Tape Gateway 사용 설명서

AWS Storage Gateway

API 버전 2013-06-30

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

AWS Storage Gateway: Tape Gateway 사용 설명서

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon의 상표 및 트레이드 드레스는 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
에 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
VM의 하드웨어 요구 사항 9
Amazon EC2 인스턴스 유형에 대한 요구 사항 10
스토리지 요구 사항 10
네트워크 및 방화벽 요구 사항 11
포트 요구 사항 12
하드웨어 어플라이언스에 대한 네트워킹 및 방화벽 요구 사항 22
게이트웨이가 방화벽 및 라우터를 통해 액세스할 수 있도록 허용 24
보안 그룹 구성 26
지원되는 하이퍼바이저 및 호스트 요구 사항 27
지원되는 iSCSI 이니시에이터 29
지원되는 타사 백업 애플리케이션 29
하드웨어 어플라이언스 사용 32
하드웨어 어플라이언스 설정 33
하드웨어 어플라이언스를 물리적으로 설치하기 34
하드웨어 어플라이언스 콘솔 액세스 36
하드웨어 어플라이언스 네트워크 파라미터 구성 37
하드웨어 어플라이언스 활성화 39
하드웨어 어플라이언스에서 게이트웨이 생성 40
하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성 41
하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거 43
하드웨어 어플라이언스 삭제 44
게이트웨이 생성 46
개요 - 게이트웨이 활성화 46
게이트웨이 설정 46

에 연결 AWS 46
검토 및 활성화 47
개요 - 게이트웨이 구성 47
개요 - 스토리지 리소스 47
Tape Gateway 생성 및 활성화 47
Tape Gateway 설정 48
Tape Gateway를에 연결 AWS 49
설정 검토 및 Tape Gateway 활성화 50
Tape Gateway 구성 51
테이프 생성 53
WORM 테이프 보호 53
수동으로 테이프 생성 54
자동 테이프 생성 허용 56
사용자 지정 테이프 풀 생성 58
유형 선택 59
테이프 보존 잠금 59
사용자 지정 테이프 풀 생성 60
VTL 디바이스 연결 61
Microsoft Windows 클라이언트에 연결 61
Linux 클라이언트에 연결 62
게이트웨이 테스트 66
Arcserve 백업 67
Bacula Enterprise 70
Commvault 74
Dell EMC NetWorker 79
IBM 데이터 보호 84
OpenText 데이터 보호기 87
Microsoft System Center DPM 94
NovaStor DataCenter/Network 98
Quest NetVault Backup 104
Veeam Backup & Replication 107
Veritas Backup Exec 110
Veritas NetBackup 114
추가 정보 121
Virtual Private Cloud(VPC)에서 게이트웨이 활성화 121
Storage Gateway용 VPC 엔드포인트 생성 122

Tape Gateway 관리 124
게이트웨이 정보 편집 125
자동 테이프 생성 관리 125
테이프 보관 128
S3 Glacier Deep Archive로 테이프 이동 128
보관한 테이프 가져오기 129
테이프 사용량 통계 보기 131
테이프 삭제 131
사용자 지정 테이프 풀 삭제 132
Tape Gateway 비활성화 133
테이프 상태 이해 134
VTL에서 테이프 상태 정보 파악 134
아카이브의 테이프 상태 확인 135
데이터를 새 게이트웨이 인스턴스로 이동 136
가상 테이프를 새 Tape Gateway로 이동 137
Storage Gateway 모니터링 141
게이트웨이 지표 이해 141
Storage Gateway 지표의 차원 145
업로드 버퍼 모니터링 145
캐시 스토리지 모니터링 147
CloudWatch 경보 이해 149
권장 CloudWatch 경보 생성 150
사용자 지정 CloudWatch 경보 생성 151
Tape Gateway 모니터링 153
Tape Gateway 상태 로그 가져오기 153
Amazon CloudWatch 지표 사용 155
가상 테이프 지표 이해 156
Tape Gateway와 간의 성능 측정 AWS 158
게이트웨이 유지 관리 161
로컬 디스크 관리 161
로컬 디스크 스토리지 용량 결정 161
업로드 버퍼 또는 캐시 스토리지 추가 165
대역폭 관리 166
Storage Gateway 콘솔을 사용하여 대역폭 조절 변경 166
대역폭 조절 예약 167
사용 AWS SDK for Java 168

사용 AWS SDK for .NET ... 170
사용 AWS Tools for Windows PowerShell ... 172
게이트웨이 업데이트 관리 ... 173
업데이트 빈도 및 예상 동작 ... 174
유지 관리 업데이트 켜기 또는 끄기 ... 175
게이트웨이 유지 관리 기간 일정 수정 ... 176
수동으로 업데이트 적용 ... 177
게이트웨이 VM 종료 ... 178
Tape Gateway 시작 및 중지 ... 178
게이트웨이 삭제 및 리소스 제거 ... 179
Storage Gateway 콘솔을 사용하여 게이트웨이 삭제 ... 180
온프레미스에 배포한 게이트웨이에서 리소스 제거 ... 181
Amazon EC2 인스턴스에 배포된 게이트웨이에서 리소스 제거 ... 182
로컬 콘솔을 사용하여 유지 관리 작업 수행 ... 184
게이트웨이 로컬 콘솔 액세스 ... 184
Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 ... 185
VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 ... 185
Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 ... 186
VM 로컬 콘솔에서 작업 수행 ... 187
Tape Gateway 로컬 콘솔에 로그인 ... 188
온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성 ... 189
게이트웨이 네트워크 구성 ... 190
게이트웨이가 인터넷에 연결되어 있는지 테스트 ... 196
온프레미스 게이트웨이에 대해 로컬 콘솔에서 Storage Gateway 명령 실행 ... 197
게이트웨이 시스템 리소스 상태 조회 ... 199
EC2 로컬 콘솔에서 작업 수행 ... 200
EC2 게이트웨이 로컬 콘솔에 로그인 ... 201
HTTP 프록시 구성 ... 202
게이트웨이 네트워크 연결 테스트 ... 202
게이트웨이 시스템 리소스 상태 조회 ... 203
로컬 콘솔에서 Storage Gateway 명령 실행 ... 204
Tape Gateway의 성능 및 최적화 ... 207
Tape Gateway의 성능 지침 ... 207
게이트웨이 성능 최적화 ... 210
권장 구성 ... 210
게이트웨이에 리소스 추가 ... 210

iSCSI 설정 최적화 213
테이프 드라이브에 더 큰 블록 크기 사용 214
가상 테이프 드라이브의 성능 최적화 214
애플리케이션 환경에 리소스 추가 214
보안 216
데이터 보호 216
데이터 암호화 217
자격 증명 및 액세스 관리 219
대상 219
ID를 통한 인증 220
정책을 사용하여 액세스 관리 221
IAM에서 AWS Storage Gateway 작동 방식 222
ID 기반 정책 예시 227
문제 해결 230
규정 준수 확인 232
복원성 232
인프라 보안 233
AWS 보안 모범 사례 234
로깅 및 모니터링 234
CloudTrail의 Storage Gateway 정보 234
Storage Gateway 로그 파일 항목 이해 235
게이트웨이 문제 해결 238
문제 해결: 게이트웨이 오프라인 문제 238
연결된 방화벽 또는 프록시 확인 239
게이트웨이 트래픽에 대해 SSL 또는 딥패킷 검사가 진행 중인지 확인 239
하이퍼바이저 호스트의 정전 또는 하드웨어 장애 확인 239
연결된 캐시 디스크에 문제가 있는지 확인 239
문제 해결: 게이트웨이 활성화 문제 240
퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결 241
Amazon VPC 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결 243
퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하는 중 동일한 VPC에 Storage Gateway VPC 엔드포인트가 있을 때 발생하는 오류 해결 247
온프레미스 게이트웨이 문제 해결 248
게이트웨이 문제 해결 지원 에 도움이 되도록 활성화 253
Microsoft Hyper-V 설정 관련 문제 해결 254
Amazon EC2 게이트웨이 문제 해결 257

몇 분 후 게이트웨이가 활성화되지 않음 ... 257
인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없음 ... 257
Amazon EBS 볼륨을 EC2 게이트웨이 인스턴스에 연결할 수 없음 ... 258
스토리지 볼륨을 추가하려고 하는데 사용 가능한 디스크가 없다는 메시지 ... 258
업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이는 방법 ... 258
EC2 게이트웨이와 주고받는 데이터의 처리량이 0으로 떨어짐 ... 258
게이트웨이 문제 해결 지원 에 도움이 되도록 활성화 ... 259
직렬 콘솔을 사용하여 Amazon EC2 게이트웨이에 연결하려는 경우 ... 261
하드웨어 어플라이언스 문제 해결 ... 261
서비스 IP 주소를 확인하는 방법 ... 261
공장 초기화를 수행하는 방법 ... 261
원격 재시작을 수행하는 방법 ... 261
Dell iDRAC 지원을 받는 방법 ... 261
하드웨어 어플라이언스 일련 번호를 찾는 방법 ... 262
하드웨어 어플라이언스 지원을 받는 방법 ... 262
가상 테이프 관련 문제 해결 ... 263
복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우 ... 263
복구 불가능한 테이프 문제 해결 ... 266
고가용성 상태 알림 ... 268
고가용성 문제 해결 ... 268
상태 알림 ... 268
Metrics ... 269
모범 사례 ... 270
모범 사례: 데이터 복구 ... 270
VM이 예기치 않게 종료된 상황에서 복구하기 ... 271
장애가 있는 게이트웨이 또는 VM에서 데이터 복구 ... 271
복구할 수 없는 테이프에서 데이터 복구 ... 271
장애가 있는 캐시 디스크에서 데이터 복구 ... 272
액세스할 수 없는 데이터 센터에서 데이터 복구 ... 272
불필요한 리소스 정리 ... 273
추가 리소스 ... 274
호스트 설정 ... 275
Tape Gateway용 기본 Amazon EC2 호스트 배포 ... 275
Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 ... 278
Amazon EC2 인스턴스 메타데이터 옵션 수정 ... 281
Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화 ... 282

VM 시간을 VMware 호스트 시간과 동기화 ... 282
반가상화된 디스크 컨트롤러 구성 ... 284
게이트웨이용 네트워크 어댑터 구성 ... 284
Storage Gateway와 함께 VMware High Availability 사용 ... 289
Tape Gateway 스토리지 리소스 작업 ... 294
게이트웨이에서 디스크 제거 ... 295
EC2 게이트웨이용 EBS 볼륨 ... 296
VTL 디바이스 작업 ... 297
테이프 관련 작업 ... 300
정품 인증 키 가져오기 ... 302
Linux(curl) ... 303
Linux(bash/zsh) ... 305
Microsoft Windows PowerShell ... 305
로컬 콘솔 사용 ... 306
iSCSI 초기자 연결 ... 307
Windows 클라이언트에 VTL 디바이스 연결 ... 308
Linux 클라이언트에 VTL 디바이스 연결 ... 311
iSCSI 설정 사용자 지정 ... 313
CHAP 인증 구성 ... 317
Storage Gateway Direct Connect 와 함께 사용 ... 323
게이트웨이 IP 주소 가져오기 ... 323
Amazon EC2 호스트에서 IP 주소 얻기 ... 324
IPv6 지원 ... 325
리소스 및 리소스 ID 이해 ... 325
리소스 ID 작업 ... 326
리소스에 태그 지정 ... 326
태그 작업 ... 327
오픈 소스 구성 요소 ... 328
할당량 ... 328
테이프 할당량 ... 329
게이트웨이에 권장되는 로컬 디스크 크기 ... 329
API 참조 ... 330
필수 요청 헤더 ... 330
요청에 서명하기 ... 332
서명 계산 예시 ... 333
오류 응답 ... 335

예외 335
작업 오류 코드 337
오류 응답 357
운영 359
문서 이력 360
이전 업데이트 375
AL2에서 AL2023으로 마이그레이션 392
빠른 링크 및 리소스 392
게이트웨이 버전 마이그레이션 참조 392
마이그레이션 타임라인 393
마이그레이션 가이드 393
지원 및 모니터링 393
FAQ 394
릴리스 노트 395
..... cdiii

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 VMware ESXi, KVM 또는 Microsoft Hyper-V 하이퍼바이저에서 실행되는 VM 어플라이언스로, 하드웨어 어플라이언스로 또는에서 Amazon EC2 인스턴스 AWS 로 배포할 수 있습니다. EC2 인스턴스에서 호스팅하는 게이트웨이는 재해 복구 및 데이터 미러링에 사용하거나, Amazon EC2에서 호스팅하는 애플리케이션에 스토리지 제공하는 데 사용할 수 있습니다.

가 가능하게 하는 AWS Storage Gateway 데 도움이 되는 다양한 사용 사례를 보려면 섹션을 참조하세요AWS Storage Gateway. 최신 요금 정보는 AWS Storage Gateway 세부 정보 페이지에서 요금을 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 지원 가상 테이프 스토리지를 제공합니다. Tape Gateway를 사용하면 백업 데이터를 비용 효율 및 내구성이 좋은 방식으로 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브할 수 있습니다. Tape Gateway는 비즈니스 요구에 따라 원활하게 규모를 조정할 수 있는 가상 테이프 인프라를 제공하여 물리적 테이프 인프라를 프로비저닝, 조정 및 유지 관리해야 하는 운영 부담을 없애줍니다.

아키텍처 개요에 대해서는 Tape Gateway 작동 방식 단원을 참조하십시오.

이 사용 설명서에는 모든 게이트웨이 유형에 공통으로 적용되는 설정 정보를 다루는 시작하기 단원이 있습니다. 또한 Tape Gateway 설정 요구 사항 및 Tape Gateway를 배포, 활성화, 구성 및 관리하는 방법을 설명하는 단원도 있습니다.

이 사용 설명서의 절차는 주로 AWS Management Console을 사용하여 게이트웨이 작업을 수행하는 데 중점을 둡니다. 이러한 작업을 프로그래밍 방식으로 수행하려면 AWS Storage Gateway API 참조를 참조하세요.

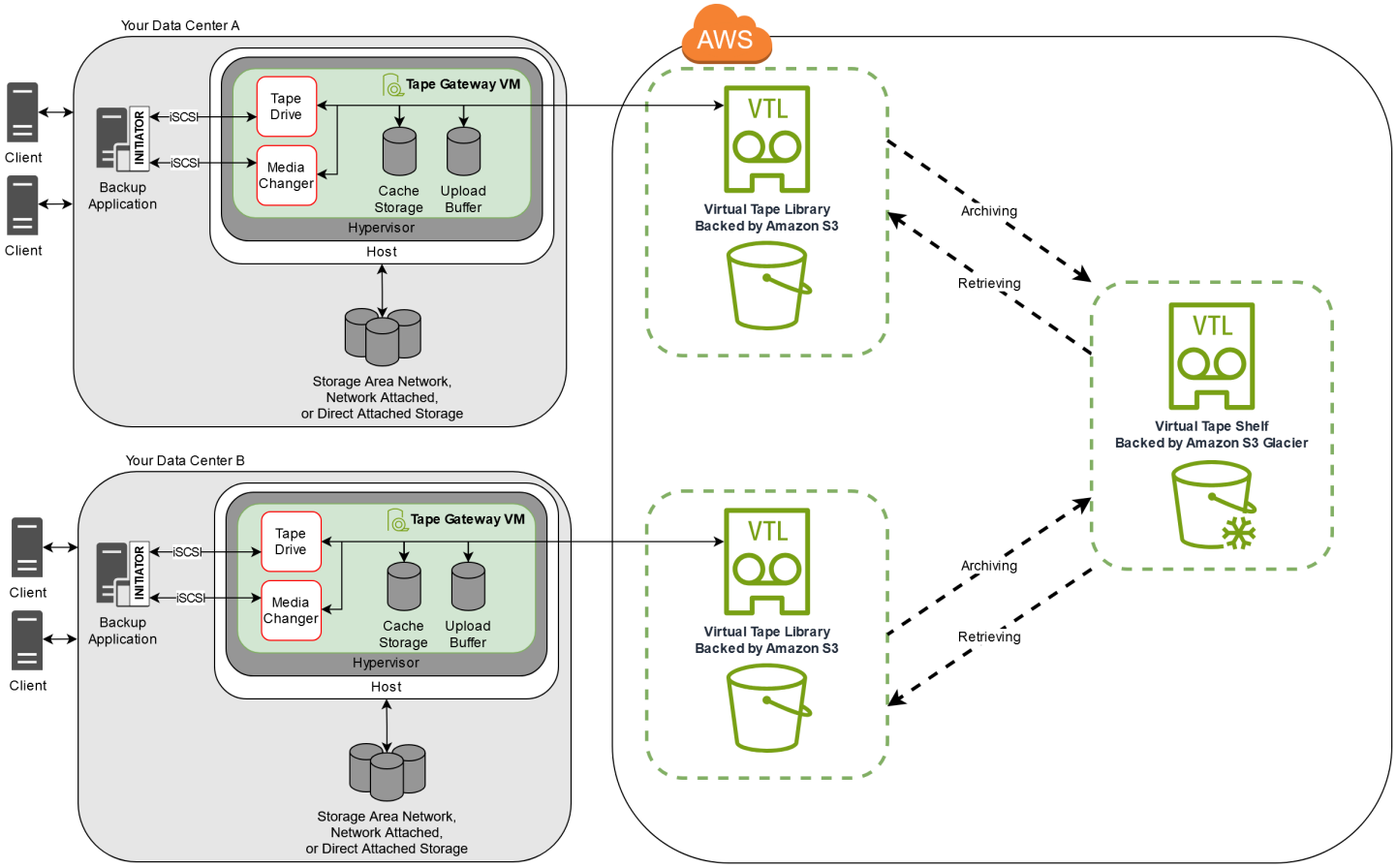
Tape Gateway 작동 방식

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 통해 기존 테이프 기반 백업 인프라를 최대한 활용하여 Tape Gateway에 생성하는 가상 테이프 카트리지에 데이터를 저장할 수 있습니다. 각 Tape Gateway에는 미디어 체인저 및 테이프 드라이브가 사전 구성되어 있습니다. 이러한 테이프 드라이브와 미디어 체인저는 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 Storage Gateway API를 사용하여 프로그램 방식으로 가상 테이프를 생성할 수 있습니다. 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 팔과 테이프 드라이브로 온프레미스에서 사용할 수 있는 물리적 테이프 라이브러리와 유사합니다. VTL에는 저장된 가상 테이프 모음이 포함됩니다. Tape Gateway마다 하나의 VTL이 제공됩니다.

  생성한 가상 테이프는 게이트웨이의 VTL에 표시됩니다. VTL의 테이프는 Amazon S3에 의해 백업됩니다. 백업 소프트웨어가 게이트웨이에 데이터를 쓰면 게이트웨이는 데이터를 로컬에 저장한 다음 VTL의 가상 테이프, 즉 Amazon S3에 비동기식으로 업로드합니다.

  - 테이프 드라이브 - VTL 테이프 드라이브는 I/O를 수행하고 테이프에서 작업을 검색할 수 있는 물리적 테이프 드라이브와 유사합니다. 각 VTL에는 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있는 테이프 드라이브 10개가 한 세트로 제공됩니다.
  - 미디어 체인저 - VTL 미디어 체인저는 물리적 테이프 라이브러리의 스토리지 슬롯 및 테이프 드라이브에서 테이프를 이동하는 로봇과 유사합니다. 각 VTL에는 백업 애플리케이션에서 iSCSI 디바이스로 사용할 수 있는 미디어 체인저가 한 개 제공됩니다.
- 아카이브 - 아카이브는 외부 테이프 보유 시설과 유사합니다. 게이트웨이의 VTL에서 아카이브로 테이프를 보관할 수 있습니다. 필요 시 아카이브에서 게이트웨이의 VTL로 테이프를 다시 가져올 수 있습니다.
  - 테이프 아카이브 - 백업 소프트웨어가 테이프를 배출하면 게이트웨이는 장기 스토리지용 아카이브로 테이프를 옮깁니다. 아카이브는 게이트웨이를 활성화한 AWS 리전에 있습니다. 아카이브의 테이프는 VTS(Virtual Tape Shelf)에 저장됩니다. VTS는 데이터 아카이브, 백업, 장기 데이터 보존을 위한 저비용 스토리지 서비스인 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive의 지원을 받습니다.
  - 테이프 가져오기 - 아카이브된 테이프는 직접 읽을 수 없습니다. 아카이브된 테이프를 읽으려면 먼저 Storage Gateway 콘솔이나 Storage Gateway API를 사용하여 Tape Gateway로 테이프를 가져와야 합니다.

  > **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 마운트합니다. 필요 시 가상 테이프를 생성할 수 있습니다. 그러고 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 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 시작하기에 대한 지침을 제공합니다 AWS. 사용을 시작하려면 AWS 계정이 필요합니다 AWS Storage Gateway. 기존 AWS 계정을 사용하거나 새 계정에 가입할 수 있습니다. 또한 Storage Gateway 작업을 수행하는 데 필요한 관리 권한이 있는 그룹에 속한 AWS 계정의 IAM 사용자가 필요합니다. 적절한 권한이 있는 사용자는 Storage Gateway 콘솔 및 Storage Gateway API에 액세스하여 게이트웨이 배포, 구성 및 유지 관리 작업을 수행할 수 있습니다. 처음 사용하는 경우 Storage Gateway를 사용하기 전에 지원되는 AWS 리전 및 Tape Gateway 설정 요구 사항 단원을 검토하는 것이 좋습니다.

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

주제

- 에 가입 AWS Storage Gateway -에 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 SDKs를 사용하여 프로그래밍 방식으로에 AWS 액세스하는 방법을 알아봅니다.
- AWS 리전 Storage Gateway를 지원하는 - Storage Gateway에서 게이트웨이를 활성화할 때 데이터를 저장하는 데 사용할 수 있는 AWS 리전을 알아봅니다.

에 가입 AWS Storage Gateway

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

이 없는 경우 다음 단계를 AWS 계정완료하여 생성합니다.

에 가입하려면 AWS 계정

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

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

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

또한에 액세스할 때 사용자에게 임시 자격 증명을 사용하도록 요구하는 것이 좋습니다 AWS. 임시 자격 증명을 제공하기 위해 페더레이션과 AWS IAM Identity Center와 같은 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 생성한 다음 관리 권한이 있는 그룹에 해당 사용자를 추가합니다. AWS Identity and Access Management 서비스를 사용하여 Storage Gateway 리소스에 대한 액세스를 제어하는 방법에 대한 자세한 내용은 섹션을 참조하세요Identity and Access Management for AWS Storage Gateway.

다음 옵션 중 하나를 선택하여 관리 사용자를 생성합니다.

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

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

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

액세스 AWS Storage Gateway

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

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

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

요금에 대한 자세한 정보는 AWS Storage Gateway 요금을 참조하세요.

AWS 리전 Storage Gateway를 지원하는

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

- Storage Gateway - Storage Gateway와 함께 사용할 수 있는 지원되는 AWS 리전 및 AWS 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.
- Storage Gateway 하드웨어 어플라이언스 - 하드웨어 어플라이언스와 함께 사용할 수 있는 지원되는 AWS 리전은의 AWS Storage Gateway 하드웨어 어플라이언스 리전을 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.

VM의 하드웨어 요구 사항

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

- VM에 지정한 가상 프로세스 4개.
- Tape Gateway의 경우 하드웨어에 할당해야 하는 RAM 양은 다음과 같습니다.
  - 16GiB의 예약 RAM(캐시 크기가 최대 16 TiB인 게이트웨이)
  - 32GiB의 예약 RAM(캐시 크기가 16TiB-32TiB인 게이트웨이)
  - 48GiB의 예약 RAM(캐시 크기가 32TiB-64TiB인 게이트웨이)
- 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 섹션을 참조하세요.

Amazon EC2 인스턴스 유형에 대한 요구 사항

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

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

Tape Gateway의 경우 게이트웨이에 사용하려는 캐시 크기에 따라 Amazon EC2 인스턴스는 다음과 같은 양의 RAM을 할당해야 합니다:

- 16GiB의 예약 RAM(캐시 크기가 최대 16 TiB인 게이트웨이)
- 32GiB의 예약 RAM(캐시 크기가 16TiB-32TiB인 게이트웨이)
- 48GiB의 예약 RAM(캐시 크기가 32TiB-64TiB인 게이트웨이)

게이트웨이 유형에 대한 권장 인스턴스 유형 중 하나를 사용합니다.

Tape Gateway에 권장

- 범용 인스턴스 패밀리 - m5 또는 m6 인스턴스 유형.
- 컴퓨팅 최적화 인스턴스 패밀리 – c5, c6, 또는 c7 인스턴스 유형. RAM 요구 사항을 충족할 수 있도록 인스턴스 크기를 2xlarge 이상으로 선택합니다.
- 메모리 최적화 인스턴스 패밀리 – r5, r6 또는 r7 인스턴스 유형.
- 스토리지 최적화 인스턴스 패밀리 - i3, i4 또는 i7 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 때 호스트(하이퍼바이저 또는 Amazon EC2 인스턴스)에 새 디스크를 생성하는 것이 중요합니다. 기존 디스크가 이전에 캐시 또는 업로드 버퍼로 할당되었던 경우, 디스크 크기를 변경하지 마세요.

게이트웨이 할당량에 대한 자세한 내용은 AWS Storage Gateway 할당량 섹션을 참조하세요.

네트워크 및 방화벽 요구 사항

게이트웨이에서 인터넷, 로컬 네트워크, 도메인 이름 서비스(DNS) 서버, 방화벽, 라우터 등에 액세스할 수 있어야 합니다. 아래에서 필수 포트에 대한 정보와 방화벽 및 라우터를 통한 액세스를 허용하는 방법에 대한 정보를 얻을 수 있습니다.

> **Note**
>
> 경우에 따라 Amazon EC2에 Storage Gateway를 배포하거나 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 값은AWS 일반 참조에서 AWS IP 주소 범위를 참조하세요.

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

합니다. 데이터 전송 패턴에 따라 워크로드 지원에 필요한 대역폭이 결정됩니다. 경우에 따라 Amazon EC2에 Storage Gateway를 배포하거나 다른 유형의 배포를 사용할 수 있습니다.

주제

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

포트 요구 사항

Tape Gateway를 성공적으로 배포하고 작동하려면 네트워크 보안을 통해 특정 포트를 허용해야 합니다. 일부 포트는 모든 게이트웨이에 필요하며, 다른 포트는 VPC 엔드포인트에 연결할 때와 같은 특정 구성에만 필요합니다.

Tape Gateway의 포트 요구 사항

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

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

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

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

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

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

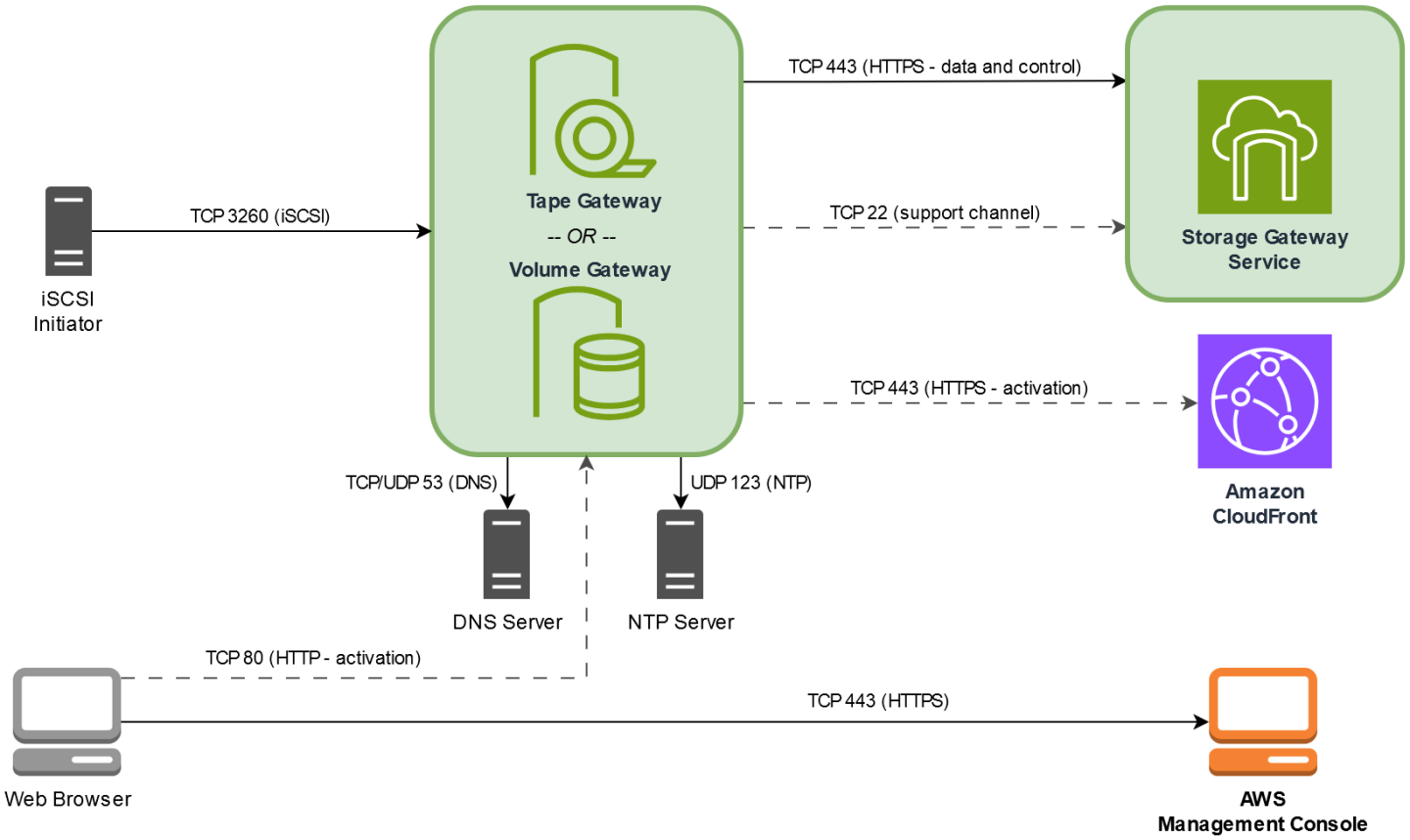
네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
Storage Gateway	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	관리 제어
Amazon CloudFront	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓	정품 인증용
VPC	Storage Gateway VM	AWS	TCP HTTPS	443	✓	✓	✓*	관리 제어 *VPC 엔드포인트를 사용하는 경우에만 필수
VPC	Storage Gateway VM	AWS	TCP HTTPS	1026		✓	✓*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

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

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

네트워크 요소	From	목적	프로토콜	포트	인바운드	아웃바운드	필수	참고
iSCSI 클라이언트	iSCSI 클라이언트	Storage Gateway VM	TCP	3260	✓	✓	✓	게이트웨이에 표시된 iSCSI 대상에 연결할 때 로컬 시스템이 사용합니다.

다음 그림은 기본 Tape Gateway 배포의 네트워크 트래픽 흐름을 보여줍니다.



Storage Gateway Hardware Appliance에 대한 네트워킹 및 방화벽 요구 사항

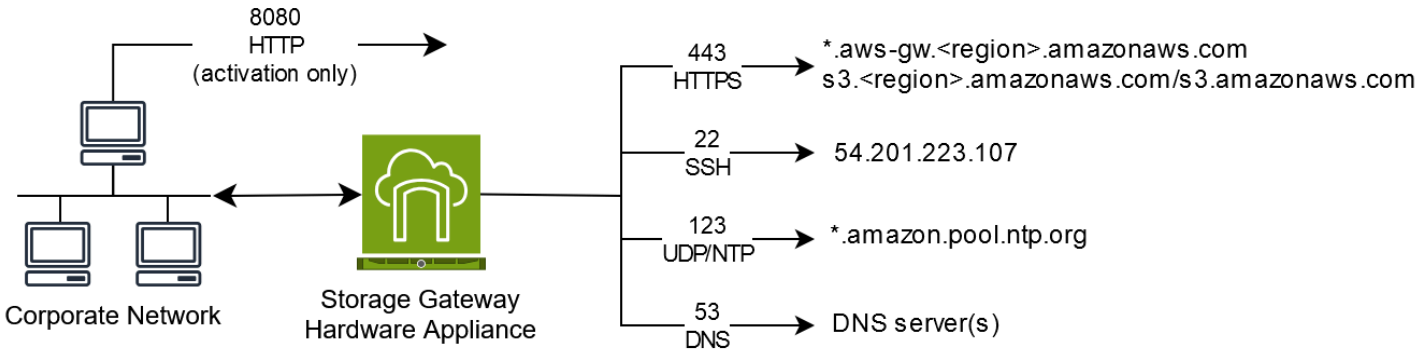
각 Storage Gateway Hardware Appliance에는 다음과 같은 네트워크 서비스가 필요합니다.

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

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

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

iDRAC 포트는 원격 서버 관리에 사용할 수 있습니다.



하드웨어 어플라이언스를 작동하려면 다음 포트가 필요합니다.

프로토콜	포트	Direction	소스	Destination	용도
SSH	22	아웃바운드	하드웨어 어플라이언스	54.201.223.107	지원 채널

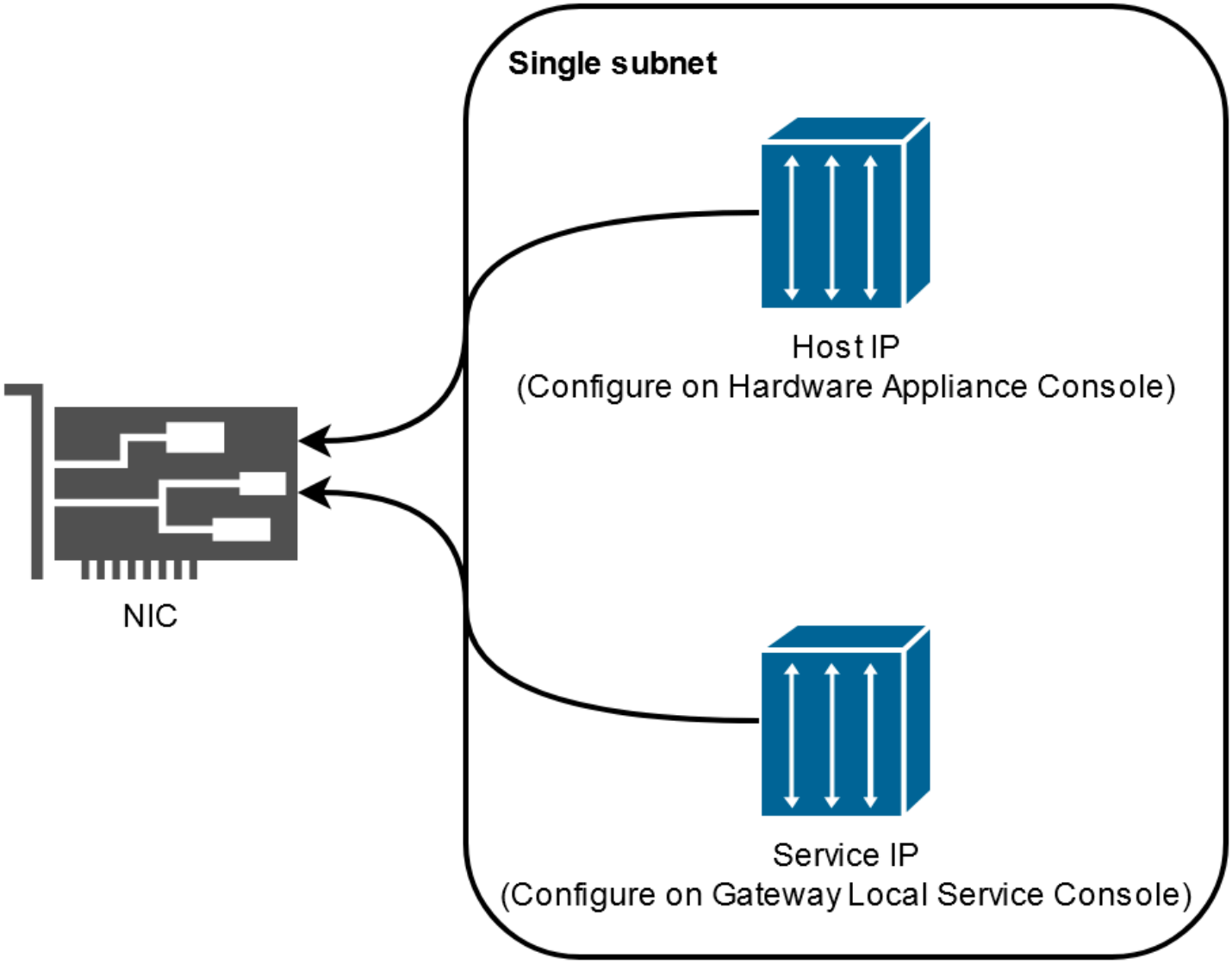
프로토콜	포트	Direction	소스	Destination	용도
DNS	53	아웃바운드	하드웨어 어플라이언스	DNS 서버	이름 확인
UDP/NTP	123	아웃바운드	하드웨어 어플라이언스	`*.amazon.pool.ntp.org`	시간 동기화
HTTPS	443	아웃바운드	하드웨어 어플라이언스	`*.amazonaws.com`	데이터 전송
HTTP	8080	인바운드	AWS	하드웨어 어플라이언스	활성화(잠시 동안)

하드웨어 어플라이언스는 설계상 다음과 같은 네트워크 및 방화벽 설정이 필요합니다.

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

> **Note**
>
> 서버 뒷면과 포트가 나와 있는 그림을 보려면 하드웨어 어플라이언스를 물리적으로 설치하기 단원을 참조하십시오.

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



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

방화벽 및 라우터를 통한 AWS Storage Gateway 액세스 허용

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

> **Note**
>
> Storage Gateway가 연결 및 데이터 전송에 사용하도록 프라이빗 VPC 엔드포인트를 구성하는 경우 AWS게이트웨이는 퍼블릭 인터넷에 액세스할 필요가 없습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하세요.

> **Important**
>
> 게이트웨이의 AWS 리전에 따라 서비스 엔드포인트의 ##을 올바른 리전 문자열로 바꿉니다.

엔드포인트 유형

표준 엔드포인트

이러한 엔드포인트는 게이트웨이 어플라이언스와 간의 IPv4 트래픽을 지원합니다 AWS.

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

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

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

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

다음 게이트웨이 서비스 엔드포인트는 API 호출에 필요합니다.

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

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

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

듀얼 스택 엔드포인트

이러한 엔드포인트는 게이트웨이 어플라이언스와 간의 IPv4 및 IPv6 트래픽을 모두 지원합니다 AWS.

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

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

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

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

다음 게이트웨이 듀얼 스택 서비스 엔드포인트는 API 호출에 필요합니다.

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

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

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

NTP 서버

Storage Gateway VM에는 다음 NTP 서버에 대한 네트워크 액세스 권한이 필요합니다.

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

지원되는 엔드포인트 AWS 리전 및 서비스 엔드포인트의 전체 목록은의 Storage Gateway를 참조하세요AWS 일반 참조.

Amazon EC2 게이트웨이 인스턴스에 대한 보안 그룹 구성

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

- 보안 그룹은 외부 인터넷에서 들어오는 연결을 허용해서는 안 됩니다. 게이트웨이 보안 그룹 내 인스턴스만 게이트웨이와 통신할 수 있도록 허용해야 합니다. 인스턴스가 보안 그룹 외부에서 게이트웨이에 연결해야 하는 경우에는 포트 3260(iSCSI 연결용) 및 포트 80(활성화용)에 대해서만 연결을 허용하는 것이 좋습니다.
- 게이트웨이 보안 그룹 외부에 있는 Amazon EC2 호스트에서 게이트웨이를 활성화하려면 호스트의 IP 주소에서 포트 80으로 들어오는 접속을 허용합니다. 활성화 호스트의 IP 주소를 확인할 수 없는 경우에는 포트 80을 열어 게이트웨이를 활성화하고 활성화가 완료되면 포트 80에 대한 액세스를 종료하는 방법을 사용할 수 있습니다.
- 문제 해결을 지원 위해를 사용하는 경우에만 포트 22 액세스를 허용합니다. 자세한 내용은 EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우 단원을 참조하십시오.

경우에 따라서는 Amazon EC2 인스턴스를 이니시에이터로 사용할 수도 있습니다. 즉, Amazon EC2에 배포한 게이트웨이에 있는 iSCSI 대상에 연결하는 데 사용합니다. 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 포트 요구 사항 섹션을 참조하세요.

지원되는 하이퍼바이저 및 호스트 요구 사항

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

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

> **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 연결하기 위한 VMware vSphere 클라이언트도 필요합니다.
- Microsoft Hyper-V Hypervisor(버전 2019, 2022 또는 2025) -이 설정의 경우 호스트에 연결하려면 Microsoft Windows 클라이언트 컴퓨터에 Microsoft Hyper-V Manager가 필요합니다.
- Linux 커널 기반 가상 머신(KVM) - 무료 오픈 소스 가상화 기술입니다. KVM은 Linux 버전 2.6.20 이상의 모든 버전에 포함되어 있습니다. Storage Gateway는 CentOS/RHEL 7.7, Ubuntu 16.04 LTS, Ubuntu 18.04 LTS 배포판에 대해 테스트 및 지원됩니다. 다른 최신 Linux 배포판이 작동하지만 기능이나 성능이 보장되지는 않습니다. KVM 환경이 이미 가동되고 있고 KVM 작동 방식에 익숙하다면 이 옵션을 사용하는 것이 좋습니다. 제안된 부팅 구성은 제공된 aws-storage-gateway.xml 파일을 참조하세요. File Gateway 2.x, Volume Gateway 3.x 및 Tape Gateway 3.x에는 보안 부팅이 비활성화된 UEFI 부팅 모드(loader_secure=no)가 필요합니다.
- 버전 10.0.1.1부터 시작하는 Nutanix AHV(Acropolis Hypervisor) - Nutanix 하이퍼 컨버지드 인프라(HCI) 솔루션에 통합된 KVM 기반 가상화 플랫폼입니다.
- Amazon EC2 인스턴스 - Storage Gateway는 게이트웨이 VM 이미지를 포함하는 Amazon Machine Image(AMI)를 제공합니다. 파일, 캐시 볼륨 및 Tape Gateway 유형만 Amazon EC2에 배포할 수 있습니다. Amazon EC2에 게이트웨이를 배포하는 방법에 대한 자세한 내용은 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 섹션을 참조하세요.
- 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 복제본에서 생성된 VM이나 Amazon EC2 AMI에서 게이트웨이를 복구하는 기능을 지원하지 않습니다. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 새로운 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다. 자세한 내용은 가상 머신이 예기치 않게 종료된 상황에서 복구하기 단원을 참조하십시오.

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

지원되는 iSCSI 이니시에이터

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

이 iSCSI 디바이스에 연결하기 위해 Storage Gateway에서 지원하는 iSCSI 이니시에이터는 다음과 같습니다.

- Microsoft Windows Server 2022
- Red Hat Enterprise Linux 8
- Red Hat Enterprise Linux 9
- VMware ESX 이니시에이터(VM의 게스트 운영 체제에서 이니시에이터를 사용하는 방식의 대안)

Important

Storage Gateway는 Windows 클라이언트에서 Microsoft Multipath I/O(MPIO)를 지원하지 않습니다.
이제 Storage Gateway는 호스트가 Windows Server Failover Clustering(WSFC)을 사용하여 액세스를 조정할 경우 한 볼륨에 여러 호스트를 연결하도록 지원합니다. 하지만 WSFC를 사용하지 않으면 한 볼륨에 여러 호스트를 연결할 수 없습니다(예: 비클러스터 NTFS/ext4 파일 시스템 공유).

Tape Gateway에 지원되는 타사 백업 애플리케이션

백업 애플리케이션을 사용하여 Tape Gateway로 테이프에 대한 읽기, 쓰기 및 관리 작업을 수행할 수 있습니다. 선택할 미디어 체인저의 유형은 사용하려고 계획한 백업 애플리케이션에 따라 달라집니다.

AWS 는 이러한 Tape Gateway 기능과의 호환성을 보장하기 위해 다음 표에서 타사 백업 애플리케이션을 테스트했습니다.

- iSCSI 초기자 연결, 미디어 체인저, 재스캔, 자동 및 수동 디바이스 매핑을 포함한 검색 기능.
- 생성, 삭제, 가져오기, 내보내기, 인벤토리 및 바코드 가시성을 포함한 테이프 함수.

- 테이프 콘텐츠를 삭제하고 후속 복원에 데이터가 포함되어 있지 않은지 확인합니다.
- 단일 및 여러 테이프로 데이터 백업, 테이프 용량을 초과하는 백업 작업이 추가 테이프를 기다리기 위해 일시 중지되는지 확인.
- 테이프에서 전체 및 부분 데이터 복원 및 데이터 무결성 확인.
- 백업 작업 중 게이트웨이 종료 및 재시작 이벤트 후 기능 및 데이터 무결성 확인.

백업 애플리케이션	버전	미디어 체인저 유형	게이트웨이 버전 테스트됨
Arcserve 백업	19	AWS-Gateway-VTL	2.12.3
Bacula Enterprise	15.0.2	AWS-Gateway-VTL 또는 STK-L700	2.12.3
Commvault	2024E/11.36.35	STK-L700	2.12.3
Dell EMC NetWorker	19.10	AWS-Gateway-VTL	2.12.3
IBM 스토리지 보호	8.1.10	IBM-03584L32-0402	모두
Micro Focus Data Protector	24.4	AWS-Gateway-VTL	2.12.3
Microsoft System Center 데이터 보호 관리자	2025	STK-L700	2.12.3
NovaStor DataCenter	9.5.3	STK-L700	2.12.3
Quest NetVault Backup	13.3	STK-L700	2.12.3
Veeam Backup & Replication	12	AWS-Gateway-VTL	모두
Veritas Backup Exec	24	AWS-Gateway-VTL	모두
Veritas NetBackup	10.5	AWS-Gateway-VTL	2.12.3

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 선택을 참조하세요.

Storage Gateway 하드웨어 어플라이언스 사용

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

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 프로세스를 통해 하드웨어 어플라이언스가 AWS 계정과 연결됩니다. 활성화 후에는 하드웨어 어플라이언스가 콘솔의 하드웨어 어플라이언스 개요 페이지에 표시됩니다. 하드웨어 어플라이언스를 S3 File Gateway, FSx File Gateway, Tape Gateway, 또는 Volume Gateway 유형으로 구성할 수 있습니다. 이러한 게이트웨이 유형을 하드웨어 어플라이언스에 배포하는 절차는 가상 플랫폼에서의 절차와 동일합니다.

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

다음 단원에서는 Storage Gateway 하드웨어 어플라이언스의 설정, 랙 마운팅, 전원 공급, 구성, 활성화, 시작, 사용, 삭제 방법에 대한 지침을 확인할 수 있습니다.

주제

- Storage Gateway 하드웨어 어플라이언스 설정
- 하드웨어 어플라이언스를 물리적으로 설치하기
- 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

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

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

하드웨어 어플라이언스를 설치하고 구성하려면

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

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

사용 가능한 캐시 스토리지 증가

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

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

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

네트워크 인터페이스 카드 옵션

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

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

하드웨어 어플라이언스를 물리적으로 설치하기

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

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

사전 조건

하드웨어 어플라이언스를 설치하려면 다음 구성 요소가 필요합니다.

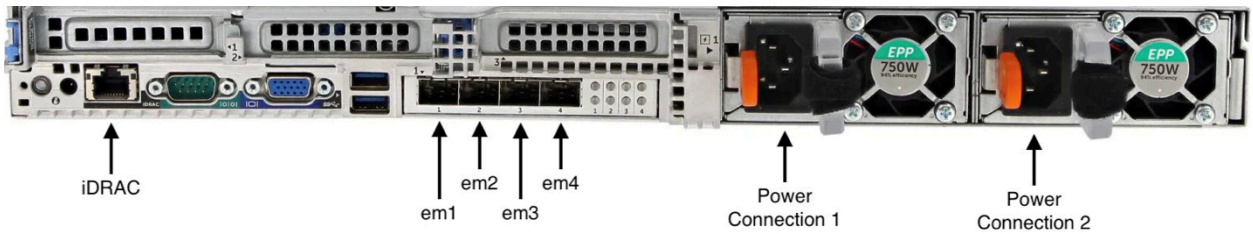
- 전원 케이블: 1개 필요, 2개 권장.
- 지원되는 네트워크 케이블(하드웨어 어플라이언스에 포함된 네트워크 인터페이스 카드(NIC)에 따라 다름). Twinax Copper DAC, SFP+ 광 모듈(Intel 호환) 또는 SFP - Base-T 구리 트랜시버.
- 키보드 및 모니터 또는 키보드, 비디오, 마우스(KVM) 스위치 솔루션.

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

하드웨어 어플라이언스를 물리적으로 설치하려면

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

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

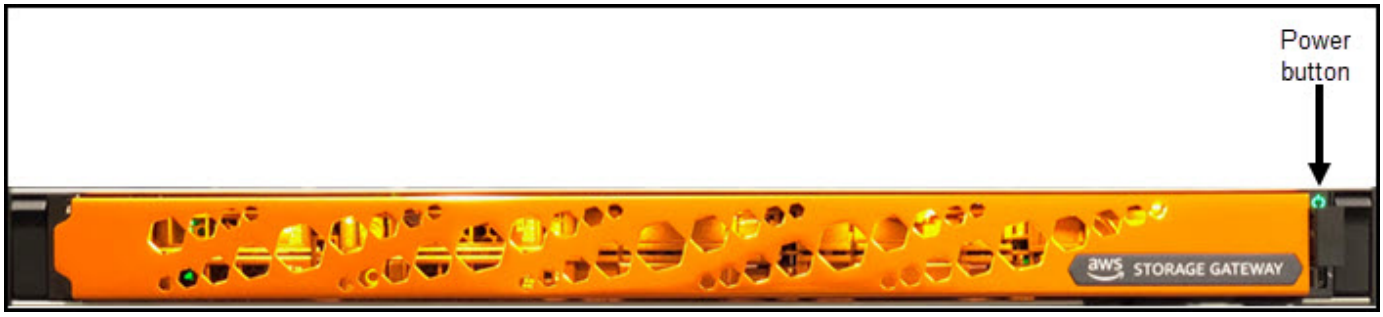
   네트워크 및 전원 커넥터 레이블이 표시된 하드웨어 어플라이언스 1 후면입니다.

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

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

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

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



전원 버튼 레이블이 표시된 하드웨어 어플라이언스 전면입니다.

다음 단계

하드웨어 어플라이언스 콘솔 액세스

하드웨어 어플라이언스 콘솔 액세스

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

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

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

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

관리자 암호를 설정하려면

- 로그인 암호 설정 프롬프트에서 다음을 수행합니다.

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

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

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

다음 단계

하드웨어 어플라이언스 네트워크 파라미터 구성

하드웨어 어플라이언스 네트워크 파라미터 구성

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

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

네트워크 주소를 설정하려면

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

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

     이 주소는 나중에 활성화 단계에서 사용할 수 있도록 기록해 둡니다.
   - 정적 IPv4 주소를 구성하려면 정적을 선택하고 `Enter` 키를 누릅니다.

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

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

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

하드웨어 콘솔에서 로그아웃하려면

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

다음 단계

Storage Gateway 하드웨어 어플라이언스 활성화

Storage Gateway 하드웨어 어플라이언스 활성화

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

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

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

Storage Gateway 하드웨어 어플라이언스 활성화

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

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

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

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

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

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

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

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

다음 단계

하드웨어 어플라이언스에서 게이트웨이 생성

하드웨어 어플라이언스에서 게이트웨이 생성

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

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

하드웨어 어플라이언스에서 게이트웨이를 생성하려면

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

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

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

다음 단계

하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성

하드웨어 어플라이언스에서 게이트웨이 IP 주소 구성

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

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

애플리케이션에서 작동하도록 어플라이언스에서 IP 주소를 구성하려면

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

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

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

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

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

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

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

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

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

게이트웨이 로컬 콘솔을 종료하려면

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

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

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

하드웨어 어플라이언스에서 게이트웨이 소프트웨어 제거

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

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

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

하드웨어 어플라이언스에서 게이트웨이를 제거하려면

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

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

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

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

Storage Gateway 하드웨어 어플라이언스 삭제

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

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

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

하드웨어 어플라이언스를 삭제하려면

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

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

게이트웨이 생성

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

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

> **Important**
>
> 신규 고객은 더 이상 Amazon FSx File Gateway를 사용할 수 없습니다. 기존 FSx File Gateway 고객은 정상적으로 서비스를 계속 이용할 수 있습니다. FSx File Gateway와 유사한 기능에 대해서는 이 블로그 게시물을 참조하세요.

개요 - 게이트웨이 활성화

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

게이트웨이 설정

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

에 연결 AWS

다음 단계는 게이트웨이를 AWS에 연결하는 것입니다. 이렇게 하려면 먼저 게이트웨이 가상 어플라이언스와 클라우드의 서비스 간의 통신에 사용할 AWS 서비스 엔드포인트 유형을 선택합니다. 이 엔드포인트는 퍼블릭 인터넷에서 액세스할 수도 있고, 사용자가 네트워크 보안 구성을 완전히 제어할 수 있

도록 Amazon VPC 내에서만 액세스할 수도 있습니다. 그런 다음 게이트웨이의 IP 주소 또는 정품 인증 키를 지정합니다. 이 정보는 게이트웨이 어플라이언스의 로컬 콘솔에 연결하여 얻을 수 있습니다.

검토 및 활성화

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

개요 - 게이트웨이 구성

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

개요 - 스토리지 리소스

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

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 Gateway를에 연결 AWS
- 설정 검토 및 Tape Gateway 활성화
- Tape Gateway 구성

Tape Gateway 설정

새 Tape Gateway를 설정하려면

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

   a. 게이트웨이 이름에 게이트웨이 이름을 입력합니다. 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 ESXi를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
      - Microsoft Hyper-V - Microsoft Hyper-V를 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다.
      - Linux KVM - Linux KVM을 사용하여 게이트웨이 가상 머신을 다운로드, 배포 및 구성합니다. 제안된 부팅 구성은 제공된 aws-storage-gateway.xml 파일을 참조하세요. File Gateway 2.x, Volume Gateway 3.x 및 Tape Gateway 3.x에는 보안 부팅이 비활성화된 UEFI 부팅 모드(loader_secure=no)가 필요합니다.
      - 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.

게이트웨이가 설정되었으므로 게이트웨이를 연결하고 통신할 방법을 선택해야 합니다 AWS. 지침은 Tape Gateway를에 연결을 참조하세요 AWS.

Tape Gateway를에 연결 AWS

새 Tape Gateway를에 연결하려면 AWS

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

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

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

   - VPC 호스팅 - 게이트웨이가 VPC와의 프라이빗 연결을 통해 AWS 와 통신하므로 사용자가 네트워크 설정을 제어할 수 있습니다. 이 옵션을 선택하는 경우 드롭다운 메뉴에서 VPC 엔드포인트 ID를 선택하거나 VPC 엔드포인트 DNS 이름 또는 IP 주소를 제공하여 기존 VPC 엔드포인트를 지정해야 합니다. 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 연결할 방법을 선택했으므로 게이트웨이를 활성화 AWS해야 합니다. 지침은 설정 검토 및 Tape Gateway 활성화를 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 Gateway를에 연결 AWS

   완료했으면 다음을 선택하여 Storage Gateway 콘솔에서 검토 및 활성화 페이지를 엽니다.
2. 페이지에서 각 섹션의 초기 게이트웨이 세부 정보를 검토합니다.
3. 섹션에 오류가 있는 경우 편집을 선택하여 해당 설정 페이지로 돌아가서 변경합니다.

   > **Note**
   >
   > 게이트웨이가 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 구성을 참조하세요.

Tape Gateway 구성

새 Tape Gateway에서 최초 구성을 수행하려면

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

   - Tape Gateway 설정
   - Tape Gateway를에 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 캐시 스토리지에 용량이 165GiB 이상인 디스크를 하나 이상 할당하고 업로드 버퍼에 용량이 150GiB 이상인 디스크를 하나 이상 할당합니다. 이 섹션에 나열된 로컬 디스크는 호스트 플랫폼에서 프로비저닝한 물리적 스토리지에 해당합니다.

3. CloudWatch 로그 그룹 섹션에서 게이트웨이의 상태를 모니터링하기 위해 Amazon CloudWatch Logs를 설정하는 방법을 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.

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

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

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

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

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

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

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

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

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

5. (선택 사항) 태그 섹션에서 새 태그 추가를 선택한 다음 대소문자를 구분하여 키-값 페어를 입력하면 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 생성을 참조하세요.

