DL 어플라이언스의 Rapid Recovery 6.0

사용 설명서

DELL EMC

참고, 주의 및 경고

노트: **"주"는 컴퓨터를 보다 효율적으로 사용하는 데 도움을 주는 중요 정보를 제공합니다.**

주의: **"주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.**

경고: **"경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.**

© 2016 Dell Inc. 저작권 본사 소유. 이 제품은 미국, 국제 저작권법 및 지적 재산권법에 의해 보호됩니다. Dell 및 Dell 로고는 미국 및/또는 기타 관할지역에서 사용되는 Dell Inc.의 상표입니다. 이 문서에 언급된 기타 모든 표시 및 이름은 각 회사의 상표일 수 있습니다.

2016 - 09

개정 A00

목차

1 DL 어플라이언스 소개 11
배포 아키텍처 11
스마트 에이전트 13
DL 어플라이언스 Core 13
스냅샷 프로세스 13
재난 복구 사이트 또는 서비스 공급자 복제 13
복구 14
제품 기능 14
리포지토리 이해 14
Rapid Recovery에서 중복 제거 15
암호화 키 이해 16
Rapid Recovery로 복제 17
보존 및 아카이빙 20
가상화 및 클라우드 21
경고 및 이벤트 관리 21
라이센스 포털 22
웹 콘솔 22
서비스 관리 API 22

2 DL Appliance Core 작업 23
Rapid Recovery Core Console 이해 23
Rapid Recovery Core Console 액세스 23
빠른 시작 안내서 이해 23
Rapid Recovery Core Console로 이동 25
보호된 시스템 메뉴 보기 28
탐색 메뉴에서 복제된 시스템 보기 32
복구 지점만 메뉴 보기 33
사용자 지정 그룹 메뉴 보기 33
오류 대화 상자 사용 34
Core 설정 34
Rapid Recovery Core 설정 34
Core 설정 백업 및 복원 61
코어 수준 도구 62
Core 구성을 위한 로드맵 64
리포지토리 64
DVM 리포지토리 관리 65
보안 관리 76
보호된 시스템에서 암호화 적용 또는 제거 76
암호화 키 관리 79
클라우드 계정 관리 85
클라우드 계정 정보 85

클라우드 계정 추가 86
클라우드 계정 편집 87
클라우드 계정 설정 구성 87
클라우드 계정 제거 88
아카이브 88
아카이브 이해 88
아카이브 만들기 88
예약된 아카이브 편집 91
예약된 아카이브 일시 중지 또는 다시 시작 92
아카이브 작업 수행 93
아카이브 검사 93
보관함 연결 94
아카이브 가져오기 95
이벤트 97
Rapid Recovery 이벤트 97
작업, 경고, 저널을 사용하여 이벤트 보기 97
이메일 알림 이해 100
시스템 이벤트에 대한 알림 그룹, SMTP 설정 및 알림 템플릿 103
알림 그룹 구성 104
반복 감소 구성 정보 106
이벤트 보존 구성 107
신속한 어플라이언스 자동 복구 107
RASR USB 키 만들기 108
RASR 실행 108
Local Mount Utility 109
Local Mount Utility 정보 109
Local Mount Utility에서 Rapid Recovery Core 시스템으로 작업 110
Local Mount Utility에서 보호되는 시스템으로 작업 113
Local Mount Utility 트레이 메뉴 사용 115

3 어플라이언스 관리 116
어플라이언스 상태 모니터링 116
Windows 백업 116
백업 상태 117
Windows 백업 정책 118
저장소 프로비저닝 119
가상 디스크의 공간 할당 삭제 120
복구 및 업데이트 유틸리티 120
어플라이언스 업그레이드 120
어플라이언스 복구 121

4 워크스테이션 및 서버 보호 122
시스템 보호 122
Rapid Recovery로 시스템을 보호하는 방법 122
보호된 시스템 진단 액세스 179

시스템 관리 180
시스템 제거 181
시스템에서 작업 취소 181
시스템에 대한 라이센스 정보 보기 181
VM 내보내기 181
Rapid Recovery에서 가상 시스템으로 내보내기 정보 182
내보내기 관리 193
에이징 데이터 관리 206
Rapid Recovery 데이터 보존 및 아카이브 정보 206
보존 정책 관리 206
복제 211
Rapid Recovery로 복제 211
복구 지점 체인 및 분리 214
복제를 시작하는 경우 215
시딩 요구 및 전략 확인 215
복제된 데이터 전송에 대한 성능 고려 사항 217
자체 관리 대상 Core로 복제 218
수신 및 발신 복제 보기 221
복제 구성 222
타사 대상 Core로 복제 223
기존 복제에 시스템 추가 227
대상 Core에서 시드 드라이브 사용 229
복제 설정 관리 230
복제 제거 237
복제된 데이터 복구 238

5 데이터 복구 240
복구 관리 240
스냅숏 및 복구 지점 240
스냅숏 및 복구 지점 관리 240
보호되는 시스템의 복구 지점 페이지 보기 240
복구 지점 마운트 242
복구 지점 분리 243
Linux 복구 지점 사용 244
스냅숏 작성 246
복구 지점 제거 246
분리된 복구 지점 체인 삭제 247
복구 지점을 다른 리포지토리로 수동 마이그레이션 247
데이터 복원 248
Rapid Recovery를 사용한 데이터 복원 정보 248
Live Recovery 이해 248
복구 지점에서 데이터 복원 249
복구 지점에서 볼륨 복원 249
클러스터 및 클러스터 노드에 대한 복원 수행 252
연결된 아카이브에서 복원 253

Windows 시스템용 Bare Metal Restore 이해 254
Windows 시스템용 Bare Metal Restore 254
Windows 시스템용 부팅 CD 생성 이해 258
BMR용 URC 사용 261
Linux 시스템용 Bare Metal Restore 수행 268
Bare Metal Restore 확인 276

6 보고서 생성 및 보기 280
Rapid Recovery 보고서 정보 280
Core Console에서 보고서 생성 281
Core Console에서 예약된 보고서 관리 284
보고서 메뉴 사용 288
보고서 도구 모음 사용 288
작업 보고서 이해 290
작업 요약 보고서 이해 290
오류 보고서 이해 291
요약 보고서 이해 291
리포지토리 보고서 이해 292
Central Management Console 293
Rapid Recovery Central Management Console 이해 293
Rapid Recovery Central Management Console 구성 294
중앙 관리 콘솔 Core 보고서 이해 297

7 Rapid Recovery Command Line Management 유틸리티 이해 299
명령 300
아카이브 301
CancelActiveJobs 302
CheckRepository 303
CreateArchiveRepository 304
createbootcd 305
CreateRepository 306
DeleteRepository 308
Dismount 308
DismountArchiveRepository 309
EditEsxServer 310
수행 311
ForceAttach 312
ForceChecksum 313
ForceLogTruncation 314
ForceMount 315
ForceReplication 316
ForceRollup 317
ForceVirtualStandby 317
도움말 318
List 319
마운트 321

MountArchiveRepository....322
NewCloudAccount....323
OpenDvmRepository....324
Pause....325
Protect....326
ProtectCluster....327
ProtectEsxServer....328
RemoveAgent....330
RemoveArchiveRepository....330
RemovePoints....331
RemoveScheduledArchive....332
RemoveVirtualStandby....333
Replicate....334
복제....335
RestoreAgent....337
RestoreArchive....338
RestoreUrc....339
Resume....340
SeedDrive....342
StartExport....343
UpdateRepository....345
버전....346
VirtualStandby....347
현지화....349
부록 A: Core Console 참조사항....351
Core Console 사용자 인터페이스 보기....351
단추 모음....352
아이콘 모음....353
왼쪽 탐색 메뉴....355
Protected Machines(보호되는 시스템) 창 보기....357
보호된 시스템에 대한 이벤트 보기....359
보호되는 시스템의 추가 메뉴 보기....361
부록 B: Rapid Recovery PowerShell Module 이해....362
PowerShell을 사용하기 위한 전제 조건....363
powershell.exe.config....363
PowerShell 실행 및 모듈 가져오기....363
명령 및 cmdlet 사용....363
cmdlet 도움말 및 예제 보기....364
Rapid Recovery PowerShell module cmdlet....364
Edit-EsxiVirtualStandby....367
Edit-HyperVVirtualStandby....368
Edit-ScheduledArchive....369
Edit-VBVirtualStandby....371
Edit-VMVirtualStandby....372
Get-ActiveJobs....374

Get-Clusters....375
Get-CompletedJobs....376
Get-ExchangeMailStores....377
Get-Failed....378
Get-FailedJobs....379
Get-Mounts....380
Get-Passed....381
Get-ProtectedServers....381
Get-ProtectionGroups....382
Get-QueuedJobs....383
Get-RecoveryPoints....384
Get-ReplicatedServers....385
Get-Repositories....386
Get-ScheduledArchives....387
Get-SqlDatabases....387
Get-UnprotectedVolumes....388
Get-VirtualizedServers....389
Get-Volumes....390
New-Base....391
New-CloudAccount....392
New-EncryptionKey....393
New-EsxiVirtualStandby....394
New-HyperVVirtualStandby....395
New-Mount....397
Resume-Replication....398
New-Repository....399
New-ScheduledArchive....400
New-Snapshot....402
New-VBVirtualStandby....403
New-VMVirtualStandby....404
Push-Replication....406
Push-Rollup....407
Remove-Agent....408
Remove-Mount....409
Remove-Mounts....409
Remove-RecoveryPoints....410
Remove-Repository....411
Remove-ScheduledArchive....412
Remove-VirtualStandby....413
Resume-Replication....414
Resume-Snapshot....415
Resume- virtualstandby....416
Resume-VMExport....417
Start-Archive....418
Start-AttachabilityCheck....419

Start- checksumcheck....420
Start-EsxiExport....421
Start-HypervExport....422
Start-LogTruncation....424
Start-MountabilityCheck....425
Start-Protect....426
Start-ProtectCluster....427
Start- repositorycheck....428
Start-RestoreArchive....429
Start-ScheduledArchive....430
Start-VBExport....431
Start- virtualstandby....432
Start-VMExport....433
Stop-ActiveJobs....435
Suspend-Replication....436
Suspend- repositoryactivity....437
Suspend-ScheduledArchive....438
Suspend-Snapshot....439
Suspend- virtualstandby....439
Suspend-VMExport....440
Update-Repository....441
현지화....442
한정자....442
부록 C: 스크립트 작성을 사용하여 Rapid Recovery 작업 확장....444
Rapid Recovery에서 PowerShell 스크립트 사용....444
PowerShell 스크립트 작성을 위한 전제 조건....445
powershell.exe.config....445
PowerShell 스크립트 테스트....445
현지화....445
한정자....445
PowerShell 스크립트 작성을 위한 입력 매개 변수....446
AgentProtectionStorageConfiguration(Replay.Common.Contracts.Agents 네임스페이스)....446
AgentTransferConfiguration(Replay.Common.Contracts.Transfer 네임스페이스)....446
BackgroundJobRequest(Replay.Core.Contracts.BackgroundJobs 네임스페이스)....448
ChecksumCheckJobRequest(Replay.Core.Contracts.Exchange.ChecksumChecks 네임스페이스)....448
DatabaseCheckJobRequestBase(Replay.Core.Contracts.Exchange 네임스페이스)....448
ExportJobRequest(Replay.Core.Contracts.Export 네임스페이스)....449
NightlyAttachabilityJobRequest(Replay.Core.Contracts.Sql 네임스페이스)....449
RollupJobRequest(Replay.Core.Contracts.Rollup 네임스페이스)....449
TakeSnapshotResponse(Replay.Agent.Contracts.Transfer 네임스페이스)....450
TransferJobRequest(Replay.Core.Contracts.Transfer 네임스페이스)....450
TransferPrescriptParameter(Replay.Common.Contracts.PowerShellExecution 네임스페이스)....451
TransferPostscriptParameter(Replay.Common.Contracts.PowerShellExecution 네임스페이스)....452
TransferScriptParameterBase(Replay.Common.Contracts.PowerShellExecution 네임스페이스)....454
VirtualMachineLocation(Replay.Common.Contracts.Virtualization 네임스페이스)....454

VolumeImageIdsCollection(Replay.Core.Contracts.RecoveryPoints 네임스페이스)....454
VolumeName(Replay.Common.Contracts.Metadata.Storage 네임스페이스)....454
VolumeNameCollection(Replay.Common.Contracts.Metadata.Storage 네임스페이스)....455
VolumeSnapshotInfo(Replay.Common.Contracts.Transfer 네임스페이스)....455
VolumeSnapshotInfoDictionary(Replay.Common.Contracts.Transfer 네임스페이스)....455
샘플 PowerShell 스크립트....456
PreTransferScript.ps1....456
PostTransferScript.ps1....456
PreExportScript.ps1....457
PostExportScript.ps1....457
PreNightlyJobScript.ps1....458
PostNightlyJobScript.ps1....459
Rapid Recovery에서 Bourne Shell 스크립팅 사용....461
Bourne Shell 스크립트 작성을 위한 전제 조건....461
지원되는 전송 및 사후 전송 스크립트 매개 변수....462
Bourne Shell 스크립트 작성 테스트....462
Bourne Shell 스크립트 작성을 위한 입력 매개 변수....462
TransferPrescriptParameters_VolumeNames....462
TransferPostscriptParameter....463
샘플 Bourne Shell 스크립트....464
PreTransferScript.sh....464
PostTransferScript.sh....464
PostExportScript.sh....465
부록 D: Rapid Recovery API....466
대상 사용자....466
Rapid Recovery REST API로 작업....466
Core 및 Agent API 다운로드 및 보기....466
권장된 추가 문서....468
Dell 정보....469
Dell에 문의하기....469
기술 지원 리소스....469
용어 해설....470

1

DL 어플라이언스 소개

Rapid Recovery 소프트웨어를 사용하는 DL 어플라이언스는 0에 가까운 복구 시간 목표와 복구 지점 목표를 제공하는 백업, 복제 및 복구 솔루션입니다. Rapid Recovery는 데이터 보호, 재난 복구 및 데이터 마이그레이션 및 데이터 관리를 제공합니다. 완전 복구를 유연하게 수행하고(유사 또는 상이한 하드웨어) 출처에 관계없이 실제 또는 가상 시스템에 백업을 복구할 수 있습니다. Rapid Recovery를 사용하면 이중화 및 보안 향상을 위해 하나 이상의 대상으로 복제할 수 있습니다.

어플라이언스는 가상 시스템(VM), 물리적 시스템 및 클라우드 환경을 보호하기 위해 가장 빠르고 안정적인 백업을 위한 단일 솔루션에 백업, 복제 및 복구를 통합함으로써 통합 데이터 보호에 대한 새로운 표준입니다. 어플라이언스는 모든 비공개 또는 공개 클라우드 인프라에 대해 기본 제공되는 글로벌 중복 제거, 압축, 암호화 및 복제 작업에서 최대 페타바이트의 데이터를 처리할 수 있습니다. 서버 응용 프로그램과 데이터는 데이터 보존과 규정 준수를 위해 몇 분만에 복구할 수 있습니다.

어플라이언스는 VMware vSphere 및 Microsoft Hyper-V 개인 및 공용 클라우드에서 멀티 하이퍼바이저 환경을 지원합니다.

Rapid Recovery는 다음 기능을 제공합니다.

- **융통성**. 물리적에서 가상으로, 가상에서 물리적으로, 가상에서 가상으로, 물리적에서 물리적으로 복원을 포함하여 여러 플랫폼에 대해 범용 복구를 수행할 수 있습니다.
- **클라우드 통합**. 독점 및 오픈 소스 플랫폼을 모두 지원하는 클라우드 저장소 벤더를 사용하여 클라우드에 아카이브하고 복제할 수 있습니다.
- **지능형 중복 제거**. 데이터를 한 번 저장하면 그 후에는 이를 참조함으로써 저장소 요구 사항을 줄일 수 있습니다(리포지토리 또는 암호화 도메인당 한 번).
- **인스턴트 복구**. 라이브 복구 기능을 사용하면 먼저 중요한 데이터에 액세스하면서 나머지 복원 작업은 병렬로 완료할 수 있습니다.
- **파일 수준 복구**. 파일 수준 온-프레미스에서 원격 위치 또는 클라우드로부터 데이터를 복구할 수 있습니다.
- **가상 지원**. 가상화에 대한 향상된 지원은 VMware® ESXi™ 5 이상에 대해 에이전트 없는 보호와 자동 검색 및 Microsoft® Hyper-V® 클러스터 공유 볼륨으로 내보내기를 포함합니다.

Rapid Recovery에 대한 자세한 내용은 다음 리소스를 참조하십시오.

- Dell Rapid Recovery 제품 지원 웹 사이트(https://support.software.dell.com/rapid-recovery/)
- 설명서 웹 사이트(https://support.software.dell.com/rapid-recovery/release-notes-guides/ 및 http://www.dell.com/support/home/).

주제:

- 배포 아키텍처
- 제품 기능

배포 아키텍처

어플라이언스는 기업 내에서나 관리 서비스 공급자가 제공하는 서비스로 유연하게 배포되는 확장 가능한 백업 및 복구 제품입니다. 배포 유형은 고객의 규모 및 요구 사항에 따라 다릅니다. 어플라이언스의 배포를 준비하려면 네트워크 저장소 토폴로지, 핵심 하드웨어와 재난 복구 인프라 및 보안을 계획해야 합니다.

배포 아키텍처는 로컬 및 원격 구성요소로 구성됩니다. 오프사이트 복구를 위해 관리 서비스 공급자 또는 재난 복구 사이트를 이용하지 않아도 되는 환경에서는 원격 구성요소가 선택사항입니다. 기본 로컬 배포는 Core라고 하는 백업 서버와 하나 이상의 보호되는 시스템으로 구성됩니다. 오프사이트 구성요소는 DR 사이트에서 전체 복구 기능을 제공하는 복제를 통해 활성화됩니다. Core에서는 기본 이미지 및 증분 스냅샷을 사용하여 보호되는 시스템의 복구 지점을 컴파일합니다.

또한 어플라이언스는 Microsoft Exchange 및 SQL과 각 데이터베이스 및 로그 파일의 유무를 감지하고 포괄적인 보호 및 효과적인 복구를 위해 종속성과 함께 이러한 볼륨을 자동으로 그룹화하므로 응용프로그램 인식형입니다. 따라서 복구를 수행할 때 항상 완전하게 백업할 수 있습니다. 백업은 응용프로그램 인식형 블록 수준 스냅샷을 사용하여 수행됩니다. 또한 어플라이언스가 보호되는 Microsoft Exchange 및 SQL 서버의 로그 자르기를 수행할 수 있습니다.

다음 다이어그램은 간단한 배포를 보여줍니다. 이 다이어그램에서 AppAsure 에이전트 소프트웨어는 파일 서버, 전자 메일 서버, 데이터베이스 서버 등과 같은 시스템이나 가상 시스템에 설치되어 연결되고 중앙 리포지토리로 구성된 단일 Core를 통해 보호됩니다. 라이센스 포털에서는 사용자 환경에서 보호되는 시스템 및 Core의 라이센스 구독, 그룹 및 사용자를 관리합니다. 사용자 환경에 허용된 라이센스에 따라 라이센스 포털을 통해 사용자가 로그인, 계정 활성화, 소프트웨어 다운로드, 보호되는 시스템 및 Core 배포를 수행할 수 있습니다.

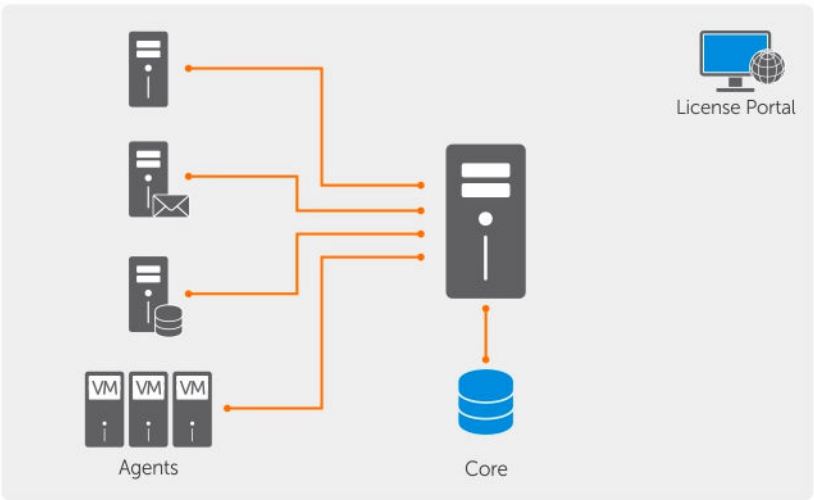


그림 1. 기본 배포 아키텍처

다음 다이어그램에서와 같이 여러 개의 Core를 배포할 수도 있습니다. 중앙 콘솔에서 여러 개의 코어를 관리합니다.

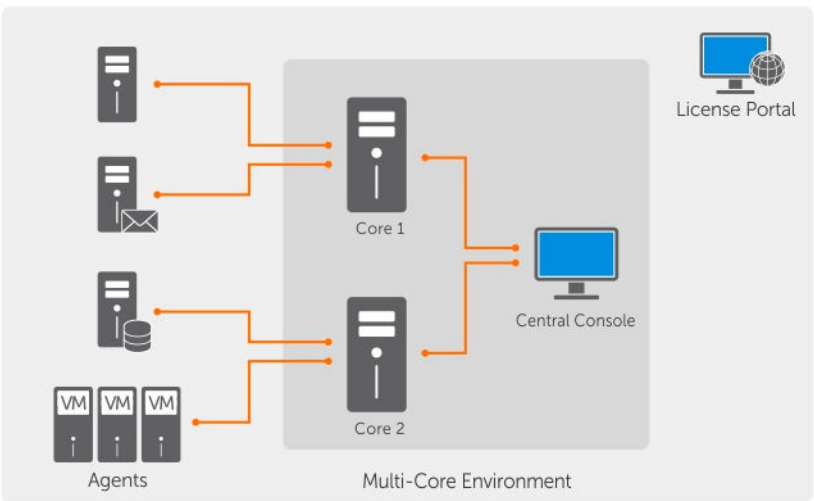


그림 2. 다중 코어 배포 아키텍처

스마트 에이전트

스마트 에이전트는 디스크 볼륨에서 변경된 블록을 추적하고 사전 정의된 보호 간격으로 변경된 블록의 이미지를 스냅합니다. 증분 영구 블록 레벨 스냅샷 접근 방법은 보호되는 시스템에서 Core로 동일한 데이터가 반복적으로 복사되지 않도록 합니다. Rapid Recovery Core에 의해 보호되는 시스템에 Rapid Recovery 스마트 에이전트가 설치됩니다.

스마트 에이전트는 응용프로그램 인식형으로, 설치되어 있는 응용프로그램 유형과 데이터 위치를 감지합니다. 이는 데이터베이스와 같은 종속성과 함께 데이터 볼륨을 자동으로 그룹화한 후 효율적으로 보호하고 빠르게 복구할 수 있도록 함께 로그합니다. Rapid Recovery 에이전트 소프트웨어가 구성되면 스마트 기술을 사용하여 보호된 디스크 볼륨에서 변경된 블록을 계속해서 추적합니다. 스냅샷이 준비되면 지능형 다중 스레드 소켓 기반 연결을 사용하여 Core에 빠르게 전송됩니다. 보호된 시스템에서 CPU 대역폭 및 메모리를 유지하려면 스마트 에이전트가 소스에서 데이터를 암호화하거나 중복 제거하지 않고, 보호되는 시스템이 보호를 위해 Core와 쌍으로 지정됩니다.

DL 어플라이언스 Core

Core는 배포 아키텍처를 중앙 구성 요소입니다. 배포 아키텍처의 중앙 구성요소입니다. Core에서는 모든 시스템 백업을 저장 및 관리하고 백업, 복구 및 보존과 복제, 보관 및 관리를 위한 Core 서비스를 제공합니다. Core는 64비트 의 Microsoft Windows 운영 체제를 실행하는 자체 포함 네트워크 주소 지정 가능 컴퓨터입니다. 어플라이언스에서 대상 기반 인라인 압축, 암호화 및 보호되는 시스템에서 받은 데이터의 데이터 중복 제거를 수행합니다. 그런 다음 Core에서 SAN(저장 영역 네트워크) 및 DAS(직접 연결된 저장소)와 같은 리포지토리에 스냅샷 백업을 저장합니다.

또한 리포지토리가 Core 내의 내부 저장소에 적용될 수 있습니다. 웹 브라우저에서 **https://CORENAME:8006/apprecovery/admin**이라는 URL에 액세스하여 Core를 관리할 수 있습니다. 내부적으로는 REST API를 통해 모든 Core 서비스에 액세스할 수 있습니다. Core 서비스에는 Core 내부에서 액세스하거나 HTTP/HTTPS 요청을 보내고 HTTP/HTTPS 응답을 받을 수 있는 응용프로그램으로부터 인터넷을 통해 직접 액세스할 수 있습니다. 모든 API 작업은 SSL을 통해 수행되고 X.509 v3 인증서를 사용하여 상호 간에 인증됩니다.

Core는 복제를 위해 다른 Core와 쌍으로 지정됩니다.

스냅샷 프로세스

스냅샷은 보호되는 시스템에서 Core로 기본 이미지가 전송될 때입니다. 스냅샷은 데이터를 생성하는 응용프로그램이 사용되고 있는 동안 지정된 시점에 디스크 볼륨의 상태를 캡처하여 저장합니다. Rapid Recovery에서는 스냅샷을 강제로 수행하고, 스냅샷을 일시적으로 일시 중지하고, 리포지토리에 있는 현재 복구 지점의 목록을 보고, 필요에 따라 삭제할 수 있습니다. 복구 지점은 보호되는 시스템을 복원하거나 로컬 파일 시스템을 마운트하는 데 사용됩니다. Rapid Recovery에 의해 수집된 스냅샷은 블록 레벨에서 수행되며 응용프로그램을 인식합니다. 즉, 열려 있는 모든 트랜잭션과 롤링 트랜잭션 로그가 완료되고 스냅샷을 생성하기 전에 캐시가 디스크로 플러시됩니다.

Rapid Recovery에서는 탑재된 볼륨에 연결되는 하위 수준 볼륨 필터 드라이버를 사용하여 다음으로 발생하는 스냅샷에 대한 모든 블록 수준 변경 사항을 추적합니다.Microsoft 볼륨 섀도 서비스(VSS)를 사용하여 응용프로그램 충돌 일치 스냅샷을 쉽게 수행할 수 있습니다.

재난 복구 사이트 또는 서비스 공급자 복제

복제 프로세스를 수행하려면 두 Core 간에 소스-대상 쌍으로 지정된 관계가 필요합니다. 소스 Core는 보호되는 시스템의 복구 지점을 복사하고, 이를 원격 재난 복구 사이트의 대상 Core에 비동기적으로 지속적으로 전송합니다. 오프사이트 위치는 회사 소유 데이터 센터(자체 관리 Core) 또는 타사 관리 서비스 공급자(MSP)의 위치나 클라우드 환경일 수 있습니다. MSP에 복제할 때 연결을 요청하고 자동 피드백 알림을 받을 수 있는 기본 제공 워크플로를 사용할 수 있습니다. 데이터를 처음 전송할 때 외부 미디어를 사용하여 데이터 시드를 수행할 수 있으며, 이는 일반적으로 링크 속도가 느린 대규모 데이터 세트 또는 사이트에 유용합니다.

심각한 정전이 발생한 경우 어플라이언스가 복제 환경에서 장애 조치와 장애 복구를 지원합니다. 포괄적인 정전이 발생한 경우에는 보조 사이트에 있는 대상 Core가 복제된 보호되는 시스템에서 인스턴스를 복구하고 장애 조치된 시스템에서 즉시 보호를 시작합니다. 기본 사이트가 복원되면 복제된 Core가 데이터를 복구된 인스턴스에서 기본 사이트의 보호되는 시스템으로 다시 장애 복구할 수 있습니다.

복구

로컬 사이트 또는 복제된 원격 사이트에서 복구를 수행할 수 있습니다. 로컬 보호 및 선택적 복제와 함께 배포가 안정적인 상태가 되면 Core를 통해 검증된 복구, 범용 복구 또는 라이브 복구를 사용하여 복구를 수행할 수 있습니다.

제품 기능

다음 특징 및 기능을 통해 중요한 데이터의 보호 및 복구를 관리할 수 있습니다.

- 리포지토리
- Rapid Recovery에서 중복 제거
- 암호화
- 복제
- 보존 및 보관
- 가상화 및 클라우드
- 경고 및 이벤트 관리
- 라이센스 포털
- 웹 콘솔
- 서비스 관리 API

리포지토리 이해

리포지토리는 보호된 워크스테이션 및 서버에서 캡처한 백업 스냅샷 데이터가 저장되고 관리되는 중앙 위치입니다. 데이터는 복구 지점의 형태의 리포지토리에 저장됩니다.

리포지토리는 SAN(Storage Area Network), DAS(Direct Attached Storage), NAS(network Attached Storage)를 포함하여 여러 저장소 기술을 이용할 수 있습니다.

노트: 기본 저장소 장치에 Rapid Recovery Core를 위한 리포지토리를 저장합니다. 저장소 볼륨의 속도는 가장 중요한 요소입니다. 데이터 도메인과 같은 보관 저장소 장치는 성능 제한 때문에 지원되지 않습니다. 마찬가지로 이러한 장치를 기본 저장소로 사용하는 경우 성능 제한이 발생할 가능성이 있으므로 클라우드에 계층화되는 NAS 필러에 리포지토리를 저장하지 마십시오.

DAS는 가장 높은 데이터 대역폭과 가장 빠른 액세스 속도를 제공합니다. 최적의 결과를 위해 RAID 6 저장소를 포함한 DAS를 사용하십시오. 자세한 내용은 Dell 기술 자료 문서 118153, "리포지토리 옵션: DAS(Direct Attached Storage), SAN(Storage Area Network) 또는 NAS(network Attached Storage)."

리포지토리의 저장소 위치는 항상 사용자가 지정하는 하위 디렉터리여야 합니다(예: **E:\Repository**). 볼륨의 루트 디렉터리(예: **E:**)는 절대 사용하지 마십시오.

Rapid Recovery 리포지토리 형식은 DVM(Deduplication Volume Manager)을 사용합니다. DVM 리포지토리는 여러 볼륨, 단일 Core에서 최대 255개 리포지토리를 지원하며 익스텐트를 사용할 수 있습니다. Windows 운영 체제를 사용하는 시스템에만 DVM 리포지토리를 생성할 수 있습니다. Rapid Recovery를 새로 설치하는 경우 이 리포지토리 유형을 사용할 수 있습니다. 생성할 때 DVM 리포지토리의 크기를 지정할 수 있으며 나중에 익스텐트를 추가할 수 있습니다.

DVM 리포지토리 기능 및 특성은 다음과 같습니다.

- Rapid Recovery 6.x 아카이브 및 복구 지점에서 복구 지원
- Windows OS에서만 저장소 위치를 지원합니다. 리포지토리 볼륨은 로컬(Core 서버에 연결된 저장소) 또는 일반 인터넷 파일 시스템(CIFS) 공유 위치에 있는 저장소 위치가 될 수 있습니다.
- 지원되는 저장소 유형은 SAN(Storage Area Network), DAS(Direct Attached Storage) 또는 NAS(network Attached Storage)를 포함합니다.
- 8GB RAM이 필요하며 가급적이면 메모리 오류 검사 및 수정(ECC)을 선호합니다.
- Core 시스템에는 쿼드 코어 프로세서가 필요합니다(이 장기적인 요구 사항은 지금 적용됨).
- 호스트당 여러 개의 DVM 리포지토리를 지원합니다
- 추가 서비스가 필요하지 않습니다. DVM 리포지토리는 Core와의 통신 및 이벤트 추적을 위해 기본 Core 서비스를 사용합니다
- 각 DVM 리포지토리는 최대 4096 리포지토리 익스텐트(저장소 위치라고도 함)를 지원합니다.
- 고정된 크기의 DVM 리포지토리는 볼륨에 리포지토리 크기를 지정해야 합니다. 지정하는 크기는 볼륨 크기를 초과할 수 없습니다. 저장소 위치로 정의하는 각 볼륨에는 최소 1GB의 여유 공간이 있어야 합니다.
- 리포지토리 저장소 위치는 단순 또는 동적 디스크가 될 수 있으며 속도가 가장 중요한 요소입니다.
- Core 콘솔에서 표준 암호화 키를 생성하고 관리할 수 있습니다(Core 기반 암호화)
- 전체 리포지토리(또는 암호화 키가 사용되는 경우 각 리포지토리 내의 암호화 도메인)에서 데이터 중복을 제거합니다
- Core 설정에서 저장소 위치를 구성 가능한 전용의 크기 조정이 가능한 DVM 중복 제거 캐시를 사용합니다.
- Core에 데이터 쓰기, 로컬 리포지토리에 스냅샷 데이터를 저장하기에 최적화되었으며, 모든 데이터가 Core를 통해 처리됩니다.
- 생성 후에는 이름을 바꿀 수 없습니다
- 이런 유형의 새 리포지토리는 REST API, Rapid Recovery 명령줄 관리 유틸리티(cmdutil.exe) 또는 Windows PowerShell® cmdlet를 사용하여 생성할 수 있습니다.

DVM 리포지토리를 생성하면 Rapid Recovery Core는 지정된 위치에 데이터 및 메타데이터에 필요한 저장 공간을 미리 할당합니다. 최소 DVM 리포지토리 크기는 1GB이며, 일반적으로 테스트를 제외하고는 실제로 사용하기에는 너무 적습니다.

DVM 중복 제거는 기본 및 보조 캐시가 필요하므로 예약된 저장 공간이 중복 제거 캐시 크기의 두 배가 되어야 합니다. 예를 들어, Core에서 DVM 중복 제거 캐시 설정에 1.5GB가 예약된 경우 캐시 볼륨에는 3GB가 필요합니다. 캐시의 기본 설치 경로는 C 드라이브에 있습니다. 자세한 내용은 중복 제거 캐시 및 저장 위치 이해을(를) 참조하십시오.

단일 Core와 연관된 여러 독립 리포지토리를 최대 255 DVM 리포지토리까지 생성할 수 있습니다. 리포지토리는 여러 저장소 기술을 적용할 수 있습니다.

새 파일 익스텐트 또는 사양을 추가하여 DVM 리포지토리의 크기를 더 늘릴 수 있습니다. 확장된 리포지토리는 여러 저장소 기술이 적용되며 최대 4096개까지 포함할 수 있습니다.

DVM 리포지토리로 작업하는 자세한 내용은 DVM 리포지토리 관리을(를) 참조하십시오.

Rapid Recovery에서 중복 제거

중복 제거는 저장소 요구 사항과 네트워크 로드 모두를 줄일 수 있는 데이터 압축 기술입니다. 이 프로세스에서는 디스크에 데이터의 고유 블록을 실제로 한 번만 저장합니다. Rapid Recovery에서 고유 데이터 블록이 리포지토리에서 다시 나타나면 데이터를 다시 저장하는 대신, 데이터에 대한 가상 참조를 저장합니다.

중복 제거는 Rapid Recovery Core에서 캡처한 백업 스냅숏에서 수행됩니다. 백업 정보는 단일 리포지토리에서 중복 제거됩니다. 여러 리포지토리에서 중복 제거할 수 없습니다.

Rapid Recovery 릴리스 6.0.2에서는 모든 DVM 리포지토리에 대해 대상 기반 중복 제거를 사용합니다. 이 모델에서 정보는 DVM 리포지토리(대상)로 전송된 후 리포지토리에서 중복 제거됩니다.

대부분의 경우 중복 제거는 백업 정보 전송 중에 인라인으로 수행됩니다.

이제 Rapid Recovery는 최대 효율을 위해 사후 처리로 수행되는 중복 제거도 제공합니다. 이러한 사후 처리를 통과 중복 제거라고도 합니다. 이 모델을 사용하면 리포지토리의 데이터를 DVM 데이터 캐시의 참조와 비교합니다. 리포지토리의 데이터 블록을 이미 저장한 경우 해당 데이터가 추가로 나타날 때마다 데이터에 대한 참조나 포인터로 바뀝니다.

이 사후 처리는 특히, 중복 제거 캐시가 모두 찬 후 추가 중복 제거를 위해 캐시가 크게 늘어난 경우에 리포지토리 저장소 공간을 절약할 수 있습니다. 이러한 중복 제거는 리포지토리 최적화 작업을 수행할 때 나타납니다. 이 기능은 DVM 리포지토리에 고유하며, 중복 제거 블록 확보라고도 합니다.

리포지토리 최적화 작업에 대한 자세한 내용은 리포지토리 최적화 작업 설명를 참조하십시오. 이 작업 수행에 대한 자세한 내용은 DVM 리포지토리 최적화를 참조하십시오.

이와 같이 Rapid Recovery는 여기에서 설명한 대상 기반 중복 제거, 인라인 중복 제거, 사후 처리 중복 제거와 같은 모든 종류의 중복 제거를 사용합니다.

DVM 리포지토리에 고유 블록에 대한 참조를 저장하는 방법에 대한 자세한 내용은 중복 제거 캐시 및 저장 위치 이해를 참조하십시오.

암호화 키 이해

Rapid Recovery Core는 Core 콘솔에서 정의하고 관리하는 암호화 키를 사용하여 모든 리포지토리 내에 있는 모든 볼륨에 대한 스냅샷 데이터를 암호화할 수 있습니다.

전체 리포지토리를 암호화하는 대신 Rapid Recovery를 사용하면 단일 Rapid Recovery Core에서 보호되는 하나 이상의 시스템에 대한 암호화 키를 지정할 수 있습니다. 각 활성 암호화 키는 암호화 도메인을 생성합니다. Core에 생성할 수 있는 암호화 키의 수는 제한이 없습니다.

다중 테넌트 환경(단일 Core가 여러 암호화 도메인을 호스팅하는 경우)에서는 각 암호화 도메인 내에서 데이터가 파티션화되고 중복 제거됩니다. 따라서 여러 보호되는 시스템 간에 중복 제거의 이점을 최대화하려는 경우 여러 보호되는 시스템에 대해 단일 암호화 키를 사용하는 것이 좋습니다.

3가지 방법 중 하나를 사용하여 Core 간에 암호화 키를 공유할 수도 있습니다. 한 가지 방법은 하나의 Rapid Recovery Core에서 암호화 키를 파일로 내보내고 다른 Core로 가져오는 것입니다. 두 번째 방법은 암호화 키를 사용하여 데이터를 보관한 다음 다른 Rapid Recovery Core로 보관한 데이터를 가져오는 것입니다. 세 번째 방법은 보호되는 시스템에서 암호화 키를 사용하여 복구 지점을 복제하는 것입니다. 보호되는 시스템을 복제한 후 소스 Core에서 사용된 암호화 키는 대상 Core에서 복제된 암호화 키로 나타납니다.

모든 경우에 가져온 후 모든 암호화 키는 Core에 잠금 상태로 나타납니다. 잠긴 암호화 키에서 데이터에 액세스하려면 잠금을 해제해야 합니다. 암호화 키 가져오기, 내보내기, 잠금 또는 잠금 해제에 대한 자세한 내용은 암호화 키 관리 항목을 참조하십시오.

키 보안 개념 및 고려 사항은 다음과 같습니다.

- 암호화는 SHA-3과 호환되는 CBC(Cipher Block Chaining) 모드에서 256비트 AES(Advanced Encryption Standard)를 사용하여 수행됩니다.
- 암호화 도메인 내에서 중복 제거가 작동하여 개인 정보를 보장합니다.
- 암호화는 성능에 영향을 미치지 않고 수행됩니다.
- 많은 보호되는 시스템에 단일 암호화 키를 적용할 수 있지만 모든 보호되는 시스템은 한 번에 한 암호화 키만 적용할 수 있습니다.
- Rapid Recovery Core에 구성된 암호화 키를 추가, 제거, 가져오기, 내보내기, 수정 및 삭제할 수 있습니다.

△ 주의: **Rapid Recovery는 보호되는 시스템에 암호화 키를 적용할 때마다 새 스냅샷을 생성합니다. 새 스냅샷은 보호되는 시스템에 대한 암호화 키를 분리한 후에도 트리거됩니다.**

Rapid Recovery Core에서 생성되는 암호화 키는 다음 표에 설명되어 있는 대로 4개의 매개변수가 포함되어 있는 텍스트 파일입니다.

표 1. 암호화 키의 구성 요소

구성 요소	설명
이름	이 값은 Rapid Recovery Core 콘솔에서 키를 추가할 때 지정한 이름과 동일합니다.
키	이 매개변수는 107자의 임의로 생성되는 영어 알파벳, 숫자 및 수학 연산자 문자로 구성됩니다.
ID	키 ID는 26자의 임의로 생성되는 대문자와 소문자로 구성됩니다.
주석	설명은 키를 생성할 때 입력한 키 설명 텍스트를 포함하고 있습니다.

Rapid Recovery로 복제

이 섹션은 Rapid Recovery에서 복제를 이해하고 구성하는 데 도움이 되는 개념 및 절차 정보를 제공합니다.

복제는 재해 복구를 위해 Rapid Recovery Core에서 복구 지점을 복사하여 다른 Rapid Recovery Core로 전송하는 프로세스입니다. 이러한 프로세스를 수행하려면 두 개 이상의 Core 간 관계가 소스-대상 쌍으로 지정되어 있어야 합니다.

소스 Core는 선택한 보호된 시스템의 복구 지점을 복사한 다음, 해당 스냅숏 데이터를 대상 Core에 비동기적으로 지속해서 전송합니다.

복제 일정을 설정하여 기본 동작을 변경하는 경우를 제외하고 Core는 모든 백업 스냅숏, 체크섬 검사, 연결 기능 검사 및 야간 작업 완료 후 즉시, 복제 작업을 시작합니다. 자세한 내용은 복제 일정 설정을(를) 참조하십시오.

최적의 데이터 보안을 위해 관리자들은 일반적으로 원격 재해 복구 사이트에서 대상 Core를 사용합니다. 회사 소유의 데이터 센터나 원격 재해 복구 사이트(즉, "자체 관리된" 대상 Core)에 아웃바운드 복제를 구성할 수 있습니다. 또는 오프사이트 백업 및 재해 복구 서비스를 호스팅하는 타사의 관리된 서비스 공급자(MSP) 또는 클라우드 공급자에 아웃바운드 복제를 구성할 수 있습니다. 타사 대상 Core에 복제할 때 연결을 요청하고 자동 피드백 알림을 수신할 수 있는 기본 워크플로를 사용할 수 있습니다.

복제는 보호된 시스템을 기준으로 관리됩니다. 소스 Core에서 보호되거나 복제된 시스템(또는 모든 시스템)은 대상 Core로 복제되도록 구성할 수 있습니다.

가능한 복제 시나리오는 다음과 같습니다.

- **로컬 위치에 복사**. 대상 Core가 로컬 데이터 센터 또는 온사이트 위치에 있으며 복제가 항상 유지 관리됩니다. 이 구성에서는 Core가 손실되어도 복구가 차단되지 않습니다.
- **오프사이트 위치에 복제**. 대상 Core가 손실 발생 시 복구를 위해 오프사이트 재해 복구 시설에 위치합니다.
- **상호 복제**. 서로 다른 위치에 있는 두 개의 데이터 센터가 Core를 포함하고 시스템을 보호하며 각 데이터 센터가 오프사이트 재해 복구 백업의 역할을 합니다. 이 시나리오에서는 각 Core가 다른 데이터 센터에 위치한 Core에 보호된 시스템을 복제합니다.
- **호스트 및 클라우드 복제**. Rapid Recovery MSP 파트너가 데이터 센터 또는 공용 클라우드에서 여러 대상 Core를 유지 관리합니다. 이러한 각 Core에서 MSP 파트너를 통해 한 명 이상의 고객이 고객의 사이트에 있는 소스 Core에서 MSP의 대상 Core로 복구 지점을 유료로 복제할 수 있습니다.

노트: 이 시나리오에서는 고객이 소유한 데이터에만 액세스할 수 있습니다.

가능한 복제 구성은 다음과 같습니다.

- **지점 간 복제**. 하나 이상의 보호된 시스템을 단일 소스 Core에서 단일 대상 Core로 복제합니다.

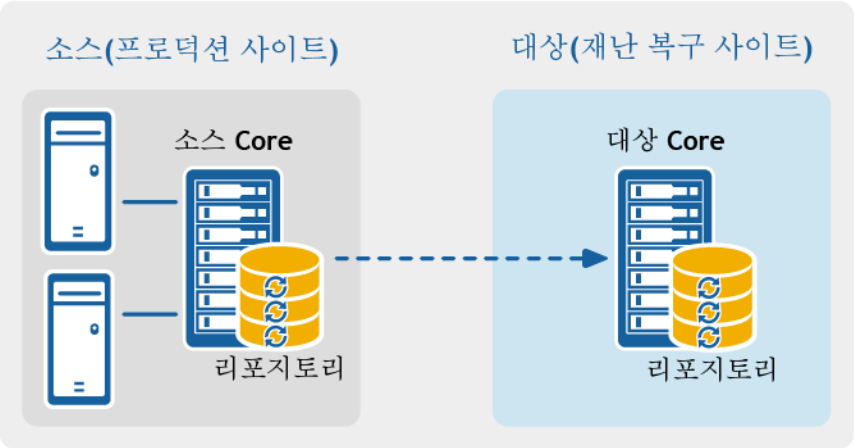


그림 3. 지점 간 복제 구성

- **다중 지점-지점 간 복제.** 보호된 시스템을 다중 소스 Core에서 단일 대상 Core로 복제합니다.

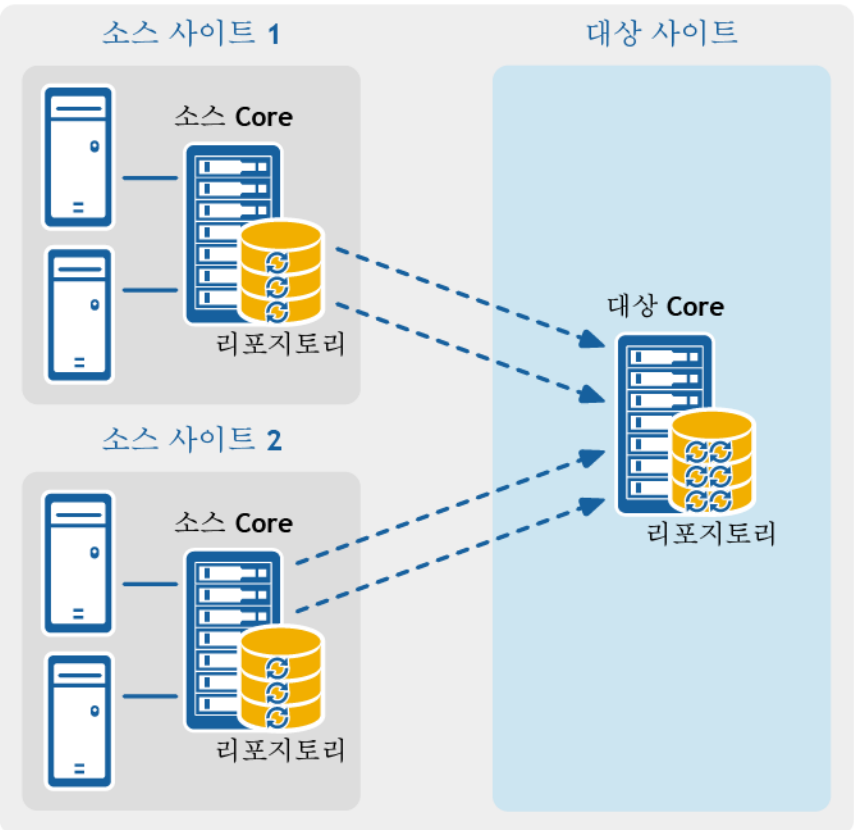


그림 4. 다중 지점-지점 간 복제 구성

- **지점-다중 지점 간 복제**. 하나 이상의 보호된 시스템을 단일 소스 Core에서 두 개 이상의 대상 Core로 복제합니다.

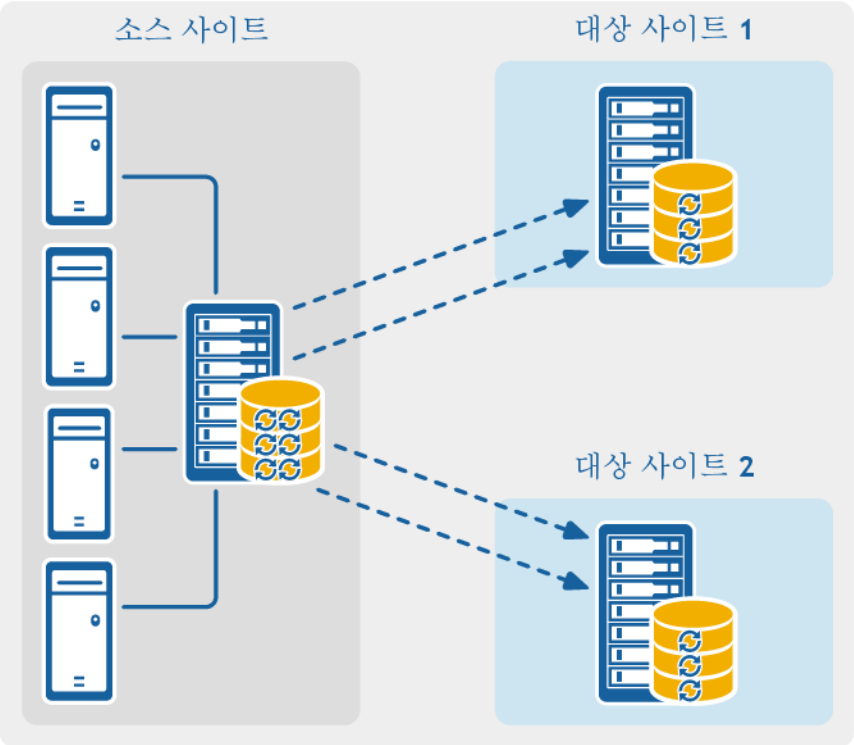


그림 5. 지점-다중 지점 간 복제 구성

- **멀티홉 복제**. 하나 이상의 보호된 시스템을 하나의 대상 Core에서 다장른 대상 Core로 복제하여 복제된 Core에서 추가적인 장애 조치 또는 복구 옵션을 생성합니다.

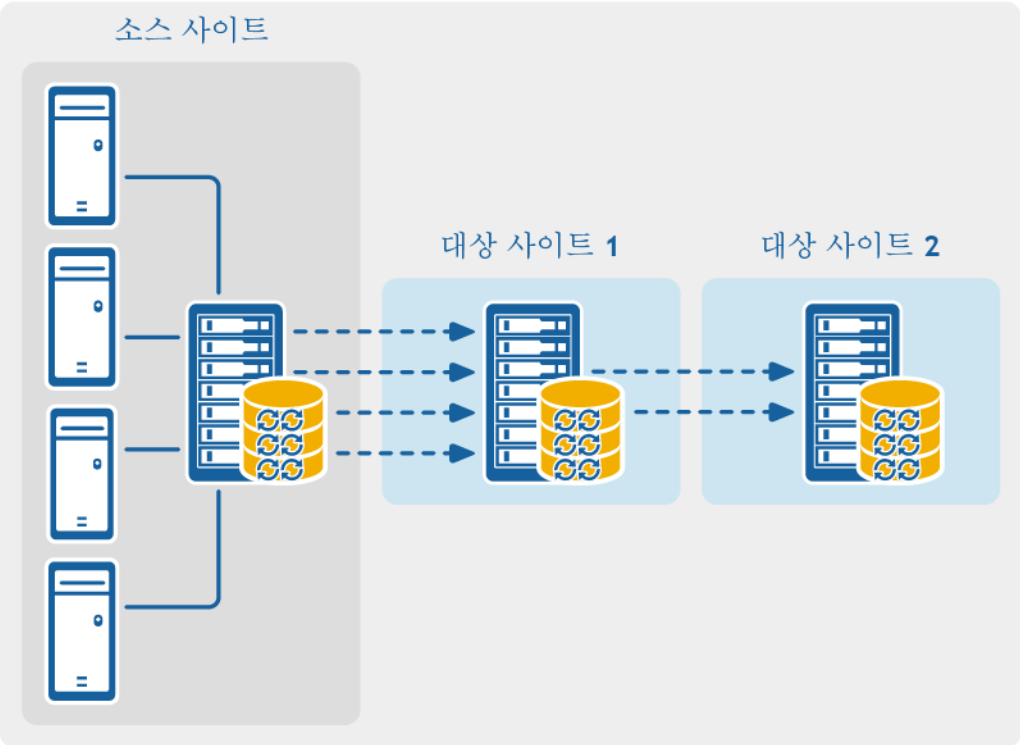


그림 6 . 멀티홉 복제 구성

DL1x00 또는 DI4x00 등의 Dell Data Protection 백업 어플라이언스를 사용할 경우 복제하는 대상 Core에는 유효한 소프트웨어 라이센스가 구성되어 있어야 합니다. 이러한 하드웨어 어플라이언스에는 구매 시 복제 대상 라이센스가 포함되어 있습니다. 어플라이언스 구매 시 사용자가 받은 환영 이메일 메시지에서 라이센스 키를 확인하십시오. 지원을 받으려면 Licensing Assistance 웹 사이트 (https://support.software.dell.com/licensing-assistance)에 방문하거나 license@software.dell.com으로 이메일을 보내 주십시오.

보존 및 아카이빙

어플라이언스에서는 백업 및 보존 정책이 유연하게 적용되므로 쉽게 구성할 수 있습니다. 조직의 필요에 맞게 보존 정책을 조정할 수 있어 호환성 요구 사항을 충족시킬 수 있으며 RTO에 대해 타협할 필요가 없습니다.

보존 정책은 속도가 빠르고 고가인 단기 미디어에 백업이 저장되는 기간을 지정합니다. 경우에 따라 특정 비즈니스 및 기술 요구 사항으로 인해 이러한 백업의 보존 기간이 연장되지만 빠른 저장소를 사용하려면 비용이 매우 많이 듭니다. 따라서 이러한 경우 속도가 느리지만 저렴한 장기간용 저장소를 사용해야 합니다. 비즈니스에서는 주로 호환 및 비호환 데이터를 모두 보관하기 위해 장기간용 저장소를 사용합니다. 아카이브 기능은 호환 및 비호환 데이터에 대한 연장 보존을 지원하며 복제 데이터를 대상 Core에 시드하는 데 사용됩니다.

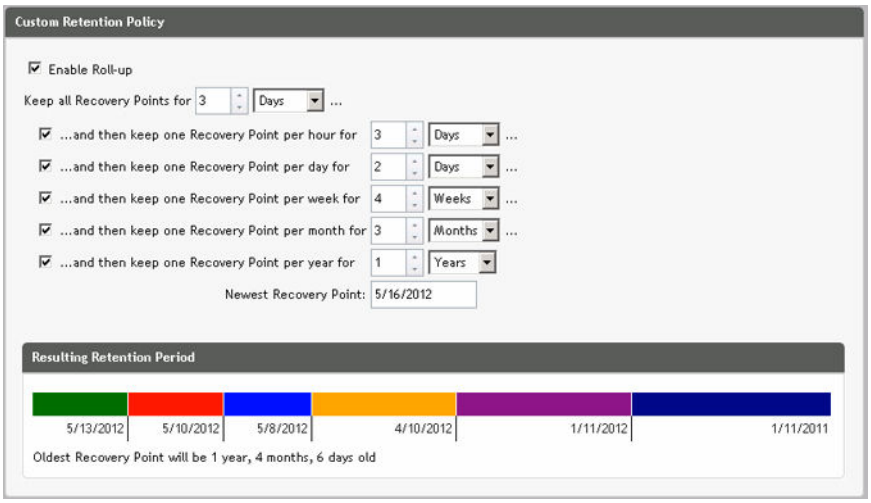


그림 7. 사용자 지정 보존 정책

어플라이언스에서는 보존 정책을 사용자 지정하여 백업 복구 지점이 유지되는 기간을 지정할 수 있습니다. 복구 지점의 기간에 따라 해당 보존 기간이 점차 줄어들게 되므로 복구 지점 기간이 지나면 보존 풀에서 제거됩니다. 일반적으로 이 프로세스는 비효율적이므로 데이터 양과 보존 기간이 빠르게 증가하기 시작하면서 결국 사용되지 않고 있습니다. 어플라이언스는 복합 보존 정책을 사용하여 대량 데이터의 보존을 관리하고 효율적인 메타데이터 작업을 통해 기간이 오래된 데이터에 대한 롤업 작업을 수행함으로써 대규모 데이터 문제를 해결합니다.

백업은 몇 분 간격으로 수행할 수 있습니다. 이러한 백업 기간은 일, 월 및 년에 따라 경과되므로 보존 정책에 따라 오래된 백업의 기간 및 삭제가 관리되고, 단순한 폭포수 방식을 통해 에이징 프로세스가 정의됩니다. 폭포 내의 수준은 분, 시간, 일, 주, 월 및 년 단위로 정의됩니다. 야간 롤업 프로세스에는 보존 정책이 강제로 적용됩니다.

장기간 보관할 수 있도록 어플라이언스에서는 이동식 미디어에 소스 또는 대상 Core의 아카이브를 생성할 수 있는 기능을 제공합니다. 아카이브는 내부적으로 최적화되고, 아카이브에 포함된 모든 데이터는 압축, 암호화 및 중복 제거됩니다. 아카이브의 전체 크기가 이동식 미디어에서 사용 가능한 공간보다 큰 경우 미디어에서 사용 가능한 공간을 기반으로 아카이브가 여러 장치에 적용됩니다. 또한 암호를 사용하여 아카이브를 잠글 수도 있습니다. 아카이브에서 복구하는 경우 새 Core가 필요하지 않으며, 관리자가 암호 및 암호화 키를 알고 있는 경우 Core에서 아카이브를 수집하고 데이터를 복구할 수 있습니다.

가상화 및 클라우드

Core에서는 클라우드를 사용할 수 있으며, 이를 통해 복구할 때 클라우드의 계산 용량을 이용할 수 있습니다.

어플라이언스에서 라이센스를 받은 VMware 또는 Hyper-V 등과 같은 가상 시스템에 보호되는 시스템 또는 복제된 시스템을 내보낼 수 있습니다. 한 번 가상 내보내기를 수행하거나 지속적인 가상 내보내기를 설정하여 가상 대기 VM을 설정할 수 있습니다. 지속적 내보내기에서는, 모든 스냅샷이 생성된 후에 가상 시스템이 증분적으로 업데이트됩니다. 증분 업데이트는 매우 빠르며 한 번의 단추 클릭으로 사용할 수 있는 대기 클론을 제공합니다. 지원되는 가상 시스템 내보내기 유형은 폴더의 VMware 워크스테이션/서버, vSphere/VMware ESX(i) 호스트에 직접 내보내기, Oracle VirtualBox에 내보내기와 Windows Server 2008(x64), 2008 R2, 2012(x64) 및 2012 R2(Hyper-V 2세대 VM 지원 포함)에서 Microsoft Hyper-V Server에 내보내기가 있습니다.

또한 Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage 또는 기타 OpenStack 기반의 클라우드 서비스를 사용하여 리포지토리 데이터를 클라우드에 아카이브할 수 있습니다.

경고 및 이벤트 관리

HTTP REST API 외에도 어플라이언스에는 전자 메일, 시스템 로그 또는 Windows 이벤트 로그를 사용하여 이벤트 로깅과 알림을 위한 광범위한 기능 집합이 포함되어 있습니다. 전자 메일 알림을 사용하여 사용자 또는 그룹에게 경고에 대한 응답으로 상태 또는 다른 이

벤트에 대한 상태를 알릴 수 있습니다. 시스템 로그와 Windows 이벤트 로그 방법은 다중 운영 체제 환경에서 리포지토리에 대한 중앙 로깅에 사용되며, Windows 전용 환경에서는 Windows 이벤트 로그만 사용됩니다.

라이센스 포털

라이센스 포털에서는 라이센스 자격을 관리할 수 있도록 쉽게 사용할 수 있는 도구를 제공합니다. 이를 통해 라이센스 키를 다운로드, 활성화, 보기 및 관리할 수 있으며 회사 프로필을 생성하여 라이센스 자산을 추적할 수 있으며, 포털에서 서비스 공급자 및 재판매 사업자가 해당 고객 라이센스를 추적하고 관리할 수도 있습니다.

웹 콘솔

어플라이언스에는 하나의 중앙 위치에서 분산된 Core를 관리하는 새로운 웹 기반 중앙 콘솔이 포함되어 있습니다. 분산 Core가 여러 개 있는 기업 고객과 MSP가 중앙 관리를 위한 통합 보기를 가져올 수 있도록 중앙 콘솔을 배포할 수 있습니다. 중앙 콘솔에서는 계층적 조직 구성 단위로 관리 Core를 구성할 수 있습니다. 이러한 조직 구성 단위는 사업부, 위치 또는 역할 기반 액세스 권한이 있는 MSP의 고객을 나타냅니다. 또한 중앙 콘솔에서 관리 Core 전반의 보고서를 실행할 수 있습니다.

서비스 관리 API

어플라이언스는 서비스 관리 API와 함께 제공되며, 중앙 관리 콘솔을 통해 사용 가능한 모든 기능에 프로그래밍 방식으로 액세스할 수 있는 권한을 제공합니다. 서비스 관리 API는 REST API입니다. 모든 API 작업은 SSL을 통해 수행되며 X.509 v3 인증서를 사용하여 상호 간에 인증됩니다. HTTPS 요청 및 응답을 보내고 받을 수 있는 응용프로그램에서 인터넷을 통해 직접 또는 환경 내에서 관리 서비스에 액세스할 수 있습니다. 이러한 방법을 통해 관계 관리 방법론(RMM) 도구 또는 대금 청구 시스템과 같은 웹 응용프로그램과 쉽게 통합할 수 있습니다. 또한 PowerShell 스크립팅에 대한 SDK 클라이언트도 포함되어 있습니다.

2

DL Appliance Core 작업

Rapid Recovery Core Console 이해

이 장에서는 Rapid Recovery Core Console 사용자 인터페이스(UI)의 다양한 요소를 설명합니다.

Rapid Recovery Core Console 액세스

Rapid Recovery Core Console에 액세스하려면 다음 단계를 완료하십시오.

- Rapid Recovery Core Console에 액세스하려면 다음 작업 중 하나를 수행하십시오.
  a Rapid Recovery Core 서버에 로컬로 로그온하고 Core Console 아이콘을 두 번 클릭합니다.
  b 또는 다음 URL 중 하나를 웹 브라우저에 입력합니다.
    - https://<yourCoreServerName>:8006/apprecovery/admin/ 또는
    - https://<yourCoreServerIPaddress>:8006/apprecovery/admin/

노트: Rapid Recovery Core Console UI는 JavaScript에 종속적이므로, Core Console에 액세스하기 위해 사용하는 웹 브라우저에는 JavaScript가 활성화되어 있어야 합니다.

Rapid Recovery 서비스의 기본 포트를 변경한 경우 위 URL의 포트를 그에 따라 업데이트하십시오.

빠른 시작 안내서 이해

빠른 시작 안내서는 Rapid Recovery Core의 구성 및 사용을 위해 권장되는 작업을 단계별로 안내하는 기능입니다.

Rapid Recovery Core를 처음 업그레이드하거나 설치하고 Core Console로 이동하면 빠른 시작 안내서가 자동으로 나타납니다. 제안된 여러 구성 작업을 보려면 이 안내서의 **시작** 페이지에서 **시작 안내서**를 클릭하십시오. **단계 건너뛰기** 및 **뒤로** 옵션을 사용하여 안내서를 탐색하십시오. 제안된 마지막 작업을 본 후에는 **마침**을 클릭하여 안내서를 닫으십시오.

Core Console의 도움말 메뉴에서 빠른 시작 안내서를 언제든지 다시 시작할 수 있습니다. 빠른 시작 안내서의 **시작** 페이지를 숨길 수도 있습니다.

빠른 시작 안내서를 숨기지 않을 경우 Rapid Recovery Core Console에 로그인하고 **홈** 페이지에 액세스할 때마다 빠른 시작 안내서가 다시 나타납니다. 자세한 내용은 빠른 시작 안내서 숨기기을(를) 참조하십시오.

안내서에서 제안한 단계를 수행할 필요는 없습니다. 제안된 작업을 확인한 후 **단계 건너뛰기** 및 **뒤로** 옵션을 사용하여 탐색할 수 있습니다. 이 안내서를 숨기려면 **안내서 종료**를 클릭할 수 있습니다.

빠른 시작 안내서에서 제안된 구성 작업을 수행하기로 선택하는 경우 안내서의 단계에 표시된 메시지를 따르십시오. 사용자 인터페이스에 적절한 마법사 또는 관련 영역이 표시됩니다. 안내서에서 제안된 각 작업을 완료하기 위한 절차는 아래 표와 같이 이 문서에 설명되어 있습니다.

노트: 빠른 시작 안내서에서 제안된 모든 구성 작업이 모든 사용자에게 필요한 것은 아닙니다. 특정 요구에 대해 어떤 작업을 수행할 것인지 알아야 합니다.

빠른 시작 안내서에는 다음과 같은 구성 작업이 설명되어 있습니다.

표 2. 빠른 시작 안내서 구성 작업

기능	간략한 설명	작업 선택의 결과, 절차에 대한 연결
보호	단일 시스템 보호, 서버 클러스터 보호 또는 대량 보호를 사용하여 여러 시스템 보호	드롭다운 메뉴에서 보호를 클릭하거나 **시스템 보호**를 선택하여 시스템 보호 마법사를 엽니다. 시스템 보호 마법사를 완료하는 방법에 대한 내용은 시스템 보호을(를) 참조하십시오. 드롭다운 메뉴에서 **클러스터 보호**를 선택하여 클러스터에 연결 대화 상자를 엽니다. 클러스터를 보호하는 방법에 대한 자세한 내용은 클러스터 보호을(를) 참조하십시오. 드롭다운 메뉴에서 **대량 보호**를 선택하여 다중 시스템 보호 마법사를 엽니다. 다중 시스템 보호 마법사를 완료하는 방법에 대한 내용은 다중 시스템 보호 정보을(를) 참조하십시오.
복제	기본(원본) Core에서 보조(대상) Core로 복제 설정	**복제**를 클릭하여 복제 페이지를 엽니다. 복제 마법사를 사용하여 대상 Core를 추가하라는 메시지가 표시됩니다. 복제 마법사를 사용하여 자체 관리된 Core에서 복제를 설정하는 방법에 대한 내용은 자체 관리 대상 Core로 복제을(를) 참조하십시오. 복제에 대한 일반적인 내용은 복제 구성을(를) 참조하십시오.
가상 내보내기	보호된 시스템에서 가상 시스템으로 한 번 내보내기 수행 또는 연속 내보내기 설정	**내보내기**를 클릭하여 보호된 시스템에서 가상 시스템으로 데이터 내보내기를 수행합니다. VM으로 한 번 내보내기를 수행하거나 연속 내보내기를 위한 가상 대기를 설정할 수 있습니다. 가상 내보내기에 대한 내용은 Rapid Recovery에서 가상 시스템으로 내보내기 정보을(를) 참조하십시오.
구성	Rapid Recovery Core에 대한 추가 구성 설정 허용	**자세히**를 클릭하여 구성하거나 관리할 수 있는 추가적인 기능을 봅니다. 아카이브, 탑재, 부팅 CD, 리포지토리, 암호화 키, 클라우드 계정, 파일 검색, 보존 정책, 알림, 보고서, 로그 등의 기능이 있습니다.
구성: 암호화	하나 이상의 보호된 시스템에 사용할 수 있는 암호화 키를 추가 또는 가져오기	암호화 키를 추가하거나 가져와서 보호된 데이터의 보안을 관리하려면 **암호화 키**를 클릭합니다. 하나 이상의 보호된 시스템에 암호화 키를 적용할 수 있습니다. 암호화는 암호화 키 이해 항목에 설명되어 있습니다.
구성: 알림	이벤트에 대한 알림, 경고 및 경보 설정	이벤트, 경고 및 경고에 대한 알림 그룹을 지정하려면 **이벤트**를 클릭합니다. 이를 이메일로 보내려면 SMTP 서버 설정도 구성해야 합니다. 이벤트를 관리하는 방법에 대한 자세한 내용은 이벤트 및 알림 그룹 구성 항목을 포함하여 이메일 서버 구성 항목을 참조하십시오.
구성: 보존	Core의 기본 보존 정책 보기 또는 변경	**보존 정책**을 클릭하여 Core의 보존 정책 페이지를 엽니다. 여기서 복구 지점을 롤업하기 전에 보관할 기간을 지정할 수 있습니다. 보존 정책에 대한 개념 정보는 에이징 데이터 관리을(를) 참조하십시오. 절차 정보는 보존 정책 관리을(를) 참조하십시오.
복원	Core의 복구 지점에서 데이터 복원	**복원**을 클릭하여 시스템 복원 마법사를 엽니다. 데이터를 복원하는 방법에 대한 내용은 복구 지점에서 볼륨 복원에서 확인하십시오.

빠른 시작 안내서 숨기기

빠른 시작 안내서는 처음 Rapid Recovery로 업그레이드하거나 설치할 때 자동으로 나타납니다.
도움말 드롭다운 메뉴에서 빠른 시작 안내서를 선택하는 경우에도 Core Console의 Home(홈) 페이지를 액세스할 때마다 나타납니다.

다음 절차에 따라 빠른 시작 안내서를 숨기십시오.

- Rapid Recovery Core Console에서 빠른 시작 안내서의 **시작** 페이지가 표시되는 경우, 다음 작업을 수행합니다.
  - 빠른 시작 안내서의 **시작** 페이지를 숨기려면 **다시 표시 안 함**을 선택합니다.

노트: 이 옵션은 다음에 빠른 시작 안내서를 열 때부터 Rapid Recovery Core를 업그레이드할 때까지 항상 시작 페이지를 숨깁니다.
이 페이지를 숨기고 나중에 고급 옵션에 액세스하려면 마법사에서 **뒤로**를 선택하여 숨겨진 시작 페이지를 표시합니다.

- 이 세션 동안 빠른 시작 안내서를 숨기려면 **닫기**를 클릭합니다.
  빠른 시작 안내서가 닫힙니다. 다음에 Core Console에서 홈 페이지에 액세스할 때 빠른 시작 안내서가 다시 나타납니다.

  빠른 시작 안내서는 도움말 메뉴에서도 열 수 있습니다.
- 빠른 시작 안내서의 한 페이지에서 **안내서 종료**를 클릭합니다.
  빠른 시작 안내서가 닫힙니다. 이 옵션을 선택할 경우에도 도움말 메뉴에서 빠른 시작 안내서를 열 수 있습니다.

Rapid Recovery Core Console로 이동

Core Console에 로그인할 때 **홈** 아이콘을 클릭하면 **홈** 페이지가 나타납니다. **홈** 페이지에서는 두 가지 옵션과 함께 Rapid Recovery Core를 보여줍니다. 기본 보기 영역에서 기본 내용은 사용자의 시스템에 일련의 실시간 보고서를 표시하는 새로운 Core 대시보드입니다. 기본 대시보드 보고서는 시스템 전송당 최근 전송 작업 상태, 보호, 복제 및 복구 시점 전용 시스템의 연결 상태, 리포지토리 개요를 포함합니다. 또는 클래식 요약 표 보기로 전환할 수 있습니다. 이 보기에서 페이지의 제목은 Rapid Recovery Core의 표시 이름을 보여주며, 보호된 시스템, 리포지토리 및 최근 경고를 보여주는 요약 표를 볼 수 있습니다. 자세한 내용은 홈 페이지 이해(요약 표 보기) 및 Core 대시보드 이해을(를) 각각 참조하십시오.

홈 페이지(및 Core Console의 모든 페이지)의 왼쪽 탐색 영역은 Core에서 보호되고 있는 항목을 보여줍니다. 다음 중 하나를 수행하여 UI에서 다른 페이지를 탐색할 수 있습니다.

- 왼쪽 탐색 영역의 아이콘 표시줄에서 해당 아이콘 클릭 아이콘 표시줄에서 액세스할 수 있는 옵션에는 Replication(복제), Virtual Standby(가상 대기), Events(이벤트), Settings(설정) 및 More(자세히)가 있습니다.
- 아이콘 표시줄의 (자세히) 메뉴를 확장한 다음 대상 선택
- 단추 표시줄에서 단추 또는 메뉴 옵션 클릭 단추에는 보호, 복원, 아카이브 및 복제가 있습니다.

왼쪽 탐색 영역에서 항목을 선택하면 Core Console의 초점이 변경되어 해당 항목에 대한 요약 정보를 표시합니다. 예를 들어, 보호된 시스템의 이름을 클릭하면 Core Console은 해당 Core가 아닌 시스템에 대한 정보만 표시합니다. 이 예에서 보호되는 시스템의 표시 이름이 페이지의 제목으로 나타납니다. 하위 메뉴가 오른쪽에 나타나 보호된 시스템에 대한 특정 정보를 볼 수 있습니다. 메뉴 옵션에는 Summary(요약), Recovery Points(복구 지점), Events(이벤트), Settings(설정), Reports(보고서) 및 More(자세히)가 있습니다.

보호되거나 복제된 여러 컴퓨터의 대시보드 보고서 또는 요약 보기를 포함하여 Core에 대한 정보 보기로 돌아가려면 UI의 왼쪽 상단에 있는 **홈** 아이콘을 클릭하십시오. **홈** 페이지에서 페이지 맨 위 오른쪽에 있는 빨간색 링크를 클릭하여 대시보드 보기와 요약 페이지 보기 사이를 전환할 수 있습니다.

Core Console의 맨 위에 있는 제목을 사용하여 Core에서 사용자가 보고 있는 정보에 대한 컨텍스트를 제공할 수 있습니다. 예:

- 페이지 제목으로 Core의 표시 이름 또는 IP 주소가 보인다면 Core에 대한 요약 정보를 보는 것입니다.
- 제목이 Dashboard(대시보드)라면 Core 대시보드를 보고 있는 것입니다.
- 보호된 시스템의 표시 이름 또는 IP 주소, 또는 페이지 맨 위에서 요약 창이 보인다면 Core에서 보호하는 또는 복제한 단일 시스템에 대한 정보를 보는 것입니다.
- Protected Machines(보호된 시스템)라는 제목이 보인다면 Rapid Recovery Core에서 보호하는 모든 시스템에 대한 정보를 보는 것입니다.
- Machines replicated from...(시스템 복제 원본...)이라는 제목이 보인다면 Rapid Recovery Core에서 복제된 모든 시스템에 대한 정보를 보는 것입니다.
- Recovery Points Only(복구 지점 전용)이라는 페이지 제목이 보인다면 이 Core에 있는 모든 복구 지점 전용 시스템에 대한 정보를 보는 것입니다.

각 페이지에서 사용할 수 있는 기능에 대한 자세한 내용은 아래 해당 섹션을 참조하십시오.

보호된 시스템을 보는 방법에 대한 자세한 내용은 보호된 시스템 메뉴 보기을(를) 참조하십시오. 보호된 시스템을 관리하는 방법에 대한 자세한 내용은 보호된 시스템 관리을(를) 참조하십시오.

복제된 시스템을 보는 방법에 대한 자세한 내용은 수신 및 발신 복제 보기을(를) 참조하십시오.

복구 지점 전용 시스템 보기에 대한 자세한 내용은 다음을 참조하십시오. 복구 지점만 메뉴 보기

왼쪽 탐색 영역 이해

Core Console의 왼쪽 탐색 영역은 사용자 인터페이스의 왼쪽에 나타납니다. 이 탐색 영역의 내용은 Rapid Recovery Core에서 보호된 개체 유형에 따라 다를 수 있습니다.

왼쪽 탐색 영역에는 항상 다음과 같은 정보가 포함되어 있습니다.

- **아이콘 표시줄.** Core Console의 기본 페이지를 탐색할 수 있습니다.
- **텍스트 필터.** 텍스트 필터는 아래 나타나는 다양한 메뉴로 표시되는 항목을 필터링할 수 있는 텍스트 필드입니다. 텍스트 필터의 오른쪽에 있는 화살표를 클릭하면 아래 나타나는 각 메뉴가 확장 및 축소됩니다.

이러한 요소에 이어 왼쪽 탐색 영역은 일반적으로 Core에서 보호되는 개체를 탐색, 필터링 및 보는 데 도움이 되는 메뉴를 표시합니다. 보호되는 시스템, 복제된 시스템 등이 포함되어 있습니다.

각 메뉴는 상황에 맞는 도움말입니다. 즉, 각 메뉴가 관련이 있는 경우에만 Core Console에 나타납니다. 예를 들어, 하나 이상의 시스템을 보호하는 경우 보호된 시스템 메뉴가 나타납니다.

자세한 내용은 Core Console 사용자 인터페이스 보기에서 왼쪽의 탐색 영역에 나타나는 표를 참조하십시오.

Rapid Recovery Core Console 홈 페이지 보기

Rapid Recovery Core Console에 로그인하거나 아이콘 표시줄에서 **홈** 아이콘을 클릭할 때마다 **홈** 페이지가 나타납니다.

Core Console의 **홈** 페이지는 새 **대시보드** 보기와 익숙한 **요약 테이블** 보기를 제공합니다. 대시보드가 보기 기본값입니다.
홈 페이지 오른쪽 상단에 있는 빨간색 링크를 클릭해 **홈** 페이지에서 보기를 전환할 수 있습니다.

홈 페이지와 Core Console의 다른 모든 페이지에서 왼쪽에 있는 탐색 영역을 사용하면 원하는 기능으로 이동할 수 있습니다.

자세한 내용은 다음 항목에서 확인하십시오.

- 왼쪽 탐색 영역 이해
- Core 대시보드 이해
- 홈 페이지 이해(요약 표 보기)

홈 페이지 이해(요약 표 보기)

홈 페이지는 Core에만 해당됩니다. 대시보드 보기에서는 실시간 그래픽 보고서를 표시합니다. 요약 표 보기로 전환하면 **홈** 페이지는 Core에서 보호하거나 복제하는 모든 시스템, Core에 연결된 저장소, 이 Core의 시스템에 대한 경고를 표시합니다.

홈 페이지에 있는 각 창의 보기는 확장하거나 축소할 수 있습니다. 예를 들어 (보기 축소) 아이콘을 클릭하면 보호된 시스템의 보기가 축소되고 창의 이름만 표시됩니다. 보기를 확장하여 보호된 시스템을 모두 보려면 (보기 확장) 아이콘을 클릭합니다.

다음 표에서는 요약 표 보기일 때 **홈** 페이지의 다양한 기본 요소에 대해 설명합니다.

표 3. 홈 페이지 옵션

UI 요소	설명
보호된 시스템	보호된 시스템 창에는 이 Core에서 보호하는 시스템이 나열됩니다. 이 창은 보호하기 위해 Core에 시스템이 추가되었는지에 관계 없이 나타납니다. 이 섹션에는 보호된 각 시스템에 대한 다음과 같은 정보가 나와 있습니다. · **시스템 유형.** 아이콘은 시스템이 물리적 시스템, 가상 시스템 또는 보호된 클러스터인지를 표시합니다. · **상태.** Status(상태) 열의 색이 있는 원은 보호된 시스템이 액세스 가능한지, 일시 중지 또는 오프라인 상태인지 및 연결할 수 없는지를 나타냅니다. · **표시 이름.** 보호된 시스템의 표시 이름 또는 IP 주소입니다. · **리포지토리 이름.** 해당 시스템에 대한 복구 지점을 저장하는 리포지토리의 이름. · **마지막 스냅숏.** Rapid Recovery에서 해당 시스템에 복구 지점 스냅숏을 생성한 가장 최근 날짜 및 시간입니다. · **복구 지점.** 보호된 각 시스템의 리포지토리 및 공간 사용량에 저장된 복구 지점의 수입니다. · **버전**. 시스템에 설치된 Rapid Recovery Agent 소프트웨어 버전입니다. 이 창에 표시된 특정 시스템 이름을 클릭하면 선택한 시스템에 대한 요약 정보를 표시하는 요약 페이지가 나타납니다. 요약 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 보호된 시스템의 요약 정보 보기을(를) 참조하십시오.
복제된 시스템	Replicated Machines(복제된 시스템) 창에는 이 Core가 다른 Core에서 복제한 시스템이 나열됩니다. Core가 다른 Core에서 시스템을 복제하지 않으면 이 창은 나타나지 않습니다. 이 섹션에는 복제된 각 시스템에 대한 다음과 같은 정보가 나와 있습니다. · **시스템 유형.** 아이콘은 시스템이 물리적 시스템, 가상 시스템 또는 보호된 클러스터인지를 표시합니다. · **상태.** Status(상태) 열의 색이 있는 원은 복제된 시스템이 액세스 가능한지, 일시 중지 또는 오프라인 상태인지 및 연결할 수 없는지를 나타냅니다. · **표시 이름.** 복제된 시스템의 표시 이름 또는 IP 주소입니다. · **복제 이름.** 이 대상 Core에서 복제하는 시스템의 원본 소스 Core 표시 이름입니다. 복제를 설정할 때 이 이름을 정의할 수 있습니다. · **리포지토리 이름.** 해당 시스템에 대한 복구 지점을 저장하는 리포지토리의 이름. · **마지막 복제된 스냅숏.** Rapid Recovery에서 원래 보호된 시스템을 복제한 가장 최근 날짜 및 시간입니다. · **복구 지점.** 복제된 각 시스템의 리포지토리 및 공간 사용량에 저장된 복구 지점의 수입니다. · **버전**. 시스템에 설치된 Rapid Recovery Agent 소프트웨어 버전입니다. 이 창에 표시된 특정 시스템 이름을 클릭하면 복제한 시스템에 대한 요약 정보를 표시하는 요약 페이지가 나타납니다.
복구 지점 전용 시스템	복구 지점이 보관된 경우 Recovery Points Only Machines(복구 지점 전용 시스템) 창에는 보호 또는 복제에서 제거된 모든 시스템이 나열됩니다. 이러한 시스템은 파일 수준 복구에 사용할 수 있지만 Bare Metal Restore, 전체 볼륨 복구, 스냅숏 데이터 추가에 사용할 수 없습니다. 이 정의에 맞는 시스템이 없으면 이 창은 나타나지 않습니다. 이 섹션에는 각 복구 지점만 시스템에 대한 다음과 같은 정보가 나와 있습니다. · **시스템 유형.** 아이콘은 시스템이 물리적 시스템, 가상 시스템 또는 보호된 클러스터인지를 표시합니다. · **상태.** Status(상태) 열의 색이 있는 원은 복구 지점 전용 시스템이 액세스 가능한지, 일시 중지 또는 오프라인 상태인지 및 연결할 수 없는지를 나타냅니다. · **표시 이름.** 복구 지점이 보관된 시스템의 표시 이름 또는 IP 주소입니다. · **리포지토리 이름.** 해당 시스템에 대한 남은 복구 지점을 저장하는 리포지토리의 이름입니다. · **복구 지점.** 각 복구 지점 전용 시스템의 리포지토리 및 공간 사용량에 저장된 복구 지점의 수입니다. 이 창에 표시된 특정 시스템 이름을 클릭하면 이 복구 지점 전용 시스템에 대한 요약 페이지가 나타납니다.

UI 요소	설명
DVM 리포지토리	이 창은 DVM 리포지토리가 생성되었는지 여부에 관계 없이 DL1000에 대해 나타납니다. Core에 DVM 하나 이상의 리포지토리가 없으면 이 창은 나타나지 않습니다. 여기에는 각 DVM 리포지토리에 대한 다음과 같은 정보가 있습니다. · **유형.** 아이콘은 리포지토리를 보여줍니다. · **상태.** Status(상태) 열의 색이 있는 원은 리포지토리가 탑재되어 복구 지점 전송을 허용할 수 있는지 또는 연결할 수 없거나 오류 상태인지를 나타냅니다. · **리포지토리 이름.** 리포지토리의 표시 이름. · **공간 사용량.** 리포지토리에서 사용된 총 공간의 양과 저장소 볼륨 또는 범위의 크기입니다. · **보호된 데이터.** 리포지토리에서 사용된 공간의 크기. · **시스템.** 리포지토리에서 복구 지점을 저장하는 시스템의 수입니다. · **복구 지점.** 리포지토리에 저장된 복구 지점의 수. · **압축률** 리포지토리에서 공간을 절약하기 위해 보호된 데이터를 압축하는 비율. 자세한 내용은 리포지토리 이해을(를) 참조하십시오.
경고	이 섹션에는 Core 및 Core가 보호하는 모든 시스템에 대한 중요 경고가 나열됩니다. 이 섹션에는 다음과 같은 정보가 나와 있습니다. · **아이콘.** 아이콘 열은 경고의 특성을 나타냅니다. 정보 메시지, 오류가 포함됩니다. · **날짜.** Rapid Recovery에서 경고가 발생한 날짜와 시간을 표시합니다. · **메시지.** 경고를 설명합니다. 이러한 세부 정보는 Core 이벤트 페이지에도 표시됩니다. 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

Core 대시보드 이해

Core 대시보드에는 사용자의 Core 및 사용자가 보호하는 시스템과 관련된 일련의 실시간 데이터 그래픽 보고서가 표시됩니다. 대시보드에는 다음 보고서가 포함됩니다.

- **전송 작업**. 이 보고서에는 최근 24시간에 완료된 모든 스냅숏 데이터 전송이 표시됩니다(기본 이미지와 증분 스냅숏 포함). 스냅숏에는 기본 이미지와 증분 스냅숏이 포함됩니다. 이 대시보드 보고서는 원그래프로 표시됩니다.
- **시스템별 전송 작업**. 이 작업에는 보호된 시스템별로 최근 24시간의 전송 작업 중 성공 및 실패 횟수가 표시됩니다. 이 대시보드 보고서는 선 그래프로 표시됩니다.
- **리포지토리**. 이 보고서에는 Core와 연결된 리포지토리가 표시됩니다. 리포지토리 개수, 각 리포지토리에서 보호되는 시스템 수, 복구 지점 수, 압축 또는 중복 제거 백분율이 표시됩니다. 이 보고서는 1분마다 새로 고쳐집니다.
- **시스템 연결**. 이 보고서에는 Core에서 보호되고 복제되는 시스템의 연결 상태가 표시됩니다. 복구 지점 전용 시스템의 데이터에 대한 연결도 표시됩니다.

대시보드에 있는 모든 보고서는 보고서 머리글에 있는 위 또는 아래 화살표를 클릭하여 뷰를 축소 또는 확대할 수 있습니다. 시스템 연결 및 리포지토리 대시보드 보고서에서는 다른 보호된 시스템 또는 다른 리포지토리를 각각 추가할 수 있는 더하기 기호가 화살표 옆에 표시됩니다.

보고서 중 하나를 끌어서 놓기 방식으로 대시보드의 다른 곳으로 이동하여 보고서를 사용하기에 가장 효과적인 방식으로 배치할 수도 있습니다.

보호된 시스템 메뉴 보기

Rapid Recovery 사용자 인터페이스에서 보호된 시스템 메뉴는 왼쪽 탐색 영역에 나타납니다. 탐색 영역의 모든 메뉴 레이블과 마찬가지로 이 메뉴의 레이블은 모두 대문자로 나타납니다. 기본적으로 이 메뉴는 완전히 확장되며, 이 Core에서 보호되는 모든 시스템의 목록이 표시됩니다. 보호하는 서버 클러스터가 있는 경우 이 목록에 해당 서버 클러스터가 포함됩니다.

이 메뉴의 왼쪽에 있는 화살표를 클릭하여 Core 내 보호된 시스템 및 서버 클러스터에 대한 보기를 확장하거나 축소할 수 있습니다.

보호된 시스템 메뉴의 오른쪽에는 모든 보호된 시스템에서 수행할 수 있는 기능을 나열하는 드롭다운 메뉴가 표시됩니다. **보호된 시스템** 오른쪽의 화살표를 클릭하여 메뉴를 표시하고 다음 작업을 수행합니다.

- 모든 시스템의 증분 스냅숏 작성
- 모든 시스템의 기본 이미지 작성
- 모든 시스템의 보호 일시 중지(보호가 활성 상태인 경우)
- 모든 시스템의 보호 다시 시작(보호가 일시 중지된 경우)
- 보호된 모든 시스템에 대한 메타데이터 새로 고침
- Core에서 보호되는 모든 시스템 제거

보호된 시스템 메뉴 아래 나열된 각 시스템에는 해당 시스템만을 위한 기능을 제어하는 드롭다운 메뉴도 있습니다. 한 시스템의 드롭다운 메뉴에서 다음 작업을 수행할 수 있습니다.

- 선택한 시스템의 증분 스냅숏 작성
- 선택한 시스템에 대한 보호 일시 중지(보호가 활성화된 경우)
- 보호 다시 시작(보호가 일시 중지된 경우)
- 메타데이터 새로 고침
- Core에서 보호되는 선택한 시스템 제거
- 선택한 시스템의 Summary(요약) 페이지로 이동
- 선택한 시스템의 Recovery Points(복구 지점) 페이지로 이동
- 선택한 시스템의 Events(이벤트) 페이지로 이동
- 선택한 시스템의 Settings(설정) 페이지로 이동
- 해당 시스템에 특정된 보고서 생성
- 시스템 정보, 탑재, 보존 정책 또는 시스템 특정 로그를 포함해 선택한 시스템에 특정된 더 많은 기능에 액세스
- 보호된 시스템 목록에 표시되는 사용자 지정 레이블 만들기

Rapid Recovery에서 서버 클러스터를 관리하는 경우 서버 클러스터는 왼쪽 탐색 메뉴에도 나타납니다. 한 클러스터의 드롭다운 메뉴에서 다음 작업을 수행할 수도 있습니다.

- 선택한 클러스터의 **보호된 노드** 페이지로 이동

보호된 시스템 메뉴 왼쪽의 화살표를 클릭하면 보호된 시스템 및 서버 클러스터 목록이 축소되고 시스템이 나열되지 않습니다. 이 화살표를 다시 클릭하면 시스템 목록이 다시 확장됩니다.

Protected Machines(보호된 시스템) 메뉴에서 시스템 이름을 클릭하면 해당 시스템에 대한 Summary(요약) 페이지가 열립니다. 요약 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 보호된 시스템의 요약 정보 보기을(를) 참조하십시오.

마지막으로 **보호된 시스템** 메뉴를 직접 클릭하면 이 Core에서 보호된 시스템을 보여주는 단일 창과 함께 **보호된 시스템** 페이지가 기본 내용 영역에 나타납니다. 보호된 시스템 페이지의 **보호된 시스템** 창에서 수행할 수 있는 작업에 대한 자세한 내용은 Protected Machines(보호되는 시스템) 창 보기을(를) 참조하십시오.

노트: 보호된 시스템 페이지에서 아이콘 표시줄의 홈 아이콘을 클릭하면 Core 측면의 보기로 돌아갈 수 있습니다.

보호된 시스템의 요약 정보 보기

Core Console에서 보호된 시스템의 이름을 클릭하면 **요약** 페이지가 나타납니다. 이 페이지는 최소한 요약 창과 볼륨 창을 포함합니다. 시스템이 복제에 추가된 경우 복제 창도 나타납니다.

하나 이상의 보호된 Exchange Server가 있는 경우 보호된 Exchange Server에 대한 정보를 포함하는 Exchange Server 정보 창도 볼 수 있습니다.

하나 이상의 보호된 SQL Server가 있는 경우 보호된 SQL Server에 대한 정보를 포함하는 SQL Server 정보 창도 볼 수 있습니다.

페이지 상단에는 보호된 시스템에서 수행할 수 있는 작업 메뉴가 표시됩니다. 아래에 최소한 요약 창과 볼륨 창이 나타납니다. 시스템이 복제에 추가된 경우 복제 창도 나타납니다.

요약 페이지 및 기타 모든 보기에서 보호된 시스템에 대한 정보를 표시하면 페이지 상단에 기능을 수행할 수 있는 메뉴가 나타납니다. 이 메뉴는 보호된 시스템 이름 바로 아래에 나타납니다.

관련 링크

요약 창 보기
보호된 시스템에서 볼륨 보기
복제 정보 보기
Exchange Server 정보 창 보기
SQL Server 정보 창 보기

요약 창 보기

요약 창은 호스트 이름, 마지막 스냅숏의 날짜 및 시간, 다음 순서로 예약된 스냅숏의 날짜 및 시간, 암호화 키 정보 및 Rapid Recovery Agent 소프트웨어의 버전 정보를 포함하여 보호된 시스템에 대한 요약 정보를 포함합니다. 시스템에 대한 세부적인 시스템 정보 페이지 링크도 있습니다.

보호된 시스템에서 볼륨 보기

보호된 시스템인 경우 볼륨 창의 요약 페이지에서 나열된 볼륨에 대한 다음 작업을 수행할 수 있습니다.

- 선택한 볼륨에 대한 보호 일정을 설정하거나 수정합니다. 일반적으로 보호 일정은 처음 시스템을 보호할 때 설정됩니다. 보호 일정 수정에 대한 자세한 내용은 보호 일정 수정을 참조하십시오.
- 기본 이미지 또는 스냅숏을 작성합니다. 일반적으로 스냅숏은 보호 일정을 기반으로 발생합니다. 그러나, 언제든지 기본 이미지 또는 선택한 볼륨에 대한 증분 스냅숏을 작성할 수 있습니다. 자세한 내용은 스냅숏 강제 적용을 참조하십시오.

복제 정보 보기

복제 창에는 복제 이름, 복제 상태 및 사용 가능한 공간을 볼 수 있는 복제된 시스템에 대한 요약 정보가 포함되어 있습니다.

Exchange Server 정보 창 보기

Exchange Server 정보 창은 보호된 시스템이 Exchange Server인 경우에만 나타납니다.

이 창에는 보호된 Exchange Server에 대한 요약 정보를 포함하여 Microsoft Exchange 설치 버전, Exchange가 설치되어 있는 경로 및 Exchange 사서함 데이터에 대해 정의된 경로가 포함되어 있습니다.

메일 저장소 그리드는 EDB(Exchange Database) 이름, EDB 파일 경로, 로그 파일이 저장되는 경로, 로그 접두사, 시스템 경로, DAG(Database Availability Group) 및 메일 저장소 유형을 표시합니다.

SQL Server 정보 창 보기

SQL Server 정보 창은 보호된 시스템이 SQL Server인 경우에만 나타납니다.

이 창에는 보호된 SQL Server에 대한 요약 정보가 포함되어 있습니다. 데이터베이스 정보를 확장하여 데이터베이스에서 각 표에 대한 세부 정보를 볼 수 있습니다. 데이터베이스나 표 이름 및 데이터베이스 경로를 볼 수 있습니다.

시스템의 복구 지점 보기

복구 지점 페이지에는 보호된 시스템에 대해 수집된 복구 지점 뿐만 아니라 관련 시스템 및 리포지토리 데이터 목록도 표시됩니다. 이 페이지에서 특정 복구 지점을 마운트, 복원 및 내보낼 수 있을 뿐만 아니라 삭제도 가능합니다.

페이지가 2개의 창, 즉 복구 지점 요약 및 복구 지점으로 나누어집니다. 요약 탭에는 실행 가능한 링크가 포함되지 않습니다. 시스템에 대한 다음과 같은 정보가 표시됩니다.

표 4. 복구 지점 요약 창 데이터

UI 요소	설명
총 복구 지점	보호된 특정 시스템에 대해 수집된 복구 지점의 수.
총 보호된 데이터	리포지토리에 저장된 보호된 시스템 데이터의 양.
리포지토리	Rapid Recovery에서 보호된 시스템의 복구 지점을 저장하는 리포지토리 이름.
리포지토리 상태	진행률 표시줄에는 리포지토리에서 사용되는 총 공간의 백분율이 표시됩니다. 사용된 데이터의 양과 리포지토리의 총 크기가 진행률 표시줄 아래 표시됩니다.

자세한 내용은 Protected Machines(보호되는 시스템) 창 보기을(를) 참조하십시오.

보호된 시스템에 대한 이벤트 보기

이벤트 페이지에서는 선택한 보호된 시스템에서 발생했거나 진행 중인 작업을 볼 수 있습니다. 페이지 상단의 단추를 사용하면 세 가지 활동 카테고리 중 하나에서 작업 목록을 탐색할 수 있습니다.

- **작업.** Rapid Recovery가 성공적으로 작동하기 위해 수행해야 하는 작업입니다.
- **경고.** 오류 및 경고가 포함된 작업 또는 이벤트와 관련된 알림입니다.
- **저널.** 모든 보호된 시스템 작업과 경고의 복합체입니다.

다음 표에는 **이벤트** 페이지의 각 요소에 대한 설명이 포함되어 있습니다.

표 5. 이벤트 페이지 요소

UI 요소	설명
키워드 검색	각 범주 내 특정 항목을 검색할 수 있습니다. 작업에만 사용할 수 있습니다.
시작	검색을 시작할 날짜를 입력하여 결과를 좁힐 수 있습니다. 작업에만 사용할 수 있습니다.
종료	검색을 중지할 날짜를 입력하여 결과를 좁힐 수 있습니다. 작업에만 사용할 수 있습니다.
상태 아이콘	각 아이콘은 서로 다른 작업 상태를 나타냅니다. 경고 및 작업의 경우 아이콘 중 하나를 클릭하여 해당 상태를 기준으로 목록을 필터링하고 보고서를 생성할 수 있습니다. 아이콘을 다시 클릭하면 해당 상태에 대한 필터가 제거됩니다. 두 개 이상의 상태를 기준으로 필터링할 수 있습니다. 상태는 다음과 같습니다. • **활성.** 진행 중인 작업입니다. • **대기열에 있음.** 시작하기 위해 다른 작업이 완료되기를 기다리고 있는 작업. • **대기 중.** 시드 드라이브와 같이 사용자의 승인 또는 완료를 대기하는 작업입니다. (시드 드라이브에 대한 자세한 내용은 복제를 참조하십시오.) • **완료.** 성공적으로 완료된 작업입니다. • **실패.** 실패하여 완료되지 못한 작업.
서비스 아이콘	이 단추는 서비스 작업을 작업 목록에 추가합니다. 이 아이콘을 클릭하면 더 작은 서비스 아이콘이 각 상태 아이콘에 나타나며, 이 아이콘을 사용하여 해당 상태(있는 경우)에 있는 서비스 작업을 기준으로 필터링할 수 있습니다. 서비스 작업의 예로는 인덱스 파일 삭제 또는 복제에서 시스템 제거 등이 있습니다.
내보내기 유형 드롭다운 목록	드롭다운 목록에는 이벤트 보고서를 내보낼 수 있는 형식이 포함됩니다. 작업에만 사용할 수 있습니다. 다음과 같은 형식이 포함됩니다. • PDF

UI 요소	설명
	• HTML • CSV • XLS • XLSX
(내보내기 아이콘)	이벤트 보고서를 사용자가 선택한 형식으로 변환합니다. 작업에만 사용할 수 있습니다.
페이지 선택	이벤트 보고서는 여러 페이지에 걸쳐 여러 작업을 포함할 수 있습니다. **이벤트** 페이지 하단의 숫자와 화살표를 사용하면 보고서의 페이지 사이를 이동할 수 있습니다.

이벤트 페이지에는 모든 이벤트가 표 형태로 표시됩니다. 다음 표는 각 항목에 대해 표시되는 정보를 나열합니다.

표 6. 이벤트 요약 표에 대한 자세한 정보

UI 요소	설명
상태	작업, 경고, 또는 저널 항목의 상태를 보여 줍니다. 경고 또는 저널 항목에 대해 사용 가능하며 상태별로 결과를 필터링하려면 머리글을 클릭합니다.
이름	이름는 작업에만 사용할 수 있습니다. 이 텍스트 필드는 이 보호된 이 시스템에 대해 완료한 작업 유형을 나열합니다. 볼륨 전송, 리포지토리 유지 관리, 롤업, 탑재 가능 검사 수행, 체크섬 검사 수행 등의 예가 있습니다.
시작 시간	작업, 경고 및 저널 항목에 사용 가능합니다. 작업 시작 시 날짜 및 시간을 표시합니다.
종료 시간	작업에만 사용할 수 있습니다. 작업 완료 시 날짜 및 시간을 나타냅니다.
작업 세부 정보	작업에만 사용할 수 있습니다. **진행 중인 작업 모니터** 대화 상자를 열면 특정 작업의 세부 정보를 볼 수 있습니다. 이러한 세부 정보에는 작업 ID, Core의 데이터 전송 속도(관련된 경우), 작업 완료 경과 시간, 총 작업량(기가바이트) 및 해당 작업과 연관된 하위 작업 등이 있습니다.
메시지	경고 및 저널 항목에 사용할 수 있습니다. 이 텍스트 필드는 경고 또는 저널에 대한 설명적 메시지를 제공합니다.

보호된 시스템에서 보고서 보기

보고서 드롭다운 메뉴에서 선택한 보호된 시스템에 대한 주문형 보고서를 생성할 수 있습니다.

작업 보고서는 선택된 시스템에서 성공한 작업 및 실패한 작업 상태에 대한 보고서를 제공합니다. 실패한 작업은 오류 보고서에서 더 볼 수 있습니다. 이 보고서 유형에 대한 자세한 내용은 작업 보고서 이해을(를) 참조하십시오.

오류 보고서는 지정된 시스템의 실패한 Core 및 취소된 Core 작업에 대한 정보를 제공합니다. 이 보고서 유형에 대한 자세한 내용은 오류 보고서 이해을(를) 참조하십시오.

이 보고서 생성에 대한 자세한 내용은 주문형 Core 보고서 생성을(를) 참조하십시오.

탐색 메뉴에서 복제된 시스템 보기

Core가 다른 Rapid Recovery Core에서 시스템을 복제하는 경우 소스 Core의 표시 이름이 Core Console의 왼쪽 탐색에서 접기 가능한 메뉴로 표시됩니다. 탐색 영역의 모든 메뉴 레이블과 마찬가지로 이 복제된 시스템의 메뉴 이름은 보호된 시스템 메뉴에 모두 대문자

로 나타납니다. 기본적으로 복제된 시스템 메뉴는 모두 펼쳐져 있으며, 소스 Core에 기반하여 대상 Core에 복제된 모든 시스템을 나열합니다.

이 메뉴의 왼쪽에 있는 화살표를 클릭하여 해당 소스 Core에서 복제된 시스템 보기를 확장하거나 축소할 수 있습니다.

각 복제된 시스템 메뉴의 오른쪽에는 해당 Core에 기반하여 복제된 모든 시스템에서 동시에 수행할 수 있는 기능이 포함된 드롭다운 메뉴가 있습니다. 복제된 시스템 메뉴의 오른쪽에 있는 화살표를 클릭하여 수행할 수 있는 기능의 드롭다운 목록을 봅니다. 다음 기능이 포함됩니다.

- 복제를 일시 중지합니다. 복제가 현재 활성화된 경우 다시 시작할 때까지 작업이 중단됩니다.
- 복제를 다시 시작합니다. 복제가 일시 중지된 경우 복제가 다시 시작됩니다.
- 복제 수행. 예약된 시간 대신 요청 시에 복제합니다.
- 복제 제거. 소스 Core와 대상 Core. 사이에 복제 관계를 제거합니다. 필요한 경우 이 Core에 저장된 복구 지점을 삭제할 수도 있습니다. 자세한 내용은 복제 제거을(를) 참조하십시오.

탐색 메뉴에서 소스 Core 이름을 직접 클릭하면 기본 콘텐츠 영역에 **[소스 Core 이름]에서 복제된 시스템** 페이지가 나타납니다. 이 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 수신 및 발신 복제 보기를 참조하십시오.

관련 링크

복제 일시 중지 및 다시 시작
복제 수행
복제 제거

복구 지점만 메뉴 보기

다음 중 하나에 해당하는 경우 왼쪽 탐색 영역에 복구 지점만 메뉴가 나타납니다.

- Rapid Recovery Core에 이전에 보호된 시스템의 복구 지점 몇 개가 보존된 경우
- 복제를 제거했지만 복구 지점을 보존하는 경우

탐색 영역의 모든 메뉴 레이블과 마찬가지로 이 메뉴의 레이블은 모두 대문자로 표시됩니다.

이 메뉴 왼쪽에 있는 화살표를 클릭하여 복구 지점만 시스템 보기를 확장하거나 축소할 수 있습니다.

이 메뉴 오른쪽에는 모든 복구 지점만 시스템에서 동시에 수행할 수 있는 기능을 나열하는 드롭다운 메뉴가 표시됩니다. 이 경우 Core에서 복구 지점을 제거하는 기능만 사용할 수 있습니다.

△ 주의: **이 작업을 수행하면 Rapid Recovery Core에서 모든 복구 지점만 시스템을 완전히 삭제하므로 이 Core에서 해당 복구 지점의 정보를 복원할 수 없습니다.**

사용자 지정 그룹 메뉴 보기

사용자 지정 그룹 메뉴는 하나 이상의 사용자 지정 그룹을 정의한 경우에만 왼쪽 탐색 영역에 표시됩니다. 탐색 영역의 모든 메뉴 레이블과 마찬가지로 이 메뉴의 레이블은 모두 대문자로 표시됩니다.

왼쪽에 있는 화살표를 클릭하여 이 메뉴 항목의 보기를 확장하거나 축소할 수 있습니다.

사용자 지정 그룹 메뉴의 오른쪽에는 해당 그룹의 모든 유사 항목에서 동시에 수행할 수 있는 기능을 나열하는 드롭다운 메뉴가 표시됩니다.

자세한 내용은 사용자 지정 그룹 이해을(를) 참조하십시오.

오류 대화 상자 사용

Rapid RecoveryRapid Recovery Core Console 사용자 인터페이스에서 오류(예: 잘못된 매개 변수 입력 시도)가 발생하면 오류 대화 상자가 표시됩니다. 대화 상자에는 일반적으로 오류의 원인이 표시되고 오류에 대한 추가 정보를 제공하는 링크와 닫기 단추가 있습니다. 계속하기 전에 오류 대화 상자를 닫아야 하지만, 오류에 대한 추가 정보를 볼 수도 있습니다.

오류 대화 상자의 다음 옵션 중에서 선택합니다.

오류 대화 상자가 표시되는 원인이 되는 사용자 인터페이스 오류는 단순한 유효성 검사 또는 데이터 입력 오류이므로 Rapid Recovery 이벤트 탭에서 추적되지 않습니다. 그러나 오류에 대한 Knowledge Base 검색 옵션을 클릭하는 경우 해당 오류에 대해 제공된 URL 링크가 CoreAppRecovery.log 파일에 기록됩니다. 로그에서 "KB article url generated" 텍스트 문자열을 검색하여 브라우저에 표시된 각 오류에 대한 URL을 확인할 수 있습니다. Core 오류 로그를 다운로드하거나 보는 방법에 대한 자세한 내용은 각각 Core 로그 파일 다운로드 및 보기 또는 Core 로그 액세스을(를) 참조하십시오.

Core 설정

이 섹션에서는 설정 아이콘에서 Rapid Recovery Core에 대한 설정을 관리하고 변경하는 방법을 설명합니다.

Rapid Recovery Core 설정

Rapid Recovery Core 설정은 기본적으로 대부분의 사용자를 위해 최적의 성능을 발휘하도록 구성됩니다. 이 설정은 Rapid Recovery Core 성능에 영향을 미치거나 경우에 따라 Rapid Recovery Core Console의 정보 표시에 영향을 미칩니다. 아이콘 표시줄에서 (설정)을 클릭하여 Core 설정에 액세스합니다. 모든 Core 설정의 목록은 왼쪽에 나타납니다. 이 목록에서 원하는 설정의 제목을 클릭해 오른쪽에 있는 해당 설정의 전체 구성으로 이동할 수 있습니다. 또는 오른쪽의 모든 Core 설정에서 아래로 스크롤하여 모든 구성 옵션을 볼 수 있습니다. 자세한 내용은 Rapid Recovery Core 설정을(를) 참조하십시오.

시스템 정보 요약을 보거나 Core 로그 파일을 다운로드할 수 있는 Core 도구에 액세스할 수도 있습니다. 자세한 내용은 코어 수준 도구를 참조하십시오.

구성 가능한 여러 Rapid Recovery Core 설정이 다음 표에 설명되어 있습니다.

표 7. Rapid Recovery Core 구성 가능 설정

구성 설정	설명
Core 구성 백업 및 복원	Rapid Recovery를 사용하면 Core 구성 설정을 XML 파일에 백업할 수 있습니다. 백업 파일이 있는 경우 백업 파일을 사용하여 Core 설정을 복원하거나 마이그레이션할 수 있습니다. Core 설정을 백업하고 복원하는 방법에 대한 자세한 내용은 Core 설정 백업 및 복원을(를) 참조하십시오.
일반	일반 설정에는 웹 서버 및 Rapid Recovery 서비스에 대한 표시 옵션과 포트를 포함하여 Rapid Recovery Core에 일반적으로 적용되는 구성 옵션이 포함됩니다. 이 설정을 구성하는 방법을 포함하여 Rapid Recovery Core의 일반 설정에 대한 자세한 내용은 Core 일반 설정 구성을(를) 참조하십시오.
업데이트	업데이트 설정에 따라 Rapid Recovery 소프트웨어의 업데이트 버전이 있는지 확인하는 자동 업데이트 기능이 관리됩니다.

구성 설정	설명
	이 설정을 구성하는 방법을 포함하여 Rapid Recovery Core를 업데이트하기 위한 설정에 대한 자세한 내용은 업데이트 설정 구성을 확인하십시오.
야간 작업	야간 작업 설정은 Core에서 매일 수행하는 자동화된 작업입니다. 작업 시작 시간과 수행될 작업을 구성할 수 있습니다. Dell은 리소스에 대한 수요가 많을 때 시스템에 대한 로드를 줄이려면 일반 업무 시간이 아닌 다른 시간에 작업 일정을 설정하는 것을 권장합니다. 자세한 내용은 야간 작업 이해, Core에 대한 야간 작업 구성 및 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.
전송 대기열	전송 대기열 설정은 리소스를 사용할 수 없어 작업에 실패하는 경우 전송 작업이 시도되는 횟수를 제어합니다. 최대 동시 전송 수와 최대 데이터 전송 재시도 횟수를 설정할 수 있습니다. 전송 대기열 설정에 대한 자세한 내용은 전송 대기열 설정 수정을(를) 참조하십시오.
클라이언트 제한 시간	클라이언트 제한 시간 설정은 시간이 초과되기 전에 특정 연결 요청 또는 읽기 및 쓰기 작업을 시도해야 하는 시간을 지정합니다. 클라이언트 제한 시간 설정에 대한 자세한 내용은 클라이언트 제한 시간 설정 조정을(를) 참조하십시오.
DVM 중복 제거 캐시	중복 제거를 통해 고유한 정보 블록이 리포지토리에 한 번만 저장되고, 반복된 데이터 블록에 대한 참조가 생성됩니다. 참조는 중복 제거 캐시에 저장됩니다. 암호화 키가 사용되는 경우 중복 제거는 각 암호화 도메인 내에서 발생합니다. DVM 중복 제거 캐시 설정을 사용하면 캐시 크기를 구성하고 기본 캐시 및 보조 캐시 뿐만 아니라 메타데이터 캐시의 위치도 지정할 수 있습니다. 중복 제거 캐시에 대한 자세한 내용은 중복 제거 캐시 및 저장 위치 이해를 참조하십시오. 설정을 조정하는 방법에 대한 자세한 내용은 DVM 중복 제거 캐시 설정 구성을(를) 참조하십시오.
Replay 엔진	Replay 엔진 설정은 Replay 엔진용 통신 채널과 관련된 정보(예: IP 주소 및 제한 시간 설정)를 제어하여 네트워크 요구에 따라 성능을 조정할 수 있습니다. Rapid Recovery 엔진 설정에 대한 자세한 내용은 Replay 엔진 설정 구성을(를) 참조하십시오.
배포	배포 설정을 사용하면 Core에서 보호할 시스템으로 Rapid Recovery Agent 소프트웨어를 배포하기 위한 옵션을 설정할 수 있습니다. 배포 설정을 구성하는 방법에 대한 자세한 내용은 배포 설정 구성을(를) 참조하십시오.
데이터베이스 연결	Rapid Recovery에서는 트랜잭션 정보를 MongoDB 서비스 데이터베이스에 저장하는데, 이 데이터베이스는 기본적으로 Core 시스템에 로컬로 설치됩니다. 정보가 데이터베이스에 유지되는 기간을 변경하거나, 더 많거나 더 적은 수의 동시 연결이 가능하도록 연결 풀 크기를 변경하기 위해 이 설정을 구성할 수 있습니다. 서비스 데이터베이스에 대해 데이터베이스 연결 설정을 지정하거나 수정하는 방법에 대한 자세한 내용은 데이터베이스 연결 설정 구성을(를) 참조하십시오.
로컬 데이터베이스	Rapid Recovery에서는 이벤트 페이지에 Core 작업, 이벤트 및 경고에 대한 정보를 표시합니다. Rapid Recovery에서는 이 트랜잭션 정보를 MongoDB 서비스 데이터베이스에 저장하는데, 이 데이터베이스는 Rapid Recovery Core와 동일한 시스템에 로컬로 설치됩니다. 로컬 데이터베이스 설정을 사용하는 로컬 Mongo 서비스 데이터베이스의 자격 증명 정보(사용자 이름과 암호)를 구성할 수 있습니다. 전원 설정 관리에 대한 자세한 내용은 로컬 데이터베이스 연결 설정 수정을(를) 참조하십시오.
SMTP 서버	Core에 대해 SMTP(Simple Mail Transfer Protocol) 서버 설정을 구성하면 Core 이벤트 정보를 이메일로 보낼 수도 있습니다. SMTP 이메일 서버를 구성하는 방법에 대한 자세한 내용은 이메일 서버 구성을(를) 참조하십시오.

구성 설정	설명
	노트: 이벤트 정보를 이메일로 보내려면 알림 그룹 설정도 구성해야 합니다. 이메일 경고를 받기 위해 이벤트를 지정하는 방법에 대한 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.
클라우드 구성	클라우드 구성 설정을 사용하면 지원되는 클라우드 저장소 계정에 대해 구성 설정을 지정할 수 있습니다. 이 설정에서는 클라우드 계정을 만들지 않습니다. 대신, 기존 클라우드 저장소 계정을 Rapid Recovery Core에 연결하여 Rapid Recovery 정보 아카이브 같은 작업을 쉽게 수행합니다. Rapid Recovery Core에서 클라우드 저장소 계정 정보를 관리하는 방법에 대한 자세한 내용은 클라우드 계정 관리를 참조하십시오.
보고서	보고서 설정에는 Rapid Recovery Core에서 보고서를 생성할 때 사용되는 글꼴을 선택할 수 있는 단일 구성 매개 변수가 포함됩니다. 보고서 설정을 변경하는 방법에 대한 자세한 내용은 보고서 설정 관리를 참조하십시오.
연결성	연결 기능 설정을 사용하면 보호된 시스템에서 SQL 연결 기능 검사를 수행할지 또는 Core에서 SQL Server 인스턴스를 사용할지를 지정할 수 있습니다. Core에서 SQL를 지정하는 경우 자격 증명 정보를 입력해야 합니다. Core에 대한 SQL 연결 기능 설정을 구성하는 방법에 대한 자세한 내용은 Core SQL 연결 기능 설정 관리를 참조하십시오.
작업	복제와 같은 작업을 시작할 때마다 Core 작업이 자동으로 생성됩니다. 작업 Core 설정을 사용하여 각 작업의 설정을 지정할 수 있습니다. 한 번에 실행할 작업의 수를 구성할 수 있습니다. 네트워크 또는 기타 통신 오류로 인해 처음에 작업을 수행할 수 없는 경우 시도 횟수 설정을 사용하여 작업 시도 횟수를 설정할 수 있습니다. Core 작업, 사용 가능한 작업, 작업 구성 방법에 대한 자세한 내용은 Core 작업 설정을(를) 참조하십시오.
라이센스	Core Console에서 Rapid Recovery를 사용하면 Core와 연결된 라이센스를 변경하고 일일 스냅숏 수를 제한하고 라이센스 풀 정보를 보거나 라이센스 서버에 연결할 수 있습니다. Core에서 라이센스를 관리하는 방법에 대한 자세한 내용은 라이센스 관리를 참조하십시오. 라이센스 관리에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery License Portal 안내서를 참조하십시오. **노트: Dell Data Protection | Rapid Recovery License Portal은 Rapid Recovery 소프트웨어와 릴리스 주기가 다릅니다. 최신 제품 설명서는 Dell 기술 문서 웹사이트에서 확인하십시오.**
SNMP 구성	SNMP(Simple Network Management Protocol)는 IP 네트워크에서 장치를 관리하기 위한 프로토콜입니다. Rapid Recovery Core를 SNMP 에이전트로 구성할 수 있습니다. 그런 다음 Core에서 경고, 리포지토리 상태, 보호된 시스템과 같은 정보를 보고할 수 있습니다. Rapid Recovery와 함께 SNMP를 사용하는 방법에 대한 자세한 내용은 SNMP 설정 이해를 참조하십시오.
vSphere	vSphere Core 설정은 에이전트 없이 보호되는 가상 시스템의 사용자에게만 적용됩니다. vSphere 호스트를 사용하는 경우, 이러한 설정에는 VM에 적용되는 연결 설정이 포함됩니다. 에이전트 없이 보호되는 VMware 또는 ESXi의 vSphere 설정에 대한 자세한 내용은 vSphere 설정 구성을(를) 참조하십시오.
로그 업로드	이 옵션이 예로 설정되면 Rapid Recovery Core에서는 전반적인 제품 품질을 향상시키기 위한 지속적인 노력으로 Dell에 분석용 로그 파일을 업로드합니다. 이 설정은 선택 사항입니다.

Core 일반 설정 구성

Rapid Recovery Core의 일반 설정으로는 Core 표시 이름, 웹 서버 포트, 서비스 포트, 로캘(Core Console 표시 언어)이 포함됩니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **일반**을 클릭합니다.
- General(일반) 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

General(일반) Core 설정이 표시됩니다.

3 변경하려는 일반 설정을 클릭합니다.

선택한 설정이 텍스트 필드 또는 드롭다운 메뉴로 표시되며, 편집 가능합니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 8. 일반 설정 정보

텍스트 상자	설명
표시 이름	Core의 새 표시 이름을 입력합니다. 이 이름은 Rapid Recovery Core Console에 표시됩니다. 최대 64자를 입력할 수 있습니다.
웹 서버 포트	웹 서버의 포트 번호를 입력합니다. 기본 포트는 8006입니다.
서비스 포트	Rapid Recovery Core 서비스의 포트 번호를 입력합니다. 기본 포트는 8006입니다.
로캘	로캘 드롭다운 목록에서 표시할 언어를 선택합니다. 한국어, 영어, 프랑스어, 독일어, 일본어, 포르투갈어, 중국어(간체) 및 스페인어 중에서 선택할 수 있습니다. **노트: 언어를 변경하는 경우 Rapid Recovery Core 서비스를 다시 시작해야만 Core Console에 업데이트된 언어가 표시된다는 메시지가 나타납니다. 이 서비스는 Windows 작업 관리자에서 다시 시작할 수 있습니다.**

5 각 설정에서 변경 내용에 만족하면 ✔를 클릭하여 변경 내용을 저장하고 편집 모드를 종료합니다. 저장하지 않고 편집 모드를 종료하려면 ✖을 클릭합니다.

업데이트 설정 구성

Rapid Recovery에는 자동 업데이트 기능이 있습니다. Rapid Recovery Core를 설치하면 새 업데이트를 사용할 수 있을 때 Rapid Recovery Core 소프트웨어를 자동으로 업데이트할지와 시스템에서 업데이트를 확인하는 빈도를 선택할 수 있습니다.

일반적으로 Rapid Recovery 릴리스 번호에는 소수점으로 구분된 4가지 정보(주 릴리스 번호, 부 릴리스 번호, 버전, 빌드 번호)가 있습니다. 예를 들어 리브랜딩된 Rapid Recovery의 첫 번째 릴리스는 6.0.1.609였습니다. 다음 릴리스는 6.0.2.142였습니다.

자동 업데이트 기능은 릴리스 번호의 모든 숫자를 비교합니다. 자동 업데이트를 활성화한 경우 Core 소프트웨어는 주 릴리스 번호와 부 릴리스 번호가 동일한 경우에만 개입 없이 업데이트됩니다. 예를 들어, Core 버전 6.0.1.609에서 6.0.2.142(두 버전 모두 6.0으로 시작)로 자동 업데이트가 수행됩니다. 동일한 시스템에서 첫 번째 소수점 이후의 숫자가 동일하지 않으므로 Core는 6.0.2.142에서 6.1.1.XXX로 자동으로 업데이트되지 않습니다. 대신 Core Console 상단의 배너가 Core 소프트웨어 업데이트를 사용할 수 있음을 알립니다. 이 알림을 통해 릴리스 정보를 검토하고 최신 Core 버전으로 업데이트하는 것이 요구 사항에 부합하는지 결정할 수 있습니다.

노트: Rapid Recovery Core 설치에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery 설치 및 업그레이드 안내서를 참조하십시오.

시스템에서 업데이트를 확인하기 위해 사용하는 설정을 언제든지 보고 변경할 수 있습니다.

주의: 복제를 사용하는 경우, 자동으로 업데이트를 설치하도록 시스템을 구성하면 대상 Core 전에 소스 Core가 업그레이드되고, 이에 따라 복제가 실패하거나 Core 간에 새로운 복제를 설정할 수 없게 될 수 있습니다. 복제 사용자의 경우, Dell은 관리자가 대상 Core에만 자동 업그레이드를 적용한 다음 소스 Core를 수동으로 업그레이드하고 마지막으로 보호된 시스템을 업그레이드하는 것을 권장합니다.

업데이트 설정을 구성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지 왼쪽에 있는 Core 설정 목록에서 **업데이트**를 클릭합니다.
- 업데이트 제목이 표시될 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

업데이트 코어 설정이 표시됩니다.

3 변경하려는 설정을 클릭합니다.

선택한 설정을 편집할 수 있게 됩니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 9. 업데이트 설정 정보

텍스트 상자	설명
새 업데이트 확인	Rapid Recovery에서 업데이트를 확인하고 설치하는 빈도를 선택합니다. 다음 옵션 중에서 선택할 수 있습니다. • 안 함 • 매일 • 매주 • 매월 자동 업데이트를 선택하면 선택한 시간 임계값이 지난 후 업데이트를 사용할 수 있으면 야간 작업이 완료된 후 업데이트가 설치됩니다.
업데이트 설치	다음 옵션 중 하나를 선택하여 사용 가능한 업데이트 처리 방법을 지정합니다. • 업데이트 확인 안 함 • 업데이트에 대해 알리지만 자동으로 설치하지 않음 • 자동으로 업데이트 설치
상태	상태에 새 업데이트를 사용 가능한지 표시됩니다.
마지막 확인	마지막 확인 필드에 시스템에서 업데이트를 마지막으로 확인한 날짜와 시간이 표시됩니다. **지금 확인**을 클릭하여 사용 가능한 소프트웨어 업데이트가 있는지 여부를 즉시 확인합니다. 이 확인은 사용자가 설정한 빈도와 상관없이 발생합니다.

5 각 설정에서 변경 내용에 만족하면 ✔ 을 클릭하여 변경 내용을 저장하고 편집 모드를 종료하거나 저장하지 않고 편집 모드를 종료하려면 ✖ 를 클릭합니다.

야간 작업 이해

야간 작업은 정상적인 업무 시간이 끝난 후 미리 결정된 시간에 발생하는 일일 자동 작업입니다. 이러한 작업은 메모리를 많이 사용하며 Rapid Recovery Core가 덜 사용될 때 가장 잘 수행되는 다양한 무결성 검사 및 데이터 통합 작업을 포함합니다.

모든 야간 작업 및 적용할 수 있는 범위는 다음 표에 설명되어 있습니다. 야간 작업은 Core 수준에서 관리됩니다(Core에서 보호되는 모든 시스템에 적용). 특정 보호되는 시스템에 적용할 수 있는 이러한 야간 작업은 "보호되는 시스템"으로 범위를 나열합니다.

표 10. 야간 작업 정보

작업 이름	범위	설명
(변경)	N/A(해당 없음)	이 컨트롤은 Nightly Jobs(야간 작업) 대화 상자를 열고, 여기에서 각 야간 작업에 대한 설정을 활성화, 비활성화 또는 변경할 수 있습니다.
야간 작업 시간	모두	이 설정은 야간 작업이 실행을 시작하도록 예약된 시간을 나타냅니다. 사용량이 적은 시간에 야간 작업을 실행하도록 Core를 구성하는 것이 좋습니다. 기본 시간은 오전 12시입니다.
롤업	Core 또는 보호되는 시스템	정책에 규정된 일정에 따라 복구 지점을 조합하거나 "롤업"하여 백업 데이터에 보존 정책을 적용합니다. 보호되는 모든 시스템에 기본적으로 적용되는 Core에 정책을 사용자 지정할 수 있습니다. 기본적으로 롤업 작업은 전체 Core에 대해 실행됩니다. 또는 ▸ 를 클릭하여 Core 정책을 사용하여 롤업할 보호되는 시스템을 정의합니다. Core에 설정된 기본 정책과 다른 보호되는 시스템의 보존 정책 사용에 대한 자세한 내용은 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.
SQL 데이터베이스의 연결 기능 검사	보호되는 시스템	SQL 데이터베이스를 포함하는 복구 지점의 무결성을 검사합니다. 프로세스: • 데이터베이스를 포함하는 보호 그룹에 대해 최신 복구 지점을 탑재합니다. • SQL Server에서 데이터베이스에 연결합니다. • 데이터베이스를 엽니다. • 데이터베이스를 닫습니다. • 복구 지점을 분리합니다. 이 야간 검사를 활성화하려면 보호되는 시스템의 SQL Server 데이터베이스에 대해 연결 기능 검사를 수행하는 데 사용할 SQL Server 인스턴스를 지정합니다. **노트: 이 옵션은 Core에서 SQL Server를 보호하지 않을 경우에는 나타나지 않습니다.**
보호되는 시스템에서 로그 다운로드	Core	로깅 서버에 보낼 수 있도록 보호되는 시스템에 대한 로그를 Core로 다운로드합니다.
보호되는 가상 시스템의 VMware 스냅샷 통합	Core 또는 보호되는 시스템	이 야간 작업은 기본 VMware API를 사용하여 Rapid Recovery 에이전트 소프트웨어 없이 시스템을 보호합니다. VMware 스냅샷은 정기적으로 통합해야 합니다. 이 야간 작업을 설정하면 매일 이러한 통합을 수행할 수 있습니다. 이 야간 작업에는 최대 동시 통합인 하나의 매개변수가 포함되어 있어 1과 100 사이의 숫자로 설정해야 합니다.
Check integrity of recovery points(복구 지점의 무결성 검사)	Core 또는 보호되는 시스템	각 보호되는 시스템에 대한 복구 지점의 무결성을 검사합니다. 기본적으로 `Check integrity of recovery points` 옵션은 활성화되어 있지 않습니다. 프로세스: • 모든 보호 그룹에 대해 최신 복구 지점을 탑재합니다. • 각 볼륨에 대한 파일 및 폴더를 열거합니다. • 복구 지점을 검사하여 유효한지 확인합니다. • 복구 지점을 분리합니다.
Exchange 데이터베이스의 체크섬 검사	보호되는 시스템	Exchange 데이터베이스(EDB) 파일을 포함한 복구 지점의 무결성을 검사합니다. **노트: 이 옵션은 Core에서 Exchange Server를 보호하지 않을 경우에는 나타나지 않습니다.**

작업 이름	범위	설명
SQL 로그 자르기 (단순 복구 모델만 해당)	보호되는 시스템	마지막 복구 지점과 일치하도록 데이터베이스 트랜잭션 로그를 잘라 SQL Server 로그의 크기를 유지합니다. **노트: 이 옵션은 Core에서 SQL Server를 보호하지 않을 경우에는 나타나지 않습니다.**
Exchange 로그 자르기	보호되는 시스템	마지막 복구 지점과 일치하도록 Exchange 데이터베이스 트랜잭션 로그를 잘라 Exchange 로그의 크기를 유지합니다. **노트: 이 옵션은 Core에서 Exchange Server를 보호하지 않을 경우에는 나타나지 않습니다.**
로그 리포지토리 통계	Core	리포지토리 통계를 로깅 서버로 보냅니다.
기존 이벤트 및 작업 삭제	Core	기존 이벤트를 제거하여 이벤트 데이터베이스의 확장을 관리합니다. 일 수는 구성 가능하며 기본값은 30일입니다.

Core에 대한 야간 작업 구성

Rapid Recovery Core에서 야간 작업 옵션을 사용할 수 있는 경우 선택한 작업이 Core에서 보호되는 모든 시스템에 대해 매일 지정된 시간에 한 번 실행됩니다. 반대로, Core 수준에서 야간 작업을 사용할 수 없는 경우 지정된 작업이 Core에서 보호되는 모든 시스템에 대해 더 이상 실행되지 않습니다.

노트: 야간 작업 이해 항목에서 설명한 대로, 야간 작업 범위에 보호된 시스템이 포함된 경우 하나 이상의 보호된 특정 시스템에 대해 개별적으로만 적용하도록 야간 작업을 구성할 수 있습니다. 보호된 특정 시스템에 야간 작업 설정을 적용하는 방법에 대한 자세한 내용은 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

야간 작업은 메모리 집약적이므로 Dell은 활동이 적은 시간에 야간 작업을 실행하도록 Core를 구성하는 것을 권장합니다. 야간 작업은 기본적으로 오전 12시에 실행됩니다. 다른 시간이 더 적합한 경우에는 다음 절차에 따라 야간 작업 시간 필드에서 이 설정을 변경하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.
- **설정** 페이지의 왼쪽에 있는 Core 설정 목록에서 **야간 작업**을 클릭합니다.
- 야간 작업 제목이 나올 때까지 **설정** 페이지 오른쪽에서 아래로 스크롤합니다.

야간 작업 Core 설정이 표시됩니다.

3 야간 작업을 변경하거나 야간 작업 실행을 시작할 시간을 변경하려면 **변경**을 클릭합니다.
야간 작업 대화 상자가 표시됩니다.

4 야간 작업을 실행할 시간을 변경하려면 **야간 작업 시간** 필드에 새 시간을 입력합니다.

5 첫 번째 열에서는 Core에 대해 설정하려는 각 야간 작업 옵션을 클릭하여 선택합니다. 선택한 옵션을 다시 클릭하면 선택이 취소됩니다.

6 **확인**을 클릭합니다.
야간 작업 대화 상자를 닫고 Core에 대한 야간 작업 설정을 저장합니다.

전송 대기열 설정 수정

전송 대기열 설정은 최대 동시 전송 수 및 최대 데이터 전송 재시도 횟수를 설정하는 Core 수준 설정입니다.

전송 대기열 설정을 수정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭한 후 다음 중 하나를 수행합니다.
- Settings(설정) 페이지 왼쪽의 Core 설정 목록에서 **Transfer Queue(전송 대기열)**를 클릭합니다.
- Transfer Queue(전송 대기열) 제목이 보일 때까지 Settings(설정) 페이지의 오른쪽을 아래로 스크롤합니다.

  Transfer Queue(전송 대기열) Core 설정이 나타납니다.

3 변경하려는 설정을 클릭합니다.

선택한 설정을 편집할 수 있게 됩니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 11. 전송 대기열 설정 정보

텍스트 상자	설명
최대 동시 전송 수	동시 전송 수를 업데이트하려면 값을 입력합니다. 1과 60 사이의 숫자를 설정합니다. 숫자가 작을수록 네트워크 및 기타 시스템 리소스에 대한 로드가 적어집니다. 처리되는 에이전트 수가 증가하면 시스템에 대한 로드도 증가합니다.
최대 다시 시도 횟수	전송 작업을 취소하기 전에 최대 시도 횟수를 설정하려면 값을 입력합니다. 1과 60 사이의 숫자를 설정합니다.

5 각 설정을 변경한 후에는 을 클릭하여 변경 사항을 저장하고 편집 모드를 종료하거나 를 클릭하여 저장하지 않고 편집 모드를 종료합니다.

클라이언트 제한 시간 설정 조정

클라이언트 제한 시간 설정은 작업 시간이 초과되기 전에 다양한 작업을 시도해야 하는 시간을 지정합니다.

노트: Dell은 사용자 환경에서 어떤 문제가 발생하거나 Dell 지원 담당자가 설정을 수정하도록 요청하지 않는 경우 기본 제한 시간 설정을 변경하지 않도록 권장합니다.

클라이언트 제한 시간 설정을 조정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지 왼쪽의 Core 설정 목록에서 **클라이언트 시간 제한**을 클릭합니다.
- 클라이언트 시간 제한 제목이 표시될 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

  클라이언트 시간 제한 코어 설정이 표시됩니다.

3 변경하려는 설정을 클릭합니다.

선택한 설정을 편집할 수 있게 됩니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

5

표 12. 클라이언트 시간 제한 설정 정보

설정	설명
연결 제한 시간	HTTP(HyperText Transfer Protocol)를 통해 데이터를 전송할 때 Core와 보호된 시스템 간의 연결 제한 시간을 제어합니다. 연결 시간 제한이 발생하기 전에 경과하려는 시간을 입력합니다. HH:MM:SS 형식을 사용합니다.

설정	설명
	노트: 기본 설정은 0:05:00 또는 5분입니다.
읽기/쓰기 제한 시간	HTTP를 통해 스트림 데이터를 읽거나 쓸 때 Core와 보호된 시스템 간의 연결 제한 시간을 제어합니다. 증분 스냅숏을 위해 보호된 시스템에서 Core로 변경된 데이터 블록을 전송하는 경우가 해당됩니다. 읽기/쓰기 이벤트 동안 시간 제한이 발생하기 전에 경과하려는 시간을 입력합니다. HH:MM:SS 형식을 사용합니다. **노트: 기본 설정은 0:05:00 또는 5분입니다.**
연결 UI 제한 시간	http를 통한 그래픽 사용자 인터페이스와 Rapid Recovery Core 서비스 간 연결에 대한 시간 제한을 제어합니다. 연결 UI 시간 제한이 발생하기 전에 경과하려는 시간을 입력합니다. HH:MM:SS 형식을 사용합니다. **노트: 기본 설정은 0:05:00 또는 5분입니다.**
읽기/쓰기 UI 제한 시간	http를 통한 그래픽 사용자 인터페이스와 Rapid Recovery Core 서비스 간 읽기 및 쓰기 데이터 스트림의 연결에 대한 시간 제한을 제어합니다. 읽기 또는 쓰기 이벤트 동안 시간 제한이 발생하기 전에 경과하려는 시간을 입력합니다. HH:MM:SS 형식을 사용합니다. **노트: 기본 설정은 0:05:00 또는 5분입니다.**

6 각 설정에서 변경 내용에 만족하면 ✔ 를 클릭하여 변경 내용을 저장하고 편집 모드를 종료하거나 저장하지 않고 편집 모드를 종료하려면 ✖ 를 클릭합니다.

중복 제거 캐시 및 저장 위치 이해

글로벌 중복 제거는 Core에서 백업하는 데이터에 필요한 디스크 저장 공간을 줄입니다. 각 리포지토리는 중복 제거되어 각 고유 블록을 실제로 한 번 디스크에 저장하고, 후속 백업에서는 이러한 블록에 대한 가상 참조 또는 포인터를 사용합니다. 중복되는 블록을 식별하기 위해 Rapid Recovery에 DVM(Deduplication Volume Manager) 리포지토리에 대한 중복 제거 캐시가 포함됩니다. 캐시에 고유한 블록 참조가 보관됩니다.

기본적으로 DVM 리포지토리의 경우 이 중복 제거 캐시는 1.5GB입니다. 이 크기는 대부분의 리포지토리에 충분합니다. 이 캐시를 초과할 때까지 리포지토리에서 데이터는 중복 제거됩니다. 중복 정보의 양이 중복 제거 캐시가 꽉 찰 정도로 클 경우, 리포지토리는 새로 추가된 데이터에 대한 중복 제거 기능을 완전하게 활용할 수 없습니다. 중복 제거 캐시가 꽉 차기 전에 리포지토리에 저장되는 데이터의 양은 백업 중인 데이터 유형에 따라 달라지며 사용자마다 다릅니다.

Rapid Recovery Core에서 중복 제거 캐시 설정을 변경하여 DVM 중복 제거 캐시의 크기를 증가시킬 수 있습니다. 캐시 크기를 증가시키는 방법에 대한 자세한 내용은 DVM 중복 제거 캐시 설정 구성 항목을 참조하십시오.

DVM 중복 제거 캐시 크기를 증가시킬 때 디스크 공간과 RAM 사용량, 두 가지 요인을 고려해야 합니다.

디스크 공간. DVM 중복 제거 캐시의 두 개 복사본(기본 캐시와 병렬 복사본인 보조 캐시)이 디스크에 저장됩니다. 즉, DVM 리포지토리에 대해 기본 캐시 크기인 1.5GB를 사용할 경우 시스템에서 3GB의 디스크 저장소가 사용됩니다. 캐시 크기가 증가함에 따라, 사용된 디스크 공간의 양과 비례적으로 캐시 크기가 2배로 유지됩니다. 적절하게, 그리고 장애 발생 시에도 성능을 발휘하도록 하기 위해 Core가 이러한 캐시의 우선순위를 동적으로 변경합니다. 두 캐시가 모두 필요하며, 기본으로 지정된 캐시가 먼저 저장된다는 점에만 차이가 있습니다.

RAM 사용량. Rapid Recovery Core가 시작될 때 중복 제거 캐시를 RAM으로 로드합니다. 따라서 캐시의 크기가 시스템의 메모리 사용량에 영향을 미칩니다. Core에서 사용되는 전체 RAM 크기는 여러 요인에 따라 달라집니다. 이러한 요소로는 실행 중인 작업, 사용자 수, 보호된 시스템 수 및 중복 제거 캐시 크기 등이 있습니다. Core에서 수행하는 각 작업(전송, 복제, 롤업 등)은 더 많은 RAM을 소비

합니다. 작업을 마치면 그에 따라 메모리 소비가 줄어듭니다. 그러나, 관리자는 충분한 작업을 위해 가장 높은 RAM 로드 요구사항을 고려해야 합니다.

Rapid Recovery Core의 기본 설정은 AppRecovery 디렉터리에 DVM 리포지토리에 대한 기본 캐시, 보조 캐시 및 메타데이터 캐시를 배치합니다. 이 폴더는 Core 시스템에 설치됩니다.

노트: 사용자 설정에 따라, AppRecovery 디렉터리가 Rapid Recovery Core에서 보이지 않을 수 있습니다. 이 디렉터리를 보려면 폴더 옵션 제어판을 숨긴 파일, 폴더 및 드라이브를 표시하도록 변경해야 할 수 있습니다.

Rapid Recovery Core가 C 드라이브에 설치되었다고 가정할 때 해당 위치는 일반적으로 다음과 같습니다.

표 13. DVM 중복 제거 캐시 설정의 기본 저장 위치

설정	기본 저장 위치
기본 캐시 위치	C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache
보조 캐시 위치	C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache
메타데이터 캐시 위치	C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata

캐시의 저장 위치를 변경할 수 있습니다. 예를 들어 내결함성이 증가한 경우, 보조 캐시의 위치를 기본 캐시와 다른 실제 드라이브로 변경할 수 있습니다(단, Rapid Recovery Core에서 이 위치에 액세스할 수 있다고 가정).

이러한 설정에 대한 저장 위치를 변경하는 방법에 대한 자세한 내용은 DVM 중복 제거 캐시 설정 구성 항목을 참조하십시오.

Dell은 중복 제거 저장소를 별도로 계획하는 것을 권장합니다. 중복 제거는 다중 리포지토리가 아니라 단일 리포지토리에서만 발생합니다. Core 기반 암호화를 사용할 경우 각 키가 단일 암호화 도메인에서 작동하는 보안상의 이유로 중복 제거가 단일 키로 보호되는 데이터로 제한됩니다.

중복 제거에 대한 자세한 내용은 Rapid Recovery에서 중복 제거을(를) 참조하십시오.

DVM 중복 제거 캐시 설정 구성

DVM 리포지토리의 중복 제거 캐시 설정을 구성하려면 이 절차의 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.

- 설정 페이지 왼쪽의 Core 설정 목록에서 **DVM 중복 제거 캐시**를 클릭합니다. 이 설정을 Core에 하나 이상의 DVM 리포지토리가 있는 경우에만 나타납니다.
- Settings(설정) 페이지의 오른쪽에서 DVM Deduplication Cache(DVM 중복 제거 캐시) 제목이 보일 때까지 아래로 스크롤합니다.

