. ALARM 상태에서는 Storage Gateway 콘솔의 경보 상태 표시등이 빨간색으로 바뀌므로 상태를 사전 예방적으로 쉽게 모니터링할 수 있습니다. 지속적인 상태 변화에 따라 자동으로 작업을 호출하도록 경보를 구성할 수 있습니다. CloudWatch 경보에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서에서 Amazon CloudWatch 경보 사용을 참조하세요.

> **Note**
>
> CloudWatch 보기 권한이 없으면 경보를 볼 수 없습니다.

활성화된 각 게이트웨이에 대해 다음과 같은 CloudWatch 경보를 생성하는 것이 좋습니다.

- 높은 IO 대기: 15분 내에 3개의 데이터 포인트에 대해 `IoWaitpercent` >= 20
- 캐시 더티 백분율: 20분 내에 4개의 데이터 포인트에 대해 `CachePercentDirty` > 80
- 업로드에 실패한 파일: 5분 이내에 데이터 포인트 1개에 대해 `FilesFailingUpload` >= 1
- 파일 공유 사용 불가: 5분 이내에 데이터 포인트 1개에 대해 `FileSharesUnavailable` >= 1
- 상태 알림: 5분 이내에 1개의 데이터 포인트에 대해 `HealthNotifications` >= 1 이 경보를 구성할 때 누락된 데이터 처리를 NotBreaching으로 설정합니다.

> **Note**
>
> CloudWatch에서 게이트웨이에 이전 상태 알림이 있는 경우에만 상태 알림 경보를 설정할 수 있습니다.

VMware 고가용성 클러스터의 일부인 VMware 호스트 플랫폼의 게이트웨이의 경우 이 추가 CloudWatch 경보도 사용하는 것이 좋습니다.

- 가용성 알림: 5분 이내에 1개의 데이터 포인트에 대해 `AvailabilityNotifications` >= 1 이 경보를 구성할 때 누락된 데이터 처리를 NotBreaching으로 설정합니다.

다음 표에서는 CloudWatch 경보 상태에 대해 설명합니다.

State	설명
정상	지표 또는 표현식이 정의된 임계값 내에 있습니다.
경보	지표 또는 표현식이 정의된 임계값을 벗어났습니다.

State	설명
데이터 부족	경보가 방금 시작되었거나, 지표를 사용할 수 없거나, 지표를 통해 경보 상태를 결정하는 데 사용할 충분한 데이터가 없습니다.
없음	게이트웨이에 대한 경보가 생성되지 않습니다. 새 경보를 생성하려면 게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성 섹션을 참조하세요.
Unavailable	경보의 상태를 알 수 없습니다. 모니터링 탭에서 오류 정보를 보려면 사용할 수 없음을 선택합니다.

게이트웨이에 대한 권장 CloudWatch 경보 생성

Storage Gateway 콘솔을 사용하여 새 게이트웨이를 생성할 때 초기 설정 프로세스의 일부로 모든 권장 CloudWatch 경보를 자동으로 생성하도록 선택할 수 있습니다. 자세한 내용은 Amazon S3 File Gateway 구성을 참조하세요. 첫 번째 설정을 완료한 후 기존 게이트웨이에 대해 권장 CloudWatch 경보를 추가하거나 업데이트하려면 다음 절차를 수행합니다.

기존 게이트웨이에 대해 권장 CloudWatch 경보를 추가하거나 업데이트하려면

> **Note**
>
> 이 기능을 사용하려면 CloudWatch 정책 권한이 필요합니다. 이 권한은 사전 구성된 Storage Gateway 전체 액세스 정책의 일부로 자동 부여되지 않습니다. 권장 CloudWatch 경보를 생성하기 전에 보안 정책이 다음 권한을 부여하는지 확인하세요.
>
> - `cloudwatch:PutMetricAlarm` - 경보 생성
> - `cloudwatch:DisableAlarmActions` - 경보 작업 끄기
> - `cloudwatch:EnableAlarmActions` - 경보 작업 켜기
> - `cloudwatch:DeleteAlarms` - 경보 삭제

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home/)을 엽니다.

2. 페이지의 왼쪽에 있는 탐색 창에서 게이트웨이를 선택한 다음 권장 CloudWatch 경보를 생성할 게이트웨이를 선택합니다.
3. 게이트웨이 세부 정보 페이지에서 모니터링 탭을 선택합니다.
4. 경보에서 권장 경보 생성을 선택합니다. 권장 경보는 자동으로 생성됩니다.

   경보 섹션에 특정 게이트웨이에 대한 모든 CloudWatch 경보가 나열됩니다. 여기서 하나 이상의 경보를 선택 및 삭제하고, 경보 작업을 켜거나 끄고, 새 경보를 생성할 수 있습니다.

게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성

CloudWatch는 경보 상태가 변경되면 Amazon Simple Notification Service(SNS)를 사용하여 경보 알림을 보냅니다. 경보는 지정한 기간 동안 단일 지표를 감시하고 여러 기간에 지정된 임계값에 대한 지표 값을 기준으로 작업을 하나 이상 수행합니다. 이 작업은 Amazon SNS 주제로 전송되는 알림입니다. CloudWatch 경보를 생성할 때 Amazon SNS 주제를 생성할 수 있습니다. Amazon SNS에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 설명서의 Amazon SNS란 무엇입니까?를 참조하세요.

Storage Gateway 콘솔에서 CloudWatch 경보를 생성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home/)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 경보를 생성할 게이트웨이를 선택합니다.
3. 게이트웨이 세부 정보 페이지에서 모니터링 탭을 선택합니다.
4. 경보에서 경보 생성을 선택하여 CloudWatch 콘솔을 엽니다.
5. CloudWatch 콘솔을 사용하여 원하는 경보 유형을 생성합니다. 다음 유형의 경보를 생성할 수 있습니다.

   - 정적 임계값 경보: 선택한 지표에 대해 설정된 임계값을 기반으로 하는 경보입니다. 지표가 지정된 수의 평가 기간에 대한 임계값을 위반할 경우 경보가 ALARM 상태로 전환됩니다.

     정적 임계값 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 정적 임계값을 기반으로 CloudWatch 경보 생성을 참조하세요.
   - 이상 탐지 경보: 이상 탐지는 과거 지표 데이터를 마이닝하고 예상 값의 모델을 생성합니다. 이상 탐지 임곗값에 대한 값을 설정합니다. 그러면 CloudWatch는 모델과 함께 이 임곗값을 사용하여 지표 값의 '정상' 범위를 결정합니다. 임곗값에 대한 값이 클수록 '정상' 값의 밴드가 더 두꺼워집니다. 지표 값이 예상 값 범위보다 높을 때만 경보를 활성화하거나, 범위보다 낮을 때만 경보를 활성화하거나, 범위보다 높거나 낮을 때 경보를 활성화하도록 선택할 수 있습니다.

이상 탐지 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 이상 탐지를 기반으로 CloudWatch 경보 생성을 참조하세요.

- 지표 수학 표현식 경보: 수학 표현식에 사용된 하나 이상의 지표에 기반한 경보입니다. 표현식, 임계값 및 평가 기간을 지정합니다.

  지표 수학 표현식 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 지표 수학 표현식을 기반으로 CloudWatch 경보 생성을 참조하세요.
- 복합 경보: 다른 경보의 경보 상태를 감시하여 경보 상태를 결정하는 경보입니다. 복합 경보를 사용하면 경보 노이즈를 줄이는 데 도움이 될 수 있습니다.

  복합 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 복합 경보 생성을 참조하세요.

6. CloudWatch 콘솔에서 경보를 생성한 후 Storage Gateway 콘솔로 돌아갑니다. 다음 중 하나를 수행하여 경보를 볼 수 있습니다.

   - 탐색 창에서 게이트웨이를 선택한 다음 경보를 확인할 게이트웨이를 선택합니다. 세부 정보 탭의 경보에서 CloudWatch 경보를 선택합니다.
   - 탐색 창에서 게이트웨이를 선택하고, 경보를 확인할 게이트웨이를 선택한 다음 모니터링 탭을 선택합니다.

     경보 섹션에 특정 게이트웨이에 대한 모든 CloudWatch 경보가 나열됩니다. 여기서 하나 이상의 경보를 선택 및 삭제하고, 경보 작업을 켜거나 끄고, 새 경보를 생성할 수 있습니다.
   - 탐색 창에서 게이트웨이를 선택한 다음 경보를 확인할 게이트웨이의 경보 상태를 선택합니다.

경보를 편집하거나 삭제하는 방법에 대한 자세한 내용은 CloudWatch 경보 편집 또는 삭제를 참조하세요.

> **Note**
>
> Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하면 게이트웨이와 관련된 CloudWatch 경보도 모두 자동으로 삭제됩니다.

S3 File Gateway 모니터링

Amazon CloudWatch 지표 및 감사 로그 AWS Storage Gateway 를 사용하여에서 S3 File GatewayFSx 및 관련 리소스를 모니터링할 수 있습니다. CloudWatch Events를 사용하여 파일 작업이 완료되면 알림을 받을 수도 있습니다.

주제

- CloudWatch 로그 그룹을 사용하여 S3 File Gateway 가져오기
- Amazon CloudWatch 지표 사용
- 파일 작업에 대한 알림 받기
- 게이트웨이 지표 이해
- 파일 공유 지표 이해
- S3 File Gateway 감사 로그 이해

CloudWatch 로그 그룹을 사용하여 S3 File Gateway 가져오기

Amazon CloudWatch Logs를 사용하여 S3 File Gateway 및 관련 리소스 상태에 대한 정보를 가져올 수 있습니다. 로그를 사용하여 게이트웨이에 로그가 발생하는지 모니터링할 수 있습니다. 또한 Amazon CloudWatch 구독 필터를 사용하여 실시간으로 로그 정보 처리를 자동화할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서에서 구독을 통한 로그 데이터 실시간 처리를 참조하세요.

예를 들어 게이트웨이를 모니터링하고, S3 File Gateway에서 Amazon S3 버킷에 파일을 업로드하는 데 실패하면 알림을 받도록 CloudWatch 로그 그룹을 구성할 수 있습니다. 게이트웨이를 활성화할 때나 게이트웨이가 활성화되어 실행된 후에 그룹을 구성할 수 있습니다. 게이트웨이를 활성화할 때 CloudWatch 로그 그룹을 구성하는 방법에 대한 자세한 내용은 Amazon S3 File Gateway 구성 섹션을 참조하세요. CloudWatch 로그 그룹에 대한 일반적인 정보는 Amazon CloudWatch 사용 설명서에서 로그 그룹 및 로그 스트림 작업을 참조하세요.

다음은 S3 File Gateway에서 보고하는 오류의 예입니다.

```
{
    "severity": "ERROR",
    "bucket": "bucket-smb-share2",
    "roleArn": "arn:aws:iam::123456789012:role/amzn-s3-demo-bucket",
    "source": "share-E1A2B34C",
    "type": "InaccessibleStorageClass",
```

```
    "operation": "S3Upload",
    "key": "myFolder/myFile.text",
    "gateway": "sgw-B1D123D4",
    "timestamp": "1565740862516"
}
```

이 오류는 S3 File Gateway가 Amazon S3 Standard 스토리지 클래스에서 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 전환되었으므로 `myFolder/myFile.text` 객체를 Amazon S3에 업로드할 수 없다는 의미입니다.

앞에 나온 게이트웨이 상태 로그에서는 다음 항목이 주어진 정보를 지정합니다.

- `source: share-E1A2B34C` - 이 오류를 일으킨 파일 공유를 나타냅니다.
- `"type": "InaccessibleStorageClass"` - 발생한 오류의 유형을 나타냅니다. 여기서는 게이트웨이가 지정된 객체를 Amazon S3에 업로드하거나 Amazon S3에서 읽으려고 할 때 이 오류가 발생했습니다. 하지만 이때 객체는 Amazon Glacier로 전환했습니다. `"type"`의 값은 S3 File Gateway가 일으키는 모든 오류일 수 있습니다. 가능한 오류 목록은 문제 해결: File Gateway 문제 섹션을 참조하세요.
- `"operation": "S3Upload"`는 게이트웨이가 이 객체를 S3에 업로드하려고 할 때 이 오류가 발생했음을 나타냅니다.
- `"key": "myFolder/myFile.text"` - 오류를 유발한 객체를 나타냅니다.
- `gateway": "sgw-B1D123D4`는 이 오류를 일으킨 S3 File Gateway를 나타냅니다.
- `"timestamp": "1565740862516"`은 오류가 발생한 시간을 나타냅니다.

S3 File Gateway에서 보고할 수 있는 오류를 해결하는 방법에 대한 자세한 내용은 문제 해결: File Gateway 문제 섹션을 참조하세요.

게이트웨이가 활성화된 후 CloudWatch 로그 그룹 구성

다음 절차에서는 게이트웨이가 활성화된 후 CloudWatch 로그 그룹을 구성하는 방법을 보여줍니다.

S3 File Gateway와 함께 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/storagegateway/home Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 작업에서 게이트웨이 정보 편집을 선택합니다.

4. 로그 그룹 설정 방법 선택에서 다음 중 하나를 선택합니다.

   - 새 CloudWatch 로그 그룹을 생성하려면 새 로그 그룹 생성을 선택합니다.
   - 기존 CloudWatch 로그 그룹을 사용하려면 기존 로그 그룹 사용을 선택합니다.

     기존 로그 그룹 목록에서 로그 그룹을 선택합니다.
   - CloudWatch 로그 그룹을 사용하여 게이트웨이를 모니터링하지 않으려면 로깅을 비활성화합니다.
5. 변경 사항 저장을 선택합니다.
6. 게이트웨이의 상태 로그를 확인하려면 다음을 수행합니다.

   1. 탐색 창에서 게이트웨이를 선택한 후 CloudWatch 로그 그룹을 구성한 게이트웨이를 선택합니다.
   2. 세부 정보 탭을 선택하고 상태 로그에서 CloudWatch 로그를 선택합니다. CloudWatch 콘솔에서 로그 그룹 세부 정보 페이지가 열립니다.

Amazon CloudWatch 지표 사용

AWS Management Console 또는 CloudWatch API를 사용하여 S3 File GatewayFSx에 대한 모니터링 데이터를 가져올 수 있습니다. 콘솔에는 CloudWatch API의 원시 데이터를 기초로 하는 일련의 그래프가 표시됩니다. AWS SDKs 중 하나 또는 Amazon CloudWatch API 도구를 통해 CloudWatch API를 사용할 수도 있습니다. 필요에 따라 콘솔에 표시되거나 API에서 가져온 그래프를 사용하는 것이 더 나을 수 있습니다.

지표를 다룰 때 사용하는 방법에 관계 없이 다음 정보를 지정해야 합니다.

- 작업할 지표 차원. 차원은 지표를 고유하게 식별하는 데 도움이 되는 이름-값 페어입니다. Storage Gateway의 차원은 `GatewayId` 및 `GatewayName`입니다. CloudWatch 콘솔에서 `Gateway Metrics` 보기를 사용하여 게이트웨이별 차원을 쉽게 선택할 수 있습니다. 차원에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서에서 차원을 참조하세요.
- `ReadBytes`와 같은 지표 이름.

다음 표에는 사용 가능한 Storage Gateway 지표 데이터의 유형이 요약되어 있습니다.

Amazon CloudWatch 네임스페이스	차원	설명
`AWS/StorageGateway`	`GatewayId`, `GatewayName`	이 차원은 게이트웨이의 여러 측면을 설명하는 지표 데이터를 필터링합니다. `GatewayId` 및 `GatewayName` 차원을 모두 지정하여 작업할 S3 File Gateway를 식별할 수 있습니다. 게이트웨이의 처리량 및 지연 시간 데이터는 게이트웨이의 모든 파일 공유를 기반으로 합니다. 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.

게이트웨이 및 파일 지표 작업은 기타 서비스 지표 작업과 유사합니다. 가장 일반적인 지표 작업 중 몇 가지에 대한 설명은 다음에 나열된 CloudWatch 문서에서 확인할 수 있습니다.

- 사용 가능한 지표 보기
- 지표에 대한 통계 가져오기
- CloudWatch 경보 생성

파일 작업에 대한 알림 받기

Storage Gateway는 파일 작업이 완료되면 다음 CloudWatch Events를 시작할 수 있습니다.

- 게이트웨이가 파일 공유에서 Amazon S3로 파일을 비동기 업로드하는 작업이 완료될 때 알림을 받을 수 있습니다. `NotificationPolicy` 파라미터를 사용하여 파일 업로드 알림을 요청합니다. 그러면 완료된 각 파일 업로드에 대한 알림이 Amazon S3로 전송됩니다. 자세한 내용은 파일 업로드 알림 받기 단원을 참조하십시오.
- 게이트웨이가 파일 공유에서 Amazon S3로 작업 파일 세트를 비동기 업로드하는 작업이 완료될 때 알림을 받을 수 있습니다. NotifyWhenUploaded API 작업을 사용하여 작업 파일 세트 업로드 알림을 요청할 수 있습니다. 그러면 작업 파일 세트의 모든 파일이 Amazon S3에 업로드되면 알림이 전송됩니다. 자세한 내용은 작업 파일 세트 업로드 알림 받기 단원을 참조하십시오.

- 게이트웨이가 S3 버킷에서 캐시 새로 고침을 완료하면 알림을 받을 수 있습니다. Storage Gateway 콘솔이나 API를 통해 RefreshCache 작업을 호출할 경우, 작업 완료 시 알림을 받도록 구독합니다. 자세한 내용은 캐시 새로 고침 알림 받기 단원을 참조하십시오.

요청한 파일 작업이 완료되면 Storage Gateway가 CloudWatch Events를 통해 알림을 전송합니다. Amazon SNS, Amazon SQS 또는 AWS Lambda 함수와 같은 이벤트 대상을 통해 알림을 보내도록 CloudWatch Events를 구성할 수 있습니다. 예를 들어 이메일 또는 문자 메시지 같은 알림을 Amazon SNS 소비자에게 전송하도록 Amazon SNS 대상을 구성할 수 있습니다. CloudWatch Events에 대한 자세한 내용은 CloudWatch Events란 무엇입니까?를 참조하세요.

CloudWatch Events 알림을 설정하려면

1. Storage Gateway에서 요청한 이벤트가 발생할 때 간접 호출할 Amazon SNS 주제 또는 Lambda 함수와 같은 대상을 생성합니다.
2. CloudWatch Events 콘솔에서 Storage Gateway의 이벤트를 기반으로 대상을 호출하기 위한 규칙을 만듭니다.
3. 규칙에 따라 이벤트 유형에 대한 이벤트 패턴을 생성합니다. 이벤트가 이 규칙 패턴과 일치할 때 알림이 전송됩니다.
4. 대상을 선택하고 설정을 구성합니다.

다음 예제는 지정된 게이트웨이와 지정된 AWS 리전에서 지정된 이벤트 유형을 시작하는 규칙을 보여줍니다. 예를 들어 이벤트 유형으로 `Storage Gateway File Upload Event`를 지정할 수 있습니다.

```
{
   "source":[
      "aws.storagegateway"
   ],
   "resources":[
      "arn:aws:storagegateway:AWS Region:account-id
                :gateway/gateway-id"
   ],
   "detail-type":[
      "Event type"
   ]
}
```

CloudWatch Events 규칙 사용 방법에 대한 자세한 내용은 Amazon CloudWatch Events 사용 설명서의 이벤트에서 트리거되는 CloudWatch Events 규칙 생성을 참조하세요.

파일 업로드 알림 받기

파일 업로드 알림은 다음과 같은 두 가지 사용 사례에서 사용할 수 있습니다.

- 업로드된 파일의 클라우드 내 처리를 자동화하기 위해 `NotificationPolicy` 파라미터를 호출하고 알림 ID를 받을 수 있습니다. 파일이 업로드되면 발생하는 알림은 API가 반환한 것과 동일한 알림 ID를 갖습니다. 이 알림 ID를 매핑하여 업로드 중인 파일 목록을 추적할 경우, 동일한 ID의 이벤트가 생성될 때 AWS 에 업로드된 파일의 처리를 시작할 수 있습니다
- 콘텐츠 배포 사용 사례의 경우 동일한 Amazon S3 버킷에 매핑되는 S3 File Gateway 두 개가 있을 수 있습니다. Gateway1용 파일 공유 클라이언트는 Amazon S3에 새 파일을 업로드할 수 있으며, Gateway2의 파일 공유 클라이언트는 이 파일을 읽습니다. 이 파일은 Amazon S3에 업로드되지만, Gateway2에서는 Amazon S3에서 로컬로 캐시된 버전의 파일을 사용하므로 새 파일이 표시되지 않습니다. Gateway2에 파일을 표시하려면 `NotificationPolicy` 파라미터를 사용하여 업로드가 완료될 때 알리도록 Gateway1의 파일 업로드 알림을 요청할 수 있습니다. 그런 다음 CloudWatch Events를 사용하여 Gateway2의 파일 공유에 대한 RefreshCache 요청을 자동으로 발행할 수 있습니다. RefreshCache 요청이 완료되면 새 파일이 Gateway2에 표시됩니다.

Example예제 - 파일 업로드 알림

다음 예제는 사용자가 생성한 규칙과 이벤트가 일치할 때 CloudWatch를 통해 사용자에게 전송되는 파일 업로드 알림을 보여 줍니다. 이 알림은 JSON 형식입니다. 이 알림을 텍스트 메시지로 대상에게 전달되도록 구성할 수 있습니다. `detail-type`은 `Storage Gateway Object Upload Event`입니다.

```
{
    "version": "0",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Object Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2020-11-05T12:34:56Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:storagegateway:us-east-1:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-1:123456789011:gateway/sgw-712345DA",
        "arn:aws:s3:::do-not-delete-bucket"
    ],
```

```
    "detail": {
        "object-size": 1024,
        "modification-time": "2020-01-05T12:30:00Z",
        "object-key": "my-file.txt",
        "event-type": "object-upload-complete",
        "prefix": "prefix/",
        "bucket-name": "amzn-s3-demo-bucket",
    }
}
```

필드 이름	설명
버전	IAM 정책의 현재 버전입니다.
id	IAM 정책을 식별하는 ID입니다.
detail-type	전송된 알림을 시작한 이벤트 유형에 대한 설명입니다.
source	요청 및 알림의 소스인 AWS 서비스입니다.
계정	요청 및 알림이 생성된 AWS 계정의 ID입니다.
시간	Amazon S3에 파일을 업로드하는 요청이 이루어진 시간입니다.
리전	요청 및 알림이 전송된 AWS 리전입니다.
리소스	정책이 적용된 Storage Gateway 리소스입니다.
객체 크기	객체의 크기(바이트)입니다.
수정 시간	클라이언트가 파일을 수정한 시간입니다.
객체 키	파일 경로입니다.
event-type	알림을 시작한 CloudWatch Events입니다.
prefix	S3 버킷의 접두사 이름.
bucket-name	S3 버킷의 이름.

작업 파일 세트 업로드 알림 받기

작업 파일 세트 업로드 알림은 다음과 같은 두 가지 사용 사례에서 사용할 수 있습니다.

- 업로드된 파일의 클라우드 내 처리를 자동화하기 위해 `NotifyWhenUploaded` API를 호출하고 알림 ID를 받을 수 있습니다. 작업 파일 세트가 업로드되면 발생하는 알림은 API가 반환한 것과 동일한 알림 ID를 갖습니다. 이 알림 ID를 매핑하여 업로드 중인 파일 목록을 추적하는 경우 ID가 동일한 이벤트가 생성될 AWS 때에 업로드되는 작업 파일 세트의 처리를 시작할 수 있습니다.
- 콘텐츠 배포 사용 사례의 경우 동일한 Amazon S3 버킷에 매핑되는 S3 File Gateway 두 개가 있을 수 있습니다. Gateway1용 파일 공유 클라이언트는 Amazon S3에 새 파일을 업로드할 수 있으며, Gateway2의 파일 공유 클라이언트는 이 파일을 읽습니다. 이 파일은 Amazon S3에 업로드되지만, Gateway2에서는 S3에서 로컬로 캐시된 버전의 파일을 사용하므로 새 파일이 표시되지 않습니다. Gateway2에 파일을 표시하려면 NotifyWhenUploaded API 작업을 사용하여 작업 파일 세트 업로드가 완료될 때 알리도록 Gateway1의 파일 업로드 알림을 요청할 수 있습니다. 그런 다음 CloudWatch Events를 사용하여 Gateway2의 파일 공유에 대한 RefreshCache 요청을 자동으로 발행할 수 있습니다. RefreshCache 요청이 완료되면 새 파일이 Gateway2에 표시됩니다. 이 작업은 파일을 게이트웨이 캐시 스토리지로 가져오지 않습니다. S3 버킷의 객체 인벤토리 변경 사항을 반영하도록 캐시된 인벤토리만 업데이트합니다.

Example예 - 작업 파일 세트 업로드 알림

다음 예제는 사용자가 생성한 규칙과 이벤트가 일치할 때 CloudWatch를 통해 사용자에게 전송되는 작업 파일 세트 업로드 알림을 보여 줍니다. 이 알림은 JSON 형식입니다. 이 알림을 텍스트 메시지로 대상에게 전달되도록 구성할 수 있습니다. `detail-type`은 `Storage Gateway File Upload Event`입니다.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway File Upload Event",
    "source": "aws.storagegateway",
    "account": "123456789012",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
```

```
        "event-type": "upload-complete",
        "notification-id": "11b3106b-a18a-4890-9d47-a1a755ef5e47",
        "request-received": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z"
    }
}
```

필드 이름	설명
버전	IAM 정책의 현재 버전입니다.
id	IAM 정책을 식별하는 ID입니다.
detail-type	전송된 알림을 시작한 이벤트 유형에 대한 설명입니다.
source	요청 및 알림의 소스인 AWS 서비스입니다.
계정	요청 및 알림이 생성된 AWS 계정의 ID입니다.
시간	Amazon S3에 파일을 업로드하는 요청이 이루어진 시간입니다.
리전	요청 및 알림이 전송된 AWS 리전입니다.
리소스	정책이 적용된 Storage Gateway 리소스입니다.
event-type	알림을 시작한 CloudWatch Events입니다.
notification-id	전송된 알림의 무작위 생성 ID입니다. 이 ID는 UUID 형식입니다. `NotifyWhenUploaded` 호출 시 반환된 알림 ID입니다.
request-received	게이트웨이가 `NotifyWhenUploaded` 요청을 받은 시간입니다.
completed	작업 세트의 모든 파일이 Amazon S3에 업로드된 시간입니다.

캐시 새로 고침 알림 받기

캐시 새로 고침 알림 사용 사례의 경우 두 개의 S3 File Gateway를 동일한 Amazon S3 버킷에 매핑할 수 있으며, Gateway1용 NFS 클라이언트는 새 파일을 S3 버킷에 업로드합니다. 파일은 Amazon S3에 업로드되지만, 캐시를 새로 고칠 때까지 Gateway2에 나타나지 않습니다. 왜냐하면 Gateway2가 Amazon S3에서 로컬에 캐시된 버전의 파일을 사용하기 때문입니다. 캐시 새로 고침이 완료될 때 Gateway2에서 파일을 처리하고 싶을 수 있습니다. 대용량 파일은 Gateway2에 표시되는 데 시간이 걸릴 수 있으므로 캐시 새로 고침이 완료될 때 알림을 받고 싶을 수 있습니다. 모든 파일이 Gateway2에서 표시될 때 이를 알려주도록 Gateway2에서 캐시 새로 고침 알림을 요청할 수 있습니다.

Example예제 - 캐시 새로 고침 알림

다음 예제에서는 사용자가 생성한 규칙과 이벤트가 일치할 때 CloudWatch를 통해 사용자에게 전송되는 캐시 새로 고침 알림을 보여줍니다. 이 알림은 JSON 형식입니다. 이 알림을 텍스트 메시지로 대상에게 전달되도록 구성할 수 있습니다. `detail-type`은 `Storage Gateway Refresh Cache Event`입니다.