Tape Gateway용 새 가상 테이프 생성

이 섹션에서는를 사용하여 새 가상 테이프를 생성하는 방법을 설명합니다 AWS Storage Gateway. AWS Storage Gateway 콘솔 또는 Storage Gateway API를 사용하여 수동으로 새 가상 테이프를 생성할 수 있습니다. 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 가상 테이프에 대한 WORM(Write Once Read Many) 및 테이프 보존 잠금을 지원합니다. WORM이 활성화된 가상 테이프는 가상 테이프 라이브러리에 있는 활성 테이프의 데이터를 덮어쓰거나 지울 수 없도록 합니다. 가상 테이프의 WORM 보호에 대한 자세한 내용은 다음 섹션 the section called “WORM 테이프 보호”을 참조하세요.

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 AWS Storage Gateway API 또는 AWS Command Line Interface ()를 사용하여이 작업을 수행할 수 있습니다AWS CLI. 자세한 내용은 CreateTapes 또는 create-tapes를 참조하십시오.

WORM(Write Once Read Many) 테이프 보호

AWS Storage Gateway에서 가상 테이프에 대한 WORM 보호를 활성화하여 가상 테이프를 덮어쓰거나 지우는 것을 방지할 수 있습니다. 가상 테이프에 대한 WORM 보호는 테이프를 생성할 때 활성화됩니다.

WORM 가상 테이프에 기록된 데이터는 덮어쓸 수 없습니다. WORM 가상 테이프에는 새 데이터만 추가할 수 있으며 기존 데이터는 지울 수 없습니다. 가상 테이프에 대해 WORM 보호를 활성화하면 테이프를 꺼내서 아카이브하기 전에 사용 중인 동안 테이프를 보호하는 데 도움이 됩니다.

WORM 구성은 테이프를 생성할 때만 설정할 수 있으며 테이프를 생성한 후에는 변경할 수 없습니다.

수동으로 테이프 생성

AWS Storage Gateway 콘솔 또는 Storage Gateway API를 사용하여 수동으로 새 가상 테이프를 생성할 수 있습니다. 이 콘솔은 무작위로 생성된 테이프 바코드의 접두사를 유연하게 지정할 수 있는 편리한 테이프 생성 인터페이스를 제공합니다. 해당 물리적 테이프의 일련 번호와 일치시키려는 경우와 같이 테이프 바코드를 완전히 사용자 지정해야 하는 경우에는 API를 사용해야 합니다. Storage Gateway API를 사용하여 테이프를 생성하는 방법에 대한 자세한 내용은 Storage Gateway API 참조에서 CreateTapeWithBarcode를 참조하세요.

Storage Gateway 콘솔을 사용하여 가상 테이프를 수동으로 생성하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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. WORM(Write Once Read Many) 가상 테이프를 생성하려면 WORM을 선택합니다. 자세한 내용은 WORM(Write Once Read Many) 테이프 보호를 참조하세요.
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 Retrieval

에 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 클래스를 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 클래스를 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 Retrieva에 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 테이프를 생성할 때 가상 테이프의 상태는 처음에는 CREATING으로 표시됩니다. 테이프 생성이 완료되면 상태가 AVAILABLE로 변경됩니다. 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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. WORM(Write Once Read Many) 가상 테이프를 생성하려면 WORM을 선택합니다. 자세한 내용은 WORM(Write Once Read Many) 테이프 보호를 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 클래스를 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 클래스를 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 Retrieva에 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.

    가상 테이프를 생성할 때 가상 테이프의 상태가 처음에는 생성 중으로 표시됩니다. 테이프 생성이 완료되면 상태가 AVAILABLE로 변경됩니다. 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 테이프가 배출될 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 클래스를 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 클래스를 참조하세요.

테이프를 S3 Glacier Flexible Retrieva에 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 `storagegateway:BypassGovernanceRetention` 수 있습니다. AWS Storage Gateway API를 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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

아래에서 가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 또는 Red Hat Enterprise Linux(RHEL) 클라이언트에 연결하는 지침을 확인할 수 있습니다.

주제

- Microsoft Windows 클라이언트에 연결
- Linux 클라이언트에 연결

Microsoft Windows 클라이언트에 연결

다음 절차는 Windows 클라이언트에 연결하기 위한 단계를 요약하여 보여줍니다.

Windows 클라이언트에서 VTL 디바이스를 연결하려면

1. Start `iscsicpl.exe`.

> **Note**
>
> iSCSI 초기자를 실행하려면 클라이언트 컴퓨터에서 관리자 권한이 있어야 합니다.

2. Microsoft iSCSI 초기자 서비스를 시작합니다.
3. iSCSI Initiator Properties(iSCSI 이니시에이터 속성) 대화 상자에서 Discovery(검색) 탭을 선택한 다음, Discover Portal(포털 검색)을 선택합니다.
4. Tape Gateway의 IP 주소를 IP 주소 또는 DNS 이름에 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 디아비스 드라이버 목록에서 고르기(Let me pick from a list of device drivers on my computer)를 선택합니다.
    d. LTO 테이프 드라이브(LTO Tape drive)를 선택하고 다음을 선택합니다.
5. 닫기를 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 위한 단계를 요약하여 보여줍니다.

Linux 클라이언트를 VTL 인스턴스에 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 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.

   연결 명령에서 올바른 *[GATEWAY_IP]* 및 IQN을 지정해야 합니다.

   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 Linux iSCSI 설정을 사용자 지정에서 설명한 것처럼 iSCSI 설정을 사용자 지정할 것을 적극 권장합니다.

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-0x000000000000002b-lun-0
 -> ../../st4
lrwxrwxrwx 1 root root 10 Aug 19 10:15 pci-0000:12:00.1-fc-0x000000000000002b-
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 사용한 설정 테스트]
- [Bacula Enterprise를 사용하여 설정 테스트]
- [Commvault를 사용한 설정 테스트]

- Dell EMC NetWorker를 사용한 설정 테스트
- IBM Data Protect를 사용하여 설정 테스트
- OpenText Data Protector를 사용하여 설정 테스트
- Microsoft System Center DPM을 사용한 설정 테스트
- NovaStor DataCenter를 사용한 설정 테스트
- Quest NetVault Backup을 사용하여 설정 테스트
- Veeam Backup and Replication을 사용한 설정 테스트
- Veritas Backup Exec을 사용한 설정 테스트
- Veritas NetBackup을 사용한 설정 테스트

Arcserve Backup을 사용한 설정 테스트

Arcserve Backup을 사용하여 데이터를 가상 테이프에 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 사용에 대한 자세한 내용은 Arcserve Backup 설명서를 참조하세요.

주제

- VTL 디바이스와 함께 작동하도록 Arcserve 구성
- 테이프를 미디어 풀로 로드
- 데이터를 테이프에 백업
- 테이프 보관
- 테이프에서 데이터 복원

VTL 디바이스와 함께 작동하도록 Arcserve 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 풀로 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 다음슬롯 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 다음슬롯 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 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 아카이브가 완료되면 테이프는 더 이상 VTL에 나열되지 않고 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 섹션을 참조하세요.
2. ARCserve를 사용하여 데이터를 복원합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다. 지침은 Arcserve Backup 설명서를 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 Enterprise를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 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 사용 방법에 대한 자세한 내용은 Bacula Systems Manuals and Documentation을 참조하거나 Bacula Systems에 문의하세요.

> **Note**
>
> Bacula는 Linux에서만 지원됩니다.

Bacula Enterprise 설정

가상 테이프 라이브러리(VTL) 디바이스를 Linux 클라이언트에 연결한 후 Bacula 소프트웨어가 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

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 Gateway를 참조하세요. 추가적인 설치 지침은 Bacula 백서 Using Cloud Services and Object Storage with Bacula Enterprise Edition을 참조하십시오.

VTL 디바이스와 함께 작동하도록 Bacula 구성

다음에는 VTL 디바이스와 함께 작동하도록 Bacula를 구성합니다. 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 생성을 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**
>
> 백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패하고 Bacula Enterprise의 테이프 상태가 전체로 변경됩니다. 테이프가 충분히 활용되지 않은 경우 수동으로 테이프 상태를 다시 APPEND로 변경하고 동일한 테이프를 사용하여 백업 작업을 계속할 수 있습니다. APPEND 상태의 다른 테이프를 사용할 수 있는 경우 다른 테이프에서 작업을 계속 진행할 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 섹션을 참조하세요.
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

Commvault를 사용하여 데이터를 가상 테이프에 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 설명서를 참조하세요.

주제

- Commvault가 VTL 디바이스와 함께 작동하도록 구성
- 스토리지 정책 및 하위 클라이언트 생성
- Commvault에서 데이터를 테이프로 백업
- Commvault에 테이프 보관
- 테이프에서 데이터 복원

Commvault가 VTL 디바이스와 함께 작동하도록 구성

VTL 디바이스를 Windows 클라이언트에 연결한 후 Commvault가 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 Windows 클라이언트에 VTL 디바이스 연결 단원을 참조하십시오.

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

Commvault를 구성하려면

1. CommCell 콘솔 메인 메뉴에서 Storage(스토리지)를 선택한 다음 Expert Storage Configuration(전문가 스토리지 구성)을 선택하여 Select MediaAgents(MediaAgents 선택)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 다음Detect/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 다음Yes(예)를 선택합니다. 구성 대화 상자를 닫습니다.
8. Does this library have a barcode reader?(이 라이브러리에 바코드 리더가 있습니까) 대화 상자에서 Yes(예)를 선택한 다음 디바이스 유형에서 IBM ULTRIUM V5를 선택합니다.
9. CommCell 브라우저에서 Storage Resources(스토리지 리소스)를 선택한 다음 Libraries(라이브러리)를 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 Policies(정책)를 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. Library for Primary Copy(기본 복사용 라이브러리)에서 VTL 라이브러리를 선택하고 Next(다음)를 선택합니다.

7. 미디어 에이전트 설정이 올바른지 확인하고 Next(다음)를 선택합니다.
8. 스크래치 풀 설정이 올바른지 확인하고 Next(다음)를 선택합니다.
9. iData Agent Backup data(iData 에이전트 백업 데이터)에서 보존 정책을 구성하고 Next(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 Client Computers(클라이언트 컴퓨터)를 선택한 다음 원하는 클라이언트 컴퓨터를 선택합니다. File System(파일 시스템)을 선택한 다음 defaultBackupSet를 선택합니다.
2. defaultBackupSet를 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업)을 선택한 다음 New Subclient(새 하위 클라이언트)를 선택합니다.
3. Subclient(하위 클라이언트) 속성 대화 상자에서 SubClient Name(하위 클라이언트 이름)에 이름을 입력한 다음 OK(확인)를 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 표시되어야 합니다.

Commvault에서 데이터를 테이프로 백업

물리적 테이프와 동일한 절차를 사용하여 백업 작업을 생성하고 가상 테이프에 데이터를 작성합니다. 자세한 내용은 Commvault 설명서를 참조하세요.

> **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 Storage Resources(스토리지 리소스), Libraries(라이브러리), Your library(사용자의 라이브러리)를 차례로 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 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 보관을 완료하면 해당 테이프가 VTL에 표시되지 않습니다.

Commvault 소프트웨어에서 테이프가 더 이상 스토리지 슬롯에 없는지 확인합니다.

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 ARCHIVED인지 확인합니다.

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 비검색 테이프에서 데이터를 복원하려면

1. CommCell 브라우저에서 Client Computers(클라이언트 컴퓨터)를 선택한 다음 원하는 클라이언트 컴퓨터를 선택합니다. File System(파일 시스템)을 선택한 다음 defaultBackupSet를 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 비검색 테이프에서 데이터를 복원하려면

1. CommCell 브라우저에서 Client Computers(클라이언트 컴퓨터)를 선택한 다음 원하는 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 Storage Resources(스토리지 리소스)를 선택하고 Libraries(라이브러리)를 선택한 다음 Your library(사용자의 라이브러리)를 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(카탈로그만를 선택한 다음 OK(확인)를 선택합니다.
4. CommCell Home(CommCell 홈)을 선택한 다음 Job Controller(작업 컨트롤러)를 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 Home(CommCell 홈)을 선택하고 Control Panel(제어판)을 선택한 다음 Browse/Search/Recovery(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 Client Computers(클라이언트 컴퓨터)를 마우스 오른쪽 버튼으로 클릭하고 원하는 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.

Dell EMC NetWorker를 사용한 설정 테스트

Dell EMC NetWorker를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 스토리지 디바이스 구성, 테이

프에 데이터 쓰기, 테이프 아카이브, 테이프에서 데이터 복원 등의 방법을 포함하여 Tape Gateway로 작업하고 백업을 수행하기 위해 Dell EMC NetWorker를 구성하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다.

Dell EMC NetWorker 소프트웨어를 설치하고 사용하는 방법에 대한 자세한 내용은 NetWorker 설명서를 참조하세요.

호환되는 백업 애플리케이션에 대한 자세한 내용은 Tape Gateway에 지원되는 타사 백업 애플리케이션 단원을 참조하십시오.

주제

- VTL 디바이스와 함께 작동하도록 구성
- WORM 테이프를 Dell EMC NetWorker로 가져오기 허용
- Dell EMC NetWorker에서 데이터를 테이프로 백업
- Dell EMC NetWorker에 테이프 보관
- Dell EMC NetWorker에 보관한 테이프에서 데이터 복원

VTL 디바이스와 함께 작동하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 클라이언트에 연결한 후 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

Tape Gateway 디바이스는 자동으로 인식되지 않습니다. VTL 디바이스를 NetWorker 소프트웨어에 노출하여 이 소프트웨어가 디바이스를 찾도록 하려면 소프트웨어를 수동으로 구성해야 합니다. 다음에서는 사용자가 소프트웨어를 올바르게 설치했으며 Management Console에 익숙하다고 가정합니다. Management Console에 대한 자세한 내용은 Dell EMC NetWorker 관리 안내서의 NetWorker Management Console 인터페이스 섹션을 참조하세요.

VTL 디바이스용 Dell EMC NetWorker 소프트웨어를 구성하려면

1. Dell EMC NetWorker Management Console 애플리케이션을 시작하고 메뉴에서 Enterprise(엔터프라이즈)를 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 권한으로 명령 창(cmd.exe)을 열고 Dell EMC NetWorker 19.5와 함께 설치된 `jbconfig` 유틸리티를 실행합니다.
   a. 메뉴 프롬프트에서 해당 숫자를 입력하여 Configure an Autodetected SCSI Jukebox(자동 감지된 SCSI 주크박스 구성)를 선택합니다.
   b. 주크박스 디바이스의 이름을 입력하라는 메시지가 표시되면 이름을 입력합니다(예: `AWSVTL`).
   c. NetWorker 자동 정리를 켤지 묻는 메시지가 표시되면 no를 입력합니다.
   d. 자동 구성을 우회할지 묻는 메시지가 표시되면 no를 입력합니다.
   e. 다른 주크박스를 구성할지 묻는 메시지가 표시되면 no를 입력합니다.
7. 'jbconfig'가 완료되면 Networker GUI로 돌아가서 F5 키를 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.

WORM 테이프를 Dell EMC NetWorker로 가져오기 허용

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

가상 테이프는 한 번 쓰고 여러 번 읽는 WORM(Write Once Read Many) 테이프입니다. 그러나 Dell EMC NetWorker는 WORM 방식이 아닌 테이프를 기대합니다. Dell EMC NetWorker가 가상 테이프와 함께 작동하려면 테이프를 WORM 방식이 아닌 미디어 풀로 가져올 수 있게 활성화해야 합니다.

WORM 테이프를 WORM 방식이 아닌 미디어 풀로 가져올 수 있게 하려면

1. NetWorker 콘솔에서 Media(미디어)를 선택하고 localhost를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 Properties(속성)를 선택합니다.
2. NetWorker Sever Properties(NetWorker 서버 속성) 창에서 Configuration(구성) 탭을 선택합니다.
3. Worm tape handling(웜 테이프 처리) 섹션에서 WORM tapes only in WORM pools(WORM 풀의 WORM 테이프만) 확인란의 선택을 취소한 다음 OK(확인)를 선택합니다.

Dell EMC NetWorker에서 데이터를 테이프로 백업

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 가이드의 데이터 백업 섹션을 참조하십시오.
2. 테이프에 데이터를 씁니다. Dell EMC NetWorker Management Console 대신에 Dell EMC NetWorker 사용자 애플리케이션을 사용하여 데이터를 백업합니다. Dell EMC NetWorker 사용자 애플리케이션은 NetWorker 설치하는 과정 중에 설치됩니다.

> **Note**
>
> Dell EMC NetWorker 사용자 애플리케이션을 사용하여 백업을 수행하지만 EMC Management Console에서 백업 상태를 확인하고 작업을 복구합니다. 상태를 보려면 Devices(디바이스) 메뉴를 선택하고 Log(로그) 창에서 상태를 봅니다.

> **Note**
>
> 백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 일시 중단되고 Dell EMC Networker의 테이프 상태가 쓰기 보호됨으로 변경됩니다. 테이프를 아카이브하거나 테이프에서 데이터를 계속 읽을 수 있습니다. 다른 테이프에서 일시 중단된 백업 작업을 재개할 수 있습니다.

Dell EMC NetWorker에 테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 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 빼냅니다.

Dell EMC NetWorker를 사용하여 테이프를 보관하려면

1. NetWorker 관리 창의 Devices(디바이스) 탭에서 localhost 또는 EMC 서버를 선택한 다음 Libraries(라이브러리)를 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 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 보관을 완료하면 해당 테이프가 VTL에 표시되지 않습니다.

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

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 ARCHIVED인지 확인합니다.

Dell EMC NetWorker에 보관한 테이프에서 데이터 복원

보관 데이터를 복원하려면 다음과 같은 두 단계를 거쳐야 합니다.

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

다음 단계

불필요한 리소스 정리

IBM Data Protect를 사용하여 설정 테스트

IBM Data Protect를와 함께 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다 AWS Storage Gateway. (IBM Data Protect는 이전에 Tivoli Storage Manager라고 불렸습니다.)

이 주제에는 Tape Gateway용 IBM Data Protect 백업 소프트웨어를 구성하는 방법에 대한 기본 정보가 포함되어 있습니다. 또한 IBM Data Protect를 사용한 백업 및 복원 작업 수행에 대한 기본 정보도 포함되어 있습니다. IBM Data Protect 백업 소프트웨어를 관리하는 방법에 대한 자세한 내용은 IBM Data Protect 설명서를 참조하세요.

IBM Data Protect 백업 소프트웨어는 다음 운영 체제 AWS Storage Gateway 에서를 지원합니다.

- Microsoft Windows Server
- Red Hat Linux

Windows용 IBM Data Protect 지원 디바이스에 대한 자세한 내용은 IBM Data Protect(이전 Tivoli Storage Manager) AIX, HP-UX, Solaris 및 Windows용 지원 디바이스를 참조하세요.

Linux용 IBM Data Protect 지원 디바이스에 대한 자세한 내용은 Linux용 IBM Data Protect(이전 Tivoli Storage Manager) 지원 디바이스를 참조하세요.

주제

- IBM Data Protect 설정
- VTL 디바이스와 함께 작동하도록 IBM Data Protect 구성
- IBM Data Protect에서 테이프에 데이터 쓰기
- IBM Data Protect에 보관된 테이프에서 데이터 복원

IBM Data Protect 설정

VTL 디바이스를 클라이언트에 연결한 후 이를 인식하도록 IBM Data Protect 소프트웨어를 구성합니다. VTL 디바이스를 클라이언트에 연결하는 방법에 대한 자세한 내용은 VTL 디바이스 연결 섹션을 참조하세요.

IBM Data Protect를 설정하려면

1. IBM에서 IBM Data Protect 소프트웨어의 라이선스 사본을 가져옵니다.

2. 온프레미스 환경 또는 클라우드 내 Amazon EC2 인스턴스에 IBM Data Protect 소프트웨어를 설치합니다. 자세한 내용은 IBM Data Protect에 대한 IBM의 설치 및 업그레이드 설명서를 참조하세요.

   IBM Data Protect 소프트웨어 구성에 대한 자세한 내용은 IBM Data Protect 서버용 Tape Gateway 가상 테이프 라이브러리 구성을 AWS 참조하세요.

VTL 디바이스와 함께 작동하도록 IBM Data Protect 구성

다음으로 VTL 디바이스와 함께 작동하도록 IBM Data Protect를 구성합니다. Microsoft Windows Server 또는 Red Hat Linux에서 VTL 디바이스와 함께 작동하도록 IBM Data Protect를 구성할 수 있습니다.

Windows용 IBM Data Protect 구성

Windows에서 IBM Data Protect를 구성하는 방법에 대한 전체 지침은 Lenovo 웹 사이트에서 Tape Device Driver-W12 6266 for Windows 2012를 참조하세요. 다음은 프로세스에 관한 기본 설명서입니다.

Microsoft Windows용 IBM Data Protect를 구성하려면

1. 미디어 체인저의 올바른 드라이버 패키지를 다운로드합니다. 테이프 디바이스 드라이버의 경우 IBM Data Protect에는 Windows 2012용 버전 W12 6266이 필요합니다. 드라이버를 다운로드하는 방법을 보려면 Lenovo 웹 사이트에서 Windows 2012용 테이프 디바이스 드라이버-W12 6266을 참조하십시오.

   > **Note**
   >
   > 드라이버의 "비독점적" 세트를 설치해야 합니다.

2. 컴퓨터에서 컴퓨터 관리를 열고 미디어 체인저 장치를 확장한 후 미디어 체인저 유형이 IBM 3584 Tape Library인지 확인합니다.
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 IBM Data Protect에 나타나는지 확인합니다. 이렇게 하려면 `\Tivoli\TSM\server>tsmdlst.exe` 명령을 사용합니다.

Linux용 IBM Data Protect 구성

다음은 Linux에서 VTL 디바이스와 함께 작동하도록 IBM Data Protect를 구성하는 기본 설명서입니다.

Linux용 IBM Data Protect를 구성하려면

1. IBM 지원 웹 사이트의 IBM Fix Central로 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 Fix Central 다운로드 페이지의 지침에 따라 IBM Data Protect를 다운로드하고 구성합니다.
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.

IBM Data Protect에서 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. IBM Data Protect 구성에 대한 자세한 내용은 IBM Data Protect의 관리 작업 개요를 참조하세요.

> **Note**
>
> 백업 작업이 진행 중인 동안 어떤 이유로든 Tape Gateway가 다시 시작되면 백업 작업이 실패할 수 있습니다. 백업 작업이 실패하면 IBM Data Protect의 테이프 상태가 ReadOnly로 변경됩니다. 테이프가 충분히 활용되지 않은 경우 수동으로 테이프 상태를 다시 ReadWrite로 변경하고 동일한 테이프를 사용하여 백업 작업을 재개하거나 다시 제출할 수 있습니다. ReadWrite 상태의 다른 테이프를 사용할 수 있는 경우 IBM Data Protect는 다른 테이프에서 실패한 백업 작업을 계속할 수 있습니다.

IBM Data Protect에 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 섹션을 참조하세요.
2. IBM Data Protect 백업 소프트웨어를 사용하여 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 복구 시점을 생성하여 복원합니다. IBM Data Protect 구성에 대한 자세한 내용은 IBM Data Protect의 관리 작업 개요를 참조하세요.

다음 단계

불필요한 리소스 정리

OpenText Data Protector를 사용하여 설정 테스트

OpenText Data Protector를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 OpenText Data Protector 소프트웨어를 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다. OpenText Data Protector 소프트웨어 사용 방법에 대한 자세한 내용은 OpenText Data Protector 설명서를 참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 Tape Gateway에 지원되는 타사 백업 애플리케이션 단원을 참조하십시오.

주제

- VTL 디바이스와 함께 작동하도록 OpenText 데이터 보호기 구성
- 데이터 보호기와 함께 사용할 가상 테이프 준비
- 테이프를 미디어 풀로 로드
- 데이터를 테이프에 백업
- 테이프 보관
- 테이프에서 데이터 복원

VTL 디바이스와 함께 작동하도록 OpenText 데이터 보호기 구성

가상 테이프 라이브러리(VTL) 디바이스를 클라이언트에 연결한 후 디바이스를 인식하도록 OpenText Data Protector를 구성합니다. VTL 디바이스를 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

OpenText Data Protector 소프트웨어는 Tape Gateway 디바이스를 자동으로 인식하지 않습니다. 소프트웨어가 이 디바이스를 인식하도록 하려면 다음 설명과 같이 디바이스를 수동으로 추가한 후 VTL 디바이스를 검색해야 합니다.

VTL 디바이스를 추가하려면

1. OpenText Data Protector 기본 창의 왼쪽 상단에 있는 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. Device Type(디바이스 유형)에서 SCSI Library(SCSI 라이브러리)]를 선택하고 Nex(다음)를 선택합니다.
3. 그 다음 화면에서 아래 작업을 수행합니다.

   a. SCSI address of the library robotic(라이브러리 로봇 공학의 SCSI 주소)에서 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)
      - Automatically discover changed SCSI address(변경된 SCSI 주소 자동 검색)
      - SCSI Reserve/Release (robotic control)(SCSI 예약/릴리스(로봇 공학 컨트롤))

   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 디바이스가 사용하는 미디어의 표준 유형으로 LTO_Ultrium을 선택한 다음 Finish(마침)를 선택하여 설정을 완료합니다.

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

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 address of data drive(데이터 드라이브의 SCSI 주소)에서 추가할 테이프 드라이브를 선택하고 Automatically discover changed SCSI address(변경된 SCSI 주소 자동 검색)를 선택한 후 Next(다음)를 선택합니다.
4. 다음 화면에서 Advanced(고급)를 선택합니다. Advanced Options(고급 옵션) 팝업 화면이 나타납니다.

    a. Settings(설정) 탭에서 다음 옵션을 고려해야 합니다.

    - CRC Check(CRC 확인)(실수로 인한 데이터 변경 감지)
    - Detect dirty drive(더티 드라이브 감지) (백업하기 전에 드라이브가 깨끗한지 확인)
    - SCSI Reserve/Release(drive)(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. Media Type(미디어 유형)에서 LTO_Ultrium을 선택한 후 Next(다음)를 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 시점에서 Data Protector에서 가상 테이프 라이브러리 사용을 시작하도록 모든 것이 구성되어 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 Backup(백업)을 선택합니다.

2. 왼쪽 창에서 Backup(백업) 탐색 트리를 확장합니다.
3. Filesystem(파일 시스템)을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 Add Backup(백업 추가)을 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 아카이브하는 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 ARCHIVING으로 바뀝니다. 아카이브가 완료되면 테이프는 더 이상 VTL에 나열되지 않고 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 섹션을 참조하세요.
2. Data Protector를 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 Restore(복원)를 선택합니다.
2. 왼쪽 탐색 트리에서 복원하려는 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 Center DPM을 사용한 설정 테스트

Microsoft System Center Data Protection Manager(DPM)를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 DPM 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다.

DPM 사용 방법에 대한 자세한 내용은 Microsoft System Center 웹 사이트의 DPM 설명서를 참조하십시오. 호환되는 백업 애플리케이션에 대한 자세한 내용은 Tape Gateway에 지원되는 타사 백업 애플리케이션 단원을 참조하십시오.

주제

- VTL 디바이스 인식을 위한 DPM 구성
- 테이프를 DPM으로 가져오기
- DPM의 테이프에 데이터 쓰기
- DPM을 사용한 테이프 보관
- DPM에 보관한 테이프에서 데이터 복원

VTL 디바이스 인식을 위한 DPM 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 DPM이 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

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

1. VTL 디바이스용 디바이스 드라이버를 업데이트하여 DPM 서버에 노출합니다.

2. VTL 디바이스를 DPM 테이프 라이브러리에 수동으로 매핑합니다.

VTL 디바이스 드라이버를 업데이트하려면

- 디바이스 관리자에서 미디어 체인저용 드라이버를 업데이트합니다. 지침은 미디어 체인저의 디바이스 드라이버 업데이트 섹션을 참조하세요.

DPMDriveMappingTool을 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 생성을 참조하세요.
2. 테이프를 DPM 라이브러리로 가져옵니다. 이렇게 하는 방법에 대한 정보는 테이프를 DPM으로 가져오기 단원을 참조하십시오.
3. DPMLA 서비스가 실행 중인 경우, 명령 터미널을 열고 명령 프롬프트에 다음과 같이 입력하여 실행을 중지합니다.

   ```
   net stop DPMLA
   ```

4. DPM 서버에서 다음 파일을 찾습니다. `%ProgramFiles%\System Center\DPM\DPM\Config\DPMLA.xml`.

   > **Note**
   >
   > 디렉터리 경로는 System Center 또는 DPM 버전에 따라 변경될 수 있습니다.
   > 이 파일이 있으면 DPMDriveMappingTool이 이 파일에 덮어쓰기 합니다. 원본 파일을 보존하려면 백업 사본을 생성해야 합니다.

5. 명령 터미널을 열어 `%ProgramFiles%\System Center\DPM\DPM\Bin` 디렉터리로 변경한 후 다음 명령을 실행합니다.

   > **Note**
   >
   > 디렉터리 경로는 System Center 또는 DPM 버전에 따라 변경될 수 있습니다.

```
C:\Microsoft System Center\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.
```

테이프를 DPM으로 가져오기

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

테이프를 DPM 백업 애플리케이션 라이브러리로 가져오려면

1. DPM 서버에서 관리 콘솔을 열고 Rescan(다시 스캔)을 선택한 다음 Refresh(새로 고침)를 선택합니다. 관리 콘솔에 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.
> 테이프의 바코드를 표시되지 않으면 미디어 체인저 드라이버를 Sun/StorageTek Library로 변경해야 합니다. 자세한 내용은 Microsoft System Center DPM에서 테이프의 바코드 표시 단원을 참조하십시오.

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

DPM의 테이프에 데이터 쓰기

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. DPM 사용 방법에 대한 자세한 내용은 Microsoft System Center 웹 사이트의 DPM 설명서를 참조하십시오.

테이프의 기본 용량은 30GB입니다. 백업 데이터가 테이프 용량보다 클 경우에는 장치 I/O 오류가 발생합니다. 이때 테이프 크기를 넘어서는 위치에서 오류가 발생하면 Microsoft DPM이 테이프 끝을 나타내는 것으로 오류를 처리합니다. 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: 30101을 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.

DPM을 사용한 테이프 보관

테이프를 아카이브하면 Tape Gateway에서 해당 테이프를 DPM 테이프 라이브러리에서 오프라인 스토리지로 이동합니다. 백업 애플리케이션, 즉 DPM을 사용하여 슬롯에서 테이프를 제거하여 테이프 아카이브를 시작합니다.

DPM에 테이프를 아카이브하려면

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 아카이브하는 가상 테이프의 상태를 확인합니다.

   보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 표시됩니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 보관을 완료하면 해당 테이프가 VTL에 표시되지 않습니다.

DPM에 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 섹션을 참조하세요.
2. DPM 백업 애플리케이션을 사용하여 해당 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 복구 시점을 생성하여 복원합니다. 관련 지침은 DPM 웹 사이트의 Recovering Client Computer Data(클라이언트 컴퓨터 데이터 복구)를 참조하십시오.

다음 단계

불필요한 리소스 정리

NovaStor DataCenter를 사용한 설정 테스트

NovaStor DataCenter/Network를 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 NovaStor DataCenter/Network 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법에 대한 기본 설명서를 찾을 수 있습니다. NovaStor DataCenter/Network를 사용하는 방법에 대한 자세한 내용은 NovaStor DataCenter/Network 설명서를 참조하세요.

NovaStor DataCenter/Network 설정

가상 테이프 라이브러리(VTL) 디바이스를 Microsoft Windows 클라이언트에 연결한 후 NovaStor 소프트웨어가 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

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

NovaStor DataCenter/Network가 VTL 디바이스와 함께 작동하도록 구성

NovaStor DataCenter/Network와 함께 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 수립하여 문제를 방지할 수 있습니다. 해결 방법을 수립하는 방법에 대한 자세한 내용은 "외부 프로그램이 올바르게 종료되지 않았습니다" 오류 해결 단원을 참조하십시오.

NovaStor DataCenter/Network가 VTL 디바이스와 함께 작동하도록 구성하려면

1. NovaStor DataCenter/Network 관리 콘솔에서 Media Management(미디어 관리)를 선택한 후 Storage Management(스토리지 관리)를 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 correctly`라는 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**
   >
   > 이러한 오류가 발생하는 이유는 스토리지 드라이브 및 테이프 드라이브에 대한 AWS Storage Gateway 의 요소 할당 범위가 NovaStor DataCenter/Network가 허용하는 수를 초과하기 때문입니다.

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. 표시되는 Attach Library(라이브러리 연결) 대화 상자에서 LTO5 미디어 유형을 선택한 후 OK(확인)를 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 이러한 슬롯을 사용할 수 있습니다.

내보내기의 경우 NovaStor DataCenter/Network는 라이브러리에서 물리적으로 꺼낼 테이프를 알아야 합니다.

가져오기의 경우 NovaStor DataCenter/Network는 테이프 라이브러리에서 내보내는 테이프 미디어를 인식하고 데이터 슬롯 또는 내보내기 슬롯에서 이를 모두 가져옵니다. 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 NovaStor DataCenter/Network 설명서를 참조하십시오.

> **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 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 보관을 완료하면 해당 테이프가 VTL에 표시되지 않습니다.

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

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 ARCHIVED인지 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 섹션을 참조하세요.
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 NovaStor DataCenter/Network 설명서를 참조하십시오.

여러 백업 작업을 테이프 드라이브에 동시에 기록

NovaStor 소프트웨어에서 멀티플렉싱 기능을 사용하여 여러 작업을 테이프 드라이브에 동시에 기록할 수 있습니다. 이 기능은 미디어 풀에서 멀티플렉서를 사용할 수 있는 경우에 사용 가능합니다. 멀티플렉싱 사용 방법에 대한 자세한 내용은 NovaStor DataCenter/Network 설명서를 참조하십시오.

"외부 프로그램이 올바르게 종료되지 않았습니다" 오류 해결

NovaStor DataCenter/Network와 함께 작동하도록 VTL 디바이스를 구성할 때 라는 오류 메시지가 표시될 수 있습니다`External Program did not exit correctly`. 이러한 오류가 발생하는 이유는 스토리지 드라이브 및 테이프 드라이브에 대한 Storage Gateway의 요소 할당 범위가 NovaStor DataCenter/Network에서 허용하는 수를 초과하기 때문입니다.

Storage Gateway는 스토리지 및 가져오기/내보내기 슬롯 3,200개를 반환하는데, 이는 NovaStor DataCenter/Network에서 허용하는 한도인 2,400개보다 많습니다. 이 문제를 해결하려면 스토리지 및 가져오기/내보내기 슬롯 수를 제한하고 요소 할당 범위를 미리 구성하도록 NovaStor 소프트웨어를 활성화하는 구성 파일을 추가합니다.

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

1. NovaStor 소프트웨어를 설치한 컴퓨터의 테이프 폴더로 이동합니다.
2. 테이프 폴더에서 텍스트 파일을 만들고 이름을 `hijacc.ini`로 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 테이프를 가져오기/내보내기 슬롯에서 라이브러리로 이동합니다. 예제 라이브러리 이름을 배포의 라이브러리 이름으로 바꿉니다.

   ```
   C:\Program Files\NovaStor\DataCenter\Hitback\tape\ophijacc.exe -c VTL-ec2amaz-uko8jfj-ec2amaz-uko8jfj.lcfg
   ```
6. 백업 서버에 라이브러리를 연결합니다.
7. NovaStor 소프트웨어에서 가져오기/내보내기 슬롯의 모든 테이프를 라이브러리로 가져옵니다.

Quest NetVault Backup을 사용하여 설정 테스트

Quest(이전 Dell) NetVault Backup을 사용하여 데이터를 가상 테이프에 백업하고, 테이프를 아카이브하고, 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다.

이 주제에서는 Tape Gateway용 Quest NetVault Backup 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다.

Quest NetVault Backup 애플리케이션 사용 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

- Quest NetVault Backup이 VTL 디바이스와 함께 작동하도록 구성
- Quest NetVault Backup 소프트웨어에서 데이터를 테이프로 백업
- Quest NetVault Backup 소프트웨어를 사용하여 테이프 보관
- QUest NetVault Backup에 보관한 테이프에서 데이터 복원

Quest NetVault Backup이 VTL 디바이스와 함께 작동하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 Quest NetVault Backup이 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

기본적으로 Quest NetVault Backup 애플리케이션은 Tape Gateway 디바이스를 자동으로 인식하지 못합니다. 디바이스를 수동으로 추가하여 Quest NetVault Backup 애플리케이션에 노출한 후 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 10개의 베이를 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 Backup 소프트웨어에서 데이터를 테이프로 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 안내서를 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 Backup 소프트웨어를 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 Configuration] 탭에서 미디어 체인저를 선택한 후 펼쳐 테이프를 확인합니다.
2. Slots(슬롯)의 설정 아이콘을 선택하여 미디어 체인저용 Slots Browser(슬롯 브라우저)를 엽니다.
3. 슬롯에서 아카이브할 테이프를 찾아 선택한 후 Export(내보내기)를 선택합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 보관을 완료하면 해당 테이프가 VTL에 표시되지 않습니다.

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

Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 ARCHIVED인지 확인합니다.

QUest NetVault Backup에 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 섹션을 참조하세요.
2. QUest NetVault Backup 애플리케이션을 사용하여 해당 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 폴더 복원 파일을 생성합니다. 복원 작업 생성에 대한 지침은 Quest NetVault Backup - 관리 안내서를 참조하세요.

다음 단계

불필요한 리소스 정리

Veeam Backup and Replication을 사용한 설정 테스트

Veeam Backup & Replication을 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 Backup & Replication 설명서를 참조하세요. 호환되는 백업 애플리케이션에 대한 자세한 내용은 Tape Gateway에 지원되는 타사 백업 애플리케이션 단원을 참조하십시오.

주제

- Veeam이 VTL 디바이스와 함께 작동하도록 구성
- 테이프를 Veeam으로 가져오기
- Veeam에서 데이터를 테이프로 백업
- Veeam을 사용한 테이프 보관
- Veeam에 보관한 테이프에서 데이터 복원

Veeam이 VTL 디바이스와 함께 작동하도록 구성

가상 테이프 라이브러리(VTL) 디바이스를 Windows 클라이언트에 연결한 후 Veeam Backup & Replication이 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

VTL 디바이스 드라이버 업데이트

소프트웨어가 Tape Gateway 디바이스와 함께 작동하도록 구성하려면 VTL 디바이스의 드라이버를 업데이트하여 Veeam 소프트웨어에 노출한 후 VTL 디바이스를 검색합니다. 디바이스 관리자에서 미디어 체인저용 드라이버를 업데이트합니다. 지침은 미디어 체인저의 디바이스 드라이버 업데이트 섹션을 참조하세요.

VTL 디바이스 검색

미디어 체인저를 알 수 없다면 Windows 드라이버 대신에 기본 SCSI 명령을 사용하여 테이프 라이브러리를 검색해야 합니다. 자세한 지침은 테이프 라이브러리를 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 지침에 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 테이프에 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 시작하기를 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 아카이브하는 가상 테이프의 상태를 확인합니다.

보관 프로세스를 완료하는 데 다소 시간이 걸릴 수 있습니다. 테이프의 초기 상태는 IN TRANSIT TO VTS로 나타납니다. 아카이브가 시작되면 상태가 ARCHIVING으로 바뀝니다. 아카이브가 완료되면 테이프는 더 이상 VTL에 나열되지 않고 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 섹션을 참조하세요.
2. Veeam 소프트웨어를 사용하여 해당 데이터를 복원합니다. 물리적 테이프에서 데이터를 복원할 때와 마찬가지로 폴더 복원 파일을 생성합니다. 관련 지침은 Veeam 도움말 센터에서 테이프에서 파일 복원을 참조하세요.

다음 단계

불필요한 리소스 정리

Veritas Backup Exec을 사용한 설정 테스트

Veritas Backup Exec을 사용하여 데이터를 가상 테이프에 백업하고 이 테이프를 아카이브하며 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Backup Exec을 사용하여 백업 및 복원 작업을 수행하는 데 필요한 기본 설명서를 찾을 수 있습니다.

보안 백업, 소프트웨어 및 하드웨어 호환성 목록, 관리자 안내서를 생성하는 방법을 포함하여 Backup Exec을 사용하는 방법에 대한 자세한 내용은 Veritas 지원 웹 사이트를 참조하세요.

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 Backup Exec 스토리지가 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

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 Exec은 VTL 디바이스인 미디어 체인저와 테이프 드라이브를 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 섹션을 참조하세요.

4. 재시작이 완료되면 Backup Exec Service Manager를 종료합니다.

Backup Exec에 있는 테이프 가져오기

이제 게이트웨이에서 슬롯으로 테이프를 가져올 준비가 되었습니다.

1. Storage(스토리지) 탭을 선택한 다음 Robotic library(로봇 공학 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 단원을 참조하십시오.

2. Slots(슬롯) 아이콘을 선택하여 모든 슬롯을 표시합니다.

> **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.

> **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 Gateway에서 해당 테이프를 게이트웨이의 가상 테이프 라이브러리(VTL)에서 오프라인 스토리지로 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 테이프가 Tape Gateway의 VTL에 IN TRANSIT TO VTS 상태로 나열됩니다. 업로드가 완료되고 아카이브 프로세스가 시작되면 상태가 ARCHIVING으로 변경됩니다. 데이터 아카이브가 완료되면 내보낸 테이프는 더 이상 VTL에 나열되지 않고 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브됩니다.
3. 해당 게이트웨이를 선택한 다음 VTL Tape Cartridges(VTL 테이프 카트리지)를 선택하고 가상 테이프 목록이 게이트웨이에 더 이상 표시되지 않는지 확인합니다.
4. Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 테이프가 ARCHIVED 상태인지 확인합니다.

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 섹션을 참조하세요.
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

Veritas NetBackup을 사용한 설정 테스트

Veritas NetBackup을 사용하여 데이터를 가상 테이프에 백업하고 이 테이프를 아카이브하며 가상 테이프 라이브러리(VTL) 디바이스를 관리할 수 있습니다. 이 주제에서는 Tape Gateway용 NetBackup 백업 애플리케이션을 구성하고 백업 및 복원 작업을 수행하는 방법을 설명하는 기본 설명서를 확인할 수 있습니다.

NetBackup 사용 방법에 대한 자세한 내용은 Veritas 웹 사이트의 Veritas Services and Operations Readiness Tools(SORT) 페이지를 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 Veritas NetBackup 스토리지가 디바이스를 인식할 수 있도록 구성합니다. VTL 디바이스를 Windows 클라이언트에 연결하는 방법에 대한 정보는 VTL 디바이스 연결 단원을 참조하십시오.

NetBackup에서 Tape Gateway의 스토리지 장치를 사용하도록 구성하려면

1. 관리자로 NetBackup 관리 콘솔을 엽니다.
2. Configure Storage Devices(스토리지 디바이스 구성)를 선택하여 Device Configuration(디바이스 구성) 마법사를 엽니다.
3. 다음을 선택합니다. NetBackup 애플리케이션은 컴퓨터를 디바이스 호스트로 감지합니다.
4. Device Hosts(디바이스 호스트) 열에서 해당 컴퓨터를 선택한 후 Next(다음)를 선택합니다. NetBackup 애플리케이션은 해당 컴퓨터의 장치를 스캔하여 모든 디바이스를 찾아냅니다.
5. Scanning Hosts(호스트 스캔 중) 페이지에서 Next(다음)를 선택한 후 다시 Next(다음)를 선택합니다. NetBackup 애플리케이션은 컴퓨터에서 모든 테이프 드라이브(10개)와 미디어 체인저를 찾아냅니다.
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 애플리케이션이 디바이스 구성을 업데이트합니다.
9. 업데이트 완료 후 Next(다음)를 선택하여 NetBackup 애플리케이션에서 디바이스를 사용할 수 있도록 합니다.
10. Finished!(완료됨!) 창에서 Finish(마침)를 선택합니다.

NetBackup 애플리케이션에서 디바이스를 확인하려면

1. NetBackup 관리 콘솔에서 Media and Device Management(미디어 및 디바이스 관리) 노드를 펼친 후 Devices(디바이스) 노드를 펼칩니다. Drives(드라이브)를 선택하여 모든 테이프 드라이브를 표시합니다.
2. Devices(디바이스) 노드에서 Robots(로봇)를 선택하여 모든 미디어 체인저를 표시합니다. NetBackup 애플리케이션에서는 미디어 체인저를 로봇이라고 합니다.
3. All Robots(모든 로봇) 창에서 TLD(0)(사용자의 로봇)를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 Inventory Robot(인벤토리 로봇)을 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.

   이 프로세스는 NetBackup Enterprise Media Management(EMM) 데이터베이스에 미디어 체인저 및 가상 테이프의 목록을 만듭니다. NetBackup은 미디어 정보, 디바이스 구성 및 테이프 상태를 EMM에 저장합니다.
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. Media(미디어) 노드에서 Robots(로봇) 노드를 펼친 후 TLD(0)를 선택하여 로봇(미디어 체인저)에서 사용할 수 있는 가상 테이프를 모두 표시합니다.

> **Note**
>
> NetBackup 애플리케이션에 다른 디바이스를 연결한 경우, 로봇이 여러 개일 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 요금을 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. Robots(로봇) 노드를 펼치고 TLD(0) 로봇을 선택하여 이 로봇이 인식하고 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) 열에 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 수락한 후 Next(다음)를 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 해보겠습니다.

수동으로 백업하려면

1. NetBackup 콘솔의 탐색 창에서 NetBackup Management(NetBackup 관리) 노드를 펼칩니다.
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 NetBackup이 파일 데이터를 작성한 가상 테이프의 바코드를 찾으려면 다음 절차에 설명한 것과 같이 Job Details(작업 세부 정보) 창을 살펴봅니다. 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 `media id 87A222`가 표시될 수 있습니다. 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 보관할 때 Tape Gateway는 해당 테이프를 게이트웨이의 가상 테이프 라이브러리(VTL)에서 오프라인 스토리지를 제공하는 아카이브로 옮깁니다. 백업 애플리케이션으로 테이프를 배출하여 테이프 보관을 시작합니다.

가상 테이프를 아카이브하려면

1. NetBackup 관리 콘솔에서 Media and Device Management(미디어 및 디바이스 관리) 노드를 펼친 후 Media(미디어) 노드를 펼칩니다.
2. Robots(로봇)를 펼친 후 TLD(0)를 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 VTL에서 아카이브하는 테이프의 상태를 확인합니다. 데이터를 AWS에 업로드하는 데 다소 시간이 걸릴 수 있습니다. 그 동안에 배출된 테이프는 IN TRANSIT TO VTS 상태로 게이트웨이의 VTL에 나열됩니다. 아카이브가 시작되면 ARCHIVING 상태가 됩니다. 데이터 업로드가 완료되면 배출된 테이프가 VTL에 더 이상 표시되지 않고, GS3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에 아카이브됩니다.
8. 가상 테이프가 게이트웨이에 표시되지 않는지 확인하려면 해당 게이트웨이를 선택한 후 VTL Tape Cartridges(VTL 테이프 카트리지)를 선택합니다.
9. Storage Gateway 콘솔의 탐색 창에서 테이프를 선택합니다. 아카이브된 테이프의 상태가 ARCHIVED인지 확인합니다.

테이프에서 데이터 복원

보관 데이터를 복원하려면 두 단계를 거쳐야 합니다.

보관 테이프에서 데이터를 복원하려면

1. 아카이브된 테이프를 Tape Gateway로 가져옵니다. 지침은 보관한 테이프 가져오기 섹션을 참조하세요.
2. Veritas NetBackup 애플리케이션과 함께 설치된 백업, 보관 및 복원 소프트웨어를 사용합니다. 이 프로세스는 물리적 테이프에서 데이터를 복원하는 절차와 동일합니다. 지침은 Veritas 웹 사이트에서 Veritas Services and Operations Readiness Tools(SORT)를 참조하십시오.

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 일부 Tape Gateway 유지 관리 작업을에서 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 볼륨 추가 및 제거와 같은 특정 유지 관리 작업을 Amazon EC2 콘솔에서 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 퍼블릭 인터넷을 통해 통신하지 않고 AWS 스토리지 서비스로 데이터를 전송할 수 있습니다. Amazon VPC 서비스를 사용하면 사용자 지정 Virtual Private Cloud(VPC)에서 프라이빗 네트워크 인터페이스 엔드포인트를 포함한 AWS 리소스를 시작할 수 있습니다. VPC를 통해 IP 주소 범위, 서브넷, 라우팅 테이블, 네트워크 게이트웨이 등의 네트워크 설정을 제어할 수 있습니다. VPC에 대한 자세한 내용은 Amazon VPC 사용 설명서에서 Amazon VPC란 무엇인가요?를 참조하세요.

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

> **Note**
>
> Storage Gateway용 VPC 엔드포인트를 생성한 리전과 동일한 리전에서 게이트웨이를 활성화해야 합니다.

주제

- Storage Gateway용 VPC 엔드포인트 생성

Storage Gateway용 VPC 엔드포인트 생성

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

Storage Gateway용 VPC 엔드포인트를 생성하려면

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

9. 엔드포인트가 생성되면 엔드포인트를 선택한 다음 새 VPC 엔드포인트를 선택합니다.
10. 선택한 스토리지 게이트웨이 엔드포인트의 세부 정보 탭의 DNS 이름에서 가용 영역을 지정하지 않은 첫 번째 DNS 이름을 사용합니다. DNS 이름은 `vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com` 과 비슷합니다.

VPC 엔드포인트가 있으므로 게이트웨이를 생성할 수 있습니다. 자세한 내용은 게이트웨이 생성을 참조하세요.

Tape Gateway 관리

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

다음은 Tape Gateway 리소스를 관리하는 방법에 대한 정보를 제공합니다.

주제

- 기본 게이트웨이 정보 편집 - Storage Gateway 콘솔을 사용하여 게이트웨이 이름, 시간대, CloudWatch 로그 그룹 등 기존 게이트웨이의 기본 정보를 편집하는 방법에 대해 알아봅니다.
- 자동 테이프 생성 관리 - 지정한 최소 사용 가능 테이프 수를 유지하기 위해 새 가상 테이프를 자동으로 생성하도록 Tape Gateway를 구성하는 방법에 대해 알아봅니다.
- 가상 테이프 보관 - 새 테이프를 생성할 때 테이프 아카이브를 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive 스토리지 클래스로 구성하는 방법에 대해 알아봅니다.
- S3 Glacier Deep Archive 스토리지 클래스로 테이프 이동 - 매우 저렴한 비용으로 장기간 데이터를 보관하고 디지털 보존을 위해 테이프를 S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 이동하는 방법에 대해 알아봅니다.
- 보관한 테이프 가져오기 - 먼저 테이프를 Tape Gateway로 가져와 아카이브된 가상 테이프에 저장된 데이터에 액세스하는 방법에 대해 알아봅니다.
- 테이프 사용량 통계 보기 - Storage Gateway 콘솔을 사용하여 테이프에 저장된 데이터의 양을 확인하는 방법에 대해 알아봅니다.
- Tape Gateway에서 가상 테이프 삭제 - Storage Gateway 콘솔을 사용하여 Tape Gateway에서 가상 테이프를 삭제하는 방법에 대해 알아봅니다.
- 사용자 지정 테이프 풀 삭제 - Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 삭제하는 방법에 대해 알아봅니다.
- Tape Gateway 비활성화 - 게이트웨이에 장애가 발생하여 장애가 발생한 게이트웨이에서 다른 게이트웨이로 테이프를 복구하려는 경우 Tape Gateway를 비활성화하는 방법에 대해 알아봅니다.
- 테이프 상태 이해 - 테이프가 정상적으로 작동하는지 또는 사용자의 조치가 필요할 수 있는 문제가 있는지 판단하는 데 도움이 되도록 Storage Gateway가 보고하는 다양한 테이프 상태 값에 대해 알아봅니다.
- 데이터를 새 게이트웨이 인스턴스로 이동 - 데이터 및 성능 요구 사항이 증가하거나 게이트웨이를 마이그레이션하라는 AWS 알림을 받는 경우 게이트웨이 간에 데이터를 이동하는 방법에 대해 알아봅니다.

기본 게이트웨이 정보 편집

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

기존 게이트웨이의 기본 정보를 편집하려면

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

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

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

자동 테이프 생성 관리

Tape Gateway는 사용자가 구성한 최소 사용 가능 테이프 수를 유지하기 위해 새 가상 테이프를 자동으로 생성합니다. 그러면 백업 애플리케이션에서 이러한 새 테이프를 가져올 수 있으므로 백업 작업이

중단 없이 실행될 수 있습니다. 자동 테이프 생성은 새로운 가상 테이프를 생성하기 위한 수동 프로세스 외에 사용자 지정 스크립팅도 필요하지 않습니다.

자동 테이프 생성 정책을 삭제하려면

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

   테이프를 S3 Glacier Flexible Retrieva에 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. 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 테이프를 생성할 때 가상 테이프의 상태가 처음에는 생성 중으로 표시됩니다. 테이프 생성이 완료되면 상태가 AVAILABLE로 변경됩니다. 자세한 내용은 테이프 상태 이해 단원을 참조하십시오.

   자동 테이프 생성 활성화에 대한 자세한 내용은 자동으로 테이프 생성을 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 클래스를 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 클래스를 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 테스트를 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 클래스를 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 Retrieva로 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 게이트웨이당 하나의 가상 테이프 라이브러리(VTL)를 제공합니다.

에 Tape Gateway가 두 개 이상 있는 경우 하나의 게이트웨이로만 테이프를 검색할 AWS 리전수 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 쉘프 탭에서 검색할 가상 테이프를 선택하고 테이프 검색을 선택합니다.

   > **Note**
   >
   > 가져오려는 가상 테이프의 상태는 ARCHIVED여야 합니다.

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

테이프의 상태가 ARCHIVED에서 RETRIEVING으로 변합니다. 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. 데이터를 모두 옮기면 아카이브에 있는 가상 테이프의 상태가 RETRIEVED로 변합니다.

> **Note**
>
> 가져온 가상 테이프는 읽기 전용입니다.

테이프 사용량 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 테이프가 RETRIEVED 상태인 경우, 테이프를 삭제하기 전에 먼저 백업 애플리케이션을 사용하여 테이프를 배출해야 합니다. Symantec NetBackup 소프트웨어를 사용하여 테이프를 배출하는 방법에 대한 지침은 테이프 아카이브를 참조하세요. 테이프를 배출하면 테이프 상태가 다시 ARCHIVED로 변합니다. 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 작업을 수행하려면 Storage Gateway API 참조에서 DeleteTapePool을 참조하세요.

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 생성 관리를 참조하세요.

Storage Gateway 콘솔을 사용하여 사용자 지정 테이프 풀을 삭제하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 상태는 테이프가 정상적으로 작동하고 있으며 사용자 측에서 조치가 필요하지 않음을 나타냅니다. 경우에 따라 상태는 사용자 측에서 조치가 필요할 수 있는 테이프 관련 문제를 나타냅니다. 다음 정보를 찾아 조치를 취해야 하는 시점을 결정하는데 도움을 받을 수 있습니다.

주제

- VTL에서 테이프 상태 정보 파악
- 아카이브의 테이프 상태 확인

VTL에서 테이프 상태 정보 파악

테이프의 상태는 테이프에(서) 읽거나 쓸 수 있도록 AVAILABLE 상태이어야 합니다. 다음 표에는 가능한 상태 값과 그에 대한 설명이 나와 있습니다.

Status	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
IN TRANSIT TO VTS	가상 테이프를 배출하여 아카이브에 업로드하고 있습니다. 이때 Tape Gateway는 데이터를에 업로드합니다 AWS. 업로드 중인 데이터의 양이 작은 경우 이 상태가 나타나지 않을 수 있습니다. 업로드를 완료하면 상태가 ARCHIVING으로 바뀝니다.	Amazon S3
ARCHIVING	Tape Gateway를 통해 가상 테이프를 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 지원하는 아카이브로 이동하는 중입니다. 이 프로세스는에 대한 데이터 업로드 AWS 가 완료된 후 발생합니다.	Amazon S3에서 S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive로 데이터를 이동하는 중입니다.

Status	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. **Note** 가상 테이프는 Tape Gateway로만 가져올 수 있습니다.	S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive에서 Amazon S3로 데이터를 이동하는 중입니다.
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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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.

Status	설명
ARCHIVED	가상 테이프를 배출하여 아카이브에 업로드하였습니다.
RETRIEVING	아카이브에서 가상 테이프를 가져오고 있습니다. **Note** 가상 테이프는 Tape Gateway로만 가져올 수 있습니다.
RETRIEVED	아카이브에서 가상 테이프를 가져왔습니다. 가져온 테이프는 읽기 전용입니다.

테이프 및 VTL 다비이스 사용 방법에 대한 자세한 내용은 가상 테이프 라이브러리에서 테이프 관리 단원을 참조하십시오.

데이터를 새 게이트웨이 인스턴스로 이동

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

- 데이터를 더 나은 호스트 플랫폼이나 최신 Amazon EC2 인스턴스로 이동합니다.
- 서버의 기본 하드웨어를 새로 고침합니다.

