



Tape Gateway 사용 설명서

AWS Storage Gateway



API 버전 2013-06-30

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Tape Gateway 사용 설명서

Copyright © 2024 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

Tape Gateway란 무엇인가요?	1
Tape Gateway 작동 방식	1
Tape Gateway	2
시작하기 AWS Storage Gateway	5
가입 AWS Storage Gateway	5
관리자 권한이 있는 IAM 사용자 생성	6
액세스 AWS Storage Gateway	7
AWS 리전 Storage Gateway를 지원하는	8
Tape Gateway 설정 요구 사항	9
하드웨어 및 스토리지 요구 사항	9
에 대한 하드웨어 요구 사항 VMs	9
Amazon EC2 인스턴스 유형에 대한 요구 사항	10
.....	10
스토리지 요구 사항	10
네트워크 및 방화벽 요구 사항	11
포트 요구 사항	12
하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항	17
게이트웨이가 방화벽 및 라우터를 통해 액세스할 수 있도록 허용	19
보안 그룹 구성	21
지원되는 하이퍼바이저 및 호스트 요구 사항	22
지원되는 iSCSI 이니시에이터	23
지원되는 타사 백업 애플리케이션	24
하드웨어 어플라이언스 사용	26
하드웨어 어플라이언스 설정	26
하드웨어 어플라이언스 물리적 설치	28
하드웨어 어플라이언스 콘솔 액세스	30
하드웨어 어플라이언스 네트워크 파라미터 구성	31
하드웨어 어플라이언스 활성화	32
하드웨어 어플라이언스에서 게이트웨이 생성	33
하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성	34
하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거	36
하드웨어 어플라이언스 삭제	37
게이트웨이 생성	38
개요 - 게이트웨이 활성화	38

게이트웨이 설정	38
에 연결 AWS	38
검토 및 활성화	39
개요 - 게이트웨이 구성	39
개요 - 스토리지 리소스	39
Tape Gateway 생성 및 활성화	39
Tape Gateway 설정	40
Tape Gateway를 에 연결 AWS	41
설정 검토 및 Tape Gateway 활성화	42
Tape Gateway 구성	42
테이프 생성	45
WORM 테이프 보호	45
수동으로 테이프 생성	46
자동 테이프 생성 허용	48
사용자 지정 테이프 풀 생성	50
유형 선택	51
테이프 보존 잠금	51
사용자 지정 테이프 풀 생성	52
VTL 디바이스 연결	53
Microsoft Windows 클라이언트에 연결	53
Linux 클라이언트에 연결	54
게이트웨이 테스트	58
Arcserve 백업	59
Bacula Enterprise	62
Commvault	66
Dell EMC NetWorker	71
IBM스펙트럼 보호	75
마이크로 포커스 데이터 보호기	79
Microsoft System Center DPM	85
NovaStor DataCenter/네트워크	90
퀘스트 NetVault 백업	96
Veeam Backup & Replication	99
Veritas Backup Exec	102
Veritas NetBackup	106
추가 정보	113
Virtual Private Cloud(VPC)에서 게이트웨이 활성화	113

Storage Gateway용 VPC 엔드포인트 생성	114
Tape Gateway 관리	116
게이트웨이 정보 편집	117
자동 테이프 생성 관리	117
테이프 보관	120
S3 Glacier Deep Archive로 테이프 이동	120
보관한 테이프 가져오기	121
테이프 사용 통계 보기	123
테이프 삭제	123
사용자 지정 테이프 풀 삭제	124
Tape Gateway 비활성화	125
테이프 상태 이해	126
의 테이프 상태 정보 이해 VTL	126
아카이브의 테이프 상태 확인	127
데이터를 새 게이트웨이로 이동	128
가상 테이프를 새 Tape Gateway로 이동	129
Storage Gateway 모니터링	133
게이트웨이 지표 이해	133
Storage Gateway 지표의 차원	136
업로드 버퍼 모니터링	137
캐시 스토리지 모니터링	139
CloudWatch 경보 이해	140
권장 CloudWatch 경보 생성	142
사용자 지정 CloudWatch 경보 생성	143
Tape Gateway 모니터링	144
Tape Gateway 상태 로그 가져오기	145
Amazon CloudWatch 지표 사용	147
가상 테이프 지표 이해	148
Tape Gateway와 간의 성능 측정 AWS	150
게이트웨이 유지 관리	153
로컬 디스크 관리	153
로컬 디스크 스토리지 용량 결정	153
업로드 버퍼 또는 캐시 스토리지 추가	157
대역폭 관리	157
Storage Gateway 콘솔을 사용하여 대역폭 조절 변경	158
대역폭 조절 예약	159

사용 AWS SDK for Java	160
사용 AWS SDK for .NET	162
사용 AWS Tools for Windows PowerShell	164
게이트웨이 업데이트 관리	165
빈도 및 예상 동작 업데이트	166
유지 관리 업데이트 켜기 또는 끄기	166
게이트웨이 유지 관리 기간 일정 수정	167
수동으로 업데이트 적용	168
게이트웨이 VM 종료	169
Tape Gateway 시작 및 중지	170
게이트웨이 삭제 및 리소스 제거	171
Storage Gateway 콘솔을 사용하여 게이트웨이 삭제	171
온프레미스에 배포한 게이트웨이에서 리소스 제거	173
Amazon EC2 인스턴스에 배포된 게이트웨이에서 리소스 제거	174
로컬 콘솔을 사용하여 유지 관리 작업 수행	176
게이트웨이 로컬 콘솔 액세스	176
Linux를 사용하여 Gateway Local Console에 액세스 KVM	177
를 사용하여 Gateway Local Console에 액세스 VMware ESXi	177
Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스	178
VM 로컬 콘솔에서 작업 수행	179
Tape Gateway 로컬 콘솔에 로그인	180
온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성	181
게이트웨이 네트워크 구성	183
인터넷에 대한 게이트웨이 연결 테스트	188
온프레미스 게이트웨이에 대해 로컬 콘솔에서 스토리지 게이트웨이 명령 실행	189
게이트웨이 시스템 리소스 상태 조회	191
EC2 로컬 콘솔에서 작업 수행	192
EC2 Gateway Local Console에 로그인	193
HTTP 프록시 구성	194
게이트웨이 네트워크 연결 테스트	194
게이트웨이 시스템 리소스 상태 조회	195
로컬 콘솔에서 Storage Gateway 명령 실행	196
Tape Gateway의 성능 및 최적화	199
Tape Gateway의 성능 지침	199
게이트웨이 성능 최적화	202
권장 구성	202

게이트웨이에 리소스 추가	202
iSCSI 설정 최적화	205
테이프 드라이브에 더 큰 블록 크기 사용	206
가상 테이프 드라이브의 성능 최적화	206
애플리케이션 환경에 리소스 추가	206
보안	208
데이터 보호	208
데이터 암호화	209
ID 및 액세스 관리	211
고객	211
ID를 통한 인증	212
정책을 사용한 액세스 관리	215
AWS Storage Gateway의 작동 방식 IAM	217
자격 증명 기반 정책 예시	223
문제 해결	226
규정 준수 확인	228
복원력	228
인프라 보안	229
AWS 보안 베스트 프랙티스	230
로깅 및 모니터링	230
Storage Gateway 정보 입력 CloudTrail	230
Storage Gateway 로그 파일 항목 이해	231
게이트웨이 문제 해결	234
문제 해결: 게이트웨이 오프라인 문제	234
연결된 방화벽 또는 프록시 확인	235
게이트웨이 트래픽에 대한 지속적인 SSL 또는 심층 패킷 검사 확인	235
하이퍼바이저 호스트에서 정전 또는 하드웨어 장애 확인	235
연결된 캐시 디스크에 문제가 있는지 확인	235
문제 해결: 게이트웨이 활성화 문제	236
퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결	237
Amazon VPC 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결	239
퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 동일한 에 Storage Gateway VPC 엔드포인트가 있는 경우 오류를 해결합니다. VPC	243
온프레미스 게이트웨이 문제 해결	244
게이트웨이 문제 해결 AWS Support 에 도움이 되도록 활성화	248
Microsoft Hyper-V 설정 관련 문제 해결	249

Amazon EC2 게이트웨이 문제 해결	252
몇 분 후 게이트웨이가 활성화되지 않음	253
인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.	253
Amazon EBS 볼륨을 EC2 게이트웨이 인스턴스에 연결할 수 없습니다.	253
스토리지 볼륨을 추가하려고 하는데 사용 가능한 디스크가 없다는 메시지	253
업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이는 방법	254
게이트웨이로 들어오거나 EC2 게이트웨이를 통한 처리량이 0으로 떨어집니다.	254
게이트웨이 문제 AWS Support 해결에 도움이 되도록 활성화합니다.	254
직렬 콘솔을 사용하여 Amazon EC2 게이트웨이에 연결	256
하드웨어 어플라이언스 문제 해결	256
서비스 IP 주소를 확인하는 방법	256
공장 초기화를 수행하는 방법	257
원격 재시작을 수행하는 방법	257
Dell iDRAC 지원을 받는 방법	257
하드웨어 어플라이언스 일련 번호를 찾는 방법	257
하드웨어 어플라이언스 지원을 받는 방법	257
가상 테이프 관련 문제 해결	258
복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우	258
복구 불가능한 테이프 문제 해결	262
고가용성 상태 알림	263
고가용성 문제 해결	263
상태 알림	263
지표	265
모범 사례	266
모범 사례: 데이터 복구	266
VM이 예기치 않게 종료된 상황에서 복구하기	267
장애가 있는 게이트웨이 또는 VM에서 데이터 복구	267
복구할 수 없는 테이프에서 데이터 복구	267
장애가 있는 캐시 디스크에서 데이터 복구	268
액세스할 수 없는 데이터 센터에서 데이터 복구	268
불필요한 리소스 정리	269
추가 리소스	270
호스트 설정	271
Tape Gateway용 기본 Amazon EC2 호스트 배포	271
Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포	274
Amazon EC2 인스턴스 메타데이터 옵션 수정	277

VM 시간을 Hyper-V 또는 Linux KVM 호스트 시간과 동기화	278
VM 시간과 VMware 호스트 시간 동기화	278
파라가상화된 디스크 컨트롤러 구성	280
게이트웨이용 네트워크 어댑터 구성	280
Storage Gateway에서 VMware고가용성 사용	285
Tape Gateway 스토리지 리소스 작업	290
게이트웨이에서 디스크 제거	291
EBS EC2 게이트웨이 볼륨	292
VTL 디바이스 작업	293
테이프 관련 작업	298
정품 인증 키 가져오기	300
Linux(curl)	301
Linux(bash/zsh)	301
마이크로소프트 윈도우 PowerShell	302
로컬 콘솔 사용	303
iSCSI 이니시에이터 연결	303
Windows 클라이언트에 VTL 디바이스 연결	304
VTL 디바이스를 Linux 클라이언트에 연결	307
iSCSI 설정 사용자 지정	309
CHAP 인증 구성	313
Storage AWS Direct Connect Gateway와 함께 사용	319
Tape Gateway에 대한 포트 요구 사항	319
게이트웨이 IP 주소 가져오기	325
Amazon EC2 호스트에서 IP 주소 가져오기	325
리소스 및 리소스에 대한 이해 IDs	326
리소스 관련 작업 IDs	327
리소스에 태그 지정	327
태그 작업	328
오픈 소스 구성 요소	329
Storage Gateway 할당량	330
테이프 할당량	330
게이트웨이에 권장되는 로컬 디스크 크기	330
API레퍼런스	332
필수 요청 헤더	332
요청에 서명하기	334
서명 계산 예시	335

오류 응답	337
예외	337
작업 오류 코드	339
오류 응답	358
운영	360
문서 기록	361
이전 업데이트	376
릴리스 정보	393
.....	CCCXCVI

Tape Gateway란 무엇인가요?

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

Storage Gateway를 온프레미스에서 ESXi, KVM또는 Microsoft Hyper-V 하이퍼바이저에서 실행되는 VMware VM 어플라이언스로, 하드웨어 어플라이언스로 또는 에서 Amazon EC2 인스턴스 AWS 로 배포할 수 있습니다. 재해 복구, 데이터 미러링 및 Amazon 에서 호스팅되는 애플리케이션을 위한 스토리지 제공을 위해 EC2 인스턴스에서 호스팅되는 게이트웨이를 사용할 수 있습니다EC2.

를 활성화하는 AWS Storage Gateway 데 도움이 되는 다양한 사용 사례를 보려면 섹션을 참조하세요 [AWS Storage Gateway](#). 최신 요금 정보는 AWS Storage Gateway 세부 정보 페이지에서 [요금](#)을 참조하세요.

AWS Storage Gateway 는 파일 기반(S3 File Gateway 및 FSx File Gateway), 볼륨 기반(Volume Gateway) 및 테이프 기반(Tape Gateway) 스토리지 솔루션을 제공합니다.

이 사용 설명서는 Tape Gateway와 관련된 정보를 제공합니다.

Tape Gateway는 클라우드 기반 가상 테이프 스토리지를 제공합니다. Tape Gateway를 사용하면 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 백업 데이터를 비용 효율적이고 지속 가능하게 보관할 수 있습니다. Tape Gateway는 비즈니스 요구 사항에 따라 원활하게 확장할 수 있는 가상 테이프 인프라를 제공하며 물리적 테이프 인프라를 프로비저닝, 확장 및 유지 관리하는 운영 부담을 제거합니다.

아키텍처 개요에 대해서는 [Tape Gateway 작동 방식](#) 단원을 참조하십시오.

이 사용 설명서에서는 모든 게이트웨이 유형에 공통적인 설정 정보를 다루는 시작하기 섹션을 찾을 수 있습니다. Tape Gateway 설정 요구 사항과 Tape Gateway 를 배포, 활성화, 구성 및 관리하는 방법을 설명하는 섹션을 찾을 수도 있습니다.

이 사용 설명서의 절차는 주로 를 사용하여 게이트웨이 작업을 수행하는 데 중점을 둡니다 AWS Management Console. 이러한 작업을 프로그래밍 방식으로 수행하려면 [AWS Storage Gateway API 참조](#)를 참조하세요.

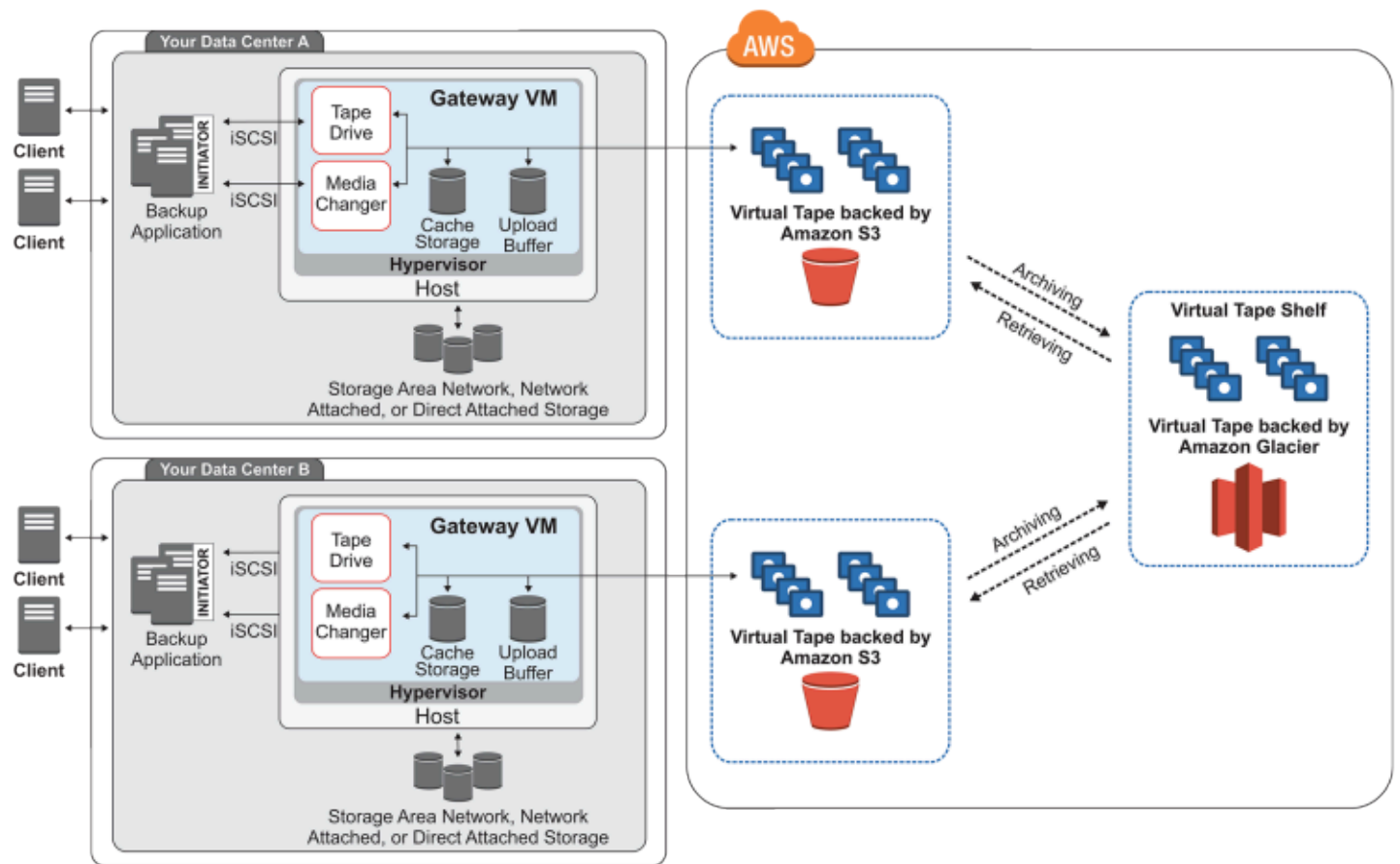
Tape Gateway 작동 방식

다음에서 Tape Gateway 솔루션의 아키텍처 개요를 확인할 수 있습니다.

Tape Gateway

Tape Gateway는 데이터를 내구성이 있고 비용 효율적인 방식으로 Amazon Web Services 클라우드에 아카이브할 수 있는 솔루션을 제공합니다. 가상 테이프 라이브러리(VTL) 인터페이스를 사용하면 기존 테이프 기반 백업 인프라를 사용하여 Tape Gateway에서 생성한 가상 테이프 카트리지에 데이터를 저장할 수 있습니다. 각 Tape Gateway에는 미디어 체인저 및 테이프 드라이브가 사전 구성되어 있습니다. 기존 클라이언트 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있습니다. 필요에 따라 테이프 카트리지를 추가하여 데이터를 보관합니다.

다음 다이어그램은 Tape Gateway 배포를 간략하게 보여줍니다.



이 다이어그램은 다음과 같은 Tape Gateway 구성 요소를 보여줍니다.

- 가상 테이프 - 가상 테이프는 물리적 테이프 카트리지와 유사합니다. 그러나 가상 테이프 데이터는 Amazon Web Services 클라우드에 저장됩니다. 물리적 테이프처럼 가상 테이프는 공백 상태로 두거나 데이터를 기록할 수 있습니다. Storage Gateway 콘솔을 사용하거나 프로그래밍 방식으로 Storage Gateway 를 사용하여 가상 테이프를 생성할 수 있습니다. API. 각 게이트웨이는 테이프를 1,500개까지 또는 한 번에 총 테이프 데이터를 1PiB까지 포함할 수 있습니다. 각 가상 테이프의 크기는 100GiB-15TiB이며, 이 크기는 테이프 생성 시 구성할 수 있습니다.

- 가상 테이프 라이브러리(VTL) - VTL은 로봇 팔 및 테이프 드라이브가 있는 온프레미스에서 사용할 수 있는 물리적 테이프 라이브러리와 같습니다. 예는 저장된 가상 테이프 모음이 VTL 포함됩니다. 각 Tape Gateway에는 하나의 가 함께 제공됩니다VTL.

생성한 가상 테이프는 게이트웨이의 에 표시됩니다VTL. 의 테이프VTL은 Amazon S3에서 백업합니다. 백업 소프트웨어가 게이트웨이에 데이터를 쓰면 게이트웨이는 데이터를 로컬에 저장한 다음 비동기식으로 의 가상 테이프, VTL 즉 Amazon S3에 업로드합니다.

- 테이프 드라이브 - VTL 테이프 드라이브는 I/O를 수행하고 테이프에서 작업을 찾을 수 있는 물리적 테이프 드라이브와 유사합니다. 각 VTL에는 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있는 10개의 테이프 드라이브 세트가 함께 제공됩니다.
- 미디어 체인저 - VTL 미디어 체인저는 물리적 테이프 라이브러리의 스토리지 슬롯 및 테이프 드라이브에서 테이프를 이동하는 로봇과 유사합니다. 각 VTL 에는 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있는 미디어 체인저가 하나씩 제공됩니다.
- 아카이브 - 아카이브는 외부 테이프 보유 시설과 유사합니다. 게이트웨이의 테이프를 아카이브VTL 에 보관할 수 있습니다. 필요한 경우 아카이브에서 게이트웨이의 로 테이프를 다시 검색할 수 있습니다VTL.
- 테이프 아카이브 - 백업 소프트웨어가 테이프를 배출하면 게이트웨이는 장기 스토리지용 아카이브로 테이프를 옮깁니다. 아카이브는 게이트웨이를 활성화한 AWS 리전에 있습니다. 아카이브의 테이프는 가상 테이프 선반()에 저장됩니다VTS. VTS 는 [S3 Glacier Flexible Retrieval](#) 또는 [S3 Glacier Deep Archive](#) , 데이터 보관, 백업 및 장기 데이터 보존을 위한 저비용 스토리지 서비스로 지원됩니다.
- 테이프 가져오기 - 아카이브된 테이프는 직접 읽을 수 없습니다. 아카이브된 테이프를 읽으려면 먼저 Storage Gateway 콘솔 또는 Storage Gateway 를 사용하여 Tape Gateway로 테이프를 검색해야 합니다API.

Important

S3 Glacier Flexible Retrieval에 테이프를 아카이브하면 일반적으로 3-5시간 내에 테이프를 가져올 수 있습니다. S3 Glacier Deep Archive에 테이프를 아카이브하면 일반적으로 12시간 내에 테이프를 가져올 수 있습니다.

Tape Gateway를 배포하고 활성화한 후 온프레미스 애플리케이션 서버에 가상 테이프 드라이브와 미디어 체인저를 iSCSI 디바이스로 탑재합니다. 필요 시 가상 테이프를 생성할 수 있습니다. 그리고 나면 기존 백업 소프트웨어 애플리케이션을 사용하여 데이터를 가상 테이프에 쓸 수 있습니다. 미디어 체인저는 가상 테이프를 가상 테이프 드라이브로 로드 및 언로드하여 읽기 및 쓰기 작업을 수행합니다.

게이트웨이 VM에 로컬 디스크 할당

게이트웨이 VM에는 로컬 디스크가 필요한데, 이를 할당하는 목적은 다음과 같습니다.

- 캐시 스토리지 - 캐시 스토리지는 업로드 버퍼에서 Amazon S3로 업로드 대기 중인 데이터를 위한 내구성 저장소 역할을 합니다.

애플리케이션이 가상 테이프에서 데이터를 읽으면 게이트웨이는 데이터를 캐시 스토리지에 저장합니다. 게이트웨이는 액세스 지연 시간을 줄이기 위해 최근에 액세스한 데이터를 캐시 스토리지에 저장합니다. 애플리케이션이 테이프 데이터를 요청하는 경우 게이트웨이는 먼저 캐시 스토리지에서 데이터를 다운로드하기 전에 캐시 스토리지에서 데이터를 확인합니다 AWS.

- 업로드 버퍼 - 업로드 버퍼는 데이터를 가상 테이프에 업로드하기 전에 게이트웨이에 스테이징 영역을 제공합니다. 또한 업로드 버퍼는 예기치 않은 장애로부터 테이프를 복구하는 데 사용할 수 있는 복구 시점을 생성할 때 아주 중요한 역할을 합니다. 자세한 내용은 [장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우](#) 단원을 참조하십시오.

백업 애플리케이션이 데이터를 게이트웨이에 쓸 때 게이트웨이는 데이터를 캐시 스토리지와 업로드 버퍼 모두로 복사합니다. 그런 다음 백업 애플리케이션에 대한 쓰기 작업 완료를 승인합니다.

캐시 스토리지 및 업로드 버퍼에 할당할 디스크 공간 크기에 대한 지침은 [로컬 디스크 스토리지 용량 결정](#) 단원을 참조하십시오.

시작하기 AWS Storage Gateway

이 섹션에서는 를 시작하기 위한 지침을 제공합니다 AWS. 사용을 시작하려면 AWS 계정이 필요합니다 AWS Storage Gateway. 기존 AWS 계정을 사용하거나 새 계정에 가입할 수 있습니다. 또한 Storage Gateway 작업을 수행하는 데 필요한 관리 권한이 있는 그룹에 속한 AWS 계정의 IAM 사용자가 필요합니다. 적절한 권한이 있는 사용자는 Storage Gateway 콘솔 및 Storage Gateway에 액세스하여 게이트웨이 배포, 구성 및 유지 관리 작업을 수행할 수 있습니다. 처음 사용하는 경우 Storage Gateway 를 사용하기 전에 [지원되는 AWS 리전](https://docs.aws.amazon.com/storagegateway/latest/tgw/Requirements.html) 및 Tape Gateway 설정 요구 사항 섹션을 검토하는 것이 좋습니다.

이 섹션에는 를 시작하는 방법에 대한 추가 정보를 제공하는 다음 주제가 포함되어 있습니다. AWS Storage Gateway

주제

- [가입 AWS Storage Gateway](#) - 가입 AWS 하고 AWS 계정을 생성하는 방법을 알아봅니다.
- [관리자 권한이 있는 IAM 사용자 생성](#) - AWS 계정에 대한 관리 권한이 있는 IAM 사용자를 생성하는 방법을 알아봅니다.
- [액세스 AWS Storage Gateway](#) - Storage Gateway 콘솔을 AWS Storage Gateway 통해 또는 를 사용하여 프로그래밍 방식으로 에 AWS 액세스하는 방법을 알아봅니다 SDKs.
- [AWS 리전 Storage Gateway를 지원하는](#) - Storage Gateway 에서 게이트웨이를 활성화할 때 데이터를 저장하는 데 사용할 수 있는 AWS 리전을 알아봅니다.

가입 AWS Storage Gateway

AWS 계정은 AWS 서비스에 액세스하기 위한 기본 요구 사항입니다. AWS 계정은 AWS 사용자로 생성한 모든 AWS 리소스의 기본 컨테이너입니다. AWS 계정은 리소스의 기본 보안 경계이기도 합니다 AWS . 계정에서 생성한 모든 리소스는 계정에 대한 보안 인증 정보가 있는 사용자가 사용할 수 있습니다. 사용을 시작하려면 먼저 에 가입 AWS Storage Gateway해야 합니다 AWS 계정.

가 없는 경우 다음 단계를 AWS 계정완료하여 를 생성합니다.

에 가입하려면 AWS 계정

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

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

에 가입하면 AWS 계정AWS 계정 루트 사용자가 생성됩니다. 루트 사용자에게는 계정의 모든 AWS 서비스 및 리소스에 액세스할 권한이 있습니다. 보안 모범 사례는 사용자에게 관리 액세스 권한을 할당하고, 루트 사용자만 사용하여 [루트 사용자 액세스 권한이 필요한 작업](#)을 수행하는 것입니다.

또한 사용자가 에 액세스할 때 임시 자격 증명을 사용하도록 하는 것이 좋습니다 AWS. 임시 자격 증명 을 제공하려면 페더레이션과 Identity Center와 같은 AWS IAM 자격 증명 공급자를 사용할 수 있습니다. 회사에서 이미 자격 증명 공급자를 사용하는 경우 페더레이션과 함께 사용하여 AWS 계정의 리소스에 대한 액세스를 제공하는 방법을 간소화할 수 있습니다.

관리자 권한이 있는 IAM 사용자 생성

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

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

관리자 를 관리 하는 방법 한 가지 선택	목적	By	다른 방법
IAM Identity Center 에서 (권장)	단기 보안 인증 정보를 사용하여 AWS에 액세스합니다. 이는 보안 모범 사례와 일치합니다. 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 예 서 보안 모범 사례를 IAM 참조하세요.	AWS IAM Identity Center 사용 설명서의 시작하기 지침을 따르세요.	AWS Command Line Interface 사용 설명서 에서 AWS CLI 사용하도록 를 구성 AWS IAM Identity Center 하여 프로그래밍 방식 액세스를 구성합니다.

관리자를 관리하는 방법 한 가지 선택	목적	By	다른 방법
에서 IAM (권장되지 않음)	장기 보안 인증 정보를 사용하여 AWS에 액세스합니다.	IAM 사용 설명서의 첫 IAM 번째 관리자 사용자 및 사용자 그룹 생성 의 지침을 따릅니다.	IAM 사용 설명서의 IAM 사용자에 대한 액세스 키를 관리 하여 프로그래밍 방식 액세스를 구성합니다.

Warning

IAM 사용자에게는 보안 위험이 있는 장기 보안 인증 정보가 있습니다. 이 위험을 줄이려면 이러한 사용자에게 작업을 수행하는 데 필요한 권한만 제공하고 더 이상 필요하지 않을 경우 이러한 사용자를 제거하는 것이 좋습니다.

액세스 AWS Storage Gateway

[AWS Storage Gateway 콘솔](#)을 사용하여 배포에서 Storage Gateway 하드웨어 어플라이언스 활성화 또는 제거, 다양한 유형의 게이트웨이 생성, 관리 및 삭제, 가상 테이프 라이브러리 스토리지 볼륨에서 테이프 생성, 관리 및 삭제, Storage Gateway 서비스의 다양한 요소의 상태 및 상태 모니터링 등 다양한 게이트웨이 구성 및 유지 관리 작업을 수행할 수 있습니다. 간편하고 사용하기 쉽도록 이 안내서에서는 Storage Gateway 콘솔 웹 인터페이스를 사용하여 작업을 수행하는 데 중점을 둡니다. 웹 브라우저를 통해 Storage Gateway 콘솔에 액세스할 수 있습니다 <https://console.aws.amazon.com/storagegateway/home/>.

프로그래밍 방식의 접근 방식을 선호하는 경우 AWS Storage Gateway Application Programming Interface(API) 또는 Command Line Interface(CLI)를 사용하여 Storage Gateway 배포에서 리소스를 설정하고 관리할 수 있습니다. Storage Gateway의 작업, 데이터 유형 및 필수 구문에 대한 자세한 내용은 [Storage Gateway API 참조](#)를 API참조하세요. Storage Gateway에 대한 자세한 내용은 [AWS CLI 명령 참조](#)를 CLI참조하세요.

를 AWS SDKs 사용하여 Storage Gateway 와 상호 작용하는 애플리케이션을 개발할 수도 있습니다. Java용 , NET. 및 는 AWS SDKs 기본 Storage Gateway를 PHP 래핑API하여 프로그래밍 작업을 간소화합니다. SDK 라이브러리 다운로드에 대한 자세한 내용은 [AWS 개발자 센터 섹션](#)을 참조하세요.

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

AWS 리전 Storage Gateway를 지원하는

AWS 리전은 가 여러 가용 영역을 AWS 가진 세계의 물리적 위치입니다. 가용 영역은 하나 이상의 이산 AWS 데이터 센터로 구성되며, 각 데이터 센터는 별도의 시설에 수용된 중복 전원, 네트워킹 및 연결을 갖추고 있습니다. 즉, 각 AWS 리전은 물리적으로 격리되어 있고 다른 리전과 독립적입니다. 리전에서는 내결함성, 안정성 및 복원성을 지원하고 지연 시간을 줄일 수도 있습니다. AWS 서비스에서 제공하는 복제 기능을 명시적으로 사용하지 않는 한 한 리전에서 생성하는 리소스는 다른 리전에 존재하지 않습니다. 예를 들어 Amazon S3 및 Amazon은 리전 간 복제를 EC2 지원합니다. 와 같은 일부 서비스에는 리전 리소스 AWS Identity and Access Management가 없습니다. 비즈니스 요구 사항을 충족하는 위치에서 AWS 리소스를 시작할 수 있습니다. 예를 들어 유럽에서 어플라이언스를 호스팅 AWS Storage Gateway 하여 AWS 리전 유럽 사용자에게 더 가깝거나 법적 요구 사항을 충족하기 위해 Amazon EC2 인스턴스를 시작할 수 있습니다. 는 특정 서비스에서 지원하는 리전 중 사용할 수 있는 리전을 AWS 계정 결정합니다.

- Storage Gateway - Storage Gateway 에 사용할 수 있는 지원되는 AWS 리전 및 AWS 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요AWS 일반 참조.
- Storage Gateway 하드웨어 어플라이언스 - 하드웨어 어플라이언스와 함께 사용할 수 있는 지원되는 AWS 리전은 의 [AWS Storage Gateway 하드웨어 어플라이언스 리전](#)을 참조하세요AWS 일반 참조.

Tape Gateway 설정 요구 사항

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

주제

- [하드웨어 및 스토리지 요구 사항](#)
- [네트워크 및 방화벽 요구 사항](#)
- [지원되는 하이퍼바이저 및 호스트 요구 사항](#)
- [지원되는 iSCSI 이니시에이터](#)
- [Tape Gateway에 지원되는 타사 백업 애플리케이션](#)

하드웨어 및 스토리지 요구 사항

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

에 대한 하드웨어 요구 사항 VMs

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

- VM에 지정한 가상 프로세스 4개.
- Tape Gateway 의 경우 하드웨어는 다음과 같은 양의 를 사용해야 합니다RAM.
 - 캐시 크기가 최대 16GiB RAM TiB
 - 캐시 크기가 16TiBGiBTiB RAM
 - 캐시 크기가 32TiBGiBTiB RAM
- VM 이미지 및 시스템 데이터 설치용 디스크 공간 80GiB.

자세한 내용은 [게이트웨이 성능 최적화](#) 단원을 참조하십시오. 하드웨어가 게이트웨이 VM의 성능에 미치는 영향에 대한 정보는 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.

Amazon EC2 인스턴스 유형에 대한 요구 사항

Amazon Elastic Compute Cloud(Amazon EC2)에 게이트웨이를 배포할 때 게이트웨이가 작동하려면 인스턴스 크기가 xlarge 이상이어야 합니다. 하지만 컴퓨팅 최적화 인스턴스 패밀리의 경우 크기가 2xlarge 이상이 되어야 합니다.

Note

Storage GatewayAMI는 Intel 또는 AMD 프로세서를 사용하는 x86 기반 인스턴스와만 호환됩니다. ARMGraviton 프로세서를 사용하는 기반 인스턴스는 지원되지 않습니다.

Tape Gateway 의 경우 Amazon EC2 인스턴스는 게이트웨이에 사용할 캐시 크기에 RAM 따라 다음과 같은 양의 를 사용해야 합니다.

- 캐시 크기가 최대 16GiB RAM TiB
- 캐시 크기가 16TiBGiBTiB RAM
- 캐시 크기가 32TiBGiBTiB RAM

게이트웨이 유형에 대한 권장 인스턴스 유형 중 하나를 사용합니다.

캐시 볼륨 및 Tape Gateway 유형별 권장 사항

- 범용 인스턴스 패밀리 – m4, m5 또는 m6 인스턴스 유형.

Note

m4.16xlarge 인스턴스 유형은 사용하지 않는 것이 좋습니다.

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

스토리지 요구 사항

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

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)	업로드 버퍼 (최소값)	업로드 버퍼 (최대값)	필요한 다른 로컬 디스크
Tape Gateway	150GiB	64TiB	150GiB	2TiB	—

Note

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

게이트웨이 할당량에 대한 자세한 내용은 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.

네트워크 및 방화벽 요구 사항

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

Note

경우에 따라 Amazon에 Storage Gateway를 배포EC2하거나 AWS IP 주소 범위를 제한하는 네트워크 보안 정책과 함께 다른 유형의 배포(온프레미스 포함)를 사용할 수 있습니다. 이러한 경우 AWS IP 범위 값이 변경될 때 게이트웨이에 서비스 연결 문제가 발생할 수 있습니다. 사용해야 하는 AWS IP 주소 범위 값은 게이트웨이를 활성화하는 AWS 리전의 Amazon 서비스 하위 집합에 있습니다. 현재 IP 범위 값은 AWS 일반 참조에서 [AWS IP 주소 범위](#)를 참조하세요.

Note

네트워크 대역폭 요구 사항은 게이트웨이가 업로드하고 다운로드하는 데이터 양에 따라 달라집니다. 게이트웨이를 성공적으로 다운로드, 활성화 및 업데이트하려면 최소 100Mbps가 필요

합니다. 데이터 전송 패턴에 따라 워크로드 지원에 필요한 대역폭이 결정됩니다. 경우에 따라 Amazon에 Storage Gateway를 배포EC2하거나 다른 유형의 배포를 사용할 수 있습니다.

주제

- [포트 요구 사항](#)
- [Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항](#)
- [방화벽 및 라우터를 통한 AWS Storage Gateway 액세스 허용](#)
- [Amazon EC2 게이트웨이 인스턴스의 보안 그룹 구성](#)

포트 요구 사항

Storage Gateway가 작동하려면 특정 포트가 허용되어야 합니다. 다음 그림은 각 게이트웨이 유형에 대해 허용해야 하는 필수 포트를 보여줍니다. 일부 포트는 모든 유형의 게이트웨이에 필요하고, 기타 일부는 특정 유형의 게이트웨이에 필요합니다. 포트 요구 사항에 대한 자세한 내용은 [Tape Gateway에 대한 포트 요구 사항](#) 단원을 참조하십시오.

모든 게이트웨이 유형에 대한 공통 포트

다음 포트는 공통이기 때문에 모든 유형의 게이트웨이에 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
TCP	443(HTTPS)	아웃바운드	Storage Gateway	AWS	Storage Gateway에서 AWS 서비스 엔드포인트로의 통신용입니다. 서비스 엔드포인트에 대한 자세한 내용은 방화벽 및 라우터를 통한 AWS Storage Gateway 액세스

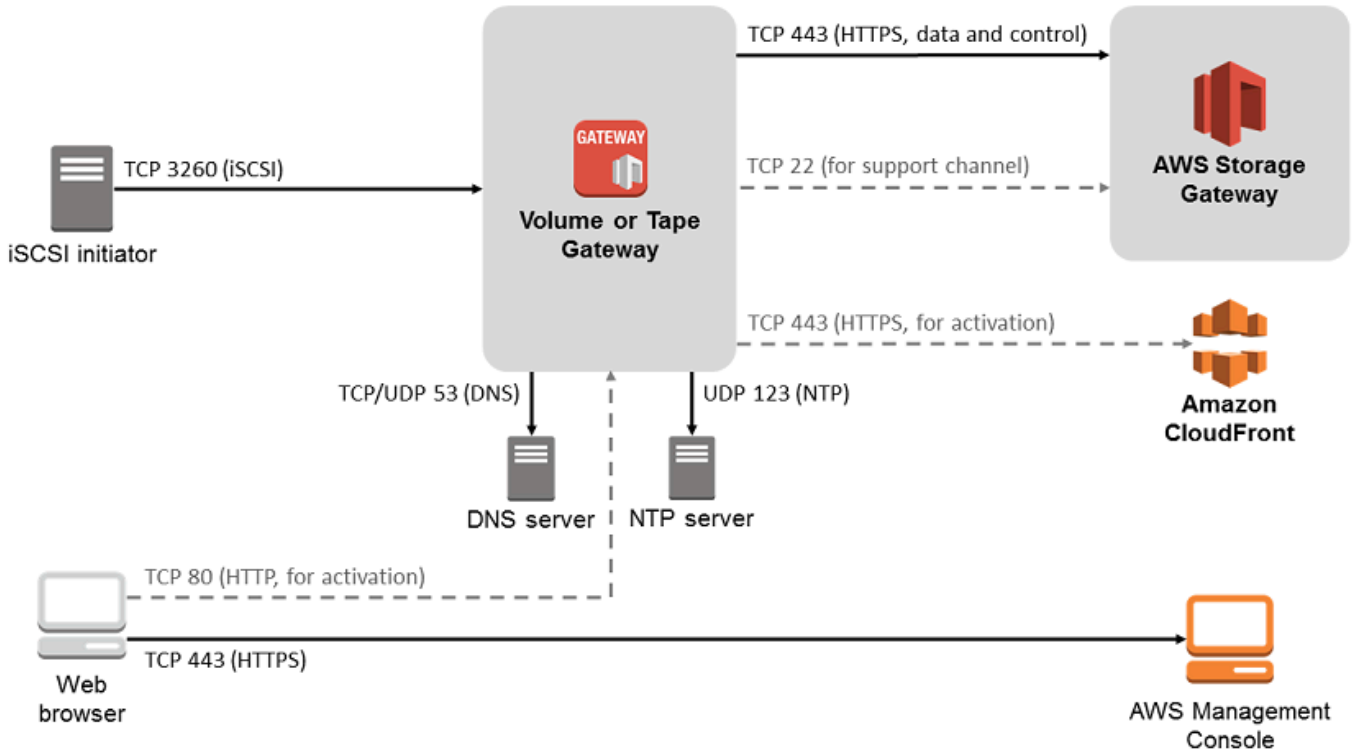
프로토콜	Port	Direction	소스	대상	용도
					세스 허용 단 원을 참조하 십시오.

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

프로토콜	Port	Direction	소스	대상	용도
					게이트웨이의 포트 80에 액세스할 수 있어야 합니다.
TCP/UDP	53(DNS)	아웃바운드	Storage Gateway	도메인 이름 서비스(DNS) 서버	Storage Gateway와 DNS 서버 간의 통신용입니다.
TCP	22(지원 채널)	아웃바운드	Storage Gateway	AWS Support	AWS Support가 게이트웨이에 액세스하여 게이트웨이 문제를 해결할 수 있도록 허용합니다. 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.

Volume Gateway 및 Tape Gateway용 포트

다음은 Tape Gateway용으로 개방할 포트를 보여줍니다.



공통 포트 외에 Tape Gateway에는 다음 포트가 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
TCP	3260(iSCSI)	인바운드	iSCSI 이니시 에이터	Storage Gateway	로컬 시스템 에서 게이트 웨이에 의해 노출된 iSCSI 대상에 연결 합니다.

포트 요구 사항에 대한 자세한 내용은 추가 Storage Gateway 리소스 섹션에서 [Tape Gateway에 대한 포트 요구 사항](#)을 참조하세요.

Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항

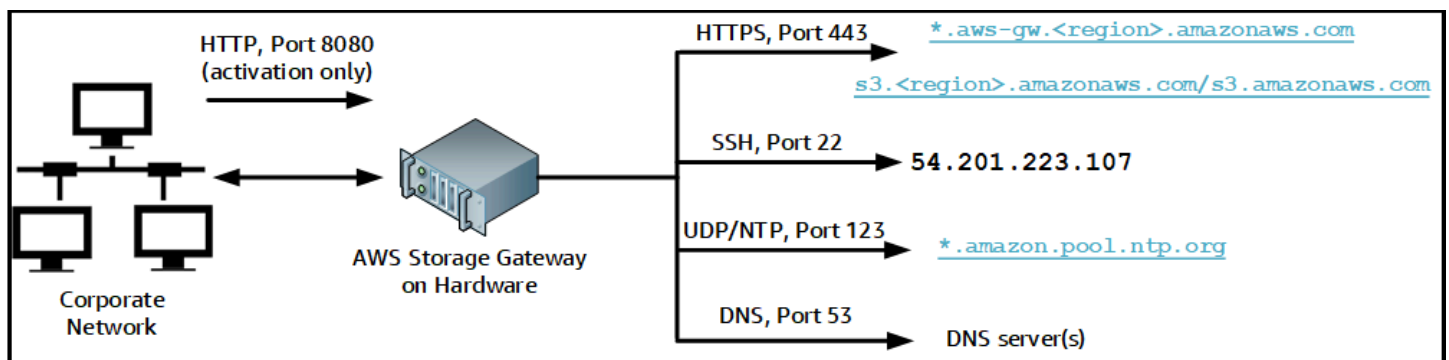
각 Storage Gateway 하드웨어 어플라이언스에는 다음과 같은 네트워크 서비스가 필요합니다.

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

원격 서버 관리에 iDRAC 포트를 사용할 수 있습니다.



하드웨어 어플라이언스를 작동하려면 다음 포트가 필요합니다.

프로토콜	Port	Direction	소스	대상	용도
SSH	22	아웃바운드	하드웨어 어플라이언스	54.201.22 3.107	지원 채널
DNS	53	아웃바운드	하드웨어 어플라이언스	DNS 서버	이름 확인
UDP/NTP	123	아웃바운드	하드웨어 어플라이언스	*.amazon. pool.ntp. org	시간 동기화
HTTPS	443	아웃바운드	하드웨어 어플라이언스	*.amazonaws.com	데이터 전송
HTTP	8080	인바운드	AWS	하드웨어 어플라이언스	활성화(잠시 동안)

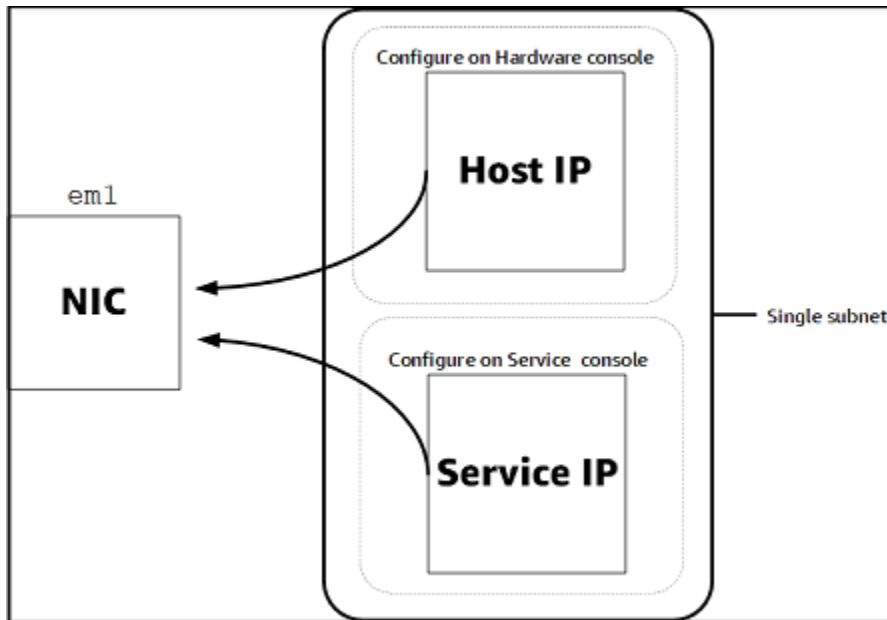
하드웨어 어플라이언스는 설계상 다음과 같은 네트워크 및 방화벽 설정이 필요합니다.

- 하드웨어 콘솔에서 연결된 모든 네트워크 인터페이스를 구성합니다.
- 각 네트워크 인터페이스는 고유한 서브넷에 있어야 합니다.
- 연결된 모든 네트워크 인터페이스에 위의 그림에 나와 있는 엔드포인트에 대한 아웃바운드 액세스를 제공합니다.
- 하드웨어 어플라이언스를 지원하는 네트워크 인터페이스를 한 개 이상 구성합니다. 자세한 내용은 [하드웨어 어플라이언스 네트워크 파라미터 구성](#) 단원을 참조하십시오.

Note

서버 뒷면과 포트가 나와 있는 그림을 보려면 [하드웨어 어플라이언스 물리적 설치](#) 단원을 참조하십시오.

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



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

방화벽 및 라우터를 통한 AWS Storage Gateway 액세스 허용

와 통신하려면 게이트웨이에서 다음 서비스 엔드포인트에 액세스해야 합니다 AWS. 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다.

Note

Storage Gateway가 와 주고받는 연결 및 데이터 전송에 사용하도록 프라이빗 VPC 엔드포인트를 구성하는 경우 AWS게이트웨이는 퍼블릭 인터넷에 액세스할 필요가 없습니다. 자세한 내용은 [Virtual Private Cloud\(VPC\)에서 게이트웨이 활성화](#)를 참조하세요.

Important

게이트웨이의 AWS 리전에 따라 를 바꿉니다. *region* 올바른 리전 문자열을 사용하여 서비스 엔드포인트에서.

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

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

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

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

API 전화를 걸려면 다음 게이트웨이 서비스 엔드포인트가 필요합니다.

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

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

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

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

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

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

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

Note

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

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

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

다음 예제는 AWS GovCloud (미국 서부) 리전의 S3 버킷에 대한 FIPS 서비스 엔드포인트입니다.

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

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
```

- Storage Gateway - Storage Gateway 에 사용할 수 있는 지원되는 AWS 리전 및 AWS 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량을](#) 참조하세요AWS 일반 참조.
- Storage Gateway 하드웨어 어플라이언스 - 하드웨어 어플라이언스와 함께 사용할 수 있는 지원되는 AWS 리전의 경우 의 [Storage Gateway 하드웨어 어플라이언스 리전](#)을 참조하세요AWS 일반 참조.

Amazon EC2 게이트웨이 인스턴스의 보안 그룹 구성

보안 그룹은 Amazon EC2 게이트웨이 인스턴스로의 트래픽을 제어합니다. 보안 그룹을 구성할 때는 다음을 수행하는 것이 좋습니다.

- 보안 그룹은 외부 인터넷에서 들어오는 연결을 허용해서는 안 됩니다. 게이트웨이 보안 그룹 내 인스턴스만 게이트웨이와 통신할 수 있도록 허용해야 합니다. 인스턴스가 보안 그룹 외부에서 게이트웨이에 연결되도록 허용해야 하는 경우 포트 3260(iSCSI 연결의 경우) 및 80(활성화의 경우)에서만 연결을 허용하는 것이 좋습니다.
- 게이트웨이 보안 그룹 외부의 Amazon EC2 호스트에서 게이트웨이를 활성화하려면 해당 호스트의 IP 주소에서 포트 80의 수신 연결을 허용하세요. 활성화 호스트의 IP 주소를 확인할 수 없는 경우에는 포트 80을 열어 게이트웨이를 활성화하고 활성화가 완료되면 포트 80에 대한 액세스를 종료하는 방법을 사용할 수 있습니다.
- 문제 해결을 AWS Support 위해 를 사용하는 경우에만 포트 22 액세스를 허용합니다. 자세한 내용은 [게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2](#) 단원을 참조하십시오.

경우에 따라 Amazon EC2 인스턴스를 시작자(즉, Amazon 에 배포한 게이트웨이의 iSCSI 대상에 연결하기 위해)로 사용할 수 있습니다EC2. 이러한 경우 2단계 접근 방식을 권장합니다.

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

게이트웨이 용도로 개방하는 포트에 대한 자세한 내용은 [Tape Gateway에 대한 포트 요구 사항](#) 단원을 참조하십시오.

지원되는 하이퍼바이저 및 호스트 요구 사항

Storage Gateway 온프레미스를 가상 머신(VM) 어플라이언스 또는 물리적 하드웨어 어플라이언스로 실행하거나 에서 Amazon EC2 인스턴스 AWS 로 실행할 수 있습니다.

Note

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

Storage Gateway에서 지원하는 하이퍼바이저 버전 및 호스트는 다음과 같습니다.

- VMware ESXi 하이퍼바이저(버전 7.0 또는 8.0) - 이 설정의 경우 호스트에 연결하려면 VMware vSphere 클라이언트도 필요합니다.
- Microsoft Hyper-V Hypervisor(버전 2012 R2, 2016, 2019 또는 2022) – Hyper-V의 무료 독립형 버전은 [Microsoft 다운로드 센터](#)에서 받을 수 있습니다. 이 설정의 경우 호스트에 연결하려면 Microsoft Windows 클라이언트 컴퓨터에서 Microsoft Hyper-V Manager를 사용해야 합니다.
- Linux 커널 기반 가상 머신(KVM) - 무료 오픈 소스 가상화 기술입니다. KVM 는 Linux 버전 2.6.20 이상의 모든 버전에 포함됩니다. Storage Gateway는 CentOS /RHEL 7.7, Ubuntu 16.04 및 Ubuntu 18.04 LTS 배포에 대해 테스트LTS되고 지원됩니다. 다른 최신 Linux 배포판이 작동하지만 기능이나 성능이 보장되지는 않습니다. KVM 이미 환경이 실행 중이고 KVM 작동 방식에 이미 익숙한 경우 이 옵션을 사용하는 것이 좋습니다.
- Amazon EC2 인스턴스 - Storage Gateway는 게이트웨이 VM 이미지가 포함된 Amazon Machine Image(AMI)를 제공합니다. Amazon 에는 파일, 캐시된 볼륨 및 Tape Gateway 유형만 배포할 수 있습니다EC2. Amazon 에 게이트웨이를 배포하는 방법에 대한 자세한 내용은 섹션을 EC2참조하세요 [Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포](#).

- Storage Gateway 하드웨어 어플라이언스 - Storage Gateway는 제한된 가상 머신 인프라 위치에 대한 온프레미스 배포 옵션으로 물리적 하드웨어 어플라이언스를 제공합니다.

Note

Storage Gateway는 다른 게이트웨이 VM의 스냅샷 또는 복제본 또는 Amazon 에서 생성된 VM에서 게이트웨이 복구를 지원하지 않습니다. EC2AMI. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 새로운 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다. 자세한 내용은 [가상 머신이 예기치 않게 종료된 상황에서 복구하기](#) 단원을 참조하십시오.

Storage Gateway는 동적 메모리 및 가상 메모리 벌루닝(ballooning)을 지원하지 않습니다.

지원되는 iSCSI 이니시에이터

Tape Gateway를 배포할 때 게이트웨이는 미디어 체인저 1개와 테이프 드라이브 10개로 사전 구성됩니다. 이러한 테이프 드라이브와 미디어 체인저는 기존 클라이언트 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있습니다.

이러한 iSCSI 디바이스에 연결하기 위해 Storage Gateway는 다음 iSCSI 이니시에이터를 지원합니다.

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows 10
- Windows 8.1
- Red Hat Enterprise Linux 5
- Red Hat Enterprise Linux 6
- Red Hat Enterprise Linux 7
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX 이니시에이터 - 의 게스트 운영 체제에서 이니시에이터를 사용하는 대신 사용할 수 있습니다. VMs

⚠ Important

Storage Gateway는 Windows 클라이언트의 Microsoft 다중 경로 I/O(MPIO)를 지원하지 않습니다.


Storage Gateway는 호스트가 Windows Server 장애 조치 클러스터링()을 사용하여 액세스를 조정하는 경우 여러 호스트를 동일한 볼륨에 연결하는 것을 지원합니다. 그러나 WSFC를 사용하지 않으면 동일한 볼륨에 여러 호스트를 연결할 수 없습니다(예: 클러스터링되지 않은 NTFS/ext4 파일 시스템 공유). WSFC

Tape Gateway에 지원되는 타사 백업 애플리케이션

백업 애플리케이션을 사용하여 Tape Gateway로 테이프에 대한 읽기, 쓰기 및 관리 작업을 수행할 수 있습니다. Tape Gateway와 함께 작동하도록 지원되는 타사 백업 애플리케이션은 다음과 같습니다.

선택할 미디어 체인저의 유형은 사용하려고 계획한 백업 애플리케이션에 따라 달라집니다. 다음 표는 테스트를 통해 Tape Gateway와 호환되는 것으로 확인된 타사 백업 애플리케이션의 목록입니다. 이 표에는 각 백업 애플리케이션에 권장되는 미디어 체인저 유형도 수록되어 있습니다.

백업 애플리케이션	미디어 체인저 유형
Arcserve 백업	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL 또는 STK-L700
Commvault V11	STK-L700
Dell EMC NetWorker 19.5	AWS-Gateway-VTL
IBM Spectrum Protect v8.1.10	IBM-03584L32-0402
마이크로 포커스(HPE) 데이터 보호기 9 또는 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 또는 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/네트워크 6.4 또는 7.1	STK-L700

백업 애플리케이션	미디어 체인저 유형
Quest NetVault Backup 12.4 또는 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014, 15, 16, 20 또는 22.x	AWS-Gateway-VTL
Veritas Backup Exec 2012	STK-L700
<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note Veritas는 Backup Exec 2012에 대한 지원을 종료했습니다.</p> </div>	
Veritas NetBackup 버전 7.x 또는 8.x	AWS-Gateway-VTL

Important

사용 중인 백업 애플리케이션에 대해 나열되는 미디어 체인저를 선택할 것을 강력하게 권장합니다. 다른 미디어 체인저를 선택하면 올바르게 작동하지 않을 수 있습니다. 게이트웨이가 활성화된 후에는 다른 미디어 체인저를 선택할 수 있습니다. 자세한 내용은 [게이트웨이 활성화 후 미디어 체인저 선택](#)을 참조하세요.

Storage Gateway 하드웨어 어플라이언스 사용

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

하드웨어 어플라이언스는 고성능 1U 서버로, 데이터 센터 또는 회사 방화벽 내 온프레미스에 배포할 수 있습니다. 하드웨어 어플라이언스를 구매하고 활성화하면 활성화 프로세스가 하드웨어 어플라이언스와 연결합니다 AWS 계정. 활성화 후 하드웨어 어플라이언스 개요 페이지의 콘솔에 하드웨어 어플라이언스가 나타납니다. 하드웨어 어플라이언스를 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway 유형으로 구성할 수 있습니다. 하드웨어 어플라이언스에 이러한 게이트웨이 유형을 배포하는 데 사용하는 절차는 가상 플랫폼과 동일합니다.

Storage Gateway 하드웨어 어플라이언스를 활성화하고 사용할 수 AWS 리전 있는 지원되는 목록은 [Storage Gateway 하드웨어 어플라이언스 리전](#)을 참조하세요 AWS 일반 참조.

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

주제

- [Storage Gateway 하드웨어 어플라이언스 설정](#)
- [하드웨어 어플라이언스 물리적 설치](#)
- [하드웨어 어플라이언스 콘솔 액세스](#)
- [하드웨어 어플라이언스 네트워크 파라미터 구성](#)
- [Storage Gateway 하드웨어 어플라이언스 활성화](#)
- [하드웨어 어플라이언스에서 게이트웨이 생성](#)
- [하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성](#)
- [하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거](#)
- [Storage Gateway 하드웨어 어플라이언스 삭제](#)

Storage Gateway 하드웨어 어플라이언스 설정

Storage Gateway 하드웨어 어플라이언스를 수신한 후 하드웨어 어플라이언스 로컬 콘솔을 사용하여 어플라이언스에 상시 연결을 제공하고 어플라이언스를 AWS 활성화하도록 네트워킹을 구성합니다. 활성화는 어플라이언스를 활성화 프로세스 중에 사용되는 AWS 계정과 연결합니다. 어플라이언스

가 활성화되면 Storage Gateway 콘솔에서 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway를 시작할 수 있습니다.

하드웨어 어플라이언스를 설치하고 구성하려면

1. 어플라이언스를 랙 마운팅하고 전원과 네트워크 연결을 가동합니다. 자세한 내용은 [하드웨어 어플라이언스 물리적 설치](#) 단원을 참조하십시오.
2. 하드웨어 어플라이언스(호스트IPv4)의 인터넷 프로토콜 버전 4() 주소를 설정합니다. 자세한 내용은 [하드웨어 어플라이언스 네트워크 파라미터 구성](#) 단원을 참조하십시오.
3. 선택한 AWS 리전의 콘솔 하드웨어 어플라이언스 개요 페이지에서 하드웨어 어플라이언스를 활성화합니다. 자세한 내용은 [Storage Gateway 하드웨어 어플라이언스 활성화](#) 단원을 참조하십시오.
4. 하드웨어 어플라이언스에서 게이트웨이를 생성합니다. 자세한 내용은 [Tape Gateway 생성 및 활성화](#) 단원을 참조하십시오.

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

사용 가능한 캐시 스토리지 증가

하드웨어 어플라이언스의 사용 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있습니다. 이렇게 하면 의 데이터에 대한 짧은 지연 시간 액세스를 위한 더 큰 캐시가 제공됩니다 AWS. 5TB 모델을 주문한 경우 1.92TBSSDs(솔리드 스테이트 드라이브) 5개를 구매하여 사용 가능한 스토리지를 12TB로 늘릴 수 있습니다.

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

1. 하드웨어 어플라이언스를 초기 설정으로 재설정합니다. 이 작업을 수행하는 방법에 대한 지침은 AWS 지원 부서에 문의하세요.
2. 어플라이언스에 1.92TBSSDs를 5개 추가합니다.

네트워크 인터페이스 카드 옵션

주문한 어플라이언스 모델에 따라 10G-Base-T RJ45 구리, 10G DA/SFP+, or 25G DA/SFP28 네트워크 카드가 함께 제공될 수 있습니다.

- 10G-Base-T NIC 구성:
 - 10G용 CAT6 케이블 또는 1G용 CAT5(e) 사용
- 10G DA/SFP+ NIC 구성:
 - Twinax 구리 직접 연결 케이블(최대 5m) 사용
 - Dell/Intel 호환 SFP+ 광학 모듈(SR 또는 LR)
 - SFP1 G-Base-T 또는 10G-Base-T용 /SFP+ 구리 트랜시버
- 25G DA/SFP28 NIC 구성:
 - Twinax 구리 직접 연결 케이블(최대 5m) 사용
 - 25G 또는 10G 광학 모듈(SR 또는 LR)
 - SFP+ 10G-Base-T용 구리 트랜시버

하드웨어 어플라이언스 물리적 설치

어플라이언스에는 1U 폼 팩터가 있으며 표준 국제 전기 기술 위원회(IEC) 규정 준수 19인치 랙에 적합합니다.

사전 조건

하드웨어 어플라이언스를 설치하려면 다음 구성 요소가 필요합니다.

- 전원 케이블: 1개 필요, 2개 권장.
- 지원되는 네트워크 케이블링(하드웨어 어플라이언스에 포함된 네트워크 인터페이스 카드(NIC)에 따라 다름).
- 키보드 및 모니터 또는 키보드, 비디오 및 마우스(KVM) 스위치 솔루션.

Note

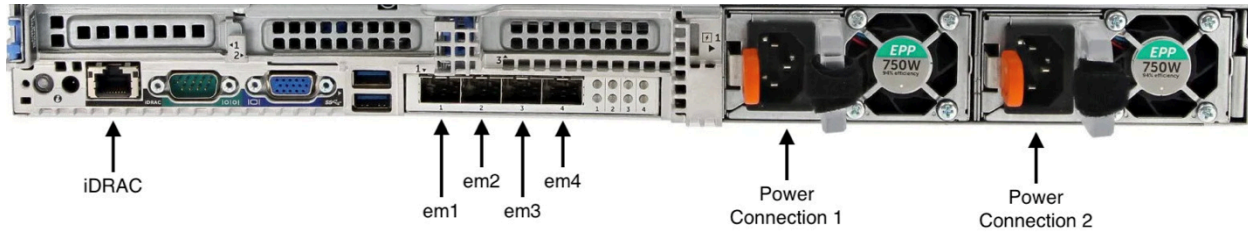
다음 절차를 수행하기 전에 [Storage Gateway 하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항](#)에 설명된 대로 Storage Gateway 하드웨어 어플라이언스에 대한 요구 사항을 모두 충족하는지 확인하세요.

하드웨어 어플라이언스를 물리적으로 설치하려면

1. 하드웨어 어플라이언스의 상자를 풀고 상자에 포함된 지침에 따라 서버를 랙 마운트합니다.

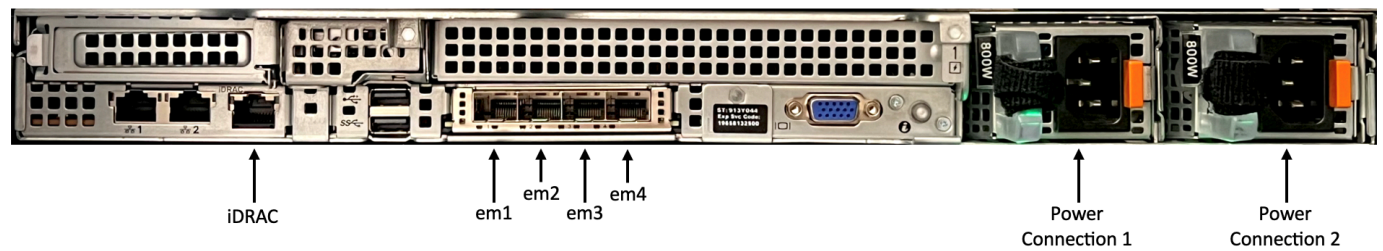
다음 이미지는 전원, 이더넷, 모니터, USB 키보드 및 i를 연결하기 위한 포트가 있는 하드웨어 어플라이언스의 뒷면을 보여줍니다. DRAC. 보유한 어플라이언스 모델에 따라 적절한 이미지를 참조하십시오.

네트워크 및 전원 커넥터 레이블이 있는 하드웨어 어플라이언스 1개 후면.



네트워크 및 전원 커넥터 레이블이 있는 하드웨어 어플라이언스 1개 후면.

네트워크 및 전원 커넥터 레이블이 있는 하드웨어 어플라이언스 2개 후면.



네트워크 및 전원 커넥터 레이블이 있는 하드웨어 어플라이언스 2개 후면.

- 2개의 전원 공급 장치 각각에 전원을 연결합니다. 하나의 전원 연결에만 연결할 수 있지만 중복성을 위해 두 전원 공급 장치에 전원 연결을 사용하는 것이 좋습니다.
- 이더넷 케이블을 em1 포트에 연결하여 상시 인터넷 연결을 제공합니다. em1 포트는 뒷면에 있는 4개의 물리 네트워크 포트 중 첫 번째(왼쪽에서 오른쪽으로)입니다.

Note

하드웨어 어플라이언스는 트VLAN링킹을 지원하지 않습니다. 하드웨어 어플라이언스를 비트링크 포트에 연결하는 스위치 VLAN 포트를 설정합니다.

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



전원 버튼 레이블이 표시된 하드웨어 어플라이언스 전면입니다.

다음 단계

[하드웨어 어플라이언스 콘솔 액세스](#)

하드웨어 어플라이언스 콘솔 액세스

하드웨어 어플라이언스의 전원을 켜면 하드웨어 어플라이언스 콘솔이 모니터에 나타납니다. 하드웨어 어플라이언스 콘솔은 관리자 암호를 설정하고, 초기 네트워크 파라미터를 구성하고, 에 대한 지원 채널을 여는 데 사용할 수 있는 고유한 사용자 인터페이스를 제공합니다.

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

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

관리자 암호를 설정하려면

- 로그인 암호 설정 프롬프트에서 다음을 수행합니다.
 - a. 암호 설정에서 암호를 입력하고 Down arrow 키를 누릅니다.
 - b. 확인에서 암호를 재입력하고 암호 저장을 선택합니다.

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

- 네트워크 구성

- 서비스 콘솔 열기
- 비밀번호 변경
- 로그아웃
- 지원 콘솔 열기

다음 단계

[하드웨어 어플라이언스 네트워크 파라미터 구성](#)

하드웨어 어플라이언스 네트워크 파라미터 구성

하드웨어 어플라이언스가 부팅되고 에 설명된 대로 하드웨어 콘솔에서 관리자 사용자 암호를 설정한 후 다음 절차에 [하드웨어 어플라이언스 콘솔 액세스](#) 따라 하드웨어 어플라이언스가 에 연결할 수 있도록 네트워크 파라미터를 구성합니다 AWS.

네트워크 주소를 설정하려면

1. 홈 페이지에서 네트워크 구성을 선택한 다음 를 누릅니다Enter. 네트워크 구성 페이지가 나타납니다. 네트워크 구성 페이지에는 하드웨어 어플라이언스의 4개 네트워크 인터페이스 각각에 대한 IP 및 DNS 정보가 표시되며, 각각에 대해 DHCP 또는 정적 주소를 구성하는 메뉴 옵션이 포함되어 있습니다.
2. em1 인터페이스의 경우 다음 중 하나를 수행합니다.
 - DHCP 를 선택하고 Enter 를 눌러 동적 호스트 구성 프로토콜(DHCP) 서버에서 물리적 네트워크 포트에 할당한 IPv4 주소를 사용합니다.

나중에 활성화 단계에서 사용할 수 있도록 이 주소를 기록해 둡니다.

- 정적을 선택하고 Enter를 눌러 정적 IPv4 주소를 구성합니다.

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

완료되면 저장을 선택한 다음 Enter 를 눌러 구성을 저장합니다.

Note

이 절차를 사용하여 em1 외에 다른 네트워크 인터페이스를 구성할 수 있습니다. 다른 인터페이스를 구성하는 경우 요구 사항에 나열된 AWS 엔드포인트에 동일한 상시 연결을 제공해야 합니다.

네트워크 결합 및 링크 집계 제어 프로토콜(LACP)은 하드웨어 어플라이언스 또는 Storage Gateway 에서 지원되지 않습니다.

라우팅 문제가 발생할 수 있으므로 동일한 서브넷에서 여러 네트워크 인터페이스를 구성하는 것은 권장하지 않습니다.

하드웨어 콘솔에서 로그아웃하려면

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

다음 단계

[Storage Gateway 하드웨어 어플라이언스 활성화](#)

Storage Gateway 하드웨어 어플라이언스 활성화

IP 주소를 구성한 후 AWS Storage Gateway 콘솔의 하드웨어 페이지에 이 IP 주소를 입력하여 하드웨어 어플라이언스를 활성화합니다. 활성화 프로세스는 어플라이언스를 계정에 AWS 등록합니다.

지원되는 에서 하드웨어 어플라이언스를 활성화하도록 선택할 수 있습니다 AWS 리전. 지원되는 의 목록은 의 [Storage Gateway 하드웨어 어플라이언스 리전](#)을 AWS 리전참조하세요AWS 일반 참조.

Storage Gateway 하드웨어 어플라이언스 활성화

1. [AWS Storage Gateway 관리 콘솔](#)을 열고 난 다음 하드웨어를 활성화하는 데 사용할 계정 보안 인증 정보로 로그인합니다.

Note

활성화를 위해서는 다음이 충족되어야 합니다.

- 브라우저가 하드웨어 어플라이언스와 동일한 네트워크에 있어야 합니다.
- 방화벽은 인바운드 트래픽을 위해 포트 8080에서 어플라이언스에 대한 HTTP 액세스를 허용해야 합니다.

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

IP 주소 구성에 대한 자세한 내용은 [네트워크 파라미터 구성](#) 섹션을 참조하십시오.

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

시간대는 하드웨어 업데이트가 수행되는 시간을 제어하며, 오전 2시가 기본 업데이트 예정 시간으로 사용됩니다. 시간대를 올바르게 설정하면 기본적으로 현지 근무일 시간 외에 업데이트가 이루어집니다.

7. 하드웨어 어플라이언스 세부 정보 섹션에서 활성화 파라미터를 검토하십시오. 필요한 경우 이전을 선택하여 돌아가서 변경할 수 있습니다. 그렇지 않으면 활성화를 선택하여 활성화를 완료하십시오.

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

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

다음 단계

[하드웨어 어플라이언스에서 게이트웨이 생성](#)

하드웨어 어플라이언스에서 게이트웨이 생성

배포의 모든 Storage Gateway 하드웨어 어플라이언스에서 S3 File Gateway, FSx File Gateway, Tape Gateway 또는 Volume Gateway를 생성할 수 있습니다.

하드웨어 어플라이언스에서 게이트웨이를 생성하려면

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/storagegateway/> [집에서](#) Storage Gateway 콘솔을 엽니다.
2. [게이트웨이 생성](#) 게이트웨이 에 설명된 절차에 따라 배포하려는 Storage Gateway 유형을 설정, 연결 및 구성합니다.

Storage Gateway 콘솔에서 게이트웨이 생성이 완료되면 Storage Gateway 소프트웨어가 하드웨어 어플라이언스에 자동으로 설치되기 시작합니다. 동적 호스트 구성 프로토콜(DHCP)을 사용하는 경우 게이트웨이가 콘솔에 온라인 상태로 표시되는 데 5~10분이 걸릴 수 있습니다. 설치된 게이트웨이에 정적 IP 주소를 할당하려면 [게이트웨이의 IP 주소 구성](#) 참조하세요.

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

다음 단계

[하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성](#)

하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성

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

애플리케이션에서 작동하도록 어플라이언스에서 IP 주소를 구성하려면

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

기본 계정은 admin이고 기본 암호는 password입니다.

Note

AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 게이트웨이 콘솔에 해당하는 번호를 입력한 다음 `passwd` 명령을 실행하여 기본 암호를 변경하는 것이 좋습니다. 명령을 실행하는 방법에 대한 정보는 [온프레미스 게이트웨이에 대해 로컬 콘솔에서 스토리지 게이트웨이 명령 실행](#) 섹션을 참조하십시오. Storage Gateway 콘솔에서 암호를 설정할 수도 있습니다. 자세한 내용은 [Storage Gateway 콘솔에서 로컬 콘솔 암호 설정](#) 단원을 참조하십시오.

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

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

Note

일부 옵션은 특정 게이트웨이 유형 또는 호스트 플랫폼에만 표시됩니다.

해당하는 숫자를 입력하여 네트워크 구성 페이지로 이동합니다.

4. 게이트웨이 IP 주소를 구성하려면 다음 중 하나를 수행합니다.

- 동적 호스트 구성 프로토콜(DHCP) 서버에서 할당한 IP 주소를 사용하려면 구성DHCP에 해당하는 숫자를 입력한 다음 다음 다음 페이지에서 유효한 DHCP 구성 정보를 입력합니다.
- 정적 IP 주소를 할당하려면 정적 IP 구성에 해당하는 숫자를 입력한 다음 다음 페이지에 유효한 IP 주소와 DNS 정보를 입력합니다.

Note

여기에서 지정하는 IP 주소는 하드웨어 어플라이언스 활성화 중에 사용되는 IP 주소와 동일한 서브넷에 있어야 합니다.

게이트웨이 로컬 콘솔을 종료하려면

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

Note

키 입력을 통해서만 게이트웨이 로컬 콘솔을 종료할 수 있습니다.

하드웨어 어플라이언스가 활성화되고 구성되면 콘솔에 어플라이언스가 나타납니다. 이제 Storage Gateway 콘솔에서 게이트웨이의 설정 및 구성 절차를 계속할 수 있습니다. 지침은 단원을 참조하세요.

하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거

하드웨어 어플라이언스에 배포한 특정 Storage Gateway가 더 이상 필요하지 않은 경우 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거할 수 있습니다. 게이트웨이 소프트웨어를 제거한 후 새 게이트웨이를 배포하거나 Storage Gateway 콘솔에서 하드웨어 어플라이언스 자체를 삭제하도록 선택할 수 있습니다. 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거하려면 다음 절차를 수행합니다.

하드웨어 어플라이언스에서 게이트웨이를 제거하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 콘솔 페이지 왼쪽의 탐색 창에서 하드웨어를 선택한 다음 게이트웨이 소프트웨어를 제거할 어플라이언스의 하드웨어 어플라이언스 이름을 선택합니다.
3. 작업 드롭다운 메뉴에서 게이트웨이 제거 를 선택합니다.

확인 대화 상자가 표시됩니다.

4. 지정된 하드웨어 어플라이언스에서 게이트웨이 소프트웨어를 제거할지 확인한 다음 **remove** 확인 상자에 단어를 입력합니다.
5. 제거를 선택하여 게이트웨이 소프트웨어를 영구적으로 제거합니다.

Note

게이트웨이 소프트웨어를 제거한 후에는 작업을 취소할 수 없습니다. 특정 게이트웨이 유형의 경우 삭제 시 데이터 특히, 캐싱된 데이터를 잃을 수 있습니다. 게이트웨이 삭제에 대한 자세한 내용은 [게이트웨이 삭제 및 관련 리소스 제거](#) 단원을 참조하십시오.

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

Storage Gateway 하드웨어 어플라이언스 삭제

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

Note

어플라이언스를 다른 AWS 계정 또는 로 이동하려면 먼저 다음 절차에 따라 어플라이언스를 삭제한 다음 게이트웨이의 지원 채널을 열고 AWS Support 에 문의하여 소프트웨어 재설정을 수행해야 AWS 리전합니다. 자세한 내용은 [온프레미스에서 호스팅되는 게이트웨이 문제를 해결하려면 AWS Support 액세스 켜기 온프레미스](#).

하드웨어 어플라이언스를 삭제하려면

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

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

게이트웨이 생성

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

- [Amazon S3 File Gateway 생성 및 활성화](#)
- [Amazon FSx File Gateway 생성 및 활성화](#)
- [Tape Gateway 생성 및 활성화](#)
- [Volume Gateway 생성 및 활성화](#)

Important

AWS Storage Gateway의 FSx File Gateway는 10/28/24부터 더 이상 신규 고객이 사용할 수 없습니다. 서비스를 사용하려면 해당 날짜 이전에 가입해야 합니다. FSx File Gateway의 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. FSx File Gateway와 유사한 기능은 [이 블로그 게시물을](#) 참조하세요.

개요 - 게이트웨이 활성화

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

게이트웨이 설정

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

에 연결 AWS

다음 단계는 게이트웨이를 AWS에 연결하는 것입니다. 이렇게 하려면 먼저 게이트웨이 가상 어플라이언스와 클라우드의 서비스 간의 통신에 사용할 AWS 서비스 엔드포인트 유형을 선택합니다. 이 엔드포

인트는 퍼블릭 인터넷 또는 네트워크 보안 구성을 완전히 제어할 수 VPC있는 Amazon 내에서만 액세스할 수 있습니다. 그런 다음 게이트웨이의 IP 주소 또는 정품 인증 키를 지정합니다. 이 정보는 게이트웨이 어플라이언스의 로컬 콘솔에 연결하여 얻을 수 있습니다.

검토 및 활성화

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

개요 - 게이트웨이 구성

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

개요 - 스토리지 리소스

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

Tape Gateway 생성 및 활성화

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

주제

- [Tape Gateway 설정](#)
- [Tape Gateway를 에 연결 AWS](#)
- [설정 검토 및 Tape Gateway 활성화](#)
- [Tape Gateway 구성](#)

Tape Gateway 설정

새 Tape Gateway를 설정하려면

1. AWS Management Console <https://console.aws.amazon.com/storagegateway/홈/>에서 를 열고 게이트웨이를 생성할 AWS 리전 를 선택합니다.
2. 게이트웨이 생성을 선택하여 게이트웨이 설정 페이지를 엽니다.
3. 게이트웨이 설정 섹션에서 다음을 수행합니다.
 - a. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 이 이름으로 검색하면 Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 찾을 수 있습니다.
 - b. 게이트웨이 표준 시간대에서 게이트웨이를 배포하려는 전 세계 지역의 현지 시간대를 선택합니다.
4. 게이트웨이 옵션 섹션의 게이트웨이 유형에서 Tape Gateway를 선택합니다.
5. 플랫폼 옵션 섹션에서 다음을 수행합니다.
 - a. 호스트 플랫폼에서 게이트웨이를 배포할 플랫폼을 선택한 다음 Storage Gateway 콘솔 페이지에 표시되는 플랫폼별 지침에 따라 호스트 플랫폼을 설정합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - VMware ESXi - VMware 를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다ESXi.
 - Microsoft Hyper-V - Microsoft Hyper-V를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
 - Linux KVM - Linux 를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다 KVM.
 - Amazon EC2 - 게이트웨이를 호스팅할 Amazon EC2 인스턴스를 구성하고 시작합니다. 저장 볼륨 게이트웨이에는 이 옵션을 사용할 수 없습니다.
 - 하드웨어 어플라이언스 - 에서 전용 물리적 하드웨어 어플라이언스를 주문 AWS 하여 게이트웨이를 호스팅합니다.
 - b. 게이트웨이 설정 확인의 확인란을 선택하여 선택한 호스트 플랫폼에 대한 배포 단계를 수행했는지 확인합니다. 하드웨어 어플라이언스 호스트 플랫폼에는 이 단계가 해당되지 않습니다.
6. 백업 애플리케이션 설정 섹션의 백업 애플리케이션에서 Tape Gateway와 연결된 가상 테이프에 테이프 데이터를 백업하는 데 사용할 애플리케이션을 선택합니다.

7. 다음을 선택하여 계속 진행합니다.

이제 게이트웨이가 설정되었으므로 와 연결하고 통신할 방법을 선택해야 합니다 AWS. 지침은 [Tape Gateway를 에 연결을 참조하세요 AWS](#).

Tape Gateway를 에 연결 AWS

새 Tape Gateway를 에 연결하려면 AWS

1. [Tape Gateway 설정](#)에 설명된 절차를 아직 완료하지 않은 경우 해당 절차를 완료합니다. 완료했으면 다음을 선택하여 Storage Gateway 콘솔에서 AWS에 연결 페이지를 엽니다.
2. 엔드포인트 옵션 섹션의 서비스 엔드포인트 에서 게이트웨이가 와 통신하는 데 사용할 엔드포인트 유형을 선택합니다 AWS. 다음 옵션 중에서 선택할 수 있습니다.
 - 퍼블릭 액세스 - 게이트웨이는 퍼블릭 인터넷을 AWS 통해 와 통신합니다. 이 옵션을 선택하면 FIPS 활성화된 엔드포인트 확인란을 사용하여 연결이 연방 정보 처리 표준()을 준수해야 하는지 여부를 지정합니다FIPS.

Note

명령줄 인터페이스 또는 FIPS 를 AWS 통해 에 액세스할 때 140-2개의 검증된 암호화 모듈이 필요한 경우 FIPS규정을 준수하는 엔드포인트를 API사용합니다. 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-2](#)를 참조하세요.

FIPS 서비스 엔드포인트는 일부 AWS 리전에서만 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

- VPC 호스팅 - 게이트웨이는 와의 프라이빗 연결을 AWS 통해 와 통신VPC하므로 네트워크 설정을 제어할 수 있습니다. 이 옵션을 선택하는 경우 드롭다운 메뉴에서 VPC 엔드포인트 ID를 선택하거나 VPC 엔드포인트 DNS 이름 또는 IP 주소를 제공하여 기존 VPC 엔드포인트를 지정해야 합니다. 자세한 내용은 [가상 프라이빗 클라우드에서 게이트웨이 활성화를 참조하세요](#).
3. 게이트웨이 연결 옵션 섹션의 연결 옵션에서 AWS에 대한 게이트웨이를 식별하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - IP 주소 - 해당 필드에 게이트웨이의 IP 주소를 입력합니다. 이 IP 주소는 공용이거나 현재 네트워크 내에서 액세스할 수 있어야 하며 웹 브라우저에서 연결할 수 있어야 합니다.

게이트웨이 IP 주소는 하이퍼바이저 클라이언트에서 게이트웨이의 로컬 콘솔에 로그인하거나 Amazon EC2 인스턴스 세부 정보 페이지에서 복사하여 얻을 수 있습니다.

- 정품 인증 키 - 해당 필드에 게이트웨이의 정품 인증 키를 입력합니다. 게이트웨이의 로컬 콘솔을 사용하여 정품 인증 키를 생성할 수 있습니다. 게이트웨이의 IP 주소를 사용할 수 없는 경우 이 옵션을 선택합니다.
4. 다음을 선택하여 계속 진행합니다.

게이트웨이를 에 연결하는 방법을 선택했으므로 게이트웨이를 활성화 AWS해야 합니다. 지침은 [설정 검토 및 Tape Gateway 활성화](#)를 참조하세요.

설정 검토 및 Tape Gateway 활성화

새 Tape Gateway를 활성화하려면

1. 다음 주제에 설명된 절차를 아직 완료하지 않은 경우 완료합니다.
 - [Tape Gateway 설정](#)
 - [Tape Gateway를 에 연결 AWS](#)

완료했다면 다음을 선택하여 Storage Gateway 콘솔에서 검토 및 활성화 페이지를 엽니다.

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

Note

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

4. 게이트웨이 활성화를 선택하여 계속 진행합니다.

게이트웨이를 활성화했으므로 로컬 스토리지 디스크를 할당하고 로깅을 구성하기 위한 최초 구성을 수행해야 합니다. 지침은 [Tape Gateway 구성](#)을 참조하세요.

Tape Gateway 구성

새 Tape Gateway에서 최초 구성을 수행하려면

1. 다음 주제에 설명된 절차를 아직 완료하지 않은 경우 완료합니다.
 - [Tape Gateway 설정](#)

- [Tape Gateway를 에 연결 AWS](#)
- [설정 검토 및 Tape Gateway 활성화](#)

완료했으면 다음을 선택하여 Storage Gateway 콘솔에서 게이트웨이 구성 페이지를 엽니다.

2. 스토리지 구성 섹션에서 드롭다운 메뉴를 사용하여 에 대해 165GiB 용량 이상의 디스크를 하나 이상 할당하고 CACHE STORAGE에 대해 150GiB 용량 이상의 디스크를 하나 이상 할당합니다. UPLOADBUFFER. 이 섹션에 나열된 로컬 디스크는 호스트 플랫폼에서 프로비저닝한 물리적 스토리지에 해당합니다.
3. CloudWatch 로그 그룹 섹션에서 게이트웨이 상태를 모니터링하도록 Amazon CloudWatch Logs를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - 새 로그 그룹 생성 - 게이트웨이를 모니터링할 새 로그 그룹을 설정합니다.
 - 기존 로그 그룹 사용 - 해당 드롭다운 메뉴에서 기존 로그 그룹을 선택합니다.
 - 로깅 비활성화 - Amazon CloudWatch Logs를 사용하여 게이트웨이를 모니터링하지 마세요.

Note

Storage Gateway 상태 로그를 수신하려면 로그 그룹 리소스 정책에 다음 권한이 있어야 합니다. 교체 *highlighted section* 배포에 대한 특정 로그 그룹 resourceArn 정보를 포함합니다.

