



사용 설명서

AWSStorage Gateway



API 버전 2021-03-31

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWSStorage Gateway: 사용 설명서

Copyright © Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 브랜드 디자인은 Amazon 외 제품 또는 서비스와 함께, Amazon 브랜드 이미지를 떨어뜨리거나 고객에게 혼동을 일으킬 수 있는 방식으로 사용할 수 없습니다. Amazon이 소유하지 않은 기타 모든 상표는 Amazon과 제휴 관계이거나 관련이 있거나 후원 관계와 관계없이 해당 소유자의 자산입니다.

Table of Contents

Amazon FSx 파일 게이트웨이란 무엇입니까?	1
FSx 파일 작동 방식	1
설정	5
Amazon Web Services Services에 가입	5
IAM 사용자 생성	5
요구 사항	7
필수 사전 조건	7
하드웨어 및 스토리지 요구 사항	8
네트워크 및 방화벽 요구 사항	9
지원되는 하이퍼바이저 및 호스트 요구 사항	20
파일 게이트웨이에 지원되는 SMB 클라이언트	21
지원되는 파일 시스템 작업	22
AWS Storage Gateway에 액세스	22
지원되는 AWS 리전	22
하드웨어 어플라이언스 사용	23
지원되는 AWS 리전	24
하드웨어 어플라이언스 설정	24
랙 마운팅 및 하드웨어 어플라이언스를 전원에 연결	26
하드웨어 어플라이언스	26
네트워크 파라미터 구성	27
하드웨어 어플라이언스 활성화	29
게이트웨이 시작	30
게이트웨이에 대한 IP 주소 구성	31
게이트웨이 구성	32
게이트웨이 제거	32
하드웨어 어플라이언스 삭제	33
시작하기	34
1단계: Amazon FSx 파일 시스템 생성	34
2단계: (선택 사항) VPC 엔드포인트 만들기	35
3단계: FSx 파일 게이트웨이 게이트웨이 생성 및 활성화	37
Amazon FSx 파일 게이트웨이 설정	37
Amazon FSx 파일 게이트웨이를 AWS	38
설정을 검토하고 Amazon FSx 파일 게이트웨이 활성화	39
Amazon FSx 파일 게이트웨이 구성	40

Active Directory 도메인 설정	42
Amazon FSx 파일 시스템 연결	43
파일 공유 마운트 및 사용	46
클라이언트에 SMB 파일 공유를 탑재하려면	46
FSx 파일 테스트하기	49
VPC 게이트웨이 활성화	50
Storage Gateway 대한 VPC 엔드포인트 생성	51
HTTP 프록시 설정 및 구성	52
HTTP 프록시의 필수 포트에 대한 트래픽 허용	55
Amazon FSx 파일 게이트웨이 리소스 관리	56
Amazon FSx 파일 시스템 연결	56
FSx 파일에 대한 Active Directory 구성	56
액티브 디렉터리 설정 구성	57
FSx 파일 설정 편집	57
Amazon FSx for Windows File Server 파일 시스템 설정 편집	57
Amazon FSx 파일 시스템 분리	59
파일 게이트웨이 모니터링	60
파일 게이트웨이 상태 로그 가져오기	60
게이트웨이의 CloudWatch 로그 그룹 구성	61
Amazon CloudWatch 지표 사용	62
게이트웨이 지표 이해	63
파일 시스템 지표 이해	68
파일 게이트웨이 감사 로그 이해	70
게이트웨이 유지	75
게이트웨이 VM 종료	75
로컬 디스크 관리	75
로컬 디스크 스토리지 용량 결정	75
캐시 스토리지 크기 조정	76
캐시 스토리지 구성	77
게이트웨이 업데이트 관리	77
로컬 콘솔에서 유지 관리 작업 수행	79
VM 로컬 콘솔 (파일 게이트웨이) 에서 작업 수행	79
EC2 로컬 콘솔 (파일 게이트웨이) 에서 작업 수행	93
게이트웨이 로컬 콘솔 액세스	99
게이트웨이용 네트워크 어댑터 구성	101
게이트웨이 삭제 및 리소스 제거	104

Storage Gateway 콘솔을 사용한 게이트웨이 삭제	105
온프레미스에 배포한 게이트웨이에서 리소스 제거	106
Amazon EC2 인스턴스에 배포한 게이트웨이에서 리소스 제거	106
성능	108
게이트웨이 성능 최적화	108
게이트웨이에 리소스 추가	108
애플리케이션 환경에 리소스 추가	110
Storage Gateway VMware 고가용성 사용	110
vSphere VMware HA 클러스터 구성	111
게이트웨이 유형에 대한 .ova 이미지 다운로드	112
게이트웨이 배포	112
(선택 사항) 클러스터의 다른 VM에 대한 재정의 옵션 추가	113
게이트웨이 활성화	113
VMware 고가용성 구성 테스트	113
보안	115
데이터 보호	115
데이터 암호화	116
인증 및 액세스 제어	118
인증	118
액세스 제어	119
액세스 관리 개요	121
자격 증명 기반 정책(IAM 정책) 사용	126
태그를 사용하여 리소스에 대한 액세스 제어	135
Storage Gateway API 권한 참조	138
서비스 연결 역할 사용	146
로그 및 모니터링	150
CloudTrail의 Storage Gateway 정보	150
Storage Gateway 로그 파일 항목	151
규정 준수 검증	153
복원성	153
인프라 보안	154
보안 모범 사례	154
게이트웨이 문제 해결	155
온프레미스 게이트웨이 문제 해결	155
활성화지원게이트웨이 문제를 해결하는 데 도움이 됩니다.	159
Microsoft Hyper-V 설정 관련 문제를 해결합니다.	160

Amazon EC2 게이트웨이 문제 해결	162
잠시 후 게이트웨이 활성화가 수행되지 않았습니다.	162
인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.	163
활성화지원게이트웨이 문제를 해결하는 데 도움이 됩니다.	163
하드웨어 어플라이언스 문제 해결	165
서비스 IP 주소 확인 방법	165
초기 기본값 재설정을 수행하는 방법	165
Dell iDRAC 지원을 받는 방법	165
하드웨어 어플라이언스 일련 번호를 찾는 방법	166
하드웨어 어플라이언스 지원을 받는 방법	166
파일 게이트웨이 문제 해결	166
오류: ObjectMissing	167
알림: 재부팅	167
알림: HardReboot	168
알림: HealthCheckFailure	168
알림: AvailabilityMonitorTest	168
오류: RoleTrustRelationshipInvalid	168
CloudWatch 지표를 사용한 문제 해결	169
고가용성 상태 알림	171
고가용성 관련 문제를 해결합니다.	171
Health 알림	171
지표	173
데이터 복구: 모범 사례	173
예기치 않은 VM 종료에서 복구	174
고장난 캐시 디스크에서 데이터 복구	174
액세스할 수 없는 데이터 센터에서 데이터 복구	174
추가 리소스	176
호스트 설정	176
Storage Gateway 게이트웨이용 VMware 구성	176
게이트웨이 VM 시간 동기화	179
EC2 호스트의 파일 게이트웨이	180
정품 인증 키 가져오기	182
AWS CLI	183
Linux(bash/zsh)	183
Microsoft Windows PowerShell	184
사용AWS Direct ConnectStorage Gateway	184

게이트웨이에 연결	185
Amazon EC2 호스트에서 IP 주소 얻기	186
리소스 및 리소스 ID 이해	187
리소스 ID 작업	187
리소스에 태그 지정	188
태그 작업하기	189
다음 사항도 참조하세요.	190
오픈 소스 구성 요소	190
Storage Gateway 게이트웨이용 오픈 소스 구성 요소	191
Amazon FSx 파일 게이트웨이용 오픈 소스 구성 요소	191
할당량	192
파일 시스템에 대한 할당량	192
게이트웨이에 권장되는 로컬 디스크 크기	192
API 참조	194
필수 요청 헤더	194
요청에 서명하기	196
서명 계산 예시	197
오류 응답	199
예외	199
작업 오류 코드	201
오류 응답	221
작업	223
문서 기록	224
.....	CCXXvi

Amazon FSx 파일 게이트웨이란 무엇입니까?

Storage Gateway 파일 게이트웨이, 볼륨 게이트웨이 및 테이프 게이트웨이 스토리지 솔루션을 제공합니다.

Amazon FSx 파일 게이트웨이 (FSx 파일) 는 온프레미스 시설에서 Windows 파일 서버용 클라우드 인 FSx 파일 공유에 대한 지연 시간이 짧고 효율적인 액세스를 제공하는 새로운 파일 게이트웨이 유형입니다. 대기 시간이나 대역폭 요구 사항으로 인해 온-프레미스 파일 스토리지를 유지 관리하는 경우 FSx File을 사용하여 완전히 관리되고 안정적이며 사실상 무제한의 Windows 파일 공유에 원활하게 액세스할 수 있습니다. [AWS클라우드 by FSx for Windows File Server](#)

Amazon FSx 파일 게이트웨이 사용의 이점

FSx File 에는 다음과 같은 이점이 있습니다.

- 온프레미스 파일 서버를 제거하고 모든 데이터를 통합AWS클라우드 스토리지의 규모와 경제성을 활용합니다.
- 클라우드 데이터에 대한 온프레미스 액세스가 필요한 작업을 포함하여 모든 파일 워크로드에 사용할 수 있는 옵션을 제공합니다.
- 온프레미스를 유지해야 하는 애플리케이션은 이제 동일한 짧은 지연 시간과 높은 성능을 경험할 수 있습니다. AWS네트워크에 부담을 주지 않고 가장 까다로운 애플리케이션이 겪는 지연 시간에 영향을 주지 않습니다.

아마존 FSx 파일 게이트웨이 작동 방식

Amazon FSx 파일 게이트웨이 (FSx 파일) 를 사용하려면 FSx for Windows File Server 시스템이 하나 이상 있어야 합니다. 또한 VPN 또는 다음을 통해 FSx for Windows File Server 온-프레미스 액세스 권한이 있어야 합니다. [AWS Direct Connect](#)연결. Amazon FSx 파일 시스템 사용에 대한 자세한 내용은 단원을 참조하십시오. [Amazon FSx for Windows File Server 란 무엇입니까?](#)

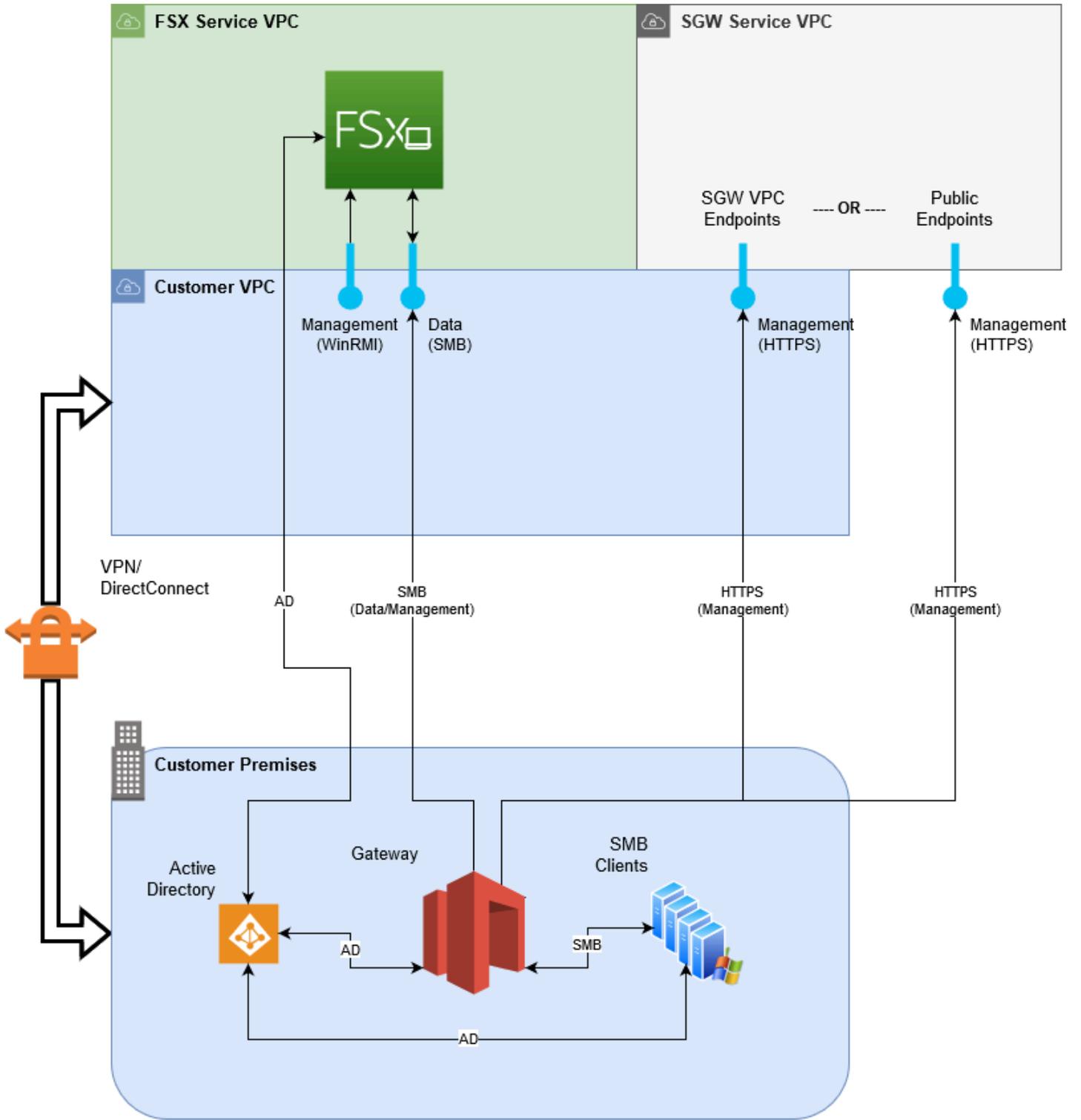
FSx 파일 VMware 가상 어플라이언스 또는AWS온프레미스 환경에 Storage Gateway 하드웨어 어플라이언스를 제공합니다. 어플라이언스를 배포한 후 Storage Gateway 콘솔 또는 Storage Gateway API를 통해 FSx 파일을 활성화합니다. Amazon Elastic Compute Cloud (Amazon EC2) 이미지를 사용하여 FSx 파일을 생성할 수도 있습니다.

Amazon FSx 파일 게이트웨이가 활성화되고 FSx for Windows File Server 액세스할 수 있는 후에는 Storage Gateway 콘솔을 사용하여 Microsoft Active Directory 도메인에 가입합니다. 게이트웨이가

도메인에 성공적으로 조인된 후에는 Storage Gateway 콘솔을 사용하여 기존 FSx for Windows File Server 게이트웨이를 연결합니다. Windows 파일 서버용 FSx는 서버의 모든 공유를 Amazon FSx 파일 게이트웨이에서 공유로 사용할 수 있도록 합니다. 그런 다음 클라이언트를 사용하여 선택한 FSx 파일에 해당하는 FSx 파일의 파일 공유를 찾아서 연결할 수 있습니다.

파일 공유가 연결되면 파일을 로컬에서 읽고 쓸 수 있으며 FSx for Windows File Server FSx에서 사용할 수 있는 모든 기능을 활용할 수 있습니다. FSx 파일은 로컬 파일 공유 및 해당 내용을 Windows 파일 서버용 FSx에 원격으로 저장된 파일 공유에 매핑합니다. 원격 파일과 로컬에서 볼 수 있는 파일과 해당 공유 간에 1:1 대응이 있습니다.

다음 다이어그램은 스토리지 Gateway를 위한 파일 스토리지 배포를 간략하게 보여줍니다.



다이어그램에서 다음 사항에 유의하십시오.

- AWS Direct Connect 또는 VPN은 FSx 파일이 SMB를 사용하여 Amazon FSx 파일 공유에 액세스하도록 허용하고 FSx for Windows File Server FSx가 온프레미스 Active Directory 도메인에 가입하도록 허용하려면 필요합니다.
- Amazon Virtual Private Cloud (Amazon VPC)은 (는) 프라이빗 엔드포인트를 사용하여 FSx for Windows File Server 서비스 VPC와 Storage Gateway 서비스 VPC 연결하는 데 필요합니다. FSx 파일은 공용 엔드포인트에도 연결할 수 있습니다.

Amazon FSx 파일 게이트웨이를 모두 사용할 수 있습니다. AWS FSx for Windows File Server 를 사용할 수 있는 지역입니다.

Amazon FSx 파일 게이트웨이에 대한 설정

이 단원에서는 Amazon FSx 파일 게이트웨이를 시작하기 위한 지침을 제공합니다. 시작하려면 우선 가입해야 합니다.AWS. 처음 사용하는 경우 다음을 수행하는 것이 좋습니다.[리전](#)과 [요구 사항](#) 섹션.

주제

- [Amazon Web Services Services에 가입](#)
- [IAM 사용자 생성](#)
- [파일 게이트웨이 설정 요구 사항](#)
- [AWS Storage Gateway에 액세스](#)
- [지원되는 AWS 리전](#)

Amazon Web Services Services에 가입

AWS 계정이 없는 경우 다음 절차에 따라 계정을 생성합니다.

AWS 계정에 가입하려면

1. <https://portal.aws.amazon.com/billing/signup>을 엽니다.
2. 온라인 지시 사항을 따릅니다.

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

IAM 사용자 생성

를 생성한 후AWS계정을 생성하려면 다음 단계를 수행합니다.AWS Identity and Access Management(IAM) 사용자. 그런 다음 관리자 권한이 있는 그룹에 해당 사용자를 추가합니다.

관리자 사용자를 직접 생성하여 관리자 그룹에 추가하려면(콘솔)

1. 루트 사용자(Root user)를 선택하고 AWS 계정 계정 이메일 주소를 입력하여 [IAM 콘솔](#)에 계정 소유자로 로그인합니다. 다음 페이지에서 암호를 입력합니다.

Note

Administrator IAM 사용자를 사용하는 아래 모범 사례를 준수하고, 루트 사용자 자격 증명을 안전하게 보관해 두는 것이 좋습니다. 몇 가지 [계정 및 서비스 관리 태스크](#)를 수행하려면 반드시 루트 사용자로 로그인해야 합니다.

2. 탐색 창에서 사용자(Users)와 사용자 추가(Add user)를 차례로 선택합니다.
3. 사용자 이름(User name)에 **Administrator**를 입력합니다.
4. AWS Management Console 액세스(console access) 옆의 확인란을 선택합니다. 그런 다음 사용자 지정 암호(Custom password)를 선택하고 텍스트 상자에 새 암호를 입력합니다.
5. (선택 사항) 기본적으로 AWS에서는 새 사용자가 처음 로그인할 때 새 암호를 생성해야 합니다. 사용자가 다음에 로그인할 때 새 암호를 생성해야 합니다(User must create a new password at next sign-in) 옆에 있는 확인란의 선택을 취소하면 새 사용자가 로그인한 후 암호를 재설정할 수 있습니다.
6. [다음: 권한(Next: Permissions)]을 선택합니다.
7. 권한 설정(Set permissions) 아래에서 그룹에 사용자 추가(Add user to group)를 선택합니다.
8. 그룹 생성(Create group)을 선택합니다.
9. 그룹 생성(Create group) 대화 상자의 그룹 이름(Group name)에 **Administrators**를 입력합니다.
10. 정책 필터링(Filter policies)을 선택한 다음 AWS 관리형 - 작업 함수(AWS managed - job function)를 선택하여 테이블 내용을 필터링합니다.
11. 정책 목록에서 AdministratorAccess 확인란을 선택합니다. 그런 다음 그룹 생성(Create group)을 선택합니다.

Note

AdministratorAccess 권한을 사용하여 AWS 결제 및 비용 관리 콘솔에 액세스하려면 먼저 결제에 대한 IAM 사용자 및 역할 액세스를 활성화해야 합니다. 이를 위해 [결제 콘솔에 액세스를 위임하기 위한 자습서 1단계](#)의 지침을 따르세요.

12. 그룹 목록으로 돌아가 새 그룹의 확인란을 선택합니다. 목록에서 그룹을 확인하기 위해 필요한 경우 새로 고침(Refresh)을 선택합니다.
13. [다음: 권한(Next: Tags)]를 선택합니다.

14. (선택 사항) 태그를 키 값 페어로 연결하여 메타데이터를 사용자에게 추가합니다. IAM에서 태그 사용에 대한 자세한 내용은 IAM 사용 설명서의 [IAM 엔터티 태깅](#)을 참조하세요.
15. [다음: 권한(Next: 검토를 클릭하여 새 사용자에게 추가될 그룹 멤버십의 목록을 확인합니다. 계속 진행할 준비가 되었으면 사용자 생성(Create user)을 선택합니다.

이와 동일한 절차에 따라 그룹이나 사용자를 추가로 생성하여 사용자에게 AWS 계정 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 특정 AWS 리소스에 대한 사용자 권한을 제한하는 정책을 사용하는 방법을 알아보려면 [액세스 관리](#) 및 [정책 예제](#)를 참조하세요.

파일 게이트웨이 설정 요구 사항

다른 언급이 없을 경우, 다음 요구 사항은 의 모든 파일 게이트웨이 유형에 공통적으로 적용됩니다. AWS Storage Gateway. 설정이 이 섹션의 요구 사항을 충족해야 합니다. 게이트웨이를 배포하기 전에 게이트웨이 설정에 적용되는 요구 사항을 검토합니다.

주제

- [필수 사전 조건](#)
- [하드웨어 및 스토리지 요구 사항](#)
- [네트워크 및 방화벽 요구 사항](#)
- [지원되는 하이퍼바이저 및 호스트 요구 사항](#)
- [파일 게이트웨이에 지원되는 SMB 클라이언트](#)
- [파일 게이트웨이에 지원되는 파일 시스템 작업](#)

필수 사전 조건

Amazon FSx 파일 게이트웨이 (FSx 파일 게이트웨이) 를 사용하기 전에 다음 요구 사항을 충족해야 합니다.

- FSx for Windows File Server 파일 시스템을 만들고 구성합니다. 지침은 단원을 참조하십시오. [단계 1: 파일 시스템 만들기](#)의 Amazon FSx for Windows File Server 사용 설명서.
- Microsoft Active Directory (AD) 구성.
- 게이트웨이 간에 네트워크 대역폭이 충분한지 확인AWS. 게이트웨이를 성공적으로 다운로드, 활성화 및 업데이트하려면 최소 100Mbps가 필요합니다.
- 프라이빗 네트워킹, VPN 구성 또는 AWS Direct ConnectAmazon Virtual Private Cloud (Amazon VPC) 와 FSx 파일 게이트웨이를 배포하는 온프레미스 환경 간

- 게이트웨이가 Active Directory 도메인 컨트롤러의 이름을 확인할 수 있는지 확인합니다. Active Directory 도메인에서 DHCP를 사용하여 해상도를 처리하거나 게이트웨이 로컬 콘솔의 네트워크 구성 설정 메뉴에서 DNS 서버를 수동으로 지정할 수 있습니다.

하드웨어 및 스토리지 요구 사항

다음 단원에서는 게이트웨이에 필요한 최소 하드웨어 및 설정, 필요한 스토리지에 할당할 최소 디스크 공간에 대한 정보를 제공합니다.

온프레미스 VM에 대한 하드웨어 요구 사항

게이트웨이를 온프레미스에서 배포하는 경우 게이트웨이 가상 머신 (VM) 을 배포하는 기본 하드웨어가 최소한의 리소스를 제공할 수 있도록 해야 합니다.

- VM에 할당된 가상 프로세서 4개
- 파일 게이트웨이를 위한 16GiB의 예약 RAM
- VM 이미지 및 시스템 데이터 설치용 디스크 공간 80GiB

Amazon EC2 인스턴스 유형에 대한 요구 사항

Amazon Elastic Compute Cloud (Amazon EC2) 에 게이트웨이를 배포하는 경우, 인스턴스 크기는 최소한 **xlarge** 게이트웨이가 작동하도록 합니다. 하지만 컴퓨팅 최적화 인스턴스 패밀리의 경우 크기가 최소 이상이어야 합니다. **2xlarge**. 게이트웨이 유형에 대한 권장 인스턴스 유형 중 하나를 사용합니다.

파일 게이트웨이별 권장 사항

- 범용 인스턴스 패밀리 m4 또는 m5 인스턴스 유형.
- 컴퓨팅 최적화 인스턴스 패밀리 c4 또는 c5 인스턴스 유형. RAM 요구 사항을 충족할 수 있도록 인스턴스 크기를 2xlarge 이상으로 선택합니다.
- 메모리 최적화 인스턴스 패밀리 r3 인스턴스 유형.
- 스토리지 최적화 인스턴스 패밀리 i3 인스턴스 유형.

Note

Amazon EC2 게이트웨이를 시작하고, 선택한 인스턴스 유형이 임시 스토리지를 지원할 경우 디스크가 자동으로 나열됩니다. Amazon EC2 인스턴스 스토리지에 대한 자세한 내용은 단원을 참조하십시오. [인스턴스 스토리지](#)의 Amazon EC2 사용 설명서.

스토리지 요구 사항

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

게이트웨이 유형	캐시 (최소값)	캐시 (최대값)			
파일 게이트웨이	150GiB	64TiB			

Note

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

네트워크 및 방화벽 요구 사항

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

네트워크 대역폭 요구 사항은 게이트웨이에서 업로드하고 다운로드한 데이터 양에 따라 다릅니다. 게이트웨이를 성공적으로 다운로드, 활성화 및 업데이트하려면 최소 100Mbps가 필요합니다. 데이터 전송 패턴은 워크로드를 지원하는 데 필요한 대역폭을 결정합니다.

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

Note

경우에 따라서는 Amazon EC2 FSx File Gateway를 배포하거나 네트워크 보안 정책을 제한하는 다른 유형의 배포 (온프레미스 포함) 를 사용할 수 있습니다. AWSIP 주소 범위. 이러한 경우, 게이트웨이에 서비스 연결 문제가 발생할 수 있습니다. AWSIP 범위 값이 변경됩니다. 이 AWS 사용해야 하는 IP 주소 범위 값은 Amazon 서비스 하위 집합에 있습니다. AWS에서 게이트웨이를 활성화하는 리전입니다. 현재 IP 범위 값은 단원을 참조하십시오. [AWSIP 주소 범위](#)의 AWS 일반 참조.

주제

- [포트 요구 사항](#)
- [Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항](#)
- [AWS Storage Gateway가 방화벽 및 라우터를 통해 액세스할 수 있도록 허용](#)
- [Amazon EC2 게이트웨이 인스턴스에 대한 보안 그룹 구성](#)

포트 요구 사항

모든 게이트웨이 유형에 대한 공통 포트

다음 포트는 공통이기 때문에 모든 유형의 게이트웨이에 필요합니다.

프로토콜	포트	Direction	소스	대상	의 활용 방식
TCP	443(HTTPS)	아웃바운드	Storage Gateway	AWS	Storage Gateway AWS 서비스 엔드 포인트. 서비스 엔드포인트에 대한 자세한 내용은 AWS Storage Gateway가 방화벽 및 라우터를 통해 액세스할 수

프로토콜	포트	Direction	소스	대상	의 활용 방식
					있도록 허용 단원을 참조 하십시오.

프로토콜	포트	Direction	소스	대상	의 활용 방식
TCP	80(HTTP)	인바운드	연결할 호스트입니다.AWS Management Console.	Storage Gateway	<p>스토리지 게이트웨이 정품 인증 키를 가져올 때 로컬 시스템이 사용됩니다. 포트 80은 Storage Gateway 어플라이언스의 정품 인증 동안에만 사용됩니다.</p> <p>Storage Gateway에 대한 공공 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. Storage Gateway 콘솔에서 게이트웨이를 정품 인증하는 경우 콘솔에 연결할 때 사용하는 호스트에 게이트</p>

프로토콜	포트	Direction	소스	대상	의 활용 방식
					웨이의 포트 80에 대한 액세스 권한이 있어야 합니다.
UDP/UDP	53(DNS)	아웃바운드	Storage Gateway	DNS 서버	Storage Gateway DNS 서버 간 통신용입니다.
TCP	22(지원 채널)	아웃바운드	Storage Gateway	지원	허용지원게이트웨이에 액세스하여 게이트웨이 문제 해결을 돕습니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다.
UDP	123(NTP)	아웃바운드	NTP 클라이언트	NTP 서버	로컬 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다.

파일 게이트웨이용 포트

FSx 파일 게이트웨이에서 도메인 사용자가 SMB (Server Message Block) 파일 공유에 액세스할 수 있게 허용하려면 Microsoft Active Directory를 사용해야 합니다. 파일 게이트웨이에서 유효한 모든 Microsoft Windows 도메인 (DNS로 확인 가능) 에 조인될 수 있습니다.

뿐만 아니라AWS Directory Service를 생성하려면[AWS Managed Microsoft AD](#)Amazon Web Services Cloud에서. 대부분의 경우AWS Managed Microsoft AD를 배포하는 경우 VPC 대한 DHCP (Dynamic Host Configuration Protocol) 서비스를 구성해야 합니다. DHCP 옵션 세트 만들기에 대한 자세한 내용은 단원을 참조하십시오.[DHCP 옵션 세트 생성](#)의AWS Directory Service관리 안내서.

FSx File Gateway에는 다음 포트가 필요합니다.

프로토콜	포트	Direction	소스	대상	의 활용 방식
UDP NetBIOS	137	인바운드 및 아웃바운드		Microsoft Active Directory	Microsoft Active Directory에 연결하려면
UDP NetBIOS	138	인바운드 및 아웃바운드			데이터그램 서비스
TCP LDAP	389	인바운드 및 아웃바운드			DSA (디렉터 리 시스템 에 이전트) 클라 이언트 연결 용
TCP v2/v3 데 이터	445	아웃바운드			FSx for Windows File Server 게이 트웨이 간 스 토리지 데이 터 전송
TCP (HTTPS)	443	아웃바운드		Storage Gateway 서 비스 엔드포 인트	관리 제어 — Storage Gateway VM 에서AWS서

프로토콜	포트	Direction	소스	대상	의 활용 방식
					비스 엔드포인트
TCP HTTPS	443	아웃바운드		Amazon CloudFront	게이트웨이 활성화용
TCP	443	아웃바운드		VPC 엔드포인트 사용	관리 제어 — Storage Gateway VM에서AWS서비스 엔드포인트.
TCP	1026	아웃바운드			트래픽 제어에 사용
TCP	1027	아웃바운드			활성화 중에만 사용되며 닫을 수 있습니다.
TCP	1028	아웃바운드			트래픽 제어에 사용
TCP	1031	아웃바운드			파일 게이트웨이의 소프트웨어 업데이트에만 사용
TCP	2222	아웃바운드			VPC 엔드포인트를 사용할 때 게이트웨이에 대한 지원 채널을 여는 데 사용 됩니다.

프로토콜	포트	Direction	소스	대상	의 활용 방식
TCP (HTTPS)	8080	인바운드			하드웨어 어플라이언스 정품 인증에 잠시 필요합니다.

Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항

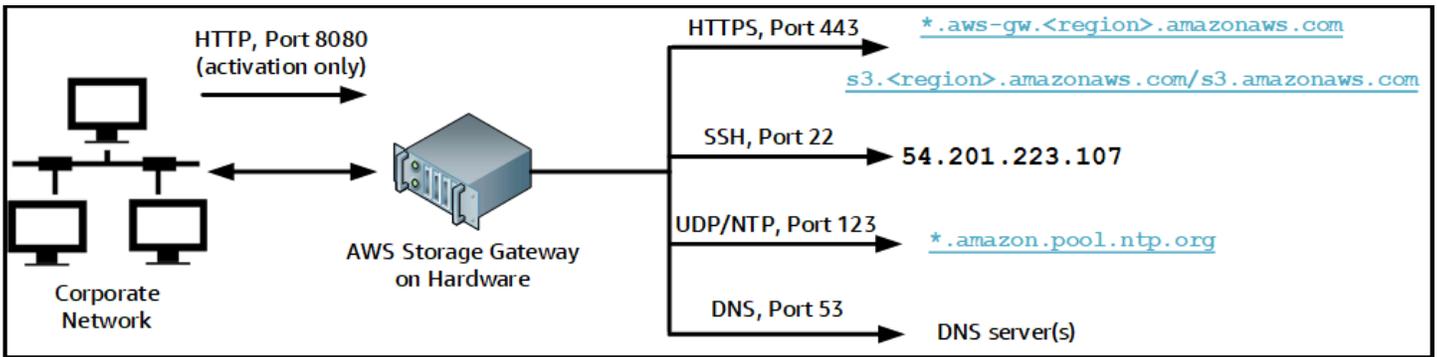
각 Storage Gateway 하드웨어 어플라이언스에는 다음 네트워크

- 인터넷 액세스— 서버의 모든 네트워크 인터페이스를 통해 인터넷에 항상 연결되는 네트워크 연결.
- DNS 서비스— 하드웨어 어플라이언스와 DNS 서버 간 통신을 위한 DNS 서비스.
- 시간 동기화— 자동으로 구성된 Amazon NTP 시간 서비스에 연결할 수 있어야 합니다.
- IP 주소— 할당된 DHCP 또는 정적 IPv4 주소. IPv6 주소는 할당할 수 없습니다.

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

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

iDRAC 포트는 원격 서버 관리에 사용할 수 있습니다.



하드웨어 어플라이언스를 작동하려면 다음 포트가 필요합니다.

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

하드웨어 어플라이언스는 설계상 다음과 같은 네트워크 및 방화벽 설정이 필요합니다.

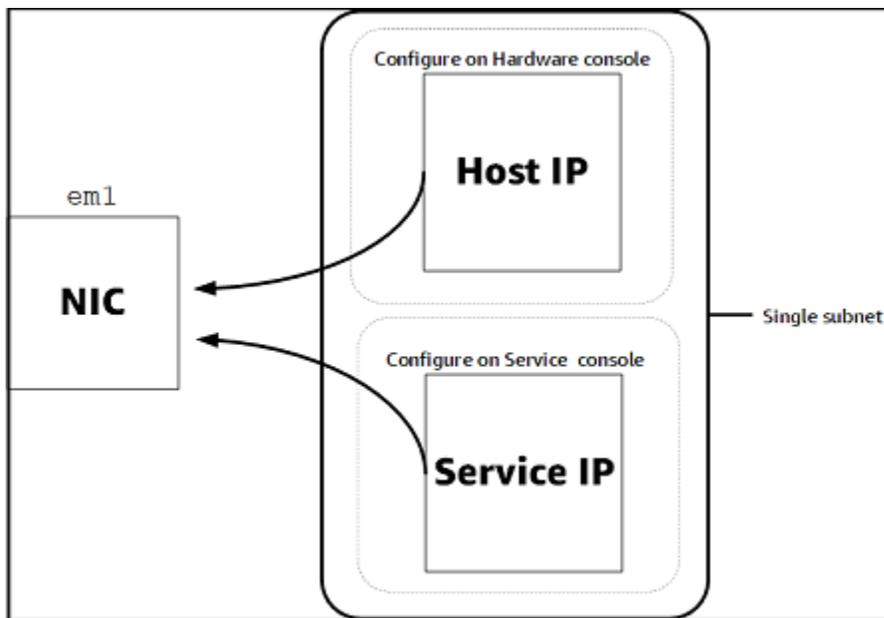
- 하드웨어 콘솔에서 연결된 모든 네트워크 인터페이스를 구성합니다.
- 각 네트워크 인터페이스는 고유한 서브넷에 있어야 합니다.
- 연결된 모든 네트워크 인터페이스에 위의 그림에 나와 있는 엔드포인트에 대한 아웃바운드 액세스를 제공합니다.

- 하드웨어 어플라이언스를 지원하는 네트워크 인터페이스를 한 개 이상 구성합니다. 자세한 정보는 [네트워크 파라미터 구성](#)을 참조하십시오.

Note

서버 뒷면과 포트가 나와 있는 그림을 보려면 단원을 참조하십시오. [하드웨어 어플라이언스를 랙 장착하고 전원에 연결.](#)

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



하드웨어 어플라이언스 활성화 및 구성에 대한 자세한 내용은 단원을 참조하십시오. [Storage Gateway 하드웨어 어플라이언스 사용.](#)

AWS Storage Gateway가 방화벽 및 라우터를 통해 액세스할 수 있도록 허용

통신하려면 게이트웨이에서 다음 서비스 엔드포인트에 액세스할 수 있어야 합니다. AWS. 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링하거나 제한하는 경우, 방화벽 및 라우터가 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. AWS.

⚠ Important

게이트웨이에 따라 다른 AWS 지역, 바꾸기 ## 올바른 Region 문자열이 있는 서비스 엔드포인트에서.

다음 서비스 엔드포인트는 모든 게이트웨이에서 헤드 버킷 작업에 필요합니다.

```
s3.amazonaws.com:443
```

제어 경로에 대한 모든 게이트웨이에서 다음 서비스 엔드포인트가 필요합니다 (anon-cp, client-cp, proxy-app) 및 데이터 경로 (dp-1) 작업.

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

다음 게이트웨이 서비스 엔드포인트는 API 호출에 필요합니다.

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

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

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

다음 Amazon CloudFront 엔드포인트는 Storage Gateway 사용 가능한 목록을 가져오는 데 필요합니다.AWS 지역.

```
https://d4kdq0yaxexbo.cloudfront.net/
```

Storage Gateway VM은 다음 NTP 서버를 사용하도록 구성됩니다.

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

- 스토리지 게이트웨이 - 지원 대상AWS지역 및 목록AWSStorage Gateway 함께 사용할 수 있는 서비스 엔드포인트는 단원을 참조하십시오.[AWS Storage Gateway엔드포인트 및 할당량](#)의AWS일반 참조.
- Storage Gateway 하드웨어 어플라이언스 지원AWS하드웨어 어플라이언스와 함께 사용할 수 있는 리전은 단원을 참조하십시오.[Storage Gateway 하드웨어 어플라이언스 지역](#)의AWS일반 참조.

Amazon EC2 게이트웨이 인스턴스에 대한 보안 그룹 구성

InAWS Storage Gateway보안 그룹은 Amazon EC2 게이트웨이 인스턴스로 가는 트래픽을 제어합니다. 보안 그룹을 구성할 때는 다음을 수행하는 것이 좋습니다.

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

인스턴스가 보안 그룹 외부에서 게이트웨이에 연결해야 하는 경우에는 포트 80으로 연결해야 하는 것이 좋습니다 (활성화용).

- 게이트웨이 보안 그룹 외부에 있는 Amazon EC2 호스트에서 게이트웨이를 활성화하려면 해당 호스트의 IP 주소에서 포트 80으로 들어오는 연결을 허용합니다. 활성화 호스트의 IP 주소를 확인할 수 없는 경우에는 포트 80을 열어 게이트웨이를 활성화하고 활성화가 완료되면 포트 80에 대한 액세스를 종료하는 방법을 사용할 수 있습니다.
- 포트 22 액세스는 문제 해결 목적으로 지원을 사용하는 경우에만 허용하십시오. 자세한 정보는 [당신이 원한다지원EC2 게이트웨이 문제를 해결하는 데 도움이 됩니다](#)을 참조하십시오.

지원되는 하이퍼바이저 및 호스트 요구 사항

Storage Gateway를 온프레미스에서 가상 머신 (VM) 어플라이언스 또는 물리적 하드웨어 어플라이언스로 실행하거나AWSAmazon EC2 인스턴스로 사용할 수 있습니다.

Storage Gateway는 다음과 같은 하이퍼바이저 버전 및 호스트

- VMware ESXi Hypervisor (버전 6.0, 6.5 또는 6.7) — VMware 무료 버전은[VMware 웹사이트](#). 이 설정의 경우 호스트에 연결하려면 VMware vSphere 클라이언트도 필요합니다.
- Microsoft Hyper-V Hypervisor (버전 2012 R2 또는 2016) — Hyper-V의 무료 독립형 버전은[마이크로소프트 다운로드 센터](#). 이 설정의 경우 호스트에 연결하려면 Microsoft Windows 클라이언트 컴퓨터에서 Microsoft Hyper-V Manager를 사용해야 합니다.

- Linux 커널 기반 가상 머신 (KVM) — 무료 오픈 소스 가상화 기술입니다. KVM은 모든 버전의 Linux 버전 2.6.20 이상에 포함되어 있습니다. Storage Gateway는 CentOS/RHEL 7.7, Ubuntu 16.04 LTS 및 Ubuntu 18.04 LTS 배포판에 대해 테스트되고 지원됩니다. 다른 최신 Linux 배포판이 작동하지만 기능이나 성능이 보장되지는 않습니다. KVM 환경이 이미 가동되고 있고 KVM 작동 방식에 익숙하다면 이 옵션을 사용하는 것이 좋습니다.
- Amazon EC2 인스턴스 — Storage Gateway VM 이미지를 포함하는 Amazon Machine Image (AMI)를 제공합니다. Amazon EC2 게이트웨이를 배포하는 방법에 대한 자세한 내용은 단원을 참조하십시오. [Amazon EC2 호스트에 파일 게이트웨이 배포](#).
- Storage Gateway 하드웨어 어플라이언스 — Storage Gateway는 제한된 가상 머신 인프라 위치에 대한 온프레미스 배포 옵션으로 물리적 하드웨어 어플라이언스

Note

Storage Gateway는 다른 게이트웨이 VM의 스냅샷이나 복제 또는 Amazon EC2 AMI로부터 생성된 VM의 게이트웨이를 복구하는 기능을 지원하지 않습니다. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 새로운 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다. 자세한 정보는 [여기](#) [키워드](#) [가상 시스템 종료에서 복구](#)를 참조하십시오. Storage Gateway는 동적 메모리 및 가상 메모리 벌루닝을 지원하지 않습니다.

파일 게이트웨이에 지원되는 SMB 클라이언트

파일 게이트웨이는 다음 SMB(Service Message Block) 클라이언트를 지원합니다.

- Microsoft Windows Server 2008 이상
- Windows 데스크톱 버전: 10, 8 및 7입니다.
- Windows Server 2008 이상에서 실행 중인 Windows Terminal Server

Note

서버 메시지 블록 암호화에는 SMB v2.1을 지원하는 클라이언트가 필요합니다.