```
{
    "version": "2012-10-17",
    "id": "2649b160-d59d-c97f-3f64-8aaa9ea6aed3",
    "detail-type": "Storage Gateway Refresh Cache Event",
    "source": "aws.storagegateway",
    "account": "209870788375",
    "time": "2017-11-06T21:34:42Z",
    "region": "us-east-2",
    "resources": [
        "arn:aws:storagegateway:us-east-2:123456789011:share/share-F123D451",
        "arn:aws:storagegateway:us-east-2:123456789011:gateway/sgw-712345DA"
    ],
    "detail": {
        "event-type": "refresh-complete",
        "notification-id": "1c14106b-a18a-4890-9d47-a1a755ef5e47",
        "started": "2018-02-06T21:34:42Z",
        "completed": "2018-02-06T21:34:53Z",
        "folderList": [
            "/"
        ]
    }
}
```

필드 이름	설명
버전	IAM 정책의 현재 버전입니다.
id	IAM 정책을 식별하는 ID입니다.
detail-type	전송된 알림을 시작한 이벤트 유형에 대한 설명입니다.
source	요청 및 알림의 소스인 AWS 서비스입니다.
계정	요청 및 알림이 생성된 AWS 계정의 ID입니다.
시간	작업 세트에서 파일 새로 고침 요청이 이루어진 시간입니다.
리전	요청 및 알림이 전송된 AWS 리전입니다.
리소스	정책이 적용된 Storage Gateway 리소스입니다.
event-type	알림을 시작한 CloudWatch Events입니다.
notification-id	전송된 알림의 무작위 생성 ID입니다. 이 ID는 UUID 형식입니다. `RefreshCache` 호출 시 반환된 알림 ID입니다.
하기	게이트웨이가 `RefreshCache` 요청을 받고 새로 고침이 시작된 시간입니다.
completed	작업 세트의 새로 고침이 완료된 시간입니다.
folderList	캐시에서 새로 고친 폴더 경로의 목록(쉼표 구분)입니다. 기본값은 ["/"]입니다.

게이트웨이 지표 이해

다음 표에서는 S3 File Gateway를 포함하는 지표를 설명합니다. 각 게이트웨이에는 연관된 지표 집합이 있습니다. 일부 게이트웨이별 지표는 특정 파일 공유별 지표와 이름이 같습니다. 이러한 지표는 동일한 종류의 측정값을 나타내지만, 파일 공유가 아닌 게이트웨이로 범위가 한정됩니다.

특정 지표 관련 작업을 할 경우 항상 게이트웨이와 파일 공유 중 어느 것과 관련된 작업을 할 것인지 지정해야 합니다. 특히 게이트웨이 지표로 작업할 때는 지표 데이터를 보려는 게이트웨이에 대한 `Gateway Name`을 지정해야 합니다. 자세한 내용은 Amazon CloudWatch 지표 사용 단원을 참조하십시오.

> **Note**
>
> 일부 지표는 가장 최근 모니터링 기간 동안 새 데이터가 생성된 경우에만 데이터 포인트를 반환합니다.

다음 표에서는 S3 File Gateway에 대한 정보를 얻는 데 사용할 수 있는 지표에 대해 설명합니다.

지표	설명
`AuditNotifications`	이 지표는 내보낸 감사 로그 수를 보고합니다. 단위: 개
`AvailabilityNotifications`	이 지표는 보고 기간 동안 게이트웨이에서 생성된 가용성 관련 상태 알림 수를 보고합니다. 단위: 개
`CacheFileSize`	이 지표는 게이트웨이 캐시의 파일 크기를 추적합니다. 이 지표를 `Average` 통계와 함께 사용하여 게이트웨이 캐시에 있는 파일의 평균 크기를 측정합니다. 이 지표를 `Max` 통계와 함께 사용하여 게이트웨이 캐시에 있는 파일의 최대 크기를 측정합니다. 단위: 바이트
`CacheFree`	이 지표는 게이트웨이 캐시에서 사용 가능한 바이트 수를 보고합니다. 단위: 바이트

지표	설명
CacheHitPercent	캐시로부터 읽는 게이트웨이의 애플리케이션 읽기 작업 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 게이트웨이로부터의 애플리케이션 읽기 작업이 없는 경우, 지표가 100%를 보고합니다. 단위: 백분율
CachePercentDirty	지속되지 않은 게이트웨이 캐시의 전체 백분율입니다 AWS. 보고 기간 종료 시점에서 샘플이 채취됩니다. Sum 통계와 함께 이 지표를 사용합니다. 이상적으로는 이 지표가 낮게 유지되어야 합니다. 단위: 백분율
CachePercentUsed	전체 게이트웨이에서 사용되는 데이터 캐시의 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 백분율
CacheUsed	이 지표는 게이트웨이 캐시에서 사용된 바이트 수를 보고합니다. 단위: 바이트

지표	설명
CloudBytesDownloaded	보고 기간 AWS 동안 게이트웨이가에서 다운로드한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트
CloudBytesUploaded	보고 기간 AWS 동안 게이트웨이가에 업로드한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 초당 입력/출력 작업 수(IOPS)를 측정할 수 있습니다. 단위: 바이트
FilesFailingUpload	이 지표는 AWS에 업로드하지 못한 파일 수를 추적합니다. 이러한 파일은 문제에 대한 자세한 정보가 포함된 상태 알림을 생성합니다. 이 지표를 통계와 함께 사용하여 현재 Sum에 업로드하지 못한 파일 수를 표시합니다 AWS. 단위: 개
FileSharesUnavailable	이 지표는 사용할 수 없음 상태인 이 게이트웨이의 파일 공유 수를 제공합니다. 이 지표가 파일 공유를 사용할 수 없다고 보고하는 경우 게이트웨이에 문제가 발생하여 워크플로가 중단될 수 있습니다. 이 지표가 0이 아닌 값을 보고할 때에 대한 경보를 생성하는 것이 좋습니다. 단위: 개

지표	설명
FilesRenamed	이 지표는 보고 기간에 이름이 변경된 파일 수를 추적합니다. 단위: 개
HealthNotifications	이 지표는 보고 기간 동안 이 게이트웨이에서 생성된 상태 알림 수를 보고합니다. 단위: 개
IndexEvictions	이 지표는 새 항목을 위한 공간을 만들기 위해 파일 메타데이터의 캐시된 인덱스에서 메타데이터가 제거된 파일 수를 보고합니다. 게이트웨이는이 메타데이터 인덱스를 유지 관리합니다.이 메타데이터 인덱스는 온디맨드 AWS 클라우드에서 채워집니다. 단위: 개
IndexFetches	이 지표는 메타데이터를 가져온 파일의 수를 보고합니다. 게이트웨이는 요청 시 AWS 클라우드에서 채워지는 파일 메타데이터의 캐시된 인덱스를 유지합니다. 단위: 개
IoWaitPercent	이 지표는 CPU가 로컬 디스크의 응답을 기다리는 시간의 비율을 보고합니다. 단위: 백분율
MemTotalBytes	이 지표는 게이트웨이의 총 메모리 양을 보고합니다. 단위: 바이트

지표	설명
MemUsedBytes	이 지표는 게이트웨이에서 사용된 메모리의 양을 보고합니다. 단위: 바이트
NfsSessions	이 지표는 게이트웨이에서 활성 상태인 NFS 세션 수를 보고합니다. 단위: 개
RootDiskFreeBytes	이 지표는 게이트웨이의 루트 디스크에서 사용 가능한 바이트 수를 보고합니다. 이 지표가 20GB 미만이 무료라고 보고하는 경우 루트 디스크의 크기를 늘려야 합니다. 루트 디스크 크기를 늘리려면 VM의 기존 루트 디스크 크기를 늘리면 됩니다. VM이 재부팅되면 게이트웨이는 루트 디스크의 증가된 크기를 인식합니다. 단위: 바이트
S3GetObjectRequestTime	이 지표는 게이트웨이가 S3 객체 가져오기 요청을 완료하는 시간을 보고합니다. 단위: 밀리초
S3PutObjectRequestTime	이 지표는 게이트웨이가 S3 객체 배치 요청을 완료하는 시간을 보고합니다. 단위: 밀리초
S3UploadPartRequestTime	이 지표는 게이트웨이가 S3 파트 업로드 요청을 완료하는 시간을 보고합니다. 단위: 밀리초

지표	설명
SmbV1Sessions	이 지표는 게이트웨이에서 활성 상태인 SMBv1 세션 수를 보고합니다. 단위: 개
SmbV2Sessions	이 지표는 게이트웨이에서 활성 상태인 SMBv2 세션 수를 보고합니다. 단위: 개
SmbV3Sessions	이 지표는 게이트웨이에서 활성 상태인 SMBv3 세션 수를 보고합니다. 단위: 개
TotalCacheSize	이 지표는 캐시의 총 크기를 보고합니다. 단위: 바이트
UserCpuPercent	이 지표는 게이트웨이 처리에 소요된 시간의 비율을 보고합니다. 단위: 백분율

파일 공유 지표 이해

파일 공유를 나타내는 Storage Gateway 지표에 대해 다음과 같은 정보를 확인할 수 있습니다. 각 파일 공유에는 연결된 지표 집합이 있습니다. 일부 파일 공유별 지표는 특정 게이트웨이별 지표와 이름이 같습니다. 이러한 지표는 동일한 종류의 측정값을 나타내지만, 그 대신 파일 공유로 범위가 한정됩니다.

지표 관련 작업을 하려면 항상 먼저 게이트웨이와 파일 공유 중 어느 것과 관련된 작업을 할 것인지 지정해야 합니다. 특히 파일 공유 지표 작업을 할 때는 지표를 보고 싶은 파일 공유를 식별하는 `File share ID`를 지정해야 합니다. 자세한 내용은 Amazon CloudWatch 지표 사용 단원을 참조하십시오.

> **Note**
>
> 일부 지표는 가장 최근 모니터링 기간 동안 새 데이터가 생성된 경우에만 데이터 포인트를 반환합니다.

다음 표에서는 파일 공유에 대한 정보를 얻는 데 사용할 수 있는 Storage Gateway 측정치에 대해 설명합니다.

지표	설명
`CacheHitPercent`	캐시로부터 읽는 파일 공유의 애플리케이션 읽기 작업 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 파일 공유로부터의 애플리케이션 읽기 작업이 없는 경우, 지표가 100%를 보고합니다. 단위: 백분율
`CachePercentDirty`	AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율 중 파일 공유가 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. `Sum` 통계와 함께 이 지표를 사용합니다. 이상적으로는 이 지표가 낮게 유지되어야 합니다. **Note** 게이트웨이의 `CachePercentDirty` 지표를 사용하면 AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율을 알 수 있습니다. 단위: 백분율

지표	설명
CachePercentUsed	전체 게이트웨이에서 사용되는 데이터 캐시의 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 이 파일 공유별 지표는 해당 게이트웨이별 지표와 동일한 값을 보고합니다. 단위: 백분율
CloudBytesUploaded	보고 기간 AWS 동안 게이트웨이가에 업로드한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트
CloudBytesDownloaded	보고 기간 AWS 동안 게이트웨이가에서 다운로드한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 초당 입력/출력 작업 수(IOPS)를 측정할 수 있습니다. 단위: 바이트
FilesFailingUpload	이 지표는 AWS에 업로드하지 못한 파일 수를 추적합니다. 이러한 파일은 문제에 대한 자세한 정보가 포함된 상태 알림을 생성합니다. 이 지표를 통계와 함께 사용하여 현재 Sum에 업로드하지 못한 파일 수를 표시합니다 AWS. 단위: 개

지표	설명
ReadBytes	파일 공유에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 읽은 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트
WriteBytes	보고 기간 동안 온프레미스 애플리케이션에 작성한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트

S3 File Gateway 감사 로그 이해

Amazon S3 File Gateway(S3 File Gateway) 감사 로그는 파일 공유 내의 파일과 폴더의 사용자 액세스에 대한 세부 정보를 제공합니다. 이러한 정보를 사용하여 사용자 활동을 모니터링하고 부적절한 활동 패턴이 식별되면 조치를 취할 수 있습니다.

운영

다음 표에서는 S3 File Gateway 감사 로그 파일 액세스 작업에 대해 설명합니다.

작업 이름	정의
데이터 읽기	파일의 내용을 읽습니다.
데이터 쓰기	파일의 내용을 변경합니다.
생성	새 파일 또는 폴더를 만듭니다.
이름 바꾸기	기존 파일 또는 폴더의 이름을 바꿉니다.

작업 이름	정의
Delete	파일 또는 폴더를 삭제합니다.
속성 쓰기	파일 또는 폴더 메타데이터(ACL, 소유자, 그룹, 권한)를 업데이트합니다.

속성

다음 표에서는 S3 File Gateway 감사 로그 파일 액세스 속성에 대해 설명합니다.

속성	정의
`accessMode`	객체에 대한 권한 설정입니다.
`accountDomain` (SMB만 해당)	클라이언트의 계정이 속한 AD(Active Directory) 도메인입니다.
`accountName` (SMB만 해당)	클라이언트의 Active Directory 사용자 이름입니다.
`bucket`	S3 버킷 이름입니다.
`clientGid` (NFS만 해당)	객체에 액세스하는 사용자 그룹의 식별자입니다.
`clientUid` (NFS만 해당)	객체에 액세스하는 사용자의 식별자입니다.
`ctime`	클라이언트에서 설정한 객체의 콘텐츠나 메타데이터가 수정된 시간입니다.
`groupId`	객체의 소유자에 대한 식별자입니다.
`fileSizeInBytes`	파일 생성 시 클라이언트에서 설정한 파일 크기(바이트)입니다.
`gateway`	스토리지 게이트웨이 ID입니다.

속성	정의
mtime	클라이언트에서 설정한 객체의 콘텐츠가 수정된 시간입니다.
newObjectName	이름이 바뀐 후 새 객체의 전체 경로입니다.
objectName	객체의 전체 경로입니다.
objectType	객체가 파일 또는 폴더인지를 정의합니다.
operation	객체 액세스 작업의 이름입니다.
ownerId	객체의 소유자에 대한 식별자입니다.
securityDescriptor (SMB만 해당)	객체에 설정된 DACL(임의 액세스 제어 목록)을 SDDL 형식으로 표시합니다.
shareName	액세스 중인 공유의 이름입니다.
source	감사할 파일 공유의 ID입니다.
sourceAddress	파일 공유 클라이언트 머신의 IP 주소입니다.
status	작업의 상태. 성공만 기록됩니다(권한 거부로 인해 발생한 실패를 제외하고 실패가 기록됩니다).
timestamp	게이트웨이의 OS 타임스탬프를 기준으로 작업이 발생한 시간입니다.
version	감사 로그 형식의 버전입니다.

작업당 로깅된 속성

다음 표에서는 각 파일 액세스 작업에서 기록된 S3 File Gateway 감사 로그 속성에 대해 설명합니다.

	데이터 읽기	데이터 쓰기	폴더 생성	파일 만들기	파일/폴더 이름 바꾸기	파일/폴더 삭제	쓰기 속성 (ACL 변경 - SMB 만 해당)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
access			X	X					X	
accoun main (SMB 만 해당)	X	X	X	X	X	X	X	X	X	X
accoun me (SMB 만 해당)	X	X	X	X	X	X	X	X	X	X
bucket	X	X	X	X	X	X	X	X	X	X
client (NFS 만 해당)	X	X	X	X	X	X		X	X	X
client (NFS 만 해당)	X	X	X	X	X	X		X	X	X
ctime			X	X						

	데이터 읽기	데이터 쓰기	폴더 생성	파일 만들기	파일/폴더 이름 바꾸기	파일/폴더 삭제	쓰기 속성 (ACL 변경 - SMB 만 해당)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
groupI			X	X						
fileSi nBytes				X						
gatewa	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
newObj Name					X					
object e	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
operat	X	X	X	X	X	X	X	X	X	X
ownerI			X	X				X		
securi escrip (SMB 만 해당)							X	X		

	데이터 읽기	데이터 쓰기	폴더 생성	파일 만들기	파일/폴더 이름 바꾸기	파일/폴더 삭제	쓰기 속성 (ACL 변경 - SMB 만 해당)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
shareN	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
source ress	X	X	X	X	X	X	X	X	X	X
status	X	X	X	X	X	X	X	X	X	X
timest	X	X	X	X	X	X	X	X	X	X
versic	X	X	X	X	X	X	X	X	X	X

S3 File Gateway에 대한 캐시 보고서 생성

이제 S3 File Gateway는 현재 특정 파일 공유의 로컬 업로드 캐시에 있는 파일에 대한 메타데이터 보고서를 생성할 수 있습니다. 보고서에 표시되는 캐시된 파일의 특정 유형을 결정하는 필터와 추가 기준을 적용할 수 있습니다. 이 보고서를 사용하여 게이트웨이 문제를 식별하고 해결할 수 있습니다. 예를 들어 게이트웨이에서 Amazon S3로 업로드하는 데 실패한 파일이 있는 경우 업로드에 실패한 특정 파일과 업로드 실패 이유를 나열하는 보고서를 생성할 수 있습니다. 보고서는 지정한 필터 파라미터 세트와 일치하는 파일 목록이 포함된 CSV 파일입니다. 출력 파일은 보고서를 구성할 때 지정한 버킷 위치에 Amazon S3 객체로 저장됩니다. AWS Storage Gateway API를 사용하여 캐시 보고서를 생성하려면 Storage Gateway API 참조의 StartCacheReport를 참조하세요. Storage Gateway 콘솔에서 캐시 보고서를 생성하려면 다음 절차를 사용합니다.

사전 조건

- 캐시 보고서를 저장할 Amazon S3 버킷에 대한 `s3:PutObject` 및 `s3:AbortMultipartUpload` 권한이 게이트웨이에 있어야 합니다.
- 현재 파일 공유에 대해 진행 중인 다른 캐시 보고서가 없어야 합니다.
- 파일 공유에 대한 기존 캐시 보고서가 10개 미만이어야 합니다.
- 게이트웨이는 온라인 상태여야 하며에 연결되어 있어야 합니다 AWS.
- 게이트웨이 루트 디스크에 최소 20GB의 여유 공간이 있어야 합니다.

Storage Gateway 콘솔을 사용하여 캐시 보고서를 생성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home/)을 엽니다.
2. 페이지 왼쪽의 탐색 창에서 파일 공유를 선택한 다음 캐시 보고서를 생성할 파일 공유를 선택합니다.
3. 작업 드롭다운 메뉴에서 캐시 보고서 생성을 선택합니다.
4. Amazon S3 위치에 Amazon S3 버킷과 완료된 캐시 보고서 CSV 파일 객체를 Amazon S3에 저장할 위치의 접두사를 입력합니다. 기존 Amazon S3 스토리지에서 버킷과 접두사를 선택하려면 S3 찾아보기를 선택합니다.
5. IAM 역할의 경우 다음 중 하나를 수행하여 캐시 보고서를 생성하고 저장할 수 있는 권한을 File Gateway에 부여하는 IAM 역할을 지정합니다.

   - 기존 IAM 역할을 지정하려면 드롭다운 목록에서 역할을 선택합니다.
   - 새 IAM 역할을 수동으로 생성하려면 역할 생성을 선택한 다음 IAM 콘솔을 사용하여 새 역할을 생성합니다.

   > **Note**
   >
   > 보고서 버킷 Amazon S3 위치에 객체를 쓰고 보고서 버킷으로의 멀티파트 업로드를 중지하려면 지정한 IAM 역할에 다음 권한이 있어야 합니다.
   >
   > - `s3:PutObject`
   > - `s3:AbortMultipartUpload`
   >
   > 또한 이 역할은 `storagegateway.amazonaws.com` 서비스가 `sts:AssumeRole` 작업을 사용하여 역할을 수임하도록 허용해야 합니다.

6. 보고서 필터의 경우 다음 중 하나를 수행하여 캐시 보고서에 포함할 파일을 결정합니다.

- 현재 Amazon S3에 업로드에 실패한 캐시된 모든 파일을 포함하려면 업로드에 실패한 모든 파일을 선택합니다.
- 특정 이유로 Amazon S3에 업로드하지 못한 파일만 포함하려면 특정 업로드 실패 이유만을 선택합니다. 그런 다음 실패의 이유로 다음 이유 중 하나 이상을 선택합니다.
  - 액세스할 수 없는 스토리지 클래스 - 게이트웨이에서 객체가 저장된 Amazon S3 스토리지 클래스에 액세스할 수 없습니다. 자세한 내용은 오류: InaccessibleStorageClass를 참조하세요.
  - 잘못된 객체 상태 - 게이트웨이의 파일 상태가 Amazon S3의 파일 상태와 일치하지 않습니다. 자세한 내용은 오류: InvalidObjectState를 참조하세요.
  - 객체 누락 - 객체가 Amazon S3에서 삭제 또는 이동되었습니다. 자세한 내용은 오류: ObjectMissing을 참조하세요.
  - S3 액세스 거부 - Amazon S3 버킷 액세스 IAM 역할이 게이트웨이가 업로드 작업을 수행하는 것을 허용하지 않습니다. 자세한 내용은 오류: S3AccessDenied를 참조하세요.

> **Note**
>
> 파일 업로드 실패 플래그는 24시간마다 그리고 게이트웨이 재부팅 중에 재설정됩니다. 이 보고서가 재설정 후 다시 플래그가 지정되기 전에 파일을 캡처하는 경우 해당 파일은 파일 업로드 실패로 보고되지 않습니다.

7. VPC 엔드포인트를 사용하여 S3에 연결?에서 다음 중 하나를 수행하여 게이트웨이가 Amazon S3 버킷에 연결하는 방법을 지정합니다.

   - Amazon VPC를 사용하지 않고 직접 연결하려면 버킷에 직접 연결을 선택합니다.
   - 기존 Amazon VPC 엔드포인트 목록을 찾아보려면 VPC 엔드포인트 선택을 선택한 다음 나타나는 VPC 엔드포인트 드롭다운 목록에서 엔드포인트를 지정합니다.
   - DNS 이름으로 기존 Amazon VPC 엔드포인트를 지정하려면 VPC 엔드포인트 DNS 이름 입력을 선택한 다음 나타나는 VPC 엔드포인트 DNS 이름 필드에 DNS 이름을 입력합니다.

   > **Note**
   >
   > 파일 공유가 VPC 엔드포인트를 사용하여 정상적인 작업을 위해 Amazon S3에 연결하는 경우 캐시 보고서를 구성할 때 동일한 VPC를 사용하는 것이 좋습니다. 게이트웨이가 잘못된 VPC 구성을 포함하여 어떤 이유로든 Amazon S3 버킷에 연결할 수 없는 경우 캐시 보고서 생성이 실패합니다.

8. (선택 사항) 태그 - 선택 사항에서 새 태그 추가를 선택한 다음 캐시 보고서에 대한 키와 값을 입력합니다.

   태그는 Storage Gateway 리소스를 분류하는 데 도움이 되는 대/소문자를 구분하는 키-값 페어입니다. 태그를 추가하면 캐시 보고서를 더 쉽게 필터링하고 검색할 수 있습니다. 이 단계를 반복하여 최대 50개의 태그를 추가할 수 있습니다.

9. 마친 후에는 보고서 생성을 선택합니다.

   Storage Gateway가 보고서 생성을 시작합니다. 파일 공유에 대한 세부 정보 페이지의 캐시 보고서 탭에서 진행 상황을 확인하고 상태를 볼 수 있습니다.

S3 File Gateway에 대한 캐시 보고서 보기 및 관리

캐시 보고서는 지정한 필터 및 기준에 따라 특정 파일 공유에 대해 현재 로컬 캐시에 있는 파일을 나열합니다. API AWS Storage Gateway 또는 Storage Gateway 콘솔을 사용하여 특정 파일 공유에 대한 기존 캐시 보고서 목록을 보고, 보고서 진행 상황 및 상태를 확인하고, 더 이상 필요하지 않은 보고서를 삭제할 수 있습니다.

API를 사용하여 캐시 보고서를 관리하려면 Storage Gateway API 참조의 다음 섹션을 참조하세요.

- ListCacheReports
- DescribeCacheReport
- CancelCacheReport
- DeleteCacheReport

Storage Gateway 콘솔에서 캐시 보고서를 관리하려면 다음 절차를 사용합니다.

Storage Gateway 콘솔을 사용하여 캐시 보고서를 관리하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home/)을 엽니다.
2. 페이지 왼쪽의 탐색 창에서 파일 공유를 선택한 다음 캐시 보고서를 관리할 파일 공유를 선택합니다.
3. 파일 공유의 세부 정보 페이지에서 캐시 보고서 탭을 선택합니다. 이 탭은 파일 공유에 대한 기존 캐시 보고서를 나열하고 보고서 파일이 Amazon S3에 저장되는 상태, 진행 상황 및 객체 경로에 대한 정보를 제공합니다.
4. 다음 중 하나를 수행하세요.

- 보고서 ARN 및 관련 태그와 같은 특정 보고서에 대한 추가 세부 정보를 보려면 보고서 ID 열에서 보고서를 선택합니다.
- 동시에 관리할 여러 보고서를 지정하려면 확인란 열을 사용하여 보고서를 선택합니다.

5. 하나 이상의 보고서를 관리하려면 작업 드롭다운 메뉴에서 다음 중 하나를 선택합니다.

- 캐시 보고서 삭제 - Storage Gateway 데이터베이스에서 캐시 보고서의 레코드를 삭제합니다. 더 이상 사용되지 않는 캐시 보고서의 레코드를 삭제하여 새 보고서를 위한 공간을 확보합니다. 각 파일 공유에는 언제든지 최대 10개의 기존 캐시 보고서가 있을 수 있습니다.

> **Note**
>
> 이 절차를 사용하여 캐시 보고서 레코드를 삭제해도 Amazon S3에서 보고서 파일 객체는 삭제되지 않습니다.

- 보고서 취소 - 현재 진행 중인 보고서를 취소합니다. 보고서 구성 중에 실수를 했거나 보고서를 완료하는 데 비정상적으로 오랜 시간이 걸리는 경우 진행 중인 보고서를 취소합니다. 메시지가 표시되면 취소를 확인합니다.

> **Note**
>
> 완료 시간은 캐시의 파일 수에 따라 크게 달라질 수 있습니다. 일반적으로 대부분의 보고서는 5분 이내에 완료됩니다.

Storage Gateway 콘솔에 취소 또는 삭제 작업의 결과를 나타내는 메시지가 표시됩니다.

S3 File Gateway 캐시 보고서에 제공된 정보 이해

캐시 보고서는 지정한 필터 및 기준에 따라 특정 파일 공유에 대해 현재 로컬 캐시에 있는 파일을 나열합니다. 각 캐시 보고서에는 다음 정보가 포함됩니다.

- 버킷 - 파일 공유와 연결된 Amazon S3 버킷 또는 액세스 포인트입니다.
- S3ObjectKey -이 파일의 데이터 및 메타데이터를 저장하는 Amazon S3 객체입니다. 이 객체에는 S3에 업로드된 최신 데이터가 있지만 S3에 업로드하지 못하는 데이터가 누락되었을 수 있습니다.
- FilePath - 게이트웨이 캐시의 파일 항목에 대한 파일 경로입니다. 여기에서 파일 공유를 탑재하고 탐색할 때 파일을 찾을 수 있습니다.

- RenamedTo - 이름이 변경된 파일의 새 경로입니다. 파일 공유에서 파일의 이름을 바꿀 때 게이트웨이는 파일의 이전 위치와 새 위치를 모두 추적해야 합니다. 이 필드는 파일이 이동된 위치를 표시하므로 파일 이름이 여러 번 바뀌더라도 파일 이름 바꾸기 작업을 추적할 수 있습니다. 이 정보는 파일 공유의 파일이 Amazon S3 버킷의 객체와 어떻게 일치하는지 이해해야 할 때 특히 유용합니다.

  다음 예제는 File Gateway를 통해 이름이 변경되는 동시에 Amazon S3에서 직접 덮어쓰는 파일과 관련된 복잡한 시나리오의 캐시 보고서 항목을 보여줍니다. 이 시나리오에서 게이트웨이는 `A.txt` 파일을 S3에 업로드한 다음 파일 콘텐츠를 제거하여 로컬 캐시에 공간을 만듭니다. 그런 다음 연결된 S3 객체를 게이트웨이가 수행한 작업이 아닌 S3에서 직접 덮어쓰게 되며, 이로 인해 S3 객체와 게이트웨이가 예상하는 것 간의 불일치로 인해 `InvalidObjectState`가 발생합니다. 동시에 게이트웨이를 통해 `A.txt` 파일의 이름이 `B.txt`로 변경되었습니다.

버킷	S3Obje ey	FilePat	Renam	Type	IsDirt	IsDataI ty	IsDelet	IsFailin ToUplc	Upload or	SizeInE es	IsWholeFi leInCache
sample ket-iad	A.txt	/B.txt		FILE	TRUE	FALSE	FALSE	TRUE	Invalid(jectSta	4	FALSE
sample ket-iad	A.txt	/A.txt	/B.txt	FILE	TRUE	FALSE	TRUE	FALSE		4	FALSE

- Type - 항목이 `FILE` 또는 `DIRECTORY`에 대한 항목인지 여부를 나타냅니다.
- IsDirty - Amazon S3에 업로드되지 않은 파일에 변경 유형이 있는 경우 `TRUE`를 보고합니다. 여기에는 파일의 데이터가 변경되지 않은 경우에도 파일 이름 및 읽기/쓰기 권한과 같은 메타데이터에 대한 변경 사항이 포함됩니다.
- IsDataDirty - Amazon S3에 업로드되지 않은 파일 데이터에 변경 사항이 있는 경우 `TRUE`를 보고합니다.
- IsDeleted - 게이트웨이에서 파일이 삭제된 경우 `TRUE`를 보고합니다. 파일이 삭제된 것으로 표시되면 항상 더티로 표시됩니다.
- IsFailingToUpload - Amazon S3에 파일을 업로드하는 데 문제가 있는 경우 `TRUE`를 보고합니다. 이 상태는 게이트웨이가 업로드를 다시 시도하고 문제가 해결되었는지 확인할 수 있도록 24시간마다 재설정됩니다. 게이트웨이는 업로드에 실패한 파일에 대한 새 쓰기 작업을 거부합니다. 게이트웨이의 캐시에 전체 파일이 없는 경우 읽기 작업도 거부합니다.

- UploadError - 파일이 Amazon S3에 업로드되지 못하게 하는 오류입니다. 이러한 오류를 해결하기 위한 자세한 내용과 권장 단계는 문제 해결: File Gateway 문제를 참조하세요.
- SizeInBytes - 파일의 총 크기입니다.
- IsWholeFileInCache - 파일의 모든 데이터가 현재 게이트웨이 캐시에 저장되어 있는 경우 TRUE를 보고합니다. 파일이 Amazon S3에 업로드되지 않는 경우 TRUE이면 게이트웨이에서 파일을 읽을 수 있습니다.

게이트웨이 유지 관리

Amazon S3 File Gateway를 유지 관리하려면 게이트웨이의 성능을 최적화하기 위한 일반적인 유지 관리를 수행해야 합니다. 이 작업은 모든 게이트웨이 유형에 공통된 것입니다.

이 섹션에는 Amazon S3 File Gateway 유지 관리와 관련된 개념과 절차를 설명하는 다음 주제가 포함되어 있습니다.

주제

- 게이트웨이 업데이트 관리 – 유지 관리 업데이트를 켜거나 끄는 방법과 File Gateway의 유지 관리 기간 일정을 수정하는 방법에 대해 알아봅니다.
- 로컬 콘솔을 사용하여 유지 관리 작업 수행 – 게이트웨이 로컬 콘솔을 사용하여 유지 관리 작업을 수행하는 방법에 대해 알아봅니다.
- 게이트웨이 VM 종료 - 하이퍼바이저에 패치를 적용할 때와 같이 유지 관리를 위해 게이트웨이 가상 머신을 종료하거나 재부팅해야 하는 경우 어떻게 해야 하는지 알아봅니다.
- 기존 S3 File Gateway를 새 인스턴스로 교체 - 성능을 개선하거나 게이트웨이 마이그레이션 알림에 응답하려는 경우 S3 File Gateway를 새 인스턴스로 교체하는 방법을 알아봅니다.
- 게이트웨이 삭제 및 연결된 리소스 제거 - AWS Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하고 연결된 리소스를 정리하여 지속적인 사용에 대한 요금이 부과되지 않도록 하는 방법을 알아봅니다.

게이트웨이 업데이트 관리

Storage Gateway는 관리형 클라우드 서비스 구성 요소와 온프레미스 또는 AWS 클라우드의 Amazon EC2 인스턴스에 배포하는 게이트웨이 어플라이언스 구성 요소로 구성됩니다. 두 구성 요소 모두 정기적으로 업데이트됩니다. 이 섹션의 주제는 이러한 업데이트의 주기, 업데이트 적용 방법 및 배포의 게이트웨이에서 업데이트 관련 설정을 구성하는 방법에 대해 설명합니다.

> **Important**
>
> Storage Gateway 어플라이언스는 관리형 가상 머신으로 취급해야 하며, 어떤 방식으로든 설치 또는 내용에 액세스하거나 수정하려고 시도해서는 안됩니다. 일반 AWS 게이트웨이 업데이트 메커니즘(예: SSM 또는 하이퍼바이저 도구) 이외의 방법을 사용하여 소프트웨어 패키지를 설치하거나 업데이트하려고 하면 게이트웨이가 오작동할 수 있습니다.

Storage Gateway는 보안 및 안정성을 유지하기 위해 어플라이언스를 자동으로 정기적으로 패치합니다. Storage Gateway 어플라이언스는 Amazon Linux를 기본 운영 체제로 사용합니다. Amazon Linux 보안 센터에서 탐지된 일반적인 취약성 및 노출(CVE) 문제의 상태를 확인할 수 있습니다. CVE 패치는 Amazon Linux 보안 센터에 표시된 대로 릴리스 후 30일 이내에 자동으로 적용됩니다. 게이트웨이가 온라인 상태인 경우 게이트웨이 유지 관리 일정 중에 패치가 설치됩니다.

Storage Gateway는 cloud-init 명령을 사용하여 Amazon EC2 게이트웨이를 수동으로 업데이트하는 기능을 지원하지 않습니다. 이 방법을 사용하여 게이트웨이를 업데이트하는 경우 게이트웨이 어플라이언스를 활성화하거나 사용하지 못하게 하는 상호 운용성 문제가 발생할 수 있습니다.

업데이트 빈도 및 예상 동작

AWS 는 배포된 게이트웨이를 중단하지 않고 필요에 따라 클라우드 서비스 구성 요소를 업데이트합니다. 배포된 게이트웨이 어플라이언스는 다음과 같은 유형의 업데이트를 받습니다.

- 유지 관리 - 정기적인 업데이트에는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안 문제를 해결하기 위한 수정 사항, 새로운 기능에 대한 액세스가 포함될 수 있습니다.
- 긴급 - 게이트웨이의 보안, 성능 또는 내구성에 즉시 영향을 미치는 문제에 필요한 수정 사항이 포함된 중요 업데이트입니다. 긴급 업데이트는 월간 유지 관리 및 기능 업데이트의 일반적인 주기 외에 언제든지 릴리스할 수 있습니다.

모든 업데이트는 누적되며 적용 시 게이트웨이를 현재 버전으로 업그레이드합니다. 각 업데이트에 포함된 특정 변경 사항에 대한 자세한 내용은 게이트웨이 어플라이언스 소프트웨어 릴리스 정보를 참조하세요.

모든 게이트웨이 어플라이언스 업데이트로 인해 서비스가 잠시 중단될 수 있습니다. 업데이트 중에 게이트웨이의 VM 호스트는 재부팅할 필요가 없지만 게이트웨이 어플라이언스가 업데이트되고 다시 시작되는 잠시 동안 게이트웨이를 사용할 수 없게 됩니다.

게이트웨이를 배포하고 활성화하면 기본 유지 관리 기간 일정이 설정됩니다. 유지 관리 기간 일정은 언제든지 수정할 수 있습니다. 유지 관리 업데이트를 끌 수도 있지만 켜두는 것이 좋습니다.

> **Note**
>
> 정기 유지 관리 업데이트가 꺼져 있더라도 유지 관리 기간 일정에 따라 긴급 업데이트가 적용됩니다.

게이트웨이에 업데이트가 적용되기 전에는 Storage Gateway 콘솔 및에 대한 메시지를 AWS 알려줍니다 AWS Health Dashboard. 자세한 내용은 AWS Health Dashboard 단원을 참조하십시오. 소프트웨어 업데이트 알림이 전송되는 이메일 주소를 수정하려면 AWS 계정 관리 참조 안내서의 AWS 계정의 대체 연락처 업데이트를 참조하세요.

업데이트가 제공되면 게이트웨이 세부 정보 탭에 유지 관리 메시지가 표시됩니다. 세부 정보 탭에서 성공적으로 업데이트가 적용된 최근 날짜와 시간도 확인할 수 있습니다.

유지 관리 업데이트 켜기 또는 끄기

유지 관리 업데이트가 켜져 있는 경우 구성된 유지 관리 기간 일정에 따라 게이트웨이에서 이러한 업데이트를 자동으로 적용합니다. 자세한 내용은 게이트웨이 유지 관리 기간 일정 수정을 참조하세요.

유지 관리 업데이트가 꺼져 있는 경우 게이트웨이에서 이러한 업데이트가 자동으로 적용되지는 않지만 언제든지 Storage Gateway 콘솔, API 또는 CLI를 사용하여 수동으로 적용할 수 있습니다. 긴급 업데이트는 이 설정과 관계없이 구성된 유지 관리 기간 동안 적용될 수 있습니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 게이트웨이 업데이트를 켜거나 끄는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조에서 UpdateMaintenanceStartTime을 참조하세요.

Storage Gateway 콘솔을 사용하여 유지 관리 업데이트를 켜거나 끄려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 업데이트에서 켜기 또는 끄기를 선택합니다.
5. 완료되었으면 변경 사항 저장을 선택합니다.

업데이트된 설정은 Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭에서 확인할 수 있습니다.

게이트웨이 유지 관리 기간 일정 수정

유지 관리 업데이트가 켜져 있는 경우 유지 관리 기간 일정에 따라 게이트웨이에서 이러한 업데이트를 자동으로 적용합니다. 긴급 업데이트는 유지 관리 업데이트 설정과 관계없이 구성된 유지 관리 기간 동안 적용될 수 있습니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조에서 UpdateMaintenanceStartTime을 참조하세요.

Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 기간 시작 시간에서 다음을 수행합니다.

    a. 일정에서 주별 또는 월별을 선택하여 유지 관리 기간 주기를 설정합니다.

    b. 주별을 선택한 경우, 요일 및 시간 값을 수정하여 유지 관리 기간이 시작될 각 주의 특정 시점을 설정합니다.

    월별을 선택한 경우, 날짜 및 시간 값을 수정하여 유지 관리 기간이 시작될 각 월의 특정 시점을 설정합니다.

    > **Note**
    >
    > 월의 날짜에 설정할 수 있는 최대값은 28입니다. 유지 관리 시작일을 29일~31일로 설정할 수 없습니다.
    > 이 설정을 구성하는 동안 오류가 발생한다면 게이트웨이 소프트웨어가 최신 버전이 아닐 수 있습니다. 게이트웨이를 수동으로 먼저 업데이트한 다음 유지 관리 기간 일정을 다시 구성해 보세요.

5. 완료되었으면 변경 사항 저장을 선택합니다.

업데이트된 설정은 Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭에서 확인할 수 있습니다.

수동으로 업데이트 적용

게이트웨이에 대한 소프트웨어 업데이트를 사용할 수 있는 경우 아래 절차에 따라 수동으로 적용할 수 있습니다. 이 수동 업데이트 프로세스는 유지 관리 기간 일정을 무시하고 유지 관리 업데이트가 꺼져 있더라도 즉시 업데이트를 적용합니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 업데이트를 수동으로 적용하는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 작업을 수행하려면 Storage Gateway API 참조에서 UpdateGatewaySoftwareNow를 참조하세요.

Storage Gateway 콘솔을 사용하여 게이트웨이 소프트웨어 업데이트를 수동으로 적용하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 업데이트할 게이트웨이를 선택합니다.

   업데이트를 사용할 수 있는 경우 콘솔의 게이트웨이 세부 정보 탭에 파란색 알림 배너가 표시되며, 여기에는 업데이트를 적용할 수 있는 옵션이 포함되어 있습니다.
3. 지금 업데이트 적용을 선택하여 게이트웨이를 즉시 업데이트합니다.

   > **Note**
   >
   > 이 작업을 수행하면 업데이트가 설치되는 동안 게이트웨이 기능이 일시적으로 중단됩니다. 이 시간 동안 게이트웨이 상태는 Storage Gateway 콘솔에 오프라인으로 표시됩니다. 업데이트 설치가 완료되면 게이트웨이가 정상 작동을 재개하고 상태가 실행 중으로 변경됩니다.

Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭을 확인하여 게이트웨이 소프트웨어가 최신 버전으로 업데이트되었는지 확인할 수 있습니다.

로컬 콘솔을 사용하여 유지 관리 작업 수행

이 섹션은 다음 주제로 구성되어 있으며, 게이트웨이 어플라이언스 로컬 콘솔을 사용하여 유지 관리 작업을 수행하는 방법에 대한 정보를 제공합니다. 게이트웨이 어플라이언스를 호스팅하는 온프레미스 가상 머신 또는 Amazon EC2 인스턴스를 통해 로컬 콘솔에 액세스하여 이러한 작업을 수행할 수 있습니다. 대부분의 작업은 여러 호스트 플랫폼에서 공통적으로 적용되지만 몇 가지 차이점도 있습니다.

주제

- 게이트웨이 로컬 콘솔 액세스 - Linux 커널 기반 가상 머신(KVM), VMware ESXi 또는 Microsoft Hyper-V Manager 플랫폼에서 호스팅되는 온프레미스 게이트웨이의 로컬 콘솔에 로그인하는 방법에 대해 알아봅니다.
- 가상 머신 로컬 콘솔에서 작업 수행 - 로컬 콘솔을 사용하여 HTTP 프록시 구성, 시스템 리소스 상태 보기, 터미널 명령 실행 등 온프레미스 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법에 대해 알아봅니다.
- Amazon EC2 게이트웨이 로컬 콘솔에서 작업 수행 - 로컬 콘솔에 로그인하여 HTTP 프록시 구성, 시스템 리소스 상태 보기, 터미널 명령 실행 등 Amazon EC2 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법에 대해 알아봅니다.

게이트웨이 로컬 콘솔 액세스

VM 로컬 콘솔에 액세스하는 방법은 게이트웨이 VM이 배포된 하이퍼바이저 종류에 따라 달라집니다. 이 섹션에서는 Linux 커널 기반 가상 머신(KVM), VMware ESXi 및 Microsoft Hyper-V Manager를 사용하여 VM 로컬 콘솔에 액세스하는 방법에 대한 정보를 찾을 수 있습니다.

주제

- Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스
- VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스
- Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스

사용 중인 Linux 배포판에 따라 KVM에서 실행되는 가상 머신을 구성하는 방법에는 여러 가지가 있습니다. 명령줄에서 KVM 구성 옵션에 액세스하는 지침은 다음과 같습니다. 지침은 KVM 구현에 따라 다를 수 있습니다.

KVM을 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

1. 다음 명령을 사용하여 현재 KVM에서 사용할 수 있는 VM을 나열합니다.

   ```
   # virsh list
   ```

   이 명령은 각각에 대한 Id, 이름 및 상태 정보가 포함된 VM 목록을 반환합니다. 게이트웨이 로컬 콘솔을 시작하려는 VM의 `Id`는 기록해 둡니다.

2. 로컬 콘솔에 액세스하려면 다음 명령을 사용합니다.

   ```
   # virsh console Id
   ```

   *Id*를 이전 단계에서 기록한 VM의 Id로 바꿉니다.

   AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

3. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 File Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스

VMware ESXi를 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

1. VMware vSphere 클라이언트에서 해당되는 게이트웨이 VM을 선택합니다.
2. 게이트웨이 VM이 켜져 있는지 확인합니다.

   > **Note**
   >
   > 게이트웨이 VM이 켜져 있으면 애플리케이션 창의 왼쪽에 있는 VM 브라우저 패널에 VM 아이콘과 함께 녹색 화살표 아이콘이 나타납니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창 상단의 도구 모음에서 녹색 전원 켜기 아이콘을 선택하여 켤 수 있습니다.

3. 애플리케이션 창의 오른쪽에 있는 기본 정보 패널에서 콘솔 탭을 선택합니다.

   잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

   > **Note**
   >
   > 콘솔 창에서 커서를 릴리스하려면 Ctrl+Alt를 누릅니다.

4. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 File Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

게이트웨이의 로컬 콘솔에 액세스하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager 애플리케이션 창의 왼쪽에 있는 가상 머신 패널에서 게이트웨이 어플라이언스 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인하세요.

   > **Note**
   >
   > 게이트웨이 VM이 켜져 있는 경우 애플리케이션 창의 왼쪽에 있는 가상 머신 패널의 VM 상태 열에 `Running`이 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창의 오른쪽에 있는 작업 패널에서 시작을 선택하여 켤 수 있습니다.

3. 작업 패널에서 연결을 선택합니다.

   그러면 Virtual Machine Connection(가상 머신 연결) 창이 표시됩니다. 인증 창이 표시되면 하이퍼바이저 관리자가 제공한 로그인 자격 증명을 입력합니다.

   잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

4. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 File Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

가상 머신 로컬 콘솔에서 작업 수행

온프레미스에서 배포한 File Gateway의 경우, VM 호스트의 로컬 콘솔을 사용하여 다음과 같은 유지 관리 작업을 할 수 있습니다. 이러한 작업은 VMware, Microsoft Hyper-V 및 Linux 커널 기반 가상 머신 (KVM) 하이퍼바이저에 공통적으로 적용됩니다.

주제

- File Gateway 로컬 콘솔에 로그인 - 게이트웨이 네트워크 설정을 구성하고 기본 암호를 변경할 수 있는 로컬 콘솔에 로그인하는 방법에 대해 알아봅니다.
- HTTP 프록시 구성 - 프록시 서버를 통해 모든 AWS 엔드포인트 트래픽을 라우팅하도록 Storage Gateway를 구성하는 방법을 알아봅니다.
- 게이트웨이 네트워크 설정 구성 - DHCP 또는 정적 IP 주소를 사용하도록 게이트웨이를 구성하는 방법에 대해 알아봅니다.
- 게이트웨이 네트워크 연결 테스트 - 게이트웨이 로컬 콘솔을 사용하여 네트워크 연결을 테스트하는 방법에 대해 알아봅니다.
- 게이트웨이 시스템 리소스 상태 조회 - 게이트웨이의 가상 CPU 코어, 루트 볼륨 크기 및 RAM을 확인하는 방법에 대해 알아봅니다.
- 게이트웨이의 네트워크 시간 프로토콜(NTP) 서버 구성 - 네트워크 시간 프로토콜(NTP) 서버 구성을 보고 편집하며, 게이트웨이와 하이퍼바이저 호스트의 시간을 동기화하는 방법에 대해 알아봅니다.
- 로컬 콘솔에서 Storage Gateway 명령 실행 - 로컬 콘솔 명령을 실행하여 라우팅 테이블 저장, 연결 등과 같은 작업을 수행하는 방법을 알아봅니다 지원.

File Gateway 로컬 콘솔에 로그인

VM이 로그인할 준비가 되면 로그인 화면이 표시됩니다. VM 로컬 콘솔에 처음 로그인하는 경우 임시 로그인 자격 증명을 사용하여 로그인합니다. 이러한 임시 자격 증명을 통해 로컬 콘솔에서 게이트웨이 네트워크 설정을 구성하고 암호를 변경할 수 있는 메뉴에 액세스할 수 있습니다. 초기 사용자 이름은 `admin`이고, 임시 암호는 `password`입니다. 처음 로그인할 때 암호를 변경해야 합니다.

임시 암호를 변경하려면

1. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 게이트웨이 콘솔에 해당하는 숫자를 입력합니다.
2. `passwd` 명령을 실행합니다. 명령을 실행하는 방법에 대한 정보는 로컬 콘솔에서 Storage Gateway 명령 실행 섹션을 참조하세요.

Storage Gateway 콘솔에서 로컬 콘솔 암호 설정

Storage Gateway 웹 기반 콘솔에서 로컬 콘솔의 암호를 관리할 수도 있습니다. 웹 기반 콘솔로 암호가 성공적으로 업데이트되면 로컬로 로그인한 적이 없는 경우 임시 암호를 포함하여 게이트웨이 VM의 로컬 콘솔에서 사용하는 암호가 재정의됩니다. 현재 네트워크를 통해 게이트웨이에 연결할 수 없는 경우 암호 업데이트 프로세스가 실패합니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호를 설정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 새 암호를 설정할 게이트웨이를 선택합니다.
3. 작업에서 Set Local Console Password(로컬 콘솔 암호 설정)을 선택합니다.
4. Set Local Console Password(로컬 콘솔 암호 설정) 대화 상자에 새 암호를 입력해 확인한 후 저장을 선택합니다.

   새 암호가 현재 암호를 대체합니다. Storage Gateway 서비스는 암호를 저장, 저장 또는 기록하지 않고 암호화된 채널을 통해 VM으로 안전하게 전송합니다. 이 암호는 안전하게 저장됩니다.

   > **Note**
   >
   > 암호는 키보드에 있는 어떤 문자로도 구성할 수 있으며, 1–512개의 문자까지 가능합니다.

HTTP 프록시 구성

File Gateway는 HTTP 프록시 구성을 지원합니다.

> **Note**
>
> File Gateway는 HTTP 프록시 구성만 지원합니다.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우에는 게이트웨이에 HTTP 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 이렇게 하면 Storage Gateway가 프록시 서버를 통해 모든 AWS 엔드포인트 트래픽을 라우팅합니다. HTTP 프록시를 사용하는 경우에도 게이트웨이와 엔드포인트 간의 통신은 암호화됩니다. 게이트웨이의 네트워크 요건에 대한 정보는 네트워크 및 방화벽 요구 사항 섹션을 참조하세요.

File Gateway에 HTTP 프록시를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Linux 커널 기반 가상 머신(KVM)의 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 HTTP 프록시 구성을 선택합니다.
3. AWS 어플라이언스 활성화 HTTP 프록시 구성 메뉴에서 수행하려는 작업에 해당하는 번호를 입력합니다.

   - HTTP 프록시 구성 - 구성을 완료하려면 호스트 이름과 포트를 입력해야 합니다.
   - 현재 HTTP 프록시 구성 보기 - HTTP 프록시가 구성되지 않은 경우 `HTTP Proxy not configured` 메시지가 표시됩니다. HTTP 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.
   - HTTP 프록시 구성 제거 - `HTTP Proxy Configuration Removed` 메시지가 표시됩니다.
4. VM을 다시 시작하여 HTTP 구성에 대한 설정을 적용합니다.

게이트웨이 네트워크 설정 구성

게이트웨이의 기본 네트워크 구성은 DHCP(Dynamic Host Configuration Protocol)입니다. DHCP를 통해 게이트웨이에 IP 주소가 자동으로 지정됩니다. 다음 설명과 같이 게이트웨이의 IP를 고정 IP 주소로 수동 지정해야 하는 경우가 있을 수 있습니다.

고정 IP 주소를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. 네트워크 구성 메뉴에서 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
네트워크 어댑터에 대한 정보 얻기	해당 숫자를 입력하여 어댑터 설명을 선택합니다. 어댑터 이름 목록이 나타나고 어댑터 이름을 입력하라는 메시지가 표시됩니다(예: **eth0**). 지정하려는 어댑터가 사용 중인 경우, 다음과 같은 어댑터 정보가 표시됩니다. • 미디어 액세스 제어(MAC) 주소 • IP 주소 • 넷마스크 • 게이트웨이 IP 주소 • DHCP 활성화 상태 정적 IP 주소를 구성하거나 게이트웨이의 기본 어댑터를 설정할 경우 여기에 나열된 어댑터 이름을 사용합니다.

수행할 작업	수행할 작업
DHCP 라우팅 구성	해당 숫자를 입력하여 DHCP 구성을 선택합니다. DHCP를 사용하도록 네트워크 인터페이스를 구성하라는 메시지가 표시됩니다.

수행할 작업	수행할 작업
게이트웨이에 고정 IP 주소 구성	해당 숫자를 입력하여 고정 IP 구성을 선택합니다. 다음 정보를 입력하여 고정 IP를 구성하라는 메시지가 표시됩니다. • 네트워크 어댑터 이름 • IP 주소 • 넷마스크 • 기본 게이트웨이 주소 • 기본 DNS(Domain Name Service) 주소 • 보조 DNS 주소 **Important** 게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오. 게이트웨이에서 네트워크 인터페이스를 한 개 이상 사용하는 경우, 활성화된 모든 인터페이스에서 DHCP 또는 정적 IP 주소를 사용하도록 설정해야 합니다.

수행할 작업	수행할 작업
	예를 들어 게이트웨이 VM이 DHCP로 구성된 인터페이스 두 개를 사용한다고 가정합시다. 나중에 한 인터페이스를 고정 IP로 설정하면 다른 하나는 비활성화됩니다. 이 경우 인터페이스를 활성화하려면 고정 IP로 설정해야 합니다. 처음에 두 인터페이스 모두 고정 IP 주소를 사용하도록 설정한 후 DHCP를 사용하도록 게이트웨이를 설정하면 두 인터페이스 모두 DHCP를 사용하게 됩니다.
게이트웨이의 호스트 이름 구성	해당 숫자를 입력하여 호스트 이름 구성을 선택합니다. 게이트웨이에서 지정한 정적 호스트 이름을 사용할지 아니면 DCHP 또는 rDNS를 통해 자동으로 할당할지를 선택하라는 메시지가 표시됩니다. 정적을 선택하면 같은 정적 호스트 이름(예: `testgateway.example.com`)을 제공하라는 메시지가 표시됩니다. y를 입력하여 구성을 적용합니다. **Note** 게이트웨이에 대해 정적 호스트 이름을 구성할 경우 제공된 호스트 이름이 게이트웨이가 조인된 도메인에 있는지 확인합니다. 또한 게이트웨이의 IP 주소가 정적 호스트 이름을 가리키는 A 레코드를 DNS 시스템에 생성해야 합니다.

수행할 작업	수행할 작업
게이트웨이의 호스트 이름 구성 조회	해당 숫자를 입력하여 호스트 이름 구성 보기를 선택합니다. 게이트웨이의 호스트 이름, 획득 모드, 도메인 및 Active Directory 영역이 표시됩니다.
게이트웨이의 모든 네트워크 구성을 DHCP로 재설정	해당 숫자를 입력하여 모두 DHCP로 재설정을 선택합니다. 모든 네트워크 인터페이스가 DHCP를 사용하도록 설정됩니다. **Important** 게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오.
게이트웨이의 기본 경로 어댑터 설정	해당 숫자를 입력하여 기본 어댑터 설정을 선택합니다. 게이트웨이에 사용할 수 있는 어댑터가 표시되고 어댑터 중 하나를 선택하라는 메시지가 표시됩니다(예: **`eth0`**).

수행할 작업	수행할 작업
게이트웨이 DSN 구성 편집	해당 숫자를 입력하여 DNS 구성 편집을 선택합니다. 주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. 새 IP 주소를 제공하라는 메시지가 나타납니다.
게이트웨이의 DNS 구성 조회	해당 숫자를 입력하여 DNS 구성 보기를 선택합니다. 주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. **Note** 일부 VMware 하이퍼바이저 버전은 이 메뉴에서 어댑터 구성을 편집할 수 있습니다.
라우팅 테이블 조회	해당 숫자를 입력하여 경로 보기를 선택합니다. 게이트웨이의 기본 경로가 표시됩니다.

게이트웨이 네트워크 연결 테스트

게이트웨이의 로컬 콘솔을 사용하여 네트워크 연결을 테스트할 수 있습니다. 이 테스트는 게이트웨이의 네트워크 문제를 해결할 때 유용합니다.

게이트웨이 네트워크 연결 테스트

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 연결 테스트를 선택합니다.

   게이트웨이가 이미 활성화된 경우 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 다음 단계에 설명된 AWS 리전 대로 엔드포인트 유형 및를 지정해야 합니다.
3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. Storage Gateway에서 사용할 수 있는 지원되는 AWS 서비스 엔드포인트 AWS 리전 및 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

테스트가 진행되면 각 엔드포인트의 연결 상태가 다음과 같이 [통과] 또는 [실패]로 표시됩니다.

메시지	설명
[통과]	Storage Gateway가 네트워크에 연결되어 있습니다.
[실패]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

게이트웨이 시스템 리소스 상태 조회

게이트웨이가 시작되고, 가상 CPU 코어 루트 볼륨 크기와 RAM을 점검합니다. 이후 시스템 리소스가 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 게이트웨이의 로컬 콘솔에서 점검 결과를 볼 수 있습니다.

시스템 리소스 점검의 상태를 보려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

   각 리소스의 상태가 다음과 같이 [확인], [경고] 또는 [실패]로 표시됩니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[실패]	리소스가 최소 요구 사항을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.

   콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

게이트웨이의 네트워크 시간 프로토콜(NTP) 서버 구성

네트워크 시간 프로토콜(NTP) 서버 구성을 보고 편집할 수 있으며, 게이트웨이와 하이퍼바이저 호스트의 VM 시간을 동기화할 수 있습니다.

시스템 시간 관리

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 시간 관리를 선택합니다.
3. 시스템 시간 관리 메뉴에서 해당 숫자를 입력하여 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
VM 시간과 NTP 서버 시간을 확인해 동기화합니다.	해당 숫자를 입력하여 시스템 시간 보기 및 동기화를 선택합니다. 현재 VM 시간이 표시됩니다. File Gateway가 게이트웨이 VM과 NTP 서버 시간 차이를 결정하며, VM 시간과 NTP 시간을 동기화하라는 메시지가 표시됩니다. 게이트웨이를 배포하고 실행한 후에 게이트웨이 VM의 시간에 오차가 생기는 경우가 있을 수 있습니다. 예를 들어 네트워크 중단이 지속되어 하이퍼바이저 호스트와 게이트웨이의 시간이 업데이트되지 않았다고 가정하겠습니다. 이 경우, 게이트웨이 VM 시간이 실제 시간과 다릅니다. 시간 오차가 있는 경우, 스냅샷과 같은 작업이 실행되도록 지정한 시간과 작업이 실제 이루어지는 시간 사이에 불일치가 발생합니다. VMware ESXi에 배포한 게이트웨이의 경우, 하이퍼바이저 호스트 시간을 설정하고 호스트에 VM 시간을 동기화하는 것만으로도 시간 오차를 방지하는 데 충분합니다. 자세한 내용은 VM 시

수행할 작업	수행할 작업
	간을 VMware 호스트 시간과 동기화 단원을 참조하십시오. Microsoft Hyper-V에 배포한 게이트웨이의 경우, VM의 시간을 주기적으로 점검해야 합니다. 자세한 내용은 Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화 단원을 참조하십시오. KVM에 배포된 게이트웨이의 경우 KVM용 `virsh` 명령줄 인터페이스를 사용하여 VM 시간을 확인하고 동기화할 수 있습니다.
NTP 서버 구성 편집	해당 숫자를 입력하여 NTP 구성 편집을 선택합니다. 선호하는 NTP 서버와 부 NTP 서버를 제공하라는 메시지가 표시됩니다.
NTP 서버 구성 보기	해당 숫자를 입력하여 NTP 구성 보기를 선택합니다. NTP 서버 구성이 표시됩니다.

로컬 콘솔에서 Storage Gateway 명령 실행

Storage Gateway의 VM 로컬 콘솔은 게이트웨이 관련 문제를 구성 및 진단할 수 있는 안전한 환경을 제공합니다. 로컬 콘솔 명령을 사용하여 라우팅 테이블 저장, 연결 등과 같은 유지 관리 작업을 수행할 수 있습니다 지원.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 **h**를 입력합니다.

   그러면 사용 가능한 명령이 나열된 사용 가능한 명령 메뉴가 콘솔에 표시됩니다.

명령	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 설정 구성을 참조하세요.
ip	라우팅, 디바이스 및 터널을 표시/조작합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다.

명령	함수
	지침은 게이트웨이 네트워크 설정 구성을 참조하세요.
iptables	IPv4 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ip6tables	IPv6 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결합니다. AWS 지원 액세스를 켜는 방법에 대한 지침은 EC2 게이트웨이 문제 해결에 도움이 되는 AWS 지원 요청 EC.
passwd	인증 토큰을 업데이트합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
tcptraceroute	대상으로 향하는 TCP 트래픽의 경로 추적 출력을 수집합니다.

명령	함수
sslcheck	인증서 발급자와 함께 출력을 반환합니다. **Note** Storage Gateway는 인증서 발급자 확인을 사용하며 SSL 검사는 지원하지 않습니다. 이 명령이 aws-appliance@amazon.com 이외의 발급자를 반환한다면 애플리케이션에서 SSL 검사를 수행 중일 가능성이 높습니다. 이 경우 Storage Gateway 어플라이언스에 대한 SSL 검사를 우회하는 것이 좋습니다.

4. 게이트웨이 콘솔 명령 프롬프트에서 사용하려는 기능에 해당하는 명령을 입력하고 지침을 따릅니다.

명령에 대해 알아보려면 명령 프롬프트에 **man** + *## ##*을 입력합니다.

Amazon EC2 게이트웨이 로컬 콘솔에서 작업 수행

일부 유지 관리 작업의 경우, Amazon EC2 인스턴스에 배포한 게이트웨이를 실행하려면 로컬 콘솔에 로그인해야 합니다. 이 섹션에서는 로컬 콘솔에 로그인하고 유지 관리 작업을 수행하는 방법에 대해 설명합니다.

주제

- Amazon EC2 게이트웨이 로컬 콘솔에 로그인 - Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스의 게이트웨이 로컬 콘솔에 연결하고 로그인하는 방법에 대해 알아봅니다.
- HTTP 프록시를 통해 Amazon EC2에 배포된 게이트웨이 라우팅 - AWS 와 Amazon EC2 인스턴스에 배포된 게이트웨이 간에 소켓 보안 버전 5(SOCKS5) 프록시를 구성하는 방법을 알아봅니다.
- 게이트웨이 네트워크 연결 테스트 - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이와 다양한 네트워크 리소스 간의 네트워크 연결을 테스트하는 방법에 대해 알아봅니다.
- 게이트웨이 시스템 리소스 상태 조회 - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이의 가상 CPU 코어, 루트 볼륨 크기 및 RAM을 확인하는 방법에 대해 알아봅니다.

- Amazon EC2 게이트웨이의 로컬 콘솔에서 Storage Gateway 명령 실행 - 라우팅 테이블 저장, 지원에 연결 등과 같은 추가 작업을 수행할 수 있는 로컬 콘솔 명령을 실행하는 방법에 대해 알아봅니다.
- Amazon EC2 게이트웨이 네트워크 설정 구성 - 로컬 콘솔을 사용하여 Amazon EC2 인스턴스의 게이트웨이에 대한 DNS 및 호스트 이름과 같은 네트워크 설정을 보고 구성하는 방법에 대해 알아봅니다.

Amazon EC2 게이트웨이 로컬 콘솔에 로그인

Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스에서 게이트웨이 로컬 콘솔에 로그인할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서에서 인스턴스에 연결을 참조하세요. 이런 방식으로 연결하려면 인스턴스를 시작할 때 지정한 SSH 키 페어가 필요합니다. Amazon EC2 키 페어에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon EC2 키 페어를 참조하세요.

게이트웨이 로컬 콘솔에 로그인하려면

1. SSH를 사용하여 Amazon EC2 인스턴스에 연결하고 관리자로 로그인합니다.
2. 로그인하면 다양한 작업을 수행할 수 있는 AWS 어플라이언스 활성화 - 구성 기본 메뉴가 나타납니다.

관련 작업	이 주제를 참조하세요.
게이트웨이에 HPPT 프록시를 구성	HTTP 프록시를 통해 Amazon EC2에 배포된 게이트웨이 라우팅
게이트웨이 네트워크 설정 구성	Amazon EC2 게이트웨이 네트워크 설정 구성
네트워크 연결 테스트	게이트웨이 네트워크 연결 테스트
시스템 리소스 점검 조회	게이트웨이 시스템 리소스 상태 조회.
Storage Gateway 콘솔 명령 실행	Amazon EC2 게이트웨이의 로컬 콘솔에서 Storage Gateway 명령 실행

게이트웨이를 종료하려면 **0**을 입력합니다.

구성 세션을 종료하려면 **X**을 입력합니다.

HTTP 프록시를 통해 Amazon EC2에 배포된 게이트웨이 라우팅

Storage Gateway는 Amazon EC2 및 AWS에 배포된 게이트웨이 간 Socket Secure 버전 5(SOCKS5) 프록시 구성을 지원합니다.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우에는 게이트웨이에 HTTP 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 이렇게 하면 Storage Gateway가 프록시 서버를 통해 모든 AWS 엔드포인트 트래픽을 라우팅합니다. HTTP 프록시를 사용하는 경우에도 게이트웨이와 엔드포인트 간의 통신은 암호화됩니다.

로컬 프록시 서버를 통해 게이트웨이 인터넷 트래픽을 라우팅하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 HTTP 프록시 구성을 선택합니다.
3. AWS 어플라이언스 활성화 HTTP 프록시 구성 메뉴에서 수행하려는 작업에 해당하는 번호를 입력합니다.

   - HTTP 프록시 구성 - 구성을 완료하려면 호스트 이름과 포트를 입력해야 합니다.
   - 현재 HTTP 프록시 구성 보기 - HTTP 프록시가 구성되지 않은 경우 `HTTP Proxy not configured` 메시지가 표시됩니다. HTTP 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.
   - HTTP 프록시 구성 제거 - `HTTP Proxy Configuration Removed` 메시지가 표시됩니다.

게이트웨이 네트워크 연결 테스트

게이트웨이의 로컬 콘솔을 사용하여 네트워크 연결을 테스트할 수 있습니다. 이 테스트는 게이트웨이의 네트워크 문제를 해결할 때 유용합니다.

게이트웨이 연결을 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 연결 테스트를 선택합니다.

게이트웨이가 이미 활성화된 경우 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 다음 단계에 설명된 AWS 리전 대로 엔드포인트 유형 및를 지정해야 합니다.

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. Storage Gateway와 함께 사용할 수 있는 지원되는 AWS 서비스 엔드포인트 및 AWS 리전 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

테스트가 진행되면 각 엔드포인트의 연결 상태가 다음과 같이 [통과] 또는 [실패]로 표시됩니다.

메시지	설명
[통과]	Storage Gateway가 네트워크에 연결되어 있습니다.
[실패]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

게이트웨이 시스템 리소스 상태 조회

File Gateway가 시작되고, 가상 CPU 코어, 루트 볼륨 크기와 RAM을 점검합니다. 이후 사용 가능한 시스템 리소스가 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 게이트웨이 로컬 콘솔을 사용하여 시스템 리소스 검사 결과를 볼 수 있습니다.

시스템 리소스 점검의 상태를 보려면

1. Amazon EC2 File Gateway 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

   게이트웨이 로컬 콘솔에 다음과 같이 리소스의 상태를 나타내는 [OK], [WARNING] 또는 [FAIL]이 표시됩니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. 게이트웨이에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[실패]	리소스가 최소 요건을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. 게이트웨이에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.

로컬 콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

Amazon EC2 게이트웨이의 로컬 콘솔에서 Storage Gateway 명령 실행

AWS Storage Gateway 콘솔은 게이트웨이 문제를 구성하고 진단하기 위한 안전한 환경을 제공하는 데 도움이 됩니다. 콘솔 명령을 사용하여 라우팅 테이블 저장 또는 연결과 같은 유지 관리 작업을 수행할 수 있습니다 지원.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 **h**를 입력합니다.

   그러면 사용 가능한 명령이 나열된 사용 가능한 명령 메뉴가 콘솔에 표시됩니다.

명령	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 설정 구성을 참조하세요.
ip	라우팅, 디바이스 및 터널을 표시/조작합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 설정 구성을 참조하세요.
iptables	IPv4 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ip6tables	IPv6 패킷 필터링 및 NAT를 위한 관리 도구입니다.

명령	함수
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
tcptraceroute	대상으로 향하는 TCP 트래픽의 경로 추적 출력을 수집합니다.

4. 게이트웨이 콘솔 명령 프롬프트에서 사용하려는 기능에 해당하는 명령을 입력하고 지침을 따릅니다.

명령에 대해 알아보려면 명령 프롬프트에 **man** + ## ##을 입력합니다.

Amazon EC2 게이트웨이 네트워크 설정 구성

게이트웨이 로컬 콘솔을 사용하여 Amazon EC2 File Gateway의 네트워크 설정을 보고 구성할 수 있습니다.

네트워크 설정을 구성하려면

1. Amazon EC2 File Gateway 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. AWS 어플라이언스 활성화 - 네트워크 구성 메뉴에서 수행하려는 작업에 해당하는 번호를 입력합니다.

   - DNS 구성 편집 - 게이트웨이 로컬 콘솔에 기본 및 보조 DNS 서버에 사용할 수 있는 어댑터가 표시됩니다. 그러면 콘솔에 새 IP 주소를 입력하라는 메시지가 표시됩니다.

- DNS 구성 보기 - 게이트웨이 로컬 콘솔에 기본 및 보조 DNS 서버에 사용할 수 있는 어댑터가 표시됩니다.
- 호스트 이름 구성 - 게이트웨이 로컬 콘솔에 게이트웨이가 지정한 정적 호스트 이름을 사용할지 아니면 DCHP 또는 rDNS를 통해 호스트 이름을 자동으로 가져올지 선택하라는 메시지가 표시됩니다.

  > **Note**
  >
  > 게이트웨이의 고정 호스트 이름을 구성하는 경우 게이트웨이의 IP 주소가 고정 호스트 이름을 가리키는 A 레코드를 DNS 시스템에 생성해야 합니다.

- 호스트 이름 구성 보기 - 게이트웨이 로컬 콘솔에 Amazon EC2 File Gateway의 호스트 이름, 획득 모드, 도메인 및 Active Directory 영역이 표시됩니다.

게이트웨이 VM 종료

하이퍼바이저에 패치를 적용할 때와 같이 유지 관리용 VM을 종료하거나 재부팅해야 할 수도 있습니다. 하이퍼바이저 인터페이스를 사용하여 온프레미스 게이트웨이 VM을 종료하고 Amazon EC2 콘솔을 사용하여 Amazon EC2 인스턴스를 종료합니다.

> **Important**
>
> 휘발성 스토리지를 사용하는 Amazon EC2 게이트웨이를 중지했다가 다시 시작하면 게이트웨이가 영구적으로 오프라인 상태가 됩니다. 이는 물리적 스토리지 디스크가 대체되기 때문에 발생합니다. 이 문제에 대한 해결 방법은 없습니다. 유일한 해결 방법은 게이트웨이를 삭제하고 새 EC2 인스턴스에서 새 게이트웨이를 활성화하는 것입니다.

기존 S3 File Gateway를 새 인스턴스로 교체

데이터 및 성능 요구 사항이 증가하거나 게이트웨이 마이그레이션 AWS 알림을 받는 경우 기존 S3 File GatewayFSx를 새 인스턴스로 바꿀 수 있습니다. 게이트웨이를 더 나은 호스트 플랫폼이나 최신 Amazon EC2 인스턴스로 이동하거나 기본 서버 하드웨어를 새로 고치려면 이 작업을 수행해야 할 수 있습니다.

기존 S3 File Gateway를 교체하는 방법에는 두 가지가 있습니다. 다음 표에서는 각 방법의 이점과 단점을 설명합니다. 이 정보를 사용하여 게이트웨이 환경에 가장 적합한 방법을 선택한 다음 아래 해당 섹션의 절차 단계를 참조하세요.

> **Note**
>
> 새 Storage Gateway 로컬 콘솔에 로그인하여 두 방법 중 하나를 완료해야 하는 경우 초기 사용자 이름은 admin이고 임시 암호는 password입니다.

> **Important**
>
> 다음 지침은 버전 1.x를 실행하는 게이트웨이 어플라이언스를 마이그레이션하는 경우에만 사용합니다. 하위 버전을 실행하는 게이트웨이 어플라이언스를 마이그레이션하는 데 사용할 수 없습니다.

	방법 1: 캐시 디스크 및 게이트웨이 ID를 대체 인스턴스로 마이그레이션*	방법 2: 빈 캐시 디스크와 새 게이트웨이 ID가 있는 대체 인스턴스
캐시 디스크 데이터	캐시 디스크의 데이터는 보존됩니다. 이 방법은 게이트웨이의 캐시 디스크가 크거나 애플리케이션이 out-of-cache 읽기 작업으로 인한 지연에 민감한 경우에 유용합니다.	캐시의 데이터는 AWS 클라우드에서 다운로드됩니다. 이 방법은 애플리케이션이 out-of-cache 읽기로 인한 지연을 허용할 수 있는 경우 쓰기 작업이 많은 워크로드에 최적화되어 있습니다.
가동 중지 시간	마이그레이션 프로세스 중에 게이트웨이가 1~2시간 동안 오프라인 상태가 됩니다.	파일 공유는 항상 사용할 수 있지만 클라이언트는 새 인스턴스로 전환하는 동안 한 파일 공유에서 다른 파일 공유로 전환할 때 짧은 전환 가동 중지 시간을 경험합니다.

	방법 1: 캐시 디스크 및 게이트웨이 ID를 대체 인스턴스로 마이그레이션*	방법 2: 빈 캐시 디스크와 새 게이트웨이 ID가 있는 대체 인스턴스
		Note 두 파일 공유에서 한 Amazon S3 버킷에 동시에 쓰는 것은 지원되지 않으므로 모든 클라이언트는 점진적으로가 아니라 한 공유에서 다른 공유로 동시에 다시 매핑해야 합니다.
게이트웨이 ID	새 게이트웨이는 대체하는 게이트웨이에서 게이트웨이 ID를 상속합니다.	기존 게이트웨이와 대체 게이트웨이에는 별도의 고유한 게이트웨이 ID가 있습니다.

	방법 1: 캐시 디스크 및 게이트웨이 ID를 대체 인스턴스로 마이그레이션*	방법 2: 빈 캐시 디스크와 새 게이트웨이 ID가 있는 대체 인스턴스
비용 영향	캐시된 데이터 보존을 사용하면 다시 다운로드할 필요가 없으므로 추가 S3 비용이 발생하지 않습니다.	이 방법은 특히 S3에서 데이터를 검색해야 하는 경우 추가 비용이 발생할 수 있습니다. 또한 이 접근 방식은 S3 버킷이 지원하는 파일 공유가 S3 Intelligent-Tiering, S3 Standard-IA, S3 One Zone-IA 또는 S3 수명 주기 정책을 통해 GLACIER로 전환된 객체와 같은 스토리지 클래스를 사용하는 경우 상당한 S3 데이터 검색 비용이 발생할 수 있습니다. SMB 파일 공유의 경우 루트 ACL이 파일 공유에 구성된 경우 마이그레이션된 게이트웨이에 다시 적용해야 합니다. 이 작업은 파일 공유 내의 모든 객체에 설정을 재귀적으로 적용하여 일부 비용에 영향을 미칩니다.

> **Note**
>
> 마이그레이션은 동일한 유형의 게이트웨이 간에만 수행할 수 있습니다. 예를 들어 설정 또는 데이터를 FSx File Gateway에서 S3 File Gateway로 마이그레이션할 수 없습니다.

방법 1: 캐시 디스크 및 게이트웨이 ID를 대체 인스턴스로 마이그레이션

S3 File Gateway의 캐시 디스크 및 게이트웨이 ID를 대체 인스턴스로 마이그레이션하려면:

1. 기존 S3 File Gateway에 쓰는 모든 애플리케이션을 중지합니다.

2. 다음 단계에 따라 게이트웨이를 최신 버전으로 업데이트합니다.

   a. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.

   b. 탐색 창에서 게이트웨이를 선택한 다음 마이그레이션하려는 이전 S3 파일 게이트웨이를 선택합니다.

   c. 사용 가능한 경우 지금 업데이트를 클릭합니다. 그렇지 않으면 게이트웨이가 이미 최신 버전입니다.

3. 기존 S3 File Gateway에 대한 모니터링 탭의 `CachePercentDirty` 지표가 `0`인지 확인합니다.

4. 하이퍼바이저 제어를 사용하여 호스트 가상 머신(VM)의 전원을 꺼서 기존 S3 File Gateway를 종료합니다.

   Amazon EC2 인스턴스 종료에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 인스턴스 중지 및 시작을 참조하세요.

   KVM, VMware 또는 Hyper-V VM 종료에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

5. 이전 게이트웨이 VM에서 루트 디스크 및 캐시 디스크를 비롯한 모든 디스크를 분리합니다.

   > **Note**
   >
   > 루트 디스크의 볼륨 ID와 해당 루트 디스크와 연결된 게이트웨이 ID를 기록해 둡니다. 이후 단계에서 새 Storage Gateway 하이퍼바이저에서 이 디스크를 분리해야 합니다.

   Amazon EC2 인스턴스를 S3 File Gateway의 VM으로 사용하는 경우, Amazon EC2 사용 설명서의 Windows 인스턴스에서 Amazon EBS 볼륨 분리 또는 Linux 인스턴스에서 Amazon EBS 볼륨 분리를 참조하세요.

   KVM, VMware 또는 Hyper-V VM에서 디스크를 분리하는 방법에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

6. 새 AWS Storage Gateway 하이퍼바이저 VM 인스턴스를 생성하되 게이트웨이로 활성화하지 마세요. 이후 단계에서 이 새 게이트웨이는 이전 게이트웨이의 ID를 사용합니다.

   새 Storage Gateway 하이퍼바이저 VM을 생성하는 방법에 대한 자세한 내용은 호스트 플랫폼 선택 및 VM 다운로드를 참조하세요.

> **Note**
>
> 새 VM에 캐시 디스크를 추가하지 마세요. 이 VM은 이전 VM에서 사용하던 것과 동일한 캐시 디스크를 사용합니다.

> **Note**
>
> VM을 다운로드한 후 콘솔 마법사를 닫습니다. 이 시점에서는 활성화를 진행하지 마십시오.

7. 이전 VM과 동일한 네트워크 설정을 사용하도록 새 Storage Gateway VM을 구성합니다.

   게이트웨이의 기본 네트워크 구성은 DHCP(Dynamic Host Configuration Protocol)입니다. DHCP를 통해 게이트웨이에 IP 주소가 자동으로 지정됩니다.

   게이트웨이 VM의 고정 IP 주소를 수동으로 구성해야 하는 경우 네트워크 파라미터 구성을 참조하세요.

   게이트웨이 VM이 소켓 보안 버전 5(SOCKS5) 프록시를 사용하여 인터넷에 연결해야 하는 경우 HTTP 프록시를 통해 EC2에 배포된 게이트웨이 라우팅을 참조하세요.

   > **Note**
   >
   > NFS 또는 SMB 클라이언트를 재구성하지 않도록 이전 게이트웨이 VM에서 동일한 고정 IP 주소 또는 호스트 이름을 재사용할 수 있습니다.

8. 새 Storage Gateway VM을 시작합니다.
9. 이전의 게이트웨이 VM에서 분리한 디스크를 새로운 게이트웨이 VM에 연결합니다. 새 게이트웨이 VM에서 기존 루트 디스크를 분리하지 마십시오.

   > **Note**
   >
   > 성공적으로 마이그레이션하려면 모든 디스크가 변경되지 않은 상태로 유지되어야 합니다. 디스크 크기 또는 기타 값을 변경하면 메타데이터에 불일치가 발생하여 마이그레이션이 성공하지 못합니다.

10. 새 게이트웨이 VM의 로컬 콘솔에 연결하거나 새 게이트웨이 VM의 IP 주소(아래 설명 참조)에 웹 요청을 수행하여 게이트웨이 마이그레이션 프로세스를 시작합니다.

    a. 로컬 콘솔을 사용하려면 게이트웨이 마이그레이션 옵션을 선택하고 메시지가 표시되면 기존 게이트웨이 ID를 제공합니다. 이전 게이트웨이에 이전에 적용된 설정을 새 게이트웨이로 복사하라는 메시지가 표시됩니다. 이를 적용하거나 나중에 수동으로 구성할 수 있습니다. 게이트웨이 로컬 콘솔 액세스를 참조하세요.

    b. 또는 다음 형식을 사용하는 URL을 사용하여 새 VM에 연결하여 게이트웨이 마이그레이션 프로세스를 시작할 수 있습니다.

    ```
    http://your-VM-IP-address/migrate?gatewayId=your-gateway-ID
    ```

    이전 게이트웨이 VM에 사용한 것과 동일한 IP 주소를 새 게이트웨이 VM에 다시 사용할 수 있습니다. URL은 다음 예와 비슷해야 합니다.

    ```
    http://198.51.100.123/migrate?gatewayId=sgw-12345678
    ```

    이 URL을 브라우저에서 사용하거나 `curl`을 사용하여 명령줄에서 사용하여 마이그레이션 프로세스를 시작합니다.

    게이트웨이 마이그레이션 프로세스가 성공적으로 완료되면 마이그레이션 성공을 확인하는 메시지가 표시됩니다.

11. 게이트웨이 상태가 AWS Storage Gateway 콘솔에서 실행 중으로 표시될 때까지 기다립니다. 사용 가능한 대역폭에 따라 최대 10분이 걸릴 수 있습니다.
12. 새 Storage Gateway VM을 중지합니다.
13. 이전에 기록한 볼륨 ID가 있는 이전 게이트웨이의 루트 디스크를 새 게이트웨이에서 분리합니다.
14. 새 Storage Gateway VM을 시작합니다.
15. 게이트웨이가 Active Directory 도메인에 조인된 경우 도메인에 다시 조인합니다. 지침은 Active Directory를 사용하여 사용자 인증을 참조하세요.

    > **Note**
    >
    > S3 File Gateway의 상태가 조인됨으로 표시되는 경우에도 이 단계를 완료해야 합니다.

16. 게이트웨이가 SMB 게스트 액세스 인증 방법을 사용하는 경우 암호를 다시 입력해야 합니다. 지침은 파일 공유에 대한 게스트 액세스 권한 제공을 참조하세요.

17. 새 게이트웨이 VM의 IP 주소에서 공유를 사용할 수 있는지 확인한 다음 이전 게이트웨이 VM을 삭제합니다.

> **Warning**
>
> 게이트웨이를 삭제하면 복구할 수 없습니다.

Amazon EC2 인스턴스 삭제에 대한 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 종료를 참조하세요. KVM, VMware 또는 Hyper-V VM 삭제에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

방법 2: 빈 캐시 디스크와 새 게이트웨이 ID가 있는 대체 인스턴스

빈 캐시 디스크와 새 게이트웨이 ID를 사용하여 대체 S3 File Gateway 인스턴스를 설정하려면:

1. 기존 S3 File Gateway에 쓰는 모든 애플리케이션을 중지합니다. 새 게이트웨이에서 파일 공유를 설정하기 전에 모니터링 탭의 `CachePercentDirty` 지표가 `0`인지 확인합니다.
2. AWS Command Line Interface (AWS CLI)를 사용하여 다음을 수행하여 기존 S3 File GatewayFSx 및 파일 공유에 대한 구성 정보를 수집하고 저장합니다.

   a. S3 File Gateway에 대한 게이트웨이 구성 정보를 저장합니다.

   ```
   aws storagegateway describe-gateway-information --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   이 명령은 게이트웨이의 이름, 네트워크 인터페이스, 구성된 시간대 및 상태(게이트웨이가 실행 중인지 여부) 등 게이트웨이에 대한 메타데이터를 반환하는 JSON 블록을 출력합니다.

   b. S3 File Gateway의 SMB(Server Message Block) 설정을 저장합니다.