```
"Sid": "AWSLogDeliveryWrite20150319",
  "Effect": "Allow",
  "Principal": {
    "Service": [
      "delivery.logs.amazonaws.com"
    ]
  },
  "Action": [
    "logs:CreateLogStream",
    "logs:PutLogEvents"
  ],
  "Resource": "arn:aws:logs:eu-west-1:1234567890:log-group:/foo/bar:log-stream:*"
```

'리소스' 요소는 권한이 개별 로그 그룹에 명시적으로 적용되도록 하려는 경우에만 필요합니다.

4. CloudWatch 경보 섹션에서 게이트웨이 지표가 정의된 한도를 벗어날 때 알리도록 Amazon CloudWatch 경보를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
 - Storage Gateway의 권장 경보 생성 - 게이트웨이가 생성될 때 모든 권장 CloudWatch 경보를 자동으로 생성합니다. 권장 경보에 대한 자세한 내용은 [CloudWatch 경보 이해](#)를 참조하세요.

Note

이 기능에는 CloudWatch 미리 구성된 Storage Gateway 전체 액세스 정책의 일부로 자동으로 부여되지 않는 정책 권한이 필요합니다. 권장 CloudWatch 경보를 생성하기 전에 보안 정책이 다음 권한을 부여하는지 확인하세요.

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

- 사용자 지정 경보 생성 - 게이트웨이의 지표를 알리도록 새 CloudWatch 경보를 구성합니다. Amazon CloudWatch 콘솔에서 경보 생성을 선택하여 지표를 정의하고 경보 작업을 지정합니다. 지침은 [Amazon 사용 설명서의 Amazon CloudWatch 경보 사용](#)을 참조하세요. CloudWatch
 - 경보 없음 - 게이트웨이 지표에 대한 알림을 받지 CloudWatch 않습니다.
5. (선택 사항) 태그 섹션에서 새 태그 추가를 선택한 다음 대소문자를 구분하여 키-값 페어를 입력하면 Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 검색하고 필터링하는 데 도움이 됩니다. 이 단계를 반복하여 필요한 만큼 태그를 추가합니다.
 6. 구성을 선택하여 게이트웨이 생성을 완료합니다.

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

게이트웨이를 생성했으므로 게이트웨이에서 사용할 가상 테이프를 생성해야 합니다. 지침은 [테이프 생성](#)을 참조하세요.

Tape Gateway용 새 가상 테이프 생성

이 섹션에서는 를 사용하여 새 가상 테이프를 생성하는 방법을 설명합니다 AWS Storage Gateway. AWS Storage Gateway 콘솔 또는 Storage Gateway 를 사용하여 수동으로 새 가상 테이프를 생성할 수 있습니다API. 또한 테이프를 자동으로 생성하도록 Tape Gateway를 구성할 수도 있습니다. 그러면 수동 테이프 관리의 필요성을 줄이고, 대규모 배포를 간소화하며, 온프레미스 및 아카이브 스토리지 요구 사항을 조정하는 데 도움이 됩니다.

Tape Gateway는 가상WORM 테이프에서 쓰기, 읽기 및 테이프 보존 잠금을 한 번 지원합니다. WORM-활성화된 가상 테이프는 가상 테이프 라이브러리의 활성 테이프에 있는 데이터를 덮어쓰거나 지울 수 없도록 하는 데 도움이 됩니다. 가상 테이프 WORM 보호에 대한 자세한 내용은 다음 섹션을 참조하세요[the section called “WORM 테이프 보호”](#).

테이프 보존 잠금 기능을 사용하면 아카이브된 가상 테이프에 보존 모드와 보존 기간을 지정하여 일정 기간(최대 100년) 동안 삭제되지 않도록 할 수 있습니다. 여기에는 테이프를 삭제하거나 보존 설정을 수정할 수 있는 사람에 대한 권한 제어 기능이 포함됩니다. 테이프 보존 잠금에 대한 자세한 내용은 [the section called “테이프 보존 잠금”](#) 섹션을 참조하세요.

Note

요금은 테이프 용량이 아니라 테이프에 기록하는 데이터 양에 대해서만 청구됩니다. AWS Key Management Service (AWS KMS)를 사용하여 Amazon Simple Storage Service(Amazon S3)에 저장된 가상 테이프에 기록된 데이터를 암호화할 수 있습니다. 현재 또는 AWS Command Line Interface ()를 AWS Storage Gateway API 사용하여 이 작업을 수행할 수 있습니다AWS CLI. 자세한 내용은 [CreateTapes](#) 또는 [create-tapes](#)를 참조하세요.

한 번 쓰기, 많은 읽기(WORM) 테이프 보호

에서 가상 테이프에 대한 WORM 보호를 활성화하여 가상 테이프를 덮어쓰거나 지워지지 않도록 할 수 있습니다 AWS Storage Gateway. WORM 테이프를 생성할 때 가상 테이프에 대한 보호가 활성화됩니다.

WORM 가상 테이프에 기록된 데이터는 덮어쓸 수 없습니다. WORM 가상 테이프에는 새 데이터만 추가할 수 있으며 기존 데이터는 삭제할 수 없습니다. 가상 테이프에 대한 WORM 보호를 활성화하면 해당 테이프가 활성 상태일 때, 배출 및 보관되기 전에 보호하는 데 도움이 됩니다.

WORM 구성은 테이프가 생성될 때만 설정할 수 있으며, 해당 구성은 테이프가 생성된 후에는 변경할 수 없습니다.

수동으로 테이프 생성

AWS Storage Gateway 콘솔 또는 Storage Gateway 를 사용하여 수동으로 새 가상 테이프를 생성할 수 있습니다. 이 콘솔은 무작위로 생성된 테이프 바코드의 접두사를 유연하게 지정할 수 있는 편리한 테이프 생성 인터페이스를 제공합니다. 테이프 바코드를 완전히 사용자 지정해야 하는 경우(예: 해당 물리적 테이프의 일련 번호와 일치시키려면) 를 사용해야 합니다. Storage Gateway를 사용하여 테이프를 생성하는 방법에 대한 자세한 내용은 Storage Gateway 참조 [CreateTapeWithBarcode](#)의 섹션을 참조하십시오. Storage Gateway API

Storage Gateway 콘솔을 사용하여 가상 테이프를 수동으로 생성하려면

1. <https://console.aws.amazon.com/storagegateway/>에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 탭을 선택합니다.
3. 테이프 생성을 선택하여 테이프 생성 창을 엽니다.
4. 게이트웨이에서 게이트웨이를 선택합니다. 테이프는 이 게이트웨이용으로 생성됩니다.
5. 테이프 유형에서 표준을 선택하여 표준 가상 테이프를 생성합니다. 한 번 읽으면 여러(WORM) 개의 가상 테이프를 생성 WORM하도록 선택합니다. 자세한 내용은 [Write Once, Read Many\(WORM\) Tape Protection](#)을 참조하십시오.
6. 테이프 개수에서 생성할 테이프의 개수를 선택합니다. 테이프 할당량에 대한 자세한 내용은 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.
7. 용량에 생성할 가상 테이프의 크기를 입력합니다. 테이프는 100GiB 이상이어야 합니다. 용량 할당량에 대한 자세한 내용은 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.
8. 바코드 접두사에 가상 테이프의 바코드 앞에 붙일 접두사를 입력합니다.

Note

가상 테이프는 바코드로 고유하게 식별되며 바코드에 접두사를 추가할 수 있습니다. 접두사를 사용하면 가상 테이프를 식별하는 데 도움이 됩니다. 접두사는 대문자(A-Z)이어야 하고 문자는 1~4개까지 사용할 수 있습니다.

9. 풀에서 Glacier 풀, Deep Archive 풀, 직접 생성한 사용자 지정 풀 중 하나를 선택합니다. 풀은 백업 소프트웨어로 테이프를 꺼낼 때 테이프가 저장되는 스토리지 클래스를 결정합니다.
 - S3 Glacier Flexible Retrieval 스토리지 클래스에 테이프를 아카이브하려면 Glacier 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 자동으로 아카이브됩니다. 일반적으로 3-5시간 이내에 테이프를 검색할 수 있는 보다 활동

적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.

- S3 Glacier Deep Archive 스토리지 클래스에 테이프를 아카이브하려면 Deep Archive 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive에 아카이브된 테이프는 일반적으로 12시간 이내에 검색할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.
- 사용 가능한 경우 사용자 지정 풀을 선택합니다. Deep Archive 풀 또는 Glacier 풀을 사용하도록 사용자 지정 테이프 풀을 구성합니다. 백업 소프트웨어로 테이프를 꺼내면 구성된 스토리지 클래스에 테이프가 아카이브됩니다.

테이프를 S3 Glacier Flexible Retrieval에 아카이브한 경우 나중에 S3 Glacier Deep Archive로 이동할 수 있습니다. 자세한 내용은 [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동](#) 단원을 참조하십시오.

Note

2019년 3월 27일 이전에 생성된 테이프는 백업 소프트웨어로 테이프를 꺼내면 S3 Glacier Flexible Retrieval에 바로 아카이브됩니다.

10. (선택 사항) 태그에서 새 태그 추가를 선택하고 키와 값을 입력하여 테이프에 태그를 추가합니다. 태그는 테이프를 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.
11. 테이프 생성을 선택합니다.
12. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

가상 테이프가 생성될 CREATING 때 가상 테이프의 상태는 처음에 로 설정됩니다. 테이프가 생성되면 상태가 로 변경됩니다AVAILABLE. 자세한 내용은 [테이프 상태 이해](#) 단원을 참조하십시오.

자동 테이프 생성 허용

Tape Gateway는 사용자가 구성한 최소 사용 가능 테이프 수를 유지하기 위해 새 가상 테이프를 자동으로 생성할 수 있습니다. 그런 다음 새 테이프를 백업 애플리케이션의 가져오기에 제공함으로써 백업 작업을 중단 없이 실행할 수 있습니다. 자동 테이프 생성을 허용하면 새 가상 테이프를 수동으로 생성하는 프로세스 외에 사용자 지정 스크립팅도 필요 없게 됩니다.

Tape Gateway는 자동 테이프 생성에 대해 지정된 최소 사용 가능 테이프 수보다 적을 때 새 테이프를 자동으로 생성합니다. 새 테이프가 생성되는 경우는 다음과 같습니다.

- 가져오기/내보내기 슬롯에서 테이프를 가져온 경우
- 테이프를 테이프 드라이브로 가져온 경우

게이트웨이는 자동 테이프 생성 정책에 지정된 바코드 접두사를 포함하는 최소 테이프 수를 유지합니다. 바코드 접두사를 포함하는 최소 테이프 수보다 적은 수의 테이프가 있는 경우 게이트웨이는 자동 테이프 생성 정책에 지정된 최소 테이프 수와 같도록 새 테이프를 자동으로 생성합니다.

테이프를 꺼내 가져오기/내보내기 슬롯에 넣으면 해당 테이프는 자동 테이프 생성 정책에 지정된 최소 테이프 수에 포함되지 않습니다. 가져오기/내보내기 슬롯에 있는 테이프만 "사용 가능"한 것으로 간주됩니다. 테이프를 내보내도 자동 테이프 생성이 시작되지 않습니다. 가져오기만 사용 가능한 테이프 수에 영향을 줍니다.

가져오기/내보내기 슬롯에서 테이프 드라이브나 스토리지 슬롯으로 테이프를 이동하면 가져오기/내보내기 슬롯에서 바코드 접두사가 같은 테이프 수가 줄어듭니다. 게이트웨이는 해당 바코드 접두사에 사용할 수 있는 최소 테이프 수를 유지하기 위해 새 테이프를 생성합니다.


자동 테이프 생성을 허용하려면

1. <https://console.aws.amazon.com/storagegateway/>집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 탭을 선택합니다.
3. 테이프를 자동으로 생성할 게이트웨이를 선택합니다.
4. 작업 메뉴에서 Configure tape auto-create(테이프 자동 생성 구성)를 선택합니다.

테이프 자동 생성 페이지가 나타납니다. 여기에서 테이프 자동 생성 옵션을 구성, 변경 또는 제거할 수 있습니다.

5. 자동 테이프 생성을 허용하려면 새 항목 추가를 선택한 다음 자동 테이프 생성 설정을 구성합니다.

6. 테이프 유형에서 표준을 선택하여 표준 가상 테이프를 생성합니다. write-once-read-many (WORM) 가상 테이프를 생성WORM하도록 선택합니다. 자세한 내용은 [Write Once, Read Many\(WORM\) Tape Protection](#)을 참조하세요.
7. 최소 테이프 수에 Tape Gateway에서 항상 사용할 수 있어야 하는 최소 가상 테이프 수를 입력합니다. 이 값의 유효한 범위는 최소 1, 최대 10입니다.
8. 용량에 가상 테이프 용량의 크기(바이트)를 입력합니다. 유효한 범위는 최소 100GiB, 최대 15TiB입니다.
9. 바코드 접두사에 가상 테이프의 바코드 앞에 붙일 접두사를 입력합니다.

 Note

가상 테이프는 바코드로 고유하게 식별되며 바코드에 접두사를 추가할 수 있습니다. 접두사는 선택 사항이긴 하지만 가상 테이프를 식별하는 데 사용할 수 있습니다. 접두사는 대문자(A-Z)이어야 하고 문자는 1~4개까지 사용할 수 있습니다.

10. 풀에서 Glacier 풀, Deep Archive 풀, 직접 생성한 사용자 지정 풀 중 하나를 선택합니다. 풀은 백업 소프트웨어로 테이프를 꺼낼 때 테이프가 저장되는 스토리지 클래스를 결정합니다.
 - S3 Glacier Flexible Retrieval 스토리지 클래스에 테이프를 아카이브하려면 Glacier 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 자동으로 아카이브됩니다. 일반적으로 3-5시간 이내에 테이프를 검색할 수 있는 보다 활동적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.
 - S3 Glacier Deep Archive 스토리지 클래스에 테이프를 아카이브하려면 Deep Archive 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive에 아카이브된 테이프는 일반적으로 12시간 이내에 검색할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.
 - 사용 가능한 경우 사용자 지정 풀을 선택합니다. Deep Archive 풀 또는 Glacier 풀을 사용하도록 사용자 지정 테이프 풀을 구성합니다. 백업 소프트웨어로 테이프를 꺼내면 구성된 스토리지 클래스에 테이프가 아카이브됩니다.

테이프를 S3 Glacier Flexible Retrieval에 아카이브한 경우 나중에 S3 Glacier Deep Archive로 이동할 수 있습니다. 자세한 내용은 [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동](#) 단원을 참조하십시오.

Note

2019년 3월 27일 이전에 생성된 테이프는 백업 소프트웨어로 테이프를 꺼내면 S3 Glacier Flexible Retrieval에 바로 아카이브됩니다.

11. 설정 구성을 완료했으면 변경 사항 저장을 선택합니다.
12. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

사용 가능한 가상 테이프의 상태는 테이프가 생성될 CREATING 때 처음으로 설정됩니다. 테이프가 생성되면 상태가 로 변경됩니다AVAILABLE. 자세한 내용은 [테이프 상태 이해](#) 단원을 참조하십시오.

자동 테이프 생성 정책을 변경하거나 Tape Gateway에서 자동 테이프 생성을 삭제하는 방법에 대한 자세한 내용은 [자동 테이프 생성 관리](#) 섹션을 참조하세요.

다음 단계

[Tape Gateway 사용](#)

사용자 지정 테이프 풀 생성

이 섹션에서는 AWS Storage Gateway에서 새 사용자 지정 테이프 풀을 생성하는 방법에 대해 설명합니다.

주제

- [테이프 풀 유형 선택](#)
- [테이프 보존 잠금 사용](#)
- [사용자 지정 테이프 풀 생성](#)

테이프 풀 유형 선택

AWS Storage Gateway 는 테이프 풀을 사용하여 테이프를 꺼낼 때 아카이브할 스토리지 클래스를 결정합니다. Storage Gateway에서 제공하는 두 가지 표준 테이프 풀은 다음과 같습니다.

- Glacier 풀 - S3 Glacier Flexible Retrieval 스토리지 클래스에 테이프를 아카이브합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 자동으로 아카이브됩니다. 일반적으로 3-5시간 이내에 테이프를 검색할 수 있는 보다 활동적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.
- Deep Archive 풀 - S3 Glacier Deep Archive 스토리지 클래스에 테이프를 아카이브합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive에 아카이브된 테이프는 일반적으로 12시간 이내에 검색할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.

테이프를 S3 Glacier Flexible Retrieval에 아카이브한 경우 나중에 S3 Glacier Deep Archive로 이동할 수 있습니다. 자세한 내용은 [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동](#) 단원을 참조하십시오.

Storage Gateway는 또한 사용자 지정 테이프 풀 생성도 지원하므로, 테이프 보존 잠금을 활성화하여 아카이브된 테이프가 일정 기간(최대 100년) 동안 삭제되거나 다른 풀로 이동되는 것을 방지할 수 있습니다. 여기에는 테이프를 삭제하거나 보존 설정을 수정할 수 있는 사람에 대한 잠금 권한 제어 기능이 포함됩니다.

테이프 보존 잠금 사용

테이프 보존 잠금을 사용하면 아카이브된 테이프를 잠글 수 있습니다. 테이프 보존 잠금은 사용자 지정 테이프 풀의 테이프에 사용할 수 있는 옵션입니다. 테이프 보존 잠금이 활성화된 테이프는 일정 기간(최대 100년) 동안 삭제하거나 다른 풀로 이동할 수 없습니다.

테이프 보존 잠금은 다음 두 가지 모드 중 하나로 구성할 수 있습니다.

- 거버넌스 모드 - 거버넌스 모드로 구성된 경우 수행할 권한이 있는 AWS Identity and Access Management (IAM) 사용자만 풀에서 테이프를 제거할 수 있습니다. `storagegateway:BypassGovernanceRetention` 수 있습니다. 를 AWS Storage Gateway API 사용하여 테이프를 제거하는 경우 도 `BypassGovernanceRetention`로 설정해야 합니다 `true`.

- 규정 준수 모드 - 규정 준수 모드로 구성된 경우 루트 AWS 계정을 포함한 어떠한 사용자도 보호를 제거할 수 없습니다.

규정 준수 모드에서 테이프를 잠그면 보존 잠금 유형을 변경할 수 없으며 보존 기간도 단축할 수 없습니다. 규정 준수 모드 잠금 유형은 보존 기간 동안 테이프를 덮어쓰거나 삭제할 수 없도록 하는 데 도움이 됩니다.

Important

사용자 지정 풀을 생성한 후에는 구성을 변경할 수 없습니다.

사용자 지정 테이프 풀을 생성할 때 테이프 보존 잠금을 활성화할 수 있습니다. 사용자 지정 풀에 연결된 새 테이프는 해당 풀의 보존 잠금 유형, 기간 및 스토리지 클래스를 상속합니다.

이 기능이 출시되기 전에 아카이브된 테이프에 대해 기본 풀과 사용자가 생성한 사용자 지정 풀 간에 테이프를 이동하는 방식으로 테이프 보존 잠금을 활성화할 수도 있습니다. 테이프가 아카이브되면 테이프 보존 잠금은 즉시 적용됩니다.

Note

아카이브된 테이프를 S3 Glacier Flexible Retrieval 및 S3 Glacier Deep Archive 스토리지 클래스 간에 이동하는 경우, 테이프 이동 요금이 부과됩니다. 스토리지 클래스가 동일하게 유지되는 경우 기본 풀에서 사용자 지정 풀로 테이프를 이동하는 데 추가 요금이 부과되지 않습니다.


사용자 지정 테이프 풀 생성

다음 단계에 따라 AWS Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 생성합니다.

사용자 지정 테이프 풀을 생성하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 왼쪽 탐색 창에서 테이프 라이브러리 탭을 선택한 다음 풀 탭을 선택합니다.
3. 풀 생성을 선택하여 풀 생성 창을 엽니다.
4. 이름에 사용자 지정 테이프 풀을 식별하는 고유한 이름을 입력합니다. 풀 이름은 2-100자 사이여야 합니다.
5. 스토리지 클래스에서 Glacier 또는 Glacier Deep Archive를 선택합니다.

6. 보존 잠금 유형으로 없음, 규정 준수 또는 거버넌스를 선택합니다.

 Note

규정 준수를 선택하면 루트 AWS 계정을 포함한 어떠한 사용자도 테이프 보존 잠금을 제거할 수 없습니다.

7. 테이프 보존 잠금 유형을 선택하는 경우 보존 기간(일)을 입력합니다. 최대 보존 기간은 36,500일 (100년)입니다.
8. (선택 사항) 태그에서 새 태그 추가를 선택하여 사용자 지정 테이프 풀에 태그를 추가합니다. 태그는 사용자 지정 풀을 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.
- 키를 입력하고 필요하면 태그 값도 입력합니다. 테이프 풀에 최대 50개의 태그를 추가할 수 있습니다.
9. 풀 생성을 선택하여 새 사용자 지정 테이프 풀을 생성합니다.

VTL 디바이스 연결

다음은 가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 또는 Red Hat Enterprise Linux(RHEL) 클라이언트에 연결하는 방법에 대한 지침입니다.

주제


- [Microsoft Windows 클라이언트에 연결](#)
- [Linux 클라이언트에 연결](#)

Microsoft Windows 클라이언트에 연결

다음 절차는 Windows 클라이언트에 연결하기 위한 단계를 요약하여 보여줍니다.

VTL 디바이스를 Windows 클라이언트에 연결하려면

1. Start `iscsicpl.exe`.

 Note

iSCSI 이니시에이터를 실행하려면 클라이언트 컴퓨터에 관리자 권한이 있어야 합니다.

2. Microsoft iSCSI 이니시에이터 서비스를 시작합니다.
3. iSCSI Initiator 속성 대화 상자에서 검색 탭을 선택한 다음 포털 검색을 선택합니다.
4. Tape Gateway for IP 주소 또는 DNS 이름 의 IP 주소를 입력합니다.
5. 대상 탭을 선택한 후 새로 고침을 선택합니다. 테이프 드라이브 10개와 미디어 체인저가 모두 검색된 대상(Discovered targets) 상자에 표시됩니다. 대상의 상태는 비활성으로 되어 있습니다.
6. 첫 번째 디바이스를 선택하여 연결합니다. 디바이스를 한 번에 하나씩 연결합니다.
7. 모든 대상을 연결합니다.

Windows 클라이언트에서 테이프 드라이브에 대한 드라이버 공급자는 Microsoft이어야 합니다. 다음 절차를 통해 드라이버 공급자를 확인하고 필요한 경우 드라이버와 공급자를 업데이트하십시오:

드라이버 및 공급자를 확인 및 업데이트하려면

1. Windows 클라이언트에서 디바이스 관리자를 시작합니다.
2. 테이프 드라이브(Tape drives)를 펼쳐 테이프 드라이브를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 속성을 선택합니다.
3. 디바이스 속성 대화 상자의 드라이버 탭에서 드라이버 제공자가 Microsoft인지 확인합니다.
4. 드라이버 제공자(Driver Provider)가 Microsoft가 아닌 경우, 값을 다음과 같이 설정합니다.
 - a. 드라이버 업데이트(Update Driver)를 선택합니다.
 - b. 드라이버 소프트웨어 업데이트(Update Driver Software) 대화 상자에서 내 컴퓨터에서 드라이버 소프트웨어 찾아보기(Browse my computer for driver software)를 선택합니다.
 - c. 드라이버 소프트웨어 업데이트(Update Driver Software) 대화 상자에서 내 컴퓨터의 디바이스 드라이버 목록에서 고르기(Let me pick from a list of device drivers on my computer)를 선택합니다.
 - d. LTO 테이프 드라이브를 선택하고 다음을 선택합니다.
5. 달기를 선택하여 드라이버 소프트웨어 업데이트(Update Driver Software) 창을 닫고 드라이버 제공자(Driver Provider) 값이 Microsoft로 설정되어 있는지 확인합니다.
6. 모든 테이프 드라이브에 대해 이 단계를 반복하여 드라이버 및 공급자를 업데이트합니다.

Linux 클라이언트에 연결

다음 절차는 RHEL 클라이언트에 연결하기 위해 따르는 단계를 요약한 것입니다.

Linux 클라이언트를 VTL 디바이스에 연결하려면

1. `iscsi-initiator-utils` RPM 패키지를 설치합니다.

다음 명령을 사용하여 패키지를 설치할 수 있습니다.

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

2. iSCSI 데몬이 실행 중인지 확인합니다.

RHEL 5 또는 6의 경우 다음 명령을 사용합니다.

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

RHEL 7, 8 또는 9의 경우 다음 명령을 사용합니다.

```
sudo service iscsid status
```

3. 게이트웨이에 대해 정의된 볼륨 또는 VTL 디바이스 대상을 검색합니다. 다음 검색 명령을 사용합니다.

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

검색 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

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

4. 대상에 연결합니다.

올바른 항목을 지정해야 합니다. `[GATEWAY_IP]` 연결 명령 IQN에서 `및` 를 선택합니다.

다음 명령을 사용합니다.

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

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

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

이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

Volume Gateway의 경우 이니시에이터를 설정한 후 에 설명된 대로 iSCSI 설정을 사용자 지정하는 것이 좋습니다 [Linux iSCSI 설정 사용자 지정](#).

VTL 디바이스가 클라이언트 시스템(이니시에이터)에 연결되어 있는지 확인합니다. 이렇게 하려면 다음 명령을 사용합니다.

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

이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

```
total 0
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-mediachanger-lun-0-changer -> ../../sg20
lrwxrwxrwx 1 root root 9 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0 -> ../../st6
lrwxrwxrwx 1 root root 10 Sep 8 11:19 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-01-lun-0-nst -> ../../nst6
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0 -> ../../st7
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-02-lun-0-nst -> ../../nst7
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0 -> ../../st8
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-03-lun-0-nst -> ../../nst8
lrwxrwxrwx 1 root root 9 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0 -> ../../st9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-04-lun-0-nst -> ../../nst9
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0 -> ../../st10
```

```

lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-05-lun-0-nst -> ../../nst10
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0 -> ../../st11
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-06-lun-0-nst -> ../../nst11
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0 -> ../../st12
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-07-lun-0-nst -> ../../nst12
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0 -> ../../st13
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-08-lun-0-nst -> ../../nst13
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0 -> ../../st14
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-09-lun-0-nst -> ../../nst14
lrwxrwxrwx 1 root root 10 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0 -> ../../st15
lrwxrwxrwx 1 root root 11 Sep 8 11:20 ip-10.6.56.90:3260-iscsi-
iqn.1997-05.com.amazon:sgw-9999999c-tapedrive-10-lun-0-nst -> ../../nst15
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000012-lun-0-
changer -> ../../sg6
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-lun-0
-> ../../st0
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001c-
lun-0-nst -> ../../nst0
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-lun-0
-> ../../st1
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x000000000000001f-
lun-0-nst -> ../../nst1
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-lun-0
-> ../../st2
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.0-fc-0x0000000000000022-
lun-0-nst -> ../../nst2
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-lun-0
-> ../../st5
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000025-
lun-0-nst -> ../../nst5
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-lun-0
-> ../../st3
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000028-
lun-0-nst -> ../../nst3

```

```
lrwxrwxrwx 1 root root 9 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000002b-lun-0
-> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x0000000000000002b-
lun-0-nst -> ../../nst4
```

다음 단계

[백업 소프트웨어를 사용하여 게이트웨이 설정 테스트](#)

백업 소프트웨어를 사용하여 게이트웨이 설정 테스트

백업 애플리케이션으로 다음 작업을 수행하여 Tape Gateway 설정을 테스트할 수 있습니다.

1. 스토리지 디바이스를 감지하도록 백업 애플리케이션을 구성합니다.

Note

I/O 성능을 개선하려면 백업 애플리케이션에서 테이프 드라이브의 블록 크기를 1MB로 설정하는 것이 좋습니다. 자세한 내용은 [테이프 드라이브에 더 큰 블록 크기 사용](#) 섹션을 참조하세요.

2. 데이터를 테이프에 백업합니다.
3. 테이프를 아카이브합니다.
4. 아카이브에서 테이프를 검색합니다.
5. 테이프에서 데이터를 복원합니다.

설정을 테스트하려면 다음 설명과 같이 호환되는 백업 애플리케이션을 사용합니다.

Note

달리 명시되지 않는 한 모든 백업 애플리케이션은 Microsoft Windows에서 검증되었습니다.

호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [Arcserve Backup을 사용하여 설정 테스트](#)
- [Bacula Enterprise를 사용하여 설정 테스트](#)
- [Commvault를 사용한 설정 테스트](#)
- [Dell을 사용하여 설정 테스트 EMC NetWorker](#)
- [IBM스펙트럼 보호를 사용하여 설정 테스트](#)
- [Micro Focus Data Protector를 사용하여 설정 테스트](#)
- [Microsoft System Center를 사용하여 설정 테스트 DPM](#)
- [를 사용하여 설정 테스트 NovaStor DataCenter](#)
- [Quest NetVault Backup을 사용하여 설정 테스트](#)
- [Veeam Backup and Replication을 사용하여 설정 테스트](#)
- [Veritas Backup Exec을 사용한 설정 테스트](#)
- [Veritas를 사용하여 설정 테스트 NetBackup](#)

Arcserve Backup을 사용하여 설정 테스트

Arcserve Backup r17.0을 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway를 사용하여 Arcserve Backup을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 확인할 수 있습니다. Arcserve Backup r17.0 사용에 대한 자세한 내용은 Arcserve 관리 안내서에서 [Arcserve Backup r17 설명서](#)를 참조하세요.

주제

- [Arcserve가 VTL 디바이스와 함께 작동하도록 구성](#)
- [테이프를 미디어 풀로 로드](#)
- [데이터를 테이프에 백업](#)
- [테이프 보관](#)
- [테이프에서 데이터 복원](#)

Arcserve가 VTL 디바이스와 함께 작동하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 클라이언트에 연결한 후 디바이스를 스캔합니다.

VTL 디바이스를 스캔하려면

1. ARCserve Backup Manager에서 유틸리티 메뉴를 선택합니다.
2. 미디어 보증 및 스캔을 선택합니다.

테이프를 미디어 폴로 로드

Arcserve 소프트웨어가 게이트웨이에 연결되고 테이프를 사용할 수 있게 되면 Arcserve에서 자동으로 테이프를 로드합니다. Arcserve 소프트웨어에서 게이트웨이를 찾을 수 없는 경우 Arcserve에서 테이프 엔진을 다시 시작해 보세요.

테이프 엔진을 다시 시작하려면

1. 빠른 시작을 선택하고 관리, 디바이스를 차례로 선택합니다.
2. 탐색 메뉴에서 게이트웨이의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 슬롯 가져오기/내보내기를 선택합니다.
3. 빠른 가져오기를 선택하고 테이프를 빈 슬롯에 할당합니다.
4. 게이트웨이의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 인벤토리/오프라인 슬롯을 선택합니다.
5. 빠른 인벤토리를 선택하여 데이터베이스에서 미디어 정보를 검색합니다.

새 테이프를 추가하는 경우 게이트웨이에서 새 테이프를 스캔해야 Arcserve에 해당 테이프가 나타납니다. 새 테이프가 표시되지 않는 경우 테이프를 가져와야 합니다.

테이프를 가져오려면

1. 빠른 시작 메뉴를 선택하고 백업, 대상 탭을 차례로 선택합니다.
2. 게이트웨이를 선택하고 테이프 한 개에 대한 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 다음 슬롯 가져오기/내보내기를 선택합니다.
3. 새 테이프 각각의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 인벤토리를 선택합니다.
4. 새 테이프 각각의 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 열고 포맷을 선택합니다.

이제 각 테이프의 바코드가 Storage Gateway 콘솔에 표시되고 각 테이프의 사용 준비가 완료되었습니다.

데이터를 테이프에 백업

테이프가 Arcserve에 로드되면 데이터를 백업할 수 있습니다. 백업 프로세스는 물리적 테이프를 백업하는 것과 같습니다.

데이터를 테이프에 백업하려면

1. 빠른 시작 메뉴에서 백업 복원 세션을 엽니다.
2. 소스 탭을 선택한 다음 백업할 파일 시스템 또는 데이터베이스 시스템을 선택합니다.
3. 일정 탭을 선택하고 사용할 반복 방식을 선택합니다.
4. 대상 탭을 선택한 다음 사용할 테이프를 선택합니다. 백업하는 데이터가 테이프에 저장할 수 있는 용량보다 큰 경우 Arcserve에서 새 테이프를 마운트하라는 메시지를 표시합니다.
5. 제출을 선택하여 데이터를 백업합니다.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패할 수 있습니다. 실패한 백업 작업을 완료하려면 해당 작업을 다시 제출해야 합니다.

테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 테이프를 배출하여 보관하기 전에 테이프에 있는 콘텐츠를 확인하고 싶은 경우가 있습니다.

테이프를 보관하려면

1. 빠른 시작 메뉴에서 백업 복원 세션을 엽니다.
2. 소스 탭을 선택한 다음 백업할 파일 시스템 또는 데이터베이스 시스템을 선택합니다.
3. 일정 탭을 선택하고 사용할 반복 방식을 선택합니다.
4. 게이트웨이를 선택하고 테이프 한 개에 대한 컨텍스트 메뉴(마우스 오른쪽 버튼 클릭)를 연 다음 슬롯 가져오기/내보내기를 선택합니다.
5. 메일 슬롯을 할당하여 테이프를 로드합니다. Storage Gateway 콘솔의 상태가 아카이브로 변경됩니다. 아카이브 프로세스는 다소 시간이 걸릴 수 있습니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다 ARCHIVING. 아카이브가 완료되면 테이프는 더 이상 에 나열되지 VTL 않지만 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브됩니다.

테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. ARCserve를 사용하여 데이터를 복원합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다. 지침은 [Arcserve Backup r17 설명서](#)를 참조하세요.

테이프에서 데이터를 복원하려면 다음 절차 대로 합니다.

테이프에서 데이터를 복원하려면

1. 빠른 시작 메뉴에서 복원 세션을 엽니다.
2. 소스 탭을 선택한 다음 복원할 파일 시스템 또는 데이터베이스 시스템을 선택합니다.
3. 대상 탭을 선택하고 기본 설정을 적용합니다.
4. 일정 탭을 선택하고 사용할 반복 방법을 선택한 다음 제출을 선택합니다.

다음 단계

[불필요한 리소스 정리](#)

Bacula Enterprise를 사용하여 설정 테스트

Bacula Enterprise 버전 10을 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 보관하고, 가상 테이프 라이브러리 (VTL) 장치를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 Bacula 버전 10 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다. Bacula 버전 10 사용 방법에 대한 자세한 내용은 [Bacula Systems 매뉴얼 및 설명서](#)를 참조하거나, Bacula Systems에 문의하십시오.

Note

Bacula는 Linux에서만 지원됩니다.

Bacula Enterprise 설정

가상 테이프 라이브러리 (VTL) 디바이스를 Linux 클라이언트에 연결한 후 디바이스를 인식하도록 Bacula 소프트웨어를 구성합니다. VTL 디바이스를 클라이언트에 연결하는 방법에 대한 자세한 내용은 [참조하십시오 VTL 디바이스 연결](#).

Bacula를 설정하려면

1. Bacula Systems에서 Bacula Enterprise 백업 소프트웨어를 다운로드합니다.
2. 온프레미스 환경 또는 인클라우드 컴퓨터에 Bacula Enterprise 소프트웨어를 설치합니다.

설치 소프트웨어를 다운로드하는 방법을 보려면 [Enterprise Backup for Amazon S3 및 Storage Gateway](#)를 참조하세요. 추가적인 설치 지침은 Bacula 백서 [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#)을 참조하십시오.

장치와 함께 VTL 작동하도록 Bacula 구성

다음으로 디바이스에서 작동하도록 Bacula를 구성하십시오. VTL 기본 구성 단계가 표시됩니다.

Bacula를 구성하려면

1. Bacula Director 및 Bacula Storage 데몬을 설치합니다. 지침은 [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula 백서의 7장을 참조하십시오.
2. Bacula Director를 실행하는 시스템에 연결하고 iSCSI 이니시에이터를 구성합니다. 이렇게 하려면 [Using Cloud Services and Object Storage with Bacula Enterprise Edition](#) Bacula 백서의 7.4 단계에서 제공된 스크립트를 사용합니다.
3. 스토리지 디바이스를 구성합니다. 앞에서 언급한 Bacula 백서에 제공된 스크립트를 사용합니다.
4. 로컬 Bacula Director를 구성하고 스토리지 대상을 추가한 후 테이프의 미디어 풀을 정의합니다. 앞에서 언급한 Bacula 백서에 제공된 스크립트를 사용합니다.

데이터를 테이프에 백업

1. Storage Gateway 콘솔에서 테이프를 생성합니다. 테이프 생성 방법에 대한 자세한 내용은 [테이프 생성](#)을 참조하세요.
2. 다음 명령을 사용하여 I/E 슬롯의 테이프를 스토리지 슬롯으로 이전합니다.

```
/opt/bacula/scripts/mtx-changer
```

예를 들어 다음 명령은 I/E 슬롯 1601을 스토리지 슬롯 1로 이전합니다.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

3. 다음 명령을 사용하여 Bacula 콘솔을 시작합니다.

```
/opt/bacula/bin/bconsole
```

Note

테이프를 생성하여 Bacula로 이전할 경우 새로 생성한 테이프를 Bacula가 인식할 수 있도록 새로 Bacula 콘솔(bconsole) 명령 `update slots storage=VTL`을 사용하십시오.

4. 다음 bconsole 명령을 사용하여 테이프에 바코드로 볼륨 이름 또는 레이블을 지정합니다.

```
label storage=VTL pool=pool.VTL barcodes === label the tapes with the  
barcode as the volume name / label
```

5. 다음 명령을 사용하여 테이프를 탑재합니다.

```
mount storage=VTL slot=1 drive=0
```

6. 물리적 테이프에 대해 수행하는 것과 동일한 절차를 사용하여, 생성한 미디어 풀을 사용하는 백업 작업을 생성하고 가상 테이프에 데이터를 작성합니다.
7. 다음 명령을 사용하여 Bacula 콘솔에서 테이프 마운트를 해제합니다.

```
umount storage=VTL slot=1 drive=0
```

Note

진행 중인 백업 작업 중에 어떤 이유로든 테이프 게이트웨이가 다시 시작되면 백업 작업이 실패하고 Bacula Enterprise의 테이프 상태가 로 변경됩니다. FULL 테이프를 충분히 활용하지 못한 경우 수동으로 테이프 상태를 로 변경하고 동일한 테이프를 사용하여 백업 작업을 계속할

수 있습니다. APPEND APPEND상태에 있는 다른 테이프를 사용할 수 있는 경우 다른 테이프에서 작업을 계속할 수도 있습니다.

테이프 보관

특정 테이프에 대한 모든 백업 작업이 완료되고 테이프를 아카이브할 수 있는 경우 mtx-changer 스크립트를 사용하여 테이프를 스토리지 슬롯에서 I/E 슬롯으로 이동하십시오. 이 작업은 다른 백업 애플리케이션의 꺼내기 작업과 비슷합니다.

테이프를 보관하려면

1. `/opt/bacula/scripts/mtx-changer` 명령을 사용하여 스토리지 슬롯의 테이프를 I/E 슬롯으로 이전합니다.

예를 들어 다음 명령은 스토리지 슬롯 1을 I/E 슬롯 1601로 이전합니다.

```
/opt/bacula/scripts/mtx-changer transfer 1 1601
```

2. 테이프가 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 아카이브되고, 테이프의 상태가 아카이브 완료인지 확인합니다.

보관 및 검색을 했었던 테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. 다음 Bacula 소프트웨어를 사용하여 데이터를 복원합니다.
 - a. `/opt/bacula/scripts/mtx-changer` 명령을 사용하여 테이프를 스토리지 슬롯으로 가져오고 I/E 슬롯에서 테이프를 이전합니다.

예를 들어 다음 명령은 I/E 슬롯 1601을 스토리지 슬롯 1로 이전합니다.

```
/opt/bacula/scripts/mtx-changer transfer 1601 1
```

- b. Bacula 콘솔을 사용하여 슬롯을 업데이트한 후 테이프를 마운트합니다.
- c. 복원 명령을 사용하여 데이터를 복원합니다. 자세한 지침은 Bacula 설명서를 참조하십시오.

Commvault를 사용한 설정 테스트

Commvault 버전 11을 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 Commvault 백업 애플리케이션을 구성하고, 백업을 수행하고, 아카이브된 테이프에서 데이터를 가져오는 방법을 설명하는 기본 문서를 확인할 수 있습니다. Commvault 사용 방법에 대한 자세한 내용은 Commvault 웹사이트의 [Commvault 빠른 시작 설명서](#)를 참조하십시오.

주제

- [VTL 디바이스와 함께 작동하도록 Commvault 구성](#)
- [스토리지 정책 및 하위 클라이언트 생성](#)
- [Commvault에서 데이터를 테이프로 백업](#)
- [Commvault에 테이프 보관](#)
- [테이프에서 데이터 복원](#)

VTL 디바이스와 함께 작동하도록 Commvault 구성

VTL 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식하도록 Commvault를 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하십시오 [Windows 클라이언트에 VTL 디바이스 연결](#).

Commvault 백업 애플리케이션은 VTL 디바이스를 자동으로 인식하지 않습니다. 디바이스를 수동으로 추가하여 Commvault 백업 애플리케이션에 노출한 후 디바이스를 검색해야 합니다.

Commvault를 구성하려면

1. CommCell 콘솔 기본 메뉴에서 스토리지를 선택한 다음 전문가 스토리지 구성을 선택하여 선택 MediaAgents 대화 상자를 엽니다.
2. 사용하려는 사용 가능한 미디어 에이전트를 선택하고 Add(추가)를 선택한 다음 OK(확인)을 선택합니다.
3. Expert Storage Configuration(전문가 스토리지 구성 대화 상자에서 Start(시작)를 선택한 다음 Detect/Configure Devices(디바이스 감지/구성)를 선택합니다.
4. Device Type(디바이스 유형) 옵션을 선택된 상태로 두고 Exhaustive Detection(철저한 감지)를 선택한 다음 OK(확인)를 선택합니다.
5. Confirm Exhaustive Detection(철저한 감지 확인) 확인 대화 상자에서 Yes(예)를 선택합니다.

6. Device Selection(디바이스 선택) 대화 상자에서 라이브러리와 라이브러리의 모든 드라이브를 선택한 다음 OK(확인)를 선택합니다. 디바이스가 감지될 때까지 기다린 다음 Close(닫기)를 선택하여 로그 보고서를 닫습니다.
7. 라이브러리를 마우스 오른쪽 버튼으로 클릭하고 Configure(구성)을 선택한 다음 Yes(예)를 선택합니다. 구성 대화 상자를 닫습니다.
8. 이 라이브러리에 바코드 판독기가 있습니까? 대화 상자에서 예를 선택한 다음 디바이스 유형에서 IBM ULTRIUM V5를 선택합니다.
9. CommCell 브라우저에서 스토리지 리소스를 선택한 다음 라이브러리를 선택하여 테이프 라이브러리를 확인합니다.
10. 라이브러리에서 테이프를 보려면 라이브러리를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Discover Media(미디어 검색), Media location(미디어 위치), Media Library(미디어 라이브러리)를 차례로 선택합니다.
11. 테이프를 탑재하려면 미디어를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Load(로드)를 선택합니다.

스토리지 정책 및 하위 클라이언트 생성

백업 및 복원 작업은 모두 스토리지 및 하위 클라이언트 정책과 연결되어 있습니다.

스토리지 정책은 데이터의 원본 위치를 미디어로 매핑합니다.

스토리지 정책을 생성하려면

1. CommCell 브라우저에서 정책을 선택합니다.
2. Storage Policies(스토리지 정책)를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 New Storage Policy(새 스토리지 정책)를 선택합니다.
3. 스토리지 정책 생성 마법사에서 Data Protection and Archiving(보호 및 아카이브)를 선택하고 Next(다음)를 선택합니다.
4. Storage Policy Name(스토리지 정책 이름)에 이름을 입력한 다음 Incremental Storage Policy(증분 스토리지 정책)를 선택합니다. 이 스토리지 정책을 증분적 로드와 연결하려면 옵션 중에서 하나를 선택합니다. 그렇지 않으면 옵션을 선택되지 않은 상태로 두고 Next(선택)를 선택합니다.
5. Do you want to Use Global Deduplication Policy?(글로벌 중복 제거 정책을 사용하시겠습니까?) 대화 상자에서 Deduplication(중복 제거) 기본 설정을 선택하고 Next(다음)를 선택합니다.
6. 기본 복사본용 라이브러리 에서 VTL 라이브러리를 선택한 다음 다음을 선택합니다.
7. 미디어 에이전트 설정이 올바른지 확인하고 Next(다음)를 선택합니다.

8. 스크래치 폴 설정이 올바른지 확인하고 Next(다음)를 선택합니다.
9. iData Agent Backup 데이터 에서 보존 정책을 구성한 다음 다음 를 선택합니다.
10. 암호화 설정을 검토하고 Next(다음)를 선택합니다.
11. 스토리지 정책을 보려면 Storage Policies(스토리지 정책)를 선택합니다.

하위 클라이언트 정책을 생성한 후 스토리지 정책과 연결합니다. 하위 클라이언트 정책에 따라 중앙 템플릿에서 유사 파일 시스템 클라이언트를 구성할 수 있기 때문에 다수의 유사 파일 시스템을 수동으로 설정할 필요가 없습니다.

하위 클라이언트 정책을 생성하려면

1. CommCell 브라우저에서 클라이언트 컴퓨터 를 선택한 다음 클라이언트 컴퓨터를 선택합니다. 파일 시스템을 선택한 다음 를 선택합니다 defaultBackupSet.
2. 를 마우스 오른쪽 버튼으로 클릭하고 모든 작업을 defaultBackupSet선택한 다음 새 하위 클라이언트 를 선택합니다.
3. 하위 클라이언트 속성 상자에서 이름 에 SubClient 이름을 입력한 다음 확인을 선택합니다.
4. Browse(찾아보기)를 선택하여 백업할 파일로 이동한 다음 Add(추가)를 선택하고 대화 상자를 닫습니다.
5. Subclient(하위 클라이언트) 속성 대화 상자에서 Storage Device(스토리지 디바이스) 탭을 선택하고 Storage policy(스토리지 정책)에서 스토리지 정책을 선택한 다음 OK(확인)를 선택합니다.
6. 다음에 나타나는 Backup Schedule(백업 일정) 창에서 새 하위 클라이언트를 백업 일정과 연결합니다.
7. 일회성/온디맨드 백업에 Do Not Schedule(예약 안 함)을 선택한 다음 OK(확인)를 선택합니다.

이제 defaultBackupSet 탭에 하위 클라이언트가 표시됩니다.

Commvault에서 데이터를 테이프로 백업

물리적 테이프와 동일한 절차를 사용하여 백업 작업을 생성하고 가상 테이프에 데이터를 작성합니다. 자세한 내용은 [Commvault 설명서](#)를 참조하십시오.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패할 수 있습니다. 경우에 따라 실패한 작업을 재개하는 옵션을 선택할 수 있습니다. 그렇지 않으면 새 작업을 제출해야 합니다. 작업 실패 후 Commvault에서 테이프를 사용 불가로 표시하는

경우 테이프를 드라이브로 다시 로드해야 쓰기를 계속할 수 있습니다. 여러 개의 테이프를 사용할 수 있는 경우 Commvault는 실패한 백업 작업을 다른 테이프에서 계속할 수 있습니다.

Commvault에 테이프 보관

보관 프로세스는 테이프를 배출하는 것부터 시작됩니다. 테이프를 아카이브하면 Tape Gateway에서 테이프를 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 테이프를 배출하여 보관하기 전에 테이프 저장되어 있는 내용을 먼저 확인하는 것이 좋습니다.

테이프를 보관하려면

1. CommCell 브라우저에서 스토리지 리소스, 라이브러리 를 선택한 다음 라이브러리 를 선택합니다. Media By Location(위치별 미디어)를 선택한 다음 Media In Library(라이브러리의 미디어)를 선택합니다.
2. 아카이브할 테이프의를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 All Tasks(모든 작업), Export(내보내기), OK(확인)를 차례로 선택합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다ARCHIVING. 아카이브가 완료되면 테이프가 더 이상 에 나열되지 않습니다VTL.

Commvault 소프트웨어에서 테이프가 더 이상 스토리지 슬롯에 없는지 확인합니다.

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 인지 확인합니다ARCHIVED.

테이프에서 데이터 복원

보관 및 검색을 하지 않았던 테이프에서 데이터를 복원하거나, 혹은 보관 및 검색을 했었던 테이프에서 데이터를 복원할 수 있습니다. 보관 및 검색을 하지 않았던 테이프(비검색 테이프)일 때는 아래와 같이 두 가지 데이터 복원 옵션이 있습니다.

- 하위 클라이언트 기준 복원
- 작업 ID 기준 복원

하위 클라이언트를 기준으로 비검사 테이프에서 데이터를 복원하려면

1. CommCell 브라우저에서 클라이언트 컴퓨터를 선택한 다음 클라이언트 컴퓨터를 선택합니다. 파일 시스템을 선택한 다음 defaultBackupSet을 선택합니다.
2. 하위 클라이언트를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Browse and Restore(찾아보기 및 복원)을 선택한 다음 View Content(콘텐츠 보기)를 선택합니다.
3. 복원할 파일들을 선택한 다음 Recover All Selected(선택한 항목 모두 복구)를 선택합니다.
4. Home(홈)을 선택한 다음 Job Controller(작업 컨트롤러)를 선택하여 복원 작업의 상태를 모니터링합니다.

작업 ID를 기준으로 비검사 테이프에서 데이터를 복원하려면

1. CommCell 브라우저에서 클라이언트 컴퓨터를 선택한 다음 클라이언트 컴퓨터를 선택합니다. File System(파일 시스템)을 마우스 오른쪽 버튼으로 클릭하고 View(보기)를 선택한 다음 Backup History(백업 기록)를 선택합니다.
2. Backup Type(백업 유형) 카테고리에서 원하는 백업 작업 유형을 선택한 다음 OK(확인)를 선택합니다. 백업 작업 기록이 포함된 탭이 표시됩니다.
3. 복원할 Job ID(작업 ID)를 찾아 마우스 오른쪽 버튼으로 클릭한 다음 Browse and Restore(찾아보기 및 복원)를 선택합니다.
4. Browse and Restore Options(찾아보기 및 복원 옵션) 대화 상자에서 View Content(콘텐츠 보기)를 선택합니다.
5. 복원할 파일을 선택한 다음 Recover All Selected(선택한 항목 모두 복구)를 선택합니다.
6. Home(홈)을 선택한 다음 Job Controller(작업 컨트롤러)를 선택하여 복원 작업의 상태를 모니터링합니다.

보관 및 검색을 했었던 테이프에서 데이터를 복원하려면

1. CommCell 브라우저에서 스토리지 리소스를 선택하고 라이브러리 를 선택한 다음 라이브러리를 선택합니다. Media By Location(위치별 미디어)를 선택한 다음 Media In Library(라이브러리의 미디어)를 선택합니다.
2. 검색된 테이프를 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업)를 선택한 다음 Catalog(카탈로그)를 선택합니다.
3. Catalog Media(카탈로그 미디어) 대화 상자에서 Catalog only(카탈로그만)를 선택한 다음 OK(확인)를 선택합니다.
4. CommCell 홈 을 선택한 다음 작업 컨트롤러를 선택하여 복원 작업의 상태를 모니터링합니다.

5. 작업이 성공한 후 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 View(보기)를 선택한 다음 View Catalog Contents(카탈로그 콘텐츠 보기)를 선택합니다. 나중에 사용할 수 있도록 Job ID(작업 ID)를 적어둡니다.
6. Recatalog/Merge를 선택합니다. 카탈로그 미디어 대화 상자에서 병합만이 선택되어 있는지 확인합니다.
7. Home(홈)을 선택한 다음 Job Controller(작업 컨트롤러)를 선택하여 복원 작업의 상태를 모니터링합니다.
8. 작업이 성공한 후 CommCell 홈 을 선택하고 제어판 를 선택한 다음 찾아보기/검색/복구 를 선택합니다.
9. Show aged data during browse and recovery(찾아보기 및 복구 중 오래된 데이터 표시)를 선택하고 OK(확인)를 선택한 다음 Control Panel(제어판)을 닫습니다.
10. CommCell 브라우저에서 클라이언트 컴퓨터 를 마우스 오른쪽 버튼으로 클릭한 다음 클라이언트 컴퓨터를 선택합니다. View(보기)를 선택한 다음 Job History(작업 기록)를 선택합니다.
11. Job History Filter(작업 기록 필터) 대화 상자에서 Advanced(고급)를 선택합니다.
12. Include Aged Data(오래된 데이터 포함)을 선택한 다음 OK(확인)를 선택합니다.
13. Job History(작업 기록) 대화 상자에서 OK(확인)를 선택하여 history of jobs(작업 기록) 탭을 엽니다.
14. 복원할 작업을 찾아서 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음, Browse and Restore(찾아보기 및 복원)를 선택합니다.
15. Browse and Restore(찾아보기 및 복원) 대화 상자에서 View Content(콘텐츠 보기)를 선택합니다.
16. 복원할 파일을 선택한 다음 Recover All Selected(선택한 항목 모두 복구)를 선택합니다.
17. Home(홈)을 선택한 다음 Job Controller(작업 컨트롤러)를 선택하여 복원 작업의 상태를 모니터링합니다.

Dell을 사용하여 설정 테스트 EMC NetWorker

Dell EMC NetWorker 19.5를 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 스토리지 디바이스 구성, 테이프에 데이터 쓰기, 테이프 아카이브 및 테이프에서 데이터 복원을 포함하여 Tape Gateway와 함께 작동하도록 Dell EMC NetWorker 소프트웨어를 구성하고 백업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다.

Dell EMC NetWorker 소프트웨어를 설치하고 사용하는 방법에 대한 자세한 내용은 [관리 안내서](#)를 참조하세요.

호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [VTL 디바이스와 함께 작동하도록 구성](#)
- [Dell로 WORM 테이프 가져오기 허용 EMC NetWorker](#)
- [Dell의 테이프에 데이터 백업 EMC NetWorker](#)
- [Dell에서 테이프 보관 EMC NetWorker](#)
- [Dell의 아카이브된 테이프에서 데이터 복원 EMC NetWorker](#)

VTL 디바이스와 함께 작동하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 클라이언트에 연결한 후 디바이스를 인식하도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 [섹션을 참조하십시오 VTL 디바이스 연결](#).

Tape Gateway 디바이스는 자동으로 인식되지 않습니다. VTL 디바이스를 NetWorker 소프트웨어에 노출하고 소프트웨어를 검색하도록 하려면 소프트웨어를 수동으로 구성합니다. 다음에서는 사용자가 소프트웨어를 올바르게 설치했으며 Management Console에 익숙하다고 가정합니다. 관리 콘솔에 대한 자세한 내용은 [Dell EMC NetWorker 관리 안내서](#)의 NetWorker 관리 콘솔 인터페이스 섹션을 참조하십시오.

VTL 디바이스에 대해 Dell EMC NetWorker 소프트웨어를 구성하려면

1. Dell EMC NetWorker Management Console 애플리케이션을 시작하고 메뉴에서 엔터프라이즈를 선택한 다음 왼쪽 창에서 localhost를 선택합니다.
2. localhost를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Launch Application(애플리케이션 시작)을 선택합니다.
3. Devices(디바이스) 탭을 선택하고 Libraries(라이브러리)를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 Scan for Devices(디바이스에 대한 스캔)를 선택합니다.
4. Scan for Devices(디바이스에 대한 스캔) 마법사에서 Start Scan(스캔 시작)을 선택하고 다음에 나타나는 대화 상자에서 OK(확인)를 선택합니다.
5. 라이브러리 폴더 트리를 확장하여 모든 라이브러리를 확인하고 F5 키를 눌러 새로 고칩니다. 이 프로세스는 디바이스를 라이브러리로 로드하는 데 몇 초 정도 걸릴 수 있습니다.
6. 관리자 권한이 있는 명령 창(cmd.exe)을 열고 Dell EMC NetWorker 19.5에 설치된 jconfig 유틸리티를 실행합니다.

- a. 메뉴 프롬프트에서 해당 숫자를 입력하여 Autodetected SCSI Jukebox 구성을 선택합니다.
 - b. 주크박스 디바이스의 이름을 입력하라는 메시지가 표시되면 와 같은 이름을 입력합니다AWSVTL.
 - c. NetWorker 자동 정리를 켜라는 메시지가 표시되면 를 입력합니다no.
 - d. 자동 구성을 우회하라는 메시지가 표시되면 를 입력합니다no.
 - e. 다른 주크박스를 구성하라는 메시지가 표시되면 를 입력합니다no.
7. "jbconfig"가 완료되면 Networker로 돌아가 F5를 GUI 눌러 새로 고칩니다.
 8. 왼쪽 창에서 테이프를 확인할 라이브러리를 선택하면 해당되는 빈 볼륨 슬롯이 오른쪽 창에 나열됩니다.
 9. 볼륨 목록에서 활성화할 볼륨을 선택하고(선택한 볼륨이 강조 표시됨) 선택한 볼륨을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 보관을 선택합니다. 이 작업으로 테이프가 I/E 슬롯에서 볼륨 슬롯으로 이동합니다.
 10. 다음에 나타나는 대화 상자에서 Yes(예)를 선택한 다음 Load the Cartridges into(다음으로 카트리지 로드) 대화 상자에서 Yes(예)를 선택합니다.
 11. 보관할 테이프가 더 이상 없으면 No(아니요) 또는 Ignore(무시)를 선택합니다. 그렇지 않으면 Yes(예)를 선택하여 추가 테이프를 보관합니다.

Dell로 WORM 테이프 가져오기 허용 EMC NetWorker

이제 Tape Gateway에서 Dell EMC NetWorker 라이브러리로 테이프를 가져올 준비가 되었습니다.

가상 테이프는 한 번 읽으면 많은 (WORM) 테이프를 쓰지만 Dell은 테이프WORM가 아닌 테이프를 EMC NetWorker 기대합니다. DellEMC NetWorker 이 가상 테이프를 사용하려면 미디어WORM 풀이 아닌 다른 풀로 테이프 가져오기를 활성화해야 합니다.

비WORM 미디어 풀로 WORM 테이프를 가져오도록 허용하려면

1. NetWorker 콘솔에서 미디어 를 선택하고 localhost 의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 연 다음 속성 을 선택합니다.
2. NetWorker 서버 속성 창에서 구성 탭을 선택합니다.
3. 웹 테이프 처리 섹션에서 WORM WORM 풀의 테이프만 지우고 확인을 선택합니다.

Dell의 테이프에 데이터 백업 EMC NetWorker

데이터를 테이프에 백업하는 절차는 두 단계로 이루어져 있습니다.

1. 데이터를 백업하려는 테이프에 레이블을 지정하고 대상 미디어 풀을 생성하고 이 테이프를 풀에 추가합니다.

물리적 테이프에 대해 수행하는 것과 동일한 절차를 사용하여 미디어 풀을 생성하고 가상 테이프에 데이터를 작성합니다. 자세한 내용은 [Dell EMC NetWorker 관리 안내서](#)의 데이터 백업 섹션을 참조하세요.

2. 테이프에 데이터를 씁니다. Dell EMC NetWorker Management Console 대신 Dell EMC NetWorker User 애플리케이션을 사용하여 데이터를 백업합니다. Dell EMC NetWorker 사용자 애플리케이션은 설치의 일부로 설치됩니다 NetWorker.

Note

Dell EMC NetWorker 사용자 애플리케이션을 사용하여 백업을 수행하지만 EMC 관리 콘솔에서 백업 및 복원 작업의 상태를 볼 수 있습니다. 상태를 보려면 Devices(디바이스) 메뉴를 선택하고 Log(로그) 창에서 상태를 봅니다.

Note

백업 작업이 진행되는 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 일시 중지되고 Dell EMC NetWorker의 테이프 상태가 Write Protected 로 변경됩니다. 테이프를 아카이브하거나 테이프에서 데이터를 계속 읽을 수 있습니다. 다른 테이프에서 일시 중단된 백업 작업을 재개할 수 있습니다.

Dell에서 테이프 보관 EMC NetWorker

테이프를 아카이브하면 Tape Gateway가 테이프를 Dell EMC NetWorker 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 테이프 드라이브의 테이프를 스토리지 슬롯을 배출하여 테이프 보관을 시작합니다. 그런 다음 백업 애플리케이션, 즉 Dell EMC NetWorker 소프트웨어를 사용하여 슬롯에서 아카이브로 테이프를 제거합니다.

Dell을 사용하여 테이프를 아카이브하려면 EMC NetWorker

1. NetWorker 관리 창의 디바이스 탭에서 localhost 또는 EMC 서버를 선택한 다음 라이브러리를 선택합니다.
2. 가상 테이프 라이브러리에서 가져온 라이브러리를 선택합니다.

3. 데이터를 기록한 테이프의 목록에서 보관할 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 Eject/Withdraw(꺼내기/회수)를 선택합니다.
4. 다음에 나타나는 확인 상자에서 OK(확인)를 선택합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다ARCHIVING. 아카이브가 완료되면 테이프가 더 이상 에 나열되지 않습니다VTL.

Dell EMC NetWorker 소프트웨어에서 테이프가 더 이상 스토리지 슬롯에 없는지 확인합니다.

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 인지 확인합니다ARCHIVED.

Dell의 아카이브된 테이프에서 데이터 복원 EMC NetWorker

보관 데이터를 복원하려면 다음과 같은 두 단계를 거쳐야 합니다.

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. Dell EMC NetWorker 소프트웨어를 사용하여 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 폴더 복원 파일을 생성합니다. 지침은 [Dell EMC NetWorker 관리 안내서](#)의 NetWorker 사용자 프로그램 사용 섹션을 참조하세요.

다음 단계

[불필요한 리소스 정리](#)

IBM스펙트럼 보호를 사용하여 설정 테스트

IBMSpectrum Protect와 함께 사용하면 데이터를 가상 테이프에 백업하고, 테이프를 보관하고, 가상 테이프 라이브러리 (VTL) 장치를 관리할 수 있습니다. AWS Storage Gateway(IBM스펙트럼 프로텍트는 이전에 티볼리 스토리지 매니저로 알려졌습니다.)

이 항목에는 테이프 게이트웨이용 IBM Spectrum Protect 버전 8.1.10 백업 소프트웨어를 구성하는 방법에 대한 기본 정보가 포함되어 있습니다. 또한 IBM Spectrum Protect를 사용하여 백업 및 복원 작업을 수행하는 방법에 대한 기본 정보도 포함되어 있습니다. IBMSpectrum Protect 백업 소프트웨어를 관리하는 방법에 대한 자세한 내용은 Spectrum [Protect의 관리 작업 개요](#)를 참조하십시오IBM. IBM

IBM스펙트럼 프로텍트 백업 소프트웨어는 다음 운영 AWS Storage Gateway 체제에서 지원됩니다.

- Microsoft Windows Server
- Red Hat Linux

Windows용 IBM 스펙트럼 프로텍트 지원 장치에 대한 자세한 내용은 [HP-UX, Solaris 및 Windows용 IBM 스펙트럼 프로텍트 \(구 Tivoli Storage Manager\) 지원 장치를](#) 참조하십시오. AIX

Linux용 IBM 스펙트럼 프로텍트 지원 장치에 대한 자세한 내용은 Linux용 스펙트럼 프로텍트 ([구 Tivoli IBM Storage Manager](#)) 지원 장치를 참조하십시오.

주제

- [스펙트럼 프로텍트 설정 IBM](#)
- [VTL디바이스와 함께 작동하도록 IBM 스펙트럼 보호 구성](#)
- [IBM스펙트럼 보호에서 테이프에 데이터 쓰기](#)
- [Spectrum Protect에 보관된 테이프에서 데이터 복원 IBM](#)

스펙트럼 프로텍트 설정 IBM

VTL디바이스를 클라이언트에 연결한 후 IBM 스펙트럼 프로텍트 버전 8.1.10 소프트웨어가 디바이스를 인식하도록 구성합니다. VTL장치를 클라이언트에 연결하는 방법에 대한 자세한 내용은 [을](#) 참조하십시오. [VTL 디바이스 연결](#)

IBM스펙트럼 보호를 설정하려면

1. 에서 IBM 스펙트럼 프로텍트 버전 8.1.10 소프트웨어의 라이선스 사본을 받으십시오. IBM
2. 온프레미스 환경 또는 클라우드 내 Amazon EC2 인스턴스에 IBM Spectrum Protect 소프트웨어를 설치합니다. 자세한 내용은 IBM Spectrum IBM Protect의 [설치 및 업그레이드](#) 설명서를 참조하십시오.

IBMSpectrum Protect 소프트웨어 구성에 대한 자세한 내용은 [IBMSpectrum Protect 서버의 AWS 테이프 게이트웨이 가상 테이프 라이브러리 구성을](#) 참조하십시오.

VTL디바이스와 함께 작동하도록 IBM 스펙트럼 보호 구성

다음으로, VTL 디바이스에서 작동하도록 IBM 스펙트럼 프로텍트를 구성하십시오. Microsoft Windows Server 또는 Red Hat Linux의 VTL 디바이스에서 작동하도록 IBM 스펙트럼 프로텍트를 구성할 수 있습니다.

윈도우용 IBM 스펙트럼 프로텍트 구성

Windows에서 IBM 스펙트럼 보호를 구성하는 방법에 대한 전체 지침은 Lenovo 웹 사이트의 [Windows 2012용 테이프 장치 드라이버-W12 6266](#)을 참조하십시오. 다음은 프로세스에 관한 기본 설명서입니다.

Microsoft Windows용 IBM 스펙트럼 보호를 구성하려면

1. 미디어 체인저의 올바른 드라이버 패키지를 다운로드합니다. 테이프 장치 드라이버의 경우 IBM 스펙트럼 보호를 사용하려면 Windows 2012용 버전 W12 6266이 필요합니다. 드라이버를 다운로드하는 방법을 보려면 Lenovo 웹 사이트에서 [Windows 2012용 테이프 디바이스 드라이버-W12 6266](#)을 참조하십시오.

Note

드라이버의 "비독점적" 세트를 설치해야 합니다.

2. 컴퓨터에서 컴퓨터 관리를 열고 미디어 체인저 장치를 확장한 다음 미디어 체인저 유형이 3584 테이프 라이브러리로 나열되어 있는지 확인합니다. IBM
3. 가상 테이프 라이브러리의 테이프 바코드가 8자리 이하인지 확인합니다. 8자보다 긴 바코드를 테이프에 지정하려고 하면 "Tape barcode is too long for media changer" 오류 메시지가 표시됩니다.
4. 모든 테이프 드라이브와 미디어 체인저가 Spectrum Protect에 나타나는지 확인하십시오. IBM 이렇게 하려면 `\Tivoli\TSM\server>tsmdlst.exe` 명령을 사용합니다.

Linux용 IBM 스펙트럼 보호를 구성합니다.

다음은 Linux의 VTL 디바이스에서 작동하도록 IBM Spectrum을 구성하는 방법에 대한 기본 설명서입니다.

Linux용 IBM 스펙트럼 보호를 구성하려면

1. IBMSupport 웹 사이트의 [IBMFix Central](#)로 이동하여 제품 선택을 선택합니다.
2. Product Group(제품 그룹)에서 System Storage(시스템 스토리지)를 선택합니다.
3. 다음에서 선택 System Storage에서 Tape systems를 선택합니다.
4. Tape systems(테이프 시스템)에서 Tape drivers and software(테이프 드라이버 및 소프트웨어)를 선택합니다.

5. Select from Tape drivers and software(테이프 드라이버 및 소프트웨어에서 선택)에서 Tape device drivers(테이프 디바이스 드라이버)를 선택합니다.
6. 플랫폼에서 해당하는 운영 체제를 선택하고 계속을 선택합니다.
7. 다운로드할 디바이스 드라이버 버전을 선택합니다. 그런 다음 픽스 센트럴 다운로드 페이지의 지침에 따라 IBM Spectrum Protect를 다운로드하고 구성하십시오.
8. 가상 테이프 라이브러리의 테이프 바코드가 8자리 이하인지 확인합니다. 8자보다 긴 바코드를 테이프에 지정하려고 하면 "Tape barcode is too long for media changer" 오류 메시지가 표시됩니다.

IBM스펙트럼 보호에서 테이프에 데이터 쓰기

물리적 테이프에 대해 수행하는 것과 동일한 절차 및 백업 정책을 사용하여 Tape Gateway 가상 테이프에 데이터를 작성합니다. 백업 및 복원 작업을 위해 필요한 구성을 생성합니다. 스펙트럼 보호 구성에 대한 자세한 내용은 IBM 스펙트럼 보호 [관리 작업 개요](#)를 참조하십시오. IBM

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패할 수 있습니다. 백업 작업이 실패하면 IBM Spectrum Protect의 테이프 상태가 ReadOnly로 변경됩니다. 테이프가 완전히 사용되지 않은 경우 수동으로 테이프 상태를 다시 변경하고 동일한 테이프를 사용하여 백업 작업을 재개하거나 다시 제출할 수 있습니다. ReadWrite IBM Spectrum Protect는 ReadWrite 상태에 있는 다른 테이프를 사용할 수 있는 경우 실패한 백업 작업을 다른 테이프에서 계속할 수 있습니다.

Spectrum Protect에 보관된 테이프에서 데이터 복원 IBM

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. IBMSpectrum Protect 백업 소프트웨어를 사용하여 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 복구 시점을 생성하여 복원합니다. 스펙트럼 보호 구성에 대한 자세한 내용은 IBM 스펙트럼 보호 [관리 작업 개요](#)를 참조하십시오. IBM

다음 단계

[불필요한 리소스 정리](#)

Micro Focus Data Protector를 사용하여 설정 테스트

Micro Focus(VTL) Data Protector v9.x를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(HPE) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway에 대해 Micro Focus (HPE) Data Protector 소프트웨어를 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다. Micro Focus (HPE) Data Protector 소프트웨어를 사용하는 방법에 대한 자세한 내용은 Hewlett Packard 설명서를 참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [VTL 디바이스와 함께 작동하도록 Micro Focus\(HPE\) 데이터 보호기 구성](#)
- [HPE 데이터 보호기와 함께 사용할 가상 테이프 준비](#)
- [테이프를 미디어 풀로 로드](#)
- [데이터를 테이프에 백업](#)
- [테이프 보관](#)
- [테이프에서 데이터 복원](#)

VTL 디바이스와 함께 작동하도록 Micro Focus(HPE) 데이터 보호기 구성

가상 테이프 라이브러리(VTL) 디바이스를 클라이언트에 연결한 후 디바이스를 인식하도록 Micro Focus(HPE) Data Protector를 구성합니다. 클라이언트에 VTL 디바이스를 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

Micro Focus (HPE) Data Protector 소프트웨어는 Tape Gateway 디바이스를 자동으로 인식하지 않습니다. 소프트웨어가 이러한 디바이스를 인식하도록 하려면 다음 설명과 같이 디바이스를 수동으로 추가한 다음 VTL 디바이스를 검색합니다.

VTL 디바이스를 추가하려면

1. 마이크로 포커스(HPE) 데이터 보호기 기본 창에서 왼쪽 상단의 목록에서 디바이스 및 미디어 선반을 선택합니다.

Devices(디바이스)를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Add Device(디바이스 추가)를 선택합니다.

2. Add Device(디바이스 추가) 탭에서 Device Name(디바이스 이름)에 값을 입력합니다. 디바이스 유형에서 SCSI 라이브러리를 선택한 다음 다음을 선택합니다.
3. 그 다음 화면에서 아래 작업을 수행합니다.
 - a. SCSI 라이브러리 로봇의 주소에서 특정 주소를 선택합니다.
 - b. Select what action Data Protector should take if the drive is busy(드라이브가 사용 중인 경우 Data Protector가 수행할 작업 선택)에서 "Abort(중단)" 또는 원하는 작업을 선택합니다.
 - c. 다음 옵션을 활성화하도록 선택합니다.
 - Barcode reader support(바코드 리더 지원)
 - 변경된 SCSI 주소 자동 검색
 - SCSI 예약/릴리스(로보틱 제어)
 - d. 시스템에 필요하지 않은 경우 Use barcode as medium label on initialization(초기화 시 미디어 레이블로 바코드 사용)을 비워둡니다(선택하지 않음).
 - e. 다음을 선택하여 계속 진행합니다.
4. 그 다음 화면에서 HP Data Protector에 사용할 슬롯을 지정합니다. 번호 사이에 하이픈("-")을 사용하여 슬롯 범위를 표시합니다(예: 1-6). 사용할 슬롯을 지정했으면 Next(다음)를 선택합니다.
5. 물리적 디바이스에서 사용하는 표준 미디어 유형에서 LTO_Ultrium을 선택한 다음 마침을 선택하여 설정을 완료합니다.

이제 테이프 라이브러리를 사용할 준비가 되었습니다. 이 라이브러리에 테이프를 로드하려면 다음 단원을 참조하십시오.

HPE 데이터 보호기와 함께 사용할 가상 테이프 준비

가상 테이프에 데이터를 백업하려면 먼저 사용할 테이프를 준비해야 합니다. 이를 위해서는 다음 작업이 필요합니다.

- 테이프 라이브러리에 가상 테이프 로드
- 슬롯에 가상 테이프 로드
- 미디어 풀 생성
- 미디어 풀에 가상 테이프 로드

다음 단원에서는 이 프로세스를 단계별로 안내합니다.

테이프 라이브러리에 가상 테이프 로드

테이프 라이브러리 목록이 Devices(디바이스) 아래에 표시됩니다. 목록이 보이지 않으면 F5를 눌러 화면을 새로 고치십시오. 라이브러리 목록이 나열되었으면 이제 가상 테이프를 라이브러리에 로드할 수 있습니다.

테이프 라이브러리에 가상 테이프를 로드하려면

1. 테이프 라이브러리 옆에 있는 더하기 기호를 선택하여 로봇 공학 경로, 드라이브 및 슬롯을 위한 노드를 표시합니다.
2. Drives(드라이브)를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Add Drive(드라이브 추가)를 선택한 다음 테이프 이름을 입력하고 Next(다음)를 선택하여 계속 진행합니다.
3. SCSI 데이터 드라이브 주소에 추가할 테이프 드라이브를 선택하고 변경된 SCSI 주소 자동 검색을 선택한 다음 다음을 선택합니다.
4. 다음 화면에서 Advanced(고급)를 선택합니다. Advanced Options(고급 옵션) 팝업 화면이 나타납니다.
 - a. Settings(설정) 탭에서 다음 옵션을 고려해야 합니다.
 - CRC 확인(우발적인 데이터 변경 감지)
 - Detect dirty drive(더티 드라이브 감지) (백업하기 전에 드라이브가 깨끗한지 확인)
 - SCSI 예약/릴리스(드라이브)(테이프 경합 방지)

테스트를 위해 이 옵션을 비활성화(선택하지 않음) 상태로 둘 수 있습니다.
 - b. Sizes(크기) 탭에서 Block size(블록 크기) (kB)를 Default(기본값) (256)로 설정합니다.
 - c. OK(확인)를 선택하여 고급 옵션 화면을 종료한 후 Next(다음)를 선택하여 계속 진행합니다.
5. 그 다음 화면에서 Device Policies(디바이스 정책)에 있는 다음 옵션을 선택합니다.
 - Device may be used for restore(디바이스를 복원에 사용할 수 있음)
 - Device may be used as source device for object copy(디바이스를 객체 복사를 위한 소스 디바이스로 사용할 수 있음)
6. Finish(마침)를 선택하여 테이프 라이브러리에 테이프 드라이브를 추가하는 작업을 마칩니다.

슬롯에 가상 테이프 로드

테이프 라이브러리에 테이프 드라이브가 있으므로 이제 가상 테이프를 슬롯에 로드할 수 있습니다.

슬롯에 테이프를 로드하려면

1. 테이프 라이브러리 트리 노드에서 Slots(슬롯)라는 레이블이 지정된 노드를 엽니다. 슬롯마다 다음과 같은 아이콘으로 상태가 표시됩니다.
 - 녹색 테이프는 테이프가 이미 슬롯에 로드되었음을 뜻합니다.
 - 회색 슬롯은 슬롯이 비어 있음을 뜻합니다.
 - 파란색 물음표는 슬롯에 있는 테이프가 포맷되어 있지 않음을 뜻합니다.
2. 빈 슬롯의 경우 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Enter(입력)를 선택합니다. 기존 테이프가 있으면 하나를 선택하여 이 슬롯에 로드합니다.

미디어 풀 생성

미디어 풀은 테이프를 체계화하는 데 사용하는 논리적 그룹입니다. 테이프 백업을 설정하려면 미디어 풀을 생성합니다.

미디어 풀을 생성하려면

1. Devices & Media(디바이스 및 미디어) 선반에서 Media(미디어)에 대한 트리 노드를 열고 Pools(풀) 노드를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Add Media Pool(미디어 풀 추가)을 선택합니다.
2. Pool name(풀 이름)에 이름을 입력합니다.
3. 미디어 유형 에서 LTO_Ultrium 을 선택한 다음 다음을 선택합니다.
4. 다음 화면에서 기본값을 적용한 후 Next(다음)를 선택합니다.
5. Finish(마침)를 선택하여 미디어 풀 생성 작업을 마칩니다.

테이프를 미디어 풀로 로드

데이터를 테이프에 백업하려면 생성한 미디어 풀에 테이프를 로드해야 합니다.

미디어 풀에 가상 테이프를 로드하려면

1. 테이프 라이브러리 트리 노드에서 Slots(슬롯) 노드를 선택합니다.
2. 로드한 테이프를 나타내는 녹색 아이콘이 있는 테이프를 선택합니다. 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Format(형식)을 선택한 후 Next(다음)를 선택합니다.
3. 생성한 미디어 풀을 선택한 후 Next(다음)를 선택합니다.

4. Medium Description(미디어 설명)에서 Use barcode(바코드 사용)를 선택한 후 Next(다음)를 선택합니다.
5. Options(옵션)에서 Force Operation(작업 강제 수행)을 선택한 후 Finish(마침)를 선택합니다.

이제 선택한 슬롯이 할당되지 않은 상태(회색)에서 테이프 삽입 상태(녹색)로 변경된 것이 보여야 합니다. 미디어가 초기화되었음을 확인하는 일련의 메시지가 표시됩니다.

이 시점에서HPE는 Data Protector와 함께 가상 테이프 라이브러리 사용을 시작하도록 구성된 모든 것이 있어야 합니다. 이를 중복 확인하려면 다음 절차를 따르십시오.

테이프 라이브러리를 사용할 수 있도록 구성했는지 확인하려면

- Drives(드라이브)를 선택한 후 해당 드라이브를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Scan(스캔)을 선택합니다.

구성이 올바르게 되었으면 미디어를 성공적으로 검색했음을 나타내는 메시지가 표시됩니다.

데이터를 테이프에 백업

테이프를 미디어 풀에 로드한 경우, 데이터를 테이프에 백업할 수 있습니다.

데이터를 테이프에 백업하려면

1. 창의 왼쪽 상단 모서리에 있는 드롭다운 메뉴에서 백업을 선택합니다.
2. 왼쪽 창에서 백업 탐색 트리를 확장합니다.
3. Filesystem을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 백업 추가를 선택합니다.
4. Create New Backup(새 백업 만들기) 화면의 Filesystem(파일 시스템)에서 Blank File System Backup(빈 파일 시스템 백업)을 선택한 후 OK(확인)를 선택합니다.
5. 해당 호스트 시스템을 표시하는 트리 노드에서 백업할 파일 시스템을 하나 또는 여러 개 선택하고 Next(다음)를 선택하여 계속 진행합니다.
6. 사용할 테이프 라이브러리의 트리 노드를 열고 사용할 테이프 드라이브를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Properties(속성)를 선택합니다.
7. 미디어 풀을 선택하고 OK(확인)를 선택한 후 Next(다음)를 선택합니다.
8. 다음 세 화면에서 기본 설정을 적용하고 Next(다음)를 선택합니다.

9. Perform finishing steps in your backup/template design(백업/템플릿 디자인에서 마무리 단계 수행) 화면에서 Save as(다른 이름으로 저장)를 선택하여 이 세션을 저장합니다. 팝업 창에서 백업의 이름을 정하고 이를 새 백업 지정을 저장할 그룹에 할당합니다.
10. Start Interactive Backup(대화형 백업 시작)을 선택합니다.

호스트 시스템이 데이터베이스 시스템을 포함하는 경우, 대상 백업 시스템으로 선택할 수 있습니다. 화면과 선택 항목은 방금 설명한 파일 시스템 백업과 비슷합니다.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패하고 Data Protector의 테이프 드라이브 상태가 더티로 표시됩니다. 또한 Data Protector는 테이프 품질을 불량으로 표시하고 테이프에 쓰기를 방지합니다. 테이프에서 데이터를 계속 읽으려면 드라이브를 청소하고 테이프를 다시 마운트해야 합니다. 실패한 백업 작업을 완료하려면 해당 작업을 새 테이프에 다시 제출해야 합니다.

테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 테이프를 배출하여 보관하기 전에 테이프에 있는 콘텐츠를 확인하고 싶은 경우가 있습니다.

보관하기 전에 테이프의 콘텐츠를 확인하려면

1. Slots(슬롯)를 선택한 후 확인할 테이프를 선택합니다.
2. Objects(객체)를 선택하고 테이프에 있는 콘텐츠가 무엇인지 확인합니다.

보관할 테이프를 선택했으면 다음 절차를 수행합니다.

테이프를 배출하여 보관하려면

1. 해당 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Eject(배출)를 선택합니다.
2. Storage Gateway 콘솔에서 게이트웨이를 선택한 다음 VTL 테이프 카트리지를 선택하고 아카이빙 중인 가상 테이프의 상태를 확인합니다.

테이프가 배출되면 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 자동으로 아카이브됩니다. 보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다 ARCHIVING. 아카이브가 완료되면 테이프는 더 이상 에 나열되지 VTL 않지만 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브됩니다.

테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. HPE 데이터 보호기를 사용하여 데이터를 복원합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다.

테이프에서 데이터를 복원하려면 다음 절차 대로 합니다.

테이프에서 데이터를 복원하려면

1. 창의 왼쪽 상단 모서리에 있는 드롭다운 메뉴에서 복원을 선택합니다.
2. 왼쪽 탐색 트리에서 복원할 파일 시스템 또는 데이터베이스 시스템을 선택합니다. 복원할 백업에 대해 상자가 선택되어 있는지 확인합니다. 복원을 선택합니다.
3. Start Restore Session(복원 세션 시작) 창에서 Needed Media(필요한 미디어)를 선택합니다. All media(모든 미디어)를 선택하면 백업에 원래 사용한 테이프가 표시되어야 합니다. 해당 테이프를 선택한 후 Close(닫기)를 선택합니다.
4. Start Restore Session(복원 세션 시작) 창에서 기본 설정을 적용하고 Next(다음)를 선택한 후 Finish(마침)를 선택합니다.

다음 단계

[불필요한 리소스 정리](#)

Microsoft System Center를 사용하여 설정 테스트 DPM

Microsoft System Center 2012 R2 또는 2016 Data Protection Manager(VTL)를 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리() 디바이스를 관리할 수 있습니다.

니다DPM. 이 주제에서는 Tape Gateway에 대한 DPM 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다.

사용 방법에 대한 자세한 내용은 Microsoft System Center 웹 사이트의 [DPM 설명서](#)를 DPM참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [VTL 디바이스를 인식DPM하도록 구성](#)
- [로 테이프 가져오기 DPM](#)
- [에서 테이프에 데이터 쓰기 DPM](#)
- [를 사용하여 테이프 보관 DPM](#)
- [에 보관된 테이프에서 데이터 복원 DPM](#)

VTL 디바이스를 인식DPM하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식DPM하도록 를 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

기본적으로 DPM 서버는 Tape Gateway 디바이스를 인식하지 않습니다. 서버가 Tape Gateway 디바이스와 함께 작동하도록 구성하려면 다음 작업을 수행해야 합니다.

1. 디바이스의 VTL 디바이스 드라이버를 업데이트하여 DPM 서버에 노출시킵니다.
2. VTL 디바이스를 DPM 테이프 라이브러리에 수동으로 매핑합니다.

VTL 디바이스 드라이버를 업데이트하려면

- 디바이스 관리자에서 미디어 체인저용 드라이버를 업데이트합니다. 지침은 [미디어 체인저의 디바이스 드라이버 업데이트](#) 단원을 참조하십시오.

DPMDriveMappingTool 를 사용하여 테이프 드라이브를 DPM 테이프 라이브러리에 매핑합니다.

테이프 드라이브를 DPM 서버 테이프 라이브러리에 매핑하려면

1. 게이트웨이용 테이프를 최소 한 개는 만들어야 합니다. 콘솔에서 이를 수행하는 방법은 [테이프 생성](#)을 참조하세요.

- 테이프를 DPM 라이브러리로 가져옵니다. 이렇게 하는 방법에 대한 정보는 [로 테이프 가져오기 DPM](#) 단원을 참조하십시오.
- DPMLA 서비스가 실행 중인 경우 명령 터미널을 열고 명령줄에 다음을 입력하여 중지합니다.

net stop DPMLA

- DPM 서버에서 다음 파일을 찾습니다 %ProgramFiles%\System Center 2016 R2\DPM\DPM\Config\DPMLA.xml.

Note

이 파일이 있는 경우는 파일을 DPMDriveMappingTool 덮어씁니다. 원본 파일을 보존하려면 백업 사본을 생성해야 합니다.

- 명령 터미널을 열어 %ProgramFiles%\System Center 2016 R2\DPM\DPM\Bin 디렉터리로 변경한 후 다음 명령을 실행합니다.