파일 게이트웨이에 지원되는 파일 시스템 작업

SMB 클라이언트는 파일에 대해 쓰기, 읽기, 삭제 및 자르기 작업을 할 수 있습니다. 클라이언트가 Storage Gateway에 쓰기 작업을 전송하면 로컬 캐시에 동기 방식으로 기록됩니다. 그런 다음 최적의 전송 방법을 통해 Amazon FSx 에 비동기 방식으로 작성합니다. 읽기 작업은 처음에 로컬 캐시를 통해 이루어집니다. 데이터를 사용할 수 없는 경우 Amazon FSx 를 통해 읽기 캐시로 가져옵니다.

쓰기 및 읽기는 변경되거나 요청된 부분만 게이트웨이를 통해 전송되는 방법으로 최적화됩니다. Amazon FSx에서 제거 파일을 삭제합니다.

AWS Storage Gateway에 액세스

이 [AWS Storage Gateway 콘솔](#) 다양한 게이트웨이 구성 및 관리 작업을 수행합니다. 이 설명서의 시작하기 단원 및 다양한 기타 단원에서는 콘솔을 사용하여 게이트웨이 기능을 설명합니다.

콘솔뿐 아니라 AWS Storage Gateway API를 사용하여 게이트웨이를 프로그래밍 방식으로 구성 및 관리할 수도 있습니다. API에 대한 자세한 내용은 [API 참조](#)를 참조하십시오.

뿐만 아니라 AWS SDK를 사용하면 Storage Gateway 상호 작용하는 애플리케이션을 개발할 수 있습니다. 이 AWS Java, .NET 및 PHP용 SDK는 프로그래밍 작업을 간소화하며 기본 Storage Gateway API를 포함합니다. SDK 라이브러리 다운로드에 대한 자세한 내용은 단원을 참조하십시오. [AWS 개발자 센터](#).

요금에 대한 자세한 정보는 [AWS Storage Gateway 요금](#)을 참조하십시오.

지원되는 AWS 리전

Amazon FSx 파일 게이트웨이는 파일 데이터를 AWS Amazon FSx 파일 시스템이 위치한 리전입니다. 게이트웨이 배포를 시작하기 전에 Storage Gateway 콘솔의 오른쪽 상단에 있는 리전을 선택합니다.

- Amazon FSx 파일 게이트웨이 — 지원되는 경우 AWS 지역 및 목록 AWS Amazon FSx 파일 게이트웨이와 함께 사용할 수 있는 서비스 엔드포인트는 단원을 참조하십시오. [Amazon FSx 파일 게이트웨이 엔드포인트 및 할당량](#)의 AWS 일반 참조.
- Storage Gateway — 지원 대상 AWS 지역 및 목록 AWS Storage Gateway 함께 사용할 수 있는 서비스 엔드포인트는 단원을 참조하십시오. [AWS Storage Gateway 엔드포인트 및 할당량](#)의 AWS 일반 참조.
- Storage Gateway 하드웨어 어플라이언스 — 하드웨어 어플라이언스와 함께 사용할 수 있는 지원되는 리전은 단원을 참조하십시오. [AWS Storage Gateway 하드웨어 어플라이언스 영역](#)의 AWS 일반 참조.

Storage Gateway 하드웨어 어플라이언스 사용

Storage Gateway 하드웨어 어플라이언스에 Storage Gateway 소프트웨어가 사전 설치된 서버 구성에 사전 설치된 물리적 하드웨어 어플라이언스입니다. 에서 하드웨어 어플라이언스를 관리할 수 있습니다. Hardware(하드웨어)의 페이지 AWS Storage Gateway 콘솔.

하드웨어 어플라이언스에 데이터 센터 또는 회사 방화벽 내 온프레미스에 배포할 수 있는 고성능 1U 서버입니다. 하드웨어 어플라이언스를 구입하여 활성화하면 활성화 프로세스에서는 하드웨어 어플라이언스와 해당 어플라이언스를 연결합니다. AWS 계정. 정품 인증 후 하드웨어 어플라이언스가 콘솔에 게이트웨이로 나타납니다. Hardware(하드웨어) 페이지 하드웨어 어플라이언스를 파일 게이트웨이, 테이프 게이트웨이, 볼륨 게이트웨이 유형 등으로 구성할 수 있습니다. 하드웨어 어플라이언스에 이러한 게이트웨이 유형을 배포하고 활성화하는 절차는 가상 플랫폼에서의 절차와 동일합니다.

Storage Gateway 하드웨어 어플라이언스는 AWS Storage Gateway 콘솔.

하드웨어 어플라이언스를 주문하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home> 를 선택하고 AWS 어플라이언스를 연결할 리전.
2. 선택 Hardware(하드웨어) 탐색 창에서.
3. 선택 어플라이언스를 선택한 다음 를 선택합니다. 계속하기. 로 리디렉션됩니다. AWS Elemental 어플라이언스 및 소프트웨어 관리 콘솔에서 판매 견적을 요청합니다.
4. 필요한 정보를 기입하고 제출.

정보가 검토되면 판매 견적이 생성되고 주문 프로세스를 진행하고 구매 발주를 제출하거나 선불 준비를 할 수 있습니다.

하드웨어 어플라이언스에 대한 판매 견적 또는 주문 내역을 보려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 선택 Hardware(하드웨어) 탐색 창에서.
3. 선택 견적 및 주문을 선택한 다음 를 선택합니다. 계속하기. 로 리디렉션됩니다. AWS Elemental 어플라이언스 및 소프트웨어 관리 콘솔로 판매 견적 및 주문 내역을 검토합니다

다음 단원에서는 Storage Gateway 하드웨어 어플라이언스를 설정, 구성, 활성화, 시작 및 사용하는 방법에 관한 지침을 확인할 수 있습니다.

주제

- [지원되는 AWS 리전](#)
- [하드웨어 어플라이언스 설정](#)
- [하드웨어 어플라이언스를 랙 장착하고 전원에 연결](#)
- [네트워크 파라미터 구성](#)
- [하드웨어 어플라이언스 활성화](#)
- [게이트웨이 시작](#)
- [게이트웨이에 대한 IP 주소 구성](#)
- [게이트웨이 구성](#)
- [하드웨어 어플라이언스에서 게이트웨이 제거](#)
- [하드웨어 어플라이언스 삭제](#)

지원되는 AWS 리전

Storage Gateway 하드웨어 어플라이언스는 미국 정부가 합법적으로 허용하고 수출할 수 있는 전 세계 배송에 사용할 수 있습니다. 지원되는 에 대한 자세한 내용AWS지역, 참조[Storage Gateway 하드웨어](#)의AWS일반 참조.

하드웨어 어플라이언스 설정

Storage Gateway 하드웨어 어플라이언스를 수령한 후 하드웨어 어플라이언스 콘솔을 사용하여 네트워크에서 상시 연결을 제공하도록 구성합니다.AWS어플라이언스를 활성화합니다. 정품 인증은 어플라이언스를AWS정품 인증 프로세스 중에 사용되는 계정입니다. 어플라이언스가 활성화되면 Storage Gateway 콘솔에서 파일, 볼륨 또는 테이프 게이트웨이를 시작할 수 있습니다.

하드웨어 어플라이언스를 설치 및 구성하려면

1. 어플라이언스를 랙 마운팅하고 전원과 네트워크 연결을 가동합니다. 자세한 정보는 [하드웨어 어플라이언스를 랙 장착하고 전원에 연결](#)을 참조하십시오.
2. 하드웨어 어플라이언스 (호스트) 및 Storage Gateway (서비스) 에 대한 인터넷 프로토콜 버전 4 (IPv4) 주소를 설정합니다. 자세한 정보는 [네트워크 파라미터 구성](#)을 참조하십시오.
3. 콘솔에서 하드웨어 어플라이언스 활성화Hardware(하드웨어)의 페이지AWS원하는 지역입니다. 자세한 정보는 [하드웨어 어플라이언스 활성화](#)을 참조하십시오.

4. 하드웨어 어플라이언스에 Storage Gateway 설치합니다. 자세한 정보는 [게이트웨이 구성](#)을 참조 하십시오.

VMware ESXi, Microsoft Hyper-V, Linux 커널 기반 가상 머신 (KVM) 또는 Amazon EC2 EC2에서 게이트웨이를 설정하는 것과 동일한 방식으로 하드웨어 어플라이언스에 게이트웨이를 설정합니다.

사용 가능한 캐시 스토리지 증가

하드웨어 어플라이언스의 사용 가능 스토리지를 5TB에서 12TB로 늘릴 수 있습니다. 대용량 캐시를 제공하므로 에서 데이터에 액세스할 때 지연 시간이 짧습니다.AWS. 5TB 모델을 주문한 경우 콘솔에서 주문할 수 있는 1.92TB SSD (Solid State Drive) 를 5개 구입하면 됩니다.Hardware(하드웨어)페이지 하드웨어 어플라이언스를 주문하고 Storage Gateway 콘솔에서 판매 견적을 요청하는 것과 동일한 주문 프로세스를 수행하여 추가 SSD를 주문할 수 있습니다.

그런 다음 활성화하기 전에 하드웨어 어플라이언스에 추가할 수 있습니다. 하드웨어 어플라이언스를 이미 활성화한 후 어플라이언스의 사용 가능 스토리지를 12TB로 늘리려면 다음과 같이 하십시오.

1. 하드웨어 어플라이언스를 초기 기본 설정으로 재설정합니다. 연락처AWS작업 방법에 대한 지침이 Support.
2. 1.92TB SSD 5개를 어플라이언스에 추가합니다.

네트워크 인터페이스 카드

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

- 10G 베이스-T NIC 구성:
 - 10G에 CAT6 케이블을 사용하거나 1G에는 CAT5 (e) 를 사용합니다.
- 10G 다/SFP+ 닉 구성:
 - Twinax 구리 직접 연결 케이블 최대 5m 사용
 - Dell/인텔 호환 SFP+ 광 모듈 (SR 또는 LR)
 - 1G 베이스-T 또는 10G 베이스-T용 SFP/SFP+ 구리 트랜시버

하드웨어 어플라이언스를 랙 장착하고 전원에 연결

Storage Gateway 하드웨어 어플라이언스의 박스를 개봉한 후 해당 지침에 따라 서버를 랙 마운팅합니다. 어플라이언스에 1U 폼 팩터가 있고 IEC (국제 전자기술 위원회) 규격 19인치 랙에 맞습니다.

하드웨어 어플라이언스를 설치하려면 다음 구성 요소가 필요합니다.

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

하드웨어 어플라이언스

하드웨어 어플라이언스를 전원에 연결하려면

Note

다음 절차를 수행하기 전에 에서 설명하는 Storage Gateway 하드웨어 어플라이언스에 대한 모든 요구 사항을 충족하는지 확인하십시오. [Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항](#).

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

다음 그림에는 각기 다른 연결이 있는 하드웨어 어플라이언스가 나와 있습니다.

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 어플라이언스가 VLAN 트렁킹을 지원하지 않습니다. 하드웨어 어플라이언스를 트렁크 모드가 아닌 VLAN 포트에 연결하려는 스위치 포트를 설정합니다.

3. 키보드 및 모니터를 연결합니다.

4. 다음 이미지와 같이 앞면 패널에 있는 전원 버튼을 눌러 서버를 켭니다.

서버가 부팅되면 하드웨어 콘솔이 모니터에 표시됩니다. 하드웨어 콘솔에 다음과 같은 사용자 인터페이스가 표시됩니다. AWS를 사용하여 초기 네트워크 파라미터를 구성할 수 있습니다. 기기를 연결하도록 이러한 매개 변수를 구성합니다. AWS 다음과 같이 문제 해결을 위해 지원 채널을 열려면 AWS Support.

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.

이 시점에서 하드웨어 콘솔이 다음과 같이 표시됩니다.

다음 단계

[네트워크 파라미터 구성](#)

네트워크 파라미터 구성

서버 부팅 이후 [하드웨어 어플라이언스를 랙 장착하고 전원 연결](#)에서 설명하는 것과 같이 하드웨어 콘솔에서 최초 암호를 입력합니다.

다음으로 하드웨어 콘솔에서 다음 단계를 수행하여 하드웨어 어플라이언스에 연결할 수 있도록 네트워크 파라미터를 구성합니다. AWS.

네트워크 주소를 설정하려면

1. 네트워크 구성을 선택하고 Enter 키를 누릅니다. 다음과 같이 네트워크 구성 화면이 표시됩니다.

2. IP 주소에서 다음 소스 중 하나로부터 유효한 IPv4 주소를 입력합니다.

- DHCP(Dynamic Host Configuration Protocol) 서버에 의해 물리 네트워크로 할당된 IPv4 주소를 사용합니다.

이를 수행한 경우 향후 활성화 단계에서 사용하도록 이 IPv4 주소를 적어두십시오.

- 정적 IPv4 주소를 할당합니다. 이렇게 하려면 를 선택합니다.고정의em1섹션 및 클릭Enter다음과 같이 Configuration IP 구성 화면을 표시합니다.

em1 섹션은 설정 그룹의 왼쪽 상단에 있습니다.

유효한 IPv4 주소를 입력한 후 Down arrow 또는 Tab 키를 누릅니다.

Note

다른 인터페이스를 구성할 경우 해당 인터페이스가 에 대한 상시 연결을 제공해야 합니다.AWS요구 사항에 나열된 엔드포인트입니다.

3. 서브넷에 유효한 서브넷 마스크를 입력한 후 Down arrow를 누릅니다.
4. 소스에 네트워크 게이트웨이의 IPv4 주소를 입력한 후 Down arrow를 누릅니다.
5. DNS1에 DNS(Domain Name Service) 서버에 대한 IPv4 주소를 입력한 후 Down arrow를 누릅니다.
6. (선택 사항) DNS2에 두 번째 IPv4 주소를 입력한 후 Down arrow를 누릅니다. 두 번째 DNS 서버를 할당하면 첫 번째 DNS 서버를 사용할 수 없을 때 중복성이 강화됩니다.
7. 저장을 선택한 후 Enter 키를 눌러 어플라이언스에 대한 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

다음에 설명된 대로 IP 주소를 구성한 후 콘솔의 하드웨어 페이지에 이 IP 주소를 입력합니다. 정품 인증 프로세스에서는 하드웨어 어플라이언스에 적절한 보안 자격 증명이 있는지 확인하고 어플라이언스를 에 등록합니다.AWS계정.

지원되는 어플라이언스에서 하드웨어 어플라이언스를 활성화하도록 선택할 수 있습니다.AWS리전. 지원되는 목록AWS지역, 참조[Storage Gateway 하드웨어](#)의AWS일반 참조.

어플라이언스를 처음으로 활성화하거나AWS게이트웨이가 배포되지 않은 리전

1. 에 로그인합니다.AWS Management Console에서 Storage Gateway 콘솔을 엽니다.[AWS Storage Gateway관리 콘솔](#)하드웨어를 활성화하는 데 사용할 계정 자격 증명을 사용합니다.

이것이 첫 번째 게이트웨이인 경우AWS리전, 스플래시 화면이 표시됩니다. 에서 게이트웨이를 생성한 후AWS지역에서는 화면이 더 이상 표시되지 않습니다.

Note

활성화를 위해서는 다음이 충족되어야 합니다.

- 브라우저가 하드웨어 어플라이언스와 동일한 네트워크에 있어야 합니다.
- 방화벽이 인바운드 트래픽에 대해 어플라이언스에 포트 8080에서 HTTP에 액세스하도록 허용해야 합니다.

2. 다음과 같이 시작하기를 선택하여 게이트웨이 마법사를 표시한 다음 호스트 플랫폼 선택 페이지에서 Hardware Appliance(하드웨어 어플라이언스)를 선택합니다.
3. 다음을 선택하여 다음과 같이 Connect to hardware(하드웨어에 연결) 화면을 표시합니다.
4. 용IP 주소의하드웨어 어플라이언스 Connect단원을 통해 어플라이언스의 IPv4 주소를 입력한 다음연결다음과 같이 를 클릭하여 하드웨어 활성화 화면으로 이동합니다.
5. Hardware name(하드웨어 이름)에 어플라이언스의 이름을 입력합니다. 이름은 최대 255자 길이며 스플래시 문자를 포함할 수 없습니다.
6. 용하드웨어 시간대에서 로컬 설정을 입력합니다.

시간대는 하드웨어 업데이트가 수행되는 시간을 제어하며, 현지 시간 오전 2시가 업데이트 시간으로 사용됩니다.

Note

표준 업데이트 시간이 일반 업무일이 아닌 시간으로 지정되도록 어플라이언스에 대한 시간대를 설정하는 것이 좋습니다.

7. (선택 사항) RAID Volume Manager를 ZFS로 설정된 상태로 둡니다.

ZFS는 더 나은 성능과 데이터 보호를 제공하기 위해 하드웨어 어플라이언스에서 RAID 볼륨 관리자로 사용됩니다. ZFS는 소프트웨어 기반 오픈 소스 파일 시스템이며 논리적 볼륨 관리자입니다. 하드웨어 어플라이언스는 ZFS RAID에 맞게 특정하게 조정됩니다. ZFS RAID에 대한 자세한 내용은 [ZFS Wikipedia 페이지](#)를 참조하십시오.

8. 다음을 선택하여 활성화를 완료합니다.

다음과 같이 하드웨어 어플라이언스가 활성화되었음을 나타내는 콘솔 배너가 하드웨어 페이지에 나타납니다.

이제 어플라이언스가 계정에 연결됩니다. 다음 단계에서는 어플라이언스에서 파일, 테이프 또는 캐싱된 볼륨 게이트웨이를 시작합니다.

다음 단계

[게이트웨이 시작](#)

게이트웨이 시작

어플라이언스에서 파일 게이트웨이, 볼륨 게이트웨이 (캐시) 또는 테이프 게이트웨이의 세 가지 스토리지 게이트웨이 중 하나를 시작할 수 있습니다.

하드웨어 어플라이언스에서 게이트웨이를 시작하려면

1. [에 로그인합니다.](https://console.aws.amazon.com/storagegateway/home) AWS Management Console에서 Storage Gateway 콘솔을 엽니다. <https://console.aws.amazon.com/storagegateway/home>.
2. 하드웨어를 선택합니다.
3. 작업에서 Launch Gateway(게이트웨이 시작)를 선택합니다.
4. 게이트웨이 유형에서 파일 게이트웨이, 테이프 게이트웨이 또는 볼륨 게이트웨이(캐시됨)를 선택합니다.

5. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 이름은 255자 길이이며 스페이스 문자를 포함할 수 없습니다.
6. Launch gateway(게이트웨이 시작)를 선택합니다.

선택한 게이트웨이 유형에 대한 Storage Gateway 소프트웨어가 어플라이언스에 설치됩니다. 게이트웨이가 다음과 같이 표시되는 데 최대 5~10분이 걸릴 수 있습니다.온라인콘솔에서.

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. 어플라이언스를 활성화하고 스토리지 게이트웨이를 시작했으므로 하드웨어 어플라이언스에서 실행되는 Storage Gateway 가상 시스템에 다른 IP 주소를 할당해야 합니다. 하드웨어 어플라이언스에 설치된 게이트웨이에 고정 IP 주소를 할당하려면 해당 게이트웨이에 대한 로컬 콘솔에서 IP 주소를 구성합니다. 애플리케이션(예: NFS 또는 SMB 클라이언트, iSCSI 초기자 등)이 IP 주소에 연결됩니다. 하드웨어 어플라이언스 콘솔에서 게이트웨이 로컬 콘솔에 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 admin이고 기본 암호는 password입니다.

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 [하드웨어 어플라이언스를 랙 장착하고 전원](#)에 연결 단원을 참조하세요.
5. 다음과 같이 게이트웨이 로컬 콘솔의 네트워크 설정 페이지로 이동합니다.
6. 다음과 같이 2를 입력하여 Network Configuration(네트워크 구성) 페이지로 이동합니다.

- 어플라이언스에 파일, 볼륨 및 테이프 게이트웨이를 제공하려면 하드웨어 어플라이언스에서 네트워크 포트에 대한 고정 또는 DHCP IP 주소를 구성합니다. 이 IP 주소는 하드웨어 어플라이언스 활성화 중에 사용한 IP 주소와 동일한 서브넷에 있어야 합니다.

게이트웨이 로컬 콘솔을 종료하려면

- Ctrl+] (달는 대괄호) 키를 누릅니다. 하드웨어 콘솔이 표시됩니다.

Note

키 입력을 통해서만 게이트웨이 로컬 콘솔을 종료할 수 있습니다.

다음 단계

[게이트웨이 구성](#)

게이트웨이 구성

하드웨어 어플라이언스를 활성화하여 구성하면 어플라이언스가 콘솔에 나타납니다. 이제 원하는 게이트웨이의 유형을 생성할 수 있습니다. 게이트웨이 유형에 대한 설치를 계속합니다. 지침은 [Amazon FSx 파일 게이트웨이 구성](#) 단원을 참조하세요.

하드웨어 어플라이언스에서 게이트웨이 제거

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

하드웨어 어플라이언스에서 게이트웨이를 제거하려면

- 게이트웨이에 대한 확인란을 선택합니다.
- 작업에서 Remove Gateway(게이트웨이 제거)를 선택합니다.
- 에서 하드웨어 어플라이언스에서 게이트웨이 제거대화 상자에서 확인.

Note

게이트웨이를 삭제할 경우 작업을 취소할 수 없습니다. 특정 게이트웨이 유형의 경우 삭제 시 데이터 특히, 캐싱된 데이터를 잃을 수 있습니다. 게이트웨이 삭제에 대한 자세한 내용은 [AWS Storage Gateway 콘솔을 사용한 게이트웨이 삭제와 연결된 리소스 제거 단원을](#) 참조하십시오.

게이트웨이를 삭제해도 하드웨어 어플라이언스가 콘솔에서 삭제되지 않습니다. 하드웨어 어플라이언스가 향후 게이트웨이 배포를 위해 유지됩니다.

하드웨어 어플라이언스 삭제

하드웨어 어플라이언스를 활성화한 후 AWS 계정을 이동한 후 활성화해야 할 수도 있습니다. AWS 계정. 이 경우 먼저 에서 어플라이언스를 삭제합니다. AWS 계정 및 다른 계정에서 활성화 AWS 계정. 에서 어플라이언스를 완전히 삭제할 수도 있습니다. AWS 계정은 더 이상 필요 없기 때문입니다. 하드웨어 어플라이언스를 삭제하려면 다음 지침을 따르십시오.

하드웨어 어플라이언스를 삭제하려면

1. 하드웨어 어플라이언스에 게이트웨이를 설치한 경우 먼저 게이트웨이를 제거해야 어플라이언스를 삭제할 수 있습니다. 하드웨어 어플라이언스에서 게이트웨이를 제거하는 방법은 단원을 참조하십시오. [하드웨어 어플라이언스에서 게이트웨이 제거](#).
2. 하드웨어 페이지에서 삭제할 하드웨어 어플라이언스를 선택합니다.
3. 작업에서 어플라이언스 삭제를 선택합니다.
4. 리소스 삭제 확인 대화 상자에서 확인용 확인란을 선택하고 삭제를 선택합니다. 성공적으로 삭제되었다는 메시지가 표시됩니다.

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

AWS Storage Gateway 시작하기

이 단원에서는 파일 게이트웨이를 생성하고 활성화하는 방법에 대한 지침을 얻을 수 있습니다. AWS Storage Gateway. 시작하기 전에 [에 설명된 필수 구성 요소 및 기타 요구 사항을 충족해야 합니다.](#) [Amazon FSx 파일 게이트웨이에 대한 설정.](#)

주제

- [1단계: Amazon FSx for Windows File Server 파일 시스템 생성](#)
- [2단계: \(선택 사항\) Amazon VPC 엔드포인트 생성](#)
- [3단계: Amazon FSx 파일 게이트웨이 생성 및 활성화](#)

1단계: Amazon FSx for Windows File Server 파일 시스템 생성

에서 Amazon FSx 파일 게이트웨이를 생성하려면 AWS Storage Gateway 첫 번째 단계는 Amazon FSx for Windows File Server 파일 시스템을 생성하는 것입니다. Amazon FSx 파일 시스템을 이미 생성한 경우 다음 단계로 진행합니다. [2단계: \(선택 사항\) Amazon VPC 엔드포인트 생성.](#)

Note

FSx 파일 게이트웨이에서 Amazon FSx 파일 시스템에 쓸 때 다음 제한 사항이 적용됩니다.

- Amazon FSx 파일 시스템과 FSx 파일 게이트웨이는 동일한 사용자가 소유해야 합니다. AWS 계정과 동일한 위치에 있습니다. AWS 리전.
- 각 게이트웨이는 5개의 연결된 파일 시스템을 지원할 수 있습니다. 파일 시스템을 연결할 때 Storage Gateway 콘솔은 선택한 게이트웨이의 용량에 해당하는지 알려줍니다. 이 경우 다른 게이트웨이를 연결하려면 먼저 다른 게이트웨이를 선택하거나 파일 시스템을 분리해야 합니다.
- FSx File Gateway는 소프트 스토리지 할당량 (사용자가 데이터 한도를 초과할 때 경고 발생)을 지원하지만 하드 할당량을 지원하지 않습니다 (쓰기 액세스를 거부하여 데이터 제한 적용). 소프트 할당량은 Amazon FSx 관리자 사용자를 제외한 모든 사용자에게 지원됩니다. 저장소 할당량 설정에 대한 자세한 내용은 단원을 참조하십시오. [스토리지 할당량](#)의 Amazon FSx for Windows File Server 사용 설명서.

FSx for Windows File Server 파일 시스템을 생성하려면

1. 열기AWS Management Console...에서<https://console.aws.amazon.com/fsx/home/>에서 게이트웨이를 생성할 리전을 선택합니다.
2. 의 지침을 따르십시오.[Amazon FSx 시작하기](#)의Amazon FSx for Windows File Server 사용 설명서.

2단계: (선택 사항) Amazon VPC 엔드포인트 생성

에서 Amazon FSx 파일 게이트웨이를 생성하는 경우에는 이 단계가 필요하지 않습니다.AWS Storage Gateway. 그러나 Storage Gateway 위한 Virtual Private Cloud (VPC) 엔드포인트를 생성하고 VPC에서 게이트웨이를 활성화하는 것이 좋습니다. 이렇게 하면 VPC와 Storage Gateway 간에 프라이빗 연결이 생성됩니다.

Storage Gateway 위한 VPC 엔드포인트가 이미 있는 경우 FSx 파일 게이트웨이에 사용할 수 있습니다. 여러 게이트웨이를 지원할 수 있는 단일 VPC 엔드포인트를 사용하면 VPC 배포된 게이트웨이를 Storage Gateway 서비스 VPC 연결할 수 있습니다. 이미 Storage Gateway 위한 VPC 엔드포인트를 생성한 경우 다음 단계로 진행합니다.[3단계: Amazon FSx 파일 게이트웨이 생성 및 활성화.](#)

Amazon VPC 엔드포인트를 생성하려면

1. 열기AWS Management Console...에서<https://console.aws.amazon.com/vpc/home/>를 선택하고 AWS게이트웨이를 생성하려는 리전.
2. 왼쪽 탐색 창에서 를 선택합니다.엔드포인트를 선택한 다음 를 선택합니다.엔드포인트 생성.
3. 온엔드포인트 생성페이지, 선택AWS서비스...에 대한서비스 범주.
4. 용서비스 이름을 열려면storagegateway. 리전은 로그인한 리전으로 기본 설정됩니다. 예를 들어,com.amazonaws.*region*.storagegateway. 따라서 미국 동부 (오하이오) 에 로그인하면com.amazonaws.us-east-2.storagegateway.
5. VPC에서 VPC를 선택하고 해당 가용 영역 및 서브넷을 기록합니다.
6. 프라이빗 DNS 이름 활성화가 선택되지 않았는지 확인합니다.
7. 용보안 그룹에서 VPC와 함께 사용할 새 보안 그룹을 생성합니다. 다음 모든 TCP 포트가 보안 그룹에서 허용되는지 확인합니다.
 - TCP 1026
 - TCP 1027
 - TCP 1028

- TCP 1031
- TCP 2222

 Note

게이트웨이는 이러한 포트를 사용하여 Storage Gateway 관리 서비스로 다시 통신합니다. VPC 엔드포인트를 사용하는 경우 게이트웨이의 IP 주소에서 인바운드 액세스를 위해 다음 포트가 열려 있어야 합니다.

8. 엔드포인트 생성을 선택합니다. 엔드포인트의 초기 상태는 다음과 같습니다. 대기 중. 엔드포인트가 생성되면 방금 생성한 VPC 엔드포인트의 ID를 기록합니다.

 Note

이 VPC 엔드포인트의 이름을 제공하는 것이 좋습니다 (예: **StorageGatewayEndpoint**).

9. 엔드포인트가 생성되면 다음을 선택합니다. 엔드포인트를 선택한 다음 새 항목을 선택합니다. VPC 엔드포인트.
10. 에서 DNS 이름 섹션에서 가용 영역을 지정하지 않은 최초의 DNS (Domain Name System) 이름을 사용합니다. DNS 이름은 다음과 같아야 합니다.

```
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

 Note

이 DNS 이름은 VPC 할당된 Storage Gateway 엔드포인트 프라이빗 IP 주소로 확인됩니다.

11. 방화벽에서 열어야 하는 포트 목록을 검토합니다.

VPC 엔드포인트를 생성했으므로 FSx 파일 게이트웨이를 생성할 수 있습니다.

다음 단계

[the section called “3단계: FSx 파일 게이트웨이 게이트웨이 생성 및 활성화”](#)

3단계: Amazon FSx 파일 게이트웨이 생성 및 활성화

이 단원에서는 파일 게이트웨이를 생성, 배포 및 활성화하는 방법에 대한 지침을 얻을 수 있습니다. AWS Storage Gateway.

주제

- [Amazon FSx 파일 게이트웨이 설정](#)
- [Amazon FSx 파일 게이트웨이를 AWS](#)
- [설정을 검토하고 Amazon FSx 파일 게이트웨이 활성화](#)
- [Amazon FSx 파일 게이트웨이 구성](#)

Amazon FSx 파일 게이트웨이 설정

새 FSx 파일 게이트웨이를 설정하려면

1. 열기 AWS Management Console...에서 <https://console.aws.amazon.com/storagegateway/home/>를 선택하고 AWS 리전 게이트웨이를 생성하려는 위치에 있습니다.
2. 선택 게이트웨이 생성을 열려면 게이트웨이 설정 페이지.
3. 에서 게이트웨이 설정 섹션에서 다음을 수행합니다.
 - a. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 게이트웨이가 생성되면 이 이름을 검색하여 의 목록 페이지에서 게이트웨이를 찾을 수 있습니다. AWS Storage Gateway 콘솔.
 - b. 용 게이트웨이 시간대 게이트웨이를 배포하려는 전 세계 지역의 현지 시간대를 선택합니다.
4. 에서 게이트웨이 옵션 섹션, 게이트웨이 유형, 선택 Amazon FSx 파일 게이트웨이.
5. 에서 플랫폼 옵션 섹션에서 다음을 수행합니다.
 - a. 옹 호스트 플랫폼에서 게이트웨이를 배포하고 싶은 플랫폼을 선택합니다. 그런 다음 Storage Gateway 콘솔 페이지에 표시된 플랫폼별 지침에 따라 호스트 플랫폼을 설정합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - VMware ESXi— VMware ESXi를 사용하여 게이트웨이 가상 시스템을 다운로드, 배포 및 구성합니다.
 - Microsoft Hyper-V— Microsoft Hyper-V를 사용하여 게이트웨이 가상 컴퓨터를 다운로드, 배포 및 구성합니다.
 - Linux KVM— Linux 커널 기반 가상 머신 (KVM) 을 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.

- Amazon EC2— 게이트웨이를 호스팅하도록 Amazon EC2 인스턴스를 구성하고 시작합니다.
 - 하드웨어 어플라이언스— 전용 물리적 하드웨어 어플라이언스 주문AWS게이트웨이를 호스팅합니다.
- b. 용게이트웨이 설정 확인에서 확인란을 선택하여 선택한 호스트 플랫폼에 대한 배포 단계를 수행했음을 확인합니다. 이 단계는 다음에 적용되지 않습니다.하드웨어 어플라이언스호스트 플랫폼입니다.
6. 이제 게이트웨이가 설정되었으므로 연결 및 통신 방법을 선택해야 합니다.AWS. 선택다음항목으로 이동합니다.

Amazon FSx 파일 게이트웨이를AWS

새 FSx 파일 게이트웨이를AWS

1. 아직 수행하지 않은 경우 에서 설명한 절차를 완료합니다.[Amazon FSx 파일 게이트웨이 설정](#). 마친 후에는 다음을 선택합니다.다음 열려면에 연결AWS의 페이지AWS Storage Gateway콘솔.
2. 에서엔드포인트 옵션섹션,서비스 엔드포인트게이트웨이가 통신하는 데 사용할 엔드포인트 유형을 선택합니다.AWS. 다음 옵션 중에서 선택할 수 있습니다.
 - [Publicly accessible]— 게이트웨이가 다음과 통신합니다.AWS공용 인터넷을 통해 이 옵션을 선택하는 경우FIPS 지원 엔드포인트연결에서 연방 정보 처리 표준 (FIPS) 을 준수해야 하는지 여부를 지정하는 확인란을 선택합니다.

Note

에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우AWS명령줄 인터페이스 또는 API를 통해 FIPS 호환 엔드포인트를 사용합니다. 자세한 내용은 [FIPS\(Federal Information Processing Standard\) 140-2](#)를 참조하세요.

FIPS 서비스 엔드포인트는 일부에서만 사용할 수 있습니다.AWS리전. 자세한 내용은 단원을 참조하십시오.[AWS Storage Gateway엔드포인트 및 할당량](#)의AWS일반 참조.

- VPC 호스팅— 게이트웨이가 다음과 통신합니다.AWS네트워크 설정을 제어할 수 있는 Virtual Private Cloud (VPC) 와의 프라이빗 연결을 통해 얻을 수 있습니다. 이 옵션을 선택하는 경우 드롭다운 목록에서 VPC 엔드포인트 ID를 선택하여 기존 VPC 엔드포인트를 지정해야 합니다. VPC 엔드포인트 DNS (Domain Name System) 이름 또는 IP 주소를 제공할 수도 있습니다.

3. 예서게이트웨이 연결 옵션섹션,연결 옵션에서 게이트웨이를 식별하는 방법을 선택합니다.AWS. 다음 옵션 중에서 선택할 수 있습니다.
 - IP 주소— 해당 필드에 게이트웨이의 IP 주소를 입력합니다. 이 IP 주소는 공개적이거나 현재 네트워크 내에서 액세스할 수 있어야 하며 웹 브라우저에서 연결할 수 있어야 합니다.

하이퍼바이저 클라이언트에서 게이트웨이의 로컬 콘솔에 로그인하거나 Amazon EC2 인스턴스 세부 정보 페이지에서 복사하여 게이트웨이 IP 주소를 가져올 수 있습니다.
 - 정품 인증 키— 해당 필드에 게이트웨이에 대한 활성화 키를 제공합니다. 게이트웨이의 로컬 콘솔을 사용하여 활성화 키를 생성할 수 있습니다. 게이트웨이의 IP 주소를 사용할 수 없는 경우 이 옵션을 선택합니다.
4. 이제 게이트웨이의 연결 방법을 선택했으므로AWS에서 게이트웨이를 활성화해야 합니다. 선택다음항목으로 이동합니다.

설정을 검토하고 Amazon FSx 파일 게이트웨이 활성화

새 FSx 파일 게이트웨이를 활성화하려면

1. 아직 수행하지 않은 경우 다음 항목에 설명된 절차를 수행합니다.
 - [Amazon FSx 파일 게이트웨이 설정](#)
 - [Amazon FSx 파일 게이트웨이를AWS](#)

마친 후에는 다음을 선택합니다.다음 열려면검토 및 활성화의 페이지AWS Storage Gateway콘솔.

2. 페이지의 각 섹션에 대한 초기 게이트웨이 세부 정보를 검토합니다.
3. 섹션에 오류가 있는 경우Edit을 눌러 해당 설정 페이지로 돌아가서 변경합니다.

Important

게이트웨이가 활성화된 후에는 게이트웨이 옵션이나 연결 설정을 수정할 수 없습니다.

4. 게이트웨이를 활성화했으므로 로컬 스토리지 디스크를 할당하고 로깅을 구성하기 위해 처음 구성을 수행해야 합니다. 선택다음항목으로 이동합니다.

Amazon FSx 파일 게이트웨이 구성

새 FSx 파일 게이트웨이에서 처음 구성을 수행하려면

1. 아직 수행하지 않은 경우 다음 항목에 설명된 절차를 수행합니다.

- [Amazon FSx 파일 게이트웨이 설정](#)
- [Amazon FSx 파일 게이트웨이를AWS](#)
- [설정을 검토하고 Amazon FSx 파일 게이트웨이 활성화](#)

마친 후에는 다음을 선택합니다. 다음을 열려면 게이트웨이 구성의 페이지 AWS Storage Gateway 콘솔.

2. **에서 캐시 스토리지 구성** 드롭다운 목록을 사용하여 최소 150GiB (GiB) 용량을 가진 로컬 디스크를 하나 이상 할당하려면 **Cache**. 이 섹션에 나열된 로컬 디스크는 호스트 플랫폼에서 프로비저닝한 물리적 스토리지에 해당합니다.
3. **에서 CloudWatch 로그 그룹** 섹션에서 게이트웨이의 상태를 모니터링하기 위해 Amazon CloudWatch Logs 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - **새 로그 그룹 생성**— 게이트웨이를 모니터링하도록 새 로그 그룹을 설정합니다.
 - **기존 로그 그룹 사용**— 해당 드롭다운 목록에서 기존 로그 그룹을 선택합니다.
 - **로깅 비활성화**— 게이트웨이를 모니터링하기 위해 Amazon CloudWatch Logs 사용하지 마십시오.
4. **에서 CloudWatch 경보** 섹션에서 게이트웨이의 메트릭이 정의된 한도에서 벗어날 때 알림을 받도록 Amazon CloudWatch 경보를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - **경보 비활성화**— 게이트웨이의 지표에 대한 알림을 받기 위해 CloudWatch 경보를 사용하지 마십시오.
 - **사용자 지정 CloudWatch 경보 생성**— 게이트웨이의 메트릭에 대한 알림을 받도록 새 CloudWatch 경보를 구성합니다. 선택경보 생성 Amazon CloudWatch 콘솔을 사용하여 지표를 정의하고 경보 작업을 지정합니다. 지침은 단원을 참조하십시오. [Amazon CloudWatch 경보 사용](#)의 Amazon CloudWatch 사용 설명서.
5. (선택 사항) **태그** 섹션, 선택 새 태그 추가를 클릭하고 의 목록 페이지에서 게이트웨이를 검색하고 필터링할 수 있도록 대소문자 구분 키 값 페어를 입력합니다. AWS Storage Gateway 콘솔. 원하는 수의 태그를 추가하려면 이 단계를 반복합니다.

6. (선택 사항)VMware 고가용성 구성 확인섹션에서 게이트웨이가 VMware 호스트에 배포되면 VMware HA (고가용성) 용으로 사용할 수 있는 클러스터의 일부로 배포된 경우 를 선택합니다.VMware HA 검증HA 구성이 제대로 작동하는지 테스트합니다.

Note

이 섹션은 VMware 호스트 플랫폼에서 실행 중인 게이트웨이에 대해서만 나타냅니다. 게이트웨이 구성 프로세스를 완료하는 데 이 단계가 필요하지 않습니다. 게이트웨이의 HA 구성은 언제든지 테스트할 수 있습니다. 확인은 몇 분 정도 걸리고 Storage Gateway 가상 머신 (VM) 을 재부팅합니다.

7. 선택구성게이트웨이를 생성하려면

에서 새 게이트웨이를 검색하려면 에서 게이트웨이를 검색합니다.게이트웨이의 페이지AWS Storage Gateway콘솔.

게이트웨이를 생성했으므로 사용할 파일 시스템을 연결해야 합니다. 지침은 단원을 참조하십시오.[Amazon FSx for Windows File Server 파일 시스템 연결](#).

연결할 기존 Amazon FSx 파일 시스템이 없는 경우 하나를 생성해야 합니다. 지침은 단원을 참조하십시오.[Amazon FSx 시작하기](#).

Active Directory 설정

이 단계에서는 Microsoft Active Directory에 가입하도록 스토리지 게이트웨이에서 Amazon FSx 파일 게이트웨이 액세스 설정을 구성합니다.

Active Directory 설정을 지정하려면

1. Storage Gateway 콘솔에서 FSx 파일 시스템 연결.
2. 온게이트웨이 확인페이지의 게이트웨이 목록에서 사용할 Amazon FSx 파일 게이트웨이를 선택합니다.

게이트웨이가 없으면 하나 만들어야 합니다. 게이트웨이가 Active Directory 도메인 컨트롤러의 이름을 확인할 수 있는지 확인합니다. 자세한 내용은 [필수 사전 조건](#) 섹션을 참조하세요.

3. 다음에 대한 값을 입력합니다. Active Directory:

Note

게이트웨이가 이미 도메인에 가입되어 있는 경우 다시 가입할 필요가 없습니다. 다음 단계로 이동합니다.

- 용도메인 이름을 열려면 사용할 Active Directory 도메인 이름을 입력합니다.
- 용도메인 사용자 Active Directory 사용자 이름을 입력합니다.
- 용도메인 암호도메인 사용자 암호를 입력합니다.

Note

이때 계정에서 서버를 도메인에 조인할 수 있어야 합니다.

- 용조직 단위 - 선택 사항을 사용하여 Active Directory가 속한 조직 구성 단위를 지정할 수 있습니다.
 - 다음에 대한 값을 입력합니다. 도메인 컨트롤러 - 선택 사항.
4. 선택 다음을 열려면 FSx 파일 시스템 연결 페이지

다음 단계

[Amazon FSx for Windows File Server 파일 시스템 연결](#)

Amazon FSx for Windows File Server 파일 시스템 연결

다음 단계는 Amazon FSx 파일 시스템을 게이트웨이에 연결하는 것입니다. Amazon FSx 파일 시스템을 연결하면 마운트할 수 있도록 Amazon FSx 파일 게이트웨이 (FSx 파일) 에서 파일 시스템의 모든 파일 공유를 사용할 수 있습니다.

Note

Amazon FSx 파일 게이트웨이에서 Amazon FSx 파일 시스템에 쓸 때 적용됩니다.

- Amazon FSx 파일 시스템 및 FSx 파일은 동일한 소유여야 합니다. AWS 계정같은 위치에 있습니다. AWS 리전.
- 각 게이트웨이는 최대 5개의 첨부 파일 시스템을 지원할 수 있습니다. 파일 시스템을 연결할 때 선택한 게이트웨이의 용량에 해당하는지 Storage Gateway 콘솔에 알립니다. 이 경우 다른 게이트웨이를 연결하려면 먼저 다른 게이트웨이를 선택하거나 파일 시스템을 분리해야 합니다.
- FSx File은 소프트 스토리지 할당량을 지원하지만 (사용자가 데이터 한도를 초과할 때 경고) 하드 할당량을 지원하지 않습니다 (쓰기 액세스를 거부하여 데이터 제한을 적용함). 소프트 할당량은 Amazon FSx 관리자 사용자를 제외한 모든 사용자에게 지원됩니다. 스토리지 할당량 설정에 대한 자세한 내용은 단원을 참조하십시오. [스토리지 할당량](#) Amazon FSx 사용 설명서의 내용을 참조하십시오.

Amazon FSx 파일 시스템을 연결하려면

1. Storage Gateway 콘솔의 FSx 파일 시스템 > FSx 파일 시스템 연결 페이지에서 다음 필드를 채웁니다. FSx 파일 시스템 설정 섹션:

- 용 FSx 파일 시스템 이름 드롭다운 목록에서 첨부할 파일 시스템을 선택합니다.
- 용 로컬 엔드포인트 IP 주소에서 클라이언트가 FSx 파일 시스템에서 파일 공유를 탐색하는 데 사용할 게이트웨이 IP 주소를 입력합니다.

Note

- 게이트웨이에 파일 시스템을 하나만 연결하려는 경우 이 필드를 비워 두면 파일 시스템의 공유를 게이트웨이의 모든 IP 주소에서 사용할 수 있습니다. 파일 시스템을 여러 개 연결할 계획이라면 각 파일 시스템에 IP 주소를 지정해야 합니다.

- IP 주소 없이 파일 시스템을 연결하고 나중에 다른 파일 시스템을 연결해야 하는 경우 첫 번째 파일 시스템을 분리하고 IP 주소로 다시 연결해야 합니다.
- Amazon EC2 게이트웨이의 경우 다른 파일 시스템에서 이미 사용하고 있지 않는 한 EC2 인스턴스의 프라이빗 IP 주소를 지정할 수 있습니다. 이 경우 게이트웨이에 새 프라이빗 주소를 추가한 다음 다시 시작해야 합니다. 자세한 내용은 단원을 참조하십시오. [다중 IP 주소의 Amazon EC2 사용 설명서](#).
- 온프레미스 게이트웨이의 경우 기본 네트워크 인터페이스 (정적 또는 DHCP)의 IP 주소를 지정할 수 있습니다. 이 경우 기본 인터페이스와 동일한 서브넷에서 다른 IP 주소를 제공해야 합니다. 이 경우 가상 IP로 사용할 수 있게 됩니다. 기본 인터페이스가 아닌 네트워크 인터페이스에 할당된 IP 주소를 사용하지 마십시오.

2. 에서서비스 계정 설정섹션에서 Amazon FSx 파일 시스템과 연결된 사용자 이름 및 암호를 입력합니다.

Note

이 사용자는 Active Directory 서비스의 Backup 운영자 그룹의 구성원이어야 하며 Amazon FSx 파일 시스템과 연결되어 있거나 이에 상응하는 권한이 있어야 합니다.

Important

파일, 폴더 및 파일 메타데이터에 대한 충분한 권한을 확보하려면 이 사용자를 파일 시스템 관리자 그룹의 멤버로 설정하는 것이 좋습니다.

사용 중인 경우AWS Directory ServiceAmazon FSx for Windows File Server for Windows Active Directory의 경우 사용자는AWS위임된 FSx 관리자 그룹입니다.

Windows 파일 서버용 Amazon FSx에서 자체 관리형 Active Directory를 사용하는 경우 사용자는 파일 시스템을 생성할 때 파일 시스템 관리를 위해 지정한 도메인 관리자 또는 사용자 지정 위임된 파일 시스템 관리자 그룹 중 하나의 구성원이어야 합니다.

자세한 내용은 단원을 참조하십시오. [Amazon FSx 서비스 계정에 권한 위임](#)의 Amazon FSx for Windows File Server 사용 설명서.

3. 에서감사 로그섹션, 선택기준 로그 그룹을 클릭하고 Amazon FSx 파일 시스템에 대한 액세스를 모니터링하는 데 사용할 로그를 선택합니다. 새 파일을 생성할 수 있습니다. 시스템을 모니터링하지 않으려면로깅 비활성화.

4. 용자동 캐시 새로 고침 설정캐시를 자동으로 새로 고치려면 새로 고침 간격 설정5분에서 30일 사이의 간격을 지정합니다.
5. (선택 사항)태그섹션, 선택새 태그 추가설정을 태그 지정하기 위한 하나 이상의 키와 값을 추가합니다.
6. 선택다음설정을 검토합니다. 설정을 변경하려면 다음을 선택할 수 있습니다.Edit각 섹션에 있습니다.
7. 완료되면 를 선택합니다.Finish.

다음 단계

[파일 공유 마운트 및 사용](#)

파일 공유 마운트 및 사용

클라이언트에 파일 공유를 마운트하기 전에 Amazon FSx 파일 시스템의 상태가 로 변경될 때까지 기다립니다. 응시 가능. 파일 공유가 마운트된 후 Amazon FSx 파일 게이트웨이 (FSx 파일) 를 사용할 수 있습니다.

주제

- [클라이언트에 SMB 파일 공유를 탑재하려면](#)
- [FSx 파일 테스트하기](#)

클라이언트에 SMB 파일 공유를 탑재하려면

이 단계에서는 SMB 파일 공유를 탑재하고 클라이언트에서 액세스할 수 있는 드라이브에 매핑합니다. 콘솔의 파일 게이트웨이 섹션에는 SMB 클라이언트에서 지원되는 탑재 명령이 표시됩니다. 다음은 몇 가지 추가 옵션들입니다.

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

- `lnet usecommand` — 를 사용하지 않으면 시스템 재부팅 시 유지되지 않습니다./persistent: (yes:no)스위치.
- `lnetCmdKey` 명령줄 유틸리티 — 재부팅 후 탑재된 SMB 파일 공유에 대해 지속적 연결을 생성합니다.
- File Explorer에 매핑된 네트워크 드라이브 — 로그인 시 다시 연결을 하고 반드시 네트워크 자격 증명을 입력하도록 탑재된 파일 공유를 구성합니다.
- PowerShell 스크립트 — 지속적일 수 있으며 탑재되는 동안 운영 체제에서 표시 또는 숨김이 가능합니다.

Note

Microsoft Active Directory 사용자는 로컬 시스템에 파일 공유를 탑재하기 전에 SMB 파일 공유에 대한 액세스 권한을 가지고 있는지 관리자에게 확인합니다.

Amazon FSx 파일 게이트웨이는 SMB 잠금 또는 SMB 확장 속성을 지원하지 않습니다.

net use 명령을 사용해 Active Directory 사용자를 위한 SMB 파일 공유를 탑재하려면

1. 로컬 시스템에 파일 공유를 탑재하기 전에 SMB 파일 공유에 대한 액세스 권한을 가지고 있는지 확인합니다.
2. Microsoft Active Directory 클라이언트의 경우, 명령 프롬프트에서 다음 명령을 입력합니다.