Important

데이터는 동일한 게이트웨이 유형 간에만 이동할 수 있습니다.
다음 마이그레이션 지침은 버전 2.x를 실행하는 게이트웨이 어플라이언스에만 사용할 수 있습니다. 하위 버전을 실행하는 게이트웨이 어플라이언스를 마이그레이션하는 데 사용할 수 없습니다.

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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 중지에 대한 자세한 내용은 Tape Gateway 시작 및 중지 섹션을 참조하세요.

5. 새 Tape Gateway를 생성합니다. 자세한 지침은 게이트웨이 생성을 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 생성을 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 클래스를 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 클래스를 참조하세요.

테이프를 S3 Glacier Flexible Retrieva에 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.

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 `ARCHIVED`여야 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 단원에서는 Amazon CloudWatch를 사용하여 게이트웨이와 관련된 리소스 모니터링하는 것을 포함하여 Storage Gateway를 모니터링하는 방법에 대해 설명합니다. 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 요금 없이 CloudWatch 지표를 제공합니다. Storage Gateway 지표는 2주 동안 기록됩니다. 이 지표를 사용하여 기록 정보에 액세스하고 게이트웨이와 볼륨이 어떻게 실행되고 있는지 더 잘 파악할 수 있습니다. 또한 Storage Gateway는 고해상도 경보를 제외한 CloudWatch 경보를 추가 비용 없이 제공합니다. CloudWatch 요금에 대한 자세한 내용은 Amazon CloudWatch 요금을 참조하세요. CloudWatch에 대한 자세한 정보는 Amazon CloudWatch 사용 설명서를 참조하세요.

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 대한 권장 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 클라우드에 전송한 총 바이트 수입니다. 이 지표는 게이트웨이에 있는 모든 볼륨의 활동을 포함합니다.

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

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

지표	설명
AvailabilityNotifications	게이트웨이에 의해 생성된 가용성 관련 상태 알림 수입니다. 이 지표를 Sum 통계에 사용하여 게이트웨이에 가용성 관련 이벤트가 발생하는지 여부를 확인할 수 있습니다. 이벤트에 대한 자세한 내용은 구성된 CloudWatch 로그 그룹을 확인하세요. 단위: 숫자
CacheHitPercent	캐시로부터 읽은 애플리케이션 읽기 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 퍼센트
CachePercentDirty	지속되지 않은 게이트웨이 캐시의 전체 백분율입니다 AWS. 보고 기간 종료 시점에서 샘플이 채취됩니다.

지표	설명	
	Sum 통계와 함께 이 지표를 사용합니다. 이상적으로는 이 지표가 낮게 유지되어야 합니다. 단위: 퍼센트	
CacheUsed	게이트웨이의 캐시 스토리지에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트	
IoWaitPercent	게이트웨이가 로컬 디스크의 응답을 대기하고 있는 시간의 백분율입니다. 단위: 퍼센트	
MemTotalBytes	게이트웨이 VM에 프로비저닝된 RAM의 양(바이트)입니다. 단위: 바이트	
MemUsedBytes	게이트웨이 VM에서 현재 사용 중인 RAM의 양(바이트)입니다. 단위: 바이트	

지표	설명	
QueuedWrites	일반적으로이 값은 쓰기를 기다리는 로컬 저장 바이트 수를 나타내지 AWS만 게이트웨이가 다시 시작될 때마다 발생하는 "부트스트래핑" 중에 로컬 데이터와 클라우드 데이터 간에 발생하는 동기화 프로세스도 반영합니다. 단위: 바이트	
TotalCacheSize	캐시의 총 크기(바이트)입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트	
UploadBufferPercentUsed	게이트웨이의 업로드 버퍼 사용 백분율입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 퍼센트	
UploadBufferUsed	게이트웨이의 업로드 버퍼에서 사용 중인 총 바이트 수입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 단위: 바이트	
UserCpuPercent	모든 코어 간에 평균된, 게이트웨이 처리에 소비된 CPU 시간의 백분율입니다. 단위: 퍼센트	

Storage Gateway 지표의 차원

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

차원	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 측정을 참조하세요.

업로드 버퍼 모니터링

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

캐시 볼륨 및 Tape Gateway 아키텍처와 동일한 방식으로 업로드 버퍼를 모니터링합니다. 자세한 내용은 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 `Average`를 사용하여 일정 기간 동안의 스토리지 사용량을 분석합니다.

사용되는 업로드 버퍼의 백분율을 측정하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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 절차에 따라 CloudWatch 콘솔을 사용하여 경보를 생성할 수 있습니다. 경보 및 임계값에 대해 자세히 알아보려면 Amazon CloudWatch 사용 설명서에서 CloudWatch 경보 생성을 참조하세요.

게이트웨이의 업로드 버퍼에 대한 경보 상한값을 설정하려면

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
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 후 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 생성한다는 것은 Amazon SNS 주제를 설정한다는 의미입니다. 자세한 정보는 Amazon CloudWatch 사용 설명서에서 Amazon SNS 설정을 참조하세요.

c. 주제에 주제에 대한 설명 이름을 입력합니다.

d. 작업 추가를 선택합니다.

e. 계속을 선택합니다.

6. 경보 설정을 검토한 후 경보를 생성합니다.

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

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

7. 경보 주제에 대한 구독을 확인합니다.

a. 주제를 생성할 때 지정한 이메일 주소로 보낸 Amazon SNS 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 `Average`를 사용하여 일정 기간 동안의 캐시 사용량을 분석합니다. `TotalCacheSize` 지표는 캐시를 게이트웨이에 추가할 때만 변합니다.
캐시에서 제공되는 읽기 요청의 백분율	`CacheHitPercent` 통계와 함께 `Average` 지표를 사용합니다. 대개의 경우 `CacheHitPercent` 를 높은 수준으로 유지하기를 바랍니다.
더티 캐시의 백분율, 즉에 업로드되지 않은 콘텐츠 포함 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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. StorageGateway: 볼륨 지표 차원을 선택한 후 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 지표와 표현식을 기반으로 게이트웨이에 대한 정보를 모니터링합니다. Storage Gateway 콘솔에서 게이트웨이에 대한 CloudWatch 경보를 추가하고 상태를 확인할 수 있습니다. Tape Gateway를 모니터링하는 데 사용되는 지표에 대한 자세한 내용은 게이트웨이 지표 이해 및 가상 테이프 지표 이해를 참조하세요. 각 경보마다 ALARM 상태 시작 조건을 지정합니다. ALARM 상태에서는 Storage Gateway 콘솔의 경보 상태 표시등이 빨간색으로 바뀌므로 상태를 사전 예방적으로 쉽게 모니터링할 수 있습니다. 지속적인 상태 변화에 따라 자동으로 작업을 호출하도록 경보를 구성할 수 있습니다. CloudWatch 경보에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서에서 Amazon CloudWatch 경보 사용을 참조하세요.

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

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

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

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

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

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

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.
없음	게이트웨이에 대한 경보가 생성되지 않습니다. 새 경보를 생성하려면 게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성 단원을 참조하십시오.
Unavailable	경보의 상태를 알 수 없습니다. 모니터링 탭에서 오류 정보를 보려면 사용할 수 없음을 선택합니다.

게이트웨이에 대한 권장 CloudWatch 경보 생성

Storage Gateway 콘솔을 사용하여 새 게이트웨이를 생성할 때 초기 설정 프로세스의 일부로 모든 권장 CloudWatch 경보를 자동으로 생성하도록 선택할 수 있습니다. 자세한 내용은 Tape Gateway 구성을 참조하세요. 기존 게이트웨이에 대해 권장 CloudWatch 경보를 추가하거나 업데이트하려면 다음 절차를 수행합니다.

기존 게이트웨이에 대해 권장 CloudWatch 경보를 추가하거나 업데이트하려면

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

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

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home/)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 권장 CloudWatch 경보를 생성할 게이트웨이를 선택합니다.
3. 게이트웨이 세부 정보 페이지에서 모니터링 탭을 선택합니다.
4. 경보에서 권장 경보 생성을 선택합니다. 권장 경보는 자동으로 생성됩니다.

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

게이트웨이에 대한 사용자 지정 CloudWatch 경보 생성

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

Storage Gateway 콘솔에서 CloudWatch 경보를 생성하려면

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

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

정적 임계값 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 정적 임계값을 기반으로 CloudWatch 경보 생성을 참조하세요.

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

  이상 탐지 경보를 생성하려면 Amazon CloudWatch 사용 설명서에서 이상 탐지를 기반으로 CloudWatch 경보 생성을 참조하세요.
- 지표 수학 표현식 경보: 수학 표현식에 사용된 하나 이상의 지표에 기반한 경보입니다. 표현식, 임계값 및 평가 기간을 지정합니다.

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

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

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

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

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

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

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

Tape Gateway 모니터링

이 단원의 이 주제에서는 Tape Gateway 모니터링 방법에 대한 절차 및 개념 정보에 대해 설명합니다. Tape Gateway와 연결된 가상 테이프, 캐시 스토리지 및 업로드 버퍼를 모니터링할 수 있습니다. AWS Management Console 를 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 실시간으로 로그 정보 처리를 자동화할 수 있습니다.

Storage Gateway는 추가 요금 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. CloudWatch에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서를 참조하세요.

데이터 처리량, 데이터 지연 시간, 초당 작업 수는 Tape Gateway에서 스토리지 애플리케이션의 성능을 파악하는 데 사용할 수 있는 지표입니다. 정확한 집계 통계를 사용하는 경우 이러한 값은 제공되는 Storage Gateway 지표를 사용하여 측정할 수 있습니다.

주제

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

CloudWatch 로그 그룹을 사용하여 Tape Gateway 상태 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 실시간으로 로그 정보 처리를 자동화할 수 있습니다. 자세한 내용은 Amazon CloudWatch 사용 설명서에서 구독을 통한 로그 데이터 실시간 처리를 참조하세요.

예를 들어, VMware HA가 활성화된 클러스터에 게이트웨이가 배포되어 있고 오류를 파악해야 하는 경우, 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 구성 섹션을 참조하세요. CloudWatch 로그 그룹에 대한 일반적인 정보는 Amazon CloudWatch 사용 설명서에서 로그 그룹 및 로그 스트림 작업을 참조하세요.

문제를 해결하고 이 오류 유형을 해결하는 방법에 대한 자세한 내용은 가상 테이프 관련 문제 해결 단원을 참조하십시오.

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

File Gateway와 함께 작동하도록 CloudWatch 로그 그룹을 구성하려면

1. 에 로그인 AWS Management Console 하고 https://console.aws.amazon.com/storagegateway/home Storage Gateway 콘솔을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 CloudWatch 로그 그룹을 구성할 게이트웨이를 선택합니다.
3. 작업에서 게이트웨이 정보 편집을 선택하거나, 세부 정보 탭의 상태 로그 및 활성화되지 않음에서 로그 그룹 구성을 선택하여 CustomerGatewayName 편집 대화 상자를 엽니다.
4. 게이트웨이 상태 로그 그룹에서 다음 중 하나를 선택합니다.

   - CloudWatch 로그 그룹을 사용하여 게이트웨이를 모니터링하지 않으려면 로깅을 비활성화를 선택합니다.
   - 새 CloudWatch 로그 그룹을 생성하려면 새 로그 그룹 생성을 선택합니다.
   - 기존 CloudWatch 로그 그룹을 사용하려면 기존 로그 그룹 사용을 선택합니다.

     기존 로그 그룹 목록에서 로그 그룹을 선택합니다.
5. 변경 사항 저장을 선택합니다.
6. 게이트웨이의 상태 로그를 확인하려면 다음을 수행합니다.

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

다음은 CloudWatch로 전송되는 Tape Gateway 이벤트 메시지의 예입니다. 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 CloudWatch API를 사용하여 Tape Gateway에 대한 모니터링 데이터를 가져올 수 있습니다. 콘솔에는 CloudWatch API의 원시 데이터를 기초로 하는 일련의 그래프가 표시됩니다. CloudWatch API는 Amazon AWS 소프트웨어 개발 키트(SDKs) 또는 Amazon CloudWatch API 도구 중 하나를 통해서도 사용할 수 있습니다. 필요에 따라 콘솔에 표시되거나 API에서 가져온 그래프를 사용하는 것이 더 나을 수 있습니다.

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

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

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

Amazon CloudWatch 네임스페이스	차원	설명
`AWS/StorageGateway`	`GatewayId` , `GatewayName`	이 차원은 Tape Gateway 게이트웨이의 여러 측면을 설명하는 지표 데이터를 필터링합니다. `GatewayId` 차원

Amazon CloudWatch 네임스페이스	차원	설명
		과 `GatewayName` 차원을 모두 지정하여 작업할 Tape Gateway를 식별할 수 있습니다. Tape Gateway의 처리량 및 지연 시간 데이터는 Tape Gateway의 모든 가상 테이프에 기반을 두고 있습니다. 자동으로 5분 기간 동안 데이터를 무료로 사용할 수 있습니다.

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

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

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	AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율 중 테이프가 차지하는 비중입니다. 보고 기간 종료 시점에서 샘플이 채취됩니다. 게이트웨이의 CachePercentDirty 지표를 사용하면 AWS에 지속되지 않은 게이트웨이 캐시의 전체 백분율을 알 수 있습니다. 자세한 내용은 게이트웨이 지표 이해 단원을 참조하십시오. 단위: 백분율
CloudTraffic	클라우드에서 테이프로 업로드 및 다운로드한 바이트 수입니다. 단위: 바이트
IoWaitPercent	테이프에서 현재 사용 중인 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.

지표	설명
	이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트
UserCpuPercent	테이프에서 현재 사용 중인 사용자에게 할당된 CPU 계산 단위의 백분율입니다. 단위: 백분율
WriteBytes	보고 기간 동안 온프레미스 애플리케이션에 작성한 총 바이트 수입니다. 이 지표를 Sum 통계와 함께 사용하면 처리량을 측정할 수 있으며 Samples 통계와 함께 사용하면 IOPS를 측정할 수 있습니다. 단위: 바이트

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. CloudWatch에서 지표 값을 보려면 데이터 지연 시간(밀리초)에 대해서는 Average 통계를, 초당 입출력 작업 처리량(IOPS)에 대해서는 Samples 통계를 사용해야 합니다. 자세한 정보는 Amazon CloudWatch 사용 설명서의 통계를 참조하세요.

다음 표는 Tape Gateway와 AWS간 처리량, 지연 시간 및 IOPS를 측정하는 데 사용할 수 있는 지표와 해당 통계를 요약한 것입니다.

관심 항목	측정 방법
Latency	`Average` CloudWatch 지표와 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 지표와 함께 `CloudBytesDownloaded` 및 `CloudBytesUploaded` 지표를 사용합니다. 예를 들어 샘플 기간 5분 동안의 지표 `Sum` 값을 `CloudBytesDownloaded` 300초로 나누면에서 Tape Gateway AWS 까지의 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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 지표 탭을 선택합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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 1.85MB입니다.

Tape Gateway에서 까지의 데이터 지연 시간을 측정하려면 AWS

1. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 지표 탭을 선택합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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. https://console.aws.amazon.com/cloudwatch/에서 CloudWatch 콘솔을 엽니다.
2. 경보 생성을 선택하여 경보 생성 마법사를 시작합니다.
3. StorageGateway: 게이트웨이 지표 차원을 선택한 후 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 `CloudDownloadLatency`가 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 삭제 등의 포함됩니다. 이 작업은 모든 게이트웨이 유형에 공통된 것입니다. 게이트웨이를 생성하지 않았으면 게이트웨이 생성 단원을 참조하십시오.

주제

- Storage Gateway의 로컬 디스크 관리 - 디스크 크기 요구 사항을 평가하고, 캐시 용량을 추가하고, 버퍼링 및 저장을 위해 Tape Gateway에 할당하는 로컬 디스크를 관리하는 방법에 대해 알아봅니다.
- Tape Gateway의 대역폭 관리 - 게이트웨이에서 사용하는 네트워크 대역폭의 양을 제어하기 AWS 위해 게이트웨이의 업로드 처리량을 로 제한하는 방법을 알아봅니다.
- 게이트웨이 업데이트 관리 - 유지 관리 업데이트를 켜거나 끄는 방법과 Tape Gateway의 유지 관리 기간 일정을 수정하는 방법에 대해 알아봅니다.
- 게이트웨이 VM 종료 - 하이퍼바이저에 패치를 적용할 때와 같이 유지 관리를 위해 게이트웨이 가상 머신을 종료하거나 재부팅해야 하는 경우 어떻게 해야 하는지 알아봅니다.
- 게이트웨이 삭제 및 연결된 리소스 제거 - AWS Storage Gateway 콘솔을 사용하여 게이트웨이를 삭제하고 연결된 리소스를 정리하여 계속 사용할 경우 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 이 버퍼 데이터를 암호화된 Secure Sockets Layer(SSL) 연결을 통해 AWS에 업로드합니다.
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 물리 스토리지 리소스는 VMware에서 데이터 스토어로 표시됩니다. 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. 이는 백업이 RAID1 같이 성능이 비교적 떨어지는 RAID 구성일 때도 마찬가지입니다.

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 볼륨 데이터를 업로드 버퍼에 쓰지 않으며 Storage Gateway가 로컬에 저장된 데이터를에 저장된 데이터의 사본과 동기화할 AWS 때까지이 데이터를에 업로드하지 않습니다 AWS. 볼륨 상태가 BOOTSTRAPPING 일 때 동기화가 일어납니다.

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.

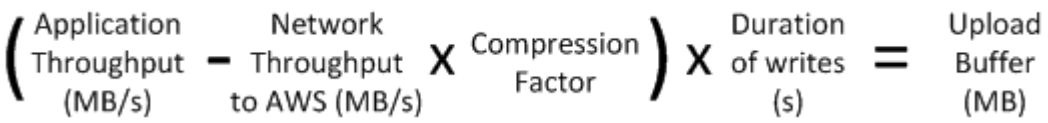
송신 데이터 속도

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 달라집니

다. 이 속도는 압축에 맞게 조정해야 합니다. 데이터를에 업로드할 때 게이트웨이는 가능한 경우 데이터 압축 AWS을 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.



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

Example

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

처음에는 이 근사치를 사용하여 게이트웨이에 업로드 버퍼 공간으로 할당할 디스크 크기를 결정할 수 있습니다. 필요한 경우 Storage Gateway 콘솔을 사용하여 업로드 버퍼 공간을 더 추가할 수 있습니다. 또한 Amazon CloudWatch 운영 지표를 사용하여 업로드 버퍼 사용량을 모니터링하고 추가 스토리지 요건을 파악할 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. 이후에는 Amazon CloudWatch 운영 지표를 사용하여 캐시 스토리지 사용량을 모니터링하고 콘솔을 사용하여

필요에 따라 추가 스토리지를 프로비저닝할 수 있습니다. 측정치 사용 및 경보 설정에 대한 정보는 캐시 스토리지 모니터링 섹션을 참조하세요.

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 경우, 게이트웨이 호스트 하이퍼바이저 또는 Amazon EC2 인스턴스에 새 디스크를 생성해야 합니다. 캐시 또는 업로드 버퍼로 이미 할당된 기존 디스크의 크기는 제거하거나 변경하지 마세요.

게이트웨이에 대한 추가 업로드 버퍼 또는 캐시 스토리지를 구성하려면

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

Tape Gateway의 대역폭 관리

게이트웨이에서 로 업로드 처리량을 제한(또는 제한) AWS 하거나에서 게이트웨이로 다운로드 처리량을 제한(또는 제한) AWS 할 수 있습니다. 대역폭 제한을 사용하면 게이트웨이에서 사용하는 네트워크 대역폭의 양을 제어할 수 있습니다. 기본적으로 활성화된 게이트웨이에는 업로드 또는 다운로드에 대한 속도 제한이 없습니다.

를 사용하거나 Storage Gateway API(UpdateBandwidthRateLimit 참조) 또는 AWS 소프트웨어 개발 키트(SDK)를 사용하여 AWS Management Console프로그래밍 방식으로 속도 제한을 지정할 수 있습니다. 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. 대역폭 속도 제한 간격을 하나 이상 정의하여 대역폭 조절을 예약할 수 있습니다. 자세한 내용은 Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절 단원을 참조하십시오.

대역폭 조절에 대한 설정을 하나로 구성한다는 것은 시작 시간을 `00:00`, 종료 시간을 `23:59`로 설정하여 매일 단일 대역폭 속도 제한 간격의 일정을 정의하는 것과 기능적으로 동일합니다.

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

주제

- Storage Gateway 콘솔을 사용하여 대역폭 조절 변경
- Storage Gateway 콘솔을 사용한 일정 기반 대역폭 조절
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for Java
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS SDK for .NET
- 를 사용하여 게이트웨이 대역폭 속도 제한 업데이트 AWS Tools for Windows PowerShell

Storage Gateway 콘솔을 사용하여 대역폭 조절 변경

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

콘솔을 사용하여 게이트웨이의 대역폭 조절을 변경하려면

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

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

   - 요일 - 대역폭 속도 제한 간격을 평일(월요일-금요일), 주말(토요일과 일요일), 모든 요일 또는 하나 이상의 특정 요일로 생성할 수 있습니다.
   - 시작 시간 - 대역폭 간격의 시작 시간을 게이트웨이의 현지 시간대(HH:MM 형식)로 입력합니다.

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

   - 종료 시간 - 대역폭 속도 제한 간격의 종료 시간을 게이트웨이의 현지 시간대(HH:MM 형식)로 입력합니다.

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

- 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.

대역폭 속도 제한 간격을 수정하려면 간격 매개변수에 수정된 값을 입력합니다.

대역폭 속도 제한 간격을 삭제하려면 삭제할 간격의 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 대역폭 속도 제한 간격을 계속 추가합니다.

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

6. 모든 대역폭 속도 제한 간격을 입력한 후 변경사항 저장을 선택하여 대역폭 속도 제한 일정을 저장합니다.

대역폭 속도 제한 일정이 성공적으로 업데이트되면 게이트웨이의 세부 정보 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 애플리

케이션을 실행하는 방법을 잘 알아야 합니다. 자세한 내용은AWS SDK for Java 개발자 안내서에서 시작하기를 참조하세요.

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

다음 Java 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN), 업로드 및 다운로드 한도를 제공해야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

```
import java.io.IOException;

import com.amazonaws.AmazonClientException;
import com.amazonaws.auth.PropertiesCredentials;
import com.amazonaws.services.storagegateway.AWSStorageGatewayClient;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitRequest;
import com.amazonaws.services.storagegateway.model.UpdateBandwidthRateLimitResult;


public class UpdateBandwidthExample {

    public static AWSStorageGatewayClient sgClient;

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

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

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

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

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

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

        UpdateBandwidth(gatewayARN, uploadRate, downloadRate);
```

```
    }

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

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

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

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

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

다음 C# 코드 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 코드를 사용하려면 서비스 엔드포인트, 게이트웨이 Amazon 리소스 이름(ARN), 업로드 및 다운로드 한도를 제공해

야 합니다. Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

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

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

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

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

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

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

            UpdateBandwidth(gatewayARN, uploadRate, downloadRate);

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

        public static void UpdateBandwidth(string gatewayARN, long uploadRate, long
 downloadRate)
        {
```

```
            try
            {
                UpdateBandwidthRateLimitRequest updateBandwidthRateLimitRequest =
                    new UpdateBandwidthRateLimitRequest()
                    .WithGatewayARN(gatewayARN)
                    .WithAverageDownloadRateLimitInBitsPerSec(downloadRate)
                    .WithAverageUploadRateLimitInBitsPerSec(uploadRate);

                UpdateBandwidthRateLimitResponse updateBandwidthRateLimitResponse =
 sgClient.UpdateBandwidthRateLimit(updateBandwidthRateLimitRequest);
                String returnGatewayARN =
 updateBandwidthRateLimitResponse.UpdateBandwidthRateLimitResult.GatewayARN;
                Console.WriteLine("Updated the bandwidth rate limits of " +
 returnGatewayARN);
                Console.WriteLine("Upload bandwidth limit = " + uploadRate + " bits per
 second");
                Console.WriteLine("Download bandwidth limit = " + downloadRate + " bits
 per second");
            }
            catch (AmazonStorageGatewayException ex)
            {
                Console.WriteLine("Error updating gateway bandwith.\n" +
 ex.ToString());
            }
        }
    }
}
```

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

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

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

다음 PowerShell 스크립트 예시에서는 게이트웨이의 대역폭 속도 제한을 업데이트합니다. 이 예제 스크립트를 사용하려면 게이트웨이 Amazon 리소스 이름(ARN), 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 정기적으로 업데이트됩니다. 이 섹션의 주제는 이러한 업데이트의 주기, 업데이트 적용 방법 및 배포의 게이트웨이에서 업데이트 관련 설정을 구성하는 방법에 대해 설명합니다.

> **Important**
>
> Storage Gateway 어플라이언스를 관리형 가상 머신으로 취급해야 하며 어떤 식으로든 설치 또는 콘텐츠에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반 AWS 게이트웨이 업데이트 메커니즘(예: SSM 또는 하이퍼바이저 도구) 이외의 방법을 사용하여 소프트웨어 패키지를 설치하거나 업데이트하려고 하면 게이트웨이가 오작동할 수 있습니다.
>
> Storage Gateway는 보안 및 안정성을 유지하기 위해 어플라이언스를 자동으로 정기적으로 패치합니다. Storage Gateway 어플라이언스는 Amazon Linux를 기본 운영 체제로 사용합니다. Amazon Linux 보안 센터에서 탐지된 일반적인 취약성 및 노출(CVE) 문제의 상태를 확인할 수 있습니다. CVE 패치는 Amazon Linux 보안 센터에 표시된 대로 릴리스 후 30일 이내에 자동으로 적용됩니다. 게이트웨이가 온라인 상태인 경우 게이트웨이 유지 관리 일정 중에 패치가 설치됩니다.
>
> Storage Gateway는 cloud-init 명령을 사용하여 Amazon EC2 게이트웨이를 수동으로 업데이트하는 기능을 지원하지 않습니다. 이 방법을 사용하여 게이트웨이를 업데이트하는 경우 게이트웨이 어플라이언스를 활성화하거나 사용하지 못하게 하는 상호 운용성 문제가 발생할 수 있습니다.

업데이트 빈도 및 예상 동작

AWS 는 배포된 게이트웨이를 중단하지 않고 필요에 따라 클라우드 서비스 구성 요소를 업데이트합니다. 배포된 게이트웨이 어플라이언스는 매월 유지 관리 업데이트를 받습니다. 월간 유지 관리 업데이트에는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안 문제를 해결하기 위한 수정 사항, 새로운 기능에 대한 액세스가 포함될 수 있습니다. 모든 업데이트는 누적되며 적용 시 게이트웨이를 현재 버전으로 업그레이드합니다. 각 업데이트에 포함된 특정 변경 사항에 대한 자세한 내용은 Tape Gateway Appliance Software 릴리스 정보를 참조하세요.

월별 유지 관리 업데이트로 인해 서비스가 잠시 중단될 수 있습니다. 업데이트 중에 게이트웨이의 VM 호스트는 재부팅할 필요가 없지만 게이트웨이 어플라이언스가 업데이트되고 다시 시작되는 잠시 동안 게이트웨이를 사용할 수 없게 됩니다. 게이트웨이의 재시작으로 인한 애플리케이션의 중단 가능성은 iSCSI 초기자의 제한 시간을 늘려서 최소화할 수 있습니다. Windows 및 Linux의 iSCSI 초기자 제한 시간을 늘리는 것에 대한 자세한 내용은 Windows iSCSI 설정 사용자 지정 및 Linux iSCSI 설정을 사용자 지정 단원을 참조하십시오.

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

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

게이트웨이에 업데이트가 적용되기 전에는 Storage Gateway 콘솔 및의 메시지를 AWS 알려줍니다 AWS Health Dashboard. 자세한 내용은 AWS Health Dashboard 단원을 참조하십시오. 소프트웨어 업데이트 알림이 전송되는 이메일 주소를 수정하려면 AWS 계정 관리 참조 안내서의 AWS 계정의 대체 연락처 업데이트를 참조하세요.

업데이트가 제공되면 게이트웨이 세부 정보 탭에 유지 관리 메시지가 표시됩니다. 세부 정보 탭에서 성공적으로 업데이트가 적용된 최근 날짜와 시간도 확인할 수 있습니다.

유지 관리 업데이트 켜기 또는 끄기

유지 관리 업데이트가 켜져 있는 경우 구성된 유지 관리 기간 일정에 따라 게이트웨이에서 이러한 업데이트를 자동으로 적용합니다. 자세한 내용은 을 참조하세요.

유지 관리 업데이트가 꺼져 있는 경우 게이트웨이에서 이러한 업데이트가 자동으로 적용되지는 않지만 언제든지 Storage Gateway 콘솔, API 또는 CLI를 사용하여 수동으로 적용할 수 있습니다. 긴급 업데이트는 이 설정과 관계없이 구성된 유지 관리 기간 동안 적용될 수 있습니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 게이트웨이 업데이트를 켜거나 끄는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조에서 UpdateMaintenanceStartTime을 참조하세요.

Storage Gateway 콘솔을 사용하여 유지 관리 업데이트를 켜거나 끄려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 업데이트에서 켜기 또는 끄기를 선택합니다.
5. 완료되었으면 변경 사항 저장을 선택합니다.

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

게이트웨이 유지 관리 기간 일정 수정

유지 관리 업데이트가 켜져 있는 경우 유지 관리 기간 일정에 따라 게이트웨이에서 이러한 업데이트를 자동으로 적용합니다. 긴급 업데이트는 유지 관리 업데이트 설정과 관계없이 구성된 유지 관리 기간 동안 적용될 수 있습니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 설정을 변경하려면 Storage Gateway API 참조에서 UpdateMaintenanceStartTime을 참조하세요.

Storage Gateway 콘솔을 사용하여 유지 관리 기간 일정을 수정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 유지 관리 업데이트를 구성할 게이트웨이를 선택합니다.
3. 작업을 선택한 다음 유지 관리 설정 편집을 선택합니다.
4. 유지 관리 기간 시작 시간에서 다음을 수행합니다.

    a. 일정에서 주별 또는 월별을 선택하여 유지 관리 기간 주기를 설정합니다.

    b. 주별을 선택한 경우, 요일 및 시간 값을 수정하여 유지 관리 기간이 시작될 각 주의 특정 시점을 설정합니다.

    월별을 선택한 경우, 날짜 및 시간 값을 수정하여 유지 관리 기간이 시작될 각 월의 특정 시점을 설정합니다.

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

5. 완료되었으면 변경 사항 저장을 선택합니다.

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

수동으로 업데이트 적용

게이트웨이에 대한 소프트웨어 업데이트를 사용할 수 있는 경우 아래 절차에 따라 수동으로 적용할 수 있습니다. 이 수동 업데이트 프로세스는 유지 관리 기간 일정을 무시하고 유지 관리 업데이트가 꺼져 있더라도 즉시 업데이트를 적용합니다.

> **Note**
>
> 다음 절차에서는 Storage Gateway 콘솔을 사용하여 업데이트를 수동으로 적용하는 방법에 대해 설명합니다. API를 사용하여 프로그래밍 방식으로 이 작업을 수행하려면 Storage Gateway API 참조에서 UpdateGatewaySoftwareNow를 참조하세요.

Storage Gateway 콘솔을 사용하여 게이트웨이 소프트웨어 업데이트를 수동으로 적용하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 업데이트할 게이트웨이를 선택합니다.

   업데이트를 사용할 수 있는 경우 콘솔의 게이트웨이 세부 정보 탭에 파란색 알림 배너가 표시되며, 여기에는 업데이트를 적용할 수 있는 옵션이 포함되어 있습니다.
3. 지금 업데이트 적용을 선택하여 게이트웨이를 즉시 업데이트합니다.

   > **Note**
   >
   > 이 작업을 수행하면 업데이트가 설치되는 동안 게이트웨이 기능이 일시적으로 중단됩니다. 이 시간 동안 게이트웨이 상태는 Storage Gateway 콘솔에 오프라인으로 표시됩니다. 업데이트 설치가 완료되면 게이트웨이가 정상 작동을 재개하고 상태가 실행 중으로 변경됩니다.

Storage Gateway 콘솔에서 선택한 게이트웨이의 세부 정보 탭을 확인하여 게이트웨이 소프트웨어가 최신 버전으로 업데이트되었는지 확인할 수 있습니다.

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 API를 사용하여 게이트웨이를 시작하고 중지할 수도 있습니다. VM을 켜면 게이트웨이를 다시 시작해야 합니다.

Important

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

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-- ShutdownGateway를 참조하세요.

Tape Gateway 시작 및 중지

a Tape Gateway를 중지하려면

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

게이트웨이 삭제 및 연결된 리소스 제거

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

게이트웨이를 삭제하면 더 이상 AWS Storage Gateway 관리 콘솔에 표시되지 않으며 이니시에이터에 대한 iSCSI 연결이 닫힙니다. 게이트웨이 삭제 절차는 모든 게이트웨이 유형에 동일합니다. 단 삭제하려는 게이트웨이의 유형과 게이트웨이를 배포한 호스트에 따라 별도 지침 대로 연결된 리소스를 제거해야 합니다.

> **Note**
>
> Tape Gateway를 삭제하면 현재 `AVAILABLE` 상태인 모든 테이프도 삭제되며 해당 테이프의 모든 데이터도 손실됩니다. 삭제하려는 게이트웨이에서 사용 중인 테이프의 데이터를 유지하려면 게이트웨이를 삭제하기 전에 테이프를 아카이브해야 합니다. 자세한 내용은 가상 테이프 아카이브를 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 AWS Storage Gateway API 참조를 참조하세요.

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

게이트웨이 삭제

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 게이트웨이를 선택한 다음 삭제할 게이트웨이를 하나 이상 선택합니다.
3. 작업에서 게이트웨이 삭제를 선택합니다. 확인 대화 상자가 표시됩니다.

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

4. 지정된 게이트웨이를 삭제할 것인지 확인한 다음 확인 상자에 delete라는 단어를 입력하고 삭제를 선택합니다.

5. (선택 사항) 삭제된 게이트웨이에 대한 피드백을 제공하려면 피드백 대화 상자를 작성한 다음 제출을 선택합니다. 그렇지 않은 경우 건너뛰기를 선택합니다.

> **Important**
>
> 게이트웨이를 삭제한 후에는 더 이상 소프트웨어 요금을 지불하지 않아도 되지만, 가상 테이프, Amazon Elastic Block Store(Amazon EBS) 스냅샷 및 Amazon EC2 인스턴스와 같은 리소스는 계속 유지됩니다. 이러한 리소스에 대해서는 계속 비용이 청구됩니다. Amazon EC2 구독을 취소하여 Amazon EC2 인스턴스 및 Amazon EBS 스냅샷을 제거하도록 선택할 수 있습니다. Amazon EC2 구독을 유지하려는 경우 Amazon EC2 콘솔을 사용하여 Amazon EBS 스냅샷을 삭제할 수 있습니다.

온프레미스에 배포한 게이트웨이에서 리소스 제거

다음 지침에 따라 온프레미스에 배포한 게이트웨이에서 리소스를 제거할 수 있습니다.

VM에 배포된 Tape Gateway에서 리소스 제거

게이트웨이 가상 테이프 라이브러리(VTL)를 삭제하는 경우 게이트웨이 삭제 전후에 추가 정리 단계를 수행해야 합니다. 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.

- Tape Gateway 연결 AWS- Tape Gateway가에 연결되어 AWS 있고 게이트웨이를 삭제하면 게이트웨이와 연결된 iSCSI 대상(즉, 가상 테이프 드라이브 및 미디어 체인저)을 더 이상 사용할 수 없습니다.
- Tape Gateway가 연결되지 않음 AWS- Tape Gateway가 연결되지 않은 경우 AWS, 예를 들어 기본 VM이 꺼져 있거나 네트워크가 다운된 경우 게이트웨이를 삭제할 수 없습니다. 이렇게 시도하면 환경이 복구되어 다시 가동된 후에 iSCSI 대상이 사용 가능한 상태로 Tape Gateway가 온프레미스에서 실행될 수 있습니다. 하지만 Tape Gateway 데이터는 업로드되거나 다운로드되지 않습니다 AWS.

삭제하려는 Tape Gateway가 작동하지 않는 경우, 다음 설명과 같이 먼저 이를 비활성화하고 삭제해야 합니다.

- 라이브러리에서 RETRIEVED 상태인 테이프를 삭제하려면 백업 소프트웨어를 사용하여 테이프를 배출합니다. 지침은 테이프 보관을 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 지침은Tape 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 게이트웨이에 사용된 AWS 리소스, 특히 Amazon EC2 인스턴스, Amazon EBS 볼륨, Tape Gateway를 배포한 경우 테이프를 정리하는 것이 좋습니다. 이렇게 하면 원하지 않는 사용 요금이 청구되는 것을 방지할 수 있습니다.

Amazon EC2에 배포된 Tape Gateway에서 리소스 제거

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 정보는 Amazon EC2 사용 설명서에서 인스턴스 및 볼륨 정리를 참조하세요.
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 단원은 다음 주제로 구성되어 있으며, 게이트웨이 어플라이언스 로컬 콘솔을 사용하여 유지 관리 작업을 수행하는 방법에 대한 정보를 제공합니다. 로컬 콘솔은 게이트웨이 어플라이언스를 호스팅하는 가상화 호스트 플랫폼에서 직접 실행됩니다. 온프레미스 게이트웨이의 경우 VMware, Hyper-v 또는 Linux KVM 가상화 호스트를 통해 로컬 콘솔에 액세스합니다. Amazon EC2 게이트웨이의 경우 SSH를 사용하여 Amazon EC2 인스턴스에 연결하여 콘솔에 액세스합니다. 대부분의 작업은 여러 호스트 플랫폼에서 공통적으로 적용되지만 몇 가지 차이점도 있습니다.

주제

- 게이트웨이 로컬 콘솔 액세스 - Linux 커널 기반 가상 머신(KVM), VMware ESXi 또는 Microsoft Hyper-V Manager 플랫폼에서 호스팅되는 온프레미스 게이트웨이의 로컬 콘솔에 로그인하는 방법에 대해 알아봅니다.
- VM 로컬 콘솔에서 작업 수행 - 로컬 콘솔을 사용하여 HTTP 프록시 구성, 시스템 리소스 상태 보기, 터미널 명령 실행 등 온프레미스 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법에 대해 알아봅니다.
- Amazon EC2 로컬 콘솔에서 작업 수행 - 로컬 콘솔에 로그인하여 HTTP 프록시 구성, 시스템 리소스 상태 보기, 터미널 명령 실행 등 Amazon EC2 게이트웨이에 대한 기본 설정 및 고급 구성 작업을 수행하는 방법에 대해 알아봅니다.

게이트웨이 로컬 콘솔 액세스

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

주제

- Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스
- VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스
- Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스

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

KVM을 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

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

   ```
   # virsh list
   ```

   이 명령은 각각에 대한 Id, 이름 및 상태 정보가 포함된 VM 목록을 반환합니다. 게이트웨이 로컬 콘솔을 시작하려는 VM의 `Id`는 기록해 둡니다.

2. 로컬 콘솔에 액세스하려면 다음 명령을 사용합니다.

   ```
   # virsh console Id
   ```

   *Id*를 이전 단계에서 기록한 VM의 Id로 바꿉니다.

   AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

3. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 Tape Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스

VMware ESXi를 사용하여 게이트웨이의 로컬 콘솔에 액세스하려면

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

> **Note**
>
> 게이트웨이 VM이 켜져 있으면 애플리케이션 창의 왼쪽에 있는 VM 브라우저 패널에 VM 아이콘과 함께 녹색 화살표 아이콘이 나타납니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창 상단의 도구 모음에서 녹색 전원 켜기 아이콘을 선택하여 켤 수 있습니다.

3. 애플리케이션 창의 오른쪽에 있는 기본 정보 패널에서 콘솔 탭을 선택합니다.

   잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

   > **Note**
   >
   > 콘솔 창에서 커서를 릴리스하려면 Ctrl+Alt를 누릅니다.

4. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 Tape Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스

게이트웨이의 로컬 콘솔에 액세스하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager 애플리케이션 창의 왼쪽에 있는 가상 머신 패널에서 게이트웨이 어플라이언스 VM을 선택합니다.
2. 게이트웨이가 켜져 있는지 확인하세요.

> **Note**
>
> 게이트웨이 VM이 켜져 있는 경우 애플리케이션 창의 왼쪽에 있는 가상 머신 패널의 VM 상태 열에 Running이 표시됩니다. 게이트웨이 VM이 켜져 있지 않은 경우 애플리케이션 창의 오른쪽에 있는 작업 패널에서 시작을 선택하여 켤 수 있습니다.

3. 작업 패널에서 연결을 선택합니다.

   그러면 Virtual Machine Connection(가상 머신 연결) 창이 표시됩니다. 인증 창이 표시되면 하이퍼바이저 관리자가 제공한 로그인 자격 증명을 입력합니다.

   잠시 후 AWS 어플라이언스 게이트웨이 로컬 콘솔에 로그인하여 네트워크 구성 및 기타 설정을 변경하라는 메시지가 표시됩니다.

4. 사용자 이름과 암호를 입력하여 게이트웨이 로컬 콘솔에 로그인합니다. 자세한 내용은 Tape Gateway 로컬 콘솔에 로그인을 참조하세요.

   로그인하면 AWS 어플라이언스 활성화 - 구성 메뉴가 나타납니다. 메뉴 옵션 중 하나를 선택하여 게이트웨이 구성 작업을 수행할 수 있습니다. 자세한 내용은 가상 머신 로컬 콘솔에서 작업 수행을 참조하세요.

VM 로컬 콘솔에서 작업 수행

온프레미스로 배포하는 Tape Gateway 의 경우 가상 머신 호스트 플랫폼에서 액세스하는 게이트웨이 로컬 콘솔을 사용하여 다음과 같은 유지 관리 작업을 수행할 수 있습니다. 이러한 작업은 VMware, Microsoft Hyper-V 및 Linux 커널 기반 가상 머신(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 - DHCP를 사용하거나 정적 IP 주소를 할당하도록 게이트웨이를 구성하는 방법에 대해 알아봅니다.
- 게이트웨이가 인터넷에 연결되어 있는지 테스트 - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이와 인터넷 간의 연결을 테스트하는 방법에 대해 알아봅니다.

- 온프레미스 게이트웨이에 대해 로컬 콘솔에서 Storage Gateway 명령 실행 - 라우팅 테이블 저장, 연결 등과 같은 추가 작업을 수행할 수 있는 로컬 콘솔 명령을 실행하는 방법에 대해 알아봅니다 지원.
- 게이트웨이 시스템 리소스 상태 조회 - 게이트웨이 어플라이언스에서 사용할 수 있는 가상 CPU 코어, 루트 볼륨 크기 및 RAM을 확인하는 방법에 대해 알아봅니다.

Tape Gateway 로컬 콘솔에 로그인

VM이 로그인할 준비가 되면 로그인 화면이 표시됩니다. VM 로컬 콘솔에 처음 로그인하는 경우 임시 로그인 자격 증명을 사용하여 로그인합니다. 이러한 임시 자격 증명을 통해 로컬 콘솔에서 게이트웨이 네트워크 설정을 구성하고 암호를 변경할 수 있는 메뉴에 액세스할 수 있습니다. 초기 사용자 이름은 `admin`이고, 임시 암호는 `password`입니다. 처음 로그인할 때 암호를 변경해야 합니다.

임시 암호를 변경하려면

1. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 게이트웨이 콘솔에 해당하는 숫자를 입력합니다.
2. `passwd` 명령을 실행합니다. 명령을 실행하는 방법에 대한 정보는 온프레미스 게이트웨이에 대해 로컬 콘솔에서 Storage Gateway 명령 실행 섹션을 참조하세요.

> **Important**
>
> 이전 버전의 Volume Gateway 또는 Tape Gateway의 경우 사용자 이름은 `sguser`이고 암호는 입니다`sgpassword`. 암호를 재설정하고 게이트웨이를 최신 버전으로 업데이트하면 사용자 이름이 관리자로 변경되지만 암호는 유지됩니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호 설정

Storage Gateway 웹 기반 콘솔에서 로컬 콘솔의 암호를 관리할 수도 있습니다. 웹 기반 콘솔로 암호가 성공적으로 업데이트되면 로컬로 로그인한 적이 없는 경우 임시 암호를 포함하여 게이트웨이 VM의 로컬 콘솔에서 사용하는 암호가 재정의됩니다. 현재 네트워크를 통해 게이트웨이에 연결할 수 없는 경우 암호 업데이트 프로세스가 실패합니다.

Storage Gateway 콘솔에서 로컬 콘솔 암호를 설정하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 다음 새 암호를 설정할 게이트웨이를 선택합니다.
3. 작업에서 Set Local Console Password(로컬 콘솔 암호 설정)을 선택합니다.

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

   새 암호가 현재 암호를 대체합니다. Storage Gateway는 암호를 저장, 저장 또는 기록하지 않고 암호화된 채널을 통해 안전하게 VM으로 전송하여 안전하게 저장합니다.

온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성

Volume Gateway와 Tape Gateway는 온프레미스 게이트웨이와 AWS간 Socket Secure 버전 5(SOCKS5) 프록시 구성을 지원합니다.

> **Note**
>
> 지원되는 유일한 프록시 구성은 SOCKS5입니다.

게이트웨이가 프록시 서버를 사용하여 인터넷과 통신해야 하는 경우에는 게이트웨이에 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 섹션을 참조하세요.

다음 절차는 Volume Gateway와 Tape Gateway에 대해 SOCKS 프록시를 구성하는 방법을 안내합니다.

Volume Gateway와Tape Gateway에 대해 SOCKS5 프록시를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi - 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - KVM - 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 SOCKS 프록시 구성을 선택합니다.
3. AWS Storage Gateway SOCKS 프록시 구성 메뉴에서 해당 숫자를 입력하여 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
SOCKS 프록시 구성	해당 숫자를 입력하여 SOCKS 프록시 구성을 선택합니다. 구성을 완료하려면 호스트 이름 및 포트를 입력해야 합니다.
현재 SOCKS 프록시 구성 조회	해당 숫자를 입력하여 현재 SOCKS 프록시 구성 보기를 선택합니다. SOCKS 프록시가 구성되어 있지 않은 경우 `SOCKS Proxy not configured` 라는 메시지가 표시됩니다. SOCKS 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.
SOCKS 프록시 구성 제거	해당 숫자를 입력하여 SOCKS 프록시 구성 제거를 선택합니다. 메시지 `SOCKS Proxy Configuration Removed` 가 나타납니다.

4. VM을 다시 시작하여 HTTP 구성을 적용합니다.

게이트웨이 네트워크 구성

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

고정 IP 주소를 사용하도록 게이트웨이를 구성하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

- VMware ESXi - 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
- Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
- KVM - 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.

2. AWS Storage Gateway - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. AWS Storage Gateway 네트워크 구성 메뉴에서 다음 작업 중 하나를 수행합니다.

수행할 작업	수행할 작업
네트워크 어댑터 설명	해당 숫자를 입력하여 어댑터 설명을 선택합니다. 어댑터 이름 목록이 나타나고 어댑터 이름을 입력하라는 메시지가 표시됩니다(예: **eth0**). 지정하려는 어댑터가 사용 중인 경우, 다음과 같은 어댑터 정보가 표시됩니다. • 미디어 액세스 제어(MAC) 주소 • IP 주소 • 넷마스크 • 게이트웨이 IP 주소 • DHCP 활성화 상태 고정 IP 주소를 구성하거나 게이트웨이의 기본 어댑터를 설정할 경우 여기에 나열된 어댑터 이름을 사용합니다.
DHCP 구성	

수행할 작업	수행할 작업
	해당 숫자를 입력하여 DHCP 구성을 선택합니다. DHCP를 사용하도록 네트워크 인터페이스를 구성하라는 메시지가 표시됩니다.

수행할 작업	수행할 작업
게이트웨이에 고정 IP 주소 구성	해당 숫자를 입력하여 고정 IP 구성을 선택합니다. 다음 정보를 입력하여 고정 IP를 구성하라는 메시지가 표시됩니다. • 네트워크 어댑터 이름 • IP 주소 • 넷마스크 • 기본 게이트웨이 주소 • 기본 DNS(Domain Name Service) 주소 • 보조 DNS 주소 **Important** 게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오. 게이트웨이에서 네트워크 인터페이스를 한 개 이상 사용하는 경우, 활성화된 모든 인터페이스에서 DHCP 또는 고정 IP 주소를 사용하도록 설정해야 합니다.

수행할 작업	수행할 작업
	예를 들어 게이트웨이 VM이 DHCP로 구성된 인터페이스 두 개를 사용한다고 가정합시다. 나중에 한 인터페이스를 고정 IP로 설정하면 다른 하나는 비활성화됩니다. 이 경우 인터페이스를 활성화하려면 고정 IP로 설정해야 합니다. 처음에 두 인터페이스 모두 고정 IP 주소를 사용하도록 설정한 후 DHCP를 사용하도록 게이트웨이를 설정하면 두 인터페이스 모두 DHCP를 사용하게 됩니다.
게이트웨이의 호스트 이름 구성	해당 숫자를 입력하여 호스트 이름 구성을 선택합니다. 게이트웨이에서 지정한 정적 호스트 이름을 사용할지 아니면 DCHP 또는 rDNS를 통해 자동으로 할당할지를 선택하라는 메시지가 표시됩니다. 정적을 선택하면 같은 정적 호스트 이름(예: `testgateway.example.com`)을 제공하라는 메시지가 표시됩니다. y를 입력하여 구성을 적용합니다. **Note** 게이트웨이에 대해 정적 호스트 이름을 구성할 경우 제공된 호스트 이름이 게이트웨이가 조인된 도메인에 있는지 확인합니다. 또한 게이트웨이의 IP 주소가 정적 호스트 이름을 가리키는 A 레코드를 DNS 시스템에 생성해야 합니다.

수행할 작업	수행할 작업
게이트웨이의 모든 네트워크 구성을 DHCP로 재설정	해당 숫자를 입력하여 모두 DHCP로 재설정을 선택합니다. 모든 네트워크 인터페이스가 DHCP를 사용하도록 설정됩니다. **Important** 게이트웨이가 이미 활성화된 경우, 설정이 적용되도록 Storage Gateway 콘솔에서 게이트웨이를 종료한 후 다시 시작해야 합니다. 자세한 내용은 게이트웨이 VM 종료 단원을 참조하십시오.
게이트웨이의 기본 경로 어댑터 설정	해당 숫자를 입력하여 기본 어댑터 설정을 선택합니다. 게이트웨이에 사용할 수 있는 어댑터가 표시되고 어댑터 중 하나를 선택하라는 메시지가 표시됩니다(예: **eth0**).
게이트웨이의 DNS 구성 조회	해당 숫자를 입력하여 DNS 구성 보기를 선택합니다. 기본 및 보조 DNS 이름 서버의 IP 주소가 표시됩니다.
라우팅 테이블 조회	해당 숫자를 입력하여 경로 보기를 선택합니다. 게이트웨이의 기본 경로가 표시됩니다.

게이트웨이가 인터넷에 연결되어 있는지 테스트

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

게이트웨이가 인터넷에 연결되어 있는지 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi - 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - KVM - 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.

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 및를 지정해야 합니다.

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

4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. 지원되는 AWS 리전 및 Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

테스트가 진행되면 각 엔드포인트의 연결 상태가 다음과 같이 [통과] 또는 [실패]로 표시됩니다.

메시지	설명
[통과]	Storage Gateway가 네트워크에 연결되어 있습니다.
[실패]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

온프레미스 게이트웨이에 대해 로컬 콘솔에서 Storage Gateway 명령 실행

Storage Gateway의 VM 로컬 콘솔은 게이트웨이 관련 문제를 구성 및 진단할 수 있는 안전한 환경을 제공합니다. 로컬 콘솔 명령을 사용하여 라우팅 테이블 저장, 연결 등과 같은 유지 관리 작업을 수행할 수 있습니다 지원.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi 로컬 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 **h**를 입력합니다.

   그러면 사용 가능한 명령이 나열된 사용 가능한 명령 메뉴가 콘솔에 표시됩니다.

명령	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또

명령	함수
	는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 구성을 참조하세요.
ip	라우팅, 디바이스 및 터널을 표시/조작합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다. 지침은 게이트웨이 네트워크 구성을 참조하세요.
iptables	IPv4 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ip6tables	IPv6 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.
open-support-channel	AWS Support에 연결합니다.
passwd	인증 토큰을 업데이트합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.

명령	함수
sslcheck	인증서 발급자와 함께 출력을 반환합니다. **Note** Storage Gateway는 인증서 발급자 확인을 사용하며 SSL 검사는 지원하지 않습니다. 이 명령이 aws-appliance@amazon.com 이외의 발급자를 반환한다면 애플리케이션에서 SSL 검사를 수행 중일 가능성이 높습니다. 이 경우 Storage Gateway 어플라이언스에 대한 SSL 검사를 우회하는 것이 좋습니다.
tcptraceroute	대상으로 향하는 TCP 트래픽의 경로 추적 출력을 수집합니다.

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

명령에 대해 알아보려면 명령 프롬프트에 **man** + *## ##*을 입력합니다.

게이트웨이 시스템 리소스 상태 조회

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

시스템 리소스 점검의 상태를 보려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - VMware ESXi 콘솔 로그인에 대한 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

- KVM 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.

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

   각 리소스의 상태가 다음과 같이 [확인], [경고] 또는 [실패]로 표시됩니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[실패]	리소스가 최소 요구 사항을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.

   콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

Amazon EC2 로컬 콘솔에서 작업 수행

일부 Storage Gateway 유지 관리 작업을 수행하려면 Amazon EC2 인스턴스에 배포한 게이트웨이의 게이트웨이 로컬 콘솔에 로그인해야 합니다. 게이트웨이 로컬 콘솔은 Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스에서 액세스할 수 있습니다. 이 단원의 주제는 게이트웨이 로컬 콘솔에 로그인하여 유지 관리 작업을 수행하는 방법에 대해 설명합니다.

주제

- Amazon EC2 게이트웨이 로컬 콘솔에 로그인 - Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스의 게이트웨이 로컬 콘솔에 연결하고 로그인하는 방법에 대해 알아봅니다.

- HTTP 프록시를 통해 EC2에 배포된 게이트웨이 라우팅 - Socket Secure 버전 AWS 5(SOCKS5) 프록시 서버를 통해 모든 엔드포인트 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 방법에 대해 알아봅니다.
- 게이트웨이 시스템 리소스 상태 조회 - 게이트웨이 로컬 콘솔을 사용하여 게이트웨이 어플라이언스에서 사용할 수 있는 가상 CPU 코어, 루트 볼륨 크기 및 RAM을 확인하는 방법에 대해 알아봅니다.
- 로컬 콘솔에서 Storage Gateway 명령 실행 - 라우팅 테이블 저장, 연결 등과 같은 추가 작업을 수행할 수 있는 로컬 콘솔 명령을 실행하는 방법에 대해 알아봅니다 지원.

Amazon EC2 게이트웨이 로컬 콘솔에 로그인

Secure Shell(SSH) 클라이언트를 사용하여 Amazon EC2 인스턴스에 연결할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서에서 인스턴스에 연결을 참조하세요. 이런 방식으로 연결하려면 인스턴스를 시작할 때 지정한 SSH 키 페어가 필요합니다. Amazon EC2 키 페어에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon EC2 키 페어를 참조하세요.

게이트웨이 로컬 콘솔에 로그인하려면

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

관련 작업	이 주제를 참조하세요.
게이트웨이에 SOCKS 프록시를 구성	HTTP 프록시를 통해 EC2에 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 통해 EC2에 배포된 게이트웨이 라우팅

Storage Gateway는 Amazon EC2 및 AWS에 배포된 게이트웨이 간 Socket Secure 버전 5(SOCKS5) 프록시 구성을 지원합니다.

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

로컬 프록시 서버를 통해 게이트웨이 인터넷 트래픽을 라우팅하려면

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

    - HTTP 프록시 구성 - 구성을 완료하려면 호스트 이름과 포트를 입력해야 합니다.
    - 현재 HTTP 프록시 구성 보기 - HTTP 프록시가 구성되지 않은 경우 `HTTP Proxy not configured` 메시지가 표시됩니다. HTTP 프록시가 구성되어 있는 경우, 프록시의 호스트 이름과 포트가 표시됩니다.
    - HTTP 프록시 구성 제거 - `HTTP Proxy Configuration Removed` 메시지가 표시됩니다.

게이트웨이 네트워크 연결 테스트

게이트웨이의 로컬 콘솔을 사용하여 네트워크 연결을 테스트할 수 있습니다. 이 테스트는 게이트웨이의 네트워크 문제를 해결할 때 유용합니다.

게이트웨이 연결을 테스트하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 네트워크 연결 테스트를 선택합니다.

게이트웨이가 이미 활성화된 경우 연결 테스트가 즉시 시작됩니다. 아직 활성화되지 않은 게이트웨이의 경우 다음 단계에 설명된 AWS 리전 대로 엔드포인트 유형 및를 지정해야 합니다.