```
C:\Microsoft System Center 2016 R2\DPM\DPM\bin>DPMDriveMappingTool.exe
```

이 명령에 대한 출력은 다음과 같습니다.

```
Performing Device Inventory ...
Mapping Drives to Library ...
Adding Standalone Drives ...
Writing the Map File ...
Drive Mapping Completed Successfully.
```

로 테이프 가져오기 DPM

이제 Tape Gateway에서 DPM 백업 애플리케이션 라이브러리로 테이프를 가져올 준비가 되었습니다.

DPM 백업 애플리케이션 라이브러리로 테이프를 가져오려면

1. DPM 서버에서 관리 콘솔을 열고 재스캔을 선택한 다음 새로 고침을 선택합니다. 관리 콘솔에는 미디어 체인저 및 테이프 드라이브가 표시됩니다.
2. Library(라이브러리) 섹션에서 미디어 체인저를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Add tape (I/E port)(테이프 추가(I/E 포트))를 선택하여 테이프를 Slots(슬롯) 목록에 추가합니다.

Note

테이프 추가 프로세스를 완료하는 데 몇 분 정도 걸릴 수 있습니다.

테이프 레이블이 Unknown(알수 없음)으로 표시되고 테이프는 사용할 수 없습니다. 테이프를 사용할 수 있으려면 먼저 해당 테이프를 식별해야 합니다.

3. 식별할 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Identify unknown tape(알수 없는 테이프 식별)를 선택합니다.

Note

테이프 식별 프로세스를 완료하는 데 몇 초 또는 몇 분이 걸릴 수 있습니다.

테이프에 바코드가 올바르게 표시되지 않으면 미디어 체인저 드라이버를 Sun/StorageTek Library로 변경해야 합니다. 자세한 내용은 [Microsoft System Center에서 테이프용 바코드 표시 DPM](#) 단원을 참조하십시오.

식별이 완료되면 테이프 레이블이 Free(사용 가능)로 바뀝니다. 즉 테이프에 데이터를 자유롭게 쓸 수 있는 상태가 됩니다.

에서 테이프에 데이터 쓰기 DPM

물리적 테이프에 대해 수행하는 것과 동일한 보호 절차 및 정책을 사용하여 Tape Gateway 가상 테이프에 데이터를 기록합니다. 보호 그룹을 생성하고 백업할 데이터를 추가한 후 복원 시점을 생성하여 데이터를 백업합니다. 사용 방법에 대한 자세한 내용은 Microsoft System Center 웹 사이트의 [DPM 설명서를](#) DPM참조하세요.

테이프의 기본 용량은 30GB입니다. 백업 데이터가 테이프 용량보다 클 경우에는 장치 I/O 오류가 발생합니다. 오류가 발생한 위치가 테이프 크기보다 크면 Microsoft는 오류를 테이프 끝의 표시로 DPM 추

급합니다. 반대로 테이프 크기를 넘지 않는 위치에서 오류가 발생하면 백업 작업이 중단됩니다. 이 문제를 해결하려면 레지스트리 항목에서 TapeSize 값을 테이프 크기에 맞게 변경하십시오. 이렇게 하는 방법에 대한 자세한 내용은 Microsoft 시스템 센터에서 [Error ID: 30101](#)을 참조하십시오.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패합니다. 실패한 백업 작업을 완료하려면 해당 작업을 다시 제출해야 합니다.

를 사용하여 테이프 보관 DPM

테이프를 아카이브하면 Tape Gateway가 테이프 라이브러리에서 오프라인 스토리지로 DPM 테이프를 이동합니다. 백업 애플리케이션, 즉 를 사용하여 슬롯에서 테이프를 제거하여 테이프 아카이브를 시작합니다DPM.

에서 테이프를 아카이브하려면 DPM

1. 보관할 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Remove tape (I/E port) (테이프 제거(I/E 포트))를 선택합니다.
2. 다음에 나타나는 대화 상자에서 Yes(예)를 선택합니다. 이렇게 하면 미디어 체인저의 스토리지 슬롯에서 테이프가 빠져나와 게이트웨이의 I/E 슬롯 중 하나로 이동합니다. 테이프가 게이트웨이의 I/E 슬롯으로 이동하면 보관을 위해 즉시 전송됩니다.
3. Storage Gateway 콘솔에서 게이트웨이를 선택한 다음 VTL 테이프 카트리지를 선택하고 보관 중인 가상 테이프의 상태를 확인합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다ARCHIVING. 아카이브가 완료되면 테이프가 더 이상 에 나열되지 않습니다VTL.

에 보관된 테이프에서 데이터 복원 DPM

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.

2. DPM 백업 애플리케이션을 사용하여 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 복구 시점을 생성하여 복원합니다. 지침은 DPM 웹 사이트의 [클라이언트 컴퓨터 데이터 복구](#)를 참조하세요.

다음 단계

[불필요한 리소스 정리](#)

를 사용하여 설정 테스트 NovaStor DataCenter

NovaStor DataCenter/Network 버전 6.4 또는 7.1을 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway에 대한 NovaStor DataCenter/Network 버전 7.1 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다. NovaStor DataCenter/Network 버전 7.1을 사용하는 방법에 대한 자세한 내용은 [설명서 NovaStor DataCenter/네트워크](#)를 참조하세요.

NovaStor DataCenter/Network 설정

가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 클라이언트에 연결한 후 디바이스를 인식하도록 NovaStor 소프트웨어를 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

NovaStor DataCenter/Network에는 드라이버 제조업체의 드라이버가 필요합니다. Windows 드라이버를 사용할 수 있으나, 먼저 다른 백업 애플리케이션을 비활성화해야 합니다.

VTL 디바이스와 함께 작동하도록 NovaStor DataCenter/Network 구성

NovaStor DataCenter/Network 버전 6.4 또는 7.1에서 작동하도록 VTL 디바이스를 구성할 때 라는 오류 메시지가 표시될 수 있습니다 External Program did not exit correctly. 이 문제가 발생하면 계속하기 전에 해결 방법을 수행해야 합니다.

VTL 디바이스 구성을 시작하기 전에 해결 방법을 생성하여 문제를 방지할 수 있습니다. 해결 방법을 수립하는 방법에 대한 자세한 내용은 ["외부 프로그램이 올바르게 종료되지 않았습니다" 오류 해결](#) 단원을 참조하십시오.

VTL 디바이스와 함께 작동하도록 NovaStor DataCenter/Network를 구성하려면

1. NovaStor DataCenter/Network Admin 콘솔에서 미디어 관리를 선택한 다음 스토리지 관리를 선택합니다.

2. Storage Targets(스토리지 대상) 메뉴에서 Media Management Servers(미디어 관리 서버)의 컨텍스트 메뉴(오른쪽 클릭)를 연 다음, New(새로 만들기)를 선택하고 OK(확인)를 선택하여 storage(스토리지) 노드를 생성하고 미리 채웁니다.

External Program did not exit correctly라는 오류 메시지가 보이면 계속하기 전에 문제를 해결합니다. 이 문제가 발생하면 해결 방법을 수행해야 합니다. 이 문제를 해결하는 방법에 대한 자세한 내용은 ["외부 프로그램이 올바르게 종료되지 않았습니다" 오류 해결](#) 단원을 참조하십시오.

Important

이 오류는 스토리지 드라이브 및 테이프 드라이브에 대한 의 AWS Storage Gateway 요소 할당 범위가 DataCenter/Network에서 NovaStor 허용하는 수를 초과하기 때문에 발생합니다.

3. 생성된 storage(스토리지) 노드의 컨텍스트(오른쪽 클릭) 메뉴를 열고 New Library(새 라이브러리)를 선택합니다.
4. 목록에서 라이브러리 서버를 선택합니다. 라이브러리 목록이 자동으로 채워집니다.
5. 라이브러리 이름을 지정하고 OK(확인)를 선택합니다.
6. 라이브러리를 선택하여 Storage Gateway 가상 테이프 라이브러리의 속성을 모두 표시합니다.
7. Storage Targets(스토리지 대상) 메뉴에서 Backup Servers(백업 서버)를 확장한 다음, 서버의 컨텍스트(오른쪽 클릭) 메뉴를 열고 Attach Library(라이브러리 연결)를 선택합니다.
8. 나타나는 라이브러리 연결 대화 상자에서 LTO5 미디어 유형을 선택한 다음 확인을 선택합니다.
9. 백업 서버를 확장하여 Storage Gateway 가상 테이프 라이브러리와 마운트된 테이프 드라이브를 모두 표시하는 라이브러리 파티션을 표시합니다.

테이프 풀 생성

테이프 풀은 NovaStor DataCenter/Network 소프트웨어에서 동적으로 생성되므로 고정된 수의 미디어를 포함하지 않습니다. 테이프가 필요한 테이프 풀은 스크래치 풀에서 테이프를 가져옵니다. 스크래치 풀은 사용할 하나 이상의 테이프 풀에서 자유롭게 이용할 수 있는 테이프 리저버입니다. 테이프 풀은 보존 시간을 초과했으며 더 이상 필요하지 않은 모든 미디어를 스크래치 풀로 반환합니다.

테이프 풀은 3단계 작업으로 생성할 수 있습니다.

1. 스크래치 풀을 생성합니다.
2. 스크래치 풀에 테이프를 할당합니다.
3. 테이프 풀을 생성합니다.

스크래치 풀을 생성하려면

1. 왼쪽 탐색 메뉴에서 Scratch Pools(스크래치 풀) 탭을 선택합니다.
2. Scratch Pools(스크래치 풀)의 컨텍스트(오른쪽 클릭) 메뉴를 열고 Create Scratch Pool(스크래치 풀 생성)을 선택합니다.
3. Scratch Pools(스크래치 풀) 대화 상자에서 스크래치 풀의 이름을 지정한 후, 미디어 유형을 선택합니다.
4. Label Volume(레이블 볼륨)을 선택한 후, 스크래치 풀의 하위 워터마크를 만듭니다. 스크래치 풀이 하위 워터마크까지 비면 경고가 표시됩니다.
5. 표시되는 경고 대화 상자에서 OK(확인)를 선택하여 스크래치 풀을 생성합니다.

스크래치 풀에 테이프를 할당하려면

1. 왼쪽 탐색 창에서 Tape Library Management(테이프 라이브러리 관리)를 선택합니다.
2. Library(라이브러리) 탭을 선택하여 라이브러리의 인벤토리를 봅니다.
3. 스크래치 풀에 할당하려는 테이프를 선택합니다. 테이프가 올바른 미디어 유형으로 설정되어 있는지 확인합니다.
4. 라이브러리의 컨텍스트(오른쪽 클릭) 메뉴를 열고 Add to Scratch Pool(스크래치 풀에 추가)을 선택합니다.

이제 테이프 풀에 사용할 수 있는 채워진 스크래치 풀이 생성되었습니다.

테이프 풀을 생성하려면

1. 왼쪽 탐색 창에서 Tape Library Management(테이프 라이브러리 관리)를 선택합니다.
2. Media Pools(미디어 풀) 탭의 컨텍스트(오른쪽 클릭) 메뉴를 열고 Create Media Pool(미디어 풀 생성)을 선택합니다.
3. 미디어 풀의 이름을 지정하고 Backup Server(백업 서버)를 선택합니다.
4. 미디어 풀의 라이브러리 파티션을 선택합니다.
5. 풀이 테이프를 가져올 스크래치 풀을 선택합니다.

6. Schedule(일정)에서 Not Scheduled(예약되지 않음)를 선택합니다.

아카이브 테이프로 미디어 가져오기 및 내보내기 구성

NovaStor DataCenter/Network는 가져오기/내보내기 슬롯이 미디어 체인저의 일부인 경우 슬롯을 사용할 수 있습니다.

내보내기의 경우 NovaStor DataCenter/네트워크는 라이브러리에서 물리적으로 제거할 테이프를 알아야 합니다.

가져오기의 경우 NovaStor DataCenter/Network는 테이프 라이브러리에서 내보내는 테이프 미디어를 인식하고 데이터 슬롯 또는 내보내기 슬롯에서 모두 가져올 것을 제안합니다. Tape Gateway는 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 테이프를 아카이브합니다.

미디어 가져오기 및 내보내기를 구성하려면

1. Tape Library Management(테이프 라이브러리 관리)로 이동하고 Media Management Server(미디어 관리 서버)에서 서버를 선택한 후, Library(라이브러리)를 선택합니다.
2. Off-site Locations(오프사이트 위치) 탭을 선택합니다.
3. 흰색 영역의 컨텍스트(오른쪽 클릭) 메뉴를 열고 Add(추가)를 선택하여 새 패널을 엽니다.
4. 패널에 **S3 Glacier Flexible Retrieval** 또는 **S3 Glacier Deep Archive**를 입력하고 텍스트 상자에 설명(선택 사항)을 추가합니다.

데이터를 테이프에 백업

물리적 테이프에 대해 수행하는 것과 동일한 절차를 사용하여 백업 작업을 생성하고 가상 테이프에 데이터를 작성합니다. NovaStor 소프트웨어를 사용하여 데이터를 백업하는 방법에 대한 자세한 내용은 [설명서 NovaStor DataCenter/네트워크](#) 를 참조하세요.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패하고 테이프에 쓸 수 없게 됩니다. 테이프를 아카이브하거나 테이프에서 데이터를 계속 읽을 수 있습니다. 실패한 백업 작업을 완료하려면 해당 작업을 새 테이프에 다시 제출해야 합니다.

테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 테이프 라이브러리에서 오프라인 스토리지로 배출합니다. 그런 다음 백업 애플리케이션, 즉 NovaStor DataCenter/Network를 사용하여 슬롯에서 아카이브로 테이프를 내보냅니다.

테이프를 보관하려면

1. 왼쪽 탐색 창에서 Tape Library Management(테이프 라이브러리 관리)를 선택합니다.
2. Library(라이브러리) 탭을 선택하여 라이브러리의 인벤토리를 봅니다.
3. 보관하려는 테이프를 강조 표시하고, 해당 테이프의 바로 가기 메뉴(마우스 오른쪽 버튼 클릭)를 연 후, 오프사이트 아카이브 위치를 선택합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다ARCHIVING. 아카이브가 완료되면 테이프가 더 이상 에 나열되지 않습니다VTL.

NovaStor DataCenter/Network에서 테이프가 더 이상 스토리지 슬롯에 없는지 확인합니다.

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 인지 확인합니다ARCHIVED.

보관 및 검색을 했던 테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. NovaStor DataCenter/Network 소프트웨어를 사용하여 데이터를 복원합니다. 이렇게 하려면 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 메일 슬롯을 새로 고치고 가져오려는 각 테이프를 빈 슬롯으로 이동합니다. 데이터 복원에 대한 자세한 내용은 [설명서 NovaStor DataCenter/네트워크](#)를 참조하세요.

여러 백업 작업을 테이프 드라이브에 동시에 기록

NovaStor 소프트웨어에서는 멀티플렉싱 기능을 사용하여 테이프 드라이브에 여러 작업을 동시에 실행할 수 있습니다. 이 기능은 미디어 풀에서 멀티플렉서를 사용할 수 있는 경우에 사용 가능합니다. 멀티플렉싱을 사용하는 방법에 대한 자세한 내용은 [설명서 NovaStor DataCenter/네트워크](#) 를 참조하세요.

"외부 프로그램이 올바르게 종료되지 않았습니다" 오류 해결

NovaStor DataCenter/Network 버전 6.4 또는 7.1에서 작동하도록 VTL 디바이스를 구성할 때 라는 오류 메시지가 표시될 수 있습니다 External Program did not exit correctly. 이 오류는 스토리지 드라이브 및 테이프 드라이브에 대한 Storage Gateway의 요소 할당 범위가 DataCenter/Network에서 허용하는 수를 초과하기 NovaStor 때문에 발생합니다.

Storage Gateway는 /Network에서 허용하는 한도인 2400개를 초과하는 3200개의 스토리지 및 가져오기 NovaStor DataCenter/내보내기 슬롯을 반환합니다. 이 문제를 해결하려면 NovaStor 소프트웨어를 활성화하여 스토리지 및 가져오기/내보내기 슬롯 수를 제한하고 요소 할당 범위를 사전 구성하는 구성 파일을 추가합니다.

"외부 프로그램이 올바르게 종료되지 않았습니다" 오류에 대한 해결 방법을 적용하려면

1. 소프트웨어를 설치한 컴퓨터의 테이프 폴더로 NovaStor 이동합니다.
2. 테이프 폴더에서 텍스트 파일을 만들고 이름을 hijacc.ini로 지정합니다.
3. 다음 콘텐츠를 복사하고, hijacc.ini 파일에 붙여 넣은 후, 파일을 저장합니다.

```
port:12001
san:no
define: A3B0S0L0
*DRIVES: 10
*FIRST_DRIVE: 10000
*SLOTS: 200
*FIRST_SLOT: 20000
*HANDLERS: 1
*FIRST_HANDLER: 0
*IMP-EXPS: 30
*FIRST_IMP-EXP: 30000
```

4. 라이브러리를 추가하고 미디어 관리 서버에 연결합니다.
5. 다음 명령을 사용하여 가져오기/내보내기 슬롯에서 라이브러리로 테이프를 이동합니다. 예제 라이브러리 이름을 배포의 라이브러리 이름으로 바꿉니다.

```
C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c VTL-ec2amaz-uko8jffj-ec2amaz-uko8jffj.lcfg
```

6. 백업 서버에 라이브러리를 연결합니다.
7. NovaStor 소프트웨어에서 가져오기/내보내기 슬롯의 모든 테이프를 라이브러리로 가져옵니다.

Quest NetVault Backup을 사용하여 설정 테스트

다음 Quest(이전 DellVTL) NetVault 백업 버전을 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리() 디바이스를 관리할 수 있습니다.

- Quest NetVault Backup 12.4
- Quest NetVault Backup 13.x

이 주제에서는 Tape Gateway에 대한 Quest NetVault Backup 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다.

Quest NetVault Backup 애플리케이션을 사용하는 방법에 대한 자세한 내용은 Quest NetVault Backup – 관리 안내서를 참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [VTL 디바이스와 함께 작동하도록 Quest NetVault Backup 구성](#)
- [Quest NetVault Backup의 테이프에 데이터 백업](#)
- [Quest NetVault Backup을 사용하여 테이프 보관](#)
- [Quest NetVault Backup에 보관된 테이프에서 데이터 복원](#)

VTL 디바이스와 함께 작동하도록 Quest NetVault Backup 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식하도록 Quest NetVault Backup을 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

Quest NetVault Backup 애플리케이션은 Tape Gateway 디바이스를 자동으로 인식하지 않습니다. 디바이스를 수동으로 추가하여 Quest NetVault Backup 애플리케이션에 노출한 다음 VTL 디바이스를 검색해야 합니다.

VTL 디바이스 추가

VTL 디바이스를 추가하려면

1. Quest NetVault Backup의 구성 탭에서 디바이스 관리를 선택합니다.
2. Manage Devices(디바이스 관리) 페이지에서 Add Devices(디바이스 추가)를 선택합니다.
3. Add Storage Wizard(스토리지 추가 마법사)에서 Tape library / media changer(테이프 라이브러리/미디어 체인저)를 선택한 후 Next(다음)를 선택합니다.
4. 그 다음 페이지에서 라이브러리에 물리적으로 연결된 클라이언트 머신을 선택하고 Next(다음)를 선택하여 디바이스를 찾습니다.
5. 디바이스를 찾으면 화면에 표시됩니다. 이 경우 미디어 체인저는 디바이스 상자에 표시됩니다.
6. 미디어 체인저를 선택하고 Next(다음)를 선택합니다. 디바이스에 대한 세부 정보가 마법사에 표시됩니다.
7. Add Tapes to Bays(베이에 테이프 추가) 페이지에서 Scan For Devices(디바이스 스캔)를 선택하고 클라이언트 머신을 선택한 후 Next(다음)를 선택합니다.

Quest NetVault Backup은 모든 드라이브와 드라이브를 추가할 수 있는 10베이를 표시합니다. 베이는 한 번에 하나씩 표시됩니다.

8. 표시된 베이에 추가할 드라이브를 선택한 후 Next(다음)를 선택합니다.

Important

베이에 드라이브를 추가할 때 해당 드라이브와 베이의 숫자가 일치해야 합니다. 예를 들어 1번 베이가 표시되면 1번 드라이브를 추가해야 합니다. 해당 드라이브가 연결되어 있지 않으면 숫자가 일치하는 베이를 비워둡니다.

9. 클라이언트 머신이 표시되면 선택한 후 Next(다음)를 선택합니다. 클라이언트 머신은 여러 차례 표시될 수 있습니다.
10. 드라이브가 표시되면 7~9단계를 반복하여 베이에 모든 드라이브를 추가합니다.
11. Configuration(구성) 탭에서 Manage devices(디바이스 관리)를 선택하고 Manage Devices(디바이스 관리) 페이지에서 미디어 체인저를 펼쳐 추가한 디바이스를 확인합니다.

Quest NetVault Backup의 테이프에 데이터 백업

물리적 테이프에 대해 수행하는 것과 동일한 절차를 사용하여 백업 작업을 생성하고 가상 테이프에 데이터를 작성합니다. 데이터 백업 방법에 대한 자세한 내용은 [Quest NetVault Backup - 관리 안내서](#)를 참조하세요.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패합니다. 실패한 백업 작업을 완료하려면 해당 작업을 다시 제출해야 합니다.

Quest NetVault Backup을 사용하여 테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 테이프 라이브러리에서 오프라인 스토리지로 배출합니다. 그런 다음 백업 애플리케이션, 즉 Quest NetVault Backup을 사용하여 슬롯에서 아카이브로 테이프를 내보냅니다.

Quest NetVault Backup에서 테이프를 아카이브하려면

1. Quest NetVault Backup 구성 탭에서 미디어 체인저를 선택하고 확장하여 테이프를 확인합니다.
2. 슬롯의 설정 아이콘을 선택하여 미디어 체인저의 슬롯 브라우저를 엽니다.
3. 슬롯에서 아카이브하려는 테이프를 선택한 다음 내보내기를 선택합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다ARCHIVING. 아카이브가 완료되면 테이프가 더 이상 에 나열되지 않습니다VTL.

Quest NetVault Backup 소프트웨어에서 테이프가 더 이상 스토리지 슬롯에 없는지 확인합니다.

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 인지 확인합니다ARCHIVED.

Quest NetVault Backup에 보관된 테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. Quest NetVault Backup 애플리케이션을 사용하여 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 폴더 복원 파일을 생성합니다. 복원 작업 생성에 대한 지침은 [Quest NetVault Backup - 관리 안내서](#)를 참조하세요.

다음 단계

[불필요한 리소스 정리](#)

Veeam Backup and Replication을 사용하여 설정 테스트

Veeam Backup & Replication 11A 를 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 Veeam Backup & Replication 소프트웨어를 구성하고 백업 및 복원 작업을 수행하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다. Veeam 소프트웨어 사용 방법에 대한 자세한 내용은 Veeam 도움말 센터에서 [Veeam Backup & Replication 정보](#)를 참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [VTL 디바이스와 함께 작동하도록 Veeam 구성](#)
- [테이프를 Veeam으로 가져오기](#)
- [Veeam에서 데이터를 테이프로 백업](#)
- [Veeam을 사용한 테이프 보관](#)
- [Veeam에 보관한 테이프에서 데이터 복원](#)

VTL 디바이스와 함께 작동하도록 Veeam 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식하도록 Veeam Backup & Replication을 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

VTL 디바이스 드라이버 업데이트

Tape Gateway 디바이스와 함께 작동하도록 소프트웨어를 구성하려면 디바이스의 VTL 디바이스 드라이버를 업데이트하여 Veeam 소프트웨어에 노출한 다음 VTL 디바이스를 검색합니다. 디바이스 관리

자에서 미디어 체인저용 드라이버를 업데이트합니다. 지침은 [미디어 체인저의 디바이스 드라이버 업데이트](#) 단원을 참조하십시오.

VTL 디바이스 검색

미디어 체인저를 알 수 없는 경우 Windows 드라이버 대신 기본 SCSI 명령을 사용하여 테이프 라이브러리를 검색해야 합니다. 자세한 지침은 [테이프 라이브러리](#)를 참조하세요.

VTL 디바이스를 검색하려면

1. Veeam 소프트웨어에서 백업 인프라를 선택합니다. Tape Gateway가 연결되면 백업 인프라 탭에 가상 테이프 목록이 표시됩니다.
2. Tape(테이프) 트리를 펼쳐 테이프 드라이브와 미디어 체인저를 확인합니다.
3. 미디어 체인저 트리를 펼칩니다. 테이프 드라이브가 미디어 체인저에 매핑된 경우, 해당 드라이브가 Drives(드라이브)에 표시됩니다. 그렇지 않은 경우에는 테이프 라이브러리와 테이프 드라이브가 별도 디바이스로 표시됩니다.

드라이브가 자동으로 매핑되지 않은 경우, [Veeam 웹 사이트의 지침](#)에 따라 드라이브를 매핑합니다.

테이프를 Veeam으로 가져오기

이제 Tape Gateway에서 Veeam 백업 애플리케이션 라이브러리로 테이프를 가져올 준비가 되었습니다.

테이프를 Veeam 라이브러리로 가져오려면

1. 미디어 체인저를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Import(가져오기)를 선택하여 테이프를 I/E 슬롯으로 가져옵니다.
2. 미디어 체인저를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Inventory Library(인벤토리 라이브러리)를 선택하여 인식되지 않은 테이프를 식별합니다. 테이프 드라이브에 새 가상 테이프를 처음 로드하는 경우, Veeam 백업 애플리케이션은 테이프를 인식하지 못합니다. 인식되지 않은 테이프를 식별하기 위해 테이프 라이브러리에 테이프 목록을 만듭니다.

Veeam에서 데이터를 테이프로 백업

데이터를 테이프로 백업하는 절차는 다음과 같이 두 단계로 이루어져 있습니다.

1. 미디어 풀을 생성하고 미디어 풀에 테이프를 추가합니다.

2. 테이프에 데이터를 씁니다.

물리적 테이프에 대해 수행하는 것과 동일한 절차를 사용하여 미디어 풀을 생성하고 가상 테이프에 데이터를 작성합니다. 데이터를 백업하는 방법에 대한 자세한 내용은 Veeam 도움말 센터에서 [테이프 시작하기](#)를 참조하세요.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패합니다. 실패한 백업 작업을 완료하려면 해당 작업을 다시 제출해야 합니다.

Veeam을 사용한 테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 Veeam 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 테이프 드라이브에서 스토리지 슬롯으로 테이프를 꺼낸 다음 백업 애플리케이션, 즉 Veeam 소프트웨어를 사용하여 슬롯에서 아카이브로 테이프를 내보내면 테이프 아카이브가 시작됩니다.

Veeam 라이브러리에 테이프를 보관하려면

1. 백업 인프라를 선택하고 아카이브할 테이프가 들어 있는 미디어 풀을 선택합니다.
2. 보관할 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Eject Tape(테이프 배출)를 선택합니다.
3. Ejecting tape(테이프 배출 중)에서 Close(닫기)를 선택합니다. 테이프가 테이프 드라이브에서 슬롯으로 이동합니다.
4. 테이프를 다시 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Export(내보내기)를 선택합니다. 테이프의 상태가 Tape drive(테이프 드라이브)에서 Offline(오프라인)으로 변경됩니다.
5. Exporting tape(테이프 내보내는 중)에서 Close(닫기)를 선택합니다. 테이프의 위치가 Slot(슬롯)에서 Offline(오프라인)으로 변경됩니다.
6. Storage Gateway 콘솔에서 게이트웨이를 선택한 다음 VTL 테이프 카트리지를 선택하고 보관 중인 가상 테이프의 상태를 확인합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 로 변경됩니다 ARCHIVING. 아카이브가 완료되면 테이프는 더 이상 에 나열되지 VTL 않지만 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브됩니다.

Veeam에 보관한 테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 아카이브에서 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. Veeam 소프트웨어를 사용하여 해당 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 폴더 복원 파일을 생성합니다. 관련 지침은 Veeam 도움말 센터에서 [테이프에서 파일 복원](#)을 참조하세요.

다음 단계

[불필요한 리소스 정리](#)

Veritas Backup Exec을 사용한 설정 테스트

Veritas Backup Exec을 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 보관하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 단원에서는 다음 Backup Exec 버전을 사용하여 백업 및 복원 작업을 수행하는 데 필요한 기본 문서를 볼 수 있습니다.

- Veritas Backup Exec 2014
- Veritas Backup Exec 15
- Veritas Backup Exec 16
- Veritas Backup Exec 20.x
- Veritas Backup Exec 22.x

Tape Gateway에서 이 버전의 Backup Exec를 사용하는 절차는 동일합니다. Backup Exec을 사용하여 보안 백업을 생성하는 방법, 소프트웨어 및 하드웨어 호환성 목록, Backup Exec에 대한 관리자 안내서를 포함하여 Backup Exec을 사용하는 방법에 대한 자세한 내용은 [Veritas 지원 웹 사이트](#)를 참조하십시오.

지원되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [Backup Exec에서 스토리지 구성](#)

- [Backup Exec에 있는 테이프 가져오기](#)
- [Backup Exec에 있는 테이프에 데이터 쓰기](#)
- [Backup Exec을 사용한 테이프 보관](#)
- [Backup Exec에 보관한 테이프에서 데이터 복원](#)
- [Backup Exec에서 테이프 드라이브 비활성화](#)

Backup Exec에서 스토리지 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식하도록 Backup Exec 스토리지를 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [VTL 디바이스 연결](#).

스토리지를 구성하려면

1. Backup Exec 소프트웨어를 시작한 후 도구 모음 왼쪽 상단에 있는 노란색 아이콘을 선택합니다.
2. Configuration and Settings(구성 및 설정)를 선택한 다음 Backup Exec Services를 선택하여 Backup Exec Service Manager를 엽니다.
3. Restart All Services(모든 서비스 다시 시작)를 선택합니다. 그러면 Backup Exec이 VTL 디바이스(즉, 미디어 체인저 및 테이프 드라이브)를 인식합니다. 재시작 프로세스에는 몇 분이 걸릴 수 있습니다.

Note

Tape Gateway는 10개의 테이프 드라이브를 제공합니다. 그러나 Backup Exec 라이선스 계약에는 테이프 드라이브 10개 미만으로 작업할 백업 애플리케이션이 필요할 수 있습니다. 이러한 경우에는 Backup Exec 로봇 공학 라이브러리에 있는 테이프 드라이브를 비활성화하여 라이선스 계약에 허용된 테이프 드라이브 개수만 활성화 상태로 유지해야 합니다. 지침은 [Backup Exec에서 테이프 드라이브 비활성화](#) 단원을 참조하십시오.

4. 재시작이 완료되면 Backup Exec Service Manager를 종료합니다.

Backup Exec에 있는 테이프 가져오기

이제 게이트웨이에서 슬롯으로 테이프를 가져올 준비가 되었습니다.

1. 스토리지 탭을 선택한 다음 로봣 라이브러리 트리를 확장하여 VTL 디바이스를 표시합니다.

⚠ Important

Veritas Backup Exec 소프트웨어에는 Tape Gateway 미디어 체인저 유형이 필요합니다. 로봇 공학 라이브러리에 나열된 미디어 체인저 유형이 Tape Gateway가 아닌 경우, 백업 애플리케이션에서 스토리지를 구성하기 전에 해당 유형을 변경해야 합니다. 다른 미디어 체인저 유형을 선택하는 방법에 대한 정보는 [게이트웨이 활성화 후 미디어 체인저 선택 단원](#)을 참조하십시오.

2. Slots(슬롯) 아이콘을 선택하여 모든 슬롯을 표시합니다.

ℹ Note

테이프를 로봇 공학 라이브러리로 가져오는 경우, 테이프는 테이프 드라이브 대신에 슬롯에 저장됩니다. 그러므로 테이프 드라이브에는 드라이브에 미디어가 없다는 것을 나타내는 메시지(No media)가 표시될 수 있습니다. 백업을 시작하거나 작업을 복원하는 경우, 테이프는 테이프 드라이브로 이동합니다.

테이프를 스토리지 슬롯으로 가져오려면 게이트웨이 테이프 라이브러리에 가용 테이프가 있어야 합니다. 테이프를 만드는 방법에 대한 지침은 [Tape Gateway용 새 가상 테이프 생성](#) 단원을 참조하십시오.

3. 빈 슬롯을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Import(가져오기)를 선택한 다음 Import media now(지금 미디어 가져오기)를 선택합니다. 슬롯을 하나 이상 선택하고 가져오기 작업 하나로 테이프를 여러 개 가져올 수 있습니다.
4. 다음에 나타나는 Media Request(미디어 요청) 창에서 View details(세부 정보 보기)를 선택합니다.
5. Action Alert: Media Intervention(작업 알림: 미디어 개입) 창에서 Respond OK(확인 응답)를 선택하여 미디어를 슬롯에 삽입합니다.

선택한 슬롯에 해당 테이프가 표시됩니다.

ℹ Note

가져온 테이프는 빈 테이프와 아카이브에서 게이트웨이로 가져온 테이프를 포함합니다.

Backup Exec에 있는 테이프에 데이터 쓰기

물리적 테이프에 대해 수행하는 것과 동일한 절차 및 백업 정책을 사용하여 Tape Gateway 가상 테이프에 데이터를 작성합니다. 자세한 내용은 Backup Exec 소프트웨어의 설명서 섹션에 있는 Backup Exec 관리 안내서를 참조하십시오.

Note

백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패할 수 있습니다. 백업 작업이 실패할 경우 Veritas Backup Exec의 테이프 상태가 추가 불가능으로 변경됩니다. 테이프를 아카이브하거나 테이프에서 데이터를 계속 읽을 수 있습니다. 실패한 백업 작업을 완료하려면 해당 작업을 새 테이프에 다시 제출해야 합니다.

Backup Exec을 사용한 테이프 보관

테이프를 아카이브하면 Tape Gateway가 게이트웨이의 가상 테이프 라이브러리(VTL)에서 오프라인 스토리지로 테이프를 이동합니다. Backup Exec 소프트웨어를 사용하여 테이프를 내보냄으로써 테이프 보관을 시작합니다.

테이프를 아카이브하려면

1. Storage(스토리지) 메뉴를 선택하고 Slots(슬롯)를 선택하고 테이프를 내보내려는 슬롯을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Export media(미디어 내보내기)를 선택한 후 Export media now(지금 미디어 내보내기)를 선택합니다. 슬롯을 하나 이상 선택하고 내보내기 작업 하나로 테이프를 여러 개 내보낼 수 있습니다.
2. 미디어 요청 팝업 창에서 세부 정보 보기를 선택한 다음 알림: 미디어 개입 창에서 확인 응답을 선택합니다.

보관 중인 테이프의 상태를 Storage Gateway 콘솔에서 확인할 수 있습니다. 데이터를 AWS에 업로드하는 데 다소 시간이 걸릴 수 있습니다. 이 시간 동안 내보낸 테이프는 Tape Gateway에 상태가 IN TRANSIT TO VTSVTL인 상태로 나열됩니다. 업로드가 완료되고 아카이브 프로세스가 시작되면 상태가 ARCHIVING으로 변경됩니다. 데이터 아카이빙이 완료되면 내보낸 테이프는 더 이상에 나열되지 않지만 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 보관됩니다.

3. 게이트웨이를 선택한 다음 VTL 테이프 카트리지를 선택하고 가상 테이프가 게이트웨이에 더 이상 나열되지 않는지 확인합니다.
4. Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 테이프의 상태가 IN ARCHIVED로 변경됩니다.

Backup Exec에 보관한 테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. Backup Exec을 사용하여 해당 데이터를 복원합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다. 관련 지침은 Backup Exec 소프트웨어의 설명서 섹션에 있는 Backup Exec 관리 안내서를 참조하십시오.

Backup Exec에서 테이프 드라이브 비활성화

Tape Gateway에서는 테이프 드라이브 10개를 제공하지만, 더 적은 수의 테이프 드라이브를 사용할 수 있습니다. 그러한 경우에는 사용하지 않는 테이프 드라이브를 비활성화합니다.

1. Backup Exec을 열고 Storage(스토리지) 탭을 선택합니다.
2. 로봇 공학 라이브러리 트리에서 비활성화할 테이프 드라이브를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 비활성화를 선택합니다.

다음 단계

[불필요한 리소스 정리](#)

Veritas를 사용하여 설정 테스트 NetBackup

Veritas 를 사용하여 가상 테이프에 데이터를 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다 NetBackup. 이 주제에서는 Tape Gateway용 NetBackup 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다. 이렇게 하려면 다음 버전의 를 사용할 수 있습니다 NetBackup.

- Veritas NetBackup 7.x
- Veritas NetBackup 8.x

Tape Gateway에서 이 버전의 Backup Exec을 사용하는 절차는 동일합니다. 사용 방법에 대한 자세한 내용은 [Veritas 웹 사이트의 Veritas 서비스 및 운영 준비 도구\(SORT\)](#)를 NetBackup참조하세요. 하드웨어 호환성에 대한 Veritas 지원 정보는 Veritas 웹 사이트의 [NetBackup 7.0 - 7.6.x 하드웨어 호환성 목록](#)

[록](#), [NetBackup 8.0 - 8.1.x 하드웨어 호환성 목록](#) 또는 [NetBackup 8.2 - 8.x.x 하드웨어 호환성 목록](#)을 참조하세요.

호환되는 백업 애플리케이션에 대한 자세한 내용은 [Tape Gateway에 지원되는 타사 백업 애플리케이션](#) 단원을 참조하십시오.

주제

- [NetBackup 스토리지 디바이스 구성](#)
- [데이터를 테이프에 백업](#)
- [테이프 보관](#)
- [테이프에서 데이터 복원](#)

NetBackup 스토리지 디바이스 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 디바이스를 인식하도록 Veritas NetBackup 스토리지를 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [VTL 디바이스 연결](#).

Tape Gateway에서 스토리지 디바이스 NetBackup 를 사용하도록 구성하려면

1. 관리자로 NetBackup 관리 콘솔을 엽니다.
2. Configure Storage Devices(스토리지 디바이스 구성)를 선택하여 Device Configuration(디바이스 구성) 마법사를 엽니다.
3. Next(다음)를 선택합니다. NetBackup 애플리케이션이 컴퓨터를 디바이스 호스트로 감지합니다.
4. Device Hosts(디바이스 호스트) 열에서 해당 컴퓨터를 선택한 후 Next(다음)를 선택합니다. NetBackup 애플리케이션은 컴퓨터에 디바이스가 있는지 스캔하고 모든 디바이스를 검색합니다.
5. Scanning Hosts(호스트 스캔 중) 페이지에서 Next(다음)를 선택한 후 다시 Next(다음)를 선택합니다. NetBackup 애플리케이션은 컴퓨터에서 10개의 테이프 드라이브와 미디어 체인저를 모두 찾습니다.
6. Backup Devices(백업 디바이스) 창에서 Next(다음)를 선택합니다.
7. Drag and Drop Configuration(구성 끌어서 놓기) 창에서 미디어 체인저가 선택되었는지 확인한 후 Next(다음)를 선택합니다.
8. 표시된 대화 상자에서 Yes(예)를 선택하여 구성을 컴퓨터에 저장합니다. NetBackup 애플리케이션은 디바이스 구성을 업데이트합니다.
9. 업데이트가 완료되면 다음을 선택하여 디바이스를 NetBackup 애플리케이션에 사용할 수 있도록 합니다.

10. Finished!(완료됨!) 창에서 Finish(마침)를 선택합니다.

NetBackup 애플리케이션에서 디바이스를 확인하려면

1. NetBackup 관리 콘솔에서 미디어 및 디바이스 관리 노드를 확장한 다음 디바이스 노드를 확장합니다. Drives(드라이브)를 선택하여 모든 테이프 드라이브를 표시합니다.
2. Devices(디바이스) 노드에서 Robots(로봇)를 선택하여 모든 미디어 체인저를 표시합니다. NetBackup 애플리케이션에서 미디어 체인저를 로봇 이라고 합니다.
3. 모든 로봇 창에서 TLD(0)(즉, 로봇)의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 인벤토리 로봇을 선택합니다.
4. 로봇 인벤토리 창의 로봇 선택 범주에 있는 디바이스-호스트 목록에서 호스트가 선택되었는지 확인합니다.
5. 로봇을 Robot(로봇) 목록에서 선택하였는지 확인합니다.
6. Robot Inventory(로봇 인벤토리) 창에서 Update volume configuration(볼륨 구성 업데이트)을 선택하고, Preview changes(변경 미리 보기)를 선택하고, Empty media access port prior to update(업데이트 전에 미디어 액세스 포트 비우기)를 선택한 후 Start(시작)를 선택합니다.

그런 다음 프로세스는 NetBackup Enterprise Media Management(EMM) 데이터베이스에서 미디어 체인저 및 가상 테이프의 인벤토리를 생성합니다. 는 미디어 정보, 디바이스 구성 및 테이프 상태를 에 NetBackup 저장합니다EMM.

7. 목록 만들기가 완료되면 Robot Inventory(로봇 인벤토리) 창에서 Yes(예)를 선택합니다. Yes(예)를 선택하면 구성을 업데이트하고 가져오기/내보내기 슬롯에서 찾은 가상 테이프를 가상 테이프 라이브러리로 이동합니다.
8. Robot Inventory(로봇 인벤토리) 창을 닫습니다.
9. 미디어 노드에서 로봇 노드를 확장하고 TLD(0)을 선택하여 로봇(중간 체인저)에 사용할 수 있는 모든 가상 테이프를 표시합니다.

Note

이전에 다른 디바이스를 NetBackup 애플리케이션에 연결한 경우 로봇이 여러 개 있을 수 있습니다. 올바른 로봇을 잘 선택해야 합니다.

디바이스를 연결하여 백업 애플리케이션에서 사용할 수 있게 했으므로 이제 게이트웨이를 테스트할 준비가 되었습니다. 게이트웨이를 테스트하려면 생성한 가상 테이프에 데이터를 백업하고 그 테이프를 보관해야 합니다.

데이터를 테이프에 백업

데이터를 가상 테이프에 백업하여 Tape Gateway 설정을 테스트합니다.

Note

- 데이터 저장, 보관 및 가져오기와 관련해 비용이 발생하기 때문에 이 '시작하기' 연습에서는 소량의 데이터만 백업해야 합니다. 요금 정보는 Storage Gateway 세부 정보 페이지에서 [요금](#)을 참조하십시오.
- 백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 일시 중단됩니다. 일시 중단된 백업 작업은 게이트웨이 재시작이 완료되면 자동으로 재개됩니다.

볼륨 풀을 생성하려면

볼륨 풀은 백업에 사용할 가상 테이프 모음입니다.

1. NetBackup 관리 콘솔을 시작합니다.
2. Media(미디어) 노드를 펼치고 Volume Pool(볼륨 풀)을 오른쪽 클릭하여 컨텍스트 메뉴를 연 후 New(새로 만들기)를 선택합니다. 그러면 New Volume Pool(새 볼륨 풀) 대화 상자가 나타납니다.
3. Name(이름)에 볼륨 풀 이름을 입력합니다.
4. Description(설명)에 볼륨 풀에 대한 설명을 입력한 후 OK(확인)를 선택합니다. 방금 생성한 볼륨 풀이 볼륨 풀 목록에 추가됩니다.

다음 스크린샷은 볼륨 풀 목록입니다.

가상 테이프를 볼륨 풀에 추가하려면

1. 로봇 노드를 확장하고 TLD(0)개의 로봇을 선택하여 이 로봇이 알고 있는 가상 테이프를 표시합니다.

이전에 로봇에 연결한 적이 있는 경우, Tape Gateway 로봇의 이름이 다를 수 있습니다.

2. 가상 테이프 목록에서 볼륨 풀에 추가할 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Change(변경)를 선택하여 Change Volumes(볼륨 변경) 대화 상자를 엽니다.
3. Volume Pool(볼륨 풀)에서 New pool(새 풀)을 선택합니다.


4. New pool(새 풀)에서 방금 생성한 풀을 선택한 후 OK(확인)를 선택합니다.

Media(미디어) 노드를 펼쳐 해당 볼륨 풀을 선택하면 방금 추가한 가상 테이프가 볼륨 풀에 포함되어 있는지 확인할 수 있습니다.

백업 정책을 생성하려면

백업 정책은 백업할 데이터, 백업 시점, 사용할 볼륨 풀을 지정합니다.

1. 마스터 서버를 선택하여 Veritas NetBackup 콘솔로 돌아갑니다.
2. Create a Policy(정책 생성)를 선택하여 Policy Configuration Wizard(정책 구성 마법사) 창을 엽니다.
3. File systems, databases, applications(파일 시스템, 데이터베이스, 애플리케이션)를 선택한 후 Next(다음)를 선택합니다.
4. Policy Name(정책 이름)에 정책 이름을 입력하고 MS-Windows를 Select the policy type(정책 유형 선택) 목록에서 선택했는지 확인한 후 Next(다음)를 선택합니다.
5. Client List(클라이언트 목록) 창에서 Add(추가)를 선택하고 Name(이름) 옆에 컴퓨터의 호스트 이름을 입력한 후 Next(다음)를 선택합니다. 이 단계는 정의하는 정책을 localhost(클라이언트 컴퓨터)에 적용합니다.
6. Files(파일) 창에서 Add(추가)를 선택한 후 해당 폴더 아이콘을 선택합니다.
7. Browse(찾아보기) 창에서 백업할 폴더 또는 파일을 검색하여 OK(확인)를 선택한 후 Next(다음)를 선택합니다.
8. Backup Types(백업 유형) 창에서 기본값을 수락한 후 Next(다음)를 선택합니다.

 Note

백업을 직접 시작하려면 User Backup(사용자 백업)을 선택합니다.

9. Frequency and Retention(빈도 및 보존) 창에서 백업에 적용할 빈도와 보존 정책을 선택합니다. 이 연습에서는 모든 기본값을 수락하고 다음을 선택할 수 있습니다.
10. Start(시작) 창에서 Off hours(휴식 시간)를 선택한 후 Next(다음)를 선택합니다. 이렇게 선택하면 폴더가 휴식 시간에만 백업됩니다.
11. Policy Configuration(정책 구성) 마법사에서 Finish(마침)를 선택합니다.

정책은 일정에 따라 백업을 실행합니다. 수동 백업도 언제든지 가능한데, 이 작업은 다음 단계에서 해 보겠습니다.

수동으로 백업하려면

1. NetBackup 콘솔의 탐색 창에서 NetBackup 관리 노드를 확장합니다.
2. Policies(정책) 노드를 펼칩니다.
3. 해당 정책을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Manual Backup(수동 백업)을 선택합니다.
4. Manual Backup(수동 백업) 창에서 일정을 선택하고 클라이언트를 선택한 후 OK(확인)를 선택합니다.
5. Manual Backup Started(수동 백업 시작됨) 대화 상자가 표시되면 OK(확인)를 선택합니다.
6. 탐색 창에서 Activity Monitor(활동 모니터)를 선택하여 Job ID(작업 ID) 열에서 백업 상태를 확인합니다.

백업 중에 파일 데이터를 NetBackup 기록한 가상 테이프의 바코드를 찾으려면 다음 절차에 설명된 대로 작업 세부 정보 창을 참조하세요. 다음 섹션의 테이프 보관 절차에서 이 바코드가 필요합니다.

테이프의 바코드를 찾으려면

1. Activity Monitor(활동 모니터)에서 Job ID(작업 ID) 열에 있는 백업 작업의 식별자를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Details(세부 정보)를 선택합니다.
2. Job Details(작업 세부 정보) 창에서 Detailed Status(세부 상태) 탭을 선택합니다.
3. Status(상태) 상자에서 미디어 ID를 찾습니다. 예를 들어 상태 보고서의 항목에 가 표시될 수 있습니다 media id 87A222. 이 ID는 데이터를 작성한 테이프가 어떤 것인지 식별하는 데 도움이 됩니다.

이제 Tape Gateway 배포, 가상 테이프 생성, 데이터 백업을 성공적으로 완료했습니다. 그 다음에는 가상 테이프를 아카이브하고 이를 아카이브에서 가져올 수 있습니다.

테이프 보관

테이프를 아카이브하면 Tape Gateway가 게이트웨이의 가상 테이프 라이브러리(VTL)에서 아카이브로 테이프를 이동시켜 오프라인 스토리지를 제공합니다. 백업 애플리케이션으로 테이프를 배출하여 테이프 보관을 시작합니다.

가상 테이프를 아카이브하려면

1. NetBackup 관리 콘솔에서 미디어 및 디바이스 관리 노드를 확장하고 미디어 노드를 확장합니다.

2. 로봇을 확장하고 TLD(0)을 선택합니다.
3. 보관할 가상 테이프를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 Eject Volume From Robot(로봇에서 볼륨 배출)을 선택합니다.
4. Eject Volumes(볼륨 배출) 창에서 Media ID(미디어 ID)가 배출하려는 가상 테이프와 일치하는지 확인한 후 Eject(배출)를 선택합니다.
5. 대화 상자에서 Yes(예)를 선택합니다.

배출 프로세스가 완료되면 Eject Volumes(볼륨 배출) 대화 상자에서 테이프 상태가 배출이 완료되었음을 표시합니다.

6. Close(닫기)를 선택하여 Eject Volumes(볼륨 배출) 창을 닫습니다.
7. Storage Gateway 콘솔에서 게이트웨이의 에 보관 중인 테이프의 상태를 확인합니다 VTL. 데이터를 AWS에 업로드하는 데 다소 시간이 걸릴 수 있습니다. 이 시간 동안 배출된 테이프는 게이트웨이의 에 나열되어 VTL 있으며 상태는 IN TRANSIT TO VTS입니다. 아카이브가 시작되면 상태는 ARCHIVING. 데이터 업로드가 완료되면 배출된 테이프는 더 이상 에 나열되지 VTL 않지만 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 보관됩니다.
8. 가상 테이프가 게이트웨이에 더 이상 나열되지 않는지 확인하려면 게이트웨이를 선택한 다음 VTL 테이프 카트리지를 선택합니다.
9. Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 인지 확인합니다 ARCHIVED.

테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.
2. Veritas NetBackup 애플리케이션과 함께 설치된 백업, 아카이브 및 복원 소프트웨어를 사용합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다. 지침은 [Veritas 웹 사이트의 Veritas 서비스 및 운영 준비 도구\(SORT\)](#)를 참조하세요.

다음 단계

[불필요한 리소스 정리](#)

추가 정보

Tape Gateway가 프로덕션 단계를 마친 후에는 테이프 추가 및 제거, 게이트웨이 작동 상태 모니터링 및 최적화, 문제 해결과 같은 여러 가지 유지 관리 작업을 수행할 수 있습니다. 이러한 관리 작업에 대한 일반적인 정보는 [Tape Gateway 관리](#) 단원을 참조하십시오.

게이트웨이의 대역폭 속도 제한 구성 및 게이트웨이 소프트웨어 업데이트 관리 AWS Management Console와 같은 Tape Gateway 유지 관리 작업 중 일부를 에서 수행할 수 있습니다. Tape Gateway를 온프레미스에 배포한 경우 해당 게이트웨이의 로컬 콘솔을 사용하여 일부 유지 관리 작업을 수행할 수 있습니다. 이러한 작업에는 프록시를 통해 Tape Gateway를 라우팅하고 고정 IP 주소를 사용하도록 게이트웨이를 구성하는 작업이 포함됩니다. 게이트웨이를 Amazon EC2 인스턴스로 실행하는 경우 Amazon EC2 콘솔에서 Amazon EBS 볼륨 추가 및 제거와 같은 특정 유지 관리 작업을 수행할 수 있습니다. Tape Gateway 유지 관리에 대한 자세한 내용은 [Tape Gateway 관리](#) 섹션을 참조하세요.

게이트웨이를 프로덕션에서 배포할 계획인 경우, 디스크 크기를 결정할 때 실제 워크로드를 고려해야 합니다. 실제 디스크 크기를 결정하는 방법에 대한 정보는 [Storage Gateway의 로컬 디스크 관리](#) 단원을 참조하십시오. 또한 Tape Gateway를 계속해서 사용할 계획이 아니라면 정리하는 것을 고려하세요. 정리를 통해 요금 발생을 방지할 수 있습니다. 정리에 대한 정보는 [불필요한 리소스 정리](#) 단원을 참조하십시오.

Virtual Private Cloud(VPC)에서 게이트웨이 활성화

온프레미스 게이트웨이 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 이 연결을 사용하여 게이트웨이를 활성화하고 공용 인터넷을 통해 통신하지 않고도 AWS 스토리지 서비스에 데이터를 전송하도록 허용할 수 있습니다. Amazon VPC 서비스를 사용하면 사용자 지정 가상 사설 클라우드 (VPC) 에서 사설 네트워크 인터페이스 엔드포인트를 비롯한 AWS 리소스를 시작할 수 있습니다. A를 VPC 사용하면 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이와 같은 네트워크 설정을 제어할 수 있습니다. 에 대한 VPCs 자세한 내용은 [Amazon이란 무엇입니까 VPC?](#) 를 참조하십시오. Amazon VPC 사용 설명서에서 확인할 수 있습니다.

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

Note

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

주제

- [Storage Gateway용 VPC 엔드포인트 생성](#)

Storage Gateway용 VPC 엔드포인트 생성

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

Storage Gateway의 VPC 엔드포인트를 생성하려면

1. 에서 Amazon VPC 콘솔에 AWS Management Console 로그인하고 엽니다 <https://console.aws.amazon.com/vpc/>.
2. 탐색 창에서 엔드포인트를 선택하고 엔드포인트 생성을 선택합니다.
3. 엔드포인트 생성 페이지에서 AWS 서비스를 서비스 범주로 선택합니다.
4. 서비스 이름에서 `com.amazonaws.region.storagegateway`를 선택합니다. 예: `com.amazonaws.us-east-2.storagegateway`.
5. 에서 원하는 가용 VPC영역을 선택하고 해당 가용 VPC 영역과 서브넷을 기록해 두십시오.
6. 프라이빗 DNS 네임 활성화가 선택되지 않았는지 확인하십시오.
7. 보안 그룹에서 사용할 보안 그룹을 선택합니다VPC. 기본 보안 그룹을 적용할 수 있습니다. 보안 그룹에 다음 TCP 포트가 모두 허용되는지 확인하십시오.
 - TCP443
 - TCP1026
 - TCP1027
 - TCP1028
 - TCP1031
 - TCP2222
8. Create endpoint(엔드포인트 생성)을 선택합니다. 엔드포인트의 초기 상태는 대기 중입니다. 엔드포인트가 생성되면 방금 생성한 VPC 엔드포인트의 ID를 기록해 둡니다.
9. 엔드포인트가 생성되면 엔드포인트를 선택한 다음 새 VPC 엔드포인트를 선택합니다.
10. 선택한 스토리지 게이트웨이 엔드포인트의 세부 정보 탭의 DNS이름에서 가용 영역을 지정하지 않은 첫 번째 DNS 이름을 사용합니다. DNS이름은 다음과 비슷합니다. `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com`

이제 VPC 엔드포인트가 생겼으니 게이트웨이를 만들 수 있습니다. 자세한 내용은 [게이트웨이 생성을 참조하세요](#).

Tape Gateway 관리

게이트웨이 관리에는 캐시 스토리지 구성 및 버퍼 공간 업로드, 가상 테이프 작업, 일반 유지 관리와 같은 작업이 포함됩니다. 게이트웨이를 생성하지 않았으면 [시작하기 AWS Storage Gateway](#) 단원을 참조하십시오.

다음은 Tape Gateway 리소스를 관리하는 방법에 대한 정보입니다.

주제

- [기본 게이트웨이 정보 편집](#) - Storage Gateway 콘솔을 사용하여 게이트웨이 이름, 시간대 및 CloudWatch 로그 그룹을 포함하여 기존 게이트웨이의 기본 정보를 편집하는 방법을 알아봅니다.
- [자동 테이프 생성 관리](#) - 지정한 최소 가용 테이프 수를 유지하도록 Tape Gateway를 구성하여 새 가상 테이프를 자동으로 생성하는 방법을 알아봅니다.
- [가상 테이프 보관](#) - 새 테이프를 생성할 때 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 테이프 아카이브를 구성하는 방법을 알아봅니다.
- [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동](#) - 장기 데이터 보존 및 디지털 보존을 위해 매우 저렴한 비용으로 테이프를 S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 이동하는 방법을 알아봅니다.
- [보관한 테이프 가져오기](#) - 먼저 테이프를 Tape Gateway로 검색하여 아카이브된 가상 테이프에 저장된 데이터에 액세스하는 방법을 알아봅니다.
- [테이프 사용 통계 보기](#) - Storage Gateway 콘솔을 사용하여 테이프에 저장된 데이터의 양을 보는 방법을 알아봅니다.
- [Tape Gateway에서 가상 테이프 삭제](#) - Storage Gateway 콘솔을 사용하여 Tape Gateway에서 가상 테이프를 삭제하는 방법을 알아봅니다.
- [사용자 지정 테이프 풀 삭제](#) - Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 삭제하는 방법을 알아봅니다.
- [Tape Gateway 비활성화](#) - 게이트웨이가 실패하고 실패한 게이트웨이에서 다른 게이트웨이로 테이프를 복구하려는 경우 Tape Gateway를 비활성화하는 방법을 알아봅니다.
- [테이프 상태 이해](#) - 테이프가 정상적으로 작동하는지 또는 사용자 측에서 조치가 필요할 수 있는 문제가 있는지 확인하는 데 도움이 되도록 Storage Gateway에서 보고하는 다양한 테이프 상태 값에 대해 알아봅니다.
- [데이터를 새 게이트웨이로 이동](#) - 데이터 및 성능 요구 사항이 증가함에 따라 또는 게이트웨이 마이그레이션 AWS 알림을 받는 경우 게이트웨이 간에 데이터를 이동하는 방법을 알아봅니다.

기본 게이트웨이 정보 편집

Storage Gateway 콘솔을 사용하여 게이트웨이 이름, 시간대 및 CloudWatch 로그 그룹을 포함하여 기존 게이트웨이의 기본 정보를 편집할 수 있습니다.

기존 게이트웨이의 기본 정보를 편집하려면

1. <https://console.aws.amazon.com/storagegateway/>에서 Storage Gateway 콘솔을 엽니다.
2. 게이트웨이를 선택한 다음 기본 정보를 편집할 게이트웨이를 선택합니다.
3. 작업 드롭다운 메뉴에서 게이트웨이 정보 편집을 선택합니다.
4. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 이 이름을 검색하여 Storage Gateway 콘솔의 목록 페이지에서 게이트웨이를 찾을 수 있습니다.

Note

게이트웨이 이름은 2~255자여야 하며 슬래시(\ 또는)를 포함할 수 없습니다/. 게이트웨이의 이름을 변경하면 게이트웨이를 모니터링하도록 설정된 모든 CloudWatch 경보의 연결이 해제됩니다. 경보를 다시 연결하려면 CloudWatch 콘솔의 각 경보에 GatewayName 대해 를 업데이트합니다.

5. 게이트웨이 표준 시간대에서 게이트웨이를 배포하려는 전 세계 지역의 현지 시간대를 선택합니다.
6. 로그 그룹 설정 방법 선택에서 게이트웨이 상태를 모니터링하도록 Amazon CloudWatch Logs를 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 - Amazon CloudWatch Logs를 사용하여 게이트웨이를 모니터링하지 마세요.
7. 변경하려는 설정 수정을 마치면 변경 사항 저장을 선택합니다.

자동 테이프 생성 관리

Tape Gateway는 사용자가 구성한 최소 사용 가능 테이프 수를 유지하기 위해 새 가상 테이프를 자동으로 생성합니다. 그런 다음 새 테이프를 백업 애플리케이션의 가져오기에 제공함으로써 백업 작업을 중단 없이 실행할 수 있습니다. 자동 테이프 생성은 새로운 가상 테이프를 생성하기 위한 수동 프로세스 외에 사용자 지정 스크립팅도 필요하지 않습니다.

자동 테이프 생성 정책을 삭제하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 탭을 선택합니다.
3. 자동 테이프 생성을 관리해야 하는 게이트웨이를 선택합니다.
4. 작업 메뉴에서 Configure tape auto-create(테이프 자동 생성 구성)를 선택합니다.
5. 게이트웨이에 대한 자동 테이프 생성 정책을 삭제하려면 삭제할 정책의 오른쪽에 있는 제거를 선택합니다.

게이트웨이에 대한 자동 테이프 생성을 중지하려면 해당 게이트웨이에 대한 자동 테이프 작성 정책을 모두 삭제합니다.

변경 사항 저장을 선택하여 선택한 Tape Gateway에 대한 테이프 자동 생성 정책의 삭제를 확인합니다.

Note

게이트웨이에서 테이프 자동 생성 정책 삭제는 실행 취소할 수 없습니다.

Tape Gateway의 자동 테이프 생성 정책을 변경하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 탭을 선택합니다.
3. 자동 테이프 생성을 관리해야 하는 게이트웨이를 선택합니다.
4. 작업 메뉴에서 테이프 자동 생성 구성을 선택하고 나타나는 페이지에서 설정을 변경합니다.
5. 최소 테이프 수에 Tape Gateway에서 항상 사용할 수 있어야 하는 최소 가상 테이프 수를 입력합니다. 이 값의 유효한 범위는 최소 1, 최대 10입니다.
6. 용량에 가상 테이프 용량의 크기(바이트)를 입력합니다. 이 값의 유효한 범위는 최소 100GiB, 최대 15TiB입니다.
7. 바코드 접두사에 가상 테이프의 바코드 앞에 붙일 접두사를 입력합니다.

Note

가상 테이프는 바코드로 고유하게 식별되며 바코드에 접두사를 추가할 수 있습니다. 접두사는 선택 사항이긴 하지만 가상 테이프를 식별하는 데 사용할 수 있습니다. 접두사는 대문자(A-Z)이어야 하고 문자는 1~4개까지 사용할 수 있습니다.

8. 풀에서 Glacier 풀 또는 Deep Archive 풀을 선택합니다. 이 풀은 백업 소프트웨어가 꺼내는 테이프가 저장되는 스토리지 클래스를 나타냅니다.

- S3 Glacier Flexible Retrieval 스토리지 클래스에 테이프를 아카이브하려면 Glacier 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 아카이브됩니다. 일반적으로 3-5시간 이내에 테이프를 검색할 수 있는 보다 활동적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.
- S3 Glacier Deep Archive에 테이프를 아카이브하려면 Deep Archive 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive에 아카이브된 테이프는 일반적으로 12시간 이내에 검색할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.

테이프를 S3 Glacier Flexible Retrieval에 아카이브한 경우 나중에 S3 Glacier Deep Archive로 이동할 수 있습니다. 자세한 내용은 [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동](#) 단원을 참조하십시오.

9. 테이프에 대한 정보는 테이프 개요 페이지에서 찾을 수 있습니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

사용 가능한 가상 테이프의 상태는 테이프가 생성될 CREATING 때 처음으로 설정됩니다. 테이프가 생성되면 상태가 로 변경됩니다AVAILABLE. 자세한 내용은 [테이프 상태 이해](#) 단원을 참조하십시오.

자동 테이프 생성 활성화에 대한 자세한 내용은 [자동으로 테이프 생성](#)을 참조하세요.

가상 테이프 보관

테이프를 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브할 수 있습니다. 테이프를 생성할 경우 테이프를 아카이브하는 데 사용하려는 아카이브 풀을 선택하십시오.

테이프를 S3 Glacier Flexible Retrieval에 아카이브하려면 Glacier 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 자동으로 아카이브됩니다. 정기적으로 데이터를 검색하고 데이터가 몇 분 내에 필요한 보다 활동적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하십시오.

S3 Glacier Deep Archive에 테이프를 아카이브하려면 Deep Archive 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 매우 저렴한 비용으로 장기적인 데이터 보존 및 디지털 보존이 필요한 경우 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive의 데이터는 자주 검색되지 않거나 거의 검색되지 않습니다. 자세한 내용은 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하십시오.

Note

2019년 3월 27일 이전에 생성된 테이프는 백업 소프트웨어로 테이프를 꺼내면 S3 Glacier Flexible Retrieval에 바로 아카이브됩니다.

백업 소프트웨어가 테이프를 꺼내면 해당 테이프를 생성할 때 선택한 풀에 자동으로 아카이브됩니다. 테이프 꺼내기 프로세스는 백업 소프트웨어에 따라 다릅니다. 일부 백업 소프트웨어에서는 테이프를 배출한 후 내보내야 아카이빙을 시작할 수 있습니다. 지원되는 백업 소프트웨어에 대한 자세한 내용은 [백업 소프트웨어를 사용하여 게이트웨이 설정 테스트](#)를 참조하세요.

S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동

S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프를 이동하면 데이터의 장기적인 보존과 매우 경제적인 디지털 보존이 가능합니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. 자세한 내용은 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하십시오.

S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프를 이동하려면

1. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용

됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.

2. S3 Glacier Deep Archive로 이동할 테이프의 확인란을 선택합니다. 풀 열에서 각 테이프와 연결된 풀을 확인할 수 있습니다.
3. 풀에 할당을 선택합니다.
4. 풀에 테이프 할당 대화 상자에서 이동하려는 테이프의 바코드를 확인하고 할당을 선택합니다.

Note

테이프가 백업 애플리케이션에 의해 배출되어 S3 Glacier Deep Archive에 아카이브된 경우에는 S3 Glacier Flexible Retrieval로 다시 이동할 수 없습니다. S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프를 이동할 경우 요금이 부과됩니다. 그리고 90일 전에 S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프를 이동하면 S3 Glacier Flexible Retrieval 조기 삭제 요금이 부과됩니다.

5. 테이프를 이동한 후에는 테이프 개요 페이지의 풀 열에서 업데이트된 상태를 확인할 수 있습니다.

보관한 테이프 가져오기

아카이브된 가상 테이프에 저장된 데이터에 액세스하려면 먼저 Tape Gateway로 필요한 테이프를 가져와야 합니다. Tape Gateway는 각 게이트웨이에 대해 하나의 가상 테이프 라이브러리(VTL)를 제공합니다.

에 Tape Gateway가 두 개 이상 있는 AWS 리전 경우 하나의 게이트웨이로만 테이프를 검색할 수 있습니다.

가져온 테이프는 쓰기 금지되어 있으므로 테이프에 있는 데이터를 읽을 수만 있습니다.

Important

S3 Glacier Flexible Retrieval에 테이프를 아카이브하면 일반적으로 3-5시간 내에 테이프를 가져올 수 있습니다. S3 Glacier Deep Archive에 테이프를 아카이브하면 일반적으로 12시간 내에 테이프를 가져올 수 있습니다.

Note

아카이브에서 테이프를 가져오는 데 요금이 부과됩니다. 자세한 요금 정보는 [Storage Gateway 요금](#) 섹션을 참조하세요.

아카이브된 테이프를 게이트웨이로 가져오려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.
3. 가상 테이프 셸프 탭에서 검색할 가상 테이프를 선택하고 테이프 검색을 선택합니다.

Note

검색하려는 가상 테이프의 상태는 여야 합니다ARCHIVED.

4. 테이프 가져오기 대화 상자의 바코드에서 해당 바코드가 가져올 가상 테이프와 일치하는지 확인하십시오
5. 게이트웨이에서 보관된 테이프를 가져오려는 게이트웨이를 선택하고 테이프 가져오기를 선택하십시오

테이프 상태가 에서 ARCHIVED로 변경됩니다RETRIEVING. 이때 데이터는 가상 테이프 셸프(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 지원)에서 가상 테이프 라이브러리(Amazon S3에서 지원)로 이동되고 있습니다. 모든 데이터가 이동되면 아카이브의 가상 테이프 상태로 변경됩니다RETRIEVED.

Note

가져온 가상 테이프는 읽기 전용입니다.

테이프 사용 통계 보기

테이프에 데이터를 쓸 때 Storage Gateway 콘솔에서 테이프에 저장된 데이터의 양을 확인할 수 있습니다. 각 테이프의 세부 정보 탭에 테이프 사용량 정보가 표시됩니다.

테이프에 저장된 데이터 양을 보려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.
3. 원하는 테이프를 선택합니다.
4. 표시되는 페이지에는 다음을 포함하여 테이프에 대한 다양한 세부 사항과 정보가 제공됩니다.
 - 크기: 선택한 테이프의 전체 용량.
 - 사용됨: 백업 애플리케이션이 테이프에 기록한 데이터의 크기.

Note

이 값은 2015년 5월 13일 이전에 생성된 테이프에는 사용할 수 없습니다.

Tape Gateway에서 가상 테이프 삭제

Storage Gateway 콘솔을 사용하여 Tape Gateway에서 가상 테이프를 삭제할 수 있습니다.

Note

Tape Gateway에서 삭제하려는 테이프의 상태가 인 경우 RETRIEVED 먼저 백업 애플리케이션을 사용하여 테이프를 꺼낸 다음 테이프를 삭제해야 합니다. Symantec NetBackup 소프트웨어를 사용하여 테이프를 꺼내는 방법에 대한 지침은 [테이프 보관을 참조하세요](#). 테이프가 제거되면 테이프 상태가 다시 로 변경됩니다 ARCHIVED. 그 다음에 테이프를 삭제할 수 있습니다.

테이프를 삭제하기 전에 데이터 사본을 생성합니다. 테이프를 삭제한 후에는 다시 되돌릴 수 없습니다.

가상 테이프를 삭제하려면

Warning

이 절차는 선택한 가상 테이프를 영구적으로 삭제합니다.

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.
3. 삭제할 테이프를 하나 이상 선택합니다.
4. 작업에서 테이프 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.
5. 지정된 테이프를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

테이프가 삭제되면 Tape Gateway에서 사라집니다.

사용자 지정 테이프 풀 삭제

다음 절차에서는 Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 삭제하는 방법을 설명합니다. 를 사용하여 프로그래밍 방식으로 이 작업을 수행하려면 Storage Gateway 참조 [DeleteTapePool](#)의 섹션을 API참조하세요. Storage Gateway API

사용자 지정 테이프 풀은 풀에 아카이브된 테이프가 없고 풀에 연결된 자동 테이프 생성 정책이 없는 경우에만 삭제할 수 있습니다. 테이프 풀에서 자동 테이프 생성 정책을 삭제해야 하는 경우 [자동 테이프 풀 생성 관리](#)를 참조하세요.

Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 삭제하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 풀을 선택하여 사용 가능한 풀을 확인합니다.
3. 삭제할 테이프 풀을 하나 이상 선택합니다.

삭제하려는 테이프 풀의 테이프 개수가 0이고 사용자 지정 테이프 풀을 참조하는 자동 테이프 생성 정책이 없는 경우 풀을 삭제할 수 있습니다.

4. Delete(삭제)를 선택합니다. 확인 대화 상자가 표시됩니다.
5. 지정된 테이프 풀을 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

Warning

이 절차는 선택한 테이프 풀을 영구적으로 삭제하며 취소할 수 없습니다.

테이프 풀을 삭제하면 테이프 라이브러리에서 사라집니다.

Tape Gateway 비활성화

Tape Gateway에 장애가 발생하여 장애가 발생한 게이트웨이에서 다른 게이트웨이로 테이프를 복구하려는 경우 Tape Gateway를 비활성화합니다.

테이프를 복구하려면 먼저 장애가 발생한 게이트웨이를 비활성화해야 합니다. Tape Gateway를 비활성화하면 해당 게이트웨이의 가상 테이프가 잠깁니다. 즉, 게이트웨이를 비활성화하면 이러한 테이프에 기록할 수 있는 데이터가 AWS로 전송되지 않습니다. 게이트웨이가 더 이상 AWS에 연결되어 있지 않은 경우에만 Storage Gateway 콘솔에서 게이트웨이를 비활성화할 수 있습니다. 게이트웨이가 연결된 경우 Tape Gateway를 비활성화 AWS할 수 없습니다.

데이터 복구의 일부로 Tape Gateway를 비활성화합니다. 테이프 복구에 관한 자세한 내용은 [장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우](#) 단원을 참조하십시오.

게이트웨이를 비활성화하려면

1. <https://console.aws.amazon.com/storagegateway/>집에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 실패한 게이트웨이를 선택하십시오.
3. 해당 게이트웨이의 세부 정보 탭을 선택하여 게이트웨이 비활성화 메시지를 표시합니다.
4. 복구 테이프 생성을 선택하십시오.
5. 게이트웨이 비활성화를 선택하십시오.

테이프 상태 이해

각 테이프에는 테이프의 상태를 한 눈에 알 수 있는 상태가 연결되어 있습니다. 대부분의 경우 그 상태는 테이프가 정상적으로 작동하고 있으므로 아무 조치도 취할 필요가 없음을 알려줍니다. 경우에 따라 이러한 상태는 사용자의 조치가 필요할 수 있는 테이프 관련 문제를 나타냅니다. 다음 정보를 찾아 조치를 취해야 하는 시점을 결정하는데 도움을 받을 수 있습니다.

주제

- [의 테이프 상태 정보 이해 VTL](#)
- [아카이브의 테이프 상태 확인](#)

의 테이프 상태 정보 이해 VTL

테이프를 읽거나 쓰AVAILABLE려면 테이프의 상태가 여야 합니다. 다음 표에는 가능한 상태 값과 그에 대한 설명이 나와 있습니다.

상태 표시기	설명	테이프 데이터 저장 위치
CREATING	가상 테이프를 생성 중입니다. 테이프가 생성 중이기 때문에 테이프 드라이브로 테이프를 로드할 수 없습니다.	—
AVAILABLE	가상 테이프가 생성되어 테이프 드라이브에 로드할 준비가 되었습니다.	Amazon S3
에서 TRANSIT 로 VTS	가상 테이프를 배출하여 아카이브에 업로드하고 있습니다. 이때 Tape Gateway는 데이터를 에 업로드합니다 AWS. 업로드 중인 데이터의 양이 작은 경우 이 상태가 나타나지 않을 수 있습니다. 업로드가 완료되면 상태로 변경됩니다ARCHIVING.	Amazon S3
ARCHIVING	Tape Gateway를 통해 가상 테이프를 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 지원하는 아카이브로 이동하는 중입니다. 이 프로세스는 에 대한 데이터 업로드 AWS 가 완료된 후 발생합니다.	Amazon S3에서 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive로 데이터를 이동하는 중입니다.

상태 표시기	설명	테이프 데이터 저장 위치
DELETING	가상 테이프를 삭제하고 있습니다.	Amazon S3에서 데이터를 삭제하는 중입니다.
DELETED	가상 테이프를 성공적으로 삭제했습니다.	—
RETRIEVING	아카이브에서 가상 테이프를 가져와 Tape Gateway로 옮기는 중입니다.	S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 Amazon S3로 데이터를 이동하는 중입니다.
	<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note 가상 테이프는 Tape Gateway로만 가져올 수 있습니다.</p> </div>	
RETRIEVED	아카이브에서 가상 테이프를 가져왔습니다. 가져온 테이프는 쓰기 금지되어 있습니다.	Amazon S3
RECOVERED	가상 테이프를 복구했고 현재 읽기 전용 상태입니다. 어떤 이유로든 Tape Gateway에 액세스할 수 없는 경우, Tape Gateway에 연결된 가상 테이프를 다른 Tape Gateway로 복구할 수 있습니다. 가상 테이프를 복구하려면 먼저 액세스할 수 없는 Tape Gateway를 비활성화합니다.	Amazon S3
IRRECOVERABLE	이 가상 테이프에서 읽을 수 없고 이 가상 테이프에 쓸 수도 없습니다. 이 상태는 Tape Gateway에 오류가 발생했음을 나타냅니다.	Amazon S3

아카이브의 테이프 상태 확인

다음 절차에 따라 아카이브의 가상 테이프 상태를 확인할 수 있습니다.

가상 테이프의 상태를 확인하려면

1. <https://console.aws.amazon.com/storagegateway/> **집에서** Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 테이프를 선택하십시오.

3. 테이프 라이브러리 그리드의 상태 열에서 테이프의 상태를 확인합니다.

테이프 상태는 각 가상 테이프의 세부 정보 탭에도 표시됩니다.

그 다음에 가능한 상태 값의 설명을 찾을 수 있습니다.

상태 표시기	설명
ARCHIVED	가상 테이프를 배출하여 아카이브에 업로드하였습니다.
RETRIEVING	아카이브에서 가상 테이프를 가져오고 있습니다.
	<div style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; background-color: #e6f2ff;"> <p> Note 가상 테이프는 Tape Gateway로만 가져올 수 있습니다.</p> </div>
RETRIEVED	아카이브에서 가상 테이프를 가져왔습니다. 가져온 테이프는 읽기 전용입니다.

테이프 및 VTL 디바이스 작업 방법에 대한 자세한 내용은 섹션을 참조하세요 [가상 테이프 라이브러리에서 테이프 관리](#).

데이터를 새 게이트웨이로 이동

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

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

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

Note

데이터는 동일한 게이트웨이 유형 간에만 이동할 수 있습니다.

가상 테이프를 새 Tape Gateway로 이동

가상 테이프를 새 Tape Gateway로 이동하려면

1. 백업 애플리케이션을 사용하여 모든 데이터를 가상 테이프에 백업할 수 있습니다. 백업이 성공적으로 완료될 때까지 기다리세요.
2. 백업 애플리케이션을 사용하여 테이프를 꺼냅니다. 테이프는 Amazon S3 스토리지 클래스 중 하나에 저장됩니다. 꺼낸 테이프는 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브되며 읽기 전용입니다.

계속하기 전에 꺼낸 테이프가 아카이브되었는지 확인합니다.

- a. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
- b. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.
- c. 목록의 상태 열에서 테이프의 상태를 확인합니다.

테이프 상태는 각 가상 테이프의 세부 정보 탭에도 표시됩니다.

아카이브에서 테이프 상태를 확인하는 방법에 대한 자세한 내용은 [아카이브의 테이프 상태 확인](#) 섹션을 참조하세요.

3. 백업 애플리케이션을 사용하여 중지하기 전에 기존 Tape Gateway로 이동하는 활성 백업 작업이 없는지 확인합니다. 활성 백업 작업이 있는 경우 게이트웨이를 중지하기 전에 해당 작업이 완료될 때까지 기다린 다음 테이프를 꺼냅니다(이전 단계 참조).
4. 다음 단계를 수행하여 기존 Tape Gateway를 중지합니다.
 - a. 탐색 창에서 게이트웨이를 선택한 다음 중지하려는 이전 Tape Gateway를 선택합니다. 게이트웨이 상태는 실행 중입니다.
 - b. 작업에서 게이트웨이 중지를 선택합니다. 대화 상자에서 게이트웨이 ID를 확인한 다음 게이트웨이 중지를 선택합니다.

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

게이트웨이 중지지에 대한 자세한 내용은 [Tape Gateway 시작 및 중지](#) 섹션을 참조하세요.

5. 새 Tape Gateway를 생성합니다. 자세한 지침은 [게이트웨이 생성](#)을 참조하세요.
6. 다음 단계를 수행하여 새 테이프를 생성합니다.
 - a. 탐색 창에서 게이트웨이 탭을 선택합니다.
 - b. 테이프 생성을 선택하여 테이프 생성 대화 상자를 엽니다.
 - c. 게이트웨이에서 게이트웨이를 선택합니다. 테이프는 이 게이트웨이용으로 생성됩니다.
 - d. 테이프 개수에서 생성할 테이프의 개수를 선택합니다. 테이프 한도에 대한 자세한 내용은 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.

이때 자동 테이프 생성을 설정할 수도 있습니다. 자세한 내용은 [자동으로 테이프 생성](#)을 참조하세요.

- e. 용량에 생성할 가상 테이프의 크기를 입력합니다. 테이프는 100GiB 이상이어야 합니다. 용량 한도에 대한 정보는 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.
- f. 바코드 접두사에 가상 테이프의 바코드 앞에 붙일 접두사를 입력합니다.

Note

가상 테이프는 바코드를 통해 고유 식별됩니다. 접두사를 바코드에 추가할 수 있습니다. 접두사는 선택 사항이지만 가상 테이프를 식별하는 데 사용할 수 있습니다. 접두사는 대문자(A-Z)이어야 하고 문자는 1~4개까지 사용할 수 있습니다.

- g. 풀에서 Glacier 풀 또는 Deep Archive 풀을 선택합니다. 이 풀은 백업 소프트웨어가 테이블을 꺼낼 때 저장될 스토리지 클래스를 나타냅니다.

테이프를 S3 Glacier Flexible Retrieval에 아카이브하려면 Glacier 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Flexible Retrieval에 자동으로 아카이브됩니다. 일반적으로 3-5시간 이내에 테이프를 검색할 수 있는 보다 활동적인 아카이브에는 S3 Glacier Flexible Retrieval을 사용합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.

테이프를 S3 Glacier Deep Archive에 아카이브하려면 Deep Archive 풀을 선택합니다. 백업 소프트웨어로 테이프를 꺼내면 테이프가 자동으로 S3 Glacier Deep Archive에 자동으로 아카이브됩니다. 1년에 한두 번 데이터에 액세스하는 장기 데이터 보존 및 디지털 보존 용도로는 S3 Glacier Deep Archive를 사용합니다. S3 Glacier Deep Archive에 아카이브된 테이프는 일

반적으로 12시간 이내에 검색할 수 있습니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [객체 아카이빙을 위한 스토리지 클래스](#)를 참조하세요.

테이프를 S3 Glacier Flexible Retrieval에 아카이브한 경우 나중에 S3 Glacier Deep Archive로 이동할 수 있습니다. 자세한 내용은 [S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동 단원](#)을 참조하십시오.

Note

2019년 3월 27일 이전에 생성된 테이프는 백업 소프트웨어로 테이프를 꺼내면 S3 Glacier Flexible Retrieval에 바로 아카이브됩니다.

- h. (선택 사항) 태그에 키와 값을 입력하여 태그를 테이프에 추가합니다. 태그는 테이프를 관리, 필터링 및 검색하는 데 도움이 되는 대소문자 구분 키-값 페어입니다.
 - i. 테이프 생성을 선택합니다.
7. 백업 애플리케이션을 사용하여 백업 작업을 시작하고 데이터를 새 테이프에 백업합니다.
 8. (선택 사항) 테이프가 아카이브되어 있는데 테이프에서 데이터를 복원해야 하는 경우 새 Tape Gateway로 가져옵니다. 테이프는 읽기 전용 모드입니다. 아카이브된 테이프 가져오기에 대한 자세한 내용은 [보관한 테이프 가져오기](#) 섹션을 참조하세요.

Note

아웃바운드 데이터 요금이 적용될 수 있습니다.

- a. 탐색 창에서 테이프 라이브러리 > 테이프를 선택하여 테이프를 확인합니다. 기본적으로 이 목록에는 한 번에 최대 1,000개의 테이프가 표시되지만, 사용자가 수행하는 검색은 모든 테이프에 적용됩니다. 검색 창을 사용하여 특정 기준에 맞는 테이프를 찾거나 테이프 목록을 1,000개 미만으로 줄일 수 있습니다. 목록에 포함된 테이프 수가 1,000개 이하인 경우 다양한 속성을 기준으로 테이프를 오름차순 또는 내림차순으로 정렬할 수 있습니다.
- b. 가져오려는 가상 테이프를 선택합니다. 작업에서 테이프 가져오기를 선택합니다.

Note

가져오려는 가상 테이프의 상태는 ARCHIVED여야 합니다.

- c. 테이프 가져오기 대화 상자의 바코드에서 해당 바코드가 가져올 가상 테이프와 일치하는지 확인하십시오
- d. 게이트웨이에서 아카이브된 테이프를 가져올 새 Tape Gateway를 선택한 다음 테이프 가져오기를 선택합니다.

새 Tape Gateway가 제대로 작동하는 것을 확인했으면 이전 Tape Gateway를 삭제할 수 있습니다.

⚠ Important

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

9. 다음 단계를 수행하여 이전 Tape Gateway를 삭제합니다.

⚠ Warning

게이트웨이를 삭제하면 복구할 수 없습니다.

- a. 탐색 창에서 게이트웨이를 선택한 다음 삭제할 게이트웨이를 선택합니다.
- b. 작업에서 게이트웨이 삭제를 선택합니다.

확인 대화 상자가 나타나면 나열된 게이트웨이 ID에 삭제할 이전 Tape Gateway가 지정되어 있는지 확인하고 확인 필드에 **delete**를 입력한 다음 삭제를 선택합니다.

- c. VM을 삭제합니다. VM 삭제에 대한 자세한 내용은 해당 하이퍼바이저 설명서를 참조하세요.

Storage Gateway 모니터링

이 섹션에서는 Amazon 를 사용하여 게이트웨이와 연결된 리소스 모니터링을 포함하여 Storage Gateway 를 모니터링하는 방법을 설명합니다 CloudWatch. 게이트웨이의 업로드 버퍼 및 캐시 스토리지를 모니터링할 수 있습니다. Storage Gateway 콘솔을 사용하여 게이트웨이에 대한 지표와 경보를 볼 수 있습니다. 예를 들어 읽기 및 쓰기 작업에 사용되는 바이트의 수, 읽기 및 쓰기 작업에 걸리는 시간, Amazon Web Services 클라우드에서 데이터를 가져오는 데 걸리는 시간을 볼 수 있습니다. 지표를 사용하여 게이트웨이의 상태를 추적하고 하나 이상의 지표가 정의한 임계값 범위를 벗어나는 경우 이를 알리도록 경보를 설정할 수 있습니다.

Storage Gateway는 추가 비용 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이 지표를 사용하여 기록 정보에 액세스하고 게이트웨이와 볼륨이 어떻게 실행되고 있는지 더 잘 파악할 수 있습니다. Storage Gateway는 고해상도 CloudWatch 경보를 제외한 경보도 추가 비용 없이 제공합니다. CloudWatch 요금에 대한 자세한 내용은 [Amazon CloudWatch 요금 섹션을](#) 참조하세요. 에 대한 자세한 내용은 [Amazon CloudWatch 사용 설명서 섹션을](#) CloudWatch참조하세요.

Tape Gateway 및 관련 리소스 모니터링에 대한 자세한 내용은 [Tape Gateway 모니터링을 참조하세요](#).


주제

- [게이트웨이 지표 이해](#)
- [업로드 버퍼 모니터링](#)
- [캐시 스토리지 모니터링](#)
- [CloudWatch 경보 이해](#)
- [게이트웨이에 권장되는 CloudWatch 경보 생성](#)
- [게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성](#)
- [Tape Gateway 모니터링](#)

게이트웨이 지표 이해

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

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

 Note

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

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

지표	설명
	단위: 바이트
IoWaitPercent	게이트웨이가 로컬 디스크의 응답을 대기하고 있는 시간의 백분율입니다. 단위: 백분율
MemTotalBytes	게이트웨이 VM에 RAM 프로비저닝된 의 양, 바이트. 단위: 바이트
MemUsedBytes	게이트웨이 VM에서 RAM 현재 사용 중인 의 양은 바이트입니다. 단위: 바이트
QueuedWrites	게이트웨이의 모든 볼륨에 대해 보고 기간 종료 시 AWS 샘플링되고 에 기록되기를 기다리는 바이트 수입니다. 이러한 바이트는 게이트웨이의 작업 스토리지에 유지됩니다. 단위: 바이트
TotalCacheSize	캐시의 총 크기(바이트)입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트

지표	설명
UploadBufferPercentUsed	게이트웨이의 업로드 버퍼 사용 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 백분율
UploadBufferUsed	게이트웨이의 업로드 버퍼에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트
UserCpuPercent	게이트웨이 처리에 소요된 CPU 시간의 백분율로, 모든 코어에서 평균입니다. 단위: 백분율

Storage Gateway 지표의 차원

Storage Gateway 서비스의 CloudWatch 네임스페이스는 `aws/storagegateway`입니다. 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.

측정기준	설명
GatewayId , GatewayName	이러한 차원은 요청하는 데이터를 게이트웨이별 지표로 필터링합니다. 작업할 게이트웨이를 GatewayId 또는 GatewayName 의 값으로 식별할 수 있습니다. 지표를 보는 데 관심이 있는 시간 범위에 대해 게이트웨이의 이름이 다른 경우 GatewayId 를 사용합니다. 게이트웨이의 처리량 및 지연 시간 데이터는 게이트웨이의 모든 볼륨에 기반을 두고 있습니다. 게이트웨이 지표 작업에 대한 자세한 내용은 게이트웨이와 AWS간 성능 측정 을 참조하세요.

업로드 버퍼 모니터링

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

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

Note

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

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

사용되는 업로드 버퍼의 백분율을 측정하려면

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

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

다음 절차를 사용하여 CloudWatch 콘솔을 사용하여 경보를 생성할 수 있습니다. 경보 및 임계값에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [CloudWatch 경보 생성을 참조하세요](#).

게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. 경보에 대한 지표를 지정합니다.
 - a. 경보 생성 마법사의 지표 선택 페이지에서 AWS/StorageGateway:GatewayId,GatewayName 차원을 선택한 다음 작업할 게이트웨이를 찾습니다.
 - b. UploadBufferPercentUsed 지표를 선택합니다. Average 통계와 5분의 시간을 사용합니다.
 - c. 계속을 선택합니다.
4. 경보 이름, 설명 및 임계값을 정의합니다.
 - a. 경보 생성 마법사의 경보 정의 페이지에서 이름 및 설명 상자에 경보의 이름과 설명을 입력하여 경보를 식별합니다.
 - b. 경보 임계값을 정의합니다.
 - c. 계속을 선택합니다.
5. 경보에 대한 이메일 작업을 구성합니다.
 - a. 경보 생성 마법사의 작업 구성 페이지에서 경보 상태에 대해 경보를 선택합니다.
 - b. 주제에 대해 이메일 주제 선택 또는 생성을 선택합니다.

이메일 주제를 생성하려면 Amazon SNS 주제를 설정해야 합니다. Amazon 에 대한 자세한 내용은 Amazon 사용 설명서의 Amazon [설정을 SNS](#) SNS참조하세요. CloudWatch

 - c. 주제에 주제에 대한 설명 이름을 입력합니다.
 - d. 작업 추가를 선택합니다.
 - e. 계속을 선택합니다.
6. 경보 설정을 검토한 후 경보를 생성합니다.
 - a. 경보 생성 마법사의 검토 페이지에서 경보 정의, 지표 및 수행할 관련 작업(예: 이메일 알림 전송)을 검토합니다.

- b. 경보 요약을 검토한 후 Save Alarm(경보 저장)을 선택합니다.
7. 경보 주제에 대한 구독을 확인합니다.
- a. 주제를 생성할 때 지정한 SNS 이메일 주소로 전송된 Amazon 이메일을 엽니다.
 - b. 이메일에 포함된 링크를 클릭하여 구독을 확인합니다.

구독 확인 메시지가 표시됩니다.

캐시 스토리지 모니터링

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

캐싱 볼륨 아키텍처에서는 캐시 스토리지만 모니터링합니다. 자세한 내용은 [Tape Gateway 작동 방식](#) 단원을 참조하십시오.

관심 항목	측정 방법
캐시 총 사용량	CachePercentUsed 통계와 함께 TotalCacheSize 및 Average 지표를 사용합니다. 예를 들어 CachePercentUsed 통계와 함께 Average를 사용하여 일정 기간 동안의 캐시 사용량을 분석합니다. TotalCacheSize 지표는 캐시를 게이트웨이에 추가할 때만 변합니다.
캐시에서 제공되는 읽기 요청의 백분율	CacheHitPercent 통계와 함께 Average 지표를 사용합니다. 대개의 경우 CacheHitPercent 를 높은 수준으로 유지하기를 바랍니다.
더러운 캐시의 비율. 즉, 업로드되지 않은 콘텐츠가 캐시에 포함되어 있습니다. AWS	CachePercentDirty 통계와 함께 Average 지표를 사용합니다. 대개의 경우 CachePercentDirty 를 낮은 수준으로 유지하기를 바랍니다.

게이트웨이 및 해당 모든 볼륨에 대해 더티인 캐시의 백분율을 측정하려면

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.

2. StorageGateway: 게이트웨이 지표 차원을 선택하고 작업할 게이트웨이를 찾습니다.
3. CachePercentDirty 지표를 선택합니다.
4. 시간 범위에서 값을 선택합니다.
5. Average 통계를 선택합니다.
6. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

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

볼륨에 대해 더티인 캐시의 백분율을 측정하려면

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. StorageGateway: 볼륨 지표 차원을 선택하고 작업할 볼륨을 찾습니다.
3. CachePercentDirty 지표를 선택합니다.
4. 시간 범위에서 값을 선택합니다.
5. Average 통계를 선택합니다.
6. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

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

CloudWatch 경보 이해


CloudWatch 경보는 지표 및 표현식을 기반으로 게이트웨이에 대한 정보를 모니터링합니다. 게이트웨이에 대한 CloudWatch 경보를 추가하고 Storage Gateway 콘솔에서 해당 상태를 볼 수 있습니다. Tape Gateway를 모니터링하는 데 사용되는 지표에 대한 자세한 내용은 [게이트웨이 지표 이해](#) 및 [가상 테이프 지표 이해](#)를 참조하세요. 각 경보에 대해 ALARM 상태를 시작할 조건을 지정합니다. Storage Gateway 콘솔의 경보 상태 표시기는 ALARM 상태가 되면 빨간색으로 바뀌므로 상태를 사전에 모니터링할 수 있습니다. 지속적인 상태 변화에 따라 자동으로 작업을 호출하도록 경보를 구성할 수 있습니다. CloudWatch 경보에 대한 자세한 내용은 [Amazon CloudWatch 사용 설명서의 Amazon 경보 사용](#)을 참조하세요. CloudWatch

Note

를 볼 수 있는 권한이 없는 경우 경보를 볼 CloudWatch수 없습니다.

활성화된 각 게이트웨이에 대해 다음 CloudWatch 경보를 생성하는 것이 좋습니다.

- 높은 IO 대기: 15분 내에 3개의 데이터 포인트에 대해 IoWaitpercent ≥ 20
- 캐시 더티 백분율: 20분 내에 4개의 데이터 포인트에 대해 CachePercentDirty > 80
- 상태 알림: 5분 이내에 1개의 데이터 포인트에 대해 HealthNotifications ≥ 1 . 이 경보를 구성할 때 누락된 데이터 처리를 로 설정합니다notBreaching.

 Note

게이트웨이에 의 이전 상태 알림이 있는 경우에만 상태 알림 경보를 설정할 수 있습니다 CloudWatch.

HA 모드가 활성화된 VMware 호스트 플랫폼의 게이트웨이의 경우 이 추가 CloudWatch 경보도 권장합니다.

- 가용성 알림: 5분 이내에 1개의 데이터 포인트에 대해 AvailabilityNotifications ≥ 1 . 이 경보를 구성할 때 누락된 데이터 처리를 로 설정합니다notBreaching.

다음 표에서는 경보 상태에 대해 설명합니다.

State	설명
정상	지표 또는 표현식이 정의된 임계값 내에 있습니다.
경보	지표 또는 표현식이 정의된 임계값을 벗어났습니다.
데이터 부족	경보가 방금 시작되었거나, 지표를 사용할 수 없거나, 지표를 통해 경보 상태를 결정하는 데 사용할 충분한 데이터가 없습니다.
None(없음)	게이트웨이에 대한 경보가 생성되지 않습니다. 새 경보를 생성하려면 게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성 단원을 참조하십시오.

State	설명
Unavailable	경보의 상태를 알 수 없습니다. 모니터링 탭에서 오류 정보를 보려면 사용할 수 없음을 선택합니다.

게이트웨이에 권장되는 CloudWatch 경보 생성

Storage Gateway 콘솔을 사용하여 새 게이트웨이를 생성할 때 초기 설정 프로세스의 일부로 모든 권장 CloudWatch 경보를 자동으로 생성하도록 선택할 수 있습니다. 자세한 내용은 [Tape Gateway 구성](#)을 참조하세요. 기존 게이트웨이에 권장되는 CloudWatch 경보를 추가하거나 업데이트하려면 다음 절차를 사용합니다.

기존 게이트웨이에 권장되는 CloudWatch 경보를 추가하거나 업데이트하려면

Note

이 기능에는 미리 구성된 Storage Gateway 전체 액세스 CloudWatch 정책의 일부로 자동으로 부여되지 않는 정책 권한이 필요합니다. 권장 CloudWatch 경보를 생성하려고 하기 전에 보안 정책이 다음 권한을 부여하는지 확인하세요.

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

1. <https://console.aws.amazon.com/storagegateway/홈/>에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 를 선택한 다음 권장 CloudWatch 경보를 생성할 게이트웨이를 선택합니다.
3. 게이트웨이 세부 정보 페이지에서 모니터링 탭을 선택합니다.
4. 경보에서 권장 경보 생성을 선택합니다. 권장 경보는 자동으로 생성됩니다.

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

게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성

CloudWatch 는 Amazon Simple Notification Service(Amazon SNS)를 사용하여 경보 상태가 변경될 때 경보 알림을 보냅니다. 경보는 지정한 기간 동안 단일 지표를 감시하고 여러 기간에 지정된 임계값에 대한 지표 값을 기준으로 작업을 하나 이상 수행합니다. 작업은 Amazon SNS 주제로 전송되는 알림입니다. CloudWatch 경보를 생성할 때 Amazon SNS 주제를 생성할 수 있습니다. Amazon 에 대한 자세한 내용은 Amazon Simple Notification Service 개발자 안내서의 Amazon [SNS?란 무엇입니까?](#)를 SNS 참조하세요.

Storage Gateway 콘솔에서 CloudWatch 경보를 생성하려면

1. <https://console.aws.amazon.com/storagegateway/홈/>에서 Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 경보를 생성할 게이트웨이를 선택합니다.
3. 게이트웨이 세부 정보 페이지에서 모니터링 탭을 선택합니다.
4. 경보에서 경보 생성을 선택하여 CloudWatch 콘솔을 엽니다.
5. CloudWatch 콘솔을 사용하여 원하는 경보 유형을 생성합니다. 다음 유형의 경보를 생성할 수 있습니다.
 - 정적 임계값 경보: 선택한 지표에 대해 설정된 임계값을 기반으로 하는 경보입니다. 지표가 지정된 평가 기간 수 동안 임계값을 위반하면 경보가 ALARM 상태가 됩니다.

정적 임계값 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 [정적 임계값을 기반으로 CloudWatch 경보 생성](#)을 참조하세요.

- 이상 탐지 경보: 이상 탐지는 과거 지표 데이터를 마이닝하고 예상 값의 모델을 생성합니다. 이상 탐지 임계값의 값을 설정하고 모델과 함께 이 임계값을 CloudWatch 사용하여 지표 값의 “정상” 범위를 결정합니다. 임계값에 대한 값이 클수록 ‘정상’ 값의 밴드가 더 두꺼워집니다. 지표 값이 예상 값 범위보다 높을 때만 경보를 활성화하거나, 범위보다 낮을 때만 경보를 활성화하거나, 범위보다 높거나 낮을 때 경보를 활성화하도록 선택할 수 있습니다.

이상 탐지 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 [이상 탐지를 기반으로 CloudWatch 경보 생성](#)을 참조하세요.

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

지표 수학 표현식 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 [지표 수학 표현식을 기반으로 CloudWatch 경보 생성](#)을 참조하세요.

- 복합 경고: 다른 경보의 경보 상태를 감시하여 경보 상태를 결정하는 경보입니다. 복합 경보를 사용하면 경보 노이즈를 줄이는 데 도움이 될 수 있습니다.

복합 경보를 생성하려면 Amazon CloudWatch 사용 설명서의 [복합 경고 생성](#)을 참조하세요.

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

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

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

- 탐색 창에서 게이트웨이를 선택한 다음 경보를 확인할 게이트웨이의 경보 상태를 선택합니다.

경보를 편집하거나 삭제하는 방법에 대한 자세한 내용은 [CloudWatch 경보 편집 또는 삭제를 참조하세요](#).

Note

Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하면 게이트웨이와 연결된 모든 CloudWatch 경보도 자동으로 삭제됩니다.

Tape Gateway 모니터링

이 섹션의 이 주제에서는 Tape Gateway를 모니터링하는 방법에 대한 절차 및 개념 정보를 설명합니다. Tape Gateway와 연결된 가상 테이프, 캐시 스토리지 및 업로드 버퍼를 모니터링할 수 있습니다. AWS Management Console를 사용하여 Tape Gateway에 대한 지표를 볼 수 있습니다. 지표를 사용하여 Tape Gateway의 상태를 추적하고 하나 이상의 지표가 정의된 임계값 범위를 벗어나는 경우 이를 알리도록 경보를 설정할 수 있습니다.

Amazon CloudWatch Logs를 사용하여 Tape Gateway 및 관련 리소스의 상태에 대한 정보를 가져올 수 있습니다. 로그를 사용하여 게이트웨이에 로그가 발생하는지 모니터링할 수 있습니다. 또한 Amazon CloudWatch 구독 필터를 사용하여 로그 정보 처리를 실시간으로 자동화할 수 있습니다.

Storage Gateway는 추가 비용 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이러한 지표를 사용하면 기록 정보에 액세스하고 Tape Gateway와 가상 테이프의 성능을 더 잘 파악할 수 있습니다. 에 대한 자세한 내용은 [Amazon CloudWatch 사용 설명서 섹션을](#) CloudWatch참조하세요.

데이터 처리량, 데이터 지연 시간 및 초당 작업은 스토리지 애플리케이션이 Tape Gateway를 사용하여 어떻게 작동하는지 이해하는 데 사용할 수 있는 측정값입니다. 정확한 집계 통계를 사용하는 경우 이러한 값은 제공되는 Storage Gateway 지표를 사용하여 측정할 수 있습니다.

주제

- [로그 그룹을 사용하여 Tape Gateway 상태 CloudWatch 로그 가져오기](#)
- [Amazon CloudWatch 지표 사용](#)
- [가상 테이프 지표 이해](#)
- [Tape Gateway와 간의 성능 측정 AWS](#)

로그 그룹을 사용하여 Tape Gateway 상태 CloudWatch 로그 가져오기

Amazon CloudWatch Logs를 사용하여 Tape Gateway 및 관련 리소스의 상태에 대한 정보를 가져올 수 있습니다. 로그를 사용하여 게이트웨이에 로그가 발생하는지 모니터링할 수 있습니다. 또한 Amazon CloudWatch 구독 필터를 사용하여 로그 정보 처리를 실시간으로 자동화할 수 있습니다. 자세한 내용은 Amazon 사용 설명서의 [구독을 통한 로그 데이터의 실시간 처리를 참조하세요](#). CloudWatch

예를 들어, 게이트웨이가 VMware HA로 활성화된 클러스터에 배포되어 있고 오류에 대해 알아야 한다고 가정해 보겠습니다. 게이트웨이를 모니터링하고 게이트웨이에 오류가 발생하면 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 [Tape Gateway 구성을 참조하세요](#). CloudWatch 로그 그룹에 대한 일반적인 내용은 Amazon 사용 설명서의 [로그 그룹 및 로그 스트림 작업을 참조하세요](#). CloudWatch

문제를 해결하고 이 오류 유형을 해결하는 방법에 대한 자세한 내용은 [가상 테이프 관련 문제 해결 단원](#)을 참조하십시오.

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

File Gateway에서 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 로그인 AWS Management Console 하고 <https://console.aws.amazon.com/storagegateway/> [에서](#) Storage Gateway 콘솔을 엽니다.

2. 탐색 창에서 게이트웨이를 선택한 다음 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 작업 에서 게이트웨이 정보 편집을 선택하거나 세부 정보 탭의 상태 로그 및 활성화되지 않음 에서 로그 그룹 구성을 선택하여 편집 CustomerGatewayName 대화 상자를 엽니다.
4. 게이트웨이 상태 로그 그룹에서 다음 중 하나를 선택합니다.
 - 로그 그룹을 사용하여 게이트웨이를 모니터링하지 않으려면 CloudWatch 로깅을 비활성화합니다.
 - 새 로그 그룹을 생성하여 새 CloudWatch 로그 그룹을 생성합니다.
 - 기존 로그 그룹을 사용하여 이미 존재하는 CloudWatch 로그 그룹을 사용합니다.

기존 로그 그룹 목록에서 로그 그룹을 선택합니다.
5. Save changes(변경 사항 저장)를 선택합니다.
6. 게이트웨이의 상태 로그를 확인하려면 다음을 수행합니다.
 1. 탐색 창에서 게이트웨이를 선택한 다음 CloudWatch 로그 그룹을 구성한 게이트웨이를 선택합니다.
 2. 세부 정보 탭을 선택하고 상태 로그 에서 CloudWatch 로그 를 선택합니다. 로그 그룹 세부 정보 페이지가 콘솔에서 CloudWatch 열립니다.

다음은 로 전송되는 Tape Gateway 이벤트 메시지의 예입니다 CloudWatch. 이 예에서는 TapeStatusTransition 메시지를 보여 줍니다.