```
net use [WindowsDriveLetter]: \\[Gateway IP Address]\[Name of the share on the FSx file system]
```

CmdKey를 사용하여 Windows에 SMB 파일 공유를 탑재하려면

1. Windows 키를 누르고 를 입력하십시오. **cmd**를 눌러 명령 프롬프트 메뉴 항목을 봅니다.
2. [] 를 오른쪽 클릭하여 컨텍스트 메뉴를 엽니다. 명령 프롬프트를 선택하고 관리자 권한으로 실행.
3. 다음 명령을 입력합니다.

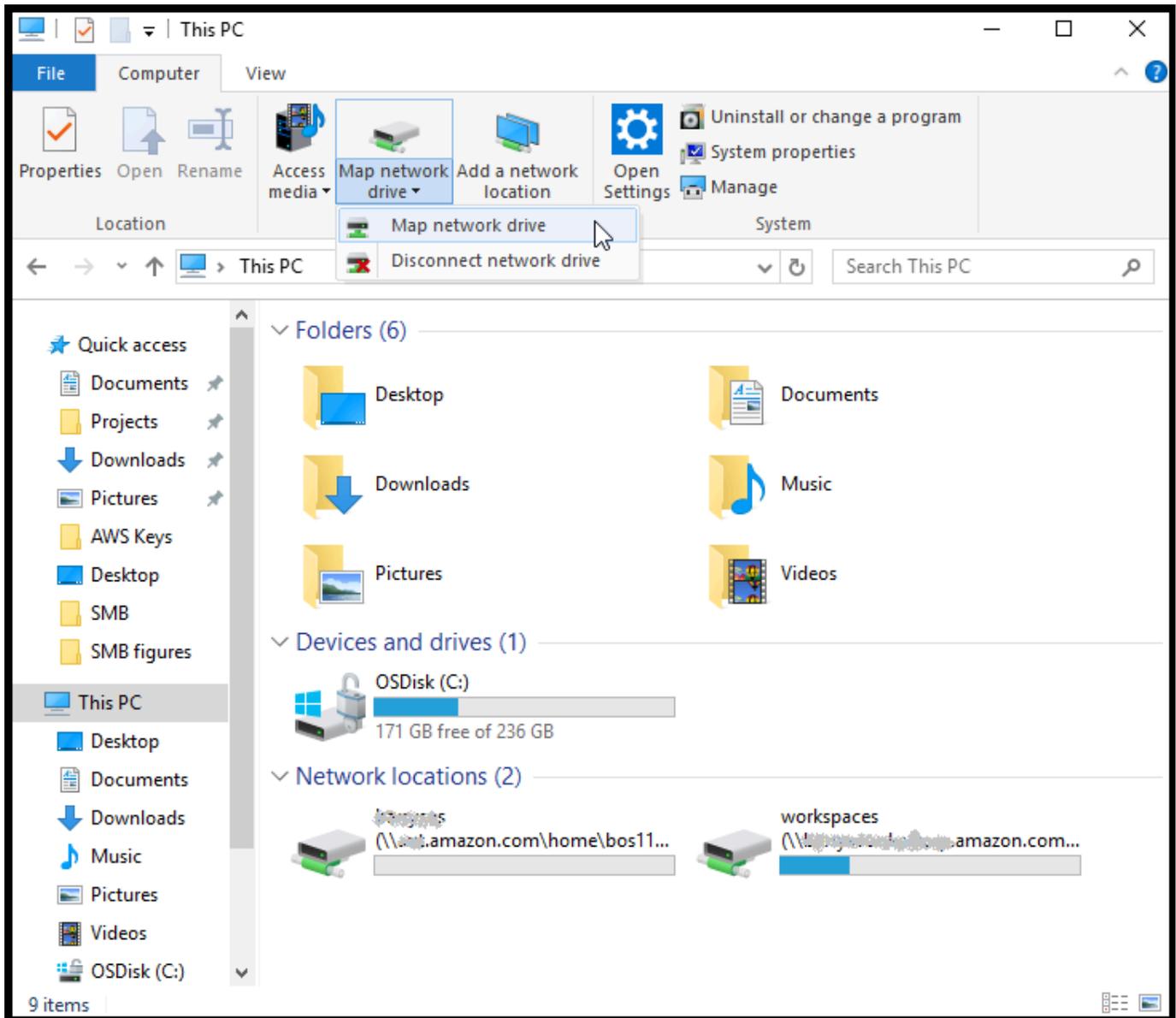
```
C:\>cmdkey /add:[Gateway VM IP address] /user:[DomainName]\[UserName] /pass:[Password]
```

Note

파일 공유를 탑재하려면 클라이언트를 재부팅한 후 파일 공유를 다시 탑재해야 할 수 있습니다.

Windows File Explorer를 사용하여 SMB 파일 공유를 탑재하려면

1. Windows 키를 누르고 를 입력하십시오. **File Explorer**의 검색 창상자 또는 누름 **Win+E**.
2. 탐색 창에서 [] 를 선택합니다. 이 PC.
3. 온컴퓨터탭, 선택네트워크 드라이브 매핑을 선택한 다음 를 선택합니다. 네트워크 드라이브 매핑다음 스크린샷과 같이 다시 한 번 표시됩니다.



4. 에서네트워크 드라이브 매핑대화 상자에서 드라이브 문자를 선택합니다.드라이브.
5. 용폴더를 입력합니다\\[File Gateway IP]\[SMB File Share Name]또는 선택검색을 눌러 대화 상자에서 SMB 파일 공유를 선택합니다.
6. (선택 사항) 재부팅 이후에 탑재 지점이 지속되기를 원하는 경우에는 가입 시 재연결(Reconnect at sign-up)을 선택합니다.
7. (선택 사항) 선택 사항다른 자격 증명을 사용하여 Connect사용자가 Active Directory 로그인 또는 게스트 계정 사용자 암호를 입력하도록 하고 싶은 경우입니다.
8. 완료(Finish)를 선택하여 탑재 지점을 완료합니다.

FSx 파일 테스트하기

매핑된 드라이브에 파일과 디렉터리를 복사할 수 있습니다. 파일은 FSx for Windows File Server 파일 시스템에 자동으로 업로드됩니다.

Windows 클라이언트의 파일을 Amazon FSx 로 업로드하려면

1. Windows 클라이언트에서 파일 공유를 탑재한 드라이브로 이동합니다. 드라이브 이름 앞에 파일 시스템 이름의 이름이 옵니다.
2. 파일 또는 디렉터리를 드라이브에 복사합니다.

Note

파일 게이트웨이는 파일 공유에 대한 하드 또는 심볼 링크를 지원하지 않습니다.

가상 프라이빗 클라우드에서 게이트웨이 활성화

온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 이제 이 소프트웨어 어플라이언스를 이용하여 에 데이터를 전송할 수 있습니다. AWS 게이트웨이와 통신하지 않는 스토리지 AWS 공용 인터넷을 통한 스토리지 서비스 Amazon VPC 서비스를 사용하여 시작할 수 있습니다. AWS 사용자 지정 가상 네트워크의 리소스. Virtual Private Cloud (VPC) 를 사용하여 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 단원을 참조하십시오. [Amazon VPC란 무엇인가?](#)의 Amazon VPC User Guide.

VPC에서 Storage Gateway VPC 엔드포인트에서 게이트웨이를 사용하려면 다음과 같이 하십시오.

- VPC 콘솔을 사용하여 Storage Gateway 대한 VPC 엔드포인트를 생성하고 VPC 엔드포인트 ID를 얻습니다. 게이트웨이를 생성하고 활성화할 때 이 VPC 엔드포인트 ID를 지정합니다.
- 파일 게이트웨이를 활성화하는 경우 Amazon S3 위한 VPC 엔드포인트를 생성합니다. 게이트웨이에 대한 파일 공유를 생성할 때 이 VPC 엔드포인트를 지정합니다.
- 파일 게이트웨이를 활성화하는 경우 HTTP 프록시를 설정하고 파일 게이트웨이 VM 로컬 콘솔에서 이를 구성합니다. VMware, Microsoft HyperV 및 Linux 커널 기반 가상 머신(KVM)을 기반으로 하는 하이퍼바이저 기반 온프레미스 파일 게이트웨이에 이 프록시가 필요합니다. 이러한 경우 게이트웨이가 VPC 외부에서 Amazon S3 프라이빗 엔드포인트에 액세스할 수 있도록 하려면 프록시가 필요합니다. HTTP 프록시를 구성하는 방법에 대한 자세한 내용은 [HTTP 프록시 구성](#) 단원을 참조하십시오.

Note

게이트웨이는 VPC 엔드포인트가 생성된 리전과 같은 리전에서 활성화 되어야 합니다. 파일 게이트웨이의 경우, 파일 공유를 위해 생성된 Amazon S3 스토리지는 Amazon S3 S3를 위한 VPC 엔드포인트를 생성한 리전과 같은 리전에 있어야 합니다.

주제

- [Storage Gateway 대한 VPC 엔드포인트 생성](#)
- [HTTP 프록시 설정 및 구성 \(온-프레미스 파일 게이트웨이에만 해당\)](#)
- [HTTP 프록시의 필수 포트에 대한 트래픽 허용](#)

Storage Gateway 대한 VPC 엔드포인트 생성

여기 나온 지침에 따라 VPC 엔드포인트를 생성합니다. Storage Gateway 대한 VPC 엔드포인트가 이미 있는 경우에는 이를 사용할 수 있습니다.

Storage Gateway 대한 VPC 엔드포인트를 생성하려면

1. AWS Management Console에 로그인하고 <https://console.aws.amazon.com/vpc/>에서 Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택하고 엔드포인트 생성을 선택합니다.
3. 온엔드포인트 생성페이지, 선택AWS서비스...에 대한서비스 범주.
4. 용서비스 이름, 선택com.amazonaws.*region*.storagegateway. 예 com.amazonaws.us-east-2.storagegateway.
5. VPC에서 VPC를 선택하고 해당 가용 영역 및 서브넷을 기록합니다.
6. 프라이빗 DNS 이름 활성화가 선택되지 않았는지 확인합니다.
7. 보안 그룹에서 VPC에 사용할 보안 그룹을 선택합니다. 기본 보안 그룹을 적용할 수 있습니다. 다음 모든 TCP 포트가 보안 그룹에서 허용되는지 확인합니다.
 - TCP 443
 - TCP 1026
 - TCP 1027
 - TCP 1028
 - TCP 1031
 - TCP 2222
8. 엔드포인트 생성을 선택합니다. 엔드포인트의 초기 상태는 대기 중입니다. 엔드포인트가 생성되면 방금 생성한 VPC 엔드포인트의 ID를 기록합니다.
9. 엔드포인트가 생성되면 엔드포인트를 선택한 다음 새 VPC 엔드포인트를 선택합니다.
10. DNS 이름 섹션에서 가용 영역을 지정하지 않은 최초의 DNS 이름을 사용합니다. DNS 이름은 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 과 비슷합니다.

VPC 엔드포인트가 있으므로 게이트웨이를 생성할 수 있습니다.

⚠ Important

파일 게이트웨이를 생성하는 경우 Amazon S3 위한 엔드포인트도 생성해야 합니다. 위의 Storage Gateway 대한 VPC 엔드포인트 생성 방법 단원에 나와 있는 것과 똑같은 단계를 따르되, `com.amazonaws.us-east-2.s3` 대신 서비스 이름 아래에 있습니다. 그런 다음, 서브넷/보안그룹 대신 S3 엔드포인트를 연결하고 싶은 라우팅 테이블을 선택합니다. 지침은 단원을 참조하십시오. [게이트웨이 엔드포인트 생성](#).

HTTP 프록시 설정 및 구성 (온-프레미스 파일 게이트웨이에만 해당)

파일 게이트웨이를 활성화하는 경우 HTTP 프록시를 설정하고 파일 게이트웨이 VM 로컬 콘솔을 사용하여 이를 구성해야 합니다. VPC 외부에서 Amazon S3 프라이빗 엔드포인트에 액세스하려면 온프레미스 파일 게이트웨이에 이 프록시가 필요합니다. Amazon EC2 이미 HTTP 프록시가 있는 경우에는 이를 사용할 수 있습니다. 그러나 다음 모든 TCP 포트가 보안 그룹에서 허용되는지 확인해야 합니다.

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

Amazon EC2 프록시가 없는 경우 다음 절차에 따라 HTTP 프록시를 설정하고 구성합니다.

프록시 서버를 설정하려면

1. Amazon EC2 Linux AMI를 실행합니다. `c5n.large` 같이 네트워크에 최적화된 인스턴스 패밀리를 사용하는 것이 좋습니다.
2. 다음 명령을 사용하여 squid: 를 설치합니다. **`sudo yum install squid`**. 이렇게 하면 기본 구성 파일이 생성됩니다. `/etc/squid/squid.conf`.
3. 이 구성 파일 내용을 다음으로 바꿉니다.

```
#
# Recommended minimum configuration:
#
```

```
# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8           # RFC1918 possible internal network
acl localnet src 172.16.0.0/12        # RFC1918 possible internal network
acl localnet src 192.168.0.0/16      # RFC1918 possible internal network
acl localnet src fc00::/7            # RFC 4193 local private network range
acl localnet src fe80::/10           # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
acl SSL_ports port 1026
acl SSL_ports port 1027
acl SSL_ports port 1028
acl SSL_ports port 1031
acl SSL_ports port 2222
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Deny requests to certain unsafe ports
http_access deny !SSL_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# Only allow cachemgr access from localhost
http_access allow localhost manager
http_access deny manager

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
http_access deny all

# Squid normally listens to port 3128
http_port 3128

# Leave coredumps in the first cache dir
```

```

coredump_dir /var/spool/squid

#
# Add any of your own refresh_pattern entries above these.
#
refresh_pattern ^ftp:          1440      20%      10080
refresh_pattern ^gopher:      1440      0%       1440
refresh_pattern -i (/cgi-bin/|\?) 0         0%       0
refresh_pattern .              0         20%     4320

```

4. 프록시 서버에 대한 잠금과 어떤 변경 작업도 필요하지 않은 경우에는 다음 명령을 사용하여 프록시 서버를 활성화 및 시작합니다. 이러한 명령은 부팅 시 서버를 시작합니다.

```

sudo chkconfig squid on
sudo service squid start

```

이제 이 명령을 사용하도록 Storage Gateway 대한 HTTP 프록시를 구성합니다. 프록시를 사용하도록 게이트웨이를 구성할 때는 기본 squid 포트 3128을 사용합니다. 생성된 squid.conf 파일에는 기본적으로 다음 필수 TCP 포트가 포함됩니다.

- TCP 443
- TCP 1026
- TCP 1027
- TCP 1028
- TCP 1031
- TCP 2222

VM 로컬 콘솔을 사용하여 HTTP 프록시를 구성하려면

1. 게이트웨이의 VM 로컬 콘솔에 로그인합니다. 자세한 로그인 방법은 [파일 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하십시오.
2. 기본 메뉴에서 Configure HTTP proxy(HTTP 프록시 구성)를 선택합니다.
3. 구성 메뉴에서 Configure HTTP proxy(HTTP 프록시 구성)를 선택합니다.
4. 프록시 서버의 호스트 이름과 포트를 입력합니다.

HTTP 프록시를 구성하는 방법에 대한 자세한 내용은 [HTTP 프록시 구성](#) 단원을 참조하십시오.

HTTP 프록시의 필수 포트에 대한 트래픽 허용

HTTP 프록시를 사용하는 경우 Storage Gateway에서 다음에 나열된 대상 및 포트로의 트래픽을 허용해야 합니다.

스토리지 게이트웨이가 퍼블릭 엔드포인트를 통해 통신을 할 때는 다음 Storage Gateway 서비스와 통신합니다.