   ```
   aws storagegateway describe-smb-settings --gateway-arn
    "arn:aws:storagegateway:us-east-2:123456789012:gateway/sgw-12A3456B"
   ```

   이 명령은 도메인 이름, Microsoft Active Directory 상태, 게스트 암호 설정 여부, 보안 전략 유형 등 SMB 파일 공유에 대한 메타데이터가 포함된 JSON 블록을 출력합니다.

   c. S3 File Gateway의 각 SMB 및 NFS(Network File System) 파일 공유에 대한 파일 공유 정보를 저장합니다.

- SMB 파일 공유에 다음 명령을 사용합니다.

```
aws storagegateway describe-smb-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-987A654B"
```

이 명령은 이름, 스토리지 클래스, 상태, IAM 역할 Amazon 리소스 이름(ARN), S3 File Gateway에 액세스할 수 있는 클라이언트 목록, SMB 클라이언트가 탑재 지점을 식별하는 데 사용하는 경로 등 SMB 파일 공유에 대한 메타데이터가 포함된 JSON 블록을 출력합니다.

- NFS 파일 공유에 다음 명령을 사용합니다.

```
aws storagegateway  describe-nfs-file-shares --file-share-arn-list
 "arn:aws:storagegateway:us-east-2:123456789012:share/share-321A978B"
```

이 명령은 이름, 스토리지 클래스, 상태, IAM 역할 ARN, S3 File Gateway에 액세스할 수 있는 클라이언트 목록, NFS 클라이언트가 탑재 지점을 식별하는 데 사용하는 경로 등 NFS 파일 공유에 대한 메타데이터가 포함된 JSON 블록을 출력합니다.

3. 이전 게이트웨이와 동일한 설정 및 구성으로 새 S3 File Gateway를 생성합니다. 필요한 경우 2단계에서 저장한 정보를 참조하세요.
4. 이전 게이트웨이에 구성된 파일 공유와 동일한 설정 및 구성을 사용하여 새 게이트웨이에 대한 새 파일 공유를 생성합니다. 필요한 경우 2단계에서 저장한 정보를 참조하세요.
5. 새 게이트웨이가 올바르게 작동하는지 확인한 다음 환경에 가장 적합한 방식으로 이전 파일 공유에서 새 파일 공유로 클라이언트를 다시 매핑/컷오버합니다.
6. 새 게이트웨이가 올바르게 작동하는지 확인한 다음 Storage Gateway 콘솔에서 이전 게이트웨이를 삭제합니다.

> **Important**
>
> S3 File Gateway를 삭제하기 전에 해당 게이트웨이의 캐시에 현재 쓰기 작업 중인 애플리케이션이 없는지 확인해야 합니다. 사용 중인 게이트웨이를 삭제하면 데이터 손실이 발생할 수 있습니다.

> **Warning**
>
> 게이트웨이를 삭제하면 복구할 수 없습니다.

7. 이전 게이트웨이 VM 또는 Amazon EC2 인스턴스를 삭제합니다.

게이트웨이 삭제 및 연결된 리소스 제거

게이트웨이를 계속 사용할 계획이 아니라면 게이트웨이와 이에 연결된 리소스를 삭제하는 것이 좋습니다. 리소스를 제거하면 계속해서 사용할 계획이 없는 리소스에 요금이 부과되지 않게 할 수 있고 월별 청구액을 줄이는 데 도움이 됩니다.

게이트웨이를 삭제하면 AWS Storage Gateway Management Console에 더 이상 표시되지 않으며 해당 파일 공유 연결이 닫힙니다. 게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 별도 지침 대로 연결된 리소스를 제거해야 합니다.

Storage Gateway 콘솔을 사용하거나 프로그래밍 방식으로 게이트웨이를 삭제할 수 있습니다. Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하는 방법에 대한 정보는 다음에서 확인할 수 있습니다. 게이트웨이를 프로그래밍 방식으로 삭제하려면 AWS Storage Gateway API 참조를 참조하세요.

Storage Gateway 콘솔을 사용하여 게이트웨이 삭제

게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 추가 작업을 수행하여 게이트웨이에 연결된 리소스를 제거해야 하는 경우도 있습니다. 이 리소스를 제거하면 향후 사용 계획이 없는 리소스에 대한 요금이 발생하는 일을 막을 수 있습니다.

> **Note**
>
> Amazon EC2 인스턴스에 배포된 게이트웨이의 경우, 해당 인스턴스는 삭제하지 않는 한 계속 존재합니다.
>
> 가상 머신(VM)에 배포한 게이트웨이의 경우, 게이트웨이를 삭제한 후에도 게이트웨이 VM은 여전히 가상화 환경에 존재합니다. VM을 제거하려면 VMware vSphere 클라이언트, Microsoft Hyper-V Manager 또는 Linux 커널 기반 가상 머신(KVM) 클라이언트를 사용하여 호스트에 연

결하고 VM을 제거합니다. 삭제한 게이트웨이의 VM을 다시 사용하여 새 게이트웨이를 활성화할 수는 없다는 점에 유의하십시오.

게이트웨이 삭제

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 삭제할 게이트웨이를 하나 이상 선택합니다.
3. 작업에서 게이트웨이 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.

   Warning

   이 단계를 수행하기 전에 게이트웨이의 볼륨에 현재 쓰기 작업을 하는 애플리케이션이 없는지 확인합니다. 게이트웨이를 사용하는 중에 삭제하면 데이터 손실이 발생할 수 있습니다. 게이트웨이를 삭제하면 복구할 수 없습니다.

4. 지정된 게이트웨이를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.
5. (선택 사항) 삭제된 게이트웨이에 대한 피드백을 제공하려면 피드백 대화 상자를 작성한 다음 제출을 선택합니다. 그렇지 않은 경우 건너뛰기를 선택합니다.

Important

게이트웨이를 삭제한 후에는 더 이상 소프트웨어 요금을 지불하지 않아도 되지만, Amazon S3 버킷 및 Amazon EC2 인스턴스와 같은 리소스는 계속 유지됩니다. File Gateway를 제거한 후 게이트웨이 Amazon EC2 인스턴스를 제거할 수 있습니다. 파일 공유와 연결된 Amazon S3 버킷의 데이터가 필요하지 않은 경우 Amazon S3 버킷을 제거하도록 선택할 수 있습니다. 지침은 버킷 삭제를 참조하세요.

성능 및 최적화

이 섹션에서는 File Gateway 성능을 최적화하기 위한 지침과 모범 사례를 설명합니다.

주제

S3 File Gateway에 대한 기본 성능 지침

이 섹션에서는 S3 File Gateway VM에 하드웨어를 프로비저닝하기 위한 구성 지침을 알아봅니다. 표에 나와 있는 인스턴스 구성은 예제이며 참고용입니다.

성능을 최적화하려면 캐시 디스크 크기를 활성 작업 세트의 크기로 변경해야 합니다. 캐시에 여러 로컬 디스크를 사용하면 데이터에 대한 액세스를 병렬화하여 성능이 확장되고 IOPS가 향상됩니다.

> **Note**
>
> 휘발성 스토리지는 사용하지 않는 것이 좋습니다. 휘발성 스토리지 사용에 대한 자세한 내용은 휘발성 스토리지와 EC2 게이트웨이를 함께 사용 섹션을 참조하세요.
> Amazon EC2 인스턴스의 경우 S3 버킷에 객체 수가 5백만개 이상이고 범용 SSD 볼륨을 사용 중인 경우 시작 시 게이트웨이가 허용 가능한 성능을 발휘하려면 최소 루트 EBS 볼륨으로 350GiB가 필요합니다. 볼륨 크기 증가 방법에 대한 자세한 내용은 탄력적 볼륨을 사용하여 EBS 볼륨 수정(콘솔)을 참조하세요.
> File Gateway에 연결하는 파일 공유 의 개별 디렉터리에 대해 제안된 크기 제한은 디렉터리당 10,000개의 파일입니다. 10,000개 이상의 파일이 있는 디렉터리에서 File Gateway를 사용할 수 있지만 성능이 영향을 받을 수 있습니다.

다음 표에서 캐시 적중 읽기 작업은 캐시에서 제공되는 파일 공유에서의 읽기입니다. 캐시 누락 읽기 작업은 Amazon S3에서 제공되는 파일 공유에서의 읽기입니다.

다음 표에는 S3 File Gateway 구성의 예가 나와 있습니다.

Linux 클라이언트의 S3 File Gateway 성능

구성의 예	프로토콜	쓰기 처리량(파일 크기 1GB)	캐시 적중 읽기 처리량	캐시 누락 읽기 처리량
루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 512GiB 캐시, io1, 1,500 프로비저닝된 IOPS 최소 네트워크 성능: 10Gbps CPU: 16 vCPU | RAM: 32GB Linux에 권장되는 NFS 프로토콜	NFSv3 - 스레드 1개	110MiB/초(0.92Gbps)	590MiB/초(4.9Gbps)	310MiB/초(2.6Gbps)
	NFSv3 - 스레드 8개	160MiB/초(1.3Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
	NFSv4 - 스레드 1개	130MiB/초(1.1Gbps)	590MiB/초(4.9Gbps)	295MiB/초(2.5Gbps)
	NFSv4 - 스레드 8개	160MiB/초(1.3Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
	SMBV3 - 스레드 1개	115MiB/초(1.0Gbps)	325MiB/초(2.7Gbps)	255MiB/초(2.1Gbps)
	SMBV3 - 스레드 8개	190MiB/초(1.6Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
Storage Gateway 하드웨어 어플라이언스 최소 네트워크 성능: 10Gbps	NFSv3 - 스레드 1개	265MiB/초(2.2Gbps)	590MiB/초(4.9Gbps)	310MiB/초(2.6Gbps)
	NFSv3 - 스레드 8개	385MiB/초(3.1Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
	NFSv4 - 스레드 1개	310MiB/초(2.6Gbps)	590MiB/초(4.9Gbps)	295MiB/초(2.5Gbps)
	NFSv4 - 스레드 8개	385MiB/초(3.1Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
	SMBV3 - 스레드 1개	275MiB/초(2.4Gbps)	325MiB/초(2.7Gbps)	255MiB/초(2.1Gbps)

구성의 예	프로토콜	쓰기 처리량(파일 크기 1GB)	캐시 적중 읽기 처리량	캐시 누락 읽기 처리량
루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 2TB NVME 캐시 디스크 4개 최소 네트워크 성능: 10Gbps CPU: 32 vCPU | RAM: 244GB Linux에 권장되는 NFS 프로토콜	SMBV3 - 스레드 8개	455MiB/초(3.8Gbps)	590MiB/초(4.9Gbps)	335MiB/초(2.8Gbps)
	NFSv3 - 스레드 1개	300MiB/초(2.5Gbps)	590MiB/초(4.9Gbps)	325MiB/초(2.7Gbps)
	NFSv3 - 스레드 8개	585MiB/초(4.9Gbps)	590MiB/초(4.9Gbps)	580MiB/초(4.8Gbps)
	NFSv4 - 스레드 1개	355MiB/초(3.0Gbps)	590MiB/초(4.9Gbps)	340MiB/초(2.9Gbps)
	NFSv4 - 스레드 8개	575MiB/초(4.8Gbps)	590MiB/초(4.9Gbps)	575MiB/초(4.8Gbps)
	SMBV3 - 스레드 1개	230MiB/초(1.9Gbps)	325MiB/초(2.7Gbps)	245MiB/초(2.0Gbps)
	SMBV3 - 스레드 8개	585MiB/초(4.9Gbps)	590MiB/초(4.9Gbps)	580MiB/초(4.8Gbps)

Windows 클라이언트의 File Gateway 성능

구성의 예	프로토콜	쓰기 처리량(파일 크기 1GB)	캐시 적중 읽기 처리량	캐시 누락 읽기 처리량
루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 512GiB 캐시, io1, 1,500 프로비저닝된 IOPS	SMBV3 - 스레드 1개	150MiB/초(1.3Gbps)	180MiB/초(1.5Gbps)	20MiB/초(0.2Gbps)
	SMBV3 - 스레드 8개	190MiB/초(1.6Gbps)	335MiB/초(2.8Gbps)	195MiB/초(1.6Gbps)
	NFSv3 - 스레드 1개	95MiB/초(0.8Gbps)	130MiB/초(1.1Gbps)	20MiB/초(0.2Gbps)

구성의 예	프로토콜	쓰기 처리량(파일 크기 1GB)	캐시 적중 읽기 처리량	캐시 누락 읽기 처리량
최소 네트워크 성능: 10Gbps CPU: 16 vCPU | RAM: 32GB Windows에 권장되는 SMB 프로토콜	NFSv3 - 스레드 8개	190MiB/초(1.6Gbps)	330MiB/초(2.8Gbps)	190MiB/초(1.6Gbps)
Storage Gateway 하드웨어 어플라이언스 최소 네트워크 성능: 10Gbps	SMBV3 - 스레드 1개	230MiB/초(1.9Gbps)	255MiB/초(2.1Gbps)	20MiB/초(0.2Gbps)
	SMBV3 - 스레드 8개	835MiB/초(7.0Gbps)	475MiB/초(4.0Gbps)	195MiB/초(1.6Gbps)
	NFSv3 - 스레드 1개	135MiB/초(1.1Gbps)	185MiB/초(1.6Gbps)	20MiB/초(0.2Gbps)
	NFSv3 - 스레드 8개	545MiB/초(4.6Gbps)	470MiB/초(4.0Gbps)	190MiB/초(1.6Gbps)

구성의 예	프로토콜	쓰기 처리량(파일 크기 1GB)	캐시 적중 읽기 처리량	캐시 누락 읽기 처리량
루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 2TB NVME 캐시 디스크 4개 최소 네트워크 성능: 10Gbps CPU: 32 vCPU | RAM: 244GB Windows에 권장되는 SMB 프로토콜	SMBV3 - 스레드 1개	230MiB/초(1.9Gbps)	265MiB/초(2.2Gbps)	30MiB/초(0.3Gbps)
	SMBV3 - 스레드 8개	835MiB/초(7.0Gbps)	780MiB/초(6.5Gbps)	250MiB/초(2.1Gbps)
	NFSv3 - 스레드 1개	135MiB/초(1.1Gbps)	220MiB/초(1.8Gbps)	30MiB/초(0.3Gbps)
	NFSv3 - 스레드 8개	545MiB/초(4.6Gbps)	570MiB/초(4.8Gbps)	240MiB/초(2.0Gbps)

> **Note**
>
> 성능은 호스트 플랫폼 구성 및 네트워크 대역폭에 따라 달라질 수 있습니다. 쓰기 처리량 성능은 파일 크기에 따라 감소하며 작은 파일(32MiB 미만)에 대해 달성 가능한 처리량이 초당 16개입니다.

여러 파일 공유가 있는 게이트웨이에 대한 성능 지침

Amazon S3 File Gateway는 단일 Storage Gateway 어플라이언스에 최대 50개의 파일 공유 연결을 지원합니다. 게이트웨이당 여러 파일 공유를 추가하면 게이트웨이와 가상 하드웨어 리소스를 더 적게 관리하면서 더 많은 사용자와 워크로드를 지원할 수 있습니다. 게이트웨이에서 관리하는 파일 공유 수는 다른 요인 외에도 해당 게이트웨이의 성능에 영향을 미칠 수 있습니다. 이 섹션에서는 연결된 파일 공유 수에 따라 게이트웨이 성능이 어떻게 변경될 것으로 예상되는지 설명하고 가상 하드웨어 구성을 권장하여 여러 공유를 관리하는 게이트웨이의 성능을 최적화합니다.

일반적으로 단일 Storage Gateway에서 관리하는 파일 공유 수를 늘리면 다음과 같은 결과가 발생할 수 있습니다.

- 게이트웨이를 다시 시작하는 데 필요한 시간이 늘어났습니다.
- vCPU 및 RAM과 같은 가상 하드웨어 리소스의 사용률 향상.
- 가상 하드웨어 리소스가 포화되면 데이터 및 메타데이터 작업 성능이 저하됩니다.

다음 표에는 여러 파일 공유를 관리하는 게이트웨이에 권장되는 가상 하드웨어 구성이 나열되어 있습니다.

게이트웨이당 파일 공유	권장 게이트웨이 용량 설정	권장 vCPU 코어	권장 RAM	권장 루트 디스크 크기			
1-10	작은	4(EC2 인스턴스 유형 m4.xlarge 이상)	16GiB	80GiB			
10~20	중간	8(EC2 인스턴스 유형 m4.2xlarge 이상)	32GiB	160GiB			
20+	대형	16(EC2 인스턴스 유형 m4.4xlarge 이상)	64GiB	240GiB			

위에서 권장하는 가상 하드웨어 구성 외에도 여러 파일 공유를 관리하는 Storage Gateway 어플라이언스를 구성하고 유지 관리하기 위한 다음 모범 사례를 따르는 것이 좋습니다.

- 파일 공유 수와 게이트웨이의 가상 하드웨어에 대한 수요 간의 관계가 반드시 선형은 아니라고 가정합니다. 일부 파일 공유는 처리량을 더 많이 생성하여 다른 파일 공유보다 하드웨어 수요를 더 많이 생성할 수 있습니다. 위 표의 권장 사항은 최대 하드웨어 용량과 다양한 파일 공유 처리량 수준을 기반으로 합니다.
- 단일 게이트웨이에 여러 파일 공유를 추가하면 성능이 저하되는 경우 가장 활성이 높은 파일 공유를 다른 게이트웨이로 이동하는 것이 좋습니다. 특히 파일 공유가 처리량이 매우 높은 애플리케이션에 사용되는 경우 해당 파일 공유에 대해 별도의 게이트웨이를 생성하는 것이 좋습니다.
- 처리량이 높은 여러 애플리케이션에 대해 하나의 게이트웨이를 구성하고 처리량이 낮은 여러 애플리케이션에 대해 다른 게이트웨이를 구성하는 것은 권장하지 않습니다. 대신 고처리량 및 저처리량 파일 공유를 게이트웨이에 균등하게 분산하여 하드웨어 포화도의 균형을 맞추십시오. 파일 공유 처리량을 측정하려면 `ReadBytes` 및 `WriteBytes` 지표를 사용하세요. 자세한 내용은 파일 공유 지표 이해를 참조하세요.

S3 File Gateway 처리량 최대화

다음 섹션에서는 NFS와 SMB 클라이언트, S3 File Gateway 및 Amazon S3 간의 처리량을 극대화하는 모범 사례를 설명합니다. 각 섹션에 제공된 지침은 전체 처리량을 개선하는 데 점진적으로 기여합니다. 이러한 권장 사항은 필요하지 않으며 상호 종속적이지 않지만가 S3 File Gateway 구현을 테스트하고 조정하는 데 지원 사용하는 논리적 방식으로 선택 및 정렬되었습니다. 이러한 제안을 구현하고 테스트할 때 각 S3 File Gateway 배포는 고유하므로 결과가 다를 수 있습니다.

S3 File Gateway는 파일과 객체 간의 기본 1:1 매핑과 함께 업계 표준 NFS 또는 SMB 파일 프로토콜을 사용하여 Amazon S3 객체를 저장하고 검색할 수 있는 파일 인터페이스를 제공합니다. S3 File Gateway를 VMware, Microsoft Hyper-V 또는 Linux KVM 환경의 온프레미스 또는 AWS 클라우드에 Amazon EC2 인스턴스로 가상 머신으로 배포합니다. S3 File Gateway는 전체 엔터프라이즈 NAS 교체로 작동하도록 설계되지 않았습니다. S3 File Gateway는 파일 시스템을 에뮬레이션하지만 파일 시스템은 아닙니다. Amazon S3를 내구성 있는 백엔드 스토리지로 사용하면 각 I/O 작업에 추가 오버헤드가 발생하므로 기존 NAS 또는 파일 서버와 비교하여 S3 File Gateway 성능을 평가하는 것은 동등한 비교가 아닙니다.

클라이언트와 동일한 위치에 게이트웨이 배포

S3 File Gateway 가상 어플라이언스와 NFS 또는 SMB 클라이언트 간에 네트워크 지연 시간을 최소화하면서 물리적 위치에 배포하는 것이 좋습니다. 게이트웨이의 위치를 선택할 때 다음 사항을 고려하세요.

- 게이트웨이의 네트워크 지연 시간이 짧으면 NFS 또는 SMB 클라이언트의 성능을 개선하는 데 도움이 될 수 있습니다.
- S3 File Gateway는 게이트웨이와 클라이언트 간에 비해 게이트웨이와 Amazon S3 간에 더 높은 네트워크 지연 시간을 허용하도록 설계되었습니다.
- Amazon EC2에 배포된 S3 File Gateway 인스턴스의 경우 게이트웨이와 NFS 또는 SMB 클라이언트를 동일한 배치 그룹에 유지하는 것이 좋습니다. 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 인스턴스에 대한 배치 그룹을 참조하세요.

느린 디스크로 인한 병목 현상 감소

`IoWaitPercent` CloudWatch 지표를 모니터링하여 S3 File Gateway의 느린 스토리지 디스크로 인해 발생할 수 있는 성능 병목 현상을 식별하는 것이 좋습니다. 디스크 관련 성능 문제를 최적화하려고 할 때는 다음 사항을 고려하세요.

- `IoWaitPercent`는 CPU가 루트 또는 캐시 디스크의 응답을 기다리는 시간의 비율을 보고합니다.
- `IoWaitPercent`가 5~10%보다 크면 일반적으로 성능 저하 디스크로 인한 게이트웨이 성능 병목 현상을 나타냅니다. 이 지표는 가능한 0%에 가까워야 합니다. 즉, 게이트웨이가 디스크를 기다리지 않으므로 CPU 리소스를 최적화하는 데 도움이 됩니다.
- Storage Gateway 콘솔의 모니터링 탭에서 `IoWaitPercent`를 확인하거나 지표가 특정 임계값을 초과하면 자동으로 알리도록 권장 CloudWatch 경보를 구성할 수 있습니다. 자세한 내용은 게이트웨이에 대한 권장 CloudWatch 경보 생성을 참조하세요.
- `IoWaitPercent`를 최소화하려면 게이트웨이의 루트 및 캐시 디스크에 NVMe 또는 SSD를 사용하는 것이 좋습니다.

CPU, RAM 및 캐시 디스크에 대한 가상 머신 리소스 할당 조정

S3 File Gateway의 처리량을 최적화하려는 경우 CPU, RAM 및 캐시 디스크를 포함하여 게이트웨이 VM에 충분한 리소스를 할당하는 것이 중요합니다. CPU 4개, 16GB RAM 및 150GB 캐시 스토리지의 최소 가상 리소스 요구 사항은 일반적으로 더 작은 워크로드에만 적합합니다. 대규모 워크로드에 가상 리소스를 할당할 때는 다음을 권장합니다.

- S3 File Gateway에서 생성되는 일반적인 CPU 사용량에 따라 할당된 CPU 수를 16~48개로 늘립니다. `UserCpuPercent` 지표를 사용하여 CPU 사용량을 모니터링할 수 있습니다. 자세한 내용은 게이트웨이 지표 이해를 참조하세요.
- 할당된 RAM을 32~64GB로 늘립니다.

> **Note**
>
> S3 File Gateway는 64GB를 초과하는 RAM을 사용할 수 없습니다.

- 루트 디스크 및 캐시 디스크에 NVMe 또는 SSD를 사용하고 게이트웨이에 쓰려는 최대 작업 데이터세트에 맞게 캐시 디스크의 크기를 조정합니다. 자세한 내용은 공식 Amazon Web Services YouTube 채널의 S3 File Gateway 캐시 크기 조정 모범 사례를 참조하세요.
- 하나의 대용량 디스크를 사용하는 대신 게이트웨이에 최소 4개의 가상 캐시 디스크를 추가합니다. 여러 가상 디스크는 동일한 기본 물리적 디스크를 공유하더라도 성능을 개선할 수 있지만, 일반적으로 가상 디스크가 서로 다른 기본 물리적 디스크에 있는 경우 성능이 향상됩니다.

  예를 들어 12TB의 캐시를 배포하려는 경우 다음 구성 중 하나를 사용할 수 있습니다.

  - 3TB 캐시 디스크 4개
  - 1.5TB 캐시 디스크 8개
  - 1TB 캐시 디스크 12개

  이를 통해 성능 외에도 시간이 지남에 따라 가상 머신을 보다 효율적으로 관리할 수 있습니다. 워크로드가 변경되면 각 개별 가상 디스크의 원래 크기를 유지하면서 캐시 디스크 수와 전체 캐시 용량을 점진적으로 늘려 게이트웨이 무결성을 유지할 수 있습니다.

  자세한 내용은 로컬 디스크 스토리지 용량 결정을 참조하세요.

S3 File Gateway를 Amazon EC2 인스턴스로 배포할 때는 다음 사항을 고려하세요.

- 선택한 인스턴스 유형은 게이트웨이 성능에 상당한 영향을 미칠 수 있습니다. Amazon EC2는 S3 File Gateway 인스턴스에 대한 리소스 할당을 조정할 수 있는 광범위한 유연성을 제공합니다.
- S3 File Gateway에 권장되는 Amazon EC2 인스턴스 유형은 Amazon EC2 인스턴스 유형에 대한 요구 사항을 참조하세요.
- 활성 S3 File Gateway를 호스팅하는 Amazon EC2 인스턴스 유형을 변경할 수 있습니다. 이를 통해 Amazon EC2 하드웨어 생성 및 리소스 할당을 쉽게 조정하여 이상적인 price-to-performance 비율을 찾을 수 있습니다. 인스턴스 유형을 변경하려면 Amazon EC2 콘솔에서 다음 절차를 사용합니다.

  1. Amazon EC2 인스턴스를 중지합니다.
  2. Amazon EC2 인스턴스 유형을 변경합니다.
  3. Amazon EC2 인스턴스의 전원을 켭니다.

> **Note**
>
> S3 File Gateway를 호스팅하는 인스턴스를 중지하면 파일 공유 액세스가 일시적으로 중단됩니다. 필요한 경우 유지 관리 기간을 예약해야 합니다.

- Amazon EC2 인스턴스의 price-to-performance 비율은 지불한 가격으로 얻을 수 있는 컴퓨팅 성능을 나타냅니다. 일반적으로 최신 세대 Amazon EC2 인스턴스는 이전 세대에 비해 비교적 저렴한 비용으로 최신 하드웨어와 향상된 성능을 갖춘 최상의 price-to-performance 비율을 제공합니다. 인스턴스 유형, 리전 및 사용 패턴과 같은 요소는 이 비율에 영향을 미치므로 비용 효율성을 최적화하려면 특정 워크로드에 적합한 인스턴스를 선택하는 것이 중요합니다.

SMB 보안 수준 조정

SMBv3 프로토콜은 성능 및 보안에 일부 장단점이 있는 SMB 서명 및 SMB 암호화를 모두 허용합니다. 처리량을 최적화하기 위해 게이트웨이의 SMB 보안 수준을 조정하여 클라이언트 연결에 적용되는 보안 기능을 지정할 수 있습니다. 자세한 내용은 게이트웨이의 보안 수준 설정을 참조하세요.

SMB 보안 수준을 조정할 때는 다음 사항을 고려하세요.

- S3 File Gateway의 기본 보안 수준은 암호화 적용입니다. 이 설정은 게이트웨이 파일 공유에 대한 SMB 클라이언트 연결에 암호화와 서명을 모두 적용합니다. 즉, 클라이언트에서 게이트웨이로의 모든 트래픽이 암호화됩니다. 이 설정은 게이트웨이에서 로의 트래픽에는 영향을 주지 않으며 AWS,이 트래픽은 항상 암호화됩니다.

  게이트웨이는 암호화된 각 클라이언트 연결을 단일 vCPU로 제한합니다. 예를 들어 암호화된 클라이언트가 1개뿐인 경우 게이트웨이에 4개 이상의 vCPU가 할당되더라도 해당 클라이언트는 1개의 vCPU로만 제한됩니다. 따라서 단일 클라이언트에서 S3 File Gateway로의 암호화된 연결에 대한 처리량은 일반적으로 40~60MB/초로 병목 현상이 발생합니다.
- 보안 요구 사항이 보다 완화된 태세를 허용하는 경우 보안 수준을 클라이언트 협상으로 변경할 수 있습니다. 그러면 SMB 암호화가 비활성화되고 SMB 서명만 적용됩니다. 이 설정을 사용하면 게이트웨이에 대한 클라이언트 연결이 여러 vCPU를 활용할 수 있으므로 일반적으로 처리량 성능이 향상됩니다.

> **Note**
>
> S3 File Gateway의 SMB 보안 수준을 변경한 후에는 파일 공유 상태가 Storage Gateway 콘솔에서 업데이트 중에서 사용 가능으로 변경될 때까지 기다린 다음 새 설정이 적용되도록 SMB 클라이언트를 연결 해제했다가 다시 연결해야 합니다.

여러 스레드와 클라이언트를 사용하여 쓰기 작업 병렬화

단일 클라이언트에서 순차적으로 쓰는 작업은 단일 스레드 작업이므로 한 번에 하나의 NFS 또는 SMB 클라이언트만 사용하여 파일을 쓰는 S3 File Gateway를 사용하면 처리량 성능을 극대화하기 어렵습니다. 대신 각 NFS 또는 SMB 클라이언트의 여러 스레드를 사용하여 여러 파일을 병렬로 쓰고 여러 NFS 또는 SMB 클라이언트를 S3 File Gateway에 동시에 사용하여 게이트웨이 처리량을 극대화하는 것이 좋습니다.

여러 스레드를 사용하면 성능이 크게 향상될 수 있습니다. 그러나 더 많은 스레드를 사용하려면 더 많은 시스템 리소스가 필요하므로 게이트웨이가 증가된 부하에 맞게 크기가 조정되지 않으면 성능에 부정적인 영향을 미칠 수 있습니다. 일반적인 배포에서는 게이트웨이의 최대 하드웨어 및 대역폭 제한에 도달할 때까지 스레드와 클라이언트를 더 추가할 때 더 나은 처리량 성능을 기대할 수 있습니다. 특정 하드웨어 및 네트워크 구성에 대한 속도와 시스템 리소스 사용량 간의 최적의 균형을 찾기 위해 다양한 스레드 수를 실험하는 것이 좋습니다.

스레드 및 클라이언트 구성을 테스트하는 데 도움이 되는 일반적인 도구에 대한 다음 정보를 고려하세요.

- robocopy와 같은 도구를 사용하여 게이트웨이의 파일 공유에 파일 세트를 복사하여 멀티스레드 쓰기 성능을 테스트할 수 있습니다. 기본적으로 robocopy는 파일을 복사할 때 8개의 스레드를 사용하지만 최대 128개의 스레드를 지정할 수 있습니다.

  robocopy와 함께 여러 스레드를 사용하려면 명령에 `/MT:n` 스위치를 추가합니다. 여기서 n은 사용하려는 스레드 수입니다. 예제:

  ```
  robocopy C:\source D:\destination /MT:64
  ```

  이 명령은 복사 작업에 64개의 스레드를 사용합니다.

> **Note**
>
> 이 방법은 단일 스레드로 제한되고 파일을 순차적으로 복사하므로 최대 처리량을 테스트할 때 Windows Explorer를 사용하여 파일을 끌어서 놓지 않는 것이 좋습니다.

자세한 내용은 Microsoft Learn 웹 사이트의 robocopy를 참조하세요.

- DISKSPD 또는 FIO와 같은 일반적인 스토리지 벤치마킹 도구를 사용하여 테스트를 수행할 수도 있습니다. 이러한 도구에는 특정 워크로드 요구 사항에 맞게 스레드 수, I/O 깊이 및 기타 파라미터를 조정할 수 있는 옵션이 있습니다.

  DiskSpd를 사용하면 `-t` 파라미터를 사용하여 스레드 수를 제어할 수 있습니다. 예제:

  ```
  diskspd -c10G -d300 -r -w50 -t64 -o32 -b1M -h -L C:\testfile.dat
  ```

  이 예제 명령에서는 다음을 수행합니다.

  - 10GB 테스트 파일 생성(`-c1G`)
  - 300초 동안 실행(`-d300`)
  - 50% 읽기 50% 쓰기로 임의 I/O 테스트 수행(`-r -w50`)
  - 스레드 64개 사용(`-t64`)
  - 대기열 깊이를 스레드당 32로 설정(`-o32`)
  - 1MB 블록 크기 사용(`-b1M`)
  - 하드웨어 및 소프트웨어 캐시 비활성화(`-h -L`)

  자세한 내용은 Microsoft Learn 웹 사이트에서 DISKSPD를 사용하여 워크로드 스토리지 성능 테스트를 참조하세요.

- FIO는 `numjobs` 파라미터를 사용하여 병렬 스레드 수를 제어합니다. 예제:

  ```
  fio --name=mixed_test --rw=randrw --rwmixread=70 --bs=1M -- iodepth=64
  --size=10G --runtime=300 --numjobs=64 --ioengine=libaio --direct=1 --
  group_reporting
  ```

  이 예제 명령에서는 다음을 수행합니다.

  - 임의 I/O 테스트 수행(`--rw=randrw`)
  - 70% 읽기 및 30% 쓰기 수행(`--rwmixread=70`)

- 1MB 블록 크기 사용(`--bs=1M`)
- I/O 깊이를 64로 설정(`--iodepth=64`)
- 10GB 파일에서 테스트(`--size=10G`)
- 5분 동안 실행(`--runtime=300`)
- 64개의 병렬 작업(스레드) 생성(`--numjobs=64`)
- 비동기 I/O 엔진 사용(`--ioengine=libaio`)
- 더 쉬운 분석을 위해 결과를 그룹화(`--group_reporting`)

  자세한 내용은 Linux 매뉴얼 페이지에서 fio를 참조하세요.

-

자동 캐시 새로 고침 끄기

자동 캐시 새로 고침 기능을 사용하면 S3 File Gateway가 메타데이터를 자동으로 새로 고칠 수 있으므로 게이트웨이를 통하지 않고 Amazon S3 버킷에 직접 작성하여 파일 세트에 대한 사용자 또는 애플리케이션의 변경 사항을 캡처할 수 있습니다. 자세한 내용은 Amazon S3 버킷 객체 캐시 새로 고침을 참조하세요.

게이트웨이 처리량을 최적화하려면 Amazon S3 버킷에 대한 모든 읽기 및 쓰기가 S3 File Gateway를 통해 수행되는 배포에서 이 기능을 끄는 것이 좋습니다.

자동화된 캐시 새로 고침을 구성할 때는 다음 사항을 고려하세요.

- 배포의 사용자 또는 애플리케이션이 때때로 Amazon S3에 직접 쓰기 때문에 자동 캐시 새로 고침을 사용해야 하는 경우 비즈니스 요구 사항에 여전히 실용적인 새로 고침 사이의 가능한 가장 긴 시간 간격을 구성하는 것이 좋습니다. 캐시 새로 고침 간격이 길수록 디렉터리를 검색하거나 파일을 수정할 때 게이트웨이가 수행해야 하는 메타데이터 작업 수를 줄일 수 있습니다.

  예를 들어 워크로드에 대해 허용 가능한 경우 자동 캐시 새로 고침을 5분이 아닌 24시간으로 설정합니다.
- 최소 시간 간격은 5분입니다. 최대 간격은 30일입니다.
- 매우 짧은 캐시 새로 고침 간격을 설정하도록 선택한 경우 NFS 및 SMB 클라이언트의 디렉터리 브라우징 환경을 테스트하는 것이 좋습니다. 게이트웨이 캐시를 새로 고치는 데 걸리는 시간은 Amazon S3 버킷의 파일 및 하위 디렉터리 수에 따라 크게 증가할 수 있습니다.

Amazon S3 업로더 스레드 수 증가

기본적으로 S3 File Gateway는 Amazon S3 데이터 업로드를 위해 8개의 스레드를 열어 대부분의 일반적인 배포에 충분한 업로드 용량을 제공합니다. 그러나 게이트웨이가 표준 8 스레드 용량으로 Amazon S3에 업로드할 수 있는 것보다 높은 속도로 NFS 및 SMB 클라이언트로부터 데이터를 수신할 수 있으며, 이로 인해 로컬 캐시가 스토리지 한도에 도달할 수 있습니다.

특정 상황에서는 게이트웨이의 Amazon S3 업로드 스레드 풀 수를 8개에서 40개로 지원 늘릴 수 있으므로 더 많은 데이터를 병렬로 업로드할 수 있습니다. 대역폭 및 배포와 관련된 기타 요인에 따라 업로드 성능이 크게 향상되고 워크로드를 지원하는 데 필요한 캐시 스토리지 양을 줄이는 데 도움이 될 수 있습니다.

`CachePercentDirty` CloudWatch 지표를 사용하여 Amazon S3에 아직 업로드되지 않은 로컬 게이트웨이 캐시 디스크에 저장된 데이터의 양을 모니터링하고 지원 에 문의하여 업로드 스레드 풀 수를 늘리면 S3 File Gateway의 처리량이 향상될 수 있는지 확인하는 것이 좋습니다. 자세한 내용은 게이트웨이 지표 이해를 참조하세요.

> **Note**
>
> 이 설정은 추가 게이트웨이 CPU 리소스를 사용합니다. 게이트웨이 CPU 사용량을 모니터링하고 필요한 경우 할당된 CPU 리소스를 늘리는 것이 좋습니다.

SMB 제한 시간 설정 증가

S3 File Gateway가 대용량 파일을 SMB 파일 공유에 복사하는 경우 SMB 클라이언트 연결은 장기간 후에 시간 초과될 수 있습니다.

파일 크기와 게이트웨이의 쓰기 속도에 따라 SMB 클라이언트의 SMB 세션 제한 시간 설정을 20분 이상으로 확장하는 것이 좋습니다. 기본값은 300초(5분)입니다. 자세한 내용은 게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생함 섹션을 참조하세요.

호환되는 애플리케이션에 대한 기회 잠금 켜기

기회 잠금 또는 "oplocks"는 새 S3 File Gateway마다 기본적으로 활성화됩니다. 호환되는 애플리케이션과 함께 oplock을 사용하는 경우 클라이언트는 여러 개의 더 작은 작업을 더 큰 작업으로 배치하므로 클라이언트, 게이트웨이 및 네트워크에 더 효율적입니다. Microsoft Office, Adobe Suite 등 클라이언트 측 로컬 캐시를 활용하는 애플리케이션을 사용하는 경우 성능을 크게 개선할 수 있으므로 기회 잠금을 켜 두는 것이 좋습니다.

기회 잠금을 끄면 일반적으로 oplock을 지원하는 애플리케이션이 대용량 파일(50MB 이상)을 훨씬 더 느리게 엽니다. 이 지연은 게이트웨이가 4KB 파트로 데이터를 전송하여 I/O가 높고 처리량이 낮기 때문에 발생합니다.

작업 파일 세트의 크기에 따라 게이트웨이 용량 조정

게이트웨이 용량 파라미터는 게이트웨이가 메타데이터를 로컬 캐시에 저장할 최대 파일 수를 지정합니다. 기본적으로 게이트웨이 용량은 Small로 설정되어 있습니다. 즉, 게이트웨이는 최대 5백만 개의 파일에 대한 메타데이터를 저장합니다. 기본 설정은 Amazon S3에 수억 개 또는 수십억 개의 객체가 있더라도 대부분의 워크로드에서 잘 작동합니다. 일반적인 배포에서는 특정 시간에 작은 하위 집합의 파일만 적극적으로 액세스하기 때문입니다. 이 파일 그룹을 "작업 세트"라고 합니다.

워크로드가 5백만 개 이상의 작업 파일 세트에 정기적으로 액세스하는 경우 게이트웨이는 RAM에 저장되고 루트 디스크에 유지되는 작은 I/O 작업인 캐시 제거를 자주 수행해야 합니다. 게이트웨이가 Amazon S3에서 새 데이터를 가져올 때 게이트웨이 성능에 부정적인 영향을 미칠 수 있습니다.

`IndexEvictions` 지표를 모니터링하여 새 항목을 위한 공간을 확보하기 위해 캐시에서 메타데이터가 제거된 파일 수를 확인할 수 있습니다. 자세한 내용은 게이트웨이 지표 이해를 참조하세요.

`UpdateGatewayInformation` API 작업을 사용하여 일반적인 작업 세트의 파일 수에 맞게 게이트웨이 용량을 늘리는 것이 좋습니다. 자세한 내용은 UpdateGatewayInformation을 참조하세요.

> **Note**
>
> 게이트웨이 용량을 늘리려면 추가 RAM 및 루트 디스크 용량이 필요합니다.
>
> - Small(5백만 파일)에는 최소 16GB의 RAM과 80GB 루트 디스크가 필요합니다.
> - Medium(1천만 파일)에는 최소 32GB의 RAM과 160GB의 루트 디스크가 필요합니다.
> - Large(2천만 파일)에는 64GB의 RAM과 240GB 루트 디스크가 필요합니다.

> **Important**
>
> 게이트웨이 용량은 줄일 수 없습니다.

대규모 워크로드를 위한 여러 게이트웨이 배포

단일 대형 게이트웨이에서 많은 파일 공유를 통합하는 대신 가능하면 워크로드를 여러 게이트웨이로 분할하는 것이 좋습니다. 예를 들어, 자주 사용되지 않는 파일 공유를 다른 게이트웨이에서 그룹화하면서 한 게이트웨이에서 많이 사용되는 파일 공유 하나를 격리할 수 있습니다.

여러 게이트웨이 및 파일 공유를 사용하여 배포를 계획할 때는 다음 사항을 고려하세요.

- 단일 게이트웨이의 최대 파일 공유 수는 50개이지만 게이트웨이에서 관리하는 파일 공유 수는 게이트웨이의 성능에 영향을 미칠 수 있습니다. 자세한 내용은 여러 파일 공유가 있는 게이트웨이에 대한 성능 지침을 참조하세요.
- 각 S3 File Gateway의 리소스는 파티셔닝 없이 모든 파일 공유에서 공유됩니다.
- 사용량이 많은 단일 파일 공유는 게이트웨이에서 다른 파일 공유의 성능에 영향을 미칠 수 있습니다.

> **Note**
>
> 하나 이상의 파일 공유가 읽기 전용이 아닌 한 여러 게이트웨이에서 동일한 Amazon S3 위치에 매핑되는 여러 파일 공유를 생성하는 것은 권장하지 않습니다.
> 여러 게이트웨이에서 동일한 파일에 동시에 쓰는 것은 데이터 무결성 문제를 일으킬 수 있는 다중 라이터 시나리오로 간주됩니다.

SQL Server 데이터베이스 백업을 위한 S3 File Gateway 최적화

데이터베이스 백업은 S3 File Gateway의 일반적인 권장 사용 사례로, Amazon S3에 데이터베이스 백업을 저장하여 비용 효율적인 단기 및 장기 보존을 제공하며 필요에 따라 비용을 절감하는 스토리지 계층을 수명 주기로 제공할 수 있습니다. 이 솔루션을 사용하면 SQL Server Management Studio 및 Oracle RMAN과 같은 기본 제공 도구를 사용하여 엔터프라이즈 백업 애플리케이션의 필요성을 줄일 수 있습니다.

다음 섹션에서는 수백 테라바이트의 SQL 데이터베이스 백업에 대한 최적화된 성능과 비용 효율적인 지원을 위해 S3 File Gateway 배포를 조정하는 모범 사례를 설명합니다. 각 섹션에 제공된 지침은 전체 처리량을 개선하는 데 점진적으로 기여합니다. 이러한 권장 사항은 필요하지 않으며 상호 종속적이지 않지만가 S3 File Gateway 구현을 테스트하고 조정하는 데 지원 사용하는 논리적 방식으로 선택 및 정렬되었습니다. 이러한 제안을 구현하고 테스트할 때 각 S3 File Gateway 배포는 고유하므로 결과가 다를 수 있습니다.

S3 File Gateway는 파일과 객체 간의 기본 1:1 매핑과 함께 업계 표준 NFS 또는 SMB 파일 프로토콜을 사용하여 Amazon S3 객체를 저장하고 검색할 수 있는 파일 인터페이스를 제공합니다. S3 File Gateway를 VMware, Microsoft Hyper-V 또는 Linux KVM 환경의 온프레미스 또는 AWS 클라우드에 Amazon EC2 인스턴스로 가상 머신으로 배포합니다. S3 File Gateway는 전체 엔터프라이즈 NAS 교체로 작동하도록 설계되지 않았습니다. S3 File Gateway는 파일 시스템을 에뮬레이션하지만 파일 시스템은 아닙니다. Amazon S3를 내구성 있는 백엔드 스토리지로 사용하면 각 I/O 작업에 추가 오버헤드가 발생하므로 기존 NAS 또는 파일 서버와 비교하여 S3 File Gateway 성능을 평가하는 것은 동등한 비교가 아닙니다.

SQL Server와 동일한 위치에 게이트웨이 배포

S3 File Gateway 가상 어플라이언스와 SQL 서버 간에 네트워크 지연 시간을 최소화하면서 물리적 위치에 배포하는 것이 좋습니다. 게이트웨이의 위치를 선택할 때 다음 사항을 고려하세요.

- 게이트웨이의 네트워크 지연 시간이 짧으면 SQL 서버와 같은 SMB 클라이언트의 성능을 개선하는 데 도움이 될 수 있습니다.
- S3 File Gateway는 게이트웨이와 클라이언트 간에 비해 게이트웨이와 Amazon S3 간에 더 높은 네트워크 지연 시간을 허용하도록 설계되었습니다.
- Amazon EC2에 배포된 S3 File Gateway 인스턴스의 경우 게이트웨이와 SQL 서버를 동일한 배치 그룹에 유지하는 것이 좋습니다. 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 인스턴스에 대한 배치 그룹을 참조하세요.

느린 디스크로 인한 병목 현상 감소

`IoWaitPercent` CloudWatch 지표를 모니터링하여 S3 File Gateway의 느린 스토리지 디스크로 인해 발생할 수 있는 성능 병목 현상을 식별하는 것이 좋습니다. 디스크 관련 성능 문제를 최적화하려고 할 때는 다음 사항을 고려하세요.

- `IoWaitPercent`는 CPU가 루트 또는 캐시 디스크의 응답을 기다리는 시간의 비율을 보고합니다.
- `IoWaitPercent`가 5~10%보다 크면 일반적으로 성능 저하 디스크로 인한 게이트웨이 성능 병목 현상을 나타냅니다. 이 지표는 가능한 0%에 가까워야 합니다. 즉, 게이트웨이가 디스크를 기다리지 않으므로 CPU 리소스를 최적화하는 데 도움이 됩니다.
- Storage Gateway 콘솔의 모니터링 탭에서 `IoWaitPercent`를 확인하거나 지표가 특정 임계값을 초과하면 자동으로 알리도록 권장 CloudWatch 경보를 구성할 수 있습니다. 자세한 내용은 게이트웨이에 대한 권장 CloudWatch 경보 생성을 참조하세요.

- `IoWaitPercent`를 최소화하려면 게이트웨이의 루트 및 캐시 디스크에 NVMe 또는 SSD를 사용하는 것이 좋습니다.

CPU, RAM 및 캐시 디스크에 대한 S3 File Gateway 가상 머신 리소스 할당 조정

S3 File Gateway의 처리량을 최적화하려는 경우 CPU, RAM 및 캐시 디스크를 포함하여 게이트웨이 VM에 충분한 리소스를 할당하는 것이 중요합니다. CPU 4개, 16GB RAM 및 150GB 캐시 스토리지의 최소 가상 리소스 요구 사항은 일반적으로 더 작은 워크로드에만 적합합니다. 대규모 워크로드에 가상 리소스를 할당할 때는 다음을 권장합니다.

- S3 File Gateway에서 생성되는 일반적인 CPU 사용량에 따라 할당된 CPU 수를 16~48개로 늘립니다. `UserCpuPercent` 지표를 사용하여 CPU 사용량을 모니터링할 수 있습니다. 자세한 내용은 게이트웨이 지표 이해를 참조하세요.
- 할당된 RAM을 32~64GB로 늘립니다.

> **Note**
>
> S3 File Gateway는 64GB를 초과하는 RAM을 사용할 수 없습니다.

- 루트 디스크 및 캐시 디스크에 NVMe 또는 SSD를 사용하고 게이트웨이에 쓰려는 최대 작업 데이터세트에 맞게 캐시 디스크의 크기를 조정합니다. 자세한 내용은 공식 Amazon Web Services YouTube 채널의 S3 File Gateway 캐시 크기 조정 모범 사례를 참조하세요.
- 하나의 대용량 디스크를 사용하는 대신 게이트웨이에 최소 4개의 가상 캐시 디스크를 추가합니다. 여러 가상 디스크는 동일한 기본 물리적 디스크를 공유하더라도 성능을 개선할 수 있지만, 일반적으로 가상 디스크가 서로 다른 기본 물리적 디스크에 있는 경우 성능이 향상됩니다.

  예를 들어 12TB의 캐시를 배포하려는 경우 다음 구성 중 하나를 사용할 수 있습니다.

  - 3TB 캐시 디스크 4개
  - 1.5TB 캐시 디스크 8개
  - 1TB 캐시 디스크 12개

  이를 통해 성능 외에도 시간이 지남에 따라 가상 머신을 보다 효율적으로 관리할 수 있습니다. 워크로드가 변경되면 각 개별 가상 디스크의 원래 크기를 유지하면서 캐시 디스크 수와 전체 캐시 용량을 점진적으로 늘려 게이트웨이 무결성을 유지할 수 있습니다.

  자세한 내용은 로컬 디스크 스토리지 용량 결정을 참조하세요.

S3 File Gateway를 Amazon EC2 인스턴스로 배포할 때는 다음 사항을 고려하세요.

- 선택한 인스턴스 유형은 게이트웨이 성능에 상당한 영향을 미칠 수 있습니다. Amazon EC2는 S3 File Gateway 인스턴스에 대한 리소스 할당을 조정할 수 있는 광범위한 유연성을 제공합니다.
- S3 File Gateway에 권장되는 Amazon EC2 인스턴스 유형은 Amazon EC2 인스턴스 유형에 대한 요구 사항을 참조하세요.
- 활성 S3 File Gateway를 호스팅하는 Amazon EC2 인스턴스 유형을 변경할 수 있습니다. 이를 통해 Amazon EC2 하드웨어 생성 및 리소스 할당을 쉽게 조정하여 이상적인 price-to-performance 비율을 찾을 수 있습니다. 인스턴스 유형을 변경하려면 Amazon EC2 콘솔에서 다음 절차를 사용합니다.

  1. Amazon EC2 인스턴스를 중지합니다.
  2. Amazon EC2 인스턴스 유형을 변경합니다.
  3. Amazon EC2 인스턴스의 전원을 켭니다.

  > **Note**
  >
  > S3 File Gateway를 호스팅하는 인스턴스를 중지하면 파일 공유 액세스가 일시적으로 중단됩니다. 필요한 경우 유지 관리 기간을 예약해야 합니다.

- Amazon EC2 인스턴스의 price-to-performance 비율은 지불한 가격으로 얻을 수 있는 컴퓨팅 성능을 나타냅니다. 일반적으로 최신 세대 Amazon EC2 인스턴스는 이전 세대에 비해 비교적 저렴한 비용으로 최신 하드웨어와 향상된 성능을 갖춘 최상의 price-to-performance 비율을 제공합니다. 인스턴스 유형, 리전 및 사용 패턴과 같은 요소는 이 비율에 영향을 미치므로 비용 효율성을 최적화하려면 특정 워크로드에 적합한 인스턴스를 선택하는 것이 중요합니다.

S3 File Gateway의 보안 수준을 조정하여 SMB 클라이언트 처리량 개선

SMBv3 프로토콜은 성능 및 보안에 일부 장단점이 있는 SMB 서명 및 SMB 암호화를 모두 허용합니다. 처리량을 최적화하기 위해 게이트웨이의 SMB 보안 수준을 조정하여 클라이언트 연결에 적용되는 보안 기능을 지정할 수 있습니다. 자세한 내용은 게이트웨이의 보안 수준 설정을 참조하세요.

SMB 보안 수준을 조정할 때는 다음 사항을 고려하세요.

- S3 File Gateway의 기본 보안 수준은 암호화 적용입니다. 이 설정은 게이트웨이 파일 공유에 대한 SMB 클라이언트 연결에 암호화와 서명을 모두 적용합니다. 즉, 클라이언트에서 게이트웨이로의 모든 트래픽이 암호화됩니다. 이 설정은 게이트웨이에서 로의 트래픽에는 영향을 주지 않으며 AWS,이 트래픽은 항상 암호화됩니다.

게이트웨이는 암호화된 각 클라이언트 연결을 단일 vCPU로 제한합니다. 예를 들어 암호화된 클라이언트가 1개뿐인 경우 게이트웨이에 4개 이상의 vCPU가 할당되더라도 해당 클라이언트는 1개의 vCPU로만 제한됩니다. 따라서 단일 클라이언트에서 S3 File Gateway로의 암호화된 연결에 대한 처리량은 일반적으로 40~60MB/초로 병목 현상이 발생합니다.

- 보안 요구 사항이 보다 완화된 태세를 허용하는 경우 보안 수준을 클라이언트 협상으로 변경할 수 있습니다. 그러면 SMB 암호화가 비활성화되고 SMB 서명만 적용됩니다. 이 설정을 사용하면 게이트웨이에 대한 클라이언트 연결이 여러 vCPU를 활용할 수 있으므로 일반적으로 처리량 성능이 향상됩니다.

> **Note**
>
> S3 File Gateway의 SMB 보안 수준을 변경한 후에는 파일 공유 상태가 Storage Gateway 콘솔에서 업데이트 중에서 사용 가능으로 변경될 때까지 기다린 다음 새 설정이 적용되도록 SMB 클라이언트를 연결 해제했다가 다시 연결해야 합니다.

SQL 백업을 여러 파일로 분할하여 SMB 클라이언트 처리량 개선

- 단일 SQL 서버에서 순차적으로 쓰는 작업은 단일 스레드 작업이므로 한 번에 하나의 SQL 서버만 파일을 쓰는 S3 File Gateway를 사용하면 최대 처리량 성능을 달성하기 어렵습니다. 대신 각 SQL 서버의 여러 스레드를 사용하여 여러 파일을 병렬로 쓰고 여러 SQL 서버를 S3 File Gateway에 동시에 사용하여 게이트웨이 처리량을 극대화하는 것이 좋습니다. SQL 백업을 사용하면 백업을 여러 파일로 분할하면 각 파일이 별도의 스레드를 활용하여 S3 File Gateway 파일 공유에 여러 파일을 동시에 쓸 수 있습니다. 스레드가 많을수록 게이트웨이 제한까지 더 많은 처리량을 달성할 수 있습니다.
- SQL Server는 단일 백업 작업 중에 동시에 여러 파일에 대한 쓰기를 지원합니다. 예를 들어 T-SQL 명령 또는 SQL Server Management Studio(SSMS)를 사용하여 여러 파일 대상을 지정할 수 있습니다. 각 파일은 별도의 스레드를 사용하여 SQL 서버에서 게이트웨이 파일 공유로 데이터를 전송합니다. 이 접근 방식을 사용하면 I/O 처리량이 향상되어 백업 속도와 효율성이 크게 향상될 수 있습니다.