```
{
  "severity": "INFO",
  "source": "FZTT16FCF5",
  "type": "TapeStatusTransition",
  "gateway": "sgw-C51DFEAC",
  "timestamp": "1581553463831",
  "newStatus": "RETRIEVED"
}
```

Amazon CloudWatch 지표 사용

AWS Management Console 또는 CLI를 사용하여 Tape Gateway에 대한 모니터링 데이터를 가져올 수 있습니다. CloudWatch API 콘솔에는 의 원시 데이터를 기반으로 일련의 그래프가 표시됩니다. CloudWatch API 는 CloudWatch API [Amazon AWS 소프트웨어 개발 키트\(SDKs\)](#) 또는 [Amazon CloudWatch API](#) 도구 중 하나를 통해서도 사용할 수 있습니다. 필요에 따라 콘솔에 표시되거나 에서 검색된 그래프를 사용하는 것이 좋습니다.

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

- 작업할 지표 차원. 차원은 지표를 고유하게 식별하는 데 도움이 되는 이름-값 페어입니다. Storage Gateway의 차원은 GatewayId 및 GatewayName입니다. CloudWatch 콘솔에서 Gateway Metrics 뷰를 사용하여 게이트웨이별 및 테이프별 차원을 쉽게 선택할 수 있습니다. 차원에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [차원](#)을 참조하세요.
- ReadBytes와 같은 지표 이름.

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

Amazon CloudWatch 네임 스페이스	측정기준	설명
AWS/StorageGateway	GatewayId , GatewayName	<p>이 차원은 Tape Gateway 게이트웨이의 여러 측면을 설명하는 지표 데이터를 필터링합니다. GatewayId 차원과 GatewayName 차원을 모두 지정하여 작업할 Tape Gateway를 식별할 수 있습니다.</p> <p>Tape Gateway의 처리량 및 지연 시간 데이터는 Tape Gateway의 모든 가상 테이프에 기반을 두고 있습니다.</p> <p>자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.</p>

게이트웨이 및 테이프 지표 작업은 기타 서비스 지표 작업과 유사합니다. 다음 설명서에서 CloudWatch 가장 일반적인 지표 작업에 대한 설명을 확인할 수 있습니다.

- [얻을 수 있는 지표 보기](#)

- [지표에 대한 통계 구하기](#)
- [경보 생성 CloudWatch](#)

가상 테이프 지표 이해

가상 테이프를 나타내는 Storage Gateway 지표에 대한 정보는 다음에서 확인할 수 있습니다. 각 테이프에는 연관된 지표 집합이 있습니다.

일부 테이프별 지표는 특정 게이트웨이별 지표와 이름이 같습니다. 이 지표는 같은 종류의 측정값을 나타내지만 게이트웨이가 아닌 테이프에 한정됩니다. 작업을 시작하기 전에 게이트웨이 지표로 작업할지 아니면 테이프 지표로 작업할지를 지정합니다. 테이프 지표로 작업하는 경우 지표를 보려는 테이프의 테이프 ID를 지정합니다. 자세한 내용은 [Amazon CloudWatch 지표 사용](#) 단원을 참조하십시오.

Note

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

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

지표	설명
CachePercentDirty	<p>AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율 중 테이프가 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다.</p> <p>게이트웨이의 CachePercentDirty 지표를 사용하면 AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율을 알 수 있습니다. 자세한 내용은 게이트웨이 지표 이해 단원을 참조하십시오.</p> <p>단위: 백분율</p>
CloudTraffic	클라우드에서 테이프를 업로드 및 다운로드한 바이트 수입니다.

지표	설명
	단위: 바이트
IoWaitPercent	현재 테이프에서 사용되는 할당된 IoWait 단위의 백분율입니다. 단위: 백분율
HealthNotification	테이프에서 보낸 상태 알림 수입니다. 단위: 개수
MemUsedBytes	테이프에서 현재 사용 중인 할당된 메모리의 백분율입니다. 단위: 바이트
MemTotalBytes	테이프에서 현재 사용 중인 총 메모리의 백분율입니다. 단위: 바이트
ReadBytes	파일 공유에 대한 보고 기간 동안 온프레미스 애플리케이션으로부터 읽은 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하여 처리량을 측정하고 통계와 함께 사용하여 Samples 를 측정합니다IOPS. 단위: 바이트
UserCpuPercent	현재 테이프에서 사용되는 사용자에게 할당된 CPU 컴퓨팅 단위의 백분율입니다. 단위: 백분율

지표	설명
WriteBytes	<p>보고 기간 동안 온프레미스 애플리케이션에 작성한 총 바이트 수입니다.</p> <p>이 지표를 Sum 통계와 함께 사용하여 처리량을 측정하고 통계와 함께 사용하여 Samples 를 측정합니다IOPS.</p> <p>단위: 바이트</p>

Tape Gateway와 간의 성능 측정 AWS

데이터 처리량, 데이터 지연 시간 및 초당 작업은 Tape Gateway를 사용하는 애플리케이션 스토리지의 성능을 파악하는 데 사용할 수 있는 지표입니다. 정확한 집계 통계를 사용하는 경우 이러한 값은 제공되는 Storage Gateway 지표를 사용하여 측정할 수 있습니다.

통계는 지정 기간에 걸친 지표를 집계한 것입니다. 에서 지표 값을 볼 때 데이터 지연 시간(밀리초)에 대한 CloudWatch Average 통계를 사용하고 초당 입/출력 작업()에 대한 통계Samples를 사용합니다 IOPS. 자세한 내용은 Amazon CloudWatch 사용 설명서의 [통계](#)를 참조하세요.

다음 표에는 Tape Gateway와 IOPS 간의 처리량, 지연 시간 및 를 측정하는 데 사용할 수 있는 지표와 해당 통계가 요약되어 있습니다 AWS.

관심 항목	측정 방법
지연 시간	Average CloudWatch 통계와 함께 ReadTime 및 WriteTime 지표를 사용합니다. 예를 들어 Average 지표의 ReadTime 값은 샘플 시간에 걸친 작업당 지연 시간에 해당합니다.
에 대한 처리량 AWS	Sum CloudWatch 통계와 함께 CloudBytesDownloaded 및 CloudBytesUploaded 지표를 사용합니다. 예를 들어 샘플 기간 5분 동안 지표 Sum 값을 CloudBytesDownloaded 300초로 나누면 에서 Tape Gateway AWS 로의 처리량이 초당 바이트 단위로 제공됩니다.
에 대한 데이터 지연 시간 AWS	CloudDownloadLatency 통계와 함께 Average 지표를 사용합니다. 예를 들어 Average 지표의 CloudDownloadLatency 통계는 작업당 지연 시간에 해당합니다.

Tape Gateway에서 로 업로드 데이터 처리량을 측정하려면 AWS

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. 지표 탭을 선택합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택하고 작업할 Tape Gateway를 찾습니다.
4. CloudBytesUploaded 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.
6. Sum 통계를 선택합니다.
7. 기간에서 5분 이상의 값을 선택합니다.
8. 그 결과로 얻은 시간순 데이터 포인트 집합에서 각 데이터 포인트를 기간(초 단위)으로 나누어 샘플 기간의 처리량을 얻습니다. 예를 들어, Tape Gateway에서 로의 처리량 AWS 이 지정된 데이터 포인트에 대해 555,544,576바이트이고 기간이 300초인 경우 대략적인 처리량은 초당 1.85메가바이트가 됩니다.

Tape Gateway에서 까지의 데이터 지연 시간을 측정하려면 AWS

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. 지표 탭을 선택합니다.
3. StorageGateway: GatewayMetrics 차원을 선택하고 작업할 Tape Gateway를 찾습니다.
4. CloudDownloadLatency 지표를 선택합니다.
5. 시간 범위에서 값을 선택합니다.
6. Average 통계를 선택합니다.
7. 기간에서 값을 5분으로 선택하여 기본 보고 시간과 일치하도록 합니다.

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

Tape Gateway의 처리량에 대한 상한 임계값 경보를 로 설정하려면 AWS

1. 에서 CloudWatch 콘솔을 엽니다 <https://console.aws.amazon.com/cloudwatch/>.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택하고 작업할 Tape Gateway를 찾습니다.
4. CloudBytesUploaded 지표를 선택합니다.

5. CloudBytesUploaded 지표가 지정한 시간 동안 지정한 값보다 크거나 같을 때 경보 상태를 정의하여 경보를 정의합니다. 예를 들어 CloudBytesUploaded 지표가 60분 동안 10메가바이트보다 클 때 경보 상태를 정의할 수 있습니다.
6. 경보 상태에 대해 취할 조치를 구성합니다. 예를 들어 이메일 알림이 전송되도록 할 수 있습니다.
7. 경보 생성을 선택합니다.

에서 데이터를 읽기 위한 상한 임계값 경보를 설정하려면 AWS

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

게이트웨이 유지 관리

Tape Gateway 유지 관리에는 캐시 스토리지 및 업로드 버퍼 공간을 위한 로컬 디스크 크기 조정 및 구성, 업데이트 관리 및 업데이트 일정 설정, 대역폭 사용량 관리, 필요한 경우 게이트웨이 및 관련 리소스 종료 또는 삭제와 같은 작업이 포함됩니다. 이 작업은 모든 게이트웨이 유형에 공통된 것입니다. 게이트웨이를 생성하지 않았으면 [게이트웨이 생성](#) 단원을 참조하십시오.

주제

- [Storage Gateway의 로컬 디스크 관리](#) - 버퍼링 및 스토리지를 위해 Tape Gateway 에 할당하는 로컬 디스크를 관리하고 디스크 크기 요구 사항을 평가하고 캐시 용량을 추가하는 방법을 알아봅니다.
- [Tape Gateway의 대역폭 관리](#) - 게이트웨이에서 사용하는 네트워크 대역폭의 양을 제어하기 위해 게이트웨이의 업로드 처리량을 AWS 로 제한하는 방법을 알아봅니다.
- [게이트웨이 업데이트 관리](#) - 유지 관리 업데이트를 켜거나 끄고 Tape Gateway 의 유지 관리 기간 일정을 수정하는 방법을 알아봅니다.
- [게이트웨이 VM 종료](#) - 하이퍼바이저에 패치를 적용할 때와 같이 유지 관리를 위해 게이트웨이 가상 머신을 종료하거나 재부팅해야 하는 경우 어떻게 해야 하는지 알아봅니다.
- [게이트웨이 삭제 및 관련 리소스 제거](#) - AWS Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하고 연결된 리소스를 정리하여 계속 사용 시 요금이 부과되지 않도록 하는 방법을 알아봅니다.

Storage Gateway의 로컬 디스크 관리

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

주제

- [로컬 디스크 스토리지 용량 결정](#)
- [추가 업로드 버퍼 또는 캐시 스토리지 구성](#)

로컬 디스크 스토리지 용량 결정

게이트웨이에 할당하려는 디스크의 개수 및 크기는 사용자가 직접 결정합니다. 배포하는 스토리지 솔루션에 따라 게이트웨이에는 다음과 같은 추가 스토리지가 필요합니다.

- Tape Gateway에는 최소 2개의 디스크가 필요합니다. 하나는 캐시로 사용하고 다른 하나는 업로드 버퍼로 사용합니다.

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

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

Note

디스크를 프로비저닝할 때 동일한 물리 리소스(동일한 디스크)를 사용하는 경우에는 업로드 버퍼 및 캐시 스토리지에 로컬 디스크를 프로비저닝하지 말 것을 적극 권장합니다. 기본 물리적 스토리지 리소스는 에서 데이터 스토어로 표시됩니다VMware. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 로컬 디스크를 프로비저닝하는 경우(예: 캐시 스토리지 또는 업로드 버퍼 용도), 가상 디스크를 동일한 데이터 스토어에 VM으로 저장하거나 다른 데이터 스토어에 저장하는 옵션을 선택할 수 있습니다.

데이터 스토어가 한 개 이상인 경우에는 캐시 스토리지에 데이터 스토어 한 개, 업로드 버퍼에 다른 데이터 스토어 한 개씩 선택할 것을 적극 권장합니다. 오직 기본 물리 디스크 한 개의 지원을 받는 데이터 스토어는 캐시 스토리지와 업로드 버퍼를 모두 지원하는 데 사용되는 경우 성능이 떨어질 수 있습니다. 백업이와 같은 성능이 떨어지는 RAID 구성인 경우에도 마찬가지입니다. RAID1.

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

할당할 업로드 버퍼의 크기 결정

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

Note

Tape Gateway의 경우, 업로드 버퍼가 정해진 용량에 도달하면 애플리케이션이 스토리지 볼륨에(서) 데이터를 계속 읽고 쓸 수 있습니다. 그러나 Tape Gateway는 업로드 버퍼에 볼륨 데이터를 쓰지 않으며 Storage Gateway가 로컬에 저장된 데이터를 에 저장된 데이터의 복사본과 동기화할 AWS 때까지 이 데이터를 에 업로드하지 않습니다 AWS. 이 동기화는 볼륨이 BOOTSTRAPPING 상태일 때 발생합니다.

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

수신 데이터 속도

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

송신 데이터 속도

이 속도는 네트워크 처리량을 가리킵니다. 즉 게이트웨이가 데이터를 AWS에 업로드할 수 있는 속도를 말합니다. 이 속도는 네트워크 속도, 사용률 및 대역폭 조절 기능 활성화 여부에 따라 달라집니다. 이 속도는 압축에 맞게 조정해야 합니다. 에 데이터를 업로드할 때 게이트웨이 AWS는 가능

한 경우 데이터 압축을 적용합니다. 예를 들어 애플리케이션 데이터가 텍스트만으로 되어 있는 경우, 약 2:1의 효과적인 압축 비율을 얻을 수 있습니다. 그러나 동영상을 작성하는 경우, 게이트웨이가 데이터 압축을 완료할 수 없고 게이트웨이에 더 많은 업로드 버퍼가 필요할 수 있습니다.

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

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

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

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

Example

$$((40 \text{ MB/sec}) - (12 \text{ MB/sec} * 2)) * (12 \text{ hours} * 3600 \text{ seconds/hour}) = 691200 \text{ megabytes}$$

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

할당할 캐시 스토리지의 크기 결정

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

초기에는 이 근사치를 사용하여 캐시 스토리지용 디스크를 프로비저닝할 수 있습니다. 그런 다음 Amazon CloudWatch 운영 지표를 사용하여 캐시 스토리지 사용량을 모니터링하고 콘솔을 사용하여

필요에 따라 더 많은 스토리지를 프로비저닝할 수 있습니다. 측정치 사용 및 경보 설정에 대한 정보는 [캐시 스토리지 모니터링](#) 단원을 참조하십시오.

추가 업로드 버퍼 또는 캐시 스토리지 구성

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

Important

기존 게이트웨이에 캐시 또는 업로드 버퍼를 추가할 때는 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에서 새 디스크를 생성해야 합니다. 캐시 또는 업로드 버퍼로 이미 할당된 기존 디스크의 크기는 제거하거나 변경하지 마세요.

게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면

1. 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에 하나 이상의 새 디스크를 프로비저닝합니다. 하이퍼바이저에서 디스크를 프로비저닝하는 방법에 대한 자세한 내용은 해당 하이퍼바이저의 설명서를 참조하세요. Amazon EC2 인스턴스의 Amazon EBS 볼륨 프로비저닝에 대한 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서의 Amazon [EBS 볼륨](#)을 참조하세요. 다음 단계에서는 이 디스크를 업로드 버퍼 또는 캐시 스토리지로 구성합니다.
2. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
3. 탐색 창에서 게이트웨이를 선택합니다.
4. 게이트웨이를 검색하고 목록에서 선택합니다.
5. 작업 메뉴에서 스토리지 구성을 선택합니다.
6. 스토리지 구성 섹션에서 프로비저닝한 디스크를 지정합니다. 디스크가 표시되지 않으면 새로 고침 아이콘을 선택하여 목록을 새로 고칩니다. 각 디스크 CACHED STORAGE에 대해 할당 대상 드롭 다운 메뉴에서 UPLOAD BUFFER 또는 를 선택합니다.
7. 변경 사항 저장을 선택하여 구성 설정을 저장합니다.

Tape Gateway의 대역폭 관리

게이트웨이에서 게이트웨이로의 업로드 처리량 또는 게이트웨이로의 다운로드 처리량을 제한 (AWS 또는 조절) AWS 할 수 있습니다. 대역폭 조절을 사용하면 게이트웨이가 사용하는 네트워크 대역폭의

전송량을 통제하는 데 도움이 됩니다. 기본적으로 활성화된 게이트웨이는 업로드 또는 다운로드에 대한 속도 제한이 없습니다.

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

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

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

Note

이 섹션의 정보는 Tape Gateway 및 Volume Gateway에만 해당됩니다. Amazon S3 File Gateway의 대역폭을 관리하려면 [Amazon S3 File Gateway의 대역폭 관리](#)를 참조하세요. Amazon FSx File Gateway에서는 현재 대역폭 속도 제한이 지원되지 않습니다.

주제

- [Storage Gateway 콘솔을 사용하여 대역폭 조절 변경](#)
- [Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절](#)
- [awscli를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java](#)
- [awscli를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for .NET](#)
- [awscli를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS Tools for Windows PowerShell](#)

Storage Gateway 콘솔을 사용하여 대역폭 조절 변경

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

콘솔을 사용하여 게이트웨이의 대역폭 조절을 변경하려면

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

2. 왼쪽 탐색 창에서 게이트웨이를 선택한 다음 관리할 게이트웨이를 선택합니다.
3. 작업에서 대역폭 제한 편집을 선택합니다.
4. 속도 제한 편집 대화 상자에서 새 제한 값을 입력한 다음 저장을 선택합니다. 변경 사항은 해당 게이트웨이의 세부 정보 탭에 표시됩니다.

Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절

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

게이트웨이 대역폭 조절 일정을 추가 또는 수정하려면

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

게이트웨이의 bandwidth-rate-limit 일정은 대역폭 속도 제한 스케줄 편집 대화 상자에 표시됩니다. 기본적으로 새 게이트웨이 bandwidth-rate-limit 일정은 비어 있습니다.

4. 대역폭 속도 제한 일정 편집 대화 상자에서 새 항목 추가를 선택하여 새 bandwidth-rate-limit 간격을 추가합니다. 각 bandwidth-rate-limit 간격에 대해 다음 정보를 입력합니다.
 - 요일 - 주중 (월요일부터 금요일까지), 주말 (토요일과 일요일), 요일별 또는 하나 이상의 특정 요일에 대한 bandwidth-rate-limit 간격을 생성할 수 있습니다.
 - 시작 시간 - 대역폭 간격의 시작 시간을 게이트웨이의 현지 시간대(HH:MM 형식)로 입력합니다.

Note

bandwidth-rate-limit 간격은 여기에 지정한 분의 시작부터 시작됩니다.

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

Important

bandwidth-rate-limit 간격은 여기에 지정된 분 말일에 종료됩니다. 한 시간이 지나면 종료되는 간격을 예약하려면 **59**를 입력합니다.

간격 사이에 중단 없이 시간 시작 시점에 전환되는 연속적인 간격을 예약하려면 첫 번째 간격의 종료 분에 **59**를 입력합니다. 다음 간격의 시작 분에는 **00**을 입력합니다.

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

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

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

변경을 완료했으면 저장을 선택합니다.

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

Important

bandwidth-rate-limit 간격은 겹칠 수 없습니다. 간격의 시작 시간은 이전 간격의 종료 시간 이후, 다음 간격의 시작 시간 이전이어야 합니다.

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

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

를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java

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

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

다음 Java 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름 (ARN), 업로드 및 다운로드 한도를 제공해

야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량을 참조하십시오](#). AWS 일반 참조

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;

public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

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

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

        // Create a Storage Gateway client
        sgClient = new AWSStorageGatewayClient(new PropertiesCredentials(
UpdateBandwidthExample.class.getResourceAsStream("AwsCredentials.properties")));
        sgClient.setEndpoint(serviceURL);

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

    }

    private static void UpdateBandwidth(String gatewayARN2, long uploadRate2,
        long downloadRate2) {
        try
        {
            UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
```

```

        new UpdateBandwidthRateLimitRequest()
            .withGatewayARN(gatewayARN)
            .withAverageDownloadRateLimitInBitsPerSec(downloadRate)
            .withAverageUploadRateLimitInBitsPerSec(uploadRate);

        UpdateBandwidthRateLimitResult updateBandwidthRateLimitResult =
sgClient.updateBandwidthRateLimit(updateBandwidthRateLimitRequest);
        String returnGatewayARN = updateBandwidthRateLimitResult.getGatewayARN();
        System.out.println("Updated the bandwidth rate limits of " +
returnGatewayARN);
        System.out.println("Upload bandwidth limit = " + uploadRate + " bits per
second");
        System.out.println("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonClientException ex)
    {
        System.err.println("Error updating gateway bandwidth.\n" + ex.toString());
    }
}
}

```

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

대역폭 속도 제한을 프로그래밍 방식으로 업데이트하면 일정 기간 동안 예약된 작업을 사용하는 등의 방법으로 자동으로 제한을 조정할 수 있습니다. 다음 예시는 AWS SDK for .NET를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예제 코드를 사용하려면 a 실행에 익숙해야 합니다. NET콘솔 애플리케이션. 자세한 내용은 AWS SDK for .NET 개발자 안내서에서 [시작하기](#)를 참조하세요.

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

다음 C# 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름 (ARN), 업로드 및 다운로드 한도를 제공해야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하십시오. AWS 일반 참조

```

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

```

```
using Amazon.StorageGateway.Model;

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

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

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

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

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

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

```

        UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
        String returnGatewayARN =
updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
        Console.WriteLine("Updated the bandwidth rate limits of " +
returnGatewayARN);
        Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
second");
        Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
per second");
    }
    catch (AmazonStorageGatewayException ex)
    {
        Console.WriteLine("Error updating gateway bandwidth.\n" +
ex.ToString());
    }
}
}
}
}

```

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

대역폭 속도 제한을 프로그래밍 방식으로 업데이트하면 일정 기간 동안 예약된 작업을 사용하는 등의 방법으로 자동으로 제한을 조정할 수 있습니다. 다음 예시는 AWS Tools for Windows PowerShell를 사용하여 게이트웨이의 대역폭 속도 제한을 업데이트하는 방법을 보여줍니다. 예제 코드를 사용하려면 PowerShell 스크립트 실행에 익숙해야 합니다. 자세한 내용은 AWS Tools for Windows PowerShell 사용 설명서에서 [시작하기](#)를 참조하세요.

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

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

```

<#
.DESCRIPTION
    Update Gateway bandwidth limits.

.NOTES
    PREREQUISITES:

```

```

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

```

.EXAMPLE

```

powershell.exe .\SG_UpdateBandwidth.ps1
#>

$UploadBandwidthRate = 51200
$DownloadBandwidthRate = 102400
$gatewayARN = "*** provide gateway ARN ***"

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

$limits = Get-SGBandwidthRateLimit -GatewayARN $gatewayARN

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

```

게이트웨이 업데이트 관리

Storage Gateway는 관리형 클라우드 서비스 구성 요소와 온프레미스 또는 AWS 클라우드의 Amazon EC2 인스턴스에 배포하는 게이트웨이 어플라이언스 구성 요소로 구성됩니다. 두 구성 요소 모두 정기적인 업데이트를 받습니다. 이 섹션의 주제에서는 이러한 업데이트의 주기, 업데이트 적용 방법, 배포의 게이트웨이에서 업데이트 관련 설정을 구성하는 방법을 설명합니다.

Important

Storage Gateway 어플라이언스는 관리형 가상 머신으로 취급해야 하며, 어떤 방식으로든 설치에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 AWS 게이트웨이 업데이트 메커니즘(예: SSM 또는 하이퍼바이저 도구) 이외의 방법을 사용하여 소프트웨어 패키지를 설치하거나 업데이트하려고 하면 게이트웨이가 오작동할 수 있습니다.

빈도 및 예상 동작 업데이트

AWS 는 배포된 게이트웨이를 중단하지 않고 필요에 따라 클라우드 서비스 구성 요소를 업데이트합니다. 배포된 게이트웨이 어플라이언스는 월별 유지 관리 업데이트를 받습니다. 월간 유지 관리 업데이트에는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안을 해결하기 위한 수정 사항, 새 기능에 대한 액세스가 포함될 수 있습니다. 모든 업데이트는 누적되며 적용 시 게이트웨이를 현재 버전으로 업그레이드합니다. 각 업데이트에 포함된 특정 변경 사항에 대한 자세한 내용은 [Tape Gateway Appliance 소프트웨어 릴리스 정보](#) .

월간 유지 관리 업데이트로 인해 서비스가 잠시 중단될 수 있습니다. 업데이트 중에는 게이트웨이의 VM 호스트를 재부팅할 필요가 없지만 게이트웨이 어플라이언스가 업데이트되고 다시 시작되는 동안 게이트웨이를 잠시 사용할 수 없습니다. iSCSI 이니시에이터의 제한 시간을 늘려 게이트웨이 재시작으로 인해 애플리케이션이 중단될 가능성을 최소화할 수 있습니다. Windows 및 Linux의 iSCSI 이니시에이터 제한 시간 증가에 대한 자세한 내용은 [Windows iSCSI 설정 사용자 지정](#) 및 [Linux iSCSI 설정 사용자 지정](#) 섹션을 참조하세요.

게이트웨이를 배포하고 활성화하면 기본 주간 유지 관리 기간 일정이 설정됩니다. 언제든지 유지 관리 기간 일정을 수정할 수 있습니다. 월간 유지 관리 업데이트를 끌 수도 있지만, 업데이트를 켜 두는 것이 좋습니다.

Note

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

업데이트가 게이트웨이에 적용되기 전에는 Storage Gateway 콘솔 및 에 대한 메시지를 AWS 알려줍니다 AWS Health Dashboard. 자세한 내용은 [AWS Health Dashboard](#) 단원을 참조하십시오. 소프트웨어 업데이트 알림이 전송되는 이메일 주소를 수정하려면 AWS 계정 관리 참조 가이드의 [AWS 계정 대체 연락처 업데이트를 참조하세요](#).

업데이트를 사용할 수 있으면 게이트웨이 세부 정보 탭에 유지 관리 메시지가 표시됩니다. 세부 정보 탭에서 마지막으로 성공한 업데이트가 적용된 날짜와 시간을 확인할 수도 있습니다.

유지 관리 업데이트 켜기 또는 끄기

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

유지 관리 업데이트가 꺼져 있는 경우 게이트웨이는 이러한 업데이트를 자동으로 적용하지 않지만 Storage Gateway 콘솔, API 또는 CLI를 사용하여 언제든지 수동으로 적용할 수 있습니다. 긴급 업데이트는 이 설정과 관계없이 구성된 유지 관리 기간 동안 때때로 적용됩니다.

Note

다음 절차에서는 Storage Gateway 콘솔을 사용하여 게이트웨이 업데이트를 켜거나 끄는 방법을 설명합니다. CLI를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway 참조 [UpdateMaintenanceStartTime](#)의 섹션을 API 참조하세요. Storage Gateway API

Storage Gateway 콘솔을 사용하여 유지 관리 업데이트를 켜거나 끄려면:

1. <https://console.aws.amazon.com/storagegateway/> **집에서** Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이 를 선택한 다음 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집 을 선택합니다.
4. 유지 관리 업데이트 에서 켜기 또는 끄기를 선택합니다.
5. 완료되면 변경 사항 저장을 선택합니다.

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

게이트웨이 유지 관리 기간 일정 수정

유지 관리 업데이트가 켜져 있는 경우 게이트웨이는 유지 관리 기간 일정에 따라 이러한 업데이트를 자동으로 적용합니다. 긴급 업데이트는 유지 관리 업데이트 설정과 관계없이 구성된 유지 관리 기간 동안 때때로 적용됩니다.

Note

다음 절차에서는 Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하는 방법을 설명합니다. CLI를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway 참조 [UpdateMaintenanceStartTime](#)의 섹션을 API 참조하세요. Storage Gateway API

Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하려면:

1. <https://console.aws.amazon.com/storagegateway/> **집에서** Storage Gateway 콘솔을 엽니다.

2. 탐색 창에서 게이트웨이를 선택한 다음 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 기간 시작 시간에서 다음을 수행합니다.
 - a. 일정에서 주간 또는 월간을 선택하여 유지 관리 기간 주기를 설정합니다.
 - b. 주간을 선택하는 경우 유지 관리 기간이 시작되는 각 주 동안 특정 시점을 설정하도록 요일 및 시간의 값을 수정합니다.

월별을 선택한 경우, 월별 요일과 시간을 수정하여 유지 관리 기간이 시작되는 각 월의 특정 시점을 설정합니다.

Note

월의 날짜에 설정할 수 있는 최대값은 28입니다. 유지 관리 일정을 29일부터 31일까지 시작하도록 설정할 수 없습니다.

이 설정을 구성하는 동안 오류가 발생하면 게이트웨이 소프트웨어가 최신 상태가 아닐 수 있습니다. 게이트웨이를 수동으로 먼저 업데이트한 다음 유지 관리 기간 일정을 다시 구성해 봅니다.

5. 완료되면 변경 사항 저장을 선택합니다.

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

수동으로 업데이트 적용

게이트웨이에 소프트웨어 업데이트를 사용할 수 있는 경우 아래 절차에 따라 수동으로 적용할 수 있습니다. 이 수동 업데이트 프로세스는 유지 관리 기간 일정을 무시하고 유지 관리 업데이트가 꺼져 있더라도 즉시 업데이트를 적용합니다.

Note

다음 절차에서는 Storage Gateway 콘솔을 사용하여 업데이트를 수동으로 적용하는 방법을 설명합니다. 를 사용하여 프로그래밍 방식으로 이 작업을 수행하려면 Storage Gateway 참조 [UpdateGatewaySoftwareNow](#)의 섹션을 API참조하세요. Storage Gateway API

Storage Gateway 콘솔을 사용하여 게이트웨이 소프트웨어 업데이트를 수동으로 적용하려면:

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 업데이트하려는 게이트웨이를 선택합니다.

업데이트를 사용할 수 있는 경우 콘솔은 게이트웨이 세부 정보 탭에 업데이트를 적용하는 옵션이 포함된 파란색 알림 배너를 표시합니다.

3. 지금 업데이트 적용을 선택하여 게이트웨이를 즉시 업데이트합니다.

Note

이 작업은 업데이트가 설치되는 동안 게이트웨이 기능에 일시적인 중단을 유발합니다. 이 시간 동안 게이트웨이 상태가 Storage Gateway 콘솔 OFFLINE에 나타납니다. 업데이트 설치가 완료되면 게이트웨이가 정상 작업을 재개하고 상태가 로 변경됩니다 RUNNING.

Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭을 확인하여 게이트웨이 소프트웨어가 최신 버전으로 업데이트되었는지 확인할 수 있습니다.

게이트웨이 VM 종료

하이퍼바이저에 패치를 적용할 때와 같이 유지 관리용 VM을 종료하거나 재부팅해야 할 수도 있습니다. VM을 종료하기 전에 게이트웨이를 중지해야 합니다. 이 섹션에서는 Storage Gateway Management Console을 사용하여 게이트웨이를 시작하고 중지하는 데 중점을 두지만 VM 로컬 콘솔 또는 Storage Gateway 를 사용하여 게이트웨이를 중지할 수도 있습니다 API. VM을 켜면 게이트웨이를 다시 시작해야 합니다.

Important

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

Note

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

- 게이트웨이 VM 로컬 콘솔 - [Tape Gateway 로컬 콘솔에 로그인](#) 섹션을 참조하세요.
- Storage Gateway API- - 참조 [ShutdownGateway](#)

Tape Gateway 시작 및 중지

a Tape Gateway를 중지하려면

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

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

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

a Tape Gateway를 시작하려면

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

게이트웨이 삭제 및 관련 리소스 제거

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

게이트웨이를 삭제하면 AWS Storage Gateway 관리 콘솔에 해당 게이트웨이가 더 이상 나타나지 않고 SCSI 이니시에이터와의 연결이 끊어집니다. 게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 별도 지침 대로 연결된 리소스를 제거해야 합니다.

Note

테이프 게이트웨이를 삭제하면 현재 AVAILABLE 상태에 있는 모든 테이프도 삭제되고 해당 테이프의 모든 데이터가 손실됩니다. 삭제하려는 게이트웨이에서 사용 중인 테이프의 데이터를 보존하려면 게이트웨이를 삭제하기 전에 테이프를 보관해야 합니다. 자세한 내용은 [가상 테이프 아카이브](#)를 참조하십시오.

Storage Gateway 콘솔을 사용하거나 프로그래밍 방식으로 게이트웨이를 삭제할 수 있습니다. Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하는 방법에 대한 정보는 다음에서 확인할 수 있습니다. [게이트웨이를 프로그래밍 방식으로 삭제하려면 참조를 참조하십시오. AWS Storage Gateway API](#)

주제

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

Storage Gateway 콘솔을 사용하여 게이트웨이 삭제

게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 추가 작업을 수행하여 게이트웨이에 연결된 리소스를 제거해야 하는 경우도 있습니다. 이 리소스를 제거하면 향후 사용 계획이 없는 리소스에 대한 요금이 발생하는 일을 막을 수 있습니다.

Note

Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 인스턴스는 삭제하기 전까지 계속 존재합니다.

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

게이트웨이를 삭제하려면

1. <https://console.aws.amazon.com/storagegateway/> **집에서** Storage Gateway 콘솔을 엽니다.
2. 게이트웨이를 선택한 다음 삭제할 게이트웨이를 하나 이상 선택합니다.
3. 작업에서 게이트웨이 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.

Warning

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

4. 지정된 게이트웨이를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.
5. (선택 사항) 삭제된 게이트웨이에 대한 피드백을 제공하려면 피드백 대화 상자를 작성한 다음 제출을 선택합니다. 그렇지 않은 경우 건너뛰기를 선택합니다.

Important

게이트웨이를 삭제한 후에는 더 이상 소프트웨어 요금을 지불하지 않아도 되지만 가상 테이프, Amazon Elastic Block Store (AmazonEBS) 스냅샷, Amazon EC2 인스턴스와 같은 리소스는 계속 유지됩니다. 이러한 리소스에 대해서는 계속 비용이 청구됩니다. Amazon 구독을 취소하여 Amazon EC2 인스턴스와 Amazon EBS 스냅샷을 제거하도록 선택할 수 있습니다. EC2 Amazon EC2 구독을 계속 유지하려면 Amazon EC2 콘솔을 사용하여 Amazon EBS 스냅샷을 삭제하면 됩니다.

온프레미스에 배포한 게이트웨이에서 리소스 제거

다음 지침에 따라 온프레미스에 배포한 게이트웨이에서 리소스를 제거할 수 있습니다.

VM에 배포된 Tape Gateway에서 리소스 제거

게이트웨이—가상 테이프 라이브러리 (VTL) 를 삭제할 때는 게이트웨이 삭제 후 추가 정리 단계를 수행합니다. 필요 없으므로 요금을 계속해서 지불할 필요가 없는 리소스를 제거하는 데 이 추가 절차가 도움이 됩니다.

삭제하려는 Tape Gateway가 가상 머신(VM)에 배포된 경우, 다음 작업을 수행하여 리소스를 정리하는 것이 좋습니다.

Important

Tape Gateway를 삭제하기 전에 테이프 가져오기 작업을 모두 취소하고 가져온 테이프를 모두 배출해야 합니다.

Tape Gateway를 삭제한 후에는 Tape Gateway와 관련된 리소스 중 필요하지 않은 리소스를 제거해야 해당 리소스에 대한 요금이 발생하지 않습니다.

Tape Gateway 삭제 시 다음 두 경우 중 하나가 발생할 수 있습니다.

- 테이프 게이트웨이가 연결된 AWS - 테이프 게이트웨이가 연결되어 있는 상태에서 게이트웨이를 삭제하면 게이트웨이와 연결된 *i* 개의 SCSI 대상 (즉, 가상 테이프 드라이브 및 미디어 체인저) 을 더 이상 사용할 수 없게 됩니다. AWS
- 테이프 게이트웨이가 연결되지 않은 경우 AWS- 테이프 게이트웨이가 연결되어 있지 않은 경우 (예: 기본 VM이 꺼져 있거나 네트워크가 다운된 경우) 게이트웨이를 삭제할 수 없습니다. AWS이렇게 하려고 하면 환경을 백업하고 실행한 후에 사용 가능한 *i* SCSI 타겟을 사용하여 온프레미스에서 테이프 게이트웨이를 실행할 수 있습니다. 하지만 테이프 게이트웨이 데이터는, 에 업로드되거나, AWS에서 다운로드되지 않습니다.

삭제하려는 Tape Gateway가 작동하지 않는 경우, 다음 설명과 같이 먼저 이를 비활성화하고 삭제해야 합니다.

- 라이브러리에서 해당 RETRIEVED 상태의 테이프를 삭제하려면 백업 소프트웨어를 사용하여 테이프를 꺼냅니다. 지침은 [테이프 보관](#)을 참조하세요.

Tape Gateway를 비활성화하여 테이프를 삭제한 후 Tape Gateway를 삭제할 수 있습니다. 게이트웨이를 삭제하는 방법에 대한 지침은 [Storage Gateway 콘솔을 사용하여 게이트웨이 삭제](#) 단원을 참조하십시오.

보관한 테이프가 있는 경우, 그 테이프는 그대로 남아 있어 이를 삭제할 때까지는 스토리지 요금을 계속 지불해야 합니다. 아카이브에서 테이프를 삭제하는 방법에 관한 지침은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.

Important

아카이브에 있는 가상 테이프의 최소 90일 스토리지에 대한 요금이 청구됩니다. 90일 미만의 기간 동안 아카이브에 저장한 가상 테이프를 가져오는 경우에는 90일 스토리지에 대해 요금이 청구됩니다.

Amazon EC2 인스턴스에 배포된 게이트웨이에서 리소스 제거

Amazon EC2 인스턴스에 배포한 게이트웨이를 삭제하려면 게이트웨이와 함께 사용된 AWS 리소스, 특히 Amazon EC2 인스턴스, 모든 Amazon EBS 볼륨, 테이프 게이트웨이를 배포한 경우 테이프를 정리하는 것이 좋습니다. 이렇게 하면 원하지 않는 사용 요금이 청구되는 것을 방지할 수 있습니다.

Amazon에 배포된 테이프 게이트웨이에서 리소스 제거 EC2

Tape Gateway를 배포한 경우 다음 작업을 수행하여 게이트웨이를 삭제하고 관련 리소스를 정리하는 것이 좋습니다.

1. Tape Gateway로 가져온 가상 테이프를 모두 삭제합니다. 자세한 내용은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.
2. 테이프 라이브러리에서 가상 테이프를 모두 삭제합니다. 자세한 내용은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.
3. Tape Gateway를 삭제합니다. 자세한 내용은 [Storage Gateway 콘솔을 사용하여 게이트웨이 삭제](#) 단원을 참조하십시오.
4. 모든 Amazon EC2 인스턴스를 종료하고 모든 Amazon EBS 볼륨을 삭제합니다. 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 및 볼륨 정리](#)를 참조하십시오.
5. 보관한 가상 테이프를 모두 삭제합니다. 자세한 내용은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.

⚠ Important

아카이브에 있는 가상 테이프의 최소 90일 스토리지에 대한 요금이 청구됩니다. 90일 미만의 기간 동안 아카이브에 저장한 가상 테이프를 가져오는 경우에는 90일 스토리지에 대해 요금이 청구됩니다.

로컬 콘솔을 사용하여 유지 관리 작업 수행

이 섹션에는 게이트웨이 어플라이언스 로컬 콘솔을 사용하여 유지 관리 작업을 수행하는 방법에 대한 정보를 제공하는 다음 주제가 포함되어 있습니다. 로컬 콘솔은 게이트웨이 어플라이언스를 호스팅하는 가상화 호스트 플랫폼에서 직접 실행됩니다. 온프레미스 게이트웨이의 경우, VMwareHyper-v 또는 Linux KVM 가상화 호스트를 통해 로컬 콘솔에 액세스합니다. Amazon EC2 게이트웨이의 경우를 사용하여 Amazon EC2 인스턴스에 연결하여 콘솔에 액세스합니다SSH. 대부분의 작업은 서로 다른 호스트 플랫폼에서 공통적이지만 몇 가지 차이점도 있습니다.

주제

- [게이트웨이 로컬 콘솔 액세스](#) - Linux 커널 기반 Virtual Machine(KVM), VMware ESXi또는 Microsoft Hyper-V Manager 플랫폼에서 호스팅되는 온프레미스 게이트웨이의 로컬 콘솔에 로그인하는 방법을 알아봅니다.
- [VM 로컬 콘솔에서 작업 수행](#) - 로컬 콘솔을 사용하여 HTTP 프록시 구성, 시스템 리소스 상태 보기 또는 터미널 명령 실행과 같은 온프레미스 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법을 알아봅니다.
- [Amazon EC2 Local Console에서 작업 수행](#) - 로컬 콘솔에 로그인하여 HTTP 프록시 구성, 시스템 리소스 상태 보기 또는 터미널 명령 실행과 같은 Amazon EC2 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법을 알아봅니다.

게이트웨이 로컬 콘솔 액세스

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

주제

- [Linux를 사용하여 Gateway Local Console에 액세스 KVM](#)
- [를 사용하여 Gateway Local Console에 액세스 VMware ESXi](#)
- [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)

Linux를 사용하여 Gateway Local Console에 액세스 KVM

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

를 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면 KVM

1. 다음 명령을 사용하여 현재 에서 사용할 수 VMs 있는 를 나열합니다KVM.

```
# virsh list
```

명령은 각각에 대한 ID , 이름 및 상태 정보가 VMs 포함된 목록을 반환합니다. 게이트웨이 로컬 콘솔을 시작하려는 VMId의 를 기록해 둡니다.

2. 로컬 콘솔에 액세스하려면 다음 명령을 사용합니다.