3. 게이트웨이가 아직 활성화되지 않은 경우 해당 숫자를 입력하여 게이트웨이의 엔드포인트 유형을 선택합니다.
4. 퍼블릭 엔드포인트 유형을 선택한 경우 해당 숫자를 입력하여 테스트할 AWS 리전 를 선택합니다. 지원되는 AWS 리전 및 Storage Gateway와 함께 사용할 수 있는 AWS 서비스 엔드포인트 목록은 의 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요AWS 일반 참조.

테스트가 진행되면 각 엔드포인트의 연결 상태가 다음과 같이 [통과] 또는 [실패]로 표시됩니다.

메시지	설명
[통과]	Storage Gateway가 네트워크에 연결되어 있습니다.
[실패]	Storage Gateway가 네트워크에 연결되어 있지 않습니다.

게이트웨이 시스템 리소스 상태 조회

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

시스템 리소스 점검의 상태를 보려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 시스템 리소스 점검 조회를 선택합니다.

   각 리소스의 상태가 다음과 같이 [확인], [경고] 또는 [실패]로 표시됩니다.

메시지	설명
[확인]	리소스가 시스템 리소스 점검을 통과하였습니다.
[경고]	리소스가 권장 요구 사항을 충족하지 못하지만 게이트웨이는 계속 작동할 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.
[실패]	리소스가 최소 요구 사항을 충족하지 않습니다. 게이트웨이가 제대로 작동하지 않을 수 있습니다. Storage Gateway에서 리소스 점검 결과를 설명하는 메시지가 표시됩니다.

콘솔의 리소스 점검 메뉴 옵션 옆에 오류와 경고 개수도 표시됩니다.

로컬 콘솔에서 Storage Gateway 명령 실행

AWS Storage Gateway 콘솔은 게이트웨이 문제를 구성하고 진단하기 위한 안전한 환경을 제공하는 데 도움이 됩니다. 콘솔 명령을 사용하여 라우팅 테이블 저장 또는 연결과 같은 유지 관리 작업을 수행할 수 있습니다 지원.

구성 또는 진단 명령을 실행하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. 게이트웨이 콘솔 명령 프롬프트에서 h를 입력합니다.

   그러면 사용 가능한 명령이 나열된 사용 가능한 명령 메뉴가 콘솔에 표시됩니다.

명령	함수
dig	DNS 문제 해결을 위해 dig에서 출력을 수집합니다.
exit	구성 메뉴로 돌아갑니다.
h	사용 가능한 명령 목록을 표시합니다.
ifconfig	네트워크 인터페이스를 표시하거나 구성합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다.
ip	라우팅, 디바이스 및 터널을 표시/조작합니다. **Note** Storage Gateway 콘솔 또는 전용 로컬 콘솔 메뉴 옵션을 사용하여 네트워크 또는 IP 설정을 구성하는 것이 좋습니다.
iptables	IPv4 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ip6tables	IPv6 패킷 필터링 및 NAT를 위한 관리 도구입니다.
ncport	네트워크의 특정 TCP 포트에 대한 연결을 테스트합니다.
nping	네트워크 문제 해결을 위해 nping에서 출력을 수집합니다.

명령	함수
open-support-channel	AWS Support에 연결합니다.
save-iptables	IP 테이블을 영구적으로 유지합니다.
save-routing-table	새로 추가된 라우팅 테이블 항목을 저장합니다.
sslcheck	네트워크 문제 해결을 위해 SSL 유효성을 확인하십시오.
tcptraceroute	대상으로 향하는 TCP 트래픽의 경로 추적 출력을 수집합니다.

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

명령에 대해 알아보려면 명령 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 나와 있는 Amazon EC2 인스턴스 크기와 유형은 예시이며 참고용으로 제공됩니다.

구성	쓰기 처리량 Gbps	캐시에서 읽기 처리량 Gbps	Amazon Web Services 클라우드에서 읽기 처리량 (GBps)
호스트 플랫폼: Amazon EC2 인스턴스 - c5.4xlarge CPU: 16 vCPU | RAM: 32GB 루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 스트라이프 RAID(2 x 500GB, io1 EBS SSD, 25000 IOPs) 업로드 버퍼 디스크: 450GB, io1 SSD, 2000IOPS 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 EC2 인스턴스 - c5d.9xlarge CPU: 36 vCPU | RAM: 72GB 루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 900GB NVMe 디스크 업로드 버퍼 디스크: 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 EC2 인스턴스 - c5d.metal CPU: 96 vCPU | RAM: 192GB 루트 디스크: 80GB, io1 SSD, 4,000 IOPS 캐시 디스크: 스트라이프 RAID(2 x 900GB NVMe 디스크) 업로드 버퍼 디스크: 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 유사한 리소스를 사용하는 자체 물리적 서버에서 얻을 수 있는 성능을 대표적으로 보여주기 위한 것입니다. 예를 들어, 스트라이프 RAID를 사용하는 EC2 구성은 일반적으로 EC2의 게이트웨이에서 지원하지 않는 특수 메커니즘을 통해 이루어졌습니다. 비슷한 성능을 얻으려면 게이트웨이를 실행하는 온프레미스 서버에 연결된 하드웨어 RAID 컨트롤러를 대신 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 24개의 전용 물리적 CPU 코어
- Tape Gateway의 경우 하드웨어에 할당해야 하는 RAM 양은 다음과 같습니다.
  - 최소 16GiB의 예약 RAM(캐시 크기가 최대 16TiB인 게이트웨이)
  - 최소 32GiB의 예약 RAM(캐시 크기가 16Ti-32TiB인 게이트웨이)
  - 최소 48GiB의 예약 RAM(캐시 크기가 32Ti-64TiB인 게이트웨이)

> **Note**
>
> 게이트웨이 성능을 최적화하려면 최소 32GiB의 RAM을 프로비저닝해야 합니다.

- 디스크 1 - 다음과 같이 게이트웨이 캐시로 사용됨
  - NVMe SSD로 구성된 스트라이프 RAID(독립 디스크의 중복 어레이)
- 디스크 2 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
  - NVMe SSD로 구성된 스트라이프 RAID
- 디스크 3 - 다음과 같이 게이트웨이 업로드 버퍼로 사용됨
  - NVMe SSD로 구성된 스트라이프 RAID
- 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 AWS에 연결하는 데 사용할 VMXNet3(10Gbps)를 추가합니다.

게이트웨이에 리소스 추가

다음 병목 현상은 Tape Gateway 의 성능을 이론적인 최대 지속 처리량(AWS 클라우드에 대한 대역폭) 미만으로 줄일 수 있습니다.

- CPU 코어 수
- 캐시/업로드 버퍼 디스크 처리량

- 총 RAM 용량
- 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.

- 스트라이프 RAID(예: RAID 10)를 사용하여 디스크 처리량을 개선합니다. 하드웨어 RAID 컨트롤러를 사용하는 것이 가장 좋습니다.

  > **Note**
  >
  > RAID(Redundant Array of Independent Disk) 또는 특히 RAID 10과 같은 디스크 스트라이프 RAID 구성은 데이터 본문을 블록으로 나누고 데이터 블록을 여러 스토리지 디바이스에 분산하는 프로세스입니다. 사용하는 RAID 수준은 달성할 수 있는 정확한 속도와 내결함성에 영향을 줍니다. I/O 워크로드를 여러 디스크에 분산하므로 RAID 디바이스의 전체 처리량은 단일 멤버 디스크의 처리량보다 훨씬 높습니다.

- 직접 연결된 고성능 디스크 사용

  게이트웨이 성능을 최적화하기 위해 SSD(Solid-State Drive) 및 NVMe 컨트롤러와 같은 고성능 디스크를 추가할 수 있습니다. Microsoft Hyper-V NTFS 대신 스토리지 영역 네트워크(SAN)에서 직접 가상 디스크를 VM에 연결할 수도 있습니다. 디스크 성능이 향상되면 일반적으로 처리량과 초당 입출력 작업 처리량(IOPS)이 증가합니다.

  처리량을 측정하려면 `ReadBytes` 및 `WriteBytes` 지표를 `Samples` Amazon CloudWatch 통계와 함께 사용합니다. 예를 들어, 5분의 샘플 기간 동안의 `ReadBytes` 지표의 `Samples` 통계를 300초로 나누면 IOPS를 알 수 있습니다. 일반적으로 게이트웨이에 대한 이러한 지표를 검토할 때는 디스크 관련 병목 현상을 나타내는 낮은 처리량과 낮은 IOPS 추세를 살펴보세요. 게이트웨이 지표에 대한 자세한 내용은 Tape Gateway와 간의 성능 측정 AWS 섹션을 참조하세요.

> **Note**
>
> CloudWatch 지표를 모든 게이트웨이에 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 ESXi에서는 기본 물리적 스토리지 리소스가 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, RAID 1 또는 RAID 6와 같이 성능이 낮은 RAID 구성을 통해 지원되는 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 프로세서에 전용 CPU 코어가 지원되는지 확인합니다. 또한 호스트 서버의 CPU를 과다 구독하고 있지 않은지 확인합니다.

게이트웨이 호스트 서버에 CPU를 추가하면 게이트웨이의 처리 능력이 향상됩니다. 이렇게 하면 게이트웨이가 애플리케이션의 데이터를 로컬 스토리지에 저장하고 이 데이터를 Amazon S3로 업로드하는 작업을 병렬로 처리할 수 있습니다. CPU를 추가하면 호스트를 다른 VM과 공유할 때 게이트웨이가 충분한 CPU 리소스를 확보할 수 있습니다. CPU 리소스를 충분히 제공하면 일반적으로 처리량이 향상되는 효과가 있습니다.

게이트웨이와 AWS 클라우드 간 대역폭 늘리기

대역폭을에서 로 늘리 AWS 면 게이트웨이로의 최대 데이터 수신 속도와 AWS 클라우드로의 송신 속도가 증가합니다. 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 중에 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 다운로드 대역폭을 초과하지 않습니다 AWS.

> **Note**
>
> 캐시/업로드 버퍼 디스크 처리량, CPU 코어 수, 총 RAM 용량 또는 이니시에이터와 게이트웨이 간 대역폭 등 여기에 나열된 다른 제한 요인으로 인해 관찰된 게이트웨이 성능이 네트워크 대역폭보다 낮을 수 있습니다. 또한, 게이트웨이의 정상 작동에는 데이터를 보호하기 위한 여러 가지 조치가 포함되므로 관찰된 성능이 네트워크 대역폭보다 낮을 수 있습니다.

iSCSI 설정 최적화

iSCSI 초기자에서 iSCSI 설정을 최적화하여 I/O 성능을 높일 수 있습니다. `MaxReceiveDataSegmentLength` 및 `FirstBurstLength`에는 256 KiB를 선택하고, `MaxBurstLength`에는 1MiB를 선택하는 것이 좋습니다. iSCSI 설정 구성에 대한 자세한 내용은 iSCSI 설정 사용자 지정 단원을 참조하십시오.

> **Note**
>
> 이러한 권장 설정을 통해 전반적으로 더 나은 성능을 실현할 수 있습니다. 그러나 성능을 최적화하는 데 필요한 특정 iSCSI 설정은 사용하는 백업 소프트웨어에 따라 다릅니다. 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 안됩니다.

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. 게이트웨이의 성능이 예상보다 현저히 떨어지는데 CPU 코어 수와 디스크 처리량을 이미 개선했다면 다음 사항을 고려하세요.

- 네트워크 케이블을 업그레이드하여 이니시에이터와 게이트웨이 간에 더 높은 대역폭을 확보합니다.
- 가능한 한 많은 테이프 드라이브를 동시에 사용합니다. iSCSI는 동일한 대상에 대해 여러 요청을 대기열에 넣는 것을 지원하지 않습니다. 즉, 테이프 드라이브를 많이 사용할수록 게이트웨이에서 동시에 처리할 수 있는 요청도 많아집니다. 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

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

Security in AWS Storage Gateway

의 클라우드 보안 AWS 이 최우선 순위입니다. AWS 고객은 보안에 가장 민감한 조직의 요구 사항을 충족하도록 구축된 데이터 센터 및 네트워크 아키텍처의 이점을 누릴 수 있습니다.

보안은 AWS 와 사용자 간의 공동 책임입니다. 공동 책임 모델은 이 사항을 클라우드의 보안 및 클라우드 내 보안으로 설명합니다.

- 클라우드 보안 - AWS 는 Amazon Web Services Cloud에서 AWS 서비스를 실행하는 인프라를 보호할 책임이 있습니다. AWS 또한는 안전하게 사용할 수 있는 서비스를 제공합니다. 타사 감사자는 AWS 규정 준수 프로그램 일환으로 보안의 효과를 정기적으로 테스트하고 확인합니다. AWS Storage Gateway에 적용되는 규정 준수 프로그램에 대한 자세한 내용은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 .
- 클라우드의 보안 - 사용자의 책임은 사용하는 AWS 서비스에 따라 결정됩니다. 또한 귀하는 귀사의 데이터 민감도, 귀사의 요구 사항, 관련 법률 및 규정을 비롯한 기타 요소에 대해서도 책임이 있습니다.

이 설명서는 Storage Gateway를 사용할 때 공동 책임 모델을 적용하는 방법을 이해하는 데 도움이 됩니다. 다음 주제에서는 보안 및 규정 준수 목적에 맞게 Storage Gateway를 구성하는 방법을 보여줍니다. 또한 Storage Gateway 리소스를 모니터링하고 보호하는 데 도움이 되는 다른 AWS 서비스를 사용하는 방법을 알아봅니다.

주제

- in AWS Storage Gateway의 데이터 보호
- Identity and Access Management for AWS Storage Gateway
- AWS Storage Gateway에 대한 규정 준수 검증
- Resilience in AWS Storage Gateway
- 인프라 보안 in AWS Storage Gateway
- AWS 보안 모범 사례
- 에서 로깅 및 모니터링 AWS Storage Gateway

in AWS Storage Gateway의 데이터 보호

AWS 공동 책임 모델 in AWS Storage Gateway의 데이터 보호에 적용됩니다. 이 모델에 설명된 대로 AWS 는 모든를 실행하는 글로벌 인프라를 보호할 책임이 있습니다 AWS 클라우드. 사용자는 인프라

에서 호스팅되는 콘텐츠를 관리해야 합니다. 사용하는 AWS 서비스 의 보안 구성과 관리 태스크에 대한 책임도 사용자에게 있습니다. 데이터 프라이버시에 대한 자세한 내용은 데이터 프라이버시 FAQ를 참조하세요. 유럽의 데이터 보호에 대한 자세한 내용은 AWS 보안 블로그의 AWS 공동 책임 모델 및 GDPR 블로그 게시물을 참조하세요.

데이터 보호를 위해 자격 증명을 보호하고 AWS 계정 AWS IAM Identity Center 또는 AWS Identity and Access Management (IAM)를 사용하여 개별 사용자를 설정하는 것이 좋습니다. 이렇게 하면 개별 사용자에게 자신의 직무를 충실히 이행하는 데 필요한 권한만 부여됩니다. 또한 다음과 같은 방법으로 데이터를 보호하는 것이 좋습니다.

- 각 계정에 다중 인증(MFA)을 사용하세요.
- SSL/TLS를 사용하여 AWS 리소스와 통신합니다. TLS 1.2는 필수이며 TLS 1.3을 권장합니다.
- 를 사용하여 API 및 사용자 활동 로깅을 설정합니다 AWS CloudTrail. CloudTrail 추적을 사용하여 AWS 활동을 캡처하는 방법에 대한 자세한 내용은 AWS CloudTrail 사용 설명서의 CloudTrail 추적 작업을 참조하세요.
- AWS 암호화 솔루션과 내부의 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 API를 AWS 통해에 액세스할 때 FIPS 140-3 검증 암호화 모듈이 필요한 경우 FIPS 엔드포인트를 사용합니다. 사용 가능한 FIPS 엔드포인트에 대한 자세한 내용은 Federal Information Processing Standard(FIPS) 140-3을 참조하세요.

고객의 이메일 주소와 같은 기밀 정보나 중요한 정보는 태그나 이름 필드와 같은 자유 형식 텍스트 필드에 입력하지 않는 것이 좋습니다. 여기에는 Storage Gateway 또는 기타 AWS 서비스 에서 콘솔 AWS CLI, API 또는 AWS SDKs를 사용하여 작업하는 경우가 포함됩니다. 이름에 사용되는 태그 또는 자유 형식 텍스트 필드에 입력하는 모든 데이터는 청구 또는 진단 로그에 사용될 수 있습니다. 외부 서버로 URL을 제공할 때 해당 서버에 대한 요청을 검증하기 위해 자격 증명 정보를 URL에 포함해서는 안 됩니다.

를 사용한 데이터 암호화 AWS KMS

Storage Gateway는 SSL/TLS(Secure Socket Layers/Transport Layer Security)를 사용하여 게이트웨이 어플라이언스와 AWS 스토리지 간에 전송되는 데이터를 암호화합니다. 기본적으로 Storage Gateway는 Amazon S3 관리형 암호화 키(SSE-S3)를 사용하여 Amazon S3에 저장되는 모든 데이터에 대해 서버 측 암호화를 수행합니다. Storage Gateway API를 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 사용하는 경우 대칭 키를 선택해야 합니다. Storage Gateway에서는 비대칭 키가 지원되지 않습니다. 자세한 내용은 AWS Key Management Service 개발자 안내서의 대칭 및 비대칭 키 사용을 참조하세요.

파일 공유 암호화

파일 공유의 경우 SSE-KMS를 사용하여 AWS KMS관리형 키로 객체를 암호화하도록 게이트웨이를 구성할 수 있습니다. Storage Gateway API를 사용하여 파일 공유에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은AWS Storage Gateway API 참조에서 CreateNFSFileShare를 참조하세요.

볼륨 암호화

캐시 및 저장된 볼륨의 경우 Storage Gateway API를 사용하여 AWS KMS관리형 키로 클라우드에 저장된 볼륨 데이터를 암호화하도록 Storage Gateway를 구성할 수 있습니다. 관리형 키 중 하나를 KMS 키로 지정할 수 있습니다. 볼륨을 암호화하는 데 사용하는 키는 볼륨이 생성된 후에는 변경할 수 없습니다. Storage Gateway API를 사용하여 캐시 또는 저장 볼륨에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은AWS Storage Gateway API 참조에서 CreateCachediSCSIVolume 또는 CreateStorediSCSIVolume을 참조하세요.

테이프 암호화

가상 테이프의 경우 Storage Gateway API를 사용하여 AWS KMS관리형 키로 클라우드에 저장된 테이프 데이터를 암호화하도록 Storage Gateway를 구성할 수 있습니다. 관리형 키 중 하나를 KMS 키로 지정할 수 있습니다. 테이프 데이터를 암호화하는 데 사용하는 키는 테이프가 생성된 후에는 변경할 수 없습니다. Storage Gateway API를 사용하여 가상 테이프에 기록된 데이터를 암호화하는 방법에 대한 자세한 내용은AWS Storage Gateway API 참조에서 CreateTapes를 참조하세요.

AWS KMS 를 사용하여 데이터를 암호화하는 경우 다음 사항에 유의하세요.

- 데이터는 클라우드에 암호화되어 저장됩니다. 즉, 데이터는 Amazon S3에서 암호화됩니다.
- IAM 사용자는 AWS KMS API 작업을 호출하는 데 필요한 권한이 있어야 합니다. 자세한 내용은AWS Key Management Service 개발자 안내서의 AWS KMS에서 IAM 정책 사용을 참조하세요.
- AWS AWS KMS 키를 삭제 또는 비활성화하거나 권한 부여 토큰을 취소하면 볼륨 또는 테이프의 데이터에 액세스할 수 없습니다. 자세한 내용은AWS Key Management Service 개발자 안내서에서 KMS 키 삭제를 참조하세요.

- KMS로 암호화된 볼륨에서 스냅샷을 생성하면 스냅샷이 암호화됩니다. 이때 스냅샷은 볼륨의 KMS 키를 상속합니다.
- KMS로 암호화된 스냅샷에서 새로운 볼륨을 생성하면 볼륨이 암호화됩니다. 이때 새로운 볼륨에 다른 KMS 키를 지정할 수 있습니다.

> **Note**
>
> Storage Gateway는 현재 KMS로 암호화된 볼륨이나 KMS로 암호화된 스냅샷의 복구 시점에서 암호화되지 않은 볼륨을 생성하는 것을 지원하지 않습니다.

에 대한 자세한 내용은 란 무엇입니까 AWS Key Management Service?를 AWS KMS참조하십시오.

Identity and Access Management for AWS Storage Gateway

AWS Identity and Access Management (IAM)는 관리자가 AWS 리소스에 대한 액세스를 안전하게 제어하는 데 도움이 AWS 서비스 되는 입니다. IAM 관리자는 누가 AWS SGW 리소스를 사용할 수 있는 인증(로그인) 및 권한(권한 있음)을 받을 수 있는지 제어합니다. IAM은 추가 비용 없이 사용할 수 AWS 서비스 있는 입니다.

주제

- 대상
- ID를 통한 인증
- 정책을 사용하여 액세스 관리
- IAM에서 AWS Storage Gateway 작동 방식
- Storage Gateway에 대한 자격 증명 기반 정책 예제
- 문제 해결 AWS Storage Gateway 자격 증명 및 액세스

대상

AWS Identity and Access Management (IAM)를 사용하는 방법은 역할에 따라 다릅니다.

- 서비스 사용자 - 기능에 액세스할 수 없는 경우 관리자에게 권한 요청(참조문제 해결 AWS Storage Gateway 자격 증명 및 액세스)

- 서비스 관리자 - 사용자 액세스 결정 및 권한 요청 제출(IAM에서 AWS Storage Gateway 작동 방식 참조)
- IAM 관리자 - 액세스를 관리하기 위한 정책 작성(Storage Gateway에 대한 자격 증명 기반 정책 예제 참조)

ID를 통한 인증

인증은 자격 증명 자격 증명을 AWS 사용하여에 로그인하는 방법입니다. AWS 계정 루트 사용자, IAM 사용자 또는 IAM 역할을 수임하여 인증되어야 합니다.

AWS IAM Identity Center (IAM Identity Center), Single Sign-On 인증 또는 Google/Facebook 자격 증명과 같은 자격 증명 소스의 자격 증명을 사용하여 페더레이션 자격 증명으로 로그인할 수 있습니다. 로그인하는 방법에 대한 자세한 내용은 AWS Sign-In 사용 설명서의 AWS 계정에 로그인하는 방법 섹션을 참조하세요.

프로그래밍 방식 액세스를 위해는 요청에 암호화 방식으로 서명할 수 있는 SDK 및 CLI를 AWS 제공합니다. 자세한 내용은 IAM 사용 설명서의 API 요청용AWS Signature Version 4 섹션을 참조하세요.

AWS 계정 루트 사용자

를 생성할 때 모든 AWS 서비스 및 리소스에 대한 완전한 액세스 권한이 있는 AWS 계정 theroot 사용자라는 하나의 로그인 자격 증명으로 AWS 계정시작합니다. 일상적인 태스크에 루트 사용자를 사용하지 않을 것을 강력히 권장합니다. 루트 사용자 자격 증명이 필요한 작업은 IAM 사용 설명서의 루트 사용자 자격 증명이 필요한 작업 섹션을 참조하세요.

페더레이션 ID

가장 좋은 방법은 인간 사용자에게 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 서비스 사용하여에 액세스하도록 요구하는 것입니다.

페더레이션 자격 증명은 엔터프라이즈 디렉터리, 웹 자격 증명 공급자 또는 자격 증명 소스의 자격 증명을 AWS 서비스 사용하여 Directory Service 에 액세스하는 사용자입니다. 페더레이션 ID는 임시 자격 증명을 제공하는 역할을 수임합니다.

중앙 집중식 액세스 관리를 위해 AWS IAM Identity Center를 추천합니다. 자세한 정보는 AWS IAM Identity Center 사용 설명서의 What is IAM Identity Center?를 참조하세요.

IAM 사용자 및 그룹

IAM 사용자는 단일 개인 또는 애플리케이션에 대한 특정 권한을 가진 ID입니다. 장기 자격 증명이 있는 IAM 사용자 대신 임시 자격 증명을 사용하는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 자격 증명 공급자와의 페더레이션을 사용하여 임시 자격 증명을 AWS 사용하여에 액세스하도록 인간 사용자에게 요구하기를 참조하세요.

IAM 그룹은 IAM 사용자 모음을 지정하고 대규모 사용자 집합에 대한 관리 권한을 더 쉽게 만듭니다. 자세한 내용은 IAM 사용 설명서의 IAM 사용자 사용 사례 섹션을 참조하세요.

IAM 역할

IAM 역할은 임시 자격 증명을 제공하는 특정 권한이 있는 자격 증명입니다. 사용자에서 IAM 역할(콘솔)로 전환하거나 또는 API 작업을 호출하여 역할을 수임할 수 있습니다. AWS CLI AWS 자세한 내용은 IAM 사용 설명서의 역할 수임 방법을 참조하세요.

IAM 역할은 페더레이션 사용자 액세스, 임시 IAM 사용자 권한, 교차 계정 액세스, 교차 서비스 액세스 및 Amazon EC2에서 실행되는 애플리케이션에 유용합니다. 자세한 내용은 IAM 사용 설명서의 교차 계정 리소스 액세스를 참조하세요.

정책을 사용하여 액세스 관리

정책을 AWS 생성하고 자격 증명 또는 리소스에 연결하여 AWS 에서 액세스를 제어합니다. 정책은 자격 증명 또는 리소스와 연결될 때 권한을 정의합니다.는 보안 주체가 요청할 때 이러한 정책을 AWS 평가합니다. 대부분의 정책은에 JSON 문서 AWS 로 저장됩니다. JSON 정책 문서에 대한 자세한 내용은 IAM 사용 설명서의 JSON 정책 개요 섹션을 참조하세요.

정책을 사용하여 관리자는 어떤 보안 주체가 어떤 리소스에 대해 어떤 조건에서 작업을 수행할 수 있는지 정의하여 누가 무엇을 액세스할 수 있는지 지정합니다.

기본적으로 사용자 및 역할에는 어떠한 권한도 없습니다. IAM 관리자는 IAM 정책을 생성하고 사용자가 수임할 수 있는 역할에 추가합니다. IAM 정책은 작업을 수행하기 위해 사용하는 방법과 관계없이 작업에 대한 권한을 정의합니다.

ID 기반 정책

ID 기반 정책은 ID(사용자, 사용자 그룹 또는 역할)에 연결하는 JSON 권한 정책 문서입니다. 이러한 정책은 자격 증명이 수행할 수 있는 작업, 대상 리소스 및 이에 관한 조건을 제어합니다. ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

ID 기반 정책은 인라인 정책(단일 ID에 직접 포함) 또는 관리형 정책(여러 ID에 연결된 독립 실행형 정책)일 수 있습니다. 관리형 정책 또는 인라인 정책을 선택하는 방법을 알아보려면 IAM 사용 설명서의 관리형 정책 및 인라인 정책 중에서 선택 섹션을 참조하세요.

리소스 기반 정책

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 예를 들어 IAM 역할 신뢰 정책 및 Amazon S3 버킷 정책이 있습니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다.

리소스 기반 정책은 해당 서비스에 있는 인라인 정책입니다. 리소스 기반 정책에서는 IAM의 AWS 관리형 정책을 사용할 수 없습니다.

기타 정책 유형

AWS 는 보다 일반적인 정책 유형에서 부여한 최대 권한을 설정할 수 있는 추가 정책 유형을 지원합니다.

- 권한 경계 - ID 기반 정책에서 IAM 엔터티에 부여할 수 있는 최대 권한을 설정합니다. 자세한 정보는 IAM 사용 설명서의 IAM 엔터티의 권한 범위를 참조하세요.
- 서비스 제어 정책(SCP) - AWS Organizations내 조직 또는 조직 단위에 대한 최대 권한을 지정합니다. 자세한 내용은AWS Organizations 사용 설명서의 서비스 제어 정책을 참조하세요.
- 리소스 제어 정책(RCP) – 계정의 리소스에 사용할 수 있는 최대 권한을 설정합니다. 자세한 내용은 AWS Organizations 사용 설명서의 리소스 제어 정책(RCP)을 참조하세요.
- 세션 정책 – 역할 또는 페더레이션 사용자에 대해 임시 세션을 프로그래밍 방식으로 생성할 때 파라미터로 전달하는 고급 정책입니다. 자세한 내용은 IAM 사용 설명서의 세션 정책을 참조하세요.

여러 정책 유형

여러 정책 유형이 요청에 적용되는 경우, 결과 권한은 이해하기가 더 복잡합니다. 에서 여러 정책 유형이 관련될 때 요청을 허용할지 여부를 AWS 결정하는 방법을 알아보려면 IAM 사용 설명서의 정책 평가 로직을 참조하세요.

IAM에서 AWS Storage Gateway 작동 방식

IAM을 사용하여 AWS SGW에 대한 액세스를 관리하기 전에 AWS SGW에서 사용할 수 있는 IAM 기능에 대해 알아봅니다.

AWS Storage Gateway와 함께 사용할 수 있는 IAM 기능

IAM 특성	AWS SGW 지원
자격 증명 기반 정책	예
리소스 기반 정책	아니요
정책 작업	예
정책 리소스	예
정책 조건 키(서비스별)	예
ACL	아니요
ABAC(정책 내 태그)	부분적
임시 자격 증명	예
전달 액세스 세션(FAS)	예
서비스 역할	예
서비스 연결 역할	예

AWS SGW 및 기타 AWS 서비스가 대부분의 IAM 기능과 작동하는 방식을 개괄적으로 알아보려면 IAM 사용 설명서의 AWS IAM으로 작업하는 서비스를 참조하세요.

AWS SGW에 대한 자격 증명 기반 정책

ID 기반 정책 지원: 예

ID 기반 정책은 IAM 사용자, 사용자 그룹 또는 역할과 같은 ID에 연결할 수 있는 JSON 권한 정책 문서입니다. 이러한 정책은 사용자 및 역할이 어떤 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 제어합니다. 자격 증명 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서에서 고객 관리형 정책으로 사용자 지정 IAM 권한 정의를 참조하세요.

IAM ID 기반 정책을 사용하면 허용되거나 거부되는 작업과 리소스뿐 아니라 작업이 허용되거나 거부되는 조건을 지정할 수 있습니다. JSON 정책에서 사용할 수 있는 모든 요소에 대해 알아보려면 IAM 사용 설명서의 IAM JSON 정책 요소 참조를 참조하세요.

AWS SGW의 자격 증명 기반 정책 예제

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Storage Gateway에 대한 자격 증명 기반 정책 예제.

AWS SGW 내 리소스 기반 정책

리소스 기반 정책 지원: 아니요

리소스 기반 정책은 리소스에 연결하는 JSON 정책 설명서입니다. 리소스 기반 정책의 예제는 IAM 역할 신뢰 정책과 Amazon S3 버킷 정책입니다. 리소스 기반 정책을 지원하는 서비스에서 서비스 관리자는 이러한 정책을 사용하여 특정 리소스에 대한 액세스를 통제할 수 있습니다. 정책이 연결된 리소스의 경우 정책은 지정된 보안 주체가 해당 리소스와 어떤 조건에서 어떤 작업을 수행할 수 있는지를 정의합니다. 리소스 기반 정책에서 보안 주체를 지정해야 합니다. 보안 주체에는 계정, 사용자, 역할, 페더레이션 사용자 또는이 포함될 수 있습니다 AWS 서비스.

교차 계정 액세스를 활성화하려는 경우, 전체 계정이나 다른 계정의 IAM 개체를 리소스 기반 정책의 보안 주체로 지정할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 IAM에서 교차 계정 리소스 액세스를 참조하세요.

AWS SGW에 대한 정책 작업

정책 작업 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

JSON 정책의 `Action`요소는 정책에서 액세스를 허용하거나 거부하는 데 사용할 수 있는 작업을 설명합니다. 연결된 작업을 수행할 수 있는 권한을 부여하기 위한 정책에 작업을 포함하세요.

AWS SGW 작업 목록을 보려면 서비스 승인 참조의AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW의 정책 작업은 작업 앞에 다음 접두사를 사용합니다.

```
sgw
```

단일 문에서 여러 작업을 지정하려면 쉼표로 구분합니다.

```
"Action": [
      "sgw:action1",
      "sgw:action2"
         ]
```

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Storage Gateway에 대한 자격 증명 기반 정책 예제.

AWS SGW에 대한 정책 리소스

정책 리소스 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Resource` JSON 정책 요소는 작업이 적용되는 하나 이상의 객체를 지정합니다. 모범 사례에 따라 Amazon 리소스 이름(ARN)을 사용하여 리소스를 지정합니다. 리소스 수준 권한을 지원하지 않는 작업의 경우, 와일드카드(*)를 사용하여 해당 문이 모든 리소스에 적용됨을 나타냅니다.

```
"Resource": "*"
```

AWS SGW 리소스 유형 및 해당 ARNs 목록을 보려면 서비스 승인 참조의 Resources Defined by AWS Storage Gateway를 참조하세요. 각 리소스의 ARN을 지정할 수 있는 작업을 알아보려면AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Storage Gateway에 대한 자격 증명 기반 정책 예제.

AWS SGW에 사용되는 정책 조건 키

서비스별 정책 조건 키 지원: 예

관리자는 AWS JSON 정책을 사용하여 누가 무엇에 액세스할 수 있는지 지정할 수 있습니다. 즉, 어떤 보안 주체가 어떤 리소스와 어떤 조건에서 작업을 수행할 수 있는지를 지정할 수 있습니다.

`Condition` 요소는 정의된 기준에 따라 문이 실행되는 시기를 지정합니다. 같음(equals) 또는 미만(less than)과 같은 조건 연산자를 사용하여 정책의 조건을 요청의 값과 일치시키는 조건식을 생성할 수

있습니다. 모든 AWS 전역 조건 키를 보려면 IAM 사용 설명서의 AWS 전역 조건 컨텍스트 키를 참조하세요.

AWS SGW 조건 키 목록을 보려면 서비스 승인 참조의 조건 키 for AWS Storage Gateway를 참조하세요. 조건 키를 사용할 수 있는 작업 및 리소스를 알아보려면AWS Storage Gateway에서 정의한 작업을 참조하세요.

AWS SGW 자격 증명 기반 정책의 예를 보려면 섹션을 참조하세요Storage Gateway에 대한 자격 증명 기반 정책 예제.

AWS SGWACLs

ACL 지원: 아니요

액세스 제어 목록(ACL)은 어떤 보안 주체(계정 멤버, 사용자 또는 역할)가 리소스에 액세스할 수 있는 권한을 가지고 있는지를 제어합니다. ACL은 JSON 정책 문서 형식을 사용하지 않지만 리소스 기반 정책과 유사합니다.

AWS SGW를 사용한 ABAC

ABAC 지원(정책의 태그): 부분적

속성 기반 액세스 제어(ABAC)는 태그라고 불리는 속성을 기반으로 권한을 정의하는 권한 부여 전략입니다. IAM 엔터티 및 AWS 리소스에 태그를 연결한 다음 보안 주체의 태그가 리소스의 태그와 일치할 때 작업을 허용하는 ABAC 정책을 설계할 수 있습니다.

태그에 근거하여 액세스를 제어하려면 `aws:ResourceTag/`*`key-name`*, `aws:RequestTag/`*`key-name`*또는 `aws:TagKeys`조건 키를 사용하여 정책의 조건 요소에 태그 정보를 제공합니다.

서비스가 모든 리소스 유형에 대해 세 가지 조건 키를 모두 지원하는 경우, 값은 서비스에 대해 예입니다. 서비스가 일부 리소스 유형에 대해서만 세 가지 조건 키를 모두 지원하는 경우, 값은 부분적입니다.

ABAC에 대한 자세한 내용은 IAM 사용 설명서의 ABAC 권한 부여를 통한 권한 정의를 참조하세요. ABAC 설정 단계가 포함된 자습서를 보려면 IAM 사용 설명서의 속성 기반 액세스 제어(ABAC) 사용을 참조하세요.

AWS SGW에서 임시 자격 증명 사용

임시 자격 증명 지원: 예

임시 자격 증명은 AWS 리소스에 대한 단기 액세스를 제공하며 페더레이션 또는 전환 역할을 사용할 때 자동으로 생성됩니다. 장기 액세스 키를 사용하는 대신 임시 자격 증명을 동적으로 생성하는 것이

AWS 좋습니다. 자세한 내용은 IAM 사용 설명서의 IAM의 임시 보안 자격 증명 및 IAM으로 작업하는 AWS 서비스 섹션을 참조하세요.

AWS SGW에 대한 전달 액세스 세션

전달 액세스 세션(FAS) 지원: 예

전달 액세스 세션(FAS)은를 호출하는 보안 주체의 권한을 다운스트림 서비스에 AWS 서비스 대한 요청과 AWS 서비스함께 사용합니다. FAS 요청 시 정책 세부 정보는 전달 액세스 세션을 참조하세요.

AWS SGW에 대한 서비스 역할

서비스 역할 지원: 예

서비스 역할은 서비스가 사용자를 대신하여 작업을 수행하는 것으로 가정하는 IAM 역할입니다. IAM 관리자는 IAM 내에서 서비스 역할을 생성, 수정 및 삭제할 수 있습니다. 자세한 내용은 IAM 사용 설명서의 AWS 서비스 AWS에 권한을 위임할 역할 생성을 참조하세요.

> **Warning**
>
> 서비스 역할에 대한 권한을 변경하면 AWS SGW 기능이 중단될 수 있습니다. AWS SGW가 관련 지침을 제공하는 경우에만 서비스 역할을 편집합니다.

AWS SGW에 대한 서비스 연결 역할

서비스 연결 역할 지원: 예

서비스 연결 역할은에 연결된 서비스 역할의 한 유형입니다 AWS 서비스. 서비스는 사용자를 대신하여 작업을 수행하기 위해 역할을 수임할 수 있습니다. 서비스 연결 역할은에 표시 AWS 계정 되며 서비스가 소유합니다. IAM 관리자는 서비스 연결 역할의 권한을 볼 수 있지만 편집은 할 수 없습니다.

서비스 연결 역할 생성 또는 관리에 대한 자세한 내용은 IAM으로 작업하는AWS 서비스를 참조하세요. 서비스 연결 역할 열에서 Yes가 포함된 서비스를 테이블에서 찾습니다. 해당 서비스에 대한 서비스 연결 역할 설명서를 보려면 예(Yes) 링크를 선택합니다.

Storage Gateway에 대한 자격 증명 기반 정책 예제

기본적으로 사용자 및 역할에는 AWS SGW 리소스를 생성하거나 수정할 수 있는 권한이 없습니다. 사용자에게 사용자가 필요한 리소스에서 작업을 수행할 권한을 부여하려면 IAM 관리자가 IAM 정책을 생성하면 됩니다.

이러한 예제 JSON 정책 문서를 사용하여 IAM ID 기반 정책을 생성하는 방법을 알아보려면 IAM 사용 설명서의 IAM 정책 생성(콘솔)을 참조하세요.

각 리소스 유형에 대한 ARNs 형식을 포함하여 AWS SGW에서 정의한 작업 및 리소스 유형에 대한 자세한 내용은 서비스 승인 참조의 Actions, Resources, and Condition Keys for AWS Storage Gateway를 참조하세요.

주제

- 정책 모범 사례
- AWS SGW 콘솔 사용
- 사용자가 자신의 고유한 권한을 볼 수 있도록 허용

정책 모범 사례

자격 증명 기반 정책에 따라 계정에서 사용자가 AWS SGW 리소스를 생성, 액세스 또는 삭제할 수 있는지 여부가 결정됩니다. 이 작업으로 인해 AWS 계정에 비용이 발생할 수 있습니다. ID 기반 정책을 생성하거나 편집할 때는 다음 지침과 권장 사항을 따르세요.

- AWS 관리형 정책을 시작하고 최소 권한으로 전환 - 사용자 및 워크로드에 권한 부여를 시작하려면 많은 일반적인 사용 사례에 대한 권한을 부여하는 AWS 관리형 정책을 사용합니다. 에서 사용할 수 있습니다 AWS 계정. 사용 사례에 맞는 AWS 고객 관리형 정책을 정의하여 권한을 추가로 줄이는 것이 좋습니다. 자세한 내용은 IAM 사용 설명서의 AWS 관리형 정책 또는 AWS 직무에 대한 관리형 정책을 참조하세요.
- 최소 권한 적용 – IAM 정책을 사용하여 권한을 설정하는 경우, 작업을 수행하는 데 필요한 권한만 부여합니다. 이렇게 하려면 최소 권한으로 알려진 특정 조건에서 특정 리소스에 대해 수행할 수 있는 작업을 정의합니다. IAM을 사용하여 권한을 적용하는 방법에 대한 자세한 정보는 IAM 사용 설명서에 있는 IAM의 정책 및 권한을 참조하세요.
- IAM 정책의 조건을 사용하여 액세스 추가 제한 – 정책에 조건을 추가하여 작업 및 리소스에 대한 액세스를 제한할 수 있습니다. 예를 들어, SSL을 사용하여 모든 요청을 전송해야 한다고 지정하는 정책 조건을 작성할 수 있습니다. AWS 서비스와 같은 특정를 통해 사용되는 경우 조건을 사용하여 서비스 작업에 대한 액세스 권한을 부여할 수도 있습니다 CloudFormation. 자세한 내용은 IAM 사용 설명서의 IAM JSON 정책 요소: 조건을 참조하세요.
- IAM Access Analyzer를 통해 IAM 정책을 확인하여 안전하고 기능적인 권한 보장 - IAM Access Analyzer에서는 IAM 정책 언어(JSON)와 모범 사례가 정책에서 준수되도록 새로운 및 기존 정책을 확인합니다. IAM Access Analyzer는 100개 이상의 정책 확인 항목과 실행 가능한 추천을 제공하

여 안전하고 기능적인 정책을 작성하도록 돕습니다. 자세한 내용은 IAM 사용 설명서의 IAM Access Analyzer에서 정책 검증을 참조하세요.

- 다중 인증(MFA) 필요 -에서 IAM 사용자 또는 루트 사용자가 필요한 시나리오가 있는 경우 추가 보안을 위해 MFA를 AWS 계정캡니다. API 작업을 직접적으로 호출할 때 MFA가 필요하면 정책에 MFA 조건을 추가합니다. 자세한 내용은 IAM 사용 설명서의 MFA를 통한 보안 API 액세스를 참조하세요.

IAM의 모범 사례에 대한 자세한 내용은 IAM 사용 설명서의 IAM의 보안 모범 사례를 참조하세요.

AWS SGW 콘솔 사용

AWS Storage Gateway 콘솔에 액세스하려면 최소 권한 집합이 있어야 합니다. 이러한 권한은에서 AWS SGW 리소스에 대한 세부 정보를 나열하고 볼 수 있도록 허용해야 합니다 AWS 계정. 최소 필수 권한보다 더 제한적인 ID 기반 정책을 생성하는 경우, 콘솔이 해당 정책에 연결된 엔티티(사용자 또는 역할)에 대해 의도대로 작동하지 않습니다.

AWS CLI 또는 AWS API만 호출하는 사용자에게는 최소 콘솔 권한을 허용할 필요가 없습니다. 대신, 수행하려는 API 작업과 일치하는 작업에만 액세스할 수 있도록 합니다.

사용자와 역할이 여전히 AWS SGW 콘솔을 사용할 수 있도록 하려면 AWS SGW *ConsoleAccess* 또는 *ReadOnly* AWS 관리형 정책도 엔터티에 연결합니다. 자세한 내용은 IAM 사용 설명서의 사용자에게 권한 추가를 참조하세요.

사용자가 자신의 고유한 권한을 볼 수 있도록 허용

이 예제는 IAM 사용자가 자신의 사용자 ID에 연결된 인라인 및 관리형 정책을 볼 수 있도록 허용하는 정책을 생성하는 방법을 보여줍니다. 이 정책에는 콘솔에서 또는 AWS CLI 또는 AWS API를 사용하여 프로그래밍 방식으로이 작업을 완료할 수 있는 권한이 포함됩니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
```

```
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

문제 해결 AWS Storage Gateway 자격 증명 및 액세스

다음 정보를 사용하여 AWS SGW 및 IAM 작업 시 발생할 수 있는 일반적인 문제를 진단하고 수정할 수 있습니다.

주제

- AWS SGW에서 작업을 수행할 권한이 없음
- iam:PassRole을 수행하도록 인증되지 않음
- 내 외부의 사람이 내 AWS SGW 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

AWS SGW에서 작업을 수행할 권한이 없음

작업을 수행할 권한이 없다는 오류가 표시되면 작업을 수행할 수 있도록 정책을 업데이트해야 합니다.

다음의 예제 오류는 `mateojackson` IAM 사용자가 콘솔을 사용하여 가상 *`my-example-widget`* 리소스에 대한 세부 정보를 보려고 하지만 가상 `sgw:`*`GetWidget`* 권한이 없을 때 발생합니다.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 sgw:GetWidget on resource: my-example-widget
```

이 경우, sgw:*GetWidget* 작업을 사용하여 *my-example-widget* 리소스에 액세스할 수 있도록 mateojackson 사용자 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

iam:PassRole을 수행하도록 인증되지 않음

iam:PassRole 작업을 수행할 권한이 없다는 오류가 수신되면 AWS SGW에 역할을 전달할 수 있도록 정책을 업데이트해야 합니다.

일부 AWS 서비스 에서는 새 서비스 역할 또는 서비스 연결 역할을 생성하는 대신 기존 역할을 해당 서비스에 전달할 수 있습니다. 이렇게 하려면 역할을 서비스에 전달할 권한이 있어야 합니다.

다음 예시 오류는 marymajor라는 IAM 사용자가 콘솔을 사용하여 AWS SGW에서 작업을 수행하려고 하는 경우에 발생합니다. 하지만 작업을 수행하려면 서비스 역할이 부여한 권한이 서비스에 있어야 합니다. Mary는 서비스에 역할을 전달할 권한이 없습니다.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

이 경우, Mary가 iam:PassRole작업을 수행할 수 있도록 Mary의 정책을 업데이트해야 합니다.

도움이 필요한 경우 AWS 관리자에게 문의하세요. 관리자는 로그인 자격 증명을 제공한 사람입니다.

내 외부의 사람이 내 AWS SGW 리소스 AWS 계정 에 액세스하도록 허용하고 싶습니다.

다른 계정의 사용자 또는 조직 외부의 사람이 리소스에 액세스할 때 사용할 수 있는 역할을 생성할 수 있습니다. 역할을 수임할 신뢰할 수 있는 사람을 지정할 수 있습니다. 리소스 기반 정책 또는 액세스 제어 목록(ACL)을 지원하는 서비스의 경우, 이러한 정책을 사용하여 다른 사람에게 리소스에 대한 액세스 권한을 부여할 수 있습니다.

자세한 내용은 다음을 참조하세요.

- SGW AWS 가 이러한 기능을 지원하는지 여부를 알아보려면 섹션을 참조하세요IAM에서 AWS Storage Gateway 작동 방식.
- 소유 AWS 계정 한의 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 소유한 다른의 IAM 사용자에게 액세스 권한 제공을 참조 AWS 계정 하세요.

- 타사에 리소스에 대한 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 타사가 AWS 계정 소유한에 대한 액세스 권한 제공을 AWS 계정참조하세요.
- ID 페더레이션을 통해 액세스 권한을 제공하는 방법을 알아보려면 IAM 사용 설명서의 외부에서 인증된 사용자에게 액세스 권한 제공(ID 페더레이션)을 참조하세요.
- 크로스 계정 액세스에 대한 역할과 리소스 기반 정책 사용의 차이점을 알아보려면 IAM 사용 설명서의 IAM의 크로스 계정 리소스 액세스를 참조하세요.

AWS Storage Gateway에 대한 규정 준수 검증

타사 감사자는 여러 규정 준수 프로그램의 일환으로 AWS Storage Gateway의 보안 및 AWS 규정 준수를 평가합니다. 여기에는 SOC, PCI, ISO, FedRAMP, HIPAA, MTSC, C5, K-ISMS, ENS High, OSPAR, HITRUST CSF가 포함됩니다.

특정 규정 준수 프로그램 범위의 AWS 서비스 목록은 규정 준수 프로그램 AWS 제공 범위 내 서비스규정 준수 프로그램 . 일반 정보는 AWS 규정 준수 프로그램.

를 사용하여 타사 감사 보고서를 다운로드할 수 있습니다 AWS Artifact. 자세한 내용은 Downloading Reports inDownloading AWS Artifact을 참조하세요.

Storage Gateway 사용 시 규정 준수 책임은 데이터의 민감도, 회사의 규정 준수 목표 및 관련 법률과 규정에 따라 결정됩니다. AWS 에서는 규정 준수에 도움이 되도록 다음과 같은 리소스를 제공합니다.

- 보안 및 규정 준수 퀵 스타트 가이드 -이 배포 가이드에서는 아키텍처 고려 사항에 대해 설명하고 보안 및 규정 준수 중심 기준 환경을 배포하기 위한 단계를 제공합니다 AWS.
- HIPAA 보안 및 규정 준수를 위한 설계 백서 -이 백서에서는 기업이 AWS 를 사용하여 HIPAA 준수 애플리케이션을 생성하는 방법을 설명합니다.
- AWS 규정 준수 리소스 -이 워크북 및 가이드 모음은 산업 및 위치에 적용될 수 있습니다.
- AWS Config 개발자 안내서의 규칙을 사용하여 리소스 평가 -이 AWS Config 서비스는 리소스 구성이 내부 관행, 업계 지침 및 규정을 얼마나 잘 준수하는지 평가합니다.
- AWS Security Hub CSPM -이 AWS 서비스는 보안 업계 표준 및 모범 사례 준수 여부를 확인하는 데 도움이 AWS 되는 내 보안 상태에 대한 포괄적인 보기를 제공합니다.

Resilience in AWS Storage Gateway

AWS 글로벌 인프라는 AWS 리전 및 가용 영역을 중심으로 구축됩니다.

AWS 리전 는 데이터 센터가 클러스터링되는 전 세계의 물리적 위치입니다. 논리적 데이터 센터의 각 그룹을 가용 영역(AZ)이라고 합니다. 각 AWS 리전 은 지리적 영역 내에서 물리적으로 분리되어 격리된 최소 3개의 AZ로 구성됩니다. 리전을 단일 데이터 센터로 정의하는 다른 클라우드 공급자와 달리 모든의 다중 AZ 설계는 고유한 이점을 AWS 리전 제공합니다. 각 AZ는 독립적인 전원, 냉각, 물리적 보안을 갖추고 있으며 이중화된 초저지연 네트워크를 통해 연결됩니다. 고가용성에 중점을 두고 배포해야 하는 경우, 서비스 및 리소스를 여러 AZ에 구성하여 내결함성을 높일 수 있습니다.

AWS 리전 는 최고 수준의 인프라 보안, 규정 준수 및 데이터 보호를 충족합니다. AZ 간에 전송되는 모든 트래픽은 암호화됩니다. 네트워크 성능은 AZ 간 동기식 복제를 수행하기에 충분합니다. AZ를 사용하면 고가용성을 위한 서비스 및 리소스를 쉽게 분할할 수 있습니다. 배포가 여러 AZ에 분할되어 있으면 정전, 낙뢰, 토네이도, 지진 등의 문제로부터 리소스를 더 잘 격리하고 보호할 수 있습니다. AZ는 물리적으로 다른 AZ와 의미 있는 거리만큼 떨어져 있지만, 모두 서로 100km(60마일) 이내에 있습니다.

AWS 리전 및 가용 영역에 대한 자세한 내용은 AWS 글로벌 인프라를 참조하세요.

AWS 글로벌 인프라 외에도 Storage Gateway는 데이터 복원성과 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 Gateway와 함께 VMware vSphere High Availability 사용 단원을 참조하십시오.
- 가상 테이프를 S3 Glacier Flexible Retrieval에 아카이브합니다. 자세한 내용은 가상 테이프 보관 단원을 참조하십시오.

인프라 보안 in AWS Storage Gateway

관리형 서비스인 AWS Storage Gateway는 Amazon Web Services: 보안 프로세스 개요 백서에 설명된 AWS 글로벌 네트워크 보안 절차로 보호됩니다.

AWS 에서 게시한 API 호출을 사용하여 네트워크를 통해 Storage Gateway에 액세스합니다. 클라이언트가 Transport Layer Security(TLS) 1.2를 지원해야 합니다. 클라이언트는 Ephemeral Diffie-Hellman(DHE) 또는 Elliptic Curve Ephemeral Diffie-Hellman(ECDHE)과 같은 Perfect Forward Secrecy(PFS)가 포함된 암호 제품군도 지원해야 합니다. Java 7 이상의 최신 시스템은 대부분 이러한 모드를 지원합니다.

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

> **Note**
>
> AWS Storage Gateway 어플라이언스를 관리형 가상 머신으로 취급해야 하며 어떤 식으로든 설치에 액세스하거나 수정하려고 시도해서는 안 됩니다. 일반적인 게이트웨이 업데이트 메커니즘이 아닌 다른 방법을 사용하여 스캔 소프트웨어를 설치하거나 소프트웨어 패키지를 업데이트하려고 하면 게이트웨이가 오작동할 수 있으며 게이트웨이 지원 또는 수정 기능에 영향을 미칠 수 있습니다.
>
> AWS 정기적으로 CVEs를 검토, 분석 및 수정합니다. 이러한 문제에 대한 수정 사항은 일반적인 소프트웨어 릴리스 주기의 일부로 Storage Gateway에 통합됩니다. 이러한 수정 사항은 일반적으로 예정된 유지 관리 기간 동안 일반 게이트웨이 업데이트 프로세스의 일부로 적용됩니다. 게이트웨이 업데이트에 대한 자세한 내용은 섹션을 참조하세요게이트웨이 업데이트 관리.

AWS 보안 모범 사례

AWS 는 자체 보안 정책을 개발하고 구현할 때 고려해야 할 여러 보안 기능을 제공합니다. 다음 모범 사례는 일반적인 지침이며 완벽한 보안 솔루션을 나타내지는 않습니다. 이러한 사례는 사용자의 환경에 적절하지 않거나 충분하지 않을 수 있으므로 규정이 아닌 참고용으로만 사용하세요. 자세한 내용은 AWS 보안 모범 사례를 참조하세요.

에서 로깅 및 모니터링 AWS Storage Gateway

Storage Gateway는 Storage Gateway에서 사용자 AWS CloudTrail, 역할 또는 서비스가 수행한 작업에 대한 레코드를 제공하는 AWS 서비스와 통합됩니다. CloudTrail은 Storage Gateway에 대한 API 호출을 이벤트로 캡처합니다. 캡처된 호출에는 Storage Gateway 콘솔에서의 호출과 Storage Gateway API 작업에 대한 코드 호출이 포함됩니다. 추적을 생성하면 Storage Gateway용 이벤트를 포함한 CloudTrail 이벤트를 지속적으로 Amazon S3 버킷에 배포할 수 있습니다. 추적을 구성하지 않은 경우에도 이벤트 기록에서 CloudTrail 콘솔의 최신 이벤트를 볼 수 있습니다. CloudTrail에서 수집한 정보를 사용하여 Storage Gateway에 수행된 요청, 요청이 수행된 IP 주소, 요청을 수행한 사람, 요청이 수행된 시간 및 추가 세부 정보를 확인할 수 있습니다.

CloudTrail에 대한 자세한 내용은 AWS CloudTrail 사용 설명서를 참조하세요.

CloudTrail의 Storage Gateway 정보

CloudTrail은 계정을 생성할 때 Amazon Web Services 계정에서 활성화됩니다. Storage Gateway에서 활동이 발생하면 해당 활동은 이벤트 기록의 다른 AWS 서비스 이벤트와 함께 CloudTrail 이벤트에 기

록됩니다. Amazon Web Services 계정에서 최신 이벤트를 확인, 검색 및 다운로드할 수 있습니다. 자세한 설명은 CloudTrail 이벤트 기록으로 이벤트 보기를 참조하세요.

Storage Gateway에 대한 이벤트를 포함하여 Amazon Web Services 계정에 이벤트를 지속적으로 기록하려면 추적을 생성합니다. CloudTrail은 추적을 사용하여 Amazon S3 버킷으로 로그 파일을 전송할 수 있습니다. 기본적으로 콘솔에서 추적을 생성하면 추적이 모든 AWS 리전에 적용됩니다. 추적은 AWS 파티션에 있는 모든 리전의 이벤트를 로깅하고 지정된 Amazon S3 버킷으로 로그 파일을 전송합니다. 또한 CloudTrail 로그에서 수집된 이벤트 데이터를 추가로 분석하고 조치를 취하도록 다른 AWS 서비스를 구성할 수 있습니다. 자세한 내용은 다음 자료를 참조하세요.

- 추적 생성 개요
- CloudTrail 지원 서비스 및 통합
- CloudTrail에서 Amazon SNS 알림 구성
- 여러 리전으로부터 CloudTrail 로그 파일 받기 및 여러 계정으로부터 CloudTrail 로그 파일 받기

모든 Storage Gateway 작업은 로깅되며 작업 주제에서 문서화됩니다. 예를 들어 `ActivateGateway`, `ListGateways` 및 `ShutdownGateway` 작업을 직접적으로 호출하면 CloudTrail 로그 파일에 항목이 생성됩니다.

모든 이벤트 또는 로그 항목에는 요청을 생성했던 사용자에 관한 정보가 포함됩니다. ID 정보를 이용하면 다음을 쉽게 판단할 수 있습니다.

- 요청이 루트 또는 AWS Identity and Access Management (IAM) 사용자 자격 증명으로 이루어졌는지 여부입니다.
- 역할 또는 페더레이션 사용자의 임시 자격 증명을 사용하여 요청이 생성되었는지 여부.
- 요청이 다른 AWS 서비스에서 이루어졌는지 여부입니다.

자세한 설명은 CloudTrail userIdentity 요소를 참조하세요.

Storage Gateway 로그 파일 항목 이해

추적이란 지정한 Amazon S3 버킷에 이벤트를 로그 파일로 전송할 수 있도록 하는 구성입니다. CloudTrail 로그 파일에는 하나 이상의 로그 항목이 포함될 수 있습니다. 이벤트는 모든 소스로부터의 단일 요청을 나타내며 요청 작업, 작업 날짜와 시간, 요청 파라미터 등에 대한 정보가 들어 있습니다. CloudTrail 로그 파일은 퍼블릭 API 직접 호출의 주문 스택 트레이스가 아니므로 특정 순서로 표시되지 않습니다.

다음 예제는 작업을 보여주는 CloudTrail 로그 항목이 나타냅니다.