  DVM Deduplication Cache(DVM 중복 제거 캐시) Core 설정이 나타납니다.

3 언제라도 기본 DVM 중복 제거 캐시 설정을 복원하려는 경우에는 다음을 수행합니다.

a 중복 제거 캐시 설정 영역의 맨 위에서 **기본값 복원**을 클릭합니다.

Restore Default(기본값 복원) 대화 상자가 나타납니다.

b **예**를 클릭하여 복원을 삭제합니다.

4 변경하려는 설정을 클릭합니다.

사용자가 선택한 설정은 편집 가능해집니다.

5 개별 중복 제거 캐시 설정을 변경하려면 다음 표에 설명된 바와 같이 구성 정보를 입력합니다.

표 14. DVM 중복 제거 캐시 설정 정보

설정	설명
기본값 복원	이 컨트롤은 DVM 캐시 위치를 각 설정에 대해 설명된 시스템 기본 위치로 재설정합니다.
기본 캐시 위치	DVM 리포지토리의 기본 캐시 위치를 변경하려면 Primary Cache Location(기본 캐시 위치) 텍스트 상자에 Core에서 액세스할 수 있는 저장 위치의 경로를 입력하십시오. 기본 위치는 다음과 같습니다. **C:\ProgramData\AppRecovery\RepositoryMetaData\PrimaryCache** 기본 및 보조 캐시는 동일한 크기이므로, 이들 두 캐시를 모두 저장하기 위해서는 중복 제거 캐시 크기에 할당된 양에 따라 두 배의 공간이 필요합니다. 예를 들어, 중복 제거 캐시 크기에 1.5GB의 기본 공간을 지정할 경우 두 저장 위치 각각에 1.5GB 이상이 할당되어야 합니다. 특히, 두 위치가 모두 동일한 드라이브(예: C 드라이브)에 속하는 경우에는 사용 가능한 디스크 공간이 3.0GB 이상 있어야 합니다.
보조 캐시 위치	DVM 리포지토리의 보조 캐시 위치를 변경하려면 Secondary Cache Location(보조 캐시 위치) 텍스트 상자에 Core에서 액세스할 수 있는 저장 위치의 경로를 입력하십시오. 기본 위치는 다음과 같습니다. **C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache**
캐시 메타데이터 위치	DVM 리포지토리의 캐시 메타데이터 위치를 변경하려면 Cache Metadata Location(캐시 메타데이터 위치) 텍스트 상자에 Core에서 액세스할 수 있는 저장 위치의 경로를 입력하십시오. 기본 위치는 다음과 같습니다. **C:\ProgramData\AppRecovery\RepositoryMetaData\CacheMetadata**
중복 제거 캐시 크기(GB)	DVM 리포지토리의 중복 제거 캐시 크기를 변경하려면 Deduplication Cache Size(중복 제거 캐시 크기) 텍스트 상자에 새 크기(GB 단위)를 입력하십시오. 기본 위치는 다음과 같습니다. **C:\ProgramData\AppRecovery\RepositoryMetaData\SecondaryCache** 최소 캐시 크기 설정은 1.5GB입니다. 또한, 캐시 크기는 설치된 RAM의 50%를 초과할 수 없습니다.

6 각 설정의 변경 사항에 대해 만족하면 ✔ 를 클릭하여 변경 사항을 저장한 다음 편집 모드를 종료하고, 저장하지 않고 편집 모드를 종료하려면 ✖ 를 클릭합니다.

Replay 엔진 설정 구성

Rapid Recovery의 통신 채널인 Replay 엔진과 관련된 정보를 구성할 수 있습니다. 이 설정에 따라 효과적인 통신을 제공하기 위한 Core 설정이 결정됩니다.

일반적으로 Dell은 기본 설정을 사용하는 것을 권장합니다. 경우에 따라 Dell 지원부에서 네트워크 요구에 따라 성능을 쉽게 조정할 수 있도록 이 설정을 수정하라는 요청을 할 수도 있습니다.

Replay 엔진 설정을 구성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.

- 설정 페이지의 왼쪽의 Core 설정의 목록에서 **재생 엔진**을 클릭합니다.
- Settings(설정) 페이지 오른쪽에서 Replay Engine(Replay 엔진) 제목이 보일 때까지 아래로 스크롤합니다.
  Replay Engine(Replay 엔진) Core 설정이 나타납니다.

3 변경하려는 설정을 클릭합니다.
사용자가 선택한 설정은 편집 가능해집니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 15. Replay 엔진 설정 정보

텍스트 상자	설명
IP 주소	Core는 복구 지점에 대한 탑재 및 복원 수행 시 이 IP 주소를 사용하여 보호된 시스템과 Core 사이의 피드백을 지원합니다. Replay 엔진에 대한 IP 주소는 Core 시스템의 IP 주소로 자동 채워집니다. 수동으로 서버 IP 주소를 입력할 경우 이 값은 보호된 시스템이 제공된 IP 주소를 자동으로 확인할 수 없을 경우에 사용됩니다. 보호된 시스템이 Core와 통신하는 데 문제가 있는 경우를 제외하고 이 값을 설정할 필요가 없습니다.
선호 포트	포트 번호를 입력하거나 기본 설정을 사용합니다. 기본 포트는 8007입니다. 포트는 Replay 엔진의 통신 채널을 지정하기 위해 사용됩니다.
사용 중인 포트	Replay 엔진 구성에 사용 중인 포트를 나타냅니다.
포트 자동 할당 허용	자동 TCP 포트 할당을 허용하려면 클릭합니다.
관리자 그룹	관리자 그룹의 새 이름을 입력합니다. 기본 이름은 BUILTIN\Administrators입니다.
최소 비동기 I/O 길이	값을 입력하거나 기본 설정을 선택합니다. 최소 비동기 입력/출력 길이에 대해 설명합니다. 기본 설정은 65536입니다.
읽기 시간 초과	읽기 제한 시간 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:05:00입니다.
쓰기 제한 시간	쓰기 제한 시간 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:05:00입니다.
수신 버퍼 크기	인바운드 버퍼 크기를 입력하거나 기본 설정을 사용합니다. 기본 설정은 8192입니다.
전송 버퍼 크기	아웃바운드 버퍼 크기를 입력하거나 기본 설정을 사용합니다. 기본 설정은 8192입니다.
지연 없음	네트워크 효율성에 영향을 미칠 수 있으므로 이 확인란을 선택하지 않은 것이 좋습니다. 이 설정을 수정하려면 Dell 지원부에 연락하여 지원을 요청하십시오.

5 각 설정에서 변경 내용에 만족하면 ✔ 를 클릭하여 변경 내용을 저장하고 편집 모드를 종료하거나 저장하지 않고 편집 모드를 종료하려면 ✖ 를 클릭합니다.

배포 설정 구성

Rapid Recovery에서는 설치 프로그램을 Rapid Recovery Core에서 보호하려는 시스템으로 다운로드할 수 있습니다.

Core에서 보호하려는 시스템으로의 Rapid Recovery Agent 배포와 관련된 설정을 구성할 수 있습니다.

배포 설정을 구성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 을 클릭하고 (설정) 다음 중 하나를 수행합니다.

- 설정 페이지 왼쪽에 있는 Core 설정 목록에서 **배포**를 클릭합니다.
- 배포 제목이 표시될 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.
  배포 코어 설정이 표시됩니다.

3 변경하려는 설정을 클릭합니다.
선택한 설정을 편집할 수 있게 됩니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 16. 배포 설정 정보

텍스트 상자	설명
Agent Installer 이름	기본 파일 이름은 Agent-web.exe입니다. 이 파일 이름을 변경하려면 이유와 관계없이 이 설정을 사용하여 Core Web Installer 실행 파일 이름을 지정할 수 있습니다. 웹에서 직접 실행되고 필요하면 프로세스를 일시 중지하고 다시 시작할 수 있는 Rapid Recovery Core 설치 프로그램 최신 버전 다운로드가 이 파일을 통해 스트리밍됩니다.
Core 주소	Core 서버의 주소를 입력합니다. 이 주소는 일반적으로 프로토콜, Core 서버 및 포트의 이름, Core 파일이 위치한 디렉터리로 구성됩니다. 예를 들어, 서버가 Sample인 경우 이 설정은 https://sample:8006/apprecovery/admin/Core입니다.
수신 실패 제한 시간	제한 시간 전에 Agent 소프트웨어의 배포를 시도해야 하는 시간. 기본 설정은 오전 00:25:00 또는 25분입니다. 이 설정을 변경하려면 읽기 또는 쓰기 이벤트 중 시간 제한이 발생하기 전에 시스템에서 Agent 소프트웨어 배포를 시도하려는 시간의 길이를 입력합니다. HH:MM:SS 형식을 사용합니다.
최대 병렬 설치	이 설정은 Core에서 한 번에 시도할 Agent 소프트웨어의 최대 배포 횟수를 제어합니다. 기본 설정은 100입니다.

5 각 설정의 변경 내용에 만족하면 ✔ 를 클릭하여 변경 내용을 저장하고 편집 모드를 저장하거나 ✖ 를 클릭하여 저장하지 않고 편집 모드를 종료합니다.

데이터베이스 연결 설정 구성

Rapid Recovery에서는 이벤트 페이지에 Core 작업, 이벤트 및 경고에 대한 정보를 표시합니다. Rapid Recovery에서는 이 트랜잭션 정보를 MongoDB 서비스 데이터베이스에 저장하는데, 이 데이터베이스는 기본적으로 Core 시스템에 로컬로 설치됩니다. 정보가 데이터베이스에 유지되는 기간을 변경하거나, 더 많거나 더 적은 수의 동시 연결이 가능하도록 연결 풀 크기를 변경하기 위해 이 설정을 구성할 수 있습니다.

두 번째 Rapid Recovery Core를 사용하는 경우, 첫 번째 Core의 데이터베이스 연결 설정을 두 번째 Core 시스템을 가리키도록 구성할 수 있습니다. 이러한 방식으로 두 Core의 이벤트 데이터가 모두 두 번째 Core의 MongoDB에 저장됩니다.

또는 네트워크를 통해 Rapid Recovery Core에 액세스할 수 있는 MongoDB가 별도로 설치된 다른 시스템을 가리키도록 Core의 데이터베이스 연결 설정을 구성할 수 있습니다. 그런 다음 Core의 이벤트 트랜잭션 데이터는 로컬로 저장되지 않고 해당 서비스 데이터베이스에 저장됩니다. 서비스 데이터베이스에 대해 데이터베이스 연결 설정을 지정하거나 수정하는 방법에 대한 자세한 내용은 데이터베이스 연결 설정 구성을(를) 참조하십시오.

노트: Rapid Recovery Core에서 이벤트 정보를 보는 방법에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

고객은 Rapid Recovery Core의 네트워크에 액세스할 수 있는 다른 시스템에 MongoDB 서비스 데이터베이스를 설치하도록 지정할 수 있습니다. Rapid Recovery Core에 대한 서비스 데이터베이스가 Rapid Recovery Core를 호스팅하는 시스템과 다른 시스템에 설치된 경우 이 설정에 데이터베이스 자격 증명(사용자 이름과 암호)을 제공해야 합니다.

Rapid Recovery Core에서 사용하는 서비스 데이터베이스에 대한 데이터베이스 연결 설정을 수정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지 왼쪽의 Core 설정 목록에서**데이터베이스 연결**을 클릭합니다.
- Settings(설정) 페이지의 오른쪽에서 Database Connection(데이터베이스 연결) 제목이 보일 때까지 아래로 스크롤합니다.
  Database Connection(데이터베이스 연결) Core 설정이 나타납니다.

3 Database Connection(데이터베이스 연결) 설정 영역에서 다음을 수행할 수 있습니다.
- **연결 테스트**를 클릭하여 설정을 확인합니다.
  데이터베이스 연결 설정을 변경할 경우 연결 테스트를 수행하는 것이 좋습니다.
- **기본값 복원**을 클릭하여 모든 기본 데이터베이스 연결 설정을 복원합니다.
  이 작업의 수행을 확인하는 메시지가 표시되고 사용자 지정 데이터베이스 연결 설정이 중단됩니다.

4 변경하려는 설정을 클릭합니다.
사용자가 선택한 설정은 편집 가능해집니다.

5 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 17. 데이터베이스 연결 설정 정보

텍스트 상자	설명
호스트 이름	데이터베이스 연결 호스트 이름을 입력합니다. ⓘ **노트: localhost가 호스트로 지정된 매개 변수인 경우 MongoDB는 Core를 호스팅하는 시스템에 로컬로 설치됩니다.**
포트	데이터베이스 연결 포트 번호를 입력합니다. ⓘ **노트: 기본 설정은 27017입니다.**
사용자 이름	MongoDB 서비스 데이터베이스에 대한 관리자 권한이 있는 사용자의 이름을 입력합니다. ⓘ **노트: 호스트 이름 매개 변수가 localhost인 경우에는 이 필드가 필요하지 않습니다.**
암호	지정한 사용자 이름과 연결된 암호를 입력합니다. ⓘ **노트: 호스트 이름 매개 변수가 localhost인 경우에는 이 필드가 필요하지 않습니다.**
보존 기간(일)	이벤트 및 작업 기록을 서비스 데이터베이스에 보존할 기간(일 수)을 입력합니다.
최대 연결 풀 크기	동적 재사용을 허용하기 위해 캐시된 데이터베이스 연결의 최대 수를 설정합니다. ⓘ **노트: 기본 설정은 100입니다.**
최소 연결 풀 크기	동적 재사용을 허용하기 위해 캐시된 데이터베이스 연결의 최소 수를 설정합니다. ⓘ **노트: 기본 설정은 0입니다.**

6 각 설정에서 변경 내용에 만족하면 ✔ 를 클릭하여 변경 내용을 저장하고 편집 모드를 종료하거나 저장하지 않고 편집 모드를 종료하려면 ✖ 를 클릭합니다.

로컬 데이터베이스 연결 설정 수정

Events(이벤트) 페이지에서는 Rapid Recovery Core와 관련된 시스템 이벤트를 볼 수 있습니다. Rapid Recovery Core에서는 이 트랜잭션 정보를 MongoDB 서비스 데이터베이스에 저장합니다. 기본적으로 이 데이터베이스는 Core 시스템에 로컬로 설치되며, 데이터베

이스 연결 설정의 호스트 이름의 기본값은 localhost입니다. 이 상황에서 루프백 인터페이스는 로컬 네트워크 인터페이스 하드웨어를 무시하므로 데이터베이스 자격 증명이 필요하지 않습니다.

필요한 경우 보안을 강화하기 위해 Rapid Recovery Core에서 사용하는 MongoDB 데이터베이스에 대한 데이터베이스 자격 증명(사용자 이름 및 암호)을 명시적으로 지정할 수 있습니다.

노트: Rapid Recovery Core에서 이벤트 정보를 보는 방법에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오. 데이터베이스 연결 설정에 대한 자세한 내용은 데이터베이스 연결 설정 구성을(를) 참조하십시오.

데이터베이스 자격 증명을 지정하도록 로컬 데이터베이스 연결 설정을 수정하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **L로컬 데이터베이스 설정**을 클릭합니다.
- 로컬 데이터베이스 설정 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.
  로컬 데이터베이스 Core 설정이 표시됩니다.

3 변경하려는 설정을 클릭합니다.
선택한 설정을 편집할 수 있습니다.

4 다음 표에서 설명한 대로, 서비스 데이터베이스에 연결하는 경우 적절한 자격 증명을 입력합니다.

표 18. 로컬 데이터베이스 설정 정보

텍스트 상자	설명
사용자 이름	MongoDB 서비스 데이터베이스에 대한 관리자 권한이 있는 사용자의 이름을 입력합니다.
암호	지정한 사용자 이름과 연결된 암호를 입력합니다.

5 각 설정에서 변경 내용에 만족하면 를 클릭하여 변경 내용을 저장하고 편집 모드를 종료합니다. 저장하지 않고 편집 모드를 종료하려면 을 클릭합니다.

SMTP Server 설정 관리

Core에 대해 SMTP(Simple Mail Transfer Protocol) 서버 설정을 구성하는 경우 작업, 이벤트 및 경고 알림을 이메일로 보낼 수 있습니다.

SMTP 이메일 서버 구성에 대한 정보는 이메일 서버 구성 항목에 설명되어 있습니다.

노트: 이벤트 정보를 이메일로 보내려면 알림 그룹 설정도 구성해야 합니다. 이메일 경고를 받기 위해 이벤트를 지정하는 방법에 대한 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

클라우드 구성 설정 관리

Rapid Recovery에서 사용 중인 저장소 계정을 Rapid Recovery Core를 사용하여 클라우드 저장소 공급자에 연결할 수 있습니다. 이를 통해 데이터 보관 기간이 길어지는 경우 보호된 시스템에서 정보를 아카이브할 수 있습니다.

Rapid Recovery는 Amazon™ S3, Microsoft Azure 및 OpenStack 오픈 소스 기술을 사용하여 관리되는 클라우드 공급자와 통합됩니다.

Rapid Recovery Core에서 클라우드 저장소 계정 정보를 관리하는 방법에 대한 자세한 내용은 클라우드 계정 관리을(를) 참조하십시오.

보고서 설정 관리

Rapid Recovery Core 또는 보호된 시스템에 대한 보고서를 생성할 수 있습니다. 생성할 수 있는 보고서에 대한 자세한 내용은 보고서 생성 및 보기을(를) 참조하십시오.

Core 보고서에 대한 보고서 설정을 관리하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭하고 다음 중 하나를 수행합니다.

- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **보고서**를 클릭합니다.
- 보고서 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

보고서 Core 설정이 표시됩니다. 보고서 설정은 다음 표에서 설명합니다.

옵션	설명
Restore Defaults(기본값 복원)	이 옵션은 모든 보고서 설정을 기본 설정으로 복원합니다. 각 설정에 대한 기본값은 아래에 나열되어 있습니다.
글꼴	이 옵션은 보고서에 사용되는 기본 글꼴을 제어합니다. 기본값은 Trebuchet MS typeface입니다. 이 글꼴은 시스템에서 사용 가능한 typeface로 변경할 수 있습니다.
Paper size(용지 크기)	이 옵션은 보고서를 인쇄할 때 기본 용지 크기를 제어합니다. 기본값은 A4입니다. 다음 용지 크기 중에서 선택할 수 있습니다. • 문자 • Tabloid • Ledger • Legal • A3 • A4 • Executive • B4 • C3Envelope • C4Envelope
Page orientation(페이지 방향)	이 옵션은 내보낸 보고서의 페이지 방향을 제어합니다. 기본 방향은 Portrait(세로)입니다. 다음 레이아웃 옵션 중에서 선택할 수 있습니다. • Portrait(세로) • Landscape(가로)

3 보고서 설정을 변경하려면 해당 설정 필드를 클릭합니다.
설정 필드가 구성 가능한 드롭다운 메뉴로 나타납니다.

4 드롭다운 메뉴를 클릭하고 사용 가능한 값 중 하나를 선택합니다.
예를 들어, 글꼴 필드에서 **Times New Roman**을 클릭합니다.

5 각 설정에서 변경 내용에 만족하면 ✔ 를 클릭하여 변경 내용을 저장하고 편집 모드를 종료합니다. 저장하지 않고 편집 모드를 종료하려면 ✖ 을 클릭합니다.
이제 선택한 옵션은 선택한 보고서 매개 변수에 대한 새 설정으로 나타납니다.

Core SQL 연결 기능 설정 관리

SQL 연결 기능 검사는 Rapid Recovery 야간 작업 파트로 발생합니다. 라이센싱 비용을 덜어주기 위해 Rapid Recovery에서는 연결 기능 검사를 수행하는 2가지 옵션이 제공됩니다. Rapid Recovery Core 시스템에 설치된 사용이 허가된 SQL Server 인스턴스를 사용하는 방법과 보호된 시스템에 이미 설치된 SQL Server 인스턴스를 사용하는 방법이 있습니다. 이제는 이 두 번째 옵션이 기본 설정입니다. 그러나 보호된 시스템이 야간 작업이 발생하는 시간 동안 이미 실행 중이라면 Core에서 SQL Server 인스턴스로 검사를 수행할 수도 있습니다.

요약하자면 Core SQL 연결 기능 설정을 관리하는 프로세스에서 다음과 같은 작업을 수행합니다.

- 데이터베이스가 포함된 보호 그룹에 대한 최신 복구 지점을 마운트합니다.
- SQL Server에서 데이터베이스에 연결합니다.
- 데이터베이스를 엽니다.
- 데이터베이스를 닫습니다.
- 복구 지점을 분리합니다.

  야간 작업을 활성화하려면 보호된 시스템의 SQL Server 데이터베이스에 대해 연결성 검사를 수행하는 데 사용할 SQL Server 인스턴스를 지정하십시오.

노트: Core에서 SQL Server를 보호하지 않는 경우에는 이 옵션이 표시되지 않습니다.

Core가 야간 작업의 일부로 SQL 연결 기능 확인을 수행하도록 구성하려면 다음 단계를 완료하십시오.

노트: 보호된 시스템에 설치된 SQL Server 인스턴스를 사용하는 옵션을 선택하면 보호된 모든 SQL 시스템에 대한 SQL 연결 기능이 해당 SQL Server 인스턴스에서 관리됩니다. 이 설정을 보호된 모든 SQL 시스템에 적용하지 않으려면 Core에서 SQL Server 사용을 선택합니다. Core에서 연결 기능 검사를 수행하려면 사용이 허가된 SQL Server 버전을 Core 시스템에서 설치하거나 사용해야 합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지 왼쪽에 있는 Core 설정 목록에서 **연결 기능**을 클릭합니다.
- 연결 기능 제목이 표시될 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

3 보호된 SQL Server 시스템에 설치된 SQL Server 인스턴스를 사용하려면 **보호된 시스템에서 SQL Server 사용**을 선택합니다. 이것은 기본 옵션입니다.

4 Rapid Recovery Core에 설치된 SQL Server 인스턴스를 사용하려면 **Core에서 SQL Server 사용**을 선택하고 다음 표에 설명된 대로 인증 정보를 입력합니다.

표 19. SQL Server 자격 증명 정보

텍스트 상자	설명
SQL Server	SQL Server 드롭다운 메뉴의 Core 서버에서 적절한 SQL Server 인스턴스를 선택합니다.
자격 증명 유형	다음 옵션 중에서 자격 증명에 대한 적절한 인증 방법을 선택합니다. • Windows • SQL
사용자 이름	선택한 자격 증명 유형을 기반으로 Core에서 SQL Server에 액세스할 사용자 이름을 지정합니다.
암호	선택한 자격 증명 유형을 기반으로 Core에서 SQL Server에 액세스할 암호를 지정합니다.

5 **연결 테스트**를 클릭합니다.

노트: 자격 증명을 잘못 입력하면 자격 증명에 실패했다는 것을 경고하는 메시지가 표시됩니다. 자격 증명 정보를 수정하고 연결을 다시 테스트합니다.

6 변경 내용에 만족하면 **적용**을 클릭합니다.

Core 작업 이해

Core 작업은 Rapid Recovery Core가 복구 지점 백업, 데이터 복제, 데이터 보관, VM으로 데이터 내보내기, 리포지토리 유지 rhksfl 등의 작업을 지원하기 위해 수행하는 과정입니다. 설정된 일정에 따른 복제나 보관 같은 일부 작업의 경우 Core 작업이 자동으로 시작됩니다. 또한 Core Console에서 다양한 요소의 요구 사항에 따라 일부 작업을 호출할 수도 있습니다.

- Core 작업 설정을 조회하거나 편집할 때 각 Core 작업에는 2개의 매개 변수(최대 동시 작업 및 시도 횟수)가 포함되어 있습니다.
  - 최대 동시 작업 매개 변수는 해당 유형을 동시에 실행할 수 있는 작업 수를 결정합니다.
  - 시도 횟수 매개 변수는 네트워크 또는 기타 통신 오류로 인해 처음에 작업을 수행할 수 없는 경우 작업을 중단하기 전에 몇 번의 작업을 시도해야 하는지 결정합니다.
- Core 작업 표의 설정 열은 제시된 작업이 Core 작업 설정에 기본적으로 포함되어 있는지, 또는 명시적으로 추가해야 하는지 나타냅니다.

다음 표는 사용 가능한 기본 Core 작업 및 해당 기능에 대해 설명합니다.

표 20. Core 작업

작업 이름	설명	최대 동시 작업	시도 횟수	설정
스냅숏에서 SQL 데이터베이스의 연결성 검사	Core에서 SQL 데이터베이스의 일관성을 확인하고 지원되는 모든 MDF(데이터) 및 LDF(로그) 파일을 백업 스냅숏에서 사용할 수 있도록 합니다. 프로세스: · SQL 데이터베이스가 포함된 보호 그룹에 대한 최신 복구 지점을 탑재합니다. · 데이터베이스를 탑재합니다. 보호된 SQL Server에서 연결성을 수행하는 경우, UNC 경로를 사용하여 탑재합니다. · SQL Server에서 데이터베이스에 연결합니다. · 연결성 검사를 수행합니다. · 정리 작업을 수행합니다. · 데이터베이스를 닫습니다. · 데이터베이스를 탑재 해제합니다. · 복구 지점을 분리합니다.	1	0	기본값
Exchange 데이터베이스의 체크섬 검사	Exchange 데이터베이스가 포함된 복구 지점의 무결성을 검사합니다. 프로세스: · SQL 데이터베이스가 포함된 보호 그룹에 대한 최신 복구 지점을 탑재합니다. · SQL Server에서 데이터베이스에 연결합니다. · 데이터베이스를 엽니다. · 데이터베이스를 닫습니다. · 복구 지점을 분리합니다.	1	0	기본값
Exchange 데이터베이스의 탑재 기능 검사	Exchange 데이터베이스가 탑재 가능한지 검사합니다.	1	0	기본값
원격 소스에서 보호된 시스템 데이터 복제	보호된 시스템의 복구 지점 사본을 소스 Core에서 대상 Core로 전송합니다. 이 작업은 들어오는 복제된 복구 지점을 수신하는 대상 Core에서 실행합니다.	3	0	기본값

작업 이름	설명	최대 동시 작업	시도 횟수	설정
보호된 시스템 데이터를 원격 대상에 복제	보호된 시스템의 복구 지점 사본을 소스 Core(원래 저장된 위치)에서 대상 Core로 전송합니다. 이 작업은 소스 Core에서 실행되며 보내는 복제를 제어합니다.	1	3	기본값
복구 지점 롤업	보존 정책에서 정의한 일정에 따라 복구 지점을 결합하거나 롤업하여 백업 데이터에 보존 정책을 적용합니다.	1	0	기본값
복구 지점 검사	복구 지점의 무결성을 검사합니다.	1	0	추가
모든 복구 지점 삭제	보호된 시스템의 전체 복구 지점을 삭제합니다.	1	0	추가
복구 지점 체인 삭제	보호된 시스템의 전체 복구 지점망을 삭제합니다.	1	0	추가
복구 지점의 범위 삭제	복구 지점 식별기나 날짜 범위에 따라 보호된 시스템의 복구 지점 집합을 삭제합니다.	1	0	추가
Agent 소프트웨어를 시스템에 배포	Rapid Recovery Agent 소프트웨어를 지정된 시스템이나 시스템에 배포합니다.	1	0	추가
Exchange 라이브러리 다운로드	Microsoft Exchange 라이브러리 다운로드를 보호된 시스템에서 Core 시스템으로 다운로드합니다(경로: C:\programdata\apprecovery\ exchangelibraries).	1	0	추가
아카이브에 내보내기	선택한 복구 지점의 아카이브를 사용하여 지정된 경로에 백업을 생성합니다. 프로세스: · 복구 지점 마운트. · 백업에 데이터를 작성합니다. · 복구 지점을 분리합니다.	1	0	추가
가상 시스템으로 내보내기	보호된 시스템의 지정된 복구 지점에서 가상 시스템으로서의 대상 경로로 데이터를 내보냅니다. 프로세스: · 복구 지점을 탑재합니다. · 대상 경로의 복구 지점 데이터에서 가상 시스템을 생성합니다. · 복구 지점을 분리합니다.	1	0	추가
아카이브 가져오기	이전에 생성한 Core 아카이브의 지정된 백업에서 복구 지점을 가져옵니다.	1	0	추가
리포지토리 유지	리포지토리의 검사를 수행합니다. 프로세스: · 리포지토리 파일 시스템을 검사합니다. · 복구 지점을 탑재합니다. · 리포지토리에 대한 중복 제거 캐시를 다시 계산합니다. · 리포지토리에서 복구 지점을 로드합니다.	1	0	추가
복구 지점 스냅숏 탑재	지정된 경로에 복구 지점 탑재를 수행합니다.	1	0	추가
ESX® 가상 시스템 보호	지정된 모든 가상 시스템을 에이전트 없는 보호에 추가합니다.	1	0	추가

작업 이름	설명	최대 동시 작업	시도 횟수	설정
	Protect Multiple Machines Wizard(다중 시스템 보호 마법사)를 사용하여 한 개 이상의 VM에 대한 에이전트 없는 보호를 Core에 추가하면 작업이 즉시 수행됩니다. 작업은 지정된 VM에 대한 ID 번호를 설정하고 Core에 대한 정보를 구성 파일에 작성하거나 파일에서 메타데이터를 검색합니다.			
복구 지점에서 복원	복구 지점에서 지정된 대상 시스템으로 복원하는 작업을 수행합니다. 프로세스: · 복구 지점을 탑재합니다. · 복구 지점의 모든 데이터를 지정된 시스템에 작성합니다. · 복구 지점을 분리합니다.	1	0	추가
로그 업로드	지정된 서버에 로그를 업로드합니다.	1	0	추가

일부 Core 작업은 설정에 포함되어 있습니다. 작업 설정을 통해 Core가 실행할 수 있는 동일한 유형의 동시 작업 개수를 지정하고 첫 번째 작업이 실패한 경우 재시도를 몇 번 해야 하는지 지정합니다.

이러한 설정에 대한 자세한 내용은 Core 작업 설정에서 확인하십시오.

작업을 Core 설정에 추가하는 방법은 설정에 Core 작업 추가을(를) 참조하십시오.

설정 목록에 있는 작업의 설정을 편집하는 방법은 Core 작업 설정 편집을(를) 참조하십시오.

Core 작업 설정

아이콘 표시줄에서 (설정)을 선택하면 일부 Core 작업을 위한 설정에 액세스할 수 있습니다. Core 설정 페이지의 **Jobs(작업)** 영역에서는 나열된 각 작업 유형에 대해 다음 두 가지 설정을 결정할 수 있습니다.

1 Core에서 한 번에 시도할 이 유형의 최대 작업 수. 1과 50 사이의 값을 설정해야 합니다.
2 네트워크 또는 기타 통신 오류로 인해 처음에 작업을 수행할 수 없는 경우 작업 시도 횟수. 0과 10 사이의 값을 설정해야 합니다.

Core 설정에는 여러 작업이 자동으로 포함됩니다. 이러한 작업은 Settings(설정) 열에 "Default(기본값)" 값이 포함됩니다(Core 작업 이해 항목 참조).

최대 작업 수 또는 이러한 기능의 재시도 횟수를 제어하기 위해 설정을 구성하려는 경우, 일부 다른 작업을 설정에 추가할 수 있습니다. 이러한 작업은 Settings(설정) 열에 "Add(추가)" 값이 포함됩니다. 이러한 작업을 설정 표에 추가하는 방법에 대한 자세한 내용은 설정에 Core 작업 추가을(를) 참조하십시오

Settings(설정)에서 사용할 수 없는 Core 작업은 이 두 가지 매개변수를 설정하는 기능을 제공하지 않습니다.

Settings(설정)에 나열되는 작업은 기존 설정을 편집할 수 있습니다. 이를 통해 두 가지 매개변수를 사용자 지정하거나 작업 설정 목록에서 작업 유형을 삭제하거나 기본 설정을 복원할 수 있습니다. 자세한 내용은 Core 작업 설정 편집 항목을 참조하십시오.

설정에 Core 작업 추가

Core 작업 설정을 통해 각 작업 유형에 대해 Core에서 한 번에 시도할 수 있는 최대 작업 수와 첫 번째 시도에 실패한 경우 작업을 다시 시도하는 횟수를 정의할 수 있습니다.

각 Core 작업 유형은 Core 작업 설정 항목에서 설명한 대로, 이 두 가지 매개 변수에 대한 기본값을 보유하고 있습니다. 또한 이 목록은 기본적으로 Core 설정에 포함하는 작업 유형을 표시합니다.

설정에 Core 작업을 추가하면 추가한 작업 유형에 대한 이 매개 변수를 변경할 수 있습니다.

Core 설정에 작업을 추가하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭하고 다음 중 하나를 수행합니다.
- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **작업**을 클릭합니다.
- 작업 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

작업 Core 설정이 표시됩니다.

3 Core 설정 페이지의 작업에서 **추가**를 클릭합니다.
작업 설정 대화 상자가 나타납니다.

4 **작업 설정** 대화 상자의 **작업** 필드에서 Core 설정에 추가할 작업의 이름을 선택합니다.
이러한 작업은 Core 작업 설정 항목에서 설명합니다.

5 Core에서 한 번에 시도할 수 있는 최대 작업 수를 설정하려면 **최대 동시 작업 수** 텍스트 상자에 1과 50 사이의 새 값을 입력합니다.

6 Core에서 작업을 중단하기 전에 시도해야 하는 횟수를 설정하려면 **시도 횟수** 텍스트 상자에 0과 10 사이의 새 값을 입력합니다.

7 **저장**을 클릭합니다.
작업 설정 대화 상자가 닫히고 새로운 작업 설정이 적용됩니다.

Core 작업 설정 편집

Core 작업을 설명하면 작업 유형별로 한 번에 시도할 수 있는 Core에 대한 최대 작업 수와 첫 번째 시도가 실패한 경우 재시도해야 하는 작업 횟수를 정의할 수 있습니다.

Core 작업 이해 항목에 설명된 대로 Core 작업 유형마다 이러한 두 매개 변수의 기본값이 있습니다. 이 목록에는 Core 설정에 기본적으로 포함되는 작업 유형도 표시됩니다. Core 작업 설정을 편집하면 다음을 수행할 수 있습니다.

- Core 작업 유형별로 설정을 사용자 지정할 수 있습니다.
- Core 설정 목록에서 작업 유형을 삭제할 수 있습니다. 작업 유형이 설정에 기본적으로 포함된 경우에는 이 기능을 사용할 수 없습니다.

노트: Core 설정에서 작업을 삭제하기만 하면 이 목록에서 작업 유형이 제거됩니다. 나중에 해당 작업 유형에 대한 Core 설정을 다시 편집하려면 설정에 Core 작업 추가 항목에 설명된 대로 리스트에 해당 작업 유형을 추가할 수 있습니다.

- 어떠한 작업 유형이든 기본 설정으로 설정을 복원할 수 있습니다.

노트: Core 설정에 기본적으로 포함된 작업 유형에 대해서만 이 기능을 사용할 수 있지만, 다른 작업 유형도 목록에서 제거했다가 다시 추가하면 기본값으로 설정할 수 있습니다.

작업 설정을 편집하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 을 클릭하고 (설정) 다음 중 하나를 수행합니다.
- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **작업**을 클릭합니다.
- 설정 페이지의 오른쪽에서 작업 제목이 표시될 때까지 아래로 스크롤합니다.

작업 코어 설정이 표시됩니다.

3 제거하려는 작업을 작업 그리드의 목록 중에서 선택합니다. 해당 작업에 대한 드롭다운 메뉴 중에서 **삭제**를 선택합니다.
목록에서 작업이 제거됩니다.

4 설정을 재설정하려는 작업을 작업 그리드의 목록 중에서 선택합니다. 해당 작업에 대한 드롭다운 메뉴 중에서 **기본값으로 재설정**을 선택합니다.

이 작업에 대한 작업 설정이 기본 설정으로 재설정됩니다.

5 변경하려는 작업을 작업 그리드에서 선택합니다. 해당 작업에 대한 드롭다운 메뉴 중에서 **편집**을 선택합니다.

6 작업 설정: [JobName] 대화 상자가 열립니다.

7 Core에서 한 번에 시도할 수 있는 최대 작업 수를 변경하려면 최대 동시 작업 수 텍스트 상자에 1과 50 사이의 새 값을 입력합니다.

8 Core에서 작업을 중단하기 전에 시도해야 하는 횟수에 대한 설정을 변경하려면 시도 횟수 텍스트 상자에 1과 10 사이의 새 값을 입력합니다.

9 **저장**을 클릭합니다.

작업 설정 대화 상자가 닫히고 새로운 작업 설정이 적용됩니다.

라이센스 관리

많은 Rapid Recovery Core 사용자가 기능이 제한된 평가판 라이센스로 시작합니다. 평가판 라이센스는 14일간 유효하며 그룹 관리자가 이 평가판 라이센스를 28일 라이센스로 한 번 연장할 수 있습니다. 평가 기간이 만료된 후 Rapid Recovery Core는 사용자가 유효한 라이센스를 얻을 때까지 스냅숏 작성을 중지합니다.

노트: 라이센스 키 또는 파일 정보(예: 평가판 라이센스를 유효한 장기 사용 라이센스로 업데이트 또는 변경)에 대한 자세한 내용은 라이센스 업데이트 또는 변경을(를) 참조하십시오.

라이센스 파일 또는 라이센스 키로 라이센스가 확인됩니다.

라이센스 파일은 .lic 파일 확장자로 끝나는 텍스트 파일입니다. 라이센스 파일의 예는 다음과 같습니다.

- 라이센스 파일은 각각 하이픈으로 구분된 세 개의 숫자 그룹으로 구성된 9자로 표시될 수 있습니다. 예를 들어, `123-456-789.lic`입니다.
- 소프트웨어 기반 라이센스는 고객 이름 또는 계정으로 명명된 그룹이 포함된 Software-<Group name>.lic 형식으로 표시될 수 있습니다. 예를 들어, `Software-YourCompany.lic`입니다.
- Dell 어플라이언스 라이센스는 고객 이름 계정으로 명명된 그룹이 포함된 <Appliance Series>-<Group name>.lic 형식으로 표시될 수 있습니다. 예를 들어, `DL4X00 Series-YourCompany.lic`입니다.

라이센스 키는 각각 하이픈으로 구분된 6개의 영숫자 문자 그룹으로, 길이는 30자입니다. 예를 들어, 샘플 라이센스 키 형식은 `ABC12-DEF3G-H45IJ-6K78L-9MN10-OPQ11`입니다.

Rapid Recovery를 사용하여 라이센스를 관리하거나 아이콘 표시줄에서 (설정)을 선택하고 **라이센싱**을 클릭하여 Core Console에서 직접 라이센스 서버에 연결할 수 있습니다.

라이센스 설정에는 다음과 같은 정보가 포함됩니다.

라이센스 세부 정보:

- **라이센스 변경**. 라이센스 파일을 업로드하거나 라이센스 키를 입력하여 Core와 연결된 기존 라이센스를 변경할 수 있습니다.
- **라이센스 추가**. 이 옵션은 Dell 백업 어플라이언스에서만 사용할 수 있으며 라이센스 파일을 업로드하거나 라이센스 키를 입력할 수 있습니다.
- **라이센스 포털 그룹**. 이 옵션은 그룹 관리를 위한 라이센스 포털을 엽니다.
- **라이센스 유형**. 라이센스 유형에는 평가판, 구독, 엔터프라이즈가 있습니다. 자세한 내용은 Dell Data Protection | Rapid Recovery License Portal 사용 설명서에 있는 Dell Data Protection | Rapid Recovery License Portal 소프트웨어 라이센스 정보 항목을 참조하십시오.
- **라이센스 상태**. 라이센스의 상태를 나타냅니다. 활성 상태에서는 스냅숏을 일정에 따라 계속 만들 수 있습니다. 라이센스가 차단 또는 만료되거나 Core에서 유예 기간 후 Dell Data Protection | Rapid Recovery License Portal과 통신할 수 없는 경우에는 라이센스 상태가 수정될 때까지 스냅숏이 일시 중지됩니다.

라이센스 제약 조건:

- **일일 최대 스냅숏**. 특정 라이센스에서 제한되는 백업 수를 나타냅니다.

라이센스 풀:

- **풀 크기**. 라이센스 풀은 Dell Data Protection | Rapid Recovery License Portal의 그룹 및 하위 그룹에 할당할 수 있는 비평가판 라이센스의 수입니다. 풀의 크기에 따라 할당할 수 있는 라이센스 수가 결정됩니다. 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 사용 설명서*에 있는 "라이센스 풀 이해" 항목을 참조하십시오.
- **이 Core에 의해 보호되는 시스템 수**. 라이센스 풀에서 이 Core에 의해 보호되는 시스템의 수를 나타냅니다.
- **그룹 내 보호되는 시스템의 총 수**. 이 Core와 동일한 라이센스 그룹 내에서 보호되는 시스템의 총 수를 나타냅니다.

라이센스 서버. 이 설정은 표준(phone home) 라이센스에 적용됩니다. 이 설정은 어플라이언스 및 기타 phone-home이 아닌 라이센스에 적용할 수 없습니다.

- **라이센스 서버 주소**. 이 Core와 연결된 라이센스 서버의 활성 URL을 표시합니다.
- **라이센싱 서버의 마지막 응답**. 라이센스 서버 포털과 마지막으로 시도한 통신이 성공했는지 여부를 나타냅니다.
- **라이센싱 서버와 마지막으로 연결한 시간**. 라이센스 서버와 마지막으로 접속에 성공한 날짜와 시간을 표시합니다.
- **다음 라이센스 서버 접속 시도**. 다음에 라이센스 서버와 통신을 시도할 날짜와 시간을 표시합니다.
- **지금 연결**. 이 단추는 요청 시 라이센스 서버에 연결합니다. 라이센스 구성을 변경한 후 다음 예약 시도를 기다리지 않고 바로 변경 사항을 등록하려는 경우 이 옵션을 사용합니다.

라이센스에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 사용 설명서*를 참조하십시오.

라이센스 키 또는 파일을 추가하거나 변경하는 방법에 대한 자세한 내용은 라이센스 업데이트 또는 변경을(를) 참조하십시오.

라이센스 포털 서버에 연결하는 방법에 대한 자세한 내용은 다음을 참조하십시오. Dell Data Protection | Rapid Recovery License Portal 서버 연결

보호된 시스템 하나에 대한 라이센스 정보도 볼 수 있습니다, 자세한 내용은 시스템에 대한 라이센스 정보 보기을(를) 참조하십시오.

라이센스 업데이트 또는 변경

장기 Rapid Recovery 라이센스를 업그레이드 또는 구입하면 라이센스 파일 또는 라이센스 키 중 하나가 이메일로 수신됩니다.

평가판 라이센스를 업그레이드하거나 기존 라이센스를 변경하려면 이 절차에서 단계를 완료하고 라이센스를 Rapid Recovery Core Console과 연결합니다.

노트: Dell 백업 어플라이언스 사용자도 필요하면 Core에 라이센스를 추가할 수 있습니다. 자세한 내용은 라이센스 추가을(를) 참조하십시오.
라이센스 키를 확보하는 방법에 관한 자세한 내용 또는 라이센스 포털을 이용하여 소프트웨어를 다운로드하고, 어플라이언스를 등록하며, 라이센스 구독 및 라이센스 그룹을 관리하고, 라이센스 포털 보고서를 생성하는 방법에 관한 세부 정보는 *Dell Data Protection | Rapid Recovery License Portal 사용 설명서*를 참조하십시오.

새 Core를 이제 막 설치했는데 라이센스 파일 또는 키 중에서 선택하라는 메시지가 표시되면 5단계로 건너뜁니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 을 클릭하고 (설정)을 클릭합니다.

3 **설정** 페이지의 오른쪽에서 라이센싱 제목이 표시될 때까지 아래로 스크롤합니다.
라이센싱에 대한 Core 설정이 표시됩니다.

4 Core와 연결된 기존 라이센스를 업데이트 또는 변경하려면 라이센스 세부 정보 코어 설정 영역의 상단에서 **라이센스 변경**을 클릭합니다.
Change License(라이센스 변경) 대화 상자가 표시됩니다.

5 라이센스 키를 입력하거나 라이센스 파일을 업로드하려면 다음 중 하나를 수행합니다.

a 라이센스 키를 *수동으로 입력*하려면 라이센스 변경 대화 상자에서 키를 정확하게 입력한 다음 **계속**을 클릭합니다.
대화 상자가 닫히고, 선택한 라이센스 파일이 인증되고, 해당 라이센스가 Core와 연결됩니다.

b 라이센스 파일을 *업로드*하려면 라이센스 변경 대화 상자에서 **파일 선택**을 클릭합니다.
파일 업로드 대화 상자에서 파일 시스템을 탐색하여 사용하려는 새 라이센스를 찾습니다. 예를 들면, `Software-YourCompany.lic`를 찾습니다.

c 라이센스 파일과 **열기**를 차례로 클릭합니다.
파일 업로드 대화 상자가 닫힙니다. 선택한 라이센스 파일이 라이센스 변경 대화 상자에 표시됩니다.

d **라이센스 변경** 대화 상자에서 **계속**을 클릭합니다.
대화 상자가 닫히고, 선택한 라이센스 파일이 인증되고, 해당 라이센스가 Core와 연결됩니다.

6 설정 페이지의 오른쪽에서 라이센스 서버 제목이 표시될 때까지 아래로 스크롤합니다.
라이센싱 코어 설정이 표시됩니다.

7 라이센스 서버 영역에서 **지금 연결**을 클릭합니다.
라이센스가 라이센스 서버에 적용되면 연결되어 있는 보호된 시스템이 모두 새 라이센스로 자동 업데이트됩니다.

라이센스 추가

Dell 백업 어플라이언스 소유자는 Rapid Recovery Core Console에 하나 이상의 라이센스를 추가할 수 있습니다.

Rapid Recovery 라이센스를 업그레이드하거나 구입하면 라이센스 파일 또는 라이센스 키를 받습니다.

기존 라이센스를 Core Console에서 업데이트하거나 변경할 수도 있습니다. 자세한 내용은 라이센스 업데이트 또는 변경을(를) 참조하십시오.

노트: Add Appliance(어플라이언스 추가) 단추는 Dell 백업 어플라이언스 사용자만 볼 수 있습니다.

노트: 라이센스 키를 얻는 방법에 대한 내용은 *Dell Data Protection | Rapid Recovery License Portal User Guide*를 참조하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭합니다.

3 라이센스 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.
라이센스에 대한 Core 설정이 나타납니다.

4 라이센스를 추가하고 Core에 연결하려면 라이센스 상세 정보 Core 설정 영역 맨 위에서 **라이센스 추가**를 클릭합니다. **라이센스 추가** 대화 상자**에서** 다음 중 하나를 수행합니다.

a 라이센스 키를 *직접 입력*하려면 라이센스 변경 대화 상자에서 키를 올바르게 입력하고 **계속**을 클릭합니다.
대화 상자를 닫고 선택한 라이센스 파일을 인증한 후 해당 라이센스를 Core에 연결합니다.

b 라이센스 파일을 *업로드*하려면 라이센스 변경 대화 상자에서 **파일 선택**을 클릭합니다.
파일 업로드 대화 상자에서 파일 시스템으로 이동하고 사용하려는 새 라이센스 파일을 찾습니다. 예를 들어, `Software-YourCompany.lic`를 찾습니다.

c 라이센스 파일을 클릭하고 **열기**를 클릭합니다.
파일 업로드 대화 상자를 닫습니다. 라이센스 변경 대화 상자에 선택한 라이센스 파일이 나타납니다.

d **라이센스 변경** 대화 상자에서 **계속**을 클릭합니다.
대화 상자를 닫고 선택한 라이센스 파일을 인증한 후 해당 라이센스를 Core에 연결합니다.

5 라이센스 서버 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.
라이센스 Core 설정이 표시됩니다.

6 라이센스 서버 영역에서 **지금 연결**을 클릭합니다.
라이센스가 라이센스 서버에 적용되면 연결되어 있는 보호된 시스템이 새 라이센스로 자동 업데이트됩니다.

Dell Data Protection | Rapid Recovery License Portal 서버 연결

Rapid Recovery Core Console은 Dell Data Protection | Rapid Recovery License Portal에서 변경한 내용을 최신 상태로 유지하기 위해 포털 서버에 자주 연결합니다.

비평가판 라이센스의 경우 Rapid Recovery Core에서 한 시간에 한 번씩 License Portal에 연결합니다. 10일 간의 유예 기간 후 License Portal에 연결할 수 없으면 Core는 스냅숏 작성을 중지합니다.

일반적으로, License Portal 서버와의 통신은 지정된 간격으로 자동 발생하지만 요청 시 통신을 시작할 수 있습니다.

License Portal 서버에 접속하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.
2 아이콘 표시줄에서 **설정**을 클릭한 다음 License Server 머리글을 볼 수 있을 때까지 **설정** 페이지의 오른쪽에서 아래 방향으로 스크롤합니다.
3 License Server 영역에서 **지금 접속**을 클릭합니다.

SNMP 설정 이해

SNMP(Simple Network Management Protocol)는 IP 네트워크에서 장치를 관리하기 위한 프로토콜입니다. SNMP는 네트워크의 장치에 주의가 필요한 상태인지 모니터링하기 위해 주로 사용됩니다. 이 프로토콜은 소프트웨어 구성 요소(에이전트)를 사용하여 관리 컴퓨터(관리자)에 정보를 보고합니다. SNMP 에이전트는 관리자의 요청을 처리하여 특정 매개 변수를 가져오거나 설정합니다. SNMP 에이전트는 관리자에게 트랩(특정 이벤트에 대한 알림)을 보낼 수도 있습니다.

SNMP 에이전트에서 관리하는 데이터 객체는 OID(Object Identifier)를 포함하는 MIB(Management Information Base)로 구성됩니다. 각 OID는 SNMP를 사용하여 읽거나 설정할 수 있는 변수를 식별합니다.

Rapid Recovery는 SNMP 버전 1.0에 대한 지원을 포함합니다.

Rapid Recovery Core를 SNMP 에이전트로 구성할 수 있습니다. 그런 다음 Core에서 경고, 리포지토리 상태, 보호된 시스템과 같은 정보를 보고할 수 있습니다. SNMP 호스트는 SNMP 브라우저라는 독립형 응용 프로그램을 사용하여 이 정보를 읽을 수 있습니다. SNMP 브라우저는 네트워크를 통해 Rapid Recovery Core에 액세스할 수 있는 모든 시스템에 설치할 수 있습니다.

Core SNMP 이벤트 알림을 SNMP 브라우저에서 수신할 수 있도록 하려면 SNMP 트랩에서 알리도록 알림 그룹의 알림 옵션을 올바르게 구성했는지 확인합니다.

노트: 이때 기본 그룹을 사용하거나 사용자 지정 알림 그룹을 만들 수 있습니다. 프로세스는 동일합니다.

알림 그룹을 열고 **알림 옵션** 탭을 선택하고 **SNMP 트랩에서 알림** 옵션이 활성화되었는지 확인합니다. 알림 그룹은 기본적으로 트랩 번호 1을 지정합니다. 필요한 경우 SNMP 브라우저에서 예상하는 설정과 일치하도록 트랩 번호를 변경할 수 있습니다.

알림 옵션 구성에 대한 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

또는 Rapid Recovery Core에서 MIB 파일을 다운로드할 수 있습니다. 이 파일은 Core에서 직접 수신하는 데이터보다 더 쉽게 SNMP 브라우저에서 읽을 수 있습니다.

이 항목은 다음과 같이 구성되어 있습니다.

- SNMP 설정 구성
- SNMP MIB 파일 다운로드

SNMP 설정 구성

Core와 SNMP 브라우저 간의 통신을 제어하려면 SNMP 설정을 사용하십시오. 이 설정에는 SNMP 포트와 트랩 수신기 포트, 트랩 수신기의 호스트 이름이 포함됩니다.

Core에 대한 SNMP 설정을 구성하려면 다음 절차를 사용하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭한 후 다음 중 하나를 수행합니다.
- Settings(설정) 페이지 왼쪽의 Core 설정 목록에서 **SNMP Configuration(SNMP 구성)**을 클릭합니다.
- SNMP Configuration(SNMP 구성) 제목이 보일 때까지 Settings(설정) 페이지의 오른쪽을 아래로 스크롤합니다. SNMP 구성 설정이 나타납니다.

3 다음 표에 설명된 대로 SNMP 설정을 수정합니다.

표 21. SNMP 연결 설정 정보

텍스트 상자	설명
수신 포트	SNMP 연결을 위한 포트 번호를 입력합니다. **노트: 기본 설정은 8161입니다.**
트랩 수신기 포트	트랩 수신기의 포트 번호를 입력합니다. 기본 설정은 162입니다.
트랩 수신기 호스트 이름	SNMP 연결을 위한 호스트 이름을 입력합니다. **노트: 기본 호스트 이름은 localhost입니다.**

4 각 설정을 변경한 후에는 ✔ 를 클릭하여 변경 사항을 저장하고 편집 모드를 종료하거나 ✖ 를 클릭하여 저장하지 않고 편집 모드를 종료합니다.

SNMP MIB 파일 다운로드

SNMP(Simple Network Management Protocol)는 네트워크의 장치에서 주의를 요하는 조건을 모니터링하는 데 사용됩니다. Rapid Recovery Core가 SNMP 에이전트로 설정된 경우 Core는 경고, 리포지토리 상태, 보호된 시스템과 같은 정보를 보고합니다. 이 정보는 SNMP 브라우저라는 독립형 응용프로그램을 사용하는 SNMP 호스트에서만 읽을 수 있습니다.

SNMP 에이전트에서 관리하는 데이터 객체는 OID(Object Identifier)를 포함하는 MIB(Management Information Base)로 구성됩니다. 각 OID는 SNMP를 사용하여 읽거나 설정할 수 있는 변수를 식별합니다.

Rapid Recovery Core에서 MIB 파일을 다운로드할 수 있습니다. 이름이 dell-aa-core.mib인 이 파일은 Core에서 직접 수신하는 데이터보다 더 쉽게 SNMP 브라우저에서 읽을 수 있습니다.

이 절차를 사용하여 Rapid Recovery Core에서 SNMP MIB 파일을 다운로드합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭하고 **다운로드**를 클릭합니다.
다운로드 페이지가 나타납니다.

3 Other Files(기타 파일) 창에서 아래로 스크롤합니다.

4 MIB 파일을 다운로드하려면 **SNMP MIB 파일** 다운로드 링크를 클릭합니다.

SNMP 구성 설정이 나타납니다.

5 **dell-aa-core.mib 열기** 대화 상자에서 다음 중 하나를 수행합니다.

- 로그 파일을 열려면 연결 프로그램을 선택하고 텍스트 기반 MIB 파일을 볼 SNMP 브라우저 응용 프로그램을 선택하고 마지막으로 **확인**을 클릭합니다.

  dell-aa-core.mib 파일은 선택한 응용 프로그램에서 열립니다.
- 로컬로 파일을 저장하려면 **파일 저장**을 선택하고 **확인**을 클릭합니다.

  dell-aa-core.mib 파일은 Downloads(다운로드) 폴더에 저장됩니다. 이 파일은 SNMP 브라우저 또는 텍스트 편집기를 사용하여 열 수 있습니다.

vSphere 설정 구성

VMware vSphere는 가상화 소프트웨어 제품군으로, 여기서 ESXi 또는 vCenter Server 가상 시스템을 관리할 수 있습니다. vSphere를 사용하면 더 이상 Rapid Recovery Agent 소프트웨어를 보호하기 위해 개별 VM으로 로드하지 않아도 됩니다. 이 기능을 에이전트 없는 보호 기능이라고 하며, 가상 시스템에만 적용합니다.

Core에 대한 vSphere 설정을 구성하려면 다음 절차를 사용합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭하고 다음 중 하나를 수행합니다.

- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **vSphere**를 클릭합니다.
- vSphere 제목이 나올 때까지 설정 페이지 오른쪽에서 아래로 스크롤합니다.

  vSphere 설정이 표시됩니다.

3 다음 표에서 설명한 대로 vSphere 설정을 수정합니다.

표 22. vSphere Core 설정 정보

UI 요소	UI 유형	설명
Connection lifetime(연결 수명)	스핀 상자	ESXi 서버와 연결하는 경우 제한 시간에 도달하기 전 시간을 설정합니다. HH:MM:SS 형식을 사용합니다. ⓘ **노트: 기본 설정은 00:10:00 또는 10분입니다.**
Maximum simultaneous consolidations(최대 동시 통합 수)	텍스트 필드	보호된 가상 시스템에 대한 최대 동시 통합 수를 설정합니다. ⓘ **노트: 기본 설정은 0입니다.**
Maximum retries(최대 다시 시도 횟수)	텍스트 필드	가상 디스크에 대한 연결 또는 제한 시간에 도달하기 전 읽기 및 쓰기 작업을 시도하는 최대 횟수를 설정합니다. ⓘ **노트: 기본 설정은 10회입니다.**
Allow parallel restore(병렬 복원 허용)	부울(확인란)	이 옵션을 선택하면 에이전트 없는 가상 시스템에 대해 병렬 복원을 활성화합니다. 이 옵션을 해제하면 이 기능은 비활성화됩니다. ⓘ **노트: 기본 설정은 아니오(해제됨)입니다.**

4 각 설정에서 변경 내용에 만족하면 체크 표시를 클릭하여 변경 내용을 저장하고 편집 모드를 종료하거나 저장하지 않고 편집 모드를 종료하려면 **X**를 클릭합니다.

Core 설정 백업 및 복원

Core 설정 정보를 파일에 백업했다가 나중에 Core 시스템에 문제가 있거나 다른 시스템에 설정을 마이그레이션하려는 경우 이 설정을 복원할 수 있습니다. 백업되는 정보에는 리포지토리 메타데이터(예: 리포지토리 이름, 데이터 경로, 메타데이터 경로), Core에서 보호되는 시스템, 복제 관계(대상 및 소스), 가상 대기로 구성되는 시스템 및 암호화 키에 대한 정보가 포함됩니다.

이 프로세스는 구성 설정만 복원하고 데이터는 복원하지 않습니다. 인증 자격 증명과 같은 보안 정보는 구성 파일에 저장되지 않습니다. Core 구성 파일에 저장할 때 보안 위험은 없습니다.

노트: 먼저 Core 설정 정보를 백업해야 이 프로세스를 사용하여 Core 설정을 복원할 수 있습니다.

Core 설정을 백업하고 복원하려면 이 절차를 수행합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 클릭합니다.

Settings(설정) 페이지가 나타납니다. 설정 창 상단의 설정 범주 위에 설정 백업 및 설정 복원, 두 개의 단추가 표시됩니다.

3 Core 설정을 백업하려면 4단계로 이동합니다. Core 설정을 복원하려면 6단계로 이동합니다.

4 현재 설정을 XML 파일로 백업하려면 설정 페이지 상단에서 **설정 백업**을 클릭합니다.

Core 구성 백업 대화 상자가 나타납니다.

5 로컬 경로 텍스트 상자에 Core 설정을 XML 파일로 저장할 Core 시스템에 로컬로 액세스 가능한 디렉터리 경로를 입력한 다음 **백업**을 클릭합니다.

예를 들어, `C:\Users\Your_User_Name\Documents\AA5CoreSettings`를 입력한 후 **백업**을 클릭합니다.

AppRecoveryCoreConfigurationBackup.xml이라는 파일이 지정한 로컬 대상에 저장됩니다.

6 이전에 이 방법을 사용하여 저장된 백업 XML 파일에서 Core 설정을 복원하려면 다음 단계를 수행하십시오.

노트: Core 구성 설정을 복원하면 Rapid Recovery Core 서비스가 다시 시작됩니다.

a **설정** 페이지 상단에서 **복원**을 클릭합니다.

Core 구성 복원 대화 상자가 나타납니다.

b **로컬 경로** 텍스트 상자에 Core 구성 설정을 저장한 위치의 로컬 경로를 입력합니다.

예를 들어, `C:\Users\Your_User_Name\Documents\AA5CoreSettings`를 입력합니다.

c 리포지토리 정보를 복원하지 않으려면 g단계로 이동합니다.

d (선택 사항) 백업 파일에 구성된 대로 리포지토리 정보를 복원하려면 **리포지토리 복원**을 선택한 다음 **복원**을 클릭합니다.

리포지토리 복원 대화 상자가 나타납니다.

백업된 구성 데이터에서 리포지토리 정보를 복원하는 경우 Core 설정이 저장될 때 구성된 모든 리포지토리가 확인을 위해 표시됩니다. 기본적으로 기존 리포지토리가 선택됩니다.

e 복원할 리포지토리 정보를 확인합니다. 확인 목록에 여러 리포지토리가 표시되지만 일부 리포지토리의 정보만 복원하려면 원하지 않는 리포지토리의 선택을 취소합니다.

f 복원할 리포지토리를 모두 선택하면 **저장**을 클릭합니다.

리포지토리 복원 대화 상자가 닫힙니다.

g **리포지토리 복원** 대화 상자에서 **복원**을 클릭합니다.

리포지토리 복원 대화 상자가 닫히고 복원 프로세스를 시작합니다. 리포지토리 서비스 구성이 변경되었다는 경고가 나타납니다.

h 구성 설정을 복원할 수 없는 경우 오류 메시지가 표시됩니다. 사용자의 작업이 필요한지 확인하려면 오류의 세부 정보를 검토합니다. 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오. 계속하려면 **닫기**를 클릭하여 오류 대화 상자를 닫습니다.

i 구성을 복원한 후 다음 사항을 확인합니다.

- 모든 암호화 키의 잠금을 해제합니다. 자세한 내용은 암호화 키 잠금 해제을(를) 참조하십시오.

- 네트워크 대상에 VM을 계속 업데이트하도록 가상 대기가 구성되어 있는 경우 가상 대기 설정에 네트워크 자격 증명을 지정해야 성공적으로 동기화할 수 있습니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.
- 클라우드 저장소 계정에 아카이브하도록 예약된 아카이브가 구성되어 있는 경우 자격 증명을 지정해야 Core를 클라우드 계정에 연결할 수 있습니다. Core를 클라우드 저장소 계정에 연결하는 방법에 대한 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.
- 복제가 설정되고 대상 Core에 복원하려면 소스 Core에서 대상 Core 설정(특히, 호스트)을 확인합니다. Core를 자체적으로 관리할 경우 자세한 내용은 자체 관리 대상 Core로 복제을(를) 참조하십시오. 타사에서 관리하는 Core로 복제할 경우 타사 대상 Core로 복제을(를) 참조하십시오.
- SQL 연결 기능 검사가 구성되어 있고 검사를 수행하는 SQL Server 인스턴스가 Core 시스템에 있는 경우, 연결 기능 설정에 SQL 자격 증명을 지정합니다. 자세한 내용은 Core SQL 연결 기능 설정 관리을(를) 참조하십시오.

  Replay 엔진 구성이 복원되었는지 확인하고 효과적으로 통신할 수 없는 경우 설정을 업데이트합니다. 자세한 내용은 Replay 엔진 설정 구성을(를) 참조하십시오.

코어 수준 도구

Core 설정을 구성하는 작업 외에도 다음 표에 설명된 Core 수준 도구를 사용할 수 있습니다.

표 23. 다른 코어 수준 도구

UI 요소	설명
시스템 정보	Rapid Recovery에서는 시스템 정보, 로컬 볼륨, 탑재된 볼륨, Replay 엔진 연결 등 Rapid Recovery Core에 대한 정보를 제공합니다. 시스템 정보 페이지에 표시되는 이 정보에 대한 자세한 내용은 Core에 대한 시스템 정보 이해을(를) 참조하십시오. 시스템 정보를 확인하는 방법에 대한 자세한 내용은 Core에 대한 시스템 정보 보기을(를) 참조하십시오.
Core 로그 파일 다운로드	Rapid Recovery Core의 다양한 작업에 대한 정보가 Core 로그 파일에 저장됩니다. 가능한 문제를 진단하려면 Rapid Recovery Core에 대한 로그를 다운로드하여 볼 수 있습니다. Core 로그 액세스 및 보기에 관한 자세한 내용은 Core 로그 액세스을(를) 참조하십시오. 각 보호된 시스템도 작업 로그를 저장합니다. 보호된 시스템의 로그를 다운로드하는 야간 작업을 선택하면 이 로그를 Core에 업로드할 수 있습니다. 야간 작업에 대한 자세한 내용은 야간 작업 이해을(를) 참조하십시오. Core에 대해 야간 작업 설정을 구성하는 방법에 대한 자세한 내용은 Core에 대한 야간 작업 구성을(를) 참조하십시오. 보호된 특정 시스템에 대해 야간 작업을 구성하는 방법에 대한 자세한 내용은 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

Core에 대한 시스템 정보 이해

Rapid Recovery에서는 Rapid Recovery Core에 대한 정보를 볼 수 있습니다. 이때 일반적인 정보, 로컬 볼륨에 대한 정보, 마운트된 볼륨에 대한 정보를 볼 수 있습니다.

일반 창에서는 다음 표에 설명된 정보를 제공합니다.

표 24. 시스템 정보

UI 요소	설명
호스트 이름	Rapid Recovery Core의 시스템 이름.
OS 버전	Rapid Recovery Core에 설치된 운영 체제 버전.
OS 아키텍처	Rapid Recovery Core를 호스팅하는 시스템의 기본 구조 및 설계를 나열합니다. 칩셋이 포함될 수 있고 64비트 시스템을 나열합니다. Rapid Recovery Core는 64비트 시스템만 지원합니다.

UI 요소	설명
메모리(실제)	Core 시스템에 설치된 RAM(Random Access Memory) 크기를 나열합니다.
표시 이름	구성 가능한 Core의 표시 이름을 보여줍니다(Core 일반 설정 구성 참조).
정규화된 도메인 이름	Core 시스템의 정규화된 도메인 이름을 표시합니다.
메타데이터 캐시 위치	메타데이터 캐시 위치의 경로를 표시합니다. 자세한 내용은 중복 제거 캐시 및 저장 위치 이해을(를) 참조하십시오.
기본 캐시 위치	기본 중복 제거 캐시 위치의 경로를 표시합니다. 자세한 내용은 중복 제거 캐시 및 저장 위치 이해을(를) 참조하십시오.
보조 캐시 위치	보조 중복 제거 캐시 위치의 경로를 표시합니다. 자세한 내용은 중복 제거 캐시 및 저장 위치 이해을(를) 참조하십시오.

볼륨 창에는 Core 시스템의 저장소 볼륨에 대한 이름, 장치 ID, 파일 시스템, 원시 용량, 포맷된 용량, 사용한 용량, 마운트 지점과 같은 정보가 있습니다.

Replay 엔진 연결 창에는 현재 마운트된 복구 지점에 대한 자세한 정보가 표시됩니다. ID, 로컬 끝점, 원격 끝점, 마운트된 이미지 에이전트 ID, 마운트된 이미지 ID, 마운트된 이미지 표시 이름을 볼 수 있습니다. 마운트가 쓰기 가능한지 확인하고 인증된 사용자, 읽은 바이트, 쓴 바이트를 볼 수 있습니다.

Mounts(마운트) 페이지에서 Core에 로컬로 마운트된 복구 지점을 분리할 수 있습니다. 복구 지점 분리에 대한 자세한 내용은 복구 지점 분리를 참조하십시오.

자세한 내용은 Core에 대한 시스템 정보 보기을(를) 참조하십시오.

Core에 대한 시스템 정보 보기

Core에 대한 시스템 정보에는 일반 정보, 로컬 볼륨에 대한 정보 및 Core에 탑재된 볼륨에 대한 정보가 포함되어 있습니다. 이 페이지에서 사용할 수 있는 정보에 대한 자세한 설명은 Core에 대한 시스템 정보 이해을(를) 참조하십시오.

Core에 대한 시스템 정보를 보려면 이 절차에 있는 단계를 완료하십시오.

노트: 보호된 특정 시스템에 대한 시스템 정보도 볼 수 있습니다. 자세한 내용은 보호된 시스템의 시스템 정보 보기을(를) 참조하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **시스템 정보**를 클릭합니다.
시스템 정보 페이지가 나타납니다.

Core 로그 액세스

Rapid Recovery Core의 다양한 작업에 대한 정보가 Core 로그 파일에 저장됩니다. 이 AppRecovery.log 파일은 기본적으로 **C:\ProgramData\AppRecovery\Logs** 경로에 저장됩니다.

노트: 사용자 설정에 따라 AppRecovery 디렉터리가 Rapid Recovery Core에서 보이지 않을 수 있습니다. 이 디렉터리를 보려면 폴더 옵션 제어판을 숨긴 파일, 폴더 및 드라이브를 표시하도록 변경해야 할 수 있습니다. 이러한 설정이 알려진 파일 형식에 대한 확장명을 숨기는 옵션을 포함하는 경우, Core 로그 파일은 .log 확장명 없이 AppRecovery로 나타날 수 있습니다.

Core 로그에는 완료된 Core 작업, 연결 실패, Core의 일부에서 라이센스 포털에 문의를 시도한 결과 등의 정보가 포함됩니다. Core 로그 파일에 저장된 각 문의 서두에는 4개의 한정자 INFO, DEBUG, ERROR, WARN 중 하나가 옵니다. 이러한 한정자는 문제를 진단할 때 로그에 저장된 정보의 특성을 분류하는 데 도움이 됩니다.

노트: 마찬가지로, Core와 통신을 시도한 내용의 정보를 담은 로그 파일이 각 보호된 시스템에도 저장됩니다. 시스템 로그에 대한 자세한 내용은 보호된 시스템 진단 액세스을(를) 참조하십시오.

로그 액세스 기능은 문제를 해결하거나 Dell Rapid Recovery 지원의 도움이 필요할 때 유용합니다. 로그에 액세스하려면 다음 절차를 참조하십시오.

- Core 로그 파일 다운로드 및 보기
- 보호된 시스템의 로그 파일 다운로드 및 보기

Core 로그 파일 다운로드 및 보기

Core에서 오류 또는 문제가 발생할 경우 Core 로그를 다운로드하여 오류 또는 문제를 확인하거나 Dell 서비스 담당자와 공유할 수 있습니다.

1 Rapid Recovery Core Console의 아이콘 표시줄에서 (자세히)를 클릭한 다음 **Core 로그**를 클릭합니다.

2 **Core 로그 다운로드** 페이지에서 **다운로드를 시작하려면 여기를 클릭하십시오**를 클릭합니다.

3 `CoreAppRecovery.log` 파일을 열거나 저장하라는 메시지가 표시되면 **저장**을 클릭합니다.

4 **CoreAppRecovery.log 열기** 대화 상자가 보이면 다음 중 하나를 수행합니다.

- 로그 파일을 열려면 **연결 프로그램**을 선택하고 텍스트 기반 로그 파일을 볼 수 있는 응용 프로그램(예: 메모장)을 선택한 다음 마지막으로 **확인**을 클릭합니다.

  선택한 응용 프로그램에서 CoreAppRecovery.log 파일이 열립니다.
- 로컬에 파일을 저장하려면 **파일 저장**을 선택하고 **확인**을 클릭합니다.

  CoreAppRecovery.log 파일이 **Downloads** 폴더에 저장됩니다. 이 파일은 텍스트 편집기를 사용하여 열 수 있습니다.

관련 링크

Core 로그 파일 다운로드 및 보기
보호된 시스템의 로그 파일 다운로드 및 보기

Core 구성을 위한 로드맵

구성 작업에는 백업 스냅샷을 저장하기 위한 리포지토리 생성 및 구성, 보호되는 데이터의 보안을 위한 암호화 키 정의, 경고 및 알림 설정이 있습니다. Core 구성을 완료한 후에는 에이전트를 보호하고 복구를 수행할 수 있습니다.

Core를 구성하려면 특정 개념을 이해하고 다음 초기 작업을 수행해야 합니다.

- 리포지토리 생성
- 암호화 키 구성
- 이벤트 알림 구성
- 보존 정책 구성
- SQL 연결 기능 구성

리포지토리

이 섹션에서는 리포지토리 사용법을 설명합니다. 중복 제거 볼륨 관리자 리포지토리를 소개하고, 관련 기능과 특성을 설명합니다. Rapid Recovery에서 사용하는 중복 제거의 유형과 이 중복 제거 기능이 응용 프로그램 전반에 걸쳐 사용되는 방법에 대해서도 설명합니다. 그 다음 이 섹션에서는 리포지토리 생성, 세부 정보 보기 및 편집, 리포지토리 삭제 등 DVM 리포지토리를 관리하는 방법을 설명합니다. 특정 Core의 리포지토리를 다른 Core에서 여는 방법도 알 수 있습니다. 마지막으로, 이 섹션에서는 하나의 리포지토리에서 다른 리포지토리로 복구 지점을 수동으로 마이그레이션하는 방법을 설명합니다.

DVM 리포지토리 관리

Rapid Recovery를 사용하려면 Rapid Recovery Core에서 하나 이상의 리포지토리를 설정해야 합니다. 리포지토리에는 보호된 데이터 즉, 사용자 환경의 보호된 서버에서 캡처된 스냅숏이 저장됩니다.

DVM 리포지토리 관리 작업은 다음과 같습니다.

1 **DVM 리포지토리 생성.** 리포지토리를 만들기 전에 적절한 기술 유형을 고려하십시오.
리포지토리에 대한 자세한 내용은 리포지토리 이해을(를) 참조하십시오.

DVM 리포지토리를 만드는 방법에 대한 자세한 내용은 DVM 리포지토리 생성을(를) 참조하십시오.

2 **새 저장 위치 추가**. 새로운 저장 위치 추가에 대한 자세한 내용은 기존 DVM 리포지토리에 저장소 위치 추가을(를) 참조하십시오.

3 **리포지토리 설정 수정**. 리포지토리 설정을 수정하는 방법에 대한 자세한 내용은 다음을(를) 참조하십시오. 리포지토리 상세 정보 보기 또는 수정

4 **리포지토리 검사**. 리포지토리를 검사하는 방법에 대한 자세한 내용은 리포지토리 검사을(를) 참조하십시오.

5 **리포지토리 최적화 작업 수행**. 리포지토리 최적화 작업에 대한 자세한 내용은 리포지토리 최적화 작업 설명를 참조하십시오. 기존 DVM 리포지토리를 최적화하는 작업 단계를 보려면 DVM 리포지토리 최적화을(를) 참조하십시오.

6 **리포지토리 삭제**. 리포지토리를 삭제하는 방법에 대한 자세한 내용은 리포지토리 삭제을(를) 참조하십시오.

DVM 리포지토리 생성

이 프로세스는 리포지토리를 DVM(Deduplication Volume Manager) 기술을 사용하여 Core에 리포지토리를 생성하는 방법을 설명합니다.

- DVM 리포지토리를 생성하려는 시스템에 대한 관리 액세스 권한이 있어야 합니다.
- 이 리포지토리 유형을 사용하려면 저장소 위치로 정의하는 볼륨에 최소 150GB의 저장소 공간이 필요합니다
- DVM 리포지토리의 저장소 위치는 Core 서버에 연결된 로컬 드라이브에 있어야 합니다.
- Core 서버는 DL 시리즈 어플라이언스(DL1000 포함)이거나 시스템 요구 사항을 충족하는 모든 소프트웨어 기반 Windows Server가 될 수 있습니다.

노트: Appliance(어플라이언스) 탭을 통해 리포지토리를 생성하는 것이 좋습니다. 자세한 내용은 저장소 프로비저닝 섹션을 참조하십시오.

DVM 리포지토리 생성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core 콘솔로 이동합니다.

2 아이콘 표시줄에서 (더 보기)를 클릭한 다음 **Repositories(리포지토리)**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

Repositories(리포지토리) 페이지에 DVM Repositories(DVM 리포지토리) 창이 나타납니다.

3 페이지 상단에서 **Add New DVM Repository(새 DVM 리포지토리 추가)**를 클릭합니다.
Add New Repository(새 리포지토리 추가) 대화 상자가 표시됩니다.

4 다음 표에 설명된 대로 정보를 입력합니다.

표 25. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다.

텍스트 상자	설명
	기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 첫 번째 리포지토리인 경우 기본 이름은 리포지토리 1입니다. 필요하면 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자를 포함해야 합니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본적으로 값은 64입니다.
설명	선택적으로 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

5 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

△ 주의: **리포지토리의 저장소 위치는 루트 내에 전용 폴더로 정의합니다. 루트 위치는 지정하지 마십시오. 예를 들어, E:\가 아닌 E:\Repository\를 사용합니다. 이 단계에서 생성하는 리포지토리를 나중에 제거하는 경우 해당 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 루트에 저장소 위치를 정의하는 경우 볼륨(예: E:\)에 있는 다른 모든 파일이 삭제되어 이는 치명적인 데이터 손실을 초래할 수 있습니다.**

Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

6 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

7 **Storage Location(저장소 위치)** 영역에 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨을 추가할 수 있습니다(예: 직접 연결된 저장소, 저장소 영역 네트워크 또는 네트워크에 연결된 저장소). 일반 인터넷 파일 시스템(CIFS) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.

- **Add file on local disk(로컬 디스크에 파일 추가)**를 선택하여 로컬 시스템을 지정하고 아래 표에 설명된 대로 정보를 입력합니다.

표 26. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Data`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Metadata`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 또는 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 선택하여 네트워크 공유 위치를 지정한 후 아래 표에 설명된 대로 정보를 입력합니다.

표 27. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다.

텍스트 상자	설명
	경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.

8 **Storage Configuration(저장소 구성)** 영역에서 **More Details(성세 정보)**를 클릭하고 아래 표에 설명된 대로 저장소 위치에 대한 상세 정보를 입력합니다.

표 28. 저장소 구성 상세 정보

텍스트 상자	설명
크기	저장소 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB이고 기본값은 250GB입니다. 다음 중에서 선택할 수 있습니다. • GB • TB **노트: 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2을 사용하는 NTFS 볼륨인 경우 파일 크기 한도는 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows 캐시 관리자가 사용되는 방법을 제어하고 다른 구성에 대해 성능을 최적화할 수 있도록 리포지토리를 조정하는 데 도움을 줍니다. 값을 다음 중 하나로 설정합니다. • 켜짐 • 꺼짐 • 동기화 기본값인 On(켜짐)으로 설정하는 경우 Windows에서 캐싱을 제어합니다. 이는 Windows 10 및 Windows Server 2012 이상 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 Off(꺼짐)입니다.** Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. Sync(동기화)로 설정하면 Windows에서 캐싱과 동기식 입력/출력을 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

9 **저장**을 클릭합니다.

Add Storage Location(저장소 위치 추가) 대화 상자가 닫히고 설정이 저장됩니다. **Add New Repository(새 리포지토리 추가)** 대화 상자가 새로운 저장소 위치를 보여 줍니다.

10 선택적으로 리포지토리에 대한 추가 저장소 위치를 추가하려면 6단계부터 9단계를 반복합니다.

11 현재 리포지토리에 대해 생성하려는 모든 저장소 위치가 정의되었으면 **Add New Repository(새 리포지토리 추가)** 대화 상자에서 **Create(생성)**를 클릭합니다.

Add New Repository(새 리포지토리 추가) 대화 상자가 닫히고 변경 사항이 적용됩니다. **Repositories(리포지토리)** 페이지가 나타나 DVM 리포지토리 요약 표에 새로 추가된 리포지토리를 보여 줍니다.

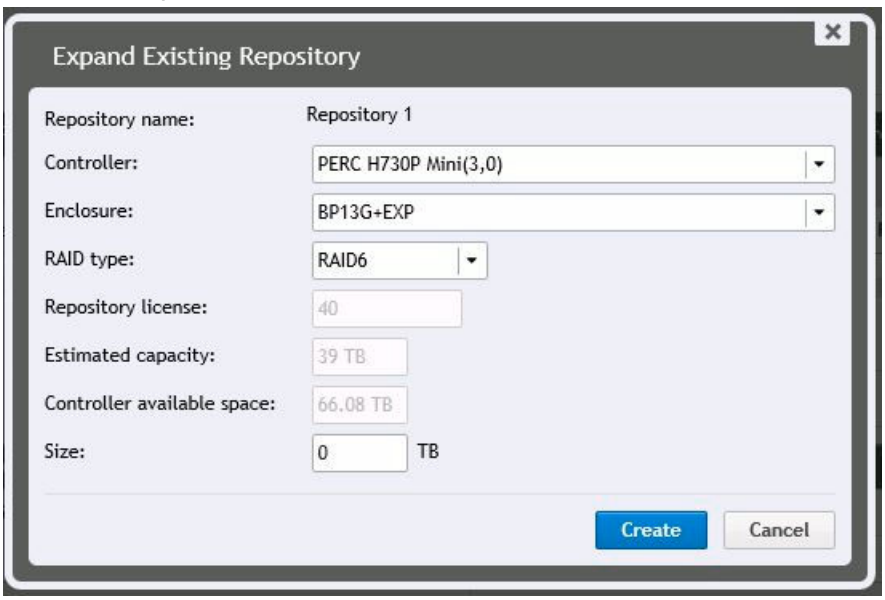
리포지토리 확장

리포지토리 확장 기능은 DL1000을 제외하고 모든 DL 모델(1300, 4300, 4000)에 사용할 수 있습니다. 적용되는 라이센스 유형은 리포지토리 크기를 제한합니다. 미사용 내부 리포지토리와 외부 인클로저의 리포지토리를 사용하여 리포지토리를 확장하려면 라이센스를 업데이트하십시오. 라이센스 키를 변경하려면 라이센스 업데이트 또는 변경 섹션을 참조하십시오. 기존 리포지토리를 확장하려면 다음 단계를 따르십시오.

1 **Appliance(어플라이언스) > Provisioning(프로비저닝)**을 클릭합니다.

2 **Repositories(리포지토리)** 섹션에서 → 확장하려는 리포지토리 옆에 있는 **Expand Existing Repository(기존 리포지토리 확장)**를 클릭합니다.

Expand Existing Repository(기존 리포지토리 확장) 대화 상자가 표시됩니다.



3 **Expand Existing Repository(기존 리포지토리 확장)** 상자에서 다음과 같은 정보를 지정합니다.

표 29. 기존 리포지토리 확장

텍스트 상자	설명
리포지토리 이름	확장할 리포지토리의 이름이 표시됩니다.
컨트롤러	내부 스토리지 또는 직접 연결된 스토리지 인클로저에 리포지토리를 생성할지 여부에 따라 적절한 스토리지 컨트롤러를 선택합니다.
Enclosure(인클로저)	적절한 스토리지 인클로저를 선택합니다.
RAID 유형	적절한 RAID 구성을 선택합니다. RAID 구성: 1, 5 또는 6의 경우 다음 옵션이 있습니다.
리포지토리 라이센스	리포지토리 라이센스가 표시됩니다.
예상 용량	리포지토리 생성에 사용 가능한 예상 용량을 표시합니다.
컨트롤러에 사용 가능한 공간	컨트롤러에서 사용 가능한 공간을 표시합니다.
크기	생성할 리포지토리의 크기를 입력합니다.

4 **Create(생성)**를 클릭합니다.

새 저장소 위치가 기존 리포지토리에 추가됩니다.

리포지토리가 지정된 크기로 확장됩니다.

리포지토리 상세 정보 보기 또는 수정

1 Rapid Recovery Core 콘솔로 이동합니다.

2 아이콘 표시줄에서 (더 보기)를 클릭한 다음 **Repositories(리포지토리)**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM Repositories(DVM 리포지토리) 창이 나타납니다.

3 **Repositories(리포지토리)** 페이지 메뉴에서 다음과 같은 일반 작업을 수행합니다.

옵션	설명
Add New DVM Repository(새 DVM 리포지토리 추가)	새 DVM 리포지토리를 추가합니다.
Open Existing DVM Repository(기존 DVM 리포지토리 열기)	이 Core에 대한 리포지토리의 소유권을 변경하는 다른 Core에서 기존 DVM 리포지토리를 엽니다. 자세한 내용은 기존 DVM 리포지토리 열기 섹션을 참조하십시오.
새로 고침	리포지토리의 목록을 보거나 새로 고칩니다.

4 **DVM Repositories(DVM 리포지토리)** 창의 DVM 리포지토리에 대한 드롭다운 메뉴에서 다음과 같은 추가 작업을 수행할 수 있습니다.

옵션	설명
Add Storage Location(저장소 위치 추가)	저장소 위치를 추가하여 기존 리포지토리를 확장합니다. **노트: DVM 리포지토리를 확장할 때 먼저 볼륨을 일시 중지한 다음 볼륨을 확장하고 마지막으로 보호를 다시 시작합니다. 이렇게 하면 특정 전송 단계와 동시에 볼륨을 확장할 때만 드물게 발생할 수 있는 오류가 방지됩니다.**
확인	리포지토리 확인 수행
설정	리포지토리 설정을 보거나 수정합니다. 이러한 설정은 다음과 같습니다. • 리포지토리 이름 보기 • 최대 동시 작업 보기 또는 변경 • 리포지토리에 대한 설명 보기 또는 변경 • 중복 제거 활성화 또는 비활성화 • 리포지토리에 저장된 데이터에 대한 압축 활성화 또는 비활성화
최적화 작업 수행	리포지토리 최적화 작업 수행
삭제	리포지토리 삭제

노트: DVM 리포지토리를 확장할 때 먼저 볼륨을 일시 중지한 다음 볼륨을 확장하고 마지막으로 보호를 다시 시작합니다. 이렇게 하면 특정 전송 단계에서 확장할 때만 드물게 발생할 수 있는 오류가 방지됩니다.

Repositories(리포지토리) 페이지에서 다음과 같은 일반적인 작업을 수행할 수 있습니다.

- 리포지토리의 목록을 보거나 새로 고칩니다.
- 새 리포지토리를 추가합니다.
- 이 리포지토리에 대한 소유권을 변경하는 다른 Core에서 기존 리포지토리를 엽니다.

기존 DVM 리포지토리에 저장소 위치 추가

노트: 어플라이언스 탭을 통해 리포지토리를 확장하는 것이 좋습니다. 참고 항목: 리포지토리 확장

DVM 리포지토리에 저장 위치를 추가하여 리포지토리나 볼륨을 저장할 위치를 지정할 수 있습니다.

리포지토리나 볼륨의 저장 위치를 지정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM 리포지토리 창이 나타납니다.

3 저장소 위치를 추가하려는 DVM 리포지토리를 나타내는 행의 리포지토리 요약 표에서 **설정**을 클릭한 뒤 **저장소 위치 추가**를 선택합니다.
저장소 위치 추가 대화 상자가 표시됩니다.

4 저장 위치에 대한 파일을 추가하는 방법을 지정합니다. 파일을 로컬 디스크 또는 CIFS 공유에 추가할 수 있습니다.

- **로컬 디스크에 파일 추가**를 선택하여 로컬 시스템을 지정한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 30. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어 `X:\Repository\Data`라고 입력합니다. 경로에 대한 동일한 제한이 적용됩니다. 공백이나 특수 문자 없이 영문자나 하이픈, 마침표만 사용하십시오.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어 `X:\Repository\Metadata`라고 입력합니다. 경로를 지정할 경우에는 영문자, 하이픈, 마침표만 사용하십시오(개별 호스트 이름과 도메인만 해당). 문자 a - z는 대소문자를 구분하지 않습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.

- 또는 **CIFS 공유에 파일 추가**를 선택하여 네트워크 공유 위치를 지정한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 31. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 경우에는 영문자, 하이픈, 마침표만 사용하십시오(개별 호스트 이름과 도메인만 해당). 문자 a - z는 대소문자를 구분하지 않습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스하기 위한 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스하기 위한 암호를 지정합니다.

5 저장소 구성 창에서 **추가 정보**를 클릭하고 다음 표에 설명된 대로 저장 위치에 대한 세부 정보를 입력합니다.

표 32. 저장 위치 세부 정보

텍스트 상자	설명
크기	저장소 위치의 크기나 용량을 설정합니다. 기본 크기는 250GB입니다. 다음 항목 중에서 선택할 수 있습니다. • GB • TB ⓘ | **노트: 최소 크기는 1GB입니다. 볼륨 크기를 초과하는 크기를 지정할 수 없습니다.**

텍스트 상자	설명
	저장 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨인 경우 파일 크기 제한은 16TB입니다. 저장 위치가 Windows 8, 8.1 또는 Windows Server 2012, 2012 R2를 사용하는 NTFS 볼륨인 경우 파일 크기 제한은 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows Cache Manager가 사용되는 방식을 제어하며 여러 구성에서 최적의 성능을 발휘할 수 있도록 리포지토리를 조정하는 데 도움이 됩니다. 값을 다음 중 하나로 설정합니다. · 설정 · 해제 · 동기화 설정(기본값)으로 지정하면 Windows가 캐싱을 제어합니다. 이는 Windows 10, Windows Server 2012 이상의 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 설정으로 지정하면 성능이 더 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 꺼짐입니다.** 꺼짐으로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. 동기화로 설정하면 Windows가 동기화 입력/출력뿐만 아니라 캐싱도 제어합니다.
섹터당 바이트 수	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트 수	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 또한 선택한 리포지토리에 대해 리포지토리 최적화 작업을 수행하려는 경우, **[리포지토리 이름]에 대한 리포지토리 최적화 작업 실행**을 선택합니다.

Dell에서는 기존 리포지토리에 저장소 위치를 추가할 때 리포지토리 최적화 작업을 수행할 것을 권장합니다. 이 작업은 리포지토리에 저장된 데이터에 중복 제거를 적용하여 여유 공간을 최적화합니다.

리포지토리의 크기, 리포지토리의 데이터 분량, 사용 가능한 네트워크 대역폭, 시스템 입/출력 시 기존 부하 등과 같은 몇 가지 요소에 따라 리포지토리 최적화 작업을 수행할 때 상당한 시간과 대역폭이 소요될 수 있습니다.

리포지토리 최적화 작업에 대한 자세한 내용은 리포지토리 최적화 작업 설명를 참조하십시오.

7 **저장**을 클릭합니다.

대화 상자가 닫히고 저장소 위치가 저장됩니다. 리포지토리 세부 정보를 확장하는 경우 생성한 저장소 위치가 리포지토리 요약 표에 표시됩니다.

DVM 리포지토리의 무결성 검사

Rapid Recovery Core에서 사용자는 소스와 대상 Core 간에 별도의 보존 정책을 설정할 수 있습니다. 복제가 다른 보존 정책과 적절히 작동하려면 대상 Core에는 소스 Core와 동일한 소프트웨어 버전(또는 최신 버전)이 있어야 합니다.

노트: Core는 릴리스 번호에서 동일한 3자리 숫자를 공유합니다(예: 둘 다 6.0.1.xxxx 또는 5.4.3.xxxx로 시작). 빌드 번호(xxxx로 표시)는 대상 Core가 최신인 경우에만 다를 수 있습니다.

관리자는 이제 소스 Core와 다른 속도로 대상 Core에 롤업을 구성할 수 있습니다. 마찬가지로 이제 모든 복제된 시스템에 대해 사용자 지정 보존 정책을 정의할 수 있습니다. 예를 들어, 소스 Core보다 더 빠르고 덜 세밀하게 대상 Core에 복구 지점을 롤백하여 공간을 절약할 수 있습니다. 또한 대상 Core보다 느린 속도로 모든 선택한 복제된 시스템에 대해 복구 지점을 롤업하여 세밀성을 더 유지할 수

있으며, 규정 준수 목적에 유용할 수 있습니다. Core에서 기본값과 다른 보존 정책을 사용하는 방법에 대한 자세한 내용은 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.

Core가 AppAssure 5.3.x의 임의 지점에서 업그레이드되었고 복제에 사용된 경우 소스 Core와 대상 Core 간에 다른 보존 정책을 구성하거나 복제된 시스템에 사용자 지정 보존 정책을 구성하기 전에 이 작업을 실행해야 합니다.

하나 이상의 적격 리포지토리(5.4.x 이전에서 생성되었고 아직 수행되지 않음)가 없으면 이 작업이 나타나지 않거나 실행하지 못할 수 있습니다.

이 작업을 실행하면 지정된 리포지토리에 저장된 모든 데이터의 무결성을 확인하여 각 스냅샷 또는 기본 이미지에서 데이터를 복구할 수 있도록 합니다. 무결성 검사 결과 리포지토리의 데이터에 문제가 발견되는 경우 작업을 즉시 중단합니다. Core에서 해당 작업에 대한 이벤트 정보는 Dell 지원에 연락하라고 표시되므로 지원 담당자와 데이터 불일치를 식별하고 복구하기 위한 추가 절차를 수행하기 위한 일정을 정할 수 있습니다.

주의: 이 작업의 실행은 오래 걸릴 것으로 예상됩니다. 걸리는 시간은 리포지토리 및 기본 저장소 시스템에 있는 데이터의 양과 유형에 따라 다릅니다. 작업이 실행되는 동안 전송(스냅샷과 기본 이미지 백업 및 복제)을 포함하여 해당 리포지토리에서는 다른 트랜잭션을 일체 수행할 수 없습니다.

이 작업이 실행되는 동안 다른 리포지토리에서는 다른 작업을 수행할 수 있습니다.

노트: 이 작업은 리포지토리 내에 있는 모든 내용의 무결성 검사합니다. 리포지토리를 마운트하고 사용할 수 있는지 확인하는 데 사용할 수 있는 `Integrity Check` 작업에 대한 자세한 내용은 리포지토리 검사을(를) 참조하십시오.

리포지토리 검사

Rapid Recovery에서는 오류 발생 시 DVM 리포지토리 볼륨에서 진단 검사를 수행할 수 있는 기능을 제공합니다. Core 오류는 부적절하게 종료되었거나, 하드웨어 장애 또는 Rapid Recovery 기능에 나타날 수 있는, 기타 환경적 낮은 IP 스택 요인의 결과일 수 있습니다.

노트: 이 절차는 진단용으로만 수행해야 합니다. 예를 들어, 하드웨어 장애, Core의 비정상적인 종료 또는 리포지토리를 가져올 때 오류가 발생한 경우 이 검사를 실행합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 뒤 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM 리포지토리 창이 나타납니다.

3 DVM 리포지토리를 검사하려면 **DVM 리포지토리** 창에서 DVM 리포지토리를 나타내는 요약 표의 아무 행에서 를 클릭하고 **검사**를 선택합니다.
Check Repository(리포지토리 검사) 대화 상자가 표시됩니다.

4 **리포지토리 검사** 대화 상자에서는 이 리포지토리와 연결된 모든 활성 작업이 취소됨을 알리고 계속 진행할 것인지 확인합니다.
활성 작업을 취소하고 리포지토리 검사 작업을 시작합니다.

5 필요한 경우 단추 표시줄에서 **실행 중인 작업** 드롭다운 메뉴를 클릭하고 리포지토리 유지 관리 작업을 선택하여 작업 상태를 추적할 수 있습니다.

리포지토리 최적화 작업 설명

DVM 리포지토리를 사용하면 각 스냅숏에서 캡처하는 데이터가 중복 제거됩니다. 이 중복 제거는 스냅숏이 리포지토리에 저장될 때마다 끊임없이 발생합니다. 각 정보 문자열 중 하나의 발생 빈도가 리포지토리에 저장됩니다. 정보 문자열이 중복 제거되면 중복 제거 캐시에서 원래 문자열에 대한 참조가 사용되므로 리포지토리의 저장소 공간이 절약됩니다.

DVM 중복 제거 캐시가 가득 차면 캐시에서 이미 참조된 스냅숏 데이터만 중복 제거됩니다. 중복 제거가 발생하면 캐시는 계속 새 고유 값으로 업데이트되면서 캐시에서 가장 오래된 값을 덮어씁니다. 이는 최적 중복 제거가 수행되지 않는 원인이 됩니다.

중복 제거에 대한 자세한 내용은 중복 제거 캐시 및 저장 위치 이해을(를) 참조하십시오.

해당 리포지토리에서 데이터의 최적 중복 제거가 지속하도록 DVM 중복 제거 캐시가 가득 차기 전에 용량을 늘릴 수 있습니다. 자세한 내용은 DVM 중복 제거 캐시 설정 구성을(를) 참조하십시오.

중복 제거 캐시가 가득 찬 뒤에도 용량을 늘릴 수 있습니다. 캐시 용량을 늘린 뒤에 리포지토리에서 공간을 확보하려면 리포지토리를 최적화할 수 있습니다. 이 작업에서는 스냅숏의 데이터가 중복 제거 캐시의 정보와 비교됩니다. 리포지토리에서 반복 문자열이 발견되면 해당 데이터가 데이터에 대한 참조로 대체되어 리포지토리의 저장소 공간이 절약됩니다. 이 중복 제거 프로세스는 스냅숏 데이터가 전송될 때마다 끊임없이 발생하는 것이 아니라 사용자 요청에 따라 발생하므로 오프라인 중복 제거라고도 합니다.

최적화 프로세스는 프로세서 집약적입니다. 이 작업을 실행하는 데 걸리는 시간은 몇 가지 요소에 따라 달라집니다. 리포지토리 크기, 리포지토리에 있는 데이터의 양, 사용 가능한 네트워크 대역폭, 시스템 입출력의 기존 부하가 이러한 요소에 포함됩니다. 리포지토리에 있는 데이터가 많을수록 이 작업이 오래 실행됩니다.

리포지토리 최적화 작업이 발생하면 다음 동작이 대체 또는 취소됩니다.

- 복구 지점 작업 삭제
- 리포지토리 작업 유지관리
- 리포지토리 무결성 작업 검사

최적화 작업이 발생하면 다음 동작이 대체 또는 취소됩니다.

- 모든 복구 지점 작업 삭제
- 복구 지점 체인 작업 삭제
- 리포지토리 작업 유지관리
- 복구 지점 작업 기준 삭제
- 리포지토리 무결성 작업 검사

기존 DVM 리포지토리를 최적화하는 단계는 DVM 리포지토리 최적화을(를) 참조하십시오.

리포지토리 최적화 작업은 필요하면 제한된 시간 동안 인터럽트할 수 있습니다. 자세한 내용은 리포지토리 최적화 작업 중단 또는 다시 시작을(를) 참조하십시오.

DVM 리포지토리 최적화

이 절차를 수행하려면 Core에 DVM 리포지토리가 있어야 합니다.

기존 DVM 리포지토리에 저장되는 데이터의 중복 제거를 오프라인으로 수행할 수 있습니다. 이는 리포지토리 최적화 작업 실행을 통해 수행됩니다.

노트: Dell에서는 중복 제거 캐시 크기를 늘린 후에만 리포지토리 최적화 작업을 수행하도록 권장합니다. 이 작업을 통해 리포지토리 공간을 확보하고 DVM 중복 제거 캐시를 보다 효과적으로 사용할 수 있습니다.

DVM 리포지토리를 최적화하려면 이 절차에 있는 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

3 리포지토리 창에서 최적화하려는 리포지토리가 표시된 열로 이동하여 을 클릭한 후 **최적화 작업 수행**을 선택합니다.
최적화 확인을 요청하는 경고 메시지가 나타납니다.

4 클릭하여 최적화를 확인합니다.
최적화 작업은 대부분의 다른 작업보다 우선합니다. 필요한 경우, 진행 중인 최적화 작업을 중단할 수 있습니다. 이 작업 중단 또는 다시 시작에 관한 자세한 내용은 리포지토리 최적화 작업 중단 또는 다시 시작을(를) 참조하십시오.

리포지토리 최적화 작업 중단 또는 다시 시작

리포지토리 최적화 작업을 시작하면 선택한 DVM 리포지토리가 중복 제거됩니다. 이 중복 제거 최적화는 리포지토리의 공간을 절약하기 위해 많은 프로세서를 사용하는 작업입니다. 자세한 내용은 리포지토리 최적화 작업 설명을(를) 참조하십시오.

작업을 시작하면 다음 절차를 사용하여 작업을 중단할 수 있습니다. 그러면 중복 제거가 일시 중지됩니다. 이미 최적화를 중단한 경우 이 절차를 사용하여 프로세스를 다시 시작할 수 있습니다.

노트: 이 절차는 DVM 리포지토리와 리포지토리 최적화 작업을 시작한 경우에만 적용됩니다.

이 절차의 단계를 완료하여 리포지토리 최적화 작업을 중단하거나 다시 시작합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 뒤 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM Repositories(DVM 리포지토리) 창이 나타납니다.

3 최적화 작업을 중단하려면 다음을 수행합니다.

a 리포지토리 요약 표 가운데 적절한 리포지토리를 나타내는 행에서 를 클릭하고 **최적화 작업 중단**을 선택합니다.
중단을 확인하는 경고 프롬프트가 나타납니다.

b 메시지를 클릭하여 최적화를 확인합니다.

4 중단된 최적화 작업을 다시 시작하려면 다음을 수행합니다.

a 리포지토리 요약 표 가운데 적절한 리포지토리를 나타내는 행에서 를 클릭하고 **최적화 작업 계속**을 선택합니다.
중단을 확인하는 경고 프롬프트가 나타납니다.

b 대화 상자에서 **중단된 지점부터 작업 계속** 옵션을 선택하고 **예**를 클릭합니다.

대화 상자를 닫고 마지막으로 중단된 지점부터 리포지토리 최적화 작업을 다시 시작합니다.

기존 DVM 리포지토리 열기

Rapid Recovery에 대한 기본 저장소 기술로서 DVM 리포지토리에는 특정 Rapid Recovery Core에서 보호된 시스템의 스냅숏 데이터(복구 지점 형태)가 포함되어 있습니다. 하나의 Core(예: Core A)에 있는 기존 리포지토리를 두 번째 Core(예: Core B)에서 열 수 있습니다.

노트: 다른 Core에서 리포지토리를 열면 리포지토리의 소유권이 변경됩니다. 기존의 리포지토리를 열면 정보가 두 번째 Core에만 액세스할 수 있습니다.

DVM 리포지토리의 경우 원래 Core(Core A)를 현재 사용하지 않아야 합니다. 예를 들어 시스템을 끄거나 네트워크에 액세스할 수 없도록 하거나 Core 서비스를 중단해야 합니다.

리포지토리는 공유 네트워크 위치에 있거나 두 번째 Core에 액세스할 수 있는 저장 장치에 있습니다.

기존 리포지토리를 열려면 다음 절차를 수행하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM 리포지토리 창도 나타납니다.

3 기존 DVM 리포지토리를 사용하는 경우 페이지 상단에서 **기존 DVM 리포지토리 열기**를 클릭합니다.
기존 DVM 리포지토리 열기 대화 상자가 나타납니다.

4 **기존 DVM 리포지토리 열기** 대화 상자에 열고자 하는 리포지토리에 대한 다음 정보를 입력한 뒤 **열기**를 클릭합니다.

표 33. Open Existing DVM Repository(기존 DVM 리포지토리 열기) 옵션

텍스트 상자	설명
경로	리포지토리의 경로. 예를 들어, 로컬 경로의 경우 **D:\work\machine**, IP 주소의 경우 **\\10.10.99.155\repositories**, 네트워크 경로의 경우 \\servername\sharename입니다.
사용자 이름	리포지토리가 네트워크 경로를 가지는 경우 네트워크 공유에 로그인하기 위한 사용자 이름을 입력합니다.
암호	리포지토리가 네트워크 경로를 가지는 경우 네트워크 공유에 로그인하기 위한 암호를 입력합니다.

대화 상자가 닫히고 선택한 리포지토리가 현재 Core에 추가됩니다.

리포지토리 삭제

리포지토리를 삭제하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

리포지토리 페이지에서 DVM 리포지토리 창이 나타납니다.

3 리포지토리 요약 테이블에서 삭제하려는 리포지토리가 있는 행을 찾고 을 클릭하여 드롭다운 메뉴를 확장한 다음 **삭제**를 선택합니다.
삭제를 확인하는 경고 메시지가 나타납니다.

4 **예**를 클릭하여 리포지토리의 삭제를 확인합니다.

주의: 리포지토리가 삭제되면 리포지토리에 포함된 데이터가 취소되며 복구할 수 없습니다.

DVM에서 리포지토리 작업 검사 실행

이 절차를 수행하여 전체 DVM 리포지토리의 무결성을 검사합니다. 이 절차는 AppAssure 5.3.x에서 5.4 릴리스로 업그레이드할 때 복제된 대상 코어에 사용하는 것이 좋습니다. 시간이 오래 걸릴 수 있는 무결성 검사를 실행하는 도중에 리포지토리에서 다른 작업을 수행할 수 없습니다.

대상 Core에 여러 리포지토리가 있으면 리포지토리마다 이 프로세스를 한 번씩 수행합니다.

노트: 무결성 검사 작업을 이미 완료한 대상 Core에 다른 DVM 리포지토리가 있거나 이 대상 Core의 새 리포지토리를 추가로 만들 경우, 지정된 DVM 리포지토리에서 무결성 검사 작업이 실행되는 동안 해당 2차 리포지토리에서 작업을 수행할 수 있습니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 을 클릭하고 (추가)를 클릭한 후 **리포지토리**를 선택합니다.
Repositories(리포지토리) 페이지가 나타납니다.

DVM 리포지토리 창이 표시됩니다.

3 리포지토리 요약표의 검사하려는 리포지토리가 표시된 행에서 을 클릭하고 **리포지토리 작업 검사**를 선택합니다.
확인 메시지가 나타납니다.

주의: 작업을 수행하겠다고 확인하기 전에 필요한 소요 시간을 신중히 고려해야 합니다. 작업이 실행되는 동안에는 해당 리포지토리에서 전송(스냅숏 및 기본 이미지 백업, 복제) 및 야간 작업 등을 포함한 다른 트랜잭션을 수행할 수 없습니다.

4 무결성 검사를 수행하려면 **리포지토리 작업 검사** 대화 상자에서 **예**를 클릭합니다.

대화 상자가 닫힙니다. 큐에 대기 중이었거나 진행 중이었던 모든 작업이 취소되고 무결성 검사 작업이 시작됩니다.

5 검사 후 추가 단계가 필요한지 아닌지 결정을 포함하여 리포지토리에 대한 리포지토리 작업 검사의 진행률을 모니터링하려면 (이벤트)를 클릭합니다.

6 **이벤트** 페이지에서 작업에 대한 **작업 세부 정보**를 클릭하여 작업 상태에 대한 자세한 내용을 확인합니다.

- 해당 작업의 하위 직업에 오류가 있으면 해당 오류를 기록하고 Dell 기술 지원 담당자에게 오류 정보를 제공하십시오.
- 리포지토리 작업 검사에서 모든 하위 작업이 완료되면 해당 리포지토리에 대한 사용자 지정 보존 정책을 설정할 수 있습니다.

보안 관리

Core는 리포지토리 내에 보호되는 시스템 스냅샷 데이터를 암호화할 수 있습니다. 전체 리포지토리를 암호화하는 대신 리포지토리에서 시스템을 보호하는 동안 다른 보호되는 시스템에 대해 키를 재사용할 수 있는 암호화 키를 지정할 수 있습니다. 각 활성 암호화 키가 암호화 도메인을 생성하므로 암호화해도 성능에 영향을 미치지 않습니다. 따라서 단일 Core에서 다중 암호화 도메인을 호스트하여 다중 테넌트를 지원할 수 있습니다. 다중 테넌트 환경에서 데이터가 파티션화되고 암호화 도메인 내에서 중복 제거됩니다. 사용자가 암호화 키를 관리하므로 볼륨 손실로 인해 키가 유출되지 않습니다. 키 보안 개념과 고려사항은 다음과 같습니다.

- 암호화는 SHA-3과 호환되는 CBC(Cipher Block Chaining) 모드에서 256비트 AES를 사용하여 수행됩니다.
- 암호화 도메인 내에서 중복 제거가 작동하여 개인 정보를 보장합니다.
- 암호화는 성능에 영향을 미치지 않고 수행됩니다.
- Core에 구성된 암호화 키를 추가, 제거, 가져오기, 내보내기, 수정 및 삭제할 수 있습니다.
- Core에 생성할 수 있는 암호화 키의 수는 제한되지 않습니다.

보호된 시스템에서 암호화 적용 또는 제거

암호화 키를 정의한 후 리포지토리에 있는 하나 이상의 보호된 시스템에 적용하여 언제든지 Core에서 보호된 데이터를 보호할 수 있습니다. 시스템 수에 상관없이 보호된 시스템에 단일 암호화 키를 적용할 수 있지만, 한 번에 하나의 암호화 키만 사용할 수 있습니다.

Rapid Recovery의 중복 제거 범위는 같은 리포지토리 및 암호화 키를 사용하는 보호된 시스템으로 제한됩니다. 따라서 중복 제거의 이점을 최대로 활용하려면 실제로 사용하는 수의 보호된 시스템에 단일 암호화 키를 적용하는 것이 좋습니다. 그러나 Core에서 만들 수 있는 암호화 키의 수에는 제한이 없습니다. 따라서 법적 준수, 보안 규칙, 개인정보 보호 정책 또는 기타 상황에서 암호화 키를 요구하는 경우에는 암호화 키를 제한 없이 추가 및 관리할 수 있습니다. 그런 다음 각 키를 보호된 시스템 한 대에만 적용하거나 리포지토리의 시스템 집합에 적용할 수 있습니다.

암호화 키를 보호된 시스템에 적용하거나 보호된 시스템에서 암호화 키를 분리할 때마다 Rapid Recovery에서는 다음 예약 또는 강제 스냅숏 시 해당 시스템의 새 기본 이미지를 적용합니다. 해당 기본 이미지(및 암호화 키가 적용되는 동안 작성된 모든 후속 증분 스냅숏)에 저장된 데이터는 256비트 고급 암호화 표준으로 보호됩니다. 이 암호화 방법보다 우수한 방법은 아직 알려지지 않았습니다.

현재 보호된 시스템에 사용되는 기존 암호화 키의 이름 또는 암호를 변경하면 다음 예약 또는 강제 스냅숏 시 Rapid Recovery에서는 업데이트된 키 속성을 캡처하여 반영합니다. 해당 기본 이미지(및 암호화 키가 적용되는 동안 만들어진 모든 후속 증분 스냅숏)에 저장된 데이터는 256비트 고급 암호화 표준으로 보호됩니다. 이 암호화 방법보다 우수한 방법은 아직 알려지지 않았습니다.

암호화 키가 생성되고 보호된 시스템에 적용되면 해당 암호화 제거에 대한 두 가지 개념이 있습니다. 첫 번째는 보호된 시스템에서 키 연결을 해제하는 것입니다. (선택 사항) 암호화 키가 모든 보호된 시스템에서 분리되면 Rapid Recovery Core에서 삭제할 수 있습니다.

이 항목은 다음과 같이 구성되어 있습니다.

- 암호화 키를 보호된 시스템과 연결
- 보호된 시스템 페이지에서 암호화 키 적용
- 보호된 시스템에서 암호화 키 연결 해제

암호화 키를 보호된 시스템과 연결

다음 두 가지 방법 중 하나를 사용하여 암호화 키를 보호된 시스템에 적용할 수 있습니다.

- **시스템 보호 방법.** 이 방법을 사용하면 암호화를 하나 또는 여러 대의 시스템에 동시에 적용할 수 있습니다. 이 방법을 통해 새 암호화 키를 추가하거나 선택한 시스템에 기존 키를 적용할 수 있습니다.

  시스템에 대한 보호를 처음 정의할 때 암호화를 사용하려면 관련 시스템 보호 마법사에서 고급 옵션을 선택해야 합니다. 이 방법을 선택하면 마법사 워크플로에 암호화 페이지가 추가됩니다. 이 페이지에서 **암호화 사용**을 선택한 다음 기존 암호화 키를 선택하거나 새 키에 대한 매개 변수를 지정합니다. 자세한 내용은 시스템 보호 또는 다중 시스템 보호 정보을(를) 각각 참조하십시오.
- **시스템에 대한 구성 설정 수정.** 이 방법은 보호된 시스템 한 대에 암호화 키 하나를 적용합니다. Rapid Recovery UI에서 시스템에 대한 구성 설정을 수정하는 두 가지 방법이 있습니다.
  - 특정 보호된 시스템에 대한 구성 설정을 수정합니다. 이 방법은 사용하려는 암호화 키가 Rapid Recovery Core에 이미 존재하고, 범용 키 유형으로 잠금 해제 상태여야 합니다. 암호화는 일반 설정에 포함됩니다. 자세한 내용은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.
  - 보호된 시스템 페이지에서 **암호화되지 않음** 아이콘을 클릭합니다. 이 방법을 사용할 때는 새 암호화 키를 만들어 적용하거나 기존의 잠금 해제된 범용 키를 지정된 보호된 시스템에 할당할 수 있습니다. 자세한 내용은 보호된 시스템 페이지에서 암호화 키 적용을(를) 참조하십시오.

보호된 시스템 페이지에서 암호화 키 적용

Rapid Recovery Core에 암호화 키를 추가했으면 시스템 수에 상관 없이 보호된 시스템에 이 키를 사용할 수 있습니다.

하나 이상의 시스템을 처음 보호할 때 암호화 키를 선택하면 이 암호화 키가 해당 마법사를 사용하여 보호하는 시스템에 자동으로 적용됩니다. 이 경우에는 암호화 키 적용 절차가 필요하지 않습니다.

이 절차를 수행합니다.

- Core에서 보호된 시스템에 기존의 범용, 잠금 해제된 암호화 키를 적용하려는 경우
- 암호화 키 추가 항목에 설명된 프로세스를 사용하여 새 암호화 키를 방금 추가했고 해당 키를 보호된 시스템에 적용하려는 경우
- 암호화가 Core의 보호된 시스템에 이미 적용되어 있지만, 이 키를 Core에서 사용 가능한 다른 범용의 잠금 해제된 키로 변경하려는 경우

주의: 보호된 시스템에 암호화 키를 적용하면 다음 예약 또는 작성된 스냅숏에서 Rapid Recovery는 해당 시스템에 대한 새로운 기본 이미지를 작성합니다.

1 Rapid Recovery Core로 이동하고 **보호된 시스템**을 클릭합니다.

보호된 시스템 페이지가 나타나고 이 Core에서 보호되는 시스템을 모두 나열합니다. 암호화 키가 적용되지 않은 컴퓨터에는 열린 자물쇠 가 나타납니다. 닫힌 자물쇠 는 보호된 컴퓨터에 암호화가 적용되었음을 나타냅니다.

2 Protected Machines(보호된 시스템) 창에서 구성할 보호된 시스템에 대한 자물쇠 아이콘을 클릭합니다.

암호화 구성 대화 상자가 나타납니다.

3 다음 작업 중 하나를 수행합니다.
   - 기존 암호화 키를 이 시스템에 적용하려는 경우 **기존 키로 Core 기반 암호화를 사용하여 데이터 암호화**를 선택하고 드롭다운 메뉴에서 적합한 키를 선택합니다. **확인**을 클릭하여 확인합니다.
   - 기존 암호화 키를 다른 범용의 잠금 해제된 키에 적용하려는 경우 **새 키로 Core 기반 암호화를 사용하여 데이터 암호화**를 선택하고 드롭다운 메뉴에서 적합한 키를 선택합니다. **확인**을 클릭하여 확인합니다.
   - 새 암호화 키를 생성하여 보호된 시스템에 적용하려는 경우 **새 키로 Core 기반 암호화를 사용하여 데이터 암호화**를 선택합니다. 그런 다음 아래 표에 설명된 대로 키에 대한 세부 정보를 입력합니다.

표 34. 새 암호화 키 세부 정보

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~64개의 영숫자를 포함해야 합니다. 금지된 문자 또는 금지된 구를 사용하지 마십시오.
설명	암호화 키에 대한 설명을 입력합니다. 이 정보는 Rapid Recovery Core Console에서 암호화 키 목록을 볼 때 설명 필드에 표시됩니다. 설명은 최대 254자를 포함할 수 있습니다. 모범 사례는 금지된 문자 및 금지된 구를 사용하지 않는 것입니다.
암호	액세스를 제어하기 위해 사용되는 암호를 입력합니다. 모범 사례는 금지된 문자를 사용하지 않는 것입니다. 암호를 안전한 곳에 적어둡니다. Dell 지원팀에서는 암호를 복구할 수 없습니다. 암호화 키를 만들어 하나 이상의 보호된 시스템에 적용하면 암호를 유실할 경우 데이터를 복구할 수 없습니다.
암호 확인	암호를 다시 입력합니다. 암호 입력을 확인하는 데 사용됩니다.

4 **확인**을 클릭합니다.

대화 상자가 닫힙니다. 지정한 암호화 키는 보호된 시스템에 대한 이후 백업에 적용되었으며 자물쇠가 닫힘으로 나타납니다.

선택적으로 암호화 키를 즉시 적용할 경우 스냅숏을 작성합니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.

주의: Rapid Recovery는 256비트 키와 함께 CBC(Cipher Block Chaining) 모드에서 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 Dell에서는 암호화 키를 설정하고 정의한 암호를 보호할 것을 적극적으로 권장합니다. 암호는 데이터 복구에 필수적이므로 안전한 장소에 보관해야 합니다. 암호가 없으면 데이터 복구가 불가능합니다.

보호된 시스템에서 암호화 키 연결 해제

보호된 시스템에 암호화 키가 적용되면 Rapid Recovery Core에 저장된 모든 후속 스냅숏 데이터가 암호화됩니다.

보호된 시스템에서 암호화 키 연결을 해제할 수 있습니다. 이 작업은 기존 백업 데이터의 암호를 해독하지 않고, 다음 예약 또는 작성된 스냅숏에서 해당 컴퓨터에 대한 새로운 기본 이미지를 작성합니다.

노트: 암호화 키 제거 항목에 설명된 대로 Core에서 암호화 키를 제거하려면 먼저 모든 보호된 시스템에서 해당 암호화 키 연결을 해제해야 합니다.

보호된 시스템에서 암호화 키 연결을 해제하려면 이 절차를 수행하십시오.

1 Rapid Recovery Core로 이동하여 **보호된 시스템**을 클릭합니다.

보호된 시스템 페이지가 나타나고 이 Core에서 보호되는 시스템을 모두 나열합니다. 암호화 키가 적용되지 않은 컴퓨터에는 열린 자물쇠 가 나타납니다. 닫힌 자물쇠 는 보호된 컴퓨터에 암호화가 적용되었음을 나타냅니다.

2 보호된 시스템 창에서 구성할 보호된 시스템에 대한 **암호화됨** 아이콘을 클릭합니다.

암호화 구성 대화 상자가 나타납니다.

3 **기존 키와 함께 Core 기반 암호화를 사용하여 데이터 암호화**를 선택하고 드롭다운 메뉴에서 **없음**을 선택한 다음 **확인**을 클릭합니다.

4 Rapid Recovery Core에서 이 암호화 키를 제거하려면 먼저 이 키를 사용하는 모든 보호된 시스템에 대해 이 절차를 반복합니다. 그런 다음 암호화 키 제거 항목에 설명된 절차를 수행합니다.

암호화 키 관리

Rapid Recovery Core에 대한 암호화 키를 관리하려면 아이콘 표시줄에서 (자세히)를 클릭한 후 **암호화 키**를 선택합니다. **암호화 키** 페이지가 나타납니다. Rapid Recovery Core에 추가된 각 암호화 키에 대해서 (아직 정의되지 않은 경우) 다음 표에 설명된 정보를 확인합니다.

표 35. 각 암호화 키에 대한 정보

UI 요소	설명
항목 선택	각 암호화 키에 대해 확인란을 선택하고 표 위에 있는 메뉴 옵션 목록에서 작업을 수행할 수 있습니다.
이름	암호화 키와 연결된 이름.
지문	이 매개 변수는 각 암호화 키를 고유하게 식별할 수 있도록 26개의 영어 대문자와 소문자로 무작위로 생성된 알파벳 문자열입니다.
유형	유형은 암호화 키의 원점과 적용 가능성을 설명합니다. 암호화 키에 가능한 두 가지 유형 중 하나를 포함할 수 있습니다. **범용**. 범용 유형은 암호화 키를 만들 때의 기본 조건입니다. 유형이 범용이고 잠금 해제 상태인 키는 보호된 시스템에 키를 적용할 수 있음을 나타냅니다. 범용 키 유형은 수동으로 잠글 수 없습니다. 암호화 키 유형 변경 절차에 설명된 대로 먼저 유형을 변경해야 합니다. **복제**. 소스 Core의 보호된 시스템에서 암호화가 활성화되었고 해당 시스템에 대한 복구 지점이 대상 Core에 복제될 때 소스에서 사용된 암호화 키가 자동으로 대상 Core에 복제 유형으로 나타납니다. 복제된 키를 수신한 후 기본 상태는 잠김입니다. 암호를 제공하면 복제 유형의 암호화 키에 대한 잠금을 해제할 수 있습니다. 키가 잠금 해제 유형인 경우 이 키를 수동으로 잠글 수 있습니다. 자세한 내용은 암호화 키 잠금 해제 항목을 참조하십시오.
주	상태는 암호화 키를 사용할 수 있는지 여부를 나타냅니다. 다음과 같은 두 가지 가능한 상태가 있습니다. • **잠금 해제**. 잠금 해제됨 상태는 키를 즉시 사용할 수 있음을 나타냅니다. 예를 들어, 보호된 시스템에 대한 스냅숏을 암호화하거나 대상 Core의 복제된 복구 지점에서 데이터 복구를 수행할 수 있습니다. • **잠금**. 잠김 상태는 암호를 제공하여 키 잠금을 해제할 때까지 키를 사용할 수 없음을 나타냅니다. 잠김은 새로 가져오거나 복제된 암호화 키의 기본 상태입니다. 암호화 키의 상태가 잠금인 경우 키를 사용하려면 먼저 키를 잠금 해제해야 합니다. 이전에 잠긴 암호화 키를 잠금 해제했고 잠금 해제를 유지하는 기간이 만료되었으면 상태가 잠금 해제에서 잠금으로 변경됩니다. 키가 자동으로 잠긴 후 키를 사용하려면 키를 다시 잠금 해제해야 합니다. 자세한 내용은 암호화 키 잠금 해제 항목을 참조하십시오.
설명	설명은 용도 또는 암호 힌트와 같은 암호화 키에 대한 유용한 정보를 제공할 것을 권장하는 선택 필드입니다.

암호화 키 창의 최상위 수준에서 암호화 키를 추가하거나 다른 Rapid Recovery Core에서 내보낸 파일을 사용하여 키를 가져올 수 있습니다. 요약 표에서 선택한 키를 삭제할 수도 있습니다.

Core에 대해 암호화 키가 존재하면 이름 또는 설명 속성을 편집하거나, 암호를 변경하거나, 잠긴 암호화 키를 잠금 해제하거나, Rapid Recovery Core에서 키를 제거하여 기존 키를 관리할 수 있습니다. 또한 키를 파일로 내보내거나 키를 다른 Rapid Recovery Core에 가져올 수 있습니다.

암호화 키 페이지에서 암호화 키를 추가하면 키가 암호화 키 목록에 나타나지만, 보호된 특정 시스템에 적용되지는 않습니다. **암호화 키** 창에서 생성되는 암호화 키를 적용하거나 Rapid Recovery Core에서 완전히 키를 삭제하는 방법에 대한 자세한 내용은 보호된 시스템에서 암호화 적용 또는 제거을(를) 참조하십시오.

암호화 키 창에서 다음 작업을 수행하여 리포지토리의 보호된 시스템에 대해 Core에 저장된 백업 데이터에 대한 보안을 관리할 수 있습니다.

- 암호화 키 추가
- 암호화 키 가져오기
- 암호화 키 잠금 해제
- 암호화 키 편집
- 암호화 키 암호 변경
- 암호화 키 내보내기
- 암호화 키 제거
- 암호화 키 유형 변경

암호화 키 추가

Rapid Recovery에는 256비트 키가 포함된 Cipher Block Chaining(CBC) 모드의 AES 256비트 암호화가 사용됩니다. 암호화 사용은 선택 사항이지만 Dell에서는 암호화 키를 설정하고 정의한 암호를 보호할 것을 적극적으로 권장합니다.

주의: 암호를 보안 위치에 저장합니다. 암호가 없으면 암호화된 복구 지점에서 데이터를 복구할 수 없습니다.

암호화 키가 정의되었으면 이 키를 사용하여 데이터를 보호할 수 있습니다. 시스템 수에 상관 없이 보호된 시스템에서 암호화 키를 사용할 수 있습니다.

이 단계에서는 Rapid Recovery Core Console에서 암호화 키를 추가하는 방법을 설명합니다. 이 프로세스는 Core에서 현재 보호하는 시스템에 키를 적용하지 않습니다. 또한 시스템을 보호하는 중에 암호화 키를 추가할 수 있습니다. 시스템 1대를 보호하는 방법 중 하나로 암호화를 추가하는 방법에 대한 자세한 내용은 시스템 보호을(를) 참조하십시오. 2대 이상의 시스템을 처음에 보호할 때 해당 시스템에 암호화를 추가하는 방법에 대한 자세한 내용은 다중 시스템 보호 정보을(를) 참조하십시오.

암호화 키를 추가하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 표시됩니다.

3 **암호화 키 추가**를 클릭합니다.
암호화 키 만들기 대화 상자가 표시됩니다.

4 **암호화 키 만들기** 대화 상자에서 다음 표에 설명된 대로 키의 세부 정보를 입력합니다.

표 36. 암호화 키 만들기.

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름에는 1~64개의 영숫자가 포함되어야 합니다. 금지된 문자 또는 금지된 구문은 사용하지 마십시오.
설명	암호화 키에 대한 설명을 입력합니다. 이 정보는 Core Console에서 암호화 키를 볼 때 설명 필드에 표시됩니다. 최대 254자를 입력할 수 있습니다. 금지된 문자와 금지된 구문을 사용하지 않는 것이 가장 좋습니다.
암호	액세스를 제어하기 위해 사용되는 암호를 입력합니다. 금지된 문자를 사용하지 않는 것이 가장 좋습니다.

텍스트 상자	설명
	주의: 암호를 안전한 곳에 적어둡니다. Dell 지원부에서는 암호를 복구할 수 없습니다. 암호화 키를 만들어 하나 이상의 보호된 시스템에 적용하면 암호를 유실할 경우 데이터를 복구할 수 없습니다.
암호 확인	암호를 다시 입력합니다. 암호 입력을 확인하는 데 사용됩니다.

5 **확인**을 클릭합니다.
대화 상자가 닫히고 작성된 암호화 키가 암호화 키 페이지에 표시됩니다.

6 보호된 시스템에 암호화 키를 적용하려면 보호된 시스템 페이지에서 암호화 키 적용을(를) 참조하십시오.

암호화 키 가져오기

다른 Rapid Recovery Core에서 암호화 키를 가져온 후 이 키를 사용하여 Core의 보호된 시스템에 대한 데이터를 암호화할 수 있습니다. 키를 가져오려면 Core 시스템에서 로컬로 또는 네트워크를 통해 키에 액세스할 수 있어야 합니다. 또한 암호화 키의 암호를 알아야 합니다.

암호화 키를 가져오려면 다음 단계를 완료하십시오.

노트: 이 절차는 보호된 시스템에 키를 적용하지 않습니다. 암호화 키 적용에 대한 자세한 내용은 보호된 시스템 페이지에서 암호화 키 적용을(를) 참조하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다.

3 **가져오기**를 클릭합니다.
파일 업로드 대화 상자가 나타납니다.

4 **파일 업로드** 대화 상자에서, 가져올 암호화 키가 포함된 네트워크 또는 로컬 디렉터리로 이동합니다.
예를 들어 로그인 사용자에 대한 **다운로드** 폴더로 이동합니다.

키 파일 이름은 "EncryptionKey-"로 시작하고 키 ID가 다음에 나오며 .key(파일 확장명)로 끝납니다. 예를 들어, 샘플 암호화 키 이름은 EncryptionKey-RandomAlphabeticCharacters.key입니다.

5 가져오려는 키를 선택한 후 **열기**를 클릭합니다.

6 **키 가져오기** 대화 상자에서 **확인**을 클릭합니다.
대화 상자가 닫히고 가져온 암호화 키가 **암호화 키** 페이지에 표시됩니다. 암호화 키를 내보내기 전에 볼륨을 보호하는 데 사용한 경우 키 상태는 잠김입니다.

암호화 키 잠금 해제

암호화 키는 잠금 해제됨 또는 잠김 상태를 포함할 수 있습니다. 리포지토리의 해당 시스템에 대해 저장된 백업 데이터를 보호하려면 보호된 시스템에 잠금 해제된 암호화 키를 적용하십시오. 잠금 해제된 암호화 키를 사용하는 Rapid Recovery Core에서는 복구 지점에서 데이터를 복구할 수도 있습니다.

암호화 키를 Rapid Recovery Core에 가져올 때 이 키의 기본 상태는 잠김입니다. 이것은 키를 명시적으로 가져왔는지 여부나 암호화된 보호된 시스템을 복제하거나 암호화된 복구 지점의 아카이브를 가져와서 Rapid Recovery Core에 암호화 키가 추가되었는지 여부와 관계 없습니다.

복제만으로 Rapid Recovery Core에 추가된 암호화 키의 경우, 키를 잠금 해제할 때 암호화 키가 잠금 해제된 상태로 유지될 기간(시간, 일 또는 개월 수)을 지정할 수 있습니다. 각 날짜는 잠금 해제 요청이 Rapid Recovery Core에 저장된 시간부터 24시간 단위를 기준으로 합니다. 예를 들어, 키가 화요일 오전 11시 24분에 잠금 해제되었고 선택한 기간이 2일이면 키는 같은 주의 목요일 오전 11시 24분에 자동으로 다시 잠깁니다.

노트: 잠긴 암호화 키를 사용하여 데이터를 복구하거나 보호된 시스템에 적용할 수 없습니다. 먼저 암호를 제공하여 키를 잠금 해제해야 합니다.

또한 잠금 해제된 암호화 키를 잠궈 키가 잠금 해제될 때까지 보호된 시스템에 키를 적용할 수 없도록 할 수 있습니다. 범용 상태의 암호화 키를 잠그려면 먼저 키 상태를 Replicated(복제됨)로 변경해야 합니다.

잠금 해제된 암호화 키가 현재 Core의 시스템을 보호하는 데 사용 중인 경우 암호화 키를 잠그려면 먼저 보호된 시스템에서 해당 키의 연결을 해제해야 합니다.

잠긴 암호화 키를 잠금 해제하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다. 상태 열은 잠긴 암호화 키를 나타냅니다.

3 잠금 해제할 암호화 키를 찾은 다음 드롭다운 메뉴 을 선택하고 **잠금 해제**를 선택합니다.
암호화 키 잠금 해제 대화 상자가 나타납니다.

4 대화 상자의 Passphrase(암호) 필드에 암호를 입력하여 이 키를 잠금 해제합니다.

5 키가 잠금 해제된 상태를 유지할 기간을 지정하려면 기간 옵션에서 다음 작업 중 하나를 수행합니다.
- 키를 명시적으로 잠글 때까지 키가 잠금 해제 상태를 유지하도록 지정하려면 Rapid Recovery에서 **수동으로 잠글 때까지**를 선택합니다.
- 시간, 일 또는 개월로 구성하는 기간 동안 키가 잠금 상태를 유지하도록 지정하려면 다음을 수행합니다.
  - 번호 필드를 선택하고 1에서 999 사이의 값을 입력합니다.
  - 기간을 시간, 일 수 또는 개월 수로 각각 선택합니다.
  - 그런 다음 **확인**을 클릭합니다.
    이 옵션은 복제로 추가된 암호화 키에 사용할 수 있습니다.

    대화 상자가 닫히고 선택한 키 암호화 키의 변경 사항이 암호화 키 페이지에 표시됩니다.
- 지정하는 날짜와 시간까지 키가 잠금 상태를 유지하도록 지정하려면 다음을 수행합니다.
  - **기한** 옵션을 선택합니다.
  - 텍스트 필드 또는 일정 및 시계 위젯을 사용하여 암호화 키를 잠그려는 날짜와 시간을 명시적으로 시정합니다.
  - 그런 다음 **확인**을 클릭합니다.
    이 옵션은 복제로 추가된 암호화 키에 사용할 수 있습니다.

    대화 상자가 닫히고 선택한 키 암호화 키의 변경 사항이 암호화 키 페이지에 표시됩니다.

암호화 키 잠금

암호화 키 상태가 잠겨 있으면 잠금이 해제될 때까지 보호된 시스템에 이 키를 적용할 수 없습니다. 범용 유형의 암호화 키를 잠그려면 먼저 키의 유형을 복제됨으로 변경해야 합니다.

암호화 키를 잠그려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다. 상태 열은 잠금 해제된 암호화 키를 나타내고 각 키의 유형을 표시합니다.

3 잠그려는 암호화 키를 찾습니다. 유형이 범용인 경우, 해당 드롭다운 메뉴 를 클릭하고 **유형을 복제됨으로 변경**을 선택합니다.
암호화 키 유형 변경 대화 상자가 나타납니다.

4 대화 상자에서 키 유형을 **복제됨**으로 변경할 것임을 확인합니다.

5 암호화 키 상태가 복제됨으로 변경되면 해당 드롭다운 메뉴 를 클릭하고 **잠금**을 선택합니다.

암호화 키 잠금 대화 상자가 나타납니다.

6 대화 상자에서 키를 잠근다는 것을 확인합니다.
대화 상자가 닫히고 선택한 암호화 키의 상태는 잠김입니다.

노트: 이 옵션은 복제로 추가된 암호화 키에 사용할 수 있습니다.

암호화 키 편집

암호화 키를 정의한 후 암호화 키의 이름이나 키에 대한 설명을 편집할 수 있습니다. 이 속성은 암호화 키 창에서 암호화 키 목록을 볼 때 표시될 수 있습니다.

잠금 해제된 기존 암호화 키의 이름이나 설명을 편집하려면 다음 단계를 완료하십시오.

주의: 하나 이상의 시스템을 보호하는 데 사용되는 암호화 키의 이름이나 설명을 편집하면 Rapid Recovery는 새로운 기본 이미지를 캡처합니다. 이 기본 이미지 스냅숏은 해당 시스템에서 다음에 예약 또는 작성된 스냅숏에 나타납니다.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다.

3 편집하려는 암호화 키를 찾아서 다음을 수행합니다.
- 키가 잠겨 있는 경우, 먼저 잠금을 해제해야 합니다. 을 참조하십시오. 암호화 키 잠금 해제
- 키가 잠금 해제된 경우, 아래에 설명된 대로 진행합니다.

4 지정된 암호화 키에 대한 드롭다운 메뉴를 클릭하고 **편집**을 선택합니다.
암호화 키 편집 대화 상자가 표시됩니다.

5 대화 상자에서 암호화 키의 이름이나 설명을 편집한 후 **확인**을 클릭합니다.
대화 상자가 닫히고 선택한 암호화 키의 변경 사항이 **암호화 키** 페이지에 표시됩니다.

암호화 키 암호 변경

보안을 최대로 유지하기 위해 기존 암호화 키에 대한 암호를 변경할 수 있습니다. 암호화 키의 암호를 변경하려면 다음 단계를 완료하십시오.

주의: 하나 이상의 시스템을 보호하는 데 사용하는 암호화 키의 암호를 편집하고 난 후 Rapid Recovery Core는 다음에 예약하거나 작성된 스냅숏에서 해당 시스템의 증분 스냅숏을 캡처합니다.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다.

3 업데이트하려는 암호화 키를 찾아서 해당 드롭다운 메뉴를 클릭하고 **암호 변경**을 선택합니다.
암호 변경 대화 상자가 표시됩니다.

4 대화 상자에서 **암호** 필드에 암호화를 위한 새 암호를 입력합니다.

5 **암호 확인** 필드에 동일한 암호를 다시 입력합니다.

6 **확인**을 클릭합니다.
대화 상자가 닫히고 암호가 업데이트됩니다.

7 선택적으로, 설명 필드에 힌트를 사용하는 경우, 암호화 키를 편집하여 힌트를 업데이트합니다. 자세한 내용은 암호화 키 편집을 (를) 참조하십시오.

주의: Rapid Recovery는 256비트 키를 가지는 CBC(Cipher Block Chaining) 모드에서 AES 256비트 암호화를 사용합니다. Dell은 안전한 위치에 암호를 기록하고 이 정보를 업데이트하도록 권장합니다. Dell 지원부에서는 암호를 복구할 수 없습니다. 암호가 없으면 암호화된 복구 지점에서 정보를 복구할 수 없습니다.

암호화 키 내보내기

다른 Core에서 암호화 키를 사용하기 위해 Rapid Recovery Core에서 암호화 키를 내보낼 수 있습니다. 이 절차를 수행할 때 암호화 키는 활성 Windows 사용자 계정에 대한 **Downloads** 폴더에 저장됩니다.

암호화 키를 내보내려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다.

3 내보내려는 암호화 키를 찾고 드롭다운 메뉴를 클릭한 다음 **내보내기**를 선택합니다.
EncryptionKey-[name.key] 열기 대화 상자가 나타납니다.

4 대화 상자에서 **파일 저장**을 선택하여 암호화 키를 안전한 위치에 저장한 후 **확인**을 클릭합니다.
암호화 키가 활성 Windows 사용자 계정의 **Downloads** 폴더와 같이 기본 위치에 텍스트 파일로 다운로드됩니다.

5 선택적으로, 이 키를 다른 Core에 가져오려는 경우 해당 Core에서 액세스할 수 있는 위치에 파일을 복사합니다.

암호화 키 제거

Encryption Keys(암호화 키) 페이지에서 암호화 키를 제거하면 해당 키가 Rapid Recovery Core에서 삭제됩니다.

노트: 암호화 키를 제거한다고 해서 이 키를 사용하여 이미 저장된 복구 지점의 암호가 해독되는 것은 아닙니다. 기존 암호화된 복구 지점의 데이터를 복구하려면 이 키에 대한 암호를 여전히 보관하고 제공해야 합니다.

이미 보호된 시스템과 연결된 암호화 키는 제거할 수 없습니다. 먼저 키를 사용하는 각 보호된 시스템에 대한 암호화 설정을 확인한 후 제거할 암호화 키를 연결 해제해야 합니다. 자세한 내용은 보호된 시스템에서 암호화 키 연결 해제 항목을(를) 참조하십시오.

암호화 키를 제거하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다.

3 제거하려는 암호화 키를 찾습니다. 해당 드롭다운을 클릭하고 **제거**를 선택합니다.
암호화 키 제거 대화 상자가 나타납니다. 암호화 키 제거 작업을 확인하는 메시지가 표시됩니다.

4 대화 상자에서 암호화 키를 제거할 것임을 확인합니다.

노트: 암호화 키를 제거한다고 해서 이 키를 사용하여 이미 저장된 복구 지점의 암호가 해독되는 것은 아닙니다. 기존 암호화된 복구 지점의 데이터를 복구하려면 이 키에 대한 암호를 여전히 보관하고 제공해야 합니다.

대화 상자가 닫히고 제거된 암호화 키가 **암호화 키** 페이지에 더 이상 표시되지 않습니다.

암호화 키 유형 변경

암호화 키는 암호화 키 창에 두 가지 가능한 상태인 범용 또는 복제 중 하나를 나열합니다. 유형은 암호화 키의 가능한 출처를 나타내고 키의 세부 정보 또는 암호를 변경할 수 있는지 여부를 결정합니다. 유형이 범용인 경우에만 이러한 특성을 수정할 수 있습니다. 복

제된 유형의 키에 대한 해당 특성을 수정하려면 이 절차에 따라 키 유형을 범용으로 변경해야 합니다. 암호화 키의 상태를 범용으로 변경할 때 키는 수동으로 잠금 해제되고 다른 보호된 시스템을 암호화하는 데 사용될 수 있습니다.

노트: 복제됨에서 범용으로 유형을 변경하려면 암호를 알고 있어야 합니다.

또한 암호화 키에는 두 가지 가능한 상태인 잠김 또는 잠금 해제됨이 있습니다. 상태에 따라 암호화 키를 보호된 시스템에 적용하거나 암호화로 복구 지점에서 데이터를 복원할 수 있습니다. 상태가 잠금 해제인 경우에만 암호화 키의 유형을 수동으로 변경할 수 있습니다.

암호화 키를 처음 만들 때 키 상태는 범용 및 잠금 해제됨입니다. 이러한 키는 즉시 사용할 수 있습니다. 예를 들어, 보호된 시스템에 대한 백업을 암호화하는 데 사용할 수 있습니다. 단, 범용 키 유형은 수동으로 잠글 수 없습니다. 범용 유형의 암호화 키를 수동으로 잠그려면 이 절차에 따라 상태를 복제됨으로 변경해야 합니다.

하나 이상의 보호된 시스템에 대한 복구 지점 암호화에 이미 사용 중인 경우 암호화 키 유형을 변경할 수 없습니다.

암호화 키 유형을 변경하려면 이 절차를 따릅니다.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **암호화 키**를 선택합니다.
암호화 키 페이지가 나타납니다. Core에 액세스할 수 있는 암호화 키가 요약 표로 나타납니다. 각각 범용 또는 복제 유형으로 나열됩니다.

3 업데이트하려는 암호화 키를 찾습니다.