```
# virsh console Id
```

Replace *Id* 이전 단계에서 기록한 VM의 ID를 사용합니다.

AWS 어플라이언스 게이트웨이 로컬 콘솔은 네트워크 구성 및 기타 설정을 변경하기 위해 로그인 하라는 메시지를 표시합니다.

3. 게이트웨이 로컬 콘솔에 로그인하려면 사용자 이름과 암호를 입력합니다. 자세한 내용은 [Tape Gateway 로컬 콘솔에 로그인](#) .

로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션에서 를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 [가상 머신 로컬 콘솔에서 작업 수행](#) .

를 사용하여 Gateway Local Console에 액세스 VMware ESXi

를 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면 VMware ESXi

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

Note

게이트웨이 VM이 켜져 있으면 애플리케이션 창 왼쪽의 VM 브라우저 패널에 VM 아이콘과 함께 녹색 화살표 아이콘이 나타납니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창 상단의 도구 모음에서 녹색 전원 켜기 아이콘을 선택하여 VM을 켤 수 있습니다.

3. 애플리케이션 창 오른쪽에 있는 기본 정보 패널에서 콘솔 탭을 선택합니다.

잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 네트워크 구성 및 기타 설정을 변경하기 위해 로그인하라는 메시지가 표시됩니다.

Note

콘솔 창에서 커서를 릴리스하려면 Ctrl+Alt를 누릅니다.

4. 게이트웨이 로컬 콘솔에 로그인하려면 사용자 이름과 암호를 입력합니다. 자세한 내용은 [Tape Gateway 로컬 콘솔에 로그인](#).

로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션에서 를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 [가상 머신 로컬 콘솔에서 작업 수행](#).

Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

게이트웨이의 로컬 콘솔에 액세스하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager 애플리케이션 창 왼쪽의 Virtual Machines 패널에서 게이트웨이 어플라이언스 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인하세요.

Note

게이트웨이 VM이 켜져 있는 경우 Running는 애플리케이션 창 왼쪽의 Virtual Machines 패널의 VM 상태 열에 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창 오른쪽에 있는 작업 패널에서 시작을 선택하여 VM을 켤 수 있습니다.

3. 작업 패널에서 연결을 선택합니다.

그러면 Virtual Machine Connection(가상 머신 연결) 창이 표시됩니다. 인증 창이 표시되면 하이퍼바이저 관리자가 제공한 로그인 자격 증명을 입력합니다.

잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 네트워크 구성 및 기타 설정을 변경하기 위해 로그인하라는 메시지가 표시됩니다.

4. 게이트웨이 로컬 콘솔에 로그인하려면 사용자 이름과 암호를 입력합니다. 자세한 내용은 [Tape Gateway 로컬 콘솔에 로그인](#).

로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션에서 를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 [가상 머신 로컬 콘솔에서 작업 수행](#).

VM 로컬 콘솔에서 작업 수행

온프레미스에 배포하는 Tape Gateway 의 경우 가상 머신 호스트 플랫폼에서 액세스하는 게이트웨이 로컬 콘솔을 사용하여 다음 유지 관리 작업을 수행할 수 있습니다. 이러한 작업은 VMware, Microsoft Hyper-V 및 Linux 커널 기반 Virtual Machine(KVM) 하이퍼바이저에 공통적으로 적용됩니다.

주제

- [Tape Gateway 로컬 콘솔에 로그인](#) - 게이트웨이 네트워크 설정을 구성하고 기본 암호를 변경할 수 있는 게이트웨이 로컬 콘솔에 로그인하는 방법에 대해 알아봅니다.
- [온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성](#) - Socket Secure 버전 5(SOCKS5) 프록시 서버를 통해 모든 AWS 엔드포인트 트래픽을 라우팅하도록 Storage Gateway를 구성하는 방법에 대해 알아봅니다.
- [게이트웨이 네트워크 구성](#) - 정적 IP 주소를 사용하거나 DHCP 할당하도록 게이트웨이를 구성하는 방법에 대해 알아봅니다.
- [인터넷에 대한 게이트웨이 연결 테스트](#) - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이와 인터넷 간의 연결을 테스트하는 방법에 대해 알아봅니다.
- [온프레미스 게이트웨이에 대해 로컬 콘솔에서 스토리지 게이트웨이 명령 실행](#) - 라우팅 테이블 저장, 에 연결 등과 같은 추가 작업을 수행할 수 있는 로컬 콘솔 명령을 실행하는 방법에 대해 알아봅니다
AWS Support.
- [게이트웨이 시스템 리소스 상태 조회](#) - 게이트웨이 어플라이언스에서 사용할 수 RAM 있는 가상 CPU 코어, 루트 볼륨 크기 및 를 확인하는 방법에 대해 알아봅니다.

Tape Gateway 로컬 콘솔에 로그인

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

게이트웨이의 로컬 콘솔에 로그인하려면

- 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

AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 게이트웨이 콘솔에 해당하는 번호를 입력한 다음 passwd 명령을 실행하여 기본 암호를 변경하는 것이 좋습니다. 명령을 실행하는 방법에 대한 정보는 [온프레미스 게이트웨이에 대해 로컬 콘솔에서 스토리지 게이트웨이 명령 실행](#) 섹션을 참조하십시오. AWS Storage Gateway 콘솔에서 자체 암호를 설정할 수도 있습니다. 자세한 내용은 [Storage Gateway 콘솔에서 로컬 콘솔 암호 설정](#) 단원을 참조하십시오.

Important

이전 버전의 볼륨 또는 Tape Gateway의 경우 사용자 이름은 sguser이고 암호는 sgpassword입니다. 암호를 재설정하고 게이트웨이가 최신 버전으로 업데이트되면 사용자 이름이 admin으로 변경되지만 암호는 유지됩니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호 설정

로컬 콘솔에 처음 로그인하는 경우, 기본 자격 증명을 사용하여 VM에 로그인합니다. 사용자 이름은 admin이고 암호는 password입니다. 새 게이트웨이를 생성한 즉시 항상 새 암호를 설정하는 것이 좋

습니다. 원하는 경우 이 암호를 로컬 콘솔이 아닌 AWS Storage Gateway 콘솔에서 설정할 수 있습니다. 새 암호를 설정하기 위해 기본 암호를 알 필요는 없습니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호를 설정하려면

1. <https://console.aws.amazon.com/storagegateway/> **집에서** Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 새 암호를 설정할 게이트웨이를 선택합니다.
3. 작업에서 Set Local Console Password(로컬 콘솔 암호 설정)을 선택합니다.
4. 로컬 콘솔 암호 설정 대화 상자에 새 암호를 입력하고 암호를 확인한 후 저장을 선택합니다. 새 암호가 기본 암호를 대체합니다. Storage Gateway는 암호를 저장하지 않지만, 대신 VM에 안전하게 전송합니다.

Note

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

온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성

볼륨 게이트웨이 및 테이프 게이트웨이는 온프레미스 게이트웨이와 간에 소켓 보안 버전 5(SOCKS5) 프록시 구성을 지원합니다 AWS.

Note

지원되는 유일한 프록시 구성은 입니다SOCKS5.

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

다음 절차에서는 Volume Gateway 및 Tape Gateway에 대한 SOCKS 프록시를 구성하는 방법을 보여줍니다.

볼륨 및 Tape Gateway에 대한 SOCKS5 프록시를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi – 자세한 내용은 [섹션을 참조하세요](#) [를 사용하여 Gateway Local Console에 액세스](#) [스 VMware ESXi](#).
 - Microsoft Hyper-V - 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#) [스](#) 섹션을 참조하세요.
 - KVM – 자세한 내용은 [섹션을 참조하세요](#) [Linux를 사용하여 Gateway Local Console에 액세스](#) [KVM](#).
2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 SOCKS 프록시 구성 을 선택 합니다.
 3. AWS Storage Gateway SOCKS 프록시 구성 메뉴에서 해당 숫자를 입력하여 다음 작업 중 하나를 수행합니다.

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

4. VM을 다시 시작하여 HTTP 구성을 적용합니다.

게이트웨이 네트워크 구성

게이트웨이의 기본 네트워크 구성은 동적 호스트 구성 프로토콜(DHCP)입니다. DHCP를 사용하면 게이트웨이에 IP 주소가 자동으로 할당됩니다. 다음 설명과 같이 게이트웨이의 IP를 고정 IP 주소로 수동 지정해야 하는 경우가 있을 수 있습니다.


고정 IP 주소를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi – 자세한 내용은 [섹션을 참조하세요](#) [를 사용하여 Gateway Local Console에 액세스](#) [스 VMware ESXi](#).
 - Microsoft Hyper-V - 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#) [스](#) 섹션을 참조하세요.
 - KVM – 자세한 내용은 [섹션을 참조하세요](#) [Linux를 사용하여 Gateway Local Console에 액세스](#) [KVM](#).
2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. AWS Storage Gateway 네트워크 구성 메뉴에서 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
네트워크 어댑터 설명	<p>해당 숫자를 입력하여 어댑터 설명을 선택합니다.</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

수행할 작업	수행할 작업
	<ul style="list-style-type: none"> DHCP 활성화 상태 <p>고정 IP 주소를 구성하거나 게이트웨이의 기본 어댑터를 설정할 경우 여기에 나열된 어댑터 이름을 사용합니다.</p>
구성 DHCP	<p>해당 숫자를 입력하여 구성을 DHCP선택합니다.</p> <p>를 사용하도록 네트워크 인터페이스를 구성하라는 메시지가 표시됩니다DHCP.</p>

수행할 작업	수행할 작업
게이트웨이에 고정 IP 주소 구성	<p>해당 숫자를 입력하여 고정 IP 구성을 선택합니다.</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 도메인 이름 서비스(DNS) 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 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오.</p> </div> <p>게이트웨이가 둘 이상의 네트워크 인터페이스를 사용하는 경우 DHCP 또는 정적 IP 주소를 사용하도록 활성화된 모든 인터페이스를 설정해야 합니다.</p>

수행할 작업	수행할 작업
	<p>예를 들어 게이트웨이 VM이 로 구성된 두 인터페이스를 사용한다고 가정해 보겠습니다DHCP . 나중에 한 인터페이스를 고정 IP로 설정하면 다른 하나는 비활성화됩니다. 이 경우 인터페이스를 활성화하려면 고정 IP로 설정해야 합니다.</p> <p>처음에 두 인터페이스가 모두 정적 IP 주소를 사용하도록 설정된 다음 게이트웨이가 를 사용하도록 설정한 경우 DHCP두 인터페이스 모두 를 사용합니다DHCP.</p>
<p>게이트웨이의 호스트 이름 구성</p>	<p>해당 숫자를 입력하여 호스트 이름을 구성을 선택합니다.</p> <p>게이트웨이에서 지정한 정적 호스트 이름을 사용할지 또는 DHCP 또는 r 을 통해 자동으로 사용할지 선택하라는 메시지가 표시됩니다DNS.</p> <p>정적 을 선택하면 와 같은 정적 호스트 이름을 제공하라는 메시지가 표시됩니다testgateway.example.com . 를 y 입력하여 구성을 적용합니다.</p> <div data-bbox="829 1230 1507 1640" style="border: 1px solid #00a0e3; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p> Note</p> <p>게이트웨이에 대해 정적 호스트 이름을 구성하는 경우 제공된 호스트 이름이 게이트웨이가 조인되는 도메인에 있는지 확인합니다. 또한 게이트웨이의 IP 주소를 정적 호스트 이름으로 가리키는 A 레코드를 DNS 시스템에 생성해야 합니다.</p> </div>

수행할 작업	수행할 작업
<p>게이트웨이의 모든 네트워크 구성을 로 재 설정 DHCP</p>	<p>해당하는 숫자를 입력하여 모두 로 재설정을 DHCP선택합니다.</p> <p>모든 네트워크 인터페이스는 를 사용하도록 설정됩니다DHCP.</p> <div style="border: 1px solid #f08080; border-radius: 10px; padding: 10px; margin-top: 10px;"> <p>⚠ Important</p> <p>게이트웨이가 이미 활성화된 경우, 설정 이 적용되도록 Storage Gateway 콘솔 에서 게이트웨이를 종료한 후 다시 시작 해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오.</p> </div>
<p>게이트웨이의 기본 경로 어댑터 설정</p>	<p>해당 숫자를 입력하여 기본 어댑터 설정을 선택 합니다.</p> <p>게이트웨이에 사용할 수 있는 어댑터가 표시되고 어댑터 중 하나를 선택하라는 메시지가 표시 됩니다(예: eth0).</p>
<p>게이트웨이 DNS 구성 보기</p>	<p>해당하는 숫자를 입력하여 DNS 구성 보기를 선택합니다.</p> <p>기본 및 보조 DNS 이름 서버의 IP 주소가 표시 됩니다.</p>
<p>라우팅 테이블 조회</p>	<p>해당 숫자를 입력하여 경로 보기를 선택합니다.</p> <p>게이트웨이의 기본 경로가 표시됩니다.</p>

인터넷에 대한 게이트웨이 연결 테스트

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

게이트웨이가 인터넷에 연결되어 있는지 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi – 자세한 내용은 섹션을 참조하세요 [를 사용하여 Gateway Local Console에 액세스](#) [스 VMware ESXi](#).
 - Microsoft Hyper-V - 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#) [스](#) 섹션을 참조하세요.
 - KVM – 자세한 내용은 섹션을 참조하세요 [Linux를 사용하여 Gateway Local Console에 액세스](#) [KVM](#).
2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 연결 테스트를 선택합니다.

게이트웨이가 이미 활성화된 경우 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 다음 단계에 설명된 AWS 리전 대로 엔드포인트 유형 및 를 지정해야 합니다.

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. Storage Gateway 에서 사용할 수 있는 지원되는 AWS 서비스 엔드포인트 AWS 리전 및 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량](#) 을 참조하세요 AWS 일반 참조.

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

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

온프레미스 게이트웨이에 대해 로컬 콘솔에서 스토리지 게이트웨이 명령 실행

Storage Gateway의 VM 로컬 콘솔은 게이트웨이 관련 문제를 구성 및 진단할 수 있는 안전한 환경을 제공합니다. 로컬 콘솔 명령을 사용하여 라우팅 테이블 저장, 에 연결 AWS Support등과 같은 유지 관리 작업을 수행할 수 있습니다.

구성 또는 진단 명령을 실행하려면

- 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 로컬 콘솔에 로그인하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [를 사용하여 Gateway Local Console에 액세스 VMware ESXi](#).
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.
 - KVM 로컬 콘솔에 로그인하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#) [Linux를 사용하여 Gateway Local Console에 액세스 KVM](#).
- AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
- 게이트웨이 콘솔 명령 프롬프트에서 **h**를 입력합니다.

콘솔에는 사용 가능한 명령이 나열된 AVAILABLE COMMANDS 메뉴가 표시됩니다.

Command	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다.

Command	함수
	<p>Note</p> <p>Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 구성을 참조하세요.</p>
ip	<p>라우팅, 디바이스 및 터널을 표시/조작합니다.</p> <p>Note</p> <p>Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 구성을 참조하세요.</p>
iptables	IPv4 패킷 필터링 및 관리 도구 NAT.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결합니다.
passwd	인증 토큰을 업데이트합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.

Command	함수
sslcheck	인증서 발급자와 함께 출력을 반환합니다.
	<div style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p>Note</p> <p>Storage Gateway는 인증서 발급자 검증을 사용하며 ssl 검사를 지원하지 않습니다. 이 명령이 aws-application@amazon.com 이외의 발급자를 반환하면 애플리케이션이 ssl 검사를 수행할 가능성이 높습니다. 이 경우 Storage Gateway 어플라이언스에 대한 ssl 검사를 우회하는 것이 좋습니다.</p> </div>
tcptraceroute	대상에 대한 TCP 트래픽에서 traceroute 출력을 수집합니다.

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

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

게이트웨이 시스템 리소스 상태 조회

게이트웨이가 시작되면 가상 CPU 코어, 루트 볼륨 크기 및 RAM을 확인합니다. 이후 시스템 리소스가 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 게이트웨이의 로컬 콘솔에서 점검 결과를 볼 수 있습니다.

시스템 리소스 점검의 상태를 보려면

- 게이트웨이의 로컬 콘솔에 로그인합니다.
 - VMware ESXi 콘솔에 로그인하는 방법에 대한 자세한 내용은 [섹션을 참조하세요](#)를 사용하여 [Gateway Local Console에 액세스 VMware ESXi](#).
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)을 참조하십시오.

- KVM 로컬 콘솔에 로그인하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [Linux를 사용하여 Gateway Local Console에 액세스 KVM](#).
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

각 리소스는 [OK], [WARNING] 또는 [FAIL]를 표시하여 다음과 같이 리소스의 상태를 나타냅니다.

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

콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

Amazon EC2 Local Console에서 작업 수행

일부 Storage Gateway 유지 관리 작업에서는 Amazon EC2 인스턴스에 배포한 게이트웨이의 게이트웨이 로컬 콘솔에 로그인해야 합니다. Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스의 게이트웨이 로컬 콘솔에 액세스할 수 있습니다. 이 섹션의 주제에서는 게이트웨이 로컬 콘솔에 로그인하고 유지 관리 작업을 수행하는 방법을 설명합니다.

주제

- [Amazon EC2 Gateway Local Console에 로그인](#) - Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스를 게이트웨이 로컬 콘솔에 연결하고 로그인하는 방법에 대해 알아봅니다.

- [HTTP 프록시를 EC2 통해 에 배포된 게이트웨이 라우팅](#) - Socket Secure 버전 5(SOCKS5) 프록시 서버를 통해 모든 AWS 인포인트 트래픽을 Amazon EC2 게이트웨이 인스턴스로 라우팅하도록 Storage Gateway를 구성하는 방법에 대해 알아봅니다.
- [게이트웨이 네트워크 연결 테스트](#) - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이와 다양한 네트워크 리소스 간의 네트워크 연결을 테스트하는 방법을 알아봅니다.
- [게이트웨이 시스템 리소스 상태 조회](#) - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이 어플라이언스에서 사용할 수 RAM 있는 가상 CPU 코어, 루트 볼륨 크기 및 를 확인하는 방법에 대해 알아봅니다.
- [로컬 콘솔에서 Storage Gateway 명령 실행](#) - 라우팅 테이블 저장, 에 연결 등과 같은 추가 작업을 수행할 수 있는 로컬 콘솔 명령을 실행하는 방법에 대해 알아봅니다 AWS Support.

Amazon EC2 Gateway Local Console에 로그인

Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스에 연결할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스에 연결을 참조하세요](#). 이렇게 연결하려면 인스턴스를 시작할 때 지정한 SSH 키 페어가 필요합니다. Amazon EC2 키 페어에 대한 자세한 내용은 [Amazon 사용 설명서의 Amazon EC2 키 페어](#)를 참조하세요. EC2

게이트웨이 로컬 콘솔에 로그인하려면

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

관련 작업	이 주제를 참조하십시오.
게이트웨이의 SOCKS 프록시 구성	HTTP 프록시를 EC2 통해 에 배포된 게이트웨이 라우팅
네트워크 연결 테스트	게이트웨이 네트워크 연결 테스트
Storage Gateway 콘솔 명령 실행	로컬 콘솔에서 Storage Gateway 명령 실행
시스템 리소스 점검 조회	게이트웨이 시스템 리소스 상태 조회 .

게이트웨이를 종료하려면 **0**을 입력합니다.

구성 세션을 종료하려면 **X**을 입력합니다.

HTTP 프록시를 EC2 통해 배포된 게이트웨이 라우팅

Storage Gateway는 Amazon에 배포된 게이트웨이 EC2와 간에 소켓 보안 버전 5(SOCKS5) 프록시의 구성을 지원합니다 AWS.

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

로컬 프록시 서버를 통해 게이트웨이 인터넷 트래픽을 라우팅하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 Gateway Local Console에 로그인](#) 단원을 참조하십시오.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 HTTP 프록시 구성을 선택합니다.
3. AWS 어플라이언스 활성화 HTTP 프록시 구성 메뉴에서 수행하려는 작업에 해당하는 숫자를 입력합니다.
 - HTTP 프록시 구성 - 구성을 완료하려면 호스트 이름과 포트를 제공해야 합니다.
 - 현재 HTTP 프록시 구성 보기 - HTTP 프록시가 구성되지 않은 경우 메시지가 HTTP Proxy not configured 표시됩니다. HTTP 프록시가 구성된 경우 프록시의 호스트 이름과 포트가 표시됩니다.
 - HTTP 프록시 구성 제거 - 메시지가 HTTP Proxy Configuration Removed 표시됩니다.

게이트웨이 네트워크 연결 테스트

게이트웨이의 로컬 콘솔을 사용하여 네트워크 연결을 테스트할 수 있습니다. 이 테스트는 게이트웨이의 네트워크 문제를 해결할 때 유용합니다.

게이트웨이 연결을 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 Gateway Local Console에 로그인](#) 단원을 참조하십시오.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 연결 테스트를 선택합니다.

게이트웨이가 이미 활성화된 경우 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 다음 단계에 설명된 AWS 리전 대로 엔드포인트 유형 및 를 지정해야 합니다.

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. Storage Gateway 에서 사용할 수 있는 지원되는 AWS 서비스 엔드포인트 AWS 리전 및 서비스 엔드포인트 목록은 의 [AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요](#) AWS 일반 참조.

테스트가 진행되면 각 엔드포인트에 [PASSED] 또는 [FAILED]가 표시되며, 다음과 같이 연결 상태를 나타냅니다.

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

게이트웨이 시스템 리소스 상태 조회

게이트웨이가 시작되면 가상 CPU 코어, 루트 볼륨 크기 및 를 확인합니다RAM. 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 Gateway Local Console에 로그인 단원을 참조하십시오](#).
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

각 리소스는 [OK], [WARNING] 또는 [FAIL]를 표시하여 다음과 같이 리소스의 상태를 나타냅니다.

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

콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

로컬 콘솔에서 Storage Gateway 명령 실행

AWS Storage Gateway 콘솔은 게이트웨이 문제를 구성하고 진단할 수 있는 안전한 환경을 제공하는 데 도움이 됩니다. 콘솔 명령을 사용하여 라우팅 테이블 저장 또는 에 연결과 같은 유지 관리 작업을 수행할 수 있습니다 AWS Support.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 [Amazon EC2 Gateway Local Console에 로그인 단원을 참조하십시오](#).
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 h를 입력합니다.

콘솔에는 사용 가능한 명령이 나열된 AVAILABLE COMMANDS 메뉴가 표시됩니다.

Command	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다. <div data-bbox="834 667 1507 932" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p>Note Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다.</p> </div>
ip	라우팅, 디바이스 및 터널을 표시/조작합니다. <div data-bbox="834 1052 1507 1316" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"> <p>Note Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다.</p> </div>
iptables	IPv4 패킷 필터링 및 관리 도구NAT.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.

Command	함수
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
sslcheck	네트워크 문제 해결의 SSL 유효성을 확인합니다.
tcptracert	대상에 대한 TCP 트래픽에서 traceroute 출력을 수집합니다.

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

명령에 대해 알아보려면 명령 이름을 입력하고 -h 옵션을 입력하십시오(예: `sslcheck -h`).

Tape Gateway의 성능 및 최적화

이 섹션에서는 Storage Gateway 성능에 대해 설명합니다.

주제

- [Tape Gateway의 성능 지침](#)
- [게이트웨이 성능 최적화](#)

Tape Gateway의 성능 지침

이 섹션에서는 Tape Gateway VM에 하드웨어를 프로비저닝하기 위한 구성 지침을 알아봅니다. 표에 나열된 Amazon EC2 인스턴스 크기 및 유형은 예제이며 참조용으로 제공됩니다.

구성	쓰기 처리량 Gbps	캐시에서 읽기 처리량 Gbps	Amazon Web Services 클라우드에서 읽기 처리량 (GBps)
호스트 플랫폼: Amazon EC2 인스턴스 - c5.4xlarge CPU: 16vCPU RAM: 32GB 루트 디스크: 80GB, io1SSD, 4,000 IOPS 캐시 디스크: 스트라이프RAID(2 x 500GB, io1EBS, 25SSD,000 IOPs) 버퍼 디스크 업로드: 450GB, io1SSD, 2000 IOPs 클라우드 측 네트워크 대역폭: 10Gbps	2.3	4.0	2.2
호스트 플랫폼: Storage Gateway 하드웨어 어플라이언스	2.3	8.8	3.8

구성	쓰기 처리량 Gbps	캐시에서 읽기 처리량 Gbps	Amazon Web Services 클라우드에서 읽기 처리량 (GBps)
캐시 디스크: 2.5TB 업로드 버퍼 디스크: 2TB 클라우드 측 네트워크 대역폭: 10Gbps			
호스트 플랫폼: Amazon EC2instance— c5d.9xlarge CPU: 36vCPU RAM: 72GB 루트 디스크: 80GB, io1SSD, 4,000 IOPS 캐시 디스크: 900GB NVMe 디스크 버퍼 디스크 업로드: 900GB NVMe 디스크 클라우드 측 네트워크 대역폭: 10Gbps	5.2	11.6	5.2

구성	쓰기 처리량 Gbps	캐시에서 읽기 처리량 Gbps	Amazon Web Services 클라우드에서 읽기 처리량 (GBps)
호스트 플랫폼: Amazon EC2instance— c5d.metal CPU: 96 vCPU RAM: 192GB 루트 디스크: 80GB, io1SSD, 4,000 IOPS 캐시 디스크: 스트라이프RAID(2 x 900GB NVMe 디스크) 버퍼 디스크 업로드: 900GB NVMe 디스크 클라우드 측 네트워크 대역폭: 10Gbps	5.2	11.6	7.2

Note

해당 성능은 1개의 1MB 블록 크기와 10개의 테이프 드라이브를 동시에 사용한 경우입니다. 위 표의 EC2 구성은 리소스가 유사한 자체 물리적 서버에서 얻을 수 있는 성능만 나타내기 위한 것입니다. 예를 들어 스트라이프를 사용하는 EC2 구성은 의 게이트웨이에서 일반적으로 지원되지 않는 특수 메커니즘을 통해 RAID 수행되었습니다EC2. 비슷한 성능을 얻으려면 대신 게이트웨이를 실행하는 온프레미스 서버에 연결된 하드웨어 RAID 컨트롤러를 사용해야 합니다. 성능은 호스트 플랫폼 구성 및 네트워크 대역폭에 따라 달라질 수 있습니다.

Tape Gateway의 쓰기 및 읽기 처리량 성능을 향상시키려면 [iSCSI 설정 최적화](#), [테이프 드라이브에 더 큰 블록 크기 사용](#), [백업 소프트웨어의 가상 테이프 드라이브 성능 최적화](#) 섹션을 참조하세요.

게이트웨이 성능 최적화

권장되는 게이트웨이 서버 구성

게이트웨이의 성능을 극대화하기 위해 Storage Gateway는 게이트웨이 호스트 서버에 다음과 같은 게이트웨이 구성을 권장합니다.

- 최소 64개의 전용 물리적 CPU 코어
- Tape Gateway 의 경우 하드웨어는 다음과 같은 양의 를 사용해야 합니다RAM.
 - 캐시 크기가 최대 16GiB 이상 예약됨 RAM TiB
 - 캐시 크기가 16TiBGiB TiB 이상 예약됨 RAM
 - 캐시 크기가 32TiBGiBTiB RAM

Note

최적의 게이트웨이 성능을 위해 최소 32GiB의 를 프로비저닝해야 합니다RAM.

- 디스크 1 - 다음과 같이 게이트웨이 캐시로 사용됨
 - 로 구성된 스트라이프RAID(독립 디스크의 중복 배열). NVMe SSDs
- 디스크 2 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
 - 로 RAID 구성된 스트라이프NVMeSSDs.
- 디스크 3 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
 - 로 RAID 구성된 스트라이프NVMeSSDs.
- VM 네트워크 1에 구성된 네트워크 어댑터 1:
 - VM 네트워크 1을 사용하고 수집에 사용할 VMXnet3 (10Gbps)를 추가합니다.
- VM 네트워크 2에 구성된 네트워크 어댑터 2:
 - VM 네트워크 2를 사용하고 에 연결하는 데 사용할 VMXnet3 (10Gbps)를 추가합니다 AWS.

게이트웨이에 리소스 추가

다음 병목 현상은 Tape Gateway 의 성능을 이론적인 최대 지속 처리량(AWS 클라우드로의 대역폭) 미만으로 감소시킬 수 있습니다.

- CPU 코어 수

- 캐시/업로드 버퍼 디스크 처리량
- 총 RAM 금액
- 에 대한 네트워크 대역폭 AWS
- 이니시에이터에서 게이트웨이까지의 네트워크 대역폭

이 섹션에서는 게이트웨이 성능을 최적화하기 위해 수행할 수 있는 단계에 대해 다룹니다. 이 지침은 게이트웨이 또는 애플리케이션 서버에 리소스를 추가하는 것을 전제로 합니다.

다음 중 하나 이상의 방법으로 게이트웨이에 리소스를 추가하여 게이트웨이 성능을 최적화할 수 있습니다.

고성능 디스크 사용

캐시 및 업로드 버퍼 디스크 처리량으로 인해 게이트웨이의 업로드 및 다운로드 성능이 제한될 수 있습니다. 게이트웨이 성능이 예상보다 현저히 낮은 경우 다음과 같이 캐시 및 업로드 버퍼 디스크 처리량을 개선하는 것이 좋습니다.

- RAID 10 RAID과 같은 줄무늬를 사용하여 디스크 처리량을 개선하는 것이 가장 좋습니다 RAID.

Note

RAID (독립 디스크의 중복 배열) 또는 RAID 10과 같은 디스크 스트라이프 RAID 구성은 데이터 본문을 블록으로 나누고 데이터 블록을 여러 스토리지 장치에 분산하는 프로세스입니다. 사용하는 RAID 수준은 달성할 수 있는 정확한 속도와 내결함성에 영향을 미칩니다. 여러 디스크에서 IO 워크로드를 제거하면 RAID 디바이스의 전체 처리량이 단일 멤버 디스크보다 훨씬 높습니다.

- 직접 연결된 고성능 디스크 사용

게이트웨이 성능을 최적화하기 위해 솔리드 스테이트 드라이브(SSDs) 및 NVMe 컨트롤러와 같은 고성능 디스크를 추가할 수 있습니다. Microsoft Hyper-V 대신 스토리지 영역 네트워크(SAN)에서 직접 가상 디스크를 VM에 연결할 수도 있습니다 NTFS. 디스크 성능이 향상되면 일반적으로 처리량이 향상되고 초당 입/출력 작업이 늘어납니다(IOPS).

처리량을 측정하려면 Samples Amazon CloudWatch 통계와 함께 ReadBytes 및 WriteBytes 지표를 사용합니다. 예를 들어 샘플 기간 Samples 5분에 대한 지표 통계를 ReadBytes 300초로 나누면 가 제공됩니다 IOPS. 일반적으로 게이트웨이에 대해 이러한 지표를 검토할 때 디스크 관련 병목 현상을 나타내는 낮은 처리량과 낮은 IOPS 추세를 찾습니다. 게이트웨이 지표에 대한 자세한 내용은 [Tape Gateway와 간의 성능 측정 AWS](#) 섹션을 참조하세요.

Note

CloudWatch 모든 게이트웨이에서 지표를 사용할 수 있는 것은 아닙니다. 게이트웨이 지표에 대한 자세한 내용은 [Storage Gateway 모니터링](#) 섹션을 참조하세요.

업로드 버퍼 디스크 추가

쓰기 처리량을 높이려면 업로드 버퍼 디스크를 두 개 이상 추가하십시오. 데이터가 게이트웨이에 기록되면 업로드 버퍼 디스크에 로컬로 기록되고 저장됩니다. 그런 다음 저장된 로컬 데이터를 디스크에서 비동기적으로 읽고 처리한 뒤 AWS에 업로드합니다. 업로드 버퍼 디스크를 추가하면 각 개별 디스크에서 수행되는 동시 I/O 작업의 양을 줄일 수 있습니다. 이로 인해 게이트웨이에 대한 쓰기 처리량이 증가할 수 있습니다.

별도의 물리적 디스크로 게이트웨이 가상 디스크 지원

게이트웨이 디스크를 프로비저닝할 때는 동일한 기본 물리적 스토리지 디스크를 사용하는 업로드 버퍼 및 캐시 스토리지에 로컬 디스크를 프로비저닝하지 않는 것이 좋습니다. 예를 들어 VMware ESXi의 경우 기본 물리적 스토리지 리소스는 데이터 스토어로 표시됩니다. 게이트웨이 VM을 배포할 경우, VM 파일을 저장할 데이터 스토어를 선택합니다. 가상 디스크를 프로비저닝할 때(예: 업로드 버퍼 용도) 가상 디스크를 VM과 동일한 데이터 스토어 또는 다른 데이터 스토어에 저장할 수 있습니다.

데이터 스토어가 두 개 이상인 경우 생성하는 로컬 스토리지의 유형별로 하나씩 데이터 스토어를 선택하는 것이 좋습니다. 기본 물리적 디스크 하나로만 지원되는 데이터 스토어는 성능 저하로 이어질 수 있습니다. 게이트웨이 설정에서 이러한 디스크를 사용하여 캐시 스토리지와 업로드 버퍼를 모두 지원하는 경우를 예로 들 수 있습니다. 마찬가지로 1 또는 RAID RAID6과 같이 성능이 떨어지는 RAID 구성으로 뒷받침되는 데이터 스토어는 성능이 저하될 수 있습니다.

게이트웨이 호스트에 CPU 리소스 추가

게이트웨이 호스트 서버의 최소 요구 사항은 가상 프로세서 4개입니다. 게이트웨이 성능을 최적화하려면 게이트웨이 VM에 할당된 각 가상 프로세서가 전용 CPU 코어로 지원되는지 확인합니다. 또한 호스트 서버의 CPUs를 과도하게 구독하지 않는지 확인합니다.

게이트웨이 호스트 서버에 CPUs를 추가하면 게이트웨이의 처리 기능이 향상됩니다. 이렇게 하면 게이트웨이가 애플리케이션의 데이터를 로컬 스토리지에 저장하고 이 데이터를 Amazon S3로 업로드하는 작업을 병렬로 처리할 수 있습니다. CPUs 또한 호스트를 다른 와 공유할 때 게이트웨이가 충분한 CPU 리소스를 얻을 수 있도록 합니다. 충분한 CPU 리소스를 제공하면 일반적으로 처리량이 향상됩니다.

게이트웨이와 AWS 클라우드 간 대역폭 늘리기

대역폭을 에서 로 늘리 AWS 면 게이트웨이로의 최대 데이터 수신률이 증가하고 AWS 클라우드로 송신됩니다. 이렇게 하면 느린 디스크나 낮은 게이트웨이-이니시에이터 연결 대역폭과 같은 다른 요인보다 네트워크 속도가 게이트웨이 구성의 제한 요소인 경우 게이트웨이 성능을 개선할 수 있습니다.

송수신 네트워크 대역폭은 지속적인 워크로드 동안 Tape Gateway의 이론적인 최대 평균 성능을 AWS 정의합니다.

- Tape Gateway에 장기간 데이터를 쓸 수 있는 평균 속도는 AWS로의 업로드 대역폭을 초과하지 않습니다.
- Tape Gateway에서 장기간 데이터를 읽을 수 있는 평균 속도는 에 대한 다운로드 대역폭을 초과하지 않습니다 AWS.

Note

캐시/업로드 버퍼 디스크 처리량, CPU 코어 수, 총RAM량 또는 이니시에이터와 게이트웨이 간의 대역폭과 같은 기타 제한 요인으로 인해 관찰된 게이트웨이 성능이 네트워크 대역폭보다 낮을 수 있습니다. 또한, 게이트웨이의 정상 작동에는 데이터를 보호하기 위한 여러 가지 조치가 포함되므로 관찰된 성능이 네트워크 대역폭보다 낮을 수 있습니다.

iSCSI 설정 최적화

I/O 성능을 높이기 위해 iSCSI 이니시에이터의 iSCSI 설정을 최적화할 수 있습니다.

MaxReceiveDataSegmentLength 및 FirstBurstLength에는 256 KiB를 선택하고, MaxBurstLength에는 1MiB를 선택하는 것이 좋습니다. iSCSI 설정 구성에 대한 자세한 내용은 섹션을 참조하세요 [iSCSI 설정 사용자 지정](#).

Note

이러한 권장 설정을 통해 전반적으로 더 나은 성능을 실현할 수 있습니다. 그러나 성능을 최적화하는 데 필요한 특정 iSCSI 설정은 사용하는 백업 소프트웨어에 따라 달라집니다. 자세한 내용은 백업 소프트웨어 설명서를 참조하십시오.

테이프 드라이브에 더 큰 블록 크기 사용

Tape Gateway의 경우 테이프 드라이브의 기본 블록 크기는 64KB입니다. 하지만 블록 크기를 최대 1MB까지 늘려 I/O 성능을 향상시킬 수 있습니다.

선택하는 블록 크기는 백업 소프트웨어가 지원하는 최대 블록 크기에 따라 달라집니다. 백업 소프트웨어에서 테이프 드라이브의 블록 크기를 가능한 한 크게 설정하는 것이 좋습니다. 그러나 이 블록 크기는 게이트웨이가 지원하는 최대 크기인 1MB를 초과해서는 안 됩니다.

Tape Gateway는 백업 소프트웨어에 설정된 크기와 자동으로 일치하도록 가상 테이프 드라이브의 블록 크기를 협상합니다. 백업 소프트웨어에서 블록 크기를 늘릴 때는 설정을 확인하여 호스트 이니시에이터가 새 블록 크기를 지원하는지도 확인하는 것이 좋습니다. 자세한 내용은 사용 중인 백업 소프트웨어의 설명서를 참조하세요. 특정 게이트웨이 성능 지침에 대한 자세한 내용은 [Tape Gateway의 성능 및 최적화](#) 섹션을 참조하세요.

백업 소프트웨어의 가상 테이프 드라이브 성능 최적화

백업 소프트웨어는 Tape Gateway에 있는 최대 10개의 가상 테이프 드라이브에 데이터를 동시에 백업할 수 있습니다. Tape Gateway에서 최소 4개의 가상 테이프 드라이브를 동시에 사용하도록 백업 소프트웨어의 백업 작업을 구성하는 것이 좋습니다. 백업 소프트웨어가 동시에 둘 이상의 가상 테이프에 데이터를 백업하면 쓰기 처리량을 높일 수 있습니다.

일반적으로 더 많은 가상 테이프에서 동시에 작업(읽기 또는 쓰기)을 수행하면 최대 처리량을 높일 수 있습니다. 테이프 드라이브를 더 많이 사용하면 게이트웨이에서 더 많은 요청을 동시에 처리할 수 있어 성능이 향상될 수 있습니다.

애플리케이션 환경에 리소스 추가

애플리케이션 서버와 게이트웨이 간의 대역폭 늘리기

iSCSI 이니시에이터와 게이트웨이 간의 연결로 인해 업로드 및 다운로드 성능이 제한될 수 있습니다. 게이트웨이가 예상보다 훨씬 성능이 나쁘고 이미 CPU 코어 수와 디스크 처리량을 개선한 경우 다음을 고려하세요.

- 네트워크 케이블을 업그레이드하여 이니시에이터와 게이트웨이 간에 더 높은 대역폭을 확보합니다.
- 가능한 한 많은 테이프 드라이브를 동시에 사용합니다. iSCSI는 동일한 대상에 대한 여러 요청 대기열을 지원하지 않습니다. 즉, 사용하는 테이프 드라이브가 많을수록 게이트웨이가 동시에 서비스할 수 있는 요청이 더 많습니다. 이렇게 하면 게이트웨이와 이니시에이터 간의 대역폭을 최대한 활용하여 게이트웨이의 예상 처리량을 늘릴 수 있습니다.

게이트웨이 성능을 최적화하려면 애플리케이션과 게이트웨이 간의 네트워크 대역폭이 애플리케이션 요구 사항을 충족할 수 있는지 확인하세요. 게이트웨이의 ReadBytes 및 WriteBytes 지표를 사용하여 총 데이터 처리량을 측정할 수 있습니다. 이러한 지표에 대한 자세한 내용은 [Tape Gateway와 간의 성능 측정 AWS](#) 섹션을 참조하세요.

애플리케이션의 경우 측정된 처리량을 원하는 처리량과 비교합니다. 측정된 처리량이 원하는 처리량보다 적을 경우, 애플리케이션과 게이트웨이 간의 대역폭을 늘리면 네트워크 병목 현상이 발생하는 경우 성능을 개선할 수 있습니다. 마찬가지로, 직접 연결되지 않은 VM과 로컬 디스크 간의 대역폭을 늘릴 수 있습니다.

애플리케이션 환경에 CPU 리소스 추가

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

보안 in AWS Storage Gateway

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 가장 보안에 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. [공동 책임 모델](#)은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 Amazon Web Services Cloud에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. 는 안전하게 사용할 수 있는 서비스 AWS 도 제공합니다. 서드 파티 감사자는 [AWS 규정 준수 프로그램](#) 프로그램의 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS Storage Gateway 에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 [AWS 규정 준수 프로그램의 범위 내 서비스](#) .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터의 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Storage Gateway를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Storage Gateway를 구성하는 방법을 보여줍니다. 또한 Storage Gateway 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법도 알아봅니다.

주제

- [in AWS Storage Gateway의 데이터 보호](#)
- [AWS Storage Gateway의 ID 및 액세스 관리](#)
- [AWS Storage Gateway의 규정 준수 검증](#)
- [Resilience in AWS Storage Gateway](#)
- [AWS Storage Gateway의 인프라 보안](#)
- [AWS 보안 베스트 프랙티스](#)
- [로그인 및 모니터링 AWS Storage Gateway](#)

in AWS Storage Gateway의 데이터 보호

AWS [공동 책임 모델](#) AWS Storage Gateway 의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든 를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프

라에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스의 보안 구성과 관리 작업에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 [데이터 프라이버시 섹션을 FAQ](#) 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 [AWS 책임 공유 모델 및 GDPR](#) 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management ()를 사용하여 개별 사용자를 설정하는 것이 좋습니다IAM. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다단계 인증(MFA)을 사용합니다.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2가 필요하며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 추적 작업을 참조](#)하세요.
- AWS 암호화 솔루션과 내의 모든 기본 보안 제어를 사용합니다 AWS 서비스.
- Amazon S3에 저장된 민감한 데이터를 검색하고 보호하는 데 도움이 되는 Amazon Macie와 같은 고급 관리형 보안 서비스를 사용하세요.
- 명령줄 인터페이스 또는 FIPS 를 AWS 통해 액세스할 때 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 API사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 [연방 정보 처리 표준\(FIPS\) 140-3](#)을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 양식 필드에 입력하지 않는 것이 좋습니다. 여기에는 콘솔, 또는 를 사용하여 Storage Gateway 또는 기타 AWS 서비스로 작업하는 경우가 포함됩니다API AWS CLI AWS SDKs. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버에 URL를 제공하는 경우 해당 서버에 대한 요청을 검증URL하기 위해 에 보안 인증 정보를 포함하지 않는 것이 좋습니다.

데이터 암호화 사용 AWS KMS

Storage Gateway는SSL/TLS(보안 소켓 계층/전송 계층 보안) 를 사용하여 게이트웨이 어플라이언스와 스토리지 간에 전송되는 데이터를 암호화합니다. AWS 기본적으로 Storage Gateway는 Amazon S3 관리형 암호화 키 (SSE-S3) 를 사용하여 Amazon S3에 저장하는 모든 데이터를 서버 측에서 암호화합니다. Storage API Gateway를 사용하여 AWS Key Management Service (SSE-KMS) 키를 사용한 서버 측 암호화를 사용하여 클라우드에 저장된 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다.

⚠ Important

서버 측 암호화에 AWS KMS 키를 사용할 때는 대칭 키를 선택해야 합니다. Storage Gateway에서는 비대칭 키가 지원되지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 [대칭 및 비대칭 키 사용](#)을 참조하세요.

파일 공유 암호화

파일 공유의 경우 -를 사용하여 AWS KMS—관리 키로 객체를 암호화하도록 게이트웨이를 구성할 수 있습니다. SSE KMS Storage API Gateway를 사용하여 파일 공유에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 AWS Storage Gateway API참조의 [CreateNFSFile 공유](#)를 참조하십시오.

볼륨 암호화

캐싱 및 저장된 볼륨의 경우 Storage Gateway를 사용하여 AWS KMS관리 키로 클라우드에 저장된 볼륨 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다. API 관리 키 중 하나를 키로 지정할 수 있습니다. KMS 볼륨을 암호화하는 데 사용하는 키는 볼륨이 생성된 후에는 변경할 수 없습니다. Storage API Gateway를 사용하여 캐시되거나 저장된 볼륨에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 참조서 [CreateCachediSCSIVolume](#) 또는 [CreateStorediSCSIVolume](#)을 AWS Storage Gateway API 참조하십시오.

테이프 암호화

가상 테이프의 경우 Storage Gateway를 사용하여 AWS KMS관리 키로 클라우드에 저장된 테이프 데이터를 암호화하도록 게이트웨이를 구성할 수 있습니다. API 관리 키 중 하나를 키로 지정할 수 있습니다. KMS 테이프 데이터를 암호화하는 데 사용하는 키는 테이프가 생성된 후에는 변경할 수 없습니다. Storage API Gateway를 사용하여 가상 테이프에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은 AWS Storage Gateway API참조를 참조하십시오 [CreateTapes](#).

를 AWS KMS 사용하여 데이터를 암호화할 때는 다음 사항에 유의하십시오.

- 데이터는 클라우드에 암호화되어 저장됩니다. 즉, 데이터는 Amazon S3에서 암호화됩니다.
- IAM사용자는 AWS KMS API 작업을 호출하는 데 필요한 권한을 가지고 있어야 합니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 IAM [정책 사용](#)을 참조하십시오. AWS KMS
- AWS AWS KMS 키를 삭제 또는 비활성화하거나 권한 부여 토큰을 취소하면 볼륨 또는 테이프의 데이터에 액세스할 수 없습니다. 자세한 내용은 개발자 안내서의 [KMS키 삭제](#)를 참조하십시오. AWS Key Management Service

- KMS 암호화된 볼륨에서 스냅샷을 생성하면 스냅샷이 암호화됩니다. 스냅샷은 볼륨의 키를 상속합니다. KMS
- 암호화된 스냅샷에서 새 볼륨을 생성하는 경우 볼륨이 KMS 암호화됩니다. 새 볼륨에 다른 KMS 키를 지정할 수 있습니다.

Note

Storage Gateway는 암호화된 볼륨 또는 암호화된 스냅샷의 복구 지점에서 KMS 암호화되지 않은 볼륨을 생성하는 것을 지원하지 않습니다. KMS

[에 대한 자세한 내용은 AWS KMS 무엇입니까를 참조하십시오. AWS Key Management Service](#)

AWS Storage Gateway의 ID 및 액세스 관리

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 되는 AWS 서비스입니다. IAM 관리자는 리소스를 사용할 AWS SGW 수 있는 인증(로그인) 및 권한 부여(권한 보유) 대상을 제어합니다. IAM 는 추가 비용 없이 사용할 수 있는 AWS 서비스입니다.

주제

- [고객](#)
- [ID를 통한 인증](#)
- [정책을 사용한 액세스 관리](#)
- [AWS Storage Gateway의 작동 방식 IAM](#)
- [Storage Gateway에 대한 자격 증명 기반 정책 예제](#)
- [AWS Storage Gateway ID 및 액세스 문제 해결](#)

고객

AWS Identity and Access Management (IAM) 사용 방법은 에서 수행하는 작업에 따라 다릅니다 AWS SGW.

서비스 사용자 - 서비스를 사용하여 AWS SGW 작업을 수행하는 경우 관리자는 필요한 자격 증명과 권한을 제공합니다. 더 많은 AWS SGW 기능을 사용하여 작업을 수행하면 추가 권한이 필요할 수 있습니다

다. 액세스 권한 관리 방식을 이해하면 적절한 권한을 관리자에게 요청할 수 있습니다. 에서 기능에 액세스할 수 없는 경우 섹션을 [AWS SGW참조하세요](#) [AWS Storage Gateway ID 및 액세스 문제 해결](#).

서비스 관리자 - 회사에서 리소스를 담당하는 AWS SGW 경우 에 대한 전체 액세스 권한이 있을 수 있습니다 AWS SGW. 서비스 사용자가 액세스해야 하는 기능과 리소스를 결정하는 AWS SGW 것은 사용자의 작업입니다. 그런 다음 IAM 관리자에게 요청을 제출하여 서비스 사용자의 권한을 변경해야 합니다. 이 페이지의 정보를 검토하여 의 기본 개념을 이해합니다IAM. 회사에서 IAM를 사용하는 방법에 대한 자세한 내용은 섹션을 [AWS SGW참조하세요](#) [AWS Storage Gateway의 작동 방식 IAM](#).

IAM 관리자 - IAM 관리자인 경우 에 대한 액세스를 관리하기 위한 정책을 작성하는 방법에 대한 세부 정보를 알고 싶을 수 있습니다 AWS SGW. 에서 사용할 수 있는 자격 증명 기반 정책 예제 AWS SGW 를 보려면 섹션을 IAM참조하세요 [Storage Gateway에 대한 자격 증명 기반 정책 예제](#).

ID를 통한 인증

인증은 자격 증명 AWS 으로 에 로그인하는 방법입니다. 로 AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증(에 로그인 AWS)되어야 합니다.

자격 증명 소스를 통해 제공된 자격 증명을 사용하여 에 페더레이션 자격 증명 AWS 으로 로그인할 수 있습니다. AWS IAM Identity Center (IAM Identity Center) 사용자, 회사의 Single Sign-On 인증 및 Google 또는 Facebook 자격 증명은 페더레이션 자격 증명의 예입니다. 페더레이션 자격 증명으로 로그인하면 관리자가 이전에 IAM 역할을 사용하여 자격 증명 페더레이션을 설정했습니다. 페더레이션을 사용하여 AWS 에 액세스하면 간접적으로 역할을 수임하게 됩니다.

사용자 유형에 따라 AWS Management Console 또는 AWS 액세스 포털에 로그인할 수 있습니다. 에 로그인하는 방법에 대한 자세한 내용은 AWS 로그인 사용 설명서의 [에 로그인하는 방법을 AWS 계정](#) AWS참조하세요.

AWS 프로그래밍 방식으로 에 액세스하는 경우는 소프트웨어 개발 키트(SDK)와 명령줄 인터페이스(CLI)를 AWS 제공하여 자격 증명을 사용하여 요청에 암호화 방식으로 서명합니다. AWS 도구를 사용하지 않는 경우 직접 요청에 서명해야 합니다. 권장 방법을 사용하여 직접 요청에 서명하는 방법에 대한 자세한 내용은 IAM 사용 설명서 의 [AWS API 요청에 대한 서명 버전 4](#)를 참조하세요.

사용하는 인증 방법에 상관없이 추가 보안 정보를 제공해야 할 수도 있습니다. 예를 들어 다중 인증(MFA)을 사용하여 계정의 보안을 강화하는 것이 AWS 좋습니다. 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [다단계 인증](#) 및 사용 설명서의 [AWS 다단계 인증을 IAM](#) 참조하세요IAM.

AWS 계정 루트 사용자

를 생성하면 계정의 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 이 자격 증명을 AWS 계정 루트 사용자라고 하며 계정을 생성하는

데 사용한 이메일 주소와 암호로 로그인하여 액세스합니다. 일상적인 작업에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 보안 인증 정보를 보호하고 루트 사용자만 수행할 수 있는 작업을 수행하는 데 사용합니다. 루트 사용자로 로그인해야 하는 작업의 전체 목록은 IAM 사용 설명서의 [루트 사용자 보안 인증이 필요한 작업을](#) 참조하세요.

페더레이션 자격 증명

가장 좋은 방법은 관리자 액세스가 필요한 사용자를 포함한 인간 사용자가 ID 공급자와의 페더레이션을 사용하여 임시 자격 증명을 사용하여 AWS 서비스에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 사용자 디렉터리, 웹 자격 증명 공급자, , AWS Directory Service Identity Center 디렉터리 또는 자격 증명 소스를 통해 제공된 자격 증명을 사용하여 AWS 서비스에 액세스하는 모든 사용자의 사용자입니다. 페더레이션 자격 증명 AWS 계정에 액세스하면 역할을 수임하고 역할은 임시 자격 증명을 제공합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center(을)를 사용하는 것이 좋습니다. IAM Identity Center에서 사용자 및 그룹을 생성하거나 및 AWS 계정 애플리케이션에서 사용할 수 있도록 자체 자격 증명 소스의 사용자 및 그룹 집합에 연결하고 동기화할 수 있습니다. IAM Identity Center에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [IAM Identity Center란 무엇입니까?](#)를 참조하세요.

IAM 사용자 및 그룹

[IAM 사용자](#)는 한 사람 또는 애플리케이션에 대한 특정 권한이 AWS 계정 있는 내 자격 증명입니다. 가능한 경우 암호 및 액세스 키와 같은 장기 보안 인증 정보가 있는 IAM 사용자를 생성하는 대신 임시 보안 인증 정보를 사용하는 것이 좋습니다. 그러나 IAM 사용자와 장기 보안 인증이 필요한 특정 사용 사례가 있는 경우 액세스 키를 교체하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [장기 보안 인증이 필요한 사용 사례에 대한 액세스 키 정기적으로 교체](#)를 참조하세요.

[IAM 그룹](#)은 IAM 사용자 컬렉션을 지정하는 자격 증명입니다. 사용자는 그룹으로 로그인할 수 없습니다. 그룹을 사용하여 여러 사용자의 권한을 한 번에 지정할 수 있습니다. 그룹을 사용하면 대규모 사용자 집합의 권한을 더 쉽게 관리할 수 있습니다. 예를 들어 라는 이름의 그룹을 지정IAMAdmins하고 해당 그룹에 IAM 리소스를 관리할 수 있는 권한을 부여할 수 있습니다.

사용자는 역할과 다릅니다. 사용자는 한 사람 또는 애플리케이션과 고유하게 연결되지만, 역할은 해당 역할이 필요한 사람이라면 누구나 수임할 수 있습니다. 사용자는 영구적인 장기 보안 인증 정보를 가지고 있지만, 역할은 임시 보안 인증만 제공합니다. 자세한 내용은 IAM 사용 설명서의 [IAM 사용자 사용 사례](#)를 참조하세요.

IAM 역할

[IAM 역할](#)은 특정 권한이 AWS 계정 있는 내 자격 증명입니다. IAM 사용자와 비슷하지만 특정 사람과는 연결되지 않습니다. 에서 IAM 역할을 일시적으로 말 AWS Management Console으려면 [사용자에서 IAM 역할\(콘솔\)로 전환할 수 있습니다](#). 또는 AWS API 작업을 호출 AWS CLI 하거나 사용자 지정 를 사용하여 역할을 수입할 수 있습니다URL. 역할 사용 방법에 대한 자세한 내용은 IAM 사용 설명서의 [역할 수입 방법을](#) 참조하세요.

IAM 임시 자격 증명이 있는 역할은 다음과 같은 상황에서 유용합니다.

- 페더레이션 사용자 액세스 - 페더레이션 ID에 권한을 부여하려면 역할을 생성하고 해당 역할의 권한을 정의합니다. 페더레이션 ID가 인증되면 역할이 연결되고 역할에 정의된 권한이 부여됩니다. 페더레이션 역할에 대한 자세한 내용은 IAM 사용 설명서의 [타사 자격 증명 공급자의 역할 생성을](#) 참조하세요. IAM Identity Center를 사용하는 경우 권한 세트를 구성합니다. 인증 후 자격 증명이 액세스할 수 있는 항목을 제어하기 위해 IAM Identity Center는 권한 세트를 의 역할과 상호 연관시킵니다IAM. 권한 세트에 대한 자세한 내용은 AWS IAM Identity Center 사용 설명서의 [권한 세트](#)를 참조하세요.
- 임시 IAM 사용자 권한 - IAM 사용자 또는 역할은 특정 작업에 대해 일시적으로 다른 권한을 받을 IAM 수 있습니다.
- 교차 계정 액세스 - IAM 역할을 사용하여 다른 계정의 누군가(신뢰할 수 있는 보안 주체)가 계정의 리소스에 액세스하도록 허용할 수 있습니다. 역할은 계정 간 액세스를 부여하는 기본적인 방법입니다. 그러나 일부 에서는 정책을 리소스에 직접 연결할 AWS 서비스수 있습니다(역할을 프록시로 사용하는 대신). 교차 계정 액세스에 대한 역할과 리소스 기반 정책의 차이점을 알아보려면 IAM 사용 설명서의 [에서 교차 계정 리소스 액세스를 IAM](#) 참조하세요.
- 교차 서비스 액세스 - 일부 는 다른 에서 기능을 AWS 서비스 사용합니다 AWS 서비스. 예를 들어 서비스에서 호출할 때 해당 서비스가 Amazon에서 애플리케이션을 실행EC2하거나 Amazon S3에 객체를 저장하는 것이 일반적입니다. 서비스는직접적으로 호출하는 보안 주체의 권한을 사용하거나, 서비스 역할을 사용하거나, 또는 서비스 연결 역할을 사용하여 이 작업을 수행할 수 있습니다.
- 전달 액세스 세션(FAS) - IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하면 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와 의 상호 작용을 완료해야 하는 요청을 수신할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [액세스 세션 전달을](#) 참조하세요.
- 서비스 역할 - 서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수입하는 [IAM 역할](#)입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다IAM. 자세한 내용은 IAM 사용 설명서의 [에 권한을 위임할 역할 생성을 AWS 서비스](#) 참조하세요.

- 서비스 연결 역할 - 서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.
- Amazon에서 실행되는 애플리케이션 EC2 - IAM 역할을 사용하여 EC2 인스턴스에서 실행되고 AWS CLI 또는 AWS API 요청을 수행하는 애플리케이션의 임시 보안 인증을 관리할 수 있습니다. 이는 EC2 인스턴스 내에 액세스 키를 저장하는 것보다 좋습니다. EC2 인스턴스에 AWS 역할을 할당하고 모든 애플리케이션에서 사용할 수 있도록 하려면 인스턴스에 연결된 인스턴스 프로파일을 생성합니다. 인스턴스 프로파일에는 역할이 포함되어 있으며 EC2 인스턴스에서 실행 중인 프로그램이 임시 자격 증명을 가져올 수 있습니다. 자세한 내용은 IAM 사용 설명서 [EC2의 IAM 역할 사용을 참조하세요](#).

정책을 사용한 액세스 관리

정책을 AWS 생성하고 AWS 자격 증명 또는 리소스에 연결하여 의 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결된 AWS 경우 권한을 정의하는 의 객체입니다. 는 보안 주체(사용자, 루트 사용자 또는 역할 세션)가 요청할 때 이러한 정책을 AWS 평가합니다. 정책에서 권한은 요청이 허용되거나 거부되는 지를 결정합니다. 대부분의 정책은 에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서의 구조 및 내용에 대한 자세한 내용은 IAM 사용 설명서 [의 JSON 정책 개요](#)를 참조하세요.

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

기본적으로, 사용자와 역할에는 어떠한 권한도 없습니다. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

IAM 정책은 작업을 수행하는 데 사용하는 방법에 관계없이 작업에 대한 권한을 정의합니다. 예를 들어, iam:GetRole 작업을 허용하는 정책이 있다고 가정합니다. 해당 정책을 사용하는 사용자는 AWS Management Console, AWS CLI 또는 에서 역할 정보를 가져올 수 있습니다 AWS API.

보안 인증 기반 정책

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [고객 관리형 정책을 사용하여 사용자 지정 IAM 권한 정의를](#) 참조하세요.

보안 인증 기반 정책은 인라인 정책 또는 관리형 정책으로 한층 더 분류할 수 있습니다. 인라인 정책은 단일 사용자, 그룹 또는 역할에 직접 포함됩니다. 관리형 정책은 의 여러 사용자, 그룹 및 역할에 연결할 수 있는 독립 실행형 정책입니다 AWS 계정. 관리형 정책에는 AWS 관리형 정책 및 고객 관리형 정책이 포함됩니다. 관리형 정책 또는 인라인 정책 중에서 선택하는 방법을 알아보려면 IAM 사용 설명서의 [관리형 정책 및 인라인 정책 중에서 선택](#)을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 이 포함될 수 있습니다 AWS 서비스.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책IAM에서는 의 AWS 관리형 정책을 사용할 수 없습니다.

액세스 제어 목록(ACLs)

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지 않습니다.

Amazon S3 AWS WAF및 AmazonVPC은 를 지원하는 서비스의 예입니다ACLs. 에 대한 자세한 내용은 Amazon Simple Storage Service 개발자 안내서의 [액세스 제어 목록\(ACL\) 개요](#)를 ACLs참조하세요.

기타 정책 타입

AWS 는 덜 일반적인 추가 정책 유형을 지원합니다. 이러한 정책 타입은 더 일반적인 정책 유형에 따라 사용자에게 부여되는 최대 권한을 설정할 수 있습니다.

- 권한 경계 - 권한 경계는 자격 증명 기반 정책이 IAM엔터티(IAM 사용자 또는 역할)에 부여할 수 있는 최대 권한을 설정하는 고급 기능입니다. 개체에 대한 권한 경계를 설정할 수 있습니다. 그 결과로 얻는 권한은 객체의 자격 증명 기반 정책과 그 권한 경계의 교집합입니다. Principal 필드에서 사용자나 역할을 지정하는 리소스 기반 정책은 권한 경계를 통해 제한되지 않습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 권한 경계에 대한 자세한 내용은 IAM 사용 설명서의 [IAM엔터티에 대한 권한 경계](#)를 참조하세요.
- 서비스 제어 정책(SCPs) - 의 조직 또는 조직 단위(OU)에 대한 최대 권한을 지정하는 SCPs JSON 정책입니다 AWS Organizations. AWS Organizations 는 비즈니스가 소유 AWS 계정 한 여러 을

그룹화하고 중앙에서 관리하기 위한 서비스입니다. 조직의 모든 기능을 활성화하면 서비스 제어 정책(SCPs)을 계정의 일부 또는 전체에 적용할 수 있습니다. 는 각 를 포함하여 멤버 계정의 엔터티에 대한 권한을 SCP 제한합니다 AWS 계정 루트 사용자. 조직 및 에 대한 자세한 내용은 AWS Organizations 사용 설명서의 [서비스 제어 정책을](#) SCPs참조하세요.

- 세션 정책 – 세션 정책은 역할 또는 페더레이션 사용자에게 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 결과적으로 얻는 세션의 권한은 사용자 또는 역할의 보안 인증 기반 정책의 교차와 세션 정책입니다. 또한 권한을 리소스 기반 정책에서 가져올 수도 있습니다. 이러한 정책 중 하나에 포함된 명시적 거부는 허용을 재정의합니다. 자세한 내용은 IAM 사용 설명서의 [세션 정책을](#) 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. AWS 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 결정하는 방법을 알아보려면 IAM 사용 설명서의 [정책 평가 로직](#)을 참조하세요.

AWS Storage Gateway의 작동 방식 IAM

IAM 를 사용하여 에 대한 액세스를 관리하기 전에 에서 사용할 수 있는 IAM 기능에 대해 AWS SGW알아봅니다 AWS SGW.

IAM AWS Storage Gateway와 함께 사용할 수 있는 기능

IAM 기능	AWS SGW 지원
ID 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACLs	아니요
ABAC (정책의 태그)	부분

IAM 기능	AWS SGW 지원
임시 보안 인증	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

및 기타 AWS 서비스가 대부분의 IAM 기능을 어떻게 사용하는지 AWS SGW 자세히 알아보려면 IAM 사용 설명서의 [에서 AWS 를 사용하는 서비스를 IAM](#) 참조하세요.

에 대한 자격 증명 기반 정책 AWS SGW

ID 기반 정책 지원: 예

자격 증명 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 자격 증명에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자와 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [고객 관리형 정책을 사용하여 사용자 지정 IAM 권한 정의를](#) 참조하세요.

IAM 자격 증명 기반 정책을 사용하면 허용되거나 거부된 작업 및 리소스와 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. 보안 인증 기반 정책에서는 보안 주체가 연결된 사용자 또는 역할에 적용되므로 보안 주체를 지정할 수 없습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 [IAM JSON 정책 요소 참조](#)를 참조하세요.

에 대한 자격 증명 기반 정책 예제 AWS SGW

자격 증명 기반 정책의 예를 AWS SGW 보려면 섹션을 참조하세요 [Storage Gateway에 대한 자격 증명 기반 정책 예제](#).

내 리소스 기반 정책 AWS SGW

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 문서입니다. 리소스 기반 정책의 예로는 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관

리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 [보안 주체를 지정](#)해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는 가 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려면 리소스 기반 정책의 보안 주체로 전체 계정 또는 다른 계정의 IAM 엔티티를 지정할 수 있습니다. 리소스 기반 정책에 크로스 계정 보안 주체를 추가하는 것은 트러스트 관계 설정의 절반밖에 되지 않는다는 것을 유념하십시오. 보안 주체와 리소스가 다른 계정에 있는 경우 신뢰할 수 있는 AWS 계정에 있는 계정의 IAM 관리자는 보안 주체 엔티티(사용자 또는 역할)에게 리소스에 액세스할 수 있는 권한도 부여해야 합니다. 엔티티에 ID 기반 정책을 연결하여 권한을 부여합니다. 하지만 리소스 기반 정책이 동일 계정의 보안 주체에 액세스를 부여하는 경우, 추가 자격 증명 기반 정책이 필요하지 않습니다. 자세한 내용은 IAM 사용 설명서의 [에서 크로스 계정 리소스 액세스를 IAM](#) 참조하세요.

에 대한 정책 작업 AWS SGW

정책 작업 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 Action 요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 정책 작업은 일반적으로 연결된 AWS API 작업과 이름이 동일합니다. 일치하는 API 작업이 없는 권한 전용 작업과 같은 몇 가지 예외가 있습니다. 정책에서 여러 작업이 필요한 몇 가지 작업도 있습니다. 이러한 추가 작업을 일컬어 종속 작업이라고 합니다.

연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하십시오.

작업 목록을 보려면 서비스 승인 참조의 AWS SGW [AWS Storage Gateway에서 정의한 작업을](#) 참조하세요.

의 AWS SGW 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
sgw
```

단일 문에서 여러 작업을 지정하려면 다음과 같이 쉼표로 구분합니다.

```
"Action": [
    "sgw:action1",
```

```
"sgw:action2"
]
```

자격 증명 기반 정책의 예를 AWS SGW 보려면 섹션을 참조하세요 [Storage Gateway에 대한 자격 증명 기반 정책 예제](#).

에 대한 정책 리소스 AWS SGW

정책 리소스 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Resource JSON 정책 요소는 작업이 적용되는 객체를 지정합니다. 문장에는 Resource 또는 NotResource 요소가 반드시 추가되어야 합니다. 가장 좋은 방법은 [Amazon 리소스 이름\(ARN\)을 사용하여 리소스를](#) 지정하는 것입니다. 리소스 수준 권한이라고 하는 특정 리소스 유형을 지원하는 작업에 대해 이 태스크를 수행할 수 있습니다.

작업 나열과 같이 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

리소스 유형 및 해당의 AWS SGW 목록을 보려면 서비스 권한 부여 참조의 [AWS Storage Gateway에서 정의한 리소스를](#) ARNs 참조하세요. 각 리소스ARN의 를 지정할 수 있는 작업을 알아보려면 [AWS Storage Gateway에서 정의한 작업을](#) 참조하세요.

자격 증명 기반 정책의 예를 AWS SGW 보려면 섹션을 참조하세요 [Storage Gateway에 대한 자격 증명 기반 정책 예제](#).

에 대한 정책 조건 키 AWS SGW

서비스별 정책 조건 키 지원: 예

관리자는 정책을 사용하여 AWS JSON 대상에 액세스할 수 있는 사용자를 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

Condition 요소(또는 Condition 블록)를 사용하면 정책이 발효되는 조건을 지정할 수 있습니다. Condition 요소는 옵션입니다. 같거나 작음과 같은 [조건 연산자](#)를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수 있습니다.

한 문에서 여러 Condition 요소를 지정하거나 단일 Condition 요소에서 여러 키를 지정하는 경우, AWS 는 논리적 AND 태스크를 사용하여 평가합니다. 단일 조건 키에 여러 값을 지정하는 경우는 논리적 OR 작업을 사용하여 조건을 AWS 평가합니다. 명문의 권한을 부여하기 전에 모든 조건을 충족해야 합니다.

조건을 지정할 때 자리 표시자 변수를 사용할 수도 있습니다. 예를 들어 IAM 리소스에 사용자 IAM 이름으로 태그가 지정된 경우에만 사용자에게 리소스에 액세스할 수 있는 권한을 부여할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [IAM 정책 요소: 변수 및 태그](#)를 참조하세요.

AWS 는 전역 조건 키 및 서비스별 조건 키를 지원합니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 [AWS 전역 조건 컨텍스트 키](#)를 참조하세요.

조건 키 목록을 보려면 서비스 승인 참조의 AWS SGW [AWS Storage Gateway용 조건 키를 참조하세요](#). 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면 [AWS Storage Gateway에서 정의한 작업을 참조하세요](#).

자격 증명 기반 정책의 예를 AWS SGW 보려면 섹션을 참조하세요 [Storage Gateway에 대한 자격 증명 기반 정책 예제](#).

ACLs 의 AWS SGW

지원 ACLs: 아니요

액세스 제어 목록(ACLs)은 리소스에 액세스할 수 있는 권한이 있는 보안 주체(계정 멤버, 사용자 또는 역할)를 제어합니다. ACLs 는 리소스 기반 정책과 유사하지만 JSON 정책 문서 형식을 사용하지는 않습니다.

ABAC 와 함께 AWS SGW

지원ABAC(정책의 태그): 부분

속성 기반 액세스 제어(ABAC)는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. 여기서 AWS이러한 속성을 태그 라고 합니다. IAM 엔터티(사용자 또는 역할) 및 여러 AWS 리소스에 태그를 연결할 수 있습니다. 엔터티 및 리소스에 태그를 지정하는 것은 의 첫 번째 단계입니다ABAC. 그런 다음 보안 주체의 태그가 액세스하려는 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계합니다.

ABAC 는 빠르게 성장하는 환경에서 유용하며 정책 관리가 번거로워지는 상황에 도움이 됩니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` 또는 `aws:TagKeys` 조건 키를 사용하여 정책의 [조건 요소](#)에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

에 대한 자세한 내용은 IAM 사용 설명서의 [ABAC 권한 부여를 사용하여 권한 정의를 ABAC참조](#) 하세요. 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 [속성 기반 액세스 제어 사용\(ABAC\)](#)을 ABAC참조하세요.

에서 임시 자격 증명 사용 AWS SGW

임시 자격 증명 지원: 예

임시 자격 증명을 사용하여 로그인할 때 작동하지 AWS 서비스 않는 경우도 있습니다. 임시 자격 증명 으로 AWS 서비스 작업하는 경우를 비롯한 자세한 내용은 IAM 사용 설명서의 [AWS 서비스 에서 작업 하는 IAM](#) 섹션을 참조하세요.

사용자 이름 및 암호를 제외한 방법을 AWS Management Console 사용하여 에 로그인하는 경우 임시 자격 증명을 사용합니다. 예를 들어 회사의 Single Sign-On(SSO) 링크를 AWS 사용하여 에 액세스하면 해당 프로세스가 임시 자격 증명을 자동으로 생성합니다. 또한 콘솔에 사용자로 로그인한 다음 역할을 전환할 때 임시 보안 인증을 자동으로 생성합니다. 역할 전환에 대한 자세한 내용은 IAM 사용 설명서의 [사용자에서 IAM 역할\(콘솔\)로 전환](#)을 참조하세요.

AWS CLI 또는 를 사용하여 임시 자격 증명을 수동으로 생성할 수 있습니다 AWS API. 그런 다음 이러한 임시 자격 증명을 사용하여 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 AWS. AWS recommends에 액세스할 수 있습니다. 자세한 내용은 [의 임시 보안 자격 증명을 IAM](#)참조 하세요.

에 대한 액세스 세션 전달 AWS SGW

전달 액세스 세션 지원(FAS): 예

IAM 사용자 또는 역할을 사용하여 에서 작업을 수행하는 경우 보안 주체로 AWS간주됩니다. 일부 서비스를 사용하는 경우 다른 서비스에서 다른 작업을 시작하는 작업을 수행할 수 있습니다. FAS 는 를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청은 서비스가 다른 AWS 서비스 또는 리소스와의 상호 작용을 완료해야 하는 요청을 수신

할 때만 수행됩니다. 이 경우 두 작업을 모두 수행할 수 있는 권한이 있어야 합니다. FAS 요청 시 정책 세부 정보는 [액세스 세션 전달](#)을 참조하세요.

AWS SGW의 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하기 위해 수임하는 [IAM 역할](#)입니다. IAM 관리자는 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 [에 권한을 위임할 역할 생성을 AWS 서비스](#) 참조하세요.

Warning

서비스 역할에 대한 권한을 변경하면 기능이 중단 AWS SGW될 수 있습니다. 가 지침을 제공하는 경우에만 AWS SGW 서비스 역할을 편집합니다.

에 대한 서비스 연결 역할 AWS SGW

서비스 링크 역할 지원: 예

서비스 연결 역할은 에 연결된 서비스 역할의 한 유형입니다. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은 에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할에 대한 권한을 볼 수 있지만 편집할 수는 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 [AWS에서 작동하는 서비스를 참조하세요](#). 서비스 연결 역할 열에서 Yes(이)가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 Yes(네) 링크를 선택합니다.

Storage Gateway에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 리소스를 생성하거나 수정할 AWS SGW 수 있는 권한이 없습니다. 또한 AWS Management Console, AWS Command Line Interface (AWS CLI) 또는 를 사용하여 작업을 수행할 수 없습니다. AWS API. 사용자에게 필요한 리소스에 대한 작업을 수행할 수 있는 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성할 수 있습니다. 그런 다음 관리자는 IAM 정책을 역할에 추가하고 사용자는 역할을 수임할 수 있습니다.

이러한 예제 정책 문서를 사용하여 IAM 자격 증명 기반 JSON 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 [IAM 정책 생성\(콘솔\)](#)을 참조하세요.

각 리소스 유형에 ARNs 대한 형식 AWS SGW등 에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 [AWS Storage Gateway에 대한 작업, 리소스 및 조건 키를 참조하세요.](#)

주제

- [정책 모범 사례](#)
- [콘솔 사용 AWS SGW](#)
- [사용자가 자신의 고유한 권한을 볼 수 있도록 허용](#)

정책 모범 사례

자격 증명 기반 정책은 계정에서 리소스를 생성, 액세스 또는 삭제할 AWS SGW 수 있는지 여부를 결정합니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따릅니다.

- AWS 관리형 정책을 시작하고 최소 권한 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 [관리 AWS 형 정책](#) 또는 [AWS 작업 함수에 대한 관리형 정책을](#) 참조하세요.
- 최소 권한 적용 - IAM 정책으로 권한을 설정할 때 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. 를 사용하여 권한을 적용하는 IAM 방법에 대한 자세한 내용은 IAM 사용 설명서의 [에서 정책 및 권한을 IAM](#) 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 - 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어 정책 조건을 작성하여 를 사용하여 모든 요청을 전송하도록 지정할 수 있습니다 SSL. AWS 서비스와 같은 특정 를 통해 서비스 작업을 사용하는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 AWS CloudFormation. 자세한 내용은 IAM 사용 설명서의 [IAM JSON 정책 요소: 조건을](#) 참조하세요.
- IAM Access Analyzer를 사용하여 IAM 정책을 검증하여 안전하고 기능적인 권한을 보장합니다. IAM Access Analyzer는 정책이 정책 언어(JSON) 및 IAM 모범 사례를 준수하도록 새 정책 및 기존 IAM 정책을 검증합니다. IAM Access Analyzer는 안전하고 기능적인 정책을 작성하는 데 도움이 되는 100개 이상의 정책 확인 및 실행 가능한 권장 사항을 제공합니다. 자세한 내용은 IAM 사용 설명서의 [IAM Access Analyzer를 사용한 정책 검증](#)을 참조하세요.
- 다중 인증 필요(MFA) - 에 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 MFA 위해 를 AWS 계정됩니다. API 작업을 호출할 MFA 때 를 요구하려면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 [를 사용한 보안 API 액세스를 MFA](#) 참조하세요.

의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 [의 보안 모범 사례를 IAM](#) 참조하세요.

콘솔 사용 AWS SGW

AWS Storage Gateway 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한을 통해 의 AWS SGW 리소스에 대한 세부 정보를 나열하고 볼 수 있어야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 자격 증명 기반 정책을 만들면 콘솔이 해당 정책에 연결된 엔터티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 에만 전화를 거는 사용자에게 최소 콘솔 권한을 허용할 필요는 없습니다 AWS API. 대신 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 허용합니다.

사용자와 역할이 콘솔을 AWS SGW 계속 사용할 수 있도록 하려면 AWS SGW *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 [사용자에게 권한 추가](#)를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제에서는 IAM 사용자가 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 를 사용하여 프로그래밍 방식으로 이 작업을 완료할 수 있는 권한이 포함되어 있습니다 AWS API.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupsForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",

```

```

        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
    ],
    "Resource": "*"
}
]
}

```

AWS Storage Gateway ID 및 액세스 문제 해결

다음 정보를 사용하면 및 으로 작업할 때 발생할 수 있는 일반적인 문제를 AWS SGW 진단하고 해결하는 데 도움이 IAM 됩니다.

주제

- [다음과 같은 작업을 수행할 권한이 없습니다. AWS SGW](#)
- [저는 IAM을 수행할 권한이 없습니다. PassRole](#)
- [외부 사용자가 내 AWS SGW 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.](#)

다음과 같은 작업을 수행할 권한이 없습니다. AWS SGW

작업을 수행할 수 있는 권한이 없다는 오류가 수신되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음 예제 오류는 mateojackson IAM 사용자가 콘솔을 사용하여 가상 *my-example-widget* 리소스에 대한 세부 정보를 보려고 하지만 가상 권한이 없는 경우 발생합니다. `sgw:GetWidget`

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
sgw:GetWidget on resource: my-example-widget
```

이 경우 `sgw:GetWidget` 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요하면 관리자에게 문의하세요. AWS 관리자는 로그인 자격 증명을 제공한 사람입니다.

저는 IAM을 수행할 권한이 없습니다. PassRole

작업을 수행할 권한이 없다는 오류가 발생하는 경우 역할을 넘길 수 있도록 정책을 업데이트해야 합니다. iam:PassRole AWS SGW

일부 AWS 서비스 서비스에서는 새 서비스 역할 또는 서비스 연결 역할을 만드는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 사용자가 서비스에 역할을 전달할 수 있는 권한을 가지고 있어야 합니다.

다음 예제 오류는 라는 IAM 사용자가 콘솔을 사용하여 에서 작업을 marymajor 수행하려고 할 때 발생합니다. AWS SGW 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 수 있는 권한을 가지고 있지 않습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

이 경우, Mary가 iam:PassRole 작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

외부 사용자가 내 AWS SGW 리소스에 액세스할 수 있도록 AWS 계정 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록 (ACLs) 을 지원하는 서비스의 경우 이러한 정책을 사용하여 사용자에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세히 알아보려면 다음을 참조하세요.

- 이러한 기능의 AWS SGW 지원 여부를 알아보려면 을 참조하십시오. [AWS Storage Gateway의 작동 방식 IAM](#)
- 소유한 리소스에 대한 액세스 권한을 AWS 계정 부여하는 방법을 알아보려면 사용 [설명서에서 AWS 계정 자신이 소유한 다른 IAM 사용자의 액세스 권한 제공을 IAM](#) 참조하십시오.
- 제3자에게 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM사용 설명서의 [제3자가 AWS 계정 소유한 리소스에 대한 액세스 제공을](#) 참조하십시오. AWS 계정

- ID 페더레이션을 통해 액세스를 [제공하는 방법을 알아보려면 사용 설명서의 외부 인증된 사용자에 게 액세스 제공 \(ID 페더레이션\)](#) 을 IAM 참조하십시오.
- 계정 간 액세스에 대한 역할 사용과 리소스 기반 정책의 차이점을 알아보려면 사용 설명서의 계정 간 [리소스 액세스](#)를 참조하십시오. IAM IAM

AWS Storage Gateway의 규정 준수 검증

타사 감사자가 여러 규정 AWS 준수 프로그램의 일환으로 AWS Storage Gateway의 보안 및 규정 준수를 평가합니다. 여기에는 SOC,, FedPCI,ISO,,RAMP,HIPAA, C5MTSC, K-, ENS High ISMSOSPAR, 및 등이 포함됩니다. HITRUST CSF

특정 규정 준수 프로그램의 범위 내 AWS 서비스 목록은 규정 준수 프로그램별 [범위 내AWS 서비스 규정 준수](#) 참조하십시오. 일반 정보는 [AWS 규정 준수 프로그램AWS 보증 프로그램 규정AWS](#) 참조하십시오.

를 사용하여 AWS Artifact타사 감사 보고서를 다운로드할 수 있습니다. 자세한 내용은 의 보고서 <https://docs.aws.amazon.com/artifact/latest/ug/downloading-documents.html> 참조하십시오 AWS Artifact.

Storage Gateway 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS에서는 규정 준수에 도움이 되도록 다음과 같은 리소스를 제공합니다.

- [보안 및 규정 준수 킷스타트 가이드](#) - 이 배포 가이드에서는 아키텍처 고려 사항을 설명하고 보안 및 규정 준수에 중점을 둔 기본 환경을 배포하기 위한 단계를 제공합니다. AWS
- [HIPAA보안 및 규정 준수를 위한 설계 백서 — 이 백서는 기업이](#) 규정을 준수하는 애플리케이션을 개발하는 데 사용할 수 있는 방법을 설명합니다. AWS HIPAA
- [AWS 규정 준수 리소스AWS](#) — 이 통합 문서 및 가이드 모음은 해당 산업 및 지역에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 [규칙을 사용하여 리소스 평가](#) — 이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- [AWS Security Hub](#)— 이 AWS 서비스는 보안 업계 표준 및 모범 사례를 준수하는지 확인하는 데 도움이 되는 내부 보안 상태를 종합적으로 보여줍니다.

Resilience in AWS Storage Gateway

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 기반으로 구축됩니다.

AWS 리전은 데이터 센터가 클러스터링되는 전 세계 물리적 위치입니다. 논리적 데이터 센터의 각 그룹을 가용 영역(AZ)이라고 합니다. 각각 AWS 리전은 지리적 영역 AZs 내에서 최소 3개의 격리된 물리적 분리로 구성됩니다. 리전을 단일 데이터 센터로 정의하는 다른 클라우드 공급자와 달리 모든 의 다중 AZ 설계 AWS 리전은 고유한 이점을 제공합니다. 각 AZ에는 독립적인 전력, 냉각 및 물리적 보안이 있으며 중복 ultra-low-latency 네트워크를 통해 연결됩니다. 배포 시 고가용성에 중점을 두어야 하는 경우 서비스 및 리소스를 여러 AZs로 구성하여 내결함성을 높일 수 있습니다.

AWS 리전은 최고 수준의 인프라 보안, 규정 준수 및 데이터 보호를 충족합니다. 사이의 모든 트래픽 AZs은 암호화됩니다. 네트워크 성능은 간에 동기식 복제를 수행하기에 충분합니다 AZs. AZs 고가용성을 위한 파티셔닝 서비스와 리소스를 쉽게 만들 수 있습니다. 배포가 를 통해 분할되면 리소스가 더 잘 격리되고 정전 AZs, 번개, 토네이도, 지진 등과 같은 문제로부터 보호됩니다. AZs 는 다른 AZ와 의미 있는 거리만큼 물리적으로 분리되지만, 모두 서로 100km(60마일) 이내에 있습니다.

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

AWS 글로벌 인프라 외에도 Storage Gateway는 데이터 복원력 및 백업 요구 사항을 지원하는 데 도움이 되는 몇 가지 기능을 제공합니다.

- VMware vSphere 고가용성(VMware HA)을 사용하면 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 자세한 내용은 [Storage Gateway에서 VMware vSphere 고가용성 사용](#) 단원을 참조하십시오.
- 가상 테이프를 S3 Glacier Flexible Retrieval에 아카이브합니다. 자세한 내용은 [가상 테이프 보관](#) 단원을 참조하십시오.

AWS Storage Gateway의 인프라 보안

관리형 서비스인 AWS Storage Gateway는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차에 따라 보호됩니다. https://d0.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf

AWS 게시된 API 호출을 사용하여 네트워크를 통해 Storage Gateway에 액세스합니다. 클라이언트는 전송 계층 보안(TLS) 1.2를 지원해야 합니다. 또한 클라이언트는 Ephemeral Diffie-Hellman(PFS) 또는 Elliptic Curve Ephemeral Diffie-Hellman()과 같은 완벽한 순방향 보안(DHE)을 갖춘 암호 제품군을 지원해야 합니다ECDHE. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

또한 액세스 키 ID와 IAM 보안 주체와 연결된 보안 액세스 키를 사용하여 요청에 서명해야 합니다. 또는 [AWS Security Token Service](#)(AWS STS)를 사용하여 임시 보안 인증을 생성하여 요청에 서명할 수 있습니다.

Note

AWS Storage Gateway 어플라이언스를 관리형 가상 머신으로 취급해야 하며 어떤 식으로든 설치에 액세스하거나 수정하려고 시도해서는 안 됩니다. 스캔 소프트웨어를 설치하거나 일반 게이트웨이 업데이트 메커니즘 이외의 방법을 사용하여 소프트웨어 패키지를 업데이트하려고 하면 게이트웨이가 오작동할 수 있으며 게이트웨이를 지원하거나 수정하는 기능에 영향을 미칠 수 있습니다.

AWS CVEs 정기적으로 검토, 분석 및 수정합니다. 이러한 문제에 대한 수정 사항을 일반적인 소프트웨어 릴리스 주기의 일부로 Storage Gateway에 통합합니다. 이러한 수정 사항은 일반적으로 예약된 유지 관리 기간 동안 일반 게이트웨이 업데이트 프로세스의 일부로 적용됩니다. 게이트웨이 업데이트에 대한 자세한 내용은 참조.

AWS 보안 베스트 프랙티스

AWS 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 사례는 사용자의 환경에 적절하지 않거나 충분하지 않을 수 있으므로 규정이 아닌 참고용으로만 사용하세요. 자세한 내용은 [AWS 보안 모범 사례](#)를 참조하세요.

로그인 및 모니터링 AWS Storage Gateway

Storage Gateway는 Storage Gateway에서 사용자, 역할 또는 AWS 서비스가 수행한 작업에 대한 기록을 제공하는 서비스와 통합됩니다. AWS CloudTrail CloudTrail Storage Gateway에 대한 모든 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Storage Gateway 콘솔에서의 통화와 Storage Gateway API 작업에 대한 코드 호출이 포함됩니다. 트레일을 생성하면 Storage Gateway에 대한 CloudTrail 이벤트를 포함하여 Amazon S3 버킷으로의 지속적인 이벤트 전송을 활성화할 수 있습니다. 트레일을 구성하지 않아도 CloudTrail 콘솔의 이벤트 기록에서 최신 이벤트를 계속 볼 수 있습니다. 에서 수집한 CloudTrail 정보를 사용하여 Storage Gateway에 이루어진 요청, 요청이 이루어진 IP 주소, 요청한 사람, 요청 시기 및 추가 세부 정보를 확인할 수 있습니다.

자세한 CloudTrail 내용은 [AWS CloudTrail 사용 설명서](#)를 참조하십시오.

Storage Gateway 정보 입력 CloudTrail

CloudTrail 계정을 만들 때 Amazon Web Services 계정에서 활성화됩니다. Storage Gateway에서 활동이 발생하면 해당 활동이 CloudTrail 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 이벤트에 기록됨

니다. Amazon Web Services 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 내용은 이벤트 [기록으로 CloudTrail 이벤트 보기를](#) 참조하십시오.

Storage Gateway에 대한 이벤트를 포함하여 Amazon Web Services 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. 트레일을 사용하면 CloudTrail Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 트레일을 생성하면 트레일이 모든 AWS 지역에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 이에 따라 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하십시오.

- [추적 생성 개요](#)
- [CloudTrail 지원되는 서비스 및 통합](#)
- [에 대한 Amazon SNS 알림 구성 CloudTrail](#)
- [여러 지역에서 CloudTrail 로그 파일 수신 및 여러 계정으로부터 CloudTrail 로그 파일 수신](#)

모든 Storage Gateway 작업은 로깅되며 [작업](#) 주제에서 문서화됩니다. 예를 들어, ActivateGatewayListGateways, 를 호출하고 ShutdownGateway 작업을 수행하면 CloudTrail 로그 파일에 항목이 생성됩니다.

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

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부.
- 역할 또는 페더레이션 사용자에게 대한 임시 보안 인증을 사용하여 요청이 생성되었는지 여부.
- 다른 AWS 서비스에서 요청했는지 여부.

자세한 내용은 [CloudTrail userIdentity요소를](#) 참조하십시오.