```
{ "Records": [{
                "eventVersion": "1.02",
                "userIdentity": {
                "type": "IAMUser",
                "principalId": "AIDAII5AUEPBH2M7JTNVC",
                "arn": "arn:aws:iam::111122223333:user/StorageGateway-team/JohnDoe",
                "accountId": "111122223333",
                "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
                 "userName": "JohnDoe"
               },
                  "eventTime": "2014-12-04T16:19:00Z",
                  "eventSource": "storagegateway.amazonaws.com",
                  "eventName": "ActivateGateway",
                  "awsRegion": "us-east-2",
                  "sourceIPAddress": "192.0.2.0",
                  "userAgent": "aws-cli/1.6.2 Python/2.7.6 Linux/2.6.18-164.el5",
                   "requestParameters": {
                                          "gatewayTimezone": "GMT-5:00",
                                          "gatewayName": "cloudtrailgatewayvtl",
                                          "gatewayRegion": "us-east-2",
                                          "activationKey": "EHFBX-1NDD0-P0IVU-PI259-
DHK88",
                                          "gatewayType": "VTL"
                                               },
                                               "responseElements": {
                                                                      "gatewayARN":
 "arn:aws:storagegateway:us-east-2:111122223333:gateway/cloudtrailgatewayvtl"
                                               },
                                               "requestID":
 "54BTFGNQI71987UJD2IHTCT8NF1Q8GLLE1QEU3KPGG6F0KSTAUU0",
                                               "eventID": "635f2ea2-7e42-45f0-
bed1-8b17d7b74265",
                                               "eventType": "AwsApiCall",
                                               "apiVersion": "20130630",
                                               "recipientAccountId": "444455556666"
             }]
}
```

다음 예는 ListGateways 작업을 보여주는 CloudTrail 로그 항목을 보여줍니다.

```
{
```

```
 "Records": [{
              "eventVersion": "1.02",
              "userIdentity": {
                               "type": "IAMUser",
                               "principalId": "AIDAII5AUEPBH2M7JTNVC",
                               "arn": "arn:aws:iam::111122223333:user/StorageGateway-
team/JohnDoe",
                               "accountId:" 111122223333", " accessKeyId ":"
 AKIAIOSFODNN7EXAMPLE",
                               " userName ":" JohnDoe "
                               },

                               " eventTime ":" 2014 - 12 - 03T19: 41: 53Z ",
                               " eventSource ":" storagegateway.amazonaws.com ",
                               " eventName ":" ListGateways ",
                               " awsRegion ":" us-east-2 ",
                               " sourceIPAddress ":" 192.0.2.0 ",
                               " userAgent ":" aws - cli / 1.6.2 Python / 2.7.6
 Linux / 2.6.18 - 164.el5 ",
                               " requestParameters ":null,
                               " responseElements ":null,
                               "requestID ":"
 6U2N42CU37KAO8BG6V1I23FRSJ1Q8GLLE1QEU3KPGG6F0KSTAUU0 ",
                               " eventID ":" f76e5919 - 9362 - 48ff - a7c4 -
 d203a189ec8d ",
                               " eventType ":" AwsApiCall ",
                               " apiVersion ":" 20130630 ",
                               " recipientAccountId ":" 444455556666"
             }]
}
```

게이트웨이 문제 해결

다음에서 게이트웨이, 호스트 플랫폼, 가상 테이프, 고가용성, 데이터 복구 및 보안과 관련된 모범 사례 및 문제 해결에 관한 정보를 찾을 수 있습니다. 온프레미스 게이트웨이 문제 해결 정보는 지원되는 가상화 플랫폼에 배포된 게이트웨이를 다룹니다. 고가용성 문제에 대한 문제 해결 정보는 VMware vSphere HA(고가용성) 플랫폼에서 실행 중인 게이트웨이를 다룹니다.

주제

- 문제 해결: 게이트웨이 오프라인 문제 - Storage Gateway 콘솔에서 게이트웨이가 오프라인으로 표시될 수 있는 문제를 진단하는 방법에 대해 알아봅니다.
- 문제 해결: 게이트웨이 활성화 중 내부 오류 발생 - Storage Gateway 활성화를 시도할 때 내부 오류 메시지가 표시되는 경우에 취해야 할 조치에 대해 알아봅니다.
- 온프레미스 게이트웨이 문제 해결 - 온프레미스 게이트웨이에서 발생할 수 있는 일반적인 문제와 문제 해결을 지원하기 위해 지원 가 게이트웨이에 연결하도록 허용하는 방법에 대해 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 EC2에 배포된 게이트웨이로 작업할 때 발생할 수 있는 일반적인 문제에 대한 정보를 찾을 수 있습니다.
- 하드웨어 어플라이언스 문제 해결 - Storage Gateway 하드웨어 어플라이언스에서 발생할 수 있는 문제를 해결하는 방법에 대해 알아봅니다.
- 가상 테이프 관련 문제 해결 - 가상 테이프에 예기치 않은 문제가 발생하는 경우 취할 수 있는 조치에 대해 알아봅니다.
- 고가용성 문제 해결 - VMware HA 환경에 배포된 게이트웨이에 문제가 발생하는 경우 취해야 할 조치에 대해 알아봅니다.

문제 해결: 게이트웨이 오프라인 문제

다음 문제 해결 정보를 참조하여 AWS Storage Gateway 콘솔에서 게이트웨이가 오프라인 상태인 것으로 표시되는 경우에 취해야 할 조치를 결정하세요.

다음 중 하나 이상의 이유로 게이트웨이가 오프라인으로 표시될 수 있습니다.

- 게이트웨이가 Storage Gateway 서비스 엔드포인트에 연결할 수 없습니다.
- 게이트웨이가 예기치 않게 종료되었습니다.

- 게이트웨이와 연결된 캐시 디스크가 연결 해제 또는 수정되었거나 실패했습니다.

게이트웨이를 다시 온라인 상태로 되돌리려면 게이트웨이를 오프라인 상태로 만든 문제를 파악하여 해결합니다.

연결된 방화벽 또는 프록시 확인

프록시를 사용하도록 게이트웨이를 구성했거나 게이트웨이를 방화벽 뒤에 배치한 경우 프록시 또는 방화벽의 액세스 규칙을 검토합니다. 프록시 또는 방화벽은 Storage Gateway에 필요한 네트워크 포트 및 서비스 엔드포인트와의 트래픽을 허용해야 합니다. 자세한 내용은 네트워크 및 방화벽 요구 사항을 참조하세요.

게이트웨이 트래픽에 대해 SSL 또는 딥패킷 검사가 진행 중인지 확인

게이트웨이와 간의 네트워크 트래픽에 대해 SSL 또는 딥 패킷 검사가 현재 수행 중인 AWS경우 게이트웨이가 필요한 서비스 엔드포인트와 통신하지 못할 수 있습니다. 게이트웨이를 다시 온라인 상태로 되돌리려면 검사를 비활성화해야 합니다.

하이퍼바이저 호스트의 정전 또는 하드웨어 장애 확인

게이트웨이의 하이퍼바이저 호스트에서 정전 또는 하드웨어 장애가 발생하면 게이트웨이가 예기치 않게 종료되어 연결이 불가능해질 수 있습니다. 전원 및 네트워크 연결을 복원하면 게이트웨이에 다시 연결할 수 있게 됩니다.

게이트웨이가 다시 온라인 상태가 되면 데이터 복구 조치를 취해야 합니다. 자세한 내용은 데이터 복구 모범 사례를 참조하세요.

연결된 캐시 디스크에 문제가 있는지 확인

게이트웨이와 연결된 캐시 디스크 중 하나 이상이 제거, 변경 또는 크기 조정되었거나 손상된 경우 게이트웨이가 오프라인 상태가 될 수 있습니다.

하이퍼바이저 호스트에서 작동 중인 캐시 디스크를 제거한 경우

1. 게이트웨이를 종료합니다.
2. 디스크를 다시 추가합니다.

> **Note**
>
> 동일한 디스크 노드에 디스크를 추가해야 합니다.

3. 게이트웨이를 다시 시작합니다.

캐시 디스크가 손상되었거나 교체되었거나 크기가 조정된 경우

1. 게이트웨이를 종료합니다.
2. 캐시 디스크를 재설정합니다.
3. 캐시 스토리지를 위해 디스크를 재구성합니다.
4. 게이트웨이를 다시 시작합니다.

Tape Gateway의 손상된 캐시 디스크 문제 해결에 대한 자세한 내용은 장애가 있는 캐시 디스크에서 가상 테이프를 복구해야 하는 경우를 참조하세요.

문제 해결: 게이트웨이 활성화 중 내부 오류 발생

Storage Gateway 활성화 요청은 두 개의 네트워크 경로를 통과합니다. 클라이언트에서 보낸 수신 활성화 요청은 포트 80을 통해 게이트웨이의 가상 머신(VM) 또는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결됩니다. 게이트웨이가 활성화 요청을 성공적으로 수신하면 게이트웨이는 Storage Gateway 엔드포인트와 통신하여 활성화 키를 받습니다. 게이트웨이가 Storage Gateway 엔드포인트에 연결할 수 없는 경우 게이트웨이는 내부 오류 메시지를 표시하며 클라이언트에 응답합니다.

다음 문제 해결 정보를 참조하여 AWS Storage Gateway를 활성화하려고 할 때 내부 오류 메시지가 표시되는 경우에 취해야 할 조치를 결정하세요.

> **Note**
>
> - 최신 가상 머신 이미지 파일 또는 Amazon Machine Image(AMI) 버전을 사용하여 새 게이트웨이를 배포해야 합니다. 오래된 AMI를 사용하는 게이트웨이를 활성화하려고 하면 내부 오류가 발생합니다.
> - AMI를 다운로드하기 전에 배포하려는 올바른 게이트웨이 유형을 선택해야 합니다. 각 게이트웨이 유형의 .ova 파일과 AMI는 서로 다르므로 서로 바꾸어 사용할 수 없습니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필수 포트 확인

온프레미스에 배포된 게이트웨이의 경우 로컬 방화벽에서 포트가 열려 있는지 확인합니다. Amazon EC2 인스턴스에 배포된 게이트웨이의 경우 인스턴스의 보안 그룹에서 포트가 열려 있는지 확인합니다. 포트가 열려 있는지 확인하려면 서버의 퍼블릭 엔드포인트에서 텔넷 명령을 실행합니다. 이 서버는 게이트웨이와 동일한 서브넷에 있어야 합니다. 예를 들어 다음 텔넷 명령은 포트 443에 대한 연결을 테스트합니다.

```
telnet d4kdq0yaxexbo.cloudfront.net 443
telnet storagegateway.region.amazonaws.com 443
telnet dp-1.storagegateway.region.amazonaws.com 443
telnet proxy-app.storagegateway.region.amazonaws.com 443
telnet client-cp.storagegateway.region.amazonaws.com 443
telnet anon-cp.storagegateway.region.amazonaws.com 443
```

게이트웨이 자체가 엔드포인트에 접속할 수 있는지 확인하려면 게이트웨이의 로컬 VM 콘솔에 액세스합니다(온프레미스에 배포된 게이트웨이의 경우). 또는 게이트웨이 인스턴스에 SSH로 접속할 수 있습니다(Amazon EC2에 배포된 게이트웨이의 경우). 그런 다음 네트워크 연결 테스트를 실행합니다. 테스트가 [PASSED]를 반환하는지 확인합니다. 자세한 내용은 게이트웨이가 인터넷에 연결되어 있는지 테스트를 참조하세요.

> **Note**
>
> 게이트웨이 콘솔의 기본 로그인 사용자 이름은 admin이고 기본 암호는 password입니다.

방화벽 보안으로 게이트웨이에서 퍼블릭 엔드포인트로 전송되는 패킷이 수정되지 않도록 확인

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안으로 인해 게이트웨이에서 전송된 패킷이 방해받을 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 것과 다르게 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 포트 443의 기본 활성화 엔드포인트

(anon-cp.storagegateway.region.amazonaws.com)에서 OpenSSL 명령을 실행합니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 시스템에서 실행해야 합니다.

```
$ openssl s_client -connect  anon-cp.storagegateway.region.amazonaws.com:443 -
servername anon-cp.storagegateway.region.amazonaws.com
```

> **Note**
>
> *region*을 로 바꿉니다 AWS 리전.

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
$ openssl s_client -connect anon-cp.storagegateway.us-east-2.amazonaws.com:443 -
servername anon-cp.storagegateway.us-east-2.amazonaws.com
CONNECTED(00000003)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-2.amazonaws.com
verify return:1
---
Certificate chain
 0 s:/CN=anon-cp.storagegateway.us-east-2.amazonaws.com
   i:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
 1 s:/C=US/O=Amazon/OU=Server CA 1B/CN=Amazon
   i:/C=US/O=Amazon/CN=Amazon Root CA 1
 2 s:/C=US/O=Amazon/CN=Amazon Root CA 1
   i:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
 3 s:/C=US/ST=Arizona/L=Scottsdale/O=Starfield Technologies, Inc./CN=Starfield Services
 Root Certificate Authority - G2
   i:/C=US/O=Starfield Technologies, Inc./OU=Starfield Class 2 Certification Authority
---
```

SSL 검사가 진행 중이면 다음과 같이 변경된 인증서 체인이 응답에 표시됩니다.

```
$ openssl s_client -connect  anon-cp.storagegateway.ap-southeast-1.amazonaws.com:443 -
servername anon-cp.storagegateway.ap-southeast-1.amazonaws.com
CONNECTED(00000003)
```

```
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=20:unable to get local issuer certificate
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.ap-
southeast-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.ap-southeast-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 엔드포인트에 대한 게이트웨이의 아웃바운드 트래픽은 네트워크의 방화벽에서 수행하는 검사에서 제외되어야 합니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간 편차가 지나치게 크면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 편차는 60초 이내여야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하세요.

Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이의 시간 동기화가 제대로 이루어질 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

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

Amazon VPC 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 오류 해결

Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트를 사용하여 게이트웨이를 활성화할 때 발생하는 활성화 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

필수 포트 확인

필수 포트가 로컬 방화벽(온프레미스에 배포된 게이트웨이의 경우) 또는 보안 그룹(Amazon EC2에 배포된 게이트웨이의 경우) 내에서 열려 있는지 확인합니다. 게이트웨이를 Storage Gateway VPC 엔드포인트에 연결하는 데 필요한 포트는 게이트웨이를 퍼블릭 엔드포인트에 연결할 때 필요한 포트와 다릅니다. Storage Gateway VPC 엔드포인트에 연결하려면 다음 포트가 필요합니다.

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

자세한 내용은 Storage Gateway용 VPC 엔드포인트 생성을 참조하세요.

또한 Storage Gateway VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 엔드포인트에 연결된 기본 보안 그룹에서 필수 포트를 허용하지 않을 수 있습니다. 게이트웨이의 IP 주소 범위에서 필수 포트를 통해 트래픽을 허용하는 새 보안 그룹을 생성합니다. 그런 다음 해당 보안 그룹을 VPC 엔드포인트에 연결합니다.

> **Note**
>
> Amazon VPC 콘솔을 사용하여 VPC 엔드포인트에 연결된 보안 그룹을 확인합니다. 콘솔에서 Storage Gateway VPC 엔드포인트를 확인한 후 보안 그룹 탭을 선택합니다.

필수 포트가 열려 있는지 확인하려면 Storage Gateway VPC 엔드포인트에서 텔넷 명령을 실행할 수 있습니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 서버에서 실행해야 합니다. 가용 영역을 지정하지 않은 첫 번째 DNS 이름에 대해 테스트를 실행할 수 있습니다. 예를 들어 다음 텔넷 명령은 DNS 이름 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com을 사용하여 필수 포트 연결을 테스트합니다.

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 443
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1026
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1027
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1028
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 1031
```

```
telnet vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com 2222
```

방화벽 보안으로 게이트웨이에서 Storage Gateway Amazon VPC 엔드포인트로 전송되는 패킷이 수정되지 않도록 확인

SSL 검사, 심층 패킷 검사 또는 기타 형태의 방화벽 보안으로 인해 게이트웨이에서 전송된 패킷이 방해받을 수 있습니다. SSL 인증서가 활성화 엔드포인트에서 예상하는 것과 다르게 수정되면 SSL 핸드셰이크가 실패합니다. 진행 중인 SSL 검사가 없는지 확인하려면 Storage Gateway VPC 엔드포인트에서 OpenSSL 명령을 실행합니다. 이 명령은 게이트웨이와 동일한 서브넷에 있는 시스템에서 실행해야 합니다. 각 필수 포트에 대해 명령을 실행합니다.

```
$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:443 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1026 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1028 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1031 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com

$ openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:2222 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
```

진행 중인 SSL 검사가 없는 경우 명령은 다음과 유사한 응답을 반환합니다.

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
```

```
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 CN = anon-cp.storagegateway.us-east-1.amazonaws.com
verify return:1
---
Certificate chain
 0 s:CN = anon-cp.storagegateway.us-east-1.amazonaws.com
   i:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
 1 s:C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
   i:C = US, O = Amazon, CN = Amazon Root CA 1
 2 s:C = US, O = Amazon, CN = Amazon Root CA 1
   i:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
 3 s:C = US, ST = Arizona, L = Scottsdale, O = "Starfield Technologies, Inc.", CN =
 Starfield Services Root Certificate Authority - G2
   i:C = US, O = "Starfield Technologies, Inc.", OU = Starfield Class 2 Certification
 Authority
---
```

SSL 검사가 진행 중이면 다음과 같이 변경된 인증서 체인이 응답에 표시됩니다.

```
openssl s_client -connect vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-
east-1.vpce.amazonaws.com:1027 -servername
 vpce-1234567e1c24a1fe9-62qntt8k.storagegateway.us-east-1.vpce.amazonaws.com
CONNECTED(00000005)
depth=2 C = US, O = Amazon, CN = Amazon Root CA 1
verify return:1
depth=1 C = US, O = Amazon, OU = Server CA 1B, CN = Amazon
verify return:1
depth=0 DC = com, DC = amazonaws, OU = AWS, CN = anon-cp.storagegateway.us-
east-1.amazonaws.com
verify error:num=21:unable to verify the first certificate
verify return:1
---
Certificate chain
 0 s:/DC=com/DC=amazonaws/OU=AWS/CN=anon-cp.storagegateway.us-east-1.amazonaws.com
   i:/C=IN/O=Company/CN=Admin/ST=KA/L=New town/OU=SGW/emailAddress=admin@company.com
---
```

활성화 엔드포인트는 SSL 인증서를 인식하는 경우에만 SSL 핸드셰이크를 허용합니다. 즉, 필수 포트를 통과하는 게이트웨이의 VPC 엔드포인트 아웃바운드 트래픽은 네트워크 방화벽에서 수행하는 검사에서 제외됩니다. 이러한 검사는 SSL 검사 또는 심층 패킷 검사일 수 있습니다.

게이트웨이 시간 동기화 확인

시간 편차가 지나치게 크면 SSL 핸드셰이크 오류가 발생할 수 있습니다. 온프레미스 게이트웨이의 경우 게이트웨이의 로컬 VM 콘솔을 사용하여 게이트웨이의 시간 동기화를 확인할 수 있습니다. 시간 편차는 60초 이내여야 합니다. 자세한 내용은 게이트웨이 VM 시간 동기화를 참조하세요.

Amazon EC2 인스턴스에서 호스팅되는 게이트웨이에서는 시스템 시간 관리 옵션을 사용할 수 없습니다. Amazon EC2 게이트웨이의 시간 동기화가 제대로 이루어질 수 있도록 하려면 Amazon EC2 인스턴스가 포트 UDP 및 TCP 123을 통해 다음 NTP 서버 풀 목록에 연결할 수 있는지 확인합니다.

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

HTTP 프록시 확인 및 관련 보안 그룹 설정 확인

활성화하기 전에 온프레미스 게이트웨이 VM에서 Amazon EC2의 HTTP 프록시가 포트 3128에서 Squid 프록시로 구성되어 있는지 확인합니다. 이 경우 다음 사항을 확인합니다.

- Amazon EC2의 HTTP 프록시에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이 인바운드 규칙은 게이트웨이 VM의 IP 주소에서 포트 3128의 Squid 프록시 트래픽을 허용해야 합니다.
- Amazon EC2 VPC 엔드포인트에 연결된 보안 그룹에는 인바운드 규칙이 있어야 합니다. 이러한 인바운드 규칙은 Amazon EC2의 HTTP 프록시 IP 주소에서 포트 1026-1028, 1031, 2222 및 443의 트래픽을 허용해야 합니다.

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하는 중 동일한 VPC에 Storage Gateway VPC 엔드포인트가 있을 때 발생하는 오류 해결

퍼블릭 엔드포인트를 사용하여 게이트웨이를 활성화하는 중 동일한 VPC에 Amazon Virtual Private Cloud(Amazon VPC) 엔드포인트가 있을 때 발생하는 오류를 해결하려면 다음 확인 및 구성을 수행합니다.

Storage Gateway VPC 엔드포인트에서 프라이빗 DNS 이름 활성화 설정이 활성화되어 있지 않은지 확인합니다.

프라이빗 DNS 이름 활성화가 활성화된 경우 해당 VPC에서 퍼블릭 엔드포인트로의 게이트웨이를 활성화할 수 없습니다.

프라이빗 DNS 이름 옵션을 비활성화하려면

1. Amazon VPC 콘솔을 엽니다.
2. 탐색 창에서 엔드포인트를 선택합니다.
3. Storage Gateway VPC 엔드포인트를 선택합니다.
4. 작업을 선택합니다.
5. 프라이빗 DNS 이름 관리를 선택합니다.
6. 프라이빗 DNS 이름 활성화에서 이 엔드포인트에 대해 활성화를 선택 취소합니다.
7. 프라이빗 DNS 이름 수정을 선택하여 설정을 저장합니다.

온프레미스 게이트웨이 문제 해결

온프레미스 게이트웨이에서 발생할 수 있는 일반적인 문제와 지원 를 활성화하여 게이트웨이 문제를 해결하는 방법에 대한 정보는 다음과 같습니다.

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

문제	취할 조치
게이트웨이의 IP 주소를 찾을 수 없습니다.	하이퍼바이저 클라이언트로 호스트에 접속하여 게이트웨이 IP 주소를 찾습니다. • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다. • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다. 그래도 게이트웨이 IP 주소를 찾기 어려운 경우:

문제	취할 조치
	• VM이 켜져 있는지 확인합니다. VM이 켜져 있는 경우에만 IP 주소가 게이트웨이에 할당됩니다. • VM이 스타트업을 마칠 때까지 기다리십시오. VM을 방금 켰다면 게이트웨이가 부팅 시퀀스를 마치는 데 몇 분이 걸릴 수 있습니다.
네트워크 또는 방화벽에 문제가 있습니다.	• 게이트웨이에 적절한 포트를 허용합니다. • SSL 인증서 검증/검사를 활성화해서는 안됩니다. Storage Gateway는 상호 TLS 인증을 사용하므로 타사 애플리케이션에서 어느 한쪽 인증서를 가로채거나 서명하려고 하면 실패합니다. • 방화벽 또는 라우터를 사용하여 네트워크 트래픽을 필터링 또는 제한하는 경우, 방화벽 및 라우터가 AWS로 가는 아웃바운드 통신을 위해 이 서비스 엔드포인트를 허용하도록 구성해야 합니다. 네트워크 및 방화벽 요건에 대한 자세한 내용은 네트워크 및 방화벽 요구 사항 섹션을 참조하세요.

문제	취할 조치
Storage Gateway Management Console에서 활성화 진행 버튼을 클릭하면 게이트웨이 활성화가 실패합니다.	• 클라이언트에서 VM을 ping하여 게이트웨이 VM에 액세스할 수 있는지 확인합니다. • VM이 인터넷에 네트워크로 연결되어 있는지 확인합니다. 연결되어 있지 않으면 SOCKS 프록시를 구성해야 합니다. 이에 대한 자세한 내용은 온프레미스 게이트웨이에 대한 SOCKS5 프록시 구성 섹션을 참조하세요. • 호스트의 시간이 올바른지, 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성되어 있는지, 게이트웨이 VM의 시간이 올바른지 확인합니다. 하이퍼바이저 호스트와 VM의 시간을 동기화하는 작업에 대한 자세한 내용은 Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 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 안됩니다. Storage Gateway는 상호 TLS 인증을 사용하므로 타사 애플리케이션에서 어느 한쪽 인증서를 가로채거나 서명하려고 하면 실패합니다. • VM의 RAM 용량이 최소 7.5GB인지 확인합니다. RAM 용량이 7.5GB 미만인 경우, 게이트웨이 할당이 되지 않습니다. 자세한 내용은 Tape Gateway 설정 요구 사항 단원을 참조하십시오.
업로드 버퍼 공간으로 할당된 디스크를 제거해야 합니다. 예를 들어 게이트웨이의 업로드 버퍼 공간을 줄이거나 업로드 버퍼로 사용하는 디스크에 장애가 있어 교체해야 할 경우가 있습니다.	업로드 버퍼 공간으로 할당된 디스크를 제거하는 작업에 대한 지침은 게이트웨이에서 디스크 제거 섹션을 참조하세요.

문제	취할 조치
게이트웨이와 AWS간 대역폭을 개선해야 합니다.	애플리케이션 및 게이트웨이 VM을 연결하는 것과 별도로 네트워크 어댑터(NIC) AWS 에서에 대한 인터넷 연결을 설정 AWS 하여 게이트웨이에서 로 대역폭을 개선할 수 있습니다. 이 접근 방식은에 고대역폭으로 연결되어 AWS 있고 특히 스냅샷 복원 중에 대역폭 경합을 피하려는 경우에 유용합니다. 고처리량 워크로드 요구 사항을 충족하기 위해 Direct Connect를 사용하여 온프레미스 게이트웨이와 AWS간에 전용 네트워크 연결을 설정할 수 있습니다. 게이트웨이에서 로의 연결 대역폭을 측정하려면 게이트웨이의 `CloudBytesDownloaded` 및 `CloudBytesUploaded` 지표를 AWS사용합니다. 이에 관한 자세한 내용은 Tape Gateway와 간의 성능 측정 AWS 섹션을 참조하세요. 인터넷 연결성을 개선하면 업로드 버퍼가 꽉 차지 않도록 하는 데 도움이 됩니다.

문제	취할 조치

게이트웨이로의 처리량 또는 게이트웨이로부터의 처리량이 0으로 떨어집니다.	• Storage Gateway 콘솔의 게이트웨이 탭에서 게이트웨이 VM의 IP 주소가 하이퍼바이저 클라이언트 소프트웨어(예: VMware vSphere 클라이언트 또는 Microsoft Hyper-V Manager)를 사용할 때 표시되는 것과 동일한지 확인합니다. 일치하지 않는 경우 게이트웨이 VM 종료에 표시된 대로 Storage Gateway 콘솔에서 게이트웨이를 다시 시작합니다. 다시 시작한 후에는 Storage Gateway 콘솔의 게이트웨이 탭에 있는 IP 주소 목록에 있는 주소가 하이퍼바이저 클라이언트에서 확인한 게이트웨이의 IP 주소와 일치해야 합니다.
	  • VMware ESXi의 경우, VM의 IP 주소는 요약 탭의 vSphere 클라이언트에서 찾을 수 있습니다.
	  • Microsoft Hyper-V의 경우에는 로컬 콘솔에 로그인하여 VM의 IP 주소를 찾을 수 있습니다.
	• 에 설명된 AWS 대로 게이트웨이의에 대한 연결을 확인합니다게이트웨이가 인터넷에 연결되어 있는지 테스트.
	• 게이트웨이의 네트워크 어댑터 구성을 확인하고 게이트웨이에 대해 활성화하려는 모든 인터페이스가 활성화되었는지 확인합니다. 게이트웨이의 네트워크 어댑터 구성을 보려면 게이트웨이 네트워크 구성 단원의 지침에 따라 게이트웨이의 네트워크 구성을 볼 수 있는 옵션을 선택합니다.
	
	게이트웨이와 주고받는 처리량은 Amazon CloudWatch 콘솔에서 확인할 수 있습니다. 게이트웨이 및 와의 처리량 측정에 대한 자세한 내용은 섹션을 AWS참조하세요Tape Gateway와 간의 성능 측정 AWS.

Microsoft Hyper-V에서 Storage Gateway를 가져오기(배포)하는 데 문제가 있습니다.	Microsoft Hyper-V에서 게이트웨이를 배포할 때 흔히 겪는 몇 가지 문제를 다루는 Microsoft Hyper-V 설정 관련 문제 해결 섹션을 참조하세요.
"게이트웨이의 볼륨에 기록된 데이터가 AWS에 안전하게 저장되지 않았습니다."라는 메시지가 표시됩니다.	게이트웨이 VM이 또 다른 게이트웨이 VM의 복제 또는 스냅샷으로부터 생성된 경우 이 메시지를 수신하게 됩니다. 그렇지 않은 경우 지원에 문의하세요.

지원 가 온프레미스에서 호스팅되는 게이트웨이 문제를 해결하는 데 도움이 되도록 허용

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이에 액세스 지원 하도록를 활성화하는 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이에 대한 지원 액세스는 비활성화됩니다. 호스트의 로컬 콘솔을 통해 이 액세스 권한을 제공해야 합니다. 게이트웨이에 대한 지원 액세스 권한을 부여하려면 먼저 호스트의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 지원 서버에 연결합니다.

게이트웨이에 대한 지원 액세스를 허용하려면

1. 호스트의 로컬 콘솔에 로그인합니다.

   - VMware ESXi - 자세한 내용은 VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
   - Microsoft Hyper-V - 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
2. 프롬프트에서 해당 숫자를 입력하여 게이트웨이 콘솔을 선택합니다.
3. **h**를 입력하여 사용 가능한 명령 목록을 엽니다.
4. 다음 중 하나를 수행하세요.

   - 게이트웨이에서 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령 창에 **`open-support-channel`**을 입력하여 Storage Gateway의 고객 지원에 연결합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
   - 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **`open-support-channel`**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

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

5. 지원 채널이 설정되면가 문제 해결 지원을 제공할 지원 수 지원 있도록 지원 서비스 번호를에 제공합니다.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. Amazon Web Services Support에서 지원 세션이 완료되었음을 알릴 때까지 세션을 닫지 마십시오.
7. **exit**를 입력하여 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
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다. "가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. [...] 위치에서 가상 머신 가져오기 파일을 찾을 수 없습니다. Hyper-V를 사용하여 가상 머신을 생성하고 내보낸 경우에만 가상 머신을 가져올 수 있습니다."	이 오류는 다음과 같은 이유로 발생할 수 있습니다. • 압축하지 않은 게이트웨이 소스 파일의 루트를 가리키지 않는 경우. 가상 머신 가져오기 대화 상자에 지정한 위치의 마지막 부분은 `AWS-Storage-Gateway` 여야 합니다. 예제: `C:\prod-gateway\unzippedSourceVM\AWS-Storage-Gateway\` . • 이미 게이트웨이를 배포했는데 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하지 않은 경우, 압축 해제된 게이트웨이 파일이 있는 위치에 VM이 생성되므로 이 위치에서 다시 가져올 수 없습니다. 이 문제를 해결하려면 압축을 해제한 게이트웨이 소스 파일의 새 사본을 얻어 이를 새 위치에 복사하면 됩니다. 새 위치를 가져오는 위치로 사용합니다. 압축을 푼 하나의 소스 파일 위치에서 여러 개의 게이트웨이를 생성하려는 경우 가상 머신 가져오기 대화 상자에서 가상 머신 복사를 선택하고 모든 파일 복제 확인란을 선택해야 합니다.
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다.	이미 게이트웨이를 배포하고 가상 하드 디스크 및 가상 머신 구성 파일이 저장된 기본 폴더를 다시 사용하는 경우, 이 오류가 발생합니다. 이 문제를 해결하려면 Hyper-V 설정 대화 상자의 왼쪽 패널에서 서버 아래에 새 위치를 지정합니다.

문제	취할 조치
"가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. 가져오기 작업이 [...]에서 파일을 복사하지 못했습니다. 파일이 존재합니다. (0x80070050)"	
게이트웨이를 가져오려고 하는데 다음과 같은 오류 메시지가 표시됩니다. "가상 머신을 가져오는 동안 서버 오류가 발생했습니다. 가져오기에 실패했습니다. Import failed because the virtual machine must have a new identifier. Select a new identifier and try the import again."라는 오류 메시지가 표시됩니다.	게이트웨이를 가져올 때 가상 머신 가져오기 대화 상자에서 가상 머신 복사 옵션과 모든 파일 복제 옵션을 선택하여 VM의 새 고유 ID를 생성해야 합니다.
게이트웨이 VM을 시작하려고 하는데 다음과 같은 오류 메시지가 나타납니다. “선택한 가상 머신을 시작하는 동안 오류가 발생했습니다. 하위 파티션 프로세서 설정이 상위 파티션과 호환되지 않습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 머신 ID [...])"	이 오류는 게이트웨이에 필요한 CPU와 호스트에서 사용 가능한 CPU 사이의 CPU 불일치로 인해 발생할 수 있습니다. 기본 하이퍼바이저가 VM CPU 개수를 지원하도록 해야 합니다. Storage Gateway 요구 사항에 대한 자세한 내용은 Tape Gateway 설정 요구 사항 섹션을 참조하세요.

문제	취할 조치
게이트웨이 VM을 시작하려고 하는데 다음과 같은 오류 메시지가 나타납니다. “선택한 가상 머신을 시작하는 동안 오류가 발생했습니다. 'AWS-Storage-Gateway'를 초기화할 수 없습니다. (가상 머신 ID [...]) 파티션을 생성하지 못했습니다. 요청된 서비스를 완료하는 데 필요한 시스템 리소스가 부족합니다. (0x800705AA)"	이 오류는 게이트웨이에 필요한 RAM과 호스트에서 사용 가능한 RAM 사이의 RAM 불일치로 인해 발생할 수 있습니다. Storage Gateway 요구 사항에 대한 자세한 내용은 Tape Gateway 설정 요구 사항 섹션을 참조하세요.
스냅샷 및 게이트웨이 소프트웨어 업데이트는 예상과 약간 다른 시각에 실행됩니다.	게이트웨이 VM의 클럭은 실제 시간과 약간 오차가 있을 수 있는데, 이를 클럭 드리프트라고 합니다. 로컬 게이트웨이 콘솔의 시간 동기화 옵션을 사용하여 VM의 시간을 점검하고 수정합니다. 자세한 내용은 Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화 단원을 참조하십시오.
압축 해제된 Microsoft Hyper-V Storage Gateway 파일은 호스트 파일 시스템에 저장해야 합니다.	일반적인 Microsoft Windows 서버에 액세스하듯이 호스트에 액세스합니다. 예를 들어 하이퍼바이저 호스트의 이름이 `hyperv-server` 인 경우에는 다음과 같이 UNC 경로인 `\\hyperv-server\c$` 를 사용할 수 있습니다. 이 경로는 `hyperv-server` 라는 이름을 로컬 호스트 파일에서 확인할 수 있거나 정의한다고 가정합니다.
하이퍼바이저에 접속할 때 자격 증명을 요구하는 메시지가 표시됩니다.	Sconfig.cmd 도구를 사용하여 사용자 자격 증명을 하이퍼바이저 호스트용 로컬 관리자로 추가합니다.
Broadcom 네트워크 어댑터를 사용하는 Hyper-V 호스트에 대해 가상 머신 대기열(VMQ)을 켜면 네트워크 성능이 저하될 수 있습니다.	해결 방법에 대한 자세한 내용은 Microsoft 설명서 VMQ가 켜져 있는 경우 Windows Server 2012 Hyper-V 호스트의 가상 머신에서 네트워크 성능이 저하됨을 참조하세요.

Amazon EC2 게이트웨이 문제 해결

다음 섹션에서는 Amazon EC2에 배포된 게이트웨이를 사용할 때 발생할 수 있는 일반적인 문제를 확인할 수 있습니다. 온프레미스 게이트웨이와 Amazon EC2에 배포한 게이트웨이 간의 차이점에 대한 자세한 내용은 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 섹션을 참조하세요.

주제

- 몇 분 후 게이트웨이가 활성화되지 않음
- 인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없음
- Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없음
- 스토리지 볼륨을 추가하려고 할 때 사용 가능한 디스크가 없다는 메시지가 표시되는 경우
- 업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우
- EC2 게이트웨이와 주고받는 데이터의 처리량이 0으로 떨어짐
- EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우
- Amazon EC2 직렬 콘솔을 사용하여 게이트웨이 인스턴스에 연결하려는 경우

몇 분 후 게이트웨이가 활성화되지 않음

Amazon EC2 콘솔에서 다음 사항을 확인하세요.

- 인스턴스와 연결한 보안 그룹에서 포트 80이 활성화되어 있는지 여부. 보안 그룹 규칙 추가에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 보안 그룹 규칙 추가를 참조하세요.
- 게이트웨이 인스턴스는 실행 중으로 표시됩니다. Amazon EC2 콘솔에서 인스턴스의 상태 값은 RUNNING이어야 합니다.
- 스토리지 요구 사항에 설명된 대로 Amazon EC2 인스턴스 유형은 최소 요구 사항을 충족하는지 여부.

문제를 해결한 후 게이트웨이를 다시 활성화합니다. 이렇게 하려면 Storage Gateway 콘솔을 열고 Amazon EC2에 새 게이트웨이 배포를 선택한 다음 인스턴스의 IP 주소를 다시 입력합니다.

인스턴스 목록에서 EC2 게이트웨이 인스턴스를 찾을 수 없음

인스턴스에 리소스 태그를 지정하지 않았는데 많은 수의 인스턴스가 실행 중인 경우에는 어떤 인스턴스를 실행했는지 파악하기 어려울 수 있습니다. 이 경우 다음 작업을 수행하여 해당 게이트웨이 인스턴스를 찾을 수 있습니다.

- 인스턴스의 설명 탭에서 Amazon Machine Image(AMI)의 이름을 확인합니다. Storage Gateway AMI 기반 인스턴스는 **aws-storage-gateway-ami**라는 텍스트로 시작해야 합니다.
- Storage Gateway AMI 기반 인스턴스가 여러 개인 경우, 인스턴스 시작 시간을 확인하여 올바른 인스턴스를 찾습니다.

Amazon EBS 볼륨을 생성했지만 EC2 게이트웨이 인스턴스에 연결할 수 없음

해당 Amazon EBS 볼륨이 게이트웨이 인스턴스와 동일한 가용 영역에 있는지 확인합니다. 가용 영역이 불일치하는 경우, 인스턴스와 동일한 가용 영역에 새 Amazon EBS 볼륨을 생성합니다.

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. Amazon EC2에 배포된 게이트웨이의 경우, 로컬 디스크는 인스턴스에 연결된 Amazon EBS 볼륨입니다. 이 오류 메시지는 해당 인스턴스에 Amazon EBS 볼륨을 정의하지 않았기 때문에 표시되는 것일 수 있습니다.

게이트웨이를 실행하는 인스턴스에 정의된 블록 디바이스를 확인합니다. 블록 디바이스(AMI와 함께 제공되는 기본 디바이스)가 두 개뿐이라면 스토리지를 추가해야 합니다. 이에 대한 자세한 내용은 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 섹션을 참조하세요. Amazon EBS 볼륨을 두 개 이상 연결한 후 게이트웨이에 볼륨 스토리지를 생성합니다.

업로드 버퍼 공간으로 할당된 디스크를 제거하여 업로드 버퍼 공간을 줄이려는 경우

할당할 업로드 버퍼의 크기 결정 섹션의 단계를 따르세요.

EC2 게이트웨이와 주고받는 데이터의 처리량이 0으로 떨어짐

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.

게이트웨이와 주고받는 처리량은 Amazon CloudWatch 콘솔에서 확인할 수 있습니다. 게이트웨이 및 와의 처리량 측정에 대한 자세한 내용은 섹션을 AWS참조하세요Tape Gateway와 간의 성능 측정 AWS.

EC2 게이트웨이 문제를 해결하는 지원 데 도움이 필요한 경우

Storage Gateway는 게이트웨이 문제 해결을 지원하기 위해 게이트웨이에 액세스 지원 하도록를 활성화하는 등 여러 유지 관리 작업을 수행하는 데 사용할 수 있는 로컬 콘솔을 제공합니다. 기본적으로 게이트웨이에 대한 지원 액세스는 비활성화됩니다. Amazon EC2 로컬 콘솔을 통해 이 액세스 권한을 제공해야 합니다. Secure Shell(SSH)을 통해 Amazon EC2 로컬 콘솔에 로그인합니다. SSH를 통해 성공적으로 로그인하려면 인스턴스의 보안 그룹에 TCP 포트 22를 개방하는 규칙이 있어야 합니다.

> **Note**
>
> 기존 보안 그룹에 새 규칙을 추가할 경우, 해당 보안 그룹을 사용하는 모든 인스턴스에 새 규칙이 적용됩니다. 보안 그룹 및 보안 그룹 규칙을 추가하는 방법에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon EC2 보안 그룹을 참조하세요.

가 게이트웨이에 지원 연결되도록 하려면 먼저 Amazon EC2 인스턴스의 로컬 콘솔에 로그인하고 Storage Gateway의 콘솔로 이동한 다음 액세스를 제공합니다.

Amazon EC2 인스턴스에 배포된 게이트웨이에 대한 지원 액세스를 활성화하려면

1. Amazon EC2 인스턴스의 로컬 콘솔에 로그인합니다. 지침은 Amazon EC2 사용 설명서에서 인스턴스에 연결을 참조하세요.

   다음 명령을 사용하여 EC2 인스턴스의 로컬 콘솔에 로그인할 수 있습니다.

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

   > **Note**
   >
   > *PRIVATE-KEY*는 Amazon EC2 인스턴스를 시작할 때 사용한 EC2 키 페어의 프라이빗 인증서를 포함하는 `.pem` 파일입니다. 자세한 내용은 Amazon EC2 사용 설명서에서 키 페어의 퍼블릭 키 검색을 참조하세요.

The *INSTANCE-PUBLIC-DNS-NAME*은 게이트웨이가 실행 중인 Amazon EC2 인스턴스의 퍼블릭 도메인 이름 시스템(DNS) 이름입니다. 이 퍼블릭 DNS 이름을 확인하려면 EC2 콘솔에서 Amazon EC2 인스턴스를 선택하고 설명 탭을 클릭합니다.

2. 프롬프트에 **6 - Command Prompt**를 입력하여 지원 채널 콘솔을 엽니다.
3. **h**를 입력하여 AVAILABLE COMMANDS(사용 가능한 명령) 창을 엽니다.
4. 다음 중 하나를 수행하세요.

   - 게이트웨이에서 퍼블릭 엔드포인트를 사용 중인 경우 사용 가능한 명령 창에 **open-support-channel**을 입력하여 Storage Gateway의 고객 지원에 연결합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.
   - 게이트웨이가 VPC 엔드포인트를 사용 중인 경우 AVAILABLE COMMANDS(사용 가능한 명령) 창에 **open-support-channel**을 입력합니다. 게이트웨이가 활성화되지 않은 경우 Storage Gateway에 대한 고객 지원에 연결할 VPC 엔드포인트 또는 IP 주소를 제공합니다. AWS에 대한 지원 채널을 열 수 있도록 TCP 포트 22를 허용합니다. 고객 지원에 연결할 때 Storage Gateway는 지원 번호를 할당합니다. 지원 번호를 기록해 둡니다.

   Note

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

5. 지원 채널이 설정되면가 문제 해결 지원을 제공할 지원 수 지원 있도록 지원 서비스 번호를에 제공합니다.
6. 지원 세션이 완료되면 **q**를 입력하여 세션을 종료합니다. 가 지원 세션이 완료되었음을 지원 알릴 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 연결하려는 경우

Amazon EC2 직렬 콘솔을 사용하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. 지침과 문제 해결 팁은 Amazon Elastic Compute Cloud 사용 설명서의 Amazon EC2 직렬 콘솔 섹션을 참조하십시오.

하드웨어 어플라이언스 문제 해결

다음 주제에서는 Storage Gateway Hardware Appliance에서 발생할 수 있는 문제와 이러한 문제를 해결하기 위한 제안 사항에 대해 설명합니다.

서비스 IP 주소를 확인할 수 없음

서비스에 연결할 때 호스트 IP 주소가 아닌 서비스의 IP 주소를 사용하고 있는지 확인합니다. 서비스 콘솔에서 서비스 IP 주소를 구성하고 하드웨어 콘솔에서 호스트 IP 주소를 구성합니다. 하드웨어 어플라이언스를 시작하면 하드웨어 콘솔이 표시됩니다. 하드웨어 콘솔에서 서비스 콘솔로 이동하려면 Open Service Console(서비스 콘솔 열기)을 선택합니다.

공장 초기화는 어떻게 수행하나요?

어플라이언스에서 공장 초기화를 수행해야 하는 경우, 다음 지원 섹션에 설명된 대로 Storage Gateway 하드웨어 어플라이언스 팀에 지원을 요청하세요.

원격 재시작은 어떻게 수행하나요?

어플라이언스를 원격으로 재시작해야 하는 경우 Dell iDRAC 관리 인터페이스를 사용하여 재시작할 수 있습니다. 자세한 내용은 Dell Technologies InfoHub 웹 사이트에서 iDRAC9 Virtual Power Cycle: Remotely power cycle Dell EMC PowerEdge Servers를 참조하세요.

Dell iDRAC 지원은 어디에서 받을 수 있나요?

Dell PowerEdge 서버에는 Dell iDRAC 관리 인터페이스가 함께 제공됩니다. 다음과 같이 하는 것이 좋습니다:

- iDRAC 관리 인터페이스를 사용하는 경우 기본 암호를 변경해야 합니다. iDRAC 자격 증명에 대한 자세한 내용은 Dell PowerEdge - iDRAC의 기본 로그인 자격 증명은 무엇입니까?를 참조하세요.

- 보안 위반을 막기 위해 펌웨어가 최신 버전인지 확인합니다.
- iDRAC 네트워크 인터페이스를 일반(em) 포트로 이동하면 성능 문제가 발생하거나 어플라이언스가 정상적으로 작동하지 않을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾을 수 없음

Storage Gateway 하드웨어 어플라이언스의 일련 번호는 Storage Gateway 콘솔을 사용하여 찾을 수 있습니다.

하드웨어 어플라이언스 일련 번호를 찾으려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 페이지 왼쪽의 탐색 메뉴에서 하드웨어를 선택합니다.
3. 목록에서 하드웨어 어플라이언스를 선택합니다.
4. 어플라이언스의 세부 정보 탭에서 일련 번호 필드를 찾습니다.

하드웨어 어플라이언스 지원은 어디에서 받을 수 있나요?

하드웨어 어플라이언스의 기술 지원에 AWS 대한 문의는 섹션을 참조하세요지원.

지원 팀이 지원 채널을 활성화하여 게이트웨이 문제를 원격으로 해결하도록 요청할 수 있습니다. 게이트웨이의 정상 작업 중에는 이 포트를 열어둘 필요가 없지만, 문제 해결 시에는 필요합니다. 다음 절차에 나온 것처럼 하드웨어 콘솔에서 지원 채널을 활성화할 수 있습니다.

에 대한 지원 채널을 열려면 AWS

1. 하드웨어 콘솔을 엽니다.
2. 하드웨어 콘솔의 메인 페이지 하단에서 지원 채널 열기를 선택한 다음 `Enter` 키를 누릅니다.

   네트워크 연결 또는 방화벽 문제가 없는 경우 할당된 포트 번호가 30초 이내에 표시되어야 합니다. 예제:

   상태: 포트 19599에서 열림
3. 포트 번호를 기록하여에 제공합니다 지원.

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. 이러한 오류는 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

Tape Gateway 또는 하이퍼바이저 호스트에서 복구할 수 없는 오류가 발생하는 경우 다른 Tape Gateway에 이미 업로드된 데이터를 복구 AWS 할 수 있습니다.

테이프에 기록한 데이터는 해당 데이프가 성공적으로 VTS에 보관될 때까지는 완전히 업로드되지 않았을 수 있다는 점을 유의하십시오. 이러한 방식으로 다른 게이트웨이로 복구된 테이프에서 데이터가 불완전하거나 비어 있을 있습니다. 복구된 모든 테이프에 대해 인벤토리를 수행하여 예상 콘텐츠를 포함하는지 확인하는 것이 좋습니다.

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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 비활성화를 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 연결된 리소스 제거 섹션을 참조하세요.

Storage Gateway가 장애가 발생한 Tape Gateway에서 사용자가 지정한 Tape Gateway로 테이프를 이동합니다. Tape Gateway에서 테이프 상태를 RECOVERED로 표시합니다.

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 S3 와 동기화되지 않은 데이터가 있는 테이프는 자동으로 복구됩니다. 이 테이프의 상태가 RECOVERED로 설정되어 있기는 하지만 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 Gateway구성을 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 게이트웨이를 선택한 후 해당 게이트웨이를 선택합니다.
3. 작업에서 로컬 스토리지 구성를 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 않은 장애가 발생하면 Storage Gateway는 장애가 있는 가상 테이프의 상태를 IRRECOVERABLE로 설정합니다. 취할 조치는 상황에 따라 달라집니다. 아래와 같이 겪을 수 있는 문제와 이 문제를 해결하는 방법에 대한 정보를 얻을 수 있습니다.

복구할 수 없는 테이프에서 데이터를 복구해야 하는 경우

IRRECOVERABLE 상태인 가상 테이프에 대한 작업을 해야 하는 경우, 다음 중 한 가지를 수행합니다.

- 활성화된 Tape Gateway가 없는 경우, 새로 활성화합니다. 자세한 내용은 게이트웨이 생성을 참조하세요.
- 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 Tape Gateway를 사용하려면 iSCSI 이니시에이터를 재구성하고 애플리케이션을 백업해야 합니다. 자세한 내용은 VTL 디바이스 연결 단원을 참조하십시오.

아카이브에 아카이브하지 않은 복구 불가능한 테이프가 필요 없게 된 경우

IRRECOVERABLE 상태의 가상 테이프가 있는데 이제 필요 없게 된 경우, 이 테이프를 아카이브에 보관한 적이 없다면 이 테이프는 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 3개의 캐시 디스크가 있는데 이 중 2개를 삭제하면, 클린 상태인 테이프나 볼륨의 상태가 AVAILABLE이 됩니다. 다른 테이프나 볼륨의 상태는 IRRECOVERABLE이 됩니다.
>
> 임시 디스크를 게이트웨이의 캐시 디스크로 사용하거나 임시 디스크에 캐시 디스크를 탑재하는 경우, 게이트웨이를 닫으면 캐시 디스크를 잃게 됩니다. 캐시 디스크 및 Amazon S3가 동기화되지 않은 상태에서 게이트웨이를 닫으면 데이터가 손실됩니다. 따라서, 임시 드라이브나 디스크를 사용하지 않는 것이 좋습니다.

고가용성 상태 알림

VMware vSphere HA(고가용성) 플랫폼에서 게이트웨이를 실행할 때 상태 알림을 받을 수 있습니다. 상태 알림에 대한 자세한 내용은 고가용성 문제 해결 섹션을 참조하세요.

고가용성 문제 해결

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

주제

- 상태 알림
- Metrics

상태 알림

VMware vSphere HA에서 게이트웨이를 실행하면 모든 게이트웨이에서는 구성된 Amazon CloudWatch 로그 그룹에 다음과 같은 상태 알림을 생성합니다. 이러한 알림은 `AvailabilityMonitor`라는 로그 스트림으로 이동합니다.

주제

- 알림: 재부팅
- 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 참조하세요.

알림: HealthCheckFailure

VMware vSphere HA에 대한 게이트웨이의 경우 상태 확인에 실패하고 VM 다시 시작을 요청하면 `HealthCheckFailure` 알림을 받을 수 있습니다. 이 이벤트는 `AvailabilityMonitorTest` 알림으로 표시된 가용성을 모니터하기 위한 테스트 도중에도 발생합니다. 이 경우 `HealthCheckFailure` 알림이 예상됩니다.

> **Note**
>
> 이 알림은 VMware 게이트웨이에만 적용됩니다.

취할 조치

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

알림: AvailabilityMonitorTest

VMware vSphere HA의 게이트웨이의 경우 VMware에서 가용성 및 애플리케이션 모니터링 시스템 테스트를 실행할 때 `AvailabilityMonitorTest` 알림을 받을 수 있습니다.

Metrics

`AvailabilityNotifications` 지표는 모든 게이트웨이에서 사용할 수 있습니다. 이 지표는 게이트웨이에 의해 생성된 가용성 관련 상태 알림의 개수입니다. `Sum` 통계를 사용하여 게이트웨이에 가용성 관련 이벤트가 발생하는지 여부를 확인할 수 있습니다. 이벤트에 대한 자세한 내용은 구성된 CloudWatch 로그 그룹에 문의하십시오.

Tape Gateway 모범 사례

이 단원은 다음 주제로 구성되어 있으며, 게이트웨이, 로컬 디스크, 스냅샷 및 데이터를 다루는 모범 사례에 대한 정보를 제공합니다. AWS Storage Gateway와 관련된 문제를 방지하기 위해 이 단원에 설명된 정보를 숙지하고 이 지침을 따르는 것이 좋습니다. 배포 시 발생할 수 있는 일반적인 문제를 진단하고 해결하는 방법에 대한 자세한 내용은 게이트웨이 문제 해결 섹션을 참조하세요.

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 섹션의 지침에 따라 테이프를 복구하는 것이 좋습니다.

> **Important**
>
> Storage Gateway는 하이퍼바이저에서 생성한 스냅샷 또는 Amazon EC2 Amazon Machine Image(AMI)에서 게이트웨이 VM을 복구하는 기능을 지원하지 않습니다. 게이트웨이 VM이 제대로 작동하지 않는 경우에는 다음 지침에 따라 새 게이트웨이를 활성화하고 그 게이트웨이에 데이터를 복구합니다.

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 게이트웨이가 인터넷에 연결되어 있는지 테스트섹션을 참조하세요.
- 테이프 설정의 경우 게이트웨이에 연결할 수 있게 되면 테이프가 BOOTSTRAPPING 상태가 됩니다. 이 기능을 사용하면 로컬에 저장된 데이터를 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 테이프의 상태가 IRRECOVERABLE인 경우에는 다음 옵션 중 한 가지를 사용하여 데이터를 복구하거나 처한 상황에 맞는 방법으로 장애를 해결하는 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 IRRECOVERABLE 상태인 경우 데이터를 복구하거나 장애를 해결하는 방법에 관한 자세한 내용은 복구 불가능한 테이프 문제 해결 단원을 참조하십시오.

장애가 있는 캐시 디스크에서 데이터 복구

캐시 디스크에 장애가 발생하면 다음 절차에 따라 처한 상황에 맞는 방법으로 데이터를 복구하는 것이 좋습니다.

- 호스트에서 캐시 디스크가 제거되어 장애가 발생한 경우, 게이트웨이를 종료하고 디스크를 다시 추가한 후 게이트웨이를 다시 시작합니다.
- 캐시 디스크가 손상되거나 캐시 디스크에 액세스할 수 없는 경우, 게이트웨이를 종료하고 캐시 디스크를 재설정하고 캐시 스토리지용 디스크를 재구성한 후 게이트웨이를 다시 시작합니다.

자세한 내용은 장애가 있는 캐시 디스크에서 가상 테이프를 복구해야 하는 경우섹션을 참조하세요.

액세스할 수 없는 데이터 센터에서 데이터 복구

게이트웨이 또는 데이터 센터에 대한 액세스가 어떤 이유로 차단되는 경우에는 데이터를 다른 데이터 센터의 다른 게이트웨이로 복구하거나 Amazon EC2 인스턴스에서 호스팅되는 게이트웨이로 복구할 수 있습니다. 따라서 다른 데이터 센터에 액세스할 수 없다면 Amazon EC2 인스턴스에서 게이트웨이를 생성하는 것이 좋습니다. 생성 방법은 데이터를 복구하는 게이트웨이 유형에 따라 다릅니다.

액세스할 수 없는 데이터 센터의 Tape Gateway에서 데이터를 복구하려면

1. Amazon EC2 호스트에서 새 Tape Gateway를 생성하여 활성화합니다. 자세한 내용은 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 단원을 참조하십시오.
2. 데이터 센터의 소스 게이트웨이에서 Amazon EC2에서 새로 생성한 게이트웨이로 테이프를 복구합니다. 자세한 내용은 복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우 섹션을 참조하세요.

   테이프가 새 Amazon EC2 게이트웨이로 복구되어야 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 정보에서 추가 정보를 확인합니다.

필요 없는 리소스를 정리하려면

1. 게이트웨이의 가상 테이프 라이브러리(VTL) 및 아카이브에서 테이브를 삭제합니다. 자세한 내용은 게이트웨이 삭제 및 연결된 리소스 제거 단원을 참조하십시오.

   a. 게이트웨이의 VTL에서 RETRIEVED 상태인 테이프를 모두 보관합니다. 지침은 테이프 보관 섹션을 참조하세요.

   b. 게이트웨이의 VTL에서 남은 테이프를 삭제합니다. 지침은 Tape Gateway에서 가상 테이프 삭제 섹션을 참조하세요.

   c. 아카이브에 있는 테이프를 모두 삭제합니다. 지침은 Tape Gateway에서 가상 테이프 삭제 섹션을 참조하세요.

2. Tape Gateway를 계속해서 사용할 계획이 아니라면 삭제합니다. 이에 관한 지침은 게이트웨이 삭제 및 연결된 리소스 제거 지침을 참조하세요.

3. 온프레미스 호스트에서 Storage Gateway VM을 삭제합니다. Amazon EC2 인스턴스에서 게이트웨이를 생성한 경우에는 해당 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 - 게이트웨이용 가상 머신 호스트를 배포하고 구성하는 방법에 대해 알아봅니다.
- Tape Gateway 스토리지 리소스 작업 - 로컬 디스크 제거, Amazon EBS 볼륨 관리, 가상 테이프 라이브러리 디바이스 작업, 가상 테이프 라이브러리에서 테이프 관리 등 Tape Gateway 스토리지 리소스와 관련된 절차에 대해 알아봅니다.
- 게이트웨이 활성화 키 받기 - 새 게이트웨이를 배포할 때 제공해야 하는 활성화 키를 찾을 수 있는 위치에 대해 알아봅니다.
- iSCSI 초기자 연결 - iSCSI(Internet Small Computer System Interface) 대상으로 노출되는 볼륨 또는 가상 테이프 라이브러리(VTL) 디바이스로 작업하는 방법에 대해 알아봅니다.
- Storage Gateway Direct Connect 와 함께 사용 - 온프레미스 게이트웨이와 AWS 클라우드 간에 전용 네트워크 연결을 생성하는 방법에 대해 알아봅니다.
- 게이트웨이 어플라이언스의 IP 주소 가져오기 - 새 게이트웨이를 배포할 때 제공해야 하는 게이트웨이의 가상 머신 호스트 IP 주소를 찾을 수 있는 위치에 대해 알아봅니다.
- IPv6 지원 - IPv6 요구 사항에 대해 알아봅니다.
- Storage Gateway 리소스 및 리소스 ID 이해 -가 Storage Gateway에서 생성한 리소스 및 하위 리소스를 AWS 식별하는 방법을 알아봅니다.
- Storage Gateway 리소스에 태그를 지정 - 메타데이터 태그를 사용하여 리소스를 분류하고 더 쉽게 관리할 수 있는 방법에 대해 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 한도 및 할당량에 대해 알아봅니다.

게이트웨이 VM 호스트 배포 및 구성

이 섹션의 주제에서는 VMware, Hyper-V 또는 Linux KVM에서 실행되는 온프레미스 어플라이언스와 AWS 클라우드의 Amazon EC2 인스턴스에서 실행되는 어플라이언스를 포함하여 Storage Gateway 어플라이언스의 가상 머신 호스트를 설정하고 관리하는 방법을 설명합니다.

주제

- Tape Gateway용 기본 Amazon EC2 호스트 배포 - 기본 지정 사항을 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Tape Gateway를 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 Gateway를 배포하고 활성화하는 방법에 대해 알아봅니다.
- Amazon EC2 인스턴스 메타데이터 옵션 수정 - MDS 버전 1(IMDSv1)을 사용하는 수신 메타데이터 요청을 수락하거나 모든 메타데이터 요청이 IMDS 버전 2(IMDSv2)를 반드시 사용하도록 Amazon EC2 게이트웨이 인스턴스를 구성하는 방법에 대해 알아봅니다.
- Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화 - 온프레미스 Hyper-V 또는 Linux KVM 게이트웨이 가상 머신의 시간을 확인하고 NTP(Network Time Protocol) 서버와 동기화하는 방법에 대해 알아봅니다.
- VM 시간을 VMware 호스트 시간과 동기화 - VMware 게이트웨이 가상 머신의 호스트 시간을 확인하고 필요한 경우 시간을 설정하고 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성하는 방법에 대해 알아봅니다.
- VMware 호스트에서 반가상화 구성 - 반가상 iSCSI(Internet Small Computer System Interface) 컨트롤러를 사용하도록 Storage Gateway 어플라이언스용 VMware 호스트 플랫폼을 구성하는 방법에 대해 알아봅니다.
- 게이트웨이용 네트워크 어댑터 구성 - VMXNET3(10GbE) 네트워크 어댑터를 사용하거나 여러 개의 네트워크 어댑터를 사용하여 여러 IP 주소에서 액세스할 수 있도록 게이트웨이를 재구성하는 방법에 대해 알아봅니다.
- Storage Gateway와 함께 VMware vSphere High Availability 사용 - VMware vSphere High Availability와 연동되도록 Storage Gateway를 구성하여 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호하는 방법에 대해 알아봅니다.

Tape Gateway용 기본 Amazon EC2 호스트 배포

이 주제에서는 기본 지정 사항으로 Amazon EC2 호스트를 배포하는 단계에 대해 설명합니다.

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Tape Gateway를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon Machine Image(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

> **Note**
>
> Storage Gateway 커뮤니티 AMI는 AWS에서 게시하고 완벽하게 지원합니다. 게시자가 AWS 확인된 공급자임을 알 수 있습니다.

1. Amazon EC2 인스턴스를 설정하려면 워크플로의 플랫폼 옵션 섹션에서 Amazon EC2를 호스트 플랫폼으로 선택합니다. Amazon EC2 인스턴스 구성에 대한 지침은 Tape Gateway를 호스팅할 Amazon EC2 인스턴스 배포를 참조하세요.
2. 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 열고 인스턴스 유형, 네트워크 설정 및 스토리지 구성과 같은 추가 설정을 사용자 지정합니다.
3. (선택 사항) Storage Gateway 콘솔에서 기본 설정 사용을 선택하여 기본 구성으로 Amazon EC2 인스턴스를 배포할 수 있습니다.

   기본 설정 사용으로 생성되는 Amazon EC2 인스턴스의 기본 지정사항은 다음과 같습니다.

   - 인스턴스 유형 - m5.xlarge
   - 네트워크 설정
     - VPC에서 EC2 인스턴스를 실행할 VPC를 선택합니다.
     - 서브넷에서 EC2 인스턴스를 시작할 서브넷을 지정합니다.

       > **Note**
       >
       > VPC 서브넷은 VPC 관리 콘솔에서 퍼블릭 IPv4 주소 자동 할당 설정이 활성화된 경우에만 드롭다운에 표시됩니다.

     - 퍼블릭 IP 자동 할당 - 활성화됨

   EC2 보안 그룹이 생성되고 EC2 인스턴스와 연결됩니다. 보안 그룹에는 다음과 같은 인바운드 포트 규칙이 적용됩니다.

> **Note**
>
> 게이트웨이 활성화 중에는 포트 80이 열려 있어야 합니다. 활성화 후에는 포트가 즉시 닫힙니다. 이후에는 선택한 VPC의 다른 포트를 통해서만 EC2 인스턴스에 액세스할 수 있습니다.
>
> 게이트웨이의 iSCSI 대상은 게이트웨이와 동일한 VPC에 있는 호스트에서만 액세스할 수 있습니다. VPC 외부의 호스트에서 iSCSI 대상에 액세스해야 하는 경우 적절한 보안 그룹 규칙을 업데이트해야 합니다.
>
> Amazon EC2 인스턴스 세부 정보 페이지로 이동한 후 보안을 선택하고 보안 그룹 세부 정보로 이동한 다음 보안 그룹 ID를 선택하여 언제든지 보안 그룹을 편집할 수 있습니다.

포트	프로토콜	파일 시스템 프로토콜				
80	TCP	활성화를 위한 HTTP 액세스				
3260	TCP	iSCSI				

- 스토리지 구성

기본 설정	AMI 루트 볼륨	볼륨 2 캐시	볼륨 3 캐시			
디바이스 이름		'/dev/sdb'	'/dev/sdc'			
Size:	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			
암호화됨	아니요	아니요	아니요			
처리량	125	125	125			

Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포

Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Tape Gateway를 배포하고 활성화할 수 있습니다. AWS Storage Gateway Amazon 머신 이미지(AMI)는 커뮤니티 AMI로 사용할 수 있습니다.

> **Note**
>
> Storage Gateway 커뮤니티 AMI는 AWS에서 게시하고 완벽하게 지원합니다. 게시자가 AWS 확인된 공급자임을 알 수 있습니다.
> Tape Gateway AMI는 다음과 같은 명명 규칙을 사용합니다. AMI 이름에 추가되는 버전 번호는 각 버전 릴리스에 따라 변경됩니다.
> `aws-storage-gateway-CLASSIC-2.9.0`

Tape Gateway를 호스팅할 Amazon EC2 인스턴스를 배포하려면

1. Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Tape Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에서 Amazon EC2를 호스트 플랫폼으로 선택한 후 다음 단계를 수행하여 Tape Gateway를 호스팅할 Amazon EC2 인스턴스를 시작합니다.
2. 인스턴스 시작을 선택하여 추가 설정을 구성할 수 있는 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 엽니다.

   기본 설정으로 Amazon EC2 인스턴스를 시작하려면 QuickLaunch를 사용합니다. Amazon EC2 Quicklaunch 기본 사양에 대한 자세한 내용은 Amazon EC2의 Quicklaunch 구성 사양을 참조하세요. 을 참조하세요.
3. 이름에 Amazon EC2 인스턴스의 이름을 입력합니다. 인스턴스를 배포한 후 이 이름을 검색하여 Amazon EC2 콘솔의 목록 페이지에서 인스턴스를 찾을 수 있습니다.

4. 인스턴스 유형 섹션의 인스턴스 유형에서 인스턴스의 하드웨어 구성을 선택합니다. 하드웨어 구성은 게이트웨이를 지원하기 위한 특정 최소 요구 사항을 충족해야 합니다. 게이트웨이가 제대로 작동하기 위한 최소 하드웨어 요구 사항을 충족하는 m5.xlarge 인스턴스 유형으로 시작하는 것이 좋습니다. 자세한 내용은 Amazon EC2 인스턴스 유형에 대한 요구 사항 단원을 참조하십시오.

   필요하다면 시작한 후 인스턴스 크기를 조정할 수 있습니다. 자세한 내용은 Amazon EC2 사용 설명서에서 인스턴스 크기 조정을 참조하세요.

   > **Note**
   >
   > 특히 i3 EC2 같은 특정한 인스턴스 유형은 NVMe SSD 디스크를 사용합니다. 이러한 경우 Tape Gateway를 시작하거나 중지할 때 문제가 발생할 수 있습니다. 예를 들어, 캐시에서 데이터가 손실될 수 있습니다. `CachePercentDirty` Amazon CloudWatch 지표를 모니터링하여 해당 파라미터가 `0`일 때만 시스템을 시작하거나 중지하세요. 게이트웨이 지표 모니터링에 대한 자세한 내용은 CloudWatch 설명서에서 Storage Gateway 지표 및 차원 섹션을 참조하세요.

5. 키 페어(로그인) 섹션에서 키 페어 이름 - 필수에서 인스턴스에 안전하게 연결하는 데 사용할 키 페어를 선택합니다. 필요한 경우 키 페어를 새로 생성할 수 있습니다. 자세한 내용은 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 키 페어 생성을 참조하세요.
6. 네트워크 설정 섹션에서 사전 구성된 설정을 검토하고 편집을 선택하여 다음 필드를 변경합니다.

   a. VPC - 필수에서 Amazon EC2 인스턴스를 시작할 VPC를 선택합니다. 자세한 내용은 Amazon Virtual Private Cloud 사용 설명서에서 Amazon VPC 작동 방식을 참조하세요.

   b. (선택 사항) 서브넷에서 Amazon EC2 인스턴스를 시작할 서브넷을 선택합니다.

   c. 퍼블릭 IP 자동 할당(Auto-assign Public IP)의 경우 활성화(Enable)를 선택합니다.
7. 방화벽(보안 그룹) 하위 섹션에서 사전 구성된 설정을 검토합니다. 원하는 경우 Amazon EC2 인스턴스용으로 생성할 새 보안 그룹의 기본 이름과 설명을 변경하거나, 기존 보안 그룹의 방화벽 규칙을 적용하도록 선택할 수도 있습니다.
8. 인바운드 보안 그룹 규칙 하위 섹션에서 클라이언트가 인스턴스에 연결하는 데 사용할 포트를 여는 방화벽 규칙을 추가합니다. Tape Gateway에 필요한 포트에 대한 자세한 내용은 포트 요구 사항을 참조하세요. 방화벽 규칙 추가에 대한 자세한 정보는 Linux 인스턴스용 Amazon Elastic Compute Cloud 사용 설명서에서 보안 그룹 규칙을 참조하세요.

> **Note**
>
> Tape Gateway에서는 인바운드 트래픽과 게이트웨이 활성화 중 일회성 HTTP 액세스를 위해 TCP 포트 80을 열어야 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 볼륨 외에도 캐시 스토리지 용도로 최소 165GiB 용량의 Amazon EBS 볼륨을 하나 이상 추가하고 업로드 버퍼 용도로 최소 150GiB 용량의 Amazon EBS 볼륨을 하나 이상 추가해야 합니다. 성능을 높이려면 캐시 스토리지에 각각 150GiB 이상의 EBS 볼륨을 여러 개 할당하는 것이 좋습니다.

11. 고급 세부 정보 섹션에서 사전 구성된 설정을 검토하고 필요한 경우 변경합니다.
12. 인스턴스 시작을 선택하여 새 Amazon EC2 게이트웨이 인스턴스를 구성된 설정으로 시작합니다.
13. 새 인스턴스가 성공적으로 시작되었는지 확인하려면 Amazon EC2 콘솔의 인스턴스 페이지로 이동하여 새 인스턴스를 이름으로 검색합니다. 인스턴스 상태가 녹색 확인 표시와 함께 실행 중으로 표시되고 상태 검사가 완료되어 녹색 확인 표시가 나타나는지 확인합니다.
14. 세부 정보 페이지에서 해당 인스턴스를 선택합니다. 인스턴스 요약 섹션에서 퍼블릭 IPv4 주소를 복사한 다음 Storage Gateway 콘솔의 게이트웨이 설정 페이지로 돌아가서 Tape Gateway 설정을 재개합니다.

Storage Gateway 콘솔을 사용하거나 AWS Systems Manager 파라미터 스토어를 쿼리하여 Tape Storage Gateway를 시작하는 데 사용할 AMI ID를 확인할 수 있습니다.

AMI ID를 확인하려면 다음 중 하나를 수행합니다.

- Storage Gateway 콘솔을 사용하여 새 게이트웨이 설정을 시작합니다. 지침은 Tape Gateway 설정을 참조하세요. 플랫폼 옵션 섹션에 도달하면 Amazon EC2를 호스트 플랫폼으로 선택한 다음 인스턴스 시작을 선택하여 Amazon EC2 콘솔에서 AWS Storage Gateway AMI 템플릿을 엽니다.

  EC2 커뮤니티 AMI 페이지로 리디렉션되며, URL에서 해당 AWS 리전의 AMI ID를 볼 수 있습니다.

- Systems Manager 파라미터 스토어를 쿼리합니다. AWS CLI 또는 Storage Gateway API를 사용하여 네임스페이스 아래의 Systems Manager 퍼블릭 파라미터를 쿼리할 수 있습니다`/aws/service/storagegateway/ami/VTL/latest`. 예를 들어 다음 CLI 명령을 사용하면 AWS 리전 지정한에서 현재 AMI의 ID가 반환됩니다.

