Volume Gateway 사용 설명서

AWS Storage Gateway

API 버전 2013-06-30

AWS Storage Gateway: Volume Gateway 사용 설명서

Table of Contents

Amazon S3 File Gateway 설명서가 Amazon S3 File Gateway란 무엇인가요?로 이동되었습니다.

Amazon FSx 파일 게이트웨이 설명서가 Amazon FSx 파일 게이트웨이란? 으로 이동되었습니다.

Tape Gateway 설명서가 Tape Gateway란 무엇인가요?로 이동되었습니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.

Volume Gateway란 무엇인가요?

AWS Storage Gateway 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지와 연결하여 온프레미스 IT 환경과 스토리지 인프라 간의 데이터 보안 기능과의 원활한 통합을 제공합니다. AWS 이 서비스를 사용하면 Amazon Web Services 클라우드에 데이터를 저장하여 데이터 보안 유지에 도움이 되는 확장 가능하면서 비용 효율적인 스토리지를 구현할 수 있습니다.

AWS Storage Gateway 는 파일 기반 파일 게이트웨이 (Amazon S3 파일 및 Amazon FSx File), 볼륨 기반 (캐시 및 저장) 및 테이프 기반 스토리지 솔루션을 제공합니다.

주제

볼륨 게이트웨이

볼륨 게이트웨이 — 볼륨 게이트웨이는 온 프레미스 애플리케이션 서버에서 인터넷 소형 컴퓨터 시스템 인터페이스 (iSCSI) 디바이스로 마운트할 수 있는 클라우드 기반 스토리지 볼륨을 제공합니다.

볼륨 게이트웨이는 온프레미스에서 VMware ESXi 실행되는 VM 어플라이언스 또는 Microsoft Hyper-V 하이퍼바이저로 하드웨어 어플라이언스로 배포하거나 Amazon 인스턴스로 AWS 배포할 수 있습니다. KVM EC2

이 게이트웨이가 지원하는 볼륨 구성은 아래와 같습니다.

- 캐시 볼륨 - 데이터는 Amazon Simple Storage Service(S3)에 저장하고 자주 액세스하는 데이터 하위 집합의 사본은 로컬에 보관합니다. 캐싱 볼륨을 통해 기본 스토리지 비용이 상당 부분 절감되고 온프레미스 스토리지를 확장할 필요성이 최소화됩니다. 자주 액세스하는 데이터에 액세스할 때는 지연 시간이 짧아지는 효과도 있습니다.
- 저장 볼륨 - 전체 데이터 세트에 대해 지연 시간이 낮은 액세스가 필요한 경우 먼저 모든 데이터를 로컬에 저장하도록 온프레미스 게이트웨이를 구성합니다. 그런 다음 이 데이터의 point-in-time 스냅샷을 Amazon S3에 비동기적으로 백업합니다. 이 구성은 로컬 데이터 센터 또는 Amazon Elastic Compute Cloud (AmazonEC2) 로 복구할 수 있는 안정적이고 저렴한 오프사이트 백업을 제공합니

다. 예를 들어 재해 복구를 위한 대체 용량이 필요한 경우 백업을 Amazon에 복구할 수 EC2 있습니다.

설명서: Volume Gateway 설명서는 볼륨 게이트웨이 생성 섹션을 참조하세요.

Storage Gateway를 처음 사용하시나요?

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

- 볼륨 게이트웨이 생성에서는 Volume Gateway를 생성 및 사용하는 방법에 대해 설명합니다. 또한 스토리지 볼륨을 만들고 이 볼륨에 데이터를 백업하는 방법을 설명합니다.

- 게이트웨이 관리에서는 게이트웨이 및 해당 리소스에 대한 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 API참조를 참조하십시오.

Volume Gateway 작동 방식(아키텍처)

다음에서 Volume Gateway 솔루션의 아키텍처 개요를 확인할 수 있습니다.

볼륨 게이트웨이

Volume Gateway의 경우 캐시 볼륨이나 저장 볼륨을 사용할 수 있습니다.

주제

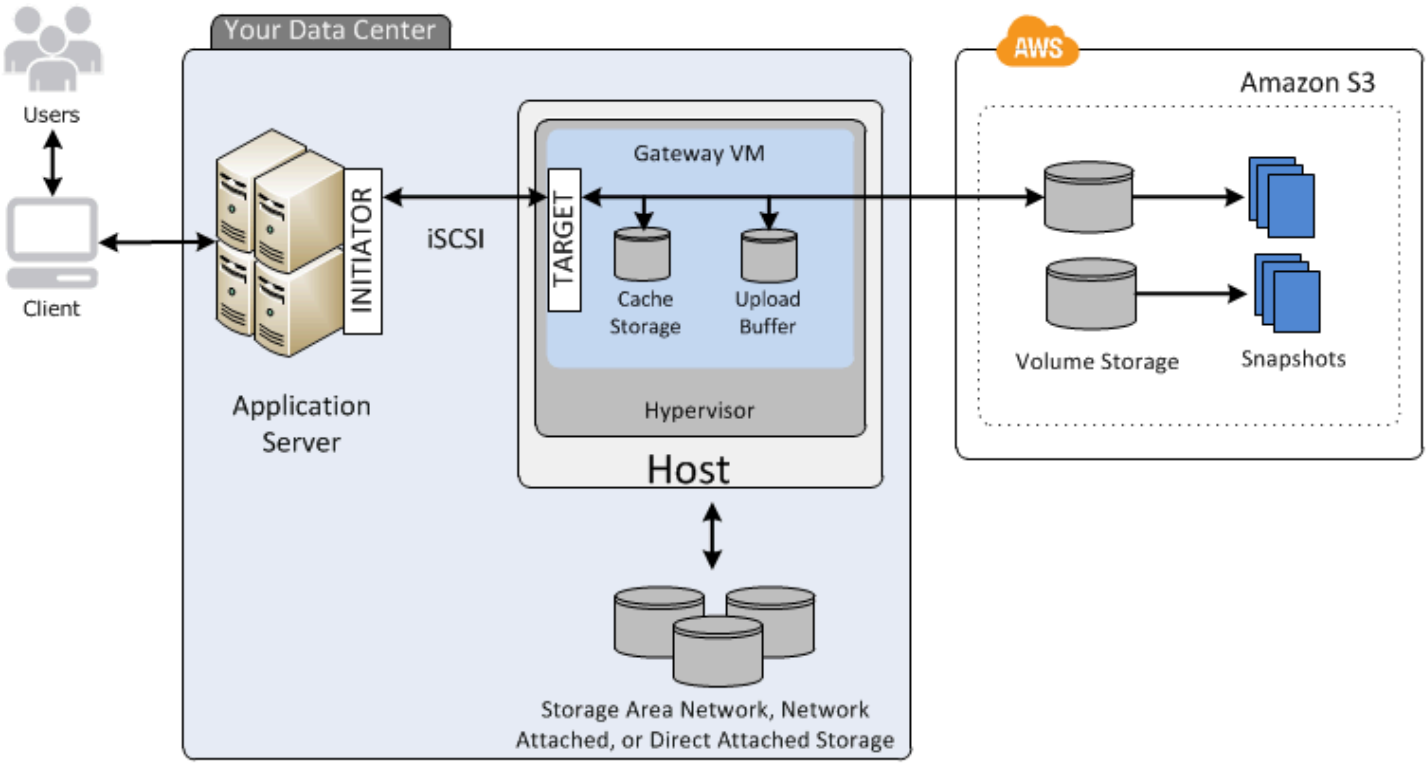
- 캐시 볼륨 아키텍처
- 저장 볼륨 아키텍처

캐시 볼륨 아키텍처

캐시 볼륨으로 Amazon S3를 기본 데이터 스토리지로 사용함과 동시에 자주 액세스하는 데이터를 Storage Gateway에 로컬 보관할 수 있습니다. 또한 온프레미스 스토리지 인프라를 확장할 필요성이 최소화되는 한편, 애플리케이션이 자주 액세스하는 데이터에 액세스할 때의 지연 시간을 짧게 유지할 수 있습니다. 최대 32TiB 크기의 스토리지 볼륨을 생성하고 온 프레미스 애플리케이션 서버에서 i SCSI 디바이스로 해당 볼륨에 연결할 수 있습니다. 게이트웨이는 이 볼륨에 작성하는 데이터는 Amazon S3에 저장하고 최근에 읽은 데이터는 온프레미스 스Storage Gateway의 캐시 및 업로드 버퍼 스토리지에 보관합니다.

캐싱 볼륨의 크기는 1GiB~32TiB이어야 하고 GiB 단위의 근사값으로 반올림해야 합니다. 캐싱 볼륨에 맞게 구성된 각 게이트웨이는 총 1,024TiB(1PiB)의 최대 스토리지 볼륨에 대해 32개까지 볼륨을 지원합니다.

캐시 볼륨 솔루션에서 Storage Gateway는 모든 온프레미스 애플리케이션 데이터를 Amazon S3의 스토리지 볼륨에 저장합니다. 다음 다이어그램은 캐싱 볼륨 배포의 개요입니다.



데이터 센터의 호스트에 Storage Gateway 소프트웨어 어플라이언스인 VM을 설치하고 활성화한 후에는 를 사용하여 Amazon S3가 지원하는 스토리지 볼륨을 프로비저닝합니다. AWS Management Console Storage Gateway API 또는 AWS SDK 라이브러리를 사용하여 프로그래밍 방식으로 스토리

지 볼륨을 프로비저닝할 수도 있습니다. 그런 다음 이러한 스토리지 볼륨을 온프레미스 애플리케이션 서버에 i SCSI 디바이스로 마운트합니다.

VM에 온 프레미스로 디스크를 할당할 수 있습니다. 이러한 온 프레미스 디스크는 다음의 목적을 달성합니다.

- 게이트웨이에서 AWS캐시 스토리지로 사용할 디스크 - 애플리케이션이 스토리지 볼륨에 데이터를 쓸 때 게이트웨이는 먼저 캐시 스토리지로 사용되는 온프레미스 디스크에 데이터를 저장합니다. 그런 다음 게이트웨이는 Amazon S3로 데이터를 업로드합니다. 캐시 스토리지는 업로드 버퍼에서 Amazon S3로 업로드 대기 중인 데이터를 위한 온프레미스 내구성 저장소 역할을 합니다.

  또한 캐시 스토리지는 지연 시간이 짧은 액세스를 위해 게이트웨이가 최근에 애플리케이션에서 액세스한 데이터를 온프레미스에 저장하도록 허용합니다. 애플리케이션에서 데이터를 요청하면 게이트웨이는 Amazon S3를 확인하기 전에 우선 캐시 스토리지에서 데이터를 확인합니다.

  다음 지침을 사용하여 캐시 스토리지를 할당할 디스크 공간의 크기를 결정할 수 있습니다. 일반적으로 기존 파일 저장소 크기의 최소 20퍼센트를 캐시 스토리지로 할당해야 합니다. 또한 캐시 스토리지는 업로드 버퍼보다 커야 합니다. 이렇게 하면 캐시 스토리지가 Amazon S3에 아직 업로드되지 않은 업로드 버퍼에 있는 모든 데이터를 일정하게 보유할 공간이 충분하도록 하는 데 도움이 됩니다.
- 게이트웨이에서 업로드 버퍼로 사용할 디스크 - 게이트웨이는 Amazon S3에 업로드하기 위한 준비 작업으로 업로드 버퍼라고 하는 스테이징 영역에 수신 데이터를 저장합니다. 게이트웨이는 암호화된 Secure Sockets Layer (SSL) 연결을 통해 이 버퍼 데이터를 AWS업로드하며, Amazon S3에 암호화된 상태로 저장됩니다.

Amazon S3에서 스토리지 볼륨의 증분 백업, 즉 스냅샷을 수행할 수 있습니다. 또한 이러한 point-in-time 스냅샷은 Amazon S3에 Amazon EBS 스냅샷으로 저장됩니다. 새 스냅샷을 만들 때 마지막 스냅샷 저장 이후에 변경된 데이터만 저장됩니다. 스냅샷이 생성되면 게이트웨이는 스냅샷 지점까지 변경 내용을 업로드한 다음 EBS Amazon을 사용하여 새 스냅샷을 생성합니다. 스냅샷을 일정에 따라 또는 일회적으로 실행할 수 있습니다. 단일 볼륨의 경우 여러 개의 스냅샷을 빠르게 연속으로 대기열에 추가할 수 있지만, 각 스냅샷의 생성이 완료되어야 다음 스냅샷을 생성할 수 있습니다. 스냅샷을 삭제할 때 다른 스냅샷에 필요하지 않은 데이터만 제거됩니다. Amazon 스냅샷에 대한 자세한 내용은 Amazon EBS EBS 스냅샷을 참조하십시오.

데이터 백업을 복구해야 하는 경우 Amazon EBS 스냅샷을 게이트웨이 스토리지 볼륨으로 복원할 수 있습니다. 또는 최대 16TiB 크기의 스냅샷의 경우 스냅샷을 새 Amazon EBS 볼륨의 시작점으로 사용할 수 있습니다. 그런 다음 이 새 Amazon EBS 볼륨을 Amazon EC2 인스턴스에 연결할 수 있습니다.

캐싱된 볼륨의 모든 게이트웨이 데이터와 스냅샷 데이터는 Amazon S3에 저장되며 서버 측 암호화 () 를 사용하여 저장 시 암호화됩니다. SSE 하지만 Amazon S3 API 또는 Amazon S3 관리 콘솔과 같은 다른 도구로는 이 데이터에 액세스할 수 없습니다.

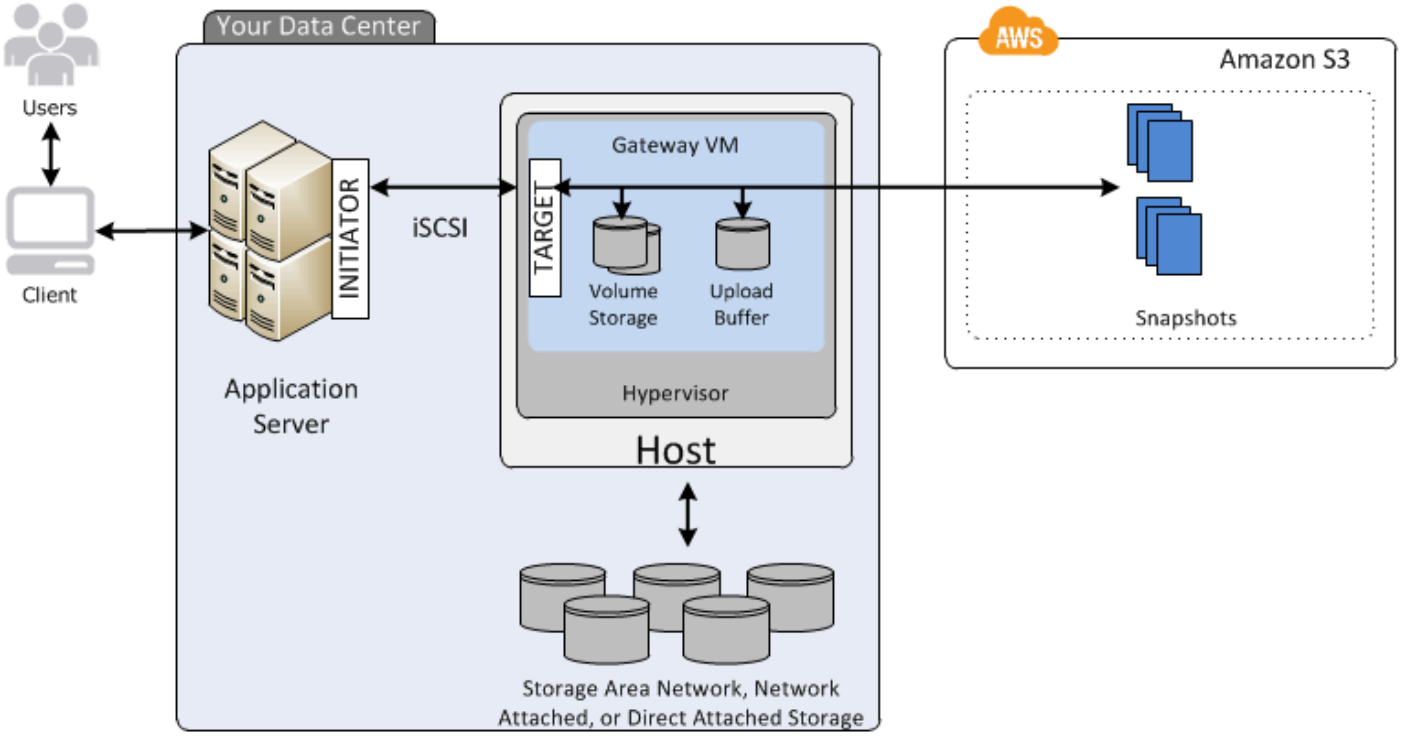
저장 볼륨 아키텍처

저장된 볼륨을 사용하면 기본 데이터를 로컬에 저장하고 해당 데이터를 비동기적으로 백업할 수 있습니다. AWS또한 저장 볼륨은 온프레미스 애플리케이션에서 전체 데이터 세트에 액세스할 때 지연 시간을 단축합니다. 이와 동시에 내구성이 우수한 오프사이트 백업을 제공합니다. 스토리지 볼륨을 생성하고 온프레미스 애플리케이션 서버에서 i SCSI 디바이스처럼 마운트할 수 있습니다. 저장 볼륨에 작성한 데이터는 온프레미스 스토리지 하드웨어에 저장됩니다. 이 데이터는 Amazon Elastic 블록 스토어 (Amazon) 스냅샷으로 Amazon S3에 비동기적으로 백업됩니다. EBS

저장 볼륨의 크기는 1GiB~16TiB이어야 하고 GiB 단위의 근사값으로 반올림해야 합니다. 저장 볼륨에 맞게 구성한 각 게이트웨이는 최대 32개 볼륨과 512TiB(0.5PiB)의 총 볼륨 스토리지를 지원할 수 있습니다.

저장 볼륨의 경우, 볼륨 스토리지를 데이터 센터에서 온프레미스 방식으로 유지 관리합니다. 다시 말하면, 모든 애플리케이션 데이터를 온 프레미스 스토리지 하드웨어에 저장하는 것입니다. 그런 다음 게이트웨이는 비용 효율적인 백업과 신속한 재해 복구를 위해 데이터 보안 유지에 도움이 되는 기능을 사용하여 Amazon Web Services 클라우드로 데이터를 업로드합니다. 이 솔루션은 모든 데이터에 액세스할 때 지연 시간이 짧아야 하고 아울러 백업을 AWS에서 유지 관리해야 하는 이유로 인해 데이터를 온프레미스 방식으로 로컬에 저장하려는 경우에 가장 적합합니다.

다음 다이어그램은 저장 볼륨 배포의 개요입니다.



데이터 센터의 호스트에 Storage Gateway 소프트웨어 어플라이언스(VM)를 설치하고 활성화한 후 게이트웨이 스토리지 볼륨을 생성할 수 있습니다. 그런 다음 온프레미스 직접 연결 스토리지 (DAS) 또는 SAN () 디스크에 매핑합니다. SAN 새 디스크로 진행해도 되고, 데이터를 이미 저장하고 있는 디스크로 진행해도 됩니다. 그런 다음 이러한 스토리지 볼륨을 온프레미스 애플리케이션 서버에 i 디바이스로 마운트할 수 있습니다. SCSI 온프레미스 애플리케이션이 데이터를 게이트웨이 저장 볼륨에서/으로 읽고 작성하면 이 데이터는 볼륨의 지정된 디스크에 저장 및 복원됩니다.

게이트웨이는 Amazon S3에 데이터를 업로드하기 위한 준비 작업으로 업로드 버퍼라고 하는 스테이징 영역에 수신 데이터를 저장합니다. 온프레미스 DAS 또는 SAN 디스크를 작업 스토리지로 사용할 수 있습니다. 게이트웨이는 암호화된 Secure Sockets Layer (SSL) 연결을 통해 업로드 버퍼의 데이터를 Amazon Web Services 클라우드에서 실행되는 Storage Gateway 서비스에 업로드합니다. 그러면 서비스는 해당 데이터를 암호화된 상태로 Amazon S3에 저장합니다.

스냅샷이라고 불리는 저장 볼륨에 대한 증분 백업을 실행할 수 있습니다. 게이트웨이는 이러한 스냅샷을 Amazon S3에 Amazon EBS 스냅샷으로 저장합니다. 새 스냅샷을 만들 때 마지막 스냅샷 저장 이후에 변경된 데이터만 저장됩니다. 스냅샷이 생성되면 게이트웨이는 스냅샷 지점까지 변경 내용을 업로드한 다음 EBS Amazon을 사용하여 새 스냅샷을 생성합니다. 스냅샷을 일정에 따라 또는 일회적으로 실행할 수 있습니다. 단일 볼륨의 경우 여러 개의 스냅샷을 빠르게 연속으로 대기열에 추가할 수 있지만, 각 스냅샷의 생성이 완료되어야 다음 스냅샷을 생성할 수 있습니다. 스냅샷을 삭제하면 다른 스냅샷이 필요하지 않은 데이터만 제거됩니다.

데이터 백업을 복구해야 하는 경우 Amazon EBS 스냅샷을 온 프레미스 게이트웨이 스토리지 볼륨으로 복원할 수 있습니다. 스냅샷을 새 Amazon EBS 볼륨의 시작점으로 사용하여 Amazon EC2 인스턴스에 연결할 수도 있습니다.

Storage Gateway 요금

가격 책정에 대한 최신 정보는 AWS Storage Gateway 세부 정보 페이지의 요금을 참조하십시오.

Storage Gateway 배포 계획

Storage Gateway 소프트웨어 어플라이언스를 사용하면 기존 온프레미스 애플리케이션 인프라를 데이터 보안 기능을 제공하는 확장 가능하고 비용 효율적인 AWS 클라우드 스토리지에 연결할 수 있습니다.

Storage Gateway를 배포하려면 먼저 다음 두 가지 사항을 결정해야 합니다.

1. 게이트웨이 유형 - 이 안내서에서는 다음 게이트웨이 유형을 다룹니다.
   - Volume Gateway - Volume Gateway를 사용하면 Amazon Web Services 클라우드에서 스토리지 볼륨을 생성할 수 있습니다. 온프레미스 애플리케이션은 인터넷 소형 컴퓨터 시스템 인터페이스(iSCSI) 대상으로 이러한 시스템에 액세스할 수 있습니다. 캐시 볼륨과 저장 볼륨의 두 가지 옵션이 있습니다.
     - 캐시된 볼륨의 경우 볼륨 데이터를 저장하고 최근에 액세스한 데이터 중 일부는 온프레미스 캐시에 저장합니다. AWS이 접근 방식을 사용하면 자주 액세스하는 데이터 세트에 신속하게(낮은 지연 시간) 액세스할 수 있습니다. 또한 저장된 전체 데이터세트에 원활하게 액세스할 수 있습니다. AWS캐싱된 볼륨을 사용하면 추가 하드웨어를 프로비저닝할 필요 없이 스토리지 리소스를 확장할 수 있습니다.
     - 저장 볼륨을 사용하면 전체 볼륨 데이터 세트를 온프레미스에 저장하고 주기적 point-in-time 백업 (스냅샷) 을 저장할 수 있습니다. AWS이 모델에서는 온프레미스 스토리지가 기본 스토리지이므로 전체 데이터세트에 대한 액세스 지연 시간이 짧습니다. AWS 스토리지는 데이터 센터에 재해가 발생할 경우 복원할 수 있는 백업입니다.

     캐싱된 볼륨과 저장된 볼륨 모두에 대해 Amazon EBS 스냅샷 형태로 볼륨 게이트웨이 볼륨의 point-in-time 스냅샷을 생성할 수 있습니다. 볼륨의 스냅샷을 새 Amazon 볼륨의 시작점으로 사용하여 Amazon EBS EC2 인스턴스에 연결할 수 있습니다. 이 접근 방식을 사용하면 데이터 처리를 위한 온디맨드 컴퓨팅 파워가 추가로 필요하거나 재해 복구를 위한 대체 용량이 필요한 EC2 경우 Amazon에서 실행되는 애플리케이션에 온 프레미스 애플리케이션의 데이터를 제공할 수 있습니

다. 이를 통해 데이터 보호, 복구, 마이그레이션 및 기타 다양한 데이터 전송 요구 사항에 맞게 공간 효율적인 버전 관리 볼륨 사본을 만들 수 있습니다.

Amazon EBS 스냅샷을 기반으로 볼륨을 생성하는 방법에 대한 자세한 내용은 볼륨 생성을 참조하십시오.

Volume Gateway의 아키텍처 개요는 캐시 볼륨 아키텍처 및 저장 볼륨 아키텍처를 참조하세요.

2. 호스팅 옵션 - Storage Gateway는 온프레미스에서 VM 어플라이언스 또는 하드웨어 어플라이언스로 실행하거나 Amazon EC2 인스턴스로 실행할 수 있습니다. AWS 자세한 내용은 볼륨 게이트웨이 설정 요구 사항 단원을 참조하십시오. 데이터 센터가 오프라인 상태이고 사용 가능한 호스트가 없는 경우 EC2 인스턴스에 게이트웨이를 배포할 수 있습니다. Storage Gateway는 게이트웨이 VM 이미지가 포함된 Amazon 머신 이미지 (AMI) 를 제공합니다.

이외에도 게이트웨이 소프트웨어 어플라이언스를 배포하도록 호스트를 구성할 때 게이트웨이 VM에 충분한 스토리지를 할당해야 합니다.

다음 단계로 넘어가기 전에 다음 작업을 완료했는지 확인합니다.

- 온프레미스에 배포된 게이트웨이의 경우 VM 호스트 유형을 선택하고 설정합니다. 옵션은 VMware ESXi 하이퍼바이저, Microsoft Hyper-V 및 Linux 커널 기반 가상 머신 () 입니다. KVM 방화벽 뒤에 게이트웨이를 배포하는 경우, 반드시 특정 포트가 게이트웨이 VM에 액세스할 수 있도록 해야 합니다. 자세한 내용은 볼륨 게이트웨이 설정 요구 사항 단원을 참조하십시오.

시작하기 AWS Storage Gateway

이 섹션에서는 Storage Gateway를 시작하는 방법에 대한 지침을 확인할 수 있습니다. 시작하려면 먼저 가입해야 AWS합니다. 처음 사용하는 경우, 먼저 리전 및 요구 사항 단원을 읽어보는 것이 좋습니다.

주제

가입하기 AWS Storage Gateway

Storage Gateway를 사용하려면 모든 AWS 리소스, 포럼, 지원 및 사용량 보고서에 대한 액세스 권한을 부여하는 Amazon Web Services 계정이 필요합니다. 서비스를 사용하지 않는다면 요금은 청구되지 않습니다. 이미 Amazon Web Services 계정이 있을 경우 이 단계를 건너뛸 수 있습니다.

Amazon Web Services 계정에 가입하려면

1. https://portal.aws.amazon.com/billing/등록 열기.
2. 온라인 지시 사항을 따릅니다.

   등록 절차 중 전화를 받고 전화 키패드로 확인 코드를 입력하는 과정이 있습니다.

   에 가입하면 AWS 계정 루트 사용자광이 생성됩니다. AWS 계정루트 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.

요금 정보는 Storage Gateway 세부 정보 페이지에서 요금을 참조하세요.

AWS 리전 Storage Gateway를 지원하는

Storage Gateway는 게이트웨이가 활성화된 AWS 지역에 볼륨, 스냅샷, 테이프 및 파일 데이터를 저장합니다. 파일 데이터는 Amazon S3 버킷이 위치한 AWS 지역에 저장됩니다. 게이트웨이 구축을 시작하기 전에 Storage Gateway 관리 콘솔의 오른쪽 상단에서 AWS 지역을 선택합니다.

- Storage Gateway—Storage Gateway에서 사용할 수 있는 지원 AWS 지역 및 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조
- Storage Gateway 하드웨어 어플라이언스 - 하드웨어 어플라이언스와 함께 사용할 수 있는 지원 AWS 지역은 의 하드웨어 어플라이언스 지역을 참조하십시오AWS Storage Gateway . AWS 일반 참조

볼륨 게이트웨이 설정 요구 사항

다른 언급이 없을 경우, 다음 요구 사항은 모든 게이트웨이 구성에 공통적으로 적용됩니다.

주제

- 하드웨어 및 스토리지 요구 사항
- 네트워크 및 방화벽 요구 사항
- 지원되는 하이퍼바이저 및 호스트 요구 사항
- i 이니시에이터 SCSI 지원

하드웨어 및 스토리지 요구 사항

이 섹션에서는 게이트웨이의 최소 하드웨어 및 설정과 필요한 스토리지에 할당할 최소 디스크 공간에 대해 설명합니다.

에 대한 하드웨어 요구 사항 VMs

게이트웨이를 배포하는 경우에는 게이트웨이 VM을 배포하는 기본 하드웨어가 다음의 최소 리소스를 제공할 수 있도록 해야 합니다.

- VM에 지정한 가상 프로세스 4개.
- 볼륨 게이트웨이 경우 하드웨어 전용으로 다음 용량을 할당해야 합니다. RAM
  - 캐시 크기가 최대 16TiB인 RAM 게이트웨이용으로 예약된 16GiB
  - 캐시 크기가 16TiB에서 32TiB인 RAM 게이트웨이용으로 예약된 32GiB
  - 캐시 크기가 32TiB에서 64TiB인 RAM 게이트웨이용으로 예약된 48GiB
- VM 이미지 및 시스템 데이터 설치용 디스크 공간 80GiB.

자세한 내용은 게이트웨이 성능 최적화 단원을 참조하십시오. 하드웨어가 게이트웨이 VM의 성능에 미치는 영향에 대한 정보는 AWS Storage Gateway 할당량 단원을 참조하십시오.

Amazon EC2 인스턴스 유형에 대한 요구 사항

Amazon Elastic Compute Cloud (AmazonEC2) 에 게이트웨이를 배포할 때 게이트웨이가 작동하려면 인스턴스 크기가 최소 xlarge 이상이어야 합니다. 하지만 컴퓨팅 최적화 인스턴스 패밀리의 경우 크기가 2xlarge 이상이 되어야 합니다.

볼륨 게이트웨이 경우, Amazon EC2 인스턴스는 게이트웨이에 사용할 캐시 크기에 RAM 따라 다음 용량을 할당해야 합니다.

- 캐시 크기가 최대 16TiB인 RAM 게이트웨이용으로 예약된 16GiB
- 캐시 크기가 16TiB에서 32TiB인 RAM 게이트웨이용으로 예약된 32GiB
- 캐시 크기가 32TiB에서 64TiB인 RAM 게이트웨이용으로 예약된 48GiB

게이트웨이 유형에 대한 권장 인스턴스 유형 중 하나를 사용합니다.

캐시 볼륨 및 Tape Gateway 유형별 권장 사항

- 범용 인스턴스 패밀리 – m4, m5 또는 m6 인스턴스 유형.

  > **Note**
  >
  > m4.16xlarge 인스턴스 유형은 사용하지 않는 것이 좋습니다.

- 컴퓨팅 최적화 인스턴스 패밀리 – c4, c5, 또는 c6 인스턴스 유형. 필요한 요구 사항을 충족하려면 2xlarge 인스턴스 크기 이상을 선택하십시오. RAM
- 메모리 최적화 인스턴스 패밀리 – r3, r5 또는 r6 인스턴스 유형.
- 스토리지 최적화 인스턴스 패밀리 – i3 또는 i4 인스턴스 유형.

스토리지 요구 사항

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

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)	업로드 버퍼 (최소값)	업로드 버퍼 (최대값)	필요한 다른 로컬 디스크
캐시 Volume Gateway	150GiB	64TiB	150GiB	2TiB	—
저장 Volume Gateway	—	—	150GiB	2TiB	저장 볼륨의 경우 1개 이상

> **Note**
>
> 캐시 및 업로드 버퍼에 대해 하나 이상의 로컬 드라이브를 최대 용량까지 구성할 수 있습니다. 기존 게이트웨이에 캐시 또는 업로드 버퍼를 추가할 때는 호스트 (하이퍼바이저 또는 Amazon EC2 인스턴스) 에 새 디스크를 생성하는 것이 중요합니다. 기존 디스크가 이전에 캐시 또는 업로드 버퍼로 할당되었던 경우, 디스크 크기를 변경하지 마십시오.

게이트웨이 할당량에 대한 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오.

네트워크 및 방화벽 요구 사항

게이트웨이에는 인터넷, 로컬 네트워크, Domain Name Service (DNS) 서버, 방화벽, 라우터 등에 대한 액세스 권한이 필요합니다. 아래에서 필수 포트에 대한 정보와 방화벽 및 라우터를 통한 액세스를 허용하는 방법에 대한 정보를 얻을 수 있습니다.

> **Note**
>
> 경우에 따라 Storage Gateway를 Amazon에 EC2 배포하거나 AWS IP 주소 범위를 제한하는 네트워크 보안 정책이 적용된 다른 유형의 배포 (온프레미스 포함) 를 사용할 수 있습니다. 이러한 경우 AWS IP 범위 값이 변경될 때 게이트웨이에서 서비스 연결 문제가 발생할 수 있습니다. 사용해야 하는 AWS IP 주소 범위 값은 게이트웨이를 활성화하는 AWS 지역의 Amazon 서비스 하위 집합에 있습니다. 현재 IP 범위 값은AWS 일반 참조에서 AWS IP 주소 범위를 참조하세요.

> **Note**
>
> 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. 경우에 따라 Amazon에 Storage Gateway를 EC2 배포하거나 다른 유형의 배포를 사용할 수 있습니다.

주제

포트 요구 사항

Storage Gateway가 작동하려면 특정 포트가 허용되어야 합니다. 다음 그림은 각 게이트웨이 유형에 대해 허용해야 하는 필수 포트를 보여줍니다. 일부 포트는 모든 유형의 게이트웨이에 필요하고, 기타 일부는 특정 유형의 게이트웨이에 필요합니다. 포트 요구 사항에 대한 자세한 내용은 볼륨 게이트웨이의 네트워크 포트 요구 사항 단원을 참조하십시오.

모든 게이트웨이 유형에 대한 공통 포트

다음 포트는 공통이기 때문에 모든 유형의 게이트웨이에 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
TCP	443 () HTTPS	아웃바운드	Storage Gateway	AWS	Storage Gateway에서 AWS 서비스 엔드포인트로의 통신용 서비스 엔드포인트에 대한 자세한 내용은 방화벽과

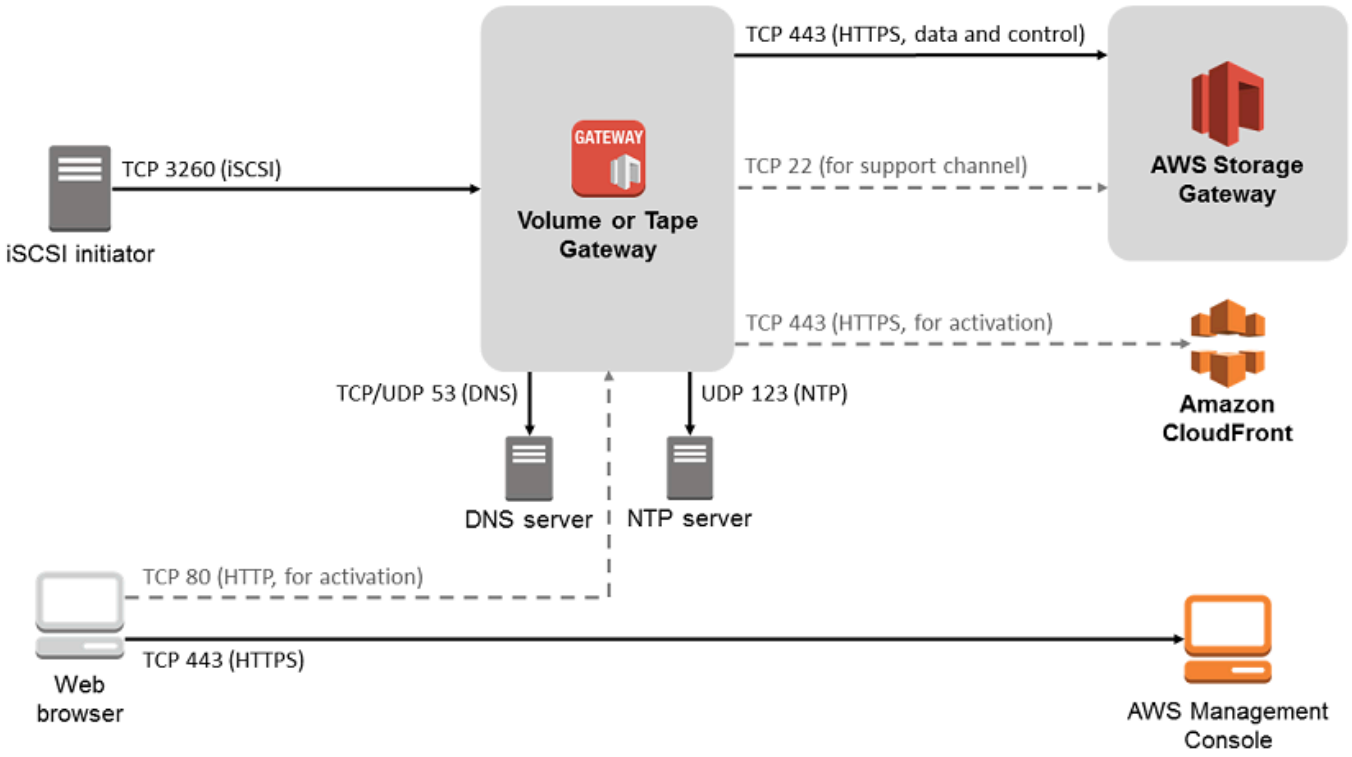
프로토콜	Port	Direction	소스	대상	용도
					AWS Storage Gateway 라우터를 통한 액세스 허용 단원을 참조하십시오.

프로토콜	Port	Direction	소스	대상	용도
TCP	80 (HTTP)	인바운드	AWS 관리 콘솔에 연결하는 데 사용하는 호스트입니다.	Storage Gateway	Storage Gateway 활성화 키를 가져올 때 로컬 시스템에서 사용합니다. 포트 80은 Storage Gateway 어플라이언스 활성화 중에만 사용됩니다. Storage Gateway에 대한 공개 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는 데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. Storage Gateway Management Console에서 게이트웨이를 활성화하는 경우, 콘솔에 연결하는 호스트가

프로토콜	Port	Direction	소스	대상	용도
					게이트웨이의 포트 80에 액세스할 수 있어야 합니다.
TCP/UDP	53 (DNS)	아웃바운드	Storage Gateway	도메인 네임 서비스 (DNS) 서버	Storage Gateway와 DNS 서버 간 통신용
TCP	22(지원 채널)	아웃바운드	Storage Gateway	AWS Support	게이트웨이 문제를 해결하는 데 도움이 되는 게이트웨이에 액세스할 수 있습니다. AWS Support 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다.
UDP	123 () NTP	아웃바운드	NTP클라이언트	NTP서버	로컬 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다.

Volume Gateway 및 Tape Gateway용 포트

다음은 Volume Gateway용으로 개방할 포트를 보여줍니다.



공통 포트 외에 Volume Gateway에는 다음 포트가 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
TCP	3260 (i) SCSI	인바운드	i 이니시에이터 SCSI	Storage Gateway	로컬 시스템을 통해 게이트웨이에 노출된 i SCSI 타겟에 연결합니다.

포트 요구 사항에 대한 자세한 내용은 추가 Storage Gateway 리소스 섹션에서 볼륨 게이트웨이의 네트워크 포트 요구 사항을 참조하세요.

Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항

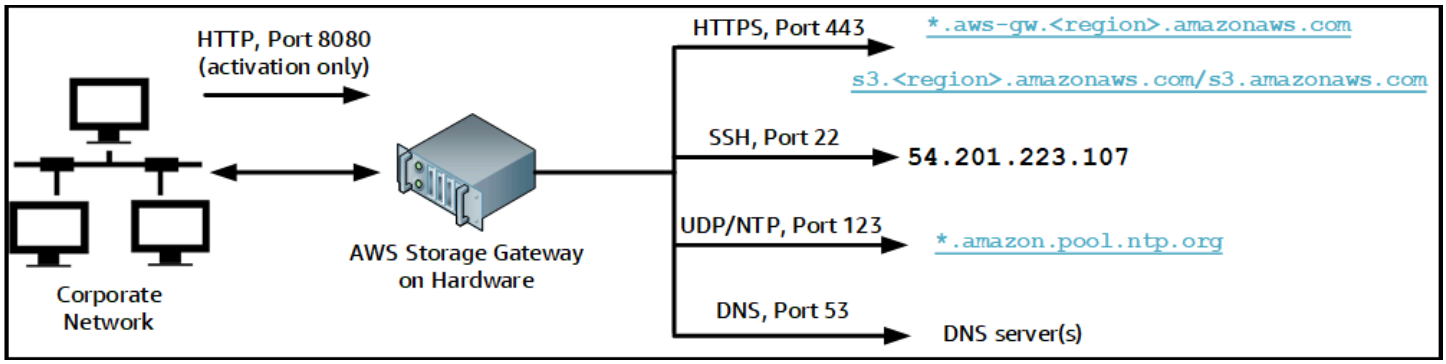
각 Storage Gateway 하드웨어 어플라이언스에는 다음과 같은 네트워크 서비스가 필요합니다.

- 인터넷 액세스 - 서버의 모든 네트워크 인터페이스를 통해 인터넷에 상시 접속할 수 있는 네트워크 연결입니다.
- DNSDNS서비스 — 하드웨어 어플라이언스와 DNS 서버 간의 통신을 위한 서비스.
- 시간 동기화 — 자동으로 구성된 Amazon NTP 시간 서비스에 연결할 수 있어야 합니다.
- IP 주소 — A DHCP 또는 고정 IPv4 주소가 할당되었습니다. IPv6주소는 할당할 수 없습니다.

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

1. i. DRAC
2. em1
3. em2
4. em3
5. em4

i DRAC 포트를 원격 서버 관리에 사용할 수 있습니다.



하드웨어 어플라이언스를 작동하려면 다음 포트가 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
SSH	22	아웃바운드	하드웨어 어플라이언스	54.201.223.107	지원 채널
DNS	53	아웃바운드	하드웨어 어플라이언스	DNS서버	이름 확인

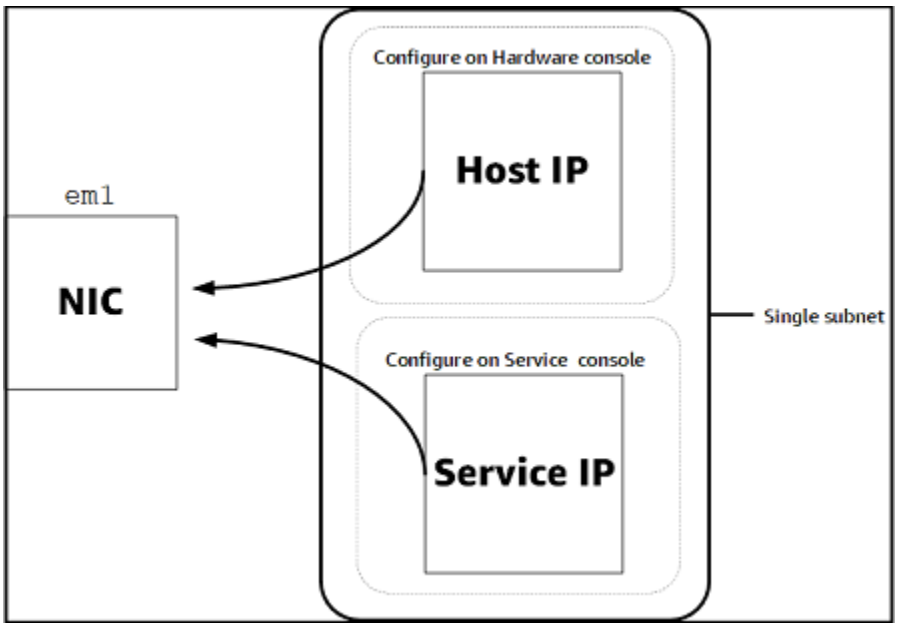
프로토콜	Port	Direction	소스	대상	용도
UDP/NTP	123	아웃바운드	하드웨어 어플라이언스	`*.amazon.pool.ntp.org`	시간 동기화
HTTPS	443	아웃바운드	하드웨어 어플라이언스	`*.amazonaws.com`	데이터 전송
HTTP	8080	인바운드	AWS	하드웨어 어플라이언스	활성화(잠시 동안)

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 네트워크 파라미터 구성 단원을 참조하십시오.

> **Note**
>
> 서버 뒷면과 포트가 나와 있는 그림을 보려면 하드웨어 어플라이언스의 물리적 설치 단원을 참조하십시오.

게이트웨이인지 호스트인지에 관계없이 동일한 네트워크 인터페이스 (NIC) 의 모든 IP 주소는 동일한 서브넷에 있어야 합니다. 다음 그림은 주소 지정 체계를 보여 줍니다.



하드웨어 어플라이언스 활성화 및 구성에 대한 자세한 내용은 Storage Gateway 하드웨어 어플라이언스 사용 단원을 참조하십시오.

방화벽과 AWS Storage Gateway 라우터를 통한 액세스 허용

게이트웨이가 통신하려면 다음 서비스 엔드포인트에 대한 액세스 권한이 필요합니다. AWS방화벽 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 Gateway에서 AWS연결 및 데이터 송수신에 사용할 프라이빗 VPC 엔드포인트를 구성하는 경우 게이트웨이는 공용 인터넷에 액세스할 필요가 없습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하세요.

> **Important**
>
> 게이트웨이 AWS 지역에 따라 다음을 대체하십시오.*region* 서비스 엔드포인트에서 올바른 지역 문자열을 사용하십시오.

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

```
s3.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
```

API전화를 걸려면 다음 게이트웨이 서비스 엔드포인트가 필요합니다.

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

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

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

다음에 표시된 Amazon S3 서비스 엔드포인트는 File Gateway에서만 사용됩니다. File Gateway에서 파일 공유가 매핑되는 S3 버킷에 액세스하려면 이 엔드포인트가 필요합니다.

```
bucketname.s3.region.amazonaws.com
```

다음 예제는 미국 동부(오하이오) 리전(us-east-2)의 S3 서비스 엔드포인트입니다.

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

> **Note**
>
> 게이트웨이가 S3 버킷이 위치한 AWS 지역을 확인할 수 없는 경우 이 서비스 엔드포인트는 기본적으로 로 s3.us-east-1.amazonaws.com 설정됩니다. 게이트웨이가 활성화되고 S3 버킷이 위치한 AWS 리전 외에 미국 동부(버지니아 북부) 리전(us-east-1)에 대한 액세스를 허용하는 것이 좋습니다.

다음은 AWS GovCloud (US) 리전에 대한 S3 서비스 엔드포인트입니다.

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

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

다음 예는 AWS GovCloud (미국 서부) 지역의 S3 버킷에 대한 FIPS 서비스 엔드포인트입니다.

```
bucket-name.s3-fips.us-gov-west-1.amazonaws.com
```

Storage Gateway 가상 머신은 다음 NTP 서버를 사용하도록 구성되어 있습니다.

```
0.amazon.pool.ntp.org
1.amazon.pool.ntp.org
2.amazon.pool.ntp.org
3.amazon.pool.ntp.org
```

- Storage Gateway—Storage Gateway에서 사용할 수 있는 지원 AWS 지역 및 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조
- Storage Gateway 하드웨어 어플라이언스 - 하드웨어 어플라이언스와 함께 사용할 수 있는 지원 AWS 지역은 의 Storage Gateway 하드웨어 어플라이언스 지역을 참조하십시오. AWS 일반 참조

Amazon EC2 게이트웨이 인스턴스의 보안 그룹 구성

보안 그룹은 Amazon EC2 게이트웨이 인스턴스로의 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 연결되도록 허용해야 하는 경우 포트 3260 (i 연결의 경우) 및 80 (활성화의 경우) 에서만 SCSI 연결을 허용하는 것이 좋습니다.
- 게이트웨이 보안 그룹 외부의 Amazon EC2 호스트에서 게이트웨이를 활성화하려면 해당 호스트의 IP 주소로부터 포트 80으로 들어오는 연결을 허용하십시오. 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 AWS Support 위해 사용하는 경우에만 포트 22 액세스를 허용하십시오. 자세한 내용은 게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2 단원을 참조하십시오.

경우에 따라 Amazon EC2 인스턴스를 이니시에이터 (즉, Amazon에 배포한 게이트웨이의 i SCSI 대상에 연결) 로 사용할 수 있습니다. EC2 이러한 경우 2단계 접근 방식을 권장합니다.

1. 게이트웨이와 동일한 보안 그룹에서 이니시에이터 인스턴스를 시작해야 합니다.
2. 이니시에이터가 게이트웨이와 통신할 수 있도록 액세스를 구성해야 합니다.

게이트웨이 용도로 개방하는 포트에 대한 자세한 내용은 볼륨 게이트웨이의 네트워크 포트 요구 사항 단원을 참조하십시오.

지원되는 하이퍼바이저 및 호스트 요구 사항

Storage Gateway는 가상 머신 (VM) 어플라이언스 또는 물리적 하드웨어 어플라이언스로 온프레미스에서 AWS 실행하거나 Amazon EC2 인스턴스로 실행할 수 있습니다.

> **Note**
>
> 제조업체가 하이퍼바이저 버전에 대한 일반 지원을 종료하면 Storage Gateway도 해당 하이퍼바이저 버전에 대한 지원을 종료합니다. 특정 버전의 하이퍼바이저 지원에 대한 자세한 내용은 제조업체 설명서를 참조하세요.

Storage Gateway에서 지원하는 하이퍼바이저 버전 및 호스트는 다음과 같습니다.

- VMwareESXi하이퍼바이저 (버전 7.0 또는 8.0) — 이 설정에는 호스트에 연결할 VMware vSphere 클라이언트도 필요합니다.
- Microsoft Hyper-V Hypervisor(버전 2012 R2, 2016, 2019 또는 2022) – Hyper-V의 무료 독립형 버전은 Microsoft 다운로드 센터에서 받을 수 있습니다. 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. KVMLinux 버전 2.6.20 이상의 모든 버전에 포함되어 있습니다. Storage Gateway는 RHEL 센토스/7.7, 우분투 16.04 및 우분투 LTS 18.04 배포판에 대해 테스트되고 지원됩니다. LTS 다른 최신 Linux 배포판이 작동하지만 기능이나 성능이 보장되지는 않습니다. 이미 실행 중인 KVM 환경이 있고 작동 방식에 이미 익숙하다면 이 옵션을 사용하는 것이 좋습니다. KVM
- Amazon EC2 인스턴스 — Storage Gateway는 게이트웨이 VM 이미지가 포함된 Amazon 머신 이미지 (AMI) 를 제공합니다. EC2Amazon에는 파일, 캐시 볼륨 및 테이프 게이트웨이 유형만 배포할 수 있습니다. EC2Amazon에 게이트웨이를 배포하는 방법에 대한 자세한 내용은 을 참조하십시오볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포.
- Storage Gateway 하드웨어 어플라이언스 - Storage Gateway는 제한된 가상 머신 인프라 위치에 대한 온프레미스 배포 옵션으로 물리적 하드웨어 어플라이언스를 제공합니다.

> **Note**
>
> Storage Gateway는 다른 게이트웨이 가상 머신 또는 EC2 AMI Amazon의 스냅샷이나 클론으로부터 생성된 가상 머신에서 게이트웨이를 복구하는 것을 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.

i 이니시에이터 SCSI 지원

캐시된 볼륨 또는 저장된 볼륨 게이트웨이를 배포할 때 게이트웨이에 i SCSI 스토리지 볼륨을 생성할 수 있습니다.

이러한 i SCSI 디바이스에 연결하기 위해 Storage Gateway는 다음과 같은 i SCSI 이니시에이터를 지원합니다.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- VMwareESX이니시에이터는 게스트 운영 체제에서 이니시에이터를 사용하는 대신 사용할 수 있는 대안을 제공합니다. VMs

> **Important**
>
> Storage Gateway는 Windows 클라이언트의 Microsoft 멀티패스 I/O (MPIO) 를 지원하지 않습니다.
> Storage Gateway는 호스트가 Windows Server 페일오버 클러스터링 () WSFC 을 사용하여 액세스를 조정하는 경우 여러 호스트를 동일한 볼륨에 연결할 수 있도록 지원합니다. 하지만 를

사용하지 않고는 여러 호스트를 동일한 볼륨에 연결할 수 없습니다 (예: 비클러스터형 NTFS / ext4 파일 시스템 공유). WSFC

액세스 AWS Storage Gateway

Storage Gateway Management Console을 사용하여 다양한 게이트웨이 구성 및 관리 작업을 수행할 수 있습니다. 이 설명서의 시작하기 단원 및 다양한 기타 단원에서는 콘솔을 사용하여 게이트웨이 기능을 설명합니다.

Storage Gateway 콘솔에 대한 브라우저 액세스를 허용하려면 브라우저가 Storage Gateway API 엔드포인트에 액세스할 수 있어야 합니다. 자세한 내용은AWS 일반 참조에서 Storage Gateway 엔드포인트 및 할당량을 참조하세요.

또한 를 사용하여 AWS Storage Gateway API 게이트웨이를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 에 대한 자세한 내용은 API 을 참조하십시오. APIStorage Gateway에 대한 참조

를 사용하여 Storage Gateway와 상호 작용하는 애플리케이션을 개발할 수도 있습니다. AWS SDKs AWS SDKsJava용,. NET기본 Storage API Gateway를 PHP 래핑하여 프로그래밍 작업을 단순화합니다. SDK라이브러리 다운로드에 대한 자세한 내용은 샘플 코드 라이브러리를 참조하십시오.

Storage Gateway 하드웨어 어플라이언스 사용

Storage Gateway 하드웨어 어플라이언스는 검증된 서버 구성에 Storage Gateway 소프트웨어가 사전 설치되어 있는 물리적 하드웨어 어플라이언스입니다. 하드웨어 어플라이언스는 AWS Storage Gateway 콘솔의 하드웨어 어플라이언스 개요 페이지에서 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 Amazon Web Services 계정과 연결됩니다. 활성화 후에는 하드웨어 어플라이언스가 콘솔의 하드웨어 어플라이언스 개요 페이지에 게이트웨이로 표시됩니다. 하드웨어 어플라이언스를 File Gateway, Tape Gateway, Volume Gateway 유형으로 구성할 수 있습니다. 하드웨어 어플라이언스에 이러한 게이트웨이 유형을 배포하고 활성화하는 절차는 가상 플랫폼에서의 절차와 동일합니다.

다음 섹션에서는 Storage Gateway 하드웨어 어플라이언스를 주문, 설정, 구성, 활성화, 시작 및 사용하는 방법에 대한 지침을 확인할 수 있습니다.

주제

지원되는 AWS 지역

Storage Gateway 하드웨어 어플라이언스를 활성화하고 사용할 수 AWS 리전 있는 지역의 지원 목록은 의 Storage Gateway 하드웨어 어플라이언스 지역을 참조하십시오 AWS 일반 참조.

하드웨어 어플라이언스 설정

Storage Gateway 하드웨어 어플라이언스를 받은 후에는 하드웨어 어플라이언스 콘솔을 사용하여 어플라이언스에 상시 접속을 제공하고 어플라이언스를 활성화하도록 네트워킹을 구성합니다. AWS 활성화를 통해 활성화 프로세스 중에 사용되는 Amazon Web Services 계정과 어플라이언스가 연결됩니다. 어플라이언스가 활성화되면 Storage Gateway 콘솔에서 파일, 볼륨 또는 Tape Gateway를 시작할 수 있습니다.

> **Note**
>
> 하드웨어 어플라이언스 펌웨어가 맞는지 확인하는 것은 사용자의 책임입니다. up-to-date

하드웨어 어플라이언스를 설치하고 구성하려면

1. 어플라이언스를 랙 마운팅하고 전원과 네트워크 연결을 가동합니다. 자세한 내용은 하드웨어 어플라이언스의 물리적 설치 단원을 참조하십시오.
2. 하드웨어 어플라이언스 (호스트IPv4) 와 Storage Gateway (서비스) 모두에 대해 인터넷 프로토콜 버전 4 () 주소를 설정합니다. 자세한 내용은 네트워크 파라미터 구성 단원을 참조하십시오.
3. 선택한 AWS 지역의 콘솔 하드웨어 어플라이언스 개요 페이지에서 하드웨어 어플라이언스를 활성화합니다. 자세한 내용은 하드웨어 어플라이언스 활성화 단원을 참조하십시오.
4. 하드웨어 어플라이언스에 Storage Gateway를 설치합니다. 자세한 내용은 게이트웨이 구성 단원을 참조하십시오.

   VMwareESXiMicrosoft Hyper-V, Linux 커널 기반 가상 머신 () 또는 Amazon에서 게이트웨이를 설정하는 것과 동일한 방식으로 하드웨어 어플라이언스에 게이트웨이를 설정합니다. KVM EC2

사용 가능한 캐시 스토리지 증가

하드웨어 어플라이언스의 사용 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있습니다. 이렇게 하면 더 큰 캐시가 제공되어 입력 데이터에 대한 액세스 지연 시간을 줄일 수 있습니다. AWS 5TB 모델을 주문한 경우 1.92TB SSDs (솔리드 스테이트 드라이브) 5개를 구입하여 사용 가능한 스토리지를 12TB까지 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. 재설정 방법에 대한 지침이 필요할 경우 Amazon Web Services Support에 문의하세요.
2. 어플라이언스에 1.92TB SSDs 5TB를 추가합니다.

네트워크 인터페이스 카드 옵션

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

- 10G-Base-T 구성: NIC
  - 10G의 경우 CAT6 케이블을 사용하거나 1G의 경우 (e) 케이블을 사용하십시오. CAT5
- 10G DA/ + 구성SFP: NIC
  - Twinax 구리 직접 연결 케이블(최대 5m) 사용
  - Dell/인텔 호환 SFP + 광학 모듈 (SR 또는 LR)
  - SFP/SFP+ 1G-Base-T 또는 10G-Base-T용 구리 트랜시버

하드웨어 어플라이언스의 물리적 설치

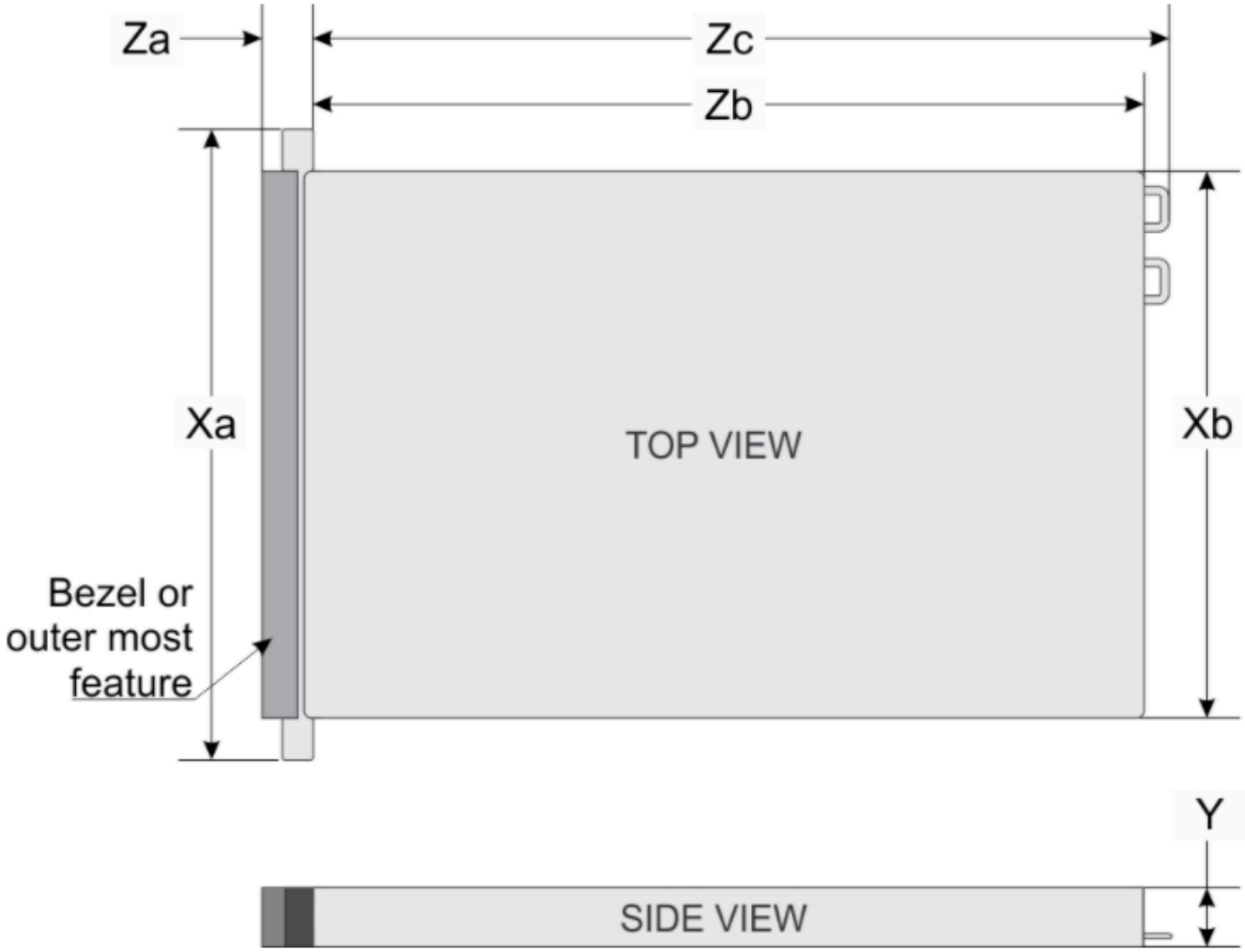
Storage Gateway 하드웨어 어플라이언스를 개봉한 후 동봉된 지침에 따라 서버를 랙에 장착합니다. 어플라이언스는 1U 폼 팩터를 사용하며 표준 국제 전기 기술 위원회 (IEC) 규정을 준수하는 19인치 랙에 맞습니다.

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 SFP Copper+DAC, 광학 모듈 (인텔 호환) 또는 Base-T 구리 SFP 트랜시버.
- 키보드 및 모니터 또는 키보드, 비디오 및 마우스 () 스위치 솔루션. KVM

하드웨어 어플라이언스 크기

장착 브래킷과 베젤을 포함한 하드웨어 어플라이언스 크기입니다.



System	Xa	Xb	Y	Za (with bezel)	Za (without bezel)	Zb*	Zc
10 x 2.5-inches	482.0 mm (18.97-inches)	434.0 mm (17.08-inches)	42.8 mm (1.68-inches)	35.84 mm (1.41-inches)	22.0 mm (0.87-inches)	733.82 mm (29.61-inches)	772.67 mm (30.42-inches)

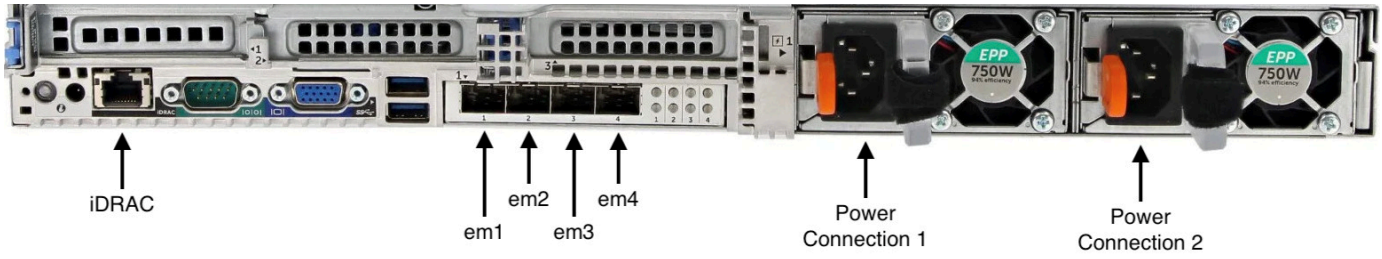
장착 브래킷과 베젤을 포함한 하드웨어 어플라이언스 크기입니다.

하드웨어 어플라이언스를 전원에 연결하려면

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

1. 2개의 전원 공급 장치 각각에 전원을 연결합니다. 하나의 전원 연결만 사용하는 것도 가능하지만 2개의 전원 공급 장치 모두에 연결하는 것이 좋습니다.

   다음 그림에는 다양한 연결이 가능한 하드웨어 어플라이언스가 나와 있습니다.
   네트워크 및 전원 커넥터 레이블이 표시된 하드웨어 어플라이언스 후면입니다.

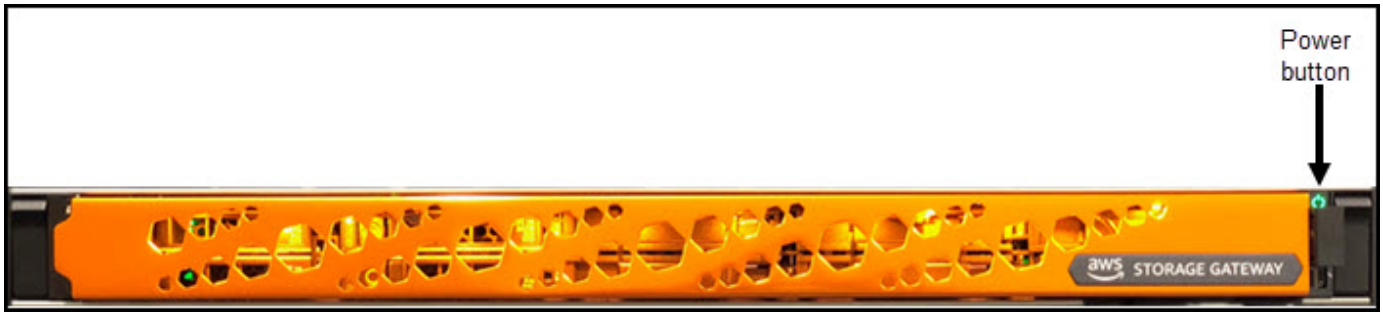
   

   네트워크 및 전원 커넥터 레이블이 표시된 하드웨어 어플라이언스 후면입니다.

2. 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 연결하는 스위치 포트를 트렁킹되지 않은 VLAN 포트로 설정합니다.

3. 키보드 및 모니터를 연결합니다.
4. 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.

서버가 부팅되면 하드웨어 콘솔이 모니터에 표시됩니다. 하드웨어 콘솔은 초기 네트워크 매개변수를 구성하는 데 사용할 수 AWS 있는 전용 사용자 인터페이스를 제공합니다. 이러한 파라미터를 구성하면 어플라이언스를 AWS 에 연결하고 Amazon Web Services Support의 문제 해결을 위한 지원 채널을 열 수 있습니다.

하드웨어 콘솔로 작업하려면 키보드를 사용하여 텍스트를 입력하고, `Up`, `Down`, `Right` 및 `Left Arrow` 키를 사용하여 화면에서 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.

최초로 암호를 설정하려면

1. 암호 설정에서 암호를 입력하고 `Down arrow` 키를 누릅니다.
2. 확인에서 암호를 재입력하고 암호 저장을 선택합니다.

하드웨어 어플라이언스 콘솔의 암호 설정 대화 상자 화면입니다.

하드웨어 어플라이언스 콘솔의 암호 설정 대화 상자 화면입니다.

이 시점에서 하드웨어 콘솔이 다음과 같이 표시됩니다.
연결 및 메뉴 옵션을 보여주는 하드웨어 어플라이언스 콘솔 기본 메뉴입니다.

연결 및 메뉴 옵션을 보여주는 하드웨어 어플라이언스 콘솔 기본 메뉴입니다.

다음 단계

네트워크 파라미터 구성

네트워크 파라미터 구성

서버 부팅 이후 하드웨어 어플라이언스의 물리적 설치에서 설명하는 것과 같이 하드웨어 콘솔에서 최초 암호를 입력합니다.

다음으로 하드웨어 콘솔에서 다음 단계를 수행하여 하드웨어 어플라이언스가 AWS에 연결될 수 있도록 네트워크 파라미터를 구성합니다.

네트워크 주소를 설정하려면

1. 네트워크 구성을 선택하고 `Enter` 키를 누릅니다. 다음과 같이 네트워크 구성 화면이 표시됩니다.
   하드웨어 어플라이언스 콘솔 네트워크 구성 화면입니다.

하드웨어 어플라이언스 콘솔 네트워크 구성 화면입니다.

2. IP 주소에 다음 소스 중 하나에서 가져온 유효한 IPv4 주소를 입력합니다.

   - 동적 호스트 구성 프로토콜 (DHCP) 서버에서 물리적 네트워크 포트에 할당한 IPv4 주소를 사용하십시오.

     그럴 경우 나중에 활성화 단계에서 사용할 수 있도록 이 IPv4 주소를 기록해 두십시오.

   - 고정 IPv4 주소를 할당하세요. 이렇게 하려면 em1 섹션에서 고정을 선택하고 Enter를 눌러 다음과 같은 고정 IP 구성 화면을 표시합니다.

     em1 섹션은 설정 그룹의 왼쪽 상단에 있습니다.

   유효한 IPv4 주소를 입력한 후 Down arrow 또는 를 누릅니다Tab.

   > **Note**
   >
   > 이 절차를 사용하여 em1 외에 다른 네트워크 인터페이스도 이중화를 위해 구성할 수 있습니다. 다른 인터페이스를 구성하는 경우 요구 사항에 나열된 엔드포인트와 동일한 Always-On 연결을 제공해야 합니다. AWS

네트워크 연결 및 링크 집계 제어 프로토콜 (LACP) 은 하드웨어 어플라이언스나 Storage Gateway에서 지원되지 않습니다.
서브넷에 여러 네트워크 인터페이스를 구성하면 라우팅 문제가 발생할 수 있으므로 권장하지 않습니다.

하드웨어 어플라이언스 NIC 콘솔을 고정 IP 화면으로 구성합니다.

하드웨어 어플라이언스 NIC 콘솔을 고정 IP 화면으로 구성합니다.

3. 서브넷에 유효한 서브넷 마스크를 입력한 후 Down arrow를 누릅니다.
4. 게이트웨이에 네트워크 게이트웨이 IPv4 주소를 입력한 다음 키를 누릅니다Down arrow.
5. 에 DNS1도메인 이름 서비스 (DNS) 서버의 IPv4 주소를 입력한 다음 키를 누릅니다Down arrow.
6. (선택 사항) 에 대해 DNS2두 번째 IPv4 주소를 입력한 다음 키를 누릅니다Down arrow. 두 번째 DNS 서버를 할당하면 첫 번째 DNS 서버를 사용할 수 없게 되는 경우에 대비하여 추가 이중화를 제공할 수 있습니다.
7. 저장을 선택한 다음 키를 Enter 눌러 어플라이언스의 고정 IPv4 주소 설정을 저장합니다.

하드웨어 콘솔에서 로그아웃하려면

1. 뒤로를 선택하여 기본 화면으로 돌아갑니다.
2. 로그아웃을 선택하여 로그인 화면으로 돌아갑니다.

다음 단계

[하드웨어 어플라이언스 활성화]

하드웨어 어플라이언스 활성화

IP 주소를 구성한 후 AWS Storage Gateway 콘솔의 하드웨어 페이지에 이 IP 주소를 입력하여 하드웨어 어플라이언스를 활성화합니다. 정품 인증 프로세스에서는 하드웨어 어플라이언스에 적절한 보안 인증 정보가 있는지 확인하고 어플라이언스를 AWS 계정에 등록합니다.

지원되는 제품 중 하나에서 하드웨어 어플라이언스를 활성화하도록 선택할 수 AWS 리전있습니다. 지원되는 AWS 리전목록은 의 Storage Gateway 하드웨어 어플라이언스 지역을 참조하십시오 AWS 일반 참조.

Storage Gateway 하드웨어 어플라이언스 활성화

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.
   > - 방화벽은 인바운드 트래픽에 대해 포트 8080을 통한 어플라이언스 HTTP 액세스를 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 참조하십시오.

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 파일 게이트웨이, FSx 파일 게이트웨이, 테이프 게이트웨이 또는 볼륨 게이트웨이를 구성하고 시작하는 것입니다.

다음 단계

게이트웨이 생성

게이트웨이 생성

하드웨어 어플라이언스에서 S3 FSx 파일 게이트웨이, 파일 게이트웨이, 테이프 게이트웨이 또는 볼륨 게이트웨이를 생성할 수 있습니다.

하드웨어 어플라이언스에서 게이트웨이를 생성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 하드웨어를 선택합니다.
3. 게이트웨이를 생성할 활성화된 하드웨어 어플라이언스를 선택한 다음 게이트웨이 생성을 선택합니다.
4. 게이트웨이 생성에 설명된 절차에 따라 선택한 게이트웨이 유형을 설정, 연결 및 구성합니다.

Storage Gateway 콘솔에서 게이트웨이 생성이 완료되면 Storage Gateway 소프트웨어가 하드웨어 어플라이언스에 자동으로 설치되기 시작합니다. 콘솔에서 게이트웨이가 온라인 상태로 표시되는 데 5-10분 정도 걸릴 수 있습니다.

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

다음 단계

게이트웨이에 대한 IP 주소 구성

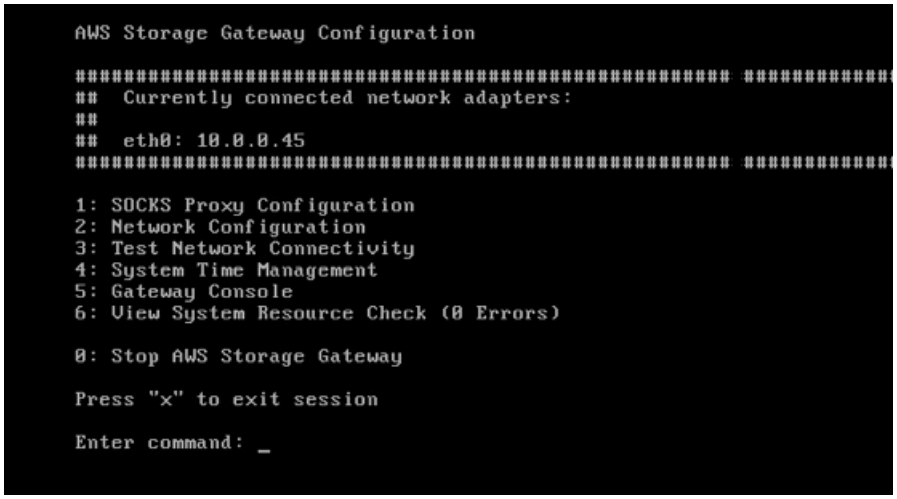
게이트웨이에 대한 IP 주소 구성

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 로컬 콘솔에서 해당 게이트웨이의 IP 주소를 구성합니다. 애플리케이션 (예: 사용자 NFS 또는 SMB 클라이언트, i SCSI 이니시에이터 등) 이 IP 주소에 연결됩니다. 게이트웨이 로컬 콘솔은 하드웨어 어플라이언스 콘솔에서 액세스할 수 있습니다.

애플리케이션에서 작동하도록 어플라이언스에서 IP 주소를 구성하려면

1. 하드웨어 콘솔에서 Open Service Console(서비스 콘솔 열기)를 선택하여 게이트웨이 로컬 콘솔에 대한 로그인 화면을 엽니다.
2. 로컬 호스트 로그인 암호를 입력한 후 `Enter` 키를 누릅니다.

   기본 계정은 `admin`이고 기본 암호는 `password`입니다.
3. 기본 암호를 변경합니다. 작업을 선택하고 Set Local Password(로컬 암호 설정)를 선택한 후 Set Local Password(로컬 암호 설정) 대화 상자에 새 자격 증명을 입력합니다.
4. (선택 사항) 프록시 설정을 구성합니다. 자세한 내용은 the section called “Storage Gateway 콘솔에서 로컬 콘솔 암호 설정” 섹션을 참조하세요.
5. 다음과 같이 게이트웨이 로컬 콘솔의 네트워크 설정 페이지로 이동합니다.
   네트워크 구성을 포함한 옵션을 보여주는 게이트웨이 로컬 콘솔 구성 페이지입니다.



네트워크 구성을 포함한 옵션을 보여주는 게이트웨이 로컬 콘솔 구성 페이지입니다.

6. 다음과 같이 2를 입력하여 Network Configuration(네트워크 구성) 페이지로 이동합니다.
고정 IP 옵션이 포함된 DHCP 게이트웨이 로컬 콘솔 네트워크 구성 페이지.

고정 IP 옵션이 포함된 DHCP 게이트웨이 로컬 콘솔 네트워크 구성 페이지

7. 하드웨어 어플라이언스의 네트워크 포트에 대한 고정 또는 DHCP IP 주소를 구성하여 애플리케이션용 파일, 볼륨 및 테이프 게이트웨이를 제공합니다. 이 IP 주소는 하드웨어 어플라이언스 활성화 중에 사용한 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.

다음 단계

게이트웨이 구성

게이트웨이 구성

하드웨어 어플라이언스가 활성화되고 구성되면 콘솔에 어플라이언스가 나타납니다. 이제 원하는 게이트웨이의 유형을 생성할 수 있습니다. 게이트웨이 유형에 맞는 게이트웨이 구성 페이지에서 설치를 계속 진행합니다. 지침은 Volume Gateway 구성을 참조하세요.

하드웨어 어플라이언스에서 게이트웨이 제거

하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거하려면 다음 절차를 수행합니다. 그러면 게이트웨이 소프트웨어가 하드웨어 어플라이언스에서 제거됩니다.

하드웨어 어플라이언스에서 게이트웨이를 제거하려면

1. Storage Gateway 콘솔의 하드웨어 페이지에서 삭제할 하드웨어 어플라이언스를 선택합니다.
2. 작업에서 Remove Gateway(게이트웨이 제거)를 선택합니다. 확인 대화 상자가 표시됩니다.
3. 지정된 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거할지 확인한 다음 확인 상자에 remove라는 단어를 입력하고 제거를 선택합니다.

> **Note**
>
> 게이트웨이 소프트웨어를 제거한 후에는 작업을 취소할 수 없습니다. 특정 게이트웨이 유형의 경우 삭제 시 데이터 특히, 캐싱된 데이터를 잃을 수 있습니다. 게이트웨이 삭제에 대한 자세한 내용은 게이트웨이 삭제 및 관련 리소스 제거 단원을 참조하십시오.

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

하드웨어 어플라이언스 삭제

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

> **Note**
>
> 어플라이언스를 다른 AWS 계정으로 이동하거나 AWS 리전하려면 먼저 다음 절차를 사용하여 어플라이언스를 삭제한 다음 게이트웨이의 지원 채널을 열고 AWS Support 문의하여 소프트 리셋을 수행해야 합니다. 자세한 내용은 문제를 해결하는 데 도움이 되도록 AWS Support 액세스 켜기를 참조하십시오.

하드웨어 어플라이언스를 삭제하려면

1. 하드웨어 어플라이언스에 게이트웨이를 설치한 경우, 먼저 게이트웨이를 제거해야 어플라이언스를 삭제할 수 있습니다. 하드웨어 어플라이언스에서 게이트웨이를 제거하는 방법은 하드웨어 어플라이언스에서 게이트웨이 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 주제에서는 Storage Gateway 생성 프로세스의 작동 방식에 대한 개괄적인 개요를 제공합니다. Storage Gateway 콘솔을 사용하여 특정 유형의 게이트웨이를 생성 볼륨 게이트웨이 생성을 참조하십시오.

개요 - 게이트웨이 활성화

게이트웨이 활성화에는 게이트웨이를 설정하고 연결한 다음 설정을 검토하고 활성화하는 작업이 포함됩니다. AWS

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 주문한 물리적 하드웨어 어플라이언스로 배포하거나 AWS 클라우드 환경의 Amazon EC2 인스턴스로 배포할 수도 있습니다. 게이트웨이 어플라이언스를 배포할 때 가상화 호스트에 로컬 물리적 디스크 공간을 할당합니다.

연결 대상 AWS

다음 단계는 게이트웨이를 AWS에 연결하는 것입니다. 이렇게 하려면 먼저 게이트웨이 가상 어플라이언스와 클라우드의 서비스 간 통신에 사용할 AWS 서비스 엔드포인트 유형을 선택합니다. 이 엔드포인트는 공용 인터넷을 통해 액세스할 수도 있고, 네트워크 보안 구성을 완전히 제어할 수 있는 Amazon VPC 내에서만 액세스할 수 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 업로

드 버퍼로 사용하도록 할당합니다. 그런 다음 Amazon CloudWatch Logs 및 CloudWatch 경보를 사용하여 게이트웨이 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.

볼륨 게이트웨이 생성

이 섹션에서는 Volume Gateway를 생성하고 사용하는 방법에 대한 지침을 확인할 수 있습니다.

주제

- 게이트웨이 생성
- 볼륨 생성
- 볼륨 사용
- 볼륨 백업

게이트웨이 생성

이 섹션에서는 Volume Gateway를 다운로드, 배포 및 활성화하는 방법에 대한 지침을 확인할 수 있습니다.

주제

- Volume Gateway 설정
- AWS에 Volume Gateway 연결
- 설정 검토 및 Volume Gateway 활성화
- Volume Gateway 구성

Volume Gateway 설정

새 Volume Gateway를 설정하려면

1. AWS Management Console https://console.aws.amazon.com/storagegateway/home/ 을 열고 게이트웨이를 생성할 AWS 리전 위치를 선택합니다.
2. 게이트웨이 생성을 선택하여 게이트웨이 설정 페이지를 엽니다.
3. 게이트웨이 설정 섹션에서 다음을 수행합니다.

   a. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 이 이름으로 검색하면 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 Volume Gateway를 선택한 다음 게이트웨이에서 사용할 볼륨 유형을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

   - 캐시 볼륨 - 기본 데이터는 Amazon S3에 저장하고 자주 액세스하는 데이터는 더 빠르게 액세스할 수 있도록 캐시에 로컬로 보관합니다.
   - 저장 볼륨 - 모든 데이터를 로컬에 저장하는 동시에 Amazon S3에 비동기적으로 백업합니다. 이 볼륨 유형을 사용하는 게이트웨이는 Amazon EC2에 배포할 수 없습니다.
5. 플랫폼 옵션 섹션에서 다음을 수행합니다.

   a. 호스트 플랫폼에서 게이트웨이를 배포할 플랫폼을 선택한 다음 Storage Gateway 콘솔 페이지에 표시되는 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 KVM을 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
      - Amazon EC2 - 게이트웨이를 호스팅할 Amazon EC2 인스턴스를 구성하고 시작합니다. 저장 볼륨 게이트웨이에는 이 옵션을 사용할 수 없습니다.
      - 하드웨어 어플라이언스 - 게이트웨이를 AWS 호스팅할 전용 물리적 하드웨어 어플라이언스를 주문하십시오.

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

6. 다음을 선택하여 계속 진행합니다.

이제 게이트웨이가 설정되었으므로 연결 및 통신 방법을 선택해야 AWS합니다. 자세한 지침은 볼륨 게이트웨이 연결 대상을 참조하십시오 AWS.

AWS에 Volume Gateway 연결

새 볼륨 게이트웨이를 연결하려면 AWS

1. Volume Gateway 설정에 설명된 절차를 아직 완료하지 않은 경우 해당 절차를 완료합니다. 완료했으면 다음을 선택하여 Storage Gateway 콘솔에서 AWS에 연결 페이지를 엽니다.
2. 엔드포인트 옵션 섹션의 서비스 엔드포인트에서 게이트웨이가 통신하는 데 사용할 엔드포인트 유형을 선택합니다 AWS. 다음 옵션 중에서 선택할 수 있습니다.

   - 공개 액세스 가능 - 게이트웨이는 공용 AWS 인터넷을 통해 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 통해 액세스할 때 FIPS 140-2로 검증된 암호화 모듈이 필요한 경우 FIPS 준수 엔드포인트를 사용하십시오. 자세한 내용은 FIPS(Federal Information Processing Standard) 140-2를 참조하세요.
     > FIPS 서비스 엔드포인트는 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 Storage Gateway 엔드포인트 및 할당량을 참조하세요.

   - VPC 호스팅 - 게이트웨이가 VPC와의 프라이빗 연결을 통해 AWS 와 통신하므로 사용자가 네트워크 설정을 제어할 수 있습니다. 이 옵션을 선택하는 경우 드롭다운 메뉴에서 VPC 엔드포인트 ID를 선택하거나 VPC 엔드포인트 DNS 이름 또는 IP 주소를 제공하여 기존 VPC 엔드포인트를 지정해야 합니다.

3. 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.
- 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.

4. 다음을 선택하여 계속 진행합니다.

게이트웨이 연결 방법을 선택했으니 이제 게이트웨이를 활성화해야 합니다. AWS지침은 설정 검토 및 Volume Gateway 활성화를 참조하세요.

설정 검토 및 Volume Gateway 활성화

새 Volume Gateway를 활성화하려면

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

   - Volume Gateway 설정
   - 볼륨 게이트웨이를 다음 위치에 연결 AWS

   완료했으면 다음을 선택하여 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.

   > **Note**
   >
   > 게이트웨이가 생성된 후에는 게이트웨이 옵션 또는 연결 설정을 수정할 수 없습니다.

4. 게이트웨이 활성화를 선택하여 계속 진행합니다.