```
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
storagegateway.region.amazonaws.com:443 (Required for making API calls)
s3.region.amazonaws.com (Required only for File Gateway)
```

Important

게이트웨이에 따라 다른 AWS 지역, 바꾸기 ##에 해당하는 리전 문자열이 있는 엔드포인트에서. 예를 들어, 미국 서부 (오레곤) 리전에 게이트웨이를 생성하는 경우, 엔드포인트는 다음과 같이 됩니다. `storagegateway.us-west-2.amazonaws.com:443`.

VPC 엔드포인트를 통해 Storage Gateway 통신을 할 때는 AWS Amazon S3 프라이빗 엔드포인트 상의 여러 포트와 Amazon S3 VPC 엔드포인트 상의 포트 443을 통해 서비스를 제공합니다.

- Storage Gateway VPC 엔드포인트 상의 TCP 포트.
 - 443, 1026, 1027, 1028, 1031 및 2222
- S3 프라이빗 엔드포인트 상의 TCP 포트
 - 443

Amazon FSx 파일 게이트웨이 리소스 관리

다음 단원에서는 Amazon FSx 파일 시스템 연결 및 분리, Microsoft Active Directory 설정 구성 등 Amazon FSx 파일 게이트웨이 (FSx 파일) 리소스를 관리하는 방법에 대한 정보를 제공합니다.

주제

- [Amazon FSx 파일 시스템 연결](#)
- [FSx 파일에 대한 액티브 디렉토리 구성](#)
- [액티브 디렉터리 설정 구성](#)
- [FSx 파일 설정 편집](#)
- [Amazon FSx for Windows File Server 파일 시스템 설정 편집](#)
- [Amazon FSx 파일 시스템 분리](#)

Amazon FSx 파일 시스템 연결

FSx for Windows File Server 파일 시스템이 있어야 FSx 파일에 연결할 수 있습니다. 파일 시스템이 없으면 하나를 생성해야 합니다. 지침은 단원을 참조하십시오. [단계 1: 파일 시스템 만들기](#)의 Amazon FSx for Windows File Server 사용 설명서.

다음 단계는 FSx 파일을 활성화하고 Active Directory 도메인에 가입하도록 게이트웨이를 구성하는 것입니다. 지침은 [Active Directory 설정](#) 단원을 참조하세요.

Note

게이트웨이가 도메인에 가입한 경우 도메인에 다시 가입하도록 구성할 필요가 없습니다.

각 게이트웨이는 최대 5개의 연결된 파일 시스템을 지원합니다. 파일 시스템을 연결하는 방법에 대한 지침은 단원을 참조하십시오. [Amazon FSx for Windows File Server 파일 시스템 연결](#).

FSx 파일에 대한 액티브 디렉토리 구성

FSx 파일을 사용하려면 Active Directory 도메인에 가입하도록 게이트웨이를 구성해야 합니다. 지침은 [Active Directory 설정](#) 단원을 참조하세요.

액티브 디렉터리 설정 구성

Active Directory 도메인에 가입하도록 게이트웨이를 구성한 후 Active Directory 설정을 편집할 수 있습니다.

액티브 디렉터리 설정을 편집하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 를 선택합니다. 게이트웨이를 선택한 다음 Active Directory 설정을 편집할 게이트웨이를 선택합니다.
3. 용작업, 선택SMB 설정 편집을 선택한 다음 를 선택합니다. 액티브 디렉터리 설정.
4. Active Directory settings (액티브 디렉터리 설정) 섹션에서 요청한 정보를 입력한 다음 를 변경 내용 저장.

FSx 파일 설정 편집

게이트웨이가 활성화된 후에는 게이트웨이 설정을 편집할 수 있습니다.

게이트웨이 설정을 편집하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 를 선택합니다. 게이트웨이를 선택한 다음 설정을 편집할 게이트웨이를 선택합니다.
3. 용작업, 선택게이트웨이 정보 편집.
4. 용게이트웨이 이름선택한 게이트웨이의 이름을 편집합니다.
5. 용게이트웨이 시간대시간대를 선택합니다.
6. 용게이트웨이 상태 로그 그룹에서 Amazon CloudWatch 로그 그룹을 사용하여 게이트웨이를 모니터링하는 옵션 중 하나를 선택합니다.

를 선택한 경우 기존 로그 그룹 사용에서 로그 그룹을 선택합니다. 기존 로그 그룹 목록을 선택한 다음 를 선택합니다. 변경 내용 저장.

Amazon FSx for Windows File Server 파일 시스템 설정 편집

Amazon FSx for Windows File Server 파일 시스템을 생성한 후 파일 시스템 설정을 편집할 수 있습니다.

Amazon FSx 파일 시스템 설정을 편집하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 를 선택합니다. 파일 시스템을 선택한 다음 설정을 편집할 파일 시스템을 선택합니다.
3. 용작업, 선택파일 시스템 설정 편집.
4. 파일 시스템 설정 섹션에서 게이트웨이, Amazon FSx 위치 및 IP 주소 정보를 확인합니다.

Note

게이트웨이에 연결된 파일 시스템의 IP 주소는 편집할 수 없습니다. IP 주소를 변경하려면 파일 시스템을 분리했다가 다시 연결해야 합니다.

5. 에서 감사 로그 섹션에서 CloudWatch 로그 그룹을 사용하여 Amazon FSx 파일 시스템에 대한 액세스를 모니터링하는 옵션을 선택합니다. 기존 로그 그룹을 사용할 수 있습니다.
6. 용자동 캐시 새로 고침 설정을 선택한 다음 를 선택합니다. 를 선택한 경우 새로 고침 간격 설정 TTL (Time To Live) 을 사용하여 파일 시스템의 캐시를 새로 고칠 시간을 일, 시간 및 분 단위로 설정합니다.

TTL은 마지막 새로 고침 이후의 시간입니다. 해당 기간 후에 디렉터리에 액세스하면 파일 게이트웨이가 Amazon FSx 파일 시스템에서 해당 디렉터리의 콘텐츠를 새로 고칩니다.

Note

유효한 새로 고침 간격 값은 5분에서 30일 사이입니다.

7. 에서 서비스 계정 설정 - 선택 사항 섹션, 사용자 이름 및 Password. 이러한 자격 증명은 Amazon FSx 파일 시스템과 연결된 Active Directory 서비스의 Backup 관리자 역할을 가진 사용자를 위한 것입니다.
8. 변경 사항 저장(Save changes)을 선택합니다.

Amazon FSx 파일 시스템 분리

파일 시스템을 분리해도 FSx for Windows File Server FSx의 데이터는 삭제되지 않습니다. 파일 시스템을 삭제하기 전에 파일 시스템의 파일 공유에 기록된 데이터는 FSx for Windows File Server FSx로 업로드됩니다.

Amazon FSx 파일 시스템을 분리하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 왼쪽 탐색 창에서 [] 를 선택합니다.파일 시스템을 선택한 다음 분리할 파일 시스템을 선택합니다. 여러 파일 시스템을 삭제할 수 있습니다.
3. 용작업, 선택파일 시스템 분리.
4. Enter**detach**상자에 확인 하 고Detach.

파일 게이트웨이 모니터링

에서 파일 게이트웨이 및 관련 리소스를 모니터링할 수 있습니다. AWS Storage Gateway Amazon CloudWatch 지표 및 파일 공유 감사 로그를 사용합니다. 또한 CloudWatch 이벤트를 사용하여 파일 작업이 완료될 때 알림을 받을 수 있습니다. 파일 게이트웨이 유형 지표에 대한 자세한 내용은 [파일 게이트웨이 모니터링](#) 단원을 참조하십시오.

주제

- [CloudWatch 로그 그룹을 사용하여 파일 게이트웨이 상태 로그 가져오기](#)
- [Amazon CloudWatch 지표 사용](#)
- [게이트웨이 지표 이해](#)
- [파일 시스템 지표 이해](#)
- [파일 게이트웨이 감사 로그 이해](#)

CloudWatch 로그 그룹을 사용하여 파일 게이트웨이 상태 로그 가져오기

Amazon CloudWatch Logs 사용하여 파일 게이트웨이 및 관련 리소스 상태에 대한 정보를 가져올 수 있습니다. 로그를 사용하여 게이트웨이에 로그가 발생하는지 모니터링할 수 있습니다. 또한 Amazon CloudWatch 구독 필터를 사용하여 실시간으로 로그 정보 처리를 자동화할 수 있습니다. 자세한 내용은 단원을 참조하십시오. [구독을 통한 로그 데이터 실시간 처리](#)의 Amazon CloudWatch 사용 설명서

예를 들어 게이트웨이를 모니터링하고, 파일 게이트웨이에서 Amazon FSx 파일 시스템에 파일을 업로드하는 데 실패하면 알림을 받도록 CloudWatch 로그 그룹을 구성할 수 있습니다. 게이트웨이를 활성화할 때나 게이트웨이가 활성화되어 실행된 후에 그룹을 구성할 수 있습니다. 게이트웨이를 활성화할 때 CloudWatch 로그 그룹을 구성하는 방법에 대한 자세한 내용은 단원을 참조하십시오. [Amazon FSx 파일 게이트웨이 구성](#). CloudWatch 로그 그룹에 대한 일반적인 내용은 단원을 참조하십시오. [로그 그룹 및 로그 스트림 작업](#)의 Amazon CloudWatch 사용 설명서

다음은 파일 게이트웨이에서 보고하는 오류의 예입니다.

앞에 나온 게이트웨이 상태 로그에서는 다음 항목이 주어진 정보를 지정합니다.

- `source`: `share-E1A2B34C` - 이 오류를 일으킨 파일 공유를 나타냅니다.
- `"type": "InaccessibleStorageClass"` - 발생한 오류의 유형을 나타냅니다. 여기서는 게이트웨이가 지정된 객체를 Amazon S3에 업로드하거나 Amazon S3 읽으려고 할 때 이 오류가 발생했습니다.

니다. 하지만 이때 객체는 Amazon S3 Glacier로 전환했습니다. "type"의 값은 파일 게이트웨이가 일으키는 모든 오류일 수 있습니다. 가능한 오류 목록은 [파일 게이트웨이 문제 해결](#) 단원을 참조하십시오.

- "operation": "S3Upload"- 게이트웨이가 이 객체를 S3에 업로드하려고 할 때 이 오류가 발생했음을 나타냅니다.
- "key": "myFolder/myFile.text" - 오류를 유발한 객체를 나타냅니다.
- gateway": "sgw-B1D123D4 - 이 오류를 일으킨 파일 게이트웨이를 나타냅니다.
- "timestamp": "1565740862516"오류 발생 시간을 나타냅니다.

문제를 해결하고 이 오류 유형을 해결하는 방법에 대한 자세한 내용은 [파일 게이트웨이 문제 해결](#) 단원을 참조하십시오.

게이트웨이가 활성화된 후 CloudWatch 로그 그룹 구성

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

파일 게이트웨이와 함께 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 로그인합니다.AWS Management Console에서 Storage Gateway 콘솔을 엽니다.<https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 를 선택합니다.게이트웨이를 클릭한 다음 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 용작업, 선택게이트웨이 정보 편집. 또는,세부 정보탭, 아래Health 로그과사용 안 함, 선택로그 그룹 구성를 열려면Edit커스텀 게이트웨이 이름대화 상자.
4. 용게이트웨이 로그 그룹다음 중 하나를 선택합니다.
 - 로깅 비활성화CloudWatch 로그 그룹을 사용하여 게이트웨이를 모니터링하지 않으려는 경우
 - 새 로그 그룹 생성를 눌러 새 CloudWatch 로그 그룹을 생성합니다.
 - 기존 로그 그룹 사용이미 존재하는 CloudWatch 로그 그룹을 사용합니다.

에서 로그 그룹을 선택합니다.기존 로그 그룹 목록.
5. 변경 사항 저장(Save changes)을 선택합니다.
6. 게이트웨이의 상태 로그를 확인하려면 다음을 수행합니다.
 1. 탐색 창에서 를 선택합니다.게이트웨이를 클릭한 다음 CloudWatch 로그 그룹을 구성한 게이트웨이를 선택합니다.

2. 를 선택합니다. 세부 정보 탭 및 아래 Health 로그, 선택 CloudWatch Logs (CloudWatch 로그). 이 로그 그룹 세부 정보 CloudWatch 콘솔에서 페이지가 열립니다.

파일 게이트웨이와 함께 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 로그인합니다. AWS Management Console에서 Storage Gateway 콘솔을 엽니다. <https://console.aws.amazon.com/storagegateway/home>.
2. 선택 게이트웨이를 클릭한 다음 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 용 작업, 선택 게이트웨이 정보 편집. 또는 세부 정보 탭, 옆에 로깅을 열려면 사용 안 함, 선택 로그 그룹 구성을 열려면 게이트웨이 정보 편집 대화 상자.
4. 용 게이트웨이 로그 그룹, 선택 기존 로그 그룹 사용을 클릭한 다음 사용할 로그 그룹을 선택합니다.

로그 그룹이 없는 경우 새 로그 그룹 만들기를 선택하여 로그 그룹을 만듭니다. 로그 그룹을 만들 수 있는 CloudWatch Logs 콘솔로 이동합니다. 새 로그 그룹을 만드는 경우 새로 고침 버튼을 선택하여 드롭다운 목록에서 새 로그 그룹을 확인합니다.

5. 마치면 [Save]를 선택합니다.
6. 게이트웨이의 로그를 보려면 게이트웨이를 선택하고 세부 정보 탭.

오류 문제 해결 방법에 대한 자세한 내용은 [파일 게이트웨이 문제 해결](#) 단원을 참조하십시오.

Amazon CloudWatch 지표 사용

다음 중 하나를 사용하여 파일 게이트웨이에 대한 모니터링 데이터를 얻을 수 있습니다. AWS Management Console 또는 CloudWatch API 를 사용합니다. 콘솔에는 CloudWatch API의 원시 데이터를 기초로 일련의 그래프가 표시됩니다. CloudWatch API는 다음 중 하나를 통해서도 사용할 수 있습니다. [AWS SDK](#) 또는 [Amazon CloudWatch API](#) 도구. 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 Gateway 게이트웨이의 크기는 다음과 같습니다. GatewayId와 GatewayName. CloudWatch 콘솔에서 다음을 사용할 수 있습니다. Gateway Metrics 뷰로 게이트웨이별 차원을 선택합니다. 차원에 대한 자세한 내용은 단원을 참조하십시오. [차원](#)의 Amazon CloudWatch 사용 설명서.
- ReadBytes와 같은 지표 이름.

다음 표에서는 사용할 수 있는 Storage Gateway 지표 데이터의 유형을 간략히 설명합니다.

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

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

- [사용 가능한 지표 보기](#)
- [지표에 대한 통계 얻기](#)
- [CloudWatch 경보 생성](#)

게이트웨이 지표 이해

다음 표에서는 FSx 파일 게이트웨이를 나타내는 지표에 대해 설명합니다. 각 게이트웨이에는 연결된 지표 집합이 있습니다. 일부 게이트웨이별 지표는 특정 파일 시스템별 지표와 이름이 같습니다. 이 지표는 같은 종류의 측정값을 나타내지만 파일 시스템이 아닌 게이트웨이에 한정됩니다.

특정 지표로 작업할 때 게이트웨이와 파일 시스템을 다룰 것인지 지정해야 합니다. 특히 게이트웨이 지표를 사용하는 경우를 지정해야 합니다. Gateway Name 지표 데이터를 확인하려는 게이트웨이의 경우입니다. 자세한 정보는 [Amazon CloudWatch 지표 사용](#)을 참조하십시오.

다음 표에서는 에 대한 정보를 얻는 데 사용할 수 있는 지표에 대해 설명합니다. FSx 파일 게이트웨이s.

지표	설명
AvailabilityNotifications	<p>이 지표는 보고 기간 동안 게이트웨이에 의해 생성된 가용성 관련 상태 알림의 수를 보고합니다.</p> <p>단위: 개수</p>
CacheDirectorySize	<p>이 측정치는 게이트웨이 캐시의 폴더 크기를 추적합니다. 폴더 크기는 첫 번째 수준의 파일 및 하위 폴더 수에 따라 결정되며 하위 폴더에는 재귀적으로 계산되지 않습니다.</p> <p>이 메트릭과 함께 사용Average게이트웨이 캐시에 있는 폴더의 평균 크기를 측정하는 통계입니다. 이 메트릭과 함께 사용Max게이트웨이 캐시에 있는 폴더의 최대 크기를 측정하는 통계입니다.</p> <p>단위: 개수</p>
CacheFileSize	<p>이 측정치는 게이트웨이 캐시의 파일 크기를 추적합니다.</p> <p>이 메트릭과 함께 사용Average게이트웨이 캐시에 있는 파일의 평균 크기를 측정하는 통계입니다. 이 메트릭과 함께 사용Max게이트웨이 캐시에 있는 파일의 최대 크기를 측정하는 통계입니다.</p> <p>단위: 바이트</p>
CacheFree	<p>이 측정치는 게이트웨이 캐시에서 사용 가능한 바이트 수를 보고합니다.</p> <p>단위: 바이트</p>
CacheHitPercent	<p>캐시로부터 읽는 게이트웨이의 애플리케이션 읽기 작업 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다.</p>

지표	설명
	<p>게이트웨이에서 애플리케이션 읽기 작업이 없는 경우, 지표가 100% 를 보고합니다.</p> <p>단위: %</p>
CachePercentDirty	<p>에 지속되지 않은 게이트웨이 캐시의 전체 백분율입니다.AWS. 보고 기간 종료 시점에서 샘플이 채취됩니다.</p> <p>단위: %</p>
CachePercentUsed	<p>사용되는 게이트웨이 캐시 스토리지의 전체 비율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다.</p> <p>단위: %</p>
CacheUsed	<p>이 측정치는 게이트웨이 캐시에 사용된 바이트 수를 보고합니다.</p> <p>단위: 바이트</p>
CloudBytesDownloaded	<p>게이트웨이가 로 업로드한 총 바이트 수입니다.AWS보고 기간 동안.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 초당 입력/출력 작업 수(IOPS)를 측정할 수 있습니다.</p> <p>단위: 바이트</p>

지표	설명
CloudBytesUploaded	<p>보고 기간 동안 게이트웨이가 AWS로부터 다운로드한 총 바이트 수입니다.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다.</p> <p>단위: 바이트</p>
FilesFailingUpload	<p>이 지표는 업로드하지 못한 파일 수를 추적합니다. AWS. 이 파일은 문제에 대한 자세한 정보가 포함된 상태 알림을 생성합니다.</p> <p>이 메트릭과 함께 사용 Sum 현재 업로드하지 못한 파일 수를 표시하는 통계 AWS.</p> <p>단위: 개수</p>
FileShares	<p>이 측정치는 게이트웨이의 파일 공유 수를 보고합니다.</p> <p>단위: 개수</p>
FileSystem-ERROR	<p>이 측정 단위는 ERROR 상태에 있는 이 게이트웨이의 파일 시스템 연결 수를 제공합니다.</p> <p>이 측정 단위가 모든 파일 시스템 연결이 ERROR 상태에 있다고 보고하면 게이트웨이에 문제가 발생하여 워크플로가 중단될 수 있습니다. 이 지표에 0이 아닌 값을 보고하는 시점에 대한 경보를 생성하는 것이 좋습니다.</p> <p>단위: 개수</p>
HealthNotifications	<p>이 지표는 보고 기간 동안 이 게이트웨이에 의해 생성된 상태 알림 수를 보고합니다.</p> <p>단위: 개수</p>

지표	설명
IoWaitPercent	이 지표는 CPU가 로컬 디스크의 응답을 대기하고 있는 시간의 비율을 보고합니다. 단위: %
MemTotalBytes	이 측정 단위는 게이트웨이의 총 메모리 양을 보고합니다. 단위: 바이트
MemUsedBytes	이 측정 단위는 게이트웨이에서 사용된 메모리 양을 보고합니다. 단위: 바이트
RootDiskFreeBytes	이 측정치는 게이트웨이의 루트 디스크에서 사용 가능한 바이트 수를 보고합니다. 이 측정 단위 보고서가 20GB 미만인 경우 루트 디스크의 크기를 늘려야 합니다. 단위: 바이트
SmbV2Sessions	이 측정치는 게이트웨이에서 활성 상태인 SMBv2 세션 수를 보고합니다. 단위: 개수
SmbV3Sessions	이 측정치는 게이트웨이에서 활성 상태인 SMBv3 세션 수를 보고합니다. 단위: 개수
TotalCacheSize	이 측정치는 캐시의 총 크기를 보고합니다. 단위: 바이트

지표	설명
UserCpuPercent	이 측정 단위는 게이트웨이 처리에 소요되는 시간의 비율을 보고합니다. 단위: %

파일 시스템 지표 이해

파일 공유를 나타내는 Storage Gateway 지표에 대해 다음과 같은 정보를 확인할 수 있습니다. 각 파일 공유에는 연결된 지표 집합이 있습니다. 일부 파일 공유별 지표는 특정 게이트웨이별 지표와 이름이 같습니다. 이러한 지표는 동일한 종류의 측정값을 나타내지만, 그 대신 파일 공유로 범위가 한정됩니다.

지표 관련 작업을 하려면 항상 먼저 게이트웨이와 파일 공유 중 어느 것과 관련된 작업을 할 것인지 지정해야 합니다. 특히 파일 공유 지표 작업을 할 때는 지표를 보고 싶은 파일 공유를 식별하는 File share ID를 지정해야 합니다. 자세한 정보는 [Amazon CloudWatch 지표 사용](#)을 참조하십시오.

다음 표에서는 파일 공유에 대한 정보를 얻는 데 사용할 수 있는 Storage Gateway 측정치에 대해 설명합니다.

지표	설명
CacheHitPercent	캐시로부터 읽는 파일 공유의 애플리케이션 읽기 작업 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 파일 공유로부터의 애플리케이션 읽기 작업이 없는 경우, 지표가 100%를 보고합니다. 단위: %
CachePercentDirty	AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율 중 파일 공유가 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 게이트웨이의 CachePercentDirty 지표를 사용하면 AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율을 알 수 있습니다.

지표	설명
CachePercentUsed	<p>단위: %</p> <p>게이트웨이의 캐시 스토리지의 전체 사용 백분율 중 파일 공유가 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다.</p> <p>게이트웨이의 CachePercentUsed 지표를 사용하면 게이트웨이의 캐시 스토리지의 전체 사용 백분율을 알 수 있습니다.</p> <p>단위: %</p>
CloudBytesUploaded	<p>게이트웨이가 로 업로드한 총 바이트 수입니다. AWS보고 기간 동안.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다.</p> <p>단위: 바이트</p>
CloudBytesDownloaded	<p>보고 기간 동안 게이트웨이가 AWS로부터 다운로드한 총 바이트 수입니다.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 초당 입력/출력 작업 수(IOPS)를 측정할 수 있습니다.</p> <p>단위: 바이트</p>

지표	설명
ReadBytes	<p>파일 공유에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 읽은 총 바이트 수입니다.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다.</p> <p>단위: 바이트</p>
WriteBytes	<p>보고 기간 동안 온프레미스 애플리케이션에 작성한 총 바이트 수입니다.</p> <p>이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다.</p> <p>단위: 바이트</p>

파일 게이트웨이 감사 로그 이해

Amazon FSx 파일 게이트웨이 (FSx 파일 게이트웨이) 감사 로그는 파일 시스템 연결 내의 파일과 폴더의 사용자 액세스에 대한 세부 정보를 제공합니다. 감사 로그를 사용하여 사용자 활동을 모니터링하고 부적절한 활동 패턴이 식별되면 조치를 취할 수 있습니다. 로그는 Windows 보안 이벤트에 대한 기존 로그 처리 도구와의 호환성을 지원하기 위해 Windows Server 보안 로그 이벤트와 유사하게 포맷됩니다.

작업

다음 표에서는 파일 게이트웨이 감사 로그 파일 액세스 작업에 대해 설명합니다.

작업 이름	정의
데이터 읽기	파일의 내용을 읽습니다.
데이터 쓰기	파일의 내용을 변경합니다.
생성	새 파일 또는 폴더를 만듭니다.

작업 이름	정의
이름 바꾸기	기존 파일 또는 폴더의 이름을 바꿉니다.
Delete	파일 또는 폴더를 삭제합니다.
쓰기 속성	파일 또는 폴더 메타데이터(ACL, 소유자, 그룹, 권한)를 업데이트합니다.

속성

다음 표에서는 FSx 파일 게이트웨이 감사 로그 파일 액세스 속성에 대해 설명합니다.

속성	정의
securityDescriptor	객체에 설정된 DACL(임의 액세스 제어 목록)을 SDDL 형식으로 표시합니다.
sourceAddress	파일 공유 클라이언트 머신의 IP 주소입니다.
SubjectDomainName	클라이언트의 계정이 속한 AD(Active Directory) 도메인입니다.
SubjectUserName	클라이언트의 Active Directory 사용자 이름입니다.
source	Storage Gateway 게이트웨이의 IDFileSystemAssociation 감사를 받고 있습니다.
mtime	클라이언트에서 설정한 객체의 콘텐츠가 수정된 시간입니다.
version	감사 로그 형식의 버전입니다.
ObjectType	객체가 파일 또는 폴더인지를 정의합니다.
locationDnsName	FSx 파일 게이트웨이 시스템 DNS 이름입니다.
objectName	객체의 전체 경로입니다.

속성	정의
ctime	클라이언트에서 설정한 객체의 콘텐츠나 메타데이터가 수정된 시간입니다.
shareName	액세스 중인 공유의 이름입니다.
operation	객체 액세스 작업의 이름입니다.
newObjectName	이름이 바뀐 후 새 객체의 전체 경로입니다.
gateway	스토리지 게이트웨이 ID입니다.
status	작업의 상태입니다. 성공만 기록됩니다 (권한 거부로 인해 발생한 실패를 제외하고 실패가 기록됩니다).
fileSizeInBytes	파일 생성 시 클라이언트에서 설정한 파일 크기 (바이트)입니다.

작업당 로깅된 속성

다음 표에서는 각 파일 액세스 작업에서 기록된 FSx 파일 게이트웨이 감사 로그 속성에 대해 설명합니다.

	데이터 읽기	데이터 쓰기	폴더 생성	파일 생성	파일/폴더 이름 바꾸기	파일/폴더 삭제	특성 쓰기 (ACL 변경)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
security							X			
source	X	X	X	X	X	X	X	X	X	X

	데이터 읽기	데이터 쓰기	폴더 생성	파일 생성	파일/폴더 이름 바꾸기	파일/폴더 삭제	특성 쓰기 (ACL 변경)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
Subject mainName	X	X	X	X	X	X	X	X	X	X
Subject erName	X	X	X	X	X	X	X	X	X	X
source	X	X	X	X	X	X	X	X	X	X
mtime			X	X						
version	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
locationName	X	X	X	X	X	X	X	X	X	X
object e	X	X	X	X	X	X	X	X	X	X
ctime			X	X						
shareName	X	X	X	X	X	X	X	X	X	X
operation	X	X	X	X	X	X	X	X	X	X
newObjectName					X					
gateway	X	X	X	X	X	X	X	X	X	X

	데이터 읽기	데이터 쓰기	폴더 생성	파일 생성	파일/폴더 이름 바꾸기	파일/폴더 삭제	특성 쓰기 (ACL 변경)	쓰기 속성 (chown)	쓰기 속성 (chmod)	쓰기 속성 (chgrp)
status	X	X	X	X	X	X	X	X	X	X
fileSize				X						

게이트웨이 유지

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.

주제

- [게이트웨이 VM 종료](#)
- [Storage Gateway 로컬 디스크 관리](#)
- [AWS Storage Gateway 콘솔을 사용한 게이트웨이 업데이트 관리](#)
- [로컬 콘솔에서 유지 관리 작업 수행](#)
- [AWS Storage Gateway 콘솔을 사용한 게이트웨이 삭제와 연결된 리소스 제거](#)

게이트웨이 VM 종료

- 게이트웨이 VM 로컬 콘솔 (참조) [로컬 콘솔에서 유지 관리 작업 수행](#).
- Storage Gateway API—을 참조하십시오. [ShutdownGateway](#)

Storage Gateway 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 캐시 스토리지의 크기 결정](#)
- [캐시 스토리지 추가](#)

로컬 디스크 스토리지 용량 결정

게이트웨이에 할당하려는 디스크의 개수 및 크기는 사용자가 직접 결정합니다. 게이트웨이를 사용하려면 다음과 같은 추가 스토리지가 필요합니다.

파일 게이트웨이에는 캐시로 사용할 디스크가 한 개 이상 필요합니다. 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	게이트웨이 유형
캐시 스토리지	캐시 스토리지는 Amazon S3 또는 파일 시스템에 업로드 보류 중인 데이터를 위한 온프레미스 내구성 저장소의 역할을 합니다.	<ul style="list-style-type: none"> 파일 게이트웨이

Note

기본 물리 스토리지 리소스는 VMware에서 데이터 스토어로 표시됩니다. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 로컬 디스크를 프로비저닝하는 경우 (예: 캐시 스토리지 용도), 가상 디스크를 동일한 데이터 스토어에 VM으로 저장하거나 다른 데이터 스토어에 저장하는 옵션을 선택할 수 있습니다.

데이터 스토어가 한 개 이상인 경우에는 캐시 스토리지에 데이터 스토어 한 개씩 선택하는 것이 좋습니다. 오직 기본 물리 디스크 한 개의 지원을 받는 데이터 스토어는 캐시 스토리지를 모두 지원하는 데 사용되는 경우 성능이 떨어질 수 있습니다. 이는 백업이 RAID1 같이 성능이 비교적 떨어지는 RAID 구성일 때도 마찬가지입니다.

게이트웨이의 초기 구성 및 배포 후에는 캐시 스토리지의 디스크를 추가하여 로컬 스토리지를 조정할 수 있습니다.

할당할 캐시 스토리지의 크기 결정

초기에는 이 근사치를 사용하여 캐시 스토리지용 디스크를 프로비저닝할 수 있습니다. 그런 다음 Amazon CloudWatch 운영 측정치를 사용하여 캐시 스토리지 사용량을 모니터링하고 콘솔을 사용하여 필요에 따라 추가 스토리지를 프로비저닝할 수 있습니다. 측정치 사용 및 경고 설정에 대한 정보는 [성능](#) 단원을 참조하십시오.

캐시 스토리지 추가

애플리케이션 요구 사항이 변화함에 따라 게이트웨이의 캐시 스토리지 용량을 늘릴 수 있습니다. 기존 게이트웨이 기능을 중지하지 않고 게이트웨이에 캐시 용량을 추가할 수 있습니다. 스토리지 용량을 추가할 때는 게이트웨이 VM이 켜져 있어야 합니다.

Important

기존 게이트웨이에 캐시를 추가할 때 호스트에 새 디스크를 생성하는 것이 중요합니다 (하이퍼바이저 또는 Amazon EC2 인스턴스). 이전에 디스크가 캐시로 할당되었던 경우, 디스크 크기를 변경하지 마십시오. 캐시 스토리지로 할당된 캐시 디스크를 제거하지 마십시오.

다음 절차는 게이트웨이에 스토리지를 구성하거나 캐시하는 방법을 안내합니다.

스토리지를 추가 및 구성 또는 캐시하려면

1. 호스트 (하이퍼바이저 또는 Amazon EC2 인스턴스) 에서 새 디스크를 프로비저닝합니다. 하이퍼바이저에서 디스크를 프로비저닝하는 방법에 대한 자세한 내용은 하이퍼바이저의 사용자 매뉴얼을 참조하십시오. 이 디스크를 캐시 스토리지로 구성합니다.
2. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
3. 탐색 창에서 게이트웨이를 선택합니다.
4. 작업 메뉴에서 로컬 디스크 편집을 선택합니다.
5. [Edit local disk] 대화 상자에서 프로비저닝한 디스크를 식별하여 캐시된 스토리지에 어떤 디스크를 사용할지 결정합니다.

해당 디스크가 보이지 않으면 새로 고침 버튼을 선택하십시오.

6. 저장을 선택하여 구성 설정을 저장합니다.

FSx 파일 게이트웨이는 임시 스토리지를 지원하지 않습니다.

AWS Storage Gateway 콘솔을 사용한 게이트웨이 업데이트 관리

Storage Gateway 대한 중요 소프트웨어 업데이트를 정기적으로 릴리스합니다. Storage Gateway Management Console에서 업데이트를 수동으로 적용하거나, 구성된 유지 관리 일정 동안 업데이트를 자동으로 적용할 때까지 기다릴 수 있습니다. Storage Gateway는 매분 업데이트를 확인하지만 유지 관리를 완료하고 나서 업데이트가 있는 경우에만 다시 시작합니다.

게이트웨이 소프트웨어 릴리스에는 운영 체제 업데이트 및 보안 패치가 정기적으로 포함됩니다. AWS. 이러한 업데이트는 일반적으로 6개월마다 릴리스되며 예약된 유지 관리 기간 동안 일반 게이트웨이 업데이트 프로세스의 일부로 적용됩니다.

Note

Storage Gateway 어플라이언스를 관리되는 내장 디바이스로 취급해야 하며, 어떤 식으로든 설치에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 게이트웨이 업데이트 메커니즘 이외의 방법 (예: SSM 또는 하이퍼바이저 도구) 을 사용하여 소프트웨어 패키지를 설치하거나 업데이트하려고 하면 게이트웨이가 오작동할 수 있습니다.

게이트웨이에 업데이트가 적용되기 전에 AWS Storage Gateway 콘솔에 메시지가 표시되고 AWS Health Dashboard. 자세한 정보는 [AWS Health Dashboard](#) 을 참조하십시오. VM이 재부팅되지는 않지만, 업데이트가 진행되고 다시 시작되는 잠시 동안은 게이트웨이를 사용할 수 없습니다.

게이트웨이를 배포하고 활성화하면 기본적인 주간 유지 관리 일정이 설정됩니다. 언제라도 유지 관리 일정을 수정할 수 있습니다. 업데이트가 제공되면 세부 정보 탭에 유지 관리 메시지가 표시됩니다. 세부 정보 탭에서는 게이트웨이에 마지막으로 성공한 업데이트가 적용된 날짜와 시간을 확인할 수 있습니다.

유지 관리 일정을 수정하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 게이트웨이를 선택한 후 업데이트 일정을 수정할 게이트웨이를 선택합니다.
3. 작업에서 유지 관리 기간 편집을 선택하여 유지 관리 시작 시간 편집 대화 상자를 엽니다.
4. 일정에서 매주 또는 매월을 선택하여 업데이트를 예약합니다.
5. 매주를 선택하는 경우 요일 및 시간의 값을 수정합니다.

매월을 선택하는 경우 일 및 시간의 값을 수정합니다. 이 옵션을 선택한 경우 오류가 발생하면 게이트웨이가 이전 버전이며 아직 최신 버전으로 업그레이드되지 않았음을 의미합니다.

Note

해당 월의 최대 값을 설정할 수 있는 값은 28입니다. 28을 선택하면 유지 관리 시작 시간은 매월 28일이 됩니다.

유지 관리 시작 시간이세부 정보다음에 다음 번 열 때 게이트웨이에 대한 탭세부 정보탭.

로컬 콘솔에서 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.

주제

- [VM 로컬 콘솔 \(파일 게이트웨이\) 에서 작업 수행](#)
- [Amazon EC2 로컬 콘솔 \(파일 게이트웨이\) 에서 작업 수행](#)
- [게이트웨이 로컬 콘솔 액세스](#)
- [게이트웨이용 네트워크 어댑터 구성](#)

VM 로컬 콘솔 (파일 게이트웨이) 에서 작업 수행

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

주제

- [파일 게이트웨이 로컬 콘솔에 로그인](#)
- [HTTP 프록시 구성](#)
- [게이트웨이 네트워크 설정 구성](#)
- [게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트](#)
- [게이트웨이 시스템 리소스 상태 보기](#)
- [게이트웨이의 네트워크 시간 프로토콜 \(NTP\) 서버 구성](#)
- [로컬 콘솔에서 스토리지 게이트웨이 명령 실행](#)
- [게이트웨이용 네트워크 어댑터 구성](#)

파일 게이트웨이 로컬 콘솔에 로그인

VM이 로그인할 준비가 되면 로그인 화면이 표시됩니다. 로컬 콘솔에 처음 로그인하는 경우, 기본 사용자 이름 및 암호를 사용하여 로그인합니다. 이 기본 로그인 자격 증명을 통해 게이트웨이 네트워크 설정을 구성하고 로컬 콘솔에서 암호를 변경할 수 있는 메뉴에 액세스할 수 있습니다. AWS Storage Gateway는 로컬 콘솔에서 암호를 변경하는 대신 Storage Gateway 콘솔에서 자신의 암호를 설정 가능하게 합니다. 새 암호를 설정하기 위해 기본 암호를 알 필요는 없습니다. 자세한 정보는 [파일 게이트웨이 로컬 콘솔에 로그인](#)을 참조하십시오.

게이트웨이의 로컬 콘솔에 로그인하려면

- 로컬 콘솔에 처음 로그인하는 경우, 기본 자격 증명을 사용하여 VM에 로그인합니다. 기본 사용자 이름과 암호는 각각 admin 및 password입니다. 또는 자격 증명을 사용하여 로그인합니다.

Note

기본 암호를 변경하는 것이 좋습니다. 로컬 콘솔 메뉴(기본 메뉴의 6번 항목)에서 passwd 명령을 실행하여 변경할 수 있습니다. 명령을 실행하는 방법에 대한 정보는 [로컬 콘솔에서 스토리지 게이트웨이 명령 실행](#) 섹션을 참조하십시오. Storage Gateway 콘솔에서 암호를 설정할 수도 있습니다. 자세한 정보는 [파일 게이트웨이 로컬 콘솔에 로그인](#)을 참조하십시오.

Storage Gateway 콘솔에서 로컬 콘솔 암호 설정

로컬 콘솔에 처음 로그인하는 경우, 기본 자격 증명을 사용하여 VM에 로그인합니다. 모든 유형의 게이트웨이에 기본 자격 증명을 사용합니다. 사용자 이름은 admin이고, 암호는 password입니다.

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

- 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
- 탐색 창에서 게이트웨이를 선택한 후 새 암호를 설정할 게이트웨이를 선택합니다.
- 작업에서 Set Local Console Password(로컬 콘솔 암호 설정)을 선택합니다.

4. Set Local Console Password(로컬 콘솔 암호 설정) 대화 상자에 새 암호를 입력해 확인한 후 저장을 선택합니다.

새 암호가 기본 암호를 대체합니다. Storage Gateway는 암호를 저장하지 않지만, 대신 VM에 안전하게 전송합니다.

Note

암호는 키보드에 있는 어떤 문자로도 구성할 수 있으며 1—512개의 문자까지 가능합니다.

HTTP 프록시 구성

파일 게이트웨이는 HTTP 프록시 구성을 지원합니다.

Note

파일 게이트웨이는 HTTP 프록시 구성만 지원합니다.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우에는 게이트웨이에 HTTP 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 그러면 Storage Gateway 가 모두 라우팅됩니다AWS프록시 서버를 통한 엔드포인트 트래픽 게이트웨이와 엔드포인트 간의 통신은 HTTP 프록시를 사용하는 경우에도 암호화됩니다. 게이트웨이의 네트워크 요건에 대한 정보는 [네트워크 및 방화벽 요구 사항](#) 단원을 참조하십시오.

파일 게이트웨이에 HTTP 프록시를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - Linux 커널 기반 가상 머신(KVM)의 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
2. 온AWS어플라이언스 활성화 - 구성기본 메뉴 입력1를 눌러 HTTP 프록시 구성을 시작하십시오.

3. HTTP Proxy Configuration(HTTP 프록시 구성) 메뉴에서 **1**을 입력하여 HTTP 프록시 서버의 호스트 이름을 제공합니다.

다음과 같이, 이 메뉴에서 다른 HTTP 설정을 구성할 수 있습니다.

To	조치
HTTP 프록시 구성	<p>1을 입력합니다.</p> <p>구성을 완료하려면 호스트 이름 및 포트를 입력해야 합니다.</p>
현재 HTTP 프록시 구성 조회	<p>2을 입력합니다.</p> <p>HTTP 프록시가 구성되어 있지 않은 경우 HTTP Proxy not configured 메시지가 표시됩니다. HTTP 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.</p>
HTTP 프록시 구성 제거	<p>3을 입력합니다.</p> <p>메시지 HTTP Proxy Configuration Removed 가 나타납니다.</p>

4. VM을 다시 시작하여 HTTP 구성에 대한 설정을 적용합니다.

게이트웨이 네트워크 설정 구성

게이트웨이의 기본 네트워크 구성은 DHCP(Dynamic Host Configuration Protocol)입니다. DHCP를 통해 게이트웨이에 IP 주소가 자동으로 지정됩니다. 다음 설명과 같이 게이트웨이의 IP를 고정 IP 주소로 수동 지정해야 하는 경우가 있을 수 있습니다.

고정 IP 주소를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - KVM 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
2. 온AWS어플라이언스 활성화 - 구성기본 메뉴 입력2를 눌러 네트워크 구성을 시작합니다.
 3. Network Configuration(네트워크 구성) 메뉴에서 다음 옵션 중 하나를 선택하십시오.

To	조치
네트워크 어댑터에 대한 정보 얻기	<p>1을 입력합니다.</p> <p>어댑터 이름 목록이 나타나고 어댑터 이름을 입력하라는 메시지가 표시됩니다 (예:eth0. 지정하려는 어댑터가 사용 중인 경우, 다음과 같은 어댑터 정보가 표시됩니다.</p> <ul style="list-style-type: none"> • 미디어 액세스 제어(MAC) 주소 • IP 주소 • 넷마스크 • 게이트웨이 IP 주소 • DHCP 활성화 상태 <p>고정 IP 주소를 구성할 때(옵션 3) 게이트웨이의 기본 경로 어댑터를 설정할 때(옵션 5)와 동일한 어댑터 이름을 사용합니다.</p>

To	조치
DHCP 구성	<p>2을 입력합니다.</p> <p>DHCP를 사용하도록 네트워크 인터페이스를 구성하라는 메시지가 표시됩니다.</p>

To	조치
게이트웨이에 고정 IP 주소 구성	<p>3을 입력합니다.</p> <p>다음 정보를 입력하여 고정 IP를 구성하라는 메시지가 표시됩니다.</p> <ul style="list-style-type: none"> • 네트워크 어댑터 이름 • IP 주소 • 넷마스크 • 기본 게이트웨이 주소 • 기본 DNS(Domain Name Service) 주소 • 보조 DNS 주소 <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin: 10px 0;"> <p>⚠ Important</p> <p>게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway Console에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 정보는 게이트웨이 VM 종료을 참조하십시오.</p> </div> <p>게이트웨이에서 네트워크 인터페이스를 한 개 이상 사용하는 경우, 모든 활성화된 인터페이스에서 DHCP 또는 고정 IP 주소를 사용하도록 설정해야 합니다.</p>

To	조치
	<p>예를 들어 게이트웨이 VM이 DHCP로 구성된 인터페이스 두 개를 사용한다고 가정합니다. 나중에 한 인터페이스를 고정 IP로 설정하면 다른 하나는 비활성화됩니다. 이 경우 인터페이스를 활성화하려면 고정 IP로 설정해야 합니다.</p> <p>처음에 두 인터페이스 모두 고정 IP 주소를 사용하도록 설정한 후 DHCP를 사용하도록 게이트웨이를 설정하면 두 인터페이스 모두 DHCP를 사용하게 됩니다.</p>
<p>게이트웨이의 모든 네트워크 구성을 DHCP로 재설정</p>	<p>4을 입력합니다.</p> <p>모든 네트워크 인터페이스가 DHCP를 사용하도록 설정됩니다.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Important</p> <p>게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway Console에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 정보는 게이트웨이 VM 종료을 참조하십시오.</p> </div>
<p>게이트웨이의 기본 경로 어댑터 설정</p>	<p>5을 입력합니다.</p> <p>게이트웨이에 사용할 수 있는 어댑터가 표시되고 어댑터 중 하나를 선택하라는 메시지가 표시됩니다 (예:eth0).</p>

To	조치
게이트웨이 DSN 구성 편집	<p>6을 입력합니다.</p> <p>주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. 새 IP 주소를 제공하라는 메시지가 나타납니다.</p>
게이트웨이의 DNS 구성 조회	<p>7을 입력합니다.</p> <p>주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다.</p> <div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>일부 VMware 하이퍼바이저 버전은 이 메뉴에서 어댑터 구성을 편집할 수 있습니다.</p> </div>
라우팅 테이블 조회	<p>8을 입력합니다.</p> <p>게이트웨이의 기본 경로가 표시됩니다.</p>

게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트

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

게이트웨이 시스템 리소스 상태 보기

게이트웨이가 시작되고, 가상 CPU 코어 루트 볼륨 크기와 RAM을 점검합니다. 이후 시스템 리소스가 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 게이트웨이의 로컬 콘솔에서 점검 결과를 볼 수 있습니다.

시스템 리소스 점검의 상태를 보려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
 - KVM 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
2. 에서AWS어플라이언스 활성화 - 구성기본 메뉴 입력4를 눌러 시스템 리소스 점검 결과를 보십시오.

다음 표의 설명처럼 콘솔에서 각 리소스에 [확인], [경고] 또는 [실패] 메시지가 표시됩니다.

Message	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 않지만 게이트웨이는 계속해서 작동합니다. Storage Gateway 리소스 점검 결과를 설명하는 메시지가 에 표시됩니다.
[실패]	리소스가 최소 요구 사항을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. Storage Gateway 리소스 점검 결과를 설명하는 메시지가 에 표시됩니다.

콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

게이트웨이의 네트워크 시간 프로토콜 (NTP) 서버 구성

네트워크 시간 프로토콜(NTP) 서버 구성을 보고 편집할 수 있으며, 게이트웨이와 하이퍼바이저 호스트의 VM 시간을 동기화할 수 있습니다.

시스템 시간 관리

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - KVM 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
2. AWS어플라이언스 활성화 - 구성기본 메뉴 입력5시스템 시간을 관리합니다.
3. System Time Management(시스템 시간 관리) 메뉴에서 다음 옵션 중 하나를 선택하십시오.

To	조치
VM 시간과 NTP 서버 시간을 확인해 동기화합니다.	<p>1을 입력합니다.</p> <p>현재 VM 시간이 표시됩니다. 파일 게이트웨이가 게이트웨이 VM과 NTP 서버 시간 차이를 결정하며, VM 시간과 NTP 시간을 동기화하라는 메시지가 표시됩니다.</p> <p>게이트웨이를 배포하고 실행한 후에 게이트웨이 VM의 시간에 오차가 생기는 경우가 있을 수 있습니다. 예를 들어 네트워크 중단이 지속되어 하이퍼바이저 호스트와 게이트웨이의 시간이 업데이트되지 않았다고 가정하겠습니다. 이 경우, 게이트웨이 VM 시간이 실제 시간과 다릅니다. 시간 오차가 있는 경우, 스냅샷과 같은 작업이 실행되도록 지정한 시간과 작업이 실제 이루어지는 시간 사이에 불일치가 발생합니다.</p> <p>VMware ESXi에 배포한 게이트웨이의 경우, 하이퍼바이저 호스트 시간을 설정하고 호스트에 VM 시간을 동기화하는 것만으로도 시간 오차를</p>

To	조치
	<p>방지하는 데 충분합니다. 자세한 정보는 VM 시간을 호스트 시간과 동기화를 참조하십시오.</p> <p>Microsoft Hyper-V에 배포한 게이트웨이의 경우, VM의 시간을 주기적으로 점검해야 합니다. 자세한 정보는 게이트웨이 VM 시간 동기화를 참조하십시오.</p> <p>KVM에 배포된 게이트웨이의 경우 KVM용 virsh 명령줄 인터페이스를 사용하여 VM 시간을 확인하고 동기화할 수 있습니다.</p>
NTP 서버 구성 편집	<p>2을 입력합니다.</p> <p>선호하는 NTP 서버와 부 NTP 서버를 제공하라는 메시지가 표시됩니다.</p>
NTP 서버 구성 보기	<p>3을 입력합니다.</p> <p>NTP 서버 구성이 표시됩니다.</p>

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 테이블을 저장하거나 Amazon Web Services Support에 접속하는 등 유지관리 작업을 수행할 수 있습니다.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
- Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.

- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
2. 온AWS어플라이언스 활성화 - 구성기본 메뉴 입력6...에 대한 명령 프롬프트.
 3. 온AWS기기 활성화 - 명령 프롬프트콘솔, 입력h를 누른 다음 를 누릅니다.돌아가기키.

콘솔에는 다음 스크린샷과 같이 AVAILABLE COMMANDS(사용 가능한 명령) 메뉴와 함께 명령의 기능이 표시됩니다.
 4. 명령 프롬프트에 사용하기 원하는 명령을 입력한 후 지침을 따릅니다.

명령에 대해 알아보려면 명령 프롬프트에 명령의 이름을 입력합니다.

게이트웨이용 네트워크 어댑터 구성

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

주제

- [VMXNET3 네트워크 어댑터를 사용하도록 게이트웨이 구성](#)

VMXNET3 네트워크 어댑터를 사용하도록 게이트웨이 구성

Storage Gateway VMware ESXi 및 Microsoft Hyper-V Hypervisor 호스트 모두에서 E1000 네트워크 어댑터 유형을 지원합니다. 그러나 VMXNET3(10GbE) 네트워크 어댑터 유형은 VMware ESXi 하이퍼바이저에서만 지원합니다. 게이트웨이를 VMware ESXi 하이퍼바이저에서 호스팅하는 경우, VMXNET3(10GbE) 어댑터 입력을 사용할 수 있도록 게이트웨이를 다시 구성할 수 있습니다. 이 어댑터에 대한 자세한 내용은 [VMware 웹 사이트](#)를 참조하십시오.

KVM 하이퍼바이저 호스트의 경우 Storage Gatewayvirtio네트워크 장치 드라이버 KVM 호스트에 대한 E1000 네트워크 어댑터 유형의 사용은 지원되지 않습니다.

⚠ Important

VMXNET3를 선택하려면 게스트 운영 체제 입력이 Other Linux64(기타 Linux64)이어야 합니다.

VMXNET3 어댑터를 사용하도록 게이트웨이를 구성하려면 다음 단계를 수행해야 합니다.

1. 기본 E1000 어댑터를 제거합니다.
2. VMXNET3 어댑터를 추가합니다.
3. 게이트웨이 다시 시작합니다.
4. 네트워크용 어댑터를 구성합니다.

각 단계를 수행하는 자세한 방법은 다음과 같습니다.

기본 E1000 어댑터를 제거하고 VMXNET3 어댑터를 사용하도록 게이트웨이를 구성하려면

1. VMware에서 게이트웨이를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 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 Enter(어댑터 입력) 섹션에서 현재 어댑터가 E1000임을 알 수 있습니다. 이 어댑터를 VMXNET3 어댑터로 교체합니다.
4. E1000 네트워크 어댑터를 선택한 후 제거를 선택합니다. 이 예에서 E1000 네트워크 어댑터는 Network adapter 1(네트워크 어댑터 1)입니다.

i Note

게이트웨이에서 E1000 및 VMXNET3 네트워크 어댑터를 동시에 실행할 수 있지만 네트워크 문제를 일으킬 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 입력 마법사에서 **VMXNET3...**에 대한 어댑터 입력을 선택한 다음을 선택합니다. 다음.

8. Virtual Machine Properties(가상 머신 속성) 마법사의 Adapter Enter(어댑터 입력) 섹션에서 Current Adapter(현재 어댑터)가 VMXNET3로 설정되어 있는지 확인한 후 OK를 선택합니다.
9. VMware VSphere 클라이언트에서 해당 게이트웨이를 종료합니다.
10. VMware VSphere 클라이언트에서 해당 게이트웨이를 재시작합니다.

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

네트워크용 어댑터를 구성하려면

1. VSphere 클라이언트에서 Console(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 정보는 [파일 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하십시오.
2. 프롬프트에서 **2**를 입력하여 Network Configuration(네트워크 구성)을 선택한 후 **Enter**를 눌러 네트워크 구성 메뉴를 엽니다.
3. 프롬프트에서 **4**를 입력하여 Reset all to DHCP(모두 DHCP로 재설정)을 선택한 후 프롬프트에 (예인 경우) **y**를 입력하여 모든 어댑터가 동적 호스트 구성 프로토콜(DHCP)을 사용하도록 설정합니다. 모든 사용 가능 어댑터가 DHCP를 사용하도록 설정됩니다.

게이트웨이가 이미 활성화된 경우, Storage Gateway 관리 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 게이트웨이를 다시 시작한 후 네트워크가 인터넷에 연결되어 있는지 테스트해야 합니다. 네트워크 연결을 테스트하는 방법에 대한 정보는 [게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트](#) 섹션을 참조하십시오.

Amazon EC2 로컬 콘솔 (파일 게이트웨이) 에서 작업 수행

일부 유지 관리 작업의 경우, Amazon EC2 인스턴스에 배포한 게이트웨이를 실행하려면 로컬 콘솔에 로그인해야 합니다. 이 단원에서는 로컬 콘솔에 로그인하여 유지 관리 작업을 수행하는 방법에 대한 정보를 얻을 수 있습니다.

주제

- [Amazon EC2 게이트웨이 로컬 콘솔에 로그인](#)

- [HTTP 프록시를 통해 EC2에 배포된 게이트웨이 라우팅](#)
- [게이트웨이 네트워크 설정 구성](#)
- [게이트웨이의 네트워크 연결 테스트](#)
- [게이트웨이 시스템 리소스 상태 보기](#)
- [로컬 콘솔에서 Storage Gateway 명령 실행](#)

Amazon EC2 게이트웨이 로컬 콘솔에 로그인

SSH (Secure Shell) 클라이언트를 사용하여 Amazon EC2 인스턴스에 연결할 수 있습니다. 자세한 내용은 단원을 참조하십시오. [인스턴스에 연결합니다](#)의 Amazon EC2 사용 설명서. 이런 방식으로 연결하려면 인스턴스를 시작할 때 지정한 SSH 키 페어가 필요합니다. Amazon EC2 키 페어에 대한 자세한 내용은 섹션을 참조하십시오. [Amazon EC2 키 페어](#)의 Amazon EC2 사용 설명서.

게이트웨이 로컬 콘솔에 로그인하려면

1. 로컬 콘솔에 로그인합니다. EC2 인스턴스에 연결하는 경우, admin으로 로그인합니다.
2. 로그인하면 다음 스크린샷과 같이 AWS 어플라이언스 정품 인증 - 구성 기본 메뉴가 표시됩니다.

이에 대해 자세히 알아봅니다.	이 주제를 참조하십시오.
게이트웨이에 HTTP 프록시를 구성	HTTP 프록시를 통해 EC2에 배포된 게이트웨이 라우팅
게이트웨이 네트워크 설정 구성	게이트웨이의 네트워크 연결 테스트
네트워크 연결 테스트	게이트웨이의 네트워크 연결 테스트
시스템 리소스 점검 조회	Amazon EC2 게이트웨이 로컬 콘솔에 로그인.
Storage Gateway 콘솔 명령 실행	로컬 콘솔에서 Storage Gateway 명령 실행

게이트웨이를 종료하려면 **0**을 입력합니다.

구성 세션을 종료하려면 **x**을 입력하여 메뉴를 종료합니다.

HTTP 프록시를 통해 EC2에 배포된 게이트웨이 라우팅

Storage Gateway Amazon EC2 배포한 게이트웨이 간 Socket Secure 버전 5 (SOCKS5) 프록시 구성을 지원합니다.AWS.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우에는 게이트웨이에 HTTP 프록시 설정을 구성해야 합니다. 이를 위해서는 프록시를 실행하는 호스트에 IP 주소와 포트 번호를 지정하면 됩니다. 그러면 Storage Gateway 가 모두 라우팅됩니다AWS프록시 서버를 통한 엔드포인트 트래픽 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 참조하세요.
2. 온AWS어플라이언스 활성화 - 구성기본 메뉴 입력1를 눌러 HTTP 프록시 구성을 시작하십시오.
3. AWS 어플라이언스 정품 인증 - 구성 HTTP Proxy Configuration(HTTP 프록시 구성) 메뉴에서 다음 옵션 중 하나를 선택합니다.

To	수행할 작업
HTTP 프록시 구성	1을 입력합니다. 구성을 완료하려면 호스트 이름 및 포트를 입력해야 합니다.
현재 HTTP 프록시 구성 조회	2을 입력합니다. HTTP 프록시가 구성되어 있지 않은 경우 HTTP Proxy not configured 라는 메시지가 표시됩니다. HTTP 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.
HTTP 프록시 구성 제거	3을 입력합니다.

To	수행할 작업
	메시지 HTTP Proxy Configuration Removed 가 나타납니다.

게이트웨이 네트워크 설정 구성

로컬 콘솔을 통해 도메인 이름 서버(DNS)를 보고 구성할 수 있습니다.

고정 IP 주소를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하세요.
2. 온AWS어플라이언스 활성화 - 구성기본 메뉴 입력2DNS 서버 구성을 시작합니다.
3. Network Configuration(네트워크 구성) 메뉴에서 다음 옵션 중 하나를 선택하십시오.

To	수행할 작업
게이트웨이 DSN 구성 편집	<p>1을 입력합니다.</p> <p>주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다. 새 IP 주소를 제공하라는 메시지가 나타납니다.</p>
게이트웨이의 DNS 구성 조회	<p>2을 입력합니다.</p> <p>주 및 부 DNS 서버에서 사용 가능한 어댑터가 표시됩니다.</p>

게이트웨이의 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 참조하세요.
2. 에서AWS어플라이언스 활성화 - 구성주 메뉴에서 선택할 해당 숫자를 입력하십시오.네트워크 연결 테스트.

게이트웨이가 이미 활성화되면 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 엔드포인트 유형을 지정해야 합니다.AWS 리전다음 단계에 설명된 대로

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 공용 끝점 유형을 선택한 경우 해당 숫자를 입력하여AWS 리전테스트하는 데 사용할 수 있습니다. 지원되는 경우AWS 리전의 목록입니다.AWSStorage Gateway 함께 사용할 수 있는 서비스 엔드포인트는 단원을 참조하십시오.[AWS Storage Gateway엔드포인트 및 할당량](#)의AWS일반 참조.

테스트가 진행됨에 따라 각 끝점은 다음 중 하나를 표시합니다.[통과]또는[실패]예: 연결 상태를 나타냅니다.

Message	설명
[통과]	Storage Gateway 게이트웨이에는 네트워크 연결이 있습니다.
[실패]	Storage Gateway 게이트웨이에는 네트워크 연결이 없습니다.

게이트웨이 시스템 리소스 상태 보기

게이트웨이가 시작되고, 가상 CPU 코어 루트 볼륨 크기와 RAM을 점검합니다. 이후 시스템 리소스가 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 게이트웨이의 로컬 콘솔에서 점검 결과를 볼 수 있습니다.

시스템 리소스 점검의 상태를 보려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하세요.
2. 에서Storage Gateway 구성기본 메뉴 입력4를 눌러 시스템 리소스 점검 결과를 보십시오.

다음 표의 설명처럼 콘솔에서 각 리소스에 [확인], [경고] 또는 [실패] 메시지가 표시됩니다.

Message	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 않지만 게이트웨이는 계속해서 작동합니다. Storage Gateway 리소스 점검 결과를 설명하는 메시지가 에 표시됩니다.
[실패]	리소스가 최소 요구 사항을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. Storage Gateway 리소스 점검 결과를 설명하는 메시지가 에 표시됩니다.

콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

로컬 콘솔에서 Storage Gateway 명령 실행

AWS Storage Gateway 콘솔은 게이트웨이 관련 문제를 구성 및 진단할 수 있는 안전한 환경을 제공합니다. 콘솔 명령을 사용하여 라우팅 테이블을 저장하거나 Amazon Web Services Support에 접속하는 등 유지관리 작업을 수행할 수 있습니다.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하세요.
2. 에서AWS어플라이언스 활성화 구성기본 메뉴 입력5...에 대한게이트웨이 콘솔.

3. 명령 프롬프트에서 **h**를 입력한 다음 Return 키를 누릅니다.

그러면 사용 가능한 명령이 있는 AVAILABLE COMMANDS(사용 가능 명령) 메뉴가 콘솔에 표시됩니다. 다음 스크린샷과 같이 메뉴에 이어 게이트웨이 콘솔 프롬프트가 나타납니다.

4. 명령 프롬프트에 사용하기 원하는 명령을 입력한 후 지침을 따릅니다.

명령에 대해 알아보려면 명령 프롬프트에 명령의 이름을 입력합니다.

게이트웨이 로컬 콘솔 액세스

VM 로컬 콘솔에 액세스하는 방법은 게이트웨이 VM이 배포된 하이퍼바이저 종류에 따라 달라집니다. 이 섹션에서는 Linux 커널 기반 가상 머신(KVM), VMware ESXi 및 Microsoft Hyper-V Manager를 사용하여 VM 로컬 콘솔에 액세스하는 방법에 대한 정보를 찾을 수 있습니다.

주제

- [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)

Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스

사용 중인 Linux 배포판에 따라 KVM에서 실행되는 가상 머신을 구성하는 방법에는 여러 가지가 있습니다. 명령줄에서 KVM 구성 옵션에 액세스하는 지침은 다음과 같습니다. 지침은 KVM 구현에 따라 다를 수 있습니다.

KVM을 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

1. 다음 명령을 사용하여 현재 KVM에서 사용할 수 있는 VM을 나열합니다.