```
aws --region us-east-2 ssm get-parameter --name /aws/service/storagegateway/ami/VTL/
latest
```

이 CLI 명령은 다음과 비슷한 출력을 반환합니다.

```
{
    "Parameter": {
        "Type": "String",
        "LastModifiedDate": 1561054105.083,
        "Version": 4,
        "ARN": "arn:aws:ssm:us-east-2::parameter/aws/service/storagegateway/ami/VTL/
latest",
        "Name": "/aws/service/storagegateway/ami/VTL/latest",
        "Value": "ami-123c45dd67d891000"
    }
}
```

Amazon EC2 인스턴스 메타데이터 옵션 수정

인스턴스 메타데이터 서비스(IMDS)는 Amazon EC2 인스턴스 메타데이터에 대한 보안 액세스를 제공하는 온 인스턴스 구성 요소입니다. IMDS 버전 1(IMDSv1)을 사용하는 수신 메타데이터 요청을 수락하거나 모든 메타데이터 요청이 IMDS 버전 2(IMDSv2)를 반드시 사용하도록 인스턴스를 구성할 수 있습니다. IMDSv2는 세션 지향 요청을 사용하며 IMDS에 액세스하기 위해 사용될 수 있는 여러 유형의 취약성을 완화합니다. IMDSv2에 대한 자세한 내용은 Amazon Elastic Compute Cloud 사용 설명서에서 인스턴스 메타데이터 서비스 버전 2 작동 방식을 참조하세요.

Storage Gateway를 호스팅하는 모든 Amazon EC2 인스턴스에는 IMDSv2를 반드시 사용해야 합니다. 새로 시작되는 모든 게이트웨이 인스턴스에는 기본적으로 IMDSv2가 필요합니다. IMDSv1 메타데이터 요청을 수락하도록 구성된 기존 인스턴스가 아직 있는 경우,Amazon Elastic Compute Cloud 사용 설명서의 IMDSv2 사용 요구 섹션을 참조하여 IMDSv2를 사용하도록 인스턴스 메타데이터 옵션을 수정합니다. 이 변경 사항을 적용해도 인스턴스를 재부팅할 필요는 없습니다.

Hyper-V 또는 Linux KVM 호스트 시간과 VM 시간 동기화

VMware ESXi에 배포된 게이트웨이의 경우 하이퍼바이저 호스트 시간을 설정하고 가상 머신 시간을 호스트와 동기화하는 것만으로도 충분히 시간 편차를 방지할 수 있습니다. 자세한 내용은 VM 시간을 VMware 호스트 시간과 동기화 단원을 참조하십시오. Microsoft Hyper-V 또는 Linux KVM에 배포된 게이트웨이의 경우 다음 절차를 수행하여 가상 머신 시간을 주기적으로 확인하는 것이 좋습니다.

하이퍼바이저 게이트웨이 가상 머신의 시간을 확인하고 NTP(Network Time Protocol) 서버와 동기화하려면

1. 게이트웨이의 로컬 콘솔에 로그인합니다.

   - Microsoft Hyper-V 로컬 콘솔 로그인에 대한 자세한 내용은 Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스을 참조하세요.
   - Linux 커널 기반 가상 머신(KVM)용 로컬 콘솔 로그인에 대한 자세한 내용은 Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스 섹션을 참조하세요.
2. Storage Gateway 구성 기본 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 관리를 선택합니다.
3. 시스템 시간 관리 메뉴 화면에서 해당 숫자를 입력하여 시스템 시간 보기 및 동기화를 선택합니다.

   게이트웨이 로컬 콘솔에서 현재 시스템 시간을 표시하고 NTP 서버에서 보고한 시간과 비교한 다음 두 시간 간의 정확한 편차를 초 단위로 보고합니다.
4. 시간 편차가 60초를 초과할 경우 **y**를 입력하여 시스템 시간을 NTP 시간과 동기화합니다. 그렇지 않은 경우 **n**을 입력합니다.

   시간 동기화에는 몇 분 정도 걸릴 수 있습니다.

VM 시간을 VMware 호스트 시간과 동기화

게이트웨이를 성공적으로 활성화하려면 VM 시간을 호스트 시간과 동기화해야 하고 호스트 시간을 올바르게 설정해야 합니다. 이 섹션에서는 먼저 VM의 시간을 호스트 시간과 동기화합니다. 그 다음 호스트 시간을 확인하고, 필요한 경우 호스트 시간을 설정하고 호스트가 자동으로 시간을 NTP(Network Time Protocol) 서버와 동기화하도록 구성합니다.

> **Important**
>
> VM 시간을 호스트 시간과 동기화하려면 게이트웨이를 성공적으로 활성화해야 합니다.

VM 시간을 호스트 시간과 동기화하려면

1. VM 시간을 구성합니다.

   a. vSphere 클라이언트에서 애플리케이션 창의 왼쪽 패널에 있는 게이트웨이 VM의 이름을 마우스 오른쪽 버튼으로 클릭하여 VM의 컨텍스트 메뉴를 연 다음 설정 편집을 선택합니다.

      그러면 Virtual Machine Properties(가상 머신 속성) 대화 상자가 열립니다.

   b. 옵션 탭을 선택하고 옵션 목록에서 VMware 도구를 선택합니다.

   c. 가상 머신 속성 대화 상자의 오른쪽에 있는 고급 섹션에서 호스트와 게스트 시간 동기화 옵션을 확인한 후 확인을 선택합니다.

      그러면 VM이 자체 시간을 호스트와 동기화합니다.

2. 호스트 시간을 구성합니다.

   호스트 클럭의 시간이 올바르게 설정되어 있는지 확인하는 것이 중요합니다. 호스트 클럭을 구성하지 않았다면 다음 절차에 따라 설정하고 NTP 서버와 동기화합니다.

   a. VMware vSphere 클라이언트의 왼쪽 패널에서 vSphere 호스트 노드를 선택한 후 구성 탭을 선택합니다.

   b. 소프트웨어 패널에서 시간 구성을 선택한 다음 속성 링크를 선택합니다.

      그러면 Time Configuration(시간 구성) 대화 상자가 나타납니다.

   c. 날짜 및 시간에서 vSphere 호스트의 날짜와 시간을 설정합니다.

   d. 호스트가 자체 시간을 자동으로 NTP 서버와 동기화하도록 구성합니다.

      i. 시간 구성 대화 상자에서 옵션을 선택한 다음 NTP 데몬(ntpd) 옵션 대화 상자의 왼쪽 패널에서 NTP 설정을 선택합니다.

      ii. 추가를 선택하여 새 NTP 서버를 추가합니다.

      iii. NTP 서버 추가 대화 상자에서 NTP 서버의 IP 주소 또는 전체 주소 도메인 이름을 입력한 후 확인을 선택합니다.

         `pool.ntp.org`를 도메인 이름으로 사용할 수 있습니다.

      iv. NTP 대몬(ntpd) 옵션 대화 상자의 왼쪽 패널에서 일반을 선택합니다.

      v. 서비스 명령에서 시작을 선택하여 서비스를 시작합니다.

         이 NTP 서버 참조를 변경하거나 나중에 하나를 더 추가하는 경우, 새 서버를 사용하려면 해당 서비스를 다시 시작해야 한다는 점에 유의하십시오.

e. 확인을 선택하여 NTP 데몬(ntpd) 옵션 대화 상자를 닫습니다.

f. 확인을 선택하여 Time Configuration(시간 구성) 대화 상자를 닫습니다.

VMware 호스트에서 반가상화 구성

다음 절차에서는 반가상화 iSCSI(Internet Small Computer System Interface) 컨트롤러를 사용하도록 Storage Gateway 어플라이언스용 VMware 호스트 플랫폼을 구성하는 방법에 대해 설명합니다. 반가상화 iSCSI 컨트롤러는 처리량을 높이고 CPU 사용량을 줄일 수 있는 고성능 스토리지 컨트롤러입니다. 이러한 컨트롤러는 고성능 스토리지 환경에 가장 적합합니다. iSCSI 컨트롤러를 이러한 방식으로 구성하면 Storage Gateway 가상 머신이 호스트 운영 체제와 함께 작동하여 게이트웨이 콘솔에서 가상 머신에 추가된 가상 디스크를 식별할 수 있습니다.

> **Note**
>
> 게이트웨이 콘솔에서 이러한 디스크를 구성할 때 디스크 식별 문제를 방지하려면 이 단계를 완료해야 합니다.

반가상화된 컨트롤러를 사용하도록 VMware 호스트 플랫폼을 구성하려면

1. VMware vSphere 클라이언트에서 애플리케이션 창의 왼쪽에 있는 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 반가상화 SCSI 컨트롤러 유형을 선택한 후 확인을 선택하여 구성을 저장합니다.

게이트웨이용 네트워크 어댑터 구성

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

주제

- VMXNET3 네트워크 어댑터를 사용하도록 게이트웨이를 구성
- 여러 개의 NIC에 게이트웨이 구성

VMXNET3 네트워크 어댑터를 사용하도록 게이트웨이를 구성

Storage Gateway는 VMware ESXi 및 Microsoft Hyper-V Hypervisor 호스트 모두에서 E1000 네트워크 어댑터 유형을 지원합니다. 그러나 VMXNET3(10GbE) 네트워크 어댑터 유형은 VMware ESXi 하이퍼바이저에서만 지원합니다. 게이트웨이를 VMware ESXi 하이퍼바이저에서 호스팅하는 경우, VMXNET3(10GbE) 어댑터 유형을 사용하도록 게이트웨이를 재구성할 수 있습니다. 이러한 어댑터에 대한 자세한 내용은 Broadcom(VMware) 웹 사이트에서 Choosing a network adapter for your virtual machine을 참조하세요.

> **Important**
>
> VMXNET3를 선택하려면 게스트 운영 체제 유형이 Other Linux64(기타 Linux64)이어야 합니다.

VMXNET3 어댑터를 사용하도록 게이트웨이를 구성하려면 다음 단계를 수행해야 합니다.

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

각 단계를 수행하는 자세한 방법은 다음과 같습니다.

기본 E1000 어댑터를 제거하고 VMXNET3 어댑터를 사용하도록 게이트웨이를 구성하려면

1. VMware에서 게이트웨이를 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.
2. Virtual Machine Properties(가상 머신 속성) 창에서 Hardware(하드웨어) 탭을 선택합니다.
3. Hardware(하드웨어)에 대해 Network adapter(네트워크 어댑터)를 선택합니다. Adapter Type(어댑터 유형) 섹션에서 현재 어댑터는 E1000임을 알 수 있습니다. 이 어댑터를 VMXNET3 어댑터로 교체해보겠습니다.

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

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

5. 추가를 선택하여 Add Hardware 마법사를 엽니다.
6. Ethernet Adapter(이더넷 어댑터)를 선택한 후 다음을 선택합니다.
7. 네트워크 유형 마법사에서 어댑터 유형으로 **VMXNET3**을 선택한 후 다음을 선택합니다.
8. Virtual Machine Properties 마법사의 Adapter Type(어댑터 유형) 섹션에서 Current Adapter(현재 어댑터)가 VMXNET3로 설정되어 있는지 확인한 후 확인을 선택합니다.
9. VMware VSphere 클라이언트에서 해당 게이트웨이를 종료합니다.
10. VMware VSphere 클라이언트에서 해당 게이트웨이를 재시작합니다.

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

네트워크용 어댑터를 구성하려면

1. VSphere 클라이언트에서 Console(콘솔) 탭을 선택하여 로컬 콘솔을 시작합니다. 이 구성 작업을 위해서는 기본 로그인 자격 증명을 사용하여 게이트웨이의 로컬 콘솔에 로그인해야 합니다. 기본 자격 증명을 사용하여 로그인하는 방법에 대한 자세한 내용은 기본 자격 증명을 사용하여 로컬 콘솔에 로그인을 참조하세요.
2. 프롬프트에서 해당 숫자를 입력하여 네트워크 구성을 선택합니다.
3. 프롬프트에서 해당 숫자를 입력하여 모두 DHCP로 재설정을 선택한 후 프롬프트에 **y**(예)를 입력하여 모든 어댑터가 Dynamic Host Configuration Protocol(DHCP)을 사용하도록 설정합니다. 모든 사용 가능 어댑터가 DHCP를 사용하도록 설정됩니다.

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

여러 개의 NIC에 게이트웨이 구성

여러 개의 네트워크 어댑터(NIC)를 사용하도록 게이트웨이를 구성하면 한 개 이상의 IP 주소에서 게이트웨이에 액세스할 수 있습니다. 이 방법은 다음과 같은 상황에서 사용할 수 있습니다.

- 처리량 극대화 - 네트워크 어댑터에 병목 현상이 발생하는 경우, 처리량을 극대화하고자 할 수 있습니다.
- 애플리케이션 분리 – 애플리케이션이 게이트웨이의 볼륨에 데이터를 기록하는 방식을 분리해야 할 수 있습니다. 예를 들어 중요 스토리지 애플리케이션이 게이트웨이에 정의한 특정 어댑터 한 개를 배타적으로 사용하도록 선택할 수 있습니다.
- 네트워크 제약 - 애플리케이션 환경에 따라 iSCSI 대상 및 이에 접속하는 이니시에이터를 게이트웨이가 AWS와 통신하는 데 사용하는 네트워크가 아닌 고립된 네트워크로 제한해야 하는 경우가 있을 수 있습니다.

일반적인 다중 어댑터 사용 사례에서는 하나의 어댑터가 게이트웨이가 통신하는 경로 AWS (즉, 기본 게이트웨이)로 구성됩니다. 이 어댑터 한 개를 제외하고 초기자는 자신이 접속하는 iSCSI 대상을 포함하는 어댑터와 동일한 서브넷에 있어야 합니다. 그렇지 않은 경우, 원하는 대상과의 통신이 불가능할 수 있습니다. 대상이 통신에 사용되는 동일한 어댑터에 구성된 경우 해당 대상 및 트래픽에 대한 AWS iSCSI AWS 트래픽은 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 하나의 네트워크 어댑터가 정의되어 있다고 가정하고 VMware ESXi에 어댑터를 추가하는 방법에 대해 설명합니다.

VMware ESXi 호스트에서 추가 네트워크 어댑터를 사용하도록 게이트웨이를 구성하려면

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

이 절차를 위해 VM을 켠 상태로 유지할 수 있습니다.

3. 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 설정 편집을 선택합니다.
4. 가상 컴퓨터 속성 대화 상자의 하드웨어 탭에서 추가를 선택하여 디바이스를 추가합니다.
5. Add Hardware 마법사의 안내에 따라 네트워크 어댑터를 추가합니다.

   a. 디바이스 유형 창에서 Ethernet Adapter(이더넷 어댑터)를 선택하여 어댑터를 추가한 후 다음을 선택합니다.

   b. 네트워크 유형 창에서 전원이 켜질 때 연결이 유형으로 선택되어 있는지 확인한 후 다음을 선택합니다.

      Storage Gateway에서는 VMXNET3 네트워크 어댑터를 사용하는 것이 좋습니다. 어댑터 목록에 표시될 어댑터 유형에 대한 자세한 내용은 ESXi 및 vCenter Server 설명서의 네트워크 어댑터 유형 섹션을 참조하세요.

   c. Ready to Complete(완료 준비) 창에서 해당 정보를 검토한 후 Finish(완료)를 선택합니다.
6. VM의 요약 탭을 선택하고 IP 주소 상자 옆에 있는 모두 보기를 선택합니다. 게이트웨이에 액세스할 때 사용할 수 있는 모든 IP 주소가 가상 머신 IP 주소 창에 표시됩니다. 게이트웨이에 두 번째 IP 주소가 표시되는지 확인합니다.

   > **Note**
   >
   > 어댑터 변경 사항이 적용되고 VM 요약 정보가 새로 고침되려면 약간의 시간이 걸릴 수 있습니다.

7. Storage Gateway 콘솔에서 게이트웨이의 전원을 켭니다.
8. Storage Gateway의 탐색 창에서 게이트웨이를 선택한 후 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 VM 로컬 콘솔에서 작업 수행 섹션을 참조하세요.

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 가상 머신 패널에서 해당 게이트웨이 가상 머신을 선택합니다.
3. 게이트웨이 VM이 아직 꺼져 있지 않은 경우 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 끄기를 선택합니다.
4. 게이트웨이 VM 이름을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 다음 설정을 선택합니다.
5. 설정 대화 상자의 하드웨어에서 하드웨어 추가를 선택합니다.
6. 설정 대화 상자 오른쪽에 있는 하드웨어 추가 패널에서 네트워크 어댑터를 선택한 다음 추가를 선택하여 디바이스를 추가합니다.
7. 네트워크 어댑터를 구성한 후 적용을 선택하여 설정을 적용합니다.
8. 설정 대화 상자의 하드웨어에서 새 네트워크 어댑터가 하드웨어 목록에 추가되었는지 확인한 다음 확인을 선택합니다.
9. Storage Gateway 콘솔을 사용하여 게이트웨이를 켭니다.
10. Storage Gateway 콘솔의 탐색 패널에서 게이트웨이를 선택한 다음 어댑터를 추가한 게이트웨이를 선택합니다. 세부 정보 탭에 두 번째 IP 주소가 표시되는지 확인합니다.

VMware, Hyper-V 및 KVM 호스트의 공통 로컬 콘솔 작업에 대한 자세한 내용은 VM 로컬 콘솔에서 작업 수행 섹션을 참조하세요.

Storage Gateway와 함께 VMware vSphere High Availability 사용

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

vSphere HA는 중복성을 위해 가상 머신과 해당 가상 머신이 상주하는 호스트를 클러스터로 풀링하여 작동합니다. 클러스터의 호스트를 모니터링하여 장애가 발생하면 장애가 발생한 호스트의 가상 머신이 대체 호스트에서 다시 시작됩니다. 일반적으로 이러한 복구는 데이터 손실 없이 신속하게 이루어집니다. vSphere HA에 대한 자세한 내용은 VMware 설명서의 How vSphere HA Works을 참조하세요.

> **Note**
>
> 장애가 발생한 가상 머신을 다시 시작하고 새 호스트에서 iSCSI 연결을 다시 설정하는 데 필요한 시간은 호스트 운영 체제 및 리소스 로드, 디스크 속도, 네트워크 연결, SAN/스토리지 인프라 등 여러 요인에 따라 달라집니다. 장애 조치 가동 중지 시간을 최소화하려면 게이트웨이 성능 최적화에 설명된 권장 사항을 구현하세요.
> VMware HA와 함께 Storage Gateway를 사용하려면 다음 작업을 수행하는 것이 좋습니다.
>
> - Storage Gateway VM이 포함된 VMware ESX `.ova` 다운로드 가능 패키지를 클러스터의 호스트 한 곳에만 배포합니다.
> - `.ova` 패키지를 배포할 때 호스트 한 곳에 대해 로컬이 아닌 데이터 스토어를 선택합니다. 그 대신에 클러스터의 모든 호스트에 액세스할 수 있는 데이터 스토어를 사용합니다. 호스트에 대해 로컬인 데이터 스토어를 선택하였는데 호스트에 장애가 생긴 경우에는 데이터 원본이 클러스터 내 기타 호스트에 액세스할 수 없고 다른 호스트에 대한 장애 조치가 성공하지 못할 수 있습니다.
> - 장애 조치 중에 초기자가 스토리지 볼륨과 접속이 끊기지 않도록 하려면 운영 체제에 권장되는 iSCSI 설정을 사용하십시오. 장애 조치 이벤트 중에는 게이트웨이 VM이 장애 조치 클러스터의 새 호스트에서 시작하는 데 몇 초에서 몇 분이 걸릴 수 있습니다. Windows 및 Linux 클라이언트에 대한 권장 iSCSI 제한 시간은 장애 조치 이벤트가 발생하는 데 걸리는 일반적인 시간보다 더 깁니다. 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 설정을 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 방법에 대해 설명합니다.

주제

- vSphere VMware HA 클러스터 구성
- Storage Gateway 콘솔에서 .ova 이미지를 다운로드합니다.
- 게이트웨이 배포
- (선택 사항) 클러스터의 다른 VM에 대한 재정의 옵션 추가
- 게이트웨이 활성화

- VMware 고가용성 구성 테스트

vSphere VMware HA 클러스터 구성

먼저 아직 VMware 클러스터를 생성하지 않은 경우 클러스터를 생성합니다. VMware 클러스터를 생성하는 방법에 대한 자세한 내용은 VMware 설명서의 vSphere HA 클러스터 생성을 참조하세요.

그런 다음 VMware 클러스터가 Storage Gateway와 함께 작동하도록 구성합니다.

VMware 클러스터를 구성하려면

1. VMware vSphere의 Edit Cluster Settings(클러스터 설정 편집) 페이지에서 VM 모니터링이 VM 및 애플리케이션 모니터링용으로 구성되어 있는지 확인합니다. 이렇게 하려면 각 옵션에 대해 다음 값을 설정합니다.

   - Host Failure Response(호스트 실패 응답): Restart VMs(VM 다시 시작)
   - Response for Host Isolation(호스트 격리에 대한 응답): Shut down and restart VMs(VM 종료 및 다시 시작)
   - Datastore with PDL(PDL 포함 데이터 스토어): 비활성화
   - Datastore with APD(APD 포함 데이터 스토어): 비활성화
   - VM Monitoring(VM 모니터링): VM and Application Monitoring(VM 및 애플리케이션 모니터링)
2. 다음 값을 조정하여 클러스터의 민감도를 미세 조정합니다.

   - 실패 간격 - 이 간격이 지나면 VM 하트비트가 수신되지 않을 경우 VM이 다시 시작됩니다.
   - 최소 가동 시간 - VM이 VM 도구의 하트비트 모니터링을 시작한 후 클러스터가 이 시간 동안 기다립니다.
   - VM당 최대 재설정 - 클러스터가 최대 재설정 시간 내에서 VM을 이 최대 횟수만큼 다시 시작합니다.
   - 최대 재설정 시간 - VM 재설정당 최대 재설정 횟수를 계산할 시간입니다.

   설정할 값을 잘 모르는 경우 다음 설정 예를 사용합니다.

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

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

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 설정에 설명된 대로.ova를 다운로드합니다.

게이트웨이 배포

구성된 클러스터에서 .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.

게이트웨이 .ova 이미지를 배포하려면

1. .ova 이미지를 클러스터의 호스트 중 하나에 배포합니다.
2. 루트 디스크 및 캐시에 대해 선택한 데이터 스토어를 클러스터의 모든 호스트에서 사용할 수 있는지 확인합니다. VMware 또는 온프레미스 환경에 Storage Gateway .ova 파일을 배포하는 경우 디스크를 반가상화된 SCSI 디스크라고 합니다. 반가상화는 VM에 추가하는 가상 디스크를 콘솔이 식별할 수 있도록 게이트웨이 VM이 호스트 운영 체제와 협력하는 모드입니다.

   VM을 구성하여 반가상화된 컨트롤러를 사용하려면

   1. VMware vSphere 클라이언트에서 게이트웨이 VM을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 연 후 설정 편집을 선택합니다.
   2. Virtual Machine Properties(가상 머신 속성) 대화 상자에서 Hardware(하드웨어) 탭을 선택하고 SCSI controller 0(SCSI 컨트롤러 0)을 선택한 후 Change Type(유형 변경)을 선택합니다.
   3. Change SCSI Controller Type(SCSI 컨트롤러 유형 변경) 대화 상자에서 VMware Paravirtual(VMware 반가상화) SCSI 컨트롤러 유형을 선택한 후 확인을 선택합니다.

(선택 사항) 클러스터의 다른 VM에 대한 재정의 옵션 추가

클러스터에서 다른 VM이 실행 중인 경우 각 VM에 맞게 클러스터 값을 설정할 수 있습니다. 지침은 VMware vSphere 온라인 설명서에서 Customize an Individual Virtual Machine을 참조하세요.

클러스터의 다른 VM에 대한 재정의 옵션을 추가하려면

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

   vSphere HA - VM 모니터링에서 각 옵션에 대해 다음 값을 설정합니다.

   - VM 모니터링: 재정의 사용 - VM 및 애플리케이션 모니터링
   - VM 모니터링 민감도: 재정의 사용 - VM 및 애플리케이션 모니터링
   - VM 모니터링: 사용자 지정
   - 실패 간격: **30**초
   - 최소 가동 시간: **120**초
   - Maximum per-VM resets(VM당 최대 재설정): **5**
   - 최대 재설정 기간: **1**시간 이내

게이트웨이 활성화

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

게이트웨이를 활성화하려면

- 다음 주제에 설명된 절차를 따릅니다.

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

2. 탐색 창에서 게이트웨이를 선택한 다음 VMware HA에 대해 테스트할 게이트웨이를 선택합니다.
3. 작업에서 Verify VMware HA(VMware HA 확인)를 선택합니다.
4. Verify VMware High Availability Configuration(VMware 고가용성 구성 확인) 상자가 나타나면 확인을 선택합니다.

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

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

Amazon CloudWatch 로그 그룹에서 VMware HA 이벤트에 대한 정보를 찾을 수 있습니다. 자세한 내용은 CloudWatch 로그 그룹을 사용하여 Tape Gateway 상태 로그 가져오기를 참조하세요.

Tape Gateway 스토리지 리소스 작업

이 단원의 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 방법에 대해 설명합니다.

주제

- 게이트웨이에서 디스크 제거 - 디스크에 장애가 발생한 경우와 같이 게이트웨이의 가상 호스트 플랫폼에서 디스크를 제거해야 하는 경우에 취해야 할 조치에 대해 알아봅니다.
- Amazon EC2 게이트웨이에서 Amazon EBS 볼륨 관리 - Amazon EC2 인스턴스에서 호스팅되는 게이트웨이의 업로드 버퍼 또는 캐시 스토리지로 사용하도록 할당된 Amazon EBS 볼륨의 양을 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.

VMware ESXi에 호스팅된 게이트웨이에서 디스크 제거

다음 절차에 따라 VMware 하이퍼바이저에서 호스팅하는 게이트웨이에서 디스크를 제거할 수 있습니다.

업로드 버퍼에 할당된 디스크를 제거하려면(VMware ESXi)

1. vSphere 클라이언트에서 마우스 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 열고 게이트웨이 VM의 이름을 선택한 후 설정 편집을 선택합니다.
2. 가상 머신 속성 대화 상자의 하드웨어 탭에서 업로드 버퍼 공간으로 할당된 디스크를 선택한 다음 제거를 선택합니다.

   가상 머신 속성 대화 상자의 가상 디바이스 노드 값이 이전에 기록한 값과 같은지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.
3. Removal Options(제거 옵션) 패널에서 옵션을 선택한 후 확인을 선택하여 디스크 제거 절차를 완료합니다.

Microsoft Hyper-V에 호스팅된 게이트웨이에서 디스크 제거

다음 절차에 따라 Microsoft Hyper-V 하이퍼바이저에서 호스팅하는 게이트웨이에서 디스크를 제거할 수 있습니다.

업로드 버퍼에 할당된 기본 디스크를 제거하려면(Microsoft Hyper-V)

1. Microsoft Hyper-V Manager에서 마우스 오른쪽 버튼을 클릭하여 컨텍스트 메뉴를 열고 게이트웨이 VM의 이름을 선택한 후 설정을 선택합니다.
2. 설정 대화 상자의 하드웨어 목록에서 제거할 디스크를 선택한 다음 제거를 선택합니다.

게이트웨이에 추가한 디스크는 하드웨어 목록의 SCSI 컨트롤러 항목 아래에 표시됩니다. 컨트롤러 및 위치 값이 앞에서 기록해 둔 값과 동일한지 확인합니다. 이렇게 하면 해당되는 디스크를 정확히 제거하는 데 도움이 됩니다.

Microsoft Hyper-V Manager에 표시된 첫 번째 SCSI 컨트롤러는 0번 컨트롤러입니다.

3. 확인을 선택하여 변경 사항을 적용합니다.

Linux KVM에 호스팅된 게이트웨이에서 디스크 제거

Linux 커널 기반 가상 머신(KVM) 하이퍼바이저에 호스팅된 게이트웨이에서 디스크를 분리하려면 다음과 유사한 `virsh` 명령을 사용할 수 있습니다.

```
$ virsh detach-disk domain_name /device/path
```

KVM 디스크 관리에 대한 자세한 내용은 Linux 배포판 설명서를 참조하십시오.

Amazon EC2 게이트웨이에서 Amazon EBS 볼륨 관리

처음에 게이트웨이가 Amazon EC2 인스턴스로 실행되도록 구성할 때 업로드 버퍼 및 캐시 스토리지로 사용할 Amazon EBS 볼륨을 할당했습니다. 추후 애플리케이션 요구 사항에 따라 이 용도로 Amazon EBS 볼륨을 추가 할당할 수 있습니다. 이전에 할당한 Amazon EBS 볼륨을 제거하여 할당한 스토리지를 줄일 수도 있습니다. Amazon EBS에 대한 자세한 내용은 Amazon EC2 사용 설명서에서 Amazon Elastic Block Store(Amazon EBS)를 참조하세요.

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. 인스턴스에 원하는 만큼의 Amazon EBS 볼륨을 연결할 수 있지만, 이러한 볼륨은 해당 스토리지 할당량까지만 업로드 버퍼 및 캐시 스토리지 공간으로 구성할 수 있습니다. 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오.

Amazon EBS 볼륨을 추가하고 게이트웨이에 맞게 구성하려면

1. Amazon EBS 볼륨을 생성합니다. 지침은 Amazon EC2 사용 설명서에서 Amazon EBS 볼륨 생성 또는 복원을 참조하세요.

2. Amazon EC2 인스턴스에 Amazon EBS 볼륨을 연결합니다. 지침은 Amazon EC2 사용 설명서에서 인스턴스에 Amazon EBS 볼륨 연결을 참조하세요.
3. 업로드 버퍼 또는 캐시 스토리지로 추가한 Amazon EBS 볼륨을 구성합니다. 지침은 Storage Gateway의 로컬 디스크 관리 섹션을 참조하세요.

업로드 버퍼에 할당한 스토리지 용량이 필요 없다는 판단을 내리게 되는 경우가 있습니다.

Amazon EBS 볼륨을 제거하려면

> **Warning**
>
> 이 단계는 업로드 버퍼 공간으로 할당된 Amazon EBS 볼륨에만 적용되며 캐시에 할당된 볼륨에는 적용되지 않습니다. 캐시 스토리지로 할당된 Amazon EBS 볼륨을 Tape Gateway에서 제거하면 게이트웨이의 가상 테이프가 IRRECOVERABLE 상태가 되어 데이터가 손실될 위험이 있습니다. IRRECOVERABLE 상태에 대한 자세한 내용은 VTL에서 테이프 상태 정보 파악 섹션을 참조하세요.

1. 게이트웨이 VM 종료 단원에서 설명하는 접근 방식에 따라 게이트웨이를 종료합니다.
2. Amazon EC2 인스턴스에서 Amazon EBS 볼륨을 분리합니다. 지침은 Amazon EC2 사용 설명서에서 인스턴스에서 Amazon EBS 볼륨 분리를 참조하세요.
3. Amazon EBS 볼륨을 삭제합니다. 지침은 Amazon EC2 사용 설명서에서 Amazon EBS 볼륨 삭제를 참조하세요.
4. 게이트웨이 VM 종료 단원에서 설명하는 접근 방식에 따라 게이트웨이를 시작합니다.

VTL 디바이스 작업

Tape Gateway를 활성화할 때 목록에서 백업 애플리케이션을 선택하고 적절한 미디어 체인저를 사용합니다. 백업 애플리케이션이 목록에 없는 경우 기타를 선택한 후 백업 애플리케이션에 사용할 미디어 체인저를 선택합니다. 지원되는 백업 애플리케이션에 권장되는 미디어 체인저 목록은 섹션을 참조하세요https://docs.aws.amazon.com/storagegateway/latest/tgw/Requirements.html#requirements-backup-sw-for-vtl.

Tape Gateway 설정은 게이트웨이를 활성화할 때 선택하는 다음과 같은 iSCSI 디바이스를 제공합니다.

중간 체인저:

- AWS-Gateway-VTL - 이 디바이스는 게이트웨이와 함께 제공됩니다.
- STK-L700 - 이 디바이스 에뮬레이션은 게이트웨이와 함께 제공됩니다.

테이프 드라이브:

- IBM-ULT3580-TD5 - 이 디바이스 에뮬레이션은 게이트웨이와 함께 제공됩니다.

주제

- 게이트웨이 활성화 후 미디어 체인저 선택
- 미디어 체인저의 디바이스 드라이버 업데이트
- Microsoft System Center DPM에서 테이프의 바코드 표시

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 초기자 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, 변경하려는 미디어 체인저를 선택한 후 미디어 체인저 변경을 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 드라이버는 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 Sony, 모델 목록에서 Sony - TSL-A500C Autoloader를 선택한 후 다음을 선택합니다.
6. 이어 나타나는 경고 상자에서 예를 선택합니다. 드라이버가 성공적으로 설치되었으면 Update drive software(드라이브 소프트웨어 업데이트) 창을 닫습니다.

Microsoft System Center DPM에서 테이프의 바코드 표시

Sony TSL-A500C Autoloader에 미디어 체인저 드라이버를 사용할 경우 Microsoft System Center Data Protection Manager는 Storage Gateway에서 생성된 가상 테이프의 바코드를 자동으로 표시하지 않습니다. 테이프의 바코드를 제대로 표시하려면 미디어 체인저 드라이버를 Sun/StorageTek Library로 변경하십시오.

바코드를 표시하려면

1. 모든 백업 작업이 완료되었고 보류 중이거나 진행 중인 작업이 없는지 확인합니다.
2. 테이프를 꺼내서 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)로 옮기고 DPM Administrator 콘솔을 종료합니다. DPM에서 테이프를 꺼내는 방법에 대한 정보는 DPM을 사용한 테이프 보관 단원을 참조하십시오.
3. 관리 도구에서 서비스를 선택한 후 자세히 창에서 DPM 서비스 를 마우스 오른쪽 버튼으로 클릭하여 바로 가기 메뉴를 열고 속성을 선택합니다.

4. 일반 탭에서 시작 유형이 자동으로 설정되었는지 확인하고 중지를 선택하여 DPM 서비스를 중지합니다.
5. Microsoft 웹 사이트의 Microsoft 업데이트 카탈로그에서 StorageTek 드라이버를 다운로드합니다.

   > **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 Library로 표시됩니다. 테이프 드라이브는 IBM ULT3580-TD5 SCSI 시퀀스 디바이스로 유지됩니다.
9. DPM 서버를 재부팅합니다.
10. Storage Gateway 콘솔에서 새 테이프를 생성합니다.
11. DPM 관리자 콘솔에서 관리를 선택한 후 Rescan for new tape libraries(새 테이프 라이브러리 다시 검색)를 선택합니다 . Sun/StorageTek library가 표시됩니다.
12. 라이브러리를 선택하고 인벤토리를 선택합니다.
13. 테이프 추가를 선택하여 DPM에 새 테이프를 추가합니다. 새 테이프가 해당 바코드를 표시합니다.

가상 테이프 라이브러리에서 테이프 관리

Storage Gateway는 활성화하는 Tape Gateway마다 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. 테이프의 상태는 테이프에 쓸 수 있도록 사용 가능 상태이어야 합니다. 이러한 테이프는 Amazon Simple Storage Service(S3)의 지원을 받습니다. 즉, 이러한 테이프에 데이터를 쓰면 Tape Gateway가 Amazon S3에 데이터를 저장합니다. 자세한 내용은 VTL에서 테이프 상태 정보 파악 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. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 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 보관 프로세스는 다음과 같이 IN TRANSIT TO VTS, ARCHIVING 및 ARCHIVED 테이프 상태로 표시되는 세 단계로 이루어집니다.

- 테이프를 백업하려면 백업 애플리케이션이 제공하는 명령을 사용합니다. 보관 프로세스가 시작되면 테이프가 IN TRANSIT TO VTS 상태로 바뀌고 백업 애플리케이션에 액세스할 수 없게 됩니다. 이 단

계에서는 Tape Gateway가 데이터를에 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 ARCHIVING으로 변경되고 Storage Gateway가 테이프를 아카이브로 이동하기 시작합니다. 이 시점에서는 보관 프로세스를 취소할 수 없습니다.
- 테이프를 아카이브로 옮기고 나면 ARCHIVED 상태로 변하고 해당 테이프를 원하는 게이트웨이로 가져올 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 Gateway에서 데이터를 AWS로 업로드하고 있습니다.
- ARCHIVING: 데이터 업로드가 완료되어 Tape Gateway에서 테이프를 아카이브로 옮기고 있습니다.
- ARCHIVED: 테이프를 다 옮겼고 아카이브가 가져오기 작업을 할 준비가 되었습니다.

테이프의 상태가 IN TRANSIT TO VTS인 경우에만 보관을 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 보관을 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 참조에서 ActivateGateway를 참조하십시오.

> **Note**
>
> 게이트웨이 활성화 키는 사용하지 않으면 30분 후에 만료됩니다.

게이트웨이 VM에 대한 요청에는 활성화가 발생하는 AWS 리전이 포함됩니다. 응답에 리디렉션으로 반환되는 URL에는 `activationkey`라는 쿼리 문자열 파라미터가 포함되어 있습니다. 이 쿼리 문자열 파라미터는 정품 인증 키입니다. 쿼리 문자열의 형식은 다음과 같습니다. `http://`*`gateway_ip_address`*`/?activationRegion=`*`activation_region`*. 이 쿼리의 출력은 활성화 리전과 활성화 키를 모두 반환합니다.

이 URL에는 VPC 엔드포인트 유형을 사용하여 연결하는 게이트웨이의 VPC 엔드포인트 ID인 `vpcEndpoint`도 포함되어 있습니다.

> **Note**
>
> 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)
- Microsoft Windows PowerShell
- 로컬 콘솔 사용

Linux(curl)

다음 예에서는 Linux(curl)를 사용하여 활성화 키를 받는 방법을 보여줍니다.

> **Note**
>
> 강조 표시된 변수를 게이트웨이의 실제 값으로 바꿉니다. 가능한 값은 다음과 같습니다.

- *gateway_ip_address* - 게이트웨이의 IPv4 주소입니다(예: 172.31.29.201).
- *gateway_type* - 활성화하려는 게이트웨이의 유형입니다(예: STORED, CACHED, VTL, FILE_S3, FILE_FSX_SMB).
- *region_code* - 게이트웨이를 활성화할 리전입니다.AWS 일반 참조 안내서에서 리전 엔드포인트를 참조하세요. 이 파라미터가 지정되지 않았거나 제공된 값의 철자가 잘못되었거나 유효한 리전과 일치하지 않는 경우 명령은 기본적으로 us-east-1 리전으로 설정됩니다.
- *vpc_endpoint* - 게이트웨이의 VPC 엔드포인트 이름입니다(예: vpce-050f90485f28f2fd0-iep0e8vq.storagegateway.us-west-2.vpce.amazonaws.com).

표준 엔드포인트

표준 엔드포인트의 활성화 키를 가져오는 방법:

```
curl "http://gateway_ip_address/?activationRegion=region_code&no_redirect"
```

듀얼 스택 엔드포인트

듀얼 스택 엔드포인트의 활성화 키를 가져오는 방법:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=DUALSTACK&ipVersion=ipv6&no_redirect"
```

FIPS 엔드포인트

FIPS 엔드포인트의 활성화 키를 가져오는 방법:

IPv4

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv4&no_redirect"
```

IPv6

```
curl "http://gateway_ip_address/?
activationRegion&endpointType=FIPS_DUALSTACK&ipVersion=ipv6&no_redirect"
```

VPC 엔드포인트

VPC 엔드포인트의 활성화 키를 받으려면:

```
curl "http://gateway_ip_address/?
activationRegion=region_code&vpcEndpoint=vpc_endpoint&no_redirect"
```

Linux(bash/zsh)

다음 예제는 Linux(bash/zsh)를 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```
function get-activation-key() {
  local ip_address=$1
  local activation_region=$2
  if [[ -z "$ip_address" || -z "$activation_region" || -z "$gateway_type" ]]; then
    echo "Usage: get-activation-key ip_address activation_region gateway_type"
    return 1
  fi

  if redirect_url=$(curl -f -s -S -w '%{redirect_url}' "http://$ip_address/?
activationRegion=$activation_region&gatewayType=$gateway_type"); then
    activation_key_param=$(echo "$redirect_url" | grep -oE 'activationKey=[A-Z0-9-]+')
    echo "$activation_key_param" | cut -f2 -d=
  else
    return 1
  fi
}
```

Microsoft Windows PowerShell

다음 예제는 Microsoft Windows PowerShell을 사용하여 HTTP 응답을 가져오고, HTTP 헤더를 구문 분석하고, 활성화 키를 받는 방법을 보여줍니다.

```
function Get-ActivationKey {
  [CmdletBinding()]
  Param(
    [parameter(Mandatory=$true)][string]$IpAddress,
    [parameter(Mandatory=$true)][string]$ActivationRegion,
    [parameter(Mandatory=$true)][string]$GatewayType
  )
  PROCESS {
    $request = Invoke-WebRequest -UseBasicParsing -Uri "http://$IpAddress/?
activationRegion=$ActivationRegion&gatewayType=$GatewayType" -MaximumRedirection 0 -
ErrorAction SilentlyContinue
    if ($request) {
      $activationKeyParam = $request.Headers.Location | Select-String -Pattern
 "activationKey=([A-Z0-9-]+)"
      $activationKeyParam.Matches.Value.Split("=")[1]
    }
  }
}
```

로컬 콘솔 사용

다음 예제에서는 로컬 콘솔을 사용하여 활성화 키를 생성하고 표시하는 방법을 보여줍니다.