4 범용 암호화 키를 복제로 변경하려는 경우 다음을 수행합니다.

a 드롭다운 메뉴 을 클릭하고 **복제로 유형 변경**을 선택합니다.
암호화 키 유형 변경 대화 상자가 나타납니다. 유형을 복제로 변경할 것인지 확인하는 메시지가 표시됩니다.

- 대화 상자에서 유형을 복제로 변경할 것을 확인합니다.

대화 상자가 닫히고 암호화 키 유형이 복제로 업데이트됩니다.

5 복제 암호화 키를 범용으로 변경하려는 경우 다음을 수행합니다.

a 드롭다운 메뉴 을 클릭하고 **범용으로 유형 변경**을 선택합니다.
암호화 키 유형 변경 대화 상자가 나타납니다. 유형을 범용으로 변경할 것인지 확인하는 메시지가 표시됩니다.

- 대화 상자의 **암호** 필드에 암호를 입력한 다음 **확인**을 클릭하여 유형을 범용으로 변경할 것을 확인합니다.

대화 상자가 닫히고 암호화 키 유형이 범용으로 업데이트됩니다.

클라우드 계정 관리

이 장에서는 기존 클라우드 저장소 공급자 계정에 대한 링크를 정의하고 Rapid Recovery에서 사용하도록 해당 클라우드 계정을 관리하는 방법에 대해 설명합니다. 예를 들어, Rapid Recovery 데이터를 클라우드에 아카이브하거나, 클라우드에서 아카이브된 데이터를 가져올 수 있습니다.

클라우드 계정 정보

Rapid Recovery를 사용하여 데이터를 다양한 클라우드 공급자에 아카이브하거나 클라우드 계정에 저장된 아카이브된 데이터를 가져올 수 있습니다. 호환 가능한 클라우드에는 Microsoft Azure, Amazon™, Rackspace 및 OpenStack 기반 제공업체가 있습니다.

Rapid Recovery Core Console에 기존 클라우드 계정을 추가할 수 있습니다. 계정을 추가했으면 정보를 편집하거나 계정 연결 옵션을 구성하거나 Rapid Recovery에서 계정을 제거할 수 있습니다.

클라우드 계정 추가

클라우드 계정 및 Core 사이에서 데이터를 이동하려면 Rapid Recovery Core Console에 클라우드 공급자 계정 정보를 추가해야 합니다. 이 정보는 Core Console에서 클라우드 계정을 식별하고 연결 정보를 안전하게 캐싱합니다. 그런 다음 이 프로세스를 사용하면 Rapid Recovery Core가 클라우드 계정에 연결하여 지정한 작업을 수행할 수 있습니다.

클라우드 계정을 추가하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console 아이콘 표시줄에서 **자세히** 아이콘을 클릭한 다음 **클라우드 계정**을 선택합니다.
클라우드 계정 페이지가 나타납니다.

2 **클라우드 계정** 페이지에서 **새 계정 추가**를 클릭합니다.
Add New Account(새 계정 추가) 대화 상자가 열립니다.

3 클라우드 유형 드롭다운 목록에서 호환 가능한 클라우드 제공업체를 선택합니다.

4 3단계에서 선택한 클라우드 유형에 따라 다음 표에 설명된 세부 정보를 입력합니다.

표 37. 클라우드 계정 세부 정보

클라우드 유형	텍스트 상자	설명
Microsoft Azure	저장소 계정 이름	Microsoft Azure 저장소 계정의 이름을 입력합니다. **노트: 이름은 Azure의 저장소 계정 이름과 정확히 일치해야 합니다. 이름은 소문자와 숫자만 포함할 수 있으며 3~24자여야 합니다.**
	액세스 키	계정에 대한 액세스 키를 입력합니다. **노트: 주 키 또는 보조 키를 입력할 수 있습니다. Azure 계정에서 액세스 키를 가져오려면 설정에서 키를 확인합니다.**
	https 프로토콜 사용	표준 http 프로토콜 대신 보안 https 프로토콜을 사용하려면 이 옵션을 선택합니다.
	표시 이름	Rapid Recovery Core Console에 표시할 이 클라우드 계정의 표시 이름을 입력합니다(예: Microsoft Azure 1).
Amazon™ S3	액세스 키	Amazon™ 클라우드 계정의 액세스 키를 입력합니다.
	비밀 키	이 계정에 대한 비밀 키를 입력합니다.
	표시 이름	Rapid Recovery Core Console에 표시할 이 클라우드 계정의 표시 이름을 입력합니다(예: Amazon 1).
OpenStack 제공	Region(지역)	사용자 클라우드 계정의 영역을 입력합니다.
	사용자 이름	OpenStack 기반 클라우드 계정에 대한 사용자 이름을 입력합니다.
	암호 또는 API 키	암호 또는 API 키를 사용할지 선택한 후 이 계정의 선택 영역을 입력합니다.
	테넌트 ID	이 계정에 대한 테넌트 ID를 입력합니다.
	인증 URL	이 계정에 대한 인증 URL를 입력합니다.
	표시 이름	Rapid Recovery Core Console에 표시할 이 클라우드 계정의 표시 이름을 입력합니다(예: OpenStack 1).

클라우드 유형	텍스트 상자	설명
Rackspace 클라우드 파일	Region(지역)	드롭다운 목록을 사용하여 계정의 영역을 선택합니다.
	사용자 이름	Rackspace 클라우드 계정에 대한 사용자 이름을 입력합니다.
	암호 또는 API 키	암호 또는 API 키를 사용할지 선택한 후 이 계정에 대한 선택 내용을 입력합니다.
	테넌트 ID	이 계정에 대한 테넌트 ID를 입력합니다.
	인증 URL	이 계정에 대한 인증 URL를 입력합니다.
	표시 이름	Rapid Recovery Core Console에 표시할 이 클라우드 계정의 표시 이름을 입력합니다(예: Rackspace 1).

5 **저장**을 클릭합니다.
대화 상자가 닫히고 계정이 Core Console의 **클라우드 계정** 페이지에 나타납니다.

클라우드 계정 편집

클라우드 계정에 연결하기 위한 정보를 변경해야 할 경우(예를 들어, 암호를 업데이트하거나 표시 이름을 편집해야 할 경우) Rapid Recovery Core Console의 클라우드 계정 페이지에서 동일한 작업을 수행할 수 있습니다. 다음 절차의 단계를 완료하여 클라우드 계정을 편집하십시오.

1 Rapid Recovery Core Console 아이콘 표시줄에서 **자세히** 아이콘을 클릭한 다음 **클라우드 계정**을 선택합니다.
클라우드 계정 페이지가 나타납니다.
2 편집할 클라우드 계정 옆에서 드롭다운 메뉴를 클릭한 다음 **편집**을 클릭합니다.
계정 편집 창이 열립니다.
3 필요에 따라 세부정보를 편집한 다음 **저장**을 클릭합니다.

노트: 클라우드 유형을 편집할 수 없습니다.

클라우드 계정 설정 구성

클라우드 구성 설정을 통해 제한된 시간 내에 Rapid Recovery에서 클라우드 계정 연결을 시도하기 위한 시간 간격을 결정할 수 있습니다. 다음 절차의 단계를 완료하여 클라우드 계정에 대한 연결 설정을 구성하십시오.

1 Rapid Recovery Core Console 아이콘 표시줄에서 **설정**을 클릭합니다.
설정 페이지가 나타납니다.
2 왼쪽 메뉴에서 **클라우드 계정**을 클릭합니다.
3 클라우드 계정 표에서 구성하려는 클라우드 계정 옆의 드롭다운 메뉴를 클릭한 후 다음 작업 중 하나를 수행합니다.
- 클라우드 계정 연결의 설정을 변경하려면 **편집**을 클릭합니다.
  1 클라우드 구성 대화 상자에서 다음 작업 중 하나를 수행합니다.
    - **요청 시간 제한:** 위쪽과 아래쪽 화살표를 사용하여 클라우드 계정 연결이 지연될 때 Rapid Recovery의 1회 연결 시도에 소요되는 시간(분/초)을 결정합니다. 입력한 시간이 지나면 연결 시도가 중단됩니다.
    - **쓰기 버퍼 크기:** 아카이브된 데이터를 클라우드에 쓰기 위해 예약하는 버퍼 크기입니다.
    - **읽기 버퍼 크기:** 클라우드에서 아카이브된 데이터를 읽기 위해 예약하는 블록 크기입니다.
  2 **확인**을 클릭합니다.
- 클라우드 구성을 기본 설정으로 되돌리려면 **재설정**을 클릭합니다.
  - **요청 시간 제한:** 01:30(분/초)

- **쓰기 버퍼 크기:** 8388608(바이트)
- **읽기 버퍼 크기:** 8388608(바이트)

클라우드 계정 제거

클라우드 서비스를 중단하거나 특정 Core에 대한 서비스 사용을 중지하기로 결정할 경우 Core Console에서 클라우드 계정을 제거할 수 있습니다. 다음 절차의 단계를 완료하여 클라우드 계정을 제거하십시오.

1 Rapid Recovery Core Console 아이콘 표시줄에서 **자세히** 아이콘을 클릭한 다음 **클라우드 계정**을 선택합니다. **클라우드 계정** 페이지가 나타납니다.
2 편집할 클라우드 계정 옆에서 드롭다운 메뉴를 클릭한 다음 **제거**를 클릭합니다.
3 **계정 삭제** 대화 상자에서 **예**를 클릭하여 계정을 제거할 것임을 확인합니다.
4 클라우드 계정을 현재 사용 중이면 두 번째 대화 상자에서도 제거할 것인지 확인합니다. **예**를 클릭하여 확인합니다.

노트: 현재 사용 중인 계정을 제거하면 이 계정에 대해 예약된 모든 아카이브 작업이 실패합니다.

아카이브

이 섹션은 아카이브 생성에 대한 비즈니스 사례, Rapid Recovery를 사용하여 아카이브를 생성하는 방법, 저장할 수 있는 위치에 대해 설명합니다.

아카이브 이해

보존 정책은 백업이 단기 미디어(가격이 높고 속도가 빠름)에 저장되는 기간을 적용합니다. 때때로 특정 비즈니스 및 기술 요구사항에 따라 이러한 백업 보존 기간을 연장해야 하지만 고속 저장소의 사용은 감당하기에 비용이 너무 많이 듭니다. 따라서 이러한 요구사항은 장기 저장소(가격이 낮고 속도가 느림)를 필요로 합니다. 종종 회사에서는 준수 및 비준수 데이터를 모두 보관하는 데 장기 저장소를 사용합니다. Rapid Recovery의 아카이브 기능은 준수 및 비준수 데이터의 연장 보존을 지원하는 데 사용되며, 복제 데이터를 원격 복제 Core에 시딩하는 데도 사용됩니다.

아카이브가 생성되면 다음과 같은 방법으로 사용할 수 있습니다.

- 아카이브를 단순 파일 또는 폴더 복구용 파일 시스템으로 탑재할 수 있습니다.
- 아카이브를 운영 체제 미설치의 소스로 사용할 수 있습니다.
- 리포지토리에 아카이브를 가져올 수 있습니다.

아카이브 만들기

이 절차를 사용하여 일회성 또는 예약된 아카이브를 만들 수 있습니다.

클라우드 위치에 아카이브를 만들려는 경우 먼저 클라우드 계정을 Rapid Recovery Core Console에 추가합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.

일회성 아카이브는 지정된 시스템에 대해 주문형으로 만든 아카이브입니다. 예약된 아카이브는 사용자가 마법사에서 지정한 날짜와 시간에 자동으로 반복되는 아카이브입니다. 이것은 매번 수동으로 아카이브를 만들어야 하는 불편함 없이, 시스템의 빈번한 아카이브를 저장하려는 위치를 수용하는 반복적인 아카이브를 예약하는 기능이 있습니다.

1 Rapid Recovery Core Console의 단추 모음에서 **아카이브**를 클릭합니다.

아카이브 마법사가 열립니다.

2 마법사의 **유형 아카이브** 페이지에서 다음 옵션 중 하나를 선택합니다.
- 일회성 아카이브
- 연속 아카이브(일정 기준)

3 **다음**을 클릭합니다.

4 **위치** 페이지의 **위치 유형** 드롭다운 목록에서 옵션을 선택한 뒤 다음 표의 설명에 따라 정보를 입력하십시오.

표 38. 아카이브의 위치 유형 옵션

옵션	텍스트 상자	설명
로컬	위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.
	폴더 이름	아카이브된 데이터를 저장할 폴더의 이름을 입력합니다.

5 **다음**을 클릭합니다.

6 마법사의 **시스템** 페이지에서, 아카이브하려는 보호된 시스템을 선택합니다.

7 **다음**을 클릭합니다.

8 다음 작업 중 하나를 수행합니다.
- 일회성 아카이브를 만들도록 선택한 경우 15단계로 건너뜁니다.
- 예약된 아카이브를 만들도록 선택한 경우 9단계를 계속 진행합니다.

9 **예약** 페이지의 **데이터 전송** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
- 매일
- 매주
- 매월

10 9단계에서 선택한 항목을 기반으로 다음 표에 설명된 대로 정보를 입력합니다.

표 39. 데이터 전송 옵션

옵션	텍스트 상자	설명
매일	시간	매일 아카이브를 만들 시간을 선택합니다.
매주	요일	아카이브를 자동으로 만들 요일을 선택합니다.
	시간	아카이브를 만들 시간을 선택합니다.
매월	날짜	아카이브를 자동으로 만들 매월 날짜를 선택합니다.
	시간	아카이브를 만들 시간을 선택합니다.

11 또한 마법사를 완료한 뒤에 다음 예약 시간에 아카이브 작업을 시작하지 않으려는 경우 **초기 아카이브 일지 중지**를 선택합니다.

노트: 아카이브가 다시 시작되기 전에 대상 위치를 준비하기 위한 시간이 필요하면 예약된 아카이브를 일시 중지해야 할 수 있습니다. 이 옵션을 선택하지 않으면 예약된 시간에 아카이브가 시작됩니다.

12 **다음**을 클릭합니다.

13 연속 아카이브의 **옵션** 페이지에서 다음 표에 설명되어 있는 재활용 작업 중 하나를 선택합니다.

표 40. 연속 아카이브 재활용 옵션

텍스트 상자	설명
증분	기존 아카이브에 복구 지점을 추가할 수 있습니다. 이것은 복구 지점을 비교하여 아카이브에 이미 있는 데이터의 중복 제거를 방지합니다.
이 Core 교체	이 Core와 관련된 기존의 아카이브된 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다.
완전 삭제	새 아카이브를 쓰기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다.

14 또한 **복구 지점망 구축(분리된 항목 수정)**을 선택한 뒤 18단계로 건너뜁니다.

15 일회성 아카이브의 **옵션** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 41. 일회성 아카이브 옵션

텍스트 상자	설명
최대 크기	대형 데이터 아카이브를 여러 세그먼트로 나눌 수 있습니다. 다음 작업 중 하나를 수행하여 아카이브를 만들기 위해 예약할 최대 공간을 선택합니다. · **전체 대상**을 선택하여 4단계에서 제공한 대상에 있는 경로에서 사용할 수 있는 모든 공간을 예약합니다. 예를 들어, 위치가 D:\work\archive인 경우 D: 드라이브에서 사용할 수 있는 모든 공간이 예약됩니다. · 빈 텍스트 상자를 선택하고 위 및 아래 화살표를 사용하여 공간을 입력한 다음, 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다. **노트: Amazon™ 클라우드 아카이브는 자동으로 50GB 세그먼트로 분할됩니다. Microsoft Azure 클라우드 아카이브는 200GB 세그먼트로 자동 분할됩니다.**
휴지통 작업	다음 휴지통 작업 옵션 중 하나를 선택합니다. · 재사용 안 함. 위치에서 기존의 아카이브된 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있지 않은 경우 Rapid Recovery에서 다른 위치를 선택합니다. · 이 Core 바꾸기. 이 Core와 관련된 기존의 아카이브된 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다. · 완전 삭제. 새 아카이브를 쓰기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다. · 증분. 기존 아카이브에 복구 지점을 추가할 수 있습니다. 이것은 복구 지점을 비교하여 아카이브에 이미 있는 데이터의 중복 제거를 방지합니다.
설명	아카이브를 캡처하기 위해 필요한 추가 정보를 입력합니다. 설명은 나중에 아카이브를 가져오면 표시됩니다.
복구 지점망 구축 (분리된 항목 수정)	이 옵션을 선택하여 전체 복구 지점망을 저장합니다. 이 옵션은 기본적으로 선택됩니다.

16 **다음**을 클릭합니다.

17 **날짜 범위** 페이지에서 저장할 복구 지점의 시작일과 종료일을 수동으로 입력하거나 캘린더 창 아래의 시계 아이콘과 캘린더 아이콘을 차례대로 클릭하여 날짜와 시간을 선택합니다.

18 **마침**을 클릭합니다.

마법사가 닫힙니다.

클라우드에 아카이브

데이터의 보존 기간이 끝날 때 오래된 데이터의 아카이브를 만들어 해당 보존 기간을 연장할 수 있습니다. 데이터를 아카이브할 때 항상 데이터를 저장할 위치의 문제가 있습니다. Rapid Recovery를 사용하면 Core Console에서 직접 다양한 클라우드 제공업체에 아카이브를 업로드할 수 있습니다. 호환 가능한 클라우드에는 Microsoft Azure, Amazon™, Rackspace 및 OpenStack 기반 제공업체가 있습니다.

Rapid Recovery를 사용하여 아카이브를 클라우드로 내보낼 경우 다음 절차가 포함됩니다.

- Rapid Recovery Core Console에 클라우드 계정을 추가합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.
- 데이터를 아카이브하고 클라우드 계정으로 내보냅니다. 자세한 내용은 아카이브 만들기을(를) 참조하십시오.
- 클라우드 위치에서 아카이브된 데이터를 가져와서 이를 검색합니다. 자세한 내용은 아카이브 가져오기를 참조하십시오.

예약된 아카이브 편집

Rapid Recovery를 사용하여 예약된 아카이브의 세부 정보를 변경할 수 있습니다. 예약된 아카이브를 편집하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console, 아이콘 표시줄에서 **자세히** 드롭다운 메뉴를 클릭한 다음 **아카이브**를 선택합니다.
2 아카이브 페이지, 아카이브 예약에서 변경하려는 아카이브 옆의 드롭다운 메뉴를 클릭한 다음 **편집**을 클릭합니다.
아카이브 추가 마법사가 열립니다.
3 아카이브 마법사의 **위치** 페이지에 있는 **위치 유형** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드
4 3단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 아카이브의 세부 정보를 입력합니다.

표 42. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.

옵션	텍스트 상자	설명
	폴더 이름	보관된 데이터를 저장하려는 폴더의 이름을 입력합니다(예: Rapid-Recovery-Archive-[DATE CREATED]-[TIME CREATED]).

5 **다음**을 클릭합니다.

6 마법사의 **시스템** 페이지에서, 아카이브할 복구 지점이 포함된 보호 시스템을 선택합니다. 아카이브하지 않을 시스템은 지웁니다.

7 **다음**을 클릭합니다.

8 **예약** 페이지의 **데이터 전송** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 매일
- 매주
- 매월

9 8단계에서 선택한 항목을 기반으로 한 다음 표와 같이 정보를 입력합니다.

표 43. 데이터 전송 옵션

옵션	텍스트 상자	설명
매일	시간	매일 아카이브를 만들 시간을 선택합니다.
매주	요일	아카이브를 자동으로 만들 요일을 선택합니다.
	시간	매일 아카이브를 만들 시간을 선택합니다.
매월	날짜	아카이브를 자동으로 만들 매월 날짜를 선택합니다.
	시간	매일 아카이브를 만들 시간을 선택합니다.

10 또는, 나중에 다시 시작하기 위해 아카이브를 연기하려면 **초기 아카이빙 일시 중지**를 선택합니다.

노트: 아카이브가 다시 시작되기 전에 대상 위치를 준비하기 위한 시간이 필요하면 예약된 아카이브를 일시 중지해야 할 수 있습니다. 이 옵션을 선택하지 않으면 예약된 시간에 아카이브가 시작됩니다.

11 **다음**을 클릭합니다.

12 **옵션** 페이지에서 **재활용 작업** 드롭다운 목록을 사용하여 다음 표에 설명된 옵션 중 하나를 선택합니다.

표 44. 아카이브 재활용 옵션

텍스트 상자	설명
Incremental(증분)	기존 아카이브에 복구 지점을 추가할 수 있습니다. 이것은 복구 지점을 비교하여 아카이브에 이미 있는 데이터의 중복 제거를 방지합니다.
이 Core 바꾸기	이 Core와 관련된 기존의 아카이브된 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다.
완전 삭제	새 아카이브를 쓰기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다.

13 또는, **복구 지점 체인 구축(분리 수정)**을 선택합니다.

14 **마침**을 클릭합니다.

Rapid Recovery는 변경 사항을 아카이브에 적용합니다.

예약된 아카이브 일시 중지 또는 다시 시작

예약된 아카이브 작업이 되풀이되면 필요에 따라 이 작업을 일시 중지하거나 다시 시작할 수 있습니다.

대상 아카이브 위치를 변경해야 하는 경우처럼, 예약된 아카이브 작업을 일시 중지해야 하는 경우가 있을 수 있습니다. 또한 아카이브 만들기 절차를 수행할 때 초기에 아카이브를 일시 중지하기로 선택했다면 나중에 예약된 아카이브를 다시 시작해야 할 수 있습니다. 다음 절차의 단계를 수행하여 예약된 아카이브를 일시 중지하거나 다시 시작하십시오.

1 Rapid Recovery Core Console의 아이콘 표시줄에서 **자세히** 메뉴를 클릭한 다음 **아카이브**를 클릭합니다.
2 **아카이브** 페이지의 예약된 아카이브 아래에서 다음 중 하나를 수행합니다.
   - 원하는 아카이브를 선택한 후, 다음 작업 중 하나를 적절하게 클릭합니다.
     - Pause
     - Resume
   - 원하는 아카이브 옆에 있는 드롭다운 메뉴를 클릭한 후, 다음 작업 중 하나를 적절하게 클릭합니다.
     - Pause
     - Resume

   아카이브 상태가 예약 열에 표시됩니다.

아카이브 작업 수행

이 절차를 사용하면 언제든지 예약된 아카이브에서 아카이브 작업을 수행하기 위해 Rapid Recovery를 수행할 수 있습니다.

아카이브 작업을 수행하려면 Core에 예약된 아카이브가 있어야 합니다.

1 아이콘 표시줄의 Rapid Recovery Core Console에서 **자세히** 드롭다운을 클릭한 다음 **아카이브**를 선택합니다.
2 아카이브 예약의 아카이브 페이지에서 강제로 적용할 아카이브 옆에 있는 드롭다운 메뉴를 클릭한 다음 **수행**을 클릭합니다.
   Rapid Recovery는 사용자가 설정한 예약된 아카이브 시간에 관계 없이 해당 아카이브에 대하여 선택한 설정에 따라 복구 지점을 아카이브합니다.

아카이브 검사

보관함을 검사하면 보관함과 해당 내용이 복원해도 될 정도로 안전한지 확인됩니다.

보관함 검사를 수행하여 보관함에서 해당 구조의 무결성, 데이터 세그먼트, 인덱스 파일을 스캔할 수 있습니다. 보관함 검사를 통해 보관함 내 필요한 모든 파일의 현재 상태와 파일의 안전 여부가 확인됩니다. 아카이브 확인을 수행하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 아이콘 표시줄의 **추가** 드롭다운 메뉴를 클릭한 후 **보관함**을 선택합니다.
2 **보관함** 페이지에서 **검사**를 클릭합니다.
   Check Archive(아카이브 확인) 대화 상자가 표시됩니다.
3 드롭다운 목록에서 다음 옵션 중 하나를 **Location Type(위치 유형)**으로 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드
4 3단계에서 선택한 위치 유형에 따라 다음 표에서 설명된 대로 보관함의 세부 정보를 입력합니다.

표 45. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	위치	아카이브 경로를 입력합니다.
네트워크	위치	아카이브 경로를 입력합니다.
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.
	폴더 이름	보관된 데이터를 저장할 폴더를 선택합니다(예: Rapid Recovery -5-Archive-[만든 날짜]-[만든 시간]).

5 다음 표에 설명된 검사 내용을 선택하거나 선택 취소합니다. 기본적으로 모두 선택되어 있습니다.

노트: 모든 검사 내용을 선택 취소하지 마십시오. 옵션을 하나 이상 선택해야 합니다.

옵션	설명
색인 파일 매핑 오프셋	보관함 내부 구조에서 모든 데이터가 올바른 위치에 있는지 검사하는 옵션입니다.
구조 무결성	특정 내부 파일의 현재 상태와 보관함 폴더 구조를 확인하는 옵션입니다. 파일 또는 폴더가 하나라도 누락되면 검사에 실패합니다.
체크섬 무결성	보관함의 데이터 세그먼트 무결성을 검사하여 세그먼트가 안전한지 확인하는 옵션입니다.

6 **파일 검사**를 클릭합니다.

Rapid Recovery에서는 선택 내용에 따라 보관함이 검사됩니다.

보관함 연결

보관함을 연결하면 보관함에서 복구 지점을 확인할 수 있습니다.

이 절차를 완료하려면 Rapid Recovery Core 6.0.1 이상에서 만들어진 보관함이 이미 있어야 합니다. 자세한 내용은 아카이브 만들기을(를) 참조하십시오.

보관함을 연결하면 사용자가 제공한 보관함 이름이 왼쪽 Core Console 탐색 메뉴에 보관함 이름으로 표시됩니다. 보관함에 복구 지점이 있는 보호된 시스템이 각각 보관함 메뉴 아래에 별도로 나열됩니다. 보관함의 아무 시스템 이름이나 클릭하여 해당 복구 지점을 찾아볼 수 있습니다. 그런 다음 현재 Core에 표시된 다른 복구 지점에도 같은 동작을 적용할 수 있습니다.

보관함을 연결하면 정보에 액세스하는 자격 증명도 캐시됩니다. 연결된 보관함 정의를 삭제할 때까지 보관함을 쉽게 다시 연결하고 분리하면서 복구 지점에 쉽게 액세스할 수 있습니다.

보관함을 연결하려면 이 절차를 사용합니다.

1 Rapid Recovery Core Console에서 **보관함** 드롭다운 메뉴를 클릭한 후 **보관함 연결**을 선택합니다.

보관함 연결 대화 상자가 표시됩니다.

2 **이름** 텍스트 상자에서 이 연결된 보관함의 이름을 입력합니다.

이 필드에 입력하는 값이 보관함 메뉴 이름으로 왼쪽 탐색 메뉴에 표시됩니다.

표시 이름의 모범 사례를 따르면 보관함 이름에는 공백을 포함하여 1~64자의 영숫자가 들어가야 합니다. 금지된 문자 또는 금지된 구문은 사용하지 마십시오.

3 **위치 유형** 드롭다운 목록의 다음 옵션 중에서 보관함의 위치 유형을 선택합니다.

- 로컬
- 네트워크
- 클라우드

4 3단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 보관함의 세부 정보를 입력합니다.

표 46. 위치 유형 세부 정보

옵션	텍스트 상자	설명
로컬	위치	보관함의 경로를 입력합니다(예: D:\Work\Archive).
네트워크	위치	보관함의 경로를 입력합니다(예: \\servername\sharename).
	사용자 이름	네트워크 공유에 로그인할 사용자 이름을 입력합니다.
	암호	네트워크 공유에 로그인할 암호를 입력합니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	계정에 연결된 보관함 컨테이너를 드롭다운 메뉴에서 선택합니다.
	폴더 이름	보관된 데이터의 폴더 이름을 입력합니다(예: Rapid-Recovery-Archive-[만든 날짜]-[만든 시간]).

5 **Attach(연결)**를 클릭합니다.

보관함이 이 Core에 연결되고 목차가 파일 시스템으로 탑재됩니다.

아카이브 가져오기

이 절차를 사용하여 한 번에 한 아카이브를 가져오거나 반복적으로 아카이브를 가져오도록 예약할 수 있습니다.

보관된 데이터를 복구하려면 지정된 위치로 전체 아카이브를 가져올 수 있습니다.

주의: 이 단계는 신중하게 고려한 후에만 수행하십시오. 아카이브를 가져오면 리포지토리가 아카이브의 내용으로 다시 채워져 아카이브를 캡처한 이후 리포지토리의 새 데이터를 교체합니다.

아카이브를 가져오려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core 콘솔의 메뉴 표시줄에서 **Archive(아카이브)** 드롭다운 메뉴를 클릭한 다음 **Import Archive(아카이브 가져오기)**를 선택합니다.

Import Archive Wizard(아카이브 가져오기 마법사)가 열립니다.

2 마법사의 **Import Type(가져오기 유형)** 페이지에서 다음 옵션 중 하나를 선택합니다.

- One-time import(일회 가져오기)
- Continuous import (by schedule)(연속 가져오기(일정에 따라))

3 **다음**을 클릭합니다.

4 **Location(위치)** 페이지의 드롭다운 목록에서 가져올 아카이브의 위치를 선택한 후에 다음 표에 설명되어 있는 대로 정보를 입력합니다.

표 47. 가져온 아카이브 위치 유형 옵션

옵션	텍스트 상자	설명
로컬	위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
	폴더 이름	보관된 데이터를 저장할 폴더의 이름을 입력합니다.

5 **다음**을 클릭합니다.

6 마법사의 **Archive Information(아카이브 정보)** 페이지에서 아카이브에 포함된 모든 시스템을 가져오려는 경우 **Import all machines(모든 시스템 가져오기)**를 선택합니다.

7 선택에 따라 다음 옵션 중 하나를 완료합니다.

- 2단계에서 **One-time import(일회 가져오기)**를 선택하고 6단계에서 **Import all machines(모든 시스템 가져오기)**를 선택하고 모든 시스템이 Core에서 보호됨, 복제됨 또는 복구 지점 전용 시스템으로 표시되는 경우 12단계로 이동합니다.
- 2단계에서 **Continuous import (by schedule)(연속 가져오기(일정에 따라))**를 선택하고 6단계에서 **Import all machines(모든 시스템 가져오기)**를 선택하고 하나 이상의 시스템이 Core에서 보호됨, 복제됨 또는 복구 지점 전용 시스템으로 표시되지 않는 경우 **Next(다음)**를 클릭한 후 9단계로 이동합니다.
- 6단계에서 모든 시스템을 가져오지 않은 경우 **Next(다음)**를 클릭한 후 8단계를 계속합니다.

8 **Machines(시스템)** 페이지에서 아카이브에서 가져오려는 시스템을 선택합니다.

- 2단계에서 **One-time import(일회 가져오기)**를 선택하고 하나 이상의 시스템이 Core에서 보호됨, 복제됨 또는 복구 지점 전용 시스템으로 표시되지 않는 경우 드롭다운 목록을 사용하여 가져오려는 각 시스템에 대한 리포지토리를 선택한 후 12단계로 이동합니다.
- 모든 시스템이 이미 Core에 보호됨, 복제됨 또는 복구 지점 전용 시스템으로 표시되는 경우 12단계로 이동합니다.

9 **다음**을 클릭합니다.

10 **Repository(리포지토리)** 페이지에서 다음 옵션 중 하나를 완료합니다.

- 리포지토리가 Core와 관련이 있는 경우 다음 표의 옵션 중 하나를 선택합니다.

표 48. 리포지토리 옵션

옵션	설명
기존 리포지토리 사용	드롭다운 목록에서 이 Core와 현재 연결된 리포지토리를 선택합니다.
리포지토리 생성	Server(서버) 텍스트 상자에 새 리포지토리를 저장하려는 서버의 이름을 입력합니다(예: servername 또는 localhost). 그런 다음, DVM 리포지토리 생성의 내용을 참조하십시오.

- 리포지토리가 Core와 관련이 없는 경우 새 리포지토리를 저장하려는 서버의 이름을 입력합니다(예: servername 또는 localhost). 그런 다음, DVM 리포지토리 생성의 내용을 참조하십시오.

11 **Schedule(일정)** 페이지의 2단계에서 **Continuous import (by schedule)(연속 가져오기(일정에 따라))**를 선택한 경우 다음 표에 설명되어 있는 옵션을 선택합니다.

표 49. 일정 가져오기 옵션

옵션	설명
매일	시계 아이콘을 클릭하고 위로 및 아래로 화살표를 사용하여 보관 작업을 시작하려는 시간을 선택합니다. 12시간 시스템을 사용하는 경우 오전 또는 오후 버튼을 클릭하여 시간을 지정합니다.
매주	요일을 선택한 다음 아카이브 작업을 시작하려는 시간을 선택합니다. 12시간 시스템을 사용하는 경우 오전 또는 오후 버튼을 클릭하여 시간을 지정합니다.
매월	일자를 선택한 다음 보관 작업을 시작하려는 시간을 선택합니다. 12시간 시스템을 사용하는 경우 오전 또는 오후 버튼을 클릭하여 시간을 지정합니다.
초기 가져오기 일시 중지	마법사를 완료한 후 다음 예약된 시간에 가져오기 작업을 시작하고 싶지 않은 경우 이 옵션을 선택합니다. **노트: 가져오기를 재개하기 전에 대상 위치를 준비할 시간이 필요할 경우 예약된 가져오기를 일시 중지할 수 있습니다. 이 옵션을 선택하지 않으면 예약된 시간에 가져오기가 시작됩니다.**

12 **마침**을 클릭합니다.

이벤트

Rapid Recovery Core에는 사전 정의된 이벤트 집합이 있습니다. 이러한 이벤트를 사용하여 관리자에게 Core에 대한 위험 문제 또는 백업, 가상 내보내기, 복제 등과 관련된 작업에서 발생하는 문제를 알릴 수 있습니다.

이 섹션에서는 Rapid Recovery Core Console에 표시되는 이벤트를 보는 방법을 설명합니다. 또한 이메일 알림 설정을 포함하여 이벤트 알림 방법 및 구성에 대해 자세히 알아볼 수 있습니다. 끝으로 알림을 구성하여 이벤트 로그를 보관하는 시간을 변경하고 반복되는 이벤트 알림을 줄일 수 있습니다.

Rapid Recovery 이벤트

Rapid Recovery Core에는 Core 또는 보호되는 시스템의 백업 작업에서 심각한 문제가 발생할 때 관리자에게 알려줄 수 있는 일련의 이벤트가 미리 정의되어 있습니다.

- 알림 그룹을 구성하여 시스템이 이러한 알림(이메일, 팝업 경고 등)에 대해 사용하는 방법뿐만 아니라 경고를 트리거하는 이벤트 유형을 정의합니다. 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.
- 관리자가 이메일을 사용하여 알림을 수신하려는 경우 알림 그룹 구성 이외에 이메일 서버를 구성하고 이메일 알림 템플릿을 구성해야 합니다. 자세한 내용은 이메일 서버 구성 및 전자 메일 알림 템플릿 구성을(를) 각각 참조하십시오.
- 반복 감소 기능을 사용하여 Events(이벤트) 페이지에 나타나는 동일한 유형 및 범위의 이벤트의 수를 줄일 수 있습니다. 반복 감소 기능은 기본값으로 활성화되어 있습니다. 이 기능을 비활성화하거나 이벤트가 이벤트 로그에서 단일 발생에 결합되는 시간 범위를 제어할 수 있습니다. 자세한 내용은 반복 감소 구성 정보을(를) 참조하십시오.
- 이벤트 및 작업 내역 정보가 Core 콘솔의 Events(이벤트) 페이지에 유지되는 기간을 제어할 수 있습니다. 자세한 내용은 이벤트 보존 구성을(를) 참조하십시오.

작업, 경고, 저널을 사용하여 이벤트 보기

Core Console에서 Core에 대한 이벤트를 볼 수 있으며, 특정 보호된 시스템 또는 복제된 시스템에 대한 이벤트도 볼 수 있습니다.

Core Console의 **이벤트** 페이지는 Rapid Recovery Core와 관련된 모든 시스템 이벤트 로그를 표시합니다. Core에 대한 이벤트에 액세스하여 내용을 보려면 (이벤트)를 클릭합니다.

특정 보호된 시스템 또는 복제된 시스템의 **이벤트** 페이지는 이 특정 시스템과 관련한 이벤트 로그를 표시합니다. 선택한 시스템의 이벤트에 액세스하여 내용을 보려면 보호된 시스템 메뉴에서 시스템 이름을 클릭하고 이 시스템의 **요약** 페이지에서 **이벤트** 메뉴를 클릭합니다.

Core 또는 지정된 시스템과 관련한 이벤트 페이지의 내용은 세 가지 섹션 즉, 작업, 경고, 저널로 나뉩니다. 이러한 보기는 다양한 이벤트의 세부 정보를 적절하게 필터링할 수 있습니다.

알림 그룹을 구성하여 다양한 이벤트를 알리는 방법을 정의할 수 있습니다. 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

모든 이벤트의 작업, 경고, 저널을 보려면 다음 단계를 완료하십시오.

- 작업 보기
- 경고 보기
- 모든 이벤트 보기

작업 보기

작업은 정기적으로 예약된 백업의 데이터 전송 또는 복구 지점에서 복원 수행 등 Rapid Recovery Core에서 수행해야 하는 작업입니다.

작업이 실행 중이면 Core Console 상단의 **실행 중인 작업** 드롭다운 메뉴에 나열됩니다. 실행 중인 작업을 클릭하면 Monitor Active Task(활성 작업 모니터링) 대화 상자가 열립니다.

Rapid Recovery Core의 모든 작업 또는 특정 시스템과 연관된 모든 작업을 볼 수도 있습니다.

1 Rapid Recovery Core에 대한 모든 작업을 보려면 아이콘 표시줄에서 (이벤트)를 클릭합니다.
특정 보호된 시스템에서 작업을 보려는 경우 특정 시스템의 **요약** 페이지로 이동한 다음 **이벤트** 메뉴를 클릭합니다.

2 작업만 보려면 페이지의 왼쪽 상단에서 **작업**을 클릭합니다. 기본 보기입니다.
이벤트 목록이 필터링되어 Core 또는 선택한 시스템의 작업만 표시됩니다.

3 (선택 사항) 키워드, 시작 날짜, 종료 날짜 또는 해당 조합으로 작업 목록을 필터링하려면 다음 작업을 수행합니다.
   a 키워드로 필터링하려면 **검색 키워드** 텍스트 상자에 키워드를 입력합니다.
   예를 들어, "롤업", "아카이브" 또는 "전송" 등의 키워드로 필터링할 수 있습니다.
   b 시작 날짜와 시간으로 필터링하려면 다음 옵션 중 하나를 사용하여 시작 날짜와 시간을 입력합니다.
      - **시작 시간** 텍스트 상자에 MM/DD/YYYY HH:MM AM/PM 형식으로 날짜와 시간을 입력합니다. 예를 들어, 2016년 1월 1일 오전 8시부터 검색하려면 1/1/2016 8:00 AM을 입력합니다.
      - 현재 날짜 및 시간을 선택하려면 **일정** 위젯을 **시작 시간** 텍스트 상자에서 클릭한 다음 현재 날짜를 클릭합니다. 현재 시간이 자동으로 나타납니다.
      - **일정** 위젯을 클릭하고 날짜를 선택한 다음 시계 위젯을 클릭하고 컨트롤을 사용하여 원하는 시간을 선택합니다. 선택한 변경 사항을 수락하려면 일정에서 클릭합니다.
   c 나타나는 작업 목록을 더욱 세분화하기 위해 동일한 형식으로 종료 날짜와 시간을 정의할 수도 있습니다.
   작업 목록이 선택한 기준에 따라 즉시 필터링됩니다.

4 (선택 사항) 다음과 같이 목록에 나타나는 작업을 필터링할 수 있습니다.

옵션	설명
	활성 작업만 보려면 **활성 작업** 아이콘을 클릭합니다.
	대기열에서 수행 대기 중인 작업만 보려면 **큐 작업** 아이콘을 클릭합니다.
	수행 대기 중인 작업만 보려면 **대기 중인 작업** 아이콘을 클릭합니다.
	완료된 작업만 보려면 **완료된 작업** 아이콘을 클릭합니다.
	실패한 작업만 보려면 **실패한 작업** 아이콘을 클릭합니다.

옵션	설명

5 작업 목록을 내보내려면 목록에서 형식을 선택한 다음 **내보내기**를 클릭합니다. 그 결과 생성되는 대화 상자에서, 내보내기를 확인한 다음 **확인**을 클릭합니다.

다음 형식을 사용하여 내보낼 수 있습니다.

표 50. 내보내기 형식

형식	설명
PDF	휴대용 문서 형식(기본 내보내기 형식)
HTML	웹 페이지 형식
CSV	Comma-separated values
XLS	Microsoft Excel® 1997 - 2003 통합 문서
XLSX	Excel Workbook

사용자가 선택한 유형의 파일이 Core 서버의 기본 위치에 다운로드됩니다.

6 작업에 대해 **작업 세부 정보** 아이콘을 클릭하여 다음과 같은 작업 세부 정보가 있는 새 창을 시작합니다.

- 상태
- Total work(총 작업)(완료된 크기 또는 백분율)
- Start Date and Time(시작 날짜 및 시간)
- End Date and Time(종료 날짜 및 시간)
- 속도
- Elapsed time(경과된 시간)
- 단계(하위 작업의 경우)

경고 보기

경고는 작업 또는 이벤트와 관련된 알림입니다. 경고 유형에는 오류, 경고 또는 정보가 포함됩니다.

Rapid Recovery Core의 중요한 경고 또는 특정 시스템과 연결된 중요한 경고의 저널을 볼 수 있습니다.

1 Rapid Recovery Core에 대한 경고를 보려면 아이콘 표시줄에서 (이벤트)를 클릭하고 **경고**를 클릭합니다.

특정 보호된 시스템에 대한 경고를 보려면 지정된 시스템의 **요약** 페이지로 이동하고 **이벤트** 메뉴를 클릭하고 **경고**를 클릭합니다.

이벤트 목록을 필터링하여 Core 또는 선택한 시스템의 중요한 경고만 표시합니다.

2 필요한 경우 시작 날짜, 종료 날짜, 경고 메시지 설명 또는 이들의 조합으로 중요한 경고 목록을 필터링하려면 다음을 수행합니다.

a 시작 날짜와 시간으로 필터링하려면 다음 옵션 중 하나를 사용하여 시작 날짜와 시간을 입력합니다.

- **시작 시간** 텍스트 상자에 MM/DD/YYYY HH:MM AM/PM 형식으로 날짜와 시간을 입력합니다. 예를 들어, 2016년 1월 1일 오전 08:00부터 검색하려면 1/1/2016 8:00 AM을 입력합니다.
- 현재 날짜 및 시간을 선택하려면 **일정** 위젯을 **시작 시간** 텍스트 상자에서 클릭한 다음 현재 날짜를 클릭합니다. 현재 시간이 자동으로 나타납니다.

- Core 오른쪽에 있는 **일정** 위젯을 클릭하고 날짜를 선택한 다음 (시계) 위젯을 클릭하고 제어를 사용하여 원하는 시간을 선택합니다. 달력이 아닌 다른 위치를 클릭하여 선택한 변경 내용을 승인합니다.

b 경고 메시지 설명으로 필터링하려면 **메시지 검색** 텍스트 상자에 설명을 입력합니다.

예를 들어, 에이전트와 관련된 경고만 보려면 "에이전트"를 입력하고, 전송과 관련된 경고를 보려면 "전송"을 입력합니다.

c 나타나는 경고 목록을 더욱 세분화하기 위해 동일한 형식으로 종료 날짜와 시간을 정의할 수도 있습니다.

선택한 기준에 따라 경고 목록을 즉시 필터링합니다.

3 (선택 사항) 모든 경고를 제거하려면 **모두 해제**를 클릭합니다.

모든 이벤트 보기

Rapid Recovery Core의 모든 이벤트 또는 특정 시스템과 연결된 모든 이벤트를 볼 수 있습니다.

1 Rapid Recovery Core에 대한 모든 이벤트의 저널을 보려면 아이콘 표시줄에서 (이벤트)를 클릭하고 **저널**을 클릭합니다.

Rapid Recovery Core에 대한 모든 이벤트를 보려면 Rapid Recovery Core 홈 페이지로 이동하고 (이벤트)를 클릭합니다.

특정 보호된 시스템에 대한 모든 이벤트의 저널을 보려면 지정된 시스템의 **요약** 페이지로 이동하고 **이벤트** 메뉴를 클릭하고 **저널**을 클릭합니다.

2 필요한 경우 시작 날짜, 종료 날짜, 경고 메시지 설명 또는 이들의 조합으로 모든 이벤트 목록을 필터링하려면 다음을 수행합니다.

a 시작 날짜와 시간으로 필터링하려면 다음 옵션 중 하나를 사용하여 시작 날짜와 시간을 입력합니다.

- **시작 시간** 텍스트 상자에 MM/DD/YYYY HH:MM AM/PM 형식으로 날짜와 시간을 입력합니다. 예를 들어, 2016년 1월 1일 오전 08:00부터 검색하려면 1/1/2016 8:00 AM을 입력합니다.
- 현재 날짜 및 시간을 선택하려면 **일정** 위젯을 **시작 시간** 텍스트 상자에서 클릭한 다음 현재 날짜를 클릭합니다. 현재 시간이 자동으로 나타납니다.
- Core 오른쪽에 있는 **일정** 위젯을 클릭하고 날짜를 선택한 다음 (시계) 위젯을 클릭하고 제어를 사용하여 원하는 시간을 선택합니다. 달력이 아닌 다른 위치를 클릭하여 선택한 변경 내용을 승인합니다.

b 경고 메시지 설명으로 필터링하려면 **메시지 검색** 텍스트 상자에 설명을 입력합니다.

예를 들어, 에이전트와 관련된 경고만 보려면 "에이전트"를 입력하고, 전송과 관련된 경고를 보려면 "전송"을 입력합니다.

c 나타나는 이벤트 목록을 더욱 세분화하기 위해 동일한 형식으로 종료 날짜와 시간을 정의할 수도 있습니다.

선택한 기준에 따라 이벤트 목록을 즉시 필터링합니다.

이메일 알림 이해

사용자가 지정하는 이메일 주소로 이메일 메시지를 보내 특정 이벤트에 대해 알리도록 Rapid Recovery Core를 설정할 수 있습니다. 경고를 트리거하는 이벤트는 다른 알림 방법과 마찬가지로 알림 그룹에 정의됩니다.

노트: 알림 그룹은 이메일을 알림 방법으로 사용하는지에 관계없이 설정해야 합니다. 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

이메일을 알림 옵션 중 하나로 선택하는 경우 이메일 SMTP 서버도 구성해야 합니다. Rapid Recovery Core는 알림 그룹에 있는 매개변수를 기반으로 경고를 보내기 위해 사용자가 정의하는 서버를 사용합니다.

또한, 이메일 알림 템플릿도 정의해야 합니다. Core에서 이 템플릿을 사용하여 각 경고에 대한 이메일 제목 줄과 이메일 메시지 본문 내용을 정의합니다. 템플릿에는 기본 설정이 있으며 기본값을 그대로 사용하거나 테스트하고 필요에 따라 수정할 수 있습니다.

이 절에는 다음과 같은 항목을 포함합니다.

- 이메일 서버 구성

이메일 서버 구성

이메일 서버를 구성하려면 다음 단계를 완료하십시오.

노트: 시스템에서 이메일 경고 메시지를 전송하려면 이메일로 알림 옵션 활성화를 포함하여 알림 그룹 설정을 구성해야 합니다. 이메일 경고를 수신하는 이벤트를 지정하는 방법에 대한 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 을 클릭하고 (설정) 다음 중 하나를 수행합니다.

- 설정 페이지 왼쪽의 Core 설정 목록에서 **SMTP 서버**를 클릭합니다.
- 설정 페이지의 오른쪽에서 **SMTP 서버** 제목이 표시될 때까지 아래로 스크롤합니다.

SMTP 서버 코어 설정이 표시됩니다.

3 변경하려는 설정을 클릭합니다.

선택한 설정을 편집할 수 있게 됩니다.

4 다음 표에 설명된 대로 구성 정보를 입력합니다.

옵션	설명
SMTP 서버	이메일 알림 템플릿에서 사용할 이메일 서버의 이름을 입력합니다. 이름 지정 규칙에는 호스트 이름, 도메인 및 접미어가 포함됩니다(예: smtp.gmail.com).
시작	반환 이메일 주소를 입력합니다. 이 주소는 이메일 알림 템플릿의 반환 이메일 주소를 지정하기 위해 사용됩니다(예: noreply@localhost.com).
사용자 이름	이메일 서버의 사용자 이름을 입력합니다.
암호	이메일 서버에 액세스하기 위해 필요한 사용자 이름과 연관된 암호를 입력합니다.
포트	포트 번호를 입력합니다. 이 번호는 이메일 서버에 대한 포트를 식별하기 위해 사용됩니다(예: Gmail의 경우 포트 587) 기본값은 25입니다.
제한 시간(초)	이메일 서버에 연결을 시도하는 기간을 지정하는 정수 값을 입력합니다. 이 값은 제한 시간이 발생하기 전의 시간(초)을 설정하는 데 사용됩니다. 기본값은 60초입니다.
TLS	메일 서버에서 TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer)과 같은 연결을 사용하는 경우 이 옵션을 선택합니다.

5 각 설정의 변경 내용에 만족하면 를 클릭하여 변경 내용을 저장하고 편집 모드를 저장하거나 를 클릭하여 저장하지 않고 편집 모드를 종료합니다.

주의: 각 변경 내용을 확인하지 않으면 설정이 변경되지 않습니다.

6 **테스트 이메일 보내기**를 클릭한 후 다음 작업을 수행합니다.

a **테스트 이메일 보내기** 대화 상자에 테스트 메시지의 대상 이메일 주소를 입력한 후 **보내기**를 클릭합니다.

b 테스트 메시지가 실패하면 오류 대화 상자와 **테스트 이메일 보내기** 대화 상자를 닫고 이메일 서버 설정을 수정합니다. 그런 다음 테스트 메시지를 다시 보냅니다.

c 테스트 메시지가 성공적이면 **확인**을 클릭하여 작업 성공을 확인합니다.

d 테스트 이메일 메시지를 보낸 이메일 계정을 확인합니다.

전자 메일 알림 템플릿 구성

전자 메일로 Rapid Recovery 이벤트의 알림을 활성화하면 기본적으로 기본 템플릿이 생성됩니다. Core에 대해 정의된 SMTP 전자 메일 서버는 이 템플릿을 사용하여 Rapid Recovery 이벤트에 관한 알림을 전자 메일을 통해 보냅니다.

이 항목에서는 기본 전자 메일 알림 템플릿 또는 콘텐츠 사용자 지정을 구성하는 과정을 설명합니다. Restore Default(기본값 복원) 옵션을 사용하면 언제든지 기본 알림 템플릿에 대한 변경 내용을 복원할 수 있습니다.

주의: 템플릿은 사용자가 위험을 감수하고 수정합니다. 템플릿 수정을 테스트할 책임은 사용자에게 있습니다. 기본 템플릿만 지원됩니다.

전자 메일 알림 템플릿을 구성하려면 이 절차의 단계를 완료하십시오.

노트: 전자 메일 경고 메시지를 보내기 전에 Notify by email(전자 메일로 알림) 활성화를 포함하여 전자 메일 서버 및 알림 그룹 설정도 구성해야 합니다. 전자 메일 경고를 수신하도록 전자 메일 서버를 구성하는 자세한 내용은 이메일 서버 구성을(를) 참조하십시오. 전자 메일 경고를 수신하도록 이벤트를 지정하는 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.

1 Rapid Recovery Core 콘솔로 이동합니다.

2 아이콘 표시줄에서 (더 보기)를 클릭한 다음 **Notifications(알림)**을 선택합니다.
Notifications(알림) 페이지가 나타납니다.

3 Email Settings(전자 메일 설정) 창에서 **Change(변경)**를 클릭합니다.
Edit Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자가 나타납니다.

4 **Enable Email Notifications(전자 메일 알림 활성화)**를 선택합니다.
전자 메일 템플릿이 활성화되고 표시됩니다. 기본 전자 메일 템플릿의 값은 다음 단계에서 설명합니다.

5 Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자의 내용을 검토하고 기본 콘텐츠가 필요한 내용인지 확인합니다.

옵션	설명
전자 메일 알림 활성화	이 설정은 전자 메일 알림 템플릿을 활성화하거나 비활성화합니다. · 전자 메일 알림을 활성화하려면 이 옵션을 선택합니다. · 전자 메일 알림을 비활성화하려면, 이 옵션을 지웁니다.
전자 메일 제목	이 텍스트 필드의 내용은 시스템 이벤트의 알림으로 전송되는 전자 메일 메시지 제목줄을 제어합니다. 기본 전자 메일 제목 행은 다음과 같습니다. `<hostName> <level>: <name> for <agentName>`

이메일	이 텍스트 영역의 내용은 시스템 이벤트의 알림으로 전송되는 전자 메일 메시지 본문을 제어합니다. 기본 전자 메일 본문 메시지는 다음과 같습니다.
	`<shortCompanyName> <coreProductName> on <hostName> has reported the <level> event "<name>"`
	
	`Date/Time: <localTimestamp>`
	
	`<message>`
	
	`<if(details.errorDetails)>`
	`<details.ErrorDetails.Message>`
	
	`<details.ErrorDetails.Details>`
	`<endif>`
	`---`
	
	`About this event: <description>`
	
	`<coreAdminUrl>`

Send Test Email(테스트 전자 메일 전송)	이 버튼을 클릭하면 **Send Test Email(테스트 전자 메일 전송)** 대화 상자에서 사용자가 지정하는 전자 메일 주소로 테스트 전자 메일 메시지가 전송됩니다.

옵션	설명
Restore Defaults(기본값 복원)	이 버튼을 클릭하면 전자 메일 템플릿에서 사용자 지정 변경 내용이 제거되고 전자 메일 제목 및 전자 메일 필드가 이 표에 설명되어 있는 기본 콘텐츠로 복원됩니다.
OK(양호)	이 버튼을 클릭하면 Edit Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자에 설정이 저장됩니다.
Cancel(취소)	이 버튼을 클릭하면 Edit Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자의 모든 변경 사항이 취소됩니다.

6 전자 메일 템플릿을 사용자 지정하려는 경우 이전 단계에서 설명한 텍스트 또는 변수를 변경하십시오. 기본적으로 사용되는 변수는 다음 표에 설명되어 있습니다.

옵션	설명
hostName	Core의 호스트 이름
details	특정 이벤트의 상세 정보 개체입니다.
agentname	이벤트가 단일 보호되는 시스템 범위를 가진 경우 이 이벤트와 관련된 보호되는 시스템의 이름입니다.
repositoryName	이벤트에 리포지토리 범위가 있는 경우 이 이벤트와 연관된 리포지토리의 이름입니다.
jobSummary	이벤트에 작업 범위가 있는 경우 이 이벤트와 연관된 작업의 요약입니다.
remoteSlaveCoreName	이벤트에 대상 Core 범위가 있는 경우 이 이벤트와 연관된 원격 대상 Core의 이름입니다.
remotemastercorename	이벤트에 소스 Core 범위가 있는 경우 이 이벤트와 연관된 원격 소스 Core의 이름입니다.
productName	제품의 이름,'Rapid Recovery Core'입니다. 이 제품 이름은 흰색 라벨을 사용하여 브랜딩을 위해 변경할 수 있습니다.
companyName	제품을 판매하는 회사의 이름입니다.

7 **Email Subject(전자 메일 제목)** 텍스트 상자에 전자 메일 템플릿의 제목을 입력합니다.

Email Subject(전자 메일 제목)는 전자 메일 알림 템플릿의 제목을 정의하는 데 사용됩니다. 예: <hostname> - <level> <name>.

8 **Email(전자 메일)** 텍스트 상자에 이벤트(이벤트가 있는 경우)와 심각도를 설명하는 템플릿 본문에 대한 정보를 입력합니다.

9 **Send Test Email(테스트 전자 메일 보내기)**를 클릭한 후 다음을 수행합니다.

a Send Test Email(테스트 전자 메일 보내기) 대화 상자에서, 테스트 메시지의 대상 전자 메일 주소를 입력한 다음 **Send(보내기)**를 클릭합니다.

b 테스트 메시지가 실패하는 경우 오류 대화 상자를 종료하고 Send Test Email(테스트 전자 메일 보내기) 대화 상자에서 **OK(확인)**를 클릭하여 현재 전자 메일 템플릿 설정을 저장합니다. 그런 다음 이메일 서버 구성 절차에 설명되어 있는 대로 전자 메일 서버 설정을 수정합니다. 해당 전자 메일 계정에 대한 암호를 다시 입력하합니다. 이러한 설정을 저장하고 이 절차로 돌아옵니다.

c 테스트 메시지가 성공하면 **OK(확인)**를 클릭하여 작업이 성공한 것을 확인합니다.

d 테스트 전자 메일 메시지를 보낸 전자 메일 계정을 확인합니다.

테스트의 결과에 만족했으면, Edit Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자로 돌아가 **OK(확인)**를 클릭하여 대화 상자를 닫고 설정을 저장합니다.

시스템 이벤트에 대한 알림 그룹, SMTP 설정 및 알림 템플릿

알림 그룹을 사용하면 사용자가 경고를 받는 특정 이벤트의 집합 및 알림이 발생하는 방식을 정의할 수 있습니다. 알림 그룹을 구성하거나 편집하려면 알림 그룹 구성을(를) 참조하십시오.

경고를 이메일 메시지로 보내려는 경우 SMTP(Simple Mail Transfer Protocol) 서버 설정도 구성해야 합니다. 이메일 서버 구성 설정을 구성하는 방법에 대한 자세한 내용은 이메일 서버 구성을(를) 참조하십시오.

이벤트 알림을 보내면 시스템은 이메일 알림을 사용합니다. 이 템플릿을 사용자 지정할 수 있습니다. 이메일 알림 템플릿 구성 또는 사용자 지정에 대한 자세한 내용은 전자 메일 알림 템플릿 구성을(를) 참조하십시오.

알림 그룹 구성

노트: 이 절차에 설명된 대로 경고를 이메일 메시지로 보내려면 SMTP(Simple Mail Transfer Protocol) 서버 설정도 구성해야 합니다. 이메일 서버 구성 설정에 대한 자세한 내용은 이메일 서버 구성에서 확인하십시오.

알림 그룹을 사용하여 사용자에게 경고할 특정 이벤트 집합과 알림이 발생하는 방식을 정의할 수 있습니다. 다음 방법을 사용하여 경고를 보내도록 구성할 수 있습니다.

- 이메일로
- Windows 이벤트 로그에서
- syslogd 사용
- Toast 경고 사용
- 경고 사용
- SNMP 트랩 사용

한 개 이상의 알림 그룹을 다양한 알림 매개변수로 구성할 수 있습니다.

알림 그룹은 Core 수준에서 또는 보호된 특정 시스템에 대해 설정할 수 있습니다.

경고에 대한 알림 그룹을 구성하려면 다음 단계를 완료하십시오.

1 다음 작업 중 하나를 수행합니다.

- 아이콘 모음에서 Core 수준으로 알림을 설정하려면 (자세히)를 클릭한 뒤 **알림**을 선택합니다.
  알림 페이지가 나타납니다.
- 보호된 특정 시스템에 대해 알림을 설정하려면 다음 작업을 수행합니다.
  1 보호된 시스템 메뉴에서 알림을 지정하려는 시스템을 클릭합니다.
  사용자 지정 알림 그룹 페이지가 표시됩니다.
  2 보호되는 시스템의 요약 페이지에 있는 자세히 드롭다운 메뉴에서 **알림**을 선택합니다.

  사용자 지정 알림 그룹 페이지가 표시됩니다.

2 **그룹 추가**를 클릭합니다.
알림 그룹 추가 대화 상자가 나타납니다.

알림 그룹을 사용하여 사용자에게 경고할 특정 이벤트 집합과 알림이 발생하는 방식을 정의할 수 있습니다. 다음 방법을 사용하여 경고를 보내도록 구성할 수 있습니다.

알림 그룹 추가 대화 상자에는 일반 설명 영역과 두 개의 탭이 포함되어 있습니다.

- 경고 사용
- 알림 옵션

3 다음 표에 설명된 대로 일반 설명 영역에 알림 그룹에 대한 기본 정보를 입력합니다.

옵션	설명
이름	이벤트 알림 그룹에 대한 이름을 입력합니다. 이 정보는 필수입니다. **주의: 알림 그룹 이름에 입력하는 값은 나중에 변경할 수 없습니다.**
설명	이벤트 알림 그룹에 대한 목적을 나타내는 설명을 입력합니다. 이 정보는 선택 사항입니다.

4 **경고 사용** 탭에서 기록하고 보고서를 작성하며 경고를 받으려는 시스템 이벤트 집합을 다음과 같이 정의합니다.

옵션	설명
모든 경고	모든 이벤트에 대한 경고를 생성하려면 **All Alerts(모든 경고)**를 선택합니다.

옵션	설명
오류	오류에 대한 경고를 생성하려면 **유형 선택** 메뉴에서 **오류**를 클릭합니다. 이 오류는 빨간색 X로 표시됩니다.
경고	오류에 대한 경고를 생성하려면 **유형 선택** 메뉴에서 **경고**를 클릭합니다. 이 경고는 노란색 느낌표 아이콘으로 표시됩니다.
정보	정보 메시지에 대한 경고를 생성하려면 **유형 선택** 메뉴에서 **정보**를 클릭합니다. 이 정보는 파란색 i로 표시됩니다.
Restore Defaults(기본값 복원)	경고 유형을 기본값으로 복원하려면 **유형 선택** 메뉴에서 **기본값 복원**을 클릭합니다. 이 항목은 왼쪽을 향하고 있는 짙은 파란색 화살표로 표시됩니다.

5 특정 이벤트 유형(오류, 경고 또는 정보 메시지)에 대한 경고를 생성하려면 다음 단계를 수행하십시오.

a **모든 경고** 옵션에 경고 그룹이 표시되지 않는 경우 모든 경고 레이블 앞의 닫는 꺾쇠 괄호 **>** 기호를 클릭합니다. 기호가 아래 방향 화살표로 바뀌고 보기가 확장되어 그룹이 표시됩니다.

b 그런 다음 특정 경고 그룹 옆의 닫는 꺾쇠 괄호 **>** 기호를 클릭하여 관련된 이벤트를 그룹에 표시합니다.

이벤트 그룹 범주는 다음과 같습니다.

- 아카이브
- 자동 보고서
- 연결성
- 자동 업데이트
- 백업 리포지토리
- 부트 CD
- 클라우드
- 클러스터
- Core 서비스
- 데이터베이스 보존
- 중복 제거 캐시
- DVM 리포지토리
- Exchange
- 내보내기
- 작업
- 라이센스
- 로컬 마운트
- 로그 잘라내기
- 메타데이터
- 야간 작업
- 알림
- Core 상태 지속
- PowerShell 스크립트 작성
- 보호
- 푸시 설치
- 복구 지점 검사
- 원격 마운트
- 리포지토리 공통
- 복제
- 복원
- 롤업
- 예약된 아카이브
- 보안

- 서버 로그
- vSphere

- 전체 그룹에서 모든 이벤트에 대한 경고를 정의하려면 **모든 경고**.확인란을 선택합니다.
- 경고 그룹의 모든 이벤트에 대해 경고를 정의하려면 해당 그룹 옆의 확인란을 선택합니다.
- 경고 그룹에서 일부 경고 유형만 선택하려면 그룹을 확장한 뒤 기록, 보고 및 경고를 설정하려는 특정 이벤트만 선택합니다.

6 **알림 옵션** 탭을 클릭합니다.

7 **알림 옵션** 탭에서 알림 프로세스 처리 방법을 지정합니다.

옵션	설명
이메일로 알림	이메일 알림의 수신자를 지정합니다. 여러 개의 이메일 주소는 물론 참조, 숨은 참조도 지정할 수 있습니다. 다음을 선택할 수 있습니다. • 수신: • 참조: • 숨은 참조:
Windows 이벤트 로그로 알림	Windows 이벤트 로그를 통해 경고를 보고하려면 이 옵션을 선택합니다.
시스템 로그로 알림	syslogd를 통해 경고를 보고하려면 이 옵션을 선택합니다. 다음 텍스트 상자에 syslogd에 대한 세부 정보를 지정합니다. • 호스트: • 포트:
Toast 경고로 알림	경고가 화면의 오른쪽 하단 모서리에 팝업으로 나타나도록 하려면 이 옵션을 선택합니다.
경고로 알림	Core Console의 우측 하단에 있는 팝업 창으로 경고를 표시하려면 이 옵션을 선택합니다.
SNMP 트랩으로 알림	Rapid Recovery Core는 SNMP 에이전트로 작동하여 트랩(특정 이벤트에 대한 알림)을 SNMP 관리자에게 보냅니다. 결과에서는 경고, 리포지토리 상태 및 보호된 시스템과 같은 Core 정보를 보고합니다. SNMP 트랩으로 Core 이벤트를 알리려면 이 옵션을 선택합니다. 또한 트랩 번호를 지정해야 합니다. 예를 들어, Rapid Recovery Core에서 사용하는 기본 트랩 번호는 162입니다.

8 **확인**을 클릭합니다.

그룹을 만든 후에는 정의된 알림 그룹 이름을 변경할 수 없다는 메시지가 표시됩니다. 알림 그룹 내 다른 속성은 언제든지 변경할 수 있습니다.

- 그룹 이름을 사용하려면 이 메시지를 확인하고 작업 내용을 저장합니다.
- 그룹 이름을 변경하려면 **아니요**를 클릭하여 알림 그룹 만들기 창으로 돌아가 그룹 이름 및 다른 알림 그룹 설정을 업데이트한 후 작업 내용을 저장합니다.

요약 표에 알림 그룹이 표시됩니다. 일련의 매개변수를 사용하여 다른 알림 그룹을 생성할 수 있습니다.

반복 감소 구성 정보

특정 이벤트 발생 시 관리자가 경고를 수신하는 기능은 중요합니다. 그러나 상황에 따라 이미 알고 있는 이벤트에 대한 알림을 반복적으로 수신하는 것이 불편할 수 있습니다. 즉시 확인하려는 환경 장애로 인해 경고가 생성되었어도 동일한 오류 조건에서 이벤트 로그에 수백 또는 수천 개의 이벤트를 생성할 수 있습니다. 이벤트 로그에서 반복을 줄이고 Core Console에서 동일한 이벤트에 대한 반복된 이메일 알림을 수신하는 불편함을 줄이기 위해 Rapid Recovery는 반복 감소 설정을 포함합니다. 이 설정은 기본적으로 활성화되었고 5분으로 설정되어 있습니다 이 설정을 최소 1분, 최대 60분으로 설정할 수 있으며, 완전히 사용하지 않을 수도 있습니다.

반복 감소를 사용할 수 없으면 동일한 유형 및 범위의 이벤트가 발생할 때마다 이벤트가 데이터베이스에 기록됩니다. 이전에 이벤트가 발생한 이후 경과한 시간에 상관 없이 이벤트는 새로 발생할 때마다 이벤트 탭의 경고 부분에 표시됩니다.

반복 감소가 구성되었으면(예를 들어, 기본 시간 5분) 특정 이벤트가 처음 발생할 때 이벤트는 데이터베이스에 기록되고 경고 로그에 표시됩니다. 이후 동일한 유형 및 범위의 이벤트가 설정된 시간 임계값 내에 다시 기록되면 데이터베이스에서 이벤트 수가 해당 임계값 내 각 반복 발생에 대해 1씩 증가합니다. 로그는 Events(이벤트) 페이지의 Alerts(경고) 영역에 표시됩니다. 그러나 최근 발생 날짜

및 시간과 함께 이벤트를 한 번만 표시합니다. 이벤트 로그는 처음 발생 후 시간 임계값이 만료되기 전에는 동일한 이벤트로 업데이트되지 않습니다. 예를 들어, 5분으로 설정된 상태에서 이벤트가 6분 후에 다시 발생하면 로그에 이벤트가 나타나고 다른 이메일 메시지를 수신합니다.

반복 감소 구성

이벤트에 대해 반복 감소를 구성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다. 아이콘 표시줄에서 (자세히)를 클릭한 다음 **알림**을 선택합니다.
알림 페이지가 나타납니다.

2 반복 감소 창에서 기존 설정을 확인합니다.

3 저장된 이벤트 임계값 시간을 활성화, 비활성화 또는 변경하려면 **변경**을 클릭합니다.
반복 감소 편집 대화 상자가 나타납니다.

4 다음 작업 중 하나를 수행합니다.
- 반복 감소를 비활성화하려면 **반복 감소 활성화** 옵션 선택을 해제합니다.
- 반복 감소를 활성화하려면 **반복 감소 활성화** 옵션을 선택합니다.
- 반복되는 동일한 이벤트가 무시되는 시간 임계값(분)을 변경하려면 **__ 분** 텍스트 상자에 1에서 60 사이의 숫자를 입력합니다.

노트: 이 값을 변경하려면 반복 감소 활성화 옵션을 선택해야 합니다.

5 **확인**을 클릭하여 설정을 저장하고 대화 상자를 닫습니다.

이벤트 보존 구성

지정된 시간에 Core에서 추적된 이벤트 및 작업 시간이 저장됩니다. 기본 설정은 30일입니다. 0에서 3652일(약 10년) 사이의 숫자로 설정할 수 있습니다.

이벤트 보존을 구성하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (설정)을 입력한 다음 다음 중 하나를 수행합니다.
- 설정 페이지의 왼쪽에 있는 Core 설정 목록에서 **데이터베이스 연결**을 클릭합니다.
- **데이터베이스 연결** 머리글을 볼 수 있을 때까지 설정의 왼쪽에서 아래쪽으로 스크롤합니다.

데이터베이스 연결 설정이 나타납니다.

3 이벤트 정보가 데이터베이스에 저장되는 일수를 변경하려면 **보존 기간(일)** 텍스트 필드를 클릭하고 0과 3652 사이의 값을 입력한 다음 를 클릭하여 변경 내용을 저장합니다.
이벤트 보존 기간이 지정한 대로 조정되었습니다.

신속한 어플라이언스 자동 복구

RASR(신속한 어플라이언스 자동 복구)는 어플라이언스를 작동 상태로 신속하게 복원하는 완전 복원 프로세스입니다.

RASR은 두 가지 복구 옵션을 제공합니다.

- 출하 시 설정 복원

- 어플라이언스를 오류 직전 상태로 복구(OS, 구성 및 설정이 복구됨)

RASR USB 키 만들기

RASR USB 키를 만들려면 다음을 수행합니다.

1 **Appliance(어플라이언스)** 탭으로 이동합니다.
2 왼쪽 탐색 창에서**Appliance(어플라이언스) > Backup(백업)**을 선택합니다.
Create RASR USB Drive(RASR USB 드라이브 생성) 창이 표시됩니다.

노트: RASR 키 생성을 시도하기 전에 16 GB 이상의 USB 키를 삽입합니다.

3 16 GB 이상의 USB 키를 삽입한 후에 **Create RASR USB Drive now(RASR USB 드라이브 지금 생성)**를 클릭합니다.
Prerequisite Check(필수 요소 확인) 메시지가 표시됩니다.
필수 요소를 확인한 후에는 **Create the RASR USB Drive(RASR USB 드라이브 생성)** 창에 USB 드라이브 생성에 필요한 최소 크기와 **가능한 대상 경로 목록**이 표시됩니다.
4 대상을 선택하고 **Create(생성)**를 클릭합니다.
경고 대화상자가 표시됩니다.
5 **Yes(예)**를 클릭합니다.
RASR USB 드라이브 키가 생성됩니다.
6 **노트: USB 키를 분리할 때에는 그에 앞서 Windows 꺼내기 드라이브 기능을 사용합니다. 그렇지 않으면 USB 키의 콘텐츠가 손상되어 USB 키가 예상대로 작동되지 않을 수 있습니다.**
각 DL 어플라이언스, 레이블에 대해 생성된 RASR USB 키를 분리하고 나중에 사용할 수 있도록 보관합니다.

RASR 실행

노트: Dell은 어플라이언스를 설정한 후 RASR USB 키를 생성할 것을 권장합니다. RASR USB 키를 생성하려면 Creating the RASR USB Key(RASR USB 키 생성)을 참조하십시오.

노트: 사용 가능한 최신 RUU가 있으며 어플라이언스에서 연결할 수 있는지 확인합니다.

.

노트: RASR을 사용하여 시스템 복구를 수행하려면 Dell.com/support/home에서 *신속한 어플라이언스 자동 복구(RASR)를 사용하여 Dell™ DL 백업 및 복구 어플라이언스 복구*를 참조하십시오.

공장 재설정을 수행하려면 다음 단계를 따르십시오.

1 생성된 RASR USB 키를 삽입합니다.
2 어플라이언스를 다시 시작해 **Boot Manager(부팅 관리자)(F11)**를 선택합니다.
3 **Boot Manager(부팅 관리자) 주 메뉴**에서 **One-shot BIOS Boot(단일 BIOS 부팅) 메뉴**를 선택합니다.
4 **Boot Manager Boot(부팅 관리자 부팅) 메뉴**에서 연결된 USB 드라이브를 선택합니다.
5 키보드 레이아웃을 선택합니다.
6 **Troubleshoot(문제 해결) > Rapid Appliance Self Recovery(신속한 어플라이언스 자동 복구)**를 클릭합니다.
7 대상 운영 체제(OS)를 선택합니다.
RASR가 시작되며 **Welcome(시작)** 화면이 표시됩니다.
8 **다음**을 클릭합니다.
Prerequisites(전제조건) 확인 화면이 표시됩니다.

노트: RASR을 수행하기 전 모든 하드웨어 및 기타 전제조건이 체크되도록 확인합니다.

9 **다음**을 클릭합니다.

세 가지 옵션과 함께 **Recovery Mode Selection(복구 모드 선택)** 화면이 표시됩니다.

- **시스템 복구**
- **Windows 복구 마법사**
- **공장 기본 재설정**

10 **Factory Reset(공장 기본 재설정)** 옵션을 선택합니다.
이 옵션을 사용하면 공장 기본 이미지에서 운영 체제 디스크가 복구됩니다.

11 **다음**을 클릭합니다.
다음과 같은 경고 메시지가 대화 상자에 표시됩니다. `This operation will recover the operating system. All OS disk data will be overwritten.`

12 **Yes(예)**를 클릭합니다.
운영 체제 디스크가 공장 기본 재설정으로 다시 복원되기 시작합니다.

13 복구 프로세스가 완료되면 **RASR Completed(RASR 완료됨)** 페이지가 표시됩니다. **Finish(마침)**를 클릭합니다.

14 복원 후 시스템을 부팅합니다.

15 **노트: AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)를 참조하는 경우에만 계속하고, 그렇지 않으면 17단계로 이동합니다.**

AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)가 로드될 때까지 기다립니다. Windows 작업 관리자를 사용하여 마법사를 닫습니다.

16 RUU 패키지에서 **launchRUU.exe** 파일을 실행합니다. 지침을 따르고 옵션을 선택하여 RUU 설치를 계속하고 RUU 설치를 완료합니다.

17 **DL Appliance Configuration Wizard(DL 어플라이언스 구성 마법사)**가 실행되고 복원 프로세스의 나머지를 안내합니다.

이제 어플라이언스가 정상적으로 작동합니다.

Local Mount Utility

이 섹션에서는 복구 지점을 탑재하기 위해 Windows 기반 Rapid Recovery LMU(Local Mount Utility)를 다운로드, 설치 및 사용하고 Rapid Recovery Core를 호스팅하지 않는 시스템을 사용하여 파일 수준에서 콘텐츠를 탐색하는 방법을 설명합니다.

Local Mount Utility 정보

LMU는 Windows 시스템의 세 가지 지원 모드에서 Rapid Recovery 복구 지점을 마운트할 수 있는, 다운로드 가능한 Windows 기반 응용 프로그램입니다. 이 경량형 유틸리티는 32비트 및 64비트 Windows 운영 체제에 설치할 수 있으며, rapidrecovery-vdisk(구 aavdisk) 및 aavstor 드라이버를 포함하지만 서비스로는 실행되지 않습니다. 이 유틸리티를 설치할 경우 기본적으로 **C:\Program Files \AppRecovery\Local Mount Utility** 디렉터리에 설치되며, 해당 시스템의 바탕 화면에 바로 가기가 나타납니다.

유틸리티는 Rapid Recovery Core 시스템에 원격으로 액세스하기 위해 설계되었지만, Rapid Recovery Core와 동일한 시스템에도 LMU를 설치할 수 있습니다. Core에서 실행할 때 응용 프로그램은 Rapid Recovery Core Console을 통해 수행된 마운트를 포함하여 해당 Core의 모든 마운트를 인식하고 표시합니다. 마찬가지로, LMU에서 수행된 마운트도 Core Console에 나타납니다.

LMU가 Mailbox Restore와 동일한 시스템에 설치된 경우 LMU를 사용하여 Exchange 데이터베이스를 열 때 Mailbox Restore을 자동으로 시작합니다. Mailbox Restore는 Microsoft Exchange 데이터 저장소 및 항목을 복원하는 데 사용하는 Dell Rapid Recovery 응용 프로그램입니다. LMU 또는 Rapid Recovery Core를 설치할 때 이 프로그램도 설치할 수 있습니다. Mailbox Restore에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery Mailbox Restore for Microsoft Exchange* 사용 설명서를 참조하십시오.

노트: Linux 시스템은 명령행 유틸리티, local_mount를 사용하여 Core에서 보호된 시스템 및 해당 복구 지점을 쿼리합니다. 마찬가지로 이 도구를 통해 사용자는 원격으로 복구 지점 볼륨을 마운트하고, 파일 수준에서 볼륨 내용을 탐색하고, 시스템 볼륨의 BMR를 포함하여 복구 지점에서 개별 파일 또는 전체 볼륨을 복원할 수 있습니다. 자세한 내용은 각각 Linux 시스템에서 복구 지점 볼륨 마운트, 명령줄을 사용하여 Linux 시스템의 볼륨 복원 및 Linux 시스템용 Bare Metal Restore 수행을(를) 참조하십시오.

Local Mount Utility에서 Rapid Recovery Core 시스템으로 작업

LMU(Local Mount Utility)를 사용하면 Core 수가 무제한인 시스템을 로컬 또는 원격으로 사용할 수 있습니다. Rapid Recovery Core 시스템에 LMU를 설치한 경우 해당 시스템이 LMU에 자동으로 localhost로 나타납니다. 모든 추가 원격 Core는 해당 Core를 추가할 때 입력한 정보에 따라 시스템 이름 또는 IP 주소로 나타납니다. LMU를 사용하여 Core 시스템을 추가, 편집 및 제거할 수 있습니다. 자세한 내용은 다음 절차에서 확인하십시오.

관련 링크

Local Mount Utility에 Core 시스템 추가
Local Mount Utility 옵션 변경
Local Mount Utility에서 Core 연결 설정 편집
Core에 다시 연결
Local Mount Utility에서 Rapid Recovery Core 시스템 제거

Local Mount Utility에 Core 시스템 추가

복구 지점을 마운트하려면 Core 시스템을 LMU에 추가해야 합니다. 추가할 수 있는 Core 수에 대한 제한은 없습니다.
Core를 추가하여 LMU를 설정하려면 다음 단계를 완료하십시오.

1 LMU가 설치된 시스템에서 바탕화면 아이콘을 두 번 클릭하여 LMU를 실행합니다.
2 다음 작업 중 하나를 수행합니다.
   - 왼쪽 위의 Local Mount Utility 메뉴에서 **Core 추가**를 클릭합니다.
   - 왼쪽 패널의 빈 공간을 마우스 오른쪽 단추로 클릭한 다음, **Core 추가**를 클릭합니다.

   Core 추가 대화 상자가 나타납니다.
3 **Core 추가** 대화 상자에 다음 표에 설명된 요청된 자격 증명을 입력합니다.

표 51. Rapid Recovery Core 자격 증명

옵션	설명
호스트 이름	복구 지점을 마운트할 Core의 이름 또는 IP 주소입니다. **노트: Rapid Recovery Core 시스템에 LMU를 설치할 경우 LMU가 자동으로 localhost 시스템을 추가합니다.**
포트	Core와 통신하는 데 사용되는 포트 번호. 기본 포트 번호는 8006입니다.
내 Windows 사용자 자격 증명 사용	Core에 액세스하는 데 사용하는 자격 증명이 Windows 자격 증명과 동일한 경우 이 옵션을 선택합니다.
특정 자격 증명 사용	Core에 액세스하는 데 사용하는 자격 증명이 Windows 자격 증명과 다른 경우 이 옵션을 선택합니다.
사용자 이름	Core 시스템에 액세스하는 데 사용된 사용자 이름입니다. **노트: 이 옵션은 특정 자격 증명을 사용할 것을 선택하는 경우에만 사용할 수 있습니다.**
암호	Core 시스템에 액세스하는 데 사용된 암호입니다.

옵션	설명
	노트: 이 옵션은 특정 자격 증명을 사용할 것을 선택하는 경우에만 사용할 수 있습니다.

4 **연결**을 클릭합니다.
5 다중 Core를 추가할 경우 필요에 따라 모든 단계를 반복합니다.

Local Mount Utility 옵션 변경

다음 절차를 완료하면 LMU에 연결된 모든 Rapid Recovery Core에 대한 옵션을 변경할 수 있습니다.

1 Local Mount Utility 사용자 인터페이스에서 **옵션**을 클릭합니다.
2 **옵션** 대화 상자에서 아래 표에 설명된 설정을 변경할 수 있습니다.

표 52. Core 설정

옵션	설명
기본 마운트 지점 리포지토리	**찾아보기** 단추를 사용하여 복구 지점 마운트에 사용할 위치에 대한 경로를 입력합니다.
내 Windows 사용자 계정 자격 증명 사용	Core에 로그인할 때 항상 기본적으로 Windows 자격 증명을 사용하려면 이 옵션을 선택합니다.
특정 자격 증명 사용	연결된 각 Core에 대해 다음과 같은 자격 증명을 사용하려면 이 옵션을 선택합니다. • **사용자 이름**: 모든 Core에 대해 사용할 사용자 이름을 입력합니다. • **암호**: 모든 Core에 대해 사용할 암호를 입력합니다.
Core 연결 시간 제한(초)	연결 시간이 초과하기 전에 LMU가 Core에 대한 연결 시도를 계속해야 하는 시간을 입력합니다(분 : 초 : 밀리초 단위).
언어	LMU를 표시할 언어를 선택합니다. 다음 옵션 중에서 선택할 수 있습니다. • 영어 • 프랑스어 • 독일어 • 포르투갈어 • 스페인어 • 중국어(간체) • 일본어 • 한국어

Local Mount Utility에서 Core 연결 설정 편집

Core를 LMU에 추가했을 때 설정된 설정을 편집하려면, 다음 절차를 완료합니다.

노트: 이 절차는 localhost Core에는 적용되지 않습니다. 원격 Core 시스템에만 적용됩니다.

1 Local Mount Utility 사용자 인터페이스에서, 설정을 편집하려는 Core를 마우스 오른쪽 단추로 클릭한 다음, **Core 편집**을 클릭합니다.
2 **Core 편집** 대화 상자에서 아래 표에 설명된 설정을 변경할 수 있습니다.

표 53. Core 설정

옵션	설명
호스트 이름	복구 지점을 마운트할 Core의 이름입니다. **노트: Rapid Recovery Core 시스템에 LMU를 설치할 경우 LMU가 자동으로 localhost 시스템을 추가합니다.**
포트	Core와 통신하는 데 사용되는 포트 번호. 기본 포트 번호는 8006입니다.
내 Windows 사용자 자격 증명 사용	Core에 액세스하는 데 사용하는 자격 증명이 Windows 자격 증명과 동일한 경우 이 옵션을 선택합니다.
특정 자격 증명 사용	Core에 액세스하는 데 사용하는 자격 증명이 Windows 자격 증명과 다른 경우 이 옵션을 선택합니다.
사용자 이름	Core 시스템에 액세스하는 데 사용된 사용자 이름입니다. **노트: 이 옵션은 특정 자격 증명을 사용할 것을 선택하는 경우에만 사용할 수 있습니다.**
암호	Core 시스템에 액세스하는 데 사용된 암호입니다. **노트: 이 옵션은 특정 자격 증명을 사용할 것을 선택하는 경우에만 사용할 수 있습니다.**

3 변경했으면 **확인**을 클릭합니다.

Core에 다시 연결

Rapid Recovery Core 시스템의 연결이 끊어지면 다음 단계를 통해 연결을 새로 고칠 수 있습니다.

Local Mount Utility 사용자 인터페이스에서 다음 중 하나를 수행합니다.

- Core가 오프라인이면 다시 연결하려는 Core를 두 번 클릭합니다.
  LMU가 Core에 다시 연결하려고 시도합니다.
- Core가 온라인이면 Core를 마우스 오른쪽 단추로 클릭하고 Core에 다시 연결을 클릭합니다.
  LMU이 연결을 새로 고칩니다.

Local Mount Utility에서 Rapid Recovery Core 시스템 제거

다음 절차를 완료하면 LMU에서 Core를 제거할 수 있습니다.

노트: 이 옵션은 localhost에 위치하여 localhost로 레이블된 Rapid Recovery Core에는 사용할 수 없습니다.

1 Local Mount Utility 사용자 인터페이스에서 제거하려는 Core를 마우스 오른쪽 단추로 클릭한 다음, **Core 제거**를 클릭합니다.
2 명령을 확인하려면 대화 상자에서 **예**를 클릭합니다.
LMU가 탐색 트리에서 Core 및 해당 보호된 시스템을 제거합니다.

Local Mount Utility에서 보호되는 시스템으로 작업

LMU(Local Mount Utility)를 사용하면 해당 시스템과 연결된 Rapid Recovery Core Console에 로그인하지 않고도 보호된 시스템에서 복구 지점을 마운트하고 찾아볼 수 있습니다. 자세한 내용은 다음 절차에서 확인하십시오.

- Local Mount Utility를 사용하여 복구 지점 마운트
- Local Mount Utility를 사용하여 마운트된 복구 지점 탐색
- 복구 지점 새로 고침
- Local Mount Utility를 사용하여 개별 복구 지점 분리
- 단일 Rapid Recovery Core 또는 보호된 시스템에서 모든 복구 지점 분리
- Local Mount Utility를 사용하여 탑재된 모든 복구 지점 분리

Local Mount Utility를 사용하여 복구 지점 마운트

LMU를 사용하면, 보호된 시스템, 복제된 시스템 및 복원 지점 전용 시스템을 포함하여 연결된 Core 시스템과 연관된 복구 지점을 마운트할 수 있습니다.

복구 지점을 마운트하기 전에 Local Mount Utility(LMU)를 복구 지점이 저장되어 있는 Core에 연결해야 합니다. 절차 Local Mount Utility에 Core 시스템 추가에 설명된 대로 LMU에 추가할 수 있는 Core 수에는 제한이 없습니다. 그러나 응용 프로그램은 한 번에 하나의 Core에만 연결할 수 있습니다. 예를 들어 한 Core에서 보호하는 시스템의 복구 지점을 마운트한 후 다른 Core에서 보호하는 다른 시스템의 복구 지점을 마운트하면 LMU가 자동으로 첫 번째 Core에서 분리되고 두 번째 Core와의 연결을 설정합니다.

1 Local Mount Utility 사용자 인터페이스에서, 탐색 트리의 Core를 확장하여 보호된 시스템을 표시합니다.

2 탐색 트리에서 복구 지점을 마운트하려는 시스템을 선택합니다.
복구 지점이 기본 프레임에 나타납니다.

3 (선택 사항) 마운트할 복구 지점을 확장하여 개별 디스크 볼륨 또는 데이터베이스를 표시합니다.

4 마운트할 복구 지점을 마우스 오른쪽 단추로 클릭한 후, 다음 옵션 중 하나를 선택합니다.

옵션	설명
마운트	이 옵션을 사용하면 복구 지점을 읽기 전용으로 마운트할 수 있습니다.
쓰기 가능으로 마운트	이 옵션을 사용하면 마운트된 복구 지점을 변경할 수 있습니다.
이전 쓰기를 포함한 읽기 전용으로 마운트	이 옵션은 복구 지점을 읽기 전용으로 마운트하고 이전에 수행된 모든 변경 사항을 포함시킵니다.
고급 마운트...	이 옵션은 고급 마운트 대화 상자를 엽니다.

5 **고급 마운트**를 선택한 경우, 다음 표에 설명되어 있는 옵션을 완료합니다.

표 54. 고급 마운트 옵션

옵션	설명
마운트 지점 경로	**찾아보기**를 클릭하여 기본 마운트 지점 경로가 아닌 다른 복구 지점에 대한 경로를 선택하거나 원하는 경로를 수동으로 입력합니다.
마운트 유형	다음 옵션 중 하나를 선택합니다. • 읽기 전용으로 마운트 • 쓰기 가능으로 마운트 • 이전 쓰기를 포함한 읽기 전용으로 마운트 각 옵션에 대한 설명은 4단계에서 참조하십시오.

- **마운트**를 클릭합니다.
LMU가 마운트된 복구 지점을 포함하는 폴더를 자동으로 엽니다.

노트: 이미 마운트된 복구 지점을 선택하는 경우 마운트 대화 상자에 복구 지점을 분리할 것인지 묻는 메시지가 나타납니다.

Local Mount Utility를 사용하여 마운트된 복구 지점 탐색

복구 지점을 탐색하면 Windows 탐색기 창에서 백업된 데이터가 열리며, 여기에서 복구하려는 항목의 볼륨이나 폴더를 검색할 수 있습니다.

그러면, Windows 탐색기와 같은 파일 관리자를 사용하여(또는 프로그래밍 방식으로 Windows API를 사용하여) 원하는 위치에 항목을 복사하여 항목을 복원할 수 있습니다. 현재 마운트된 복구 지점을 탐색하려면 다음 절차를 수행하십시오.

노트: 복구 지점을 마운트한 직후 탐색할 경우에는 마운트 절차가 완료된 후 복구 지점이 포함된 폴더가 자동으로 열리기 때문에 이 절차가 필요하지 않습니다.

1 Local Mount Utility 사용자 인터페이스에서 **활성 마운트**를 클릭합니다.
활성 마운트 창이 열리고 마운트된 모든 복구 지점을 표시합니다.
2 탐색 트리를 확장하여 각 시스템 및 해당 볼륨에 대해 마운트된 복구 지점을 표시합니다.
3 탐색하려는 볼륨 옆에 있는 **탐색**을 클릭합니다.

복구 지점 새로 고침

LMU를 Core 및 보호된 시스템에서 실시간으로 업데이트를 수신하지 않습니다. 보호된 시스템을 새로 고치고 최신 복구 지점을 보려면 다음 절차를 완료합니다.

Local Mount Utility 사용자 인터페이스에서 새로 고치려는 보호된 시스템을 마우스 오른쪽 단추로 클릭한 다음 복구 지점 새로 고침을 클릭합니다.

Local Mount Utility를 사용하여 개별 복구 지점 분리

LMU를 사용하여 원격 Core에서 복구 지점을 분리하려면 다음 절차를 완료하십시오.

1 Local Mount Utility 사용자 인터페이스에서 **활성 마운트**를 클릭합니다.
활성 마운트 창이 열리고 마운트된 모든 복구 지점을 표시합니다.
2 (선택 사항) **활성 마운트** 창에서, 더하기 또는 빼기 아이콘을 클릭하여 마운트된 각 복구 지점의 볼륨을 표시할 수 있습니다.
3 **활성 마운트** 창에서, 분리하려는 각 복구 지점 또는 볼륨 옆에 있는 **분리**를 클릭합니다.
선택한 복구 지점이 분리되면 진행률 창이 표시됩니다.
4 **활성 마운트** 창의 오른쪽 위에 있는 **x**를 클릭하여 창을 닫고 LMU로 돌아갑니다.

단일 Rapid Recovery Core 또는 보호된 시스템에서 모든 복구 지점 분리

단일 Core 또는 보호된 시스템에 탑재되어 있는 복구 지점만 분리하려면 다음 절차를 완료합니다.

1 Local Mount Utility 사용자 인터페이스에서 다음 중 하나를 수행합니다.
- 모든 복구 지점을 분리하려는 Core를 마우스 오른쪽 단추로 클릭합니다.
- 모든 복구 지점을 분리하려는 보호된 시스템을 마우스 오른쪽 단추로 클릭합니다.

2 **[machine_name]에 대하여 모두 분리**를 클릭합니다.
3 명령을 확인하려면 대화 상자에서 **예**를 클릭합니다.

노트: 기존 탑재를 사용하는 활성 작업이 있는 경우 이런 탑재를 분리하면 작업이 실패합니다.

선택에 대하여 탑재된 모든 복구 지점이 분리되었습니다.

Local Mount Utility를 사용하여 탑재된 모든 복구 지점 분리

LMU에서 한 번에 모든 복구 지점을 분리할 수 있는 두 가지 주요 방법이 있습니다. 현재 탑재된 복구 지점을 보지 않고 모든 복구 지점을 분리하거나 현재 탑재된 모든 복구 지점을 본 다음 이들을 모두 분리할 수 있습니다. 각각의 관련 절차를 참조하십시오.

모든 마운트 분리 버튼을 사용하여 모든 복구 지점 분리

마운트된 모든 복구 지점을 한 번에 분리하려면 다음 절차를 완료하십시오.

1 Local Mount Utility 메뉴에서 **모든 마운트 분리**를 클릭합니다.
2 명령을 확인하려면 대화 상자에서 **예**를 클릭합니다.

노트: 기존 탑재를 사용하는 활성 작업이 있는 경우 이런 탑재를 분리하면 작업이 실패합니다.

활성 탑재 창을 사용하여 복구 지점 모두 분리

활성 탑재 창에서 탑재된 복구 지점을 모두 한 번에 분리하려면 다음 절차를 완료합니다.

1 LMU 사용자 인터페이스에서 **활성 탑재**를 클릭합니다.
2 **활성 탑재** 창에서 **모두 분리**를 클릭합니다.
3 명령을 확인하려면 창에서 **예**를 클릭합니다.
4 **활성 탑재** 창에서 **닫기**를 클릭합니다.

Local Mount Utility 트레이 메뉴 사용

LMU 트레이 메뉴는 바탕 화면의 작업 표시줄에 있습니다. 아이콘을 마우스 오른쪽 단추로 클릭하여 다음 표에 설명된 옵션을 표시합니다.

표 55. 트레이 메뉴 옵션

옵션	설명
복구 지점 찾아보기	LMU 기본 창이 열립니다.
활성 마운트	LMU 기본 창 위에 활성 마운트 대화 상자가 열립니다.
옵션	LMU 기본 창 위에 옵션 대화 상자가 열립니다. 옵션 대화 상자에서 Local Mount Utility 사용자 인터페이스의 기본 마운트 지점 디렉터리 및 기본 Core 자격 증명을 변경할 수 있습니다.
정보	Local Mount Utility 라이센스 정보가 표시됩니다.
종료	LMU 응용프로그램이 닫힙니다.

3

어플라이언스 관리

Core 콘솔에는 공간 프로비저닝, 어플라이언스 상태 모니터링, 관리 도구 액세스에 사용할 수 있는 **Appliance(어플라이언스)** 탭이 있습니다.

주제:

- 어플라이언스 상태 모니터링
- Windows 백업
- 저장소 프로비저닝
- 가상 디스크의 공간 할당 삭제
- 복구 및 업데이트 유틸리티

어플라이언스 상태 모니터링

Appliance(어플라이언스) > **Health(상태)** 페이지를 사용하여 어플라이언스 하위 시스템의 상태를 모니터링할 수 있습니다. **Health(상태)** 페이지에는 각 하위 시스템 옆에 상태 표시등과 하위 시스템의 상태를 나타내는 상태 설명이 표시됩니다.

Health(상태) 페이지는 경고 또는 오류 문제를 해결하는 데 유용할 수 있는 각 하위 시스템의 상세 정보를 드릴다운하는 도구에 대한 링크를 제공합니다. 저장소 프로비저닝 하위 시스템에 사용할 수 있는 **Provisioning Status(프로비저닝 상태)** 링크는 해당 하위 시스템의 프로비저닝 상태를 표시하는 **Provisioning(프로비저닝)** 화면을 엽니다. Rapid Appliance Self Recovery(신속한 어플라이언스 자동 복구) 하위 시스템에 사용 가능한 **Rapid Appliance Self Recovery(신속한 어플라이언스 자동 복구)** 링크는 **Backup(백업)** 페이지를 열고, 여기에서 RASR USB 키를 생성하고 Windows 백업 상태를 모니터링하고 Windows 백업 정책을 구성할 수 있습니다. VM Management 링크는 **Virtual Standby(가상 대기)** 페이지를 열고 여기에서 가상 시스템을 관리할 수 있습니다. Storage Hardware(저장소 하드웨어) 하위 시스템에 사용 가능한 **Server Administrator(서버 관리자)** 링크는 컨트롤러, 인클로저, 물리적 드라이브 등의 상태를 분석할 수 있는 시스템의 상태 페이지를 엽니다. Appliance Hardware(어플라이언스 하드웨어)에 사용 가능한 **Controllers(컨트롤러)** 링크는 **Controllers(컨트롤러)** 페이지를 열고 컨트롤러 및 컨트롤러와 연관된 물리적 드라이브의 상세 정보를 제공합니다.

Windows 백업

Windows 백업 기능은 DL 1000을 제외한 모든 DL에서 사용할 수 있습니다. **Appliance(어플라이언스)** > **Backup(백업)** 탭을 사용하면 Windows 백업 정책을 구성하고 마지막 백업과 이전에 백업한 항목의 상태를 표시할 수 있습니다. 이 Windows 백업 기능을 사용하려면 Windows 백업 가상 디스크가 존재해야 합니다.

- 최신 RUU(3.0.x)가 있는 어플라이언스를 업그레이드한 후 Windows 백업 VD(AppAssure 환경에서 생성)가 존재하지 않는 경우 DL Appliance Configuration Wizard(DL 어플라이언스 구성 마법사)를 완료하면 Windows 백업 가상 디스크가 생성됩니다. 이 경우, Windows 백업 VD가 존재하지 않는 경우 **Windows Backup Policy(Windows 백업 정책)** 섹션의 **Backup(백업)** 페이지에서 **+ Create WinBackups VD(+ WinBackups VD 생성)**를 클릭합니다. DL 4000 및 DL 4300에서 295GB 크기의 VD가 생성되고 DL1300에서는 210GB 크기의 VD가 생성됩니다.

- 최신 RUU가 있는 어플라이언스를 업그레이드한 후 AppAssure 환경에서 생성한 Windows 백업 VD가 존재하는 경우 이러한 단계를 수행하여 RR 환경에 Windows 백업 VD 생성하십시오.

  a ApplianceProvisioningConfiguration.xml을 편집합니다(이 파일은 각 볼륨의 루트에 있으므로 한 번 편집한 다음 필요하면 복사할 수 있음).

  △ 주의: **기존 Windows 백업 VD를 삭제하지 마십시오.**

  1 <BackupVolumes> 태그 사이의 모든 텍스트를 삭제합니다.
  2 </BackupVolumes> 태그를 삭제합니다.
  3 <BackupVolumes>이 되도록 <Backupvolume/> 태그를 편집합니다.
  4 저장하고 닫습니다.

  b Core 콘솔로 이동합니다.
  c **Appliance(어플라이언스)** > **RASR** 탭을 클릭합니다.
  d **Create Windows Backup volume(Windows 백업 볼륨 생성)** 버튼을 클릭합니다.
  e 충분한 공간이 있는 경우 Windows 백업 VD가 생성됩니다.

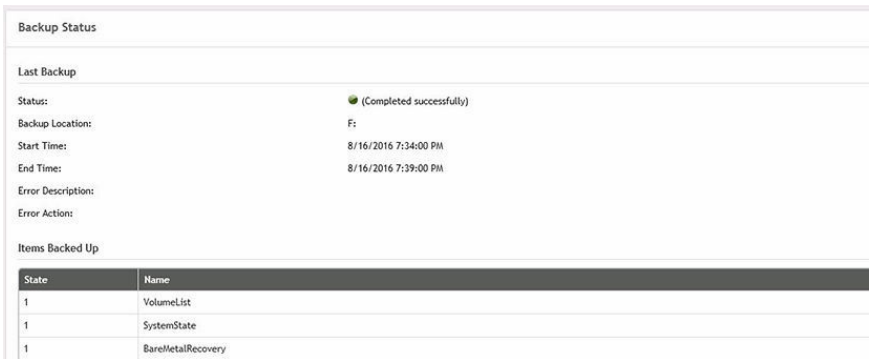
ⓘ 노트: **Windows Server 백업 기능을 사용하여 Windows 백업을 구성하고 어떤 위치에나 백업을 저장할 수도 있지만 이 경우 RASR 페이지에 오류가 표시됩니다. 그 이유는 백업을 제어할 수 없고 RASR을 사용하면 일관성 있게 복원이 수행된다는 보장을 할 수 없기 때문입니다.**

백업 상태

Last Backup(마지막 백업) 탭에서 Microsoft Windows 백업 상태를 확인할 수 있습니다. 현재 백업이 실행 중인 경우에는 **Current Backup(현재 백업)** 탭 아래에 정보가 표시됩니다. 마지막 백업을 보려면 다음 단계를 수행하십시오.

1 Core 콘솔에서**Appliance(어플라이언스)** > **Backup(백업)**탭으로 이동합니다.
2 **Status(상태)** 단추 옆에 있는 화살표를 클릭하여 백업 상태를 봅니다.
3 **Last Backup(마지막 백업)** 창에 다음 정보가 표시됩니다.
   - 상태
   - 상태
   - 백업 위치
   - 시작 시간
   - 종료 시간
   - 오류 설명
   - 백업된 항목

ⓘ 노트: **위의 정보에 Windows 백업 정책 실행 여부가 표시됩니다.**



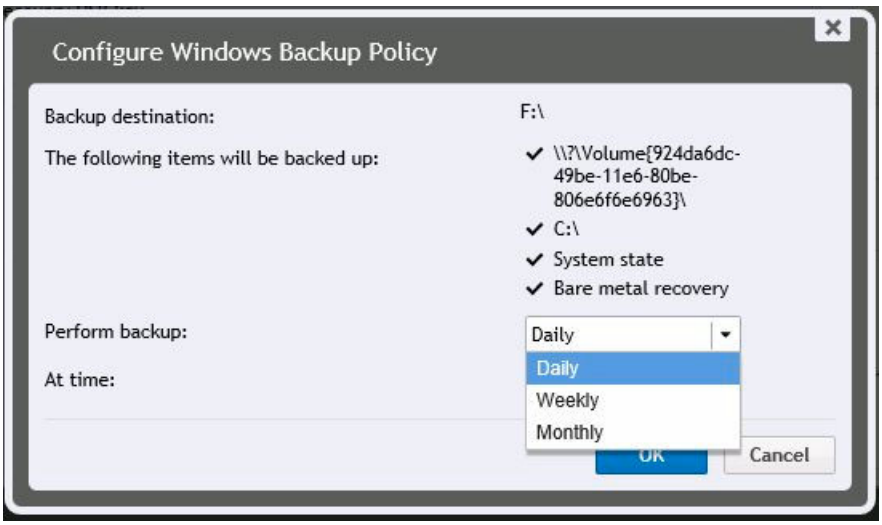
백업이 실행되는 경우 **Current Backup Progress(현재 백업 진행률)** 및 **Start Time(시작 시간)**에 관한 정보가 표시됩니다.

Windows 백업 정책

Windows 백업 정책을 구성하려면 다음 단계를 수행하십시오.

1 Core 콘솔에서**Appliance(어플라이언스) > Backup(백업)**으로 이동합니다.

2 **Configure Policy(정책 구성)** 단추를 클릭합니다.
Windows Backup Policy(Windows 백업 정책) 창이 표시됩니다.

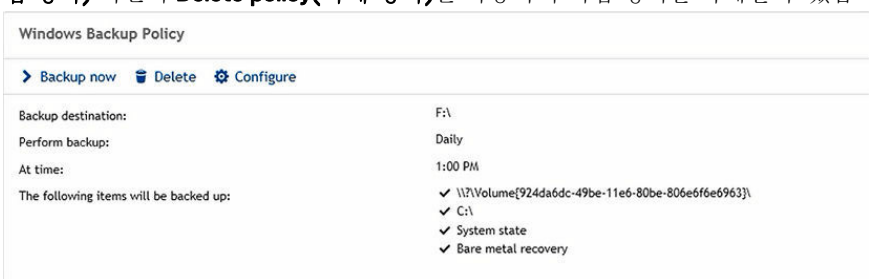


3 아래에 설명된 대로 매개변수를 입력합니다.

텍스트 상자	설명
다음 항목이 백업됩니다.	• OS 볼륨 • 복구 파티션 • 완전 복구 이진 파일 위의 항목은 모두 기본적으로 선택되어 있습니다.
백업 수행	Winbackup이 수행되는 빈도를 선택합니다. 다음과 같은 옵션을 선택할 수 있습니다: 매일, 매주 및 매월.
백업을 예약할 시간을 선택합니다.	백업을 예약할 시간을 입력합니다.

4 **Configure(구성)**를 클릭합니다.
Winbackup 정책이 구성되며 세부 사항이 **Windows 백업 정책** 섹션에 표시됩니다.

구성되면 **Backup now(지금 백업)** 옵션을 사용하여 모든 인스턴스에서 선택한 항목을 백업하고 **Windows Backup Policy(Windows 백업 정책)** 섹션의 **Delete policy(삭제 정책)**를 사용하여 백업 정책을 삭제할 수 있습니다.



저장소 프로비저닝

어플라이언스는 다음에 대해 사용 가능한 내부 스토리지 및 연결된 모든 지원되는 외부 스토리지 인클로저를 구성합니다.

- 리포지토리\
- 대기 VM 또는 기타 용도의 디스크 볼륨

디스크에서 스토리지의 프로비저닝을 시작하기 전에 대기 가상 시스템에 할당할 저장소의 양을 파악해야 합니다. Rapid Recovery 리포지토리를 생성한 뒤 대기 가상 컴퓨터에 사용 가능한 용량의 백분율을 할당할 수 있습니다. 예를 들어, SRM(Storage Resource Management)을 사용하는 경우, Rapid Recovery 리포지토리를 생성한 뒤 가상 컴퓨터를 호스트하기 위해 프로비저닝되는 모든 장치에 최대 100%의 용량을 할당할 수 있습니다. 사용 가능한 공간은 가상 컴퓨터를 호스트하기 위해 프로비저닝된 대기 VM에만 할당될 수 있습니다. Rapid Recovery의 라이브 복구 기능을 사용하면 이러한 가상 컴퓨터를 통해 어플라이언스에서 차단하는 실패한 서버를 모두 신속하게 교체할 수 있습니다.

대기 가상 시스템이 필요하지 않은 중간 규모의 환경에서는, 모든 저장소를 사용하여 상당한 개수의 에이전트를 백업할 수 있습니다. 하지만 대기 가상 시스템에 더 많은 리소스가 필요하고 더 적은 수의 에이전트 시스템을 백업해야 하는 경우에는 규모가 더 큰 VM을 위해 리소스를 추가할 수 있습니다.

Appliance > Provisioning(어플라이언스 프로비저닝) 탭을 선택하면 Rapid Recovery 어플라이언스 소프트웨어는 시스템에서 지원되는 모든 컨트롤러에 사용할 수 있는 저장소 공간을 찾고 하드웨어가 요구사항을 충족하는지 유효성을 검사합니다.

사용 가능한 모든 저장소의 디스크 프로비저닝을 완료하려면 다음을 수행합니다.

1 **Appliance > Provisioning(어플라이언스 프로비저닝)**을 클릭합니다.
Provisioning(프로비저닝) 화면에 **Repositories(리포지토리)** 및 **Storage Volumes(스토리지 볼륨)** 섹션이 표시됩니다.

△ 주의: **계속 진행하기 전에 이 절차의 2단계부터 4단계까지 수행해야 합니다.**

2 생성하는 데 사용할 수 있는 스토리지를 프로비저닝합니다.
   - 리포지토리
   - 대기 VM 또는 기타 용도의 디스크 볼륨

3 리포지토리를 생성하려면 다음을 수행하십시오.
   a **Provisioning(프로비저닝)** 페이지의 **Repositories(리포지토리)** 섹션에서 **Add New Repository(새 리포지토리 추가)**를 클릭합니다.
   Add New Repository(새 리포지토리 추가) 대화 상자가 표시됩니다.
   b 다음 표에 설명된 대로 정보를 입력합니다.

표 56. 저장소 프로비저닝

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 두 번째 리포지토리인 경우 기본 이름은 리포지토리 2입니다. 필요하면 이름을 변경합니다. 리포지토리 이름은 공백을 포함하여 1 - 40개의 영숫자를 포함해야 합니다. 금지되는 문자 또는 금지되는 구문은 사용하지 마십시오. 자세한 내용은 *Dell 데이터 보호 | Rapid Recovery 6.0 사용자 설명서*에서 '금지되는 문자' 또는 '금지되는 구문' 항목을 참조하십시오.
컨트롤러	내부 스토리지 또는 직접 연결된 스토리지 인클로저에 리포지토리를 생성할지 여부에 따라 적절한 스토리지 컨트롤러를 선택합니다.
Enclosure(인클로저)	적절한 스토리지 인클로저를 선택합니다.
RAID 유형	적절한 RAID 레벨을 선택합니다. RAID 구성: 1, 5 또는 6의 경우 다음 옵션이 있습니다.

텍스트 상자	설명
	노트: 시스템은 스토리지가 구성되어 있는 RAID 레벨에만 리포지토리를 생성할 수 있으며 출고되면 사용할 수 있습니다. 원하는 RAID 구성에서 리포지토리를 생성하려면 원하는 RAID 레벨에서 스토리지를 구성해야 합니다. 원하는 RAID 레벨에서 스토리지를 구성하려면 www.dell.com/support/home에서 Dell 어댑터 설명서를 참조하십시오.
예상 용량	리포지토리 생성에 사용 가능한 예상 용량을 표시합니다.
컨트롤러에 사용 가능한 공간	컨트롤러에서 사용 가능한 공간을 표시합니다.
크기	리포지토리의 크기를 입력합니다.

c **Create(생성)**를 클릭합니다.
새 리포지토리가 생성됩니다.

4 대기 VM 또는 기타 용도를 위한 디스크 볼륨을 생성하려면:

a **Storage Volume(스토리지 볼륨)** 섹션에서 **Create Volume(볼륨 생성)**을 클릭합니다.

b **Create Volume(볼륨 생성)** 대화 상자에서 새 디스크 볼륨에 대해 다음과 같은 볼륨 이름, 컨트롤러, 인클로저, RAID 유형 및 크기 등의 정보를 지정합니다.
컨트롤러에 사용 가능한 공간은 기본적으로 표시됩니다. 다음과 같은 RAID 구성: 1, 5 또는 6 중 하나를 선택할 수 있습니다.

c **Create(생성)**를 클릭합니다.
새 스토리지 볼륨이 생성됩니다.

가상 디스크의 공간 할당 삭제

이 경우 프로비저닝 구성을 변경해야 하는 경우 기술 지원에 문의하십시오. 자세한 내용은 **Dell에 문의하기** 섹션을 참조하십시오.

복구 및 업데이트 유틸리티

복구 및 업데이트 유틸리티(RUU)는 DL 어플라이언스(DL1000, DL1300, DL4000 및 DL4300)를 복구 및 업데이트하기 위한 올인원 설치 프로그램입니다. 여기에는 Rapid Recovery Core 소프트웨어 및 어플라이언스별 구성 요소가 포함되어 있습니다.

RUU는 Windows Server 역할 및 기능, .Net 4.5.2, LSI Provider, DL 응용프로그램, OpenManage Server Administrator 및 Rapid Recovery Core 소프트웨어의 업데이트된 버전으로 구성되어 있습니다. 추가적으로, 복구 및 업데이트 유틸리티는 Rapid Appliance Self Recovery(RASR) 컨텐츠도 업데이트합니다.

노트: 현재 AppAssure Core의 모든 버전, Rapid Recovery Core 6.0.2.144 이전 버전을 사용하는 경우 RUU는 페이로드에서 사용할 수 있는 최신 버전으로 강제 업데이트합니다. 업데이트를 건너뛸 수 없으며 이 업데이트는 되돌릴 수 없습니다. Core 소프트웨어를 업그레이드하고 싶지 않은 경우 RUU를 실행하지 마십시오.

어플라이언스 업그레이드

어플라이언스를 업그레이드하려면 다음을 수행하십시오.

1 Downloads(다운로드) 섹션 아래에서 라이센스 포털로 이동하거나 **support.dell.com**으로 이동하고 RUU 설치 프로그램을 다운로드합니다.

2 유틸리티를 응용프로그램 바탕화면에 복사하고 파일의 압축을 풉니다.

3 **launchRUU** 아이콘을 두 번 클릭합니다.

4 메시지가 표시되면 **Yes(예)**를 클릭하여 나열된 프로세스를 실행하지 않음을 확인합니다.

5 **Recovery and Update Utility(복구 및 업데이트 유틸리티)** 화면이 나타나면 **Start(시작)**를 클릭합니다.

6 다시 부팅 메시지가 표시되면 **OK(확인)**를 클릭합니다.
Windows Server Roles and Features, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator 및 Rapid Recovery Core 소프트웨어의 업데이트 버전이 복구 및 업데이트 유틸리티의 일부로 설치됩니다. 또한 복구 및 업데이트 유틸리티를 통해 RASR 내용도 업데이트됩니다.

노트: 현재 Rapid Recovery Core 버전 6.0.2.144 이전 버전인 AppAssure Core의 모든 버전을 사용하는 경우 RUU는 페이로드에서 사용할 수 있는 최신 버전으로 강제 업데이트합니다. 업데이트를 건너뛸 수 없으며 이 업데이트는 되돌릴 수 없습니다. Core 소프트웨어를 업그레이드하지 않으려면 RUU를 실행하지 마십시오.

7 메시지가 표시되면 시스템을 다시 부팅합니다.

8 모든 서비스와 응용프로그램이 설치되면 **Proceed(계속)**를 클릭합니다.

Core 콘솔이 실행됩니다.

어플라이언스 복구

어플라이언스를 복구하려면 다음을 수행하십시오.

1 Downloads(다운로드) 섹션 아래에서 라이센스 포털로 이동하거나 **support.dell.com**으로 이동하고 RUU 설치 프로그램을 다운로드합니다.

2 유틸리티를 응용프로그램 바탕화면에 복사하고 파일의 압축을 풉니다.

3 **launchRUU** 아이콘을 두 번 클릭합니다.

4 메시지가 표시되면 **Yes(예)**를 클릭하여 나열된 프로세스를 실행하지 않음을 확인합니다.

5 Recovery and Update Utility(복구 및 업데이트 유틸리티) 화면이 표시되면 **Start(시작)**를 클릭합니다.

6 다시 부팅 메시지가 표시되면 **OK(확인)**를 클릭합니다.

Windows Server Roles 및 Features, .Net 4.5.2, LSI Provider, DL Applications, OpenManage Server Administrator 및 Rapid Recovery Core 소프트웨어의 업데이트 버전이 복구 및 업데이트 유틸리티의 일부로 설치됩니다.

7 유틸리티에 번들된 버전이 설치된 버전과 동일하면, 복구 및 업데이트 유틸리티가 복구 설치를 실행할지 묻는 메시지를 표시합니다. Rapid Recovery Core의 복구 설치가 필요하지 않을 경우에는 이 단계를 생략해도 됩니다.

8 유틸리티에 번들된 버전이 설치된 버전보다 높으면, 복구 및 업데이트 유틸리티가 Rapid RecoveryCore 소프트웨어를 업그레이드하라는 메시지를 표시합니다.

노트: Rapid Recovery Core 소프트웨어 다운그레이드는 지원되지 않습니다.

9 메시지가 표시되면 시스템을 다시 부팅합니다.

10 모든 서비스와 응용프로그램이 설치되면 **Proceed(계속)**를 클릭합니다.

복구 후 시스템을 다시 구성해야 하는 경우 DLAppliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)가 실행되고, 그렇지 않으면 Core 콘솔이 실행됩니다.

4

워크스테이션 및 서버 보호

시스템 보호

이 장에서는 Rapid Recovery 환경에서 보호된 시스템을 보호하고, 구성 및 관리하는 방법을 설명합니다.

Rapid Recovery로 시스템을 보호하는 방법

Rapid Recovery를 사용하여 데이터를 보호하려면 Rapid Recovery Core Console에서 보호할 워크스테이션과 서버를 추가해야 합니다(예: Exchange Server, SQL Server, Linux 서버 등).

Core에서 보호하려는 모든 물리적 시스템 또는 가상 시스템에 Rapid Recovery Agent 소프트웨어를 추가해야 합니다.

노트: 이 규칙의 예외로, VMware 또는 ESXi 호스트에서 물리적 시스템을 보호하려는 경우에는 에이전트 없는 보호를 사용할 수 있습니다. 에이전트 없는 보호의 제한 사항을 포함하여 자세한 내용은 Rapid Snap for Virtual 이해을(를) 참조하십시오.

Rapid Recovery Core Console에서 Protect Machine(시스템 보호) 마법사 중 하나를 사용하여 사용자가 보호하려는 시스템을 식별할 수 있습니다. 다음 작업을 수행할 수 있습니다.

- 네트워크 호스트 이름 또는 IP 주소를 사용하여 시스템에 연결하는 단일 시스템은 Protect Machine(시스템 보호) 마법사를 사용하여 보호할 수 있습니다. 단일 시스템을 보호하는 방법에 대한 자세한 내용은 시스템 보호을(를) 참조하십시오.
- 네트워크 호스트 이름 또는 IP 주소를 사용하여 클러스터와 해당 노드에 연결하는 네트워크 클러스터는 Protect Cluster(클러스터 보호) 기능을 사용하여 보호할 수 있습니다.
- Microsoft Active Directory®를 사용하여 시스템에 연결하거나 vCenter 또는 ESXi 호스트에 연결하는 여러 시스템은 Protect Multiple Machines(여러 시스템 보호) 마법사를 사용하여 동시에 보호할 수 있습니다.

노트: Dell에서는 보호 작업이 실패하는 원인이 될 수도 있는 리소스 제약이 발생하지 않도록 동시에 보호하는 시스템 수를 50대 이하로 제한할 것을 권장합니다.

단일 시스템의 보호 요구 사항을 마법사에서 식별하면 보호할 볼륨을 지정할 수 있습니다. 다중 시스템을 보호하면 기본적으로 모든 볼륨이 보호됩니다. 나중에 이를 개별 시스템 기준으로 변경할 수 있습니다.

마법사를 통해 보호에 대한 사용자 지정 일정을 정의하거나 기존 일정을 재사용할 수 있습니다.

고급 옵션을 사용하면 보호하려는 시스템의 백업에 암호화 키를 지정 또는 적용하여 추가 보안 조치를 추가할 수 있습니다.

마지막으로, 리포지토리가 하나도 없으면 마법사를 사용하여 리포지토리를 정의할 수 있습니다.

Agent 소프트웨어 설치가 끝나면 설치 후 각 시스템을 다시 시작해야 합니다.

워크스테이션과 서버를 보호하는 방법에 대한 자세한 내용은 시스템 보호을(를) 참조하십시오.

주의: Rapid Recovery에서는 ext2 부트 파티션이 있는 Linux 시스템의 Bare Metal Restore(BMR)가 지원되지 않습니다. 이 유형의 파티션이 있는 시스템에서 BMR를 수행할 경우 시스템이 시작되지 않습니다. ext2 부트 파티션이 있는 Linux 시스템에서 BMR를 수행할 수 있으려면 시스템 보호 및 백업을 시작하기 전에 모든 ext2 부트 파티션을 ext3 또는 ext4로 변환해야 합니다.

Rapid Recovery를 사용한 Linux 시스템 보호 정보

Rapid Recovery Agent 소프트웨어는 여러 Linux 기반 운영 체제(자세한 내용은 *Rapid Recovery 설치 및 업그레이드 안내서* 또는 *Rapid Recovery 릴리스 노트*에 포함되어 있는 시스템 요구 사항 참조)와 호환됩니다. Rapid Recovery Core는 Windows 시스템과만 호환됩니다. Rapid Recovery Core Console에서 보호된 Linux 시스템을 관리할 수 있지만 Linux 시스템과 관련된 여러 절차에는 Windows 시스템과 다른 단계가 있습니다. 또한 local_mount 명령줄 유틸리티를 사용하여 보호된 Linux 시스템에서 직접 일부 작업을 수행할 수 있습니다.

노트: local_mount 유틸리티의 이전 명칭은 aamount입니다.

Rapid Recovery Core에서 Exchange 및 SQL Server 관리 정보

소프트웨어 및 관련 파일의 인스턴스가 보호 대상 서버에서 탐지될 때에만 Exchange Server 및 SQL Server에 대한 특정 옵션이 Rapid Recovery Core Console에 나타납니다. 이러한 경우 Core Console에서 보호된 시스템을 선택하면 추가 옵션을 사용할 수 있습니다.

예를 들어, 왼쪽 탐색 메뉴에서 보호 대상 Exchange Server를 선택하면 보호된 시스템에서 나타나는 메뉴 옵션에는 **Exchange** 드롭다운 메뉴 옵션이 있습니다.

왼쪽 탐색 메뉴에서 보호 대상 SQL Server를 선택하면 보호된 시스템에서 나타나는 메뉴 옵션에는 **SQL** 드롭다운 메뉴가 있습니다.

이 옵션은 다르게 작동할 수도 있지만 몇 가지 공통점이 있습니다. 다음은 다른 보호된 시스템이 아니라, 보호 대상 Exchange 및 SQL Server에서만 수행할 수 있는 기능입니다.

- **로그 잘라내기 수행.** SQL Server와 Exchange Server는 모두 서버 로그를 포함합니다. SQL 로그를 잘라내기 위한 프로세스는 서버에서 사용할 수 있는 공간을 식별합니다. Exchange Server 서버의 로그를 잘라낼 때 프로세스는 사용 가능한 공간을 식별하고 서버에 더 많은 공간을 확보합니다.
- **관련 서버에 대한 자격 증명 설정.** Exchange Server를 사용할 경우 보호 대상 서버에 대한 요약 페이지에서 보호된 시스템에 대한 자격 증명을 설정할 수 있습니다. SQL Server를 사용할 경우 단일 보호 대상 SQL Server 시스템에 대한 자격 증명을 설정하거나, 모든 보호 대상 SQL Server에 대한 기본 자격 증명을 설정할 수 있습니다.
- **Exchange 서버 또는 SQL Server의 복구 지점에서 검사 상태 보기**. 보호된 SQL 또는 Exchange Server는 해당하는 색상 상태 표시기를 표시합니다. 이러한 색상은 SQL Server 또는 Exchange Server와 관련된 여러 검사의 성공/실패 여부를 나타냅니다.

이 절에서는 Exchange Server 또는 SQL Server를 사용하는 보호 대상 시스템 관리와 관련된 다음 항목을 다룹니다.

- 복구 지점 상태 표시기 이해
- 보호된 Exchange 서버의 설정 및 기능
- 보호되는 SQL Server의 설정 및 기능

서버 클러스터 보호 정보

Rapid Recovery에서 서버 클러스터 보호는 개별 클러스터 노드(클러스터에 있는 개별 시스템)에 설치된 Rapid Recovery 보호된 시스템과 이러한 시스템을 모두 하나의 복합 시스템처럼 보호하는 Rapid Recovery Core와 연결됩니다.

Rapid Recovery Core가 쉽게 클러스터를 보호하고 관리하도록 구성할 수 있습니다. Core Console에서 클러스터는 개별 엔터티로 구성되어 관련 노드를 포함하는 컨테이너 역할을 수행합니다. 예를 들어, 왼쪽 탐색 영역의 **보호된 시스템** 메뉴 아래에 보호된 클러스터가 나열됩니다. 각 클러스터 바로 아래에 연결된 개별 노드 또는 에이전트 시스템이 나타납니다. 각 시스템은 Rapid Recovery Agent 소프트웨어가 설치된 보호된 시스템입니다. 클러스터를 클릭할 경우 Core Console에 클러스터에 대한 **요약** 페이지가 나타납니다.

Core 및 클러스터 수준에서 관련된 노드 및 공유 볼륨 목록과 같은 클러스터에 대한 정보를 볼 수 있습니다. Core Console에 클러스터 정보를 표시할 때 맨 위 탐색 메뉴에서 **보호된 노드**를 클릭하여 클러스터에 있는 개별 노드의 요약 표를 볼 수 있습니다. 이 요약 표를 통해 각 노드에 대해 강제로 스냅숏 생성, 1회 내보내기 수행 또는 가상 대기 설정, 복구 지점 조회 또는 마운트, 복구 지점에서 복원, 클러스터 노드를 고유한 보호된 시스템으로 변환, 보호에서 노드 제거와 같은 기능을 수행할 수 있습니다. 노드가 Exchange 또는 SQL Server인 경우 로그를 자르는 옵션도 제공됩니다.

또한 클러스터 수준에서 클러스터의 노드에 대한 해당 Exchange 및 SQL 클러스터 메타데이터도 볼 수 있습니다. 전체 클러스터 및 해당 클러스터에 있는 공유 볼륨에 대한 설정을 지정할 수 있습니다.

왼쪽 탐색 메뉴에서 클러스터에 있는 노드를 클릭하면 Core Console에 표시되는 정보는 클러스터의 해당 노드에 특정한 정보입니다. 여기에서 해당 노드에 특정한 정보를 보거나 해당 노드에 대한 설정만 구성할 수 있습니다.

클러스터 공유 볼륨에 대한 지원

Rapid Recovery 릴리스 6.x에서 클러스터 공유 볼륨(CSV)에 대한 지원은 Windows Server 2008 R2을 실행하는 CSV의 기본 백업으로 제한됩니다. 또한 복구 지점에서 Windows Server 2008 R2를 실행하는 CSV 볼륨을 복원하거나 Windows Server 2008 R2를 실행하는 Hyper-V CSV로 가상 내보내기를 수행할 수도 있습니다. 클러스터 공유 볼륨의 가상 내보내기는 수행할 수 없습니다. Rapid Recovery 릴리스 6.0.1 이상의 새로운 기능은 Windows Server 2012 또는 Windows Server 2012 R2를 실행하는 Hyper-V CSV로 가상 내보내기를 수행하는 기능입니다.

노트: Hyper-V 에이전트 없는 기능은 Windows Server 2012 R2 이상에서만 호환됩니다.

다른 운영 체제의 경우 Rapid Recovery 에이전트 서비스는 클러스터의 모든 노드에서 실행할 수 있으며 클러스터는 Rapid Recovery Core 내의 클러스터로 보호될 수 있습니다. 그러나 CSV는 Core 콘솔에 표시되지 않으며 보호할 수 있습니다. 모든 로컬 디스크(예: 운영 체제 볼륨)는 보호할 수 있습니다.

다음 표에서는 클러스터 공유 볼륨에 대한 Rapid Recovery Core의 최신 지원을 설명합니다.

표 57. 클러스터 공유 볼륨에 대한 Rapid Recovery 지원

Rapid Recovery 클러스터 공유 볼륨 지원	보호, 복제, 롤업, 마운트, 보관	CSV 볼륨 복원	Hyper-V CSV에 가상 내보내기
Rapid Recovery	6.0	6.0	6.0.x
Windows Server 2008 R2	Yes	Yes	Yes
Windows Server 2012	아니오	아니오	Yes
Windows Server 2012 R2	아니오	아니오	Yes

[1] Windows Server 2012 R2 이상에서만 호환되는Hyper-V 에이전트 없는 기능은 제외됩니다.

Rapid Recovery를 사용하면 클러스터 공유 볼륨의 일부 다른 운영 체제를 보호할 수 있습니다. 이때 사용자가 위험을 감수해야 합니다. 위 표의 구성만 Dell에서 지원합니다.

동적 및 기본 볼륨에 대한 지원

Rapid Recovery에서는 모든 동적 및 기본 볼륨의 스냅숏 만들기가 지원됩니다. 또한, Rapid Recovery에서는 단일 실제 디스크에 있는 단순 동적 볼륨 내보내기도 지원됩니다. 이름에서 알 수 있듯이 단순 동적 볼륨은 스트라이프, 미러, 스팬 또는 RAID 볼륨이 아닙니다.

동적 디스크 가상 내보내기의 동작은 내보내려는 볼륨이 Rapid Recovery Agent 소프트웨어로 보호되는지, 아니면 에이전트 없는 보호를 사용하는 VM인지에 따라 달라집니다. 이는 비단순 즉 복합 동적 볼륨에는 Rapid Recovery Agent에서 완전히 해석할 수 없는 임의의 디스크 지오메트리가 있기 때문입니다.

Rapid Recovery Agent 소프트웨어로 시스템에서 복합 동적 디스크를 내보내려고 시도하면 엑스포트가 단순 동적 볼륨으로 한정 및 제한된다고 경고하는 알림이 사용자 인터페이스에 표시됩니다. 단순 동적 볼륨이 아니면 Rapid Recovery Agent로 내보내기를 시도하는 경우 내보내기 작업이 모두 실패합니다.

반면, 에이전트 없이 보호하는 VM의 동적 볼륨에 대해서는 보호, 가상 내보내기, 데이터 복원 및 BMR가 지원됩니다. 리포지토리 저장소도 지원되지만 몇 가지 중요한 제한 사항이 있습니다. 예:

- **보호:** 동적 볼륨이 여러 디스크에 걸쳐 있는 경우 볼륨의 무결성을 유지하려면 해당 디스크를 다 함께 보호해야 합니다.

- **가상 내보내기:** 에이전트 없는 보호를 사용하여 스트라이프, 미러, 스팬 또는 RAID 볼륨과 같은 복합 동적 볼륨을 ESXi 호스트에서 내보낼 수 있습니다.

  그러나, 볼륨 구문 분석 없이 디스크 수준에서 볼륨이 내보내집니다. 예를 들어, 2개의 디스크에 걸쳐 있는 동적 볼륨을 내보내는 경우 2개의 별개 디스크 볼륨이 내보내기에 포함됩니다.

  주의: 여러 디스크에 걸친 동적 볼륨을 내보내려면 원래 시스템 볼륨이 있는 동적 디스크를 내보내 디스크 유형을 보존해야 합니다.
- **데이터 복원**: 여러 디스크에 걸친 동적 볼륨을 복원할 때는 원래 시스템 볼륨이 있는 동적 디스크를 복원하여 디스크 유형을 보존해야 합니다. 하나의 디스크만 복원하면 디스크 구성이 손상됩니다.

리포지토리 저장소: 또한, Rapid Recovery에서는 복합 동적 볼륨(스트라이프, 미러, 스팬 또는 RAID)에 대한 리포지토리 생성이 지원됩니다. 리포지토리를 호스팅하는 시스템의 파일 시스템은 NTFS 또는 ReFS여야 합니다.

Rapid Recovery Agent 소프트웨어 설치 프로그램 이해

Rapid Recovery를 통해 Rapid Recovery Core에서 설치 프로그램을 다운로드할 수 있습니다. **다운로드** 페이지에서 Agent Installer, LMU(Local Mount Utility) 또는 SNMP MIB 파일을 다운로드하도록 선택할 수 있습니다. LMU에 대한 자세한 내용은 Local Mount Utility을(를) 참조하십시오. SNMP에 대한 자세한 내용은 SNMP 설정 이해을(를) 참조하십시오.

노트: Agent Installer에 액세스하는 방법은 Rapid Recovery Agent Installer 다운로드을(를) 참조하십시오. Agent Installer를 배포하는 방법에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery 설치 및 업그레이드 안내서를 참조하십시오.

Agent Installer는 Rapid Recovery Core에서 보호하려는 시스템에 Rapid Recovery Agent 응용 프로그램을 설치하는 데 사용됩니다. 시스템에 Agent Installer를 설치하기 위해 Rapid Recovery Core Console의 다운로드 페이지에서 Web Installer를 다운로드하십시오.

노트: Core 다운로드는 Dell Data Protection | Rapid Recovery License Portal에서 수행됩니다. Rapid Recovery Core 설치 프로그램을 다운로드하려면 https://licenseportal.com을 방문하십시오. 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 사용 설명서*를 참조하십시오.

Rapid Recovery Agent Installer 다운로드

Rapid Recovery Agent Installer를 다운로드하여 Rapid Recovery Core에서 보호하려는 시스템에 배포합니다. Web Installer를 다운로드하려면 다음 단계를 완료하십시오.

1 보호하려는 시스템에서 직접 Agent Web Installer를 다운로드하려면 다음 단계를 수행하십시오.
   a 웹 브라우저에서 https://licenseportal.com의 Dell Data Protection | Rapid Recovery License Portal을 엽니다.
   b 왼쪽 탐색 메뉴에서 **다운로드**를 클릭합니다.
   c **Windows 기반 응용 프로그램** 창에서 **Windows Agent** 행까지 아래로 스크롤하여 해당 설치 프로그램(32비트 또는 64비트 시스템)에 대한 **다운로드**를 클릭합니다.

   설치 프로그램 파일(예: `Agent-X64-6.0.1.xxxx.exe`)이 다운로드 대상 폴더에 저장됩니다.

2 Core에서 웹 설치 프로그램을 다운로드하려면 Core Console 아이콘 표시줄에서 **자세히** 아이콘을 클릭한 다음 **다운로드**를 선택합니다.
3 **다운로드** 페이지의 **Agent** 창에서 **웹 설치 프로그램 다운로드**를 클릭합니다.
4 **Agent-Web.exe 열기** 대화 상자에서 **파일 저장**을 클릭합니다.

   설치 프로그램 파일(예: `Agent-X64-6.0.1.xxxx.exe`)이 다운로드 대상 폴더에 저장됩니다.
5 이 설치 프로그램을 해당 시스템으로 이동하고 Rapid Recovery Agent 소프트웨어를 설치합니다.

   Rapid Recovery Agent 소프트웨어 설치에 대한 자세한 내용은 Rapid Recovery *설치 및 업그레이드 안내서*를 참조하십시오.

Core 콘솔에서 에이전트를 다중 시스템에 동시에 배포

Rapid Recovery 에이전트 소프트웨어를 여러 Windows 시스템에 동시에 배포할 수 있습니다. 시스템은 Active Directory 도메인 또는 vCenter나 ESX(i) 가상 호스트의 일부가 될 수 있거나 Rapid Recovery 에이전트 업그레이드 경우처럼 로컬 Rapid Recovery Core에 의

해 보호되는 시스템일 수 있습니다. 또한 특정 도메인 또는 호스트와 연관이 없는 시스템에 소프트웨어를 수동으로 배포하는 옵션도 있습니다.

Rapid Recovery 에이전트 소프트웨어를 Core 콘솔에서 하나 이상의 Linux 시스템에 수동으로 배포할 수도 있습니다.

△ 주의: **AppAssure 에이전트가 이전에 Linux 시스템에 설치된 경우 다음 Rapid Recovery 에이전트를 설치하기 전에 쉘 스크립트를 사용하여 시스템에서 AppAssure 에이전트를 제거합니다. Linux 시스템에서 에이전트를 제거하는 방법에 대한 자세한 내용은 Linux 시스템에서 AppAssure 에이전트 소프트웨어 제거 항목을 참조하십시오. Linux 시스템에 에이전트 소프트웨어를 성공적으로 배포하려면 Linux 시스템에 에이전트 소프트웨어 설치 정보 항목의 필수 조건을 참조하십시오. 이러한 주제는 *Dell Data Protection | Rapid Recovery 설치 및 업그레이드 설명서*에서 볼 수 있습니다.**

Rapid Recovery 에이전트 소프트웨어를 배포해도 시스템이 자동으로 보호되지 않습니다. 배포 후에 Core의 콘솔의 버튼 모음에서 **Protect Multiple Machines(여러 시스템 보호)** 옵션을 선택해야 합니다.

ⓘ **노트: 여러 시스템에 동시에 배포하는 기능을 이전에는 "일괄 배포"라고도 했습니다. 여러 시스템을 동시에 보호하는 기능을 이전에는 "일괄 보호"라고도 했습니다.**

여러 시스템을 동시에 배포하고 보호하려면 다음 작업을 수행하십시오.

- 여러 시스템에 Rapid Recovery 에이전트 배포합니다(하나 이상의 시스템에 Rapid Recovery Agent 소프트웨어 배포 참조).
- 배포를 모니터합니다(다중 시스템에 배포 확인 참조).
- 다중 시스템을 보호합니다(다중 시스템 보호 정보 참조).

ⓘ **노트: Protect Machine After Install(설치 후 시스템 보호) 옵션을 선택한 경우 배포하는 동안 이 작업을 건너뛰십시오.**

- 일괄 보호 활동을 모니터합니다(다중 시스템의 보호 모니터링 참조).

하나 이상의 시스템에 Rapid Recovery Agent 소프트웨어 배포

Agent 소프트웨어 배포 마법사를 사용하여 하나 이상의 Windows 시스템에 Rapid Recovery Agent 소프트웨어를 간편하게 배포할 수 있습니다.

ⓘ **노트: 이전에 이 기능을 "일괄 배포"라고 했습니다.**

Agent 소프트웨어 배포 마법사를 사용하면 호스트에 있는 시스템을 Rapid Recovery에서 자동으로 감지하여 배포할 시스템을 선택할 수 있도록 합니다. Active Directory나 vCenter/ESX(i)가 아닌 도메인 또는 호스트에 있는 시스템은 IP 주소와 해당 자격 증명을 사용하여 개별 시스템에 수동으로 연결할 수 있습니다. 또한 로컬 Rapid Recovery Core에서 이미 보호하고 있는 시스템에 이 소프트웨어의 업그레이드를 배포할 수 있습니다.

Core Console 내에서 완료할 수 있는 작업은 다음과 같습니다.

- Active Directory 도메인의 시스템에 배포
- VMware vCenter/ESX(i) 가상 호스트의 시스템에 배포
- 보호된 시스템에 Rapid Recovery Agent 소프트웨어 업그레이드 배포
- 시스템에 수동으로 배포

ⓘ **노트: Dell은 리소스 제약 조건으로 인해 배포 작업에 실패하는 일이 없도록 동시에 배포할 수 있는 시스템 수를 최대 50대로 제한하도록 권장합니다.**

ⓘ **노트: 대상 시스템에서 BITS를 다운로드 및 설치하려면 인터넷 액세스가 필요합니다. Rapid Recovery에서는 Rapid Recovery Agent Installer의 웹 버전을 사용하여 설치 구성 요소를 배포하기 때문입니다. 인터넷 액세스를 사용할 수 없는 경우에는 Core Console을 사용하여 USB 드라이브와 같은 매체에 설치 프로그램을 다운로드한 후 보호하려는 시스템에 이 소프트웨어를 물리적으로 설치하면 됩니다. 자세한 내용은 Rapid Recovery Agent Installer 다운로드을(를) 참조하십시오.**

Active Directory 도메인의 시스템에 배포

이 절차를 사용하여 Rapid Recovery Agent 소프트웨어를 Active Directory 도메인에 있는 하나 이상의 시스템에 동시에 배포합니다.

이 절차를 시작하기 전에 Active Directory 서버의 도메인 정보와 로그온 자격 증명이 있어야 합니다.

1 Rapid Recovery Core Console에서 **보호** 드롭다운 메뉴를 클릭하고 **Agent 소프트웨어 배포**를 클릭합니다.
Deploy Agent Software Wizard(에이전트 소프트웨어 배포 마법사)가 열립니다.
2 마법사의 **연결** 페이지 중 **소스** 드롭다운 목록에서 **Active Directory**를 선택합니다.
3 다음 표에서 설명한 대로, 도메인 정보와 로그온 자격 증명을 입력합니다.

표 58. 도메인 정보 및 자격 증명

텍스트 상자	설명
호스트	Active Directory 도메인의 호스트 이름 또는 IP 주소.
사용자 이름	도메인에 연결하는 데 사용되는 사용자 이름(예: Administrator 또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator).
암호	도메인에 연결하는 데 사용되는 보안 암호.

4 **다음**을 클릭합니다.
5 **시스템** 페이지에서 Rapid Recovery Agent 소프트웨어를 배포할 시스템을 선택합니다.
6 필요한 경우 Agent 설치 후 보호된 시스템을 자동으로 다시 시작하려면 **Agent 설치 후 시스템 자동으로 다시 시작(권장)**을 선택합니다.
7 **마침**을 클릭합니다.
그러면 시스템은 선택한 각 시스템을 자동으로 확인합니다.
Rapid Recovery에서 자동 확인 중 문제점을 감지하면 마법사는 Warnings(경고) 페이지로 이동합니다. 이 페이지에서는 선택 내용에서 시스템을 지우고 선택한 시스템을 수동으로 확인할 수 있습니다. 추가한 시스템이 자동 확인에 통과하면 Deploy Agent to Machines(시스템에 Agent 배포) 창에 시스템이 나타납니다.
8 경고 페이지가 나타났지만 선택한 내용에 만족하면 **마침**을 다시 클릭합니다.