게이트웨이를 활성화했으므로 로컬 스토리지 디스크를 할당하고 로깅을 구성하기 위한 최초 구성을 수행해야 합니다. 지침은 Volume Gateway 구성을 참조하세요.

Volume Gateway 구성

새 Volume Gateway에서 최초 구성을 수행하려면

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

   - Volume Gateway 설정
   - 볼륨 게이트웨이를 다음 위치에 연결 AWS
   - 설정 검토 및 Volume Gateway 활성화

   완료했으면 다음을 선택하여 Storage Gateway 콘솔에서 게이트웨이 구성 페이지를 엽니다.
2. 스토리지 구성 섹션에서 드롭다운 메뉴를 사용하여 캐시 스토리지에 용량이 165GiB 이상인 디스크를 하나 이상 할당하고 업로드 버퍼에 용량이 150GiB 이상인 디스크를 하나 이상 할당합니다. 이 섹션에 나열된 로컬 디스크는 호스트 플랫폼에서 프로비저닝한 물리적 스토리지에 해당합니다.
3. CloudWatch 로그 그룹 섹션에서 Amazon CloudWatch Logs를 설정하여 게이트웨이의 상태를 모니터링하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

   - 새 로그 그룹 생성 - 게이트웨이를 모니터링할 새 로그 그룹을 설정합니다.
   - 기존 로그 그룹 사용 - 해당 드롭다운 메뉴에서 기존 로그 그룹을 선택합니다.
   - 로깅 비활성화 - Amazon CloudWatch Logs를 사용하여 게이트웨이를 모니터링하지 마십시오.

   > **Note**
   >
   > Storage Gateway 상태 로그를 수신하려면 로그 그룹 리소스 정책에 다음 권한이 있어야 합니다. ## ### ### ### 대한 특정 로그 그룹 ResourceARN 정보로 바꾸십시오.

   ```
   "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:*"
```

"리소스" 요소는 권한을 개별 로그 그룹에 명시적으로 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 경보 이해를 참조하십시오. CloudWatch

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

   - 사용자 지정 경보 생성 - 게이트웨이의 지표에 대해 알리도록 새 CloudWatch 경보를 구성하십시오. Amazon CloudWatch 콘솔에서 지표를 정의하고 경보 조치를 지정하려면 [Create alarm]을 선택합니다. 지침은 Amazon 사용 CloudWatch 설명서의 Amazon CloudWatch 경보 사용을 참조하십시오.
   - 알람 없음 — 게이트웨이 지표에 대한 CloudWatch 알림을 받지 마십시오.

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

6. 구성을 선택하여 게이트웨이 생성을 완료합니다.

   새 게이트웨이의 상태를 확인하려면 Storage Gateway의 게이트웨이 개요 페이지에서 해당 게이트웨이를 검색합니다.

게이트웨이를 생성했으므로 게이트웨이에서 사용할 볼륨을 생성해야 합니다. 지침은 볼륨 생성을 참조하세요.

볼륨 생성

앞서 추가한 로컬 디스크를 VM 캐시 스토리지 및 업로드 버퍼에 할당하였습니다. 이제 애플리케이션이 데이터를 읽고 쓸 스토리지 볼륨을 생성합니다. 게이트웨이는 볼륨이 최근에 액세스한 데이터를 캐시 스토리지에 로컬로 유지 관리하고, 아울러 Amazon S3에 비동기식으로 전송한 데이터를 유지 관리합니다. 저장 볼륨의 경우, 추가한 로컬 디스크를 VM 업로드 버퍼 및 애플리케이션 데이터에 할당하였습니다.

> **Note**
>
> AWS Key Management Service (AWS KMS) 를 사용하여 Amazon S3에 저장된 캐시 볼륨에 기록된 데이터를 암호화할 수 있습니다. 현재AWS Storage Gateway API 참조를 사용하여 이를 수행할 수 있습니다. 자세한 내용은 CreateCachediSCSIVolume 또는 을 참조하십시오. create-cached-iscsi-volume

볼륨을 생성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. Storage Gateway 콘솔에서 볼륨 생성을 선택합니다.
3. 볼륨 생성 대화 상자의 게이트웨이에서 게이트웨이를 선택합니다.
4. 캐시 볼륨의 경우, 용량에 용량을 입력합니다.

   저장 볼륨의 경우, 목록에서 디스크 ID 값을 선택합니다.
5. 볼륨 콘텐츠의 경우, 볼륨을 생성하는 게이트웨이의 유형에 따라 선택 사항이 달라집니다.

   캐싱 볼륨의 경우, 다음과 같은 옵션이 있습니다.

   - 새 빈 볼륨 생성(Create a new empty volume).
   - Amazon EBS 스냅샷을 기반으로 볼륨 생성. 이 옵션을 선택하는 경우 EBS 스냅샷 ID의 값을 지정합니다.

     > **Note**
     >
     > 스토리지 게이트웨이는 AWS Marketplace 볼륨의 스냅샷에서 캐시 볼륨을 생성하는 기능을 지원하지 않습니다.

- 마지막 볼륨 복구 지점에서 복제. 이 옵션을 선택하는 경우 소스 볼륨의 볼륨 ID를 선택합니다. 리전에 볼륨이 없으면 이 옵션이 표시되지 않습니다.

저장 볼륨의 경우, 다음과 같은 옵션이 있습니다.

- 새 빈 볼륨 생성(Create a new empty volume).
- 스냅샷을 기반으로 볼륨 생성(Create a volume based on a snapshot). 이 옵션을 선택하는 경우 EBS 스냅샷 ID의 값을 지정합니다.
- 디스크의 기존 데이터 보존

6. iSCSI 대상 이름에 이름을 입력합니다.

   대상 이름은 소문자, 숫자, 마침표(.), 하이픈(-)을 포함할 수 있습니다. 이 대상 이름은 검색 후 iSCSI Microsoft 이니시에이터 UI의 대상 탭에 iSCSI 대상 노드 이름으로 나타납니다. 예를 들어 `target1`이라는 이름은 `iqn.1007-05.com.amazon:target1`으로 표시됩니다. 대상 이름이 스토리지 영역 네트워크(SAN) 내에서 전역적으로 고유한지 확인합니다.

7. 네트워크 인터페이스 설정에 선택된 IP 주소가 있는지 확인하여 없을 경우 네트워크 인터페이스에서 IP 주소를 선택합니다. 네트워크 인터페이스의 경우, 게이트웨이 VM에 대해 구성된 각 어댑터마다 IP 주소 하나가 표시됩니다. 게이트웨이 VM이 네트워크 어댑터 한 개에만 구성된 경우, IP 주소가 하나밖에 없으므로 네트워크 인터페이스 목록은 표시되지 않습니다.

   iSCSI 대상은 선택하는 네트워크 어댑터에서 사용할 수 있습니다.

   여러 네트워크 어댑터를 사용하도록 게이트웨이를 정의한 경우 스토리지 애플리케이션이 볼륨에 액세스하는 데 사용해야 할 IP 주소를 선택합니다. 다중 네트워크 어댑터 구성에 대한 자세한 내용은 다중 게이트웨이 구성 NICs 단원을 참조하십시오.

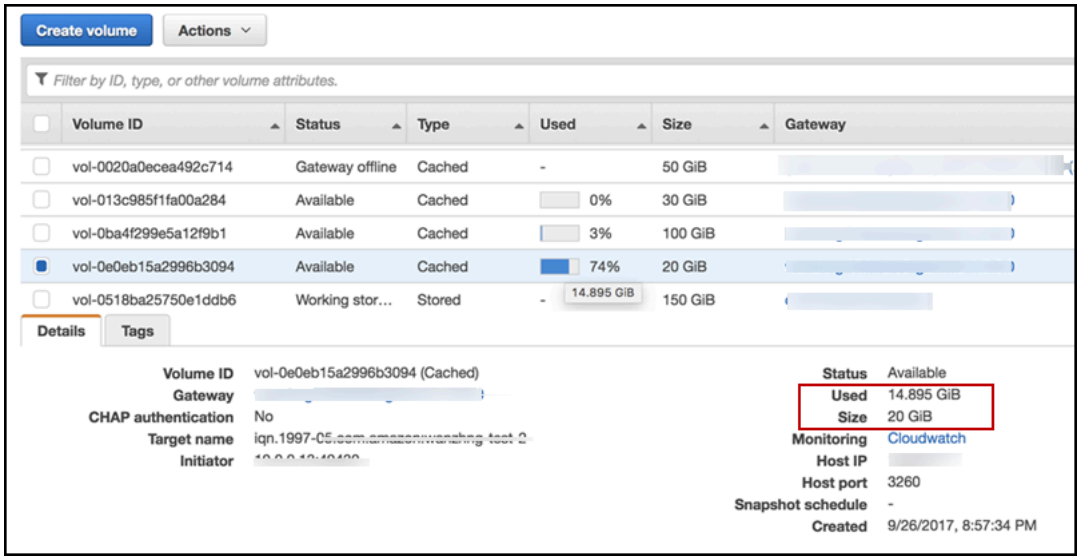
   > **Note**
   >
   > 네트워크 어댑터를 선택한 후에는 이 설정을 변경할 수 없습니다.

8. (선택 사항) 태그에 키와 값을 입력하여 태그를 볼륨에 추가합니다. 태그는 볼륨을 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.

9. 볼륨 생성을 선택합니다.

   이 리전에서 이전에 볼륨을 생성한 적이 있다면 Storage Gateway 콘솔에 해당 볼륨이 나열됩니다.

그러면 CHAP 인증 구성 대화 상자가 나타납니다. 이때 볼륨에 대해 CHAP(Challenge-Handshake Authentication Protocol)을 구성하거나 취소를 선택하여 나중에 CHAP을 구성할 수 있습니다. CHAP 설정에 대한 자세한 내용은 볼륨에 대한 CHAP 인증 구성 섹션을 참조하세요.



CHAP를 설정하지 않으려면 볼륨 사용을 시작합니다. 자세한 설명은 볼륨 사용 섹션을 참조하세요.

볼륨에 대한 CHAP 인증 구성

CHAP은 스토리지 볼륨 대상에 액세스하려할 때 인증을 요청함으로써 재생 공격을 방지합니다. CHAP 인증 구성 대화 상자에서 볼륨의 CHAP를 구성하는 데 필요한 정보를 입력합니다.

CHAP을 구성하려면

1. CHAP을 구성하고자 하는 볼륨을 선택합니다.
2. 작업에서 CHAP 인증 구성을 선택합니다.
3. 이니시에이터 이름에 이니시에이터 이름을 입력합니다.
4. 이니시에이터 암호에 iSCSI 이니시에이터를 인증하는 데 사용할 비밀 문구를 입력합니다.
5. 대상 암호에 상호 CHAP에 대해 대상을 인증하는 데 사용할 비밀 문구를 지정합니다.
6. 저장을 선택하여 항목을 저장합니다.

   CHAP 인증 설정에 대한 자세한 내용은 i 타겟에 대한 CHAP 인증 구성 SCSI 단원을 참조하십시오.

다음 단계

볼륨 사용

볼륨 사용

아래에서 볼륨을 사용하는 방법에 대한 지침을 얻을 수 있습니다. 볼륨을 사용하려면 먼저 클라이언트에 i SCSI 타겟으로 연결한 다음 초기화하고 포맷해야 합니다.

주제

- 볼륨을 클라이언트에 연결
- 볼륨 초기화 및 포맷
- 게이트웨이 테스트
- 추가 정보

볼륨을 클라이언트에 연결

클라이언트의 i SCSI 이니시에이터를 사용하여 볼륨에 연결합니다. 다음 절차를 마치면 볼륨을 클라이언트에서 로컬 장치로 사용할 수 있습니다.

> **Important**
>
> Storage Gateway를 사용하면 호스트가 Windows Server 페일오버 클러스터링 () WSFC 을 사용하여 액세스를 조정하는 경우 여러 호스트를 동일한 볼륨에 연결할 수 있습니다. 비클러스터형 NTFS /ext4 파일 시스템을 공유하는 WSFC 등의 방법을 사용하지 않고는 여러 호스트를 동일한 볼륨에 연결할 수 없습니다.

주제

- Microsoft Windows 클라이언트에 연결
- Red Hat Enterprise Linux 클라이언트에 연결

Microsoft Windows 클라이언트에 연결

다음 절차는 Windows 클라이언트에 연결하기 위한 단계를 요약하여 보여줍니다. 자세한 내용은 SCSI 이니시에이터 연결 단원을 참조하십시오.

Windows 클라이언트에 연결하려면

1. iscsicpl.exe를 시작합니다.

2. i SCSI 이니시에이터 속성 대화 상자에서 검색 탭을 선택한 다음 검색 포털을 선택합니다.
3. 대상 포털 검색 대화 상자에서 IP 주소 또는 DNS 이름으로 i SCSI 대상의 IP 주소를 입력합니다.
4. 새로운 대상 포털을 게이트웨이의 스토리지 볼륨 대상에 연결합니다.
5. 대상을 선택한 후 연결(Connect)을 선택합니다.
6. 대상(Targets) 탭에서 대상 상태 값이 연결되었음을 나타내는 연결됨(Connected)인지 확인한 후 확인(OK)을 선택합니다.

Red Hat Enterprise Linux 클라이언트에 연결

다음 절차는 Red Hat Enterprise Linux (RHEL) 클라이언트에 연결하기 위해 수행하는 단계를 요약한 것입니다. 자세한 내용은 SCSI이니시에이터 연결 단원을 참조하십시오.

Linux 클라이언트를 i SCSI 타겟에 연결하려면

1. iscsi-initiator-utils RPM패키지를 설치합니다.

   다음 명령을 사용하여 패키지를 설치할 수 있습니다.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. i SCSI 데몬이 실행 중인지 확인하십시오.

   RHEL5 또는 6의 경우 다음 명령을 사용하십시오.

   ```
   sudo /etc/init.d/iscsi status
   ```

   RHEL7의 경우 다음 명령을 사용합니다.

   ```
   sudo service iscsid status
   ```

3. 게이트웨이에 정의된 볼륨 또는 VTL 디바이스 타겟을 검색하십시오. 다음 검색 명령을 사용합니다.

   ```
   sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
   ```

   검색 명령은 다음 예시 출력과 비슷하게 출력됩니다.

   Volume Gateway: *[GATEWAY_IP]*:3260, 1 iqn.1997-05.com.amazon:myvolume

Tape Gateway의 경우: `iqn.1997-05.com.amazon:[GATEWAY_IP]-tapedrive-01`

4. 대상에 연결합니다.

   정확하게 지정해야 합니다.*[GATEWAY_IP]* 그리고 연결 IQN 명령에서

   다음 명령을 사용합니다.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. 볼륨이 클라이언트 시스템(초기자)에 연결되어 있는지 확인하십시오. 이렇게 하려면 다음 명령을 사용합니다.

```
ls -l /dev/disk/by-path
```

   이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

   `lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda`

   이니시에이터를 설정한 후에는 에서 Linux i 설정 사용자 지정하기 SCSI 설명한 대로 i SCSI 설정을 사용자 지정하는 것이 좋습니다.

볼륨 초기화 및 포맷

클라이언트의 i SCSI 이니시에이터를 사용하여 볼륨에 연결한 후 볼륨을 초기화하고 포맷합니다.

주제

- Microsoft Windows에서 볼륨 초기화 및 포맷
- Red Hat Enterprise Linux에서 볼륨 초기화 및 포맷

Microsoft Windows에서 볼륨 초기화 및 포맷

다음 절차를 사용하여 Windows에서 볼륨을 초기화하고 포맷할 수 있습니다.

스토리지 볼륨을 초기화 및 포맷하려면

1. **diskmgmt.msc**를 시작하여 디스크 관리 콘솔을 엽니다.

2. 디스크 초기화 대화 상자에서 볼륨을 MBR(마스터 부트 레코드) 파티션으로 초기화합니다. 파티션 스타일을 선택할 때 다음 표와 같이 연결하려는 볼륨의 유형(캐시 또는 저장)을 고려해야 합니다.

파티션 유형	다음 조건에서 사용
MBR(마스터 부트 레코드)	• 게이트웨이가 저장 볼륨이고 스토리지 볼륨의 크기가 1TiB로 제한된 경우 • 게이트웨이가 캐싱 볼륨이고 스토리지 볼륨의 크기가 2TiB 미만인 경우
GPT(GUID파티션 테이블)	게이트웨이 스토리지 볼륨의 크기가 2TiB 이상인 경우

3. 다음과 같이 단순 볼륨을 생성합니다.

   a. 볼륨을 온라인으로 전환하여 초기화합니다. 디스크 관리 콘솔에는 사용 가능한 모든 볼륨이 표시됩니다.

   b. 디스크를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 새 단순 볼륨(New Simple Volume)을 선택합니다.

   > **Important**
   >
   > 착오로 다른 디스크를 포맷하지 않도록 주의합니다. 포맷하고 있는 디스크가 게이트웨이 VM에 할당한 로컬 디스크의 크기와 일치하고 할당되지 않음(Unallocated) 상태에 있는지 확인합니다.

   c. 최대 디스크 크기를 지정합니다.

   d. 볼륨에 드라이브 문자 또는 경로를 지정하고 빠른 포맷 수행(Perform a quick format)을 선택하여 볼륨을 포맷합니다.

   > **Important**
   >
   > 캐시 볼륨에는 빠른 포맷 수행(Perform a quick format)을 사용할 것을 적극 권장합니다. 이렇게 하면 초기화 I/O가 더 적어지고 초기 스냅샷 크기가 더 작아지며 최단 시간에 사용 가능 볼륨으로 만들 수 있기 때문입니다. 또한 전체 포맷 프로세스에 대한 캐시 볼륨 공간 사용을 방지할 수 있습니다.

> **Note**
>
> 볼륨 포맷에 소요되는 시간은 볼륨 크기에 따라 다릅니다. 이 프로세스를 완료하는 데 몇 분이 걸릴 수 있습니다.

Red Hat Enterprise Linux에서 볼륨 초기화 및 포맷

다음 절차를 사용하여 Red Hat Enterprise Linux () RHEL 에서 볼륨을 초기화하고 포맷하십시오.

스토리지 볼륨을 초기화 및 포맷하려면

1. 디렉터리를 `/dev` 폴더로 변경합니다.
2. `sudo cfdisk` 명령을 실행합니다.
3. 다음 명령을 사용하여 새 볼륨을 식별합니다. 새 볼륨을 찾으려면 볼륨의 파티션 레이아웃을 나열합니다.

   ```
   $ lsblk
   ```

   파티션 처리되지 않은 새 볼륨에 대해 "인식할 수 없는 볼륨 레이블" 오류가 표시됩니다.
4. 새 볼륨을 초기화합니다. 파티션 스타일을 선택할 때는 다음 표와 같이 연결하려는 볼륨의 크기와 유형(캐시 또는 저장)을 고려해야 합니다.

파티션 유형	다음 조건에서 사용
MBR(마스터 부트 레코드)	• 게이트웨이가 저장 볼륨이고 스토리지 볼륨의 크기가 1TiB로 제한된 경우 • 게이트웨이가 캐싱 볼륨이고 스토리지 볼륨의 크기가 2TiB 미만인 경우
GPT(GUID파티션 테이블)	게이트웨이 스토리지 볼륨의 크기가 2TiB 이상인 경우

   MBR파티션의 경우 다음 명령을 사용합니다. `sudo parted /dev/`*`your volume`* `mklabel msdos`

GPT파티션의 경우 다음 명령을 사용합니다. `sudo parted /dev/your volume mklabel gpt`

5. 다음 명령을 사용하여 파티션을 생성합니다.

   ```
   sudo parted -a opt /dev/your volume mkpart primary file system 0% 100%
   ```

6. 다음 명령을 사용하여 파티션에 드라이브 문자를 지정하고 파일 시스템을 생성합니다.

   ```
   sudo mkfs -L datapartition /dev/your volume
   ```

7. 다음 명령을 사용하여 파일 시스템을 탑재합니다.

   ```
   sudo mount -o defaults /dev/your volume /mnt/your directory
   ```

게이트웨이 테스트

다음 작업을 수행하여 Volume Gateway 설정을 테스트합니다.

1. 볼륨에 데이터를 씁니다.
2. 스냅샷을 만듭니다.
3. 스냅샷을 다른 볼륨에 복원합니다.

볼륨의 스냅샷 백업을 만들고 스냅샷을 에 저장하여 게이트웨이 설정을 확인합니다 AWS. 그 다음에 스냅샷을 새 볼륨에 복원합니다. 게이트웨이는 지정된 스냅샷의 데이터를 새 AWS 볼륨에 복사합니다.

> **Note**
>
> 암호화된 Amazon Elastic 블록 스토어 (AmazonEBS) 볼륨에서 데이터를 복원하는 것은 지원되지 않습니다.

마이크로소프트 윈도우에서 스토리지 볼륨의 Amazon EBS 스냅샷을 만들려면

1. Windows 컴퓨터에서 일부 데이터를 매핑된 스토리지 볼륨으로 복사합니다.

   이 예시에서는 복사한 데이터의 양은 중요하지 않습니다. 작은 파일로도 복원 프로세스를 충분히 보여줄 수 있습니다.

2. Storage Gateway 콘솔의 탐색 창에서 볼륨을 선택합니다.

3. 게이트웨이용으로 생성한 스토리지 볼륨을 선택합니다.

   이 게이트웨이에는 스토리지 볼륨이 한 개만 있어야 합니다. 볼륨을 선택하면 속성이 표시됩니다.

4. [Actions] 에서 [EBS스냅샷 생성] 을 선택하여 볼륨의 스냅샷을 생성합니다.

   디스크의 데이터 양과 업로드 대역폭에 따라 스냅샷을 완료하는 데 몇 초가 걸릴 수 있습니다. 스냅샷을 생성한 볼륨의 볼륨 ID를 적어 둡니다. ID를 사용하여 스냅샷을 찾습니다.

5. EBS스냅샷 생성 대화 상자에서 스냅샷에 대한 설명을 입력합니다.

6. (선택 사항) 태그에 키와 값을 입력하여 태그를 스냅샷에 추가합니다. 태그는 스냅샷을 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.

7. [스냅샷 생성(Create Snapshot)]을 클릭합니다. 스냅샷은 Amazon EBS 스냅샷으로 저장됩니다. 스냅샷 ID를 기록해 둡니다. 볼륨에 생성한 스냅샷의 개수가 스냅샷 열에 표시됩니다.

8. EBS스냅샷 열에서 스냅샷을 생성한 볼륨의 링크를 선택하면 Amazon EC2 콘솔에서 EBS 스냅샷을 볼 수 있습니다.

스냅샷을 다른 볼륨에 복원하려면

볼륨 생성을 참조하세요.

추가 정보

이전 단원에서는 게이트웨이를 생성 및 프로비저닝했고 Windows 호스트를 게이트웨이 스토리지 볼륨에 연결했습니다. 게이트웨이의 i SCSI 볼륨에 데이터를 추가하고, 볼륨의 스냅샷을 만든 다음, 새 볼륨에 연결된 새 볼륨에 복원하고, 데이터가 해당 볼륨에 표시되는지 확인했습니다.

연습을 마친 후 다음 사항을 고려합니다.

- 게이트웨이를 지속적으로 사용할 계획이라면 업로드 버퍼를 실제 워크로드에 맞게 보다 적절한 크기로 조정하는 방법을 읽어 보십시오. 자세한 내용은 실제 워크로드에 맞게 게이트웨이 스토리지 크기 조정하기 단원을 참조하십시오.
- 게이트웨이를 계속 사용할 계획이 아니라면 게이트웨이를 삭제하여 요금이 부과되지 않도록 합니다. 자세한 내용은 필요 없는 리소스 정리 단원을 참조하십시오.

이 가이드의 다른 섹션에는 다음 작업을 수행하는 방법에 대한 정보가 포함되어 있습니다.

- 스토리지 볼륨과 이를 관리하는 방법에 대해 자세히 알아보려면 게이트웨이 관리 단원을 참조하십시오.

- 게이트웨이 문제를 해결하려면 게이트웨이 문제 해결 단원을 참조하십시오.
- 게이트웨이를 최적화하려면 게이트웨이 성능 최적화 단원을 참조하십시오.
- Storage Gateway 지표와 게이트웨이의 성능을 모니터링하는 방법에 대해 알아보려면 Storage Gateway 모니터링 섹션을 참조하세요.
- 데이터를 저장하도록 게이트웨이의 i SCSI 타겟을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오볼륨을 Windows 클라이언트에 연결.

실제 워크로드에 맞게 Volume Gateway의 스토리지 크기를 조정하고 필요 없는 리소스를 정리하는 방법에 대해 알아보려면 다음 섹션을 참조하세요.

실제 워크로드에 맞게 게이트웨이 스토리지 크기 조정하기

이 시점이 되면 간단한 작업 게이트웨이를 구현하게 됩니다. 그러나 이 게이트웨이를 생성할 때 가정한 사항들은 실제 워크로드에는 적절하지 않습니다. 이 게이트웨이를 실제 워크로드에 사용하려면 다음 두 작업을 해야 합니다.

1. 업로드 버퍼 크기를 적절히 조정합니다.
2. 업로드 버퍼에 대한 모니터링을 설정하지 않았다면 이를 설정합니다.

아래에서 이 두 작업을 수행하는 방법을 볼 수 있습니다. 캐싱 볼륨에 대해 게이트웨이를 활성화한 경우, 실제 워크로드에 대해서도 캐시 스토리지의 크기를 조정해야 합니다.

게이트웨이 캐싱 설정을 위한 업로드 버퍼 및 캐시 스토리지 크기 조정하기

- 업로드 버퍼의 크기를 조정하려면 할당할 업로드 버퍼의 크기 결정 단원에 있는 수식을 사용합니다. 업로드 버퍼에 최소 150GiB를 할당하도록 강력히 권장합니다. 업로드 버퍼 수식을 사용해 얻은 결과 값이 150GiB 미만인 경우, 150GiB를 할당된 업로드 버퍼로 사용합니다.

  업로드 버퍼 공식은 애플리케이션에서 게이트웨이까지의 처리량과 게이트웨이에서 전송되는 처리량 간의 차이에 데이터 쓰기 예상 시간을 곱한 값을 고려합니다. AWS예를 들어, 애플리케이션이 게이트웨이에 텍스트 데이터를 초당 40MB로 매일 12시간 작성하며 네트워크 처리량은 초당 12MB라고 가정합니다. 텍스트 데이터의 압축 요소가 2:1이라고 가정할 때 공식은 약 675GiB의 업로드 버퍼 공간을 할당할 필요가 있다고 명시합니다.

저장한 설정에 맞게 업로드 버퍼 크기를 조정하려면

- 할당할 업로드 버퍼의 크기 결정에서 논의된 공식을 사용합니다. 업로드 버퍼에 최소 150GiB를 할당하도록 강력히 권장합니다. 업로드 버퍼 수식을 사용해 얻은 결과 값이 150GiB 미만인 경우, 150GiB를 할당된 업로드 버퍼로 사용합니다.

  업로드 버퍼 공식은 애플리케이션에서 게이트웨이까지의 처리량과 게이트웨이에서 전송되는 처리량 간의 차이에 데이터 쓰기 예상 시간을 곱한 값을 고려합니다. AWS예를 들어, 애플리케이션이 게이트웨이에 텍스트 데이터를 초당 40MB로 매일 12시간 작성하며 네트워크 처리량은 초당 12MB라고 가정합니다. 텍스트 데이터의 압축 요소가 2:1이라고 가정할 때 공식은 약 675GiB의 업로드 버퍼 공간을 할당할 필요가 있다고 명시합니다.

업로드 버퍼 모니터링하기

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 게이트웨이 탭을 선택하고 세부 정보 탭을 선택한 후 Upload Buffer Used(사용된 버퍼 업로드) 필드를 찾아 게이트웨이의 현재 업로드 버퍼를 확인합니다.
3. 경보를 한 개 이상 설정하여 업로드 버퍼 사용량에 대해 알립니다.

   Amazon CloudWatch 콘솔에서 하나 이상의 업로드 버퍼 경보를 생성하는 것이 좋습니다. 예를 들어 경고를 받기 원하는 사용량 수준에 대해 경보를 설정할 수 있고, 초과 시 조치를 취하도록 하는 근거가 되는 사용량 수준에 대한 경보를 설정할 수 있습니다. 그 조치는 업로드 버퍼 공간을 추가하는 것일 수 있습니다. 자세한 내용은 게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면 단원을 참조하십시오.

필요 없는 리소스 정리

게이트웨이를 예제 또는 테스트 용도로 생성한 경우, 이를 깨끗이 정리하여 예기치 않은 또는 불필요한 요금이 발생하지 않도록 합니다.

필요 없는 리소스를 정리하려면

1. 스냅샷을 모두 삭제합니다. 지침은 스냅샷 삭제 단원을 참조하십시오.
2. 게이트웨이를 계속해서 사용할 계획이 아니라면 삭제합니다. 자세한 내용은 게이트웨이 삭제 및 관련 리소스 제거 단원을 참조하십시오.
3. 온프레미스 호스트에서 Storage Gateway VM을 삭제합니다. Amazon EC2 인스턴스에 게이트웨이를 생성한 경우 인스턴스를 종료하십시오.

볼륨 백업

Storage Gateway를 사용하면 클라우드 기반 스토리지에 Storage Gateway 볼륨을 사용하는 온프레미스 비즈니스 애플리케이션을 보호할 수 있습니다. Storage Gateway 또는 AWS Backup의 기본 스냅샷 스케줄러를 사용하여 온프레미스 Storage Gateway 볼륨을 백업할 수 있습니다. 두 경우 모두 Storage Gateway 볼륨 백업은 Amazon Web Services에 Amazon EBS 스냅샷으로 저장됩니다.

주제

- Storage Gateway를 사용하여 볼륨 백업
- 볼륨 AWS Backup 백업에 사용

Storage Gateway를 사용하여 볼륨 백업

Storage Gateway Management Console을 사용하여 Amazon EBS 스냅샷을 생성하고 Amazon Web Services에 스냅샷을 저장하여 볼륨을 백업할 수 있습니다. 일회용 스냅샷을 생성하거나 Storage Gateway에서 관리하는 스냅샷 일정을 설정할 수 있습니다. 나중에 Storage Gateway 콘솔을 사용하여 스냅샷을 새 볼륨으로 복원할 수 있습니다. Storage Gateway에서 데이터를 백업하고 백업을 관리하는 방법에 대한 자세한 내용은 다음 주제를 참조하세요.

- 게이트웨이 테스트
- 일회용 스냅샷 생성
- 볼륨 복제

볼륨 AWS Backup 백업에 사용

AWS Backup Amazon Web AWS Services Cloud와 온프레미스의 서비스 전반에 걸쳐 애플리케이션 데이터를 쉽고 비용 효율적으로 백업할 수 있는 중앙 집중식 백업 서비스입니다. 이렇게 하면 비즈니스 및 규제 백업 규정 준수 요구 사항을 충족하는 데 도움이 됩니다. AWS Backup 다음을 수행할 수 있는 중앙 위치를 제공하여 AWS 스토리지 볼륨, 데이터베이스 및 파일 시스템을 간단하게 보호할 수 있습니다.

- 백업할 AWS 리소스를 구성하고 감사하십시오.
- 백업 예약을 자동화합니다.
- 보존 정책을 설정합니다.
- 최근 백업 및 복원 활동을 모두 모니터링합니다.

Storage Gateway는 와 AWS Backup통합되므로 고객은 Storage Gateway 볼륨을 클라우드 기반 스토리지로 사용하는 온프레미스 비즈니스 애플리케이션을 백업하는 데 사용할 수 있습니다. AWS Backup AWS Backup 캐시된 볼륨과 저장된 볼륨 모두의 백업 및 복원을 지원합니다. 에 대한 AWS Backup자세한 내용은 AWS Backup 설명서를 참조하십시오. 에 대한 AWS Backup자세한 내용은 AWS Backup 무엇입니까를 참조하십시오. AWS Backup 사용 설명서에서

를 사용하여 Storage Gateway 볼륨의 백업 및 복구 작업을 관리할 수 있으므로 사용자 지정 스크립트를 생성하거나 백업을 수동으로 관리할 point-in-time 필요가 없습니다. AWS Backup 를 사용하면 AWS Backup단일 대시보드에서 클라우드 내 AWS 리소스와 함께 온프레미스 볼륨 백업을 모니터링할 수도 있습니다. AWS Backup 를 AWS Backup 사용하여 일회성 온디맨드 백업을 생성하거나 에서 관리되는 백업 계획을 정의할 수 있습니다. AWS Backup

에서 가져온 Storage Gateway 볼륨 AWS Backup 백업은 Amazon S3에 Amazon EBS 스냅샷으로 저장됩니다. AWS Backup 콘솔 또는 Amazon EBS 콘솔에서 Storage Gateway 볼륨 백업을 볼 수 있습니다.

모든 온프레미스 게이트웨이 또는 클라우드 내 게이트웨이를 통해 관리되는 Storage Gateway 볼륨을 쉽게 AWS Backup 복원할 수 있습니다. 이러한 볼륨을 Amazon EC2 인스턴스와 함께 사용할 수 있는 Amazon EBS 볼륨으로 복원할 수도 있습니다.

Storage Gateway 볼륨 AWS Backup 백업에 사용할 때의 이점

Storage Gateway 볼륨을 AWS Backup 백업하는 데 사용할 때의 이점은 규정 준수 요구 사항을 충족하고 운영 부담을 없애고 백업 관리를 중앙 집중화할 수 있다는 것입니다. AWS Backup 다음을 수행할 수 있습니다.

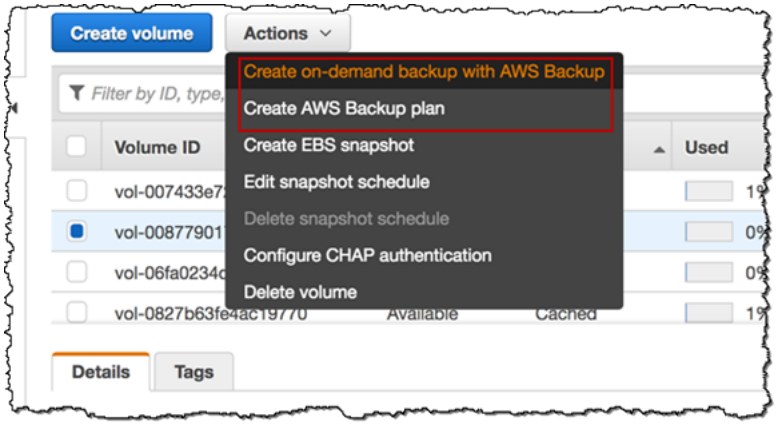
- 백업 요구 사항을 따를 수 있는 사용자 지정 일정 백업 정책을 지정합니다.
- 더 이상 사용자 지정 스크립트를 개발하거나 볼륨 point-in-time 백업을 수동으로 관리할 필요가 없도록 백업 보존 및 만료 규칙을 설정합니다.
- 여러 게이트웨이의 백업과 기타 AWS 리소스를 중앙에서 관리하고 모니터링할 수 있습니다.

볼륨 백업을 생성하는 AWS Backup 데 사용합니다.

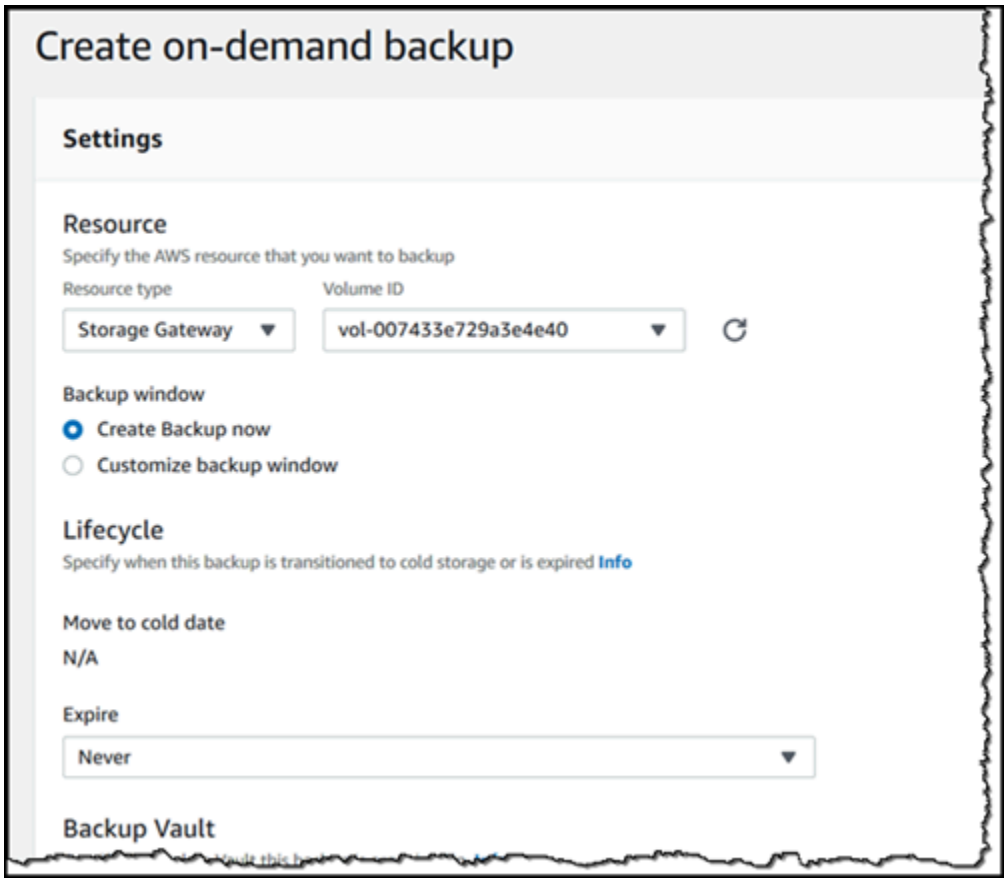
> **Note**
>
> AWS Backup AWS Backup 소비하는 AWS Identity and Access Management (IAM) 역할을 선택해야 합니다. 이 역할은 자동으로 AWS Backup 생성되지 않으므로 직접 생성해야 합니다. 또한 이 IAM 역할 간에 AWS Backup 신뢰 관계를 생성해야 합니다. 이 작업을 실행하는 방법은

AWS Backup 사용 설명서를 참조하세요. 이 작업을 실행하는 방법은AWS Backup 사용 설명서에서 백업 계획 생성을 참조하세요.

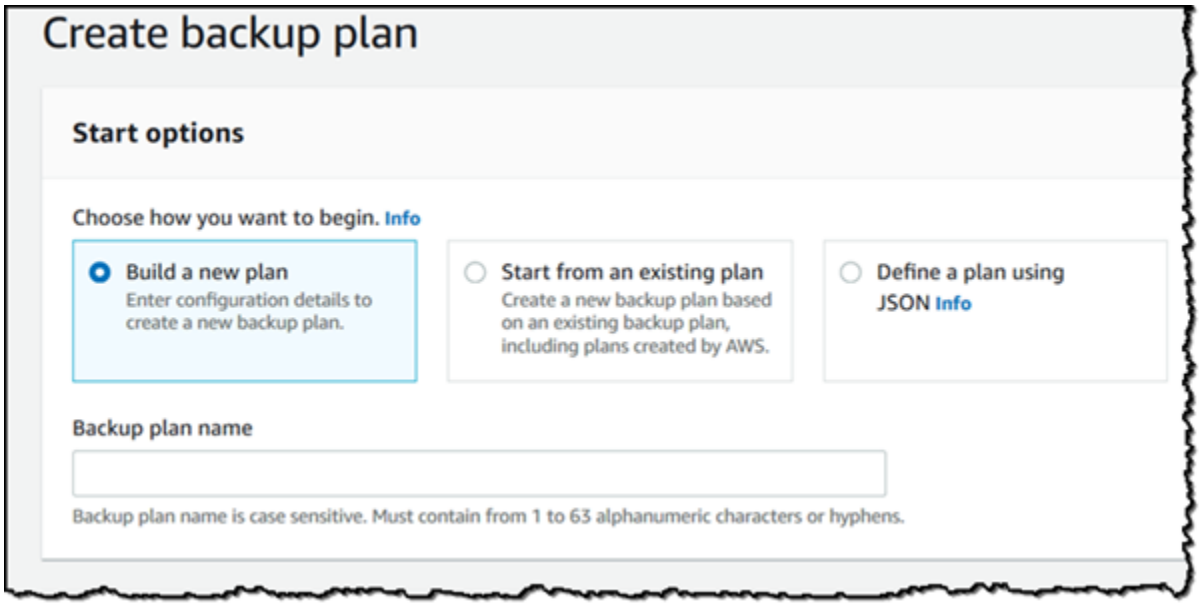
1. Storage Gateway 콘솔을 열고 왼쪽 탐색 창에서 볼륨을 선택합니다.
2. Actions에서 온디맨드 백업 생성 AWS Backup 또는 AWS 백업 계획 생성을 선택합니다.



Storage Gateway 볼륨의 온디맨드 백업을 생성하려면 다음을 사용하여 온디맨드 백업 생성을 선택합니다. AWS Backup콘솔로 이동합니다. AWS Backup



새 AWS Backup 계획을 만들려면 AWS 백업 계획 생성을 선택합니다. AWS Backup 콘솔로 이동합니다.



AWS Backup 콘솔에서 백업 계획을 생성하고, Storage Gateway 볼륨을 백업 계획에 할당하고, 백업을 생성할 수 있습니다. 지속적으로 백업 관리 작업을 수행할 수도 있습니다.

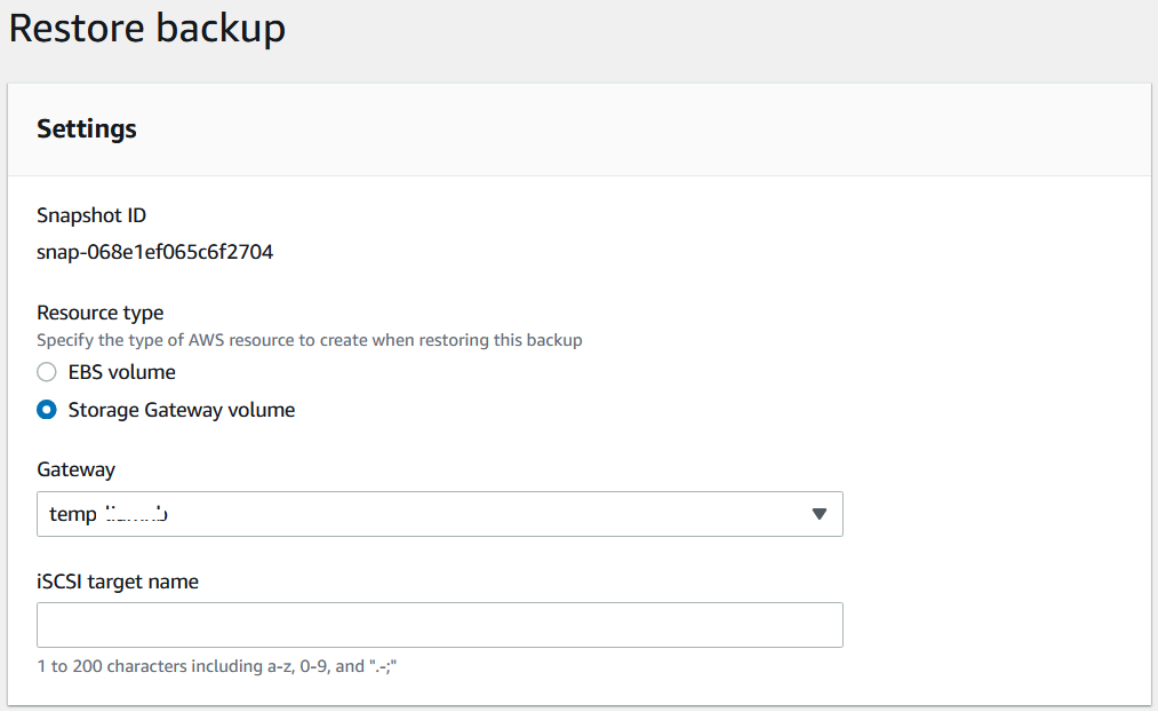
AWS Backup에서 볼륨 검색 및 복원

AWS Backup 콘솔에서 백업 Storage Gateway 볼륨을 찾아 복원할 수 있습니다. 자세한 내용은 AWS Backup 사용 설명서를 참조하십시오. 자세한 내용은AWS Backup 사용 설명서에서 복구 지점을 참조하세요.

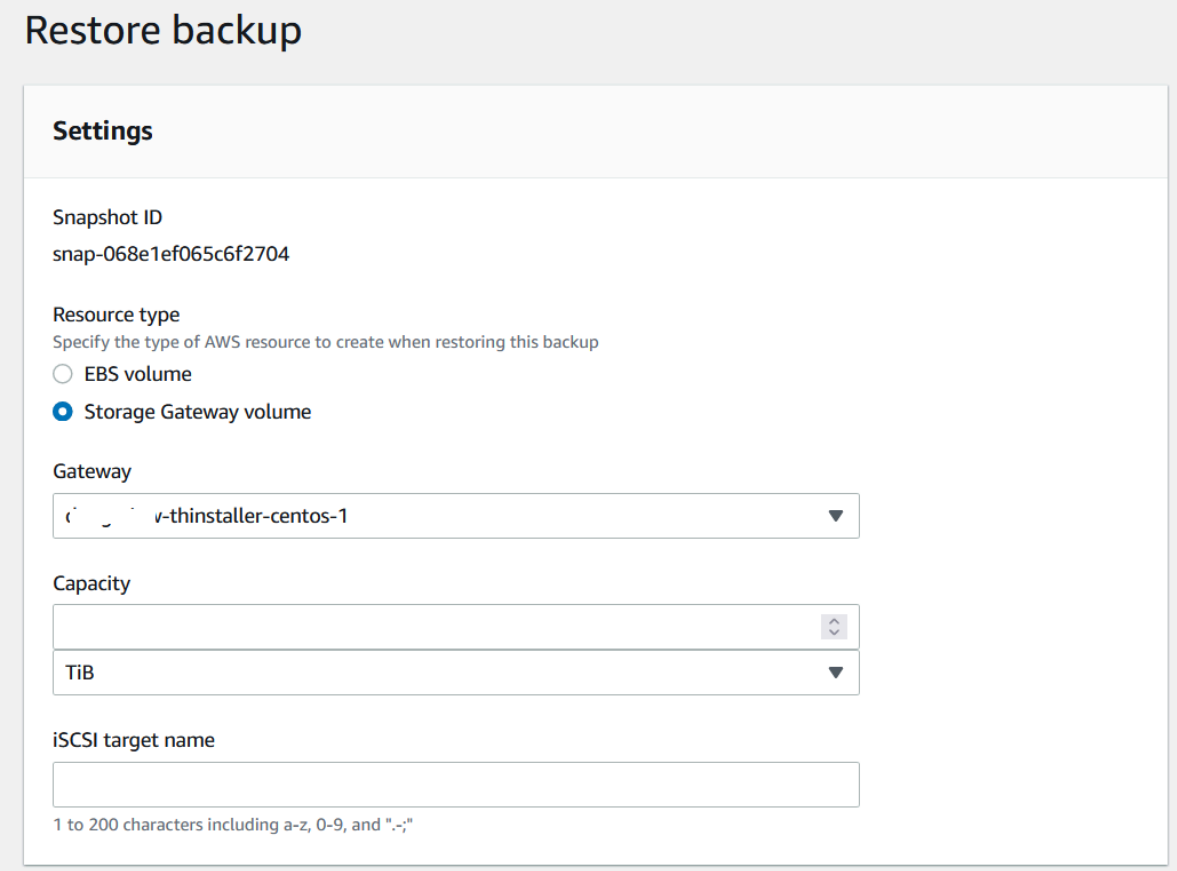
볼륨 검색 및 복원

1. AWS Backup 콘솔을 열고 복원할 Storage Gateway 볼륨 백업을 찾습니다. Storage Gateway 볼륨 백업은 Amazon EBS 볼륨 또는 Storage Gateway 볼륨으로 복원할 수 있습니다. 복원 요구 사항에 적합한 옵션을 선택합니다.
2. 복원 유형에서 복구할 저장 또는 캐시 Storage Gateway 볼륨을 선택하고 필요한 정보를 입력합니다.

   - 저장 볼륨의 경우 게이트웨이 이름, 디스크 ID(Disk ID), iSCSI 대상 이름을 입력합니다.



- 캐시 볼륨의 경우 게이트웨이 이름, 용량, iSCSI 대상 이름을 입력합니다.



3. 볼륨을 복원하려면 리소스 복원(Restore resource)을 선택합니다.

> **Note**
>
> 에서 생성한 AWS Backup스냅샷은 Amazon EBS 콘솔을 사용하여 삭제할 수 없습니다.

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 공용 인터넷을 통해 통신하지 않고도 AWS 스토리지 서비스에 데이터를 전송하도록 허용할 수 있습니다. Amazon VPC 서비스를 사용하면 사용자 지정 가상 사설 클라우드 (VPC) 에서 사설 네트워크 인터페이스 엔드포인트를 비롯한 AWS 리소스를 시작할 수 있습니다. A를 VPC 사용하면 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이와 같은 네트워크 설정을 제어할 수 있습니다. 에 대한 VPCs 자세한 내용은 Amazon이란 무엇입니까 VPC? 를 참조하십시오. Amazon VPC 사용 설명서에서 확인할 수 있습니다.

에서 게이트웨이를 활성화하려면 Amazon VPC Console을 사용하여 Storage Gateway용 VPC 엔드포인트를 생성하고 VPC 엔드포인트 ID를 가져온 다음, 게이트웨이를 생성하고 활성화할 때 이 VPC 엔드포인트 ID를 지정하십시오. VPC 자세한 내용은 볼륨 연결을 참조하십시오 AWS.

> **Note**
>
> Storage Gateway의 VPC 엔드포인트를 생성한 지역과 동일한 지역에서 게이트웨이를 활성화해야 합니다.

주제

- Storage Gateway용 VPC 엔드포인트 생성

Storage Gateway용 VPC 엔드포인트 생성

다음 지침에 따라 VPC 엔드포인트를 생성하십시오. Storage Gateway용 VPC 엔드포인트가 이미 있는 경우 이를 사용하여 게이트웨이를 활성화할 수 있습니다.

Storage Gateway의 VPC 엔드포인트를 생성하려면

1. 에서 Amazon VPC 콘솔에 AWS Management Console 로그인하고 엽니다 https://console.aws.amazon.com/vpc/.

2. 탐색 창에서 엔드포인트를 선택하고 엔드포인트 생성을 선택합니다.
3. 엔드포인트 생성 페이지에서 AWS 서비스를 서비스 범주로 선택합니다.
4. 서비스 이름에서 com.amazonaws.*region*.storagegateway를 선택합니다. 예: com.amazonaws.us-east-2.storagegateway.
5. 에서 원하는 가용 VPC영역을 선택하고 해당 가용 VPC 영역과 서브넷을 기록해 두십시오.
6. 프라이빗 DNS 네임 활성화가 선택되지 않았는지 확인하십시오.
7. 보안 그룹에서 사용할 보안 그룹을 선택합니다VPC. 기본 보안 그룹을 적용할 수 있습니다. 보안 그룹에 다음 TCP 포트가 모두 허용되는지 확인하십시오.

   - TCP443
   - TCP1026
   - TCP1027
   - TCP1028
   - TCP1031
   - TCP2222

8. Create endpoint(엔드포인트 생성)을 선택합니다. 엔드포인트의 초기 상태는 대기 중입니다. 엔드포인트가 생성되면 방금 생성한 VPC 엔드포인트의 ID를 기록해 둡니다.
9. 엔드포인트가 생성되면 엔드포인트를 선택한 다음 새 VPC 엔드포인트를 선택합니다.
10. 선택한 스토리지 게이트웨이 엔드포인트의 세부 정보 탭의 DNS이름에서 가용 영역을 지정하지 않은 첫 번째 DNS 이름을 사용합니다. DNS이름은 다음과 비슷합니다. vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

이제 VPC 엔드포인트가 생겼으니 게이트웨이를 만들 수 있습니다. 자세한 내용은 게이트웨이 생성을 참조하세요.

게이트웨이 관리

게이트웨이 관리에는 캐시 스토리지 및 업로드 버퍼 공간 구성, 볼륨 또는 가상 테이프 작업, 일반 유지 관리 수행 등과 같은 작업이 포함됩니다. 게이트웨이를 생성하지 않았으면 시작하기 AWS Storage Gateway 단원을 참조하십시오.

게이트웨이 소프트웨어 릴리스에는 검증된 OS 업데이트 및 보안 패치가 주기적으로 포함됩니다. 이러한 업데이트는 예정된 유지 관리 기간 동안 정기 게이트웨이 업데이트 프로세스의 일부로 적용되며, 일반적으로 6개월마다 릴리스됩니다. 참고: 사용자는 Storage Gateway 어플라이언스를 관리형 가상 머신으로 취급해야 하며 Storage Gateway 어플라이언스 인스턴스에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 게이트웨이 업데이트 메커니즘 이외의 다른 방법 (예: SSM 또는 하이퍼바이저 도구) 을 사용하여 소프트웨어 패키지를 설치하거나 업데이트하려고 하면 게이트웨이가 제대로 작동하지 않을 수 있습니다.

주제

- 볼륨 게이트웨이 관리
- 데이터를 새 게이트웨이로 이동

볼륨 게이트웨이 관리

다음은 Volume Gateway 리소스를 관리하는 방법에 대한 자세한 내용입니다.

캐싱 볼륨은 애플리케이션 데이터를 저장할 수 있는 SCSI i 타겟으로 노출되는 Amazon Simple Storage Service (Amazon S3) 의 볼륨입니다. 캐싱된 설정에 대한 볼륨을 추가 및 삭제하는 자세한 방법을 확인할 수 있습니다. Amazon EC2 게이트웨이에서 Amazon 엘라스틱 블록 스토어 (AmazonEBS) 볼륨을 추가하고 제거하는 방법도 배울 수 있습니다.

주제

- 기본 게이트웨이 정보 편집
- 볼륨 추가
- 볼륨 크기 확장
- 볼륨 복제
- 볼륨 사용량 보기
- 볼륨에서 청구 대상 스토리지의 양 줄이기
- 볼륨 삭제

- 볼륨을 다른 게이트웨이로 이동
- 일회용 스냅샷 생성
- 스냅샷 일정 편집
- 스냅샷 삭제
- 볼륨 상태 및 전환 이해

> **Important**
>
> 캐시 볼륨이 Amazon S3에 기본 데이터를 유지하는 경우, 전체 볼륨에 모든 데이터를 읽거나 쓰는 프로세스를 방지해야 합니다. 예를 들어 캐싱 볼륨 전체를 스캔하는 바이러스 검사 소프트웨어는 사용하지 않는 것이 좋습니다. 그러한 스캔 작업은 필요에 따른 것이든 일정에 따른 것이든 간에 스캔을 위해 Amazon S3에 저장된 모든 데이터를 로컬로 다운로드하기 때문에 대역폭 사용량이 크게 늘어납니다. 전체 디스크 검사를 수행하는 대신 실시간 바이러스 검사, 즉 캐시 볼륨에서 데이터를 읽거나 캐시 볼륨에 쓸 때 데이터를 검사하는 방법을 사용할 수 있습니다.

볼륨 크기 조정은 지원하지 않습니다. 볼륨 크기를 변경하려면 볼륨의 스냅샷을 생성한 후 스냅샷에서 캐싱 볼륨을 새로 생성합니다. 새 볼륨은 스냅샷에서 생성했던 볼륨보다 더 클 수 있습니다. 볼륨 제거 절차에 대해서는 볼륨을 삭제하려면 단원을 참조하십시오. 볼륨 추가 및 기존 데이터 보존 절차에 대해서는 볼륨 삭제 단원을 참조하십시오.

캐시된 모든 볼륨 데이터와 스냅샷 데이터는 Amazon S3에 저장되며 서버 측 암호화 () 를 사용하여 저장 시 암호화됩니다. SSE 하지만 Amazon S3 API 또는 Amazon S3 관리 콘솔과 같은 다른 도구를 사용하여 이 데이터에 액세스할 수는 없습니다.

기본 게이트웨이 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. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 게이트웨이를 선택한 다음 기본 정보를 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 게이트웨이 정보 편집을 선택합니다.

4. 변경할 설정을 선택한 다음 변경 사항 저장을 선택합니다.

> **Note**
>
> 게이트웨이 이름을 변경하면 게이트웨이를 모니터링하도록 설정된 모든 CloudWatch 경보 연결이 끊어집니다. 경보를 다시 연결하려면 콘솔에서 각 경보에 GatewayName대해를 업데이트하십시오. CloudWatch

볼륨 추가

애플리케이션 요구 사항이 늘어남에 따라 게이트웨이에 볼륨을 추가해야 할 경우가 있을 수 있습니다. 볼륨을 추가할 때 게이트웨이에 할당한 캐시 스토리지 및 업로드 버퍼의 크기를 고려해야 합니다. 게이트웨이에 새 볼륨을 추가하기에 충분한 버퍼 및 캐시 공간이 있어야 합니다. 자세한 설명은 할당할 업로드 버퍼의 크기 결정 섹션을 참조하세요.

Storage Gateway 콘솔 또는 Storage Gateway API를 사용하여 볼륨을 추가할 수 있습니다. Storage Gateway API를 사용하여 볼륨을 추가하는 방법에 대한 자세한 내용은 CreateCachediSCSIVolume을 참조하십시오. Storage Gateway 콘솔을 사용하여 볼륨을 추가하는 방법에 대한 지침은 볼륨 생성 섹션을 참조하세요.

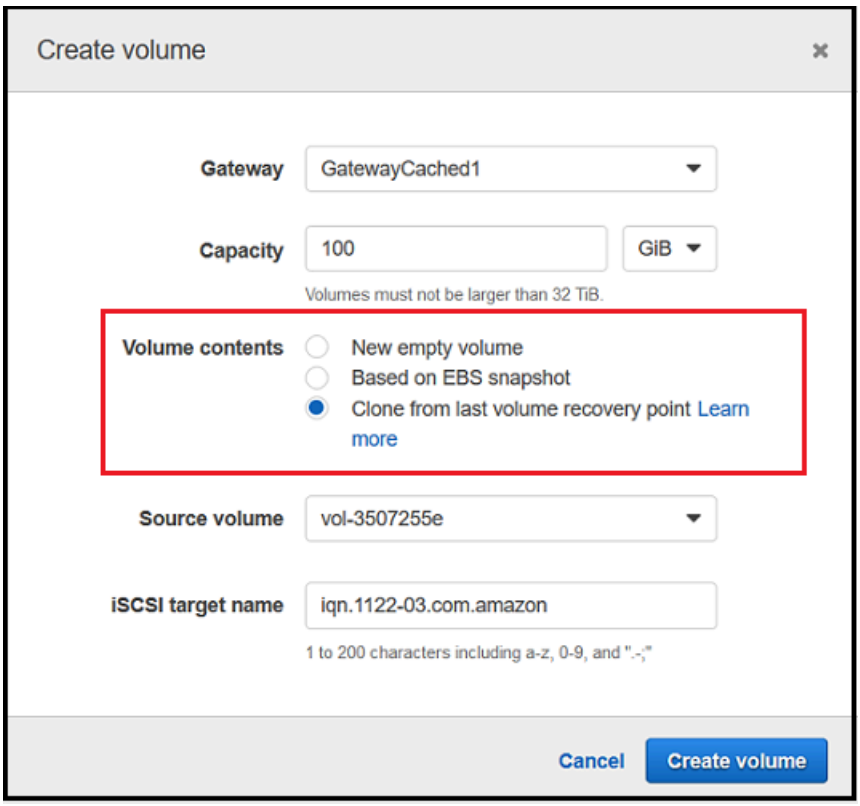
볼륨 크기 확장

애플리케이션 요구 사항이 늘어남에 따라 게이트웨이에 볼륨을 추가하는 대신 볼륨을 확장하기를 원할 수 있습니다. 이런 경우 다음 중 한 가지를 수행할 수 있습니다.

- 확장하려는 볼륨의 스냅샷을 생성한 후 그 스냅샷을 사용하여 더 큰 볼륨을 새로 생성합니다. 스냅샷을 생성하는 방법에 대한 자세한 내용은 일회용 스냅샷 생성 단원을 참조하십시오. 스냅샷을 사용하여 새 볼륨을 생성하는 방법에 대한 자세한 내용은 볼륨 생성 단원을 참조하십시오.
- 확장하려는 캐싱 볼륨을 사용하여 더 큰 새 볼륨을 복제합니다. 볼륨 복제에 대한 자세한 내용은 볼륨 복제 단원을 참조하십시오. 볼륨 생성에 대한 자세한 내용은 볼륨 생성 단원을 참조하십시오.

볼륨 복제

동일한 AWS 지역의 기존 캐시 볼륨에서 새 볼륨을 생성할 수 있습니다. 새 볼륨은 선택한 볼륨의 가장 최근 복구 시점에서 생성됩니다. 볼륨 복구 시점은 모든 데이터가 일관된 시점입니다. 볼륨을 복제하려면 볼륨 생성 대화 상자에서 마지막 복구 지점에서 복제 옵션을 선택한 다음 소스로 사용할 볼륨을 선택합니다. 다음 스크린샷은 Change volume(볼륨 변경) 대화 상자입니다.



기존 볼륨에서 복제하는 것이 Amazon EBS 스냅샷을 생성하는 것보다 더 빠르고 비용 효율적입니다. 복제는 원본 볼륨의 가장 최근 복구 지점을 사용하여 원본 볼륨에서 새 볼륨으로 데이터를 byte-to-byte 복사합니다. Storage Gateway는 캐시 볼륨의 복구 지점을 자동으로 생성합니다. 마지막 복구 지점이 언제 생성되었는지 확인하려면 Amazon에서 `TimeSinceLastRecoveryPoint` 메트릭을 확인하십시오 CloudWatch.

복제된 볼륨은 소스 볼륨과 독립적입니다. 즉, 복제 후 어느 한 볼륨을 변경해도 다른 볼륨에는 영향을 주지 않습니다. 예를 들어 소스 볼륨을 삭제한 경우 복제된 볼륨은 영향을 받지 않습니다. 초기자가 연결되고 활성 상태일 동안 소스 볼륨을 복제할 수 있습니다. 이렇게 하더라도 소스 볼륨의 성능에는 영향을 미치지 않습니다. 볼륨 복제에 대한 자세한 내용은 볼륨 생성 단원을 참조하십시오.

복구 시나리오에서도 복제 프로세스를 사용할 수 있습니다. 자세한 설명은 캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우 섹션을 참조하세요.

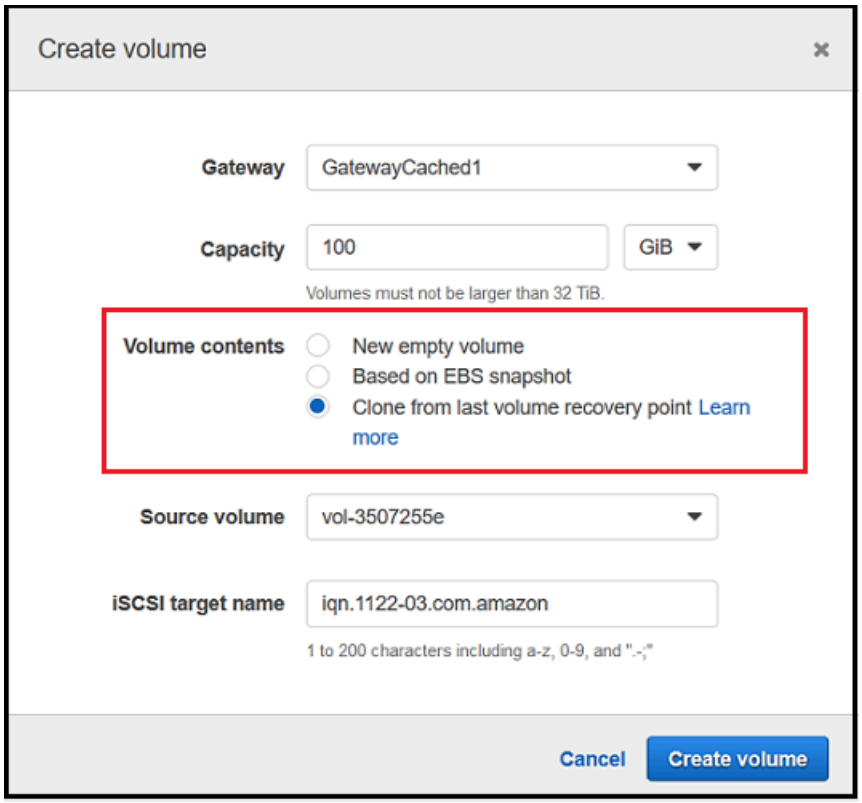
볼륨 복구 시점에서 복제

다음 절차는 볼륨 복구 시점에서 볼륨을 복제하는 방법과 해당 볼륨의 사용 방법을 보여줍니다.

접속 불가능한 게이트웨이로부터 볼륨을 복제하여 사용하려면

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

2. Storage Gateway 콘솔에서 볼륨 생성을 선택합니다.
3. 볼륨 생성 대화 상자의 게이트웨이에서 게이트웨이를 선택합니다.
4. 용량에 볼륨의 용량을 입력하십시오. 이 용량은 소스 볼륨과 같거나 커야 합니다.
5. Clone from last recovery point(마지막 복구 시점에서 복제)를 선택하고 소스 볼륨에서 볼륨 ID를 선택합니다. 소스 볼륨은 선택한 AWS 지역의 모든 캐시된 볼륨일 수 있습니다.



6. iSCSI 대상 이름에 이름을 입력합니다.

   대상 이름은 소문자, 숫자, 마침표(.), 하이픈(-)을 포함할 수 있습니다. 이 대상 이름은 검색 후 iSCSI Microsoft 이니시에이터 UI의 대상 탭에 iSCSI 대상 노드 이름으로 나타납니다. 예를 들어 `target1`이라는 이름은 `iqn.1007-05.com.amazon:target1`으로 표시됩니다. 대상 이름이 스토리지 영역 네트워크(SAN) 내에서 전역적으로 고유한지 확인합니다.

7. 네트워크 인터페이스 설정이 게이트웨이의 IP 주소인지 확인하여 아닐 경우 네트워크 인터페이스에서 IP 주소를 선택합니다.

   여러 네트워크 어댑터를 사용하도록 게이트웨이를 정의한 경우 스토리지 애플리케이션에서 볼륨에 액세스하는 데 사용하는 IP 주소를 선택합니다. 게이트웨이에 정의된 각 네트워크 어댑터는 선택할 수 있는 IP 주소 한 개를 나타냅니다.

게이트웨이 VM이 두 개 이상의 네트워크 어댑터에 대해 구성된 경우 볼륨 생성 대화 상자에 네트워크 인터페이스 목록이 표시됩니다. 이 목록에서 게이트웨이 VM에 대해 구성된 각 어댑터의 IP 주소 하나가 표시됩니다. 게이트웨이 VM이 하나의 네트워크 어댑터에 대해서만 구성된 경우 IP 주소가 하나 뿐이기 때문에 목록이 나타나지 않습니다.

8. 볼륨 생성을 선택합니다. 그러면 CHAP 인증 구성 대화 상자가 나타납니다. 나중에 CHAP를 구성할 수 있습니다. 자세한 내용은 i 타겟에 대한 CHAP 인증 구성 SCSI 섹션을 참조하세요.

다음 단계는 볼륨을 클라이언트에 연결하는 것입니다. 자세한 설명은 볼륨을 클라이언트에 연결 섹션을 참조하세요.

복구 스냅샷 생성

다음 절차는 볼륨 복구 시점에서 스냅샷을 생성하여 그 스냅샷을 사용하는 방법을 보여줍니다. 필요에 따라 일회용 스냅샷을 만들거나 해당 볼륨에 대한 스냅샷 일정을 설정할 수 있습니다.

접속할 수 없는 게이트웨이에서 볼륨의 복구 스냅샷을 생성하여 사용하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택합니다.
3. 접속할 수 없는 게이트웨이를 선택한 후 세부 정보 탭을 선택합니다.

   복구 스냅샷 메시지가 탭에 표시됩니다.

4. 복구 스냅샷 생성을 선택하여 복구 스냅샷 생성 대화 상자를 엽니다.
5. 표시된 볼륨 목록에서 복구할 볼륨을 선택한 후 스냅샷 생성을 선택합니다.

   Storage Gateway에서 스냅샷 프로세스를 시작합니다.
6. 스냅샷을 찾아서 복구합니다.

볼륨 사용량 보기

볼륨에 데이터를 쓸 때 Storage Gateway Management Console에서 볼륨에 저장된 데이터 양을 볼 수 있습니다. 각 볼륨의 세부 정보 탭에 볼륨 사용량 정보가 표시됩니다.

볼륨에 기록된 데이터 양을 보려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 볼륨을 선택한 다음, 관심 있는 볼륨을 선택합니다.
3. 세부 정보 탭을 선택하십시오.

   다음 필드에 볼륨에 대한 정보가 표시됩니다.

   - 크기: 선택한 볼륨의 전체 용량입니다.
   - 사용됨: 볼륨에 저장된 데이터의 크기입니다.

   > **Note**
   >
   > 볼륨에 데이터를 저장할 때까지 2015년 5월 13일 이전에 생성된 볼륨에는 이러한 값을 사용할 수 없습니다.

볼륨에서 청구 대상 스토리지의 양 줄이기

파일 시스템에서 파일을 삭제해도 반드시 기본 블록 디바이스에서 데이터가 삭제되거나 볼륨에 저장된 데이터 양이 줄어드는 것은 아닙니다. 볼륨에서 청구 대상 스토리지의 양을 줄이려면 파일을 0으로 덮어써 스토리지를 실제 스토리지의 매우 미미한 양으로 압축하는 것이 좋습니다. Storage Gateway는 압축된 스토리지를 기준으로 볼륨 사용량에 대해 요금을 부과합니다.

> **Note**
>
> 난수 데이터로 볼륨의 데이터를 덮어쓰는 삭제 도구를 사용하는 경우에는 사용량이 줄지 않습니다. 이는 난수 데이터는 압축할 수 없기 때문입니다.

볼륨 삭제

예를 들어, 더 큰 스토리지 볼륨을 사용하기 위해 애플리케이션을 마이그레이션하는 경우와 같이 애플리케이션에 변경이 필요하면 볼륨을 삭제해야 할 수 있습니다. 볼륨을 삭제하기 전에 현재 볼륨에 쓰기

작업을 하는 애플리케이션이 없는지 확인합니다. 또한 볼륨에 대해 진행 중인 스냅샷이 없는지도 확인합니다. 볼륨에 대해 스냅샷 일정이 정의되어 있는 경우 Storage Gateway 콘솔의 스냅샷 일정 탭에서 확인할 수 있습니다. 자세한 내용은 스냅샷 일정 편집 단원을 참조하십시오.

Storage Gateway 콘솔 또는 Storage Gateway를 사용하여 볼륨을 삭제할 수 API 있습니다. Storage Gateway를 사용하여 볼륨을 제거하는 API 방법에 대한 자세한 내용은 볼륨 삭제를 참조하십시오. 다음은 콘솔 사용 절차입니다.

볼륨을 삭제하기 전에 데이터를 백업하거나 중요한 데이터의 스냅샷을 생성합니다. 저장된 볼륨의 경우 로컬 디스크를 지워지지 않습니다. 볼륨을 삭제한 후에는 다시 되돌릴 수 없습니다.

볼륨을 삭제하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 볼륨을 선택한 다음 삭제할 볼륨을 하나 이상 선택합니다.
3. 작업에서 볼륨 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.
4. 지정된 볼륨을 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

볼륨을 다른 게이트웨이로 이동

데이터 및 성능 요구 사항이 증가함에 따라 볼륨을 다른 Volume Gateway로 이동하고 싶을 수 있습니다. 이 작업을 위해 Storage Gateway 콘솔 또는 API를 사용해 볼륨을 연결하거나 분리할 수 있습니다.

볼륨 이동 및 연결을 통해 다음이 가능합니다.

- 볼륨을 더 나은 호스트 플랫폼 또는 신규 Amazon EC2 인스턴스로 이동합니다.
- 서버의 기본 하드웨어를 새로 고침합니다.
- 하이퍼바이저 유형 간 볼륨을 이동합니다.

볼륨을 분리하면 게이트웨이는 볼륨 데이터 및 메타데이터를 AWS의 Storage Gateway 서비스에 업로드하고 저장합니다. 분리된 볼륨은 이후 지원되는 모든 호스트 플랫폼의 게이트웨이에 쉽게 연결할 수 있습니다.

> **Note**
>
> 분리된 볼륨을 삭제하기 전까지 스탠다드 볼륨 스토리지 요금이 부과됩니다. 요금을 줄이는 방법에 대한 자세한 내용은 볼륨에서 청구 대상 스토리지의 양 줄이기을 참조하십시오.

> **Note**
>
> 볼륨 연결 및 분리 시 몇 가지 제약이 있습니다.
>
> - 볼륨을 분리하는 데 오랜 시간이 걸릴 수 있습니다. 볼륨을 분리하면 게이트웨이는 볼륨이 분리되기 AWS 전에 볼륨의 모든 데이터를 업로드합니다. 업로드가 완료되는 데 걸리는 시간은 AWS에 업로드해야 할 데이터의 양과 네트워크 연결에 따라 달라집니다.
> - 캐시 볼륨을 분리할 경우 저장 볼륨으로 다시 연결할 수 없습니다.
> - 저장 볼륨을 분리할 경우 캐시 볼륨으로 다시 연결할 수 없습니다.
> - 분리된 볼륨은 게이트웨이에 연결될 때까지 사용할 수 없습니다.
> - 저장 볼륨을 연결하는 경우 게이트웨이에 연결하기 위해서는 사전에 복원이 완료되어야 합니다.
> - 볼륨 연결 또는 분리를 시작하면 작업이 끝날 때까지 해당 볼륨을 사용할 수 없습니다.
> - 현재 강제 볼륨 삭제는 API에서만 지원합니다.
> - 게이트웨이에서 볼륨을 분리하던 중 게이트웨이를 삭제하면 데이터 손실이 발생합니다. 게이트웨이를 삭제하시려면 볼륨 분리 작업이 완료될 때까지 기다리십시오.
> - 저장된 게이트웨이가 복원 중인 경우 해당 게이트웨이에서는 볼륨을 분리할 수 없습니다.

다음 단계는 Storage Gateway 콘솔을 사용하여 볼륨을 분리 및 연결하는 방법을 설명합니다. API를 사용하여 이 작업을 수행하는 방법에 대한 자세한 내용은 API AttachVolume참조의 DetachVolumeAWS Storage Gateway 또는 항목을 참조하십시오.

게이트웨이에서 볼륨을 분리하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 볼륨을 선택한 다음 분리할 볼륨을 하나 이상 선택합니다.
3. 작업(Actions)에서 볼륨 분리(Detach Volume)를 선택합니다. 확인 대화 상자가 표시됩니다.
4. 지정된 볼륨을 분리할 것인지 확인한 다음 확인 상자에 detach라는 단어를 입력하고 분리를 선택합니다.

> **Note**
>
> 분리하는 볼륨에 데이터가 많은 경우 모든 데이터의 업로드가 종료될 때까지 연결됨에서 분리 중으로 상태가 전환됩니다. 이후 상태가 분리 완료로 전환됩니다. 데이터의 양이 적은 경우 분리 중 상태가 표시되지 않을 수 있습니다. 볼륨에 데이터가 없는 경우 상태는 연결됨에서 분리 완료로 전환됩니다.

이제 해당 볼륨을 다른 게이트웨이에 연결할 수 있습니다.

게이트웨이에 볼륨을 연결하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 볼륨을 선택합니다. 분리된 각 볼륨의 상태가 분리됨으로 표시됩니다.
3. 분리된 볼륨 목록에서 연결할 볼륨을 선택합니다. 한 번에 하나의 볼륨만 연결할 수 있습니다.
4. 작업(Actions)에서, 볼륨 연결(Attach Volume)을 선택합니다.
5. 볼륨 연결(Attach Volume) 대화 상자에서 볼륨을 연결할 게이트웨이를 선택하고 볼륨을 연결할 iSCSI 대상을 입력하십시오.

   저장 볼륨을 연결하려는 경우 디스크 ID(Disk ID)에 디스크 식별자를 입력하십시오.
6. 볼륨 연결(Attach Volume)을 선택합니다. 첨부하는 볼륨에 많은 데이터가 있는 경우, `AttachVolume` 작업이 성공하면 해당 볼륨은 분리됨에서 연결됨으로 전환됩니다.
7. CHAP 인증 구성 마법사가 나타나면 이니시에이터 이름, 이니시에이터 암호 및 대상 암호를 각각의 상자에 입력하고 저장을 선택합니다. CHAP(Challenge-Handshake Authentification Protocol) 인증을 사용하는 방법에 대한 자세한 내용은 i 타겟에 대한 CHAP 인증 구성 SCSI를 참조하십시오.

일회용 스냅샷 생성

Volume Gateway에 대해 예정된 스냅샷 이외에 일회성 임시 스냅샷을 생성할 수 있습니다. 이를 통해 다음 예약 스냅샷을 기다릴 필요 없이 바로 스토리지 볼륨을 백업할 수 있습니다.

스토리지 볼륨의 일회용 스냅샷을 생성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 볼륨을 선택하고 스냅샷을 생성할 볼륨을 선택합니다.

3. 작업(Actions)에서 스냅샷 생성(Create snapshot)을 선택합니다.
4. 스냅샷 생성 대화 상자에 스냅샷 설명을 입력하고 스냅샷 생성을 선택합니다.

   콘솔을 사용하여 스냅샷이 생성되었는지 확인할 수 있습니다.

생성된 스냅샷은 볼륨과 같은 행에 있는 스냅샷에 표시됩니다.

스냅샷 일정 편집

저장된 볼륨의 경우 하루에 한 번씩의 기본 스냅샷 일정을 AWS Storage Gateway 생성합니다.

> **Note**
>
> 기본 스냅샷 일정은 제거할 수 없습니다. 저장 볼륨은 하나 이상의 스냅샷 일정이 필요합니다. 그러나 매일 스냅샷이 생성되는 시간, 빈도(1, 2, 4, 8, 12 또는 24시간마다) 또는 둘 다를 지정하여 스냅샷 일정을 변경할 수 있습니다.

캐시된 볼륨의 경우 기본 스냅샷 일정을 만들지 AWS Storage Gateway 않습니다. 데이터가 Amazon S3에 저장되므로 기본 일정이 생성되지 않습니다. 따라서 재해 복구를 위한 스냅샷 또는 스냅샷 일정이 필요하지 않습니다. 그러나 필요하다면 언제든지 스냅샷 일정을 설정할 수 있습니다. 캐싱 볼륨에 대해 스냅샷을 생성하면 필요할 경우 데이터를 복구할 수 있는 추가적인 방법이 확보됩니다.

다음 절차를 통해 볼륨의 스냅샷 일정을 편집할 수 있습니다.

볼륨의 스냅샷 일정을 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 볼륨을 선택하고 스냅샷을 생성한 볼륨을 선택합니다.
3. 작업에서 스냅샷 일정 편집을 선택합니다.
4. 스냅샷 일정 편집 대화 상자에서 일정을 수정한 후 저장을 선택합니다.

스냅샷 삭제

스토리지 볼륨의 스냅샷을 삭제할 수 있습니다. 예를 들어, 시간이 지남에 따라 많은 수의 스토리지 볼륨 스냅샷이 생성되어 이전 스냅샷이 필요 없는 경우 삭제하려고 할 수 있습니다. 스냅샷은 증분식 백업이기 때문에 스냅샷을 삭제하면 다른 스냅샷에 필요하지 않은 데이터만 삭제됩니다.

주제

- Java용 AWS SDK를 사용한 스냅샷 삭제
- .NET용 AWS SDK를 사용한 스냅샷 삭제
- AWS Tools for Windows PowerShell를 사용하여 스냅샷을 삭제합니다.

Amazon EBS 콘솔에서 스냅샷을 한 번에 하나씩 삭제할 수 있습니다. Amazon EBS 콘솔을 사용하여 스냅샷을 삭제하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon EBS 스냅샷 삭제를 참조하세요.

한 번에 여러 스냅샷을 삭제하려면 Storage Gateway 작업을 지원하는 AWS SDK 중 하나를 사용할 수 있습니다. 예시는 Java용 AWS SDK를 사용한 스냅샷 삭제, .NET용 AWS SDK를 사용한 스냅샷 삭제 및 AWS Tools for Windows PowerShell를 사용하여 스냅샷을 삭제합니다. 단원을 참조하십시오.

Java용 AWS SDK를 사용한 스냅샷 삭제

볼륨과 연결된 여러 스냅샷을 삭제할 때는 프로그래밍 접근 방식을 사용할 수 있습니다. 다음 예시는 Java용 AWS SDK를 사용하여 스냅샷을 삭제하는 방법을 보여줍니다. 예시 코드를 사용하려면 Java 콘솔 애플리케이션을 실행하는 방법을 잘 알아야 합니다. 자세한 내용은 Java용AWS SDK 개발자 안내서에서 시작하기를 참조하세요. 스냅샷을 몇 개만 삭제하는 경우, 스냅샷 삭제 단원의 설명 대로 콘솔을 사용하여 삭제합니다.

Example : Java용 AWS SDK를 사용하여 스냅샷 삭제

다음 Java 코드 예시에는 게이트웨이의 각 볼륨에 대한 스냅샷과 함께 스냅샷 시작 시각이 지정한 날짜 이전인지 이후인지 여부가 나열되어 있습니다. Storage Gateway와 Amazon EC2용 Java API용 AWS SDK를 사용합니다. Amazon EC2 API에는 스냅샷 처리를 위한 작업이 포함되어 있습니다.

서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN) 및 스냅샷을 저장하려는 이전 일수를 제공하도록 코드를 업데이트합니다. 이 기간 이전에 생성된 스냅샷은 삭제됩니다. 또한 부울 값 `viewOnly`를 지정해야 합니다. 이 값은 삭제할 스냅샷을 보길 원하는지, 아니면 스냅샷 삭제를 실제로 수행하길 원하는지 알려줍니다. 코드가 삭제하는 항목을 확인하려면 보기 옵션만 사용하여(즉, `viewOnly`가 `true`로 설정됨) 먼저 코드를 실행합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

```
import java.io.IOException;
import java.util.ArrayList;
import java.util.Calendar;
import java.util.Collection;
```

```
import java.util.Date;
import java.util.GregorianCalendar;
import java.util.List;

import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.ec2.AmazonEC2Client;
import com.amazonaws.services.ec2.model.DeleteSnapshotRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsRequest;
import com.amazonaws.services.ec2.model.DescribeSnapshotsResult;
import com.amazonaws.services.ec2.model.Filter;
import com.amazonaws.services.ec2.model.Snapshot;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.ListVolumesRequest;
import com.amazonaws.services.storagegateway.model.ListVolumesResult;
import com.amazonaws.services.storagegateway.model.VolumeInfo;

public class ListDeleteVolumeSnapshotsExample {

    public static AWSStorageGatewayClient sgClient;
    public static AmazonEC2Client ec2Client;
    static String serviceURLSG = "https://storagegateway.us-east-1.amazonaws.com";
    static String serviceURLEC2 = "https://ec2.us-east-1.amazonaws.com";

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

    // The number of days back you want to save snapshots. Snapshots before this cutoff
 are deleted
    // if viewOnly = false.
    public static int daysBack = 10;

    // true = show what will be deleted; false = actually delete snapshots that meet
 the daysBack criteria
    public static boolean viewOnly = true;

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

        // Create a Storage Gateway and amazon ec2 client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(

 ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));

        sgClient.setEndpoint(serviceURLSG);
```

```
        ec2Client = new AmazonEC2Client(new PropertiesCredentials(

ListDeleteVolumeSnapshotsExample.class.getResourceAsStream("AwsCredentials.properties")));
        ec2Client.setEndpoint(serviceURLEC2);

        List<VolumeInfo> volumes = ListVolumesForGateway();
        DeleteSnapshotsForVolumes(volumes, daysBack);

    }
    public static List<VolumeInfo> ListVolumesForGateway()
    {
        List<VolumeInfo> volumes = new ArrayList<VolumeInfo>();

        String marker = null;
        do {
            ListVolumesRequest request = new
ListVolumesRequest().withGatewayARN(gatewayARN);
            ListVolumesResult result = sgClient.listVolumes(request);
            marker = result.getMarker();

            for (VolumeInfo vi : result.getVolumeInfos())
            {
                volumes.add(vi);
                System.out.println(OutputVolumeInfo(vi));
            }
        } while (marker != null);

        return volumes;
    }
    private static void DeleteSnapshotsForVolumes(List<VolumeInfo> volumes,
            int daysBack2) {

        // Find snapshots and delete for each volume
        for (VolumeInfo vi : volumes) {

            String volumeARN = vi.getVolumeARN();
            String volumeId =
volumeARN.substring(volumeARN.lastIndexOf("/")+1).toLowerCase();
            Collection<Filter> filters = new ArrayList<Filter>();
            Filter filter = new Filter().withName("volume-id").withValues(volumeId);
            filters.add(filter);

            DescribeSnapshotsRequest describeSnapshotsRequest =
                new DescribeSnapshotsRequest().withFilters(filters);
```

```
            DescribeSnapshotsResult describeSnapshotsResult =
                ec2Client.describeSnapshots(describeSnapshotsRequest);

            List<Snapshot> snapshots = describeSnapshotsResult.getSnapshots();
            System.out.println("volume-id = " + volumeId);
            for (Snapshot s : snapshots){
                StringBuilder sb = new StringBuilder();
                boolean meetsCriteria = !CompareDates(daysBack, s.getStartTime());
                sb.append(s.getSnapshotId() + ", " + s.getStartTime().toString());

                sb.append(", meets criteria for delete? " + meetsCriteria);
                sb.append(", deleted? ");
                if (!viewOnly & meetsCriteria) {
                    sb.append("yes");
                    DeleteSnapshotRequest deleteSnapshotRequest =
                        new DeleteSnapshotRequest().withSnapshotId(s.getSnapshotId());
                    ec2Client.deleteSnapshot(deleteSnapshotRequest);
                }
                else {
                    sb.append("no");
                }
                System.out.println(sb.toString());
            }
        }
    }

    private static String OutputVolumeInfo(VolumeInfo vi) {

        String volumeInfo = String.format(
                 "Volume Info:\n" +
                 "  ARN: %s\n" +
                 "  Type: %s\n",
                 vi.getVolumeARN(),
                 vi.getVolumeType());
        return volumeInfo;
     }

    // Returns the date in two formats as a list
    public static boolean CompareDates(int daysBack, Date snapshotDate) {
        Date today = new Date();
        Calendar cal = new GregorianCalendar();
        cal.setTime(today);
        cal.add(Calendar.DAY_OF_MONTH, -daysBack);
        Date cutoffDate = cal.getTime();
```

```
        return (snapshotDate.compareTo(cutoffDate) > 0) ? true : false;
    }

}
```

.NET용 AWS SDK를 사용한 스냅샷 삭제

볼륨과 연결된 여러 스냅샷을 삭제할 때는 프로그래밍 접근 방식을 사용할 수 있습니다. 다음 예시는 .NET용 AWS SDK 버전 2 및 3을 사용하여 스냅샷을 삭제하는 방법을 보여줍니다. 예시 코드를 사용하려면 .NET 콘솔 애플리케이션을 실행하는 방법을 잘 알아야 합니다. 자세한 내용은 .NET용AWS SDK 개발자 안내서에서 시작하기를 참조하세요. 스냅샷을 몇 개만 삭제하는 경우, 스냅샷 삭제 단원의 설명 대로 콘솔을 사용하여 삭제합니다.