Storage Gateway 로그 파일 항목 이해

트레일은 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있는 구성입니다. CloudTrail 로그 파일은 하나 이상의 로그 항목을 포함합니다. 이벤트는 모든 소스의 단일 요청을 나타내며 요청된 작업, 작업 날짜 및 시간, 요청 매개 변수 등에 대한 정보를 포함합니다. CloudTrail 로그 파일은 공개 API 호출의 정렬된 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```

{ "Records": [{
    "eventVersion": "1.02",
    "userIdentity": {
      "type": "IAMUser",
      "principalId": "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": "cloudtrailgatewayv1",
      "gatewayRegion": "us-east-2",
      "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
      "gatewayType": "VTL"
    },
    "responseElements": {
      "gatewayARN":
"arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayv1"
    },
    "requestID":
"54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
    "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
    "eventType": "AwsApiCall",
    "apiVersion": "20130630",
    "recipientAccountId": "444455556666"
  ]
}

```

다음 예제는 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다. ListGateways

```

{
  "Records": [{
    "eventVersion": "1.02",

```

```

    "userIdentity": {
        "type": "IAMUser",
        "principalId": "AIDAI15AUEPBH2M7JTNVC",
        "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"
  ]]
}

```

게이트웨이 문제 해결

다음은 게이트웨이, 호스트 플랫폼, 가상 테이프, 고가용성, 데이터 복구 및 보안과 관련된 모범 사례 및 문제 해결에 대한 정보를 찾을 수 있습니다. 온프레미스 게이트웨이 문제 해결 정보는 지원되는 가상화 플랫폼에 배포된 게이트웨이를 다룹니다. 고가용성 문제에 대한 문제 해결 정보는 VMware vSphere 고가용성(HA) 플랫폼에서 실행되는 게이트웨이를 다룹니다.

주제

- [문제 해결: 게이트웨이 오프라인 문제](#) - Storage Gateway 콘솔에서 게이트웨이가 오프라인으로 표시될 수 있는 문제를 진단하는 방법을 알아봅니다.
- [문제 해결: 게이트웨이 활성화 중 내부 오류](#) - Storage Gateway 활성화를 시도할 때 내부 오류 메시지가 표시되는 경우 어떻게 해야 하는지 알아봅니다.
- [온프레미스 게이트웨이 문제 해결](#) - 온프레미스 게이트웨이에서 발생할 수 있는 일반적인 문제와 가 게이트웨이에 AWS Support 연결하여 문제 해결을 지원하는 방법을 알아봅니다.
- [Microsoft Hyper-V 설정 관련 문제 해결](#) - Microsoft Hyper-V 플랫폼에 Storage Gateway를 배포할 때 발생할 수 있는 일반적인 문제에 대해 알아봅니다.
- [Amazon EC2 게이트웨이 문제 해결](#) - Amazon 에 배포된 게이트웨이로 작업할 때 발생할 수 있는 일반적인 문제에 대한 정보를 찾습니다EC2.
- [하드웨어 어플라이언스 문제 해결](#) - Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제를 해결하는 방법을 알아봅니다.
- [가상 테이프 관련 문제 해결](#) - 가상 테이프에 예상치 못한 문제가 발생할 경우 취할 수 있는 조치에 대해 알아봅니다.
- [고가용성 문제 해결](#) - VMware HA 환경에 배포된 게이트웨이에 문제가 발생하는 경우 어떻게 해야 하는지 알아봅니다.

문제 해결: 게이트웨이 오프라인 문제

다음 문제 해결 정보를 사용하여 콘솔에 AWS Storage Gateway 게이트웨이가 오프라인 상태인 것으로 표시되는 경우 수행할 작업을 결정합니다.

게이트웨이는 다음 이유 중 하나 이상으로 인해 오프라인으로 표시될 수 있습니다.

- 게이트웨이가 Storage Gateway 서비스 엔드포인트에 연결할 수 없습니다.
- 게이트웨이가 예기치 않게 종료되었습니다.

- 게이트웨이와 연결된 캐시 디스크가 연결 해제 또는 수정되었거나 실패했습니다.

게이트웨이를 다시 온라인 상태로 전환하려면 게이트웨이가 오프라인 상태가 되는 문제를 식별하고 해결합니다.

연결된 방화벽 또는 프록시 확인

프록시를 사용하도록 게이트웨이를 구성했거나 게이트웨이를 방화벽 뒤에 배치한 경우 프록시 또는 방화벽의 액세스 규칙을 검토합니다. 프록시 또는 방화벽은 Storage Gateway 에 필요한 네트워크 포트 및 서비스 엔드포인트와의 트래픽을 허용해야 합니다. 자세한 내용은 사항 [네트워크 및 방화벽 요구 사항](#) 참조하세요.

게이트웨이 트래픽에 대한 지속적인 SSL 또는 심층 패킷 검사 확인

게이트웨이와 간의 네트워크 트래픽에 대해 SSL 또는 딥 패킷 검사를 현재 수행 중인 경우 AWS게이트웨이가 필요한 서비스 엔드포인트와 통신하지 못할 수 있습니다. 게이트웨이를 다시 온라인 상태로 전환하려면 검사를 비활성화해야 합니다.

하이퍼바이저 호스트에서 정전 또는 하드웨어 장애 확인

게이트웨이의 하이퍼바이저 호스트에서 정전 또는 하드웨어 장애가 발생하면 게이트웨이가 예기치 않게 종료되어 연결할 수 없게 될 수 있습니다. 전원 및 네트워크 연결을 복원하면 게이트웨이에 다시 연결할 수 있게 됩니다.

게이트웨이가 다시 온라인 상태가 된 후에는 데이터를 복구하기 위한 조치를 취해야 합니다. 자세한 내용은 [복구 모범 사례 데이터](#) .

연결된 캐시 디스크에 문제가 있는지 확인

게이트웨이와 연결된 캐시 디스크 중 하나 이상이 제거, 변경 또는 크기 조정되었거나 손상된 경우 게이트웨이가 오프라인 상태가 될 수 있습니다.

하이퍼바이저 호스트에서 작동 중인 캐시 디스크를 제거한 경우:

1. 게이트웨이를 종료합니다.
2. 디스크를 다시 추가합니다.

Note

동일한 디스크 노드에 디스크를 추가해야 합니다.

3. 게이트웨이를 다시 시작합니다.

캐시 디스크가 손상되거나 교체되거나 크기가 조정된 경우:

1. 게이트웨이를 종료합니다.
2. 캐시 디스크를 재설정합니다.
3. 캐시 스토리지를 위해 디스크를 재구성합니다.
4. 게이트웨이를 다시 시작합니다.

테이프 게이트웨이의 손상된 캐시 디스크 문제 해결에 대한 자세한 내용은 [오작동하는 캐시 디스크에서 가상 테이프를 복구해야 함을 참조하세요](#).

문제 해결: 게이트웨이 활성화 중 내부 오류

Storage Gateway 활성화 요청은 두 네트워크 경로를 통과합니다. 클라이언트가 보낸 수신 활성화 요청은 포트 80을 통해 게이트웨이의 가상 머신(VM) 또는 Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스에 연결됩니다. 게이트웨이가 활성화 요청을 성공적으로 수신하면 게이트웨이는 Storage Gateway 엔드포인트와 통신하여 활성화 키를 수신합니다. 게이트웨이가 Storage Gateway 엔드포인트에 연결할 수 없는 경우 게이트웨이는 내부 오류 메시지로 클라이언트에 응답합니다.

다음 문제 해결 정보를 사용하여 를 활성화하려고 할 때 내부 오류 메시지가 표시되는 경우 수행할 작업을 결정합니다 AWS Storage Gateway.

Note

- 최신 가상 머신 이미지 파일 또는 Amazon Machine Image(AMI) 버전을 사용하여 새 게이트웨이를 배포해야 합니다. 오래된 를 사용하는 게이트웨이를 활성화하려고 하면 내부 오류가 발생합니다AMI.
- 를 다운로드하기 전에 배포하려는 올바른 게이트웨이 유형을 선택해야 합니다AMI. 각 게이트웨이 유형에 AMIs 대한 .ova 파일 및 는 서로 다르며 상호 교환할 수 없습니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필요한 포트 확인

온프레미스에 배포된 게이트웨이의 경우 포트가 로컬 방화벽에서 열려 있는지 확인합니다. Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 인스턴스의 보안 그룹에서 포트가 열려 있는지 확인합니다. 포트가 열려 있는지 확인하려면 서버의 퍼블릭 엔드포인트에서 텔넷 명령을 실행합니다. 이 서버는 게이트웨이와 동일한 서브넷에 있어야 합니다. 예를 들어 다음 텔넷 명령은 포트 443에 대한 연결을 테스트합니다.

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

게이트웨이 자체가 엔드포인트에 도달할 수 있는지 확인하려면 게이트웨이의 로컬 VM 콘솔(온프레미스에 배포된 게이트웨이의 경우)에 액세스합니다. 또는 게이트웨이의 인스턴스SSH로 이동할 수 있습니다(Amazon 에 배포된 게이트웨이의 경우EC2). 그런 다음 네트워크 연결 테스트를 실행합니다. 테스트가 를 반환하는지 확인합니다[PASSED]. 자세한 내용은 [인터넷에 대한 게이트웨이 연결 테스트](#).

Note

게이트웨이 콘솔의 기본 로그인 사용자 이름은 이고 기본 암호admin는 입니다password.

방화벽 보안이 게이트웨이에서 퍼블릭 엔드포인트로 전송된 패킷을 수정하지 않는지 확인합니다.

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안은 게이트웨이에서 전송되는 패킷을 방해할 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 대로 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 포트 443의 기본 활성화 엔드포인트(anon-cp.storagegateway.region.amazonaws.com)에서 OpenSSL 명령을 실행합니다. 게이트웨이와 동일한 서브넷에 있는 시스템에서 이 명령을 실행해야 합니다.

```
$ openssl s_client -connect anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

Note

Replace *region* 를 사용합니다 AWS 리전.

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
  i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
  i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
  i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
  Root Certificate Authority - G2
  i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

지속적인 SSL 검사가 있는 경우 응답에는 다음과 유사한 변경된 인증서 체인이 표시됩니다.

```
$ openssl s_client -connect anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
```



```
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 엔드포인트에 대한 게이트웨이의 아웃바운드 트래픽은 네트워크의 방화벽에서 수행하는 검사에서 제외되어야 합니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간이 너무 오래 걸리면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 왜곡은 60초 이하여야 합니다. 자세한 내용은 게이트웨이 VM 시간 [동기화 게이트웨이 VM 시간](#).

시스템 시간 관리 옵션은 Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 사용할 수 없습니다. Amazon EC2 게이트웨이가 시간을 적절하게 동기화할 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

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

Amazon VPC 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

Amazon Virtual Private Cloud(AmazonVPC) 엔드포인트를 사용하여 게이트웨이를 활성화할 때 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필요한 포트 확인


로컬 방화벽(온프레미스에 배포된 게이트웨이의 경우) 또는 보안 그룹(Amazon 에 배포된 게이트웨이의 경우EC2) 내에 필요한 포트가 열려 있는지 확인합니다. 게이트웨이를 Storage Gateway VPC 엔드

포인트에 연결하는 데 필요한 포트는 게이트웨이를 퍼블릭 엔드포인트에 연결하는 데 필요한 포트와 다릅니다. Storage Gateway VPC 엔드포인트에 연결하려면 다음 포트가 필요합니다.

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

자세한 내용은 Storage [Storage Gateway용 VPC 엔드포인트 생성](#)을 참조.

또한 Storage Gateway VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 엔드포인트에 연결된 기본 보안 그룹은 필요한 포트를 허용하지 않을 수 있습니다. 게이트웨이의 IP 주소 범위에서 필요한 포트를 통해 트래픽을 허용하는 새 보안 그룹을 생성합니다. 그런 다음 해당 보안 그룹을 VPC 엔드포인트에 연결합니다.

 Note

[Amazon VPC 콘솔](#)을 사용하여 VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 콘솔에서 Storage Gateway VPC 엔드포인트를 확인한 다음 보안 그룹 탭을 선택합니다.

필요한 포트가 열려 있는지 확인하기 위해 Storage Gateway VPC 엔드포인트에서 텔넷 명령을 실행할 수 있습니다. 게이트웨이와 동일한 서브넷에 있는 서버에서 이러한 명령을 실행해야 합니다. 가용 영역을 지정하지 않은 DNS 이름에서 테스트를 실행할 수 있습니다. 예를 들어 다음 텔넷 명령은 `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com` DNS 이름을 사용하여 필요한 포트 연결을 테스트합니다.

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

방화벽 보안이 게이트웨이에서 Storage Gateway Amazon VPC 엔드포인트로 전송된 패킷을 수정하지 않는지 확인합니다.

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안은 게이트웨이에서 전송되는 패킷을 방해할 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 대로 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 Storage Gateway VPC 엔드포인트에서 OpenSSL 명령을 실행합니다. 게이트웨이와 동일한 서브넷에 있는 시스템에서 이 명령을 실행해야 합니다. 필요한 각 포트에 대해 명령을 실행합니다.

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:443 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1026 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1028 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1031 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:2222 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
```

```

verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
  i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
  i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
  i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
Starfield Services Root Certificate Authority - G2
  i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
Authority
---
```

지속적인 SSL 검사가 있는 경우 응답에는 다음과 유사한 변경된 인증서 체인이 표시됩니다.

```

openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
  i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 필요한 포트를 통해 VPC 엔드포인트로 전송되는 게이트웨이의 아웃바운드 트래픽은 네트워크 방화벽에서 수행하는 검사에서 제외됩니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간이 너무 오래 걸리면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 왜곡은 60초 이하여야 합니다. 자세한 내용은 게이트웨이 VM 시간 [동기화 게이트웨이 VM 시간](#).

시스템 시간 관리 옵션은 Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 사용할 수 없습니다. Amazon EC2 게이트웨이가 시간을 적절하게 동기화할 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

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

HTTP 프록시 확인 및 관련 보안 그룹 설정 확인

활성화하기 전에 온프레미스 게이트웨이 VM에 포트 3128의 Squid HTTP 프록시로 EC2 구성된 Amazon의 프록시가 있는지 확인합니다. 이 경우 다음을 확인합니다.

- Amazon의 HTTP 프록시에 연결된 보안 그룹에는 인바운드 규칙이 EC2 있어야 합니다. 이 인바운드 규칙은 게이트웨이 VM의 IP 주소에서 포트 3128의 Squid 프록시 트래픽을 허용해야 합니다.
- Amazon EC2 VPC 엔드포인트에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이러한 인바운드 규칙은 Amazon의 HTTP 프록시 IP 주소에서 포트 1026-1028, 1031, 2222 및 443의 트래픽을 허용해야 합니다EC2.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 동일한 에 Storage Gateway VPC 엔드포인트가 있는 경우 오류를 해결합니다. VPC

동일한 에 Amazon Virtual Private Cloud(Amazon VPC) 인포인트가 있는 경우 퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 오류를 해결하려면 다음 확인 및 구성을 VPC수행합니다.

Storage Gateway VPC 엔드포인트에서 프라이빗 DNS 이름 활성화 설정이 활성화되지 않았는지 확인합니다.

프라이빗 DNS 이름 활성화가 활성화된 경우 해당 게이트웨이에서 퍼블릭 엔드포인트로의 게이트웨이를 활성화VPC할 수 없습니다.

프라이빗 DNS 이름 옵션을 비활성화하려면:

1. [Amazon VPC 콘솔](#) 을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Storage Gateway VPC 엔드포인트를 선택합니다.
4. 작업을 선택합니다.
5. 프라이빗 DNS 이름 관리를 선택합니다.
6. 프라이빗 DNS 이름 활성화 에서 이 엔드포인트 에 대해 활성화를 선택 취소합니다.
7. 개인 DNS 이름 수정을 선택하여 설정을 저장합니다.

온프레미스 게이트웨이 문제 해결

온프레미스 게이트웨이에서 발생할 수 있는 일반적인 문제와 게이트웨이 문제를 해결하기 위해 AWS Support 를 활성화하는 방법에 대한 다음 정보를 찾을 수 있습니다.

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

문제	취할 조치
게이트웨이의 IP 주소를 찾을 수 없습니다.	<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. • 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 켜다면 게이트웨이가 부팅 시퀀스를 마치는 데 몇 분이 걸릴 수 있습니다.
네트워크 또는 방화벽에 문제가 있습니다.	<ul style="list-style-type: none"> • 게이트웨이에 적절한 포트를 허용합니다.

문제	취할 조치
	<ul style="list-style-type: none"> • SSL 인증서 검증/검사를 활성화해서는 안 됩니다. Storage Gateway는 타사 애플리케이션이 두 인증서를 가로채거나 서명하려고 하면 실패하는 상호 TLS 인증을 사용합니다. • 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. 네트워크 및 방화벽 요건에 대한 자세한 내용은 네트워크 및 방화벽 요구 사항 단원을 참조하십시오.
<p>Storage Gateway Management Console에서 활성화 진행 버튼을 클릭하면 게이트웨이 활성화가 실패합니다.</p>	<ul style="list-style-type: none"> • 클라이언트에서 VM을 ping하여 게이트웨이 VM에 액세스할 수 있는지 확인합니다. • VM이 인터넷에 네트워크로 연결되어 있는지 확인합니다. 그렇지 않으면 SOCKS 프록시를 구성해야 합니다. 이에 대한 자세한 내용은 온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성 섹션을 참조하세요. • 호스트에 올바른 시간이 있는지, 호스트가 Network Time Protocol(NTP) 서버에 자동으로 시간을 동기화하도록 구성되어 있는지, 게이트웨이 VM에 올바른 시간이 있는지 확인합니다. 하이퍼바이저 호스트 및 시간 동기화에 대한 자세한 내용은 VM 시간을 Hyper-V 또는 Linux KVM 호스트 시간과 동기화 섹션을 참조하세요. • 이 단계를 수행한 후 Storage Gateway 콘솔과 게이트웨이 설정 및 활성화 마법사를 사용하여 게이트웨이 배포를 다시 시도할 수 있습니다. • SSL 인증서 검증/검사를 활성화해서는 안 됩니다. Storage Gateway는 타사 애플리케이션이 두 인증서를 가로채거나 서명하려고 하면 실패하는 상호 TLS 인증을 사용합니다. • VM에 7.5GB 이상의 RAM이 있는지 확인합니다. 7.5GB 미만의 RAM이 있는 경우 게이트웨이 할당이 실패합니다. 자세한 내용은 Tape Gateway 설정 요구 사항 단원을 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>업로드 버퍼 공간으로 할당된 디스크를 제거하는 작업에 대한 지침은 게이트웨이에서 디스크 제거 섹션을 참조하세요.</p>
<p>게이트웨이와 AWS간 대역폭을 개선해야 합니다.</p>	<p>애플리케이션 및 게이트웨이 VM을 연결하는 것과는 별도로 네트워크 어댑터(NIC) AWS 에서 에 대한 인터넷 연결을 설정 AWS 하여 게이트웨이에서 로 대역폭을 개선할 수 있습니다. 이 접근 방식은 에 고 대역폭 연결이 있고 특히 스냅샷 복원 중에 대역폭 경합을 피 AWS 하려는 경우에 유용합니다. 고처리량 워크로드 요구 사항을 충족하기 위해 AWS Direct Connect를 사용하여 온프레미스 게이트웨이와 AWS간에 전용 네트워크 연결을 설정할 수 있습니다. 게이트웨이에서 로의 연결 대역폭을 측정하려면 게이트웨이의 CloudBytesDownloaded 및 CloudBytesUploaded 지표를 AWS사용합니다. 이에 관한 자세한 내용은 Tape Gateway와 간의 성능 측정 AWS 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"> • Storage Gateway 콘솔의 게이트웨이 탭에서 게이트웨이 VM의 IP 주소가 하이퍼바이저 클라이언트 소프트웨어(즉, VMware vSphere 클라이언트 또는 Microsoft Hyper-V Manager)를 사용하여 표시되는 것과 동일한지 확인합니다. 일치하지 않는 경우 게이트웨이 VM 종료에 표시된 대로 Storage Gateway 콘솔에서 게이트웨이를 다시 시작합니다. 다시 시작한 후에는 Storage Gateway 콘솔의 게이트웨이 탭에 있는 IP 주소 목록에 있는 주소가 하이퍼바이저 클라이언트에서 확인한 게이트웨이의 IP 주소와 일치해야 합니다. • VMware ESXi의 경우 VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다. • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. • 에 설명된 AWS 대로 게이트웨이의 에 대한 연결을 확인합니다 인터넷에 대한 게이트웨이 연결 테스트. • 게이트웨이의 네트워크 어댑터 구성을 확인하고 게이트웨이에 대해 활성화하려는 모든 인터페이스가 활성화되었는지 확인합니다. 게이트웨이의 네트워크 어댑터 구성을 보려면 게이트웨이 네트워크 구성 단원의 지침에 따라 게이트웨이의 네트워크 구성을 볼 수 있는 옵션을 선택합니다. <p>Amazon CloudWatch 콘솔에서 게이트웨이를 오가는 처리량을 볼 수 있습니다. 게이트웨이 및 에서 주고받는 처리량 측정에 대한 자세한 내용은 섹션을 AWS참조하세요 Tape Gateway와 간의 성능 측정 AWS.</p>
<p>Microsoft Hyper-V에서 Storage Gateway를 가져오기(배포)하는 데 문제가 있습니다.</p>	<p>Microsoft Hyper-V에서 게이트웨이를 배포할 때 흔히 겪는 몇 가지 문제를 다루는 Microsoft Hyper-V 설정 관련 문제 해결 단원을 참조하십시오.</p>

문제	취할 조치
"게이트웨이의 볼륨에 기록된 데이터가 AWS에 안전하게 저장되지 않았습니다."라는 메시지가 표시됩니다.	게이트웨이 VM이 또 다른 게이트웨이 VM의 복제 또는 스냅샷으로 부터 생성된 경우 이 메시지를 수신하게 됩니다. 그렇지 않은 경우 AWS Support에 문의하세요.

AWS Support 가 온프레미스에서 호스팅되는 게이트웨이 문제를 해결하는데 도움이 되도록 허용

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이에 액세스 AWS Support 하도록 활성화하는 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이에 대한 AWS Support 액세스는 비활성화됩니다. 호스트의 로컬 콘솔을 통해 이 액세스 권한을 제공해야 합니다. 게이트웨이에 대한 AWS Support 액세스 권한을 부여하려면 먼저 호스트의 로컬 콘솔에 로그인한 다음 Storage Gateway의 콘솔로 이동한 다음 지원 서버에 연결합니다.

게이트웨이에 대한 AWS Support 액세스를 허용하려면

- 호스트의 로컬 콘솔에 로그인합니다.
 - VMware ESXi – 자세한 내용은 섹션을 참조하세요 [를 사용하여 Gateway Local Console에 액세스](#) [스 VMware ESXi](#).
 - Microsoft Hyper-V - 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#) [스](#) 섹션을 참조하세요.
- 프롬프트에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
- h**를 입력하여 사용 가능한 명령 목록을 엽니다.
- 다음 중 하나를 수행합니다.
 - 게이트웨이가 퍼블릭 엔드포인트를 사용하는 경우 AVAILABLE COMMANDS 창에서 **l**를 입력하여 Storage Gateway **open-support-channel**에 대한 고객 지원에 연결합니다. 에 대한 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 사용하는 경우 AVAILABLE COMMANDS 창에 **l**를 입력합니다 **open-support-channel**. 게이트웨이가 활성화되지 않은 경우 Storage Gateway 에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. 에 대한 지원 채널을 열 수 있

도록 TCP 포트 22를 허용합니다. AWS. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

Note

채널 번호는 전송 제어 프로토콜/사용자 데이터그램 프로토콜(TCP/UDP) 포트 번호가 아닙니다. 대신 게이트웨이는 보안 셸(SSH)(TCP 22)을 Storage Gateway 서버에 연결하고 연결에 대한 지원 채널을 제공합니다.

5. 지원 채널이 설정된 후 에 지원 서비스 번호를 제공 AWS Support 하면 가 문제 해결 지원을 제공할 AWS Support 수 있습니다.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. Amazon Web Services Support에서 지원 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **exit**를 입력하여 게이트웨이 콘솔에서 로그아웃합니다.
8. 프롬프트 메시지에 따라 로컬 콘솔을 종료합니다.

Microsoft Hyper-V 설정 관련 문제 해결

다음 표는 Microsoft Hyper-V 플랫폼에 Storage Gateway를 배포할 때 발생할 수 있는 일반적인 문제를 나열한 것입니다.

문제	취할 조치
<p>게이트웨이를 가져오려고 하면 다음과 같은 오류 메시지가 표시됩니다.</p> <p>“가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. 위치 [...]에서 가상 머신 가져오기 파일을 찾을 수 없습니다. Hyper-V를 사용하여 가상 머신을 생성하고 내보내는 경우에만 가상 머신을 가져올 수 있습니다.”</p>	<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. 가상 머신 가져오기 대화 상자에서 지정하는 위치의 마지막 부분은 여야 합니다 <code>AWS-Storage-Gateway</code> . 예: <code>C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\</code> . • 이미 게이트웨이를 배포했는데 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하지 않은 경우, 압축 해제된 게이트웨이 파일이 있는 위치에 VM이 생성되므로 이 위치에서 다시 가져올 수 없습니다. 이 문제를 해결하려면 압축을

문제	취할 조치
	<p>해제한 게이트웨이 소스 파일의 새 사본을 얻어 이를 새 위치에 복사하면 됩니다. 새 위치를 가져오는 위치로 사용합니다.</p> <p>압축을 풀지 않은 소스 파일 위치 하나에서 여러 게이트웨이를 생성하려는 경우 가상 머신 복사를 선택하고 가상 머신 가져오기 대화 상자에서 모든 파일 복제 상자를 선택해야 합니다.</p>
<p>게이트웨이를 가져오려고 하면 다음과 같은 오류 메시지가 표시됩니다.</p> <p>“가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. 가져오기 작업이 [...]에서 파일을 복사하지 못했습니다. 파일이 존재합니다. (0x80070050)”</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 설정 대화 상자 왼쪽의 패널에 있는 서버 아래에 새 위치를 지정합니다.</p>
<p>게이트웨이를 가져오려고 하면 다음과 같은 오류 메시지가 표시됩니다.</p> <p>“가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again.”라는 오류 메시지가 표시됩니다.</p>	<p>게이트웨이를 가져올 때 가상 머신 복사를 선택하고 가상 머신 가져오기 대화 상자에서 모든 파일 복제 확인란을 선택하여 VM에 대한 새 고유 ID를 생성해야 합니다.</p>

문제	취할 조치
<p>게이트웨이 VM을 시작하려고 하면 다음 오류 메시지가 표시됩니다.</p> <p>“선택한 가상 머신(들)을 시작하는 동안 오류가 발생했습니다. 하위 파티션 프로세서 설정이 상위 파티션과 호환되지 않습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 기계 ID [...])'</p>	<p>이 오류는 게이트웨이CPU에 필요한 와 호스트CPU에서 사용 가능한 간의 CPU 불일치로 인해 발생할 수 있습니다. 기본 하이퍼바이저에서 VM CPU 수를 지원하는지 확인합니다.</p> <p>Storage Gateway 요구 사항에 대한 자세한 내용은 Tape Gateway 설정 요구 사항 섹션을 참조하세요.</p>
<p>게이트웨이 VM을 시작하려고 하면 다음 오류 메시지가 표시됩니다.</p> <p>“선택한 가상 머신(들)을 시작하는 동안 오류가 발생했습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 기계 ID [...]) 파티션 생성 실패: 요청된 서비스를 완료하기에 시스템 리소스가 부족합니다. (0x800705AA)'</p>	<p>이 오류는 게이트웨이RAM에 필요한 과 호스트RAM에서 사용 가능한 간의 RAM 불일치로 인해 발생할 수 있습니다.</p> <p>Storage Gateway 요구 사항에 대한 자세한 내용은 Tape Gateway 설정 요구 사항 섹션을 참조하세요.</p>
<p>스냅샷 및 게이트웨이 소프트웨어 업데이트는 예상과 약간 다른 시각에 실행됩니다.</p>	<p>게이트웨이 VM의 클럭은 실제 시간과 약간 오차가 있을 수 있는데, 이를 클럭 드리프트라고 합니다. 로컬 게이트웨이 콘솔의 시간 동기화 옵션을 사용하여 VM의 시간을 점검하고 수정합니다. 자세한 내용은 VM 시간을 Hyper-V 또는 Linux KVM 호스트 시간과 동기화 단원을 참조하십시오.</p>

문제	취할 조치
압축 해제된 Microsoft Hyper-V Storage Gateway 파일은 호스트 파일 시스템에 저장해야 합니다.	일반적인 Microsoft Windows 서버에 액세스하듯이 호스트에 액세스합니다. 예를 들어 하이퍼바이저 호스트가 이름 hyperv-server 인 경우 다음 UNC 경로를 사용할 수 있습니다. \\hyperv-server\c\$ 이 경로는 이름을 확인할 hyperv-server 수 있거나 로컬 호스트 파일에 정의되어 있다고 가정합니다.
하이퍼바이저에 접속할 때 자격 증명을 요구하는 메시지가 표시됩니다.	Sconfig.cmd 도구를 사용하여 사용자 자격 증명을 하이퍼바이저 호스트용 로컬 관리자로 추가합니다.
Broadcom 네트워크 어댑터를 사용하는 Hyper-V 호스트에 대해 가상 머신 대기열 (VMQ)을 켜면 네트워크 성능이 저하될 수 있습니다.	해결 방법에 대한 자세한 내용은 Microsoft 설명서를 참조하세요. 이 VMQ 켜져 있는 경우 Windows Server 2012 Hyper-V 호스트의 가상 머신에서 네트워크 성능 저하를 참조하세요.

Amazon EC2 게이트웨이 문제 해결

다음 섹션에서는 Amazon에 배포된 게이트웨이와 관련하여 발생할 수 있는 일반적인 문제를 확인할 수 EC2 있습니다. 온프레미스 게이트웨이와 EC2 Amazon에 배포된 게이트웨이의 차이에 대한 자세한 내용은 [참조하십시오 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포.](#)

주제

- [몇 분 후 게이트웨이가 활성화되지 않음](#)
- [인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.](#)
- [Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없습니다.](#)
- [스토리지 볼륨을 추가하려고 할 때 사용 가능한 디스크가 없다는 메시지가 표시되는 경우](#)
- [업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우](#)
- [게이트웨이로 들어오거나 EC2 게이트웨이에서 나가는 처리량이 0으로 떨어집니다.](#)
- [게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2](#)
- [Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려고 합니다.](#)

몇 분 후 게이트웨이가 활성화되지 않음

Amazon EC2 콘솔에서 다음을 확인하십시오.

- 인스턴스와 연결한 보안 그룹에서 포트 80이 활성화되어 있는지 여부. 보안 그룹 규칙 추가에 대한 자세한 내용은 Amazon EC2 User Guide의 [보안 그룹 규칙 추가](#)를 참조하십시오.
- 게이트웨이 인스턴스는 실행 중으로 표시됩니다. Amazon EC2 콘솔에서 인스턴스의 상태 값은 다음과 같아야 RUNNING 합니다.
- Amazon EC2 인스턴스 유형이 에 설명된 최소 요구 사항을 충족하는지 확인하십시오 [스토리지 요구 사항](#).

문제를 해결한 후 게이트웨이를 다시 활성화합니다. 이렇게 하려면 Storage Gateway 콘솔을 열고 EC2Amazon에 새 게이트웨이 배포를 선택한 다음 인스턴스의 IP 주소를 다시 입력합니다.

인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없습니다.

인스턴스에 리소스 태그를 지정하지 않았는데 많은 수의 인스턴스가 실행 중인 경우에는 어떤 인스턴스를 실행했는지 파악하기 어려울 수 있습니다. 이 경우 다음 작업을 수행하여 해당 게이트웨이 인스턴스를 찾을 수 있습니다.

- 인스턴스의 설명 탭에서 Amazon 머신 이미지 (AMI) 의 이름을 확인합니다. Storage Gateway 기반 인스턴스는 텍스트로 AMI 시작해야 **aws-storage-gateway-ami** 합니다.
- Storage AMI Gateway를 기반으로 하는 인스턴스가 여러 개 있는 경우 인스턴스 시작 시간을 확인하여 올바른 인스턴스를 찾으십시오.

Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없습니다.

해당 Amazon EBS 볼륨이 게이트웨이 인스턴스와 동일한 가용 영역에 있는지 확인합니다. 가용 영역에 불일치가 있는 경우 인스턴스와 동일한 가용 영역에 새 Amazon EBS 볼륨을 생성하십시오.

스토리지 볼륨을 추가하려고 할 때 사용 가능한 디스크가 없다는 메시지가 표시되는 경우

새로 활성화된 게이트웨이에 볼륨 스토리지가 정의되지 않았습니다. 볼륨 스토리지를 정의하려면 먼저 게이트웨이에 업로드 버퍼 및 캐시 스토리지로 사용할 로컬 디스크를 할당해야 합니다. Amazon에

배포된 게이트웨이의 EC2 경우 로컬 디스크는 인스턴스에 연결된 Amazon EBS 볼륨입니다. 이 오류 메시지는 인스턴스에 대해 정의된 Amazon EBS 볼륨이 없기 때문에 발생할 수 있습니다.

게이트웨이를 실행하는 인스턴스에 정의된 블록 디바이스를 확인합니다. 블록 디바이스 (와 함께 제공되는 기본 디바이스AMI) 가 두 개뿐인 경우 스토리지를 추가해야 합니다. 이에 대한 자세한 내용은 [Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포](#) 섹션을 참조하세요. 두 개 이상의 Amazon EBS 볼륨을 연결한 후 게이트웨이에 볼륨 스토리지를 생성해 보십시오.

업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우

[할당할 업로드 버퍼의 크기 결정](#) 단원의 단계를 따르세요.

게이트웨이로 들어오거나 EC2 게이트웨이에서 나가는 처리량이 0으로 떨어집니다.

게이트웨이 인스턴스가 실행 중인지 확인합니다. 예를 들어 해당 인스턴스가 재부팅되고 있는 중이라면 인스턴스가 다시 시작할 때까지 기다립니다.

또한 게이트웨이 IP가 변경되지 않았는지 확인합니다. 인스턴스를 중단했다가 다시 시작한 경우, 인스턴스의 IP 주소가 변경되었을 수 있습니다. 이 경우 새 게이트웨이를 활성화해야 합니다.

Amazon CloudWatch 콘솔에서 게이트웨이로 들어오고 나가는 처리량을 볼 수 있습니다. 게이트웨이로 들어오고 나가는 처리량을 측정하는 방법에 대한 자세한 내용은 [Tape Gateway와 간의 성능 측정 AWS](#)를 참조하십시오.

게이트웨이 문제 AWS Support 해결에 도움을 주고 싶으신가요? EC2

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이 액세스를 활성화하는 AWS Support 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이 AWS Support 액세스는 비활성화됩니다. Amazon EC2 로컬 콘솔을 통해 이 액세스 권한을 제공합니다. 보안 셸 (SSH) 을 통해 Amazon EC2 로컬 콘솔에 로그인합니다. 성공적으로 로그인하려면 인스턴스의 보안 그룹에 TCP 포트 22를 여는 규칙이 있어야 합니다. SSH

Note

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

게이트웨이에 AWS Support 연결하려면 먼저 Amazon EC2 인스턴스의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 액세스 권한을 제공해야 합니다.

Amazon EC2 인스턴스에 배포된 게이트웨이에 대한 AWS Support 액세스를 활성화하려면

1. Amazon EC2 인스턴스의 로컬 콘솔에 로그인합니다. 지침을 보려면 Amazon 사용 EC2 설명서의 [인스턴스에 Connect](#)를 참조하십시오.

다음 명령을 사용하여 EC2 인스턴스의 로컬 콘솔에 로그인할 수 있습니다.

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

Note

The *PRIVATE-KEY* Amazon EC2 인스턴스를 시작하는 데 사용한 EC2 키 페어의 사실 인증서가 들어 있는 .pem 파일입니다. 자세한 내용은 Amazon EC2 사용 설명서의 [키 쌍에 대한 퍼블릭 키 검색](#)을 참조하십시오.

The *INSTANCE-PUBLIC-DNS-NAME* 게이트웨이가 실행되는 Amazon EC2 인스턴스의 퍼블릭 도메인 이름 시스템 (DNS) 이름입니다. EC2콘솔에서 Amazon EC2 인스턴스를 선택하고 Description 탭을 클릭하면 이 퍼블릭 DNS 이름을 얻을 수 있습니다.

2. 프롬프트에 **6 - Command Prompt**를 입력하여 AWS Support 채널 콘솔을 엽니다.
3. **h**를 입력하여 AVAILABLECOMMANDS창을 엽니다.
4. 다음 중 하나를 수행합니다.
 - 게이트웨이가 퍼블릭 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에서 **l**를 입력하여 **open-support-channel** Storage Gateway에 대한 고객 지원에 연결하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
 - 게이트웨이가 VPC 엔드포인트를 사용하는 경우 AVAILABLECOMMANDS창에 **l**를 입력합니다 **open-support-channel**. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공하십시오. 지원 채널을 열 수 있도록 TCP 포트 22를 AWS허용하십시오. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

Note

채널 번호는 전송 제어 프로토콜/사용자 데이터그램 프로토콜 (TCP/UDP) 포트 번호가 아닙니다. 대신 게이트웨이는 Secure Shell (SSH) (TCP22) 을 Storage Gateway 서버에 연결하고 연결을 위한 지원 채널을 제공합니다.

5. 지원 채널이 설정되면 문제 해결에 도움을 줄 AWS Support 수 AWS Support 있도록 지원 서비스 번호를 제공하십시오.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. 지원 세션이 AWS Support 완료되었다는 알림이 올 때까지 세션을 닫지 마십시오.
7. **exit**를 입력하여 Storage Gateway 콘솔을 종료합니다.
8. 콘솔 메뉴에 따라 Storage Gateway 인스턴스에서 로그아웃합니다.

Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려고 합니다.

Amazon EC2 직렬 콘솔을 사용하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. 지침과 문제 해결 팁은 [Amazon Elastic Compute 클라우드 사용 설명서의 Amazon EC2 시리얼 콘솔](#)을 참조하십시오.

하드웨어 어플라이언스 문제 해결

다음 주제에서는 Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제와 이러한 문제를 해결하기 위한 제안 사항에 대해 설명합니다.

서비스 IP 주소를 확인할 수 없음

서비스에 연결할 때 호스트 IP 주소가 아닌 서비스의 IP 주소를 사용하고 있는지 확인합니다. 서비스 콘솔에서 서비스 IP 주소를 구성하고 하드웨어 콘솔에서 호스트 IP 주소를 구성합니다. 하드웨어 어플라이언스를 시작하면 하드웨어 콘솔이 표시됩니다. 하드웨어 콘솔에서 서비스 콘솔로 이동하려면 Open Service Console(서비스 콘솔 열기)을 선택합니다.

공장 초기화는 어떻게 수행하나요?

어플라이언스에서 공장 초기화를 수행해야 하는 경우, 다음 지원 섹션에 설명된 대로 Storage Gateway 하드웨어 어플라이언스 팀에 지원을 요청하세요.

원격 재시작은 어떻게 수행하나요?

어플라이언스를 원격으로 다시 시작해야 하는 경우 Dell iDRAC 관리 인터페이스를 사용하여 다시 시작할 수 있습니다. 자세한 내용은 [Dell Technologies 웹 사이트의 iDRAC9 Virtual Power Cycle: Remotely Power Cycle Dell EMC PowerEdge Servers](#)를 참조하세요. InfoHub

Dell iDRAC 지원은 어디에서 얻을 수 있나요?

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

- iDRAC 관리 인터페이스를 사용하는 경우 기본 암호를 변경해야 합니다. iDRAC 보안 인증에 대한 자세한 내용은 [Dell PowerEdge - i 의 기본 로그인 보안 인증은 무엇입니까DRAC?](#)를 참조하세요.
- 보안 위반을 방지하기 위해 펌웨어가 인지 up-to-date 확인합니다.
- iDRAC 네트워크 인터페이스를 일반(em) 포트로 이동하면 성능 문제가 발생하거나 어플라이언스가 정상적으로 작동하지 않을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾을 수 없음

Storage Gateway 콘솔을 사용하여 Storage Gateway 하드웨어 어플라이언스의 일련 번호를 찾을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾으려면:

1. <https://console.aws.amazon.com/storagegateway/> [집에서](#) Storage Gateway 콘솔을 엽니다.
2. 페이지 왼쪽의 탐색 메뉴에서 하드웨어를 선택합니다.
3. 목록에서 하드웨어 어플라이언스를 선택합니다.
4. 어플라이언스의 세부 정보 탭에서 일련 번호 필드를 찾습니다.

하드웨어 어플라이언스 지원은 어디에서 받을 수 있나요?

하드웨어 어플라이언스에 대한 기술 지원에 AWS 대한 문의는 섹션을 참조하세요 [AWS Support](#).

AWS Support 팀이 지원 채널을 활성화하여 게이트웨이 문제를 원격으로 해결하도록 요청할 수 있습니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다. 다음 절차에 나온 것처럼 하드웨어 콘솔에서 지원 채널을 활성화할 수 있습니다.

에 대한 지원 채널을 열려면 AWS

1. 하드웨어 콘솔을 엽니다.
2. 하드웨어 콘솔의 메인 페이지 하단에서 지원 채널 열기를 선택한 다음 를 누릅니다Enter.

네트워크 연결 또는 방화벽 문제가 없는 경우 30초 이내에 할당된 포트 번호가 나타나야 합니다.
예:

상태: 포트 19599에서 열기

3. 포트 번호를 기록하여 에 제공합니다 AWS Support.

가상 테이프 관련 문제 해결

아래와 같이 가상 테이프와 관련해 예기치 않은 문제를 겪는 경우 취해야 할 조치에 대한 정보를 얻을 수 있습니다.

주제

- [복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우](#)
- [복구 불가능한 테이프 문제 해결](#)
- [고가용성 상태 알림](#)

복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우

드물긴 하지만 Tape Gateway에 복구 불가능한 장애가 발생할 수 있습니다. 그러한 장애는 하이퍼바이저 호스트, 게이트웨이 자체 또는 캐시 디스크에서 발생할 수 있습니다. 장애가 발생하면 이 단원의 문제 해결 지침에 따라 테이프를 복구할 수 있습니다.

주제

- [장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우](#)
- [장애가 있는 캐시 디스크에서 가상 테이프를 복구해야 하는 경우](#)

장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우

테이프 게이트웨이 또는 하이퍼바이저 호스트에서 복구할 수 없는 오류가 발생하는 경우 다른 테이프 게이트웨이에 이미 업로드된 모든 데이터를 복구할 수 있습니다. AWS

단, 테이프에 기록된 데이터는 해당 테이프가 성공적으로 보관될 때까지 완전히 업로드되지 않을 수 있습니다. VTS 이러한 방식으로 다른 게이트웨이로 복구된 테이프에서 데이터가 불완전하거나 비어 있을 수 있습니다. 모든 복구된 테이프에서 인벤토리를 수행하여 예상한 대로 콘텐츠가 들어 있는지 확인할 것을 권장합니다.

테이프를 다른 Tape Gateway로 복구하려면

1. 복구 대상 게이트웨이로 사용할 기존 Tape Gateway를 찾습니다. 테이프를 복구할 Tape Gateway가 없으면 Tape Gateway를 새로 생성합니다. 게이트웨이 생성 방법에 대한 자세한 내용은 [게이트웨이 생성](#) 섹션을 참조하세요.
2. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
3. 탐색 창에서 게이트웨이를 선택한 다음 테이프를 복구할 Tape Gateway를 선택합니다.
4. 세부 정보 탭을 선택하십시오. 테이프 복구 메시지가 탭에 표시됩니다.
5. 복구 테이프 생성을 선택하여 게이트웨이를 비활성화합니다.
6. 표시된 대화 상자에서 게이트웨이 비활성화를 선택합니다.

이 프로세스는 Tape Gateway의 정상적 기능을 영구적으로 중단하고 사용 가능한 모든 복구 시점을 노출합니다. 지침은 [Tape Gateway 비활성화](#)를 참조하세요.

7. 비활성화된 게이트웨이가 표시하는 테이프에서 복구할 가상 테이프와 복구 시점을 선택합니다. 가상 테이프에 복구 시점이 여러 개인 경우가 있습니다.
8. 대상 Tape Gateway에 필요한 테이프 복구를 시작하려면 복구 테이프 생성을 선택합니다.
9. 복구 테이프 생성 대화 상자에서 복구할 가상 테이프의 바코드를 확인합니다.
10. 게이트웨이에서 가상 테이프를 복구할 Tape Gateway를 선택합니다.
11. 복구 테이프 생성을 선택합니다.
12. 요금이 청구되지 않도록 장애가 있는 Tape Gateway를 삭제합니다. 지침은 [게이트웨이 삭제 및 관련 리소스 제거](#) 단원을 참조하십시오.

Storage Gateway가 장애가 발생한 Tape Gateway에서 사용자가 지정한 Tape Gateway로 테이프를 이동합니다. 테이프 게이트웨이는 테이프 상태를 로 표시합니다RECOVERED.

장애가 있는 캐시 디스크에서 가상 테이프를 복구해야 하는 경우

캐시 디스크에 오류가 발생하는 경우, 게이트웨이가 게이트웨이 내 가상 테이프에 읽기 및 쓰기 작업이 수행되지 않도록 방지합니다. 예를 들어 디스크가 손상되거나 게이트웨이에서 제거된 경우 오류가 발생할 수 있습니다. Storage Gateway 콘솔이 오류 관련 메시지를 표시합니다.

오류 메시지에서 Storage Gateway는 테이프를 복구할 수 있는 두 가지 조치 중 하나를 수행하라는 메시지를 다음과 같이 표시합니다.

- 디스크를 종료하고 다시 추가 - 디스크에 손상되지 않은 데이터가 있는 채로 디스크가 삭제되어버린 경우 이 방법을 선택합니다. 예를 들어 우발적으로 호스트에서 디스크가 삭제되어 오류가 발생하였으나 디스크와 데이터는 손상되지 않은 경우, 디스크를 다시 추가할 수 있습니다. 이 작업을 위해서는 이 단원 후반부의 절차를 참조하십시오.
- 캐시 디스크 재설정 - 캐시 디스크가 손상되었거나 액세스할 수 없는 경우 이 방법을 선택합니다. 디스크 오류로 인해 캐시 디스크가 액세스할 수 없거나 사용할 수 없거나 손상된 경우, 디스크를 재설정할 수 있습니다. 캐시 디스크를 재설정하면 클린 데이터가 있는 테이프(즉 캐시 디스크 및 Amazon S3의 데이터가 동기화된 테이프)를 계속해서 사용할 수 있습니다. 그러나 Amazon S3와 동기화되지 않은 데이터가 있는 테이프는 자동으로 복구됩니다. 이러한 테이프의 상태는 RECOVERED 설정되지만 테이프는 읽기 전용입니다. 호스트에서 디스크를 제거하는 방법에 대한 정보는 [할당할 업로드 버퍼의 크기 결정](#) 단원을 참조하십시오.

Important

재설정하는 캐시 디스크에 아직 Amazon S3에 업로드하지 않은 데이터가 있는 경우, 해당 데이터가 손실될 수 있습니다. 캐시 디스크를 재설정한 후에는 구성된 캐시 디스크가 게이트웨이에 남아 있지 않으므로 캐시 디스크를 최소 한 개 구성하여 게이트웨이가 제대로 작동하도록 해야 합니다.

캐시 디스크를 재설정하려면 이 단원 후반부의 절차를 참조하십시오.

디스크를 종료한 후 다시 추가하려면

1. 게이트웨이를 종료합니다. 게이트웨이를 종료하는 방법에 대한 정보는 [게이트웨이 VM 종료](#) 단원을 참조하십시오.
2. 디스크를 다시 호스트에 추가하고 디스크의 디스크 노드 번호가 변경되지 않았는지 확인합니다. 디스크를 추가하는 방법에 대한 정보는 [할당할 업로드 버퍼의 크기 결정](#) 단원을 참조하십시오.

3. 게이트웨이를 다시 시작합니다. 게이트웨이를 다시 시작하는 방법에 대한 정보는 [게이트웨이 VM 종료](#) 단원을 참조하십시오.

게이트웨이가 다시 시작된 후 캐시 디스크의 상태를 확인할 수 있습니다. 디스크의 상태는 다음 중 한 가지에 해당할 수 있습니다.

- 존재함 - 디스크를 사용할 수 있습니다.
- 누락 - 디스크가 게이트웨이에 연결되어 있지 않습니다.
- 불일치 - 부정확한 메타데이터가 있는 디스크가 디스크 노드를 차지하고 있거나 디스크 콘텐츠가 손상되었습니다.

캐시 디스크를 재설정하고 재구성하려면

1. 앞서 표시된 디스크 오류가 발생했습니다. 오류 메시지에서 Reset Cache Disk(캐시 디스크 재설정)를 선택합니다.
2. 게이트웨이 구성 페이지에서 캐시 스토리지용 디스크를 구성합니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 [Tape Gateway 구성](#)을 참조하세요.
3. 캐시 스토리지를 구성한 후에는 이전 절차에서 설명한 대로 게이트웨이를 종료하고 다시 시작합니다.

다시 시작하면 게이트웨이가 복구됩니다. 그 다음에 캐시 디스크의 상태를 확인할 수 있습니다.

캐시 디스크의 상태를 확인하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 해당 게이트웨이를 선택합니다.
3. 작업에서 로컬 스토리지 구성을 선택하여 로컬 스토리지 구성 대화 상자를 표시합니다. 이 대화 상자는 게이트웨이에 있는 모든 로컬 디스크를 표시합니다.

디스크 옆에 캐시 디스크 노드 상태가 표시됩니다.

Note

복구 절차를 완료하지 않으면 게이트웨이가 로컬 스토리지를 구성하라는 내용의 배너를 표시합니다.

복구 불가능한 테이프 문제 해결

가상 테이프에 예기치 않게 장애가 발생하는 경우 Storage Gateway는 장애가 발생한 가상 테이프의 상태를 `IRRECOVERABLE` 취할 조치는 상황에 따라 달라집니다. 아래와 같이 겪을 수 있는 문제와 이 문제를 해결하는 방법에 대한 정보를 얻을 수 있습니다.

테이프에서 데이터를 복구해야 합니다. IRRECOVERABLE

상태가 `IRRECOVERABLE` 다음과 같은 가상 테이프가 있고 해당 가상 테이프를 사용해야 하는 경우 다음 중 하나를 시도해 보십시오.

- 활성화된 Tape Gateway가 없는 경우, 새로 활성화합니다. 자세한 내용은 [게이트웨이 생성](#)을 참조하십시오.
- 복구 불가능한 테이프가 포함된 Tape Gateway를 비활성화하고 복구 시점에서 새 Tape Gateway로 테이프를 복구합니다. 자세한 내용은 [장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우](#) 단원을 참조하십시오.

Note

새 테이프 게이트웨이를 사용하려면 iSCSI 이니시에이터 및 백업 애플리케이션을 재구성해야 합니다. 자세한 내용은 [VTL 디바이스 연결](#) 단원을 참조하십시오.

보관되지 않은 `IRRECOVERABLE` 테이프는 필요하지 않습니다.

상태가 `IRRECOVERABLE` 다음과 같은 가상 테이프가 있고 필요하지 않으며 테이프가 보관된 적이 없는 경우에는 테이프를 삭제해야 합니다. 자세한 내용은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.

게이트웨이의 캐시 디스크에 장애가 발생한 경우

게이트웨이에 있는 하나 이상의 캐시 디스크에 오류가 발생하는 경우, 게이트웨이가 가상 테이프 및 볼륨에 읽기 및 쓰기 작업이 수행되지 않도록 막습니다. 정상 기능을 재개하려면 다음과 같이 게이트웨이를 다시 구성하십시오.

- 캐시 디스크를 액세스할 수 없거나 사용할 수 없으면, 게이트웨이 구성에서 디스크를 삭제합니다.
- 캐시 디스크를 액세스할 수 없거나 사용할 수 없으면, 게이트웨이에 이를 다시 연결합니다.

Note

캐시 디스크를 삭제하면 게이트웨이가 정상 기능을 재개할 때 클린 데이터(즉, 캐시 디스크 및 Amazon S3에 있는 데이터가 동기화된 데이터)가 있는 테이프 또는 볼륨을 계속해서 사용할 수 있습니다. 예를 들어 게이트웨이에 캐시 디스크가 세 개 있는데 두 개를 삭제하면 문제가 없는 테이프나 볼륨은 상태가 됩니다. AVAILABLE 다른 테이프와 볼륨은 IRRECOVERABLE 상태가 됩니다.

임시 디스크를 게이트웨이의 캐시 디스크로 사용하거나 임시 디스크에 캐시 디스크를 탑재하는 경우, 게이트웨이를 닫으면 캐시 디스크를 잃게 됩니다. 캐시 디스크 및 Amazon S3가 동기화되지 않은 상태에서 게이트웨이를 닫으면 데이터가 손실됩니다. 따라서, 임시 드라이브나 디스크를 사용하지 않는 것이 좋습니다.

고가용성 상태 알림

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

고가용성 문제 해결

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

주제

- [상태 알림](#)
- [지표](#)

상태 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 시작될 수 있습니다.

취할 조치

게이트웨이가 이러한 환경에서 실행되는 경우 HealthCheckFailure 알림이 있는지 확인하고 VM에 대한 VMware 이벤트 로그를 참조하십시오.

알림: HealthCheckFailure

VMware vSphere HA에 대한 게이트웨이의 경우 상태 확인에 실패하고 VM 다시 시작을 요청하면 HealthCheckFailure 알림을 받을 수 있습니다. 이 이벤트는 AvailabilityMonitorTest 알림으로 표시된 가용성을 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 AWS Support.

알림: AvailabilityMonitorTest

VMware vSphere HA의 게이트웨이의 경우 VMware에서 [가용성 및 애플리케이션 모니터링 시스템 테스트를 실행](#)할 때 AvailabilityMonitorTest 알림을 받을 수 있습니다.

지표

AvailabilityNotifications 지표는 모든 게이트웨이에서 사용할 수 있습니다. 이 지표는 게이트웨이에 의해 생성된 가용성 관련 상태 알림의 개수입니다. Sum 통계를 사용하여 게이트웨이에 가용성 관련 이벤트가 발생하는지 여부를 확인할 수 있습니다. 이벤트에 대한 자세한 내용은 구성된 CloudWatch 로그 그룹에 문의하십시오.

Tape Gateway 모범 사례

이 섹션에는 게이트웨이, 로컬 디스크, 스냅샷 및 데이터 작업에 대한 모범 사례에 대한 정보를 제공하는 다음 주제가 포함되어 있습니다. 이 섹션에 설명된 정보를 숙지하고 에 문제가 발생하지 않도록 다음 지침을 따르도록 하는 것이 좋습니다 AWS Storage Gateway. 배포 시 발생할 수 있는 일반적인 문제를 진단하고 해결하는 방법에 대한 자세한 내용은 섹션을 참조하세요 [게이트웨이 문제 해결](#).

주제

- [모범 사례: 데이터 복구](#)
- [불필요한 리소스 정리](#)

모범 사례: 데이터 복구

드물긴 하지만 게이트웨이에 복구 불가능한 장애가 발생할 수 있습니다. 그러한 장애는 가상 머신 (VM), 게이트웨이 자체, 로컬 스토리지 등에서 발생할 수 있습니다. 장애가 발생하면 이어지는 적절한 단원의 지침에 따라 테이프를 복구하는 것이 좋습니다.

Important

Storage Gateway는 하이퍼바이저 또는 EC2 Amazon Machine Image()에서 생성된 스냅샷에서 게이트웨이 VM 복구를 지원하지 않습니다AMI. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 다음 지침에 따라 새 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다.

주제

- [가상 머신이 예기치 않게 종료된 상황에서 복구하기](#)
- [장애가 있는 게이트웨이 또는 VM에서 데이터 복구](#)
- [복구할 수 없는 테이프에서 데이터 복구](#)
- [장애가 있는 캐시 디스크에서 데이터 복구](#)
- [액세스할 수 없는 데이터 센터에서 데이터 복구](#)

가상 머신이 예기치 않게 종료된 상황에서 복구하기

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

- 정전으로 인해 네트워크 연결에 문제가 발생하면 그 문제를 해결할 수 있습니다. 네트워크 연결을 테스트하는 방법에 대한 정보는 [인터넷에 대한 게이트웨이 연결 테스트](#) 섹션을 참조하세요.
- 테이프 설정의 경우 게이트웨이에 연결할 수 있게 되면 테이프가 BOOTSTRAPPING 상태가 됩니다. 이 기능을 사용하면 로컬에 저장된 데이터를 와 계속 동기화할 수 있습니다 AWS. 이 상태에 대한 자세한 내용은 [테이프 상태 이해](#) 단원을 참조하십시오.
- 게이트웨이가 제대로 작동하지 않고 예기치 않은 종료로 인해 볼륨 또는 테이프에서 문제가 발생하는 경우, 데이터를 복구할 수 있습니다. 데이터를 복구하는 방법에 대한 자세한 내용은 다음 중 해당되는 상황과 관련된 단원을 참조하십시오.

장애가 있는 게이트웨이 또는 VM에서 데이터 복구

Tape Gateway 또는 하이퍼바이저 호스트에 복구할 수 없는 장애가 발생하면 다음 절차에 따라 장애가 있는 Tape Gateway에서 다른 Tape Gateway로 테이프를 복구할 수 있습니다.

1. 복구 대상으로 사용할 Tape Gateway를 지정하거나 새로 생성합니다.
2. 장애가 있는 게이트웨이를 비활성화합니다.
3. 복구하려는 각 테이프에 대한 복구 테이프를 생성하고 대상 Tape Gateway를 지정합니다.
4. 장애가 있는 Tape Gateway를 삭제합니다.

장애가 있는 Tape Gateway에서 다른 Tape Gateway로 테이프를 복구하는 방법에 대한 자세한 내용은 [장애가 있는 Tape Gateway에서 가상 테이프를 복구해야 하는 경우](#) 섹션을 참조하세요.

복구할 수 없는 테이프에서 데이터 복구

테이프에 장애가 발생하고 테이프 상태가 인 경우 다음 옵션 중 하나를 사용하여 상황에 따라 데이터를 복구하거나 장애를 해결하는 IRRECOVERABLE 것이 좋습니다.

- 복구 불가능한 테이프에 있는 데이터가 필요한 경우, 해당 테이프를 새로운 게이트웨이로 복구할 수 있습니다.

- 테이프에 있는 데이터가 필요 없게 된 경우, 이 테이프를 아카이브에 보관한 적이 없다면 Tape Gateway에서 이 테이프를 간단히 삭제할 수 있습니다.

테이프가 인 경우 데이터를 복구하거나 오류를 해결하는 방법에 대한 자세한 내용은 섹션을 [IRRECOVERABLE참조하세요 복구 불가능한 테이프 문제 해결](#).

장애가 있는 캐시 디스크에서 데이터 복구

캐시 디스크에 장애가 발생하면 다음 절차에 따라 처한 상황에 맞는 방법으로 데이터를 복구하는 것이 좋습니다.

- 호스트에서 캐시 디스크가 제거되어 장애가 발생한 경우, 게이트웨이를 종료하고 디스크를 다시 추가한 후 게이트웨이를 다시 시작합니다.
- 캐시 디스크가 손상되거나 캐시 디스크에 액세스할 수 없는 경우, 게이트웨이를 종료하고 캐시 디스크를 재설정하고 캐시 스토리지용 디스크를 재구성한 후 게이트웨이를 다시 시작합니다.

자세한 내용은 [장애가 있는 캐시 디스크에서 가상 테이프를 복구해야 하는 경우](#) 섹션을 참조하세요.

액세스할 수 없는 데이터 센터에서 데이터 복구

어떤 이유로든 게이트웨이 또는 데이터 센터에 액세스할 수 없게 되면 다른 데이터 센터의 다른 게이트웨이로 데이터를 복구하거나 Amazon EC2 인스턴스에서 호스팅되는 게이트웨이로 복구할 수 있습니다. 다른 데이터 센터에 액세스할 수 없는 경우 Amazon EC2 인스턴스에서 게이트웨이를 생성하는 것이 좋습니다. 생성 방법은 데이터를 복구하는 게이트웨이 유형에 따라 다릅니다.

액세스할 수 없는 데이터 센터의 Tape Gateway에서 데이터를 복구하려면

1. Amazon EC2 호스트에서 새 Tape Gateway를 생성하고 활성화합니다. 자세한 내용은 [Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포](#) 단원을 참조하십시오.
2. 데이터 센터의 소스 게이트웨이에서 Amazon에서 생성한 새 게이트웨이로 테이프를 복구합니다. EC2 자세한 내용은 섹션을 참조하세요 [복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우](#).

테이프를 새 Amazon EC2 게이트웨이로 덮어야 합니다.

불필요한 리소스 정리

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

Tape Gateway를 계속해서 사용할 계획이라면 [추가 정보](#)에서 추가 정보를 확인합니다.

필요 없는 리소스를 정리하려면

1. 게이트웨이의 가상 테이프 라이브러리(VTL)와 아카이브 모두에서 테이프를 삭제합니다. 자세한 내용은 [게이트웨이 삭제 및 관련 리소스 제거](#) 단원을 참조하십시오.
 - a. 게이트웨이의 에 RETRIEVED 상태가 있는 모든 테이프를 보관합니다VTL. 지침은 [테이프 보관](#) 단원을 참조하십시오.
 - b. 게이트웨이의 에서 나머지 테이프를 삭제합니다VTL. 지침은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.
 - c. 아카이브에 있는 테이프를 모두 삭제합니다. 지침은 [Tape Gateway에서 가상 테이프 삭제](#) 단원을 참조하십시오.
2. Tape Gateway를 계속해서 사용할 계획이 아니라면 삭제합니다. 이에 관한 지침은 [게이트웨이 삭제 및 관련 리소스 제거](#) 지침을 참조하세요.
3. 온프레미스 호스트에서 Storage Gateway VM을 삭제합니다. Amazon EC2 인스턴스에서 게이트웨이를 생성한 경우 인스턴스를 종료합니다.

추가 Storage Gateway 리소스

이 섹션에서는 게이트웨이 및 Storage Gateway 할당량을 설정하거나 관리하는 데 도움이 되는 AWS 및 타사 소프트웨어, 도구 및 리소스에 대해 설명합니다.

주제

- [게이트웨이 VM 호스트 배포 및 구성](#) - 게이트웨이에 가상 머신 호스트를 배포하고 구성하는 방법을 알아봅니다.
- [Tape Gateway 스토리지 리소스 작업](#) - 로컬 디스크 제거, Amazon EBS 볼륨 관리, 가상 테이프 라이브러리 디바이스 작업, 가상 테이프 라이브러리의 테이프 관리 등 Tape Gateway 스토리지 리소스와 관련된 절차에 대해 알아봅니다.
- [게이트웨이 활성화 키 받기](#) - 새 게이트웨이를 배포할 때 제공해야 하는 활성화 키를 어디에서 찾을 수 있는지 알아봅니다.
- [iSCSI 이니시에이터 연결](#) - Internet Small Computer System Interface(iVTL) 대상으로 노출되는 볼륨 또는 가상 테이프 라이브러리(SCSI) 디바이스로 작업하는 방법을 알아봅니다.
- [Storage AWS Direct Connect Gateway와 함께 사용](#) - 온프레미스 게이트웨이와 AWS 클라우드 간에 전용 네트워크 연결을 생성하는 방법을 알아봅니다.
- [Tape Gateway에 대한 포트 요구 사항](#) - Tape Gateway에 필요한 네트워크 포트에 대한 특정 정보를 찾습니다.
- [게이트웨이 어플라이언스의 IP 주소 가져오기](#) - 새 게이트웨이를 배포할 때 제공해야 하는 게이트웨이의 가상 머신 호스트 IP 주소를 어디에서 찾을 수 있는지 알아봅니다.
- [Storage Gateway 리소스 및 리소스에 대한 이해 IDs](#) - 가 Storage Gateway 에서 생성한 리소스 및 하위 리소스를 AWS 식별하는 방법을 알아봅니다.
- [Storage Gateway 리소스에 태그를 지정](#) - 메타데이터 태그를 사용하여 리소스를 분류하고 더 쉽게 관리할 수 있는 방법을 알아봅니다.
- [Storage Gateway용 오픈 소스 구성 요소 작업](#) - Storage Gateway 기능을 제공하는 데 사용되는 타사 도구 및 라이선스에 대해 알아봅니다.
- [AWS Storage Gateway 할당량](#) - 테이프 크기 및 수량에 대한 최대 제한, 로컬 디스크 크기 권장 사항을 포함하여 Tape Gateway의 제한 및 할당량에 대해 알아봅니다.

게이트웨이 VM 호스트 배포 및 구성

이 섹션의 주제에서는, VMwareHyper-V 또는 Linux에서 실행되는 온프레미스 어플라이언스와 AWS 클라우드의 Amazon EC2 인스턴스에서 실행되는 어플라이언스를 포함하여 Storage Gateway KVM어플라이언스의 가상 머신 호스트를 설정하고 관리하는 방법을 설명합니다.

주제

- [Tape Gateway용 기본 Amazon EC2 호스트 배포](#) - 기본 사양을 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Tape Gateway 를 배포하고 활성화하는 방법에 대해 알아봅니다.
- [Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포](#) - 사용자 지정 설정을 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Tape Gateway 를 배포하고 활성화하는 방법에 대해 알아봅니다.
- [Amazon EC2 인스턴스 메타데이터 옵션 수정](#) - IMDS 버전 1(IMDSv1)을 사용하거나 모든 메타데이터 요청에서 IMDS 버전 2()를 사용하도록 요구하는 수신 메타데이터 요청을 수락하도록 Amazon EC2 게이트웨이 인스턴스를 구성하는 방법에 대해 알아봅니다IMDSv2.
- [VM 시간을 Hyper-V 또는 Linux KVM 호스트 시간과 동기화](#) - 온프레미스 Hyper-V 또는 Linux KVM 게이트웨이 가상 머신의 시간을 보고 Network Time Protocol(NTP) 서버와 동기화하는 방법에 대해 알아봅니다.
- [VM 시간과 VMware 호스트 시간 동기화](#) - VMware 게이트웨이 가상 머신의 호스트 시간을 확인하고 필요한 경우 시간을 설정하고 호스트가 Network Time Protocol(NTP) 서버에 시간을 자동으로 동기화하도록 구성하는 방법에 대해 알아봅니다.
- [VMware 호스트에서 파라가상화 구성](#) - Storage Gateway 어플라이언스에 대한 VMware 호스트 플랫폼이 가상 인터넷 소형 컴퓨터 시스템 인터페이스 프로토콜(iSCSI) 컨트롤러를 사용하도록 구성하는 방법에 대해 알아봅니다.
- [게이트웨이용 네트워크 어댑터 구성](#) - VMXNET3 (10GbE) 네트워크 어댑터를 사용하거나 여러 네트워크 어댑터를 사용하여 이중 IP 주소에 액세스할 수 있도록 게이트웨이를 재구성하는 방법에 대해 알아봅니다.
- [Storage Gateway에서 VMware vSphere 고가용성 사용](#) - VMware vSphere 고가용성으로 작동하도록 Storage Gateway를 구성하여 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호하는 방법에 대해 알아봅니다.

Tape Gateway용 기본 Amazon EC2 호스트 배포

이 주제에서는 기본 사양을 사용하여 Amazon EC2 호스트를 배포하는 단계를 나열합니다.

Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스에서 Tape Gateway 를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon Machine Image(AMI)는 커뮤니티 로 사용할 수 있습니다 AMI.

Note

Storage Gateway 커뮤니티AMIs는 에서 게시하고 완전히 지원합니다 AWS. 게시자가 검증된 공급자 AWS인 임을 확인할 수 있습니다.

1. Amazon 를 설정하려면 워크플로의 플랫폼 옵션 섹션에서 AmazonEC2을 호스트 플랫폼으로 EC2instance선택합니다. Amazon EC2 인스턴스 구성에 대한 지침은 [Tape Gateway를 호스팅하는 Amazon EC2 인스턴스 배포](#) .
2. 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 열고 인스턴스 유형 , 네트워크 설정 및 스토리지 구성 과 같은 추가 설정을 사용자 지정합니다.
3. 필요에 따라 Storage Gateway 콘솔에서 기본 설정 사용을 선택하여 기본 구성으로 Amazon EC2 인스턴스를 배포할 수 있습니다.

기본 설정 사용에서 생성하는 Amazon EC2 인스턴스의 기본 사양은 다음과 같습니다.

- 인스턴스 유형 - m5.xlarge
- 네트워크 설정
 - 에서 VPC EC2 인스턴스를 실행할 를 VPC선택합니다.
 - 서브넷 의 경우 EC2 인스턴스를 시작할 서브넷을 지정합니다.

Note

VPC 서브넷은 VPC 관리 콘솔에서 퍼블릭 IPv4 주소 자동 할당 설정이 활성화된 경우에만 드롭다운에 표시됩니다.

- 퍼블릭 IP 자동 할당 - 활성화됨

EC2 보안 그룹이 생성되어 EC2 인스턴스와 연결됩니다. 보안 그룹에는 다음과 같은 인바운드 포트 규칙이 적용됩니다.

Note

게이트웨이 활성화 중에는 포트 80이 열려 있어야 합니다. 활성화 후에는 포트가 즉시 닫힙니다. 그런 다음 선택한 의 다른 포트를 통해서만 EC2 인스턴스에 액세스할 수 있습니다VPC.

게이트웨이의 iSCSI 대상은 게이트웨이VPC와 동일한 의 호스트에서만 액세스할 수 있습니다. 외부 호스트에서 iSCSI 대상에 액세스해야 하는 경우 적절한 보안 그룹 규칙을 업데이트VPC해야 합니다.

언제든지 Amazon EC2 인스턴스 세부 정보 페이지로 이동하여 보안 을 선택하고, 보안 그룹 세부 정보 로 이동하고, 보안 그룹 ID를 선택하여 보안 그룹을 편집할 수 있습니다.

포트	프로토콜	파일 시스템 프로토콜				
80	TCP	HTTP 활성화에 대한 액세스				
3260	TCP	iSCSI				

• 스토리지 구성

기본 설정	AMI 루트 볼륨	볼륨 2 캐시	볼륨 3 캐시			
디바이스 이름		'/dev/sdb'	'/dev/sdc'			
크기	80GiB	165GiB	150GiB			
볼륨 유형	gp3	gp3	gp3			
IOPS	3000	3000	3000			

기본 설정	AMI 루트 볼륨	볼륨 2 캐시	볼륨 3 캐시			
종료 시 삭제	예	예	예			
Encrypted	아니요	아니요	아니요			
처리량	125	125	125			

Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포

Amazon Elastic Compute Cloud(AmazonEC2) 인스턴스에서 Tape Gateway 를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon Machine Image(AMI)는 커뮤니티 로 사용할 수 있습니다 AMI.

Note

Storage Gateway 커뮤니티AMIs는 에서 게시하고 완전히 지원합니다 AWS. 게시자가 검증된 공급자 AWS인 임을 확인할 수 있습니다.

Tape Gateway 는 다음 명명 규칙을 AMIs 사용합니다. 각 버전 릴리스에서 AMI 이름 변경에 추가된 버전 번호입니다.

`aws-storage-gateway-CLASSIC-2.9.0`

Amazon EC2 인스턴스를 배포하여 Tape Gateway를 호스팅하려면

1. Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 [Tape Gateway 설정](#)을 참조하세요. 플랫폼 옵션 섹션에 도달하면 AmazonEC2을 호스트 플랫폼 으로 선택한 다음 다음 다음 단계에 따라 Tape Gateway 를 호스팅할 Amazon EC2 인스턴스를 시작합니다.
2. 인스턴스 시작을 AWS Storage Gateway AMI 선택하여 추가 설정을 구성할 수 있는 Amazon EC2 콘솔에서 템플릿을 엽니다.

Quicklaunch를 사용하여 기본 설정으로 Amazon EC2 인스턴스를 시작합니다. Amazon EC2 Quicklaunch 기본 세분화에 대한 자세한 내용은 [Amazon용 Quicklaunch 구성 사양을 참조하세요 EC2](#).

3. 이름 에 Amazon EC2 인스턴스의 이름을 입력합니다. 인스턴스를 배포한 후 이 이름을 검색하여 Amazon EC2 콘솔의 목록 페이지에서 인스턴스를 찾을 수 있습니다.
4. 인스턴스 유형 섹션의 인스턴스 유형에서 인스턴스의 하드웨어 구성을 선택합니다. 하드웨어 구성은 게이트웨이를 지원하기 위한 특정 최소 요구 사항을 충족해야 합니다. 게이트웨이가 제대로 작동하기 위한 최소 하드웨어 요구 사항을 충족하는 m5.xlarge 인스턴스 유형으로 시작하는 것이 좋습니다. 자세한 내용은 [Amazon EC2 인스턴스 유형에 대한 요구 사항](#) 단원을 참조하십시오.

필요하다면 시작한 후 인스턴스 크기를 조정할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 크기 조정을 참조하세요](#).

Note

특정 인스턴스 유형, 특히 i3 는 NVMe SSD 디스크를 EC2사용합니다. 이러한 경우 Tape Gateway를 시작하거나 중지할 때 문제가 발생할 수 있습니다. 예를 들어, 캐시에서 데이터가 손실될 수 있습니다. CachePercentDirty Amazon CloudWatch 지표를 모니터링하고 해당 파라미터가 인 경우에만 시스템을 시작하거나 중지합니다. 게이트웨이의 지표 모니터링에 대한 자세한 내용은 CloudWatch 설명서의 [Storage Gateway 지표 및 차원](#)을 참조하세요.

5. 키 페어(로그인) 섹션에서 키 페어 이름 - 필수에서 인스턴스에 안전하게 연결하는 데 사용할 키 페어를 선택합니다. 필요한 경우 키 페어를 새로 생성할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 [키 페어 생성](#)을 참조하세요.
6. 네트워크 설정 섹션에서 사전 구성된 설정을 검토하고 편집을 선택하여 다음 필드를 변경합니다.
 - a. VPC - 필수 에서 Amazon EC2 인스턴스를 시작할 VPC 을 선택합니다. 자세한 내용은 [Amazon Virtual Private Cloud 사용 설명서의 Amazon VPC 작동 방식](#)을 참조하세요. Amazon Virtual Private Cloud
 - b. (선택 사항) 서브넷 에서 Amazon EC2 인스턴스를 시작할 서브넷을 선택합니다.
 - c. 퍼블릭 IP 자동 할당(Auto-assign Public IP)의 경우 활성화(Enable)를 선택합니다.
7. 방화벽(보안 그룹) 하위 섹션에서 사전 구성된 설정을 검토합니다. 원하는 경우 Amazon EC2 인스턴스에 대해 생성할 새 보안 그룹의 기본 이름과 설명을 변경하거나 기존 보안 그룹에서 방화벽 규칙을 대신 적용하도록 선택할 수 있습니다.
8. 인바운드 보안 그룹 규칙 하위 섹션에서 클라이언트가 인스턴스에 연결하는 데 사용할 포트를 여는 방화벽 규칙을 추가합니다. Tape Gateway에 필요한 포트에 대한 자세한 내용은 [포트 요구 사항](#)을 참조하세요. 방화벽 규칙 추가에 대한 자세한 정보는 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 [보안 그룹 규칙](#)을 참조하세요.

Note

Tape Gateway를 사용하려면 인바운드 트래픽에 대해 TCP 포트 80을 열고 게이트웨이 활성화 중에 일회성 HTTP 액세스를 해야 합니다. 활성화한 후에는 이 포트를 닫을 수 있습니다.

또한 iSCSI 액세스를 위해 TCP 포트 3260을 열어야 합니다.

9. 고급 네트워크 구성 하위 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
10. 스토리지 구성 섹션에서 새 볼륨 추가를 선택하여 게이트웨이 인스턴스에 스토리지를 추가합니다.

Important

사전 구성된 루트 EBS 볼륨 외에도 캐시 스토리지에 대해 최소 165GiB 용량을 가진 Amazon EBS 볼륨 하나 이상과 업로드 버퍼에 대해 최소 150GiB 용량을 가진 Amazon 볼륨 하나를 추가해야 합니다. 성능을 높이려면 캐시 스토리지에 대해 각각 150GiB 이상의 여러 EBS 볼륨을 할당하는 것이 좋습니다.

11. 고급 세부 정보 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
12. 인스턴스 시작을 선택하여 구성된 설정으로 새 Amazon EC2 게이트웨이 인스턴스를 시작합니다.
13. 새 인스턴스가 성공적으로 시작되었는지 확인하려면 Amazon EC2 콘솔의 인스턴스 페이지로 이동하여 이름으로 새 인스턴스를 검색합니다. 인스턴스 상태가 녹색 확인 표시와 함께 실행 중으로 표시되고 상태 검사가 완료되어 녹색 확인 표시가 나타나는지 확인합니다.
14. 세부 정보 페이지에서 해당 인스턴스를 선택합니다. 인스턴스 요약 섹션에서 퍼블릭 IPv4 주소를 복사한 다음 Storage Gateway 콘솔의 게이트웨이 설정 페이지로 돌아가 Tape Gateway 설정을 다시 시작합니다.

Storage Gateway 콘솔을 사용하거나 AWS Systems Manager 파라미터 스토어를 쿼리하여 Tape Gateway를 시작하는 데 사용할 AMI ID를 결정할 수 있습니다.

AMI ID를 확인하려면 다음 중 하나를 수행합니다.

- Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 [Tape Gateway 설정](#)을 참조하세요. 플랫폼 옵션 섹션에 도달하면 AmazonEC2을 호스트 플랫폼으로 선택한 다음 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 템플릿을 엽니다 AWS Storage Gateway AMI.

EC2 커뮤니티 AMI 페이지로 리디렉션됩니다. 이 페이지에서는 에서 AWS 리전의 AMI ID를 볼 수 있습니다URL.

- Systems Manager 파라미터 스토어를 쿼리합니다. AWS CLI 또는 Storage Gateway를 사용하여 네임스페이스 아래의 Systems Manager 퍼블릭 파라미터를 API 쿼리할 수 있습니다/aws/service/storagegateway/ami/VTL/latest. 예를 들어 다음 CLI 명령을 사용하면 AWS 리전 지정한 AMI의 현재 ID가 반환됩니다.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/latest
```

CLI 명령은 다음과 유사한 출력을 반환합니다.

```
{
  "Parameter": {
    "Type": "String",
    "LastModifiedDate": 1561054105.083,
    "Version": 4,
    "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/latest",
    "Name": "/aws/service/storagegateway/ami/VTL/latest",
    "Value": "ami-123c45dd67d891000"
  }
}
```

Amazon EC2 인스턴스 메타데이터 옵션 수정

인스턴스 메타데이터 서비스 (IMDS) 는 Amazon 인스턴스 메타데이터에 대한 보안 액세스를 제공하는 온 EC2 인스턴스 구성 요소입니다. IMDS버전 1 (IMDSv1) 을 사용하는 수신 메타데이터 요청을 수락하거나 모든 메타데이터 요청에 IMDS 버전 2 (IMDSv2) 를 사용하도록 요구하는 인스턴스를 구성할 수 있습니다. IMDSv2세션 지향 요청을 사용하고 액세스를 시도하는 데 사용될 수 있는 여러 유형의 취약성을 완화합니다. IMDS 에 대한 IMDSv2 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서의 [인스턴스 메타데이터 서비스 버전 2의 작동 방식](#)을 참조하십시오.

Storage Gateway를 호스팅하는 모든 Amazon EC2 인스턴스에 IMDSv2 요구하는 것이 좋습니다. IMDSv2새로 시작된 모든 게이트웨이 인스턴스에는 기본적으로 필요합니다. IMDSv1메타데이터 요청을 수락하도록 구성된 기존 인스턴스가 있는 경우 Amazon Elastic Compute Cloud 사용 설명서의 [사](#)

[용 필요를](#) 참조하여 사용을 요구하도록 인스턴스 메타데이터 옵션을 수정하는 지침을 참조하십시오. IMDSv2. IMDSv2 이 변경 사항을 적용할 때는 인스턴스를 재부팅할 필요가 없습니다.

VM 시간을 Hyper-V 또는 Linux KVM 호스트 시간과 동기화

에 배포된 게이트웨이의 경우 VMware ESXi 하이퍼바이저 호스트 시간을 설정하고 가상 머신 시간을 호스트와 동기화하는 것으로 시간 변동을 피할 수 있습니다. 자세한 내용은 [VM 시간과 VMware 호스트 시간 동기화](#) 단원을 참조하십시오. Microsoft Hyper-V 또는 Linux 에 배포된 게이트웨이의 경우 다음 절차에 따라 가상 머신 시간을 주기적으로 확인하는 KVM 것이 좋습니다.

하이퍼바이저 게이트웨이 가상 머신의 시간을 보고 Network Time Protocol(NTP) 서버와 동기화하려면

- 게이트웨이의 로컬 콘솔에 로그인합니다.
 - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)를 참조하십시오.
 - Linux 커널 기반 Virtual Machine용 로컬 콘솔에 로그인하는 방법에 대한 자세한 내용은 섹션을 참조하세요(KVM). [Linux를 사용하여 Gateway Local Console에 액세스 KVM](#)
- Storage Gateway 구성 기본 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 관리를 선택합니다.
- 시스템 시간 관리 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 보기 및 동기화를 선택합니다.

게이트웨이 로컬 콘솔은 현재 시스템 시간을 표시하고 NTP 서버에서 보고한 시간과 비교한 다음 두 시간 간의 정확한 불일치를 초 단위로 보고합니다.

- 시간 불일치가 60초를 초과하는 경우 **y**를 입력하여 시스템 시간을 NTP 시간과 동기화합니다. 그렇지 않은 경우 **n**을 입력합니다.

시간 동기화에는 몇 분 정도 걸릴 수 있습니다.

VM 시간과 VMware 호스트 시간 동기화

게이트웨이를 성공적으로 활성화하려면 VM 시간을 호스트 시간과 동기화해야 하고 호스트 시간을 올바르게 설정해야 합니다. 이 단원에서는 먼저 VM의 시간을 호스트 시간과 동기화합니다. 그런 다음 호스트 시간을 확인하고 필요한 경우 호스트 시간을 설정하고 호스트가 Network Time Protocol(NTP) 서버와 시간을 자동으로 동기화하도록 구성합니다.

⚠ Important

VM 시간을 호스트 시간과 동기화하려면 게이트웨이를 성공적으로 활성화해야 합니다.

VM 시간을 호스트 시간과 동기화하려면

1. VM 시간을 구성합니다.

- a. vSphere 클라이언트에서 애플리케이션 창 왼쪽에 있는 패널에서 게이트웨이 VM의 이름을 마우스 오른쪽 버튼으로 클릭하여 VM의 컨텍스트 메뉴를 연 다음 설정 편집을 선택합니다.

그러면 Virtual Machine Properties(가상 머신 속성) 대화 상자가 열립니다.

- b. 옵션 탭을 선택한 다음 옵션 목록에서 VMware 도구를 선택합니다.
- c. 가상 머신 속성 대화 상자 오른쪽의 고급 섹션에서 호스트와 게스트 시간 동기화 옵션을 확인한 다음 확인을 선택합니다.

그러면 VM이 자체 시간을 호스트와 동기화합니다.

2. 호스트 시간을 구성합니다.

호스트 클럭의 시간이 올바르게 설정되어 있는지 확인하는 것이 중요합니다. 호스트 클럭을 구성하지 않은 경우 다음 단계를 수행하여 NTP 서버와 설정하고 동기화합니다.

- a. VMware vSphere 클라이언트에서 왼쪽 패널의 vSphere 호스트 노드를 선택한 다음 구성 탭을 선택합니다.
- b. 소프트웨어 패널에서 시간 구성을 선택한 다음 속성 링크를 선택합니다.

그러면 Time Configuration(시간 구성) 대화 상자가 나타납니다.

- c. 날짜 및 시간 에서 vSphere 호스트의 날짜 및 시간을 설정합니다.
- d. 호스트가 시간을 NTP 서버에 자동으로 동기화하도록 구성합니다.
 - i. 시간 구성 대화 상자에서 옵션을 선택한 다음 NTP 대몬(ntpd) 옵션 대화 상자에서 왼쪽 패널에서 NTP 설정을 선택합니다.
 - ii. 추가를 선택하여 새 NTP 서버를 추가합니다.
 - iii. NTP 서버 추가 대화 상자에서 NTP 서버의 IP 주소 또는 정규화된 도메인 이름을 입력한 다음 확인을 선택합니다.

pool.ntp.org 를 도메인 이름으로 사용할 수 있습니다.

- iv. NTP Daemon(ntpd) 옵션 대화 상자에서 왼쪽 패널에서 일반을 선택합니다.
- v. 서비스 명령어에서 시작을 선택하여 서비스를 시작합니다.

이 NTP 서버 참조를 변경하거나 나중에 다른 를 추가하는 경우 새 서버를 사용하려면 서비스를 다시 시작해야 합니다.