Rapid Recovery Agent 소프트웨어는 지정된 시스템에 배포됩니다. 시스템은 아직 보호 상태가 아닙니다. 보호는 Active Directory 도메인에서 다중 시스템 보호를 완료한 후에 시작됩니다.

VMware vCenter/ESX(i) 가상 호스트의 시스템에 배포

이 절차를 사용하여 VMware vCenter/ESX(i) 가상 호스트에 있는 하나 이상의 시스템에 Rapid Recovery Agent 소프트웨어를 동시에 배포합니다.
이 절차를 시작하려면 다음 정보가 있어야 합니다.

- VMware vCenter/ESX(i) 가상 호스트에 대한 로그온 자격 증명.
- 호스트 위치.
- 보호하려는 각 시스템에 대한 로그온 자격 증명.

노트: 모든 가상 시스템에는 VMware 도구가 설치되어 있어야 합니다. 그렇지 않으면 배포할 가상 시스템의 호스트 이름을 Rapid Recovery에서 검색하지 못합니다. Rapid Recovery에서는 호스트 이름 대신 가상 시스템 이름을 사용하므로 호스트 이름이 가상 시스템 이름과 다르면 문제가 발생할 수도 있습니다.

1 Rapid Recovery Core Console에서 드롭다운 메뉴 **보호**를 클릭한 다음 **Agent 소프트웨어 배포**를 클릭합니다.
Agent 소프트웨어 배포 마법사가 열립니다.
2 마법사의 **연결** 페이지에서, 드롭다운 목록 **원본** 중에서 **vCenter / ESX(i)**를 선택합니다.
3 다음 표에 설명된 대로 호스트 정보와 로그온 자격 증명을 입력합니다.

표 59. vCenter/ESX(i) 연결 설정

텍스트 상자	설명
호스트	VMware vCenter Server/ESX(i) 가상 호스트의 이름 또는 IP 주소.
포트	가상 호스트에 연결하는 데 사용되는 포트. 기본 설정은 443입니다.
사용자 이름	가상 호스트에 연결하는 데 사용되는 사용자 이름(예: 관리자 또는 시스템이 도메인에 있는 경우 [도메인 이름]\관리자).
암호	이 가상 호스트에 연결하는 데 사용되는 보안 암호.

4 **다음**을 클릭합니다.

5 마법사의 **시스템** 페이지에서, 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 호스트 및 클러스터
- VM 및 템플릿

6 시스템의 목록을 확장한 다음 소프트웨어를 배포하려는 VM을 선택합니다.

오프라인 상태인 시스템 또는 설치되지 않은 VMware 도구가 Rapid Recovery에서 검색되면 알림이 표시됩니다.

7 배포 후 시스템을 자동으로 다시 시작하려면 **Agent 설치 후 시스템을 자동으로 다시 시작(권장 사항)**을 선택합니다.

8 **다음**을 클릭합니다.

선택한 각 시스템이 Rapid Recovery에서 자동으로 확인됩니다.

9 마법사의 **조정** 페이지에서, 각 시스템에 대한 자격 증명을 `hostname::username::password` 형식으로 입력합니다.

노트: 줄마다 시스템을 하나씩 입력합니다.

10 **마침**을 클릭합니다.

선택한 각 시스템이 시스템에서 자동으로 확인됩니다.

Rapid Recovery에서 자동 확인 진행 중 문제가 하나라도 검색되면 마법사가 시스템을 선택 취소하고 선택한 시스템을 수동으로 확인할 수 있는 경고 페이지로 넘어갑니다. 추가한 시스템이 자동 확인을 통과하면 시스템에 Agent 배포 창이 표시됩니다.

11 경고 페이지가 표시되어도 선택 내용에 만족하면 **마침**을 다시 클릭합니다.

Rapid Recovery Agent 소프트웨어가 지정된 시스템에 배포됩니다. 아직은 시스템이 보호되지 않습니다. VMware vCenter/ESX(i) 가상 호스트에서 여러 시스템 보호을(를) 완료해야 보호가 시작됩니다.

보호된 시스템에 Rapid Recovery Agent 소프트웨어 업그레이드 배포

Deploy Agent Software Wizard(Agent 소프트웨어 배포 마법사)를 사용하여 이미 로컬 Rapid Recovery Core의 보호를 받는 시스템에 Rapid Recovery Agent 소프트웨어 업그레이드를 배포할 수 있습니다.

1 Rapid Recovery Core Console에서 **보호** 드롭다운 메뉴를 클릭한 다음 **Agent 소프트웨어 배포**를 클릭합니다

Agent 소프트웨어 배포 마법사가 열립니다.

2 마법사의 **연결** 페이지에서 **소스** 드롭다운 목록의 **로컬 Core**를 선택합니다.

3 **다음**을 클릭합니다.

4 마법사의 **시스템** 페이지에서 Rapid Recovery Agent 소프트웨어 업그레이드를 배포하려는 보호된 시스템을 선택합니다.

5 **마침**을 클릭합니다.

선택한 각 시스템을 시스템에서 자동으로 확인합니다.

자동 확인하는 동안 Rapid Recovery에서 우려 사항을 감지하는 경우, 마법사는 **경고** 페이지를 실행합니다. 이 페이지에서 선택 항목의 시스템을 지우고 해당 시스템을 수동으로 확인할 수 있습니다. 추가한 시스템이 자동 확인을 통과하면 **시스템에 Agent 배포** 창에 이 시스템이 나타납니다.

6 **경고** 페이지가 나타나도 선택 사항에 만족하면 **마침**을 다시 클릭합니다.

시스템에 수동으로 배포

Rapid Recovery Agent를 로컬 Core, Active Directory, vCenter/ESXi가 아닌 호스트 유형의 다중 시스템에 배포하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 **보호** 드롭다운 메뉴를 클릭한 다음 **Agent 소프트웨어 배포**를 선택합니다.
Agent 소프트웨어 배포 마법사가 열립니다.
2 마법사의 **연결** 페이지에서 **소스** 드롭다운 목록의 **수동으로**를 선택합니다.
3 **다음**을 클릭합니다.
4 마법사의 **시스템** 페이지에서 `hostname::username::password::port` 형식으로 시스템의 세부 정보를 대화 상자에 입력합니다. 예를 들면 다음과 같습니다.

```
10.255.255.255::administrator::&11@yYz90z::8006

abc-host-00-1::administrator::99!zU$o83r::168
```

5 배포 후 자동으로 시스템을 다시 시작하려면 **Agent 설치 후 자동으로 시스템 다시 시작(권장)**을 선택합니다.
6 **마침**을 클릭합니다.
선택한 각 시스템을 시스템에서 자동으로 확인합니다.
자동 확인하는 동안 Rapid Recovery에서 우려 사항을 감지하는 경우, 마법사는 **경고** 페이지를 실행합니다. 이 페이지에서 선택 항목의 시스템을 지우고 해당 시스템을 수동으로 확인할 수 있습니다. 추가한 시스템이 자동 확인을 통과하면 **시스템에 Agent 배포** 창에 이 시스템이 나타납니다.
7 **경고** 페이지가 나타나도 선택 사항에 만족하면 **마침**을 다시 클릭합니다.

Rapid Recovery Agent 소프트웨어가 지정된 시스템에 배포됩니다. 이 시스템은 아직 보호되지 않으며, 수동으로 다중 시스템 보호을(를) 완료한 후 보호가 시작됩니다.

다중 시스템에 배포 확인

Rapid Recovery Agent 소프트웨어를 두 대 이상의 시스템에 동시에 배포한 후 보호된 시스템 메뉴 아래 나열되는 각 시스템을 보고 성공 여부를 확인할 수 있습니다.

또한 이벤트 페이지에서 일괄 배포 프로세스와 관련된 정보를 확인할 수 있습니다. 배포를 확인하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동하여 (이벤트)를 클릭한 다음 **경고**를 클릭합니다.
이벤트가 시작된 시간과 메시지를 보여주는 경고 이벤트가 목록에 나타납니다. 성공한 각 Agent 소프트웨어 배포에 대해 보호된 시스템이 추가되었음을 나타내는 경고가 표시됩니다.
2 (선택 사항) 보호된 시스템의 링크를 클릭합니다.
다음과 같은 관련 정보를 보여주는, 선택한 시스템의 **요약** 페이지가 나타납니다.

- 보호된 시스템의 호스트 이름
- 마지막 스냅숏(해당되는 경우)
- 선택한 시스템의 보호 일정에 따라 예약된 다음 스냅숏 시간
- 이 보호된 시스템에 사용되는 암호화 키(있는 경우)
- Agent 소프트웨어 버전.

배포 설정 수정

배포 설정을 수정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 (설정)을 클릭합니다.
2 **설정** 창의 왼쪽 열에서 배포 섹션으로 이동하려면 **배포**를 클릭합니다.

3 텍스트 상자 또는 드롭다운 목록으로 편집이 가능하도록 변경하려는 설정을 클릭해 다음 옵션 중 하나를 수정하고 ✔ 을 클릭하여 설정을 저장합니다.

표 60. 배포 옵션

옵션	설명
에이전트 설치 프로그램 이름	에이전트 실행 파일 이름을 입력합니다. 기본값은 Agent-web.exe입니다.
Core 주소	Core의 주소를 입력합니다.
수신 실패 제한 시간	제한 시간 초과 전 활동하지 않고 대기할 시간을 분으로 입력합니다.
최대 병렬 설치	동시에 설치하려는 최대 설치 수를 입력합니다. 기본 및 제한은 100입니다.
설치 후 자동 재부팅	예에 대한 확인란을 선택하거나 아니요에 대한 확인란 선택을 취소합니다.
배포 후 보호	예에 대한 확인란을 선택하거나 아니요에 대한 확인란 선택을 취소합니다.

보호 일정 이해

보호 일정은 보호된 에이전트 시스템에서 Rapid Recovery Core로 백업이 전송될 시기를 정의합니다.

Core에 저장된 최초 백업 전송을 기본 이미지 스냅숏이라고 합니다. 지정된 모든 볼륨에 있는 모든 데이터(운영 체제, 응용 프로그램 및 설정 포함)가 Core에 저장되며, 전송 중인 데이터 크기에 따라 상당한 시간이 소요될 수 있습니다. 이후에는 증분 스냅숏(마지막 백업 이후 보호된 시스템에서 변경된 데이터로만 구성되는 더 작은 백업)이 정의된 간격(예: 60분마다)에 따라 정기적으로 Core에 저장됩니다. 이 백업에는 기본 이미지보다 적은 데이터가 포함되므로 전송하는 시간이 짧습니다.

보호 일정은 처음에 시스템 보호 마법사 또는 다중 시스템 보호 마법사를 사용하여 정의됩니다. 마법사를 사용하여 비즈니스 요건에 맞게 보호 일정을 사용자 지정할 수 있습니다(기간 또는 일별 보호 시간 선택). 그런 다음 보호된 특정 시스템의 요약 페이지에 있는 보호 일정 대화 상자에서 언제든지 기존 일정을 수정하거나 새로운 일정을 생성할 수 있습니다.

Rapid Recovery에서는 기본 보호 일정을 제공하며, 기본 보호 일정에는 단일 기간(오전 12:00 ~ 오후 11:59)이 정의된 상태에서 주의 모든 날짜를 포함하는 단일 기간이 포함됩니다. 기본 간격(스냅숏 간의 기간)은 60분입니다. 보호를 처음 활성화할 때 일정도 활성화합니다. 따라서 기본 설정을 사용하면 현재 시간에 관계없이 최초 백업이 시간 단위로 매시간 발생합니다(오전 12:00, 오전 1:00, 오전 2:00 등).

기간을 선택하면 기본 보호 일정을 보고 그에 따라 조정할 수 있습니다. 일별 보호 시간을 선택하면 Rapid Recovery Core가 지정한 시간에 매일 한 번씩 지정된 보호된 시스템을 백업합니다.

일정을 사용자 지정하여 가능한 평일 및 주말 기간으로 사용량이 가장 많은 시간과 적은 시간을 정의할 수 있습니다. 예를 들어, 보호된 시스템을 평일에 많이 사용하는 경우 매 시간마다 세 번의 스냅숏을 작성하도록 평일 간격을 20분으로 줄일 수 있습니다. 또는 트래픽이 낮으면 주말 간격을 60분에서 180분으로 늘려 3시간마다 한 번 스냅숏을 작성할 수 있습니다.

또는 기본 일정을 변경하여 매일 피크 시간 및 피크 시간대가 아닌 시간을 정의할 수 있습니다. 이 작업을 수행하려면 기본 시작 및 종료 시간을 더 작은 시간 범위로 변경하고(예: 오전 12:00 ~ 오후 4:59) 적합한 간격을 설정합니다(예: 20분). 이는 피크 시간대 동안 빈번한 백업을 나타냅니다. 그런 다음, 나머지 시간(오후 5:00 ~ 오후 11:59)에 대한 평일 시간 범위를 추가한 후 적절한(대부분 더 큰) 간격(예: 180분)을 설정할 수 있습니다. 이 설정은 매일 오후 5:00에서 자정까지 포함되는 피크 시간대 이외의 시간을 정의합니다. 이렇게 사용자 지정하면 오후 5:00에서 오후 11:59까지는 3시간마다, 자정부터 오후 4:59까지는 20분마다 스냅숏이 작성됩니다.

보호 일정 대화 상자를 사용하여 보호 일정을 수정하거나 생성할 때 Rapid Recovery에 일정을 재사용 가능한 템플릿으로 저장할 수 있는 옵션이 있으므로 다른 보호된 시스템에도 적용할 수 있습니다.

보호 마법사의 기타 옵션에는 일별 보호 시간 설정이 포함됩니다. 이 설정은 매일 정의된 기간에 단일 백업을 생성합니다(기본 설정은 오후 12:00).

마법사를 사용하여 하나 또는 다중 시스템을 보호 중인 경우 처음에 보호를 일시 중지하여 시스템을 보호하지 않은 상태에서 보호 일정을 정의할 수 있습니다. 설정된 보호 일정에 따라 시스템을 보호할 준비가 되면 명시적으로 보호를 다시 시작해야 합니다. 보호를 재개하는 방법에 대한 자세한 내용은 보호 일시 중지 및 다시 시작을(를) 참조하십시오. (선택 사항) 시스템을 즉시 보호하려는 경우 스냅숏을 수행할 수 있습니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.

시스템 보호

보호하려는 시스템에 Rapid Recovery 에이전트 소프트웨어가 이미 설치되어 있지만 아직 재시작하지 않은 경우 지금 시스템을 재시작합니다.

이 항목에서는 Protect Machine Wizard(시스템 보호 마법사)를 사용하여 사용자가 지정하는 단일 시스템의 데이터를 보호하는 방법에 대해 설명합니다.

노트: VMware 또는 ESXi 호스트에서 에이전트 없는 보호를 사용하지 않는 한, 보호 기능을 이용하려면 보호하려는 시스템에 Rapid Recovery 에이전트 소프트웨어가 설치되어 있어야 합니다. 이 절차 전에 에이전트 소프트웨어를 설치하거나 Protect Machine Wizard(시스템 보호 마법사) 완료의 일부로 대상 시스템에 소프트웨어를 배포할 수 있습니다.
에이전트 없는 보호 및 해당 제한 사항에 대한 자세한 내용은 Rapid Snap for Virtual 이해을(를) 참조하십시오.

에이전트 소프트웨어를 설치하는 방법에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 설치 및 업그레이드 설명서*에서 "Rapid Recovery 에이전트 소프트웨어 설치"를 참조하십시오. 시스템을 보호하기 전에 에이전트 소프트웨어가 설치되어 있지 않은 경우 보호할 특정 볼륨을 이 마법사에 포함하도록 선택할 수 없게 됩니다. 이 경우 기본적으로 에이전트 시스템에 있는 모든 볼륨이 보호됩니다. Rapid Recovery는 EISA 파티션으로 구성된 시스템의 보호 및 복구를 지원합니다. 지원은 Windows Recovery Environment(Windows RE)를 사용하는 Windows 8과 Windows 8.1 및 Windows 2012와 2012 R2 시스템으로도 확장됩니다.

동시에 하나의 프로세스를 사용하여 다중 시스템 보호하려면 다중 시스템 보호 정보을(를) 참조하십시오.

보호를 추가하면 IP 주소 및 포트 같은 연결 정보를 정의하고 보호할 시스템의 자격 증명을 제공해야 합니다. 선택적으로 IP 주소 대신 Core 콘솔에 나타낼 표시 이름을 제공할 수도 있습니다. 이를 변경하는 경우 Core 콘솔의 상세 정보를 볼 때 보호되는 시스템에 대한 IP 주소가 표시되지 않습니다. 시스템에 대한 보호 일정도 정의해야 합니다.

보호 프로세스는 고급 구성을 선택하는 경우 액세스할 수 있는 옵션 단계를 포함합니다. 고급 옵션은 리포지토리 기능과 암호화를 포함합니다. 예를 들어 스냅샷을 저장할 기존 Rapid Recovery 리포지토리를 지정하거나 새 리포지토리를 생성합니다. 기존 암호화 키를 지정할 수도 있습니다. 이 시스템에 대해 Core에 저장된 데이터에 적용할 기존 암호화 키(또는 새 암호화 키를 추가)를 지정할 수도 있습니다. 암호화 키에 대한 자세한 내용은 암호화 키 이해을(를) 참조하십시오.

보호 마법사의 워크플로우는 사용자 환경에 따라 약간 다를 수 있습니다. 예를 들어, Rapid Recovery 에이전트 소프트웨어가 보호하려는 시스템에 설치되어 있는 경우 마법사에서 설치하라는 메시지가 표시되지 않습니다. 마찬가지로, Core에 리포지토리가 이미 존재하는 경우, 만들 것인지 묻는 메시지가 표시되지 않습니다.

주의: Rapid Recovery는 ext2 부트 타피션이 있는 Linux 시스템의 운영 체제 미설치 복원(BMR)을 지원하지 않습니다. 이런 유형의 파티션이 있는 시스템에서 수행된 BMR은 시스템이 시작되지 않는 결과를 초래합니다. 향후 이 시스템에서 BMR을 수행하려면 시스템을 보호하고 백업하기 전에 ext2 파티션을 ext3 또는 ext4 파티션으로 변환해야 합니다.

1 다음 중 하나를 수행합니다.
- Protect Machine Wizard(시스템 보호 마법사)를 시작하는 경우 2단계로 진행하십시오.
- Rapid Recovery Core 콘솔에서 시작하는 경우 버튼 모음에서 **Protect(보호)**를 클릭합니다.

Protect Machine Wizard(시스템 보호 마법사)가 나타납니다.

2 **Welcome(시작)** 페이지에서 적절한 설치 옵션을 선택합니다.
- 리포지토리를 정의할 필요가 없거나 암호화를 설정할 필요가 없을 경우에는 **Typical(일반)**을 선택합니다.
- 리포지토리를 생성하거나 선택한 시스템의 백업을 위해 다른 리포지토리를 정의해야 하는 경우 또는 마법사를 사용하여 암호화를 설정하고자 하는 경우 **Advanced (show optional steps)(고급(옵션 단계 표시)**를 선택합니다.

- 선택적으로 나중에 Protect Machine Wizard(시스템 보호 마법사)에 **Welcome(시작)** 페이지가 표시되지 않도록 하려면 **Skip this Welcome page the next time the wizard opens(다음에 마법사를 열 때 이 시작 페이지 건너뛰기)** 옵션을 선택합니다.

3 Welcome(시작) 페이지의 선택 사항에 만족하면 **Next(다음)**를 클릭합니다.

Connection(연결) 페이지가 나타납니다.

4 **Connection(연결)** 페이지에서, 아래 표에 설명된 대로 연결할 시스템에 대한 정보를 입력하고 **Next(다음)**를 클릭합니다.

표 61. 시스템 연결 설정

텍스트 상자	설명
호스트	보호할 시스템의 호스트 이름 또는 IP 주소입니다.
포트	Rapid Recovery Core가 시스템의 에이전트와 통신하는 포트 번호입니다. 기본 포트 번호는 8006입니다.
사용자 이름	이 시스템에 연결하는 데 사용되는 사용자 이름입니다. 예를 들어, 관리자(또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator)입니다.
암호	이 시스템에 연결하는 데 사용되는 암호입니다.

Protect Machine Wizard(시스템 보호 마법사) 옆에 **Install Agent(에이전트 설치)** 페이지가 나타나는 경우 Rapid Recovery가 시스템의 Rapid Recovery 에이전트 감지하지 못하며 최신 버전의 소프트웨어를 설치합니다. 7단계로 이동합니다.

마법사에서 다음에 **Upgrade Agent(에이전트 업그레이드)** 페이지가 나타나는 경우 이전 버전의 에이전트 소프트웨어가 보호하려는 시스템에 존재하는 것입니다.

노트: 보호하려는 시스템에 에이전트 소프트웨어를 설치해야 하며 Core에 백업하기 전에 해당 시스템을 재시작해야 합니다. 설치 프로그램이 시스템을 보호하도록 하려면 After installation, restart the machine automatically (recommended)(설치 후 시스템을 자동으로 재시작(권장)) 옵션을 선택한 후 Next(다음)를 클릭합니다.

5 **Upgrade Agent(에이전트 업그레이드)** 페이지에서 다음 중 하나를 수행합니다.

- 새 버전의 에이전트 소프트웨어를 배포하려면(Rapid Rapid Recovery의 버전과 일치) **Upgrade the Agent to the latest version of the software(에이전트를 최신 버전의 소프트웨어로 업그레이드)**를 선택합니다.
- 에이전트 소프트웨어 버전을 업데이트하지 않고 시스템을 계속 보호하려면 **Upgrade the Agent to the latest version of the software(에이전트를 최신 버전의 소프트웨어로 업그레이드)** 옵션을 선택 취소합니다

6 **다음**을 클릭합니다.

7 선택적으로, **Protection(보호)** 페이지에서 이 보호되는 시스템의 Rapid Recovery Core 콘솔에 IP 주소 외에 이름을 표시하려는 경우 **Display Name(표시 이름)** 필드의 대화 상자에 이름을 입력합니다.

최대 64자를 입력할 수 있습니다. 금지된 문자 항목에 설명되어 있는 특수 문자를 사용하지 마십시오. 또한, 금지된 구 항목에 설명되어 있는 문자 조합 중 하나로 표시 이름을 시작하지 마십시오.

8 아래에 설명된 대로 적절한 보호 일정을 선택합니다.

- 기본 보호 일정을 사용하려면 Schedule Settings(일정 설정) 옵션에서 **Default protection(기본 보호)**를 선택합니다.

기본 보호 일정을 사용하면 Core는 1시간에 한 번 보호되는 시스템에 있는 모든 볼륨의 스냅샷을 생성합니다. 마법사를 닫은 후 보호할 볼륨 선택을 포함하여 언제든지 보호 설정을 변경하려면 볼륨을 보호하려면 특정 보호 시스템에 대한 요약 페이지로 이동합니다.

- 다른 보호 일정을 정의하려면 Schedule Settings(일정 설정) 옵션에서 **Custom protection(사용자 지정 보호)**을 선택합니다.

9 다음과 같이 구성을 계속 진행합니다.

- **Protect Machine Wizard(시스템 보호 마법사)**에 대해 Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 Finish(마침)를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.

  시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(즉, 보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Rapid Recovery Core의 리포지토리에 전송됩니다.
- Protect Machine Wizard(시스템 보호 마법사)에서 Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.
- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 14단계를 계속 진행하여 리포지토리 및 암호화 옵션을 확인합니다.

- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 11단계를 계속 진행하여 보호할 볼륨을 선택합니다.

10 **Protection Volumes(보호 볼륨)** 페이지에서, 보호할 볼륨을 선택합니다. 보호하지 않을 볼륨이 나열될 경우 Check(확인) 열을 클릭하여 선택 항목을 지우고 **Next(다음)**를 클릭합니다.

노트: 일반적으로 최소한 시스템에서 사용한 볼륨과 운영 체제가 있는 볼륨(일반적으로 C 드라이브)을 보호하는 것이 좋습니다.

11 **Protection Schedule(보호 일정)** 페이지에서 사용자 지정 보호 일정을 정의한 후 **Next(다음)**를 클릭합니다. 사용자 지정 보호 일정을 정의하는 자세한 내용은 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

리포지토리 정보가 이미 구성되어 있고 1단계에서 Advanced(고급) 옵션을 선택한 경우 Encryption(암호화) 페이지가 나타납니다. 13단계로 진행합니다.

12 **Repository(리포지토리)** 페이지에서 다음을 수행합니다.

- 리포지토리가 이미 있고 보호를 위해 기존 리포지토리에 이 시스템의 데이터를 저장하려는 경우 다음을 수행합니다:
  1 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
  2 목록에서 기존 리포지토리를 선택합니다.
  3 **다음**을 클릭합니다.

  Encryption(암호화) 페이지가 나타납니다. 선택적으로 암호화를 정의하려면 13단계로 건너뜁니다.
- 리포지토리를 생성하려는 경우 **Create a Repository(리포지토리 생성)**를 선택한 후 다음 단계를 완료합니다.
  1 **Repository(리포지토리)** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 62. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 첫 번째 리포지토리인 경우 기본 이름은 리포지토리 1입니다. 필요하면 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자를 포함해야 합니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본적으로 값은 64입니다.
설명	선택적으로 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

  2 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

주의: 리포지토리의 저장소 위치는 루트 내에 전용 폴더로 정의합니다. 루트 위치는 지정하지 마십시오. 예를 들어, E:\가 아닌 E:\Repository\를 사용합니다. 이 단계에서 생성하는 리포지토리를 나중에 제거하는 경우 해당 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 루트에 저장소 위치를 정의하는 경우 볼륨(예: E:\)에 있는 다른 모든 파일이 삭제되어 이는 치명적인 데이터 손실을 초래할 수 있습니다.

  Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

  3 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

  4 **Storage Location(저장소 위치)** 영역에 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨을 추가할 수 있습니다(예: 직접 연결된 저장소, 저장소 영역 네트워크 또는 네트워크에 연결된 저장소). 일반 인터넷 파일 시스템(CIFS) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.

  - **Add file on local disk(로컬 디스크에 파일 추가)**를 선택하여 로컬 시스템을 지정하고 아래 표에 설명된 대로 정보를 입력합니다.

표 63. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다.

텍스트 상자	설명
	예를 들어, `X:\Repository\Data`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Metadata`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 또는 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 선택하여 네트워크 공유 위치를 지정한 후 아래 표에 설명된 대로 정보를 입력합니다.

표 64. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.

5 **Storage Configuration(저장소 구성)** 영역에서 **More Details(상세 정보)**를 클릭하고 아래 표에 설명된 대로 저장소 위치에 대한 상세정보를 입력합니다.

표 65. 저장소 구성 상세 정보

텍스트 상자	설명
크기	저장소 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB이고 기본값은 250GB입니다. 다음 중에서 선택할 수 있습니다. • GB • TB **노트: 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2을 사용하는 NTFS 볼륨인 경우 파일 크기 한도는 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows 캐시 관리자가 사용되는 방법을 제어하고 다른 구성에 대해 성능을 최적화할 수 있도록 리포지토리를 조정하는 데 도움을 줍니다. 값을 다음 중 하나로 설정합니다. • 켜짐 • 꺼짐 • 동기화

텍스트 상자	설명
	기본값인 On(켜짐)으로 설정하는 경우 Windows에서 캐싱을 제어합니다. 이는 Windows 10 및 Windows Server 2012 이상 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 Off(꺼짐)입니다.** Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. Sync(동기화)로 설정하면 Windows에서 캐싱과 동기식 입력/출력을 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 **다음**을 클릭합니다.

1단계에서 **Advanced(고급)** 옵션을 선택한 경우 **Encryption(암호화)** 페이지가 나타납니다.

13 선택적으로 **Encryption(암호화)** 페이지에서 암호화를 활성화하려면 **Enable Encryption(암호화 활성화)**을 선택합니다.

Encryption(암호화) 페이지에 Encryption key(암호화 키) 필드가 나타납니다.

노트: 암호화를 활성화하면 이 시스템의 모든 보호되는 볼륨에 있는 데이터에 적용됩니다. Rapid Recovery Core 콘솔에서 나중에 암호화 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 암호화 키 이해 항목을 참조하십시오.

주의: Rapid Recovery에서는 CBC(Cipher Block Chaining) 모드에서 256바이트 키와 함께 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 암호화 키를 설정하고 정의하는 암호를 보호할 것을 권장합니다. 암호는 데이터 복구에 매우 중요하므로 안전한 위치에 저장해 두십시오. 암호가 없으면 데이터를 복구할 수 없습니다.

14 **Encryption(암호화)** 페이지에서 다음 옵션 중 하나를 선택합니다.

- 이 Rapid Recovery Core에 이미 정의된 암호화 키를 사용하여 이 보호되는 시스템을 암호화하려면 **Encrypt data using an existing Encryption key(기존 암호화 키를 사용하여 데이터 암호화)**를 선택한 다음 드롭다운 메뉴에서 적절한 키를 선택합니다. 다음 단계로 진행합니다.
- Core에 새 암호화 키를 추가하고 해당 키를 이 보호되는 시스템에 적용하려는 경우 다음 표에 설명된 대로 정보를 입력합니다.

표 66. 암호화 키 설정

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~130자 사이의 영숫자를 포함해야 합니다. 백슬래시, 사선, 파이프, 콜론, 별표, 따옴표, 물음표, 여는 대괄호나 닫는 대괄호, 앰퍼샌드 또는 해시 같은 특수 문자를 포함할 수 없습니다.
설명	암호화 키의 설명을 입력합니다. 이 정보는 Core 콘솔에서 암호화 키를 볼 때 Description(설명) 필드에 나타납니다.
암호	액세스 제어에 사용되는 암호를 입력합니다. 모범 사례는 위에 나열된 특수 문자의 사용을 피하기 위한 것입니다. 안전한 장소에 암호를 적어 두십시오. Dell 지원에서 암호를 복구할 수 없습니다. 암호화 키를 생성하고 이를 하나 이상의 보호되는 시스템에 적용한 후에는 암호를 분실할 경우 데이터를 복구할 수 없습니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

15 **Finish(마침)**를 클릭하여 저장하고 설정을 적용합니다.

시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(즉, 보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Rapid Recovery Core의 리포지토리에 전송됩니다.

클러스터 보호

이 항목에서는 Rapid Recovery에서 보호를 위해 클러스터를 추가하는 방법에 대해 설명합니다. 보호에 클러스터를 추가할 때 클러스터의 호스트 이름 또는 IP 주소, 클러스터 응용프로그램 또는 Rapid Recovery Agent 소프트웨어를 포함하는 클러스터 노드 또는 시스템 중 하나를 지정해야 합니다.

노트: 리포지토리는 보호된 노드에서 캡처된 데이터의 스냅숏을 저장하는 데 사용됩니다. 클러스터에서 데이터 보호를 시작하기 전에 Rapid Recovery Core와 연결된 리포지토리를 하나 이상 설정했어야 합니다.

리포지토리 설정에 대한 자세한 내용은 리포지토리 이해을(를) 참조하십시오.

1 Rapid Recovery Core Console에서 **보호** 단추 드롭다운 메뉴를 클릭한 다음 **클러스터 보호**를 클릭합니다.
2 Connect to Cluster(클러스터에 연결) 대화 상자에 다음 정보를 입력합니다.

표 67. 클러스터에 연결 설정

텍스트 상자	설명
호스트	클러스터의 호스트 이름 또는 IP 주소, 클러스터 응용프로그램 또는 클러스터 노드 중 하나.
포트	Rapid Recovery Core가 Agent와 통신하는 시스템의 포트 번호입니다. 기본 포트는 8006입니다.
사용자 이름	이 시스템에 연결하는 데 사용된 도메인 관리자의 사용자 이름입니다(예: domain_name\administrator). **노트: 도메인 이름은 필수 사항입니다. 로컬 관리자 사용자 이름을 사용하여 클러스터에 연결할 수 없습니다.**
암호	이 시스템에 연결하는 데 사용되는 암호입니다.

3 **연결**을 클릭합니다.
4 클러스터 보호 대화 상자에서 이 클러스터에 대한 리포지토리를 선택합니다.
5 Core 기반 암호화를 사용하여이 클러스터에 대한 복구 지점을 보호하려면 암호화 키를 선택합니다.
6 이 절차를 완료한 후 즉시 보호가 시작되지 않게 하려면 **초기 보호 일시 중지**를 선택합니다.
7 기본 설정에 기반한 클러스터를 보호하려면 기본 보호 노드를 선택하고 10단계로 건너뜁니다.

노트: 기본 설정은 60분 간격으로 모든 볼륨의 스냅숏을 예약합니다.

8 클러스터에 대한 사용자 지정 설정을 입력(예: 공유 볼륨에 대한 보호 일정 사용자 지정)하려면 다음 중 하나를 수행하고 사용자 지정 보호 일정 만들기을(를) 참조하십시오.
   - 개별 노드에 대한 설정을 사용자 지정하려면 사용자 지정하려는 노드 옆의 **설정**을 클릭한 다음 관련 볼륨 옆의 **기능**을 클릭합니다.
   - 클러스터에 대한 설정을 사용자 지정하려면 대화 상자 맨 아래에서 설정 단추를 클릭한 다음 관련 볼륨 옆의 **기능**을 클릭합니다.

   노드 사용자 지정에 대한 자세한 내용은 클러스터의 노드 보호를 참조하십시오.
9 필요한 내용을 모두 변경했으면 **저장**을 클릭합니다.
10 클러스터 보호 대화 상자에서 **보호**를 클릭합니다.

클러스터 노드 설정 수정

클러스터 노드에 대한 보호를 추가한 후 이러한 시스템 또는 노드에 대한 기본 구성 설정(예: 표시 이름, 호스트 이름 등) 및 보호 설정(예: 시스템의 로컬 볼륨에 대한 보호 일정 변경, 볼륨 추가 또는 제거, 보호 일시 중지) 등을 쉽게 수정할 수 있습니다.

클러스터 노드 설정을 수정하려면 다음 작업을 수행해야 합니다.

- Rapid Recovery Core 콘솔에서 수정하려는 노드가 포함되어 있는 클러스터로 이동하고 수정하려는 시스템 또는 노드를 선택합니다.

- 구성 설정을 수정하고 보려면 알림 그룹 구성을 참조하십시오.
- 시스템 이벤트에 대한 알림 그룹을 구성하려면 보호된 시스템 설정 보기 및 수정을 참조하십시오.
- 보존 정책 설정을 사용자 지정하려면 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을 참조하십시오.
- 보호 일정을 수정하려면 보호 일정 수정을 참조하십시오.
- 전송 설정을 수정하려면 전송 설정 수정 정보을 참조하십시오.

클러스터의 노드 보호

이 작업 전에 클러스터를 먼저 보호해야 합니다. 자세한 내용은 클러스터 보호을(를) 참조하십시오.

이 항목에서는 Rapid Recovery Agent가 설치된 클러스터 노드 또는 시스템의 데이터를 보호하는 방법을 설명합니다. 이 절차에서는 클러스터를 보호할 때 빠뜨렸을 수도 있는 개별 노드를 보호에 추가할 수 있습니다.

1 Rapid Recovery Core Console의 보호된 시스템 아래에서 보호하려는 노드가 있는 클러스터를 클릭합니다.
2 클러스터의 요약 페이지에서 **보호된 노드**를 클릭합니다.
3 보호된 노드 페이지에서 **클러스터 노드 보호**를 클릭합니다.
4 클러스터 노드 보호 대화 상자에서 다음 중 적절한 정보를 선택하거나 입력합니다.

표 68. 클러스터 노드 보호 설정

텍스트 상자	설명
호스트	보호할 수 있는 클러스터의 노드로 구성된 드롭다운 목록.
포트	Rapid Recovery Core에서 노드의 에이전트와 통신하는 포트 번호.
사용자 이름	이 노드에 연결하는 데 사용된 도메인 관리자의 사용자 이름. 예: example_domain\administrator 또는 administrator@example_domain.com.
암호	이 시스템에 연결하는 데 사용되는 암호입니다.

5 노드를 추가하려면 **연결**을 클릭합니다.
6 기본 보호 설정으로 이 노드 보호를 시작하려면 13단계로 이동합니다.

노트: 기본 설정을 사용하면 시스템의 모든 볼륨이 60분 주기의 일정으로 보호됩니다.

7 기본 설정이 아닌 리포지토리를 사용하려면 [노드 이름] 보호 대화 상자에서 드롭다운 목록을 사용하여 리포지토리를 선택합니다.
8 Core 기반 암호화를 사용하여 이 클러스터의 복구 지점을 보안하려면 드롭다운 목록을 사용하여 암호화 키를 선택합니다.
9 이 절차를 완료한 후 즉시 보호가 시작되지 않게 하려면 **초기 보호 일시 중지**를 선택합니다.
10 사용자 지정 설정(예: 공유 볼륨의 보호 일정 사용자 지정)을 입력하려면 다음을 수행합니다.
   a 개별 볼륨의 설정을 사용자 지정하려면, 사용자 지정하려는 볼륨 옆으로 이동하여 관련 볼륨 옆의 **기능**을 클릭합니다.
   b 사용자 지정 보호 일정 만들기을(를) 참조하십시오.
11 **Protect(보호)**를 클릭합니다.

사용자 지정 보호 일정 만들기

마법사를 사용하여 보호를 정의할 때 보호된 시스템에서 데이터를 보호할 사용자 지정 일정을 만들려면 이 절차의 단계를 완료하십시오.

1 보호 마법사(시스템 보호, 여러 시스템 보호, 클러스터 보호)의 **보호** 페이지에서 사용자 지정 보호를 선택합니다.
2 **다음**을 클릭합니다.
3 **보호 볼륨** 페이지에서 보호하려는 볼륨을 선택한 후 **다음**을 클릭합니다.
4 **보호 일정** 페이지에서 기간의 간격 일정을 변경하려면 다음을 수행합니다.
   a **기간**을 선택합니다.

기존 기간이 표시되며 수정할 수 있습니다. 편집 가능한 필드에는 각 기간의 시작 시간, 종료 시간 및 간격(X분 주기)이 포함됩니다.

b 기간마다 간격 텍스트 상자를 클릭하여 적절한 간격을 분 단위로 입력합니다.

예를 들어, 이 기간 중 20분 주기로 스냅숏을 수행하려면 기본 간격 60에 강조 표시하여 값을 20으로 바꿉니다.

5 평일의 정점 및 비정점 기간을 만들려면 평일 기간의 시간 범위를 24시간 기간이 포함되지 않도록 변경하고, 정점 범위의 최적 간격을 선택하고, **나머지 시간 동안 스냅숏 생성**을 선택한 후 다음을 수행하여 비정점 간격을 설정합니다.

a **기간**을 선택합니다.

기존 기간이 표시되며 수정할 수 있습니다.

b **시작** 상자를 클릭하거나 시계 아이콘을 사용하여 이 기간의 시작 시간을 변경합니다.

c **종료** 상자를 클릭하거나 시계 아이콘을 사용하여 이 기간의 종료 시간을 변경합니다.

d 간격 텍스트 상자를 클릭하여 적절한 간격을 분 단위로 입력합니다.

예를 들어, 이 기간에 대해 선택한 시간 범위 동안 20분 주기로 스냅숏을 수행하려면 기본 간격 60에 강조 표시하여 값을 20으로 바꿉니다.

e **나머지 시간 동안 스냅숏 생성**을 선택한 후 간격을 분 단위로 입력합니다.

6 매일 단일 백업이 발생하는 날짜의 단일 시간을 설정하려면 **일별 보호 시간**을 선택한 다음 HH:MM AM 형식으로 시간을 입력합니다. 예를 들어, 오후 9:00에 일별 백업을 수행하려면 09:00 PM을 입력합니다.

7 백업을 시작하지 않고 일정을 정의하려면 **초기 보호 일시 중지**를 선택합니다.

마법사에서 보호를 일시 중지하면 명시적으로 보호를 다시 시작하기 전까지 일시 중지된 상태로 남아 있습니다. 보호를 다시 시작하면 설정한 일정에 따라 백업이 발생합니다. 보호를 다시 시작하는 방법에 대한 자세한 내용은 보호 일시 중지 및 다시 시작을 참조하십시오.

8 변경한 보호 일정을 사용하려면 **마침** 또는 **다음** 중에서 하나를 클릭합니다. 해당 마법사의 절차로 돌아가서 나머지 필요한 작업을 완료합니다.

보호 일정 수정

보호 일정은 보호된 에이전트 시스템에서 Rapid Recovery Core로 백업이 전송될 시기를 정의합니다. 보호 일정은 처음에 시스템 보호 마법사 또는 다중 시스템 보호 마법사를 사용하여 정의됩니다.

언제든지 특정 에이전트 시스템에 대해 요약 탭에서 기존 보호 일정을 수정할 수 있습니다.

노트: 보호 일정에 대한 개념적 정보는 보호 일정 이해을(를) 참조하십시오. 단일 시스템 보호에 대한 자세한 내용은 시스템 보호을(를) 참조하십시오. 일괄 보호(다중 시스템 보호)에 대한 자세한 내용은 다중 시스템 보호 정보을(를) 참조하십시오. 마법사 중 하나를 사용하여 에이전트를 보호할 때 보호 기간을 사용자 지정하는 방법에 대한 자세한 내용은 사용자 지정 보호 일정 만들기을(를) 참조하십시오. 기존 보호 일정을 수정하는 방법에 대한 자세한 내용은 보호 일정 수정을(를) 참조하십시오.

보호된 시스템의 볼륨에 대해 기존 보호 일정을 수정하려면 다음 단계를 완료하십시오.

1 Core Console의 보호된 시스템 목록에서 보호 일정을 변경할 보호된 시스템을 클릭합니다.

2 선택한 시스템에 대한 페이지에서 해당 볼륨을 선택한 후 **일정 설정**을 클릭합니다.

모든 볼륨을 동시에 선택하려면 헤더 행의 확인란을 클릭합니다. 처음에는 모든 볼륨이 동일한 보호 일정을 공유합니다.

노트: 일반적으로, 최소한 시스템 예약 볼륨 및 운영 체제가 있는 볼륨(보통 C 드라이브)을 보호하는 것이 좋습니다.

보호 일정 대화 상자가 나타납니다.

3 보호 일정 대화 상자에서 다음 중 하나를 수행합니다.

- 이전에 보호 일정 템플릿을 만들었고 이 템플릿을 보호된 시스템에 적용하려면, 드롭다운 목록에서 템플릿을 선택한 후 7단계로 이동합니다.
- 일정에서 기존 기간을 제거하려면 각 기간 옵션 옆의 확인란 선택을 취소한 후 7단계로 이동합니다. 다음과 같은 옵션이 포함됩니다.
  - 월 - 금: 이 시간 범위는 일반적인 평일 5일을 나타냅니다.
  - 토 - 일: 이 시간 범위는 일반적인 주말을 나타냅니다.
- 새 보호 일정을 템플릿으로 저장하려면 4단계로 계속합니다.

4 평일 시작 및 종료 시간이 오전 12:00부터 오후 11:59까지인 경우 단일 기간이 존재합니다. 정의된 기간의 시작 또는 종료 시간을 변경하려면 다음 작업을 수행합니다.

a 해당 기간을 선택합니다.
b 이 기간의 시작 시간을 변경하려면 **시작 시간**아래에 있는 시계 아이콘을 사용합니다.
예를 들어, 화살표를 사용하여 오전 8시를 표시합니다.
c 이 기간의 종료 시간을 변경하려면 **종료 시간**아래에 있는 시계 아이콘을 사용합니다.
예를 들어, 화살표를 사용하여 오후 6시를 표시합니다.
d 필요에 따라 간격을 변경합니다. 예를 들어, 피크 시간대를 정의하는 경우 시간당 세 번 스냅숏을 작성하도록 간격을 60분에서 20분으로 변경합니다.

5 7단계에서 오전 12:00부터 오후 11:59까지 이외의 기간을 정의한 경우, 나머지 시간 범위에서 백업이 발생하도록 하려면 다음과 같이 추가적인 기간을 추가하여 보호를 정의해야 합니다.
a 해당 범주 아래에서 **기간 추가**를 클릭합니다.
b 시계 아이콘을 클릭하고 원하는 시작 및 종료 시간을 적절하게 선택합니다.
예를 들어, 시작 시간으로 오전 12:00 및 종료 시간으로 오전 7:59를 설정합니다.
c 필요에 따라 간격을 변경합니다. 예를 들어, 피크 시간대가 아닌 기간을 정의하는 경우 두 시간마다 스냅숏을 작성하도록 간격을 60분에서 120분으로 변경합니다.

6 필요한 경우 추가 기간을 계속 생성하고 시작 및 종료 시간을 적절히 설정합니다.

노트: 추가한 기간을 제거하려면 기간의 맨 오른쪽에 있는 휴지통 아이콘을 클릭한 후 예를 클릭하여 확인합니다.

7 설정하는 일정에서 템플릿을 만들려면 **템플릿으로 저장**을 클릭합니다.
8 템플릿 저장 대화 상자에 템플릿 이름을 입력하고 **저장**을 클릭합니다.
9 보호 일정이 요구사항에 맞으면 **Apply(적용)**을 클릭합니다.
보호 일정 대화 상자가 닫힙니다.

보호 일시 중지 및 다시 시작

보호를 일시 중지하면 선택한 시스템에서 Rapid Recovery Core로 전송하는 모든 데이터가 일시적으로 중지됩니다. 보호를 다시 시작하면 Rapid Recovery Core가 보호 일정의 요구 사항에 따라 해당 일정에 맞춰 정기적으로 데이터를 백업합니다.

Rapid Recovery로 보호된 시스템에서 보호를 일시 중지할 수 있습니다.

- 시스템 보호 마법사 또는 다중 시스템 보호 마법사를 사용하여 보호를 설정하는 경우
- Rapid Recovery Core의 왼쪽 탐색 영역에 있는 보호된 시스템 드롭다운 메뉴에서(모든 보호된 시스템에 대한 보호 일시 중지)
- 보호된 시스템 메뉴를 클릭하여 액세스할 수 있는 보호된 시스템 페이지에서
- 보호된 시스템 드롭다운 메뉴의 보호된 특정 시스템에서
- 보호된 특정 시스템에 대한 모든 페이지 맨 위에서

시스템 보호 마법사 또는 다중 시스템 보호 마법사를 사용하여 보호를 일시 중지하면 명시적으로 다시 시작할 때까지 보호가 일시 중지됩니다.

마법사 외부에서 보호를 일시 중지하는 경우 다시 시작할 때까지 보호를 일시 중지하거나 지정된 시간(일, 시간 및 분 조합으로 지정) 동안 일시 중지할지 여부를 선택할 수 있습니다. 일정 기간 동안 중지하는 경우 해당 시간이 만료되면 시스템이 보호 일정에 따라 자동으로 보호를 다시 시작합니다.

일시 중지한 Rapid Recovery로 보호된 시스템에 대해 보호를 다시 시작할 수 있습니다.

- Rapid Recovery Core의 왼쪽 탐색 영역에 있는 보호된 시스템 드롭다운 메뉴에서(모든 보호된 시스템에 대한 보호 재개)
- 보호된 시스템 드롭다운 메뉴의 보호된 특정 시스템에서
- 보호된 시스템 메뉴를 클릭하여 액세스할 수 있는 보호된 시스템 페이지에서
- 보호된 특정 시스템에 대한 모든 페이지 맨 위에서

보호를 적절히 일시 중지하거나 다시 시작하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 모든 시스템에 대한 보호를 일시 중지하려면 왼쪽 탐색 영역에서 보호된 시스템 드롭다운 메뉴를 클릭한 후 다음을 수행합니다.
a **보호 일시 중지**를 선택합니다.

보호 일시 중지 대화 상자가 나타납니다.

b 아래 설명된 옵션 중 하나를 사용하여 적절한 설정을 선택한 후 **확인**을 클릭합니다.

- 명시적으로 다시 시작할 때까지 보호를 일시 중지하려면 **다시 시작될 때까지 일시 중지**를 선택합니다.
- 지정된 기간 동안 보호를 일시 중지하려면 **일시 중지 기간**을 선택한 후 일, 시간 및 분 컨트롤에 적절한 일시 중지 기간을 입력하거나 선택합니다.

2 모든 시스템에 대한 보호를 다시 시작하려면 다음을 수행합니다.

a **보호 다시 시작**을 선택합니다.

보호 다시 시작 대화 상자가 나타납니다.

b 보호 다시 시작 대화 상자에서 **예**를 선택합니다.

보호 다시 시작 대화 상자가 닫히고 모든 시스템에 대해 보호가 다시 시작됩니다.

3 단일 시스템에 대한 보호를 일시 중지하려면 왼쪽 탐색 영역에서 적용할 시스템의 오른쪽에 있는 드롭다운 메뉴를 클릭한 후 다음을 수행합니다.

a **보호 일시 중지**를 선택합니다.

보호 일시 중지 대화 상자가 나타납니다.

b 아래 설명된 옵션 중 하나를 사용하여 적절한 설정을 선택한 후 **확인**을 클릭합니다.

- 명시적으로 다시 시작할 때까지 보호를 일시 중지하려면 **다시 시작될 때까지 일시 중지**를 선택합니다.
- 지정된 기간 동안 보호를 일시 중지하려면 **일시 중지 기간**을 선택한 후 일, 시간 및 분 컨트롤에 적절한 일시 중지 기간을 입력하거나 선택합니다.

4 단일 시스템에 대한 보호를 다시 시작하려면 다음을 수행합니다.

a **보호 다시 시작**을 선택합니다.

보호 다시 시작 대화 상자가 나타납니다.

b 보호 다시 시작 대화 상자에서 **예**를 선택합니다.

보호 다시 시작 대화 상자가 닫히고 선택한 시스템에 대해 보호가 다시 시작됩니다.

5 시스템 페이지에서 단일 시스템에 대한 보호를 일시 중지하려면 적용할 시스템으로 이동합니다.

선택한 시스템에 대한 요약 페이지가 표시됩니다.

a 페이지 맨 위에서 **일시 중지**를 클릭합니다.

보호 일시 중지 대화 상자가 나타납니다.

b 아래 설명된 옵션 중 하나를 사용하여 적절한 설정을 선택한 후 **확인**을 클릭합니다.

- 명시적으로 다시 시작할 때까지 보호를 일시 중지하려면 **다시 시작될 때까지 일시 중지**를 선택합니다.
- 지정된 기간 동안 보호를 일시 중지하려면 **일시 중지 기간**을 선택한 후 일, 시간 및 분 컨트롤에 적절한 일시 중지 기간을 입력하거나 선택합니다.

.

6 보호를 다시 시작하려면 다음 작업을 수행합니다.

a 페이지 맨 위에서 **재개**를 클릭합니다.

b 보호 다시 시작 대화 상자에서 **예**를 클릭합니다.

보호 다시 시작 대화 상자가 닫히고 선택한 시스템에 대한 보호가 다시 시작됩니다.

보호된 시스템 관리

이 장에서는 Rapid Recovery 환경에서 보호된 시스템을 보고, 구성 및 관리하는 방법을 설명합니다.

보호된 시스템 관리 정보

보호된 시스템을 관리하기 위해 수행할 수 있는 작업은 몇 가지 범주로 나누어져 있습니다.

- Rapid Recovery 항목에 설명된 옵션을 사용하여 Rapid Recovery Core에서 보호된 시스템을 볼 수 있습니다.
- 시스템 설정을 구성하거나 시스템 정보에 액세스하거나 특정 시스템 관련 이벤트에 대한 알림을 구성할 수 있습니다. 자세한 내용은 시스템 설정 구성을(를) 참조하십시오.
- 보호된 시스템에 대한 진단에 액세스할 수 있습니다. 자세한 내용은 보호된 시스템의 로그 파일 다운로드 및 보기을(를) 참조하십시오.

- 보호에서 시스템을 제거하거나 현재 작업을 취소하거나 보호된 시스템에 대한 라이센스 정보를 볼 수 있습니다. 자세한 내용은 시스템 관리을(를) 참조하십시오.
- Core에 저장된 데이터를 보고 관리할 수 있습니다. 자세한 내용은 스냅숏 및 복구 지점 관리을(를) 참조하십시오.

보호된 시스템 보기

Rapid Recovery Core Console의 **홈** 페이지에서 요약 표 보기를 볼 때 보호된 시스템 창에서 Core가 보호하는 시스템에 대한 요약 정보를 볼 수 있습니다.

노트: 소프트웨어 에이전트가 사용자 대신 특정 작업을 수행합니다. 보호된 시스템은 Rapid Recovery Agent 소프트웨어를 실행하여 Rapid Recovery Core에서 데이터 백업 및 복제를 쉽게 수행하므로, 때때로 에이전트라고 합니다.

상태, 각 시스템의 표시 이름, 시스템에서 사용하는 리포지토리, 마지막 스냅숏의 날짜 및 시간, 시스템에 대한 리포지토리에 존재하는 복구 지점 수, 그리고 리포지토리에서 스냅숏이 사용하는 총 저장 공간을 볼 수 있습니다.

보호된 시스템의 양상을 관리하려면 보거나 구성 또는 관리할 시스템으로 이동하여 시작합니다. 홈 페이지에서 보호된 시스템으로 이동하는 세 가지 방법이 있습니다.

- Protected Machines(보호된 시스템) 창에서 보호된 시스템의 IP 주소 또는 표시 이름을 클릭합니다. 그러면 선택한 보호된 시스템에 대한 Summary (요약) 페이지로 이동합니다.
- 왼쪽 탐색 영역에 있는 **보호된 시스템** 메뉴의 제목을 클릭합니다. 보호된 시스템 페이지가 표시됩니다. Protected Machines(보호된 시스템) 페이지에서 각 시스템에 대한 요약 정보를 확인할 수 있습니다. 이 페이지에 대한 자세한 설명은 보호된 시스템의 요약 정보 보기를 참조하십시오.
- 왼쪽 탐색 영역의 Protected Machines(보호된 시스템) 메뉴에서 보호된 시스템 IP 주소 또는 표시 이름을 클릭할 수 있습니다. 그러면 선택한 보호된 시스템에 대한 Summary (요약) 페이지로 이동합니다. 이 페이지에 대한 자세한 설명은 에서 확인하십시오. 보호된 시스템의 요약 정보 보기

클러스터 요약 정보 보기

클러스터에 대해 연결된 쿼럼에 대한 정보를 포함하여 클러스터 요약 정보를 보려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 보호된 시스템 아래에서 보려는 클러스터를 클릭합니다.
시스템의 요약 페이지가 표시됩니다.

2 요약 페이지에서 클러스터 이름, 클러스터 유형, 쿼럼 유형(해당하는 경우) 및 쿼럼 경로(해당하는 경우) 등의 정보를 볼 수 있습니다. 또한 이 페이지는 크기 및 보호 일정을 포함하여 이 클러스터의 볼륨에 대한 개요 정보를 표시합니다. 해당되는 경우 다른 클러스터에 대한 SQL Server 또는 Exchange Server 정보도 볼 수 있습니다.

3 가장 현재 정보를 보려면 **새로 고침**을 클릭합니다.

클러스터의 개별 시스템 또는 노드에 대한 요약 및 상태 정보 보기에 대한 자세한 내용은 보호된 시스템 보기을(를) 참조하십시오.

시스템 설정 구성

Rapid Recovery에서 보호할 시스템을 추가했으면 해당 보호되는 시스템의 동작을 제어하는 설정을 손쉽게 보고 수정할 수 있습니다. 특정 시스템에 대한 설정을 수정하는 경우, 이러한 설정은 코어 수준에서 설정된 동작을 대체합니다.

Rapid Recovery Core 콘솔에서 다음 시스템 설정을 보고 구성할 수 있습니다.

- **General(일반)**. 일반 시스템 구성 설정은 표시 이름, 호스트 이름, 포트, 암호화 키 및 리포지토리를 포함합니다. 시스템에 대한 일반 설정 구성에 대한 자세한 내용은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.
- **Nightly jobs(야간 작업)**. 보호되는 특정 시스템에 대해 나타나는 Core 야간 작업 설정의 하위 집합을 사용하면 Core 수준에서 설정된 야간 작업 설정 집합을 대체할 수 있습니다. 여기에는 보존 정책을 관리할 수 있는 롤업이 포함됩니다. 일부 설정은 보호되는 시스템 유형에 따라 다를 수 있습니다.
- **Transfer settings(전송 설정).** 선택한 보호되는 시스템에 대한 데이터 전송 프로세스를 관리하는 설정입니다. 이러한 설정의 영향을 받는 데이터 전송 유형에 대한 자세한 내용은 전송 설정 수정 정보을(를) 참조하십시오.
- **Excluded writers(제외된 기록기)**. 이러한 설정을 사용하면 기록기를 제외할 수 있습니다. 기록기는 Microsoft VSS에 다른 소프트웨어 구성 요소를 참여하기 위해 Microsoft에서 제공하는 특정한 API입니다. 볼륨 스냅샷에 참가하는 Rapid Recovery의 각 기록기는 Excluded writers(제외된 기록기) 설정에 나열됩니다. 작성기가 성공적인 백업 전송을 간섭하거나 방해하는 경우 하나씩 비활성화될 수 있습니다. Dell 지원 담당자가 그렇게 하도록 지시하는 경우가 아니면 이러한 설정은 그대로 두는 것이 좋습니다.

- **License details(라이센스 상세 정보)**. 이는 보호되는 특정 시스템에 대한 라이센스 정보입니다. 이러한 설정은 Core 및 Dell Data Protection | Rapid Recovery License Portal의 정보를 보고합니다. 이러한 설정은 읽기 전용입니다. 설정을 변경하려면 Core 및 라이센스 포털 간에 라이센스 정보를 업데이트하십시오. 자세한 내용은 라이센스 관리자에게 문의하십시오. 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 사용자 설명서*를 참조하십시오.

시스템 수준 설정을 보거나 변경하는 절차는 작성기 및 라이센스 세부 정보를 제외하고는 일반적으로 동일합니다. 자세한 내용은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.

시스템에 대한 야간 작업을 수정하는 절차는 다릅니다. 시스템에 대한 야간 작업 설정 구성에 대한 자세한 내용은 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

경우에 따라 보호되는 시스템에 대한 데이터 전송 속도를 조정이 필요할 수 있습니다. 자세한 내용은 전송 설정 수정 정보을(를) 참조하십시오.

보호된 시스템 설정 보기 및 수정

시스템 설정으로 Core에서 보호하는 시스템의 동작을 지정할 수 있습니다. 특정 시스템의 설정을 수정할 때 이 설정은 Core 수준에서 설정한 동작보다 우선합니다.

이 절차의 단계를 완료하여 일반 설정, 전송 설정, 제외된 기록기 설정 및 보호된 시스템의 라이센스 설정을 보고 수정합니다.

노트: 야간 작업 설정을 보고 수정하려면 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

이 작업은 또한 클러스터 노드 설정 수정의 단계입니다.

1 Rapid Recovery Core Console의 보호된 시스템 메뉴 아래에서 구성 설정을 보거나 수정할 시스템의 IP 주소 또는 시스템 이름을 클릭합니다.

선택한 시스템에 대한 **요약** 페이지가 나타납니다.

2 **설정** 메뉴를 클릭합니다.

선택한 시스템에 대한 설정을 표시하는 **설정** 페이지가 나타납니다. 필요에 따라 페이지 어디에서나 설정 범주를 표시하려면 페이지 왼쪽에서 적합한 하이퍼링크를 클릭합니다.

변경할 설정을 클릭할 때 해당 설정은 텍스트 필드 또는 드롭다운 메뉴로 편집할 수 있게 됩니다.

각 설정에 대해 변경을 마치면 ✔ 를 클릭하여 변경 사항을 저장하고 편집 모드를 종료하거나 ✖ 를 클릭하여 저장하지 않고 편집 모드를 종료합니다.

3 보호된 시스템의 일반 설정을 수정하려면 해당 설정을 클릭한 후 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 69. 보호된 시스템의 일반 설정

텍스트 상자	설명
표시 이름	시스템의 표시 이름을 입력합니다. Rapid Recovery Core Console에서 보호된 시스템에 대해 표시되는 이름입니다. 최대 64자를 입력할 수 있습니다. 기본적으로 이 이름은 시스템의 호스트 이름입니다. 필요에 따라 사용자에게 더 익숙한 이름으로 변경할 수 있습니다. 금지된 문자 또는 금지된 구을(를) 사용하지 마십시오.
호스트 이름	시스템의 호스트 이름을 입력합니다.
포트	시스템의 포트 번호를 입력합니다. 포트는 Rapid Recovery Core 서비스가 이 시스템과 통신하는 데 사용됩니다. 기본 포트는 8006입니다.
암호화 키	이 Rapid Recovery Core에 대해 정의된 암호화 키를 이 보호된 시스템의 모든 볼륨의 데이터에 적용할 경우 여기서 암호화 키를 지정할 수 있습니다. 키의 잠금을 해제해야 합니다. 암호화 키가 없는 경우 암호화 키를 추가할 수 있습니다. 암호화 키 관리에 대한 자세한 내용은 암호화 키 관리을(를) 참조하십시오.

텍스트 상자	설명
	보호된 시스템의 볼륨이 암호화된 경우 다른 암호화 키로 변경할 수 있습니다. 또는 **암호화 키** 드롭다운 메뉴에서 **(없음)**을 선택하여 암호화 키를 연결 해제할 수 있습니다. **노트: 암호화 키를 적용하거나, 암호화 키를 변경하거나, 보호된 시스템에 대한 암호화 키를 연결 해제하면, Rapid Recovery가 다음 예약 또는 강제된 스냅숏에서 새 기본 이미지를 작성합니다.**
리포지토리	복구 지점의 리포지토리를 선택합니다. 이 시스템의 데이터를 저장할 Rapid Recovery Core에 구성된 리포지토리를 표시합니다. 리포지토리 볼륨은 로컬(Core 서버에 연결된 저장소) 또는 CIFS 공유 위치의 볼륨이 될 수 있습니다. **노트: 복구 지점이 없거나 이전 리포지토리가 없는 경우에만 이 페이지의 리포지토리 설정을 변경할 수 있습니다.**

4 보호된 시스템의 야간 작업 설정을 수정하려면 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

5 보호된 Exchange 서버의 Exchange 설정을 수정하려면 Exchange Server 설정 섹션에서 **자동 탑재 기능 검사 사용**을 클릭한 후 다음을 수행합니다.

- 자동 탑재 기능 검사를 사용하려면 확인란을 선택한 다음 ✔ 를 클릭합니다.
- 자동 탑재 기능 검사를 사용하지 않으려면 확인란을 선택 해제한 후 ✖ 을 클릭합니다.

자동 탑재 기능 검사에 대한 자세한 내용은 Exchange 데이터베이스 마운트 가능성 검사 정보을(를) 참조하십시오.

6 보호된 시스템의 전송 설정을 수정하려면 해당 설정을 클릭한 후 다음 표에 설명된 대로 구성 정보를 입력합니다.

노트: 전송 설정에 대한 개념적 정보는 전송 설정 수정 정보을(를) 참조하십시오.

표 70. 보호된 시스템의 전송 설정

텍스트 상자	설명
↶ 기본값 복원	이 컨트롤은 모든 전송 설정을 시스템 기본 설정으로 복원합니다.
우선 순위	보호된 시스템 간의 전송 우선 순위를 설정합니다. 다른 보호된 시스템과의 비교를 통해 우선 순위를 할당할 수 있습니다. 1부터 10까지 숫자를 선택합니다(1은 가장 높은 우선 순위). 기본 설정은 우선 순위 5로 설정됩니다. **노트: 우선 순위는 대기열에 있는 전송에 적용됩니다.**
최대 동시 스트림 수	DVM 리포지토리에 보호된 시스템에 대해 보호된 시스템별로 동시에 처리할 Core에 전송되는 TCP 링크의 최대 수를 설정합니다. **노트: Dell은 이 값을 8로 설정할 것을 권장합니다. 패킷 삭제가 발생하면 이 설정을 높여 보십시오.**
최대 동시 쓰기 수	보호된 시스템 연결당 동시 디스크 쓰기 작업의 최대 수를 설정합니다. **노트: Dell는 이 값을 최대 동시 스트림 수에 대해 선택한 값과 동일하게 설정하도록 권장합니다. 패킷 손실이 발생하면 이 값을 약간 낮게 설정하십시오. 예를 들어, 최대 동시 스트림 수가 8인 경우 이 값을 7로 설정하십시오.**
Core 기본 최대 재시도 횟수 사용	일부 작업이 완료되지 않을 경우 각 보호된 시스템에 대해 기본 재시도 횟수를 사용하려면 이 옵션을 선택합니다.
최대 세그먼트 크기	컴퓨터가 단일 TCP 세그먼트에서 수신할 수 있는 가장 큰 데이터 크기를 바이트 단위로 지정합니다. 기본 설정은 4194304입니다.

텍스트 상자	설명
	Dell 지원 담당자가 지시한 경우가 아니라면 이 기본 설정을 변경하지 마십시오.
최대 전송 대기열 깊이	동시에 보낼 수 있는 명령 크기를 지정합니다. 기본 설정은 64입니다. 시스템에 많은 동시 입력/출력 작업이 있는 경우 이 값을 더 높은 숫자로 조정할 수 있습니다.
스트림당 대기 중인 읽기 수	백엔드에 저장할 대기열에 보관되는 읽기 작업 수를 지정합니다. 이 설정을 사용하면 보호된 시스템의 대기열 보관을 제어할 수 있습니다. 기본 설정은 0입니다.
전송 데이터 서버 포트	전송 포트를 설정합니다. 기본 설정은 8009입니다.
전송 시간 초과	패킷이 전송되지 않는 기간을 분 및 초 단위로 지정합니다.
스냅숏 시간 초과	스냅숏을 작성하기 위한 최대 대기 시간을 분 및 초 단위로 지정합니다.
스냅숏 정리 시간 제한	보호된 시스템에서 VSS 스냅숏을 삭제하는 프로세스에 대한 최대 대기 시간을 분 및 초 단위로 지정합니다.
네트워크 읽기 시간 초과	읽기 연결을 위한 최대 대기 시간을 분 및 초 단위로 지정합니다. 이 시간에 네트워크 읽기를 수행할 수 없으면 작업이 다시 시도됩니다.
네트워크 쓰기 시간 초과	쓰기 연결을 위한 최대 대기 시간을 초 단위로 지정합니다. 이 시간에 네트워크 쓰기를 수행할 수 없으면 작업이 다시 시도됩니다.

7 제외된 작성기의 설정을 수정하려면 해당 설정을 클릭한 후 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 71. 보호된 시스템의 제외된 작성기 설정

텍스트 상자	설명
제외된 작성기	제외하려는 작성기를 선택합니다. 목록에 나타나는 작성기는 구성 중인 시스템에 따라 다르기 때문에 목록에 모든 작성기가 표시되지는 않습니다. 예를 들어, 다음과 같은 작성기를 볼 수 있습니다. • ASR 작성기 • COM+ REGDB 작성기 • 성능 카운터 작성기 • 레지스트리 작성기 • 섀도 복사 최적화 작성기 • SQLServerWriter • 시스템 작성기 • 작업 스케줄러 작성기 • VSS 메타데이터 저장소 작성기 • WMI 작성기

8 보호된 시스템의 라이센스 세부 정보는 읽기 전용입니다. 라이센스 세부 정보는 다음 표에 설명되어 있습니다.

표 72. 보호된 시스템의 라이센스 세부 정보

텍스트 상자	설명
만료 날짜	선택한 보호된 시스템의 라이센스 만료 날짜를 나타냅니다.
라이센스 상태	선택한 보호된 시스템의 라이센스 현재 상태를 나타냅니다.
라이센스 유형	선택한 보호된 시스템의 라이센스 유형을 나타냅니다.
에이전트 유형	현재 보호된 시스템이 물리적 에이전트인지 가상 에이전트인지를 나타냅니다.

Hyper-V 호스트 또는 노드에 대한 설정 변경

이 절차는 Rapid Recovery Rapid Snap for Virtual(에이전트 없는 보호)를 사용하여 가상 시스템(VM)을 보호하는 Hyper-V 호스트 또는 노드에 적용됩니다.
Rapid Snap for Virtual(에이전트 없는 보호)를 사용하여 VM을 보호하는 Hyper-V 호스트는 호스트 아이콘의 왼쪽 탐색 영역에 나타납니다. 에이전트 없이 보호되는 VM이 있는 Hyper-V에 대한 설정은 일반적으로 보호되는 시스템과 같지 않습니다. 호스트에 대한 설정의 모든 변경 사항은 해당 호스트의 VM에 적용됩니다.

1 Core 콘솔의 왼쪽 탐색 영역에 있는 Protected Machines(보호되는 시스템) 아래에서 설정을 변경하고자 하는 Hyper-V 호스트를 클릭합니다.
호스트에 대한 **Summary(요약)** 페이지가 열립니다.
2 호스트에 대한 메뉴 표시줄에서 **Settings(설정)**를 클릭합니다.
Settings(설정) 페이지가 열립니다.
3 **General(일반)** 아래에서 변경하려는 설정을 클릭합니다.
선택한 설정이 텍스트 필드 또는 드롭다운 메뉴처럼 편집 가능하게 됩니다.
4 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 73. 일반 설정 정보

텍스트 상자	설명
표시 이름	Rapid Recovery Core 콘솔에서 보호되는 시스템에 대해 표시되는 이름입니다. 최대 64자를 입력할 수 있습니다. 기본적으로, 이 이름은 시스템의 호스트 이름입니다. 필요한 경우 사용하기 쉽게 이름을 변경할 수 있습니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
호스트 이름	시스템의 메타데이터에 나타나는 보호되는 시스템의 이름입니다. **노트: 이 설정은 변경하지 마십시오. 변경하면 보호되는 시스템과 Core 간의 연결이 끊어질 수 있습니다.**

5 **Transfer Queue(전송 큐)** 아래에서 한 번에 호스트에서 발생할 수 있는 전송 작업의 수를 변경하려면 **Maximum concurrent transfers(최대 동시 전송)**에 대한 설정을 클릭합니다.

노트: 최적의 성능을 위해 이 Hyper-V 호스트 또는 노드에 대한 최대 동시 전송을 기본 설정인 1로 설정하는 것이 좋습니다.

6 **Nightly Jobs(야간 작업)** 아래에서 사용 가능한 야간 작업에 대한 설정을 변경하려면 **Change(변경)**를 클릭합니다.
Nightly Jobs(야간 작업) 창이 나타납니다.
7 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 74. 야간 작업 설정 정보

텍스트 상자	설명
Clear orphaned registry keys on protected Hyper-V host(보호되는 Hyper-V 호스트에서 분리된 레지스트리 키 지우기)	데이터 전송 중에 가상 디스크를 연결하고 분리할 때 발생하는 불필요한 파일을 레지스트리에서에서 제거합니다.
Check integrity of recovery points(복구 지점의 무결성 검사)	Hyper-V 호스트에서 가상 시스템에 대해 생성된 각 복구 지점의 무결성 검사를 수행합니다.

8 **확인**을 클릭합니다.
9 **Auto Protection(자동 보호)** 아래에서 Hyper-V 호스트에 추가된 새 가상 시스템을 자동으로 보호할지 여부를 확인하려면 **Auto protect new virtual machines(새 가상 시스템 자동 보호)** 설정을 클릭합니다.

Hyper-V 보호된 가상 시스템에 대한 설정 변경
이 절차는 Rapid Recovery Rapid Snap for Virtual(에이전트 없는 보호)을 사용하여 보호되는 Hyper-V 가상 시스템(VM)에 적용됩니다.

Rapid Snap for Virtual(에이전트 없는 보호)이 보호하는 Hyper-V VM은 왼쪽 탐색 영역에 호스트 아이콘 으로 표시됩니다. Hyper-V 에이전트 없는 VM에 대한 설정은 **Settings** 페이지 하단의 Hyper-V 섹션을 제외하면 일반적인 보호된 시스템의 설정과 동일합니다. 다음 작업은 **Hyper-V** 섹션 설정에만 사용할 수 있는 지침을 제공합니다. 다른 모든 보호된 시스템 설정은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.

1 Core Console의 **보호된 시스템** 왼쪽 탐색 영역에서 설정을 변경하려는 Hyper-V VM을 클릭합니다.
VM의 **요약** 페이지가 표시됩니다.
2 호스트의 메뉴 표시줄에서 **설정**을 클릭합니다.
설정 페이지가 열립니다.
3 왼쪽의 목록에서 **Hyper-V**를 클릭합니다.
선택한 설정이 텍스트 필드 또는 드롭다운 메뉴로 표시되며, 편집 가능합니다.
4 **Hyper-V**에서 **스냅숏 구성**을 클릭합니다.
선택한 설정이 편집 가능한 드롭다운 메뉴로 표시됩니다.
5 드롭다운 메뉴에서 다음 표에 있는 옵션 중 하나를 선택합니다.

표 75. Hyper-V 설정 정보

텍스트 상자	설명
첫 번째 전송 중에 VSS 스냅숏을 생성하려 시도하고 실패하는 경우 검사점 생성	VSS 스냅샷이 성공하는 경우 복구 지점은 응용 프로그램에서 일관적인 상태가 됩니다. VSS 스냅샷이 실패하고 검사점이 생성된 경우 복구 지점은 계속 충돌됩니다.
전송 중에 VSS 스냅숏을 생성하지 마십시오.	계속 충돌하는 상태에서 복구 지점을 생성합니다.
전송 중에 VSS 스냅숏만 사용하십시오. VSS 스냅숏 생성이 실패하는 경우 전체 전송이 실패합니다.	응용 프로그램에서 일관적인 복구 지점만 생성하십시오. VSS 스냅샷숏이 실패하는 경우 보구 지점이 생성되지 않습니다.

VMware 보호된 가상 시스템의 vSphere 설정 변경
이 절차는 Rapid Recovery Rapid Snap for Virtual(에이전트 없는 보호)을 사용하여 보호되는 VMware ESXi 또는 Workstation 가상 시스템(VM)에 적용됩니다.
에이전트 없이 보호되는 VMware VM의 설정은 한 가지를 제외하면 일반적인 보호된 시스템에 사용하는 것과 설정이 동일합니다. **설정** 페이지의 **vSphere** 섹션에는 에이전트 없이 보호되는 VMware VM에만 적용되는 설정이 있습니다. 다음 작업은 **설정** 페이지의 **vSphere** 섹션에만 적용할 수 있는 지침을 제공합니다. 다른 모든 보호된 시스템 설정은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.

1 Core Console 왼쪽 탐색 영역의 보호된 시스템에서 설정을 변경하려는 Hyper-V 호스트를 클릭합니다.
호스트의 **요약** 페이지가 표시됩니다.
2 호스트의 메뉴 표시줄에서 **설정**을 클릭합니다.
설정 페이지가 열립니다.
3 왼쪽의 목록에서 **vSphere**를 클릭합니다.
선택한 설정이 텍스트 필드 또는 드롭다운 메뉴로 표시되며, 편집 가능합니다.
4 **vSphere**에서 변경하려는 설정을 클릭합니다.
선택한 설정이 텍스트 필드 또는 드롭다운 메뉴로 표시되며, 편집 가능합니다.
5 다음 표에 설명된 대로 구성 정보를 입력합니다.

표 76. vSphere 설정 정보

텍스트 상자	설명
Rapid Recovery를 허용하여 사용자가 생성한 VMware 삭제	기본 설정은 아니오입니다.
유효하지 않은 사용한 용량이 있는 볼륨 전송 허용	기본 설정은 예입니다.
정지된 스냅숏 허용	기본 설정은 예입니다.

전송 설정 수정 정보

Rapid Recovery에서 보호되는 시스템의 데이터 전송 프로세스를 관리하는 설정을 수정할 수 있습니다. 이 섹션에 설명된 전송 설정은 보호되는 시스템 수준의 설정입니다. Core 수준의 전송을 적용하려면 전송 대기열 설정 수정을(를) 참조하십시오.

Rapid Recovery는 정상 전송, 기본과 증분은 물론 복원, 미설치 복원 및 가상 시스템 내보내기의 경우 Windows 8 및 Windows Server 2012를 지원합니다.

Rapid Recovery에는 다음과 같은 세 가지 전송 유형이 있습니다.

- **스냅샷.** 보호되는 시스템의 데이터를 백업합니다. 모든 보호되는 데이터의 기본 이미지 및 마지막 스냅샷 이후에 업데이트된 데이터의 증분 스냅샷 등 두 가지 유형의 스냅샷이 가능합니다. 이런 유형의 전송은 Core와 연관된 리포지토리에 저장되는 복구 지점을 생성합니다. 자세한 내용은 스냅숏 및 복구 지점 관리을(를) 참조하십시오.
- **가상 시스템 내보내기**. 복구 지점에 보호되는 시스템의 백업에 있는 모든 데이터와 VM이 부팅 가능하도록 운영 체제와 드라이버 및 관련 데이터를 포함하는 가상 시스템(VM)을 생성합니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.
- **복원**. 보호되는 시스템으로 백업 정보를 복원합니다. 자세한 내용은 복구 지점에서 볼륨 복원을(를) 참조하십시오.

노트: 전체 볼륨은 항상 EFI 시스템 파티션을 사용하여 Windows 시스템을 복원하는 동안 다시 작성됩니다.

Rapid Recovery의 데이터 전송은 네트워크를 통해 보호되는 시스템에서 Core로 데이터 볼륨을 전송하는 작업이 포함됩니다. 또한 복제가 수행될 경우 소스 Core에서 대상 Core로 전송됩니다.

특정 성능 옵션 설정을 통해 시스템의 데이터 전송을 최적화할 수 있습니다. 이러한 설정은 보호되는 시스템 백업 수행, VM 내보내기, 복원을 수행하는 동안 데이터 대역폭 사용량을 제어합니다. 데이터 전송 성능에 영향을 주는 몇 가지 요소는 다음과 같습니다.

- 동시 에이전트 데이터 전송 수
- 동시 데이터 스트림 수
- 디스크의 데이터 변경량
- 사용 가능한 네트워크 대역폭
- 리포지토리 디스크 하위 시스템 성능
- 데이터 버퍼링에 사용 가능한 메모리 양

비즈니스 요건에 가장 적합하게 성능 옵션을 조정하고 환경에 따라 성능을 미세 조정할 수 있습니다. 자세한 내용은 전송 속도 제한을(를) 참조하십시오.

전송 속도 제한
보호된 시스템과 Core 간에 백업 데이터 또는 복제된 복구 지점을 네트워크를 통해 전송할 때 전송 속도를 의도적으로 줄일 수 있습니다. 이 프로세스를 제한이라고 합니다.

전송 속도를 제한하면 Rapid Recovery에서 파일 전송 전용인 네트워크 대역폭의 양을 제한합니다. 예를 들어 복제를 설정하는 경우, 제한 기능을 사용하면 이전 복구 지점을 복제된 Core로 전송할 때 네트워크 대역폭을 모두 사용할 가능성을 줄일 수 있습니다.

주의: 전송 속도 제한이 항상 필요하거나 권장되지는 않습니다. 이 정보는 Rapid Recovery 환경에서 성능 문제에 대한 가능한 해결책을 이해하는 데 도움이 됩니다. 예를 들어, 속도를 제한하면 반복된 전송 오류 및 보호되거나 복제된 Core의 상당히 많은 데이터를 전송하여 생긴 네트워크 속도 저하와 관련된 문제를 해결할 수 있는 경우가 있습니다.

최고의 속도 제한 방법을 결정하는 데 영향을 미치는 요소가 여러 가지 있습니다. 그중 보호되는 시스템의 유형은 핵심 요소입니다. 예를 들어, 사용 중인 Microsoft Exchange Server는 거의 사용하지 않는 레거시 웹 서버보다 변경률이 훨씬 높습니다.

보호된 시스템에 있는 저장소 볼륨의 입력 및 출력 기능도 효율성에 영향을 줄 수 있습니다.

네트워크의 속도 또한 중요한 요소 중 하나이며, 변수가 많습니다. 준비되어 있는 네트워크 백본(예: 1GbE과 10GbE), 아키텍처, 구성, NIC 티밍 내부 사용 및 사용된 케이블 유형은 모두 네트워크 전송 속도에 영향을 미칩니다. 저속 광역 통신망을 사용하고 있고 전송 작업이 백업 또는 복제에 실패한 경우 이러한 일부 설정을 사용하여 전송 속도를 제한하는 것을 고려하십시오.

궁극적으로 네트워크 제한 프로세스에는 시행착오가 동반됩니다. Dell은 전송 설정을 조정 및 테스트하고 이러한 설정을 주기적으로 다시 검토하여 현재 설정이 요구사항에 맞는지를 확인하는 것을 권장합니다.

전송 속도 조정은 개별 시스템 단위로 수행해야 합니다. Core Console에서 특정 시스템을 탐색하고 설정을 선택한 후 전송 속도를 조정합니다. 이러한 설정을 보고 변경하는 방법에 대한 자세한 내용은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오. 이 항목에서는 전송 제한에 사용되는 각 설정에 대해서도 설명합니다. 먼저 실험해야 하는 설정을 결정하는 데 유용한 설명이 있습니다.

전송 속도 제한과 관련된 기본 설정 네 가지는 다음 표에 설명되어 있습니다.

표 77. 전송 속도를 제한하는 데 사용되는 보호된 시스템 설정

시스템 수준 설정	기본 설정	제안된 제한 설정
최대 동시 스트림 수	8	4
최대 동시 쓰기 수	8	4
최대 세그먼트 크기	4194304	2097152
스트림당 대기 중인 읽기 수	0	24에서 시작

Dell은 Dell 지원 담당자가 지시한 경우가 아니라면 스트림당 대기 중인 읽기의 기본 설정을 변경하기 전에 다른 설정을 조정 및 테스트하는 것을 권장합니다. 이 설정을 조정 및 테스트할 경우 시작 값은 24입니다.

보호된 시스템 전송 매개 변수에 제한을 지정할 경우 이러한 제한 사항은 작업별로 적용됩니다. 전송 작업 2개가 동시에 발생하거나 겹치는 경우 대역폭이 2배 사용됩니다. 마찬가지로 네트워크에서 전송 작업 4개가 겹치는 경우 대역폭이 4배 사용됩니다.

보호되는 시스템에 대한 야간 작업 사용자 지정

해당 Configuration(구성) 탭에서 Core 수준 및 시스템 수준에서 야간 작업을 구성할 수 있습니다. 야간 작업을 Core 수준에서 설정하면 변경 사항이 해당 Core에 의해 보호되는 모든 관련 시스템에 적용됩니다. 시스템 수준에서 야간 작업의 변경 사항은 Core 수준의 지정된 시스템에만 적용됩니다.

설명과 각 야간 작업에 사용할 수 있는 범위를 포함하여 야간 작업의 목록을 보려면 야간 작업 이해을(를) 참조하십시오.

단일 보호되는 시스템에 대한 야간 작업을 변경하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core 콘솔의 Protected Machines(보호되는 시스템) 메뉴 아래에서 야간 작업을 사용자 지정하려는 시스템의 IP 주소 또는 시스템 이름을 클릭합니다.
선택한 시스템에 대한 **Summary(요약)** 페이지가 나타납니다.

2 **Settings(설정)** 메뉴를 클릭합니다.
선택한 시스템의 구성 설정을 보여 주는 **Settings(설정)** 페이지가 나타납니다.

3 선택적으로, Settings(설정) 페이지로 스크롤하여 야간 작업 설정을 보려면 **Nightly Jobs(야간 작업)** 링크를 클릭합니다.

4 Nightly Jobs(야간 작업) 제목 아래에서 **Change(변경)**을 클릭합니다.
Nightly Jobs(야간 작업) 대화 상자가 표시됩니다.

노트: 사용자 지정 보존 정책 설정을 포함하여 롤업 설정에 대한 정보는 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.

5 **Nightly Jobs(야간 작업)** 대화 상자에서 야간에 실행하기 위해 포함할 작업을 선택하거나 이 시스템에서 생략하려는 옵션을 선택 취소합니다.

노트: 옵션은 시스템마다 다를 수 있습니다. 예를 들어, Exchange Server를 사용하는 보호되는 시스템은 Exchange 데이터베이스의 체크섬 검사 및 Exchange 로그의 자르기를 포함할 수 있습니다.

6 **확인**을 클릭합니다.

노트: 이 절차의 결과는 선택한 보호되는 시스템에만 적용됩니다. 모든 곳에 적용하려면 사용자 지정하려는 각 시스템에 대해 위의 절차를 반복합니다. Core에 의해 보호되는 모든 시스템에 대한 야간 작업 설정을 변경하려면 Core에 대한 야간 작업 구성을(를) 참조하십시오.

보호된 시스템의 시스템 정보 보기

Rapid Recovery Core Console에서는 Core의 보호를 받는 시스템의 시스템 정보를 쉽게 확인할 수 있습니다.

General(일반) 창에는 Core 시스템과 환경에 대한 일반 정보가 포함되어 있습니다. **Volumes(볼륨)** 창에는 Core 시스템의 저장소 볼륨에 대한 정보가 나열됩니다. **Replay Engine Connections(Replay 엔진 연결)** 창에는 보호 중인 시스템의 전체 볼륨이 표시됩니다.

보호된 시스템의 상세한 시스템 정보를 보려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동하여 왼쪽 탐색 영역의 보호된 시스템 메뉴에서 보호된 시스템 이름을 클릭합니다.
해당 보호된 시스템에 대한 **요약** 페이지가 나타납니다.

2 **요약** 페이지에서 **요약** 창 아래쪽에 있는 **시스템 정보**를 클릭합니다.

3 **시스템 정보** 페이지에서는 선택한 보호된 시스템에 대한 세부 정보를 볼 수 있습니다.

- **시스템 정보:** 호스트 이름, OS 버전, OS 아키텍처, 메모리(물리적), 표시 이름, 정규화된 도메인 이름, 캐시 메타데이터 위치, 기본 캐시 위치, 보조 캐시 위치, 가상 시스템 유형(해당되는 경우)이 포함됩니다.
- **볼륨:** 볼륨 이름, 장치 ID, 파일 시스템, 포맷된 용량, 사용된 용량, 탑재 지점이 포함됩니다.
- **프로세서:** 아키텍처와 코어 수가 포함됩니다.
- **네트워크 어댑터:** 어댑터 유형과 속도가 포함됩니다.
- **IP 주소:** IP 주소와 패밀리가 포함됩니다.

시스템 관리

이 섹션에서는 시스템을 관리할 때 수행할 수 있는 다양한 작업에 대해 설명합니다. 이 섹션은 다음과 같은 항목으로 구성됩니다.

- 시스템 제거
- 보호에서 클러스터 제거
- 시스템에 대한 라이센스 정보 보기
- 보호된 시스템의 로그 파일 다운로드 및 보기
- 보호된 클러스터 노드를 보호된 시스템으로 변환

시스템 제거

Rapid Recovery Core의 보호에서 시스템을 제거할 때 지금까지 RR Core에 저장된 복구 지점을 유지하거나 복구 지점을 제거하는 두 가지 옵션을 사용할 수 있습니다. 복구 지점을 유지할 경우 "복구 지점만" 시스템으로 알려진 시스템만 사용하게 됩니다. 현재 보호에서 제거된 시스템에 대한 이러한 복구 지점을 사용하여 이후 시스템 복원을 계속할 수 있지만, 저장된 복구 지점에서 캡처된 상태까지만 복원할 수 있습니다.

복구 지점을 제거할 경우, 이 작업의 결과로 이전에 보호된 시스템에 대한 스냅숏 데이터가 Rapid Recovery Core에서 모두 삭제됩니다.

주의: 복구 지점을 삭제할 경우 더 이상 해당 시스템에 대한 데이터를 복원할 수 없습니다.

Rapid Recovery 환경의 보호에서 시스템을 제거하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 창에 표시된 Protected Machines(보호된 시스템) 아래에서 제거하려는 시스템을 클릭합니다.
2 관련 시스템에 대한 Summary(요약) 페이지에서 **Remove Machine(시스템 제거)**을 클릭합니다.
3 리포지토리에서도 이 시스템에 대한 모든 복구 지점을 삭제하려면 대화 상자에서 **Remove with recovery points(복구 지점과 함께 제거)**를 선택합니다.
4 시스템을 제거하려는 선택을 확인하기 위해 **Yes(예)**를 클릭합니다.
Rapid Recovery는 이 시스템을 보호 대상에서 제거하고, 이 시스템에 대한 모든 활성 작업을 취소합니다.

보호에서 클러스터 제거

보호에서 클러스터를 제거하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 보호된 시스템에서 제거하려는 클러스터를 클릭합니다.
2 클러스터에 대한 요약 페이지에서 **클러스터 제거**를 클릭합니다.
3 선택적으로, 대화 상자의 리포지토리에서 이 클러스터에 대해 현재 저장된 모든 복구 지점을 제거하려면 **복구 지점과 함께 제거**를 선택합니다.
4 대화 상자에서 **예**를 클릭하여 제거를 확인합니다.

보호에서 클러스터 노드 제거

보호에서 클러스터 노드를 제거하려면 다음 단계를 완료하십시오.

클러스터에서 노드를 제거하려는 경우 보호된 클러스터 노드를 보호된 시스템으로 변환을(를) 참조하십시오.

1 Rapid Recovery Core Console의 보호된 시스템에서 제거하려는 클러스터 노드를 클릭합니다.
2 노드에 대한 요약 페이지에서 **시스템 제거**를 클릭합니다.
노드 제거 대화 상자가 나타납니다.
3 선택적으로, 대화 상자의 리포지토리에서 이 클러스터에 대해 현재 저장된 모든 복구 지점을 제거하려면 **복구 지점과 함께 제거**를 선택합니다.
4 대화 상자에서 **예**를 클릭하여 제거를 확인합니다.

보호에서 클러스터의 모든 노드 제거

보호에서 클러스터의 모든 노드를 제거하려면 다음 단계를 완료하십시오.

△| 주의: **모든 클러스터 노드를 제거할 경우 클러스터도 제거됩니다.**

1 Rapid Recovery Core Console의 보호된 시스템에서 제거하려는 노드가 있는 클러스터를 클릭합니다.
2 클러스터에 대한 요약 페이지에서 **보호된 노드**를 클릭합니다.
3 보호된 노드 페이지에서 모든 노드를 선택합니다.
4 **시스템 제거** 드롭다운 메뉴를 클릭하고 다음 표에 설명된 옵션 중 하나를 선택합니다.

표 78. 노드 제거 옵션

옵션	설명
복구 지점 제거 및 유지	이 클러스터에 현재 저장된 모든 복구 지점을 유지합니다.
복구 지점 제거	이 클러스터에 대해 현재 저장된 모든 복구 지점을 리포지토리에서 제거합니다.

5 노드 삭제 대화 상자에서 **예**를 클릭하여 삭제를 확인합니다.

시스템에 대한 라이센스 정보 보기

보호된 시스템에 설치된 Rapid Recovery Agent 소프트웨어에 대한 현재 라이센스 상태 정보를 볼 수 있습니다.

1 Rapid Recovery Core Console에 있는 보호된 시스템에서 수정하려는 시스템을 클릭합니다.

시스템 선택에 대한 **요약** 페이지가 나타납니다.

2 **설정** 메뉴를 클릭합니다.
선택한 시스템에 대한 구성 설정을 표시하는 **설정** 페이지가 나타납니다.

3 **라이센싱** 링크를 클릭하고 설정 페이지에서 아래쪽으로 스크롤하여 시스템별 라이센싱 설정을 확인합니다.
상태 화면이 나타나고 제품 라이센스에 대한 세부 정보가 표시됩니다.

보호된 시스템의 로그 파일 다운로드 및 보기

보호된 시스템에서 오류 또는 문제가 발생할 경우 시스템 로그를 다운로드하여 오류 또는 문제를 확인하거나 Dell 서비스 담당자와 공유할 수 있습니다.

1 Core Console의 왼쪽 탐색 영역의 보호된 시스템 메뉴에서 관련 보호된 시스템에 대한 상황에 맞는 메뉴를 확장하려면 화살표를 클릭합니다. **추가**까지 아래로 스크롤하고 메뉴를 확장한 다음 **에이전트 로그**를 선택합니다.
에이전트 로그 다운로드 페이지가 나타납니다.

2 **에이전트 로그 다운로드** 페이지에서 **다운로드를 시작하려면 여기를 클릭하십시오**를 클릭합니다.

3 **AgentAppRecovery.log 열기** 대화 상자에서 다음 중 하나를 수행합니다.

- 로그 파일을 열려면 **연결 프로그램**을 선택하고 텍스트 기반 로그 파일을 볼 수 있는 응용 프로그램(예: 메모장)을 선택한 다음 마지막으로 **확인**을 클릭합니다.
  선택한 응용 프로그램에서 AgentAppRecovery.log 파일이 열립니다.
- 로컬에 파일을 저장하려면 **파일 저장**을 선택한 다음 **확인**을 클릭합니다.
  AgentAppRecovery.log 파일이 Downloads 폴더에 저장됩니다. 이 파일은 텍스트 편집기를 사용하여 열 수 있습니다.

관련 링크

Core 로그 파일 다운로드 및 보기

보호된 클러스터 노드를 보호된 시스템으로 변환

Rapid Recovery에서 보호된 클러스터 노드를 여전히 Core에서 관리하지만 더 이상 클러스터의 부분이 아닌 보호된 시스템으로 변환할 수 있습니다. 이것은 클러스터에서 클러스터 노드를 제거하지만, 클러스터 노드를 계속 보호해야 할 경우 유용합니다.

1 Rapid Recovery Core Console에서 변환할 시스템을 포함하는 클러스터로 이동한 다음 **보호된 노드**를 클릭합니다.

2 **보호된 노드** 페이지의 변환할 특정 노드에서 작업 드롭다운 메뉴를 클릭하고 **에이전트로 변환**을 선택합니다.

3 시스템을 클러스터에 다시 추가하려면 해당 시스템을 선택한 다음 요약 페이지의 작업 메뉴에서 **클러스터 노드로 변환**을 선택한 다음 **예**를 클릭하여 작업을 확인합니다.

사용자 지정 그룹 이해

Rapid Recovery Core Console은 왼쪽 탐색 영역에 보호된 시스템 메뉴를 표시합니다. 여기에는 Rapid Recovery Core에서 보호하기 위해 추가된 모든 시스템 또는 서버 클러스터가 포함되어 있습니다. 이 메뉴 아래에 Core의 해당 개체를 포함할지 여부에 따라 다른 메뉴가 나타날 수 있습니다. 같은 방식으로, 왼쪽 탐색 영역의 마지막 메뉴 유형으로 표시되는 사용자 지정 그룹을 생성할 수 있습니다.

사용자 지정 그룹의 주요 이점은 Core 개체를 논리적 컨테이너에 함께 그룹화할 수 있는 기능입니다. 이를 통해 특정 목적으로 Core 개체를 구성하고 관리할 수 있습니다(예: 조직, 비용 센터, 부서, 지역 등의 기준으로).

그룹을 생성하면 항상 하나의 그룹 구성원(예: 보호된 시스템 또는 서버 클러스터, 복제된 시스템, 또는 복구 지점 전용 시스템)이 새 사용자 지정 그룹에 추가됩니다. 추가된 개체는 그룹을 생성하는 원래 위치에 따라 결정됩니다. 그런 다음 일반적으로, 그룹에 구성원이 추가됩니다. 그 이후 그룹 작업 수행에 설명된 대로 해당 사용자 지정 그룹의 모든 구성원에 적용되는 그룹 작업을 수행할 수 있습니다.

사용자 지정 그룹은 보호된 시스템, 서버 클러스터, 복제된 시스템 및 복구 지점 전용 시스템을 포함할 수 있습니다. 서버 클러스터는 서버 클러스터와 서버 클러스터 노드가 단일 엔터티로 작동하는 점을 제외하고, 보호된 시스템과 동일하게 작동합니다. 서버 클러스터의 노드를 그룹에 추가하려고 하면 전체 클러스터가 추가됩니다.

사용자 지정 그룹에는 비슷하거나 다른 형식의 구성원이 포함될 수 있습니다. 비슷한 구성원 그룹의 경우 모든 그룹 작업이 그룹의 모든 구성원에 적용됩니다. 예를 들어, 보호된 시스템의 사용자 지정 그룹에 대한 스냅숏을 작성하면 각 시스템이 백업됩니다. 다른 형식의 구성원(예: 보호된 시스템과 복제된 시스템) 그룹의 경우 복제 실행과 같은 그룹 작업을 적용하면 복제된 시스템에만 적용됩니다.

하나 이상의 그룹을 만들 수 있습니다. 한 보호된 시스템 또는 복제된 시스템은 하나 이상의 그룹에 포함될 수 있습니다. 이러한 방식으로, Core의 시스템을 원하는 대로 그룹으로 나누고 해당 특정 그룹에 작업을 수행할 수 있습니다.

각 사용자 지정 그룹은 지정한 레이블로 왼쪽 탐색 영역에 표시됩니다. 표준 보호된 시스템이 있는 그룹이 사용자 지정 그룹의 맨 처음에 나타나고 복제된 시스템은 보호된 시스템 아래에 나타납니다. 복구 지점 전용 시스템이 있는 경우 복제된 시스템 아래에 나열됩니다.

왼쪽 탐색 영역에서 Core에서 보호된 개체는 자체 메뉴에 각각 나타납니다. 이러한 메뉴 중 사용자 지정 그룹이 마지막으로 나타납니다.

시스템을 그룹에 포함해도 원래 위치에서 제거되지 않습니다. 예를 들어, Agent1, Agent2, Agent3 등 보호된 시스템이 세 대 있고 Agent1을 CustomGroup1에 추가하는 경우 Agent1이 두 위치에 모두 표시됩니다.

자세한 내용은 다음 항목에서 확인하십시오.

- 사용자 지정 그룹 이름 수정
- 사용자 지정 그룹 제거
- 그룹 작업 수행
- 사용자 지정 그룹의 모든 시스템을 한 페이지에서 보기

사용자 지정 그룹 만들기

보호된 시스템 또는 복제된 시스템 메뉴에서 시스템 이름 위로 커서를 스크롤하면 드롭다운 메뉴를 여는 화살표가 표시됩니다. 이 메뉴에서 사용자 지정 레이블을 만들 수 있습니다.

사용자 지정 그룹을 만들려면 다음 절차를 수행하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 보호된 시스템, 복제된 시스템 또는 복구 지점 전용 시스템 메뉴에서 다음 작업을 수행합니다.

   a 메뉴의 시스템 이름 위에 커서를 놓습니다.

   b 해당 시스템의 드롭다운 메뉴를 클릭합니다.

   c 아래로 스크롤하여 **다음 이름으로 레이블 지정**을 선택한 후 **새 레이블**을 클릭합니다.

   레이블 생성 대화 상자가 나타납니다.

3 **이름** 필드에서 사용자 지정 그룹에 대한 적절한 레이블을 입력합니다.

   그룹의 목적을 잘 설명하는 이름을 사용합니다. 예를 들어, 부서별로 보호된 시스템과 복제된 시스템, 복구 지점 전용 시스템을 그룹화하려면 `Accounting Department`를 입력합니다. 나중에 그룹 이름을 바꿀 수 있습니다.

   노트: 레이블은 50자 이하여야 합니다. 단어 사이에 공백 하나를 포함할 수 있습니다. 사용자 지정 그룹에 대한 레이블을 제공해야 합니다.

4 레이블 이름에 만족하면 **확인**을 클릭합니다.

   대화 상자가 닫히고 왼쪽 탐색 영역에서 사용자 지정 그룹이 마지막 요소로 나타납니다.

5 선택적으로, 보호된 시스템이나 복제된 시스템, 복구 지점 전용 시스템을 이 그룹에 추가할 수 있습니다. 해당 메뉴의 시스템 이름으로 이동하여 드롭다운 메뉴를 클릭하고, 아래로 스크롤하여 **다음 이름으로 레이블 지정**을 선택한 후 사용자 지정 그룹의 이름을 클릭합니다.

   이제 이 그룹에 그룹 작업을 수행할 수 있습니다. 자세한 내용은 그룹 작업 수행을(를) 참조하십시오.

사용자 지정 그룹 이름 수정

사용자 지정 그룹의 이름을 수정하는 경우 레이블만 변경됩니다. 시스템 이름은 변경되지 않습니다.

사용자 지정 그룹 이름을 수정하려면 다음 절차를 수행하십시오.

1 Rapid Recovery Core Console로 이동합니다.
2 보호된 시스템 메뉴에서 수정하려는 사용자 지정 그룹 위로 커서를 스크롤합니다.
3 해당 그룹의 드롭다운 메뉴를 클릭한 후 **편집**을 클릭합니다.
사용자 지정 그룹 이름을 편집할 수 있는 **레이블 편집** 대화 상자가 나타납니다.
4 **이름** 필드에서 텍스트를 업데이트하거나 기존 레이블 텍스트를 삭제하고 새 레이블 또는 사용자 지정 그룹을 입력합니다.
그룹의 목적을 잘 설명하는 이름을 사용합니다. 예를 들어, 지역별로 보호된 시스템과 복제된 시스템, 복구 지점 전용 시스템을 그룹화하려면 `Tokyo`를 입력합니다. 나중에 그룹 이름을 바꿀 수 있습니다.

노트: 레이블은 50자 이하여야 합니다. 단어 사이에 공백 하나를 포함할 수 있습니다. 사용자 지정 그룹에 대한 레이블을 제공해야 합니다.

5 레이블 이름에 만족하면 **확인**을 클릭합니다.
대화 상자가 닫히고 수정된 사용자 지정 그룹이 왼쪽 탐색 영역의 마지막 요소로 나타납니다.
6 선택적으로, 보호된 시스템이나 복제된 시스템, 복구 지점 전용 시스템을 이 그룹에 추가할 수 있습니다. 해당 메뉴의 시스템 이름으로 이동하여 드롭다운 메뉴를 클릭하고, 아래로 스크롤하여 **다음 이름으로 레이블 지정**을 선택한 후 사용자 지정 그룹의 이름을 클릭합니다.

사용자 지정 그룹 제거

사용자 지정 그룹을 제거하면 해당 그룹이 보호된 시스템 메뉴에서 제거됩니다. 그룹에 있던 시스템는 제거되지 않으며 해당 표준 메뉴에서 계속 찾을 수 있습니다.

사용자 지정 그룹을 제거하려면 다음 절차를 수행하십시오.

1 Rapid Recovery Core Console로 이동합니다.
2 보호된 시스템 메뉴에서 제거하려는 사용자 지정 그룹 위로 커서를 스크롤합니다.
3 해당 그룹의 드롭다운 메뉴를 클릭한 후 **레이블 제거**를 클릭합니다.
그룹 제거 확인을 요청하는 메시지가 표시됩니다.
4 사용자 지정 그룹 제거를 확인합니다.
대화 상자가 닫히고 사용자 지정 그룹이 탐색 영역에서 제거됩니다.

그룹 작업 수행

Rapid Recovery Core Console의 왼쪽 탐색 영역에 표시되는 모든 그룹에서 그룹 작업을 수행할 수 있습니다. 그룹에 다른 형식의 구성원(예를 들어, 복제된 시스템 및 복구 지점만 있는 시스템)이 포함되어 있는 경우 관련 그룹 구성원에 대해서만 요청하는 작업이 수행됩니다.

사용자 지정 그룹에 대해 그룹 작업을 수행하려면 다음 절차를 수행하십시오.

1 Rapid Recovery Core Console로 이동합니다.
2 보호된 시스템 메뉴에서 그룹 작업을 수정하려는 사용자 지정 그룹 위로 커서를 스크롤합니다.
3 해당 그룹의 드롭다운 메뉴를 클릭한 후 다음과 같이 작업을 수행합니다.
- 그룹에서 모든 보호된 시스템의 기본 이미지를 적용하거나 증분 스냅숏을 강제로 수행하려면 **스냅숏 수행** 또는 **기본 이미지 적용**을 적절히 클릭합니다. 자세한 내용은 스냅숏 작성을 참조하십시오.
- 그룹에서 모든 보호된 시스템의 보호를 일시 중지하려면 **보호 일시 중지**를 클릭한 후 다시 시작 매개 변수를 지정합니다. 자세한 내용은 복제 일시 중지 및 다시 시작을 참조하십시오.
- 보호가 일시 중지된 그룹의 모든 보호된 시스템에 대한 보호를 다시 시작하려면 **보호 다시 시작**을 클릭한 후 다시 시작함을 확인합니다. 자세한 내용은 복제 일시 중지 및 다시 시작을 참조하십시오.
- 그룹에 있는 모든 개체에 대해 정보를 새로 고치려면 **메타데이터 새로 고침**을 클릭합니다.
- 이 그룹에 있는 모든 복제된 시스템의 복제를 일시 중지하려면 복제 아래에서 **일시 중지**를 클릭합니다. 자세한 내용은 복제 일시 중지 및 다시 시작을 참조하십시오.
- 복제가 일시 중지된 이 그룹의 모든 복제된 시스템에 대한 복제를 다시 시작하려면 복제 아래에서 **다시 시작**을 클릭합니다.
참고 항목: 복제 일시 중지 및 다시 시작

- 이 그룹에 있는 모든 복제된 시스템에 대한 복제를 강제로 수행하려면 복제 아래에서 **강제**를 클릭합니다. 자세한 내용은 복제 수행을 참조하십시오.
- 이 그룹에 있는 모든 복제된 시스템에 대한 복제를 제거하려면 복제 아래에서 **제거**를 클릭합니다. 자세한 내용은 대상 Core에서 들어오는 복제 제거를 참조하십시오.
- 이 Core에서 복구 지점만 있는 시스템을 제거하고 복구 지점을 무시하려면 복구 지점만 아래에서 **복구 지점 제거**를 클릭합니다.
- 사용자 지정 그룹의 경우 사용자 지정 그룹에 대한 레이블을 수정하려면 **편집**을 선택합니다. 자세한 내용은 사용자 지정 그룹 이름 수정을 참조하십시오.
- 사용자 지정 그룹에서만 사용자 지정 그룹을 제거하려면 **레이블 제거**를 선택합니다. 자세한 내용은 사용자 지정 그룹 제거를 참조하십시오.

사용자 지정 그룹의 모든 시스템을 한 페이지에서 보기

사용자 지정 그룹의 이름을 클릭하면 해당 사용자 지정 그룹의 모든 시스템이 나열된 시스템 페이지로 이동합니다. 그런 다음 작업 메뉴에서 모든 시스템에 대해 일부 기능을 수행하거나 각 시스템에서 명령을 선택하여 개별적으로 기능을 수행할 수 있습니다.

다중 시스템 보호 정보

Protect Multiple Machines Wizard(다중 시스템 보호 마법사)를 사용하여 Rapid Recovery Core에서 보호에 대해 두 대 이상의 Windows 시스템을 동시에 추가할 수 있습니다. Rapid Recovery를 사용하여 데이터를 보호하려면 Rapid Recovery Core Console에서 보호할 워크스테이션과 서버를 추가해야 합니다(예: Exchange Server, SQL Server, Linux 서버 등).

개별 시스템 보호와 마찬가지로, 다중 시스템을 동시에 보호하려면 보호할 각 시스템에 Rapid Recovery Agent 소프트웨어를 설치해야 합니다.

노트: 이 규칙에 대한 예외적인 경우로, VMware 또는 ESXi 호스트에서 가상 시스템을 보호할 때 에이전트 없는 보호를 사용할 수 있습니다. 에이전트 없는 보호에 대한 제한 사항을 포함하여 자세한 내용은 Rapid Snap for Virtual 이해을(를) 참조하십시오.

원격 설치가 가능한 보안 정책으로 보호된 시스템을 구성해야 합니다.

시스템에 연결하려면 시스템 전원을 켜고 시스템에 액세스가 가능해야 합니다.

Agent 소프트웨어를 다중 시스템에 동시에 배포하는 여러 가지 방법이 있습니다. 예:

- Deploy Agent Software Wizard(에이전트 소프트웨어 배포 마법사)를 사용하여 여러 시스템에 Rapid Recovery Agent 소프트웨어를 설치할 수 있습니다. 자세한 내용은 하나 이상의 시스템에 Rapid Recovery Agent 소프트웨어 배포을(를) 참조하십시오.
- Protect Multiple Machines Wizard(다중 시스템 보호 마법사)에서 Rapid Recovery Agent 소프트웨어를 배포할 수 있습니다.

다중 시스템을 보호하는 프로세스 중에는 고급 구성을 선택하는 경우 액세스할 수 있는 선택적 단계가 포함됩니다. 고급 옵션에는 리포지토리 기능 및 암호화가 포함됩니다. 예를 들어, 스냅숏을 저장할 기존 Rapid Recovery 리포지토리를 지정하거나 새 리포지토리를 만들 수 있습니다. 또한 보호할 시스템의 Core에 저장된 데이터에 적용할 기존 암호화 키를 지정하거나 새 암호화 키를 추가할 수 있습니다.

다중 시스템 보호 마법사의 워크플로는 환경에 따라 약간 다를 수 있습니다. 예를 들어, 보호하려는 시스템에 Rapid Recovery Agent 소프트웨어가 설치된 경우 마법사에서 해당 소프트웨어를 설치하라는 메시지가 표시되지 않습니다. 마찬가지로, Core에 이미 리포지토리가 존재하는 경우 리포지토리를 작성하라는 메시지는 표시되지 않습니다.

다중 시스템을 보호할 때 구성에 따라 적절한 절차를 따릅니다. 다중 시스템을 보호할 때 다음 옵션을(를) 참조하십시오.

- Active Directory 도메인에서 다중 시스템 보호
- VMware vCenter/ESX(i) 가상 호스트에서 여러 시스템 보호
- 수동으로 다중 시스템 보호

Active Directory 도메인에서 다중 시스템 보호

이 절차를 이용하여 Active Directory 도메인에서 하나 이상의 시스템을 동시에 보호합니다.

1 Rapid Recovery Core 콘솔에서 **Protect(보호)** 드롭다운 메뉴를 클릭한 다음 **Protect Multiple Machines(여러 시스템 보호)**를 클릭합니다.

Protect Multiple Machines(여러 시스템 보호) 마법사가 열립니다.

2 마법사의 **Welcome(시작)** 페이지에서 다음 옵션 중 하나를 선택합니다.

- 일반
- Advanced(고급)(옵션 단계 표시)

3 **다음**을 클릭합니다.

4 마법사의 **Connection(연결)** 페이지에 있는 **Source(소스)** 드롭다운 목록에서 **Active Directory**를 선택합니다.

5 다음 표에 설명된 대로 도메인 정보와 로그온 자격 증명을 입력합니다.

표 79. 도메인 정보 및 자격 증명

텍스트 상자	설명
호스트	Active Directory 도메인의 호스트 이름 또는 IP 주소입니다.
사용자 이름	도메인에 연결하는 데 사용되는 사용자 이름입니다. 예를 들어, 관리자 또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator)입니다.
암호	도메인에 연결하는 데 사용되는 보안 암호입니다.

6 **다음**을 클릭합니다.

7 마법사의 **Select Machines(시스템 선택)** 페이지에서 보호하려는 시스템을 선택합니다.

시스템이 자동으로 사용자가 선택한 각 시스템을 확인합니다.

8 **다음**을 클릭합니다.

Protect Multiple Machines(다중 시스템 보호) 마법사 옆에 **Protection(보호)** 페이지가 나타나는 경우 11단계로 건너뜁니다.

에이전트 소프트웨어가 아직 보호할 시스템에 배포되지 않았거나 사용자가 지정한 컴퓨터 중 하나라도 다른 이유로 보호할 수 없는 경우, 선택한 시스템이 경고 페이지에 나타납니다.

9 선택적으로 마법사의 **Warnings(경고)** 페이지에서 시스템을 선택한 다음 도구 모음에서 **Verify(확인)**을 클릭하면 시스템을 확인할 수 있습니다.

10 선택적으로, **Warnings(경고)** 페이지에서 **After Agent installation, restart the machines automatically(에이전트 설치 후 시스템을 자동으로 재시작)**를 선택합니다.

노트: 이 옵션을 사용하는 것이 좋습니다. 시스템을 보호하려면 에이전트 시스템을 재시작해야 합니다.

11 시스템에 연결할 수 있다는 상태가 표시되면 **Next(다음)**를 클릭하여 Rapid Recovery 에이전트 소프트웨어를 설치합니다.

Protection(보호) 페이지가 나타납니다.

12 마법사의 **Protection(보호)** 페이지에서 아래에 설명된 대로 적절한 보호 일정을 선택합니다.

- 기본 보호 일정을 사용하려면 Schedule Settings(일정 설정) 옵션에서 **Default protection (hourly snapshots of all volumes)(기본 보호(매시간 모든 볼륨의 스냅샷))**를 선택합니다.
- 다른 보호 일정을 정의하려면 Schedule Settings(일정 설정) 옵션에서 **Custom protection(사용자 지정 보호)**을 선택합니다.

13 다음과 같이 구성을 계속 진행합니다.

- Protect Machine Wizard(시스템 보호 마법사)에 대해 Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 **Finish(마침)**를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.

  시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(즉, 보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Rapid Recovery Core의 리포지토리에 전송됩니다.
- Protect Machine Wizard(시스템 보호 마법사)에서 Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭합니다(사용자 지정 보호 일정 만들기 참조).
- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 15단계를 계속 진행하여 리포지토리 및 암호화 옵션을 확인합니다.

- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

14 **다음**을 클릭합니다.

15 마법사의 **Repository(리포지토리)** 페이지에서 다음 중 하나를 수행합니다.

- 리포지토리가 이미 있고 보호를 위해 기존 리포지토리에 이 시스템의 데이터를 저장하려는 경우 다음을 수행합니다:
  1 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
  2 목록에서 기존 리포지토리를 선택합니다.
  3 **다음**을 클릭합니다.

  Encryption(암호화) 페이지가 나타납니다. 선택적으로 암호화를 정의하려면 19단계로 건너뜁니다.
- 리포지토리를 생성하려는 경우 **Create a Repository(리포지토리 생성)**를 선택한 후 다음 단계를 완료합니다.
  1 **Repository(리포지토리)** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 80. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 첫 번째 리포지토리인 경우 기본 이름은 리포지토리 1입니다. 필요하면 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자를 포함해야 합니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본적으로 값은 64입니다.
설명	선택적으로 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

  2 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

> **주의: 리포지토리의 저장소 위치는 루트 내에 전용 폴더로 정의합니다. 루트 위치는 지정하지 마십시오. 예를 들어, E:\가 아닌 E:\Repository\를 사용합니다. 이 단계에서 생성하는 리포지토리를 나중에 제거하는 경우 해당 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 루트에 저장소 위치를 정의하는 경우 볼륨(예: E:\)에 있는 다른 모든 파일이 삭제되어 이는 치명적인 데이터 손실을 초래할 수 있습니다.**

  Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

  3 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

  4 **Storage Location(저장소 위치)** 영역에 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨을 추가할 수 있습니다(예: 직접 연결된 저장소, 저장소 영역 네트워크 또는 네트워크에 연결된 저장소). 일반 인터넷 파일 시스템(CIFS) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.

- **Add file on local disk(로컬 디스크에 파일 추가)**를 선택하여 로컬 시스템을 지정하고 아래 표에 설명된 대로 정보를 입력합니다.

표 81. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Data`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다.

텍스트 상자	설명
	예를 들어, `X:\Repository\Metadata`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 또는 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 선택하여 네트워크 공유 위치를 지정한 후 아래 표에 설명된 대로 정보를 입력합니다.

표 82. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.

5 **Storage Configuration(저장소 구성)** 영역에서 **More Details(상세 정보)**를 클릭하고 아래 표에 설명된 대로 저장소 위치에 대한 상세 정보를 입력합니다.

표 83. 저장소 구성 상세 정보

텍스트 상자	설명
크기	저장소 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB이고 기본값은 250GB입니다. 다음 중에서 선택할 수 있습니다. • GB • TB **노트: 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2을 사용하는 NTFS 볼륨인 경우 파일 크기 한도는 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows 캐시 관리자가 사용되는 방법을 제어하고 다른 구성에 대해 성능을 최적화할 수 있도록 리포지토리를 조정하는 데 도움을 줍니다. 값을 다음 중 하나로 설정합니다. • 켜짐 • 꺼짐 • 동기화 기본값인 On(켜짐)으로 설정하는 경우 Windows에서 캐싱을 제어합니다. 이는 Windows 10 및 Windows Server 2012 이상 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 Off(꺼짐)입니다.** Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다.

텍스트 상자	설명
	Sync(동기화)로 설정하면 Windows에서 캐싱과 동기식 입력/출력을 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 **다음**을 클릭합니다.

1단계에서 **Advanced(고급)** 옵션을 선택한 경우 **Encryption(암호화)** 페이지가 나타납니다.

16 선택적으로 마법사의 **Encryption(암호화)** 페이지에서 암호화를 활성화하려면 **Enable Encryption(암호화 사용)**을 선택합니다.
Encryption(암호화) 페이지에 Encryption key(암호화 키) 필드가 나타납니다.

노트: 암호화를 활성화하면 이 시스템의 모든 보호되는 볼륨에 있는 데이터에 적용됩니다. Rapid Recovery Core 콘솔의 Encryption Keys(암호화 키) 페이지에서 나중에 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 암호화 키 이해 항목을 참조하십시오.

주의: Rapid Recovery에서는 CBC(Cipher Block Chaining) 모드에서 256바이트 키와 함께 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 암호화 키를 설정하고 정의하는 암호를 보호할 것을 권장합니다. 암호는 데이터 복구에 매우 중요하므로 안전한 위치에 저장해 두십시오. 암호가 없으면 데이터를 복구할 수 없습니다.

17 이 Rapid Recovery Core에 이미 정의된 암호화 키를 사용하여 이 보호되는 시스템을 암호화하려면 **Encrypt data using an existing Encryption key(기존 암호화 키를 사용하여 데이터 암호화)**를 선택한 다음 드롭다운 메뉴에서 적절한 키를 선택합니다.
19단계로 진행합니다.

18 Core에 새 암호화 키를 추가하고 해당 키를 이 보호되는 시스템에 적용하려는 경우 다음 표에 설명된 대로 정보를 입력합니다.

표 84. 암호화 키 설정

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~130자 사이의 영숫자를 포함해야 합니다. 백슬래시, 사선, 파이프, 콜론, 별표, 따옴표, 물음표, 여는 대괄호나 닫는 대괄호, 앰퍼샌드 또는 해시 같은 특수 문자를 포함할 수 없습니다.
설명	암호화 키의 설명을 입력합니다. 이 정보는 Core 콘솔에서 암호화 키를 볼 때 Description(설명) 필드에 나타납니다.
암호	액세스 제어에 사용되는 암호를 입력합니다. 모범 사례는 위에 나열된 특수 문자의 사용을 피하기 위한 것입니다. 안전한 장소에 암호를 적어 두십시오. Dell 지원에서 암호를 복구할 수 없습니다. 암호화 키를 생성하고 이를 하나 이상의 보호되는 시스템에 적용한 후에는 암호를 분실할 경우 데이터를 복구할 수 없습니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

19 **Finish(마침)**를 클릭하여 저장하고 설정을 적용합니다.
마법사가 닫힙니다.

20 **Warning(경고)** 페이지가 나타났고 여전히 선택한 항목에 만족하는 경우 다시 **Finish(마침)**를 클릭합니다.

필요한 경우 Rapid Recovery 에이전트 소프트웨어가 지정된 시스템에 배포되며 시스템이 Core의 보호에 추가됩니다.

VMware vCenter/ESX(i) 가상 호스트에서 여러 시스템 보호

VMware vCenter/ESX(i) 가상 호스트에서 하나 이상의 시스템을 동시에 보호하려면 이 절차를 사용합니다.

△ 주의: **에이전트 없는 보호를 사용하는 경우 VM을 한 번에 200개 이상 보호하지 않도록 제한하는 것이 좋습니다. 예를 들어, Protect Multiple Machines Wizard(여러 시스템 보호 마법사)를 사용할 때 VM을 200개 이상 선택하지 마십시오. VM을 200개 이상 보호하면 성능이 저하됩니다. Core가 시간에 따라 에이전트 없이 보호할 수 있는 VM 수에는 제한이 없습니다. 예를 들어, 오늘 VM을 200개 보호하고 내일 다른 VM을 200개 보호할 수 있습니다.**

1 Rapid Recovery Core 콘솔에서 **Protect(보호)** 드롭다운 메뉴를 클릭한 다음 **Protect Multiple Machines(여러 시스템 보호)**를 클릭합니다.

Protect Multiple Machines(여러 시스템 보호) 마법사가 열립니다.

2 Welcome(시작) 페이지에서 다음 옵션 중 하나를 선택합니다.

- 일반
- Advanced(고급)(옵션 단계 표시)

3 **다음**을 클릭합니다.

4 마법사의 Connection(연결) 페이지의 **Source(소스)** 드롭다운 목록에서 **vvCenter / ESX(i)**를 선택합니다.

5 다음 표에 설명된 대로 호스트 정보와 로그온 자격 증명을 입력합니다.

표 85. vCenter/ESX(i) 연결 설정

텍스트 상자	설명
호스트	VMware vCenter Server/ESX(i) 가상 호스트의 이름이나 IP 주소.
포트	가상 호스트에 연결하는 데 사용되는 포트입니다. 기본 설정은 443입니다.
사용자 이름	가상 호스트에 연결하는 데 사용되는 사용자 이름입니다. 예를 들어, 관리자 또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator입니다.
암호	이 가상 호스트에 연결하는 데 사용할 안전한 암호입니다.

- 에이전트 없는 보호를 사용하려면 **Protect selected VMs Agentlessly(선택한 VM을 에이전트 없이 보호)**를 선택한 다음 Rapid Recovery 에이전트 없이 vCenter/ESXi가상 시스템 보호을(를) 참조하십시오.

6 Select Machines(시스템 선택) 페이지의 드롭다운 메뉴에서 다음 옵션 중 하나를 선택합니다.

- 호스트 및 클러스터
- VM 및 템플릿

7 시스템의 목록을 확장하고 보호할 VM을 선택합니다.

Rapid Recovery가 시스템이 오프라인이거나 VMware 도구가 설치되지 않았음을 감지하는 경우 알림이 나타납니다.

8 **다음**을 클릭합니다.

9 Adjustments(조정) 페이지에서 `hostname::username::password`의 형식으로 각 시스템의 자격 증명을 입력합니다.

ⓘ 노트: **각 줄에 시스템 1개를 입력합니다.**

10 **다음**을 클릭합니다.

Protect Multiple Machines (여러 시스템 보호) 옆에 Protection(보호) 페이지가 나타나는 경우 14단계로 건너뜁니다.

에이전트 소프트웨어가 아직 보호할 시스템에 배포되지 않았거나 사용자가 지정한 컴퓨터 중 하나라도 다른 이유로 보호할 수 없는 경우, 선택한 시스템이 경고 페이지에 나타납니다.

11 선택적으로, 경고 페이지에서 시스템을 선택하고 도구 모음에서 **Verify(확인)**를 클릭하여 시스템을 확인할 수 있습니다.

12 선택적으로, 경고 페이지에서 **After Agent installation, restart the machines automatically(에이전트 설치 후 시스템을 자동으로 재시작)**를 선택합니다.

ⓘ 노트: **이 옵션을 사용하는 것이 좋습니다. 시스템을 보호하려면 에이전트 시스템을 재시작해야 합니다.**

13 상태가 시스템이 연결할 수 있음을 나타내는 경우 **Next (다음)**를 클릭하여 에이전트 소프트웨어를 설치합니다.

Protection(보호) 페이지가 나타납니다.

14 Protection(보호) 페이지에서 아래에 설명된 대로 적절한 보호 일정을 선택합니다.

- 기본 보호 일정을 사용하려면 Schedule Settings(일정 설정) 옵션에서 **Default protection (hourly snapshots of all volumes)(기본 보호(매시간 모든 볼륨의 스냅샷))**를 선택합니다.

- 다른 보호 일정을 정의하려면 Schedule Settings(일정 설정) 옵션에서 **Custom protection(사용자 지정 보호)**을 선택합니다.

15 다음과 같이 구성을 계속 진행합니다.

- Protect Machine Wizard(시스템 보호 마법사)에서 Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 **Finish(마침)**를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.

  시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Rapid Recovery Core의 리포지토리에 전송됩니다.
- Protect Machine Wizard(시스템 보호 마법사)에서 Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.
- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 17단계를 계속 진행하여 리포지토리 및 암호화 옵션을 확인합니다.
- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

16 **다음**을 클릭합니다.

17 **Repository(리포지토리)** 페이지에서 다음 중 하나를 수행합니다.

- 리포지토리가 이미 있고 보호를 위해 기존 리포지토리에 이 시스템의 데이터를 저장하려는 경우 다음을 수행합니다:
  1 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
  2 목록에서 기존 리포지토리를 선택합니다.
  3 **다음**을 클릭합니다.

  Encryption(암호화) 페이지가 나타납니다. 선택적으로 암호화를 정의하려면 18단계로 건너뜁니다.
- 리포지토리를 생성하려는 경우 **Create a Repository(리포지토리 생성)**을 선택한 후 다음 단계를 완료합니다.
  1 **Repository(리포지토리)** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 86. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 첫 번째 리포지토리인 경우 기본 이름은 리포지토리 1입니다. 필요하면 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자를 포함해야 합니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본적으로 값은 64입니다.
설명	선택적으로 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

  2 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

> △ 주의: **리포지토리의 저장소 위치는 루트 내에 전용 폴더로 정의합니다. 루트 위치는 지정하지 마십시오. 예를 들어, E:\가 아닌 E:\Repository\를 사용합니다. 이 단계에서 생성하는 리포지토리를 나중에 제거하는 경우 해당 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 루트에 저장소 위치를 정의하는 경우 볼륨(예: E:\)에 있는 다른 모든 파일이 삭제되어 이는 치명적인 데이터 손실을 초래할 수 있습니다.**

  Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

  3 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

  4 **Storage Location(저장소 위치)** 영역에 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨을 추가할 수 있습니다(예: 직접 연결된 저장소, 저장소 영역 네트워크 또는 네트워크에 연결된 저장소). 일반 인터넷 파일 시스템(CIFS) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.
     - **Add file on local disk(로컬 디스크에 파일 추가)**를 선택하여 로컬 시스템을 지정하고 아래 표에 설명된 대로 정보를 입력합니다.

표 87. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Data`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Metadata`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 또는 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 선택하여 네트워크 공유 위치를 지정한 후 아래 표에 설명된 대로 정보를 입력합니다.

표 88. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.

5 **Storage Configuration(저장소 구성)** 영역에서 **More Details(상세 정보)**를 클릭하고 아래 표에 설명된 대로 저장소 위치에 대한 상세 정보를 입력합니다.

표 89. 저장소 구성 상세정보

텍스트 상자	설명
크기	저장소 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB이고 기본값은 250GB입니다. 다음 중에서 선택할 수 있습니다. • GB • TB **노트: 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2을 사용하는 NTFS 볼륨인 경우 파일 크기 한도는 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows 캐시 관리자가 사용되는 방법을 제어하고 다른 구성에 대해 성능을 최적화할 수 있도록 리포지토리를 조정하는 데 도움을 줍니다.

텍스트 상자	설명
	값을 다음 중 하나로 설정합니다. · 켜짐 · 꺼짐 · 동기화 기본값인 On(켜짐)으로 설정하는 경우 Windows에서 캐싱을 제어합니다. 이는 Windows 10 및 Windows Server 2012 이상 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 Off(꺼짐)입니다.** Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. Sync(동기화)로 설정하면 Windows에서 캐싱과 동기식 입력/출력을 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 **다음**을 클릭합니다.

1단계에서 **Advanced(고급)** 옵션을 선택한 경우 **Encryption(암호화)** 페이지가 나타납니다.

18 선택적으로 Encryption(암호화) 페이지에서 암호화를 활성화하려면 **Enable Encryption(암호화 활성화)**을 선택합니다.
Encryption(암호화) 페이지에 Encryption key(암호화 키) 필드가 나타납니다.

노트: 암호화를 활성화하면 이 에이전트 시스템에 모든 보호되는 볼륨에 있는 데이터에 적용됩니다. Rapid Recovery Core 콘솔의 Configuration(구성) 탭에서 나중에 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 암호화 키 이해을(를) 참조하십시오.

주의: Rapid Recovery에서는 CBC(Cipher Block Chaining) 모드에서 256바이트 키와 함께 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 암호화 키를 설정하고 정의하는 암호를 보호할 것을 권장합니다. 암호는 데이터 복구에 매우 중요하므로 안전한 위치에 저장해 두십시오. 암호가 없으면 데이터를 복구할 수 없습니다.

19 이 Rapid Recovery Core에 이미 정의된 암호화 키를 사용하여 이 보호되는 시스템을 암호화하려면 **Encrypt data using an existing Encryption key(기존 암호화 키를 사용하여 데이터 암호화)**를 선택한 다음 드롭다운 메뉴에서 적절한 키를 선택합니다.
21단계로 진행합니다.

20 Core에 새 암호화 키를 추가하고 해당 키를 이 보호되는 시스템에 적용하려는 경우 다음 표에 설명된 대로 정보를 입력합니다.

표 90. 암호화 키 설정

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~130자 사이의 영숫자를 포함해야 합니다. 백슬래시, 사선, 파이프, 콜론, 별표, 따옴표, 물음표, 여는 대괄호나 닫는 대괄호, 앰퍼샌드 또는 해시 같은 특수 문자를 포함할 수 없습니다.
설명	암호화 키의 설명을 입력합니다. 이 정보는 Core 콘솔에서 암호화 키를 볼 때 Description(설명) 필드에 나타납니다.
암호	액세스 제어에 사용되는 암호를 입력합니다. 모범 사례는 위에 나열된 특수 문자의 사용을 피하기 위한 것입니다. 안전한 장소에 암호를 적어 두십시오. Dell 지원에서 암호를 복구할 수 없습니다. 암호화 키를 생성하고 이를 하나 이상의 보호되는 시스템에 적용한 후에는 암호를 분실할 경우 데이터를 복구할 수 없습니다.

텍스트 상자	설명
암호 확인	방금 입력한 암호를 다시 입력합니다.

21 **Finish(마침)**를 클릭하여 저장하고 설정을 적용합니다.

22 경고 페이지가 나타났고 여전히 선택한 항목에 만족하는 경우 다시 **Finish(마침)**를 클릭합니다.

필요한 경우 Rapid Recovery 에이전트 소프트웨어가 지정된 시스템에 배포되며 시스템이 Core의 보호에 추가됩니다.

수동으로 다중 시스템 보호

이 절차에 따라 보호할 각 시스템을 수동으로 입력합니다. 예를 들어 Linux 시스템 보호 시 사용합니다.

1 Rapid Recovery Core Console에서 **보호** 드롭다운 메뉴를 클릭한 다음 **다중 시스템 보호**를 클릭합니다.
다중 시스템 보호 마법사가 열립니다.

2 **시작** 페이지에서 다음 옵션 중 하나를 선택합니다.
- 일반
- 고급(선택 사항 단계 표시)

3 **다음**을 클릭합니다.

4 마법사의 **연결** 페이지에서 **소스** 드롭다운 목록의 **수동으로**를 선택합니다.

5 **다음**을 클릭합니다.

6 **시스템 선택** 페이지에서 대화 상자에 시스템 세부 정보를 `hostname::username::password::port` 형식으로 입력합니다. 포트 설정은 선택 사항입니다. 예:

```
10.255.255.255::administrator::&11@yYz90z::8006

abc-host-00-1::administrator::99!zU$o83r::168
```

7 **다음**을 클릭합니다.
그럼 다음, 다중 시스템 보호 마법사에 **보호** 페이지가 나타나면 11단계로 건너뜁니다.
Agent 소프트웨어가 아직 보호하려는 시스템에 배포되지 않았거나 지정한 시스템을 다른 이유로 보호할 수 없으면 선택한 시스템이 **경고** 페이지에 나타납니다.

8 (선택 사항) **시스템 경고** 페이지에서 시스템을 선택한 후 도구 모음에서 **확인**을 클릭하여 시스템을 확인할 수 있습니다.

9 (선택 사항) **시스템 경고** 페이지에서 **에이전트 설치 후 자동으로 시스템 재시작**을 선택합니다.

> **노트: Dell에서는 이 옵션을 권장합니다. 에이전트 시스템을 보호하려면 먼저 재시작해야 합니다. 재시작하면 에이전트 서비스가 실행 중이며 관련된 경우, 해당 시스템을 보호하는 데 적절한 커널 모듈이 사용됩니다.**

10 시스템이 접속할 수 있는 상태로 나타나면 **다음**을 클릭하여 Agent 소프트웨어를 설치합니다.
보호 페이지가 나타납니다.

11 **보호** 페이지에서 아래 설명된 대로 적합한 보호 일정을 선택합니다.
- 기본 보호 일정을 사용하려면 일정 설정 옵션에서 **기본 보호(모든 볼륨의 시간별 스냅숏)**를 선택합니다.
- 다른 보호 일정을 정의하려면 일정 설정 옵션에서 **사용자 지정 보호**를 선택합니다.

12 다음과 같이 구성을 계속합니다.
- 시스템 보호 마법사에서 일반 구성을 선택하고 기본 보호를 지정한 경우 **마침**을 클릭하여 선택 사항을 확인하고 마법사를 닫고 지정한 시스템을 보호합니다.
  시스템에 보호를 처음 추가하면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(보호되는 볼륨에 있는 모든 데이터의 스냅숏)가 Rapid Recovery Core의 리포지토리에 전송됩니다.
- 시스템 보호 마법사에서 일반 구성을 선택하고 사용자 지정 보호를 지정한 경우 **다음**을 클릭하여 사용자 지정 보호 일정 만들기를 확인합니다.
- 시스템 보호 마법사에서 고급 구성을 선택하고 기본 보호를 지정한 경우 리포지토리 및 암호화 옵션을 확인하려면 **다음**을 클릭하여 14단계로 이동합니다.
- 시스템 보호 마법사에서 고급 구성을 선택하고 사용자 지정 보호를 지정한 경우**다음**을 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정 정의에 대한 자세한 내용은 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

13 **리포지토리** 페이지에서 다음 중 하나를 수행합니다.
- 이미 리포지토리가 있고 보호할 이 시스템의 데이터를 기존 리포지토리에 저장하려는 경우 다음을 수행합니다.

1 **기존 리포지토리 사용**을 선택합니다.
2 목록에서 기존 리포지토리를 선택합니다.
3 **다음**을 클릭합니다.

Encryption(암호화) 페이지가 나타납니다. 선택적으로 암호화를 정의하려면 19단계로 건너뜁니다.

- 리포지토리를 생성할 경우 **리포지토리 생성**을 선택한 후 다음 단계를 완료하십시오.

1 다음 표에 설명된 대로 **리포지토리**에서 정보를 입력합니다.

표 91. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로, 이 텍스트 상자는 Repository라는 단어와 번호로 구성되며 이 Core의 리포지토리 번호에 해당합니다. 예를 들어, 첫 번째 리포지토리의 기본 이름은 Repository 1입니다. 필요에 따라 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자가 포함되어야 합니다. 금지된 문자 또는 금지된 구 문자는 사용하지 마십시오.
동시 작업	리포지토리에서 지원하려는 동시 요청의 수를 정의합니다. 기본값은 64입니다.
설명	(선택 사항) 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

2 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의하려면 **저장소 위치 추가**를 클릭합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

> △ 주의: **리포지토리의 저장소 위치에 대한 루트 내에 전용 폴더를 정의합니다. 루트 위치를 지정하지 마십시오. 예를 들어, E:\가 아니라 E:\Repository\를 사용하십시오. 이 단계에서 만드는 리포지토리를 나중에 제거하는 경우, 리포지토리의 저장소 위치에 있는 파일이 모두 삭제됩니다. 루트 위치에 저장소 위치를 정의하면 볼륨(예: E:\) 내부의 다른 모든 파일이 삭제되어 치명적인 데이터 손실이 발생할 수 있습니다.**

Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

3 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의하려면 **저장소 위치 추가**를 클릭합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

4 **저장소 위치** 영역에서 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨(예: 직접 연결 저장소, 저장소 영역 네트워크 또는 네트워크 연결 저장소 등) 추가를 선택할 수 있습니다. CIFS(Common Internet File System) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.

- **로컬 디스크에 파일 추가**를 선택하여 로컬 시스템을 지정한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 92. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어 `X:\Repository\Data`라고 입력합니다. 경로를 지정할 경우에는 영문자, 하이픈, 마침표만 사용하십시오(개별 호스트 이름과 도메인만 해당). 백슬래시 문자는 경로의 레벨을 정의하는 용도로만 사용할 수 있습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어 `X:\Repository\Metadata`라고 입력합니다. 경로를 지정할 경우에는 영문자, 하이픈, 마침표만 사용하십시오(개별 호스트 이름과 도메인만 해당). 백슬래시 문자는 경로의 레벨을 정의하는 용도로만 사용할 수 있습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.

- 또는 **CIFS 공유에 파일 추가**를 선택하여 네트워크 공유 위치를 지정한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 93. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 경우에는 영문자, 하이픈, 마침표만 사용하십시오(개별 호스트 이름과 도메인만 해당). 문자 a - z는 대소문자를 구분하지 않습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스하기 위한 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스하기 위한 암호를 지정합니다.

5 **저장소 구성** 영역에서 **추가 정보**를 클릭하고 다음 표에 설명된 대로 저장소 위치에 대한 세부 정보를 입력합니다.

표 94. 저장소 구성 세부 정보

텍스트 상자	설명
크기	저장 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB입니다. 기본값은 250GB입니다. 다음 항목 중에서 선택할 수 있습니다. • GB • TB **노트: 볼륨 크기를 초과하는 크기를 지정할 수 없습니다.** 저장 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨인 경우 파일 크기 제한은 16TB입니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2를 사용하는 NTFS 볼륨일 경우 파일 크기는 256TB로 제한됩니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows Cache Manager가 사용되는 방식을 제어하며 여러 구성에서 최적의 성능을 발휘할 수 있도록 리포지토리를 조정하는 데 도움이 됩니다. 값을 다음 중 하나로 설정합니다. • 설정 • 해제 • 동기화 설정(기본값)으로 지정하면 Windows가 캐싱을 제어합니다. Windows 10 및 Windows Server 2012 이상 버전에 적합합니다. **노트: 쓰기 캐싱 정책을 설정으로 지정하면 성능이 더 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우, Off(꺼짐)로 설정하는 것이 좋습니다.** Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. 동기화로 설정하면 Windows가 동기화 입력/출력뿐만 아니라 캐싱도 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 **다음**을 클릭합니다.

1단계에서 **고급** 옵션을 선택한 경우 **암호화** 페이지가 나타납니다.

14 (선택 사항) **암호화** 페이지에서, 암호화를 사용하려면 **암호화 사용**을 선택합니다.

암호화 페이지에 암호화 키 필드가 나타납니다.

노트: 암호화를 사용하면 이 시스템에 대한 모든 보호된 볼륨의 데이터에 암호화가 적용됩니다. 나중에 Rapid Recovery Core Console의 암호화 키 페이지에서 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 암호화 키 이해 항목을 참조하십시오.

주의: Rapid Recovery에서는 256비트 키가 있는 CBC(Cipher Block Chaining) 모드에서 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 Dell에서는 암호화 키를 설정하고 정의한 암호를 보호할 것을 적극적으로 권장합니다. 암호는 데이터 복구에 필수적이므로 안전한 장소에 보관해야 합니다. 암호가 없으면 데이터 복구가 불가능합니다.

15 Rapid Recovery Core에 이미 정의된 암호화 키를 사용하여 보호된 시스템을 암호화하려면 **기존 암호화 키를 사용하여 데이터 암호화**를 선택하고 드롭다운 메뉴에서 적절한 키를 선택합니다.

17단계를 진행합니다.

16 새 암호화 키를 Core에 추가하고 해당 키를 보호된 시스템에 적용하려면 다음 표에 설명된 대로 정보를 입력합니다.

표 95. 암호화 키 설정

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~130개의 영숫자를 포함해야 합니다. 백슬래시, 슬래시, 파이프, 콜론, 별표, 따옴표, 물음표, 여는 괄호, 닫는 괄호, 앰퍼샌드, 해시 등 특수 문자는 포함할 수 없습니다.
설명	암호화 키에 대한 설명을 입력합니다. 이 정보는 Core Console에서 암호화 키를 볼 때 설명 필드에 표시됩니다.
암호	액세스를 제어하기 위해 사용되는 암호를 입력합니다. 가능하면 위에 나열된 특수 문자를 사용하지 않는 것이 가장 좋습니다. 암호를 안전한 곳에 적어둡니다. Dell 지원팀에서는 암호를 복구할 수 없습니다. 암호화 키를 만들어 하나 이상의 보호된 시스템에 적용하면 암호를 유실할 경우 데이터를 복구할 수 없습니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

17 **마침**을 클릭하여 설정을 저장하고 적용합니다.