```
# virsh list
```

Id별로 사용 가능한 VM을 선택할 수 있습니다.

2. 로컬 콘솔에 액세스하려면 다음 명령을 사용합니다.

```
# virsh console VM_Id
```

3. 로컬 콘솔에 로그인하기 위한 기본 자격 증명을 얻으려면 [파일 게이트웨이 로컬 콘솔에 로그인](#) 단원을 참조하십시오.
4. 로그인한 후 게이트웨이를 활성화하고 구성할 수 있습니다.

VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스

VMware ESXi를 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

1. VMware vSphere 클라이언트에서 해당되는 게이트웨이 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인합니다.

Note

게이트웨이 VM이 켜져 있는 경우, 다음 스크린샷과 같이 VM 아이콘과 함께 녹색 화살표 아이콘이 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 녹색을 선택하여 켤 수 있습니다. 전원 켜기의 아이콘 도구 모음 메뉴.

3. 콘솔 탭을 선택합니다.

잠시 후 VM은 로그인할 준비가 됩니다.

Note

콘솔 창에서 커서를 릴리스하려면 Ctrl+Alt를 누릅니다.

- 기본 자격 증명을 사용하여 로그인하려면 계속해서 [파일 게이트웨이 로컬 콘솔에 로그인](#) 절차를 수행합니다.

Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

게이트웨이의 로컬 콘솔에 액세스하려면(Microsoft Hyper-V)

- Microsoft Hyper-V Manager의 Virtual Machines(가상 머신) 목록에서 해당 게이트웨이 VM을 선택합니다.
- 게이트웨이가 켜져 있는지 확인합니다.

Note

게이트웨이 VM이 켜져 있으면Running는 다음과 같이 표시됩니다.상태VM의 예: 다음 스크린샷과 같습니다. 게이트웨이 VM이 켜져 있지 않은 경우 다음을 선택하여 켤 수 있습니다.Start의작업창.

- 작업 창에서 연결을 선택합니다.

그러면 Virtual Machine Connection(가상 머신 연결) 창이 표시됩니다. 인증 창이 표시되면 하이퍼바이저 관리자가 제공한 사용자 이름과 암호를 입력합니다.

잠시 후 VM은 로그인할 준비가 됩니다.

- 기본 자격 증명을 사용하여 로그인하려면 계속해서 [파일 게이트웨이 로컬 콘솔에 로그인](#) 절차를 수행합니다.

게이트웨이용 네트워크 어댑터 구성

이 섹션에서는 게이트웨이에 여러 네트워크 어댑터를 구성하는 방법에 대한 정보를 얻을 수 있습니다.

주제

- [VMware ESXi 호스트에서 여러 개의 NIC에 게이트웨이 구성](#)
- [Microsoft Hyper-V 호스트에서 여러 개의 NIC에 게이트웨이 구성](#)

VMware ESXi 호스트에서 여러 개의 NIC에 게이트웨이 구성

다음 절차에서는 게이트웨이 VM에 네트워크 어댑터 한 개가 이미 정의되어 있고 이제 두 번째 어댑터를 추가한다고 가정합니다. 다음은 VMware ESXi에 어댑터를 추가하는 방법에 대한 절차입니다.

VMware ESXi 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이를 종료합니다.
2. VMware vSphere 클라이언트에서 해당되는 게이트웨이 VM을 선택합니다.

이 절차를 위해 VM을 켜 상태로 유지할 수 있습니다.

3. 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.
4. 온Hardware(하드웨어)의 탭가상 머신 속성대화 상자에서 다음을 선택합니다. Add디바이스를 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. 에서네트워크 유형창, 확인전원 켜기 시 Connect에 대해 선택됨유형을 선택한 다음 를 선택합니다.다음.

Storage Gateway 함께 E1000 네트워크 어댑터를 사용하는 것이 좋습니다. 어댑터 목록에 표시될 어댑터 유형에 대한 자세한 내용은 [ESXi 및 vCenter Server 설명서](#)의 '네트워크 어댑터 유형' 단원을 참조하십시오.

- c. Ready to Complete(완료 준비) 창에서 해당 정보를 검토한 후 Finish(완료)를 선택합니다.

- 를 선택합니다. 요약 VM의 탭을 선택하고 모두 보기 다음 IP 주소 상자. 게이트웨이에 액세스할 때 사용할 수 있는 모든 IP 주소가 Virtual Machine IP Addresses(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.

다음 이미지는 단지 설명을 위한 것입니다. 실제로는 IP 주소 중 하나는 게이트웨이가 AWS와 통신하는 주소가 되고 다른 하나는 다른 서브넷에 있는 주소가 됩니다.

- Storage Gateway 콘솔에서 게이트웨이를 엽니다.
- 에서 탐색 Storage Gateway 콘솔의 창에서 게이트웨이어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 [VM 로컬 콘솔 \(파일 게이트웨이\)에서 작업 수행](#) 단원을 참조하십시오.

Microsoft Hyper-V 호스트에서 여러 개의 NIC에 게이트웨이 구성

다음 절차에서는 게이트웨이 VM에 네트워크 어댑터 한 개가 이미 정의되어 있고 이제 두 번째 어댑터를 추가한다고 가정합니다. 이번 절차에서는 Microsoft Hyper-V 호스트에 어댑터를 추가하는 방법에 대해서 살펴보겠습니다.

Microsoft Hyper-V 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

- Storage Gateway 콘솔에서 게이트웨이를 끕니다.
- Microsoft Hyper-V Manager에서 게이트웨이 VM을 선택합니다.
- VM이 이미 꺼져 있는 경우, 게이트웨이를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Turn Off(끄기)를 선택합니다.
- 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. 예시설정대화 상자Hardware(하드웨어)두 번째 어댑터가 추가되었는지 확인한 다음확인.
9. Storage Gateway 콘솔에서 게이트웨이를 엽니다.
10. Navigation(탐색) 창에서 게이트웨이를 선택한 후 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 [VM 로컬 콘솔 \(파일 게이트웨이\)에서 작업 수행](#) 단원을 참조하십시오.

AWS Storage Gateway 콘솔을 사용한 게이트웨이 삭제와 연결된 리소스 제거

게이트웨이를 계속 사용할 계획이 아니라면 게이트웨이와 이에 연결된 리소스를 삭제하는 것이 좋습니다. 리소스를 제거하면 계속해서 사용할 계획이 없는 리소스에 요금이 부과되지 않게 할 수 있고 월별 청구액을 줄이는 데 도움이 됩니다.

게이트웨이를 삭제하면 AWS Storage Gateway Management Console에 표시되지 않고 초기자에 대한 iSCSI 연결이 종료됩니다. 게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 별도 지침 대로 연결된 리소스를 제거해야 합니다.

Storage Gateway 콘솔이나 프로그래밍 방식으로 게이트웨이를 삭제할 수 있습니다. Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하는 방법에 대한 정보를 얻을 수 있습니다. 프로그래밍 방식으로 게이트웨이를 삭제하려면 [.를 참조하십시오.AWS Storage GatewayAPI 참조](#).

주제

- [Storage Gateway 콘솔을 사용한 게이트웨이 삭제](#)
- [온프레미스에 배포한 게이트웨이에서 리소스 제거](#)
- [Amazon EC2 인스턴스에 배포한 게이트웨이에서 리소스 제거](#)

Storage Gateway 콘솔을 사용한 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 배포한 게이트웨이의 경우, 해당 인스턴스는 삭제하지 않는 한 계속 존재합니다.

가상 머신(VM)에 배포한 게이트웨이의 경우, 게이트웨이를 삭제한 후에도 게이트웨이 VM은 여전히 가상화 환경에 존재합니다. VM을 제거하려면 VMware vSphere 클라이언트, Microsoft Hyper-V Manager 또는 Linux 커널 기반 가상 머신(KVM) 클라이언트를 사용하여 호스트에 연결하고 VM을 제거합니다. 삭제한 게이트웨이의 VM을 다시 사용하여 새 게이트웨이를 활성화할 수는 없다는 점에 유의하십시오.

게이트웨이를 삭제하려면

1. 에서 Storage Gateway 콘솔 열기 <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 게이트웨이를 선택한 후 삭제할 게이트웨이를 선택합니다.
3. 작업에서 게이트웨이 삭제를 선택합니다.
- 4.

Warning

이 단계를 수행하기 전에 게이트웨이의 볼륨에 현재 쓰기 작업을 하는 애플리케이션이 없는지 확인합니다. 게이트웨이를 사용하는 중에 삭제하면 데이터 손실이 발생할 수 있습니다.

또한 게이트웨이를 삭제하면 복구할 수 없습니다.

표시된 확인 대화 상자에서 확인란을 선택하여 삭제를 확인합니다. 열거된 게이트웨이 ID가 삭제하려는 게이트웨이를 명시하는지 확인한 후 삭제를 선택하십시오.

Important

게이트웨이를 삭제한 후에는 소프트웨어 요금을 지불하지 않지만, 가상 테이프, Amazon EBS (Amazon EBS) 스냅샷 및 Amazon EC2 인스턴스와 같은 리소스는 계속 유지됩니다. 이러한 리소스에 대해서는 계속 비용이 청구됩니다. Amazon EC2 구독을 취소하여 Amazon EC2 인스턴스 및 Amazon EBS 스냅샷을 제거하도록 선택할 수 있습니다. Amazon EC2 구독을 유지하려면 Amazon EC2 콘솔을 사용하여 Amazon EBS 스냅샷을 삭제할 수 있습니다.

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.

Amazon EC2 인스턴스에 배포한 게이트웨이에서 리소스 제거

Amazon EC2 인스턴스에 배포한 게이트웨이를 삭제하려면 AWS 게이트웨이와 함께 사용된 리소스, 이렇게 하면 원하지 않는 사용 요금이 청구되는 것을 방지할 수 있습니다.

Amazon EC2 배포한 캐시 볼륨에서 리소스 제거

EC2에서 캐싱 볼륨으로 게이트웨이를 배포한 경우, 다음 작업을 수행하여 게이트웨이를 삭제하고 관련 리소스를 정리하는 것이 좋습니다.

1. Storage Gateway 콘솔에서 단원의 설명 대로 게이트웨이를 삭제하십시오. [Storage Gateway 콘솔을 사용한 게이트웨이 삭제](#).

2. 인스턴스를 다시 사용할 계획인 경우 Amazon EC2 콘솔에서 해당 EC2 인스턴스를 중지합니다. 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 없다면 Amazon EC2 콘솔에서 인스턴스에 연결된 모든 Amazon EBS 볼륨을 제거하십시오. 자세한 내용은 단원을 참조하십시오. [인스턴스 및 볼륨 정리](#)의 Linux 인스턴스용 Amazon EC2 사용 설명서.

성능

이 섹션에서는 Storage Gateway 성능에 대한 정보를 얻을 수 있습니다.

주제

- [게이트웨이 성능 최적화](#)
- [Storage Gateway VMware vSphere 고가용성 사용](#)

게이트웨이 성능 최적화

아래에서 게이트웨이의 성능을 최적화하는 자세한 방법을 확인할 수 있습니다. 이 지침은 게이트웨이에 리소스를 추가하고 애플리케이션 서버에 리소스를 추가하는 것을 기반으로 합니다.

게이트웨이에 리소스 추가

다음 방법 중 하나 이상을 사용하여 게이트웨이에 리소스를 추가하여 게이트웨이 성능을 최적화할 수 있습니다.

고성능 디스크 사용

게이트웨이 성능을 최적화하기 위해 SSD (솔리드 스테이트 드라이브) 및 NVMe 컨트롤러와 같은 고성능 디스크를 추가할 수 있습니다. Microsoft Hyper-V NTFS 대신 SAN (저장소 영역 네트워크)에서 직접 가상 디스크를 VM에 연결할 수도 있습니다. 디스크 성능이 향상되면 일반적으로 처리량이 향상되고 IOPS (초당 입력/출력 작업 수)가 증가합니다. 디스크 추가에 대한 자세한 내용은 단원을 참조하십시오. [캐시 스토리지 추가](#).

처리량을 측정하려면 ReadBytes과 WriteBytes를 포함한 지표 Samples Amazon CloudWatch 통계. 예: Samples의 통계입니다. ReadBytes 5분 동안의 샘플 시간에 걸친 지표를 300초로 나누면 IOPS가 됩니다. 일반적으로 게이트웨이에 대한 이러한 메트릭을 검토할 때는 낮은 처리량과 낮은 IOPS 추세를 찾아 디스크 관련 병목 현상을 나타냅니다.

Note

CloudWatch 지표를 일부 게이트웨이에 사용할 수 있는 것은 아닙니다. 게이트웨이 지표에 대한 자세한 내용은 단원을 참조하십시오. [파일 게이트웨이 모니터링](#).

게이트웨이 호스트에 CPU 리소스 추가

게이트웨이 호스트 서버의 최소 요구 사항은 4개의 가상 프로세서입니다. 게이트웨이 성능을 최적화하려면 게이트웨이 VM에 할당된 4개의 가상 프로세서가 4개의 코어로 지원되는지 확인합니다. 또한 호스트 서버의 CPU를 과다 구독하고 있지 않은지 확인합니다.

게이트웨이 호스트 서버에 CPU를 추가하면 게이트웨이의 처리 기능이 향상됩니다. 이렇게 하면 게이트웨이가 애플리케이션의 데이터를 로컬 스토리지로 저장하고 이 데이터를 Amazon S3 업로드할 수 있습니다. 또한 추가 CPU는 호스트가 다른 VM과 공유될 때 게이트웨이가 충분한 CPU 리소스를 확보할 수 있도록 도와줍니다. 충분한 CPU 리소스를 제공하면 처리량이 향상되는 일반적인 효과가 있습니다.

Storage Gateway 호스트 서버에서 24개의 CPU 사용을 지원합니다. 24개의 CPU를 사용하여 게이트웨이의 성능을 크게 향상시킬 수 있습니다. 게이트웨이 호스트 서버에 대해 다음 게이트웨이 구성을 권장합니다.

- 24CPU.
- 파일 게이트웨이용 16GiB 예약 RAM
 - 캐시 크기가 최대 16TiB인 게이트웨이를 위한 16GiB 예약 RAM
 - 캐시 크기가 16TiB에서 32TiB인 게이트웨이를 위한 32GiB의 예약된 RAM
 - 캐시 크기가 32TiB에서 64TiB인 게이트웨이를 위한 48GiB의 예약된 RAM
- 반가상화 컨트롤러 1에 연결된 디스크 1은 다음과 같이 게이트웨이 캐시로 사용됩니다.
 - NVMe 컨트롤러를 사용하는 SSD.
- 반가상화 컨트롤러 1에 연결된 디스크 2는 다음과 같이 게이트웨이 업로드 버퍼로 사용됩니다.
 - NVMe 컨트롤러를 사용하는 SSD
- 반가상화 컨트롤러 2에 연결된 디스크 3은 다음과 같이 게이트웨이 업로드 버퍼로 사용됩니다.
 - NVMe 컨트롤러를 사용하는 SSD.
- VM 네트워크 1에 구성된 네트워크 어댑터 1:
 - VM 네트워크 1을 사용하고 수집에 사용할 VMXNet3 (10Gbps) 을 추가합니다.
- VM 네트워크 2에 구성된 네트워크 어댑터 2:
 - VM 네트워크 2를 사용하고 연결에 사용할 VMXNet3 (10Gbps) 을 추가합니다.AWS.

별도의 물리적 디스크가 있는 백 게이트웨이 가상 디스크

게이트웨이 디스크를 프로비저닝할 때 동일한 기본 물리 스토리지 디스크를 사용하는 로컬 스토리지에 프로비저닝하지 말 것을 적극 권장합니다. 예를 들어 VMware ESXi의 경우 기본 물리 스토리지 리소스가 데이터 스토어로 표시됩니다. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이

터 스토어를 선택합니다. 가상 디스크를 프로비저닝하는 경우 (예: 업로드 버퍼 용도), 가상 디스크를 동일한 데이터 스토어에 VM으로 저장하거나 다른 데이터 스토어에 저장할 수 있습니다.

데이터 스토어가 한 개 이상인 경우에는 만드는 로컬 스토리지 유형마다 데이터 스토어 한 개씩 선택하는 것이 좋습니다. 기본 물리 디스크 한 개만 지원하는 데이터 스토어는 성능이 떨어질 수 있습니다. 예를 들어 이러한 디스크를 사용하여 게이트웨이 설정에서 캐시 스토리지와 업로드 버퍼를 모두 백업하는 경우를 들 수 있습니다. 마찬가지로 RAID 1과 같이 성능이 낮은 RAID 구성으로 뒷받침되는 데이터 저장소는 성능이 저하될 수 있습니다.

애플리케이션 환경에 리소스 추가

애플리케이션 서버와 게이트웨이 간 대역폭 증가

게이트웨이 성능을 최적화하려면 애플리케이션과 게이트웨이 간의 네트워크 대역폭이 애플리케이션 요구를 유지할 수 있는지 확인하십시오. 이 ReadBytes과 WriteBytes 전체 데이터 처리량을 측정하기 위한 게이트웨이의 메트릭입니다.

애플리케이션의 경우 측정된 처리량을 원하는 처리량과 비교합니다. 측정된 처리량이 원하는 처리량보다 작은 경우 네트워크가 병목 현상일 경우 애플리케이션과 게이트웨이 간의 대역폭을 늘리면 성능이 향상될 수 있습니다. 마찬가지로 VM과 로컬 디스크가 직접 연결되지 않은 경우 VM과 로컬 디스크 간의 대역폭을 늘릴 수 있습니다.

애플리케이션 환경에 CPU 리소스 추가

애플리케이션에서 추가 CPU 리소스를 사용할 수 있는 경우 CPU를 더 추가하면 애플리케이션이 I/O 로드를 확장하는 데 도움이 될 수 있습니다.

Storage Gateway VMware vSphere 고가용성 사용

Storage Gateway VMware vSphere HA (VMware vSphere 고가용성) 와 통합된 애플리케이션 수준의 상태 확인 세트를 통해 VMware에서 고가용성을 제공합니다. 이러한 접근 방식을 통해 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 또한 연결 시간 초과, 파일 공유 또는 볼륨 사용 불가와 같은 소프트웨어 오류로부터 보호할 수 있습니다.

이러한 통합을 통해 온프레미스 VMware 환경 또는 VMware Cloud on AWS에 배포된 게이트웨이는 대부분의 서비스 중단으로부터 자동으로 복구됩니다. 일반적으로 데이터 손실 없이 60초 이내에 이 작업을 수행합니다.

Storage Gateway와 함께 VMware HA를 사용하려면 다음 단계를 수행하십시오.

주제

- [vSphere VMware HA 클러스터 구성](#)
- [게이트웨이 유형에 대한 .ova 이미지 다운로드](#)
- [게이트웨이 배포](#)
- [\(선택 사항\) 클러스터의 다른 VM에 대한 재정의 옵션 추가](#)
- [게이트웨이 활성화](#)
- [VMware 고가용성 구성 테스트](#)

vSphere VMware HA 클러스터 구성

먼저 아직 VMware 클러스터를 생성하지 않은 경우 클러스터를 생성합니다. VMware 클러스터를 생성하는 방법에 대한 자세한 내용은 VMware 설명서의 [vSphere HA 클러스터 생성](#)을 참조하십시오.

그런 다음 VMware 클러스터가 Storage Gateway 함께 작동하도록 구성합니다.

VMware 클러스터를 구성하려면

1. VMware vSphere의 Edit Cluster Settings(클러스터 설정 편집) 페이지에서 VM 모니터링이 VM 및 애플리케이션 모니터링용으로 구성되어 있는지 확인합니다. 이렇게 하려면 다음 옵션을 나열된 대로 설정합니다.
 - 호스트 오류 응답: VM 재시작
 - 호스트 격리에 대한 응답: VM 종료 및 다시 시작
 - PDL (PDL 포함 데이터 스토어): 비활성
 - APD (APD 포함 데이터 스토어): 비활성
 - VM 모니터링: VM 및 애플리케이션 모니터링

예를 들어, 다음 스크린샷을 참조하십시오.

2. 다음 값을 조정하여 클러스터의 민감도를 미세 조정합니다.
 - 고장 간격— VM 하트비트가 수신되지 않은 경우 이 간격 후 VM을 다시 시작합니다.
 - 최소 가동 시간— VM이 VM 도구의 하트비트에 대한 모니터링을 시작한 후 클러스터가 이 시간 동안 기다립니다.

- 최대 VM당 재설정— 클러스터가 최대 재설정 시간 내에서 VM을 이 최대 횟수만큼 다시 시작합니다.
- 최대 재설정 시간— VM 재설정당 최대 재설정 수를 구할 시간입니다.

설정할 값을 잘 모르는 경우 다음 설정 예를 사용합니다.

- Failure interval(실패 간격): **30초**
- Minimum uptime(최소 가동 시간): **120초**
- Maximum per-VM resets(VM당 최대 재설정): **3**
- Maximum resets time window(최대 재설정 시간): **1시간**

클러스터에서 다른 VM이 실행 중인 경우 이러한 값을 해당 VM에 맞게 설정할 수 있습니다. .ova에서 VM을 배포할 때까지는 이 작업을 수행할 수 없습니다. 이러한 값 설정에 대한 자세한 내용은 [\(선택 사항\) 클러스터의 다른 VM에 대한 재정의 옵션 추가](#) 단원을 참조하십시오.

게이트웨이 유형에 대한 .ova 이미지 다운로드

다음 절차에 따라 .ova 이미지를 다운로드합니다.

게이트웨이 유형에 대한 .ova 이미지를 다운로드하려면

- 다음 중 하나에서 해당 게이트웨이 유형에 대한 .ova 이미지를 다운로드합니다.
 - 파일 게이트웨이 —

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.

(선택 사항) 클러스터의 다른 VM에 대한 재정의의 옵션 추가

클러스터에서 다른 VM이 실행 중인 경우 각 VM에 맞게 클러스터 값을 설정할 수 있습니다.

클러스터의 다른 VM에 대한 재정의의 옵션을 추가하려면

1. VMware vSphere의 요약 페이지에서 클러스터를 선택하여 클러스터 페이지를 연 다음 구성을 선택합니다.
2. 구성 탭을 선택한 다음 VM Overrides(VM 재정의)를 선택합니다.
3. 새 VM 재정의의 옵션을 추가하여 각 값을 변경합니다.

재정의의 옵션은 다음 스크린샷을 참조하십시오.

게이트웨이 활성화

게이트웨이에 대한 .ova를 배포한 후 게이트웨이를 활성화합니다. 각 게이트웨이 유형마다 서로 다른 방법에 대한 지침입니다.

게이트웨이를 활성화하려면

- 게이트웨이 유형에 따라 활성화 지침을 선택합니다.
 - 파일 게이트웨이 —

VMware 고가용성 구성 테스트

게이트웨이를 활성화한 후 구성을 테스트합니다.

VMware HA 구성을 테스트하려면

1. 에서 Storage Gateway 콘솔을 엽니다. <https://console.aws.amazon.com/storagegateway/home>.
2. 탐색 창에서 게이트웨이를 선택한 다음 VMware HA에 대해 테스트할 게이트웨이를 선택합니다.
3. 작업에서 Verify VMware HA(VMware HA 확인)를 선택합니다.
4. Verify VMware High Availability Configuration(VMware 고가용성 구성 확인) 상자가 나타나면 확인을 선택합니다.

 Note

VMware HA 구성을 테스트하면 게이트웨이 VM이 재부팅되고 게이트웨이 연결이 중단됩니다. 테스트를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

테스트가 성공하면 콘솔에 있는 게이트웨이의 세부 정보 탭에 확인됨 상태가 나타납니다.

5. 종료를 선택합니다.

Amazon CloudWatch 로그 그룹에서 VMware HA 이벤트에 대한 정보를 찾을 수 있습니다. 자세한 내용은 [CloudWatch 로그 그룹을 사용하여 파일 게이트웨이 상태 로그 가져오기](#) 단원을 참조하세요.

의 보안AWSStorage Gateway

AWS에서 클라우드 보안을 가장 중요하게 생각합니다. AWS 고객은 보안에 매우 민감한 조직의 요구 사항에 부합하도록 구축된 데이터 센터 및 네트워크 아키텍처의 혜택을 누릴 수 있습니다.

보안은 AWS와 귀하의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드 내 보안 및 클라우드의 보안으로 설명합니다.

- 클라우드의 보안 - AWS는 AWS 클라우드에서 AWS 서비스를 실행하는 인프라를 보호합니다. AWS는 또한 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 [AWS 규정 준수 프로그램](#)의 일환으로 보안 효과를 정기적으로 테스트하고 검증합니다. 에 적용되는 규정 준수 프로그램에 대해 알아보려면 [AWSStorage GatewayAWS규정 준수 프로그램 제공 범위 내 서비스](#).
- 클라우드 내 보안 - 귀하의 책임은 귀하가 사용하는 AWS 서비스에 의해 결정됩니다. 또한 귀하는 데이터의 민감도, 회사 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 항목에서는 보안 및 규정 준수 목적에 맞게 Storage Gateway를 구성하는 방법을 보여줍니다. 또한 기타 사용 방법을 배웁니다. AWSStorage Gateway 리소스를 모니터링하고 보호하는 데 도움이 되는 서비스입니다.

주제

- [의 데이터 보호AWSStorage Gateway](#)
- [Storage Gateway 인증 및 액세스 제어](#)
- [AWS Storage Gateway의 로깅 및 모니터링](#)
- [의 규정 준수 확인AWSStorage Gateway](#)
- [의 복원성AWSStorage Gateway](#)
- [의 인프라 보안AWSStorage Gateway](#)
- [Storage Gateway 보안 모범 사례](#)

의 데이터 보호AWSStorage Gateway

이 [AWS 공동 책임 모델](#)의 데이터 보호에 적용AWSStorage Gateway. 이 모델에서 설명하는 것처럼 AWS는 모든 AWS 클라우드를 실행하는 글로벌 인프라를 보호할 책임이 있습니다. 이 인프라에서 호스팅되는 콘텐츠에 대한 제어를 유지하는 것은 사용자의 책임입니다. 이 콘텐츠에는 사용하는 AWS

서비스에 대한 보안 구성 및 관리 작업이 포함됩니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 FAQ](#)를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그에서 [AWS 공동 책임 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터를 보호하려면 AWS 계정 자격 증명을 보호하고 AWS Identity and Access Management(IAM)를 사용하여 개별 사용자 계정을 설정하는 것이 좋습니다. 이러한 방식에서는 각 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정마다 멀티 팩터 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2 이상을 권장합니다.
- AWS CloudTrail으로 API 및 사용자 활동 로깅을 설정합니다.
- AWS 암호화 솔루션을 AWS 서비스 내의 모든 보안 컨트롤 기본값과 함께 사용합니다.
- Amazon S3에 저장된 개인 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용합니다.
- 명령줄 인터페이스 또는 API를 통해 AWS에 액세스할 때 FIPS 140-2 검증된 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [Federal Information Processing Standard\(FIPS\) 140-2](#)를 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름(Name) 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 Storage Gateway나 다른 용도로 작업하는 경우가 포함됩니다. AWS 콘솔을 사용하는 서비스, API, AWS CLI 또는 AWSSDK. 이름에 사용되는 태그 또는 자유 형식 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함해서는 안 됩니다.

를 사용하여 데이터 암호화 AWS KMS

SSL/TLS (Secure Socket Layers/Transport Layer Security) 를 사용하여 Storage Gateway 어플라이언스와 함께 전송되는 데이터를 암호화합니다. 기본적으로 Storage Gateway Amazon S3가 관리하는 암호화 키 (SSE-S3) 를 사용하여 Amazon S3 저장되는 모든 데이터를 서버 측 암호화합니다. Storage Gateway API를 사용하여 클라우드에 저장된 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다. AWS Key Management Service(SSE-KMS) 고객 마스터 키 (CMK) 입니다.

⚠ Important

를 사용할 때 AWS KMS 서버 측 암호화에 CMK를 사용하려면 대칭 CMK를 선택해야 합니다. 비대칭 CMK를 지원하지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 [대칭 및 비대칭 키 사용](#)을 참조하세요.

파일 공유 암호화

파일 공유의 경우 다음을 사용하여 객체를 암호화하도록 게이트웨이를 구성할 수 있습니다. AWS KMS — SSE-KMS를 사용하여 관리되는 키 Storage Gateway API를 사용하여 파일 공유에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 단원을 참조하십시오. [Create NFS File Share](#)의 AWS Storage Gateway API 참조.

파일 시스템 암호화

자세한 내용은 단원을 참조하십시오. [아마존 FSx의 데이터 암호화](#)의 Amazon FSx for Windows File Server 사용 설명서.

AWS KMS를 사용하여 데이터를 암호화할 경우 다음 사항에 유의하십시오.

- 데이터는 클라우드에 암호화되어 저장됩니다. 즉, 데이터는 Amazon S3에서 암호화됩니다.
- IAM 사용자는 에 호출하는 데 필요한 권한이 있어야 합니다. AWS KMS API 작업 자세한 내용은 단원을 참조하십시오. [의 IAM 정책 사용 AWS KMS](#)의 AWS Key Management Service 개발자 안내서.
- CMK를 삭제 또는 비활성화하거나 권한 부여 토큰을 취소하면, 볼륨 또는 테이프의 데이터에 액세스할 수 없습니다. 자세한 내용은 단원을 참조하십시오. [고객 마스터 키 삭제](#)의 AWS Key Management Service 개발자 안내서.
- KMS로 암호화된 볼륨에서 스냅샷을 생성하면 스냅샷이 암호화됩니다. 이때 스냅샷은 볼륨의 KMS 키를 상속합니다.
- KMS로 암호화된 스냅샷에서 새로운 볼륨을 생성하면 볼륨이 암호화됩니다. 이때 새로운 볼륨에 다른 KMS 키를 지정할 수 있습니다.

ℹ Note

Storage Gateway는 KMS로 암호화된 스냅샷이나 KMS로 암호화된 스냅샷의 복구 지점에서 암호화되지 않은 볼륨을 생성하는 것을 지원하지 않습니다.

AWS KMS에 대한 자세한 내용은 [AWS Key Management Service란 무엇입니까?](#)를 참조하십시오.

Storage Gateway 인증 및 액세스 제어

AWS Storage Gateway에 액세스하려면 AWS가 요청을 인증하는 데 사용할 수 있는 자격 증명이 필요합니다. 이러한 자격 증명에는 액세스 권한이 있어야 합니다. AWS 리소스 (예: 게이트웨이, 파일 공유, 테이프) 다음 단원에서는 사용 방법에 대한 세부 정보를 제공합니다. [AWS Identity and Access Management\(IAM\)](#) 및 Storage Gateway는 리소스에 액세스할 수 있는 대상을 제어하여 리소스를 보호하는 데 도움이 되는

- [인증](#)
- [액세스 제어](#)

인증

다음과 같은 유형의 자격 증명으로 AWS에 액세스할 수 있습니다.

- AWS 계정 루트 사용자 – AWS 계정을(를) 처음 생성하는 경우에는 계정의 전체 AWS 서비스 및 계정 리소스에 대해 완전한 액세스 권한을 지닌 단일 로그인 자격 증명으로 시작합니다. 이 자격 증명은 AWS 계정 루트 사용자라고 하며, 계정을 생성할 때 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업, 심지어 관리 작업의 경우에도 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 대신, [IAM 사용자를 처음 생성할 때만 루트 사용자를 사용하는 모범 사례](#)를 준수하세요. 그런 다음 루트 사용자 자격 증명을 안전하게 보관하고 몇 가지 계정 및 서비스 관리 태스크를 수행할 때만 사용합니다.
- IAM 사용자— An [IAM 사용자](#) 귀하의 신분입니다. AWS 계정 특정 사용자 지정 권한 (예: Storage Gateway에서 게이트웨이를 생성할 권한) 이 있는 경우 IAM 사용자 이름과 암호를 사용하여 [AWS Management Console](#), [AWS 토론 포럼](#) 또는 [AWS Support](#) 센터같은 보안 웹 페이지에 로그인할 수 있습니다.

사용자 이름과 암호 외에도 각 사용자에 대해 [액세스 키](#)를 생성할 수 있습니다. [여러 SDK 중 하나](#)를 통해 또는 [AWS Command Line Interface\(CLI\)](#)를 사용하여 AWS 서비스에 프로그래밍 방식으로 액세스할 때 이러한 키를 사용할 수 있습니다. SDK 및 CLI 도구는 액세스 키를 사용하여 암호화 방식으로 요청에 서명합니다. AWS 도구를 사용하지 않는 경우 요청에 직접 서명해야 합니다. Storage Gateway 지원서명 버전 4는 인바운드 API 요청을 인증하기 위한 프로토콜입니다. 요청 인증에 대한 자세한 정보는 AWS 일반 참조의 [서명 버전 4 서명 프로세스](#)를 참조하세요.

- IAM 역할 – [IAM 역할](#)은 계정에 만들 수 있는, 특정 권한을 지닌 IAM 자격 증명입니다. AWS에서 자격 증명이 할 수 있는 것과 없는 것을 결정하는 권한 정책을 갖춘 AWS 자격 증명이라는 점에서 IAM 역할은 IAM 사용자와 유사합니다. 그러나 역할은 한 사람과만 연관되지 않고 해당 역할이 필요한 사람이라면 누구든지 맡을 수 있어야 합니다. 또한 역할에는 그와 연관된 암호 또는 액세스 키와 같은 표준 장기 자격 증명도 없습니다. 대신에 역할을 맡은 사람에게는 해당 역할 세션을 위한 임시 보안 자격 증명도 제공됩니다. 임시 자격 증명도 있는 IAM 역할은 다음과 같은 상황에서 유용합니다.
- 연합된 사용자 액세스 – IAM 사용자를 생성하는 대신 AWS Directory Service의 기존 자격 증명, 엔터프라이즈 사용자 디렉터리 또는 웹 자격 증명 공급자를 사용할 수 있습니다. 이 사용자를 페더레이션 사용자라고 합니다. AWS에서는 [자격 증명 공급자](#)를 통해 액세스가 요청되면 페더레이션 사용자에게 역할을 할당합니다. 연합된 사용자에 대한 자세한 정보는 IAM 사용 설명서의 [연합된 사용자 및 역할](#)을 참조하세요.
- AWS 서비스 액세스 – 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 맡는 [IAM 역할](#)입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [AWS 서비스에 대한 권한을 위임할 역할 생성](#)을 참조하세요.
- Amazon EC2에서 실행 중인 애플리케이션 – IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 자격 증명을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장할 때 권장되는 방법입니다. EC2 인스턴스에 AWS 역할을 할당하고 해당 역할을 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행되는 프로그램이 임시 자격 증명을 얻을 수 있습니다. 자세한 정보는 IAM 사용 설명서의 [IAM 역할을 사용하여 Amazon EC2 인스턴스에서 실행되는 애플리케이션에 권한 부여](#)를 참조하세요.

액세스 제어

요청을 인증하는 데 유효한 자격 증명도 있더라도 권한이 없다면 Storage Gateway 리소스를 생성하거나 액세스할 수 없습니다. 예를 들어 Storage Gateway에서 게이트웨이를 생성할 권한이 있어야 합니다.

다음 단원에서는 Storage Gateway의 권한을 관리하는 방법을 설명합니다. 먼저 개요를 읽어 보면 도움이 됩니다.

- [Storage Gateway에 대한 액세스 권한 관리 개요](#)
- [자격 증명 기반 정책\(IAM 정책\)](#)

Storage Gateway에 대한 액세스 권한 관리 개요

ERYAWS리소스는 Amazon Web Services 계정의 소유이고, 리소스 생성 또는 리소스 액세스 권한은 권한 정책에 따라 결정됩니다. 계정 관리자는 IAM 자격 증명(즉, 사용자, 그룹, 역할)에 권한 정책을 연결할 수 있고, 일부 서비스(예: AWS Lambda)에서는 리소스에 대한 권한 정책 연결도 지원합니다.

Note

계정 관리자 또는 관리자 사용자는 관리자 권한이 있는 사용자입니다. 자세한 내용은 IAM 사용 설명서의 [IAM 모범 사례](#) 단원을 참조하세요.

권한을 부여하려면 권한을 부여 받을 사용자, 권한 대상이 되는 리소스, 해당 리소스에 허용되는 특정 작업을 결정합니다.

주제

- [Storage Gateway 리소스](#)
- [리소스 소유권 이해](#)
- [리소스 액세스 관리](#)
- [정책 요소 지정: 작업, 효과, 리소스 및 보안 주체](#)
- [정책에서 조건 지정](#)

Storage Gateway 리소스

Storage Gateway의 기본 리소스는 게이트웨이. 또한 Storage Gateway는 파일 공유, 볼륨, 가상 테이프 라이브러리 (VTL) 디바이스 등과 같은 추가 리소스 유형을 지원합니다. 이 유형들은 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

다음 표에 나와 있는 것처럼 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

리소스 유형	ARN 형식
Gateway ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i>

리소스 유형	ARN 형식
파일 시스템 ARN	<code>arn:aws:fsx: <i>region</i>:<i>account-id</i> :file-system/ <i>filesystem-id</i></code>

Note

Storage Gateway 리소스 ID는 대문자입니다. 이러한 리소스 ID를 Amazon EC2 API에서 사용하는 경우, Amazon EC2 리소스 ID가 소문자일 것으로 기대합니다. EC2 API에서 사용할 수 있도록 리소스 ID를 소문자로 변경해야 합니다. 예를 들어 Storage Gateway에서 볼륨의 ID는 `vol-1122AABB`일 수 있습니다. 이 ID를 EC2 API에서 사용하는 경우, `vol-1122aabb`로 변경해야 합니다. 그렇게 하지 않으면 EC2 API가 예상 대로 작동하지 않을 수 있습니다. 2015년 9월 2일 이전에 활성화한 게이트웨이의 ARN은 게이트웨이 ID 대신에 게이트웨이 이름을 포함합니다. 게이트웨이의 ARN을 얻으려면 `DescribeGatewayInformation` API 작업을 사용하십시오.

테이프 생성과 같은 특정 API 작업에 대한 권한을 부여하기 위해 Storage Gateway는 이 리소스 및 하위 리소스를 생성하고 관리할 수 있는 일련의 API 작업을 제공합니다. API 작업 목록은 단원을 참조하십시오. [작업](#)의 AWS Storage Gateway API 참조.

테이프 생성과 같은 특정 API 작업에 대한 권한을 부여하기 위해 Storage Gateway는 권한 정책에서 지정할 수 있는 일련의 작업을 정의하여 특정 API 작업에 대한 권한을 부여합니다. API 작업에는 둘 이상의 작업에 대한 권한이 필요할 수 있습니다. 모든 Storage Gateway API 작업과 해당 작업이 적용되는 리소스를 보여주는 표는 단원을 참조하십시오. [Storage Gateway API 권한: 작업, 리소스 및 조건 참조](#).

리소스 소유권 이해

A 리소스 소유자는 리소스를 생성한 Amazon Web Services 계정입니다. 즉, 리소스 소유자는 보안 주체(루트 계정, IAM 사용자 또는 IAM 역할)는 리소스를 생성하는 요청을 인증합니다. 다음 예에서는 이 계정의 작동 방식을 설명합니다.

- Amazon Web Services 계정의 루트 계정 자격 증명을 사용하여 게이트웨이를 활성화하면 그 Amazon Web Services 계정이 해당 리소스의 소유자가 됩니다 (Storage Gateway 게이트웨이에서는 리소스는 게이트웨이임).

- Amazon Web Services 계정에서 IAM 사용자를 생성하고 에 대한 권한을 부여하는 경우 ActivateGateway이 사용자에게 작업을 수행하면 이 사용자가 게이트웨이를 활성화할 수 있습니다. 하지만 이 사용자가 속한 Amazon Web Services 계정이 게이트웨이 리소스를 소유합니다.
- Amazon Web Services 계정에서 게이트웨이를 활성화할 권한이 있는 IAM 역할을 생성하는 경우, 해당 역할을 담당할 수 있는 사람은 누구나 게이트웨이를 활성화할 수 있습니다. 이 경우 역할이 속한 Amazon Web Services Services의 계정이 게이트웨이 리소스를 소유합니다.

리소스 액세스 관리

권한 정책은 누가 무엇에 액세스 할 수 있는지를 나타냅니다. 다음 섹션에서는 권한 정책을 만드는 데 사용 가능한 옵션에 대해 설명합니다.

Note

이번 단원에서는 Storage Gateway 게이트웨이의 맥락에서 IAM을 사용하는 방법에 대해 설명합니다. IAM 서비스에 대한 자세한 정보는 다루지 않습니다. IAM 설명서 전체 내용은 단원을 참조하십시오. [IAM이란 무엇입니까?](#)의 IAM 사용 설명서. IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 [AWS IAM 정책 참조](#) 섹션을 참조하세요.

IAM 자격 증명에 연결된 정책을 자격 증명 기반 정책(IAM 정책)이라 하고, 리소스에 연결된 정책을 리소스 기반 정책이라고 합니다. Storage Gateway는 자격 증명 기반 정책 (IAM 정책) 만 지원합니다.

주제

- [자격 증명 기반 정책\(IAM 정책\)](#)
- [리소스 기반 정책](#)

자격 증명 기반 정책(IAM 정책)

정책을 IAM 자격 증명에 연결할 수 있습니다. 예를 들면,

- 계정 내 사용자 또는 그룹에 권한 정책 연결— 계정 관리자는 특정 사용자에게 연결된 권한 정책을 사용하여 해당 사용자에게 게이트웨이, 볼륨, 테이프와 같은 Storage Gateway 리소스 생성 권한을 부여할 수 있습니다.
- 역할에 권한 정책 연결(교차 계정 권한 부여) – 자격 증명 기반 권한 정책을 IAM 역할에 연결하여 교차 계정 권한을 부여할 수 있습니다. 예를 들어 계정 A의 관리자는 다른 Amazon Web Services 계정

(예: 계정 B) 또는 계정에 교차 계정 권한을 부여할 역할을 생성할 수 있습니다. AWS 서비스는 다음과 같습니다.

1. 계정 A 관리자는 IAM 역할을 생성하고 계정 A의 리소스에 대한 권한을 부여하는 역할에 권한 정책을 연결합니다.
2. 계정 A 관리자는 계정 B를 역할을 수입할 보안 주체로 식별하는 역할에 신뢰 정책을 연결합니다.
3. 계정 B 관리자는 계정 B의 사용자에게 역할을 수입할 권한을 위임할 수 있습니다. 그러면 계정 B의 사용자가 계정 A에서 리소스를 생성하거나 액세스할 수 있습니다. AWS 서비스에 역할 수입 권한을 부여할 경우 신뢰 정책의 보안 주체가 AWS 서비스 보안 주체이기도 합니다.

IAM을 사용하여 권한을 위임하는 방법에 대한 자세한 내용은 IAM User Guide의 [Access Management](#)를 참조하세요.

다음은 모든 리소스의 모든 List* 작업에 대한 권한을 부여하는 정책의 예시입니다. 이 작업은 읽기 전용 작업입니다. 따라서 이 정책은 사용자가 리소스의 상태를 변경하도록 허용하지 않습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowAllListActionsOnAllResources",
      "Effect": "Allow",
      "Action": [
        "storagegateway:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

Storage Gateway에서 자격 증명 기반 정책을 사용하는 방법에 대한 자세한 내용은 단원을 참조하십시오. [Storage Gateway에 자격 증명 기반 정책 \(IAM 정책\) 사용](#). 사용자, 그룹, 역할 및 권한에 대한 자세한 내용은 IAM 사용 설명서의 [자격 증명\(사용자, 그룹 및 역할\)](#)을 참조하세요.

리소스 기반 정책

Amazon S3과 같은 다른 서비스도 리소스 기반 권한 정책을 지원합니다. 예를 들어, 정책을 S3 버킷에 연결하여 해당 버킷에 대한 액세스 권한을 관리할 수 있습니다. Storage Gateway는 리소스 기반 정책을 지원하지 않습니다.

정책 요소 지정: 작업, 효과, 리소스 및 보안 주체

각 Storage Gateway 리소스에 대해 (참조)[Storage Gateway API 권한: 작업, 리소스 및 조건 참조](#))에서는 일련의 API 작업을 정의합니다 (참조).[작업](#)). 이러한 API 작업에 대한 권한을 부여하기 위해 Storage Gateway는 정책에서 지정할 수 있는 작업을 정의합니다. 예를 들어 Storage Gateway Gateway 리소스에 대해서는 다음 작업이 정의됩니다. ActivateGateway, DeleteGateway, 및 DescribeGatewayInformation. API 작업을 수행하려면 둘 이상의 작업에 대한 권한이 필요할 수 있습니다.

다음은 가장 기본적인 정책 요소입니다.

- 리소스 – 정책에서 Amazon 리소스 이름(ARN)을 사용하여 정책을 적용할 리소스를 식별합니다. Storage Gateway 리소스의 경우에는 항상 와일드카드 문자를 사용합니다.(*)의 IAM 정책입니다. 자세한 정보는 [Storage Gateway 리소스](#)을 참조하십시오.
- 작업 – 작업 키워드를 사용하여 허용 또는 거부할 리소스 작업을 식별합니다. 예를 들어, 지정된 값에 따라 Effect, storagegateway:ActivateGateway 권한 - Storage Gateway의 수행 권한을 허용하거나 거부합니다. ActivateGateway 작업.
- 결과 – 사용자가 특정 작업을 요청하는 경우의 결과를 지정합니다. 이는 허용 또는 거부 중에 하나가 될 수 있습니다. 명시적으로 리소스에 대한 액세스 권한을 부여(허용)하지 않는 경우, 액세스는 묵시적으로 거부됩니다. 다른 정책에서 액세스 권한을 부여하는 경우라도 사용자가 해당 리소스에 액세스할 수 없도록 하기 위해 리소스에 대한 권한을 명시적으로 거부할 수도 있습니다.
- 보안 주체 – 자격 증명 기반 정책(IAM 정책)에서 정책이 연결되는 사용자는 암시적인 보안 주체입니다. 리소스 기반 정책의 경우 사용자, 계정, 서비스 또는 권한의 수신자인 기타 개체를 지정합니다(리소스 기반 정책에만 해당). Storage Gateway는 리소스 기반 정책을 지원하지 않습니다.

IAM 정책 구문과 설명에 대한 자세한 내용은 IAM 사용 설명서의 [AWS IAM 정책 참조](#) 섹션을 참조하십시오.

모든 Storage Gateway API 작업을 보여 주는 표는 단원을 참조하십시오. [Storage Gateway API 권한: 작업, 리소스 및 조건 참조](#).

정책에서 조건 지정

권한을 부여할 때 IAM 정책 언어를 사용하여 정책이 적용되는 조건을 지정할 수 있습니다. 예를 들어, 특정 날짜 이후에만 정책을 적용할 수 있습니다. 정책 언어에서의 조건 지정에 관한 자세한 내용은 IAM 사용 설명서의 [조건](#)을 참조하십시오.

조건을 표시하려면 미리 정의된 조건 키를 사용합니다. Storage Gateway에 고유한 조건 키는 없습니다. 하지만 필요에 따라 사용할 수 있는 AWS 차원의 조건 키는 있습니다. AWS 전체 키의 전체 목록은 IAM 사용 설명서의 [사용 가능한 키](#)를 참조하세요.

Storage Gateway에 자격 증명 기반 정책 (IAM 정책) 사용

이 항목에서는 계정 관리자가 IAM 자격 증명(사용자, 그룹, 역할)에 권한 정책을 연결할 수 있는 자격 증명 기반 정책의 예를 제공합니다.

Important

먼저 Storage Gateway 리소스에 대한 액세스 관리를 위해 제공되는 기본 개념과 옵션 설명에 대한 소개 주제 부분을 우선 읽어 보는 것이 좋습니다. 자세한 정보는 [Storage Gateway에 대한 액세스 권한 관리 개요](#)를 참조하십시오.

이 주제의 섹션에서는 다음 내용을 학습합니다.

- [Storage Gateway 콘솔 사용에 필요한 권한](#)
- [AWSStorage Gateway 대한 관리형 정책](#)
- [고객 관리형 정책 예](#)

다음은 권한 정책의 예입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedActionsOnAllGateways",
      "Effect": "Allow",
      "Action": [
        "storagegateway:ActivateGateway",
        "storagegateway:ListGateways"
      ],
      "Resource": "*"
    },
    {
      "Sid": "AllowsSpecifiedEC2ActionsOnAllGateways",
      "Effect": "Allow",
```

```

    "Action": [
      "ec2:DescribeSnapshots",
      "ec2>DeleteSnapshot"
    ],
    "Resource": "*"
  }
]
}