Amazon Linux 2(AL2) 기반 게이트웨이

AL2 기반 게이트웨이의 표준 또는 FIPS 엔드포인트를 선택할 수 있습니다.

> **Note**
>
> FIPS 엔드포인트를 전혀 사용할 수 없습니다 AWS 리전. 자세한 내용은 서비스별 FIPS 엔드포인트를 참조하세요.

로컬 콘솔에서 AL2-based 게이트웨이의 활성화 키를 가져오려면

1. 로컬 콘솔에 관리자로 로그인합니다.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 0를 선택하여 활성화 키 가져오기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 게이트웨이를 활성화하려는 AWS 리전을 입력합니다.
5. 네트워크 유형에 퍼블릭 1 또는 VPC에 2를 입력합니다.

6. 엔드포인트 유형에 1 표준 또는 연방 정보 처리 표준(FIPS)2을 입력합니다.

Amazon Linux 2023(AL2023) 기반 게이트웨이

AL2023 기반 게이트웨이의 경우 다음 엔드포인트를 사용할 수 있습니다.

- 표준 엔드포인트(IPv4만 지원)
- FIPS 엔드포인트(IPv4만 지원)
- 듀얼 스택 엔드포인트(IPv4 및 IPv6 지원)
- 듀얼 스택 FIPS 엔드포인트(IPv4 및 IPv6 지원)

자세한 내용은 엔드포인트 유형 단원을 참조하십시오.

로컬 콘솔에서 AL2023-based 게이트웨이의 활성화 키를 가져오려면

1. 로컬 콘솔에 로그인합니다. Amazon EC2 인스턴스에 연결하는 경우, admin으로 로그인합니다.
2. AWS 어플라이언스 활성화 - 구성 기본 메뉴에서 0를 선택하여 활성화 키 가져오기를 선택합니다.
3. 게이트웨이 제품군 옵션으로 Storage Gateway를 선택합니다.
4. 게이트웨이를 활성화하려는 AWS 리전을 입력합니다.
5. 네트워크 유형에 퍼블릭 1 또는 VPC 엔드포인트에 2를 입력합니다.
6. 엔드포인트 유형 선택, FIPS 활성화?에 FIPSY를 활성화하거나 비 FIPS 엔드포인트를 사용하려면 N를 입력합니다.
7. 엔드포인트 유형에 표준 엔드포인트 1 또는 듀얼 스택 엔드포인트2에를 입력합니다.
    - 듀얼 스택 엔드포인트의 경우 IP 버전 선택 또는 종료:에 IPv4 또는 IPv61에 2를 입력합니다.

iSCSI 초기자 연결

게이트웨이를 관리할 때는 iSCSI(Internet Small Computer System Interface) 대상으로 노출되는 볼륨 또는 가상 테이프 라이브러리(VTL) 디바이스로 작업합니다. Volume Gateway의 경우, iSCSI 대상은 볼륨입니다. Tape Gateway의 경우 대상은 VTL 디바이스입니다. 이 작업의 일부로 이 대상에 대한 연결, iSCSI 설정에 대한 사용자 지정, Red Hat Linux 클라이언트에서 연결, 챌린지-핸드셰이크 인증 규약(CHAP) 구성과 같은 작업을 합니다.

주제

- Windows 클라이언트에 VTL 디바이스 연결

- Linux 클라이언트에 VTL 디바이스 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 목록에서는 iSCSI 연결 및 관련 구성 요소를 설명하는 데 사용하는 용어 중 일부를 정의합니다.

iSCSI 초기자

iSCSI 네트워크의 클라이언트 구성 요소. 초기자는 iSCSI 대상에 요청을 전송합니다. 이니시에이터는 소프트웨어 또는 하드웨어로 구현할 수 있습니다. Storage Gateway는 소프트웨어 이니시에이터만 지원합니다.

iSCSI 대상

초기자의 요청을 수신하고 응답하는 iSCSI 네트워크의 서버 구성 요소. 각 볼륨은 iSCSI 대상으로 노출됩니다. 각 iSCSI 대상에 iSCSI 초기자를 하나만 연결합니다.

Microsoft iSCSI 초기자

클라이언트 컴퓨터(즉 게이트웨이에 쓰려는 데이터를 보유한 애플리케이션을 실행하는 컴퓨터)를 외부 iSCSI 기반 어레이(즉 게이트웨이)에 연결할 수 있게 해주는 Microsoft Windows 컴퓨터의 소프트웨어 프로그램입니다. 호스트 컴퓨터의 이더넷 네트워크 어댑터 카드를 사용하여 연결합니다. Microsoft iSCSI 이니시에이터는 Windows Server 2022의 Storage Gateway로 검증되었습니다. 이니시에이터는 운영 체제에 내장되어 있습니다.

Red Hat iSCSI 초기자

`iscsi-initiator-utils` 리소스 패키지 관리자(RPM) 패키지에서는 Red Hat Linux용 소프트웨어로 구현된 iSCSI 이니시에이터를 제공합니다. 이 패키지는 iSCSI 프로토콜용 서버 데몬을 포함합니다.

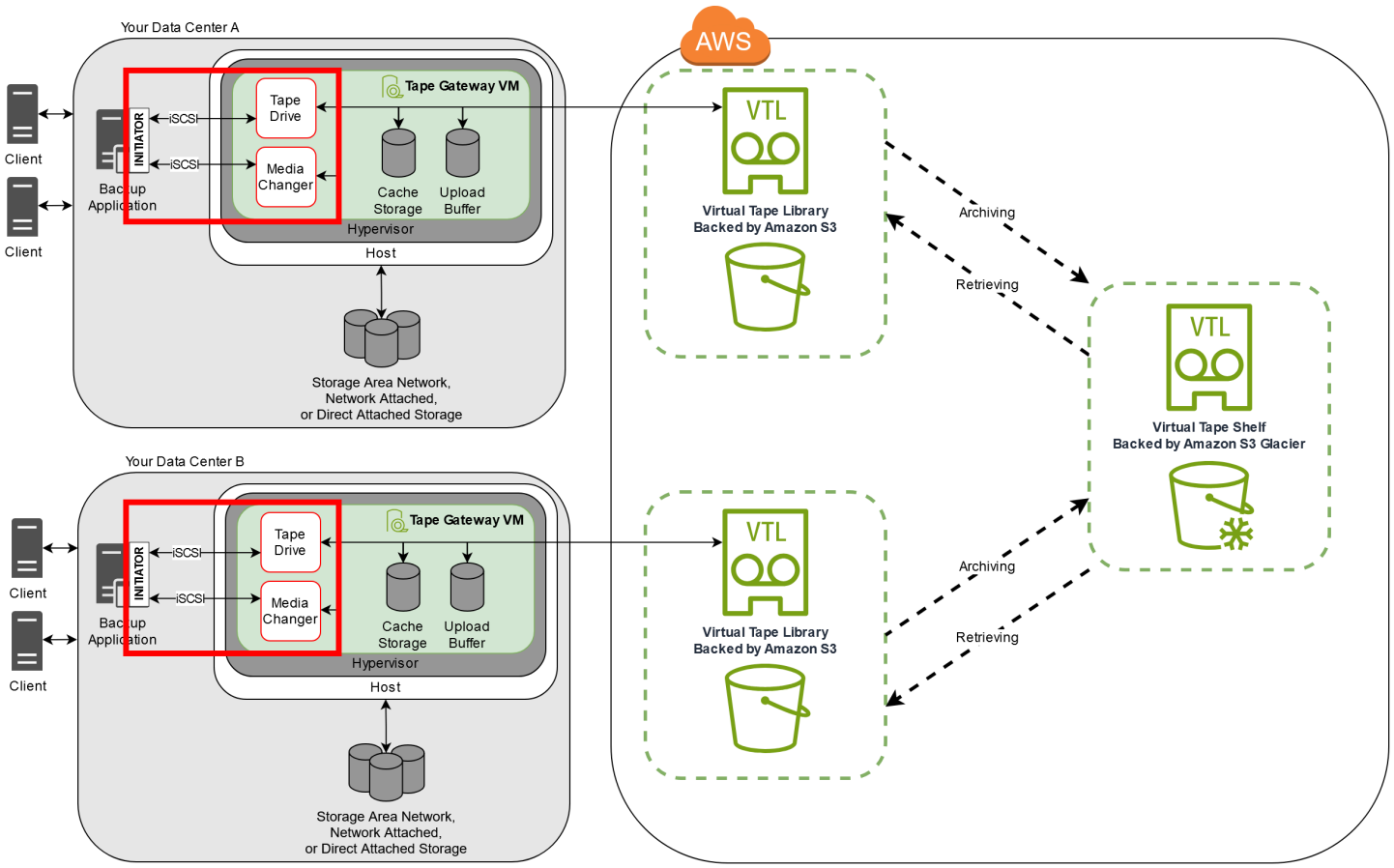
게이트웨이의 각 유형은 iSCSI 디바이스에 연결할 수 있고, 이러한 연결은 다음 설명과 같이 사용자 지정할 수 있습니다.

Windows 클라이언트에 VTL 디바이스 연결

Tape Gateway는 여러 개의 테이프 드라이브와 미디어 체인저(통칭하여 VTL 디바이스라고 함)를 iSCSI 대상으로 노출합니다. 자세한 내용은 Tape Gateway 설정 요구 사항 단원을 참조하십시오.

> **Note**
>
> 각 iSCSI 대상에 애플리케이션을 하나만 연결합니다.

아래 다이어그램의 Storage Gateway 아키텍처 확대 그림에서는 iSCSI 대상이 강조 표시되어 있습니다. 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 초기자를 실행하려면 클라이언트 컴퓨터에서 관리자 권한이 있어야 합니다.

2. 선택하라는 메시지가 표시되면 예를 선택하여 Microsoft iSCSI 초기자 서비스를 시작합니다.
3. iSCSI Initiator Properties(iSCSI 이니시에이터 속성) 대화 상자에서 Discovery(검색) 탭을 선택한 다음, Discover Portal(포털 검색)을 선택합니다.
4. 대상 포털 검색 대화 상자에서 IP 주소 또는 DNS 이름에 Tape Gateway의 IP 주소를 입력한 후 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 배포한 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 이니시에이터 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 디아비스 드라이버 목록에서 고르기(Let me pick from a list of device drivers on my computer)를 선택합니다.

d. LTO Tape drive(LTO 테이프 드라이브)를 선택하고 다음을 선택합니다.

e. 닫기를 선택하여 드라이버 소프트웨어 업데이트 창을 닫고 드라이버 공급자 값이 이제 Microsoft로 설정되었는지 확인합니다.

5. 4.1~4.5단계를 반복하여 모든 테이프 드라이브를 업데이트합니다.

Linux 클라이언트에 VTL 디바이스 연결

Red Hat Enterprise Linux(RHEL)를 사용할 경우 `iscsi-initiator-utils` RPM 패키지를 사용하여 게이트웨이 iSCSI 대상(볼륨 또는 VTL 디바이스)에 연결할 수 있습니다.

Linux 클라이언트를 iSCSI 대상에 연결하려면

1. `iscsi-initiator-utils` RPM 패키지가 아직 클라이언트에 설치되지 않은 경우 설치합니다.

   다음 명령을 사용하여 패키지를 설치할 수 있습니다.

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

2. iSCSI 데몬이 실행 중인지 확인합니다.

   a. 다음 명령 중 하나를 사용하여 iSCSI 데몬이 실행 중인지 확인합니다.

      RHEL 8 또는 9의 경우 다음 명령을 사용합니다.

      ```
      sudo service iscsid status
      ```

   b. 상태 명령이 running 상태를 반환하지 않으면 다음 명령 중 하나를 사용하여 데몬을 시작합니다.

      RHEL 8 또는 9의 경우 다음 명령을 사용합니다. 일반적으로 `iscsid` 서비스를 명시적으로 시작할 필요가 없습니다.

      ```
      sudo service iscsid start
      ```

3. 게이트웨이에 정의한 볼륨 또는 VTL 디바이스 대상을 검색하려면 다음 검색 명령을 사용합니다.

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

이전 명령에서 게이트웨이의 IP 주소를 *[GATEWAY_IP]* 변수로 대체합니다. 게이트웨이 IP는 Storage Gateway 콘솔에 있는 볼륨의 iSCSI 대상 정보 속성에서 찾을 수 있습니다.

검색 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

Tape Gateways: iqn.1997-05.com.amazon:*[GATEWAY_IP]*-tapedrive-01

iSCSI 정규화 이름(IQN)은 IQN 값이 조직에 고유한 것이므로 앞선 경우와는 다릅니다. 대상의 이름은 볼륨 생성 시 지정한 이름입니다. Storage Gateway 콘솔에서 볼륨을 선택할 때 iSCSI 대상 정보 속성 창에서도 이 대상 이름을 찾을 수 있습니다.

4. 대상에 접속하려면 다음 명령을 사용하십시오.

   접속 명령에서 올바른 *[GATEWAY_IP]* 및 IQN을 지정해야 한다는 점에 유의하십시오.

   > **Warning**
   >
   > Amazon EC2 인스턴스에 배포한 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
```

5. 볼륨이 클라이언트 머신(초기자)에 연결되었는지 확인하려면 다음 명령을 사용해야 합니다.

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

   이 명령은 다음 예시 출력과 비슷하게 출력됩니다.

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

이니시에이터를 설정한 후 Linux iSCSI 설정을 사용자 지정에서 설명한 것처럼 iSCSI 설정을 사용자 지정할 것을 적극 권장합니다.

iSCSI 설정 사용자 지정

초기자를 설정한 후에 iSCSI 설정을 사용자 지정하여 초기자가 대상과 접속이 끊기는 일을 방지할 것을 적극 권장합니다.

다음 절차와 같이 iSCSI 제한 시간 값을 늘리면 시간이 오래 걸리는 쓰기 작업과 네트워크 장애와 같은 기타 일시적인 문제를 애플리케이션이 더 잘 해결할 수 있습니다.

> **Note**
>
> 레지스트리를 변경하기 전에 레지스트리의 백업 사본을 만들어야 합니다. 백업 복사본을 만드는 방법과 레지스트리 작업 시 따라야 할 기타 모범 사례에 대한 자세한 내용은 Microsoft TechNet Library에서 레지스트리 모범 사례를 참조하세요.

주제

- Windows iSCSI 설정 사용자 지정
- Linux iSCSI 설정을 사용자 지정

Windows iSCSI 설정 사용자 지정

Tape Gateway 설정의 경우, Microsoft iSCSI 이니시에이터를 사용하여 VTL 디바이스에 연결하려면 다음과 같이 두 단계를 거쳐야 합니다.

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. 이 예시에서는 Symantec NetBackup 백업 애플리케이션을 사용합니다. 자세한 내용은 VTL 디바이스 연결 및 NetBackup 스토리지 디바이스 구성 섹션을 참조하세요.

Windows iSCSI 설정을 사용자 지정하려면

1. 요청이 대기하는 최대 시간을 늘립니다.

a. 레지스트리 편집기(Regedit.exe)를 시작합니다.

b. 아래와 같이 iSCSI 컨트롤러 설정을 포함하는 디바이스 클래스에 대한 GUID(Globally Unique Identifier) 키로 이동합니다.

> **Warning**
>
> ControlSet001 또는 ControlSet002와 같은 다른 제어 세트가 아닌 CurrentControlSet 하위 키에서 작업하고 있는지 확인하세요.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}
```

c. 아래에 *[<Instance Number]*로 표시된 Microsoft iSCSI 초기자에 대한 하위 키를 찾습니다.

하위 키는 0000과 같이 네 자리 숫자로 표시됩니다.

```
HKEY_Local_Machine\SYSTEM\CurrentControlSet\Control\Class\{4D36E97B-E325-11CE-BFC1-08002BE10318}\[<Instance Number]
```

컴퓨터에 무엇이 설치되어 있느냐에 따라 Microsoft iSCSI 초기자가 0000이라는 하위 키가 아닐 수 있습니다. 올바른 하위 키를 선택했는지 확인하려면 DriverDesc 문자열의 값이 Microsoft iSCSI Initiator인지 확인하면 됩니다.

d. iSCSI 설정을 표시하려면 Parameters 하위 키를 선택합니다.

e. MaxRequestHoldTime DWORD(32비트) 값을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 수정을 선택한 후 값을 **600**으로 변경합니다.

MaxRequestHoldTime은 상위 계층에 Device Removal 이벤트를 알리기 전에 Microsoft iSCSI 이니시에이터가 미해결 명령을 보류하고 재시도하는 시간(초)을 지정합니다. 이 값은 대기 시간 600초를 나타냅니다.

2. 다음 파라미터를 수정하여 iSCSI 패킷으로 전송할 수 있는 최대 데이터 양을 늘릴 수 있습니다.

- FirstBurstLength는 요청하지 않은 쓰기 요청에서 전송할 수 있는 최대 데이터 양을 제어합니다. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.

- MaxBurstLength는 FirstBurstLength와 유사하지만 요청한 쓰기 시퀀스로 전송될 수있는 최대 데이터 양을 설정합니다. 이 값을 **1048576** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.
- MaxRecvDataSegmentLength는 단일 프로토콜 데이터 단위(PDU)와 연결된 최대 데이터 세그먼트 크기를 제어합니다. 이 값을 **262144** 또는 Windows OS 기본값 중 더 높은 값으로 설정합니다.

> **Note**
>
> 서로 다른 iSCSI 설정을 사용하여 최상의 성능을 발휘하도록 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.

   a. 레지스트리 편집기(`Regedit.exe`)를 아직 시작하지 않았다면 지금 시작하십시오.

   b. 다음과 같이 CurrentControlSet의 서비스 하위 키에서 디스크 하위 키로 이동합니다.

   ```
   HKEY_Local_Machine\SYSTEM\CurrentControlSet\Services\Disk
   ```

   c. TimeOutValue DWORD(32비트) 값을 마우스 오른쪽 버튼으로 클릭하여 컨텍스트 메뉴를 열고 수정을 선택한 후 값을 **600**으로 변경합니다.

   TimeOutValue는 연결을 끊었다가 다시 설정하여 세션 복구를 시도하기 전에 iSCSI 이니시에이터가 대상의 응답을 기다리는 시간(초)을 지정합니다. 이 값은 제한 시간 600초를 나타냅니다.

4. 새 구성 값을 적용하려면 시스템을 다시 시작해야 합니다.

   다시 시작하기 전에 볼륨에 대한 모든 쓰기 작업의 결과가 플러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 매핑한 스토리지 볼륨 디스크를 모두 오프라인으로 전환해야 합니다.

Linux iSCSI 설정을 사용자 지정

게이트웨이에 대한 이니시에이터를 설정한 후에는 이니시에이터가 대상에서 연결이 끊기지 않도록 iSCSI 설정을 사용자 지정하는 것이 좋습니다. 다음과 같이 iSCSI 제한 시간 값을 늘리면 시간이 오래 걸리는 쓰기 작업과 네트워크 장애와 같은 기타 일시적인 문제를 애플리케이션이 더 잘 해결할 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. *[replacement_timeout_value]* 값을 **600**으로 설정합니다.

   [noop_out_interval_value] 값을 **60**으로 설정합니다.

   [noop_out_timeout_value] 값을 **600**으로 설정합니다.

   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.

[replacement_first_burst_length_value] 값을 **262144** 또는 Linux OS 기본값 중 더 높은 값으로 설정합니다.

[replacement_max_burst_length_value] 값을 **1048576** 또는 Linux OS 기본값 중 더 높은 값으로 설정합니다.

[replacement_segment_length_value] 값을 **262144** 또는 Linux OS 기본값 중 더 높은 값으로 설정합니다.

> **Note**
>
> 서로 다른 iSCSI 설정을 사용하여 최상의 성능을 발휘하도록 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 플러시되어 있는지 확인합니다. 이를 위해서는 다시 시작하기 전에 테이프를 마운트 해제합니다.

iSCSI 대상에 대한 CHAP 인증 구성

Storage Gateway는 CHAP(Challenge-Handshake Authentication Protocol)을 사용하여 게이트웨이와 iSCSI 이니시에이터 간의 인증을 지원합니다. CHAP은 iSCSI 이니시에이터의 ID가 볼륨 및 VTL 디바이스 대상에 액세스할 수 있는 인증된 상태인지 주기적으로 확인하여 재생 공격으로부터 보호합니다.

> **Note**
>
> CHAP 구성은 선택 사항이지만 적극 권장됩니다.

CHAP을 설정하려면 Storage Gateway 콘솔과 대상에 연결하는 데 사용하는 iSCSI 이니시에이터 소프트웨어에서 모두 구성해야 합니다. Storage Gateway에서는 이니시에이터는 대상을 인증하고 대상은 이니시에이터를 인증하는 상호 CHAP이 사용됩니다.

대상에 상호 CHAP를 설정하려면

1. Storage Gateway 콘솔에서 VTL 디바이스 대상에 대해 CHAP을 구성하려면에 설명된 대로 Storage Gateway 콘솔에서 CHAP을 구성합니다.
2. 클라이언트 초기자 소프트웨어에서 다음과 같이 CHAP 구성을 완료합니다.

   - Windows 클라이언트에서 상호 CHAP를 구성하려면 Windows 클라이언트에서 상호 CHAP를 구성하려면 단원을 참조하십시오.
   - Red Hat Linux 클라이언트에서 상호 CHAP를 구성하려면 Red Hat Linux 클라이언트에서 상호 CHAP를 구성하려면 단원을 참조하십시오.

Storage Gateway 콘솔에서 VTL 디바이스 대상에 대해 CHAP을 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. 해당 게이트웨이를 선택한 후 VTL 디바이스 탭을 선택하여 모든 VTL 디바이스를 표시합니다.
3. CHAP을 구성할 디바이스를 선택합니다.
4. CHAP 인증 구성 대화 상자에 요청된 정보를 입력합니다.

   a. 이니시에이터 이름에 iSCSI 이니시에이터의 이름을 입력합니다. 이 이름은 Amazon iSCSI 공인 이름(IQN)으로, `iqn.1997-05.com.amazon:`으로 시작하여 뒤에 대상 이름이 붙습니다. 다음은 예입니다.

      ```
      iqn.1997-05.com.amazon:your-tape-device-name
      ```

      iSCSI 초기자 소프트웨어를 사용하여 초기자 이름을 찾을 수 있습니다. 예를 들어 Windows 클라이언트의 경우, 그 이름은 iSCSI 초기자의 구성 탭에 있는 값입니다. 자세한 내용은 Windows 클라이언트에서 상호 CHAP를 구성하려면 단원을 참조하십시오.

> **Note**
>
> 이니시에이터 이름을 변경하려면 먼저 CHAP을 비활성화하고 iSCSI 이니시에이터 소프트웨어에서 이니시에이터 이름을 변경한 후 새 이름으로 CHAP을 활성화해야 합니다.

b. 이니시에이터를 인증하는 데 사용되는 암호에 요청된 암호를 입력합니다.

   이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 초기자(즉 Windows 클라이언트)가 대상과의 CHAP에 참여하기 위해 알아야 하는 비밀 키입니다.

c. 대상을 인증하는 데 사용되는 암호(상호 CHAP)에 요청된 암호를 입력합니다.

   이 비밀 문구는 최소 12자, 최대 16자여야 합니다. 이 값은 대상이 초기자와의 CHAP에 참여하기 위해 알아야 하는 비밀 키입니다.

> **Note**
>
> 대상을 인증하는 데 사용한 비밀 문구는 초기자 인증을 위한 비밀 문구와는 달라야 합니다.

d. 저장을 선택합니다.

5. VTL 디바이스 탭에서 iSCSI CHAP 인증 필드가 true로 설정되어 있는지 확인합니다.

Windows 클라이언트에서 상호 CHAP를 구성하려면

이 절차에서는 콘솔의 볼륨에 CHAP를 구성하는 데 사용한 것과 동일한 키를 사용하여 Microsoft iSCSI 초기자에 CHAP를 구성합니다.

1. iSCSI 이니시에이터가 아직 시작되지 않은 경우, Windows 클라이언트 컴퓨터의 시작 메뉴에서 실행을 선택하고 **`iscsicpl.exe`**를 입력한 후 확인을 선택하여 프로그램을 실행합니다.
2. 초기자(즉 Windows 클라이언트)에 대해 다음과 같이 상호 CHAP를 구성합니다.

   a. 구성 탭을 선택합니다.

> **Note**
>
> 이니시에이터 이름 값은 초기자 및 회사에 고유합니다. 앞에 표시된 이름은 Storage Gateway 콘솔의 CHAP 인증 구성 대화 상자에서 사용한 값입니다.
> 예시 이미지에 표시된 이름은 데모용일 뿐입니다.

b. CHAP를 선택합니다.

c. iSCSI 이니시에이터 CHAP 암호 대화 상자에 상호 CHAP 암호 값을 입력합니다.

이 대화 상자에서 초기자(Windows 클라이언트)가 대상(스토리지 볼륨)을 인증하는 데 사용하는 비밀 문구를 입력합니다. 이 비밀 문구를 사용하면 대상이 초기자에(서) 읽고 쓸 수 있습니다. 이 암호는 CHAP 인증 구성 대화 상자의 대상을 인증하는 데 사용되는 암호(상호 CHAP) 상자에 입력한 암호와 동일합니다. 자세한 내용은 iSCSI 대상에 대한 CHAP 인증 구성 단원을 참조하십시오.

d. 입력한 키의 길이가 12자 미만이거나 16자를 초과하는 경우, 이니시에이터 CHAP 암호 오류 대화 상자가 나타납니다.

확인을 선택한 후 키를 다시 입력합니다.

3. 초기자의 비밀 문구로 대상을 구성하여 상호 CHAP 구성을 완료합니다.

a. 대상 탭을 선택합니다.

b. CHAP에 구성할 대상이 현재 연결되어 있으면 대상을 선택하고 연결 해제를 선택하여 대상의 연결을 해제합니다.

c. CHAP에 구성할 대상을 선택한 후 연결을 선택합니다.

d. Connect to Target(대상으로 연결) 대화 상자에서 고급을 선택합니다.

e. 고급 설정 대화 상자에서 CHAP를 구성합니다.

i. CHAP 로그온 활성화를 선택합니다.

ii. 이니시에이터를 인증하는 데 필요한 암호를 입력합니다. 이 암호는 CHAP 인증 구성 대화 상자의 이니시에이터를 인증하는 데 사용되는 암호 상자에 입력한 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 클라이언트에서 상호 CHAP를 구성하려면

이 절차에서는 Storage Gateway 콘솔에서 볼륨의 CHAP을 구성할 때 사용한 것과 동일한 키를 사용하여 Linux iSCSI 이니시에이터에 CHAP을 구성합니다.

1. iSCSI 데몬이 실행 중이고 대상에 이미 연결했는지 확인합니다. 이 두 작업을 완료하지 않은 경우, Linux 클라이언트에 연결 섹션을 참조하세요.
2. CHAP를 구성하려고 하는 대상에 대한 모든 기존 구성을 연결 해제하고 제거합니다.

   a. 대상 이름을 찾고 그것이 정의된 구성인지 확인하려면 다음 명령을 사용하여 저장된 구성의 목록을 조회합니다.

   ```
   sudo /sbin/iscsiadm --mode node
   ```

   b. 대상에서 연결을 해제합니다.

   다음 명령은 Amazon iSCSI 정규화 이름(IQN)에 정의된**myvolume**이라는 대상에서 연결을 해제합니다. 상황에 따라 대상 이름과 IQN을 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 CHAP을 활성화합니다.

   a. 초기자(즉 사용 중인 클라이언트)의 이름을 가져옵니다.

   다음 명령은 `/etc/iscsi/initiatorname.iscsi` 파일에서 초기자 이름을 가져옵니다.

   ```
   sudo cat /etc/iscsi/initiatorname.iscsi
   ```

   이 명령의 출력은 다음과 같습니다.

```
InitiatorName=iqn.1994-05.com.redhat:8e89b27b5b8
```

b. `/etc/iscsi/iscsid.conf` 파일을 엽니다.

c. 파일에서 다음 줄에 대한 주석 처리를 해제하고 *username*, *password*, *username_in*, *password_in*에 올바른 값을 지정합니다.

```
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
### ##	이 절차의 이전 단계에서 찾은 초기자 이름. 그 값은 IQN으로 시작합니다. 예를 들어 **iqn.1994-05.com.redhat:8e89b27b5b8** 는 유효한 *username* 값입니다.
password	초기자(사용 중인 클라이언트)가 볼륨과 통신할 때 초기자를 인증하는 데 사용하는 비밀 키
username_in	대상 볼륨의 IQN. 이 값은 IQN으로 시작하여 대상 이름으로 끝납니다. 예를 들어 **iqn.1997-05.com.amazon:myvolume** 는 유효한 *username_in* 값입니다.
password_in	대상(볼륨)이 초기자와 통신할 때 대상을 인증하는 데 사용하는 비밀 키

d. 구성 파일에 변경 사항을 저장한 후 파일을 닫습니다.

4. 대상을 검색하여 로그인합니다. 이렇게 하려면 Linux 클라이언트에 연결에 설명된 단계를 수행하세요.

Storage Gateway Direct Connect 와 함께 사용

Direct Connect 는 내부 네트워크를 Amazon Web Services 클라우드에 연결합니다. Storage Gateway 와 Direct Connect 함께를 사용하면 처리량이 많은 워크로드 요구 사항에 맞는 연결을 생성하여 온프레미스 게이트웨이와 간에 전용 네트워크 연결을 제공할 수 있습니다 AWS.

Storage Gateway는 퍼블릭 엔드포인트를 사용합니다. Direct Connect 연결이 설정되면 퍼블릭 가상 인터페이스를 생성하여 트래픽을 Storage Gateway 엔드포인트로 라우팅할 수 있습니다. 퍼블릭 가상 인터페이스는 네트워크 경로에서 인터넷 서비스 제공업체를 우회합니다. Storage Gateway 서비스 퍼블릭 엔드포인트는 위치와 동일한 AWS 리전 Direct Connect 에 있거나 다른 AWS 리전에 있을 수 있습니다.

다음 그림은가 Storage Gateway에서 Direct Connect 작동하는 방식의 예를 보여줍니다.
AWS 직접 연결을 사용하여 클라우드에 연결된 Storage Gateway를 보여주는 네트워크 아키텍처입니다.

다음 절차에서는 생성된 게이트웨이가 제대로 작동 중이라고 가정합니다.

Storage Gateway Direct Connect 와 함께를 사용하려면

1. 온프레미스 데이터 센터와 Storage Gateway 엔드포인트 간에 AWS Direct Connect 연결을 생성하고 설정합니다. 연결 생성 방법에 대한 자세한 내용은Direct Connect 사용 설명서에서 Direct Connect시작하기를 참조하세요.
2. 온프레미스 Storage Gateway 어플라이언스를 Direct Connect 라우터에 연결합니다.
3. 퍼블릭 가상 인터페이스를 생성하고 이에 따라 온프레미스 라우터를 구성합니다. Direct Connect 를 사용하는 경우에도 HAProxy를 사용하여 VPC 엔드포인트를 생성해야 합니다. 자세한 내용은 Direct Connect 사용 설명서에서 가상 인터페이스 생성을 참조하세요.

자세한 내용은 Direct Connect 사용 설명서의 란 무엇입니까 Direct Connect?를 Direct Connect참조하세요.

게이트웨이 어플라이언스의 IP 주소 가져오기

호스트를 선택하고 게이트웨이 VM을 배포한 후 게이트웨이를 연결하고 활성화합니다. 이렇게 하려면 게이트웨이 VM의 IP 주소가 필요합니다. IP 주소는 게이트웨이의 로컬 콘솔에서 얻을 수 있습니다. 로컬 콘솔에 로그인하여 콘솔 페이지의 상단에서 IP 주소를 얻습니다.

온프레미스에 배포된 게이트웨이의 경우, 하이퍼바이저에서 IP 주소를 얻을 수도 있습니다. Amazon EC2 게이트웨이의 경우, Amazon EC2 Management Console에서 Amazon EC2 인스턴스의 IP 주소를 얻을 수도 있습니다. 게이트웨이의 IP 주소를 얻는 방법은 다음 중 하나를 참조하세요.

- VMware 호스트: VMware ESXi를 사용하여 게이트웨이 로컬 콘솔에 액세스
- HyperV 호스트: Microsoft Hyper-V를 사용하여 게이트웨이 로컬 콘솔에 액세스
- Linux 커널 기반 가상 머신(KVM) 호스트: Linux KVM을 사용하여 게이트웨이 로컬 콘솔에 액세스
- EC2 호스트: Amazon EC2 호스트에서 IP 주소 얻기

IP 주소를 찾았으면 적어 둡니다. 그런 다음 Storage Gateway 콘솔로 돌아가서 콘솔에 IP 주소를 입력합니다.

Amazon EC2 호스트에서 IP 주소 얻기

게이트웨이가 배포된 Amazon EC2 인스턴스의 IP 주소를 얻으려면 EC2 인스턴스의 로컬 콘솔에 로그인합니다. 그런 다음 콘솔 페이지 상단에서 IP 주소를 얻습니다. 지침은 Amazon EC2 게이트웨이 로컬 콘솔에 로그인 섹션을 참조하세요.

Amazon EC2 Management Console에서도 IP 주소를 얻을 수 있습니다. 활성화에는 퍼블릭 IP 주소를 사용하는 것이 좋습니다. 퍼블릭 IP 주소를 얻으려면 절차 1을 사용합니다. 그 대신 탄력적 IP 주소를 사용하려면 절차 2를 사용합니다.

절차 1: 퍼블릭 IP 주소를 사용하여 게이트웨이에 연결하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 퍼블릭 IP 주소를 적어 둡니다. 이 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 IP 주소를 입력합니다.

활성화에 탄력적 IP 주소를 사용하려면 다음 절차를 사용합니다.

절차 2: 탄력적 IP 주소를 사용하여 게이트웨이에 연결하려면

1. https://console.aws.amazon.com/ec2/에서 Amazon EC2 콘솔을 엽니다.
2. 탐색 창에서 인스턴스를 선택한 후 게이트웨이가 배포된 EC2 인스턴스를 선택합니다.
3. 하단의 설명 탭을 선택한 후 탄력적 IP 값을 적어 둡니다. 이 탄력적 IP 주소를 사용하여 게이트웨이에 연결하게 됩니다. Storage Gateway 콘솔로 돌아가서 탄력적 IP 주소를 입력합니다.

4. 게이트웨이가 활성화되면 방금 활성화한 게이트웨이를 선택한 후 하단 패널에서 VTL 디바이스 탭을 선택합니다.
5. 모든 VTL 디바이스의 이름을 얻습니다.
6. 각 대상에 대해 다음 명령을 실행하여 대상을 구성합니다.

   ```
   iscsiadm -m node -o new -T [$TARGET_NAME] -p [$Elastic_IP]:3260
   ```

7. 각 대상에 대해 다음 명령을 실행하여 로그인합니다.

   ```
   iscsiadm -m node -p [$ELASTIC_IP]:3260 --login
   ```

   이제 게이트웨이가 EC2 인스턴스의 탄력적 IP 주소를 사용하여 연결되었습니다.

IPv6 지원

IPv6 지원은 게이트웨이 어플라이언스 버전 3.x 이상에서만 사용할 수 있습니다. 게이트웨이 어플라이언스 버전 1.x 및 2.x는 3.x로 업데이트할 수 없습니다. IPv6 지원을 받으려면 게이트웨이 어플라이언스 버전 1.x 또는 2.x를 마이그레이션하거나 교체해야 합니다.

IPv6에는 다음과 같은 듀얼 스택 엔드포인트가 필요합니다. 자세한 내용은 엔드포인트 유형 단원을 참조하십시오.

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

Storage Gateway 리소스 및 리소스 ID 이해

Storage Gateway에서 기본 리소스는 게이트웨이지만 다른 리소스 유형으로 볼륨, 가상 테이프, iSCSI 대상, vtl 디바이스가 있습니다. 이 유형들은 하위 리소스라고 하며 게이트웨이와 연결되어 있지 않은 경우에는 존재하지 않습니다.

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

리소스 유형	ARN 형식
Gateway ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id*
테이프 ARN	arn:aws:storagegateway: *region*:*account-id* :tape/*tapebarcode*
대상 ARN(iSCSI 대상)	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /target/*iSCSItarget*
VTL 디바이스 ARN	arn:aws:storagegateway: *region*:*account-id* :gateway/ *gateway-id* /device/*vtldevice*

Storage Gateway는 EC2 인스턴스, EBS 볼륨 및 스냅샷 사용을 지원합니다. 이 리소스는 Storage Gateway에서 사용하는 Amazon EC2 리소스입니다.

리소스 ID 작업

리소스를 생성할 때 Storage Gateway에서는 리소스에 고유 리소스 ID를 할당합니다. 이 리소스 ID는 리소스 ARN의 일부입니다. 리소스 ID는 리소스 식별자, 하이픈, 8개의 문자와 숫자의 고유한 조합 . 예를 들어 게이트웨이 ID는가 게이트웨이의 리소스 식별자sgw-12A3456Bsgw인 형식합니다.

가상 테이프의 경우, 바코드 ID 앞에 접두사 문자를 최대 네 개까지 추가할 수 있어 테이프 체계화에 도움이 됩니다.

Storage Gateway 리소스에 태그를 지정

Storage Gateway에서 태그를 사용하여 리소스를 관리할 수 있습니다. 태그를 사용하면 메타데이터를 리소스에 추가하고 리소스를 분류하여 관리하기가 편해집니다. 각 태그는 사용자가 정의하는 키-값 페어로 구성됩니다. 게이트웨이, 볼륨 및 가상 테이프에 태그를 추가할 수 있습니다. 추가하는 태그에 따라 이 리소스를 검색하고 필터링할 수 있습니다.

예를 들어 태그를 사용하여 조직 내 각 부서에서 사용하는 Storage Gateway 리소스를 식별할 수 있습니다. key=department 및 value=accounting과 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 유효한 문자는 UTF-8 문자 및 숫자, 공백, 특수 문자(+ - = . _ : / @)입니다.

태그 작업

Storage Gateway 콘솔, Storage Gateway API 또는 Storage Gateway 명령줄 인터페이스(CLI)를 사용하여 태그 관련 작업을 수행할 수 있습니다. 다음 절차에서는 콘솔에서 태그를 추가, 편집, 삭제하는 방법을 안내합니다.

태그를 추가하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 탐색 창에서 태그를 지정하려는 리소스를 선택합니다.

   예를 들어 게이트웨이에 태그를 지정하려면 게이트웨이를 선택한 후 게이트웨이 목록에서 태그를 지정할 게이트웨이를 선택합니다.
3. 태그를 선택한 후 태그 추가/편집을 선택합니다.
4. 태그 추가/편집 대화 상자에서 태그 생성을 선택합니다.
5. 키에 키를 입력하고 값에 값을 입력합니다. 예를 들어 키로는 **`Department`**를, 값으로는 **`Accounting`**을 입력할 수 있습니다.

   > **Note**
   >
   > 값 상자를 공백으로 둘 수도 있습니다.

6. 태그 생성을 선택하여 태그를 추가합니다. 리소스 한 개에 태그를 여러 개 추가할 수 있습니다.
7. 태그 추가를 완료했으면 저장을 선택합니다.

태그를 편집하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 편집하려는 태그가 있는 리소스를 선택합니다.
3. 태그를 선택하여 태그 추가/편집 대화 상자를 엽니다.
4. 편집하고자 하는 태그 옆의 연필 아이콘을 선택하여 태그를 편집합니다.
5. 태그 편집을 완료했으면 저장을 선택합니다.

태그를 삭제하려면

1. Storage Gateway 콘솔(https://console.aws.amazon.com/storagegateway/home)을 엽니다.
2. 삭제하려는 태그가 있는 리소스를 선택합니다.
3. 태그를 선택한 후 태그 추가/편집을 선택하여 태그 추가/편집 대화 상자를 엽니다.
4. 삭제하고자 하는 태그 옆의 X 아이콘을 선택한 후 저장을 선택합니다.

Storage Gateway용 오픈 소스 구성 요소 작업

이 섹션에서는 Storage Gateway 기능을 제공하기 위해 사용하는 타사 도구 및 라이센스에 대해 설명합니다.

AWS Storage Gateway 소프트웨어에 포함된 특정 오픈 소스 소프트웨어 구성 요소의 소스 코드는 다음 위치에서 다운로드할 수 있습니다.

- VMware ESXi에 배포된 게이트웨이의 경우 sources.tar을 다운로드합니다.
- Microsoft Hyper-V에 배포된 게이트웨이의 경우 sources_hyperv.tar을 다운로드합니다.
- Linux 커널 기반 가상 머신(KVM)에 배포된 게이트웨이의 경우 sources_KVM.tar을 다운로드합니다.

이 제품은 OpenSSL 도구 키트(http://www.openssl.org/)에서 사용하기 위해 OpenSSL 프로젝트가 개발한 소프트웨어를 포함합니다. 모든 종속 타사 도구에 대한 관련 라이선스는 타사 라이선스를 참조하십시오.

AWS Storage Gateway 할당량

이 주제에서는 Storage Gateway의 볼륨 및 테이프 할당량, 구성 및 성능 한도에 대한 정보를 확인할 수 있습니다.

주제

- 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

게이트웨이 유형	캐시(최소값)	캐시(최대값)	업로드 버퍼(최소값)	업로드 버퍼(최대값)
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 때 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.

Storage Gateway용 API 참조

콘솔을 사용하는 것 외에도 AWS Storage Gateway API를 사용하여 게이트웨이를 프로그래밍 방식으로 구성하고 관리할 수 있습니다. 이 섹션에서는 AWS Storage Gateway 작업, 인증을 위한 요청 서명 및 오류 처리에 대해 설명합니다. Storage Gateway에 사용할 수 있는 리전 및 엔드포인트에 대한 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.

> **Note**
>
> 를 사용하여 애플리케이션을 개발할 때 AWS SDKs 사용할 수도 있습니다 AWS Storage Gateway. Java, .NET 및 PHP용 AWS SDKs는 기본 AWS Storage Gateway API를 래핑하여 프로그래밍 작업을 간소화합니다. SDK 라이브러리 다운로드에 대한 정보는 샘플 코드 라이브러리 섹션을 참조하세요.

주제

- Storage Gateway 필수 요청 헤더
- 요청에 서명하기
- 오류 응답
- 작업

Storage Gateway 필수 요청 헤더

이 단원에서는 Storage Gateway에 대한 모든 POST 요청과 함께 전송해야 하는 필수 헤더에 대해 설명합니다. 호출하려는 작업을 포함하는 요청에 대한 핵심 정보, 요청 날짜 및 요청 전송자의 권한을 부여함을 나타내는 정보를 식별할 HTTP 헤더를 포함해야 합니다. 헤더는 대소문자를 구별하고 헤더의 순서는 중요하지 않습니다.

다음은 ActivateGateway 작업에서 사용하는 헤더의 예입니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
Content-Type: application/x-amz-json-1.1
```

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120425/us-east-2/
storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target,
 Signature=9cd5a3584d1d67d57e61f120f35102d6b3649066abdd4bf4bbcf05bd9f2f8fe2
x-amz-date: 20120912T120000Z
x-amz-target: StorageGateway_20120630.ActivateGateway
```

다음은 Storage Gateway에 대한 POST 요청과 함께 포함해야 하는 헤더입니다. 아래에 표시된 "x-amz"로 시작하는 헤더는 AWS특정 헤더입니다. 나머지 헤더는 HTTP 트랜잭션에 사용되는 공통 헤더입니다.

헤더	설명
`Authorization`	권한 부여 헤더는 Storage Gateway가 해당 요청이 요청자에게 유효한 작업인지 판단할 수 있게 해주는 요청에 대한 몇 가지 정보를 포함합니다. 이 헤더의 형식은 다음과 같습니다(가독성을 높이기 위해 줄 바꿈 추가). `Authorization: AWS4-HMAC_SHA456 Credentials= YourAccessKey /yyymmdd/region/storagegateway/aws4_request, SignedHeaders=content-type;host;x-amz-date;x-amz-target, Signature= CalculatedSignature` 이전 구문에서는 YourAccessKey, 연도, 월, 일(yyyymmdd), 해당 리전 및 CalculatedSignature를 지정합니다. 권한 부여 헤더의 형식은 AWS V4 서명 프로세스의 요구 사항에 따라 결정됩니다. 서명 관련 세부 정보는 요청에 서명하기 섹션에 나와 있습니다.
`Content-Type`	`application/x-amz-json-1.1` 을 Storage Gateway에 대한 모든 요청의 콘텐츠 유형으로 사용합니다. `Content-Type: application/x-amz-json-1.1`
`Host`	호스트 헤더를 사용하여 요청을 전송하는 Storage Gateway 엔드포인트를 지정합니다. 예를 들어, `storagegateway.us-east-2.amazonaws.com` 은 미국 동부(오하이오) 리전의 엔드포인트입니다. Storage Gateway에 사용할 수 있는 엔드포인트에 대한 자세한 내용은

헤더	설명
	AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요. `Host: storagegateway. region.amazonaws.com`
`x-amz-date`	HTTP `Date` 헤더 또는 헤더에 타임스탬프를 AWS `x-amz-date` 제공해야 합니다. 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'HHMMSS'Z' 형식의 ISO8601 기본이어야 합니다. `Date` 및 `x-amz-date` 헤더를 모두 사용하는 경우, Date 헤더의 형식이 ISO8601일 필요는 없습니다. `x-amz-date: YYYYMMDD'T'HHMMSS'Z'`
`x-amz-target`	이 헤더는 API의 버전과 요청 중인 작업을 지정합니다. 대상 헤더 값은 API 버전을 API 이름과 연결하여 구성하며 형식은 다음과 같습니다. `x-amz-target: StorageGateway_ APIversion .operationName` OperationName 값(예: "ActivateGateway")은 API 목록, Storage Gateway용 API 참조에서 찾을 수 있습니다.

요청에 서명하기

Storage Gateway에서는 요청에 서명하여 전송하는 모든 요청을 인증해야 합니다. 요청에 서명하려면 암호화 해시 함수를 이용해 디지털 서명을 계산해야 합니다. 암호화 해시는 입력을 근거로 하여 고유 해시 값을 반환하는 함수입니다. 해시 함수에 대한 입력에는 요청 텍스트와 시크릿 액세스 키가 포함됩니다. 해시 함수는 요청에 서명으로 포함하는 해시 값을 반환합니다. 서명은 요청에서 `Authorization` 헤더의 일부입니다.

Storage Gateway는 요청을 수신한 후, 사용자가 요청에 서명할 때와 동일한 해시 함수 및 입력을 사용하여 서명을 재계산합니다. 결과 서명이 요청 서명과 일치할 경우 Storage Gateway에서 요청을 처리합니다. 그렇지 않으면 요청이 거부됩니다.

Storage Gateway는 AWS Signature Version 4를 이용한 인증을 지원합니다. 서명을 계산하기 위한 프로세스는 다음 세 작업으로 나뉠 수 있습니다.

- 작업 1: 정식 요청 생성

  HTTP 요청을 정규 형식으로 재배열합니다. 정규 형식을 사용해야 하는 이유는 Storage Gateway에서 서명을 재계산하여 사용자가 보낸 서명과 비교할 때 동일한 정규 형식을 사용하기 때문입니다.
- 작업 2: 서명할 문자열 생성

  암호화 해시 함수에 대한 입력 값 중 하나로 사용할 문자열을 만듭니다. 서명할 문자열이라는 문자열은 해시 알고리즘의 이름, 요청 날짜, 자격 증명 범위 문자열, 이전 작업에서 정규화된 요청을 연결한 것입니다. 자격 증명 범위 문자열 자체는 날짜, 리전 및 서비스 정보를 연결한 것입니다.
- 작업 3: 서명 생성

  서명할 문자열과 파생된 키의 두 입력 문자열을 허용하는 암호화 해시 함수를 사용하여 요청에 대한 서명을 만듭니다. 파생된 키는 보안 액세스 키로 시작해 자격 증명 범위 문자열을 사용하여 일련의 해시 기반 메시지 인증 코드(HMAC)를 생성하는 방법으로 계산합니다.

서명 계산 예시

다음 예시에서는 ListGateways에 대해 서명을 생성하는 세부 과정을 안내합니다. 이 예시는 서명 계산 방법을 점검하기 위한 참조로 사용할 수 있습니다. 다른 참조 계산은 Amazon Web Services 글로서리의 서명 버전 4 테스트 제품군에 포함되어 있습니다.

이 예시에서는 다음과 같이 가정합니다.

- 해당 요청의 타임스탬프는 "2012년 9월 10일 월요일 00:00:00시" GMT입니다.
- 엔드포인트는 미국 동부(오하이오) 리전입니다.

일반 요청 구문(JSON 본문 포함)은 다음과 같습니다.

```
POST / HTTP/1.1
Host: storagegateway.us-east-2.amazonaws.com
```

```
x-amz-Date: 20120910T000000Z
Authorization: SignatureToBeCalculated
Content-type: application/x-amz-json-1.1
x-amz-target: StorageGateway_20120630.ListGateways
{}
```

작업 1: 정식 요청 생성에 대해 계산한 요청의 정규 형식은 다음과 같습니다.

```
POST
/

content-type:application/x-amz-json-1.1
host:storagegateway.us-east-2.amazonaws.com
x-amz-date:20120910T000000Z
x-amz-target:StorageGateway_20120630.ListGateways

content-type;host;x-amz-date;x-amz-target
44136fa355b3678a1146ad16f7e8649e94fb4fc21fe77e8310c060f61caaff8a
```

표준 요청의 마지막 줄은 요청 본문의 해시입니다. 또한 표준 요청에서 비어 있는 세 번째 줄에 주의해야 합니다. 비어 있는 이유는 이 API(또는 Storage Gateway API)에 대한 쿼리 파라미터가 없기 때문입니다.

작업 2: 서명할 문자열 생성의 경우 서명할 문자열은 다음과 같습니다.

```
AWS4-HMAC-SHA256
20120910T000000Z
20120910/us-east-2/storagegateway/aws4_request
92c0effa6f9224ac752ca179a04cecbede3038b0959666a8160ab452c9e51b3e
```

서명할 문자열의 첫째 줄은 알고리즘, 둘째 줄은 타임스탬프, 셋째 줄은 자격 증명 범위, 마지막 줄은 작업 1 정규 요청의 해시입니다.

작업 3: 서명 생성을 위한 파생된 키는 다음과 같이 표시할 수 있습니다.

```
derived key = HMAC(HMAC(HMAC(HMAC("AWS4" + YourSecretAccessKey,"20120910"),"us-
east-2"),"storagegateway"),"aws4_request")
```

시크릿 액세스 키인 wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY를 사용하는 경우, 계산된 서명은 다음과 같습니다.

```
6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

마지막 단계는 Authorization 헤더를 생성하는 것입니다. 데모용 액세스 키 AKIAIOSFODNN7EXAMPLE의 경우 헤더는 다음과 같습니다(가독성을 높이기 위해 줄 바꿈을 추가함).

```
Authorization: AWS4-HMAC-SHA256 Credential=AKIAIOSFODNN7EXAMPLE/20120910/us-east-2/
storagegateway/aws4_request,
SignedHeaders=content-type;host;x-amz-date;x-amz-target,
Signature=6d4c40b8f2257534dbdca9f326f147a0a7a419b63aff349d9d9c737c9a0f4c81
```

오류 응답

주제

- 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 오류 예외 InvalidSignatureException은 요청 서명에 문제가 있는 경우 모든 API 응답이 반환합니다. 그러나 작업 오류 코드 ActivationKeyInvalid는 ActivateGateway API에 대해서만 반환됩니다.

오류 유형에 따라 Storage Gateway는 예외만 반환하거나 예외와 작업 오류 코드를 모두 반환할 수 있습니다. 오류 응답 예시는 오류 응답에 있습니다.

예외

다음 표에는 AWS Storage Gateway API 예외가 나열되어 있습니다. AWS Storage Gateway 작업이 오류 응답을 반환하면 응답 본문에 이러한 예외 중 하나가 포함됩니다. InternalServerError와 InvalidGatewayRequestException은 특정 작업 오류 코드를 부여하는 작업 오류 코드(작업 오류 코드) 메시지 코드 중 하나를 반환합니다.

예외	메시지	HTTP 상태 코드
IncompleteSignatureException	지정한 서명이 불완전합니다.	400 잘못된 요청
InternalFailure	알 수 없는 오류, 예외 또는 장애로 인해 요청 처리가 실패했습니다.	500 Internal Server Error
InternalServerError	작업 오류 코드 작업 오류 코드 메시지 중 하나입니다.	500 Internal Server Error
InvalidAction	요청된 동작 또는 작업이 유효하지 않습니다.	400 잘못된 요청
InvalidClientTokenId	제공된 X.509 인증서 또는 AWS 액세스 키 ID가 레코드에 존재하지 않습니다.	403 금지됨
InvalidGatewayRequestException	작업 오류 코드의 작업 오류 코드 메시지 중 하나입니다.	400 잘못된 요청
InvalidSignatureException	우리가 계산한 요청 서명이 사용자가 제공한 서명과 일치하지 않습니다. AWS 액세스 키 및 서명 방법을 확인합니다.	400 잘못된 요청
MissingAction	요청에서 작업 또는 작업 파라미터가 누락되었습니다.	400 잘못된 요청
MissingAuthenticationToken	요청에 유효한 (등록된) AWS 액세스 키 ID 또는 X.509 인증서가 포함되어야 합니다.	403 금지됨
RequestExpired	요청이 만료 날짜 또는 요청 날짜(15분 패딩)를 지났거나 요청 날짜가 향후 15분 초과 후에 효력이 발생합니다.	400 잘못된 요청

예외	메시지	HTTP 상태 코드
SerializationException	직렬화 도중에 오류가 발생했습니다. JSON 페이로드의 형식이 올바른지 확인합니다.	400 잘못된 요청
ServiceUnavailable	서버의 일시적 장애로 인해 요청이 실패했습니다.	[503 Service Unavailable]
SubscriptionRequiredException	AWS 액세스 키 ID에는 서비스에 대한 구독이 필요합니다.	400 잘못된 요청
ThrottlingException	속도를 초과하였습니다.	400 잘못된 요청
TooManyRequests	요청이 너무 많음.	429 요청이 너무 많음
UnknownOperationException	알 수 없는 작업을 지정하였습니다. 유효한 작업은 Storage Gateway의 작업에 나열되어 있습니다.	400 잘못된 요청
UnrecognizedClientException	요청에 포함된 보안 토큰이 유효하지 않습니다.	400 잘못된 요청
ValidationException	입력 파라미터의 값이 잘못되었거나 범위를 벗어났습니다.	400 잘못된 요청

작업 오류 코드

다음 표에는 AWS Storage Gateway 작업 오류 코드와 코드를 반환할 수 있는 APIs 간의 매핑이 나와 있습니다. 모든 작업 오류 코드는 예외에 설명된 두 가지 일반 예외(InternalServerError 및 InvalidGatewayRequestException) 중 하나와 함께 반환됩니다.