Example : .NET용 AWS SDK를 사용하여 스냅샷 삭제

다음 C# 코드 예제에서 AWS Identity and Access Management 사용자는 게이트웨이의 각 볼륨에 대한 스냅샷을 나열할 수 있습니다. 그런 다음 스냅샷 시작 시간이 지정된 날짜(보존 기간) 이전 또는 이후인지 확인하고 보존 기간이 지난 스냅샷을 삭제합니다. 이 예에서는 Storage Gateway 및 Amazon EC2의 .NET API용 AWS SDK를 사용합니다. Amazon EC2 API에는 스냅샷 처리를 위한 작업이 포함되어 있습니다.

다음 코드 예제는.NET용 AWS SDK 버전 2와 3을 사용합니다. .NET의 이전 버전을 새 버전으로 마이그레이션할 수 있습니다. 자세한 내용은 .NET용 AWS SDK의 최신 버전으로 코드 마이그레이션을 참조하십시오.

서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN) 및 스냅샷을 저장하려는 이전 일수를 제공하도록 코드를 업데이트합니다. 이 기간 이전에 생성된 스냅샷은 삭제됩니다. 또한 부울 값 `viewOnly`를 지정해야 합니다. 이 값은 삭제할 스냅샷을 보길 원하는지, 아니면 스냅샷 삭제를 실제로 수행하길 원하는지 알려줍니다. 코드가 삭제하는 항목을 확인하려면 보기 옵션만 사용하여(즉, `viewOnly`가 `true`로 설정됨) 먼저 코드를 실행합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

먼저 IAM 사용자를 생성하고 이 사용자에게 최소 IAM 정책을 연결합니다. 그 다음에 게이트웨이에 대한 자동 스냅샷을 예약합니다.

다음 코드에서는 사용자가 스냅샷을 삭제하도록 허용하는 최소 정책을 생성합니다. 이 예제에서 정책 이름은 **`sgw-delete-snapshot`**입니다.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StmtEC2Snapshots",
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots"
            ],
            "Resource": [
                "*"
            ]
        },
        {
            "Sid": "StmtSgwListVolumes",
            "Effect": "Allow",
            "Action": [
                "storagegateway:ListVolumes"
            ],
            "Resource": [
                "*"
            ]
        }
    ]
}
```

다음 C# 코드는 지정된 게이트웨이에서 볼륨과 지정된 기간과 일치하는 스냅샷을 모두 찾아 삭제합니다.

```
using System;
using System.Collections.Generic;
using System.Text;
using Amazon.EC2;
using Amazon.EC2.Model;
using Amazon.StorageGateway.Model;
using Amazon.StorageGateway;

namespace DeleteStorageGatewaySnapshotNS
{
    class Program
    {
        /*
         * Replace the variables below to match your environment.
```

```
         */

         /* IAM AccessKey */
        static String AwsAccessKey = "AKIA..............";

        /* IAM SecretKey */
        static String AwsSecretKey = "******************************";

        /* Account number, 12 digits, no hyphen */
        static String OwnerID = "123456789012";

        /* Your Gateway ARN. Use a Storage Gateway ID, sgw-XXXXXXXX* */
        static String GatewayARN = "arn:aws:storagegateway:ap-
southeast-2:123456789012:gateway/sgw-XXXXXXXX";

        /* Snapshot status: "completed", "pending", "error" */

        static String SnapshotStatus = "completed";

        /* Region where your gateway is activated */
        static String AwsRegion = "ap-southeast-2";

        /* Minimum age of snapshots before they are deleted (retention policy) */
        static int daysBack = 30;

        /*
         * Do not modify the four lines below.
         */
        static AmazonEC2Config ec2Config;
        static AmazonEC2Client ec2Client;
        static AmazonStorageGatewayClient sgClient;
        static AmazonStorageGatewayConfig sgConfig;

        static void Main(string[] args)
        {
            // Create an EC2 client.
            ec2Config = new AmazonEC2Config();
            ec2Config.ServiceURL = "https://ec2." + AwsRegion + ".amazonaws.com";
            ec2Client = new AmazonEC2Client(AwsAccessKey, AwsSecretKey, ec2Config);

            // Create a Storage Gateway client.
            sgConfig = new AmazonStorageGatewayConfig();
            sgConfig.ServiceURL = "https://storagegateway." + AwsRegion +
 ".amazonaws.com";
```

```
            sgClient = new AmazonStorageGatewayClient(AwsAccessKey, AwsSecretKey,
sgConfig);

            List<VolumeInfo> StorageGatewayVolumes = ListVolumesForGateway();
            List<Snapshot> StorageGatewaySnapshots =
ListSnapshotsForVolumes(StorageGatewayVolumes,
                                                    daysBack);
            DeleteSnapshots(StorageGatewaySnapshots);
        }

        /*
         * List all volumes for your gateway
         * returns: A list of VolumeInfos, or null.
         */
        private static List<VolumeInfo> ListVolumesForGateway()
        {
            ListVolumesResponse response = new ListVolumesResponse();
            try
            {
                ListVolumesRequest request = new ListVolumesRequest();
                request.GatewayARN = GatewayARN;
                response = sgClient.ListVolumes(request);

                foreach (VolumeInfo vi in response.VolumeInfos)
                {
                    Console.WriteLine(OutputVolumeInfo(vi));
                }
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine(ex.Message);
            }
            return response.VolumeInfos;
        }

        /*
         * Gets the list of snapshots that match the requested volumes
         * and cutoff period.
         */
        private static List<Snapshot> ListSnapshotsForVolumes(List<VolumeInfo> volumes,
int snapshotAge)
        {
            List<Snapshot> SelectedSnapshots = new List<Snapshot>();
            try
```

```
            {
                foreach (VolumeInfo vi in volumes)
                {
                    String volumeARN = vi.VolumeARN;
                    String volumeID = volumeARN.Substring(volumeARN.LastIndexOf("/") +
1).ToLower();

                    DescribeSnapshotsRequest describeSnapshotsRequest = new
DescribeSnapshotsRequest();

                    Filter ownerFilter = new Filter();
                    List<String> ownerValues = new List<String>();
                    ownerValues.Add(OwnerID);
                    ownerFilter.Name = "owner-id";
                    ownerFilter.Values = ownerValues;
                    describeSnapshotsRequest.Filters.Add(ownerFilter);

                    Filter statusFilter = new Filter();
                    List<String> statusValues = new List<String>();
                    statusValues.Add(SnapshotStatus);
                    statusFilter.Name = "status";
                    statusFilter.Values = statusValues;
                    describeSnapshotsRequest.Filters.Add(statusFilter);

                    Filter volumeFilter = new Filter();
                    List<String> volumeValues = new List<String>();
                    volumeValues.Add(volumeID);
                    volumeFilter.Name = "volume-id";
                    volumeFilter.Values = volumeValues;
                    describeSnapshotsRequest.Filters.Add(volumeFilter);

                    DescribeSnapshotsResponse describeSnapshotsResponse =
                      ec2Client.DescribeSnapshots(describeSnapshotsRequest);

                    List<Snapshot> snapshots = describeSnapshotsResponse.Snapshots;
                    Console.WriteLine("volume-id = " + volumeID);
                    foreach (Snapshot s in snapshots)
                    {
                        if (IsSnapshotPastRetentionPeriod(snapshotAge, s.StartTime))
                        {
                            Console.WriteLine(s.SnapshotId + ", " + s.VolumeId + ",
                               " + s.StartTime + ", " + s.Description);
                            SelectedSnapshots.Add(s);
                        }
```

```
                    }
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
            return SelectedSnapshots;
        }

        /*
         * Deletes a list of snapshots.
         */
        private static void DeleteSnapshots(List<Snapshot> snapshots)
        {
            try
            {
                foreach (Snapshot s in snapshots)
                {

                    DeleteSnapshotRequest deleteSnapshotRequest = new
DeleteSnapshotRequest(s.SnapshotId);
                    DeleteSnapshotResponse response =
ec2Client.DeleteSnapshot(deleteSnapshotRequest);
                    Console.WriteLine("Volume: " +
                              s.VolumeId +
                              " => Snapshot: " +
                              s.SnapshotId +
                              " Response: "
                              + response.HttpStatusCode.ToString());
                }
            }
            catch (AmazonEC2Exception ex)
            {
                Console.WriteLine(ex.Message);
            }
        }

        /*
         * Checks if the snapshot creation date is past the retention period.
         */
        private static Boolean IsSnapshotPastRetentionPeriod(int daysBack, DateTime
snapshotDate)
        {
```

```
            DateTime cutoffDate = DateTime.Now.Add(new TimeSpan(-daysBack, 0, 0, 0));
            return (DateTime.Compare(snapshotDate, cutoffDate) < 0) ? true : false;
        }

        /*
         * Displays information related to a volume.
         */
        private static String OutputVolumeInfo(VolumeInfo vi)
        {
            String volumeInfo = String.Format(
                "Volume Info:\n" +
                "  ARN: {0}\n" +
                "  Type: {1}\n",
                vi.VolumeARN,
                vi.VolumeType);
            return volumeInfo;
        }
    }
}
```

AWS Tools for Windows PowerShell를 사용하여 스냅샷을 삭제합니다.

볼륨과 연결된 여러 스냅샷을 삭제할 때는 프로그래밍 접근 방식을 사용할 수 있습니다. 다음 예시는 AWS Tools for Windows PowerShell를 사용하여 스냅샷을 삭제하는 방법을 보여줍니다. 예제 스크립트를 사용하려면 스크립트 실행에 익숙해야 합니다. PowerShell 자세한 내용은 시작하기(출처: AWS Tools for Windows PowerShell)를 참조하십시오. 스냅샷을 몇 개만 삭제하는 경우, 스냅샷 삭제 단원의 설명 대로 콘솔을 사용하여 삭제합니다.

Example : 를 사용하여 스냅샷 삭제 AWS Tools for Windows PowerShell

다음 PowerShell 스크립트 예제는 게이트웨이의 각 볼륨에 대한 스냅샷과 스냅샷 시작 시간이 지정된 날짜 이전인지 이후인지를 나열합니다. Storage Gateway와 Amazon EC2용 AWS Tools for Windows PowerShell cmdlet을 사용합니다. Amazon EC2 API에는 스냅샷 처리를 위한 작업이 포함되어 있습니다.

스크립트를 업데이트해 게이트웨이 Amazon 리소스 이름(ARN) 및 스냅샷을 저장하려는 이전 일수를 제공해야 합니다. 이 기간 이전에 생성된 스냅샷은 삭제됩니다. 또한 부울 값 `viewOnly`를 지정해야 합니다. 이 값은 삭제할 스냅샷을 보길 원하는지, 아니면 스냅샷 삭제를 실제로 수행하길 원하는지 알려줍니다. 코드가 삭제하는 항목을 확인하려면 보기 옵션만 사용하여(즉, `viewOnly`가 `true`로 설정됨) 먼저 코드를 실행합니다.

```
<#
```

```
.DESCRIPTION
    Delete snapshots of a specified volume that match given criteria.

.NOTES
    PREREQUISITES:
    1) AWS Tools for Windows PowerShell from https://aws.amazon.com/powershell/
    2) Credentials and AWS 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_DeleteSnapshots.ps1
#>

# Criteria to use to filter the results returned.
$daysBack = 18
$gatewayARN = "*** provide gateway ARN ***"
$viewOnly = $true;

#ListVolumes
$volumesResult = Get-SGVolume -GatewayARN $gatewayARN
$volumes = $volumesResult.VolumeInfos
Write-Output("`nVolume List")
foreach ($volumes in $volumesResult)
  { Write-Output("`nVolume Info:")
    Write-Output("ARN:  " + $volumes.VolumeARN)
    write-Output("Type: " + $volumes.VolumeType)
  }

Write-Output("`nWhich snapshots meet the criteria?")
foreach ($volume in $volumesResult)
  {
    $volumeARN = $volume.VolumeARN

    $volumeId = ($volumeARN-split"/")[3].ToLower()

    $filter = New-Object Amazon.EC2.Model.Filter
    $filter.Name = "volume-id"
    $filter.Value.Add($volumeId)

    $snapshots = get-EC2Snapshot -Filter $filter
    Write-Output("`nFor volume-id = " + $volumeId)
    foreach ($s in $snapshots)
    {
```

```
        $d = ([DateTime]::Now).AddDays(-$daysBack)
        $meetsCriteria = $false
        if ([DateTime]::Compare($d, $s.StartTime) -gt 0)
        {
             $meetsCriteria = $true
        }

        $sb = $s.SnapshotId + ", " + $s.StartTime + ", meets criteria for delete? " +
$meetsCriteria
        if (!$viewOnly -AND $meetsCriteria)
        {
            $resp = Remove-EC2Snapshot -SnapshotId $s.SnapshotId
            #Can get RequestId from response for troubleshooting.
            $sb = $sb + ", deleted? yes"
        }
        else {
            $sb = $sb + ", deleted? no"
        }
        Write-Output($sb)
    }
 }
```

볼륨 상태 및 전환 이해

각 볼륨에는 볼륨의 상태를 한 눈에 알 수 있는 상태가 연결되어 있습니다. 대부분의 경우 그 상태는 볼륨이 정상적으로 작동하고 있으므로 사용자가 아무 조치도 취할 필요가 없음을 나타냅니다. 어떤 경우에는 상태를 통해 사용자의 조치가 필요한 또는 필요 없는 문제가 볼륨에 있음을 나타냅니다. 다음 정보를 찾아 조치를 취해야 하는 시점을 결정하는데 도움을 받을 수 있습니다. Storage Gateway 콘솔에서 또는 Storage Gateway API 작업 중 하나 (예: DescribeCachediSCSIVolumes또는) 를 사용하여 볼륨 상태를 볼 수 DescribeStorediSCSIVolumes있습니다.

주제

- 볼륨 상태 이해
- 연결 상태 이해
- 캐싱된 볼륨 상태 전환 이해
- 저장된 볼륨 상태 전환 이해

볼륨 상태 이해

다음 표는 Storage Gateway 콘솔에 표시되는 볼륨 상태를 나타냅니다. 볼륨 상태는 해당 게이트웨이의 각 스토리지 볼륨에 대한 상태 열에 표시됩니다. 정상적으로 작동하는 볼륨의 상태는 응시 가능입니다.

다음 표에는 각 스토리지 볼륨 상태에 대한 설명과 해당 상태를 기반으로 조치를 취해야 하는지 여부 및 그 시점이 나와 있습니다. 응시 가능 상태는 볼륨의 정상 상태입니다. 사용 중인 모든 경우 또는 거의 대부분의 경우에 볼륨은 이 상태여야 합니다.

상태 표시기	의미
사용 가능	볼륨을 사용할 수 있습니다. 이 상태는 볼륨이 정상적으로 작동하고 있음을 나타냅니다. 부트스트래핑 단계가 완료되면 볼륨은 다시 응시 가능 상태로 돌아갑니다. 즉 게이트웨이가 처음 전달상태로 전환된 이후 볼륨에 대한 변경 사항을 모두 동기화했습니다.
부트스트래핑	게이트웨이는 데이터를 저장된 데이터 사본과 로컬로 동기화하고 있습니다. AWS스토리지 볼륨은 대부분의 경우 응시 가능 상태를 자동으로 확인하기 때문에 일반적으로 이 상태에 대해서는 조치를 취할 필요가 없습니다. 다음은 볼륨 상태가 부트스트래핑인 경우입니다. • 게이트웨이가 예기치 않게 종료되었습니다. • 게이트웨이의 업로드 버퍼를 초과하였습니다. 이 경우 해당 볼륨이전달 상태가 되고 빈 업로드 버퍼의 크기가 충분히 증가하면 부트스트래핑이 발생합니다. 빈 업로드 버퍼 공간의 비율을 늘리기 위한 한 가지 방법으로 추가 업로드 버퍼 공간을 제공할 수 있습니다. 이 경우에 한해 스토리지 볼륨은 전달 상태에서 부트스트래핑, 응시 가능 상태로 전환됩니다. 부트스트래핑 기간 중에 이 볼륨을 계속 사용할 수 있습니다. 그러나 이 시점에서는 볼륨의 스냅샷을 생성할 수 없습니다. • 저장된 Volume Gateway를 생성하고 기존 로컬 디스크 데이터를 보존합니다. 이 시나리오에서는 게이트웨이가 모든 데이터를 에 업로드하기

상태 표시기	의미
	시작합니다. AWS볼륨은 로컬 디스크의 모든 데이터가 복사될 때까지 부트스트래핑 상태를 유지합니다. AWS이 부트스트래핑 기간 중에 이 볼륨을 사용할 수 있습니다. 그러나 이 시점에서는 볼륨의 스냅샷을 생성할 수 없습니다.
[생성 중]	볼륨이 현재 생성 중이므로 아직 사용할 준비가 되지 않았습니다. 생성 중(Creating)상태는 중간 단계입니다. 아무 조치도 필요하지 않습니다.
[삭제 중]	현재 볼륨이 삭제되는 중입니다. 삭제 중(Deleting) 상태는 중간 단계입니다. 아무 조치도 필요하지 않습니다.
복구할 수 없음	오류가 발생하여 볼륨을 복구할 수 없습니다. 이러한 상황에서 해야 할 일에 대한 자세한 내용은 볼륨 문제 해결 단원을 참조하십시오.

상태 표시기	의미
전달	로컬에서 유지 관리되는 데이터는 저장된 데이터와 동기화되지 않습니다. AWS볼륨이 전달 상태일 때 볼륨에 쓴 데이터는 볼륨 상태가 부트스트래핑이 될 때까지 캐시에 남아 있습니다. 이 데이터는 부트스트래핑 상태가 시작될 AWS 때 업로드되기 시작합니다. 전달 상태는 다음과 같은 몇 가지 이유로 발생할 수 있습니다. • 게이트웨이에 업로드 버퍼 공간이 부족한 경우, 전달 상태가 됩니다. 볼륨이 전달 상태인 동안에 애플리케이션은 스토리지 볼륨에(서) 데이터를 계속 읽고 쓸 수 있습니다. 그러나 게이트웨이는 업로드 버퍼에 볼륨 데이터를 쓰지 않거나 AWS로 데이터를 업로드하지 않습니다. 볼륨이 전달 상태로 전환되기 전에 게이트웨이는 계속해서 볼륨에 기록된 데이터를 업로드합니다. 볼륨이 전달 상태인 동안에는 스토리지 볼륨에 대해 보류 중인 또는 예정된 스냅샷이 모두 실패합니다. 업로드 버퍼가 초과되어 스토리지 볼륨의 상태가 전달이 되었을 때 취해야 할 조치에 대한 자세한 내용은 볼륨 문제 해결 단원을 참조하십시오. Pass Throuh의 볼륨이 ACTIVE 상태로 돌아가려면 부트스트래핑 단계를 완료해야 합니다. 부트스트래핑 중에 볼륨은 내에서 AWS다시 동기화를 설정하여 볼륨에 대한 변경 사항 기록 (로그) 을 재개하고 기능을 활성화할 수 있습니다. `CreateSnapshot` 부트스트래핑 동안 볼륨 쓰기는 업로드 버퍼에 기록됩니다. • 스토리지 볼륨 부트스트래핑이 한 번에 하나 이상인 경우에 전달 상태가 됩니다. 한 번에 게이트웨이 스토리지 볼륨 하나만 부트스트래핑할 수 있습니다. 예를 들어, 스토리지 볼륨을 두 개 생성하여 기존 데이터를 둘 다에 아카이브하도록 선택했다고 가정합니다. 이 경우, 두 번째 스토리지 볼륨은 첫 번째 스토리지 볼륨이 부트스트래핑을 마칠 때까지 전달 상태입니다. 이 시나리오에서는 조치를 취할 필요가 없습니다. 각 스토리지 볼륨은 생성을 마치면 자동으로 응시 가능 상태로 변경됩니다. 스토리지 볼륨이 전달 또는 부트스트래핑 상태인 동안 스토리지 볼륨에(서) 읽고 쓸 수 있습니다. •

상태 표시기	의미
	드물게 전달 상태가 업로드 버퍼 사용에 할당한 디스크에 장애가 있음을 나타내는 경우가 있습니다. 이 경우에 취할 조치에 대한 정보는 볼륨 문제 해결 단원을 참조하십시오. • 전달 상태는 볼륨이 활성 또는 부트스트래핑 상태일 때 발생할 수 있습니다. 이 경우 볼륨이 쓰기를 수신하지만 해당 쓰기를 기록(로깅)하기에는 업로드 버퍼의 용량이 부족합니다. • 전달 상태는 볼륨의 상태와 상관 없이 게이트웨이가 완전히 종료되지 않은 경우 발생합니다. 이러한 유형의 종료는 소프트웨어가 충돌했거나 VM의 전원을 끄지 않았기 때문에 발생할 수 있습니다. 이 경우 볼륨은 어떤 상태에서도 전달 상태로 전환됩니다.
복원 중	기존 스냅샷에서 볼륨을 복원하는 중입니다. 이 상태는 저장 볼륨에만 적용됩니다. 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 단원을 참조하십시오. 스토리지 볼륨 두 개를 동시에 복원하는 경우, 두 스토리지 볼륨은 복원 중 상태를 표시합니다. 각 스토리지 볼륨은 생성을 마치면 자동으로 응시 가능 상태로 변경됩니다. 스토리지 볼륨이 복원 중 상태인 동안 스토리지 볼륨에(서) 읽고 쓸 수 있으며 스냅샷을 만들 수 있습니다.
복원 및 전달	기존 스냅샷에서 볼륨을 복원하는 중에 업로드 버퍼 문제가 발생하였습니다. 이 상태는 저장 볼륨에만 적용됩니다. 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 단원을 참조하십시오. 복원 및 전달 상태의 한 가지 원인은 게이트웨이에 업로드 버퍼 공간이 모자란 경우입니다. 스토리지 볼륨이 복원 및 전달 상태인 동안에 애플리케이션은 스토리지 볼륨에(서) 데이터를 계속 읽고 쓸 수 있습니다. 그러나 복원 및 전달 상태 기간에는 스토리지 볼륨의 스냅샷을 생성할 수 없습니다. 업로드 버퍼 용량을 초과하여 스토리지 볼륨이 복원 및 전달 상태가 된 경우에 취할 조치에 대한 정보는 볼륨 문제 해결 단원을 참조하십시오. 드물게 복원 및 전달 상태가 업로드 버퍼에 할당한 디스크에 장애가 있음을 나타내는 경우가 있습니다. 이 경우에 취할 조치에 대한 정보는 볼륨 문제 해결 단원을 참조하십시오.

상태 표시기	의미
구성된 업로드 버퍼 없음(Upload Buffer Not Configured)	게이트웨이에 구성된 업로드 버퍼가 없기 때문에 볼륨을 생성하거나 사용할 수 없습니다. 캐싱된 볼륨 설정에서 볼륨에 대한 업로드 버퍼 용량을 추가하는 자세한 방법은 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오. 저장된 볼륨 설정에서 볼륨에 대한 업로드 버퍼 용량을 추가하는 자세한 방법은 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오.

연결 상태 이해

Storage Gateway 콘솔 또는 를 사용하여 게이트웨이에서 볼륨을 분리하거나 API 게이트웨이에 연결할 수 있습니다. 다음 표는 Storage Gateway 콘솔에 표시되는 볼륨 연결 상태를 나타냅니다. 볼륨 연결 상태는 해당 게이트웨이의 각 스토리지 볼륨에 대한 연결 상태 열에 표시됩니다. 예를 들어 게이트웨이에서 분리된 볼륨은 분리됨으로 표시됩니다. 볼륨 연결 및 분리에 대한 자세한 내용은 볼륨을 다른 게이트웨이로 이동 단원을 참조하십시오.

상태 표시기	의미
연결됨	볼륨이 게이트웨이에 연결되었습니다.
분리됨	볼륨이 게이트웨이에서 분리되었습니다.
분리 중	볼륨이 게이트웨이에서 분리되는 중입니다. 분리 중인 볼륨에 데이터가 없는 경우 이 상태가 나타나지 않을 수 있습니다.

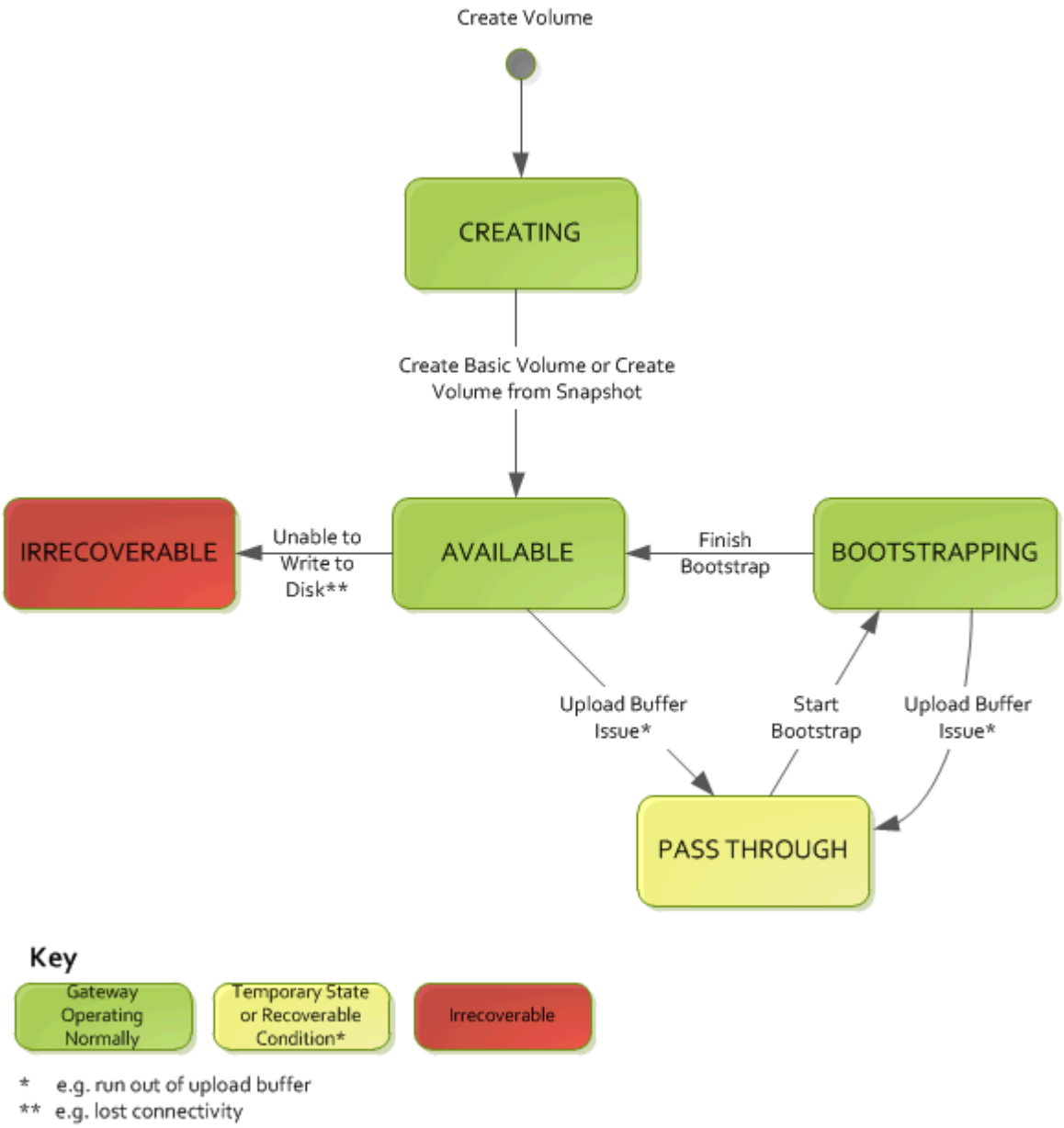
캐싱된 볼륨 상태 전환 이해

다음 상태 다이어그램을 보면 캐싱된 게이트웨이에서 볼륨의 가장 일반적인 상태 간 전환을 이해할 수 있습니다. 이 다이어그램을 상세하게 이해하지 않아도 게이트웨이를 효과적으로 사용할 수 있습니다. Volume Gateway의 작동 방식에 대해 더 자세히 알고 싶다면 이 다이어그램에서 자세한 내용을 확인할 수 있습니다.

이 다이어그램에는 구성된 업로드 버퍼 없음(Upload Buffer Not Configured) 상태 또는 삭제 중 상태는 나와 있지 않습니다. 이 다이어그램의 볼륨 상태는 녹색, 노란색 및 빨간색 상자로 표시됩니다. 각 색상은 아래 설명처럼 해석할 수 있습니다.

색상	볼륨 상태
녹색	게이트웨이가 정상적으로 작동하고 있습니다. 볼륨 상태가 응시 가능이거나 결국 응시 가능이 됩니다.
노란색	볼륨이 전달 상태입니다. 이는 스토리지 볼륨에 문제가 있을 수 있음을 나타냅니다. 업로드 버퍼 공간이 차서 이 상태가 나타난 경우에는 버퍼 공간이 다시 사용 가능으로 바뀌는 경우가 있습니다. 이 시점에 스토리지 볼륨은 자체 교정을 통해 응시 가능 상태가 됩니다. 또는 게이트웨이에 업로드 버퍼 공간을 추가하여 스토리지 볼륨 상태가 응시 가능이 되도록 해야 하는 경우도 있습니다. 업로드 버퍼 용량을 초과한 경우 문제를 해결하는 방법에 대한 정보는 볼륨 문제 해결 단원을 참조하십시오. 업로드 버퍼 용량을 추가하는 방법에 대한 정보는 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오.
빨간색	스토리지 볼륨이 복구할 수 없음 상태입니다. 이 경우에는 볼륨을 삭제해야 합니다. 이렇게 하는 방법에 대한 정보는 볼륨을 삭제하려면 단원을 참조하십시오.

다이어그램에서 두 상태 간의 전환은 선에 설명이 붙어 있습니다. 예를 들어, 생성 중(Creating) 상태에서 응시 가능 상태로 전환되면 기본 볼륨 생성(Create Basic Volume) 또는 스냅샷에서 볼륨 생성(Create Volume from Snapshot)이라는 레이블이 지정됩니다. 이러한 전환은 캐싱된 볼륨 생성을 나타냅니다. 스토리지 볼륨 생성에 대한 자세한 내용은 볼륨 추가 단원을 참조하십시오.



> **Note**
>
> 볼륨 상태 전달은 이 다이어그램에서 노란색으로 나타납니다. 그러나 이는 Storage Gateway 콘솔의 상태 상자에 표시되는 이 상태 아이콘의 색상과 다릅니다.

저장된 볼륨 상태 전환 이해

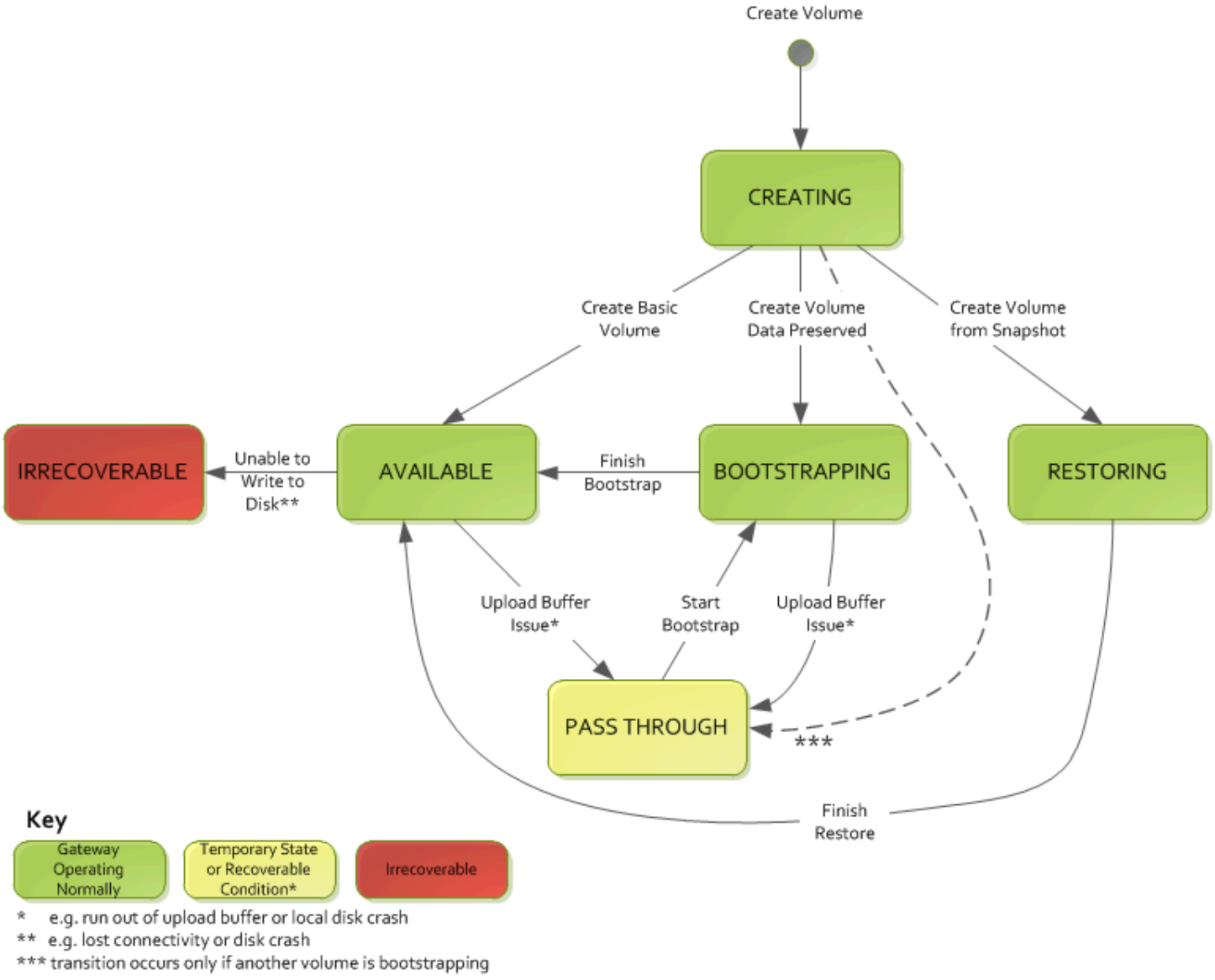
다음 상태 다이어그램을 보면 저장된 게이트웨이에서 볼륨의 가장 일반적인 상태 간 전환을 이해할 수 있습니다. 이 다이어그램을 상세하게 이해하지 않아도 게이트웨이를 효과적으로 사용할 수 있습니다.

그보다는 Volume Gateway 작동 방식을 더 깊이 이해하고 싶은 경우, 이 다이어그램에서 자세한 정보를 얻을 수 있습니다.

이 다이어그램에는 구성된 업로드 버퍼 없음(Upload Buffer Not Configured) 상태 또는 삭제 중 상태는 나와 있지 않습니다. 이 다이어그램의 볼륨 상태는 녹색, 노란색 및 빨간색 상자로 표시됩니다. 각 색상은 아래 설명처럼 해석할 수 있습니다.

색상	볼륨 상태
녹색	게이트웨이가 정상적으로 작동하고 있습니다. 볼륨 상태가 응시 가능이거나 결국 응시 가능이 됩니다.
노란색	스토리지 볼륨 하나를 생성하여 데이터를 보존하는 중에 다른 볼륨이 부트스트래핑 중이면 생성 중(Creating) 상태에서 전달 상태까지의 경로가 발생합니다. 이 경우 첫 번째 볼륨이 부트스트래핑을 마치면전달 상태인 볼륨이 부트스트래핑 상태로 바뀐 후 다시 응시 가능 상태가 됩니다. 언급한 특정 시나리오 이외에 노란색(전달 상태)은 스토리지 볼륨에 문제가 있을 수 있음을 나타내는데, 가장 흔한 문제는 업로드 버퍼와 관련된 것입니다. 업로드 버퍼 용량이 초과된 경우에는 버퍼 공간이 다시 사용 가능으로 바뀌는 경우가 있습니다. 이 시점에 스토리지 볼륨은 자체 교정을 통해 응시 가능 상태가 됩니다. 또는 게이트웨이에 업로드 버퍼 용량을 추가하여 스토리지 볼륨 상태가 응시 가능로 되돌아가도록 해야 하는 경우도 있습니다. 업로드 버퍼 용량을 초과한 경우 문제를 해결하는 방법에 대한 정보는 볼륨 문제 해결 단원을 참조하십시오. 업로드 버퍼 용량을 추가하는 방법에 대한 정보는 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오.
빨간색	스토리지 볼륨이 복구할 수 없음 상태입니다. 이 경우에는 볼륨을 삭제해야 합니다. 이렇게 하는 방법에 대한 정보는 볼륨 삭제 단원을 참조하십시오.

다음 다이어그램에서 두 상태 간의 전환은 선에 설명이 붙어 있습니다. 예를 들어, 생성 중(Creating) 상태에서 응시 가능 상태로 전환되면 기본 볼륨 생성(Create Basic Volume)이라는 레이블이 지정됩니다. 이 전환은 데이터 유지하거나 스냅샷에서 볼륨을 생성하지 않고 스토리지 볼륨을 생성한다는 것을 의미합니다.



> **Note**
>
> 볼륨 상태 전달은 이 다이어그램에서 노란색으로 나타납니다. 그러나 이는 Storage Gateway 콘솔의 상태 상자에 표시되는 이 상태 아이콘의 색상과 다릅니다.

데이터를 새 게이트웨이로 이동

데이터 및 성능 요구 사항이 증가하거나 게이트웨이를 마이그레이션하라는 AWS 알림을 받는 경우 게이트웨이 간에 데이터를 이동할 수 있습니다. 다음은 몇 가지 이유입니다.

- 데이터를 더 나은 호스트 플랫폼 또는 최신 Amazon EC2 인스턴스로 이동하십시오.
- 서버의 기본 하드웨어를 새로 고침합니다.

데이터를 새 게이트웨이로 이동하는 단계는 사용 중인 게이트웨이 유형에 따라 다릅니다.

> **Note**
>
> 데이터는 동일한 게이트웨이 유형 간에만 이동할 수 있습니다.

저장 볼륨을 새로운 저장 Volume Gateway로 이동

저장 볼륨을 새로운 저장 Volume Gateway로 이동하려면

1. 이전에 저장된 Volume Gateway에 쓰기 작업 중인 애플리케이션이 있으면 모두 중지합니다.
2. 다음 단계를 수행하여 볼륨의 스냅샷을 생성한 다음 스냅샷이 완료될 때까지 기다립니다.

    a. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.

    b. 탐색 창에서 볼륨을 선택한 다음 스냅샷을 생성할 볼륨을 선택합니다.

    c. 작업(Actions)에서 스냅샷 생성(Create snapshot)을 선택합니다.

    d. 스냅샷 생성 대화 상자에 스냅샷 설명을 입력하고 스냅샷 생성을 선택합니다.

    콘솔을 사용하여 스냅샷이 생성되었는지 확인할 수 있습니다. 데이터가 볼륨에 아직 업로드되는 중이면 업로드가 완료될 때까지 기다렸다가 다음 단계로 진행합니다. 스냅샷 상태를 확인하고 보류 중인 스냅샷이 없는지 검증하려면 볼륨에서 스냅샷 링크를 선택합니다.
3. 다음 단계를 수행하여 이전에 저장된 Volume Gateway를 중지합니다.

    a. 탐색 창에서 게이트웨이를 선택한 다음 중지하려는 이전에 저장된 Volume Gateway를 선택합니다. 게이트웨이 상태는 실행 중입니다.

    b. 작업에서 게이트웨이 중지를 선택합니다. 대화 상자에서 게이트웨이 ID를 확인한 다음 게이트웨이 중지를 선택합니다.

게이트웨이가 중지되는 동안 게이트웨이의 상태를 표시하는 메시지가 표시될 수 있습니다. 게이트웨이가 종료되면 세부 정보 탭에 메시지와 게이트웨이 시작 버튼이 나타납니다. 게이트웨이가 종료되면 게이트웨이 상태는 종료입니다.

c. 하이퍼바이저 컨트롤을 사용하여 VM을 종료합니다.

게이트웨이 중지에 대한 자세한 내용은 Volume Gateway 시작 및 중지 섹션을 참조하세요.

4. 저장 볼륨과 연결된 스토리지 디스크를 게이트웨이 VM에서 분리합니다. 그러면 VM의 루트 디스크가 제외됩니다.
5. 집에 https://console.aws.amazon.com/storagegateway/ 있는 Storage Gateway 콘솔에서 사용할 수 있는 새 하이퍼바이저 VM 이미지로 저장된 새 볼륨 게이트웨이를 활성화합니다.
6. 5단계에서 이전에 저장된 Volume Gateway VM에서 분리한 물리적 스토리지 디스크를 연결합니다.
7. 디스크의 기존 데이터를 보존하려면 다음 단계를 수행하여 저장 볼륨을 생성합니다.

   a. Storage Gateway 콘솔에서 볼륨 생성을 선택합니다.

   b. 볼륨 생성 대화 상자에서 5단계에서 생성한 저장 Volume Gateway를 선택합니다.

   c. 목록에서 디스크 ID 값을 선택합니다.

   d. 볼륨 콘텐츠의 경우 디스크의 기존 데이터 보존 옵션을 선택합니다.

   볼륨 생성에 대한 자세한 내용은 볼륨 생성 섹션을 참조하세요.

8. (선택 사항) 표시되는 CHAP인증 구성 마법사에서 이니시에이터 이름, 이니시에이터 암호, 대상 암호를 입력한 다음 [Save] 를 선택합니다.

   챌린지-핸드셰이크 인증 프로토콜 () 인증 사용에 대한 자세한 내용은 을 참조하십시오. CHAP i 타겟에 대한 CHAP 인증 구성 SCSI
9. 저장 볼륨에 쓰는 애플리케이션을 시작합니다.
10. 새 저장 Volume Gateway가 제대로 작동하는 것을 확인했으면 이전에 저장된 Volume Gateway를 삭제할 수 있습니다.

> **Important**
>
> 게이트웨이를 삭제하기 전에 해당 게이트웨이의 볼륨에 현재 쓰기 작업 중인 애플리케이션이 없는지 확인해야 합니다. 사용 중인 게이트웨이를 삭제하면 데이터 손실이 발생할 수 있습니다.

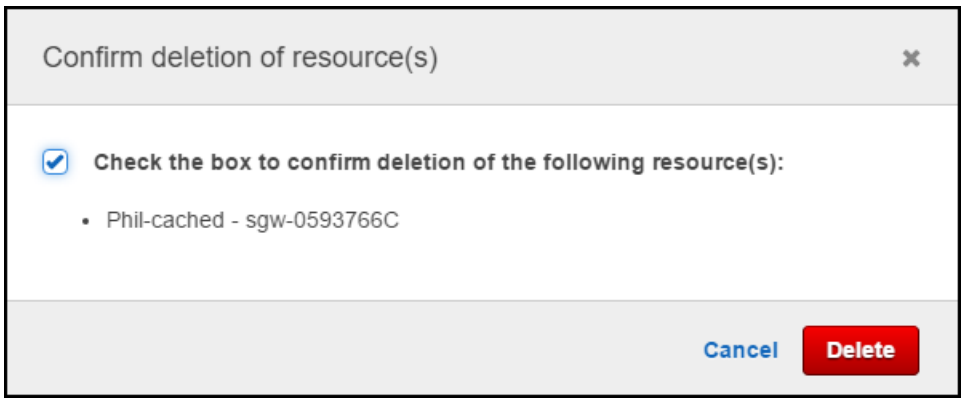
다음 단계를 수행하여 이전에 저장된 Volume Gateway를 삭제합니다.

> **Warning**
>
> 게이트웨이를 삭제하면 복구할 수 없습니다.

a. 탐색 창에서 게이트웨이를 선택한 다음 삭제하려는 이전에 저장된 Volume Gateway를 선택합니다.

b. 작업에서 게이트웨이 삭제를 선택합니다.

c. 표시된 확인 대화 상자에서 확인란을 선택하여 삭제를 확인합니다. 나열된 게이트웨이 ID에 삭제하려는 이전에 저장된 Volume Gateway가 지정되어 있는지 확인한 다음 삭제를 선택합니다.



11. 이전 게이트웨이 VM을 삭제합니다. VM 삭제에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

캐시 볼륨을 새로운 캐시 Volume Gateway 가상 머신으로 이동

캐시 볼륨을 새로운 캐시 Volume Gateway 가상 머신(VM)으로 이동하려면

1. 이전에 캐시된 Volume Gateway에 쓰기 작업 중인 애플리케이션이 있으면 모두 중지합니다.
2. i SCSI 볼륨을 사용 중인 모든 클라이언트에서 볼륨을 마운트 해제하거나 연결 해제하십시오. 이렇게 하면 클라이언트가 해당 볼륨을 변경하거나 해당 볼륨에 데이터를 추가하는 것을 방지하여 해당 볼륨의 데이터를 일관되게 유지할 수 있습니다.
3. 다음 단계를 수행하여 볼륨의 스냅샷을 생성한 다음 스냅샷이 완료될 때까지 기다립니다.

   a. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.

   b. 탐색 창에서 볼륨을 선택한 다음 스냅샷을 생성할 볼륨을 선택합니다.

   c. 작업(Actions)에서 스냅샷 생성(Create snapshot)을 선택합니다.

   d. 스냅샷 생성 대화 상자에 스냅샷 설명을 입력하고 스냅샷 생성을 선택합니다.

   콘솔을 사용하여 스냅샷이 생성되었는지 확인할 수 있습니다. 데이터가 볼륨에 아직 업로드되는 중이면 업로드가 완료될 때까지 기다렸다가 다음 단계로 진행합니다. 스냅샷 상태를 확인하고 보류 중인 스냅샷이 없는지 검증하려면 볼륨에서 스냅샷 링크를 선택합니다.

   콘솔에서 볼륨 상태를 확인하는 방법에 대한 자세한 내용은 볼륨 상태 및 전환 이해 섹션을 참조하세요. 캐시 볼륨 상태에 대한 자세한 내용은 캐싱된 볼륨 상태 전환 이해 섹션을 참조하세요.
4. 다음 단계를 수행하여 이전에 캐시된 Volume Gateway를 중지합니다.

   a. 탐색 창에서 게이트웨이를 선택한 다음 중지하려는 이전에 캐시된 Volume Gateway를 선택합니다. 게이트웨이 상태는 실행 중입니다.

   b. 작업에서 게이트웨이 중지를 선택합니다. 대화 상자에서 게이트웨이 ID를 확인한 다음 게이트웨이 중지를 선택합니다. 이후 단계에서 사용해야 하므로 게이트웨이 ID를 기록해 둡니다.

   이전 게이트웨이가 중지되는 동안 게이트웨이의 상태를 나타내는 메시지가 표시될 수 있습니다. 이전 게이트웨이가 종료되면 세부 정보 탭에 메시지와 게이트웨이 시작 버튼이 나타납니다. 게이트웨이가 종료되면 게이트웨이 상태는 종료입니다.

   c. 하이퍼바이저 컨트롤을 사용하여 이전 VM을 종료합니다. Amazon EC2 인스턴스 종료에 대한 자세한 내용은 Amazon EC2사용 설명서의 인스턴스 중지 및 시작을 참조하십시오. KVMVMware, 또는 Hyper-V VM 종료에 대한 자세한 내용은 하이퍼바이저 설명서를 참조하십시오.

게이트웨이 중지에 대한 자세한 내용은 Volume Gateway 시작 및 중지 섹션을 참조하세요.

5. 이전 게이트웨이 VM에서 루트 디스크, 캐시 디스크, 업로드 버퍼 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 분리합니다. (11단계 참조)

   Amazon EC2 인스턴스를 캐시된 볼륨 게이트웨이의 VM으로 사용하는 경우, Amazon 사용 EC2 설명서의 Linux 인스턴스에서 Amazon EBS 볼륨 분리를 참조하십시오. KVMVMware, 또는 Hyper-V VM에서 디스크를 분리하는 방법에 대한 자세한 내용은 하이퍼바이저 설명서를 참조하십시오.

6. 새 Storage Gateway 하이퍼바이저 VM 인스턴스를 생성하되 게이트웨이로 활성화하지는 마세요. 새 Storage Gateway 하이퍼바이저 VM을 생성하는 방법에 대한 자세한 내용은 Volume Gateway 설정 섹션을 참조하세요. 이 새 게이트웨이는 이전 게이트웨이의 ID를 사용합니다.

   > **Note**
   >
   > 새 VM에 캐시 또는 업로드 버퍼용 디스크를 추가하지 마세요. 새 VM은 이전 VM에서 사용하던 것과 동일한 캐시 디스크와 업로드 버퍼 디스크를 사용합니다.

7. 새 Storage Gateway 하이퍼바이저 VM 인스턴스는 이전 VM과 동일한 네트워크 구성을 사용해야 합니다. 게이트웨이의 기본 네트워크 구성은 동적 호스트 구성 프로토콜 () 입니다. DHCP 를 사용하면 DHCP 게이트웨이에 IP 주소가 자동으로 할당됩니다.

   새 VM의 고정 IP 주소를 수동으로 구성해야 하는 경우 자세한 내용은 게이트웨이 네트워크 구성 섹션을 참조하세요. 게이트웨이가 Socket Secure 버전 5 (SOCKS5) 프록시를 사용하여 인터넷에 연결해야 하는 경우 프록시를 통한 온프레미스 게이트웨이 라우팅 자세한 내용은 을 참조하십시오.

8. 새 VM을 시작합니다.

9. 5단계에서 이전의 캐시 Volume Gateway VM에서 분리한 디스크를 새로운 캐시 Volume Gateway에 연결합니다. 이전 게이트웨이 VM에 있는 것과 같은 순서로 디스크를 새 게이트웨이 VM에 연결합니다.

   모든 디스크는 변경되지 않은 상태로 전환해야 합니다. 볼륨 크기를 변경하면 메타데이터가 일관성이 없어지므로 변경하지 마세요.

10. 다음 형식을 사용하는 VM으로 새 VM에 연결하여 게이트웨이 마이그레이션 프로세스를 시작합니다. URL

    ```
    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. 다음 예와 비슷하게 URL 보일 것입니다.

    ```
    http://198.51.100.123/migrate?gatewayId=sgw-12345678
    ```

    브라우저 또는 명령줄에서 사용하여 `curl` 마이그레이션 프로세스를 시작할 수 있습니다. URL

    게이트웨이 마이그레이션 프로세스가 성공적으로 시작되면 다음과 같은 메시지가 표시됩니다.

    ```
    Successfully imported Storage Gateway information. Please refer to
    Storage Gateway documentation to perform the next steps to complete the
    migration.
    ```

11. 이전 게이트웨이의 루트 디스크를 분리합니다. 이 디스크의 볼륨 ID는 5단계에서 기록한 것입니다.

12. 게이트웨이를 시작합니다.

    다음 단계를 수행하여 새로운 캐시 Volume Gateway를 시작합니다.

    a. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.

    b. 탐색 창에서 게이트웨이를 선택한 다음 시작할 새 게이트웨이를 선택합니다. 게이트웨이 상태는 종료입니다.

    c. 세부 정보를 선택한 다음 게이트웨이 시작을 선택합니다.

    게이트웨이 시작에 대한 자세한 내용은 Volume Gateway 시작 및 중지 섹션을 참조하세요.

13. 이제 새 게이트웨이 VM의 IP 주소로 애플리케이션에서 볼륨을 사용할 수 있습니다.

14. 볼륨을 사용할 수 있는지 확인하고 이전 게이트웨이 VM을 삭제합니다. VM 삭제에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

Storage Gateway 모니터링

이 섹션에서는 Amazon을 사용하여 게이트웨이와 관련된 리소스를 모니터링하는 것을 포함하여 게이트웨이를 모니터링하는 방법을 설명합니다 CloudWatch. 게이트웨이의 업로드 버퍼 및 캐시 스토리지를 모니터링할 수 있습니다. Storage Gateway 콘솔을 사용하여 게이트웨이에 대한 지표와 경보를 볼 수 있습니다. 예를 들어 읽기 및 쓰기 작업에 사용되는 바이트의 수, 읽기 및 쓰기 작업에 걸리는 시간, Amazon Web Services 클라우드에서 데이터를 가져오는 데 걸리는 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 비용 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이 지표를 사용하여 기록 정보에 액세스하고 게이트웨이와 볼륨이 어떻게 실행되고 있는지 더 잘 파악할 수 있습니다. 또한 Storage Gateway는 고해상도 CloudWatch 경보를 제외한 경보를 추가 비용 없이 제공합니다. CloudWatch 요금에 대한 자세한 내용은 Amazon CloudWatch 요금을 참조하십시오. 에 대한 CloudWatch 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오.

주제

- 게이트웨이 지표 이해
- Storage Gateway 지표의 차원
- 업로드 버퍼 모니터링
- 캐시 스토리지 모니터링
- CloudWatch 알람에 대한 이해
- 게이트웨이에 대한 권장 CloudWatch 경보 생성
- 게이트웨이에 대한 사용자 지정 CloudWatch 알람 생성
- 볼륨 게이트웨이 모니터링

게이트웨이 지표 이해

이 주제에서는 게이트웨이 지표를 게이트웨이로 범위가 한정된 지표, 즉 게이트웨이에 대한 특정 내용을 측정하는 지표로 정의합니다. 게이트웨이에는 볼륨이 한 개 이상 포함되어 있으므로 게이트웨이별 지표는 게이트웨이의 모든 볼륨을 대표합니다. 예를 들어 `CloudBytesUploaded` 지표는 게이트웨이가 보고 기간 동안 클라우드에 전송한 총 바이트 수입니다. 이 지표는 게이트웨이에 있는 모든 볼륨의 활동을 포함합니다.

게이트웨이 지표 데이터 관련 작업을 할 때 지표를 보고 싶은 해당 게이트웨이의 고유 ID를 지정합니다. 이를 위해 `GatewayId` 및 `GatewayName` 값을 모두 지정합니다. 게이트웨이 지표 관련 작업을 할 때는 지표 네임스페이스에서 게이트웨이별 지표와 볼륨별 지표를 구분해주는 게이트웨이 차원을 지정합니다. 자세한 내용은 아마존 CloudWatch 메트릭스 사용 단원을 참조하십시오.

> **Note**
>
> 일부 지표는 가장 최근 모니터링 기간 동안 새 데이터가 생성된 경우에만 데이터 포인트를 반환합니다.

지표	설명
`AvailabilityNotifications`	게이트웨이에 의해 생성된 가용성 관련 상태 알림 수입니다. 이 지표를 `Sum` 통계에 사용하여 게이트웨이에 가용성 관련 이벤트가 발생하는지 여부를 확인할 수 있습니다. 이벤트에 대한 자세한 내용은 구성된 CloudWatch 로그 그룹을 확인하십시오. 단위: 숫자
`CacheHitPercent`	캐시로부터 읽은 애플리케이션 읽기 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 백분율
`CacheUsed`	게이트웨이의 캐시 스토리지에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다.

지표	설명	
	단위: 바이트	
IoWaitPercent	게이트웨이가 로컬 디스크의 응답을 대기하고 있는 시간의 백분율입니다. 단위: 백분율	
MemTotalBytes	게이트웨이 VM에 RAM 프로비저닝된 양 (바이트) 단위: 바이트	
MemUsedBytes	게이트웨이 VM에서 RAM 현재 사용 중인 양 (바이트) 단위: 바이트	
QueuedWrites	보고 기간이 끝날 때 게이트웨이의 모든 볼륨에 AWS대해 샘플링한 쓰기 대기 중인 바이트 수입니다. 이러한 바이트는 게이트웨이의 작업 스토리지에 유지됩니다. 단위: 바이트	
ReadBytes	게이트웨이의 모든 볼륨에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 읽은 총 바이트 수입니다. 이 측정치를 Sum 통계와 함께 사용하여 처리량을 측정하고 통계를 측정할 수 있습니다. Samples IOPS 단위: 바이트	

지표	설명
ReadTime	게이트웨이의 모든 볼륨에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 읽기 작업을 하는 데 소요된 총 밀리초 수입니다. 이 지표를 Average 통계와 함께 사용하면 지연 시간을 측정할 수 있습니다. 단위: 밀리초
TimeSinceLastRecoveryPoint	사용 가능한 마지막 복구 시점 이후 경과된 시간입니다. 자세한 내용은 캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우 단원을 참조하십시오. 단위: 초
TotalCacheSize	캐시의 총 크기(바이트)입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트
UploadBufferPercentUsed	게이트웨이의 업로드 버퍼 사용 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 백분율

지표	설명
UploadBufferUsed	게이트웨이의 업로드 버퍼에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트
UserCpuPercent	게이트웨이 처리에 소요된 CPU 시간의 백분율로, 모든 코어의 평균입니다. 단위: 백분율
WorkingStorageFree	게이트웨이의 작업 스토리지에서 사용하지 않은 총 공간 크기입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트
WorkingStoragePercentUsed	게이트웨이의 업로드 버퍼 사용 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 백분율
WorkingStorageUsed	게이트웨이의 업로드 버퍼에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트

지표	설명
WriteBytes	게이트웨이의 모든 볼륨에 대한 보고 기간 동안 온프레미스 애플리케이션에 작성한 총 바이트 수입니다. 이 측정치를 Sum 통계와 함께 사용하여 처리량을 측정하고 통계를 측정할 수 Samples 있습니다. IOPS 단위: 바이트
WriteTime	게이트웨이의 모든 볼륨에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 쓰기 작업을 하는 데 소요된 총 밀리초 수입니다. 이 지표를 Average 통계와 함께 사용하면 지연 시간을 측정할 수 있습니다. 단위: 밀리초

Storage Gateway 지표의 차원

Storage Gateway 서비스의 CloudWatch 네임스페이스는 입니다. AWS/StorageGateway 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.

측정기준	설명
GatewayId , GatewayName	이러한 차원은 요청하는 데이터를 게이트웨이별 지표로 필터링합니다. 작업할 게이트웨이를 GatewayId 또는 GatewayName 의 값으로 식별할 수 있습니다. 지표를 보는 데 관심이 있는

측정기준	설명
	시간 범위에 대해 게이트웨이의 이름이 다른 경우 `GatewayId` 를 사용합니다. 게이트웨이의 처리량 및 지연 시간 데이터는 게이트웨이의 모든 볼륨에 기반을 두고 있습니다. 게이트웨이 메트릭 사용에 대한 자세한 내용은 게이트웨이와 게이트웨이 간 성능 측정을 참조하십시오. AWS
`VolumeId`	이 차원은 요청하는 데이터를 볼륨에 따른 지표로 필터링합니다. 작업할 스토리지 볼륨을 해당 `VolumeId` 값으로 식별합니다. 볼륨 지표 작업에 대한 자세한 내용은 애플리케이션과 게이트웨이 간 성능 측정을 참조하십시오.

업로드 버퍼 모니터링

아래와 같이 게이트웨이의 업로드 버퍼를 모니터링하는 방법과 경보를 생성하여 버퍼가 지정한 임계값을 초과할 경우 알림을 받는 방법에 대한 정보를 얻을 수 있습니다. 이 접근 방식을 사용하면 게이트웨이가 꽉 차서 스토리지 애플리케이션이 AWS로 백업하지 못하는 일이 발생하기 전에 게이트웨이에 버퍼 스토리지를 추가할 수 있습니다.

캐시 볼륨 및 Tape Gateway 아키텍처와 동일한 방식으로 업로드 버퍼를 모니터링합니다. 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 단원을 참조하십시오.

> **Note**
>
> `WorkingStoragePercentUsed`, `WorkingStorageUsed`, `WorkingStorageFree` 지표는 Storage Gateway에서 캐시 볼륨 기능을 릴리스하기 전 저장 볼륨에 대한 업로드 버퍼만 나타냅니다. 이제는 동일한 업로드 버퍼 지표인 `UploadBufferPercentUsed`, `UploadBufferUsed` 및 `UploadBufferFree`를 사용합니다. 이 지표는 게이트웨이 아키텍처 둘 다에 적용됩니다.

관심 항목	측정 방법
업로드 버퍼 사용량	`UploadBufferPercentUsed` 통계와 함께 `UploadBufferUsed`, `UploadBufferFree` 및 `Average` 지표를 사용합니다. 예를 들어 `UploadBufferUsed` 통계와 함께 `Average`를 사용하여 일정 기간 동안의 스토리지 사용량을 분석합니다.

사용되는 업로드 버퍼의 백분율을 측정하려면

1. 에서 CloudWatch 콘솔을 엽니다 https://console.aws.amazon.com/cloudwatch/.
2. StorageGateway: 게이트웨이 지표 차원을 선택하고 사용할 게이트웨이를 찾으십시오.
3. `UploadBufferPercentUsed` 지표를 선택합니다.
4. 시간 범위에서 값을 선택합니다.
5. `Average` 통계를 선택합니다.
6. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

그 결과로 얻은 시간순 데이터 포인트 집합은 사용한 업로드 버퍼의 백분율을 포함합니다.

다음 절차에 따라 CloudWatch 콘솔을 사용하여 경보를 생성할 수 있습니다. 경보 및 임계값에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 CloudWatch 경보 생성을 참조하십시오.

게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면

1. 에서 콘솔을 여십시오. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. 경보에 대한 지표를 지정합니다.
   a. 경보 생성 마법사의 지표 선택 페이지에서 AWS/StorageGateway:GatewayId, GatewayName 차원을 선택한 다음 사용할 게이트웨이를 찾으십시오.
   b. `UploadBufferPercentUsed` 지표를 선택합니다. `Average` 통계와 5분의 시간을 사용합니다.
   c. 계속을 선택합니다.
4. 경보 이름, 설명 및 임계값을 정의합니다.

a. 경보 생성 마법사의 경보 정의 페이지에서 이름 및 설명 상자에 경보의 이름과 설명을 입력하여 경보를 식별합니다.

b. 경보 임계값을 정의합니다.

c. 계속을 선택합니다.

5. 경보에 대한 이메일 작업을 구성합니다.

a. 경보 생성 마법사의 작업 구성 페이지에서 경보 상태에 대해 경보를 선택합니다.

b. 주제에 대해 이메일 주제 선택 또는 생성을 선택합니다.

이메일 주제를 생성한다는 것은 Amazon SNS 주제를 설정한다는 의미입니다. SNSAmazon에 대한 자세한 내용은 Amazon SNS CloudWatch 사용 설명서의 Amazon 설정을 참조하십시오.

c. 주제에 주제에 대한 설명 이름을 입력합니다.

d. 작업 추가를 선택합니다.

e. 계속을 선택합니다.

6. 경보 설정을 검토한 후 경보를 생성합니다.

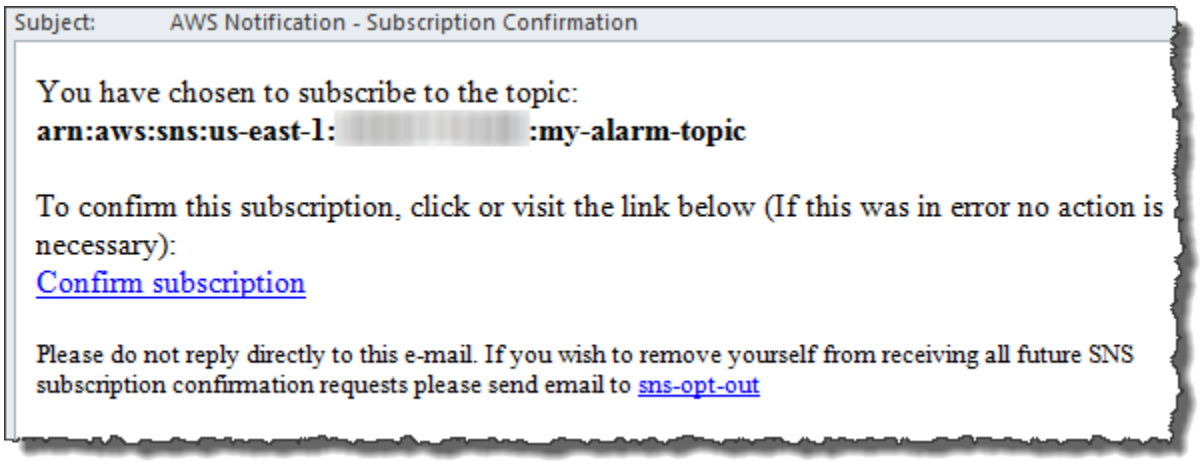
a. 경보 생성 마법사의 검토 페이지에서 경보 정의, 지표 및 수행할 관련 작업(예: 이메일 알림 전송)을 검토합니다.

b. 경보 요약을 검토한 후 Save Alarm(경보 저장)을 선택합니다.

7. 경보 주제에 대한 구독을 확인합니다.

a. 주제를 생성할 때 지정한 이메일 주소로 전송된 Amazon SNS 이메일을 엽니다.

다음 이미지는 일반적인 이메일 알림을 보여줍니다.



b. 이메일에 포함된 링크를 클릭하여 구독을 확인합니다.

   구독 확인 메시지가 표시됩니다.

캐시 스토리지 모니터링

아래와 같이 게이트웨이의 캐시 스토리지를 모니터링하는 방법과 경보를 생성하여 캐시의 파라미터가 지정한 임계값을 초과할 경우 알림을 받는 방법에 대한 정보를 얻을 수 있습니다. 이 경보를 통해 게이트웨이에 캐시 스토리지를 추가할 시점을 알 수 있습니다.

캐싱 볼륨 아키텍처에서는 캐시 스토리지만 모니터링합니다. 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 단원을 참조하십시오.

관심 항목	측정 방법
캐시 총 사용량	`CachePercentUsed` 통계와 함께 `TotalCacheSize` 및 `Average` 지표를 사용합니다. 예를 들어 `CachePercentUsed` 통계와 함께 `Average`를 사용하여 일정 기간 동안의 캐시 사용량을 분석합니다. `TotalCacheSize` 지표는 캐시를 게이트웨이에 추가할 때만 변합니다.
캐시에서 제공되는 읽기 요청의 백분율	`CacheHitPercent` 통계와 함께 `Average` 지표를 사용합니다. 대개의 경우 `CacheHitPercent` 를 높은 수준으로 유지하기를 바랍니다.
캐시 중 오염된 캐시 비율 (즉, 업로드되지	`CachePercentDirty` 통계와 함께 `Average` 지표를 사용합니다.

관심 항목	측정 방법
않은 콘텐츠가 포함되어 있음) AWS	대개의 경우 `CachePercentDirty` 를 낮은 수준으로 유지하기를 바랍니다.

게이트웨이 및 해당 모든 볼륨에 대해 더티인 캐시의 백분율을 측정하려면

1. 에서 콘솔을 엽니다. CloudWatch https://console.aws.amazon.com/cloudwatch/
2. StorageGateway: 게이트웨이 지표 차원을 선택하고 사용할 게이트웨이를 찾으십시오.
3. `CachePercentDirty` 지표를 선택합니다.
4. 시간 범위에서 값을 선택합니다.
5. `Average` 통계를 선택합니다.
6. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

그 결과로 얻은 시간순 데이터 포인트 집합은 5분 동안 변경된 캐시의 백분율을 포함합니다.

볼륨에 대해 더티인 캐시의 백분율을 측정하려면

1. 에서 CloudWatch 콘솔을 엽니다 https://console.aws.amazon.com/cloudwatch/.
2. StorageGateway: Volume Metrics 차원을 선택하고 사용하려는 볼륨을 찾으세요.
3. `CachePercentDirty` 지표를 선택합니다.
4. 시간 범위에서 값을 선택합니다.
5. `Average` 통계를 선택합니다.
6. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

그 결과로 얻은 시간순 데이터 포인트 집합은 5분 동안 변경된 캐시의 백분율을 포함합니다.

CloudWatch 알람에 대한 이해

CloudWatch 경보는 지표와 표현식을 기반으로 게이트웨이에 대한 정보를 모니터링합니다. Storage Gateway 콘솔에서 게이트웨이에 대한 CloudWatch 경보를 추가하고 상태를 볼 수 있습니다. Volume Gateway를 모니터링하는 데 사용되는 지표에 대한 자세한 내용은 게이트웨이 지표 이해 및 가상 테이프 지표 이해를 참조하세요. 각 경보에 대해 상태를 시작하는 조건을 지정합니다. ALARM 상태가 되면 Storage Gateway 콘솔의 경보 상태 표시등이 빨간색으로 바뀌므로 상태를 사전 예방적으로 모니터링

하기가 더 쉽습니다. ALARM 지속적인 상태 변화에 따라 자동으로 작업을 호출하도록 경보를 구성할 수 있습니다. CloudWatch 경보에 대한 자세한 내용은 Amazon 사용 CloudWatch 설명서의 Amazon CloudWatch 경보 사용을 참조하십시오.

> **Note**
>
> 보기 CloudWatch 권한이 없는 경우 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
- 상태 알림: 5분 이내에 1개의 데이터 포인트에 대해 `HealthNotifications` >= 1. 이 경보를 구성할 때는 누락된 데이터 처리를 로 notBreaching설정하십시오.

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

HA 모드가 활성화된 VMware 호스트 플랫폼의 게이트웨이의 경우 다음과 같은 추가 CloudWatch 경보도 사용하는 것이 좋습니다.

- 가용성 알림: 5분 이내에 1개의 데이터 포인트에 대해 `AvailabilityNotifications` >= 1. 이 경보를 구성할 때는 누락된 데이터 처리를 로 notBreaching설정하십시오.

다음 표에서는 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.
None(없음)	게이트웨이에 대한 경보가 생성되지 않습니다. 새 경보를 생성하려면 게이트웨이에 대한 사용자 지정 CloudWatch 알람 생성 단원을 참조하십시오.
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 Volume Gateway 구성을 참조하세요. 기존 게이트웨이에 대한 권장 CloudWatch 경보를 추가하거나 업데이트하려면 다음 절차를 사용하십시오.

기존 게이트웨이에 대한 권장 CloudWatch 경보를 추가하거나 업데이트하려면

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

1. https://console.aws.amazon.com/storagegateway/홈/에서 Storage Gateway 콘솔을 엽니다.

2. 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.

   Alarms 섹션에는 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 알람 생성

CloudWatch Amazon 심플 알림 서비스 (AmazonSNS) 를 사용하여 알람 상태가 변경될 때 알람 알림을 보냅니다. 경보는 지정한 기간 동안 단일 지표를 감시하고 여러 기간에 지정된 임계값에 대한 지표 값을 기준으로 작업을 하나 이상 수행합니다. 작업은 Amazon SNS 주제로 전송되는 알림입니다. CloudWatch 경보를 생성할 때 Amazon SNS 주제를 생성할 수 있습니다. Amazon에 대한 자세한 내용은 SNS Amazon이란 무엇입니까SNS? 를 참조하십시오. Amazon 심플 알림 서비스 개발자 가이드에서 확인할 수 있습니다.

Storage Gateway 콘솔에서 CloudWatch 경보를 생성하려면

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

   - 정적 임계값 경보: 선택한 지표에 대해 설정된 임계값을 기반으로 하는 경보입니다. 경보는 지표가 지정된 평가 기간 수의 임계값을 위반할 때 ALARM 상태가 됩니다.

     정적 임계값 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 정적 임계값을 기반으로 CloudWatch 경보 생성을 참조하십시오.
   - 이상 탐지 경보: 이상 탐지는 과거 지표 데이터를 마이닝하고 예상 값의 모델을 생성합니다. 예외 항목 탐지 임계값을 설정하고 이 임계값을 모델과 함께 CloudWatch 사용하여 지표의 “정상” 값 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.

예외 항목 탐지 경보를 생성하려면 Amazon 사용 설명서의 예외 항목 탐지에 기반한 CloudWatch 경보 생성을 참조하십시오. CloudWatch

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

  메트릭 수학 표현식 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 지표 수학 식을 기반으로 CloudWatch 경보 생성을 참조하십시오.

- 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 설명서의 복합 경보 생성을 참조하십시오.

6. CloudWatch 콘솔에서 경보를 생성한 후 Storage Gateway 콘솔로 돌아가십시오. 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.

     Alarms 섹션에는 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 경보 편집 또는 삭제를 CloudWatch 참조하십시오.

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

볼륨 게이트웨이 모니터링

이 단원에서는 게이트웨이에 연결된 볼륨 모니터링 및 업로드 버퍼 모니터링을 포함해 캐시 볼륨 또는 저장 볼륨 설정에서 게이트웨이를 모니터링하는 방법에 대해 설명합니다. 를 사용하여 게이트웨이의

메트릭을 볼 수 있습니다. AWS Management Console 예를 들어 읽기 및 쓰기 작업에 사용되는 바이트의 수, 읽기 및 쓰기 작업에 걸리는 시간, Amazon Web Services 클라우드에서 데이터를 가져오는 데 걸리는 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 비용 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이 지표를 사용하여 기록 정보에 액세스하고 게이트웨이와 볼륨이 어떻게 실행되고 있는지 더 잘 파악할 수 있습니다. 에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하십시오. CloudWatch

주제

- Amazon Logs로 볼륨 게이트웨이 상태 CloudWatch 로그 가져오기
- 아마존 CloudWatch 메트릭스 사용
- 애플리케이션과 게이트웨이 간 성능 측정
- 게이트웨이와 AWS간 성능 측정
- 볼륨 지표 이해

Amazon Logs로 볼륨 게이트웨이 상태 CloudWatch 로그 가져오기

Amazon CloudWatch Logs를 사용하여 볼륨 게이트웨이 및 관련 리소스의 상태에 대한 정보를 얻을 수 있습니다. 이러한 로그를 사용하여 게이트웨이에서 로그가 발생하는지 모니터링할 수 있습니다. 또한 Amazon CloudWatch 구독 필터를 사용하여 실시간으로 로그 정보 처리를 자동화할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 구독을 통한 로그 데이터의 실시간 처리를 참조하십시오.

예를 들어, VMware 고가용성(HA)이 활성화된 클러스터에 게이트웨이가 배포되어 있고 오류를 파악해야 하는 경우, 게이트웨이를 모니터링하고 게이트웨이에 오류가 발생할 경우 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 을 참조하십시오. Volume Gateway 구성 CloudWatch 로그 그룹에 대한 일반 정보는 Amazon CloudWatch 사용 설명서의 로그 그룹 및 로그 스트림 작업을 참조하십시오.

문제를 해결하고 이 오류 유형을 해결하는 방법에 대한 자세한 내용은 볼륨 문제 해결 단원을 참조하십시오.

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

게이트웨이와 함께 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 AWS Management Console 로그인하고 https://console.aws.amazon.com/storagegateway/home 에서 Storage Gateway 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 게이트웨이를 선택한 다음 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 작업에 대해 게이트웨이 정보 편집을 선택하거나 세부 정보 탭의 Health logs 및 Not Enabled에서 로그 그룹 구성을 선택하여 편집 ***CustomerGatewayName***대화 상자를 엽니다.
4. 게이트웨이 상태 로그 그룹에서 다음 중 하나를 선택합니다.
   - CloudWatch 로그 그룹을 사용하여 게이트웨이를 모니터링하지 않으려면 로깅을 비활성화하십시오.
   - 새 로그 그룹을 생성하여 새 CloudWatch 로그 그룹을 생성하십시오.
   - 기존 로그 그룹을 사용하여 이미 존재하는 CloudWatch 로그 그룹을 사용하십시오. 기존 로그 그룹 목록에서 로그 그룹을 선택합니다.
5. 변경 사항 저장를 선택합니다.
6. 게이트웨이의 상태 로그를 확인하려면 다음을 수행합니다.
   1. 왼쪽 탐색 창에서 Gateways를 선택한 다음 CloudWatch 로그 그룹을 구성한 게이트웨이를 선택합니다.
   2. 세부 정보 탭을 선택하고 Health logs에서 Logs (로그) 를 선택합니다CloudWatch . Amazon CloudWatch 콘솔에서 로그 그룹 세부 정보 페이지가 열립니다.

아마존 CloudWatch 메트릭스 사용

AWS Management Console 또는 CloudWatch API를 사용하여 게이트웨이에 대한 모니터링 데이터를 가져올 수 있습니다. 콘솔은 CloudWatch API의 원시 데이터를 기반으로 일련의 그래프를 표시합니다. AWS 소프트웨어 개발 키트 (SDK) 또는 Amazon CloudWatch API 도구 중 하나를 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`, `GatewayName`, `VolumeId`입니다. CloudWatch 콘솔에서 `Gateway Metrics` 및 `Volume Metrics` 보기를 사용하여 게이트웨이별 및 볼륨별 차원을 쉽게

선택할 수 있습니다. 치수에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 치수를 참조하십시오.

- `ReadBytes`와 같은 지표 이름.

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

CloudWatch 네임스페이스	측정기준	설명
`AWS/StorageGateway`	`GatewayId`, `GatewayName`	이 차원은 게이트웨이의 여러 측면을 설명하는 지표 데이터를 필터링합니다. `GatewayId` 및 `GatewayName` 차원을 모두 지정하여 작업할 게이트웨이를 식별할 수 있습니다. 게이트웨이의 처리량 및 지연 시간 데이터는 게이트웨이의 모든 볼륨에 기반을 두고 있습니다. 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.
	`VolumeId`	이 차원은 볼륨에 고유한 지표 데이터를 필터링합니다. `VolumeId` 차원을 사용하여 작업할 볼륨을 식별합니다. 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.

게이트웨이 및 볼륨 지표 작업은 기타 서비스 지표 작업과 유사합니다. 아래 나열된 CloudWatch 문서에서 가장 흔한 지표 작업 일부에 대한 논의를 보실 수 있습니다.

- 얻을 수 있는 지표 보기
- 지표에 대한 통계 구하기
- CloudWatch 경보 생성

애플리케이션과 게이트웨이 간 성능 측정

데이터 처리량, 데이터 지연 시간 및 초당 작업은 게이트웨이를 사용하고 있는 애플리케이션 스토리지가 어떤 성능을 나타내고 있는지 알기 위해 사용할 수 있는 세 가지 지표입니다. 정확한 집계 통계를 사용하는 경우 Storage Gateway 지표를 사용하여 이러한 값을 측정할 수 있습니다.

통계는 지정 기간에 걸친 지표를 집계한 것입니다. 에서 지표 값을 볼 때는 데이터 지연 시간 (밀리초) `Average` 통계를 사용하고 CloudWatch, 데이터 처리량 (초당 바이트) `Sum` 통계를 사용하고, 초당 입/출력 작업 수 (IOPS) `Samples` 통계를 사용합니다. 자세한 내용은 Amazon CloudWatch 사용 설명서의 통계를 참조하십시오.

다음 표는 애플리케이션과 게이트웨이 간 처리량, 지연 시간 및 IOPS를 측정하는 데 사용할 수 있는 지표와 해당 통계를 요약한 것입니다.

관심 항목	측정 방법
처리량	`ReadBytes` 통계와 함께 `WriteBytes` 및 Sum CloudWatch 지표를 사용합니다. 예를 들어 5분 동안의 샘플 시간에 걸친 `Sum` 지표의 `ReadBytes` 값을 300초로 나누면 초당 바이트 속도의 처리량이 나옵니다.
지연 시간	`ReadTime` 통계와 함께 `WriteTime` 및 `Average` CloudWatch 지표를 사용합니다. 예를 들어 `Average` 지표의 `ReadTime` 값은 샘플 시간에 걸친 작업당 지연 시간에 해당합니다.
IOPS	`ReadBytes` 통계와 함께 `WriteBytes` 및 `Samples` CloudWatch 지표를 사용합니다. 예를 들어 5분 동안의 샘플 시간에 걸친 `Samples` 지표의 `ReadBytes` 값을 300초로 나누면 IOPS가 됩니다.

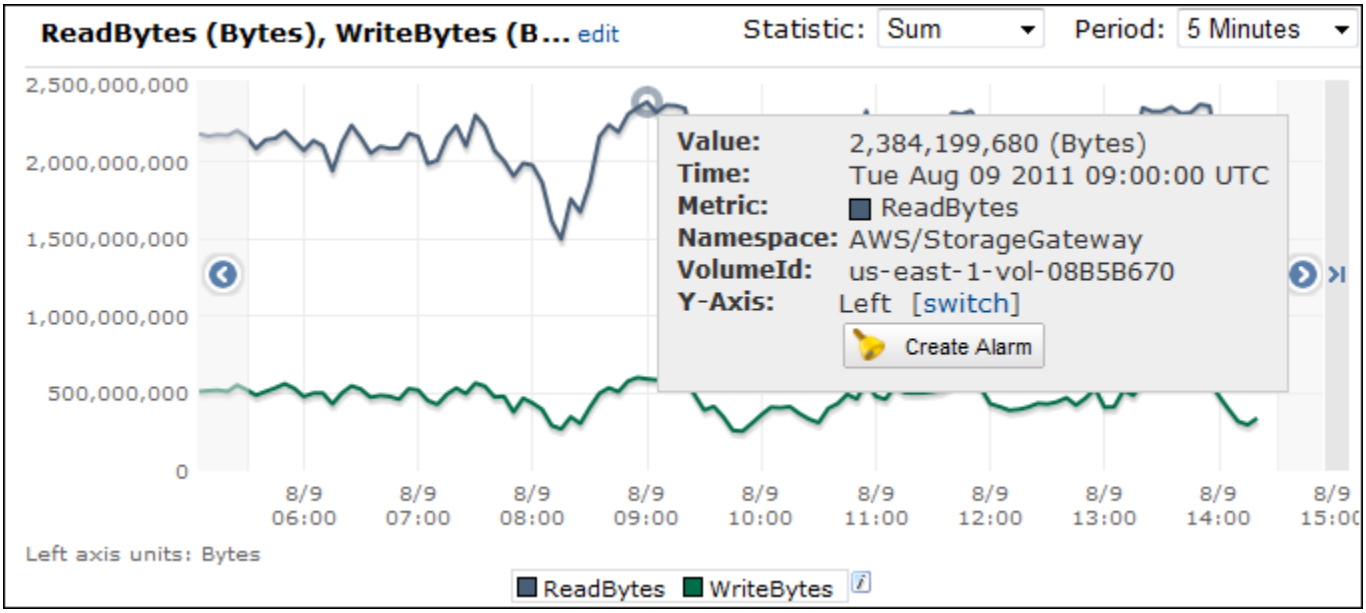
평균 지연 시간 그래프 및 평균 크기 그래프의 경우 기간 중 완료된 총 작업(그래프에 해당하는 읽기 또는 쓰기) 수를 기준으로 평균을 계산합니다.

애플리케이션에서 볼륨까지 데이터 처리량을 측정하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 측정치를 선택하고 모든 측정치 탭을 선택한 후 Storage Gateway를 선택합니다.
3. Volume metrics 차원을 선택한 후 작업할 볼륨을 찾습니다.
4. [`ReadBytes`] 및 [`WriteBytes`] 지표를 선택합니다.

5. 시간 범위에서 값을 선택합니다.
6. Sum 통계를 선택합니다.
7. 기간에서 5분 이상의 값을 선택합니다.
8. 그 결과로 얻은 시간순 데이터 포인트 집합(ReadBytes 및 WriteBytes에 대해 각각 하나씩)에서 각 데이터 포인트를 기간(초 단위)으로 나누어 샘플 포인트의 처리량을 얻습니다. 총 처리량은 각 처리양의 합계입니다.

다음 이미지는 ReadBytes 통계와 함께 한 볼륨에 대한 WriteBytes 및 Sum 지표입니다. 이 이미지에서 데이터 포인트 위에 놓인 커서는 값과 바이트 수를 포함한 데이터 포인트 정보를 표시합니다. 동일 포인트의 데이터 처리량을 얻으려면 바이트 값을 기간 값(5분)으로 나눕니다. 강조 표시한 포인트의 경우, 읽기 처리량은 2,384,199,680바이트이고, 이를 300초로 나누면 초당 7.6메가바이트입니다.

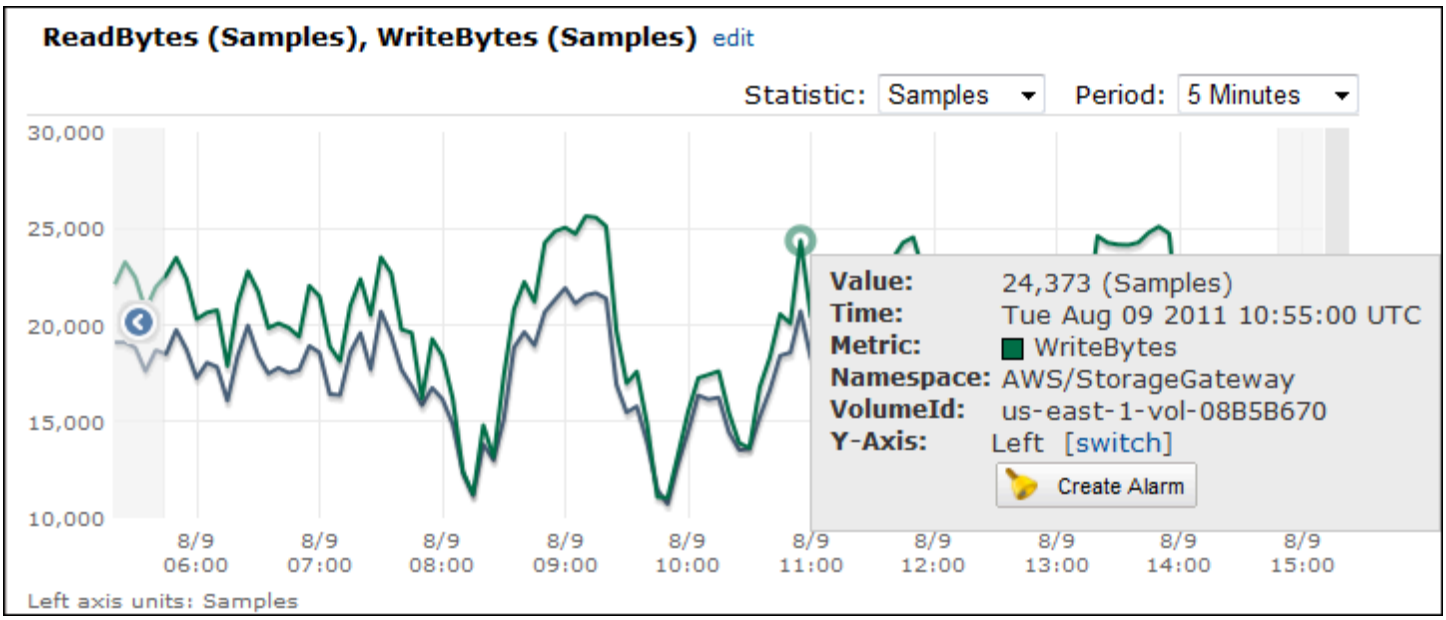


애플리케이션에서 볼륨까지 초당 데이터 입력/출력 작업을 측정하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 측정치를 선택하고 모든 측정치 탭을 선택한 후 Storage Gateway를 선택합니다.
3. Volume metrics 차원을 선택한 후 작업할 볼륨을 찾습니다.
4. [ReadBytes] 및 [WriteBytes] 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.
6. Samples 통계를 선택합니다.
7. 기간에서 5분 이상의 값을 선택합니다.

8. 그 결과로 얻은 시간순 데이터 포인트 집합(ReadBytes 및 WriteBytes에 대해 각각 하나씩)에서 각 데이터 포인트를 기간(초 단위)으로 나누어 IOPS를 얻습니다.

다음 이미지는 ReadBytes 통계와 함께 스토리지 하나에 대한 WriteBytes 및 Samples 지표입니다. 이 이미지에서 데이터 포인트 위에 놓인 커서는 값과 샘플 수를 포함한 데이터 포인트 정보를 표시합니다. 동일 포인트의 초당 작업을 얻으려면 샘플 값을 기간 값(5분)으로 나눕니다. 강조 표시한 포인트의 경우, 쓰기 작업의 수는 24,373바이트이고, 이를 300초로 나누면 초당 쓰기 작업은 81건입니다.



게이트웨이와 AWS간 성능 측정

데이터 처리량, 데이터 지연 시간 및 초당 작업은 Storage Gateway를 사용하는 애플리케이션 스토리지의 성능을 파악하는 데 사용할 수 있는 세 가지 지표입니다. 이 세 가지 값은 정확한 집계 통계를 사용할 때 제공되는 Storage Gateway 지표를 사용하여 측정할 수 있습니다. 다음 표는 게이트웨이와 AWS간 처리량, 지연 시간 및 초당 입출력 작업 처리량(IOPS)을 측정하는 데 사용할 지표와 해당 통계를 요약한 것입니다.

관심 항목	측정 방법
처리량	ReadBytes 통계와 함께 WriteBytes 및 Sum CloudWatch 지표를 사용합니다. 예를 들어 5분 동안의 샘플 시간에 걸친 Sum 지표의 ReadBytes 값을 300초로 나누면 초당 바이트 속도의 처리량이 나옵니다.

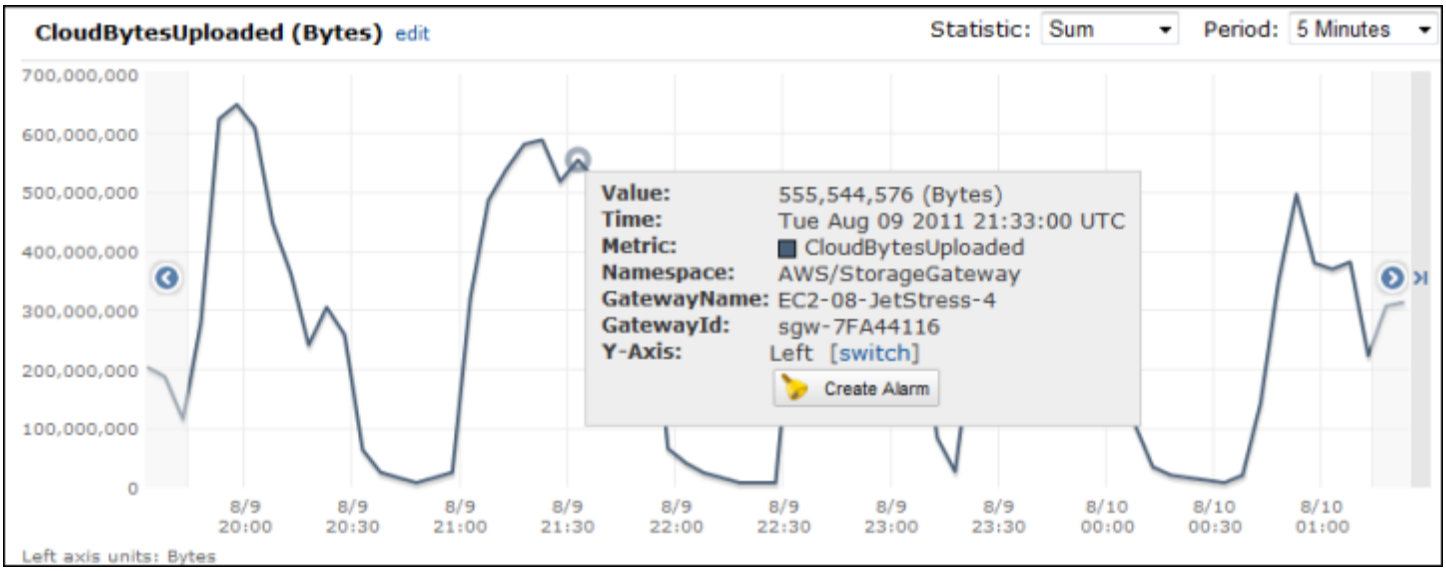
관심 항목	측정 방법
지연 시간	`ReadTime` 통계와 함께 `WriteTime` 및 `Average` CloudWatch 지표를 사용합니다. 예를 들어 `Average` 지표의 `ReadTime` 값은 샘플 시간에 걸친 작업당 지연 시간에 해당합니다.
IOPS	`ReadBytes` 통계와 함께 `WriteBytes` 및 `Samples` CloudWatch 지표를 사용합니다. 예를 들어 5분 동안의 샘플 시간에 걸친 `Samples` 지표의 `ReadBytes` 값을 300초로 나누면 IOPS가 됩니다.
처리량은 AWS	`Sum` CloudWatch 통계와 함께 `CloudBytesDownloaded` 및 `CloudBytesUploaded` 지표를 사용하십시오. 예를 들어, 샘플 기간 5분 동안의 `CloudBytesDownloaded` 지표 `Sum` 값을 300초로 나눈 값은 게이트웨이에서 AWS 전송되는 처리량을 초당 바이트 수로 나타냅니다.
데이터 지연 시간: AWS	`CloudDownloadLatency` 통계와 함께 `Average` 지표를 사용합니다. 예를 들어 `Average` 지표의 `CloudDownloadLatency` 통계는 작업당 지연 시간에 해당합니다.

게이트웨이에서 다음으로 향하는 업로드 데이터 처리량을 측정하려면 AWS

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 측정치를 선택하고 모든 측정치 탭을 선택한 후 Storage Gateway를 선택합니다.
3. 게이트웨이 지표 차원을 선택한 후 작업할 볼륨을 찾습니다.
4. `CloudBytesUploaded` 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.
6. `Sum` 통계를 선택합니다.
7. 기간에서 5분 이상의 값을 선택합니다.
8. 그 결과로 얻은 시간순 데이터 포인트 집합에서 각 데이터 포인트를 기간(초 단위)으로 나누어 샘플 기간의 처리량을 얻습니다.

다음 이미지는 `CloudBytesUploaded` 통계와 함께 게이트웨이 볼륨에 대한 `Sum` 지표입니다. 이 이미지에서 데이터 포인트 위에 놓인 커서는 값과 업로드한 바이트 수를 포함한 데이터 포인트 정보를 표시합니다. 동일 포인트의 데이터 처리량을 얻으려면 이 값을 기간 값(5분)으로 나눕니다. 강조 표시된

지점의 경우, 게이트웨이에서 까지의 AWS 처리량은 555,544,576바이트를 300초로 나눈 값이며, 이는 초당 1.7메가바이트입니다.



게이트웨이의 작업당 지연 시간을 측정하려면

1. https://console.aws.amazon.com/cloudwatch/ 에서 콘솔을 엽니다. CloudWatch
2. 측정치를 선택하고 모든 측정치 탭을 선택한 후 Storage Gateway를 선택합니다.
3. 게이트웨이 지표 차원을 선택한 후 작업할 볼륨을 찾습니다.
4. [ReadTime] 및 [WriteTime] 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.
6. Average 통계를 선택합니다.
7. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.
8. 그 결과로 얻은 시간순 포인트 집합(ReadTime 및 WriteTime에 대해 각각 하나씩)에서 동일한 시간 샘플의 데이터 포인트를 더해 밀리초 단위의 총 지연 시간을 얻습니다.

게이트웨이에서의 데이터 지연 시간을 측정하려면 AWS

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 측정치를 선택하고 모든 측정치 탭을 선택한 후 Storage Gateway를 선택합니다.
3. 게이트웨이 지표 차원을 선택한 후 작업할 볼륨을 찾습니다.
4. CloudDownloadLatency 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.

6. Average 통계를 선택합니다.
7. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

그 결과로 얻은 데이터 포인트 집합은 밀리초 단위의 지연 시간을 포함합니다.

게이트웨이 처리량에 대한 상한 임계값 경보를 다음과 같이 설정하려면 AWS

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 경보를 선택합니다.
3. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
4. Storage Gateway 차원을 선택한 후 작업할 게이트웨이를 찾습니다.
5. CloudBytesUploaded 지표를 선택합니다.
6. 경보를 정의하려면 CloudBytesUploaded 지표가 지정한 시간 동안 지정한 값보다 크거나 같을 때 경보 상태를 정의합니다. 예를 들어 CloudBytesUploaded 지표가 60분 동안 10MB보다 클 때 경보 상태를 정의할 수 있습니다.
7. 경보 상태에 대해 취할 조치를 구성합니다. 예를 들어 이메일 알림이 전송되도록 할 수 있습니다.
8. 경보 생성을 선택합니다.

에서 데이터를 읽을 때 상한 임계값 경보를 설정하려면 AWS

1. https://console.aws.amazon.com/cloudwatch/ 에서 CloudWatch 콘솔을 엽니다.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. StorageGateway: 게이트웨이 메트릭 차원을 선택하고 사용할 게이트웨이를 찾으십시오.
4. CloudDownloadLatency 지표를 선택합니다.
5. CloudDownloadLatency 지표가 지정한 시간 동안 지정한 값보다 크거나 같을 때 경보 상태를 정의하여 경보를 정의합니다. 예를 들어 CloudDownloadLatency가 2시간 이상의 시간 동안 60,000밀리초보다 클 때 경보 상태를 정의할 수 있습니다.
6. 경보 상태에 대해 취할 조치를 구성합니다. 예를 들어 이메일 알림이 전송되도록 할 수 있습니다.
7. 경보 생성을 선택합니다.

볼륨 지표 이해

게이트웨이의 볼륨을 나타내는 Storage Gateway 지표에 대한 정보는 다음에서 확인할 수 있습니다. 게이트웨이의 각 볼륨에는 연결된 지표 집합이 있습니다.

일부 볼륨별 지표는 특정 게이트웨이별 지표와 이름이 같습니다. 이 지표는 같은 종류의 측정값을 나타내지만 게이트웨이가 아닌 볼륨에 한정됩니다. 작업을 시작하기 전에 게이트웨이 지표로 작업할지 아니면 볼륨 지표로 작업할지를 지정합니다. 특히 볼륨 지표로 작업할 때는 지표를 보려는 스토리지 볼륨의 볼륨 ID를 지정합니다. 자세한 설명은 아마존 CloudWatch 메트릭스 사용 섹션을 참조하세요.

> **Note**
>
> 일부 지표는 가장 최근 모니터링 기간 동안 새 데이터가 생성된 경우에만 데이터 포인트를 반환합니다.

다음 표에서는 스토리지 볼륨에 대한 정보를 얻는 데 사용할 수 있는 Storage Gateway 지표에 대해 설명합니다.

지표	설명	캐싱 볼륨	저장 볼륨
`AvailabilityNotification`	볼륨에서 보낸 사용 가능성 알림 수입니다. 단위: 개수	예	예
`CacheHitPercent`	캐시로부터 읽는 볼륨의 애플리케이션 읽기 작업 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 볼륨으로부터의 애플리케이션 읽기 작업이 없는 경우, 지표가 100%를 보고합니다. 단위: 백분율	예	아니요
`CachePercentDirty`	AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율 중 볼륨이 차지하는 비중입니다.	예	예

지표	설명	캐싱 볼륨	저장 볼륨
	보고 기간 종료 시점에서 샘플이 채취됩니다. 게이트웨이의 CachePercentDirty 지표를 사용하면 AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율을 알 수 있습니다. 자세한 설명은 게이트웨이 지표 이해 섹션을 참조하세요. 단위: 백분율		
CachePercentUsed	게이트웨이의 캐시 스토리지의 전체 사용 백분율 중 볼륨이 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 게이트웨이의 CachePercentUsed 지표를 사용하면 게이트웨이의 캐시 스토리지의 전체 사용 백분율을 알 수 있습니다. 자세한 설명은 게이트웨이 지표 이해 섹션을 참조하세요. 단위: 백분율	예	아니요

지표	설명	캐싱 볼륨	저장 볼륨
CloudBytesDownloaded	클라우드에서 볼륨으로 다운로드된 바이트 수입니다. 단위: 바이트	예	예
CloudBytesUploaded	클라우드에서 볼륨으로 업로드된 바이트 수입니다. 단위: 바이트	예	예
HealthNotification	볼륨에서 보낸 상태 알림 수입니다. 단위: 개수	예	예
IoWaitPercent	볼륨에서 현재 사용하고 있는 IoWaitPercent 단위의 비율입니다. 단위: 백분율	예	예
MemTotalBytes	볼륨에서 현재 사용 중인 총 메모리의 백분율입니다. 단위: 백분율	예	아니요
MemoryUsage	볼륨에서 현재 사용 중인 메모리의 백분율입니다. 단위: 백분율	예	아니요

지표	설명	캐싱 볼륨	저장 볼륨
ReadBytes	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	예	예
ReadTime	보고 기간 동안 온프레미스 애플리케이션으로부터 읽기 작업을 하는 데 소요된 총 밀리초 수입니다. 이 지표를 Average 통계와 함께 사용하면 지연 시간을 측정할 수 있습니다. 단위: 밀리초	예	예
UserCpuPercent	볼륨에서 현재 사용 중인 할당된 CPU 계산 단위의 백분율입니다. 단위: 백분율	예	예

지표	설명	캐싱 볼륨	저장 볼륨
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	예	예
WriteTime	보고 기간 동안 온프레미스 애플리케이션으로부터 쓰기 작업을 하는 데 소요된 총 밀리초 수입니다. 이 지표를 Average 통계와 함께 사용하면 지연 시간을 측정할 수 있습니다. 단위: 밀리초	예	예
QueuedWrites	보고 기간 말에 샘플링한 AWS, 쓰기 대기 중인 바이트 수입니다. 단위: 바이트	예	예

게이트웨이 유지 관리

게이트웨이 유지 관리에는 캐시 스토리지 및 업로드 버퍼 공간 구성, 게이트웨이 성능에 대한 일반적인 유지 관리 작업이 포함됩니다. 이 작업은 모든 게이트웨이 유형에 공통된 것입니다. 게이트웨이를 생성하지 않았으면 게이트웨이 생성 단원을 참조하십시오.

주제

게이트웨이 VM 종료

하이퍼바이저에 패치를 적용할 때와 같이 유지 관리용 VM을 종료하거나 재부팅해야 할 수도 있습니다. VM을 종료하기 전에 게이트웨이를 중지해야 합니다. File Gateway의 경우, VM만 종료합니다. 이 섹션에서는 Storage Gateway Management 콘솔을 사용하여 게이트웨이를 시작하고 중지하는 데 중점을 두지만 VM 로컬 콘솔 또는 Storage Gateway를 사용하여 게이트웨이를 중지할 수도 API 있습니다. VM을 켜면 게이트웨이를 다시 시작해야 합니다.

Important

임시 스토리지를 사용하는 Amazon EC2 게이트웨이를 중지했다가 시작하면 게이트웨이는 영구적으로 오프라인 상태가 됩니다. 이는 물리적 스토리지 디스크가 대체되기 때문에 발생합니다. 이 문제에 대한 해결 방법은 없습니다. 유일한 해결 방법은 게이트웨이를 삭제하고 새 인스턴스에서 새 게이트웨이를 활성화하는 것입니다. EC2

Note

백업 소프트웨어가 테이프에서 쓰거나 읽는 동안 게이트웨이를 중지하면 쓰기 또는 읽기 작업이 실패할 수 있습니다. 게이트웨이를 중지하기 전에 백업 소프트웨어와 진행 중인 작업의 백업 일정을 확인해야 합니다.

- 게이트웨이 VM 로컬 콘솔 - 기본 자격 증명을 사용하여 로컬 콘솔에 로그인 섹션을 참조하세요.
- Storage Gateway API —참조 ShutdownGateway

File Gateway의 경우, VM만 종료합니다. 게이트웨이를 종료하지 마십시오.

Volume Gateway 시작 및 중지

a Volume Gateway를 중지하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 중지할 게이트웨이를 선택합니다. 게이트웨이 상태는 실행 중입니다.
3. 작업에서 게이트웨이 중지를 선택하고 대화 상자에서 게이트웨이의 ID를 확인한 후 게이트웨이 중지를 선택합니다.

   게이트웨이가 중지되는 동안 게이트웨이의 상태를 표시하는 메시지가 표시될 수 있습니다. 게이트웨이가 종료되면 세부 정보 탭에 메시지와 게이트웨이 시작 버튼이 나타납니다.

게이트웨이를 중지하면 스토리지를 시작할 때까지 스토리지 리소스에 액세스할 수 없습니다. 게이트웨이가 중지될 때 데이터를 업로드 중이었다면 게이트웨이를 시작하면 업로드가 재개됩니다.

a Volume Gateway를 시작하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 시작할 게이트웨이를 선택합니다. 게이트웨이 상태는 종료입니다.
3. 세부 정보를 선택한 다음 게이트웨이 시작을 선택합니다.

Storage Gateway의 로컬 디스크 관리

게이트웨이 가상 머신(VM)은 버퍼링 및 스토리지에 온프레미스로 할당하는 로컬 디스크를 사용합니다. Amazon EC2 인스턴스에서 생성된 게이트웨이는 Amazon EBS 볼륨을 로컬 디스크로 사용합니다.

주제

- 로컬 디스크 스토리지 용량 결정
- 할당할 업로드 버퍼의 크기 결정

- 할당할 캐시 스토리지의 크기 결정
- 추가 업로드 버퍼 또는 캐시 스토리지 구성

로컬 디스크 스토리지 용량 결정

게이트웨이에 할당하려는 디스크의 개수 및 크기는 사용자가 직접 결정합니다. 배포하는 스토리지 솔루션에 따라(Storage Gateway 배포 계획 단원 참조) 게이트웨이에는 다음과 같은 추가 스토리지가 필요합니다.

- Volume Gateway:
  - 저장된 게이트웨이에는 업로드 버퍼로 사용할 디스크가 한 개 이상 필요합니다.
  - 캐싱 게이트웨이에는 디스크가 두 개 이상 필요합니다. 하나는 캐시로 사용하고 다른 하나는 업로드 버퍼로 사용합니다.

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다. 게이트웨이를 설정한 후, 그리고 워크로드 요구의 증가에 따라 로컬 스토리지를 추가할 수 있습니다.

로컬 스토리지	설명	
업로드 버퍼	업로드 버퍼는 게이트웨이가 Amazon S3에 데이터를 업로드하기 전에 데이터를 위한 스테이징 영역을 제공합니다. 게이트웨이는 암호화된 Secure Sockets Layer (SSL) 연결을 통해 이 버퍼 데이터를 업로드합니다. AWS	
캐시 스토리지	캐시 스토리지는 업로드 버퍼에서 Amazon S3로 업로드 보류 중인 데이터를 위한 온프레미스 내구성 저장소 역할을 합니다. 애플리케이션이 볼륨 또는 테이프에서 I/O를 수행하는 경우, 게이트웨이는 지연 시간이 짧은 액세스를 위해 데이터를 캐시 스토리지에 저장합니다. 애플리케이션이 볼륨 또는 테이프에	

로컬 스토리지	설명	
	데이터를 요청하면 게이트웨이는 AWS에서 데이터를 다운로드하기 전에 우선 캐시 스토리지에서 데이터를 확인합니다.	

> **Note**
>
> 디스크를 프로비저닝할 때 동일한 물리 리소스(동일한 디스크)를 사용하는 경우에는 업로드 버퍼 및 캐시 스토리지에 로컬 디스크를 프로비저닝하지 말 것을 적극 권장합니다. 기본 물리적 스토리지 리소스는 의 데이터 저장소로 표시됩니다. VMware 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 로컬 디스크를 프로비저닝하는 경우(예: 캐시 스토리지 또는 업로드 버퍼 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 개, 업로드 버퍼에 다른 데이터 스토어 한 개씩 선택할 것을 적극 권장합니다. 오직 기본 물리 디스크 한 개의 지원을 받는 데이터 스토어는 캐시 스토리지와 업로드 버퍼를 모두 지원하는 데 사용되는 경우 성능이 떨어질 수 있습니다. 백업이 다음과 같이 성능이 떨어지는 RAID 구성인 경우에도 마찬가지입니다. RAID1

해당 게이트웨이의 초기 구성 및 배포 후에는 업로드 버퍼용 디스크를 추가 또는 제거하여 로컬 스토리지를 조정할 수 있습니다. 또한 캐시 스토리지용 디스크를 추가하는 것도 가능합니다.

할당할 업로드 버퍼의 크기 결정

업로드 버퍼 공식을 사용하여 할당할 업로드 버퍼의 크기를 결정할 수 있습니다. 업로드 버퍼에 최소 150GiB를 할당할 것을 적극 권장합니다. 공식이 150GiB 미만의 값을 반환하는 경우, 150GiB를 업로드 버퍼에 할당하는 크기로 사용합니다. 각 게이트웨이에 업로드 버퍼 용량을 최대 2TiB까지 구성할 수 있습니다.

> **Note**
>
> Volume Gateways의 경우 업로드 버퍼가 용량에 도달하면 볼륨이 상태로 PASS THROUGH 전환됩니다. 이 상태에서는 애플리케이션이 쓰는 새 데이터가 로컬에 AWS 유지되지만 즉시 업로드되지는 않습니다. 따라서 새 스냅샷을 만들 수 없습니다. 업로드 버퍼 용량이 확보되면

볼륨은 상태가 됩니다. BOOTSTRAPPING 이 상태에서는 로컬에 보관된 새 데이터가 모두 업로드됩니다. AWS마지막으로 볼륨이 ACTIVE 상태로 돌아갑니다. 그러면 Storage Gateway가 로컬에 저장된 데이터와 저장된 복제본의 정상적인 동기화를 재개하여 새 스냅샷 생성을 시작할 수 있습니다. AWS볼륨 상태에 대한 자세한 내용은 볼륨 상태 및 전환 이해 단원을 참조하십시오.

할당할 업로드 버퍼의 크기를 추산하기 위해 예상 수신 및 송신 데이터 속도를 파악하여 이를 다음 공식에 대입합니다.

수신 데이터 속도

이 속도는 애플리케이션 처리량을 가리킵니다. 즉 온프레미스 애플리케이션이 일정 기간 동안 해당 게이트웨이에 데이터를 쓰는 속도를 말합니다.

송신 데이터 속도

이 속도는 네트워크 처리량을 가리킵니다. 즉 게이트웨이가 데이터를 AWS에 업로드할 수 있는 속도를 말합니다. 이 속도는 네트워크 속도, 사용률 및 대역폭 조절 기능 활성화 여부에 따라 달라집니다. 이 속도는 압축에 맞게 조정해야 합니다. 에 데이터를 업로드할 때 게이트웨이는 가능한 AWS경우 데이터 압축을 적용합니다. 예를 들어 애플리케이션 데이터가 텍스트만으로 되어 있는 경우, 약 2:1의 효과적인 압축 비율을 얻을 수 있습니다. 그러나 동영상을 작성하는 경우, 게이트웨이가 데이터 압축을 완료할 수 없고 게이트웨이에 더 많은 업로드 버퍼가 필요할 수 있습니다.

다음 중 하나가 true인 경우 적어도 150GiB의 업로드 버퍼 공간을 할당하는 것이 좋습니다.

- 수신 요금이 발신 요금보다 높습니다.
- 수식은 150GiB 미만의 값을 반환합니다.

$$\left(\text{Application Throughput (MB/s)} - \text{Network Throughput to AWS (MB/s)} \times \text{Compression Factor}\right) \times \text{Duration of writes (s)} = \text{Upload Buffer (MB)}$$

예를 들어, 비즈니스 애플리케이션이 게이트웨이에 텍스트 데이터를 초당 40MB로 매일 12시간 작성하며 네트워크 처리량은 초당 12MB라고 가정합니다. 텍스트 데이터의 압축비가 2:1이라고 가정할 때 업로드 버퍼용 공간으로 약 690GiB를 할당합니다.

Example