```

정책에는 두 설명문이 있습니다(두 설명문 안의 Action 및 Resource 요소에 주의).

- 첫 번째 문은 두 Storage Gateway 작업에 대한 권한을 부여합니다(storagegateway:ActivateGateway와storagegateway:ListGateways) 게이트웨이 리소스에서

와일드카드 문자 (*) 는 이 문이 어떤 리소스와도 일치할 수 있음을 뜻합니다. 이 경우 이 명령문은 다음을 허용합니다.storagegateway:ActivateGateway와storagegateway:ListGateways모든 게이트웨이에서 작업을 수행합니다. 와일드카드 문자가 게이트웨이를 생성한 후에라야 리소스 ID를 알 수 있으므로 여기서 와일드카드 문자가 사용됩니다. 정책에서 와일드카드 문자(*)를 사용하는 방법에 대한 정보는 [예제 2: 게이트웨이에 대한 읽기 전용 액세스 허용](#) 단원을 참조하십시오.

Note

ARN이 고유하게 식별AWS있습니다. 자세한 내용은 AWS General Reference의 [Amazon Resource Names \(ARNs\) and AWS Service Namespaces](#)를 참조하세요.

특정 작업을 사용할 수 있는 권한을 특정 게이트웨이에만 부여하려면 정책에서 그 작업에 대해 별도의 설명문을 생성하고 그 설명문에 게이트웨이 ID를 지정하십시오.

- 두 번째 설명문은 ec2:DescribeSnapshots 및 ec2>DeleteSnapshot 작업을 사용할 수 있는 권한을 부여합니다. Storage Gateway 게이트웨이에서 생성한 스냅샷은 Amazon EBS (엘라스틱 블록 스토어) 에 저장되고 Amazon EC2 리소스로 관리되므로 이 Amazon 엘라스틱 컴퓨팅 클라우드 (Amazon EC2) 작업을 하려면 권한이 필요하고, 따라서 해당 EC2 작업이 필요합니다. 자세한 내용은 단원을 참조하십시오.[작업](#)의Amazon EC2 API 레퍼런스. 이러한 Amazon EC2 작업은 리소스 수준 권한을 지원하지 않으므로 정책은 와일드카드 문자 (*) 를Resource게이트웨이 ARN을 지정하는 대신 값입니다.

모든 Storage Gateway API 작업과 해당 작업이 적용되는 리소스를 보여주는 표는 단원을 참조하십시오. [Storage Gateway API 권한: 작업, 리소스 및 조건 참조](#).

Storage Gateway 콘솔 사용에 필요한 권한

Storage Gateway 콘솔을 사용하려면 읽기 전용 권한을 부여해야 합니다. 스냅샷을 설명할 계획이라면 다음 권한 정책과 같이 추가 작업에 대한 권한도 부여해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsSpecifiedEC2ActionOnAllGateways",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Resource": "*"
    }
  ]
}
```

이 추가 권한이 필요한 이유는 Storage Gateway 게이트웨이에서 생성한 Amazon EBS 스냅샷이 Amazon EC2 리소스로 관리되기 때문입니다.

Storage Gateway 콘솔을 탐색하는 데 필요한 최소 권한을 설정하려면 단원을 참조하십시오. [예제 2: 게이트웨이에 대한 읽기 전용 액세스 허용](#).

AWSStorage Gateway 대한 관리형 정책

Amazon Web Services Services는 에서 생성하고 관리하는 독립형 IAM 정책을 제공하여 많은 일반 사용 사례를 처리합니다. AWS. 관리형 정책은 사용자가 필요한 권한을 조사할 필요가 없도록 일반 사용 사례에 필요한 권한을 부여합니다. 에 대한 자세한 내용 AWS관리 정책 단원을 참조하십시오. [AWS관리형 정책](#)의 IAM 사용 설명서.

다음과 같습니다. AWS계정의 사용자에게 연결할 수 있는 관리형 정책은 Storage Gateway에 고유합니다.

- AWS스토리지게이트웨이를레독으로 액세스— 에 대한 읽기 전용 액세스 권한을 부여합니다. AWS Storage Gateway있습니다.

- AWS스토리지게이트웨이 풀 액세스—에 대한 전체 액세스 권한을 부여합니다.AWS Storage Gateway있습니다.

Note

IAM 콘솔에 로그인하고 이 콘솔에서 특정 정책을 검색하여 이러한 권한 정책을 검토할 수 있습니다.

고유의 사용자 지정 IAM 정책을 생성하여 AWS Storage Gateway API 작업에 대한 권한을 허용할 수도 있습니다. 해당 권한이 필요한 IAM 사용자 또는 그룹에 이러한 사용자 지정 정책을 연결할 수 있습니다.

고객 관리형 정책 예

이 단원에서는 다양한 Storage Gateway 작업에 대한 권한을 부여하는 사용자 정책의 예를 제공합니다. 이러한 정책은 사용 중인 경우에 유효합니다.AWSSDK 및AWS CLI. 콘솔을 사용하는 경우 [Storage Gateway 콘솔 사용에 필요한 권한](#)의 설명과 같이 콘솔에 특정한 추가 권한을 부여해야 합니다.

Note

모든 예에서는 미국 서부(오리건) 리전(us-west-2)을 사용하며 가상의 계정 ID를 포함합니다.

주제

- [예제 1: 모든 게이트웨이에서 모든 Storage Gateway 작업 허용](#)
- [예제 2: 게이트웨이에 대한 읽기 전용 액세스 허용](#)
- [예제 3: 특정 게이트웨이에 대한 액세스 허용](#)
- [예 4: 사용자가 특정 볼륨에 액세스할 수 있도록 허용](#)
- [예 5: 특정 접두사가 있는 게이트웨이에 대한 모든 작업 허용](#)

예제 1: 모든 게이트웨이에서 모든 Storage Gateway 작업 허용

다음 정책은 사용자가 모든 Storage Gateway 작업을 수행할 수 있도록 허용합니다. 이 정책은 사용자가 Amazon EC2 작업을 수행할 수도 있도록 허용합니다. [DescribeSnapshots](#)과 [DeleteSnapshot](#) Storage Gateway 게이트웨이에서 생성된 Amazon EBS 스냅샷입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowsAllAWSStorageGatewayActions",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsSpecifiedEC2Actions",
      "Action": [
        "ec2:DescribeSnapshots",
        "ec2:DeleteSnapshot"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}
```

{You can use Windows ACLs only with file shares that are enabled for Active Directory.

예제 2: 게이트웨이에 대한 읽기 전용 액세스 허용

다음의 정책은 모든 리소스에 대한 모든 List* 및 Describe* 작업을 허용합니다. 이 작업들은 읽기 전용 작업임에 유의하십시오. 따라서 정책은 사용자가 리소스의 상태를 변경하도록 허용하지 않습니다. 즉, 정책에서는 사용자가 다음과 같은 작업을 수행하도록 허용하지 않습니다. DeleteGateway, ActivateGateway, 및 ShutdownGateway.

이 정책은 DescribeSnapshots Amazon EC2 작업도 허용합니다. 자세한 내용은 단원을 참조하십시오. [DescribeSnapshots](#)의 Amazon EC2 API 레퍼런스.

```
{
  "Version": "2012-10-17",
```

```

"Statement": [
  {
    "Sid": "AllowReadOnlyAccessToAllGateways",
    "Action": [
      "storagegateway:List*",
      "storagegateway:Describe*"
    ],
    "Effect": "Allow",
    "Resource": "*"
  },
  {
    "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
    "Action": [
      "ec2:DescribeSnapshots"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

이전 정책에서는 와일드카드 문자(*)를 사용하는 대신에 다음 예시와 같이 정책이 적용되는 리소스를 특정 게이트웨이에 한정할 수 있습니다. 그러면 정책은 특정 게이트웨이에서만 해당 작업을 허용합니다.

```

"Resource": [
  "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
  "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
]

```

게이트웨이 내에서는 다음 예시와 같이 리소스의 범위를 게이트웨이 볼륨만으로 더 제한할 수 있습니다.

```

"Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/*"

```

예제 3: 특정 게이트웨이에 대한 액세스 허용

다음의 정책은 특정 게이트웨이에서의 모든 작업을 허용합니다. 사용자는 자신이 배포했을 수 있는 기타 게이트웨이에 액세스할 수 없도록 제한을 받습니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowReadOnlyAccessToAllGateways",
      "Action": [
        "storagegateway:List*",
        "storagegateway:Describe*"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsUserToDescribeSnapshotsOnAllGateways",
      "Action": [
        "ec2:DescribeSnapshots"
      ],
      "Effect": "Allow",
      "Resource": "*"
    },
    {
      "Sid": "AllowsAllActionsOnSpecificGateway",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": [
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/",
        "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
      ]
    }
  ]
}

```

이전의 정책에서는 정책에 연결된 사용자가 API 또는 AWS 게이트웨이에 액세스하기 위한 SDK입니다. 그러나 사용자가 Storage Gateway 콘솔을 사용하려고 하는 경우에는 를 허용할 수 있는 권한도 부여해야 합니다. ListGateways 다음 예제에 표시된 대로 을 사용합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {

```

```

    "Sid": "AllowsAllActionsOnSpecificGateway",
    "Action": [
      "storagegateway:*"
    ],
    "Effect": "Allow",
    "Resource": [
      "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id",
      "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/*"
    ]
  },
  {
    "Sid": "AllowsUserToUseAWSConsole",
    "Action": [
      "storagegateway:ListGateways"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

예 4: 사용자가 특정 볼륨에 액세스할 수 있도록 허용

다음 정책은 사용자가 게이트웨이의 특정 볼륨에 대해 모든 작업을 수행하도록 허용합니다. 사용자가 모든 권한을 기본적으로 받는 것은 아니기 때문에 정책은 사용자가 특정 볼륨에만 액세스하도록 제한합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantsPermissionsToSpecificVolume",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
    },
    {
      "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
      "Action": [
        "storagegateway:ListGateways"
      ]
    }
  ]
}

```

```

    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

이전의 정책에서는 정책에 연결된 사용자가 API 또는 AWS 볼륨에 액세스하기 위한 SDK입니다. 그러나 이 사용자가 AWS Storage Gateway 또한 콘솔을 허용하는 권한을 부여할 수도 있습니다. `ListGateways` 다음 예제에 표시된 대로 을 사용합니다.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "GrantsPermissionsToSpecificVolume",
      "Action": [
        "storagegateway:*"
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/gateway-id/volume/volume-id"
    },
    {
      "Sid": "GrantsPermissionsToUseStorageGatewayConsole",
      "Action": [
        "storagegateway:ListGateways"
      ],
      "Effect": "Allow",
      "Resource": "*"
    }
  ]
}

```

예 5: 특정 접두사가 있는 게이트웨이에 대한 모든 작업 허용

다음 정책은 이름이 `DeptX` 로 시작하는 게이트웨이에 대해 사용자가 모든 Storage Gateway 작업을 수행하도록 허용합니다. 이 정책은 또한 허용합니다. `DescribeSnapshots` 스냅샷을 설명하려는 경우에 필요한 Amazon EC2 작업입니다.

```

{

```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "AllowsActionsGatewayWithPrefixDeptX",
    "Action": [
      "storagegateway:*"
    ],
    "Effect": "Allow",
    "Resource": "arn:aws:storagegateway:us-west-2:123456789012:gateway/DeptX"
  },
  {
    "Sid": "GrantsPermissionsToSpecifiedAction",
    "Action": [
      "ec2:DescribeSnapshots"
    ],
    "Effect": "Allow",
    "Resource": "*"
  }
]
}

```

이전의 정책에서는 정책에 연결된 사용자가 API 또는 AWS 게이트웨이에 액세스하기 위한 SDK입니다. 그러나 이 사용자가 AWS Storage Gateway 콘솔에서 설명한 대로 추가 권한을 부여해야 합니다. [예제 3: 특정 게이트웨이에 대한 액세스 허용](#).

태그를 사용하여 게이트웨이 및 리소스에 대한 액세스 제어

게이트웨이 리소스 및 작업에 대한 액세스를 제어하려면 태그를 기반으로 AWS Identity and Access Management(IAM) 정책을 사용할 수 있습니다. 두 가지 방법으로 제어할 수 있습니다.

1. 해당 리소스의 태그를 기반으로 게이트웨이 리소스에 대한 액세스를 제어합니다.
2. IAM 요청 조건에 어떤 태그가 전달될 수 있는지를 제어합니다.

태그를 사용하여 액세스를 제어하는 자세한 방법은 [태그를 사용하여 액세스 제어](#)를 참조하십시오.

리소스의 태그를 기반으로 액세스 제어

사용자나 역할이 게이트웨이 리소스에서 어떤 작업을 수행할 수 있는지를 제어하려면 게이트웨이 리소스의 태그를 사용할 수 있습니다. 예를 들어, 리소스에 있는 태그의 키-값 페어를 기반으로 파일 게이트웨이 리소스에서 특정 API 작업을 허용하거나 거부할 수 있습니다.

다음 예제는 사용자나 역할이 모든 리소스에서 ListTagsForResource, ListFileShares 및 DescribeNFSFileShares 작업을 수행할 수 있도록 허용합니다. 정책은 리소스의 태그에 allowListAndDescribe로 설정된 키와 yes로 설정된 값이 있을 경우에만 적용됩니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:ListTagsForResource",
        "storagegateway:ListFileShares",
        "storagegateway:DescribeNFSFileShares"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/allowListAndDescribe": "yes"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:*"
      ],
      "Resource": "arn:aws:storagegateway:region:account-id:*/*"
    }
  ]
}
```

IAM 요청의 태그를 기반으로 액세스 제어

IAM 사용자가 게이트웨이 리소스에서 무엇을 수행할 수 있는지를 제어하려면 태그를 기반으로 IAM 정책의 조건을 사용할 수 있습니다. 예를 들어 IAM 사용자가 리소스를 생성할 때 제공한 태그를 기반으로 특정 API 작업을 수행할 수 있도록 허용하거나 거부하는 정책을 작성할 수 있습니다.

다음 예제에서 첫 번째 명령문은 게이트웨이를 생성할 때 제공한 키-값 페어가 **Department** 및 **Finance**인 경우에만 사용자가 게이트웨이를 생성할 수 있도록 허용합니다. API 작업을 사용할 경우 이 태그를 활성화 요청에 추가합니다.

두 번째 명령문은 게이트웨이의 태그 키-값 페어가 일치할 경우에만 사용자가 게이트웨이에서 네트워크 파일 시스템 (NFS) 또는 서버 메시지 블록 (SMB) 공유를 생성할 수 있도록 허용합니다. **Department**과 **Finance**. 또한 사용자는 태그를 파일 공유에 추가해야 하며, 태그의 키-값 페어는 **Department** 및 **Finance**여야 합니다. 파일 공유를 생성할 때 파일 공유에 태그를 추가할 수 있습니다. AddTagsToResource 또는 RemoveTagsFromResource 작업에 대한 권한은 없기 때문에 사용자는 게이트웨이나 파일 공유에서 이러한 작업을 수행할 수 없습니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:ActivateGateway"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestTag/Department": "Finance"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "storagegateway:CreateNFSFileShare",
        "storagegateway:CreateSMBFileShare"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/Department": "Finance",
          "aws:RequestTag/Department": "Finance"
        }
      }
    }
  ]
}
```

Storage Gateway API 권한: 작업, 리소스 및 조건 참조

IAM 자격 증명에 연결할 수 있는 [액세스 제어](#) 및 쓰기 권한 정책(자격 증명 기반 정책)을 설정할 때 다음 표를 참조로 사용할 수 있습니다. 표에는 각 Storage Gateway API 작업, 작업을 수행할 권한을 부여할 수 있는 해당 작업, AWS 권한을 부여할 수 있는 리소스입니다. 정책의 Action 필드에서 작업을 지정하고, 정책의 Resource 필드에서 리소스 값을 지정합니다.

사용할 수 있습니다. AWSStorage Gateway 정책에서 차원 조건 키를 사용하면 조건을 표시할 수 있습니다. AWS 전체 키의 전체 목록은 IAM 사용 설명서의 [사용 가능한 키](#)를 참조하세요.

Note

작업을 지정하려면 storagegateway: 접두사 다음에 API 작업 이름을 사용합니다(예: storagegateway:ActivateGateway). 각 Storage Gateway 작업에 대해 와일드카드 문자 (*) 를 리소스로 지정할 수 있습니다.

해당 ARN 형식의 Storage Gateway 리소스 목록은 단원을 참조하십시오. [Storage Gateway 리소스](#).

Storage Gateway API 및 작업에 필요한 권한은 다음과 같습니다.

[ActivateGateway](#)

작업: storagegateway:ActivateGateway

리소스: *

[AddCache](#)

작업: storagegateway:AddCache

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[AddTagsToResource](#)

작업: storagegateway:AddTagsToResource

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

또는

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

또는

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

AddUploadBuffer

작업: storagegateway:AddUploadBuffer

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

AddWorkingStorage

작업: storagegateway:AddWorkingStorage

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CancelArchival

작업: storagegateway:CancelArchival

리소스: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CancelRetrieval

작업: storagegateway:CancelRetrieval

리소스: arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

CreateCachediSCSIVolume

작업: storagegateway>CreateCachediSCSIVolume

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateSnapshot

작업: storagegateway>CreateSnapshot

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

CreateSnapshotFromVolumeRecoveryPoint

작업: storagegateway>CreateSnapshotFromVolumeRecoveryPoint

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

CreateStorediSCSIVolume

작업: storagegateway:CreateStorediSCSIVolume

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

CreateTapes

작업: storagegateway:CreateTapes

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteBandwidthRateLimit

작업: storagegateway>DeleteBandwidthRateLimit

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteChapCredentials

작업: storagegateway>DeleteChapCredentials

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
target/*iSCSITarget*

DeleteGateway

작업: storagegateway>DeleteGateway

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteSnapshotSchedule

작업: storagegateway>DeleteSnapshotSchedule

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DeleteTape

작업: storagegateway>DeleteTape

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DeleteTapeArchive

작업: storagegateway>DeleteTapeArchive

리소스: *

[DeleteVolume](#)

작업: storagegateway:DeleteVolume

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

[DescribeBandwidthRateLimit](#)

작업: storagegateway:DescribeBandwidthRateLimit

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeCache](#)

작업: storagegateway:DescribeCache

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeCachediSCSIVolumes](#)

작업: storagegateway:DescribeCachediSCSIVolumes

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

[DescribeChapCredentials](#)

작업: storagegateway:DescribeChapCredentials

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
target/*iSCSItarget*

[DescribeGatewayInformation](#)

작업: storagegateway:DescribeGatewayInformation

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[DescribeMaintenanceStartTime](#)

작업: storagegateway:DescribeMaintenanceStartTime

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeSnapshotSchedule

작업: storagegateway:DescribeSnapshotSchedule

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DescribeStorediSCSIVolumes

작업: storagegateway:DescribeStorediSCSIVolumes

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

DescribeTapeArchives

작업: storagegateway:DescribeTapeArchives

리소스: *

DescribeTapeRecoveryPoints

작업: storagegateway:DescribeTapeRecoveryPoints

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeTapes

작업: storagegateway:DescribeTapes

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeUploadBuffer

작업: storagegateway:DescribeUploadBuffer

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeVTLDevices

작업: storagegateway:DescribeVTLDevices

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

DescribeWorkingStorage

작업: storagegateway:DescribeWorkingStorage

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[DisableGateway](#)

작업: `storagegateway:DisableGateway`

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[ListGateways](#)

작업: `storagegateway:ListGateways`

리소스: *

[ListLocalDisks](#)

작업: `storagegateway:ListLocalDisks`

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[ListTagsForResource](#)

작업: `storagegateway:ListTagsForResource`

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

또는

`arn:aws:storagegateway:region:account-id:gateway/gateway-id/
volume/volume-id`

또는

`arn:aws:storagegateway:region:account-id:tape/tapebarcode`

[ListTapes](#)

작업: `storagegateway:ListTapes`

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id`

[ListVolumeInitiators](#)

작업: `storagegateway:ListVolumeInitiators`

리소스: `arn:aws:storagegateway:region:account-id:gateway/gateway-id/
volume/volume-id`

ListVolumeRecoveryPoints

작업: storagegateway:ListVolumeRecoveryPoints

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

ListVolumes

작업: storagegateway:ListVolumes

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RemoveTagsFromResource

작업: storagegateway:RemoveTagsFromResource

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

또는

arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

또는

arn:aws:storagegateway:*region*:*account-id*:tape/*tapebarcode*

ResetCache

작업: storagegateway:ResetCache

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeArchive

작업: storagegateway:RetrieveTapeArchive

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

RetrieveTapeRecoveryPoint

작업: storagegateway:RetrieveTapeRecoveryPoint

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[ShutdownGateway](#)

작업: storagegateway:ShutdownGateway

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[StartGateway](#)

작업: storagegateway:StartGateway

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateBandwidthRateLimit](#)

작업: storagegateway:UpdateBandwidthRateLimit

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateChapCredentials](#)

작업: storagegateway:UpdateChapCredentials

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
target/*iSCSItarget*

[UpdateGatewayInformation](#)

작업: storagegateway:UpdateGatewayInformation

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateGatewaySoftwareNow](#)

작업: storagegateway:UpdateGatewaySoftwareNow

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateMaintenanceStartTime](#)

작업: storagegateway:UpdateMaintenanceStartTime

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*

[UpdateSnapshotSchedule](#)

작업: storagegateway:UpdateSnapshotSchedule

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
volume/*volume-id*

[UpdateVTLDeviceType](#)

작업: storagegateway:UpdateVTLDeviceType

리소스: arn:aws:storagegateway:*region*:*account-id*:gateway/*gateway-id*/
device/*vtldevice*

관련 주제

- [액세스 제어](#)
- [고객 관리형 정책 예](#)

Storage Gateway에 서비스 연결 역할 사용

Storage Gateway 사용AWS Identity and Access Management(IAM)[서비스 연결 역할](#). 서비스 연결 역할은 Storage Gateway에 직접 연결된 고유한 유형의 IAM 역할입니다. 서비스 연결 역할은 Storage Gateway에서 사전 정의하며, 서비스에서 다른 사람을 호출하기 위해 필요한 모든 권한을 포함합니다. AWS사용자를 대신하여 서비스를 제공합니다.

서비스 연결 역할을 사용하면 필요한 권한을 수동으로 추가할 필요가 없으므로 Storage Gateway를 더 쉽게 설정할 수 있습니다. Storage Gateway에서 서비스 연결 역할의 권한을 정의하므로 다르게 정의되지 않은 한, Storage Gateway 게이트웨이만 해당 역할을 수임할 수 있습니다. 정의된 권한에는 신뢰 정책과 권한 정책이 포함되며, 이 권한 정책은 다른 IAM 엔터티에 연결할 수 없습니다.

서비스 연결 역할을 지원하는 기타 서비스에 대한 자세한 내용은 [IAM과 작동하는 AWS 서비스](#)를 참조하고 서비스 연결 역할(Service-Linked Role) 열의 예(Yes)가 있는 서비스를 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예 링크를 선택합니다.

Storage Gateway의 서비스 연결 역할 권한

Storage Gateway는 서비스 연결 역할을 사용합니다. AWS서비스포어스토리지게이트웨이— AWS서비스포어스토리지게이트웨이.

AWSServiceRoleForStorageGateway 서비스 연결 역할은 역할을 수임하기 위해 다음 서비스를 신뢰합니다.

- storagegateway.amazonaws.com

역할 권한 정책은 Storage Gateway가 지정된 리소스에서 다음 작업을 완료하도록 허용합니다.

- 작업: `arn:aws:fsx:*:*:backup/*`에 대한 `fsx:ListTagsForResource`

IAM 개체 (사용자, 그룹, 역할 등) 가 서비스 연결 역할을 생성하고 편집할 수 있도록 권한을 구성할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 권한](#)을 참조하세요.

Storage Gateway에 대한 서비스 연결 역할 생성

서비스 연결 역할은 수동으로 생성할 필요가 없습니다. Storage Gateway 게이트웨이를 만들 때 `AssociateFileSystem`의 API 호출 AWS Management Console, AWS CLI, 또는 AWS API Storage Gateway에서 서비스 연결 역할을 생성합니다.

Important

이 서비스 연결 역할은 이 역할이 지원하는 기능을 사용하는 다른 서비스에서 작업을 완료했을 경우 계정에 나타날 수 있습니다. 또한 2021년 3월 31일 이전에 Storage Gateway 서비스가 서비스 연결 역할을 지원하기 시작한 이전에 이 서비스를 사용 중이었다면 Storage Gateway 사용자 계정에 `AWSServiceRoleForStorageGateway` 역할을 생성했습니다. 자세한 내용은 [내 IAM 계정에 표시되는 새 역할](#)을 참조하세요.

이 서비스 연결 역할을 삭제한 다음 다시 생성해야 하는 경우 동일한 프로세스를 사용하여 계정에서 역할을 다시 생성할 수 있습니다. Storage Gateway 게이트웨이를 만들 때 `AssociateFileSystemAPI` 호출 시 Storage Gateway에서 서비스 연결 역할을 다시 생성합니다.

IAM 콘솔을 사용하여 에서 서비스 연결 역할을 생성할 수도 있습니다. AWS 서비스 포어 스토리지 게이트웨이 사용 사례 AWS CLI 또는 AWS API에서 `storagegateway.amazonaws.com` 서비스 이름의 서비스 연결 역할을 생성합니다. 자세한 내용은 단원을 참조하십시오. [서비스 연결 역할 만들기](#)의 IAM 사용 설명서. 이 서비스 연결 역할을 삭제한 후에는 동일한 프로세스를 사용하여 역할을 다시 생성할 수 있습니다.

Storage Gateway에 대한 서비스 연결 역할 편집

Storage Gateway 게이트웨이에서는 `AWSServiceRoleForStorageGateway` 서비스 연결 역할을 편집할 수 없습니다. 서비스 연결 역할을 생성한 후에는 다양한 개체가 역할을 참조할 수 있기 때문에 역할 이름을 변경할 수 없습니다. 하지만 IAM을 사용하여 역할의 설명을 편집할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [서비스 연결 역할 편집](#)을 참조하세요.

Storage Gateway에 대한 서비스 연결 역할 삭제

Storage Gateway AWSServiceRoleForStorageGateway의 역할을 자동으로 삭제합니다. AWSServiceForStorageGateway 역할을 삭제하려면 다음을 호출해야 합니다. iam:DeleteSLR API. 서비스 연결 역할에 종속되는 스토리지 게이트웨이 리소스가 없으면 삭제가 성공하고 그렇지 않으면 삭제가 실패합니다. 서비스 연결 역할을 삭제하려면 IAM API를 사용해야 합니다. iam:DeleteRole 또는 iam:DeleteServiceLinkedRole. 이 경우 Storage Gateway API를 사용하여 계정의 게이트웨이 또는 파일 시스템 연결을 먼저 삭제한 다음 다음을 사용하여 서비스 연결 역할을 삭제해야 합니다. iam:DeleteRole 또는 iam:DeleteServiceLinkedRole API. IAM을 사용하여 서비스 연결 역할을 삭제하는 경우 Storage Gateway 게이트웨이를 사용해야 합니다. DisassociateFileSystemAssociation API는 먼저 계정의 모든 파일 시스템 연결을 삭제합니다. 그렇지 않으면 삭제 작업이 실패합니다.

Note

리소스를 삭제할 때 Storage Gateway 서비스가 역할을 사용 중이면 삭제에 실패할 수 있습니다. 이 문제가 발생하면 몇 분 기다렸다가 작업을 다시 시도하세요.

AWSServiceRoleForStorageGateway에서 사용하는 Storage Gateway 리소스를 삭제하려면

1. 서비스 콘솔, CLI 또는 API를 사용하여 리소스를 정리하고 역할을 삭제하는 호출을 하거나 IAM 콘솔, CLI 또는 API를 사용하여 삭제를 수행합니다. 이 경우 Storage Gateway API를 사용하여 계정의 게이트웨이 및 파일 시스템 연결을 먼저 삭제해야 합니다.
2. IAM 콘솔, CLI 또는 API를 사용하는 경우 IAM을 사용하여 서비스 연결 역할을 삭제합니다. DeleteRole 또는 DeleteServiceLinkedRole API.

IAM을 사용하여 수동으로 서비스 연결 역할 삭제

IAM 콘솔을 사용합니다. AWS CLI, 또는 AWS AWSServiceRoleForStorageGateway 서비스 연결 역할을 삭제하는 API입니다. 자세한 내용은 [IAM 사용 설명서](#)의 서비스 연결 역할 삭제 단원을 참조하세요.

Storage Gateway 서비스 연결 역할을 지원하는 리전

Storage Gateway는 서비스가 제공되는 모든 리전에서 서비스 연결 역할을 사용할 수 있도록 지원합니다. 자세한 내용은 [AWS 서비스 엔드포인트](#)를 참조하세요.

Storage Gateway는 서비스가 제공되는 모든 리전에서 서비스 연결 역할 사용을 지원하지 않습니다. 다음 리전에서 AWSServiceRoleForStorageGateway 역할을 사용할 수 있습니다.

리전 이름	리전 자격 증명	Storage Gateway Gateway의 Support
미국 동부(버지니아 북부)	us-east-1	예
미국 동부(오하이오)	us-east-2	예
미국 서부(캘리포니아 북부 지역)	us-west-1	예
미국 서부(오레곤)	us-west-2	예
Asia Pacific (Mumbai)	ap-south-1	예
아시아 태평양(오사카)	ap-northeast-3	예
Asia Pacific (Seoul)	ap-northeast-2	예
아시아 태평양(싱가포르)	ap-southeast-1	예
아시아 태평양(시드니)	ap-southeast-2	예
Asia Pacific (Tokyo)	ap-northeast-1	예
Canada (Central)	ca-central-1	예
Europe (Frankfurt)	eu-central-1	예
유럽(아일랜드)	eu-west-1	예
Europe (London)	eu-west-2	예
Europe (Paris)	eu-west-3	예
남아메리카(상파울루)	sa-east-1	예
AWS GovCloud (US)	us-gov-west-2	예

AWS Storage Gateway의 로깅 및 모니터링

Storage Gateway 다음과 통합됩니다. AWS CloudTrail, 사용자, 역할 또는 에서 수행한 작업 기록을 제공하는 서비스 AWS Storage Gateway 게이트웨이에서 서비스를 제공합니다. CloudTrail은 Storage Gateway 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처되는 호출에는 Storage Gateway 콘솔로 부터의 호출과 Storage Gateway API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Storage Gateway 이벤트를 비롯하여 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 CloudTrail 콘솔의 이벤트 기록(Event history)에서 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Storage Gateway에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하세요.

CloudTrail의 Storage Gateway 정보

CloudTrail은 계정 생성 시 AWS 계정에서 사용되도록 설정됩니다. Storage Gateway 활동이 발생하면 해당 활동이 다른 작업과 함께 CloudTrail 이벤트에 기록됩니다. AWS의 서비스 이벤트이벤트 기록. AWS 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 [CloudTrail 이벤트 기록을 사용하여 이벤트 보기](#)를 참조하세요.

의 이벤트를 지속적으로 기록하려면 AWS Storage Gateway의 이벤트를 비롯하여 계정에서 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 콘솔에서 추적을 생성하면 기본적으로 모든 AWS 리전에 추적이 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또는 CloudTrail 로그에서 수집된 이벤트 데이터를 추가 분석 및 처리하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- [추적 생성 개요](#)
- [CloudTrail 지원 서비스 및 통합](#)
- [CloudTrail에 대한 Amazon SNS 알림 구성](#)
- [여러 리전에서 CloudTrail 로그 파일 받기 및 여러 계정에서 CloudTrail 로그 파일 받기](#)

모든 Storage Gateway 작업이 로깅되고 에서 문서화됩니다. [작업](#) 주제. 예를 들어 ActivateGateway, ListGateways 및 ShutdownGateway 작업을 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 및 로그 항목에는 요청을 생성한 사용자에게 대한 정보가 들어 있습니다. 자격 증명 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청을 루트로 했는지 아니면 AWS Identity and Access Management(IAM) 사용자 자격 증명으로 했는지.
- 역할 또는 연합된 사용자에게 대한 임시 보안 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 [CloudTrail userIdentity 요소](#)를 참조하세요.

Storage Gateway 로그 파일 항목

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 입력할 수 있게 하는 구성입니다.

CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 퍼블릭 API 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음은 작업을 보여주는 CloudTrail 로그 항목이 나타낸 예제입니다.

```
{ "Records": [{
  "eventVersion": "1.02",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAI5AUPEBH2M7JTNVC",
    "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"
  ]]
}

```

다음은 ListGateways 작업을 보여 주는 CloudTrail 로그 항목의 예입니다.

```

{
  "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDAI5AUEPBH2M7JTNVC",
      "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": "
6U2N42CU37KA08BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
    "eventID": "f76e5919 - 9362 - 48ff - a7c4 -
d203a189ec8d ",
    "eventType": "AwsApiCall ",
    "apiVersion": "20130630 ",

```

```

    " recipientAccountId ":" 444455556666"
  }
}

```

의 규정 준수 확인AWSStorage Gateway

타사 감사자가 의 보안 및 규정 준수를 평가합니다.AWS다중 구성의 일부인 Storage GatewayAWS 규정 준수 프로그램. 여기에는 SOC, PCI, ISO, FedRAMP, HIPAA, MTCS, MTCS, C5, K-ISMS, ENS High, OSPAR 및 HITRUST CSF가 포함됩니다.

특정 규정 준수 프로그램의 범위 내에 있는 AWS 서비스 목록은 [규정 준수 프로그램 제공 범위 내 AWS 서비스](#)를 참조하세요. 일반적인 내용은 [AWS 규정 준수 프로그램](#)을 참조하세요.

AWS Artifact를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 [AWS Artifact에서 보고서 다운로드](#)를 참조하세요.

Storage Gateway 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률 및 규정에 따라 결정됩니다.AWS규정 준수에 도움이 되도록 다음 리소스를 제공합니다.

- [보안 및 규정 준수 빠른 시작 안내서](#) - 이 배포 안내서에서는 아키텍처 고려 사항에 관해 설명하고 AWS에서 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다.
- [HIPAA 보안 및 규정 준수 기술 백서 아키텍팅](#) - 이 백서는 기업에서 AWS를 사용하여 HIPAA를 준수 하는 애플리케이션을 생성하는 방법을 설명합니다.
- [AWS 규정 준수 리소스](#) - 고객 조직이 속한 산업 및 위치에 적용될 수 있는 워크북 및 가이드 모음입니다.
- AWS Config 개발자 가이드의 [규칙을 사용하여 리소스 평가](#) - AWS Config 서비스는 내부 사례, 산업 지침 및 규제에 대한 리소스 구성의 준수 상태를 평가합니다.
- [AWS Security Hub](#) - 이 AWS 서비스는 보안 산업 표준 및 모범 사례 규정 준수 여부를 확인하는 데 도움이 되도록 AWS 내 보안 상태를 종합적으로 보여줍니다.