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
ActivationKeyExpired	지정한 정품 인증 키가 만료되었습니다.	ActivateGateway

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
ActivationKeyInvalid	지정한 정품 인증 키가 유효하지 않습니다.	ActivateGateway
ActivationKeyNotFound	지정한 정품 인증 키를 찾을 수 없습니다.	ActivateGateway
BandwidthThrottleScheduleNotFound	지정한 대역폭 스로틀링을 찾을 수 없습니다.	DeleteBandwidthRateLimit
CannotExportSnapshot	지정한 스냅샷을 내보낼 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
InitiatorNotFound	지정된 초기자를 찾을 수 없습니다.	DeleteChapCredentials
DiskAlreadyAllocated	지정한 디스크가 이미 할당되었습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskDoesNotExist	지정한 디스크가 존재하지 않습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateStorediSCSIVolume
DiskSizeNotGigAligned	지정한 디스크가 기가바이트 정렬되어 있지 않습니다.	CreateStorediSCSIVolume
DiskSizeGreaterThanVolumeMaxSize	지정한 디스크 크기가 최대 볼륨 크기보다 큽니다.	CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
DiskSizeLessThanVolumeSize	지정한 디스크 크기가 볼륨 크기보다 작습니다.	CreateStorediSCSIVolume
DuplicateCertificateInfo	지정한 인증서 정보가 중복되어 있습니다.	ActivateGateway

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayInternalError	게이트웨이 내부 오류가 발생하였습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotConnected	지정한 게이트웨이가 연결되지 않았습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateStorediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayNotFound	지정한 게이트웨이를 찾을 수 없습니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListLocalDisks ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
GatewayProxyNetworkConnectionBusy	지정한 게이트웨이 프록시 네트워크 연결이 사용 중입니다.	AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes DescribeWorkingStorage ListLocalDisks

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InternalError	내부 오류가 발생했습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
InvalidParameters	지정한 요청에 잘못된 파라미터가 포함되어 있습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
`LocalStorageLimitExceeded`	로컬 스토리지 한도를 초과했습니다.	AddCache AddUploadBuffer AddWorkingStorage
`LunInvalid`	지정된 LUN이 올바르지 않습니다.	CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
MaximumVolumeCount Exceeded	최대 볼륨 수를 초과하였습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes
NetworkConfigurati onChanged	게이트웨이 네트워크 구성이 변경되었습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
NotSupported	지정한 작업을 지원하지 않습니다.	ActivateGateway AddCache AddUploadBuffer AddWorkingStorage CreateCachediSCSIVolume CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteBandwidthRateLimit DeleteChapCredentials DeleteGateway DeleteVolume DescribeBandwidthRateLimit DescribeCache DescribeCachediSCSIVolumes DescribeChapCredentials DescribeGatewayInformation DescribeMaintenanceStartTime DescribeSnapshotSchedule DescribeStorediSCSIVolumes

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
		DescribeWorkingStorage ListLocalDisks ListGateways ListVolumes ListVolumeRecoveryPoints ShutdownGateway StartGateway UpdateBandwidthRateLimit UpdateChapCredentials UpdateMaintenanceStartTime UpdateGatewayInformation UpdateGatewaySoftwareNow UpdateSnapshotSchedule
OutdatedGateway	지정한 게이트웨이의 날짜가 만료되었습니다.	ActivateGateway
SnapshotInProgressException	지정한 스냅샷이 진행 중입니다.	DeleteVolume
SnapshotIdInvalid	지정한 스냅샷이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
StagingAreaFull	스테이징 영역이 가득 찼습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
TargetAlreadyExists	지정한 대상이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
TargetInvalid	지정한 대상이 유효하지 않습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials UpdateChapCredentials
TargetNotFound	지정한 대상을 찾을 수 없습니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume DeleteChapCredentials DescribeChapCredentials DeleteVolume UpdateChapCredentials

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
UnsupportedOperationForGatewayType	지정한 작업이 게이트웨이 유형에 유효하지 않습니다.	AddCache AddWorkingStorage CreateCachediSCSIVolume CreateSnapshotFromVolumeRecoveryPoint CreateStorediSCSIVolume DeleteSnapshotSchedule DescribeCache DescribeCachediSCSIVolumes DescribeStorediSCSIVolumes DescribeUploadBuffer DescribeWorkingStorage ListVolumeRecoveryPoints
VolumeAlreadyExists	지정한 볼륨이 이미 존재합니다.	CreateCachediSCSIVolume CreateStorediSCSIVolume
VolumeIdInvalid	지정한 볼륨이 유효하지 않습니다.	DeleteVolume
VolumeInUse	지정한 볼륨이 이미 사용 중입니다.	DeleteVolume

작업 오류 코드	메시지	이 오류 코드를 반환하는 작업
VolumeNotFound	지정한 볼륨을 찾을 수 없습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint DeleteVolume DescribeCachediSCSIVolumes DescribeSnapshotSchedule DescribeStorediSCSIVolumes UpdateSnapshotSchedule
VolumeNotReady	지정한 볼륨이 아직 준비되지 않았습니다.	CreateSnapshot CreateSnapshotFromVolumeRecoveryPoint

오류 응답

오류가 있는 경우, 응답 헤더 정보에는 다음 내용이 포함됩니다.

- Content-Type: application/x-amz-json-1.1
- 적절한 4xx 또는 5xx HTTP 상태 코드

오류 응답의 본문에는 발생한 오류에 대한 정보가 포함됩니다. 다음 샘플 오류 응답은 모든 오류 응답에 공통된 응답 요소의 출력 구문을 나타냅니다.

```
{
    "__type": "String",
    "message": "String",
    "error":
        { "errorCode": "String",
          "errorDetails": "String"
        }
```

```
}
```

다음 표는 이전 구문에 표시된 JSON 오류 응답 필드를 설명합니다.

__타입

예외의 예외 중 하나.

유형: 문자열

오류

API별 오류의 세부 정보를 포함합니다. 일반적인 오류(즉 API에 고유한 오류가 아닌 경우)에서는 이 오류 정보가 표시되지 않습니다.

유형: 컬렉션

errorCode

작업 오류 코드 중 하나입니다 .

유형: 문자열

errorDetails

이 필드는 현재 API 버전에서는 사용되지 않습니다.

유형: 문자열

message

작업 오류 코드 메시지 중 하나입니다.

유형: 문자열

오류 응답 예시

DescribeStorediSCSIVolumes API를 사용할 경우 존재하지 않는 게이트웨이 ARN 요청 입력을 지정하면 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidGatewayRequestException",
  "message": "The specified volume was not found.",
  "error": {
```

```
    "errorCode": "VolumeNotFound"
  }
}
```

Storage Gateway가 요청과 함께 전송된 서명과 일치하지 않는 서명을 계산할 경우 다음 JSON 본문이 반환됩니다.

```
{
  "__type": "InvalidSignatureException",
  "message": "The request signature we calculated does not match the signature you
 provided."
}
```

Storage Gateway의 작업

Storage Gateway 작업 목록은AWS Storage Gateway API 참조에서 작업을 참조하세요.

Tape Gateway 사용 설명서의 문서 기록

다음 표에서는 2018년 4월 이후AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다. 이 설명서에 대한 업데이트 알림을 받으려면 RSS 피드를 구독하면 됩니다.

변경 사항	설명	날짜
IPv6 지원	IPv6 지원은 게이트웨이 어플라이언스 버전 3.x 이상에서 사용할 수 있습니다.	2025년 9월 10일
FSx File Gateway의 가용성 변경 알림	신규 고객은 더 이상 Amazon FSx File Gateway를 사용할 수 없습니다. 기존 FSx File Gateway 고객은 정상적으로 서비스를 계속 이용할 수 있습니다. FSx File Gateway와 유사한 기능에 대해서는 이 블로그 게시물을 참조하세요.	2024년 10월 28일
FSx File Gateway의 가용성 변경 알림	AWS Storage Gateway의 FSx File Gateway는 10월 28일 24시부터 더 이상 신규 고객이 사용할 수 없습니다. 이 서비스를 사용하려면 해당 날짜 이전에 가입해야 합니다. 기존 FSx File Gateway 고객은 정상적으로 서비스를 계속 이용할 수 있습니다. FSx File Gateway와 유사한 기능에 대해서는 이 블로그 게시물을 참조하세요.	2024년 9월 26일
유지 관리 업데이트 켜기 또는 끄기 옵션이 추가됨	Storage Gateway는 운영 체제 및 소프트웨어 업그레이드, 안정성, 성능 및 보안을 해결하기 위한 수정 사항, 새로운 기능에 대한 액세스가 포함된 정기	2024년 6월 6일

	유지 관리 업데이트를 받습니다. 이제 배포의 각 개별 게이트웨이에 대해 이러한 업데이트를 켜거나 끄도록 설정을 구성할 수 있습니다. 자세한 내용은 콘솔을 사용하여 게이트웨이 업데이트 관리 AWS Storage Gateway 콘솔을 .	
Snowball Edge에서 Tape Gateway에 대한 지원 중단	Snowball Edge 디바이스에서 더 이상 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 테스트를 참조하십시오.	2023년 10월 24일
권장되는 CloudWatch 경보가 업데이트됨	이제 CloudWatch `HealthNotifications` 경보가 모든 게이트웨이 유형 및 호스트 플랫폼에 적용되며 권장됩니다. `HealthNotifications` 및 `AvailabilityNotifications` 에 대한 권장 구성 설정도 업데이트되었습니다. 자세한 내용은 CloudWatch 경보 이해를 참조하세요.	2023년 10월 2일

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 할당량을 참조하세요.	2022년 10월 4일
Tape Gateway와 Volume Gateway 사용 설명서가 분리됨	Tape Gateway와 Volume Gateway 유형에 대한 정보를 모두 포함하고 있던 Storage Gateway 사용 설명서가 Tape Gateway 사용 설명서와 Volume Gateway 사용 설명서로 분리되어, 각 설명서에 한 가지 게이트웨이 유형에 대한 정보만 포함되어 있습니다. 자세한 내용은 Tape Gateway 사용 설명서 및 Volume Gateway 사용 설명서를 참조하세요.	2022년 3월 23일
게이트웨이 생성 절차가 업데이트됨	Storage Gateway 콘솔을 사용하여 모든 게이트웨이 유형을 생성하는 절차가 업데이트되었습니다. 자세한 내용은 게이트웨이 생성을 참조하세요.	2022년 1월 18일
새 테이프 인터페이스	AWS Storage Gateway 콘솔의 테이프 개요 페이지가 새로운 검색 및 필터링 기능으로 업데이트되었습니다. 새로운 기능을 설명하도록 이 설명서의 모든 관련 절차가 업데이트되었습니다. 자세한 내용은 Tape Gateway 관리를 참조하세요.	2021년 9월 23일

Tape Gateway용 Quest NetVault Backup 13 지원	Tape Gateway는 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 Linux에서 Tape Gateway용 IBM Spectrum Protect 8.1.10 지원	Tape Gateway가 이제 Microsoft Windows Server 및 Linux에서 실행되는 IBM Spectrum Protect 버전 8.1.10을 지원합니다. 자세한 내용은 IBM Spectrum Protect를 사용한 설정 테스트를 참조하세요.	2020년 11월 24일
FedRAMP 규정 준수	Storage Gateway가 이제 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 예약을 참조하세요.	2020년 11월 9일
캐시 볼륨 및 Tape Gateway 로컬 캐시 스토리지가 4배 증가함	Storage Gateway에서 이제 캐시 볼륨과 Tape Gateway에 최대 64TB의 로컬 캐시를 지원하여 대규모 작업 데이터 세트에 대한 지연 시간이 짧은 액세스를 제공하므로 온프레미스 애플리케이션의 성능이 향상됩니다. 자세한 내용은 게이트웨이에 권장되는 로컬 디스크 크기를 참조하세요.	2020년 11월 9일
게이트웨이 마이그레이션	Storage Gateway에서 이제 캐시 Volume Gateway를 새 가상 머신으로 마이그레이션하는 기능을 지원합니다. 자세한 내용은 캐시 볼륨을 새로운 캐시 Volume Gateway 가상 머신으로 이동을 참조하세요.	2020년 9월 10일

테이프 보존 잠금 및 WORM(Write Once Read Many) 보호 지원	Storage Gateway에서 가상 테이프에 대한 테이프 보존 잠금 및 WORM(Write Once Read Many)을 지원합니다. 테이프 보존 잠금 기능을 사용하면 아카이브된 가상 테이프에 보존 모드와 보존 기간을 지정하여 일정 기간(최대 100년) 동안 삭제되지 않도록 할 수 있습니다. 여기에는 테이프를 삭제하거나 보존 설정을 수정할 수 있는 사람에 대한 권한 제어 기능이 포함됩니다. 자세한 내용은 테이프 보존 잠금 사용을 참조하세요. WORM이 활성화된 가상 테이프는 가상 테이프 라이브러리에 있는 활성 테이프의 데이터를 덮어쓰거나 지울 수 없도록 합니다. 자세한 내용은 WORM(Write Once Read Many) 테이프 보호를 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 사용을 참조하세요.	2020년 8월 12일

새 AWS 리전에서 Federal Information Processing Standard(FIPS) 엔드포인트 지원	이제 FIPS 엔드포인트를 사용하는 게이트웨이를 미국 동부(오하이오), 미국 동부(버지니아 북부), 미국 서부(캘리포니아 북부), 미국 서부(오리건), 캐나다(중부) 리전에서 활성화할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 7월 31일
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 참조하세요.	2020년 5월 29일
FIPS(Federal Information Processing Standard) 엔드포인트 지원	이제 AWS GovCloud (US) 리전에서 FIPS 엔드포인트가 있는 게이트웨이를 활성화할 수 있습니다. Volume Gateway에 대해 FIPS 엔드포인트를 선택하려면 서비스 엔드포인트 선택을 참조하세요. Tape Gateway에 대해 FIPS 엔드포인트를 선택하려면 AWS에 Tape Gateway 연결을 참조하세요.	2020년 5월 22일

새 AWS 리전	이제 아프리카(케이프타운) 및 유럽(밀라노) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 5월 7일
S3 Intelligent-Tiering 스토리지 클래스 지원	Storage Gateway에서 이제 S3 Intelligent-Tiering 스토리지 클래스를 지원합니다. S3 Intelligent-Tiering 스토리지 클래스는 성능 영향 또는 운영 오버헤드 없이 가장 비용 효율적인 스토리지 액세스 계층으로 데이터를 자동으로 이동하여 스토리지 비용을 최적화합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 자주 액세스하는 객체와 자주 액세스하지 않는 객체를 자동으로 최적화하는 스토리지 클래스를 참조하세요.	2020년 4월 30일
Tape Gateway 쓰기 및 읽기 성능 2배 향상	Storage Gateway를 사용하면 Tape Gateway에서 가상 테이프로부터 읽어 들이는 성능과 가상 테이프로 쓰는 성능을 2배 향상시킴으로써 백업 및 복구 작업을 이전보다 신속하게 수행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Tape Gateway에 대한 성능 지침을 참조하세요.	2020년 4월 23일

자동 테이프 생성 지원	Storage Gateway에서 이제 새 가상 테이프를 자동으로 생성하는 기능을 제공합니다. Tape Gateway는 사용자가 구성한 사용 가능한 최소 테이프 수를 유지하기 위해 자동으로 새 가상 테이프를 생성한 다음 백업 애플리케이션에서 이 새 테이프를 가져올 수 있도록 설정하므로 백업 작업을 중단 없이 실행할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 자동으로 테이프 생성을 참조하세요.	2020년 4월 23일
새 AWS 리전	이제 Storage Gateway를 AWS GovCloud(미국 동부) 리전에서 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2020년 3월 12일
Linux 커널 기반 가상 머신(KVM) 하이퍼바이저 지원	Storage Gateway에서 이제 KVM 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. KVM에 배포된 게이트웨이에는 기존 온프레미스 게이트웨이와 동일한 기능이 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하세요.	2020년 2월 4일

VMware vSphere High Availability 지원	Storage Gateway에서 이제 VMware에서의 고가용성을 지원하므로 하드웨어, 하이퍼바이저 또는 네트워크 장애로부터 스토리지 워크로드를 보호할 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Storage Gateway와 함께 VMware vSphere High Availability 사용을 참조하세요. 이 릴리스에는 성능 향상도 포함되어 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 성능을 참조하세요.	2019년 11월 20일
Tape Gateway의 새 AWS 리전	이제 남아메리카(상파울루) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 9월 24일
Linux에서 IBM Spectrum Protect 버전 7.1.9 지원 및 Tape Gateway의 최대 테이프 크기를 5TiB로 늘림	Tape Gateway가 이제 Linux 및 Microsoft Windows에서 실행되는 IBM Spectrum Protect(Tivoli Storage Manager) 버전 7.1.9를 지원합니다. 자세한 내용은 Storage Gateway 사용 설명서에서 IBM Spectrum Protect를 사용한 설정 테스트를 참조하세요. 또한 Tape Gateway의 경우 가상 테이프의 최대 크기가 2.5TiB에서 5TiB로 증가했습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 테이프 할당량을 참조하세요.	2019년 9월 10일

Amazon CloudWatch Logs 지원	이제 Amazon CloudWatch 로그 그룹으로 File Gateway를 구성하여 오류 및 게이트웨이와 리소스의 상태에 대한 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway 사용 설명서에서 Amazon CloudWatch 로그 그룹으로 게이트웨이 상태 및 오류에 대한 알림 받기를 참조하세요.	2019년 9월 4일
새 AWS 리전	이제 아시아 태평양(홍콩) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 8월 14일
새 AWS 리전	이제 중동(바레인) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 엔드포인트 및 할당량을 참조하세요.	2019년 7월 29일
Virtual Private Cloud(VPC)에서 게이트웨이 활성화 지원	이제 VPC에서 게이트웨이를 활성화할 수 있습니다. 온프레미스 소프트웨어 어플라이언스와 클라우드 기반 스토리지 인프라 간에 프라이빗 연결을 생성할 수 있습니다. 자세한 내용은 Virtual Private Cloud(VPC)에서 게이트웨이 활성화를 참조하세요.	2019년 6월 20일

S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 가상 테이프 이동 지원	이제부터는 S3 Glacier Flexible Retrieval 스토리지 클래스에 저장된 가상 테이프를 비용 효과가 좋고 장기간 데이터를 보존할 수 있는 S3 Glacier Deep Archive 스토리지 클래스로 옮길 수 있습니다. 자세한 내용은 S3 Glacier Flexible Retrieval에서 S3 Glacier Deep Archive로 테이프 이전을 참조하세요.	2019년 5월 28일
Microsoft Windows ACL용 SMB 파일 공유 지원	File Gateway의 경우 Microsoft Windows 액세스 제어 목록(ACL)을 사용하여 SMB(Server Message Block) 파일 공유에 대한 액세스를 제어할 수 있습니다. 자세한 내용은 Microsoft Windows ACL를 사용하여 SMB 파일 공유에 대한 액세스 제어를 참조하세요.	2019년 5월 8일
S3 Glacier Deep Archive와 통합	Tape Gateway는 S3 Glacier Deep Archive와 통합됩니다. 이제 데이터를 장기간 보존하기 위해 가상 테이프를 S3 Glacier Deep Archive에 아카이브할 수 있습니다. 자세한 내용은 가상 테이프 아카이브를 참조하십시오.	2019년 3월 27일

유럽에서 Storage Gateway 하드웨어 어플라이언스 사용 가능	이제 유럽에서 Storage Gateway Hardware Appliance를 사용할 수 있습니다. 자세한 내용은AWS 일반 참조에서 AWS Storage Gateway 하드웨어 어플라이언스 리전을 참조하세요. 또한 Storage Gateway 하드웨어 어플라이언스에서 사용 가능한 스토리지를 5TB에서 12TB로 늘릴 수 있고, 설치된 동선 네트워크 카드를 10기가비트 광섬유 네트워크 카드로 교체할 수 있습니다. 자세한 내용은 하드웨어 어플라이언스 설정을 참조하세요.	2019년 2월 25일
와 통합 AWS Backup	Storage Gateway는와 통합됩니다 AWS Backup. 이제 AWS Backup 를 사용하여 클라우드 지원 스토리지에 Storage Gateway 볼륨을 사용하는 온프레미스 비즈니스 애플리케이션을 백업할 수 있습니다. 자세한 내용은 볼륨 백업을 참조하십시오.	2019년 1월 16일

Bacula Enterprise 및 IBM Spectrum Protect 지원	Tape Gateway에서 이제 Bacula Enterprise 및 IBM Spectrum Protect를 지원합니다. Storage Gateway에서는 또한 최신 버전의 Veritas NetBackup, Veritas Backup Exec 및 Quest NetVault 백업을 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 테스트를 참조하십시오.	2018년 11월 13일
Storage Gateway 하드웨어 어플라이언스 지원	Storage Gateway Hardware Appliance에는 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 Manager(DPM) 호환성	Tape Gateway가 이제 Microsoft System Center 2016 Data Protection Manager(DPM)와 호환됩니다. 이제 Microsoft DPM을 사용하여 Amazon S3에 데이터를 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 테스트를 참조하십시오.	2018년 7월 18일
SMB(Server Message Block) 프로토콜 지원	File Gateway에서 SMB(Server Message Block) 프로토콜에 대한 지원을 파일 공유에 추가했습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2018년 6월 20일
파일 공유, 캐시 볼륨 및 가상 테이프 암호화 지원	이제 AWS Key Management Service (AWS KMS)를 사용하여 파일 공유, 캐시 볼륨 또는 가상 테이프에 기록된 데이터를 암호화할 수 있습니다. 현재 AWS Storage Gateway API를 사용하여 이를 수행할 수 있습니다. 자세한 내용은 AWS KMS를 사용하여 데이터 암호화를 참조하세요.	2018년 6월 12일

NovaStor DataCenter/Network 지원	Tape Gateway에서 이제 NovaStor DataCenter/Network를 지원합니다. 이제 NovaStor DataCenter/Network 버전 6.4 또는 7.1을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 NovaStor DataCenter/Network를 사용하여 설정 테스트를 참조하십시오.	2018년 5월 24일

이전 업데이트

다음 표에서는 2018년 5월 이전 AWS Storage Gateway 사용 설명서의 각 릴리스에서 변경된 중요 사항에 대해 설명합니다.

변경	설명	변경 날짜
S3 One Zone_IA 스토리지 클래스 지원	File Gateway의 경우 S3 One Zone_IA를 파일 공유에 대한 기본 스토리지 클래스로 선택할 수 있습니다. 이 스토리지 클래스를 사용하여 Amazon S3의 단일 가용 영역에 객체 데이터를 저장할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2018년 4월 4일
새로운 리전	이제 아시아 태평양(싱가포르) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2018년 3월 4일
Amazon S3 버킷에 대한 캐시 새로 고침 알림, 요청자 지불 및 미리 준비	이제 게이트웨이가 Amazon S3 버킷에서 캐시 새로 고침을 완료하면 File Gateway를 통해 알림을 받을 수 있습니다. 자세한 내용은 API Gateway API 참조에서 RefreshCache.html를 참조하세요.	2018년 3월 1일

변경	설명	변경 날짜
된 ACL을 지원합니다.	이제 File Gateway를 통해 버킷 소유자가 아닌 요청자나 리더가 액세스 요금을 지불할 수 있습니다. 또한 File Gateway를 통해 NFS 파일 공유에 매핑되는 S3 버킷 소유자에게 완전한 제어 권한을 제공할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	
Dell EMC NetWorker V9.x 지원	이제 Tape Gateway에서 Dell EMC NetWorker V9.x를 지원합니다. 이제 Dell EMC NetWorker V9.x를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Dell EMC NetWorker를 사용한 설정 테스트를 참조하세요.	2018년 2월 27일
새로운 리전	이제 유럽(파리) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2017년 12월 18일
파일 업로드 알림 및 MIME 유형 추측 지원	이제 File Gateway를 통해 NFS 파일 공유에 기록한 모든 파일이 Amazon S3에 업로드되었을 때 알림을 받을 수 있습니다. 자세한 내용은 Storage Gateway API 참조에서 NotifyWhenUploaded를 참조하십시오. 이제 File Gateway를 통해 파일 확장자를 기반으로 업로드되는 객체의 MIME 유형을 추측할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요.	2017년 11월 21일
VMware ESXi Hypervisor 버전 6.5 지원	AWS Storage Gateway 는 이제 VMware ESXi Hypervisor 버전 6.5를 지원합니다. 이는 버전 4.1, 5.0, 5.1, 5.5 및 6.0에 추가된 지원 기능입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2017년 9월 13일

변경	설명	변경 날짜
Commvault 11과의 호환성	Tape Gateway가 이제 Commvault 11과 호환됩니다. 이제 Commvault를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Commvault를 사용한 설정 테스트를 참조하세요.	2017년 9월 12일
Microsoft Hyper-V 하이퍼바이저의 File Gateway 지원	이제 Microsoft Hyper-V 하이퍼바이저에 File Gateway를 배포할 수 있습니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하세요.	2017년 6월 22일
아카이브로부터 3~5시간 테이프 검색 지원	Tape Gateway의 경우 이제 아카이브에서 3-5시간 후에 테이프를 검색할 수 있습니다. 또한 백업 애플리케이션 또는 가상 테이프 라이브러리(VTL)에서 테이프로 기록되는 데이터의 양을 결정할 수도 있습니다. 자세한 내용은 테이프 사용량 보기를 참조하세요.	2017년 5월 23일
새로운 리전	이제 아시아 태평양(뭄바이) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2017년 5월 02일
파일 공유 설정 업데이트 파일 공유에 대한 캐시 새로 고침 지원	이제 File Gateway를 통해 파일 공유 설정에 마운팅 옵션을 추가할 수 있습니다. 이제 파일 공유에 대해 스쿼시 및 읽기 전용 옵션을 설정할 수 있습니다. 자세한 내용은 파일 공유 생성을 참조하세요. 이제 File Gateway를 통해 게이트웨이가 마지막으로 버킷의 콘텐츠를 나열하고 결과를 캐싱한 이후에 추가 또는 제거된 Amazon S3 버킷에서 객체를 찾을 수 있습니다. 자세한 내용은 API 참조의 RefreshCache를 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 복제를 참조하세요.	2017년 3월 16일

변경	설명	변경 날짜
Amazon EC2에서 File Gateway 지원	AWS Storage Gateway 는 이제 Amazon EC2에 파일 게이트웨이를 배포할 수 있는 기능을 제공합니다. 이제 커뮤니티 AMI로 사용할 수 있는 Storage Gateway Amazon Machine Image(AMI)를 사용하여 Amazon EC2에서 File Gateway를 시작할 수 있습니다. File Gateway를 생성하여 EC2 인스턴스에 배포하는 방법에 대한 자세한 내용은 Amazon S3 File Gateway 작성 및 활성화 또는 Amazon FSx File Gateway 작성 및 활성화를 참조하세요. File Gateway AMI를 시작하는 방법에 대한 자세한 내용은 Amazon EC2 호스트에 S3 File Gateway 배포 또는 Amazon EC2 호스트에 FSx File Gateway 배치를 참조하세요.	2017년 2월 08일
Arcserve 17과의 호환성	Tape Gateway가 이제 Arcserve 17과 호환됩니다. 이제 Arcserve를 사용하여 데이터를 Amazon S3에 백업하고 S3 Glacier Flexible Retrieval에 직접 아카이브할 수 있습니다. 자세한 내용은 Arcserve Backup r17.0을 사용한 설정 테스트를 참조하세요.	2017년 1월 17일
새로운 리전	이제 EU(런던) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 12월 13일
새로운 리전	이제 캐나다(중부) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 08월 12일
File Gateway 지원	Storage Gateway에서 이제 Volume Gateway 및 Tape Gateway 외에도 File Gateway를 제공합니다. File Gateway는 서비스와 가상 소프트웨어 어플라이언스를 결합함으로써 네트워크 파일 시스템(NFS)과 같은 업계 표준 파일 프로토콜을 사용하여 Amazon S3에(서) 객체를 저장하고 가져올 수 있게 해줍니다. 이 게이트웨이를 통해 NFS 마운트 포인트에 있는 파일인 Amazon S3 내 객체에 액세스할 수 있습니다.	2016년 11월 29일

변경	설명	변경 날짜
Backup Exec 16	Tape Gateway가 이제 Backup Exec 16과 호환됩니다. 이제 Backup Exec 16을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2016년 11월 7일
Micro Focus(HPE) Data Protector 9.x와의 호환성	Tape Gateway가 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) Data Protector를 사용한 설정 테스트를 참조하세요.	2016년 11월 2일
새로운 리전	이제 미국 동부(오하이오) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2016년 10월 17일
Storage Gateway 콘솔 재설계	Storage Gateway Management Console을 재설계하여 게이트웨이, 볼륨 및 가상 테이프를 구성, 관리 및 모니터링하는 작업이 더 수월해졌습니다. 이제 사용자 인터페이스는 필터링할 수 있는 뷰를 제공하고 CloudWatch 및 Amazon EBS와 같은 통합 AWS 서비스에 대한 직접 링크를 제공합니다. 자세한 내용은 에 가입 AWS Storage Gateway 단원을 참조하십시오.	2016년 8월 30일
Veeam Backup & Replication V9 업데이트 2 이상과의 호환성	Tape Gateway가 이제 Veeam Backup & Replication V9 업데이트 2 이상(즉 버전 9.0.0.1715 이상)과 호환됩니다. 이제 Veeam Backup Replication V9 업데이트 2 이상을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veeam Backup & Replication를 사용한 설정 테스트 참조하세요.	2016년 8월 15일

변경	설명	변경 날짜
더 긴 볼륨 및 스냅샷 ID	Storage Gateway는 현재 더 긴 볼륨 및 스냅샷 ID를 도입하고 있습니다. 볼륨, 스냅샷 및 기타 지원되는 AWS 리소스에 대해 더 긴 ID 형식을 활성화할 수 있습니다. 자세한 내용은 Storage Gateway 리소스 및 리소스 ID 이해 단원을 참조하십시오.	2016년 4월 25일
새로운 리전 저장 볼륨에 대한 최대 512TiB 크기의 스토리지 지원 Storage Gateway 로컬 콘솔에 대한 기타 게이트웨이 업데이트 및 개선 사항	이제 아시아 태평양(서울) 리전에서 Tape Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는 단원을 참조하십시오. 저장 볼륨의 경우, 최대 크기가 16TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 512TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요. 가상 테이프 라이브러리에 있는 모든 테이프의 총 크기가 1PiB로 증가하였습니다. 자세한 내용은 AWS Storage Gateway 할당량 단원을 참조하십시오. 이제 Storage Gateway 콘솔에서 VM 로컬 콘솔의 암호를 설정할 수 있습니다. 자세한 내용은 Storage Gateway 콘솔에서 로컬 콘솔 암호 설정 단원을 참조하세요.	2016년 3월 21일
Dell EMC NetWorker 8.x와의 호환성	Tape Gateway가 이제 Dell EMC NetWorker 8.x와 호환됩니다. 이제 Dell EMC NetWorker를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Dell EMC NetWorker를 사용한 설정 테스트를 참조하세요.	2016년 2월 29일

변경	설명	변경 날짜
VMware ESXi Hypervisor 버전 6.0 및 Red Hat Enterprise Linux 7 iSCSI 초기자 지원	AWS Storage Gateway 는 이제 VMware ESXi Hypervisor 버전 6.0과 Red Hat Enterprise Linux 7 iSCSI 초기자를 지원합니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 및 지원되는 iSCSI 이니시에이터 섹션을 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.	
캐싱 볼륨에 대한 최대 1,024TiB 크기의 스토리지 지원	캐싱 볼륨의 경우, 최대 크기가 32TiB인 각 스토리지 볼륨을 최대 32개까지 생성하여 전체 스토리지를 최대 1,024TiB까지 구성할 수 있습니다. 자세한 내용은 캐시 볼륨 아키텍처 및 AWS Storage Gateway 할당량 섹션을 참조하세요.	2015년 9월 16일
VMware ESXi 하이퍼바이저의 VMXNET3(10GbE) 네트워크 어댑터 유형 지원	게이트웨이를 VMware ESXi 하이퍼바이저에서 호스팅하는 경우, 게이트웨이에서 VMXNET3 어댑터 유형을 사용하도록 재구성할 수 있습니다. 자세한 내용은 게이트웨이용 네트워크 어댑터 구성 단원을 참조하십시오.	
성능 개선 사항	Storage Gateway의 최대 업로드 속도를 초당 120MB로 개선하였고, 최대 다운로드 속도는 초당 20MB로 개선하였습니다.	
Storage Gateway 로컬 콘솔에 대한 기타 개선 사항 및 업데이트	유지 관리 작업을 수행하는 데 도움이 되는 부가 기능으로 Storage Gateway 로컬 콘솔을 업데이트 및 강화하였습니다. 자세한 내용은 게이트웨이 네트워크 구성 단원을 참조하십시오.	

변경	설명	변경 날짜
태그 지정 지원	Storage Gateway에서 이제 리소스 태그 지정을 지원합니다. 이제 게이트웨이, 볼륨, 가상 테이프에 태그를 추가하여 더 쉽게 관리할 수 있습니다. 자세한 내용은 Storage Gateway 리소스에 태그를 지정 단원을 참조하십시오.	2015년 9월 2일
Quest(이전 명칭은 Dell) NetVault Backup 10.0과의 호환성	Tape Gateway가 이제 Quest NetVault Backup 10.0과 호환됩니다. 이제 Quest NetVault Backup 10.0을 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Quest NetVault Backup를 사용한 설정 테스트 참조하세요.	2015년 6월 22일

변경	설명	변경 날짜
저장 볼륨 게이트웨이 설정에 대한 16TiB 스토리지 볼륨 지원	Storage Gateway에서 이제 저장 Volume Gateway 설정에 대해 16TiB 스토리지 볼륨을 지원합니다. 이제 16TiB 스토리지 볼륨을 최대 12개까지 생성하여 전체 스토리지를 최대 192TiB까지 구성할 수 있습니다. 자세한 내용은 저장 볼륨 아키텍처를 참조하세요.	2015년 6월 3일
Storage Gateway 로컬 콘솔에서 시스템 리소스 점검 기능 지원	이제 시스템 리소스(가상 CPU 코어, 루트 볼륨 크기 및 RAM)이 게이트웨이가 제대로 작동하는 데 충분한지 판단할 수 있습니다. 자세한 내용은 게이트웨이 시스템 리소스 상태 조회 또는 게이트웨이 시스템 리소스 상태 조회을 참조하세요.	
Red Hat Enterprise Linux 6 iSCSI 초기자 지원	Storage Gateway에서 이제 Red Hat Enterprise Linux 6 iSCSI 이니시에이터를 지원합니다. 자세한 내용은 Tape Gateway 설정 요구 사항 단원을 참조하십시오.	
	이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다. • 이제 Storage Gateway 콘솔에서 게이트웨이에 소프트웨어 업데이트를 성공적으로 적용한 최종 날짜와 시간을 볼 수 있습니다. 자세한 내용은 게이트웨이 업데이트 관리 단원을 참조하십시오. • Storage Gateway에서 이제 스토리지 볼륨에 연결된 iSCSI 이니시에이터를 나열하는 데 사용할 수 있는 API를 제공합니다. 자세한 내용은 API 참조의 ListVolumeInitiators를 참조하십시오.	

변경	설명	변경 날짜
Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2 지원	Storage Gateway에서 이제 Microsoft Hyper-V 하이퍼바이저 버전 2012 및 2012 R2를 지원합니다. 이것은 Microsoft Hyper-V 하이퍼바이저 버전 2008 R2 지원에 추가된 것입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 4월 30일
Symantec Backup Exec 15와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 15와 호환됩니다. 이제 Symantec Backup Exec 15를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2015년 4월 6일
스토리지 볼륨에 대한 CHAP 인증 지원	Storage Gateway에서 이제 스토리지 볼륨에 대한 CHAP 인증을 지원합니다. 자세한 내용은 볼륨에 대한 CHAP 인증 구성을 참조하세요.	2015년 4월 2일
VMware ESXi Hypervisor 버전 5.1 및 5.5 지원	Storage Gateway에서 이제 VMware ESXi Hypervisor 버전 5.1 및 5.5를 지원합니다. 이는 VMware ESXi Hypervisor 버전 4.1 및 5.0 지원에 추가된 것입니다. 자세한 내용은 지원되는 하이퍼바이저 및 호스트 요구 사항 단원을 참조하십시오.	2015년 3월 30일
Windows CHKDSK 유틸리티 지원	Storage Gateway에서 이제 Windows CHKDSK 유틸리티를 지원합니다. 이 유틸리티를 사용하여 볼륨의 무결성을 확인하고 볼륨의 오류를 수정할 수 있습니다. 자세한 내용은 볼륨 문제 해결을 참조하세요.	2015년 3월 04일

변경	설명	변경 날짜
API 호출을 캡처 AWS CloudTrail 하기 위해와 통합	이제 Storage Gateway가 Amazon Web Services 계정에서 Storage Gateway에 의해 또는 Storage Gateway를 대신하여 수행된 AWS CloudTrail API 호출을 AWS CloudTrail캡처하고 지정한 Amazon S3 버킷에 로그 파일을 전송합니다. 자세한 내용은 에서 로깅 및 모니터링 AWS Storage Gateway 단원을 참조하십시오. 이 릴리스는 다음과 같은 Storage Gateway 개선 사항 및 업데이트를 포함합니다. • 이제 캐시 스토리지에 오손 데이터(dirty data)가 있는 가상 테이프, 즉 AWS에 업로드하지 않은 콘텐츠를 포함하는 가상 테이프는 게이트웨이의 캐싱된 드라이브가 변경될 때 복구됩니다. 자세한 내용은 복구할 수 없는 게이트웨이에서 가상 테이프를 복구하는 경우를 참조하세요.	2014년 12월 16일

변경	설명	변경 날짜
추가 백업 소프트웨어 및 미디어 체인저와의 호환성	Tape Gateway가 이제 다음 백업 소프트웨어와 호환됩니다. • Symantec Backup Exec 2014 • Microsoft System Center 2012 R2 Data Protection Manager • Veeam Backup & Replication V7 • Veeam Backup & Replication V8 이제 Storage Gateway 가상 테이프 라이브러리(VTL)에 이 네 가지 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. Storage Gateway에서 이제 새 백업 소프트웨어와 함께 작동하는 추가 미디어 체인저를 제공합니다. 이 릴리스에는 기타 AWS Storage Gateway 개선 사항 및 업데이트가 포함되어 있습니다.	2014년 11월 3일
유럽(프랑크푸르트) 리전	이제 유럽(프랑크푸르트) 리전에서 Storage Gateway를 사용할 수 있습니다. 자세한 내용은 AWS 리전 Storage Gateway를 지원하는섹션을 참조하세요.	2014년 10월 23일

변경	설명	변경 날짜
콘텐츠 재구성	모든 게이트웨이 솔루션에 공통된 시작하기 단원을 만들었습니다. 아래에서는 게이트웨이를 다운로드, 배포 및 활성화하는 방법에 대한 지침을 얻을 수 있습니다. 게이트웨이를 배포하고 활성화한 후 저장 볼륨, 캐시 볼륨 및 Tape Gateway 설정에 따른 추가 지침에 따라 작업을 수행할 수 있습니다. 자세한 내용은 Tape Gateway 생성을 참조하세요.	2014년 5월 19일
Symantec Backup Exec 2012와의 호환성	Tape Gateway가 이제 Symantec Backup Exec 2012와 호환됩니다. 이제 Symantec Backup Exec 2012를 사용하여 Amazon S3에 데이터를 백업하고, 오프라인 스토리지(S3 Glacier Flexible Retrieval 또는 S3 Glacier Deep Archive)에 직접 아카이브할 수 있습니다. 자세한 내용은 Veritas Backup Exec을 사용한 설정 테스트를 참조하세요.	2014년 4월 28일

변경	설명	변경 날짜
Windows Server Failover Clustering 지원 VMware ESX 초기자 지원 Storage Gateway 로컬 콘솔에서 구성 작업을 수행하도록 지원	• Storage Gateway에서 이제 호스트가 Windows Server Failover Clustering(WSFC)을 사용하여 액세스를 조정할 경우 한 볼륨에 여러 호스트를 연결하도록 지원합니다. 하지만 WSFC를 사용하지 않으면 한 볼륨에 여러 호스트를 연결할 수 없습니다. • Storage Gateway를 사용하여 이제 ESX 호스트를 통해 직접 스토리지 연결을 관리할 수 있습니다. 이는 VM의 게스트 OS에 상주하는 초기자를 사용하는 방식의 대안입니다. • 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 배포한 게이트웨이에서 구성 작업을 수행하는 방법에 대한 정보는 Amazon EC2 로컬 콘솔에서 작업 수행 또는 Amazon EC2 로컬 콘솔에서 작업 수행 단원을 참조하십시오.	2014년 1월 31일

변경	설명	변경 날짜
가상 테이프 라이브러리(VTL) 지원 및 API 버전 2013-06-30 도입	Storage Gateway는 온프레미스 소프트웨어 어플라이언스를 클라우드 기반 스토리지와 연결하여 온프레미스 IT 환경을 AWS 스토리지 인프라와 통합합니다. Storage Gateway에서 이제 Volume Gateway 캐시 볼륨 및 저장 볼륨 이외에도 게이트웨이 가상 테이프 라이브러리(VTL)를 지원합니다. Tape Gateway에 게이트웨이당 가상 테이프 드라이브를 최대 10개까지 구성할 수 있습니다. 각 가상 테이프 드라이브는 SCSI 명령 세트에 반응하므로 기존 온프레미스 백업 애플리케이션은 수정하지 않고도 작동합니다. 자세한 내용은AWS Storage Gateway 사용 설명서에서 다음 주제를 참조하세요. • 아키텍처 개요는 Tape Gateway 작동 방식(아키텍처)을 참조하세요. • Tape Gateway를 시작하려면 Tape Gateway 생성을 참조하세요.	2013년 11월 5일
Microsoft Hyper-V 지원	Storage Gateway에서 이제 Microsoft Hyper-V 가상화 플랫폼에 온프레미스 게이트웨이를 배포할 수 있는 기능을 제공합니다. Microsoft Hyper-V에 배포한 게이트웨이에는 기존 온프레미스 Storage Gateway와 동일한 기능이 있습니다. Microsoft Hyper-V를 이용해 게이트웨이 배포를 시작하려면 지원되는 하이퍼바이저 및 호스트 요구 사항을 참조하십시오.	2013년 10월 4일

변경	설명	변경 날짜
Amazon EC2에서 게이트웨이 배포 지원	Storage Gateway에서 이제 Amazon Elastic Compute Cloud(Amazon EC2)에 게이트웨이를 배포할 수 있는 기능을 제공합니다. AWS Marketplace에서 제공하는 Storage Gateway AMI를 사용하여 Amazon EC2에서 게이트웨이 인스턴스를 시작할 수 있습니다. Storage Gateway AMI를 사용해 게이트웨이 배포를 시작하려면 Tape Gateway용 사용자 지정 Amazon EC2 인스턴스 배포 섹션을 참조하세요.	2013년 1월 15일
캐싱 볼륨 지원 및 API 버전 2012-06-30 도입	이번 릴리스에서는 Storage Gateway에 캐시 볼륨에 대한 지원을 도입했습니다. 캐싱 볼륨은 온프레미스 스토리지 인프라를 확장할 필요성을 최소화하는 한편, 애플리케이션이 활성 데이터에 액세스할 때의 지연 시간을 짧게 유지하도록 해줍니다. 최대 32TiB 크기의 스토리지 볼륨을 생성하고, 이를 온 프레미스 애플리케이션 서버의 iSCSI 디바이스로 마운트할 수 있습니다. 캐시 볼륨에 작성한 데이터는 Amazon Simple Storage Service(S3)에 저장되고, 최근에 쓰고 읽은 데이터의 캐시만 온프레미스 스토리지 하드웨어에 로컬로 저장됩니다. 캐시 볼륨을 사용하면 짧은 액세스 지연 시간이 필요한 데이터에 대한 온프레미스 스토리지를 유지하는 한편, 더 오래되고 덜 자주 액세스하는 데이터와 같이 더 긴 가져오기 지연 시간을 수용할 수 있는 데이터에 대해서는 Amazon S3를 활용할 수 있습니다. 이 릴리스에서 Storage Gateway는 현재 작업을 지원할 뿐 아니라 새 작업을 제공하여 캐시 볼륨을 지원하는 새로운 API 버전을 도입하였습니다. 두 가지 Storage Gateway 솔루션에 대한 자세한 내용은 Tape Gateway 작동 방식 섹션을 참조하세요. 테스트 설정을 시도해 볼 수도 있습니다. 지침은 Tape Gateway 생성을 참조하세요.	2012년 10월 29일

변경	설명	변경 날짜
API 및 IAM 지원	이 릴리스에서 Storage Gateway는 API 지원과 AWS Identity and Access Management(IAM)에 대한 지원을 도입합니다. • API 지원 - 이제 Storage Gateway 리소스를 프로그래밍 방식으로 구성 및 관리할 수 있습니다. API에 대한 자세한 내용은AWS Storage Gateway 사용 설명서에서 Storage Gateway용 API 참조 섹션을 참조하세요. • IAM 지원 - AWS Identity and Access Management (IAM)를 사용하면 IAM 정책을 통해 사용자를 생성하고 Storage Gateway 리소스에 대한 사용자 액세스를 관리할 수 있습니다. IAM 정책에 대한 예시는 Identity and Access Management for AWS Storage Gateway 단원을 참조하세요. IAM에 대한 자세한 내용은 AWS Identity and Access Management (IAM) 세부 정보 페이지를 참조하세요.	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

Storage Gateway AL2에서 AL2023으로 마이그레이션 캠페인

AWS 는 새로운 하이브리드 클라우드 스토리지 기능을 활성화하고 최적의 성능 및 보안 표준을 유지하기 위해 Storage Gateway 어플라이언스 운영 체제(OS)를 Amazon Linux 2에서 AL2023으로 전환하고 있습니다. 이 전환은 모든 AL2-based Storage Gateway 어플라이언스 버전 S3 File Gateway 버전 1.x, Tape Gateway 버전 2.x 및 Volume Gateway 버전 2.x에 영향을 미칩니다. 는 이후 이러한 시스템 지원을 중단하므로 2026년 6월 30일 이전에 마이그레이션을 완료해야 AWS 합니다.

여러 방법을 통해 게이트웨이에 마이그레이션이 필요한지 여부를 식별할 수 있습니다. AWS 콘솔은 영향을 받는 게이트웨이에 대한 게이트웨이의 세부 정보 탭에 사용 중단 메시지를 표시합니다. 또한 `DescribeGatewayInformation` API는 사용 중단 날짜 필드를 확인할 수 있는 프로그래밍 방식의 액세스를 제공합니다. AWS 상태 대시보드는 영향을 받는 리소스 탭 아래에 영향을 받는 게이트웨이를 나열합니다. 그러나 게이트웨이가 마이그레이션된 직후에는 목록이 업데이트되지 않습니다. 마이그레이션 프로세스 자체는 데이터 안전을 우선시하도록 설계되었으며, 필요한 경우 쉽게 복구할 수 있도록 마이그레이션이 시작되기 AWS 전에 온프레미스 게이트웨이 VM 데이터의 사본을에 저장합니다.

AWS 는 각 게이트웨이 유형에 맞는 포괄적인 마이그레이션 가이드를 제공합니다. 마이그레이션을 완료한 후에는 AWS 콘솔의 게이트웨이 세부 정보 탭에 사용 중단 경고가 더 이상 나타나지 않는지 확인하거나 `DescribeGatewayInformation` API를 사용하여 사용 중단 날짜 필드가 없는지 확인하여 성공을 확인해야 합니다. 되돌리면 운영 문제가 발생할 수 있으므로 AL2023으로 성공적으로 마이그레이션한 후에는 AL2 게이트웨이로 되돌리지 않아야 합니다.

마이그레이션 기간 동안 AWS 는 이메일을 통해 월별 알림 알림과 AWS 상태 대시보드의 예약된 변경 사항 탭을 보내 마이그레이션을 계획하고 완료하는 데 도움을 줍니다. 마이그레이션 중에 문제가 발생하면 AWS Support에 문의하여 지원 및 문제 해결 지침을 받으세요.

빠른 링크 및 리소스

게이트웨이 버전 마이그레이션 참조

마이그레이션이 필요한 게이트웨이를 이해하는 것은 게이트웨이 소프트웨어 버전 번호에 따라 간단합니다. Amazon Linux 2 OS를 기반으로 최근에 활성화된 게이트웨이도 2026년 6월 30일까지 마이그레이션해야 합니다.

게이트웨이 유형	AL2 버전(마이그레이션 필요)	AL2023 버전(대상)
S3 File Gateway	버전 1.x	버전 2.x
Tape Gateway	버전 2.x	버전 3.x
Volume Gateway	버전 2.x	버전 3.x

마이그레이션 타임라인

마이그레이션 타임라인에는 다음과 같은 몇 가지 중요한 마일스톤이 포함되어 있습니다.

- 2025년 10월 28일: Storage Gateway 콘솔에서 시작된 모든 새 게이트웨이 배포는 기본적으로 AL2023 이미지로 설정됩니다.
- 2026년 1월 5일: AWS 새 AL2 게이트웨이 활성화를 제한하기 시작합니다.
- 2026년 6월 30일: AL2-based 게이트웨이는 소프트웨어 업데이트 수신을 중단하고 AWS 지원이 종료됩니다. 이 날짜 이후에는 AL2-based 어플라이언스를 계속 사용할 수 있지만 새 소프트웨어 업데이트, 보안 패치 또는 버그 수정은 없으며 이러한 시스템을 유지 관리하는 것은 전적으로 사용자의 책임입니다.

마이그레이션 가이드

- S3 파일 게이트웨이 마이그레이션 가이드
- Tape Gateway 마이그레이션 가이드
- Volume Gateway 마이그레이션 가이드

지원 및 모니터링

- Storage Gateway 콘솔
- AWS 개인 상태 대시보드
- AWS Support에 문의

FAQ

마이그레이션 중에 내 데이터는 어떻게 되나요?

마이그레이션 프로세스 AWS 전반에 걸쳐 데이터는에 안정적으로 저장됩니다. 마이그레이션 절차에는 필요한 경우 쉽게 복구할 수 AWS 있도록 온프레미스 게이트웨이 VM 데이터의 사본을에 저장하는 작업이 포함됩니다.

마이그레이션 중에 가동 중지가 발생하나요?

마이그레이션 타이밍과 잠재적 서비스 중단은 게이트웨이 유형 및 구성에 따라 달라집니다. 자세한 내용은 배포에 대한 게이트웨이별 마이그레이션 가이드를 검토하세요.

2026년 6월 30일까지 마이그레이션하지 않으면 어떻게 되나요?

게이트웨이는 계속 정상적으로 작동하며 데이터는 안전하게 저장되지만 업데이트 및 지원을 계속 받으려면 2026년 6월 30일까지 영향을 받는 게이트웨이를 마이그레이션 AWS해야 합니다.

마이그레이션 후에도 AL2 기반 게이트웨이를 계속 사용할 수 있나요?

아니요. 성공적으로 마이그레이션한 후에는 새 AL2023 게이트웨이와 함께 AL2 게이트웨이를 사용해서는 안 됩니다. 앞으로는 새 AL2023-based 게이트웨이만 사용합니다. AL2 및 AL2023 게이트웨이를 동시에 사용하면 운영 문제가 발생할 수 있습니다.

마이그레이션 중에 문제가 발생했습니다. 어떻게 해야 합니까?

AWS Support에 문의하여 도움을 받으세요. 지원 팀은 마이그레이션 문제를 해결하고 프로세스를 안내할 수 있습니다.

Tape Gateway 어플라이언스 소프트웨어 릴리스 정보

이 릴리스 정보에서는 Tape Gateway 어플라이언스의 각 버전에 포함된 새로운 기능과 업데이트된 기능, 개선 사항 및 수정 사항에 대해 설명합니다. 각 소프트웨어 버전은 릴리스 날짜와 고유 버전 번호로 식별됩니다.

Storage Gateway 콘솔에서 세부 정보 페이지를 확인하거나 다음과 유사한 AWS CLI 명령을 사용하여 DescribeGatewayInformation API 작업을 호출하여 Storage Gateway의 소프트웨어 버전 번호를 확인할 수 있습니다.

```
aws storagegateway describe-gateway-information --gateway-arn
 "arn:aws:storagegateway:us-west-2:123456789012:gateway/sgw-12A3456B"
```

버전 번호는 API 응답의 `SoftwareVersion` 필드에 반환됩니다.

> **Note**
>
> 다음과 같은 상황에서는 게이트웨이가 소프트웨어 버전 정보를 보고하지 않습니다.
>
> - 게이트웨이가 오프라인 상태입니다.
> - 게이트웨이에서 버전 보고를 지원하지 않는 이전 소프트웨어를 실행 중입니다.
> - 게이트웨이 유형이 FSx File Gateway입니다.

게이트웨이의 기본 자동 유지 관리 및 업데이트 일정을 수정하는 방법을 포함하여 Tape Gateway VolumeGateway 업데이트에 대한 자세한 내용은 스토리지 게이트웨이 콘솔을 AWS Storage Gateway .

Amazon Linux 2에서 AL2023으로 Tape Gateway를 마이그레이션하는 방법에 대한 자세한 내용은 섹션을 참조하세요AL2에서 AL2023으로 마이그레이션.

Amazon Linux 2023(AL2023) 기반 게이트웨이

다음 표에는 AL2023 기반 게이트웨이의 릴리스 정보가 나와 있습니다.

> **Note**
>
> 게이트웨이 버전 2.x.x는 3.x.x로 업데이트할 수 없습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-03-02	3.2.3	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 일부 게이트웨이의 게이트웨이 로그 관련 문제를 해결했습니다.
2026-02-12	3.2.2	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • VPC 엔드포인트(VPCE)가 정적 IP 주소로 설정된 AL2023 게이트웨이의 소프트웨어 업데이트 관련 문제를 해결했습니다.
2026-02-02	3.2.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-01-06	3.1.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-12-04	3.0.6	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-11-06	3.0.5	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위

릴리스 날짜	소프트웨어 버전	릴리스 정보
		해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-10-10	3.0.4	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-09-12	3.0.3	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-08-29	3.0.2	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 고정 IP 구성 관련 문제를 해결했습니다.
2025-08-18	3.0.1	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 관리자가 가상 테이프가 `IRRECOVERABLE` 상태로 전환되는 시점을 모니터링하는 데 도움이 되는 CloudWatch Logs 이벤트 추가
2025-07-16	3.0.0	• 새 운영 체제의 최초 릴리스 • IPv6 지원 추가

Amazon Linux 2(AL2) 기반 게이트웨이

다음 표에는 AL2 기반 게이트웨이의 릴리스 정보가 나와 있습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2026-03-02	2.14.2	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-02-02	2.14.1	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2026-01-05	2.14.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-12-05	2.13.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-11-03	2.12.15	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-10-01	2.12.14	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-09-02	2.12.13	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
		• 관리자가 가상 테이프가 IRRECOVERABLE 상태로 전환되는 시점을 모니터링하는 데 도움이 되는 CloudWatch Logs 이벤트 추가
2025-07-31	2.12.12	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-07-01	2.12.11	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-06-02	2.12.10	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-05-01	2.12.9	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-05-01	2.12.8	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-04-01	2.12.7	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2025-03-04	2.12.6	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2025-02-04	2.12.5	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 소프트웨어 업데이트 후 게이트웨이가 종료 상태에서 멈출 수 있는 문제를 해결했습니다.
2025-01-07	2.12.3	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-12-06	2.12.2	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-11-06	2.12.1	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-10-03	2.12.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-08-30	2.11.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-07-29	2.10.0	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 기타 버그 수정 및 개선 사항
2024-06-17	2.9.2	• 신규 및 기존 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2024-05-28	2.9.0	• 소프트웨어 업데이트 중 게이트웨이 재시작 시간 단축 • 네트워크 대역폭을 추정하기 위해 전송되는 데이터 양 감소
2024-05-08	2.8.3	• SOCKS5 프록시 사용 시 클라우드 연결 문제 해결 • 특정 조건(예: 테이프 삭제 작업 횟수가 많은 경우)에서 발생하는 업로드 성능 저하 문제 해결

릴리스 날짜	소프트웨어 버전	릴리스 정보
2024-04-10	2.8.1	• 2.8.0에서 발생하던 메모리 사용량 문제 해결 • 보안 패치 업데이트 • 소프트웨어 업데이트 프로세스 개선 • 새 게이트웨이에 대한 NTP(Network Time Protocol) 구성 요소 누락 문제 해결
2024-03-06	2.8.0	• 새 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다. • 보안 패치 업데이트 • 동시 백업 및 복원 워크로드에 대한 성능 개선
2023-12-19	2.7.0	• 새 게이트웨이의 보안 및 성능을 개선하기 위해 운영 체제 및 소프트웨어 요소를 업데이트했습니다.
2023-12-14	2.6.6	• 5TiB보다 큰 테이프에서 상대적 위치 지정 문제를 수정했습니다.
2023-10-19	2.6.5	• 게이트웨이 재시작 후 클라이언트의 테이프 덮어쓰기를 방지하는 안전 장치 추가

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