마법사가 닫힙니다.

18 **경고** 페이지가 나타났지만 선택 사항에 만족하는 경우 **마침**을 다시 클릭합니다.

Rapid Recovery Agent 소프트웨어가 지정된 시스템에 배포되고, 필요에 따라 해당 시스템은 Core에서 보호 대상으로 추가됩니다.

다중 시스템의 보호 모니터링

Rapid Recovery가 시스템에 보호 정책과 일정을 적용할 때 진행률을 모니터링할 수 있습니다.

Rapid Recovery Core Console에서 Rapid Recovery 홈 페이지로 이동한 다음 (이벤트)를 클릭합니다.

작업, 경고 및 이벤트로 구분된 **이벤트** 페이지가 표시됩니다. 볼륨이 전송되면 상태, 시작 시간 및 종료 시간이 작업 창에 표시됩니다.

상태별로 작업을 필터링할 수도 있습니다(활성, 대기 중, 완료됨, 대기 상태임 및 실패함). 자세한 내용은 작업 보기을(를) 참조하십시오.

노트: 수행 대기 중인 작업만 보려면 대기 중인 작업 아이콘을 선택해야 합니다.

각 보호된 시스템을 추가하면 작업이 성공했는지 오류가 기록되었는지 나타내는 경고가 기록됩니다. 자세한 내용은 경고 보기을(를) 참조하십시오.

모든 이벤트 보기에 대한 내용은 모든 이벤트 보기을(를) 참조하십시오.

보호된 Exchange 서버의 설정 및 기능

Core에서 Microsoft Exchange Server를 보호 중인 경우 Rapid Recovery Core Console에서 구성할 수 있는 추가 설정이 있고, 수행할 수 있는 추가 기능이 있습니다.

단일 설정인 **자동 탑재 기능 검사 사용**을 SQL Server와 관련된 Core Console에서 사용할 수 있습니다. 활성화하면 Exchange 서버 탑재 기능 검사가 자동으로 수행됩니다. 이 설정은 보호된 시스템의 상태가 녹색(활성) 또는 노란색(일시 중지됨)일 때 사용할 수 있습니다.

자세한 내용은 Exchange 데이터베이스 마운트 가능성 검사 정보을(를) 참조하십시오.

보호된 Exchange 서버 시스템의 복구 지점 창에서 주문형 탑재 기능 검사를 수행할 수도 있습니다. 자세한 내용은 Exchange 데이터베이스의 마운트 가능성 검사 수행을(를) 참조하십시오.

다음은 Core에서 보호되는 Exchange 서버에 대해 수행할 수 있는 기능입니다.

- **Exchange 서버 자격 증명을 지정합니다.** Rapid Recovery Core에서는 Core에서 인증하여 Exchange 서버에서 정보를 다운로드할 수 있도록 자격 증명을 설정할 수 있습니다.
  Exchange 서버의 자격 증명 설정에 대한 자세한 내용은 Exchange Server 시스템에 대한 자격 증명 설정을(를) 참조하십시오.
- **Exchange 로그를 잘라냅니다**. Exchange 서버 로그의 로그 잘라내기를 강제로 수행하면 보호된 서버의 사용 가능한 공간과 회수 공간이 이 프로세스에서 식별됩니다.
  주문형 Exchange 서버 로그를 잘라내는 방법에 대한 자세한 내용은 Exchange 시스템에 대한 로그 잘라내기 수행을(를) 참조하십시오. 이 프로세스를 야간 작업 파트로 수행할 수도 있습니다.
- **Exchange 데이터베이스의 탑재 기능 강제 검사**. 이 기능에서는 Exchange 서버의 모든 데이터가 복구될 수 있도록 손상을 검색하여 관리자에게 경고하기 위해 Exchange 데이터베이스가 탑재 가능한지 검사합니다.
  주문형 탑재 기능을 강제 검사하는 방법에 대한 자세한 내용은 Exchange 데이터베이스의 마운트 가능성 검사 수행을(를) 참조하십시오.

  탑재 기능 강제 검사를 각 스냅숏 후 자동으로 발생하도록 설정할 수도 있습니다. 탑재 기능 검사에 대한 자세한 내용은 Exchange 데이터베이스 마운트 가능성 검사 정보을(를) 참조하십시오.
- **Exchange Server 복구 지점의 체크섬 강제 검사** 이 기능에서는 Exchange 데이터베이스 파일이 포함된 복구 지점의 무결성을 검사합니다.
  주문형 체크섬을 강제 검사하는 방법에 대한 자세한 내용은 Exchange 데이터베이스 파일의 체크섬 검사 수행을(를) 참조하십시오.

야간 작업 파트로 Exchange 로그를 잘라내고 체크섬을 강제 검사할 수 있습니다. 야간 작업으로 예약할 수 있는 작업에 대한 자세한 내용은 야간 작업 이해을(를) 참조하십시오. 야간 작업 구성 방법에 대한 자세한 내용은 Core에 대한 야간 작업 구성을(를) 참조하십시오.

Exchange Server 시스템에 대한 자격 증명 설정

로그인 자격 증명을 설정하려면 보호된 볼륨에 Exchange Server가 있어야 합니다. Rapid Recovery에서 데이터베이스의 존재를 감지하지 못하면 자격 증명 설정 기능이 Core Console에 나타나지 않습니다.

Microsoft Exchange Server의 데이터를 보호하면 Rapid Recovery Core Console에서 로그인 자격 증명을 설정할 수 있습니다.

각 Exchange Server에 대한 자격 증명을 설정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 자격 증명을 설정할 보호된 Exchange Server 시스템을 선택합니다.
보호된 Exchange Server에 대한 **요약** 페이지가 나타납니다.

2 **요약** 페이지 상단의 링크에서 Exchange 메뉴 오른쪽에 있는 아래쪽 방향의 화살표 ▼를 클릭한 후 표시되는 드롭다운 메뉴에서 **자격 증명 설정**을 선택합니다.
보호된 Exchange Server에 대한 **Exchange 자격 증명 편집** 대화 상자가 나타납니다.

3 **Exchange 자격 증명 편집** 대화 상자에서 다음과 같이 사용자의 자격 증명을 입력합니다.
   a **사용자 이름** 텍스트 필드에는 Exchange Server에 대한 권한을 가진 사용자의 사용자 이름을 입력합니다. 예를 들어 Administrator 또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator가 됩니다.
   b **암호** 텍스트 필드에는 Exchange Server 연결을 위해 지정한 사용자 이름과 연관된 암호를 입력합니다.
   c **확인**을 클릭하여 설정을 확인하고 대화 상자를 닫습니다.

Exchange 시스템에 대한 로그 잘라내기 수행

로그 자르기를 강제로 수행하려면 보호된 볼륨에 Exchange 데이터베이스가 있어야 합니다. Rapid Recovery가 데이터베이스의 존재를 탐지하지 못하면 로그 자르기 기능이 Core Console에 나타나지 않습니다.

보호된 Exchange Server에 로그 자르기를 강제로 수행하면 로그 크기가 줄어듭니다. 필요에 따라 로그 자르기를 강제로 수행하려면 이 절차에 있는 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 로그 자르기를 강제로 수행하려는 보호된 Exchange Server를 선택합니다.
   보호된 시스템에 대한 **요약** 페이지가 나타납니다.
2 페이지 상단에서 **Exchange** 드롭다운 메뉴를 클릭하고 **로그 자르기 강제 적용**을 선택합니다.
3 결과 대화 상자에서 클릭해 로그 자르기 강제 적용을 확인합니다.
   대화 상자가 닫힙니다. 시스템에서 Exchange Server 로그를 자르기 시작합니다. 이런 유형의 이벤트에 대한 팝업 경고가 활성화되어 있는 경우 로그 자르기 프로세스가 시작되었다는 메시지를 볼 수 있습니다.

Exchange 데이터베이스 마운트 가능성 검사 정보

Rapid Recovery를 사용하여 Microsoft Exchange Server를 백업하는 경우, 각 스냅숏 이후 모든 Exchange 데이터베이스에 대해 마운트 가능성 검사를 수행할 수 있습니다. 이 손상 탐지 기능을 사용하면 관리자에게 잠재적 실패를 경고하고, 장애 발생 시 Exchange 서버의 모든 데이터를 성공적으로 복구할 수 있습니다.

이 기능을 활성화 또는 비활성화하려면 보호된 시스템의 **설정** 메뉴로 가서 **자동 마운트 가능성 검사 사용** 옵션을 예 또는 아니요로 설정합니다. 보호된 시스템의 설정을 수정하는 방법에 대한 자세한 내용은 보호된 시스템 설정 보기 및 수정을(를) 참조하십시오.

마운트 가능성 검사는 야간 설정의 일부가 아닙니다. 그러나 자동 마운트 가능성 검사가 Exchange 로그 잘라내기 야간 작업과 함께 활성화되면 로그 잘라내기 작업이 완료된 후 마운트 가능성 검사가 트리거됩니다.

또한 보호된 Exchange Server 시스템의 **복구 지점** 창에서 요청 시 마운트 가능성 검사를 수행할 수 있습니다. 자세한 내용은 Exchange 데이터베이스의 마운트 가능성 검사 수행을(를) 참조하십시오.

노트: 마운트 가능성 검사는 Microsoft Exchange 2007, 2010 및 2013에만 적용됩니다. 또한 Rapid Recovery Agent 서비스 계정을 Exchange의 조직 관리자 역할에 할당해야 합니다.

Exchange 데이터베이스의 마운트 가능성 검사 수행

마운트 가능성 검사를 수행하려면 보호된 볼륨에 Exchange 데이터베이스가 있어야 합니다. Rapid Recovery에서 데이터베이스의 존재를 감지하지 못하면 마운트 가능성 검사 기능이 Core Console에 나타나지 않습니다.

요청 시 시스템에서 특정 Exchange Server 복구 지점에 대해 마운트 가능성 검사를 수행하도록 하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 마운트 가능성 검사를 수행할 보호된 Exchange Server 시스템을 선택한 후 **복구 지점** 메뉴를 클릭합니다.
2 **복구 지점** 창을 아래로 스크롤합니다.
3 원하는 복구 지점을 찾기 위해 복구 지점을 탐색합니다. 선택적으로, 목록에서 복구 지점 오른쪽에 있는 ▸ 화살표를 클릭하여 보기를 확장합니다.
   확장된 복구 지점 정보에서 복구 지점에 포함된 볼륨을 볼 수 있습니다.
4 **복구 지점** 창에서 올바른 복구 지점을 나타내는 행의 ⚙ 을 클릭하고 드롭다운 메뉴에서 **마운드 가능성 검사 수행**을 선택합니다.
5 대화 상자가 나타나면 마운트 가능성 검사 수행을 확인하기 위해 클릭합니다.

대화 상자가 닫힙니다. 시스템이 마운트 가능성 검사를 수행합니다. 이 유형의 이벤트에 대해 팝업 경고가 활성화되어 있으면 마운트 가능성 검사 시작을 알리는 메시지가 나타납니다.

마운트 가능성 검사의 상태를 보는 방법에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

Exchange 데이터베이스 파일의 체크섬 검사 수행

체크섬 검사를 수행하려면 보호된 볼륨에 Exchange 데이터베이스가 있어야 합니다. Rapid Recovery에서 데이터베이스의 존재를 감지하지 못하면 체크섬 검사 기능이 Core Console에 나타나지 않습니다.

시스템에서 특정 Exchange Server 복구 지점에 대해 체크섬 검사를 수행하도록 하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console 콘솔의 왼쪽 탐색 영역에서 체크섬 검사를 수행할 보호된 Exchange Server를 선택한 후 **복구 지점** 메뉴를 클릭합니다.

복구 지점 페이지가 보호된 Exchange Server에 나타납니다.

2 **복구 지점** 창을 아래로 스크롤합니다.

3 원하는 복구 지점을 찾기 위해 복구 지점을 탐색합니다. 선택적으로, 목록에서 복구 지점 오른쪽에 있는 ▶ 화살표를 클릭하여 보기를 확장합니다.

확장된 복구 지점 정보에서 복구 지점에 포함된 볼륨을 볼 수 있습니다.

4 **복구 지점** 창에서 올바른 복구 지점을 나타내는 행의 ⚙ 을 클릭한 후 드롭다운 메뉴에서 **체크섬 검사 수행**을 선택합니다.

5 대화 상자가 나타나면 체크섬 검사 수행을 확인하기 위해 클릭합니다.

대화 상자가 닫힙니다. 시스템에서 체크섬 검사를 수행합니다. 이 유형의 이벤트에 대해 팝업 경고가 활성화되어 있으면 체크섬 검사 시작을 알리는 메시지가 나타납니다.

체크섬 검사의 상태를 보는 방법에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

보호되는 SQL Server의 설정 및 기능

Core에서 Microsoft SQL Server를 보호 중인 경우 Rapid Recovery Core Console에서 구성할 수 있는 추가 설정이 있으며, 수행할 수 있는 추가 기능이 있습니다.

단일 설정인 **연결 기능**을 SQL Server와 관련된 Core Console에서 사용할 수 있습니다.

Rapid Recovery Core에서 SQL 연결 기능 검사를 수행하여 SQL 데이터베이스가 포함된 복구 지점의 무결성을 확인할 수 있습니다. 이 작업을 통해 SQL 데이터베이스의 일관성이 검사되고 지원되는 모든 MDF(데이터) 및 LDF(로그) 파일을 백업 스냅숏에서 사용할 수 있게 됩니다.

이전 릴리스에서는 SQL 연결 기능을 검사하려면 Core 시스템에 사용이 허가된 SQL Server의 버전이 있어야 했습니다. 이제 Rapid Recovery Core에서는 Core의 SQL Server 인스턴스 또는 보호된 SQL Server 시스템의 사용이 허가된 SQL Server 버전에서 SQL 연결 기능 검사를 수행할 수 있습니다.

연결 기능을 설정하면 이 검사를 수행하는 데 사용되는 사용이 허가된 SQL Server 버전을 지정할 수 있습니다. 연결 기능 설정을 구성하는 방법에 대한 자세한 내용은 Core SQL 연결 기능 설정 관리을(를) 참조하십시오.

SQL 연결 기능에 대한 자세한 내용은 SQL 연결 기능 정보을(를) 참조하십시오.

다음은 Core에서 보호되는 SQL 서버에 대해 수행할 수 있는 기능입니다.

- **SQL Server 자격 증명을 지정합니다.** Rapid Recovery Core에서는 정보를 획득할 SQL Server를 Core에서 인증할 수 있도록 자격 증명을 설정할 수 있습니다. 하나의 보호된 SQL 서버 시스템에 대한 자격 증명을 설정할 수도 있고, 모든 보호된 SQL Server에 대한 기본 자격 증명을 설정할 수도 있습니다.

  SQL Server의 자격 증명 설정에 대한 자세한 내용은 SQL Server 시스템에 대한 자격 증명 설정을(를) 참조하십시오.
- **SQL 로그를 잘라냅니다.** SQL Server 로그의 로그 잘라내기를 강제로 수행하면 보호된 서버에서 사용 가능한 공간이 이 프로세스에서 식별됩니다. 이 프로세스에서 공간이 확보되지는 않습니다.

필요 시 SQL Server 로그를 잘라내는 방법에 대한 자세한 내용은 SQL 시스템에 대한 로그 잘라내기 수행을(를) 참조하십시오.

- **SQL Server**의 연결 기능 검사를 강제로 수행합니다. 이 기능을 통해 SQL 데이터베이스의 일관성이 검사되고 지원되는 모든 MDF(데이터) 및 LDF(로그) 파일을 백업 스냅숏에서 사용할 수 있게 됩니다.

  필요 시 SQL Server의 연결 기능 검사를 수행하는 방법에 대한 자세한 내용은 SQL Server 연결성 검사 수행을(를) 참조하십시오.

자격 증명 지정 외에는, 앞의 목록에서 설명한 각각의 기능을 필요 시 수행할 수 있으며 Core에 대해 수행되는 야간 작업의 일부로 발생하도록 구성할 수도 있습니다. 야간 작업으로 예약할 수 있는 작업에 대한 자세한 내용은 야간 작업 이해을(를) 참조하십시오. 야간 작업 구성 방법에 대한 자세한 내용은 Core에 대한 야간 작업 구성을(를) 참조하십시오.

SQL Server 시스템에 대한 자격 증명 설정

이 절차를 수행하기 전에 Rapid Recovery Core에서 SQL Server 시스템을 보호 대상에 추가해야 합니다. 시스템 보호에 대한 자세한 내용은 시스템 보호를 참조합십시오.

Microsoft SQL Server 시스템에서 데이터를 보호하는 경우 Rapid Recovery Core Console에서 모든 SQL Server 또는 하나의 인스턴스에 대한 로그인 자격 증명을 설정할 수 있습니다.

각 SQL Server에 대한 자격 증명을 설정하려면 이 절차의 단계를 완료합니다.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 자격 증명을 설정하려는 보호 대상 SQL Server 시스템을 선택합니다.

보호 대상 SQL Server에 대한 **요약** 페이지가 나타납니다.

2 **요약** 페이지 맨 위에 있는 링크에서 SQL 메뉴 오른쪽에 있는 아래 화살표 ▼를 클릭하고 결과로 표시되는 드롭다운 메뉴에서 다음 중 하나를 수행합니다.

- 모든 SQL Server 데이터베이스 인스턴스에 대한 자격 증명을 설정하려면 **모든 인스턴스에 대해 기본 자격 증명 설정**을 클릭하고 **기본 자격 증명 편집** 대화 상자에서 다음 작업을 수행합니다.
  1 **사용자 이름** 텍스트 필드에 연결된 모든 SQL Server에 대한 권한을 가지는 사용자의 사용자 이름(예: Administrator)을 입력합니다(또는 시스템이 도메인에 있는 경우, [도메인 이름]\Administrator).
  2 **암호** 텍스트 필드에 SQL Server에 연결하기 위해 지정한 사용자 이름과 연결된 암호를 입력합니다.
  3 **확인**을 클릭하여 설정을 확인하고 대화 상자를 닫습니다.
- 단일 SQL Server 데이터베이스 인스턴스에 대한 자격 증명을 설정하려면 보호 대상 SQL Server 시스템의 표시 이름을 클릭하고 **인스턴스 자격 증명 편집**에서 다음 작업을 수행합니다.
  1 자격 증명 유형(기본값, Windows 또는 SQL)을 선택합니다.
  2 **사용자 이름** 텍스트 필드에 SQL Server에 대한 권한을 가지는 사용자의 사용자 이름(예: Administrator)을 입력합니다(또는 시스템이 도메인에 있는 경우, [도메인 이름]\Administrator).
  3 **암호** 텍스트 필드에 SQL Server에 연결하기 위해 지정한 사용자 이름과 연결된 암호를 입력합니다.
  4 **확인**을 클릭하여 설정을 확인하고 대화 상자를 닫습니다.

SQL 시스템에 대한 로그 잘라내기 수행

SQL Server를 사용하는 시스템에 대해 로그 잘라내기를 수행할 수 있습니다. 로그 잘라내기를 수행하려면 다음 단계를 완료하십시오.

노트: SQL 시스템에 대해 실시했을 때 잘라내기는 디스크의 사용 가능한 공간을 식별하지만, 로그의 크기를 줄이지는 않습니다.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 로그 자르기를 강제로 수행하려는 시스템을 선택합니다.

보호된 시스템에 대한 **요약** 페이지가 나타납니다.

2 페이지 상단에 있는 **요약** 페이지(또는 이 보호된 시스템의 모든 페이지에서)에서 **SQL** 드롭다운 메뉴를 클릭하고 **로그 자르기 강제 적용**을 선택합니다.

3 **예**를 클릭하여 로그 잘라내기를 수행할 것임을 확인합니다.

SQL 연결 기능 정보

SQL 연결 기능을 통해 Rapid Recovery Core는 SQL 마스터 데이터베이스 파일(.MDF 파일)을 연결하고 데이터베이스 파일(.LDF 파일)을 보호된 SQL Server의 스냅숏으로 기록할 수 있습니다. 스냅숏은 Microsoft SQL Server의 로컬 인스턴스를 사용하여 캡처됩니다.

SQL Server 시스템을 보호하는 Rapid Recovery 사용자에 대한 관련 문제는 연결 기능을 수행하는 SQL Server 인스턴스, 그리고 SQL 연결 기능 수행 방식(주문형 또는 야간 작업의 일부)이 포함되어 있습니다.

Core에서는 연결 기능 검사를 통해 SQL 데이터베이스의 일관성을 검사하고 백업 스냅숏에서 모든 MDF 및 LDF 파일을 사용할 수 있는지 확인할 수 있습니다.

연결 기능 검사는 특정 복구 지점에 대해 또는 야간 작업의 일부로 요청 시 실행할 수 있습니다.

SQL 연결 기능 검사를 수행하려면 SQL Server 연결성 검사 수행을(를) 참조하십시오. SQL 연결 기능을 하루에 한번 야간 작업 중 지정한 시간에 수행하려면 야간 작업에서 **SQL 데이터베이스의 가용성 검사** 옵션을 활성화하십시오. Core에 대해 야간 작업을 설정하는 방법에 대한 자세한 내용은 Core에 대한 야간 작업 구성을(를) 참조하십시오. 특정 시스템(이 경우에 보호된 SQL Server)에 대해 야간 작업을 설정하는 방법에 대한 자세한 내용은 보호되는 시스템에 대한 야간 작업 사용자 지정을(를) 참조하십시오.

이전 버전에서는 SQL 연결 기능을 수행하려면 Microsoft SQL Server 로컬 인스턴스가 Core 시스템에 설치되고 구성되어 있어야 합니다. 이제 Rapid Recovery Core에서는 Core의 SQL Server 인스턴스 또는 보호된 SQL Server 시스템의 SQL Server 인스턴스에서 연결 기능 검사 여부를 선택할 수 있습니다. 사용자가 선택하는 인스턴스는 Microsoft 또는 공인 대리점에서 제공하는 정품 라이센스 버전의 SQL Server여야 합니다. Microsoft는 수동적인 SQL 라이센스 사용을 허용하지 않습니다.

그런 다음, 지정하는 SQL Server 인스턴스는 모든 연결 검사에 사용됩니다. 연결 기능은 Core 설정과 야간 작업 간에 동기화됩니다. 예를 들어, 야간 작업을 위해 SQL Server의 Core 인스턴스 사용을 지정할 경우 주문형 연결 기능 검사에서도 해당 Core를 사용합니다. 반대로, 특정 보호된 시스템에서 SQL Server 인스턴스 사용을 지정할 경우 모든 주문형 및 야간 연결 기능 검사에서 보호된 시스템의 로컬 인스턴스를 사용합니다.

전역 Core 설정의 일부로 사용할 SQL Server 인스턴스를 선택합니다. 자세한 내용은 Core SQL 연결 기능 설정 관리을(를) 참조하십시오.

노트: 보호된 SQL Server 시스템에서 연결 기능 검사를 수행하려면 Rapid Recovery Agent 소프트웨어가 해당 서버에 설치되어야 합니다. 에이전트 없는 보호는 SQL 연결 기능에 대해 지원되지 않습니다.

Rapid Recovery Core에서 연결 기능은 SQL Server 2005, 2008, 2008 R2, 2012 및 2014를 지원합니다. 테스트에 사용되는 계정에는 SQL Server 인스턴스에서 sysadmin 역할을 부여해야 합니다.

SQL Server 온디스크 저장 형식은 64-bit 및 32-bit 환경에서 모두 동일하며 연결성은 두 가지 버전에서 모두 작동합니다. 한 환경에서 실행 중인 서버 인스턴스에서 분리된 데이터베이스는 다른 환경에서 실행되는 서버 인스턴스에 추가할 수 있습니다.

노트: Core의 SQL Server 버전은 SQL Server가 설치된 모든 보호된 시스템의 SQL Server 버전과 같거나 이후 버전이어야 합니다.

SQL Server 연결성 검사 수행

연결성 검사를 수행하려면 보호된 볼륨에 SQL 데이터베이스가 있어야 합니다. Rapid Recovery에서 데이터베이스의 존재를 감지하지 못하면 연결성 검사 기능이 Core Console에 나타나지 않습니다.

시스템에서 특정 SQL Server 복구 지점에 대해 연결성 검사를 수행하도록 하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 영역에서 연결성 검사를 수행할 보호된 SQL Server 시스템을 선택한 후 **복구 지점** 메뉴를 클릭합니다.
2 **복구 지점** 창을 아래로 스크롤합니다.
3 원하는 복구 지점을 찾기 위해 복구 지점을 탐색합니다. 선택적으로, 목록에서 복구 지점 오른쪽에 있는 ▶ 화살표를 클릭하여 보기를 확장합니다.
   확장된 복구 지점 정보에서 복구 지점에 포함된 볼륨을 볼 수 있습니다.
4 **복구 지점** 창에서 올바른 복구 지점을 나타내는 행의 을 클릭하고 드롭다운 메뉴에서 **연결성 검사 수행**을 선택합니다.
5 대화 상자가 나타나면 연결성 검사 수행을 확인하기 위해 클릭합니다.
   대화 상자가 닫힙니다. 시스템이 연결성 검사를 수행합니다.

연결성 검사의 상태를 보는 방법에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

Rapid Snap for Virtual 이해

Rapid Recovery 에이전트 소프트웨어를 설치함으로써 Rapid Recovery Core에서 실제 또는 가상 시스템에 보호할 수 있습니다. 지원되는 운영 체제는 "Rapid Recovery 에이전트 소프트웨어 요구 사항" 항목의 시스템 요구 사항에 표시되어 있습니다.

Rapid Recovery는 이제 시스템을 보호하기 위한 다른 접근법을 제공합니다.

Rapid Snap for Virtual 기능은 Rapid Recovery의 에이전트 없는 보호라고도 하며 Rapid Recovery 에이전트를 모든 VM에 설치하지 않고 VMware ESXi 또는 Hyper-V 호스트에서 가상 시스템(VM)을 보호할 수 있습니다.

△ 주의: **Dell은 에이전트 없이 VM을 한 번에 200개 이상 보호하지 않도록 제한하는 것을 권장합니다. 예를 들어, Protect Multiple Machines Wizard(여러 시스템 보호 마법사)를 사용할 때 VM을 200개 이상 선택하지 마십시오. VM을 200개 이상 보호하면 성능이 저하됩니다. Core 가 시간에 따라 에이전트 없이 보호할 수 있는 VM 수에는 제한이 없습니다. 예를 들어, 오늘 VM을 200개 보호하고 내일 다른 VM을 200개 보호할 수 있습니다.**

vCenter/ESXi VM 보호

Rapid Recovery를 사용하면 VM 또는 ESXi 호스트에 Rapid Recovery 에이전트를 설치하지 않고 vCenter/ESXi VM을 보호하여 에이전트 없는 보호를 달성할 수 있습니다. ESXi 환경을 보호하기 위해 Rapid Recovery Core는 VMware에 기본 제공되는 스냅샷 기술을 사용합니다.

Rapid Recovery 에이전트 없는 보호는 ESXi 클라이언트와 기존 응용 프로그램 인터페이스(API)를 사용하여 Rapid Recovery 에이전트 소프트웨어를 설치하지 않고 단일 호스트에서 선택한 VM을 보호합니다. Rapid Recovery Core는 가상 시스템 디스크(VMDK)와 통신하여 보호되는 볼륨의 필요한 상세 정보를 확인합니다. Rapid Recovery는 VMDK가 아닌 볼륨을 기반으로 복구 지점을 생성하므로 각 볼륨을 개별적으로 마운트, 복원 및 내보낼 수 있습니다.

ⓘ 노트: **Rapid Recovery에서는 vSphere or ESXi에서 보호하려는 가상 시스템(VM)에 VMware 도구를 설치할 것을 권장합니다. Windows 운영 체제(OS)를 사용하는 VM에 VMware 도구가 설치되면 Rapid Recovery Core에서 캡처하는 백업은 Microsoft 볼륨 섀도 서비스(VSS)를 사용합니다. VMware 도구를 사용하거나 사용하지 않는 에이전트 없는 VM에 대한 자세한 내용은 에이전트 없는 보호를 위한 VMware 도구 설치 이점을(를) 참조하십시오.**

또한 에이전트 없는 보호는 증분 스냅샷에 필요한 시간을 줄이기 위해 VMware CBT(Changed Block Tracking)를 사용합니다. CBT는 VMDK 파일에서 변경된 블록을 확인하고 Rapid Recovery가 디스크에서 마지막 스냅샷 이후로 변경된 부분만 백업하도록 합니다. 이 백업 방법으로 인해 종종 백업 작업이 더 단축되고 네트워크 및 저장소에 대한 리소스 소모가 감소됩니다.

에이전트 없는 보호 사용에는 여러 가지 이점이 있습니다. 가장 유용한 특성 몇 가지는 다음과 같은 특성이 있습니다.

- 호스트 시스템에 추가 소프트웨어는 필요하지 않습니다.
- 에이전트 없는 보호를 사용하면 ESXi 호스트에 추가된 새 VM을 자동으로 보호할 수 있습니다.
- 보호 프로세스 중에는 재시작할 필요가 없습니다.
- 각 개별 VM에 자격 증명을 요구하지 않습니다.
- 에이전트 없는 보호를 사용하면 전원이 꺼져 있는 경우에도 VM을 보호할 수 있습니다.
- 에이전트 없는 보호를 사용하면 디스크로 복원할 수 있습니다.
- 에이전트 없는 보호는 전송 중에 볼륨에 사용 가능한 공간이 필요하지 않습니다.
- 에이전트 없는 보호는 모든 게스트 운영 체제를 지원합니다.
- 에이전트 없는 보호를 사용하면 동적 디스크 또는 볼륨을 내보낼 수 있습니다.

ⓘ 노트: **동적 볼륨이 복잡한 경우(스트라이핑, 미러링, 스팬, 또는 RAID) 디스크 이미지로 내보내고 내보낸 VM에서 내보내기 작업이 완료된 후 볼륨으로 구문 분석합니다.**

ESXi VM에 대해 에이전트 없는 보호를 사용하는 많은 이유가 있지만 사용자 환경 및 비즈니스 요구에 가장 적합한 보호 방법을 선택하십시오. 앞에서 언급한 이점과 함께 에이전트 없는 보호를 선택할 때 다음과 같은 고려 사항도 염두에 두어야 합니다.

- 에이전트 없는 보호는 볼륨 레벨에서 동적 볼륨(예: 스팬, 스트라이핑, 미러링 또는 RAID 볼륨)의 보호를 지원하지 않습니다. 이 보호는 디스크 레벨에서 보호합니다.
- 에이전트 없는 보호는 라이브 복구를 지원하지 않습니다. 이 기능에 대한 자세한 내용은 Live Recovery 이해을(를) 참조하십시오.
- 단일 볼륨을 보호되는 VM으로 복원한 후에는 VM을 다시 시작해야 합니다.
- 에이전트 없는 보호에서는 Microsoft SQL 또는 Microsoft Exchange 메타데이터를 수집하지 않습니다.
- 에이전트 없이 보호되는 시스템에서는 SQL 연결 기능 검사, 로그 자르기 또는 캡처되는 복구 지점의 마운트 기능 검사를 수행할 수 없습니다.
- 에이전트 없는 보호는 볼륨 레이블 또는 드라이브 문자를 수집하거나 표시하지 않습니다.
- 에이전트 없는 보호는 가상 디스크 유형이 Thick Provision Eager Zeroed인 경우 VM에 사용되는 공간의 실제 용량을 표시하지 않습니다.

ESXi VM에 대해 에이전트 없는 보호를 사용하도록 선택하는 경우 호스트는 에이전트 없는 보호를 성공적으로 수행하려면 다음의 최소 요구 사항을 충족해야 합니다.

- 호스트 시스템은 ESXi 버전 5.0.0 빌드 623860 이상을 실행하고 있어야 합니다.
- 호스트 시스템은 최소 시스템 요구 사항을 충족해야 합니다 *Rapid Recovery 설치 및 업그레이드 설명서*에 나와 있는 최소 시스템 요구 사항을 충족해야 합니다.
- 볼륨 레벨 보호의 경우 VMDK는 마스터 부트 레코드(MBR) 파티션 테이블 또는 GUID 파티션 테이블을(GPT) 중 하나를 포함해야 합니다. 이러한 파티션 테이블이 없는 VMDK는 개별 볼륨이 아닌 전체 디스크로 보호됩니다.
- 각 VMware 가상 시스템에는 스냅샷 일관성을 보장하기 위해 VMware 도구가 설치되어 있어야 합니다.

Hyper-V 서버 및 클러스터 보호

Hyper-V 서버를 에이전트 없이 보호하기 위해 모든 VM에 Rapid Recovery 에이전트를 설치할 필요가 없습니다. 호스트 시스템 또는 클러스터 노드만 설치하면 됩니다. 에이전트는 호스트에 있는 가상 하드 디스크를 보호하며 파일 시스템에 따라 하드 디스크 파일의 변경 사항을 볼륨 이미지로 변환합니다. 새 드라이버는 호스트 및 클러스터 공유 볼륨(CSV)의 VM에 대해 파일 레벨 지원을 제공합니다.

노트: Rapid Recovery는 VHDx 디스크 파일 형식을 지원하며 VHD 형식은 지원하지 않습니다.

CSV에서 VM을 보호하는 경우 Rapid Recovery 에이전트 및 드라이버가 Protect Multiple Machines(여러 시스템 보호) 마법사의 자동 배포 기능을 사용하여 각 클러스터 노드에 설치되어 있어야 합니다. 노드에서 에이전트는 모든 파일에 대해 두 가지 유형의 변경 사항을 생성하여 CSV의 모든 VM 작업을 보호할 수 있습니다. 첫 번째 변경 유형은 스냅샷 또는 클린 시스템 재시작 전이나 후에만 저장됩니다. 두 번째 변경 유형은 디스크에 저장되어 정전이나 더티 셧다운이 있는 경우에도 증분 스냅샷을 사용할 수 있도록 합니다. 노드에 설치된 에이전트는 데이터를 전송하기 전에 모든 변경 사항을 하나로 병합합니다.

호스트 또는 노드가 실행 중이면 Rapid Recovery는 응용 프로그램 일치 백업을 생성합니다. 호스트가 실행되고 있지 않은 경우 백업을 생성할 수 없지만 노드 중 하나가 실행되고 있지 않은 경우 Rapid Recovery는 클러스터에 VM의 스냅샷을 계속해서 만들 수 있습니다.

노트: 최상의 성능을 위해 이 Hyper-V 호스트 또는 노드에 대한 최대 동시 전송을 기본 설정인 1로 설정하는 것이 좋습니다.

에이전트 없는 Hyper-V 보호는 다음과 같이 모든 VM에 에이전트가 설치되는 전통적인 보호와 동일한 기능을 다수 갖추고 있습니다.

- 아카이빙
- 복구 지점 무결성 검사
- 복구 지점 마운트
- 새 VM의 자동 검색(에이전트 없는 보호에만 제공)
- 복제
- VM 복원
- CSV 복원
- VHDX 형식을 사용하여 CIFS 복원
- 게스트 VHDX 형식의 파일 복원
- 롤업

- ESXi, VMware Workstation 및 VirtualBox를 포함하여 Hyper-V VM 및 기타 하이퍼바이저로 가상 내보내기

하지만 에이전트 없는 Hyper-V 보호를 선택할 때 고려할 제한 사항이 있습니다. 수행되지 않는 기능은 다음과 같습니다.

- Exchange 마운트 무결성 검사
- SQL 연결 기능 검사
- 라이브 복구
- VHD 형식을 사용하여 CIFS에 VM 복원
- 게스트 VHD 형식의 파일 복원

노트: 응용 프로그램 일치 스냅샷의 경우 각 VM에 SCSI 컨트롤러가 설치되어 있어야 합니다. 이 컨트롤러가 없으면 결과는 항상 충돌 일치 스냅샷입니다.

에이전트 없는 보호를 위한 VMware 도구 설치 이점

Rapid Recovery Agent를 사용하지 않고 가상 시스템을 보호하는 경우 Dell에서는 Microsoft VSS(Volume Shadow Services) 기능을 최대한 활용하도록 vSphere 또는 ESXi 호스트의 보호된 VM에 VMware 도구 설치를 권장합니다.

에이전트 없는 보호는 VMware에 고유한 스냅숏 기술을 사용하여 보호되는 데이터를 백업합니다. Windows 운영 체제의 VM에 VMware 도구를 설치하면 Rapid Recovery Core에서 캡처하는 백업도 VSS를 사용할 수 있습니다. VMware 도구가 설치되어 있지 않으면 Rapid Recovery에서 계속 스냅숏을 수집해도, VMware 도구가 없기 때문에 보호된 VM에서 데이터 상태에 부정적인 영향을 줄 수 있습니다.

다음과 같은 두 가지 데이터 상태가 나타날 수 있습니다.

- **충돌 일치.** VM OS가 시작되며 파일 시스템을 읽고 인식할 수 있습니다.
- **응용 프로그램 일치.** VM OS가 시작되며 파일 시스템을 읽고 인식할 수 있습니다. 또한 트랜잭션 응용 프로그램에 대한 파일은 일관된 상태를 유지합니다. 예를 들어, SQL Server에서 로그는 데이터베이스 파일과 일치하고, 데이터베이스를 더 빠르고 쉽게 열 수 있습니다.

충돌 일치 상태에서 트랜잭션 응용 프로그램을 복구하면 데이터베이스는 마지막으로 유효한 상태로 돌아갑니다. 최근 유효한 상태는 충돌 시점이거나 충돌 시점보다 더 이전일 수도 있습니다. 충돌 시점보다 더 이전인 경우 데이터베이스는 데이터 파일이 로그의 정보와 일치하도록 일부 작업을 롤포워드해야 합니다. 데이터베이스를 처음 여는 경우 시스템을 시작할 때 지연이 발생하므로 이 프로세스가 오래 걸릴 수 있습니다.

VMware 도구의 설치 여부와 VM의 전원 상태에 따라 다음과 같은 조건을 적용합니다.

표 96. VM에 대한 백업 유형 조건

VMware 도구	VM 전원 상태	백업 유형
Not installed(설치 안 됨)	예	충돌 일치
Not installed(설치 안 됨)	아니요(더티 종료)	충돌 일치
Not installed(설치 안 됨)	아니요(완전한 종료)	응용 프로그램 일치
설치됨	예	응용 프로그램 일치
설치됨	아니요(더티 종료)	충돌 일치
설치됨	아니요(완전한 종료)	응용 프로그램 일치

Rapid Recovery 에이전트 없이 vCenter/ESXi가상 시스템 보호

에이전트 없이 ESXi 가상 시스템을 보호하려면 다음 절차를 완료합니다.

노트: Rapid Recovery에서는 vSphere or ESXi에서 보호하려는 가상 시스템(VM)에 VMware 도구를 설치할 것을 권장합니다. Windows 운영 체제(OS)를 사용하는 VM에 VMware 도구가 설치되면 Rapid Recovery Core에서 캡처하는 백업은 Microsoft 볼륨 섀도 서비스(VSS)를 사용합니다. VMware 도구를 사용하거나 사용하지 않는 에이전트 없는 VM에 대한 자세한 내용은 에이전트 없는 보호를 위한 VMware 도구 설치 이점을(를) 참조하십시오.

주의: 에이전트 없이 VM을 한 번에 200개 이상 보호하지 않도록 제한하는 것이 좋습니다. 예를 들어, Protect Multiple Machines Wizard(여러 시스템 보호 마법사)를 사용할 때 VM을 200개 이상 선택하지 마십시오. VM을 200개 이상 보호하면 성능이 저하됩니다. Core가 시간에 따라 에이전트 없이 보호할 수 있는 VM 수에는 제한이 없습니다. 예를 들어, 오늘 VM을 200개 보호하고 내일 다른 VM을 200개 보호할 수 있습니다.

1 Rapid Recovery Core 콘솔에서 **Protect(보호)** 드롭다운 메뉴를 클릭한 다음 **Protect Multiple Machines(여러 시스템 보호)**를 클릭합니다.

Protect Multiple Machines(여러 시스템 보호) 마법사가 열립니다.

2 **Welcome(시작)** 페이지에서 다음 옵션 중 하나를 선택합니다.

- 일반
- Advanced(고급)(옵션 단계 표시)

3 **다음**을 클릭합니다.

4 마법사의 **Connection(연결)** 페이지에 있는 **Source(소스)** 드롭다운 목록에서 **vCenter / ESX(i)**를 선택합니다.

5 다음 표에 설명된 대로 호스트 정보와 로그온 자격 증명을 입력합니다.

표 97. vCenter/ESX(i) 연결 설정

텍스트 상자	설명
호스트	VMware vCenter Server/ESX(i) 가상 호스트의 이름이나 IP 주소입니다.
포트	가상 호스트에 연결하는 데 사용되는 포트입니다. 기본 설정은 443입니다.
사용자 이름	가상 호스트에 연결하는 데 사용되는 사용자 이름입니다. 예를 들어, 관리자 또는 시스템이 도메인에 있는 경우 [도메인 이름]\Administrator입니다.
암호	이 가상 호스트에 연결하는 데 사용할 안전한 암호입니다.

6 **Protect selected VMs Agentlessly(선택한 VM을 에이전트 없이 보호)** 가 선택되어 있는지 확인합니다(이 옵션은 기본적으로 선택되어 있습니다).

7 **Select Machines(시스템 선택)** 페이지에서 보호하려는 VM을 선택합니다. 드롭다운 메뉴를 사용하여 호스트 및 클러스터의 목록 또는 VM 및 템플릿의 목록을 표시할 수 있습니다.

노트: 보호하려는 각 VM에서 VMware Changed Block Tracking (CBT)이 활성화되어 있어야 합니다. 활성화되지 않은 경우 Rapid Recovery는 보호를 위해 CBT를 자동으로 활성화합니다.

8 호스트에 추가될 때 새 VM을 자동으로 보호하려는 경우 **Auto protect new machines(새 시스템 자동 보호)**를 선택한 후 다음 단계를 수행하십시오.

a **다음**을 클릭합니다.

b **Auto Protection(자동 보호)** 페이지에서 새 시스템을 추가할 것으로 예상되는 컨테이너를 선택합니다.

9 **다음**을 클릭합니다.

10 Protection(보호) 페이지에서 다음 보호 일정 중 하나를 선택합니다.

- 기본 보호 일정을 사용하려면 Schedule Settings(일정 설정) 옵션에서 **Default protection (hourly snapshots of all volumes)(기본 보호(매시간 모든 볼륨의 스냅샷))**를 선택합니다.
- 다른 보호 일정을 정의하려면 Schedule Settings(일정 설정) 옵션에서 **Custom protection(사용자 지정 보호)**을 선택합니다.

11 다음과 같이 구성을 계속 진행합니다.

- Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 **Finish(마침)**를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.

  시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Rapid Recovery Core의 리포지토리에 전송됩니다.
- Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 13단계를 계속 진행하여 리포지토리 및 암호화 옵션을 확인합니다.
- Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 사용자 지정 보호 일정 만들기을(를) 참조하십시오.

12 **다음**을 클릭합니다.

13 **Repository(리포지토리)** 페이지에서 다음을 수행합니다.

- 리포지토리가 이미 있고 보호를 위해 기존 리포지토리에 이 시스템의 데이터를 저장하려는 경우 다음을 수행합니다:
  1 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
  2 목록에서 기존 리포지토리를 선택합니다.
  3 **다음**을 클릭합니다.

  Encryption(암호화) 페이지가 나타납니다. 선택적으로 암호화를 정의하려면 19단계로 건너뜁니다.
- 리포지토리를 생성하려는 경우 **Create a Repository(리포지토리 생성)**를 선택한 후 다음 단계를 완료합니다.
  1 **Repository(리포지토리)** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 98. 새 리포지토리 설정 추가

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 이 Core의 리포지토리 번호에 해당하는 번호로 구성됩니다. 예를 들어, 이것이 첫 번째 리포지토리인 경우 기본 이름은 리포지토리 1입니다. 필요하면 이름을 변경합니다. 리포지토리 이름에는 공백을 포함하여 1~40자의 영숫자 문자를 포함해야 합니다. 금지된 문자 또는 금지된 구은(는) 사용하지 마십시오.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본적으로 값은 64입니다.
설명	선택적으로 이 리포지토리에 대해 설명하는 메모를 입력합니다. 최대 254자를 입력할 수 있습니다. 예를 들어, **DVM Repository 2**를 입력합니다.

  2 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

> △ 주의: **리포지토리의 저장소 위치는 루트 내에 전용 폴더로 정의합니다. 루트 위치는 지정하지 마십시오. 예를 들어, E:\가 아닌 E:\Repository\를 사용합니다. 이 단계에서 생성하는 리포지토리를 나중에 제거하는 경우 해당 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 루트에 저장소 위치를 정의하는 경우 볼륨(예: E:\)에 있는 다른 모든 파일이 삭제되어 이는 치명적인 데이터 손실을 초래할 수 있습니다.**

  Add Storage Location(저장소 위치 추가) 대화 상자가 표시됩니다.

  3 **Add Storage Location(저장소 위치 추가)**를 클릭하여 리포지토리에 대한 특정 저장소 위치 또는 볼륨을 정의합니다. 이 볼륨은 기본 저장소 위치여야 합니다.

  4 **Storage Location(저장소 위치)** 영역에 저장소 위치의 파일을 추가하는 방법을 지정합니다. 로컬로 연결된 저장소 볼륨을 추가할 수 있습니다(예: 직접 연결된 저장소, 저장소 영역 네트워크 또는 네트워크에 연결된 저장소). 일반 인터넷 파일 시스템(CIFS) 공유 위치에 저장소 볼륨을 지정할 수도 있습니다.

  - **Add file on local disk(로컬 디스크에 파일 추가)**를 선택하여 로컬 시스템을 지정하고 아래 표에 설명된 대로 정보를 입력합니다.

표 99. 로컬 디스크 설정

텍스트 상자	설명
데이터 경로	보호된 데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Data`를 입력합니다.

텍스트 상자	설명
	경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호된 메타데이터를 저장할 위치를 입력합니다. 예를 들어, `X:\Repository\Metadata`를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. 백슬래시 문자는 경로에서 레벨을 정의하는 데만 사용할 수 있습니다. 공백은 사용하지 마십시오. 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 또는 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 선택하여 네트워크 공유 위치를 지정한 후 아래 표에 설명된 대로 정보를 입력합니다.

표 100. CIFS 공유 자격 증명

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있는 경우 전용 폴더 이름(예: `Repository`)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.

5 **Storage Configuration(저장소 구성)** 영역에서 **More Details(상세 정보)**를 클릭하고 아래 표에 설명된 대로 저장소 위치에 대한 상세정보를 입력합니다.

표 101. 저장소 구성 상세 정보

텍스트 상자	설명
크기	저장소 위치의 크기 또는 용량을 설정합니다. 최소 크기는 1GB이고 기본값은 250GB입니다. 다음 중에서 선택할 수 있습니다. • GB • TB **노트: 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다. 저장소 위치가 Windows 8, 8.1, Windows 10 또는 Windows Server 2012, 2012 R2을 사용하는 NTFS 볼륨인 경우 파일 크기 한도는 256TB입니다. **노트: Rapid Recovery에서 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 Windows Management Instrumentation(WMI)이 설치되어 있어야 합니다.**
쓰기 캐싱 정책	쓰기 캐싱 정책은 리포지토리에서 Windows 캐시 관리자가 사용되는 방법을 제어하고 다른 구성에 대해 성능을 최적화할 수 있도록 리포지토리를 조정하는 데 도움을 줍니다. 값을 다음 중 하나로 설정합니다. • 켜짐 • 꺼짐 • 동기화 기본값인 On(켜짐)으로 설정하는 경우 Windows에서 캐싱을 제어합니다. 이는 Windows 10 및 Windows Server 2012 이상 버전에 적합합니다.

텍스트 상자	설명
	노트: 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2008 SP2 또는 Windows Server 2008 R2 SP2를 사용하는 경우 권장되는 설정은 Off(꺼짐)입니다. Off(꺼짐)로 설정하면 Rapid Recovery에서 캐싱을 제어합니다. Sync(동기화)로 설정하면 Windows에서 캐싱과 동기식 입력/출력을 제어합니다.
섹터당 바이트	각 섹터에 포함할 바이트 수를 지정합니다. 기본값은 512입니다.
레코드당 평균 바이트	레코드당 평균 바이트 수를 지정합니다. 기본값은 8192입니다.

6 **다음**을 클릭합니다.

1단계에서 **Advanced(고급)** 옵션을 선택한 경우 **Encryption(암호화)** 페이지가 나타납니다.

14 선택적으로 Encryption(암호화) 페이지에서 암호화를 활성화하려면 **Enable Encryption(암호화 사용)**을 선택합니다.

Encryption(암호화) 페이지에 Encryption key(암호화 키) 필드가 나타납니다.

노트: 암호화를 활성화하면 이 시스템의 모든 보호되는 볼륨에 있는 데이터에 적용됩니다. Rapid Recovery Core 콘솔의 Configuration (구성) 탭에서 나중에 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 암호화 키 이해을(를) 참조하십시오.

주의: Rapid Recovery에서는 CBC(Cipher Block Chaining) 모드에서 256바이트 키와 함께 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택 사항이지만 암호화 키를 설정하고 정의하는 암호를 보호할 것을 권장합니다. 암호는 데이터 복구에 매우 중요하므로 안전한 위치에 저장해 두십시오. 암호가 없으면 데이터를 복구할 수 없습니다.

15 이 Rapid Recovery Core에 이미 정의된 암호화 키를 사용하여 이 보호되는 시스템을 암호화하려면 **Encrypt data using an existing Encryption key(기존 암호화 키를 사용하여 데이터 암호화)**를 선택한 다음 드롭다운 메뉴에서 적절한 키를 선택합니다.

17단계로 진행합니다.

16 Core에 암호화 키를 추가하고 해당 키를 이러한 보호되는 시스템에 적용하려는 경우 다음 표에 설명된 대로 정보를 입력합니다.

표 102. 암호화 키 설정

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다. 암호화 키 이름은 1~130자 사이의 영숫자를 포함해야 합니다. 백슬래시, 사선, 파이프, 콜론, 별표, 따옴표, 물음표, 여는 대괄호나 닫는 대괄호, 앰퍼샌드 또는 해시 같은 특수 문자를 포함할 수 없습니다.
설명	암호화 키의 설명을 입력합니다. 이 정보는 Core 콘솔에서 암호화 키를 볼 때 Description(설명) 필드에 나타납니다.
암호	액세스 제어에 사용되는 암호를 입력합니다. 모범 사례는 이 표의 이름 설명에 나와 있는 특수 문자가 사용하지 않는 것입니다. 안전한 장소에 암호를 적어 두십시오. Dell 지원에서 암호를 복구할 수 없습니다. 암호화 키를 생성하고 이를 하나 이상의 보호되는 시스템에 적용한 후에는 암호를 분실할 경우 데이터를 복구할 수 없습니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

17 **마침**을 클릭합니다.

Rapid Recovery는 보호되는 시스템의 목록에 선택한 VM 및 해당 호스트를 추가합니다.

보호된 시스템 진단 액세스

Rapid Recovery에서 개별 보호된 시스템에 대한 진단 정보를 다운로드하고 볼 수 있습니다. 또한 Rapid Recovery를 사용하여 Core에 대한 로그 데이터를 다운로드하고 볼 수 있습니다.

로그에 액세스하려면 다음 절차를 참조하십시오.

- Core 로그 파일 다운로드 및 보기
- 보호된 시스템의 로그 파일 다운로드 및 보기

보호된 시스템의 로그 파일 다운로드 및 보기

보호된 시스템에서 오류 또는 문제가 발생할 경우 시스템 로그를 다운로드하여 오류 또는 문제를 확인하거나 Dell 서비스 담당자와 공유할 수 있습니다.

1 Core Console의 왼쪽 탐색 영역의 보호된 시스템 메뉴에서 관련 보호된 시스템에 대한 상황에 맞는 메뉴를 확장하려면 화살표를 클릭합니다. **추가**까지 아래로 스크롤하고 메뉴를 확장한 다음 **에이전트 로그**를 선택합니다.
에이전트 로그 다운로드 페이지가 나타납니다.

2 **에이전트 로그 다운로드** 페이지에서 **다운로드를 시작하려면 여기를 클릭하십시오**를 선택합니다.

3 **AgentAppRecovery.log 열기** 대화 상자에서 다음 중 하나를 수행합니다.
- 로그 파일을 열려면 **연결 프로그램**을 선택하고 텍스트 기반 로그 파일을 볼 수 있는 응용 프로그램(예: 메모장)을 선택한 다음 마지막으로 **확인**을 클릭합니다.
  선택한 응용 프로그램에서 AgentAppRecovery.log 파일이 열립니다.
- 로컬에 파일을 저장하려면 **파일 저장**을 선택한 다음 **확인**을 클릭합니다.
  AgentAppRecovery.log 파일이 Downloads 폴더에 저장됩니다. 이 파일은 텍스트 편집기를 사용하여 열 수 있습니다.

보호된 시스템의 로그 파일 다운로드 및 보기

보호된 시스템에서 오류 또는 문제가 발생할 경우 시스템 로그를 다운로드하여 오류 또는 문제를 확인하거나 Dell 서비스 담당자와 공유할 수 있습니다.

1 Core Console의 왼쪽 탐색 영역의 보호된 시스템 메뉴에서 관련 보호된 시스템에 대한 상황에 맞는 메뉴를 확장하려면 화살표를 클릭합니다. **추가**까지 아래로 스크롤하고 메뉴를 확장한 다음 **에이전트 로그**를 선택합니다.
에이전트 로그 다운로드 페이지가 나타납니다.

2 **에이전트 로그 다운로드** 페이지에서 **다운로드를 시작하려면 여기를 클릭하십시오**를 클릭합니다.

3 **AgentAppRecovery.log 열기** 대화 상자에서 다음 중 하나를 수행합니다.
- 로그 파일을 열려면 **연결 프로그램**을 선택하고 텍스트 기반 로그 파일을 볼 수 있는 응용 프로그램(예: 메모장)을 선택한 다음 마지막으로 **확인**을 클릭합니다.
  선택한 응용 프로그램에서 AgentAppRecovery.log 파일이 열립니다.
- 로컬에 파일을 저장하려면 **파일 저장**을 선택한 다음 **확인**을 클릭합니다.
  AgentAppRecovery.log 파일이 Downloads 폴더에 저장됩니다. 이 파일은 텍스트 편집기를 사용하여 열 수 있습니다.

관련 링크

Core 로그 파일 다운로드 및 보기

시스템 상태 및 기타 상세 정보 보기

시스템에 대한 기타 상세 정보뿐만 아니라 상태를 보려면 이 절차의 단계를 완료하십시오.

Rapid Recovery Core 콘솔에서, 확인할 보호 시스템으로 이동합니다.
시스템에 대한 정보가 Summary(요약) 페이지에 표시됩니다. 표시되는 상세 정보는 다음과 같습니다.

- 호스트 이름
- 마지막으로 생성된 스냅샷
- 예약된 다음 스냅샷
- 암호화 상태
- 버전 번호
  시스템에 Exchange Server가 설치되어 있는 경우, 다음과 같은 서버에 대한 상세 정보도 표시됩니다.
- 마지막 성공한 마운트 기능 검사 수행
- 마지막 성공한 체크섬 검사 수행
- 마지막으로 수행된 로그 자르기
  다음과 같이 이 시스템에 있는 볼륨에 대한 자세한 정보도 나타납니다.
- 볼륨 이름
- Schedule(일정)
- 현재 일정
- 다음 스냅샷
- 파일 시스템 유형
- 총 크기 중 사용한 공간
- 시스템에 SQL Server가 설치되어 있는 경우, 다음과 같은 서버에 대한 자세한 정보도 표시됩니다.

  온라인 상태
- 이름
- 설치 경로
- 버전
  시스템에 Exchange Server가 설치되어 있는 경우, 다음과 같은 서버 및 메일 저장소에 대한 자세한 정보도 나타납니다.
- 버전
- 설치 경로
- 데이터 경로
- 데이터베이스 이름
- Exchange 데이터베이스 경로
- 로그 파일 경로
- 로그 접두사
- 시스템 경로
- 메일 저장소 유형

시스템 관리

이 섹션에서는 시스템을 관리할 때 수행할 수 있는 다양한 작업에 대해 설명합니다. 이 섹션은 다음과 같은 항목으로 구성됩니다.

- 시스템 제거
- 보호에서 클러스터 제거
- 시스템에 대한 라이센스 정보 보기
- 보호된 시스템의 로그 파일 다운로드 및 보기

- 보호된 클러스터 노드를 보호된 시스템으로 변환

시스템 제거

Rapid Recovery Core의 보호에서 시스템을 제거할 때 지금까지 RR Core에 저장된 복구 지점을 유지하거나 복구 지점을 제거하는 두 가지 옵션을 사용할 수 있습니다. 복구 지점을 유지할 경우 "복구 지점만" 시스템으로 알려진 시스템만 사용하게 됩니다. 현재 보호에서 제거된 시스템에 대한 이러한 복구 지점을 사용하여 이후 시스템 복원을 계속할 수 있지만, 저장된 복구 지점에서 캡처된 상태까지만 복원할 수 있습니다.

복구 지점을 제거할 경우, 이 작업의 결과로 이전에 보호된 시스템에 대한 스냅숏 데이터가 Rapid Recovery Core에서 모두 삭제됩니다.

△| 주의: **복구 지점을 삭제할 경우 더 이상 해당 시스템에 대한 데이터를 복원할 수 없습니다.**

Rapid Recovery 환경의 보호에서 시스템을 제거하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 왼쪽 탐색 창에 표시된 Protected Machines(보호된 시스템) 아래에서 제거하려는 시스템을 클릭합니다.
2 관련 시스템에 대한 Summary(요약) 페이지에서 **Remove Machine(시스템 제거)**을 클릭합니다.
3 리포지토리에서도 이 시스템에 대한 모든 복구 지점을 삭제하려면 대화 상자에서 **Remove with recovery points(복구 지점과 함께 제거)**를 선택합니다.
4 시스템을 제거하려는 선택을 확인하기 위해 **Yes(예)**를 클릭합니다.
Rapid Recovery는 이 시스템을 보호 대상에서 제거하고, 이 시스템에 대한 모든 활성 작업을 취소합니다.

시스템에서 작업 취소

현재 실행 중인 시스템의 작업을 취소할 수 있습니다. 현재 스냅숏만 취소 또는 모든 현재 작업(내보내기, 복제 등) 취소 등을 지정할 수 있습니다.

1 Rapid Recovery Core Console에 있는 보호된 시스템의 왼쪽 탐색 영역에서 작업을 취소하려는 시스템을 선택합니다.
2 **이벤트**를 클릭합니다.
3 진행 중인 이벤트나 취소하려는 작업 맨 오른쪽에 있는 작업 세부사항 아이콘을 클릭합니다.
4 진행 중인 작업 모니터 대화 상자에서 **취소**를 클릭합니다.

시스템에 대한 라이센스 정보 보기

보호된 시스템에 설치된 Rapid Recovery Agent 소프트웨어에 대한 현재 라이센스 상태 정보를 볼 수 있습니다.

1 Rapid Recovery Core Console에 있는 보호된 시스템에서 수정하려는 시스템을 클릭합니다.
시스템 선택에 대한 **요약** 페이지가 나타납니다.
2 **설정** 메뉴를 클릭합니다.
선택한 시스템에 대한 구성 설정을 표시하는 **설정** 페이지가 나타납니다.
3 **라이센싱** 링크를 클릭하고 설정 페이지에서 아래쪽으로 스크롤하여 시스템별 라이센싱 설정을 확인합니다.
상태 화면이 나타나고 제품 라이센스에 대한 세부 정보가 표시됩니다.

VM 내보내기

이 장에서는 복구 지점을 내보내 가상 시스템을 만드는 방법에 대해 설명합니다.

Rapid Recovery에서 가상 시스템으로 내보내기 정보

Rapid Recovery Core를 통해 리포지토리에서 가상 시스템으로 복구 지점을 내보낼 수 있습니다. 가상 내보내기라고도 하는 이 프로세스는 복구 지점에서 가상 시스템을 생성하는 P2V(Physical-to-Virtual) 프로세스입니다. VM은 보호된 시스템의 부팅 가능한 클론입니다.

노트: 사용하는 복구 지점은 전체 복구 지점 체인에 속해야 합니다. 복구 지점 체인에 대한 자세한 내용은 복구 지점 체인 및 분리 항목을 참조하십시오.

Core Console에서 가상 대기 페이지를 사용하거나 단추 표시줄에서 **VM 내보내기**(**복원** 드롭다운 메뉴 내)를 선택하여 가상 내보내기를 수행할 수 있습니다.

Rapid Recovery Core에서 가상 내보내기를 수행하는 경우 두 가지 옵션이 있습니다.

- **1회 가상 내보내기**를 수행할 수 있습니다. 즉, 복구 지점의 정보에서 특정 시점 단일 스냅숏을 말합니다.
- **가상 대기**를 생성할 수 있습니다. 가상 대기를 사용하는 경우 선택한 복구 지점에서 생성하는 VM 스냅숏은 소스 시스템에서 강제로 스냅숏을 생성하거나 스케줄에 따라 스냅숏을 생성할 때마다 Core에서 지속적으로 업데이트됩니다. 이를 통해 데이터 복구를 위한 고가용성 리소스를 생성합니다. 보호된 시스템에서 장애가 발생하면 가상 시스템을 부팅하여 신속하게 임시로 원래 시스템을 대체하므로, 가동 중지 시간을 비교적 짧게 유지하면서 원래 보호된 시스템을 복구할 수 있습니다.

다음 도표에는 가상 시스템으로 데이터 내보내기의 일반적인 배포 과정이 나와 있습니다.

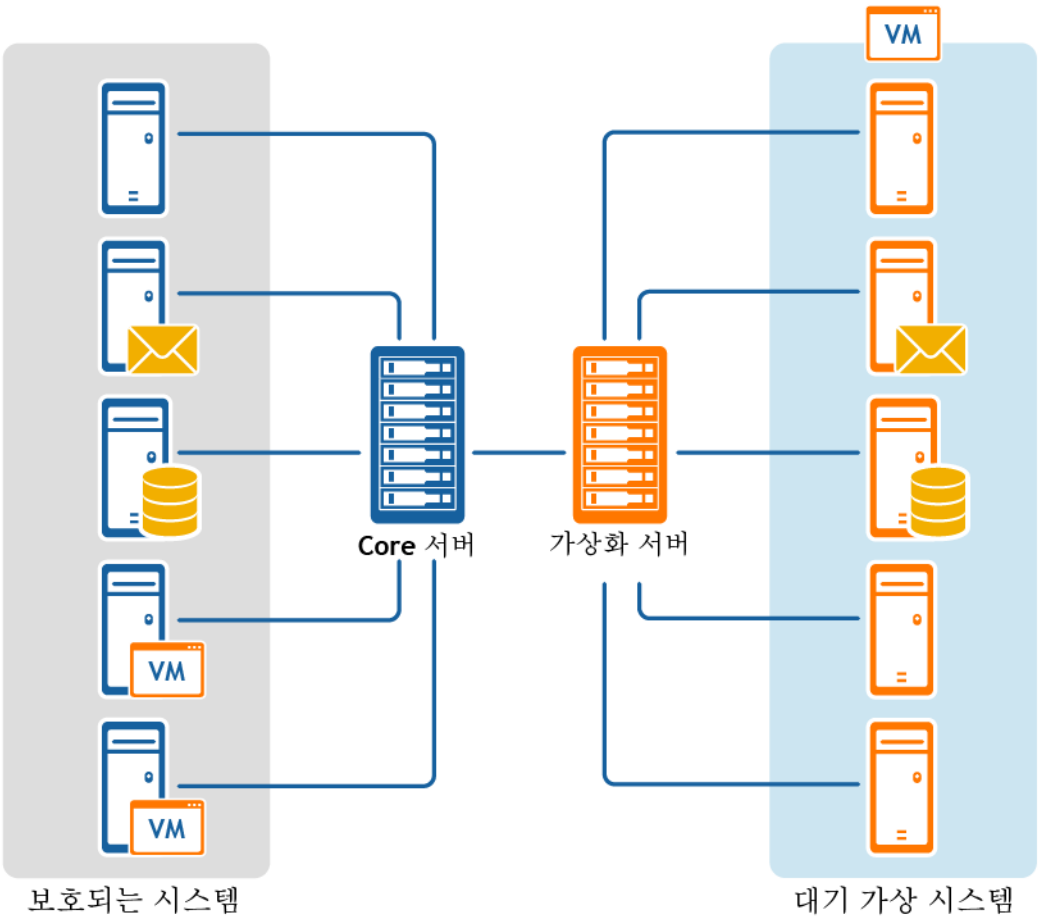


그림 8 . 가상 대기 배포

노트: **구성 관련 복제인 경우 표시되는 Core는 대상 Core입니다.**

가상 시스템으로 내보낼 때 다음 정보를 내보냅니다.

- 복구 지점의 모든 백업 데이터
- 원래 보호된 시스템의 운영 체제 및 설정

VMware, ESXi, Hyper-V 및 VirtualBox로 보호 대상 Windows 또는 Linux 시스템에 대한 복구 지점의 가상 내보내기를 수행할 수 있습니다.

노트: **ESXi, VMware Workstation 또는 Hyper-V의 경우 가상 시스템 버전이 평가판 또는 무료 버전이 아니라 이러한 가상 시스템의 라이센스 버전이어야 합니다.**

두 Core(소스 및 대상) 간에 복제가 설정되어 있으면 초기 복제가 완료된 후 대상 Core의 데이터만 내보낼 수 있습니다.

1회 ESXi 내보내기 수행

ESXi로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 작업 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.

4 Machines(시스템) 페이지에서 내보내려는 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 Recovery Points(복구 지점) 페이지에서 내보낼 복구 지점을 선택한 후 다음을 클릭합니다.
7 **다음**을 클릭합니다.
8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **ESX(i)**를 선택합니다.
9 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력하고 **다음**을 클릭합니다.

표 103. 가상 시스템 매개 변수

옵션	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본값은 443입니다.
사용자 이름	호스트 시스템 로그온에 사용할 사용자 이름을 입력합니다.
암호	호스트 시스템 로그온에 사용할 암호를 입력합니다.

10 가상 시스템 옵션 페이지에 다음 표에 설명된 정보를 입력합니다.

표 104. 가상 시스템 옵션

옵션	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
VM 구성 위치	드롭다운 목록에서 데이터 저장소를 선택합니다.
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.
디스크 프로비저닝	다음 옵션 중에서 디스크 프로비저닝 유형을 선택합니다. • Thin(씬). 씬 프로비저닝은 볼륨 크기 전체가 아니라 원래 볼륨에 사용된 공간 크기의 가상 디스크를 생성합니다. 예를 들어, 원래 볼륨이 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 2GB의 가상 디스크를 생성합니다. • Thick(씩). 씩 프로비저닝은 원래 볼륨의 일부만 사용되고 있더라도 보호된 서버에서 원래 볼륨과 같은 크기의 새 디스크 또는 볼륨을 생성합니다. 예를 들어, 볼륨 크기가 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 1TB의 가상 디스크를 생성합니다.
디스크 매핑	다음 옵션 중에서 디스크 매핑 유형을 지정합니다. • 자동 • 수동 • VM 포함
버전	드롭다운 목록에서 가상 시스템 생성에 사용하려는 ESXi 버전을 선택합니다.

11 **다음**을 클릭합니다.
12 볼륨 페이지에서 내보낼 볼륨을 선택한 후 **다음**을 클릭합니다.
13 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: **Virtual Standby(가상 대기) 또는 Events(이벤트) 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.**

연속(가상 대기) ESXi 내보내기 수행

Rapid Recovery를 사용하여 ESXi 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.

- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 내보내기 마법사의 **대상** 페이지에 있는 가상 시스템으로 복구 드롭다운 메뉴에서 **ESXi**를 선택합니다.

7 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 정보를 입력하고 **다음**을 클릭합니다.

표 105. ESXi 자격 증명

옵션	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본값은 443입니다.
사용자 이름	호스트 시스템의 로그온 자격 증명을 입력합니다.
암호	호스트 시스템의 로그온 자격 증명을 입력합니다.

8 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 다음 표에 설명된 대로 정보를 입력합니다.

표 106. 가상 시스템 옵션

옵션	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
데이터 저장소	드롭다운 목록에서 데이터 저장소를 선택합니다.
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.

옵션	설명
디스크 프로비저닝	다음 옵션 중에서 디스크 프로비저닝 유형을 선택합니다. • Thin(씬). 씬 프로비저닝은 볼륨 크기 전체가 아니라 원래 볼륨에 사용된 공간 크기의 가상 디스크를 생성합니다. 예를 들어, 원래 볼륨이 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 2GB의 가상 디스크를 생성합니다. • Thick(씩). 씩 프로비저닝은 원래 볼륨의 일부만 사용되고 있더라도 보호된 서버에서 원래 볼륨과 같은 크기의 새 디스크 또는 볼륨을 생성합니다. 예를 들어, 볼륨 크기가 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 1TB의 가상 디스크를 생성합니다.
디스크 매핑	디스크 매핑 유형을 적절하게 지정합니다(자동, 수동 또는 VM 사용).
버전	가상 시스템의 버전을 선택합니다.
처음 1회 내보내기를 수행합니다.	다음으로 예약된 스냅숏 후(선택 사항) 대신 즉시 가상 내보내기를 수행하려면 선택합니다.

9 **다음**을 클릭합니다.

10 **볼륨** 페이지에서 내보낼 볼륨을 선택한 후 **다음**을 클릭합니다.

11 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

1회 VMware Workstation 내보내기 수행

VMware Workstation으로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 클릭합니다.

2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.

3 **다음**을 클릭합니다.

4 Machines(시스템) 페이지에서 내보내려는 보호된 시스템을 선택합니다.

5 **다음**을 클릭합니다.

6 Recovery Points(복구 지점) 페이지에서 내보낼 복구 지점을 선택한 후 다음을 클릭합니다.

7 **다음**을 클릭합니다.

8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **VMware Workstation**을 선택한 후 **다음**을 클릭합니다.

9 가상 시스템 옵션 페이지에서 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력합니다.

표 107. 가상 시스템 매개 변수

옵션	설명
VM 시스템 위치	가상 시스템을 만들 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다. **노트: 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
사용자 이름	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 사용자 이름을 입력해야 합니다. • 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.
암호	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 암호를 입력해야 합니다.

옵션	설명
	• 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
VM 이름	만들려는 가상 시스템의 이름(예: VM-0A1B2C3D4)을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
버전	가상 시스템에 대한 VMware Workstation 버전을 지정합니다. 다음 항목 중에서 선택할 수 있습니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
RAM 크기(MB)	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.

10 **다음**을 클릭합니다.

11 볼륨 페이지에서 내보낼 볼륨(예: C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.

12 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 탭을 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) VMware Workstation 내보내기 수행

Rapid Recovery를 사용하여 VMware Workstation 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 가상 시스템 내보내기 마법사의 **대상** 페이지에 있는 가상 시스템으로 복구 드롭다운 메뉴에서 **VMware 워크스테이션**을 선택하고 **다음**을 클릭합니다.

7 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

표 108. 가상 시스템 매개 변수

옵션	설명
대상 경로	가상 시스템을 만들 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다. **노트: 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
사용자 이름	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 사용자 이름을 입력해야 합니다. • 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.
암호	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 암호를 입력해야 합니다. • 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
가상 시스템	만들려는 가상 시스템의 이름(예: VM-0A1B2C3D4)을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
버전	가상 시스템에 대한 VMware Workstation 버전을 지정합니다. 다음 항목 중에서 선택할 수 있습니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.

8 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.
9 **다음**을 클릭합니다.
10 **볼륨** 페이지에서 내보낼 볼륨(C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.
11 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

1회 Hyper-V 내보내기 수행

Hyper-V로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭하고, **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.

3 **다음**을 클릭합니다.
4 **시스템** 페이지에서 내보낼 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택합니다.
7 **다음**을 클릭합니다.
8 **대상** 페이지의 가상 시스템으로 내보내기 드롭다운 메뉴에서 **Hyper-V**를 선택합니다.
9 Hyper-V 역할이 할당된 로컬 시스템으로 내보내려면 **로컬 시스템 사용**을 클릭합니다.
10 Hyper-V 서버가 원격 시스템에 있음을 나타내려면 **원격 호스트**를 클릭한 후 다음 표의 설명에 따라 원격 호스트의 정보를 입력합니다.

표 109. 원격 호스트 정보

텍스트 상자	설명
호스트 이름	Hyper-V 서버의 IP 주소 또는 호스트 이름을 입력합니다. 원격 Hyper-V 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자의 사용자 이름을 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.
암호	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자 계정의 암호를 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.

11 **다음**을 클릭합니다.
12 **가상 시스템 옵션** 페이지의 **VM 시스템 위치** 텍스트 상자에 가상 시스템의 경로(예: D:\export)를 입력합니다. 가상 시스템의 위치를 나타내기 위해 사용됩니다.

노트: 로컬 및 원격 Hyper-V 서버 모두에 대한 가상 시스템 위치를 지정해야 합니다. 경로는 Hyper-V 서버에 대한 유효한 로컬 경로여야 합니다. 존재하지 않는 디렉터리가 자동으로 생성됩니다. 디렉터리를 수동으로 만들면 안 됩니다. 공유 폴더(예: \\data\share)로 내보내기는 허용되지 않습니다.

13 **가상 시스템 이름** 텍스트 상자에 가상 시스템의 이름을 입력합니다.
입력한 이름이 Hyper-V Manager 콘솔의 가상 시스템 목록에 나타납니다.
14 메모리 사용량을 지정하려면 다음 중 하나를 클릭하십시오.
- **원본 시스템과 동일한 RAM 크기 사용**. 가상 시스템과 원본 시스템 사이에 동일한 RAM을 사용하고 있는지 식별하려면 이 옵션을 선택합니다.
- **특정 RAM 크기 사용.** RAM 크기를 MB 단위로 지정하려면 이 옵션을 선택합니다.
  최소 크기는 1024MB이고, 응용 프로그램에서 허용하는 최대 크기는 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

15 디스크 형식을 지정하려면 디스크 형식 옆에서 다음 중 하나를 클릭합니다.
- VHDX
- VHD

노트: Hyper-V 내보내기는 대상 시스템에서 Windows 8(Windows Server 2012) 이상을 실행하는 경우 VHDX 디스크 형식을 지원합니다. VHDX가 지원되지 않는 환경의 경우 옵션이 비활성화됩니다.
Hyper-V 2세대로 내보낼 경우 VHDX 디스크 형식만 지원됩니다.

16 내보내기에 사용할 Hyper-V 세대를 지정하려면 다음 항목 중 하나를 클릭합니다.
- 1세대
- 2세대

노트: 2세대만 보안 부트 옵션을 지원합니다.
17 내보낸 VM에 대한 해당 네트워크 어댑터를 지정합니다.
18 **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다(예: C:\).

노트: 선택한 볼륨이 아래에 표시된 대로 응용프로그램에서 지원하는 적절한 최대 할당보다 크거나 사용 가능한 공간을 초과할 경우 오류가 발생합니다.

- VHDX 디스크 형식의 경우 선택한 볼륨은 64TB보다 크지 않아야 합니다.
- VHD 디스크 형식의 경우 선택한 볼륨은 2040GB보다 크지 않아야 합니다.

19 **볼륨** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) Hyper-V 내보내기 수행

Rapid Recovery를 사용하는 Hyper-V 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료합니다.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭한 후 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 시작합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보낼 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택합니다.

5 **다음**을 클릭합니다.

6 **대상** 페이지의 가상 시스템으로 내보내기 드롭다운 메뉴에서 **Hyper-V**를 선택한 후 다음 중 하나를 수행합니다.

- Hyper-V 역할이 할당된 로컬 시스템으로 내보내려면 **로컬 시스템 사용**을 클릭합니다.
- Hyper-V 서버가 원격 시스템에 있음을 나타내려면 **원격 호스트**를 클릭한 후 다음 표의 설명에 따라 원격 호스트의 매개 변수를 입력합니다.

표 110. 원격 호스트 정보

텍스트 상자	설명
호스트 이름	Hyper-V 서버의 IP 주소 또는 호스트 이름을 입력합니다. 원격 Hyper-V 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자의 사용자 이름을 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.
암호	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자 계정의 암호를 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.

7 **다음**을 클릭합니다.

8 **가상 시스템 옵션** 페이지의 **VM 시스템 위치** 텍스트 상자에 가상 시스템의 경로(예: D:\export)를 입력합니다. 가상 시스템의 위치를 나타내기 위해 사용됩니다.

노트: 로컬 및 원격 Hyper-V 서버 모두에 대한 가상 시스템 위치를 지정해야 합니다. 경로는 Hyper-V 서버에 대한 유효한 로컬 경로여야 합니다. 존재하지 않는 디렉터리가 자동으로 생성됩니다. 디렉터리를 수동으로 만들면 안 됩니다. 공유 폴더(예: \\data\share)로 내보내기는 허용되지 않습니다.

9 **가상 시스템 이름** 텍스트 상자에 가상 시스템의 이름을 입력합니다.
입력한 이름이 Hyper-V Manager 콘솔의 가상 시스템 목록에 나타납니다.

10 메모리 사용량을 지정하려면 다음 중 하나를 클릭하십시오.

- **원본 시스템과 동일한 RAM 크기 사용**. 가상 시스템과 원래 시스템 사이에 동일한 RAM을 사용하고 있는지 식별하려면 이 옵션을 선택합니다.
- **특정 RAM 크기 사용.** RAM 크기를 MB 단위로 지정하려면 이 옵션을 선택합니다.
  최소 크기는 1024MB이고, 응용 프로그램에서 허용하는 최대 크기는 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

11 디스크 형식을 지정하려면 디스크 형식 옆에서 다음 중 하나를 클릭합니다.
- VHDX
- VHD

> **노트: Hyper-V 내보내기는 대상 시스템에서 Windows 8(Windows Server 2012) 이상을 실행하는 경우 VHDX 디스크 형식을 지원합니다. VHDX가 지원되지 않는 환경의 경우 옵션이 비활성화됩니다.**
> Hyper-V 2세대로 내보낼 경우 VHDX 디스크 형식만 지원됩니다.

12 내보내기에 사용할 Hyper-V 세대를 지정하려면 다음 항목 중 하나를 클릭합니다.
- 1세대
- 2세대

> **노트: 2세대만 보안 부트 옵션을 지원합니다.**

13 내보낸 VM에 대한 해당 네트워크 어댑터를 지정합니다.
14 **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다(예: C:\).

> **노트: 선택한 볼륨이 아래에 표시된 대로 응용프로그램에서 지원하는 적절한 최대 할당보다 크거나 사용 가능한 공간을 초과할 경우 오류가 발생합니다.**

- VHDX 디스크 형식의 경우 선택한 볼륨은 64TB보다 크지 않아야 합니다.
- VHD 디스크 형식의 경우 선택한 볼륨은 2040GB보다 크지 않아야 합니다.

15 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.
16 **볼륨** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

> **노트: 가상 대기 또는 이벤트 페이지를 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.**

1회 VirtualBox 내보내기 수행

VirtualBox로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭하고 **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.
4 시스템 페이지에서 내보내려는 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 복구 지점 페이지에서 내보내기에 사용하려는 복구 지점을 선택합니다.
7 **다음**을 클릭합니다.
8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **VirtualBox**를 선택한 후 **다음**을 클릭합니다.
9 가상 시스템 옵션 페이지에서 **Windows 컴퓨터 사용**을 선택합니다.
10 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력합니다.

표 111. 가상 시스템 매개 변수

옵션	설명
가상 시스템 이름	만들려는 가상 시스템의 이름을 입력합니다.

옵션	설명
	노트: 기본 이름은 소스 시스템의 이름입니다.
대상 경로	가상 시스템을 만들기 위한 로컬 또는 원격 대상 경로를 지정합니다. **노트: 대상 경로는 루트 디렉터리가 아니어야 합니다.** **네트워크 공유 경로를 지정하는 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명(사용자 이름과 암호)을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

11 가상 시스템에 대한 사용자 계정을 지정하려면 **내보낸 가상 시스템의 사용자 계정을 지정합니다**를 선택한 후 다음 정보를 입력합니다. 이 계정은 가상 시스템에 여러 개의 사용자 계정이 있는 경우 가상 시스템이 등록될 특정 사용자 계정을 가리킵니다. 이 사용자 계정이 로그온된 경우 해당 사용자만 VirtualBox 관리자에서 이 가상 시스템을 볼 수 있습니다. 계정이 지정되지 않은 경우 VirtualBox가 설치된 Windows 컴퓨터의 모든 기존 사용자에 대해 가상 시스템이 등록됩니다.

- 사용자 이름 - 가상 시스템이 등록되는 사용자 이름을 입력합니다.
- 암호 - 이 사용자 계정의 암호를 입력합니다.

12 **다음**을 클릭합니다.

13 볼륨 페이지에서 내보낼 볼륨(예: C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.

14 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 탭을 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) VirtualBox 내보내기 수행

이 단계를 수행하려면 VirtualBox가 Core 시스템에 설치되어 있어야 합니다.

Rapid Recovery를 사용하여 VirtualBox 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 내보내기 마법사의 **대상** 페이지에 있는 **가상 시스템으로 복구** 드롭다운 메뉴에서 **VirtualBox**를 선택합니다.

7 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서 **Remote Linux Machine(원격 Linux 시스템)**을 선택합니다.

8 다음 표의 설명에 따라 가상 시스템에 대한 정보를 입력합니다.

표 112. 원격 Linux 시스템 설정

옵션	설명
VirtualBox 호스트 이름	VirtualBox 서버의 IP 주소 또는 호스트 이름을 입력합니다. 이 필드는 원격 VirtualBox 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. 이 번호는 Core가 이 시스템과 통신하는 포트를 나타냅니다.
가상 시스템 이름	만들려는 가상 시스템의 이름을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
대상 경로	가상 시스템을 만들기 위한 대상 경로를 지정합니다. **노트: 루트에서 루트 폴더를 만들어 가상 시스템이 루트에서 실행되도록 하는 것이 좋습니다. 루트를 사용하지 않는 경우 내보내기를 설정하기 전에 대상 시스템에 수동으로 대상 폴더를 만들어야 합니다. 또한 내보내기 후 수동으로 가상 시스템을 연결하거나 로드해야 합니다.**
사용자 이름	대상 시스템의 계정에 대한 사용자 이름(예: root).
암호	대상 시스템의 사용자 계정 암호.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

9 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.

10 **다음**을 클릭합니다.

11 **Volumes(볼륨)** 페이지에서, 내보낼 데이터의 볼륨을 선택하고 **Next(다음)**를 클릭합니다.

12 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

내보내기 관리

Core에 가상 내보내기가 설정되어 있으면 각 가상 내보내기에 대한 구성 매개변수가 **가상 대기** 페이지에 행으로 표시됩니다. 여기에서 현재 설정한 내보내기 상태를 보고 가상 대기 시스템을 관리할 수 있습니다. 가상 대기를 추가하거나, 내보내기를 수행하거나, 가상 대기를 일시 중지 또는 재개하거나, 연속 내보내기에 대한 요구를 제거할 수 있습니다.

1회 내보내기가 수행되면 작업이 **가상 대기** 페이지의 내보내기 대기열에 나열됩니다. 이 시간 동안 내보내기 작업을 일시 중지, 재개 또는 취소할 수 있습니다.

노트: Rapid Recovery는 Window 8, Window 8.1, Windows Server 2012 및 2012 R2로 Hyper-V 내보내기를 지원합니다.

VM의 전원이 켜져 있으면 가상 대기 VM으로 가상 내보내기가 수행되지 않습니다.

가상 내보내기를 관리하려면 이 절차의 단계를 완료합니다.

1 Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
가상 대기 페이지가 나타납니다. 여기서 두 개의 저장된 내보내기 설정 표를 볼 수 있습니다. 다음 표에 설명된 정보를 포함합니다.

표 113. 가상 대기 정보

열	설명
항목 선택	요약 표에 있는 각 행의 확인란을 선택하고 표 앞에 있는 메뉴 옵션 목록에서 작업을 수행할 수 있습니다.
상태 표시기	상태 열의 색상 영역은 가상 대기의 상태를 나타냅니다. 색상 원으로 커서를 가져가면 상태 조건이 표시됩니다. · 녹색. 가상 대기가 성공적으로 구성되고 활성화되었으며 일시 중지되지 않았습니다. 다음 스냅숏이 완료되는 즉시 다음 내보내기가 수행됩니다. · 노란색. 가상 대기가 일시 중지되었지만 매개변수는 Core에 정의되고 저장된 채로 남아 있습니다. 그러나 새로운 전송 후에 내보내기 작업이 자동으로 시작되지 않고 상태가 변경될 때까지 보호된 시스템에 대해 새로운 내보내기가 없습니다.
시스템 이름	소스 시스템의 이름.
대상	데이터를 내보내는 가상 시스템 및 경로.
내보내기 유형	내보내기를 위한 가상 시스템 유형(예: ESXi, VMware, Hyper-V 또는 VirtualBox).
마지막 내보내기	마지막 내보내기의 날짜와 시간. 내보내기가 추가되었지만 완료되지 않은 경우 내보내기가 아직 수행되지 않았다는 메시지가 표시됩니다. 내보내기가 실패하거나 취소되면 해당 메시지도 표시됩니다.
설정	드롭다운 메뉴에서 다음 기능을 수행할 수 있습니다. · **편집**. 가상 대기 설정을 편집할 수 있습니다. · **수행**. 가상 내보내기를 수행합니다. · **일시 중지**. 가상 내보내기를 일시 중지합니다. 활성 상태일 때만 사용할 수 있습니다. · **재개**. 가상 내보내기를 재개합니다. 일지 중지 상태일 때만 사용할 수 있습니다. · **제거**. 연속 내보내기에 대한 요구를 제거합니다. 가장 최근에 업데이트된 내보낸 VM은 제거되지 않습니다.

표 114. 내보내기 대기열 정보

열	설명
항목 선택	요약 표에 있는 각 행의 확인란을 선택하고 표 앞에 있는 메뉴 옵션 목록에서 작업을 수행할 수 있습니다.
대상	데이터를 내보내는 가상 시스템 및 경로.
내보내기 유형	내보내기를 위한 가상 시스템 유형(예: ESXi, VMware, Hyper-V 또는 VirtualBox).
일정 유형	내보내기 유형(1회 또는 연속).
상태	내보내기의 진행 상황으로, 진행률 표시줄에 백분율로 표시됩니다.

2 저장된 내보내기 설정을 관리하려면 내보내기를 선택한 후 다음 중 하나를 클릭합니다.

· **편집**. **가상 시스템 내보내기 마법사**에서 **VM 옵션** 페이지를 엽니다. 여기서 내보낸 VM의 위치를 변경하거나, VM 유형의 버전을 변경하거나, 내보내기를 위한 RAM 또는 프로세서를 지정할 수 있습니다. VM 내보내기를 바로 시작하려면 **최초 1회 내보내기 수행**을 선택합니다.

·

· **수행**. 새 내보내기를 수행합니다. 이 옵션은 가상 대기가 일시 중지된 다음 다시 시작된 경우에만 유용할 수 있습니다. 즉, 새로운 전송 후에만 내보내기 작업이 다시 시작됩니다. 새 전송을 기다리지 않으려는 경우 내보내기를 수행할 수 있습니다.

· **일시 중지**. 활성 내보내기를 일시 중지합니다.

· **재개**. 다음으로 예약되거나 수행된 스냅숏에서 연속 내보내기에 대한 요구를 재개합니다.

3 시스템에서 내보내기를 제거하려면 내보내기를 선택한 후 **제거**를 클릭합니다.

내보내기 구성이 시스템에서 영구적으로 제거됩니다. 가상 대기 구성을 제거해도 구성 결과로 내보낸 가상 시스템은 제거되지 않습니다.

4 동시에 실행할 수 있는 내보내기 수를 관리하려면 다음을 수행합니다.
   - 내보내기 대기열 아래에서 **설정**을 클릭합니다.
   - **최대 동시 내보내기** 대화 상자에 동시에 실행할 내보내기 수를 입력합니다. 기본 숫자는 5입니다.
   - **저장**을 클릭합니다.
5 현재 내보내기 대기열에 나열된 1회 또는 연속 내보내기를 취소하려면 내보내기를 선택한 후 **취소**를 클릭합니다.
6 새 가상 대기 내보내기를 추가하려면 **추가**를 클릭하여 내보내기 마법사를 실행합니다. 특정 가상 시스템의 가상 대기 설정에 대한 자세한 내용은 다음 항목 중 하나를 참조하십시오.
   - ESXi 가상 시스템으로 데이터 내보내기
   - VMware Workstation 가상 시스템으로 데이터 내보내기
   - Hyper-V 가상 시스템으로 데이터 내보내기
   - VirtualBox 가상 시스템으로 데이터 내보내기

ESXi 가상 시스템으로 데이터 내보내기

Rapid Recovery에서 1회 내보내기를 수행하거나 연속 내보내기(가상 대기의 경우)를 설정하여 ESXi를 통해 데이터를 내보낼 수 있습니다. 적절한 내보내기 유형에 대한 해당 단계를 완료합니다.

1회 ESXi 내보내기 수행

ESXi로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 작업 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.
4 Machines(시스템) 페이지에서 내보내려는 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 Recovery Points(복구 지점) 페이지에서 내보낼 복구 지점을 선택한 후 다음을 클릭합니다.
7 **다음**을 클릭합니다.
8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **ESX(i)**를 선택합니다.
9 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력하고 **다음**을 클릭합니다.

표 115. 가상 시스템 매개 변수

옵션	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본값은 443입니다.
사용자 이름	호스트 시스템 로그온에 사용할 사용자 이름을 입력합니다.
암호	호스트 시스템 로그온에 사용할 암호를 입력합니다.

10 가상 시스템 옵션 페이지에 다음 표에 설명된 정보를 입력합니다.

표 116. 가상 시스템 옵션

옵션	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
VM 구성 위치	드롭다운 목록에서 데이터 저장소를 선택합니다.

옵션	설명
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. · 소스 시스템과 동일한 양의 RAM 사용 · 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.
디스크 프로비저닝	다음 옵션 중에서 디스크 프로비저닝 유형을 선택합니다. · Thin(씬). 씬 프로비저닝은 볼륨 크기 전체가 아니라 원래 볼륨에 사용된 공간 크기의 가상 디스크를 생성합니다. 예를 들어, 원래 볼륨이 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 2GB의 가상 디스크를 생성합니다. · Thick(씩). 씩 프로비저닝은 원래 볼륨의 일부만 사용되고 있더라도 보호된 서버에서 원래 볼륨과 같은 크기의 새 디스크 또는 볼륨을 생성합니다. 예를 들어, 볼륨 크기가 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 1TB의 가상 디스크를 생성합니다.
디스크 매핑	다음 옵션 중에서 디스크 매핑 유형을 지정합니다. · 자동 · 수동 · VM 포함
버전	드롭다운 목록에서 가상 시스템 생성에 사용하려는 ESXi 버전을 선택합니다.

11 **다음**을 클릭합니다.

12 볼륨 페이지에서 내보낼 볼륨을 선택한 후 **다음**을 클릭합니다.

13 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: **Virtual Standby(가상 대기) 또는 Events(이벤트) 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.**

연속(가상 대기) ESXi 내보내기 수행

Rapid Recovery를 사용하여 ESXi 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 내보내기 마법사의 **대상** 페이지에 있는 가상 시스템으로 복구 드롭다운 메뉴에서 **ESXi**를 선택합니다.

7 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 정보를 입력하고 **다음**을 클릭합니다.

표 117. ESXi 자격 증명

옵션	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본값은 443입니다.
사용자 이름	호스트 시스템의 로그온 자격 증명을 입력합니다.
암호	호스트 시스템의 로그온 자격 증명을 입력합니다.

8 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 다음 표에 설명된 대로 정보를 입력합니다.

표 118. 가상 시스템 옵션

옵션	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
데이터 저장소	드롭다운 목록에서 데이터 저장소를 선택합니다.
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.
디스크 프로비저닝	다음 옵션 중에서 디스크 프로비저닝 유형을 선택합니다. • Thin(씬). 씬 프로비저닝은 볼륨 크기 전체가 아니라 원래 볼륨에 사용된 공간 크기의 가상 디스크를 생성합니다. 예를 들어, 원래 볼륨이 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 2GB의 가상 디스크를 생성합니다. • Thick(씩). 씩 프로비저닝은 원래 볼륨의 일부만 사용되고 있더라도 보호된 서버에서 원래 볼륨과 같은 크기의 새 디스크 또는 볼륨을 생성합니다. 예를 들어, 볼륨 크기가 1TB이지만 사용된 공간의 2GB만 포함되어 있는 경우 Rapid Recovery는 1TB의 가상 디스크를 생성합니다.
디스크 매핑	디스크 매핑 유형을 적절하게 지정합니다(자동, 수동 또는 VM 사용).
버전	가상 시스템의 버전을 선택합니다.
처음 1회 내보내기를 수행합니다.	다음으로 예약된 스냅숏 후(선택 사항) 대신 즉시 가상 내보내기를 수행하려면 선택합니다.

9 **다음**을 클릭합니다.

10 **볼륨** 페이지에서 내보낼 볼륨을 선택한 후 **다음**을 클릭합니다.

11 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

VirtualBox 가상 시스템으로 데이터 내보내기

Rapid Recovery에서 1회 내보내기를 수행하거나 연속 내보내기(가상 대기의 경우)를 설정하여 VirtualBox 내보내기를 통해 데이터를 내보낼 수 있습니다.

노트: Windows 10을 사용하는 보호된 시스템에서 VirtualBox 내보내기는 현재 지원되지 않습니다.

적절한 내보내기 유형에 대한 해당 단계를 완료합니다.

노트: 이러한 유형의 내보내기를 수행하려면 Core 시스템에 VirtualBox가 설치되어 있어야 합니다. Windows 호스트에서 VirtualBox 버전 4.2.18 이상이 지원됩니다.

1회 VirtualBox 내보내기 수행

VirtualBox로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭하고 **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.
4 시스템 페이지에서 내보내려는 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 복구 지점 페이지에서 내보내기에 사용하려는 복구 지점을 선택합니다.
7 **다음**을 클릭합니다.
8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **VirtualBox**를 선택한 후 **다음**을 클릭합니다.
9 가상 시스템 옵션 페이지에서 **Windows 컴퓨터 사용**을 선택합니다.
10 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력합니다.

표 119. 가상 시스템 매개 변수

옵션	설명
가상 시스템 이름	만들려는 가상 시스템의 이름을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
대상 경로	가상 시스템을 만들기 위한 로컬 또는 원격 대상 경로를 지정합니다. **노트: 대상 경로는 루트 디렉터리가 아니어야 합니다.** **네트워크 공유 경로를 지정하는 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명(사용자 이름과 암호)을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

11 가상 시스템에 대한 사용자 계정을 지정하려면 **내보낸 가상 시스템의 사용자 계정을 지정합니다**를 선택한 후 다음 정보를 입력합니다. 이 계정은 가상 시스템에 여러 개의 사용자 계정이 있는 경우 가상 시스템이 등록될 특정 사용자 계정을 가리킵니다. 이 사용자 계정이 로그온된 경우 해당 사용자만 VirtualBox 관리자에서 이 가상 시스템을 볼 수 있습니다. 계정이 지정되지 않은 경우 VirtualBox가 설치된 Windows 컴퓨터의 모든 기존 사용자에 대해 가상 시스템이 등록됩니다.
   • 사용자 이름 - 가상 시스템이 등록되는 사용자 이름을 입력합니다.
   • 암호 - 이 사용자 계정의 암호를 입력합니다.
12 **다음**을 클릭합니다.
13 볼륨 페이지에서 내보낼 볼륨(예: C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.
14 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 탭을 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) VirtualBox 내보내기 수행

이 단계를 수행하려면 VirtualBox가 Core 시스템에 설치되어 있어야 합니다.

Rapid Recovery를 사용하여 VirtualBox 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 내보내기 마법사의 **대상** 페이지에 있는 **가상 시스템으로 복구** 드롭다운 메뉴에서 **VirtualBox**를 선택합니다.

7 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서 **Remote Linux Machine(원격 Linux 시스템)**을 선택합니다.

8 다음 표의 설명에 따라 가상 시스템에 대한 정보를 입력합니다.

표 120. 원격 Linux 시스템 설정

옵션	설명
VirtualBox 호스트 이름	VirtualBox 서버의 IP 주소 또는 호스트 이름을 입력합니다. 이 필드는 원격 VirtualBox 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. 이 번호는 Core가 이 시스템과 통신하는 포트를 나타냅니다.
가상 시스템 이름	만들려는 가상 시스템의 이름을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
대상 경로	가상 시스템을 만들기 위한 대상 경로를 지정합니다. **노트: 루트에서 루트 폴더를 만들어 가상 시스템이 루트에서 실행되도록 하는 것이 좋습니다. 루트를 사용하지 않는 경우 내보내기를 설정하기 전에 대상 시스템에 수동으로 대상 폴더를 만들어야 합니다. 또한 내보내기 후 수동으로 가상 시스템을 연결하거나 로드해야 합니다.**
사용자 이름	대상 시스템의 계정에 대한 사용자 이름(예: root).
암호	대상 시스템의 사용자 계정 암호.
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

9 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.

10 **다음**을 클릭합니다.

11 **Volumes(볼륨)** 페이지에서, 내보낼 데이터의 볼륨을 선택하고 **Next(다음)**를 클릭합니다.

12 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

VMware Workstation 가상 시스템으로 데이터 내보내기

Rapid Recovery에서 1회 내보내기를 수행하거나 연속 내보내기(가상 대기의 경우)를 설정하여 VMware Workstation을 통해 데이터를 내보낼 수 있습니다. 적절한 내보내기 유형에 대한 해당 단계를 완료합니다.

1회 VMware Workstation 내보내기 수행

VMware Workstation으로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.
4 Machines(시스템) 페이지에서 내보내려는 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 Recovery Points(복구 지점) 페이지에서 내보낼 복구 지점을 선택한 후 다음을 클릭합니다.
7 **다음**을 클릭합니다.
8 내보내기 마법사의 대상 페이지에 있는 가상 시스템에 복구 드롭다운 메뉴에서 **VMware Workstation**을 선택한 후 **다음**을 클릭합니다.
9 가상 시스템 옵션 페이지에서 다음 표의 설명에 따라 가상 시스템에 액세스하기 위한 매개 변수를 입력합니다.

표 121. 가상 시스템 매개 변수

옵션	설명
VM 시스템 위치	가상 시스템을 만들 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다. **노트: 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
사용자 이름	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 사용자 이름을 입력해야 합니다. • 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.
암호	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 암호를 입력해야 합니다. • 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
VM 이름	만들려는 가상 시스템의 이름(예: VM-0A1B2C3D4)을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
버전	가상 시스템에 대한 VMware Workstation 버전을 지정합니다. 다음 항목 중에서 선택할 수 있습니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0

옵션	설명
RAM 크기(MB)	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. · 소스 시스템과 동일한 양의 RAM 사용 · 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.

10 **다음**을 클릭합니다.

11 볼륨 페이지에서 내보낼 볼륨(예: C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.

12 요약 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 탭을 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) VMware Workstation 내보내기 수행

Rapid Recovery를 사용하여 VMware Workstation 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 표시줄에서 **복원** 드롭다운 메뉴를 클릭한 다음 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 실행합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보내려는 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택한 후

5 **다음**을 클릭합니다.

6 가상 시스템 내보내기 마법사의 **대상** 페이지에 있는 가상 시스템으로 복구 드롭다운 메뉴에서 **VMware 워크스테이션**을 선택하고 **다음**을 클릭합니다.

7 **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

표 122. 가상 시스템 매개 변수

옵션	설명
대상 경로	가상 시스템을 만들 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다. **노트: 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 로그온 자격 증명을 입력해야 합니다. 계정에는 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.**
사용자 이름	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. · 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 사용자 이름을 입력해야 합니다. · 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.

옵션	설명
암호	내보내기를 위한 네트워크 위치에 대한 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록되는 계정에 대해 유효한 암호를 입력해야 합니다. • 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
가상 시스템	만들려는 가상 시스템의 이름(예: VM-0A1B2C3D4)을 입력합니다. **노트: 기본 이름은 소스 시스템의 이름입니다.**
버전	가상 시스템에 대한 VMware Workstation 버전을 지정합니다. 다음 항목 중에서 선택할 수 있습니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0 • VMware Workstation 10.0 • VMware Workstation 11.0 • VMware Workstation 12.0
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • 소스 시스템과 동일한 양의 RAM 사용 • 특정 양의 RAM 사용을 선택한 후 양(MB)을 지정 최소 양은 1024MB이고, 응용프로그램에서 허용하는 최대 양은 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.
프로세서 개수	내보낸 가상 시스템에 원하는 프로세서(CPU) 수입니다. 최소값은 1입니다.
프로세서당 코어 개수	각 프로세서에 탑재하려는 코어 수입니다. 최소값은 1입니다.

8 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.

9 **다음**을 클릭합니다.

10 **볼륨** 페이지에서 내보낼 볼륨(C:\ 및 D:\)을 선택한 후 **다음**을 클릭합니다.

11 **요약** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 보고 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

Hyper-V 가상 시스템으로 데이터 내보내기

Rapid Recovery에서 1회 내보내기를 수행하거나 연속 내보내기(가상 대기의 경우)를 설정하여 Hyper-V 내보내기를 통해 데이터를 내보낼 수 있습니다.

Rapid Recovery는 다음 호스트에 대한 1세대 Hyper-V 내보내기를 지원합니다.

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Rapid Recovery는 다음 호스트에 대한 2세대 Hyper-V 내보내기를 지원합니다.

- Windows 8.1
- Windows Server 2012 R2

노트: 일부 보호 대상 시스템은 Hyper-V 2세대 호스트로 내보낼 수 없습니다.

다음 UEFI(Unified Extensible Firmware Interface) 운영 체제가 설치된 보호 대상 시스템만 Hyper-V 2세대 호스트에 대한 가상 내보내기를 지원합니다.

- Windows 8(UEFI)
- Windows 8.1(UEFI)
- Windows Server 2012(UEFI)
- Windows Server 2012 R2(UEFI)

노트: 2세대 VM으로 Hyper-V 내보내기는 Hyper-V 호스트에 내보내기를 수행하기 위해 할당된 RAM이 충분하지 않다면 실패할 수 있습니다.

적절한 내보내기 유형에 대한 해당 단계를 완료합니다.

1회 Hyper-V 내보내기 수행

Hyper-V로 1회 내보내기를 수행하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭하고, **VM 내보내기**를 클릭합니다.
2 가상 시스템 내보내기 마법사에서 **1회 내보내기**를 선택합니다.
3 **다음**을 클릭합니다.
4 **시스템** 페이지에서 내보낼 보호된 시스템을 선택합니다.
5 **다음**을 클릭합니다.
6 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택합니다.
7 **다음**을 클릭합니다.
8 **대상** 페이지의 가상 시스템으로 내보내기 드롭다운 메뉴에서 **Hyper-V**를 선택합니다.
9 Hyper-V 역할이 할당된 로컬 시스템으로 내보내려면 **로컬 시스템 사용**을 클릭합니다.
10 Hyper-V 서버가 원격 시스템에 있음을 나타내려면 **원격 호스트**를 클릭한 후 다음 표의 설명에 따라 원격 호스트의 정보를 입력합니다.

표 123. 원격 호스트 정보

텍스트 상자	설명
호스트 이름	Hyper-V 서버의 IP 주소 또는 호스트 이름을 입력합니다. 원격 Hyper-V 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자의 사용자 이름을 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.
암호	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자 계정의 암호를 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.

11 **다음**을 클릭합니다.
12 **가상 시스템 옵션** 페이지의 **VM 시스템 위치** 텍스트 상자에 가상 시스템의 경로(예: D:\export)를 입력합니다. 가상 시스템의 위치를 나타내기 위해 사용됩니다.

노트: 로컬 및 원격 Hyper-V 서버 모두에 대한 가상 시스템 위치를 지정해야 합니다. 경로는 Hyper-V 서버에 대한 유효한 로컬 경로여야 합니다. 존재하지 않는 디렉터리가 자동으로 생성됩니다. 디렉터리를 수동으로 만들면 안 됩니다. 공유 폴더(예: \\data\share)로 내보내기는 허용되지 않습니다.

13 **가상 시스템 이름** 텍스트 상자에 가상 시스템의 이름을 입력합니다.
입력한 이름이 Hyper-V Manager 콘솔의 가상 시스템 목록에 나타납니다.
14 메모리 사용량을 지정하려면 다음 중 하나를 클릭하십시오.
- **원본 시스템과 동일한 RAM 크기 사용**. 가상 시스템과 원본 시스템 사이에 동일한 RAM을 사용하고 있는지 식별하려면 이 옵션을 선택합니다.

- **특정 RAM 크기 사용.** RAM 크기를 MB 단위로 지정하려면 이 옵션을 선택합니다.
  최소 크기는 1024MB이고, 응용 프로그램에서 허용하는 최대 크기는 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

15 디스크 형식을 지정하려면 디스크 형식 옆에서 다음 중 하나를 클릭합니다.

- VHDX
- VHD

노트: Hyper-V 내보내기는 대상 시스템에서 Windows 8(Windows Server 2012) 이상을 실행하는 경우 VHDX 디스크 형식을 지원합니다. VHDX가 지원되지 않는 환경의 경우 옵션이 비활성화됩니다.
Hyper-V 2세대로 내보낼 경우 VHDX 디스크 형식만 지원됩니다.

16 내보내기에 사용할 Hyper-V 세대를 지정하려면 다음 항목 중 하나를 클릭합니다.

- 1세대
- 2세대

노트: 2세대만 보안 부트 옵션을 지원합니다.

17 내보낸 VM에 대한 해당 네트워크 어댑터를 지정합니다.

18 **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다(예: C:\).

노트: 선택한 볼륨이 아래에 표시된 대로 응용프로그램에서 지원하는 적절한 최대 할당보다 크거나 사용 가능한 공간을 초과할 경우 오류가 발생합니다.

- VHDX 디스크 형식의 경우 선택한 볼륨은 64TB보다 크지 않아야 합니다.
- VHD 디스크 형식의 경우 선택한 볼륨은 2040GB보다 크지 않아야 합니다.

19 **볼륨** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

연속(가상 대기) Hyper-V 내보내기 수행

Rapid Recovery를 사용하는 Hyper-V 가상 시스템(VM)으로 연속 내보내기를 수행하려면 이 절차의 단계를 완료합니다.

1 Rapid Recovery Core Console에서 다음 중 하나를 수행합니다.

- Core Console의 단추 모음에서 **복원** 드롭다운 메뉴를 클릭한 후 **VM 내보내기**를 선택합니다.
  1 가상 시스템 내보내기 마법사에서 **연속(가상 대기)**을 선택합니다.
  2 **다음**을 클릭합니다.
- Core Console의 아이콘 표시줄에서 (가상 대기)를 클릭합니다.
  - **가상 대기** 페이지에서 **추가**를 클릭하여 가상 시스템 내보내기 마법사를 시작합니다.

2 가상 시스템 내보내기 마법사의 **시스템** 페이지에서 내보낼 보호된 시스템을 선택합니다.

3 **다음**을 클릭합니다.

4 **복구 지점** 페이지에서 내보내기에 사용할 복구 지점을 선택합니다.

5 **다음**을 클릭합니다.

6 **대상** 페이지의 가상 시스템으로 내보내기 드롭다운 메뉴에서 **Hyper-V**를 선택한 후 다음 중 하나를 수행합니다.

- Hyper-V 역할이 할당된 로컬 시스템으로 내보내려면 **로컬 시스템 사용**을 클릭합니다.
- Hyper-V 서버가 원격 시스템에 있음을 나타내려면 **원격 호스트**를 클릭한 후 다음 표의 설명에 따라 원격 호스트의 매개 변수를 입력합니다.

표 124. 원격 호스트 정보

텍스트 상자	설명
호스트 이름	Hyper-V 서버의 IP 주소 또는 호스트 이름을 입력합니다. 원격 Hyper-V 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자의 사용자 이름을 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.
암호	Hyper-V 서버가 설치된 워크스테이션에 대해 관리자 권한이 있는 사용자 계정의 암호를 입력합니다. 가상 시스템의 로그온 자격 증명을 지정하는 데 사용됩니다.

7 **다음**을 클릭합니다.

8 **가상 시스템 옵션** 페이지의 **VM 시스템 위치** 텍스트 상자에 가상 시스템의 경로(예: **D:\export**)를 입력합니다. 가상 시스템의 위치를 나타내기 위해 사용됩니다.

노트: 로컬 및 원격 Hyper-V 서버 모두에 대한 가상 시스템 위치를 지정해야 합니다. 경로는 Hyper-V 서버에 대한 유효한 로컬 경로여야 합니다. 존재하지 않는 디렉터리가 자동으로 생성됩니다. 디렉터리를 수동으로 만들면 안 됩니다. 공유 폴더(예: \\data\share)로 내보내기는 허용되지 않습니다.

9 **가상 시스템 이름** 텍스트 상자에 가상 시스템의 이름을 입력합니다.

입력한 이름이 Hyper-V Manager 콘솔의 가상 시스템 목록에 나타납니다.

10 메모리 사용량을 지정하려면 다음 중 하나를 클릭하십시오.

- **원본 시스템과 동일한 RAM 크기 사용**. 가상 시스템과 원래 시스템 사이에 동일한 RAM을 사용하고 있는지 식별하려면 이 옵션을 선택합니다.
- **특정 RAM 크기 사용.** RAM 크기를 MB 단위로 지정하려면 이 옵션을 선택합니다.

  최소 크기는 1024MB이고, 응용 프로그램에서 허용하는 최대 크기는 65536MB입니다. 최대 메모리 사용량은 호스트 시스템에 사용할 수 있는 RAM의 양으로 제한됩니다.

11 디스크 형식을 지정하려면 디스크 형식 옆에서 다음 중 하나를 클릭합니다.

- VHDX
- VHD

노트: Hyper-V 내보내기는 대상 시스템에서 Windows 8(Windows Server 2012) 이상을 실행하는 경우 VHDX 디스크 형식을 지원합니다. VHDX가 지원되지 않는 환경의 경우 옵션이 비활성화됩니다.

Hyper-V 2세대로 내보낼 경우 VHDX 디스크 형식만 지원됩니다.

12 내보내기에 사용할 Hyper-V 세대를 지정하려면 다음 항목 중 하나를 클릭합니다.

- 1세대
- 2세대

노트: 2세대만 보안 부트 옵션을 지원합니다.

13 내보낸 VM에 대한 해당 네트워크 어댑터를 지정합니다.

14 **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다(예: C:\).

노트: 선택한 볼륨이 아래에 표시된 대로 응용프로그램에서 지원하는 적절한 최대 할당보다 크거나 사용 가능한 공간을 초과할 경우 오류가 발생합니다.

- VHDX 디스크 형식의 경우 선택한 볼륨은 64TB보다 크지 않아야 합니다.
- VHD 디스크 형식의 경우 선택한 볼륨은 2040GB보다 크지 않아야 합니다.

15 **초기 1회 내보내기 수행**을 선택하여 예약된 다음 스냅숏 후 대신 즉시 다음 내보내기를 수행합니다.

16 **볼륨** 페이지에서 **마침**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

노트: 가상 대기 또는 이벤트 페이지를 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

에이징 데이터 관리

이 섹션에서는 리포지토리에 저장되는 에이징 스냅숏 데이터를 관리하는 방법에 대해 설명합니다. 섹션에는 공간을 절약할 수 있도록 리포지토리의 복구 지점 보관, 보존 정책 및 결과로 수행되는 복구 지점 롤업 프로세스에 대한 정보가 포함되어 있습니다. 섹션에서는 리포지토리의 복구 지점을 Dell DR 백업 및 중복 제거 어플라이언스로 재배치하는 새 기능에 대해 설명합니다.

또한 이 섹션에서는 롤업 대상이 아닌 장기 보관용 데이터를 아카이브하고 아카이브된 복구 지점에 액세스하는 방법에 대해 설명합니다.

Rapid Recovery 데이터 보존 및 아카이브 정보

Core에서 스냅숏을 캡처할 때마다 데이터를 리포지토리에 복구 지점으로 저장합니다. 그러면 시간이 경과하며 복구 지점이 누적됩니다. Core는 보존 정책을 통해 리포지토리에서 스냅숏 데이터를 보관하는 기간을 결정합니다. 야간 작업의 롤업 중 Core는 보존 정책을 시행하여 소비되는 저장 공간의 크기를 줄입니다. 롤업 중에 각 복구 지점의 날짜를 최근 복구 지점 날짜와 비교합니다. 그리고 이전 복구 지점을 결합하거나 "롤업"합니다. 시간이 경과하면 이전 복구 지점은 가장 오래된 보존 시간을 초과하여 새 복구 지점으로 바뀝니다.

결합되어 삭제되지 않도록 복구 지점을 유지하기 위해 Core Console에서 아카이브를 생성할 수 있습니다. 아카이브는 생성 시점에 Core에서 보호하는 시스템의 전체 복구 지점 집합을 포함하는 파일입니다.

아카이브는 파일 시스템이나 클라우드의 저장소 계정에 저장할 수 있습니다.

복구 지점의 데이터에 액세스해야 하는 경우 Rapid Recovery 6.x 이상이면 나중에 첨부하거나 아카이브를 가져와서 해당 복구 지점을 리포지토리로 복원할 수 있습니다. 그리고 현재 Core의 다른 복구 지점과 마찬가지로 해당 데이터에서 동일한 작업을 수행할 수 있습니다.

노트: Core는 아카이브에서 복구 지점의 원래 날짜를 인식하므로 가져온 복구 지점은 다음 야간 작업 기간에 다시 롤업되거나 삭제될 수 있습니다. 이전 복구 지점을 보존하려는 경우 관련 시스템에서 롤업을 비활성화하거나 보존 기간을 연장할 수 있습니다.

보존 정책 관리

보존 정책은 롤업을 시작하기 전에 복구 지점을 유지하기 위해 Core에 대한 기간을 나타내는 규칙 집합입니다. 보존 정책은 시간, 일, 주, 월 및 년을 기반으로 롤업하도록 설정할 수 있습니다. 최대 6가지 규칙(기본 정책은 5가지 규칙을 설정)을 설정할 수 있습니다.

5분마다 자주 백업할 수 있기 때문에 일반적으로 보존 정책의 첫 번째 규칙은 모든 복구 지점을 유지하는 시간을 설정합니다. 예를 들어, 15분마다 시스템을 복구하는 경우 롤업이 시작될 때까지 매일 해당 시스템에 대한 리포지토리에 96개 복구 지점이 저장됩니다. 보존 정책을 관리하지 않으면 이런 데이터의 양이 리포지토리를 빠르게 채울 수 있습니다.

노트: 관리자는 빈번한 백업은 네트워크에 영향을 줄 수 있음에 유의해야 합니다. 네트워크 트래픽에 영향을 미치는 기타 요인으로는 다른 전송(예: 복제), 데이터 변경률 및 네트워크 하드웨어, 케이블 및 스위치가 포함됩니다.

Core에는 기본 보존 정책과 함께 사전 설정이 제공됩니다. 기본 정책은 계속 유지합니다:

- 3일 동안 모든 복구 지점
- 2일 동안 시간당 하나의 복구 지점
- 4일 동안 하루당 하나의 복구 지점
- 3주 동안 주당 하나의 복구 지점
- 2개월 동안 월당 하나의 복구 지점
- X년 동안 년당 하나의 복구 지점(기본 정책에서는 사용 안 함)

이 기본 정책 다음으로 가장 오래된 복구 지점은 일반적으로 92일입니다. 기본 정책의 날짜가 경과된 데이터는 삭제됩니다.

Core 레벨에서 보존 정책을 설정하면 Core에서 보호하는 모든 시스템에 자동으로 적용됩니다. 기본 정책은 사용자의 필요에 맞게 변경할 수 있습니다.

모든 시스템에 대해 사용자 지정 보존 정책을 생성할 수도 있습니다. 시스템 레벨에서 정책을 설정하면 기본 Core 정책과는 다른 보존 정책을 지정할 수 있습니다. 보존 정책 구성에 대한 자세한 내용은 Core 기본 보존 정책 설정 구성 및 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.

Core 기본 보존 정책 설정 구성

Core에 대한 보존 정책은 보호되는 시스템의 복구 지점이 리포지토리에 저장되는 기간을 지정합니다.

Core 보존 정책은 야간 작업을 실행하는 하나의 구성 요소로 수행되는 롤업 프로세스에 의해 시행됩니다. 그런 다음, 보존 정책에 지정된 기간이 지난 복구 지점은 덜 세밀한 기간을 적용하는 더 적은 수의 복구 지점으로 "롤업"(결합)됩니다. 야간 작업에 보존 정책을 적용하면 오래된 백업을 계속해서 롤업하게 됩니다. 이렇게 하면 결국 해당 보존 정책에 지정된 요구 사항에 따라 가장 오래된 복구 지점이 삭제됩니다.

소스 및 대상 Core에 대해 다른 보존 설정을 구성할 수 있습니다.

노트: 이 항목은 해당 Rapid Recovery Core의 보존 정책 설정의 사용자 지정에 관한 것입니다. 사용자 지정 보존 정책 설정을 Core에 저장하면 기본 보존 정책이 설정되어 이 Core로 보호되는 모든 시스템에 적용할 수 있습니다. 개별적으로 보호되는 시스템에 대한 보존 정책 설정의 사용자 지정에 대한 자세한 내용은 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.

1 Rapid Recovery Core 콘솔로 이동합니다.

2 아이콘 표시줄에서 (설정)를 클릭한 후 다음 중 하나를 수행합니다.

- Settings(설정) 페이지 왼쪽의 Core 설정 목록에서 **Nightly Jobs(야간 작업)**를 클릭합니다.
- **Nightly Jobs(야간 작업)** 머리글이 보일 때까지 Settings(설정) 페이지의 오른쪽을 아래로 스크롤합니다.

Nightly Jobs(야간 작업) 설정이 나타납니다.

3 **Nightly Jobs(야간 작업)** 아래에서 **Change(변경)**를 클릭합니다.

Nightly Jobs(야간 작업) 대화 상자가 표시됩니다.

4 Nightly Jobs(야간 작업) 창에서 필요에 따라 백업 데이터를 보존할 시간 간격을 지정하려면 **Rollup(롤업)**을 선택하고 **Settings(설정)**를 클릭합니다.

Core 기본 보존 정책에 대한 **Configuration(구성)** 대화 상자가 나타납니다.

5 언제든지 Core 보존 정책 설정을 기본값으로 복원하려면 Configuration(구성) 대화 상자의 하단에서 **Restore Defaults(기본값 복원)**을 클릭하고 **Yes(예)**를 클릭하여 확인합니다.

모든 설정이 6단계의 표에 설명되어 있는 기본값으로 복원됩니다.

6 보존 정책을 정의하려면 먼저 초기 백업 스냅샷이 보존되는 기간을 결정하는 기본 설정을 지정한 다음, 복구 지점이 롤업되는 간격을 결정하는 일련의 연속되는 롤업 요구사항을 정의합니다.

보존 정책 옵션은 다음 표에 설명되어 있습니다.

표 125. 기본 보존 정책에 대한 일정 옵션

텍스트 상자	설명
n [보존 기간] 동안 모든 복구 지점 유지	복구 지점에 대한 보존 기간을 지정합니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 3입니다.

텍스트 상자	설명
	일, 주, 월 또는 년 중에서 선택할 수 있습니다.
...n [보존 기간] 동안 한 시간에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 기본 설정에 대한 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2입니다. 일, 주, 월 또는 년 중에서 선택할 수 있습니다.
...n [보존 기간] 동안 하루에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 4입니다. 일, 주, 월 또는 년 중에서 선택할 수 있습니다.
n[보존 기간] 동안 한 주에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 3주입니다. 주, 월 또는 년 중에서 선택할 수 있습니다.
n[보존 기간] 동안 한 달에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2개월입니다. 월 또는 년 중에서 선택할 수 있습니다.
n[보존 기간] 동안 일 년에 하나의 복구 지점 유지	보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 년에서 선택할 수 있습니다.

가장 오래된 복구 지점은 보존 정책 설정에 따라 결정됩니다.

보존 정책이 계산되는 방법에 대한 예는 다음과 같습니다.

3일 동안 모든 복구 지점을 유지합니다.

...3일 동안 한 시간에 하나의 복구 지점 유지

...4일 동안 하루에 하나의 복구 지점 유지

...3주 동안 한 주에 하나의 복구 지점 유지

...2개월 동안 한 달에 하나의 복구 지점 유지

...1년 동안 한 달에 하나의 복구 지점 유지

이 예에서 가장 오래된 복구 지점은 1년, 4개월 및 6일이 지난 복구 지점입니다.

7 보존 정책 설정에 만족하는 경우 **Save(저장)**를 클릭합니다.
Configuration(구성) 대화 상자가 닫힙니다.

8 **Nightly Jobs(야간 작업)** 대화 상자에서 **OK(확인)**를 클릭합니다.
Nightly Jobs(야간 작업) 대화 상자가 닫힙니다. 정의한 보존 정책은 야간 롤업 동안 적용됩니다.

개별적으로 보호되는 시스템에 대한 보존 정책을 지정할 때 이러한 설정을 적용할 수도 있습니다. 보호되는 시스템에 대한 보존 정책 설정에 대한 자세한 내용은 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.

보호되는 시스템에 대한 보존 정책 설정 사용자 지정

보호되는 시스템에 대한 보존 정책은 리포지토리에 복구 지점을 저장하는 기간을 지정합니다. 일반적으로, 각 보호되는 시스템은 이 절차에 설명되어 있는 사용자 지정 보존 정책을 지정하지 않는 한 Core에 대해 설정한 기본 보존 정책을 사용합니다.

복제된 시스템을 포함하여 보호되는 시스템에 대한 사용자 지정 보존 정책을 정의하려면 이 절차를 사용합니다.

1 Rapid Recovery Core 콘솔의 Protected Machines(보호되는 시스템) 메뉴에서 수정할 시스템의 이름을 클릭합니다.
선택 시스템에 대한 **Summary(요약)** 페이지가 나타납니다.

2 **Settings(설정)** 메뉴를 클릭합니다.
선택한 시스템의 구성 설정을 보여 주는 **Settings(설정)** 페이지가 나타납니다.

3 선택적으로, Settings(설정) 페이지로 스크롤하여 야간 작업 설정을 보려면 **Nightly Jobs(야간 작업)** 링크를 클릭합니다.

4 Nightly Jobs(야간 작업) 제목 아래에서 **Change(변경)**를 클릭합니다.
Nightly Jobs(야간 작업) 대화 상자가 표시됩니다.

5 필요에 따라 백업 데이터를 보존할 시간 간격을 지정하려면 **Rollup(롤업)**을 선택하고 **Settings(설정)**를 클릭합니다.
보존 정책에 대한 **Configuration(구성)** 대화 상자가 나타납니다.

6 복제된 시스템에 대한 보존 정책 설정을 사용자 지정하고 리포지토리에서 무결성 검사를 수행할 것을 알리는 경우 이 단계를 진행합니다. 그렇지 않은 경우, 다음 단계로 건너뜁니다.
   a 작업을 수행할 준비가 되면 **Check Integrity(무결성 확인)**를 클릭합니다.
   b **Yes(예)**를 클릭하여 무결성 검사 작업을 확인합니다.

> **노트: 이 작업을 실행하는 데 리포지토리의 크기에 따라 상당한 시간이 걸릴 수 있습니다. 이 시간 동안 리포지토리에서 다른 작업(스냅샷, 복제, 가상 내보내기 등)을 수행할 수 없습니다. 이 작업에 대한 자세한 내용은 DVM 리포지토리의 무결성 검사을(를) 참조하십시오.**

   - 무결성 검사 작업에서 모든 하위 작업이 성공적으로 완료되면 이 절차로 돌아와 다음 단계를 계속합니다.

7 **Configuration(구성)** 대화 상자에서 다음 중 하나를 수행합니다.
   - 이 보호되는 시스템에 대한 기본 보존 정책을 사용하려면 **Use Core default retention policy(Core 기본 보존 정책 사용)**를 선택한 다음 **Save(저장)**를 클릭합니다. 기본 정책이 이 에이전트에 적용됩니다.
   - 이 에이전트에 대한 사용자 지정 보존 정책을 정의하려면 **Use custom retention policy(사용자 지정 보존 정책 사용)**를 선택한 후에 다음 단계를 계속합니다.

Configuration(구성) 대화 상자를 확장하여 사용자 지정 보존 정책 정보를 표시합니다.

8 다음 표에 설명된 대로 복구 지점을 보존하는 사용자 지정 일정을 입력합니다.

표 126. 사용자 지정 보존 정책에 대한 일정 옵션

텍스트 상자	설명
n [보존 기간] 동안 모든 복구 지점 유지	복구 지점에 대한 보존 기간을 지정합니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 3입니다. 일, 주, 월 및 년 중에서 선택할 수 있습니다.
n [보존 기간] 동안 한 시간에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 기본 설정에 대한 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2입니다. 일, 주, 월 및 년 중에서 선택할 수 있습니다.
...n [보존 기간] 동안 하루에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다.

텍스트 상자	설명
	보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 4입니다. 일, 주, 월 및 년 중에서 선택할 수 있습니다.
...n[보존 기간] 동안 한 주에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 3주입니다. 주, 월 및 년 중에서 선택할 수 있습니다.
...n[보존 기간] 동안 한 달에 하나의 복구 지점 유지	보다 세부적인 보존 기간을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있도록 구성 블록으로 사용됩니다. 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2개월입니다. 월 및 년 중에서 선택할 수 있습니다.
...n[보존 기간] 동안 일 년에 하나의 복구 지점 유지	보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 년에서 선택할 수 있습니다.

보존 정책이 계산되는 방법에 대한 예는 다음과 같습니다.

3일 동안 모든 복구 지점을 유지합니다.

...3일 동안 한 시간에 하나의 복구 지점 유지

...4일 동안 하루에 하나의 복구 지점 유지

...3주 동안 한 주에 하나의 복구 지점 유지

...2개월 동안 한 달에 하나의 복구 지점 유지

...1년 동안 한 달에 하나의 복구 지점 유지

이 예에서 가장 오래된 복구 지점은 1년, 3개월이 지난 복구 지점입니다.

9 기본 리포지토리에 모든 복구 지점을 유지하려면 **Relocate outdated recovery points to an R3 repository(R3 리포지토리에 오래된 복구 지점 재배치)** 옵션을 선택 취소하고 다음 단계로 건너뜁니다.

10 Dell DR 시리즈 백업 어플라이언스에 저장된 R3 리포지토리로 기본 리포지토리의 복구 지점을 재배치하려는 경우 다음을 수행하십시오.

a **Relocate outdated recovery points to an R3 repository(R3 리포지토리로 오래된 복구 지점 재배치)** 옵션을 선택합니다.

b R3 리포지토리에 기본 리포지토리의 복구 지점을 재배치하려는 기간을 지정합니다.
주, 월 또는 년별로 기간을 지정할 수 있습니다. 설정할 수 있는 가장 짧은 기간은 1주일입니다.

c **Select a repository(리포지토리 선택)** 드롭다운 메뉴에서 지정된 복구 지점 계층에 원하는 R3 리포지토리를 선택합니다.

노트: 복구 지점이 있는 위치에 관계없이(로컬 DVM 리포지토리 또는 DR 백업 어플라이언스의 원격 R3 리포지토리), 계속 보존 정책이 적용되며 롤업됩니다. 이전 복구 지점을 유지해야 하는 경우 한 가지 방법은 보관하는 것입니다. 다른 접근법은 롤업을 비활성화하거나 관련된 보호되는 시스템의 보존 기간을 연장하는 것입니다.

11 **저장**을 클릭합니다.

보호된 시스템에 대해 롤업 수행

보호된 시스템 수준에서 복구 지점을 롤업하여 예약된 보존 정책을 건너뛸 수 있습니다.

1 Rapid Recovery Core Console의 보호된 시스템에서 특정 보호된 시스템 이름을 클릭합니다.

시스템 선택에 대한 **요약** 페이지가 나타납니다.

2 보호된 시스템 보기 상단에서 **자세히** 드롭다운 메뉴를 클릭한 다음 **보존 정책**을 선택합니다.
지정된 시스템에 대한 **보존 정책** 페이지가 나타납니다.

3 **롤업 수행**을 클릭합니다.

4 대화 상자에서 **예**를 클릭하여 제거를 확인합니다.
Rapid Recovery는 보존 정책 일정에 관계없이 이 시스템에 대한 롤업을 초기화합니다.

복제

이 섹션에서는 재해 복구를 위해 Rapid Recovery 소스 Core에서 Rapid Recovery 대상 Core로 보호된 데이터의 복제를 구성하고 관리하는 방법에 대해 설명합니다.

Rapid Recovery로 복제

이 섹션은 Rapid Recovery에서 복제를 이해하고 구성하는 데 도움이 되는 개념 및 절차 정보를 제공합니다.

복제는 재해 복구를 위해 Rapid Recovery Core에서 복구 지점을 복사하여 다른 Rapid Recovery Core로 전송하는 프로세스입니다. 이러한 프로세스를 수행하려면 두 개 이상의 Core 간 관계가 소스-대상 쌍으로 지정되어 있어야 합니다.

소스 Core는 선택한 보호된 시스템의 복구 지점을 복사한 다음, 해당 스냅숏 데이터를 대상 Core에 비동기적으로 지속해서 전송합니다.

복제 일정을 설정하여 기본 동작을 변경하는 경우를 제외하고 Core는 모든 백업 스냅숏, 체크섬 검사, 연결 기능 검사 및 야간 작업 완료 후 즉시, 복제 작업을 시작합니다. 자세한 내용은 복제 일정 설정을(를) 참조하십시오.

최적의 데이터 보안을 위해 관리자들은 일반적으로 원격 재해 복구 사이트에서 대상 Core를 사용합니다. 회사 소유의 데이터 센터나 원격 재해 복구 사이트(즉, "자체 관리된" 대상 Core)에 아웃바운드 복제를 구성할 수 있습니다. 또는 오프사이트 백업 및 재해 복구 서비스를 호스팅하는 타사의 관리된 서비스 공급자(MSP) 또는 클라우드 공급자에 아웃바운드 복제를 구성할 수 있습니다. 타사 대상 Core에 복제할 때 연결을 요청하고 자동 피드백 알림을 수신할 수 있는 기본 워크플로를 사용할 수 있습니다.

복제는 보호된 시스템을 기준으로 관리됩니다. 소스 Core에서 보호되거나 복제된 시스템(또는 모든 시스템)은 대상 Core로 복제되도록 구성할 수 있습니다.

가능한 복제 시나리오는 다음과 같습니다.

- **로컬 위치에 복사**. 대상 Core가 로컬 데이터 센터 또는 온사이트 위치에 있으며 복제가 항상 유지 관리됩니다. 이 구성에서는 Core가 손실되어도 복구가 차단되지 않습니다.
- **오프사이트 위치에 복제**. 대상 Core가 손실 발생 시 복구를 위해 오프사이트 재해 복구 시설에 위치합니다.
- **상호 복제**. 서로 다른 위치에 있는 두 개의 데이터 센터가 Core를 포함하고 시스템을 보호하며 각 데이터 센터가 오프사이트 재해 복구 백업의 역할을 합니다. 이 시나리오에서는 각 Core가 다른 데이터 센터에 위치한 Core에 보호된 시스템을 복제합니다.
- **호스트 및 클라우드 복제**. Rapid Recovery MSP 파트너가 데이터 센터 또는 공용 클라우드에서 여러 대상 Core를 유지 관리합니다. 이러한 각 Core에서 MSP 파트너를 통해 한 명 이상의 고객이 고객의 사이트에 있는 소스 Core에서 MSP의 대상 Core로 복구 지점을 유료로 복제할 수 있습니다.

노트: 이 시나리오에서는 고객이 소유한 데이터에만 액세스할 수 있습니다.

가능한 복제 구성은 다음과 같습니다.

- **지점 간 복제**. 하나 이상의 보호된 시스템을 단일 소스 Core에서 단일 대상 Core로 복제합니다.

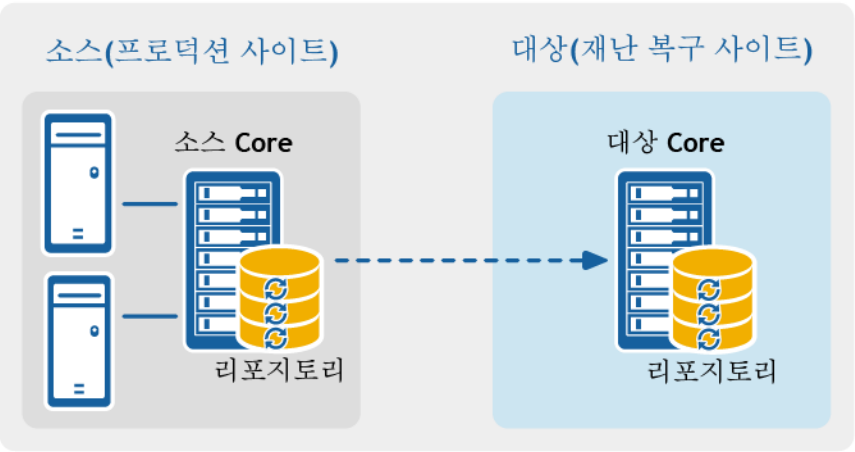


그림 9 . 지점 간 복제 구성

- **다중 지점-지점 간 복제.** 보호된 시스템을 다중 소스 Core에서 단일 대상 Core로 복제합니다.

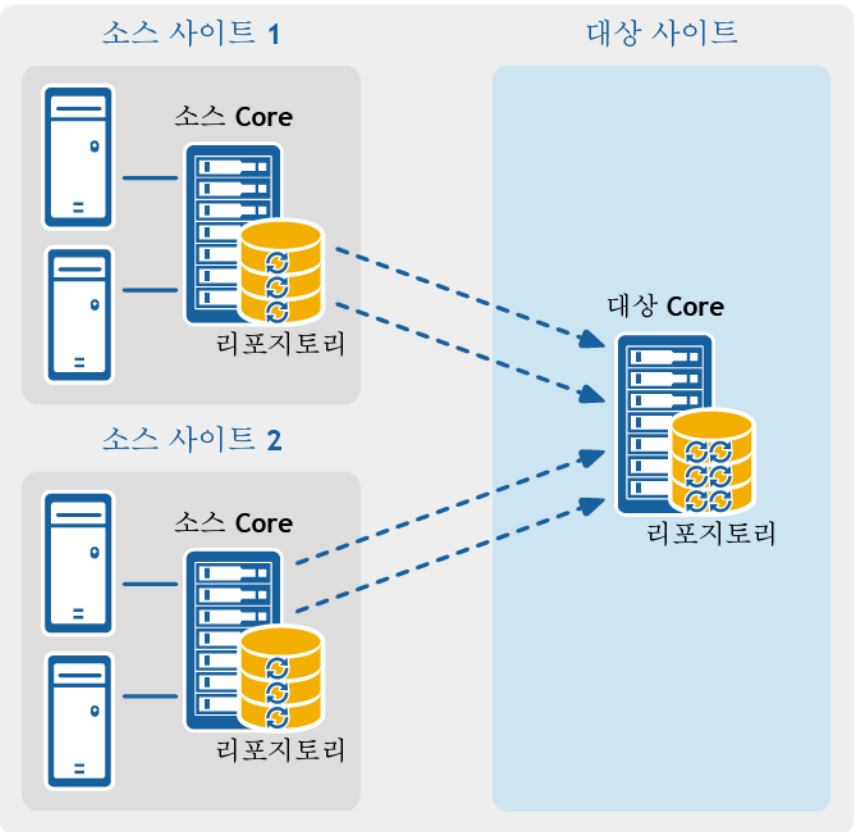


그림 10 . 다중 지점-지점 간 복제 구성

- **지점-다중 지점 간 복제**. 하나 이상의 보호된 시스템을 단일 소스 Core에서 두 개 이상의 대상 Core로 복제합니다.

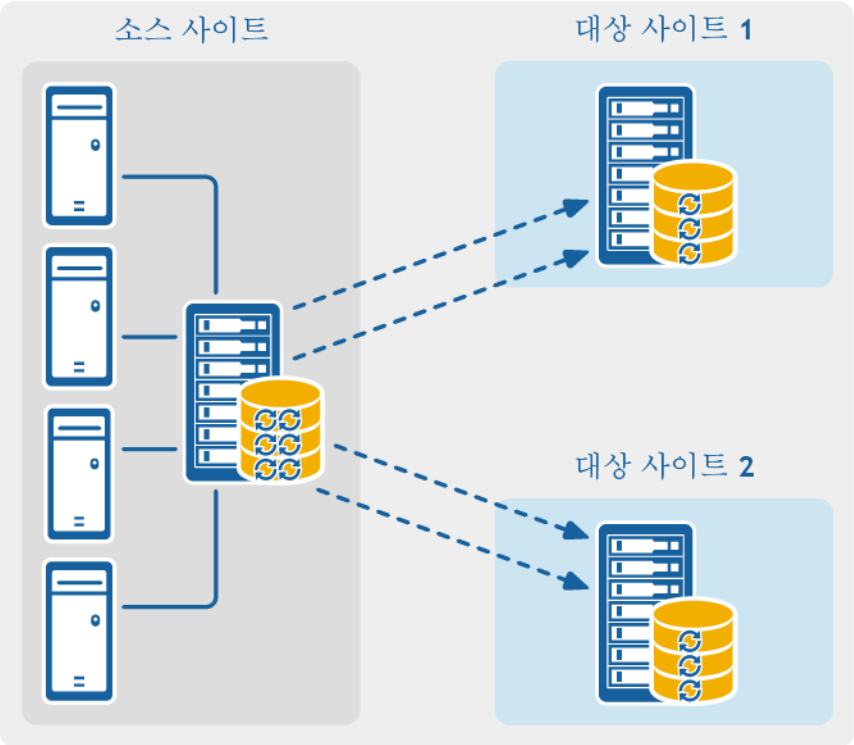


그림 11 . 지점-다중 지점 간 복제 구성

- **멀티홉 복제**. 하나 이상의 보호된 시스템을 하나의 대상 Core에서 다장른 대상 Core로 복제하여 복제된 Core에서 추가적인 장애 조치 또는 복구 옵션을 생성합니다.

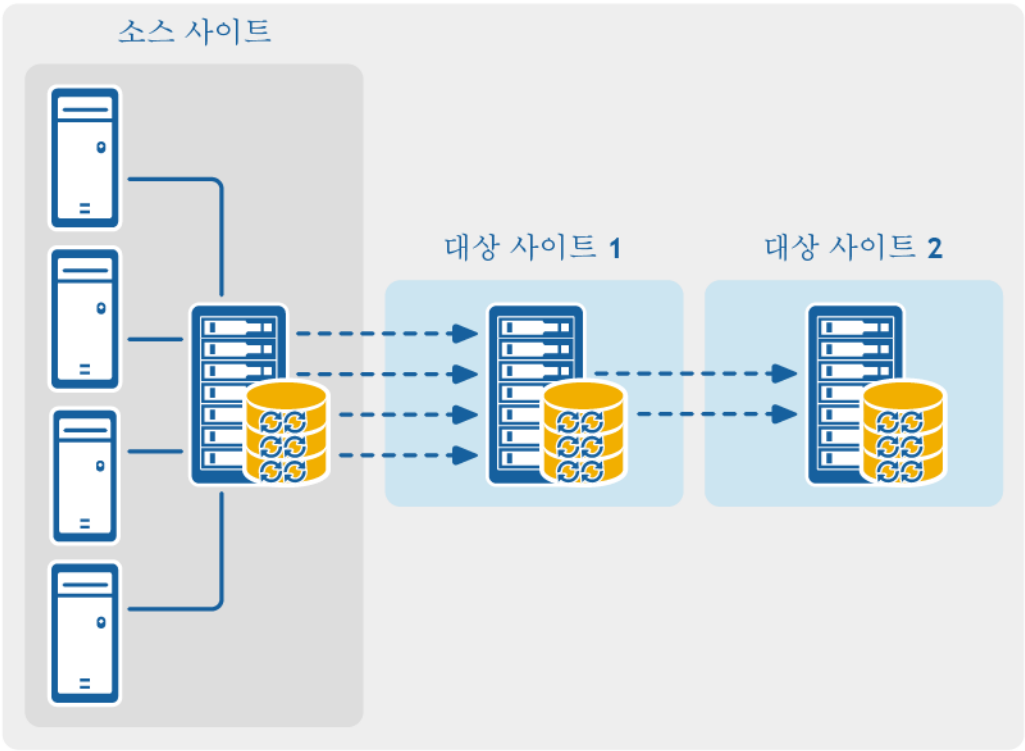


그림 12 . 멀티홉 복제 구성

DL1x00 또는 DI4x00 등의 Dell Data Protection 백업 어플라이언스를 사용할 경우 복제하는 대상 Core에는 유효한 소프트웨어 라이센스가 구성되어 있어야 합니다. 이러한 하드웨어 어플라이언스에는 구매 시 복제 대상 라이센스가 포함되어 있습니다. 어플라이언스 구매 시 사용자가 받은 환영 이메일 메시지에서 라이센스 키를 확인하십시오. 지원을 받으려면 Licensing Assistance 웹 사이트 (https://support.software.dell.com/licensing-assistance)에 방문하거나 license@software.dell.com으로 이메일을 보내 주십시오.