```
((40 MB/sec) - (12 MB/sec * 2)) * (12 hours * 3600 seconds/hour) = 691200 megabytes
```

처음에는 이 근사치를 사용하여 게이트웨이에 업로드 버퍼 공간으로 할당할 디스크 크기를 결정할 수 있습니다. 필요한 경우 Storage Gateway 콘솔을 사용하여 업로드 버퍼 공간을 더 추가할 수 있습니다. 또한 Amazon CloudWatch 운영 지표를 사용하여 업로드 버퍼 사용량을 모니터링하고 추가 스토리지 요구 사항을 결정할 수 있습니다. 측정치 및 경보 설정에 대한 정보는 업로드 버퍼 모니터링 단원을 참조하십시오.

할당할 캐시 스토리지의 크기 결정

게이트웨이는 최근에 액세스한 데이터에 대한 액세스 지연 시간을 줄이기 위해 자체 캐시 스토리지를 사용합니다. 캐시 스토리지는 업로드 버퍼에서 Amazon S3로 업로드 보류 중인 데이터를 위한 온프레미스 내구성 저장소 역할을 합니다. 일반적으로 말하자면 캐시 스토리지의 크기를 업로드 버퍼 크기의 1.1배로 조정합니다. 캐시 스토리지 크기를 추산하는 방법에 대한 자세한 내용은 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오.

초기에는 이 근사치를 사용하여 캐시 스토리지용 디스크를 프로비저닝할 수 있습니다. 그런 다음 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 캐시 스토리지 모니터링 단원을 참조하십시오.

추가 업로드 버퍼 또는 캐시 스토리지 구성

애플리케이션 요구 사항이 변화함에 따라 게이트웨이의 업로드 버퍼 또는 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 캐시 또는 업로드 버퍼를 추가할 때는 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에 새 디스크를 생성해야 합니다. 캐시 또는 업로드 버퍼로 이미 할당된 기존 디스크의 크기는 제거하거나 변경하지 마세요.

게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면

1. 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에 새 디스크를 하나 이상 프로비저닝합니다. 하이퍼바이저에서 디스크를 프로비저닝하는 방법에 대한 자세한 내용은 해당 하이퍼바이저의 설명서를 참조하세요. Amazon 인스턴스용 Amazon EBS 볼륨 프로비저닝에 대한 자세한 내용은 Linux EC2 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EBS 볼륨을 참조하십시오. 다음 단계에서는 이 디스크를 업로드 버퍼 또는 캐시 스토리지로 구성합니다.
2. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
3. 탐색 창에서 게이트웨이를 선택합니다.
4. 게이트웨이를 검색하고 목록에서 선택합니다.
5. 작업 메뉴에서 스토리지 구성을 선택합니다.
6. 스토리지 구성 섹션에서 프로비저닝한 디스크를 지정합니다. 디스크가 표시되지 않으면 새로 고침 아이콘을 선택하여 목록을 새로 고칩니다. 각 디스크에 대해 할당 대상 드롭다운 메뉴에서 하나 UPLOADBUFFER또는 CACHESTORAGE하나를 선택합니다.

   > **Note**
   >
   > UPLOADBUFFER저장 볼륨 게이트웨이에 디스크를 할당하는 데 사용할 수 있는 유일한 옵션입니다.

7. 변경 사항 저장을 선택하여 구성 설정을 저장합니다.

Volume Gateway의 대역폭 관리

게이트웨이에서 게이트웨이로의 업로드 처리량 또는 게이트웨이로의 다운로드 처리량을 제한 (AWS 또는 조절) AWS 할 수 있습니다. 대역폭 조절을 사용하면 게이트웨이가 사용하는 네트워크 대역폭의 전송량을 통제하는 데 도움이 됩니다. 기본적으로 활성화된 게이트웨이는 업로드 또는 다운로드에 대한 속도 제한이 없습니다.

속도 제한은 를 사용하거나 Storage Gateway API (참조 UpdateBandwidthRateLimit) 또는 AWS 소프트웨어 개발 키트 (SDK) 를 사용하여 프로그래밍 방식으로 지정할 수 있습니다. AWS Management Console프로그래밍 방식으로 대역폭을 조절하면 작업을 예약하여 대역폭을 변경하는 등의 방식으로 하루 종일 자동으로 제한을 변경할 수 있습니다.

게이트웨이에 대해 일정 기반 대역폭 조절을 정의할 수도 있습니다. 하나 이상의 간격을 정의하여 대역폭 제한을 예약합니다. bandwidth-rate-limit 자세한 내용은 Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절 단원을 참조하십시오.

대역폭 조절을 위한 단일 설정을 구성하는 것은 매일에 대해 단일 bandwidth-rate-limit 간격을 설정하고 시작 시간과 종료 시간을 1로 하여 일정을 정의하는 것과 동일한 기능입니다. **00:00** 23:59

> **Note**
>
> 이 섹션의 정보는 Tape Gateway 및 Volume Gateway에만 해당됩니다. Amazon S3 File Gateway의 대역폭을 관리하려면 Amazon S3 File Gateway의 대역폭 관리를 참조하세요. Amazon FSx File Gateway에서는 현재 대역폭 속도 제한이 지원되지 않습니다.

주제

Storage Gateway 콘솔을 사용하여 대역폭 조절 변경

다음은 Storage Gateway 콘솔에서 게이트웨이의 대역폭 조절을 변경하는 방법을 보여주는 절차입니다.

콘솔을 사용하여 게이트웨이의 대역폭 조절을 변경하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 게이트웨이를 선택한 다음 관리할 게이트웨이를 선택합니다.
3. 작업에서 대역폭 제한 편집을 선택합니다.
4. 속도 제한 편집 대화 상자에서 새 제한 값을 입력한 다음 저장을 선택합니다. 변경 사항은 해당 게이트웨이의 세부 정보 탭에 표시됩니다.

Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절

다음은 Storage Gateway 콘솔에서 게이트웨이의 대역폭 조절 변경을 예약하는 방법을 보여 줍니다.

게이트웨이 대역폭 조절 일정을 추가 또는 수정하려면

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

   게이트웨이의 bandwidth-rate-limit 일정은 대역폭 속도 제한 스케줄 편집 대화 상자에 표시됩니다. 기본적으로 새 게이트웨이 bandwidth-rate-limit 일정은 비어 있습니다.
4. 대역폭 속도 제한 일정 편집 대화 상자에서 새 항목 추가를 선택하여 새 bandwidth-rate-limit 간격을 추가합니다. 각 bandwidth-rate-limit 간격에 대해 다음 정보를 입력합니다.

   - 요일 - 주중 (월요일부터 금요일까지), 주말 (토요일과 일요일), 요일별 또는 하나 이상의 특정 요일에 대한 bandwidth-rate-limit 간격을 생성할 수 있습니다.
   - 시작 시간 - 대역폭 간격의 시작 시간을 게이트웨이의 현지 시간대(HH:MM 형식)로 입력합니다.

     > **Note**
     >
     > bandwidth-rate-limit 간격은 여기에 지정한 분의 시작부터 시작됩니다.

   - 종료 시간 - HH:MM 형식을 사용하여 해당 bandwidth-rate-limit 간격의 종료 시간을 게이트웨이의 현지 시간대로 입력합니다.

     > **Important**
     >
     > bandwidth-rate-limit 간격은 여기에 지정된 분 말일에 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.

   - 다운로드 속도 - 다운로드 속도 제한을 초당 킬로비트(Kbps) 단위로 입력하거나 제한 없음을 선택하여 다운로드를 위한 대역폭 조절을 비활성화합니다. 다운로드 속도의 최소값은 100Kbps입니다.
   - 업로드 속도 - 업로드 속도 제한을 Kbps 단위로 입력하거나 제한 없음을 선택하여 업로드를 위한 대역폭 조절을 비활성화합니다. 업로드 속도의 최소값은 50Kbps입니다.

   bandwidth-rate-limit 간격을 수정하려면 간격 매개변수에 수정된 값을 입력할 수 있습니다.

bandwidth-rate-limit 간격을 제거하려면 삭제할 구간의 오른쪽에 있는 제거를 선택하면 됩니다.

변경을 완료했으면 저장을 선택합니다.

5. 새 항목 추가를 선택하고 날짜, 시작 및 종료 시간, 다운로드 및 업로드 속도 제한을 입력하여 bandwidth-rate-limit 간격을 계속 추가합니다.

> **Important**
>
> B andwidth-rate-limit 간격은 겹칠 수 없습니다. 간격의 시작 시간은 이전 간격의 종료 시간 이후, 다음 간격의 시작 시간 이전이어야 합니다.

6. 모든 bandwidth-rate-limit 간격을 입력한 후 변경 사항 저장을 선택하여 bandwidth-rate-limit 일정을 저장합니다.

bandwidth-rate-limit 일정이 성공적으로 업데이트되면 게이트웨이의 디테일 패널에서 현재 다운로드 및 업로드 속도 제한을 확인할 수 있습니다.

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 및 다운로드 한도를 제공해야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

```
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.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;
```

```
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 = 51200;  // Bits per second, minimum 51200
    static long downloadRate = 102400;   // Bits per second, minimum 102400

    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, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
            long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                new UpdateBandwidthRateLimitRequest()
                .withGatewayARN(gatewayARN)
                .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
                .withAverageUploadRateLimitInBitsPerSec(uploadRate);

            UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
 sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
            String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
            System.out.println("Updated the bandwidth rate limits of " +
 returnGatewayARN);
```

```
            System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
 second");
            System.out.println("Download bandwidth limit = " + downloadRate + " 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 예시는 AWS SDK for .NET를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예제 코드를 사용하려면 a 실행에 익숙해야 합니다. NET콘솔 애플리케이션. 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 및 다운로드 한도를 제공해야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

```
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 = 51200;  // Bits per second, minimum 51200
        static long downloadRate = 102400;   // Bits per second, minimum 102400

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
downloadRate)
        {
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " 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. 예제 코드를 사용하려면 PowerShell 스크립트 실행에 익숙해야 합니다. 자세한 내용은 AWS Tools for Windows PowerShell 사용 설명서에서 시작하기를 참조하세요.

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

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

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

.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 = 51200
```

```
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

#Update Bandwidth Rate Limits
Update-SGBandwidthRateLimit -GatewayARN $gatewayARN `
                            -AverageUploadRateLimitInBitsPerSec $UploadBandwidthRate `
                            -AverageDownloadRateLimitInBitsPerSec
 $DownloadBandwidthRate

$limits =  Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

Write-Output("`nGateway: " + $gatewayARN);
Write-Output("`nNew Upload Rate: " + $limits.AverageUploadRateLimitInBitsPerSec)
Write-Output("`nNew Download Rate: " + $limits.AverageDownloadRateLimitInBitsPerSec)
```

게이트웨이 업데이트 관리

Storage Gateway는 관리형 클라우드 서비스 구성 요소와 게이트웨이 어플라이언스 구성 요소로 구성되어 있으며, 이 구성 요소는 온프레미스 또는 AWS 클라우드의 Amazon EC2 인스턴스에 배포합니다. 두 구성 요소 모두 정기적인 업데이트를 받습니다. 이 섹션의 항목에서는 이러한 업데이트의 주기, 적용 방법, 배포의 게이트웨이에서 업데이트 관련 설정을 구성하는 방법에 대해 설명합니다.

> **Important**
>
> Storage Gateway 어플라이언스는 관리형 가상 머신으로 취급해야 하며, 어떤 방식으로든 설치에 액세스하거나 수정하려고 시도해서는 안됩니다. 일반적인 AWS 게이트웨이 업데이트 메커니즘 이외의 방법 (예: 하이퍼바이저 도구) 을 사용하여 소프트웨어 패키지를 SSM 설치하거나 업데이트하려고 하면 게이트웨이가 오작동할 수 있습니다.

업데이트 빈도 및 예상 동작

AWS 배포된 게이트웨이를 중단시키지 않으면서 필요에 따라 클라우드 서비스 구성 요소를 업데이트합니다. 배포된 게이트웨이 어플라이언스는 월별 유지 관리 업데이트를 받습니다. 월간 유지 관리 업데이트에는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능, 보안 문제 해결, 새로운 기능에 대한 액세스가 포함될 수 있습니다. 모든 업데이트는 누적되며 적용 시 게이트웨이를 현재 버전으로 업그레이드합니다. 각 업데이트에 포함된 특정 변경 사항에 대한 자세한 내용은 볼륨 게이트웨이 어플라이언스 소프트웨어의 릴리스 노트를 참조하십시오.

월별 유지 관리 업데이트로 인해 서비스가 잠시 중단될 수 있습니다. 업데이트 중에 게이트웨이의 VM 호스트를 재부팅할 필요는 없지만 게이트웨이 어플라이언스가 업데이트되고 다시 시작되는 동안에는 잠시 동안 게이트웨이를 사용할 수 없습니다.

게이트웨이를 배포하고 활성화하면 기본 주간 유지 관리 기간 일정이 설정됩니다. 유지 관리 기간 일정은 언제든지 수정할 수 있습니다. 월별 유지 관리 업데이트를 끌 수도 있지만 계속 켜두는 것이 좋습니다.

> **Note**
>
> 정기 유지 관리 업데이트가 꺼져 있더라도 유지 관리 기간 일정에 따라 긴급 업데이트가 적용되는 경우가 있습니다.

게이트웨이에 업데이트를 적용하기 전에 Storage Gateway 콘솔 및 콘솔에 메시지를 보내 AWS 사용자에게 알립니다. AWS Health Dashboard자세한 내용은 AWS Health Dashboard 단원을 참조하십시오. 소프트웨어 업데이트 알림이 전송되는 이메일 주소를 수정하려면 계정 관리 참조 가이드에서 AWS 계정의 대체 연락처 업데이트를 참조하십시오.AWS

업데이트가 제공되면 게이트웨이 세부 정보 탭에 유지 관리 메시지가 표시됩니다. 세부 정보 탭에서도 마지막으로 성공한 업데이트가 적용된 날짜와 시간을 확인할 수 있습니다.

유지 관리 업데이트를 켜거나 끕니다.

유지 관리 업데이트가 켜지면 게이트웨이는 구성된 유지 관리 기간 일정에 따라 이러한 업데이트를 자동으로 적용합니다. 자세한 내용은 게이트웨이 유지 관리 기간 일정 참조하십시오.

유지 보수 업데이트가 해제된 경우 게이트웨이는 이러한 업데이트를 자동으로 적용하지 않지만 언제든지 Storage Gateway 콘솔 또는 를 사용하여 수동으로 적용할 수 CLI 있습니다. API 이 설정과 관계없이 구성된 유지 관리 기간 중에 긴급 업데이트가 적용되는 경우가 있습니다.

> **Note**
>
> 다음 절차는 Storage Gateway 콘솔을 사용하여 게이트웨이 업데이트를 켜거나 끄는 방법을 설명합니다. 를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조의 내용을 참조하십시오 UpdateMaintenanceStartTime. API

Storage Gateway 콘솔을 사용하여 유지 관리 업데이트를 켜거나 끄려면:

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 업데이트의 경우 켜기 또는 끄기를 선택합니다.
5. 완료되면 변경 내용 저장을 선택합니다.

Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭에서 업데이트된 설정을 확인할 수 있습니다.

게이트웨이 유지 관리 기간 일정을 수정하십시오.

유지 관리 업데이트가 켜져 있는 경우 게이트웨이는 유지 관리 기간 일정에 따라 이러한 업데이트를 자동으로 적용합니다. 유지 관리 업데이트 설정에 관계없이 구성된 유지 관리 기간 중에 긴급 업데이트가 적용되는 경우가 있습니다.

> **Note**
>
> 다음 절차는 Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하는 방법을 설명합니다. 를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조의 내용을 참조하십시오 UpdateMaintenanceStartTime. API

Storage Gateway 콘솔을 사용하여 유지 보수 기간 일정을 수정하려면:

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 창 시작 시간에서 다음을 수행하십시오.

    a. 일정에서 매주 또는 매월을 선택하여 유지 관리 기간 주기를 설정합니다.

    b. 주간을 선택하는 경우 요일 및 시간 값을 수정하여 유지 관리 기간이 시작되는 각 주의 특정 시점을 설정하십시오.

    매월을 선택하는 경우 월 중 일 및 시간 값을 수정하여 유지 관리 기간이 시작되는 각 달의 특정 시점을 설정하십시오.

> **Note**
>
> 월의 날짜에 설정할 수 있는 최대값은 28입니다. 29~31일에 시작하도록 유지 관리 일정을 설정할 수 없습니다.
> 이 설정을 구성하는 동안 오류가 발생하면 게이트웨이 소프트웨어가 최신 버전이 아닐 수 있습니다. 먼저 게이트웨이를 수동으로 업데이트한 다음 유지 관리 기간 일정을 다시 구성해 보십시오.

5. 완료되면 변경 내용 저장을 선택합니다.

Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭에서 업데이트된 설정을 확인할 수 있습니다.

로컬 콘솔을 사용하여 유지 관리 작업 수행

호스트의 로컬 콘솔을 사용하여 다음과 같은 유지 관리 작업을 수행할 수 있습니다. 로컬 콘솔 작업은 VM 호스트 또는 Amazon EC2 인스턴스에서 수행할 수 있습니다. 대부분 작업이 여러 호스트에 공통된 작업이지만, 일부 차이도 있습니다.

VM 로컬 콘솔에서 작업 수행

온프레미스에서 배포한 게이트웨이의 경우, VM 호스트의 로컬 콘솔을 사용하여 다음과 같은 유지 관리 작업을 할 수 있습니다. 이러한 작업은 Hyper-V 및 Linux 커널 기반 가상 컴퓨터 () 호스트에 공통적으로 적용됩니다. VMware KVM

주제

- 기본 자격 증명을 사용하여 로컬 콘솔에 로그인
- Storage Gateway 콘솔에서 로컬 콘솔 암호 설정
- 프록시를 통한 온프레미스 게이트웨이 라우팅
- 게이트웨이 네트워크 구성
- 게이트웨이가 인터넷에 연결되어 있는지 테스트
- 게이트웨이 VM 시간 동기화
- 로컬 콘솔에서 스토리지 게이트웨이 명령 실행
- 게이트웨이 시스템 리소스 상태 조회
- 게이트웨이용 네트워크 어댑터 구성

기본 자격 증명을 사용하여 로컬 콘솔에 로그인

VM이 로그인할 준비가 되면 로그인 화면이 표시됩니다. 로컬 콘솔에 처음 로그인하는 경우 기본 로그인 자격 증명을 사용하여 로그인합니다. 이러한 기본 로그인 자격 증명을 통해 로컬 콘솔에서 게이트웨이 네트워크 설정을 구성하고 암호를 변경할 수 있는 메뉴에 액세스할 수 있습니다. Storage Gateway를 사용하면 로컬 AWS Storage Gateway 콘솔에서 암호를 변경하는 대신 콘솔에서 암호를 직접 설정할 수 있습니다. 새 암호를 설정하기 위해 기본 암호를 알 필요는 없습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정 단원을 참조하십시오.

게이트웨이의 로컬 콘솔에 로그인하려면

1. 로컬 콘솔에 처음 로그인하는 경우, 기본 자격 증명을 사용하여 VM에 로그인합니다. 기본 사용자 이름과 암호는 각각 `admin` 및 `password`입니다.

   또는 자격 증명을 사용하여 로그인합니다.

   > **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 스토리지 게이트웨이 명령 실행 섹션을 참조하십시오. AWS Storage Gateway 콘솔에서 직접 암호를 설정할 수도 있습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정 단원을 참조하십시오.

   > **Important**
   >
   > 이전 버전의 볼륨 또는 Tape Gateway의 경우 사용자 이름은 `sguser`이고 암호는 `sgpassword`입니다. 암호를 재설정하고 게이트웨이가 최신 버전으로 업데이트되면 사용자 이름이 admin으로 변경되지만 암호는 유지됩니다.

2. 로그인하면 다양한 작업을 수행할 수 있는 AWS Storage Gateway 구성 기본 메뉴가 나타납니다.

관련 작업	이 주제를 참조하십시오.
게이트웨이의 SOCKS 프록시를 구성하십시오.	프록시를 통한 온프레미스 게이트웨이 라우팅.

관련 작업	이 주제를 참조하십시오.
네트워크 구성	게이트웨이 네트워크 구성.
네트워크 연결 테스트	게이트웨이가 인터넷에 연결되어 있는지 테스트.
VM 시간 관리	게이트웨이 VM 시간 동기화.
Storage Gateway 콘솔 명령 실행	로컬 콘솔에서 스토리지 게이트웨이 명령 실행.
시스템 리소스 점검 조회	게이트웨이 시스템 리소스 상태 조회.

게이트웨이를 종료하려면 **0**을 입력합니다.

구성 세션을 종료하려면 **x**을 입력합니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호 설정

로컬 콘솔에 처음 로그인하는 경우, 기본 자격 증명을 사용하여 VM에 로그인합니다. 사용자 이름은 `admin`이고 암호는 `password`입니다. 새 게이트웨이를 생성한 즉시 항상 새 암호를 설정하는 것이 좋습니다. 원하는 경우 이 암호를 로컬 콘솔이 아닌 AWS Storage Gateway 콘솔에서 설정할 수 있습니다. 새 암호를 설정하기 위해 기본 암호를 알 필요는 없습니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호를 설정하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 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. 로컬 콘솔 암호 설정 대화 상자에 새 암호를 입력하고 암호를 확인한 후 저장을 선택합니다. 새 암호가 기본 암호를 대체합니다. Storage Gateway는 암호를 저장하지 않지만, 대신 VM에 안전하게 전송합니다.

> **Note**
>
> 암호는 키보드에 있는 어떤 문자로도 구성할 수 있으며 1개에서 512개의 문자까지 가능합니다.

프록시를 통한 온프레미스 게이트웨이 라우팅

볼륨 게이트웨이와 테이프 게이트웨이는 온프레미스 게이트웨이와 간에 Socket Secure 버전 5 (SOCKS5) 프록시를 구성할 수 있도록 지원합니다. AWS

> **Note**
>
> 지원되는 유일한 프록시 구성은 입니다. SOCKS5

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우 게이트웨이의 SOCKS 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 그러면 Storage Gateway가 프록시 서버를 통해 모든 HTTPS 트래픽을 라우팅합니다. 게이트웨이의 네트워크 요건에 대한 정보는 네트워크 및 방화벽 요구 사항 단원을 참조하십시오.

다음 절차는 볼륨 게이트웨이 및 테이프 게이트웨이에 대한 SOCKS 프록시를 구성하는 방법을 보여줍니다.

볼륨 및 테이프 게이트웨이의 SOCKS5 프록시를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
   - VMwareESXi— 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - KVM— 자세한 내용은 을 참조하십시오Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM.
2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 SOCKS프록시 구성을 선택합니다.
3. AWS Storage Gateway SOCKS 프록시 구성 메뉴에서 해당하는 숫자를 입력하여 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
프록시 구성 SOCKS	해당 숫자를 입력하여 SOCKS프록시 구성을 선택합니다.

수행할 작업	수행할 작업
	구성을 완료하려면 호스트 이름 및 포트를 입력해야 합니다.
현재 SOCKS 프록시 구성 보기	해당 숫자를 입력하여 현재 SOCKS 프록시 구성 보기를 선택합니다. SOCKS프록시가 구성되지 않은 경우 메시지가 `SOCKS Proxy not configured` 표시됩니다. SOCKS프록시가 구성된 경우 프록시의 호스트 이름과 포트가 표시됩니다.
SOCKS프록시 구성 제거	해당 숫자를 입력하여 SOCKS프록시 구성 제거를 선택합니다. 메시지 `SOCKS Proxy Configuration Removed` 가 나타납니다.

4. HTTP구성을 적용하려면 VM을 다시 시작합니다.

게이트웨이 네트워크 구성

게이트웨이의 기본 네트워크 구성은 동적 호스트 구성 프로토콜 (DHCP) 입니다. 를 사용하면 DHCP 게이트웨이에 IP 주소가 자동으로 할당됩니다. 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.

   - VMwareESXi— 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - KVM— 자세한 내용은 을 참조하십시오Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM.

2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.

3. AWS Storage Gateway 네트워크 구성 메뉴에서 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
네트워크 어댑터 설명	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 • DHCP활성화 상태 고정 IP 주소를 구성하거나 게이트웨이의 기본 어댑터를 설정할 경우 여기에 나열된 어댑터 이름을 사용합니다.
구성 DHCP	해당 숫자를 입력하여 구성을 DHCP 선택합니다. 사용할 DHCP 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 도메인 네임 서비스 (DNS) 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. 게이트웨이가 두 개 이상의 네트워크 인터페이스를 사용하는 경우 활성화된 모든 인터페이스를 사용하도록 DHCP 설정하거나 고정 IP 주소를 사용해야 합니다.

수행할 작업	수행할 작업
	예를 들어 게이트웨이 VM이 로 DHCP 구성된 두 개의 인터페이스를 사용한다고 가정해 보겠습니다. 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 다음 게이트웨이를 사용하도록 DHCP 설정하면 두 인터페이스 모두 사용됩니다. DHCP
게이트웨이의 호스트 이름 구성	해당 숫자를 입력하여 호스트 이름 구성을 선택합니다. 게이트웨이에서 지정한 정적 호스트 이름을 사용할지 또는 r을 통해 DCHP 자동으로 할당할지를 선택하라는 메시지가 표시됩니다. DNS 정적을 선택하면 정적 호스트 이름 (예:) 을 제공하라는 메시지가 표시됩니다. `testgateway.example.com` 구성을 y 적용하려면 를 입력합니다. **Note** 게이트웨이의 고정 호스트 이름을 구성하는 경우 제공된 호스트 이름이 게이트웨이가 연결된 도메인에 있는지 확인하십시오. 또한 게이트웨이의 IP 주소가 고정 호스트 이름을 가리키는 A 레코드를 DNS 시스템에 생성해야 합니다.

수행할 작업	수행할 작업
모든 게이트웨이의 네트워크 구성을 다음으로 재설정합니다. DHCP	해당 숫자를 입력하여 DHCP 모두 재설정을 선택합니다. 모든 네트워크 인터페이스가 사용하도록 DHCP 설정되어 있습니다. **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**).
게이트웨이 DNS 구성 보기	해당 숫자를 입력하여 DNS구성 보기를 선택합니다. 기본 및 보조 DNS 네임 서버의 IP 주소가 표시됩니다.
라우팅 테이블 조회	해당 숫자를 입력하여 경로 보기를 선택합니다. 게이트웨이의 기본 경로가 표시됩니다.

게이트웨이가 인터넷에 연결되어 있는지 테스트

게이트웨이의 로컬 콘솔을 사용하여 인터넷에 연결되어 있는지 테스트할 수 있습니다. 이 테스트는 게이트웨이의 네트워크 문제를 해결할 때 유용합니다.

게이트웨이가 인터넷에 연결되어 있는지 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMwareESXi— 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - KVM— 자세한 내용은 을 참조하십시오Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM.

2. AWS Storage Gateway - 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 유형을 지정해야 합니다.

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.

4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트하려는 유형을 선택합니다. AWS 리전 Storage Gateway에서 사용할 수 있는 지원 엔드포인트 AWS 리전 및 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

테스트가 진행됨에 따라 각 엔드포인트에는 [PASSED] 또는 [FAILED] 가 표시되어 다음과 같이 연결 상태를 나타냅니다.

메시지	설명
[PASSED]	Storage Gateway가 네트워크에 연결되어 있습니다.
[FAILED]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

게이트웨이 VM 시간 동기화

게이트웨이를 배포하고 실행한 후에 게이트웨이 VM의 시간에 오차가 생기는 경우가 있을 수 있습니다. 예를 들어 네트워크 중단이 지속되어 하이퍼바이저 호스트와 게이트웨이의 시간이 업데이트되지 않으면 게이트웨이 VM의 시간은 진태양시와 달라집니다. 시간 오차가 있는 경우, 스냅샷과 같은 작업이 실행되도록 지정한 시간과 작업이 실제 이루어지는 시간 사이에 불일치가 발생합니다.

에 VMware ESXi 배포된 게이트웨이의 경우 하이퍼바이저 호스트 시간을 설정하고 VM 시간을 호스트와 동기화하는 것만으로도 시간 변동을 피할 수 있습니다. 자세한 내용은 VM 시간을 호스트 시간과 동기화 단원을 참조하십시오.

Microsoft Hyper-V에 배포한 게이트웨이의 경우, VM의 시간을 주기적으로 점검해야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화 단원을 참조하십시오.

로컬 콘솔에서 스토리지 게이트웨이 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. AWS Support

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMwareESXi로컬 콘솔 로그인에 대한 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하십시오.
   - KVM로컬 콘솔 로그인에 대한 자세한 내용은 을 참조하십시오Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 **h**를 입력합니다.

   콘솔에는 사용 가능한 명령이 나열된 AVAILABLECOMMANDS메뉴가 표시됩니다.

Command	함수
dig	DNS문제 해결을 위해 dig에서 결과를 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 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 구성을 참조하세요.
iptables	IPv4패킷 필터링을 위한 관리 도구 및 NAT
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.

Command	함수
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결하세요.
passwd	인증 토큰을 업데이트합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
sslcheck	인증서 발급자와 함께 출력을 반환합니다. **Note** Storage Gateway는 인증서 발급자 확인을 사용하며 SSL 검사를 지원하지 않습니다. 이 명령이 aws-appliance@amazon.com 이외의 발급자를 반환하는 경우 애플리케이션이 SSL 검사를 수행하는 것일 수 있습니다. 이 경우 Storage Gateway 어플라이언스에 대한 ssl 검사를 생략하는 것이 좋습니다.
tcptraceroute	목적지로 향하는 TCP 트래픽에 대한 추적 경로 출력을 수집합니다.

4. 게이트웨이 콘솔 명령 프롬프트에서 사용하려는 기능에 해당하는 명령을 입력하고 지침을 따릅니다.

명령에 대해 알아보려면 +를 입력하십시오. **man** *command name* 명령 프롬프트에서

게이트웨이 시스템 리소스 상태 조회

게이트웨이가 시작되면 가상 CPU 코어, 루트 볼륨 크기 등을 RAM 확인합니다. 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.

   - VMwareESXi콘솔 로그인에 대한 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하십시오.
   - KVM로컬 콘솔 로그인에 대한 자세한 내용은 을 참조하십시오Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

   각 리소스에는 [OK], [WARNING] 또는 [FAIL] 가 표시되어 다음과 같이 리소스 상태를 나타냅니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[WARNING]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[FAIL]	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.

게이트웨이용 네트워크 어댑터 구성

기본적으로 Storage Gateway는 E1000 네트워크 어댑터 유형을 사용하도록 구성되어 있지만 VMXNET3 (10GbE) 네트워크 어댑터를 사용하도록 게이트웨이를 재구성할 수 있습니다. Storage Gateway를 한 개 이상의 IP 주소에서 액세스할 수 있도록 구성할 수도 있습니다. 이를 위해서는 게이트웨이가 네트워크 어댑터를 한 개 이상 사용하도록 구성하면 됩니다.

주제

네트워크 어댑터를 사용하도록 게이트웨이 구성 VMXNET3

Storage Gateway는 Microsoft Hyper-V 하이퍼바이저 VMware ESXi 호스트 모두에서 E1000 네트워크 어댑터 유형을 지원합니다. 하지만 VMXNET3 (10GbE) 네트워크 어댑터 유형은 VMware ESXi 하이퍼바이저에서만 지원됩니다. 게이트웨이가 VMware ESXi 하이퍼바이저에서 호스팅되는 경우 (VMXNET310GbE) 어댑터 유형을 사용하도록 게이트웨이를 재구성할 수 있습니다. 이러한 어댑터에 대한 자세한 내용은 Broadcom () 웹 사이트에서 가상 컴퓨터용 네트워크 어댑터 선택을 참조하십시오. VMware

> **Important**
>
> 선택하려면 VMXNET3 게스트 운영 체제 유형이 기타 Linux64여야 합니다.

어댑터를 사용하도록 게이트웨이를 구성하기 위해 수행하는 단계는 다음과 같습니다. VMXNET3

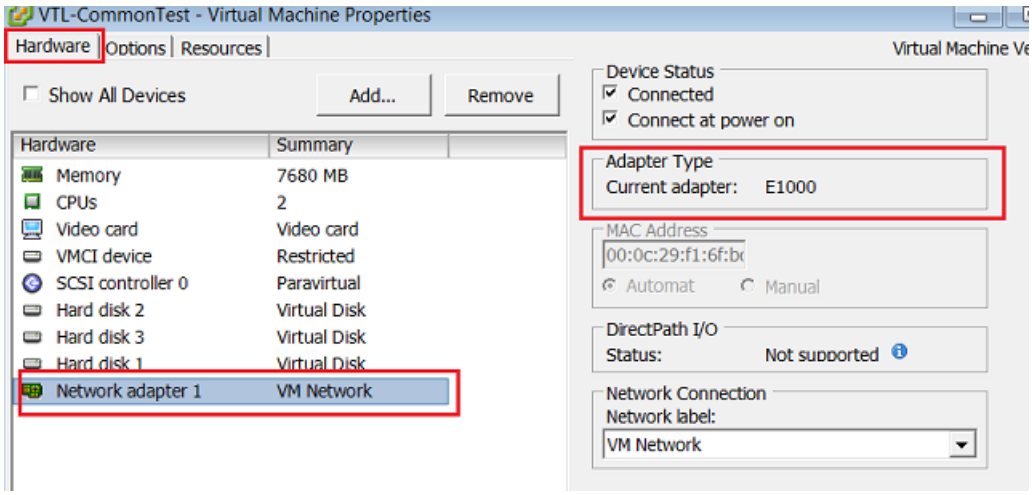
1. 기본 E1000 어댑터를 제거합니다.
2. VMXNET3어댑터를 추가합니다.
3. 게이트웨이 다시 시작합니다.
4. 네트워크용 어댑터를 구성합니다.

각 단계를 수행하는 자세한 방법은 다음과 같습니다.

기본 E1000 어댑터를 제거하고 해당 어댑터를 사용하도록 게이트웨이를 구성하려면 VMXNET3

1. 에서 VMware 게이트웨이의 컨텍스트 메뉴 (마우스 오른쪽 버튼 클릭) 를 열고 설정 편집을 선택합니다.

2. Virtual Machine Properties(가상 머신 속성) 창에서 Hardware(하드웨어) 탭을 선택합니다.
3. Hardware(하드웨어)에 대해 Network adapter(네트워크 어댑터)를 선택합니다. Adapter Type(어댑터 유형) 섹션에서 현재 어댑터는 E1000임을 알 수 있습니다. 이 어댑터를 어댑터로 교체합니다. VMXNET3



4. E1000 네트워크 어댑터를 선택한 후 제거를 선택합니다. 이 예에서 E1000 네트워크 어댑터는 Network adapter 1(네트워크 어댑터 1)입니다.

> **Note**
>
> 게이트웨이에서 E1000 및 VMXNET3 네트워크 어댑터를 동시에 실행할 수 있지만 네트워크 문제가 발생할 수 있으므로 그렇게 하지 않는 것이 좋습니다.

5. 추가를 선택하여 Add Hardware 마법사를 엽니다.
6. Ethernet Adapter(이더넷 어댑터)를 선택한 후 다음을 선택합니다.
7. 네트워크 유형 마법사에서 어댑터 유형으로 **VMXNET3**을 선택한 후 다음을 선택합니다.
8. 가상 컴퓨터 속성 마법사의 어댑터 유형 섹션에서 현재 어댑터가 설정되어 있는지 확인한 다음 확인을 선택합니다. VMXNET3
9. VMwareVSphere클라이언트에서 게이트웨이를 종료합니다.
10. VMwareVSphere클라이언트에서 게이트웨이를 다시 시작합니다.

게이트웨이가 다시 시작하면 방금 추가한 어댑터를 재구성하여 네트워크가 인터넷에 연결되었는지 확인합니다.

네트워크용 어댑터를 구성하려면

1. VSphere클라이언트에서 콘솔 탭을 선택하여 로컬 콘솔을 시작합니다. 이 구성 작업을 위해서는 기본 로그인 자격 증명을 사용하여 게이트웨이의 로컬 콘솔에 로그인해야 합니다. 기본 자격 증명을 사용하여 로그인하는 방법에 대한 자세한 내용은 기본 자격 증명을 사용하여 로컬 콘솔에 로그인을 참조하세요.
2. 프롬프트에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. 프롬프트에서 해당 숫자를 입력하여 모두 재설정을 선택한 다음 프롬프트에 **y** (예) 를 입력하여 모든 어댑터가 동적 호스트 구성 프로토콜 (DHCP) 을 사용하도록 설정합니다. DHCP 사용 가능한 모든 어댑터가 사용하도록 DHCP 설정되어 있습니다.

   게이트웨이가 이미 활성화된 경우, Storage Gateway Management Console에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 게이트웨이를 다시 시작한 후 네트워크가 인터넷에 연결되어 있는지 테스트해야 합니다. 네트워크 연결을 테스트하는 방법에 대한 자세한 내용은 게이트웨이가 인터넷에 연결되어 있는지 테스트를 참조하세요.

다중 게이트웨이 구성 NICs

여러 네트워크 어댑터 (NICs) 를 사용하도록 게이트웨이를 구성하면 둘 이상의 IP 주소로 액세스할 수 있습니다. 이 방법은 다음과 같은 상황에서 사용할 수 있습니다.

- 처리량 극대화 - 네트워크 어댑터에 병목 현상이 발생하는 경우, 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 환경에서는 i SCSI 대상과 해당 대상에 연결하는 이니시에이터를 게이트웨이가 통신하는 네트워크와 다른 격리된 네트워크에 보관해야 할 수도 있습니다. AWS

일반적인 다중 어댑터 사용 사례에서는 한 어댑터가 게이트웨이가 통신하는 경로 AWS (즉, 기본 게이트웨이) 로 구성됩니다. 이 어댑터를 제외하고 이니시에이터는 연결되는 i SCSI 대상이 포함된 어댑터와 동일한 서브넷에 있어야 합니다. 그렇지 않은 경우, 원하는 대상과의 통신이 불가능할 수 있습니다. 통신에 사용되는 것과 동일한 어댑터에 대상이 구성된 경우 해당 대상에 대한 i SCSI 트래픽과 AWS 트래픽은 동일한 어댑터를 통해 전달됩니다. AWS

어댑터 1개를 Storage Gateway 콘솔에 연결하도록 구성한 후 두 번째 어댑터를 추가할 경우 Storage Gateway는 두 번째 어댑터가 선호하는 경로로 사용되도록 자동으로 라우팅 테이블을 구성합니다. 다중 어댑터의 구성 방법에 대한 자세한 내용은 다음 단원을 참조하십시오.

- 한 NICs VMware ESXi 호스트에서 여러 개를 위한 게이트웨이 구성
- Microsoft Hyper-V NICs 호스트에서 여러 개를 위한 게이트웨이 구성

Amazon EC2 로컬 콘솔에서 작업 수행

Amazon EC2 인스턴스에 배포된 게이트웨이를 실행할 때 일부 유지 관리 작업을 수행하려면 로컬 콘솔에 로그인해야 합니다. 이 섹션에서는 로컬 콘솔에 로그인하고 유지 관리 작업을 수행하는 방법에 대해 설명합니다.

주제

- Amazon EC2 게이트웨이 로컬 콘솔에 로그인
- HTTP프록시를 EC2 통해 배포된 게이트웨이를 라우팅합니다.
- 게이트웨이 네트워크 연결 테스트
- 게이트웨이 시스템 리소스 상태 조회
- 로컬 콘솔에서 Storage Gateway 명령 실행

Amazon EC2 게이트웨이 로컬 콘솔에 로그인

Secure Shell (SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스에 연결할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스에 연결을 참조하십시오. 이 방법으로 연결하려면 인스턴스를 시작할 때 지정한 SSH 키 페어가 필요합니다. Amazon EC2 키 페어에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon EC2 키 페어를 참조하십시오.

게이트웨이 로컬 콘솔에 로그인하려면

1. 로컬 콘솔에 로그인합니다. Windows 컴퓨터에서 EC2 인스턴스에 연결하는 경우 관리자로 로그인하십시오.
2. 로그인하면 다양한 작업을 수행할 수 있는 AWS Storage Gateway - 구성 기본 메뉴가 나타납니다.

관련 작업	이 주제를 참조하십시오.
게이트웨이의 SOCKS 프록시를 구성하십시오.	HTTP프록시를 EC2 통해 배포된 게이트웨이를 라우팅합니다.
네트워크 연결 테스트	게이트웨이 네트워크 연결 테스트
Storage Gateway 콘솔 명령 실행	로컬 콘솔에서 Storage Gateway 명령 실행
시스템 리소스 점검 조회	게이트웨이 시스템 리소스 상태 조회.

게이트웨이를 종료하려면 **0**을 입력합니다.

구성 세션을 종료하려면 **x**을 입력합니다.

HTTP프록시를 EC2 통해 배포된 게이트웨이를 라우팅합니다.

Storage Gateway는 EC2 Amazon에 배포된 게이트웨이와 간에 소켓 보안 버전 5 (SOCKS5) 프록시를 구성할 수 있도록 지원합니다 AWS.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우 게이트웨이의 HTTP 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 이렇게 하면 Storage Gateway가 모든 AWS 엔드포인트 트래픽을 프록시 서버를 통해 라우팅합니다. 게이트웨이와 엔드포인트 간의 통신은 HTTP 프록시를 사용하는 경우에도 암호화됩니다.

로컬 프록시 서버를 통해 게이트웨이 인터넷 트래픽을 라우팅하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 단원을 참조하십시오.
2. AWS 기기 활성화 - 구성 기본 메뉴에서 해당 번호를 입력하여 프록시 구성을 선택합니다. HTTP
3. AWS 기기 활성화 HTTP 프록시 구성 메뉴에서 수행하려는 작업에 해당하는 번호를 입력합니다.

   - HTTP프록시 구성 - 구성을 완료하려면 호스트 이름과 포트를 제공해야 합니다.
   - 현재 HTTP 프록시 구성 보기 - HTTP 프록시가 구성되지 않은 경우 메시지가 `HTTP Proxy not configured` 표시됩니다. HTTP프록시가 구성된 경우 프록시의 호스트 이름과 포트가 표시됩니다.
   - HTTP프록시 구성 제거 - 메시지가 `HTTP Proxy Configuration Removed` 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 단원을 참조하십시오.
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 유형을 지정해야 합니다.
3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트하려는 유형을 선택합니다. AWS 리전 Storage Gateway에서 사용할 수 있는 지원 엔드포인트 AWS 리전 및 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오. AWS 일반 참조

테스트가 진행됨에 따라 각 엔드포인트에는 [PASSED] 또는 [FAILED] 가 표시되어 다음과 같이 연결 상태를 나타냅니다.

메시지	설명
[PASSED]	Storage Gateway가 네트워크에 연결되어 있습니다.
[FAILED]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

게이트웨이 시스템 리소스 상태 조회

게이트웨이가 시작되면 가상 CPU 코어, 루트 볼륨 크기 등을 확인합니다. RAM 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. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 단원을 참조하십시오.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

   각 리소스에는 [OK], [WARNING] 또는 [FAIL] 가 표시되어 다음과 같이 리소스 상태를 나타냅니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[WARNING]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[FAIL]	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.

로컬 콘솔에서 Storage Gateway 명령 실행

AWS Storage Gateway 콘솔은 게이트웨이와 관련된 문제를 구성하고 진단할 수 있는 안전한 환경을 제공하는 데 도움이 됩니다. 콘솔 명령을 사용하여 라우팅 테이블을 저장하거나 연결과 같은 유지 관리 작업을 수행할 수 있습니다. AWS Support

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 단원을 참조하십시오.

2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 h를 입력합니다.

   콘솔에는 사용 가능한 명령이 나열된 AVAILABLECOMMANDS메뉴가 표시됩니다.

Command	함수
dig	DNS문제 해결을 위해 dig에서 결과를 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.
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.
iptables	IPv4패킷 필터링을 위한 관리 도구 및NAT.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.

Command	함수
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결하세요.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
sslcheck	네트워크 문제 해결의 SSL 유효성을 확인하세요.
tcptraceroute	목적지까지의 TCP 트래픽에 대한 추적 경로 출력을 수집합니다.

4. 게이트웨이 콘솔 명령 프롬프트에서 사용하려는 기능에 해당하는 명령을 입력하고 지침을 따릅니다.

명령에 대해 알아보려면 명령 이름을 입력하고 `-h` 옵션을 입력하십시오(예: `sslcheck -h`).

게이트웨이 로컬 콘솔 액세스

VM 로컬 콘솔에 액세스하는 방법은 게이트웨이 VM이 배포된 하이퍼바이저 종류에 따라 달라집니다. 이 섹션에서는 Linux 커널 기반 가상 머신 (KVM) 및 Microsoft Hyper-V Manager를 사용하여 VM 로컬 콘솔에 액세스하는 방법에 대한 정보를 찾을 수 있습니다. VMware ESXi

주제

- Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM
- 를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi
- Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM

사용 중인 Linux 배포판에 KVM 따라 실행 중인 가상 컴퓨터를 구성하는 다양한 방법이 있습니다. 명령줄에서 KVM 구성 옵션에 액세스하는 방법은 다음과 같습니다. 지침은 KVM 구현에 따라 다를 수 있습니다.

게이트웨이의 로컬 콘솔에 액세스하려면 KVM

1. 다음 명령을 사용하여 현재 사용할 수 VMs 있는 항목을 KVM 나열합니다.

   ```
   # virsh list
   ```

   사용 가능 기준을 선택할 VMs 수 Id 있습니다.

   ```
   [[root@localhost vms]# virsh list
    Id    Name                           State
   ----------------------------------------------------
    7     SGW_KVM                        running

   [root@localhost vms]# virsh console 7
   ```

2. 로컬 콘솔에 액세스하려면 다음 명령을 사용합니다.

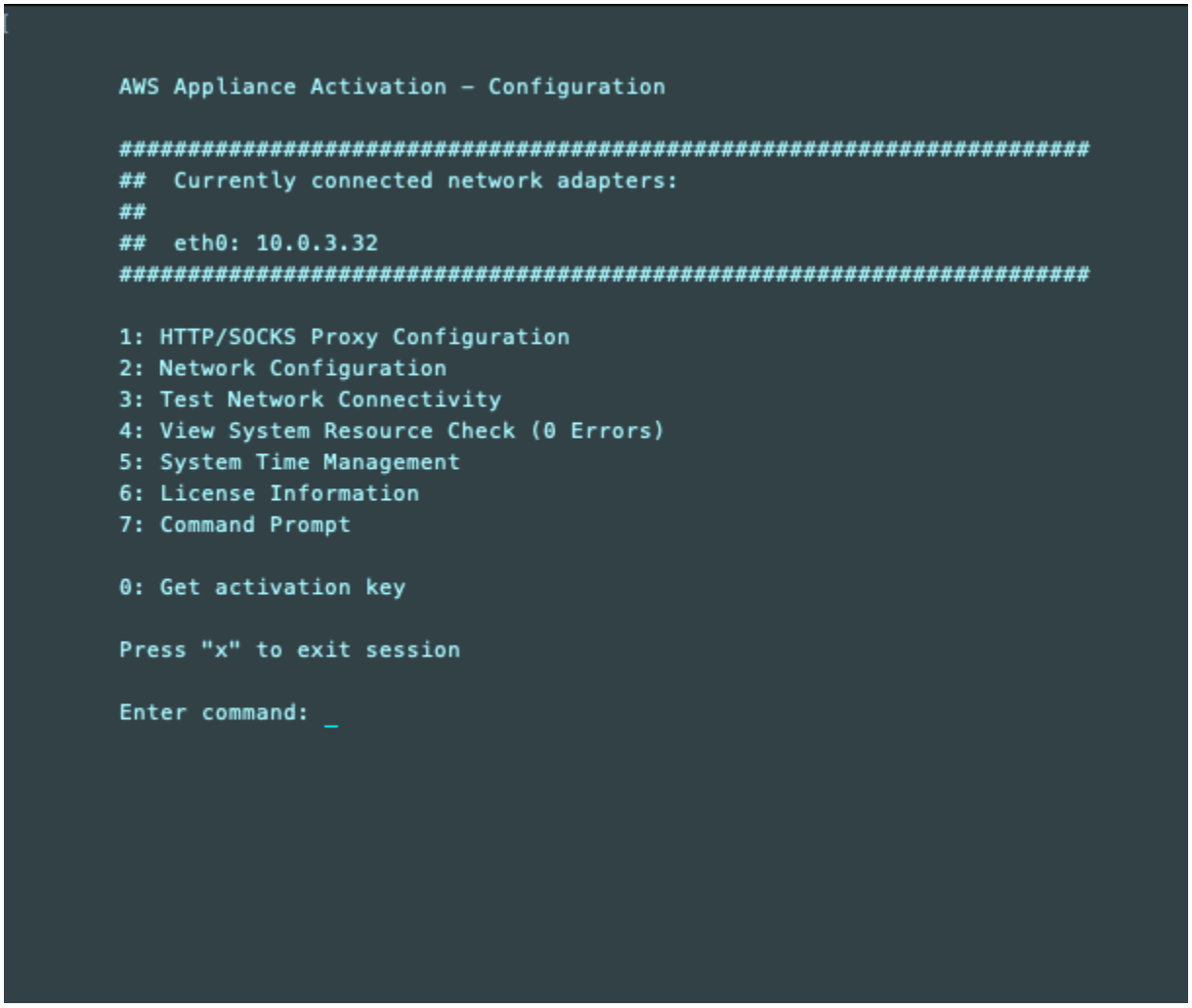
   ```
   # virsh console VM_Id
   ```

   ```
   [[root@localhost vms]# virsh console 7
   Connected to domain SGW_KVM
   Escape character is ^]

   AWS Appliance

   Login to change your network configuration and other settings.
   localhost login: _
   ```

3. 로컬 콘솔에 로그인하기 위한 기본 자격 증명을 얻으려면 기본 자격 증명을 사용하여 로컬 콘솔에 로그인 단원을 참조하십시오.
4. 로그인한 후 게이트웨이를 활성화하고 구성할 수 있습니다.

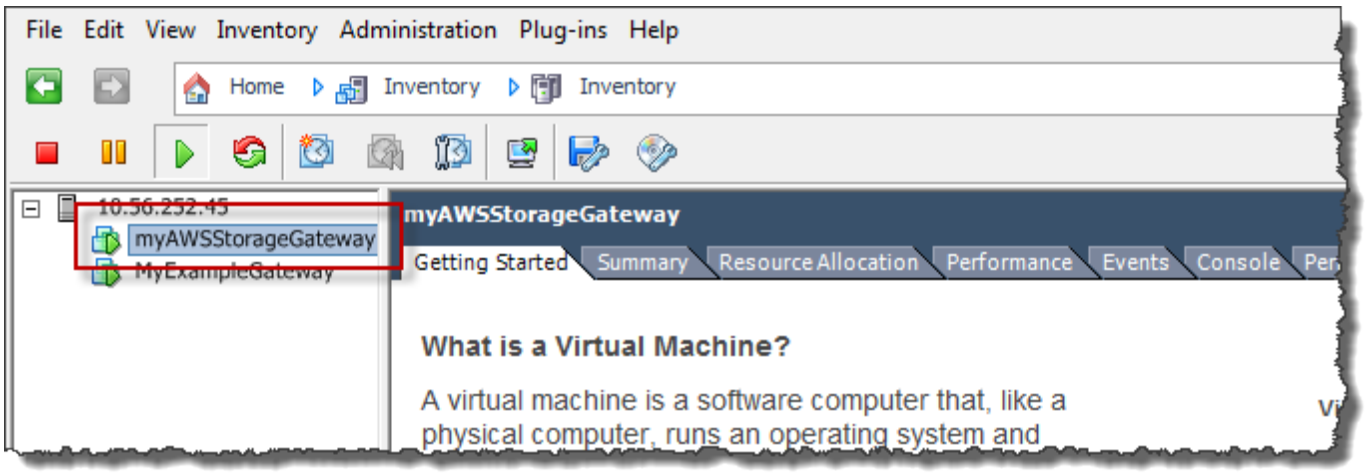


를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi

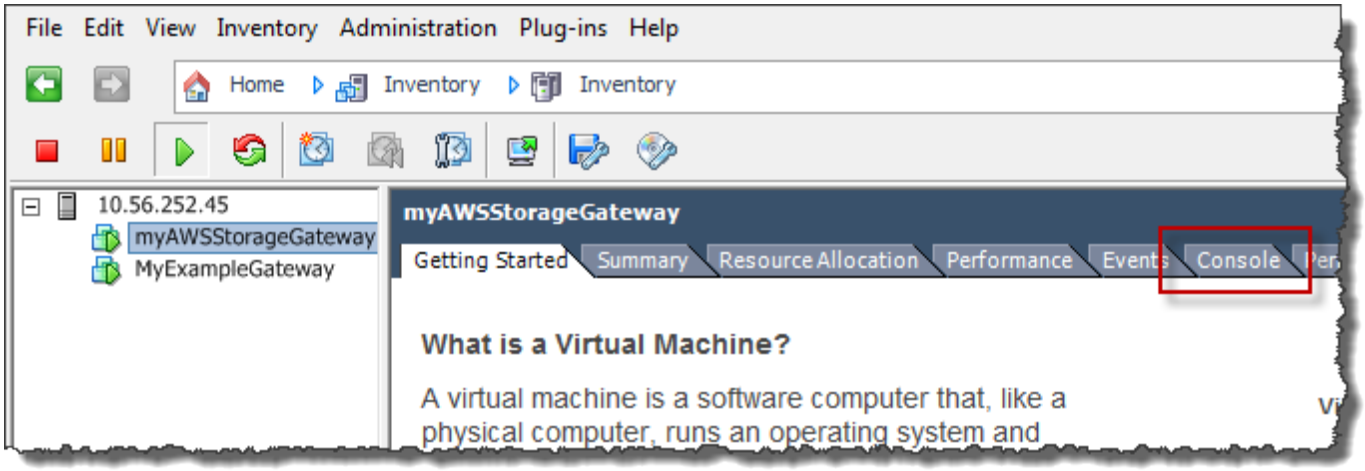
게이트웨이의 로컬 콘솔에 액세스하려면 VMware ESXi

1. VMware vSphere 클라이언트에서 게이트웨이 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인하세요.

> **Note**
>
> 게이트웨이 VM이 켜져 있는 경우, 다음 스크린샷과 같이 VM 아이콘과 함께 녹색 화살표 아이콘이 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 도구 모음 메뉴에서 녹색 전원 켜기 아이콘을 선택하여 켤 수 있습니다.

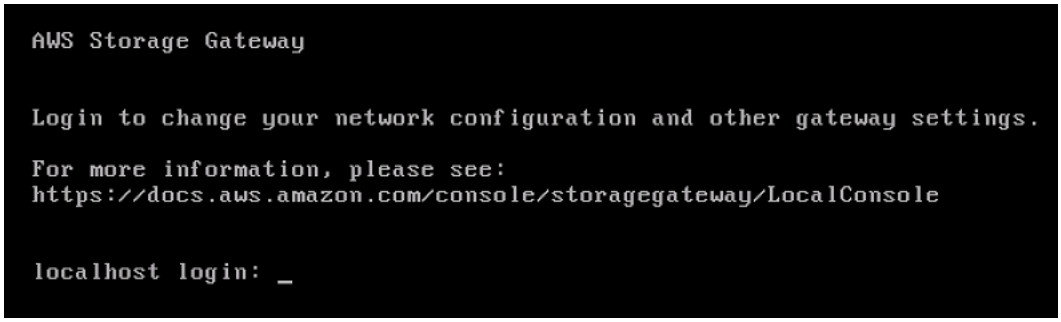


3. 콘솔 탭을 선택합니다.



잠시 후 VM은 로그인할 준비가 됩니다.

> **Note**
>
> 콘솔 창에서 커서를 릴리스하려면 Ctrl+Alt를 누릅니다.



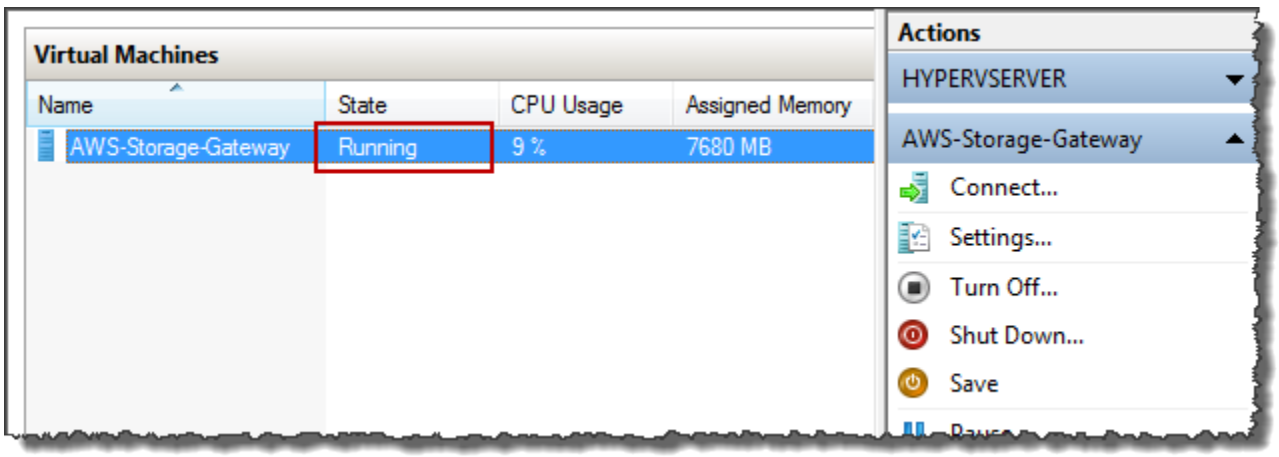
4. 기본 자격 증명을 사용하여 로그인하려면 계속해서 기본 자격 증명을 사용하여 로컬 콘솔에 로그인 절차를 수행합니다.

Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

게이트웨이의 로컬 콘솔에 액세스하려면(Microsoft Hyper-V)

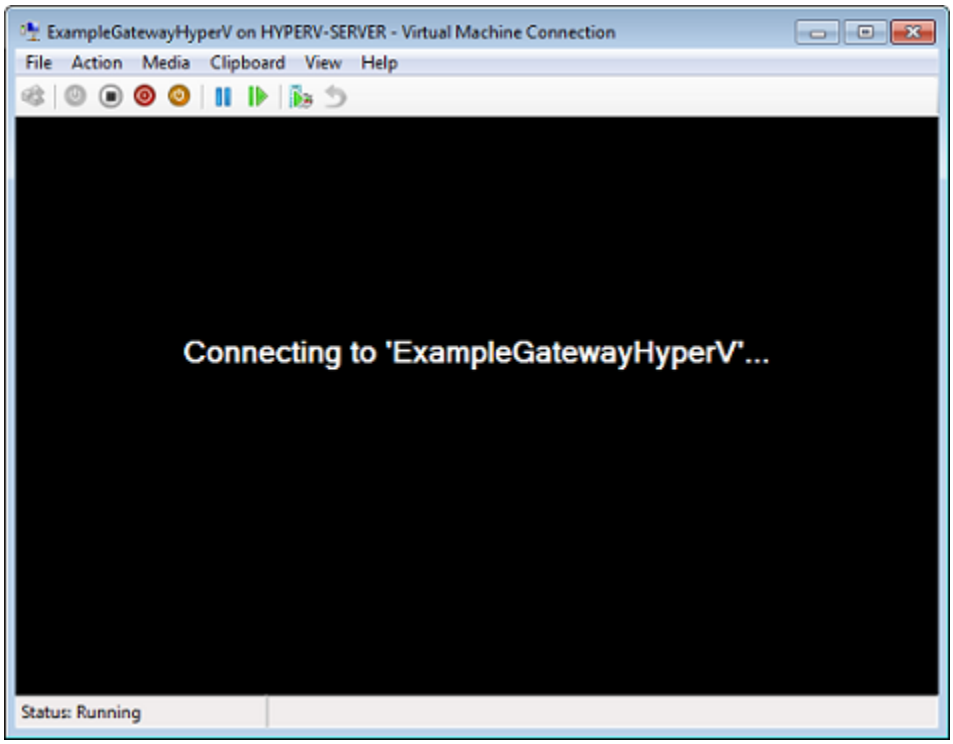
1. Microsoft Hyper-V Manager의 Virtual Machines(가상 머신) 목록에서 해당 게이트웨이 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인하세요.

> **Note**
>
> 게이트웨이 VM이 켜져 있는 경우 다음 스크린샷과 같이 Running이 VM의 상태로 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 작업 창에서 시작을 선택하여 켤 수 있습니다.

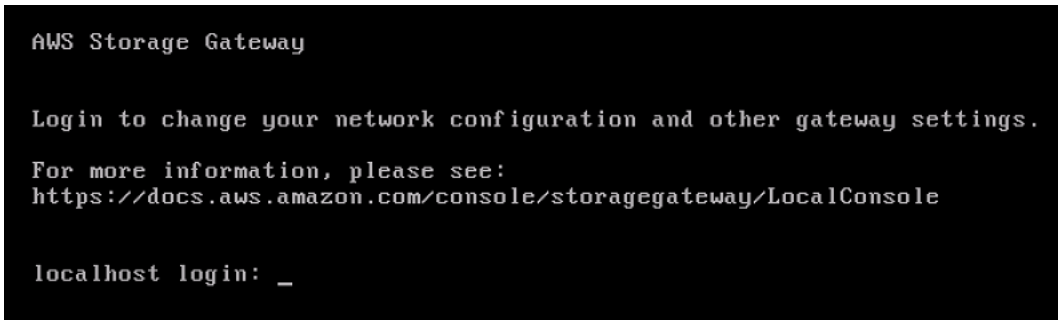


3. 작업 창에서 연결을 선택합니다.

   그러면 Virtual Machine Connection(가상 머신 연결) 창이 표시됩니다. 인증 창이 표시되면 하이퍼바이저 관리자가 제공한 로그인 자격 증명을 입력합니다.



   잠시 후 VM은 로그인할 준비가 됩니다.



4. 기본 자격 증명을 사용하여 로그인하려면 계속해서 기본 자격 증명을 사용하여 로컬 콘솔에 로그인 절차를 수행합니다.

게이트웨이용 네트워크 어댑터 구성

이 섹션에서는 게이트웨이에 여러 네트워크 어댑터를 구성하는 방법에 대한 정보를 얻을 수 있습니다.

주제

한 NICs VMware ESXi 호스트에서 여러 개를 위한 게이트웨이 구성

다음 절차에서는 게이트웨이 VM에 VMware ESXi 이미 하나의 네트워크 어댑터가 정의되어 있다고 가정하고 어댑터를 추가하는 방법을 설명합니다.

호스트에서 VMware ESXi 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이를 종료합니다.
2. VMware vSphere 클라이언트에서 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 Gateway와 함께 VMXNET3 네트워크 어댑터를 사용하는 것이 좋습니다. 어댑터 목록에 나타날 수 있는 어댑터 유형에 대한 자세한 내용은 ESXi및 vCenter 서버 설명서의 네트워크 어댑터 유형을 참조하십시오.

   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.

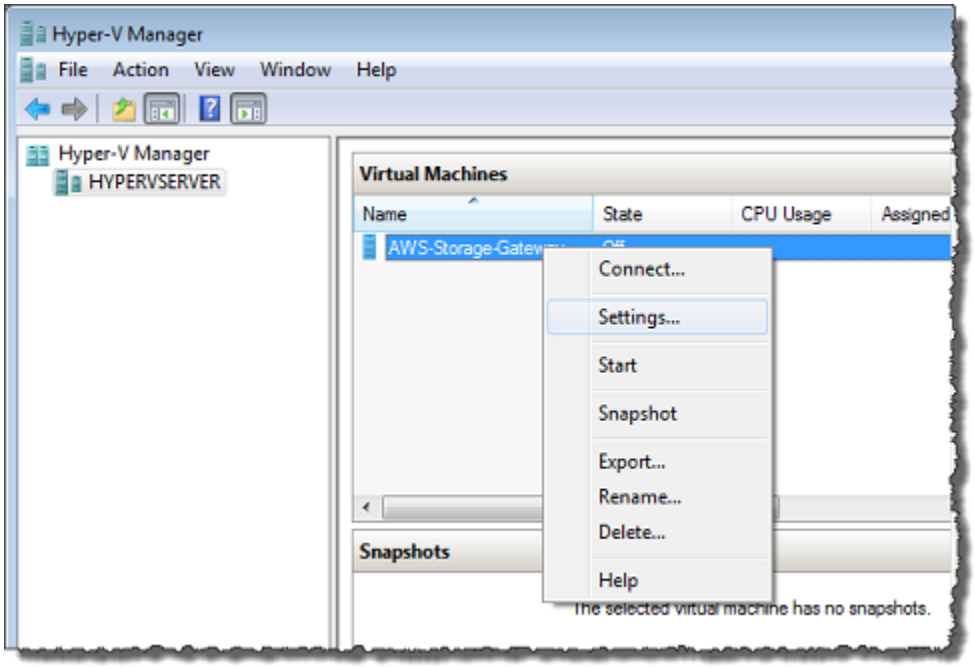
Hyper-V 및 KVM 호스트에 VMware 공통적인 로컬 콘솔 작업에 대한 자세한 내용은 을 참조하십시오. VM 로컬 콘솔에서 작업 수행

Microsoft Hyper-V NICs 호스트에서 여러 개를 위한 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.

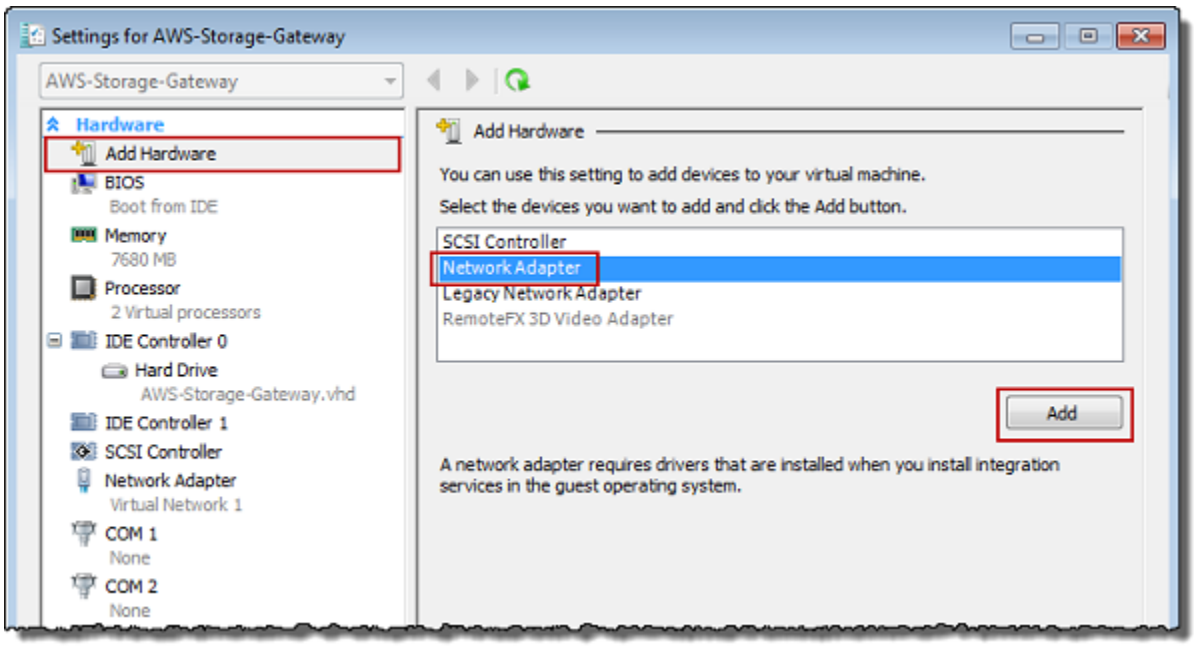
Microsoft Hyper-V 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. Storage Gateway 콘솔에서 게이트웨이를 끕니다. 지침은 a Volume Gateway를 중지하려면 단원을 참조하십시오.
2. Microsoft Hyper-V Manager에서 게이트웨이 VM을 선택합니다.
3. VM이 이미 꺼져 있는 경우, 게이트웨이를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Turn Off(끄기)를 선택합니다.
4. 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정을 선택합니다.



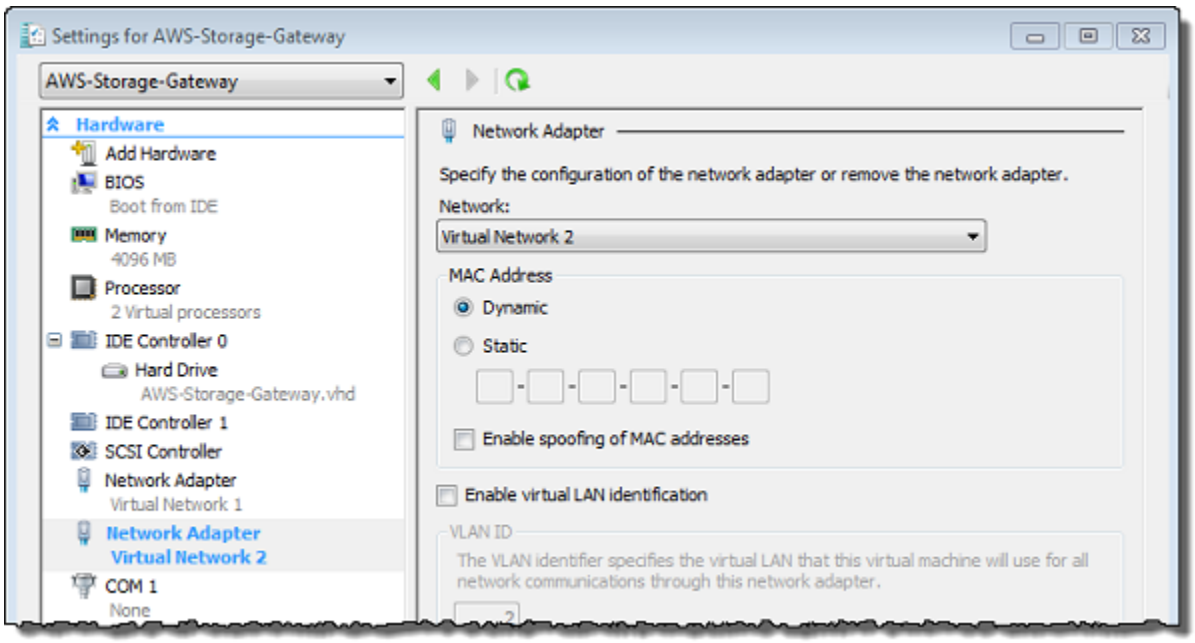
5. VM에 대한 설정 대화 상자의 Hardware(하드웨어)에서 Add Hardware(하드웨어 추가)를 선택합니다.

6. Add Hardware(하드웨어 추가) 창에서 Network Adapter(네트워크 어댑터)를 선택한 후 추가를 선택하여 디바이스를 추가합니다.



7. 네트워크 어댑터를 구성한 후 적용을 선택하여 설정을 적용합니다.

   다음 예시에서는 새 어댑터에 대해 Virtual Network 2(가상 네트워크 2)를 선택하였습니다.



8. 설정 대화 상자의 하드웨어에서 두 번째 어댑터가 추가되었는지 확인한 다음 확인을 선택합니다.
9. Storage Gateway 콘솔에서 게이트웨이를 켭니다. 지침은 a Volume Gateway를 시작하려면 단원을 참조하십시오.
10. Navigation(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.

Hyper-V 및 호스트에 VMware 공통적인 로컬 콘솔 작업에 대한 자세한 내용은 을 참조하십시오. KVM VM 로컬 콘솔에서 작업 수행

게이트웨이 삭제 및 관련 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 관리 콘솔에 해당 게이트웨이가 더 이상 나타나지 않고 SCSI 이니시에이터와의 연결이 끊어집니다. 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 참조를 참조하십시오.AWS Storage Gateway API

주제

- Storage Gateway 콘솔을 사용하여 게이트웨이 삭제
- 온프레미스에 배포한 게이트웨이에서 리소스 제거
- Amazon EC2 인스턴스에 배포된 게이트웨이에서 리소스 제거

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 인스턴스는 삭제하기 전까지 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 관리자 또는 Linux 커널 기반 가상 컴퓨터 (KVM) 클라이언트를 사용하여 호스트에 연결하고 VM을 제거합니다. 삭제한 게이트웨이의 VM을 다시 사용하여 새 게이트웨이를 활성화할 수는 없다는 점에 유의하십시오.

게이트웨이를 삭제하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 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 가상 테이프, Amazon Elastic Block Store (AmazonEBS) 스냅샷, Amazon EC2 인스턴스와 같은 리소스는 계속 유지됩니다. 이러한 리소스에 대해서는 계속 비용이 청구됩니다. Amazon 구독을 취소하여 Amazon EC2 인스턴스와 Amazon EBS 스냅샷을 제거하도록 선택할 수 있습니다. EC2 Amazon EC2 구독을 계속 유지하려면 Amazon EC2 콘솔을 사용하여 Amazon EBS 스냅샷을 삭제하면 됩니다.

온프레미스에 배포한 게이트웨이에서 리소스 제거

다음 지침에 따라 온프레미스에 배포한 게이트웨이에서 리소스를 제거할 수 있습니다.

VM에 배포한 볼륨 게이트웨이에서 리소스 제거

삭제하려는 게이트웨이가 가상 머신(VM)에 배포된 경우, 다음 작업을 수행하여 리소스를 정리하는 것이 좋습니다.

- 게이트웨이를 삭제합니다. 지침은 Storage Gateway 콘솔을 사용하여 게이트웨이 삭제 단원을 참조하십시오.
- 필요하지 않은 Amazon EBS 스냅샷을 모두 삭제하십시오. 지침은 Amazon 사용 EC2설명서의 Amazon EBS 스냅샷 삭제를 참조하십시오.

Amazon EC2 인스턴스에 배포된 게이트웨이에서 리소스 제거

Amazon EC2 인스턴스에 배포한 게이트웨이를 삭제하려면 게이트웨이와 함께 사용된 AWS 리소스, 특히 Amazon EC2 인스턴스, 모든 Amazon EBS 볼륨, 테이프 게이트웨이를 배포한 경우 테이프를 정리하는 것이 좋습니다. 이렇게 하면 원하지 않는 사용 요금이 청구되는 것을 방지할 수 있습니다.

Amazon에 배포된 캐시 볼륨에서 리소스 제거 EC2

캐시된 볼륨이 있는 게이트웨이를 배포한 경우 다음 조치를 취하여 게이트웨이를 삭제하고 해당 리소스를 정리하는 것이 좋습니다. EC2

1. Storage Gateway 콘솔에서 Storage Gateway 콘솔을 사용하여 게이트웨이 삭제의 설명대로 게이트웨이를 삭제합니다.
2. Amazon EC2 콘솔에서 EC2 인스턴스를 다시 사용할 계획이라면 인스턴스를 중지하십시오. 또는 인스턴스를 종료합니다. 볼륨을 삭제할 계획인 경우에는 인스턴스를 종료하기 전에 인스턴스에 연결된 블록 디바이스와 디바이스의 식별자를 적어둡니다. 이것은 삭제할 볼륨을 식별하는 데 필요합니다.
3. 다시 사용할 계획이 없는 경우 Amazon EC2 콘솔에서 인스턴스에 연결된 모든 Amazon EBS 볼륨을 제거하십시오. 자세한 내용은 Amazon EC2 사용 설명서의 인스턴스 및 볼륨 정리를 참조하십시오.

볼륨 게이트웨이의 성능 및 최적화

이 섹션에서는 Storage Gateway 성능에 대해 설명합니다.

주제

게이트웨이 성능 최적화

권장되는 게이트웨이 서버 구성

게이트웨이의 성능을 극대화하기 위해 Storage Gateway는 게이트웨이 호스트 서버에 다음과 같은 게이트웨이 구성을 권장합니다.

- 최소 24개의 전용 물리적 코어 CPU
- 경우 하드웨어 전용으로 다음 용량을 할당해야 합니다. RAM
  - 게이트웨이 전용 RAM 16GiB 이상, 캐시 크기 최대 16TiB
  - 캐시 크기가 16TiB에서 32TiB인 RAM 게이트웨이용으로 예약된 최소 32GiB
  - 캐시 크기가 32TiB에서 64TiB인 RAM 게이트웨이용으로 예약된 최소 48GiB
- 디스크 1 - 다음과 같이 게이트웨이 캐시로 사용됨
  - SSDNVMe컨트롤러 사용.
- 디스크 2 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
  - SSD컨트롤러 사용. NVMe
- 디스크 3 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
  - SSDNVMe컨트롤러 사용.
- VM 네트워크 1에 구성된 네트워크 어댑터 1:
  - VM 네트워크 1을 사용하고 수집에 사용할 추가 VMXnet3 (10Gbps) 를 추가합니다.
- VM 네트워크 2에 구성된 네트워크 어댑터 2:
  - VM 네트워크 2를 사용하고 연결에 사용할 a VMXnet3 (10Gbps) 를 추가합니다. AWS

게이트웨이에 리소스 추가

다음과 같은 병목 현상으로 인해 성능이 이론상 최대 지속 처리량 (클라우드로의 대역폭) 이하로 떨어질 수 있습니다. AWS

- CPU코어 수
- 캐시/업로드 버퍼 디스크 처리량
- 총 RAM 금액
- 네트워크 대역폭: AWS
- 이니시에이터에서 게이트웨이까지의 네트워크 대역폭

이 섹션에서는 게이트웨이 성능을 최적화하기 위해 수행할 수 있는 단계에 대해 다룹니다. 이 지침은 게이트웨이 또는 애플리케이션 서버에 리소스를 추가하는 것을 전제로 합니다.

다음 중 하나 이상의 방법으로 게이트웨이에 리소스를 추가하여 게이트웨이 성능을 최적화할 수 있습니다.

고성능 디스크 사용

캐시 및 업로드 버퍼 디스크 처리량으로 인해 게이트웨이의 업로드 및 다운로드 성능이 제한될 수 있습니다. 게이트웨이 성능이 예상보다 현저히 낮은 경우 다음과 같이 캐시 및 업로드 버퍼 디스크 처리량을 개선하는 것이 좋습니다.

- RAIDRAID10과 같은 스트라이프를 사용하면 디스크 처리량을 높일 수 있습니다. 하드웨어 RAID 컨트롤러를 사용하는 것이 가장 좋습니다.

  > **Note**
  >
  > RAID(독립 디스크의 중복 배열), 특히 RAID 10과 같은 디스크 스트라이프 RAID 구성은 데이터 본문을 블록으로 나누고 데이터 블록을 여러 저장 장치에 분산시키는 프로세스입니다. 사용하는 RAID 수준에 따라 달성할 수 있는 정확한 속도와 내결함성이 달라집니다. 여러 디스크에 I/O 워크로드를 스트라이핑하면 RAID 디바이스의 전체 처리량이 단일 멤버 디스크의 처리량보다 훨씬 높습니다.

- 직접 연결된 고성능 디스크 사용

  게이트웨이 성능을 최적화하기 위해 솔리드 스테이트 드라이브 (SSDs) 및 컨트롤러와 같은 고성능 디스크를 추가할 수 있습니다. NVMe Microsoft NTFS Hyper-V 대신 스토리지 영역 네트워크

(SAN) 에서 직접 가상 디스크를 VM에 연결할 수도 있습니다. 디스크 성능이 향상되면 일반적으로 처리량이 향상되고 초당 입/출력 작업 수가 늘어납니다 (). IOPS

처리량을 측정하려면 `Samples` Amazon CloudWatch 통계와 함께 `ReadBytes` 및 `WriteBytes` 지표를 사용하십시오. 예를 들어, 샘플 기간 5분에 대한 `ReadBytes` 지표 `Samples` 통계를 300초로 나눈 값을 구하면 결과를 얻을 수 있습니다. IOPS 일반적으로 게이트웨이에 대한 이러한 메트릭을 검토할 때는 디스크 관련 병목 현상을 나타내는 낮은 처리량과 낮은 IOPS 추세를 살펴보는 것이 좋습니다. .

> **Note**
>
> CloudWatch 모든 게이트웨이에서 메트릭을 사용할 수 있는 것은 아닙니다. 게이트웨이 지표에 대한 자세한 내용은 Storage Gateway 모니터링 섹션을 참조하세요.

업로드 버퍼 디스크 추가

쓰기 처리량을 높이려면 업로드 버퍼 디스크를 두 개 이상 추가하십시오. 데이터가 게이트웨이에 기록되면 업로드 버퍼 디스크에 로컬로 기록되고 저장됩니다. 그런 다음 저장된 로컬 데이터를 디스크에서 비동기적으로 읽고 처리한 뒤 AWS에 업로드합니다. 업로드 버퍼 디스크를 추가하면 각 개별 디스크에서 수행되는 동시 I/O 작업의 양을 줄일 수 있습니다. 이로 인해 게이트웨이에 대한 쓰기 처리량이 증가할 수 있습니다.

별도의 물리적 디스크로 게이트웨이 가상 디스크 지원

게이트웨이 디스크를 프로비저닝할 때는 동일한 기본 물리적 스토리지 디스크를 사용하는 업로드 버퍼 및 캐시 스토리지에 로컬 디스크를 프로비저닝하지 않는 것이 좋습니다. 예를 들어 VMwareESXi, 의 경우 기본 물리적 스토리지 리소스는 데이터 저장소로 표시됩니다. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 가상 디스크를 프로비저닝할 때(예: 업로드 버퍼 용도) 가상 디스크를 VM과 동일한 데이터 스토어 또는 다른 데이터 스토어에 저장할 수 있습니다.

데이터 스토어가 두 개 이상인 경우 생성하는 로컬 스토리지의 유형별로 하나씩 데이터 스토어를 선택하는 것이 좋습니다. 기본 물리적 디스크 하나로만 지원되는 데이터 스토어는 성능 저하로 이어질 수 있습니다. 게이트웨이 설정에서 이러한 디스크를 사용하여 캐시 스토리지와 업로드 버퍼를 모두 지원하는 경우를 예로 들 수 있습니다. 마찬가지로 RAID 1 또는 RAID 6과 같이 성능이 낮은 RAID 구성으로 지원되는 데이터 저장소는 성능이 저하될 수 있습니다.

게이트웨이 CPU 호스트에 리소스를 추가합니다.

게이트웨이 호스트 서버의 최소 요구 사항은 가상 프로세서 4개입니다. 게이트웨이 성능을 최적화하려면 게이트웨이 VM에 할당된 각 가상 프로세서가 전용 CPU 코어를 지원하는지 확인하세요. 또한 호스트 서버를 과도하게 구독하고 있지 않은지 CPUs 확인하십시오.

게이트웨이 호스트 서버를 CPUs 추가하면 게이트웨이의 처리 용량이 늘어납니다. 이렇게 하면 게이트웨이가 애플리케이션의 데이터를 로컬 스토리지에 저장하고 이 데이터를 Amazon S3로 업로드하는 작업을 병렬로 처리할 수 있습니다. CPUs또한 호스트를 다른 사람과 공유할 때 게이트웨이가 충분한 CPU 리소스를 확보하도록 하는 데도 도움이 VMs 됩니다. CPU리소스를 충분히 제공하면 일반적으로 처리량이 개선되는 효과가 있습니다.

게이트웨이와 AWS 클라우드 간 대역폭 늘리기

송수신 대역폭을 AWS 늘리면 게이트웨이로의 최대 데이터 수신 및 클라우드 송신 속도가 증가합니다. AWS 이렇게 하면 느린 디스크나 낮은 게이트웨이-이니시에이터 연결 대역폭과 같은 다른 요인보다 네트워크 속도가 게이트웨이 구성의 제한 요소인 경우 게이트웨이 성능을 개선할 수 있습니다.

> **Note**
>
> 캐시/업로드 버퍼 디스크 처리량, CPU 코어 수, RAM 총량 또는 이니시에이터와 게이트웨이 간 대역폭과 같은 여기에 나열된 다른 제한 요인으로 인해 관찰된 게이트웨이 성능이 네트워크 대역폭보다 낮을 수 있습니다. 또한, 게이트웨이의 정상 작동에는 데이터를 보호하기 위한 여러 가지 조치가 포함되므로 관찰된 성능이 네트워크 대역폭보다 낮을 수 있습니다.

볼륨 구성 변경

Volume Gateway의 경우 게이트웨이에 볼륨을 더 추가해도 게이트웨이 처리량이 줄어든다면 볼륨을 별도의 게이트웨이에 추가하는 것이 좋습니다. 특히 처리량이 많은 애플리케이션에 볼륨을 사용하는 경우, 처리량이 많은 애플리케이션을 위한 별도의 게이트웨이를 생성하는 것이 좋습니다. 그러나 일반적으로 한 게이트웨이는 처리량이 높은 모든 애플리케이션에 사용하고 다른 게이트웨이는 처리량이 낮은 모든 애플리케이션에 사용해서는 안됩니다. 볼륨 처리량을 측정하려면 `ReadBytes` 및 `WriteBytes` 지표를 사용하세요.

이러한 지표에 대한 자세한 내용은 애플리케이션과 게이트웨이 간 성능 측정 섹션을 참조하세요.

최적화 i 설정 SCSI

i SCSI 이니시에이터의 i SCSI 설정을 최적화하여 I/O 성능을 높일 수 있습니다. `MaxReceiveDataSegmentLength` 및 `FirstBurstLength`에는 256 KiB를 선택하고, `MaxBurstLength`에는 1MiB를 선택하는 것이 좋습니다. i SCSI 설정 구성에 대한 자세한 내용은 을 참조하십시오i 설정 사용자 지정 SCSI.

> **Note**
>
> 이러한 권장 설정을 통해 전반적으로 더 나은 성능을 실현할 수 있습니다. 하지만 성능을 최적화하는 데 필요한 특정 i SCSI 설정은 사용하는 백업 소프트웨어에 따라 다릅니다. 자세한 내용은 백업 소프트웨어 설명서를 참조하십시오.

애플리케이션 환경에 리소스 추가

애플리케이션 서버와 게이트웨이 간의 대역폭 늘리기

i SCSI 이니시에이터와 게이트웨이 간의 연결로 인해 업로드 및 다운로드 성능이 제한될 수 있습니다. 게이트웨이 성능이 예상보다 현저히 떨어지고 CPU 코어 수 및 디스크 처리량이 이미 개선되었다면 다음을 고려해 보십시오.

- 네트워크 케이블을 업그레이드하여 이니시에이터와 게이트웨이 간에 더 높은 대역폭을 확보합니다.

게이트웨이 성능을 최적화하려면 애플리케이션과 게이트웨이 간의 네트워크 대역폭이 애플리케이션 요구 사항을 충족할 수 있는지 확인하세요. 게이트웨이의 `ReadBytes` 및 `WriteBytes` 지표를 사용하여 총 데이터 처리량을 측정할 수 있습니다.

애플리케이션의 경우 측정된 처리량을 원하는 처리량과 비교합니다. 측정된 처리량이 원하는 처리량보다 적을 경우, 애플리케이션과 게이트웨이 간의 대역폭을 늘리면 네트워크 병목 현상이 발생하는 경우 성능을 개선할 수 있습니다. 마찬가지로, 직접 연결되지 않은 VM과 로컬 디스크 간의 대역폭을 늘릴 수 있습니다.

애플리케이션 환경에 리소스 추가 CPU

애플리케이션에서 추가 CPU 리소스를 사용할 수 있는 경우 리소스를 더 추가하면 애플리케이션이 I/O 부하를 확장하는 데 도움이 될 CPUs 수 있습니다.

Storage Gateway와 함께 VMware vSphere 고가용성 사용

Storage Gateway는 고가용성 (VMwareHA) 과 통합된 일련의 애플리케이션 수준 상태 점검을 VMware 통해 VMware vSphere 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.

vSphere HA는 이중화를 위해 가상 시스템과 가상 시스템이 상주하는 호스트를 클러스터로 풀링하는 방식으로 작동합니다. 클러스터의 호스트를 모니터링하며 장애가 발생할 경우 장애가 발생한 호스트의 가상 시스템이 대체 호스트에서 다시 시작됩니다. 일반적으로 이러한 복구는 데이터 손실 없이 신속하게 이루어집니다. vSphere HA에 대한 자세한 내용은 VMware 설명서의 vSphere HA 작동 방식을 참조하십시오.

> **Note**
>
> 장애가 발생한 가상 시스템을 다시 시작하고 새 호스트에서 i SCSI 연결을 다시 설정하는 데 필요한 시간은 호스트 운영 체제 및 리소스 로드, 디스크 속도, 네트워크 연결 및 SAN /storage 인프라와 같은 여러 요인에 따라 달라집니다.

Storage Gateway와 함께 VMware HA를 사용하려면 다음 단계를 수행하십시오.

주제

- vSphere VMwareHA 클러스터 구성
- Storage Gateway 콘솔에서 .ova 이미지를 다운로드합니다.
- 게이트웨이 배포
- (선택 사항) 클러스터의 다른 VMs 항목에 대한 재정의 옵션 추가
- 게이트웨이 활성화
- VMware고가용성 구성 테스트

vSphere VMwareHA 클러스터 구성

먼저 클러스터를 아직 생성하지 않았다면 VMware 클러스터를 생성하십시오. VMware클러스터를 생성하는 방법에 대한 자세한 내용은 VMware 설명서의 vSphere HA 클러스터 생성을 참조하십시오.

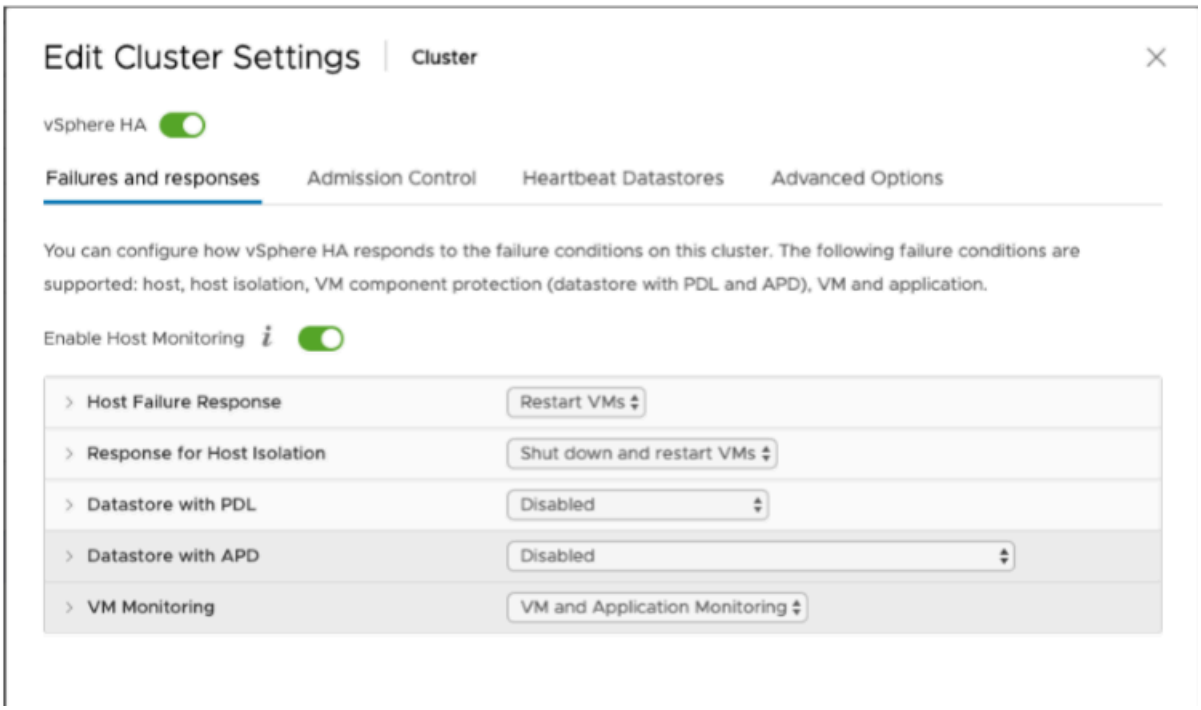
다음으로 Storage Gateway와 함께 작동하도록 VMware 클러스터를 구성합니다.

VMware클러스터를 구성하려면

1. 의 클러스터 설정 편집 페이지에서 VM 모니터링이 VM 및 애플리케이션 모니터링을 위해 구성되어 있는지 확인합니다. VMware vSphere 이렇게 하려면 다음 옵션을 나열된 대로 설정합니다.

   - 호스트 장애 응답: 재시작 VMs
   - 호스트 분리에 대한 응답: 종료 및 재시작 VMs
   - PDL: 비활성화 상태인 데이터스토어
   - : 비활성화된 APD 데이터스토어
   - VM Monitoring(VM 모니터링): VM and Application Monitoring(VM 및 애플리케이션 모니터링)

   예를 들어, 다음 스크린샷을 참조하십시오.



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 VMs 실행 중인 다른 값이 있는 경우 해당 VM에 맞게 이러한 값을 설정하는 것이 좋습니다. .ova에서 VM을 배포할 때까지는 이 작업을 수행할 수 없습니다. 이러한 값 설정에 대한 자세한 내용은 (선택 사항) 클러스터의 다른 VMs 항목에 대한 재정의 옵션 추가 단원을 참조하십시오.

Storage Gateway 콘솔에서 .ova 이미지를 다운로드합니다.

게이트웨이에 대한 .ova 이미지를 다운로드하려면

- Storage Gateway 콘솔의 게이트웨이 설정 페이지에서 게이트웨이 유형과 호스트 플랫폼을 선택한 다음 콘솔에 제공된 링크를 사용하여 Volume Gateway 설정에 설명된 대로.ova를 다운로드합니다.

게이트웨이 배포

구성된 클러스터에서 .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.

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. Storage Gateway .ova 파일을 온프레미스 VMware 환경이나 온프레미스 환경에 배포하는 경우 디스크를 반가상화 디스크라고 합니다. SCSI 반가상화는 VM에 추가하는 가상 디스크를 콘솔이 식별할 수 있도록 게이트웨이 VM이 호스트 운영 체제와 협력하는 모드입니다.

   VM을 구성하여 반가상화된 컨트롤러를 사용하려면

   1. VMware vSphere 클라이언트에서 게이트웨이 VM의 컨텍스트 (마우스 오른쪽 버튼 클릭) 메뉴를 연 다음 설정 편집을 선택합니다.

2. 가상 시스템 속성 대화 상자에서 하드웨어 탭을 선택하고 SCSI컨트롤러 0을 선택한 다음 유형 변경을 선택합니다.
3. SCSI컨트롤러 유형 변경 대화 상자에서 VMware반가상화 SCSI 컨트롤러 유형을 선택한 다음 확인을 선택합니다.

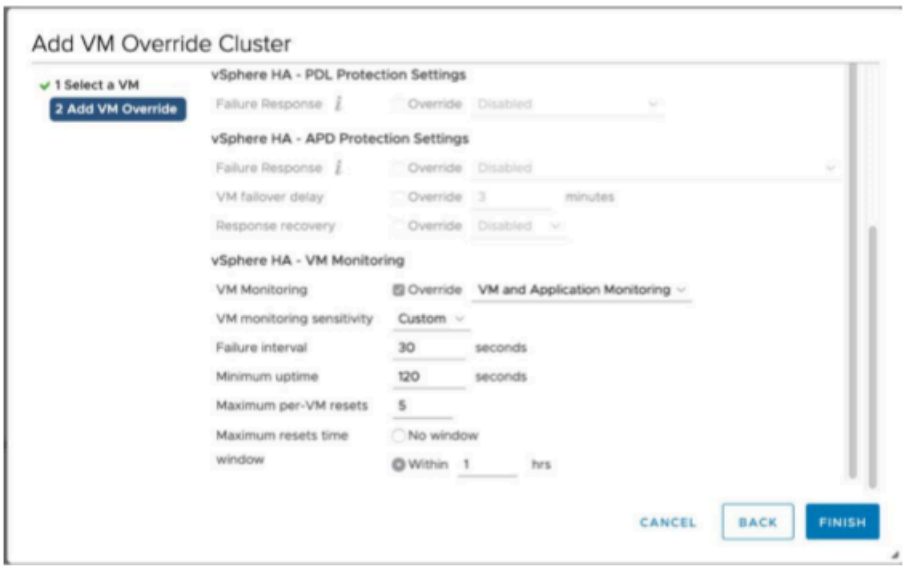
(선택 사항) 클러스터의 다른 VMs 항목에 대한 재정의 옵션 추가

클러스터에서 VMs 실행 중인 다른 VM이 있는 경우 각 VM에 맞게 클러스터 값을 설정하는 것이 좋습니다.

클러스터의 다른 VMs 항목에 대한 재정의 옵션을 추가하려면

1. 의 요약 페이지에서 클러스터를 선택하여 클러스터 페이지를 연 다음 구성을 선택합니다. VMware vSphere
2. 구성 탭을 선택한 다음 VM Overrides(VM 재정의)를 선택합니다.
3. 새 VM 재정의 옵션을 추가하여 각 값을 변경합니다.

   재정의 옵션은 다음 스크린샷을 참조하십시오.



게이트웨이 활성화

게이트웨이에 대한 .ova를 배포한 후 게이트웨이를 활성화합니다. 각 게이트웨이 유형마다 서로 다른 방법에 대한 지침입니다.

게이트웨이를 활성화하려면

- 다음 주제에 설명된 절차를 따릅니다.

  a. 볼륨 게이트웨이를 다음 위치에 연결 AWS
  b. 설정 검토 및 Volume Gateway 활성화
  c. Volume Gateway 구성

VMware고가용성 구성 테스트

게이트웨이를 활성화한 후 구성을 테스트합니다.

VMwareHA 구성을 테스트하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 VMware HA를 테스트할 게이트웨이를 선택합니다.
3. [작업] 에서 VMwareHA 확인을 선택합니다.
4. 나타나는 VMware고가용성 구성 확인 상자에서 확인을 선택합니다.

   > **Note**
   >
   > VMwareHA 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 로그 그룹이 포함된 볼륨 게이트웨이 상태 CloudWatch 로그 가져오기를 참조하십시오.

AWS Storage Gateway의 보안

클라우드 AWS 보안이 최우선 과제입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 기업과 기업 간의 AWS 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 — AWS Amazon Web AWS Services 클라우드에서 서비스를 실행하는 인프라를 보호하는 역할을 합니다. AWS 또한 안전하게 사용할 수 있는 서비스를 제공합니다. AWS Storage Gateway에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램별 범위 내 서비스 규정 준수 참조하십시오.
- 클라우드에서의 보안 — 사용하는 AWS 서비스에 따라 책임이 결정됩니다. 또한 귀하는 귀사의 데이터의 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 방법도 알아봅니다.

주제

- AWS Storage Gateway에서의 데이터 보호
- AWS Storage Gateway의 ID 및 액세스 관리
- 로그인 및 모니터링 AWS Storage Gateway
- AWS Storage Gateway의 규정 준수 검증
- AWS Storage Gateway의 레질리언스
- AWS Storage Gateway의 인프라 보안
- AWS 보안 베스트 프랙티스

AWS Storage Gateway에서의 데이터 보호

AWS 공동 책임 모델 공동 책임 모델 AWS Storage Gateway의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 것을 실행하는 글로벌 인프라를 보호하는 역할을 AWS 클라우드합니다. 사용자는 인프라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리

작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시를 참조하십시오FAQ. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 공동 책임 모델 및AWS 보안 GDPR 블로그의 블로그 게시물을 참조하십시오.

데이터 보호를 위해 AWS 계정 자격 증명을 보호하고 개별 사용자에게 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM) 를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정마다 다단계 인증 (MFA) 을 사용하십시오.
- SSLTLS/를 사용하여 AWS 리소스와 통신하세요. TLS1.2가 필요하고 TLS 1.3을 권장합니다.
- API를 사용하여 사용자 활동 로깅을 설정합니다 AWS CloudTrail.
- 포함된 모든 기본 보안 제어와 함께 AWS 암호화 솔루션을 사용하십시오 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 API an을 AWS 통해 액세스할 때 FIPS 140-3개의 검증된 암호화 모듈이 필요한 경우 엔드포인트를 사용하십시오. FIPS 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 연방 정보 처리 표준 () 140-3을 참조하십시오. FIPS

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, API AWS CLI, 또는 를 AWS 서비스 사용하여 Storage Gateway 또는 다른 작업을 수행하는 경우가 포함됩니다 AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL a를 제공하는 경우 해당 서버에 대한 요청을 URL 검증하기 위해 자격 증명 정보를 에 포함하지 않는 것이 좋습니다.

데이터 암호화 사용 AWS KMS

Storage Gateway는SSL/TLS(보안 소켓 계층/전송 계층 보안) 를 사용하여 게이트웨이 어플라이언스와 스토리지 간에 전송되는 데이터를 암호화합니다. AWS 기본적으로 Storage Gateway는 Amazon S3 관리형 암호화 키 (SSE-S3) 를 사용하여 Amazon S3에 저장하는 모든 데이터를 서버 측에서 암호화합니다. Storage API Gateway를 사용하여 AWS Key Management Service (SSE-KMS) 키를 사용한 서버 측 암호화를 사용하여 클라우드에 저장된 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다.

> **Important**
>
> 서버 측 암호화에 AWS KMS 키를 사용할 때는 대칭 키를 선택해야 합니다. Storage Gateway 에서는 비대칭 키가 지원되지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 대칭 및 비대칭 키 사용을 참조하세요.

파일 공유 암호화

파일 공유의 경우 -를 사용하여 AWS KMS—관리 키로 객체를 암호화하도록 게이트웨이를 구성할 수 있습니다. SSE KMS Storage API Gateway를 사용하여 파일 공유에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 AWS Storage Gateway APIC reateNFSFile 공유를 참조하십시오.

볼륨 암호화

캐싱 및 저장된 볼륨의 경우 Storage Gateway를 사용하여 AWS KMS관리 키로 클라우드에 저장된 볼륨 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다. API 관리 키 중 하나를 키로 지정할 수 있습니다. KMS 볼륨을 암호화하는 데 사용하는 키는 볼륨이 생성된 후에는 변경할 수 없습니다. Storage API Gateway를 사용하여 캐시되거나 저장된 볼륨에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 참조서 CreateCachediSCSIVolume또는 CreateStorediSCSIVolume을AWS Storage Gateway API 참조하십시오.

테이프 암호화

가상 테이프의 경우 Storage Gateway를 사용하여 AWS KMS관리 키로 클라우드에 저장된 테이프 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다. API 관리 키 중 하나를 키로 지정할 수 있습니다. KMS 테이프 데이터를 암호화하는 데 사용하는 키는 테이프가 생성된 후에는 변경할 수 없습니다. Storage API Gateway를 사용하여 가상 테이프에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 AWS Storage Gateway APIC참조를 참조하십시오 CreateTapes.

를 AWS KMS 사용하여 데이터를 암호화할 때는 다음 사항에 유의하십시오.

- 데이터는 클라우드에 암호화되어 저장됩니다. 즉, 데이터는 Amazon S3에서 암호화됩니다.
- IAM사용자는 AWS KMS API 작업을 호출하는 데 필요한 권한을 가지고 있어야 합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 IAM 정책 사용을 참조하십시오. AWS KMS
- AWS AWS KMS 키를 삭제 또는 비활성화하거나 권한 부여 토큰을 취소하면 볼륨 또는 테이프의 데이터에 액세스할 수 없습니다. 자세한 내용은 개발자 안내서의 KMS키 삭제를 참조하십시오.AWS Key Management Service

- KMS암호화된 볼륨에서 스냅샷을 생성하면 스냅샷이 암호화됩니다. 스냅샷은 볼륨의 키를 상속합니다. KMS
- 암호화된 스냅샷에서 새 볼륨을 생성하는 경우 볼륨이 KMS 암호화됩니다. 새 볼륨에 다른 KMS 키를 지정할 수 있습니다.

> **Note**
>
> Storage Gateway는 암호화된 볼륨 또는 암호화된 스냅샷의 복구 지점에서 KMS 암호화되지 않은 볼륨을 생성하는 것을 지원하지 않습니다. KMS

에 대한 자세한 내용은 AWS KMS무엇입니까를 참조하십시오. AWS Key Management Service

볼륨에 대한 CHAP 인증 구성

스토리지 게이트웨이에서 iSCSI 이니시에이터는 볼륨에 iSCSI 대상으로 연결됩니다. 스토리지 게이트웨이는 CHAP(Challenge-Handshake Authentication Protocol)을 사용하여 iSCSI 및 이니시에이터 연결을 인증합니다. CHAP은 스토리지 볼륨 대상에 액세스하려 할 때 인증을 요청함으로써 재생 공격을 방지합니다. 각 볼륨 대상의 경우 하나 이상의 CHAp 자격 증명을 정의할 수 있습니다. [Configure CHAP Credentials] 대화 상자에서 다양한 초기자에 대해 이러한 자격 증명을 보고 편집할 수 있습니다.

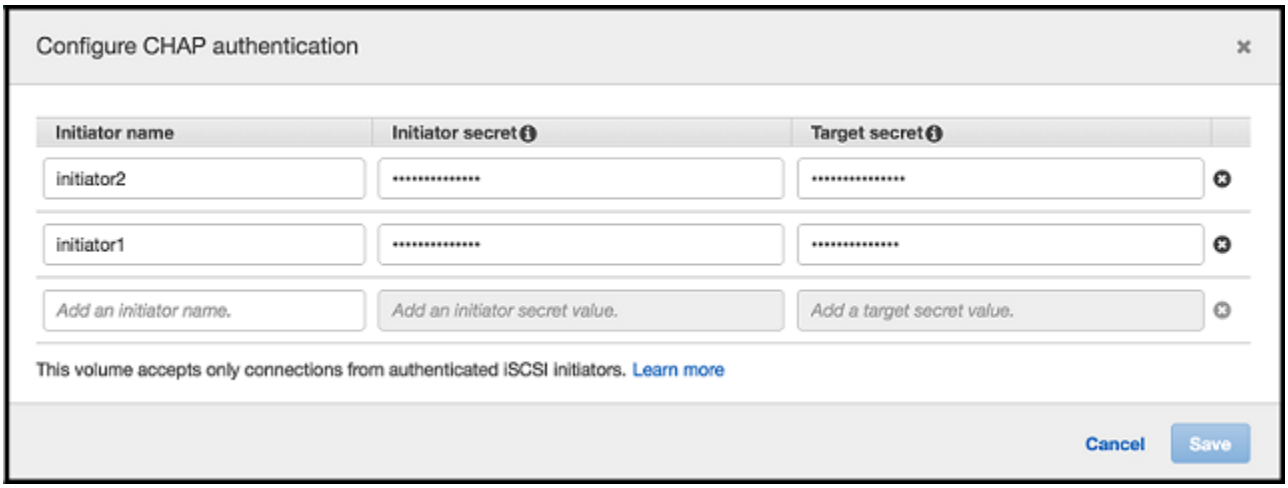
CHAP 자격 증명을 구성하려면

1. Storage Gateway 콘솔에서 볼륨을 선택하고 CHAP 자격 증명을 구성할 볼륨을 선택합니다.
2. 작업에서 CHAP 인증 구성을 선택합니다.
3. 이니시에이터 이름에 초기 사용자의 이름을 입력합니다. 이 이름은 1자 ~ 255자여야 합니다.
4. 이니시에이터 암호에 iSCSI 이니시에이터를 인증하는 데 사용할 비밀 문구를 입력합니다. 초기 사용자 비밀 문구는 12~16자여야 합니다.
5. 대상 암호에 상호 CHAP에 대해 대상을 인증하는 데 사용할 비밀 문구를 지정합니다. 대상 비밀 문구는 12~16자여야 합니다.
6. 저장을 선택하여 항목을 저장합니다.

CHAP 자격 증명을 보거나 업데이트하려면 해당 작업을 수행하는 데 필요한 IAM 역할 권한이 있어야 합니다.

CHAP 자격 증명 보기 및 편집

각 사용자마다 CHAP 자격 증명을 추가, 제거 또는 업데이트할 수 있습니다. CHAP 자격 증명을 보거나 편집하려면 필요한 IAM 역할 권한이 있어야 하며, 이니시에이터 대상이 작동하는 게이트웨이에 연결되어 있어야 합니다.



CHAP 자격 증명을 추가하려면

1. Storage Gateway 콘솔에서 볼륨을 선택하고 CHAP 자격 증명을 추가할 볼륨을 선택합니다.
2. 작업에서 CHAP 인증 구성을 선택합니다.
3. CHAPS 구성 페이지에서 이니시에이터 이름, 이니시에이터 암호 및 대상 암호를 각각의 상자에 제공하고 저장을 선택합니다.

CHAP 자격 증명을 제거하려면

1. Storage Gateway 콘솔에서 볼륨을 선택하고 CHAP 자격 증명을 제거할 볼륨을 선택합니다.
2. 작업에서 CHAP 인증 구성을 선택합니다.
3. 제거할 자격 증명 옆에 있는 X를 클릭하고 저장을 선택합니다.

CHAP 자격 증명을 업데이트하려면

1. Storage Gateway 콘솔에서 볼륨을 선택하고 CHAP을 업데이트할 볼륨을 선택합니다.
2. 작업에서 CHAP 인증 구성을 선택합니다.
3. [Configure CHAP Credentials] 페이지에서 업데이트할 자격 증명에 대한 항목을 변경합니다.
4. 저장을 선택합니다.

AWS Storage Gateway의 ID 및 액세스 관리

AWS Identity and Access Management (IAM) 는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어할 수 AWS 서비스 있도록 도와줍니다. IAM관리자는 AWS SGW 리소스를 사용할 수 있는 인증 (로그인) 및 권한 부여 (권한 보유) 를 받을 수 있는 사용자를 제어합니다. IAM추가 비용 없이 사용할 AWS 서비스 수 있습니다.

주제

고객

AWS Identity and Access Management (IAM) 를 사용하는 방법은 수행하는 작업에 따라 다릅니다. AWS SGW

서비스 사용자 - AWS SGW 서비스를 사용하여 작업을 수행하는 경우 관리자가 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS SGW 기능을 사용하여 작업을 수행함에 따라 추가 권한이 필요할 수 있습니다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 에서 AWS SGW 기능에 액세스할 수 없는 경우 을 참조하십시오AWS Storage Gateway ID 및 액세스 문제 해결.

서비스 관리자 — 회사에서 AWS SGW 리소스를 담당하고 있다면 전체 액세스 권한이 있을 것입니다 AWS SGW. 서비스 사용자가 액세스해야 하는 AWS SGW 기능과 리소스를 결정하는 것은 여러분의 몫입니다. 그런 다음 IAM 관리자에게 서비스 사용자의 권한을 변경해 달라는 요청을 제출해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 IAM 이해하십시오. 회사에서 wth를 사용하는 방법에 대한 자세한 내용은 IAM AWS SGW 을 참조하십시오AWS Storage Gateway의 작동 방식 IAM.

IAM관리자 — IAM 관리자인 경우 액세스 관리를 위한 정책을 작성하는 방법에 대해 자세히 알아보는 것이 좋습니다 AWS SGW. 에서 IAM 사용할 수 있는 AWS SGW ID 기반 정책의 예를 보려면 을 참조하십시오. AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

ID를 통한 인증

인증은 ID 자격 증명을 AWS 사용하여 로그인하는 방법입니다. IAM사용자로서 또는 역할을 수임하여 인증 (로그인 AWS) 을 받아야 합니다. AWS 계정 루트 사용자 IAM

ID 소스를 통해 제공된 자격 증명을 사용하여 페더레이션 ID로 로그인할 수 있습니다. AWS AWS IAM Identity Center (IAMID 센터) 사용자, 회사의 SSO (Single Sign-On) 인증, Google 또는 Facebook 자격 증명이 페더레이션 ID의 예입니다. 페더레이션 ID로 로그인하는 경우 관리자는 이전에 역할을 사용하여 ID 페더레이션을 설정했습니다. IAM 페더레이션을 AWS 사용하여 액세스하는 경우 간접적으로 역할을 수임하는 것입니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 로그인에 대한 자세한 내용은 AWS 로그인 사용 설명서의 내 로그인 방법을 참조하십시오. AWS AWS 계정

AWS 프로그래밍 방식으로 액세스하는 경우 자격 증명을 사용하여 요청에 암호로 서명할 수 있는 소프트웨어 개발 키트 (SDKCLI) 와 명령줄 인터페이스 () 가 AWS 제공됩니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 사용 IAM설명서의 AWS API요청 서명을 참조하십시오.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어, 계정 보안을 강화하기 위해 다단계 인증 (MFA) 을 사용할 AWS 것을 권장합니다. 자세한 내용은 사용 설명서의 다단계 인증 및 사용 AWS IAM Identity Center 설명서의 다단계 인증 사용 (MFA) 을 IAM 참조하십시오. AWS

AWS 계정 루트 사용자

계정을 AWS 계정만들 때는 먼저 계정의 모든 AWS 서비스 리소스에 대한 완전한 액세스 권한을 가진 하나의 로그인 ID로 시작합니다. 이 ID를 AWS 계정 루트 사용자라고 하며, 계정을 만들 때 사용한 이메일 주소와 비밀번호로 로그인하여 액세스할 수 있습니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 사용 설명서의 루트 사용자 자격 증명이 필요한 작업을 참조하십시오. IAM

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 비롯한 수동 AWS 서비스 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 액세스하도록 하는 것입니다.

페더레이션 ID는 기업 사용자 디렉토리, 웹 ID 공급자, Identity Center 디렉터리의 사용자 또는 ID 소스를 통해 제공된 자격 증명을 사용하여 액세스하는 AWS 서비스 모든 사용자를 말합니다. AWS

Directory Service페더레이션 ID에 AWS 계정액세스하면 이들이 역할을 맡고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAMIdentity Center에서 사용자 및 그룹을 만들거나 자체 ID 소스의 사용자 및 그룹 집합에 연결하고 동기화하여 AWS 계정 모든 사용자 및 애플리케이션에서 사용할 수 있습니다. ID 센터에 대한 자세한 내용은 IAM ID 센터란 IAM 무엇입니까? 를 참조하십시오. AWS IAM Identity Center 사용 설명서에서

IAM 사용자 및 그룹

IAM사용자란 단일 사용자 또는 애플리케이션에 대한 특정 권한을 가진 사용자 내의 ID입니다. AWS 계정 가능하면 암호 및 액세스 키와 같은 장기 자격 증명을 가진 IAM 사용자를 만드는 대신 임시 자격 증명을 사용하는 것이 좋습니다. 하지만 특정 사용 사례에서 IAM 사용자의 장기 자격 증명이 필요한 경우에는 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 사용 설명서의 장기 자격 증명이 필요한 사용 사례에 대한 정기적인 액세스 키 IAM 교체를 참조하십시오.

IAM그룹은 IAM 사용자 컬렉션을 지정하는 ID입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 이름을 지정한 IAMAdmins그룹을 만들고 해당 그룹에 IAM 리소스를 관리할 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세히 알아보려면 사용 설명서의 역할 대신 IAM 사용자를 만드는 시기를 참조하십시오. IAM

IAM역할

IAM역할은 특정 권한을 AWS 계정 가진 사용자 내의 ID입니다. IAM사용자와 비슷하지만 특정인과 관련이 있는 것은 아닙니다. 역할을 AWS Management Console 전환하여 에서 일시적으로 IAM 역할을 맡을 수 있습니다. AWS CLI or AWS API 작업을 호출하거나 사용자 지정을 사용하여 역할을 수임할 수 URL 있습니다. 역할 사용 방법에 대한 자세한 내용은 사용 IAM설명서의 IAM역할 사용을 참조하십시오.

IAM임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션을 위한 역할에 대한 자세한 내용은 IAM사용 설명서의 타사 ID 제공자를 위한 역할 생성을 참조하십시오. IAMIdentity Center를 사용하는 경우 권한 집합을 구성합니다. ID가 인증된 후 액세스할

수 있는 대상을 제어하기 위해 IAM Identity Center는 권한 집합을 역할의 상관 관계와 연결합니다. IAM 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 권한 세트를 참조하세요.

- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할이 역할을 맡아 특정 작업에 대해 일시적으로 다른 권한을 부여받을 수 있습니다. IAM
- 계정 간 액세스 - IAM 역할을 사용하여 다른 계정의 사용자 (신뢰할 수 있는 사용자) 가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 하지만 일부 AWS 서비스경우에는 역할을 프록시로 사용하는 대신 정책을 리소스에 직접 연결할 수 있습니다. 계정 간 액세스에 대한 역할과 리소스 기반 정책 간의 차이점을 알아보려면 사용 설명서의 교차 계정 리소스 액세스를 참조하십시오. IAM IAM
- 서비스 간 액세스 — 일부는 다른 기능을 AWS 서비스 사용합니다. AWS 서비스예를 들어, 서비스를 호출하면 해당 서비스가 Amazon에서 애플리케이션을 EC2 실행하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
  - 전달 액세스 세션 (FAS) — IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS전화를 거는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하라는 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.
  - 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM 역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 만들고, 수정하고, 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스
  - 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행 중인 애플리케이션 EC2 — IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS API 요청을 보내는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. AWS CLI EC2인스턴스 내에 액세스 키를 저장하는 것보다 이 방법이 더 좋습니다. EC2인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있게 하려면 인스턴스에 연결된 인스턴스 프로필을 만들어야 합니다. 인스턴스 프로필에는 역할이 포함되며, 이를 통해 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 내용은 사용 설명서의 IAM역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여를 IAM 참조하십시오.

IAM역할을 사용할지 IAM 사용자를 사용할지 알아보려면 사용 설명서의 IAM 역할 생성 시기 (사용자 대신) 를 IAM참조하십시오.

정책을 사용한 액세스 관리

정책을 만들고 이를 AWS ID 또는 리소스에 AWS 연결하여 액세스를 제어할 수 있습니다. 정책은 ID 또는 리소스와 연결될 때 AWS 해당 권한을 정의하는 객체입니다. AWS 주도자 (사용자, 루트 사용자 또는 역할 세션) 가 요청할 때 이러한 정책을 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는지를 결정합니다. 대부분의 정책은 JSON 문서로 AWS 저장됩니다. JSON정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM사용 설명서의 JSON 정책 개요를 참조하십시오.

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

IAM정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, `iam:GetRole` 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI, 또는 에서 역할 정보를 가져올 수 AWS API 있습니다.

보안 인증 기반 정책

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 내 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립형 정책입니다. AWS 계정관리형 정책에는 AWS 관리형 정책과 고객 관리형 정책이 포함됩니다. 관리형 정책과 인라인 정책 중 하나를 선택하는 방법을 알아보려면 IAM사용 설명서의 관리형 정책과 인라인 정책 중 선택을 참조하십시오.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리

자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 IAM 정책에서는 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록 () ACLs

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

지원하는 서비스의 VPC 예로는 Amazon S3와 Amazon이 ACLs 있습니다. AWS WAF자세한 내용은 Amazon 심플 스토리지 서비스 개발자 안내서의 액세스 제어 목록 (ACL) 개요를 참조하십시오. ACLs

기타 정책 타입

AWS 일반적이지 않은 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 ID 기반 정책이 IAM 엔티티 (IAM사용자 또는 역할) 에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. `Principal` 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 사용 IAM설명서의 IAM 엔티티에 대한 권한 경계를 참조하십시오.
- 서비스 제어 정책 (SCPs) - SCPs 조직 또는 OU (조직 구성 단위) 에 대한 최대 권한을 지정하는 JSON AWS Organizations정책입니다. AWS Organizations 기업이 소유한 여러 AWS 계정 개를 그룹화하고 중앙에서 관리하는 서비스입니다. 조직의 모든 기능을 사용하도록 설정하면 일부 또는 모든 계정에 서비스 제어 정책 (SCPs) 을 적용할 수 있습니다. 각 항목을 포함하여 구성원 계정의 엔티티에 대한 권한을 SCP AWS 계정 루트 사용자제한합니다. Organizations 및 SCPs 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하십시오.
- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM사용 설명서의 세션 정책을 참조하십시오.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 여러 정책 유형이 관련된 경우 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM사용 설명서의 정책 평가 로직을 참조하십시오.

AWS Storage Gateway의 작동 방식 IAM

액세스를 관리하는 IAM 데 사용하기 전에 사용할 수 있는 IAM 기능에 대해 알아보십시오 AWS SGW. AWS SGW

IAM AWS Storage Gateway와 함께 사용할 수 있는 기능

IAM기능	AWS SGW지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC(정책의 태그)	부분
임시 보안 인증	예
포워드 액세스 세션 (FAS)	예
서비스 역할	예
서비스 연결 역할	예

대부분의 IAM 기능과 함께 작동하는 방식 AWS SGW 및 기타 AWS 서비스를 개괄적으로 보려면 IAM 사용 IAM 설명서에서 함께 작동하는AWS 서비스를 참조하십시오.

아이덴티티 기반 정책은 다음과 같습니다. AWS SGW

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. ID 기반 정책을 만드는 방법을 알아보려면 사용 설명서의 IAM정책 생성을 참조하십시오. IAM

IAMID 기반 정책을 사용하면 허용 또는 거부된 작업 및 리소스는 물론 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 사용 IAM설명서의 IAM JSON 정책 요소 참조를 참조하십시오.

아이덴티티 기반 정책 예시 AWS SGW

AWS SGWID 기반 정책의 예를 보려면 을 참조하십시오. AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

내 리소스 기반 정책 AWS SGW

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 연동 사용자 등이 포함될 수 있습니다. AWS 서비스

계정 간 액세스를 활성화하려면 다른 계정의 전체 계정 또는 IAM 엔티티를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 AWS 계정경우 신뢰할 수 있는 계정의 IAM 관리자는 보안 주체 (사용자 또는 역할) 에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔터티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM

에 대한 정책 조치 AWS SGW

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.

정책 `Action` 요소는 JSON 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 관련 AWS API 작업과 이름이 같습니다. 일치하는 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. API 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

AWS SGW작업 목록을 보려면 서비스 권한 부여 참조의 AWS Storage Gateway에서 정의한 작업을 참조하십시오.

정책 조치는 조치 앞에 다음 접두사를 AWS SGW 사용합니다.

```
sgw
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

AWS SGWID 기반 정책의 예를 보려면 을 참조하십시오. AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

에 대한 정책 리소스 AWS SGW

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`JSON정책 요소는 작업이 적용되는 하나 또는 여러 개의 객체를 지정합니다. 문장에는 `Resource`또는 `NotResource`요소가 반드시 추가되어야 합니다. Amazon 리소스 이름 (ARN) 을 사용하여 리소스를 지정하는 것이 가장 좋습니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS SGW리소스 유형 및 해당 ARNs 리소스 유형 목록을 보려면 서비스 권한 부여 참조의 AWS Storage Gateway에서 정의한 리소스를 참조하십시오. 각 리소스에 지정할 수 있는 작업을 알아보려면 AWS Storage Gateway에서 정의하는 작업을 참조하십시오. ARN

AWS SGWID 기반 정책의 예를 보려면 을 참조하십시오. AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

에 대한 정책 조건 키 AWS SGW

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소(또는 `Condition` 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. `Condition` 요소는 옵션입니다. 같거나 작음과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 `Condition` 요소를 지정하거나 단일 `Condition` 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 `AND` 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우 는 논리적 `OR` 연산을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 리소스에 IAM 사용자 이름이 태그가 지정된 경우에만 리소스에 대한 액세스 권한을 IAM 사용자에게 부여할 수 있습니다. 자세한 내용은 IAM사용 설명서의 IAM 정책 요소: 변수 및 태그를 참조하십시오.

AWS 글로벌 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 글로벌 조건 키를 보려면 IAM사용 설명서의AWS 글로벌 조건 컨텍스트 키를 참조하십시오.

AWS SGW조건 키 목록을 보려면 서비스 권한 부여 참조의 AWS Storage Gateway의 조건 키를 참조하십시오. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 AWS Storage Gateway에서 정의한 작업을 참조하십시오.

AWS SGWID 기반 정책의 예를 보려면 을 참조하십시오. AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

ACLs에서 AWS SGW

지원ACLs: 아니요

액세스 제어 목록 (ACLs) 은 리소스에 액세스할 수 있는 권한을 가진 주체 (계정 구성원, 사용자 또는 역할) 를 제어합니다. ACLs정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 JSON 비슷합니다.

ABAC... AWS SGW

지원 ABAC (정책의 태그): 부분

속성 기반 액세스 제어 (ABAC) 는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. AWS에서는 이러한 속성을 태그라고 합니다. IAM엔티티 (사용자 또는 역할) 및 여러 AWS 리소스에 태그를 첨부할 수 있습니다. 의 ABAC 첫 번째 단계는 엔티티와 리소스에 태그를 지정하는 것입니다. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하도록 ABAC 정책을 설계합니다.

ABAC빠르게 성장하는 환경에서 유용하며 정책 관리가 복잡해지는 상황에도 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 What is ABAC? 를 참조하십시오. ABAC IAM사용 설명서에서. 설정 ABAC 단계가 포함된 자습서를 보려면 사용 IAM설명서의 속성 기반 액세스 제어 사용 (ABAC) 을 참조하십시오.

임시 자격 증명 사용: AWS SGW

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인하면 작동하지 AWS 서비스 않는 것도 있습니다. 임시 자격 증명을 사용하는 AWS 서비스 방법을 비롯한 추가 정보는 IAM사용 설명서의 AWS 서비스 해당 자격 증명을 참조하십시오. IAM

사용자 이름과 암호를 제외한 다른 방법을 AWS Management Console 사용하여 로그인하는 경우 임시 자격 증명을 사용하는 것입니다. 예를 들어 회사의 Single Sign-On (SSO) 링크를 AWS 사용하여 액세스하는 경우 이 프로세스에서 자동으로 임시 자격 증명을 생성합니다. 또한 콘솔에 사용자로 로그

인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM사용 설명서의 역할 전환 (콘솔) 을 참조하십시오.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 AWS API 있습니다. 그런 다음 해당 임시 자격 증명을 사용하여 액세스할 수 AWS있습니다. AWS 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성할 것을 권장합니다. 자세한 내용은 의 임시 보안 자격 증명을 참조하십시오. IAM

포워드 액세스 세션: AWS SGW

순방향 액세스 세션 지원 (FAS): 예

에서 IAM 사용자 또는 역할을 사용하여 작업을 수행하는 AWS경우 사용자는 보안 주체로 간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS를 호출하는 주체의 권한을 다운스트림 서비스에 AWS 서비스 요청하기 위한 요청과 결합하여 사용합니다. AWS 서비스 FAS요청은 다른 서비스 AWS 서비스 또는 리소스와의 상호 작용이 필요한 요청을 서비스가 수신한 경우에만 이루어집니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS요청 시 적용되는 정책 세부 정보는 전달 액세스 세션을 참조하십시오.

AWS SGW의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 간주하는 IAM역할입니다. IAM관리자는 내부에서 IAM 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 사용 설명서의 역할 만들기를 참조하여 권한을 위임하십시오IAM. AWS 서비스

> **Warning**
>
> 서비스 역할의 권한을 변경하면 AWS SGW 기능이 중단될 수 있습니다. 서비스 역할을 편집하기 위한 지침이 AWS SGW 제공되는 경우에만 서비스 역할을 편집하십시오.

서비스 연결 역할은 다음과 같습니다. AWS SGW

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할 유형입니다. AWS 서비스서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 사용자에게 AWS 계정 표시되며 해당 서비스가 소유합니다. IAM관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할을 만들거나 관리하는 방법에 대한 자세한 내용은 함께 작동하는 AWS 서비스를 참조하십시오. IAM 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

AWS Storage Gateway에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS SGW 리소스를 만들거나 수정할 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수도 없습니다 AWS API. IAM관리자는 IAM 정책을 생성하여 필요한 리소스에서 작업을 수행할 수 있는 권한을 사용자에게 부여할 수 있습니다. 그러면 관리자가 역할에 IAM 정책을 추가할 수 있으며, 사용자는 역할을 수임할 수 있습니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 만드는 방법을 알아보려면 사용 IAM설명서에서 IAM 정책 생성을 참조하십시오.

각 리소스 유형의 형식을 비롯하여 에서 정의한 AWS SGW 작업 및 리소스 유형에 ARNs 대한 자세한 내용은 서비스 권한 부여 참조의 AWS Storage Gateway의 작업, 리소스 및 조건 키를 참조하십시오.

주제

- 정책 모범 사례
- AWS SGW콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

ID 기반 정책은 누군가가 사용자 계정에서 AWS SGW 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책으로 시작하여 최소 권한 권한으로 이동 — 사용자와 워크로드에 권한을 부여하려면 여러 일반적인 사용 사례에 권한을 부여하는 AWS 관리형 정책을 사용하세요. 해당 내용은 에서 사용할 수 있습니다. AWS 계정사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 더 줄이는 것이 좋습니다. 자세한 내용은 IAM사용 설명서의 AWS 관리형 정책 또는 작업 기능에 대한AWS 관리형 정책을 참조하십시오.
- 최소 권한 적용 — IAM 정책으로 권한을 설정하는 경우 작업 수행에 필요한 권한만 부여하십시오. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 IAM 적용하는 방법에 대한 자세한 내용은 사용 설명서의 정책 및 권한을 참조하십시오. IAM IAM

- IAM정책의 조건을 사용하여 액세스를 추가로 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, 를 사용하여 모든 요청을 전송하도록 지정하는 정책 조건을 작성할 수 SSL 있습니다. 예를 AWS 서비스들어 특정 작업을 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 AWS CloudFormation있습니다. 자세한 내용은 IAM사용 설명서의 IAMJSON정책 요소: 조건을 참조하십시오.
- IAMAccess Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 새 정책과 기존 정책을 검증하여 정책이 IAM 정책 언어 (JSON) 및 IAM 모범 사례를 준수하는지 확인합니다. IAMAccess Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 검사와 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 사용 설명서의 IAMAccess Analyzer 정책 검증을 참조하십시오. IAM
- 다단계 인증 필요 (MFA) - 사용자 또는 루트 IAM 사용자가 필요한 시나리오가 있는 경우 보안을 강화하려면 이 기능을 MFA 켜십시오. AWS 계정 API작업 호출 MFA 시기를 요구하려면 정책에 MFA 조건을 추가하세요. 자세한 내용은 IAM사용 설명서의 MFA -보호된 API 액세스 구성을 참조하십시오.

의 모범 사례에 IAM 대한 자세한 내용은 IAM사용 설명서의 보안 모범 사례를 참조하십시오. IAM

AWS SGW콘솔 사용

AWS Storage Gateway 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 내 AWS SGW 리소스의 세부 정보를 나열하고 볼 수 있어야 AWS 계정합니다. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 AWS API 없습니다. 대신 수행하려는 작업과 일치하는 API 작업에만 액세스를 허용하세요.

사용자와 역할이 AWS SGW 콘솔을 계속 사용할 수 있도록 하려면 AWS SGW *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔티티에 연결하세요. 자세한 내용은 사용 설명서의 IAM사용자에게 권한 추가를 참조하십시오.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 만드는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 OR를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 AWS CLI 권한이 포함됩니다. AWS API

```
{
    "Version": "2012-10-17",
```

```
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

AWS Storage Gateway ID 및 액세스 문제 해결

다음 정보를 사용하면 및 으로 작업할 때 발생할 수 있는 일반적인 문제를 AWS SGW 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- 다음과 같은 작업을 수행할 권한이 없습니다. AWS SGW
- 저는 IAM을 수행할 권한이 없습니다. PassRole
- 외부 사용자가 내 AWS SGW 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다음과 같은 작업을 수행할 권한이 없습니다. AWS SGW

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. sgw:*GetWidget*

```
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 mateojackson사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류가 발생하는 경우 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. iam:PassRole AWS SGW

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 에서 작업을 marymajor 수행하려고 할 때 발생합니다. AWS SGW 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS SGW 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제

어 목록 (ACLs) 을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 AWS SGW 지원 여부를 알아보려면 을 참조하십시오. AWS Storage Gateway의 작동 방식 IAM
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 사용 설명서에서 AWS 계정 자신이 소유한 다른 IAM 사용자의 액세스 권한 제공을 IAM 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을 참조하십시오. AWS 계정
- ID 페더레이션을 통해 액세스를 제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에게 액세스 제공 (ID 페더레이션) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 리소스 액세스를 참조하십시오. IAM IAM

로그인 및 모니터링 AWS Storage Gateway

Storage Gateway는 Storage Gateway에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공하는 서비스와 통합됩니다. AWS CloudTrail CloudTrail Storage Gateway에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Storage Gateway 콘솔에서의 통화와 Storage Gateway API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Storage Gateway에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로의 지속적인 이벤트 전송을 활성화할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Storage Gateway에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 AWS CloudTrail 사용 설명서를 참조하십시오.

Storage Gateway 정보 입력 CloudTrail

CloudTrail 계정을 만들 때 Amazon Web Services 계정에서 활성화됩니다. Storage Gateway에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됩니다. Amazon Web Services 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 기록으로 CloudTrail 이벤트 보기를 참조하십시오.

Storage Gateway에 대한 이벤트를 포함하여 Amazon Web Services 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할

수 있습니다. 기본적으로 콘솔에서 트레일을 생성하면 트레일이 모든 AWS 지역에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- 추적 생성 개요
- CloudTrail 지원되는 서비스 및 통합
- 에 대한 Amazon SNS 알림 구성 CloudTrail
- 여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신

모든 Storage Gateway 작업은 로깅되며 작업 주제에서 문서화됩니다. 예를 들어, `ActivateGatewayListGateways`, 를 호출하고 `ShutdownGateway` 작업을 수행하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에 대한 정보가 들어 있습니다. 보안 인증 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에 대한 임시 보안 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 CloudTrail userIdentity요소를 참조하십시오.

Storage Gateway 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 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": "2014-12-04T16:19:00Z",
                  "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 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. ListGateways

```
{
 "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"
             }]
}
```

AWS Storage Gateway의 규정 준수 검증

타사 감사자가 여러 규정 AWS 준수 프로그램의 일환으로 AWS Storage Gateway의 보안 및 규정 준수를 평가합니다. 여기에는SOC,, FedPCI,ISO,,RAMP,HIPAA, C5MTSC, K-, ENS High ISMSOSPAR, 및 등이 포함됩니다. HITRUST CSF

특정 규정 준수 프로그램의 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 범위 내AWS 서비스 규정 준수 참조하십시오. 일반 정보는 AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html 참조하십시오 AWS Artifact.

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 사항을 설명하고 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다. AWS
- HIPAA보안 및 규정 준수를 위한 설계 백서 — 이 백서는 기업이 규정을 준수하는 애플리케이션을 개발하는 데 사용할 수 있는 방법을 설명합니다. AWS HIPAA
- AWS 규정 준수 리소스AWS — 이 통합 문서 및 가이드 모음은 해당 산업 및 지역에 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— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 AWS 되는 내부 보안 상태를 종합적으로 보여줍니다.

AWS Storage Gateway의 레질리언스

AWS 글로벌 인프라는 AWS 지역 및 가용 영역을 중심으로 구축됩니다. AWS 지역은 물리적으로 분리되고 격리된 여러 가용 영역을 제공하며, 이러한 가용 영역은 지연 시간이 짧고 처리량이 높으며 중복성이 높은 네트워킹으로 연결됩니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 극복 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 지역 및 가용 영역에 대한 자세한 내용은 글로벌 인프라를 참조하십시오AWS .

AWS 글로벌 인프라 외에도 Storage Gateway는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 여러 기능을 제공합니다.

- VMware vSphere 고가용성 (VMwareHA) 을 사용하면 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 자세한 내용은 Storage Gateway와 함께 VMware vSphere 고가용성 사용 단원을 참조하십시오.
- 볼륨을 AWS Backup 백업하는 데 사용합니다. 자세한 내용은 볼륨 백업 단원을 참조하십시오.
- 복구 지점에서 볼륨을 복제합니다. 자세한 내용은 볼륨 복제 단원을 참조하십시오.

AWS Storage Gateway의 인프라 보안

관리형 서비스인 AWS Storage Gateway는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 따라 보호됩니다.

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Storage Gateway에 액세스할 수 있습니다. 클라이언트는 전송 계층 보안 (TLS) 1.2를 지원해야 합니다. 또한 클라이언트는 Ephemeral Diffie-Hellman () 또는 타원 곡선 Epememeral Diffie-Hellman (PFS) 과 같이 완벽한 순방향 기밀성 () 을 갖춘 암호 제품군을 지원해야 합니다. DHE ECDHE Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID 및 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. IAM 또는 AWS Security Token Service(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

> **Note**
>
> AWS Storage Gateway 어플라이언스는 관리되는 가상 시스템으로 취급해야 하며, 어떤 식으로든 설치를 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 게이트웨이 업데이트 메커니즘 이외의 방법을 사용하여 스캔 소프트웨어를 설치하거나 소프트웨어 패키지를 업데이트하려고 하면 게이트웨이가 오작동하고 게이트웨이를 지원하거나 수정하는 데 영향을 미칠 수 있습니다.
>
> AWS 정기적으로 검토, 분석 및 CVEs 수정합니다. 당사는 일반적인 소프트웨어 릴리스 주기의 일환으로 이러한 문제에 대한 수정 사항을 Storage Gateway에 통합합니다. 이러한 수정 사항은 일반적으로 정기 유지 관리 기간 중에 일반 게이트웨이 업데이트 프로세스의 일부로 적용됩니다. 게이트웨이 업데이트에 대한 자세한 내용은 콘솔을 참조하십시오. AWS Storage Gateway

AWS 보안 베스트 프랙티스

AWS 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.

게이트웨이 문제 해결

아래와 같이 게이트웨이, 파일 공유, 볼륨, 가상 테이프 및 스냅샷과 관련된 문제의 해결에 대한 정보를 얻을 수 있습니다. 온-프레미스 게이트웨이 문제 해결 정보는 Microsoft Hyper-V VMware ESXi 클라이언트와 Microsoft Hyper-V 클라이언트 모두에 배포된 게이트웨이를 다룹니다. 파일 공유에 대한 문제 해결 정보는 File Gateway 유형에 적용됩니다. 볼륨에 대한 문제 해결 정보는 Volume Gateway 유형에 적용됩니다. 테이프에 대한 문제 해결 정보는 Tape Gateway 유형에 적용됩니다. 게이트웨이 문제에 대한 문제 해결 정보는 메트릭 사용에 적용됩니다. CloudWatch 고가용성 문제에 대한 문제 해결 정보는 VMware vSphere 고가용성 (HA) 플랫폼에서 실행되는 게이트웨이를 다룹니다.

주제

문제 해결: Storage Gateway 콘솔의 게이트웨이 오프라인

다음 문제 해결 정보를 사용하여 AWS Storage Gateway 콘솔에 게이트웨이가 오프라인 상태인 것으로 표시되는 경우 어떻게 해야 할지 결정하십시오.

다음 이유 중 하나 이상으로 인해 게이트웨이가 오프라인으로 표시될 수 있습니다.

- 게이트웨이는 Storage Gateway 서비스 엔드포인트에 연결할 수 없습니다.
- 게이트웨이가 예기치 않게 종료되었습니다.
- 게이트웨이와 연결된 캐시 디스크의 연결이 끊겼거나 수정되었거나 장애가 발생했습니다.

게이트웨이를 다시 온라인 상태로 전환하려면 게이트웨이가 오프라인으로 전환된 원인이 된 문제를 식별하여 해결하십시오.

연결된 방화벽 또는 프록시를 확인하세요.

프록시를 사용하도록 게이트웨이를 구성했거나 게이트웨이를 방화벽 뒤에 배치한 경우 프록시 또는 방화벽의 액세스 규칙을 검토하십시오. 프록시 또는 방화벽은 Storage Gateway에 필요한 네트워크 포트 및 서비스 엔드포인트로 들어오고 나가는 트래픽을 허용해야 합니다. 자세한 내용은 네트워크 및 방화벽 요구 사항 사항을 참조하십시오.

게이트웨이 트래픽에 대한 지속적 SSL 또는 심층 패킷 검사가 이루어지는지 확인하세요.

게이트웨이와 사이의 네트워크 트래픽에 대해 현재 SSL 또는 딥 패킷 검사가 수행되고 있는 경우 게이트웨이가 필요한 서비스 엔드포인트와 통신하지 못할 수 있습니다. AWS게이트웨이를 다시 온라인 상태로 전환하려면 검사를 비활성화해야 합니다.

하이퍼바이저 호스트의 정전 또는 하드웨어 장애 확인

게이트웨이의 하이퍼바이저 호스트에서 정전이나 하드웨어 장애가 발생하면 게이트웨이가 예기치 않게 종료되고 연결할 수 없게 될 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 복구 모범 사례를 참조하십시오.

관련 캐시 디스크에 문제가 있는지 확인하세요.

게이트웨이와 연결된 캐시 디스크 중 하나 이상이 제거, 변경 또는 크기 조정되었거나 손상된 경우 게이트웨이가 오프라인 상태가 될 수 있습니다.

하이퍼바이저 호스트에서 작업 중인 캐시 디스크를 제거한 경우:

1. 게이트웨이를 종료합니다.
2. 디스크를 다시 추가합니다.

> **Note**
>
> 디스크를 동일한 디스크 노드에 추가했는지 확인하십시오.

3. 게이트웨이를 다시 시작합니다.

캐시 디스크가 손상되었거나 교체되었거나 크기가 조정된 경우:

1. 게이트웨이를 종료합니다.
2. 캐시 디스크를 재설정합니다.
3. 캐시 스토리지용으로 디스크를 재구성하십시오.
4. 게이트웨이를 다시 시작합니다.

문제 해결: 게이트웨이 활성화 중 내부 오류

Storage Gateway 활성화 요청은 두 네트워크 경로를 통과합니다. 클라이언트가 보낸 수신 활성화 요청은 포트 80을 통해 게이트웨이의 가상 머신 (VM) 또는 Amazon Elastic Compute Cloud (AmazonEC2) 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 메시지로 클라이언트에 응답합니다.

다음 문제 해결 정보를 사용하여 활성화를 시도할 때 내부 오류 메시지가 나타나는 경우 취해야 할 조치를 결정하십시오. AWS Storage Gateway

> **Note**
>
> - 최신 가상 머신 이미지 파일 또는 Amazon Machine Image (AMI) 버전을 사용하여 새 게이트웨이를 배포해야 합니다. 오래된 AMI 게이트웨이를 사용하는 게이트웨이를 활성화하려고 하면 내부 오류가 발생합니다.
> - 다운로드하기 전에 배포하려는 올바른 게이트웨이 유형을 선택했는지 확인하십시오. AMI .ova 파일과 AMIs 각 게이트웨이 유형은 서로 다르며 서로 바꿔서 사용할 수 없습니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류를 해결합니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 확인 및 구성을 수행하십시오.

필요한 포트를 확인하세요.

온프레미스에 배포된 게이트웨이의 경우 로컬 방화벽에서 포트가 열려 있는지 확인하세요. Amazon 인스턴스에 배포된 게이트웨이의 경우 EC2 인스턴스의 보안 그룹에서 포트가 열려 있는지 확인하십시

오. 포트가 열려 있는지 확인하려면 서버의 퍼블릭 엔드포인트에서 텔넷 명령을 실행하십시오. 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 도달할 수 있는지 확인하려면 게이트웨이의 로컬 VM 콘솔 (온프레미스에 배포된 게이트웨이의 경우) 에 액세스하십시오. 또는 게이트웨이 인스턴스 (SSHAmazon에 배포된 게이트웨이의 경우EC2) 로 이동할 수 있습니다. 그런 다음 네트워크 연결 테스트를 실행합니다. 테스트가 반환되는지 확인합니다[PASSED]. 자세한 내용은 게이트웨이의 네트워크 연결 테스트 게이트웨이의 인터넷 연결 테스트를 참조하십시오.

> **Note**
>
> 게이트웨이 콘솔의 기본 로그인 사용자 이름은 이고 admin 기본 비밀번호는 입니다password.

방화벽 보안이 게이트웨이에서 퍼블릭 엔드포인트로 전송되는 패킷을 수정하지 않는지 확인하십시오.

SSL검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안은 게이트웨이에서 전송되는 패킷을 방해할 수 있습니다. 활성화 엔드포인트가 예상한 것과 SSL 다르게 인증서를 수정하면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 포트 443의 기본 활성화 엔드포인트 (anon-cp.storagegateway.region.amazonaws.com) 에서 Open SSL 명령을 실행합니다. 게이트웨이와 동일한 서브넷에 있는 시스템에서 이 명령을 실행해야 합니다.

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> Replace *region* 당신과 함께. AWS 리전

진행 중인 SSL 검사가 없는 경우 명령은 다음과 비슷한 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
---
```

SSL검사가 진행 중인 경우 응답에는 다음과 같이 변경된 인증서 체인이 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 인증서를 인식하는 경우에만 SSL 핸드셰이크를 수락합니다. SSL 즉, 엔드포인트로 향하는 게이트웨이의 아웃바운드 트래픽은 네트워크의 방화벽이 수행하는 검사에서 제외되어야 합니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화를 확인하세요.