SQL Server 백업을 구성할 때는 다음 사항을 고려하세요.

- SQL Server 관리자는 백업을 여러 파일로 분할하여 백업 시간을 최적화하고 대규모 데이터베이스 백업을 보다 효과적으로 관리할 수 있습니다.
- 사용되는 파일 수는 서버의 스토리지 구성 및 성능 요구 사항에 따라 달라집니다. 대규모 데이터베이스의 경우 백업을 각각 10GB~20GB의 작은 여러 파일로 나누는 것이 좋습니다.

- SQL Server가 백업 중에 쓸 수 있는 파일 수에는 엄격한 제한이 없지만 스토리지 아키텍처 및 네트워크 대역폭과 같은 실용적인 고려 사항이 이 선택을 안내해야 합니다.

자세한 내용은 다음을 참조하세요.

- 여러 파일에 기록하여 SQL Server 43~67% 더 빠르게 백업
- File Gateway를 사용하여 SQL Server 백업을 Amazon S3에 쉽게 저장할 수 있습니다

SMB 제한 시간 설정을 늘려 대용량 파일 복사 실패 방지

S3 File Gateway가 대용량 SQL 백업 파일을 SMB 파일 공유에 복사하는 경우 SMB 클라이언트 연결은 장기간 후에 시간 초과될 수 있습니다. 파일 크기와 게이트웨이의 쓰기 속도에 따라 SQL Server SMB 클라이언트의 SMB 세션 제한 시간 설정을 20분 이상으로 확장하는 것이 좋습니다. 기본값은 300초(5분)입니다. 자세한 내용은 게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생함 섹션을 참조하세요.

Amazon S3 업로더 스레드 수 증가

기본적으로 S3 File Gateway는 Amazon S3 데이터 업로드를 위해 8개의 스레드를 열어 대부분의 일반적인 배포에 충분한 업로드 용량을 제공합니다. 그러나 게이트웨이가 표준 8 스레드 용량으로 Amazon S3에 업로드할 수 있는 것보다 높은 속도로 SQL 서버로부터 데이터를 수신할 수 있으며, 이로 인해 로컬 캐시가 스토리지 한도에 도달할 수 있습니다.

특정 상황에서는 게이트웨이의 Amazon S3 업로드 스레드 풀 수를 8개에서 40개로 지원 늘릴 수 있으므로 더 많은 데이터를 병렬로 업로드할 수 있습니다. 대역폭 및 배포와 관련된 기타 요인에 따라 업로드 성능이 크게 향상되고 워크로드를 지원하는 데 필요한 캐시 스토리지 양을 줄이는 데 도움이 될 수 있습니다.

`CachePercentDirty` CloudWatch 지표를 사용하여 Amazon S3에 아직 업로드되지 않은 로컬 게이트웨이 캐시 디스크에 저장된 데이터의 양을 모니터링하고 지원 에 문의하여 업로드 스레드 풀 수를 늘리면 S3 File Gateway의 처리량이 향상될 수 있는지 확인하는 것이 좋습니다. 자세한 내용은 게이트웨이 지표 이해를 참조하세요.

> **Note**
>
> 이 설정은 추가 게이트웨이 CPU 리소스를 사용합니다. 게이트웨이 CPU 사용량을 모니터링하고 필요한 경우 할당된 CPU 리소스를 늘리는 것이 좋습니다.

자동 캐시 새로 고침 끄기

자동 캐시 새로 고침 기능을 사용하면 S3 File Gateway가 메타데이터를 자동으로 새로 고칠 수 있으므로 게이트웨이를 통하지 않고 Amazon S3 버킷에 직접 작성하여 파일 세트에 대한 사용자 또는 애플리케이션의 변경 사항을 캡처할 수 있습니다. 자세한 내용은 Amazon S3 버킷 객체 캐시 새로 고침을 참조하세요.

게이트웨이 처리량을 최적화하려면 Amazon S3 버킷에 대한 모든 읽기 및 쓰기가 S3 File Gateway를 통해 수행되는 배포에서 이 기능을 끄는 것이 좋습니다.

자동화된 캐시 새로 고침을 구성할 때는 다음 사항을 고려하세요.

- 배포의 사용자 또는 애플리케이션이 때때로 Amazon S3에 직접 쓰기 때문에 자동 캐시 새로 고침을 사용해야 하는 경우 비즈니스 요구 사항에 여전히 실용적인 새로 고침 사이의 가능한 가장 긴 시간 간격을 구성하는 것이 좋습니다. 캐시 새로 고침 간격이 길수록 디렉터리를 검색하거나 파일을 수정할 때 게이트웨이가 수행해야 하는 메타데이터 작업 수를 줄일 수 있습니다.

  예를 들어 워크로드에 대해 허용 가능한 경우 자동 캐시 새로 고침을 5분이 아닌 24시간으로 설정합니다.
- 최소 시간 간격은 5분입니다. 최대 간격은 30일입니다.
- 매우 짧은 캐시 새로 고침 간격을 설정하도록 선택한 경우 SQL 서버의 디렉터리 브라우징 환경을 테스트하는 것이 좋습니다. 게이트웨이 캐시를 새로 고치는 데 걸리는 시간은 Amazon S3 버킷의 파일 및 하위 디렉터리 수에 따라 크게 증가할 수 있습니다.

워크로드를 지원하기 위해 여러 게이트웨이 배포

Storage Gateway는 워크로드를 여러 게이트웨이로 분할하여 수백 개의 SQL 데이터베이스, 여러 SQL Server 및 수백 테라바이트의 백업 데이터가 있는 대규모 환경에서 SQL 백업을 지원할 수 있습니다.

여러 게이트웨이 및 SQL 서버를 사용하여 배포를 계획할 때는 다음 사항을 고려하세요.

- 단일 게이트웨이는 일반적으로 충분한 하드웨어 리소스와 대역폭으로 하루에 최대 20TB를 업로드할 수 있습니다. Amazon S3 업로더 스레드 수를 늘려 하루에 최대 40TB까지 이 제한을 늘릴 수 있습니다.
- proof-of-concept 테스트를 수행하여 성능을 측정하고 배포의 모든 변수를 고려하는 것이 좋습니다. SQL 백업 워크로드의 최대 처리량을 결정한 후 요구 사항에 맞게 게이트웨이 수를 조정할 수 있습니다.

- 시간이 지남에 따라 데이터베이스 수와 데이터베이스 크기가 증가할 수 있으므로 확장을 염두에 두고 솔루션을 설계하는 것이 좋습니다. 증가하는 워크로드를 계속 확장하고 지원하기 위해 필요에 따라 추가 게이트웨이를 배포할 수 있습니다.

데이터베이스 백업 워크로드를 위한 추가 리소스

- 를 사용하여 SQL Server 백업을 Amazon S3에 저장 AWS Storage Gateway
- File Gateway를 사용하여 SQL Server 백업을 Amazon S3에 쉽게 저장할 수 있습니다
- AWS Storage Gateway 를 사용하여 Amazon S3에 Oracle 데이터베이스 백업 저장
- 대규모로 Amazon S3에 Oracle 데이터베이스 백업
- 를 사용하여 SAP ASE 데이터베이스를 Amazon S3에 통합 AWS Storage Gateway
- 한 AWS 히어로가 클라우드 내 백업 AWS Storage Gateway 에 사용하는 방법
- S3 File Gateway 캐시 크기 조정 모범 사례

Security in AWS Storage Gateway

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 클라우드에서 AWS AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS Storage Gateway에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Storage Gateway를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Storage Gateway를 구성하는 방법을 보여줍니다. 또한 Storage Gateway 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

in AWS Storage Gateway의 데이터 보호

AWS 공동 책임 모델 in AWS Storage Gateway의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 이 인프라에 호스팅되는 콘텐츠에 대한 통제 권한을 유지할 책임이 있습니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 관한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용합니다.

- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- 내부의 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Storage Gateway 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명을 URL에 포함해서는 안 됩니다.

를 사용한 데이터 암호화 AWS KMS

Storage Gateway는 SSL/TLS(Secure Socket Layers/Transport Layer Security)를 사용하여 게이트웨이 어플라이언스와 AWS 스토리지 간에 전송되는 데이터를 암호화합니다. 기본적으로 Storage Gateway는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 Amazon S3에 저장되는 모든 데이터에 대해 서버 측 암호화를 수행합니다. Storage Gateway API를 사용하면 AWS Key Management Service (SSE-KMS) 키를 사용하는 서버 측 암호화로 클라우드에 저장된 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다.

파일 공유 암호화

SSE-KMS 또는 DSSE-KMS를 사용하여 AWS KMS관리형 키로 객체를 암호화하도록 S3 File Gateway에서 파일 공유를 구성할 수 있습니다. 지원되는 파일 공유 암호화 방법에 대한 자세한 내용은 Amazon S3의 File Gateway에 저장된 객체 암호화를 참조하세요.

AWS KMS 를 사용하여 데이터를 암호화하는 경우 다음 사항에 유의하세요.

- 데이터는 클라우드에 암호화되어 저장됩니다. 즉, 데이터는 Amazon S3에서 암호화됩니다.

- IAM 사용자는 AWS KMS API 작업을 호출하는 데 필요한 권한이 있어야 합니다. 자세한 내용은AWS Key Management Service 개발자 안내서의 AWS KMS에서 IAM 정책 사용을 참조하세요.

> **Important**
>
> 서버 측 암호화에 AWS KMS 키를 사용하는 경우 대칭 키를 선택해야 합니다. Storage Gateway에서는 비대칭 키가 지원되지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 대칭 및 비대칭 키 사용을 참조하세요.

에 대한 자세한 내용은 란 무엇입니까 AWS Key Management Service?를 AWS KMS참조하십시오.

AWS Storage Gateway의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 AWS SGW 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조문제 해결 AWS Storage Gateway 자격 증명 및 액세스)

- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(IAM에서 AWS Storage Gateway 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(AWS Storage Gateway의 자격 증명 기반 정책 예제 참조)

ID를 통한 인증

인증은 AWS 자격 증명으로에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS Sign-In 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 IAM 사용 설명서의 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

IAM에서 AWS Storage Gateway 작동 방식

IAM을 사용하여 AWS SGW에 대한 액세스를 관리하기 전에 AWS SGW에서 사용할 수 있는 IAM 기능을 알아봅니다.

AWS Storage Gateway와 함께 사용할 수 있는 IAM 기능

IAM 특성	AWS SGW 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACL	아니요
ABAC(정책 내 태그)	부분적
임시 자격 증명	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

AWS SGW 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

AWS SGW에 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 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

AWS SGW에 대한 자격 증명 기반 정책 예제

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요AWS Storage Gateway의 자격 증명 기반 정책 예제.

AWS SGW 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

AWS SGW에 대한 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. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS SGW 작업 목록을 보려면 서비스 승인 참조의AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
sgw
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요AWS Storage Gateway의 자격 증명 기반 정책 예제.

AWS SGW에 대한 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. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS SGW 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 Resources Defined by AWS Storage Gateway를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요AWS Storage Gateway의 자격 증명 기반 정책 예제.

AWS SGW에 사용되는 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` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수

있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS SGW 조건 키 목록을 보려면 서비스 승인 참조의 조건 키 for AWS Storage Gateway를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요AWS Storage Gateway의 자격 증명 기반 정책 예제.

AWS SGWACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS SGW를 사용한 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AWS SGW에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션을 사용하거나 역할을 전환할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것

이 AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는AWS 서비스 섹션을 참조하세요.

AWS SGW에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS SGW에 대한 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 AWS SGW 기능이 중단될 수 있습니다. AWS SGW가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS SGW에 대한 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 나타나 AWS 계정 며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

AWS Storage Gateway의 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS SGW 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS SGW에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Actions, Resources, and Condition Keys for AWS Storage Gateway를 참조하세요.

주제

- 정책 모범 사례
- AWS SGW 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS SGW 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하

여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.

- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정캡니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS SGW 콘솔 사용

AWS Storage Gateway 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 AWS SGW 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 여전히 AWS SGW 콘솔을 사용할 수 있도록 하려면 AWS SGW *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여 줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

문제 해결 AWS Storage Gateway 자격 증명 및 액세스

다음 정보를 사용하여 AWS SGW 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- AWS SGW에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 AWS SGW 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

AWS SGW에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `sgw:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

이 경우, sgw:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS SGW에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예시 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS SGW에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

> **Important**
>
> Storage Gateway는 iam:PassRole 정책 작업을 사용하여 전달된 기존 서비스 역할을 수임할 수 있지만 iam:PassedToService 컨텍스트 키를 사용하여 작업을 특정 서비스로 제한하는 IAM 정책은 지원하지 않습니다.
> 자세한 내용은AWS Identity and Access Management 사용 설명서에서 다음 주제를 참조하세요.
>
> - IAM: 특정 AWS 서비스에 IAM 역할 전달
> - 사용자에게 AWS 서비스에 역할을 전달할 수 있는 권한 부여
> - IAM에 사용 가능한 키

내 외부의 사람이 내 AWS SGW 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- SGW AWS 가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요IAM에서 AWS Storage Gateway 작동 방식.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.
- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

태그를 사용하여 게이트웨이 및 리소스에 대한 액세스 제어

게이트웨이 리소스 및 작업에 대한 액세스를 제어하기 위해 태그를 기반으로 AWS Identity and Access Management (IAM) 정책을 사용할 수 있습니다. 두 가지 방법으로 제어할 수 있습니다.

1. 해당 리소스의 태그를 기반으로 게이트웨이 리소스에 대한 액세스를 제어합니다.
2. IAM 요청 조건에 어떤 태그가 전달될 수 있는지를 제어합니다.

태그를 사용하여 액세스를 제어하는 자세한 방법은 태그를 사용하여 액세스 제어를 참조하세요.

리소스의 태그를 기반으로 액세스 제어

사용자나 역할이 게이트웨이 리소스에서 어떤 작업을 수행할 수 있는지를 제어하려면 게이트웨이 리소스의 태그를 사용할 수 있습니다. 예를 들어, 리소스에 있는 태그의 키-값 페어를 기반으로 File Gateway 리소스에서 특정 API 작업을 허용하거나 거부할 수 있습니다.

다음 예제는 사용자나 역할이 모든 리소스에서 `ListTagsForResource`, `ListFileShares` 및 `DescribeNFSFileShares` 작업을 수행할 수 있도록 허용합니다. 정책은 리소스의 태그에 `allowListAndDescribe`로 설정된 키와 `yes`로 설정된 값이 있을 경우에만 적용됩니다.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListTagsForResource",
                "storagegateway:ListFileShares",
                "storagegateway:DescribeNFSFileShares"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/allowListAndDescribe": "yes"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "storagegateway:*"
            ],
            "Resource": "arn:aws:storagegateway:us-east-1:111122223333:*/*"
        }
    ]
}
```

IAM 요청의 태그를 기반으로 액세스 제어

사용자가 게이트웨이 리소스에서 무엇을 수행할 수 있는지를 제어하려면 태그를 기반으로 IAM 정책의 조건을 사용할 수 있습니다. 예를 들어 사용자가 리소스를 생성할 때 제공한 태그를 기반으로 특정 API 작업을 수행할 수 있도록 허용하거나 거부하는 정책을 작성할 수 있습니다.

다음 예제에서 첫 번째 명령문은 게이트웨이를 생성할 때 제공한 키-값 페어가 **Department** 및 **Finance**인 경우에만 사용자가 게이트웨이를 생성할 수 있도록 허용합니다. API 작업을 사용할 경우 이 태그를 활성화 요청에 추가합니다.

두 번째 명령문은 게이트웨이의 태그 키-값 페어가 **Department** 및 **Finance**와 일치할 경우에만 사용자가 게이트웨이에서 NFS(Network File System) 또는 SMB(Server Message Block) 공유를 생성할 수 있도록 허용합니다. 또한 사용자는 태그를 파일 공유에 추가해야 하며, 태그의 키-값 페어는 **Department** 및 **Finance**여야 합니다. 파일 공유를 생성할 때 파일 공유에 태그를 추가할 수 있습니다. AddTagsToResource 또는 RemoveTagsFromResource 작업에 대한 권한은 없기 때문에 사용자는 게이트웨이나 파일 공유에서 이러한 작업을 수행할 수 없습니다.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:ActivateGateway"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:RequestTag/Department":"Finance"
            }
         }
      },
      {
         "Effect":"Allow",
         "Action":[
            "storagegateway:CreateNFSFileShare",
            "storagegateway:CreateSMBFileShare"
         ],
         "Resource":"*",
         "Condition":{
            "StringEquals":{
               "aws:ResourceTag/Department":"Finance",
               "aws:RequestTag/Department":"Finance"
            }
         }
```

```
        }
    ]
}
```

Windows ACL을 사용하여 SMB 파일 공유 액세스 제한

Amazon S3 File Gateway는 SMB 파일 공유를 통해 저장된 파일 및 디렉터리에 대한 액세스를 제어하는 두 가지 방법, 즉 POSIX 권한 또는 Windows ACL을 지원합니다.

이 섹션에서는 인증에 Microsoft Active Directory(AD)를 사용하는 SMB 파일 공유에서 Microsoft Windows 액세스 제어 목록(ACL)을 사용하는 방법을 설명합니다. Windows ACL을 사용하여 SMB 파일 공유에서 파일 및 폴더에 대한 세분화된 권한을 설정할 수 있습니다.

다음은 SMB 파일 공유에서 Windows ACL의 몇 가지 중요한 특징입니다.

- File Gateway가 Active Directory 도메인에 조인될 때 SMB 파일 공유에 대해 Windows ACL이 기본적으로 선택됩니다.
- ACL이 활성화되면 Amazon S3 객체 메타데이터에 ACL 정보가 유지됩니다.
- 게이트웨이는 파일 또는 폴더당 최대 10개의 ACL을 유지합니다.
- ACL이 활성화된 SMB 파일 공유를 사용하여 게이트웨이 밖에서 생성된 S3 객체에 액세스하면 객체들이 상위 폴더에서 ACL 정보를 상속합니다.

> **Note**
>
> SMB 파일 공유용 기본 루트 ACL은 모두에게 전체 액세스 권한을 부여하지만 루트 ACL의 권한을 변경할 수 있습니다. 루트 ACL을 사용하여 파일 공유에 대한 액세스를 제어할 수 있습니다. 파일 공유를 마운트(드라이브 매핑)할 수 있는 주체와 파일 공유에서 사용자가 파일과 폴더에 대해 반복해서 받을 수 있는 권한을 설정할 수 있습니다. 그렇지만 ACL이 유지되도록 S3 버킷의 최상위 폴더에 이 권한을 설정하는 것이 좋습니다.

새 SMB 파일 공유를 생성할 때 CreateSMBFileShare API 작업을 사용하여 Windows ACL을 활성화할 수 있습니다. 또는 UpdateSMBFileShare API 작업을 사용하여 기존 SMB 파일에 Windows ACL을 활성화할 수 있습니다.

새 SMB 파일 공유에 Windows ACL 활성화

다음 단계에 따라 새 SMB 파일 공유에 Windows ACL을 활성화합니다.

SMB 파일 공유를 생성할 때 Windows ACL을 활성화하려면

1. File Gateway가 아직 없다면 지금 만드세요. 자세한 내용은 게이트웨이 생성 단원을 참조하십시오.
2. 게이트웨이가 도메인에 조인되어 있지 않으면 도메인에 추가하십시오. 자세한 내용은 Active Directory를 사용하여 사용자 인증을 참조하세요.
3. SMB 파일 공유를 생성하십시오. 자세한 내용은 다음 섹션을 참조하세요.
4. Storage Gateway 콘솔에서 파일 공유의 Windows ACL을 활성화합니다.

   Storage Gateway 콘솔을 사용하려면 다음을 수행합니다.

   a. 파일 공유를 선택하고 파일 공유 편집을 선택합니다.

   b. 제어되는 파일/디렉터리 액세스 옵션에서 Windows 액세스 제어 목록을 선택합니다.
5. (선택 사항) 파일 공유의 모든 파일과 폴더에 ACL을 업데이트할 권한을 관리자 사용자에게 부여하려면 AdminUsersList에 관리자 사용자를 추가합니다.

   > **Note**
   >
   > SMB 파일 공유의 설정에서 허용 및 거부된 사용자 및 그룹 목록을 구성한 경우 ACL은 해당 목록을 재정의하는 액세스 권한을 부여하지 않습니다.
   > 허용 및 거부된 사용자 및 그룹 목록은 ACL보다 먼저 평가되며 파일 공유를 탑재하거나 액세스할 수 있는 사용자를 제어합니다. 허용 목록에 사용자 또는 그룹이 있는 경우 해당 목록은 활성으로 간주되며 해당 사용자만 파일 공유를 탑재할 수 있습니다.
   > 사용자가 파일 공유를 탑재한 후 ACL은 사용자가 액세스할 수 있는 특정 파일 또는 폴더를 제어하는 보다 세분화된 보호를 제공합니다.
6. 루트 폴더 아래에 상위 폴더의 ACL을 업데이트합니다. 그럴려면 Windows File Explorer를 사용하여 SMB 파일 공유의 폴더에 ACL을 구성합니다.

   > **Note**
   >
   > 루트 아래에 있는 상위 폴더 대신 루트에 ACL을 구성할 경우에는 ACL 권한이 Amazon S3에 유지되지 않습니다.

   파일 공유의 루트에서 직접 ACL을 설정하지 맑 파일 공유의 루트 아래에 있는 최상위 폴더에 ACL을 설정하는 것이 좋습니다. 이렇게 하면 정보가 객체 메타데이터로 Amazon S3에 유지됩니다.

7. 필요에 따라 상속을 켭니다.

> **Note**
>
> 2019년 5월 8일 이후에 생성한 파일 공유의 상속을 활성화할 수 있습니다.

상속을 활성화하고 권한을 재귀적으로 업데이트하면 Storage Gateway가 S3 버킷의 모든 객체를 업데이트합니다. 버킷의 객체 수에 따라 업데이트를 완료하는 데 시간이 걸릴 수 있습니다.

기존 SMB 파일 공유에서 Windows ACL 활성화

다음 단계에 따라 POSIX 권한이 있는 기존 SMB 파일 공유에서 Windows ACL을 활성화합니다.

Storage Gateway 콘솔을 사용하여 기존 SMB 파일 공유에서 Windows ACL을 활성화하려면

1. 파일 공유를 선택하고 파일 공유 편집을 선택합니다.
2. 제어되는 파일/디렉터리 액세스 옵션에서 Windows 액세스 제어 목록을 선택합니다.
3. 필요에 따라 상속을 켭니다.

> **Note**
>
> ACL을 루트 레벨에 설정하는 것은 권장하지 않습니다. 이 경우 게이트웨이를 삭제하면 ACL을 다시 재설정해야 하기 때문입니다.

상속을 활성화하고 권한을 재귀적으로 업데이트하면 Storage Gateway가 S3 버킷의 모든 객체를 업데이트합니다. 버킷의 객체 수에 따라 업데이트를 완료하는 데 시간이 걸릴 수 있습니다.

Windows ACL을 사용할 때의 제한 사항

Windows ACL을 사용하여 SMB 파일 공유에 대한 액세스를 제어할 때 다음과 같은 제한 사항을 명심해야 합니다.

- Windows ACL은 Windows SMB 클라이언트를 사용하여 파일 공유에 액세스할 때 인증을 위해 Active Directory를 사용하는 파일 공유에서만 지원됩니다.
- File Gateway는 각 파일과 디렉터리에 대해 최대 10개의 ACL 항목을 지원합니다.
- File Gateway는 시스템 액세스 제어 목록(SACL) 항목인 `Audit` 및 `Alarm` 항목을 지원하지 않습니다. File Gateway는 임의 액세스 제어 목록(DACL) 항목인 `Allow` 및 `Deny` 항목을 지원합니다.

- File Gateway는 고급 액세스 제어 항목(ACE) 권한을 지원하지 않습니다.
- SMB 파일 공유의 루트 ACL 설정은 게이트웨이에만 있으며, 게이트웨이 업데이트 및 재시작 시 유지됩니다.

> **Note**
>
> 루트 아래에 있는 상위 폴더 대신 루트에 ACL을 구성할 경우에는 ACL 권한이 Amazon S3에 유지되지 않습니다.

이러한 조건을 고려하여 다음을 수행해야 합니다.

- 동일한 Amazon S3 버킷에 액세스할 여러 게이트웨이를 구성할 경우에는 각 게이트웨이마다 루트 ACL을 구성하여 권한을 유지하십시오.
- 파일 공유를 삭제하고 동일 Amazon S3 버킷에서 다시 생성할 경우에는 동일한 루트 ACL 세트를 사용해야 합니다.

AWS Storage Gateway에 대한 규정 준수 검증

타사 감사자는 여러 규정 준수 프로그램의 일환으로 AWS Storage Gateway의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, C5, K-ISMS, ENS High, OSPAR 및 HITRUST CSF가 포함됩니다.

특정 규정 준수 프로그램의 범위에 속하는 AWS 서비스 목록은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 . 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 에서 보고서 다운로드 AWS Artifact에서 .

Storage Gateway 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS 에서는 규정 준수에 도움이 되도록 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 -이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- HIPAA 보안 및 규정 준수 백서 설계 -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 준수 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.

- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub CSPM -이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수 여부를 확인하는 데 도움이 AWS 되는 내 보안 상태에 대한 포괄적인 보기를 제공합니다.

Resilience in AWS Storage Gateway

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.

AWS 리전 는 데이터 센터가 클러스터링되는 전 세계의 물리적 위치입니다. 논리적 데이터 센터의 각 그룹을 가용 영역(AZ)이라고 합니다. 각 AWS 리전 은 지리적 영역 내에서 물리적으로 분리되어 격리된 최소 3개의 AZ로 구성됩니다. 리전을 단일 데이터 센터로 정의하는 다른 클라우드 공급자와 달리 모든의 다중 AZ 설계 AWS 리전 는 고유한 이점을 제공합니다. 각 AZ는 독립적인 전원, 냉각, 물리적 보안을 갖추고 있으며 이중화된 초저지연 네트워크를 통해 연결됩니다. 고가용성에 중점을 두고 배포해야 하는 경우, 서비스 및 리소스를 여러 AZ에 구성하여 내결함성을 높일 수 있습니다.

AWS 리전 는 최고 수준의 인프라 보안, 규정 준수 및 데이터 보호를 충족합니다. AZ 간에 전송되는 모든 트래픽은 암호화됩니다. 네트워크 성능은 AZ 간 동기식 복제를 수행하기에 충분합니다. AZ를 사용하면 고가용성을 위한 서비스 및 리소스를 쉽게 분할할 수 있습니다. 배포가 여러 AZ에 분할되어 있으면 정전, 낙뢰, 토네이도, 지진 등의 문제로부터 리소스를 더 잘 격리하고 보호할 수 있습니다. AZ는 물리적으로 다른 AZ와 의미 있는 거리만큼 떨어져 있지만, 모두 서로 100km(60마일) 이내에 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 Storage Gateway는 VMware vSphere 고가용성(VMware HA)을 지원하여 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호합니다. 자세한 내용은 Storage Gateway와 함께 VMware vSphere High Availability 사용을 참조하세요.

인프라 보안 in AWS Storage Gateway

관리형 서비스인 AWS Storage Gateway는 Security Pillar - AWS Well-Architected Framework에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Storage Gateway에 액세스합니다. 클라이언트가 Transport Layer Security(TLS) 1.2를 지원해야 합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 Perfect Forward Secrecy(PFS)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 위탁자와 관련된 시크릿 액세스 키를 사용하여 서명해야 합니다. 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

> **Note**
>
> AWS Storage Gateway 어플라이언스를 관리형 가상 머신으로 취급해야 하며 어떤 식으로든 설치에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 게이트웨이 업데이트 메커니즘이 아닌 다른 방법을 사용하여 스캔 소프트웨어를 설치하거나 소프트웨어 패키지를 업데이트하려고 하면 게이트웨이가 오작동할 수 있으며 게이트웨이 지원 또는 수정 기능에 영향을 미칠 수 있습니다.
>
> AWS 정기적으로 CVEs를 검토, 분석 및 수정합니다. 이러한 문제에 대한 수정 사항은 일반적인 소프트웨어 릴리스 주기의 일부로 Storage Gateway에 통합됩니다. 이러한 수정 사항은 일반적으로 예정된 유지 관리 기간 동안 일반 게이트웨이 업데이트 프로세스의 일부로 적용됩니다. 게이트웨이 업데이트에 대한 자세한 내용은 콘솔을 사용하여 게이트웨이 업데이트 관리 AWS Storage Gateway 콘솔을 .

AWS 보안 모범 사례

AWS 는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 사례는 사용자의 환경에 적절하지 않거나 충분하지 않을 수 있으므로 규정이 아닌 참고용으로만 사용하세요. 자세한 내용은 AWS 보안 모범 사례를 참조하세요.

에서 로깅 및 모니터링 AWS Storage Gateway

Storage Gateway는 Storage Gateway에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Storage Gateway에 대한 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Storage Gateway 콘솔에서의 호출과 Storage Gateway API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Storage Gateway용 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Storage Gateway에 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 Storage Gateway 정보

CloudTrail은 AWS 계정을 생성할 때 계정에서 활성화됩니다. Storage Gateway에서 활동이 발생하면 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기록됩니다. AWS 계정에서 최근 이벤트를 보고 검색하고 다운로드할 수 있습니다. 자세한 설명은 CloudTrail 이벤트 기록으로 이벤트 보기를 참조하세요.

Storage Gateway에 대한 이벤트를 포함하여 AWS 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 추적을 생성하면 추적이 모든 AWS 리전에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성
- 여러 리전으로부터 CloudTrail 로그 파일 받기 및 여러 계정으로부터 CloudTrail 로그 파일 받기

모든 Storage Gateway 작업은 로깅되며 작업 주제에서 문서화됩니다. 예를 들어 `ActivateGateway`, `ListGateways` 및 `ShutdownGateway` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부입니다.

자세한 설명은 CloudTrail userIdentity 요소를 참조하세요.

Storage Gateway 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의

단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 작업을 보여주는 CloudTrail 로그 항목이 나타냅니다.


```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

다음 예는 ListGateways 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
 "Records": [{
               "eventVersion": "1.02",
               "userIdentity": {
                                "type": "IAMUser",
                                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                                "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                                "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                                " userName ":" JohnDoe "
                                },

                                " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                                " eventSource ":" storagegateway.amazonaws.com ",
                                " eventName ":" ListGateways ",
                                " awsRegion ":" us-east-2 ",
                                " sourceIPAddress ":" 192.0.2.0 ",
                                " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                                " requestParameters ":null,
                                " responseElements ":null,
                                "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                                " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                                " eventType ":" AwsApiCall ",
                                " apiVersion ":" 20130630 ",
                                " recipientAccountId ":" 444455556666"
             }]
}
```

Storage Gateway 배포 문제 해결

다음에서 게이트웨이, 호스트 플랫폼, 가상 테이프, 고가용성, 데이터 복구 및 보안과 관련된 모범 사례 및 문제 해결에 관한 정보를 찾을 수 있습니다. 온프레미스 게이트웨이 문제 해결 정보는 지원되는 가상화 플랫폼에 배포된 게이트웨이를 다룹니다. 고가용성 문제에 대한 문제 해결 정보는 VMware vSphere HA(고가용성) 플랫폼에서 실행 중인 게이트웨이를 다룹니다.

주제

- 문제 해결: 게이트웨이 오프라인 문제 - Storage Gateway 콘솔에서 게이트웨이가 오프라인으로 표시될 수 있는 문제를 진단하는 방법에 대해 알아봅니다.
- 문제 해결: Active Directory 문제 - File Gateway를 Microsoft Active Directory 도메인에 조인하려고 할 때 `NETWORK_ERROR`, `TIMEOUT` 또는 `ACCESS_DENIED`와 같은 오류 메시지가 수신되면 어떻게 해야 하는지 알아봅니다.
- 문제 해결: 게이트웨이 활성화 문제 - Storage Gateway 활성화를 시도할 때 내부 오류 메시지가 표시되는 경우에 취해야 할 조치에 대해 알아봅니다.
- 문제 해결: 온프레미스 게이트웨이 문제 - 온프레미스 게이트웨이 작업 시 발생할 수 있는 일반적인 문제와가 게이트웨이에 지원 연결하여 문제 해결을 지원하는 방법을 알아봅니다.
- 문제 해결: Microsoft Hyper-V 설정 관련 문제 - Microsoft Hyper-V 플랫폼에 Storage Gateway를 배포할 때 발생할 수 있는 일반적인 문제에 대해 알아봅니다.
- 문제 해결: Amazon EC2 게이트웨이 문제 - Amazon EC2에 배포된 게이트웨이로 작업할 때 발생할 수 있는 일반적인 문제에 대한 정보를 찾을 수 있습니다.
- 문제 해결: 하드웨어 어플라이언스 문제 - AWS Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제를 해결하는 방법을 알아봅니다.
- 문제 해결: File Gateway 문제 - File Gateway의 CloudWatch 로그에 나타나는 오류 및 상태 알림의 원인을 이해하는 데 도움이 되는 정보를 찾습니다.
- 문제 해결: 파일 공유 문제 - 파일 공유에 예기치 않은 문제가 발생하는 경우 취할 수 있는 조치에 대해 알아봅니다.
- 문제 해결: 고가용성 문제 - VMware HA 환경에 배포된 게이트웨이에 문제가 발생하는 경우 취해야 할 조치에 대해 알아봅니다.

문제 해결: Storage Gateway 콘솔에서 게이트웨이 오프라인

다음 문제 해결 정보를 참조하여 AWS Storage Gateway 콘솔에서 게이트웨이가 오프라인 상태인 것으로 표시되는 경우에 취해야 할 조치를 결정하세요.

다음 중 하나 이상의 이유로 게이트웨이가 오프라인으로 표시될 수 있습니다.

- 게이트웨이가 Storage Gateway 서비스 엔드포인트에 연결할 수 없습니다.
- 게이트웨이가 예기치 않게 종료되었습니다.
- 게이트웨이와 연결된 캐시 디스크가 연결 해제 또는 수정되었거나 실패했습니다.

게이트웨이를 다시 온라인 상태로 되돌리려면 게이트웨이를 오프라인 상태로 만든 문제를 파악하여 해결합니다.

연결된 방화벽 또는 프록시 확인

프록시를 사용하도록 게이트웨이를 구성했거나 게이트웨이를 방화벽 뒤에 배치한 경우 프록시 또는 방화벽의 액세스 규칙을 검토합니다. 프록시 또는 방화벽은 Storage Gateway에 필요한 네트워크 포트 및 서비스 엔드포인트와의 트래픽을 허용해야 합니다. 자세한 내용은 네트워크 및 방화벽 요구 사항을 참조하세요.

게이트웨이 트래픽에 대해 SSL 또는 딥패킷 검사가 진행 중인지 확인

게이트웨이와 간의 네트워크 트래픽에 대해 SSL 또는 딥 패킷 검사가 현재 수행 중인 AWS경우 게이트웨이가 필요한 서비스 엔드포인트와 통신하지 못할 수 있습니다. 게이트웨이를 다시 온라인 상태로 되돌리려면 검사를 비활성화해야 합니다.

재부팅 또는 소프트웨어 업데이트 후 IOWaitPercent 지표 확인

재부팅 또는 소프트웨어 업데이트 후 File Gateway의 `IOWaitPercent` 지표가 10 이상인지 확인합니다. 이 경우 인덱스 캐시를 RAM에 다시 빌드하는 동안 게이트웨이의 응답 속도가 느려질 수 있습니다. 자세한 내용은 문제 해결: CloudWatch 지표 사용을 참조하세요.

하이퍼바이저 호스트의 정전 또는 하드웨어 장애 확인

게이트웨이의 하이퍼바이저 호스트에서 정전 또는 하드웨어 장애가 발생하면 게이트웨이가 예기치 않게 종료되어 연결이 불가능해질 수 있습니다. 전원 및 네트워크 연결을 복원하면 게이트웨이에 다시 연결할 수 있게 됩니다.

게이트웨이가 다시 온라인 상태가 되면 데이터 복구 조치를 취해야 합니다. 자세한 내용은 모범 사례: 데이터 복구를 참조하세요.

연결된 캐시 디스크에 문제가 있는지 확인

게이트웨이와 연결된 캐시 디스크 중 하나 이상이 제거, 변경 또는 크기 조정되었거나 손상된 경우 게이트웨이가 오프라인 상태가 될 수 있습니다.

하이퍼바이저 호스트에서 작동 중인 캐시 디스크를 제거한 경우

1. 게이트웨이를 종료합니다.
2. 디스크를 다시 추가합니다.

   > **Note**
   >
   > 동일한 디스크 노드에 디스크를 추가해야 합니다.

3. 게이트웨이를 다시 시작합니다.

캐시 디스크가 손상되었거나 교체되었거나 크기가 조정된 경우

- 기존 S3 File Gateway를 새 인스턴스로 교체에 설명된 방법 2 절차에 따라 새 게이트웨이를 설정하고 AWS 클라우드에서 캐시 디스크 정보를 다시 다운로드합니다.

문제 해결: 게이트웨이를 Active Directory에 조인하는 문제

다음 문제 해결 정보를 사용하여 File Gateway를 Microsoft Active Directory 도메인에 조인하려고 할 때 `NETWORK_ERROR`, `TIMEOUT` 또는 `ACCESS_DENIED`와 같은 오류 메시지가 수신되는 경우 수행할 작업을 결정합니다.

이러한 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

nping 테스트를 실행하여 게이트웨이가 도메인 컨트롤러에 도달할 수 있는지 확인

nping 테스트를 실행하려면:

1. 온프레미스 게이트웨이용 하이퍼바이저 관리 소프트웨어(VMware, Hyper-V 또는 KVM) 또는 Amazon EC2 게이트웨이용 ssh를 사용하여 게이트웨이 로컬 콘솔에 연결합니다.

2. 해당 숫자를 입력하여 게이트웨이 콘솔을 선택한 다음 h를 입력하여 사용 가능한 모든 명령을 나열합니다. Storage Gateway 가상 머신과 도메인 간의 연결을 테스트하려면 다음 명령을 실행합니다.

   ```
   nping -d corp.domain.com -p 389 -c 1 -t tcp
   ```

   > **Note**
   >
   > corp.domain.com을 Active Directory 도메인 DNS 이름으로 바꾸고 389를 환경의 LDAP 포트로 바꿉니다.
   > 방화벽 내에서 필요한 포트를 열었는지 확인합니다.

다음은 게이트웨이가 도메인 컨트롤러에 도달할 수 있었던 성공적인 nping 테스트의 예입니다.

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:24 UTC
SENT (0.0553s) TCP 10.10.10.21:9783 > 10.10.10.10:389 S ttl=64 id=730 iplen=40
 seq=2597195024 win=1480
RCVD (0.0556s) TCP 10.10.10.10:389 > 10.10.10.21:9783 SA ttl=128 id=22332 iplen=44
 seq=4170716243 win=8192 <mss 8961>

Max rtt: 0.310ms | Min rtt: 0.310ms | Avg rtt: 0.310ms
Raw packets sent: 1 (40B) | Rcvd: 1 (44B) | Lost: 0 (0.00%)
Nping done: 1 IP address pinged in 1.09 seconds<br>
```

다음은 corp.domain.com 대상과의 연결 또는 응답이 없는 nping 테스트의 예입니다.

```
nping -d corp.domain.com -p 389 -c 1 -t tcp

Starting Nping 0.6.40 ( http://nmap.org/nping ) at 2022-06-30 16:26 UTC
SENT (0.0421s) TCP 10.10.10.21:47196 > 10.10.10.10:389  S ttl=64 id=30318 iplen=40
 seq=1762671338 win=1480

Max rtt: N/A | Min rtt: N/A | Avg rtt: N/A
Raw packets sent: 1 (40B) | Rcvd: 0 (0B) | Lost: 1 (100.00%)
Nping done: 1 IP address pinged in 1.07 seconds
```

Amazon EC2 게이트웨이 인스턴스의 VPC에 설정된 DHCP 옵션 확인

File Gateway가 Amazon EC2 인스턴스에서 실행 중인 경우 DHCP 옵션 세트가 올바르게 구성되고 게이트웨이 인스턴스가 포함된 Amazon Virtual Private Cloud(Amazon VPC)에 연결되어 있는지 확인해야 합니다. 자세한 정보는 Amazon VPC의 DHCP 옵션 세트를 참조하세요.

게이트웨이가 dig 쿼리를 실행하여 도메인을 확인할 수 있는지 확인

게이트웨이에서 도메인을 확인할 수 없는 경우 게이트웨이는 도메인에 조인할 수 없습니다.

dig 쿼리를 실행하려면:

1. 온프레미스 게이트웨이용 하이퍼바이저 관리 소프트웨어(VMware, Hyper-V 또는 KVM) 또는 Amazon EC2 게이트웨이용 ssh를 사용하여 게이트웨이 로컬 콘솔에 연결합니다.
2. 해당 숫자를 입력하여 게이트웨이 콘솔을 선택한 다음 h를 입력하여 사용 가능한 모든 명령을 나열합니다. 게이트웨이가 도메인을 확인할 수 있는지 테스트하려면 다음 명령을 실행합니다.

   ```
   dig -d corp.domain.com
   ```

   > **Note**
   >
   > `corp.domain.com`을 Active Directory 도메인 DNS 이름으로 바꿉니다.

다음은 성공적인 응답의 예입니다.

```
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.amzn2.5.2 <<>> corp.domain.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24817
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4000
;; QUESTION SECTION:
;corp.domain.com.        IN    A

;; ANSWER SECTION:
corp.domain.com.    600    IN    A    10.10.10.10
corp.domain.com.    600    IN    A    10.10.20.10
```