복구 지점 체인 및 분리

Rapid Recovery는 보호된 시스템의 스냅숏을 캡처하고 데이터를 *복구 지점*으로 리포지토리에 저장합니다. Core에 저장된 최초 복구 지점을 *기본 이미지*라고 합니다. 기본 이미지로는, 운영 체제, 응용 프로그램, 보호하려는 각 볼륨의 설정, 해당 볼륨에 있는 모든 데이터가 포함됩니다. 연속 백업은 *증분 스냅숏*이라고 하며, 마지막 백업 이후 보호된 볼륨에서 변경된 데이터로만 구성됩니다. 기본 이미지와 모든 증분 스냅숏을 합치면 전체 *복구 지점 체인*이 구성됩니다.

전체 복구 지점 체인에서 Rapid Recovery에서 지원하는 모든 복구 옵션을 사용하여 쉽고 정확하게 데이터를 복원할 수 있습니다. 지원되는 옵션으로는, 파일 수준 복원, 볼륨 수준 복원, Bare Metal 복원이 있습니다.

이론적으로는 존재하지 않는 데이터에서 복원할 수 없으므로, 불완전한 복구 지점 체인이 발생하면 볼륨 수준에서 데이터를 복원하거나 Bare Metal 복원을 수행할 수 없습니다. 이 경우 파일 수준에서 복구 지점에 존재하는 데이터는 계속 복원할 수 있습니다.

복구 지점에서 복원하려는 정보가 Core에서는 사용할 수 없는 이전 백업에 있는 경우(이전 증분 스냅숏이나 기본 이미지) 복구 지점이 *분리*되었다고 합니다. 분리된 복구 지점은 일부 복제 시나리오에서 흔히 볼 수 있습니다.

예를 들어, 먼저 복제를 설정하면 복제된 복구 지점에서 데이터를 복원하는 옵션이 제한됩니다. 소스 Core의 모든 백업 데이터를 대상 Core로 전송하기 전에는 분리 지점에서 전체 복구 지점 체인을 생성할 때 파일 수준 복원만 수행할 수 있습니다.

복제를 시작하는 경우

기본적으로 복제 전송 작업은 정기적으로 예약된 각 백업 전송을 마친 후에 즉시 자동으로 대기합니다. 따라서 보호된 시스템에 대한 복제 예약을 사용자 지정하기 전에는 복제 일정은 해당 표준 백업 스냅숏 일정에 따릅니다.

처음에 복제를 설정할 때 소스 Core에 하나 이상의 복구 지점이 있으면 다음 조건을 만족하지 않는 한, 복제 프로세스를 즉시 시작합니다.

- 처음에 복제를 일시 중지하는 옵션을 선택합니다.
- 시드 드라이브를 사용하여 초기 전송을 수행하는 옵션을 선택합니다.

처음에 복제를 일시 중지하는 경우 복제를 명시적으로 다시 시작하면 복제가 시작됩니다.

복제를 설정하고 시드 드라이브 사용을 지정한 경우 다음에 정기적으로 예약된 백업 스냅숏을 통해 대상 Core로의 복제가 시작됩니다.

노트: 복제를 설정한 후에 보호된 시스템을 강제로 백업할 수도 있습니다. 그러면 보호된 시스템 스냅숏을 완료한 후 즉시 복제가 시작됩니다.

복제를 설정할 때 시드 드라이브를 지정하면 향후 백업 전송만 복제합니다. 대상 Core에 원래 보호된 시스템의 기본 복구 지점이 있으려면 보호된 시스템에서 데이터를 시드해야 합니다. 데이터를 시드하려면 소스 Core에서 시드 드라이브를 생성하고 대상 Core에서 시드 드라이브를 사용합니다.

보호된 시스템의 복제 일정을 사용자 지정할 수도 있습니다. 예를 들어, 시간당 하나의 백업에 대한 기본 보호 일정을 사용하는 경우 소스 Core는 다른 일정(예를 들어, 매일 오전 2시에 한 번)으로 대상 Core에 복제하도록 지정할 수 있습니다.

시딩 요구 및 전략 확인

다음 항목은 복제된 데이터의 복원 및 소스 Core에서 복구 지점 데이터를 시드해야 하는지에 대해 설명합니다.

시딩 데이터가 필요한 시기

복제를 처음 설정하면 시드 드라이브 사용을 지정하지 않는 한 선택한 시스템에 대한 모든 복구 지점을 소스 Core에서 대상 Core로 전송하기 시작합니다. 네트워크를 통해 데이터를 전송하면 긴 시간이 소요됩니다. 네트워크 속도, 네트워크 아키텍처의 강력함, 대상 Core로 전송되는 데이터 양을 포함한 요인이 원인이 될 수 있습니다. 예를 들어, 소스 Core의 백업 데이터 크기가 10GB이고 WAN 링크가 24Mbps를 전송하는 경우 전송이 완료되는 데 약 1시간이 걸립니다.

대상 Core에 복사하려고 하는 정보의 양에 따라 시드 드라이브가 수백 또는 수천 기가바이트의 데이터를 추가할 수 있습니다. 대부분의 조직에서는 필수적인 네트워크 대역폭을 소비하지 않고 대신 시드 드라이브를 정의하여 사용하도록 선택합니다. 자세한 내용은 복제된 데이터 전송에 대한 성능 고려 사항을(를) 참조하십시오.

복제를 정의할 때 시드 드라이브의 사용을 지정하는 경우 복제를 설정한 *후* 소스 Core에 저장된 복구 지점만 대상 Core에 복제됩니다. 복제가 설정되기 *전*에 소스 Core에 저장된 백업은 사용자가 다음 절차에 따라 명시적으로 데이터를 *시드*할 때까지 대상 Core에 표시되지 않습니다.

내역 데이터의 집중적인 전송으로 인해 네트워크의 속도가 느려지지 않도록 하려면 **시드 드라이브**를 사용하여 데이터를 대상 Core에 백업하기 전에 시드하십시오. 시드 드라이브는 중복 제거된 기본 이미지 집합과 소스 Core의 증분 스냅숏을 **복사**하는 아카이브 파일입니다. 시드 드라이브는 사용자가 소스 Core에서 대상 Core로 복제하려는 보호된 시스템에 대한 이전의 전체 복구 지점을 포함하고 있습니다.

시드 드라이브 파일을 저장소 볼륨으로 이동하면 대상 Core에서 사용할 수 있습니다. 그런 다음 시드 드라이브의 정보를 **사용합니다.** 여기에는 시드 드라이브 이미지가 있는 볼륨을 대상 Core에 연결하고 Core Console의 리포지토리로 데이터를 가져오는 과정이 포함

되어 있습니다. 이 프로세스에서 대상 Core에 복제된 증분 스냅숏을 기본 이미지와 결합하여 분리된 항목을 수정하면 하나 이상의 완전한 복구 지점망을 형성할 수 있습니다. 이 프로세스를 copy-consume이라고도 합니다.

소스 Core의 데이터를 항상 시딩할 필요는 없습니다. 예:

- 새 Rapid Recovery Core에 복제를 설정하는 경우 시드가 필요하지 않습니다.
- 이전 스냅숏의 데이터가 복제된 데이터에 위험하지 않은 경우 복제를 설정한 뒤에 저장된 데이터만 복구해야 하며 시딩이 필요하지 않습니다.

노트: 이 경우 Dell에서는 복제를 설정하기 전이나 설정한 직후에 새로운 기본 이미지를 캡처하도록 권장합니다. 이 단계에서 이후에 데이터를 복원할 대상 Core에 전체 복구 지점망이 있는지 확인합니다.

- 복제를 설정하기 직전에 기본 이미지를 캡처한 경우 해당 데이터 이후에 캡처된 데이터만 복원해야 하며 시딩이 필요하지 않습니다.
- 시드 드라이브를 지정하지 않고 복제를 설정하는 경우 스냅숏 데이터가 네트워크를 통해 소스 Core에서 대상 Core로 전송됩니다.

이러한 상황 중 하나에 해당한다면 데이터를 시드할 필요가 없습니다. 이러한 경우에는 소스 Core에서만 복제를 완전히 수행할 수 있습니다.

기존의 복구 지점이 있는 Core에 복제를 설정하고 볼륨 수준에서 복원해야 하는 경우 BMR을 수행하거나 이전 기본 이미지 또는 증분 스냅숏에서 데이터를 복원하려고 할 수 있습니다. 이 경우 시딩이 필요합니다. 이러한 상황에서는 시딩 요구 및 전략을 고려해 보십시오. 본 항목의 정보를 검토하고 대상 Core를 시드할지 여부와 어떤 접근 방식을 사용할지 결정합니다.

데이터 시딩 방식

대상 Core의 복제된 시스템에 원본 소스 Core에 있는 이전에 저장된 데이터에 대한 액세스 권한을 부여하려면 다음 방법 중 하나를 사용하여 대상 Core를 시드합니다.

1 **네트워크 연결을 통해 대상 Core에 시드합니다.** 복제를 정의할 때 시드 드라이브 사용을 지정합니다. 시드 드라이브가 포함된 폴더를 대상 Core와 공유하고 네트워크를 통해 시드 드라이브 파일을 사용할 수 있습니다. 데이터 용량이 크거나 연결 속도가 느린 경우, 이 방법으로 시드하면 긴 시간이 소요되거나 상당한 네트워크 대역폭을 소비할 수 있습니다.

노트: Dell에서는 네트워크 연결을 통해 대량의 데이터를 시딩하는 것을 권장하지 않습니다. 초기 시딩에는 매우 많은 양의 데이터가 포함될 가능성이 있으므로, 일반적인 WAN 연결에 큰 부담이 될 수 있습니다.

2 **물리적 저장소 매체를 사용하여 소스 Core에서 백업 데이터를 전송합니다.** 시드 드라이브 파일을 휴대 가능한 외부 이동식 저장 장치로 전송합니다. 일반적으로 이 방법은 대규모 데이터 세트나 연결 속도가 느린 사이트에 유용합니다. 이 방법을 사용하여 시딩하려면 다음 단계를 수행해야 합니다.

   a 이동식 매체에 저장하여 소스 Core에서 시드 아카이브를 생성합니다.

   b 시드 드라이브를 대상 Core의 물리적 위치로 전송합니다.

   c 드라이브를 대상 Core에 연결합니다.

   d 시드 드라이브의 데이터를 대상 Core의 리포지토리로 소비합니다.

   타사 Core를 복제하는 경우 MSP에서 매체를 수신하면 일반적으로 데이터 센터 담당자가 매체를 장착하여 시드 데이터를 Core에 소비(또는 가져오기)할 준비가 되면 알립니다.

노트: 저장 장치에 대량의 데이터를 복사해야 하므로 eSATA, USB 3.0 또는 기타 고속 연결 장치를 사용하는 것이 좋습니다. 시드 데이터 아카이브의 전체 크기가 이동식 매체에서 사용할 수 있는 공간보다 클 경우 아카이브는 여러 장치로 확장될 수 있습니다.

3 **가상 호스트에 저장된 소스 및 대상 Core의 경우 가상 하드 디스크를 사용하여 백업 데이터를 전송합니다.** 소스 Core 및 대상 Core가 모두 가상 호스트에 있는 경우 가상 저장소 매체에서 시드 드라이브를 정의하고 소비할 수 있습니다. 이 방법을 사용하여 시딩하려면 다음 단계를 수행해야 합니다.

   a 가상 저장소 볼륨에 저장하여 소스 Core에서 시드 드라이브 파일을 생성합니다.

   b 소스 Core에서 볼륨을 분리하고 대상 Core에 부착합니다.

   c 시드 드라이브의 데이터를 대상 Core의 리포지토리로 소비합니다.

노트: 시드가 완료되기 전에 소스 Core와 대상 Core 간에 증분 스냅숏의 복제가 발생할 수 있지만 소스에서 대상으로 전송된 복제된 스냅숏은 초기 데이터가 소모될 때까지 분리된 상태로 남아 있게 되며, 복제된 기본 이미지와 결합됩니다.

관련 링크

- 시드 드라이브 소비 과정에 대한 자세한 내용은 대상 Core에서 시드 드라이브 사용을(를) 참조하십시오.
- 분리된 복구 지점에 대한 자세한 내용은 분리된 복구 지점 체인 삭제에서 확인하십시오.
- 시드 드라이브를 준비하는 방법에 대한 자세한 내용은 시스 드라이브 이해 및 대상 Core에서 시드 드라이브 사용을 참조하십시오.

관련 링크

대상 Core에서 시드 드라이브 사용
분리된 복구 지점 체인 삭제

복제된 데이터 전송에 대한 성능 고려 사항

소스 Core와 대상 Core 간의 대역폭이 저장된 복구 지점 전송을 수용할 수 없는 경우 복제를 설정하고 시드 드라이브의 사용을 지정하십시오. 이 프로세스는 소스 Core에서 보호된 선택한 서버의 기본 이미지 및 복구 지점으로 대상 Core를 시딩합니다. 시딩 프로세스는 언제든지 수행할 수 있습니다. 시딩은 정기적으로 예약된 복제의 토대로 작용하는 데이터의 초기 전송 일부로 수행할 수 있습니다. 또한, 복제가 일시 중지 또는 삭제된 경우 이전에 복제한 시스템에 대한 데이터를 시딩할 수도 있습니다. 이 경우 "복구 지점 체인 구축"을 사용하여 아직 복제되지 않은 복구 지점을 시드 드라이브에 복사할 수 있습니다.

복제를 준비할 때 다음 요소를 고려해야 합니다.

- **변경 속도.** 변경 속도는 보호된 데이터의 양이 누적되는 속도입니다. 속도는 보호된 볼륨에서 변경되는 데이터의 양 및 볼륨의 보호 간격에 따라 다릅니다. Exchange 이메일 서버 등 일부 시스템 유형의 변경 속도는 일반적으로 더 높습니다. 변경 속도를 줄이기 위해 한 가지 방법은 보호 간격을 줄이는 것입니다.
- **대역폭.** 대역폭은 소스 Core와 대상 Core 사이에 사용할 수 있는 전송 속도입니다. 스냅숏이 생성하는 복구 지점을 유지하기 위해서는 대역폭이 복제에 대한 변경 속도보다 커야 합니다. Core에서 Core로의 대용량 데이터 전송의 경우 최대 1GB의 이더넷 연결 속도의 유선 속도로 여러 개의 병렬 스트림을 수행해야 할 수도 있습니다.

  노트: ISP에서 시정하는 대역폭은 일반적으로 총 사용 가능한 대역폭입니다. 네트워크의 모든 장치는 발신 대역폭을 공유합니다. 복제에서 변경 속도를 수용하기 위해 사용할 수 있는 충분한 대역폭이 있는지 확인하십시오.
- **보호된 시스템의 수.** 소스 Core당 보호된 시스템 수와 대상에 복제할 시스템 수를 고려해야 합니다. 소스 Core에서 보호된 모든 시스템을 복제할 필요는 없습니다. Rapid Recovery를 통해 보호된 시스템 단위로 복제할 수 있으므로, 원하는 경우 일부 시스템만 복제할 수도 있습니다. 소스 Core의 모든 보호된 시스템을 복제해야 하는 경우 일반적으로 변경 속도가 더 높습니다. 이 요소는 소스와 대상 Core 사이의 대역폭이 복제할 복구 지점의 양과 크기에 부족한 경우 관련 있습니다.

아래 표에는 WAN 연결 유형의 최대 변경 속도가 합리적인 변경 속도에 대한 기가바이트당 필요한 대역폭의 예와 함께 표시되어 있습니다.

표 127. 기가바이트당 대역폭 예제

광대역	대역폭	최대 변경 속도
DSL	768Kbps 이상	시간당 330MB
케이블	1Mbps 이상	시간당 429MB
T1	1.5Mbps 이상	시간당 644MB
광섬유	20Mbps 이상	시간당 8.38GB

노트: 최적의 결과를 얻을 수 있도록 이전 표에 나열된 권장 사항을 준수하십시오.

데이터 전송 중에 연결이 끊기는 경우 연결 기능이 복원되면 이전의 전송 장애 지점에서 복제가 다시 시작됩니다.

네트워크 구성에 따라 복제 프로세스에 많은 시간이 걸릴 수도 있습니다. 복제, 백업 등의 다른 Rapid Recovery 전송, 그리고 사용자가 실행해야 하는 기타 중요 응용 프로그램을 수용할 충분한 대역폭이 있는지 확인하십시오.

네트워크를 통해 데이터를 성공적으로 전송하는 데 문제가 있을 경우, 특히 일부 보호 또는 복제된 시스템은 해당 시스템의 데이터 전송률 조정을 고려하십시오. 자세한 내용은 전송 설정 수정 정보 및 전송 속도 제한를 참조하십시오.

복제 및 암호화된 복구 지점 정보

시드 드라이브에는 소스 Core 레지스트리 및 인증서의 백업이 포함되지 않지만 소스에서 대상으로 복제되는 복구 지점이 암호화된 경우 소스 Core의 암호화 키가 포함됩니다. 복제된 복구 지점은 대상 Core로 전송된 후 암호화된 상태를 유지합니다. 대상 Core의 소유자 또는 관리자가 암호화된 데이터를 복구하려면 암호가 필요합니다.

복제에 대한 보존 정책 정보

소스 및 대상 Core의 보존 정책은 동기화되지 않습니다. 롤업 및 주문형 삭제는 각 Core에서 초기 작업 시는 물론 야간 작업 중에 독립적으로 수행됩니다.

보존 정책에 대한 자세한 내용은 보존 정책 관리을(를) 참조하십시오.

자체 관리 대상 Core로 복제

이 구성은 오프사이트 위치에 대한 복제 및 상호 복제에 적용됩니다. 다음 단계는 필수 구성 요소입니다.

- 모든 소스 및 대상 시스템에 Rapid Recovery Core가 설치되어 있어야 합니다.
- 다중 지점-지점간 복제를 위한 Rapid Recovery를 구성하는 경우 모든 소스 Core 및 하나의 대상 Core에서 이 작업을 수행해야 합니다. 이러한 복제 구성에 대한 설명은 복제을(를) 참조하십시오.
- 시드 드라이브를 생성하고 물리적 이동식 저장 볼륨으로 전송하여 기존 복구 지점의 초기 전송을 수행하려면 휴대용 저장 장치를 준비해야 합니다. 드라이브를 시드 드라이브 아카이브에 연결하려면 소스 Core 시스템에 물리적으로 액세스해야 합니다.
- 자체 관리되는 대상 Core에서 시드 드라이브를 사용하는 경우 사용자 또는 신뢰할 수 있는 관리자가 대상 Core에 물리적 액세스 권한을 갖고 있어야 합니다.

자체 관리 대상 Core는 사용자가 액세스할 수 있는 Core입니다. 예를 들어, 자체 관리 Core는 종종 오프사이트 위치의 사용자 회사에서 관리하거나 소스 Core와는 다른 지리적 위치에서 호스팅됩니다. 복제는 시드 드라이브를 사용하여 데이터를 시드하도록 선택하지 않는 경우 소스 Core에만 설치할 수 있습니다. 이 경우 이 절차를 사용하여 시드 드라이브를 생성해야 하며 나중에 시드 드라이브를 대상 Core에 연결하여 보관된 복구 지점 데이터를 사용할 수 있습니다. 자세한 내용은 시딩 요구 및 전략 확인을(를) 참조하십시오.

자체 관리 대상 Core에 복제하도록 소스 Core를 구성하려면 다음 절차의 단계를 완료하십시오.

1 소스 Core의 Rapid Recovery Core 콘솔로 이동합니다.

2 버튼 모음에서 **Replicate(복제)**를 클릭합니다.
Replication Wizard(복제 마법사) 마법사가 나타납니다.

3 Replication Wizard(복제 마법사)의 **Target Core(대상 Core)** 페이지에서 이전에 소스 Core와 페어링된 대상 Core를 사용하여 복제를 설정하는 경우 **Use an existing target Core(기존 대상 Core 사용)**를 선택한 다음 드롭다운 목록에서 적절한 대상 Core를 선택합니다. 5단계로 건너뜁니다.

4 Replication Wizard(복제 마법사)의 **Target Core(대상 Core)** 페이지에서 처음으로 이 소스 Core에서 대상 Core를 사용하여 복제를 설정하는 경우 **I have my own Target Core(내 전용 대상 Core가 있음)**를 선택한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 128. 대상 Core 정보

텍스트 상자	설명
호스트 이름	복제할 Core 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
포트	Rapid Recovery Core가 시스템과 통신하는 포트 번호를 입력합니다.

텍스트 상자	설명
	기본 포트 번호는 8006입니다.
사용자 이름	시스템에 액세스하는 사용자 이름을 입력합니다.
암호	시스템에 액세스할 암호를 입력합니다.

5 **다음**을 클릭합니다.

노트: 리포지토리가 대상 Core에 없는 경우 소스 Core를 대상 Core와 페어링할 수 있지만 리포지토리를 설정할 때까지는 이 위치로 에이전트(보호되는 시스템)를 복제할 수 없음을 알리는 경고 메시지가 나타납니다. Core에 리포지토리를 설정하는 방법에 대한 자세한 내용은 DVM 리포지토리 생성을(를) 참조하십시오.

6 **Request(요청)** 페이지에서 이 복제 구성에 대한 이름(예: SourceCore1)을 입력합니다. 이 이름은 대상 Core의 복제 페이지에서 대한 Incoming Replication(들어오는 복제) 창에 사용되는 표시 이름입니다.

7 **다음**을 클릭합니다.

8 **Protected Machines(보호되는 시스템)** 페이지에서 복제할 보호되는 시스템을 선택하고 Repository(리포지토리) 열에 있는 드롭다운 목록에서 각 보호되는 시스템의 리포지토리를 선택합니다.

9 기본 데이터의 전송을 위한 시드 프로세스를 수행하려면 다음 단계를 완료하십시오.

노트: 휴대용 저장 장치에 대량 데이터를 복사해야 하므로 휴대용 저장 장치에 eSATA, USB 3.0 또는 기타 고속 연결 장치를 사용하는 것이 좋습니다.

a Replication Wizard(복제 마법사)의 **Protected Machines(보호되는 시스템)** 페이지에서 **Use a seed drive to perform the initial transfer(초기 전송을 수행하기 위해 시드 드라이브 사용)**를 선택합니다.
   - 현재 대상 Core에 보호되는 시스템을 하나 이상 복제하는 경우 **Include already replicated recovery points in the seed drive(시드 드라이브에 이미 복제된 복구 지점 포함)**를 선택하여 시드 드라이브에 이러한 보호되는 시스템을 포함할 수 있습니다

b **다음**을 클릭합니다.

c Replication Wizard(복제 마법사)의 **Seed Drive Location(시드 드라이브 위치)** 페이지에서 **Location Type(위치 유형)** 드롭다운 목록을 사용하여 다음 대상 유형 중에서 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드

d c단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 시드 드라이브 파일의 세부 정보를 입력합니다.

표 129. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이 위치는 시드 드라이브 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: D:\work\archive).
네트워크	출력 위치	출력 위치를 입력합니다. 이 위치는 시드 드라이브 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.

옵션	텍스트 상자	설명
	폴더 이름	아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 Rapid-Recovery-Archive-[DATE CREATED]-[TIME CREATED]입니다.

e **다음**을 클릭합니다.

f Replication Wizard(복제 마법사)의 **Seed Drive Options(시드 드라이브 옵션)** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 130. 시드 드라이브 옵션

항목	설명
최대 크기	대규모 데이터 아카이브는 여러 개의 세그먼트로 나눌 수 있습니다. 다음 중 하나를 수행하여 시드 드라이브 생성을 위해 예약할 최대 세그먼트 크기를 선택합니다. · Seed Drive Location(시드 드라이브 위치) 페이지에 입력된 경로에서 나중에 사용할 수 있도록 모든 사용 가능한 공간을 예약하려면 **Entire Target(전체 대상)**을 선택합니다. 예를 들어, 위치가 **D:\work\archive**일 경우 시드 드라이브를 복사할 때 필요하면 D: 드라이브에 있는 모든 사용 가능한 공간이 예약되지만 복사 프로세스가 시작된 후 곧바로 예약되지는 않습니다. · 텍스트 상자를 선택하고 공간의 양을 입력한 다음 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다. 기본값은 250MB입니다.
재활용 작업	경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다. · **Do not reuse(재사용 안 함)** - 위치에서 기존 시드 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있는 경우 시드 드라이브 쓰기가 실패합니다. · **Replace this core(이 코어 대체)**: 이 코어와 관련된 기존의 시드 데이터를 덮어쓰지만 다른 코어의 데이터는 그대로 남아 있게 됩니다. · **Erase completely(완전히 지우기)** - 시드 드라이브를 쓰기 전에 디렉터리에서 모든 시드 데이터를 지웁니다.
주석	시드 드라이브를 설명하는 주석을 입력합니다.
Add all Agents to Seed Drive(시드 드라이브에 모든 에이전트 추가)	시드 드라이브를 사용하여 소스 Core에 있는 모든 보호되는 시스템을 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다.
복구 지점 체인 빌드(분리된 복구 해결)	전체 복구 지점망을 시드 드라이브에 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본으로 선택되어 있습니다. **노트: AppAssure 5.4에서 일반적인 시딩 작업은 시드 드라이브에 최신 복구 지점만 복제하므로 시드 드라이브를 생성하는 데 필요한 시간과 공간을 절약할 수 있습니다. 시드 드라이브에 복구 지점(RP)망 빌드를 사용하려면 지정된 보호되는 시스템의 최신 복구 지점을 저장할 수 있는 충분한 공간이 시드 드라이브에 있어야 하며 작업이 완료되는 데 추가적인 시간이 소요될 수 있습니다.**

g 다음 중 하나를 수행합니다.

· **Add all Agents to Seed Drive(시드 드라이브에 모든 에이전트 추가)** 확인란 선택을 취소한 경우 **Next(다음)**를 클릭합니다.

· **Add all Agents to Seed Drive(시드 드라이브에 모든 에이전트 추가)**를 선택한 경우 10단계로 이동합니다.

h Replication Wizard(복제 마법사)의 **Protected Machines(보호되는 시스템)** 페이지에서 시드 드라이브를 사용하여 대상 Core에 복제합니다.

10 **마침**을 클릭합니다.

11 시드 드라이브를 생성한 후 대상 Core에 전송합니다.

소스 Core와 대상 Core의 페어링이 완료되었습니다.

초기에 복제를 일시 중지하기 위한 옵션을 선택한 경우가 아니라면, 복제 프로세스가 즉시 시작됩니다.

1 시드 드라이브를 사용하는 옵션을 선택한 경우, 복제는 시드 드라이브가 사용되고 필요한 기본 이미지를 제공할 때까지 대상 Core에 분리된 복구 지점을 생성합니다.

2 사용할 드라이브를 지정한 경우 시드 드라이브 아카이브 파일을 볼륨(공유 폴더, 가상 디스크 또는 이동식 저장소 매체)으로 전송합니다. 그런 다음 시드 드라이브를 사용합니다.

수신 및 발신 복제 보기

아이콘 표시줄에서 **복제** 아이콘을 클릭하면 **복제** 페이지가 나타납니다. 이 페이지에서 Core 범위 내의 복제 개념을 이해할 수 있습니다. 다음과 같은 두 개의 창이 표시됩니다.

- **보내는 복제** 창에는 다른 Core에 복제된 이 Core에서 보호되는 시스템이 나열됩니다.
- **들어오는 복제** 창에는 이 Core에 복제된 시스템과 해당 시스템이 복제된 소스 Core가 나열됩니다.

이 섹션에서는 창에 표시되는 정보를 설명합니다.

다음 표에서는 이 Rapid Recovery Core에서 보내는 복제에 대한 정보를 설명합니다.

표 131. 발신 복제 정보

UI 요소	설명
Select item(항목 선택)	요약 표에 있는 각 행의 확인란을 선택하고 표 위에 있는 메뉴 옵션 목록에서 작업을 수행할 수 있습니다.
유형	시스템 유형을 표시합니다. 대상 Core를 확장하여 각 복제된 시스템을 표시할 수 있습니다.
상태 표시기	복제 상태. 상태 열의 색상 원이 복제된 시스템이 온라인 상태인지 연결할 수 없는 상태인지 보여줍니다. 색상 원으로 커서를 가져가면 상태 조건이 표시됩니다. 상태 조건에는 녹색(복제가 설정되고 온라인 상태임), 노란색(복제 일시 중지됨), 빨간색(인증 오류) 및 회색(오프라인이거나 연결할 수 없음)이 있습니다.
Replication Name(복제 이름)	이 소스 Core에 있는 시스템이 복제되는 Core 시스템의 표시 이름.
시스템	선택한 대상 Core로 복제되는 시스템 수를 나열합니다.
동기화	대상 Core에 마지막으로 복제를 전송한 날짜 및 시간.
	이 열에서 작업 드롭다운 메뉴를 클릭하면 특정 복제 관계에 대해 수행할 수 있는 작업 목록이 표시됩니다.

Outgoing Replication(보내는 복제) 그리드에 나열된 두 개 이상의 대상 Core에서 작업을 수행할 수 있습니다. 여러 대상 Core에서 작업을 수행하려면 그리드에 있는 각 Core의 확인란을 선택한 후 그리드 위에 있는 메뉴에서 수행할 작업을 선택하십시오. 다음 표에 설명되어 있는 작업을 수행할 수 있습니다.

표 132. Outgoing Replication(보내는 복제) 창에서 사용할 수 있는 전역 작업

UI 요소	설명
대상 Core 추가	이 소스 Core에서 보호되는 시스템을 복제할 다른 대상 Core를 정의할 수 있습니다.
새로 고침	표에 표시된 정보를 새로 고칩니다.
수행	복제를 수행합니다.
Pause	설정한 복제를 일시 중지합니다.
Resume	일시 중지한 복제를 재개합니다.
복사	선택한 보호된 시스템에 대한 기존 복구 지점을 시드 드라이브로 복사할 수 있는 복제 마법사를 엽니다.
삭제	발신 복제를 삭제합니다.

UI 요소	설명
Seed Drives(시드 드라이브)	복제를 설정했을 때 시드 드라이브로 데이터가 복사된 경우 이 메뉴 옵션이 나타납니다. 시드 드라이브가 저장된 시간 및 데이터를 포함하여 시드 드라이브 파일에 대한 정보가 표시됩니다. 축소 가능한 메뉴는 시드 드라이브 파일이 생성된 보호된 시스템 및 대상 Core를 나타냅니다.
	이 열에서 작업 드롭다운 메뉴를 클릭하면 특정 복제 관계에 대해 수행할 수 있는 작업 목록이 표시됩니다.

다음 표에서는 다른 Core에서 들어오는 복제에 대한 정보를 설명합니다.

표 133. 수신 복제 정보

UI 요소	설명
Select item(항목 선택)	요약 표에 있는 각 행의 확인란을 선택하고 표 위에 있는 메뉴 옵션 목록에서 작업을 수행할 수 있습니다.
유형	시스템 유형을 표시합니다. 소스 Core를 확장하여 각 복제된 시스템을 표시할 수 있습니다.
상태 표시기	복제 상태. 상태 열의 색상 원이 복제된 시스템이 온라인 상태인지 연결할 수 없는 상태인지 보여줍니다. 색상 원으로 커서를 가져가면 상태 조건이 표시됩니다. 상태 조건에는 녹색(복제가 설정되고 온라인 상태임), 노란색(복제 일시 중지됨), 빨간색(인증 오류) 및 회색(오프라인이거나 연결할 수 없음)이 있습니다.
Replication Name(복제 이름)	이 대상 Core에 복제된 보호된 시스템을 포함하는 소스 Core 시스템의 표시 이름. 이 이름은 복제 마법사를 사용하여 소스 Core에서 복제를 설정할 때 필요에 따라 지정할 수 있습니다.
시스템	이 대상 Core로 복제된 소스 Core에서 보호되는 시스템의 수를 나열합니다.
동기화	소스 Core에 마지막으로 복제를 전송한 날짜 및 시간.
	이 열에서 작업 드롭다운 메뉴를 클릭하면 특정 복제 관계에 대해 수행할 수 있는 작업 목록이 표시됩니다.

Incoming Replication(들어오는 복제) 그리드에 나열된 두 개 이상의 소스 Core에서 작업을 수행할 수 있습니다. 여러 소스 Core에서 작업을 수행하려면 그리드에 있는 각 Core의 확인란을 선택한 후 그리드 위에 있는 메뉴에서 수행할 작업을 선택하십시오. 다음 표에 설명되어 있는 작업을 수행할 수 있습니다.

표 134. Incoming Replication(들어오는 복제) 창에서 사용할 수 있는 전역 작업

UI 요소	설명
새로 고침	표에 표시된 정보를 새로 고칩니다.
수행	복제를 수행합니다.
Pause	설정한 복제를 일시 중지합니다.
Resume	일시 중지한 복제를 재개합니다.
삭제	수신 복제를 삭제합니다.

복제 구성

Rapid Recovery를 사용하여 데이터를 복제하려면 소스 및 대상 Core를 복제할 수 있도록 구성해야 합니다. 복제를 구성한 후 보호되는 시스템 데이터를 복제하고, 복제를 모니터 및 관리하고, 복구를 수행할 수 있습니다.

Rapid Recovery에서 복제를 수행하면 다음 작업이 수행됩니다.

- 대상 Core의 리포지토리를 설정합니다. 대상 Core에 리포지토리를 추가하는 자세한 내용은 DVM 리포지토리 생성을(를) 참조하십시오.
- 자체 관리 복제를 구성합니다. 자체 관리 대상 Core에 복제에 대한 자세한 내용은 자체 관리 대상 Core로 복제를 참조하십시오.
- 타사 복제를 구성합니다. 타사 대상 Core에 복제에 대한 자세한 내용은 타사 대상 Core로 복제을(를) 참조하십시오.
- 기존의 보호되는 시스템을 복제합니다. 이미 소스 Core에 의해 보호되는 시스템 복제에 대한 자세한 내용은 기존 복제에 시스템 추가을(를) 참조하십시오.
- 시드 드라이브를 사용합니다. 대상 Core에서 시드 드라이브 데이터 사용에 대한 자세한 내용은 대상 Core에서 시드 드라이브 사용을(를) 참조하십시오.
- 보호되는 시스템의 복제 우선순위를 설정합니다. 보호되는 시스템의 복제 우선순위 설정에 대한 자세한 내용은 보호된 시스템의 복제 우선 순위 설정을(를) 참조하십시오.
- 보호되는 시스템에 대한 복제 일정을 설정합니다. 복제 일정 설정에 대한 자세한 내용은 복제 일정 설정을(를) 참조하십시오.
- 필요한 경우 복제를 모니터합니다. 복제 모니터링에 대한 자세한 내용은 수신 및 발신 복제 보기을(를) 참조하십시오.
- 필요에 따라 복제 설정을 관리합니다. 복제 설정 관리에 대한 자세한 내용은 복제 설정 관리를 참조하십시오.
- 재난 또는 데이터 유실이 발생할 경우 복제된 데이터를 복구합니다. 복제된 데이터 복구에 대한 자세한 내용은 복제된 데이터 복구를 참조하십시오.

타사 대상 Core로 복제

타사 Core는 MSP에 의해 관리되고 유지되는 대상 Core입니다. 타사에 의해 관리되는 Core에 복제하는 경우 고객이 대상 Core에 액세스할 필요가 없습니다.

타사 Core로의 복제 프로세스에는 고객 및 타사가 완료해야 하는 작업이 포함됩니다. 고객이 소스 Core에서 복제 요청을 제출한 후 MSP에서 요청을 검토하여 대상 Core 구성을 완료해야 합니다.

노트: 이 구성은 호스트 및 클라우드 복제에 적용됩니다. Rapid Recovery Core를 모든 소스 Core 시스템에 설치해야 합니다. 멀티 포인트 투 포인트 복제를 위해 Rapid Recovery를 구성하는 경우 모든 소스 Core에서 이 작업을 수행해야 합니다.

타사에 의해 관리되는 대상 Core에 복제하려면 다음 작업을 완료하십시오.

- 타사 서비스 공급자에게 복제 요청 제출
- 고객의 복제 요청 검토
- 고객의 복제 요청 무시

타사 서비스 공급자에게 복제 요청 제출

MSP 등 타사에 의해 관리되는 Core를 구독하는 최종 사용자의 경우 타사 서비스 공급자에게 복제 요청을 제출하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core로 이동합니다.

2 아이콘 단추 모음에서 **복제**를 클릭합니다.
복제 마법사가 나타납니다.

3 복제 마법사의 **대상 Core** 페이지에서 **타사가 제공하는 오프사이트 백업 및 재해 복구 서비스에 가입했습니다**를 선택한 후 다음 표에 설명된 대로 정보를 입력합니다.

표 135. 타사 대상 Core 정보

텍스트 상자	설명
호스트 이름	타사 Core 시스템의 호스트 이름, IP 주소 또는 FQDN을 입력합니다.
포트	타사 서비스 공급자가 제공한 포트 번호를 입력합니다. 기본 포트 번호는 8006입니다.

- 추가할 Core가 이전에 소스 Core와 페어링된 경우 다음 단계를 수행할 수 있습니다.
  1. **기존 대상 Core 사용**을 선택합니다.
  2. 드롭다운 목록에서 대상 Core를 선택합니다.
  3. **다음**을 클릭합니다.
  4. 7단계로 건너뜁니다.

4. **다음**을 클릭합니다.
5. 복제 마법사의 **요청** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 136. 타사 대상 Core 세부 정보

텍스트 상자	설명
이메일 주소	타사 서비스 구독과 연결된 이메일 주소를 입력합니다.
고객 ID(선택 사항)	(선택 사항) 서비스 공급자가 할당한 고객 ID를 입력합니다.

6. **다음**을 클릭합니다.
7. 복제 마법사의 **보호된 시스템** 페이지에서 타사 Core로 복제하려는 보호된 시스템을 선택합니다.
8. 기본 데이터 전송에 대해 시딩 프로세스를 수행하려면 다음 단계를 완료합니다.

노트: 대량의 데이터를 휴대용 저장 장치에 복사해야 하므로 eSATA, USB 3.0 또는 휴대용 저장 장치에 대한 기타 고속 연결이 권장됩니다.

a. 복제 마법사의 **보호된 시스템** 페이지에서 **시드 드라이브를 사용하여 초기 전송 수행**을 선택합니다.
   - 현재 대상 Core로 복제 중인 하나 이상의 보호된 시스템이 있는 경우 **이미 시드 드라이브에 복제된 복구 지점이 포함됨** 옵션을 선택하여 시드 드라이브에 이러한 시스템을 포함할 수 있습니다.

b. **다음**을 클릭합니다.

c. 복제 마법사의 **시드 드라이브 위치** 페이지에서 **위치** 유형 드롭다운 목록을 사용하여 다음과 같은 대상 유형에서 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드

d. C단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 아카이브의 세부 정보를 입력합니다.

표 137. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이것은 시드 드라이브 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: D:\work\archive).
네트워크	출력 위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.

옵션	텍스트 상자	설명
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가를 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.
	폴더 이름	아카이브된 데이터를 저장할 폴더의 이름을 입력합니다. 기본 이름은 Rapid-Recovery-Archive-[작성된 날짜]-[작성된 시간]입니다.

e **다음**을 클릭합니다.

f 복제 마법사의 **시드 드라이브 옵션** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 138. 시드 드라이브 옵션

항목	설명
최대 크기	대형 데이터 아카이브를 여러 세그먼트로 나눌 수 있습니다. 다음 작업 중 하나를 수행하여 시드 드라이브를 만들기 위해 예약할 공간의 최대 크기를 선택합니다. • **전체 대상**을 선택하여 시드 드라이브 위치 페이지에 제공된 경로에서 사용 가능한 모든 공간을 예약합니다. 예를 들어, 위치가 D:\work\archive인 경우 D: 드라이브의 모든 사용 가능한 공간이 예약됩니다. • 빈 텍스트 상자를 선택하고 양을 입력한 후 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다.
휴지통 작업	경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다. • **재사용 안 함**. 위치의 기존 시드 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있지 않은 경우 시드 드라이브 쓰기가 실패합니다. • **이 Core 바꾸기**. 이 Core와 관련된 기존 시드 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다. • **완전 삭제**. 시드 드라이브를 쓰기 전에 디렉터리에서 모든 시드 데이터를 지웁니다.
설명	시드 드라이브를 나타내는 설명을 입력합니다.
시드 드라이브에 모든 Agent 추가	시드 드라이브를 사용하여 소스 Core의 모든 보호된 시스템을 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다.
Build recovery points chains (fix orphans)(복구 지점망 구축(분리된 항목 수정))	전체 복구 지점 체인을 시드 드라이브에 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다. **노트: AppAssure 5.4의 일반적인 시딩은 최신 복구 지점만 시드 드라이브에 복제하며, 이에 따라 시드 드라이브를 만드는 데 필요한 시간과 공간이 줄어듭니다. 시드 드라이브에 복구 지점(RP) 체인을 구축하려면 지정한 보호된 시스템의 최신 복구 지점을 저장하기 위한 시드 드라이브의 공간이 필요하며, 이 작업을 완료하기 위해 시간이 더 걸릴 수 있습니다.**

g 다음 작업 중 하나를 수행합니다.

- **시드 드라이브에 모든 Agent 추가** 확인란을 선택 해제한 경우 **다음**을 클릭합니다.
- **시드 드라이브에 모든 Agent 추가**를 선택한 경우 9단계로 이동합니다.

h 복제 마법사의 **시스템** 페이지에서 시드 드라이브를 사용하여 대상 Core로 복제하려는 보호된 시스템을 선택합니다.

9 **마침**을 클릭합니다.

10 시드 드라이브를 만든 경우 타사 서비스 공급자가 지시한 대로 보냅니다.

고객의 복제 요청 검토

최종 사용자가 타사 서비스 공급자에게 복제 요청 제출 절차를 완료한 후 복제 요청이 소스 Core에서 타사 대상 Core로 전송됩니다. 타사는 요청을 검토한 후 승인하여 고객을 위해 복제를 시작하거나 요청을 거부하여 복제가 발생하지 않도록 차단할 수 있습니다.

다음 옵션 중에서 선택합니다.

- 복제 요청 승인
- 복제 요청 거부

복제 요청 승인

타사 대상 Core에서 복제 요청을 승인하려면 다음 절차를 완료하십시오.

1 대상 Core에서 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

3 **복제** 페이지에서 **요청 (#)**를 클릭합니다.
Pending Replication Requests(보류 중인 복제 요청) 섹션이 표시됩니다.

4 보류 중인 복제 요청에서 검토할 요청 옆의 드롭다운 메뉴를 클릭한 후 **검토**를 클릭합니다.
Review Replication Request(복제 요청 검토) 창이 표시됩니다.

노트: 이 창의 소스 Core ID 섹션에 나타나는 정보는 고객이 완료하는 요청에 의해 결정됩니다.

5 소스 Core ID에서 다음 작업 중 하나를 수행합니다.
- **Replace an existing replicated Core(복제된 기존 Core 생성)**를 선택하고 드롭다운 목록에서 Core를 선택합니다.
- **새 소스 Core 만들기**를 선택한 후 제공된 Core 이름, 고객 이메일 주소, 고객 ID가 올바른지 확인합니다. 필요한 경우 정보를 편집합니다.

6 에이전트 아래에서 승인할 시스템을 선택한 후 리포지토리 열의 드롭다운 목록을 사용하여 각 시스템에 대해 적절한 리포리토리를 선택합니다.

7 (선택 사항) **설명** 텍스트 상자에 고객에게 보낼 응답에 포함할 설명이나 메시지를 입력합니다.

8 **응답 보내기**를 클릭합니다.
복제가 허용됩니다.

복제 요청 거부

고객이 타사 Core에 보낸 복제 요청을 거부하려면 다음 단계를 완료하십시오.

요청을 검토하지 않고 거부하려면 고객의 복제 요청 무시을(를) 참조하십시오.

1 대상 Core에서 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

3 **복제** 페이지에서 **요청 (#)**을 클릭합니다.
Pending Replication Requests(보류 중인 복제 요청) 섹션이 표시됩니다.

4 보류 중인 복제 요청에서 검토할 요청 옆의 드롭다운 메뉴를 클릭한 후 **검토**를 클릭합니다.
Review Replication Request(복제 요청 검토) 창이 표시됩니다.

5 **거부**를 클릭합니다.

복제가 거부됩니다. 소스 Core의 이벤트 페이지에 있는 경고 아래 거부 알림이 나타납니다.

고객의 복제 요청 무시

대상 Core의 타사 서비스 공급자는 고객이 보낸 복제 요청을 무시할 수 있습니다. 이 옵션은 요청이 잘못 전송되었거나 요청을 검토하지 않고 거부하려는 경우 유용합니다.

복제 요청에 대한 자세한 내용은 고객의 복제 요청 검토을(를) 참조하십시오.

고객의 복제 요청을 무시하려면 다음 절차를 완료하십시오.

1 대상 Core에서 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

3 **복제** 페이지에서 **요청 (#)**을 클릭합니다.
Pending Replication Requests(보류 중인 복제 요청) 섹션이 표시됩니다.

4 보류 중인 복제 요청에서 무시할 요청 옆의 드롭다운 메뉴를 클릭한 후 **무시**를 클릭합니다.

5 **요청 무시** 대화 상자에서 **예**를 클릭하여 명령을 확인합니다.
요청이 무시되었다는 알림이 소스 Core에 전송되고 요청이 대상 Core의 복제 페이지에서 제거됩니다.

기존 복제에 시스템 추가

소스 Core와 대상 Core 사이에 복제가 설정된 후 대상으로 복제할 새로운 보호된 시스템을 추가할 수 있습니다. 복제를 위해 페어링된 대상 Core에 새로운 보호된 시스템을 추가하려면 소스 Core에서 다음 절차의 단계를 완료하십시오.

복제에 대한 자세한 내용은 복제 및 자체 관리 대상 Core로 복제을(를) 참조하십시오.

1 소스 Core의 Rapid Recovery Core Console로 이동합니다.

2 단추 모음에서 **복제**를 클릭합니다.
복제 마법사에서 **보호된 시스템** 페이지가 열립니다.

3 **보호된 시스템** 페이지에서 복제하려는 보호된 시스템을 선택한 후 리포지토리 열의 드롭다운 목록을 사용하여 각 보호된 시스템에 대해 리포지토리를 선택합니다.

4 기본 데이터 전송에 대해 시딩 프로세스를 수행하려면 다음 단계를 완료하십시오.

노트: 대량의 데이터를 휴대용 저장 장치에 복사해야 하므로 eSATA, USB 3.0 또는 휴대용 저장 장치에 대한 기타 고속 연결이 권장됩니다.

a 복제 마법사의 **보호된 시스템** 페이지에서 **시드 드라이브를 사용하여 초기 전송 수행**을 선택합니다.
- 현재 대상 Core로 복제 중인 하나 이상의 보호된 시스템이 있는 경우 **이미 복제된 복구 지점을 시드 드라이브에 포함** 옵션을 선택하여 시드 드라이브에 해당 시스템을 포함할 수 있습니다.

b **다음**을 클릭합니다.

c 마법사의 **시드 드라이브 위치** 페이지에서 **위치** 유형 드롭다운 목록을 사용하여 다음 대상 유형 중에서 선택합니다.
- 로컬
- 네트워크
- 클라우드

d c단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 아카이브의 세부 정보를 입력합니다.

표 139. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	출력 위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.
	폴더 이름	아카이브된 데이터를 저장할 폴더의 이름을 입력합니다. 기본 이름은 Rapid-Recovery-Archive-[생성된 날짜]-[생성된 시간]입니다.

e **다음**을 클릭합니다.

f 마법사의 **시드 드라이브 옵션** 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 140. 시드 드라이브 옵션

항목	설명
최대 크기	대형 데이터 아카이브를 여러 세그먼트로 나눌 수 있습니다. 다음 작업 중 하나를 수행하여 시드 드라이브를 만들기 위해 예약할 공간의 최대 크기를 선택합니다. • **전체 대상**을 선택하여 시드 드라이브 위치 페이지에 제공된 경로에서 사용 가능한 모든 공간을 예약합니다. 예를 들어, 위치가 D:\work\archive인 경우 D: 드라이브의 모든 사용 가능한 공간이 예약됩니다. • 빈 텍스트 상자를 선택하고 양을 입력한 후 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다.
휴지통 작업	경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다. • 재사용 안 함. 위치의 기존 시드 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있지 않은 경우 시드 드라이브 쓰기가 실패합니다. • 이 Core 바꾸기. 이 Core와 관련된 기존 시드 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다. • 완전 삭제. 시드 드라이브를 쓰기 전에 디렉터리에서 모든 시드 데이터를 지웁니다.
설명	시드 드라이브를 나타내는 설명을 입력합니다.
시드 드라이브에 모든 Agent 추가	시드 드라이브를 사용하여 소스 Core의 모든 보호된 시스템을 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다.
복구 지점 체인 구축(분리된 항목 수정)	전체 복구 지점 체인을 시드 드라이브에 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다.

항목	설명
	노트: Rapid Recovery 5.4의 일반적인 시딩은 최신 복구 지점만 시드 드라이브에 복제하고, 이에 따라 시드 드라이브를 만드는 데 필요한 시간과 공간이 줄어듭니다. 시드 드라이브에 복구 지점(RP) 체인을 구축하려면 지정한 보호된 시스템의 최신 복구 지점을 저장하기 위한 시드 드라이브의 공간이 필요하며, 이 작업을 완료하기 위해 시간이 더 걸릴 수 있습니다.

g 다음 작업 중 하나를 수행합니다.

- **시드 드라이브에 모든 Agent 추가** 확인란을 선택 해제한 경우 **다음**을 클릭합니다.
- **시드 드라이브에 모든 Agent 추가**를 선택한 경우 5단계로 이동합니다.

h 마법사의 **보호된 시스템** 페이지에서 시드 드라이브를 사용하는 대상 Core로 복제할 보호된 시스템을 선택합니다.

5 **마침**을 클릭합니다.

대상 Core에서 시드 드라이브 사용

대상 Core의 시드 드라이브 파일에서 데이터를 사용하려면 다음 절차를 완료하십시오.

노트: 이 절차는 자체 관리 대상 Core로 복제 또는 타사 대상 Core로 복제 파트로 시드 드라이브 파일이 만들어진 경우에만 필요합니다.

1 시드 드라이브 파일이 휴대용 저장 장치(예: USB 드라이브)에 저장되어 있으면 드라이브를 대상 Core에 연결합니다.

2 대상 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 표시됩니다.

3 **복제** 페이지의 들어오는 복제 아래에서 올바른 원본 Core의 드롭다운 메뉴를 클릭한 후 **사용**을 클릭합니다.
사용 대화 상자가 표시됩니다.

4 **위치 유형** 필드의 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.

- 로컬
- 네트워크
- 클라우드

5 4단계에서 선택한 위치 유형에 따라 다음 표에 설명된 대로 시드 드라이브 보관 파일의 세부 정보를 입력합니다.

표 141. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	위치	아카이브 경로를 입력합니다.
네트워크	위치	아카이브 경로를 입력합니다.
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.

옵션	텍스트 상자	설명
	폴더 이름	보관된 데이터를 저장할 폴더 이름을 입력합니다(예: Rapid-Recovery-Archive-[만든 날짜]-[만든 시간]).

6 **파일 검사**를 클릭합니다.
Core가 파일을 검색합니다.

파일을 찾으면 4단계, 5단계 및 파일에서 수집된 데이터로 미리 채워진 다음 텍스트 상자가 사용 창에 표시됩니다. 시드 드라이브에 포함된 가장 오래된 복구 지점과 가장 최신 복구 지점의 날짜가 날짜 범위에 표시됩니다. 시드 드라이브를 만들 때 입력된 모든 설명을 자동으로 가져옵니다.

7 **사용** 대화 상자의 에이전트 아래에서 데이터를 사용하려는 시스템을 선택합니다.

8 **사용**을 클릭합니다.

9 데이터 사용의 진행 상태를 모니터링하려면 이벤트 페이지를 확인합니다.

시드 드라이브 취소

대상 Core에서 사용하기 위해 시드 드라이브를 생성했지만 나중에 이를 사용하지 않으려는 경우 시드 드라이브를 취소할 수 있습니다.

시드 드라이브를 취소하거나 사용하기 전에는 대기 중인 시드 드라이브에 대한 링크는 소스 Core의 보내는 복제 창에 남아 있습니다.

시드 드라이브에서 정보를 전송한 후에만 대상 Core가 아닌 원래 보호된 시스템에 있는 분리된 복구 지점을 사용하여 데이터를 복원할 수 있습니다.

주의: 시드 드라이브를 취소하면 시드 드라이브 파일에 정의된 원래 복구 지점은 다음 복제 작업 중에 네트워크를 통해 대상 Core로 전송됩니다. 네트워크를 통해 이전 복구 지점을 전송하는 경우 복구 지점이 많으면 특히 네트워크 속도가 느려질 수 있습니다.

대기 중인 시드 드라이브를 취소하려면 다음 단계를 완료하십시오.

노트: Core Console에서 시드 드라이브를 취소하면 해당 저장 위치의 시드 드라이브 파일에는 영향을 주지 않습니다.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)을 클릭합니다.
복제 페이지가 나타납니다.

2 **복제** 페이지의 보내는 복제 창에서 **시드 드라이브 번호**를 클릭합니다.
Outgoing Replication(보내는 복제) 창에는 대기 중인 시드 드라이브에 대한 정보를 포함하는 섹션이 나타납니다.

3 필요한 경우 아래 화살표 ▼를 클릭하여 축소할 수 있는 메뉴를 확장합니다.
시드 드라이브에 포함된 복구 지점의 날짜 범위와 대상 Core를 포함하여 대기 중인 시드 드라이브에 대한 정보가 나타납니다.

4 그런 다음, 를 클릭하여 취소할 시드 드라이브 파일의 드롭다운 메뉴를 열고 **취소**를 선택합니다.

5 확인 창에서 시드 드라이브를 취소할 것인지 확인합니다.
시드 드라이브가 제거됩니다.

소스 Core에 시드 드라이브가 더 없으면 Outgoing Replication(보내는 복제) 창에서 시드 드라이브 번호와 대기 중인 시드 드라이브 섹션이 제거됩니다.

복제 설정 관리

Rapid Recovery를 사용하면 복제를 전체, Core 및 보호된 시스템 수준에서 모니터링, 예약 및 조정할 수 있습니다.

다음과 같은 복제 설정을 편집할 수 있습니다.

- 복제 작업 일정을 설정하려면 복제 일정 설정을(를) 참조하십시오.
- 이미 복제를 위해 페어링한 보호된 시스템의 시드 드라이브를 만들려면 다음을 참조하십시오. 복사 기능을 사용하여 시드 드라이브 만들기
- 복제 작업의 진행 상태를 모니터링하려면 수신 및 발신 복제 보기을(를) 참조하십시오.
- 복제 작업을 일시 중지하거나 일시 중지된 복제 작업을 다시 시작하려면 복제 일시 중지 및 다시 시작을(를) 참조하십시오.
- 수신 또는 발신 보호된 시스템 복제를 수행하려면 복제 수행을(를) 참조하십시오.
- 모든 대상 Core 및 복제 절차에 대한 설정을 관리하려면 발신 복제 설정 관리을(를) 참조하십시오.
- 개별 대상 Core에 대한 설정을 관리하려면 대상 Core 설정 변경을(를) 참조하십시오.
- 대상 Core로 복제되는 개별 보호된 시스템에 대한 우선 순위 설정을 관리하려면 보호된 시스템의 복제 우선 순위 설정을(를) 참조하십시오.

복제 일정 설정

복제 일정을 설정하여 기본 동작을 변경하지 않으면 Core에서는 모든 백업 스냅숏, 체크섬 검사, 연결 기능 검사, 야간 작업을 완료한 후 즉시 복제 작업을 시작합니다. 자세한 내용은 복제 일정 설정을(를) 참조하십시오.

네트워크의 부하를 줄이기 위해 복제 일정을 변경할 수 있습니다.

다음 절차의 단계를 완료하여 복제된 시스템에 대한 복제 일정을 설정합니다.

1 대상 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

2 보내는 복제 창에서 을 클릭하여 복제 일정을 설정하려는 Core 옆의 드롭다운 메뉴를 열고 **예약**을 선택합니다.
[CoreName]의 복제 일정 대화 상자가 열립니다.

3 다음 세 가지 옵션 중 하나를 선택합니다.
- **항상**. 모든 새 스냅숏, 체크섬 검사, 연결성 검사 및 야간 작업 완료 후 복제합니다.
- **매일(지정된 기간 동안만 복제 시작)**. 제공된 시간 범위 내에서만 복제를 시작합니다.
  1 **시작** 텍스트 상자에 복제 시작 시간을 입력합니다.
  2 **종료** 텍스트 상자에 복제 종료 시간을 입력합니다.

  노트: 예약 시간이 종료될 때 복제가 진행 중이면 할당된 기간 후에 복제 작업이 완료됩니다.
- **사용자 지정**. 제공된 시간 범위에서만 복제를 시작하여 평일에는 하나의 시간 범위, 주말에는 다른 시간 범위를 설정할 수 있습니다.
  1 평일 옆의 **시작** 텍스트 상자에 평일의 복제 시작 시간을 입력한 후 **종료** 텍스트 상자에 평일의 복제 종료 시간을 입력합니다.
  2 주말 옆의 **시작** 텍스트 상자에 주말의 복제 시작 시간을 입력한 후 **종료** 텍스트 상자에 주말의 복제 종료 시간을 입력합니다.

4 **저장**을 클릭합니다.
일정이 선택한 대상 Core의 모든 복제에 적용됩니다.

복사 기능을 사용하여 시드 드라이브 만들기

복제를 구성할 때 시드 드라이브를 만들지 않은 경우에는 보호된 시스템 드롭다운 메뉴의 복사 기능을 사용하여 시드 드라이브를 만들 수 있습니다.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)을 클릭합니다.

복제 페이지가 나타납니다.

2 **복제** 페이지의 보내는 복제 창에서 ▼을 클릭하여 시드 드라이브를 생성할 시스템을 보호하는 Core를 확장합니다.
지정된 Core에 있는 각 보호된 시스템을 표시하도록 선택 내용이 확장됩니다.

3 표의 첫 번째 행을 클릭하여 시드 드라이브를 생성할 각각의 시스템을 선택합니다.

4 보내는 복제 창에 있는 메뉴에서 **복사**를 클릭합니다.
복제 마법사가 나타납니다.

5 마법사의 **시드 드라이브 위치** 페이지에서 **위치** 드롭다운 목록을 사용하여 다음 대상 유형 중에서 선택합니다.
- 로컬
- 네트워크
- 클라우드

6 앞 단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 시드 드라이브 아카이브의 세부 정보를 입력합니다.

표 142. 아카이브 세부 정보

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	출력 위치	출력 위치를 입력합니다. 이것은 아카이브를 둘 위치 경로를 정의하는 데 사용됩니다(예: \\servername\sharename).
	사용자 이름	사용자 이름을 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이 사용자 이름은 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트: 클라우드 계정을 선택하려면 우선 Core Console에서 클라우드 계정을 추가해야 합니다. 자세한 내용은 클라우드 계정 추가을(를) 참조하십시오.**
	컨테이너	드롭다운 메뉴에서 계정에 관련된 컨테이너를 선택하십시오.
	폴더 이름	아카이브된 데이터를 저장할 폴더의 이름을 입력합니다. 기본 이름은 Rapid-Recovery-Archive-[생성된 날짜]-[생성된 시간]입니다.

7 **다음**을 클릭합니다.

8 시드 드라이브 옵션 페이지에서 다음 표에 설명된 대로 정보를 입력합니다.

표 143. 시드 드라이브 옵션

항목	설명
최대 크기	대형 데이터 아카이브를 여러 세그먼트로 나눌 수 있습니다. 다음 작업 중 하나를 수행하여 시드 드라이브를 만들기 위해 예약할 공간의 최대 크기를 선택합니다. - **전체 대상**을 선택하여 시드 드라이브 위치 페이지에 제공된 경로에서 사용 가능한 모든 공간을 예약합니다. 예를 들어, 위치가 D:\work\archive인 경우 D: 드라이브의 모든 사용 가능한 공간이 예약됩니다. - 빈 텍스트 상자를 선택하고 양을 입력한 후 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다.
휴지통 작업	경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다. - **재사용 안 함.** 위치의 기존 시드 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있지 않은 경우 시드 드라이브 쓰기가 실패합니다. - **이 Core 대체**. 이 Core와 관련된 기존 시드 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다.

항목	설명
	• **완전히 지우기**. 시드 드라이브를 쓰기 전에 디렉터리에서 모든 시드 데이터를 지웁니다.
설명	시드 드라이브를 나타내는 설명을 입력합니다.
시드 드라이브에 모든 Agent 추가	시드 드라이브를 사용하여 소스 Core의 모든 보호된 시스템을 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다.
복구 지점 체인 구축(분리된 항목 수정)	전체 복구 지점 체인을 시드 드라이브에 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본적으로 선택됩니다. **노트: Rapid Recovery 5.4.x의 일반적인 시딩은 최신 복구 지점만 시드 드라이브에 복제하고, 이에 따라 시드 드라이브를 만드는 데 필요한 시간과 공간이 줄어듭니다. 시드 드라이브에 복구 지점 체인을 구축하려면 지정한 보호된 시스템의 최신 복구 지점을 저장하기 위한 시드 드라이브의 공간이 필요하며, 이 작업을 완료하기 위해 시간이 더 걸릴 수 있습니다.**

9 다음 작업 중 하나를 수행합니다.
- **시드 드라이브에 모든 Agent 추가** 확인란을 선택 해제한 경우 **다음**을 클릭합니다.
- **시드 드라이브에 모든 Agent 추가**를 선택한 경우 10단계로 이동합니다.

10 마법사의 **보호된 시스템** 페이지에서 시드 드라이브를 생성할 보호된 시스템을 선택합니다.

11 **마침**을 클릭합니다.

복제 모니터링

복제가 설정된 경우 소스 및 대상 Core에 대한 복제 작업의 상태를 모니터링할 수 있습니다. 상태 정보를 새로 고치고 복제 세부 정보 등을 볼 수 있습니다.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

2 이 페이지에서는 다음 표에 설명된 대로 복제 작업에 대한 정보를 보고 복제 작업의 상태를 모니터링할 수 있습니다.

표 144. 복제 작업

섹션	설명	사용 가능한 작업
시드 드라이브 수	복제 정의 시 시드 드라이브의 사용을 지정한 후 이를 중단 또는 사용할 때까지 **시드 드라이브 수** 링크가 소스 Core의 발신 복제 창에 나타납니다. 표시되는 번호는 보류 중인 시드 드라이브 수를 나타냅니다. **노트: 이 링크는 시드 드라이브가 보류 중이 아닌 경우 나타나지 않습니다.** 작성되었지만 아직 대상 Core에서 사용되지 않은 시드 드라이브를 나열하려면 이 링크를 클릭하십시오. 또한, 대상 Core와 시드 드라이브에 포함된 복구 지점의 날짜 범위를 포함해 남아 있는 시드 드라이브에 대한 정보를 표시하려면 축소 가능 메뉴를 확장합니다.	드롭다운 메뉴에서 **중단**을 클릭하여 시드 프로세스를 중단하거나 취소합니다. wn 메뉴
발신 복제	소스 Core가 복제되는 모든 대상 Core를 나열합니다. 여기에는 상태 표시기, 대상 Core 이름, 복제하려는 시스템 수 및 복제 전송 진행 상황 등이 있습니다.	소스 Core의 드롭다운 메뉴에서 다음 옵션을 선택할 수 있습니다.

섹션	설명	사용 가능한 작업
		• **세부 정보** - ID, URL, 표시 이름, 상태, 고객 ID, 이메일 주소 및 복제된 Core에 대한 주석을 나열합니다. • **설정 변경.** 표시 이름을 나열하며 대상 Core의 호스트 및 포트를 편집할 수 있습니다. • **예약.** 이 대상 Core로의 복제에 대한 사용자 지정 일정을 설정할 수 있습니다. • **시스템 추가.** 드롭다운 목록에서 호스트를 선택하고 복제를 위해 보호된 시스템을 선택한 다음 새로운 보호된 시스템의 초기 전송을 위한 시드 드라이브를 만들 수 있습니다. 경우에 따라 이미 복제에 추가된 시스템의 복구 지점을 포함하도록 선택할 수 있습니다. • **삭제.** 소스와 대상 Core 간의 복제 관계를 삭제할 수 있습니다. 이렇게 하면 이 Core로의 모든 복제가 중단됩니다.
수신 복제	대상이 복제된 데이터를 수신하는 모든 원본 시스템이 나열됩니다. 여기에는 원격 Core 이름, 상태, 시스템 및 진행 상황이 포함됩니다. 대상이 복제된 데이터를 수신하는 모든 소스 Core를 나열합니다. 나열된 소스 Core에 대한 표시 이름은 복제 정의 시 복제 마법사에서 값으로 채워집니다. 여기에는 상태 표시기, 원격 Core 이름 및 복제 전송 진행 상황 등이 있습니다.	대상 Core의 ⚙ 드롭다운 메뉴에서 다음 옵션을 선택할 수 있습니다. • **세부 정보.** 복제된 Core의 ID, 호스트 이름, 고객 ID, 이메일 주소 및 주석을 나열합니다. • **사용.** 시드 드라이브의 초기 데이터를 사용하고 로컬 리포지토리에 저장합니다. • **삭제.** 대상과 소스 Core 간의 복제 관계를 삭제할 수 있습니다. 이렇게 하면 이 Core에서 모든 복제가 중단됩니다.
보류 중인 복제 요청	이 정보는 관리 서비스 공급자에게만 적용됩니다. 고객이 수신 복제 창에서 **요청** 링크를 클릭하면 요청에 대한 고객 ID, 이메일 주소 및 호스트 이름이 나열된 요약 표 섹션이 나타납니다.	드롭다운 메뉴에서 요청을 무시하거나 거절하려면 **무시**를 클릭하고 보류 중 요청을 검토하려면 **검토**를 클릭합니다.

복제 일시 중지 및 다시 시작

소스(발신) Core 또는 대상(수신) Core에 대한 복제를 일시 중지할 수 있습니다.

복제를 일시 중지하는 옵션은 복제가 활성 상태일 때만 사용할 수 있습니다. 복제를 다시 시작하는 옵션은 복제가 일시 중지된 상태일 때만 사용할 수 있습니다.

다음 절차의 단계를 수행하여 복제를 일시 중지하거나 다시 시작합니다.

1 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)을 클릭합니다.
복제 페이지가 나타납니다.
2 복제된 모든 시스템에 대한 복제를 일시 중지하려면 다음을 수행합니다.
   a 요약 표 맨 위에 있는 확인란을 클릭하여 원본 또는 대상 Core를 선택합니다.
   b 요약 표 앞에 나오는 메뉴에서 **일시 중지**를 클릭합니다.
   선택한 Core에 있는 모든 보호된 시스템에 대한 복제가 일시 중지됩니다.
3 특정 시스템에 대한 복제만 일시 중지하려면 다음을 수행합니다.
   a Core 오른쪽에 있는 ▼ 화살표를 클릭합니다.
   복제 중인 선택한 Core의 각 보호된 시스템을 표시하도록 보기를 확장합니다.
   b 복제를 일시 중지할 각 시스템을 선택하려면 첫 번째 열을 클릭합니다. 일시 중지하지 않으려는 시스템의 확인란을 지우려면 선택한 열을 다시 클릭합니다.
   c 요약 표 앞에 나오는 메뉴에서 **일시 중지**를 클릭합니다.

선택한 보호된 시스템에 대한 복제가 일시 중지됩니다.

4 복제된 모든 시스템에 대한 복제를 다시 시작하려면 다음을 수행합니다.
   a 요약 표 맨 위에 있는 확인란을 클릭하여 원본 또는 대상 Core를 선택합니다.
   b 요약 표 맨 위에 있는 메뉴에서 **다시 시작**을 클릭합니다.
   선택한 Core에 있는 모든 보호된 시스템에 대한 복제가 다시 시작됩니다.
5 특정 시스템에 대한 복제만 다시 시작하려면 다음을 수행합니다.
   a Core 오른쪽에 있는 ▼ 화살표를 클릭합니다.
   복제 중인 선택한 Core의 각 보호된 시스템을 표시하도록 보기를 확장합니다.
   b 복제를 다시 시작할 각 시스템을 선택하려면 첫 번째 열을 클릭합니다. 다시 시작하지 않으려는 시스템의 확인란을 지우려면 선택한 열을 다시 클릭합니다.
   c 요약 표 맨 위에 있는 메뉴에서 **다시 시작**을 클릭합니다.
   선택한 보호된 시스템에 대한 복제가 다시 시작됩니다.

복제 수행

소스 Core에서 백업 또는 연결성 검사와 같은 특정 이벤트 이후에 복제 작업이 대기열에서 지연되는 일 없이 언제든지 복제를 수행할 수 있습니다.

소스 Core 또는 대상 Core에서 복제를 수행하려면 다음 단계를 완료하십시오.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다
복제 페이지가 나타납니다.
2 다음 작업 중 하나를 수행합니다.

- 소스 Core에서 복제를 수행하려면 **발신 복제** 창에서 Core를 선택하고 요약 표 위쪽의 메뉴에서 **수행**을 클릭합니다.
- 대상 Core에서 복제를 수행하려면 **들어오는 복제** 창에서 Core를 선택하고 요약 표 위쪽의 메뉴에서 **수행**을 클릭합니다.

복제 수행 대화 상자가 나타납니다.
3 선택적으로, 복구 지점의 모든 분리된 체인을 복원하려면 **분리된 복구 지점 체인 복원**을 선택합니다.
4 확인을 위해 복제 수행 대화 상자에서 **예**를 클릭합니다.
대화 상자가 닫히고 복제가 수행됩니다.

발신 복제 설정 관리

이 설정을 변경하면 이 소스 Core와 연결된 모든 대상 Core로의 데이터 전송에 영향을 줍니다.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.
2 **발신 복제** 창의 요약 표 위쪽에서 (설정)을 클릭합니다.
복제 설정 대화 상자가 나타납니다.
3 **복제 설정** 대화 상자에서 다음 표에 설명된 대로 복제 설정을 편집합니다.

표 145. 복제 설정

옵션	설명
캐시 수명(초)	소스 Core에서 실행되는 대상 Core 상태 요청의 시간 간격을 지정합니다.
볼륨 이미지 세션 제한 시간(분)	소스 Core가 대상 Core로의 볼륨 이미지 전송을 시도하기 위해 사용하는 시간을 지정합니다.
최대 병렬 스트림	보호된 시스템 하나에서 해당 시스템의 데이터를 한 번에 복제하기 위해 사용할 수 있는 네트워크 연결의 수를 지정합니다.
최대 전송 속도(MB/s)	복제된 데이터의 전송 속도 제한을 지정합니다.
최대 데이터 전송 크기(GB)	복제된 데이터의 블록 전송에 필요한 최대 크기(GB)를 지정합니다.
Restore Defaults	모든 복제 설정을 시스템 기본값으로 변경하려면 이 옵션을 선택합니다. **노트: 이 옵션을 선택하기 전에 사용자 지정 설정을 기록해 둡니다. 이 작업을 확인하는 메시지가 표시되지 않습니다.**

4 선택 사항에 만족하면 **저장**을 클릭하여 복제 설정을 저장하고 대화 상자를 닫습니다.

대상 Core 설정 변경

소스 Core에서 개별 대상 Core에 대한 호스트 및 포트 설정을 변경할 수 있습니다.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

보내는 복제 창에서 요약 표는 이 소스 Core의 복구 지점을 복제하기 위해 구성된 각 대상 Core에 대한 행을 포함합니다.

2 수정하려는 대상 Core에 대한 (설정) 드롭다운 메뉴를 클릭한 다음 **설정 변경**을 선택합니다.
Settings(설정) 대화 상자가 나타납니다.

3 다음 표에 설명된 옵션 중 하나를 편집합니다.

표 146. 대상 Core 설정

옵션	설명
호스트	대상 Core의 호스트를 입력합니다.
포트	소스 Core와의 통신에 사용할 대상 Core의 포트를 입력합니다. **노트: 기본 포트는 8006입니다.**

4 **저장**을 클릭합니다.

보호된 시스템의 복제 우선 순위 설정

복제 우선 순위에서는 Core에 첫 번째로 전송되는 복제 작업이 결정됩니다. 우선 순위는 1부터 10까지 서수로 설정되는데 우선 순위 1은 첫 번째 우선 순위, 우선 순위 10은 마지막 우선 순위를 나타냅니다. 시스템에 대한 복제를 처음 설정할 때는 우선 순위가 5로 설정됩니다. 원본 Core의 보호된 시스템 수준에서 우선 순위를 보고 변경할 수 있습니다.

때로는 일부 복제 작업을 중단하는 것도 가능합니다. 예를 들어, 환경의 변경률이 비정상적으로 높거나 네트워크의 대역폭이 충분하지 않으면 복제 작업을 중단할 수 있습니다. 환경에서 복제가 진행되는 시간이 제한되도록 일정을 설정하면 이런 상황이 발생할 가능성이 특히 큽니다. 복제 일정 설정에 대한 자세한 내용은 복제 일정 설정을(를) 참조하십시오.

중요한 시스템에서 복제가 먼저 진행되게 하려면 중요 서버의 우선 순위를 낮은 번호(1부터 5 사이)로 지정합니다. 상대적으로 덜 중요한 시스템은 우선 순위를 높은 번호(6부터 10 사이)로 지정합니다.

보호된 시스템의 복제 우선 순위를 4로 설정하면 기본 복제 우선 순위가 5인 시스템에 앞서 복제 작업이 시작됩니다. 우선 순위가 3인 시스템의 복제 작업을 4에 앞서 큐에 넣는 식으로 진행됩니다. 우선 순위 번호가 낮을수록 복제 작업이 일찍 전송됩니다. 우선 순위 1이 가장 중요하다는 것을 잊지 말고 기억하십시오. 복제 우선 순위가 1인 시스템이 복제 큐의 첫 번째 시스템입니다.

보호된 시스템의 복제 우선 순위를 지정하는 설정을 편집하려면 다음 단계를 완료하십시오.

1 원본 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 표시됩니다.

2 **보내는 복제** 창에서 원본 코어의 오른쪽으로 ▼ 화살표를 클릭합니다.
뷰가 확장되어 지정된 대상 Core로 복제되고 있는 이 원본 Core에서 보호된 시스템이 각각 표시됩니다.

3 우선 순위를 지정하려는 보호된 컴퓨터의 (설정) 드롭다운 메뉴를 클릭한 후 **설정**을 클릭합니다.
대화 상자가 표시됩니다.

4 **우선 순위** 드롭다운 목록을 클릭하고 요구 사항을 기준으로 **1(최고)**부터 **10(최저)**까지 우선 순위를 선택합니다.

5 **저장**을 클릭합니다.
대화 상자가 닫히고 선택한 시스템의 복제 우선 순위가 업데이트됩니다.

복제 제거

복제는 하나의 Rapid Recovery Core(소스 Core)에서 두 번째 Core(대상 Core)로 보호된 시스템의 복구 지점을 의도적으로 중복해 설정하는 것입니다.

복제의 목표는 중복을 통해 원래 보호된 시스템의 사용 가능성을 최대화하는 것입니다. 최적의 데이터 보안을 위해 Dell은 별도의 지리적 위치에 대상 Core를 배치하도록 권장합니다.

복제 일정을 설정하여 기본 동작을 변경하지 않는다면 Core는 모든 백업 스냅숏, 체크섬 검사, 연결성 검사, 야간 작업이 완료된 즉시 복제 작업을 시작합니다. 자세한 내용은 복제 일정 설정을(를) 참조하십시오.

복제를 제거하면 그 이후부터 소스 Core에서 대상 Core로의 복구 지점 복사가 중단됩니다. 복제를 제거해도 원래 (소스) Core에 저장된 데이터에는 영향을 주지 않습니다.

또한 복제를 제거할 때 원래 시스템에서 복제된 복구 지점을 대상 Core에 그대로 남겨둘 것인지, 아니면 삭제할 것인지를 선택할 수 있습니다. 제거하는 복제된 시스템에 대해 복구 지점을 유지하면 이 시스템의 복구 지점은 Core에서 복구 지점만 있는 시스템으로 표시됩니다. 이러한 복구 지점이 대상 Core에 유지되는 동안에는 이 유지되는 복구 지점에서 데이터를 탐색하거나 파일 수준에서 파일을 복원할 수 있습니다.

다음 방법 중 하나를 사용하여 복제를 제거할 수 있습니다.

- 소스 Core의 발신 복제 제거
- 대상 Core에서 들어오는 복제 제거

소스 Core의 발신 복제 제거

소스 Core의 복제 작업에서 하나 이상의 보호된 시스템을 제거하려면 다음 단계를 완료하십시오.

1 소스 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)를 클릭합니다.
복제 페이지가 나타납니다.

발신 복제 창의 요약 표에는 이 소스 Core에서 복구 지점을 복제하도록 구성된 각 대상 Core에 대한 행이 포함되어 있습니다.

2 선택적으로, 특정 대상 Core의 오른쪽에 있는 ▼ 화살표를 클릭합니다.
보기가 확장되어 현재 이 지정된 대상 Core로 복제되고 있는, 이 소스 Core의 각 보호된 시스템이 표시됩니다.

3 다음과 같이 발신 복제에서 제거하려는 보호된 시스템을 선택합니다.

- 이 소스 Core와 특정 대상 Core 간에 기존 복제 관계를 완전히 제거하려면 이 대상 Core에 대한 (설정) 드롭다운 메뉴를 클릭한 다음 **삭제**를 선택합니다.
- 이 지정된 대상 Core의 하위 시스템 집합에 대한 발신 복제를 제거하려면 보기를 확장하여 현재 복제되는 모든 시스템을 표시하고 제거하려는 각 복제된 시스템의 확인란을 선택합니다. 계속 복제하려는 시스템의 확인란은 선택을 취소합니다. 그 다음 요약 표 위의 메뉴에서 **삭제**를 클릭합니다.

복제 관계를 제거할 것인지를 묻는 확인 메시지가 나타납니다.

4 이 대화 상자에서 **예**를 클릭하여 삭제를 확인합니다.

대상 Core에서 들어오는 복제 제거

이 절차의 단계를 완료하여 대상 Core의 복제에서 하나 이상의 보호된 시스템을 제거합니다.

노트: 소스 Core의 복제 페이지에서는 보내는 복제 창에서 보호된 시스템의 복제를 제거할 수도 있습니다. 참고 항목: 소스 Core의 발신 복제 제거

1 대상 Core에서 Rapid Recovery Core Console을 열고 아이콘 표시줄에서 (복제)을 클릭합니다.
복제 페이지가 나타납니다. Incoming Replication(들어오는 복제) 창의 요약 표는 이 대상 Core가 복제하는 보호된 시스템과 함께 각 소스 Core에 대한 행을 포함합니다.

2 복제된 시스템을 선택하여 다음과 같이 제거합니다.

- 소스 Core에서 대상 Core로 복제된 **모든** 시스템을 삭제하려면 들어오는 복제 창에서 해당 Core에 대한 확인란을 선택합니다.
- 동일한 소스 Core에서 더 적은 시스템의 하위 집합을 삭제하려면 다음을 수행합니다.

  a Core 오른쪽에 있는 ▼ 화살표를 클릭합니다.
  선택한 소스 Core에서 대상 Core에서 복제된 각 시스템을 표시하도록 보기를 확장합니다.

  b 제거할 각 복제된 시스템에 대한 확인란을 선택합니다.

  c 선택한 소스 Core의 상위 행에서 (설정) 드롭다운 메뉴를 클릭하고 **삭제**를 선택합니다.
  복제 제거 대화 상자가 나타납니다.

3 **복제 제거** 대화 상자에서 다음 중 하나를 수행합니다.

- 대상 Core에 복제된 복구 지점을 그대로 두려는 경우 **기존 복구 지점 삭제** 옵션을 선택 취소합니다.
- 소스 Core는 물론, 해당 시스템에서 수신한 모든 복제된 복구 지점도 복제에서 삭제하려면 **기존 복구 지점 삭제**를 선택합니다.

4 **예**를 클릭하여 삭제를 확인합니다.

경고: 이 옵션을 선택하면 이 Core에 복제되는 모든 복구 지점을 삭제합니다.

소스 Core에서 보호하는 선택된 시스템은 이 대상 Core의 복제에서 제거됩니다. 필요한 경우 복구 지점을 삭제하는 옵션을 선택하면 이 Core의 리포지토리에서도 제거됩니다.

복제된 데이터 복구

일상적인 복제 기능은 소스 Core에서 유지되지만, 대상 Core에서만 재난 복구에 필요한 기능을 완료할 수 있습니다.

재난 복구를 위해 대상 Core에서 복제된 복구 지점을 사용하여 보호된 시스템을 복구할 수 있습니다. 대상 Core에서 다음 복구 옵션을 수행할 수 있습니다.

- **복구 지점 탑재**. 자세한 내용은 복구 지점 마운트을(를) 참조하십시오.
- **복구 지점으로 롤백**. 자세한 내용은 복구 지점에서 볼륨 복원 또는 명령줄을 사용하여 Linux 시스템의 볼륨 복원을 참조하십시오.
- **가상 시스템(VM) 내보내기 수행**. 자세한 내용은 Rapid Recovery에서 가상 시스템으로 내보내기 정보을(를) 참조하십시오.
- **운영 체제 미설치 복원(BMR) 수행**. 자세한 내용은 Windows 시스템에 대한 미설치 복원 수행을(를) 참조하십시오.

5

데이터 복구

복구 관리

Rapid Recovery Core에서는 즉시 데이터를 복원하거나 시스템을 복구 지점으로부터 실제 또는 가상 시스템에 복구할 수 있습니다. 복구 지점에는 블록 수준에서 수집된 에이전트 볼륨 스냅샷이 포함됩니다. 이러한 스냅샷은 응용프로그램 인식형이므로, 열려 있는 모든 트랜잭션과 롤링 트랜잭션 로그가 완료되고 스냅샷을 생성하기 전에 캐시가 디스크에 플러시됩니다. 복구 보증과 함께 응용프로그램 인식형 스냅샷을 사용하면 Core에서 다음을 비롯한 여러 가지 유형의 복구를 수행할 수 있습니다.

- 파일 및 폴더 복구
- 라이브 복구를 포함한 데이터 볼륨 복구
- 라이브 복구를 사용하여 Microsoft Exchange Server 및 Microsoft SQL Server에 대한 데이터 볼륨 복구
- 범용 복구를 사용하여 운영 체제 미설치 복원
- 범용 복구를 사용하여 다른 하드웨어에 운영 체제 미설치 복원
- 가상 시스템에 임시 및 지속적 내보내기

스냅숏 및 복구 지점

이 섹션에서는 Rapid Recovery에 의해 생성된 스냅숏 및 복구 지점을 사용하고 관리하는 방법에 대해 설명합니다 여기에는 복구 지점 탑재, 보기, 강제 적용 뿐만 아니라 마이그레이션과 삭제가 포함됩니다.

스냅숏 및 복구 지점 관리

복구 지점은 개별 디스크 볼륨에서 작성되고 리포지토리에 저장된 스냅숏 모음입니다. 스냅숏은 데이터를 생성하는 응용프로그램이 계속 사용 중인 동안 지정된 시점에서 디스크 볼륨의 상태를 캡처하고 저장합니다. Rapid Recovery에서는 스냅숏을 작성하고, 스냅숏을 일시적으로 중지하거나 리포지토리에서 동시 복구 지점 목록을 보고, 필요한 경우 삭제할 수도 있습니다. 복구 지점은 보호된 시스템을 복원하거나 로컬 파일 시스템으로 마운트하는 데 사용됩니다.

Rapid Recovery에서 캡처하는 스냅숏은 블록 수준에서 수행되며 응용프로그램 인식형입니다. 이것은 스냅숏을 만들기 전에 열려 있는 모든 트랜잭션 및 롤링 트랜잭션 로그가 완료되고 캐시가 디스크로 플러시됨을 의미합니다.

Rapid Recovery는 마운트된 볼륨에 연결되는 저수준 볼륨 필터 드라이버를 사용하여 다음에 수행될 스냅숏의 모든 블록 수준 변경 사항을 추적합니다. Microsoft VSS(볼륨 섀도 복사본)는 응용프로그램 크래쉬에 대비한 백업 스냅숏 작성(application crash consistent snapshots)을 쉽게 수행하는 데 사용됩니다.

보호되는 시스템의 복구 지점 페이지 보기

보호되는 시스템의 복구 지점 전체 목록을 보려면 다음 절차의 단계를 완료하십시오.

노트: DAG 또는 CCR 서버 클러스터에서 데이터를 보호하는 경우 연결된 복구 지점은 클러스터 수준에서 나타나지 않습니다. 해당 복구 지점은 노드 또는 시스템 수준에서만 표시됩니다.

1 Rapid Recovery Core Console에서 복구 지점을 확인할 보호된 시스템으로 이동합니다.
2 페이지를 상단 메뉴에서 **복구 지점**을 클릭합니다.

복구 지점 요약 창과 복구 지점 창이 표시되는 복구 지점 페이지가 나타납니다.

다음 표의 설명에 따라 시스템의 복구 지점에 대한 요약 정보를 볼 수 있습니다.

표 147. 복구 지점 요약 정보

정보	설명
복구 지점 총 개수	이 시스템의 리포지토리에 저장된 총 복구 지점 개수를 나열합니다.
보호된 총 데이터	이러한 복구 지점의 리포지토리에 사용되는 저장소 공간 크기를 나타냅니다.
DVM 리포지토리	이러한 복구 지점이 저장되어 있는 리포지토리의 이름을 나열합니다.
DVM 리포지토리 상태	복구 지점에서 소비되는 공간의 양을 그래픽적으로 표시합니다. 사용된 리포지토리, 공간 크기, 리포지토리 전체 공간의 비율을 표시합니다. 남은 공간의 양을 확인하려면 그래프를 클릭하십시오.

다음 표의 설명에 따라 시스템의 복구 지점에 대한 정보를 볼 수 있습니다.

표 148. 복구 지점 정보

정보	설명
아이콘	복구 지점 또는 확장된 경우, 복구 지점 내의 볼륨 의 그래픽 묘사입니다. 복구 지점은 세부 항목을 확장할 수 있음을 나타내는 오른쪽 화살표 를 표시합니다.
암호화됨	복구 지점이 암호화되었는지 여부를 나타냅니다.
상태	복구 지점의 현재 상태를 나타냅니다.
콘텐츠	복구 지점에 포함된 볼륨을 나열합니다. (정보)를 클릭하여 공간 사용량과 파일 시스템을 볼 수 있습니다.
유형	복구 지점을 기본 이미지 또는 증분(차등) 스냅숏으로 정의합니다.
만든 날짜	복구 지점을 만든 날짜를 표시합니다.
크기	복구 지점이 리포지토리에서 차지하는 공간의 크기를 표시합니다.
	설정 드롭다운 메뉴에서 선택한 복구 지점에 대한 특정 기능을 수행할 수 있습니다.

3 경우에 따라 복구 지점을 확장하여 보호되는 볼륨을 볼 수 있습니다.

관련 링크

시스템의 복구 지점 보기

복구 지점 상태 표시기 이해

보호된 SQL 또는 Exchange Server에 대한 복구 지점을 캡처한 후 응용 프로그램에서 복구 지점 표에 해당하는 색상 상태 표시기를 표시합니다. 이 표는 특정 시스템에 대한 복구 지점을 볼 때 **복구 지점** 창에 표시됩니다. 표시되는 색상은 다음 표에서 설명한 대로, 보호된 시스템에 대한 검사 설정과 해당 검사의 성공/실패 여부에 기반합니다.

노트: 복구 지점 보기에 대한 자세한 내용은 보호되는 시스템의 복구 지점 페이지 보기을(를) 참조하십시오.

Exchange 데이터베이스에 대한 복구 상태 지점 색상

다음 표에는 Exchange 데이터베이스에 대해 표시되는 상태 표시기가 나열되어 있습니다.

표 149. Exchange 데이터베이스 상태 표시기

상태 색상	설명
흰색	Exchange 데이터베이스가 복구 지점, 볼륨 또는 볼륨 그룹에서 감지되지 않았음을 나타냅니다.
노란색	Exchange 데이터베이스 마운트 가능성 검사가 아직 실행되지 않았음을 나타냅니다.
빨간색	하나 이상의 데이터베이스에서 마운트 가능성 또는 체크섬 검사에 실패했다는 것을 나타냅니다.
녹색	복구 지점이 하나 이상의 데이터베이스를 포함하고, 마운트 가능성 검사가 활성화되었으며, 마운트 가능성 검사에 통과했거나 체크섬 검사에 통과했음을 나타냅니다.

SQL 데이터베이스에 대한 복구 상태 지점 색상

다음 표에는 SQL 데이터베이스에 대해 표시되는 상태 표시기가 나열되어 있습니다.

표 150. SQL 데이터베이스 상태 표시기

상태 색상	설명
흰색	SQL 데이터베이스가 복구 지점, 볼륨 또는 볼륨 그룹에서 감지되지 않았음을 나타냅니다.
노란색	SQL 데이터베이스가 오프라인 상태이고 연결 기능 검사가 불가능하며 수행되지 않았음을 나타냅니다.
빨간색	연결 기능 검사에 실패했거나 SQL 데이터베이스가 오프라인 상태임을 나타냅니다.
녹색	연결성 검사를 통과했다는 것을 나타냅니다.

노트: Exchange 또는 SQL 데이터베이스가 연결되지 않은 복구 지점에는 흰색 상태 표시기가 표시됩니다. 복구 지점에 대해 Exchange 및 SQL 데이터베이스가 모두 존재하는 경우에는 복구 지점에 대해 가장 심각한 상태 표시기가 표시됩니다.

복구 지점 마운트

Rapid Recovery에서 Windows 시스템의 복구 지점을 탑재하여 로컬 파일 시스템을 통해 저장된 데이터에 액세스할 수 있습니다.

노트: `local_mount` 유틸리티로 Linux 복구 지점을 탑재하려면 Linux 시스템에서 복구 지점 볼륨 마운트을(를) 참조하십시오.

노트: 데이터 중복 제거가 사용 가능한 시스템에서 복원된 데이터로부터 복구 지점을 마운트할 때 Core 서버에서도 중복 제거를 사용해야 합니다.

1 Rapid Recovery Core Console에서 로컬 파일 시스템에 탑재하려는 시스템으로 이동합니다.
선택한 보호된 시스템의 **요약** 페이지가 표시됩니다.

2 **복구 지점** 메뉴를 클릭합니다.
선택한 보호된 시스템의 **복구 지점** 페이지가 표시됩니다.

3 (선택 사항) 복구 지점 창의 **복구 지점** 목록에서 오른쪽 화살표 ▸ 기호를 클릭하여 복구 지점 정보를 확장하면 복구 지점에 포함된 볼륨이 표시됩니다.

4 탑재하려는 복구 지점의 행에서 를 클릭하고 드롭다운 메뉴에서 **탑재**를 선택합니다.
탑재 마법사가 나타나며 **볼륨** 페이지가 표시됩니다.

5 **볼륨** 페이지에서 탑재하려는 복구 지점의 각 볼륨을 선택한 후 **다음**을 클릭합니다.

탑재 마법사의 **탑재 옵션** 페이지가 표시됩니다.

6 **탑재 옵션** 페이지에서 다음 표에 설명된 대로 복구 지점을 탑재하는 설정을 편집합니다.

표 151. 탑재 옵션 설정

옵션	설명
로컬 폴더	마운트된 복구 지점에 액세스하기 위해 사용하는 경로를 지정합니다. 예를 들어, `C:\ProgramData\AppRecovery\MountPoints\ MountPoint1`을 선택합니다.
마운트 유형	마운트된 복구 지점의 데이터 액세스 방법을 지정합니다. · 읽기 전용 · 이전 쓰기가 포함된 읽기 전용 · 쓰기 가능
이 마운트의 Windows 공유 만들기	(선택 사항) 이 확인란을 선택하여 탑재된 복구 지점을 공유할 수 있는지를 지정한 후 공유 이름 및 허용된 그룹을 포함하여 액세스 권한을 설정합니다.

7 **마침**을 클릭하여 복구 지점을 탑재합니다.

노트: 마운트된 복구 지점에서 다른 Windows 시스템으로 디렉터리나 파일을 복사하려면 Windows 탐색기를 사용하여 기본 권한이나 원래 파일 액세스 권한으로 복사하면 됩니다. 자세한 내용은 Windows 탐색기를 사용하여 디렉터리 또는 파일 복원 및 Windows 탐색기를 사용하여 디렉터리 또는 파일 복원 및 권한 보존을(를) 참조하십시오.

8 (선택 사항) 작업이 진행 중인 동안 Core Console의 **실행 중인 작업** 드롭다운 메뉴에서 진행률을 보거나 **이벤트** 페이지에서 세부 정보를 볼 수 있습니다. Rapid Recovery 이벤트 모니터링에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

복구 지점 분리

Core에서 마운트된 복구 지점을 분리하려면 다음 단계를 완료하십시오.

노트: 원격으로 마운트된 복구 지점을 분리하는 경우 *연결을 해제*한다라고 합니다.

1 Rapid Recovery Core Console의 아이콘 표시줄에서 (자세히)를 클릭하고 **마운트**를 선택합니다.
마운트 페이지가 나타납니다. 로컬 마운트(Core에서 마운트된 복구 지점)에 대한 창과 원격 마운트(Local Mount Utility를 사용하여 마운트된 복구 지점)에 대한 또 다른 창이 있습니다. 각 창에서 각각의 마운트된 복구 지점이 목록에 나타납니다.

2 로컬 마운트를 분리하려면 **로컬 마운트** 창에서 다음을 수행합니다.

a 분리하려는 하나 이상의 로컬 마운트 지점을 선택합니다.

- 모든 복구 지점을 분리하려면 Local Mounts(로컬 마운트) 표의 제목 표시줄에 있는 확인란을 클릭하여 모든 마운트 지점을 선택합니다.
- 하나 이상의 복구 지점을 분리하려면 분리하려는 마운트 지점을 나타내는 각 행의 첫 번째 열에 있는 확인란을 클릭합니다.

b 그리고, **분리**를 클릭합니다.
확인 대화 상자가 나타납니다.

c 선택한 복구 지점를 분리할 것인지 클릭하여 확인합니다.
그러면 로컬 복구 지점이 분리됩니다.

노트: 알림 경고가 활성화된 경우 적절한 마운트 지점이 분리 중임을 알리는 경고가 나타날 수 있습니다.

3 원격으로 마운트된 복구 지점을 연결 해제하려면 **원격 마운트** 창에서 다음을 수행합니다.

a 연결 해제하려는 하나 이상의 원격 마운트 지점을 선택합니다.

- 모든 복구 지점을 연결 해제하려면 Remote Mounts(원격 마운트) 표의 제목 표시줄에 있는 확인란을 클릭하여 모든 마운트 지점을 선택합니다.
- 하나 이상의 복구 지점을 연결 해제하려면 분리하려는 마운트 지점을 나타내는 각 행의 첫 번째 열에 있는 확인란을 클릭합니다.

b 그리고, **연결 해제**를 클릭합니다.
확인 대화 상자가 나타납니다.

c 선택한 복구 지점를 연결 해제할 것인지 클릭하여 확인합니다.
그러면 로컬 복구 지점이 연결 해제됩니다.

노트: 알림 경고가 활성화된 경우 적절한 마운트 지점이 연결 해제 중임을 알리는 경고가 나타날 수 있습니다.

4 상황에 따라 이전에 마운트된 복구 지점은 더 이상 로컬 마운트 또는 원격 마운트 목록에 나타나지 않음을 확인합니다.

Linux 복구 지점 사용

보호된 Linux 시스템에서 복구 지점을 탑재하고 분리하기 위해 권장 및 지원되는 방법은 *local_mount* 유틸리티를 사용하는 것입니다.

이 절차에서는 local_mount를 사용하여 Linux 복구 지점을 탑재하고 분리하는 방법에 대해 자세히 설명합니다.

노트: 기타 관리를 Core Console에서 모두 수행할 수 있으므로, 다른 방법으로 Linux 복구 지점을 관리하려면 스냅숏 및 복구 지점 관리을 참조하십시오.

Linux 시스템에서 복구 지점 볼륨 마운트

Rapid Recovery에서 복구 지점에서 볼륨을 로컬 볼륨으로 원격 탑재할 수 있습니다.

노트: 이 절차를 수행하는 경우 복구 지점을 aavdisk 파일이 포함된 /tmp 폴더에 마운트하지 마십시오.

1 복구 지점을 마운트할 새 디렉터리를 만듭니다(예: `mkdir` 명령 사용).
2 디렉터리가 있는지 확인합니다(예: `ls` 명령 사용).
3 Rapid Recovery local_mount 유틸리티를 루트 또는 수퍼 사용자로 실행합니다. 예를 들어, 다음과 같습니다.

```
sudo local_mount
```

4 Rapid Recovery 탑재 프롬프트에 다음 명령을 입력하여 보호된 시스템을 나열합니다.

```
lm
```

5 메시지가 표시되면 Rapid Recovery Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.
6 Core 서버의 로그온 자격 증명 즉, 사용자 이름과 암호를 입력합니다.
Rapid Recovery 서버에 의해 보호되는 시스템의 목록이 표시됩니다. 각 시스템은 시스템의 라인 항목 번호, 호스트/IP 주소 및 ID 번호로 식별됩니다.

예: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba
7 다음 명령을 입력하여 지정된 시스템에 사용 가능한 복구 지점을 나열합니다.

```
lr <line_number_of_machine>
```

노트: 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템의 기본 및 증분 복구 지점 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 날짜 및 타임스탬프, 볼륨 위치, 복구 지점 크기, 그리고 복구 지점을 나타내는 시퀀스 번호가 끝에 나오는 볼륨의 ID 번호가 포함됩니다.

예: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2
8 다음 명령을 입력하여 지정된 마운트 지점/경로에서 지정된 복구 지점을 선택하고 마운트합니다.

```
m <volume_recovery_point_ID_number> <volume-letter> [flag] <path>
```

명령의 플래그에 따라 복구 지점을 마운트하는 방법이 결정됩니다. 다음 옵션 중 하나를 사용할 수 있습니다.

- [r] - 읽기 전용 마운트(기본값). 이 플래그를 사용하면 복구 지점을 마운트할 수 있지만 복구 지점을 변경할 수는 없습니다.
- [w] - 쓰기 가능 마운트. 이 플래그를 사용하면 복구 지점을 마운트하고 변경할 수 있습니다.
- [v] - 이전 쓰기를 포함하여 마운트. "v" 플래그를 사용하여 마운트하면 복구 지점을 마운트하고, 이전 쓰기 가능 마운트 중에 변경되었지만 복구 지점에는 존재하지 않는 변경 사항을 포함할 수 있습니다.
- [n] - nbd를 <path>에 마운트하지 않음. nbd(network block device)는 로컬 마운트 수행 시 Core와 보호된 시스템 사이에 소켓 연결을 만듭니다. 이 플래그를 사용하면 nbd를 마운트하지 않고 복구 지점을 마운트할 수 있어, 복구 지점의 파일 시스템을 수동으로 검사하려는 경우에 유용합니다.

노트: 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 나타낼 수도 있습니다. 이 경우 시스템 라인 번호(lm 출력에서), 복구 지점 라인 번호 및 볼륨 문자, 경로를 차례로 사용합니다(예: m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>). 예를 들어, `lm` 출력이 세 개의 보호된 시스템이 나열되고 2번에 대해 `lr` 명령을 입력한 후 23 복구 지점 볼륨 b를 /tmp/mount_dir에 탑재하려는 경우 명령은 `m 2 23 b /tmp/mount_dir`입니다.

노트: 호환되는 운영 체제 시스템 BTRFS 볼륨을 탑재하려는 경우(*Dell Data Protection | Rapid Recovery 설치 및 업그레이드 지침*의 "Rapid Recovery 릴리스 6.1 운영 체제 설치 및 호환성 매트릭스" 참조) 다음 매개 변수를 포함시켜야 합니다.

```
mount -o nodatasum,device=/dev/xxx /dev/xxx /mnt/yyy
```

9 마운트 성공 여부를 확인하려면 다음 명령을 입력하여 연결된 원격 볼륨을 나열합니다.

```
l
```

Linux 시스템에서 복구 지점 분리

Linux 시스템에서 복구 지점을 분리하려면 아래 절차의 각 단계를 완료하십시오.

1 Rapid Recovery local_mount 유틸리티를 루트 또는 수퍼 사용자로 실행합니다. 예:

```
sudo local_mount
```

2 Rapid Recovery 마운트 프롬프트에서 다음 명령을 입력하여 보호된 시스템을 나열합니다.

```
lm
```

3 메시지가 표시되면 Rapid Recovery Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.

4 Core 서버의 로그온 자격 증명(사용자 이름과 암호)을 입력합니다.

Rapid Recovery 서버에서 보호하는 시스템 목록이 표시됩니다.

5 다음 명령을 입력하여 지정된 시스템에 사용 가능한 복구 지점을 나열합니다.

```
lr <line_number_of_machine>
```

노트: 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템의 기본 및 증분 복구 지점 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 날짜/타임스탬프, 볼륨 위치, 복구 지점의 크기, 그리고 복구 지점을 나타내는 시퀀스 번호가 끝에 포함된 볼륨의 ID 번호가 포함됩니다.

예를 들면 다음과 같습니다. 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2

6 `l or list` 명령을 실행하여 마운트된 NBD(Network Block Device) 장치의 목록을 얻습니다. 복구 지점을 마운트하는 경우에는 `l or list` 명령을 실행한 후 NBD 장치로 연결되는 경로를 얻게 됩니다.

7 다음 명령을 입력하여 복구 지점을 분리합니다.

```
unmount <path_of_nbd-device>
```

8 `l or list` 명령을 실행하여 복구 지점이 성공적으로 분리되었는지를 확인합니다.

스냅숏 작성

스냅숏을 작성하면 현재 보호된 시스템에 대한 데이터 전송을 수행할 수 있습니다. 스냅숏을 작성하면 바로 전송이 시작되거나 다른 작업이 실행 중인 경우 대기열에 추가됩니다.

두 가지 유형의 스냅숏에서 선택할 수 있습니다.

증분 스냅숏을 선택하고 이전 복구 지점이 없는 경우에는 기본 이미지가 캡처됩니다. 스냅숏을 작성한다고 해서 일정 스냅숏의 타이밍이 변경되지 않습니다.

노트: Rapid Recovery는 기본 및 증분 전송을 위해 Window 8, Windows 8.1, Windows Server 2012 및 Windows Server 2012 R2를 지원합니다.

- 기본 이미지는 시스템의 선택된 볼륨에 있는 모든 데이터의 스냅숏입니다.
- 증분 스냅숏은 마지막 스냅숏 이후 변경된 모든 데이터를 캡처합니다.

1 Rapid Recovery Core Console에서 스냅숏을 작성할 복구 지점이 있는 시스템 또는 클러스터로 이동합니다.
2 Summary(요약) 페이지의 Summary(요약) 창에서 **Force Snapshot(스냅숏 작성)**을 클릭합니다.
Force Snapshot(스냅숏 작성) 대화 상자가 나타납니다.
3 Force Snapshot(스냅숏 작성) 대화 상자의 확인란에서 하나 이상의 볼륨 또는 보호 그룹을 클릭합니다.
4 **Force Snapshot(스냅숏 작성)** 또는 Force Base Image(기본 이미지 작성)를 각각 클릭합니다.
5 기본 이미지를 선택한 경우 기본 이미지 적용을 확인하기 위해 클릭합니다.
기본 이미지는 백업하려는 볼륨의 데이터 양에 따라 상당한 시간이 소요될 수 있습니다.

선택한 스냅숏이 대기열에 있을 때는 다른 작업이 완료되는 즉시 작업이 시작됩니다.

복구 지점 제거

리포지토리에서 특정 시스템의 복구 지점을 쉽게 제거할 수 있습니다. Rapid Recovery에서 복구 지점을 삭제하는 경우 다음 옵션 중 하나를 지정할 수 있습니다.

- **모든 복구 지점 삭제**. 리포지토리에서 선택한 보호된 시스템의 모든 복구 지점을 제거합니다.
- **복구 지점의 범위 삭제**. 시스템에 있는 모든 데이터인 현재 이전부터 기본 이미지를 포함하여 지정된 범위의 모든 복구 지점은 물론 현재 이후부터 다음 기본 이미지까지 모든 복구 지점을 제거합니다.

노트: 삭제한 복구 지점은 복구할 수 없습니다. 복구 지점에 저장된 데이터가 필요하면 먼저 데이터 아카이브를 고려합니다.

1 Rapid Recovery Core Console의 **보호된 시스템** 메뉴에서 복구 지점을 보고 제거할 시스템의 이름 또는 IP 주소를 클릭합니다.
선택한 보호된 시스템에 대한 요약 보기가 나타납니다.
2 시스템 이름 또는 IP 주소 옆에 있는 **복구 지점** 메뉴를 클릭합니다.
선택한 시스템의 **복구 지점** 페이지가 나타납니다.
3 **복구 지점** 창을 아래로 스크롤합니다.
창 제목 아래에는 Refresh(새로 고침), Delete Range(범위 삭제), Delete All(모두 삭제)을 비롯한 옵션이 표시됩니다.
4 현재 저장된 모든 복구 지점을 삭제하려면 Recovery Points(복구 지점) 창 제목 아래에서 **모두 삭제**를 클릭하고 확인 대화 상자에서 클릭하여 삭제를 확인합니다.
5 특정 데이터 범위의 복구 지점 집합을 삭제하려면 다음을 수행합니다.
a 복구 지점 창 제목 아래에서 **범위 삭제**를 클릭합니다.
특정 범위의 복구 지점 삭제 대화 상자가 나타납니다.
b **특정 범위의 복구 지점 삭제** 대화 상자의 **시작 시간** 필드에서 복구 지점 삭제를 시작할 날짜 및 시간을 선택합니다.
c **종료 시간** 필드에서 삭제할 마지막 복구 지점을 정의하는 날짜 및 시간을 선택합니다.

d **Delete(삭제)**를 클릭합니다.
e 확인 대화 상자에서 클릭하여 삭제를 확인합니다.

분리된 복구 지점 체인 삭제

분리된 복구 지점은 기본 이미지와 연관되지 않은 증분 스냅숏입니다. 후속 스냅숏은 계속 이 복구 지점을 기반으로 작성되지만 기본 이미지가 없기 때문에 최종 복구 지점은 불완전하고 대부분 복구를 완료하는 데 필요한 데이터를 포함하지 않습니다. 이러한 복구 지점은 분리된 복구 지점 체인의 일부로 간주됩니다. 이러한 상황이 발생하면 최선의 해결책은 체인을 삭제하고 새로운 기본 이미지를 만드는 것입니다.

기본 이미지 작성에 대한 자세한 내용은 스냅숏 작성을(를) 참조하십시오.

1 Rapid Recovery Core Console에서, 분리된 복구 지점 체인을 삭제하려는 보호된 시스템으로 이동합니다.
2 페이지를 상단 메뉴에서 **복구 지점**을 클릭합니다.
3 복구 지점 창에서 분리된 복구 지점을 확장합니다.
이 복구 지점은 유형 열에 "증분, 분리됨" 레이블로 표시됩니다.
4 작업 옆의 **삭제**를 클릭합니다.
복구 지점 삭제 창이 나타납니다.
5 복구 지점 삭제 창에서 **예**를 클릭합니다.

주의: 이 복구 지점을 삭제하면 이전 또는 이후부터 다음 기본 이미지까지 발생하는 모든 증분 복구 지점을 포함한 전체 복구 지점 체인이 삭제됩니다. 이 작업은 취소할 수 없습니다.

분리된 복구 지점 체인이 삭제됩니다.

복구 지점을 다른 리포지토리로 수동 마이그레이션

보호된 시스템의 복구 지점을 삭제하는 대신 리포지토리에서 제거하려면 이 절차를 사용하여 수동으로 복구 지점을 다른 리포지토리로 마이그레이션할 수 있습니다. 이 프로세스는 소스 리포지토리에서 복구 지점을 아카이브한 후 아카이브를 대상 리포지토리로 가져오는 작업과 관련이 있습니다.

예를 들어, 기존 리포지토리가 가득 차거나, 사용자의 요구 사항이 바뀌어 다른 Core 및 리포지토리를 사용하는 시스템을 보호해야 하는 경우 이 절차를 수행할 수 있습니다.

주의: 이전에 AppAssure 5.3 또는 5.4에서 리포지토리를 업그레이드했고 복제를 사용한 경우 Dell에서는 마이그레이션하기 전에 대상 Core의 각 리포지토리에서 리포지토리 검사 작업을 수행하도록 권장합니다. 이 작업을 수행하면 불규칙한 데이터가 새로운 대상 리포지토리로 복사되는 것을 방지합니다. 리포지토리 검사 작업은 사용자의 Core에 적용되는 경우에만 UI에서 사용할 수 있으며 실행하는 데 오랜 시간이 걸릴 수 있습니다. 이 작업에 대한 내용은 DVM 리포지토리의 무결성 검사에서 확인하십시오. 이 작업 수행에 대한 내용은 DVM에서 리포지토리 작업 검사 실행에서 확인하십시오.

1 Rapid Recovery Core Console에서 복구 지점을 마이그레이션할 보호된 시스템에 대한 보호를 일시 중지합니다. 자세한 내용은 보호 일시 중지 및 다시 시작을(를) 참조하십시오.
2 복구 지점을 마이그레이션할 보호된 시스템에 대한 현재 작업을 모두 취소하거나 모두 완료될 때까지 대기합니다.
3 일시 중지한 시스템에 대한 복구 지점을 아카이브합니다. 자세한 내용은 아카이브 만들기을(를) 참조하십시오.
4 아카이브 및 아카이브 확인 후 마이그레이션할 보호된 시스템의 기존 복구 지점을 제거합니다. 자세한 내용은 복구 지점 제거을(를) 참조하십시오.

노트: 기존 복구 지점을 제거하지 않으면 보호된 시스템에 대한 리포지토리를 변경할 수 없습니다.

5 마이그레이션된 복구 지점에 대한 새로운 리포지토리를 생성하거나 새로운 대상 리포지토리가 있는지 확인합니다. 자세한 내용은 DVM 리포지토리 생성를 참조하십시오.
- 기존 리포지토리를 사용하려면 6단계로 계속합니다.

6 다음 단계를 완료하여 일시 중지한 각 시스템에 대한 리포지토리를 변경합니다.

a Core Console의 탐색 트리에서 보호된 시스템을 클릭합니다.
b 보호된 시스템의 **요약** 페이지에서 **설정**을 클릭합니다.
c **설정** 페이지의 **일반** 창에서 **리포지토리** 드롭다운 목록을 클릭한 후 4단계에서 생성한 리포지토리 이름을 선택합니다.
   - 기존 리포지토리를 사용하려면 기존 리포지토리의 이름을 선택합니다.

     노트: 복구 지점을 기존 리포지토리로 마이그레이션할 때 기존 리포지토리에 마이그레이션된 복구 지점을 포함할 만큼 공간이 충분한지 확인하십시오.

d **확인**을 클릭합니다.

7 일시 중지한 시스템에 대한 보호를 다시 시작합니다. 자세한 내용은 보호 일시 중지 및 다시 시작을(를) 참조하십시오.
8 이동한 각 보호된 시스템에 대한 새 기본 이미지를 작성합니다. 자세한 내용은 스냅숏 작성을(를) 참조하고, 기본 이미지 강제 적용 옵션을 사용합니다.
9 마이그레이션할 시스템에 대해 아카이브된 데이터를 가져옵니다. 자세한 내용은 아카이브 가져오기를 참조하십시오.

데이터 복원

이 장에서는 백업된 데이터를 복원하는 방법에 대해 설명합니다.

Rapid Recovery를 사용한 데이터 복원 정보

Rapid Recovery Core는 복구 지점에서 물리적 또는 가상 시스템으로 즉시 데이터를 복원하고 시스템을 복구할 수 있습니다. 복구 지점에는 블록 수준에서 캡처된 에이전트 볼륨 스냅숏이 포함됩니다. 이러한 스냅숏은 응용프로그램 인식형으로, 열려 있는 모든 트랜잭션 및 롤링 트랜잭션 로그가 완료되고 스냅숏을 만들기 전에 캐시가 디스크로 업데이트됨을 의미합니다. Verified Recovery와 함께 응용프로그램 인식형 스냅숏을 사용하면 다음과 같은 여러 가지 유형의 복구를 수행할 수 있습니다.

- 파일 및 폴더 복구
- 데이터 볼륨 복구(Live Recovery 사용)
- Microsoft Exchange Server 및 Microsoft SQL Server용 데이터 볼륨 복구(Live Recovery 사용)
- Bare Metal Restore(Universal Recovery 사용)
- 다른 형식의 하드웨어에 대한 Bare Metal Restore(Universal Recovery 사용)
- 가상 시스템으로 임시 및 연속 내보내기

노트: 데이터를 복원하거나 가상 내보내기를 수행할 때 사용된 복구 지점은 전체 복구 지점 체인의 일부여야 합니다. 복구 지점 체인에 대한 자세한 내용은 복구 지점 체인 및 분리을(를) 참조하십시오.

Live Recovery 이해

Live Recovery는 Rapid Recovery Core에서 데이터를 복원하는 기능입니다. 보호된 시스템의 비 시스템 Windows 볼륨에 데이터 오류가 발생하는 경우 Rapid Recovery Core의 복구 지점에서 데이터를 복원할 수 있습니다. Restore Wizard의 Live Recovery를 선택하면 사용자가 가동 중지 시간 없이 비즈니스 작업을 지속적으로 할 수 있습니다. 복원 중 Live Recovery를 사용하면 Rapid Recovery가 백그라운드에서 데이터를 계속 복원하는 동안에도 데이터에 즉시 액세스할 수 있습니다. 이 기능을 사용하면 복원할 데이터가 테라바이트 크기더라도 눈 깜짝할 사이에 이를 복구할 수 있습니다.

Rapid Recovery Core는 고유한 블록 기반 백업 및 복구 기술을 사용하여 복구 프로세스 동안에도 대상 서버에 전체 사용자 액세스할 수 있습니다. 요청된 블록은 원활한 복구를 위해 요청 시에 복원됩니다.

Live Recovery는 다음 사항을 제외하고 Rapid Recovery Core에 의해 보호되는 물리적 및 가상 시스템에 적용됩니다.

- Live Recovery는 비 시스템 Windows 볼륨에 액세스할 수 있습니다. C:\ 드라이브 및 시스템 예약 파티션은 Live Recovery를 사용하여 복원할 수 없습니다.
- Live Recovery는 Rapid Recovery 에이전트를 사용하여 Windows 기반 볼륨에 액세스할 수 있습니다. 에이전트 없는 볼륨 또는 Linux 볼륨은 Live Recovery를 활용할 수 없습니다.

Live Recovery는 백업 파일로부터 물리적 또는 가상 서버를 즉시 복원할 수 있습니다. 비 시스템 볼륨 복원 도중 Rapid Recovery는 볼륨 메타데이터를 운영 체제에 즉시 제공하여 필요 시 해당 데이터를 사용할 수 있도록 해줍니다. 예를 들어, Microsoft Exchange의 데이터베이스 볼륨이 손상되면, Live Recovery가 볼륨, 데이터베이스 및 Exchange 서비스를 바로 복원할 수 있습니다.

이 기능을 사용하면 가동 중지 시간을 최소화하면서 대량의 데이터를 가장 빠르게 복구할 수 있습니다. 사용자는 비즈니스 작업을 즉시 계속할 수 있습니다.

Live Recovery가 시작되면 복원된 볼륨 및 해당 내용을 즉시 사용할 수 있게 됩니다. Rapid Recovery Core는 볼륨, 해당 데이터, 응용 프로그램 및 서비스가 이미 다시 사용되고 있어도 계속해서 백그라운드에서 데이터를 복원합니다. 특정 데이터를 요청한 경우 백그라운드 프로세스에서 즉시 해당 데이터 복원을 우선적으로 처리합니다. 이러한 강력한 기능 덕분에 가장 까다로운 서비스 수준 계약도 충족할 수 있습니다.

Live Recovery가 시작되면, 대상 볼륨의 메타데이터(디렉터리 구조, 보안 설명자, NTFS 파일 특성, 사용 가능한 공간 맵 등)가 보호된 시스템에 빠르게 복원됩니다. 그런 다음에는 볼륨 및 해당 내용을 시스템에서 사용할 수 있습니다. Rapid Recovery 에이전트는 Rapid Recovery Core 서버에서 데이터 블록의 복원과 대상 볼륨에 블록 쓰기를 시작합니다.

아직 복원되지 않은 데이터를 요청하는 경우 요청 프로그램이나 블록이 방금 복원되었다는 사실을 모르는 시스템을 사용하여 즉시 응답됩니다.

복구 지점에서 데이터 복원

Windows 및 Linux 시스템의 사용자 데이터가 Rapid Recovery에서 보호됩니다. 보호된 에이전트 시스템의 백업 내용이 Rapid Recovery Core에 복구 지점으로 저장됩니다. 이러한 복구 지점에서 3가지 방법 중 하나를 사용하여 데이터를 복원할 수 있습니다.

Rapid Recovery Core Console에서, 시스템 이외 볼륨의 복구 지점에서 전체 볼륨을 복원하여 대상 시스템의 볼륨을 대체할 수 있습니다. Windows 시스템에서만 이 작업을 수행할 수 있습니다. 자세한 내용은 복구 지점에서 볼륨 복원를 참조하십시오.

복원 중인 시스템이 복원 프로세스에 포함된 운영 체제와 드라이버를 사용 중이기 때문에 복구 지점에서 직접 운영 체제가 있는 볼륨을 복원할 수 없습니다. 복구 지점에서 시스템 볼륨(예: 에이전트 시스템의 C 드라이브)으로 복원하려면 BMR(Bare Metal Restore)를 수행해야 합니다. BMR에는 복구 지점에서 운영 체제 및 구성 파일과 데이터를 포함한 부팅 가능한 이미지를 만들고, 부팅 가능한 이미지에서 대상 시스템을 시작하여 복원을 완료하는 과정이 포함됩니다. 부트 이미지는 복원하려는 시스템이 Windows 운영 체제를 사용하는지 Linux 운영 체제를 사용하는지 여부에 따라 다릅니다. 복구 지점에서 Windows 시스템의 시스템 볼륨으로 복원하려면 Windows 시스템에 대한 미설치 복원 수행을(를) 참조하십시오. Linux 시스템의 시스템 볼륨 복구 지점에서 복원하려면 Windows 시스템에 대한 미설치 복원 수행을(를) 참조하십시오.

마지막으로 전체 볼륨 복원과 반대로, Windows 시스템에서 복구 지점을 마운트하고 개별 폴더와 파일을 탐색하여 특정 파일 집합만 복구할 수 있습니다. 자세한 내용은 Windows 탐색기를 사용하여 디렉터리 또는 파일 복원을(를) 참조하십시오. 원래 파일 권한을 보존한 상태에서 이 작업을 수행하려면(예: 파일 서버에서 사용자의 폴더를 복원하는 경우) Windows 탐색기를 사용하여 디렉터리 또는 파일 복원 및 권한 보존을(를) 참조하십시오.

이 섹션의 항목에서는 실제 시스템에서 데이터를 복원하는 방법을 설명합니다. Windows 시스템에서 가상 시스템으로 보호된 데이터를 내보내는 방법에 대한 자세한 내용은 VM 내보내기을(를) 참조하십시오.

노트: Windows 시스템에서 데이터를 복구할 때 복원할 볼륨에 Windows 데이터 중복 제거가 사용하도록 설정되어 있으면 Core 서버에서도 중복 제거를 사용해야 합니다. Rapid Recovery에서는 Windows 8, Windows 8.1, Windows 10, Windows Server 2012, Windows Server 2012 R2의 일반 전송(기본 및 증분 모두)은 물론 데이터 복원, 완전 복원 및 가상 내보내기가 지원됩니다. 백업 및 복구에 대해 지원되거나 지원되지 않는 볼륨 유형에 대한 자세한 내용은 동적 및 기본 볼륨에 대한 지원을(를) 참조하십시오.

복구 지점에서 볼륨 복원

Rapid Recovery Core에 저장된 복구 지점에서 보호되는 시스템에 볼륨을 복원할 수 있습니다.

노트: 이전 릴리스에서는 이 프로세스를 롤백 수행이라고 했습니다.

노트: Rapid Recovery는 EISA 파티션으로 구성된 시스템의 보호와 복구를 지원합니다. 지원은 Windows 복구 환경(Windows RE)을 사용하는 Window 8, Windows 8.1, Windows Server 2012 및 Windows Server 2012 R2 시스템으로 확장됩니다.

Rapid Recovery 단추 표시줄에서 복원 아이콘을 클릭하여 Rapid Recovery Core 콘솔의 모든 위치에서 복원을 시작할 수 있습니다. 이런 방식으로 복원을 시작하면 복원하려는 Core에서 보호되는 시스템의 지정한 다음 복원하려는 볼륨으로 드릴다운해야 합니다.

또는 특정 시스템에 대한 복구 지점 페이지로 이동하려면 특정 복구 지점에 대한 드롭다운 메뉴를 클릭한 다음 **Restore(복원)**를 선택합니다. 이런 방식으로 복원을 시작하는 경우 5단계에서 시작되는 이 절차를 수행합니다.

복구 지점에서 시스템 볼륨으로 복원하거나 복구 지점에서 부팅 CD를 사용하여 복원하는 경우 미설치 복원(BMR)을 수행해야 합니다. BMR에 대한 자세한 내용은 Windows 시스템용 Bare Metal Restore 이해을(를) 참조하고 Windows 또는 Linux 운영 체제에 대한 필수조건 정보는 각각 Windows 시스템에서 Bare Metal Restore 수행을 위한 전제 조건 및 Linux 시스템에서 Bare Metal Restore 수행을 위한 전제 조건을(를) 참조하십시오. 각 운영 체제 시스템을 위한 로드맵에 설명된 대로 Core 콘솔에서 BMR 기능에 액세스 할 수 있습니다. Restore Machines Wizard(시스템 복원 마법사)에서도 BMR을 수행할 수 있습니다. 이 절차는 마법사의 적절한 위치에서 절차 시스템 복원 마법사를 사용하여 Bare Metal Restore 복원 수행로 안내합니다.

복구 지점에서 볼륨 복원

보호된 시스템에 Agent 소프트웨어가 설치되어 있고 복원 작업을 수행할 수 있는 복구 지점이 있어야 합니다.

다음 절차에 따라 복구 지점에서 볼륨을 복원하십시오.

1 복원 아이콘으로 보호된 시스템의 볼륨을 복원하려면 Core Console로 이동하여 Rapid Recovery 단추 모음에서 **복원**을 클릭합니다.

시스템 복원 마법사가 나타납니다.

2 보호된 시스템 페이지에서 데이터를 복원하려는 보호된 시스템을 선택한 후 **다음**을 클릭합니다.

복구 지점 페이지가 나타납니다.

3 복구 지점 목록에서 에이전트 시스템으로 복원하려는 스냅숏을 검색합니다.

- 필요한 경우 페이지 하단의 단추를 사용하여 복구 지점 추가 페이지를 표시합니다.
- (선택 사항) 마법사의 복구 지점 페이지에 표시되는 복구 지점 수를 제한하려는 경우 볼륨별로 (정의된 경우) 또는 복구 지점의 생성 날짜별로 필터링할 수 있습니다.

4 복구 지점을 클릭하여 선택한 후 **다음**을 클릭합니다.

대상 페이지가 나타납니다.

5 대상 페이지에서 다음과 같이 데이터를 복원하려는 시스템을 선택합니다.

- 선택한 복구 지점에서 동일한 시스템으로 데이터를 복원하고 복원할 볼륨에 시스템 볼륨을 포함하지 않으려면 **보호된 시스템으로 복구(비시스템 볼륨만)**을 선택하고 대상 시스템이 선택되었는지 확인한 후 **다음**을 클릭합니다.

  볼륨 매핑 페이지가 나타납니다. 9단계로 이동합니다.
- 선택한 복구 지점에서 다른 보호된 시스템으로 데이터를 복원하려면(예를 들어, Machine2의 내용을 Machine1의 데이터로 변경하려면) **보호된 시스템으로 복구(비시스템 볼륨만)**를 선택하고 목록에서 대상 시스템을 선택한 후 **다음**을 클릭합니다.

  볼륨 매핑 페이지가 나타납니다. 9단계로 이동합니다.
- 선택한 복구 지점에서 동일한 시스템으로 또는 부트 CD를 사용하여 다른 시스템으로 복원하려는 경우, BMR(Bare Metal Restore)로 간주됩니다. BMR에 대한 자세한 내용은 Windows 시스템용 Bare Metal Restore 이해을(를) 참조하십시오.

  노트: BMR을 수행하는 경우 복원할 에이전트 시스템의 운영 체제에 따른 특정한 요구사항이 있습니다. 이러한 필수 구성 요소를 이해하려면 Windows 시스템에서 Bare Metal Restore 수행을 위한 전제 조건 및 Linux 시스템에서 Bare Metal Restore 수행을 위한 전제 조건을(를) 각각 참조하십시오.

  복원할 볼륨에 시스템 볼륨을 포함하려면 **부트 CD를 사용하여 대상 시스템에 복구**를 선택합니다. 이 옵션은 부트 CD를 작성하라는 메시지를 표시합니다.

  - 시스템 복원 마법사를 사용하여 선택한 복구 지점의 정보가 포함된 부트 CD를 계속 만들려면 **다음**을 클릭한 후 Windows 시스템에 대한 미설치 복원 수행로 이동합니다.
  - 이미 부트 CD를 만들었으며 대상 시스템이 부트 CD를 사용하여 시작된 경우 #GUID-07C2DA5A-B8E2-4D01-82D5-E7A1F14E155E/ID-2490-0000487F 항목의 8단계로 계속합니다.
- 복구 지점에서 시스템 볼륨(예: Machine1 에이전트 시스템의 C 드라이브)으로 복원하려는 경우 BMR로 간주됩니다. **부트 CD를 사용하여 대상 시스템에 복구**를 선택합니다. 이 옵션은 부트 CD를 작성하라는 메시지를 표시합니다.

- 시스템 복원 마법사를 사용하여 선택한 복구 지점의 정보가 포함된 부트 CD를 계속 만들려면 다음을 클릭한 후 Windows 시스템에 대한 미설치 복원 수행로 이동합니다.
- 부트 CD를 이미 만들었으면 6단계로 진행합니다.

6 부트 CD를 사용하여 복원할 시스템을 시작합니다. Windows 시스템에서 BMR에 대한 자세한 내용은 부트 CD 로드 및 대상 시스템 시작을(를), Linux 시스템에서 BMR에 대한 자세한 내용은 Live DVD 로드 및 대상 시스템 시작을(를) 참조하십시오.

7 Core 서버의 시스템 복원 마법사의 대상 페이지에서 **이미 대상 시스템에서 실행 중인 부트 CD가 있습니다**를 선택하고 다음 표와 같이 연결할 시스템에 대한 정보를 입력합니다.

표 152. 시스템 정보

텍스트 상자	설명
IP 주소	복원하려는 시스템의 IP 주소. 이 항목은 URC에 표시되는 IP 주소와 동일합니다.
인증 키	선택한 서버에 연결하는 데 사용할 고유 암호. 이 항목은 URC에 표시되는 인증 키와 동일합니다.

8 **다음**을 클릭합니다.

입력한 연결 정보가 URC와 일치하고 Core와 대상 서버가 네트워크에서 서로 올바르게 식별할 수 있으면 선택한 복구 지점의 볼륨이 로드됩니다. 디스크 매핑 페이지가 나타납니다.

시스템 복원 마법사에서 BMR을 완료하려면 #unique_342/ID-2490-00004B0D 항목의 9단계로 진행합니다.

노트: Rapid Recovery는 FAT32 및 ReFS 파티션를 지원합니다. 드라이버 제한으로 지원되는 전체 복원 및 BMR만 ReFS와 존재합니다. 복원은 사용자 모드, VM 내보내기 등에서 구현됩니다. Core가 ReFS 파일 시스템을 포함하는 하나 이상의 에이전트 볼륨을 보호하는 경우 Windows 8/2012가 ReFS의 기본 지원을 제공하므로, 이러한 컴퓨터에 Core를 설치해야 합니다. 그렇지 않으면 기능이 제한되고 볼륨 이미지 탑재 등이 포함된 작업이 작동하지 않습니다. 이러한 발생 빈도에 해당하는 오류 메시지가 Rapid Recovery Core Console에 표시됩니다.

저장 공간 디스크 구성의 Bare Metal Restore(Windows 8.1의 기능)도 이 릴리스에서 지원되지 않습니다. 자세한 내용은 Rapid Recovery 설치 및 업그레이드 안내서를 참조하십시오.

9 볼륨 매핑 페이지에서 복원하려는 복구 지점의 각 볼륨에 대해 적합한 대상 볼륨을 선택합니다. 볼륨을 복원하지 않으려면 대상 볼륨 열에서 **복원 안 함**을 선택합니다.

10 **고급 옵션 표시**를 선택한 후 다음 작업을 수행합니다.

- Windows 시스템으로 복원의 경우 Live Recovery를 사용하려면 **Live Recovery**를 선택합니다.

  Rapid Recovery에서 Live Recovery 인스턴트 복구 기술을 사용하면 Windows 시스템의 저장된 복구 지점에서 실제 시스템 또는 가상 시스템으로 데이터를 즉시 복구하거나 복원할 수 있고, 여기에는 Microsoft Windows 저장 공간이 포함됩니다. Live Recovery는 Linux 시스템 또는 에이전트 없는 보호를 사용하는 VM에 사용할 수 없습니다.
- 복원이 시작되기 전에 선택한 볼륨을 분리하려는 경우 **강제 분리**를 선택합니다.

  주의: 데이터를 복원하기 전에 강제로 분리하지 않으면 볼륨이 사용 중이라는 오류가 표시되어 복원이 실패할 수 있습니다.

11 **다음**을 클릭합니다.

12 데이터베이스 분리 페이지에서 복원하려는 볼륨이 SQL 또는 Microsoft Exchange 데이터베이스를 포함하는 경우 분리하라는 메시지가 표시됩니다.

복원이 완료된 후에 이러한 데이터베이스를 다시 마운트하려면 **복구 지점이 복원된 후 자동으로 모든 데이터베이스 다시 마운트**를 선택합니다.

13 **다음**을 클릭합니다.

경고 페이지가 표시되어 복원하려는 볼륨의 모든 프로그램을 닫으라는 메시지가 표시될 수 있습니다. 이 경우 다시 **다음**을 클릭합니다.

14 요약 페이지에서 **중요!** 옵션을 선택합니다. **이 작업은 선택한 볼륨을 선택한 복구 지점의 데이터로 덮어씁니다**로 복원 볼륨의 결과를 이해했음을 확인합니다.

경고: 이 옵션은 선택한 복구 지점의 날짜와 시간 이후에 선택한 볼륨에 저장된 모든 데이터가 복원시 손실된다는 결과를 설명합니다.

15 **마침**을 클릭합니다.

Windows 탐색기를 사용하여 디렉터리 또는 파일 복원

Windows 탐색기를 사용하여 마운트된 복구 지점에서 디렉터리와 파일을 복사하여 Windows 시스템으로 붙여 넣을 수 있습니다. 이 기능은 복구 지점의 일부만 사용자에게 배포하려는 경우 유용합니다.

디렉터리와 파일을 복사할 때 복사 작업을 수행 중인 사용자의 액세스 권한이 사용되고 붙여 넣은 디렉터리와 파일에 적용됩니다. 원래 파일 권한을 보존한 상태에서 디렉터리와 파일을 복원하려면(예를 들어, 파일 서버에서 사용자의 폴더를 복원하는 경우) Windows 탐색기를 사용하여 디렉터리 또는 파일 복원 및 권한 보존을(를) 참조하십시오.

1 복원할 데이터가 포함된 복구 지점을 마운트합니다. 자세한 내용은 복구 지점 마운트을(를) 참조하십시오.
2 Windows 탐색기에서 마운트된 복구 지점으로 이동하여 복원할 디렉터리와 파일을 선택합니다. 마우스 오른쪽 단추로 클릭한 다음 **복사**를 선택합니다.
3 Windows 탐색기에서 데이터를 복원할 시스템 위치로 이동합니다. 마우스 오른쪽 단추를 클릭한 다음 **붙여넣기**를 선택합니다.

Windows 탐색기를 사용하여 디렉터리 또는 파일 복원 및 권한 보존

Windows 탐색기를 사용하여 파일 액세스 권한을 보존한 상태로 마운트된 복구 지점에서 디렉터리와 파일을 복사하여 Windows 시스템으로 붙여넣을 수 있습니다.

예를 들어, 파일 서버에서 특정 사용자만 액세스하는 폴더를 복원하려면 복사 및 권한을 사용하여 붙여넣기 명령을 통해 복원한 파일이 액세스를 제한하는 권한을 보유하도록 하십시오. 이 방법을 사용하면 복원한 디렉터리와 파일에 수동으로 권한을 적용할 필요가 없습니다.

노트: 권한을 사용하여 붙여넣기 명령은 Rapid Recovery Core 및 Agent 소프트웨어와 함께 설치됩니다. Local Mount Utility에서는 이 명령을 사용할 수 없습니다.

1 복원할 데이터가 포함된 복구 지점을 마운트합니다. 자세한 내용은 복구 지점 마운트을(를) 참조하십시오.
2 Windows 탐색기에서 마운트된 복구 지점으로 이동하여 복원할 디렉터리와 파일을 선택합니다. 마우스 오른쪽 단추로 클릭한 다음 **복사**를 선택합니다.
3 Windows 탐색기에서 데이터를 복원할 시스템 위치로 이동합니다. 마우스 오른쪽 단추를 클릭한 다음 **권한을 사용하여 붙여넣기**를 선택합니다.

노트: 이 단계에서 마우스 오른쪽 단추 메뉴에 권한을 사용하여 붙여넣기 명령이 비활성화되면 Windows 탐색기에서 복사할 파일을 인식하지 못합니다. 2단계를 반복하여 마우스 오른쪽 단추 메뉴에서 권한을 사용하여 붙여넣기 명령을 활성화합니다.

클러스터 및 클러스터 노드에 대한 복원 수행

복원은 복구 지점으로부터 시스템의 볼륨을 복원하는 프로세스입니다. 서버 클러스터에 대해 노드 또는 시스템 수준에서 복원을 수행합니다. 이 섹션에서는 클러스터 볼륨의 복원 수행에 대한 지침을 제공합니다.

CCR 및 DAG(Exchange) 클러스터에 대한 복원 수행

CCR 및 DAG(Exchange) 클러스터에 대한 복원을 수행하려면 이 절차의 단계를 완료하십시오.

1 하나를 제외한 나머지 노드를 모두 끕니다.
2 복구 지점에서 볼륨 복원 및 명령줄을 사용하여 Linux 시스템의 볼륨 복원 에 설명된 대로 시스템에 대한 표준 Rapid Recovery 절차를 사용하여 복원을 수행합니다.
3 복원이 완료되면 클러스터 볼륨에 모든 데이터베이스를 마운트합니다.
4 기타 모든 노드를 해제합니다.
5 Exchange의 경우, Exchange Management 콘솔을 탐색하여 각 데이터베이스에 데이터베이스 복사 업데이트 작업을 수행합니다.

SCC(Exchange, SQL) 클러스터에 대한 복원 수행

SCC(Exchange, SQL) 클러스터에 대한 복원을 수행하려면 이 절차의 단계를 완료하십시오.

1 하나를 제외한 나머지 노드를 모두 끕니다.
2 복구 지점에서 볼륨 복원 및 명령줄을 사용하여 Linux 시스템의 볼륨 복원 에 설명된 대로 시스템에 대한 표준 Rapid Recovery절차를 사용하여 복원을 수행합니다.
3 복원이 완료되면 클러스터 볼륨에서 모든 데이터베이스를 마운트합니다.
4 나머지 모든 노드를 하나씩 켭니다.

노트: 쿼럼 디스크는 롤백할 필요가 없습니다. 쿼럼 디스크는 자동으로 다시 생성되거나 클러스터 서비스 기능을 사용하여 다시 생성할 수 있습니다.

연결된 아카이브에서 복원

아카이브에서 데이터를 복원하는 방법은 두 가지가 있습니다. 미설치 복원(BMR)을 위한 소스로 아카이브를 사용하거나 아카이브를 연결하고 아카이브에서 복원 지점을 마운트한 다음 아카이브된 데이터를 복원할 수 있습니다.

아카이브를 연결하면 Core 콘솔의 Archives(아카이브) 페이지의 Attached Archives(연결된 아카이브) 아래 나타나지만 아카이브의 내용은 왼쪽 탐색 영역에서 액세스할 수 있습니다. 내용은 아카이브의 이름 아래에 나타납니다. 아카이브된 시스템은 복구 지점을 마운트하고 복구할 항목을 찾은 다음 Windows 탐색기를 사용하여 항목을 대상에 붙여넣는, 현재 보호되는 시스템과 같은 방식으로 복구 지점에 액세스할 수 있도록 복구 지점 전용 시스템으로 나타납니다.

그러면 아카이브를 리포지토리로 가져오는 대신 연결된 아카이브에서 복원할 수 있다는 장점이 있습니다.

- 연결된 아카이브에서 복원하면 전체 아카이브를 리포지토리로 가져오는 데 사용될 수 있는 시간이 절약됩니다.
- 또한, 아카이브를 가져올 때 아카이브된 복구 지점이 리포지토리에 추가됩니다.
  이러한 보관된 복구 지점은 리포지토리에서 가장 오래된 항목이 될 수 있으므로 다음 야간 작업 중에 보존 정책에 따라 롤업될 수 있 수 있습니다(하지만, 이 조치로는 아카이브에서 삭제되지 않으며 다음 날 다시 가져올 수 있습니다).
- 마지막으로, Core는 아카이브를 분리하더라도 아카이브와 연결 관계를 기억하므로 나중에 다시 아카이브를 쉽고 빠르게 연결할 수 있습니다.
  연결을 삭제하면 연결을 제거할 수 있습니다.

연결된 아카이브에서 데이터를 복원하려면 관련 링크를 사용하여 다음 단계를 수행하십시오.

노트: 연결된 아카이브에서 복원하는 절차는 롤업된 복구 지점의 아카이브가 이미 있다고 가정합니다.

1 아카이브를 연결합니다.
2 복구하려는 데이터를 포함하는 복구 지점을 마운트합니다.
3 다음 방법을 사용하여 데이터를 복원합니다.
   - 파일 또는 폴더와 같은 데이터를 복구 지점에서 복원합니다.
   - 전체 복구 지점을 복원합니다.
   - 복구 지점을 가상 시스템으로 내보냅니다.

관련 링크

보관함 연결
복구 지점 마운트
Windows 탐색기를 사용하여 디렉터리 또는 파일 복원
Rapid Recovery에서 가상 시스템으로 내보내기 정보
Windows 백업
아카이브 이해
아카이브 가져오기
아카이브에서 BMR 수행

Windows 시스템용 Bare Metal Restore 이해

이 섹션에서는 Bare Metal과 유사하거나 다른 형식의 하드웨어에서 보호된 Windows 시스템을 복원하는 방법을 설명합니다.

Windows 시스템용 Bare Metal Restore

서버가 예상대로 작동되면 수행하도록 구성한 작업이 실행되고 수행됩니다. 실패한 경우에는 작업이 실행되거나 수행되지 않습니다. 서버 작동이 중단되는 심각한 문제가 발생하면 즉각적인 조치를 수행하여 해당 시스템의 모든 기능을 복원해야 합니다.