의 복원성AWSStorage Gateway

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다. AWS 리전은 물리적으로 분리되고 격리된 다수의 가용 영역을 제공하며 이러한 가용 영역은 짧은 지연 시간, 높은 처리량 및 높은 중복성을 갖춘 네트워크에 연결되어 있습니다. 가용 영역을 사용하면 중단 없이 영역 간에 자동으로 장애 조치가 이루어지는 애플리케이션 및 데이터베이스를 설계하고 운영할 수 있습니다. 가용 영역은 기존의 단일 또는 다중 데이터 센터 인프라보다 가용성, 내결함성, 확장성이 뛰어납니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 [AWS 글로벌 인프라](#)를 참조하세요.

뿐만 아니라 AWS 글로벌 인프라 Storage Gateway는 데이터 복원성과 백업 요구 사항을 지원하는 다양한 기능을 제공합니다.

- VMware vSphere 고가용성 (VMware HA) 을 사용하면 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 자세한 내용은 단원을 참조하십시오. [Storage Gateway VMware vSphere 고가용성 사용](#).
- AWS Backup를 사용해 볼륨을 백업합니다. 자세한 내용은 단원을 참조하십시오. [사용 AWS Backup 볼륨을 백업합니다](#).
- 복구 지점에서 볼륨을 복제합니다. 자세한 내용은 단원을 참조하십시오. [볼륨 복제](#).
- Amazon S3 Glacier에 가상 테이프를 아카이빙합니다. 자세한 내용은 단원을 참조하십시오. [가상 테이프 아카이빙](#).

의 인프라 보안 AWSStorage Gateway

관리형 서비스로서 AWSStorage Gateway AWS에 설명된 글로벌 네트워크 보안 절차 [Amazon Web Services: 보안 프로세스 개요](#) 백서.

사용하는 경우 AWS 네트워크를 통해 Storage Gateway에 액세스하는 API 호출을 게시한 클라이언트가 전송 계층 보안(TLS) 1.0 이상을 지원해야 합니다. TLS 1.2 이상을 권장합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 PFS(전달 완전 보안, Perfect Forward Secrecy)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 요청은 액세스 키 ID 및 IAM 주체와 관련된 보안 액세스 키를 사용하여 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 자격 증명을 생성하여 요청에 서명할 수 있습니다.

Storage Gateway 보안 모범 사례

AWSStorage Gateway는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 모범 사례는 환경에 적절하지 않거나 충분하지 않을 수 있으므로 참고용으로만 사용해 주세요. 자세한 내용은 단원을 참조하십시오. [AWS 보안 모범 사례](#).

게이트웨이 문제 해결

아래와 같이 게이트웨이, 파일 공유, 볼륨, 가상 테이프 및 스냅샷과 관련된 문제의 해결에 대한 정보를 얻을 수 있습니다. 온프레미스 게이트웨이 문제 해결에 대한 정보에서는 VMware ESXi 및 Microsoft Hyper-V 클라이언트에 배포하는 게이트웨이를 다룹니다. 파일 공유 관련 문제 해결 정보는 Amazon S3 파일 게이트웨이 유형에 적용됩니다. 볼륨 관련 문제 해결 정보는 볼륨 게이트웨이 유형에 적용됩니다. 테이프 관련 문제 해결 정보는 테이프 게이트웨이 유형에 적용됩니다. 게이트웨이 문제에 대한 문제 해결 정보는 CloudWatch 지표 사용에 적용됩니다. 고가용성 문제에 대한 문제 해결 정보는 VMware vSphere HA(고가용성) 플랫폼에서 실행 중인 게이트웨이를 다룹니다.

주제

- [온프레미스 게이트웨이 문제 해결](#)
- [Microsoft Hyper-V 설정 문제를 해결합니다.](#)
- [Amazon EC2 게이트웨이 문제 해결](#)
- [하드웨어 어플라이언스 문제 해결](#)
- [파일 게이트웨이 문제 해결](#)
- [고가용성 상태 알림](#)
- [고가용성 관련 문제를 해결합니다.](#)
- [데이터 복구를 위한 모범 사례](#)

온프레미스 게이트웨이 문제 해결

온프레미스 게이트웨이 관련 작업 시 발생할 수 있는 일반적인 문제와 사용 방법에 대한 정보를 확인할 수 있습니다. 지원 게이트웨이 관련 문제를 해결합니다.

다음 표는 온프레미스 게이트웨이 관련 작업 시 발생할 수 있는 전형적인 문제를 나열한 것입니다.

문제	취할 조치
게이트웨이의 IP 주소를 찾을 수 없습니다.	<p>하이퍼바이저 클라이언트로 호스트에 접속하여 게이트웨이 IP 주소를 찾습니다.</p> <ul style="list-style-type: none"> • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다.

문제	취할 조치
	<ul style="list-style-type: none"> • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. <p>그래도 게이트웨이 IP 주소를 찾기 어려운 경우:</p> <ul style="list-style-type: none"> • VM이 켜져 있는지 확인합니다. VM이 켜져 있는 경우에만 IP 주소가 게이트웨이에 할당됩니다. • VM이 스타트업을 마칠 때까지 기다리십시오. VM을 방금 켜었다면 게이트웨이가 부팅 시퀀스를 마치는 데 몇 분이 걸릴 수 있습니다.
<p>네트워크 또는 방화벽에 문제가 있습니다.</p>	<ul style="list-style-type: none"> • 게이트웨이에 적절한 포트를 허용합니다. • 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링하거나 제한하는 경우, 방화벽 및 라우터가 에 대한 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. AWS. 네트워크 및 방화벽 요건에 대한 자세한 내용은 네트워크 및 방화벽 요구 사항 단원을 참조하십시오.
<p>를 클릭하면 게이트웨이의 활성화가 실패합니다. 활성화를 진행합니다.Storage Gateway 관리 콘솔의 버튼을 클릭합니다.</p>	<ul style="list-style-type: none"> • 클라이언트에서 VM을 ping하여 게이트웨이 VM에 액세스할 수 있는지 확인합니다. • VM이 인터넷에 네트워크로 연결되어 있는지 확인합니다. 연결되어 있지 않으면 SOCKS 프록시를 구성해야 합니다. 이에 대한 자세한 내용은 게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트 섹션을 참조하세요. • 호스트의 시간이 올바른지, 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성되어 있는지, 게이트웨이 VM의 시간이 올바른지 확인합니다. 하이퍼바이저 호스트와 VM의 시간을 동기화하는 작업에 대한 자세한 내용은 게이트웨이의 네트워크 시간 프로토콜 (NTP) 서버 구성 단원을 참조하십시오. • 이 절차를 수행한 후 Storage Gateway 콘솔 및 게이트웨이 설정 및 활성화 마법사. • VM의 RAM 용량이 최소 7.5GB인지 확인합니다. RAM 용량이 7.5GB 미만인 경우, 게이트웨이 할당이 되지 않습니다. 자세한 정보는 파일 게이트웨이 설정 요구 사항을 참조하십시오.

문제	취할 조치
<p>업로드 버퍼 공간으로 할당된 디스크를 제거해야 합니다. 예를 들어 게이트웨이의 업로드 버퍼 공간을 줄이거나 업로드 버퍼로 사용하는 디스크에 장애가 있어 교체해야 할 경우가 있습니다.</p>	
<p>게이트웨이와 간 대역폭을 개선해야 합니다.AWS.</p>	<p>애플리케이션 및 게이트웨이 VM을 연결하는 것과는 별도로 네트워크 어댑터(NIC)에서 AWS에 대한 인터넷 연결을 설정하여 게이트웨이에서 AWS까지의 대역폭을 개선할 수 있습니다. 이 접근 방식은 AWS에 고대역폭으로 연결되어 있어 특히 스냅샷 복원 중에 대역폭 경합을 방지하고자 하는 경우에 유용하다. 처리량이 많은 워크로드 요구 사항의 경우 AWS Direct Connect 온프레미스 게이트웨이 간에 전용 네트워크 연결을 설정합니다.AWS. 게이트웨이에서 AWS까지의 연결 대역폭을 측정하기 위해 게이트웨이의 CloudBytesDownloaded 및 CloudBytesUploaded 지표를 사용합니다. 이에 관한 자세한 내용은 성능 단원을 참조하십시오. 인터넷 연결성을 개선하면 업로드 버퍼가 꽉 차지 않도록 하는 데 도움이 됩니다.</p>

문제	취할 조치
<p>게이트웨이로의 처리량 또는 게이트웨이로부터의 처리량이 0으로 떨어집니다.</p>	<ul style="list-style-type: none"> • 온게이트웨이Storage Gateway 콘솔의 탭에서 게이트웨이 VM의 IP 주소가 하이퍼바이저 클라이언트 소프트웨어 (즉, VMware vSphere 클라이언트 또는 Microsoft Hyper-V 관리자) 를 사용하는 것과 동일한지 확인합니다. 불일치하는 경우, 단원에 나와 있는 것처럼 Storage Gateway 콘솔에서 게이트웨이를 다시 시작합니다.게이트웨이 VM 종료. 다시 시작한 후의 주소는IP 주소Storage Gateway 콘솔의 목록게이트웨이탭은 하이퍼바이저 클라이언트에서 결정하는 게이트웨이의 IP 주소와 일치해야 합니다. • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다. • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. • 게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트 단원의 설명 대로 게이트웨이가 AWS에 연결되어 있는지 확인합니다. • 게이트웨이의 네트워크 어댑터 구성을 점검하고 게이트웨이에서 사용하도록 설정하려는 인터페이스가 모두 사용 가능 상태인지 확인합니다. 게이트웨이의 네트워크 어댑터 구성을 보려면 게이트웨이용 네트워크 어댑터 구성 단원의 지침에 따라 게이트웨이의 네트워크 구성을 볼 수 있는 옵션을 선택합니다. <p>Amazon CloudWatch 콘솔에서 게이트웨이로의 처리량과 게이트로부터의 처리량을 볼 수 있습니다. 게이트웨이에서 및 에서 게이트웨이로의 처리량 측정에 대한 자세한 정보AWS참조,성능.</p>
<p>Microsoft Hyper-V에서 Storage Gateway 가져오기 (배포) 할 수 없습니다.</p>	<p>Microsoft Hyper-V에서 게이트웨이를 배포할 때 흔히 겪는 몇 가지 문제를 다루는 Microsoft Hyper-V 설정 문제를 해결합니다. 단원을 참조하십시오.</p>
<p>다음과 같은 메시지가 나타납니다. “게이트웨이에서 볼륨에 기록된 데이터는 다음에 안전하게 저장되지 않습니다.AWS”.</p>	<p>게이트웨이 VM이 또 다른 게이트웨이 VM의 복제 또는 스냅샷으로부터 생성된 경우 이 메시지를 수신하게 됩니다. 그렇지 않은 경우 문의하십시오.지원.</p>

활성화지원은프리미스에서 호스팅되는 게이트웨이 문제 해결

Storage Gateway 는 활성화와 같은 다양한 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 지원 게이트웨이 액세스를 허용하여 게이트웨이 문제 해결을 돕습니다. 기본적으로 지원 게이트웨이 액세스가 비활성화되어 있습니다. 호스트의 로컬 콘솔을 통해 이 액세스 권한을 활성화합니다. 를 부여하려면 지원 게이트웨이에 액세스하려면 먼저 호스트용 로컬 콘솔에 로그인하여 스토리지 게이트웨이의 콘솔로 이동한 후 지원 서버에 접속합니다.

를 활성화하려면 지원 게이트웨이 액세스

1. 호스트의 로컬 콘솔에 로그인합니다.

- VMware ESXi — 자세한 내용은 단원을 참조하십시오. [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스.](#)
- Microsoft Hyper-V — 자세한 내용은 단원을 참조하십시오. [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스.](#)

로컬 콘솔 화면은 다음과 같습니다.

2. 프롬프트에서 를 입력합니다. 5를 열려면 지원 Channel 콘솔.

3. **h**를 입력하여 AVAILABLE COMMANDS(사용 가능한 명령) 창을 엽니다.

4. 다음 중 하나를 수행하세요.

- 게이트웨이가 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령창, 입력 **open-support-channel** Storage Gateway 대한 고객 지원 센터에 연결할 수 있습니다. 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. AWS. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
- 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **open-support-channel**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway 에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. AWS. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

Note

채널 번호는 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 포트 번호가 아닙니다. 그 대신에 게이트웨이는 Storage Gateway 서버에 SSH (Secure Shell) (TCP 22) 로 접속하여 해당 연결에 지원 채널을 제공합니다.

5. 지원 채널이 설정되면 에 대한 지원 서비스 번호를 제공하십시오. 지원그래서지원문제 해결 지원을 제공할 수 있습니다.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. Amazon Web Services 지원팀에서 Support 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **Enterexit**를 눌러 Storage Gateway 콘솔에서 로그아웃
8. 프롬프트 메시지에 따라 로컬 콘솔을 종료합니다.

Microsoft Hyper-V 설정 문제를 해결합니다.

다음 표에는 Microsoft Hyper-V 플랫폼에서 Storage Gateway 배포 시 발생할 수 있는 일반적인 문제가 나와 있습니다.

문제	취할 조치
게이트웨이 가져오기를 시도하면 다음과 같이 오류 메시지가 표시됩니다. "가져오기에 실패했습니다. Unable to find virtual machine import file under location ..."라는 오류 메시지가 표시됩니다.	<p>이 오류는 다음과 같은 이유로 발생할 수 있습니다.</p> <ul style="list-style-type: none"> • 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 배포했지만 선택하지 않은 경우 가상 머신 복사 옵션을 선택하고 모든 파일 복제에 있는 옵션 가상 머신 가져오기 대화 상자에서 압축이 풀린 게이트웨이 파일이 있는 위치에 VM이 만들어졌으므로 이 위치에서 다시 가져올 수 없습니다. 이 문제를 해결하려면 압축을 해제한 게이트웨이 소스 파일의 새 사본을 얻어 이를 새 위치에 복사하면 됩니다. 새 위치를 가져오는 위치로 사용합니다. 다음 예시는 압축 해제한 소스 파일 위치에서 게이트웨이를 여러 개 생성할 계획인 경우, 확인해야 할 옵션입니다.

문제	취할 조치
<p>게이트웨이 가져오기를 시도하면 다음과 같이 오류 메시지가 표시됩니다. “가져오기에 실패했습니다. Import task failed to copy file.”라는 오류 메시지가 표시됩니다.</p>	<p>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.</p>
<p>게이트웨이 가져오기를 시도하면 다음과 같이 오류 메시지가 표시됩니다. “가져오기에 실패했습니다. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again.”라는 오류 메시지가 표시됩니다.</p>	<p>게이트웨이를 가져올 때 다음을 선택해야 합니다. 가상 머신 복사 옵션을 선택하고 모든 파일 복제에 있는 옵션 가상 머신 가져오기 VM에 대한 새 고유 ID를 생성하는 대화 상자입니다. 다음 예시는 Import Virtual Machine(가상 머신 가져오기) 대화 상자에서 사용해야 할 옵션입니다.</p>
<p>게이트웨이 VM을 시작하려 하면 "The child partition processor setting is incompatible with parent partition."이라는 오류 메시지가 표시됩니다.</p>	<p>이 오류는 게이트웨이에 필요한 CPU와 호스트에서 사용 가능한 CPU 사이의 CPU 불일치로 인해 발생할 수 있습니다. 기본 하이퍼바이저가 VM CPU 개수를 지원하도록 해야 합니다.</p> <p>Storage Gateway 요구 사항에 대한 자세한 내용은 단원을 참조하십시오. 파일 게이트웨이 설정 요구 사항.</p>
<p>게이트웨이 VM을 시작하려 하면 “Failed to create partition: 요청된 서비스를 완료하기 위한 리소스가 부족합니다.”</p>	<p>이 오류는 게이트웨이에 필요한 RAM과 호스트에서 사용 가능한 RAM 사이의 RAM 불일치로 인해 발생할 수 있습니다.</p> <p>Storage Gateway 요구 사항에 대한 자세한 내용은 단원을 참조하십시오. 파일 게이트웨이 설정 요구 사항.</p>

문제	취할 조치
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 정보는 게이트웨이의 네트워크 시간 프로토콜 (NTP) 서버 구성 을 참조하십시오.
호스트 파일 시스템에 압축 해제된 Microsoft Hyper-V Storage Gateway 파일을 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.

Amazon EC2 게이트웨이 문제 해결

다음 섹션에서는 Amazon EC2 EC2에 배포된 게이트웨이 사용 시 발생할 수 있는 일반적인 문제를 확인할 수 있습니다. 온프레미스 게이트웨이와 Amazon EC2 배포한 게이트웨이 간의 차이점에 대한 자세한 내용은 단원을 참조하십시오. [Amazon EC2 호스트에 파일 게이트웨이 배포](#).

주제

- [잠시 후 게이트웨이 활성화가 이루어지지 않았습니다.](#)
- [인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.](#)
- [당신이 원한다지원EC2 게이트웨이 문제를 해결하는 데 도움이 됩니다.](#)

잠시 후 게이트웨이 활성화가 이루어지지 않았습니다.

Amazon EC2 콘솔에서 다음을 확인합니다.

- 인스턴스와 연결한 보안 그룹에서 포트 80이 활성화되어 있는지 여부. 보안 그룹 규칙 추가에 대한 자세한 내용은 단원을 참조하십시오. [보안 그룹 규칙 추가](#)의 Linux 인스턴스용 Amazon EC2 사용 설명서.
- 게이트웨이 인스턴스는 실행 중으로 표시됩니다. Amazon EC2 콘솔에서는 상태인스턴스의 값은 RUNNING이어야 합니다.
- 단원에서 설명한 대로 Amazon EC2 인스턴스 유형이 최소 요구 사항을 충족해야 합니다. [스토리지 요구 사항](#).

문제를 해결한 후 게이트웨이를 다시 활성화합니다. 이렇게 하려면 Storage Gateway 콘솔을 열고 Amazon EC2 새 게이트웨이 배포를 누르고 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 Machine Image(AMI)의 이름을 확인합니다. Storage Gateway AMI 기반 인스턴스는 텍스트로 시작해야 합니다. **aws-storage-gateway-ami**.
- Storage Gateway AMI 기반 인스턴스가 여러 개인 경우, 인스턴스 시작 시간을 확인하여 올바른 인스턴스를 찾습니다.

당신이 원한다 지원 EC2 게이트웨이 문제를 해결하는 데 도움이 됩니다.

Storage Gateway 는 활성화와 같은 다양한 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 지원 게이트웨이 액세스를 허용하여 게이트웨이 문제 해결을 돕습니다. 기본적으로 지원 게이트웨이 액세스가 비활성화되어 있습니다. Amazon EC2 로컬 콘솔을 통해 이 액세스 권한을 활성화합니다. SSH (Secure Shell) 을 통해 Amazon EC2 로컬 콘솔에 로그인합니다. SSH를 통해 성공적으로 로그인하려면 인스턴스의 보안 그룹에 TCP 포트 22를 개방하는 규칙이 있어야 합니다.

Note

기존 보안 그룹에 새 규칙을 추가할 경우, 해당 보안 그룹을 사용하는 모든 인스턴스에 새 규칙이 적용됩니다. 보안 그룹 및 보안 그룹 규칙을 추가하는 방법에 대한 자세한 내용은 단원을 참조하십시오. [Amazon EC2 보안 그룹](#)의 Amazon EC2 사용 설명서.

를 허용하려면 지원 게이트웨이에 접속하려면 먼저 Amazon EC2 인스턴스용 로컬 콘솔에 로그인하여 스토리지 게이트웨이의 콘솔로 이동한 후 액세스 권한을 제공합니다.

를 활성화하려면 지원 Amazon EC2 인스턴스에 배포한 게이트웨이에 대한 액세스

1. Amazon EC2 인스턴스용 로컬 콘솔에 로그인합니다. 지침은 을 참조하세요. [인스턴스에 연결합니다](#)의 Amazon EC2 사용 설명서.

다음 명령을 사용하여 EC2 인스턴스의 로컬 콘솔에 로그인할 수 있습니다.

```
ssh -i PRIVATE-KEY admin@INSTANCE-PUBLIC-DNS-NAME
```

Note

이 **#####** #입니다. pem Amazon EC2 인스턴스를 시작할 때 사용한 EC2 key pair 페어의 프라이빗 인증서를 포함하는 파일입니다. 자세한 내용은 단원을 참조하십시오. [키 페어에 맞는 퍼블릭 키 검색](#)의 Amazon EC2 사용 설명서.

이 **#####-PUBLIC-DNS-NAME**는 게이트웨이가 실행 중인 Amazon EC2 인스턴스의 퍼블릭 DNS (도메인 이름 시스템) 이름입니다. EC2 콘솔에서 Amazon EC2 인스턴스를 선택하고 설명 탭.

2. 프롬프트에서 를 입력합니다. **6 - Command Prompt**를 열려면 지원 Channel 콘솔.
3. **h**를 입력하여 AVAILABLE COMMANDS(사용 가능한 명령) 창을 엽니다.
4. 다음 중 하나를 수행하세요.
 - 게이트웨이가 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령창, 입력 **open-support-channel** Storage Gateway 대한 고객 지원 센터에 연결할 수 있습니다. 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. AWS. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
 - 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **open-support-channel**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway 에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. AWS. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

Note

채널 번호는 TCP/UDP(Transmission Control Protocol/User Datagram Protocol) 포트 번호가 아닙니다. 그 대신에 게이트웨이는 Storage Gateway 서버에 SSH (Secure Shell) (TCP 22) 로 접속하여 해당 연결에 지원 채널을 제공합니다.

5. 지원 채널이 설정되면 에 대한 지원 서비스 번호를 제공하십시오. 지원 그래서 지원 문제 해결 지원을 제공할 수 있습니다.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. Amazon Web Services 지원팀에서 Support 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **Enterexit**를 눌러 Storage Gateway 콘솔을
8. 콘솔 메뉴에 따라 Storage Gateway 인스턴스에서 로그아웃합니다.

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 없습니다.

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.

초기 기본값 재설정은 어떻게 수행합니까?

어플라이언스에서 초기 기본값 재설정을 수행해야 하는 경우, Storage Gateway 하드웨어 어플라이언스 팀에 지원을 요청하십시오.

Dell iDRAC 지원은 어디에서 받을 수 있습니까?

Dell PowerEdge R640 서버는 Dell iDRAC 관리 인터페이스와 함께 제공됩니다. 다음과 같이 하는 것이 좋습니다.

- iDRAC 관리 인터페이스를 사용하는 경우 기본 암호를 변경해야 합니다. iDRAC 자격 증명에 대한 자세한 내용은 단원을 참조하십시오. [Dell PowerEdge - iDRAC의 기본 사용자 이름 및 암호는 무엇입니까?](#)
- 보안 위반을 막기 위해 펌웨어가 최신 버전인지 확인합니다.
- iDRAC 네트워크 인터페이스를 일반(em) 포트로 이동하면 성능 문제가 발생하거나 어플라이언스가 정상적으로 작동하지 않을 수 있습니다.

하드웨어 기기 일련 번호를 찾을 수 없습니다.

하드웨어 기기의 일련 번호를 찾으려면 Hardware(하드웨어)아래와 같이 Storage Gateway 콘솔의 페이지

하드웨어 어플라이언스 지원을 받을 수 있는 곳

Storage Gateway 하드웨어 어플라이언스 지원에 문의하려면 [지원](#).

이 지원팀에서는 지원 채널을 활성화하여 게이트웨이 문제를 원격으로 해결하도록 요청할 수 있습니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어서 필요하지 않지만, 문제 해결 시에는 필요합니다. 다음 절차에 나온 것처럼 하드웨어 콘솔에서 지원 채널을 활성화할 수 있습니다.

에 대한 지원 채널을 열려면 AWS

1. 하드웨어 콘솔을 엽니다.
2. 다음과 같이 Open Support Channel(지원 채널 열기)를 선택합니다.

네트워크 연결 또는 방화벽 문제가 없는 경우 할당된 포트 번호가 30초 이내에 표시됩니다.

3. 포트 번호를 기록하고 지원.

파일 게이트웨이 문제 해결

VMware vSphere HA (고가용성) 를 실행할 때 Amazon CloudWatch 로그 그룹을 사용하여 파일 게이트웨이를 구성할 수 있습니다. 이 경우 파일 게이트웨이의 상태 및 파일 게이트웨이에서 발생한 오류에 대한 알림을 받습니다. 이러한 오류 및 상태 알림에 대한 정보는 CloudWatch Logs 로그에서 찾을 수 있습니다.

이 단원에서는 각 오류의 원인 및 상태 알림과 문제 해결 방법을 이해하는 데 도움이 되는 정보를 찾을 수 있습니다.

주제

- [오류: ObjectMissing](#)
- [알림: 재부팅](#)
- [알림: HardReboot](#)
- [알림: HealthCheckFailure](#)
- [알림: AvailabilityMonitorTest](#)
- [오류: RoleTrustRelationshipInvalid](#)
- [CloudWatch 지표를 이용한 문제 해결](#)

오류: ObjectMissing

당신은 얻을 수 있습니다ObjectMissing지정된 파일 게이트웨이 이외의 쓰기가 Amazon FSx에서 지정된 파일을 삭제할 때 오류가 발생합니다. 이후에 Amazon FSx로 업로드하거나 Amazon FSx에서 객체를 가져오는 작업이 모두 실패합니다.

ObjectMissing 오류를 해결하려면

1. SMB 클라이언트의 로컬 파일 시스템에 파일의 최신 복사본을 저장합니다 (3단계에서 이 파일 사본이 필요함).
2. SMB 클라이언트를 사용하여 파일 게이트웨이에서 파일을 삭제합니다.
3. SMB 클라이언트를 사용하여 1단계에서 저장한 파일의 최신 버전을 Amazon FSx에서 저장한 파일을 SMB 클라이언트를 사용하여 복사합니다. 파일 게이트웨이를 통해 이 작업을 합니다.

알림: 재부팅

게이트웨이 VM을 다시 시작할 때 재부팅 알림을 받을 수 있습니다. VM 하이퍼바이저 관리 콘솔 또는 Storage Gateway 콘솔을 사용하여 게이트웨이 VM을 다시 시작할 수 있습니다. 게이트웨이의 유지 관리 주기 동안 게이트웨이 소프트웨어를 사용하여 다시 시작할 수도 있습니다.

재부팅이 게이트웨이에서 구성된 [유지 관리 시작 시간](#) 10분 이내에 수행되는 경우 이 재부팅은 정상적인 현상일 수 있으며 문제의 징조가 아닙니다. 유지 관리 기간을 크게 벗어나 재부팅이 수행된 경우 게이트웨이가 수동으로 다시 시작되었는지 확인합니다.

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 트리거될 수 있습니다.

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 모니터링하기 위한 테스트 도중에도 발생합니다. 이 경우 HealthCheckFailure 알림이 예상됩니다.

Note

이 알림은 VMware 게이트웨이에만 적용됩니다.

AvailabilityMonitorTest 알림 없이 이 이벤트가 반복적으로 발생하면 VM 인프라(스토리지, 메모리 등)에 문제가 있는지 확인하십시오. 추가 지원이 필요한 경우 문의하십시오. 지원.

알림: AvailabilityMonitorTest

당신은 AvailabilityMonitorTest 본인의 경우 알림 [테스트 실행의 가용성 및 애플리케이션 모니터링](#) VMware vSphere HA 플랫폼에서 실행되는 게이트웨이의 시스템입니다.

오류: RoleTrustRelationshipInvalid

파일 공유에 대한 IAM 역할에 잘못 구성된 IAM 신뢰 관계가 있는 경우 (즉, IAM 역할이 이라는 Storage Gateway 보안 주체를 신뢰하지 않는 경우) 이 오류가 발생합니다. (storagegateway.amazonaws.com). 따라서 파일 게이트웨이는 파일 공유를 지원하는 S3 버킷에서 작업을 실행하기 위한 자격 증명을 가져올 수 없습니다.

RoleTrustRelationshipInvalid 오류를 해결하려면

- IAM 콘솔 또는 IAM API를 사용하여 다음을 포함합니다. `storagegateway.amazonaws.com` 파일 공유의 IAMRole에서 신뢰하는 보안 주체로 사용됩니다. IAM 역할에 대한 자세한 내용은 단원을 참조하십시오. [자습서: 액세스 권한 위임AWSIAM 역할을 사용하는 계정.](#)

CloudWatch 지표를 이용한 문제 해결

Storage Gateway 함께 Amazon CloudWatch 지표를 사용하여 문제를 해결하는 작업에 대한 다음 정보를 찾을 수 있습니다.

주제

- [디렉토리를 탐색할 때 게이트웨이가 느리게 반응합니다.](#)
- [게이트웨이가 응답하지 않는 경우](#)
- [Amazon FSx 파일 시스템에 파일이 표시되지 않습니다.](#)
- [게이트웨이가 Amazon FSx로 데이터를 전송하는 속도가 느립니다.](#)
- [게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생하는 경우](#)

디렉토리를 탐색할 때 게이트웨이가 느리게 반응합니다.

를 실행할 때 파일 게이트웨이가 느리게 반응하는 경우 `ls` 명령 또는 디렉토리 찾기, `IndexFetch`과 `IndexEviction` CloudWatch 지표:

- 만약 `IndexFetch`를 실행할 때 지표가 0보다 큼니다. `ls` 명령 또는 찾아보기 디렉터리, 파일 게이트웨이는 영향을 받은 디렉터리 콘텐츠에 대한 정보 없이 시작했으며 Amazon S3 액세스해야 했습니다. 해당 디렉터리의 콘텐츠를 나열하려는 후속 노력이 더 빨리 이루어져야 합니다.
- 만약 `IndexEviction` 지표가 0보다 크면 파일 게이트웨이가 해당 시점에 캐시에서 관리할 수 있는 항목 한계에 도달했음을 의미합니다. 이 경우 파일 게이트웨이는 새 디렉터를 나열하기 위해 가장 이전에 액세스한 디렉터리에서 일부 스토리지 공간을 비워야 합니다. 이 문제가 자주 발생하고 성능에 영향을 주는 경우 문의하십시오. 지원.

와 토론 지원 관련 Amazon FSx 파일 시스템의 내용과 사용 사례에 따라 성능을 향상시킬 수 있는 권장 조치에 대한 설명

게이트웨이가 응답하지 않는 경우

파일 게이트웨이가 응답하지 않는 경우 다음을 수행합니다.

- 최근 재부팅 또는 소프트웨어 업데이트가 있었다면 `IOWaitPercent` 지표를 확인하십시오. 이 지표는 처리되지 않은 디스크 I/O 요청이 있을 때 CPU가 유휴 상태인 시간의 백분율을 보여줍니다. 경우에 따라 이 값이 높고(10 이상) 서버가 재부팅되거나 업데이트된 후에 증가했을 수 있습니다. 이 경우 인덱스 캐시를 RAM으로 재구성함에 따라 느린 루트 디스크로 인해 파일 게이트웨이에 병목 현상이 발생할 수 있습니다. 루트 디스크에 더 빠른 물리적 디스크를 사용하여 이 문제를 해결할 수 있습니다.
- 만약 `MemUsedBytes` 메트릭은 다음과 거의 같거나 거의 같습니다. `MemTotalBytes` 지표를 선택하면 파일 게이트웨이에 사용 가능한 RAM이 부족해집니다. 파일 게이트웨이에 필요한 최소 RAM이 있는지 확인합니다. 이미 이를 확인했다면 워크로드 및 사용 사례에 따라 파일 게이트웨이에 RAM을 추가해 보십시오.

파일 공유가 SMB인 경우 파일 공유에 연결된 SMB 클라이언트 수 때문일 수도 있습니다. 지정된 시간에 연결된 클라이언트 수를 확인하려면 `SMBV(1/2/3)Sessions` 지표를 확인합니다. 연결된 클라이언트가 많은 경우 파일 게이트웨이에 RAM을 더 추가해야 할 수 있습니다.

Amazon FSx 파일 시스템에 파일이 표시되지 않습니다.

게이트웨이의 파일이 Amazon FSx 파일 시스템에 반영되지 않는 경우 `FilesFailingUpload` 지표. 지표가 일부 파일 업로드에 실패했다고 보고하는 경우 상태 알림을 확인합니다. 파일 업로드에 실패하면 게이트웨이가 문제에 대한 자세한 내용을 포함하는 상태 알림을 생성합니다.

게이트웨이가 Amazon FSx로 데이터를 전송하는 속도가 느립니다.

파일 게이트웨이에서 Amazon S3 데이터를 전송하는 속도가 느린 경우 다음을 수행합니다.

- 만약 `CachePercentDirty` 지표가 80 이상인 경우 파일 게이트웨이는 데이터를 Amazon S3 업로드할 수 있는 것보다 더 빨리 디스크에 데이터를 쓰고 있습니다. 파일 게이트웨이에서 업로드를 위한 대역폭을 늘리거나, 캐시 디스크를 하나 이상 추가하거나, 클라이언트 쓰기 속도를 늦추는 것이 좋습니다.
- 만약 `CachePercentDirty` 지표가 낮은 경우 `IOWaitPercent` 지표. 다음의 경우, `IOWaitPercent`가 10보다 큰 경우 파일 게이트웨이가 로컬 캐시 디스크의 속도로 인해 병목 현상이 발생할 수 있습니다. 캐시에 로컬 SSD(Solid State Drive) 디스크를 사용하는 것이 좋습니다. 추천 제품은 NVMe(NVM Express)입니다. 이러한 디스크를 사용할 수 없는 경우 성능 향상을 위해 별도의 물리적 디스크에서 여러 캐시 디스크를 사용해 보십시오.

게이트웨이 백업 작업이 실패하거나 게이트웨이에 쓸 때 오류가 발생하는 경우

파일 게이트웨이 백업 작업이 실패하거나 파일 게이트웨이에 쓸 때 오류가 발생하는 경우 다음을 수행합니다.

- 만약 CachePercentDirty 지표가 90% 이상이면 캐시 디스크에 사용 가능한 공간이 부족하기 때문에 파일 게이트웨이가 디스크에 대한 새 쓰기를 허용할 수 없습니다. Amazon FSx 또는 Amazon S3에 파일 게이트웨이가 업로드하는 속도를 확인하려면 CloudBytesUploaded 지표. 해당 메트릭과 비교 WriteBytesMetric - 클라이언트가 파일 게이트웨이에 파일을 쓰는 속도를 보여 줍니다. 파일 게이트웨이가 Amazon FSx 또는 Amazon S3에 업로드할 수 있는 것보다 빨리 쓰는 경우 최소한 백업 작업의 크기를 처리할 수 있도록 캐시 디스크를 더 추가합니다. 또는 업로드 대역폭을 늘립니다.
- 백업 작업이 실패하지만 CachePercentDirty 지표가 80% 미만인 경우 파일 게이트웨이가 클라이언트 측 세션 제한 시간에 도달했을 수 있습니다. SMB의 경우 PowerShell 명령 Set-SmbClientConfiguration -SessionTimeout 300을 사용하여 이 제한 시간을 늘릴 수 있습니다. 이 명령을 실행하면 이 제한 시간이 300초로 설정됩니다.

NFS의 경우 소프트 마운트 대신 하드 마운트를 사용하여 클라이언트를 마운트해야 합니다.

고가용성 상태 알림

VMware vSphere HA(고가용성) 플랫폼에서 게이트웨이를 실행할 때 상태 알림을 받을 수 있습니다. 상태 알림에 대한 자세한 내용은 [고가용성 관련 문제를 해결합니다](#). 단원을 참조하십시오.

고가용성 관련 문제를 해결합니다.

가용성 문제가 발생할 경우 수행할 작업에 대한 다음 정보를 찾을 수 있습니다.

주제

- [Health 알림](#)
- [지표](#)

Health 알림

VMware vSphere HA에서 게이트웨이를 실행하면 모든 게이트웨이가 구성된 Amazon CloudWatch 로그 그룹에 다음과 같은 상태 알림을 생성합니다. 이러한 알림은 AvailabilityMonitor라는 로그 스트림으로 이동합니다.

주제

- [알림: 재부팅](#)
- [알림: HardReboot](#)
- [알림: HealthCheckFailure](#)
- [알림: AvailabilityMonitorTest](#)

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 트리거될 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 모니터링하기 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. 지원.

알림: AvailabilityMonitorTest

VMware vSphere HA의 게이트웨이의 경우 AvailabilityMonitorTest 본인의 경우 [알림 테스트 실행의 가용성 및 애플리케이션 모니터링](#) VMware의 시스템.

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 복구를 위한 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 Gateway 하이퍼바이저에서 생성한 스냅샷 또는 Amazon EC2 Amazon 머신 이미지 (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

- [예기치 않은 가상 시스템 종료에서 복구](#)
- [고장난 캐시 디스크에서 데이터 복구](#)
- [액세스할 수 없는 데이터 센터에서 데이터 복구](#)

예기치 않은 가상 시스템 종료에서 복구

예를 들어 정전으로 인해 VM이 예기치 않게 종료된 경우, 게이트웨이에 접속할 수 없습니다. 전원과 네트워크 연결이 복구되면 게이트웨이에 접속할 수 있고 게이트웨이가 정상적으로 작동하기 시작합니다. 다음은 이 시점에 수행할 수 있는 데이터 복구 지원 절차입니다.

- 정전으로 인해 네트워크 연결에 문제가 발생하면 그 문제를 해결할 수 있습니다. 네트워크 연결을 테스트하는 방법에 대한 정보는 [게이트웨이 엔드포인트에 대한 FSx 파일 게이트웨이 게이트웨이 연결 테스트](#) 섹션을 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 해당 되는 상황과 관련된 단원을 참조하십시오.

고장난 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.

자세한 내용은 [고장난 캐시 디스크에서 데이터 복구](#) 섹션을 참조하세요.

액세스할 수 없는 데이터 센터에서 데이터 복구

게이트웨이 또는 데이터 센터에 대한 액세스가 어떤 이유로 차단되는 경우 데이터를 다른 데이터 센터의 다른 게이트웨이로 복구하거나 Amazon EC2 인스턴스에 호스팅되어 있는 게이트웨이로 복구할 수 있습니다. 따라서 다른 데이터 센터에 액세스할 수 없다면 Amazon EC2 인스턴스에서 게이트웨이를 생성하도록 권장합니다. 생성 방법은 데이터를 복구하는 게이트웨이 유형에 따라 다릅니다.

액세스할 수 없는 데이터 센터의 파일 게이트웨이에서 데이터를 복구하려면

파일 게이트웨이일 때는 새로운 파일 공유를 복구할 데이터가 저장되어 있는 Amazon S3 버킷으로 매핑합니다.

1. Amazon EC2 호스트에서 새로운 파일 게이트웨이를 생성하여 활성화합니다. 자세한 정보는 [Amazon EC2 호스트에 파일 게이트웨이 배포](#)를 참조하십시오.
2. 생성한 EC2 게이트웨이에서 새로운 파일 공유를 생성합니다. 자세한 내용은 단원을 참조하십시오. [파일 공유 생성](#).
3. 파일 공유를 클라이언트에 마운트한 후 복구할 데이터가 저장된 S3 버킷에 매핑합니다. 자세한 내용은 단원을 참조하십시오. [파일 공유 마운트 및 사용](#).

추가 Storage Gateway 리소스

이 단원에서는 에 대한 정보를 볼 수 있습니다.AWS게이트웨이를 설정하거나 관리하는 데 도움이 되는 타사 소프트웨어, 도구 및 리소스, 그리고 Storage Gateway 할당량에 대한 정보를 얻을 수 있습니다.

주제

- [호스트 설정](#)
- [게이트웨이 활성화 키 받기](#)
- [사용AWS Direct ConnectStorage Gateway](#)
- [게이트웨이에 연결](#)
- [Storage Gateway 리소스 및 리소스 ID 이해](#)
- [Storage Gateway 리소스 태그 지정](#)
- [오픈 소스 구성 요소 작업AWS Storage Gateway](#)
- [할당량](#)

호스트 설정

주제

- [Storage Gateway 게이트웨이용 VMware 구성](#)
- [게이트웨이 VM 시간 동기화](#)
- [Amazon EC2 호스트에 파일 게이트웨이 배포](#)

Storage Gateway 게이트웨이용 VMware 구성

Storage Gateway를 구성할 때 VM 시간을 호스트 시간과 동기화하고, 스토리지를 프로비저닝할 때 반 가상화된 디스크 컨트롤러를 사용하도록 VM을 구성하고, 게이트웨이 VM을 지원하는 인프라 계층에서 발생하는 장애에 대한 보호를 제공해야 합니다.

주제

- [VM 시간을 호스트 시간과 동기화](#)
- [VMware 고가용성으로 Storage Gateway 사용](#)

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. 그 다음 호스트 시간을 확인하고, 필요한 경우 호스트 시간을 설정하고 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성합니다.

Important

VM 시간을 호스트 시간과 동기화하려면 게이트웨이를 성공적으로 활성화해야 합니다.

VM 시간을 호스트 시간과 동기화하려면

1. VM 시간을 구성합니다.

- a. vSphere 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.

그러면 Virtual Machine Properties(가상 머신 속성) 대화 상자가 열립니다.

- b. 옵션 탭을 선택하고 옵션 목록에서 VMware 도구를 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 클럭을 구성하지 않았다면 다음 절차에 따라 설정하고 NTP 서버와 동기화합니다.

- a. VMware vSphere 클라이언트의 왼쪽 창에서 vSphere 호스트 노드를 선택한 후 구성 탭을 선택합니다.
- b. Select시간 구성의소프트웨어패널을 선택한 다음속성링크

그러면 Time Configuration(시간 구성) 대화 상자가 나타납니다.