```
;; Query time: 0 msec
;; SERVER: 10.10.20.228#53(10.10.20.228)
;; WHEN: Thu Jun 30 16:36:32 UTC 2022
;; MSG SIZE  rcvd: 78
```

도메인 컨트롤러 설정 및 역할 확인

도메인 컨트롤러가 읽기 전용으로 설정되어 있지 않고 도메인 컨트롤러에 컴퓨터가 조인할 수 있는 충분한 역할이 있는지 확인합니다. 이를 테스트하려면 게이트웨이 VM과 동일한 VPC 서브넷의 다른 서버를 도메인에 조인해 보십시오.

게이트웨이가 가장 가까운 도메인 컨트롤러에 조인되었는지 확인

게이트웨이 어플라이언스와 지리적으로 가까운 도메인 컨트롤러에 게이트웨이를 조인하는 것이 좋습니다. 게이트웨이 어플라이언스가 네트워크 지연 시간으로 인해 20초 이내에 도메인 컨트롤러와 통신할 수 없는 경우 도메인 조인 프로세스가 시간 초과될 수 있습니다. 예를 들어 게이트웨이 어플라이언스가 미국 동부(버지니아 북부)에 AWS 리전 있고 도메인 컨트롤러가 아시아 태평양(싱가포르)에 있는 경우 프로세스가 시간 초과될 수 있습니다 AWS 리전.

> **Note**
>
> 기본 제한 시간 값을 20초로 늘리려면 AWS Command Line Interface (AWS CLI)에서 join-domain 명령을 실행하고 시간을 늘리는 `--timeout-in-seconds` 옵션을 포함할 수 있습니다. JoinDomain API 호출을 사용하고 `TimeoutInSeconds` 파라미터를 포함하여 시간을 늘릴 수도 있습니다. 최대 제한 시간 값은 3,600초입니다.
> AWS CLI 명령을 실행할 때 오류가 발생하면 최신 AWS CLI 버전을 사용하고 있는지 확인합니다.

Active Directory가 기본 조직 단위(OU)에 새 컴퓨터 객체를 생성하는지 확인

Microsoft Active Directory에 기본 OU 이외의 위치에 새 컴퓨터 객체를 생성하는 그룹 정책 객체가 없는지 확인합니다. 게이트웨이를 Active Directory 도메인에 조인하려면 먼저 기본 OU에 새 컴퓨터 객체가 있어야 합니다. 일부 Active Directory 환경은 새로 생성된 객체에 대해 서로 다른 OU를 갖도록 사용자 지정됩니다. 게이트웨이 VM의 새 컴퓨터 객체가 기본 OU에 있는지 확인하려면 게이트웨이를 도메인에 조인하기 전에 도메인 컨트롤러에서 수동으로 컴퓨터 객체를 생성해 보십시오. AWS CLI를 사용하여 join-domain 명령을 실행할 수도 있습니다. 그런 다음 `--organizational-unit`에 대한 옵션을 지정합니다.

> **Note**
>
> 컴퓨터 객체를 생성하는 프로세스를 사전 스테이징이라고 합니다.

도메인 컨트롤러 이벤트 로그 확인

이전 섹션에 설명된 다른 모든 검사 및 구성을 시도한 후 게이트웨이를 도메인에 조인할 수 없는 경우 도메인 컨트롤러 이벤트 로그를 검사하는 것이 좋습니다. 도메인 컨트롤러의 이벤트 뷰어에 오류가 있는지 확인합니다. 게이트웨이 쿼리가 도메인 컨트롤러에 도달했는지 확인합니다.

문제 해결: 게이트웨이 활성화 중 내부 오류 발생

Storage Gateway 활성화 요청은 두 개의 네트워크 경로를 통과합니다. 클라이언트에서 보낸 수신 활성화 요청은 포트 80을 통해 게이트웨이의 가상 머신(VM) 또는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결됩니다. 게이트웨이가 활성화 요청을 성공적으로 수신하면 게이트웨이는 Storage Gateway 엔드포인트와 통신하여 활성화 키를 받습니다. 게이트웨이가 Storage Gateway 엔드포인트에 연결할 수 없는 경우 게이트웨이는 내부 오류 메시지를 표시하며 클라이언트에 응답합니다.

다음 문제 해결 정보를 참조하여 AWS Storage Gateway를 활성화하려고 할 때 내부 오류 메시지가 표시되는 경우에 취해야 할 조치를 결정하세요.

> **Note**
>
> - 최신 가상 머신 이미지 파일 또는 Amazon Machine Image(AMI) 버전을 사용하여 새 게이트웨이를 배포해야 합니다. 오래된 AMI를 사용하는 게이트웨이를 활성화하려고 하면 내부 오류가 발생합니다.
> - AMI를 다운로드하기 전에 배포하려는 올바른 게이트웨이 유형을 선택해야 합니다. 각 게이트웨이 유형의 .ova 파일과 AMI는 서로 다르므로 서로 바꾸어 사용할 수 없습니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필수 포트 확인

온프레미스에 배포된 게이트웨이의 경우 로컬 방화벽에서 포트가 열려 있는지 확인합니다. Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 인스턴스의 보안 그룹에서 포트가 열려 있는지 확인합니다. 포트가 열려 있는지 확인하려면 서버의 퍼블릭 엔드포인트에서 텔넷 명령을 실행합니다. 이 서버는 게이트웨이와 동일한 서브넷에 있어야 합니다. 예를 들어 다음 텔넷 명령은 포트 443에 대한 연결을 테스트합니다.

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

게이트웨이 자체가 엔드포인트에 접속할 수 있는지 확인하려면 게이트웨이의 로컬 VM 콘솔에 액세스합니다(온프레미스에 배포된 게이트웨이의 경우). 또는 게이트웨이 인스턴스에 SSH로 접속할 수 있습니다(Amazon EC2에 배포된 게이트웨이의 경우). 그런 다음 네트워크 연결 테스트를 실행합니다. 테스트가 [PASSED]를 반환하는지 확인합니다. 자세한 내용은 게이트웨이의 네트워크 연결 테스트를 참조하세요.

> **Note**
>
> 게이트웨이 콘솔의 기본 로그인 사용자 이름은 admin이고 기본 암호는 password입니다.

방화벽 보안으로 게이트웨이에서 퍼블릭 엔드포인트로 전송되는 패킷이 수정되지 않도록 확인

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안으로 인해 게이트웨이에서 전송된 패킷이 방해받을 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 것과 다르게 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 포트 443의 기본 활성화 엔드포인트(anon-cp.storagegateway.region.amazonaws.com)에서 OpenSSL 명령을 실행합니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 시스템에서 실행해야 합니다.

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region*을 로 바꿉니다 AWS 리전.

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

SSL 검사가 진행 중이면 다음과 같이 변경된 인증서 체인이 응답에 표시됩니다.

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
```

```
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 엔드포인트에 대한 게이트웨이의 아웃바운드 트래픽은 네트워크의 방화벽에서 수행하는 검사에서 제외되어야 합니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간 편차가 지나치게 크면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 편차는 60초 이내여야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하세요.

Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이의 시간 동기화가 제대로 이루어질 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

- time.aws.com
- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

Amazon VPC 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필수 포트 확인

필수 포트가 로컬 방화벽(온프레미스에 배포된 게이트웨이의 경우) 또는 보안 그룹(Amazon EC2에 배포된 게이트웨이의 경우) 내에서 열려 있는지 확인합니다. 게이트웨이를 Storage Gateway VPC 엔드

포인트에 연결하는 데 필요한 포트는 게이트웨이를 퍼블릭 엔드포인트에 연결할 때 필요한 포트와 다릅니다. Storage Gateway VPC 엔드포인트에 연결하려면 다음 포트가 필요합니다.

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

자세한 내용은 Storage Gateway용 VPC 엔드포인트 생성을 참조하세요.

또한 Storage Gateway VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 엔드포인트에 연결된 기본 보안 그룹에서 필수 포트를 허용하지 않을 수 있습니다. 게이트웨이의 IP 주소 범위에서 필수 포트를 통해 트래픽을 허용하는 새 보안 그룹을 생성합니다. 그런 다음 해당 보안 그룹을 VPC 엔드포인트에 연결합니다.

> **Note**
>
> Amazon VPC 콘솔을 사용하여 VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 콘솔에서 Storage Gateway VPC 엔드포인트를 확인한 후 보안 그룹 탭을 선택합니다.

필수 포트가 열려 있는지 확인하려면 Storage Gateway VPC 엔드포인트에서 텔넷 명령을 실행할 수 있습니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 서버에서 실행해야 합니다. 가용 영역을 지정하지 않은 첫 번째 DNS 이름에 대해 테스트를 실행할 수 있습니다. 예를 들어 다음 텔넷 명령은 DNS 이름 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com을 사용하여 필수 포트 연결을 테스트합니다.

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

방화벽 보안으로 게이트웨이에서 Storage Gateway Amazon VPC 엔드포인트로 전송되는 패킷이 수정되지 않도록 확인

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안으로 인해 게이트웨이에서 전송된 패킷이 방해받을 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 것과 다르게 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 Storage Gateway VPC 엔드포인트에서 OpenSSL 명령을 실행합니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 시스템에서 실행해야 합니다. 각 필수 포트에 대해 명령을 실행합니다.

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
```

```
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

SSL 검사가 진행 중이면 다음과 같이 변경된 인증서 체인이 응답에 표시됩니다.

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 필수 포트를 통과하는 게이트웨이의 VPC 엔드포인트 아웃바운드 트래픽은 네트워크 방화벽에서 수행하는 검사에서 제외됩니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간 편차가 지나치게 크면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 편차는 60초 이내여야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하세요.

Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이의 시간 동기화가 제대로 이루어질 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

HTTP 프록시 확인 및 관련 보안 그룹 설정 확인

활성화하기 전에 온프레미스 게이트웨이 VM에서 Amazon EC2의 HTTP 프록시가 포트 3128에서 Squid 프록시로 구성되어 있는지 확인합니다. 이 경우 다음 사항을 확인합니다.

- Amazon EC2의 HTTP 프록시에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이 인바운드 규칙은 게이트웨이 VM의 IP 주소에서 포트 3128의 Squid 프록시 트래픽을 허용해야 합니다.
- Amazon EC2 VPC 엔드포인트에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이러한 인바운드 규칙은 Amazon EC2의 HTTP 프록시 IP 주소에서 포트 1026-1028, 1031, 2222 및 443의 트래픽을 허용해야 합니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하는 중 동일한 VPC에 Storage Gateway VPC 엔드포인트가 있을 때 발생하는 오류 해결

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하는 중 동일한 VPC에 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트가 있을 때 발생하는 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

Storage Gateway VPC 엔드포인트에서 프라이빗 DNS 이름 활성화 설정이 활성화되어 있지 않은지 확인합니다.

프라이빗 DNS 이름 활성화가 활성화된 경우 해당 VPC에서 퍼블릭 엔드포인트로의 게이트웨이를 활성화할 수 없습니다.

프라이빗 DNS 이름 옵션을 비활성화하려면

1. Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Storage Gateway VPC 엔드포인트를 선택합니다.
4. 작업을 선택합니다.
5. 프라이빗 DNS 이름 관리를 선택합니다.
6. 프라이빗 DNS 이름 활성화에서 이 엔드포인트에 대해 활성화를 선택 취소합니다.
7. 프라이빗 DNS 이름 수정을 선택하여 설정을 저장합니다.

문제 해결: 온프레미스 게이트웨이 문제

온프레미스 게이트웨이에서 발생할 수 있는 일반적인 문제와가 게이트웨이에 지원 연결하여 문제 해결을 지원하는 방법에 대한 다음 정보를 찾을 수 있습니다.

다음 표는 온프레미스 게이트웨이 관련 작업 시 발생할 수 있는 전형적인 문제를 나열한 것입니다.

문제	취할 조치
게이트웨이의 IP 주소를 찾을 수 없습니다.	하이퍼바이저 클라이언트로 호스트에 접속하여 게이트웨이 IP 주소를 찾습니다. • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다. • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. 그래도 게이트웨이 IP 주소를 찾기 어려운 경우:

문제	취할 조치
	• VM이 켜져 있는지 확인합니다. VM이 켜져 있는 경우에만 IP 주소가 게이트웨이에 할당됩니다. • VM이 스타트업을 마칠 때까지 기다리십시오. VM을 방금 켰다면 게이트웨이가 부팅 시퀀스를 마치는 데 몇 분이 걸릴 수 있습니다.
네트워크 또는 방화벽에 문제가 있습니다.	• 게이트웨이에 적절한 포트를 허용합니다. • 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. 네트워크 및 방화벽 요건에 대한 자세한 내용은 네트워크 및 방화벽 요구 사항 섹션을 참조하세요.
Storage Gateway Management Console에서 활성화 진행 버튼을 클릭하면 게이트웨이 활성화가 실패합니다.	• 클라이언트에서 VM을 ping하여 게이트웨이 VM에 액세스할 수 있는지 확인합니다. • VM이 인터넷에 네트워크로 연결되어 있는지 확인합니다. 연결되어 있지 않으면 SOCKS 프록시를 구성해야 합니다. 이에 대한 자세한 내용은 게이트웨이 네트워크 연결 테스트 섹션을 참조하세요. • 호스트의 시간이 올바른지, 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성되어 있는지, 게이트웨이 VM의 시간이 올바른지 확인합니다. 하이퍼바이저 호스트와 VM의 시간을 동기화하는 작업에 대한 자세한 내용은 게이트웨이의 네트워크 시간 프로토콜(NTP) 서버 구성 섹션을 참조하세요. • 이 단계를 수행한 후 Storage Gateway 콘솔과 게이트웨이 설정 및 활성화 마법사를 사용하여 게이트웨이 배포를 다시 시도할 수 있습니다. • VM에 16GB 이상의 RAM이 있는지 확인합니다. RAM이 16GB 미만인 경우 게이트웨이 할당이 실패합니다. 자세한 내용은 File Gateway 설정 요구 사항 단원을 참조하십시오.

문제	취할 조치
게이트웨이와 AWS간 대역폭을 개선해야 합니다.	애플리케이션 및 게이트웨이 VM을 연결하는 것과 별도로 네트워크 어댑터(NIC) AWS 에서에 대한 인터넷 연결을 설정 AWS 하여 게이트웨이에서 로 대역폭을 개선할 수 있습니다. 이 접근 방식은에 고 대역폭으로 연결되어 AWS 있고 특히 스냅샷 복원 중에 대역폭 경합을 피하려는 경우에 유용합니다. 고처리량 워크로드 요구 사항을 충족하기 위해 Direct Connect를 사용하여 온프레미스 게이트웨이와 AWS간에 전용 네트워크 연결을 설정할 수 있습니다. 게이트웨이에서 로의 연결 대역폭을 측정하려면 게이트웨이의 `CloudBytesDownloaded` 및 `CloudBytesUploaded` 지표를 AWS사용합니다. 이에 관한 자세한 내용은 성능 및 최적화 섹션을 참조하세요. 인터넷 연결성을 개선하면 업로드 버퍼가 꽉 차지 않도록 하는 데 도움이 됩니다.

문제	취할 조치

게이트웨이로의 처리량 또는 게이트웨이로부터의 처리량이 0으로 떨어집니다.	• Storage Gateway 콘솔의 게이트웨이 탭에서 게이트웨이 VM의 IP 주소가 하이퍼바이저 클라이언트 소프트웨어(예: VMware vSphere 클라이언트 또는 Microsoft Hyper-V Manager)를 사용할 때 표시되는 것과 동일한지 확인합니다. 일치하지 않는 경우 게이트웨이 VM 종료에 표시된 대로 Storage Gateway 콘솔에서 게이트웨이를 다시 시작합니다. 다시 시작한 후에는 Storage Gateway 콘솔의 게이트웨이 탭에 있는 IP 주소 목록에 있는 주소가 하이퍼바이저 클라이언트에서 확인한 게이트웨이의 IP 주소와 일치해야 합니다.
	  • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다.
	  • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다.
	• 에 설명된 AWS 대로 게이트웨이의에 대한 연결을 확인합니다게이트웨이 네트워크 연결 테스트.
	• 하이퍼바이저 관리 클라이언트에서 게이트웨이의 네트워크 어댑터 구성을 확인하고 게이트웨이에 대해 사용하려는 모든 인터페이스가 활성화되었는지 확인합니다.
	• 게이트웨이 로컬 콘솔에서 게이트웨이의 네트워크 어댑터 구성을 확인합니다. 지침은 게이트웨이 네트워크 설정 구성 섹션을 참조하세요.
	
	게이트웨이와 주고받는 처리량은 Amazon CloudWatch 콘솔에서 확인할 수 있습니다. 게이트웨이와 주고받는 처리량 측정에 대한 자세한 내용은 섹션을 AWS참조하세요성능 및 최적화.

Microsoft Hyper-V에서 Storage Gateway를 가져오기(배포)하는 데 문제가 있습니다.	Microsoft Hyper-V에서 게이트웨이를 배포할 때 흔히 겪는 몇 가지 문제를 다루는 문제 해결: Microsoft Hyper-V 설 섹션을 참조하세요.

문제	취할 조치
"게이트웨이의 볼륨에 기록된 데이터가 AWS에 안전하게 저장되지 않았습니다."라는 메시지가 표시됩니다.	게이트웨이 VM이 또 다른 게이트웨이 VM의 복제 또는 스냅샷으로부터 생성된 경우 이 메시지를 수신하게 됩니다. 그렇지 않은 경우 지원에 문의하세요.

문제 해결: 보안 스캔에서 열린 NFS 포트 표시

특정 NFS 포트는 SMB 파일 공유에만 사용하는 게이트웨이에서도 기본적으로 활성화됩니다. Qualys와 같은 타사 보안 소프트웨어를 사용하여 File Gateway가 배포된 네트워크를 스캔하는 경우 스캔 결과에서 이러한 열린 NFS 포트를 잠재적 보안 취약성으로 보고할 수 있습니다. 게이트웨이를 SMB 파일 공유에만 사용하고 보안상의 이유로 사용하지 않는 NFS 포트를 비활성화하려는 경우 다음 절차를 사용합니다.

File Gateway에서 NFS 포트를 비활성화하려면:

1. 로컬 콘솔에서 Storage Gateway 명령 실행에 설명된 절차를 사용하여 게이트웨이 로컬 콘솔 명령 프롬프트에 액세스합니다.
2. NFS 트래픽을 비활성화하려면 다음 명령을 입력하십시오.

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

3. 다음 명령을 입력하여 차단된 NFS 포트가 IP 테이블에 나타나는지 확인합니다.

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

온프레미스에서 호스팅되는 게이트웨이 문제를 해결하는 데 도움이 되는 지원 액세스 활성화

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해가 게이트웨이에 지원 액세스할 수 있도록 허용하는 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이에 대한 지원 액세스는 꺼져 있습니다. 호스트의 로컬 콘솔을 통해 이 액세스 권한을 활성화합니다. 게이트웨이에 대한 지원 액세스 권한을 부여하려면 먼저 호스트의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 지원 서버에 연결합니다.

게이트웨이에 대한 지원 액세스를 켜려면

1. 호스트의 로컬 콘솔에 로그인합니다.

   - VMware ESXi - 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.

2. 프롬프트에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. **h**를 입력하여 사용 가능한 명령 목록을 엽니다.
4. 다음 중 하나를 수행하세요.

   - 게이트웨이에서 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령 창에 **open-support-channel**을 입력하여 Storage Gateway의 고객 지원에 연결합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

- 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **`open-support-channel`**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

> **Note**
>
> 채널 번호는 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 포트 번호가 아닙니다. 그 대신에 게이트웨이는 Storage Gateway 서버에 Secure Shell(SSH)(TCP 22)로 접속하여 해당 연결에 지원 채널을 제공합니다.

5. 지원 채널이 설정되면가 문제 해결 지원을 제공할 지원 수 지원 있도록에 지원 서비스 번호를 제공합니다.
6. 지원 세션이 완료되면 **`q`**를 입력하여 세션을 종료합니다. Amazon Web Services Support에서 지원 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **`exit`**를 입력하여 Storage Gateway 콘솔에서 로그아웃합니다.
8. 프롬프트 메시지에 따라 로컬 콘솔을 종료합니다.

문제 해결: Microsoft Hyper-V 설

다음 표는 Microsoft Hyper-V 플랫폼에 Storage Gateway를 배포할 때 발생할 수 있는 일반적인 문제를 나열한 것입니다.

문제	취할 조치
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다. "가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. [...] 위치에서 가상 머신 가져오기 파일을 찾을 수 없습	이 오류는 다음과 같은 이유로 발생할 수 있습니다. • 압축하지 않은 게이트웨이 소스 파일의 루트를 가리키지 않는 경우. 가상 머신 가져오기 대화 상자에 지정한 위치의 마지막 부분은 `AWS-Storage-Gateway` 여야 합니다. 예제: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\ .` • 이미 게이트웨이를 배포했는데 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하지 않은 경우,

문제	취할 조치
니다. Hyper-V를 사용하여 가상 머신을 생성하고 내보낸 경우에만 가상 머신을 가져올 수 있습니다."	압축 해제된 게이트웨이 파일이 있는 위치에 VM이 생성되므로 이 위치에서 다시 가져올 수 없습니다. 이 문제를 해결하려면 압축을 해제한 게이트웨이 소스 파일의 새 사본을 얻어 이를 새 위치에 복사하면 됩니다. 새 위치를 가져오는 위치로 사용합니다. 압축을 푼 하나의 소스 파일 위치에서 여러 개의 게이트웨이를 생성하려는 경우 가상 머신 가져오기 대화 상자에서 가상 머신 복사를 선택하고 모든 파일 복제 확인란을 선택해야 합니다.
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다. "가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. 가져오기 작업이 [...]에서 파일을 복사하지 못했습니다. 파일이 존재합니다. (0x80070050)"	이미 게이트웨이를 배포하고 가상 하드 디스크 및 가상 머신 구성 파일이 저장된 기본 폴더를 다시 사용하는 경우, 이 오류가 발생합니다. 이 문제를 해결하려면 Hyper-V 설정 대화 상자의 왼쪽 패널에서 서버 아래에 새 위치를 지정합니다.
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다. "가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."라는 오류 메시지가 표시됩니다.	게이트웨이를 가져올 때 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하여 VM의 새 고유 ID를 생성해야 합니다.

문제	취할 조치
게이트웨이 VM을 시작하려고 하는데 다음과 같은 오류 메시지가 나타납니다. “선택한 가상 머신을 시작하는 동안 오류가 발생했습니다. 하위 파티션 프로세서 설정이 상위 파티션과 호환되지 않습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 머신 ID [...])"	이 오류는 게이트웨이에 필요한 CPU와 호스트에서 사용 가능한 CPU 사이의 CPU 불일치로 인해 발생할 수 있습니다. 기본 하이퍼바이저가 VM CPU 개수를 지원하도록 해야 합니다. Storage Gateway 요구 사항에 대한 자세한 내용은 File Gateway 설정 요구 사항 섹션을 참조하세요.
게이트웨이 VM을 시작하려고 하는데 다음과 같은 오류 메시지가 나타납니다. “선택한 가상 머신을 시작하는 동안 오류가 발생했습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 머신 ID [...]) 파티션을 생성하지 못했습니다. 요청된 서비스를 완료하는 데 필요한 시스템 리소스가 부족합니다. (0x800705AA)"	이 오류는 게이트웨이에 필요한 RAM과 호스트에서 사용 가능한 RAM 사이의 RAM 불일치로 인해 발생할 수 있습니다. Storage Gateway 요구 사항에 대한 자세한 내용은 File Gateway 설정 요구 사항 섹션을 참조하세요.
스냅샷 및 게이트웨이 소프트웨어 업데이트는 예상과 약간 다른 시각에 실행됩니다.	게이트웨이 VM의 클럭은 실제 시간과 약간 오차가 있을 수 있는데, 이를 클럭 드리프트라고 합니다. 로컬 게이트웨이 콘솔의 시간 동기화 옵션을 사용하여 VM의 시간을 점검하고 수정합니다. 자세한 내용은 게이트웨이의 네트워크 시간 프로토콜(NTP) 서버 구성 단원을 참조하십시오.

문제	취할 조치
압축 해제된 Microsoft Hyper-V Storage Gateway 파일은 호스트 파일 시스템에 저장해야 합니다.	일반적인 Microsoft Windows 서버에 액세스하듯이 호스트에 액세스합니다. 예를 들어 하이퍼바이저 호스트의 이름이 `hyperv-server` 인 경우에는 다음과 같이 UNC 경로인 `\\hyperv-server\c$` 를 사용할 수 있습니다. 이 경로는 `hyperv-server` 라는 이름을 로컬 호스트 파일에서 확인할 수 있거나 정의한다고 가정합니다.
하이퍼바이저에 접속할 때 자격 증명을 요구하는 메시지가 표시됩니다.	Sconfig.cmd 도구를 사용하여 사용자 자격 증명을 하이퍼바이저 호스트용 로컬 관리자로 추가합니다.
Broadcom 네트워크 어댑터를 사용하는 Hyper-V 호스트에 대해 가상 머신 대기열(VMQ)을 켜면 네트워크 성능이 저하될 수 있습니다.	해결 방법에 대한 자세한 내용은 Microsoft 설명서 VMQ가 켜져 있는 경우 Windows Server 2012 Hyper-V 호스트의 가상 머신에서 네트워크 성능이 저하됨을 참조하세요.

문제 해결: Amazon EC2 게이트웨이 문제

다음 섹션에서는 Amazon EC2에 배포된 게이트웨이를 사용할 때 발생할 수 있는 일반적인 문제를 확인할 수 있습니다. 온프레미스 게이트웨이와 Amazon EC2에 배포한 게이트웨이 간의 차이점에 대한 자세한 내용은 S3 File Gateway용 기본 Amazon EC2 호스트 배포 섹션을 참조하세요.

휘발성 스토리지 사용에 대한 자세한 내용은 휘발성 스토리지와 EC2 게이트웨이를 함께 사용 섹션을 참조하세요.

주제

- 몇 분 후 게이트웨이가 활성화되지 않음
- 인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없음
- Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려는 경우
- Amazon EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우

몇 분 후 게이트웨이가 활성화되지 않음

Amazon EC2 콘솔에서 다음 사항을 확인하세요.

- 인스턴스와 연결한 보안 그룹에서 포트 80이 열려 있습니다. 보안 그룹 규칙 추가에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 보안 그룹 규칙 추가를 참조하세요.
- 게이트웨이 인스턴스는 실행 중으로 표시됩니다. Amazon EC2 콘솔에서 인스턴스의 상태 값은 RUNNING이어야 합니다.
- 스토리지 요구 사항에 설명된 대로 Amazon EC2 인스턴스 유형은 최소 요구 사항을 충족하는지 여부.

문제를 해결한 후 게이트웨이를 다시 활성화합니다. 이렇게 하려면 Storage Gateway 콘솔을 열고 Amazon EC2에 새 게이트웨이 배포를 선택한 다음 인스턴스의 IP 주소를 다시 입력합니다.

인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없음

인스턴스에 리소스 태그를 지정하지 않았는데 많은 수의 인스턴스가 실행 중인 경우에는 어떤 인스턴스를 실행했는지 파악하기 어려울 수 있습니다. 이 경우 다음 작업을 수행하여 해당 게이트웨이 인스턴스를 찾을 수 있습니다.

- 인스턴스의 설명 탭에서 Amazon Machine Image(AMI)의 이름을 확인합니다. Storage Gateway AMI 기반 인스턴스는 **`aws-storage-gateway-ami`**라는 텍스트로 시작해야 합니다.
- Storage Gateway AMI 기반 인스턴스가 여러 개인 경우, 인스턴스 시작 시간을 확인하여 올바른 인스턴스를 찾습니다.

Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려는 경우

Amazon EC2 직렬 콘솔을 사용하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. 지침과 문제 해결 팁은 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 직렬 콘솔 섹션을 참조하세요.

Amazon EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해가 게이트웨이에 지원 액세스할 수 있도록 허용하는 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이에 대한 지원 액세스는 꺼져 있습니다. Amazon EC2 로컬 콘솔을 통해 이 액세스 권한을 활성화 합니다. Secure Shell(SSH)을 통해 Amazon EC2 로컬 콘솔에 로그인합니다. SSH를 통해 성공적으로 로그인하려면 인스턴스의 보안 그룹에 TCP 포트 22를 개방하는 규칙이 있어야 합니다.

> **Note**
>
> 기존 보안 그룹에 새 규칙을 추가할 경우, 해당 보안 그룹을 사용하는 모든 인스턴스에 새 규칙이 적용됩니다. 보안 그룹 및 보안 그룹 규칙을 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon EC2 보안 그룹을 참조하세요.

가 게이트웨이에 지원 연결되도록 하려면 먼저 Amazon EC2 인스턴스의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 액세스를 제공합니다.

Amazon EC2 인스턴스에 배포된 게이트웨이에 대한 지원 액세스를 켜려면

1. Amazon EC2 인스턴스의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 사용 설명서에서 인스턴스에 연결을 참조하세요.

   다음 명령을 사용하여 EC2 인스턴스의 로컬 콘솔에 로그인할 수 있습니다.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > *PRIVATE-KEY*는 Amazon EC2 인스턴스를 시작할 때 사용한 EC2 키 페어의 프라이빗 인증서를 포함하는 `.pem` 파일입니다. 자세한 내용은 Amazon EC2 사용 설명서에서 키 페어의 퍼블릭 키 검색을 참조하세요.
   >
   > The *INSTANCE-PUBLIC-DNS-NAME*은 게이트웨이가 실행 중인 Amazon EC2 인스턴스의 퍼블릭 도메인 이름 시스템(DNS) 이름입니다. 이 퍼블릭 DNS 이름을 확인하려면 EC2 콘솔에서 Amazon EC2 인스턴스를 선택하고 설명 탭을 클릭합니다.

2. 프롬프트에 **`6 - Command Prompt`**를 입력하여 지원 채널 콘솔을 엽니다.
3. **h**를 입력하여 AVAILABLE COMMANDS(사용 가능한 명령) 창을 엽니다.
4. 다음 중 하나를 수행하세요.

   - 게이트웨이에서 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령 창에 **`open-support-channel`**을 입력하여 Storage Gateway의 고객 지원에 연결합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

- 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **`open-support-channel`**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

> **Note**
>
> 채널 번호는 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 포트 번호가 아닙니다. 그 대신에 게이트웨이는 Storage Gateway 서버에 Secure Shell(SSH)(TCP 22)로 접속하여 해당 연결에 지원 채널을 제공합니다.

5. 지원 채널이 설정되면가 문제 해결 지원을 제공할 지원 수 지원 있도록에 지원 서비스 번호를 제공합니다.
6. 지원 세션이 완료되면 **`q`**를 입력하여 세션을 종료합니다. Amazon Web Services Support에서 지원 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **`exit`**를 입력하여 Storage Gateway 콘솔을 종료합니다.
8. 콘솔 메뉴에 따라 Storage Gateway 인스턴스에서 로그아웃합니다.

문제 해결: 하드웨어 어플라이언스 문제

> **Note**
>
> 가용성 종료 공지: 2025년 5월 12일부터 AWS Storage Gateway 하드웨어 어플라이언스가 더 이상 제공되지 않습니다. AWS Storage Gateway 하드웨어 어플라이언스를 사용하는 기존 고객은 2028년 5월까지를 계속 사용하고 지원을 받을 수 있습니다. 또는 AWS Storage Gateway 서비스를 사용하여 온프레미스 및 클라우드 내 애플리케이션에 사실상 무제한의 클라우드 스토리지에 대한 액세스 권한을 부여할 수 있습니다.

다음 주제에서는 AWS Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제와 이러한 문제 해결에 대한 제안 사항에 대해 설명합니다.

주제

- 공장 초기화는 어떻게 수행하나요?
- 원격 재시작은 어떻게 수행하나요?
- Dell iDRAC 지원은 어디에서 받을 수 있나요?
- 하드웨어 어플라이언스 일련 번호를 찾을 수 없음
- 하드웨어 어플라이언스 지원은 어디에서 받을 수 있나요?

서비스 IP 주소를 확인할 수 없음

서비스에 연결할 때 호스트 IP 주소가 아닌 서비스의 IP 주소를 사용하고 있는지 확인합니다. 서비스 콘솔에서 서비스 IP 주소를 구성하고 하드웨어 콘솔에서 호스트 IP 주소를 구성합니다. 하드웨어 어플라이언스를 시작하면 하드웨어 콘솔이 표시됩니다. 하드웨어 콘솔에서 서비스 콘솔로 이동하려면 Open Service Console(서비스 콘솔 열기)을 선택합니다.

공장 초기화는 어떻게 수행하나요?

어플라이언스에서 공장 초기화를 수행해야 하는 경우 다음 지원 섹션에 설명된 대로 AWS Storage Gateway 하드웨어 어플라이언스 팀에 지원을 문의하세요.

원격 재시작은 어떻게 수행하나요?

어플라이언스를 원격으로 재시작해야 하는 경우 Dell iDRAC 관리 인터페이스를 사용하여 재시작할 수 있습니다. 자세한 내용은 Dell Technologies InfoHub 웹 사이트에서 iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers를 참조하세요.

Dell iDRAC 지원은 어디에서 받을 수 있나요?

Dell PowerEdge 서버에는 Dell iDRAC 관리 인터페이스가 함께 제공됩니다. 다음과 같이 하는 것이 좋습니다:

- iDRAC 관리 인터페이스를 사용하는 경우 기본 암호를 변경해야 합니다. iDRAC 자격 증명에 대한 자세한 내용은 Dell PowerEdge - iDRAC의 기본 로그인 자격 증명은 무엇입니까?를 참조하세요.
- 보안 위반을 막기 위해 펌웨어가 최신 버전인지 확인합니다.
- iDRAC 네트워크 인터페이스를 일반(em) 포트로 이동하면 성능 문제가 발생하거나 어플라이언스가 정상적으로 작동하지 않을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾을 수 없음

Storage AWS Storage Gateway 콘솔을 사용하여 Storage Gateway 하드웨어 어플라이언스의 일련 번호를 찾을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾으려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 페이지 왼쪽의 탐색 메뉴에서 하드웨어를 선택합니다.
3. 목록에서 하드웨어 어플라이언스를 선택합니다.
4. 어플라이언스의 세부 정보 탭에서 일련 번호 필드를 찾습니다.

하드웨어 어플라이언스 지원은 어디에서 받을 수 있나요?

하드웨어 어플라이언스의 기술 지원에 AWS 대한 문의는 섹션을 참조하세요지원.

지원 팀이 지원 채널을 활성화하여 게이트웨이 문제를 원격으로 해결하도록 요청할 수 있습니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다. 다음 절차에 나온 것처럼 하드웨어 콘솔에서 지원 채널을 활성화할 수 있습니다.

에 대한 지원 채널을 열려면 AWS

1. 하드웨어 콘솔을 엽니다.
2. 하드웨어 콘솔의 메인 페이지 하단에서 지원 채널 열기를 선택한 다음 `Enter` 키를 누릅니다.

   네트워크 연결 또는 방화벽 문제가 없는 경우 할당된 포트 번호가 30초 이내에 표시되어야 합니다. 예제:

   상태: 포트 19599에서 열림
3. 포트 번호를 기록하여에 제공합니다 지원.

문제 해결: File Gateway 문제

Amazon CloudWatch 로그 그룹에 로그 항목을 기록하도록 File Gateway를 구성할 수 있습니다. 이 경우 게이트웨이의 상태 및 게이트웨이에서 발생한 오류에 대한 알림을 받습니다. 이러한 오류 및 상태 알림에 대한 정보는 CloudWatch Logs에서 찾을 수 있습니다.

이 섹션에서는 각 오류의 원인 및 상태 알림과 문제 해결 방법을 이해하는 데 도움이 되는 정보를 찾을 수 있습니다.

주제

오류: 1344(0x00000540)

Amazon S3로 파일을 마이그레이션하는 동안 ACE(ACEs 제어 항목)가 10개 이상인 파일을 Amazon S3로 복사하려는 `ERROR 1344 (0x00000540)`가 발생할 수 있습니다. 액세스 제어 항목은 액세스 제어 목록(ACL)에 나열됩니다.

Amazon S3 File Gateway는 지정된 파일 또는 폴더당 10개의 ACE 항목만 보존할 수 있습니다.

오류 1344 해결 방법: 대상 디렉터리에 NTFS 보안 복사.

10개 이상의 항목이 포함된 파일 또는 폴더에 대한 Windows 권한의 항목 수를 줄입니다. 일반적인 접근 방식은 전체 항목 목록이 포함된 그룹을 생성한 다음 항목 목록을 해당 단일 그룹으로 바꾸는 것입니다. 항목 수가 10개보다 작으면 파일 또는 폴더를 게이트웨이에 다시 복사할 수 있습니다.

오류: GatewayClockOutOfSync

게이트웨이가 로컬 시스템 시간과 AWS Storage Gateway 서버에서 보고한 시간 간에 5분 이상의 차이를 감지하면 `GatewayClockOutOfSync` 오류가 발생할 수 있습니다. 클록 동기화 문제는 게이트웨

이와 간의 연결에 부정적인 영향을 미칠 수 있습니다 AWS. 게이트웨이 클럭이 동기화되지 않은 경우 NFS 및 SMB 연결에 I/O 오류가 발생할 수 있으며 SMB 사용자에게 인증 오류가 발생할 수 있습니다.

GatewayClockOutOfSync 오류를 해결하려면

- 게이트웨이와 NTP 서버 간의 네트워크 구성을 확인합니다. 게이트웨이 VM 시간 동기화 및 NTP 서버 구성 업데이트에 대한 자세한 내용은 게이트웨이의 NTP(Network Time Protocol) 서버 구성을 참조하세요.

오류: InaccessibleStorageClass

객체가 Amazon S3 Standard 스토리지 클래스에서 벗어나면 `InaccessibleStorageClass` 오류가 발생할 수 있습니다.

일반적으로 File Gateway는 지정된 객체를 Amazon S3 버킷에 업로드하거나 Amazon S3 버킷에서 객체를 읽으려고 할 때 오류가 발생합니다. 일반적으로 이 오류는 객체가 Amazon Glacier로 이동했으며 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스에 있음을 의미합니다.

S3 File Gateway는 이 오류로 인해 현재 Amazon S3에 업로드하지 못한 게이트웨이 캐시의 모든 파일을 나열하는 캐시 보고서를 생성할 수 있습니다. 이 보고서의 정보는를 사용하여 게이트웨이, Amazon S3 또는 IAM 구성 문제를 해결하는 지원 데 도움이 될 수 있습니다. 자세한 내용은 캐시 보고서 생성을 참조하세요.

InaccessibleStorageClass 오류를 해결하려면

- S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스에서 S3의 원래 스토리지 클래스로 객체를 복원합니다.

  업로드 오류를 수정하기 위해 객체를 S3 버킷으로 복원하면 파일이 결국 업로드됩니다. 읽기 오류를 수정하기 위해 객체를 복원하면 File Gateway의 SMB 또는 NFS 클라이언트가 파일을 읽을 수 있습니다.

오류: InvalidObjectState

지정된 File Gateway 이외의 라이터가 지정된 Amazon S3 버킷에서 지정된 파일을 수정할 때 `InvalidObjectState` 오류가 발생할 수 있습니다. 따라서 File Gateway의 파일 상태가 Amazon S3에서의 해당 상태와 일치하지 않습니다. 이후에 Amazon S3으로 파일을 업로드하거나 Amazon S3에서 파일을 검색하지 못합니다.

S3 File Gateway는 이 오류로 인해 현재 Amazon S3에 업로드하지 못한 게이트웨이 캐시의 모든 파일을 나열하는 캐시 보고서를 생성할 수 있습니다. 이 보고서의 정보는를 사용하여 게이트웨이, Amazon S3 또는 IAM 구성 문제를 해결하는 지원 데 도움이 될 수 있습니다. 자세한 내용은 캐시 보고서 생성을 참조하세요.

InvalidObjectState 오류를 해결하려면

파일을 수정하는 작업이 `S3Upload` 또는 `S3GetObject`인 경우 다음을 수행합니다.

1. SMB 또는 NFS 클라이언트의 로컬 파일 시스템에 파일의 최신 복사본을 저장합니다(4단계에서 이 파일 복사본이 필요함). Amazon S3에 있는 파일 버전이 최신이면 그 버전을 다운로드합니다. AWS Management Console 또는를 사용하여이 작업을 수행할 수 있습니다 AWS CLI.
2. AWS Management Console 또는를 사용하여 Amazon S3에서 파일을 삭제합니다 AWS CLI.
3. SMB 또는 NFS 클라이언트를 사용하여 File Gateway에서 파일을 삭제합니다.
4. SMB 또는 NFS 클라이언트를 사용하여 1단계에서 저장한 파일의 최신 버전을 Amazon S3에 복사합니다. File Gateway를 통해 이 작업을 합니다.

오류: ObjectMissing

지정된 File Gateway 이외의 라이터가 S3 버킷에서 지정된 파일을 삭제할 때 `ObjectMissing` 오류가 발생할 수 있습니다. 이후에 Amazon S3에 업로드하거나 Amazon S3에서 객체를 가져오는 작업이 모두 실패합니다.

S3 File Gateway는 이 오류로 인해 현재 Amazon S3에 업로드하지 못한 게이트웨이 캐시의 모든 파일을 나열하는 캐시 보고서를 생성할 수 있습니다. 이 보고서의 정보는를 사용하여 게이트웨이, Amazon S3 또는 IAM 구성 문제를 해결하는 지원 데 도움이 될 수 있습니다. 자세한 내용은 캐시 보고서 생성을 참조하세요.

ObjectMissing 오류를 해결하려면

파일을 수정하는 작업이 `S3Upload` 또는 `S3GetObject`인 경우 다음을 수행합니다.

1. SMB 또는 NFS 클라이언트의 로컬 파일 시스템에 파일의 최신 복사본을 저장합니다(3단계에서 이 파일 복사본이 필요함).
2. SMB 또는 NFS 클라이언트를 사용하여 File Gateway에서 파일을 삭제합니다.
3. SMB 또는 NFS 클라이언트를 사용하여 1단계에서 저장한 파일의 최신 버전을 복사합니다. File Gateway를 통해 이 작업을 합니다.

오류: RoleTrustRelationshipInvalid

파일 공유에 대한 IAM 역할에 잘못 구성된 IAM 신뢰 관계가 있는 경우(즉, IAM 역할이 `storagegateway.amazonaws.com`이라는 Storage Gateway 보안 주체를 신뢰하지 않는 경우) 이 오류가 발생합니다. 따라서 File Gateway는 파일 공유를 지원하는 S3 버킷에서 작업을 실행하기 위한 자격 증명을 가져올 수 없습니다.

RoleTrustRelationshipInvalid 오류를 해결하려면

- `storagegateway.amazonaws.com`을 파일 공유의 IAM 역할에서 신뢰하는 있는 보안 주체로 포함하려면 IAM 콘솔 또는 IAM API를 사용합니다. IAM 역할에 대한 자세한 내용은 자습서: IAM 역할을 사용하여 AWS 계정 간에 액세스 위임을 참조하세요.

오류: S3AccessDenied

파일 공유의 Amazon S3 버킷 액세스 AWS Identity and Access Management (IAM) 역할에 `S3AccessDenied` 오류가 발생할 수 있습니다. 이 경우 오류에서 `roleArn`에 의해 지정된 S3 버킷 액세스 IAM 역할은 관련 작업을 허용하지 않습니다. Amazon S3 접두사에 의해 지정된 디렉터리의 객체에 대한 권한 때문에 해당 작업이 허용되지 않습니다.

S3 File Gateway는 이 오류로 인해 현재 Amazon S3에 업로드하지 못한 게이트웨이 캐시의 모든 파일을 나열하는 캐시 보고서를 생성할 수 있습니다. 이 보고서의 정보는를 사용하여 게이트웨이, Amazon S3 또는 IAM 구성 문제를 해결하는 지원 데 도움이 될 수 있습니다. 자세한 내용은 캐시 보고서 생성을 참조하세요.

S3AccessDenied 오류를 해결하려면

- File Gateway 상태 로그에서 `roleArn`에 연결된 Amazon S3 액세스 정책을 수정하여 Amazon S3 작업을 위한 권한을 허용합니다. 액세스 정책이 오류를 일으킨 작업에 대한 권한을 허용하는지 확인합니다. 또한 `prefix`에 대한 로그에 지정된 디렉터리에 대한 권한을 허용합니다. Amazon S3 권한에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 정책에서 권한 지정을 참조하세요.

  다음 작업으로 인해 `S3AccessDenied` 오류가 발생할 수 있습니다.

  - `S3HeadObject`
  - `S3GetObject`
  - `S3ListObjects`
  - `S3DeleteObject`

- `S3PutObject`

오류: DroppedNotifications

게이트웨이 루트 디스크의 여유 스토리지 공간이 1GB 미만이거나 1분 간격 내에 100개 이상의 상태 알림이 생성되는 경우 다른 예상 유형의 CloudWatch 로그 항목 대신 `DroppedNotifications` 오류가 발생할 수 있습니다. 이러한 상황에서 게이트웨이는 예방 조치로 자세한 CloudWatch 로그 알림 생성을 중지합니다.

DroppedNotifications 오류를 해결하려면

1. Storage Gateway 콘솔의 게이트웨이 모니터링 탭에서 `Root Disk Usage` 지표를 확인하여 사용 가능한 루트 디스크 공간이 부족한지 확인합니다.
2. 사용 가능한 공간이 1GB 미만인 경우 게이트웨이의 루트 스토리지 디스크 크기를 늘립니다. 지침은 가상 머신 하이퍼바이저 설명서를 참조하세요.

   Amazon EC2 게이트웨이의 루트 디스크 크기를 늘리려면 Amazon Elastic Compute Cloud 사용 설명서의 EBS 볼륨에 대한 수정 요청을 참조하세요.

   > **Note**
   >
   > AWS Storage Gateway Hardware Appliance의 루트 디스크 크기를 늘릴 수 없습니다.

3. 게이트웨이 다시 시작합니다.

알림: HardReboot

게이트웨이 VM이 예기치 않게 다시 시작될 때 `HardReboot` 알림을 받을 수 있습니다. 이러한 다시 시작의 원인은 정전, 하드웨어 오류 또는 다른 이벤트일 수 있습니다. VMware 게이트웨이의 경우 vSphere 고가용성 애플리케이션 모니터링을 통해 재설정하면 이 이벤트가 시작될 수 있습니다.

게이트웨이가 이러한 환경에서 실행되는 경우 `HealthCheckFailure` 알림이 있는지 확인하고 VM에 대한 VMware 이벤트 로그를 참조하세요.

알림: 재부팅

게이트웨이 VM을 다시 시작할 때 재부팅 알림을 받을 수 있습니다. VM 하이퍼바이저 관리 콘솔 또는 Storage Gateway 콘솔을 사용하여 게이트웨이 VM을 다시 시작할 수 있습니다. 게이트웨이의 유지 관리 주기 동안 게이트웨이 소프트웨어를 사용하여 다시 시작할 수도 있습니다.

재부팅이 게이트웨이에서 구성된 유지 관리 시작 시간 10분 이내에 수행되는 경우 이 재부팅은 정상적인 현상일 수 있으며 문제의 징조가 아닙니다. 유지 관리 기간을 크게 벗어나 재부팅이 수행된 경우 게이트웨이가 수동으로 다시 시작되었는지 확인합니다.

문제 해결: 보안 스캔에서 열린 NFS 포트 표시

특정 NFS 포트는 SMB 파일 공유에만 사용하는 게이트웨이에서도 기본적으로 활성화됩니다. Qualys와 같은 타사 보안 소프트웨어를 사용하여 File Gateway가 배포된 네트워크를 스캔하는 경우 스캔 결과에서 이러한 열린 NFS 포트를 잠재적 보안 취약성으로 보고할 수 있습니다. 게이트웨이를 SMB 파일 공유에만 사용하고 보안상의 이유로 사용하지 않는 NFS 포트를 비활성화하려는 경우 다음 절차를 사용합니다.

File Gateway에서 NFS 포트를 비활성화하려면:

1. 로컬 콘솔에서 Storage Gateway 명령 실행에 설명된 절차를 사용하여 게이트웨이 로컬 콘솔 명령 프롬프트에 액세스합니다.
2. NFS 트래픽을 비활성화하려면 다음 명령을 입력하십시오.

   IPv4

   ```
   iptables -I INPUT -p udp -m udp --dport 111 -j DROP
   iptables -I INPUT -p udp -m udp --dport 2049 -j DROP
   iptables -I INPUT -p udp -m udp --dport 20048 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   iptables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
   ```

   IPv6

   ```
   ip6tables -I INPUT -p udp -m udp --dport 111 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 2049 -j DROP
   ip6tables -I INPUT -p udp -m udp --dport 20048 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 111 -j DROP
   ip6tables -I INPUT -p tcp -m tcp --dport 2049 -j DROP
   ```