Rapid Recovery는 Windows 또는 Linux 시스템에서 BMR(Bare Metal Restore)를 수행할 수 있는 기능을 제공합니다. BMR는 특정 시스템의 전체 소프트웨어 구성을 복원하는 프로세스입니다. 복원 작업이 서버의 데이터를 복원할 뿐만 아니라 하드 드라이브를 다시 포맷하고 운영 체제와 모든 소프트웨어 응용프로그램도 다시 설치하기 때문에 "bare metal"이라는 용어를 사용합니다. BMR를 수행하려면 보호 대상 시스템에서 복구 지점을 지정하고 지정된 실제 시스템 또는 가상 시스템으로 롤백합니다(복원을 수행합니다). 시스템 볼륨으로 복원을 수행하는 경우 BMR로 간주됩니다. 복원을 수행할 경우와 부트 CD가 필요한 경우 BMR로 간주됩니다. Bare Metal Restore를 수행하도록 선택할 수 있는 다른 환경에는 하드웨어 업그레이드 또는 서버 교체가 포함되며, 두 경우 모두 복구 지점에서 업그레이드 또는 교체된 하드웨어로의 복원을 수행합니다.

Rapid Recovery는 FAT32 EFI 파티션에서 부팅되는 Windows 8, 8.1 및 Windows Server 2012, 2012 R2 운영 체제를 보호 또는 복구할 뿐만 아니라 ReFS(Resilient File System) 볼륨에도 사용할 수 있도록 지원합니다.

노트: 저장 공간 디스크 구성의 Bare Metal Restore(Windows 8.1의 기능)도 이 릴리스에서 지원되지 않습니다. 현재는 ReFS에 드라이버 제한이 있기 때문에 전체 복원 및 BMR만 지원되므로 복원은 사용자 모드, VM 내보내기 등에서 구현됩니다. Core가 ReFS 파일 시스템을 포함하는 하나 이상의 에이전트 볼륨을 보호하는 경우 Window 8, Windows 8.1, Windows Server 2012 또는 Windows Server 2012 R2 운영 체제가 ReFS의 기본 지원을 제공하므로 이러한 시스템에 Core를 설치해야 합니다. 그렇지 않으면 기능이 제한되고 볼륨 이미지 마운트와 같은 항목을 포함하는 작업이 수행됩니다. 이 경우 Rapid Recovery Core Console은 해당되는 오류 메시지를 표시합니다.

지원되는 Linux 운영 체제만 보호 또는 복구할 수 있습니다. 여기에는 Ubuntu®, Red Hat® Enterprise Linux®, CentOS™, and SUSE® Linux Enterprise Server(SLES®)가 포함됩니다. 자세한 내용은 *Dell Data Protection | Rapid Recovery 설치 및 업그레이드 안내서*를 참조하십시오.

BMR는 물리적 또는 가상 시스템에서 수행할 수 있습니다. 또한 Rapid Recovery에서는 하드웨어가 유사하거나 형식이 달라도 BMR를 수행할 수 있습니다. Rapid Recovery에서 BMR를 수행하면 운영 체제를 특정 플랫폼에서 분리하여 이동성을 제공합니다.

유사 하드웨어에 대한 BMR 수행의 예로는 기존 시스템의 하드 드라이브 교체 또는 작동 중단된 서버를 동일한 시스템으로 스와핑이 포함됩니다.

다른 형식의 하드웨어에 대한 BMR 수행의 예로는 다른 제조업체가 제조하거나 다른 구성을 가진 작동 중단된 시스템 복원이 포함됩니다. 이 프로세스에는 부트 CD 이미지 만들기, 이미지를 디스크에 굽기, 부트 이미지의 대상 서버에서 시작, 복구 콘솔 인스턴스에 연결, 볼륨 매핑, 복구 시작, 프로세스 모니터링이 포함됩니다. Bare Metal Restore가 완료되면 복원된 서버에서 운영 체제 및 소프트웨어 응용프로그램 로드 작업을 계속한 다음 구성에 필요한 고유 설정을 구현할 수 있습니다.

Bare Metal Restore는 재해 복구 시나리오에서는 물론 서버 업그레이드 또는 교체 시 데이터 마이그레이션에도 사용됩니다.

Windows 시스템에 대한 미설치 복원 수행

Windows 시스템에 대한 미설치 복원 수행하려면 다음 작업을 수행합니다.

- Windows 부팅 이미지를 생성합니다. 이 부팅 CD ISO 이미지는 대상 드라이브를 시작하는 데 사용됩니다. 여기에서 범용 복구 콘솔에 액세스하여 Core에 있는 백업과 통신할 수 있습니다. Windows 시스템용 부팅 CD 생성 이해을(를) 참조하십시오.
  - 대상 시스템을 시작하려면 실제 미디어가 필요한 경우 부팅 CD ISO 이미지를 미디어로 전송해야 합니다. 부트 CD ISO 이미지를 미디어로 전송을(를) 참조하십시오.
  - 모든 경우에 대상 서버에 부팅 이미지를 로드하고 부팅 이미지에서 서버를 시작합니다. 부트 CD 로드 및 대상 시스템 시작을(를) 참조하십시오.

    노트: 이 프로세스는 Create Boot CD(부팅 CD 생성) 대화 상자에서 부팅 CD 이미지를 관리하는 방법에 대해 설명합니다. 마법사의 Boot CD(부팅 CD) 페이지에서 시작하여 Restore Machine Wizard(시스템 복원 마법사)의 이러한 단계를 수행할 수도 있습니다. 마법사의 Destination(대상) 페이지에서 부팅 CD를 사용하여 대상 시스템에 대한 복원을 지정할 때 여기에 액세스합니다. Restore Machine Wizard(시스템 복원 마법사)에서 미설치 복원을 위해 Windows 부팅 이미지를 관리하는 단계별 지침은 시스템 복원 마법사를 사용하여 Bare Metal Restore 수행 정보을(를) 참조하십시오.
- Windows에 대한 미설치 복원을 시작합니다. 대상 시스템이 부팅 CD에서 시작되면 BMR을 시작할 수 있습니다. BMR용 URC 사용을(를) 참조하십시오. 여기에는 다음과 같은 작업을 수행합니다.
  - Core의 복구 지점에서 복원을 시작합니다. 복구 지점 선택 및 BMR 시작을(를) 참조하십시오.
  - 볼륨을 매핑합니다(완전 복원의 디스크 매핑 방법 참조).
  - 다른 종류의 하드웨어로 복원하고 부팅 CD에 필요한 저장소 및 네트워크 드라이버가 없는 경우 휴대용 미디어 장치에서 드라이버를 로드해야 할 수 있습니다. 자세한 내용은 Universal Recovery Console을 사용하여 드라이버 로드을(를) 참조하십시오.
- Restore Machine Wizard(시스템 복원 마법사)에서 BMR 수행. 선택적으로, Windows 부팅 이미지를 관리하고 모든 하위 작업을 포함하여 BMR을 실행하는 프로세스는 Restore Machine Wizard(시스템 복원 마법사)에서 수행할 수 있습니다. 마법사 실행에 대한 자세한 내용은 복구 지점에서 볼륨 복원의 1~5단계를 참조한 후 시스템 복원 마법사를 사용하여 Bare Metal Restore 수행 정보을(를) 참조하십시오.
- 미설치 복원 확인. 미설치 복원을 시작한 후 진행률을 확인하고 모니터링할 수 있습니다. Bare Metal Restore 확인을(를) 참조하십시오.
  - 복원의 진행 상태를 모니터링할 수 있습니다. 복구 진행 상황 보기을(를) 참조하십시오.
  - 작업이 완료되면 복원된 서버를 시작할 수 있습니다. 복원된 대상 서버 시작 을(를) 참조하십시오.
  - BMR 프로세스의 문제를 해결합니다. Universal Recovery Console에 대한 연결 문제 해결 및 부팅 문제 복구을(를) 참조하십시오.

Windows 시스템에서 Bare Metal Restore 수행을 위한 전제 조건

Windows 시스템에서 Bare Metal Restore 수행을 시작하기 전에 다음과 같은 조건과 기준을 충족해야 합니다.

- 64비트 CPU Rapid Recovery 부트 CD는 Win PE 5.1 운영 체제를 포함합니다. Rapid Recovery BMR는 x86 기반 CPU와 호환되지 않습니다. 64비트 CPU에서만 BMR를 수행할 수 있습니다.

노트: 이 요구 사항이 6.0의 새로운 기능입니다.

- 복원할 시스템 백업. 복원하려는 보호된 서버의 복구 지점이 있는 작동 중인 Rapid Recovery Core가 있어야 합니다.
- 복원할 하드웨어(신규 또는 기존, 비슷한 형식 또는 다른 형식). 대상 시스템은 에이전트의 설치 요구 사항을 충족해야 합니다. 자세한 내용은 *Dell Data Protection | Rapid Recovery 설치 및 업그레이드 안내서*를 참조하십시오.
- 이미지 미디어 및 소프트웨어. 빈 CD나 DVD와 디스크 굽기 소프트웨어 또는 ISO 이미지를 만들 소프트웨어가 있어야 합니다. UltraVNC와 같은 가상 네트워크 컴퓨팅 소프트웨어를 사용하여 원격으로 시스템을 관리하는 경우, VNC Viewer가 있어야 합니다.
- 호환 가능한 저장소 드라이버 및 네트워크 어댑터 드라이버. 다른 형식의 하드웨어로 복원하는 경우 RAID, AHCI 및 칩셋 드라이버를 비롯한 대상 시스템용 호환 저장소 드라이버와 네트워크 어댑터 드라이버가 있어야 합니다(해당되는 경우).
- 저장 공간 및 파티션(해당하는 경우). 하드 드라이브에 소스 볼륨을 포함할 대상 시스템의 대상 파티션을 만들기에 충분한 공간이 있는지 확인합니다. 모든 대상 파티션은 최소한 원래 소스 파티션보다 커야 합니다.
- 호환 파티션. FAT32 EFI 파티션에서 부팅되는 Windows 8, Windows 8.1, Windows 10, Windows Server 2012 및 Windows Server 2012 R2 운영 체제는 물론, ReFS(Resilient File System) 볼륨도 보호 또는 복구에 사용할 수 있습니다. UEFI 파티션은 단순 FAT32 볼륨으로 간주됩니다. 증분 전송은 완벽히 지원되고 보호됩니다. Rapid Recovery는 자동 파티셔닝 GPT 디스크를 포함한 BMR의 UEFI 시스템을 지원합니다.

시스템 복원 마법사를 사용하여 Bare Metal Restore 수행 정보

마법사를 통해 Windows 부팅 이미지를 관리하려면 다음 작업을 수행하십시오.

- 부팅 CD 생성을 시작합니다.
- Core 시스템의 이미지에 대한 경로를 정의합니다.
- 복원하려는 하드웨어에 해당하는 복구 환경을 선택합니다.
- 필요에 따라 복원되는 에이전트에서 네트워크 또는 UltraVNC를 사용하도록 연결 매개변수를 정의합니다.
- 필요에 따라 선택하려는 하드웨어에 드라이버를 삽입합니다.
- 필요에 따라 실제 미디어에 부팅 이미지를 전송합니다.
- 부팅 CD에서 데이터를 복원할 시스템을 부팅합니다.
- URC(Universal Recovery Console)에 연결합니다.
- 볼륨을 매핑합니다.
- Core의 선택한 복구 지점에서 Bare Metal Restore을 시작합니다.

노트: 이 프로세스는 시스템 복원 마법사를 사용하여 BMR을 수행하기 위한 프로세스의 일부분으로, 시스템 복원 마법사에서 부트 CD 이미지를 관리하기 위한 방법을 설명합니다. 또한 부트 CD 만들기 대화 상자에서 부트 이미지를 관리할 수도 있습니다. 시스템 복원 마법사 외부에서 부트 CD 이미지 관리에 대한 자세한 내용은 Windows 시스템용 부팅 CD 생성 이해을(를) 참조하십시오.

시스템 복원 마법사를 사용하여 Bare Metal Restore 복원 수행

Restore Wizard를 사용하여 Bare Metal Restore(BMR) 수행뿐만 아니라 부팅 CD를 생성할 수 있습니다.

BMR을 수행하려면 Windows 시스템에서 Bare Metal Restore 수행을 위한 전제 조건 또는 Linux 시스템에서 Bare Metal Restore 수행을 위한 전제 조건를 상황에 따라 참조하십시오. Core Console에서 Windows 시스템에 대해 BMR을 시작하려면 Windows 시스템에 대한 미설치 복원 수행를 참조하십시오.

보호된 시스템에 Agent 소프트웨어가 설치되어 있고 복원 작업을 수행할 수 있는 복구 지점이 있어야 합니다.

1 보호된 시스템의 볼륨을 복원하려면 Core Console로 이동하여 Rapid Recovery 단추 모음에서 **복원**을 클릭합니다.
시스템 복원 마법사가 나타납니다.

2 시스템 페이지에서 복원하려는 보호된 시스템을 선택한 후 **다음**을 클릭합니다.
복구 지점 페이지가 나타납니다.

3 시스템을 복원할 때 사용하려는 복구 지점을 선택합니다.
- 또한 표시되는 복구 지점 수를 제한하려는 경우 볼륨별로 (정의된 경우) 또는 복구 지점의 생성 날짜별로 필터링할 수 있습니다. 또한 특정 복구 지점에 대한 검색을 수행할 수도 있습니다.

4 **다음**을 클릭합니다.

5 대상 페이지에서 **부팅 CD를 사용하여 대상 시스템에 복구**를 선택합니다.
- 복원하려는 시스템에 부팅 CD를 로드하지 않은 경우 **다음**을 클릭한 후 6단계를 계속 수행합니다.
- BMR 대상 시스템에 이미 부팅 CD가 로드되어 있는 경우 **대상 시스템에서 실행 중인 부팅 CD가 있습니다**를 선택하고 **다음**을 클릭한 뒤 16단계로 이동합니다.

6 부팅 CD 페이지의 출력 경로 텍스트 상자에 부팅 CD ISO 이미지를 저장할 경로를 입력합니다.

노트: 이미지를 저장하려는 공유 드라이브의 디스크 공간이 부족하면 필요에 따라 경로에 디스크를 생성할 수 있습니다(예: F:\filename.iso).

노트: 파일 확장명은 .iso여야 합니다. 경로를 지정할 경우에는 영숫자 문자, 하이픈, 백슬래시(경로 구분 기호로만 사용) 및 마침표(개별 호스트 이름과 도메인에만 사용)만 사용합니다. 문자 a - z는 대소문자를 구분하지 않습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.

7 또한 대상 시스템에 대해 네트워크 매개 변수를 설정하거나 UltraVNC 기능을 추가하려면 **고급 옵션 표시**를 선택하고 다음 단계 중 하나를 수행합니다.
- BMR 대상에 네트워크 연결을 설정하려면 **다음 IP 주소 사용**을 선택한 뒤 다음 표의 설명에 따라 정보를 입력합니다.

표 153. 네트워크 연결 옵션

옵션	설명
IP 주소	복원된 시스템의 IP 주소입니다.
서브넷 마스크	복원된 시스템의 서브넷 마스크입니다.
기본 게이트웨이	복원된 시스템의 기본 게이트웨이를 지정합니다.
DNS Server(DNS 서버)	복원된 시스템의 도메인 이름 서버를 지정합니다.

- UltraVNC 계정이 있으며 해당 계정을 사용하여 BMR을 완료하려는 경우 **UltraVNC 추가**를 선택한 뒤 다음 표의 설명에 따라 정보를 입력합니다.

표 154. UltraVNC 연결 자격 증명

옵션	설명
암호	UltraVNC 계정에 대한 암호입니다.
포트	BMR 대상에 연결하기 위해 사용하는 포트입니다. 기본 포트는 5900입니다.

8 **다음**을 클릭합니다.

9
- 복원된 시스템에 대해 네트워크 연결을 설정하려면 다음 표의 설명에 따라 **다음 IP 주소 사용**을 선택합니다.
- UltraVNC 정보를 정의하려면 다음 표의 설명에 따라 **UltraVNC 추가**를 선택합니다.
  복구 콘솔에 원격으로 액세스하려면 이 옵션을 사용합니다. 부트 CD 사용 중에 Microsoft 터미널 서비스를 사용하여 로그온할 수 없습니다.

표 155. UltraVNC 연결

옵션	설명
암호	이 UltraVNC 연결의 암호를 지정합니다.
포트	이 UltraVNC 연결의 포트를 지정합니다. 기본 포트는 5900입니다.

10 부트 CD 페이지에서 선택한 항목을 사용하려면 **다음**을 클릭합니다.

11 또한 드라이버 추가 페이지에서 다른 종류의 하드웨어로 복원하려는 경우 다음 단계에 따라 대상 시스템에 적절한 저장 컨트롤러와 다른 드라이버를 추가합니다.

a 서버 제조업체의 웹 사이트에서 드라이버를 다운로드하여 압축을 해제합니다.
b 압축 유틸리티(예: WinZip)를 사용하여 각 드라이버를 .zip 파일로 압축합니다.
c 시스템 복원 마법사의 드라이버 추가 페이지에서 **드라이버의 아카이브 추가**를 클릭합니다.
d 파일 시스템을 탐색하여 압축된 드라이버 파일을 찾아 선택한 다음 **열기**를 클릭합니다.
e 필요한 모든 드라이버를 추가할 때까지 C단계 및 D단계를 적절하게 반복합니다.
드라이버 추가에 대한 자세한 내용은 부팅 CD의 드라이버 추가 이해를 참조하십시오.

노트: Windows의 일부 버전은 자동 드라이버 추가와 호환되지 않습니다. 운영 체제가 호환되지 않는 경우 드라이버를 C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\에 수동으로 저장합니다.

Rapid Recovery로 부팅 CD ISO 이미지를 생성합니다.

12 **다음**을 클릭합니다.

13 BMR 대상 시스템을 시작한 뒤 다음 옵션 중 하나를 완료합니다.
- 부팅 CD ISO 이미지에서 대상 시스템을 시작할 수 있으면 지금 시작하십시오.
- 대상 시스템을 시작할 수 없으면 ISO 이미지를 실제 미디어(CD 또는 DVD)로 복사하고 대상 시스템에 디스크를 로드하거나 부팅 CD에서 로드하도록 시스템을 구성하고 부팅 CD에서 재시작합니다.

노트: 처음 로드되는 볼륨이 부팅 CD가 되도록 대상 시스템의 BIOS 설정을 변경해야 합니다.

대상 시스템이 부팅 CD에서 시작되면 URC(Universal Recovery Console) 인터페이스가 표시됩니다. 이 환경은 Rapid Recovery Core에서 직접 시스템 드라이브를 복원하거나 볼륨을 선택할 때 사용됩니다. URC에 있는 IP 주소와 인증 키 자격 증명은 부트 CD에서 시작할 때마다 갱신됩니다.

14 Core Console에서 시스템 복원 마법사의 연결 페이지로 이동하여 다음과 같이 복원하려는 시스템의 URC 인스턴스에서 인증 정보를 입력합니다.

표 156. 인증 옵션

옵션	설명
IP 주소	대상 시스템의 URC에 제공되는 IP 주소입니다.
인증 키	대상 시스템의 URC에 제공되는 인증 키입니다.

15 **다음**을 클릭합니다.

16 디스크 매핑 페이지에서 볼륨을 수동으로 매핑하려는 경우 10단계를 계속 진행합니다. 볼륨을 자동으로 매핑하려면 다음 단계를 완료합니다.

a 볼륨 매핑 드롭다운 메뉴에서 **자동**을 선택합니다.

b 볼륨 목록에서 복원하려는 볼륨을 선택했는지 확인합니다. 볼륨은 모두 기본적으로 선택되어 있습니다.

나열된 볼륨을 복원하지 않으려면 해당 옵션을 선택 해제합니다.

노트: 복원을 수행하려면 볼륨을 하나 이상 선택해야 합니다.

c 오른쪽에서 복원 대상 디스크를 선택합니다.

d **다음**을 클릭합니다.

e 디스크 매핑 미리 보기에서 선택한 복원 작업의 매개 변수를 검토합니다.

f 18단계로 이동합니다.

17 볼륨을 수동으로 매핑하려면 디스크 매핑 페이지에서 다음 단계를 완료하십시오.

a 볼륨 매핑 드롭다운 메뉴에서 **수동**을 선택합니다.

b 대상 열에서 복원하려는 대상 볼륨을 선택합니다. (선택 사항) 나열된 볼륨을 복원하지 않으려면 해당 옵션을 선택 해제합니다.

노트: 복원을 수행하려면 볼륨을 하나 이상 선택해야 합니다.

18 **마침**을 클릭합니다.

주의: 대상 드라이브에 있는 기존의 모든 파티션과 데이터가 영구적으로 제거되며, 운영 체제 및 모든 데이터를 비롯하여 선택한 복구 지점의 내용으로 대체됩니다.

19 복원하려는 볼륨에 SQL 또는 Microsoft Exchange 데이터베이스가 있는 경우, 그리고 데이터베이스 분리 페이지에서 라이브 복원을 수행할 경우 해당 데이터베이스를 분리할지 묻는 메시지가 나타납니다. (선택 사항) 복원이 완료된 후에 이러한 데이터베이스를 다시 마운트하려면 **복구 지점이 복원된 후 자동으로 모든 데이터베이스 다시 마운트**를 선택합니다.

20 **복원**을 클릭합니다.

21 상태 메시지에서 **확인**을 클릭하여 복원 절차가 시작되었는지 확인합니다.

복원을 시작합니다. 이벤트 페이지에서 진행 상황을 모니터링할 수 있습니다. 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

Windows 시스템용 부팅 CD 생성 이해

Windows에 대한 BMR(Bare Metal Restore) 작업에는 부팅 CD로 불리는 부팅 이미지가 필요하며, 이 이미지는 Rapid Recovery Core Console에서 매개 변수를 정의하여 생성할 수 있습니다. 이 이미지는 필요에 따라 조정됩니다. 이 이미지를 사용하여 대상 Windows 시스템을 시작합니다. 사용자 환경에 따라 이 이미지를 CD 또는 DVD와 같은 실제 미디어로 전송해야 할 수도 있습니다. 그런 다음 가상으로 또는 실제로 부트 이미지를 로드하고 부트 이미지에서 Windows 서버를 시작합니다.

Windows 시스템에 대한 BMR(Bare Metal Restore)을 수행하는 첫 번째 단계는 Rapid Recovery Core Console에서 부팅 CD 파일을 만드는 것입니다. 이 파일은 Rapid Recovery Core에서 직접 시스템 드라이브 또는 전체 서버를 복원하는 데 사용하는 환경인 Rapid Recovery Universal Recovery Console(URC) 인터페이스가 포함된, 부팅 가능한 ISO 이미지입니다.

생성하는 부트 CD ISO 이미지는 복원 중인 시스템에 따라 조정되므로, 올바른 네트워크 및 대용량 저장소 드라이버를 포함해야 합니다. 복구 지점이 시작된 시스템에서 다른 하드웨어로 복원하려면 부트 CD에 저장소 컨트롤러와 기타 드라이버를 포함해야 합니다. 이러한 드라이버를 부팅 CD에 삽입하는 방법에 대한 자세한 내용은 부팅 CD에 드라이버 삽입하는 내용 이해을(를) 참조하십시오.

부팅 CD에 드라이버 삽입하는 내용 이해

부팅 CD 이미지에는 서버의 드라이브를 인식하기 위한 저장소 드라이버와 네트워크를 통해 Rapid Recovery Core와 통신하기 위한 네트워크 어댑터 드라이버가 필요합니다.

일반적인 Windows 8.1 x64 저장소 컨트롤러와 네트워크 어댑터 드라이버 세트는 Windows용 부팅 CD를 생성할 때 자동으로 포함됩니다. 이는 최신 Dell 시스템의 요구 사항을 충족합니다. 다른 제조업체의 시스템이나 이전 Dell 시스템은 부트 CD를 만들 때 저장소 컨트롤러 또는 네트워크 어댑터 드라이버를 삽입해야 합니다. 생성한 부트 CD에 복원을 완료하는 데 필요한 드라이버가 없는 경우 URC를 사용하여 대상 시스템에 드라이버를 로드할 수도 있습니다. 자세한 내용은 Universal Recovery Console을 사용하여 드라이버 로드을(를) 참조하십시오.

부트 CD를 만들 때 대상 서버의 복구 콘솔, 네트워크 어댑터 및 저장소 간의 운용성을 개선하기 위해 드라이버 삽입이 사용됩니다.

복구 지점에서 복원되는 데이터에는 이전에 있던 하드웨어용 드라이버가 포함됩니다. 다른 형식의 하드웨어로 Bare Metal Restore를 수행하는 경우, 데이터가 드라이브로 복원된 후 URC를 사용하여 복원할 운영 체제에 저장소 컨트롤러 드라이버도 삽입해야 합니다. 그러면 새 하드웨어 집합을 사용하여 복원된 운영 체제를 부팅할 수 있습니다. 복원 후 OS가 부팅되면 OS에서 필요한 추가 드라이버를 다운로드하고 설치하여 새 하드웨어와 상호 작용할 수 있습니다.

부팅 CD ISO 이미지 만들기

부팅 CD는 Rapid Recovery가 Bare Metal Restore(BMR)를 수행하기 위해 예약한 ISO 이미지의 휴대용 저장소 위치를 지칭하기 위해 사용하는 용어입니다. 이미지는 Rapid Recovery Universal Recovery Console(URC)을 포함합니다.

시스템에서 BMR을 수행하려면 URC를 실행하는 부팅 CD에서 시스템을 시작해야 합니다. URC를 사용하면 복원을 완료하는 데 사용할 복구 지점 위치에 BMR 대상을 연결할 수 있습니다.

1 복원할 서버가 보호되는 Rapid Recovery Core Console의 아이콘 표시줄에서 자세히 메뉴를 클릭한 후 **부팅 CD**를 클릭합니다.
2 부팅 CD 페이지에서 **부팅 CD 생성**을 클릭합니다.
부트 CD 만들기 대화 상자가 표시됩니다.
3 부팅 CD 생성 대화 상자의 **출력 경로** 텍스트 상자에 부팅 CD ISO 이미지를 저장할 위치를 입력합니다.

노트: 파일 확장명은 .iso여야 합니다. 경로를 지정할 경우에는 영숫자 문자, 하이픈, 백슬래시(경로 구분 기호로만 사용) 및 마침표(개별 호스트 이름과 도메인에만 사용)만 사용합니다. 문자 a~z는 대소문자를 구분하지 않습니다. 공백은 사용하지 않습니다. 다른 기호나 구두점 문자는 사용할 수 없습니다.

4 연결 옵션에서 다음 중 하나를 수행합니다.
- DHCP(동적 호스트 구성 프로토콜)를 사용하여 IP 주소를 동적으로 얻으려면 **자동으로 IP 주소 얻기**를 선택합니다.
- URC에 대한 고정 IP 주소를 지정하려면 **다음 IP 주소 사용**을 선택한 후 다음 정보를 입력합니다.
  - IP 주소
  - 서브넷 마스크
  - 기본 게이트웨이
  - DNS Server(DNS 서버)

노트: 이 4개의 필드를 모두 지정해야 합니다.

5 복구 콘솔에 원격으로 액세스해야 하고 UltraVNC가 설치되어 있는 경우 UltraVNC 옵션에서 다음 단계를 완료합니다.

노트: UltraVNC를 사용하는 동안 URC를 원격으로 관리할 수 있습니다. 부트 CD 사용 중에 Microsoft 터미널 서비스를 사용하여 로그온할 수 없습니다.

a **UltraVNC 추가**를 선택합니다.
b **UltraVNC 암호**를 입력합니다.
c **UltraVNC 포트**를 입력합니다. 기본 포트는 5900입니다.

노트: UltraVNC가 이미 설치되어 있는 경우에만 UltraVNC 옵션을 사용할 수 있습니다. 옵션을 사용하려면 http://www.uvnc.com/downloads/ultravnc/(으)로 이동하여 x64 아키텍처용 UltraVNC 버전 1.0.9.1 이상을 다운로드합니다. 설치하고 winvnc.exe 파일을 C:\Program Files\AppRecovery\Core\BootCdKit\UltraVnc_x64\에 저장합니다.

6 다른 종류의 하드웨어로 복원하려면 다음 단계에 따라 알맞은 저장소 컨트롤러 및 대상 시스템에 맞는 다른 드라이버를 삽입합니다.

노트: 일부 Windows 버전은 자동 드라이버 삽입과 호환되지 않습니다. 사용자의 운영 체제가 호환되지 않으면 드라이버를 C:\Program Files\AppRecovery\Core\BootCdKit\Drivers\에 수동으로 저장합니다.

a 서버 제조업체의 웹 사이트에서 드라이버를 다운로드하고 압축을 풉니다.
b 압축 유틸리티(예: WinZip)를 사용하여 각 드라이버를 .zip 파일로 압축합니다.
c 부팅 CD 생성 대화 상자의 드라이버 창에서 **드라이버 아카이브 추가**를 클릭합니다.
d 파일 시스템을 탐색하여 압축된 드라이버 파일을 찾아 선택한 다음 **열기**를 클릭합니다.
부팅 CD 생성 대화 상자의 드라이버 창에 드라이버 파일이 나타납니다.
e 필요한 드라이버를 모두 추가할 때까지 c단계와 d단계를 적절하게 반복합니다.
f 드라이버 창에서 삽입하려는 드라이버를 선택합니다.

드라이버 삽입에 대한 자세한 내용은 부팅 CD에 드라이버 삽입하는 내용 이해을(를) 참조하십시오.

7 **부팅 CD 생성**을 클릭합니다.
Rapid Recovery가 부팅 CD를 생성하고 사용자가 제공한 파일 이름으로 저장합니다.

8 이 작업의 진행률을 모니터링하려면 아이콘 표시줄로 이동하여 이벤트 아이콘을 클릭합니다.
Rapid Recovery 이벤트 모니터링에 대한 자세한 내용은 작업, 경고, 저널을 사용하여 이벤트 보기을(를) 참조하십시오.

ISO 이미지 생성을 완료하면 부팅 CD 페이지에 이미지 레코드가 나타나 아이콘 표시줄에 있는 자세히 메뉴에서 액세스할 수 있습니다.

ISO 이미지에 액세스하려면 지정한 출력 경로로 이동하거나 부팅 CD 페이지에 있는 링크를 클릭하여 이미지를 원하는 위치로 저장한 다음 새 시스템(예: 네트워크 드라이브)으로 로드할 수 있습니다.

부트 CD ISO 이미지를 미디어로 전송

부트 CD 파일을 만들면 지정한 경로에 ISO 이미지로 저장됩니다. Bare Metal Restore를 수행 중인 서버의 드라이브로 이 이미지를 마운트할 수 있어야 합니다.

부트 CD ISO 이미지를 시스템 시작 시 액세스할 수 있는 CD 또는 DVD에 구울 수 있습니다.

부트 CD에서 시스템을 시작하면 Universal Recovery Console이 자동으로 시작됩니다.

가상 시스템에서 BMR를 수행하는 경우에는 이 단계가 필요하지 않습니다. ISO 이미지를 드라이브에 로드하고 해당 VM에 대한 설정을 편집하여 해당 드라이브에서 시작합니다.

부트 CD 로드 및 대상 시스템 시작

부트 CD 이미지를 만든 후에 새로 만든 부트 CD로 대상 서버를 부팅해야 합니다.

Rapid Recovery Core Console에 연결하거나 추가 드라이버를 다운로드하는 데 크롬을 사용하려면 이더넷 컨트롤러 및 네트워크 어댑터를 먼저 로드해야 합니다. 자세한 내용은 Universal Recovery Console을 사용하여 드라이버 로드을(를) 참조하십시오.

노트: DHCP를 사용하여 부트 CD를 만든 경우 IP 주소와 암호를 캡처해야 합니다.

1 새 서버에서 적절한 위치의 부트 CD 이미지를 로드한 다음 부트 CD 이미지에서 서버를 시작하여 Rapid Recovery Agent 소프트웨어 및 Win PE 5.1을 로드합니다.

대상 시스템에 화면 위쪽에 3개의 아이콘 단추가 있는 파란색 Dell 화면이 표시됩니다.

2 Rapid Recovery URC(Universal Recovery Console) 사용자 인터페이스를 열려면 화면 위쪽에 있는 Dell 아이콘을 클릭합니다.

시스템의 IP 주소 및 암호가 인증 아래에 나타납니다.

노트: 부트 CD로 시스템을 시작할 때마다 새 임시 암호가 생성됩니다. 네트워크 어댑터 설정 창에 표시된 IP 주소와 인증 창에 표시된 인증 암호를 기록해 둡니다. 나중에 데이터 복구 프로세스 동안 콘솔에 다시 기록하기 위해 이 정보가 필요합니다.

노트: 제공된 IP 주소가 없으면, 이더넷 컨트롤러 및 네트워크 어댑터를 로드합니다.

3 IP 주소를 변경하려면 IP 주소를 선택하고 **변경**을 클릭합니다.

노트: 부트 CD 만들기 대화 상자에서 IP 주소를 지정한 경우 Universal Recovery Console에서 해당 주소를 사용하고 이를 네트워크 어댑터 설정 화면에 표시합니다.

시스템에서 Core에 연결할 준비가 되고 복구 지점을 선택하고 Bare Metal Restore 프로세스를 계속합니다.

BMR용 URC 사용

Windows 시스템의 BMR(Bare Metal Restore)를 시작하려면 다음과 같은 조건을 충족해야 합니다.

- Core에 저장된 복구 지점을 복원하려면 적절한 하드웨어가 설치되어 있어야 합니다. 자세한 내용은 Windows 시스템에서 Bare Metal Restore 수행을 위한 전제 조건을(를) 참조하십시오.
- BMR 대상 Windows 시스템이 부트 CD 이미지를 사용하여 시작되어야 합니다. 자세한 내용은 Windows 시스템용 부팅 CD 생성 이해을(를) 참조하십시오.

BMR은 선택한 복구 지점을 사용하여 시스템을 시작합니다. 복원 지점에는 이전 하드웨어의 드라이버가 포함됩니다. 다른 형식의 하드웨어로 복원하는 경우, 데이터가 드라이브로 복원된 후 URC를 사용하여 복원할 운영 체제에 저장소 컨트롤러 드라이버를 삽입해야 합니다. 그러면 새 하드웨어 세트를 사용하여 복원된 운영 체제를 시작할 수 있습니다. OS를 시작한 후 OS가 새 하드웨어와 상호작용하는 데 필요한 추가 드라이버를 다운로드하고 설치할 수 있습니다.

Rapid Recovery Core Console에서 BMR를 실행하려면 다음 작업을 수행합니다.

- 복구 지점 선택 및 BMR 시작
- 완전 복원의 디스크 매핑 방법
- Universal Recovery Console을 사용하여 드라이버 로드

이 프로세스는 Windows 시스템에 대한 미설치 복원 수행의 한 단계입니다.

Universal Recovery Console 도구 정보

URC(Universal Recovery Console)에는 BMR(Bare Metal Restore)를 완료하는 데 도움을 줄 수 있는 도구에 대한 액세스가 포함되어 있습니다.

URC로 부팅되는 BMR 대상에서 Dell 시작 화면의 상단에 있는 중앙 아이콘을 클릭하면 다음과 같은 도구를 찾을 수 있습니다.

- **Far Manager.** 이 도구는 Windows 탐색기와 유사하며, BMR를 완료한 후 Windows 탐색기와 같은 자체 탐색 기능이 있는 운영 체제를 설치할 때까지 서버의 파일을 찾는 방법을 제공합니다.
- **크롬.** 이 브라우저는 Google Chrome™의 공개 소스 기반 프로그램으로, URC를 통해 로드된 네트워크 컨트롤러가 있는 서버에서 인터넷을 탐색할 수 있게 해줍니다.
- **PuTTY.** 이 도구는 공개 소스 터미널 에뮬레이터입니다. Rapid Recovery BMR 환경에서, 사용자 인터페이스가 포함되어 있지 않은 NAS 저장소 장치에 연결할 수 있게 해줍니다. 이 기능은 NAS에 있는 아카이브에서 복원하려는 경우 필요할 수 있습니다.

- **메모장.** Windows 운영 체제에서와 같이, 서식 없는 메모를 입력하고 로그 파일을 볼 수 있게 해줍니다.
- **작업 관리자.** Windows 운영 체제에서와 같이, 복원 프로세스 동안 프로세스를 관리하고 서버의 성능을 모니터할 수 있게 해줍니다.
- **레지스트리 편집기.** Windows 운영 체제에서와 같이, BMR 대상의 시스템 레지스트리를 변경할 수 있게 해줍니다.
- **명령 프롬프트.** 이 도구는 사용자 인터페이스를 설치할 때까지 URC 외부의 BMR 대상에서 명령을 수행할 수 있게 해줍니다.

Universal Recovery Console을 사용하여 드라이버 로드

이 기능을 사용하면 ISO 이미지에 포함하지 않았지만 성공적인 Bare Metal Restore를 위해 필요한 드라이버를 추가할 수 있습니다.

이 작업은 Windows 시스템에 대한 미설치 복원 수행의 한 단계로, BMR용 URC 사용 프로세스의 일부입니다.
부트 CD를 만들 때 ISO 이미지에 필요한 드라이버를 추가할 수 있습니다. 대상 시스템으로 부팅한 후 URC(Universal Recovery Console)에서 저장소 또는 네트워크 드라이버를 로드할 수 있습니다.

다른 형식의 하드웨어로 복원하는 경우 저장소 컨트롤러, RAID, AHCI, 칩셋 및 기타 드라이버가 아직 부트 CD에 없으면 해당 항목을 삽입해야 합니다. 복원 프로세스에 따라 시스템을 다시 시작한 후에는 해당 드라이버가 있어야 운영 체제에서 대상 서버의 모든 장치를 성공적으로 작동할 수 있습니다.

URC를 사용하여 드라이버를 로드하려면 다음 절차 중 하나에서 단계를 완료하십시오.

- 휴대용 미디어를 사용하여 URC(Universal Recovery Console)에서 드라이버 로드
- 크롬을 사용하여 URC 도중 드라이버 로드

휴대용 미디어를 사용하여 URC(Universal Recovery Console)에서 드라이버 로드

다음 작업은 다음 절차의 전제 조건입니다.

- 부팅 CD ISO 이미지 만들기
- 부트 CD ISO 이미지를 미디어로 전송
- 부트 CD 로드 및 대상 시스템 시작

다음 절차를 완료하여 URC(Universal Recovery Console)에서 드라이버를 로드하는 데 휴대용 미디어 장치를 사용할 수 있습니다.

1 인터넷에 연결된 시스템을 사용하여 제조업체의 웹 사이트에서 해당 서버용 드라이버를 다운로드하고 압축을 풉니다.
2 압축 유틸리티(예: WinZip)를 사용하여 각 드라이버를 .zip 파일로 압축합니다.
3 USB 드라이브와 같은 휴대용 미디어 장치로 드라이버의 .zip 파일을 복사하고 저장합니다..
4 연결된 시스템에서 미디어를 제거하고 부트 대상 서버에 삽입합니다.
5 대상 서버에서 부트 CD를 로드한 후 시스템을 시작합니다.
Dell 스플래시 화면이 나타납니다.
6 URC를 시작하려면 **Dell 아이콘**을 클릭합니다.
URC가 열리고 부트 CD 드라이버 관리자 탭이 표시됩니다.
7 **기타 장치** 목록을 확장합니다.
이 목록은 하드웨어에 필요하지만, 부트 CD에 없는 드라이버를 보여 줍니다.
8 목록에서 장치를 마우스 오른쪽 단추로 클릭하고 **드라이버 로드**를 클릭합니다.
9 드라이버 로드 모드 선택 창에서 다음 옵션 중 하나를 선택합니다.
   - 단일 드라이버 패키지 로드(드라이버가 장치 지원의 확인하지 않고 로드됨)
   - 드라이버 패킷에 대한 폴더 스캔(선택한 장치의 드라이버는 선택한 폴더에서 검색)
10 휴대용 미디어 장치에 대한 드라이버를 확장하고 드라이버(파일 확장명 .inf)를 선택하고 **확인**을 클릭합니다.
드라이버가 현재 운영 체제 시스템으로 로드됩니다.
11 정보 창에서 **확인**을 클릭하여 드라이버를 로드되었음을 확인합니다.
12 필요에 따라 로드할 각 드라이버에 대해 이 절차를 반복합니다.

크롬을 사용하여 URC 도중 드라이버 로드

다음 작업은 다음 절차의 전제 조건입니다.

- 부팅 CD ISO 이미지 만들기
- 부트 CD ISO 이미지를 미디어로 전송
- 부트 CD 로드 및 대상 시스템 시작

다음 절차를 완료하면 부트 CD에 설치되어 제공되는 크롬 브라우저를 사용하여 URC 도중 드라이버를 로드할 수 있습니다.

1 대상 서버에서 부트 CD를 로드한 후 시스템을 시작합니다.
Dell 스플래시 화면이 나타납니다.
2 URC를 시작하려면 **Dell 아이콘**을 클릭합니다.
URC가 열리고 부트 CD 드라이버 관리자 탭이 표시됩니다.
3 BMR 대상에서 화면 상단에 있는 도구(중앙 아이콘)를 클릭한 다음, **크롬**을 클릭합니다.
4 크롬 브라우저에서 필요한 드라이버를 다운로드할 수 있는 웹 사이트로 이동합니다.
5 로컬 폴더 또는 네트워크 파일 공유와 같이 선택한 위치에 드라이버를 다운로드합니다.
6 **기타 장치** 목록을 확장합니다.
이 목록은 하드웨어에 필요하지만, 부트 CD에 없는 드라이버를 보여 줍니다.
7 목록에서 장치를 마우스 오른쪽 단추로 클릭하고 **드라이버 로드**를 클릭합니다.
8 드라이버 로드 모드 선택 창에서 다음 옵션 중 하나를 선택합니다.
   - 단일 드라이버 패키지 로드(드라이버가 장치 지원 여부 확인 없이 로드됨).
   - 드라이버 패킷에 대한 폴더 스캔(선택한 장치의 드라이버는 선택한 폴더에서 검색)
9 드라이버를 저장한 위치로 이동하고, 드라이버를 선택한 다음, **확인**을 클릭합니다.
드라이버가 현재 운영 체제 시스템으로 로드됩니다.
10 정보 창에서 **확인**을 클릭하여 드라이버를 로드되었음을 확인합니다.
11 필요에 따라 로드할 각 드라이버에 대해 이 절차를 반복합니다.

복구 지점 선택 및 BMR 시작

BMR(Bare Metal Restore) 대상 시스템에서 URC(Universal Recovery Console)를 액세스할 수 있게 되면 복원하려는 복구 지점을 선택해야 합니다.

Core Console로 이동하여 로드하려는 복구 지점을 선택하고 복구 콘솔을 복원된 데이터의 대상으로 지정합니다.

노트: 이 단계는 모든 Windows 시스템에서 BMR를 수행하고 선택적으로 Linux 시스템에서 BMR를 수행해야 합니다.

이 작업은 Windows 시스템에 대한 미설치 복원 수행의 한 단계로, BMR용 URC 사용 프로세스의 일부입니다.

Core Console에서 Linux 시스템에 대해 BMR를 수행하는 경우 이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계이기도 하며 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행의 프로세스 중 일부입니다.

1 Rapid Recovery Core Console의 보호된 시스템 목록에서 복원하려는 보호된 시스템 이름을 클릭합니다.
선택한 시스템에 대한 요약 페이지가 나타납니다.
2 **복구 지점**을 클릭합니다.
3 BMR에 대해 사용하려는 복구 지점 옆에서 드롭다운 메뉴를 클릭한 다음 **복원**을 클릭합니다.
시스템 복원 마법사가 나타납니다.
4 **부트 CD를 사용하여 대상 시스템에 복구**를 선택합니다.
5 **이미 대상 시스템에서 실행 중인 부트 CD가 있습니다**를 선택합니다.
인증 텍스트 상자가 나타납니다.

6 다음 표의 설명에 따라 복원하려는 시스템에 대한 정보를 입력합니다.

표 157. 대상 시스템 정보

텍스트 상자	설명
IP 주소	복원하려는 시스템의 IP 주소. 이 항목은 URC에 표시되는 IP 주소와 동일합니다.
인증 키	선택한 서버에 연결하는 데 사용할 고유 암호. 이 항목은 URC에 표시되는 인증 키와 동일합니다.

7 **다음**을 클릭합니다.
입력한 연결 정보가 URC와 일치하고 Core와 대상 서버가 네트워크에서 서로 올바르게 식별할 수 있으면 선택한 복구 지점의 볼륨이 로드되고 디스크 매핑 페이지가 나타납니다. 이러한 경우 다음 단계는 볼륨을 매핑하는 것입니다.

8 완전 복원의 디스크 매핑 방법(으)로 이동하여 디스크 매핑 옵션에 대해 알아봅니다.

완전 복원의 디스크 매핑 방법

Universal Recovery Console에 연결되면 복구 지점에 나열된 볼륨과 대상 하드웨어에 존재하는 볼륨 사이에 볼륨을 매핑해야 합니다.

Rapid Recovery에서 볼륨 매핑이 자동으로 시도됩니다. 기본 매핑을 사용하면 대상 시스템의 디스크가 지워지고 다시 파티션이 설정되며 기존의 모든 데이터가 삭제됩니다. 볼륨이 복구 지점에 나열된 순서대로 정렬되고 크기 등에 따라 적절히 디스크에 볼륨이 할당됩니다. 대상 드라이브에 충분한 공간이 있다고 가정하면 자동 디스크 정렬 사용 시 파티션을 만들 필요가 없습니다. 한 디스크를 여러 볼륨에서 사용할 수 있습니다. 드라이브를 수동으로 매핑하는 경우 동일한 디스크를 두 번 사용할 수 없습니다.

수동 매핑의 경우 복원하기 전에 이미 새 시스템이 제대로 포맷되어 있어야 합니다. 대상 시스템은 시스템 예약 볼륨을 포함한 복구 지점의 각 볼륨에 대해 별도의 파티션이 있어야 합니다. 자세한 내용은 BMR용 URC 사용을(를) 참조하십시오.

다음 디스크 매핑 옵션 중 하나의 절차를 완료하십시오.

- BMR를 위한 자동 디스크 매핑
- BMR를 위한 수동 디스크 매핑

△ 주의: **Rapid Recovery에서는 FAT32 및 ReFS 파티션이 지원되지만, 현재는 ReFS에 드라이버 제한이 있기 때문에 전체 복원 및 BMR만 지원되므로 사용자 모드, VM 내보내기 등에서 복원이 구현됩니다. ReFS 파일 시스템이 포함된 하나 이상의 에이전트 볼륨이 Core에서 보호 중인 경우 ReFS 기본 지원이 제공되는 Window 8, Windows 8.1, Windows 10, Windows Server 2012 또는 Windows Server 2012 R2 시스템에 해당 볼륨이 설치되어야 합니다. 그렇지 않으면 기능이 제한되고 볼륨 이미지 탑재 등이 포함된 작업이 작동하지 않습니다. 이러한 발생 빈도에 해당하는 오류 메시지가 Rapid Recovery Core Console에 표시됩니다.**

△ 주의: **저장소 공간 디스크 구성의 완전 복원(Windows 8.1의 기능)은 이 릴리스에서 지원되지 않습니다. 자세한 내용은 *Dell Data Protection | Rapid Recovery 설치 및 업그레이드 가이드를 참조하십시오.***

이 작업은 Windows 시스템에 대한 미설치 복원 수행의 한 단계로, BMR용 URC 사용 프로세스의 일부입니다.

Core Console에서 Linux 시스템의 BMR를 수행하면 이 작업이 Linux 시스템용 Bare Metal Restore 수행 단계에도 포함됩니다. Linux용 Bare Metal Restore 실행 프로세스의 일부입니다.

BMR를 위한 자동 디스크 매핑

이 절차를 수행하면 시스템 복원 마법사를 사용하여 BMR(Bare Metal Restore) 동안 디스크를 자동으로 매핑할 수 있습니다.

복구하려는 볼륨과 이 볼륨을 복원할 위치를 자동으로 선택하려면 다음 단계를 완료하십시오.

1 시스템 복원 마법사의 디스크 매핑 페이지에서 볼륨 매핑 옆에 있는 드롭다운 메뉴의 **자동**을 선택합니다.
2 왼쪽 표에서 해당 볼륨이 나열되어 있고 선택되어 있는지 확인합니다.

ⓘ **노트: 일반적으로 BMR의 경우 최소한 시스템 예약 볼륨과 시스템 볼륨을 복원해야 합니다(대부분 C:\ 볼륨). BMR를 수행할 하나 이상의 볼륨을 선택해야 합니다.**

3 오른쪽 표에서 대상 시스템에 볼륨을 매핑하려는 디스크를 선택합니다.

4 **다음**을 클릭합니다.
5 디스크 매핑 미리보기 페이지에서, 복원할 복구 지점 볼륨과 대상 볼륨의 매핑을 검토합니다.
6 복원을 시작하려면 **마침**을 클릭합니다.

주의: 복원 시작을 선택하면 대상 드라이브에 있는 기존의 모든 파티션과 데이터가 영구적으로 제거되며, 운영 체제 및 모든 데이터를 비롯하여 선택한 복구 지점의 내용으로 대체됩니다.

BMR를 위한 수동 디스크 매핑

이 절차는 복원되는 시스템의 위치에 저장해야 할 디스크를 지정하는 방법을 설명합니다.

디스크를 수동으로 매핑하려면 먼저 대상 볼륨을 생성 및 포맷하기 위해 BMR 대상 시스템의 명령줄에서 DiskPart를 사용해야 합니다. 자세한 내용은 Microsoft Developer Network의 DiskPart 명령줄 옵션(Standard 7 SP1)을 참조하십시오.

복구하려는 볼륨과 이 볼륨을 복원할 위치를 수동으로 선택하려면 다음 단계를 완료하십시오.

1 시스템 복원 마법사의 디스크 매핑 페이지에서 볼륨 매핑 옆에 있는 드롭다운 메뉴의 **수동**을 선택합니다.

노트: BMR(Bare Metal Restore)을 수행 중인 시스템의 드라이브에 볼륨이 존재하지 않으면 이 옵션을 보거나 수동으로 볼륨을 매핑할 수 없습니다.

2 볼륨 매핑 영역의 소스 볼륨 아래에서 소스 볼륨이 선택되었는지, 해당 볼륨이 그 아래 나열되고 선택되었는지 확인합니다.
3 대상 아래 드롭다운 메뉴에서, 선택한 복구 지점의 BMR을 수행할 대상 볼륨에 해당하는 적절한 대상을 선택한 다음 **복원**을 클릭합니다.
4 확인 대화 상자에서 복구 지점의 소스와 복원할 대상 볼륨의 매핑을 검토합니다.
5 복원을 시작하려면 **복원 시작**을 클릭합니다.

주의: 복원 시작을 선택하는 경우, 대상 드라이브의 모든 기존 파티션 및 데이터가 영구히 제거되며 운영 체제 및 모든 데이터를 포함하여 선택한 복구 지점의 내용으로 변경됩니다.

아카이브에서 BMR 수행

Rapid Recovery를 사용하면 보관된 복구 지점을 사용하여 운영 체제 미설치 상태에서 시스템을 복원할 수 있습니다.

다음 작업은 다음 절차의 전제 조건입니다.

- 부팅 CD ISO 이미지 만들기
- 부트 CD 로드 및 대상 시스템 시작

URC(Universal Recovery Console)에서 사용자가 Rapid Recovery Core에 액세스할 수 있고 복원할 복구 지점을 검색할 수 있습니다. 또는, 아카이브에 저장된 복구 지점에서 운영 체제 미설치 시스템을 복원할 수 있어도 됩니다. URC를 사용하면 이 아카이브가 로컬 드라이브, 네트워크 공유 또는 클라우드 계정 중 어디에 있더라도 이에 액세스할 수 있습니다.

1 URC에서 **아카이브에서 복원** 탭을 클릭합니다.
2 **위치 유형** 드롭다운 목록에서 아카이브 위치를 선택합니다. 다음 옵션 중에서 선택할 수 있습니다.
   - 로컬
   - 네트워크
   - 클라우드
3 위치 유형 선택에 따라 다음 표에 설명되어 있는 자격 증명을 입력합니다.

표 158. 위치 유형 자격 증명 옵션

위치 유형	옵션	설명
로컬	로컬 경로	아카이브의 현재 위치.
네트워크	네트워크 경로	아카이브의 현재 위치.
	사용자	네트워크 공유 액세스의 사용자 이름.
	암호	네트워크 공유 액세스의 암호.
클라우드	클라우드 유형	클라우드 저장소 위치의 공급자. 다음 옵션을 선택합니다. • Microsoft Azure • Amazon™ S3 • OpenStack 제공 • Rackspace® 클라우드 파일

4 클라우드 유형을 선택한 경우, 클라우드 공급자와 관련된 자격 증명을 완료합니다.

- Microsoft Azure의 경우 다음과 같은 단계를 완료합니다.
  1 다음 명령을 입력합니다.
    - 저장소 계정 이름
    - 액세스 키
  2 컨테이너 이름은 드롭다운 목록에서 컨테이너를 선택합니다.
  3 클라우드 경로는 드롭다운 목록에서 아카이브에 대한 경로를 선택합니다.
- Amazon™ S3의 경우 다음 단계를 완료합니다.
  1 다음 명령을 입력합니다.
    - 액세스 키
    - 비밀 키
  2 컨테이너 이름은 드롭다운 목록에서 컨테이너를 선택합니다.
  3 클라우드 경로는 드롭다운 목록에서 아카이브에 대한 경로를 선택합니다.
- Powered by OpenStack 또는 Rackspace 클라우드 파일 계정의 경우 다음 단계를 완료합니다.
  1 다음 정보를 입력합니다.
    - Region(지역)
    - 사용자
  2 다음 옵션 중 하나를 선택합니다.
    - 암호
    - API 키
  3 텍스트 상자에, C단계에서 선택한 내용에 따라 정보를 입력합니다.
  4 다음 정보를 입력합니다.
    - 테넌트 ID
    - 인증 URL
    - 컨테이너 이름
    - 클라우드 경로

5 **다음**을 클릭합니다.

6 **시스템** 페이지에서 복원하려는 시스템을 선택한 후 **다음**을 클릭합니다.

7 **복구 지점** 페이지에서 시스템을 복원하는 데 사용하려는 복구 지점을 선택한 후 **다음**을 클릭합니다.

8 **매핑** 페이지에서 다음 옵션 중 하나를 선택한 다음, 해당 단계를 완료합니다.

- **볼륨 매핑** 드롭다운 목록에서 **자동**을 선택합니다.
  1 왼쪽 표에서 해당 볼륨이 나열되어 있고 선택되어 있는지 확인합니다.

노트: 일반적으로 BMR의 경우 최소한 시스템 예약 볼륨과 시스템 볼륨을 복원해야 합니다(대부분 C:\ 볼륨). BMR를 수행할 하나 이상의 볼륨을 선택해야 합니다.

2 오른쪽 표에서 대상 시스템에 볼륨을 매핑하려는 디스크를 선택합니다.

- **볼륨 매핑** 드롭다운에서 **수동**을 선택합니다.

  노트: 디스크를 수동으로 매핑하려면 먼저 대상 볼륨을 생성 및 포맷하기 위해 명령줄에서 DiskPart를 사용해야 합니다. 자세한 내용은 Microsoft Developer Network의 DiskPart 명령줄 옵션(Standard 7 SP1)을(를) 참조하십시오.

  노트: BMR(Bare Metal Restore)을 수행 중인 시스템의 드라이브에 볼륨이 존재하지 않으면 이 옵션을 보거나 수동으로 볼륨을 매핑할 수 없습니다.

  - **대상 볼륨** 아래의 드롭다운 메뉴에서 복구 지점의 각 볼륨에 대해 적절한 대상 볼륨을 선택합니다.

9 **마운트 맵 경로** 텍스트 상자에서 매핑 파일의 임시 저장소에 대한 대상을 입력합니다.

기본 위치는 X:\ProgramData\AppRecovery\IndexEntriesMaps입니다.

노트: 대상에 여유 공간이 충분한지 확인하려면 총 마운트 볼륨 용량을 1,024로 나눕니다. 예를 들어, 수식 `(Mount volume total capacity) / 1024 = Free space`를 사용한 다음, `1 TB / 1024 = 1 GB`를 사용합니다.

10 **복원**을 클릭합니다.

URC가 볼륨을 새 디스크에 매핑합니다.

11 **복원**을 클릭합니다.

URC가 데이터를 대상 시스템에 복원합니다. **복원 진행 상태** 탭에서 진행 상태를 볼 수 있습니다.

12 복원이 완료되면 부트 CD를 꺼냅니다.

13 BMR 대상 시스템을 Windows로 부팅하려면 시스템을 다시 시작합니다.

운영 체제에 드라이버 로딩

이 절차는 BMR(Bare Metal Restore) 대상의 운영 체제에 드라이버를 로드하는 방법을 설명합니다.

운영 체제에 드라이버를 삽입하려면 사전에 다음 작업이 완료되어야 합니다.

- Rapid Recovery Core Console에서 부팅 CD 작성기를 사용하여 부팅 CD가 생성되어야 합니다. 자세한 내용은 부팅 CD ISO 이미지 만들기을(를) 참조하십시오.
- BMR 대상에 부팅 CD를 로드해야 합니다. 자세한 내용은 부트 CD 로드 및 대상 시스템 시작을(를) 참조하십시오.
- 저장소와 네트워킹에 필요한 드라이버 또는 컨트롤러를 로드해야 합니다. 자세한 내용은 Universal Recovery Console을 사용하여 드라이버 로드을(를) 참조하십시오.
- Rapid Recovery Core Console의 시스템 복원 마법사를 사용하거나 URC(Universal Recovery Console)에서 아카이브를 사용하여 복원이 수행되어야 합니다. 자세한 내용은 시스템 복원 마법사를 사용하여 Bare Metal Restore 복원 수행 및 아카이브에서 BMR 수행을(를) 참조하십시오.

복원을 수행한 후 BMR(Bare Metal Restore) 대상의 운영 체제에 드라이버를 삽입해야 비로소 이 프로세스가 완료됩니다. 이 외에도 다음과 같이 URC에서 드라이버를 로드할 수 있습니다.

1 선택한 BMR 절차에서 복원을 클릭한 후(필수 조건 참조), **기존 Windows 드라이버 관리** 탭을 클릭합니다.

2 드롭다운 목록에서 운영 체제를 선택합니다.

URC에서 사용 가능한 드라이버를 검색합니다.

3 추가 드라이버를 로드하려면, **로드 수행**을 클릭합니다.

4 파일 정리 시스템을 탐색하여 압축된 드라이버 파일을 찾은 후 파일을 선택합니다.

5 **확인**을 클릭합니다.

URC에서 선택한 운영 체제에 드라이버를 로드합니다.

6 로드해야 할 각 추가 드라이버에 대해 3단계에서 5단계를 반복합니다.

7 BMR 대상 시스템을 다시 시작합니다.

BMR이 완료되었습니다. 다시 시작하는 데 문제가 있으면 부팅 문제 복구을(를) 참조하십시오.

Linux 시스템용 Bare Metal Restore 수행

Rapid Recovery에서 Linux 시스템에 대해 시스템 볼륨 복원을 포함한 BMR(Bare Metal Restore)를 수행할 수 있습니다. Linux 시스템 복원 시 부트 볼륨 복구 지점으로 롤백합니다. BMR 기능은 명령줄 `local_mount` 유틸리티 사용 및 Core Console UI에서 지원됩니다.

주의: BMR 프로세스를 시작하기 전에 복원할 Linux 시스템에 ext2 부트 파티션이 포함되지 않았는지 확인하십시오. ext2 파티션 유형이 있는 시스템에서 BMR를 수행할 경우 일반적으로 시스템이 시작되지 않는 결과가 초래됩니다. 이 경우 BMR를 수행하려면 시스템을 보호하고 백업하기 전에 모든 ext2 파티션을 ext3, ext4 또는 XFS로 변환해야 합니다.

주의: BMR 후 복원된 Linux 시스템을 처음으로 부팅할 때 Rapid Recovery는 복원된 시스템의 기본 이미지를 가져옵니다. 이 프로세스는 시스템의 데이터 양에 따라 증분 스냅숏을 작성하는 것보다 많은 시간이 걸립니다. 기본 이미지 및 증분 스냅숏에 대한 자세한 내용은 보호 일정 이해을(를) 참조하십시오.

Linux 시스템의 Bare Metal Restore를 수행하려면 다음 작업을 수행합니다.

- Linux 부트 이미지 관리. Linux Live DVD 부트 ISO 이미지는 대상 드라이브를 시작하는 데 사용되며, Universal Recovery Console에 액세스하여 Core의 백업과 통신할 수 있습니다. Linux 부트 이미지 관리을(를) 참조하십시오.
  - BMR에 대한 부팅 이미지를 얻으려면 먼저 필요한 이미지를 확인한 다음, 라이센스 포털에서 다운로드해야 합니다. Linux용 부트 ISO 이미지 정보 및 Linux용 부트 ISO 이미지 다운로드을(를) 참조하십시오.
  - 대상 Linux 시스템을 시작하기 위해 실제 미디어가 필요하면 ISO 이미지를 미디어로 전송해야 합니다. Live DVD ISO 이미지를 미디어에 저장을(를) 참조하십시오.
  - 모든 경우 부트 이미지를 대상 서버에 로드하고 부트 이미지에서 서버를 시작해야 합니다. Live DVD 로드 및 대상 시스템 시작을(를) 참조하십시오.
  - 미디어를 로드한 후에는 Rapid Recovery Core에 Linux 시스템을 연결해야 합니다. Rapid Recovery Core에서 BMR 대상에 연결을(를) 참조하십시오.
- 파티션 관리. Linux 시스템에서 BMR를 수행하기 전에 파티션을 만들거나 마운트해야 하는 경우가 있습니다. Linux 파티션 관리을(를) 참조하십시오.
  - BMR를 수행 중인 Linux 시스템은 복구 지점의 소스 볼륨과 동일한 파티션을 가져야 합니다. 필요에 따라 대상 시스템에 추가 파티션을 만들어야 합니다. 대상 드라이브에 파티션 만들기을(를) 참조하십시오.
  - 수동 BMR를 수행 중인 경우 먼저 파티션을 마운트해야 합니다. 명령줄에서 파티션 마운트을(를) 참조하십시오. 파티션을 마운트하는 단계는 명령줄에서 BMR를 수행하기 위한 프로세스에 포함됩니다. 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행을(를) 참조하십시오.

    Core Console에서 BMR에 대해 자동 파티션 만들기를 사용할 경우 파티션을 마운트할 필요가 없습니다. Rapid Recovery는 복원 중인 복구 지점에 포함된 것과 동일한 파티션을 복원합니다.
- Linux의 Bare Metal Restore 시작. Live DVD 부트 이미지에서 대상 시스템을 시작한 후 BMR를 시작할 수 있습니다. 필요한 작업은 이 작업을 Rapid Recovery 사용자 인터페이스에서 수행하는지, 아니면 local_mount 유틸리티를 사용하여 명령줄에서 수행하는 지에 따라 다릅니다. Linux용 Bare Metal Restore 실행을(를) 참조하십시오.
  - Core Console을 사용하는 경우 Core의 복구 지점에서 복원을 시작해야 합니다. 복구 지점 선택 및 BMR 시작을(를) 참조하십시오.
  - Core Console을 사용하는 경우 UI에서 볼륨을 매핑해야 합니다. 완전 복원의 디스크 매핑 방법을(를) 참조하십시오.
  - (선택 사항) 명령줄에서 복원하는 경우 screen 유틸리티를 사용하여 스크롤 기능을 개선하고 터미널 콘솔에서 명령을 볼 수 있습니다. 이 유틸리티는 기본적으로 열립니다. 닫는 경우에도 다시 시작할 수 있습니다. 자세한 내용은 Screen 유틸리티 시작을(를) 참조하십시오.
  - local_mount를 사용하는 경우 모든 작업이 명령줄에서 수행됩니다. 자세한 내용은 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행을(를) 참조하십시오.
- Bare Metal Restore 확인. Bare Metal Restore를 시작한 후 진행 상태를 확인하고 모니터링할 수 있습니다. 명령줄에서 Bare Metal Restore 확인을(를) 참조하십시오.
  - 복원 진행 상태를 모니터링할 수 있습니다. 복구 진행 상황 보기을(를) 참조하십시오.
  - 완료되면 복원된 서버를 시작할 수 있습니다. 복원된 대상 서버 시작을(를) 참조하십시오.
  - BMR 프로세스 문제 해결. Universal Recovery Console에 대한 연결 문제 해결 및 부팅 문제 복구을(를) 참조하십시오.

Linux 시스템에서 Bare Metal Restore 수행을 위한 전제 조건

Linux 시스템에서 Bare Metal Restore 수행을 시작하기 전에 다음과 같은 조건과 기준을 충족해야 합니다.

- 복원할 시스템 백업. 복원하려는 보호된 서버의 복구 지점이 있는 작동 중인 Rapid Recovery Core가 있어야 합니다.
- 복원할 하드웨어(신규 또는 기존, 비슷한 형식 또는 다른 형식). 대상 시스템은 에이전트의 설치 요구 사항을 충족해야 합니다. 자세한 내용은 Rapid Recovery 설치 및 업그레이드 안내서를 참조하십시오.
- Live DVD 부트 이미지. 부팅 가능한 Linux 버전을 포함한 Linux Live DVD ISO 이미지를 얻습니다. Dell Data Protection | Rapid Recovery License Portal(https://licenseportal.com)에서 다운로드합니다. Live DVD를 다운로드하는 데 문제가 있으면 Dell Rapid Recovery 지원에 문의합니다.
- 이미지 미디어 및 소프트웨어. 실제 미디어를 사용하는 경우 빈 CD나 DVD와 디스크 굽기 소프트웨어 또는 ISO 이미지를 만들 소프트웨어가 있어야 합니다.
- 호환 가능한 저장소 드라이버 및 네트워크 어댑터 드라이버. 다른 형식의 하드웨어로 복원하는 경우 RAID, AHCI 및 대상 운영 체제용 칩셋 드라이버를 비롯한 대상 시스템용 호환 저장소 드라이버와 네트워크 어댑터 드라이버가 있어야 합니다(해당되는 경우).
- 저장 공간 및 파티션(해당하는 경우). 하드 드라이브에 소스 볼륨을 포함할 대상 시스템의 대상 파티션을 만들기에 충분한 공간이 있는지 확인합니다. 모든 대상 파티션은 최소한 원래 소스 파티션보다 커야 합니다.
- 경로를 복원합니다. 복원 경로(장치 파일 설명자의 경로)를 식별합니다. 장치 파일 설명자의 경로를 식별하려면 터미널 창에서 `fdisk` 명령을 사용합니다.

Linux 부트 이미지 관리

Linux의 BMR(Bare Metal Restore)을 사용하려면 Live DVD 부트 이미지가 필요하며 Dell Data Protection | Rapid Recovery License Portal에서 다운로드할 수 있습니다. 이 이미지를 사용하여 대상 Linux 시스템을 시작합니다. 사용자 환경에 따라 이 이미지를 CD 또는 DVD와 같은 실제 미디어로 전송해야 할 수도 있습니다. 그런 다음 가상으로 또는 실제로 부트 이미지를 로드하고 부트 이미지에서 Linux 서버를 시작합니다.

노트: Live DVD는 이전에 Live CD로 알려졌었습니다.

Linux 부트 이미지 관리는 Linux 시스템용 Bare Metal Restore 수행의 한 단계입니다.

다음 작업을 수행할 수 있습니다.

Linux용 부트 ISO 이미지 정보

Linux 시스템에 대해 BMR(Bare Metal Restore)를 수행하는 첫 번째 단계는 Dell Data Protection | Rapid Recovery License Portal에서 Linux Live DVD ISO 이미지를 다운로드하는 것입니다. Live DVD는 Rapid Recovery에서 지원되는 모든 Linux 파일 시스템에서 작동하며, 부팅 가능한 Linux 버전, Screen 유틸리티 및 Rapid Recovery URC(Universal Recovery Console) 인터페이스를 포함합니다. Rapid Recovery Universal Recovery Console은 Rapid Recovery Core에서 직접 시스템 드라이브나 전체 서버를 복원하는 데 사용되는 환경입니다.

노트: ISO(International Organization for Standardization)는 파일 시스템 기준을 설정하는 여러 국가 기관 대표자들의 국제단체입니다. ISO 9660은 데이터 교환용 광 디스크 미디어에 사용되는 파일 시스템 표준으로, 다양한 운영 체제를 지원합니다. ISO 이미지는 디스크의 모든 섹터는 물론 디스크 파일 시스템의 데이터가 포함된 아카이브 파일 또는 디스크 이미지입니다.

Linux용 부트 ISO 이미지 다운로드

자신의 Rapid Recovery 버전과 일치하는 Live DVD ISO 이미지를 다운로드해야 합니다. 현재 버전의 Live DVD는 Dell Data Protection | Rapid Recovery License Portal(https://licenseportal.com)에서 제공됩니다. 다른 버전이 필요하면 Dell Rapid Recovery 지원에 문의하십시오.

노트: Dell Data Protection | Rapid Recovery License Portal에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery License Portal License Portal 사용 설명서를 참조하십시오.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, Linux 부트 이미지 관리 프로세스의 일부입니다.

Live DVD ISO 이미지를 다운로드하려면 다음 단계를 완료하십시오.

1 Dell Data Protection | Rapid Recovery License Portal(https://licenseportal.com)에 로그인합니다.
2 다운로드 영역에 액세스합니다.
3 Linux 기반 응용프로그램으로 스크롤하고 Linux Live DVD 섹션에서 **다운로드**를 클릭합니다.
4 Live DVD ISO 이미지를 저장합니다. 가상 시스템을 복원하는 경우 네트워크 위치에 저장하고 ISO 이미지와 연관된 CD 또는 DVD 드라이브에서 시작하도록 VM을 설정할 수 있습니다.
5 실제 시스템에서 복원하는 경우 부트 CD ISO 이미지를 대상 시스템을 시작할 수 있는 CD 또는 DVD에 굽습니다. 자세한 내용은 Live DVD ISO 이미지를 미디어에 저장을(를) 참조하십시오.

Live DVD ISO 이미지를 미디어에 저장

Linux Live DVD 파일을 다운로드하면 지정한 경로에 ISO 이미지로 저장됩니다. Live DVD 이미지에서 대상 Linux 시스템을 부팅할 수 있어야 합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, Linux 부트 이미지 관리 프로세스의 일부입니다.

부트 CD ISO 이미지를 CD 또는 DVD에 굽습니다.

가상 시스템에서 BMR를 수행하는 경우에는 이 단계가 필요하지 않습니다. ISO 이미지를 드라이브에 로드하고 해당 VM에 대한 시스템 설정을 편집하여 해당 드라이브에서 시작합니다. 가상 내보내기를 사용하여 Linux VM을 복원할 수도 있습니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.

Live DVD 로드 및 대상 시스템 시작

Live DVD ISO 이미지를 얻은 후에는 새로 만든 Live DVD에서 Linux 시스템을 시작해야 합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계입니다. Linux 부트 이미지 관리 프로세스의 일부입니다.

1 새 서버로 이동하여 해당 위치에서 Live DVD 이미지를 로드합니다. 서버가 Live DVD 이미지에서 시작되도록 지정합니다.
2 시스템을 시작합니다.

Rapid Recovery 시작 화면이 나타나고 시스템의 IP 주소와 인증 암호가 표시된 터미널 창이 열립니다.

노트: Live DVD 이미지로 시스템을 시작할 때마다 새 임시 암호가 생성됩니다.

3 소개 화면에 표시된 IP 주소와 인증 암호를 기록해 둡니다. 나중에 데이터 복구 프로세스 동안 콘솔에 다시 기록하기 위해 이 정보가 필요합니다.

Rapid Recovery Core에서 BMR 대상에 연결

Live DVD로 대상 Linux 시스템을 시작하면 Core에서 이 시스템에 연결하여 Bare Metal Restore 프로세스를 시작할 준비가 됩니다. 다음 두 가지 방법 중 하나를 사용하여 이 프로세스를 수행할 수 있습니다.

- Rapid Recovery Core Console에서 복원을 시작합니다. 자세한 내용은 Linux용 Bare Metal Restore 실행을(를) 참조하십시오.
- aamount 유틸리티를 사용하여 명령줄에서 복원 시작. 자세한 내용은 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행을(를) 참조하십시오.

Linux 파티션 관리

BMR 수행 시 데이터를 복원할 대상 드라이브에 복원 중인 복구 지점과 동일한 파티션이 있어야 합니다. 이 요구 사항을 충족하도록 파티션을 만들어야 할 수도 있습니다.

aamount 유틸리티를 사용하여 명령줄에서 복원을 시작하거나 Rapid Recovery Core Console에서 복원을 시작할 수 있습니다. 사용자 인터페이스를 사용하여 복원하는 경우 먼저 파티션을 마운트해야 합니다.

Linux 파티션 관리는 Linux 시스템용 Bare Metal Restore 수행의 한 단계입니다.

다음 작업을 수행할 수 있습니다.

관련 링크

대상 드라이브에 파티션 만들기
대상 드라이브에서 파티션 포맷
명령줄에서 파티션 마운트

대상 드라이브에 파티션 만들기

종종 BMR 수행 시 대상 드라이브가 단일 파티션으로 구성될 수 있는 새 볼륨입니다. 대상 시스템의 드라이브에 볼륨 크기를 포함하여 복구 지점과 동일한 파티션 테이블이 있어야 합니다. 대상 드라이브에 동일한 파티션이 없으면 Bare Metal Restore를 수행하기 전에 해당 파티션을 만들어야 합니다. fdisk 유틸리티를 사용하여 대상 드라이브에 소스 드라이브의 파티션과 동일한 파티션을 만듭니다.

주의: 아래 절차는 예일 뿐입니다. 고객 환경은 이와 다를 수 있습니다. 환경의 특성에 맞춰 사용하는 명령을 변경해야 합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, Linux 파티션 관리 프로세스의 일부입니다.

1 (선택 사항) Screen 유틸리티를 사용할 수 있습니다. 이 유틸리티는 기본적으로 시작되며, 시스템을 재부팅할 때까지 활성 상태로 유지됩니다.

노트: 명시적으로 이를 닫았다가 다시 열려면 Screen 유틸리티 시작을(를) 참조하십시오.

2 명령줄에서 다음 명령을 입력한 후 **Enter** 키를 눌러 관리자로 실행하도록 권한을 변경하고 기존 디스크 파티션을 나열합니다.

```
sudo fdisk -l
```

모든 볼륨 목록이 나타납니다.

이 예에서는 파티션을 만들려는 볼륨이 /dev/sda라고 가정합니다. 볼륨이 다른 경우(예를 들어, 이전 드라이브의 경우 /dev/hda로 나타날 수 있음) 그에 따라 명령을 변경합니다.

3 새 부트 파티션을 만들려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
sudo fdisk /dev/sda
```

4 새 부트 파티션을 만들려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
n
```

5 새 기본 파티션을 만들려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
p
```

6 파티션 번호를 지정하려면 파티션 번호를 입력한 다음 **Enter** 키를 누릅니다. 예를 들어, 파티션 1을 지정하려면 1을 입력한 다음 **Enter** 키를 누릅니다.

7 첫 번째 섹터 2048을 사용하려면 **Enter** 키를 누릅니다.

8 + 기호와 할당량을 입력하여 부트 파티션에 해당 수량을 할당한 다음 **Enter** 키를 누릅니다.

예를 들어, 부트 파티션에 500M를 할당하려면 다음을 입력한 후 **Enter** 키를 누릅니다.

```
+512000K
```

9 부트 파티션에 대해 부팅 가능 플래그를 전환하려면(파티션을 부팅 가능으로 만들려면) 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
a
```

10 해당 파티션에 부팅 가능 플래그를 할당하려면 파티션 번호를 입력한 다음 **Enter** 키를 누릅니다. 예를 들어, 파티션 1에 부팅 가능 플래그를 할당하려면 1을 입력한 다음 **Enter** 키를 누릅니다.

11 필요한 경우 계속하여 디스크의 파티션을 만듭니다.

12 fdisk 유틸리티에서 모든 변경 사항을 저장하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
w
```

대상 드라이브에서 파티션 포맷

대상 드라이브의 새 볼륨에 파티션을 생성하여 Bare Metal Restore를 수행한 후에는 자동 파티션을 사용하지 않는 경우 파티션을 포맷해야 이를 마운트할 수 있습니다. 이 상황에 해당되면 이 절차에 따라 ext3, ext4 또는 XFS 형식으로 파티션을 포맷하십시오.

이 상황에 해당되지 않으면 이 항목에 설명되어 있는 대로 파티션을 포맷하지 않아도 됩니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, Linux 파티션 관리 프로세스의 일부입니다.

1 (선택 사항) Screen 유틸리티를 사용할 수 있습니다. 이 유틸리티는 기본적으로 시작되며, 시스템을 재부팅할 때까지 활성 상태로 유지됩니다.

노트: 명시적으로 이를 닫았다가 다시 열려면 Screen 유틸리티 시작을(를) 참조하십시오.

2 명령줄에서 다음 명령을 입력한 후 **Enter** 키를 눌러 관리자로 실행하도록 권한을 변경하고 기존 디스크 파티션을 나열합니다.

```
sudo fdisk -l
```

모든 볼륨 목록이 나타납니다.

이 예에서는 포맷하려는 파티션이 /dev/sda1이라고 가정합니다. 볼륨이 다른 경우(예를 들어, 이전 드라이브의 경우 /dev/hda로 나타날 수 있음) 그에 따라 명령을 변경합니다.

3 대상 파티션에 사용할 형식을 기반으로 다음 명령 중 하나를 선택합니다.

- ext3 형식으로 파티션을 포맷하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
sudo mkfs.ext3 /dev/sda1
```

- ext4 형식으로 파티션을 포맷하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
sudo mkfs.ext4 /dev/sda1
```

- XFS 형식으로 파티션을 포맷하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
sudo mkfs.xfs /dev/sda1
```

선택한 파티션이 적절하게 포맷됩니다.

4 선택 사항으로, 다른 파티션을 포맷해야 할 경우 이 절차를 반복하십시오.

명령줄에서 파티션 마운트

Rapid Recovery Core Console을 사용하여 BMR를 수행하는 경우, 먼저 대상 시스템에서 해당 파티션을 마운트해야 합니다. Universal Recovery Console의 명령줄에서 이 작업을 수행합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, Linux 파티션 관리 프로세스의 일부입니다.

복원을 수행하기 전에 Linux 시스템에서 파티션을 마운트하려면 다음 단계를 완료하십시오.

1 명령줄에서 다음 명령을 입력한 후 **Enter** 키를 눌러 관리자로 실행하도록 권한을 변경하고 기존 디스크 파티션을 나열합니다.

```
sudo fdisk -l
```

모든 볼륨 목록이 나타납니다.

2 BMR을 수행해야 하는 모든 파티션을 마운트 디렉터리로 포맷합니다. 이들은 복구 지점에 있는 볼륨과 일치해야 합니다. 예를 들어, 마운트할 볼륨이 sda1이고 마운트 디렉터리가 mnt인 경우 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

3 BMR를 수행해야 하는 모든 파티션을 마운트 디렉터리로 마운트합니다. 이들은 복구 지점에 있는 볼륨과 일치해야 합니다. 예를 들어, 마운트할 볼륨이 sda1이고 마운트 디렉터리가 mnt인 경우 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
mount /dev/sda1 /mnt
```

4 필요에 따라 모든 필요한 볼륨을 마운트할 때까지 3단계를 반복합니다.

볼륨이 마운트되면 Rapid Recovery Core Console에서 대상 Linux 시스템으로 복원을 수행할 수 있습니다. Linux용 Bare Metal Restore 실행을(를) 참조하십시오.

Linux용 Bare Metal Restore 실행

Linux 시스템의 BMR(Bare Metal Restore)을 실행하려면 다음과 같은 필수 조건을 충족해야 합니다.

- Core에 저장된 복구 지점을 복원하려면 적절한 하드웨어가 설치되어 있어야 합니다. 자세한 내용은 Linux 시스템에서 Bare Metal Restore 수행을 위한 전제 조건을(를) 참조하십시오.
- BMR 대상 Linux 시스템이 Live DVD 부트 이미지를 사용하여 시작되어야 합니다. 자세한 내용은 Linux 부트 이미지 관리을(를) 참조하십시오.

- 복원할 Linux 시스템의 볼륨 수가 복구 지점의 볼륨 수와 일치해야 합니다. 또한 Rapid Recovery Core Console에서 복원할지, 아니면 local_mount를 사용하여 명령줄에서 복원할지 결정해야 합니다. 자세한 내용은 Linux 파티션 관리을(를) 참조하십시오.
- Core Console UI에서 복원하는 경우 BMR를 시작하는 첫 번째 단계는 적합한 복구 지점을 선택한 다음 Universal Recovery Console에서 얻은 IP 주소와 임시 암호를 지정하여 하드웨어로 복원을 시작하는 것입니다. 그런 다음 드라이브를 매핑하고 복원을 시작해야 합니다.

이 프로세스는 Linux 시스템용 Bare Metal Restore 수행의 한 단계입니다.

Rapid Recovery Core Console에서 BMR를 실행하려면 다음 작업을 수행하십시오.

- 복구 지점 선택 및 BMR 시작
- 완전 복원의 디스크 매핑 방법

local_mount 유틸리티를 사용하여 명령줄에서 복원하는 경우, 먼저 해당 권한을 설정하고, 볼륨을 마운트하고, local_mount를 실행하고, 시스템 목록에서 Core에 대한 정보를 얻고, Core에 연결하고, 복구 지점 목록을 얻고, Bare Metal로 롤백할 복구 지점을 선택하고, 복원을 시작해야 합니다.

(선택 사항) Screen 유틸리티를 시작할 수 있습니다.

명령줄에서 BMR를 실행하려면 다음 작업을 수행합니다.

- Screen 유틸리티 시작
- 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행

Screen 유틸리티 시작

Screen 유틸리티는 Live DVD에 포함되어 있으며 Live DVD에서 Universal Recovery Console로 부팅할 때 사용할 수 있습니다. 사용자는 Screen 유틸리티를 통해 SSH(Single Secure Shell) 세션 또는 콘솔 창에서 여러 셸을 동시에 관리할 수 있습니다. 따라서 터미널 창에서 한 작업(마운트된 볼륨 확인 등)을 수행하고 해당 작업이 실행 중인 동안 다른 셸 인스턴스를 열거나 해당 인스턴스로 전환하여 다른 작업(local_mount 유틸리티 실행 등)을 수행할 수 있습니다.

또한 screen 유틸리티는 자체 스크롤백 버퍼를 갖고 있어서 화면을 스크롤하여 복구 지점 목록 등 더 큰 데이터를 볼 수 있습니다.

노트: Screen 유틸리티는 편의를 위해 제공되는 것이므로 이 유틸리티 사용은 선택 사항입니다.

Screen 유틸리티는 기본적으로 Live DVD로 부팅된 시스템에서 시작합니다. 그러나 이 응용프로그램을 닫았으면 다음 절차에 따라 Live DVD에서 Screen 유틸리티를 시작해야 합니다.

시스템을 Live DVD에서 부팅했으면 터미널 창에서 screen을 입력하고 **Enter** 키를 누릅니다.
Screen 유틸리티가 시작됩니다.

명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행

BMR를 수행하려는 시스템에서 Live DVD ISO 이미지에 액세스할 수 있고 대상 시스템과 Bare Metal Restore를 수행할 복구 지점 간에 볼륨 수와 크기가 일치하면 local_mount 유틸리티를 사용하여 명령줄에서 복원을 시작할 수 있습니다.

노트: 이 구성 요소는 이전의 `aamount`입니다.

Rapid Recovery Core Console UI를 사용하여 BMR를 수행하려면 복구 지점 선택 및 BMR 시작을(를) 참조하십시오.

노트: 이 절차를 수행하는 경우 복구 지점을 apidrecovery-vdisk(이전 aavdisk) 파일이 포함된 /tmp 폴더로 탑재하려고 하지 마십시오.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, 명령줄을 사용하여 Linux 시스템용 Bare Metal Restore 실행 프로세스의 일부입니다.

물리적 또는 가상 BMR 대상 시스템으로 롤백할 Core의 복구 지점을 선택하려면 다음 단계를 완료하십시오.

1 Rapid Recovery local_mount 유틸리티를 루트로 실행하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
sudo local_mount
```

2 보호된 시스템을 나열하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
lm
```

3 프롬프트가 나타나면 다음 표의 설명에 따라 Rapid Recovery Core의 연결 정보를 입력하고 필요한 명령을 입력한 후 Enter 키를 누릅니다.

표 159. Rapid Recovery Core 연결 정보

텍스트 상자	설명	필수
Rapid Recovery Core IP 주소 또는 호스트 이름	Rapid Recovery Core의 IP 주소 또는 호스트 이름.	예
도메인	Rapid Recovery Core의 도메인. 이 항목은 선택 사항입니다.	아니요
사용자	Core에서 관리자 권한을 가진 사용자 이름	예
암호	관리자 권한을 가진 사용자가 Core에 연결하는 데 사용되는 암호.	예

이 Rapid Recovery Core에서 보호되는 시스템을 표시하는 목록이 나타납니다. 시스템의 라인 항목 번호, 호스트 표시 이름 또는 IP 주소, ID 번호로 찾은 시스템이 나열됩니다.

4 복원하려는 시스템의 복구 지점을 나열하려면 다음 구문을 사용하여 복구 지점 나열 명령을 입력한 후 **Enter** 키를 누릅니다.

```
lr <machine_line_item_number>
```

노트: 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템의 기본 및 증분 복구 지점이 목록에 표시됩니다. 이 목록에는 다음 정보가 포함됩니다.

- 라인 항목 번호
- 날짜 및 시간 스탬프
- 복구 지점 내의 문자화된 볼륨 목록
- 볼륨 위치
- 복구 지점 크기
- 복구 지점을 식별하는 일련 번호가 끝에 있는 볼륨의 ID 번호

5 복원할 복구 지점을 선택하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
r <recovery_point_ID_number> <path>
```

주의: 시스템 볼륨이 마운트되지 않아야 합니다.

노트: Live DVD에서 시스템을 시작한 경우 시스템 볼륨이 마운트되지 않습니다.

이 명령은 Core에서 ID로 지정된 볼륨 이미지를 지정된 경로로 롤백합니다. 복원 경로는 장치 파일 설명자의 경로이고 해당 항목이 마운트되는 디렉터리가 아닙니다.

노트: 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 나타낼 수도 있습니다. 이 경우 에이전트/시스템 라인 번호(lm 출력에서), 복구 지점 라인 번호 및 볼륨 문자(복구 지점 내의 문자화된 볼륨 목록에서), 경로를 차례로 사용합니다. 예:

```
r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>
```

예를 들어, 다음을 입력합니다.

```
r 1 24 a /dev/sda1
```

이 명령에서, <path>는 실제 볼륨에 대한 파일 설명자입니다.

6 계속할지 묻는 메시지가 나타나면 y(예)를 입력한 다음 **Enter** 키를 누릅니다.
복원이 시작된 후에는 복원 완료 상태를 알려주는 일련의 메시지가 나타납니다.

노트: 예외 메시지가 나타나는 경우 local_mount.log 파일에서 해당 예외와 관련된 세부 정보를 찾을 수 있습니다. local_mount.log 파일은 /var/log/apprecovery에 있습니다.

7 복원에 성공하면 `exit`를 입력하여 local_mount를 종료한 다음 **Enter** 키를 누릅니다.

8 다음 단계는 복원을 확인하는 것입니다. 자세한 내용은 명령줄에서 Bare Metal Restore 확인을(를) 참조하십시오.

명령줄을 사용하여 Linux 시스템의 볼륨 복원

Rapid Recovery에서 명령줄 `local_mount` 유틸리티를 사용하여 보호된 Linux 시스템의 볼륨을 복원할 수 있습니다.

노트: 이 프로세스는 이전에 *롤백*이라고 불렀습니다. 이 절차를 수행하는 경우 복구 지점을 apidrecovery-vdisk(이전 aavdisk) 파일이 포함된 /tmp 폴더로 탑재하려고 하지 마십시오. Rapid Recovery Core Console의 보호된 시스템에 대한 볼륨 복원도 지원됩니다. 자세한 내용은 복구 지점에서 볼륨 복원를 참조하십시오.

주의: 시스템이나 루트(/) 파티션 또는 전체 운영 체제를 복원하려면 Linux 시스템용 Bare Metal Restore 수행을 참조하십시오.

1 Rapid Recovery `local_mount` 유틸리티를 루트로 실행합니다. 예를 들어, 다음과 같습니다.

```
sudo local_mount
```

2 Rapid Recovery 탑재 프롬프트에 다음 명령을 입력하여 보호된 시스템을 나열합니다.

```
lm
```

3 메시지가 표시되면 Rapid Recovery Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.

4 이 서버의 로그온 자격 증명 즉, 사용자 이름과 암호를 입력합니다.
이 Rapid Recovery 서버에서 보호되는 시스템을 표시하는 목록이 나타납니다. 이 목록에는 라인 항목 번호, 호스트/IP 주소 및 시스템의 ID 번호별로 보호된 시스템이 나열됩니다(예: 7d658e5f-fa08-4600-95f0-5f486bc1b6a4#de0896fd-571a-4cc5-aeed-264d2c3c72f4#f377e145-dd4d-3ac3-5b15-37ce8f4913ba:2).

5 다음 명령을 입력하여 현재 지정된 시스템에 대해 마운트된 복구 지점을 나열합니다.

```
lr <machine_line_item_number>
```

노트: 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템의 기본 및 증분 복구 지점을 보여주는 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 날짜/타임스탬프, 볼륨 위치, 복구 지점의 크기 및 끝에 복구 지점을 나타내는 시퀀스 번호가 포함된 볼륨의 ID 번호(예: "293cc667-44b4-48ab-91d8-44bc74252a4f:2")가 포함됩니다.

6 다음 명령을 입력하여 복원할 복구 지점을 선택합니다.

```
r <volume_recovery_point_ID_number> <device path>
```

이 명령은 Core에서 ID로 지정된 볼륨 이미지를 지정된 경로로 복원합니다. 복원 경로는 장치 파일 설명자의 경로이고 해당 항목이 탑재되는 디렉터리가 아닙니다.

- 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 나타낼 수도 있습니다. 이 경우 보호된 시스템 라인 번호(lm 출력에서), 복구 지점 라인 번호 및 볼륨 문자, 경로를 차례로 사용합니다(예: r <machine_line_item_number> <recovery_point_line_number> <volume_letter> <path>). 이 명령에서 <path>는 실제 볼륨의 파일 설명자입니다.

  예를 들어, `lm` 출력에 세 개의 보호된 시스템이 나열되고 `lr` 명령을 보호된 시스템 번호 2에 대해 입력하며 `e23` 복구 지점 볼륨 `b`를 디렉터리 `/dev/sda5`,에 탑재되었던 볼륨으로 복원하려는 경우 명령은 다음과 같습니다.

  ```
  r2 23 b /dev/sda5
  ```

  노트: 필요한 경우 /로 복원할 수 있습니다. Live DVD를 사용하여 Bare Metal Restore를 수행할 경우 사용자가 다른 시스템으로 복원하려는 것으로 간주됩니다. 자세한 내용은 Linux용 Bare Metal Restore 실행을(를) 참조하십시오.

7 계속 진행할지 묻는 메시지가 나타나면 예를 의미하는 `y`를 입력합니다.

복원이 진행되면 상태를 알려주는 일련의 메시지가 나타납니다.

8 복원이 성공하면 대상이 이전에 보호되고 마운트된 경우 `local_mount` 유틸리티가 자동으로 커널 모듈을 마운트하고 복원된 볼륨에 다시 연결합니다. 그렇지 않은 경우, 복원된 볼륨을 로컬 디스크로 탑재한 다음 파일이 복원되는지 확인해야 합니다(예를 들어, `sudo mount` 명령을 사용한 다음 `ls` 명령을 사용할 수 있습니다).

Bare Metal Restore 확인

BMR(Bare Metal Restore)을 수행한 후 복원 진행 상황을 확인할 수 있습니다. 작업이 성공적으로 완료되면 복원된 서버를 시작할 수 있습니다. Universal Recovery Console에 연결하여 복원을 완료하는 데 문제가 발생하거나 복원된 시스템에서 시작 문제를 해결해야 할 경우 이를 위한 문제 해결 단계가 포함됩니다.

다음 작업을 수행할 수 있습니다.

관련 링크

복구 진행 상황 보기
복원된 대상 서버 시작
Universal Recovery Console에 대한 연결 문제 해결
부팅 문제 복구

복구 진행 상황 보기

Rapid Recovery Core Console에서 시작된 복구 지점의 데이터 복원(Bare Metal Restore 포함) 진행 상황을 보려면 이 절차에 있는 단계를 완료하십시오.

1 복구 지점에서 데이터를 복원하는 프로세스를 시작한 후에 작업이 진행 중인 동안 Core Console의 실행 중인 작업 드롭다운 메뉴에서 진행 상황을 볼 수 있습니다.

2 (선택 사항) 이벤트 페이지에서 세부 정보를 볼 수 있습니다. Rapid Recovery 이벤트 모니터링에 대한 자세한 내용은 작업, 경고 및 이벤트 보기를 참조하십시오.

복원된 대상 서버 시작

복원된 대상 서버를 시작하려면 다음 단계를 완료하십시오.

노트: 복원된 대상 서버를 시작하기 전에 복구에 성공했는지 확인해야 합니다. 자세한 내용은 복구 진행 상황 보기을(를) 참조하십시오.

이 작업은 Windows 시스템에 대한 미설치 복원 수행의 한 단계로, Bare Metal Restore 확인 프로세스의 일부입니다.

1 대상 서버에서 Rapid Recovery Universal Recovery Console이 활성화되어 있는지 확인합니다.

2 복원된 서버에서 부트 CD를 제거하거나 부트 CD 이미지가 있는 실제 미디어를 제거합니다.

3 Universal Recovery Console에서 화면 상단에 있는 전원 메뉴 아이콘을 클릭한 다음 **재부팅**을 클릭합니다.

4 운영 체제를 정상적으로 시작하도록 지정합니다.

5 시스템에 로그온합니다. 시스템이 복구 지점에서 캡처된 상태로 복원되어야 합니다.

Universal Recovery Console에 대한 연결 문제 해결

다음은 복구 지점 선택 및 BMR 시작 프로세스의 일부로 부트 CD 이미지에 연결 시 문제 해결 단계입니다.

Core가 원격 서버에 연결할 수 없다는 오류 메시지가 표시되는 경우 가능한 여러 가지 원인이 있을 수 있습니다.

- URC에 표시된 IP 주소와 현재 암호가 Recovery Console 인스턴스 대화 상자에 입력한 정보와 일치하는지 확인합니다.
- 데이터를 복원할 서버에 접속하려면 Core가 네트워크의 서버를 식별할 수 있어야 합니다. 서버 식별이 가능한지 알려면 Core에서 명령 프롬프트를 열고 대상 BMR 서버의 IP 주소를 ping하면 됩니다. 대상 서버에서 명령 프롬프트를 열고 Rapid Recovery Core의 IP 주소를 ping할 수도 있습니다.
- Core와 대상 BMR 서버 간에 네트워크 어댑터 설정이 호환되는지 확인합니다.

부팅 문제 복구

다음 작업은 다음 절차의 전제 조건입니다.

- 부팅 CD ISO 이미지 만들기
- 부트 CD 로드 및 대상 시스템 시작
- Universal Recovery Console을 사용하여 드라이버 로드

시작 문제를 해결하려면 다음 단계를 완료하십시오. 다른 형식의 하드웨어로 복원하는 경우 저장소 컨트롤러, RAID, AHCI, 칩셋 및 기타 드라이버가 아직 부트 CD에 없으면 해당 항목을 삽입해야 한다는 점에 주의하십시오. 이러한 드라이버가 있어야 운영 체제에서 대상 서버의 모든 장치를 성공적으로 작동할 수 있습니다. 자세한 내용은 Universal Recovery Console을 사용하여 드라이버 로드을(를) 참조하십시오. 대상 서버에서 시작 문제를 해결하려면 다음 단계를 완료하십시오.

1 Universal Recovery Console에서 **기존 Windows 드라이버 관리자** 탭을 클릭합니다.
2 **부팅 문제 복구**를 클릭합니다.
대상 서버 부트 레코드의 시작 매개 변수가 자동으로 복구됩니다.

명령줄에서 Bare Metal Restore 확인

Dell은 다음 단계를 수행하여 명령줄에서 완료된 Bare Metal Restore를 확인하도록 권장합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로,

관련 링크

복원된 볼륨에서 파일 시스템 검사 수행
명령줄을 사용하여 복원된 Linux 시스템을 부팅 가능하도록 만들기

복원된 볼륨에서 파일 시스템 검사 수행

명령줄에서 Bare Metal Restore를 실행한 후 복원된 볼륨에서 파일 시스템 검사를 수행하여 복구 지점에서 복원된 데이터가 손상되지 않았는지 확인해야 합니다.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, 명령줄에서 Bare Metal Restore 확인 프로세스의 일부입니다.

아래 작업을 수행하여 복원된 볼륨에서 파일 시스템 검사를 수행합니다.

1 복원한 Linux 시스템의 Universal Recovery Console의 명령줄에서 해당 파티션이 마운트되는지 확인하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
df
```

2 복원된 볼륨이 마운트되지 않으면 3단계로 건너뜁니다. 복원된 볼륨이 마운트되면 다음 명령을 입력하여 마운트 해제한 후 Enter 키를 누릅니다.

```
umount <mount point>
```

3 다음 명령을 입력하여 복원된 볼륨에서 파일 시스템 검사를 실행한 다음 Enter 키를 누릅니다.

```
fsck -f <volume>
```

fsck가 clean을 반환하면 파일 시스템이 확인됩니다.

4 `mount <volume> <folder>` 형식으로 다음 명령을 입력하여 해당 볼륨을 다시 한 번 마운트한 다음 **Enter** 키를 누릅니다.

예를 들어, 볼륨 경로가 prod/sda1이고 마운트하려는 폴더가 mnt인 경우 다음을 입력한 후 **Enter** 키를 누릅니다.

```
mount /dev/sda1 /mnt
```

명령줄을 사용하여 복원된 Linux 시스템을 부팅 가능하도록 만들기

복원된 볼륨에서 클린 파일 시스템 검사가 완료되면 부팅 가능한 파티션을 만들어야 합니다.

GRUB(GNU Grand Unified Bootloader)는 관리자가 시스템을 시작하는 데 사용할 운영 체제나 특정 커널 구성을 구성할 수 있는 부트 로더입니다. BMR 후에 시스템이 루트 볼륨에 대해 적합한 UUID(Universally Unique Identifier)를 사용하도록 GRUB의 구성 파일을 수정해야 합니다. 이 단계 전에 루트 및 부트 볼륨을 마운트하고 각각에 대해 UUID를 확인해야 합니다. 이렇게 하면 파티션에서 부팅할 수 있습니다.

노트: 이 절차는 GRUB1 또는 GRUB2를 사용하는 Linux 시스템에 적용됩니다. 이 절차를 사용하는 경우 부트 파티션이 정상적이고 보호되는 상태인지 확인하십시오.

일반적으로 GRUB 또는 GRUB2가 Linux 운영 체제와 함께 설치됩니다. Linux 배포 시 함께 제공되는 버전을 사용하여 이 절차를 수행할 수 있습니다. GRUB 버전이 설치되어 있지 않은 경우, Linux 배포에 맞는 기본 버전을 다시 설치해야 합니다.

주의: BMR 후 복원된 Linux 시스템을 처음으로 부팅할 때 Rapid Recovery는 복원된 시스템의 기본 이미지를 가져옵니다. 이 프로세스는 시스템의 데이터 양에 따라 증분 스냅숏을 작성하는 것보다 많은 시간이 걸립니다. 기본 이미지 및 증분 스냅숏에 대한 자세한 내용은 보호 일정 이해을(를) 참조하십시오.

이 작업은 Linux 시스템용 Bare Metal Restore 수행의 한 단계로, 명령줄에서 Bare Metal Restore 확인 프로세스의 일부입니다.

아래 작업을 수행하여 명령줄을 사용하여 부팅 가능한 파티션을 만듭니다.

1 먼저 루트 볼륨을 마운트한 다음 부트 볼륨을 마운트해야 합니다. 다음 명령을 사용하여 복원된 각 볼륨을 마운트합니다.

a 루트 볼륨을 마운트하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
mount /<restored volume[root]> /mnt
```

예를 들어, /dev/sda2가 루트 볼륨이면 mount /dev/sda2 /mnt를 입력한 후 **Enter** 키를 누릅니다.

b 부트 볼륨을 마운트하려면 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
mount /<restored volume[boot]> /mnt/boot
```

예를 들어, /dev/sda1이 부트 볼륨이면 mount /dev/sda1 /mnt/boot를 입력한 후 **Enter** 키를 누릅니다.

노트: 일부 시스템 구성은 부트 디렉터리를 루트 볼륨의 일부로 포함할 수 있습니다.

2 볼륨 크기가 증가하면 즉, 새 Linux 시스템의 대상 볼륨이 복구 지점에 있던 볼륨보다 크면 기존 비트맵 데이터 파일을 삭제해야 합니다.

3 `blkid` 명령을 사용하여 새 볼륨의 UUID(Universally Unique Identifier)를 얻습니다. 다음 명령을 입력한 후 **Enter** 키를 누릅니다.

```
blkid [volume]
```

노트: `ls -l /dev/disk/by-uuid` 명령을 사용할 수도 있습니다.

4 대상 시스템의 새 디스크에서 BMR를 수행하는 경우, 루트 볼륨의 fstab에서 스왑 파티션을 주석 처리합니다.

5 fstab 및 mtab 경로는 Live DVD가 아니라 복원된 볼륨에서 수정해야 합니다. Live DVD에서 경로를 수정할 필요가 없습니다. 다음 명령을 입력하여 GRUB(Grand Unified Bootloader) 설치를 준비합니다. 각 명령 다음에 **Enter** 키를 누릅니다.

```
mount --bind /dev /mnt/dev

mount --bind /proc /mnt/proc

mount --bind /sys /mnt/sys
```

6 다음 명령을 입력하여 루트 디렉터리를 변경한 다음 **Enter** 키를 누릅니다.

```
chroot /mnt /bin/bash
```

7 마운트된 복구 지점 `/etc/fstab` 파일에서 파티션의 기존 UUID를 얻고 다음 명령을 입력하여 루트(Ubuntu 및 CentOS), 부트(CentOS 및 RHEL) 또는 데이터 파티션의 UUID와 비교한 다음 **Enter** 키를 누릅니다.

```
less /mnt/etc/fstab
```

8 마운트된 복구 지점 `/etc/mtab` 파일에서 파티션의 기존 UUID를 얻고 다음 명령을 입력하여 루트(Ubuntu 및 CentOS), 부트(CentOS 및 RHEL) 및 데이터 파티션의 UUID와 비교한 다음 **Enter** 키를 누릅니다.

```
less /mnt/etc/mtab
```

9 SLES 11을 사용할 경우 다음 명령을 입력하고 각 명령 입력 후 Enter 키를 눌러 GRUB를 설치합니다.

```
grub-install --recheck /dev/sda

grub-install /dev/sda
```

10 Ubuntu, CentOS 6.x, RHEL 6.x 또는 Oracle Linux 6.x를 사용하는 경우, 다음 명령을 입력하여 GRUB 설치 후 Enter 키를 누릅니다.

```
grub-install /dev/sda
```

11 SLES 12, CentOS 7, RHEL 7 또는 Oracle 7을 사용하는 경우, 다음 명령을 입력하여 GRUB2 설치 후 Enter 키를 누릅니다.

```
grub2-install /dev/sda
```

12 설치를 완료한 후 다음 업데이트 중 하나를 실행합니다.

- SLES의 경우:

  ```
  grub-install.unsupported --recheck /dev/sda
  grub-install.unsupported /dev/sda
  update-grub
  ```

  노트: Linux 배포에 `update-grub` 명령이 존재하지 않으면 이 옵션을 생략하십시오.

- 다른 배포의 경우:

  ```
  grub-install /dev/sda
  update-grub
  ```

  노트: Linux 배포에 `update-grub` 명령이 존재하지 않으면 이 옵션을 생략하십시오.

13 Live DVD 디스크를 CD-ROM 또는 DVD 드라이브에서 제거하고 Linux 시스템을 재시작합니다.

6

보고서 생성 및 보기

이 섹션에서는 Rapid Recovery Core 및 Rapid Recovery Central Management Console에서 사용할 수 있는 보고 개요를 제공합니다.

주제:

- Rapid Recovery 보고서 정보
- Central Management Console

Rapid Recovery 보고서 정보

Rapid Recovery Core Console에서 보고서를 생성할 수 있습니다. 일부 보고서는 Central 관리 콘솔에서도 사용할 수 있습니다.

사용할 수 있는 보고서를 다음 표에서 설명합니다.

표 160. Rapid Recovery 보고서

보고서 유형	설명
작업 보고서	성공한 작업, 실패한 작업 및 오류가 발생한 작업의 상태 보고서를 제공합니다. 실패한 작업은 오류 보고서에서 자세히 볼 수 있습니다. 이 작업 유형은 Core Console 및 Central 관리 콘솔에서 실행할 수 있습니다. • Core에서 실행할 경우 이 보고서에는 한 개 이상의 Core에 대한 세부 정보를 지정할 수 있습니다.기본적으로 이 정보 세트에는 모든 보호된 시스템, 복제된 시스템 및 지정된 Core에 있는 복구 지점 전용 시스템 등, 모든 시스템에 대한 작업이 포함됩니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 일부 시스템을 선택하거나 제외하려면 필터를 사용합니다. 보고서에 Core 작업에 대한 상태만 표시할 경우 시스템과 연관된 작업을 선택하거나 제외할 수도 있습니다. • Core Console에서 보호된 시스템의 관점에서 실행할 때는 결과 보고서에 보호된 시스템에 대한 작업의 상태만 표시됩니다. • Central 관리 콘솔에서 실행할 때는 보고서에 콘솔에서 구성한 Core 또는 Core 그룹의 원하는 조합으로 세부 정보를 지정할 수 있습니다. 구성 가능한 매개 변수는 보고서 유형 및 날짜 범위입니다. 이 보고서 유형에 대한 자세한 내용은 작업 보고서 이해을(를) 참조하십시오.
오류 보고서	지정된 기준에 따라 실패한 Core 작업에 대한 정보를 제공합니다. 이 작업 유형은 Core Console 및 Central 관리 콘솔에서 실행할 수 있습니다. • Core에서 실행할 경우 이 보고서에 보호된 시스템 세부 정보를 포함하거나 제외할 수 있습니다. 작업 보고서와 유사하게 이 보고서도 Core에서 선택한 보호된 시스템에서만 실행할 수 있습니다. 결과 보고서에 선택한 보호된 시스템에 대해서만 실패한 작업의 세부 정보를 표시합니다. • Central 관리 콘솔에서 실행할 때는 보고서에 콘솔에서 구성한 Core 또는 Core 그룹의 원하는 조합으로 오류 이벤트를 지정할 수 있습니다. 구성 가능한 매개 변수는 보고서 유형 및 날짜 범위입니다. 이 보고서 유형에 대한 자세한 내용은 오류 보고서 이해을(를) 참조하십시오.
요약 보고서	요약 정보를 제공합니다.기본적으로 이 정보 세트에는 모든 보호된 시스템, 복제된 시스템 및 지정된 Core에 있는 복구 지점 전용 시스템 등, 모든 시스템에 대한 작업이 포함됩니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 일부 시스템을 선택하거나 제외하려면 필터를 사용합니다. 보고서에 Core 작업에 대한 상태만 표시할 경우 시스템과 연관된 작업을 선택하거나 제외할 수도 있습니다.

보고서 유형	설명
	보호된 단일 시스템의 관점에서는 이 보고서를 사용할 수 없습니다. 이 작업 유형은 Core Console 및 Central 관리 콘솔에서 실행할 수 있습니다. • Core Console에서 실행할 경우 이 보고서의 정보 범주에는 Core, 라이센스 및 리포지토리가 포함됩니다. 정보는 목록, 차트 및 표 형식으로 표시됩니다. • Central 관리 콘솔에서 실행할 때는 보고서에 콘솔에서 구성한 Core 또는 Core 그룹의 원하는 조합으로 요약 정보를 지정할 수 있습니다. 구성 가능한 매개 변수는 보고서 유형 및 날짜 범위입니다. 이 보고서의 정보 범주에는 Core, 라이센스 및 리포지토리가 포함됩니다. 요약 보고서에는 보호된 시스템 및 모든 작업 중 성공한 작업의 비율에 대한 보고서도 포함됩니다. 정보는 목록, 차트 및 표 형식으로 표시됩니다. 이 보고서 유형에 대한 자세한 내용은 요약 보고서 이해을(를) 참조하십시오.
리포지토리 보고서	이 보고서 유형은 선택한 Core에 있는 모든 리포지토리에 대한 보고서를 제공합니다. Core에서 사용 가능한 단일 리포지토리를 선택할 수도 있습니다. 이 보고서는 Core Console에서 Core의 관점에서만 사용할 수 있습니다. 이 보고서 유형에 대한 자세한 내용은 리포지토리 보고서 이해을(를) 참조하십시오.
예약된 보고서	Core Console에서 보고서를 예약할 수도 있습니다. 보고서를 예약하면 정의하는 일정에 따라 반복적으로 지정한 보고서를 생성합니다. 선택적으로 보고서가 생성될 때마다 이메일 알림을 설정할 수도 있습니다. 보고서 예약, 수정, 일시 중지 또는 삭제에 대한 자세한 내용은 Core Console에서 예약된 보고서 관리을(를) 참조하십시오.

선택하는 보고서 유형 및 매개 변수에 따라 한 개 이상의 Rapid Recovery Core에서 또는 한 대 이상의 보호된 시스템에 대해 보고서를 생성할 수 있습니다.

Central 관리 콘솔에서는 콘솔에서 구성한 Core 또는 Core 그룹의 원하는 조합으로 보고서를 생성할 수 있습니다.

Core Console에서 보고서 생성

Core Console에서 주문형 보고서를 생성할 수 있습니다. 다음과 같은 규칙이 적용됩니다.

- Core의 관점에서 모든 보고서를 생성할 수 있습니다.
- 또한 두 가지 작업 유형(작업 보고서 및 오류 보고서)을 보호된 시스템의 관점에서 생성할 수 있습니다. 그러한 보고서를 위해 선택한 시스템에 관련된 경우에만 데이터가 생성됩니다.
- 선택한 Core(또는 보호된 시스템)의 작업에 오류가 발생한 경우에만 오류 보고서에 데이터가 포함됩니다.

주문형 보고서를 생성하는 방법은 보고서를 Core에 초점을 맞춰 생성하거나, 보호된 시스템 관점에 따라 생성하는 것이 유사합니다. 그러나 탐색은 약간 차이가 있습니다.

또한 반복적으로 보고서를 예약할 수 있습니다. 보고서 예약, 수정, 일시 중지 또는 삭제에 대한 자세한 내용은 Core Console에서 예약된 보고서 관리을 참조하십시오.

주문형 Core 보고서 생성

Rapid Recovery 보고서 정보 항목에 설명된 대로 Core Console에서 사용 가능한 보고서의 전체 범위를 생성할 수 있습니다.

Rapid Recovery Core의 관점에서 보고서를 생성하려면 다음 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭한 다음 **보고서**를 선택합니다.

작업 보고서 페이지가 나타납니다. 페이지 제목의 보고서 이름 오른쪽에 아래 방향 화살표가 나타나면 다른 보고서 유형을 선택할 수 있습니다.

작업 보고서를 생성하려면 6단계로 이동하여 보고서 기준을 지정합니다.

3 다른 보고서 유형을 선택하려는 경우 보고서 이름 오른쪽에 있는 화살표를 클릭하면 사용 가능한 보고서 메뉴가 표시됩니다.

4 예약된 보고서 정의의 경우 보고서 예약를 참조하십시오.

5 리포지토리 보고서만 생성하려면 11단계로 건너뜁니다.

6 작업, 작업 요약, 오류 또는 요약 보고서의 경우 **날짜 범위** 드롭다운 메뉴에서 날짜 범위를 선택합니다.

날짜 범위를 선택하지 않으면 기본 옵션(마지막 31일)이 사용됩니다. 다음 표의 옵션에서 선택할 수 있습니다.

옵션	설명
마지막 24시간	보고서를 생성한 시간에 비례하여 마지막 날에 대한 보고서 활동
마지막 7일	보고서를 생성한 시간에 비례하여 마지막 주에 대한 보고서 활동
마지막 31일	보고서를 생성한 시간에 비례하여 마지막 31일에 대한 보고서 활동
마지막 90일	보고서를 생성한 시간에 비례하여 마지막 90일에 대한 보고서 활동
마지막 365일	보고서를 생성한 시간에 비례하여 전년도에 대한 보고서 활동
모든 시간	기간이 Core의 수명까지 확대됩니다.
사용자 지정 설치	이 기간은 시작일과 종료일을 추가로 지정할 때 필요합니다.
월-일	현재 달력(월)의 첫 번째 날짜부터 보고서를 생성한 날짜까지의 보고서 활동입니다.
년-일	현재 달력(년도)의 첫 번째 날짜부터 보고서를 생성한 날짜까지의 보고서 활동입니다.

노트: Core 소프트웨어가 배포되기 전이나 시스템이 Core에서 보호되기 전에 모든 호출에서 보고서 데이터를 사용할 수 없습니다.

7 작업 또는 오류 보고서의 경우, **대상 Core** 드롭다운 메뉴에서 적절한 Core나 보고서를 생성하려는 Core를 선택합니다.

기본 선택 항목에 사용할 수 있는 모든 Core가 포함되어 있습니다.

8 **보호된 시스템** 드롭다운 메뉴에서 보고서를 생성하려면 시스템을 선택합니다.

기본적으로 이 일련의 정보에는 모든 시스템(예: 보호된 모든 시스템, 복제된 시스템, 지정된 Core의 복구 지점만 시스템)에 대한 작업이 포함되어 있습니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 필터를 사용하여 일부 시스템을 선택하거나 제외시킬 수 있습니다. 또는 시스템과 별도인 작업을 선택하거나 제외시킬 수도 있습니다. 이 경우 보고서에 Core 작업에 대한 상태만 표시됩니다.

다음 항목 중에서 선택할 수 있습니다.

옵션	설명
모두 선택	이 옵션은 이 Core에서 보호되는 모든 보호된 시스템을 선택합니다. **노트: 모든 시스템을 선택한 뒤 일부 선택 항목을 삭제하여 모든 시스템에 대한 하위 집합을 지정할 수 있습니다.**
시스템과 별도	이 옵션을 선택하여 Core 관점의 작업이 포함되어 있는 보고서를 생성할 수 있습니다. 리포지토리 생성 또는 삭제, 부팅 CD 생성과 같은 작업 유형은 특정 시스템과 연관되어 있지 않습니다. Agent 소프트웨어를 아직 보호되지 않은 시스템에 배포하는 경우 이 작업 유형은 시스템과 별도인 것으로 간주됩니다. 이러한 작업은 결과 보고서의 보호된 시스템 열에 보호된 시스템을 나열하지 않습니다. 반대로, Agent 소프트웨어를 Core에서 이미 보호되는 시스템에 배포하는 경우 보호된 시스템 이름이 보고서에 포함됩니다. 이것은 시스템과 별도인 것으로 간주되지 않습니다.
보호된 시스템	이 옵션은 이 Core에서 보호되는 시스템을 나열합니다. 모두 선택하거나 보호된 시스템의 하위 집합을 선택할 수 있습니다.
복구 지점만	이 옵션은 한 번 보호된 시스템을 나열하지만 리포지토리에 복구 지점이 저장됩니다.
[소스 Core]	Core가 대상 Core인 경우 소스 Core에서 보호된 모든 시스템의 복구 지점이 복제되며, 소스 Core의 이름이 대문자로 표시됩니다. 이 옵션은 해당 소스 Core에서 보호되는 모든 시스템을 나열합니다. 이 대상 Core에서 복제된 모든 시스템을 선택하거나 해당 시스템의 하위 집합을 선택할 수 있습니다.
[사용자 지정 그룹]	이 Core에 생성된 사용자 지정 그룹이 있는 경우 모든 사용자 지정 그룹의 이름이 옵션으로 나타납니다. 해당 사용자 지정 그룹에 모든 개체가 표시됩니다. 그룹에서 모든 개체를 선택하거나 하위 집합을 선택할 수 있습니다.

9 요약 보고서를 생성하는 경우 12단계로 건너뜁니다.

10 작업, 작업 요약 또는 오류 보고서의 경우, **작업 유형** 드롭다운 메뉴에서 적절한 작업 유형을 선택합니다.

기본적으로 이 일련의 정보에는 선택한 보호된 시스템에 대한 모든 작업이 포함되어 있습니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 필터를 사용하여 기본 작업 범주에서 모든 작업을 선택하거나 제외시킬 수 있습니다. 또한 기타 작업 범주에서 모든 작업을 선택하거나 제외시킬 수도 있습니다. 또한 작업 매개 변수를 정의할 때 이러한 범주를 확장하여 보고서에 표시하려는 각 범주에서 작업 유형만 선택할 수 있습니다. 모든 작업 유형에 대한 확인란을 클릭하여 해당 유형을 선택하거나 삭제합니다. 범주 중 하나에서 일부 또는 모든 작업을 선택할 수 있습니다.

다음 **기타** 작업 유형에서 선택할 수 있습니다.

11 리포지토리 보고서의 경우, 리포지토리 메뉴에서 보고서에 포함하려는 리포지토리를 선택합니다.

기본 선택 항목에 사용할 수 있는 모든 리포지토리가 포함되어 있습니다.

12 **미리보기**를 클릭하여 지정된 기준의 보고서를 생성할 수 있습니다.

선택한 보고서 기준을 찾을 수 없는 경우, 보고서는 여전히 생성되지만 보고서에 빈 행이 포함되어 있습니다. 예를 들어 오류가 없는 경우, 오류 열의 콘텐츠가 보고서에서 null입니다.

13 다음 작업 중 하나를 수행합니다.

- 생성되는 보고서를 온라인으로 봅니다.
- 기준을 변경하여 보고서를 동적으로 업데이트한 뒤 **미리보기**를 다시 클릭합니다.
- **보고서 메뉴**를 사용하여 내보내기 형식(기본 형식인 PDF 포함)을 선택한 뒤 를 클릭하여 보고서를 내보낼 수 있습니다. 보고서 메뉴에 대한 자세한 정보는 보고서 메뉴 사용를 참조하십시오.
- **보고서 도구 모음**을 사용하여 보고서를 보거나 조작 또는 인쇄할 수 있습니다. 보고서 도구 모음에 대한 자세한 내용은 보고서 도구 모음 사용을(를) 참조하십시오.

보호된 주문형 시스템 보고서 생성

보호된 시스템에 대한 작업 보고서 또는 오류 보고서를 생성할 수 있습니다.

보호된 시스템에 대한 보고서를 생성하려면 다음 절차의 단계를 완료합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 보호된 시스템 메뉴에서 보고서로 검토할 보호된 시스템을 클릭합니다.

선택한 보호된 시스템에 대한 요약 페이지가 나타납니다.

3 페이지 상단의 보호된 시스템 이름 옆에 있는 메뉴 옵션에서 보고서 옆에 있는 아래쪽 화살표를 클릭한 후 보고서 유형을 선택합니다.

- 실패한 작업을 포함하여 보호된 시스템과 관련된 모든 작업에 대한 보고서를 생성하려면 **작업 보고서**를 클릭하고 보고서 기준 지정을 시작합니다.
- 보호된 시스템과 관련된 실패한 작업 목록만 생성하려면 **오류 보고서**를 클릭하고 보고서 기준 지정을 시작합니다.

4 작업 또는 오류 보고서의 경우 **날짜 범위** 드롭다운 메뉴에서 날짜 범위를 선택합니다.

날짜 범위를 선택하지 않는 경우 기본 옵션(최근 31일)이 사용됩니다. 다음 표에 있는 옵션 중에서 선택할 수 있습니다.

옵션	설명
최근 24시간	보고서를 생성하는 시간 기준으로 마지막 날에 대한 활동 보고서.
최근 7일	보고서를 생성하는 시간 기준으로 지난 주에 대한 활동 보고서.
최근 31일	보고서를 생성하는 시간 기준으로 지난 31일 대한 활동 보고서.
최근 90일	보고서를 생성하는 시간 기준으로 지난 90일 대한 활동 보고서.
최근 365일	보고서를 생성하는 시간 기준으로 지난 해에 대한 활동 보고서.
모든 시간	이 기간은 Core의 수명 기간을 모두 포함합니다.
사용자 지정 설치	이 기간은 시작 및 종료 날짜를 추가로 지정해야 합니다.
월간 누계	보고서를 생성하는 날짜가 포함된 현재 월의 첫째 날부터 활동 보고서 생성.
연간 누계	보고서를 생성하는 날짜가 포함된 현재 연도의 첫째 날부터 활동 보고서 생성.

노트: 통화 케이스의 경우 Core 소프트웨어가 배포되기 이전 또는 시스템이 Core에서 보호되기 이전의 보고서 데이터는 사용할 수 없습니다.

5 **작업 유형** 드롭다운 메뉴에서 알맞은 작업 유형을 선택합니다.

기본적으로 이 정보 세트에는 선택한 보호된 시스템에 대한 모든 작업이 포함됩니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 필터를 사용하여 기본 작업 범주에 있는 모든 작업 및 기타 작업 범주에 있는 모든 작업을 선택하거나 제외할 수 있습니다. 또는 작업 매개변수를 정의할 때 이러한 각각의 범주를 확장하거나, 보고서에 표시할 범주에서만 작업 유형을 선택할 수도 있습니다. 확인란을 클릭하여 작업 유형을 선택하거나 해당 유형의 선택을 취소합니다. 범주에서 작업을 일부 또는 모두 선택할 수 있습니다.

6 **미리 보기**를 클릭하여 지정된 기준으로 보고서를 생성합니다.

선택한 보고서 기준을 찾을 수 없는 경우 보고서는 생성되지만 보고서에 빈 행이 포함됩니다. 예를 들어, 오류가 없을 경우 보고서에서 오류 열의 내용은 null입니다.

7 다음 작업 중 하나를 수행합니다.

- 생성된 보고서를 온라인으로 봅니다.
- 기준을 변경하여 동적으로 보고서를 업데이트한 후 **미리 보기**를 다시 클릭합니다.
- **보고서 메뉴**를 사용하여 내보내기 형식을 선택하고 보고서를 내보냅니다. 보고서 메뉴에 대한 자세한 내용은 보고서 메뉴 사용을(를) 참조하십시오.
- **보고서 도구 모음**을 사용하여 보고서를 보거나, 조작하거나, 인쇄합니다. 보고서 도구 모음에 대한 자세한 내용은 보고서 도구 모음 사용을(를) 참조하십시오.

Core Console에서 예약된 보고서 관리

Core Console에서 사용 가능한 모든 보고서를 예약할 수 있습니다. 보고서를 예약하면 나중에 반복적으로 생성됩니다. 예약은 보고서를 매일, 매주 또는 매월 단위로 생성할지 여부를 정의합니다.

선택적으로, Rapid Recovery를 사용하면 각 보고서가 생성되었을 때 하나 이상의 받는 사람에게 이메일 알림을 보낼 수 있습니다. 이메일은 보고서 유형, 보고서 형식 및 날짜 범위를 지정하고 보고서를 첨부 파일로 포함합니다.

노트: Core를 위한 SMTP 서버를 구성해야 보고서를 이메일로 전송할 수 있습니다. 자세한 내용은 이메일 서버 구성을(를) 참조하십시오.

이메일 알림을 보내도록 선택하거나 선택하지 않을 때 생성된 보고서를 로컬 또는 Core 서버에서 액세스할 수 있는 네트워크 위치에 저장할 수 있습니다.

이메일 알림과 전달 또는 보고서를 저장할 위치를 지정해야 합니다. 또한 옵션을 둘 다 선택할 수도 있습니다.

이 항목은 다음과 같이 구성되어 있습니다.

관련 링크

보고서 예약
보고서 일정 수정
예약된 보고서 일시 중지, 계속 또는 삭제

보고서 예약

Core Console에서 사용 가능한 보고서를 예약할 수 있습니다. 보고서를 일시 중지하거나 삭제할 때까지 정의한 일정에 따라 보고서가 생성됩니다.

이메일 알림 및 전달을 지정하거나 보고서를 저장할 위치를 지정해야 합니다. 두 옵션을 모두 선택할 수도 있습니다.

보고서를 예약하려면 이 절차의 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 를 클릭한 다음 **보고서**를 선택합니다.

작업 보고서 페이지가 나타납니다. 현재 보고서 이름 오른쪽에 아래 방향의 화살표가 표시됩니다.

3 보고서 이름의 오른쪽에 있는 화살표를 클릭한 뒤 드롭다운 메뉴에서 **예약된 보고서**를 클릭합니다.

예약된 보고서 페이지가 나타납니다.

4 보고서가 반복적으로 생성되도록 예약하려면 **추가**를 클릭합니다.

보고 예약 설정 마법사가 나타납니다.

5 마법사의 **구성** 페이지에서 예약하려는 보고서의 세부정보를 입력한 뒤 **다음**을 클릭합니다. 구성 옵션은 다음 표에 설명되어 있습니다.

표 161. 예약된 보고서 구성 옵션

시스템	사용 가능한 보고서
이름	이 특정 일정에 할당하려는 표시 이름을 입력합니다. 기본 이름은 Schedule report 1입니다. 이름은 64자 이하로 제한됩니다. 금지된 문자 또는 금지된 구를 사용하지 마십시오.
보고서 형식	보고서 출력 형식을 선택합니다. 값을 선택하지 않은 경우, 기본 형식(pdf)이 사용됩니다.
보고서 유형	반복적으로 생성하려는 보고서 유형을 선택합니다.
레이블	예약된 보고서에 표시하려는 레이블을 선택합니다. 최소 하나 이상의 레이블이 필요합니다. 레이블을 정의하는 경우 사용자 지정 그룹 기능을 사용하여 하나의 논리 컨테이너에 Core 개체를 그룹화할 수 있습니다. 보고 예약 설정 마법사에서 레이블 매개 변수를 사용하여 예약된 보고서가 실행되는 사용자 지정 그룹을 선택할 수 있습니다. 사용자 지정 레이블이 없는 경우 레이블 드롭다운 메뉴에 사용 가능한 옵션(예: 모두 선택, 보호된 시스템)이 있습니다. 사용자 지정 그룹이 표시되는 경우 각 그룹은 옵션으로 나타납니다. 예약된 보고서에서 이러한 개체를 포함 또는 제외하는 옵션을 선택하거나 취소할 수 있습니다.
보호된 시스템	하나 이상의 보호된 시스템을 보고서에 포함하도록 선택합니다. 리포지토리 보고서에 이 옵션은 사용할 수 없습니다.
작업 유형	보고서에 표시하려는 작업 유형을 선택합니다. 기본적으로 이 일련의 정보에는 모든 시스템(예: 보호된 모든 시스템, 복제된 시스템, 지정된 Core의 복구 지점만 시스템)에 대한 작업이 포함되어 있습니다. 보고서 매개 변수에서 보고서를 사용자 지정할 수 있습니다. 필터를 사용하여 일부 시스템을 선택하거나 제외시킬 수 있습니다. 또는 시스템과 별도인 작업을 선택하거나 제외시킬 수도 있습니다. 이 경우 보고서에 Core 작업에 대한 상태만 표시됩니다. 작업 유형 매개변수는 Core 요약 및 리포지토리 예약 보고서 유형에 사용할 수 없습니다.

6 마법사의 **대상** 페이지에서 예약하려는 보고서 대상을 선택합니다. 다음 중 하나를 선택하거나 모두 선택할 수 있습니다. 선택하면 **다음**을 클릭합니다.

- **이메일 주소로 보내기** 필드에 하나 이상의 유효한 이메일 주소를 입력하여 예약된 보고서가 생성되면 이메일 메시지로 사용자에게 알릴 수 있습니다.

  노트: 이메일 알림 및 전달을 지정하지 않은 경우 저장 위치를 지정해야 합니다.

- **파일로 저장**을 선택하여 생성된 보고서 파일을 지정한 위치에 저장하고 **위치 유형** 드롭다운 메뉴에서 로컬, 네트워크 또는 클라우드 저장소 옵션을 선택합니다. 그런 다음 **위치** 필드에서 다음 표에 설명된 대로 추가 위치 정보를 지정합니다.

표 162. 예약된 보고서에 대한 위치 옵션

위치 유형	위치 유형 설명	위치
로컬	위치 유형으로 로컬을 선택하여 생성된 보고서를 Core에 액세스할 수 있는 로컬 경로에 저장합니다.	위치 필드에 경로를 지정합니다. Core에 로컬로 액세스할 수 있는 위치를 입력합니다.

위치 유형	위치 유형 설명	위치
		예를 들어 D 드라이브의 Reports 폴더에 보고서를 저장하려면 **D:\Reports**를 입력합니다.
네트워크	위치 유형으로 네트워크를 선택하여 생성된 보고서를 네트워크로 Core에 액세스할 수 있는 경로에 저장합니다. 위치 필드에 경로를 지정합니다.	위치 필드에 경로를 지정합니다. 네트워크에서 Core에 액세스할 수 있는 위치를 입력합니다. \\servername\sharename 형식을 사용합니다. 예를 들어 Data 서버의 보고서를 Reports라고 하는 공유 폴더에 저장하려면 **\\Data\Reports**를 입력합니다. 사용자 이름 및 암호 필드에 네트워크 자격 증명을 지정합니다.
클라우드	위치 유형으로 클라우드를 선택하여 생성된 보고서를 Core에 구성된 클라우드 저장소 계정에 저장합니다. 이 단계를 수행하기 전에 저장소 계정을 미리 정의해야 합니다. Core에서 사용할 수 있도록 클라우드 저장소 계정을 설정하는 방법에 대한 자세한 내용은 클라우드 계정 관리을(를) 참조하십시오.	계정 필드에서 적절한 클라우드 저장소 계정을 선택하여 생성된 보고서를 저장할 수 있습니다. 컨테이너 필드에서 저장소 계정에 해당하는 컨테이너를 지정합니다. 폴더 이름 필드에서 이후에 생성된 보고서를 저장할 폴더를 지정합니다.

7 대상 옵션을 지정하면 **다음**을 클릭합니다.

8 마법사의 **예약** 페이지로 이동하여 **데이터 전송** 메뉴에서 옵션을 선택하여 지정한 보고서를 생성할 빈도를 결정합니다. 보고서는 매일, 매주 또는 매월 생성할 수 있습니다. 각 옵션에는 다음 표에 설명된 것과 같은 자체 매개 변수가 있습니다.

표 163. 예약된 보고서 생성 빈도 옵션

생성 빈도	빈도 세부정보	빈도 매개 변수
매일	지정된 보고서를 매일 한 번씩 정해진 시간에 생성하여 저장하거나 전송합니다. 이 작업에 대한 기본 시간은 오전 12:00(Core 서버 시간 기준)입니다.	보고서가 생성되는 기본 시간을 변경하려면 시간 텍스트 필드에 새 값을 입력하거나 컨트롤을 사용하여 시간, 분, AM/PM을 변경합니다.
매주	지정된 보고서를 매주 한 번씩 정해진 요일에 생성하여 저장하거나 전송합니다. 이 작업에 대한 기본 시간은 일요일 오전 12:00(Core 서버 시간 기준)입니다.	보고서가 생성되는 기본 요일을 변경하려면 요일 메뉴에서 요일을 선택합니다. 보고서가 생성되는 기본 시간을 변경하려면 시간 텍스트 필드에 새 값을 입력하거나 컨트롤을 사용하여 시간, 분, AM/PM을 변경합니다.
매월	지정된 보고서를 매달 한 번씩 정해진 날짜와 시간에 생성하여 저장하거나 전송합니다. 이 작업에 대한 기본 시간은 매월 1일 오전 12:00(Core 서버 시간 기준)입니다.	보고서가 생성되는 기본 날짜를 변경하려면 날짜 메뉴에서 날짜를 선택합니다. 보고서가 생성되는 기본 시간을 변경하려면 시간 텍스트 필드에 새 값을 입력하거나 컨트롤을 사용하여 시간, 분, AM/PM을 변경합니다.

9 또는 일시 중지된 보고서를 다시 재개할 때까지 보고서가 생성하지 않도록 하려면 마법사의 **예약** 페이지에서 **처음에 보고 일시 중지**를 선택합니다.

이 보고서를 예약된 대로 생성하려면 이 옵션을 선택 취소합니다.

10 예약을 지정하면 **마침**을 클릭하여 마법사를 종료하고 사용자의 작업을 저장합니다.

요약 보고서의 요약 표에 새 보고서 일정이 표시됩니다.

보고서 일정 수정

보고서를 예약하면 매개변수 또는 세부 정보를 수정할 수 있습니다. 보고서 이름, 출력 형식, 보고서 유형, 포함된 리포지토리 등 보고서 구성 정보를 편집할 수 있습니다. 이메일 알림 옵션뿐 아니라 생성된 보고서를 저장할 대상을 변경할 수도 있습니다. 마지막으로, 보고서의 일정을 변경할 수 있습니다.

예약된 보고서의 매개변수를 수정하려면 다음 단계를 완료하십시오.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)을 클릭한 다음 **보고서**를 선택합니다.
작업 보고서 페이지가 나타납니다. 현재 보고서 이름의 오른쪽에 아래쪽 방향 화살표가 나타납니다.

3 보고서 이름의 오른쪽에 있는 이 화살표를 클릭하고 드롭다운 메뉴에서 **예약된 보고서**를 선택합니다.
예약된 보고서 페이지가 나타납니다.

4 예약된 보고서 요약 표에서 수정하려는 보고서 행의 설정 아이콘을 클릭한 다음 **편집**을 선택합니다.
보고서 일정 설정 마법사가 나타납니다.

5 이 마법사의 페이지들을 탐색하여 필요한 매개 변수를 변경합니다. 이 마법사의 매개 변수에 대한 자세한 내용은 보고서 예약 항목을 참조하십시오.

6 마법사의 **일정** 페이지에서 **마침**을 클릭하여 마법사를 종료하고 변경 사항을 저장합니다.
마법사가 닫히고 보고서 일정이 수정됩니다.

예약된 보고서 일시 중지, 계속 또는 삭제

보고서를 예약하면 정의된 일정에 따라 보고서를 생성합니다. 일시적으로 예약된 보고서 생성을 중지한 경우 일정을 일시 중지할 수 있습니다.

예약된 보고서를 일시 중지하고 보고서 생성을 다시 시작하려는 경우 이 절차의 설명에 따라 보고서를 다시 시작할 수 있습니다.

현재 예약된 보고서를 생성하고 있으며 더 이상 해당 보고서를 생성하지 않아도 되는 경우 이 보고서를 삭제할 수 있습니다.

예약된 보고서를 일시 중지할 것인지 결정하려면 예약된 보고서 요약 표에서 상태 열을 확인합니다. 녹색 타원은 활성 상태의 예약된 보고서, 노란색 타원은 일시 중지된 보고서, 빨간색 타원은 오류를 나타냅니다.

이 절차의 단계를 완료하여 보고서에 대한 예약을 일시 중지하거나 다시 시작하거나 삭제합니다.

1 Rapid Recovery Core Console로 이동합니다.

2 아이콘 표시줄에서 (자세히)를 클릭하고 **보고서**를 선택합니다.
작업 보고서 페이지가 나타납니다. 현재 보고서 이름 옆에 아래 화살표가 있습니다.

3 보고서 이름 오른쪽에 있는 화살표를 클릭하고 드롭다운 메뉴에서 **예약된 보고서**를 선택합니다.
예약된 보고서 페이지가 나타납니다.

4 예약된 보고서 요약 표에서 색상 표시기를 통해 예약된 모든 보고서의 상태를 확인하십시오.

5 일시 중지하거나 다시 시작하려는 각 보고서에 대해 첫 번째 열에 있는 확인란을 선택합니다.

6 요약 표 위에 있는 예약된 보고서 옵션에서 다음 중 하나를 수행합니다.
- 선택한 보고서의 생성을 일시 중지하려면 **일시 중지**를 클릭합니다.
- 일시 중지된 예약된 보고서 생성을 다시 시작하려면 **다시 시작**을 클릭합니다.
- 기존 예약된 보고서에 대해 선택한 일정을 삭제하려면 **삭제**를 클릭합니다.
  예약된 보고서를 삭제하면 향후 보고서의 생성만 중단합니다. 이전의 예약된 보고서를 저장했으면 제거되지 않습니다.

보고서 메뉴 사용

보고서 메뉴는 보고서를 볼 때 페이지 맨 위에 나타납니다. 보고서 제목을 포함하는 이 메뉴는 사용 가능한 보고서 유형을 볼 수 있는 드롭다운 메뉴이기도 합니다. 이 메뉴 아래에는 보고서 기준을 정의할 수 있는 하나 이상의 필터가 있습니다.

사용 가능한 특정 필터는 보고서 유형에 따라 다릅니다. 각 보고서 유형에 적용하는 매개 변수에 대한 정보는 해당 보고서 유형을 설명하는 항목을 참조하십시오.

보고서 메뉴 오른쪽에는 일부 제어가 나타납니다. 다음 표에서 설명하는 이러한 제어는 보고서를 생성하고 내보내는 데 유용합니다.

표 164. 보고서 메뉴 제어

UI 요소	설명
미리보기 단추	제공된 단추를 클릭하여 필터에 지정된 보고서 매개 변수와 선택한 보고서 유형에 따라 보고서를 생성합니다.
내보내기 형식 드롭다운 메뉴	내보내기 드롭다운 메뉴를 사용하면 보고서 출력 형식을 선택할 수 있습니다. 값을 선택하지 않으면 기본 형식(pdf)을 사용합니다.
다운로드 단추/아이콘	다운로드 단추는 내보내기 메뉴에서 선택한 형식 유형으로 생성한 보고서를 내보냅니다.

보고서는 열의 표시 단위(GB, TB 또는 초 단위)를 더 쉽게 확인할 수 있도록 측정 단위를 포함합니다.

생성되거나 내보낸 보고서의 형식에 만족하지 않은 경우 보고서에서 사용된 글꼴을 변경할 수 있습니다. 자세한 내용은 보고서 설정 관리을(를) 참조하십시오.

보고서를 생성한 후에는 보고서 도구 모음을 사용할 수 있습니다.

관련 링크

작업 보고서 이해
오류 보고서 이해
요약 보고서 이해
중앙 관리 콘솔 Core 보고서 이해

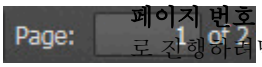
보고서 도구 모음 사용

보고서 메뉴에서 생성하면 해당 보고서는 보고서 도구 모음 아래에 나타납니다. 도구 모음을 통해 보고서 저장 및 인쇄를 포함해 보고서 출력을 조작할 수 있습니다.

도구 모음의 왼쪽에 토글 사이드바 옵션이 있습니다. 이 도구를 사용하면 사이드바가 확장 또는 축소되어 더 많은 표시 옵션을 표시할 수 있습니다. 도구 모음 오른쪽에 도구 옵션은 드롭다운 메뉴를 확장하여 보고서 탐색 컨트롤을 제공합니다. 보고서 도구 모음의 요소는 다음 표에 설명되어 있습니다.

표 165. 보고서 도구 모음 아이콘

아이콘	설명
	토글 사이드바. 모든 보고서 페이지가 미리 보기로 표시됩니다. 사이드바의 다른 옵션은 지원되지 않습니다.
	사이드바: 미리 보기를 표시합니다. 생성된 보고서의 모든 페이지에 대한 기본 보기입니다.

아이콘	설명
	사이드바: 문서 개요 표시. 이 기능은 지원되지 않습니다.
	사이드바: 첨부 파일 표시. 보고서에 대한 첨부 파일이 없습니다. 이 기능은 지원되지 않습니다.
	찾기. 생성된 보고서 내에서 텍스트를 검색할 수 있습니다. 사용자가 입력하는 조건과 일치하는 모든 텍스트 강조 표시 및 대소문자 구분 또는 무시 옵션이 포함되어 있습니다.
	이전 페이지. 보고서 보기를 이전 페이지로 이동합니다.
	다음 페이지. 보고서 보기에서 다음 페이지로 진행합니다.
	**페이지 번호 입력**. 페이지 번호 텍스트 필드를 클릭하고 유효한 페이지 번호를 입력한 다음 보고서 보기에서 해당 창으로 진행하려면 Enter 키를 누릅니다.
	축소. 생성된 보고서의 보기를 축소할 수 있습니다. 연속해서 클릭할 때마다 최소 25%까지 더 축소됩니다.
	확대. 생성되는 보고서 보기를 확대할 수 있습니다. 연속해서 클릭할 때마다 최대 1000%까지 더 확대됩니다.
	자동 확대/축소. 실제 크기, 페이지 맞추기, 전체 너비, 50%, 75%, 100%, 125%, 150%, 200%, 300% 또는 400%를 포함한 비율 기준으로 보기를 포함해 생성된 보고서의 확대/축소 보기를 제어할 수 있습니다.
	파일 열기. 파일 시스템을 탐색하여 저장된 보고서를 찾아 열 수 있습니다.
	인쇄. 생성된 보고서를 인쇄할 수 있습니다.
	도구. 이 아이콘을 클릭하면 도구 드롭다운 메뉴가 확장 또는 축소됩니다. 도구 옵션은 아래 설명되어 있습니다.
	도구: 첫 페이지로 이동. 생성된 보고서의 첫 페이지로 이동합니다.
	도구: 마지막 페이지로 이동. 생성된 보고서의 마지막 페이지로 이동합니다.
	도구: 시계 방향으로 회전. 이 옵션은 생성된 보고서의 캔버스를 시계 방향으로 회전합니다.
	도구: 시계 반대 방향으로 회전. 이 옵션은 생성된 보고서의 캔버스를 시계 반대 방향으로 회전합니다.
	도구: 손 도구. 이 도구를 선택하면 화면 전체에서 보고서를 클릭하여 끌어 이동할 수 있습니다.
	도구: 문서 속성. 생성된 보고서의 문서 속성에 대한 정보를 제공합니다. 이 창을 닫으려면 **닫기**를 클릭합니다.

보고서 생성에 대한 자세한 내용은 Core Console에서 보고서 생성을 참조하십시오. Central Management Console에서 다중 Core에 대한 보고서 생성 방법에 대한 자세한 내용은 Central Management Console에서 보고서 생성을 참조하십시오.

작업 보고서 이해

작업 보고서는 Rapid Recovery Core 및 Core에서 보호하는 시스템에 대해 사용 가능합니다. 이 보고서에서는 선택한 Core 또는 보호된 시스템에서 수행한 작업의 상태를 확인할 수 있습니다. 보고서에 나타나는 데이터의 행 또는 열에 데이터가 없으면 테스트하는 매개 변수가 null임을 나타냅니다. 예를 들어, 오류와 같은 열이 아무런 정보 없이 나타나면 선택한 레코드에 대해서는 오류가 발생하지 않은 것입니다. 보고서가 빈 행을 생성하면 선택한 레코드에 대한 작업은 시스템과는 독립된 활동임을 반영합니다.

Core에서 작업 보고서를 생성하는 방법에 대한 자세한 내용은 주문형 Core 보고서 생성을 참조하십시오. 보호된 시스템에 대한 보고서를 생성하는 방법에 대한 자세한 내용은 보호된 주문형 시스템 보고서 생성을 참조하십시오.

작업 보고서를 생성하면 보고서 세부 정보에는 다음 정보가 포함됩니다.

- 보고서에 대한 선택 기준
- 지정한 날짜 범위에 있는 각 작업의 행을 표시하는 요약 표. 각 행은 해당되는 Core, 보호된 시스템 및 작업 유형과 함께 다음을 포함합니다.
  - 작업에 대한 요약
  - 작업 상태
  - 작업과 관련된 오류
  - 작업의 시작 및 종료 날짜
  - 작업 기간(초)
  - 전체 작업(MB)

특정 카테고리와 관련된 정보가 아니면 셀은 보고서에 정보 없이 나타납니다. 예를 들어, 지정한 보호된 시스템에 대한 Core에 오류가 없으면 보고서의 해당 행에서 오류 열은 비어 있습니다.

작업 요약 보고서 이해

작업 요약 보고서는 Core 관점에서 보고할 때 사용할 수 있습니다. 이 보고서는 보호된 시스템의 보고서에서는 사용할 수 없습니다. 이 보고서는 Core에서 수행된 모든 작업에 대한 요약 정보를 표시하는 단일 요약이 있으며, 실패, 통과, 취소된 작업이 포함됩니다. 보고서에서 각 작업을 별도의 줄로 지정하므로 작업 보고서보다 자세한 정보를 표시합니다.

작업 요약 보고서를 생성하는 방법에 대한 내용은 Core Console에서 보고서 생성를 참조하십시오.

이 보고서 유형의 보고서 매개 변수에는 다음이 포함됩니다.

- 날짜 범위
- 보호된 시스템
- 작업 유형

작업 요약 보고서를 생성하면 보호된 시스템, 볼륨 및 작업 유형에 대한 정보 뿐만 아니라 보고서 선택 기준도 보고서 세부 정보에 포함됩니다.

Core 정보

요약 보고서의 Core 부분에는 보고되고 있는 Rapid Recovery Core 관련 데이터가 포함됩니다. 이 정보에 포함되는 내용:

- Rapid Recovery Core에서 보호되는 시스템 개수
- 실패한 작업이 있는 시스템 수

보호된 시스템 요약

요약 보고서의 보호된 시스템 부분에는 선택한 Rapid Recovery Core 및 해당 시스템의 볼륨에서 보호되는 모든 시스템에 대한 데이터가 포함됩니다.

차트는 각 시스템에 대한 작업 유형 행이 표시되고, 성공적인 유형별 작업 비율, 통과한 작업 개수, 실패한 작업 개수 및 취소한 작업이 포함되어 있습니다. (취소된 작업은 이러한 통계에 반영되지 않습니다.)

오류 보고서 이해

오류 보고서는 Rapid Recovery Core 및 Core의 보호를 받는 시스템에 사용할 수 있는 작업 보고서의 하위 집합입니다. 오류 보고서는 작업 보고서 목록에서 취소 및 실패한 작업들로 구성되며, 인쇄하거나 내보낼 수 있는 단일 보고서로 컴파일됩니다. 행이 비어 있는 보고서가 생성되면 보고서 기준에 지정된 날짜 범위 내에 오류가 없음을 나타냅니다.

노트: 대상 Cores 및 보호된 시스템 매개변수에 대한 결과는 Core 수준 보고서에만 표시됩니다.

Core에서 보고서를 생성하는 방법에 대한 자세한 내용은 주문형 Core 보고서 생성을(를) 참조하십시오. 보호된 시스템의 작업 보고서를 생성하는 방법에 대한 자세한 내용은 보호된 주문형 시스템 보고서 생성을(를) 참조하십시오.

오류 보고서를 생성하면 지정된 날짜 범위 내의 각 작업에 대한 행을 보여주는 요약 표가 나타납니다. 각 행에는 해당 Core와 보호된 시스템, 작업 유형 외에도 다음 내용이 포함됩니다.

- 작업 요약
- 작업 상태
- 작업과 관련된 모든 오류
- 작업의 시작 및 종료 날짜
- 작업 기간(초 단위)
- 총 작업량(MB)

요약 보고서 이해

하나 이상의 Core에 대한 요약 보고서를 사용할 수 있습니다. 보호된 시스템에 대한 보고서에서는 이 보고서를 사용할 수 없습니다. 요약 보고서에는 선택한 Rapid Recovery Core의 리포지토리에 대한 정보와 해당 코어에서 보호되는 시스템에 대한 정보가 포함됩니다. 정보는 한 보고서 내에서 두 개의 요약으로 나타납니다.

요약 보고서를 생성하는 방법에 대한 내용은 Core Console에서 보고서 생성을(를) 참조하십시오.

이 보고서 유형의 보고서 매개 변수에는 다음이 포함됩니다.

- 날짜 범위
- 보호된 시스템

요약 보고서를 생성하면 리포지토리 및 보호된 시스템에 대한 정보뿐만 아니라 리포트 선택 기준도 보고서 세부 정보에 포함됩니다.

Core 정보

요약 보고서의 Core 부분에는 보고되고 있는 Rapid Recovery Core 관련 데이터가 포함됩니다. 이 정보에 포함되는 내용:

- 라이센스 키(식별자)
- Rapid Recovery Core 소프트웨어의 현재 버전

리포지토리 요약

요약 보고서의 리포지토리 부분에는 선택한 Rapid Recovery Core에 있는 리포지토리에 대한 데이터가 포함됩니다. 이 정보에 포함되는 내용:

- Rapid Recovery Core의 리포지토리 수
- Core의 리포지토리 요약.

보호된 시스템 요약

요약 보고서의 보호된 시스템 부분에는 선택한 Rapid Recovery Core 또는 Core들에서 보호되는 모든 시스템에 대한 데이터가 포함됩니다. 여기에는 차트와 요약표가 포함됩니다.

차트에는 보호된 시스템이 실패한 작업 대비 성공한 작업(모든 유형 대상) 비율별로 표시됩니다. (취소된 작업은 이러한 통계에 반영되지 않습니다.)

X 즉 가로축에는 보호된 시스템 수가 표시됩니다. Y 즉 세로축에는 성공 계층이 표시됩니다. 특히, Y 축에는 보호된 시스템별로 다음 횟수가 표시됩니다.

- 수행된 작업 없음
- 성공률 50% 미만
- 성공률 50% 이상
- 성공률 100%

차트 아래에는 보호된 시스템에 대한 정보가 표시됩니다. 이 정보에 포함되는 내용:

- 보호된 시스템의 양
- 실패한 작업이 있는 보호된 시스템 수
- 다음 내용이 표시된 보호된 시스템별 요약표:
  - 보호된 시스템 이름
  - 시스템에서 보호되는 볼륨
  - 보호된 공간(GB 단위, 전체 및 현재)
  - 일별 변경 비율(평균 및 중앙값)
  - 작업 통계(성공, 완료됨, 실패함, 취소됨)
  - 암호화 적용 여부
- Core 버전

리포지토리 보고서 이해

리포지토리 보고서는 선택한 Rapid Recovery Core의 리포지토리에 대한 정보와 해당 Core에서 보호하는 시스템에 대한 정보를 포함합니다. 정보는 한 보고서 내에서 두 개의 요약으로 나타납니다.

Core에서 리포지토리 보고서를 생성하는 방법에 대한 내용은 주문형 Core 보고서 생성을(를) 참조하십시오.

이 보고서 유형에 대한 보고서 매개 변수에는 리포지토리만 포함됩니다.

리포지토리 보고서를 생성하는 경우 각 리포지토리의 보고서 세부 정보에는 Core의 리포지토리 요약 목록이 있습니다

Central Management Console

Rapid Recovery Central Management Console은 둘 이상의 Rapid Recovery Core를 사용하는 환경에 알맞은 선택적 구성 요소입니다. 이 구성 요소는 여러 Core에 대한 보고서를 그룹화, 관리 및 생성할 수 있는 중앙 인터페이스를 제공하는 웹 포털입니다.

CMC(Chassis Management Console)의 운영 체제 요구 사항은 Rapid Recovery Core에 대한 요구 사항과 동일합니다. 이러한 구성 요소는 사용자의 필요 사항에 따라 같은 시스템 또는 다른 시스템에 설치할 수 있습니다.

설치 후, 관리하고자 하는 Core를 추가하여 Central Management Console을 구성하거나, 개별적으로 Core 그룹의 일부로 구성해야 합니다.

노트: 로컬 관리자 권한으로 Installer를 실행해야 합니다.

또한 Windows 8, 8.1 및 10과 Windows Server 2012 및 2012 R2 운영 체제의 경우 GUI를 올바르게 로드하려면 서버에 ASP.NET 4.5 기능이 설치되어 있어야 합니다. 이 구성은 Rapid Recovery Installer 일부로 자동으로 포함됩니다.

이 구성 요소 설치에 대한 자세한 내용은 *Rapid Recovery 설치 및 업그레이드 안내서에서 "Dell Data Protection | Rapid Recovery Central Management Console 설치" 항목을 참조하십시오.*

이 구성 요소 구성에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery 사용 설명서*에서 *Dell Data Protection | Rapid Recovery* 항목을 참조하십시오.

이 구성 요소 UI 이해에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery *사용 설명서*에서 Dell Data Protection | Rapid Recovery 항목을 참조하십시오.

Rapid Recovery Central Management Console 이해

Central Management Console을 열면 콘솔 보기에 정보가 표시됩니다. **시작** 페이지가 표시되고 다음 요소를 참조할 수 있습니다.

표 166. Rapid Recovery Central Management Console의 UI 요소

UI 요소	설명
브랜드 영역	일반적인 환경에서는 Central Management Console의 왼쪽 상단에 전체 상위 제품 이름인 Dell Data Protection | Rapid Recovery가 브랜드로 표시되어 있습니다. 브랜드 영역의 아무 곳이나 클릭하면 웹 브라우저 사용자에게 Dell 지원 웹 사이트의 제품 문서가 표시됩니다.
왼쪽 탐색 영역	왼쪽 탐색 영역은 사용자 인터페이스 왼쪽의 브랜드 영역 아래 표시되고, 탐색 영역의 기능은 중앙 관리 콘솔의 오른쪽 상단에서 선택한 모드에 따라 달라집니다. **콘솔 모드** 탐색 영역에서 Console 모드에 있을 때 Core 또는 Core 그룹을 클릭하면 Rapid Recovery Core Console에서 선택한 Core 또는 Core 그룹이 열립니다. **보고서 모드** 탐색 영역에서 보고서 모드에 있을 때 Core 또는 Core 그룹을 선택하면 보고서를 생성할 때 표시될 정보를 결정합니다. **관리 모드** 탐색 영역에서 관리 모드에 있을 때 Core 또는 Core 그룹의 설정을 탐색할 수 있습니다. 또한 관리 모드에서 Core 및 Core 그룹을 추가하고 삭제할 수도 있습니다. 화살표를 클릭하면 메뉴가 확장되거나 축소됩니다. 조직, Core 그룹 및 Core와 같은 계층 구조 레벨이 포함되어 있습니다. 왼쪽 화살표를 클릭하면 탐색 영역이 축소됩니다. 탐색 영역을 확장하려면 오른쪽 화살표를 클릭합니다.
링크 메뉴	**Dell 지원팀에 문의하십시오.** 라이브 채팅, 비디오 자습서, Rapid Recovery 기술 문서, 자주 물어보는 질문 등에 액세스할 수 있는 Dell 지원 웹 사이트가 새 브라우저 창에서 연결됩니다.
링크 메뉴	**설명서.** 라이브 채팅, 비디오 자습서, Rapid Recovery 기술 문서, 자주 물어보는 질문 등에 액세스할 수 있는 Dell 지원 웹 사이트가 새 브라우저 창에서 연결됩니다.
링크 메뉴	**버전.** 중앙 관리 콘솔의 현재 버전이 나열됩니다. 이 링크를 클릭하면 정보 대화 상자가 열립니다.

UI 요소	설명
링크 메뉴	**모드 선택기** 링크 메뉴의 오른쪽 상단에, 현재 로그인된 Windows 사용자 이름이 드롭다운 메뉴에 나타납니다. 이 메뉴에서, Central Management Console의 보기를 변경할 수 있습니다. 다음 보기 중에서 선택할 수 있습니다. **콘솔** 기본 모드로, 한 위치에서 사용자 환경의 Core 및 Core 그룹을 볼 수 있습니다. **보고서.** 이 모드에서는 이 콘솔에 구성되어 있는 Core의 보고서를 생성하고 보고 내보낼 수 있습니다. **관리.** 관리 모드에서는 Central Management Console 자체나 그룹에 Core를 제거하거나 추가할 수 있습니다. **언어** 현지화를 지원하는 버전으로 언어 옵션이 나열됩니다. 이 옵션을 선택하면 중앙 관리 콘솔의 표시 언어를 선택할 수 있는 언어 전환 대화 상자가 열립니다. . **계정 캐시 지우기.** 이 옵션을 사용하면 로그인 사용자 계정에 대한 기존 정보를 지울 수 있습니다.

모드 선택기(페이지의 오른쪽 상단에 있는 드롭다운 메뉴)에서 옵션을 선택하여 Central Management Console의 보기를 변경할 수 있습니다. 예:

- 이미 구성되어 있는 Core 또는 Core 그룹을 관리하려면, 콘솔 보기를 사용합니다.
- Central Management Console을 구성하려면 관리 보기로 전환합니다.
- 보고서를 생성하려면 보고서 보기로 전환합니다.

왼쪽 탐색 메뉴에 보고 관리할 수 있는 Core가 표시됩니다. 개별 Core를 구성하거나 그룹으로 조직할 수 있습니다. Windows 사용자 이름 또는 그룹을 사용하여 특정 그룹에 있는 Core에 대한 액세스를 제한할 수 있습니다.

Rapid Recovery Central Management Console 구성

Rapid Recovery Central Management Console 구성에는 Core 및 Core 그룹 추가, 해당 설정 지정, 필요 시 그룹에 대한 액세스 설정 지정 작업이 포함됩니다.

구성을 완료한 후 단일 중앙 위치에서 설정과 모든 Core를 관리할 수 있습니다.

중앙 관리 콘솔을 구성하기 위해 아래의 관련 링크에 나열된 모든 작업을 수행할 수 있습니다.

관련 링크

Central Management Console에 Core 추가
Central Management Console에서 Core 설정 구성
Central Management Console에 Core 그룹 추가
Core 그룹 설정 구성
Core 그룹 액세스 구성

Central Management Console에 Core 추가

Core 그룹에 Core를 추가하려는 경우, 그룹을 먼저 생성해야 합니다. 자세한 내용은 Central Management Console에 Core 그룹 추가을(를) 참조하십시오. 나중에 Core 세부 정보를 편집하여 그룹을 지정할 수도 있습니다.

Central Management Console에 하나 이상의 Core를 추가하여 단일 인터페이스에서 이를 관리하거나 보고서를 생성할 수 있습니다.

다음 절차의 단계를 완료하여 Central Management Console에 Core를 추가하십시오.

1 Rapid Recovery Central Management Console에서 모드 선택기 드롭다운을 클릭하고 **관리**를 선택합니다.
페이지가 새로 고침되고 Core 추가, 그룹 추가 및 삭제 아이콘이 표시됩니다.
2 왼쪽 탐색 메뉴 위쪽에서 **Core 추가**를 클릭합니다.

Core 추가 페이지가 나타납니다.

3 다음 표에서 설명한 대로, Core에 연결하는 데 필요한 정보를 입력합니다.

표 167. Core 추가 세부 정보

텍스트 상자	설명
상위 그룹	(선택 사항) Core를 기존 Core 그룹에 가입시키려면, 적절한 조직의 상위 그룹을 선택합니다.
표시 이름	Core의 표시 이름을 입력합니다. 표시 이름은 150자 이하로 제한해야 합니다. 33자 이하로 유지하는 것이 가장 좋습니다. 금지된 문자 또는 금지된 구를 사용하지 마십시오. 금지된 문자 또는 금지된 구에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery 사용 설명서*를 참조하십시오.
호스트 이름	Core 액세스용 IP 주소를 입력합니다. 추가하는 Core가 현재 서버인 경우 localhost를 사용할 수 있습니다.
포트	연결용 포트 번호를 입력합니다. 기본값은 8006입니다.
사용자 이름	새로 추가한 Core에 대해 Core 서비스에 액세스할 사용자 이름을 입력합니다.
암호	새로 추가한 Core에 대해 Core 서비스에 액세스하는 데 사용할 암호를 입력합니다.

4 **연결 테스트**를 클릭하여 구성을 테스트합니다.
테스트가 성공하면, 성공 메시지가 표시됩니다. **확인**을 클릭하여 확인 메시지를 닫습니다.

5 **저장**을 클릭합니다.
변경 사항이 저장되고 Core가 이제 상위 그룹에 추가됩니다.

관련 링크

Central Management Console에 Core 그룹 추가

Central Management Console에서 Core 설정 구성

다음 절차의 단계를 수행하여 Central Management Console에 Core 설정을 구성하십시오.

1 Rapid Recovery Central Management Console에서 모드 선택기 드롭다운을 클릭하고 **관리**를 선택합니다.
페이지가 새로 고침되고 Core 추가, 그룹 추가 및 삭제 아이콘이 표시됩니다.

2 왼쪽 탐색 메뉴에서 해당 Core 이름을 클릭합니다.
선택한 Core의 **설정** 페이지가 표시됩니다.

3 설정 탭에서 다음 표에 설명된 대로 Core 정보를 수정합니다.

표 168. Core 설정

텍스트 상자	설명
상위 그룹	추가할 새 Core 설정에 대해 Core의 상위 그룹을 선택합니다.
표시 이름	Core의 표시 이름을 입력합니다.
사용자 이름	Core의 사용자 이름을 입력합니다.
암호	Core의 암호를 입력합니다.
관리 포털에서 [Core name]에	연결을 지정하는 옵션을 선택합니다. 다음을 선택할 수 있습니다. • [Core 이름]의 마지막으로 알려진 IP 주소(xxx.xxx.xxx.xxx)를 사용하거나 • 호스트 이름 또는 IP 주소[호스트 이름 또는 IP 주소]를 사용합니다.

텍스트 상자	설명
연결하려면 어떻게 해야 합니까?	호스트 이름 또는 IP 주소를 사용하여 연결을 지정하도록 선택한 경우 호스트 이름이나 IP 주소 필드에 해당 정보를 입력해야 합니다.
[Core 이름]이 수신 대기 중인 포트는 무엇입니까?	포트 옵션 중 하나를 선택합니다. 다음을 선택할 수 있습니다. . 기본 포트(8006) 또는 . 사용자 지정 포트 [포트] 포트를 지정하도록 선택한 경우 사용자 지정 포트 필드에 포트 번호를 입력합니다.

4 **연결 테스트**를 클릭합니다.
테스트가 성공하면 연결이 성공했음을 나타내는 메시지가 표시됩니다.
5 **저장**을 클릭합니다.

Central Management Console에 Core 그룹 추가

다음 절차의 단계를 완료하면 Rapid Recovery Central Management Console에 Core 그룹을 추가할 수 있습니다.

1 Rapid Recovery Central Management Console에서 모드 선택기 드롭다운을 클릭하고 **관리**를 선택합니다.
페이지가 새로 고쳐지고 Core 추가, Core 그룹 추가 및 삭제 아이콘이 표시됩니다.
2 왼쪽 탐색 메뉴 위쪽에서 **그룹 추가**를 클릭합니다.
그룹 추가 페이지가 나타납니다.
3 다음 표에 설명된 대로 상위 그룹과 표시 이름을 선택합니다.

표 169. Core 그룹 추가

텍스트 상자	설명
상위 그룹	추가할 새 Core 그룹에 대해 Core의 상위 그룹을 선택합니다.
표시 이름	Core 그룹의 표시 이름을 입력합니다. 표시 이름은 150자 이하로 제한해야 합니다. 33자 이하로 유지하는 것이 가장 좋습니다. 금지된 문자 또는 금지된 구를 사용하지 마십시오. 금지된 문자 또는 금지된 구에 대한 자세한 내용은 *Dell Data Protection | Rapid Recovery 사용 설명서*를 참조하십시오.

4 **저장**을 클릭합니다.

관련 링크

Central Management Console에 Core 그룹 추가

Core 그룹 설정 구성

Core 그룹 설정이나 액세스를 구성하기 전에 그룹을 먼저 생성해야 합니다. 자세한 내용은 Central Management Console에 Core 그룹 추가을(를) 참조하십시오.

다음 절차의 단계를 완료하여 Core 그룹 설정을 구성하십시오.

1 Rapid Recovery Central Management Console에서 모드 선택기 드롭다운을 클릭하고 **관리**를 선택합니다.
페이지가 새로 고쳐지고 Core 추가, Core 그룹 추가 및 삭제 아이콘이 표시됩니다.
2 왼쪽 탐색 메뉴에서 구성하려는 Core 그룹 이름을 클릭합니다.
선택한 Core 그룹의 설정 페이지가 표시됩니다.
3 다음 표에 설명된 대로 Core 그룹에 대한 정보를 수정합니다.

표 170. Core 그룹 설정

텍스트 상자	설명
상위 그룹	추가할 새 Core 그룹 설정에 대해 Core의 상위 그룹을 선택합니다.
표시 이름	Core 그룹의 표시 이름을 입력합니다. 표시 이름은 150자 이하로 제한해야 합니다. 33자 이하로 유지하는 것이 가장 좋습니다. 금지된 문자 또는 금지된 구를 사용하지 마십시오. 금지된 문자 또는 금지된 구에 대한 자세한 내용은 Dell Data Protection | Rapid Recovery 사용 설명서를 참조하십시오.

4 **저장**을 클릭합니다.

Core 그룹 액세스 구성

Core 그룹 설정이나 액세스를 구성하기 전에 그룹을 먼저 생성해야 합니다. 자세한 내용은 Central Management Console에 Core 그룹 추가을(를) 참조하십시오.

Central Management Console에서 Core를 추가하거나 보려면 현재 사용자 계정이 Active Directory 도메인 관리자가 그룹의 구성원이어야 합니다. 또는, 다음 절차를 사용하여 개별 사용자 또는 그룹에 대한 액세스를 제공할 수도 있습니다.

다음 절차의 단계를 완료하여 Core 그룹 액세스를 구성하십시오.

1 Rapid Recovery Central Management Console에서 모드 선택기 드롭다운을 클릭하고 **관리**를 선택합니다.
페이지가 새로 고침되고 Core 추가, 그룹 추가 및 삭제 아이콘이 표시됩니다.

2 왼쪽 탐색 메뉴에서 구성하려는 Core 그룹 이름을 클릭합니다.
선택한 Core 그룹의 **설정** 페이지가 표시됩니다.

3 **액세스** 탭을 클릭합니다.
Core 그룹에 대한 액세스 설정이 표시됩니다.

4 **추가**를 클릭합니다.
액세스 허용 대화 상자가 나타납니다. 개별 사용자 또는 그룹에 액세스를 제공할 수 있습니다.

5 다음 작업 중 하나를 수행합니다.
- 개별 사용자에게 액세스를 제공하려면 **이름** 텍스트 필드에 개별 사용자의 이름을 입력한 다음, **사용자**를 클릭합니다. 이것은 기본 옵션입니다.
  예를 들어, Administrator(또는 시스템이 도메인에 있는 경우 [도메인 이름] \Administrator)를 입력합니다.
- 그룹에 액세스를 제공하려면 **이름** 텍스트 필드에 그룹의 이름을 입력한 다음 **그룹**을 클릭합니다.
  예를 들어, AdminGroup(또는 시스템이 도메인에 있는 경우 [도메인 이름] \AdminGroup)을 입력합니다.

6 **이름 확인**을 클릭하여 지정한 사용자 이름 또는 그룹 이름에 액세스할 수 있는지 확인합니다.
입력한 이름이 유효하면, 계정 확인됨 메시지가 나타납니다.

7 이름을 입력하고 확인했으면 **저장**을 클릭합니다.
액세스 허용 대화 상자가 닫히고 변경 사항이 저장됩니다. 액세스 이름이 Core 그룹의 액세스 탭에 표시됩니다.

중앙 관리 콘솔 Core 보고서 이해

Rapid Recovery를 통해 여러 Rapid Recovery Core에 대한 작업 보고서, 오류 보고서 및 요약 정보를 생성할 수 있습니다. Core에 대한 상세정보는 섹션 작업 보고서 이해, 오류 보고서 이해및요약 보고서 이해 에 설명되어 있는 것과 동일한 범주의 요약 표에 제공됩니다.

여러 Core에 대한 보고서를 생성하는 방법에 대한 자세한 내용은 Central Management Console에서 보고서 생성을 참조하십시오.

Central Management Console에서 보고서 생성

Central Management Console에서 다중 Rapid Recovery Core에 대한 보고서를 생성하려면 다음 절차를 완료하십시오.

1 Rapid Recovery Central Management Console의 오른쪽 상단에 있는 모드 선택기 드롭다운 메뉴를 클릭하고 **보고서**를 선택합니다.

보고서 선택 페이지가 나타납니다. CoreJobReport는 기본적으로 선택됩니다. 보고서 이름 오른쪽에 있는 아래 화살표가 나타납니다. 이 화살표로 다른 보고서 유형을 선택할 수 있습니다.

2 왼쪽 탐색 메뉴에서 보고서에 포함하려는 개별 Rapid Recovery Core 또는 Core 그룹의 조합을 선택합니다.

3 보고서 유형 드롭다운 메뉴에서 생성할 보고서 유형을 선택합니다. 다음 옵션 중 하나에서 선택할 수 있습니다.

- 작업 보고서
- 오류 보고서
- 요약 보고서
- 작업 요약 보고서

이러한 보고서 유형에 대한 자세한 내용은 다음을 참조하십시오 Rapid Recovery 보고서 정보.

4 날짜 범위 드롭다운 메뉴에서 날짜 범위를 선택합니다.

다음 표에 있는 옵션 중에서 선택할 수 있습니다.

옵션	설명
일	보고서를 생성한 시간을 기준으로 마지막 날의 보고서 작업.
주	보고서를 생성한 시간을 기준으로 마지막 주의 보고서 작업.
월	보고서를 생성한 시간을 기준으로 마지막 한 달(31일)의 보고서 작업.
연도	보고서를 생성한 시간을 기준으로 마지막 해의 보고서 작업.
모든 시간	이 기간은 Core의 수명과 같습니다.
사용자 지정 설치	이 기간에서는 시작 및 종료 날짜를 지정해야 합니다.

노트: 항상 Core 소프트웨어를 배포하기 전에 또는 Core에서 시스템을 보호하기 전에 사용 가능한 보고서 데이터가 없습니다.

5 다음 작업 중 하나를 수행합니다.

- **미리보기**를 클릭하여 생성된 보고서를 생성하고 온라인으로 확인합니다.
- 보고서 기준을 변경하여 동적으로 보고서를 업데이트하고 **미리보기**를 다시 클릭합니다.
- 기본 형식(XLSX)을 포함하여 내보내기 형식을 선택하고 **다운로드**를 클릭합니다.
- **보고서 도구 모음**을 사용하여 보고서를 보거나 조작하거나 인쇄합니다. 보고서 도구 모음에 대한 자세한 내용은 다음을 참조하십시오 보고서 도구 모음 사용.

7

Rapid Recovery Command Line Management 유틸리티 이해

Dell Data Protection | Rapid Recovery에는 여러 가지 소프트웨어 구성 요소가 포함됩니다. 이 항목과 관련된 주요 구성 요소는 다음과 같습니다.

- Rapid Recovery Core는 보호된 시스템 인증, 백업 및 복제를 위한 데이터 전송 일정, 가상 시스템에 내보내기, 보고, 유사한 또는 다른 종류의 하드웨어에 대한 BMR(Bare Metal Restore) 등의 작업을 관리합니다.
- Rapid Recovery Agent는 볼륨 스냅숏을 작성하고, Core에서 관리하는 리포지토리로 데이터를 신속하게 전송하는 작업을 수행합니다.
- Rapid Recovery Command Line Management 유틸리티인 cmdutil.exe는 시스템 기능을 관리하기 위한 제3자 액세스를 제공합니다. 이 도구를 사용하여 Rapid Recovery Core 관리 기능의 스크립트 작업이 가능합니다.

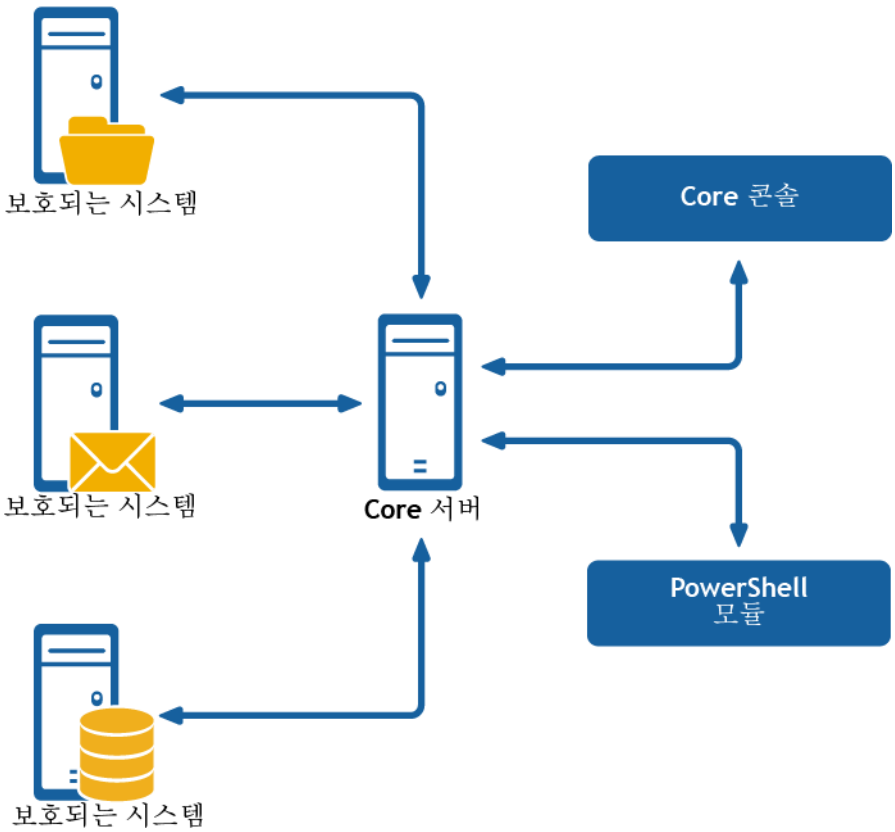


그림 13 . Rapid Recovery Command Line Management는 명령줄 기능 제공

Rapid Recovery Command Line Management는 사용자가 Rapid Recovery Core 서버와 상호 작용할 수 있도록 해주는 Windows 명령줄 유틸리티입니다. 이 유틸리티는 Rapid Recovery Core Console 그래픽 사용자 인터페이스가 제공하는 일부 동일한 기능을 제공합니다. 예를 들어, Rapid Recovery Command Line Management 유틸리티는 복구 지점을 마운트하거나 스냅숏을 작성할 수 있습니다.

Rapid Recovery Command Line Management 유틸리티는 Rapid Recovery Core의 모든 설치 작업에 포함됩니다. 기본 설치에서 Command Line Management 유틸리티를 열려면 **C:\Program Files\AppRecovery\Core\CoreService** 경로로 이동하여 `cmdutil.exe` 파일을 두 번 클릭합니다.

명령줄 모드에서는 명령 옵션과 한정자 선택을 통해 작업 플래그를 Rapid Recovery Command Line Management 유틸리티에 전달하여 제한된 관리 기능을 수행할 수 있도록 합니다.

주제:

- 명령
- 현지화

명령

이 항목에서는 Rapid Recovery Command Line Management 유틸리티에 사용 가능한 명령과 옵션에 대해 설명합니다. 사용할 수 있는 명령은 다음과 같습니다.

- 아카이브
- CancelActiveJobs
- CheckRepository
- CreateArchiveRepository
- createbootcd
- CreateRepository
- DeleteRepository
- Dismount
- DismountArchiveRepository
- EditEsxServer
- 수행
- ForceAttach
- ForceChecksum
- ForceLogTruncation
- ForceMount
- ForceReplication
- ForceRollup
- ForceVirtualStandby
- 도움말
- List
- 마운트
- MountArchiveRepository
- NewCloudAccount
- OpenDvmRepository
- Pause
- Protect
- ProtectCluster
- ProtectEsxServer
- RemoveAgent
- RemoveArchiveRepository
- RemovePoints

- RemoveScheduledArchive
- RemoveVirtualStandby
- Replicate
- 복제
- RestoreAgent
- RestoreArchive
- RestoreUrc
- Resume
- SeedDrive
- StartExport
- UpdateRepository
- 버전
- VirtualStandby

아카이브

종종 회사에서는 장기 저장 장치를 사용하여 준수 및 비준수 데이터를 모두 아카이브합니다. Rapid Recovery의 아카이브 기능은 준수 및 비준수 데이터의 장기 보존을 지원합니다. 관리자는 `-path` 매개 변수와 자격 증명을 지정하여 로컬 저장 장치 또는 네트워크 위치에 아카이브를 저장할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/archive -core [host name] -user [user name] -password [password] -all | -protectedserver [name | IP address] -path [location] -startdate [time string] -enddate [time string] -archiveusername [name] -archivepassword [password] -comment [text]
```