- c. 날짜 및 시간 창에서 날짜 및 시간을 설정합니다.
- d. 호스트가 자체 시간을 자동으로 NTP 서버와 동기화하도록 구성합니다.
 - i. 선택옵션의시간 구성대화 상자를 누른 다음NTP 데몬 (ntpd) 옵션대화 상자에서NTP 설정왼쪽 창에서
 - ii. 추가를 선택하여 새 NTP 서버를 추가합니다.
 - iii. NTP 서버 추가 대화 상자에서 NTP 서버의 IP 주소 또는 전체 주소 도메인 이름을 입력한 후 확인을 선택합니다.

다음 예시와 같이 pool.ntp.org를 사용할 수 있습니다.

- iv. NTP 데몬(ntpd) 옵션 대화 상자에서 왼쪽 창에 있는 일반을 선택합니다.
- v. Service Commands(서비스 명령) 창에서 Start(시작)를 선택하여 해당 서비스를 시작합니다.

이 NTP 서버 참조를 변경하거나 나중에 하나를 더 추가하는 경우, 새 서버를 사용하려면 해당 서비스를 다시 시작해야 한다는 점에 유의하십시오.

- e. 확인을 선택하여 NTP 데몬(ntpd) 옵션 대화 상자를 닫습니다.
- f. 확인을 선택하여 Time Configuration(시간 구성) 대화 상자를 닫습니다.

VMware 고가용성으로 Storage Gateway 사용

VMware 고가용성(HA)은 게이트웨이 VM을 지원하는 인프라 계층의 장애로부터 보호할 수 있는 vSphere의 구성 요소입니다. VMware HA는 클러스터로 구성된 호스트를 여러 개 사용함으로써 게이트웨이 VM을 실행 중인 호스트에 장애가 발생하면 게이트웨이 VM이 클러스터 내의 다른 호스트에서 자동으로 다시 시작하는 방법으로 보호 기능을 제공합니다. VMware HA에 대한 자세한 내용은 단원을 참조하십시오. [VMware HA: 개념 및 모범 사례](#) VMware 웹 사이트의 내용을 참조하십시오.

VMware HA에서 Storage Gateway 사용하려면 다음 작업을 수행하는 것이 좋습니다.

- VMware ESX 배포 .ova 클러스터의 호스트 한 곳에만 Storage Gateway VM이 포함된 다운로드 가능 패키지는 아닙니다.
- .ova 패키지를 배포할 때 호스트 한 곳에 대해 로컬이 아닌 데이터 스토어를 선택합니다. 그 대신에 클러스터의 모든 호스트에 액세스할 수 있는 데이터 스토어를 사용합니다. 호스트에 대해 로컬인 데이터 스토어를 선택하였는데 호스트에 장애가 생긴 경우에는 데이터 원본이 클러스터 내 기타 호스트에 액세스할 수 없고 다른 호스트에 대한 장애 조치가 성공하지 못할 수 있습니다.
- 클러스터링의 경우, .ova 패키지를 클러스터에 배포한다면 프롬프트 메시지에 따라 호스트를 선택합니다. 또는 클러스터의 호스트에 직접 배포할 수도 있습니다.

게이트웨이 VM 시간 동기화

VMware ESXi에 배포한 게이트웨이의 경우, 하이퍼바이저 호스트 시간을 설정하고 호스트에 VM 시간을 동기화하는 것만으로도 시간 오차를 방지하는 데 충분합니다. 자세한 정보는 [VM 시간을 호스트 시간과 동기화](#)를 참조하십시오. Microsoft Hyper-V에 배포한 게이트웨이의 경우, 다음 절차에 따라 VM의 시간을 주기적으로 점검해야 합니다.

하이퍼바이저 게이트웨이 VM의 시간을 보고 네트워크 시간 프로토콜(NTP) 서버와 동기화하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
 - Linux 커널 기반 가상 머신(KVM)용 로컬 콘솔 로그인에 대한 자세한 내용은 [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
2. 온Storage Gateway 구성기본 메뉴4...에 대한 시스템 시간 관리.
3. 온시스템 시간 관리메뉴, 입력1...에 대한 시스템 시간 보기 및 동기화.
4. 그 결과가 VM의 시간을 NTP 시간에 동기화해야 하는 것으로 나타나면 **y**을 입력합니다. 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.

Amazon EC2 호스트에 파일 게이트웨이 배포

Amazon Elastic Compute Cloud (Amazon EC2) 인스턴스에서 파일 게이트웨이를 배포하고 활성화할 수 있습니다. 파일 게이트웨이 Amazon Machine Image(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

Amazon EC2 인스턴스에 게이트웨이를 배포하려면

1. 호스트 플랫폼 선택 페이지에서 Amazon EC2를 선택합니다.
2. 인스턴스 시작을 선택하여 스토리지 게이트웨이 EC2 AMI를 시작합니다. 인스턴스 유형을 선택할 수 있는 Amazon EC2 콘솔로 리디렉션됩니다.
3. 온단계 2: 인스턴스 유형 선택페이지에서 인스턴스의 하드웨어 구성을 선택합니다. Storage Gateway는 특정 최소 요구 사항을 충족하는 인스턴스 유형에서 지원됩니다. 게이트웨이가 제대로 작동하기 위한 최소 요건을 만족하는 m4.xlarge 인스턴스 유형으로 시작하는 것이 좋습니다. 자세한 정보는 [온프레미스 VM에 대한 하드웨어 요구 사항](#)을 참조하십시오.

필요하다면 시작한 후 인스턴스 크기를 조정할 수 있습니다. 자세한 내용은 단원을 참조하십시오. [인스턴스 크기 조정](#)의 Linux 인스턴스용 Amazon EC2 사용 설명서.

Note

특히 i3 EC2 같은 특정한 인스턴스 유형은 NVMe SSD 디스크를 사용합니다. 이러한 경우 파일 게이트웨이를 시작하거나 중지할 때 문제가 발생할 수 있습니다. 예를 들어 캐시에서 데이터가 손실될 수 있습니다. 모니터링CachePercentDirtyAmazon CloudWatch 지표를 선택하면 해당 파라미터가 다음과 같은 경우에만 시스템을 시작하거나 중단하십시오. 0. 게이트웨이의 지표 모니터링에 대한 자세한 내용은 단원을 참조하십시오. [Storage Gateway 지표 및 차원](#)CloudWatch 설명서에 나와 있습니다. Amazon EC2 인스턴스 유형 요구 사항에 대한 자세한 내용은 단원을 참조하십시오. [the section called "Amazon EC2 인스턴스 유형에 대한 요구 사항"](#).

4. [다음: 권한(Next: 인스턴스 세부 정보 구성.

5. 온단계 3: 인스턴스 세부 정보 구성 페이지에서 값을 선택합니다. 퍼블릭 IP 자동 할당. 퍼블릭 인터넷에서 인스턴스에 액세스할 수 있어야 하는 경우 퍼블릭 IP 자동 할당이 활성화로 설정되어 있는지 확인합니다. 인터넷에서 인스턴스에 액세스할 수 없어야 하는 경우 퍼블릭 IP 자동 할당에 대해 비활성화를 선택합니다.
6. IAM 역할을 선택합니다. AWS Identity and Access Management 게이트웨이에 사용할 (IAM) 역할입니다.
7. [다음: 권한(Next: 스토리지 추가를 선택합니다.
8. 온단계 4: 스토리지 추가 페이지, 선택 새 볼륨 추가 파일 게이트웨이 인스턴스에 스토리지를 추가합니다. 캐시 스토리지에 구성할 Amazon EBS 볼륨이 최소 한 개 필요합니다.

권장 디스크 크기: 캐시 (최소) 150GiB 및 캐시 (최대) 64TiB

9. 온단계 5: 태그 추가 페이지에서 인스턴스에 선택적 태그를 추가할 수 있습니다. 다음을 선택합니다. 보안 그룹 구성을 선택합니다.
10. 온단계 6: 보안 그룹 구성 페이지에서 인스턴스에 도달할 특정 트래픽에 방화벽 규칙을 추가합니다. 새 보안 그룹을 생성하거나 기존 보안 그룹을 선택할 수 있습니다.

Important

NFS 클라이언트는 Storage Gateway 정품 인증과 SSH (Secure Shell) 액세스 포트 외에도 추가 포트에 대한 액세스 권한이 필요합니다. 자세한 내용은 [네트워크 및 방화벽 요구 사항](#) 섹션을 참조하세요.

11. 검토 및 시작을 선택하여 구성을 검토합니다.
12. 온단계 7: 인스턴스 시작 검토 페이지, 선택 시작.
13. 기존 키 페어 선택 또는 새 키 페어 생성 대화 상자에서 기존 키 페어 선택을 선택한 후 설정할 때 만든 키 페어를 선택합니다. 준비가 되었으면 승인 상자를 선택한 후 인스턴스 시작을 선택합니다.

확인 페이지를 통해 인스턴스가 시작 중임을 알 수 있습니다.

14. 인스턴스 보기(View Instances)를 선택하여 확인 페이지를 닫고 콘솔로 돌아갑니다. 인스턴스 (Instances) 화면에서 인스턴스의 상태를 볼 수 있습니다. 인스턴스를 시작하는 데 약간 시간이 걸립니다. 인스턴스를 시작하면 초기 상태는 대기 중입니다. 인스턴스는 시작한 후 상태가 running(실행 중)으로 바뀌고 퍼블릭 DNS 이름을 받습니다.
15. 인스턴스를 선택하고 다음 위치에 퍼블릭 IP 주소를 적어 둡니다. 설명태그를 지정하고 연결 AWS 게이트웨이 설정을 계속하려면 Storage Gateway 콘솔에서 페이지를 참조하십시오.

Storage Gateway 콘솔을 사용하거나 쿼리하여 파일 게이트웨이를 시작하는 데 사용할 AMI ID를 확인할 수 있습니다.AWS Systems Manager파라미터 저장소

AMI ID를 확인하려면

1. 에 로그인합니다.AWS Management Console에서 Storage Gateway 콘솔을 엽니다.<https://console.aws.amazon.com/storagegateway/home>.
2. 게이트웨이를 선택하고 파일 게이트웨이를 선택한 후 다음을 선택합니다.
3. Choose host platform(호스트 플랫폼 선택) 페이지에서 Amazon EC2를 선택합니다.
4. 선택인스턴스 실행Storage Gateway EC2 AMI를 시작합니다. EC2 커뮤니티 AMI 페이지로 리디렉션됩니다. 이 페이지에서는 에 대한 AMI ID를 볼 수 있습니다.AWSURL의 지역입니다.

또는 Systems Manager 파라미터 저장소를 쿼리할 수 있습니다. 이AWS CLI또는 네임스페이스 아래의 Systems Manager 퍼블릭 파라미터를 쿼리하는 Storage Gateway API/aws/service/storagegateway/ami/FILE_S3/latest. 예를 들어 다음 CLI 명령을 사용하면 현재 AMI의 ID가 반환됩니다.AWS리전.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/FILE_S3/latest
```

이 CLI 명령은 다음과 비슷한 출력을 반환합니다.

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 4,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/FILE_FSX/latest",
    "Name": "/aws/service/storagegateway/ami/FILE_S3/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

게이트웨이 활성화 키 받기

게이트웨이 활성화 키를 받으려면 게이트웨이 VM에 대한 웹 요청을 생성합니다. 그러면 게이트웨이 VM이 활성화 키가 포함된 리디렉션을 반환합니다. 활성화 키는 ActivateGateway API 작업에 대

한 파라미터 중 하나로 전달되어 게이트웨이 구성을 지정합니다. 자세한 내용은 단원을 참조하십시오. [ActivateGateway](#)의 Storage Gateway API 참조.

게이트웨이 VM에 대해 생성한 요청에는 AWS 활성화가 발생하는 지역입니다. 응답에 리디렉션이 반환한 URL에는 activationkey라는 쿼리 문자열 파라미터가 포함되어 있습니다. 이 쿼리 문자열 파라미터는 정품 인증 키입니다. 쿼리 문자열의 형식은 다음과 같습니다. `http://gateway_ip_address/?activationRegion=activation_region`.

주제

- [AWS CLI](#)
- [Linux\(bash/zsh\)](#)
- [Microsoft Windows PowerShell](#)

AWS CLI

AWS CLI를 아직 설치하지 않았다면 이를 설치하고 구성해야 합니다. 이를 위해 AWS Command Line Interface 사용 설명서에서 다음 지침을 따르세요.

- [다음 설치AWS Command Line Interface](#)
- [구성AWS Command Line Interface](#)

다음 예에서는 curl을 사용하는 방법을 보여줍니다. AWS CLI HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고 활성화 키를 받습니다.

```
wget 'ec2_instance_ip_address/?activationRegion=eu-west-2' 2>&1 | \
grep -i location | \
grep -i key | \
cut -d=' ' -f2 | \
cut -d'&' -f1
```

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 "$activation_region" ]]; then
    echo "Usage: get-activation-key ip_address activation_region"
    return 1
fi
if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
else
    return 1
fi
}

```

Microsoft Windows PowerShell

다음 예제는 Microsoft Windows PowerShell을 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```

function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion" -MaximumRedirection 0 -ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=( [A-Z0-9-]+ )"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}

```

사용AWS Direct ConnectStorage Gateway

AWS Direct ConnectAmazon Web Services 클라우드에 내부 네트워크를 연결합니다. 를 사용하여 AWS Direct ConnectStorage Gateway를 사용하면 고처리량 워크로드 요구 사항을 충족하기 위한 연결을 설정하여 온프레미스 게이트웨이와 간에 전용 네트워크 연결을 제공할 수 있습니다.AWS.

Storage Gateway 퍼블릭 엔드포인트를 사용합니다. 함께AWS Direct Connect연결이 설정되면 트래픽을 Storage Gateway 엔드포인트로 라우팅할 수 있는 퍼블릭 가상 인터페이스를 생성할 수 있습니다. 퍼블릭 가상 인터페이스는 네트워크 경로에서 인터넷 서비스 제공업체를 우회합니다. Storage Gateway 서비스 퍼블릭 엔드포인트가 동일할 수 있음AWS지역으로AWS Direct Connect위치 또는 다른 위치에 있을 수 있습니다.AWS리전.

다음 그림에 예가 나와 있습니다.AWS Direct ConnectStorage Gateway 함께 작동합니다.

다음 절차에서는 생성된 게이트웨이가 제대로 작동 중이라고 가정합니다.

를 사용하려면AWS Direct ConnectStorage Gateway

1. 생성 및 설정AWS Direct Connect온프레미스 데이터 센터와 Storage Gateway Endpoint 간 연결 연결을 생성하는 방법에 대한 자세한 내용은 단원을 참조하십시오.[시작하기AWS Direct Connect](#)의AWS Direct Connect사용 설명서.
2. 온프레미스 Storage Gateway 어플라이언스를AWS Direct Connect라우터
3. 퍼블릭 가상 인터페이스를 생성하고 이에 따라 온프레미스 라우터를 구성합니다. 자세한 내용은 단원을 참조하십시오.[가상 인터페이스 생성](#)의AWS Direct Connect사용 설명서.

에 대한 자세한 내용은AWS Direct Connect를 참조하십시오.[란 무엇입니까?AWS Direct Connect?](#)의AWS Direct Connect사용 설명서.

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 얻을 수도 있습니다. 게이트웨이의 IP 주소를 얻는 방법은 다음 중 하나를 참조하십시오.

- VMware 호스트: [VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- HyperV 호스트: [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- Linux 커널 기반 가상 머신(KVM) 호스트: [Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- EC2 호스트: [Amazon EC2 호스트에서 IP 주소 얻기](#)

IP 주소를 찾았으면 적어 둡니다. 그런 다음 Storage Gateway Console로 돌아가서 콘솔에 IP 주소를 입력합니다.

Amazon EC2 호스트에서 IP 주소 얻기

게이트웨이가 배포된 Amazon EC2 인스턴스의 IP 주소를 얻으려면 EC2 인스턴스의 로컬 콘솔에 로그인합니다. 그런 다음 콘솔 페이지 상단에서 IP 주소를 얻습니다. 지침은 단원을 참조하세요.

Amazon EC2 관리 콘솔에서도 IP 주소를 얻을 수 있습니다. 활성화에는 퍼블릭 IP 주소를 사용하는 것이 좋습니다. 퍼블릭 IP 주소를 얻으려면 절차 1을 사용합니다. 그 대신 탄력적 IP 주소를 사용하려면 절차 2를 사용합니다.

절차 1: 퍼블릭 IP 주소를 사용하여 게이트웨이에 연결하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 퍼블릭 IP 주소를 적어 둡니다. 이 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 IP 주소를 입력합니다.

활성화에 탄력적 IP 주소를 사용하려면 다음 절차를 사용합니다.

절차 2: 탄력적 IP 주소를 사용하여 게이트웨이에 연결하려면

1. <https://console.aws.amazon.com/ec2/>에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 탄력적 IP 값을 적어 둡니다. 이 탄력적 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 탄력적 IP 주소를 입력합니다.
4. 게이트웨이가 활성화되면 방금 활성화한 게이트웨이를 선택한 후 하단 패널에서 VTL 디바이스 탭을 선택합니다.
5. 모든 VTL 디바이스의 이름을 얻습니다.
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 게이트웨이가 EC2 인스턴스의 탄력적 IP 주소를 사용하여 연결되었습니다.

Storage Gateway 리소스 및 리소스 ID 이해

Storage Gateway에서 기본 리소스는 게이트웨이 다른 리소스 유형에는 다음이 포함됩니다. 음량, 가상 테이프, iSCSI 대상, 및 vtl 디바이스. 이 유형들은 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

다음 표에 나와 있는 것처럼 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름(ARN)이 연결되어 있습니다.

리소스 유형	ARN 형식
Gateway ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i>
파일 공유 ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :share/ <i>share-id</i>
Volume ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /volume/ <i>volume-id</i>
테이프 ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :tape/ <i>tapebarcode</i>
대상 ARN(iSCSI 대상)	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSITarget</i>
VTL 디바이스 ARN	arn:aws:storagegateway: <i>region</i> : <i>account-id</i> :gateway/ <i>gateway-id</i> /device/ <i>vtldevice</i>

Storage Gateway EC2 인스턴스, EBS 볼륨 및 스냅샷 사용을 지원합니다. 이러한 리소스는 Storage Gateway 게이트웨이에서 사용되는 Amazon EC2 리소스입니다.

리소스 ID 작업

리소스를 생성하면 Storage Gateway에서 리소스에 고유 리소스 ID가 할당됩니다. 이 리소스 ID는 리소스 ARN의 일부입니다. 리소스 ID는 리소스 식별자 다음에 하이픈, 그리고 문자 및 숫자의 고유 조합(8자리)이 오는 형식을 취합니다. 예를 들어 게이트웨이 ID가 sgw-12A3456B와 같은 형식이라면 여기

에서 `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 리소스 ID는 대문자입니다. 그러나 Amazon EC2 API에서 이러한 리소스 ID를 사용하는 경우 Amazon EC2는 리소스 ID가 소문자일 것으로 예상합니다. EC2 API에서 사용할 수 있도록 리소스 ID를 소문자로 변경해야 합니다. 예를 들어 Storage Gateway에서 볼륨의 ID는 `vol-1122AABB`일 수 있습니다. 이 ID를 EC2 API에서 사용하는 경우, `vol-1122aabb`로 변경해야 합니다. 그렇게 하지 않으면 EC2 API가 예상 대로 작동하지 않을 수 있습니다.

Important

게이트웨이 볼륨에서 생성한 Storage Gateway 볼륨 및 Amazon EBS 스냅샷의 ID는 더 긴 형식으로 변경될 예정입니다. 2016년 12월부터 모든 신규 볼륨 및 스냅샷은 문자 17개로 구성된 문자열로 생성됩니다. 2016년 4월부터 이와 같이 더 긴 ID를 사용할 수 있으므로 이러한 새 형식으로 시스템을 테스트할 수 있습니다. 자세한 내용은 [더 긴 EC2 및 EBS 리소스 ID](#) 단원을 참조하십시오.

더 긴 볼륨 ID 형식을 지닌 볼륨 ARN의 예:

```
arn:aws:storagegateway:us-west-2:111122223333:gateway/sgw-12A3456B/volume/vol-1122AABBCCDDEEFFG.
```

더 긴 ID 형식을 지닌 스냅샷 ID의 예: `snap-78e226633445566ee`

자세한 내용은 단원을 참조하십시오. [공지 사항: Heads-up — Longer Storage Gateway 볼륨 및 스냅샷 IDs.](#)

Storage Gateway 리소스 태그 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.

예컨대 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 게이트

웨이 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.

게이트웨이에 대해 태그를 사용하여 리소스에 대한 액세스를 제어할 수 있습니다. 이를 위한 자세한 방법은 [태그를 사용하여 게이트웨이 및 리소스에 대한 액세스 제어](#) 섹션을 참조하세요.

태그에는 의미가 없으며 문자열로 해석됩니다.

태그에 적용되는 제한은 다음과 같습니다.

- 태그 키와 값은 대/소문자를 구분합니다.
- 각 리소스의 최대 태그 수는 50입니다.
- 태그 키는 `aws:`로 시작할 수 없습니다. 이 접두사는 에 예약되어 있습니다.AWS를 사용합니다.
- 키 속성에 유효한 문자는 UTF-8 문자 및 숫자, 공백, 특수 문자(+ - = . _ : / @)입니다.

태그 작업하기

Storage Gateway 콘솔, Storage Gateway API 또는 [CLI \(Storage Gateway 명령줄 인터페이스\)](#). 다음 절차에서는 콘솔에서 태그를 추가, 편집, 삭제하는 방법을 안내합니다.

태그를 추가하려면

1. 에서 Storage Gateway 콘솔을 엽니다.<https://console.aws.amazon.com/storagegateway/home>.
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. 에서 Storage Gateway 콘솔을 엽니다. <https://console.aws.amazon.com/storagegateway/home>.
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. 에서 Storage Gateway 콘솔을 엽니다. <https://console.aws.amazon.com/storagegateway/home>.
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.

다음 사항도 참조하세요.

[태그를 사용하여 게이트웨이 및 리소스에 대한 액세스 제어](#)

오픈 소스 구성 요소 작업AWS Storage Gateway

이 단원에서는 Storage Gateway 기능을 제공하는 데 사용하는 타사 도구와 라이선스에 대한 정보를 제공합니다.

주제

- [Storage Gateway 게이트웨이용 오픈 소스 구성 요소](#)

- [Amazon FSx 파일 게이트웨이용 오픈 소스 구성 요소](#)

Storage Gateway 게이트웨이용 오픈 소스 구성 요소

블록 게이트웨이, 테이프 게이트웨이 및 Amazon S3 File Gateway에 대한 기능을 제공하는 데 여러 타사 도구 및 라이선스가 사용됩니다.

다음 링크를 사용하여 에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드를 다운로드합니다. AWS Storage Gateway 소프트웨어:

- VMware ESXi에 배포된 게이트웨이의 경우: [sources.tar](#)
- Microsoft Hyper-V에 배포된 게이트웨이의 경우: [sources_hyperv.tar](#)
- Linux 커널 기반 가상 머신 (KVM) 에 배포된 게이트웨이의 경우: [sources_KVM.tar](#)

이 제품은 OpenSSL 도구 키트 (에서 사용하기 위해 OpenSSL 프로젝트가 개발한 소프트웨어를 포함합니다. <http://www.openssl.org/>). 모든 종속 타사 도구에 대한 관련 라이선스는 단원을 참조하십시오. [타사 라이선스](#).

Amazon FSx 파일 게이트웨이용 오픈 소스 구성 요소

Amazon FSx 파일 게이트웨이 (FSx 파일 게이트웨이) 기능을 제공하는 데 여러 타사 도구 및 라이선스가 사용됩니다.

다음 링크를 통해 FSx File Gateway 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드를 다운로드합니다.

- 2021년 7월 7일 Amazon FSx 파일 게이트웨이 2021년 7월 7일 릴리스의 경우 [sgw-파일-fsx-smb 오픈 소스.tgz](#)
- 아마존 FSx 파일 게이트웨이 2021-04-06 릴리스의 경우: [SGW 파일-fsx-SMB-20210406-오픈 소스.tgz](#)

이 제품은 OpenSSL 도구 키트 (에서 사용하기 위해 OpenSSL 프로젝트가 개발한 소프트웨어를 포함합니다. <http://www.openssl.org/>). 모든 종속 타사 도구에 대한 관련 라이선스는 다음 링크를 참조하십시오.

- 2021년 7월 7일 Amazon FSx 파일 게이트웨이 2021년 7월 7일 릴리스의 경우 [타사 라이선스](#).
- 아마존 FSx 파일 게이트웨이 2021-04-06 릴리스의 경우: [타사 라이선스](#).

할당량

파일 시스템에 대한 할당량

다음 표에는 파일 시스템에 대한 할당량이 나와 있습니다.

리소스	파일 시스템당 제한
최대 태그 수	50
자동 백업을 위한 최대 보존 기간	90일
계정당 단일 대상 리전으로 진행된 최대 백업 사본 요청 수입니다.	5
최소 저장 용량, SSD 파일 시스템	32GiB
최소 저장 용량, HDD 파일 시스템	2,000GiB
최대 저장 용량, SSD 및 HDD	64TiB
최소 처리량	8Mbps
최대 처리량 용량	2,048Mbps
최대 파일 공유 개수	100,000건

게이트웨이에 권장되는 로컬 디스크 크기

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)	필요한 다른 로컬 디스크
FSx 파일 게이트웨이	150GiB	64TiB	—

Note

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

API 참조

콘솔의 사용 외에도, AWS Storage Gateway API를 사용하여 게이트웨이를 프로그래밍 방식으로 구성 및 관리할 수 있습니다. 이 섹션은 AWS Storage Gateway 운영, 인증 요청 확인 및 오류 처리를 설명합니다. Storage Gateway에 사용할 수 있는 리전 및 엔드포인트에 대한 자세한 내용은 [AWS Storage Gateway 엔드포인트 및 할당량](#)의 AWS 일반 참조를 참조하십시오.

Note

도 사용할 수 있습니다. AWSStorage Gateway를 사용하여 애플리케이션을 개발할 때 SD 이 AWSJava, .NET 및 PHP용 SDK는 기본 Storage Gateway API를 포함하여 프로그래밍 작업을 간소화합니다. SDK 라이브러리 다운로드에 대한 정보는 [샘플 코드 라이브러리](#) 단원을 참조하십시오.

주제

- [AWS Storage Gateway 필수 요청 헤더](#)
- [요청에 서명하기](#)
- [오류 응답](#)
- [작업](#)

AWS Storage Gateway 필수 요청 헤더

이 단원에서는 모든 POST 요청과 함께 전송해야 하는 필수 헤더에 대해 설명합니다. AWS Storage Gateway. 호출하려는 작업을 포함하는 요청에 대한 핵심 정보, 요청 날짜 및 요청 전송자의 권한을 부여함을 나타내는 정보를 식별할 HTTP 헤더를 포함해야 합니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음은 [ActivateGateway](#) 작업에서 사용하는 헤더의 예입니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

다음은 POST 요청과 함께 포함해야 하는 헤더입니다.AWS Storage Gateway. 아래에 표시된 헤더는 “x-amz”로 시작합니다.AWS-지정 헤더입니다. 나머지 헤더는 HTTP 트랜잭션에 사용되는 공통 헤더입니다.

헤더	설명
Authorization	<p>권한 부여 헤더는 활성화하는 요청에 대한 몇 가지 정보를 포함합니다.AWS Storage Gateway를 사용하여 요청이 요청자에게 유효한 작업인지 확인합니다. 이 헤더의 형식은 다음과 같습니다(가독성을 높이기 위해 줄 바꿈 추가).</p> <div data-bbox="472 930 1507 1209" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= <i>CalculatedSignature</i></pre> </div> <p>이전 구문에서는 <i>YourAccessKey</i>, 연도, 월, 일(<i>yyyymmdd</i>), 해당 리전 및 <i>CalculatedSignature</i>를 지정합니다. 권한 부여 헤더의 형식은 다음 요구 사항에 따라 결정됩니다.AWSV4 서명 프로세스. 서명 관련 세부 정보는 요청에 서명하기 단원에 나와 있습니다.</p>
Content-Type	<p>사용 <code>application/x-amz-json-1.1</code> 에 대한 모든 요청에 대한 콘텐츠 유형으로AWS Storage Gateway.</p> <div data-bbox="472 1623 1507 1707" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre>Content-Type: application/x-amz-json-1.1</pre> </div>
Host	<p>호스트 헤더를 사용하여 다음을 지정합니다.AWS Storage Gateway요청을 보내는 엔드포인트입니다. 예, <code>storagegateway.us-east-2.amazonaws.com</code> 은 미국 동부 (오하이오) 리전의 엔드포인트입니다. 에서</p>

헤더	설명
	<p>사용할 수 있는 엔드포인트에 대한 자세한 내용은 AWS Storage Gateway 참조 AWS Storage Gateway 엔드포인트 및 할당량의 AWS 일반 참조.</p> <pre data-bbox="474 361 1507 441">Host: storagegateway. <i>region</i>.amazonaws.com</pre>
x-amz-date	<p>HTTP Date 헤더 또는 AWS x-amz-date 헤더에 타임스탬프를 제공해야 합니다. 일부 HTTP 클라이언트 라이브러리에서는 Date 헤더를 설정할 수 없습니다. 언제? x-amz-date 헤더가 있으면 AWS Storage Gateway를 무시합니다. Date 요청 인증 중에 헤더입니다. x-amz-date 형식은 YYYYMMDD'T'HHMMSS'Z' 형식의 ISO8601 기본이어야 합니다. Date 및 x-amz-date 헤더를 모두 사용하는 경우, Date 헤더의 형식이 ISO8601일 필요는 없습니다.</p> <pre data-bbox="474 873 1507 953">x-amz-date: <i>YYYYMMDD'T'HHMMSS'Z'</i></pre>
x-amz-target	<p>이 헤더는 API의 버전과 요청 중인 작업을 지정합니다. 대상 헤더 값은 API 버전을 API 이름과 연결하여 구성하며 형식은 다음과 같습니다.</p> <pre data-bbox="474 1142 1507 1222">x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></pre> <p>이 <i>operationName</i> 값 (예: "ActivateGateway")은 API 목록에서 찾을 수 있으며, API 참조.</p>

요청에 서명하기

Storage Gateway는 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 Gateway는 요청을 처리합니다. 그렇지 않으면 요청이 거부됩니다.

다음을 사용하는 인증 지원 [AWS서명 버전 4](#). 서명을 계산하기 위한 프로세스는 다음 세 작업으로 나뉠 수 있습니다.

- [작업 1: 정규 요청 생성](#)

HTTP 요청을 정규 형식으로 재배열합니다. 정규 형식을 사용해야 하는 이유는 Storage Gateway가 서명을 재계산하여 본인이 전송한 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 시작해 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드(HMAC)를 생성하는 방법으로 계산합니다.

서명 계산 예시

다음 예시에서는 [ListGateways](#)에 대해 서명을 생성하는 세부 과정을 안내합니다. 이 예시는 서명 계산 방법을 점검하기 위한 참조로 사용할 수 있습니다. 다른 참조 계산은 Amazon Web Services 글로서리의 [서명 버전 4 테스트 제품군](#)에 포함되어 있습니다.

이 예시에서는 다음과 같이 가정합니다.

- 해당 요청의 타임스탬프는 "2012년 9월 10일 월요일 00:00:00시" GMT입니다.
- 엔드포인트는 미국 동부 (오하이오) 리전입니다.

일반 요청 구문(JSON 본문 포함)은 다음과 같습니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
```

```
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

[작업 1: 정규 요청 생성](#)에 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. 이유는 이 API (또는 Storage Gateway API)에 대해 쿼리 파라미터가 없기 때문입니다.

이서명할 문자열...에 대한 [작업 2: 서명할 문자열 생성](#) 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 생성](#)을 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/bPxRfiCYEXAMPLEKEY 사용되는 경우 계산된 서명은 다음과 같습니다.

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

마지막 단계는 Authorization 헤더를 생성하는 것입니다. 데모용 액세스 키 AKIAIOSFODNN7EXAMPLE 의 경우 헤더는 다음과 같습니다 (가독성을 높이기 위해 줄 바꿈을 추가함). AKIAIOSFODNN7EXAMPLE

```
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

- [예외](#)
- [작업 오류 코드](#)
- [오류 응답](#)

이 단원에서는 AWS Storage Gateway 오류에 대한 참조 정보를 제공합니다. 이 오류는 오류 예외 및 작업 오류 코드로 표시됩니다. 예를 들어 오류 예외 `InvalidSignatureException`은 요청 서명에 문제가 있는 경우 모든 API 응답이 반환합니다. 그러나 작업 오류 코드 `ActivationKeyInvalid`는 [ActivateGateway](#) API에 대해서만 반환됩니다.

오류 유형에 따라 Storage Gateway는 예외만 반환하거나 예외 및 작업 오류 코드를 모두 반환할 수 있습니다. 오류 응답 예시는 [오류 응답](#)에 있습니다.

예외

다음 표에는 AWS Storage Gateway API 예외가 나와 있습니다. AWS Storage Gateway 작업이 오류 응답을 반환할 때 응답 본문에는 이러한 예외 중 하나가 포함되어 있습니다. `InternalServerError`와 `InvalidGatewayRequestException`은 특정 작업 오류 코드를 부여하는 작업 오류 코드([작업 오류 코드](#)) 메시지 코드 중 하나를 반환합니다.

예외	Message	HTTP 상태 코드
IncompleteSignatureException	지정한 서명이 불완전합니다.	400 잘못된 요청
InternalFailure	알 수 없는 오류, 예외 또는 장애로 인해 요청 처리가 실패했습니다.	500 Internal Server Error
InternalServerError	작업 오류 코드 작업 오류 코드 메시지 중 하나입니다.	500 Internal Server Error
InvalidAction	요청된 동작 또는 작업이 유효하지 않습니다.	400 잘못된 요청
InvalidClientTokenId	X.509 인증서 또는 AWS 제공된 액세스 키 ID가 AWS의 레코드에 존재하지 않습니다.	403 금지됨
InvalidGatewayRequestException	작업 오류 코드 의 작업 오류 코드 메시지 중 하나입니다.	400 잘못된 요청
InvalidSignatureException	우리가 계산한 요청 서명이 사용자가 제공한 서명과 일치하지 않습니다. 확인 AWS 액세스 키와 서명 방법.	400 잘못된 요청
MissingAction	요청에서 작업 또는 작업 파라미터가 누락되었습니다.	400 잘못된 요청
MissingAuthenticationToken	요청은 유효한 (등록된) 를 포함해야 합니다. AWS 키 ID 또는 X.509 인증서에 액세스합니다.	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. JSON 페이로드의 형식이 올바른지 확인합니다.	400 잘못된 요청

예외	Message	HTTP 상태 코드
ServiceUnavailable	서버의 일시적 장애로 인해 요청이 실패하였습니다.	[503 Service Unavailable]
SubscriptionRequiredException	이AWS액세스 키 ID는 서비스 가입이 필요합니다.	400 잘못된 요청
ThrottlingException	속도를 초과하였습니다.	400 잘못된 요청
UnknownOperationException	알 수 없는 작업을 지정하였습니다. 유효한 작업은 Storage Gateway 에 나열되어 있습니다.	400 잘못된 요청
UnrecognizedClientException	요청에 포함된 보안 토큰이 잘못되었습니다.	400 잘못된 요청
ValidationException	입력 파라미터의 값이 잘못되었거나 범위를 벗어났습니다.	400 잘못된 요청

작업 오류 코드

다음 표에는 AWS Storage Gateway 작업 오류 코드와 해당 코드를 반환할 수 있는 API 간의 매핑이 나와 있습니다. 모든 작업 오류 코드는 두 가지 일반적인 예외 중 하나와 함께 반환됩니다. `InternalServerError`과 `InvalidGatewayRequestException`—[설명됨 예외](#).

작업 오류 코드	Message	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

작업 오류 코드	Message	이 오류 코드를 반환하는 작업
BandwidthThrottleScheduleNotFound	지정한 대역폭 제한을 찾을 수 없습니다.	DeleteBandwidthRateLimit
CannotExportSnapshot	지정한 스냅샷을 내보낼 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	지정된 초기자를 찾을 수 없습니다.	DeleteChapCredentials
DiskAlreadyAllocated	지정한 디스크가 이미 할당되었습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	지정한 디스크가 존재하지 않습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	지정한 디스크가 기가바이트 정렬되어 있지 않습니다.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	지정한 디스크 크기가 최대 볼륨 크기보다 큼니다.	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	지정한 디스크 크기가 볼륨 크기보다 작습니다.	CreateStorediSCSIVolume

작업 오류 코드	Message	이 오류 코드를 반환하는 작업
DuplicateCertificateInfo	지정한 인증서 정보가 중복되어 있습니다.	ActivateGateway
파일 시스템연결엔드포인트 구성 충돌	기존 파일 시스템 연결 엔드포인트 구성이 지정된 구성과 충돌합니다.	어소시에이트파일 시스템
파일 시스템연관엔드포인트패드드레스레디사용	지정된 엔드포인트 IP 주소가 이미 사용 중입니다.	어소시에이트파일 시스템
파일 시스템연관엔드포인트패드드레스시스	파일 시스템 연결 엔드포인트 IP 주소가 누락되었습니다.	어소시에이트파일 시스템
파일 시스템연결찾을 수 없음	지정한 파일 시스템 연결을 찾을 수 없습니다.	Update파일 시스템 연결 연결 해제 파일 시스템 설명파일 시스템연관
파일 시스템찾을 수 없음	지정한 파일 시스템을 찾을 수 없습니다.	어소시에이트파일 시스템

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		<u>DescribeWorkingStorage</u> <u>ListLocalDisks</u> <u>ListGateways</u> <u>ListVolumes</u> <u>ListVolumeRecoveryPoints</u> <u>ShutdownGateway</u> <u>StartGateway</u> <u>UpdateBandwidthRateLimit</u> <u>UpdateChapCredentials</u> <u>UpdateMaintenanceStartTime</u> <u>UpdateGatewayInformation</u> <u>UpdateGatewaySoftwareNow</u> <u>UpdateSnapshotSchedule</u>

작업 오류 코드	Message	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	Message	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	로컬 스토리지 한도를 초과했습니다.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	지정한 LUN이 유효하지 않습니다.	CreateStoragediSCSIVolume

작업 오류 코드	Message	이 오류 코드를 반환하는 작업
MaximumVolumeCount Exceeded	최대 볼륨 수를 초과하였습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurationChanged	게이트웨이 네트워크 구성이 변경되었습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	Message	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	Message	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	Message	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	Message	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	Message	이 오류 코드를 반환하는 작업
VolumeNotFound	지정한 볼륨을 찾을 수 없습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	지정한 볼륨이 아직 준비되지 않았습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

오류 응답

오류가 있는 경우, 응답 헤더 정보에는 다음 내용이 포함됩니다.

- Content-Type: application/x-amz-json-1.1
- 적절한 4xx 또는 5xx HTTP 상태 코드

오류 응답의 본문에는 발생한 오류에 대한 정보가 포함됩니다. 다음 샘플 오류 응답은 모든 오류 응답에 공통된 응답 요소의 출력 구문을 나타냅니다.

```
{
  "__type": "String",
  "message": "String",
  "error":
    { "errorCode": "String",
      "errorDetails": "String"
    }
}
```

```
}

```

다음 표는 이전 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__유형

[예외](#)의 예외 중 하나.

Type: 문자열

오류

API별 오류의 세부 정보를 포함합니다. 일반적인 오류(즉 API에 고유한 오류가 아닌 경우)에서는 이 오류 정보가 표시되지 않습니다.

Type: 수집

errorCode

작업 오류 코드 중 하나입니다 .

Type: 문자열

errorDetails

이 필드는 현재 API 버전에서는 사용되지 않습니다.

Type: 문자열

message

작업 오류 코드 메시지 중 하나입니다.

Type: 문자열

오류 응답 예시

DescribeStorediSCSIVolumes API를 사용할 경우 존재하지 않는 게이트웨이 ARN 요청 입력을 지정하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {

```

```
"errorCode": "VolumeNotFound"
}
}
```

Storage Gateway가 요청과 함께 전송된 서명과 일치하지 않는 서명을 계산하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Storage Gateway

Storage Gateway 작업 목록은 단원을 참조하십시오. [작업](#)의 AWS Storage Gateway API 참조.

Amazon FSx 파일 게이트웨이 사용 설명서에 대한 문서 이력

- API 버전: 2013-06-30
- 최신 문서 업데이트: 2021년 7월 07일

다음 표에서는 Amazon FSx File Gateway의 설명서 릴리스 관련 사항을 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

update-history-change	update-history-description	update-history-date
다중 파일 시스템 지원	Amazon FSx 파일 게이트웨이는 이제 최대 5개의 연결된 Amazon FSx 파일 시스템을 지원합니다. 자세한 내용은 단원을 참조하십시오. Amazon FSx for Windows File Server 파일 시스템 연결 .	2021년 7월 7일
아마존 FSx 소프트 스토리지 할당량 지원	Amazon FSx File Gateway는 이제 스토리지 할당량이 구성된 연결된 Amazon FSx 파일 시스템에 쓸 때 소프트 스토리지 할당량 (사용자가 데이터 한도를 초과할 때 경고)을 지원합니다. 하드 할당량 (쓰기 액세스를 거부하여 데이터 제한을 적용하는)은 지원되지 않습니다. 소프트 할당량은 Amazon FSx 관리자 사용자를 제외한 모든 사용자에게 적용됩니다. 스토리지 할당량 설정에 대한 자세한 내용은 단원을 참조하십시오. 스토리지 할당량 의 Amazon FSx for Windows File Server 사용 설명서.	2021년 7월 7일

새 설명서

Storage Gateway 게이트웨이는 원본 파일 게이트웨이 (현재 Amazon S3 파일 게이트웨이라고도 함) 외에도 Amazon FSx 파일 게이트웨이 (FSx 파일) 를 제공합니다. FSx 파일은 온프레미스 시설에서 Windows 파일 서버용 클라우드 인 FSx 파일 공유에 대한 지연 시간이 짧고 효율적인 액세스를 제공합니다. 자세한 내용은 단원을 참조하십시오. [Amazon FSx 파일 게이트웨이란 무엇입니까?](#)

2021년 4월 27일

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