```
ip6tables -I INPUT -p tcp -m tcp --dport 20048 -j DROP
```

3. 다음 명령을 입력하여 차단된 NFS 포트가 IP 테이블에 나타나는지 확인합니다.

   IPv4

   ```
   iptables -n -L -v --line-numbers
   ```

   IPv6

   ```
   ip6tables -n -L -v --line-numbers
   ```

문제 해결: CloudWatch 지표 사용

Storage Gateway에서 Amazon CloudWatch 지표를 사용하여 문제를 해결하는 작업에 대한 다음 정보를 찾을 수 있습니다.

주제

- 디렉터리를 찾아볼 때 게이트웨이가 느리게 반응
- 게이트웨이가 응답하지 않음
- 게이트웨이에서 데이터를 Amazon S3로 전송하는 속도가 느림
- 게이트웨이가 예상보다 많은 Amazon S3 작업을 수행하고 있습니다.
- Amazon S3 버킷에 파일이 표시되지 않음
- 게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생함

디렉터리를 찾아볼 때 게이트웨이가 느리게 반응

ls 명령을 실행하거나 디렉터리를 찾아볼 때 File Gateway가 느리게 반응하는 경우 `IndexFetch` 및 `IndexEviction` CloudWatch 지표를 확인합니다.

- `ls` 명령을 실행하거나 디렉터리를 찾아볼 때 `IndexFetch` 지표가 0보다 큰 경우 File Gateway가 영향을 받은 디렉터리 콘텐츠에 대한 정보 없이 시작했으며 Amazon S3에 액세스해야 했습니다. 해당 디렉터리의 콘텐츠를 나열하려는 후속 노력이 더 빨리 이루어져야 합니다.
- `IndexEviction` 지표가 0보다 크면 File Gateway가 해당 시점에 캐시에서 관리할 수 있는 항목 한계에 도달했음을 의미합니다. 이 경우 File Gateway는 새 디렉터리를 나열하기 위해 가장 이전에 액

세스한 디렉터리에서 일부 스토리지 스페이스를 비워야 합니다. 이 문제가 자주 발생하고 성능에 영향을 미치는 경우에 문의하세요 지원.

관련 S3 버킷의 지원 내용과 사용 사례에 따라 성능을 개선하기 위한 권장 사항을 논의합니다.

게이트웨이가 응답하지 않음

File Gateway가 응답하지 않는 경우 다음을 수행합니다.

- 최근 재부팅 또는 소프트웨어 업데이트가 있었다면 `IOWaitPercent` 지표를 확인하십시오. 이 지표는 처리되지 않은 디스크 I/O 요청이 있을 때 CPU가 유휴 상태인 시간의 백분율을 보여줍니다. 경우에 따라 이 값이 높고(10 이상) 서버가 재부팅되거나 업데이트된 후에 증가했을 수 있습니다. 이러한 경우 인덱스 캐시를 RAM으로 재구성함에 따라 느린 루트 디스크로 인해 File Gateway에 병목 현상이 발생할 수 있습니다. 루트 디스크에 더 빠른 물리적 디스크를 사용하여 이 문제를 해결할 수 있습니다.
- `MemUsedBytes` 지표가 `MemTotalBytes` 지표와 같거나 거의 같으면 File Gateway에 사용 가능한 RAM이 부족해집니다. File Gateway에 필요한 최소 RAM이 있는지 확인합니다. 이미 이를 확인했다면 워크로드 및 사용 사례에 따라 File Gateway에 RAM을 추가해 보십시오.

  파일 공유가 SMB인 경우 파일 공유에 연결된 SMB 클라이언트 수 때문일 수도 있습니다. 지정된 시간에 연결된 클라이언트 수를 확인하려면 `SMBV(1/2/3)Sessions` 지표를 확인합니다. 연결된 클라이언트가 많은 경우 File Gateway에 RAM을 더 추가해야 할 수 있습니다.

게이트웨이에서 데이터를 Amazon S3로 전송하는 속도가 느림

File Gateway에서 Amazon S3로의 데이터 전송 속도가 느리면 다음을 수행합니다.

- `CachePercentDirty` 지표가 80 이상인 경우 File Gateway는 데이터를 Amazon S3에 업로드할 수 있는 것보다 더 빨리 디스크에 데이터를 쓰고 있습니다. File Gateway에서 업로드를 위한 대역폭을 늘리거나, 캐시 디스크를 하나 이상 추가하거나, 클라이언트 쓰기 속도를 늦추는 것이 좋습니다.
- `CachePercentDirty` 지표가 낮은 경우 `IoWaitPercent` 지표를 확인합니다. `IoWaitPercent`가 10보다 큰 경우 로컬 캐시 디스크의 속도로 인해 File Gateway에 병목 현상이 발생할 수 있습니다. 캐시에 로컬 SSD(Solid State Drive) 디스크를 사용하는 것이 좋습니다. 추천 제품은 NVMe(NVM Express)입니다. 이러한 디스크를 사용할 수 없는 경우 성능 향상을 위해 별도의 물리적 디스크에서 여러 캐시 디스크를 사용해 보십시오.

- `S3PutObjectRequestTime`, `S3UploadPartRequestTime` 또는 `S3GetObjectRequestTime`이 높으면 네트워크 병목 현상이 발생할 수 있습니다. 네트워크를 분석하여 게이트웨이에 예상 대역폭이 있는지 확인합니다.

게이트웨이가 예상보다 많은 Amazon S3 작업을 수행하고 있습니다.

File Gateway가 예상보다 많은 Amazon S3 작업을 수행하는 경우 `FilesRenamed` 지표를 확인합니다. 이름 바꾸기 작업은 Amazon S3에서 실행하는 데 비용이 많이 듭니다. 워크플로를 최적화하여 이름 바꾸기 작업 수를 최소화합니다.

Amazon S3 버킷에 파일이 표시되지 않음

게이트웨이의 파일이 Amazon S3 버킷에 반영되지 않는 경우 `FilesFailingUpload` 지표를 확인합니다. 지표에서 일부 파일이 업로드에 실패한다고 보고하는 경우 상태 알림을 확인합니다. 파일을 업로드하지 못하면 게이트웨이는 문제에 대한 세부 정보가 포함된 상태 알림을 생성합니다.

게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생함

File Gateway 백업 작업이 실패하거나 File Gateway에 쓸 때 오류가 발생하는 경우 다음을 수행합니다.

- `CachePercentDirty` 지표가 90% 이상이면 캐시 디스크에 사용 가능한 공간이 부족하기 때문에 File Gateway가 디스크에 대한 새 쓰기를 허용할 수 없습니다. File Gateway가 Amazon S3에 업로드되는 속도를 확인하려면 `CloudBytesUploaded` 지표를 확인합니다. 클라이언트가 File Gateway에 파일을 쓰는 속도를 보여 주는 `WriteBytes` 지표를 이 지표와 비교합니다. SMB 클라이언트가 Amazon S3로 업로드할 수 있는 것보다 더 빨리 File Gateway에 쓰는 경우 최소한 백업 작업의 크기를 처리할 수 있도록 캐시 디스크를 더 추가합니다. 또는 업로드 대역폭을 늘립니다.
- 백업 작업과 같은 대용량 파일 복사가 실패했지만 `CachePercentDirty` 지표가 80% 미만인 경우 File Gateway가 클라이언트 측 세션 제한 시간에 도달할 수 있습니다. SMB의 경우 PowerShell 명령 `Set-SmbClientConfiguration -SessionTimeout 300`을 사용하여 이 제한 시간을 늘릴 수 있습니다. 이 명령을 실행하면 이 제한 시간이 300초로 설정됩니다.

  NFS의 경우 소프트 마운트 대신 하드 마운트를 사용하여 클라이언트를 마운트해야 합니다.

문제 해결: 파일 공유 문제

아래와 같이 파일 공유와 관련해 예기치 않은 문제를 겪는 경우 취해야 할 조치에 대한 정보를 얻을 수 있습니다.

주제

파일 공유가 CREATING, UPDATING 또는 DELETING 상태에서 멈춤

파일 공유 상태는 파일 공유의 상태를 요약합니다. S3 File Gateway 파일 공유가 `CREATING`, `UPDATING`또는 `DELETING` 상태에서 멈춘 경우 다음 문제 해결 단계를 사용하여 문제를 식별하고 해결합니다.

IAM 역할 권한 및 신뢰 관계 확인

파일 공유와 연결된 AWS Identity and Access Management (IAM) 역할에는 Amazon S3 버킷에 액세스할 수 있는 충분한 권한이 있어야 합니다. 또한 역할의 신뢰 정책은 역할을 수임할 수 있는 권한을 Storage Gateway 서비스에 부여해야 합니다.

IAM 역할 권한을 확인하려면:

1. IAM 콘솔(https://console.aws.amazon.com/iam/)을 엽니다.
2. 탐색 창에서 역할을 선택합니다.
3. 파일 공유와 연결된 IAM 역할을 선택합니다.
4. 신뢰 관계 탭을 선택합니다.

5. Storage Gateway가 신뢰할 수 있는 엔터티로 나열되어 있는지 확인합니다. Storage Gateway가 신뢰할 수 있는 엔터티가 아닌 경우 신뢰 관계 편집을 선택한 후 다음 정책을 추가합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "storagegateway.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

6. IAM 역할에 올바른 권한이 있고 Amazon S3 버킷이 IAM 정책에 리소스로 나열되어 있는지 확인합니다. 자세한 내용은 Amazon S3 버킷에 액세스할 수 있는 권한 부여 단원을 참조하십시오.

> **Note**
>
> 교차 서비스 혼동된 대리자 방지 문제를 방지하려면 조건 컨텍스트 키가 포함된 신뢰 관계 정책을 사용합니다. 자세한 내용은 the section called “교차 서비스 혼동된 대리인 방지” 단원을 참조하십시오.

해당 리전에서 AWS STS가 활성화되었는지 확인

AWS 리전에서 AWS Security Token Service (AWS STS)가 비활성화된 경우 파일 공유가 `CREATING` 또는 `UPDATING` 상태에서 멈출 수 있습니다.

AWS STS 상태를 확인하려면:

1. https://console.aws.amazon.com/iam/ AWS Identity and Access Management 콘솔을 엽니다.
2. 탐색 창에서 계정 설정(Account settings)를 선택합니다.
3. 보안 토큰 서비스(STS) 섹션에서 파일 공유를 생성하려는 AWS 리전의 상태가 활성인지 확인합니다.
4. 상태가 비활성인 경우 활성화를 선택하여 해당 리전 AWS STS 에서를 활성화합니다.

S3 버킷이 존재하고 이름 지정 규칙을 따르는지 확인

파일 공유에는 Amazon S3 명명 규칙을 따르는 유효한 Amazon S3 버킷이 필요합니다.

S3 버킷을 확인하려면:

1. https://console.aws.amazon.com/s3/에서 S3 콘솔을 엽니다.
2. 파일 공유에 매핑된 Amazon S3 버킷이 있는지 확인합니다. 버킷이 없는 경우 버킷을 생성합니다. 버킷을 생성한 후 파일 공유 상태가 로 변경됩니다`AVAILABLE`. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 버킷 생성을 참조하세요.
3. Amazon Simple Storage Service 사용 설명서의 버킷 이름이 버킷 이름 지정 규칙을 준수하는지 확인합니다.

> **Note**
>
> S3 File Gateway는 버킷 이름에 마침표(`.`)가 있는 Amazon S3 버킷을 지원하지 않습니다.

삭제 중 상태에서 멈춘 파일 공유 강제 삭제

파일 공유를 삭제하면 게이트웨이는 연결된 Amazon S3 버킷에서 공유를 제거합니다. 그러나 현재 업로드 중인 데이터는 삭제가 완료되기 전에 계속 업로드됩니다. 이 프로세스 중에 파일 공유에 `DELETING` 상태가 표시됩니다.

> **Important**
>
> `CachePercentDirty` 게이트웨이의 Amazon CloudWatch 지표를 확인하여 업로드 보류 중인 데이터의 양을 확인합니다. Storage Gateway 지표에 대한 자세한 내용은 섹션을 참조하세요the section called “S3 File Gateway 모니터링”.

진행 중인 모든 업로드가 완료될 때까지 기다리지 않으려면 파일 공유를 강제로 삭제할 수 있습니다.

파일 공유를 강제로 삭제하려면:

1. https://console.aws.amazon.com/storagegateway/ Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 파일 공유를 선택합니다.
3. 삭제할 파일 공유를 선택합니다.

4. 세부 정보 탭을 선택하고 이 파일 공유가 삭제 중입니다 메시지를 검토합니다.
5. 메시지에서 파일 공유의 ID를 확인한 다음 확인 상자를 선택합니다.

> **Note**
>
> 강제 삭제 작업은 취소할 수 없습니다.

6. 지금 강제 삭제를 선택합니다.

또는 `--force-delete` 파라미터가 로 설정된 상태에서 AWS CLI delete-file-share 명령을 사용할 수 있습니다`true`.

> **Important**
>
> 파일 공유를 강제로 삭제하기 전에 게이트웨이가 `OFFLINE` 상태가 아닌지 확인합니다. 게이트웨이가 오프라인 상태인 경우 먼저 오프라인 문제를 해결합니다. 자세한 내용은 the section called “문제 해결: 게이트웨이 오프라인 문제” 단원을 참조하십시오.

게이트웨이 가상 머신(VM)이 이미 삭제된 경우 Storage Gateway 콘솔에서 게이트웨이를 삭제하여 `DELETING` 상태에서 멈춘 파일 공유를 포함하여 연결된 모든 파일 공유를 제거해야 합니다. 자세한 내용은 the section called “게이트웨이 삭제 및 리소스 제거” 단원을 참조하십시오.

네트워크 연결 문제 해결

네트워크 문제로 인해 파일 공유가 `CREATING`, `UPDATING`또는 `DELETING` 상태에서 전환되지 않을 수 있습니다. 일반적인 네트워크 문제는 다음과 같습니다.

- 게이트웨이가 오프라인 상태이거나 게이트웨이 VM이 삭제됩니다.
- Storage Gateway와 Amazon S3 서비스 엔드포인트 간의 네트워크 액세스가 차단됩니다.
- 게이트웨이가 Amazon S3와 통신하는 데 사용하는 Amazon S3 Amazon VPC 엔드포인트가 삭제되었습니다.
- 필요한 네트워크 포트가 열려 있지 않거나 네트워크 라우팅이 잘못 구성되었습니다.

게이트웨이 로컬 콘솔에서 S3 연결 테스트

S3 연결을 테스트하려면:

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 자세한 내용은 the section called “File Gateway 로컬 콘솔에 로그인” 단원을 참조하십시오.
2. Storage Gateway - 구성 기본 메뉴에서 S3 연결 테스트에 해당하는 번호를 입력합니다.
3. Amazon S3 엔드포인트 유형을 선택합니다.
   - 인터넷 게이트웨이, NAT 게이트웨이, 전송 게이트웨이 또는 Amazon S3 게이트웨이 Amazon VPC 엔드포인트를 통해 흐르는 Amazon S3 트래픽의 경우 퍼블릭을 선택합니다.
   - Amazon S3 인터페이스 Amazon VPC 엔드포인트를 통해 흐르는 Amazon S3 트래픽의 경우 VPC(PrivateLink)를 선택합니다.
   - FIPS 엔드포인트의 경우 FIPS 옵션을 선택합니다.
4. Amazon S3 버킷 리전을 입력합니다.
5. Amazon VPC 엔드포인트를 사용하는 경우 Amazon S3 Amazon VPC 엔드포인트 DNS 이름(예: `vpce-0329c2790456f2d01-0at85l34`)을 입력합니다.

게이트웨이는 네트워크 연결과 SSL 연결을 모두 검증하는 연결 테스트를 자동으로 수행합니다. 테스트가 실패하는 경우:

- 네트워크 테스트 실패 - 일반적으로 방화벽 규칙, 보안 그룹 구성 또는 부적절한 네트워크 라우팅으로 인해 발생합니다. 필요한 포트가 열려 있고 네트워크 라우팅이 올바르게 구성되어 있는지 확인합니다.
- SSL 테스트 실패 - 게이트웨이 VM과 Amazon S3 서비스 엔드포인트 간에 SSL 검사 또는 심층 패킷 검사가 발생하고 있음을 나타냅니다. Storage Gateway 트래픽에 대한 SSL 및 심층 패킷 검사를 비활성화합니다.

프록시 구성 확인

게이트웨이가 프록시 서버를 사용하는 경우 프록시가 네트워크 통신을 차단하지 않는지 확인합니다.

프록시 구성을 확인하려면:

1. Storage Gateway - 구성 기본 메뉴에서 HTTP/SOCKS 프록시 구성에 해당하는 번호를 입력합니다.
2. 현재 네트워크 프록시 구성을 보려면 옵션을 선택합니다.

3. 프록시가 구성된 경우 Amazon S3 트래픽이 포트 3128(또는 구성된 리스너 포트)을 통해 Storage Gateway에서 프록시 서버로 흐른 다음 포트 443을 통해 Amazon S3 엔드포인트로 흐를 수 있는지 확인합니다.
4. 프록시 또는 방화벽이 Storage Gateway에 필요한 네트워크 포트 및 서비스 엔드포인트와의 트래픽을 허용하는지 확인합니다. 자세한 내용은 필요한 네트워크 포트를 참조하세요.

문제가 지속되면 프록시 구성을 일시적으로 제거하여 프록시가 문제를 일으키는지 확인할 수 있습니다.

보안 그룹 및 네트워크 라우팅 확인

- Amazon EC2의 게이트웨이의 경우 - 보안 그룹에 Amazon S3 엔드포인트에 개방된 포트 443이 있는지 확인합니다. Amazon EC2 서브넷의 라우팅 테이블이 Amazon S3 트래픽을 Amazon S3 엔드포인트로 올바르게 라우팅하는지 확인합니다. 자세한 내용은 필요한 네트워크 포트를 참조하세요.
- 온프레미스 게이트웨이의 경우 - 방화벽 규칙이 필요한 포트를 허용하고 로컬 라우팅 테이블이 Amazon S3 트래픽을 Amazon S3 엔드포인트로 올바르게 라우팅하는지 확인합니다. 자세한 내용은 필요한 네트워크 포트를 참조하세요.
- VPC 엔드포인트 - 게이트웨이에서 사용하는 Amazon S3 Amazon VPC 엔드포인트가 삭제되지 않았는지 확인합니다. Amazon VPC 엔드포인트가 삭제되고 게이트웨이에 퍼블릭 IP 주소가 없는 경우 게이트웨이가 Amazon S3와 통신할 수 없습니다.

파일 공유를 생성할 수 없음

1. 파일 공유가 CREATING 상태로 고착되어 파일 공유를 생성할 수 없는 경우 파일 공유를 매핑한 S3 버킷이 존재하는지 확인합니다. 이에 관한 자세한 내용은 위 파일 공유가 CREATING, UPDATING 또는 DELETING 상태에서 멈춤 섹션을 참조하세요.
2. S3 버킷이 있는 경우 파일 공유를 생성하는 리전에서 AWS Security Token Service 가 활성화되어 있는지 확인합니다. 보안 토큰이 활성화되지 않은 경우 활성화해야 합니다. 를 사용하여 토큰을 활성화하는 방법에 대한 자세한 내용은 IAM 사용 설명서의 AWS 리전에서 AWS STS 활성화 및 비활성화를 AWS Security Token Service참조하세요.

SMB 파일 공유가 여러 다른 액세스 방법을 허용하지 않음

SMB 파일 공유에는 다음과 같은 제약 조건이 있습니다.

1. 동일한 클라이언트가 Active Directory 및 게스트 액세스 SMB 파일 공유를 모두 탑재하려고 시도하면 다음 오류 메시지가 표시됩니다. `Multiple connections to a server or shared resource by the same user, using more than one user name, are not allowed. Disconnect all previous connections to the server or shared resource and try again.`
2. Windows 사용자는 두 개의 게스트 액세스 SMB 파일 공유에 연결된 상태를 유지할 수 없으며 새 게스트 액세스 연결이 설정되면 연결이 끊어질 수 있습니다.
3. Windows 클라이언트는 게스트 액세스와 동일한 게이트웨이에서 내보낸 Active Directory SMB 파일 공유를 모두 탑재할 수 없습니다.

여러 파일 공유가 매핑된 S3 버킷에 쓸 수 없음

여러 파일 공유가 하나의 S3 버킷에 쓸 수 있도록 S3 버킷을 구성하는 것은 권장하지 않습니다. 이 접근 방법은 예기치 않은 결과를 유발할 수 있습니다.

각 S3 버킷에 하나의 파일 공유만 쓸 수 있도록 허용하는 것이 좋습니다. 파일 공유와 연결된 역할만 버킷에 쓸 수 있도록 허용하는 버킷 정책을 생성합니다. 자세한 내용은 File Gateway의 모범 사례 섹션을 참조하세요.

감사 로그 사용 시 삭제된 로그 그룹에 대한 알림

로그 그룹이 없는 경우 사용자는 해당 메시지 아래의 로그 그룹 링크를 선택하여 새 로그 그룹을 생성하거나 기존 로그 그룹을 사용하여 감사 로그의 대상으로 사용할 수 있습니다.

S3 버킷에 파일을 업로드할 수 없음

S3 버킷에 파일을 업로드할 수 없는 경우 다음을 수행합니다.

1. Amazon S3 File Gateway가 파일을 S3 버킷으로 업로드하는 데 필요한 액세스 권한을 부여했는지 확인합니다. 자세한 내용은 Amazon S3 버킷에 액세스할 수 있는 권한 부여 단원을 참조하십시오.
2. 버킷을 생성한 역할이 S3 버킷에 쓸 수 있는 권한이 있는지 확인합니다. 자세한 내용은 File Gateway의 모범 사례 섹션을 참조하세요.
3. File Gateway가 암호화에 SSE-KMS 또는 DSSE-KMS를 사용하는 경우 파일 공유와 연결된 IAM 역할에 kms:Encrypt, kms:Decrypt, kms:ReEncrypt*, kms:GenerateDataKey 및 kms:DescribeKey 권한이 포함되어 있는지 확인합니다. 자세한 내용은 Storage Gateway에 대한 자격 증명 기반 정책(IAM 정책) 사용을 참조하세요.

SSE-KMS를 사용하여 내 S3 버킷에 저장된 개체를 암호화하도록 기본 암호화를 변경할 수 없음

기본 암호화를 변경하고 SSE-KMS(AWS KMS관리형 키를 통한 서버 측 암호화)를 S3 버킷의 기본값으로 설정하는 경우 Amazon S3 File Gateway가 버킷에 저장하는 객체는 SSE-KMS로 암호화되지 않습니다. S3 File Gateway는 기본적으로 S3 버킷에 데이터를 작성할 때 Amazon S3를 통해 관리하는 서버 측 암호화(SSE-S3)를 사용합니다. 기본값을 변경해도 암호화가 자동으로 변경되지 않습니다.

자체 AWS KMS 키와 함께 SSE-KMS를 사용하도록 암호화를 변경하려면 SSE-KMS 암호화를 켜야 합니다. 이때는 파일 공유를 생성하면서 KMS 키의 Amazon 리소스 이름(ARN)을 입력합니다. 그 밖에 `UpdateNFSFileShare` 또는 `UpdateSMBFileShare` API 작업을 통해 파일 공유에 대한 KMS 설정을 업데이트할 수도 있습니다. 이렇게 업데이트하면 이후 S3 버킷에 저장된 객체에 적용됩니다. 자세한 내용은 를 사용한 데이터 암호화 AWS KMS 단원을 참조하십시오.

객체 버전 관리가 켜져 있는 S3 버킷에서 직접 변경하면 파일 공유에 표시되는 내용에 영향을 미칠 수 있습니다.

S3 버킷에 다른 클라이언트가 기록한 객체가 있는 경우, S3 버킷 객체 버전 관리의 결과로 S3 버킷 보기가 최신이 아닐 수 있습니다. 관심 있는 파일을 검사하기 전에 항상 캐시를 새로 고쳐야 합니다.

객체 버전 관리는 동일한 이름의 객체 사본을 여러 개 저장하여 데이터를 보호해 주는 S3 버킷의 옵션 기능입니다. 각 사본에는 서로 다른 ID 값이 있습니다(예: `file1.jpg: ID="xxx"` 및 `file1.jpg: ID="yyy"`). 동일한 이름의 객체 수와 수명은 Amazon S3 수명 주기 정책으로 제어됩니다. 이러한 Amazon S3 개념에 대한 자세한 내용은 Amazon S3 개발자 안내서의 버전 관리 사용 및 객체 수명 주기 관리를 참조하세요.

버전이 지정된 객체를 삭제할 경우 해당 객체에 삭제 마커가 표시되지만 보존됩니다. S3 버킷 소유자만 버전 관리가 켜져 있는 객체를 영구적으로 삭제할 수 있습니다.

S3 File Gateway에서 표시되는 파일은 객체를 가져왔거나 캐시를 새로 고쳤을 당시에 S3 버킷의 최신 객체 버전입니다. S3 File Gateway는 삭제 표시된 모든 객체 또는 이전 버전을 무시합니다. 파일을 읽을 때 최신 버전에서 데이터를 읽습니다. 파일 공유에 파일을 쓰면 S3 File Gateway는 변경 사항이 있는 새 버전의 명명된 객체를 만들며, 이 버전이 최신 버전이 됩니다.

S3 File Gateway는 이전 버전에서 계속 읽으며, 애플리케이션 외부의 S3 버킷에 새 버전이 추가되면 이전 버전을 기반으로 업데이트를 수행합니다. 최신 버전의 객체를 읽으려면 RefreshCache API 작업을 사용하거나 Amazon S3 버킷 객체 새로 고침에 설명된 대로 콘솔에서 새로 고칩니다.

> **Important**
>
> 파일 공유 외부에서 S3 File Gateway S3 버킷에 객체 또는 파일을 기록하지 않는 것이 좋습니다.

버전 관리가 켜져 있는 S3 버킷에 쓸 때 Amazon S3 File Gateway는 여러 버전의 Amazon S3 객체를 생성할 수 있습니다.

객체 버전 관리를 켜면 NFS 또는 SMB 클라이언트의 파일을 업데이트할 때마다 Amazon S3에 여러 버전의 객체가 생성될 수 있습니다. 다음은 S3 버킷에 여러 버전의 객체가 생성될 수 있는 시나리오입니다.

- 파일이 Amazon S3에 업로드된 후 NFS 또는 SMB 클라이언트에 의해 Amazon S3 File Gateway에서 수정된 경우 S3 File Gateway는 전체 파일을 업로드하는 대신 새 데이터 또는 수정된 데이터를 업로드합니다. 파일을 수정하면 Amazon S3 객체의 새 버전이 생성됩니다.
- 파일이 NFS 또는 SMB 클라이언트에 의해 S3 File Gateway에 기록되면 S3 File Gateway는 파일의 데이터를 Amazon S3에 업로드한 다음 메타데이터(소유권, 타임스탬프 등)를 업로드합니다. 파일 데이터를 업로드하면 Amazon S3 객체가 생성되고 파일의 메타데이터를 업로드하면 Amazon S3 객체의 메타데이터가 업데이트됩니다. 이 프로세스는 객체의 다른 버전을 생성하여 객체의 두 버전을 생성합니다.
- S3 File Gateway가 더 큰 파일을 업로드하는 경우 클라이언트가 File Gateway에 쓰기를 완료하기 전에 작은 파일 청크를 업로드해야 할 수 있습니다. 여기에는 캐시 공간 확보 또는 파일에 대한 높은 쓰기 속도가 포함됩니다. 이로 인해 S3 버킷에 여러 버전의 객체가 생성될 수 있습니다.

객체를 다른 스토리지 클래스로 이동하도록 수명 주기 정책을 설정하기 전에 S3 버킷을 모니터링하여 객체의 버전 수를 확인해야 합니다. S3 버킷의 객체에 대한 버전 수를 최소화하려면 이전 버전의 수명 주기 만료를 구성해야 합니다. S3 버킷 간에 동일 리전 복제(SRR) 또는 교차 리전 복제(CRR)를 사용하면 사용되는 스토리지가 증가합니다. 복제에 대한 자세한 내용은 복제 섹션을 참조하세요.

> **Important**
>
> 객체 버전 관리가 켜져 있을 때 사용되는 스토리지의 양을 이해할 때까지 S3 버킷 간 복제를 구성하지 마십시오.

버전이 지정된 S3 버킷 사용은 Amazon S3의 스토리지의 양을 크게 늘릴 수 있습니다. 파일에 대한 각 수정이 S3 객체의 새 버전을 생성하기 때문입니다. 이 동작을 재정의하고 유지되는 버전 수를 제한하는 정책을 특별히 만들지 않는 한, 기본적으로 Amazon S3는 이러한 모든 버전을 계속 저장합니다. 객체 버전 관리 사용으로 스토리지 사용량이 비정상적으로 많아지면, 스토리지 정책이 적절하게 설정되어 있는지 확인하십시오. 브라우저 요청에 대한 `HTTP 503-slow down` 응답 수 증가도 객체 버전 관리 문제로 인해 발생한 결과일 수 있습니다.

S3 File Gateway를 설치한 후 객체 버전 관리를 활성화하면, 고유한 모든 객체가 보존되며 (`ID="NULL"`) 파일 시스템에서 이를 모두 볼 수 있습니다. 새 버전의 객체에는 고유한 ID가 할당됩니다 (이전 버전은 유지됨). 객체의 타임스탬프를 기반으로 최신 버전의 객체만 NFS 파일 시스템에서 볼 수 있습니다.

객체 버전 관리를 활성화한 후에는 S3 버킷을 버전 관리를 사용하지 않는 상태로 되돌릴 수 없습니다. 그러나 버전 관리를 일시 중지할 수는 있습니다. 버전 관리를 일시 중지하면 새 객체에 ID가 할당됩니다. 동일한 이름의 객체가 `ID="NULL"` 값으로 존재하는 경우, 이전 버전을 덮어쓰게 됩니다. 그러나 `NULL`이 아닌 ID가 포함된 모든 버전은 유지됩니다. 타임스탬프는 새 객체를 최신 객체로 식별하며, 이 객체가 NFS 파일 시스템에 표시됩니다.

S3 버킷에 대한 변경 사항은 Storage Gateway에 반영되지 않습니다.

Storage Gateway는 파일 공유를 사용하여 로컬에서 캐시에 파일을 쓸 때 파일 공유 캐시를 자동으로 업데이트합니다. 그러나 파일을 Amazon S3에 직접 업로드할 때 Storage Gateway는 캐시를 자동으로 업데이트하지 않습니다. 이렇게 하려면 `RefreshCache` 작업을 수행하여 파일 공유의 변경 사항을 확인해야 합니다. 파일 공유가 두 개 이상인 경우 각 파일 공유에서 `RefreshCache` 작업을 실행해야 합니다.

Storage Gateway 콘솔과 AWS Command Line Interface (AWS CLI)를 사용하여 캐시를 새로 고칠 수 있습니다.

- Storage Gateway 콘솔을 사용하여 캐시를 새로 고치려면 Amazon S3 버킷의 객체 새로 고침을 참조하세요.
- AWS CLI를 사용하여 캐시를 새로 고치려면:
  1. `aws storagegateway list-file-shares` 명령 실행
  2. 파일 공유의 Amazon 리소스 번호(ARN)를 새로 고치려는 캐시로 복사합니다.
  3. ARN을 `--file-share-arn`의 값으로 사용하여 `refresh-cache` 명령을 실행합니다.

     ```
     aws storagegateway refresh-cache --file-share-arn
     arn:aws:storagegateway:eu-west-1:12345678910:share/share-FFDEE12
     ```

`RefreshCache` 작업을 자동화하려면 Storage Gateway에서 RefreshCache 작업을 자동화하려면 어떻게 해야 합니까?를 참조하세요.

ACL 권한이 예상대로 작동하지 않음

ACL(액세스 제어 목록) 권한이 SMB 파일 공유에서 예상대로 작동하지 않을 경우에는 테스트를 실시하십시오.

먼저 Microsoft Windows 파일 서버 또는 로컬 Windows 파일 공유에서 권한을 테스트해봅니다. 그런 다음 그 동작을 게이트웨이의 파일 공유와 비교합니다.

재귀 작업을 수행한 후 게이트웨이 성능 저하됨

일부 경우에서는 재귀 작업을 수행하고(예: 디렉터리 이름 바꾸기 또는 ACL 상속 활성화) 트리에 적용할 수 있습니다. 이 경우 S3 File Gateway가 파일 공유의 모든 객체에 이 작업을 재귀적으로 적용합니다.

예를 들어, S3 버킷의 기존 객체에 상속을 적용하는 경우, S3 File Gateway는 버킷의 모든 객체에 상속을 재귀적으로 적용합니다. 이러한 작업 때문에 게이트웨이 성능이 거부될 수 있습니다.

고가용성 상태 알림

VMware vSphere HA(고가용성) 플랫폼에서 게이트웨이를 실행할 때 상태 알림을 받을 수 있습니다. 상태 알림에 대한 자세한 내용은 문제 해결: 고가용성 문제 섹션을 참조하세요.

문제 해결: 고가용성 문제

가용성 문제가 발생할 경우 수행할 작업에 대한 다음 정보를 찾을 수 있습니다.

주제

- 상태 알림
- Metrics

상태 알림

VMware vSphere HA에서 게이트웨이를 실행하면 모든 게이트웨이에서는 구성된 Amazon CloudWatch 로그 그룹에 다음과 같은 상태 알림을 생성합니다. 이러한 알림은 `AvailabilityMonitor`라는 로그 스트림으로 이동합니다.

주제

알림: 재부팅

게이트웨이 VM을 다시 시작할 때 재부팅 알림을 받을 수 있습니다. VM 하이퍼바이저 관리 콘솔 또는 Storage Gateway 콘솔을 사용하여 게이트웨이 VM을 다시 시작할 수 있습니다. 게이트웨이의 유지 관리 주기 동안 게이트웨이 소프트웨어를 사용하여 다시 시작할 수도 있습니다.

취할 조치

재부팅이 게이트웨이에서 구성된 유지 관리 시작 시간 10분 이내에 수행되는 경우 이는 정상적인 현상일 수 있으며 문제의 징조가 아닙니다. 유지 관리 기간을 크게 벗어나 재부팅이 수행된 경우 게이트웨이가 수동으로 다시 시작되었는지 확인합니다.

알림: HardReboot

게이트웨이 VM이 예기치 않게 다시 시작될 때 `HardReboot` 알림을 받을 수 있습니다. 이러한 다시 시작의 원인은 정전, 하드웨어 오류 또는 다른 이벤트일 수 있습니다. VMware 게이트웨이의 경우 vSphere 고가용성 애플리케이션 모니터링을 통해 재설정하면 이 이벤트가 시작될 수 있습니다.

취할 조치

게이트웨이가 이러한 환경에서 실행되는 경우 `HealthCheckFailure` 알림이 있는지 확인하고 VM에 대한 VMware 이벤트 로그를 참조하세요.

알림: HealthCheckFailure

VMware vSphere HA에 대한 게이트웨이의 경우 상태 확인에 실패하고 VM 다시 시작을 요청하면 `HealthCheckFailure` 알림을 받을 수 있습니다. 이 이벤트는 `AvailabilityMonitorTest` 알림으로 표시된 가용성을 모니터하기 위한 테스트 도중에도 발생합니다. 이 경우 `HealthCheckFailure` 알림이 예상됩니다.

> **Note**
>
> 이 알림은 VMware 게이트웨이에만 적용됩니다.

취할 조치

`AvailabilityMonitorTest` 알림 없이 이 이벤트가 반복적으로 발생하면 VM 인프라(스토리지, 메모리 등)에 문제가 있는지 확인하십시오. 추가 지원이 필요한 경우에 문의하십시오 지원.

알림: AvailabilityMonitorTest

VMware vSphere HA의 게이트웨이의 경우 VMware에서 가용성 및 애플리케이션 모니터링 시스템 테스트를 실행할 때 `AvailabilityMonitorTest` 알림을 받을 수 있습니다.

Metrics

`AvailabilityNotifications` 지표는 모든 게이트웨이에서 사용할 수 있습니다. 이 지표는 게이트웨이에 의해 생성된 가용성 관련 상태 알림의 개수입니다. `Sum` 통계를 사용하여 게이트웨이에 가용성 관련 이벤트가 발생하는지 여부를 확인할 수 있습니다. 이벤트에 대한 자세한 내용은 구성된 CloudWatch 로그 그룹에 문의하십시오.

File Gateway 모범 사례

이 섹션은 다음 주제로 구성되어 있으며, 게이트웨이, 파일 공유, 버킷 및 데이터를 다루는 모범 사례에 대한 정보를 제공합니다. AWS Storage Gateway와 관련된 문제를 방지하기 위해 이 단원에 설명된 정보를 숙지하고 이 지침을 따르는 것이 좋습니다. 배포 시 발생할 수 있는 일반적인 문제를 진단하고 해결하는 방법에 대한 자세한 내용은 Storage Gateway 배포 문제 해결 섹션을 참조하세요.

주제

모범 사례: 데이터 복구

드물긴 하지만 게이트웨이에 복구 불가능한 장애가 발생할 수 있습니다. 그러한 장애는 가상 머신(VM), 게이트웨이 자체, 로컬 스토리지 등에서 발생할 수 있습니다. 장애가 발생하면 이어지는 적절한 섹션의 지침에 따라 테이프를 복구하는 것이 좋습니다.

> **Important**
>
> Storage Gateway는 하이퍼바이저에서 생성한 스냅샷 또는 Amazon EC2 Amazon Machine Image(AMI)에서 게이트웨이 VM을 복구하는 기능을 지원하지 않습니다. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 다음 지침에 따라 새 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다.

가상 머신이 예기치 않게 종료된 상황에서 복구하기

예를 들어 정전으로 인해 VM이 예기치 않게 종료된 경우, 게이트웨이에 접속할 수 없습니다. 전원과 네트워크 연결이 복구되면 게이트웨이에 접속할 수 있고 게이트웨이가 정상적으로 작동하기 시작합니다. 다음은 이 시점에 수행할 수 있는 데이터 복구 지원 절차입니다.

- 정전으로 인해 네트워크 연결에 문제가 발생하면 그 문제를 해결할 수 있습니다. 네트워크 연결을 테스트하는 방법에 대한 정보는 게이트웨이 네트워크 연결 테스트섹션을 참조하세요.

장애가 있는 캐시 디스크에서 데이터 복구

캐시 디스크에 장애가 발생하면 다음 절차에 따라 처한 상황에 맞는 방법으로 데이터를 복구하는 것이 좋습니다.

- 호스트에서 캐시 디스크가 제거되어 장애가 발생한 경우, 게이트웨이를 종료하고 디스크를 다시 추가한 후 게이트웨이를 다시 시작합니다.

액세스할 수 없는 데이터 센터에서 데이터 복구

게이트웨이 또는 데이터 센터에 대한 액세스가 어떤 이유로 차단되는 경우에는 데이터를 다른 데이터 센터의 다른 게이트웨이로 복구하거나 Amazon EC2 인스턴스에서 호스팅되는 게이트웨이로 복구할 수 있습니다. 따라서 다른 데이터 센터에 액세스할 수 없다면 Amazon EC2 인스턴스에서 게이트웨이를 생성하는 것이 좋습니다. 생성 방법은 데이터를 복구하는 게이트웨이 유형에 따라 다릅니다.

액세스할 수 없는 데이터 센터의 File Gateway에서 데이터를 복구하려면

File Gateway의 경우 복구하려는 데이터가 포함된 Amazon S3 버킷에 새 을 매핑합니다.

1. Amazon EC2 호스트에서 새 File Gateway를 생성하여 활성화합니다. 자세한 내용은 S3 File Gateway용 기본 Amazon EC2 호스트 배포 단원을 참조하십시오.
2. 생성한 EC2 게이트웨이에서 새로운 을 생성합니다. 자세한 내용은 파일 공유 생성을 참조하세요.
3. 파일 공유을 클라이언트에 마운트한 후 복구할 데이터가 저장된 S3 버킷로 매핑합니다. 자세한 내용은 파일 공유 탑재 및 사용을 참조하세요.

모범 사례: 멀티파트 업로드 관리

대용량 파일을 전송할 때 S3 File Gateway는 Amazon S3 멀티파트 업로드 기능을 사용하여 파일을 더 작은 부분으로 분할하고 병렬로 전송하여 효율성을 개선합니다. 멀티파트 업로드에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 멀티파트 업로드를 사용한 객체 업로드 및 복사를 참조하세요.

어떤 이유로든 멀티파트 업로드가 성공적으로 완료되지 않으면 게이트웨이는 일반적으로 전송을 중지하고 Amazon S3에서 부분적으로 전송된 파일을 삭제한 다음 전송을 다시 시도합니다. 드문 경우지만

하드웨어 또는 네트워크 장애로 인해 멀티파트 업로드 실패 후 게이트웨이가 정리되지 않는 경우 부분적으로 전송된 파일의 일부가 Amazon S3에 남아 있어 스토리지 요금이 발생할 수 있습니다.

불완전한 멀티파트 업로드로 인한 Amazon S3 스토리지 비용을 최소화하는 모범 사례로, 지정된 일 수 후에 `AbortIncompleteMultipartUpload` API 작업을 사용하여 전송 실패를 자동으로 중지하고 연결된 파일 부분을 삭제하는 Amazon S3 버킷 수명 주기 규칙을 구성하는 것이 좋습니다. 지침은 Amazon Simple Storage Service 사용 설명서의 불완전한 멀티파트 업로드를 삭제하도록 버킷 수명 주기 구성을 참조하세요.

모범 사례: 게이트웨이에 복사하기 전에 압축된 파일의 압축을 로컬에서 풉니다.

게이트웨이에 저장되어 있는 동안 수천 개의 파일이 포함된 압축된 아카이브의 압축을 풀려고 하면 상당한 성능 관련 지연이 발생할 수 있습니다. 모든 유형의 네트워크 파일 공유에 많은 수의 파일이 포함된 아카이브의 압축을 풀려면 기본적으로 많은 양의 입력/출력 작업, 메타데이터 캐시 조작, 네트워크 오버헤드 및 지연 시간이 필요합니다. 또한 Storage Gateway는 아카이브의 각 파일의 압축 해제가 완료된 시기를 확인할 수 없으며, 프로세스가 완료되기 전에 파일 업로드를 시작할 수 있으므로 성능에 추가 영향을 미칩니다. 이러한 문제는 아카이브 내의 파일이 많지만 크기가 작을 때 복잡해집니다.

압축된 아카이브를 압축 해제하기 전에 먼저 게이트웨이에서 로컬 시스템으로 전송하는 것이 좋습니다. 그런 다음 필요한 경우 robocopy 또는 rsync와 같은 도구를 사용하여 압축을 푼 파일을 게이트웨이로 다시 전송할 수 있습니다.

Windows Server에서 데이터를 복사할 때 파일 속성 유지

Microsoft Windows의 기본 `copy` 명령을 사용하여 파일을 File Gateway에 복사할 수 있지만 이 명령은 기본적으로 파일 데이터만 복사하여 보안 설명자와 같은 특정 파일 속성을 생략합니다. 해당 보안 제한 및 임의 액세스 제어 목록(DACL) 정보 없이 파일을 게이트웨이에 복사하는 경우 권한이 없는 사용자가 파일에 액세스할 수 있습니다.

Microsoft Windows Server의 게이트웨이에 파일을 복사할 때 모든 파일 속성과 보안 정보를 보존하는 모범 사례로, 각각 `/copy:DS`또는 `/o` 플래그와 함께 `robocopy` 또는 `xcopy` 명령을 사용하는 것이 좋습니다. 자세한 내용은 Microsoft Windows Server 명령 참조 설명서의 robocopy 및 xcopy를 참조하세요.

모범 사례: 캐시 디스크의 적절한 크기 조정

최상의 성능을 위해서는 전체 디스크 캐시 크기가 활성 작업 세트의 크기를 포함할 만큼 커야 합니다. 읽기 중심 및 읽기/쓰기 혼합 워크로드의 경우 읽기에 대한 캐시 적중률을 높일 수 있습니다. S3 File Gateway의 `CacheHitPercent` 지표를 통해 이를 모니터링할 수 있습니다.

쓰기 작업이 많은 워크로드(예: 백업 및 아카이브용)의 경우 S3 File Gateway는 이 데이터를 Amazon S3에 비동기식으로 복사하기 전에 디스크 캐시의 수신 쓰기를 버퍼링합니다. 작성된 데이터를 버퍼링할 수 있는 충분한 캐시 용량이 있는지 확인해야 합니다. `CachePercentDirty` 지표는 아직 유지되지 않은 디스크 캐시의 백분율을 나타냅니다 AWS.

`CachePercentDirty`의 낮은 값이 바람직합니다. 지속적으로 100%에 가까운 값은 S3 File Gateway가 수신 쓰기 트래픽 속도를 따라잡을 수 없음을 나타냅니다. 프로비저닝된 디스크 캐시 용량을 늘리거나 S3 File Gateway에서 Amazon S3로 사용 가능한 전용 네트워크 대역폭을 늘리거나 둘 다 늘리면 이를 방지할 수 있습니다.

캐시 디스크 크기 조정에 대한 자세한 내용은 공식 Amazon Web Services YouTube 채널의 Amazon S3 File Gateway 캐시 크기 조정 모범 사례를 참조하세요.

여러 파일 공유 및 Amazon S3 버킷 작업

여러 게이트웨이 또는 파일 공유가 버킷에 쓸 수 있도록 단일 Amazon S3 버킷을 구성하면 결과를 예측할 수 없습니다. 예측할 수 없는 결과를 방지하기 위해 두 가지 방법 중 하나로 버킷을 구성할 수 있습니다. 다음 옵션 중에서 사용 사례에 가장 적합한 구성 방법을 선택합니다.

- 각 버킷에 하나의 파일 공유만 쓸 수 있도록 S3 버킷을 구성합니다. 다른 파일 공유를 사용하여 각 버킷에 씁니다.

  이를 수행하기 위해서는 버킷에서 객체를 추가 또는 삭제하기 위해 특정 파일 공유에 사용한 역할 이외의 모든 역할을 거부하는 S3 버킷 정책을 생성합니다. 각 버킷에 작성할 다른 파일 공유를 지정하여 각 버킷에 유사한 정책을 연결합니다.

  다음 예제 정책은 버킷을 생성한 역할을 제외한 모든 역할에 대해 S3 버킷에 쓸 수 있는 권한을 거부합니다. `s3:DeleteObject`를 제외한 모든 역할에 대해 `s3:PutObject` 및 `"TestUser"` 작업이 거부됩니다. 이 정책은 `"arn:aws:s3:::amzn-s3-demo-bucket/*"` 버킷의 모든 객체에 적용됩니다.

  JSON

```
{
```

```
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"DenyMultiWrite",
         "Effect":"Deny",
         "Principal":"*",
         "Action":[
            "s3:DeleteObject",
            "s3:PutObject"
         ],
         "Resource":"arn:aws:s3:::amzn-s3-demo-bucket/*",
         "Condition":{
            "StringNotLike":{
               "aws:userid":"TestUser:*"
            }
         }
      }
   ]
}
```

- 여러 파일 공유를 동일한 Amazon S3 버킷에 쓰려면 파일 공유가 동일한 객체에 동시에 쓰려고 시도하지 않도록 해야 합니다.

  이렇게 하려면 각 파일 공유에 대해 별도의 고유한 객체 접두사를 구성합니다. 즉, 각 파일 공유는 해당 접두사가 있는 객체에만 쓰고 배포의 다른 파일 공유와 연결된 객체에는 쓰지 않습니다. 새 파일 공유를 생성할 때 S3 접두사 이름 필드에서 객체 접두사를 구성합니다.

불필요한 리소스 정리

예기치 않거나 불필요한 요금이 발생하지 않도록 Storage Gateway 리소스를 정리하는 것이 가장 좋습니다. 예를 들어 데모 연습 또는 테스트로 게이트웨이를 생성한 경우 배포에서 게이트웨이와 가상 어플라이언스를 삭제하는 것이 좋습니다. 다음 절차에 따라 리소스를 정리합니다.

필요 없는 리소스를 정리하려면

1. 더 이상 게이트웨이를 계속 사용할 계획이 없는 경우 삭제합니다. 자세한 내용은 게이트웨이 삭제 및 연결된 리소스 제거 단원을 참조하십시오.
2. 온프레미스 호스트에서 Storage Gateway VM을 삭제합니다. Amazon EC2 인스턴스에서 게이트웨이를 생성한 경우에는 해당 인스턴스를 종료합니다.

추가 Storage Gateway 리소스

이 섹션에는 AWS Storage Gateway설정 및 사용과 관련된 추가 정보와 리소스를 제공하는 다음 주제가 포함되어 있습니다.

주제

- 호스트 설정 - 게이트웨이용 가상 머신 호스트를 배포하고 구성하는 방법에 대해 알아봅니다.
- VMware HA에서 Storage Gateway 사용 - VMware vSphere 고가용성 기능과 함께 작동하도록 Storage Gateway를 설정하는 방법을 알아봅니다.
- 정품 인증 키 가져오기 - 새 게이트웨이를 배포할 때 제공해야 하는 활성화 키를 찾을 수 있는 위치에 대해 알아봅니다.
- 파일 속성 지원 - 게이트웨이가 DOS 및 Windows 파일 속성을 처리하는 방법을 알아봅니다.
- 사용 Direct Connect - 온프레미스 게이트웨이와 AWS 클라우드 간에 전용 네트워크 연결을 생성하는 방법에 대해 알아봅니다.
- Active Directory 권한 - 서비스 계정이 게이트웨이를 Active Directory 도메인에 조인할 수 있으려면 어떤 권한을 갖고 있어야 하는지 알아봅니다.
- 게이트웨이 어플라이언스의 IP 주소 가져오기 - 새 게이트웨이를 배포할 때 제공해야 하는 게이트웨이의 가상 머신 호스트 IP 주소를 찾을 수 있는 위치에 대해 알아봅니다.
- 리소스 및 리소스 ID 이해 -가 Storage Gateway에서 생성한 리소스 및 하위 리소스를 AWS 식별하는 방법을 알아봅니다.
- 리소스에 태깅 - 메타데이터 태그를 사용하여 리소스를 분류하고 더 쉽게 관리할 수 있는 방법에 대해 알아봅니다.
- 오픈 소스 구성 요소 - Storage Gateway 기능을 제공하는 데 사용되는 타사 도구 및 라이선스에 대해 알아봅니다.
- 할당량 - 파일 공유 및 로컬 캐시 디스크의 최소 및 최대 제한을 포함하여 File Gateway의 제한 및 할당량에 대해 알아봅니다.
- 스토리지 클래스 사용 - File Gateway가 지원하는 Amazon S3 스토리지 클래스와 스토리지 클래스를 선택할 때 고려해야 할 사항에 대해 알아봅니다.
- Kubernetes CSI 드라이버 사용 - Kubernetes 인스턴스가 스토리지에 File Gateway를 사용할 수 있도록 컨테이너 스토리지 인터페이스(CSI) 드라이버를 설치하고 구성하는 방법을 알아봅니다.
- Terraform 모듈 - Terraform을 사용하여 File Gateway를 가상 머신으로 배포하는 방법을 알아봅니다.

게이트웨이 VM 호스트 배포 및 구성

다음 주제에서는 게이트웨이의 가상 머신 호스트 플랫폼 설정에 대한 정보를 제공합니다.

주제

S3 File Gateway용 기본 Amazon EC2 호스트 배포

이 주제에서는 기본 지정 사항으로 Amazon EC2 호스트를 배포하는 단계에 대해 설명합니다.

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Amazon S3 File Gateway를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon 머신 이미지(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

> **Note**
>
> Storage Gateway 커뮤니티 AMI는 AWS에서 게시하고 완벽하게 지원합니다. 게시자가 AWS 확인된 공급자임을 알 수 있습니다.

1. Amazon EC2 인스턴스를 설정하려면 워크플로의 플랫폼 옵션 섹션에서 Amazon EC2를 호스트 플랫폼으로 선택합니다. Amazon EC2 인스턴스 구성에 대한 지침은 Amazon S3 File Gateway를 호스팅할 Amazon EC2 인스턴스 배포를 참조하세요.
2. 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 열고 인스턴스 유형, 네트워크 설정 및 스토리지 구성과 같은 추가 설정을 사용자 지정합니다.
3. (선택 사항) Storage Gateway 콘솔에서 기본 설정 사용을 선택하여 기본 구성으로 Amazon EC2 인스턴스를 배포할 수 있습니다.

   기본 설정 사용으로 생성되는 Amazon EC2 인스턴스의 기본 지정사항은 다음과 같습니다.

- 인스턴스 유형 - m5.xlarge
- 네트워크 설정
  - VPC에서 EC2 인스턴스를 실행할 VPC를 선택합니다.
  - 서브넷에서 EC2 인스턴스를 시작할 서브넷을 지정합니다.

> **Note**
>
> VPC 서브넷은 VPC 관리 콘솔에서 퍼블릭 IP 주소 자동 할당 설정이 활성화된 경우에만 드롭다운에 표시됩니다.

  - 퍼블릭 IP 자동 할당 - 활성화됨
  - EC2 보안 그룹이 생성되고 EC2 인스턴스와 연결됩니다. 보안 그룹에는 다음과 같은 인바운드 포트 규칙이 적용됩니다.

> **Note**
>
> 게이트웨이 활성화 중에는 포트 80이 열려 있어야 합니다. 활성화 후에는 포트가 즉시 닫힙니다. 이후에는 선택한 VPC의 다른 포트를 통해서만 EC2 인스턴스에 액세스할 수 있습니다.
> 게이트웨이의 파일 공유는 게이트웨이와 동일한 VPC에 있는 호스트에서만 액세스할 수 있습니다. VPC 외부의 호스트에서 파일 공유에 액세스해야 하는 경우 적절한 보안 그룹 규칙을 업데이트해야 합니다.
> Amazon EC2 인스턴스 세부 정보 페이지로 이동한 후 보안을 선택하고 보안 그룹 세부 정보로 이동한 다음 보안 그룹 ID를 선택하여 언제든지 보안 그룹을 편집할 수 있습니다.

포트	프로토콜	파일 시스템 프로토콜				
80	TCP	활성화를 위한 HTTP 액세스				

포트	프로토콜	파일 시스템 프로토콜				
111	TCP, UDP	NFSv3				
139	TCP, UDP	SMB				
445	TCP	SMB				
2049	TCP, UDP	NFS				
20048	TCP, UDP	NFSv3				

- 스토리지 구성

기본 설정	AMI 루트 볼륨	볼륨 2 캐시				
디바이스 이름		'/dev/sdb'				
Size:	80GiB	165GiB				
볼륨 유형	gp3	gp3				
IOPS	3000	3000				
종료 시 삭제	예	예				
암호화됨	아니요	아니요				
처리량	125	125				

S3 File Gateway용 사용자 지정 Amazon EC2 호스트 배포

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Amazon S3 File Gateway를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon 머신 이미지(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

> **Note**
>
> Storage Gateway 커뮤니티 AMI는 AWS에서 게시하고 완벽하게 지원합니다. 게시자가 AWS 확인된 공급자임을 알 수 있습니다.
> S3 File Gateway AMI는 다음과 같은 명명 규칙을 사용합니다. AMI 이름에 추가되는 버전 번호는 각 버전 릴리스에 따라 변경됩니다.
> `aws-storage-gateway-FILE_S3-1.25.0`

Amazon S3 File Gateway를 호스팅할 Amazon EC2 인스턴스를 배포하려면

1. Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Amazon S3 File Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에서 Amazon EC2를 호스트 플랫폼으로 선택한 후 다음 단계를 수행하여 File Gateway를 호스팅할 Amazon EC2 인스턴스를 시작합니다.
2. 인스턴스 시작을 선택하여 추가 설정을 구성할 수 있는 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 엽니다.

   기본 설정으로 Amazon EC2 인스턴스를 시작하려면 QuickLaunch를 사용합니다. Amazon EC2 Quicklaunch 기본 사양에 대한 자세한 내용은 Amazon EC2의 Quicklaunch 구성 사양을 참조하세요.
3. 이름에 Amazon EC2 인스턴스의 이름을 입력합니다. 인스턴스를 배포한 후 이 이름을 검색하여 Amazon EC2 콘솔의 목록 페이지에서 인스턴스를 찾을 수 있습니다.
4. 인스턴스 유형 섹션의 인스턴스 유형에서 인스턴스의 하드웨어 구성을 선택합니다. 하드웨어 구성은 게이트웨이를 지원하기 위한 특정 최소 요구 사항을 충족해야 합니다. 게이트웨이가 제대로 작동하기 위한 최소 하드웨어 요구 사항을 충족하는 m5.xlarge 인스턴스 유형으로 시작하는 것이 좋습니다. 자세한 내용은 Amazon EC2 인스턴스 유형에 대한 요구 사항 단원을 참조하십시오.

   필요하다면 시작한 후 인스턴스 크기를 조정할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서에서 인스턴스 크기 조정을 참조하세요.

> **Note**
>
> 특히 i3 EC2 같은 특정한 인스턴스 유형은 NVMe SSD 디스크를 사용합니다. 이러한 경우 File Gateway를 시작하거나 중지할 때 문제가 발생할 수 있습니다. 예를 들어 캐시에서 데이터가 손실될 수 있습니다. `CachePercentDirty` Amazon CloudWatch 지표를 모니터링하여 해당 파라미터가 `0`일 때만 시스템을 시작하거나 중지하세요. 게이트웨이 지표 모니터링에 대한 자세한 내용은 CloudWatch 설명서에서 Storage Gateway 지표 및 차원 섹션을 참조하세요.

5. 키 페어(로그인) 섹션에서 키 페어 이름 - 필수에서 인스턴스에 안전하게 연결하는 데 사용할 키 페어를 선택합니다. 필요한 경우 키 페어를 새로 생성할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 키 페어 생성을 참조하세요.
6. 네트워크 설정 섹션에서 사전 구성된 설정을 검토하고 편집을 선택하여 다음 필드를 변경합니다.
   a. VPC - 필수에서 Amazon EC2 인스턴스를 시작할 VPC를 선택합니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서에서 Amazon VPC 작동 방식을 참조하세요.
   b. (선택 사항) 서브넷에서 Amazon EC2 인스턴스를 시작할 서브넷을 선택합니다.
   c. 퍼블릭 IP 자동 할당(Auto-assign Public IP)의 경우 활성화(Enable)를 선택합니다.
7. 방화벽(보안 그룹) 하위 섹션에서 사전 구성된 설정을 검토합니다. 원하는 경우 Amazon EC2 인스턴스용으로 생성할 새 보안 그룹의 기본 이름과 설명을 변경하거나, 기존 보안 그룹의 방화벽 규칙을 적용하도록 선택할 수도 있습니다.
8. 인바운드 보안 그룹 규칙 하위 섹션에서 클라이언트가 인스턴스에 연결하는 데 사용할 포트를 여는 방화벽 규칙을 추가합니다. Amazon S3 File Gateway에 필요한 포트에 대한 자세한 내용은 포트 요구 사항을 참조하세요. 방화벽 규칙 추가에 대한 자세한 정보는 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 보안 그룹 규칙을 참조하세요.

> **Note**
>
> Amazon S3 File Gateway에서는 인바운드 트래픽과 게이트웨이 활성화 중 일회성 HTTP 액세스를 위해 TCP 포트 80을 열어야 합니다. 활성화한 후에는 이 포트를 닫을 수 있습니다.
>
> NFS 파일 공유를 생성하려는 경우 NFS 액세스의 경우 TCP/UDP 포트 2049, NFSv3 액세스의 경우 TCP/UDP 포트 111, NFSv3 액세스의 경우 TCP/UDP 포트 20048을 열어야 합니다.
>
> SMB 파일 공유를 생성하려는 경우 SMB 액세스를 위해 TCP 포트 445를 열어야 합니다.

9. 고급 네트워크 구성 하위 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
10. 스토리지 구성 섹션에서 새 볼륨 추가를 선택하여 게이트웨이 인스턴스에 스토리지를 추가합니다.

    > **Important**
    >
    > 미리 구성된 루트 볼륨 외에도 캐시 스토리지 용량이 150GiB 이상인 Amazon EBS 볼륨을 하나 이상 추가해야 합니다. 성능을 높이려면 캐시 스토리지에 각각 150GiB 이상의 EBS 볼륨을 여러 개 할당하는 것이 좋습니다.

11. 고급 세부 정보 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
12. 인스턴스 시작을 선택하여 새 Amazon EC2 게이트웨이 인스턴스를 구성된 설정으로 시작합니다.
13. 새 인스턴스가 성공적으로 시작되었는지 확인하려면 Amazon EC2 콘솔의 인스턴스 페이지로 이동하여 새 인스턴스를 이름으로 검색합니다. 인스턴스 상태가 녹색 확인 표시와 함께 실행 중으로 표시되고 상태 검사가 완료되어 녹색 확인 표시가 나타나는지 확인합니다.
14. 세부 정보 페이지에서 해당 인스턴스를 선택합니다. 인스턴스 요약 섹션에서 퍼블릭 IP 주소를 복사한 다음 Storage Gateway 콘솔의 게이트웨이 설정 페이지로 돌아가서 Amazon S3 File Gateway 설정을 재개합니다.

Storage Gateway 콘솔을 사용하거나 AWS Systems Manager 파라미터 스토어를 쿼리하여 파일 게이트웨이를 시작하는 데 사용할 AMI ID를 확인할 수 있습니다.

AMI ID를 확인하려면 다음 중 하나를 수행합니다.

- Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Amazon S3 File Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에 도달하면 Amazon EC2를 호스트 플랫폼으로 선택한 다음 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 엽니다.

  EC2 커뮤니티 AMI 페이지로 리디렉션되며, URL에서 해당 AWS 리전의 AMI ID를 볼 수 있습니다.
- Systems Manager 파라미터 스토어를 쿼리합니다. AWS CLI 또는 Storage Gateway API를 사용하여 네임스페이스 아래의 Systems Manager 퍼블릭 파라미터를 쿼리할 수 있습니다`/aws/service/storagegateway/ami/FILE_S3/latest`. 예를 들어 다음 CLI 명령을 사용하면 AWS 리전 지정한에서 현재 AMI의 ID가 반환됩니다.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
FILE_S3/latest
```

이 CLI 명령은 다음과 비슷한 출력을 반환합니다.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/
FILE_S3/latest",
        "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Amazon EC2 인스턴스 메타데이터 옵션 수정

인스턴스 메타데이터 서비스(IMDS)는 Amazon EC2 인스턴스 메타데이터에 대한 보안 액세스를 제공하는 온 인스턴스 구성 요소입니다. IMDS 버전 1(IMDSv1)을 사용하는 수신 메타데이터 요청을 수락하거나 모든 메타데이터 요청이 IMDS 버전 2(IMDSv2)를 반드시 사용하도록 인스턴스를 구성할 수 있습니다. IMDSv2는 세션 지향 요청을 사용하며 IMDS에 액세스하기 위해 사용될 수 있는 여러 유형의 취약성을 완화합니다. IMDSv2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서에서 인스턴스 메타데이터 서비스 버전 2 작동 방식을 참조하세요.

Storage Gateway를 호스팅하는 모든 Amazon EC2 인스턴스에는 IMDSv2를 반드시 사용해야 합니다. 새로 시작되는 모든 게이트웨이 인스턴스에는 기본적으로 IMDSv2가 필요합니다. IMDSv1 메타데이터 요청을 수락하도록 구성된 기존 인스턴스가 아직 있는 경우,Amazon Elastic Compute Cloud 사용 설명서의 IMDSv2 사용 요구 섹션을 참조하여 IMDSv2를 사용하도록 인스턴스 메타데이터 옵션을 수정합니다. 이 변경 사항을 적용해도 인스턴스를 재부팅할 필요는 없습니다.

Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화

VMware ESXi에 배포된 게이트웨이의 경우 하이퍼바이저 호스트 시간을 설정하고 가상 머신 시간을 호스트와 동기화하는 것만으로도 충분히 시간 편차를 방지할 수 있습니다. 자세한 내용은 VM 시간을 VMware 호스트 시간과 동기화 단원을 참조하십시오. Microsoft Hyper-V 또는 Linux KVM에 배포된 게이트웨이의 경우 다음 절차를 수행하여 가상 머신 시간을 주기적으로 확인하는 것이 좋습니다.

하이퍼바이저 게이트웨이 가상 머신의 시간을 확인하고 NTP(Network Time Protocol) 서버와 동기화하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Linux 커널 기반 가상 머신(KVM)용 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
2. Storage Gateway 구성 기본 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 관리를 선택합니다.
3. 시스템 시간 관리 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 보기 및 동기화를 선택합니다.

   게이트웨이 로컬 콘솔에서 현재 시스템 시간을 표시하고 NTP 서버에서 보고한 시간과 비교한 다음 두 시간 간의 정확한 편차를 초 단위로 보고합니다.
4. 시간 편차가 60초를 초과할 경우 **y**를 입력하여 시스템 시간을 NTP 시간과 동기화합니다. 그렇지 않은 경우 **n**을 입력합니다.

   시간 동기화에는 몇 분 정도 걸릴 수 있습니다.

VM 시간을 VMware 호스트 시간과 동기화

게이트웨이를 성공적으로 활성화하려면 VM 시간을 호스트 시간과 동기화해야 하고 호스트 시간을 올바르게 설정해야 합니다. 이 섹션에서는 먼저 VM의 시간을 호스트 시간과 동기화합니다. 그 다음 호스트 시간을 확인하고, 필요한 경우 호스트 시간을 설정하고 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성합니다.

> **Important**
>
> VM 시간을 호스트 시간과 동기화하려면 게이트웨이를 성공적으로 활성화해야 합니다.

VM 시간을 호스트 시간과 동기화하려면

1. VM 시간을 구성합니다.

   a. vSphere 클라이언트에서 애플리케이션 창의 왼쪽 패널에 있는 게이트웨이 VM의 이름을 마우스 오른쪽 버튼으로 클릭하여 VM의 컨텍스트 메뉴를 연 다음 설정 편집을 선택합니다.

그러면 Virtual Machine Properties(가상 머신 속성) 대화 상자가 열립니다.

b. 옵션 탭을 선택하고 옵션 목록에서 VMware 도구를 선택합니다.

c. 가상 머신 속성 대화 상자의 오른쪽에 있는 고급 섹션에서 호스트와 게스트 시간 동기화 옵션을 확인한 후 확인을 선택합니다.

그러면 VM이 자체 시간을 호스트와 동기화합니다.

2. 호스트 시간을 구성합니다.

호스트 클럭의 시간이 올바르게 설정되어 있는지 확인하는 것이 중요합니다. 호스트 클럭을 구성하지 않았다면 다음 절차에 따라 설정하고 NTP 서버와 동기화합니다.

a. VMware vSphere 클라이언트의 왼쪽 패널에서 vSphere 호스트 노드를 선택한 후 구성 탭을 선택합니다.

b. 소프트웨어 패널에서 시간 구성을 선택한 다음 속성 링크를 선택합니다.

그러면 Time Configuration(시간 구성) 대화 상자가 나타납니다.

c. 날짜 및 시간에서 vSphere 호스트의 날짜와 시간을 설정합니다.

d. 호스트가 자체 시간을 자동으로 NTP 서버와 동기화하도록 구성합니다.

i. 시간 구성 대화 상자에서 옵션을 선택한 다음 NTP 데몬(ntpd) 옵션 대화 상자의 왼쪽 패널에서 NTP 설정을 선택합니다.

ii. 추가를 선택하여 새 NTP 서버를 추가합니다.

iii. NTP 서버 추가 대화 상자에서 NTP 서버의 IP 주소 또는 전체 주소 도메인 이름을 입력한 후 확인을 선택합니다.

`pool.ntp.org`를 도메인 이름으로 사용할 수 있습니다.

iv. NTP 대몬(ntpd) 옵션 대화 상자의 왼쪽 패널에서 일반을 선택합니다.

v. 서비스 명령에서 시작을 선택하여 서비스를 시작합니다.

이 NTP 서버 참조를 변경하거나 나중에 하나를 더 추가하는 경우, 새 서버를 사용하려면 해당 서비스를 다시 시작해야 한다는 점에 유의하십시오.

e. 확인을 선택하여 NTP 데몬(ntpd) 옵션 대화 상자를 닫습니다.

f. 확인을 선택하여 Time Configuration(시간 구성) 대화 상자를 닫습니다.

게이트웨이용 네트워크 어댑터 구성

Storage Gateway는 기본적으로 단일 VMXNET3(10GbE) 네트워크 어댑터를 사용하지만 여러 IP 주소에서 액세스할 수 있도록 둘 이상의 네트워크 어댑터를 사용하도록 게이트웨이를 구성할 수 있습니다. 이 방법은 다음과 같은 상황에서 사용할 수 있습니다.

- 처리량 극대화 - 네트워크 어댑터에 병목 현상이 발생하는 경우, 게이트웨이에 대한 처리량을 극대화하고자 할 수 있습니다.
- 애플리케이션 분리 – 애플리케이션이 게이트웨이의 볼륨에 데이터를 기록하는 방식을 분리해야 할 수 있습니다. 예를 들어 중요 스토리지 애플리케이션이 게이트웨이에 정의한 특정 어댑터 한 개를 배타적으로 사용하도록 선택할 수 있습니다.
- 네트워크 제약 – 애플리케이션 환경에 따라 파일 공유 및 여기에 연결되는 이니시에이터를 고립된 네트워크에 유지해야 할 수도 있습니다. 게이트웨이가 AWS과 통신하는 네트워크가 아닌 다른 네트워크입니다.

일반적인 다중 어댑터 사용 사례에서는 하나의 어댑터가 게이트웨이가 통신하는 경로 AWS (즉, 기본 게이트웨이)로 구성됩니다. 이 어댑터 한 개를 제외하고 이니시에이터는 자신이 접속하는 파일 공유를 포함하는 어댑터와 동일한 서브넷에 있어야 합니다. 그렇지 않은 경우, 원하는 대상과의 통신이 불가능할 수 있습니다. 대상이 와의 통신에 사용되는 것과 동일한 어댑터에 구성된 AWS경우 해당 대상에 대한 파일 공유 트래픽과 AWS 트래픽은 동일한 어댑터를 통해 흐릅니다.

Storage Gateway 콘솔에 연결할 어댑터 하나를 구성한 후, 두 번째 어댑터를 추가하는 경우가 있을 수 있습니다. 이 경우, Storage Gateway가 두 번째 어댑터가 선호하는 경로로 사용되도록 자동으로 라우팅 테이블을 구성합니다. 다중 어댑터의 구성 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

주제

- VMware ESXi 호스트에서 여러 개의 NIC에 게이트웨이 구성
- Microsoft Hyper-V 호스트에서 여러 개의 NIC에 게이트웨이 구성

VMware ESXi 호스트에서 여러 개의 NIC에 게이트웨이 구성

다음 절차에서는 게이트웨이 VM에 이미 하나의 네트워크 어댑터가 정의되어 있다고 가정하고 VMware ESXi에 어댑터를 추가하는 방법에 대해 설명합니다.

VMware ESXi 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이를 종료합니다.

2. VMware vSphere 클라이언트에서 해당되는 게이트웨이 VM을 선택합니다.

   이 절차를 위해 VM을 켠 상태로 유지할 수 있습니다.

3. 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.

4. 가상 컴퓨터 속성 대화 상자의 하드웨어 탭에서 추가를 선택하여 디바이스를 추가합니다.

5. Add Hardware 마법사의 안내에 따라 네트워크 어댑터를 추가합니다.

   a. 디바이스 유형 창에서 Ethernet Adapter(이더넷 어댑터)를 선택하여 어댑터를 추가한 후 다음을 선택합니다.

   b. 네트워크 유형 창에서 전원이 켜질 때 연결이 유형으로 선택되어 있는지 확인한 후 다음을 선택합니다.

      Storage Gateway에서는 VMXNET3 네트워크 어댑터를 사용하는 것이 좋습니다. 어댑터 목록에 표시될 어댑터 유형에 대한 자세한 내용은 ESXi 및 vCenter Server 설명서의 네트워크 어댑터 유형 섹션을 참조하세요.

   c. Ready to Complete(완료 준비) 창에서 해당 정보를 검토한 후 Finish(완료)를 선택합니다.

6. VM의 요약 탭을 선택하고 IP 주소 상자 옆에 있는 모두 보기를 선택합니다. 게이트웨이에 액세스할 때 사용할 수 있는 모든 IP 주소가 가상 머신 IP 주소 창에 표시됩니다. 게이트웨이에 두 번째 IP 주소가 표시되는지 확인합니다.

   > **Note**
   >
   > 어댑터 변경 사항이 적용되고 VM 요약 정보가 새로 고침되려면 약간의 시간이 걸릴 수 있습니다.

7. Storage Gateway 콘솔에서 게이트웨이의 전원을 켭니다.

8. Storage Gateway의 탐색 창에서 게이트웨이를 선택한 후 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

   > **Note**
   >
   > Storage Gateway 콘솔의 파일 공유 정보 페이지에 제공되는 마운팅 명령 예제에는 항상 파일 공유의 연결된 게이트웨이에 가장 최근에 추가된 네트워크 어댑터의 IP 주소가 포함됩니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행 섹션을 참조하세요.

Microsoft Hyper-V 호스트에서 여러 개의 NIC에 게이트웨이 구성

다음 절차에서는 게이트웨이 VM에 네트워크 어댑터 한 개가 이미 정의되어 있고 이제 두 번째 어댑터를 추가한다고 가정합니다. 이번 절차에서는 Microsoft Hyper-V 호스트에 어댑터를 추가하는 방법에 대해서 살펴보겠습니다.

Microsoft Hyper-V 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. Storage Gateway 콘솔에서 게이트웨이를 끕니다.
2. Microsoft Hyper-V Manager의 가상 머신 패널에서 해당 게이트웨이 가상 머신을 선택합니다.
3. 게이트웨이 VM이 아직 꺼져 있지 않은 경우 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 끄기를 선택합니다.
4. 게이트웨이 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 설정을 선택합니다.
5. 설정 대화 상자의 하드웨어에서 하드웨어 추가를 선택합니다.
6. 설정 대화 상자 오른쪽에 있는 하드웨어 추가 패널에서 네트워크 어댑터를 선택한 다음 추가를 선택하여 디바이스를 추가합니다.
7. 네트워크 어댑터를 구성한 후 적용을 선택하여 설정을 적용합니다.
8. 설정 대화 상자의 하드웨어에서 새 네트워크 어댑터가 하드웨어 목록에 추가되었는지 확인한 다음 확인을 선택합니다.
9. Storage Gateway 콘솔을 사용하여 게이트웨이를 켭니다.
10. Storage Gateway 콘솔의 탐색 패널에서 게이트웨이를 선택한 다음 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

> **Note**
>
> Storage Gateway 콘솔의 파일 공유 정보 페이지에 제공되는 마운팅 명령 예제에는 항상 파일 공유의 연결된 게이트웨이에 가장 최근에 추가된 네트워크 어댑터의 IP 주소가 포함됩니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행 섹션을 참조하세요.

Storage Gateway와 함께 VMware vSphere High Availability 사용

Storage Gateway는 VMware vSphere High Availability(VMware HA)와 통합된 애플리케이션 수준의 상태 확인 세트를 통해 VMware에서 고가용성을 제공합니다. 이러한 접근 방식을 통해 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 또한 연결 시간 초과, 파일 공유 또는 볼륨 사용 불가와 같은 소프트웨어 오류로부터 보호할 수 있습니다.

이 통합을 통해 온프레미스의 VMware 환경 또는의 VMware Cloud에 배포된 게이트웨이는 대부분의 서비스 중단으로부터 AWS 자동으로 복구됩니다. 일반적으로 데이터 손실 없이 60초 이내에 이 작업을 수행합니다.

> **Note**
>
> VMware HA 클러스터에 Storage Gateway를 배포하는 경우 다음 작업을 수행하는 것이 좋습니다.
>
> - Storage Gateway VM이 포함된 VMware ESX .ova 다운로드 가능 패키지를 클러스터의 호스트 한 곳에만 배포합니다.
> - .ova 패키지를 배포할 때 호스트 한 곳에 대해 로컬이 아닌 데이터 스토어를 선택합니다. 그 대신에 클러스터의 모든 호스트에 액세스할 수 있는 데이터 스토어를 사용합니다. 호스트에 대해 로컬인 데이터 스토어를 선택하였는데 호스트에 장애가 생긴 경우에는 데이터 원본이 클러스터 내 기타 호스트에 액세스할 수 없고 다른 호스트에 대한 장애 조치가 성공하지 못할 수 있습니다.
> - 클러스터링의 경우, .ova 패키지를 클러스터에 배포한다면 프롬프트 메시지에 따라 호스트를 선택합니다. 또는 클러스터의 호스트에 직접 배포할 수도 있습니다.