- e. 확인을 선택하여 NTP Daemon(ntpd) 옵션 대화 상자를 닫습니다.
- f. 확인을 선택하여 Time Configuration(시간 구성) 대화 상자를 닫습니다.

VMware 호스트에서 파라가상화 구성

다음 절차에서는 Storage Gateway 어플라이언스가 가상 인터넷 소형 컴퓨터 시스템 인터페이스 프로토콜(iSCSI) 컨트롤러를 사용하도록 VMware 호스트 플랫폼을 구성하는 방법을 설명합니다. Paravirtual iSCSI 컨트롤러는 처리량을 높이고 CPU 사용량을 줄일 수 있는 고성능 스토리지 컨트롤러입니다. 이러한 컨트롤러는 고성능 스토리지 환경에 가장 적합합니다. 이렇게 iSCSI 컨트롤러를 구성하면 Storage Gateway 가상 머신이 호스트 운영 체제와 함께 작동하여 게이트웨이 콘솔이 가상 머신에 추가하는 가상 디스크를 식별할 수 있습니다.

Note

게이트웨이 콘솔에서 디스크를 구성할 때 이러한 디스크를 식별하는 데 문제가 발생하지 않도록 하려면 이 단계를 완료해야 합니다.

파라가상화 컨트롤러를 사용하도록 VMware 호스트 플랫폼을 구성하려면

1. VMware vSphere 클라이언트에서 애플리케이션 창 왼쪽의 탐색 창에서 게이트웨이 가상 머신의 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 설정 편집을 선택합니다.
2. 가상 머신 속성 대화 상자에서 하드웨어 탭을 선택합니다.
3. 하드웨어 탭에서 SCSI 컨트롤러 0을 선택한 다음 유형 변경을 선택합니다.
4. SCSI 컨트롤러 유형 변경 대화 상자에서 VMware Paravirtual SCSI 컨트롤러 유형을 선택한 다음 확인을 선택하여 구성을 저장합니다.

게이트웨이용 네트워크 어댑터 구성

기본적으로 Storage Gateway는 E1000 네트워크 어댑터 유형을 사용하도록 구성되지만 VMXNET3 (10GbE) 네트워크 어댑터를 사용하도록 게이트웨이를 재구성할 수 있습니다. Storage Gateway를 한

개 이상의 IP 주소에서 액세스할 수 있도록 구성할 수도 있습니다. 이를 위해서는 게이트웨이가 네트워크 어댑터를 한 개 이상 사용하도록 구성하면 됩니다.

주제

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

VMXNET3 네트워크 어댑터를 사용하도록 게이트웨이 구성

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

Important

를 선택하려면 VMXNET3 게스트 운영 체제 유형이 기타 Linux64여야 합니다.

다음은 VMXNET3 어댑터를 사용하도록 게이트웨이를 구성하는 단계입니다.


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. 에서 게이트웨이 VMware의 컨텍스트(마우스 오른쪽 버튼 클릭) 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 Type(어댑터 유형) 섹션에서 현재 어댑터는 E1000임을 알 수 있습니다. 이 어댑터를 VMXNET3 어댑터로 바꿉니다.
4. E1000 네트워크 어댑터를 선택한 후 제거를 선택합니다. 이 예에서 E1000 네트워크 어댑터는 Network adapter 1(네트워크 어댑터 1)입니다.

 Note

게이트웨이에서 E1000과 VMXNET3 네트워크 어댑터를 동시에 실행할 수 있지만 네트워크 문제가 발생할 수 있으므로 실행하지 않는 것이 좋습니다.

5. 추가를 선택하여 Add Hardware 마법사를 엽니다.
6. Ethernet Adapter(이더넷 어댑터)를 선택한 후 다음을 선택합니다.
7. 네트워크 유형 마법사에서 어댑터 유형으로 **VMXNET3**을 선택한 후 다음을 선택합니다.
8. 가상 머신 속성 마법사의 어댑터 유형 섹션에서 현재 어댑터가 로 설정되어 있는지 확인한 VMXNET3다음 확인을 선택합니다.
9. VMware VSphere 클라이언트에서 게이트웨이를 종료합니다.
10. VMware VSphere 클라이언트에서 게이트웨이를 다시 시작합니다.

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

네트워크용 어댑터를 구성하려면

1. VSphere 클라이언트에서 콘솔 탭을 선택하여 로컬 콘솔을 시작합니다. 이 구성 작업을 위해서는 기본 로그인 자격 증명을 사용하여 게이트웨이의 로컬 콘솔에 로그인해야 합니다. 기본 자격 증명을 사용하여 로그인하는 방법에 대한 자세한 내용은 [기본 자격 증명을 사용하여 로컬 콘솔에 로그인](#)을 참조하세요.
2. 프롬프트에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. 프롬프트에서 해당 숫자를 입력하여 모두 로 재설정을 DHCP선택한 다음 프롬프트에 **y** (예인 경우)를 입력하여 모든 어댑터가 동적 호스트 구성 프로토콜()을 사용하도록 설정합니다DHCP. 사용 가능한 모든 어댑터는 를 사용하도록 설정되어 있습니다DHCP.

게이트웨이가 이미 활성화된 경우, Storage Gateway Management Console에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 게이트웨이를 다시 시작한 후 네트워크가 인터넷에 연결되어 있는

지 테스트해야 합니다. 네트워크 연결을 테스트하는 방법에 대한 자세한 내용은 [게이트웨이가 인터넷에 연결되어 있는지 테스트](#)를 참조하세요.

다중 게이트웨이 구성 NICs

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

- 처리량 극대화 - 네트워크 어댑터에 병목 현상이 발생하는 경우, 처리량을 극대화하고자 할 수 있습니다.
- 애플리케이션 분리 - 애플리케이션이 게이트웨이의 볼륨에 데이터를 기록하는 방식을 분리해야 할 수 있습니다. 예를 들어 중요 스토리지 애플리케이션이 게이트웨이에 정의한 특정 어댑터 한 개를 배타적으로 사용하도록 선택할 수 있습니다.
- 네트워크 제약 조건 - 애플리케이션 환경에서는 게이트웨이가 와 통신하는 네트워크와 다른 격리된 네트워크에서 iSCSI 대상과 해당 대상에 연결하는 이니시에이터를 유지해야 할 수 있습니다 AWS.

일반적인 다중 어댑터 사용 사례에서는 하나의 어댑터가 게이트웨이가 통신하는 경로 AWS (즉, 기본 게이트웨이)로 구성됩니다. 이 하나의 어댑터를 제외하고 이니시에이터는 연결된 iSCSI 대상을 포함하는 어댑터와 동일한 서브넷에 있어야 합니다. 그렇지 않은 경우, 원하는 대상과의 통신이 불가능할 수 있습니다. 대상이와의 통신에 사용되는 것과 동일한 어댑터에 구성된 경우 해당 대상 및 트래픽에 대한 AWS iSCSI AWS 트래픽이 동일한 어댑터를 통해 흐릅니다.

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

- [VMware ESXi 호스트에서 여러 네트워크 어댑터 구성](#)
- [Microsoft Hyper-V 호스트에서 여러 네트워크 어댑터 구성](#)

VMware ESXi 호스트에서 여러 네트워크 어댑터 구성

다음 절차에서는 게이트웨이 VM에 이미 정의된 네트워크 어댑터가 하나 있다고 가정하고 VMware 에 어댑터를 추가하는 방법을 설명합니다ESXi.

VMware ESXi 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이를 종료합니다.

2. VMware vSphere 클라이언트에서 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. 가상 컴퓨터 속성 대화 상자의 하드웨어 탭에서 추가를 선택하여 디바이스를 추가합니다.
5. Add Hardware 마법사의 안내에 따라 네트워크 어댑터를 추가합니다.
 - a. 디바이스 유형 창에서 Ethernet Adapter(이더넷 어댑터)를 선택하여 어댑터를 추가한 후 다음을 선택합니다.
 - b. 네트워크 유형 창에서 전원이 켜질 때 연결이 유형으로 선택되어 있는지 확인한 후 다음을 선택합니다.

Storage Gateway 에서 VMXNET3 네트워크 어댑터를 사용하는 것이 좋습니다. 어댑터 목록에 표시될 수 있는 어댑터 유형에 대한 자세한 내용은 [ESXi 및 vCenter 서버 설명서](#)의 네트워크 어댑터 유형을 참조하세요.

- c. Ready to Complete(완료 준비) 창에서 해당 정보를 검토한 후 Finish(완료)를 선택합니다.
6. VM의 요약 탭을 선택하고 IP 주소 상자 옆에 있는 모두 보기를 선택합니다. 게이트웨이에 액세스할 때 사용할 수 있는 모든 IP 주소가 가상 머신 IP 주소 창에 표시됩니다. 게이트웨이에 두 번째 IP 주소가 표시되는지 확인합니다.

Note

어댑터 변경 사항이 적용되고 VM 요약 정보가 새로 고침되려면 약간의 시간이 걸릴 수 있습니다.

7. Storage Gateway 콘솔에서 게이트웨이의 전원을 켭니다.
8. Storage Gateway의 탐색 창에서 게이트웨이를 선택한 후 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트에 일반적인 로컬 콘솔 작업에 대한 자세한 내용은 섹션을 참조하세요. [VM 로컬 콘솔에서 작업 수행](#)

Microsoft Hyper-V 호스트에서 여러 네트워크 어댑터 구성

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

Microsoft Hyper-V 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

1. Storage Gateway 콘솔에서 게이트웨이를 끕니다.
2. Microsoft Hyper-V Manager의 Virtual Machines 패널에서 게이트웨이 VM을 선택합니다.
3. 게이트웨이 VM이 아직 꺼져 있지 않은 경우 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 끄기를 선택합니다.
4. 게이트웨이 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 설정을 선택합니다.
5. 설정 대화 상자의 하드웨어에서 하드웨어 추가를 선택합니다.
6. 설정 대화 상자 오른쪽에 있는 하드웨어 추가 패널에서 네트워크 어댑터를 선택한 다음 추가를 선택하여 디바이스를 추가합니다.
7. 네트워크 어댑터를 구성한 후 적용을 선택하여 설정을 적용합니다.
8. 설정 대화 상자의 하드웨어에서 새 네트워크 어댑터가 하드웨어 목록에 추가되었는지 확인한 다음 확인을 선택합니다.
9. Storage Gateway 콘솔을 사용하여 게이트웨이를 켭니다.
10. Storage Gateway 콘솔의 탐색 패널에서 게이트웨이를 선택한 다음 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 나열되어 있는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트에 일반적인 로컬 콘솔 작업에 대한 자세한 내용은 섹션을 참조하세요. [VM 로컬 콘솔에서 작업 수행](#)

Storage Gateway에서 VMware vSphere 고가용성 사용

Storage Gateway는 고가용성(VMware HA)과 통합된 애플리케이션 수준 상태 확인을 VMware 통해서 VMware vSphere 고가용성을 제공합니다. 이러한 접근 방식을 통해 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 또한 연결 시간 초과, 파일 공유 또는 볼륨 사용 불가와 같은 소프트웨어 오류로부터 보호할 수 있습니다.

vSphere HA는 중복성을 위해 가상 머신과 가상 머신이 상주하는 호스트를 클러스터에 풀링하여 작동합니다. 클러스터의 호스트가 모니터링되고 장애가 발생하면 장애가 발생한 호스트의 가상 머신이 대

체 호스트에서 다시 시작됩니다. 일반적으로 이러한 복구는 데이터 손실 없이 빠르게 이루어집니다. vSphere HA에 대한 자세한 내용은 VMware 설명서의 [vSphere HA 작동 방식](#)을 참조하세요.

Note

실패한 가상 머신을 다시 시작하고 새 호스트에서 iSCSI 연결을 다시 설정하는 데 필요한 시간은 호스트 운영 체제 및 리소스 로드, 디스크 속도, 네트워크 연결 및 SAN/스토리지 인프라와 같은 여러 요인에 따라 달라집니다. 장애 조치 가동 중지 시간을 최소화하려면 [게이트웨이 성능 최적화](#)에 설명된 권장 사항을 구현합니다.

VMware HA와 함께 Storage Gateway를 사용하려면 다음 작업을 수행하는 것이 좋습니다.

- 클러스터의 한 호스트에만 Storage Gateway VM이 포함된 VMware ESX .ova 다운로드 가능한 패키지를 배포합니다.
- .ova 패키지를 배포할 때 호스트 한 곳에 대해 로컬이 아닌 데이터 스토어를 선택합니다. 그 대신에 클러스터의 모든 호스트에 액세스할 수 있는 데이터 스토어를 사용합니다. 호스트에 대해 로컬인 데이터 스토어를 선택하였는데 호스트에 장애가 생긴 경우에는 데이터 원본이 클러스터 내 기타 호스트에 액세스할 수 없고 다른 호스트에 대한 장애 조치가 성공하지 못할 수 있습니다.
- 장애 조치 중에 이니시에이터가 스토리지 볼륨 대상에서 연결을 끊지 않도록 하려면 운영 체제에 권장되는 iSCSI 설정을 따르세요. 장애 조치 이벤트 중에는 게이트웨이 VM이 장애 조치 클러스터의 새 호스트에서 시작하는 데 몇 초에서 몇 분이 걸릴 수 있습니다. Windows 및 Linux 클라이언트 모두에 권장되는 iSCSI 제한 시간은 장애 조치가 발생하는 데 걸리는 일반적인 시간보다 큼니다. Windows 클라이언트의 제한 시간 설정을 사용자 정의하는 방법에 대한 자세한 내용은 [Windows iSCSI 설정 사용자 지정](#) 단원을 참조하십시오. Linux 클라이언트의 제한 시간 설정을 사용자 정의하는 방법에 대한 자세한 내용은 [Linux iSCSI 설정 사용자 지정](#) 단원을 참조하십시오.
- 클러스터링의 경우, .ova 패키지를 클러스터에 배포한다면 프롬프트 메시지에 따라 호스트를 선택합니다. 또는 클러스터의 호스트에 직접 배포할 수도 있습니다.

다음 주제에서는 VMware HA 클러스터에 Storage Gateway를 배포하는 방법을 설명합니다.

주제

- [HA 클러스터 구성 vSphere VMware](#)
- [Storage Gateway 콘솔에서 .ova 이미지를 다운로드합니다.](#)
- [게이트웨이 배포](#)

- [\(선택 사항\) 클러스터VMs에서 다른 에 대한 재정의 옵션 추가](#)
- [게이트웨이 활성화](#)
- [VMware 고가용성 구성 테스트](#)

HA 클러스터 구성 vSphere VMware

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

다음으로 Storage Gateway 에서 작동하도록 VMware 클러스터를 구성합니다.

VMware 클러스터를 구성하려면

1. 의 클러스터 설정 편집 페이지에서 VM 모니터링이 VM 및 애플리케이션 모니터링에 맞게 구성되어 있는지 VMware vSphere 확인합니다. 이렇게 하려면 각 옵션에 대해 다음 값을 설정합니다.
 - 호스트 실패 응답: 다시 시작 VMs
 - 호스트 격리에 대한 응답: 종료 및 재시작 VMs
 - 를 사용하는 데이터 스토어PDL: 비활성화됨
 - 를 사용하는 데이터 스토어APD: 비활성화됨
 - VM Monitoring(VM 모니터링): VM and Application Monitoring(VM 및 애플리케이션 모니터링)
2. 다음 값을 조정하여 클러스터의 민감도를 미세 조정합니다.
 - 실패 간격 - 이 간격이 지나면 VM 하트비트가 수신되지 않을 경우 VM이 다시 시작됩니다.
 - 최소 가동 시간 - VM이 VM 도구의 하트비트 모니터링을 시작한 후 클러스터가 이 시간 동안 기다립니다.
 - VM당 최대 재설정 - 클러스터가 최대 재설정 시간 내에서 VM을 이 최대 횟수만큼 다시 시작합니다.
 - 최대 재설정 시간 - VM 재설정당 최대 재설정 횟수를 계산할 시간입니다.

설정할 값을 잘 모르는 경우 다음 설정 예를 사용합니다.

- Failure interval(실패 간격): **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 롤 VMs 실행하는 경우 VM에 맞게 이러한 값을 특별히 설정할 수 있습니다. .ova에서 VM을 배포할 때까지는 이 작업을 수행할 수 없습니다. 이러한 값 설정에 대한 자세한 내용은 [\(선택 사항\) 클러스터VMs에서 다른 에 대한 재정의 옵션 추가](#) 단원을 참조하십시오.

Storage Gateway 콘솔에서 .ova 이미지를 다운로드합니다.

게이트웨이에 대한 .ova 이미지를 다운로드하려면

- Storage Gateway 콘솔의 게이트웨이 설정 페이지에서 게이트웨이 유형과 호스트 플랫폼을 선택한 다음 콘솔에 제공된 링크를 사용하여 [Tape Gateway 설정](#)에 설명된 대로 .ova를 다운로드합니다.

게이트웨이 배포

구성된 클러스터에서 .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.

게이트웨이 .ova 이미지를 배포하려면

- .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.
- 루트 디스크 및 캐시에 대해 선택한 데이터 스토어를 클러스터의 모든 호스트에서 사용할 수 있는지 확인합니다. VMware 또는 온프레미스 환경에서 Storage Gateway .ova 파일을 배포할 때 디스크는 가상화된 SCSI 디스크로 설명됩니다. 반가상화는 VM에 추가하는 가상 디스크를 콘솔이 식별할 수 있도록 게이트웨이 VM이 호스트 운영 체제와 협력하는 모드입니다.

VM을 구성하여 반가상화된 컨트롤러를 사용하려면

- VMware vSphere 클라이언트에서 게이트웨이 VM의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 설정 편집을 선택합니다.
- 가상 머신 속성 대화 상자에서 하드웨어 탭을 선택하고 SCSI 컨트롤러 0을 선택한 다음 유형 변경을 선택합니다.
- SCSI 컨트롤러 유형 변경 대화 상자에서 VMware Paravirtual SCSI 컨트롤러 유형을 선택한 다음 확인을 선택합니다.

(선택 사항) 클러스터VMs에서 다른 에 대한 재정의 옵션 추가

클러스터에서 다른 롤 VMs 실행하는 경우 각 VM에 대해 클러스터 값을 특별히 설정할 수 있습니다. 지침은 VMware vSphere 온라인 설명서의 [개별 가상 머신 사용자 지정](#)을 참조하세요.

클러스터VMs의 다른 에 대한 재정의의 옵션을 추가하려면

1. 의 요약 페이지에서 클러스터를 VMware vSphere 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.

vSphere HA - VM 모니터링에서 각 옵션에 대해 다음 값을 설정합니다.

- VM 모니터링 : Override Enabled - VM 및 애플리케이션 모니터링
- VM 모니터링 민감도: Override Enabled - VM 및 Application Monitoring
- VM 모니터링 : 사용자 지정
- 실패 간격: **30** 초
- 최소 가동 시간: **120** 초
- Maximum per-VM resets(VM당 최대 재설정): **5**
- 최대 재설정 기간: **1** 시간 이내

게이트웨이 활성화

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

게이트웨이를 활성화하려면

- 다음 주제에 설명된 절차를 따릅니다.
 - a. [Tape Gateway를 에 연결 AWS](#)
 - b. [설정 검토 및 Tape Gateway 활성화](#)
 - c. [Tape Gateway 구성](#)

VMware 고가용성 구성 테스트

게이트웨이를 활성화한 후 구성을 테스트합니다.

VMware HA 구성을 테스트하려면

1. <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.

2. 탐색 창에서 게이트웨이를 선택한 다음 VMware HA를 테스트할 게이트웨이를 선택합니다.
3. 작업 에서 VMware HA 확인을 선택합니다.
4. 나타나는 VMware고가용성 구성 확인 상자에서 확인을 선택합니다.

Note

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

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

5. 종료를 선택합니다.

Amazon CloudWatch 로그 그룹에서 VMware HA 이벤트에 대한 정보를 찾을 수 있습니다. 자세한 내용은 로그 [그룹으로 Tape Gateway 상태 로그 가져오기 CloudWatch 로그](#).

Tape Gateway 스토리지 리소스 작업

이 섹션의 주제에서는 게이트웨이의 가상 호스트 플랫폼에 연결된 물리적 디스크, 게이트웨이의 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨, 미디어 체인저와 같은 가상 테이프 라이브러리 디바이스, 가상 테이프 라이브러리의 테이프 등 Tape Gateway와 연결된 스토리지 리소스를 관리하는 방법을 설명합니다.

주제

- [게이트웨이에서 디스크 제거](#) - 예를 들어 실패한 디스크가 있는 경우와 같이 게이트웨이의 가상 호스트 플랫폼에서 디스크를 제거해야 하는 경우 어떻게 해야 하는지 알아봅니다.
- [Amazon EC2 게이트웨이에서 Amazon EBS 볼륨 관리](#) - Amazon EC2 인스턴스에서 호스팅되는 게이트웨이의 업로드 버퍼 또는 캐시 스토리지로 사용하도록 할당된 Amazon EBS 볼륨의 쿼니티를 늘리거나 줄이는 방법에 대해 알아봅니다.
- [VTL 디바이스 작업](#) - Tape Gateway의 미디어 체인저를 선택하는 방법, 미디어 체인저의 디바이스 드라이버를 업데이트하는 방법, Microsoft System Center Data Protection Manager에서 테이프에 대한 바코드를 표시하는 방법을 포함하여 가상 테이프 라이브러리 디바이스를 관리하는 방법에 대해 알아봅니다.

- [가상 테이프 라이브러리에서 테이프 관리](#) - 테이프를 수동으로 아카이브하고 진행 중인 테이프 아카이브를 취소하는 방법을 포함하여 Tape Gateway와 연결된 테이프 및 가상 테이프 라이브러리를 관리하는 방법에 대해 알아봅니다.

게이트웨이에서 디스크 제거

게이트웨이에서의 기본 디스크 제거는 권장되지 않지만, 예를 들어 장애가 발생한 디스크를 게이트웨이에서 제거하고 싶을 수 있습니다.

에서 호스팅된 게이트웨이에서 디스크 제거 VMware ESXi

다음 절차에 따라 VMware 하이퍼바이저에서 호스팅되는 게이트웨이에서 디스크를 제거할 수 있습니다.

업로드 버퍼에 할당된 디스크를 제거하려면(VMware ESXi)

1. vSphere 클라이언트에서 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 게이트웨이 VM의 이름을 선택한 다음 설정 편집을 선택합니다.
2. 가상 머신 속성 대화 상자의 하드웨어 탭에서 업로드 버퍼 공간으로 할당된 디스크를 선택한 다음 제거를 선택합니다.

가상 머신 속성 대화 상자의 가상 디바이스 노드 값이 이전에 기록한 값과 같은지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.

3. Removal Options(제거 옵션) 패널에서 옵션을 선택한 후 확인을 선택하여 디스크 제거 절차를 완료합니다.

Microsoft Hyper-V에 호스팅된 게이트웨이에서 디스크 제거

다음 절차에 따라 Microsoft Hyper-V 하이퍼바이저에서 호스팅하는 게이트웨이에서 디스크를 제거할 수 있습니다.

업로드 버퍼에 할당된 기본 디스크를 제거하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager에서 마우스 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 열고 게이트웨이 VM의 이름을 선택한 후 설정을 선택합니다.
2. 설정 대화 상자의 하드웨어 목록에서 제거할 디스크를 선택한 다음 제거를 선택합니다.

게이트웨이에 추가하는 디스크는 하드웨어 목록의 SCSI 컨트롤러 항목 아래에 나타납니다. 컨트롤러 및 위치 값이 앞에서 기록해 둔 값과 동일한지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.

Microsoft Hyper-V Manager에 표시된 첫 번째 SCSI 컨트롤러는 컨트롤러 0입니다.

3. 확인을 선택하여 변경 사항을 적용합니다.

Linux에서 호스팅된 게이트웨이에서 디스크 제거 KVM

Linux 커널 기반 Virtual Machine(KVM) 하이퍼바이저에서 호스팅되는 게이트웨이에서 디스크를 분리하려면 다음 명령과 유사한 `virsh` 명령을 사용할 수 있습니다.

```
$ virsh detach-disk domain_name /device/path
```

KVM 디스크 관리에 대한 자세한 내용은 Linux 배포 설명서를 참조하세요.

Amazon EC2 게이트웨이에서 Amazon EBS 볼륨 관리

처음에 게이트웨이가 Amazon EC2 인스턴스로 실행되도록 구성된 경우 업로드 버퍼 및 캐시 스토리지로 사용할 Amazon EBS 볼륨을 할당했습니다. 시간이 지남에 따라 애플리케이션이 변경되면 이 용도로 추가 Amazon EBS 볼륨을 할당할 수 있습니다. 이전에 할당된 Amazon EBS 볼륨을 제거하여 할당된 스토리지를 줄일 수도 있습니다. Amazon에 대한 자세한 내용은 Amazon EC2 사용 설명서의 Amazon [Elastic Block Store\(Amazon EBS\)](#)를 EBS참조하세요.

게이트웨이에 스토리지를 추가하기 전에 게이트웨이에 대한 애플리케이션 요구 사항에 따라 업로드 버퍼와 캐시 스토리지의 크기를 조정하는 방법을 검토해야 합니다. 그렇게 하려면 [할당할 업로드 버퍼의 크기 결정](#) 및 [할당할 캐시 스토리지의 크기 결정](#) 단원을 참조하십시오.

업로드 버퍼 및 캐시 스토리지로 할당할 수 있는 최대 스토리지에는 할당량이 있습니다. 원하는 만큼 많은 Amazon EBS 볼륨을 인스턴스에 연결할 수 있지만 이러한 볼륨을 업로드 버퍼로 구성하고 이러한 스토리지 할당량까지만 스토리지 공간을 캐시할 수 있습니다. 자세한 내용은 [AWS Storage Gateway 할당량](#) 단원을 참조하십시오.

Amazon EBS 볼륨을 추가하고 게이트웨이에 맞게 구성하려면

1. Amazon EBS 볼륨을 생성합니다. 지침은 [Amazon 사용 설명서의 Amazon EBS 볼륨 생성 또는 복원](#)을 참조하세요. EC2

2. Amazon EBS 볼륨을 Amazon EC2 인스턴스에 연결합니다. 지침은 [Amazon 사용 설명서의 인스턴스에 Amazon EBS 볼륨 연결을 참조하세요](#). EC2
3. 업로드 버퍼 또는 캐시 스토리지로 추가한 Amazon EBS 볼륨을 구성합니다. 지침은 [Storage Gateway의 로컬 디스크 관리](#) 단원을 참조하십시오.

업로드 버퍼에 할당된 스토리지 용량이 필요 없다는 판단을 내리게 되는 경우가 있습니다.

Amazon EBS 볼륨을 제거하려면

Warning

이 단계는 업로드 버퍼 공간으로 할당된 Amazon EBS 볼륨에만 적용되며 캐시에 할당된 볼륨에는 적용되지 않습니다. Tape Gateway에서 캐시 스토리지로 할당된 Amazon EBS 볼륨을 제거하면 게이트웨이의 가상 테이프 IRRECOVERABLE 상태가 유지되고 데이터 손실이 발생할 수 있습니다. IRRECOVERABLE 상태에 대한 자세한 내용은 [섹션을 참조하세요](#)의 [테이프 상태 정보 이해 VTL](#).

1. [게이트웨이 VM 종료](#) 단원에서 설명하는 접근 방식에 따라 게이트웨이를 종료합니다.
2. Amazon EC2 인스턴스에서 Amazon EBS 볼륨을 분리합니다. 지침은 [Amazon 사용 설명서의 인스턴스에서 Amazon EBS 볼륨 분리](#)를 참조하세요. EC2
3. Amazon EBS 볼륨을 삭제합니다. 지침은 [Amazon 사용 설명서의 Amazon EBS 볼륨 삭제](#)를 참조하세요. EC2
4. [게이트웨이 VM 종료](#) 단원에서 설명하는 접근 방식에 따라 게이트웨이를 시작합니다.

VTL 디바이스 작업

Tape Gateway 설정은 게이트웨이를 활성화할 때 선택하는 다음 SCSI 디바이스를 제공합니다.

주제

- [게이트웨이 활성화 후 미디어 체인저 선택](#)
- [미디어 체인저의 디바이스 드라이버 업데이트](#)
- [Microsoft System Center에서 테이프용 바코드 표시 DPM](#)

미디어 체인저의 경우 는 다음과 함께 AWS Storage Gateway 작동합니다.

- AWS-Gateway-VTL – 이 디바이스는 게이트웨이와 함께 제공됩니다.
- STK-L700 – 이 디바이스 에뮬레이션은 게이트웨이와 함께 제공됩니다.

Tape Gateway를 활성화할 때 목록에서 백업 애플리케이션을 선택하면 Storage Gateway에서 적절한 미디어 체인저를 사용합니다. 백업 애플리케이션이 목록에 없는 경우 기타를 선택한 후 백업 애플리케이션에 사용할 미디어 체인저를 선택합니다.

선택할 미디어 체인저의 유형은 사용하려고 계획한 백업 애플리케이션에 따라 달라집니다. 다음 표는 테스트를 통해 Tape Gateway와 호환되는 것으로 확인된 타사 백업 애플리케이션의 목록입니다. 이 표에는 각 백업 애플리케이션에 권장되는 미디어 체인저 유형도 수록되어 있습니다.

백업 애플리케이션	미디어 체인저 유형
Arcserve 백업	AWS-Gateway-VTL
Bacula Enterprise V10.x	AWS-Gateway-VTL 또는 STK-L700
Commvault V11	STK-L700
Dell EMC NetWorker 19.5	AWS-Gateway-VTL
IBM Spectrum Protect v8.1.10	IBM-03584L32-0402
마이크로 포커스(HPE) 데이터 보호기 9 또는 11.x	AWS-Gateway-VTL
Microsoft System Center 2012 R2 또는 2016 Data Protection Manager	STK-L700
NovaStor DataCenter/네트워크 6.4 또는 7.1	STK-L700
Quest NetVault Backup 12.4 또는 13.x	STK-L700
Veeam Backup & Replication 11A	AWS-Gateway-VTL
Veritas Backup Exec 2014, 15, 16, 20 또는 22.x	AWS-Gateway-VTL
Veritas Backup Exec 2012	STK-L700

백업 애플리케이션	미디어 체인저 유형
<p>Note</p> <p>Veritas는 Backup Exec 2012에 대한 지원을 종료했습니다.</p>	
Veritas NetBackup 버전 7.x 또는 8.x	AWS-Gateway-VTL

Important

사용 중인 백업 애플리케이션에 대해 나열되는 미디어 체인저를 선택할 것을 강력하게 권장합니다. 다른 미디어 체인저를 선택하면 올바르게 작동하지 않을 수 있습니다. 게이트웨이가 활성화된 후에는 다른 미디어 체인저를 선택할 수 있습니다. 자세한 내용은 [게이트웨이 활성화 후 미디어 체인저 선택](#)을 참조하세요.

테이프 드라이브의 경우, Storage Gateway는 다음과 함께 작동합니다.

- IBM-ULT3580- TD5- 이 디바이스 에뮬레이션은 게이트웨이와 함께 제공됩니다.

게이트웨이 활성화 후 미디어 체인저 선택

게이트웨이가 활성화된 후에 다른 미디어 체인저 유형을 선택할 수 있습니다.

게이트웨이 활성화 후 다른 미디어 체인저 유형을 선택하려면

1. 백업 소프트웨어에서 실행 중인 모든 관련 작업을 중단합니다.
2. Windows 서버에서 iSCSI 이니시에이터 속성 창을 엽니다.
3. 대상 탭을 선택하여 검색된 대상을 표시합니다.
4. 검색된 대상 창에서 변경하려는 미디어 체인저를 선택하고 연결 해제를 선택한 후 확인을 선택합니다.
5. Storage Gateway 콘솔의 탐색 창에서 게이트웨이를 선택한 후 미디어 체인저를 변경할 게이트웨이를 선택합니다.

6. VTL 디바이스 탭을 선택하고 변경할 미디어 체인저를 선택한 다음 미디어 체인저 변경 을 선택합니다.
7. 표시된 미디어 체인저 유형 변경 대화 상자의 드롭다운 목록 상자에서 변경하려는 미디어 체인저를 선택한 후 저장을 선택합니다.

미디어 체인저의 디바이스 드라이버 업데이트

1. Windows 서버에서 장치 관리자를 열고 미디어 체인저 장치 트리를 펼칩니다.
2. 알 수 없는 미디어 체인저를 마우스 오른쪽 버튼을 클릭하여 바로 가기 메뉴를 열고 드라이버 소프트웨어 업데이트를 선택하여 드라이버 소프트웨어 업데이트-알 수 없는 미디어 체인저 창이 열립니다.
3. How do you want to search for driver software(드라이버 소프트웨어를 검색하시겠습니까)? 섹션에서 Browse my computer for driver software(내 컴퓨터에서 드라이버 소프트웨어 찾아보기)를 선택합니다.
4. Let me pick from a list of device drivers on my computer(내 컴퓨터의 장치 드라이버 목록에서 선택)를 선택합니다.

Note

Sony TSL-A500C Autoloader 드라이버를 Veeam Backup & Replication 11A 및 Microsoft System Center Data Protection Manager 백업 소프트웨어와 함께 사용하는 것이 좋습니다. 이 Sony 드라이버는 이러한 유형의 백업 소프트웨어(Windows Server 2019 포함)에서 테스트되었습니다.

5. 이 하드웨어에 설치할 디바이스 드라이버 선택 섹션에서 호환 하드웨어 표시 확인란의 선택을 취소하고 제조업체 목록에서 Sony를 선택한 다음 모델 목록에서 Sony - TSL-A500C 오토로더를 선택한 다음 다음 을 선택합니다.
6. 이어 나타나는 경고 상자에서 예를 선택합니다. 드라이버가 성공적으로 설치되었으면 Update drive software(드라이브 소프트웨어 업데이트) 창을 닫습니다.

Microsoft System Center에서 테이프용 바코드 표시 DPM

Sony TSL-A500C Autoloader에 미디어 체인저 드라이버를 사용하는 경우 Microsoft System Center Data Protection Manager는 Storage Gateway 에서 생성된 가상 테이프에 대한 바코드를 자동으로 표시하지 않습니다. 테이프에 대한 바코드를 올바르게 표시하려면 미디어 체인저 드라이버를 Sun/StorageTek Library로 변경합니다.

바코드를 표시하려면

1. 모든 백업 작업이 완료되었고 보류 중이거나 진행 중인 작업이 없는지 확인합니다.
2. 테이프를 꺼내 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)로 이동하고 DPM 관리자 콘솔을 종료합니다. 에서 테이프를 꺼내는 방법에 대한 자세한 내용은 섹션을 DPM참조하세요 [를 사용하여 테이프 보관 DPM](#).
3. 관리 도구 에서 서비스를 선택하고 세부 정보 창에서 DPM 서비스의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 연 다음 속성을 선택합니다.
4. 일반 탭에서 시작 유형이 자동으로 설정되어 있는지 확인하고 중지를 선택하여 DPM 서비스를 중지합니다.
5. Microsoft 웹 사이트의 [Microsoft Update Catalog](#)에서 StorageTek 드라이버를 가져옵니다.

Note

다양한 크기의 여러 드라이버를 기록해 둡니다.

크기가 18K인 경우 x86 드라이버를 선택합니다.

크기가 19K인 경우 x64 드라이버를 선택합니다.

6. Windows 서버에서 장치 관리자를 열고 미디어 체인저 장치 트리를 펼칩니다.
7. 알 수 없는 미디어 체인저를 마우스 오른쪽 버튼을 클릭하여 바로 가기 메뉴를 열고 드라이버 소프트웨어 업데이트를 선택하여 드라이버 소프트웨어 업데이트-알 수 없는 미디어 체인저 창이 열립니다.
8. 새 드라이버 위치 경로를 찾아 설치합니다. 드라이버는 Sun/StorageTek Library 로 표시됩니다. 테이프 드라이브는 IBM ULT3580-TD5SCSI순차 디바이스로 유지됩니다.
9. DPM 서버를 재부팅합니다.
10. Storage Gateway 콘솔에서 새 테이프를 생성합니다.
11. DPM 관리자 콘솔을 열고 관리를 선택한 다음 새 테이프 라이브러리 재스캔 을 선택합니다. Sun/StorageTek library 가 표시됩니다.
12. 라이브러리를 선택하고 인벤토리를 선택합니다.
13. 테이프 추가를 선택하여 새 테이프를 추가합니다DPM. 새 테이프가 해당 바코드를 표시합니다.

가상 테이프 라이브러리에서 테이프 관리

Storage Gateway는 활성화하는 각 Tape Gateway에 대해 하나의 가상 테이프 라이브러리(VTL)를 제공합니다. 초기에 이 라이브러리는 테이프를 포함하지 않지만 필요할 때는 언제든지 테이프를 생성할 수 있습니다. 애플리케이션은 Tape Gateway의 모든 가용 테이프에(서) 읽고 쓸 수 있습니다. 테이프에 쓰AVAILABLE려면 테이프의 상태가 여야 합니다. 이러한 테이프는 Amazon Simple Storage Service(S3)의 지원을 받습니다. 즉, 이러한 테이프에 데이터를 쓰면 Tape Gateway가 Amazon S3에 데이터를 저장합니다. 자세한 내용은 [의 테이프 상태 정보 이해 VTL](#) 단원을 참조하십시오.

주제

- [테이프 보관](#)
- [테이프 보관 취소](#)

테이프 라이브러리는 Tape Gateway에 있는 테이프를 보여줍니다. 이 라이브러리는 테이프 바코드, 상태 및 크기, 테이프 사용량, 테이프가 연결되어 있는 게이트웨이를 표시합니다.

라이브러리에 다수의 테이프가 있는 경우, 콘솔은 바코드, 상태 또는 이 두 가지를 모두 사용하여 테이프를 검색하는 기능을 지원합니다. 바코드를 검색할 때 상태 및 게이트웨이를 조건으로 하여 필터링할 수 있습니다.

바코드, 상태, 게이트웨이를 기준으로 검색하려면

1. <https://console.aws.amazon.com/storagegateway/> [집에서](#) Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 테이프를 선택한 후 검색 상자에 값을 입력합니다. 이 값은 바코드, 상태 또는 게이트웨이일 수 있습니다. 기본적으로 Storage Gateway는 모든 가상 테이프를 검색합니다. 그러나 상태를 기준으로 검색을 필터링할 수도 있습니다.

상태를 필터링하면 기준과 일치하는 테이프가 Storage Gateway 콘솔의 라이브러리에 표시됩니다.

게이트웨이를 필터링하면 해당 게이트웨이와 연결된 테이프가 Storage Gateway 콘솔의 라이브러리에 표시됩니다.

Note

기본적으로 Storage Gateway는 상태에 관계없이 모든 테이프를 표시합니다.

테이프 보관

Tape Gateway에 있는 가상 테이프를 보관할 수 있습니다. 테이프를 아카이브하면 Storage Gateway에서 테이프를 아카이브로 옮깁니다.

테이프를 보관하려면 백업 소프트웨어를 사용합니다. 테이프 아카이브 프로세스는 테이프 상태 IN TRANSIT TO VTS, ARCHIVING, 로 표시되는 세 단계로 구성됩니다 ARCHIVED.

- 테이프를 백업하려면 백업 애플리케이션이 제공하는 명령을 사용합니다. 아카이브 프로세스가 시작되면 테이프 상태가 IN TRANSIT TO VTS로 변경되고 백업 애플리케이션에서 테이프에 더 이상 액세스할 수 없습니다. 이 단계에서는 Tape Gateway가 데이터를 에 업로드합니다 AWS. 필요한 경우, 진행 중인 보관을 취소할 수 있습니다. 보관 취소에 대한 자세한 내용은 [테이프 보관 취소](#) 단원을 참조하십시오.

Note

테이프 보관 절차는 백업 애플리케이션에 따라 다릅니다. 자세한 지침은 백업 애플리케이션 설명서를 참조하십시오.

- 데이터 업로드가 AWS 완료되면 테이프 상태가 로 변경 ARCHIVING되고 Storage Gateway가 테이프를 아카이브로 이동하기 시작합니다. 이 시점에서는 보관 프로세스를 취소할 수 없습니다.
- 테이프가 아카이브로 이동되면 상태가 로 변경 ARCHIVED되고 모든 게이트웨이로 테이프를 검색할 수 있습니다. 테이프 가져오기에 대한 자세한 내용은 [보관한 테이프 가져오기](#) 단원을 참조하십시오.

테이프 보관에 필요한 절차는 백업 소프트웨어에 따라 다릅니다. Symantec NetBackup 소프트웨어를 사용하여 테이프를 아카이브하는 방법에 대한 지침은 [테이프 아카이브를 참조하세요](#).

테이프 보관 취소

테이프 보관을 시작한 후에 테이프를 다시 가져와야겠다고 판단하는 경우가 있을 수 있습니다. 예를 들어 보관 프로세스가 너무 오래 걸려 보관 프로세스를 취소하고 테이프를 다시 가져와야겠다고 판단하거나 테이프에서 데이터를 읽어야 할 경우가 있을 수 있습니다. 보관 중인 테이프는 다음과 같이 세 가지 상태를 거칩니다.

- IN TRANSIT TO VTS: Tape Gateway가 데이터를 에 업로드하고 있습니다 AWS.
- ARCHIVING: 데이터 업로드가 완료되고 Tape Gateway가 테이프를 아카이브로 이동 중입니다.
- ARCHIVED: 테이프가 이동되고 아카이브가 검색에 사용할 수 있습니다.

테이프의 상태가 IN TRANSIT TO인 경우에만 아카이브를 취소할 수 있습니다. 업로드 대역폭, 업로드 중인 데이터 양과 같은 요인에 따라 이 상태가 Storage Gateway 콘솔에 표시될 수도 있고 표시되지 않을 수도 있습니다. 테이프 아카이브를 취소하려면 API 참조의 [CancelRetrieval](#) 작업을 사용합니다.

게이트웨이 활성화 키 받기

게이트웨이 활성화 키를 받으려면 게이트웨이 가상 머신(VM)으로 웹 요청을 보내야 합니다. VM은 활성화 키를 포함한 리디렉션을 반환하며, 이 키는 ActivateGateway API 작업의 파라미터 중 하나로 전달되어 게이트웨이 구성을 지정합니다. 자세한 내용은 Storage Gateway API 참조를 참조하십시오 [ActivateGateway](#).

Note

게이트웨이 활성화 키는 사용하지 않으면 30분 후에 만료됩니다.

게이트웨이 VM에 보내는 요청에는 활성화가 발생하는 AWS 지역이 포함됩니다. 응답에 리디렉션으로 반환되는 URL에는 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`. 이 쿼리의 출력은 활성화 리전과 활성화 키를 모두 반환합니다.

이 URL에는 VPC 엔드포인트 유형을 사용하여 연결하는 게이트웨이의 VPC 엔드포인트 ID인 vpcEndpoint도 포함되어 있습니다.

Note

Storage Gateway 하드웨어 어플라이언스, VM 이미지 템플릿, Amazon EC2 Amazon Machine Image(AMI)에는 이 페이지에 설명된 웹 요청을 수신하고 이에 응답하는 데 필요한 HTTP 서비스가 사전 구성되어 있습니다. 게이트웨이에 추가 서비스를 설치할 필요는 없으며 권장하지도 않습니다.

주제

- [Linux\(curl\)](#)
- [Linux\(bash/zsh\)](#)

- [마이크로소프트 윈도우 PowerShell](#)
- [로컬 콘솔 사용](#)

Linux(curl)

다음 예에서는 Linux(curl)를 사용하여 활성화 키를 받는 방법을 보여줍니다.

Note

강조 표시된 변수를 게이트웨이의 실제 값으로 바꿉니다. 가능한 값은 다음과 같습니다.

- *gateway_ip_address* - 게이트웨이의 IPv4 주소입니다(예: 172.31.29.201).
- *gateway_type* - 활성화하려는 게이트웨이 유형 (예:, STORED CACHEDVTL, FILE_S3 또는). FILE_FSX_SMB
- *region_code* - 게이트웨이를 활성화할 리전입니다.AWS 일반 참조 안내서에서 [리전 엔드 포인트](#)를 참조하세요. 이 매개 변수가 지정되지 않았거나 제공된 값의 철자가 틀렸거나 유효한 지역과 일치하지 않는 경우 명령은 기본적으로 지역을 사용합니다. us-east-1
- *vpc_endpoint* - 게이트웨이의 VPC 엔드포인트 이름입니다(예: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com).

퍼블릭 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

VPC 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux(bash/zsh)

다음 예제는 Linux(bash/zsh)를 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```
function get-activation-key() {
    local ip_address=$1
    local activation_region=$2
    if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
        echo "Usage: get-activation-key ip_address activation_region gateway_type"
        return 1
    fi

    if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
        activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
        echo "$activation_key_param" | cut -f2 -d=
    else
        return 1
    fi
}
```

마이크로소프트 윈도우 PowerShell

다음 예제는 Microsoft PowerShell Windows를 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 가져오는 방법을 보여줍니다.

```
function Get-ActivationKey {
    [CmdletBinding()]
    Param(
        [parameter(Mandatory=$true)][string]$IpAddress,
        [parameter(Mandatory=$true)][string]$ActivationRegion,
        [parameter(Mandatory=$true)][string]$GatewayType
    )
    PROCESS {
        $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
        if ($request) {
            $activationKeyParam = $request.Headers.Location | Select-String -Pattern
"activationKey=( [A-Z0-9-]+ )"
            $activationKeyParam.Matches.Value.Split("=")[1]
        }
    }
}
```


로컬 콘솔 사용

다음 예에서는 로컬 콘솔을 사용하여 활성화 키를 생성하고 표시하는 방법을 보여줍니다.

로컬 콘솔에서 게이트웨이 활성화 키를 가져오려면

1. 로컬 콘솔에 로그인합니다. Amazon EC2 인스턴스에 연결하는 경우, admin으로 로그인합니다.
2. 로그인하여 AWS 어플라이언스 활성화 - 구성 기본 메뉴가 표시되면 0을 선택하여 활성화 키 받기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 메시지가 표시되면 게이트웨이를 활성화할 AWS 지역을 입력합니다.
5. 네트워크 유형으로 퍼블릭의 경우 1을, VPC 엔드포인트의 경우 2를 입력합니다.
6. 엔드포인트 유형으로 표준의 경우 1을, FIPS(Federal Information Processing Standard)의 경우 2를 입력합니다.

iSCSI 이니시에이터 연결

게이트웨이를 관리할 때 Internet Small Computer System Interface(iVTL) 대상으로 노출되는 볼륨 또는 가상 테이프 라이브러리(SCSI) 디바이스로 작업합니다. 볼륨 게이트웨이의 경우 iSCSI 대상은 볼륨입니다. Tape Gateway의 경우 대상은 VTL 디바이스입니다. 이 작업의 일환으로 이러한 대상에 연결, iSCSI 설정 사용자 지정, Red Hat Linux 클라이언트에서 연결, Challenge-Handshake 인증 프로토콜 구성()과 같은 작업을 수행합니다CHAP.

주제

- [Windows 클라이언트에 VTL 디바이스 연결](#)
- [VTL 디바이스를 Linux 클라이언트에 연결](#)
- [iSCSI 설정 사용자 지정](#)
- [iSCSI 대상에 대한 CHAP 인증 구성](#)

iSCSI 표준은 IP 기반 스토리지 디바이스와 클라이언트 간의 연결을 시작하고 관리하기 위한 인터넷 프로토콜(IP) 기반 스토리지 네트워킹 표준입니다. 다음 목록은 iSCSI 연결 및 관련 구성 요소를 설명하는 데 사용되는 몇 가지 용어를 정의합니다.

iSCSI 이니시에이터

iSCSI 네트워크의 클라이언트 구성 요소입니다. 이니시에이터는 iSCSI 대상에 요청을 보냅니다. 이니시에이터는 소프트웨어 또는 하드웨어로 구현할 수 있습니다. Storage Gateway는 소프트웨어 이니시에이터만 지원합니다.

iSCSI 대상

이니시에이터의 요청을 수신하고 응답하는 iSCSI 네트워크의 서버 구성 요소입니다. 각 볼륨은 iSCSI 대상으로 노출됩니다. 각 iSCSI 대상에 하나의 iSCSI 이니시에이터만 연결합니다.

Microsoft iSCSI 이니시에이터

클라이언트 컴퓨터(즉, 게이트웨이에 데이터를 쓰려는 애플리케이션을 실행하는 컴퓨터)를 외부 iSCSI 기반 배열(즉, 게이트웨이)에 연결할 수 있는 Microsoft Windows 컴퓨터의 소프트웨어 프로그램입니다. 호스트 컴퓨터의 이더넷 네트워크 어댑터 카드를 사용하여 연결합니다. Microsoft iSCSI 이니시에이터는 Windows 8.1, Windows 10, Windows Server 2012 R2, Windows Server 2016 및 Windows Server 2019에서 Storage Gateway로 검증되었습니다. 이니시에이터는 이러한 운영 체제에 기본 제공됩니다.

Red Hat iSCSI 이니시에이터

`iscsi-initiator-utils` 리소스 패키지 관리자(RPM) 패키지는 Red Hat Linux용 소프트웨어에 구현된 iSCSI 이니시에이터를 제공합니다. 패키지에는 iSCSI 프로토콜용 서버 데몬이 포함되어 있습니다.

각 게이트웨이 유형은 iSCSI 디바이스에 연결할 수 있으며, 다음에 설명된 대로 이러한 연결을 사용자 지정할 수 있습니다.

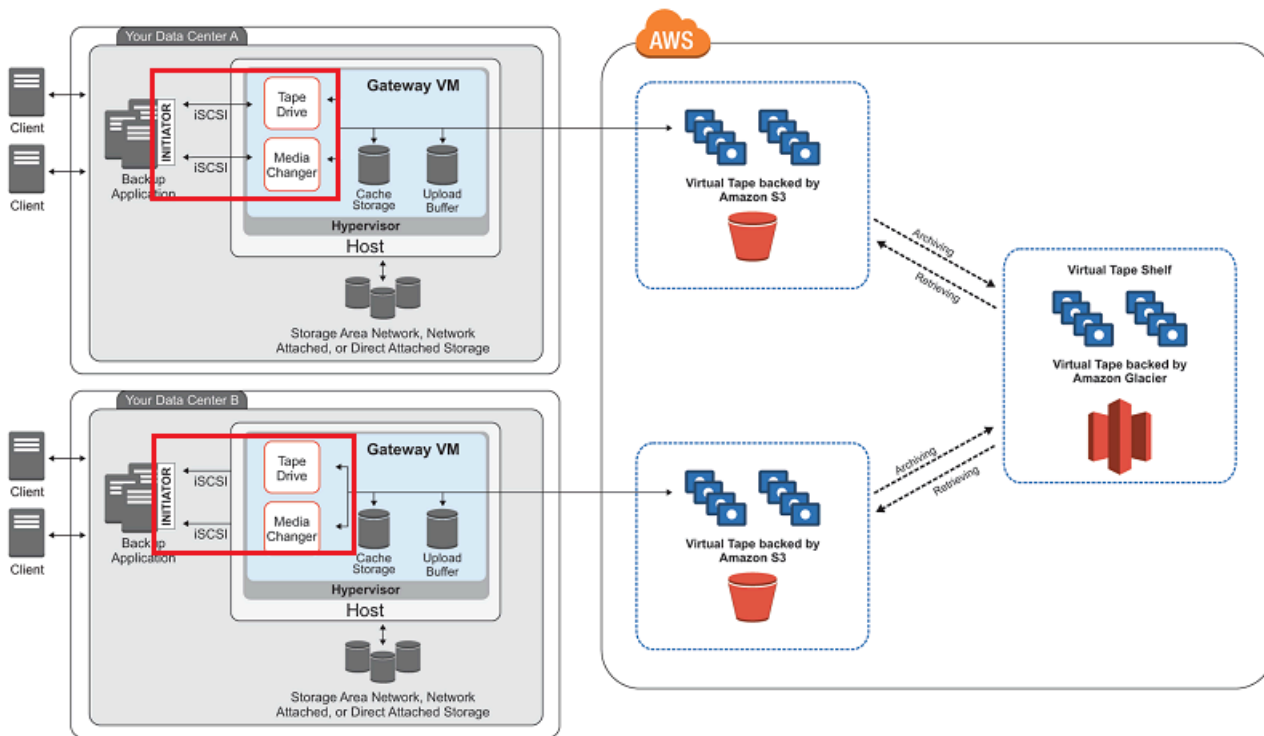
Windows 클라이언트에 VTL 디바이스 연결

Tape Gateway는 여러 테이프 드라이브와 미디어 체인저를 iSCSI 대상으로 통칭하여 VTL 디바이스라고 합니다. 자세한 내용은 [Tape Gateway 설정 요구 사항](#) 단원을 참조하십시오.

Note

각 iSCSI 대상에 하나의 애플리케이션만 연결합니다.

다음 다이어그램은 Storage Gateway 아키텍처의 큰 그림에서 iSCSI 대상을 강조 표시합니다. Storage Gateway 아키텍처에 대한 자세한 내용은 [Tape Gateway 작동 방식\(아키텍처\)](#)을 참조하세요.



Windows 클라이언트를 VTL 디바이스에 연결하려면

1. Windows 클라이언트 컴퓨터의 시작 메뉴에서 프로그램 및 파일 검색 상자에 **iscsicpl.exe** 를 입력하고 iSCSI 이니시에이터 프로그램을 찾은 다음 실행합니다.

Note

iSCSI 이니시에이터를 실행하려면 클라이언트 컴퓨터에 관리자 권한이 있어야 합니다.

2. 메시지가 표시되면 예를 선택하여 Microsoft iSCSI 이니시에이터 서비스를 시작합니다.
3. iSCSI Initiator 속성 대화 상자에서 검색 탭을 선택한 다음 포털 검색을 선택합니다.
4. 대상 포털 검색 대화 상자에서 Tape Gateway for IP 주소 또는 DNS 이름 의 IP 주소를 입력한 다음 확인을 선택합니다. 게이트웨이의 IP 주소를 가져오려면 Storage Gateway 콘솔의 게이트웨이 탭을 확인합니다. Amazon EC2 인스턴스에 게이트웨이를 배포한 경우 Amazon EC2 콘솔의 설명 탭에서 퍼블릭 IP 또는 DNS 주소를 찾을 수 있습니다.

⚠ Warning

Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 퍼블릭 인터넷 연결을 통해 게이트웨이에 액세스하는 것은 지원되지 않습니다. Amazon EC2 인스턴스의 탄력적 IP 주소는 대상 주소로 사용할 수 없습니다.

5. 대상 탭을 선택한 후 새로 고침을 선택합니다. 테이프 드라이브 10개와 미디어 체인저가 모두 검색된 대상 상자에 표시됩니다. 대상의 상태는 비활성으로 되어 있습니다.
6. 첫 번째 디바이스를 선택하고 연결을 선택합니다. 디바이스를 한 번에 하나씩 연결합니다.
7. Connect to Target(대상으로 연결) 대화 상자에서 확인을 선택합니다.
8. 각 디바이스에 대해 6단계와 7단계를 반복하여 모든 디바이스를 연결한 다음 iSCSI Initiator 속성 대화 상자에서 확인을 선택합니다.

Windows 클라이언트에서 테이프 드라이브에 대한 드라이버 공급자는 Microsoft이어야 합니다. 다음 절차를 통해 드라이버 공급자를 확인하고 필요한 경우 드라이버와 공급자를 업데이트하십시오.

드라이버 공급자를 확인하고 필요한 경우 Windows 클라이언트에서 공급자와 드라이버를 업데이트하려면

1. Windows 클라이언트에서 디바이스 관리자를 시작합니다.
2. Tape drives(테이프 드라이브)를 펼쳐 테이프 드라이브를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 선택하고 Properties(속성)를 선택합니다.
3. 디바이스 속성 대화 상자의 드라이버 탭에서 드라이버 공급자가 Microsoft인지 확인합니다.
4. 드라이버 공급자가 Microsoft가 아닌 경우 값을 다음과 같이 설정합니다.
 - a. 드라이버 업데이트(Update Driver)를 선택합니다.
 - b. 드라이버 소프트웨어 업데이트(Update Driver Software) 대화 상자에서 내 컴퓨터에서 드라이버 소프트웨어 찾아보기(Browse my computer for driver software)를 선택합니다.
 - c. 드라이버 소프트웨어 업데이트(Update Driver Software) 대화 상자에서 내 컴퓨터의 디바이스 드라이버 목록에서 고르기(Let me pick from a list of device drivers on my computer)를 선택합니다.
 - d. LTO 테이프 드라이브를 선택하고 다음을 선택합니다.
 - e. 달기를 선택하여 드라이버 소프트웨어 업데이트 창을 닫고 드라이버 공급자 값이 이제 Microsoft로 설정되었는지 확인합니다.

- 4.1~4.5단계를 반복하여 모든 테이프 드라이브를 업데이트합니다.

VTL 디바이스를 Linux 클라이언트에 연결

Red Hat Enterprise Linux(RHEL)를 사용하는 경우 `iscsi-initiator-utils` RPM 패키지를 사용하여 게이트웨이 iSCSI 대상(볼륨 또는 VTL 디바이스)에 연결합니다.

Linux 클라이언트를 iSCSI 대상에 연결하려면

- 클라이언트에 아직 설치되지 않은 경우 `iscsi-initiator-utils` RPM 패키지를 설치합니다.

다음 명령을 사용하여 패키지를 설치할 수 있습니다.

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

- iSCSI 데몬이 실행 중인지 확인합니다.

- 다음 명령 중 하나를 사용하여 iSCSI 데몬이 실행 중인지 확인합니다.

RHEL 5 또는 6의 경우 다음 명령을 사용합니다.

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

RHEL 7, 8 또는 9의 경우 다음 명령을 사용합니다.

```
sudo service iscsid status
```

- 상태 명령이 `running` 상태를 반환하지 않으면 다음 명령 중 하나를 사용하여 데몬을 시작합니다.

RHEL 5 또는 6의 경우 다음 명령을 사용합니다.

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

RHEL 7의 경우 다음 명령을 사용합니다. RHEL 7의 경우 일반적으로 `iscsid` 서비스를 명시적으로 시작할 필요가 없습니다.

```
sudo service iscsid start
```

- 게이트웨이에 대해 정의된 볼륨 또는 VTL 디바이스 대상을 검색하려면 다음 검색 명령을 사용합니다.

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

게이트웨이의 IP 주소를 로 대체합니다. `[GATEWAY_IP]` 이전 명령의 변수입니다. Storage Gateway 콘솔에서 볼륨의 iSCSI Target Info 속성에서 Storage Gateway IP를 찾을 수 있습니다.

검색 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

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

IQN 값은 조직에 고유하기 때문에 iSCSI 적격 이름(IQN)은 앞서 표시된 것과 다릅니다. 대상의 이름은 볼륨 생성 시 지정한 이름입니다. Storage Gateway 콘솔에서 볼륨을 선택하면 iSCSI Target Info 속성 창에서 이 대상 이름을 찾을 수도 있습니다.

- 대상에 접속하려면 다음 명령을 사용하십시오.

올바른 를 지정해야 합니다. `[GATEWAY_IP]` 연결 명령 IQN에서 및 를 선택합니다.

Warning

Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 퍼블릭 인터넷 연결을 통해 게이트웨이에 액세스하는 것은 지원되지 않습니다. Amazon EC2 인스턴스의 탄력적 IP 주소는 대상 주소로 사용할 수 없습니다.

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

- 볼륨이 클라이언트 머신(초기자)에 연결되었는지 확인하려면 다음 명령을 사용해야 합니다.

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

이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

이니시에이터를 설정한 후 에 설명된 대로 iSCSI 설정을 사용자 지정하는 것이 좋습니다 [Linux iSCSI 설정 사용자 지정](#).

iSCSI 설정 사용자 지정

이니시에이터를 설정한 후에는 이니시에이터가 대상에서 연결 해제되지 않도록 iSCSI 설정을 사용자 지정하는 것이 좋습니다.

다음 단계에 표시된 대로 iSCSI 제한 시간 값을 늘리면 시간이 오래 걸리는 쓰기 작업과 네트워크 중단과 같은 기타 일시적인 문제를 더 잘 처리할 수 있습니다.

Note

레지스트리를 변경하기 전에 레지스트리의 백업 사본을 만들어야 합니다. 백업 복사본 생성 및 레지스트리 작업 시 따라야 할 기타 모범 사례에 대한 자세한 내용은 Microsoft TechNet 라이브러리의 [레지스트리 모범 사례](#) 섹션을 참조하세요.

주제

- [Windows iSCSI 설정 사용자 지정](#)
- [Linux iSCSI 설정 사용자 지정](#)

Windows iSCSI 설정 사용자 지정

Tape Gateway 설정의 경우 Microsoft iSCSI 이니시에이터를 사용하여 VTL 디바이스에 연결하는 과정은 2단계 프로세스입니다.

1. Tape Gateway 디바이스를 Windows 클라이언트에 연결합니다.
2. 백업 애플리케이션을 사용하는 경우, 애플리케이션에서 디바이스를 사용하도록 구성합니다.

시작하기의 설정 예시에서는 이 두 단계에 대한 지침을 제공합니다. Symantec NetBackup 백업 애플리케이션을 사용합니다. 자세한 내용은 [VTL 디바이스 연결](#) 및 [NetBackup 스토리지 디바이스 구성](#) 단원을 참조하세요.

Windows iSCSI 설정을 사용자 지정하려면

1. 요청이 대기하는 최대 시간을 늘립니다.

- a. 레지스트리 편집기(Regedit.exe)를 시작합니다.
- b. 다음과 같이 iSCSI 컨트롤러 설정이 포함된 디바이스 클래스의 전역 고유 식별자(GUID) 키로 이동합니다.

⚠ Warning

ControlSet001 또는 00ControlSet2와 같은 다른 제어 세트가 아닌 CurrentControlSet 하위 키에서 작업해야 합니다.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

- c. 다음과 같이 Microsoft iSCSI 이니시에이터의 하위 키를 찾습니다. [*Instance Number*].

하위 키는 0000과 같이 네 자리 숫자로 표시됩니다.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

컴퓨터에 설치된 항목에 따라 Microsoft iSCSI 이니시에이터가 하위 키가 아닐 수 있습니다. 문자열에 값이 있는지 확인하여 올바른 하위 키를 선택했는지 확인할 수 있습니다. DriverDesc 값이 Microsoft iSCSI Initiator.

- d. iSCSI 설정을 표시하려면 파라미터 하위 키를 선택합니다.
- e. MaxRequestHoldTime DWORD (32비트) 값의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 수정을 선택한 다음 값을 로 변경합니다. **600**.

MaxRequestHoldTime 는 Device Removal 이벤트의 상위 계층에 알리기 전에 Microsoft iSCSI 이니시에이터가 미해결 명령을 보류하고 재시도해야 하는 초를 지정합니다. 이 값은 대기 시간 600초를 나타냅니다.

2. 다음 파라미터를 수정하여 iSCSI 패킷으로 전송할 수 있는 최대 데이터 양을 늘릴 수 있습니다.
 - FirstBurstLength 는 원치 않는 쓰기 요청으로 전송할 수 있는 최대 데이터 양을 제어합니다. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.

- MaxBurstLength 는 와 유사FirstBurstLength하지만 요청된 쓰기 시퀀스로 전송할 수 있는 최대 데이터 양을 설정합니다. 이 값을 **1048576** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.
- MaxRecvDataSegmentLength 는 단일 프로토콜 데이터 유닛()과 연결된 최대 데이터 세그먼트 크기를 제어합니다PDU. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.

Note

다양한 iSCSI 설정을 사용하여 가장 잘 작동하도록 다양한 백업 소프트웨어를 최적화할 수 있습니다. 이러한 파라미터의 값이 최상의 성능을 제공하는지 확인하려면 백업 소프트웨어 설명서를 참조하십시오.

3. 다음과 같이 디스크 제한 시간 값을 늘립니다.

- 레지스트리 편집기(Regedit.exe)를 아직 시작하지 않았다면 지금 시작하십시오.
- 다음과 CurrentControlSet같이 의 서비스 하위 키에서 디스크 하위 키로 이동합니다.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
```

- TimeOutValue DWORD (32비트) 값의 컨텍스트(마우스 오른쪽 버튼 클릭) 메뉴를 열고 수정을 선택한 다음 값을 로 변경합니다**600**.

TimeOutValue 는 연결을 끊었다가 다시 설정하여 세션 복구를 시도하기 전에 iSCSI 이니시에이터가 대상의 응답을 대기하는 시간을 지정합니다. 이 값은 600초의 제한 시간을 나타냅니다.

4. 새 구성 값을 적용하려면 시스템을 다시 시작해야 합니다.

다시 시작하기 전에 볼륨에 대한 모든 쓰기 작업의 결과가 풀러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 매핑한 스토리지 볼륨 디스크를 모두 오프라인으로 전환해야 합니다.

Linux iSCSI 설정 사용자 지정

게이트웨이의 이니시에이터를 설정한 후에는 이니시에이터가 대상에서 연결을 끊지 않도록 iSCSI 설정을 사용자 지정하는 것이 좋습니다. 다음과 같이 iSCSI 제한 시간 값을 늘리면 시간이 오래 걸리는 쓰기 작업과 네트워크 중단과 같은 기타 일시적인 문제를 더 잘 처리할 수 있습니다.

Note

다른 유형의 Linux인 경우, 명령이 약간 다를 수 있습니다. 다음은 Red Hat Linux의 예시입니다.

Linux iSCSI 설정을 사용자 지정하려면

1. 요청이 대기하는 최대 시간을 늘립니다.

- a. `/etc/iscsi/iscsid.conf` 파일을 열고 다음 줄을 검색합니다.

```
node.session.timeo.replacement_timeout = [replacement_timeout_value]
node.conn[0].timeo.noop_out_interval = [noop_out_interval_value]
node.conn[0].timeo.noop_out_timeout = [noop_out_timeout_value]
```

- b. 다음을 설정합니다. `[replacement_timeout_value]` 값을 로 지정합니다 **600**.

다음을 설정합니다. `[noop_out_interval_value]` 값을 로 지정합니다 **60**.

다음을 설정합니다. `[noop_out_timeout_value]` 값을 로 지정합니다 **600**.

세 값은 모두 초 단위입니다.

Note

`iscsid.conf`는 게이트웨이를 검색하기 전에 설정해야 합니다. 게이트웨이를 이미 검색하였거나 대상에 로그인하였거나, 아니면 둘 다인 경우에는 다음 명령을 사용하여 검색 데이터베이스에서 항목을 삭제할 수 있습니다. 그 다음에는 다시 검색하거나 로그인하여 새 구성을 가져올 수 있습니다.

```
iscsiadm -m discoverydb -t sendtargets -p [GATEWAY_IP]:3260 -o delete
```

2. 각 응답에서 전송할 수 있는 데이터 양의 최대값을 늘립니다.

- a. `/etc/iscsi/iscsid.conf` 파일을 열고 다음 줄을 검색합니다.

```
node.session.iscsi.FirstBurstLength = [replacement_first_burst_length_value]
node.session.iscsi.MaxBurstLength = [replacement_max_burst_length_value]
```

```
node.conn[0].iscsi.MaxRecvDataSegmentLength
= [replacement_segment_length_value]
```

- b. 성능 향상을 위해 다음 값을 사용하는 것이 좋습니다. 백업 소프트웨어는 다른 값을 사용하도록 최적화되었을 수 있으므로 최상의 결과를 얻으려면 백업 소프트웨어 설명서를 참조하십시오.

다음을 설정합니다. `[replacement_first_burst_length_value]` 값이 **262144** 또는 Linux OS 기본값 중 더 높은 값입니다.

다음을 설정합니다. `[replacement_max_burst_length_value]` 값이 **1048576** 또는 Linux OS 기본값 중 더 높은 값입니다.

다음을 설정합니다. `[replacement_segment_length_value]` 값이 **262144** 또는 Linux OS 기본값 중 더 높은 값입니다.

Note

다양한 iSCSI 설정을 사용하여 가장 잘 작동하도록 다양한 백업 소프트웨어를 최적화할 수 있습니다. 이러한 파라미터의 값이 최상의 성능을 제공하는지 확인하려면 백업 소프트웨어 설명서를 참조하십시오.

3. 시스템을 다시 시작하여 새 구성 값이 적용되었는지 확인합니다.

다시 시작하기 전에 해당 테이프에 대한 모든 쓰기 작업의 결과가 플래시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 테이프를 마운트 해제합니다.

iSCSI 대상에 대한 CHAP 인증 구성

Storage Gateway는 Challenge-Handshake 인증 프로토콜()을 사용하여 게이트웨이와 iSCSI 이니시에이터 간의 인증을 지원합니다. CHAP은 볼륨 및 VTL 디바이스 대상에 액세스하기 위해 인증된 iSCSI 이니시에이터의 ID를 주기적으로 확인하여 재생 공격으로부터 보호합니다.

Note

CHAP 구성은 선택 사항이지만 적극 권장됩니다.

를 설정하려면 Storage Gateway 콘솔과 대상에 연결하는 데 사용하는 iSCSI 이니시에이터 소프트웨어에서 모두 구성해야 CHAP합니다. Storage Gateway는 상호 를 사용합니다. 즉CHAP, 이니시에이터가 대상을 인증하고 대상이 이니시에이터를 인증하는 경우입니다.

대상CHAP에 대해 상호 설정하려면

1. CHAP 에 설명된 대로 Storage Gateway 콘솔에서 를 구성합니다 [Storage Gateway 콘솔에서 VTL 디바이스 대상에 CHAP 대해 를 구성하려면](#).
2. 클라이언트 이니시에이터 소프트웨어에서 CHAP 구성을 완료합니다.
 - Windows 클라이언트CHAP에서 상호를 구성하려면 섹션을 참조하세요 [Windows 클라이언트 CHAP에서 상호 구성](#).
 - Red Hat Linux 클라이언트CHAP에서 상호를 구성하려면 섹션을 참조하세요 [Red Hat Linux 클라이언트CHAP에서 상호 구성](#).

Storage Gateway 콘솔에서 VTL 디바이스 대상에 CHAP 대해 를 구성하려면

이 절차에서는 가상 테이프에 읽고 쓰는 데 사용하는 비밀 키 두 개를 지정합니다. 이 동일한 키 두 개는 클라이언트 초기자를 구성하는 절차에서 사용합니다.

1. 탐색 창에서 게이트웨이를 선택합니다.
2. 게이트웨이를 선택한 다음 VTL 디바이스 탭을 선택하여 모든 VTL 디바이스를 표시합니다.
3. 구성할 디바이스를 선택합니다CHAP.
4. CHAP 인증 구성 대화 상자에 요청된 정보를 입력합니다.
 - a. 이니시에이터 이름에 iSCSI 이니시에이터의 이름을 입력합니다. 이 이름은 Amazon iSCSI 자격 증명 이름(IQN)으로, 앞에 `iqn.1997-05.com.amazon:` 대상 이름이 붙습니다. 다음은 예입니다.

`iqn.1997-05.com.amazon:your-tape-device-name`

iSCSI initiator 소프트웨어를 사용하여 이니시에이터 이름을 찾을 수 있습니다. 예를 들어 Windows 클라이언트의 경우 이름은 iSCSI 이니시에이터의 구성 탭에 있는 값입니다. 자세한 내용은 [Windows 클라이언트CHAP에서 상호 구성](#) 단원을 참조하십시오.

Note

이니시에이터 이름을 변경하려면 먼저 를 비활성화하고 iSCSI 이니시에이터 소프트웨어에서 이니시에이터 이름을 CHAP변경한 다음 CHAP 새 이름으로 활성화해야 합니다.

- b. 이니시에이터를 인증하는 데 사용되는 암호에 요청된 암호를 입력합니다.

이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 이니시에이터(즉, Windows 클라이언트)가 CHAP 대상에 참여하기 위해 알아야 하는 보안 키입니다.

- c. 대상 인증에 사용되는 보안 암호(상호 CHAP)에 요청된 보안 암호를 입력합니다.

이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 대상이 CHAP 이니시에이터에 참여하기 위해 알아야 하는 보안 키입니다.

Note

대상을 인증하는 데 사용한 비밀 문구는 초기자 인증을 위한 비밀 문구와는 달라야 합니다.

- d. 저장(Save)을 선택합니다.

5. VTL 디바이스 탭에서 iSCSI CHAP 인증 필드가 true 로 설정되어 있는지 확인합니다.

Windows 클라이언트CHAP에서 상호 구성

이 절차에서는 콘솔CHAP의 볼륨에 CHAP 대해 구성하는 데 사용한 것과 동일한 키를 사용하여 Microsoft iSCSI 이니시에이터에서 를 구성합니다.

1. iSCSI 이니시에이터가 아직 시작되지 않은 경우 Windows 클라이언트 컴퓨터의 시작 메뉴에서 실행 을 선택하고 를 입력한 **iscsicpl.exe** 다음 확인을 선택하여 프로그램을 실행합니다.
2. 이니시에이터(즉, Windows 클라이언트)에 대한 상호 CHAP 구성을 구성합니다.
 - a. 구성 탭을 선택합니다.

Note

이니시에이터 이름 값은 초기자 및 회사에 고유합니다. 앞의 이름은 Storage Gateway 콘솔의 CHAP 인증 구성 대화 상자에서 사용한 값입니다.
예시 이미지에 표시된 이름은 데모용일 뿐입니다.

- b. 를 선택합니다CHAP.
- c. iSCSI Initiator Mutual Chap Secret 대화 상자에서 상호 CHAP 비밀 값을 입력합니다.

이 대화 상자에서 초기자(Windows 클라이언트)가 대상(스토리지 볼륨)을 인증하는 데 사용하는 비밀 문구를 입력합니다. 이 비밀 문구를 사용하면 대상이 초기자에(서) 읽고 쓸 수 있습니다. 이 보안 암호는 CHAP 인증 구성 대화 상자의 대상 인증(상호 CHAP)에 사용되는 보안 암호 상자에 입력된 보안 암호와 동일합니다. 자세한 내용은 [iSCSI 대상에 대한 CHAP 인증 구성](#) 단원을 참조하십시오.

- d. 입력한 키의 길이가 12자 미만이거나 16자를 초과하는 경우 이니시에이터 CHAP 보안 암호 오류 대화 상자가 나타납니다.

확인을 선택한 후 키를 다시 입력합니다.

3. 이니시에이터의 보안 암호로 대상을 구성하여 상호 CHAP 구성을 완료합니다.

- a. 대상 탭을 선택합니다.
- b. 에 대해 구성하려는 대상이 CHAP 현재 연결되어 있는 경우 대상을 선택하고 연결 해제를 선택합니다.
- c. 에 구성할 대상을 선택한 CHAP다음 연결을 선택합니다.
- d. Connect to Target(대상으로 연결) 대화 상자에서 고급을 선택합니다.
- e. 고급 설정 대화 상자에서 를 구성합니다CHAP.
 - i. CHAP 로그인 활성화를 선택합니다.
 - ii. 이니시에이터를 인증하는 데 필요한 암호를 입력합니다. 이 보안 암호는 CHAP 인증 구성 대화 상자의 시작자 인증에 사용되는 보안 암호 상자에 입력된 보안 암호와 동일합니다. 자세한 내용은 [iSCSI 대상에 대한 CHAP 인증 구성](#) 단원을 참조하십시오.
 - iii. Perform mutual authentication(상호 인증 수행)을 선택합니다.
 - iv. 변경 사항을 적용하려면 확인을 선택합니다.
- f. Connect to Target(대상으로 연결) 대화 상자에서 확인을 선택합니다.

4. 정확한 비밀 키를 입력하면 대상이 연결 상태 상태로 표시됩니다.

Red Hat Linux 클라이언트CHAP에서 상호 구성

이 절차에서는 Storage Gateway 콘솔CHAP의 볼륨에 CHAP 대해 를 구성하는 데 사용한 것과 동일한 키를 사용하여 Linux iSCSI 이니시에이터에서 를 구성합니다.

1. iSCSI 데몬이 실행 중이고 대상에 이미 연결되어 있는지 확인합니다. 이 두 작업을 완료하지 않은 경우, [Linux 클라이언트에 연결](#) 섹션을 참조하세요.
2. 구성하려는 대상에 대한 기존 구성을 분리하고 제거합니다CHAP.
 - a. 대상 이름을 찾고 그것이 정의된 구성인지 확인하려면 다음 명령을 사용하여 저장된 구성의 목록을 조회합니다.

```
sudo /sbin/iscsiadm --mode node
```

- b. 대상에서 연결을 해제합니다.

다음 명령 **myvolume**은 Amazon iSCSI 적격 이름()에 정의된 라는 대상과 연결이 해제됩니다 IQN. 상황에 IQN 따라 대상 이름 및 를 변경합니다.

```
sudo /sbin/iscsiadm --mode node --logout GATEWAY_IP:3260,1  
iqn.1997-05.com.amazon:myvolume
```

- c. 대상에 대한 구성을 제거합니다.

다음 명령은 **myvolume** 대상에 대한 구성을 제거합니다.

```
sudo /sbin/iscsiadm --mode node --op delete --targetname  
iqn.1997-05.com.amazon:myvolume
```

3. iSCSI 구성 파일을 편집하여 를 활성화합니다CHAP.

- a. 초기자(즉 사용 중인 클라이언트)의 이름을 가져옵니다.

다음 명령은 `/etc/iscsi/initiatorname.iscsi` 파일에서 초기자 이름을 가져옵니다.

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

이 명령의 출력은 다음과 같습니다.

InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8

- b. /etc/iscsi/iscsid.conf 파일을 엽니다.
- c. 파일에서 다음 줄의 주석을 취소하고 에 대한 올바른 값을 지정합니다. *username*, *password*, *username_in*, 및 *password_in*.

```
node.session.auth.authmethod = CHAP
node.session.auth.username = username
node.session.auth.password = password
node.session.auth.username_in = username_in
node.session.auth.password_in = password_in
```

지정할 값에 대한 지침은 다음 표를 참조하십시오.

구성 설정	값
<i>username</i>	이 절차의 이전 단계에서 찾은 초기자 이름. 그 값은 IQN으로 시작합니다. 예를 들어 iqn.1994-05.com.redhat:8e89b27b5b8 는 유효한 <i>username</i> 값입니다.
<i>password</i>	초기자(사용 중인 클라이언트)가 볼륨과 통신할 때 초기자를 인증하는 데 사용하는 비밀 키
<i>username_in</i>	대상 볼륨IQN의 . 이 값은 IQN으로 시작하여 대상 이름으로 끝납니다. 예를 들어 iqn.1997-05.com.amazon:myvolume 는 유효한 <i>username_in</i> 값입니다.
<i>password_in</i>	대상(볼륨)이 초기자와 통신할 때 대상을 인증하는 데 사용하는 비밀 키

- d. 구성 파일에 변경 사항을 저장한 후 파일을 닫습니다.
4. 대상을 검색하여 로그인합니다. 이렇게 하려면 [Linux 클라이언트에 연결](#)에 설명된 단계를 수행하세요.

Storage AWS Direct Connect Gateway와 함께 사용

AWS Direct Connect 내부 네트워크를 Amazon Web Services 클라우드에 연결합니다. Storage AWS Direct Connect Gateway와 함께 사용하면 처리량이 높은 워크로드 요구 사항에 맞는 연결을 생성하여 온프레미스 게이트웨이와 간에 전용 네트워크 연결을 제공할 수 있습니다. AWS

Storage Gateway는 퍼블릭 엔드포인트를 사용합니다. AWS Direct Connect 연결이 설정되면 퍼블릭 가상 인터페이스를 생성하여 트래픽이 Storage Gateway 엔드포인트로 라우팅되도록 할 수 있습니다. 퍼블릭 가상 인터페이스는 네트워크 경로에서 인터넷 서비스 제공업체를 우회합니다. Storage Gateway 서비스 퍼블릭 엔드포인트는 AWS Direct Connect 위치와 동일한 AWS 지역에 있거나 다른 AWS 지역에 있을 수 있습니다.

다음 그림은 Storage Gateway와 함께 AWS Direct Connect 작동하는 방식의 예를 보여줍니다. Storage Gateway가 AWS 직접 연결을 사용하여 클라우드에 연결된 것을 보여주는 네트워크 아키텍처

다음 절차에서는 생성된 게이트웨이가 제대로 작동 중이라고 가정합니다.

Storage AWS Direct Connect Gateway와 함께 사용하려면

1. 온프레미스 데이터 센터와 Storage Gateway 엔드포인트 간의 AWS Direct Connect 연결을 생성하고 설정합니다. 연결 생성 방법에 대한 자세한 내용은 [AWS Direct Connect 사용 설명서에서 AWS Direct Connect 시작하기](#)를 참조하세요.
2. 온프레미스 Storage Gateway 어플라이언스를 AWS Direct Connect 라우터에 연결합니다.
3. 퍼블릭 가상 인터페이스를 생성하고 이에 따라 온프레미스 라우터를 구성합니다. Direct Connect를 사용하는 경우에도 VPC 엔드포인트는 를 사용하여 생성해야 합니다. HAProxy 자세한 내용은 [AWS Direct Connect 사용 설명서에서 가상 인터페이스 생성](#)을 참조하세요.