시간 차이가 너무 심하면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 차이는 60초를 넘지 않아야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하십시오.

Amazon EC2 인스턴스에 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이가 시간을 제대로 동기화할 수 있도록 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인하십시오.

- 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 (AmazonVPC) 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 검사 및 구성을 수행하십시오.

필요한 포트를 확인하십시오.

로컬 방화벽 (온프레미스에 배포된 게이트웨이의 경우) 또는 보안 그룹 (EC2Amazon에 배포된 게이트웨이의 경우) 내의 필수 포트가 열려 있는지 확인하십시오. 게이트웨이를 Storage Gateway 엔드포인트에 연결하는 데 필요한 VPC 포트는 게이트웨이를 퍼블릭 엔드포인트에 연결할 때 필요한 포트와 다릅니다. Storage Gateway VPC 엔드포인트에 연결하려면 다음 포트가 필요합니다.

- TCP443
- TCP1026
- TCP1027
- TCP1028

- TCP1031
- TCP2222

자세한 내용은 Storage 엔드포인트 생성을 참조하십시오.

또한 Storage Gateway VPC 엔드포인트에 연결된 보안 그룹을 확인하십시오. 엔드포인트에 연결된 기본 보안 그룹은 필요한 포트를 허용하지 않을 수 있습니다. 필요한 포트를 통해 게이트웨이의 IP 주소 범위에서 들어오는 트래픽을 허용하는 새 보안 그룹을 생성하십시오. 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 다음 보안 그룹 탭을 선택합니다.

필요한 포트가 열려 있는지 확인하려면 Storage Gateway VPC 엔드포인트에서 텔넷 명령을 실행할 수 있습니다. 게이트웨이와 동일한 서브넷에 있는 서버에서 이러한 명령을 실행해야 합니다. 가용 영역을 지정하지 않은 DNS 이름에서 테스트를 실행할 수 있습니다. 예를 들어 다음 텔넷 명령은 DNS vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com이라는 이름을 사용하여 필요한 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
```

게이트웨이에서 Storage Gateway Amazon VPC 엔드포인트로 전송되는 패킷을 방화벽 보안이 수정하지 않도록 하십시오.

SSL검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안은 게이트웨이에서 전송되는 패킷을 방해할 수 있습니다. 활성화 엔드포인트가 예상한 것과 SSL 다르게 인증서를 수정하면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 Storage Gateway VPC 엔드포인트에서 Open SSL 명령을 실행합니다. 게이트웨이와 동일한 서브넷에 있는 시스템에서 이 명령을 실행해야 합니다. 필요한 각 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 비슷한 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
---
```

SSL검사가 진행 중인 경우 응답에는 다음과 같이 변경된 인증서 체인이 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 인증서를 인식하는 경우에만 SSL 핸드셰이크를 수락합니다. SSL 즉, 필수 포트를 통해 VPC 엔드포인트로 향하는 게이트웨이의 아웃바운드 트래픽은 네트워크 방화벽이 수행하는 검사에서 제외됩니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화를 확인하세요.

시간 차이가 너무 심하면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 차이는 60초를 넘지 않아야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하십시오.

Amazon EC2 인스턴스에 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이가 시간을 제대로 동기화할 수 있도록 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인하십시오.

- 0.amazon.pool.ntp.org
- 1.amazon.pool.ntp.org
- 2.amazon.pool.ntp.org
- 3.amazon.pool.ntp.org

HTTP프록시를 확인하고 관련 보안 그룹 설정을 확인합니다.

활성화하기 전에 Amazon HTTP 프록시가 온프레미스 게이트웨이 VM에 포트 3128의 Squid 프록시로 EC2 구성되어 있는지 확인하십시오. 이 경우 다음을 확인하십시오.

- Amazon의 HTTP 프록시에 연결된 보안 그룹에는 인바운드 규칙이 EC2 있어야 합니다. 이 인바운드 규칙은 게이트웨이 VM의 IP 주소에서 포트 3128을 통한 Squid 프록시 트래픽을 허용해야 합니다.
- Amazon EC2 VPC 엔드포인트에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이러한 인바운드 규칙은 아마존에 있는 프록시의 IP 주소에서 들어오는 포트 1026-1028, 1031, 2222 및 443에서의 트래픽을 허용해야 합니다. HTTP EC2

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하고 동일한 엔드포인트에 Storage Gateway VPC 엔드포인트가 있는 경우 발생하는 오류를 해결합니다. VPC

Amazon Virtual Private Cloud (AmazonVPC) 엔드포인트가 있는 경우 퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류를 해결하려면 다음 검사 및 구성을 수행하십시오. VPC

Storage Gateway VPC 엔드포인트에서 프라이빗 DNS 이름 활성화 설정이 활성화되어 있지 않은지 확인합니다.

프라이빗 DNS 이름 활성화가 활성화된 경우 해당 게이트웨이에서 퍼블릭 엔드포인트로 연결되는 게이트웨이를 VPC 활성화할 수 없습니다.

프라이빗 DNS 네임 옵션을 비활성화하려면:

1. Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Storage Gateway VPC 엔드포인트를 선택합니다.
4. 작업을 선택합니다.
5. 개인 DNS 이름 관리를 선택합니다.

6. 프라이빗 DNS 이름 활성화에서 이 엔드포인트에 대한 활성화를 선택 해제하십시오.
7. 개인 DNS 이름 수정을 선택하여 설정을 저장합니다.

온프레미스 게이트웨이 문제 해결

온프레미스 게이트웨이를 사용할 때 발생할 수 있는 일반적인 문제와 게이트웨이 문제 해결에 도움이 되도록 AWS Support 활성화하는 방법에 대한 정보는 다음과 같습니다.

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. • 의 VMware ESXi 경우 VM의 IP 주소는 vSphere 클라이언트의 요약 탭에서 찾을 수 있습니다. • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. 그래도 게이트웨이 IP 주소를 찾기 어려운 경우: • 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. • SSL인증서 검증/검사를 활성화해서는 안 됩니다. Storage Gateway는 상호 TLS 인증을 사용하므로 타사 애플리케이션이 인증서 중 하나를 가로채거나 서명하려고 하면 실패합니다. • 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 단원을 참조하십시오.

문제	취할 조치
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. 그렇지 않으면 프록시를 구성해야 합니다. SOCKS 이에 대한 자세한 내용은 프록시를 통한 온프레미스 게이트웨이 라우팅 섹션을 참조하세요. • 호스트의 시간이 정확한지, 호스트가 네트워크 시간 프로토콜 (NTP) 서버와 시간을 자동으로 동기화하도록 구성되어 있는지, 게이트웨이 VM의 시간이 올바른지 확인하십시오. 하이퍼바이저 호스트의 시간 동기화에 대한 자세한 내용은 을 참조하십시오. VMs 게이트웨이 VM 시간 동기화 • 이 단계를 수행한 후 Storage Gateway 콘솔과 게이트웨이 설정 및 활성화 마법사를 사용하여 게이트웨이 배포를 다시 시도할 수 있습니다. • SSL인증서 검증/검사를 활성화해서는 안 됩니다. Storage Gateway는 상호 TLS 인증을 사용하므로 타사 애플리케이션이 인증서 중 하나를 가로채거나 서명하려고 하면 실패합니다. • VM의 용량이 7.5GB 이상인지 확인하십시오. RAM 게이트웨이 할당이 7.5GB 미만이면 게이트웨이 할당이 RAM 실패합니다. 자세한 내용은 볼륨 게이트웨이 설정 요구 사항 단원을 참조하십시오.
업로드 버퍼 공간으로 할당된 디스크를 제거해야 합니다. 예를 들어 게이트웨이의 업로드 버퍼 공간을 줄이거나 업로드 버퍼로 사용하는 디스크에 장애가 있어 교체해야 할 경우가 있습니다.	업로드 버퍼 공간으로 할당된 디스크를 제거하는 작업에 대한 지침은 게이트웨이에서 디스크 제거 섹션을 참조하세요.

문제	취할 조치
게이트웨이와 AWS간 대역폭을 개선해야 합니다.	애플리케이션과 게이트웨이 VM을 연결하는 어댑터와는 별도로 네트워크 어댑터 (NIC) 에서 인터넷 연결을 AWS 설정하여 게이트웨이에서의 대역폭을 향상시킬 수 있습니다. AWS 이 접근 방식은 연결 대역폭이 높고 특히 스냅샷 복원 중에 대역폭 경합을 방지하려는 경우에 유용합니다. AWS 고처리량 워크로드 요구 사항을 충족하기 위해 AWS Direct Connect를 사용하여 온프레미스 게이트웨이와 AWS간에 전용 네트워크 연결을 설정할 수 있습니다. 게이트웨이에서 연결되는 대역폭을 AWS측정하려면 게이트웨이의 `CloudBytesDownloaded` 및 `CloudBytesUploaded` 지표를 사용하십시오. 이에 관한 자세한 내용은 게이트웨이와 AWS간 성능 측정 단원을 참조하십시오. 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 (즉, 클라이언트 또는 Microsoft Hyper-V Manager) 에 VMware vSphere 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.
	  • 의 VMware ESXi 경우 VM의 IP 주소는 vSphere 클라이언트의 요약 탭에서 찾을 수 있습니다.
	  • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다.
	• 에 설명된 AWS 대로 게이트웨이의 연결 상태를 확인하십시오게이트웨이가 인터넷에 연결되어 있는지 테스트.
	• 게이트웨이의 네트워크 어댑터 구성을 확인하고 게이트웨이에 대해 활성화하려는 모든 인터페이스가 활성화되었는지 확인합니다. 게이트웨이의 네트워크 어댑터 구성을 보려면 게이트웨이 네트워크 구성 단원의 지침에 따라 게이트웨이의 네트워크 구성을 볼 수 있는 옵션을 선택합니다.
	
	Amazon CloudWatch 콘솔에서 게이트웨이로 들어오고 나가는 처리량을 볼 수 있습니다. 게이트웨이로 들어오고 나가는 처리량을 측정하는 방법에 대한 자세한 내용은 을 참조하십시오 게이트웨이와 AWS간 성능 측정. AWS

Microsoft Hyper-V에서 Storage Gateway를 가져오기(배포)하는 데 문제가 있습니다.	Microsoft Hyper-V에서 게이트웨이를 배포할 때 흔히 겪는 몇 가지 문제를 다루는 Microsoft Hyper-V 설정 관련 문제 해결 단원을 참조하십시오.
"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 AWS Support에 문의하세요.

온프레미스에서 호스팅되는 게이트웨이 문제를 해결하는 AWS Support 데 도움이 되도록 허용

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이 액세스를 활성화하는 AWS Support 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이 AWS Support 액세스는 비활성화됩니다. 호스트의 로컬 콘솔을 통해 이 액세스 권한을 제공해야 합니다. 게이트웨이에 AWS Support 대한 액세스 권한을 부여하려면 먼저 호스트의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 지원 서버에 연결해야 합니다.

게이트웨이 AWS Support액세스를 허용하려면

1. 호스트의 로컬 콘솔에 로그인합니다.

   - VMwareESXi— 자세한 내용은 을 참조하십시오를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi.
   - 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 수행합니다.

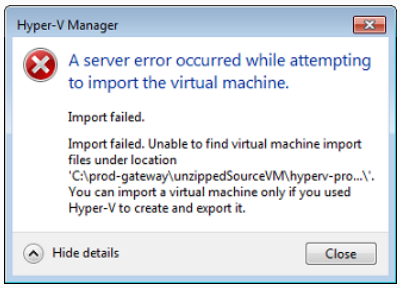
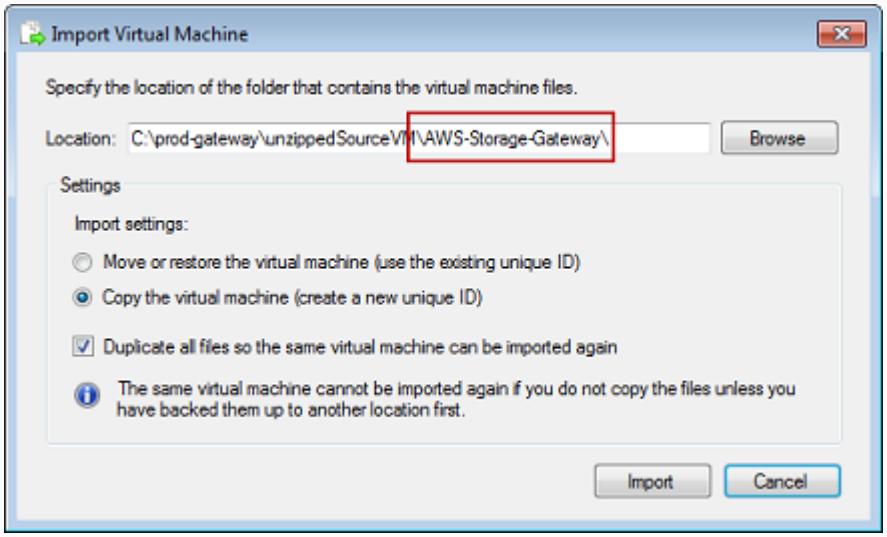
   - 게이트웨이가 퍼블릭 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에서 를 입력하여 **`open-support-channel`** Storage Gateway에 대한 고객 지원에 연결하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
   - 게이트웨이가 VPC 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에 를 입력합니다**`open-support-channel`**. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

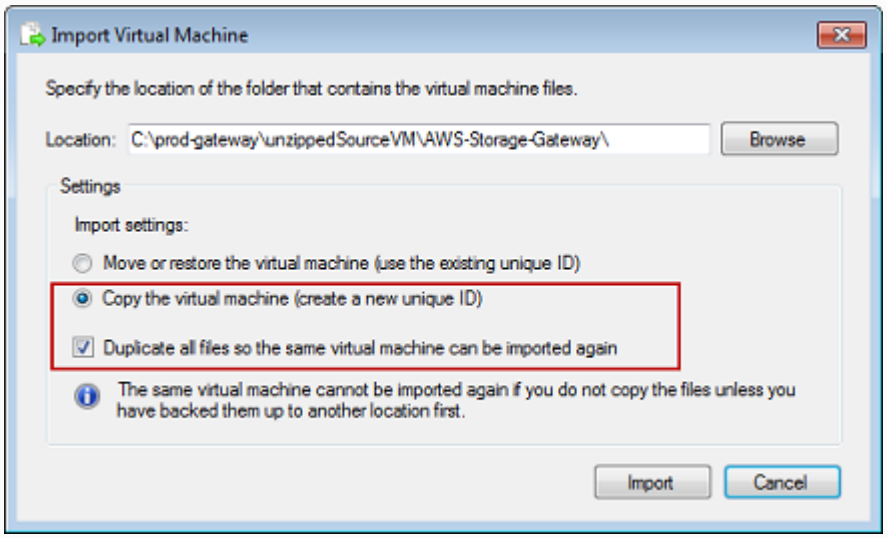
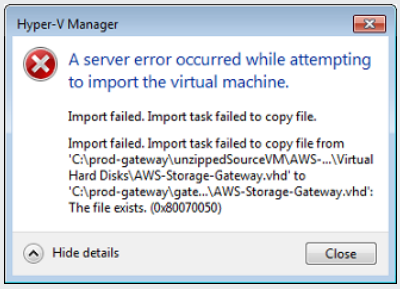
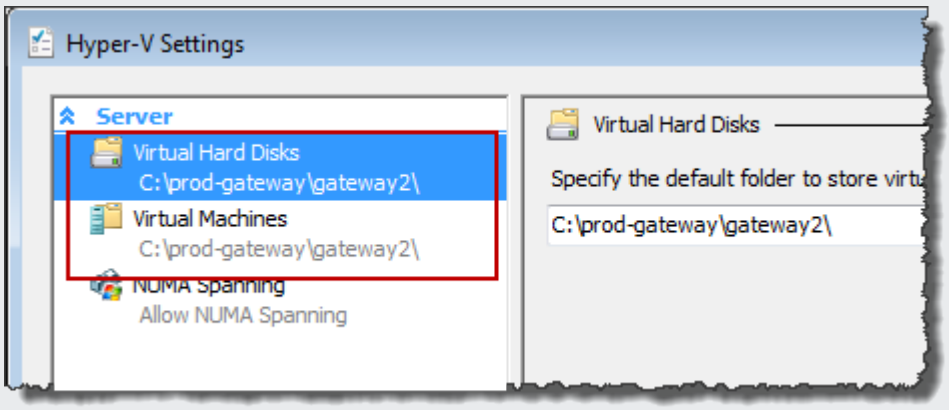
> **Note**
>
> 채널 번호는 전송 제어 프로토콜/사용자 데이터그램 프로토콜 (TCP/UDP) 포트 번호가 아닙니다. 대신 게이트웨이는 Secure Shell (SSH) (TCP22) 을 Storage Gateway 서버에 연결하고 연결을 위한 지원 채널을 제공합니다.

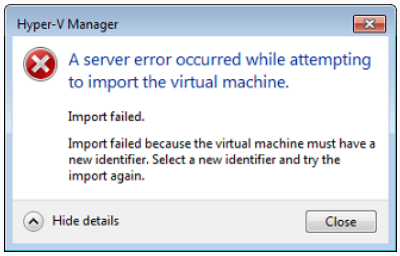
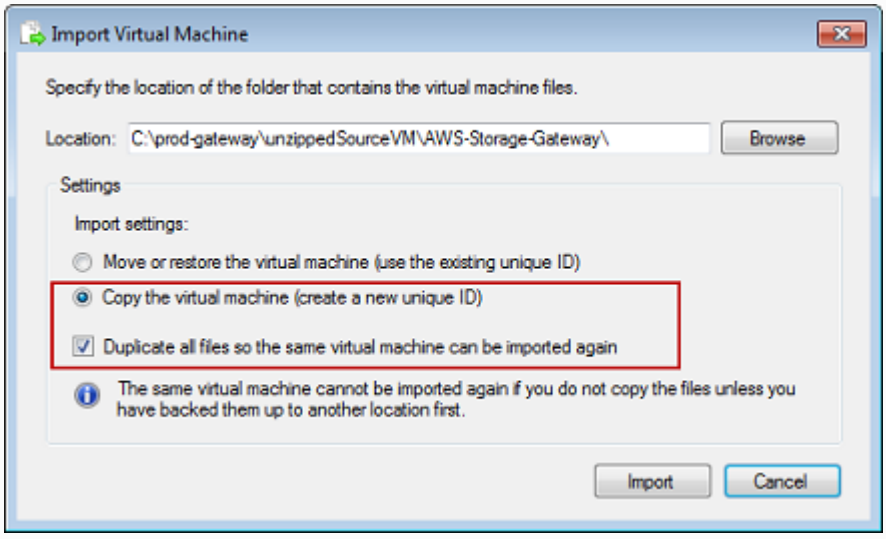
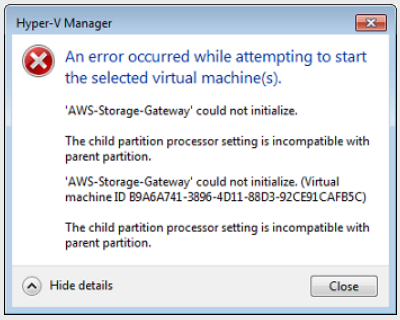
5. 지원 채널이 설정되면 문제 해결에 도움을 줄 AWS Support 수 AWS Support 있도록 지원 서비스 번호를 제공하십시오.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. Amazon Web Services Support에서 지원 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **exit**를 입력하여 게이트웨이 콘솔에서 로그아웃합니다.
8. 프롬프트 메시지에 따라 로컬 콘솔을 종료합니다.

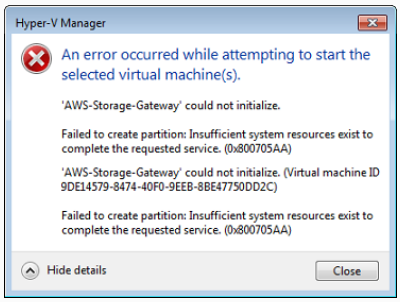
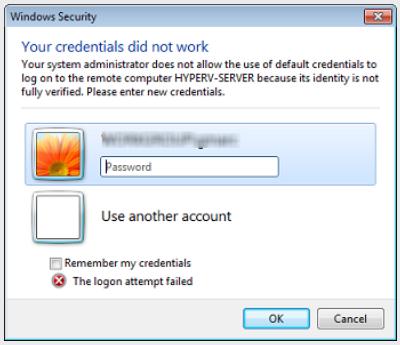
Microsoft Hyper-V 설정 관련 문제 해결

다음 표는 Microsoft Hyper-V 플랫폼에 Storage Gateway를 배포할 때 발생할 수 있는 일반적인 문제를 나열한 것입니다.

문제	취할 조치
게이트웨이 가져오기를 시도하면 "Import failed. Unable to find virtual machine import file under location ..."라는 오류 메시지가 표시됩니다. 	이 오류는 다음과 같은 이유로 발생할 수 있습니다. • 압축하지 않은 게이트웨이 소스 파일의 루트를 가리키지 않는 경우. Import Virtual Machine(가상 머신 가져오기) 대화 상자에서 지정하는 위치의 마지막 부분은 다음 예시와 같이 `AWS-Storage-Gateway` 이어야 합니다.  • 이미 게이트웨이를 배포했는데 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하지 않은 경우, 압축 해제된 게이트웨이 파일이 있는 위치에 VM이 생성되므로 이 위치에서 다시 가져올 수 없습니다. 이 문제를 해결하려면 압축을

문제	취할 조치
	해제한 게이트웨이 소스 파일의 새 사본을 얻어 이를 새 위치에 복사하면 됩니다. 새 위치를 가져오는 위치로 사용합니다. 다음 예시는 압축 해제한 소스 파일 위치에서 게이트웨이를 여러 개 생성할 계획인 경우, 확인해야 할 옵션입니다. 
게이트웨이 가져오기를 시도하면 "Import failed. Import task failed to copy file."라는 오류 메시지가 표시됩니다. 	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 Settings(Hyper-V 설정) 대화 상자에서 새 위치를 지정해야 합니다. 

문제	취할 조치
게이트웨이 가져오기를 시도하면 "Import failed. 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 때는 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하여 VM의 새 고유 ID를 생성해야 합니다. 다음 예시는 Import Virtual Machine(가상 머신 가져오기) 대화 상자에서 사용해야 할 옵션입니다. 
게이트웨이 VM을 시작하려 하면 "The child partition processor setting is incompatible with parent partition."이라는 오류 메시지가 표시됩니다. 	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 볼륨 게이트웨이 설정 요구 사항 섹션을 참조하세요.

문제	취할 조치
게이트웨이 VM을 시작하려 하면 "Failed to create partition: Insufficient resources exist to complete the requested service."라는 오류 메시지가 표시됩니다. 	이 오류는 게이트웨이에 필요한 RAM과 호스트에서 사용 가능한 RAM 사이의 RAM 불일치로 인해 발생할 수 있습니다. Storage Gateway 요구 사항에 대한 자세한 내용은 볼륨 게이트웨이 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 설명은 게이트웨이 VM 시간 동기화 섹션을 참조하세요.
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.

문제	취할 조치
Broadcom 네트워크 어댑터를 사용하는 Hyper-V 호스트에서 가상 머신 대기열(VMQ)을 활성화하면 네트워크 성능이 저하될 수 있습니다.	해결 방법에 대한 자세한 내용은 Microsoft 설명서, VMQ가 활성화된 경우 Windows Server 2012 Hyper-V 호스트의 가상 머신에서 네트워크 성능이 저하됨을 참조하세요.

Amazon EC2 게이트웨이 문제 해결

다음 섹션에서는 Amazon에 배포된 게이트웨이와 관련하여 발생할 수 있는 일반적인 문제를 확인할 수 EC2 있습니다. 온프레미스 게이트웨이와 EC2 Amazon에 배포된 게이트웨이의 차이에 대한 자세한 내용은 을 참조하십시오볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포.

주제

- 몇 분 후 게이트웨이가 활성화되지 않음
- 인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.
- Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없습니다.
- 게이트웨이의 볼륨 대상에는 이니시에이터를 연결할 수 없습니다. EC2
- 스토리지 볼륨을 추가하려고 할 때 사용 가능한 디스크가 없다는 메시지가 표시되는 경우
- 업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우
- 게이트웨이로 들어오거나 EC2 게이트웨이에서 나가는 처리량이 0으로 떨어집니다.
- 게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2
- Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려고 합니다.

몇 분 후 게이트웨이가 활성화되지 않음

Amazon EC2 콘솔에서 다음을 확인하십시오.

- 인스턴스와 연결한 보안 그룹에서 포트 80이 활성화되어 있는지 여부. 보안 그룹 규칙 추가에 대한 자세한 내용은 Amazon EC2 User Guide의 보안 그룹 규칙 추가를 참조하십시오.
- 게이트웨이 인스턴스는 실행 중으로 표시됩니다. Amazon EC2 콘솔에서 인스턴스의 상태 값은 다음과 같아야 RUNNING 합니다.

- Amazon EC2 인스턴스 유형이 에 설명된 최소 요구 사항을 충족하는지 확인하십시오스토리지 요구 사항.

문제를 해결한 후 게이트웨이를 다시 활성화합니다. 이렇게 하려면 Storage Gateway 콘솔을 열고 EC2Amazon에 새 게이트웨이 배포를 선택한 다음 인스턴스의 IP 주소를 다시 입력합니다.

인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.

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 머신 이미지 (AMI) 의 이름을 확인합니다. Storage Gateway 기반 인스턴스는 텍스트로 AMI 시작해야 **`aws-storage-gateway-ami`** 합니다.
- Storage AMI Gateway를 기반으로 하는 인스턴스가 여러 개 있는 경우 인스턴스 시작 시간을 확인하여 올바른 인스턴스를 찾으십시오.

Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없습니다.

해당 Amazon EBS 볼륨이 게이트웨이 인스턴스와 동일한 가용 영역에 있는지 확인합니다. 가용 영역에 불일치가 있는 경우 인스턴스와 동일한 가용 영역에 새 Amazon EBS 볼륨을 생성하십시오.

게이트웨이의 볼륨 대상에는 이니시에이터를 연결할 수 없습니다. EC2

인스턴스를 시작한 보안 그룹에 i SCSI 액세스에 사용 중인 포트를 허용하는 규칙이 포함되어 있는지 확인하십시오. 포트는 대개 3260으로 설정되어 있습니다. 볼륨 연결에 대한 자세한 내용은 볼륨을 Windows 클라이언트에 연결 단원을 참조하십시오.

스토리지 볼륨을 추가하려고 할 때 사용 가능한 디스크가 없다는 메시지가 표시되는 경우

새로 활성화된 게이트웨이에 볼륨 스토리지가 정의되지 않았습니다. 볼륨 스토리지를 정의하려면 먼저 게이트웨이에 업로드 버퍼 및 캐시 스토리지로 사용할 로컬 디스크를 할당해야 합니다. Amazon에 배포된 게이트웨이의 EC2 경우 로컬 디스크는 인스턴스에 연결된 Amazon EBS 볼륨입니다. 이 오류 메시지는 인스턴스에 대해 정의된 Amazon EBS 볼륨이 없기 때문에 발생할 수 있습니다.

게이트웨이를 실행하는 인스턴스에 정의된 블록 디바이스를 확인합니다. 블록 디바이스 (와 함께 제공되는 기본 디바이스AMI) 가 두 개뿐인 경우 스토리지를 추가해야 합니다. 이에 대한 자세한 내용은 볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포 섹션을 참조하세요. 두 개 이상의 Amazon EBS 볼륨을 연결한 후 게이트웨이에 볼륨 스토리지를 생성해 보십시오.

업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우

할당할 업로드 버퍼의 크기 결정 단원의 단계를 따르세요.

게이트웨이로 들어오거나 EC2 게이트웨이에서 나가는 처리량이 0으로 떨어집니다.

게이트웨이 인스턴스가 실행 중인지 확인합니다. 예를 들어 해당 인스턴스가 재부팅되고 있는 중이라면 인스턴스가 다시 시작할 때까지 기다립니다.

또한 게이트웨이 IP가 변경되지 않았는지 확인합니다. 인스턴스를 중단했다가 다시 시작한 경우, 인스턴스의 IP 주소가 변경되었을 수 있습니다. 이 경우 새 게이트웨이를 활성화해야 합니다.

Amazon CloudWatch 콘솔에서 게이트웨이로 들어오고 나가는 처리량을 볼 수 있습니다. 게이트웨이로 들어오고 나가는 처리량을 측정하는 방법에 대한 자세한 내용은 을 참조하십시오 게이트웨이와 AWS간 성능 측정. AWS

게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이 액세스를 활성화하는 AWS Support 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이 AWS Support 액세스는 비활성화됩니다. Amazon EC2 로컬 콘솔을 통해 이 액세스 권한을 제공합니다. 보안 셸 (SSH) 을 통해 Amazon EC2 로컬 콘솔에 로그인합니다. 성공적으로 로그인하려면 인스턴스의 보안 그룹에 TCP 포트 22를 여는 규칙이 있어야 합니다. SSH

> **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 설명서의 Amazon EC2 보안 그룹을 참조하십시오.

게이트웨이에 AWS Support 연결하려면 먼저 Amazon EC2 인스턴스의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 액세스 권한을 제공해야 합니다.

Amazon EC2 인스턴스에 배포된 게이트웨이에 대한 AWS Support 액세스를 활성화하려면

1. Amazon EC2 인스턴스의 로컬 콘솔에 로그인합니다. 지침을 보려면 Amazon 사용 EC2 설명서의 인스턴스에 Connect를 참조하십시오.

   다음 명령을 사용하여 EC2 인스턴스의 로컬 콘솔에 로그인할 수 있습니다.

   ```
   ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
   ```

   > **Note**
   >
   > The *PRIVATE-KEY* Amazon EC2 인스턴스를 시작하는 데 사용한 EC2 키 페어의 사설 인증서가 들어 있는 `.pem` 파일입니다. 자세한 내용은 Amazon EC2 사용 설명서의 키 쌍에 대한 퍼블릭 키 검색을 참조하십시오.
   > The *INSTANCE-PUBLIC-DNS-NAME* 게이트웨이가 실행되는 Amazon EC2 인스턴스의 퍼블릭 도메인 이름 시스템 (DNS) 이름입니다. EC2콘솔에서 Amazon EC2 인스턴스를 선택하고 Description 탭을 클릭하면 이 퍼블릭 DNS 이름을 얻을 수 있습니다.

2. 프롬프트에 **`6 - Command Prompt`**를 입력하여 AWS Support 채널 콘솔을 엽니다.
3. **`h`**를 입력하여 AVAILABLECOMMANDS창을 엽니다.
4. 다음 중 하나를 수행합니다.

   - 게이트웨이가 퍼블릭 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에서 를 입력하여 **`open-support-channel`** Storage Gateway에 대한 고객 지원에 연결하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
   - 게이트웨이가 VPC 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에 를 입력합니다**`open-support-channel`**. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

> **Note**
>
> 채널 번호는 전송 제어 프로토콜/사용자 데이터그램 프로토콜 (TCP/UDP) 포트 번호가 아닙니다. 대신 게이트웨이는 Secure Shell (SSH) (TCP22) 을 Storage Gateway 서버에 연결하고 연결을 위한 지원 채널을 제공합니다.

5. 지원 채널이 설정되면 문제 해결에 도움을 줄 AWS Support 수 AWS Support 있도록 지원 서비스 번호를 제공하십시오.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. 지원 세션이 AWS Support 완료되었다는 알림이 올 때까지 세션을 닫지 마십시오.
7. **exit**를 입력하여 Storage Gateway 콘솔을 종료합니다.
8. 콘솔 메뉴에 따라 Storage Gateway 인스턴스에서 로그아웃합니다.

Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려고 합니다.

Amazon EC2 직렬 콘솔을 사용하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. 지침과 문제 해결 팁은 Amazon Elastic Compute 클라우드 사용 설명서의 Amazon EC2 시리얼 콘솔을 참조하십시오.

하드웨어 어플라이언스 문제 해결

다음 주제에서는 Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제와 이러한 문제를 해결하기 위한 제안 사항에 대해 설명합니다.

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 Storage Gateway 하드웨어 어플라이언스 팀에 지원을 요청하세요.

원격 재시작은 어떻게 수행하나요?

어플라이언스를 원격으로 재시작해야 하는 경우 Dell i DRAC 관리 인터페이스를 사용하여 재시작할 수 있습니다. 자세한 내용은 Dell Technologies InfoHub 웹 사이트의 i DRAC9 가상 전원 주기: Dell EMC PowerEdge 서버의 전원 공급을 원격으로 껐다가 다시 켜기를 참조하십시오.

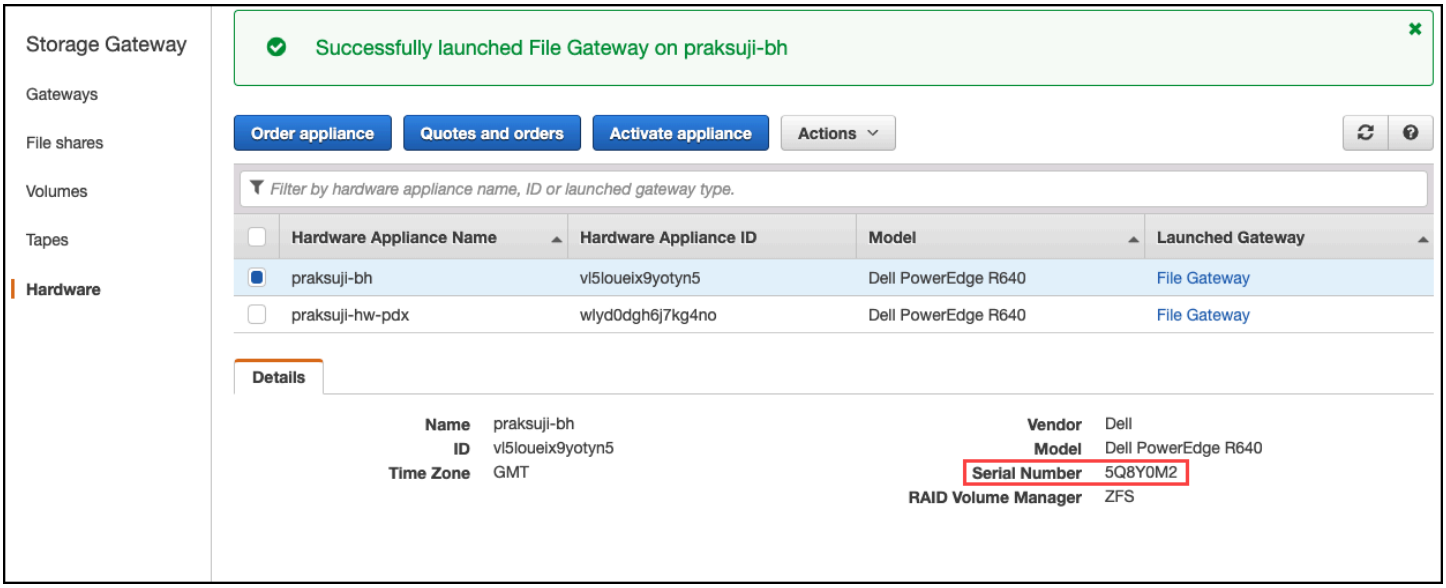
Dell i DRAC 지원은 어디서 받을 수 있습니까?

Dell PowerEdge R640 서버는 Dell i DRAC 관리 인터페이스와 함께 제공됩니다. 다음과 같이 하는 것이 좋습니다:

- i DRAC 관리 인터페이스를 사용하는 경우 기본 암호를 변경해야 합니다. i DRAC 자격 증명에 대한 자세한 내용은 Dell PowerEdge - i의 기본 로그인 자격 증명은 무엇입니까? 를 참조하십시오. DRAC .
- 펌웨어가 보안 침해를 up-to-date 방지하기 위한 것인지 확인하십시오.
- i DRAC 네트워크 인터페이스를 normal (em) 포트로 이동하면 성능 문제가 발생하거나 어플라이언스가 정상적으로 작동하지 않을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾을 수 없음

하드웨어 어플라이언스의 일련 번호를 찾으려면 다음에 표시된 것과 같이 Storage Gateway 콘솔의 하드웨어 어플라이언스 개요 페이지로 이동합니다.
어플라이언스가 선택되고 세부 정보가 표시되어 있는 Storage Gateway 콘솔의 하드웨어 탭입니다.



어플라이언스가 선택되고 세부 정보가 표시되어 있는 Storage Gateway 콘솔의 하드웨어 탭입니다.

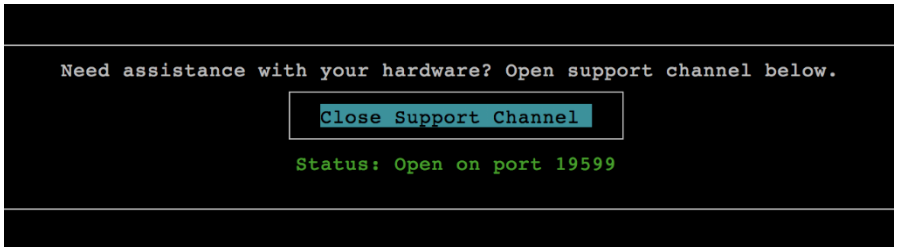
하드웨어 어플라이언스 지원은 어디에서 받을 수 있나요?

Storage Gateway 하드웨어 어플라이언스 지원팀에 문의하려면 AWS Support 섹션을 참조하세요.

AWS Support 팀에서 게이트웨이 문제를 원격으로 해결하기 위해 지원 채널을 활성화하도록 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.

지원 채널을 열려면 AWS

1. 하드웨어 콘솔을 엽니다.
2. 다음과 같이 Open Support Channel(지원 채널 열기)를 선택합니다.
   지원 채널 상태가 표시되어 있는 하드웨어 어플라이언스 콘솔입니다.



   지원 채널 상태가 표시되어 있는 하드웨어 어플라이언스 콘솔입니다.

   네트워크 연결 또는 방화벽 문제가 없는 경우 할당 된 포트 번호가 30초 이내에 표시됩니다.
3. 포트 번호를 적어두고 에 제공하십시오 AWS Support.

볼륨 문제 해결

볼륨 관련 작업 시 겪을 수 있는 가장 일반적인 문제와 이 문제를 해결하기 위해 취해야 할 조치에 대한 정보를 얻을 수 있습니다.

주제

볼륨을 구성하지 않았다고 콘솔이 표시하는 경우

볼륨이 UPLOAD BUFFER NOT CONFIGURED 상태에 있다고 Storage Gateway 콘솔에 표시되는 경우, 게이트웨이에 업로드 버퍼 용량을 추가합니다. 게이트웨이에 업로드 버퍼를 구성하지 않은 경우, 게이트웨이를 사용하여 애플리케이션 데이터를 저장할 수 없습니다. 자세한 설명은 게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면 섹션을 참조하세요.

볼륨을 복구할 수 없다고 콘솔이 표시하는 경우

저장 볼륨의 경우, 볼륨이 IRRECOVERABLE 상태에 있다고 Storage Gateway 콘솔에 표시되면 더 이상 이 볼륨을 사용할 수 없습니다. Storage Gateway 콘솔에서 볼륨 삭제를 시도할 수 있습니다. 볼륨에 데이터가 있는 경우, 볼륨을 생성하기 위해 처음 사용한 VM의 로컬 디스크를 기반으로 하여 새 볼륨을 생성할 때 해당 데이터를 복구할 수 있습니다. 새 볼륨을 생성할 때 Preserve existing data(기존 데이터

보존)를 선택합니다. 볼륨을 삭제하기 전에 볼륨에서 보류 중인 스냅샷을 삭제해야 합니다. 자세한 설명은 스냅샷 삭제 섹션을 참조하세요. Storage Gateway 콘솔에서 볼륨을 삭제하려고 하는데 잘 되지 않는 경우, 볼륨에 할당한 디스크가 VM에서 부적절하게 제거되어 어플라이언스에서 제거할 수 없기 때문일 수 있습니다.

캐시 볼륨의 경우, 볼륨이 IRRECOVERABLE 상태에 있다고 Storage Gateway 콘솔에 표시되면 더 이상 이 볼륨을 사용할 수 없습니다. 볼륨에 데이터가 있는 경우 볼륨의 스냅샷을 생성하고 스냅샷에서 데이터를 복구하거나 마지막 복구 시점에서 볼륨을 복제할 수 있습니다. 데이터를 복구한 후에는 볼륨을 삭제할 수 있습니다. 자세한 설명은 캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우 섹션을 참조하세요.

저장 볼륨의 경우, 복구할 수 없는 볼륨을 생성하는 데 사용한 디스크에서 새 볼륨을 생성할 수 있습니다. 자세한 설명은 볼륨 생성 섹션을 참조하세요. 볼륨 상태에 대한 내용은 볼륨 상태 및 전환 이해 단원을 참조하십시오.

캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우

게이트웨이를 종료한 경우와 같이 게이트웨이에 접속할 수 없을 때는 볼륨 복구 시점에서 스냅샷을 생성하여 그 스냅샷을 사용하거나 기존 볼륨의 마지막 복구 시점에서 새 볼륨을 복제하는 옵션이 있습니다. 볼륨 복구 시점에서 복제하는 것이 스냅샷을 생성하는 것보다 빠르고 비용 효과적입니다. 볼륨 복제에 대한 자세한 내용은 볼륨 복제 단원을 참조하십시오.

Storage Gateway는 캐시된 Volume Gateway 아키텍처의 각 볼륨마다 복구 지점을 제공합니다. 볼륨 복구 시점은 볼륨의 모든 데이터가 일관되고 스냅샷을 생성하거나 볼륨을 복제할 수 있는 시점입니다.

볼륨이 PASS THROUGH 상태라고 콘솔이 표시하는 경우

어떤 경우에는 볼륨이 PASSTHROUGH 상태에 있다고 Storage Gateway 콘솔에 표시될 수 있습니다. 한 볼륨은 여러 가지 이유로 PASSTHROUGH 상태가 될 수 있습니다. 조치가 필요한 이유가 있고 필요 없는 이유가 있습니다.

볼륨이 PASS THROUGH 상태일 때 조치를 취해야 하는 경우의 한 가지 예로 게이트웨이에 업로드 버퍼 공간이 모자란 경우를 들 수 있습니다. 과거에 업로드 버퍼가 초과되었는지 확인하려면 Amazon CloudWatch 콘솔에서 `UploadBufferPercentUsed` 지표를 볼 수 있습니다. 자세한 내용은 을 참조하십시오업로드 버퍼 모니터링. 업로드 버퍼 공간이 부족하여 게이트웨이가 PASS THROUGH 상태인 경우 게이트웨이에 더 많은 업로드 버퍼 공간을 할당해야 합니다. 버퍼 공간을 더 추가하면 볼륨이 PASS THROUGH에서 BOOTSTRAPPING을 거쳐 AVAILBAILLE로 자동 전환됩니다. 볼륨이 BOOTSTRAPPING 상태인 동안에 게이트웨이는 볼륨의 디스크에서 데이터를 읽고 이 데이터를 Amazon S3에 업로드하며 필요에 따라 갱신합니다. 게이트웨이가 갱신되어 볼륨 데이터를 Amazon

S3에 저장하면 볼륨 상태가 AVAILABLE로 변경되고 스냅샷을 다시 시작할 수 있습니다. 볼륨이 PASS THROUGH 또는 BOOTSTRAPPING 상태인 경우, 볼륨 디스크에서 데이터를 계속 읽고 쓸 수 있다는 점에 유의하십시오. 업로드 버퍼 공간 추가에 대한 자세한 내용은 할당할 업로드 버퍼의 크기 결정 단원을 참조하십시오.

업로드 버퍼를 초과하기 전에 조치를 취하려면 게이트웨이의 업로드 버퍼에 임계값 경보를 설정합니다. 자세한 설명은 게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면 섹션을 참조하세요.

이와 대조적으로 볼륨이 PASS THROUGH 상태인데도 조치를 취할 필요가 없는 경우의 한 가지 예로 현재 다른 볼륨을 부트스트래핑 중이어서 해당 볼륨이 부트스트래핑을 기다리고 있는 경우를 들 수 있습니다. 게이트웨이는 볼륨을 한 번에 하나씩 부트스트래핑합니다.

드물게 PASS THROUGH 상태가 업로드 버퍼에 할당한 디스크에 장애가 있음을 나타내는 경우가 있습니다. 이 경우 해당 디스크를 제거해야 합니다. 자세한 설명은 볼륨 게이트웨이 섹션을 참조하세요. 볼륨 상태에 대한 내용은 볼륨 상태 및 전환 이해 단원을 참조하십시오.

볼륨 무결성을 확인하고 가능한 오류를 수정하고자 하는 경우

볼륨 무결성을 확인하고 가능한 오류를 수정하고자 하는 경우, 그리고 게이트웨이에서 Microsoft Windows 초기자를 사용하여 볼륨에 연결하는 경우, Windows CHKDSK 유틸리티를 사용하여 볼륨의 무결성을 확인하고 볼륨에 있는 모든 오류를 수정할 수 있습니다. 볼륨 손상을 감지하면 Windows는 자동으로 CHKDSK 도구를 실행합니다. 아니면 수동으로 실행할 수도 있습니다.

Windows 디스크 관리 콘솔이 볼륨의 iSCSI 대상을 표시하지 않는 경우

Windows에서 디스크 관리 콘솔이 볼륨의 iSCSI 대상을 표시하지 않는 경우에는 게이트웨이에 업로드 버퍼를 구성했는지 확인합니다. 자세한 설명은 게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면 섹션을 참조하세요.

볼륨의 iSCSI 대상 이름을 변경하고자 하는 경우

볼륨의 iSCSI 대상 이름을 변경하고자 하는 경우에는 해당 볼륨을 삭제한 후 새 대상 이름으로 다시 추가해야 합니다. 이렇게 하면 볼륨의 데이터를 보존할 수 있습니다.

예약 볼륨 스냅샷이 생기지 않은 경우

예약 볼륨 스냅샷이 생기지 않은 경우에는 볼륨이 PASSTHROUGH 상태인지, 아니면 게이트웨이의 업로드 버퍼가 예약된 스냅샷 시간 바로 전에 가득 찼는지 여부를 확인합니다. Amazon CloudWatch 콘솔에서 게이트웨이의 `UploadBufferPercentUsed` 지표를 확인하고 이 지표에 대한 경보를 생성할

수 있습니다. 자세한 내용은 업로드 버퍼 모니터링 및 게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면 섹션을 참조하세요.

장애를 일으킨 디스크를 제거하거나 교체해야 하는 경우

장애를 일으킨 볼륨 디스크를 교체하거나, 혹은 필요 없는 볼륨을 제거해야 하는 경우에는 먼저 Storage Gateway 콘솔을 사용하여 해당 볼륨을 제거해야 합니다. 자세한 설명은 볼륨을 삭제하려면 섹션을 참조하세요. 그 다음에는 다음과 같이 하이퍼바이저 클라이언트를 사용하여 지원 스토리지를 제거합니다.

- VMware ESXi의 경우, 볼륨 삭제 단원의 지침에 따라 지원 스토리지를 제거합니다.
- Microsoft Hyper-V의 경우, 지원 스토리지를 제거합니다.

애플리케이션에서 볼륨까지 처리량이 0으로 떨어진 경우

애플리케이션에서 볼륨까지 처리량이 0으로 떨어진 경우에는 다음과 같이 합니다.

- VMware vSphere 클라이언트를 사용하는 경우, 볼륨의 호스트 IP 주소가 요약 탭의 vSphere 클라이언트에 표시되는 주소 중 하나와 일치하는지 확인합니다. 스토리지 볼륨의 호스트 IP 주소는 Storage Gateway 콘솔의 볼륨 세부 정보 탭에서 찾을 수 있습니다. 예를 들어 게이트웨이에 새로운 고정 IP 주소를 할당하면 IP 주소 불일치가 발생할 수 있습니다. 불일치하는 경우, 게이트웨이 VM 종료에 표시된 대로 Storage Gateway 콘솔에서 게이트웨이를 다시 시작합니다. 다시 시작한 후에는 스토리지 볼륨의 iSCSI 대상 정보 탭에 있는 호스트 IP 주소가 게이트웨이의 요약 탭에 있는 vSphere 클라이언트에 표시된 IP 주소와 일치해야 합니다.
- 볼륨에 대한 호스트 IP 상자에 IP 주소가 없고 게이트웨이가 온라인인 경우. 예를 들어 네트워크 어댑터가 두 개 이상인 게이트웨이에 있는 네트워크 어댑터 한 개의 IP 주소와 연결된 볼륨을 생성할 경우 이 오류가 발생할 수 있습니다. 볼륨이 연결된 네트워크 어댑터를 제거하거나 비활성화하면 호스트 IP 상자에 IP 주소가 표시되지 않을 수 있습니다. 이 문제를 해결하려면 볼륨을 삭제한 후 다시 생성하여 기존 데이터를 보존합니다.
- 애플리케이션에서 사용하는 iSCSI 초기자가 스토리지 볼륨의 iSCSI 대상에 올바르게 매핑되어 있는지 확인합니다. 스토리지 볼륨 연결에 대한 자세한 내용은 볼륨을 Windows 클라이언트에 연결 단원을 참조하십시오.

Amazon CloudWatch 콘솔에서 볼륨 처리량을 확인하고 경보를 생성할 수 있습니다. 애플리케이션에서 볼륨까지 처리량 측정에 대한 자세한 내용은 애플리케이션과 게이트웨이 간 성능 측정 단원을 참조하십시오.

게이트웨이의 캐시 디스크에 장애가 발생한 경우

게이트웨이에 있는 하나 이상의 캐시 디스크에 오류가 발생하는 경우, 게이트웨이가 가상 테이프 및 볼륨에 읽기 및 쓰기 작업이 수행되지 않도록 막습니다. 정상 기능을 재개하려면 다음과 같이 게이트웨이를 다시 구성하십시오.

- 캐시 디스크를 액세스할 수 없거나 사용할 수 없으면, 게이트웨이 구성에서 디스크를 삭제합니다.
- 캐시 디스크를 액세스할 수 없거나 사용할 수 없으면, 게이트웨이에 이를 다시 연결합니다.

> **Note**
>
> 캐시 디스크를 삭제하면 게이트웨이가 정상 기능을 재개할 때 클린 데이터(즉, 캐시 디스크 및 Amazon S3에 있는 데이터가 동기화된 데이터)가 있는 테이프 또는 볼륨을 계속해서 사용할 수 있습니다. 예를 들어, 게이트웨이에 3개의 캐시 디스크가 있는데 이 중 2개를 삭제하면, 클린 상태인 테이프나 볼륨의 상태가 AVAILABLE이 됩니다. 다른 테이프나 볼륨의 상태는 IRRECOVERABLE이 됩니다.
>
> 임시 디스크를 게이트웨이의 캐시 디스크로 사용하거나 임시 디스크에 캐시 디스크를 탑재하는 경우, 게이트웨이를 닫으면 캐시 디스크를 잃게 됩니다. 캐시 디스크 및 Amazon S3가 동기화되지 않은 상태에서 게이트웨이를 닫으면 데이터가 손실됩니다. 따라서, 임시 드라이브나 디스크를 사용하지 않는 것이 좋습니다.

볼륨 스냅샷이 예상보다 오래 PENDING 상태에 있는 경우

볼륨 스냅샷이 예상보다 오래 PENDING 상태에 있는 경우에는 게이트웨이 VM이 예기치 않게 충돌했거나 볼륨의 상태가 PASSTHROUGH 또는 IRRECOVERABLE로 변경되었기 때문일 수 있습니다. 이 중 어떤 경우에도 스냅샷은 PENDING 상태를 유지하고 성공적으로 완료되지 않습니다. 이러한 경우 스냅샷은 삭제하는 것이 좋습니다. 자세한 설명은 스냅샷 삭제 섹션을 참조하세요.

볼륨이 AVAILABLE 상태로 돌아가면 볼륨의 새 스냅샷을 생성합니다. 볼륨 상태에 대한 내용은 볼륨 상태 및 전환 이해 단원을 참조하십시오.

고가용성 상태 알림

VMware vSphere HA(고가용성) 플랫폼에서 게이트웨이를 실행할 때 상태 알림을 받을 수 있습니다. 상태 알림에 대한 자세한 내용은 고가용성 문제 해결 단원을 참조하십시오.

고가용성 문제 해결

가용성 문제가 발생할 경우 수행할 작업에 대한 다음 정보를 찾을 수 있습니다.

주제

상태 알림

VMware vSphere HA에서 게이트웨이를 실행하면 모든 게이트웨이가 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 참조하십시오.

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 경우 문의하십시오 AWS Support.

알림: AvailabilityMonitorTest

VMware vSphere HA의 게이트웨이의 경우 VMware에서 가용성 및 애플리케이션 모니터링 시스템 테스트를 실행할 때 AvailabilityMonitorTest 알림을 받을 수 있습니다.

지표

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.

데이터 복구 모범 사례

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 단원의 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.

주제

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 게이트웨이가 인터넷에 연결되어 있는지 테스트섹션을 참조하세요.
- 캐시 볼륨 설정의 경우 게이트웨이에 연결할 수 있게 되면 볼륨이 BOOTSTRAPPING 상태가 됩니다. 이 기능을 사용하면 로컬에 저장된 데이터를 계속 동기화할 수 있습니다. AWS이 상태에 대한 자세한 내용은 볼륨 상태 및 전환 이해 단원을 참조하십시오.
- 게이트웨이가 제대로 작동하지 않고 예기치 않은 종료로 인해 볼륨 또는 테이프에서 문제가 발생하는 경우, 데이터를 복구할 수 있습니다. 데이터를 복구하는 방법에 대한 자세한 내용은 다음 중 해당되는 상황과 관련된 단원을 참조하십시오.

장애가 있는 게이트웨이 또는 VM에서 데이터 복구

게이트웨이 또는 가상 머신이 오작동하는 경우 Amazon S3의 볼륨에 AWS 업로드되고 저장된 데이터를 복구할 수 있습니다. 캐싱 볼륨 게이트웨이의 경우, 복구 스냅샷에서 데이터를 복구합니다. 저장

볼륨 게이트웨이의 경우, 가장 최근의 Amazon EBS 스냅샷에서 데이터를 복구할 수 있습니다. Tape Gateway의 경우, 복구 지점에서 새 Tape Gateway로 하나 이상의 테이프를 복구합니다.

캐싱 볼륨 게이트웨이에 접속할 수 없는 경우, 다음 절차에 따라 복구 스냅샷에서 데이터를 복구할 수 있습니다.

1. 에서 오작동하는 게이트웨이를 선택하고 복구할 볼륨을 선택한 다음 해당 게이트웨이에서 복구 스냅샷을 생성합니다. AWS Management Console
2. 새로운 Volume Gateway를 배포하고 활성화합니다. 또는 제대로 작동하는 기존 Volume Gateway가 있는 경우, 해당 게이트웨이를 사용하여 볼륨 데이터를 복구할 수 있습니다.
3. 생성한 스냅샷을 찾아 제대로 작동하는 게이트웨이의 새 볼륨으로 복원합니다.
4. 새 볼륨을 iSCSI 장치로 온프레미스 애플리케이션 서버에 마운트합니다.

복구 스냅샷에서 캐싱 볼륨 데이터를 복구하는 방법에 관한 자세한 내용은 캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우 단원을 참조하십시오.

복구할 수 없는 볼륨에서 데이터 복구

볼륨이 IRRECOVERABLE 상태인 경우, 이 볼륨을 더는 사용할 수 없습니다.

저장 볼륨의 경우, 다음 절차에 따라 복구할 수 없는 볼륨에서 새 볼륨으로 데이터를 가져올 수 있습니다.

1. 복구할 수 없는 볼륨을 생성하는 데 사용한 디스크에서 새 볼륨을 생성합니다.
2. 새 볼륨을 생성할 때 기존 데이터를 보존합니다.
3. 복구할 수 없는 볼륨에서 보류 중인 스냅샷 작업을 모두 삭제합니다.
4. 게이트웨이에서 복구할 수 없는 볼륨을 삭제합니다.

캐싱 볼륨의 경우 마지막 복구 시점을 사용하여 새 볼륨을 복제하는 것이 좋습니다.

복구할 수 없는 볼륨에서 새 볼륨으로 데이터를 가져오는 방법에 대한 자세한 내용은 볼륨을 복구할 수 없다고 콘솔이 표시하는 경우 단원을 참조하십시오.

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.
- 캐시 디스크가 손상되거나 캐시 디스크에 액세스할 수 없는 경우, 게이트웨이를 종료하고 캐시 디스크를 재설정하고 캐시 스토리지용 디스크를 재구성한 후 게이트웨이를 다시 시작합니다.

손상된 파일 시스템에서 데이터 복구

파일 시스템이 손상된 경우에는 **fsck** 명령을 사용하여 파일 시스템의 오류를 점검하고 수정할 수 있습니다. 파일 시스템의 오류를 수정할 수 있다면 다음 설명과 같이 파일 시스템에 있는 볼륨에서 데이터를 복구할 수 있습니다.

1. 가상 머신을 종료하고 Storage Gateway Management Console을 사용하여 복구 스냅샷을 생성합니다. 이 스냅샷은 저장된 가장 최신 데이터를 나타냅니다. AWS

   > **Note**
   >
   > 파일 시스템의 오류를 수정할 수 없거나 스냅샷 생성 프로세스를 성공적으로 완료할 수 없는 경우, 이 스냅샷을 대체 방법으로 사용합니다.

   복구 스냅샷을 생성하는 방법에 대한 자세한 내용은 캐싱된 게이트웨이에 액세스할 수 없어서 데이터 복구를 원하는 경우 단원을 참조하십시오.
2. **fsck** 명령을 사용하여 파일 시스템의 오류를 점검하고 수정을 시도할 수 있습니다.
3. 게이트웨이 VM을 다시 시작합니다.
4. 하이퍼바이저 호스트가 부팅을 시작하면 Shift 키를 길게 눌러 GRUB 부트 메뉴로 들어갑니다.
5. 메뉴에서 **e**를 눌러 편집합니다.
6. 커널 라인(두 번째 줄)을 선택한 후 **e**를 눌러 편집합니다.
7. **init=/bin/bash**라는 옵션을 커널 명령줄에 추가합니다. 스페이스를 사용하여 이전 옵션과 방금 추가한 옵션을 분리합니다.
8. `console=` 행을 모두 삭제합니다. 이때 쉼표로 구분된 값을 포함하여 = 기호 뒤에 오는 모든 값을 삭제해야 합니다.
9. **Return**을 눌러 변경 사항을 저장합니다.
10. **b**를 눌러 수정된 커널 옵션으로 컴퓨터를 부팅합니다. 컴퓨터는 bash# 프롬프트로 부팅됩니다.

11. 파일 시스템을 점검하고 오류를 수정하기 위해 프롬프트에서 **/sbin/fsck -f *dev/sda1***을 입력하여 이 명령을 수동으로 실행합니다. 명령이 /dev/sda1 경로에서 작동하지 않는 경우 **lsblk**를 사용하여 /에 대한 루트 파일시스템 디바이스를 확인한 다음 해당 경로를 대신 사용할 수 있습니다.
12. 파일 시스템 점검 및 오류 수정을 마친 후 인스턴스를 다시 부팅합니다. GRUB 설정은 원래 값으로 돌아가고 게이트웨이는 정상적으로 부팅됩니다.
13. 원래 게이트웨이에서 진행 중인 스냅샷이 완료되기를 기다린 후 스냅샷 데이터의 유효성을 검증합니다.

계속해서 원래 볼륨을 있는 그대로 사용하거나 복구 스냅샷 또는 완료된 스냅샷을 바탕으로 새 볼륨이 있는 새 게이트웨이를 생성할 수 있습니다. 또는 이 볼륨에서 완료된 스냅샷 중 어떤 것으로부터도 새 볼륨을 생성할 수 있습니다.

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 Volume Gateway에서 데이터를 복구하려면

1. Amazon EC2 호스트에서 새 Volume Gateway를 생성하여 활성화합니다. 자세한 설명은 볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포 섹션을 참조하세요.

   > **Note**
   >
   > 게이트웨이 저장 볼륨은 Amazon EC2 인스턴스에서 호스팅할 수 없습니다.

2. 새 볼륨을 생성하고 EC2 게이트웨이를 대상 게이트웨이로 선택합니다. 자세한 설명은 볼륨 생성 섹션을 참조하세요.

   Amazon EBS 스냅샷을 기반으로 새 볼륨을 생성하거나 복구할 볼륨의 마지막 복구 시점에서 복제합니다.

   볼륨이 스냅샷을 기반으로 하는 경우 스냅샷 ID를 입력합니다.

   복구 시점에서 볼륨을 복제하는 경우 소스 볼륨을 선택합니다.

추가 Storage Gateway 리소스

이 섹션에서는 게이트웨이와 Storage Gateway 할당량을 설정하거나 관리하는 데 도움이 되는 타사 소프트웨어, 툴 및 리소스에 대해 설명합니다 AWS .

주제

게이트웨이 VM 호스트 배포 및 구성

주제

Storage Gateway 구성 VMware

Storage Gateway를 구성할 VMware 때는 VM 시간을 호스트 시간과 동기화하고, 스토리지를 프로비저닝할 때 반가상화된 디스크 컨트롤러를 사용하도록 VM을 구성하고, 게이트웨이 VM을 지원하는 인프라 계층의 장애로부터 보호해야 합니다.

주제

VM 시간을 호스트 시간과 동기화

게이트웨이를 성공적으로 활성화하려면 VM 시간을 호스트 시간과 동기화해야 하고 호스트 시간을 올바르게 설정해야 합니다. 이 단원에서는 먼저 VM의 시간을 호스트 시간과 동기화합니다. 그런 다음 호스트 시간을 확인하고 필요한 경우 호스트 시간을 설정하고 시간이 네트워크 시간 프로토콜 () 서버와 자동으로 동기화되도록 호스트를 구성합니다. NTP

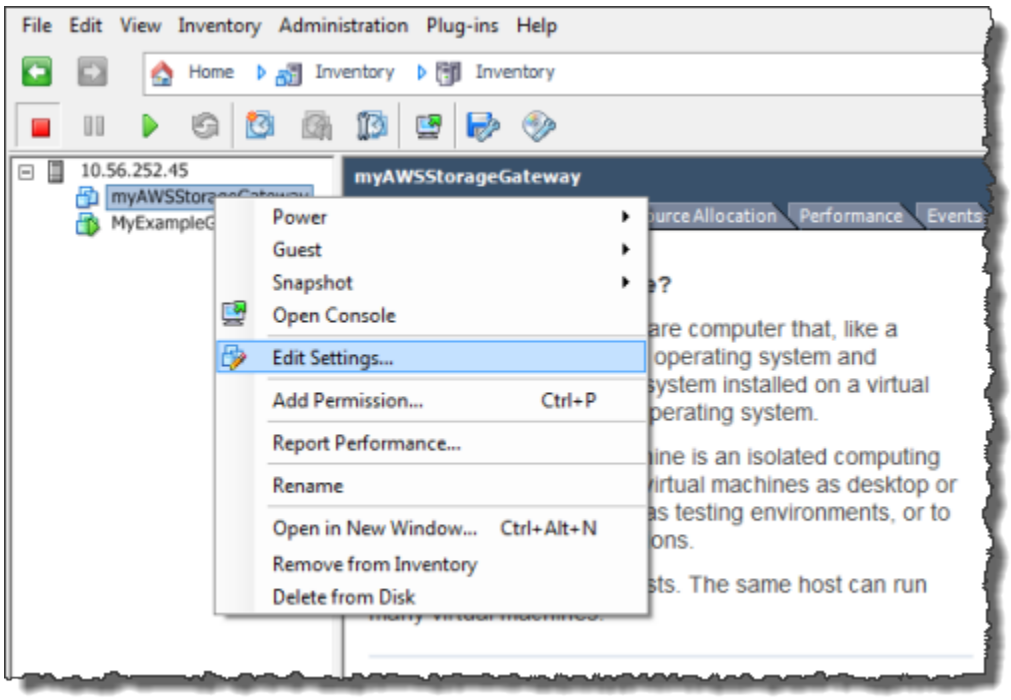
> **Important**
>
> VM 시간을 호스트 시간과 동기화하려면 게이트웨이를 성공적으로 활성화해야 합니다.

VM 시간을 호스트 시간과 동기화하려면

1. VM 시간을 구성합니다.

   a. vSphere 클라이언트에서 게이트웨이 VM의 컨텍스트 메뉴 (마우스 오른쪽 버튼 클릭) 를 열고 설정 편집을 선택합니다.

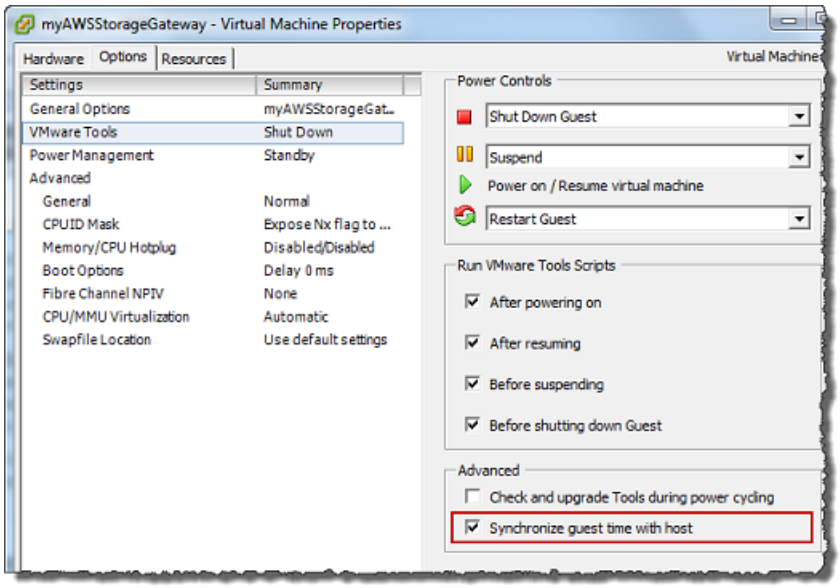
      그러면 Virtual Machine Properties(가상 머신 속성) 대화 상자가 열립니다.



b. 옵션 탭을 선택하고 옵션 목록에서 VMware툴을 선택합니다.

c. Synchronize guest time with host(호스트와 게스트 시간 동기화) 옵션을 선택한 후 확인을 선택합니다.

그러면 VM이 자체 시간을 호스트와 동기화합니다.



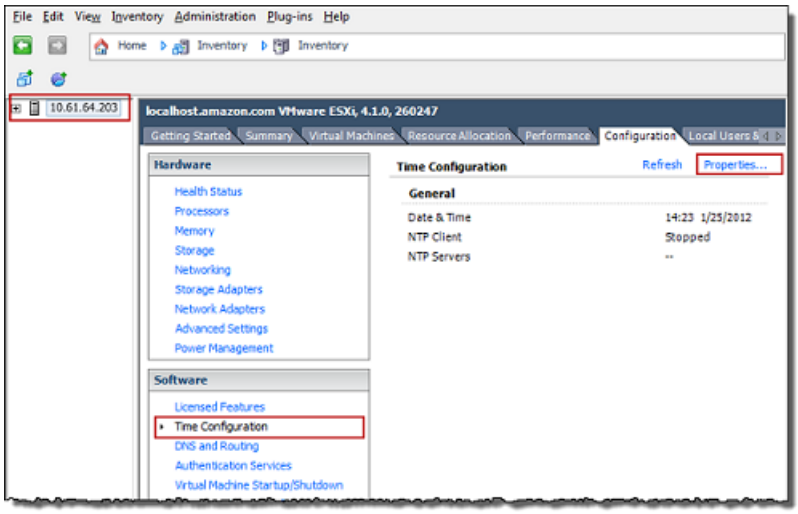
2. 호스트 시간을 구성합니다.

호스트 클럭의 시간이 올바르게 설정되어 있는지 확인하는 것이 중요합니다. 호스트 시계를 구성하지 않은 경우 다음 단계를 수행하여 호스트 시계를 설정하고 NTP 서버와 동기화하십시오.

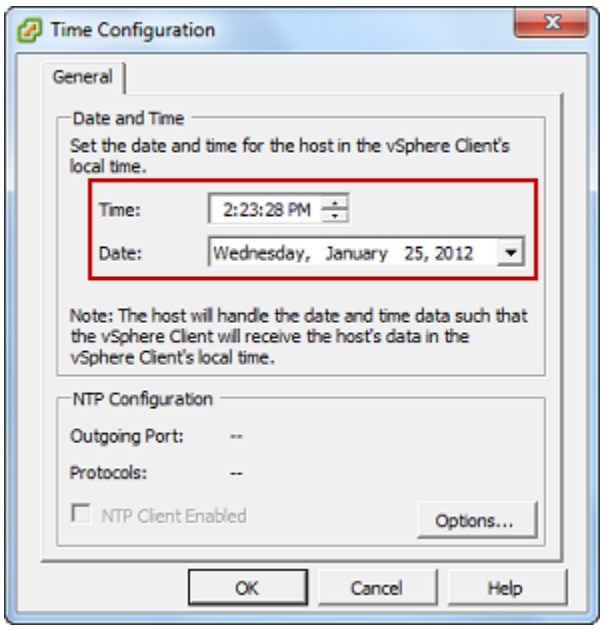
a. VMware vSphere 클라이언트의 왼쪽 창에서 vSphere 호스트 노드를 선택한 다음 구성 탭을 선택합니다.

b. 소프트웨어 패널에서 시간 구성을 선택한 다음 속성 링크를 선택합니다.

그러면 Time Configuration(시간 구성) 대화 상자가 나타납니다.

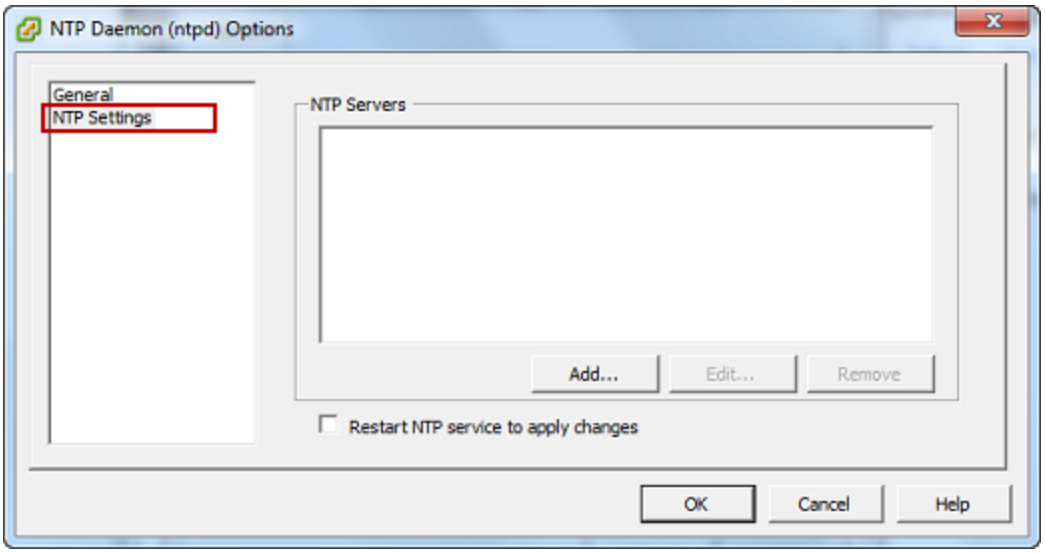


c. 날짜 및 시간 창에서 날짜 및 시간을 설정합니다.



d. 시간을 NTP 서버와 자동으로 동기화하도록 호스트를 구성합니다.

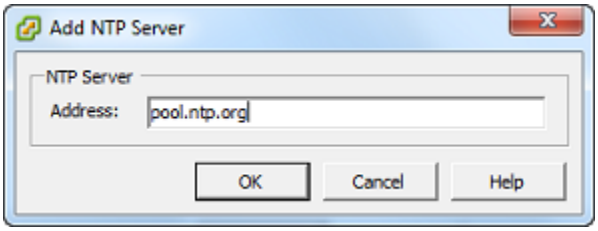
i. 시간 구성 대화 상자에서 옵션을 선택한 다음 NTP데몬 (ntpd) 옵션 대화 상자의 왼쪽 창에서 NTP설정을 선택합니다.



ii. 추가를 선택하여 새 서버를 추가합니다. NTP

iii. [NTP서버 추가] 대화 상자에서 서버의 IP 주소 또는 정규화된 도메인 이름을 입력한 다음 [확인] 을 선택합니다. NTP

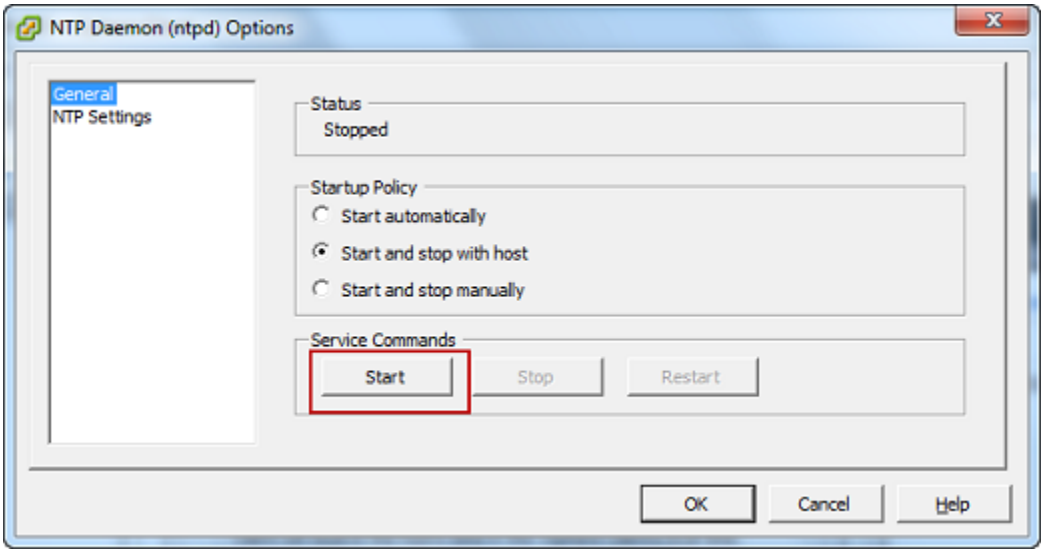
다음 예시와 같이 `pool.ntp.org`를 사용할 수 있습니다.



iv. NTP데몬 (ntpd) 옵션 대화 상자의 왼쪽 창에서 일반을 선택합니다.

v. Service Commands(서비스 명령) 창에서 Start(시작)를 선택하여 해당 서비스를 시작합니다.

참고로 이 NTP 서버 참조를 변경하거나 나중에 다른 서버 참조를 추가하는 경우 새 서버를 사용하려면 서비스를 다시 시작해야 합니다.



e. 확인을 선택하여 NTP데몬 (ntpd) 옵션 대화 상자를 닫습니다.

f. 확인을 선택하여 Time Configuration(시간 구성) 대화 상자를 닫습니다.

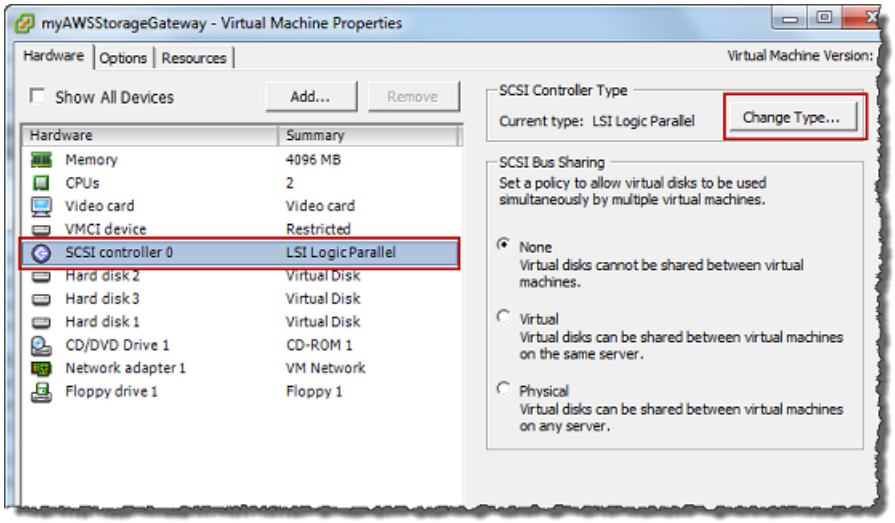
반가상화된 디스크 컨트롤러를 사용하도록 AWS Storage Gateway VM 구성

이 작업에서는 VM이 반가상화를 사용하도록 i SCSI 컨트롤러를 설정합니다. 반가상화는 VM에 추가하는 가상 디스크를 콘솔이 식별할 수 있도록 게이트웨이 VM이 호스트 운영 체제와 협력하는 모드입니다.

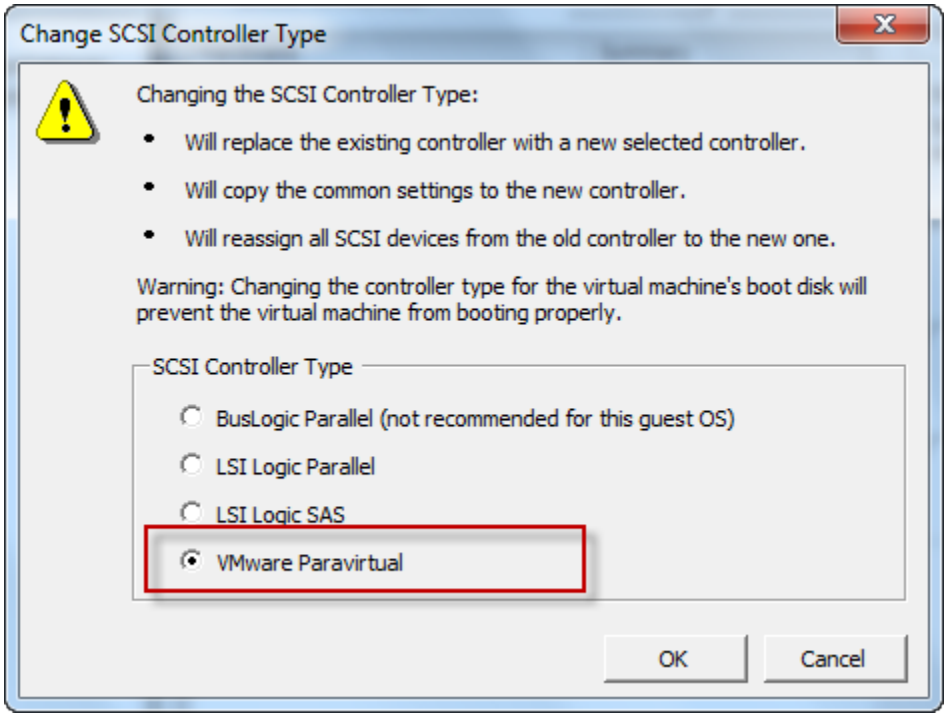
> **Note**
>
> 게이트웨이 콘솔에서 이 디스크를 구성할 때 디스크를 식별하는 과정에서 발생할 수 있는 문제를 방지하려면 이 단계를 완료해야 합니다.

VM을 구성하여 반가상화된 컨트롤러를 사용하려면

1. VMware vSphere 클라이언트에서 게이트웨이 VM의 컨텍스트 메뉴 (마우스 오른쪽 버튼 클릭) 를 연 다음 설정 편집을 선택합니다.
2. 가상 시스템 속성 대화 상자에서 하드웨어 탭을 선택하고 SCSI컨트롤러 0을 선택한 다음 유형 변경을 선택합니다.



3. SCSI컨트롤러 유형 변경 대화 상자에서 VMware반가상화 SCSI 컨트롤러 유형을 선택한 다음 확인을 선택합니다.



VMware고가용성을 갖춘 Storage Gateway 사용

VMware고가용성 (HA) 은 게이트웨이 VM을 지원하는 인프라 계층의 vSphere 장애로부터 보호할 수 있는 구성 요소입니다. VMwareHA는 클러스터로 구성된 여러 호스트를 사용하여 이를 수행하므로 게이트웨이 VM을 실행하는 호스트에 장애가 발생할 경우 클러스터 내의 다른 호스트에서 게이트웨

이 VM을 자동으로 다시 시작할 수 있습니다. VMwareHA에 대한 자세한 내용은 VMware 웹 사이트의 VMware vSphere 고가용성 클러스터 모범 사례를 참조하십시오.

Storage Gateway를 VMware HA와 함께 사용하려면 다음 작업을 수행하는 것이 좋습니다.

- Storage Gateway VM이 포함된 VMware ESX `.ova` 다운로드 가능한 패키지를 클러스터의 한 호스트에만 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.
- 페일오버 중에 이니시에이터와 스토리지 볼륨 타겟의 연결이 끊기지 않도록 하려면 운영 체제의 권장 i SCSI 설정을 따르십시오. 장애 조치 이벤트 중에는 게이트웨이 VM이 장애 조치 클러스터의 새 호스트에서 시작하는 데 몇 초에서 몇 분이 걸릴 수 있습니다. Windows 및 Linux 클라이언트 모두에 권장되는 i SCSI 제한 시간은 페일오버가 발생하는 데 걸리는 일반적인 시간보다 깁니다. Windows 클라이언트의 제한 시간 설정을 사용자 정의하는 방법에 대한 자세한 내용은 Windows i SCSI 설정 사용자 지정하기 단원을 참조하십시오. Linux 클라이언트의 제한 시간 설정을 사용자 정의하는 방법에 대한 자세한 내용은 Linux i 설정 사용자 지정하기 SCSI 단원을 참조하십시오.
- 클러스터링의 경우, `.ova` 패키지를 클러스터에 배포한다면 프롬프트 메시지에 따라 호스트를 선택합니다. 또는 클러스터의 호스트에 직접 배포할 수도 있습니다.

게이트웨이 VM 시간 동기화

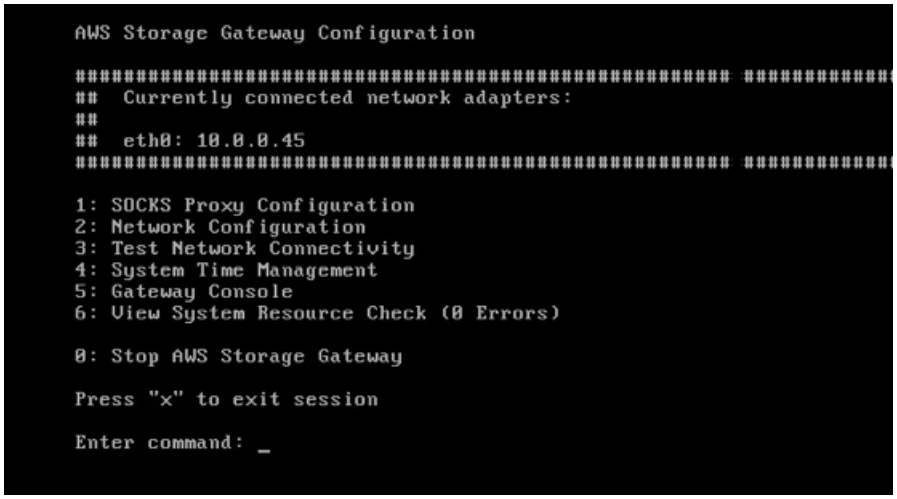
게이트웨이가 배포된 경우 하이퍼바이저 호스트 시간을 설정하고 VM 시간을 호스트와 동기화하는 것만으로도 시간 변동을 피할 수 있습니다. VMware ESXi 자세한 내용은 VM 시간을 호스트 시간과 동기화 단원을 참조하십시오. Microsoft Hyper-V에 배포한 게이트웨이의 경우, 다음 절차에 따라 VM의 시간을 주기적으로 점검해야 합니다.