다음 주제에서는 VMware HA 클러스터에 Storage Gateway를 배포하는 방법에 대해 설명합니다.

주제

vSphere VMware HA 클러스터 구성

먼저 아직 VMware 클러스터를 생성하지 않은 경우 클러스터를 생성합니다. VMware 클러스터를 생성하는 방법에 대한 자세한 내용은 VMware 설명서의 vSphere HA 클러스터 생성을 참조하세요.

그런 다음 VMware 클러스터가 Storage Gateway와 함께 작동하도록 구성합니다.

VMware 클러스터를 구성하려면

1. VMware vSphere의 Edit Cluster Settings(클러스터 설정 편집) 페이지에서 VM 모니터링이 VM 및 애플리케이션 모니터링용으로 구성되어 있는지 확인합니다. 이렇게 하려면 각 옵션에 대해 다음 값을 설정합니다.

   - Host Failure Response(호스트 실패 응답): Restart VMs(VM 다시 시작)
   - Response for Host Isolation(호스트 격리에 대한 응답): Shut down and restart VMs(VM 종료 및 다시 시작)
   - Datastore with PDL(PDL 포함 데이터 스토어): 비활성화
   - Datastore with APD(APD 포함 데이터 스토어): 비활성화
   - VM Monitoring(VM 모니터링): VM and Application Monitoring(VM 및 애플리케이션 모니터링)
2. 다음 값을 조정하여 클러스터의 민감도를 미세 조정합니다.

   - 실패 간격 - 이 간격이 지나면 VM 하트비트가 수신되지 않을 경우 VM이 다시 시작됩니다.
   - 최소 가동 시간 - VM이 VM 도구의 하트비트 모니터링을 시작한 후 클러스터가 이 시간 동안 기다립니다.
   - VM당 최대 재설정 - 클러스터가 최대 재설정 시간 내에서 VM을 이 최대 횟수만큼 다시 시작합니다.
   - 최대 재설정 시간 - VM 재설정당 최대 재설정 횟수를 계산할 시간입니다.

   설정할 값을 잘 모르는 경우 다음 설정 예를 사용합니다.

   - Failure interval(실패 간격): **30**초
   - Minimum uptime(최소 가동 시간): **120**초
   - Maximum per-VM resets(VM당 최대 재설정): **3**
   - Maximum resets time window(최대 재설정 시간): **1**시간

클러스터에서 다른 VM이 실행 중인 경우 이러한 값을 해당 VM에 맞게 설정할 수 있습니다. .ova에서 VM을 배포할 때까지는 이 작업을 수행할 수 없습니다. 이러한 값 설정에 대한 자세한 내용은 (선택 사항) 클러스터의 다른 VM에 대한 재정의 옵션 추가 섹션을 참조하세요.

게이트웨이 유형 설정

다음 절차에 따라 게이트웨이를 설정합니다.

게이트웨이 유형에 대한 .ova 이미지를 다운로드하려면

- 다음 중 하나에서 해당 게이트웨이 유형에 대한 .ova 이미지를 다운로드합니다.
  - File Gateway - Amazon S3 File Gateway 생성 및 활성화

게이트웨이 배포

구성된 클러스터에서 .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다. 지침은 VMware vSphere 온라인 설명서의 OVF 또는 OVA 템플릿 배포를 참조하세요.

게이트웨이 .ova 이미지를 배포하려면

1. .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.
2. 루트 디스크 및 캐시에 대해 선택한 데이터 스토어를 클러스터의 모든 호스트에서 사용할 수 있는지 확인합니다.

(선택 사항) 클러스터의 다른 VM에 대한 재정의 옵션 추가

클러스터에서 다른 VM이 실행 중인 경우 각 VM에 맞게 클러스터 값을 설정할 수 있습니다. 지침은 VMware vSphere 온라인 설명서에서 Customize an Individual Virtual Machine을 참조하세요.

클러스터의 다른 VM에 대한 재정의 옵션을 추가하려면

1. VMware vSphere의 요약 페이지에서 클러스터를 선택하여 클러스터 페이지를 연 다음 구성을 선택합니다.
2. 구성 탭을 선택한 다음 VM Overrides(VM 재정의)를 선택합니다.
3. 새 VM 재정의 옵션을 추가하여 각 값을 변경합니다.

   vSphere HA - VM 모니터링에서 각 옵션에 대해 다음 값을 설정합니다.

   - VM 모니터링: 재정의 사용 - VM 및 애플리케이션 모니터링

- VM 모니터링 민감도: 재정의 사용 - VM 및 애플리케이션 모니터링
- VM 모니터링: 사용자 지정
- 실패 간격: **30**초
- 최소 가동 시간: **120**초
- Maximum per-VM resets(VM당 최대 재설정): **5**
- 최대 재설정 기간: **1**시간 이내

게이트웨이 활성화

VMware 환경에 .ova를 배포한 후 Storage Gateway 콘솔을 사용하여 게이트웨이를 활성화합니다. 지침은 설정 검토 및 Amazon S3 File Gateway 활성화를 참조하세요.

VMware 고가용성 구성 테스트

게이트웨이를 활성화한 후 구성을 테스트합니다.

VMware HA 구성을 테스트하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 VMware HA에 대해 테스트할 게이트웨이를 선택합니다.
3. 작업에서 Verify VMware HA(VMware HA 확인)를 선택합니다.
4. Verify VMware High Availability Configuration(VMware 고가용성 구성 확인) 상자가 나타나면 확인을 선택합니다.

   > **Note**
   >
   > VMware HA 구성을 테스트하면 게이트웨이 VM이 재부팅되고 게이트웨이 연결이 중단됩니다. 테스트를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

   테스트가 성공하면 콘솔에 있는 게이트웨이의 세부 정보 탭에 확인됨 상태가 나타납니다.
5. 종료를 선택합니다.

Amazon CloudWatch 로그 그룹에서 VMware HA 이벤트에 대한 정보를 찾을 수 있습니다. 자세한 내용은 CloudWatch 로그 그룹을 사용하여 S3 File Gateway 가져오기 단원을 참조하십시오.

게이트웨이 활성화 키 받기

게이트웨이 활성화 키를 받으려면 게이트웨이 가상 머신(VM)으로 웹 요청을 보내야 합니다. VM은 활성화 키를 포함한 리디렉션을 반환하며, 이 키는 `ActivateGateway` API 작업의 파라미터 중 하나로 전달되어 게이트웨이 구성을 지정합니다. 자세한 내용은 Storage Gateway API 참조에서 ActivateGateway를 참조하세요.

> **Note**
>
> 게이트웨이 활성화 키는 사용하지 않으면 30분 후에 만료됩니다.

게이트웨이 VM에 대한 요청에는 활성화가 발생하는 AWS 리전이 포함됩니다. 응답에 리디렉션으로 반환되는 URL에는 `activationkey`라는 쿼리 문자열 파라미터가 포함되어 있습니다. 이 쿼리 문자열 파라미터는 정품 인증 키입니다. 쿼리 문자열의 형식은 다음과 같습니다. `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. 이 쿼리의 출력은 활성화 리전과 활성화 키를 모두 반환합니다.

이 URL에는 VPC 엔드포인트 유형을 사용하여 연결하는 게이트웨이의 VPC 엔드포인트 ID인 `vpcEndpoint`도 포함되어 있습니다.

> **Note**
>
> The AWS Storage Gateway 하드웨어 어플라이언스, VM 이미지 템플릿 및 Amazon EC2 Amazon Machine Image(AMI)는이 페이지에 설명된 웹 요청을 수신하고 응답하는 데 필요한 HTTP 서비스로 미리 구성되어 있습니다. 게이트웨이에 추가 서비스를 설치할 필요는 없으며 권장하지도 않습니다.

주제

- Linux(curl)
- Linux(bash/zsh)
- Microsoft Windows PowerShell
- 로컬 콘솔 사용

Linux(curl)

다음 예에서는 Linux(curl)를 사용하여 활성화 키를 받는 방법을 보여줍니다.

> **Note**
>
> 강조 표시된 변수를 게이트웨이의 실제 값으로 바꿉니다. 가능한 값은 다음과 같습니다.
>
> - *gateway_ip_address* - 게이트웨이의 IPv4 주소입니다(예: 172.31.29.201).
> - *gateway_type* - 활성화하려는 게이트웨이의 유형입니다(예: STORED, CACHED, VTL, FILE_S3, FILE_FSX_SMB).
> - *region_code* - 게이트웨이를 활성화할 리전입니다.AWS 일반 참조 안내서에서 리전 엔드포인트를 참조하세요. 이 파라미터가 지정되지 않았거나 제공된 값의 철자가 잘못되었거나 유효한 리전과 일치하지 않는 경우 명령은 기본적으로 us-east-1 리전으로 설정됩니다.
> - *vpc_endpoint* - 게이트웨이의 VPC 엔드포인트 이름입니다(예: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com).

퍼블릭 엔드포인트

퍼블릭 엔드포인트에 대한 활성화 키를 가져오려면 다음 명령 중 하나를 사용합니다.

표준 엔드포인트

표준 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

듀얼 스택 엔드포인트

듀얼 스택 엔드포인트의 활성화 키를 받으려면:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS 엔드포인트

FIPS 엔드포인트의 활성화 키를 받으려면:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC 엔드포인트

VPC 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux(bash/zsh)

다음 예제는 Linux(bash/zsh)를 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi
```

```
  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

다음 예제는 Microsoft Windows PowerShell을 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

로컬 콘솔 사용

다음 예에서는 로컬 콘솔을 사용하여 활성화 키를 생성하고 표시하는 방법을 보여줍니다.

Amazon Linux 2(AL2) 기반 게이트웨이

AL2 기반 게이트웨이의 표준 또는 FIPS 엔드포인트를 선택할 수 있습니다.

> **Note**
>
> FIPS 엔드포인트를 전혀 사용할 수 없습니다 AWS 리전. 자세한 내용은 서비스별 FIPS 엔드포인트를 참조하세요.

로컬 콘솔에서 AL2 기반 게이트웨이 활성화 키를 가져오려면

1. 로컬 콘솔에 admin으로 로그인합니다.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 0을 선택하여 정품 인증 키 가져오기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 게이트웨이를 활성화하려는 AWS 리전을 입력합니다.
5. 네트워크 유형으로 퍼블릭의 경우 1 또는 VPC의 경우 2를 입력합니다.
6. 엔드포인트 유형으로 표준의 경우 1, FIPS(Federal Information Processing Standard)의 경우 2를 입력합니다.

Amazon Linux 2023(AL2023) 기반 게이트웨이

AL2023 기반 게이트웨이의 경우 다음 엔드포인트를 사용할 수 있습니다.

- 표준 엔드포인트(IPv4만 지원)
- FIPS 엔드포인트(IPv4만 지원)
- 듀얼 스택 엔드포인트(IPv4 및 IPv6 지원)
- 듀얼 스택 FIPS 엔드포인트(IPv4 및 IPv6 지원)

자세한 내용은 엔드포인트 유형 단원을 참조하십시오.

로컬 콘솔에서 AL2023 기반 게이트웨이 활성화 키를 가져오려면

1. 로컬 콘솔에 로그인합니다. Amazon EC2 인스턴스에 연결하는 경우, admin으로 로그인합니다.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 0을 선택하여 정품 인증 키 가져오기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 게이트웨이를 활성화하려는 AWS 리전을 입력합니다.

5. 네트워크 유형으로 퍼블릭의 경우 1, VPC 엔드포인트의 경우 2를 입력합니다.
6. 엔드포인트 유형 선택, FIPS 활성화?에 Y를 입력하여 FIPS를 활성화하거나 N을 입력하여 비 FIPS 엔드포인트를 사용합니다.
7. 엔드포인트 유형에 표준 엔드포인트의 경우 1 또는 듀얼 스택 엔드포인트의 경우 2를 입력합니다.
    - 듀얼 스택 엔드포인트의 경우 IP 버전 선택 또는 종료:에 IPv4의 경우 1 또는 IPv6의 경우 2를 입력합니다.

Amazon S3 File Gateway의 파일 속성 지원

Amazon S3 File Gateway는 기본적으로 DOS 또는 Windows 파일 속성을 지원합니다. S3 File Gateway를 사용하면 파일 데이터와 메타데이터를 보존하고 항목을 Amazon S3에 배치할 때 보관된 것으로 표시하는 등 설정을 업데이트할 수 있습니다. DOS 및 Windows 파일 속성에 대한 자세한 내용은 Windows 앱 개발 설명서 웹 사이트의 파일 속성 상수 문서를 참조하세요.

S3 File Gateway는 다음 속성을 지원합니다.

- ReadOnly - S3 File Gateway는 ReadOnly 속성이 설정된 파일의 변경을 방지합니다.
- 아카이브 - S3 File Gateway는 게이트웨이에 파일이 처음 추가될 때 이 속성을 설정합니다.

> **Note**
>
> 백업 애플리케이션은 일반적으로 아카이브 비트가 설정된 파일을 백업한 다음 백업 성공 후 비트를 지웁니다.

- 숨김 - SMB(Server Message Block) 클라이언트는 이 비트 세트를 사용하는 파일을 숨깁니다.
- 시스템 - 이 속성은 설정한 후에도 유지됩니다.

속성이 설정된 S3 File Gateway에 파일을 복사하면 파일의 DOS 또는 Windows 속성이 S3 File Gateway 및 Amazon S3에 보존됩니다. 게이트웨이의 파일에 대해 이러한 속성을 업데이트할 수 있으며, 이러한 업데이트는 Amazon S3의 객체에도 적용됩니다. 게이트웨이에서 파일이 제거되면 게이트웨이는 요청 시 Amazon S3에서 파일, 메타데이터 및 영구 속성을 가져옵니다.

> **Note**
>
> DOS 속성은 SMB 공유 및 Windows 액세스 제어 목록에 의해 액세스가 제어되는 경우에만 지원됩니다.

Storage Gateway Direct Connect 에서 사용

Direct Connect 는 내부 네트워크를 Amazon Web Services 클라우드에 연결합니다. Storage Gateway와 Direct Connect 함께를 사용하면 처리량이 많은 워크로드 요구 사항에 맞는 연결을 생성하여 온프레미스 게이트웨이와 간에 전용 네트워크 연결을 제공할 수 있습니다 AWS.

Storage Gateway는 퍼블릭 엔드포인트를 사용합니다. Direct Connect 연결이 설정되면 퍼블릭 가상 인터페이스를 생성하여 트래픽을 Storage Gateway 엔드포인트로 라우팅할 수 있습니다. 퍼블릭 가상 인터페이스는 네트워크 경로에서 인터넷 서비스 제공업체를 우회합니다. Storage Gateway 서비스 퍼블릭 엔드포인트는 위치와 동일한 AWS 리전 Direct Connect 에 있거나 다른 AWS 리전에 있을 수 있습니다.

다음 그림은가 Storage Gateway에서 Direct Connect 작동하는 방식의 예를 보여줍니다.
AWS 직접 연결을 사용하여 클라우드에 연결된 Storage Gateway를 보여주는 네트워크 아키텍처입니다.

다음 절차에서는 생성된 게이트웨이가 제대로 작동 중이라고 가정합니다.

Storage Gateway Direct Connect 와 함께를 사용하려면

1. 온프레미스 데이터 센터와 Storage Gateway 엔드포인트 간에 AWS Direct Connect 연결을 생성하고 설정합니다. 연결 생성 방법에 대한 자세한 내용은Direct Connect 사용 설명서에서 Direct Connect시작하기를 참조하세요.
2. 온프레미스 Storage Gateway 어플라이언스를 Direct Connect 라우터에 연결합니다.
3. 퍼블릭 가상 인터페이스를 생성하고 이에 따라 온프레미스 라우터를 구성합니다. 자세한 내용은 Direct Connect 사용 설명서에서 가상 인터페이스 생성을 참조하세요.

자세한 내용은 Direct Connect 사용 설명서의 란 무엇입니까 Direct Connect?를 Direct Connect참조하세요.

Active Directory 서비스 계정 권한 요구 사항

Microsoft Active Directory를 사용하여의 파일 공유 대한 사용자 인증 액세스를 제공하려는 경우 Active Directory 서비스 계정이 있고 서비스 계정에 컴퓨터를 도메인에 조인할 수 있는 위임된 권한이 있는지 AWS Storage Gateway확인해야 합니다. 서비스 계정은 특정 작업을 수행할 권한이 위임된 Active Directory 사용자 계정입니다. Storage Gateway를 Active Directory 도메인에 조인할 때 이 계정의 사용자 이름과 암호 자격 증명을 제공합니다.

게이트웨이에 조인하려는 OU에서 Active Directory 서비스 계정에 다음 권한을 위임해야 합니다.

- 컴퓨터 객체를 생성하고 삭제할 수 있는 기능
- 암호 재설정 기능
- 권한 수정 기능
- 계정의 데이터 읽기 및 쓰기 제한 기능
- 계정 제한 사항을 읽고 쓸 수 있는 검증된 기능
- 검증된 서비스 위탁자 이름 쓰기 기능
- 검증된 DNS 호스트 이름 쓰기 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.

게이트웨이 어플라이언스의 IP 주소 가져오기

호스트를 선택하고 게이트웨이 VM을 배포한 후 게이트웨이를 연결하고 활성화합니다. 이렇게 하려면 게이트웨이 VM의 IP 주소가 필요합니다. IP 주소는 게이트웨이의 로컬 콘솔에서 얻을 수 있습니다. 로컬 콘솔에 로그인하여 콘솔 페이지의 상단에서 IP 주소를 얻습니다.

온프레미스에 배포된 게이트웨이의 경우, 하이퍼바이저에서 IP 주소를 얻을 수도 있습니다. Amazon EC2 게이트웨이의 경우, Amazon EC2 Management Console에서 Amazon EC2 인스턴스의 IP 주소를 얻을 수도 있습니다. 게이트웨이의 IP 주소를 얻는 방법은 다음 중 하나를 참조하세요.

- VMware 호스트: VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스
- HyperV 호스트: Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스
- Linux 커널 기반 가상 머신(KVM) 호스트: Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스
- EC2 호스트: Amazon EC2 호스트에서 IP 주소 얻기

IP 주소를 찾았으면 적어 둡니다. 그런 다음 Storage Gateway 콘솔로 돌아가서 콘솔에 IP 주소를 입력합니다.

Amazon EC2 호스트에서 IP 주소 얻기

게이트웨이가 배포된 Amazon EC2 인스턴스의 IP 주소를 얻으려면 EC2 인스턴스의 로컬 콘솔에 로그인합니다. 그런 다음 콘솔 페이지 상단에서 IP 주소를 얻습니다. 지침은 다음을 참조하세요.

Amazon EC2 Management Console에서도 IP 주소를 얻을 수 있습니다. 활성화에는 퍼블릭 IP 주소를 사용하는 것이 좋습니다. 퍼블릭 IP 주소를 얻으려면 절차 1을 사용합니다. 그 대신 탄력적 IP 주소를 사용하려면 절차 2를 사용합니다.

절차 1: 퍼블릭 IP 주소를 사용하여 게이트웨이에 연결하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 퍼블릭 IP 주소를 적어 둡니다. 이 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 IP 주소를 입력합니다.

활성화에 탄력적 IP 주소를 사용하려면 다음 절차를 사용합니다.

절차 2: 탄력적 IP 주소를 사용하여 게이트웨이에 연결하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 탄력적 IP 값을 적어 둡니다. 이 탄력적 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 탄력적 IP 주소를 입력합니다.

IPv6 지원

IPv6 지원은 게이트웨이 어플라이언스 버전 2.x 이상에서만 사용할 수 있습니다. 게이트웨이 어플라이언스 버전 1.x는 버전 2.x로 업데이트할 수 없습니다. IPv6 지원을 받으려면 게이트웨이 어플라이언스 버전 1.x를 마이그레이션하거나 교체해야 합니다.

IPv6에는 다음과 같은 듀얼 스택 엔드포인트가 필요합니다.

```
storagegateway.region.api.aws:443
activation-storagegateway.region.api.aws:443
```

```
controlplane-storagegateway.region.api.aws:443
proxy-storagegateway.region.api.aws:443
dataplane-storagegateway.region.api.aws:443
s3.dualstack.region.amazonaws.com
```

Storage Gateway 리소스 및 리소스 ID 이해

Storage Gateway에서 기본 리소스는 게이트웨이이지만 다른 리소스 유형은 파일 공유입니다. 파일 공유는 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

다음 표에 나와 있는 것처럼 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

리소스 유형	ARN 형식
Gateway ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
파일 공유 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:share/`*`share-id`*

리소스 ID 작업

리소스를 생성할 때 Storage Gateway에서는 리소스에 고유 리소스 ID를 할당합니다. 이 리소스 ID는 리소스 ARN의 일부입니다. 리소스 ID는 리소스 식별자 다음에 하이픈, 그리고 문자 및 숫자의 고유 조합(8자리)이 오는 형식을 취합니다. 예를 들어 게이트웨이 ID가 `sgw-12A3456B`와 같은 형식이라면 여기에서 `sgw`는 게이트웨이의 리소스 식별자입니다.

Storage Gateway 리소스 ID는 대문자입니다. 그러나 이 리소스 ID를 Amazon EC2 API에서 사용하는 경우, Amazon EC2에서는 리소스 ID가 소문자일 것으로 예상합니다. EC2 API에서 사용할 수 있도록 리소스 ID를 소문자로 변경해야 합니다. 예를 들어 Storage Gateway에서 볼륨의 ID는 `vol-1122AABB`일 수 있습니다. 이 ID를 EC2 API에서 사용하는 경우, `vol-1122aabb`로 변경해야 합니다. 그렇게 하지 않으면 EC2 API가 예상 대로 작동하지 않을 수 있습니다.

> **Important**
>
> 게이트웨이 볼륨에서 생성한 Storage Gateway 볼륨 및 Amazon EBS 스냅샷의 ID는 더 긴 형식으로 변경될 예정입니다. 2016년 12월부터 모든 신규 볼륨 및 스냅샷은 문자 17개로 구성된

문자열로 생성됩니다. 2016년 4월부터 이와 같이 더 긴 ID를 사용할 수 있으므로 이러한 새 형식으로 시스템을 테스트할 수 있습니다. 자세한 내용은 더 긴 EC2 및 EBS 리소스 ID 섹션을 참조하세요.
더 긴 볼륨 ID 형식을 지닌 볼륨 ARN의 예: `arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG`.
더 긴 ID 형식을 지닌 스냅샷 ID의 예: `snap-78e226633445566ee`
자세한 내용은 Announcement: Heads-up – Longer Storage Gateway volume and snapshot IDs coming in 2016을 참조하세요.

Storage Gateway 리소스에 태그를 지정

Storage Gateway에서 태그를 사용하여 리소스를 관리할 수 있습니다. 태그를 사용하면 메타데이터를 리소스에 추가하고 리소스를 분류하여 관리하기가 편해집니다. 각 태그는 사용자가 정의하는 키-값 페어로 구성됩니다. 게이트웨이, 볼륨 및 가상 테이프에 태그를 추가할 수 있습니다. 추가하는 태그에 따라 이 리소스를 검색하고 필터링할 수 있습니다.

예를 들어 태그를 사용하여 조직 내 각 부서에서 사용하는 Storage Gateway 리소스를 식별할 수 있습니다. `key=department` 및 `value=accounting`과 같이 회계 부서에서 사용하는 게이트웨이 및 볼륨에 태그를 지정할 수 있습니다. 그 다음에 이 태그로 필터링하여 회계 부서에서 사용하는 모든 게이트웨이 및 볼륨을 식별하고 이 정보를 통해 비용을 파악할 수 있습니다. 자세한 내용은 비용 할당 태그 사용 및 Tag Editor 작업 섹션을 참조하세요.

태그를 지정한 가상 테이프를 아카이브하는 경우, 테이프는 아카이브에서 자체 태그를 유지합니다. 이와 마찬가지로 아카이브에서 다른 게이트웨이로 테이프를 가져오는 경우, 태그는 새 게이트웨이에 유지됩니다.

File Gateway에 대해 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있습니다. 이를 위한 자세한 방법은 태그를 사용하여 게이트웨이 및 리소스에 대한 액세스 제어 섹션을 참조하세요.

태그에는 의미가 없으며 문자열로 해석됩니다.

태그에 적용되는 제한은 다음과 같습니다.

- 태그 키와 값은 대/소문자를 구분합니다.
- 각 리소스의 최대 태그 수는 50입니다.
- 태그 키는 `aws:`로 시작할 수 없습니다. 이 접두사는 AWS 용으로 예약되어 있습니다.
- 키 속성에 유효한 문자는 UTF-8 문자 및 숫자, 공백, 특수 문자(+ - = . _ : / @)입니다.

태그 작업

Storage Gateway 콘솔, Storage Gateway API 또는 Storage Gateway 명령줄 인터페이스(CLI)를 사용하여 태그 관련 작업을 수행할 수 있습니다. 다음 절차에서는 콘솔에서 태그를 추가, 편집, 삭제하는 방법을 안내합니다.

태그를 추가하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 태그를 지정하려는 리소스를 선택합니다.

   예를 들어 게이트웨이에 태그를 지정하려면 게이트웨이를 선택한 후 게이트웨이 목록에서 태그를 지정할 게이트웨이를 선택합니다.
3. 태그를 선택한 후 태그 추가/편집을 선택합니다.
4. 태그 추가/편집 대화 상자에서 태그 생성을 선택합니다.
5. 키에 키를 입력하고 값에 값을 입력합니다. 예를 들어 키로는 **`Department`**를, 값으로는 **`Accounting`**을 입력할 수 있습니다.

   > **Note**
   >
   > 값 상자를 공백으로 둘 수도 있습니다.
6. 태그 생성을 선택하여 태그를 추가합니다. 리소스 한 개에 태그를 여러 개 추가할 수 있습니다.
7. 태그 추가를 완료했으면 저장을 선택합니다.

태그를 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 편집하려는 태그가 있는 리소스를 선택합니다.
3. 태그를 선택하여 태그 추가/편집 대화 상자를 엽니다.
4. 편집하고자 하는 태그 옆의 연필 아이콘을 선택하여 태그를 편집합니다.
5. 태그 편집을 완료했으면 저장을 선택합니다.

태그를 삭제하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.

2. 삭제하려는 태그가 있는 리소스를 선택합니다.
3. 태그를 선택한 후 태그 추가/편집을 선택하여 태그 추가/편집 대화 상자를 엽니다.
4. 삭제하고자 하는 태그 옆의 X 아이콘을 선택한 후 저장을 선택합니다.

에 대한 오픈 소스 구성 요소 작업 AWS Storage Gateway

이 섹션에서는 AWS Storage Gateway 기능을 제공하기 위해 사용하는 타사 도구 및 라이센스에 대해 설명합니다.

주제

Storage Gateway용 오픈 소스 구성 요소

Volume Gateway, Tape Gateway 및 Amazon S3 File Gateway에 대한 기능을 제공하기 위해 여러 타사 도구 및 라이선스가 사용됩니다.

다음 링크를 사용하여 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드를 다운로드합니다 AWS Storage Gateway .

- VMware ESXi에 배포된 Storage Gateway 어플라이언스의 경우: sources.tar
- Microsoft Hyper-V에 배포된 Storage Gateway 어플라이언스의 경우 sources_hyperv.tar
- Linux 커널 기반 가상 머신(KVM)에 배포된 Storage Gateway 어플라이언스의 경우 sources_KVM.tar

이 제품은 OpenSSL 도구 키트(http://www.openssl.org/)에서 사용하기 위해 OpenSSL 프로젝트가 개발한 소프트웨어를 포함합니다. 모든 종속 서드 파티 도구와 관련된 라이선스는 서드 파티 라이선스를 참조하세요.

Amazon S3 File Gateway의 오픈 소스 구성 요소

Amazon S3 File Gateway(S3 File Gateway) 기능을 제공하기 위해 여러 타사 도구 및 라이선스가 사용됩니다.

다음 링크를 사용하여 S3 File Gateway 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드를 다운로드합니다.

- Amazon S3 File Gateway의 경우: sgw-file-s3-open-source.tgz

이 제품은 OpenSSL 도구 키트(http://www.openssl.org/)에서 사용하기 위해 OpenSSL 프로젝트가 개발한 소프트웨어를 포함합니다. 모든 종속 서드 파티 도구와 관련된 라이선스는 서드 파티 라이선스를 참조하세요.

Amazon S3 File Gateway에 대한 제한 및 할당량

파일 공유 할당량

다음 표에는 파일 공유 할당량이 나와 있습니다.

설명	Limit
게이트웨이당 최대 파일 공유 개수 **Note** 각 파일 공유는 하나의 S3 버킷에만 연결할 수 있지만 여러 파일 공유는 동일한 버킷에 연결할 수 있습니다. 둘 이상의 파일 공유를 동일한 버킷에 연결하는 경우 읽기/쓰기 충돌을 방지하기 위해 중복되지 않는 고유한 접두사 이름을 사용하도록 각 파일 공유를 구성해야 합니다. 게이트웨이에서 관리하는 파일 공유 수는 게이트웨이의 성능에 영향을 미칠 수 있습니다. 자세한 내용은 여러 파일 공유가 있는 게이트웨이에 대한 성능 지침을 참조하세요.	50
게이트웨이가 메타데이터를 동시에 캐시할 수 있는 최대 파일 수	게이트웨이 용량: Small - 5M 파일 Medium - 10M 파일 Large - 20M 파일

설명	Limit
Note S3 File Gateway는 Amazon S3에서 지원하므로 게이트웨이를 사용하여 저장하거나 액세스할 수 있는 파일 수에는 최대 폴더 크기나 제한이 없습니다. 각 게이트웨이에는 메타데이터를 동시에 캐시할 수 있는 파일 수를 결정하는 구성 가능한 제한이 있습니다. UpdateGatewayInformation API 작업을 사용하여 GatewayCapacity를 `Small`, `Medium` 또는 `Large`로 설정할 수 있습니다. 이 설정은 게이트웨이 성능 및 하드웨어 권장 사항에 영향을 줍니다. 자세한 내용은 여러 파일 공유가 있는 게이트웨이에 대한 성능 지침을 참조하세요.	
개별 파일의 최대 크기	5TiB
Note 크기 제한보다 큰 파일을 하나씩 작성하려고 하면 처음 5TiB만 업로드됩니다. 크기 제한보다 큰 파일을 한 번에 쓰려고 하면 Windows 클라이언트에서는 파일이 생성되지 않고 Linux 클라이언트에서는 크기가 0인 파일이 생성됩니다.	

설명	Limit
최대 경로 길이 **Note** 클라이언트는 이 길이를 초과하는 경로를 생성할 수 없으며 따라서 이렇게 하면 오류가 발생합니다. 이 한도는 File Gateway, NFS, SMB가 지원하는 모든 프로토콜에 적용됩니다. 바이트 단위의 경로 길이는 UTF-8 인코딩의 문자 비트 값에서 계산됩니다.	1024B
최대 파일 이름 길이 **Note** File Gateway는 이 길이를 초과하는 파일 이름을 지원하지 않습니다. 바이트 단위의 파일 이름 길이는 UTF-8 인코딩의 문자 비트 값에서 계산됩니다.	255바이트

게이트웨이에 권장되는 로컬 디스크 크기

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)
S3 File Gateway	150GiB	64TiB

Note

캐시에 대해 하나 이상의 로컬 드라이브를 최대 용량까지 구성할 수 있습니다.

기존 게이트웨이에 캐시를 추가할 때 호스트(하이퍼바이저 또는 Amazon EC2 인스턴스)에 새 디스크를 생성하는 것이 중요합니다. 기존 디스크가 이전에 캐시로 할당되었던 경우, 디스크 크기를 변경하지 마십시오.

스토리지 클래스 사용

Amazon S3 File Gateway는 Amazon S3 Standard, Amazon S3 Standard-Infrequent Access, Amazon S3 One Zone-Infrequent Access, Amazon S3 Intelligent-Tiering 및 Amazon Glacier 스토리지 클래스를 지원합니다. 스토리지 클래스에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 Amazon S3 스토리지 클래스를 참조하세요.

Note

S3 File Gateway는 현재 Amazon S3 Glacier Instant Retrieval 스토리지 클래스를 지원하지 않습니다.

주제

File Gateway에 스토리지 클래스 사용

파일 공유를 생성하거나 업데이트하는 경우 객체에 대한 스토리지 클래스를 선택할 수 있습니다. Amazon S3 Standard 스토리지 클래스(Standard 스토리지 클래스) 또는 S3 Standard-IA, S3 One Zone-IA, S3 Intelligent-Tiering 스토리지 클래스 중 하나를 선택할 수 있습니다. 수명 주기 정책을 사용하여 이러한 스토리지 클래스 중 하나에 저장된 객체를 GLACIER로 전환할 수 있습니다.

Amazon S3 스토리지 클래스	고려 사항
표준	표준을 선택하면 지리적으로 분리된 여러 가용 영역에 자주 액세스하는 객체 파일을 중복 저장합니다. 이것이 기본 스토리지 클래스입니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

Amazon S3 스토리지 클래스	고려 사항
S3 Intelligent-Tiering	지능형 계층화를 선택하면 가장 비용 효과적인 스토리지 액세스 계층으로 데이터를 자동으로 이동하여 스토리지 비용을 최적화합니다. 128KB 미만의 객체는 Intelligent-Tiering 스토리지 클래스의 자동 계층화 대상이 아닙니다. 이러한 객체는 액세스 계층 요금이 자주 부과되며 자동 계층화된 객체에 대해서는 모니터링 요금이 부과되지 않습니다. S3 Intelligent-Tiering은 이제 Archive Access 계층 및 Deep Archive Access 계층을 지원합니다. S3 Intelligent-Tiering은 90일 동안 액세스하지 않은 객체를 Archive Access 계층으로 자동 이동하고, 액세스하지 않은지 180일 후에는 Deep Archive Access 계층으로 자동 이동합니다. 아카이브 액세스 계층 중 하나의 객체가 복원될 때마다 객체는 몇 시간 내에 Frequent Access 계층으로 이동하여 검색할 준비가 됩니다. 이렇게 하면 객체가 두 아카이브 계층 중 하나에만 있는 경우 파일 공유를 통해 파일에 액세스하려는 사용자 또는 애플리케이션에 시간 초과 오류가 발생합니다. 애플리케이션이 File Gateway에서 제공하는 파일 공유를 통해 파일에 액세스하는 경우 S3 Intelligent-Tiering에서 아카이브 계층을 사용하지 마세요. File Gateway에서 관리하는 파일에 대해 메타데이터를 업데이트하는 파일 작업(예: 소유자, 타임스탬프, 권한 및 ACL)을 수행하면 기존 객체가 삭제되고 이 Amazon S3 스토리지 클래스에 새 버전의 객체가 생성됩니다. 프로덕션에서 이 스토리지 클래스를 사용하기 전에 파일 작업이 객체 생성에 미치는 영향을 검증합니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

Amazon S3 스토리지 클래스	고려 사항
S3 Standard-IA	Standard-IA를 선택하면 지리적으로 분리된 여러 가용 영역에 자주 액세스하지 않는 객체 데이터를 중복 저장합니다. Standard-IA 스토리지 클래스에 저장된 객체는 30일 이내에 스토리지 클래스 간에 덮어쓰거나, 삭제하거나, 요청하거나, 검색하거나, 전환할 경우 추가 요금이 부과될 수 있습니다. 최소 스토리지 기간은 30일입니다. 30일 이전에 삭제된 객체에는 남은 일수 동안의 스토리지 요금과 동일한 비례 할당 요금이 발생합니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 128KB 미만의 객체에는 128KB가 청구되며 조기 삭제 요금이 적용됩니다. File Gateway에서 관리하는 파일에 대해 메타데이터를 업데이트하는 파일 작업(예: 소유자, 타임스탬프, 권한 및 ACL)을 수행하면 기존 객체가 삭제되고 이 Amazon S3 스토리지 클래스에 새 버전의 객체가 생성됩니다. 조기 삭제 요금이 적용되므로 프로덕션 환경에서 이 스토리지 클래스를 사용하기 전에 파일 작업이 객체 생성에 미치는 영향을 검증해야 합니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

Amazon S3 스토리지 클래스	고려 사항
S3 One Zone-IA	One Zone-IA를 선택하면 단일 가용 영역에 자주 액세스하지 않는 객체를 저장합니다. One Zone-IA 스토리지 클래스에 저장된 객체는 30일 이내에 스토리지 클래스 간에 덮어쓰거나, 삭제하거나, 요청하거나, 검색하거나, 전환할 경우 추가 요금이 부과될 수 있습니다. 최소 스토리지 기간은 30일이며, 30일 이전에 삭제된 객체에는 나머지 일 동안의 스토리지 요금과 동일한 비례 할당 요금이 발생합니다. 이 객체가 얼마나 자주 변경되는지, 이 객체를 얼마나 오래 유지할 계획인지, 이 객체에 얼마나 자주 액세스해야 하는지 고려합니다. 128KB 미만의 객체에는 128KB가 청구되며 조기 삭제 요금이 적용됩니다. File Gateway에서 관리하는 파일에 대해 메타데이터를 업데이트하는 파일 작업(예: 소유자, 타임스탬프, 권한 및 ACL)을 수행하면 기존 객체가 삭제되고 이 Amazon S3 스토리지 클래스에 새 버전의 객체가 생성됩니다. 조기 삭제 요금이 적용되므로 프로덕션 환경에서 이 스토리지 클래스를 사용하기 전에 파일 작업이 객체 생성에 미치는 영향을 검증해야 합니다. 자세한 내용은 Amazon S3 요금을 참조하세요.

파일 공유에서 S3-Standard-IA, S3-One Zone-IA 또는 S3 Intelligent-Tiering 스토리지 클래스로 직접 객체를 쓸 수 있지만, 특히 보관 후 30일 내에 객체를 업데이트하거나 삭제할 것으로 예상되는 경우에는 파일 공유에서 직접 쓰는 대신 수명 주기 정책을 사용하여 객체를 전환하는 것이 좋습니다. 수명 주기 정책에 대한 자세한 내용은 객체 수명 주기 관리를 참조하세요.

File Gateway에 GLACIER 스토리지 클래스 사용

Amazon S3 수명 주기 정책을 통해 Amazon Glacier로 파일을 전환하는 경우 캐시를 통해 파일 공유 클라이언트에 파일이 표시되면 파일을 업데이트할 때 IO 오류가 표시됩니다. 이러한 IO 오류가 발생할 때

알림을 받고 알림을 사용하여 작업을 수행하도록 CloudWatch Events를 설정하는 것이 좋습니다. 예를 들어 보관된 객체를 Amazon S3로 복원하는 작업을 수행할 수 있습니다. 객체가 S3로 복원되면 파일 공유 클라이언트에서 파일 공유를 통해 이 객체를 액세스하고 업데이트할 수 있습니다.

아카이브된 객체를 복원하는 방법에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 아카이브된 객체 복원 섹션을 참조하세요.

> **Important**
>
> S3 File Gateway는 S3 Glacier Instant Retrieval 스토리지 클래스를 공식적으로 지원하지 않습니다. 수명 주기 정책 또는 직접 PUT 요청을 사용하여 S3 Glacier Instant Retrieval용 파일 공유 버킷의 객체를 지정할 수 있지만 S3 File Gateway는 해당 스토리지 클래스에 있는 파일을 인식할 수 없으며 다른 객체와 마찬가지로 파일 작업을 수행합니다. S3 Glacier Instant Retrieval은 다른 Amazon S3 스토리지 클래스보다 액세스 비용이 높기 때문에 신중하게 관리하지 않으면 바이러스 스캔, `rsync` 및 이름 변경과 같은 대량 파일 작업으로 인해 대규모 Amazon S3 요금이 발생할 수 있습니다. 따라서 S3 File Gateway와 함께 S3 Glacier Instant Retrieval을 사용하지 않는 것이 좋습니다.

Kubernetes 컨테이너 스토리지 인터페이스 드라이버 사용

Kubernetes는 컨테이너화된 애플리케이션의 배포, 규모 조정 및 관리 자동화를 위한 오픈 소스 시스템입니다. Kubernetes 환경에서 컨테이너는 VM과 유사하지만 컨테이너에는 애플리케이션 간에 운영 체제(OS)를 공유하기 위한 완화된 격리 속성이 있습니다. 따라서 컨테이너는 VM보다 더 가벼운 것으로 간주됩니다. VM과 마찬가지로 컨테이너에는 자체 파일 시스템, 할당된 CPU, 메모리, 프로세스 공간 등의 공유가 있습니다. 기본 인프라와 분리되므로 클라우드 및 OS 배포판에서 이식할 수 있습니다. Kubernetes 클러스터가 있는 경우 기존 Amazon S3 File Gateway를 스토리지에 사용할 수 있도록 클러스터의 인스턴스에 Kubernetes 컨테이너 스토리지 인터페이스(CSI) 드라이버를 설치하고 구성할 수 있습니다.

사용하려는 파일 공유 유형에 대한 CSI 드라이버를 설치한 후 하나 이상의 스토리지 객체를 생성해야 합니다. 포드가 스토리지를 요청할 때 Kubernetes가 사용할 프로비저닝 유형에 따라 Kubernetes 컴퓨팅 포드를 파일 공유에 연결하려면 단일 Kubernetes `StorageClass` 객체 또는 `PersistentVolume` 객체와 `PersistentVolumeClaim` 객체를 모두 생성해야 합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/의 Kubernetes 온라인 설명서를 참조하세요.

주제

- SMB CSI 드라이버 작업

- NFS CSI 드라이버 작업

SMB CSI 드라이버 작업

이 섹션의 절차에 따라 Kubernetes 클러스터의 스토리지에 Amazon S3 File Gateway에서 SMB 파일 공유를 사용하는 데 필요한 CSI 드라이버를 설치, 구성 또는 삭제합니다. 자세한 내용은 https://github.com/kubernetes-csi/csi-driver-smb/blob/master/docs/install-csi-driver-master.md의 GitHub에서 오픈 소스 SMB CSI 드라이버 설명서를 참조하세요.

> **Note**
>
> `PersistentVolume` 객체 또는 `StorageClass` 객체를 생성할 때 `ReclaimPolicy` 파라미터를 지정하여 객체가 삭제될 때 외부 스토리지에 어떤 일이 발생하는지 결정할 수 있습니다. SMB CSI 드라이버는 `Retain` 및 `Recycle` 옵션을 지원하지만 현재 `Delete` 옵션은 지원하지 않습니다.

드라이버 설치

Kubernetes SMB CSI 드라이버를 설치하려면:

1. Kubernetes 클러스터의 `kubectl`에 대한 액세스 권한이 있는 명령줄 터미널에서 다음 명령을 실행합니다.

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/install-driver.sh | bash -s master --

2. 이전 명령이 완료될 때까지 기다린 후 다음 명령을 사용하여 CSI 드라이버 포드가 실행 중인지 확인합니다.

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-controller

   kubectl -n kube-system get pod -o wide --watch -l app=csi-smb-node

   출력은 다음과 비슷하게 보여야 합니다.

```
NAME                                  READY   STATUS    RESTARTS   AGE     IP
            NODE
```

```
csi-smb-controller-56bfddd689-dh5tk       4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-smb-controller-56bfddd689-8pgr4       4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-cvgbs                        3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-smb-node-dr4s4                        3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

SMB StorageClass 객체 생성

Kubernetes 클러스터에 대한 새 SMB StorageClass 객체를 생성하려면:

1. 다음 예제와 유사한 콘텐츠가 포함된 `storageclass.yaml`이라는 이름의 구성 파일을 생성합니다. 표시된 *`ExampleValues`*를 사용자의 배포 관련 정보로 대체합니다.

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: ExampleStorageClassName
provisioner: smb.csi.k8s.io
parameters:
    source: "//gateway-dns-name-or-ip-address/example-share-name"
    # if csi.storage.k8s.io/provisioner-secret is provided, will create a sub
 directory
    # with PV name under source
    csi.storage.k8s.io/provisioner-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/provisioner-secret-namespace: "examplenamespace"
    csi.storage.k8s.io/node-stage-secret-name: "examplesmbcreds"
    csi.storage.k8s.io/node-stage-secret-namespace: "examplenamespace"
volumeBindingMode: Immediate
reclaimPolicy: Retain
mountOptions:
    - dir_mode=0777
    - file_mode=0777
    - uid=1001
    - gid=1001
```

2. `kubectl` 및 `storageclass.yaml`에 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

kubectl apply -f storageclass.yaml

> **Note**
>
> 이전 단계의 `.yaml` 구성 텍스트를 대부분의 타사 Kubernetes 관리 및 컨테이너화 플랫폼에 제공하여 StorageClass를 생성할 수도 있습니다.

3. 생성한 새 StorageClass를 사용하도록 Kubernetes 클러스터의 포드를 구성합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/의 Kubernetes 온라인 설명서를 참조하세요.

SMB PersistentVolume 및 PersistentVolumeClaim 객체 생성

새 SMB PersistentVolume 및 PersistentVolumeClaim 객체를 생성하려면:

1. 2개의 구성 파일을 생성합니다. 이름이 `persistentvolume.yaml`인 1개와 이름이 `persistentvolumeclaim.yaml`인 1개입니다.
2. `persistentvolume.yaml`의 경우 다음 예와 유사한 콘텐츠를 추가합니다. 표시된 *`ExampleValues`*를 사용자의 배포 관련 정보로 대체합니다.

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-smb-example-name
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    capacity:
        storage: 100Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - dir_mode=0777
        - file_mode=0777
        - vers=3.0
    csi:
        driver: smb.csi.k8s.io
        readOnly: false
```

```
        volumeHandle: examplehandle  # make sure it's a unique id in the cluster
        volumeAttributes:
            source: "//gateway-dns-name-or-ip-address/example-share-name"
        nodeStageSecretRef:
            name: example-smbcreds
            namespace: smb-example-namespace
```

3. persistentvolumeclaim.yaml의 경우 다음 예와 유사한 콘텐츠를 추가합니다. 표시된 *ExampleValues*를 사용자의 배포 관련 정보로 대체합니다.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-smb-static
    namespace: smb-example-namespace # PersistentVolume and PersistentVolumeClaim
 must use the same namespace parameter
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
        volumeName: pv-smb-example-name # make sure specfied volumeName matches the
 name of the PersistentVolume you created
        storageClassName: ""
```

4. kubectl 및 생성한 두 .yaml 파일에 모두 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

> **Note**
>
> 이전 단계의 .yaml 구성 텍스트를 대부분의 타사 Kubernetes 관리 및 컨테이너화 플랫폼에 제공하여 PersistentVolume 및 PersistentVolumeClaim 객체를 생성할 수도 있습니다.

5. 생성한 새 PersistentVolumeClaim을 사용하도록 Kubernetes 클러스터의 포드를 구성합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/의 Kubernetes 온라인 설명서를 참조하세요.

드라이버 제거

Kubernetes SMB CSI 드라이버를 제거하려면:

- Kubernetes 클러스터의 `kubectl`에 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-smb/master/deploy/uninstall-driver.sh | bash -s --

NFS CSI 드라이버 작업

이 섹션의 절차에 따라 Kubernetes 클러스터의 스토리지에 Amazon S3 File Gateway에서 NFS 파일 공유를 사용하는 데 필요한 CSI 드라이버를 설치, 구성 또는 삭제합니다. 자세한 내용은 https://github.com/kubernetes-csi/csi-driver-nfs/blob/master/docs/install-csi-driver-master.md의 GitHub에서 오픈 소스 NFS CSI 드라이버 설명서를 참조하세요.

드라이버 설치

Kubernetes NFS CSI 드라이버를 설치하려면:

1. Kubernetes 클러스터의 `kubectl`에 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

   curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/install-driver.sh | bash -s master --

2. 이전 명령이 완료될 때까지 기다린 후 다음 명령을 사용하여 CSI 드라이버 포드가 실행 중인지 확인합니다.

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-controller

   kubectl -n kube-system get pod -o wide -l app=csi-nfs-node

   출력은 다음과 비슷하게 보여야 합니다.

```
NAME                                        READY   STATUS    RESTARTS   AGE     IP
            NODE
csi-nfs-controller-56bfddd689-dh5tk         4/4     Running   0          35s
 10.240.0.19    k8s-agentpool-22533604-0
csi-nfs-controller-56bfddd689-8pgr4         4/4     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-cvgbs                          3/3     Running   0          35s
 10.240.0.35    k8s-agentpool-22533604-1
csi-nfs-node-dr4s4                          3/3     Running   0          35s
 10.240.0.4     k8s-agentpool-22533604-0
```

NFS StorageClass 객체 생성

Kubernetes 클러스터에 대한 NFS StorageClass 객체를 생성하려면:

1. 다음 예제와 유사한 콘텐츠가 포함된 `storageclass.yaml`이라는 이름의 구성 파일을 생성합니다. 표시된 *ExampleValues*를 사용자의 배포 관련 정보로 대체합니다.

```
---
apiVersion: storage.k8s.io/v1
kind: StorageClass
metadata:
    name: example-nfs-classname
    namespace: example-namespace
provisioner: nfs.csi.k8s.io
parameters:
    server: gateway-dns-name-or-ip-address
    share: /example-share-name
reclaimPolicy: Retain
volumeBindingMode: Immediate
mountOptions:
    - hard
    - nfsvers=4.1
```

2. `kubectl` 및 `storageclass.yaml`에 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

   kubectl apply -f storageclass.yaml

> **Note**
>
> 이전 단계의 `.yaml` 구성 텍스트를 대부분의 타사 Kubernetes 관리 및 컨테이너화 플랫폼에 제공하여 StorageClass를 생성할 수도 있습니다.

3. 생성한 새 StorageClass 객체를 사용하도록 Kubernetes 클러스터의 포드를 구성합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/의 Kubernetes 온라인 설명서를 참조하세요.

NFS PersistentVolume 및 PersistentVolumeClaim 객체 생성

새 NFS PersistentVolume 및 PersistentVolumeClaim 객체를 생성하려면:

1. `persistentvolume.yaml` 및 `persistentvolumeclaim.yaml`이라는 이름의 구성 파일 2개를 생성합니다.
2. `persistentvolume.yaml`의 경우 다음 예와 유사한 콘텐츠를 추가합니다. 표시된 *`ExampleValues`*를 사용자의 배포 관련 정보로 대체합니다.

```
---
apiVersion: v1
kind: PersistentVolume
metadata:
    name: pv-nfs-examplename
spec:
    capacity:
        storage: 10Gi
    accessModes:
        - ReadWriteMany
    persistentVolumeReclaimPolicy: Retain
    mountOptions:
        - hard
        - nolock
        - nfsvers=4.1
    csi:
        driver: nfs.csi.k8s.io
        readOnly: false
        volumeHandle: unique-volumeid-example # make sure it's a unique id in the
 cluster
        volumeAttributes:
            server: gateway-dns-name-or-ip-address
```

```
            share: /example-share-name
```

3. persistentvolumeclaim.yaml의 경우 다음 예와 유사한 콘텐츠를 추가합니다. 표시된 *ExampleValues*를 사용자의 배포 관련 정보로 대체합니다.

```
---
kind: PersistentVolumeClaim
apiVersion: v1
metadata:
    name: examplename-pvc-nfs-static
spec:
    accessModes:
        - ReadWriteMany
    resources:
        requests:
            storage: 10Gi
    volumeName: pv-nfs-examplename # make sure specfied volumeName matches the name
 of the PersistentVolume you created
    storageClassName: ""
```

4. kubectl 및 두 .yaml 파일에 모두 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

   kubectl apply -f persistentvolume.yaml

   kubectl apply -f persistentvolumeclaim.yaml

   > **Note**
   >
   > 이전 단계의 .yaml 구성 텍스트를 대부분의 타사 Kubernetes 관리 및 컨테이너화 플랫폼에 제공하여 PersistentVolume 및 PersistentVolumeClaim 객체를 생성할 수도 있습니다.

5. 생성한 새 PersistentVolumeClaim 객체를 사용하도록 Kubernetes 클러스터의 포드를 구성합니다. 자세한 내용은 https://kubernetes.io/docs/concepts/storage/의 Kubernetes 온라인 설명서를 참조하세요.

드라이버 제거

Kubernetes NFS CSI 드라이버를 제거하려면:

- Kubernetes 클러스터의 `kubectl`에 액세스할 수 있는 명령줄 터미널에서 다음 명령을 실행합니다.

  curl -skSL https://raw.githubusercontent.com/kubernetes-csi/csi-driver-nfs/master/deploy/uninstall-driver.sh | bash -s master --

AWS Storage Gateway Terraform 모듈

HashiCorpTerraform은 HashiCorp 구성 언어(HCL)를 사용하여 개발된 오픈 소스 코드형 인프라(IaC) 엔진입니다. Terraform은 백엔드 인프라용 Amazon S3 File Gateway와 함께 사용할 수 있는 일관된 명령줄 인터페이스(CLI) 워크플로우를 제공하며, 이를 통해 수백 개의 클라우드 서비스를 관리하고 클라우드 API를 선언적 구성 파일에 체계화할 수 있습니다.

Terraform을 사용하여 Amazon S3 File Gateway를 온프레미스 가상 인프라에 가상 머신(VM)으로 안전하게 배포할 수 있습니다. Terraform은 온프레미스 가상 인프라를 자동화합니다. 온프레미스 VMware 가상 환경 내에서 Terraform을 사용하여 Amazon S3 File Gateway를 빠르게 배포하는 방법에 대한 자세한 내용은 HashiCorp의 Terraform을 사용하여 VMware에서 Amazon S3 File Gateway 배포 자동화를 참조하세요.

> **Note**
>
> 선호하는 하이퍼바이저 플랫폼에 대한 최신 버전의 AWS Storage Gateway 머신 이미지를 가져오도록 Terraform을 구성해야 할 수 있습니다. Storage Gateway 머신 이미지는 다음 명명 규칙을 사용합니다. 이미지 이름에 추가되는 버전 번호는 각 버전 릴리스에 따라 변경됩니다.
> `aws-storage-gateway-FILE_S3-1.25.0`

이 자동화는 VM 환경에 게이트웨이와 파일 공유를 완전히 배포하는 데 필요한 모든 리소스와 종속성을 Amazon S3 File Gateway에 프로비저닝하는 데 사용할 수 있는 사용자 지정 가능한 Terraform 모듈을 제공합니다. Terraform 모듈은 게이트웨이 VM을 프로비저닝하고, 게이트웨이를 활성화하고, 캐시 디스크를 구성하고, 게이트웨이를 도메인에 조인하고, Amazon S3 버킷을 생성하고, 파일 공유를 생성하고, 버킷에 매핑합니다. 온프레미스에서 Amazon S3 File Gateway를 실행하는 데 필요한 리소스를 생성하는 Terraform 코드가 포함된 리포지토리의 전체 예는 GitHub의 Terraform Storage Gateway 모듈 소스 코드를 참조하세요.

> **Note**
>
> Terraform용 Amazon S3 File Gateway 모듈은 커뮤니티에서 지원하는 작업입니다. AWS 서비스의 일부가 아닙니다. 최선의 지원은 AWS 스토리지 커뮤니티에서 제공합니다.