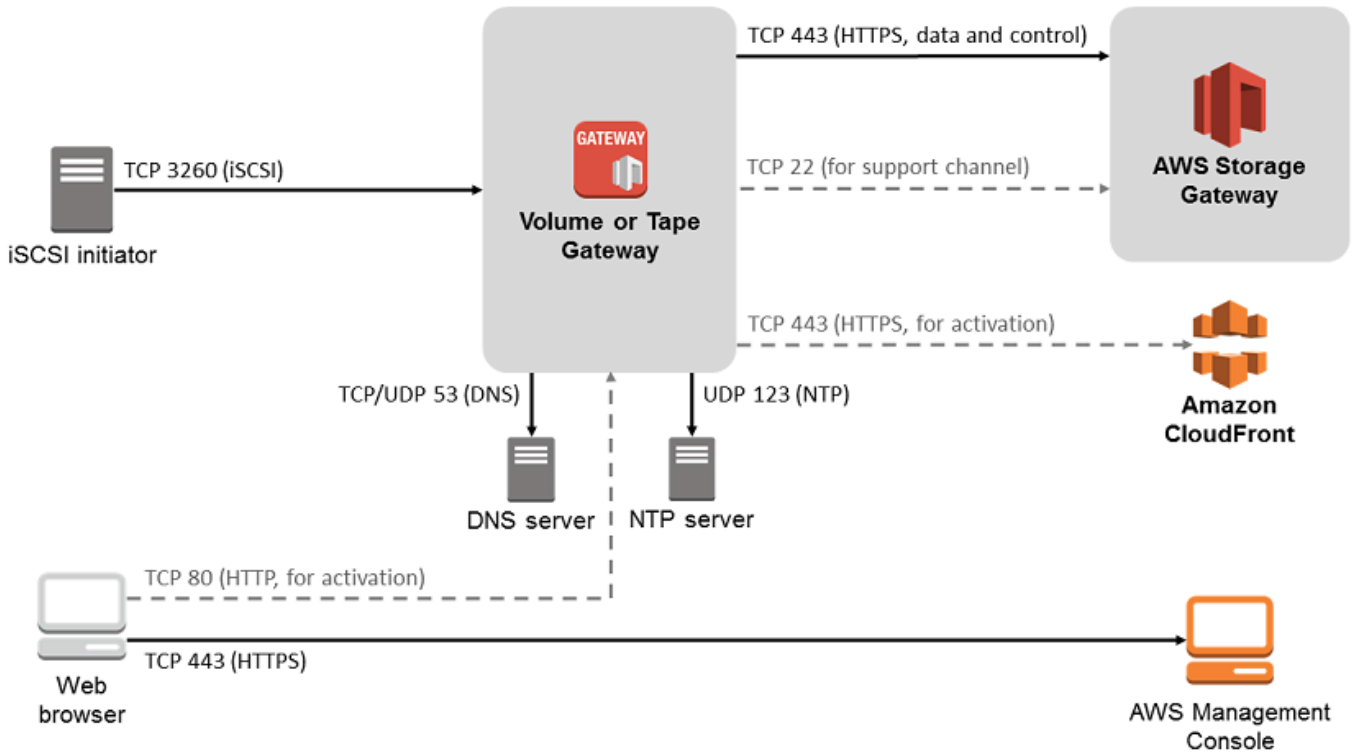
에 대한 자세한 내용은 [AWS Direct Connect AWS Direct Connect 무엇입니까](#)를 참조하십시오. AWS Direct Connect 사용 설명서에서.

Tape Gateway에 대한 포트 요구 사항

Storage Gateway가 작동하려면 다음 포트가 필요합니다. 일부 포트는 모든 게이트웨이 유형에 공통적으로 필요한 포트입니다. 그 밖에 특정 유형의 게이트웨이에 필요한 포트도 있습니다. 이 섹션에서는 Tape Gateway에 필요한 포트의 그림과 목록을 확인할 수 있습니다.

Tape Gateway

다음은 Tape Gateway 게이트웨이 작동을 위해 열어야 하는 모든 포트를 보여주는 그림입니다.



다음 포트는 모든 게이트웨이 유형에 공통적으로 필요한 포트입니다.

From	To	프로토콜	Port	용도
Storage Gateway VM	AWS	전송 제어 프로토콜(TCP)	443(HTTPS)	Storage Gateway 아웃바운드 VM에서 AWS 서비스 엔드포인트로의 통신용입니다. 서비스 엔드포인트에 대한 자세한 내용은 방화벽 및 라우터를 통한 AWS Storage Gateway 액세스

From	To	프로토콜	Port	용도	
				세스 허용 단 원을 참조하 십시오.	

From	To	프로토콜	Port	용도
웹 브라우저	Storage Gateway VM	TCP	80(HTTP)	<p>Storage Gateway 활성화 키를 가져올 때 로컬 시스템에서 사용합니다. 포트 80은 Storage Gateway 어플라이언스 활성화 중에만 사용됩니다.</p> <p>Storage Gateway VM에 대한 공개 액세스에는 포트 80이 필요하지 않습니다. 포트 80에 액세스하는데 필요한 권한 수준은 네트워크 구성에 따라 다릅니다. Storage Gateway Management Console에서 게이트웨이를 활성화하는 경우, 콘솔에 연결하</p>

From	To	프로토콜	Port	용도
				는 호스트가 게이트웨이의 포트 80에 액세스할 수 있어야 합니다.
Storage Gateway VM	도메인 이름 서비스(DNS) 서버	사용자 데이터그램 프로토콜(UDP)/UDP	53(DNS)	Storage Gateway VM 과 DNS 서버 간의 통신용입니다.
Storage Gateway VM	AWS	TCP	22(지원 채널)	AWS Support 가 게이트웨이에 액세스하여 게이트웨이 문제를 해결할 수 있도록 허용합니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다.

From	To	프로토콜	Port	용도
Storage Gateway VM	Network Time Protocol(NTP) 서버	UDP	123(NTP)	<p>로컬 시스템이 VM 시간을 호스트 시간과 동기화하는 데 사용됩니다. Storage Gateway VM은 다음 NTP 서버를 사용하도록 구성됩니다.</p> <ul style="list-style-type: none"> • 0.amazon.pool.ntp.org • 1.amazon.pool.ntp.org • 2.amazon.pool.ntp.org • 3.amazon.pool.ntp.org
Storage Gateway 하드웨어 어플라이언스	하이퍼텍스트 전송 프로토콜(HTTP) 프록시	TCP	8080(HTTP)	정품 인증에 잠시 필요합니다.

공통 포트 외에 Tape Gateway에는 다음 포트가 필요합니다.

From	To	프로토콜	Port	용도
iSCSI 이니시 에이터	Storage Gateway VM	TCP	3260(iSCSI)	로컬 시스템에서 게이트웨이에 의해 노출된 iSCSI 대상에 연결합니다.

게이트웨이 어플라이언스의 IP 주소 가져오기

호스트를 선택하고 게이트웨이 VM을 배포한 후 게이트웨이를 연결하고 활성화합니다. 이렇게 하려면 게이트웨이 VM의 IP 주소가 필요합니다. IP 주소는 게이트웨이의 로컬 콘솔에서 얻을 수 있습니다. 로컬 콘솔에 로그인하여 콘솔 페이지의 상단에서 IP 주소를 얻습니다.

온프레미스에 배포된 게이트웨이의 경우, 하이퍼바이저에서 IP 주소를 얻을 수도 있습니다. Amazon EC2 게이트웨이의 경우 Amazon EC2 Management Console에서 Amazon EC2 인스턴스의 IP 주소를 가져올 수도 있습니다. 게이트웨이의 IP 주소를 얻는 방법은 다음 중 하나를 참조하십시오.

- VMware 호스트: [를 사용하여 Gateway Local Console에 액세스 VMware ESXi](#)
- HyperV 호스트: [Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스](#)
- Linux 커널 기반 가상 머신(KVM) 호스트: [Linux를 사용하여 Gateway Local Console에 액세스 KVM](#)
- EC2 호스트: [Amazon EC2 호스트에서 IP 주소 가져오기](#)

IP 주소를 찾았으면 적어 둡니다. 그런 다음 Storage Gateway 콘솔로 돌아가서 콘솔에 IP 주소를 입력합니다.

Amazon EC2 호스트에서 IP 주소 가져오기

게이트웨이가 배포된 Amazon EC2 인스턴스의 IP 주소를 가져오려면 EC2 인스턴스의 로컬 콘솔에 로그인합니다. 그런 다음 콘솔 페이지 상단에서 IP 주소를 얻습니다. 지침은 [Amazon EC2 Gateway Local Console에 로그인](#) 단원을 참조하십시오.

Amazon EC2 Management Console에서 IP 주소를 가져올 수도 있습니다. 활성화에는 퍼블릭 IP 주소를 사용하는 것이 좋습니다. 퍼블릭 IP 주소를 얻으려면 절차 1을 사용합니다. 그 대신 탄력적 IP 주소를 사용하려면 절차 2를 사용합니다.

절차 1: 퍼블릭 IP 주소를 사용하여 게이트웨이에 연결하려면

1. 에서 Amazon EC2 콘솔을 엽니다 <https://console.aws.amazon.com/ec2/>.
2. 탐색 창에서 인스턴스 를 선택한 다음 게이트웨이가 배포되는 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 퍼블릭 IP 주소를 적어 둡니다. 이 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 IP 주소를 입력합니다.

활성화에 탄력적 IP 주소를 사용하려면 다음 절차를 사용합니다.

절차 2: 탄력적 IP 주소를 사용하여 게이트웨이에 연결하려면

1. 에서 Amazon EC2 콘솔을 엽니다 <https://console.aws.amazon.com/ec2/>.
2. 탐색 창에서 인스턴스 를 선택한 다음 게이트웨이가 배포되는 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 탄력적 IP 값을 적어 둡니다. 이 탄력적 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 탄력적 IP 주소를 입력합니다.
4. 게이트웨이가 활성화되면 방금 활성화한 게이트웨이를 선택한 다음 하단 패널에서 VTL 디바이스 탭을 선택합니다.
5. 모든 VTL 디바이스의 이름을 가져옵니다.
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 연결됩니다.

Storage Gateway 리소스 및 리소스에 대한 이해 IDs

Storage Gateway에서 기본 리소스는 게이트웨이이지만 다른 리소스 유형으로는 볼륨, 가상 테이프, iSCSI 타겟, vtl 디바이스 등이 있습니다. 이 유형들은 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

다음 표와 같이 이러한 리소스와 하위 리소스에는 고유한 Amazon 리소스 이름 (ARNs) 이 연결되어 있습니다.

리소스 유형	ARN형식
게이트웨이 ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i>
테이프 ARN	arn:aws:storagegateway: <i>region:account-id</i> :tape/ <i>tapebarcode</i>
타겟 ARN (iSCSI 타겟)	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /target/ <i>iSCSItarget</i>
VTLD디바이스 ARN	arn:aws:storagegateway: <i>region:account-id</i> :gateway/ <i>gateway-id</i> /device/ <i>vtldevice</i>

Storage Gateway는 EC2 인스턴스, EBS 볼륨 및 스냅샷의 사용도 지원합니다. 이러한 리소스는 Storage Gateway에서 사용되는 Amazon EC2 리소스입니다.

리소스 관련 작업 IDs

리소스를 생성할 때 Storage Gateway에서는 리소스에 고유 리소스 ID를 할당합니다. 이 리소스 ID는 리소스의 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 여기에서 sgw는 게이트웨이의 리소스 식별자입니다. 볼륨 ID가 vol-3344CCDD와 같은 형식이라면 여기에서 vol은 볼륨의 리소스 식별자입니다.

가상 테이프의 경우, 바코드 ID 앞에 접두사 문자를 최대 네 개까지 추가할 수 있어 테이프 체계화에 도움이 됩니다.

Storage Gateway IDs 리소스는 대문자입니다. 하지만 IDs Amazon에서 이러한 리소스를 사용하는 경우 EC2 API Amazon은 리소스가 IDs 소문자로 EC2 표시될 것으로 예상합니다. 와 함께 사용하려면 리소스 ID를 소문자로 변경해야 합니다. EC2 API 예를 들어 Storage Gateway에서 볼륨의 ID는 vol-1122AABB일 수 있습니다. 이 ID를 와 함께 사용하는 EC2 API 경우 이 ID를 로 변경해야 합니다. vol-1122aabb 그렇지 않으면 예상대로 작동하지 EC2 API 않을 수 있습니다.

Storage Gateway 리소스에 태그를 지정

Storage Gateway에서 태그를 사용하여 리소스를 관리할 수 있습니다. 태그를 사용하면 메타데이터를 리소스에 추가하고 리소스를 분류하여 관리하기가 편해집니다. 각 태그는 사용자가 정의하는 키-값 페

어로 구성됩니다. 게이트웨이, 볼륨 및 가상 테이프에 태그를 추가할 수 있습니다. 추가하는 태그에 따라 이 리소스를 검색하고 필터링할 수 있습니다.

예를 들어 태그를 사용하여 조직 내 각 부서에서 사용하는 Storage Gateway 리소스를 식별할 수 있습니다. `key=department` 및 `value=accounting`과 같이 회계 부서에서 사용하는 게이트웨이 및 볼륨에 태그를 지정할 수 있습니다. 그 다음에 이 태그로 필터링하여 회계 부서에서 사용하는 모든 게이트웨이 및 볼륨을 식별하고 이 정보를 통해 비용을 파악할 수 있습니다. 자세한 내용은 [비용 할당 태그 사용](#) 및 [Tag Editor 작업](#) 단원을 참조하십시오.

태그를 지정한 가상 테이프를 아카이브하는 경우, 테이프는 아카이브에서 자체 태그를 유지합니다. 이와 마찬가지로 아카이브에서 다른 게이트웨이로 테이프를 가져오는 경우, 태그는 새 게이트웨이에 유지됩니다.

태그에는 의미가 없으며 문자열로 해석됩니다.

태그에 적용되는 제한은 다음과 같습니다.

- 태그 키와 값은 대/소문자를 구분합니다.
- 각 리소스의 최대 태그 수는 50입니다.
- 태그 키는 `aws:`로 시작할 수 없습니다. 이 접두사는 AWS 용으로 예약되어 있습니다.
- 키 속성에 사용할 수 있는 문자는 UTF-8자의 문자와 숫자, 공백, 특수 문자 `+ - = . _ /` 및 `@`입니다.

태그 작업

Storage Gateway 콘솔, Storage Gateway 또는 Storage [Gateway API 명령줄 인터페이스 \(CLI\)](#) 를 사용하여 태그를 사용할 수 있습니다. 다음 절차에서는 콘솔에서 태그를 추가, 편집, 삭제하는 방법을 안내합니다.


태그를 추가하려면

1. <https://console.aws.amazon.com/storagegateway/> [집에서](#) Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 태그를 지정하려는 리소스를 선택합니다.

예를 들어 게이트웨이에 태그를 지정하려면 게이트웨이를 선택한 후 게이트웨이 목록에서 태그를 지정할 게이트웨이를 선택합니다.

3. 태그를 선택한 후 태그 추가/편집을 선택합니다.
4. 태그 추가/편집 대화 상자에서 태그 생성을 선택합니다.

- 키에 키를 입력하고 값에 값을 입력합니다. 예를 들어 키로는 **Department**를, 값으로는 **Accounting**을 입력할 수 있습니다.

 Note

값 상자를 공백으로 둘 수도 있습니다.

- 태그 생성을 선택하여 태그를 추가합니다. 리소스 한 개에 태그를 여러 개 추가할 수 있습니다.
- 태그 추가를 완료했으면 저장을 선택합니다.

태그를 편집하려면

- <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
- 편집하려는 태그가 있는 리소스를 선택합니다.
- 태그를 선택하여 태그 추가/편집 대화 상자를 엽니다.
- 편집하고자 하는 태그 옆의 연필 아이콘을 선택하여 태그를 편집합니다.
- 태그 편집을 완료했으면 저장을 선택합니다.

태그를 삭제하려면

- <https://console.aws.amazon.com/storagegateway/집에서> Storage Gateway 콘솔을 엽니다.
- 삭제하려는 태그가 있는 리소스를 선택합니다.
- 태그를 선택한 후 태그 추가/편집을 선택하여 태그 추가/편집 대화 상자를 엽니다.
- 삭제하고자 하는 태그 옆의 X 아이콘을 선택한 후 저장을 선택합니다.

Storage Gateway용 오픈 소스 구성 요소 작업

이 섹션에서는 Storage Gateway 기능을 제공하기 위해 사용하는 타사 도구 및 라이선스에 대해 설명합니다.

AWS Storage Gateway 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드는 다음 위치에서 다운로드할 수 있습니다.

- 에 배포된 게이트웨이의 경우 [source.tar](#)를 VMware ESXi 다운로드합니다.
- Microsoft Hyper-V에 배포된 게이트웨이의 경우 [sources_hyperv.tar](#)을 다운로드합니다.

- Linux 커널 기반 가상 머신(KVM)에 배포된 게이트웨이의 경우 [source_KVM.tar](#)를 다운로드합니다.

이 제품에는 OpenSSL Toolkit(<http://www.openssl.org/>)에서 사용할 수 있도록 OpenSSL Project에서 개발한 소프트웨어가 포함되어 있습니다. 모든 종속 타사 도구에 대한 관련 라이선스는 [타사 라이선스](#)를 참조하십시오.

AWS Storage Gateway 할당량

이 주제에서는 Storage Gateway의 볼륨 및 테이프 할당량, 구성 및 성능 한도에 대한 정보를 확인할 수 있습니다.

주제

- [테이프 할당량](#)
- [게이트웨이에 권장되는 로컬 디스크 크기](#)

테이프 할당량


다음 표에는 테이프 할당량이 나와 있습니다.

설명	Tape Gateway
가상 테이프의 최소 크기	100GiB
가상 테이프의 최대 크기	15TiB
게이트웨이에 할당된 최대 가상 테이프 수	1,500
게이트웨이에 할당된 모든 테이프의 총 크기	1PiB
아카이브에 있는 가상 테이프의 최대 개수	제한 없음
아카이브에 있는 모든 테이프의 총 크기	제한 없음

게이트웨이에 권장되는 로컬 디스크 크기

다음은 배포된 게이트웨이의 로컬 디스크 스토리지에 권장되는 크기를 보여주는 표입니다.

게이트웨이 유형	캐시(최소값)	캐시(최대값)	업로드 버퍼 (최소값)	업로드 버퍼 (최대값)	필요한 다른 로컬 디스크
Tape Gateway	150GiB	64TiB	150GiB	2TiB	—

 Note

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

APIStorage Gateway에 대한 참조

콘솔을 사용하는 것 외에도 를 사용하여 AWS Storage Gateway API 게이트웨이를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 이 섹션에서는 AWS Storage Gateway 작업, 인증을 위한 요청 서명 및 오류 처리에 대해 설명합니다. Storage Gateway에 사용할 수 있는 리전 및 엔드포인트에 대한 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

Note

를 사용하여 애플리케이션을 개발할 AWS SDKs 때도 를 사용할 수 AWS Storage Gateway 있습니다. Java의 AWS SDKs 경우, NET기본 AWS Storage Gateway API 요소를 PHP 래핑하여 프로그래밍 작업을 단순화합니다. SDK라이브러리 다운로드에 대한 자세한 내용은 [샘플 코드 라이브러리](#)를 참조하십시오.

주제

- [Storage Gateway 필수 요청 헤더](#)
- [요청에 서명하기](#)
- [오류 응답](#)
- [작업](#)

Storage Gateway 필수 요청 헤더

이 섹션에서는 모든 POST 요청과 함께 Storage Gateway에 전송해야 하는 필수 헤더에 대해 설명합니다. HTTP헤더를 포함하여 호출하려는 작업, 요청 날짜, 요청 발신자의 승인을 나타내는 정보 등 요청의 주요 정보를 식별할 수 있습니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음 예제는 작업에 사용되는 헤더를 보여줍니다. [ActivateGateway](#)

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
```

```
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

Storage Gateway에 대한 POST 요청에 포함해야 하는 헤더는 다음과 같습니다. “x-amz”로 시작하는 아래 헤더는 특정 헤더입니다. AWS나열된 다른 모든 헤더는 트랜잭션에 사용되는 공통 헤더입니다.
HTTP

헤더	설명
Authorization	<p>권한 부여 헤더는 Storage Gateway가 해당 요청이 요청자에게 유효한 작업인지 판단할 수 있게 해주는 요청에 대한 몇 가지 정보를 포함합니다. 이 헤더의 형식은 다음과 같습니다(가독성을 높이기 위해 줄 바꿈 추가).</p> <pre>Authorization: AWS4-HMAC_SHA456 Credentials= <i>YourAccessKey</i> /<i>yyyymmdd</i>/<i>region</i>/storagegateway/aw s4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-targ et, Signature= <i>CalculatedSignature</i></pre> <p>위 구문에서는 년, 월 <i>YourAccessKey</i>, 일 (<i>yyyymmdd</i>), 지역 및 시간을 지정합니다. <i>CalculatedSignature</i> 승인 헤더의 형식은 V4 서명 프로세스의 요구 사항에 따라 달라집니다. AWS 서명 관련 세부 정보는 요청에 서명하기 단원에 나와 있습니다.</p>
Content-Type	<p>application/x-amz-json-1.1 을 Storage Gateway에 대한 모든 요청의 콘텐츠 유형으로 사용합니다.</p> <pre>Content-Type: application/x-amz-json-1.1</pre>
Host	<p>호스트 헤더를 사용하여 요청을 전송하는 Storage Gateway 엔드포인트를 지정합니다. 예를 들어, storagegateway.us-east-2.amazonaws.com 은 미국 동부(오하이오) 리전의 엔드포인트입니다. Storage Gateway에 사용할 수 있는 엔드포인트에 대한 자세한 내용은 AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.</p>

헤더	설명
	Host: storagegateway. <i>region</i> .amazonaws.com
x-amz-date	<p>HTTPDate헤더 또는 헤더에 타임스탬프를 제공해야 합니다. AWS x-amz-date (일부 HTTP 클라이언트 라이브러리에서는 Date 헤더를 설정할 수 없습니다.) x-amz-date 헤더가 있으면 Storage Gateway는 요청 인증 중 모든 Date 헤더를 무시합니다. x-amz-date 형식은 YYYYMMDD 'T' Z HHMMSS '형식의 ISO86 01 Basic이어야 합니다. Date 및 x-amz-date 헤더를 모두 사용하는 경우 Date 헤더의 형식은 ISO86 01이 아니어도 됩니다.</p> <p>x-amz-date: <i>YYYYMMDD 'T' HHMMSS 'Z'</i></p>
x-amz-target	<p>이 헤더는 요청하려는 작업 API 및 의 버전을 지정합니다. 대상 헤더 값은 API 버전과 API 이름을 연결하여 구성되며 형식은 다음과 같습니다.</p> <p>x-amz-target: StorageGateway_ <i>APIversion</i> .<i>operationName</i></p> <p>operationName값 (예: "ActivateGateway")은 API 목록에서 찾을 수 있습니다. APIStorage Gateway에 대한 참조</p>

요청에 서명하기

Storage Gateway에서는 요청에 서명하여 전송하는 모든 요청을 인증해야 합니다. 요청에 서명하려면 암호화 해시 함수를 이용해 디지털 서명을 계산해야 합니다. 암호화 해시는 입력을 근거로 하여 고유 해시 값을 반환하는 함수입니다. 해시 함수에 대한 입력에는 요청 텍스트와 보안 액세스 키가 포함됩니다. 해시 함수는 요청에 서명으로 포함하는 해시 값을 반환합니다. 서명은 요청에서 Authorization 헤더의 일부입니다.

Storage Gateway는 요청을 수신한 후, 사용자가 요청에 서명할 때와 동일한 해시 함수 및 입력을 사용하여 서명을 재계산합니다. 결과 서명이 요청 서명과 일치할 경우 Storage Gateway에서 요청을 처리합니다. 그렇지 않으면 요청이 거부됩니다.

Storage Gateway는 [AWS Signature Version 4](#)를 이용한 인증을 지원합니다. 서명을 계산하기 위한 프로세스는 다음 세 작업으로 나뉠 수 있습니다.

- [작업 1: 정식 요청 생성](#)

HTTP요청을 표준 형식으로 재배열하십시오. 정규 형식을 사용해야 하는 이유는 Storage Gateway에서 서명을 재계산하여 사용자가 보낸 서명과 비교할 때 동일한 정규 형식을 사용하기 때문입니다.

- [작업 2: 서명할 문자열 생성](#)

암호화 해시 함수에 대한 입력 값 중 하나로 사용할 문자열을 만듭니다. 서명할 문자열이라는 문자열은 해시 알고리즘의 이름, 요청 날짜, 자격 증명 범위 문자열, 이전 작업에서 정규화된 요청을 연결한 것입니다. 자격 증명 범위 문자열 자체는 날짜, 리전 및 서비스 정보를 연결한 것입니다.

- [작업 3: 서명 생성](#)

서명할 문자열과 파생된 의 두 입력 문자열을 허용하는 암호화 해시 함수를 사용하여 요청에 대한 서명을 만듭니다. 파생된 키는 보안 액세스 키로 시작하여 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드 () 를 생성하여 계산됩니다. HMACs

서명 계산 예시

다음 예제에서는 서명을 만드는 방법에 대한 세부 정보를 안내합니다. [ListGateways](#) 이 예시는 서명 계산 방법을 점검하기 위한 참조로 사용할 수 있습니다. 다른 참조 계산은 Amazon Web Services 글로셔리의 [서명 버전 4 테스트 제품군](#)에 포함되어 있습니다.

이 예시에서는 다음과 같이 가정합니다.

- 요청의 타임스탬프는 “2012년 9월 10일 월요일 00:00:00 “입니다. GMT
- 엔드포인트는 미국 동부(오하이오) 리전입니다.

일반 요청 구문 (본문 포함) 은 JSON 다음과 같습니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

[작업 1: 정식 요청 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. 이 API (또는 Storage Gateway APIs) 에 대한 쿼리 매개 변수가 없기 때문입니다.

[작업 2: 서명할 문자열 생성](#)의 경우 서명할 문자열은 다음과 같습니다.

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

서명할 문자열의 첫째 줄은 알고리즘, 둘째 줄은 타임스탬프, 셋째 줄은 자격 증명 범위, 마지막 줄은 작업 1 정규 요청의 해시입니다.

[작업 3: 서명 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/bPxrFiCYEXAMPLEKEY를 사용하는 경우, 계산된 서명은 다음과 같습니다.

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

마지막 단계는 Authorization 헤더를 생성하는 것입니다. 데모 액세스 키의 AKIAIOSFODNN7EXAMPLE 경우 헤더 (가독성을 위해 줄 바꿈을 추가함) 는 다음과 같습니다.

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

오류 응답

주제

- [예외](#)
- [작업 오류 코드](#)
- [오류 응답](#)

이 섹션에서는 AWS Storage Gateway 오류에 대한 참조 정보를 제공합니다. 이 오류는 오류 예외 및 작업 오류 코드로 표시됩니다. 예를 들어 요청 서명에 문제가 있는 경우 모든 API 응답에서 오류 `InvalidSignatureException` 예외가 반환됩니다. 그러나 작업 오류 `ActivationKeyInvalid` 코드는 에 대해서만 반환됩니다 [ActivateGatewayAPI](#).

오류 유형에 따라 Storage Gateway는 예외만 반환하거나 예외와 작업 오류 코드를 모두 반환할 수 있습니다. 오류 응답 예시는 [오류 응답](#)에 있습니다.

예외

다음 표에는 AWS Storage Gateway API 예외가 나열되어 있습니다. AWS Storage Gateway 작업에서 오류 응답을 반환하는 경우 응답 본문에는 이러한 예외 중 하나가 포함됩니다.

`InternalServerError`와 `InvalidGatewayRequestException`은 특정 작업 오류 코드를 부여하는 작업 오류 코드([작업 오류 코드](#)) 메시지 코드 중 하나를 반환합니다.

예외	메시지	HTTP상태 코드
<code>IncompleteSignatureException</code>	지정한 서명이 불완전합니다.	400 잘못된 요청
<code>InternalFailure</code>	알 수 없는 오류, 예외 또는 장애로 인해 요청 처리가 실패했습니다.	500 Internal Server Error
<code>InternalServerError</code>	작업 오류 코드 작업 오류 코드 메시지 코드 중 하나입니다.	500 Internal Server Error

예외	메시지	HTTP상태 코드
InvalidAction	요청된 동작 또는 작업이 유효하지 않습니다.	400 잘못된 요청
InvalidClientTokenId	제공된 X.509 인증서 또는 AWS 액세스 키 ID는 당사 기록에 존재하지 않습니다.	403 금지됨
InvalidGatewayRequestException	작업 오류 코드 의 작업 오류 코드 메시지 중 하나입니다.	400 잘못된 요청
InvalidSignatureException	우리가 계산한 요청 서명이 사용자가 제공한 서명과 일치하지 않습니다. AWS 액세스 키와 서명 방법을 확인하세요.	400 잘못된 요청
MissingAction	요청에서 작업 또는 작업 파라미터가 누락되었습니다.	400 잘못된 요청
MissingAuthenticationToken	요청에는 유효한 (등록된) AWS 액세스 키 ID 또는 X.509 인증서가 포함되어야 합니다.	403 금지됨
RequestExpired	요청이 만료 날짜 또는 요청 날짜(15분 패딩)를 지났거나 요청 날짜가 향후 15분 초과 후에 효력이 발생합니다.	400 잘못된 요청
SerializationException	직렬화 도중에 오류가 발생했습니다. JSON페이로드의 형식이 올바른지 확인하세요.	400 잘못된 요청
ServiceUnavailable	서버의 일시적 장애로 인해 요청이 실패했습니다.	[503 Service Unavailable]
SubscriptionRequiredException	AWS 액세스 키 ID를 사용하려면 서비스에 가입해야 합니다.	400 잘못된 요청
ThrottlingException	속도를 초과하였습니다.	400 잘못된 요청

예외	메시지	HTTP상태 코드
TooManyRequests	요청이 너무 많음.	429 요청이 너무 많음
UnknownOperationException	알 수 없는 작업을 지정하였습니다. 유효한 작업은 Storage Gateway의 작업 에 나열되어 있습니다.	400 잘못된 요청
UnrecognizedClientException	요청에 포함된 보안 토큰이 유효하지 않습니다.	400 잘못된 요청
ValidationException	입력 파라미터의 값이 잘못되었거나 범위를 벗어났습니다.	400 잘못된 요청

작업 오류 코드

다음 표에는 작업 오류 코드와 해당 코드를 반환할 수 APIs 있는 AWS Storage Gateway 작업 오류 코드 간의 매핑이 나와 있습니다. 모든 작업 오류 코드는 [예외](#)에 설명된 두 가지 일반 예외 (InternalServerError 및 InvalidGatewayRequestException) 중 하나와 함께 반환됩니다.

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
ActivationKeyExpired	지정한 정품 인증 키가 만료되었습니다.	ActivateGateway
ActivationKeyInvalid	지정한 정품 인증 키가 유효하지 않습니다.	ActivateGateway
ActivationKeyNotFound	지정한 정품 인증 키를 찾을 수 없습니다.	ActivateGateway
BandwidthThrottleScheduleNotFound	지정한 대역폭 제한을 찾을 수 없습니다.	DeleteBandwidthRateLimit
CannotExportSnapshot	지정한 스냅샷을 내보낼 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InitiatorNotFound	지정된 초기자를 찾을 수 없습니다.	DeleteChapCredentials
DiskAlreadyAllocated	지정한 디스크가 이미 할당되었습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	지정한 디스크가 존재하지 않습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	지정한 디스크가 기가바이트 정렬되어 있지 않습니다.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	지정한 디스크 크기가 최대 볼륨 크기보다 큼니다.	CreateStorediSCSIVolume
DiskSizeLessThanVolumeSize	지정한 디스크 크기가 볼륨 크기보다 작습니다.	CreateStorediSCSIVolume
DuplicateCertificateInfo	지정한 인증서 정보가 중복되어 있습니다.	ActivateGateway

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayInternalError	게이트웨이 내부 오류가 발생하였습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotConnected	지정한 게이트웨이가 연결되지 않았습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotFound	지정한 게이트웨이를 찾을 수 없습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListLocalDisks
		ListVolumes
		ListVolumeRecoveryPoints
		ShutdownGateway
		StartGateway
		UpdateBandwidthRateLimit
		UpdateChapCredentials
		UpdateMaintenanceStartTime
		UpdateGatewaySoftwareNow
		UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayProxyNetworkConnectionBusy	지정한 게이트웨이 프록시 네트워크 연결이 사용 중입니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InternalError	내부 오류가 발생했습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		<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	메시지	이 오류 코드를 반환하는 작업
InvalidParameters	지정한 요청에 잘못된 파라미터가 포함되어 있습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
LocalStorageLimitExceeded	로컬 스토리지 한도를 초과했습니다.	AddCache AddUploadBuffer AddWorkingStorage
LunInvalid	지정된 내용이 LUN 을 바르지 않습니다.	CreateStorédiSCSIVolume

작업 오류 코드	메시지	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	메시지	이 오류 코드를 반환하는 작업
NotSupported	지정한 작업을 지원하지 않습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	지정한 게이트웨이의 날짜가 만료되었습니다.	ActivateGateway
SnapshotInProgressException	지정한 스냅샷이 진행 중입니다.	DeleteVolume
SnapshotIdInvalid	지정한 스냅샷이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	스테이징 영역이 가득 찼습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
TargetAlreadyExists	지정한 대상이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	지정한 대상이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	지정한 대상을 찾을 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
UnsupportedOperationForGatewayType	지정한 작업이 게이트웨이 유형에 유효하지 않습니다.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	지정한 볼륨이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	지정한 볼륨이 유효하지 않습니다.	DeleteVolume
VolumeInUse	지정한 볼륨이 이미 사용 중입니다.	DeleteVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
VolumeNotFound	지정한 볼륨을 찾을 수 없습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	지정한 볼륨이 아직 준비되지 않았습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

오류 응답

오류가 있는 경우, 응답 헤더 정보에는 다음 내용이 포함됩니다.

- 콘텐츠 유형: 애플리케이션/ -1.1 x-amz-json
- 적절한 또는 상태 코드 4xx 5xx HTTP

오류 응답의 본문에는 발생한 오류에 대한 정보가 포함됩니다. 다음 샘플 오류 응답은 모든 오류 응답에 공통된 응답 요소의 출력 구문을 나타냅니다.

```
{
  "__type": "String",
  "message": "String",
  "error":
    { "errorCode": "String",
      "errorDetails": "String"
    }
}
```



```
}

```

다음 표에서는 위 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__타입

[예외](#)의 예외 중 하나.

유형: 문자열

오류

API특정 오류 세부 정보가 들어 있습니다. 일반적인 오류 (즉, 특정 오류가 아닌 경우API) 에는 이 오류 정보가 표시되지 않습니다.

유형: 컬렉션

errorCode

작업 오류 코드 중 하나입니다 .

유형: 문자열

errorDetails

이 필드는 최신 버전의 에서는 사용되지 않습니다API.

유형: 문자열

message

작업 오류 코드 메시지 중 하나입니다.

유형: 문자열

오류 응답 예시

를 사용하고 존재하지 않는 게이트웨이 ARN 요청 입력을 지정하면 다음 JSON 본문이 반환됩니다.

DescribeStoreId SCSIVolumes API

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {

```

```
"errorCode": "VolumeNotFound"
}
```

Storage Gateway에서 요청과 함께 전송된 서명과 일치하지 않는 서명을 계산하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
provided."
}
```

Storage Gateway의 작업

Storage Gateway 작업 목록은 AWS Storage Gateway API참조 자료의 [작업을](#) 참조하십시오.

Tape Gateway 사용 설명서의 문서 기록

- API 버전: 2013-06-30
- 최신 설명서 업데이트: 2020년 11월 24일

다음 표에서는 2018년 4월 이후 AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서의 업데이트에 대한 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
FSx File Gateway의 가용성 변경 알림	AWS Storage Gateway의 FSx File Gateway는 10/28/24부터 더 이상 신규 고객이 사용할 수 없습니다. 서비스를 사용하려면 해당 날짜 이전에 가입해야 합니다. FSx File Gateway의 기존 고객은 서비스를 정상적으로 계속 사용할 수 있습니다. FSx File Gateway와 유사한 기능은 이 블로그 게시물을 참조하세요.	2024년 9월 26일
유지 관리 업데이트를 켜거나 끄는 옵션 추가	Storage Gateway는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안을 해결하기 위한 수정 사항, 새로운 기능에 대한 액세스를 포함할 수 있는 정기 유지 관리 업데이트를 받습니다. 이제 배포의 각 개별 게이트웨이에 대해 이러한 업데이트를 켜거나 끄도록 설정을 구성할 수 있습니다. 자세한 내용은 AWS Storage Gateway 콘솔을 사용하여 게이트웨이	2024년 6월 6일

	업데이트 관리를 참조하세요. 콘솔.	
Snowball Edge의 Tape Gateway에 대한 지원 중단	더 이상 Snowball Edge 디바이스에서 Tape Gateway를 호스팅할 수 없습니다.	2024년 3월 14일
타사 애플리케이션을 사용하여 게이트웨이 설정을 테스트하기 위한 지침이 업데이트됨	타사 애플리케이션을 사용하여 게이트웨이 설정을 테스트하는 지침에 진행 중인 백업 작업 중에 게이트웨이가 다시 시작될 때 예상되는 동작이 설명되어 있습니다. 자세한 내용은 백업 소프트웨어를 사용하여 게이트웨이 설정 테스트 를 참조하십시오.	2023년 10월 24일
권장 CloudWatch 경보 업데이트	이제 경보가 CloudWatch HealthNotifications 모든 게이트웨이 유형 및 호스트 플랫폼에 적용되며 에 권장됩니다. HealthNotifications 및 AvailabilityNotifications 에 대한 권장 구성 설정도 업데이트되었습니다. 자세한 내용은 CloudWatch 경보 이해를 참조하세요.	2023년 10월 2일
Tape Gateway의 최대 테이프 크기를 15TiB로 늘림	Tape Gateway의 경우, 이제 가상 테이프의 최대 크기가 5TiB에서 15TiB로 증가했습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 테이프 할당량 을 참조하세요.	2022년 10월 4일

[Tape Gateway와 Volume Gateway 사용 설명서가 분리될](#)

Tape Gateway와 Volume Gateway 유형에 대한 정보를 모두 포함하고 있던 Storage Gateway 사용 설명서가 Tape Gateway 사용 설명서와 Volume Gateway 사용 설명서로 분리되어, 각 설명서에 한 가지 게이트웨이 유형에 대한 정보만 포함되어 있습니다. 자세한 내용은 [Tape Gateway 사용 설명서](#) 및 [Volume Gateway 사용 설명서](#)를 참조하세요.

2022년 3월 23일

[게이트웨이 생성 절차가 업데이트됨](#)

Storage Gateway 콘솔을 사용하여 모든 게이트웨이 유형을 생성하는 절차가 업데이트되었습니다. 자세한 내용은 [게이트웨이 생성](#)을 참조하세요.

2022년 1월 18일

[새 테이프 인터페이스](#)

AWS Storage Gateway 콘솔의 테이프 개요 페이지가 새 검색 및 필터링 기능으로 업데이트되었습니다. 새로운 기능을 설명하도록 이 설명서의 모든 관련 절차가 업데이트되었습니다. 자세한 내용은 [Tape Gateway 관리](#)를 참조하세요.

2021년 9월 23일

[Tape Gateway용 Quest NetVault Backup 13 지원](#)

Tape Gateways는 이제 Microsoft Windows Server 2012 R2 또는 Microsoft Windows Server 2016에서 실행되는 Quest NetVault Backup 13을 지원합니다. 자세한 내용은 [Quest NetVault Backup을 사용하여 설정 테스트를 참조하세요](#).

2021년 8월 22일

[Tape Gateway 및 Volume Gateway 설명서에서 S3 File Gateway 주제가 제거됨](#)

각 게이트웨이 유형을 설정하는 고객이 Tape Gateway 및 Volume Gateway 사용 설명서를 더 쉽게 따라할 수 있도록 일부 불필요한 주제가 제거되었습니다.

2021년 7월 21일

[Windows 및 Linux for Tape Gateway에서 IBM Spectrum Protect 8.1.10 지원](#)

이제 Tape Gateway는 Microsoft Windows Server 및 Linux에서 실행되는 IBM Spectrum Protect 버전 8.1.10을 지원합니다. 자세한 내용은 [IBM Spectrum Protect를 사용하여 설정 테스트를 참조하세요](#).

2020년 11월 24일

[연준RAMP 규정 준수](#)

이제 Storage Gateway가 FedRAMP를 준수합니다. 자세한 내용은 [Storage Gateway에 대한 규정 준수 검증을 참조하세요](#).

2020년 11월 24일

[일정 기반 대역폭 조절](#)

Storage Gateway에서 이제 Tape Gateway 및 Volume Gateway에 대해 일정 기반 대역폭 조절을 지원합니다. 자세한 내용은 [Storage Gateway 콘솔을 사용한 대역폭 조절 예](#)를 참조하세요.

2020년 11월 9일

[캐시 볼륨 및 Tape Gateway 로컬 캐시 스토리지가 4배 증가함](#)

Storage Gateway에서 이제 캐시 볼륨과 Tape Gateway에 최대 64TB의 로컬 캐시를 지원하여 대규모 작업 데이터 세트에 대한 지연 시간이 짧은 액세스를 제공하므로 온프레미스 애플리케이션의 성능이 향상됩니다. 자세한 내용은 [게이트웨이에 권장되는 로컬 디스크 크기를 참조하세요](#).

2020년 11월 9일

[게이트웨이 마이그레이션](#)

Storage Gateway에서 이제 캐시 Volume Gateway를 새 가상 머신으로 마이그레이션하는 기능을 지원합니다. 자세한 내용은 [캐시 볼륨을 새로운 캐시 Volume Gateway 가상 머신으로 이동을 참조하세요](#).

2020년 9월 10일

[테이프 보존 잠금 및 write-once-read-many \(WORM\) 테이프 보호 지원](#)

Storage Gateway는 가상 테이프에서 테이프 보존 잠금을 지원하며 읽기가 많으면 쓸 수 있습니다(WORM). 테이프 보존 잠금 기능을 사용하면 아카이브된 가상 테이프에 보존 모드와 보존 기간을 지정하여 일정 기간(최대 100년) 동안 삭제되지 않도록 할 수 있습니다. 여기에는 테이프를 삭제하거나 보존 설정을 수정할 수 있는 사람에 대한 권한 제어 기능이 포함됩니다. 자세한 내용은 [테이프 보존 잠금 사용](#)을 참조하세요. WORM-활성화된 가상 테이프는 가상 테이프 라이브러리의 활성 테이프에 있는 데이터를 덮어쓰거나 지울 수 없도록 하는 데 도움이 됩니다. 자세한 내용은 [Write Once, Read Many\(WORM\) Tape Protection](#)을 참조하세요.

2020년 8월 19일

[콘솔을 통해 하드웨어 어플라이언스 주문](#)

이제 AWS Storage Gateway 콘솔을 통해 하드웨어 어플라이언스를 주문할 수 있습니다. 자세한 내용은 [Storage Gateway 하드웨어 어플라이언스 사용](#)을 참조하세요.

2020년 8월 12일

[새 AWS 리전의 연방 정보 처리 표준\(FIPS\) 엔드포인트 지원](#)

이제 미국 동부(오하이오), 미국 동부(버지니아 북부), 미국 서부(캘리포니아 북부), 미국 서부(오레곤) 및 캐나다(중부) 리전에 FIPS 엔드포인트가 있는 게이트웨이를 활성화할 수 있습니다. 자세한 내용은 [AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요](#).

2020년 7월 31일

[게이트웨이 마이그레이션](#)

Storage Gateway에서 이제 테이프 및 저장 Volume Gateway를 새 가상 머신으로 마이그레이션하는 기능을 지원합니다. 자세한 내용은 [데이터를 새 게이트웨이로 이동을 참조하세요](#).

2020년 7월 31일

[Storage Gateway 콘솔에서 Amazon CloudWatch 경보 보기](#)

이제 Storage Gateway 콘솔에서 CloudWatch 경보를 볼 수 있습니다. 자세한 내용은 [CloudWatch 경보 이해를 참조](#).

2020년 5월 29일

[연방 정보 처리 표준\(FIPS\) 엔드포인트 지원](#)

이제 리전의 FIPS 엔드포인트를 사용하여 게이트웨이를 AWS GovCloud (US) 활성화할 수 있습니다. Volume Gateway의 FIPS 엔드포인트를 선택하려면 [서비스 엔드포인트 선택을 참조하세요](#). Tape Gateway의 FIPS 엔드포인트를 선택하려면 [Tape Gateway를 연결을 참조하세요 AWS](#).

2020년 5월 22일

[새 AWS 리전](#)

이제 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량을 참조](#) 하세요.

2020년 5월 7일

[S3 Intelligent-Tiering 스토리지 클래스 지원](#)

Storage Gateway에서 이제 S3 Intelligent-Tiering 스토리지 클래스를 지원합니다. S3 Intelligent-Tiering 스토리지 클래스는 성능 영향 또는 운영 오버헤드 없이 가장 비용 효율적인 스토리지 액세스 계층으로 데이터를 자동으로 이동하여 스토리지 비용을 최적화합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [자주 액세스하는 객체와 자주 액세스하지 않는 객체를 자동으로 최적화하는 스토리지 클래스](#)를 참조하세요.

2020년 4월 30일

[Tape Gateway 쓰기 및 읽기 성능 2배 향상](#)

Storage Gateway를 사용하면 Tape Gateway에서 가상 테이프로부터 읽어 들이는 성능과 가상 테이프를 쓰는 성능을 2배 향상시킴으로써 백업 및 복구 작업을 이전보다 신속하게 수행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 [Tape Gateway에 대한 성능 지침](#)을 참조하세요.

2020년 4월 23일

[자동 테이프 생성 지원](#)

Storage Gateway에서 이제 새 가상 테이프를 자동으로 생성하는 기능을 제공합니다. Tape Gateway는 사용자가 구성한 사용 가능한 최소 테이프 수를 유지하기 위해 자동으로 새 가상 테이프를 생성한 다음 백업 애플리케이션에서 이 새 테이프를 가져올 수 있도록 설정하므로 백업 작업을 중단 없이 실행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 [자동으로 테이프 생성](#)을 참조하세요.

2020년 4월 23일

[새 AWS 리전](#)

이제 Storage Gateway를 AWS GovCloud (미국 동부) 리전에서 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

2020년 3월 12일

[Linux 커널 기반 가상 머신 \(KVM\) 하이퍼바이저 지원](#)

이제 Storage Gateway는 KVM 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. 예 배포된 게이트웨이KVM에는 기존 온프레미스 게이트웨이와 동일한 기능과 기능이 모두 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 [지원되는 하이퍼바이저 및 호스트 요구 사항](#)을 참조하세요.

2020년 2월 4일

[VMware vSphere 고가용성 지원](#)

이제 Storage Gateway는 에서 고가용성을 지원VMware 하여 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호합니다. 자세한 내용은 [Storage Gateway 사용 설명서의 Storage Gateway에서 VMware vSphere 고가용성 사용을 참조하세요](#). Storage Gateway 이 릴리스에는 성능 향상도 포함되어 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 [성능](#)을 참조하세요.

2019년 11월 20일

[Tape Gateway의 새 AWS 리전](#)

이제 남아메리카(상파울루) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

2019년 9월 24일

[Linux에서 IBM Spectrum Protect 버전 7.1.9 지원 및 Tape Gateway의 경우 최대 테이프 크기가 5TiB로 증가](#)

이제 Tape Gateways는 Microsoft Windows에서 실행되는 것 외에도 Linux에서 실행되는 IBM Spectrum Protect(Tivoli Storage Manager) 버전 7.1.9를 지원합니다. 자세한 내용은 Storage Gateway 사용 설명서의 [IBM Spectrum Protect를 사용하여 설정 테스트를 참조하세요](#). Storage Gateway 또한 Tape Gateway의 경우 가상 테이프의 최대 크기가 2.5TiB에서 5TiB로 증가했습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 [테이프 할당량](#)을 참조하세요.

2019년 9월 10일

[Amazon CloudWatch Logs 지원](#)

이제 Amazon CloudWatch Log Groups로 File Gateways를 구성하여 오류와 게이트웨이 및 해당 리소스의 상태에 대한 알림을 받을 수 있습니다. 자세한 내용은 Storage [Gateway 사용 설명서의 Amazon CloudWatch Log Groups에서 Gateway 상태 및 오류에 대한 알림 받기](#)를 참조하세요. Storage Gateway

2019년 9월 4일

[새 AWS 리전](#)

이제 아시아 태평양(홍콩) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

2019년 8월 14일

[새 AWS 리전](#)

이제 중동(바레인) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 엔드포인트 및 할당량](#)을 참조하세요.

2019년 7월 29일

[가상 프라이빗 클라우드에서 게이트웨이 활성화 지원\(VPC\)](#)

이제 에서 게이트웨이를 활성화할 수 있습니다 VPC. 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 자세한 내용은 [Virtual Private Cloud\(VPC\)에서 게이트웨이 활성화](#)를 참조하십시오.

2019년 6월 20일

[S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 가상 테이프 이동 지원](#)

이제부터는 S3 Glacier Flexible Retrieval 스토리지 클래스에 저장된 가상 테이프를 비용 효과가 좋고 장기간 데이터를 보존할 수 있는 S3 Glacier Deep Archive 스토리지 클래스로 옮길 수 있습니다. 자세한 내용은 [S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프 이전](#)을 참조하세요.

2019년 5월 28일

[SMB Microsoft Windows에 대한 파일 공유 지원 ACLs](#)

파일 게이트웨이의 경우 이제 Microsoft Windows 액세스 제어 목록(ACLs)을 사용하여 서버 메시지 블록(SMB) 파일 공유에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 [Microsoft Windows ACLs를 사용하여 SMB 파일 공유에 대한 액세스 제어를 참조](#)하세요.

2019년 5월 8일

[S3 Glacier Deep Archive와 통합](#)

Tape Gateway는 S3 Glacier Deep Archive와 통합됩니다. 이제 데이터를 장기간 보존하기 위해 가상 테이프를 S3 Glacier Deep Archive에 아카이브할 수 있습니다. 자세한 내용은 [가상 테이프 아카이브](#)를 참조하십시오.

2019년 3월 27일

[유럽에서 Storage Gateway 하드웨어 어플라이언스 사용 가능](#)

이제 유럽에서 Storage Gateway 하드웨어 어플라이언스를 사용할 수 있습니다. 자세한 내용은 AWS 일반 참조에서 [AWS Storage Gateway 하드웨어 어플라이언스 리전](#)을 참조하십시오. 또한 Storage Gateway 하드웨어 어플라이언스에서 사용할 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있고, 설치된 동선 네트워크 카드를 10기가비트 광섬유 네트워크 카드로 교체할 수 있습니다. 자세한 내용은 [하드웨어 어플라이언스 설정](#)을 참조하십시오.

2019년 2월 25일

[와 통합 AWS Backup](#)

Storage Gateway는 와 통합됩니다 AWS Backup. 이제 AWS Backup 를 사용하여 클라우드 지원 스토리지에 Storage Gateway 볼륨을 사용하는 온프레미스 비즈니스 애플리케이션을 백업할 수 있습니다. 자세한 내용은 [볼륨 백업](#)을 참조하십시오.

2019년 1월 16일

[Bacula Enterprise 및 IBM Spectrum Protect 지원](#)

Tape Gateway는 이제 Bacula Enterprise 및 IBM Spectrum Protect를 지원합니다. Storage Gateway는 이제 최신 버전의 Veritas NetBackup, Veritas Backup Exec 및 Quest NetVault 백업도 지원합니다. 이제 이러한 백업 애플리케이션을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 [백업 소프트웨어를 사용하여 게이트웨이 설정 테스트](#)를 참조하십시오.

2018년 11월 13일

[Storage Gateway 하드웨어 어플라이언스 지원](#)

Storage Gateway 하드웨어 어플라이언스에는 타사 서버에 사전 설치된 Storage Gateway 소프트웨어가 포함되어 있습니다. AWS Management Console에서 어플라이언스를 관리할 수 있습니다. 어플라이언스는 파일, 테이프 및 Volume Gateway를 호스팅할 수 있습니다. 자세한 내용은 [Storage Gateway 하드웨어 어플라이언스 사용](#) 섹션을 참조하세요.

2018년 9월 18일

[Microsoft System Center 2016 Data Protection Manager와의 호환성\(DPM\)](#)

Tape Gateway는 이제 Microsoft System Center 2016 Data Protection Manager()와 호환됩니다DPM. 이제 MicrosoftDPM를 사용하여 데이터를 Amazon S3에 백업하고 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 [Microsoft System Center Data Protection Manager를 사용한 설정 테스트](#)를 참조하십시오.

2018년 7월 18일

[서버 메시지 블록\(SMB\) 프로토콜 지원](#)

File Gateways는 파일 공유에 서버 메시지 블록(SMB) 프로토콜에 대한 지원을 추가했습니다. 자세한 내용은 [파일 공유 생성](#)을 참조하십시오.

2018년 6월 20일

[파일 공유, 캐시 볼륨 및 가상 테이프 암호화 지원](#)

이제 AWS Key Management Service (AWS KMS)를 사용하여 파일 공유, 캐시된 볼륨 또는 가상 테이프에 기록된 데이터를 암호화할 수 있습니다. 현재 이를 사용하여 이 작업을 수행할 수 있습니다 AWS Storage Gateway API. 자세한 내용은 [AWS KMS를 사용하여 데이터 암호화](#)를 참조하세요.

2018년 6월 12일

[NovaStor DataCenter/Network](#) 지원

이제 Tape Gateways는 버전 6.4 또는 7.1을 지원 NovaStor DataCenter/Network. You can now use NovaStor DataCenter/Network하여 데이터를 Amazon S3에 백업하고 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브합니다. 자세한 내용은 [NovaStor DataCenter/Network](#)를 사용하여 설정 테스트를 참조하세요.

2018년 5월 24일

이전 업데이트

다음 표에서는 2018년 5월 이전 AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경 사항	설명	변경 날짜
S3 One Zone_IA 스토리지 클래스 지원	File Gateway의 경우 S3 One Zone_IA를 파일 공유에 대한 기본 스토리지 클래스로 선택할 수 있습니다. 이 스토리지 클래스를 사용하여 Amazon S3의 단일 가용 영역에 객체 데이터를 저장할 수 있습니다. 자세한 내용은 파일 공유 생성 을 참조하세요.	2018년 4월 4일
새로운 리전	이제 아시아 태평양(싱가포르) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.	2018년 3월 4일
Amazon S3 버킷에 ACLs 대한 캐시 새로 고침 알림, 요청자 지불 및 사전 준비 지원.	이제 게이트웨이가 Amazon S3 버킷에서 캐시 새로 고침을 완료하면 File Gateway를 통해 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway API 참조의 RefreshCache.html 을 참조하세요.	2018년 3월 1일

변경 사항	설명	변경 날짜
	<p>이제 File Gateway를 통해 버킷 소유자가 아닌 요청자나 리더가 액세스 요금을 지불할 수 있습니다.</p> <p>이제 파일 게이트웨이를 사용하면 NFS 파일 공유에 매핑되는 S3 버킷의 소유자에게 전체 제어 권한을 부여할 수 있습니다.</p> <p>자세한 내용은 파일 공유 생성을 참조하세요.</p>	
Dell EMC NetWorker V9.x 지원	<p>이제 Tape Gateway가 Dell EMC NetWorker V9.x를 지원합니다. 이제 Dell EMC NetWorker V9.x를 사용하여 데이터를 Amazon S3에 백업하고 오프라인 스토리지 (S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Dell을 사용하여 설정 테스트를 참조하세요EMC NetWorker.</p>	2018년 2월 27일
새로운 리전	<p>이제 유럽(파리) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.</p>	2017년 12월 18일
파일 업로드 알림 및 MIME 유형 추측 지원	<p>이제 파일 공유에 기록된 모든 파일이 Amazon S3에 업로드되면 NFS File Gateways에서 알림을 보낼 수 있습니다. 자세한 내용은 Storage Gateway 참조NotifyWhenUploaded의 섹션을 참조하세요. Storage Gateway API</p> <p>이제 파일 게이트웨이를 사용하면 파일 확장을 기반으로 업로드된 객체의 MIME 유형을 추측할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.</p>	2017년 11월 21일
VMware ESXi Hypervisor 버전 6.5 지원	<p>AWS Storage Gateway 는 이제 VMware ESXi Hypervisor 버전 6.5를 지원합니다. 이는 버전 4.1, 5.0, 5.1, 5.5 및 6.0에 추가된 지원 기능입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.</p>	2017년 9월 13일

변경 사항	설명	변경 날짜
Commvault 11과의 호환성	Tape Gateway가 이제 Commvault 11과 호환됩니다. 이제 Commvault를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Commvault를 사용한 설정 테스트 를 참조하세요.	2017년 9월 12일
Microsoft Hyper-V 하이퍼바이저의 File Gateway 지원	이제 Microsoft Hyper-V 하이퍼바이저에 File Gateway를 배포할 수 있습니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 을 참조하세요.	2017년 6월 22일
아카이브로부터 3~5시간 테이프 검색 지원	Tape Gateway의 경우 이제 아카이브에서 3-5시간 후에 테이프를 검색할 수 있습니다. 백업 애플리케이션 또는 가상 테이프 라이브러리()에서 테이프에 기록된 데이터의 양을 확인할 수도 있습니다 VTL. 자세한 내용은 테이프 사용량 보기 를 참조하세요.	2017년 5월 23일
새로운 리전	이제 아시아 태평양(뭄바이) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.	2017년 5월 02일
파일 공유 설정 업데이트 파일 공유에 대한 캐시 새로 고침 지원	이제 File Gateway를 통해 파일 공유 설정에 마운팅 옵션을 추가할 수 있습니다. 이제 파일 공유에 대해 스쿼시 및 읽기 전용 옵션을 설정할 수 있습니다. 자세한 내용은 파일 공유 생성 을 참조하세요. 이제 File Gateway를 통해 게이트웨이가 마지막으로 버킷의 콘텐츠를 나열하고 결과를 캐싱한 이후에 추가 또는 제거된 Amazon S3 버킷에서 객체를 찾을 수 있습니다. 자세한 내용은 API 참조 RefreshCache 의 섹션을 참조하세요.	2017년 3월 28일
볼륨 복제 지원	캐시된 Volume Gateway의 경우는 AWS Storage Gateway 이제 기존 볼륨에서 볼륨을 복제할 수 있는 기능을 지원합니다. 자세한 내용은 볼륨 복제 를 참조하세요.	2017년 3월 16일

변경 사항	설명	변경 날짜
Amazon의 File Gateway 지원 EC2	AWS Storage Gateway 이제 는 Amazon 에 파일 게이 트웨이를 배포할 수 있는 기능을 제공합니다EC2. 이제 커뮤니티 로 사용할 수 있는 Storage Gateway Amazon Machine Image(AMI)를 EC2 사용하여 Amazon에 서 File Gateway를 시작할 수 있습니다AMI. Storage Gateway File Gateway를 생성하고 EC2 인스턴스 에 배포하는 방법에 대한 자세한 내용은 Amazon S3 File Gateway 생성 및 활성화 또는 Amazon FSx File Gateway 생성 및 활성화 를 참조하세요. 파일 게이트 웨이를 시작하는 방법에 대한 자세한 내용은 Amazon EC2 호스트에 S3 파일 게이트웨이 배포 또는 Amazon 호스트에 파일 게이트웨이 배포를 AMI참조하세요. FSx EC2	2017년 2월 08일
Arcserve 17과의 호환성	Tape Gateway가 이제 Arcserve 17과 호환됩니다. 이제 Arcserve를 사용하여 데이터를 Amazon S3에 백업하고 S3 Glacier Flexible Retrieval에 직접 아카이브할 수 있습니다. 자세한 내용은 Arcserve Backup r17.0을 사용한 설정 테스트 를 참조하세요.	2017년 1월 17일
새로운 리전	이제 EU(런던) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.	2016년 12월 13일
새로운 리전	이제 캐나다(중부) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.	2016년 08월 12일

변경 사항	설명	변경 날짜
File Gateway 지원	Storage Gateway에서 이제 Volume Gateway 및 Tape Gateway 외에도 File Gateway를 제공합니다. File Gateway는 서비스와 가상 소프트웨어 어플라이언스를 결합하여 Network File System()과 같은 업계 표준 파일 프로토콜을 사용하여 Amazon S3에 객체를 저장하고 검색할 수 있습니다. NFS. 게이트웨이는 Amazon S3의 객체에 대한 액세스를 NFS 탑재 지점의 파일로 제공합니다.	2016년 11월 29일
Backup Exec 16	Tape Gateway가 이제 Backup Exec 16과 호환됩니다. 이제 Backup Exec 16을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트 를 참조하세요.	2016년 11월 7일
Micro Focus(HPE) Data Protector 9.x와의 호환성	Tape Gateway는 이제 Micro Focus(HPE) Data Protector 9.x와 호환됩니다. 이제 HPE Data Protector를 사용하여 데이터를 Amazon S3에 백업하고 S3 Glacier Flexible Retrieval에 직접 아카이브할 수 있습니다. 자세한 내용은 Micro Focus(HPE) 데이터 보호기를 사용하여 설정 테스트 를 참조하세요.	2016년 11월 2일
새로운 리전	이제 미국 동부(오하이오) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.	2016년 10월 17일
Storage Gateway 콘솔 재설계	Storage Gateway Management Console을 재설계하여 게이트웨이, 볼륨 및 가상 테이프를 구성, 관리 및 모니터링하는 작업이 더 수월해졌습니다. 이제 사용자 인터페이스는 필터링할 수 있는 뷰를 제공하고 CloudWatch 및 Amazon 과 같은 통합 AWS 서비스에 대한 직접 링크를 제공합니다. 자세한 내용은 가입 AWS Storage Gateway 단원을 참조하십시오.	2016년 8월 30일

변경 사항	설명	변경 날짜
Veeam Backup & Replication V9 업데이트 2 이상과의 호환성	Tape Gateway가 이제 Veeam Backup & Replication V9 업데이트 2 이상(즉 버전 9.0.0.1715 이상)과 호환됩니다. 이제 Veeam Backup Replication V9 업데이트 2 이상을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veeam Backup & Replication를 사용한 설정 테스트 참조하세요.	2016년 8월 15일
더 긴 볼륨 및 스냅샷 IDs	Storage Gateway는 볼륨 및 스냅샷IDs에 더 긴 기간을 도입하고 있습니다. 볼륨, 스냅샷 및 기타 지원되는 AWS 리소스에 대해 더 긴 ID 형식을 활성화할 수 있습니다. 자세한 내용은 Storage Gateway 리소스 및 리소스에 대한 이해 IDs 단원을 참조하십시오.	2016년 4월 25일
<p>새로운 리전</p> <p>저장 볼륨에 대한 최대 512TiB 크기의 스토리지 지원</p> <p>Storage Gateway 로컬 콘솔에 대한 기타 게이트웨이 업데이트 및 개선 사항</p>	<p>이제 아시아 태평양(서울) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 단원을 참조하십시오.</p> <p>저장 볼륨의 경우, 최대 크기가 16TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 512TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요.</p> <p>가상 테이프 라이브러리에 있는 모든 테이프의 총 크기가 1PiB로 증가하였습니다. 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오.</p> <p>이제 Storage Gateway 콘솔에서 VM 로컬 콘솔의 암호를 설정할 수 있습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정을 참조하세요.</p>	2016년 3월 21일

변경 사항	설명	변경 날짜
와 Dell EMC NetWorker 8.x의 호환성	Tape Gateway는 이제 Dell EMC NetWorker 8.x와 호환됩니다. 이제 Dell EMC NetWorker 을 사용하여 데이터를 Amazon S3에 백업하고 오프라인 스토리지 (S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Dell을 사용하여 설정 테스트를 참조하세요EMC NetWorker.	2016년 2월 29일
VMware ESXi Hypervisor 버전 6.0 및 Red Hat Enterprise Linux 7 iSCSI 이니시에이터 지원	AWS Storage Gateway 이제 는 VMware ESXi Hypervisor 버전 6.0 및 Red Hat Enterprise Linux 7 iSCSI 이니시에이터를 지원합니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 및 지원되는 iSCSI 이니시에이터 단원을 참조하세요.	2015년 10월 20일
콘텐츠 재구성	이 릴리스가 포함하는 개선점은 다음과 같습니다. 즉 모든 게이트웨이 솔루션에 공통된 관리 작업을 모아놓은 "Managing Your Activated Gateway" 단원이 설명서에 포함되었습니다. 아래에서는 게이트웨이를 배포하고 활성화한 후 관리하는 방법에 대한 지침을 얻을 수 있습니다. 자세한 내용은 Tape Gateway 관리 단원을 참조하십시오.	

변경 사항	설명	변경 날짜
<p>캐싱 볼륨에 대한 최대 1,024TiB 크기의 스토리지 지원</p> <p>VMware ESXi 하이퍼바이저에서 VMXNET3 (10GbE) 네트워크 어댑터 유형 지원</p> <p>성능 개선 사항</p> <p>Storage Gateway 로컬 콘솔에 대한 기타 개선 사항 및 업데이트</p>	<p>캐싱 볼륨의 경우, 최대 크기가 32TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 1,024TiB까지 구성할 수 있습니다. 자세한 내용은 캐싱 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요.</p> <p>게이트웨이가 VMware ESXi 하이퍼바이저에서 호스팅 되는 경우 VMXNET3 어댑터 유형을 사용하도록 게이트웨이를 재구성할 수 있습니다. 자세한 내용은 게이트웨이용 네트워크 어댑터 구성 단원을 참조하십시오.</p> <p>Storage Gateway의 최대 업로드 속도를 초당 120MB로 개선하였고, 최대 다운로드 속도는 초당 20MB로 개선하였습니다.</p> <p>유지 관리 작업을 수행하는 데 도움이 되는 추가 기능으로 Storage Gateway 로컬 콘솔을 업데이트 및 강화하였습니다. 자세한 내용은 게이트웨이 네트워크 구성 단원을 참조하십시오.</p>	<p>2015년 9월 16일</p>
<p>태그 지정 지원</p>	<p>Storage Gateway에서 이제 리소스 태그 지정을 지원합니다. 이제 게이트웨이, 볼륨, 가상 테이프에 태그를 추가하여 더 쉽게 관리할 수 있습니다. 자세한 내용은 Storage Gateway 리소스에 태그를 지정 단원을 참조하십시오.</p>	<p>2015년 9월 2일</p>
<p>Quest(이전 Dell) NetVault Backup 10.0과의 호환성</p>	<p>이제 Tape Gateway가 Quest NetVault Backup 10.0과 호환됩니다. 이제 Quest NetVault Backup 10.0을 사용하여 데이터를 Amazon S3에 백업하고 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Quest NetVault Backup을 사용하여 설정 테스트를 참조하세요.</p>	<p>2015년 6월 22일</p>

변경 사항	설명	변경 날짜
<p>저장 볼륨 게이트웨이 설정에 대한 16TiB 스토리지 볼륨 지원</p> <p>Storage Gateway 로컬 콘솔에서 시스템 리소스 점검 기능 지원</p> <p>Red Hat Enterprise Linux 6 iSCSI 이니시에이터 지원</p>	<p>Storage Gateway에서 이제 저장 Volume Gateway 설정에 대해 16TiB 스토리지 볼륨을 지원합니다. 이제 16TiB 스토리지 볼륨을 최대 12개까지 생성하여 전체 스토리지를 최대 192TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처를 참조하세요.</p> <p>이제 시스템 리소스(가상 CPU 코어, 루트 볼륨 크기 및 RAM)가 게이트웨이가 제대로 작동하기에 충분한지 확인할 수 있습니다. 자세한 내용은 게이트웨이 시스템 리소스 상태 조회 또는 게이트웨이 시스템 리소스 상태 조회를 참조하세요.</p> <p>이제 Storage Gateway가 Red Hat Enterprise Linux 6 iSCSI 이니시에이터를 지원합니다. 자세한 내용은 Tape Gateway 설정 요구 사항 단원을 참조하십시오.</p> <p>이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다.</p> <ul style="list-style-type: none"> 이제 Storage Gateway 콘솔에서 게이트웨이에 소프트웨어 업데이트를 성공적으로 적용한 최종 날짜와 시간을 볼 수 있습니다. 자세한 내용은 게이트웨이 업데이트 관리 단원을 참조하십시오. 이제 Storage Gateway는 스토리지 볼륨에 연결된 iSCSI 이니시에이터를 나열하는 데 사용할 API 수 있는 를 제공합니다. 자세한 내용은 API 참조 ListVolumeInitiators의 섹션을 참조하세요. 	<p>2015년 6월 3일</p>

변경 사항	설명	변경 날짜
Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2 지원	Storage Gateway에서 이제 Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2를 지원합니다. 이것은 Microsoft Hyper-V 하이퍼바이저 버전 2008 R2 지원에 추가된 것입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 4월 30일
Symantec Backup Exec 15와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 15와 호환됩니다. 이제 Symantec Backup Exec 15를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트 를 참조하세요.	2015년 4월 6일
CHAP 스토리지 볼륨에 대한 인증 지원	이제 Storage Gateway는 스토리지 볼륨에 대한 CHAP 인증 구성을 지원합니다. 자세한 내용은 볼륨에 대한 CHAP 인증 구성을 참조하세요 .	2015년 4월 2일
VMware ESXi Hypervisor 버전 5.1 및 5.5 지원	Storage Gateway는 이제 VMware ESXi Hypervisor 버전 5.1 및 5.5를 지원합니다. 이는 VMware ESXi Hypervisor 버전 4.1 및 5.0에 대한 지원에 추가됩니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 3월 30일
Windows CHKDSK 유틸리티 지원	이제 Storage Gateway가 Windows CHKDSK 유틸리티를 지원합니다. 이 유틸리티를 사용하여 볼륨의 무결성을 확인하고 볼륨의 오류를 수정할 수 있습니다. 자세한 내용은 볼륨 문제 해결 을 참조하세요.	2015년 3월 04일

변경 사항	설명	변경 날짜
<p>와 통합하여 API 통화 AWS CloudTrail 캡처</p>	<p>이제 Storage Gateway는 Amazon Web Services 계정에서 Storage Gateway에 의해 또는 Storage Gateway를 대신하여 수행된 API 호출을 AWS CloudTrail AWS CloudTrail 캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 자세한 내용은 로그인 및 모니터링 AWS Storage Gateway 단원을 참조하십시오.</p> <p>이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다.</p> <ul style="list-style-type: none"> 이제 캐시 스토리지에 오손 데이터(dirty data)가 있는 가상 테이프, 즉 AWS에 업로드하지 않은 콘텐츠를 포함하는 가상 테이프는 게이트웨이의 캐싱된 드라이브가 변경될 때 복구됩니다. 자세한 내용은 복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우를 참조하십시오. 	<p>2014년 12월 16일</p>

변경 사항	설명	변경 날짜
<p>추가 백업 소프트웨어 및 미디어 체인저와의 호환성</p>	<p>Tape Gateway가 이제 다음 백업 소프트웨어와 호환됩니다.</p> <ul style="list-style-type: none"> • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 <p>이제 Storage Gateway 가상 테이프 라이브러리(VTL)와 함께 이러한 4개의 백업 소프트웨어 제품을 사용하여 Amazon S3에 백업하고 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 백업 소프트웨어를 사용하여 게이트웨이 설정 테스트를 참조하십시오.</p> <p>Storage Gateway에서 이제 새 백업 소프트웨어와 함께 작동하는 추가 미디어 체인저를 제공합니다.</p> <p>이 릴리스에는 기타 AWS Storage Gateway 개선 사항 및 업데이트가 포함되어 있습니다.</p>	<p>2014년 11월 3일</p>
<p>Europe (Frankfurt) Region</p>	<p>이제 유럽(프랑크푸르트) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 섹션을 참조하세요.</p>	<p>2014년 10월 23일</p>

변경 사항	설명	변경 날짜
콘텐츠 재구성	모든 게이트웨이 솔루션에 공통된 시작하기 단원을 만들었습니다. 아래에서는 게이트웨이를 다운로드, 배포 및 활성화하는 방법에 대한 지침을 얻을 수 있습니다. 게이트웨이를 배포하고 활성화한 후 저장 볼륨, 캐시 볼륨 및 Tape Gateway 설정에 따른 추가 지침에 따라 작업을 수행할 수 있습니다. 자세한 내용은 Tape Gateway 생성 을 참조하세요.	2014년 5월 19일
Symantec Backup Exec 2012와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 2012와 호환됩니다. 이제 Symantec Backup Exec 2012를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트 를 참조하세요.	2014년 4월 28일

변경 사항	설명	변경 날짜
<p>Windows Server Failover Clustering 지원</p> <p>VMware ESX 이니시에이터 지원</p> <p>Storage Gateway 로컬 콘솔에서 구성 작업을 수행하도록 지원</p>	<ul style="list-style-type: none"> 이제 Storage Gateway는 호스트가 Windows Server 장애 조치 클러스터링()을 사용하여 액세스를 조정하는 경우 여러 호스트를 동일한 볼륨에 연결할 수 있도록 지원합니다WSFC. 그러나 를 사용하지 않으면 여러 호스트를 동일한 볼륨에 연결할 수 없습니다WSFC. 이제 Storage Gateway를 사용하면 ESX 호스트를 통해 스토리지 연결을 직접 관리할 수 있습니다. 이렇게 하면 의 게스트 OS에 있는 이니시에이터를 사용하는 대신 사용할 수 있습니다VMs. Storage Gateway에서 이제 Storage Gateway 로컬 콘솔에서 구성 작업을 수행할 수 있도록 지원합니다. 온프레미스에 배포한 게이트웨이에서 구성 작업을 수행하는 방법에 대한 정보는 VM 로컬 콘솔에서 작업 수행 또는 VM 로컬 콘솔에서 작업 수행 단원을 참조하십시오. EC2 인스턴스에 배포된 게이트웨이에서 구성 작업을 수행하는 방법에 대한 자세한 내용은 Amazon EC2 Local Console에서 작업 수행 또는 섹션을 참조하세요Amazon EC2 Local Console에서 작업 수행. 	<p>2014년 1월 31일</p>

변경 사항	설명	변경 날짜
<p>가상 테이프 라이브러리(VTL) 및 API 버전 2013-06-30 도입 지원</p>	<p>Storage Gateway는 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지와 연결하여 온프레미스 IT 환경을 AWS 스토리지 인프라와 통합합니다. 이제 Storage Gateway는 Volume Gateway(캐치된 볼륨 및 저장된 볼륨) 외에도 게이트웨이 가상 테이프 라이브러리()를 지원합니다. VTL. Tape Gateway에 게이트웨이당 가상 테이프 드라이브를 최대 10개까지 구성할 수 있습니다. 각 가상 테이프 드라이브는 SCSI 명령 세트에 응답하므로 기존 온프레미스 백업 애플리케이션은 수정 없이 작동합니다. 자세한 내용은 AWS Storage Gateway 사용 설명서에서 다음 주제를 참조하세요.</p> <ul style="list-style-type: none"> • 아키텍처 개요는 Tape Gateway 작동 방식(아키텍처)을 참조하세요. • Tape Gateway를 시작하려면 Tape Gateway 생성을 참조하세요. 	2013년 11월 5일
<p>Microsoft Hyper-V 지원</p>	<p>Storage Gateway에서 이제 Microsoft Hyper-V 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. Microsoft Hyper-V에 배포한 게이트웨이에는 기존 온프레미스 Storage Gateway와 동일한 기능이 있습니다. Microsoft Hyper-V를 이용해 게이트웨이 배포를 시작하려면 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하십시오.</p>	2013년 10월 4일
<p>Amazon에 게이트웨이 배포 지원 EC2</p>	<p>이제 Storage Gateway는 Amazon Elastic Compute Cloud(Amazon)에 게이트웨이를 배포할 수 있는 기능을 제공합니다. EC2. 에서 AMI 사용할 수 있는 Storage Gateway를 EC2 사용하여 Amazon에서 게이트웨이 인스턴스를 시작할 수 있습니다. AWS Marketplace. Storage Gateway를 사용하여 게이트웨이 배포를 시작하려면 섹션을 AMI참조하세요 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포.</p>	2013년 1월 15일

변경 사항	설명	변경 날짜
<p>캐시된 볼륨 및 API 버전 2012-06-30 도입 지원</p>	<p>이번 릴리스에서는 Storage Gateway에 캐시 볼륨에 대한 지원을 도입했습니다. 캐싱 볼륨은 온프레미스 스토리지 인프라를 확장할 필요성을 최소화하는 한편, 애플리케이션이 활성 데이터에 액세스할 때의 지연 시간을 짧게 유지하도록 해줍니다. 최대 32TiB 크기의 스토리지 볼륨을 생성하고 온프레미스 애플리케이션 서버에서 iSCSI 디바이스로 탑재할 수 있습니다. 캐시 볼륨에 작성한 데이터는 Amazon Simple Storage Service(S3)에 저장되고, 최근에 쓰고 읽은 데이터의 캐시만 온프레미스 스토리지 하드웨어에 로컬로 저장됩니다. 캐시 볼륨을 사용하면 짧은 액세스 지연 시간이 필요한 데이터에 대한 온프레미스 스토리지를 유지하는 한편, 더 오래되고 덜 자주 액세스하는 데이터와 같이 더 긴 가져오기 지연 시간을 수용할 수 있는 데이터에 대해서는 Amazon S3를 활용할 수 있습니다.</p> <p>이 릴리스에서는 Storage Gateway가 현재 작업을 지원하는 것 외에도 캐시된 볼륨을 지원하는 새 작업을 제공하는 새 API 버전을 소개합니다.</p> <p>두 가지 Storage Gateway 솔루션에 대한 자세한 내용은 Tape Gateway 작동 방식 섹션을 참조하세요.</p> <p>테스트 설정을 시도해 볼 수도 있습니다. 지침은 Tape Gateway 생성을 참조하세요.</p>	<p>2012년 10월 29일</p>

변경 사항	설명	변경 날짜
API 및 IAM 지원	<p>이번 릴리스에서 Storage Gateway는 AWS Identity and Access Management()에 대한 API 지원과 지원을 도입합니다IAM.</p> <ul style="list-style-type: none"> API 지원 - 이제 Storage Gateway 리소스를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 에 대한 자세한 내용은 사용 설명서APIStorage Gateway에 대한 참조의 섹션을 API참조하세요. AWS Storage Gateway IAM 지원 - AWS Identity and Access Management (IAM) 정책을 통해 사용자를 생성하고 Storage Gateway 리소스에 대한 사용자 액세스를 관리할 수 있습니다IAM. IAM 정책에 대한 예시는 AWS Storage Gateway의 ID 및 액세스 관리 단원을 참조하십시오. 에 대한 자세한 내용은 AWS Identity and Access Management (IAM) 세부 정보 페이지를 IAM참조하세요. 	2012년 5월 9일
고정 IP 지원	이제 로컬 게이트웨이에 고정 IP를 지정할 수 있습니다. 자세한 내용은 게이트웨이 네트워크 구성 단원을 참조하십시오.	2012년 3월 5일
새 안내서	이 설명서는 AWS Storage Gateway 사용 설명서의 첫 번째 릴리스입니다.	2012년 1월 24일

Tape Gateway 어플라이언스 소프트웨어 릴리스 정보

이 릴리스 정보에서는 Tape Gateway 어플라이언스의 각 버전에 포함된 새로운 기능, 개선 사항 및 수정 사항을 설명합니다. 각 소프트웨어 버전은 릴리스 날짜와 고유한 버전 번호로 식별됩니다.

Storage Gateway 콘솔에서 세부 정보 페이지를 확인하거나 다음과 유사한 AWS CLI 명령을 사용하여 [DescribeGatewayInformation](#) API 작업을 호출하여 Storage Gateway의 소프트웨어 버전 번호를 확인할 수 있습니다.

```
aws storagegateway describe-gateway-information --gateway-arn
"arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

버전 번호는 API 응답 SoftwareVersion 필드에 반환됩니다.

Note

게이트웨이는 다음과 같은 상황에서는 소프트웨어 버전 정보를 보고하지 않습니다.

- 게이트웨이가 오프라인 상태입니다.
- 게이트웨이가 버전 보고를 지원하지 않는 이전 소프트웨어를 실행하고 있습니다.
- 게이트웨이 유형은 FSx File Gateway입니다.

게이트웨이의 기본 자동 유지 관리 및 업데이트 일정을 수정하는 방법을 포함하여 Tape Gateway 업데이트에 대한 자세한 내용은 [AWS Storage Gateway 콘솔을 사용하여 게이트웨이 업데이트 관리 Storage Gateway](#) .

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-10-03	2.12.0	<ul style="list-style-type: none"> • 새 게이트웨이 및 기존 게이트웨이의 운영 체제 업데이트
2024-08-30	2.11.0	<ul style="list-style-type: none"> • 새 게이트웨이 및 기존 게이트웨이의 운영 체제 업데이트

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-07-29	2.10.0	<ul style="list-style-type: none"> • 새 게이트웨이 및 기존 게이트웨이의 운영 체제 업데이트 • 기타 버그 수정 및 개선 사항
2024-06-17	2.9.2	<ul style="list-style-type: none"> • 새 게이트웨이 및 기존 게이트웨이의 운영 체제 업데이트
2024-05-28	2.9.0	<ul style="list-style-type: none"> • 소프트웨어 업데이트 중 게이트웨이 재시작 시간 단축 • 네트워크 대역폭을 추정하기 위해 전송되는 데이터 양 감소
2024-05-08	2.8.3	<ul style="list-style-type: none"> • SOCKS5 프록시 사용 시 클라우드 연결 문제 해결 • 특정 조건(예: 많은 수의 테이프 삭제 작업)에서 업로드 성능 저하 문제를 해결했습니다.
2024-04-10	2.8.1	<ul style="list-style-type: none"> • 2.8.0에 도입된 메모리 사용량 문제를 해결했습니다. • 보안 패치 업데이트 • 소프트웨어 업데이트 프로세스 개선 • 새 게이트웨이에 대한 누락된 Network Time Protocol(NTP) 구성 요소를 해결했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-03-06	2.8.0	<ul style="list-style-type: none">• 새 게이트웨이의 운영 체제 업데이트• 보안 패치 업데이트• 동시 백업 및 복원 워크로드의 성능 개선
2023-12-19	2.7.0	<ul style="list-style-type: none">• 새 게이트웨이의 운영 체제 업데이트
2023-12-14	2.6.6	<ul style="list-style-type: none">• 5TiB 테이프보다 큰 테이프에서 상대적 위치 지정 문제를 해결했습니다.
2023-10-19	2.6.5	<ul style="list-style-type: none">• 게이트웨이 재시작 후 클라이언트의 테이프 덮어쓰기에 대한 보호 추가

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