하이퍼바이저 게이트웨이 VM의 시간을 보고 네트워크 시간 프로토콜 () 서버와 동기화하는 방법 NTP

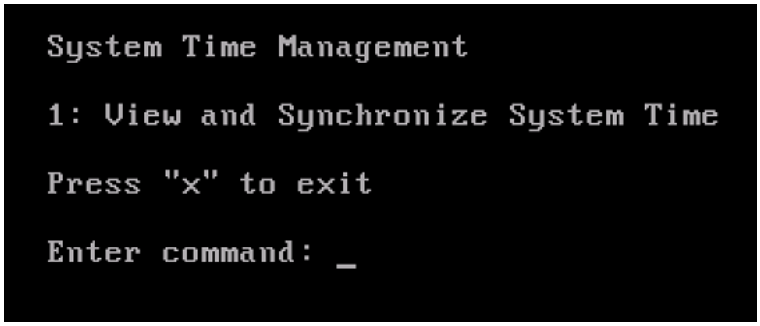
1. 게이트웨이의 로컬 콘솔에 로그인합니다.
   - VMwareESXi로컬 콘솔 로그인에 대한 자세한 내용은 을 참조하십시오. 를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하십시오.

- Linux 커널 기반 Virtuam Machine (KVM) 의 로컬 콘솔에 로그인하는 방법에 대한 자세한 내용은 을 참조하십시오. Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM

2. Storage Gateway 구성 기본 메뉴에서 시스템 시간 관리에 **4**을 입력합니다.



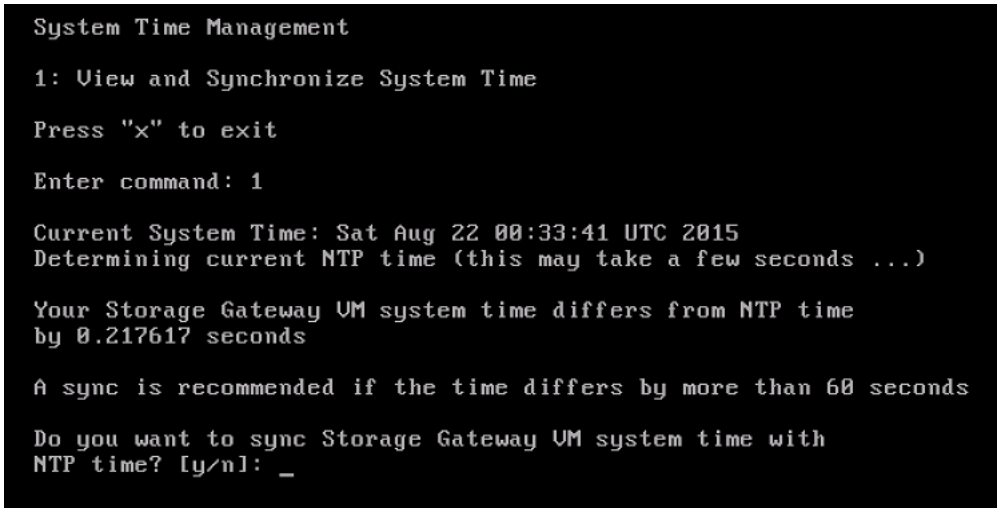
3. 시스템 시간 관리 메뉴에서 시스템 시간 보기 및 동기화에 **1**을 입력합니다.



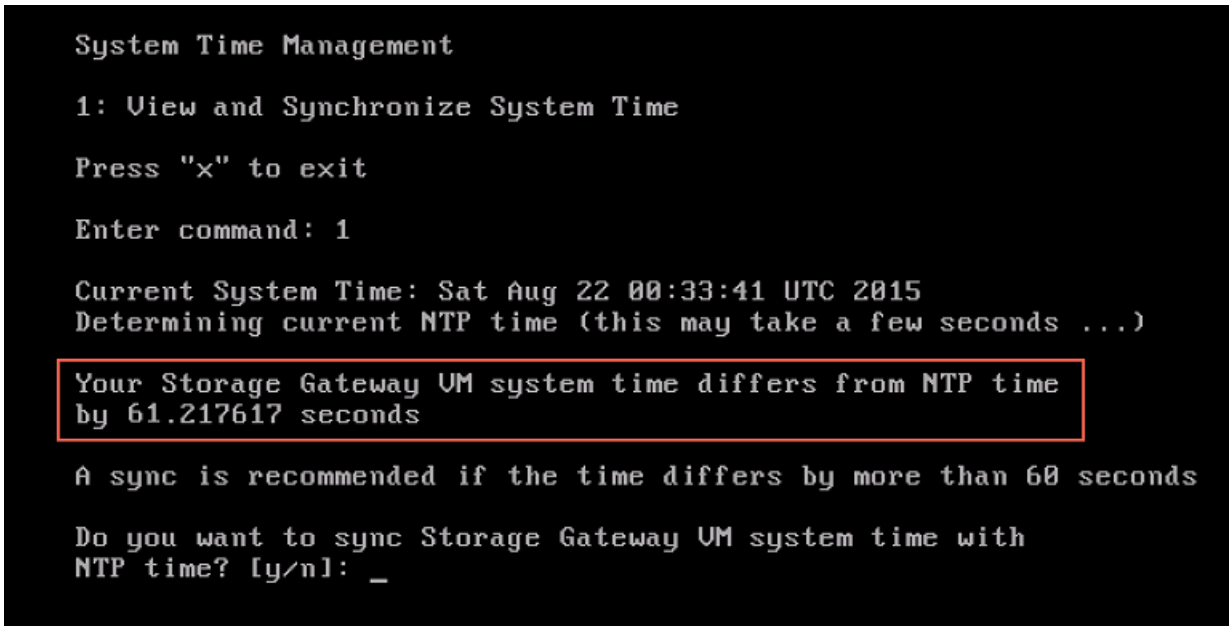
4. VM의 시간을 해당 시간과 동기화해야 한다는 결과가 나오면 를 입력하십시오. NTP **y** 그렇지 않은 경우 **n**을 입력합니다.

   동기화를 위해 **y**를 입력하면 동기화에 약간의 시간이 걸릴 수 있습니다.

   다음 스크린샷은 시간 동기화가 필요 없는 VM을 나타낸 것입니다.



다음 스크린샷은 시간 동기화가 필요한 VM을 나타낸 것입니다.



볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포

Amazon Elastic Compute Cloud (AmazonEC2) 인스턴스에 볼륨 게이트웨이를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon 머신 이미지 (AMI) 는 커뮤니티로 제공됩니다AMI.

> **Note**
>
> Storage Gateway AMIs 커뮤니티는 에서 게시하고 전적으로 지원합니다 AWS. 게시자가 검증된 공급자임을 알 수 있습니다. AWS

다음과 같은 명명 규칙을 AMIs 사용합니다. 이름에 추가된 버전 번호는 각 버전 AMI 릴리스마다 변경됩니다.

```
aws-storage-gateway-CLASSIC-2.9.0
```

Amazon EC2 인스턴스를 배포하여 볼륨 게이트웨이를 호스팅하려면

1. Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Volume Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에서 Amazon을 호스트 EC2 플랫폼으로 선택하고 다음 단계를 사용하여 호스팅할 Amazon EC2 인스턴스를 시작합니다.

   > **Note**
   >
   > Amazon EC2 호스트 플랫폼은 캐시된 볼륨만 지원합니다. 저장된 볼륨 게이트웨이는 인스턴스에 배포할 수 없습니다. EC2

2. Launch instance를 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 열고 추가 설정을 구성할 수 있습니다.

   QuickLaunch를 사용하여 기본 설정으로 Amazon EC2 인스턴스를 시작합니다. Amazon EC2 QuickLaunch 기본 사양에 대한 자세한 내용은 Amazon의 참조하십시오. EC2 EC2Amazon용 퀵 런치 구성 사양.

3. [Name] 에는 Amazon EC2 인스턴스의 이름을 입력합니다. 인스턴스를 배포한 후 Amazon EC2 콘솔의 목록 페이지에서 이 이름을 검색하여 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 설명서의 인스턴스 크기 조정을 참조하십시오.

   > **Note**
   >
   > 특정 인스턴스 유형, 특히 EC2 i3은 디스크를 사용합니다 NVMeSSD. 이러한 경우 Volume Gateway를 시작하거나 중지할 때 문제가 발생할 수 있습니다. 예를 들어, 캐시에서 데이터가 손실될 수 있습니다. `CachePercentDirty`Amazon CloudWatch 메트릭을 모니터링하고 해당 파라미터가 모니터링될 때만 시스템을 시작하거나 중지하십시오`0`. 게

이트웨이의 모니터링 지표에 대한 자세한 내용은 CloudWatch 설명서의 Storage Gateway 지표 및 차원을 참조하십시오.

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-의 경우 Amazon EC2 인스턴스를 시작할 VPC 위치를 선택합니다. 자세한 내용은 Amazon Virtual Private 클라우드 사용 설명서의 Amazon VPC 작동 방식을 참조하십시오.
   b. (선택 사항) Subnet의 경우 Amazon EC2 인스턴스를 시작하려는 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 인스턴스에 대해 생성할 새 보안 그룹의 기본 이름 및 설명을 변경하거나 기존 보안 그룹의 방화벽 규칙을 대신 적용하도록 선택할 수 있습니다.
8. 인바운드 보안 그룹 규칙 하위 섹션에서 클라이언트가 인스턴스에 연결하는 데 사용할 포트를 여는 방화벽 규칙을 추가합니다. Volume 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**
>
> 볼륨 게이트웨이를 사용하려면 게이트웨이 활성화 중에 인바운드 트래픽과 일회성 HTTP 액세스를 위해 TCP 포트 80이 열려 있어야 합니다. 활성화한 후에는 이 포트를 닫을 수 있습니다.
> 또한 i 액세스를 위해서는 TCP 포트 3260을 열어야 합니다. SCSI

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**
>
> 사전 구성된 루트 EBS 볼륨 외에도 캐시 스토리지용 용량이 165GiB 이상인 EBS Amazon 볼륨을 하나 이상 추가하고 업로드 버퍼용 용량이 150GiB 이상인 Amazon 볼륨을 하나 이

상 추가해야 합니다. 성능을 높이려면 각각 150GiB 이상의 캐시 스토리지에 여러 EBS 볼륨을 할당하는 것이 좋습니다.

11. 고급 세부 정보 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
12. Launch 인스턴스를 선택하여 구성된 설정으로 새 Amazon EC2 게이트웨이 인스턴스를 시작합니다.
13. 새 인스턴스가 성공적으로 시작되었는지 확인하려면 Amazon EC2 콘솔의 Instances 페이지로 이동하여 새 인스턴스를 이름으로 검색하십시오. 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 IPv4 주소를 복사한 다음 Storage Gateway 콘솔의 게이트웨이 설정 페이지로 돌아가서 설정을 재개합니다.

Storage Gateway 콘솔을 사용하거나 AWS Systems Manager 파라미터 저장소를 쿼리하여 볼륨 게이트웨이를 시작하는 데 사용할 AMI ID를 결정할 수 있습니다.

AMIID를 확인하려면 다음 중 하나를 수행하십시오.

- Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Volume Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에 도달하면 Amazon을 호스트 EC2 플랫폼으로 선택한 다음 Launch instance를 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 엽니다.

  EC2커뮤니티 AMI 페이지로 리디렉션되며, 여기에서 해당 AWS URL 지역의 AMI ID를 볼 수 있습니다.

- Systems Manager 파라미터 스토어를 쿼리합니다. AWS CLI 또는 Storage API Gateway를 사용하여 네임스페이스에서 캐시된 볼륨 게이트웨이 또는 저장 볼륨 게이트웨이에 `/aws/service/storagegateway/ami/CACHED/latest` 대한 Systems Manager 공용 매개 변수를 쿼리할 수 `/aws/service/storagegateway/ami/STORED/latest` 있습니다. 예를 들어, 다음 CLI 명령을 사용하면 지정한 현재 AMI 항목의 ID가 반환됩니다. AWS 리전

  ```
  aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/
  STORED/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/
STORED/latest",
        "Name": "/aws/service/storagegateway/ami/STORED/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

기본 설정을 사용하여 Amazon EC2 배포

이 주제에서는 기본 지정 사항으로 Amazon EC2 호스트를 배포하는 단계에 대해 설명합니다.

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Volume Gateway를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon Machine Image(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

> **Note**
>
> Storage Gateway 커뮤니티 AMI는 AWS에서 게시하고 완벽하게 지원합니다. 게시자가 검증된 제공자임을 알 수 있습니다. AWS

1. Amazon EC2 인스턴스를 설정하려면 워크플로의 플랫폼 옵션 섹션에서 Amazon EC2를 호스트 플랫폼으로 선택합니다. Amazon EC2 인스턴스 구성에 대한 지침은 Volume 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 IPv4 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 iSCSI 대상은 게이트웨이와 동일한 VPC에 있는 호스트에서만 액세스할 수 있습니다. VPC 외부의 호스트에서 iSCSI 대상에 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				
3260	TCP	iSCSI				

- 스토리지 구성

기본 설정	AMI 루트 볼륨	볼륨 2 캐시	볼륨 3 캐시			
디바이스 이름		'/dev/sdb'	'/dev/sdc'			
크기	80GiB	165GiB	150GiB			
볼륨 유형	gp3	gp3	gp3			
IOPS	3000	3000	3000			
종료 시 삭제	예	예	예			
Encrypted	아니요	아니요	아니요			
처리량	125	125	125			

Amazon EC2 인스턴스 메타데이터 옵션 수정

인스턴스 메타데이터 서비스 (IMDS) 는 Amazon 인스턴스 메타데이터에 대한 보안 액세스를 제공하는 온 EC2 인스턴스 구성 요소입니다. IMDS버전 1 (IMDSv1) 을 사용하는 수신 메타데이터 요청을 수락하거나 모든 메타데이터 요청에 IMDS 버전 2 (IMDSv2) 를 사용하도록 요구하는 인스턴스를 구성할 수 있습니다. IMDSv2세션 지향 요청을 사용하고 액세스를 시도하는 데 사용될 수 있는 여러 유형의 취약성을 완화합니다. IMDS 에 대한 IMDSv2 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 인스턴스 메타데이터 서비스 버전 2의 작동 방식을 참조하십시오.

Storage Gateway를 호스팅하는 모든 Amazon EC2 인스턴스에 IMDSv2 요구하는 것이 좋습니다. IMDSv2새로 시작된 모든 게이트웨이 인스턴스에는 기본적으로 필요합니다. IMDSv1메타데이터 요청을 수락하도록 구성된 기존 인스턴스가 있는 경우 Amazon Elastic Compute Cloud 사용 설명서의 사용 필요를 참조하여 사용을 요구하도록 인스턴스 메타데이터 옵션을 수정하는 지침을 참조하십시오 IMDSv2. IMDSv2 이 변경 사항을 적용할 때는 인스턴스를 재부팅할 필요가 없습니다.

볼륨 게이트웨이

주제

게이트웨이에서 디스크 제거

게이트웨이에서의 기본 디스크 제거는 권장되지 않지만, 예를 들어 장애가 발생한 디스크를 게이트웨이에서 제거하고 싶을 수 있습니다.

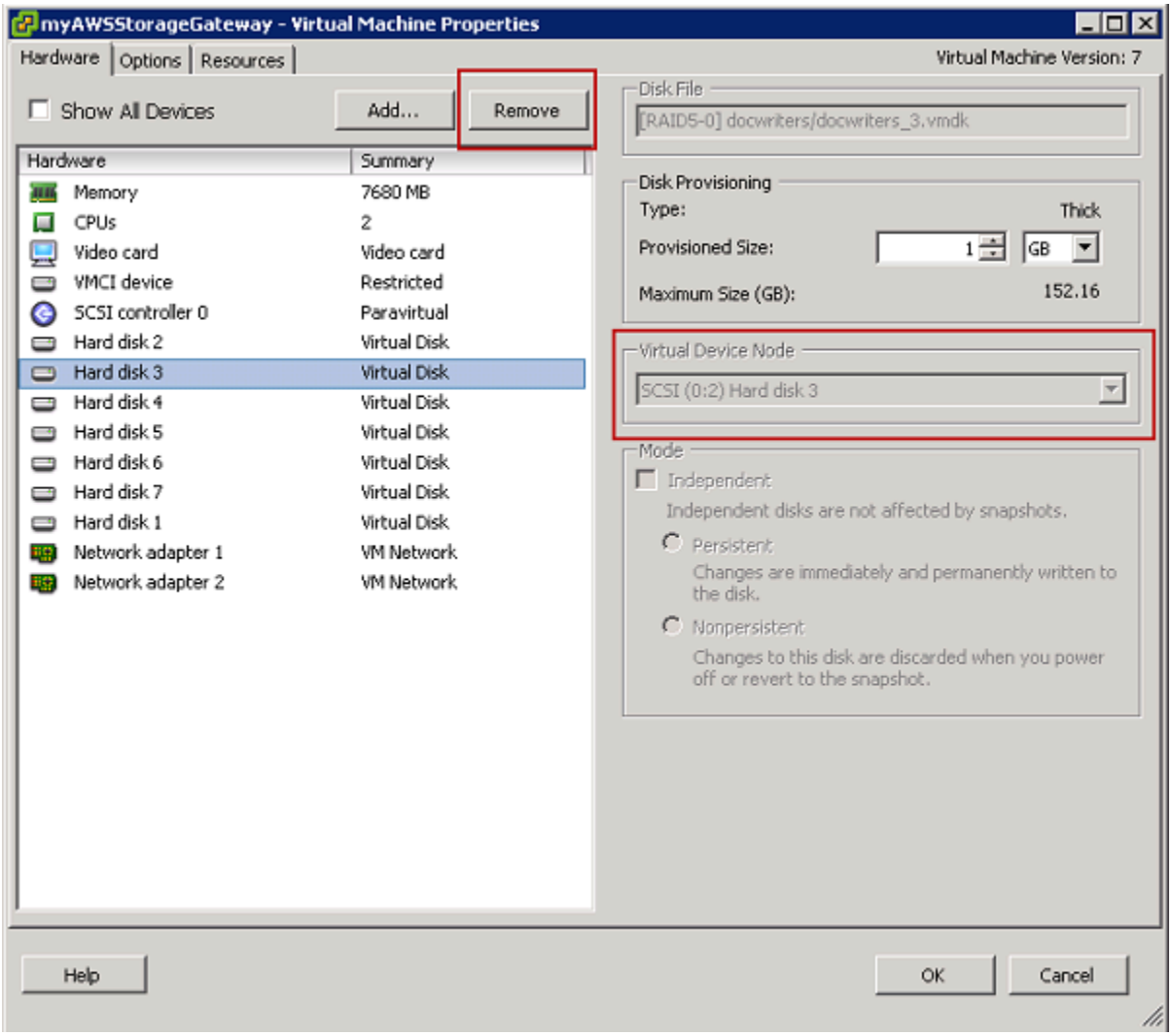
에 호스팅된 게이트웨이에서 디스크 제거 VMware ESXi

다음 절차를 사용하여 VMware 하이퍼바이저에서 호스팅되는 게이트웨이에서 디스크를 제거할 수 있습니다.

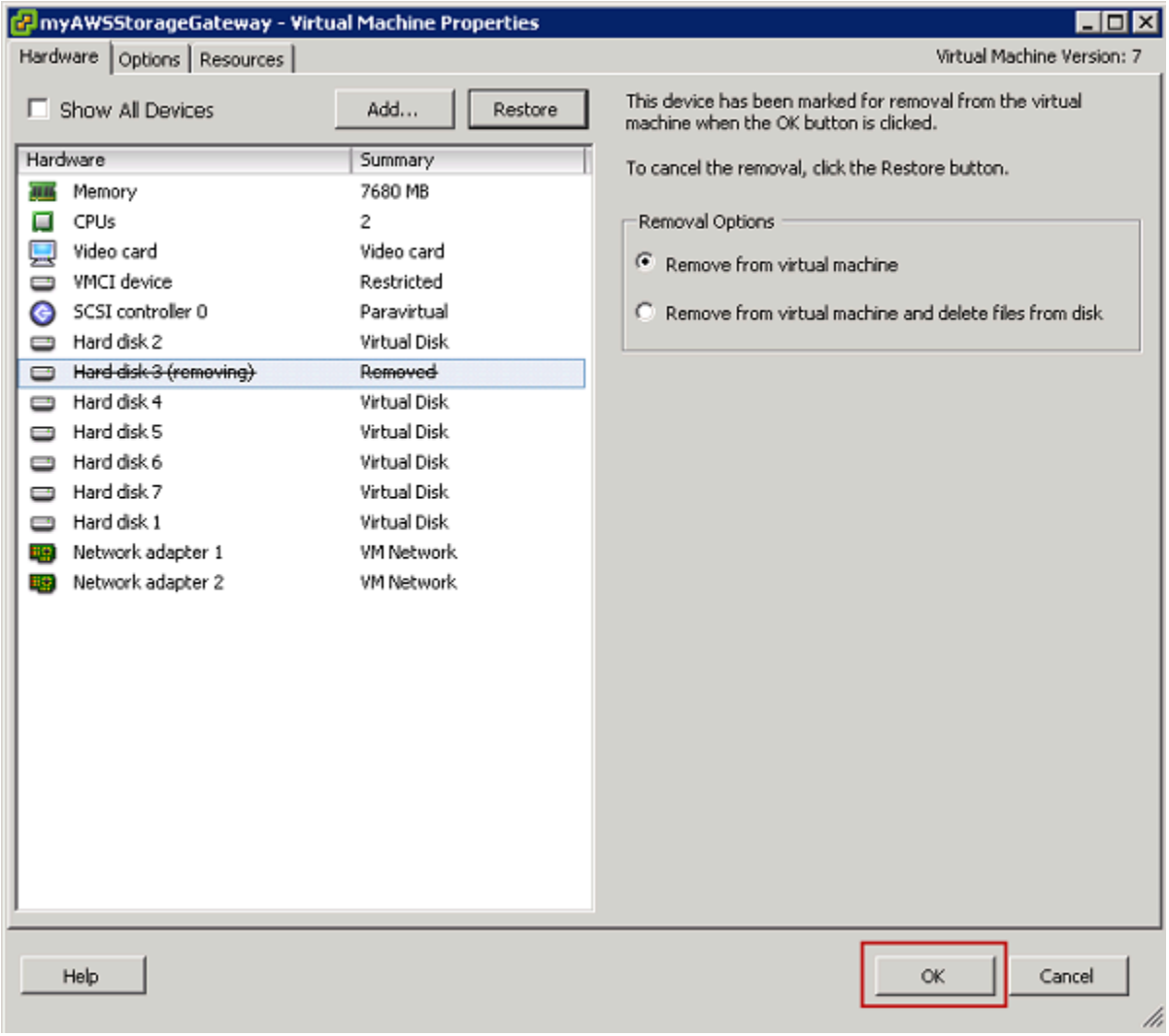
업로드 버퍼에 할당된 디스크를 제거하려면 () VMware ESXi

1. vSphere 클라이언트에서 컨텍스트 (마우스 오른쪽 버튼 클릭) 메뉴를 열고 게이트웨이 VM의 이름을 선택한 다음 설정 편집을 선택합니다.
2. 가상 머신 속성 대화 상자의 하드웨어 탭에서 업로드 버퍼 공간으로 할당된 디스크를 선택한 다음 제거를 선택합니다.

   가상 머신 속성 대화 상자의 가상 디바이스 노드 값이 이전에 기록한 값과 같은지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.



3. Removal Options(제거 옵션) 패널에서 옵션을 선택한 후 확인을 선택하여 디스크 제거 절차를 완료합니다.



Microsoft Hyper-V에 호스팅된 게이트웨이에서 디스크 제거

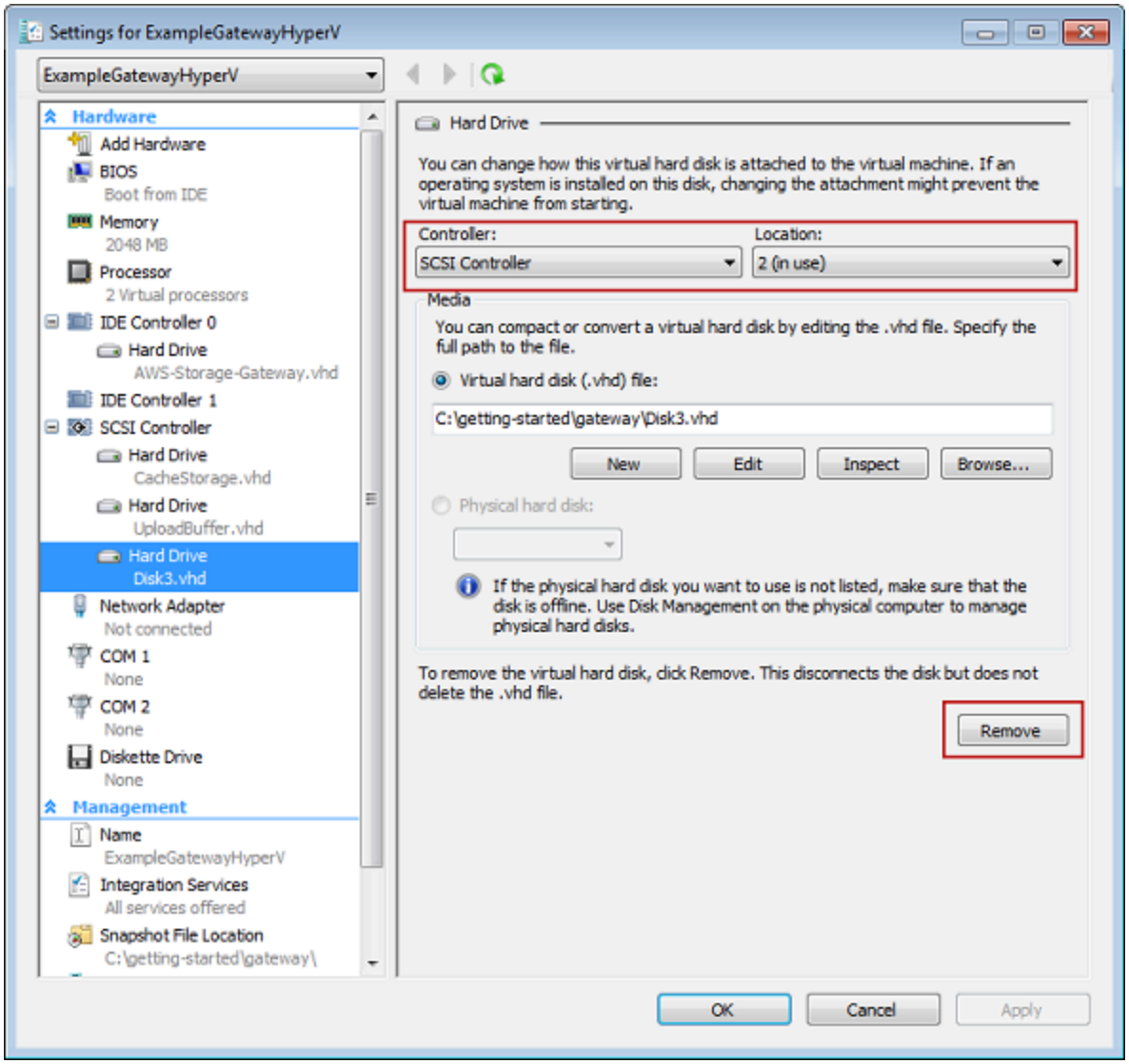
다음 절차에 따라 Microsoft Hyper-V 하이퍼바이저에서 호스팅하는 게이트웨이에서 디스크를 제거할 수 있습니다.

업로드 버퍼에 할당된 기본 디스크를 제거하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager에서 마우스 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 열고 게이트웨이 VM의 이름을 선택한 후 설정을 선택합니다.
2. 설정 대화 상자의 하드웨어 목록에서 제거할 디스크를 선택한 다음 제거를 선택합니다.

   게이트웨이에 추가한 디스크는 하드웨어 목록의 SCSI컨트롤러 항목 아래에 표시됩니다. 컨트롤러 및 위치 값이 앞에서 기록해 둔 값과 동일한지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.

Microsoft Hyper-V 관리자에 표시되는 첫 SCSI 번째 컨트롤러는 컨트롤러 0입니다.



3. 확인을 선택하여 변경 사항을 적용합니다.

Linux에서 호스팅되는 게이트웨이에서 디스크 제거 KVM

Linux 커널 기반 Virtual Machine (KVM) 하이퍼바이저에서 호스팅되는 게이트웨이에서 디스크를 분리하려면 다음과 비슷한 `virsh` 명령을 사용할 수 있습니다.

```
$ virsh detach-disk domain_name /device/path
```

KVM디스크 관리에 대한 자세한 내용은 Linux 배포판 설명서를 참조하십시오.

Amazon EC2 게이트웨이용 Amazon EBS 볼륨 추가 및 제거

Amazon EC2 인스턴스로 실행되도록 게이트웨이를 처음 구성할 때 Amazon EBS 볼륨을 업로드 버퍼 및 캐시 스토리지로 사용하도록 할당했습니다. 시간이 지나면서 애플리케이션 요구 사항이 변경되면 이 용도로 Amazon EBS 볼륨을 추가로 할당할 수 있습니다. 이전에 할당된 Amazon EBS 볼륨을 제거하여 할당한 스토리지를 줄일 수도 있습니다. Amazon에 대한 자세한 내용은 Amazon EBS EC2사용 설명서의 Amazon Elastic Block Store (AmazonEBS) 를 참조하십시오.

게이트웨이에 스토리지를 추가하기 전에 게이트웨이에 대한 애플리케이션 요구 사항에 따라 업로드 버퍼와 캐시 스토리지의 크기를 조정하는 방법을 검토해야 합니다. 그렇게 하려면 할당할 업로드 버퍼의 크기 결정 및 할당할 캐시 스토리지의 크기 결정 단원을 참조하십시오.

업로드 버퍼 및 캐시 스토리지로 할당할 수 있는 최대 스토리지에는 할당량이 있습니다. Amazon EBS 볼륨을 원하는 만큼 인스턴스에 연결할 수 있지만, 이러한 볼륨은 해당 스토리지 할당량까지만 업로드 버퍼 및 캐시 스토리지 공간으로 구성할 수 있습니다. 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오.

Amazon EBS 볼륨을 추가하고 게이트웨이에 맞게 구성하려면

1. Amazon EBS 볼륨을 생성합니다. 지침은 Amazon 사용 EC2설명서의 Amazon EBS 볼륨 생성 또는 복원을 참조하십시오.
2. Amazon EBS 볼륨을 Amazon EC2 인스턴스에 연결합니다. 지침은 Amazon 사용 EC2설명서의 인스턴스에 Amazon EBS 볼륨 연결을 참조하십시오.
3. 추가한 Amazon EBS 볼륨을 업로드 버퍼 또는 캐시 스토리지로 구성합니다. 지침은 Storage Gateway의 로컬 디스크 관리 단원을 참조하십시오.

업로드 버퍼에 할당한 스토리지 용량이 필요 없다는 판단을 내리게 되는 경우가 있습니다.

Amazon EBS 볼륨을 제거하려면

> **Warning**
>
> 이 단계는 업로드 버퍼 공간으로 할당된 Amazon EBS 볼륨에만 적용되며 캐시에 할당된 볼륨에는 적용되지 않습니다.

1. 게이트웨이 VM 종료 단원에서 설명하는 접근 방식에 따라 게이트웨이를 종료합니다.

2. Amazon EC2 인스턴스에서 Amazon EBS 볼륨을 분리합니다. 지침은 Amazon 사용 EC2설명서의 인스턴스에서 Amazon EBS 볼륨 분리를 참조하십시오.
3. Amazon EBS 볼륨을 삭제합니다. 지침은 Amazon 사용 EC2설명서의 Amazon EBS 볼륨 삭제를 참조하십시오.
4. 게이트웨이 VM 종료 단원에서 설명하는 접근 방식에 따라 게이트웨이를 시작합니다.

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 참조를 참조하십시오 ActivateGateway.

> **Note**
>
> 게이트웨이 활성화 키는 사용하지 않으면 30분 후에 만료됩니다.

게이트웨이 VM에 보내는 요청에는 활성화가 발생하는 AWS 지역이 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**
>
> Storage Gateway 하드웨어 어플라이언스, VM 이미지 템플릿, Amazon EC2 Amazon Machine Image(AMI)에는 이 페이지에 설명된 웹 요청을 수신하고 이에 응답하는 데 필요한 HTTP 서비스가 사전 구성되어 있습니다. 게이트웨이에 추가 서비스를 설치할 필요는 없으며 권장하지도 않습니다.

주제

- Linux(curl)

- Linux(bash/zsh)
- 마이크로소프트 윈도우 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 게이트웨이 유형 (예:, STORED CACHEDVTL, FILE_S3 또는). FILE_FSX_SMB
> - *region_code* - 게이트웨이를 활성화할 리전입니다.AWS 일반 참조 안내서에서 리전 엔드포인트를 참조하세요. 이 매개 변수가 지정되지 않았거나 제공된 값의 철자가 틀렸거나 유효한 지역과 일치하지 않는 경우 명령은 기본적으로 해당 지역을 사용합니다. us-east-1
> - *vpc_endpoint* - 게이트웨이의 VPC 엔드포인트 이름입니다(예: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com).

퍼블릭 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

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
}
```

마이크로소프트 윈도우 PowerShell

다음 예제는 Microsoft PowerShell Windows를 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 가져오는 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.

로컬 콘솔에서 게이트웨이 활성화 키를 가져오려면

1. 로컬 콘솔에 로그인합니다. Amazon EC2 인스턴스에 연결하는 경우, admin으로 로그인합니다.
2. 로그인하여 AWS 어플라이언스 활성화 - 구성 기본 메뉴가 표시되면 0을 선택하여 활성화 키 받기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 메시지가 표시되면 게이트웨이를 활성화할 AWS 지역을 입력합니다.
5. 네트워크 유형으로 퍼블릭의 경우 1을, VPC 엔드포인트의 경우 2를 입력합니다.
6. 엔드포인트 유형으로 표준의 경우 1을, FIPS(Federal Information Processing Standard)의 경우 2를 입력합니다.

SCSI이니시에이터 연결

게이트웨이를 관리할 때는 인터넷 소형 컴퓨터 시스템 인터페이스 (iVTL) 대상으로 노출되는 볼륨 또는 가상 테이프 라이브러리 (SCSI) 장치를 사용합니다. 볼륨 게이트웨이의 경우 i SCSI 타겟은 볼륨입니다. 테이프 게이트웨이의 경우 타겟은 디바이스입니다. VTL 이 작업의 일환으로 해당 대상에 연결하고, SCSI 설정을 사용자 지정하고, Red Hat Linux 클라이언트에서 연결하고, 챌린지-핸드셰이크 인증 프로토콜 () 구성과 같은 작업을 수행합니다. CHAP

주제

- 볼륨을 Windows 클라이언트에 연결
- Linux 클라이언트에 볼륨 또는 VTL 디바이스 연결
- i 설정 사용자 지정 SCSI
- i 타겟에 대한 CHAP 인증 구성 SCSI

i SCSI 표준은 IP 기반 스토리지 장치와 클라이언트 간의 연결을 시작하고 관리하기 위한 인터넷 프로토콜 (IP) 기반 스토리지 네트워킹 표준입니다. 다음 목록에는 i SCSI 연결 및 관련 구성 요소를 설명하는 데 사용되는 몇 가지 용어가 정의되어 있습니다.

i SCSI 이니시에이터

i SCSI 네트워크의 클라이언트 구성 요소. 이니시에이터는 i SCSI 타겟에 요청을 보냅니다. 이니시에이터는 소프트웨어 또는 하드웨어로 구현할 수 있습니다. Storage Gateway는 소프트웨어 이니시에이터만 지원합니다.

i 타겟 SCSI

이니시에이터의 요청을 수신하고 이에 응답하는 i SCSI 네트워크의 서버 구성 요소. 각 볼륨은 i SCSI 타겟으로 노출됩니다. 각 i SCSI 타겟에는 i SCSI 이니시에이터를 하나만 연결합니다.

마이크로소프트 i SCSI 이니시에이터

클라이언트 컴퓨터 (즉, 게이트웨이에 데이터를 쓰려는 응용 프로그램을 실행하는 컴퓨터) 를 외부 i SCSI 기반 배열 (게이트웨이) 에 연결할 수 있게 해주는 Microsoft Windows 컴퓨터의 소프트웨어 프로그램입니다. 호스트 컴퓨터의 이더넷 네트워크 어댑터 카드를 사용하여 연결합니다. Microsoft i SCSI 이니시에이터는 윈도우 8.1, 윈도우 10, 윈도우 서버 2012 R2, 윈도우 서버 2016 및 윈도우 서버 2019에서 Storage Gateway로 검증되었습니다. 이니시에이터는 이러한 운영 체제에 기본 제공됩니다.

Red Hat은 이니시에이터입니다. SCSI

`iscsi-initiator-utils`리소스 패키지 관리자 (RPM) 패키지는 Red Hat Linux용 소프트웨어로 구현된 i SCSI 이니시에이터를 제공합니다. 패키지에는 i 프로토콜용 서버 데몬이 포함되어 있습니다. SCSI

각 유형의 게이트웨이는 i SCSI 기기에 연결할 수 있으며, 다음 설명과 같이 이러한 연결을 사용자 지정할 수 있습니다.

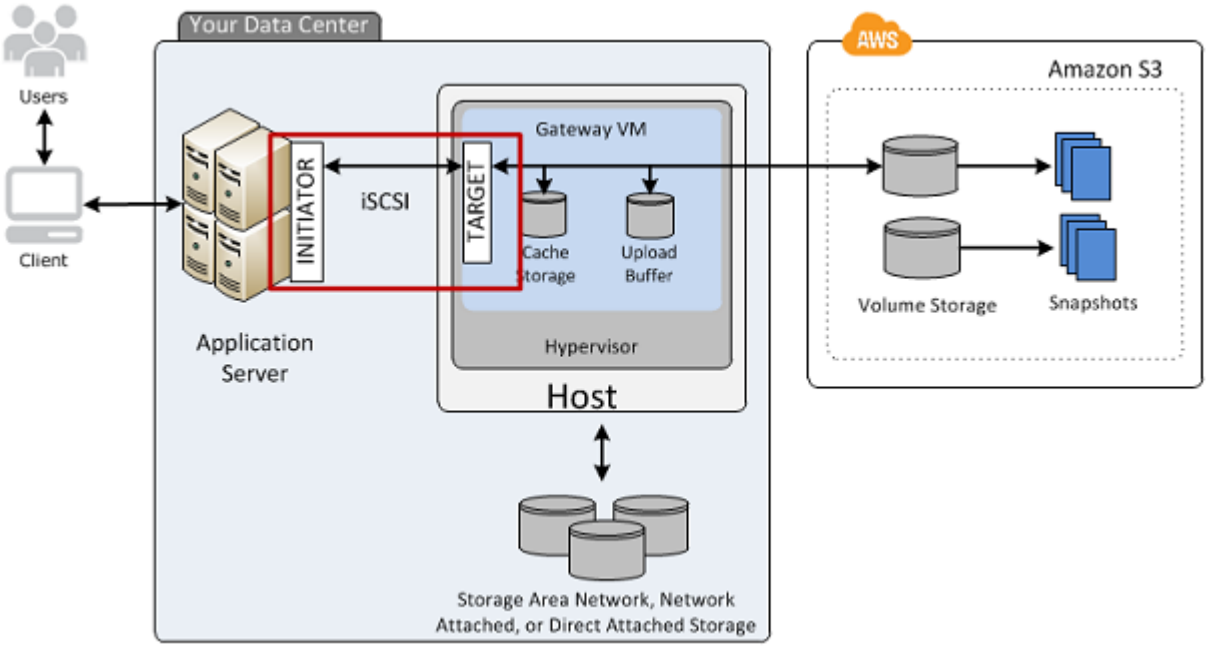
볼륨을 Windows 클라이언트에 연결

볼륨 게이트웨이는 게이트웨이용으로 생성한 볼륨을 i SCSI 타겟으로 노출합니다. 자세한 내용은 볼륨을 클라이언트에 연결 단원을 참조하십시오.

> **Note**
>
> 볼륨 대상에 연결하려면 해당 게이트웨이에 업로드 버퍼를 구성되어 있어야 합니다. 게이트웨이에 업로드 버퍼가 구성되지 않은 경우 볼륨 상태가 로 UPLOAD BUFFER NOT CONFIGURED 표시됩니다. 저장 볼륨 설정에 게이트웨이용 업로드 버퍼를 구성하려면 게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면 단원을 참조하십시오. 캐싱

볼륨 설정에 게이트웨이용 업로드 버퍼를 구성하려면 게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면 단원을 참조하십시오.

다음 다이어그램은 Storage Gateway 아키텍처의 큰 그림에서 i SCSI 타겟을 강조 표시합니다. 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 단원을 참조하십시오.



Windows 또는 Red Hat Linux 클라이언트에서 볼륨에 연결할 수 있습니다. 두 클라이언트 유형 중 하나를 선택적으로 구성할 CHAP 수 있습니다.

게이트웨이는 볼륨을 사용자가 지정한 이름과 앞에 붙인 i SCSI 타겟으로 노출합니다. `iqn.1997-05.com.amazon:` 예를 들어, 대상 이름을 지정하는 경우 `myvolume` 볼륨에 연결하는 데 사용하는 i SCSI 대상은 입니다. `iqn.1997-05.com.amazon:myvolume` SCSIi를 통해 볼륨을 마운트하도록 애플리케이션을 구성하는 방법에 대한 자세한 내용은 을 참조하십시오볼륨을 Windows 클라이언트에 연결.

To	다음을 참조하십시오.
Windows에서 볼륨에 연결	Microsoft Windows 클라이언트에 연결
Red Hat Linux에서 볼륨에 연결	Red Hat Enterprise Linux 클라이언트에 연결

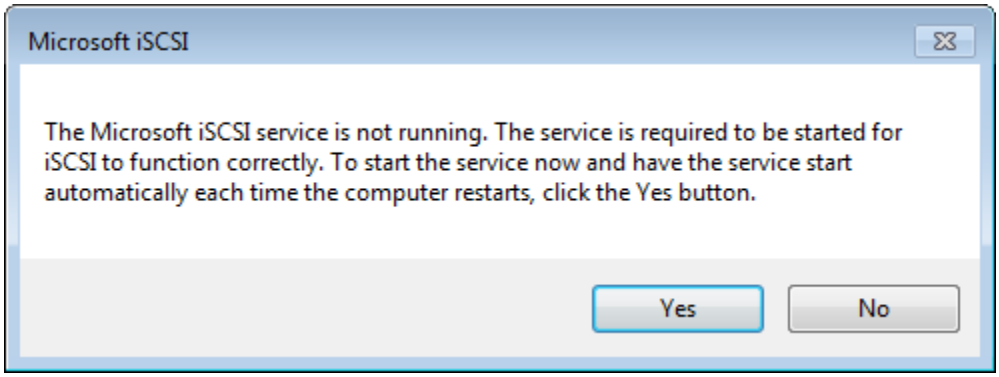
To	다음을 참조하십시오.
윈도우 및 레드햇 리눅스에 대한 CHAP 인증을 구성하십시오.	i 타겟에 대한 CHAP 인증 구성 SCSI

Windows 클라이언트를 스토리지 볼륨에 연결하려면

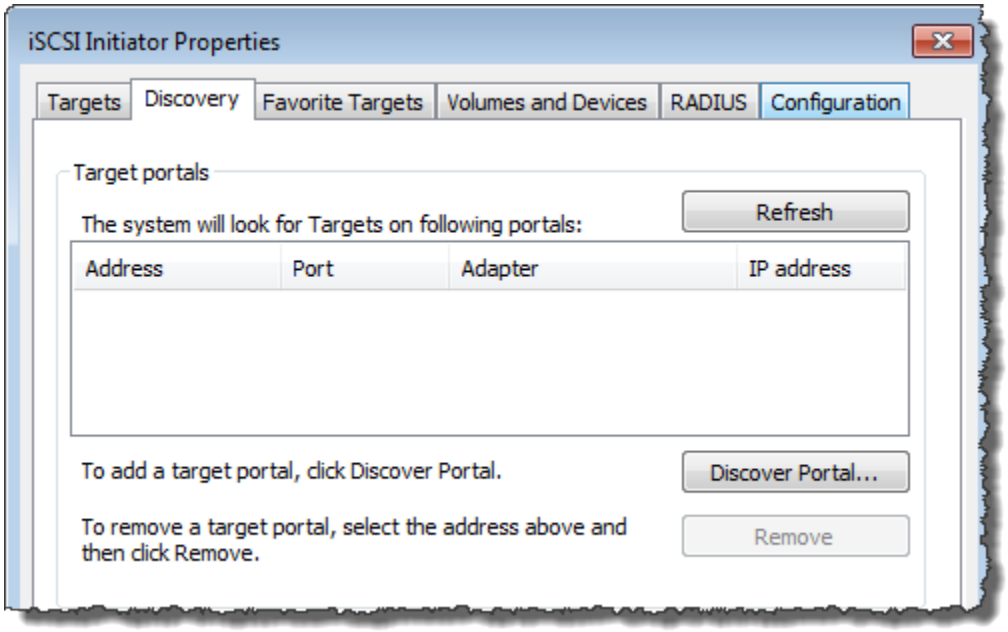
1. Windows 클라이언트 컴퓨터의 시작 메뉴에서 프로그램 및 파일 검색 상자에 를 입력하고 **`iscsicpl.exe`** i SCSI 이니시에이터 프로그램을 찾은 다음 실행합니다.

   > **Note**
   >
   > i SCSI 이니시에이터를 실행하려면 클라이언트 컴퓨터에 대한 관리자 권한이 있어야 합니다.

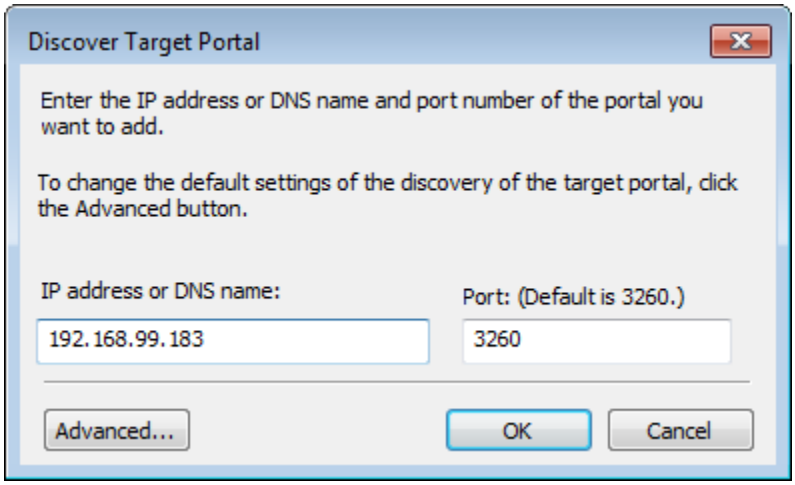
2. 메시지가 표시되면 [예] 를 선택하여 Microsoft i SCSI 이니시에이터 서비스를 시작합니다.



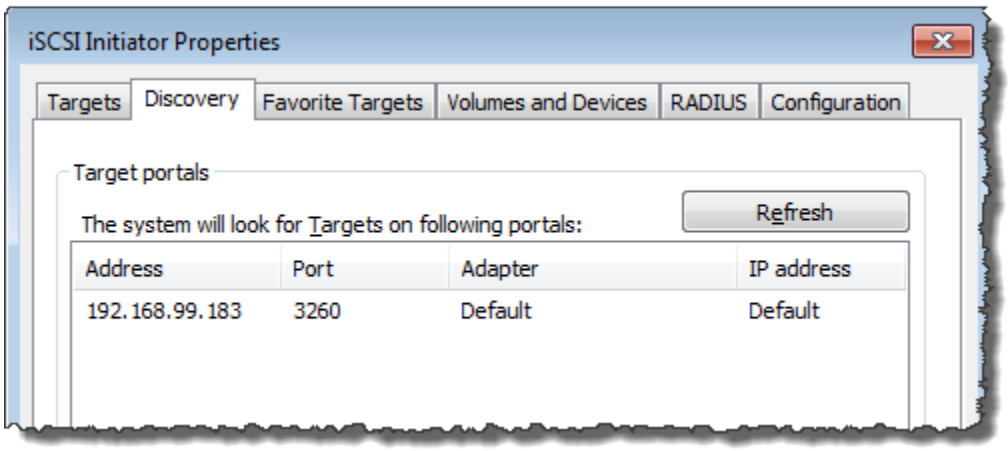
3. i SCSI 이니시에이터 속성 대화 상자에서 검색 탭을 선택한 다음 검색 포털을 선택합니다.



4. 대상 포털 검색 대화 상자에서 IP 주소 또는 DNS 이름으로 i SCSI 대상의 IP 주소를 입력한 다음 확인을 선택합니다. 게이트웨이의 IP 주소를 가져오려면 Storage Gateway 콘솔의 게이트웨이 탭을 확인합니다. Amazon EC2 인스턴스에 게이트웨이를 배포한 경우 Amazon EC2 콘솔의 설명 탭에서 퍼블릭 IP 또는 DNS 주소를 찾을 수 있습니다.



이제 IP 주소가 검색 탭의 대상 포털 목록에 나타납니다.

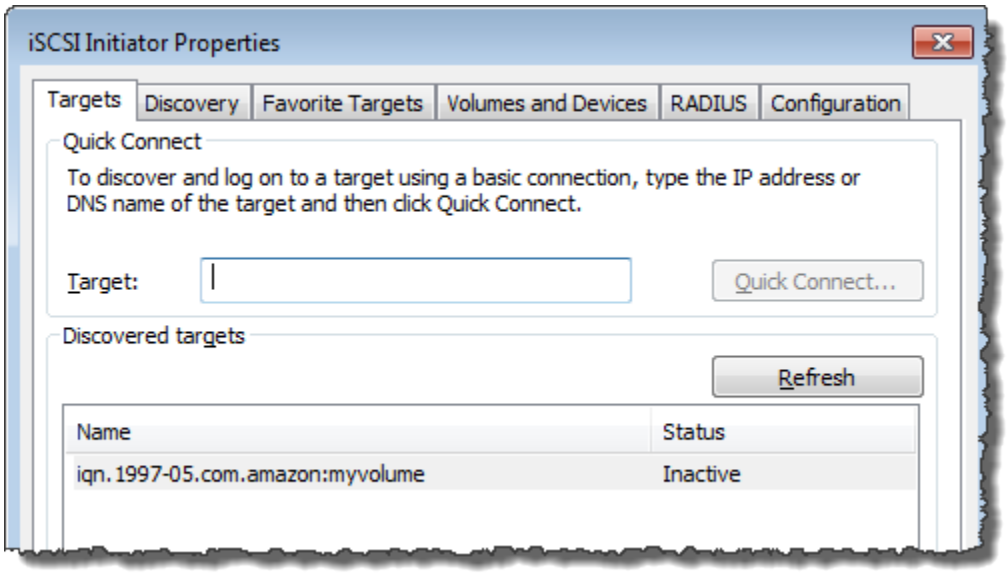


> **Warning**
>
> Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 퍼블릭 인터넷 연결을 통한 게이트웨이 액세스는 지원되지 않습니다. Amazon EC2 인스턴스의 엘라스틱 IP 주소는 대상 주소로 사용할 수 없습니다.

5. 새로운 대상 포털을 게이트웨이의 스토리지 볼륨 대상에 연결합니다.

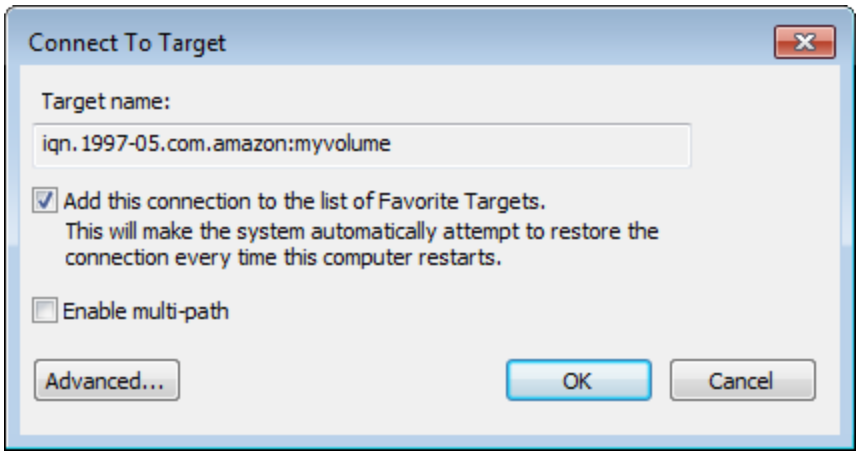
   a. 대상 탭을 선택합니다.

      새 대상 포털은 비활성 상태로 표시됩니다. 표시된 대상 이름은 1단계에서 스토리지 볼륨에 지정한 이름과 같아야 합니다.

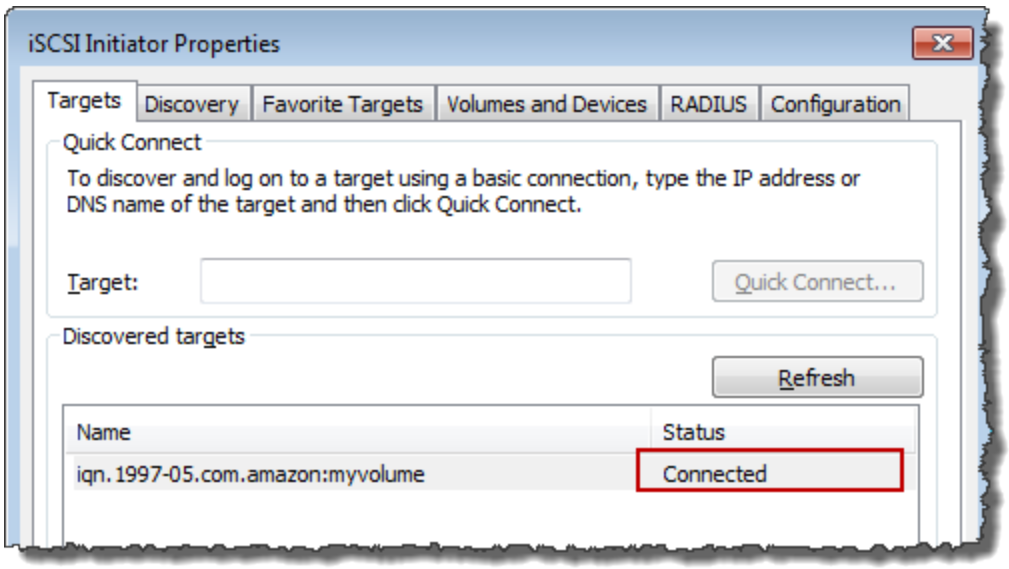


   b. 대상을 선택한 후 연결을 선택합니다.

대상 이름이 아직 입력되지 않은 경우 1단계와 같이 대상 이름을 입력합니다. 대상에 연결 대화 상자에서 즐겨찾는 대상 목록에 이 연결 추가를 선택한 다음 확인을 선택합니다.



c. 대상 탭에서 대상 상태가 대상이 연결되어 있음을 나타내는 연결 상태라는 값으로 되어 있는지 확인한 후 확인을 선택합니다.



이제 이 Windows용 스토리지 볼륨을 초기화하고 포맷하여 이 볼륨에 데이터 저장을 시작할 수 있습니다. Windows 디스크 관리 도구를 사용하여 이 작업을 할 수 있습니다.

> **Note**
>
> 이 연습에서는 필수는 아니지만 에서 설명한 대로 실제 애플리케이션에 맞게 i SCSI 설정을 사용자 지정하는 것이 좋습니다. Windows i SCSI 설정 사용자 지정하기

Linux 클라이언트에 볼륨 또는 VTL 디바이스 연결

Red Hat Enterprise Linux (RHEL) 를 사용할 때는 `iscsi-initiator-utils` RPM 패키지를 사용하여 게이트웨이 i SCSI 타겟 (볼륨 또는 VTL 디바이스) 에 연결합니다.

Linux 클라이언트를 i SCSI 타겟에 연결하려면

1. `iscsi-initiator-utils`RPM패키지를 설치하세요 (클라이언트에 아직 설치되지 않은 경우).

   다음 명령을 사용하여 패키지를 설치할 수 있습니다.

   ```
   sudo yum install iscsi-initiator-utils
   ```

2. i SCSI 데몬이 실행 중인지 확인하십시오.

   a. 다음 명령 중 하나를 사용하여 i SCSI 데몬이 실행되고 있는지 확인합니다.

      RHEL5 또는 6의 경우 다음 명령을 사용합니다.

      ```
      sudo /etc/init.d/iscsi status
      ```

      RHEL7의 경우 다음 명령을 사용합니다.

      ```
      sudo service iscsid status
      ```

   b. 상태 명령이 running 상태를 반환하지 않으면 다음 명령 중 하나를 사용하여 데몬을 시작합니다.

      RHEL5 또는 6의 경우 다음 명령을 사용합니다.

      ```
      sudo /etc/init.d/iscsi start
      ```

      RHEL7의 경우 다음 명령을 사용합니다. RHEL7의 경우 일반적으로 서비스를 명시적으로 시작할 필요가 없습니다. `iscsid`

```
sudo service iscsid start
```

3. 게이트웨이에 정의된 볼륨 또는 VTL 장치 대상을 검색하려면 다음 검색 명령을 사용합니다.

```
sudo /sbin/iscsiadm --mode discovery --type sendtargets --portal [GATEWAY_IP]:3260
```

게이트웨이의 IP 주소를 다음으로 대체하십시오.*[GATEWAY_IP]* 이전 명령의 변수. 게이트웨이 IP는 Storage Gateway 콘솔의 볼륨의 i SCSI 타겟 정보 속성에서 찾을 수 있습니다.

검색 명령은 다음 예시 출력과 비슷하게 출력됩니다.

Volume Gateway: *[GATEWAY_IP]*:3260, 1 iqn.1997-05.com.amazon:myvolume

Tape Gateway의 경우: iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

IQN값은 조직마다 고유하므로 SCSI 자격 있는 이름 (IQN) 은 앞에 표시된 것과 다릅니다. 대상의 이름은 볼륨 생성 시 지정한 이름입니다. Storage Gateway 콘솔에서 볼륨을 선택할 때 i SCSI 타겟 정보 속성 창에서도 이 타겟 이름을 찾을 수 있습니다.

4. 대상에 접속하려면 다음 명령을 사용하십시오.

참고로, 올바른 이름을 지정해야 합니다.*[GATEWAY_IP]* 그리고 연결 IQN 명령에서.

> **Warning**
>
> Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 퍼블릭 인터넷 연결을 통한 게이트웨이 액세스는 지원되지 않습니다. Amazon EC2 인스턴스의 엘라스틱 IP 주소는 대상 주소로 사용할 수 없습니다.

```
sudo /sbin/iscsiadm --mode node --targetname
 iqn.1997-05.com.amazon:[ISCSI_TARGET_NAME] --portal [GATEWAY_IP]:3260,1 --login
```

5. 볼륨이 클라이언트 머신(초기자)에 연결되었는지 확인하려면 다음 명령을 사용해야 합니다.

```
ls -l /dev/disk/by-path
```

이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

```
lrwxrwxrwx. 1 root root 9 Apr 16 19:31 ip-[GATEWAY_IP]:3260-iscsi-
iqn.1997-05.com.amazon:myvolume-lun-0 -> ../../sda
```

이니시에이터를 설정한 후에는 에서 Linux i 설정 사용자 지정하기 SCSI 설명한 대로 i SCSI 설정을 사용자 지정하는 것이 좋습니다.

i 설정 사용자 지정 SCSI

이니시에이터를 설정한 후에는 이니시에이터와 대상과의 연결이 끊기지 않도록 i SCSI 설정을 사용자 지정하는 것이 좋습니다.

다음 단계에 표시된 대로 i SCSI timeout 값을 늘리면 응용 프로그램에서 시간이 오래 걸리는 쓰기 작업과 네트워크 중단과 같은 기타 일시적인 문제를 더 잘 처리할 수 있습니다.

> **Note**
>
> 레지스트리를 변경하기 전에 레지스트리의 백업 사본을 만들어야 합니다. 백업 복사본을 만드는 방법과 레지스트리 사용 시 따라야 할 기타 모범 사례에 대한 자세한 내용은 Microsoft TechNet Library의 레지스트리 모범 사례를 참조하십시오.

주제

- Windows i SCSI 설정 사용자 지정하기
- Linux i 설정 사용자 지정하기 SCSI
- Volume Gateway의 Linux 디스크 제한 시간 설정 사용자 지정

Windows i SCSI 설정 사용자 지정하기

Windows 클라이언트를 사용하는 경우 Microsoft i SCSI 이니시에이터를 사용하여 게이트웨이 볼륨에 연결합니다. 볼륨에 접속하는 방법에 대한 지침은 볼륨을 클라이언트에 연결 단원을 참조하십시오.

1. Tape Gateway 디바이스를 Windows 클라이언트에 연결합니다.
2. 백업 애플리케이션을 사용하는 경우, 애플리케이션에서 디바이스를 사용하도록 구성합니다.

Windows i 설정을 사용자 지정하려면 SCSI

1. 요청이 대기하는 최대 시간을 늘립니다.

   a. 레지스트리 편집기(`Regedit.exe`)를 시작합니다.

   b. 다음과 같이 i SCSI 컨트롤러 설정이 포함된 장치 클래스의 글로벌 고유 식별자 (GUID) 키로 이동합니다.

   > **Warning**
   >
   > ControlSet001 또는 ControlSet 002와 같은 다른 제어 세트가 아닌 CurrentControlSet하위 키에서 작업하고 있는지 확인하십시오.

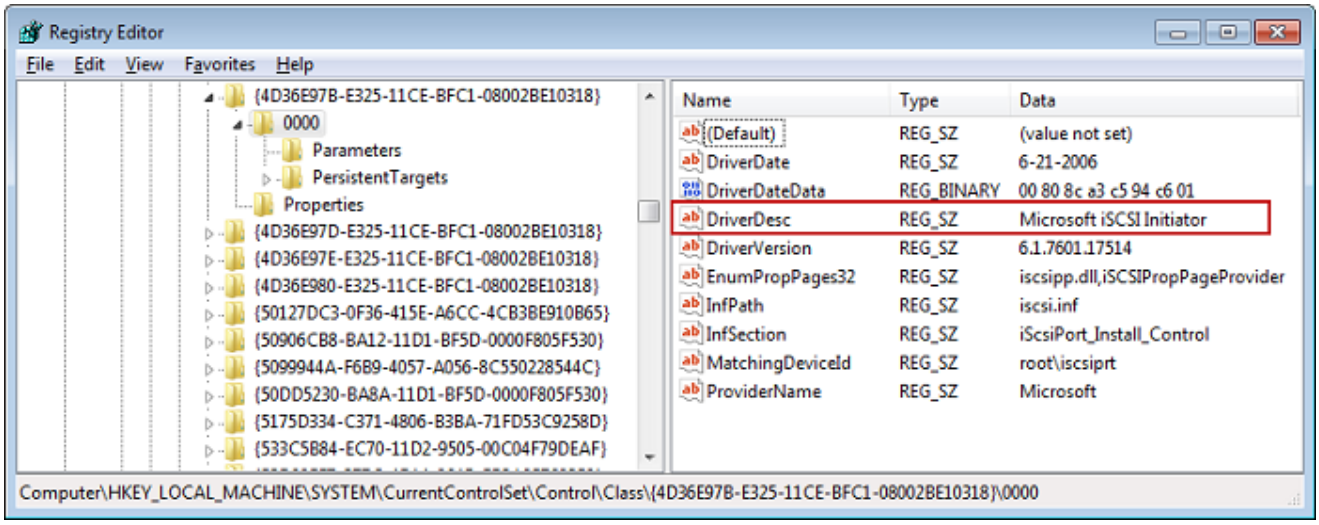
   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
   ```

   c. 다음과 같이 Microsoft i SCSI 이니시에이터의 하위 키를 찾으십시오.*[<Instance Number]*.

   하위 키는 `0000`과 같이 네 자리 숫자로 표시됩니다.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
   ```

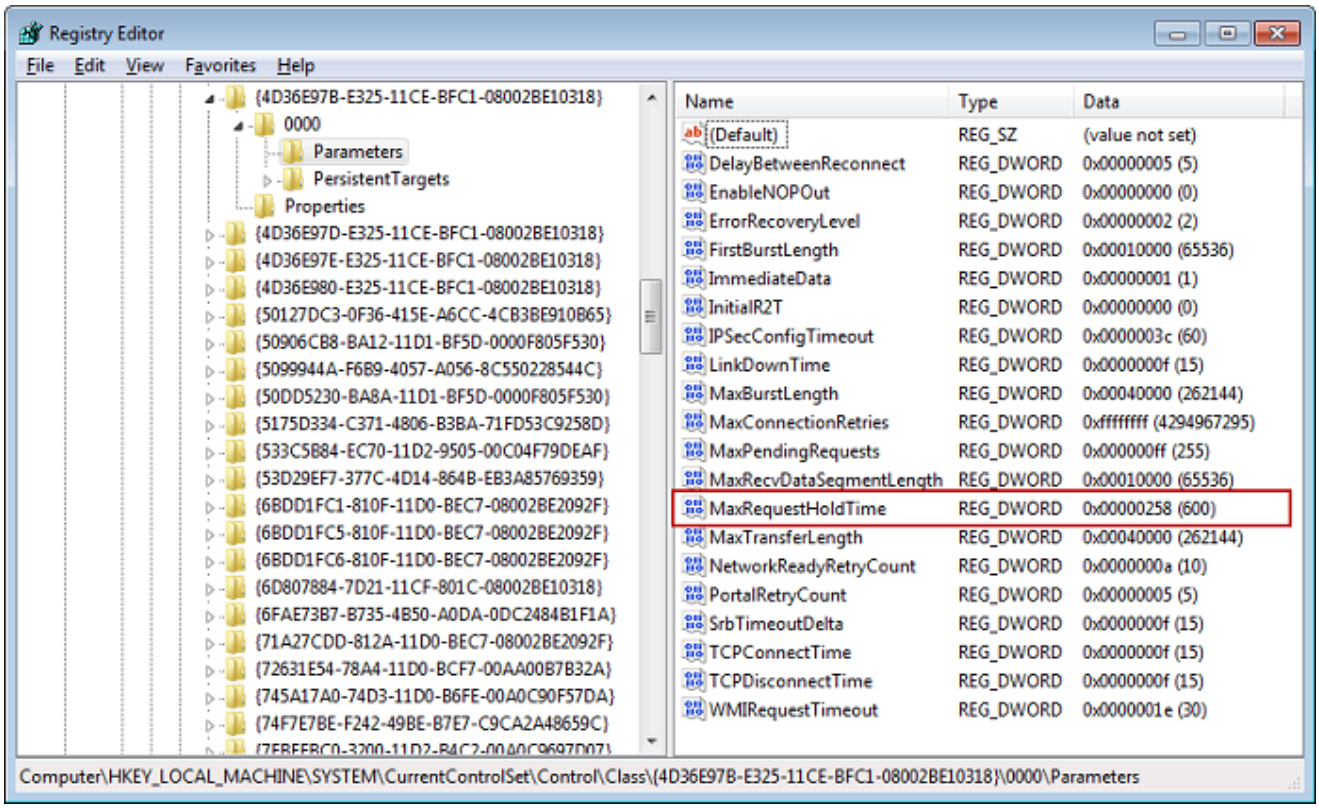
   컴퓨터에 설치된 항목에 따라 Microsoft i SCSI 이니시에이터가 하위 `0000` 키가 아닐 수도 있습니다. 다음 예시에서처럼 `DriverDesc`라는 문자열이 `Microsoft iSCSI Initiator`라는 값을 갖는지 확인하여 정확한 하위 키를 선택했는지 확인할 수 있습니다.



d. i SCSI 설정을 표시하려면 매개 변수 하위 키를 선택합니다.

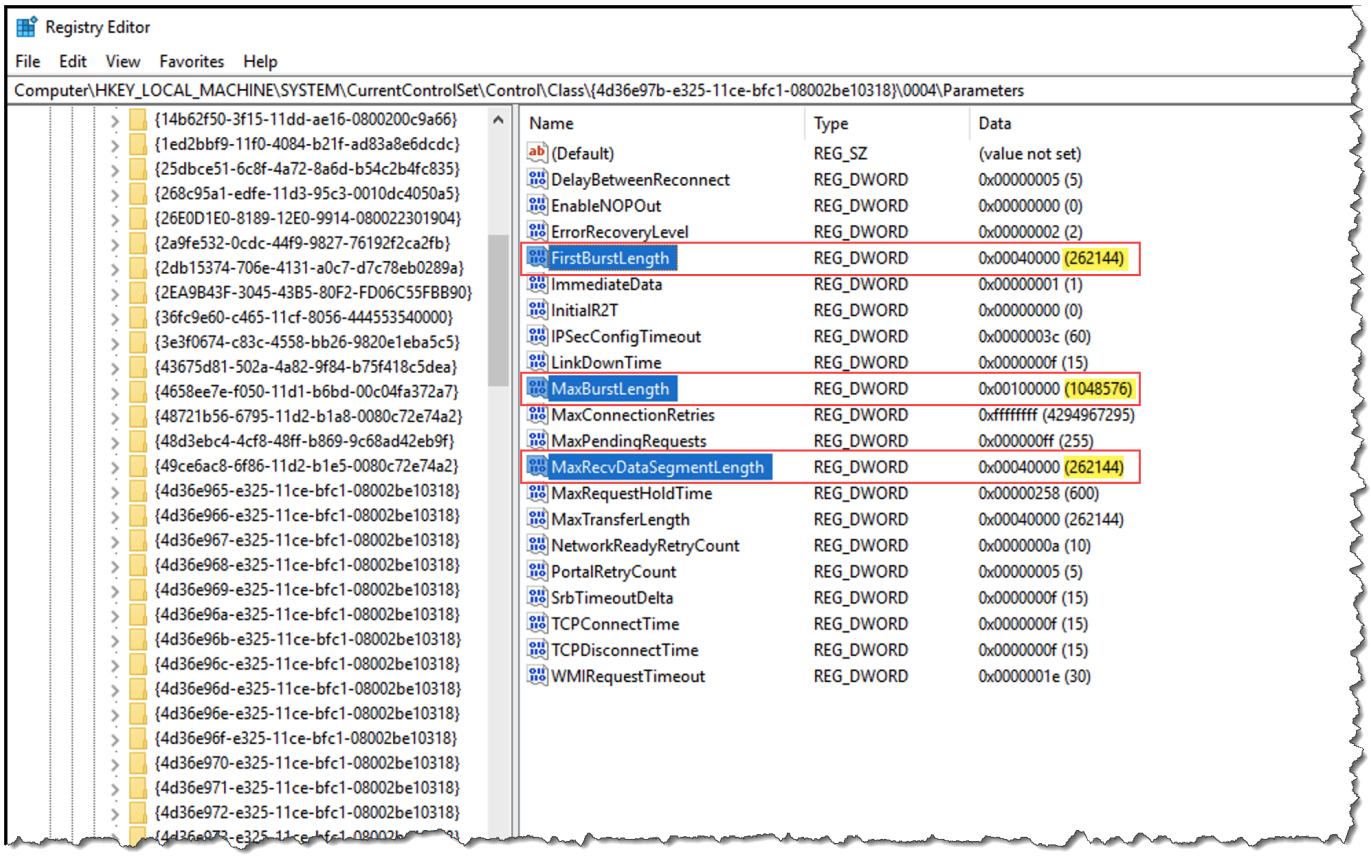
e. (32비트) 값에 대한 컨텍스트 메뉴 MaxRequestHoldTimeDWORD(마우스 오른쪽 버튼 클릭)를 열고 수정을 선택한 다음 값을 로 변경합니다. **`600`**

MaxRequestHoldTimeMicrosoft i SCSI Initiator가 이벤트의 상위 계층에 알리기 전에 미해결 명령을 보류하고 재시도해야 하는 시간을 초 단위로 지정합니다. `Device Removal` 다음 예와 같이 이 값은 600초의 보류 시간을 나타냅니다.



2. 다음 매개 변수를 수정하여 i SCSI 패킷으로 전송할 수 있는 최대 데이터 양을 늘릴 수 있습니다.

   - FirstBurstLength요청되지 않은 쓰기 요청으로 전송할 수 있는 최대 데이터 양을 제어합니다. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.
   - MaxBurstLength와 FirstBurstLength비슷하지만 요청된 쓰기 시퀀스로 전송할 수 있는 최대 데이터 양을 설정합니다. 이 값을 **1048576** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.
   - MaxRecvDataSegmentLength단일 프로토콜 데이터 단위 (PDU) 와 관련된 최대 데이터 세그먼트 크기를 제어합니다. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.



> **Note**
>
> 다양한 i SCSI 설정을 사용하여 최상의 성능을 발휘하도록 여러 백업 소프트웨어를 최적화할 수 있습니다. 이러한 파라미터의 값이 최상의 성능을 제공하는지 확인하려면 백업 소프트웨어 설명서를 참조하십시오.

3. 다음과 같이 디스크 제한 시간 값을 늘립니다.

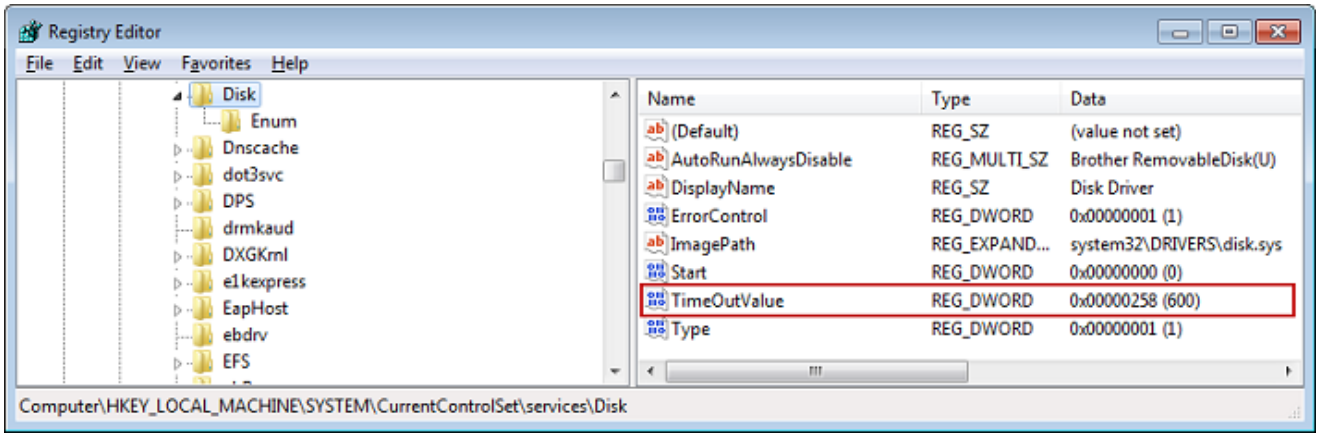
   a. 레지스트리 편집기(Regedit.exe)를 아직 시작하지 않았다면 지금 시작하십시오.

   b. 다음과 같이 의 서비스 하위 키에서 디스크 하위 키로 이동합니다. CurrentControlSet

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. (32비트) 값에 대한 컨텍스트 TimeOutValueDWORD(마우스 오른쪽 단추 클릭) 메뉴를 열고 [수정] 을 선택한 다음 값을 로 변경합니다. **600**

   TimeOutValue연결을 끊었다가 다시 SCSI 설정하여 세션 복구를 시도하기 전에 이니시에이터가 타겟의 응답을 기다리는 시간을 초 단위로 지정합니다. 다음 예와 같이 이 값은 600초의 제한 시간을 나타냅니다.



4. 새 구성 값을 적용하려면 시스템을 다시 시작해야 합니다.

   다시 시작하기 전에 볼륨에 대한 모든 쓰기 작업의 결과가 플러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 매핑한 스토리지 볼륨 디스크를 모두 오프라인으로 전환해야 합니다.

Linux i 설정 사용자 지정하기 SCSI

게이트웨이의 이니시에이터를 설정한 후에는 이니시에이터와 대상과의 연결이 끊기지 않도록 i SCSI 설정을 사용자 지정하는 것이 좋습니다. 다음과 같이 i SCSI timeout 값을 늘리면 응용 프로그램에서 시간이 오래 걸리는 쓰기 작업과 네트워크 중단과 같은 기타 일시적인 문제를 더 잘 처리할 수 있습니다.

> **Note**
>
> 다른 유형의 Linux인 경우, 명령이 약간 다를 수 있습니다. 다음은 Red Hat Linux의 예시입니다.

Linux i 설정을 사용자 지정하려면 SCSI

1. 요청이 대기하는 최대 시간을 늘립니다.

   a. `/etc/iscsi/iscsid.conf` 파일을 열고 다음 줄을 검색합니다.

   ```
   node.session.timeo.replacement_timeout = [replacement_timeout_value]
   node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
   node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
   ```

   b. 다음을 설정합니다.*[replacement_timeout_value]* 값은 **600** 0입니다.

   다음을 설정합니다.*[noop_out_interval_value]* 값: **~60**.

   다음을 설정합니다.*[noop_out_timeout_value]* 값: **~600**.

   세 값은 모두 초 단위입니다.

   > **Note**
   >
   > `iscsid.conf`는 게이트웨이를 검색하기 전에 설정해야 합니다. 게이트웨이를 이미 검색하였거나 대상에 로그인하였거나, 아니면 둘 다인 경우에는 다음 명령을 사용하여 검색 데이터베이스에서 항목을 삭제할 수 있습니다. 그 다음에는 다시 검색하거나 로그인하여 새 구성을 가져올 수 있습니다.
   >
   > ```
   > iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
   > ```

2. 각 응답에서 전송할 수 있는 데이터 양의 최대값을 늘립니다.

   a. `/etc/iscsi/iscsid.conf` 파일을 열고 다음 줄을 검색합니다.

   ```
   node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
   node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
   ```

```
node.conn[0].iscsi.MaxRecvDataSegmentLength
 = [replacement_segment_length_value]
```

b. 성능 향상을 위해 다음 값을 사용하는 것이 좋습니다. 백업 소프트웨어는 다른 값을 사용하도록 최적화되었을 수 있으므로 최상의 결과를 얻으려면 백업 소프트웨어 설명서를 참조하십시오.

다음을 설정합니다.*[replacement_first_burst_length_value]* 값 **262144** 또는 Linux OS 기본값 중 더 높은 값

다음을 설정합니다.*[replacement_max_burst_length_value]* 값과 Linux OS 기본값 중 더 높은 값 **1048576**

다음을 설정합니다.*[replacement_segment_length_value]* 값 = **262144** 또는 Linux OS 기본값 중 더 높은 값

> **Note**
>
> 다양한 i SCSI 설정을 사용하여 최상의 성능을 발휘하도록 백업 소프트웨어를 최적화할 수 있습니다. 이러한 파라미터의 값이 최상의 성능을 제공하는지 확인하려면 백업 소프트웨어 설명서를 참조하십시오.

3. 시스템을 다시 시작하여 새 구성 값이 적용되었는지 확인합니다.

다시 시작하기 전에 해당 테이프에 대한 모든 쓰기 작업의 결과가 플러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 테이프를 마운트 해제합니다.

Volume Gateway의 Linux 디스크 제한 시간 설정 사용자 지정

볼륨 게이트웨이를 사용하는 경우 이전 섹션에서 설명한 i 설정 외에도 다음과 같은 Linux 디스크 시간 제한 SCSI 설정을 사용자 지정할 수 있습니다.

Linux 디스크 제한 시간 설정을 사용자 지정하려면

1. 규칙 파일에서 디스크 제한 시간 값을 늘립니다.

a. RHEL5 이니시에이터를 사용하는 경우 `/etc/udev/rules.d/50-udev.rules` 파일을 열고 다음 줄을 찾으십시오.

```
ACTION=="add", SUBSYSTEM=="scsi" , SYSFS{type}=="0|7|14", \
```

```
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

이 규칙 파일은 RHEL 6개 또는 7개의 이니시에이터에는 존재하지 않으므로 다음 규칙을 사용하여 생성해야 합니다.

```
ACTION=="add", SUBSYSTEMS=="scsi" , ATTRS{model}=="Storage Gateway",
RUN+="/bin/sh -c 'echo [timeout] > /sys$$DEVPATH/timeout'"
```

RHEL6의 제한 시간 값을 수정하려면 다음 명령을 사용하고 앞에 표시된 코드 줄을 추가합니다.

```
sudo vim /etc/udev/rules.d/50-udev.rules
```

RHEL7의 제한 시간 값을 수정하려면 다음 명령을 사용하고 앞에 표시된 코드 줄을 추가합니다.

```
sudo su -c "echo 600 > /sys/block/[device name]/device/timeout"
```

b. 다음을 설정합니다.*[timeout]* 값은 ~입니다. **600**

이 값은 제한 시간 600초를 나타냅니다.

2. 시스템을 다시 시작하여 새 구성 값이 적용되었는지 확인합니다.

다시 시작하기 전에 해당 볼륨에 대한 모든 쓰기 작업의 결과가 플러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 스토리지 볼륨의 마운트를 해제해야 합니다.

3. 다음 명령을 사용하여 구성을 테스트할 수 있습니다.