Storage Gateway용 API 참조

콘솔을 사용하는 것 외에도 AWS Storage Gateway API를 사용하여 게이트웨이를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 이 섹션에서는 AWS Storage Gateway 작업, 인증을 위한 요청 서명 및 오류 처리에 대해 설명합니다. Storage Gateway에 사용할 수 있는 리전 및 엔드포인트에 대한 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

> **Note**
>
> Storage Gateway를 사용하여 애플리케이션을 개발할 때 AWS SDKs를 사용할 수도 있습니다. Java, .NET, PHP용 AWS SDK는 기본 Storage Gateway API를 포함하고 있어 프로그래밍 작업을 간소화합니다. SDK 라이브러리 다운로드에 대한 정보는 샘플 코드 라이브러리 섹션을 참조하세요.

주제

AWS Storage Gateway 필수 요청 헤더

이 섹션에서는 AWS Storage Gateway에 대한 모든 POST 요청과 함께 전송해야 하는 필수 헤더에 대해 설명합니다. 호출하려는 작업을 포함하는 요청에 대한 핵심 정보, 요청 날짜 및 요청 전송자의 권한을 부여함을 나타내는 정보를 식별할 HTTP 헤더를 포함해야 합니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음은 ActivateGateway 작업에서 사용하는 헤더의 예입니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

다음은 POST 요청에 포함해야 하는 헤더입니다 AWS Storage Gateway. 아래에 표시된 "x-amz"로 시작하는 헤더는 AWS특정 헤더입니다. 나머지 헤더는 HTTP 트랜잭션에 사용되는 공통 헤더입니다.

헤더	설명
`Authorization`	권한 부여 헤더에는가 요청이 요청자에게 유효한 작업인지 AWS Storage Gateway 확인할 수 있도록 요청에 대한 몇 가지 정보가 포함되어 있습니다. 이 헤더의 형식은 다음과 같습니다(가독성을 높이기 위해 줄 바꿈 추가). `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 이전 구문에서는 YourAccessKey, 연도, 월, 일(yyyymmdd), 해당 리전 및 CalculatedSignature를 지정합니다. 권한 부여 헤더의 형식은 AWS V4 서명 프로세스의 요구 사항에 따라 결정됩니다. 서명 관련 세부 정보는 요청에 서명하기 섹션에 나와 있습니다.
`Content-Type`	를 모든 요청의 콘텐츠 유형`application/x-amz-json-1.1` 으로 사용합니다 AWS Storage Gateway. `Content-Type: application/x-amz-json-1.1`
`Host`	호스트 헤더를 사용하여 요청을 보내는 AWS Storage Gateway 엔드포인트를 지정합니다. 예를 들어, `storagegateway.us-east-2.amazonaws.com` 은 미국 동부(오하이오) 리전의 엔드포인트입니다. 사용

헤더	설명
	가능한 엔드포인트에 대한 자세한 내용은의 AWS Storage Gateway 엔드포인트 및 할당량을 AWS Storage Gateway참조하세요AWS 일반 참조. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	HTTP `Date` 헤더 또는 AWS `x-amz-date` 헤더에 타임스탬프를 제공해야 합니다. 일부 HTTP 클라이언트 라이브러리에서는 `Date` 헤더를 설정할 수 없습니다. `x-amz-date` 헤더가 있으면는 요청 인증 중에 `Date` 헤더를 AWS Storage Gateway 무시합니다. `x-amz-date` 형식은 YYYYMMDD'T'HHMMSS'Z' 형식의 ISO8601 기본이어야 합니다. `Date` 및 `x-amz-date` 헤더를 모두 사용하는 경우, Date 헤더의 형식이 ISO8601일 필요는 없습니다. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	이 헤더는 API의 버전과 요청 중인 작업을 지정합니다. 대상 헤더 값은 API 버전을 API 이름과 연결하여 구성하며 형식은 다음과 같습니다. `x-amz-target: StorageGateway_ APIversion .operationName` OperationName 값(예: "ActivateGateway")은 API 목록, Storage Gateway용 API 참조에서 찾을 수 있습니다.

요청에 서명하기

Storage Gateway에서는 요청에 서명하여 전송하는 모든 요청을 인증해야 합니다. 요청에 서명하려면 암호화 해시 함수를 이용해 디지털 서명을 계산해야 합니다. 암호화 해시는 입력을 근거로 하여 고유 해시 값을 반환하는 함수입니다. 해시 함수에 대한 입력에는 요청 텍스트와 시크릿 액세스 키가 포함됩니다. 해시 함수는 요청에 서명으로 포함하는 해시 값을 반환합니다. 서명은 요청에서 `Authorization` 헤더의 일부입니다.

Storage Gateway는 요청을 수신한 후, 사용자가 요청에 서명할 때와 동일한 해시 함수 및 입력을 사용하여 서명을 재계산합니다. 결과 서명이 요청 서명과 일치할 경우 Storage Gateway에서 요청을 처리합니다. 그렇지 않으면 요청이 거부됩니다.

Storage Gateway는 AWS Signature Version 4를 이용한 인증을 지원합니다. 서명을 계산하기 위한 프로세스는 다음 세 작업으로 나뉠 수 있습니다.

- 작업 1: 정식 요청 생성

  HTTP 요청을 정규 형식으로 재배열합니다. 정규 형식을 사용해야 하는 이유는 Storage Gateway에서 서명을 재계산하여 사용자가 보낸 서명과 비교할 때 동일한 정규 형식을 사용하기 때문입니다.
- 작업 2: 서명할 문자열 생성

  암호화 해시 함수에 대한 입력 값 중 하나로 사용할 문자열을 만듭니다. 서명할 문자열이라는 문자열은 해시 알고리즘의 이름, 요청 날짜, 자격 증명 범위 문자열, 이전 작업에서 정규화된 요청을 연결한 것입니다. 자격 증명 범위 문자열 자체는 날짜, 리전 및 서비스 정보를 연결한 것입니다.
- 작업 3: 서명 생성

  서명할 문자열과 파생된 키의 두 입력 문자열을 허용하는 암호화 해시 함수를 사용하여 요청에 대한 서명을 만듭니다. 파생된 키는 보안 액세스 키로 시작해 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드(HMAC)를 생성하는 방법으로 계산합니다.

서명 계산 예시

다음 예시에서는 ListGateways에 대해 서명을 생성하는 세부 과정을 안내합니다. 이 예시는 서명 계산 방법을 점검하기 위한 참조로 사용할 수 있습니다.

이 예시에서는 다음과 같이 가정합니다.

- 해당 요청의 타임스탬프는 "2012년 9월 10일 월요일 00:00:00시" GMT입니다.
- 엔드포인트는 미국 동부(오하이오) 리전입니다.

일반 요청 구문(JSON 본문 포함)은 다음과 같습니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
```

```
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

작업 1: 정식 요청 생성에 대해 계산한 요청의 정규 형식은 다음과 같습니다.

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

표준 요청의 마지막 줄은 요청 본문의 해시입니다. 또한 표준 요청에서 비어 있는 세 번째 줄에 주의해야 합니다. 비어 있는 이유는 이 API(또는 Storage Gateway API)에 대한 쿼리 파라미터가 없기 때문입니다.

작업 2: 서명할 문자열 생성의 경우 서명할 문자열은 다음과 같습니다.

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

서명할 문자열의 첫째 줄은 알고리즘, 둘째 줄은 타임스탬프, 셋째 줄은 자격 증명 범위, 마지막 줄은 작업 1 정규 요청의 해시입니다.

작업 3: 서명 생성을 위한 파생된 키는 다음과 같이 표시할 수 있습니다.

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

시크릿 액세스 키인 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY를 사용하는 경우, 계산된 서명은 다음과 같습니다.

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

마지막 단계는 Authorization 헤더를 생성하는 것입니다. 데모용 액세스 키 AKIAIOSFODNN7EXAMPLE의 경우 헤더는 다음과 같습니다(가독성을 높이기 위해 줄 바꿈을 추가함).

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

오류 응답

주제

이 섹션에서는 AWS Storage Gateway 오류에 대한 참조 정보를 제공합니다. 이 오류는 오류 예외 및 작업 오류 코드로 표시됩니다. 예를 들어 오류 예외 InvalidSignatureException은 요청 서명에 문제가 있는 경우 모든 API 응답이 반환합니다. 그러나 작업 오류 코드 ActivationKeyInvalid는 ActivateGateway API에 대해서만 반환됩니다.

오류 유형에 따라 Storage Gateway는 예외만 반환하거나 예외와 작업 오류 코드를 모두 반환할 수 있습니다. 오류 응답 예시는 오류 응답에 있습니다.

예외

다음 표에는 AWS Storage Gateway API 예외가 나열되어 있습니다. AWS Storage Gateway 작업이 오류 응답을 반환하면 응답 본문에 이러한 예외 중 하나가 포함됩니다. InternalServerError와 InvalidGatewayRequestException은 특정 작업 오류 코드를 부여하는 작업 오류 코드(작업 오류 코드) 메시지 코드 중 하나를 반환합니다.

예외	메시지	HTTP 상태 코드
IncompleteSignatureException	지정한 서명이 불완전합니다.	400 잘못된 요청
InternalFailure	알 수 없는 오류, 예외 또는 장애로 인해 요청 처리가 실패했습니다.	500 Internal Server Error
InternalServerError	작업 오류 코드 작업 오류 코드 메시지 중 하나입니다.	500 Internal Server Error
InvalidAction	요청된 동작 또는 작업이 유효하지 않습니다.	400 잘못된 요청
InvalidClientTokenId	제공된 X.509 인증서 또는 AWS 액세스 키 ID가 레코드에 존재하지 않습니다.	403 금지됨
InvalidGatewayRequestException	작업 오류 코드의 작업 오류 코드 메시지 중 하나입니다.	400 잘못된 요청
InvalidSignatureException	우리가 계산한 요청 서명이 사용자가 제공한 서명과 일치하지 않습니다. AWS 액세스 키 및 서명 방법을 확인합니다.	400 잘못된 요청
MissingAction	요청에서 작업 또는 작업 파라미터가 누락되었습니다.	400 잘못된 요청
MissingAuthenticationToken	요청에 유효한(등록된) AWS 액세스 키 ID 또는 X.509 인증서가 포함되어야 합니다.	403 금지됨
RequestExpired	요청이 만료 날짜 또는 요청 날짜(15분 패딩)를 지났거나 요청 날짜가 향후 15분 초과 후에 효력이 발생합니다.	400 잘못된 요청

예외	메시지	HTTP 상태 코드
SerializationException	직렬화 도중에 오류가 발생했습니다. JSON 페이로드의 형식이 올바른지 확인합니다.	400 잘못된 요청
ServiceUnavailable	서버의 일시적 장애로 인해 요청이 실패했습니다.	[503 Service Unavailable]
SubscriptionRequiredException	AWS 액세스 키 ID에는 서비스에 대한 구독이 필요합니다.	400 잘못된 요청
ThrottlingException	속도를 초과하였습니다.	400 잘못된 요청
TooManyRequests	요청이 너무 많음.	429 요청이 너무 많음
UnknownOperationException	알 수 없는 작업을 지정하였습니다. 유효한 작업은 Storage Gateway API 작업에 나열되어 있습니다.	400 잘못된 요청
UnrecognizedClientException	요청에 포함된 보안 토큰이 잘못되었습니다.	400 잘못된 요청
ValidationException	입력 파라미터의 값이 잘못되었거나 범위를 벗어났습니다.	400 잘못된 요청

작업 오류 코드

다음 표에는 AWS Storage Gateway 작업 오류 코드와 코드를 반환할 수 있는 APIs 간의 매핑이 나와 있습니다. 모든 작업 오류 코드는 예외에 설명된 두 가지 일반 예외(InternalServerError 및 InvalidGatewayRequestException) 중 하나와 함께 반환됩니다.

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
ActivationKeyExpired	지정한 정품 인증 키가 만료되었습니다.	ActivateGateway

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
ActivationKeyInvalid	지정한 정품 인증 키가 유효하지 않습니다.	ActivateGateway
ActivationKeyNotFound	지정한 정품 인증 키를 찾을 수 없습니다.	ActivateGateway
BandwidthThrottleScheduleNotFound	지정한 대역폭 스로틀링을 찾을 수 없습니다.	DeleteBandwidthRateLimit
CannotExportSnapshot	지정한 스냅샷을 내보낼 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	지정된 초기자를 찾을 수 없습니다.	DeleteChapCredentials
DiskAlreadyAllocated	지정한 디스크가 이미 할당되었습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	지정한 디스크가 존재하지 않습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	지정한 디스크가 기가바이트 정렬되어 있지 않습니다.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	지정한 디스크 크기가 최대 볼륨 크기보다 큽니다.	CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
DiskSizeLessThanVolumeSize	지정한 디스크 크기가 볼륨 크기보다 작습니다.	CreateStorediSCSIVolume
DuplicateCertificateInfo	지정한 인증서 정보가 중복되어 있습니다.	ActivateGateway
FileSystemAssociationEndpointConfigurationConflict	기존 파일 시스템 연결 엔드포인트 구성이 지정된 구성과 충돌합니다.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressAlreadyInUse	지정된 엔드포인트 IP 주소가 이미 사용 중입니다.	AssociateFileSystem
FileSystemAssociationEndpointIpAddressMissing	파일 시스템 연결 엔드포인트 IP 주소가 누락되었습니다.	AssociateFileSystem
FileSystemAssociationNotFound	지정된 파일 시스템 연결을 찾을 수 없습니다.	UpdateFileSystemAssociation DisassociateFileSystem DescribeFileSystemAssociations
FileSystemNotFound	지정된 파일 시스템을 찾을 수 없습니다.	AssociateFileSystem

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayInternalError	게이트웨이 내부 오류가 발생하였습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotConnected	지정한 게이트웨이가 연결되지 않았습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotFound	지정한 게이트웨이를 찾을 수 없습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayProxyNetworkConnectionBusy	지정한 게이트웨이 프록시 네트워크 연결이 사용 중입니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InternalError	내부 오류가 발생했습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InvalidParameters	지정한 요청에 잘못된 파라미터가 포함되어 있습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	로컬 스토리지 한도를 초과했습니다.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	지정한 LUN이 유효하지 않습니다.	CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
MaximumVolumeCount Exceeded	최대 볼륨 수를 초과하였습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurati onChanged	게이트웨이 네트워크 구성이 변경되었습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
NotSupported	지정한 작업을 지원하지 않습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	지정한 게이트웨이의 날짜가 만료되었습니다.	ActivateGateway
SnapshotInProgressException	지정한 스냅샷이 진행 중입니다.	DeleteVolume
SnapshotIdInvalid	지정한 스냅샷이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	스테이징 영역이 가득 찼습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
TargetAlreadyExists	지정한 대상이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	지정한 대상이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	지정한 대상을 찾을 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
UnsupportedOperationForGatewayType	지정한 작업이 게이트웨이 유형에 유효하지 않습니다.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	지정한 볼륨이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	지정한 볼륨이 유효하지 않습니다.	DeleteVolume
VolumeInUse	지정한 볼륨이 이미 사용 중입니다.	DeleteVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
VolumeNotFound	지정한 볼륨을 찾을 수 없습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	지정한 볼륨이 아직 준비되지 않았습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

오류 응답

오류가 있는 경우, 응답 헤더 정보에는 다음 내용이 포함됩니다.

- Content-Type: application/x-amz-json-1.1
- 적절한 4xx 또는 5xx HTTP 상태 코드

오류 응답의 본문에는 발생한 오류에 대한 정보가 포함됩니다. 다음 샘플 오류 응답은 모든 오류 응답에 공통된 응답 요소의 출력 구문을 나타냅니다.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

다음 표는 이전 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__타입

예외의 예외 중 하나.

유형: 문자열

오류

API별 오류의 세부 정보를 포함합니다. 일반적인 오류(즉 API에 고유한 오류가 아닌 경우)에서는 이 오류 정보가 표시되지 않습니다.

유형: 컬렉션

errorCode

작업 오류 코드 중 하나입니다 .

유형: 문자열

errorDetails

이 필드는 현재 API 버전에서는 사용되지 않습니다.

유형: 문자열

message

작업 오류 코드 메시지 중 하나입니다.

유형: 문자열

오류 응답 예시

DescribeStorediSCSIVolumes API를 사용할 경우 존재하지 않는 게이트웨이 ARN 요청 입력을 지정하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

Storage Gateway가 요청과 함께 전송된 서명과 일치하지 않는 서명을 계산할 경우 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway API 작업

Storage Gateway 작업 목록은AWS Storage Gateway API 참조에서 작업을 참조하세요.

Amazon S3 File Gateway 사용 설명서에 대한 문서 이력

다음 표에서는 2018년 4월 이후 이 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
IPv6 지원	IPv6 지원은 게이트웨이 어플라이언스 버전 2.x 이상에서 사용할 수 있습니다.	2025년 9월 10일
처리량 및 최적화 지침 추가	성능 및 최적화 장에는 이제 S3 File Gateway의 처리량을 극대화하고 SQL Server 데이터베이스 백업 사용 사례에 맞게 배포를 최적화하기 위한 권장 사항과 모범 사례가 포함되어 있습니다. 자세한 내용은 S3 File Gateway 처리량 최대화 및 SQL Server 데이터베이스 백업을 위한 S3 File Gateway 최적화를 참조하세요.	2025년 6월 13일
캐시 보고서 기능 추가	이제 S3 File Gateway는 현재 특정 파일 공유의 로컬 업로드 캐시에 있는 파일에 대한 메타데이터 보고서를 생성할 수 있습니다. 자세한 내용은 S3 File Gateway에 대한 캐시 보고서 생성, S3 File Gateway에 대한 캐시 보고서 보기 및 관리, S3 File Gateway 캐시 보고서에 제공된 정보 이해를 참조하세요.	2025년 3월 31일
AWS KMS 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)에 대한 지원 추가	이제 AWS KMS 키를 사용한 이중 계층 서버 측 암호화를 사용하여 S3 File Gateway	2024년 9월 13일

	가 Amazon S3에 업로드하는 파일을 암호화할 수 있습니다. DSSE-KMS에 대한 자세한 내용은 Amazon S3의 File Gateway에 저장된 객체 암호화를 참조하세요.	
유지 관리 업데이트 켜기 또는 끄기 옵션이 추가됨	Storage Gateway는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안을 해결하기 위한 수정 사항, 새로운 기능에 대한 액세스가 포함된 정기 유지 관리 업데이트를 받습니다. 이제 배포의 각 개별 게이트웨이에 대해 이러한 업데이트를 켜거나 끄도록 설정을 구성할 수 있습니다. 자세한 내용은 콘솔을 사용하여 게이트웨이 업데이트 관리 AWS Storage Gateway 콘솔을 .	2024년 6월 6일
새 SMB 보안 수준 추가	S3 File Gateway는 이제 SMB 클라이언트 연결에 256비트 AES 암호화를 적용하는 데 사용할 수 있는 추가 보안 수준을 지원합니다. 자세한 내용은 게이트웨이의 보안 수준 설정을 참조하세요.	2024년 5월 23일

S3 File Gateway에 대한 게이트웨이 어플라이언스 소프트웨어 버전 보고 및 릴리스 정보	추가된 릴리스 정보에서는 Amazon S3 File Gateway 어플라이언스의 각 버전에 포함된 새로운 기능과 업데이트된 기능, 개선 사항 및 수정 사항에 대해 설명합니다. Storage Gateway 콘솔에서 또는 AWS CLI를 사용하여 Storage Gateway의 소프트웨어 버전 번호를 확인할 수 있습니다. 자세한 내용은 릴리스 정보 - 게이트웨이 어플라이언스 소프트웨어를 참조하세요.	2023년 10월 5일
권장되는 CloudWatch 경보가 업데이트됨	이제 CloudWatch `HealthNotifications` 경보가 모든 게이트웨이 유형 및 호스트 플랫폼에 적용되며 권장됩니다. `HealthNotifications` 및 `AvailabilityNotifications` 에 대한 권장 구성 설정도 업데이트되었습니다. 자세한 내용은 CloudWatch 경보 이해를 참조하세요.	2023년 10월 2일
게이트웨이당 최대 파일 공유 증가	S3 File Gateway는 이제 게이트웨이당 최대 50개의 파일 공유를 지원하며 이전 한도인 10개에서 증가했습니다. 이렇게 하면 단일 게이트웨이에서 더 많은 파일 공유를 생성하여 관리해야 하는 게이트웨이 수를 줄일 수 있습니다. 자세한 내용은 파일 공유 할당량을 참조하세요.	2023년 1월 18일

DOS 속성에 대한 지원 추가	S3 File Gateway는 이제 Amazon S3에 저장된 파일에 대해 DOS 속성을 지원합니다. 이렇게 하면 파일이 Amazon S3에 업로드될 때 읽기 전용, 숨김, 시스템 및 아카이브와 같은 Windows 파일 속성을 보존할 수 있습니다. 자세한 내용은 Amazon S3 File Gateway의 파일 속성 지원을 참조하세요.	2023년 1월 18일
GatewayClockOutOfSync 문제 해결 팁 추가	문제 해결: 파일 게이트웨이 문제 섹션에는 이제 게이트웨이 시스템 클럭이 AWS Storage Gateway 서버 시간과 동기화되지 않은 경우 발생할 수 있는 문제를 진단하는 데 도움이 되는 문제 해결 지침이 포함되어 있습니다. 자세한 내용은 오류: GatewayClockOutOfSync를 참조하세요.	2022년 10월 19일
일정 기반 네트워크 대역폭 스로틀링 추가	S3 File Gateway는 이제 Amazon S3로의 데이터 업로드에 대한 일정 기반 네트워크 대역폭 스로틀링을 지원합니다. 이 기능을 사용하면 게이트웨이가 특정 기간 동안 사용하는 네트워크 대역폭의 양을 제한하여 피크 업무 시간 동안 네트워크 사용량을 관리할 수 있습니다. 자세한 내용은 S3 File Gateway의 대역폭 관리를 참조하세요.	2022년 1월 18일

게이트웨이 생성 절차가 업데이트됨	Storage Gateway 콘솔의 Storage Gateway 생성 절차가 업데이트되었습니다. 자세한 내용은 Amazon S3 File Gateway 생성 및 활성화를 참조하세요.	2021년 10월 12일
SMB 파일 공유에서 강제 종료 파일 지원	이제 로컬 그룹 설정을 사용하여 게이트웨이 관리자 권한을 할당할 수 있습니다. 게이트웨이 관리자는 공유 폴더 Microsoft Management Console 스냅인을 사용하여 SMB 파일 공유에서 열려 있고 잠긴 파일을 강제로 닫을 수 있습니다. 자세한 정보는 게이트웨이용 로컬 그룹 구성을 참조하세요.	2021년 10월 12일
NFS 파일 공유에 대한 감사 로그 지원	이제 NFS 파일 공유를 구성하여 파일 공유 내의 파일 및 폴더에 대한 사용자 액세스에 대한 세부 정보를 제공하는 감사 로그를 생성할 수 있습니다. 이러한 로그를 사용하여 사용자 활동을 모니터링하고 부적절한 활동 패턴이 식별되면 조치를 취할 수 있습니다. 자세한 내용은 File Gateway 감사 로그 이해를 참조하세요.	2021년 10월 12일
액세스 포인트 별칭 지원	File Gateway 파일 공유는 이제 버킷 스타일 액세스 포인트 별칭을 사용하여 Amazon S3 스토리지에 연결할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2021년 10월 12일

VPC 엔드포인트 및 액세스 포인트 지원	File Gateway 파일 공유는 이제 AWS PrivateLink로 구동되는 VPC의 액세스 포인트 또는 인터페이스 엔드포인트를 통해 S3 버킷에 연결할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2021년 7월 7일
기회 잠금 지원	File Gateway 파일 공유는 이제 기회 잠금을 사용하여 파일 버퍼링 전략을 최적화할 수 있으므로 대부분의 경우 특히 Windows 컨텍스트 메뉴에서 성능이 향상됩니다. 자세한 내용은 SMB 파일 공유 생성을 참조하세요.	2021년 7월 7일
FedRAMP 규정 준수	Storage Gateway가 이제 FedRAMP를 준수합니다. 자세한 내용은 Storage Gateway에 대한 규정 준수 검증을 참조하세요.	2020년 11월 24일
File Gateway에 대한 파일 업로드 알림	File Gateway는 이제 파일 업로드 알림을 제공하여 File Gateway가 Amazon S3에 파일을 완전히 업로드한 시기를 알려줍니다. 자세한 내용은 파일 업로드 알림 받기를 참조하세요.	2020년 11월 9일

File Gateway에 대한 액세스 기반 열거	File Gateway는 이제 액세스 기반 열거 기능을 제공합니다. 이 기능은 공유의 ACL을 기준으로 SMB 파일 공유의 파일 및 폴더 열거를 필터링합니다. 자세한 내용은 SMB 파일 공유 생성을 참조하세요.	2020년 11월 9일
File Gateway 마이그레이션	File Gateway는 이제 기존 File Gateway를 새 File Gateway로 교체하는 문서화된 프로세스를 제공합니다. 자세한 내용은 File Gateway를 새 File Gateway로 교체를 참조하세요.	2020년 10월 30일
File Gateway 콜드 캐시 읽기 성능 4배 증가	Storage Gateway는 콜드 캐시 읽기 성능을 4배 높였습니다. 자세한 내용은 File Gateway 성능 지침을 참조하세요.	2020년 8월 31일
콘솔을 통해 하드웨어 어플라이언스 주문	이제 AWS Storage Gateway 콘솔을 통해 하드웨어 어플라이언스를 주문할 수 있습니다. 자세한 내용은 AWS Storage Gateway Hardware Appliance 사용을 참조하세요.	2020년 8월 12일
새 AWS 리전에서 Federal Information Processing Standard(FIPS) 엔드포인트 지원	이제 FIPS 엔드포인트를 사용하는 게이트웨이를 미국 동부(오하이오), 미국 동부(버지니아 북부), 미국 서부(캘리포니아 북부), 미국 서부(오리건), 캐나다(중부) 리전에서 활성화할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 7월 31일

단일 Amazon S3 버킷에 연결된 여러 파일 공유 지원	File Gateway는 이제 단일 S3 버킷에 대해 여러 파일 공유를 생성하고 디렉터리 액세스 빈도에 따라 File Gateway의 로컬 캐시를 버킷과 동기화할 수 있도록 지원합니다. File Gateway에서 생성하는 파일 공유를 관리하는 데 필요한 버킷 수를 제한할 수 있습니다. S3 버킷에 대해 여러 S3 접두사를 정의하고 단일 S3 접두사를 단일 게이트웨이 파일 공유에 매핑할 수 있습니다. 온프레미스 파일 공유 이름 지정 규칙에 맞게 버킷 이름과 무관하게 게이트웨이 파일 공유 이름을 정의할 수도 있습니다. 자세한 내용은 NFS 파일 공유 생성 또는 SMB 파일 공유 생성을 참조하세요.	2020년 7월 7일
File Gateway 로컬 캐시 스토리지 4배 증가	Storage Gateway에서 이제 캐시 볼륨과 File Gateway에 최대 64TB의 로컬 캐시를 지원하여 대규모 작업 데이터세트에 대한 지연 시간이 짧은 액세스를 제공하므로 온프레미스 애플리케이션의 성능이 향상됩니다. 자세한 내용은 Storage Gateway 사용 설명서의 게이트웨이에 권장되는 로컬 디스크 크기를 참조하세요.	2020년 7월 7일

Storage Gateway 콘솔에서 Amazon CloudWatch 경보 보기	이제 Storage Gateway 콘솔에서 CloudWatch 경보를 볼 수 있습니다. 자세한 내용은 CloudWatch 경보 이해를 참조하세요.	2020년 5월 29일
FIPS(Federal Information Processing Standard) 엔드포인트 지원	이제 AWS GovCloud (US) 리전에서 FIPS 엔드포인트가 있는 게이트웨이를 활성화할 수 있습니다. File Gateway에 대한 FIPS 엔드포인트를 선택하려면 서비스 엔드포인트 선택을 참조하세요.	2020년 5월 22일
새 AWS 리전	이제 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 5월 7일

S3 Intelligent-Tiering 스토리지 클래스 지원	Storage Gateway에서 이제 S3 Intelligent-Tiering 스토리지 클래스를 지원합니다. S3 Intelligent-Tiering 스토리지 클래스는 성능 영향 또는 운영 오버헤드 없이 가장 비용 효율적인 스토리지 액세스 계층으로 데이터를 자동으로 이동하여 스토리지 비용을 최적화합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 자주 액세스하는 객체와 자주 액세스하지 않는 객체를 자동으로 최적화하는 스토리지 클래스를 참조하세요.	2020년 4월 30일
새 AWS 리전	이제 Storage Gateway를 AWS GovCloud(미국 동부) 리전에서 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 3월 12일
Linux 커널 기반 가상 머신(KVM) 하이퍼바이저 지원	Storage Gateway에서 이제 KVM 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. KVM에 배포된 게이트웨이에는 기존 온프레미스 게이트웨이와 동일한 기능이 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하세요.	2020년 2월 4일

VMware vSphere High Availability 지원	Storage Gateway에서 이제 VMware에서의 고가용성을 지원하므로 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Storage Gateway와 함께 VMware vSphere High Availability 사용을 참조하세요. 이 릴리스에는 성능 향상도 포함되어 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 성능을 참조하세요.	2019년 11월 20일
Amazon CloudWatch Logs 지원	이제 Amazon CloudWatch 로그 그룹으로 File Gateway를 구성하여 오류 및 게이트웨이와 리소스의 상태에 대한 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Amazon CloudWatch 로그 그룹으로 게이트웨이 상태 및 오류에 대한 알림 받기를 참조하세요.	2019년 9월 4일
New AWS 리전	이제 아시아 태평양(홍콩) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 8월 14일

New AWS 리전	이제 중동(바레인) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 7월 29일
Virtual Private Cloud(VPC)에서 게이트웨이 활성화 지원	이제 VPC에서 게이트웨이를 활성화할 수 있습니다. 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하세요.	2019년 6월 20일
Microsoft Windows ACL용 SMB 파일 공유 지원	File Gateway의 경우 Microsoft Windows 액세스 제어 목록(ACL)을 사용하여 SMB(Server Message Block) 파일 공유에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 Microsoft Windows ACL를 사용하여 SMB 파일 공유에 대한 액세스 제어를 참조하세요.	2019년 5월 8일
File Gateway의 태그 기반 권한 부여 지원	File Gateway가 이제 태그 기반 권한 부여를 지원합니다. File Gateway 리소스의 태그를 기반으로 리소스에 대한 액세스를 제어할 수 있습니다. IAM 요청 조건에 전달할 수 있는 태그를 기반으로 액세스를 제어할 수도 있습니다. 자세한 내용은 File Gateway 리소스에 대한 액세스 제어를 참조하세요.	2019년 3월 4일

유럽의 AWS Storage Gateway 하드웨어 어플라이언스 가용성	이제 유럽에서 AWS Storage Gateway 하드웨어 어플라이언스를 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 AWS Storage Gateway Hardware Appliance 리전을 참조하세요. 또한 이제 AWS Storage Gateway 하드웨어 어플라이언스의 사용 가능한 스토리지를 5TB에서 12TB로 늘리고 설치된 동선 네트워크 카드를 10기가비트 광섬유 네트워크 카드로 교체할 수 있습니다. 자세한 내용은 하드웨어 어플라이언스 설정을 참조하세요.	2019년 2월 25일
AWS Storage Gateway 하드웨어 어플라이언스 지원	AWS Storage Gateway 하드웨어 어플라이언스에는 타사 서버에 사전 설치된 Storage Gateway 소프트웨어가 포함되어 있습니다. AWS Management Console에서 어플라이언스를 관리할 수 있습니다. 어플라이언스는 파일, 테이프 및 Volume Gateway를 호스팅할 수 있습니다. 자세한 내용은 Storage Gateway 하드웨어 어플라이언스 사용 섹션을 참조하세요.	2018년 9월 18일
SMB(Server Message Block) 프로토콜 지원	File Gateway에서 SMB(Server Message Block) 프로토콜에 대한 지원을 파일 공유에 추가했습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2018년 6월 20일

이전 업데이트

다음 표에서는 2018년 5월 이전 AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경	설명	변경 날짜
S3 One Zone_IA 스토리지 클래스 지원	File Gateway의 경우 S3 One Zone_IA를 파일 공유에 대한 기본 스토리지 클래스로 선택할 수 있습니다. 이 스토리지 클래스를 사용하여 Amazon S3의 단일 가용 영역에 객체 데이터를 저장할 수 있습니다. 자세한 내용은 파일 공유 생성 단원을 참조하십시오.	2018년 4월 4일
신규 AWS 리전	이제 아시아 태평양(싱가포르) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2018년 3월 4일
Amazon S3 버킷에 대한 캐시 새로 고침 알림, 요청자 지불 및 미리 준비된 ACL 지원	이제 게이트웨이가 Amazon S3 버킷에서 캐시 새로 고침을 완료하면 File Gateway를 통해 알림을 받을 수 있습니다. 자세한 내용은 API Gateway API 참조에서 RefreshCache.html를 참조하세요. File Gateway의 경우 이제 버킷 소유자 대신 요청자 또는 리더가 액세스 요금을 지불하도록 지정할 수 있습니다. 또한 File Gateway를 통해 NFS 파일 공유에 매핑되는 S3 버킷 소유자에게 작성된 파일에 대한 완전한 제어 권한을 제공할 수 있습니다. 자세한 내용은 파일 공유 생성 단원을 참조하십시오.	2018년 3월 1일
신규 AWS 리전	이제 유럽(파리) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2017년 12월 18일
파일 업로드 알림 및 MIME(Multipurpose Internet	이제 File Gateway를 통해 NFS 파일 공유에 기록한 모든 파일이 Amazon S3에 업로드되었을 때 알림을 받을	2017년 11월 21일

변경	설명	변경 날짜
Mail Extension) 유형 추측 지원	수 있습니다. 자세한 내용은 Storage Gateway API 참조에서 NotifyWhenUploaded를 참조하세요. 이제 File Gateway를 통해 파일 확장자를 기반으로 업로드되는 객체의 MIME 유형을 추측할 수 있습니다. 자세한 내용은 파일 공유 생성 단원을 참조하십시오.	
VMware ESXi Hypervisor 버전 6.5 지원	AWS Storage Gateway 는 이제 VMware ESXi Hypervisor 버전 6.5를 지원합니다. 이는 버전 4.1, 5.0, 5.1, 5.5 및 6.0에 추가된 지원 기능입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2017년 9월 13일
Microsoft Hyper-V 하이퍼바이저의 File Gateway 지원	이제 Microsoft Hyper-V 하이퍼바이저에 File Gateway를 배포할 수 있습니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하세요.	2017년 6월 22일
신규 AWS 리전	이제 아시아 태평양(뭄바이) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2017년 5월 02일
파일 공유 설정 업데이트 파일 공유에 대한 캐시 새로 고침 지원	이제 File Gateway를 통해 파일 공유 설정에 마운팅 옵션을 추가할 수 있습니다. 이제 파일 공유에 대해 스쿼시 및 읽기 전용 옵션을 설정할 수 있습니다. 자세한 내용은 파일 공유 생성 단원을 참조하십시오. 이제 File Gateway를 통해 게이트웨이가 마지막으로 버킷의 콘텐츠를 나열하고 결과를 캐시한 이후에 추가 또는 제거된 Amazon S3 버킷에서 객체를 찾을 수 있습니다. 자세한 내용은 API 참조의 RefreshCache를 참조하세요.	2017년 3월 28일

변경	설명	변경 날짜
Amazon EC2에서 File Gateway 지원	AWS Storage Gateway 는 이제 Amazon EC2에 파일 게이트웨이를 배포할 수 있는 기능을 제공합니다. 이제 커뮤니티 AMI로 사용할 수 있는 Storage Gateway Amazon Machine Image(AMI)를 사용하여 Amazon EC2에서 File Gateway를 시작할 수 있습니다. File Gateway를 생성하여 EC2 인스턴스에 배포하는 방법에 대한 정보는 Amazon S3 File Gateway 생성 및 활성화 섹션을 참조하세요. File Gateway AMI를 시작하는 방법에 대한 정보는 S3 File Gateway용 기본 Amazon EC2 호스트 배포 섹션을 참조하세요. 뿐만 아니라 File Gateway는 이제 HTTP 프록시 구성을 지원합니다. 자세한 내용은 HTTP 프록시를 통해 Amazon EC2에 배포된 게이트웨이 라우팅 단원을 참조하십시오.	2017년 2월 08일
신규 AWS 리전	이제 유럽(런던) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 12월 13일
신규 AWS 리전	이제 캐나다(중부) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 08월 12일
File Gateway 지원	Storage Gateway에서 이제 Volume Gateway 및 Tape Gateway 외에도 File Gateway를 제공합니다. File Gateway는 서비스와 가상 소프트웨어 어플라이언스를 결합함으로써 네트워크 파일 시스템(NFS)과 같은 업계 표준 파일 프로토콜을 사용하여 Amazon S3에(서) 객체를 저장하고 가져올 수 있게 해줍니다. 이 게이트웨이를 통해 NFS 마운트 포인트에 있는 파일인 Amazon S3 내 객체에 액세스할 수 있습니다.	2016년 11월 29일

Storage Gateway AL2에서 AL2023으로 마이그레이션 캠페인

AWS 는 새로운 하이브리드 클라우드 스토리지 기능을 활성화하고 최적의 성능 및 보안 표준을 유지하기 위해 Storage Gateway 어플라이언스 운영 체제(OS)를 Amazon Linux 2에서 AL2023으로 전환하고 있습니다. 이 전환은 모든 AL2-based Storage Gateway 어플라이언스 버전 S3 File Gateway 버전 1.x, Tape Gateway 버전 2.x 및 Volume Gateway 버전 2.x에 영향을 미칩니다. 는 이후 이러한 시스템 지원을 중단하므로 2026년 6월 30일 이전에 마이그레이션을 완료해야 AWS 합니다.

여러 방법을 통해 게이트웨이에 마이그레이션이 필요한지 여부를 식별할 수 있습니다. AWS 콘솔은 영향을 받는 게이트웨이에 대한 게이트웨이의 세부 정보 탭에 사용 중단 메시지를 표시합니다. 또한 `DescribeGatewayInformation` API는 사용 중단 날짜 필드를 확인할 수 있는 프로그래밍 방식의 액세스를 제공합니다. AWS 상태 대시보드는 영향을 받는 리소스 탭 아래에 영향을 받는 게이트웨이를 나열합니다. 그러나 게이트웨이가 마이그레이션된 직후에는 목록이 업데이트되지 않습니다. 마이그레이션 프로세스 자체는 데이터 안전을 우선시하도록 설계되었으며, 필요한 경우 쉽게 복구할 수 있도록 마이그레이션이 시작되기 AWS 전에 온프레미스 게이트웨이 VM 데이터의 사본을에 저장합니다.

AWS 는 각 게이트웨이 유형에 맞는 포괄적인 마이그레이션 가이드를 제공합니다. 마이그레이션을 완료한 후에는 AWS 콘솔의 게이트웨이 세부 정보 탭에 사용 중단 경고가 더 이상 나타나지 않는지 확인하거나 `DescribeGatewayInformation` API를 사용하여 사용 중단 날짜 필드가 없는지 확인하여 성공을 확인해야 합니다. 되돌리면 운영 문제가 발생할 수 있으므로 AL2023으로 성공적으로 마이그레이션한 후에는 AL2 게이트웨이로 되돌리지 않아야 합니다.

마이그레이션 기간 동안 AWS 는 이메일을 통해 월별 알림 알림과 AWS 상태 대시보드의 예약된 변경 사항 탭을 보내 마이그레이션을 계획하고 완료하는 데 도움을 줍니다. 마이그레이션 중에 문제가 발생하면 AWS Support에 문의하여 지원 및 문제 해결 지침을 받으세요.

빠른 링크 및 리소스

게이트웨이 버전 마이그레이션 참조

마이그레이션이 필요한 게이트웨이를 이해하는 것은 게이트웨이 소프트웨어 버전 번호에 따라 간단합니다. Amazon Linux 2 OS를 기반으로 최근에 활성화된 게이트웨이도 2026년 6월 30일까지 마이그레이션해야 합니다.

게이트웨이 유형	AL2 버전(마이그레이션 필요)	AL2023 버전(대상)
S3 File Gateway	버전 1.x	버전 2.x
Tape Gateway	버전 2.x	버전 3.x
Volume Gateway	버전 2.x	버전 3.x

마이그레이션 타임라인

마이그레이션 타임라인에는 다음과 같은 몇 가지 중요한 마일스톤이 포함되어 있습니다.

- 2025년 10월 28일: Storage Gateway 콘솔에서 시작된 모든 새 게이트웨이 배포는 기본적으로 AL2023 이미지로 설정됩니다.
- 2026년 1월 5일: AWS 새 AL2 게이트웨이 활성화를 제한하기 시작합니다.
- 2026년 6월 30일: AL2-based 게이트웨이는 소프트웨어 업데이트 수신을 중단하고 AWS 지원이 종료됩니다. 이 날짜 이후에는 AL2-based 어플라이언스를 계속 사용할 수 있지만 새 소프트웨어 업데이트, 보안 패치 또는 버그 수정은 없으며 이러한 시스템을 유지 관리하는 것은 전적으로 사용자의 책임입니다.

마이그레이션 가이드

- S3 파일 게이트웨이 마이그레이션 가이드
- Tape Gateway 마이그레이션 가이드
- Volume Gateway 마이그레이션 가이드

지원 및 모니터링

- Storage Gateway 콘솔
- AWS 개인 상태 대시보드
- AWS Support에 문의

FAQ

마이그레이션 중에 내 데이터는 어떻게 되나요?

마이그레이션 프로세스 AWS 전반에 걸쳐 데이터는에 안정적으로 저장됩니다. 마이그레이션 절차에는 필요한 경우 쉽게 복구할 수 AWS 있도록 온프레미스 게이트웨이 VM 데이터의 사본을에 저장하는 작업이 포함됩니다.

마이그레이션 중에 가동 중지가 발생하나요?

마이그레이션 타이밍과 잠재적 서비스 중단은 게이트웨이 유형 및 구성에 따라 달라집니다. 자세한 내용은 배포에 대한 게이트웨이별 마이그레이션 가이드를 검토하세요.

2026년 6월 30일까지 마이그레이션하지 않으면 어떻게 되나요?

게이트웨이는 계속 정상적으로 작동하며 데이터는 안전하게 저장되지만 업데이트 및 지원을 계속 받으려면 2026년 6월 30일까지 영향을 받는 게이트웨이를 마이그레이션 AWS해야 합니다.

마이그레이션 후에도 AL2 기반 게이트웨이를 계속 사용할 수 있나요?

아니요. 성공적으로 마이그레이션한 후에는 새 AL2023 게이트웨이와 함께 AL2 게이트웨이를 사용해서는 안 됩니다. 앞으로는 새 AL2023-based 게이트웨이만 사용합니다. AL2 및 AL2023 게이트웨이를 동시에 사용하면 운영 문제가 발생할 수 있습니다.

마이그레이션 중에 문제가 발생했습니다. 어떻게 해야 합니까?

AWS Support에 문의하여 도움을 받으세요. 지원 팀은 마이그레이션 문제를 해결하고 프로세스를 안내할 수 있습니다.

게이트웨이 어플라이언스 소프트웨어 릴리스 정보

이 릴리스 정보에서는 Amazon S3 File Gateway 어플라이언스의 각 버전에 포함된 새로운 기능과 업데이트된 기능, 개선 사항 및 수정 사항에 대해 설명합니다. 각 소프트웨어 버전은 릴리스 날짜와 고유 버전 번호로 식별됩니다.

Storage Gateway 콘솔에서 세부 정보 페이지를 확인하거나 다음과 유사한 AWS CLI 명령을 사용하여 DescribeGatewayInformation API 작업을 호출하여 Storage Gateway의 소프트웨어 버전 번호를 확인할 수 있습니다.

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

버전 번호는 API 응답의 `SoftwareVersion` 필드에 반환됩니다.

> **Note**
>
> 다음과 같은 상황에서는 게이트웨이가 소프트웨어 버전 정보를 보고하지 않습니다.
>
> - 게이트웨이가 오프라인 상태입니다.
> - 게이트웨이에서 버전 보고를 지원하지 않는 이전 소프트웨어를 실행 중입니다.
> - 게이트웨이 유형이 S3 File Gateway가 아닙니다.

게이트웨이의 기본 자동 유지 관리 및 업데이트 일정을 수정하는 방법을 포함하여 S3 File GatewayFSx Gateway 업데이트에 대한 자세한 내용은 스토리지 게이트웨이 콘솔을 AWS Storage Gateway .

Amazon Linux 2에서 AL2023으로 S3 파일 게이트웨이를 마이그레이션하는 방법에 대한 자세한 내용은 섹션을 참조하세요AL2에서 AL2023으로 마이그레이션.

Amazon Linux 2023(AL2023) 기반 게이트웨이

다음 표에는 AL2023 기반 게이트웨이의 릴리스 정보가 나와 있습니다.

> **Note**
>
> 게이트웨이 버전 1.x.x는 2.x.x로 업데이트할 수 없습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-03-02	2.0.7	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-02-12	2.1.2	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다. • SMB 공유에서 Windows Explorer를 사용할 때 보안 및 할당량 탭이 누락되는 문제를 해결합니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-02-02	2.1.1	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
		• 대/소문자를 구분하지 않는 파일 액세스와 관련된 SMB 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-01-21	2.0.6	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-01-16	2.1.0	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다. • SMB 스택을 업데이트했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-12-15	2.0.5	유지 관리 업데이트: • 루트 디스크 크기 지표 관련 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-11-12	2.0.4	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-11-12	2.0.4	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-10-15	2.0.3	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-09-15	2.0.2	유지 관리 업데이트: • 게이트웨이 용량을 변경하지 못하는 문제를 수정했습니다. • `UpdateSMBLocalGroups` API 관련 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-08-29	2.0.1	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 온프레미스 게이트웨이의 최초 릴리스입니다.
2025-08-21	2.0.0	기능: • 새 운영 체제의 최초 릴리스입니다. • IPv6 지원 추가됨

Amazon Linux 2(AL2) 기반 게이트웨이

다음 표에는 AL2 기반 게이트웨이의 릴리스 정보가 나와 있습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-02-27	1.27.20	유지 관리 업데이트:

릴리스 날짜	소프트웨어 버전	릴리스 정보
		• 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-02-11	1.28.2	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다. • SMB 공유에서 Windows Explorer를 사용할 때 보안 및 할당량 탭이 누락되는 문제를 해결합니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-02-02	1.28.1	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다. • 대/소문자를 구분하지 않는 파일 액세스와 관련된 SMB 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-01-21	1.27.19	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-01-16	1.28.0	유지 관리 업데이트: **Note** 롤아웃이 일시 중지되었습니다. 이 릴리스는 제한된 게이트웨이 세트로 롤아웃되었습니다. • SMB 스택을 업데이트했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-12-15	1.27.18	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-11-17	1.27.17	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-10-15	1.27.16	유지 관리 업데이트: • 업로드 이름 바꾸기 순서 로그의 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-09-22	1.27.15	유지 관리 업데이트: • 업로드 이름 바꾸기 순서 로그의 문제를 수정했습니다.
2025-09-15	1.27.14	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-08-21	1.27.13	유지 관리 업데이트: • 게이트웨이 성능에 대한 심층적인 인사이트를 제공하는 시스템 통계 및 지표가 추가되었습니다.
2025-08-18	1.27.12	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-08-11	1.27.11	유지 관리 업데이트: • 일부 게이트웨이의 특정 파일 작업에서 S3 메타데이터 업데이트에 영향을 미치는 문제를 수정했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-07-15	1.27.10	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 게이트웨이에 대한 업로드 이름 바꾸기 순서 로그 문제를 해결했습니다.
2025-06-23	1.27.9	유지 관리 업데이트: • 게이트웨이에 대한 업로드 이름 바꾸기 순서 로그 문제를 해결했습니다. • 새 게이트웨이에 대한 업로드 이름 바꾸기 순서 로그를 활성화했습니다. • 게이트웨이가 이제 성공적으로 업로드되지 않은 파일에 대한 삭제 작업을 올바르게 처리하도록 문제를 수정했습니다.
2025-06-16	1.27.8	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-05-26	1.27.7	유지 관리 업데이트: • 이름 바꾸기 순서에 대한 문제를 해결했습니다. **Note** 이 문제는 일부 게이트웨이에만 영향을 미칩니다. 게이트웨이를 업데이트해야 하는 경우 알림을 받게 됩니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-05-15	1.27.6	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-04-28	1.27.5	유지 관리 업데이트: • 업로드 이름 바꾸기 순서 로그와 관련된 문제를 수정했습니다. • 업로드 문제의 원인을 파악하는 데 도움이 되는 디버그 도구가 추가되었습니다. • 게이트웨이 성능에 대한 심층적인 인사이트를 위한 시스템 통계 및 지표가 추가되었습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-04-14	1.27.4	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-04-01	1.27.3	유지 관리 업데이트: • 게이트웨이 로깅 구성을 업데이트합니다. 고객의 조치는 필요하지 않습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-03-17	1.27.2	유지 관리 업데이트: • 게이트웨이에서 Amazon S3로 업로드하지 못한 파일의 캐시된 파일 공유 데이터 및 메타데이터를 제거하는 API 작업이 추가되었습니다. 이 함수를 사용하려면가 허용 목록에 있어야 AWS 계정 합니다. 게이트웨이에 파일 업로드 실패 문제가 있는 경우는 함수를 잠금 해제하고 사용에 대한 지침을 제공할 AWS Support 수 있습니다. • 새 게이트웨이가 객체 이름 바꾸기 업로드 작업의 순서를 로깅할 수 있는 기능이 추가되었습니다. 이렇게 하면 이름 바꾸기 작업을 반복하거나 겹친 후 파일이 Amazon S3에 업로드되지 않도록 방지할 수 있습니다. • 실수로 포트를 여는 SMB와 관련된 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-02-17	1.27.1	유지 관리 업데이트: • Java 11을 제거했습니다. • 지원 사용할 캐시 함수가 추가되었습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-01-17	1.27.0	기능: • 캐시 보고서(제공 예정) - S3 File Gateway에서 현재 캐시한 파일 메타데이터에 대한 보고서를 생성하도록 설계된 예정된 기능의 출시를 지원하도록 게이트웨이 소프트웨어를 업데이트했습니다. 게이트웨이에서 Amazon S3로 업로드하는 데 실패한 파일이 있는 경우 이러한 보고서를 사용하여 문제를 해결할 수 있습니다. 유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-01-09	1.26.9	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-12-18	1.26.8	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-11-18	1.26.7	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-10-17	1.26.6	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-09-30	1.26.5	유지 관리 업데이트: • 지원 채널을 허용하지 않는 온프레미스 게이트웨이 관련 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-09-16	1.26.3	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-08-21	1.26.1	유지 관리 업데이트: • 로깅과 관련된 문제를 수정했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-08-19	1.26.0	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-07-16	1.25.2	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-06-17	1.25.1	유지 관리 업데이트: • 프록시를 사용하고 DNS가 비활성화된 경우 업그레이드 관련 문제를 해결했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-05-15	1.25.0	기능: • AES-128 또는 AES-256 암호화 최소값을 설정하는 기능이 추가되었습니다. 이는 게이트웨이 변경 사항일 뿐이며 향후 릴리스에서 Storage Gateway 콘솔에서 사용할 수 있습니다. • 디스크 공간이 부족할 때 시스템 로그의 회전이 증가합니다. 이전에는 루트 디스크를 채운 로그 쓰기로 인해 게이트웨이가 중지되었습니다. 이제 공간이 줄어들면 게이트웨이는 이전 로그를 제거하여 최신 로그를 위한 공간을 더 많이 확보할 수 있습니다. • 파일 업로드 오류에 대한 상태 알림에 S3 경로가 추가되었습니다. 이전에는 상태 알림에 게이트웨이의 파일 경로만 표시되었습니다. 이제 알림에 사용자가 S3에서 파일을 찾는 데 도움이 되는 경로가 표시됩니다. • 이제 서비스는 강제 파일 공유 삭제 중에 백엔드 차단기를 무시합니다. 이전에는 강제 삭제가 블로커가 발생할 때 설명 없이 중지되었습니다. 이제 이러한 시나리오에

릴리스 날짜	소프트웨어 버전	릴리스 정보
		서 강제 삭제가 중단 없이 계속됩니다. 유지 관리 업데이트: • NFS 스택을 업데이트했습니다. • Java 17 JRE를 업그레이드했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-04-15	1.24.5	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-04-01	1.24.4	유지 관리 업데이트: • NTP(Network Time Protocol) 구성 요소 누락 문제를 해결했습니다.
2024-03-18	1.24.3	유지 관리 업데이트: • 대/소문자를 구분하는 조회 성능과 관련된 문제를 수정했습니다. • 프로세스가 충돌하는 문제를 수정했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-01-12	1.24.2	유지 관리 업데이트: • SMB 로깅 문제를 해결했습니다.
2023-12-27	1.24.1	유지 관리 업데이트: • SMB 안정성 문제를 해결했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보

2023-12-01	1.24.0	기능:
		• SMB 스택을 업데이트했습니다.
		  • AES-256 암호화에 대한 지원과 이를 요청하는 SMB 3.1.1 클라이언트를 사용할 때 AES-128 암호화 및 서명의 보다 안전한 변형이 추가되었습니다.
		  • SMBv1(LANMAN/CIFS) 서버 측 복사 및 서버 측 와일드카드 확장 기능이 제거되었습니다. (SMBv2 및 SMBv3는 영향을 받지 않습니다.) 이는 특정 SMBv1 워크로드의 성능에 부정적인 영향을 미칠 수 있습니다. SMBv1을 사용하는 경우 SMBv2 또는 SMBv3로 마이그레이션하는 것이 좋습니다.
		
		유지 관리 업데이트:
		• 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

2023-10-24	1.23.2	유지 관리 업데이트: • 지원 채널이 특정 사용자에 대해 제대로 연결되지 않는 것과 관련된 문제를 수정했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2023-08-14	1.23.1	유지 관리 업데이트: • 새 게이트웨이에 동기화 서버를 사용하도록 NTP 서버를 업데이트했습니다.
2023-06-12	1.23.0	기능: • 일부 AWS 계정의 업로드 스레드가 증가했습니다. 유지 관리 업데이트: • 대용량 사본에 대한 액세스 위반 문제를 수정했습니다. • NFS 문제가 수정되었습니다. • Java 8을 제거했습니다. • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2023-04-19	1.22.1	유지 관리 업데이트: • 폴더 및 파일 이름 변경과 관련된 문제를 수정했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2023-01-18	1.22.0	기능: • DOS 속성에 대한 지원 추가. • 게이트웨이당 지원되는 파일 공유 수를 10개에서 50개로 늘렸습니다. • 게이트웨이와 서비스가 동기화되지 않는 시점을 결정하는 클럭 스큐 감지 메커니즘을 구현했습니다. 유지 관리 업데이트: • SMB 스택을 업데이트했습니다.
2022-07-06	1.21.2	유지 관리 업데이트: • 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2022-02-16	1.21.1	기능: • 캐시의 이름 변경 및 삭제에 대한 새 지표가 추가되었습니다. 유지 관리 업데이트: • 기타 문제를 수정했습니다

릴리스 날짜	소프트웨어 버전	릴리스 정보
2022-01-18	1.21.0	기능: • 새로운 CloudWatch 지표가 추가되었습니다. • 데이터 업로드에 대한 대역폭 스로틀링 추가.
2021-12-12	1.20.0	## ####: • Log4j 취약성을 해결했습니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.