```
udevadm test [PATH_TO_ISCSI_DEVICE]
```

이 명령은 i SCSI 기기에 적용되는 udev 규칙을 보여줍니다.

i 타겟에 대한 CHAP 인증 구성 SCSI

Storage Gateway는 챌린지-핸드셰이크 인증 프로토콜 () 을 사용하여 게이트웨이와 i SCSI 이니시에이터 간의 인증을 지원합니다. CHAP CHAPi SCSI 이니시에이터의 ID를 볼륨 및 디바이스 대상에 액세스할 수 있도록 인증된 것으로 정기적으로 확인하여 재생 공격으로부터 보호합니다. VTL

> **Note**
>
> CHAP구성은 선택 사항이지만 적극 권장됩니다.

CHAP설정하려면 Storage Gateway 콘솔과 대상에 연결하는 데 사용하는 SCSI 이니시에이터 소프트웨어에서 모두 구성해야 합니다. Storage Gateway는 이니시에이터가 대상을 인증하고 대상이 이니시에이터를 인증하는 상호 CHAP 방식을 사용합니다.

타겟을 상호 설정하려면 CHAP

1. CHAP에 설명된 대로 Storage Gateway 콘솔에서 구성합니다 Storage Gateway 콘솔에서 볼륨 타겟을 CHAP 구성하려면.
2. 클라이언트 이니시에이터 소프트웨어에서 CHAP 구성을 완료하십시오.
   - Windows CHAP 클라이언트에서 상호 구성을 구성하려면 을 참조하십시오Windows CHAP 클라이언트에서 상호 구성하기.
   - Red Hat Linux 클라이언트에서 상호 CHAP 설정을 하려면 을 참조하십시오Red Hat Linux CHAP 클라이언트에서 상호 설정하기.

Storage Gateway 콘솔에서 볼륨 타겟을 CHAP 구성하려면

이 절차에서는 볼륨에 읽고 쓰는 데 사용하는 비밀 키 두 개를 지정합니다. 이 동일한 키 두 개는 클라이언트 초기자를 구성하는 절차에서 사용합니다.

1. Storage Gateway 콘솔의 탐색 창에서 볼륨을 선택합니다.
2. [작업] 에서 [CHAP인증 구성] 을 선택합니다.
3. CHAP인증 구성 대화 상자에 요청된 정보를 제공합니다.
   a. 이니시에이터 이름에는 i SCSI 이니시에이터의 이름을 입력합니다. 이 이름은 Amazon i SCSI 공인 이름 (IQN) 이며 앞에 대상 이름이 `iqn.1997-05.com.amazon:` 붙습니다. 다음은 예입니다.

      ```
      iqn.1997-05.com.amazon:your-volume-name
      ```

      i SCSI 이니시에이터 소프트웨어를 사용하여 이니시에이터 이름을 찾을 수 있습니다. 예를 들어, Windows 클라이언트의 경우 이름은 i SCSI 이니시에이터의 구성 탭에 있는 값입니다. 자세한 내용은 Windows CHAP 클라이언트에서 상호 구성하기 단원을 참조하십시오.

> **Note**
>
> 이니시에이터 이름을 변경하려면 먼저 i SCSI 이니시에이터 소프트웨어를 CHAP 비활성화하고 이니시에이터 이름을 변경한 다음 새 이름으로 CHAP 활성화해야 합니다.

b. 이니시에이터를 인증하는 데 사용되는 암호에 요청된 암호를 입력합니다.

   이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 이니시에이터 (즉, Windows 클라이언트) 가 대상에 참여하기 위해 알아야 하는 비밀 키입니다. CHAP

c. 대상 인증에 사용되는 암호 (상호CHAP) 에는 요청된 암호를 입력합니다.

   이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 대상이 이니시에이터와 CHAP 함께 참여하기 위해 알아야 하는 비밀 키입니다.

> **Note**
>
> 대상을 인증하는 데 사용한 비밀 문구는 초기자 인증을 위한 비밀 문구와는 달라야 합니다.

d. 저장(Save)을 선택합니다.

4. 세부 정보 탭을 선택하고 i SCSI CHAP 인증이 true로 설정되었는지 확인합니다.

Windows CHAP 클라이언트에서 상호 구성하기

이 절차에서는 CHAP 콘솔에서 볼륨을 구성할 때 사용한 것과 동일한 키를 사용하여 Microsoft i SCSI 이니시에이터에서 구성합니다CHAP.

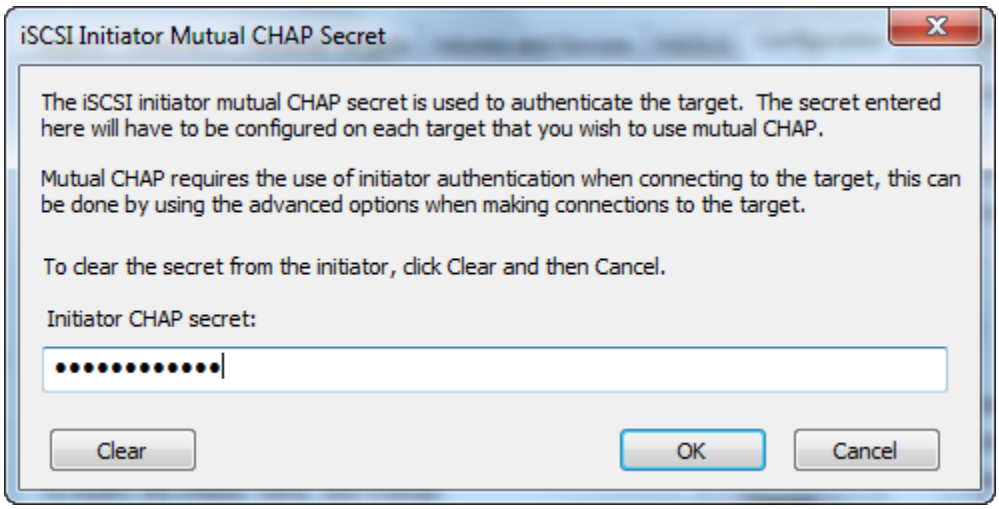
1. i SCSI 이니시에이터가 아직 시작되지 않은 경우 Windows 클라이언트 컴퓨터의 시작 메뉴에서 실행을 선택하고 를 입력한 **`iscsicpl.exe`** 다음 확인을 선택하여 프로그램을 실행합니다.
2. 이니시에이터 (즉, Windows 클라이언트) 의 상호 CHAP 구성을 구성합니다.

   a. 구성 탭을 선택합니다.

   > **Note**
   >
   > 이니시에이터 이름 값은 초기자 및 회사에 고유합니다. 앞에 표시된 이름은 Storage Gateway 콘솔의 CHAP인증 구성 대화 상자에서 사용한 값입니다.
   > 예시 이미지에 표시된 이름은 데모용일 뿐입니다.

   b. 선택합니다 CHAP.

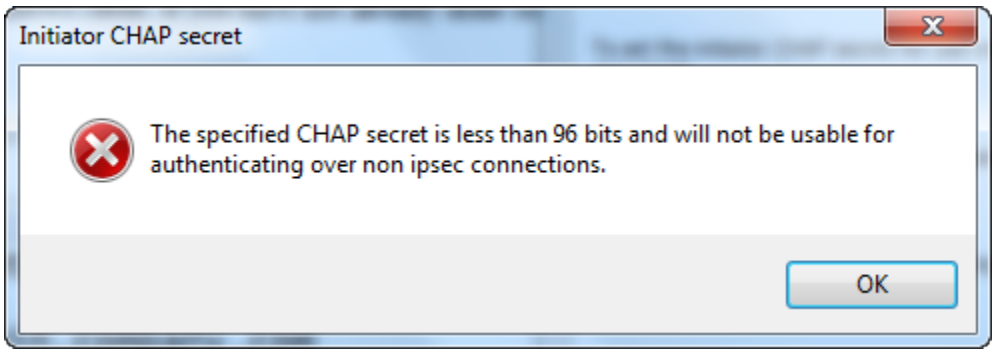
   c. i SCSI 이니시에이터 상호 칩 암호 대화 상자에 상호 CHAP 암호 값을 입력합니다.



   이 대화 상자에서 초기자(Windows 클라이언트)가 대상(스토리지 볼륨)을 인증하는 데 사용하는 비밀 문구를 입력합니다. 이 비밀 문구를 사용하면 대상이 초기자에(서) 읽고 쓸 수 있습니다. 이 암호는 인증 구성 CHAP 대화 상자의 대상 인증에 사용되는 암호 (상호CHAP) 상자에 입력한 암호와 동일합니다. 자세한 내용은 i 타겟에 대한 CHAP 인증 구성 SCSI 단원을 참조하십시오.

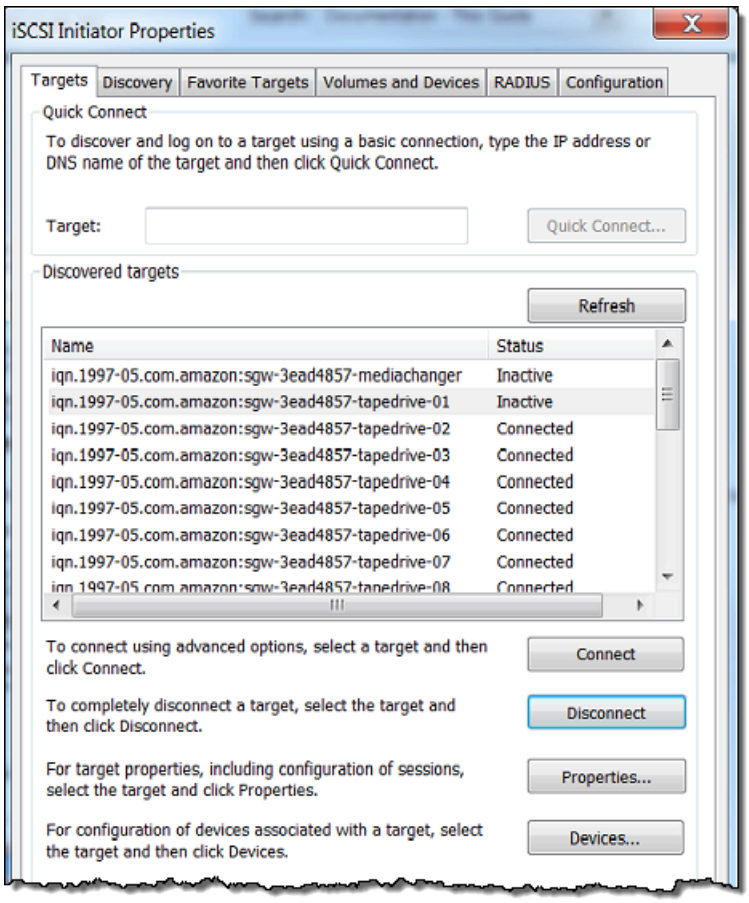
   d. 입력한 키가 12자 미만 또는 16자 이상인 경우 이니시에이터 CHAP 암호 오류 대화 상자가 나타납니다.

   확인을 선택한 후 키를 다시 입력합니다.



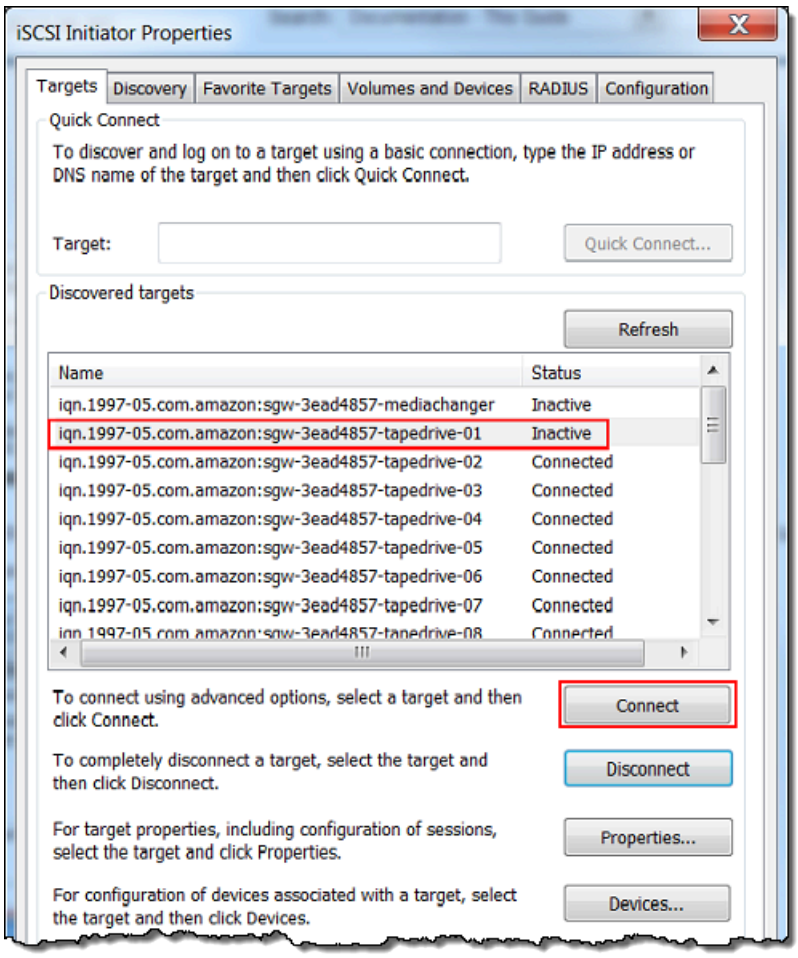
3. 이니시에이터 암호로 대상을 구성하여 상호 구성을 완료하십시오. CHAP

   a. 대상 탭을 선택합니다.

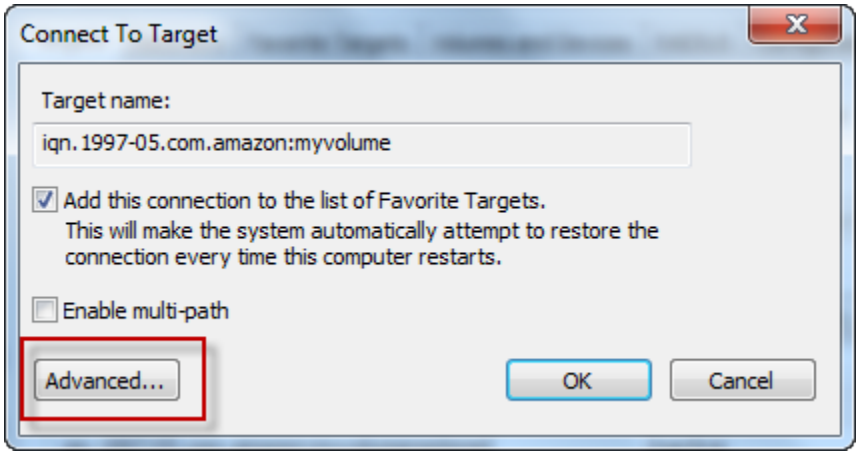


   b. 구성하려는 대상이 현재 CHAP 연결되어 있는 경우 대상을 선택하고 연결 끊기를 선택하여 연결을 끊습니다.

   c. 구성할 대상을 선택한 다음 Connect를 선택합니다. CHAP



d. Connect to Target(대상으로 연결) 대화 상자에서 고급을 선택합니다.



e. 고급 설정 대화 상자에서 구성합니다CHAP.

i. CHAP로그온 활성화를 선택합니다.

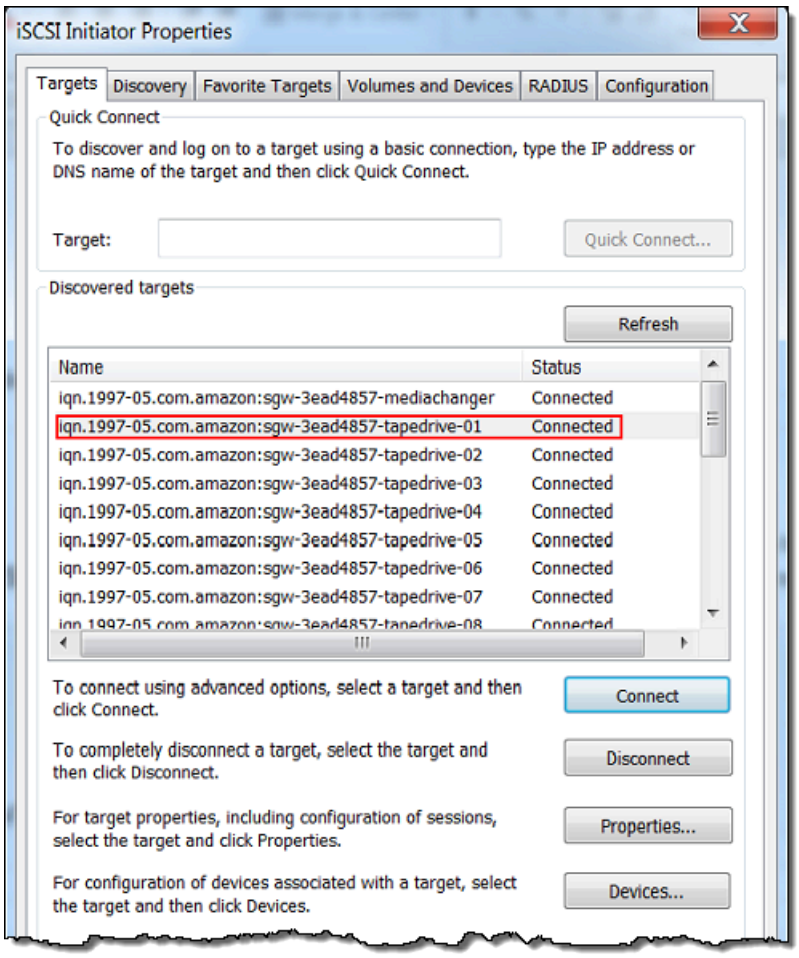
ii. 이니시에이터를 인증하는 데 필요한 암호를 입력합니다. 이 암호는 CHAP인증 구성 대화 상자의 이니시에이터 인증에 사용되는 암호 상자에 입력한 암호와 동일합니다. 자세한 내용은 i 타겟에 대한 CHAP 인증 구성 SCSI 단원을 참조하십시오.

iii. Perform mutual authentication(상호 인증 수행)을 선택합니다.

iv. 변경 사항을 적용하려면 확인을 선택합니다.

f. Connect to Target(대상으로 연결) 대화 상자에서 확인을 선택합니다.

4. 정확한 비밀 키를 입력하면 대상이 연결 상태 상태로 표시됩니다.



Red Hat Linux CHAP 클라이언트에서 상호 설정하기

이 절차에서는 Storage Gateway CHAP 콘솔에서 볼륨을 구성할 때 사용한 것과 동일한 키를 사용하여 Linux i SCSI 이니시에이터에서 구성합니다CHAP.

1. i SCSI 데몬이 실행 중이고 대상에 이미 연결되어 있는지 확인하십시오. 이 두 작업을 완료하지 않은 경우, Red Hat Enterprise Linux 클라이언트에 연결 섹션을 참조하세요.

2. 구성하려는 대상의 기존 구성을 모두 연결 해제하고 제거합니다. CHAP

   a. 대상 이름을 찾고 그것이 정의된 구성인지 확인하려면 다음 명령을 사용하여 저장된 구성의 목록을 조회합니다.

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. 대상에서 연결을 해제합니다.

   다음 명령은 Amazon i SCSI 정규화된 이름 (IQN) 에 정의된 이름의 **myvolume** 대상과의 연결을 끊습니다. 상황에 따라 IQN 필요에 따라 대상 이름을 변경하십시오.

   ```
   sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1
    iqn.1997-05.com.amazon:myvolume
   ```

   c. 대상에 대한 구성을 제거합니다.

   다음 명령은 **myvolume** 대상에 대한 구성을 제거합니다.

   ```
   sudo /sbin/iscsiadm --mode node --op delete --targetname
    iqn.1997-05.com.amazon:myvolume
   ```

3. i SCSI 구성 파일을 편집하여 CHAP 활성화합니다.

   a. 초기자(즉 사용 중인 클라이언트)의 이름을 가져옵니다.

   다음 명령은 `/etc/iscsi/initiatorname.iscsi` 파일에서 초기자 이름을 가져옵니다.

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

   이 명령의 출력은 다음과 같습니다.

   ```
   InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
   ```

   b. `/etc/iscsi/iscsid.conf` 파일을 엽니다.

   c. 파일에서 다음 줄의 주석을 제거하고 올바른 값을 지정하십시오.*username*, *password*, *username_in*, 및 *password_in*.

   ```
   node.session.auth.authmethod = CHAP
   node.session.auth.username = username
   node.session.auth.password = password
   node.session.auth.username_in = username_in
   ```

```
node.session.auth.password_in = password_in
```

지정할 값에 대한 지침은 다음 표를 참조하십시오.

구성 설정	값
username	이 절차의 이전 단계에서 찾은 초기자 이름. 그 값은 IQN으로 시작합니다. 예를 들어, **iqn.1994-05.com.redhat:8e89b27b5b8** 는 유효합니다.*username* 값.
password	초기자(사용 중인 클라이언트)가 볼륨과 통신할 때 초기자를 인증하는 데 사용하는 비밀 키
username_in	대상 IQN 볼륨의 값입니다. 이 값은 IQN으로 시작하여 대상 이름으로 끝납니다. 예를 들어, **iqn.1997-05.com.amazon:myvolume** 는 유효합니다.*username_in* 값.
password_in	대상(볼륨)이 초기자와 통신할 때 대상을 인증하는 데 사용하는 비밀 키

d. 구성 파일에 변경 사항을 저장한 후 파일을 닫습니다.

4. 대상을 검색하여 로그인합니다. 이렇게 하려면 Red Hat 엔터프라이즈 Linux 클라이언트에 연결에 설명된 단계를 수행하세요.

Storage AWS Direct Connect Gateway와 함께 사용

AWS Direct Connect 내부 네트워크를 Amazon Web Services 클라우드에 연결합니다. Storage AWS Direct Connect Gateway와 함께 사용하면 처리량이 높은 워크로드 요구 사항에 맞는 연결을 생성하여 온프레미스 게이트웨이와 간에 전용 네트워크 연결을 제공할 수 있습니다. AWS

Storage Gateway는 퍼블릭 엔드포인트를 사용합니다. AWS Direct Connect 연결이 설정되면 퍼블릭 가상 인터페이스를 생성하여 트래픽이 Storage Gateway 엔드포인트로 라우팅되도록 할 수 있습니다. 퍼블릭 가상 인터페이스는 네트워크 경로에서 인터넷 서비스 제공업체를 우회합니다. Storage Gateway 서비스 퍼블릭 엔드포인트는 AWS Direct Connect 위치와 동일한 AWS 지역에 있거나 다른 AWS 지역에 있을 수 있습니다.

다음 그림은 Storage Gateway와 함께 AWS Direct Connect 작동하는 방식의 예를 보여줍니다. Storage Gateway가 AWS 직접 연결을 사용하여 클라우드에 연결된 것을 보여주는 네트워크 아키텍처

다음 절차에서는 생성된 게이트웨이가 제대로 작동 중이라고 가정합니다.

Storage AWS Direct Connect Gateway와 함께 사용하려면

1. 온프레미스 데이터 센터와 Storage Gateway 엔드포인트 간의 AWS Direct Connect 연결을 생성하고 설정합니다. 연결 생성 방법에 대한 자세한 내용은AWS Direct Connect 사용 설명서에서 AWS Direct Connect시작하기를 참조하세요.
2. 온프레미스 Storage Gateway 어플라이언스를 AWS Direct Connect 라우터에 연결합니다.
3. 퍼블릭 가상 인터페이스를 생성하고 이에 따라 온프레미스 라우터를 구성합니다. Direct Connect를 사용하는 경우에도 VPC 엔드포인트는 를 사용하여 생성해야 합니다. HAProxy 자세한 내용은 AWS Direct Connect 사용 설명서에서 가상 인터페이스 생성을 참조하세요.

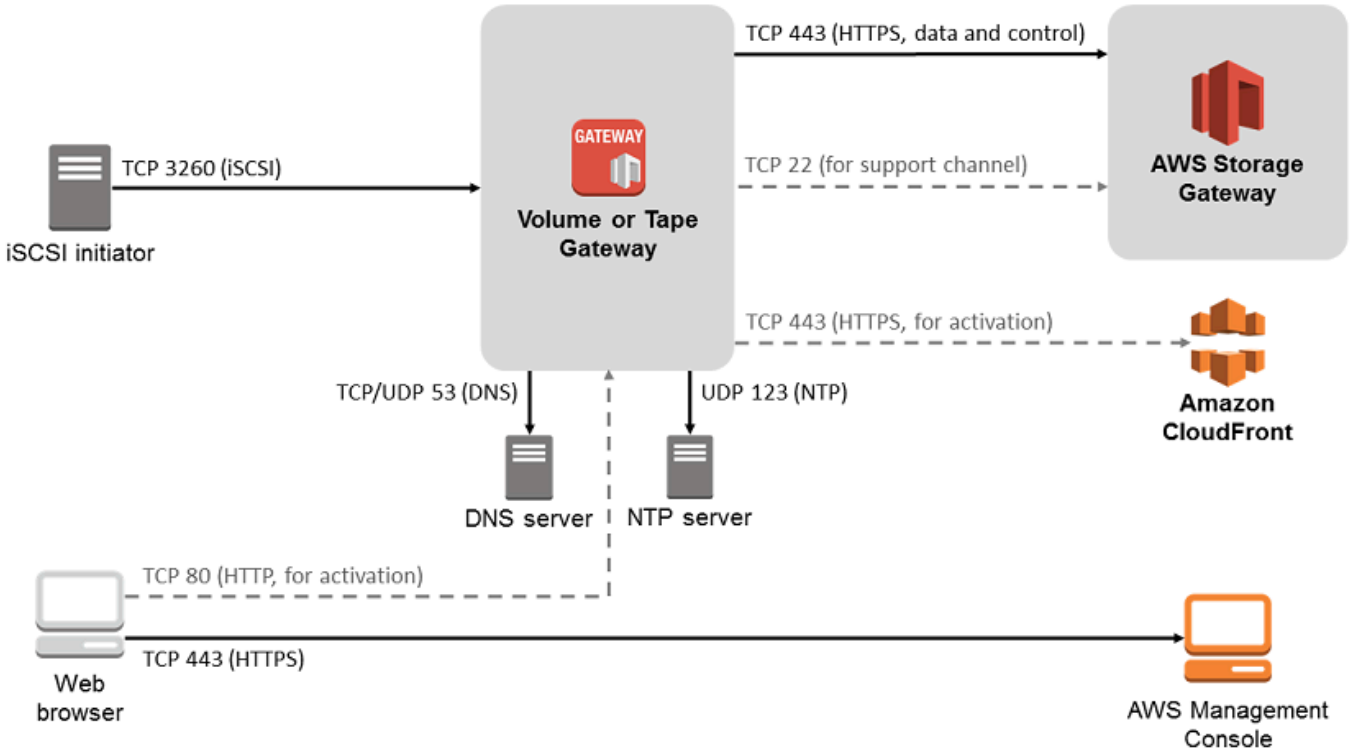
에 대한 자세한 내용은 AWS Direct ConnectAWS Direct Connect무엇입니까를 참조하십시오. AWS Direct Connect 사용 설명서에서.

볼륨 게이트웨이의 네트워크 포트 요구 사항

Storage Gateway가 작동하려면 다음 포트가 필요합니다. 일부 포트는 모든 게이트웨이 유형에 공통적으로 필요한 포트입니다. 그 밖에 특정 유형의 게이트웨이에 필요한 포트도 있습니다. 이 섹션에서는 Volume Gateway에 필요한 포트의 그림과 목록을 확인할 수 있습니다.

Volume Gateway

다음은 Volume Gateway 게이트웨이 작동을 위해 열어야 하는 모든 포트를 보여주는 그림입니다.



다음 포트는 모든 게이트웨이 유형에 공통적으로 필요한 포트입니다.

From	To	프로토콜	Port	용도	
Storage Gateway VM	AWS	전송 제어 프로토콜 (TCP)	443 () HTTPS	Storage Gateway 아웃바운드 가상 머신에서 AWS 서비스 엔드포인트로의 통신용 서비스 엔드포인트에 대한 자세한 내용은 방화벽과 AWS Storage Gateway 라우터를 통한 액세스 허용	

From	To	프로토콜	Port	용도	
				단원을 참조하십시오.	

From	To	프로토콜	Port	용도	
웹 브라우저	Storage Gateway VM	TCP	80 () HTTP	Storage Gateway 활성화 키를 가져올 때 로컬 시스템에서 사용합니다. 포트 80은 Storage Gateway 어플라이언스 활성화 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, 콘솔에 연결하	

From	To	프로토콜	Port	용도	
				는 호스트가 게이트웨이의 포트 80에 액세스할 수 있어야 합니다.	
Storage Gateway VM	도메인 네임 서비스 (DNS) 서버	사용자 데이터그램 프로토콜 (UDP)/UDP	53 () DNS	Storage Gateway 가상 머신과 DNS 서버 간 통신용	
Storage Gateway VM	AWS	TCP	22(지원 채널)	게이트웨이 문제를 해결하는 데 도움이 되는 게이트웨이에 액세스할 수 있습니다. AWS Support 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다.	

From	To	프로토콜	Port	용도	
Storage Gateway VM	네트워크 타임 프로토콜 (NTP) 서버	UDP	123 () NTP	로컬 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다. Storage Gateway 가상 머신은 다음 NTP 서버를 사용하도록 구성되어 있습니다. • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org	
Storage Gateway 하드웨어 어플라이언스	하이퍼텍스트 전송 프로토콜 (HTTP) 프록시	TCP	8080 () HTTP	정품 인증에 잠시 필요합니다.	

공통 포트 외에 Volume Gateway에는 다음 포트가 필요합니다.

From	To	프로토콜	Port	용도	
i 이니시에이터 SCSI	Storage Gateway VM	TCP	3260 (i) SCSI	로컬 시스템을 통해 게이트웨이에 노출된 i SCSI 타겟에 연결합니다.	

게이트웨이에 연결

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 관리 콘솔에서 Amazon EC2 인스턴스의 IP 주소를 가져올 수도 있습니다. 게이트웨이의 IP 주소를 얻는 방법은 다음 중 하나를 참조하십시오.

- VMware호스트: 를 사용하여 게이트웨이 로컬 콘솔에 액세스 VMware ESXi
- HyperV 호스트: Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스
- Linux 커널 기반 가상 머신 (KVM) 호스트: Linux를 사용하여 게이트웨이 로컬 콘솔에 액세스 KVM
- EC2호스트: 아마존 EC2 호스트에서 IP 주소 가져오기

IP 주소를 찾았으면 적어 둡니다. 그런 다음 Storage Gateway 콘솔로 돌아가서 콘솔에 IP 주소를 입력합니다.

아마존 EC2 호스트에서 IP 주소 가져오기

게이트웨이가 배포된 Amazon EC2 인스턴스의 IP 주소를 가져오려면 EC2 인스턴스의 로컬 콘솔에 로그인하십시오. 그런 다음 콘솔 페이지 상단에서 IP 주소를 얻습니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 단원을 참조하십시오.

Amazon EC2 관리 콘솔에서도 IP 주소를 가져올 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. 에서 Amazon EC2 콘솔을 엽니다 https://console.aws.amazon.com/ec2/.
2. 탐색 창에서 [Instances] 를 선택한 다음 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. 에서 Amazon EC2 콘솔을 엽니다 https://console.aws.amazon.com/ec2/.
2. 탐색 창에서 [Instances] 를 선택한 다음 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.
4. 게이트웨이가 활성화되면 방금 활성화한 게이트웨이를 선택한 다음 하단 패널에서 VTL디바이스 탭을 선택합니다.
5. 모든 VTL 디바이스의 이름을 확인하세요.
6. 각 대상에 대해 다음 명령을 실행하여 대상을 구성합니다.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```
7. 각 대상에 대해 다음 명령을 실행하여 로그인합니다.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   이제 게이트웨이는 EC2 인스턴스의 엘라스틱 IP 주소를 사용하여 연결되었습니다.

Storage Gateway 리소스 및 리소스에 대한 이해 IDs

Storage Gateway에서 기본 리소스는 게이트웨이이지만 다른 리소스 유형으로는 볼륨, 가상 테이프, iSCSI 타겟, vtl 디바이스 등이 있습니다. 이 유형들은 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

다음 표와 같이 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름 (ARNs) 이 연결되어 있습니다.

리소스 유형	ARN형식
게이트웨이 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`*
볼륨 ARN	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/volume/`*`volume-id`*
타겟 ARN (iSCSI 타겟)	`arn:aws:storagegateway:` *`region`*`:`*`account-id`* `:gateway/` *`gateway-id`* `/target/`*`iSCSItarget`*

Storage Gateway는 EC2 인스턴스, EBS 볼륨 및 스냅샷의 사용도 지원합니다. 이러한 리소스는 Storage Gateway에서 사용되는 Amazon EC2 리소스입니다.

리소스 관련 작업 IDs

리소스를 생성할 때 Storage Gateway에서는 리소스에 고유 리소스 ID를 할당합니다. 이 리소스 ID는 리소스의 일부입니다ARN. 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. 볼륨 ID가 `vol-3344CCDD`와 같은 형식이라면 여기에서 `vol`은 볼륨의 리소스 식별자입니다.

가상 테이프의 경우, 바코드 ID 앞에 접두사 문자를 최대 네 개까지 추가할 수 있어 테이프 체계화에 도움이 됩니다.

Storage Gateway IDs 리소스는 대문자입니다. 하지만 IDs Amazon에서 이러한 리소스를 사용하는 경우 EC2 API Amazon은 리소스가 IDs 소문자로 EC2 표시될 것으로 예상합니다. 와 함께 사용하려면 리소스 ID를 소문자로 변경해야 합니다. EC2 API 예를 들어 Storage Gateway에서 볼륨의 ID는 `vol-1122AABB`일 수 있습니다. 이 ID를 와 함께 사용하는 EC2 API 경우 이 ID를 로 변경해야 합니다. `vol-1122aabb` 그렇지 않으면 예상대로 작동하지 EC2 API 않을 수 있습니다.

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 단원을 참조하십시오.

태그를 지정한 가상 테이프를 아카이브하는 경우, 테이프는 아카이브에서 자체 태그를 유지합니다. 이와 마찬가지로 아카이브에서 다른 게이트웨이로 테이프를 가져오는 경우, 태그는 새 게이트웨이에 유지됩니다.

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 사용할 수 있는 문자는 UTF -8자의 문자와 숫자, 공백, 특수 문자 + - =. _:/및 @입니다.

태그 작업

Storage Gateway 콘솔, Storage Gateway 또는 Storage Gateway API 명령줄 인터페이스 (CLI) 를 사용하여 태그를 사용할 수 있습니다. 다음 절차에서는 콘솔에서 태그를 추가, 편집, 삭제하는 방법을 안내합니다.

태그를 추가하려면

1. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 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. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 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. https://console.aws.amazon.com/storagegateway/집에서 Storage Gateway 콘솔을 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.

AWS Storage Gateway용 오픈 소스 구성 요소 작업

이 섹션에서는 Storage Gateway 기능을 제공하기 위해 사용하는 타사 도구 및 라이센스에 대해 설명합니다.

AWS Storage Gateway 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드는 다음 위치에서 다운로드할 수 있습니다.

- 에 배포된 게이트웨이의 VMware ESXi 경우 sources.tar 다운로드
- Microsoft Hyper-V에 배포된 게이트웨이의 경우 sources_hyperv.tar을 다운로드합니다.
- Linux 커널 기반 가상 머신 (KVM) 에 배포된 게이트웨이의 경우 sources_.tar를 다운로드하십시오. KVM

이 제품에는 오픈 툴킷 (http://www.openssl.org/) 에서 사용하기 위해 오픈 SSL 프로젝트에서 개발한 소프트웨어가 포함되어 있습니다. SSL 모든 종속 타사 도구에 대한 관련 라이선스는 타사 라이선스를 참조하십시오.

AWS Storage Gateway 할당량

이 주제에서는 Storage Gateway의 볼륨 및 테이프 할당량, 구성 및 성능 한도에 대한 정보를 확인할 수 있습니다.

주제

- 볼륨 할당량
- 게이트웨이에 권장되는 로컬 디스크 크기

볼륨 할당량

다음 표에는 볼륨 할당량이 나와 있습니다.

설명	캐싱 볼륨	저장 볼륨
볼륨의 최대 크기 **Note** 크기가 16TiB를 초과하는 캐시된 볼륨에서 스냅샷을 생성하는 경우, 이를 Storage Gateway 볼륨으로 복원할 수 있지만 Amazon Elastic 블록 스토어 (EBSAmazon) 볼륨에는 복원할 수 없습니다.	32TiB	16TiB
게이트웨이당 최대 볼륨 수	32	32
한 게이트웨이에 있는 모든 볼륨의 총 크기	1,024TiB	512TiB

게이트웨이에 권장되는 로컬 디스크 크기

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)	업로드 버퍼 (최소값)	업로드 버퍼 (최대값)	필요한 다른 로컬 디스크
캐시된 볼륨 게이트웨이	150GiB	64TiB	150GiB	2TiB	—
저장된 볼륨 게이트웨이	—	—	150GiB	2TiB	저장 볼륨의 경우 1개 이상

> **Note**
>
> 캐시 및 업로드 버퍼에 대해 하나 이상의 로컬 드라이브를 최대 용량까지 구성할 수 있습니다. 기존 게이트웨이에 캐시 또는 업로드 버퍼를 추가할 때는 호스트 (하이퍼바이저 또는 Amazon EC2 인스턴스) 에 새 디스크를 생성하는 것이 중요합니다. 기존 디스크가 이전에 캐시 또는 업로드 버퍼로 할당되었던 경우, 디스크 크기를 변경하지 마십시오.

APIStorage Gateway에 대한 참조

콘솔을 사용하는 것 외에도 를 사용하여 AWS Storage Gateway API 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**
>
> 를 사용하여 애플리케이션을 개발할 AWS SDKs 때도 를 사용할 수 AWS Storage Gateway있습니다. Java의 AWS SDKs 경우. NET기본 AWS Storage Gateway API 요소를 PHP 래핑하여 프로그래밍 작업을 단순화합니다. SDK라이브러리 다운로드에 대한 자세한 내용은 샘플 코드 라이브러리를 참조하십시오.

주제

Storage Gateway 필수 요청 헤더

이 섹션에서는 모든 POST 요청과 함께 Storage Gateway에 전송해야 하는 필수 헤더에 대해 설명합니다. HTTP헤더를 포함하여 호출하려는 작업, 요청 날짜, 요청 발신자의 승인을 나타내는 정보 등 요청의 주요 정보를 식별할 수 있습니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음 예제는 작업에 사용되는 헤더를 보여줍니다. ActivateGateway

```
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
```

Storage Gateway에 대한 POST 요청에 포함해야 하는 헤더는 다음과 같습니다. “x-amz”로 시작하는 아래 헤더는 특정 헤더입니다. AWS나열된 다른 모든 헤더는 트랜잭션에 사용되는 공통 헤더입니다. HTTP

헤더	설명
`Authorization`	권한 부여 헤더는 Storage Gateway가 해당 요청이 요청자에게 유효한 작업인지 판단할 수 있게 해주는 요청에 대한 몇 가지 정보를 포함합니다. 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` 위 구문에서는 년, 월 YourAccessKey, 일 (yyyymmdd), 지역 및 시간을 지정합니다. CalculatedSignature 승인 헤더의 형식은 V4 서명 프로세스의 요구 사항에 따라 달라집니다. AWS 서명 관련 세부 정보는 요청에 서명하기 단원에 나와 있습니다.
`Content-Type`	`application/x-amz-json-1.1` 을 Storage Gateway에 대한 모든 요청의 콘텐츠 유형으로 사용합니다. `Content-Type: application/x-amz-json-1.1`
`Host`	호스트 헤더를 사용하여 요청을 전송하는 Storage Gateway 엔드포인트를 지정합니다. 예를 들어, `storagegateway.us-east-2.amazonaws.com` 은 미국 동부(오하이오) 리전의 엔드포인트입니다. Storage Gateway에 사용할 수 있는 엔드포인트에 대한 자세한 내용은 AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

헤더	설명
	`Host: storagegateway. region.amazonaws.com`
`x-amz-date`	HTTPDate헤더 또는 헤더에 타임스탬프를 제공해야 합니다. AWS `x-amz-date` (일부 HTTP 클라이언트 라이브러리에서는 `Date` 헤더를 설정할 수 없습니다.) `x-amz-date` 헤더가 있으면 Storage Gateway는 요청 인증 중 모든 `Date` 헤더를 무시합니다. `x-amz-date` 형식은 YYYYMMDD 'T' Z HHMMSS '형식의 ISO86 01 Basic이어야 합니다. `Date`및 `x-amz-date` 헤더를 모두 사용하는 경우 Date 헤더의 형식은 ISO86 01이 아니어도 됩니다. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	이 헤더는 요청하려는 작업 API 및 의 버전을 지정합니다. 대상 헤더 값은 API 버전과 API 이름을 연결하여 구성되며 형식은 다음과 같습니다. `x-amz-target: StorageGateway_ APIversion .operationName` operationName값 (예: "ActivateGateway“) 은 API 목록에서 찾을 수 있습니다. APIStorage Gateway에 대한 참조

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 보안 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

  HTTP요청을 표준 형식으로 재배열하십시오. 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 의 두 입력 문자열을 허용하는 암호화 해시 함수를 사용하여 요청에 대한 서명을 만듭니다. 파생된 키는 보안 액세스 키로 시작하여 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드 () 를 생성하여 계산됩니다. HMACs

서명 계산 예시

다음 예제에서는 서명을 만드는 방법에 대한 세부 정보를 안내합니다. ListGateways 이 예시는 서명 계산 방법을 점검하기 위한 참조로 사용할 수 있습니다. 다른 참조 계산은 Amazon Web Services 글로서리의 서명 버전 4 테스트 제품군에 포함되어 있습니다.

이 예시에서는 다음과 같이 가정합니다.

- 요청의 타임스탬프는 “2012년 9월 10일 월요일 00:00:00 “입니다. GMT
- 엔드포인트는 미국 동부(오하이오) 리전입니다.

일반 요청 구문 (본문 포함) 은 JSON 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
```

정규 요청의 마지막 줄은 요청 본문의 해시입니다. 또한 정규 요청에서 비어 있는 세 번째 줄에 주의해야 합니다. 이 API (또는 Storage GatewayAPIs) 에 대한 쿼리 매개 변수가 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")
```

보안 액세스 키인 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY를 사용하는 경우, 계산된 서명은 다음과 같습니다.

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

마지막 단계는 Authorization 헤더를 생성하는 것입니다. 데모 액세스 키의 AKIAIOSFODNN7EXAMPLE 경우 헤더 (가독성을 위해 줄 바꿈을 추가함) 는 다음과 같습니다.

```
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 요청 서명에 문제가 있는 경우 모든 API 응답에서 오류 `InvalidSignatureException` 예외가 반환됩니다. 그러나 작업 오류 `ActivationKeyInvalid` 코드는 에 대해서만 반환됩니다 ActivateGatewayAPI.

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 작업에서 오류 응답을 반환하는 경우 응답 본문에는 이러한 예외 중 하나가 포함됩니다. `InternalServerError`와 `InvalidGatewayRequestException`은 특정 작업 오류 코드를 부여하는 작업 오류 코드(작업 오류 코드) 메시지 코드 중 하나를 반환합니다.

예외	메시지	HTTP상태 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

예외	메시지	HTTP상태 코드
InvalidAction	요청된 동작 또는 작업이 유효하지 않습니다.	400 잘못된 요청
InvalidClientTokenId	제공된 X.509 인증서 또는 AWS 액세스 키 ID는 당사 기록에 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 키와 서명 방법을 확인하세요.	400 잘못된 요청
MissingAction	요청에서 작업 또는 작업 파라미터가 누락되었습니다.	400 잘못된 요청
MissingAuthenticationToken	요청에는 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
SerializationException	직렬화 도중에 오류가 발생했습니다. JSON페이로드의 형식이 올바른지 확인하세요.	400 잘못된 요청
ServiceUnavailable	서버의 일시적 장애로 인해 요청이 실패했습니다.	[503 Service Unavailable]
SubscriptionRequiredException	AWS 액세스 키 ID를 사용하려면 서비스에 가입해야 합니다.	400 잘못된 요청
ThrottlingException	속도를 초과하였습니다.	400 잘못된 요청

예외	메시지	HTTP상태 코드
TooManyRequests	요청이 너무 많음.	429 요청이 너무 많음
UnknownOperationException	알 수 없는 작업을 지정하였습니다. 유효한 작업은 Storage Gateway의 작업에 나열되어 있습니다.	400 잘못된 요청
UnrecognizedClientException	요청에 포함된 보안 토큰이 유효하지 않습니다.	400 잘못된 요청
ValidationException	입력 파라미터의 값이 잘못되었거나 범위를 벗어났습니다.	400 잘못된 요청

작업 오류 코드

다음 표에는 작업 오류 코드와 해당 코드를 반환할 수 APIs 있는 AWS Storage Gateway 작업 오류 코드 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
ActivationKeyInvalid	지정한 정품 인증 키가 유효하지 않습니다.	ActivateGateway
ActivationKeyNotFound	지정한 정품 인증 키를 찾을 수 없습니다.	ActivateGateway
BandwidthThrottleScheduleNotFound	지정한 대역폭 제한을 찾을 수 없습니다.	DeleteBandwidthRateLimit
CannotExportSnapshot	지정한 스냅샷을 내보낼 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
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
DiskSizeLessThanVolumeSize	지정한 디스크 크기가 볼륨 크기보다 작습니다.	CreateStorediSCSIVolume
DuplicateCertificateInfo	지정한 인증서 정보가 중복되어 있습니다.	ActivateGateway

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	지정된 내용이 LUN 올바르지 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.

- 콘텐츠 유형: 애플리케이션/ -1.1 x-amz-json
- 적절한 또는 상태 코드 4xx 5xx HTTP

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 표에서는 위 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__타입

예외의 예외 중 하나.

유형: 문자열

오류

API특정 오류 세부 정보가 들어 있습니다. 일반적인 오류 (즉, 특정 오류가 아닌 경우API) 에는 이 오류 정보가 표시되지 않습니다.

유형: 컬렉션

errorCode

작업 오류 코드 중 하나입니다 .

유형: 문자열

errorDetails

이 필드는 최신 버전의 에서는 사용되지 않습니다API.

유형: 문자열

message

작업 오류 코드 메시지 중 하나입니다.

유형: 문자열

오류 응답 예시

를 사용하고 존재하지 않는 게이트웨이 ARN 요청 입력을 지정하면 다음 JSON 본문이 반환됩니다. DescribeStoredi SCSIVolumes API

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

Storage Gateway에서 요청과 함께 전송된 서명과 일치하지 않는 서명을 계산하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway의 작업

Storage Gateway 작업 목록은 AWS Storage Gateway API참조 자료의 작업을 참조하십시오.

Volume Gateway 사용 설명서의 문서 기록

- API버전: 2013-06-30
- 최신 설명서 업데이트: 2020년 11월 24일

다음 표에서는 2018년 4월 이후AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 피드를 구독하면 이 설명서의 업데이트에 대한 알림을 받을 수 있습니다. RSS

변경 사항	설명	날짜
유지 관리 업데이트를 켜거나 끄는 옵션이 추가되었습니다.	Storage Gateway는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능, 보안 문제 해결, 새로운 기능에 대한 액세스 등이 포함될 수 있는 정기적인 유지 관리 업데이트를 받습니다. 이제 배포의 각 개별 게이트웨이에 대해 이러한 업데이트를 켜거나 끄도록 설정을 구성할 수 있습니다. 자세한 내용은 콘솔을 사용하여 게이트웨이 업데이트 관리를 참조하십시오. AWS Storage Gateway	2024년 6월 6일
Snowball Edge의 테이프 게이트웨이 지원이 중단되었습니다.	더 이상 Snowball Edge 디바이스에서 테이프 게이트웨이를 호스팅할 수 없습니다.	2024년 3월 14일
타사 애플리케이션을 사용하여 게이트웨이 설정을 테스트하기 위한 지침이 업데이트됨	타사 애플리케이션을 사용하여 게이트웨이 설정을 테스트하는 지침에 진행 중인 백업 작업 중에 게이트웨이가 다시 시작될 때 예상되는 동작이 설명되어 있습니다. 자세한 내용은 를 참조하십시오.	2023년 10월 24일

권장 CloudWatch 경보가 업데이트되었습니다.	이제 이 CloudWatch `HealthNotifications` 경보는 모든 게이트웨이 유형 및 호스트 플랫폼에 적용되고 권장됩니다. `HealthNotifications` 및 `AvailabilityNotifications` 에 대한 권장 구성 설정도 업데이트되었습니다. 자세한 내용은 경보 참조하십시오.	2023년 10월 2일
Tape Gateway와 Volume Gateway 사용 설명서가 분리됨	Tape Gateway와 Volume Gateway 유형에 대한 정보를 모두 포함하고 있던 Storage Gateway 사용 설명서가 Tape Gateway 사용 설명서와 Volume Gateway 사용 설명서로 분리되어, 각 설명서에 한 가지 게이트웨이 유형에 대한 정보만 포함되어 있습니다. 자세한 내용은 Tape Gateway 사용 설명서 및 Volume Gateway 사용 설명서를 참조하세요.	2022년 3월 23일
게이트웨이 생성 절차가 업데이트됨	Storage Gateway 콘솔을 사용하여 모든 게이트웨이 유형을 생성하는 절차가 업데이트되었습니다. 자세한 내용은 게이트웨이 생성을 참조하세요.	2022년 1월 18일

새 테이프 인터페이스	AWS Storage Gateway 콘솔의 테이프 개요 페이지가 새로운 검색 및 필터링 기능으로 업데이트되었습니다. 새로운 기능을 설명하도록 이 설명서의 모든 관련 절차가 업데이트되었습니다. 자세한 내용은 Tape Gateway 관리를 참조하세요.	2021년 9월 23일
테이프 게이트웨이용 Quest NetVault Backup 13 지원	테이프 게이트웨이는 이제 마이크로소프트 윈도우 서버 2012 R2 또는 마이크로소프트 윈도우 서버 2016에서 실행되는 Quest NetVault Backup 13을 지원합니다. 자세한 내용은 Quest NetVault Backup을 사용하여 설정 테스트를 참조하십시오.	2021년 8월 22일
Tape Gateway 및 Volume Gateway 설명서에서 S3 File Gateway 주제가 제거됨	각 게이트웨이 유형을 설정하는 고객이 Tape Gateway 및 Volume Gateway 사용 설명서를 더 쉽게 따라할 수 있도록 일부 불필요한 주제가 제거되었습니다.	2021년 7월 21일
윈도우 및 리눅스의 테이프 게이트웨이용 IBM 스펙트럼 프로텍트 8.1.10 지원	테이프 게이트웨이는 이제 Microsoft Windows Server 및 Linux에서 실행되는 IBM 스펙트럼 보호 버전 8.1.10을 지원합니다. 자세한 내용은 Spectrum Protect를 사용하여 IBM 설정 테스트를 참조하십시오.	2020년 11월 24일

연방 RAMP 규정 준수	Storage Gateway는 이제 RAMP 연준을 준수합니다. 자세한 내용은 Storage Gateway에 대한 규정 준수 검증을 참조하세요.	2020년 11월 24일
일정 기반 대역폭 조절	Storage Gateway에서 이제 Tape Gateway 및 Volume Gateway에 대해 일정 기반 대역폭 조절을 지원합니다. 자세한 내용은 Storage Gateway 콘솔을 사용한 대역폭 조절 예약을 참조하세요.	2020년 11월 9일
캐시 볼륨 및 Tape Gateway 로컬 캐시 스토리지가 4배 증가함	Storage Gateway에서 이제 캐시 볼륨과 Tape Gateway에 최대 64TB의 로컬 캐시를 지원하여 대규모 작업 데이터 세트에 대한 지연 시간이 짧은 액세스를 제공하므로 온프레미스 애플리케이션의 성능이 향상됩니다. 자세한 내용은 게이트웨이에 권장되는 로컬 디스크 크기를 참조하세요.	2020년 11월 9일
게이트웨이 마이그레이션	Storage Gateway에서 이제 캐시 Volume Gateway를 새 가상 머신으로 마이그레이션하는 기능을 지원합니다. 자세한 내용은 캐시 볼륨을 새로운 캐시 Volume Gateway 가상 머신으로 이동을 참조하세요.	2020년 9월 10일

테이프 보존 잠금 및 write-once-read-many (WORM) 테이프 보호 지원	Storage Gateway는 가상 테이프에 대한 테이프 보존 잠금 및 한 번 읽은 후 여러 번 쓸 수 있도록 지원합니다 (WORM). 테이프 보존 잠금 기능을 사용하면 아카이브된 가상 테이프에 보존 모드와 보존 기간을 지정하여 일정 기간(최대 100년) 동안 삭제되지 않도록 할 수 있습니다. 여기에는 테이프를 삭제하거나 보존 설정을 수정할 수 있는 사람에 대한 권한 제어 기능이 포함됩니다. 자세한 내용은 테이프 보존 잠금 사용을 참조하세요. WORM-활성화된 가상 테이프를 사용하면 가상 테이프 라이브러리의 활성 테이프에 있는 데이터를 덮어쓰거나 지울 수 없습니다. 자세한 내용은 Write Once, Read Many () 테이프 보호를 참조하십시오. WORM	2020년 8월 19일
콘솔을 통해 하드웨어 어플라이언스 주문	이제 AWS Storage Gateway 콘솔을 통해 하드웨어 어플라이언스를 주문할 수 있습니다. 자세한 내용은 Storage Gateway 하드웨어 어플라이언스 사용을 참조하세요.	2020년 8월 12일

새 AWS 지역의 연방 정보 처리 표준 (FIPS) 엔드포인트 지원	이제 미국 동부 (오하이오), 미국 동부 (버지니아 북부), 미국 서부 (캘리포니아 북부), 미국 서부 (오레곤) 및 캐나다 (중부) 지역에 FIPS 엔드포인트가 있는 게이트웨이를 활성화할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 7월 31일
게이트웨이 마이그레이션	Storage Gateway에서 이제 테이프 및 저장 Volume Gateway를 새 가상 머신으로 마이그레이션하는 기능을 지원합니다. 자세한 내용은 데이터를 새 게이트웨이로 이동을 참조하세요.	2020년 7월 31일
Storage Gateway 콘솔에서 Amazon CloudWatch 경보 보기	이제 Storage Gateway 콘솔에서 CloudWatch 경보를 볼 수 있습니다. 자세한 내용은 경보 참조하십시오.	2020년 5월 29일
연방 정보 처리 표준 (FIPS) 엔드포인트 지원	이제 지역에 FIPS 엔드포인트가 있는 게이트웨이를 활성화할 수 있습니다. AWS GovCloud (US) 볼륨 게이트웨이의 FIPS 엔드포인트를 선택하려면 서비스 엔드포인트 선택을 참조하십시오. 테이프 게이트웨이의 FIPS 엔드포인트를 선택하려면 테이프 게이트웨이 연결 대상을 참조하십시오 AWS.	2020년 5월 22일

새 AWS 지역	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
Tape Gateway 쓰기 및 읽기 성능 2배 향상	Storage Gateway를 사용하면 Tape Gateway에서 가상 테이프로부터 읽어 들이는 성능과 가상 테이프로 쓰는 성능을 2배 향상시킴으로써 백업 및 복구 작업을 이전보다 신속하게 수행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Tape Gateway에 대한 성능 지침을 참조하세요.	2020년 4월 23일

자동 테이프 생성 지원	Storage Gateway에서 이제 새 가상 테이프를 자동으로 생성하는 기능을 제공합니다. Tape Gateway는 사용자가 구성한 사용 가능한 최소 테이프 수를 유지하기 위해 자동으로 새 가상 테이프를 생성한 다음 백업 애플리케이션에서 이 새 테이프를 가져올 수 있도록 설정하므로 백업 작업을 중단 없이 실행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 자동으로 테이프 생성을 참조하세요.	2020년 4월 23일
새 AWS 지역	Storage Gateway는 이제 AWS GovCloud (미국 동부) 지역에서 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 Gateway는 이제 KVM 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. 에 배포된 게이트웨이는 기존 온프레미스 게이트웨이와 동일한 기능과 특징을 KVM 모두 갖추고 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하세요.	2020년 2월 4일

VMware vSphere 고가용성 지원	Storage Gateway는 이제 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호하는 VMware 데 도움이 되는 고가용성을 지원합니다. 자세한 내용은 Storage Gateway 사용 설명서의 Storage Gateway를 통한 VMware vSphere 고가용성 사용을 참조하십시오. 이 릴리스에는 성능 향상도 포함되어 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 성능을 참조하세요.	2019년 11월 20일
테이프 게이트웨이의 새 AWS 지역	이제 남아메리카(상파울루) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 9월 24일

Linux에서 IBM 스펙트럼 보호 버전 7.1.9를 지원하고 테이프 게이트웨이의 경우 최대 테이프 크기를 5TiB로 늘렸습니다.	테이프 게이트웨이는 이제 Microsoft Windows에서 실행되는 것 외에도 Linux에서 실행되는 IBM 스펙트럼 보호 (Tivoli Storage Manager) 버전 7.1.9를 지원합니다. 자세한 내용은 Storage Gateway 사용 설명서의 IBMSpectrum Protect를 사용한 설정 테스트를 참조하십시오. . 또한 Tape Gateway의 경우 가상 테이프의 최대 크기가 2.5TiB에서 5TiB로 증가했습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 테이프 할당량을 참조하세요.	2019년 9월 10일
아마존 CloudWatch 로그 지원	이제 Amazon CloudWatch Log Groups로 파일 게이트웨이를 구성하여 게이트웨이와 해당 리소스의 오류 및 상태에 대한 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서의 게이트웨이 상태 및 Amazon CloudWatch Log 그룹 오류에 대한 알림 받기를 참조하십시오.	2019년 9월 4일
새 AWS 지역	이제 아시아 태평양(홍콩) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 8월 14일

새 AWS 지역	이제 중동(바레인) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 7월 29일
가상 사설 클라우드의 게이트웨이 활성화 지원 () VPC	이제 a에서 게이트웨이를 활성화할 수 있습니다. VPC 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하십시오.	2019년 6월 20일
S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 가상 테이프 이동 지원	이제부터는 S3 Glacier Flexible Retrieval 스토리지 클래스에 저장된 가상 테이프를 비용 효과가 좋고 장기간 데이터를 보존할 수 있는 S3 Glacier Deep Archive 스토리지 클래스로 옮길 수 있습니다. 자세한 내용은 S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프 이전을 참조하세요.	2019년 5월 28일
SMB마이크로소프트 윈도우용 파일 공유 지원 ACLs	파일 게이트웨이의 경우 이제 Microsoft Windows 액세스 제어 목록 (ACLs) 을 사용하여 서버 메시지 블록 (SMB) 파일 공유에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 Microsoft Windows를 사용하여 SMB 파일 ACLs 공유에 대한 액세스 제어를 참조하십시오.	2019년 5월 8일

S3 Glacier Deep Archive와 통합	Tape Gateway는 S3 Glacier Deep Archive와 통합됩니다. 이제 데이터를 장기간 보존하기 위해 가상 테이프를 S3 Glacier Deep Archive에 아카이브할 수 있습니다. 자세한 내용은 가상 테이프 아카이브를 참조하십시오.	2019년 3월 27일
유럽에서 Storage Gateway 하드웨어 어플라이언스 사용 가능	이제 유럽에서 Storage Gateway 하드웨어 어플라이언스를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 하드웨어 어플라이언스 리전을 참조하세요. 또한 Storage Gateway 하드웨어 어플라이언스에서 사용 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있고, 설치된 동선 네트워크 카드를 10기가비트 광섬유 네트워크 카드로 교체할 수 있습니다. 자세한 내용은 하드웨어 어플라이언스 설정을 참조하십시오.	2019년 2월 25일
다음과 통합 AWS Backup	Storage Gateway는 와 통합됩니다. AWS Backup이제 클라우드 기반 스토리지용 Storage Gateway 볼륨을 사용하는 온프레미스 비즈니스 애플리케이션을 백업하는 AWS Backup 데 사용할 수 있습니다. 자세한 내용은 볼륨 백업을 참조하십시오.	2019년 1월 16일

바큘라 엔터프라이즈 및 IBM 스펙트럼 보호 지원	테이프 게이트웨이는 이제 Bacula Enterprise 및 IBM Spectrum Protect를 지원합니다. Storage Gateway는 이제 최신 버전의 베리타스, 베리타스 Backup NetBackup Exec 및 Quest 백업도 지원합니다. NetVault 이제 이러한 백업 애플리케이션을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 백업 소프트웨어를 사용하여 게이트웨이 설정 테스트를 참조하십시오.	2018년 11월 13일
Storage Gateway 하드웨어 어플라이언스 지원	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

Microsoft System Center 2016 데이터 보호 관리자와의 호환성 (DPM)	테이프 게이트웨이는 이제 Microsoft System Center 2016 데이터 보호 관리자 (DPM) 와 호환됩니다. 이제 Microsoft를 사용하여 Amazon DPM S3 에 데이터를 백업하고 오프라인 스토리지 (S3 Glacier 플렉시블 검색 또는 S3 Glacier Deep Archive) 에 직접 보관할 수 있습니다. 자세한 내용은 Microsoft System Center Data Protection Manager를 사용한 설정 테스트를 참조하십시오.	2018년 7월 18일
서버 메시지 블록 (SMB) 프로토콜 지원	파일 게이트웨이는 파일 공유에 서버 메시지 블록 (SMB) 프로토콜에 대한 지원을 추가했습니다. 자세한 내용은 파일 공유 생성을 참조하십시오.	2018년 6월 20일
파일 공유, 캐시 볼륨 및 가상 테이프 암호화 지원	이제 AWS Key Management Service (AWS KMS) 를 사용하여 파일 공유, 캐시된 볼륨 또는 가상 테이프에 기록된 데이터를 암호화할 수 있습니다. 현재는 를 사용하여 이 작업을 수행할 수 있습니다. AWS Storage Gateway API 자세한 내용은 AWS KMS를 사용하여 데이터 암호화를 참조하세요.	2018년 6월 12일

NovaStor DataCenter/네트워크 지원	테이프 게이트웨이는 이제 /Network를 지원합니다. NovaStor DataCenter 이제 NovaStor DataCenter / Network 버전 6.4 또는 7.1을 사용하여 Amazon S3에 데이터를 백업하고 오프라인 스토리지 (S3 Glacier 플렉시블 검색 또는 S3 Glacier Deep Archive)에 직접 보관할 수 있습니다. 자세한 내용은 /Network를 사용하여 설정 테스트를 참조하십시오. NovaStor DataCenter	2018년 5월 24일

이전 업데이트

다음 표에서는 2018년 5월 이전 AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	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 생성을 참조하세요.	2018년 4월 4일
새로운 리전	이제 아시아 태평양(싱가포르) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2018년 3월 4일
캐시 새로 고침 알림, 요청자 지불 및 Amazon S3 ACLs 버킷용 캔을 지원합니다.	이제 게이트웨이가 Amazon S3 버킷에서 캐시 새로 고침을 완료하면 File Gateway를 통해 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway API 참조의 RefreshCache .html을 참조하십시오.	2018년 3월 1일

변경 사항	설명	변경 날짜
	이제 File Gateway를 통해 버킷 소유자가 아닌 요청자나 리더가 액세스 요금을 지불할 수 있습니다. 이제 파일 게이트웨이를 통해 NFS 파일 공유에 매핑되는 S3 버킷의 소유자에게 모든 권한을 부여할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	
Dell EMC NetWorker V9.x에 대한 지원	테이프 게이트웨이는 이제 Dell V9.x를 지원합니다. EMC NetWorker 이제 Dell EMC NetWorker V9.x를 사용하여 Amazon S3에 데이터를 백업하고 오프라인 스토리지 (S3 Glacier 플렉시블 검색 또는 S3 Glacier Deep Archive) 에 직접 보관할 수 있습니다. 자세한 내용은 Dell을 사용한 설정 테스트를 참조하십시오. EMC NetWorker	2018년 2월 27일
새로운 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 유형 추측 지원 MIME	이제 파일 게이트웨이는 NFS 파일 공유에 기록된 모든 파일이 Amazon S3에 업로드되면 이를 사용자에게 알릴 수 있습니다. 자세한 내용은 Storage Gateway API 참조를 참조하십시오 NotifyWhenUploaded. 이제 파일 게이트웨이를 통해 파일 확장자를 기반으로 업로드된 객체의 MIME 유형을 추측할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2017년 11월 21일
VMwareESXi하이퍼바이저 버전 6.5 지원	AWS Storage Gateway 이제 VMware ESXi 하이퍼바이저 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

변경 사항	설명	변경 날짜
Commvault 11과의 호환성	Tape Gateway가 이제 Commvault 11과 호환됩니다. 이제 Commvault를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Commvault를 사용한 설정 테스트를 참조하세요.	2017년 9월 12일
Microsoft Hyper-V 하이퍼바이저의 File Gateway 지원	이제 Microsoft Hyper-V 하이퍼바이저에 File Gateway를 배포할 수 있습니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하세요.	2017년 6월 22일
아카이브로부터 3~5시간 테이프 검색 지원	Tape Gateway의 경우 이제 아카이브에서 3-5시간 후에 테이프를 검색할 수 있습니다. 또한 백업 애플리케이션 또는 가상 테이프 라이브러리 () VTL 에서 테이프에 기록되는 데이터의 양을 확인할 수 있습니다. 자세한 내용은 테이프 사용량 보기를 참조하세요.	2017년 5월 23일
새로운 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 생성을 참조하세요. 이제 File Gateway를 통해 게이트웨이가 마지막으로 버킷의 콘텐츠를 나열하고 결과를 캐싱한 이후에 추가 또는 제거된 Amazon S3 버킷에서 객체를 찾을 수 있습니다. 자세한 내용은 RefreshCacheAPI참조를 참조하십시오.	2017년 3월 28일
볼륨 복제 지원	캐시된 볼륨 게이트웨이의 경우 AWS Storage Gateway 이제 기존 볼륨에서 볼륨을 복제하는 기능을 지원합니다. 자세한 내용은 볼륨 복제를 참조하세요.	2017년 3월 16일

변경 사항	설명	변경 날짜
Amazon의 파일 게이트웨이 지원 EC2	AWS Storage Gateway 이제 Amazon에 파일 게이트웨이를 배포할 수 있는 기능을 제공합니다EC2. 이제 커뮤니티로 제공되는 Storage Gateway Amazon 머신 이미지 (AMI) EC2 를 사용하여 Amazon에서 파일 게이트웨이를 시작할 수 AMI 있습니다. 파일 게이트웨이를 생성하고 EC2 인스턴스에 배포하는 방법에 대한 자세한 내용은 Amazon S3 파일 게이트웨이 생성 및 활성화 또는 Amazon 파일 게이트웨이 생성 및 활성화를 참조하십시오. FSx 파일 게이트웨이를 AMI 시작하는 방법에 대한 자세한 내용은 Amazon 호스트에 S3 파일 게이트웨이 배포 또는 Amazon EC2 호스트에 FSx 파일 게이트웨이 배포를 참조하십시오. EC2	2017년 2월 08일
Arcserve 17과의 호환성	Tape Gateway가 이제 Arcserve 17과 호환됩니다. 이제 Arcserve를 사용하여 데이터를 Amazon S3에 백업하고 S3 Glacier Flexible Retrieval에 직접 아카이브할 수 있습니다. 자세한 내용은 Arcserve Backup r17.0을 사용한 설정 테스트를 참조하세요.	2017년 1월 17일
새로운 리전	이제 EU(런던) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 12월 13일
새로운 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. 파일 게이트웨이는 서비스와 가상 소프트웨어 어플라이언스를 결합하여, 네트워크 파일 시스템 (NFS) 과 같은 업계 표준 파일 프로토콜을 사용하여 Amazon S3에 객체를 저장하고 검색할 수 있도록 합니다. 게이트웨이는 Amazon S3의 객체에 대한 액세스를 NFS 마운트 포인트에 있는 파일로 제공합니다.	2016년 11월 29일

변경 사항	설명	변경 날짜
Backup Exec 16	Tape Gateway가 이제 Backup Exec 16과 호환됩니다. 이제 Backup Exec 16을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2016년 11월 7일
마이크로 포커스 (HPE) 데이터 프로텍터 9.x와의 호환성	테이프 게이트웨이는 이제 마이크로 포커스 (HPE) 데이터 프로텍터 9.x와 호환됩니다. 이제 HPE 데이터 프로텍터를 사용하여 Amazon S3에 데이터를 백업하고 S3 Glacier 플렉서블 검색에 직접 보관할 수 있습니다. 자세한 내용은 Micro Focus (HPE) 데이터 프로텍터를 사용한 설정 테스트를 참조하십시오.	2016년 11월 2일
새로운 리전	이제 미국 동부(오하이오) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 10월 17일
Storage Gateway 콘솔 재설계	Storage Gateway Management Console을 재설계하여 게이트웨이, 볼륨 및 가상 테이프를 구성, 관리 및 모니터링하는 작업이 더 수월해졌습니다. 이제 사용자 인터페이스에서 필터링할 수 있는 뷰를 제공하고, CloudWatch Amazon과 같은 통합 AWS 서비스에 대한 직접 링크를 제공합니다EBS. 자세한 내용은 가입하기 AWS Storage Gateway 단원을 참조하십시오.	2016년 8월 30일
Veeam Backup & Replication V9 업데이트 2 이상과의 호환성	Tape Gateway가 이제 Veeam Backup & Replication V9 업데이트 2 이상(즉 버전 9.0.0.1715 이상)과 호환됩니다. 이제 Veeam Backup Replication V9 업데이트 2 이상을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veeam Backup & Replication를 사용한 설정 테스트 참조하세요.	2016년 8월 15일

변경 사항	설명	변경 날짜
더 긴 볼륨 및 스냅샷 IDs	Storage Gateway는 볼륨과 IDs 스냅샷에 더 긴 시간을 도입하고 있습니다. 볼륨, 스냅샷 및 기타 지원되는 AWS 리소스에 대해 더 긴 ID 형식을 활성화할 수 있습니다. 자세한 내용은 Storage Gateway 리소스 및 리소스에 대한 이해 IDs 단원을 참조하십시오.	2016년 4월 25일
새로운 리전 저장 볼륨에 대한 최대 512TiB 크기의 스토리지 지원 Storage Gateway 로컬 콘솔에 대한 기타 게이트웨이 업데이트 및 개선 사항	이제 아시아 태평양(서울) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 단원을 참조하십시오. 저장 볼륨의 경우, 최대 크기가 16TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 512TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요. 가상 테이프 라이브러리에 있는 모든 테이프의 총 크기가 1PiB로 증가하였습니다. 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오. 이제 Storage Gateway 콘솔에서 VM 로컬 콘솔의 암호를 설정할 수 있습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정을 참조하세요.	2016년 3월 21일
Dell EMC NetWorker 8.x용과의 호환성	테이프 게이트웨이는 이제 Dell EMC NetWorker 8.x와 호환됩니다. 이제 EMC NetWorker Dell을 사용하여 Amazon S3에 데이터를 백업하고 오프라인 스토리지 (S3 Glacier 플렉서블 검색 또는 S3 Glacier Deep Archive) 에 직접 보관할 수 있습니다. 자세한 내용은 Dell을 사용한 설정 테스트를 참조하십시오. EMC NetWorker	2016년 2월 29일

변경 사항	설명	변경 날짜
VMwareESXi하이퍼바이저 버전 6.0 및 레드햇 엔터프라이즈 리눅스 7 i 이니시에이터 지원 SCSI	AWS Storage Gateway 이제 VMware ESXi 하이퍼바이저 버전 6.0과 Red Hat 엔터프라이즈 리눅스 7 i 이니시에이터를 지원합니다. SCSI 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 및 i 이니시에이터 SCSI 지원 단원을 참조하세요.	2015년 10월 20일
콘텐츠 재구성	이 릴리스가 포함하는 개선점은 다음과 같습니다. 즉 모든 게이트웨이 솔루션에 공통된 관리 작업을 모아놓은 "Managing Your Activated Gateway" 단원이 설명서에 포함되었습니다. 아래에서는 게이트웨이를 배포하고 활성화한 후 관리하는 방법에 대한 지침을 얻을 수 있습니다. 자세한 내용은 게이트웨이 관리 단원을 참조하십시오.	
캐싱 볼륨에 대한 최대 1,024TiB 크기의 스토리지 지원	캐싱 볼륨의 경우, 최대 크기가 32TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 1,024TiB까지 구성할 수 있습니다. 자세한 내용은 캐시 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요.	2015년 9월 16일
하이퍼바이저의 VMXNET3 (10GbE) 네트워크 어댑터 유형 지원 VMware ESXi	게이트웨이가 VMware ESXi 하이퍼바이저에서 호스팅되는 경우 어댑터 유형을 사용하도록 게이트웨이를 재구성할 수 있습니다. VMXNET3 자세한 내용은 게이트웨이용 네트워크 어댑터 구성 단원을 참조하십시오.	
성능 개선 사항	Storage Gateway의 최대 업로드 속도를 초당 120MB로 개선하였고, 최대 다운로드 속도는 초당 20MB로 개선하였습니다.	
Storage Gateway 로컬 콘솔에 대한 기타 개선 사항 및 업데이트	유지 관리 작업을 수행하는 데 도움이 되는 부가 기능으로 Storage Gateway 로컬 콘솔을 업데이트 및 강화하였습니다. 자세한 내용은 게이트웨이 네트워크 구성 단원을 참조하십시오.	

변경 사항	설명	변경 날짜
태그 지정 지원	Storage Gateway에서 이제 리소스 태그 지정을 지원합니다. 이제 게이트웨이, 볼륨, 가상 테이프에 태그를 추가하여 더 쉽게 관리할 수 있습니다. 자세한 내용은 Storage Gateway 리소스에 태그를 지정 단원을 참조하십시오.	2015년 9월 2일
퀘스트 (구 Dell) 백업 NetVault 10.0과의 호환성	테이프 게이트웨이는 이제 Quest NetVault Backup 10.0과 호환됩니다. 이제 Quest NetVault Backup 10.0을 사용하여 Amazon S3에 데이터를 백업하고 오프라인 스토리지 (S3 빙하 플렉시블 검색 또는 S3 Glacier Deep Archive) 에 직접 보관할 수 있습니다. 자세한 내용은 Quest NetVault Backup을 사용하여 설정 테스트를 참조하십시오.	2015년 6월 22일

변경 사항	설명	변경 날짜
저장 볼륨 게이트웨이 설정에 대한 16TiB 스토리지 볼륨 지원	Storage Gateway에서 이제 저장 Volume Gateway 설정에 대해 16TiB 스토리지 볼륨을 지원합니다. 이제 16TiB 스토리지 볼륨을 최대 12개까지 생성하여 전체 스토리지를 최대 192TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처를 참조하세요.	2015년 6월 3일
Storage Gateway 로컬 콘솔에서 시스템 리소스 점검 기능 지원	이제 시스템 리소스 (가상 CPU 코어, 루트 볼륨 크기 등 RAM) 가 게이트웨이가 제대로 작동하는 데 충분한지 확인할 수 있습니다. 자세한 내용은 게이트웨이 시스템 리소스 상태 조회 또는 게이트웨이 시스템 리소스 상태 조회을 참조하세요.	
레드햇 엔터프라이즈 리눅스 6 i SCSI 이니시에이터 지원	Storage Gateway는 이제 Red Hat 엔터프라이즈 리눅스 6 i SCSI 이니시에이터를 지원합니다. 자세한 내용은 볼륨 게이트웨이 설정 요구 사항 단원을 참조하십시오. 이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다. • 이제 Storage Gateway 콘솔에서 게이트웨이에 소프트웨어 업데이트를 성공적으로 적용한 최종 날짜와 시간을 볼 수 있습니다. 자세한 내용은 게이트웨이 업데이트 관리 단원을 참조하십시오. • Storage Gateway는 이제 스토리지 볼륨에 연결된 SCSI 이니시에이터를 나열하는 데 사용할 수 있는 기능을 제공합니다. API 자세한 내용은 ListVolumeInitiatorsAPI참조를 참조하십시오.	

변경 사항	설명	변경 날짜
Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2 지원	Storage Gateway에서 이제 Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2를 지원합니다. 이것은 Microsoft Hyper-V 하이퍼바이저 버전 2008 R2 지원에 추가된 것입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 4월 30일
Symantec Backup Exec 15와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 15와 호환됩니다. 이제 Symantec Backup Exec 15를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2015년 4월 6일
CHAP스토리지 볼륨에 대한 인증 지원	Storage Gateway는 이제 스토리지 볼륨에 대한 CHAP 인증 구성을 지원합니다. 자세한 내용은 볼륨에 대한 CHAP 인증 구성을 참조하십시오.	2015년 4월 2일
VMwareESXi하이퍼바이저 버전 5.1 및 5.5 지원	Storage Gateway는 이제 VMware ESXi 하이퍼바이저 버전 5.1 및 5.5를 지원합니다. 이는 VMware ESXi 하이퍼바이저 버전 4.1 및 5.0에 대한 지원과 함께 제공됩니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 3월 30일
윈도우 CHKDSK 유틸리티 지원	Storage Gateway는 이제 Windows CHKDSK 유틸리티를 지원합니다. 이 유틸리티를 사용하여 볼륨의 무결성을 확인하고 볼륨의 오류를 수정할 수 있습니다. 자세한 내용은 볼륨 문제 해결을 참조하세요.	2015년 3월 04일

변경 사항	설명	변경 날짜
와 AWS CloudTrail 통합하여 API 통화를 캡처합니다.	이제 Storage Gateway가 와 AWS CloudTrail통합되었습니다. AWS CloudTrail Amazon Web Services 계정의 Storage Gateway에서 또는 Storage Gateway를 대신하여 이루어진 API 호출을 캡처하고 지정한 Amazon S3 버킷으로 로그 파일을 전송합니다. 자세한 내용은 로그인 및 모니터링 AWS Storage Gateway 단원을 참조하십시오. 이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다. • 이제 캐시 스토리지에 오손 데이터(dirty data)가 있는 가상 테이프, 즉 AWS에 업로드하지 않은 콘텐츠를 포함하는 가상 테이프는 게이트웨이의 캐싱된 드라이브가 변경될 때 복구됩니다. 자세한 내용은 복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우를 참조하세요.	2014년 12월 16일

변경 사항	설명	변경 날짜
추가 백업 소프트웨어 및 미디어 체인저와의 호환성	Tape Gateway가 이제 다음 백업 소프트웨어와 호환됩니다. • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 이제 이 네 가지 백업 소프트웨어 제품을 Storage Gateway 가상 테이프 라이브러리 (VTL) 와 함께 사용하여 Amazon S3에 백업하고 오프라인 스토리지 (S3 Glacier 플렉시블 검색 또는 S3 Glacier Deep Archive)에 직접 보관할 수 있습니다. 자세한 내용은 백업 소프트웨어를 사용하여 게이트웨이 설정 테스트를 참조하십시오. Storage Gateway에서 이제 새 백업 소프트웨어와 함께 작동하는 추가 미디어 체인저를 제공합니다. 이번 릴리스에는 기타 개선 사항 및 업데이트가 포함되어 있습니다. AWS Storage Gateway	2014년 11월 3일
Europe (Frankfurt) Region	이제 유럽(프랑크푸르트) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2014년 10월 23일

변경 사항	설명	변경 날짜
콘텐츠 재구성	모든 게이트웨이 솔루션에 공통된 시작하기 단원을 만들었습니다. 아래에서는 게이트웨이를 다운로드, 배포 및 활성화하는 방법에 대한 지침을 얻을 수 있습니다. 게이트웨이를 배포하고 활성화한 후 저장 볼륨, 캐시 볼륨 및 Tape Gateway 설정에 따른 추가 지침에 따라 작업을 수행할 수 있습니다. 자세한 내용은 Tape Gateway 생성을 참조하세요.	2014년 5월 19일
Symantec Backup Exec 2012와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 2012와 호환됩니다. 이제 Symantec Backup Exec 2012를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2014년 4월 28일

변경 사항	설명	변경 날짜
Windows Server Failover Clustering 지원 VMwareESX이니시에이터 지원 Storage Gateway 로컬 콘솔에서 구성 작업을 수행하도록 지원	• 이제 Storage Gateway는 호스트가 Windows Server 페일오버 클러스터링 () WSFC 을 사용하여 액세스를 조정하는 경우 동일한 볼륨에 여러 호스트를 연결할 수 있도록 지원합니다. 하지만 를 사용하지 않고는 동일한 볼륨에 여러 호스트를 연결할 수 없습니다. WSFC • 이제 Storage Gateway를 사용하면 ESX 호스트를 통해 직접 스토리지 접속을 관리할 수 있습니다. 이렇게 하면 게스트 운영 체제에 있는 이니시에이터를 사용하는 대신 사용할 수 있습니다. VMs • Storage Gateway에서 이제 Storage Gateway 로컬 콘솔에서 구성 작업을 수행할 수 있도록 지원합니다. 온프레미스에 배포한 게이트웨이에서 구성 작업을 수행하는 방법에 대한 정보는 VM 로컬 콘솔에서 작업 수행 또는 VM 로컬 콘솔에서 작업 수행 단원을 참조하십시오. EC2인스턴스에 배포된 게이트웨이에서 구성 작업을 수행하는 방법에 대한 자세한 내용은 또는 을 참조하십시오Amazon EC2 로컬 콘솔에서 작업 수행. Amazon EC2 로컬 콘솔에서 작업 수행	2014년 1월 31일

변경 사항	설명	변경 날짜
가상 테이프 라이브러리 (VTL) 에 대한 지원 및 API 버전 2013-06-30 소개	Storage Gateway는 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지와 연결하여 온프레미스 IT 환경을 스토리지 인프라와 통합합니다 AWS . 이제 Storage Gateway는 볼륨 게이트웨이 (캐시된 볼륨 및 저장된 볼륨) 외에도 게이트웨이—가상 테이프 라이브러리 () 를 지원합니다. VTL Tape Gateway에 게이트웨이당 가상 테이프 드라이브를 최대 10개까지 구성할 수 있습니다. 각 가상 테이프 드라이브는 SCSI 명령 세트에 응답하므로 기존 온프레미스 백업 애플리케이션을 수정하지 않고도 사용할 수 있습니다. 자세한 내용은 AWS Storage Gateway 사용 설명서에서 다음 주제를 참조하세요. • 아키텍처 개요는 Tape Gateway 작동 방식(아키텍처)을 참조하세요. • Tape Gateway를 시작하려면 Tape Gateway 생성을 참조하세요.	2013년 11월 5일
Microsoft Hyper-V 지원	Storage Gateway에서 이제 Microsoft Hyper-V 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. Microsoft Hyper-V에 배포한 게이트웨이에는 기존 온프레미스 Storage Gateway와 동일한 기능이 있습니다. Microsoft Hyper-V를 이용해 게이트웨이 배포를 시작하려면 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하십시오.	2013년 10월 4일

변경 사항	설명	변경 날짜
Amazon에서의 게이트웨이 배포 지원 EC2	Storage Gateway는 이제 Amazon Elastic Compute Cloud (AmazonEC2) 에 게이트웨이를 배포할 수 있는 기능을 제공합니다. 에서 AMI 제공되는 Storage EC2 Gateway를 사용하여 Amazon에서 게이트웨이 인스턴스를 시작할 수 AWS Marketplace있습니다. Storage Gateway를 사용하여 게이트웨이 배포를 시작하려면 을 참조하십시오볼륨 게이트웨이를 호스팅하기 위한 Amazon EC2 인스턴스 배포. AMI	2013년 1월 15일
캐시된 볼륨에 대한 지원 및 API 버전 2012-06-30의 소개	이번 릴리스에서는 Storage Gateway에 캐시 볼륨에 대한 지원을 도입했습니다. 캐싱 볼륨은 온프레미스 스토리지 인프라를 확장할 필요성을 최소화하는 한편, 애플리케이션이 활성 데이터에 액세스할 때의 지연 시간을 짧게 유지하도록 해줍니다. 최대 32TiB 크기의 스토리지 볼륨을 생성하고 이를 온프레미스 애플리케이션 서버에서 i SCSI 디바이스로 마운트할 수 있습니다. 캐시 볼륨에 작성한 데이터는 Amazon Simple Storage Service(S3)에 저장되고, 최근에 쓰고 읽은 데이터의 캐시만 온프레미스 스토리지 하드웨어에 로컬로 저장됩니다. 캐시 볼륨을 사용하면 짧은 액세스 지연 시간이 필요한 데이터에 대한 온프레미스 스토리지를 유지하는 한편, 더 오래되고 덜 자주 액세스하는 데이터와 같이 더 긴 가져오기 지연 시간을 수용할 수 있는 데이터에 대해서는 Amazon S3를 활용할 수 있습니다. 이번 릴리즈에서 Storage Gateway는 현재 작업을 지원하는 것 외에도 캐시된 볼륨을 지원하는 새 작업을 제공하는 새 API 버전도 도입했습니다. 두 가지 Storage Gateway 솔루션에 대한 자세한 내용은 Volume Gateway 작동 방식(아키텍처) 섹션을 참조하세요. 테스트 설정을 시도해 볼 수도 있습니다. 지침은 Tape Gateway 생성을 참조하세요.	2012년 10월 29일

변경 사항	설명	변경 날짜
API및 지원 IAM	이번 릴리즈에서 Storage Gateway는 AWS Identity and Access Management(IAM) 에 대한 지원과 지원을 API 도입했습니다. • API지원 - 이제 Storage Gateway 리소스를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 에 대한 자세한 내용은 AWS Storage Gateway 사용 설명서의 API 내용을 참조하십시오APIStorage Gateway에 대한 참조. • IAMsupport — AWS Identity and Access Management (IAM) 를 사용하면 IAM 정책을 통해 사용자를 생성하고 Storage Gateway 리소스에 대한 사용자 액세스를 관리할 수 있습니다. IAM 정책에 대한 예시는 AWS Storage Gateway의 ID 및 액세스 관리 단원을 참조하십시오. 에 대한 자세한 내용은 AWS Identity and Access Management (IAM) 세부 정보 페이지를 참조하십시오. IAM	2012년 5월 9일
고정 IP 지원	이제 로컬 게이트웨이에 고정 IP를 지정할 수 있습니다. 자세한 내용은 게이트웨이 네트워크 구성 단원을 참조하십시오.	2012년 3월 5일
새 안내서	이 설명서는 AWS Storage Gateway 사용 설명서의 첫 번째 릴리스입니다.	2012년 1월 24일

볼륨 게이트웨이 어플라이언스 소프트웨어의 릴리스 노트

이 릴리스 노트에서는 어플라이언스의 각 버전에 포함된 신규 및 업데이트된 기능, 개선 사항 및 수정 사항에 대해 설명합니다. 각 소프트웨어 버전은 릴리스 날짜와 고유한 버전 번호로 식별됩니다.

Storage Gateway 콘솔의 세부 정보 페이지를 확인하거나 다음과 유사한 AWS CLI 명령을 사용하여 DescribeGatewayInformationAPI작업을 호출하여 게이트웨이의 소프트웨어 버전 번호를 확인할 수 있습니다.

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

API응답 `SoftwareVersion` 필드에 버전 번호가 반환됩니다.

> **Note**
>
> 게이트웨이는 다음과 같은 상황에서는 소프트웨어 버전 정보를 보고하지 않습니다.
>
> - 게이트웨이가 오프라인 상태입니다.
> - 게이트웨이에서 버전 보고를 지원하지 않는 이전 소프트웨어가 실행되고 있습니다.
> - 게이트웨이 유형은 FSx 파일 게이트웨이입니다.

게이트웨이의 기본 자동 유지 관리 및 업데이트 일정을 수정하는 방법을 포함하여 볼륨 게이트웨이 업데이트에 대한 자세한 내용은 Storage Gateway 콘솔을 참조하십시오. AWS

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-07-29	2.10.0	• 신규 및 기존 게이트웨이에 대한 운영 체제 업데이트 • 기타 버그 수정 및 개선 사항
2024-06-17	2.9.2	• 신규 및 기존 게이트웨이에 대한 운영 체제 업데이트
2024-05-28	2.9.0	• 소프트웨어 업데이트 중 게이트웨이 재시작 시간 단축

릴리스 날짜	소프트웨어 버전	릴리스 정보
		• 네트워크 대역폭 추정을 위해 전송되는 데이터의 양을 줄였습니다.
2024-05-08	2.8.3	• 프록시 사용 시 클라우드 연결 문제 해결 SOCKS5
2024-04-10	2.8.1	• 2.8.0에 도입된 메모리 사용 문제 해결 • 보안 패치 업데이트 • 소프트웨어 업데이트 프로세스 개선 • 새 게이트웨이의 네트워크 시간 프로토콜 (NTP) 구성 요소가 누락된 문제를 해결했습니다.
2024-03-06	2.8.0	• 새 게이트웨이를 위한 운영 체제 업데이트 • 보안 패치 업데이트
2023-12-19	2.7.0	• 새 게이트웨이를 위한 운영 체제 업데이트
2023-12-14	2.6.6	• 유지 관리 릴리스