명령 옵션

다음 표에서는 `archive` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 171. Archive 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
`-all`	Core의 모든 보호된 시스템에 대한 복구 지점을 모두 아카이브합니다.
`-protectedserver`	아카이브할 복구 지점이 있는 보호된 시스템. 여러 시스템 이름을 큰따옴표로 묶고 공백으로 구분해서 지정할 수 있습니다.

옵션	설명
-path	아카이브한 데이터를 저장해야 하는 경로. 예: d:\work\archive 또는 network path \\servername\sharename.
-startdate	만든 날짜를 기준으로 복구 지점을 선택할 때 사용할 시작 날짜. 값은 큰 따옴표로 묶어야 합니다. 예: "04/30/2012 02:55 PM".
-enddate	선택 사항. 만든 날짜를 기준으로 복구 지점을 선택할 때 사용할 종료 날짜. 값은 큰 따옴표로 묶어야 합니다. 예: "05/31/2012 11:00 AM". 기본적으로 현재 시간 체계가 사용됩니다.
-archiveusername	선택 사항. 원격 시스템의 사용자 이름. 네트워크 경로에만 필요합니다.
-archivepassword	선택 사항. 원격 시스템 암호. 네트워크 경로에만 필요합니다.
-comment	선택 사항. 설명 텍스트는 큰 따옴표로 묶어야 합니다. 예: -comment "comment goes here...".

예:

Core의 모든 시스템에 대해 만든 날짜가 04/30/2012 02:55 PM 이후인 모든 복구 지점 아카이브:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path d:\work
\archive -startdate "04/30/2012 02:55 PM" -all
```

날짜 범위에 속하는 보호된 시스템 2대의 복구 지점 아카이브:

```
>cmdutil /archive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
"10.20.30.40" "20.20.10.1" -path d:\work\archive -startdate "04/30/2012 02:55 PM" -enddate
"05/31/2012 11:00 AM"
```

CancelActiveJobs

cancelactivejobs 명령을 사용하여 전송이나 복제 등 진행 중인 모든 특정 유형의 작업 실행을 취소할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/cancelactivejobs -core [host name] -user [user name] -password [password] -jobtype [job type
filter]
```

명령 옵션

다음 표에서는 cancelactivejobs 명령에 사용 가능한 옵션에 대해 설명합니다.

표 172. CancelActiveJobs 명령 옵션

옵션	설명
-?	명령에 대한 도움말을 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그인되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	어느 보호된 시스템에서 작업을 취소해야 하는지 결정합니다.
-all	모든 보호된 시스템에 대해 지정된 유형의 이벤트를 선택 및 취소합니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 다음과 같습니다. • 'transfer'(데이터 전송) • 'repository'(리포지토리 유지 관리) • 'replication'(로컬 및 원격 복제) • 'backup'(백업 및 복원) • 'bootcdbuilder'(부팅 CD 만들기) • 'diagnostics'(로그 업로드) • 'exchange'(Exchange Server 파일 검사) • 'export'(복구 지점 내보내기) • 'pushinstall'(에이전트 배포) • 'restore'(복구 지점 복원) • 'rollup'(복구 지점 롤업) • 'sqlattach'(에이전트 연결성 검사) • 'mount'(리포지토리 마운트) 기본적으로 지정된 유형의 모든 작업이 취소됩니다.

예:

Core 10.10.10.10의 모든 전송 작업 취소:

```
>cmdutil /cancelactivejobs -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -jobtype transfer
```

CheckRepository

CheckRepository 명령을 사용하여 AppAssure Core 또는 Rapid Recovery Core에서 생성된 기존 DVM 리포지토리의 무결성을 확인할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/checkrepository -repository [repository name] | -all [check all repositories] -core [host name] -user [user name] -password [password] name] -force
```

명령 옵션

다음 표에서는 CheckRepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 173. CheckRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	선택 사항. 이 옵션은 Core와 연관된 모든 DVM 리포지토리를 검사합니다.
-repository	DVM 리포지토리 이름.
-force	선택 사항. 이 옵션은 사용자 확인 없이 검사를 수행합니다.

예:

DVM 리포지토리 검사 시작:

```
>cmdutil /checkrepository -repository "Repository1" -core 10.10.10.10 -user administrator -
password 23WE@#$sdd
```

CreateArchiveRepository

아카이브 리포지토리를 생성하는 경우 예약된 아카이브의 내용에 대한 대상을 만듭니다. 이 기능을 사용하면 아카이브된 복구 지점을 마운트하고, 아카이브를 가져오지 않고도 시스템을 복원할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/createarchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name] -path [path to the archive] -archiveusernamme [network user name] -
archivepassword [network password] -cloudaccountname [name of the cloud account] -
cloudcontainer [name of the cloud container]
```

명령 옵션

다음 표에서는 CreateArchiveRepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 174. CreateArchiveRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-name	필수. 아카이브 리포지토리의 이름.
-path	기존 아카이브에 대한 경로. 로컬, 네트워크 또는 클라우드 위치일 수 있습니다. 예: d:\work\archive 또는 \\servername\sharename.
-archiveusername	선택 사항. 이 옵션은 원격 시스템에 대한 로그인입니다. 네트워크 경로에서만 필요합니다.
-archivepassword	선택 사항. 이 옵션은 원격 시스템에 대한 암호입니다. 네트워크 경로에서만 필요합니다.
-cloudaccountname	선택 사항. 이 옵션은 기존 클라우드 계정에 대한 표시 이름입니다. 클라우드 경로에서만 필요합니다.
-cloudcontainer	선택 사항. 클라우드 컨테이너는 아카이브가 있는 위치입니다. 클라우드 경로에서만 필요합니다.

예:

이름이 "NewArchive"인 아카이브 리포지토리를 만듭니다.

```
>cmdutil /createarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -path d:\work\archive
```

또한 아카이브에 하나 이상의 위치가 있으면 명령은 1부터 N까지 정렬된 모든 세그먼트에 대한 경로를 포함해야 합니다. 여기서, N은 세그먼트 수와 같습니다.

이름이 "NewSegmentArchive"인 아카이브 리포지토리를 만듭니다.

```
>cmdutil /createarchiverepository -name NewSegmentArchive -path1 \\RemmoteServer1\Share\Archive
\Segment1 - archiveusername1 Administrator -archivepassword1 23WE@#$sdd -path2 Archives
\NewSegment -cloudcontainer2 ArchiveContainer -cloudaccountname AmazonS3Local - path3 d:\work
\archive\Third
```

createbootcd

이 명령은 Rapid Recovery Core Console을 사용하지 않고 BMR(Bare Metal Restore) 부팅 CD를 생성할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/createbootcd -ip [IP address] -mask -defaultgateway -dnsserver -vncpassword -vncport -
isofilepath [destination for the boot image]
```

명령 옵션

다음 표에서는 CreateBootCD 명령에 사용 가능한 옵션에 대해 설명합니다.

표 175. CreateBootCD 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-ip	선택 사항. 이 옵션은 대상 BMR 시스템의 IP 주소를 지정합니다. 기본적으로 자동 생성됩니다.
-mask	선택 사항. 이 옵션은 대상 BMR 시스템의 서브넷 마스크를 지정합니다. 기본적으로 자동 생성됩니다.
-defaultgateway	선택 사항. 이 옵션은 대상 BMR 시스템의 기본 게이트웨이를 지정합니다. 기본적으로 자동 생성됩니다.
-dnsserver	선택 사항. 이 옵션은 대상 BMR 시스템에 대한 DNS 서버를 지정합니다. 기본적으로 자동 생성됩니다.
-vncpassword	선택 사항. 이 옵션은 기존 UltraVNC 계정의 사용자 암호를 지정합니다. 기본적으로 이 옵션은 빈 상태입니다.
-vncport	선택 사항. 이 옵션은 UltraVNC에 사용할 포트를 지정합니다. -vncpassword 옵션을 사용한 경우에만 이를 변경할 수 있습니다. 기본적으로 포트는 5900입니다.
-isofilepath	선택 사항. 이 옵션은 부팅 CD 파일에 대한 패치를 지정합니다. 기본 경로는 C:\ProgramData\AppRecovery \Boot CDs입니다.

예:

부팅 CD를 생성합니다.

```
>cmdutil /createbootcd -ip 192.168.20.188 -mask 255.255.255.0 -defaultgateway 192.168.20.2 -
dnsserver 192.168.20.2 -isofilepath D:\bcd\newbcd3.iso
```

CreateRepository

createrepository 명령을 사용하여 로컬 시스템 또는 CIFS 공유 위치에서 새 DVM 리포지토리를 생성할 수 있습니다.

용도

로컬 위치에 리포지토리를 만들 때는 명령을 다음과 같이 사용합니다.

```
/createrepository -name [repository name] -size [size allocated for repository] -datapath [data
path of repository] -metadatapath [metadata path of repository] -core [host name] -user [user
name] -password [password]
```

공유 위치에서 DVM 리포지토리를 만들 때는 명령을 다음과 같이 사용합니다.

```
/createrepository -name [repository name] -size [size allocated for repository] -uncpath [path for data and metadata] -shareusername [user name for share location] -sharepassword [password for share user name] -concurrentoperations [number of operations to occur at one time] -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 createrepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 176. CreateRepository 명령 옵션

옵션	설명
-?	명령에 대한 도움말을 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-name	리포지토리 이름.
-size	리포지토리 저장 위치의 크기. 사용 가능한 단위는 b, Kb, Mb, Gb, Tb 및 Pb입니다.
-datapath	로컬 위치에만 해당. 리포지토리 저장 위치의 데이터 경로를 결정합니다.
-metadatapath	로컬 위치에만 해당. 리포지토리 저장 위치의 메타데이터 경로를 결정합니다.
-uncpath	공유 위치에만 해당. 리포지토리 저장 위치의 데이터 및 메타데이터 경로를 결정합니다.
-shareusername	공유 위치에만 해당. 공유 위치에 대한 사용자 이름을 결정합니다.
-sharepassword	공유 위치에만 해당. 공유 위치 암호를 결정합니다.
-comment	선택 사항. 리포지토리 설명.
-concurrentoperations	선택 사항. 동시에 보류 가능한 최대 작업 수. 기본값: 64.

예:

로컬 위치에 DVM 리포지토리를 만듭니다.

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -datapath d:\repository -metadatapath d:\repository -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

공유 위치에 DVM 리포지토리를 만듭니다.

```
>cmdutil /createrepository -name "Repository 1" -size 200 Gb -uncpath \\share\repository -shareusername login -sharepassword pass123 -comment "First repository." -concurrentoperations 8 -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

DeleteRepository

DeleteRepository 명령을 사용하여 AppAssure Core 또는 Rapid Recovery Core에서 생성된 전체 DVM 리포지토리를 제거할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/deleterepository -core [host name] -user [user name] -password [password] name] -name
[repository name] | -a [all repositories]
```

명령 옵션

다음 표에서는 DeleteRepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 177. DeleteRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템의 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-a	선택 사항. 이 옵션은 Core와 연관된 모든 DVM 리포지토리를 삭제합니다.
-name	삭제할 DVM 리포지토리의 이름입니다.

예:

모든 DVM 리포지토리를 삭제합니다.

```
>cmdutil /deleterepository -a
```

"RepositoryName:" 이름의 리포지토리를 삭제합니다.

```
>cmdutil /deleterepository -name RepositoryName
```

Dismount

dismount 명령을 사용하여 -path 옵션으로 지정한 마운트된 복구 지점을 분리하거나 -protectedserver 매개변수로 선택한 에이전트의 지점을 분리할 수 있으며, -all 옵션으로 모든 마운트된 복구 지점을 분리할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/dis[mount] -core [host name] -user [user name] -password [password] [-all | -
protectedserver [name | IP address] | -path [location]
```

명령 옵션

다음 표에서는 dismount 명령에 사용 가능한 옵션에 대해 설명합니다.

표 178. Dismount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	모든 마운트된 복구 지점을 분리합니다.
-protectedserver	현재 에이전트에 대해 마운트된 복구 지점을 모두 분리합니다.
-path	선택한 마운트 지점을 분리합니다.

예:

c:\mountedrecoverypoint 폴더에 마운트된 복구 지점 분리:

```
>cmdutil /dismount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path c:
\mountedRecoveryPoint
```

DismountArchiveRepository

탑재된 아카이브에서 원하는 정보를 검색한 후 잠재적인 문제를 방지하려면 아카이브를 분리해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/dismountarchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name]
```

명령 옵션

다음 표에서는 DismountArchiveRepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 179. DismountArchiveRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-name	필수입니다. 아카이브 리포지토리 이름입니다.

예:

이름이 "NewArchive"인 리포지토리를 분리합니다.

```
>cmdutil /dismountarchiverepository -name NewArchive -core 10.10.10.10 -user administrator -
password 23WE@#$sdd -path d:\work\archive
```

EditEsxServer

에이전트 없이 보호하려는 VMware ESX(i) 가상 시스템 수를 변경하려는 경우 언제나 editesxserver 명령을 사용할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/editEsxServer -core [host name] -user [user name] -password [password] -protectedserver [name
| IP address] -add | -remove -virtualMachines [virtual machines collection | all] -autoProtect
[object ID or name collection]
```

명령 옵션

다음 표에서는 editesxserver 명령에 사용 가능한 옵션에 대해 설명합니다.

표 180. EditEsxServer 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-repository	필수. Core에 연결되었으며, 가상 시스템을 보호하는 데 사용하려는 리포지토리 이름. **노트: 이름은 큰따옴표로 묶어야 합니다.**
-protectedserver	특정 보호된 시스템에 대한 vCenter 및 ESX(i) 개체를 편집하려면 이 옵션을 사용합니다.
-add	지정된 vCenter 또는 ESXi 개체를 추가하려면 이 옵션을 사용합니다.
-remove	지정된 vCenter 또는 ESXi 개체를 제거하려면 이 옵션을 사용합니다.
-virtualmachines	선택 사항. 이 옵션을 사용하면 보호할 가상 시스템을 표시할 수 있습니다.
-autoprotect	선택 사항. 이 옵션을 사용하면 자동으로 보호할 새 가상 시스템을 표시할 수 있습니다.

예:

자동으로 Core에서 vCenter 또는 ESXi 서버의 특정 vCenter 또는 ESXi 개체를 보호합니다.

```
>cmdutil /editEsxServer -protectedserver 10.10.8.150 -add -autoprotect "Folder1" "Folder2"
```

수행

force 명령은 지정된 보호된 서버의 스냅숏을 작성합니다. 스냅숏을 작성하면 현재 보호된 시스템에 대한 데이터 전송을 수행할 수 있습니다. 스냅숏을 작성하면 전송이 즉시 시작되거나 대기열에 추가됩니다. 이전 복구 지점에서 변경된 데이터만 전송됩니다. 이전 복구 지점이 없을 경우 보호된 볼륨의 모든 데이터가 전송됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/force [snapshot] default | [base] [-all | -protectedserver [name | IP address]] -core [host
name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 force 명령에 사용 가능한 옵션을 설명합니다.

표 181. Force 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-force	선택 사항. 작성할 스냅숏 유형. 사용 가능한 값: 'snapshot'(증분 스냅숏)과 'base'(기본 이미지 스냅숏). 기본적으로 증분 스냅숏이 수행됩니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	Core의 모든 시스템에 대해 스냅숏을 작성합니다.
-protectedserver	특정한 보호된 시스템에 대해 스냅숏을 작성합니다.

예:

Core의 모든 시스템에 대해 스냅숏 작성:

```
>cmdutil /force snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

ForceAttach

forceattach 명령을 사용하여 SQL 데이터베이스 파일 연결성 검사를 수행할 수 있습니다. 체크섬 검사를 실행하면 즉시 검사가 시작됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/forceattach -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -rpn [number | numbers] | -time [time string]
```

명령 옵션

다음 표에서는 forceattach 명령에 사용 가능한 옵션에 대해 설명합니다.

표 182. ForceAttach 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	연결성 검사를 수행할 보호된 시스템.
-rpn	검사를 수행할 복구 지점의 일련 번호(번호를 얻으려면 /list rps 명령 실행). 명령 하나로 여러 복구 지점에 대해 검사를 수행하려면 여러 번호를 공백으로 구분하여 지정할 수 있습니다.
-time	만든 날짜를 기준으로 복구 지점을 선택합니다. 정확한 시간을 "mm/dd/yyyy hh:mm tt" 형식으로 지정해야 합니다(예: "2/24/2012 09:00 AM"). 날짜 및 시간 값을 PC에 설정된 시간대로 지정해야 함을 잊지 마십시오.

예:

번호가 5와 7인 복구 지점에 대해 연결성 검사 수행:

```
>cmdutil /forceattach -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceChecksum

forcechecksum 명령을 사용하면 지정된 하나 이상의 복구 지점에 존재하는 MDB(Exchange Message Databases)의 무결성 검사를 수행할 수 있습니다. 체크섬 검사를 수행하면 즉시 명령이 시작됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/forcechecksum -core [host name] -user [user name] -password [password] -protectedserver [name
| IP address] -rpn [number | numbers] -time [time string]
```

명령 옵션

다음 표에서는 forcechecksum 명령에 사용 가능한 옵션에 대해 설명합니다.

표 183. ForceChecksum 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.

옵션	설명
-protectedserver	체크섬 검사를 수행할 보호된 시스템.
-rpn	검사를 수행할 복구 지점의 일련 번호(번호를 얻으려면 /list rps 명령 실행). 명령 하나로 여러 복구 지점에 대해 검사를 수행하려면 여러 번호를 공백으로 구분하여 지정할 수 있습니다.
-time	만든 날짜를 기준으로 복구 지점을 선택합니다. 정확한 시간을 "mm/dd/yyyy hh:mm tt" 형식으로 지정해야 합니다(예: "2/24/2012 09:00 AM"). 날짜 및 시간 값을 PC에 설정된 시간대로 지정해야 함을 잊지 마십시오.

예:

번호가 5와 7인 복구 지점에 대해 체크섬 검사 수행:

```
>cmdutil /forcechecksum -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

ForceLogTruncation

로그 잘라내기 수행 작업은 필요할 때 즉시 한 번에 완료할 수 있습니다. 이 명령은 지정된 SQL Server 에이전트 시스템에 대한 로그를 즉시 잘라냅니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/[forcelogtruncation | flt] -core [host name] -user [user name] -password [password] -
protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 forcelogtruncation 명령에 사용 가능한 옵션에 대해 설명합니다.

표 184. ForceLogTruncation 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	로그 파일 잘라내기를 수행할 보호된 시스템.

예:

보호된 서버에 대해 로그 잘라내기 수행:

```
>cmdutil /forcelogtruncation -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.20.20
```

ForceMount

forcemount 명령은 복구 지점 연결성 검사를 한 번 수행하기 위해 사용합니다. 이 명령은 지정된 하나 이상의 복구 지점을 마운트하고 백업된 데이터의 복원에 사용할 수 있는지 결정합니다. 검사를 수행할 특정 복구 지점을 하나 이상 나열하거나 복구 지점이 만들어진 시간 범위를 지정해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/forcemount -core [host name] -user [user name] -password [password] -protectedserver [name |
IP address] -rpn [number | numbers] | -time [time string]
```

명령 옵션

다음 표에서는 forcemount 명령에 사용 가능한 옵션에 대해 설명합니다.

표 185. ForceMount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	연결성 검사를 수행할 보호된 시스템.
-rpn	검사를 수행할 복구 지점의 일련 번호(번호를 얻으려면 /list rps 명령 실행). 명령 하나로 여러 복구 지점에 대해 검사를 수행하려면 여러 번호를 공백으로 구분하여 지정할 수 있습니다.
-time	만든 날짜를 기준으로 복구 지점을 선택합니다. 정확한 시간을 “mm/dd/yyyy hh:mm tt” 형식으로 지정해야 합니다(예: “2/24/2012 09:00 AM”). 날짜 및 시간 값을 PC에 설정된 시간대로 지정해야 함을 잊지 마십시오.

예:

번호가 5와 7인 복구 지점에 대해 마운트 가능성 검사 수행:

```
>cmdutil /forcemount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.20.20 -rpn 5 7
```

ForceReplication

forcereplication 명령을 사용하여 복제된 데이터를 소스 Core에서 대상 Core로 1회 전송할 수 있습니다. 특정한 보호된 서버 1대를 복제하거나 모든 보호된 서버를 복제할 수 있습니다. 보호된 서버에서 복제를 사용할 수 있도록 미리 구성해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/[forcereplication |frep] -core [host name] -user [user name] -password [password] -targetcore
[host name] -all | -protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 forcereplication 명령에 사용 가능한 옵션을 설명합니다.

표 186. ForceReplication 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-targetcore	복제를 수행할 대상 Core의 호스트 이름.
-protectedserver	복제하려는 보호된 시스템.
-all	대상 Core에 복제되는 모든 시스템에 대해 복제를 수행합니다.

예:

특정 대상 Core의 보호된 서버에 대해 복제 수행:

```
>cmdutil /forcereplication -target core 10.10.10.10 -protectedserver 10.20.30.40
```

ForceRollup

forcerollup 명령은 보호된 시스템에서 복구 지점 롤업을 수행하기 위해 사용합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/[forcerollup | fro] -core [host name] -user [user name] -password [password] -protectedserver
[name | IP address]
```

명령 옵션

다음 표에서는 forcerollup 명령에 사용 가능한 옵션에 대해 설명합니다.

표 187. ForceRollup 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	선택 사항. 롤업을 수행하는 보호된 시스템입니다.

예:

Core에서 10.10.10.1 에이전트에 대해 롤업 수행:

```
>cmdutil /forcerollup -core 10.10.10.10 - user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.1
```

ForceVirtualStandby

보호된 시스템에서 가상 시스템으로 데이터를 내보내면 가상 대기 시스템이 생성됩니다. 지속적인 가상 내보내기를 설정해 둔 경우 이 명령을 사용하여 사전 설정된 일정과 상관없이 Rapid Recovery가 필요 시 데이터를 내보내도록 강제할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/forcevirtualstandby -core [host name] -user [user name] -password [password login] -
protectedserver [name] | -all
```

명령 옵션

다음 표에서는 ForceVirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 188. ForceVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	가상 시스템의 이름 또는 공간으로 구분된 이름.
-all	이 명령은 모든 예정된 가상 내보내기를 강제 실행할지 여부를 지정합니다.

예:

모든 가상 대기 내보내기 강제 실행:

```
>cmdutil /forcevirtualstandby -all
```

두 대의 시스템에 대한 가상 대기 강제 실행:

```
>cmdutil /forcevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

도움말

help 명령은 사용 가능한 명령과 각 명령의 정의가 나열된 목록을 표시합니다. 저작권 및 버전 세부 정보도 제공됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/help
```

예:

명령줄 도움말 요청:

```
>cmdutil /help
```

List

list 명령으로 모든 복구 지점, 활성 작업, 완료된 작업, 실패한 작업, 잘못된(실패한) 복구 지점, 유효한(통과된) 복구 지점, 탑재, 보호된 서버, 볼륨, 가상화된 서버, 보호되지 않은 볼륨, 클러스터, 보호 그룹, SQL 데이터베이스, Exchange 데이터베이스, 복제된 서버 및 지정된 에이전트 또는 현재 Core에서 보호되고 있는 서버 목록의 리포지토리에 대한 정보가 반환됩니다. 기본적으로 최근 기록이 반환됩니다. 모든 기록을 나열하거나 숫자 매개 변수를 사용하여 표시할 기록 수를 지정할 수 있습니다. 이 매개 변수에는 최근 복구 지점을 나타내는 글자 "l"와 첫 번째 복구 지점을 나타내는 글자"f"가 포함되어야 합니다. 각 복구 지점에는 관리자가 마운트에 사용할 수 있는 고유 번호가 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/list [rps | passed | failed | mounts | volumes | protectedservers | activejobs | completed
jobs | failedjobs | virtualizedservers | unprotectedvolumes | clusters | protectiongroups |
sqldatabases | exchangemailstores | replicatedservers | repositories] -protectedserver [name |
IP address] -core [host name] -user [user name] -password [password] -number [all | l<number> |
f<number> | <number>] -jobtype
```

명령 옵션

list 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 189. List 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-list	다음 옵션 중 하나를 선택합니다. • 모든 복구 지점('rps') • 유효한 복구 지점('passed') • 유효하지 않은 복구 지점('failed') • 마운트('mounts') • 보호된 볼륨('volumes') • 보호되지 않는 볼륨('unprotectedvolumes') • 보호된 시스템('protectedservers') • 활성 작업('activejobs') • 실패한 작업('failedjobs') • 완료된 작업('completedjobs') • 가상 서버('virtualizedservers') • 클러스터('clusters') • 보호 그룹('protectiongroups') • SQL Server 데이터베이스('sqldatabases')

옵션	설명
	• MS Exchange 데이터베이스('exchangemailstores') • 복제된 서버('replicatedservers') • 리포지토리('repositories')
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	작업 표시에만 해당. Core 서버의 특정 이벤트 유형(활성/실패/완료)을 모두 표시합니다.
-protectedserver	표시할 복구 지점이 있는 보호된 시스템.
-number	선택 사항. 표시할 데이터 항목 수. 다음 지정자만 함께 사용합니다: 'rps', 'activejobs', 'completedjobs', 'failedjobs'. 사용 가능한 값은 다음과 같습니다. • all(모든 데이터 항목 가져오기) • l[number] 또는 [number](상위 ##개 데이터 항목 가져오기) • f[number](첫 ##개 데이터 항목 가져오기) 복구 지점 및 작업을 표시할 때만 적용됩니다.
-jobtype	선택 사항. 작업 유형별로 출력을 필터링합니다. 사용 가능한 값은 다음과 같습니다. • 'transfer'(데이터 전송) • 'repository'(리포지토리 유지 관리) • 'replication'(로컬 및 원격 복제) • 'backup'(백업 및 복원) • 'bootcdbuilder'(부팅 CD 만들기) • 'diagnostics'(로그 업로드) • 'exchange'(Exchange Server 파일 검사) • 'export'(복구 지점 내보내기) • 'pushinstall'(에이전트 배포) • '복원'(복구 지점 복원) • 'rollup'(보호된 시스템 롤업) • 'sqlattach'(에이전트 연결성 검사) • 'mount'(리포지토리 마운트)

예:

최근 복구 지점 30개 나열:

```
>cmdutil /list rps -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -number l30
```

보호된 시스템에 의해 수행된 모든 실패한 데이터 전송 작업 보기:

```
>cmdutil /list failed jobs -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -number all -jobtype transfer
```

마운트

mount 명령으로 드라이브 하나 이상의 스냅숏이 탑재됩니다. 마운트를 읽기, 쓰기 또는 이전 쓰기 포함 읽기 전용으로 지정할 수 있습니다. 기본 설정은 읽기 전용입니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/mount -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -mounttype [read | write | readOnlyWithPreviousWrites] -drives [drive names] -volumes [volume names] -path [location] -rpn [number | numbers] | -time [time string]
```

명령 옵션

mount 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 190. Mount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	마운트할 복구 지점이 있는 보호된 시스템.
-mounttype	선택 사항. 마운트 모드를 지정합니다. 사용 가능한 값은 'read' (read-only), 'readOnlyWithPreviousWrites'(이전 쓰기가 포함된 읽기 전용), 'write' (쓰기 가능)입니다. 기본 모드는 read-only입니다.
-volumes	선택 사항. 마운트할 볼륨 이름의 목록. 지정하지 않으면 모든 볼륨이 마운트됩니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다(예: "c:" "d:"). 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.
-path	복구 지점을 마운트해야 하는 Core 서버의 폴더 경로. 폴더가 존재하지 않으면 자동으로 만듭니다.
-rpn	선택 사항. 탑재할 복구 지점의 순번(번호를 가져오려면 /list rps 명령 사용). 명령 하나로 여러 복구 지점을 마운트하려면 여러 번호를 공백으로 구분하여 지정하십시오. 그러면 각 복구 지점의 데이터가 별도의 하위 폴더에 저장됩니다. 참고: -time 및 -rpn 옵션을 모두 지정하지 않으면 무결성 검사를 최근에 통과한 복구 지점이 마운트됩니다.
-time	선택 사항. 마운트하기 위해 선택할 복구 지점을 하나 이상 결정합니다. 사용 가능한 값에는 'latest', 'passed', "mm/dd/yyyy hh:mm tt" 형식의 정확한 시간(예: "2/24/2012 09:00 AM") 등이 있습니다. 날짜 시간 값은 PC에 설정된 시간대로 지정해야 합니다. -time 옵션과 -rpn 옵션을 모두 지정하지 않으면 최근에 무결성 검사를 통과한 복구 지점이 마운트됩니다.

옵션	설명
-localdrive	선택 사항. 로컬 PC의 사용자 디스크에 마운트하는 작업을 수행합니다.

예:

"c:\" 및 "d:\" 읽기 전용 모드 볼륨을 포함하는 최근 복구 지점 마운트:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path c:\mountedrecoverypoint -mounttype read -volumes "c:" "d:"
```

번호가 2와 7인 복구 지점 마운트:

```
>cmdutil /mount -core 10.10.10.10 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path c:\mountedrecoverypoint -rpn 2 7
```

MountArchiveRepository

Rapid Recovery의 아카이브에서 데이터를 복원하려면 먼저 탑재해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/mountarchiverepository -core [host name] -user [user name] -password [password] -name [archive
repository name]
```

명령 옵션

다음 표에서는 mountarchiverepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 191. MountArchiveRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-name	필수입니다. 아카이브 리포지토리 이름입니다.

예:

이름이 "NewArchive"인 리포지토리를 탑재합니다.

```
>cmdutil /mountarchiverepository -name NewArchive
```

NewCloudAccount

NewCloudAccount 명령을 사용하여 Rapid Recovery Core에 클라우드 공급자용 계정을 추가할 수 있습니다. 그런 다음, 해당 계정을 사용하여 보존이나 복제 시 사용할 아카이브를 저장할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/newcloudaccount -core [host name] -user [user name] -password [password] -displayname [name
for the account] -type [cloud account provider] -useername [user name for the account] -key
[secret key] -region [region for account] tenanatid [tenant ID] -authurl [authorization URL]
```

명령 옵션

다음 표에서는 NewCloudAccount 명령에 사용 가능한 옵션에 대해 설명합니다.

표 192. NewCloudAccount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-displayname	클라우드 계정에 사용하려는 이름입니다.
-type	클라우드 계정의 유형입니다. 지원되는 값은 다음과 같습니다. • amazon • openstack • rackspace • windowsazure • "windows azure" • azure
-username	추가할 클라우드 계정의 사용자 이름입니다. 이는 인증 프로세스에서 사용하는 자격 증명입니다. 속성은 클라우드 유형에 따라 다음과 같이 변합니다. • Amazon - 액세스 키 • OpenStack - 사용자 이름 • Rackspace - 사용자 이름 • Windows Azure - 저장소 계정 이름
-key	추가하려는 클라우드 계정의 인증 키입니다. 이는 인증 프로세스에서 사용하는 자격 증명입니다. 속성은 클라우드 유형에 따라 다음과 같이 변합니다.

옵션	설명
	• Amazon - 비밀 키 • OpenStack - API 키 • Rackspace - API 키 • Windows Azure - 액세스 키
-region	추가하려는 클라우드 계정의 지역입니다. OpenStack 및 Rackspace 계정에 대해서만 이 옵션이 필요합니다.
-tenantid	OpenStack 클라우드 계정을 인증하는 데 사용하는 ID입니다. OpenStack 계정에 대해서만 이 옵션이 필요합니다.
-authurl	OpenStack 클라우드 계정을 인증하는 데 사용하는 URL입니다. OpenStack 계정에 대해서만 이 옵션이 필요합니다.

예:

액세스 키 "akey" 및 비밀 키 "skey"를 사용하여 이름이 "Amazon S3 계정"인 새 클라우드 계정 추가:

```
>cmdutil /newcloudaccount -displayname "Amazon S3 Account" -type amazon -useername akey -key
skey
```

OpenDvmRepository

이 명령을 사용하면 AppAssure Core 또는 Rapid Recovery Core에서 생성된 기존 DVM 리포지토리를 열 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/opendvmrepository -localpath [local path] -sharepath [network share path] -shareusername [user
name for network share] -sharepassword [network share password]
```

명령 옵션

다음 표에서는 OpenDvmRepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 193. OpenDvmRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-localpath	로컬 Core의 DVM 리포지토리가 있는 폴더에 대한 경로.
-sharepath	CIFS 공유의 DVM 리포지토리가 있는 폴더에 대한 경로.
-shareusername	공유 폴더에 로그인하는 데 사용하는 사용자 이름.
-sharepassword	공유 폴더에 로그인하는 데 사용하는 암호.

예:

로컬 시스템의 기존 DVM 리포지토리 열기:

```
>cmdutil /opendvmrepository -localpath E:\Repository
```

Pause

관리자는 스냅숏을 일시 중지하거나 가상 시스템으로 내보내거나 Core를 복제할 수 있습니다. pause 명령에는 snapshot, vmexport 및 replication 등 3개의 매개 변수를 사용할 수 있지만, 매개 변수 하나만 지정할 수 있습니다. 시간 매개 변수를 지정할 경우 스냅숏을 특정 시간까지 일지 중지할 수 있습니다.

사용자는 다음 세 가지 방법으로 복제를 일시 중지할 수 있습니다.

- 모든 보호된 시스템에 대한 소스 Core에서(-[outgoing]).
  관리자가 소스 Core에서 발신 복제를 일시 중지하려면 원격 시스템 이름을 발신 복제 연결과 함께 지정해야 합니다.

  ```
  >cmdutil /pause replication /o 10.10.12.10
  ```
- 하나의 보호된 시스템에 대한 소스 Core에서(-protectedserver):
  ```
  >cmdutil /pause replication /protectedserver 10.10.12.97
  ```
- 대상 Core에서(-incoming).
  로컬 Core가 대상 Core일 경우 관리자는 수신 매개 변수를 사용하여 소스 Core를 지정함으로써 복제를 일시 중지할 수 있습니다.

  ```
  >cmdutil /pause replication /i 10.10.12.25
  ```

용도

이 명령의 사용법은 다음과 같습니다.

```
/pause [snapshot | vmexport | replication] -core [host name] -user [user name] -password
[password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host
name] -time [time string]
```

명령 옵션

다음 표에서는 pause 명령에 사용 가능한 옵션에 대해 설명합니다.

표 194. Pause 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-pause	[snapshots], [replication] 또는 [vmexport].
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	선택 사항. 선택된 Core의 모든 에이전트를 일시 중지합니다.
-protectedserver	선택 사항. 현재 보호된 서버를 일시 중지합니다.
-incoming	선택 사항. Core 시스템에 복제하는 원격 Core의 호스트 이름.
-outgoing	선택 사항. 데이터가 복제되는 원격 대상 Core의 호스트 이름.
-time	선택 사항. 스냅숏이 다시 작성될 '날짜-시간-분' 형식의 시간(스냅숏 일지 중지에만 해당).

예:

특정한 보호된 서버에 대한 스냅숏 작성 일시 중지:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4
```

보호된 서버에 대해 스냅숏 작성을 일시 중지하고 3일, 20시간, 50분 후에 다시 시작:

```
>cmdutil /pause snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4 -time 3-20-50
```

Core의 모든 보호된 시스템에 대해 가상 시스템으로 내보내기 일시 중지:

```
>cmdutil /pause vmexport -core 10.10.10.10 /user administrator -password 23WE@#$sdd –all
```

Core에서 특정한 보호된 시스템에 대해 발신 복제 일시 중지:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd –
protectedserver 10.10.1.76
```

대상 Core의 모든 보호된 시스템에 대해 발신 복제 일시 중지:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password -23WE@#$sdd –
outgoing 10.10.1.63
```

대상 Core의 모든 시스템에 대해 수신 복제 일시 중지:

```
>cmdutil /pause replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd –
incoming 10.10.1.82
```

Protect

protect 명령은 Core로 보호할 서버를 추가하기 위해 사용합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/protect -core [host name] -user [user name] -password [password] -repository [name] -agentname
[name | IP address] -agentusername [user name] -agentpassword [password] -agentport [port] -
volumes [volume names]
```

명령 옵션

다음 표에서는 protect 명령에 사용 가능한 옵션에 대해 설명합니다.

표 195. Protect 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-repository	보호된 시스템 데이터를 저장해야 하는 Core의 리포지토리 이름. 이름을 큰따옴표로 묶어야 합니다.
-agentname	보호할 서버의 이름 또는 IP 주소.
-agentusername	보호할 서버의 사용자 이름.
-agentpassword	보호할 서버의 암호.
-agentport	보호된 서버 포트 번호.
-volumes	보호할 볼륨 목록. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오(예: “c:” “d:”).

예:

Core를 사용하여 서버의 특정 볼륨 보호:

```
>cmdutil /protect -core 10.10.10.10 -username administrator -password 23WE@#$sdd -repository
“Repository 1” -agentname 10.10.9.120 -agentport 5002 -agentusername administrator
agentpassword 12345 -volumes “c:” “d:”
```

ProtectCluster

protectcluster 명령은 Core로 보호할 클러스터를 추가하기 위해 사용합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/protectcluster -core [host name] -user [user name] -password [password] -repository [name] -
clustername [name | IP address] -clusterusername [user name] -clusterpassword [password] -
clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes collection]
```

명령 옵션

다음 표에서는 protectcluster 명령에 사용 가능한 옵션에 대해 설명합니다.

표 196. ProtectCluster 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-repository	보호된 시스템 데이터를 저장해야 하는 Core의 리포지토리 이름. 이름을 큰따옴표로 묶어야 합니다.
-clustername	보호할 클러스터의 이름 또는 IP 주소.
-clusterusername	보호할 클러스터의 사용자 이름.
-clusterpassword	보호할 클러스터의 암호.
-clusterport	보호된 클러스터 서버 포트 번호.
-clustervolumes	보호할 볼륨 목록. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오(예: “c:” “d:”).
-clusternodes	각 노드에서 보호할 클러스터 노드와 볼륨 목록.

예:

Core를 사용하여 클러스터 서버의 특정 볼륨 보호:

```
>cmdutil /protectcluster -core 10.10.10.10 -username administrator -password 23WE@#$sdd -
repository “Repository 1” -clustername 10.10.8.150 -clusterport 8006 -clusterusername
clusterAdmin clusterpassword password -volumes “C:\ClusterStorage\Volume1” -clusternodes
nodeName 10.10.8.150 volumes “c:” nodeName 10.10.8.151 volumes “c:”
```

ProtectEsxServer

protectesxserver 명령은 VMware ESX(i) 가상 시스템을 보호 대상에 추가하는 경우 항상 사용할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/protectesxserver -core [host name] -user [user name] -password [password] -repository
[repository name] -server [name | IP address] -serverusername [user name] -serverpassword
[password for server login] -serverport [port] -virtualMachines [virtual machines collection |
all] -autoProtect [object ID or name collection]
```

명령 옵션

다음 표에서는 protectesxserver 명령에 사용 가능한 옵션에 대해 설명합니다.

표 197. ProtectEsxServer 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-repository	필수. Core에 연결되었으며, 가상 시스템을 보호하는 데 사용하려는 리포지토리 이름. **노트: 이름은 큰따옴표로 묶어야 합니다.**
-server	보호할 vCenter 또는 ESXi 서버의 이름 또는 IP 주소.
-serverusername	보호할 vCenter 또는 ESXi 서버에 로그인할 때 사용할 사용자 이름.
-serverpassword	보호할 vCenter 또는 ESXi 서버에 로그인할 때 사용할 암호.
-serverport	선택 사항. 보호할 vCenter 또는 ESXi 서버의 포트 번호.
-virtualmachines	선택 사항. 이 옵션을 사용하면 보호할 가상 시스템을 표시할 수 있습니다.
-autoprotect	선택 사항. 이 옵션을 사용하면 자동으로 보호할 새 가상 시스템을 표시할 수 있습니다.

예:

Core에서 vCenter 또는 ESXi 서버의 특정 가상 시스템을 보호합니다.

```
>cmdutil /protectesxserver -core 10.10.10.10 -user admin -password password -repository
"Repository 1" -server 10.10.8.150 -serverport 443 -serverusername root -serverpassword
password -virtualmachines "VM1" "VM2" -autoprotect "Folder1"
```

RemoveAgent

RemoveAgent 명령을 사용하여 보호된 시스템을 Core 보호 환경에서 제거하고, 필요에 따라 제거된 시스템의 복구 지점을 삭제할 수 있습니다. 복구 지점을 삭제하지 않는 경우 Rapid Recovery에서는 복구 지점을 유지하고 복구 지점 전용 시스템으로 레이블을 붙입니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/removeagent -core [host name] -user [user name] -password [password] -protectedserver [name | IP address] -deleterecoverypoints
```

명령 옵션

다음 표에서는 RemoveAgent 명령에 사용 가능한 옵션에 대해 설명합니다.

표 198. RemoveAgent 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	보호에서 제거할 서버의 이름 또는 IP 주소.
-deleterecoverypoints	선택 사항. 제거할 시스템에서 모든 복구 지점을 삭제합니다.

예:

시스템을 보호에서 제거하고 연결된 복구 지점 삭제:

```
>cmdutil /removeagent -protectedserver 10.10.1.1 -deleterecoverypoints
```

RemoveArchiveRepository

removearchiverepository 명령을 사용하여 Rapid Recovery Core에서 리포지토리를 삭제할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/removearchiverepository -core [host name] -user [user name] -password [password] name] -name
[archive repository name]
```

명령 옵션

다음 표에서는 removearchiverepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 199. RemoveArchiveRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-name	필수입니다. 아카이브 리포지토리 이름입니다.

예:

로컬 Core에서 “NewArchive”로 명명된 리포지토리를 제거합니다.

```
>cmdutil /removearchiverepository -name NewArchive
```

RemovePoints

removepoints 명령을 사용하여 보호된 시스템의 특정 복구 지점을 삭제할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/removepoints -core [host name] -user [user name] -password [password] -protectedserver [name |
IP address] -rpn [number | numbers] | -time [time string]
```

명령 옵션

다음 표에서는 removepoints 명령에 사용 가능한 옵션에 대해 설명합니다.

표 200. RemovePoints 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	복구 지점을 삭제할 서버의 이름 또는 IP 주소.
-rpn	선택 사항. 삭제할 복구 지점의 일련 번호이며, 번호를 얻으려면 `/list rps` 명령을 사용합니다. 명령 하나로 여러 복구 지점을 삭제하려면 여러 번호를 공백으로 구분하여 지정합니다.
-time	선택 사항. 생성 시간을 기준으로 삭제할 복구 지점을 결정합니다. 정확한 시간을 "mm/dd/yyyy hh:mm tt" 형식으로 지정합니다(예: "2/24/2012 09:00 AM"). 날짜 시간 값은 PC에 설정된 시간대로 지정해야 합니다.

예:

번호가 5와 7인 복구 지점 삭제:

```
>cmdutil /removepoints -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

RemoveScheduledArchive

이 명령을 사용하면 기존 Rapid Recovery 예약된 연속 아카이브를 중단할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/removescheduledarchive -core [host name] -user [user name] -password [password] name] -all -
ids [id | id1 id2]
```

명령 옵션

다음 표에서는 `removescheduledarchive` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 201. RemoveScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름입니다. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호입니다. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	이 옵션은 이 Core와 연관된 모든 예약된 아카이브를 제거할지 여부를 지정합니다.
-ids	이 옵션을 사용하면 제거하려는 각 예약된 아카이브의 ID를 나열할 수 있습니다. 여러 개의 ID는 공백으로 구분합니다.

예:

예약된 모든 아카이브 분리:

```
>cmdutil /removescheduledarchive -all
```

하나의 예약된 아카이브 분리:

```
>cmdutil /removescheduledarchive -ids 6c123c39-5058-4586-bd0c-7c375e72017b
```

RemoveVirtualStandby

이 명령을 사용하면 Rapid Recovery 명령 유틸리티에서 가상 시스템으로의 지속적인 데이터 내보내기를 중단할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/removevirtualstandby -core [host name] -user [user name] -password [password login] -
protectedserver [name] | -all
```

명령 옵션

다음 표에서는 removevirtualstandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 202. RemoveVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	가상 시스템의 이름 또는 공간으로 구분된 이름.

옵션	설명
-all	이 명령은 모든 예정된 가상 내보내기를 제거할지 여부를 지정합니다.

예:

모든 가상 대기 내보내기 제거:

```
>cmdutil /removevirtualstandby -all
```

두 대의 시스템에 대한 가상 대기 내보내기 제거:

```
>cmdutil /removevirtualstandby -protectedserver 10.10.35.48 10.10.35.69
```

Replicate

Replicate 명령을 사용하여 두 개의 Rapid Recovery Core 사이에서 복제를 설정할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/replicate -request [email | email customer ID] -targetserver [host name | hostname port |
hostname user name password | hostname port user name password] -replicationname [name] -
seeddrive [localpath | network path username password] [comment] -protectedserver [name | name
repository]
```

명령 옵션

다음 표에서는 Replicate 명령에 사용 가능한 옵션에 대해 설명합니다.

표 203. Replicate 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-request	선택 사항. 오프사이트 백업 및 재난 복구 서비스의 타사 공급자에 대한 구독을 사용하려는 경우 이 옵션을 지정합니다.
-targetserver	복제를 설정하려는 서버의 이름. 다음과 같은 매개 변수를 포함합니다. • port • user name • password

옵션	설명
	port 매개 변수는 선택 사항이고, 기본값은 8006입니다. request 옵션을 사용한 경우 대상 서버에 대한 사용자 이름과 암호도 사용해야 합니다.
-replicationname	선택 사항. request 옵션을 사용하지 않으면 복제 작업 이름을 사용합니다.
-seeddrive	선택 사항. 초기 데이터 전송에 대한 시드 드라이브를 지정하려면 이 옵션을 사용합니다. comment 매개 변수는 선택 사항입니다.
-protectedserver	복제하려는 보호된 시스템 목록. request 옵션을 사용하는 경우, 보호된 시스템의 이름 또는 IP 주소만 표시합니다. 그렇지 않으면 보호된 시스템과 해당하는 원격 리포지토리 이름을 모두 표시합니다.

예:

네트워크 공유에서 시드 드라이브를 사용하는 원격 Core로 두 개의 보호된 시스템을 복제합니다.

```
>cmdutil /replicate -targetserver 10.10.1.100 Administrator 123Q -replicationname
ReplicationName -seeddrive Network \\10.10.1.100\seeddrive Administrator 123Q -protectedserver
10.10.1.1 Repository1 10.10.1.2 Repository2
```

복제

replication 명령을 사용하여 두 Rapid Recovery Core 간의 기존 복제를 제어하고 보류 중인 복제 요청을 관리할 수 있습니다.

노트: 이 명령은 Core 간에 페어링이라는 연결을 설정하고 초기 데이터 전송을 위해 시드 드라이브를 사용하는 Replicate 명령 다음에 사용합니다. 이 명령에 대한 자세한 내용은 Replicate을(를) 참조하십시오.

용도

이 명령의 사용법은 다음과 같습니다.

```
/replication [-list [incoming | outgoing | pending] -accept | -deny | -ignore | -delete | -
edit] -id [replication ID] -protectedserver [name | name repository] -responsecomment [comment]
-deleterecoverypoints -scheduletype [type] -dailystarttime [time] -dailyendtime [time] -
weekdaystarttime [time] -weekdayendtime [time] -weekendstarttime [time] -weekendendtime [time]
```

명령 옵션

다음 표에서는 replication 명령에서 사용할 수 있는 옵션에 대해 설명합니다.

표 204. Replication 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-list	수신 또는 발신 복제 작업 또는 보류 중인 복제 요청 목록.
-accept	복제 요청을 수락합니다.
-deny	복제 요청을 거부합니다.
-ignore	복제 요청을 무시합니다.
-delete	복제 작업에서 기존 복제 작업 또는 시스템을 삭제하려면 이 옵션을 사용합니다. 전체 복제 관계를 삭제하려면 -id 매개 변수만 지정하고, 복제에서 특정 시스템만 삭제하려면 -id 및 -protectedserver 매개 변수를 둘 다 지정합니다.
-edit	기존 복제 작업의 일정을 편집합니다.
-id	복제 작업 또는 보류 중인 복제 요청의 식별자. 원격 Core ID, 호스트 이름, 고객 ID, 이메일 주소 또는 보류 중인 복제 요청 ID일 수 있습니다.
-protectedserver	복제 요청에 응답할 때 보호된 서버 목록에 리포지토리 이름이나 ID로 응답을 적용하려면 이 옵션을 사용합니다. 모든 요청된 시스템에 응답을 적용하려면 "all" 매개 변수를 사용합니다.
-responsecomment	보류 중인 복제 요청에 대한 응답에 제공하는 설명.
-deleterecoverypoints	삭제된 복제 시스템에서 특정 복구 지점을 함께 제거해야 하는 경우 이 옵션을 사용합니다.
-scheduletype	-edit 옵션을 사용하는 경우 이 옵션은 복제 일정의 유형을 지정합니다. 다음 4개 값 중 하나를 포함합니다. • atalltimes - 언제든지 자동으로 복제합니다. • daily - 매일 복제합니다. -dailystarttime 및 -dailyendtime 매개 변수를 지정합니다. • custom - 매일 복제를 사용할 때 이 값을 사용하여 평일 또는 주말에 복제를 예약합니다. -weekdaystarttime, -weekdayendtime, -weekendstarttime 및 -weekendendtime 매개 변수를 지정합니다.
-dailystarttime	-scheduletype 옵션의 daily 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 하루 중 복제를 시작할 가장 이른 시간을 지정하는 데 이 옵션을 사용합니다.
-dailyendtime	-scheduletype 옵션의 daily 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 하루 중 복제를 시작할 가장 늦은 시간을 지정하는 데 이 옵션을 사용합니다.
-weekdaystarttime	-scheduletype 옵션의 custom 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 평일에 복제를 시작할 가장 이른 시간을 지정하는 데 이 옵션을 사용합니다.
-weekdayendtime	-scheduletype 옵션의 custom 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 평일에 복제를 시작할 가장 늦은 시간을 지정하는 데 이 옵션을 사용합니다.
-weekendstarttime	-scheduletype 옵션의 custom 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 주말에 복제를 시작할 가장 이른 시간을 지정하는 데 이 옵션을 사용합니다.
-weekendendtime	-scheduletype 옵션의 custom 값에만 사용합니다. 복제가 발생해야 할 일정 시간을 설정하는 데 사용됩니다. 주말에 복제를 시작할 가장 늦은 시간을 지정하는 데 이 옵션을 사용합니다.

예:

모든 수신 복제 나열:

```
>cmdutil /replication -list incoming
```

두 대의 보호 시스템에 대해 보류 중인 복제 요청 수락:

```
>cmdutil /replication -accept -id customer@email.address -protectedserver 10.10.1.1 Repository1
10.10.1.2 Repository2 -responsecomment A response comment
```

보류 중인 복제 요청 거부:

```
>cmdutil /replication -deny -id customer@email.address
```

복제된 복구 지점과 함께 기존 복제 삭제:

```
>cmdutil /replication -delete -id RemoteServerHostname -deleterecoverypoints
```

기존 복제에서 두 대의 시스템 제거:

```
>cmdutil /replication -delete -id "156d7a46-8e44-43f4-9ed8-60d998e582bf" -protectedserver
10.10.1.1 10.10.1.2
```

지정한 평일 및 주말 시간으로 복제 일정 편집:

```
>cmdutil /replication -edit -id RemoteServerHostName -scheduletype custom -weekdaystarttime
"9:00 AM" -weekdayendtime "6:00 PM" -weekendstarttime "9:00 AM" -weekendendtime "6:00 PM"
```

RestoreAgent

`restoreagent` 명령을 사용하면 특정 Rapid Recovery 복구 지점에서 보호된 시스템이나 볼륨을 복원할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/restoreagent -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs |
names | all] -targetmachine [name] -targetvolume [volume name] -forcedismount -autorestart
```

명령 옵션

다음 표에서는 `restoreagent` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 205. RestoreAgent 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	복원할 서버의 이름 또는 IP 주소.
-rpn	시스템을 복원하는 데 사용하려는 복구 지점의 식별 번호. 올바른 번호를 찾으려면 /list rps 명령을 사용합니다.
-volumes	복원할 볼륨의 ID 또는 이름. 모든 보호된 볼륨을 복원하려면 -volumes all을 사용합니다.
-targetmacchine	보호된 시스템을 복원하려는 시스템의 이름.
-targetvolume	시스템을 복원하려는 볼륨의 이름 또는 ID.
-forcedismount	선택 사항. 이 옵션을 사용하면 필요 시 데이터베이스를 강제 분리할 수 있습니다.
-autorestart	선택 사항. Exchange Server 시스템을 다시 시작해야 하는 경우 이 명령을 사용합니다.

예:

데이터베이스 강제 분리 옵션을 포함하여 IP 주소가 192.168.20.130인 보호된 시스템으로 시스템 복원:

```
>cmdutil /restoreagent -protectedserver 192.168.20.130 -rpn 259 -volumes "F:" "E:" "C:" -
targetmachine 192.168.20.174 -targetvolume "E:" "G:" "F:" -forcedismount
```

RestoreArchive

이 명령은 로컬 아카이브 또는 공유 위치에 있는 아카이브를 복원하고 복원된 데이터를 지정된 리포지토리에 저장합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/restorearchive -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address] -repository [name] -archiveusername [name] -archivepassword
[password] -path [location]
```

명령 옵션

다음 표에서는 restorearchive 명령에 사용 가능한 옵션을 설명합니다.

표 206. RestoreArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	모든 보호된 시스템의 데이터를 아카이브 파일에서 복원합니다.
-protectedserver	복원할 복구 지점이 있는 보호된 시스템. 여러 시스템 이름을 큰따옴표로 묶고 공백으로 구분해서 지정할 수 있습니다.
-repository	복원된 복구 지점을 저장해야 하는 Core의 리포지토리 이름. 이름을 큰따옴표로 묶어야 합니다.
-archiveusername	선택 사항. 원격 시스템의 사용자 이름. 네트워크 경로에만 필요합니다.
-archivepassword	선택 사항. 원격 시스템 암호. 네트워크 경로에만 필요합니다.
-path	복원할 아카이브 데이터의 위치. 예: d:\work\archive 또는 network path \\servename\sharename.

예:

모든 보호된 서버의 아카이브 데이터 복원:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -all -repository repository1 -path d:\work\archive
```

특정한 보호된 서버의 아카이브 데이터 복원:

```
>cmdutil /restorearchive -core 10.10.10.10 -username administrator -password 23WE@#$sdd -protectedserver "10.10.20.30" "20.10.10.5" -repository repository1 -path d:\work\archive
```

RestoreUrc

restoreurc 명령을 사용하면 특정 Rapid Recovery 복구 지점에서 URC(Universal Recovery Console)를 사용하는 Bare Metal 시스템으로 보호된 시스템 또는 볼륨을 복원할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/restoreurc -protectedserver [name | IP address] -rpn [recovery point number] -volumes [IDs | names | all] -targetmachine [IP address] -urcpassword [password from the URC] -targetdisk [disk number | all]
```

명령 옵션

다음 표에서는 restoreurc 명령에 사용 가능한 옵션에 대해 설명합니다.

표 207. RestoreUrc 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	URC를 복원하려는 서버의 이름 또는 IP 주소.
-rpn	시스템을 복원하는 데 사용하려는 복구 지점의 식별 번호. 올바른 번호를 찾으려면 /list rps 명령을 사용합니다.
-volumes	복원할 볼륨의 ID 또는 이름. 모든 보호된 볼륨을 복원하려면 -volumes all을 사용합니다.
-targetmacchine	보호된 시스템을 복원하려는 시스템의 이름.
-urcpassword	URC의 인증 키.
-targetdisk	시스템을 복원하려는 디스크 수. URC를 사용하여 시스템에서 모든 디스크를 선택하려면 -targetdisk all을 사용합니다.

예:

URC를 사용하는 시스템의 디스크 0과 디스크 1로 시스템을 복원합니다. 이때 URC 시스템의 IP 주소는 192.168.20.175입니다.

```
>cmdutil /restoreurc -protectedserver 192.168.20.130 -rpn 259 -volumes "C:" "E:" -targetmachine
192.168.20.175 -urcpassword ******** -targetdisk 0 1
```

Resume

관리자는 이 명령을 사용하여 스냅숏 작성을 다시 시작하고 가상 시스템으로 내보내고 복제할 수 있습니다. 매개 변수를 사용하여 다시 시작해야 함을 지정해야 합니다. 유효한 매개 변수는 snapshot, vmexport 및 replication입니다. 자세한 내용은 Pause을(를) 참조하십시오.

용도

이 명령의 사용법은 다음과 같습니다.

```
/resume [snapshot | vmexport | replication] -core [host name] -user [user name] -password
[password] -all | -protectedserver [name | IP address] -incoming [host name] | outgoing [host
name] -time [time string]
```

명령 옵션

다음 표에서는 resume 명령에 사용 가능한 옵션에 대해 설명합니다.

표 208. Resume 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-restore	[snapshots], [replication] 또는 [vmexport].
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-all	선택된 Core의 모든 에이전트를 다시 시작합니다.
-protectedserver	현재 보호된 서버를 다시 시작합니다.
-incoming	Core 시스템에 복제하는 원격 Core의 호스트 이름.
-outgoing	데이터가 복제되는 원격 대상 Core의 호스트 이름.

예:

특정한 보호된 서버의 스냅숏 작성 다시 시작:

```
>cmdutil /resume snapshot -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.10.4
```

Core의 모든 보호된 시스템에 대해 가상 시스템으로 내보내기 다시 시작:

```
>cmdutil /resume vmexport -core 10.10.10.10 -user administrator -password 23WE@#$sdd -all
```

Core의 특정한 보호된 시스템에 대해 발신 복제 다시 시작:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.1.76
```

대상 Core의 모든 보호된 시스템에 대해 발신 복제 다시 시작:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
outgoing 10.10.1.63
```

대상 Core의 모든 시스템에 대해 수신 복제 다시 시작:

```
>cmdutil /resume replication -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
incoming 10.10.1.82
```

SeedDrive

Rapid Recovery 복제를 설정할 때 초기 데이터 전송에 대해 시드 드라이브를 사용할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/seeddrive [-list | -startcopy | -startconsume | -abandon] -path [local | network path] -
seeddriveusername [user name] -seeddrivepassword [password] -remotecore [name] [-targetcore
[name or IP] | -protectedserver [name] | -all] -usecompatibleformat
```

명령 옵션

다음 표에서는 seeddrive 명령에 사용 가능한 옵션에 대해 설명합니다.

표 209. SeedDrive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-list	확장된 정보를 포함하는 대기 중인 시드 드라이브 목록.
-startcopy	시드 드라이브로 데이터 복사를 시작합니다.
-startconsume	시드 드라이브를 사용하기 시작합니다.
-abandon	대기 중인 시드 드라이브 요청을 취소합니다.
-path	시드 드라이브의 로컬 또는 네트워크 경로.
-seeddriveusername	선택 사항. 시드 드라이브의 네트워크 위치에 대한 사용자 이름.
-seeddrivepassword	선택 사항. 시드 드라이브의 네트워크 위치에 대한 암호.
-targetcore	선택 사항. -copy 옵션과만 사용합니다. 원격 Core의 이름 또는 IP 주소입니다. 이 Core로 복제하는 모든 보호된 시스템은 시드 드라이브 복구 지점을 수신합니다.
-remotecore	-consume 옵션과만 사용합니다. 시드 드라이브 복구 지점을 만들거나 사용하는 원격 Core의 이름입니다.

옵션	설명
-protectedserver	복구 지점의 시드 드라이브를 만들거나 사용하는 데 사용할 보호된 시스템의 이름 또는 IP 주소. 예: -protectedserver "10.10.60.48" "10.10.12.101."
-all	이 옵션은 사용 가능한 보호된 시스템을 모두 사용할 것인지, 아니면 복사할 것인지 여부를 지정합니다.
-usecompatibleformat	새 아카이브 형식은 성능을 향상시킬 수 있지만, 이전 Core와 호환되지 않습니다. 기존 AppAssure Core로 작업을 수행할 때 이 옵션을 사용합니다.

예:

대기 중인 시드 드라이브를 표시합니다.

```
>cmdutil /seeddrive -list
```

네트워크 공유 위치에서 시드 드라이브로 두 개의 보호된 시스템을 복사합니다.

```
>cmdutil /seeddrive -startcopy -remotecore TargetCoreName -path \\10.10.1.1\Share\Seed\ -
seeddriveusername Administrator -seeddrivepassword 12345 -usecompatibleformat
```

시드 드라이브를 사용하기 시작합니다.

```
>cmdutil /seeddrive -startconsume -path \\10.10.1.1\Share\Seed\ -seeddriveusername
Adminsitrator -seeddrivepassword 12345 -remotecore RemoteCoreName
```

대기 중인 시드 드라이브 요청을 취소합니다.

```
>cmdutil /seeddrive -abandon RemoteCoreHostName
```

StartExport

`startexport` 명령은 보호된 시스템에서 가상 서버로 데이터를 한 번 내보내는 작업을 수행합니다. ESXi, VMware Workstation, Hyper-V 또는 VirtualBox 가상 시스템으로 내보낼 수 있습니다. ESXi로 내보내려면 thick 또는 thin 디스크 프로비저닝을 지정해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/startexport -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name] -
password [password] -protectedserver [name | IP address] -volumes [volume names] -rpn [recovery
point number | numbers] | -time [time string] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual hostport number] -hostusername [virtual host user name] -
hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning
[thin | thick] -diskmapping [automatic | manual | withvm] -targetpath [location] -pathusername
[user name] -pathpassword [password] [-uselocalmachine]
```

명령 옵션

다음 표에서는 `startexport` 명령에서 사용할 수 있는 옵션에 대해 설명합니다.

표 210. StartExport 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-exporttype	보호된 서버에서 ESXi 서버('esxi'), VMware Workstation 서버('vm'), Hyper-V 서버('hyperv') 또는 VirtualBox 서버('vb')로 내보내기를 수행합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	내보낼 복구 지점이 있는 보호된 시스템.
-volumes	선택 사항. 내보낼 볼륨 이름의 목록. 지정하지 않으면 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 예: "c:" "d:". 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.
-rpn	선택 사항. 내보낼 복구 지점의 일련 번호(번호를 얻으려면 Get-RecoveryPoints 명령 사용). 'time'과 'rpn' 옵션을 모두 지정하지 않으면 최근 복구 지점이 내보내집니다.
-time	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. 정확한 시간을 "mm/dd/yyyy hh:mm tt" 형식으로 지정해야 합니다(예: "2/24/2012 09:00 AM"). 날짜 시간 값은 PC에 설정된 시간대로 지정해야 합니다. 참고: 'time'과 'rpn' 옵션을 모두 지정하지 않으면 최근 복구 지점이 내보내집니다.
-vmname	가상 시스템의 Windows 이름.
-hostname	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트 이름.
-linuxhostname	VirtualBox 내보내기에만 해당. 가상 서버 호스트 이름.
-hostport	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 포트 번호.
-hostusername	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트의 사용자 이름.
-hostpassword	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트의 암호.
-ram	특정 크기의 RAM을 가상 서버에 할당하려면 이 옵션을 사용합니다.
-usesourceram	선택 사항. 원본 시스템에 포함된 가상 서버에 동일한 크기의 RAM을 할당하려면 이 옵션을 사용합니다.
-diskprovisioning	ESXi 내보내기에 대해서만 이 옵션을 사용합니다. 선택 사항. 가상 시스템에 할당할 디스크 공간의 크기. 다음 두 가지 사양 중 하나를 사용합니다. • Thick - 이 사양은 보호된 시스템에 있는 원래 드라이브와 동일한 크기의 가상 디스크를 만듭니다. • Thin - 이 사양은 원래 드라이브에서 사용된 실제 디스크 공간 크기에 약간의 메가바이트를 추가하여 할당합니다. 기본 사양은 "thin"입니다.
-diskmapping	ESXi 내보내기에 대해서만 이 옵션을 사용합니다. 선택 사항. 이 옵션은 보호된 시스템에서 가상 시스템으로 디스크를 매핑하는 방법을 결정합니다. 다음 값 중 하나를 사용합니다. • auto - 이 값은 디스크를 자동으로 매핑합니다. • manual - 이 값을 사용하여 디스크를 수동으로 매핑할 수 있습니다. • withvm - 이 값은 선택하는 데이터 저장소에 가상 디스크를 저장합니다.

옵션	설명
	기본값은 "auto"입니다.
-targetpath	VMware Workstation 또는 VirtualBox 내보내기에만 해당. 이 옵션은 가상 시스템 파일을 저장할 폴더에 대한 로컬, 네트워크 경로 또는 Linux 경로(VirtualBox만 해당)를 지정합니다.
-pathusername	VMware Workstation 내보내기에만 해당. 네트워크 시스템의 사용자 이름입니다. -targetpath 옵션에 네트워크 경로를 지정할 때만 필요합니다.
-pathpassword	VMware Workstation 내보내기에만 해당. 네트워크 시스템의 암호입니다. -targetpath 옵션에 네트워크 경로를 지정할 때만 필요합니다.
-uselocalmachine	Hyper-V 내보내기에만 해당. 선택 사항. 로컬 Hyper-V 서버에 연결하려면 이 명령을 사용합니다. 이 옵션은 -hostname, -hostport, -hostusername 및 -hostpassword 옵션을 무시합니다.

예:

RAM 및 디스크 크기가 보호된 소스 서버와 같은 특정 이름의 ESXi 가상 시스템으로 데이터 내보내기:

```
>cmdutil     /startexport -exporttype esxi -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport
443 -hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

4번 복구 지점을 사용하여 보호된 데이터가 있는 로컬 드라이브에 VMware Workstation 시스템 파일 만들기:

```
>cmdutil /startexport -exporttype vmstation -core 10.10.10.10 -user administrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -rpn 4 -vmname Win2008-Smith -targetpath c:
\virtualmachines -ram 4096
```

원격 시스템에 저장할 Hyper-V 시스템 파일 만들기:

```
>cmdutil /startexport -exporttype hyperv -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmlocation \\WIN7-Bobby\virtualmachines -hostname 10.10.10.23
-hostport 443 -hostusername root -hostpassword 12QWsdxc@# -ram 4096
```

UpdateRepository

updaterepository 명령은 기존 DVM 리포지토리에 새 저장 위치를 추가합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/updaterepository -name [repository name] -size [size of the repository] [-datapath [data path]
-metadatapath [metadata path] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password] -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 updaterepository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 211. UpdateRepository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-name	리포지토리 이름.
-size	리포지토리 저장 위치의 크기. 사용 가능한 단위는 b, Kb, Mb, Gb, Tb 및 Pb입니다.
-datapath	로컬 위치에만 해당. 리포지토리 저장 위치의 데이터 경로를 결정합니다.
-metadatapath	로컬 위치에만 해당. 리포지토리 저장 위치의 메타데이터 경로를 결정합니다.
-uncpath	공유 위치에만 해당. 리포지토리 저장 위치의 데이터 및 메타데이터 경로를 결정합니다.
-shareusername	공유 위치에만 해당. 공유 위치에 대한 사용자 이름을 결정합니다.
-sharepassword	공유 위치에만 해당. 공유 위치 암호를 결정합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.

예:

로컬 DVM 리포지토리에 새 저장 위치를 생성합니다.

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -datapath d:\repository -
metadatapath d:\repository -core 10.10.10.10:8006 -username administrator -password 23WE@#$sdd
```

공유 위치에 DVM 리포지토리의 저장 위치를 생성합니다.

```
>cmdutil /updaterepository -name "Repository 1" -size 200Gb -uncpath \\share\repository -
shareusername login -sharepassword 23WE@#$sdd -core 10.10.10.10:8006 -username administrator -
password 23WE@#$sdd
```

버전

version 명령은 지정된 서버에 설치된 Rapid Recovery 소프트웨어 버전에 대한 정보를 표시합니다. Core 또는 보호된 서버를 지정하지 않는 경우 반환된 정보는 현재 사용 중인 Core에 적용됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/[version | ver] -protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 version 명령에 사용 가능한 옵션에 대해 설명합니다.

표 212. Version 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	선택 사항. 버전 정보를 확인하려는 보호된 시스템. 보호된 시스템을 지정하지 않는 경우 사용 중인 Core 시스템에 대한 정보가 반환됩니다.

예:

현재 Rapid Recovery Core에 설치된 Rapid Recovery 버전에 대한 정보 표시:

```
>cmdutil /version
```

VirtualStandby

virtualstandby 명령을 사용하여 Rapid Recovery로 보호되는 시스템에서 호환되는 가상 시스템으로 데이터를 내보낼 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
/virtualstandby -edit -exporttype [esxi | vm | hyperv | vb] -core [host name] -user [user name]
-password [password] -protectedserver [name | IP address] -volumes [volume names] -vmname
[virtual machine name] -gen2 -hostname [virtual host name] -hostport [virtual host port number]
-hostusername [virtual host user name] -hostpassword [virtual host password] [-ram [total
megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic | manual |
withvm] -targetpath [location] -pathusername [user name] -pathpassword [password] [-uselocal
machine] -initialexport
```

명령 옵션

다음 표에서는 virtualstandby 명령에서 사용할 수 있는 옵션에 대해 설명합니다.

표 213. VirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-exporttype	이 옵션은 보호된 시스템에서 다음 지정된 가상 서버 중 하나로 데이터를 내보냅니다. • esxi(ESXi) • vm(VMware Workstation) • hyperv(Hyper-V) • vb(VirtualBox)
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템의 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 입력하지 않으면 로그온되어 있는 사용자의 자격 증명이 사용됩니다.
-protectedserver	내보낼 복구 지점의 보호된 시스템을 지정하려면 이 옵션을 사용합니다.
-volumes	선택 사항. 내보낼 볼륨의 이름을 나열하려면 이 옵션을 사용합니다. 볼륨을 지정하지 않으면 복구 지점에 있는 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분합니다. 예: "c:" "d:". 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.
-ram	특정 크기의 RAM을 가상 서버에 할당하려면 이 옵션을 사용합니다.
-usesourceram	선택 사항. 원본 시스템에 포함된 가상 서버에 동일한 크기의 RAM을 할당하려면 이 옵션을 사용합니다.
-vmname	가상 시스템의 Windows 이름.

-gen2	선택 사항. 이 옵션은 VM 서버의 Generation 2를 지정합니다. 세대를 지정하지 않으면 명령에서 Generation 1을 사용합니다. 다음 운영 체제가 Generation 2를 지원합니다.
	• Windows
	  • Windows Server 2012 R2
	  • Windows 8.1
	• Ubuntu Linux
	  • CentOs
	  • RHEL
	  • Oracle Linux 7

-hostname	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트 이름.
-linuxhostname	VirtualBox 내보내기에만 해당. 가상 서버 호스트 이름.
-hostport	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 포트 번호.
-hostusername	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트의 사용자 이름.
-hostpassword	ESXi 및 Hyper-V 가상 내보내기에만 해당. 가상 서버 호스트의 암호.
-diskprovisioning	ESXi 내보내기에만 해당. 선택 사항. 가상 시스템에 할당할 디스크 공간의 크기. 다음 두 가지 사양 중 하나를 사용합니다. • Thick - 이 사양은 보호된 시스템에 있는 원래 드라이브와 동일한 크기의 가상 디스크를 만듭니다.

옵션	설명
	• Thin - 이 사양은 원래 드라이브에서 사용된 실제 디스크 공간 크기에 약간의 메가바이트를 추가하여 할당합니다. 기본 사양은 "thin"입니다.
-diskmapping	ESXi 내보내기에만 해당. 선택 사항. 이 옵션은 보호된 시스템에서 가상 시스템으로 디스크를 매핑하는 방법을 결정합니다. 다음 값 중 하나를 사용합니다. • auto - 이 값은 디스크를 자동으로 매핑합니다. • manual - 이 값을 사용하여 디스크를 수동으로 매핑할 수 있습니다. • withvm - 이 값은 선택하는 데이터 저장소에 가상 디스크를 저장합니다. 기본값은 "auto"입니다.
-targetpath	VMware Workstation 또는 VirtualBox 내보내기에만 해당. 이 옵션은 가상 시스템 파일을 저장할 폴더에 대한 로컬, 네트워크 경로 또는 Linux 경로(VirtualBox만 해당)를 지정합니다.
-pathusername	VMware Workstation 내보내기에만 해당. 네트워크 시스템의 사용자 이름입니다. -targetpath 옵션에 네트워크 경로를 지정할 때만 필요합니다.
-pathpassword	VMware Workstation 내보내기에만 해당. 네트워크 시스템의 암호입니다. -targetpath 옵션에 네트워크 경로를 지정할 때만 필요합니다.
-uselocalmachine	Hyper-V 내보내기에만 해당. 선택 사항. 로컬 Hyper-V 서버에 연결하려면 이 명령을 사용합니다. 이 옵션은 -hostname, -hostport, -hostusername 및 -hostpassword 옵션을 무시합니다.
-edit	선택 사항. 이 옵션을 사용하면 기존 가상 시스템을 편집할 수 있습니다. -exporttype 및 -initialexport 옵션을 무시합니다.
-initialexport	선택 사항. 이 옵션은 지속적 가상 대기를 구성한 후 초기 주문형 가상 시스템 내보내기를 시작할지 지정합니다.

예:

보호된 소스 서버의 이름, RAM 크기 및 디스크 크기와 함께 ESXi 가상 시스템으로 가상 대기 내보내기 설정:

```
>cmdutil /virtualstandby -exporttype esxi -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -hostname 10.10.10.23 -hostport 443 -
hostusername root -hostpassword 12QWsdxc@# -usesourceram -diskprovisioning thick
```

로컬 드라이브에 있는 VMware Workstation 시스템 파일로 가상 대기 내보내기 설정:

```
>cmdutil /virtualstandby -exporttype vm -core 10.10.10.10 -user administrator -password 23WE@#
$sdd -protectedserver 10.10.5.22 -vmname Win2008-Smith -targetpath c:\virtualmachines -ram 4096
```

Hyper-V 시스템 파일로 가상 대기 내보내기를 설정하고 원격 시스템에 저장:

```
>cmdutil /virtualstandby -exporttype hyperv -core 10.10.10.10 -user adminstrator -password
23WE@#$sdd -protectedserver 10.10.5.22 -vmname Win20008-Smith -vmlocation \\WIN7-Bobby
\virtualmachines -hostname 10.10.10.23 -hostport 443 -hostusername root -hostpassword
12QWsdxc@# -ram 4096
```

현지화

Rapid Recovery Core가 설치된 동일한 시스템에서 실행할 때 Rapid Recovery Command Line Management 유틸리티에서는 Rapid Recovery Core에 대해 설정된 언어가 표시 언어로 사용됩니다. 이 릴리스에서는 한국어, 영어, 중국어(간체), 프랑스어, 독일어, 일본어, 포르투갈어(브라질) 및 스페인어가 지원됩니다.

Rapid Recovery Command Line Management 유틸리티가 별도의 시스템에 설치된 경우에는 영어만 지원됩니다.

A

Core Console 참조사항

이 부록에는 Rapid Recovery Core Console에서 사용할 수 있는 다양한 아이콘과 기능을 설명하는 표가 포함되어 있습니다. *Dell Data Protection | Rapid Recovery 사용자 안내서*의 Dell Data Protection | Rapid Recovery 챕터에 대한 보완 자료로 제공합니다.

주제:

- Core Console 사용자 인터페이스 보기
- Protected Machines(보호되는 시스템) 창 보기

Core Console 사용자 인터페이스 보기

Core Console은 사용자가 Rapid Recovery와 상호 작용하기 위해 사용하는 기본 UI(사용자 인터페이스)입니다. Rapid Recovery Core Console에 로그인하면 다음과 같은 요소가 표시됩니다.

표 214. Core Console에 포함된 UI 요소

UI 요소	설명
브랜드 영역	일반적인 환경에서는 Core Console의 왼쪽 측면 맨 위에 Dell 로고가 포함된 제품 전체 이름이 표기되어 있습니다. 브랜딩 영역을 아무 곳이나 클릭하면 웹 브라우저에서 새 탭이 열리면서 지원 웹 사이트에 있는 제품 설명서가 표시됩니다.
단추 모음	브랜딩 영역의 오른쪽에 표시되는 단추 모음에는 Core Console의 어느 곳에서나 액세스할 수 있는 단추가 포함되어 있습니다. 이러한 단추는 마법사를 실행하여 시스템 보호, 복구 지점에서 복원 수행, 아카이브 생성, 연결 또는 가져오기, 소스 Core에서 대상 Core로 복제 등과 같은 일반적인 작업을 수행할 수 있습니다. 단추 모음에 있는 각 단추는 표 215. 단추 모음 단추 및 메뉴 표에 자세히 설명되어 있습니다.
실행 중인 작업 수	현재 실행 중인 작업 수를 표시합니다. 이 값은 시스템 상태에 따라 변경됩니다. 드롭다운 메뉴를 클릭하면 현재 실행 중인 모든 작업에 대한 상태 요약이 표시됩니다. **X**를 클릭하면 해당 작업을 취소할 수 있습니다.
도움말 드롭다운 메뉴	**도움말** 메뉴에는 다음 옵션이 있습니다. • **도움말**. 제품 도움말로 연결되며 별도의 브라우저 창에서 열립니다. • **설명서**. Dell 지원 웹 사이트의 Rapid Recovery 기술 문서로 연결됩니다. • **지원**. 라이브 채팅, 비디오 자습서, Rapid Recovery 기술 문서, 자주 물어보는 질문 등에 액세스할 수 있는 Dell 지원 웹 사이트로 연결됩니다. • **빠른 시작 안내서**. 빠른 시작 안내서는 Rapid Recovery를 구성 및 사용하기 위해 권장되는 작업을 단계별로 안내합니다. 이 기능을 사용하지 않도록 설정하지 않은 경우 이 안내서는 Core Console에 로그인할 때마다 자동으로 열립니다. 빠른 시작 안내서는 도움말 메뉴에서도 열 수 있습니다. Quick Start Guide(빠른 시작 안내서)에 대한 자세한 내용은 빠른 시작 안내서 이해에서 확인하십시오. • **정보**. 소프트웨어의 버전 정보 및 설명이 표시된 Dell Data Protection | Rapid Recovery Core 정보 대화 상자를 엽니다.
서버 날짜 및 시간	Core Console의 오른쪽 상단에 Rapid Recovery Core 서비스를 실행 중인 시스템의 현재 시간이 표시됩니다. 시간 위에 마우스를 올려 놓으면 서버 날짜가 표시됩니다. 이것은 로깅, 예약, 보고 등의 이벤트에 대해 시스템에서 기록하는 날짜 및 시간입니다. 예를 들어, 보호 일정 적용 시 Core Console에 표시된 시간이 사용됩니다. 브라우저를 실행 중인 데이터베이스 서버 또는 클라이언트 시스템의 시간대가 다른 경우에도 마찬가지입니다.

UI 요소	설명
아이콘 모음	아이콘 모음에는 Core Console에서 액세스할 수 있는 주요 기능을 나타내는 그래픽이 포함되어 있습니다. 브랜딩 영역의 바로 아래에 있는 UI(사용자 인터페이스) 왼쪽 측면에 나타납니다. 아이콘 모음에서 적절한 항목을 클릭하면 해당 기능을 관리할 수 있는 UI 섹션으로 이동합니다. 아이콘 모음에 있는 각 아이콘은 표 216. 아이콘 모음 표에 자세히 설명되어 있습니다.
왼쪽 탐색 영역	왼쪽 탐색 영역은 아이콘 모음 아래에 있는 사용자 인터페이스 왼쪽 측면에 나타납니다. · 왼쪽 탐색 영역에는 텍스트 필터 및 Protected Machines(보호된 시스템) 메뉴가 포함되어 있습니다. · 복제를 이 Core에 추가한 경우 이 영역에는 복제된 시스템 메뉴가 포함됩니다. · 보호에서 제거되었지만 복구 지점이 저장된 시스템이 있는 경우 이 영역에는 복구 지점만 메뉴가 포함됩니다. · 사용자 지정 그룹을 추가한 경우 이 영역에는 사용자 지정 그룹 메뉴가 포함됩니다. · 아카이브에 연결된 경우 이 영역에는 연결된 아카이브 메뉴가 포함됩니다. 왼쪽 탐색 영역을 표시하거나 표시하지 않을 수 있습니다. 이 기능은 UI의 기본 탐색 영역에 더 많은 콘텐츠를 표시해야 하는 경우 유용합니다. 이 섹션을 숨기려면 왼쪽 탐색 영역과 기본 탐색 영역 사이의 회색 경계를 클릭합니다. 이 UI 요소를 다시 표시하려면 회색 경계를 다시 클릭합니다. 왼쪽 탐색 영역에 있는 각 요소는 표 218. 왼쪽 탐색 영역 및 메뉴 표에 자세히 설명되어 있습니다.
상황별 도움말	Rapid Recovery Core Console에서 도움말 아이콘(파란색 물음표)을 클릭할 때마다 두 개의 프레임이 사용된 크기 조정이 가능한 브라우저 창이 열립니다. 왼쪽 프레임에는 Dell Rapid Recovery 사용자 안내서의 주제 항목을 표시하는 탐색 트리가 포함되어 있습니다. 오른쪽 프레임은 선택한 도움말 항목에 대한 내용을 표시합니다. 지정된 시간에 도움말 탐색 트리는 선택한 항목의 계층 구조에서 위치를 나타내도록 확장됩니다. 이 상황별 도움말 기능을 사용하여 모든 사용자 안내서 항목을 탐색할 수 있습니다. 항목 탐색을 마쳤으면 브라우저를 닫으십시오. **도움말** 메뉴의 **도움말** 옵션에서 도움말을 열 수도 있습니다.

단추 모음

단추 모음에 대한 상세 정보는 다음 표에 제시됩니다.

표 215. 단추 모음 단추 및 메뉴

UI 요소	설명	
단추 모음: 단추 및 메뉴 보호		**보호** 단추를 클릭하면 시스템 보호 마법사가 실행되어 Rapid Recovery Core에서 단일 시스템을 보호할 수 있습니다. 또한 다른 보호 옵션의 경우 이 단추 옆의 드롭다운 메뉴에 액세스할 수 있으며 다음과 같은 옵션이 포함되어 있습니다. · **시스템 보호** 옵션은 시스템 보호 마법사를 실행하여 단일 시스템을 보호할 수 있는 또 다른 방법입니다. · **클러스터 보호** 옵션을 통해서는 서버 클러스터에 연결할 수 있습니다. · **다중 시스템 보호** 옵션은 두 대 이상의 시스템을 동시에 보호할 수 있는 다중 시스템 보호 마법사를 엽니다. · **Agent 소프트웨어 배포** 옵션을 사용하면 Rapid Recovery Agent 소프트웨어를 한 대 이상의 시스템에 동시에 설치할 수 있습니다. 이 기능은 Deploy Agent Software Wizard(Agent 소프트웨어 배포 마법사)를 사용합니다.
단추 모음: 단추 및 메뉴 복원		**복원** 단추는 보호된 컴퓨터에서 저장된 복구 지점에서 데이터를 복원할 수 있는 컴퓨터 복원 마법사를 엽니다.

UI 요소	설명
	또한 다른 복원 또는 내보내기 옵션의 경우 이 단추 옆의 드롭다운 메뉴에 액세스할 수 있으며 다음과 같은 옵션이 포함되어 있습니다. • **시스템 복원** 옵션은 시스템 복원 마법사를 실행하여 데이터를 복원할 수 있는 또 다른 방법입니다. • **복구 지점 탑재** 옵션은 보호된 시스템의 복구 지점을 탑재할 수 있는 탑재 마법사를 실행합니다. • **VM 내보내기** 옵션은 내보내기 마법사를 엽니다. 이 마법사를 사용하면 Rapid Recovery Core에 저장된 복구 지점에서 가상 시스템을 만들 수 있습니다. 한 번 내보내기를 만들거나 보호된 컴퓨터의 스냅숏을 작성할 때마다 계속 업데이트되는 VM에 대한 매개 변수를 정의할 수 있습니다.
단추 모음: 단추 및 메뉴 아카이브	**아카이브** 단추는 아카이브 마법사를 엽니다. 이 마법사를 사용하여 선택한 복구 지점에서 일회성 아카이브를 생성하거나 아카이브를 생성한 뒤 정의한 일정에 따라 해당 아카이브에 지속적으로 저장할 수 있습니다. 또한 다른 아카이브 옵션의 경우 이 단추 옆의 드롭다운 메뉴에 액세스할 수 있으며 다음과 같은 옵션이 포함되어 있습니다. • **아카이브 생성** 옵션은 아카이브 생성 마법사를 실행하여 일회성 아카이브를 생성하거나 지속적으로 아카이브할 수 있는 또 다른 방법입니다. • **아카이브 가져오기** 옵션은 아카이브 가져오기 마법사를 실행하여 아카이브를 가져올 수 있습니다. • **아카이브 연결** 옵션은 아카이브를 탑재하여 콘텐츠를 파일 시스템으로 읽을 수 있습니다.
단추 모음: 복제 단추	**복제** 단추는 복제 마법사를 엽니다. 이 마법사에서 대상 Core를 지정하고, 소스 Core에서 보호된 시스템을 선택하며, 선택한 시스템의 복구 지점을 사용자가 지정한 리포지토리의 대상 Core로 복제할 수 있습니다. 정의할 때 복제를 일시 중지하거나 복제를 즉시 시작할 수 있습니다. 또한, 기존 복구 지점의 데이터를 대상 Core에 복사할 때 시드 드라이브를 사용할지 여부를 지정할 수도 있습니다.

아이콘 모음

아이콘 모음에 대한 상세 정보는 다음 표에 제시됩니다.

표 216. 아이콘 모음

UI 요소	설명
아이콘 모음	아이콘 모음에는 Core Console에서 액세스할 수 있는 주요 기능을 나타내는 그래픽이 포함되어 있습니다. 적절한 항목을 클릭하면 사용자 인터페이스에서 해당 기능을 관리할 수 있는 섹션으로 이동합니다. 아이콘 모음에 있는 아이콘은 다음과 같습니다.
아이콘 모음: 홈 아이콘	**홈**. Core 홈 페이지로 이동하려면 홈 아이콘을 클릭합니다.
아이콘 모음: 복제 아이콘	**복제**. 수신 복제 또는 발신 복제를 보거나 관리하려면 복제 아이콘을 클릭합니다.
아이콘 모음: 가상 대기 아이콘	**가상 대기**. 복구 지점에서 부팅 가능한 가상 시스템으로 정보를 내보내려면 가상 대기 아이콘을 클릭합니다.

UI 요소	설명	
아이콘 모음: 이벤트 아이콘		**이벤트**. Rapid Recovery Core와 관련된 모든 시스템 이벤트의 로그를 보려면 이벤트 아이콘을 클릭합니다.
아이콘 모음: 설정 아이콘		**설정**. Rapid Recovery Core에 대한 설정을 보고 관리하려면 설정 아이콘을 클릭합니다. Core 구성 설정을 백업하거나 복원할 수 있습니다. 일반 설정을 통해 포트를 제어하거나 화면을 표시할 수 있습니다. 또한 다음과 같은 카테고리에서 설정을 구성할 수 있습니다: 자동 업데이트; 야간 작업; 전송 대기열 설정; 클라이언트 제한 시간 설정; DVM 중복 제거 캐시 설정; Replay 엔진 설정; 배포 설정. 데이터베이스 연결, SMTP 서버 설정, 클라우드 저장소 계정, 보고서 글꼴 설정 변경을 보거나 변경할 수 있습니다. SQL 연결성 설정, Core 작업 설정, 라이센스 설정, SNMP 설정 및 vSphere 설정을 구성할 수 있습니다.
아이콘 모음: 자세히 아이콘		**자세히**. 자세히 아이콘을 클릭하여 다른 중요한 기능에 액세스할 수 있습니다. 각각의 자세히 아이콘에는 자체 아이콘이 아래 나열되어 있습니다.
아이콘 모음: 자세히 아이콘	시스템 정보	**시스템 정보**. 시스템 정보 아이콘을 클릭하면 Rapid Recovery Core에 대한 데이터를 표시할 수 있습니다. Core용 호스트 이름, OS, 아키텍처 및 메모리를 볼 수 있습니다. Core Console에 표시되는 이름을 볼 수 있습니다. 또한 네트워크에서 Core의 정규화된 도메인 이름 및 캐시 메타데이터와 중복 제거 캐시의 경로를 볼 수 있습니다. 표시 이름 변경에 대한 자세한 내용은 Core에 대한 시스템 정보 이해에서 확인하십시오. 중복 제거 캐시에 대한 자세한 내용은 중복 제거 캐시 및 저장 위치 이해에서 확인하십시오. 설정을 조정하는 방법에 대한 자세한 내용은 DVM 중복 제거 캐시 설정 구성에서 확인하십시오.
아이콘 모음: 자세히 아이콘	아카이브	**아카이브**. Rapid Recovery에서 Core의 정보에 대한 아카이브를 관리할 수 있습니다. 예약 또는 연결된 아카이브에 대한 정보를 조회하거나 아카이브를 추가, 확인 또는 가져올 수 있습니다.
아이콘 모음: 자세히 아이콘	마운트	**탑재**. 로컬 탑재를 보고 장착 해제하거나 원격 탑재를 보고 분리할 수 있습니다.
아이콘 모음: 자세히 아이콘	부트 CD	**부팅 CD**. Bare Metal Restore(BMR)에 일반적으로 사용되는 부팅 CD를 관리할 수 있습니다. 부팅 CD ISO 이미지를 생성하고 기존 이미지를 삭제하거나 이미지 경로를 클릭하여 열거나 저장할 수 있습니다.
아이콘 모음: 자세히 아이콘	리포지토리	**리포지토리**. Core와 연관된 리포지토리를 보고 관리할 수 있습니다.
아이콘 모음: 자세히 아이콘	암호화 키	**암호화 키**. 보호된 시스템에 적용할 수 있는 암호화 키를 보고 관리하며 가져오거나 추가할 수 있습니다. 암호화 키를 사용하고 있지 않으면 삭제할 수 있습니다.
아이콘 모음: 자세히 아이콘	클라우드 계정	**클라우드 계정** Core와 클라우드 저장소 계정 간의 연결을 보고 관리할 수 있습니다.
아이콘 모음: 자세히 아이콘	보존 정책	**보존 정책**. Core 보존 정책을 보고 수정할 수 있습니다(롤업 및 삭제 이전에 복구 지점을 유지하는 기간 포함).
아이콘 모음: 자세히 아이콘	알림	**알림**. Core 이벤트에 대한 알림을 구성하고, SMTP 서버 설정을 이메일 알림으로 정의하고, 반복 감소를 설정하여 동일한 이벤트에 대한 반복적인 알림을 표시하지 않을 수 있습니다.

UI 요소	설명		
아이콘 모음: 자세히 아이콘	다운로드		다운로드. Agent 소프트웨어 웹 설치 프로그램, Local Mount Utility, SNMP 브라우저에서 사용할 수 있는 이벤트 정보가 포함된 MIB 파일을 다운로드할 수 있습니다.
아이콘 모음: 자세히 아이콘	보고서		보고서. Core 보고서에 액세스하거나 보고서를 지속적으로 생성하도록 일정을 예약할 수 있습니다.
아이콘 모음: 자세히 아이콘	Core 로그		Core 로그. 진단을 위해 Core 로그 파일을 다운로드할 수 있습니다.

왼쪽 탐색 메뉴

왼쪽 탐색 영역에 나타나는 전체 메뉴 세트는 다음 표에 설명되어 있습니다.

표 217. 왼쪽 탐색 메뉴 옵션

UI 요소	설명
보호된 시스템 메뉴	보호된 시스템 메뉴는 하나 이상의 시스템이 Core에서 보호되고 있는 경우 왼쪽 탐색 영역의 첫 번째 메뉴로 나타납니다. 이 창에 표시되는 특정 시스템 이름을 클릭하면 선택한 시스템에 대한 요약 정보를 보여 주는 요약 페이지가 나타납니다. 요약 페이지에서 수행할 수 있는 작업에 대한 자세한 내용은 보호된 시스템의 요약 정보 보기을(를) 참조하십시오.
복제된 시스템 메뉴	최상위 수준 탐색 메뉴로 다른 Rapid Recovery Core의 이름이 보일 경우 Core Console을 보고 있는 Core가 대상 Core입니다. 메뉴 이름이 원본 Core를 따라 지정되고 아래에 나열되는 각 시스템은 이 대상에서 복제된 원본 Core에서 나온 시스템을 나타냅니다. 대상 Core가 두 개 이상의 원본 Core에서 복구 지점을 복제할 경우 각 출처 Core는 왼쪽 탐색 영역의 자체 탐색 가능한 메뉴로 나타납니다. 복제된 시스템 메뉴에 표시된 특정 시스템 이름을 클릭하면 선택한 복제 시스템에 대한 요약 정보를 보여 주는 요약 페이지가 나타납니다. 복제에 대한 자세한 내용은 복제을(를) 참조하십시오.
복구 지점만 메뉴	복구 지점만 메뉴가 보이는 경우 Core에 보호 또는 복제된 시스템에 대한 복제 지점이 포함되어 있습니다. 시스템이 더 이상 새 스냅숏 캡처를 계속하지 않을 경우 이전에 Core에서 캡처한 복구 지점이 그대로 유지됩니다. 이러한 복구 지점은 파일 수준 복구에 사용할 수 있지만 Bare Metal Restore, 전체 볼륨 복구 또는 스냅숏 데이터 추가에 사용할 수 없습니다.
사용자 지정 그룹 메뉴	사용자 지정 그룹을 생성한 경우 사용자 지정 그룹 메뉴가 탐색 메뉴에 나타납니다. 사용자 지정 그룹은 시스템을 함께 그룹화(예를 들어, 기능, 조직 또는 지리적 위치별)하는 데 사용되는 논리적 컨테이너입니다. 사용자 지정 그룹은 유형이 다른 개체(보호된 시스템, 복제된 시스템 등)를 포함할 수 있습니다. 다른 메뉴와 같이 사용자 지정 그룹에 대한 레이블을 정의할 수 있습니다. 이름은 메뉴에 모두 대문자로 나타납니다. 사용자 지정 그룹 제목의 화살표를 클릭하여 사용자 지정 그룹의 유사한 항목에 대한 작업을 수행할 수 있습니다. 예를 들어, 사용자 지정 그룹에서 모든 보호된 시스템에 대한 스냅숏을 강제 실행할 수 있습니다. 사용자 지정 그룹 생성 및 관리에 대한 자세한 내용은 사용자 지정 그룹 이해를 참조하십시오.
연결된 아카이브 메뉴	Core에 아카이브를 연결할 경우 각 아카이브가 왼쪽 탐색 메뉴에 목록으로 표시됩니다. 해당 레이블은 아카이브의 이름입니다. 이 목록에는 해당 아카이브에 포함된 각 시스템이 포함되어 있습니다.

왼쪽 탐색 영역에 있는 요소에 대한 상세 정보는 다음 표에 제시됩니다.

표 218. 왼쪽 탐색 영역 및 메뉴

UI 요소	설명
시스템 메뉴 텍스트 필터	텍스트 필터는 Protected Machines(보호된 시스템), Replicated Machines(중복된 시스템), Recovery-Point Only machines(복구 지점만 시스템) 메뉴에 표시된 항목을 필터링할 수 있는 텍스트 필드입니다. 이 필터에 기준을 입력하면 기준을 충족하는 시스템만 해당 메뉴에 표시됩니다.
확장 및 축소 세부 정보	텍스트 필터의 오른쪽에 있는 화살표를 클릭하면 Protected Machines(보호된 시스템), Replicated Machines(중복된 시스템), Recovery-Point Only machines(복구 지점만 시스템)에 대한 세부 정보를 확장 및 축소할 수 있습니다.
보호된 시스템 메뉴	보호된 시스템 메뉴는 UI의 왼쪽 탐색 영역에 표시됩니다. 이 메뉴에서는 Core에 구성된 모든 보호된 시스템, 보호된 클러스터 또는 복제된 시스템을 볼 수 있습니다. 보호된 그룹 또는 복구 지점만 시스템이 있는 경우에도 이 메뉴의 일부로 표시됩니다. 메뉴 라벨의 왼쪽에 있는 화살표를 클릭하여 Core 내 보호된 시스템에 대한 보기를 확장하거나 축소할 수 있습니다. 시스템 유형을 설명하는 아이콘: · 단순한 시스템 아이콘은 실제 시스템이나 Rapid Recovery Agent 소프트웨어가 설치된 보호된 VM을 나타냅니다. · 다중 시스템 아이콘는 보호된 클러스터를 나타냅니다. · 비어 있는 2중 시스템 아이콘은 에이전트 없는 보호를 사용하는 VMware VM을 나타냅니다. · 비어 있는 3중 시스템 아이콘은 VMware vCenter 호스트를 나타냅니다. Protected Machines(보호된 시스템) 메뉴를 클릭하면 Protected Machines(보호된 시스템) 페이지가 나타나고 Protected Machines(보호된 시스템) 창에 이 Core의 보호된 시스템이 모두 표시됩니다. 자세한 내용은 보호된 시스템 메뉴 보기을(를) 참조하십시오.
복제된 시스템 메뉴	다른 Rapid Recovery Core에서 시스템을 복제하는 경우 해당 Core의 이름이 Protected Machines(보호된 시스템) 메뉴 아래에 별도의 메뉴로 표시됩니다. 소스 Core 목록에서 이 대상 Core에 복제된 모든 시스템은 이 메뉴 아래에 표시됩니다. 복제된 각 시스템의 아이콘은 복제된 시스템 유형을 나타냅니다. 예를 들어, 단일 시스템 복제의 경우 아이콘이 한 개의 시스템을 표시됩니다. 서버 클러스터 복제의 경우 아이콘이 클러스터를 표시합니다. 이 메뉴 라벨의 왼쪽에 있는 화살표를 클릭하여 이러한 복제된 시스템 보기를 확장하거나 축소할 수 있습니다. 복제된 시스템 메뉴에서는 복제된 모든 시스템에 대해 작업을 수행할 수 있습니다. 복제된 시스템 메뉴를 클릭하면 시스템 페이지가 나타납니다. 이 페이지는 해당 대상 Core로 복제된 다른 소스 Core에서 보호되는 모든 시스템을 표시합니다. 자세한 내용은 탐색 메뉴에서 복제된 시스템 보기을(를) 참조하십시오.
복구 지점만 메뉴	이전에 Core에서 보호되었던 시스템이 보호에서 제거되었지만 복구 지점이 삭제되지 않은 경우 복구 지점만 메뉴가 나타납니다. 복구 지점이 남아 있으며 이전에 보호되었던 시스템은 이 목록에 표시됩니다. 이 메뉴 라벨 왼쪽에 있는 화살표를 클릭하여 복구 지점만 시스템 복구 보기를 확장하거나 축소할 수 있습니다. 복구 지점만 메뉴에서 이 Core의 모든 복구 지점만 시스템에 대한 복구 지점을 제거할 수 있습니다. 복구 지점만 메뉴를 클릭하면 시스템 페이지가 나타나고 복구 지점이 저장된 시스템이 표시됩니다. 자세한 내용은 복구 지점만 메뉴 보기을(를) 참조하십시오.

UI 요소	설명
사용자 지정 그룹 메뉴	Core에 사용자 지정 그룹이 포함되어 있는 경우 왼쪽 탐색 영역에 사용자 지정 그룹 메뉴가 표시됩니다. 사용자 지정 그룹의 각 개체는 이 목록에 표시됩니다. 메뉴 라벨의 왼쪽에 있는 화살표를 클릭하여 Core 내 사용자 지정 그룹에 대한 보기를 확장하거나 축소할 수 있습니다. 사용자 지정 그룹 메뉴에서 그룹의 유사 항목에 대한 작업을 수행할 수 있습니다. 사용자 지정 그룹 메뉴를 클릭하면 시스템 페이지가 나타나고 보호된 시스템, 복제된 시스템, 복구 지점만 시스템 그룹에 나타나는 각 Rapid Recovery 개체에 대한 창이 표시됩니다. 자세한 내용은 사용자 지정 그룹 메뉴 보기을(를) 참조하십시오.
연결된 아카이브 메뉴	아카이브를 Core에 연결하면 왼쪽 탐색 영역에 연결된 각 아카이브에 대한 메뉴가 포함되어 있습니다. 아카이브에 포함된 모든 Protected Machines(보호된 시스템)는 이 목록에 표시됩니다. 아카이브를 저장하면 메뉴 레이블에서 지정된 이름을 사용합니다. 메뉴 라벨의 왼쪽에 있는 화살표를 클릭하여 Core에 연결된 아카이브에 대한 보기를 확장하거나 축소할 수 있습니다. 연결된 아카이브 메뉴에서 그룹의 유사 항목에 대한 작업을 수행할 수 있습니다. 연결된 아카이브 메뉴를 클릭하면 시스템 페이지가 나타나고 보호된 시스템, 복제된 시스템, 복구 지점만 시스템 그룹에 나타나는 각 Rapid Recovery 개체에 대한 창이 표시됩니다. 자세한 내용은 사용자 지정 그룹 메뉴 보기을(를) 참조하십시오.

Protected Machines(보호되는 시스템) 창 보기

Protected Machines(보호되는 시스템) 창에는 이 Rapid Recovery Core에서 보호되는 모든 시스템에 대한 정보가 포함되어 있습니다. 각 보호되는 시스템(아직 보호되고 있는 경우)에 대해 다음 표에 설명되어 있는 정보가 나열됩니다.

표 219. 각 보호되는 시스템에 대한 정보

UI 요소	설명
항목 선택	요약 표의 각 행에 대해 위 표에 있는 메뉴 옵션 목록에서 작업을 수행하려면 확인란을 선택할 수 있습니다.
유형	시스템 유형을 보여 줍니다.
상태 표시등	Status(상태) 열의 컬러 열은 시스템이 온라인인지 또는 연결할 수 없는지 여부를 보여줍니다. 컬러 원 위로 커서를 올려 놓으면 상태 조건이 표시됩니다. 상태 조건은 녹색(온라인 및 보호됨), 노란색(보호가 일시 중지됨), 빨간색(인증 오류) 및 회색(오프라인 또는 연결할 수 없음)을 포함합니다.
암호화 상태	자물쇠 아이콘은 선택한 보호되는 시스템에 대한 암호화 상태를 나타냅니다. 열린 자물쇠는 암호화가 없음을 나타내고 잠긴 자물쇠는 암호화 키가 설정되어 있음을 나타냅니다. 암호화에 대한 자세한 내용은 암호화 키 이해을(를) 참조하십시오.
표시 이름	보호되는 시스템의 표시 이름
마지막 스냅샷	이 시스템의 마지막 백업 전송의 날짜 및 시간을 나열합니다.
리포지토리 이름	이 시스템의 데이터가 저장되는 리포지토리를 나열합니다.
Recovery Points(복구 지점)	복구 지점의 수와 리포지토리에서 공간을 얼마나 차지하는지 나열합니다.
버전	시스템에 로드된 Rapid Recovery 에이전트 소프트웨어의 버전입니다.
조치	이 열에서 Settings(설정) 드롭다운 메뉴를 클릭하면 선택한 보호되는 시스템에서 특별히 수행할 조치 목록이 표시됩니다.

이 Core에서 보호되는 시스템이 가상 대기용으로 구성된 경우 다음 표에 설명된 대로 추가 정보가 표시됩니다.

표 220. 가상 대기용으로 구성된 보호되는 시스템에 대한 정보

UI 요소	설명
마지막 내보내기	마지막 가상 내보내기의 날짜 및 시간입니다.
대상	보호되는 시스템을 가상 시스템으로 저장하기 위한 대상입니다. 예를 들어, ESXi, VMware Workstation, Hyper-V 또는 VirtualBox.
상태	가상 대기용으로 구성된 시스템의 상태입니다. 상태는 "In Sync(동기화 중)", "Paused(일시 중지됨)" 및 "Not enabled(활성화되지 않음)"를 포함합니다.

Protected Machines(보호되는 시스템) 창의 Actions(작업) 드롭다운 메뉴에서 다음 표에 설명되어 있는 작업을 수행할 수 있습니다. 일부 옵션은 표시된 대로 Exchange Server 또는 SQL Server의 경우에만 나타납니다.

표 221. Protected Machines(보호되는 시스템) 창에서 사용 가능한 작업

UI 요소	설명
Force Snapshot(스냅샷 강제 적용)	선택한 보호되는 시스템의 보호되는 모든 볼륨에 대한 기본 이미지를 증분 스냅샷을 강제로 수행할 수 있습니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.
One-time Export(1회 내보내기)	Virtual Machine Export Wizard(가상 컴퓨터 내보내기 마법사)를 실행합니다. 이 마법사를 사용하면 모든 지원되는 VM 형식으로 보호되는 시스템에서 가상 시스템으로 복구 지점 데이터의 1회 내보내기를 수행할 수 있습니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.
Virtual Standby(가상 대기)	Virtual Machine Export Wizard(가상 컴퓨터 내보내기 마법사)를 실행합니다. 이 마법사를 사용하면 모든 지원되는 VM 형식으로 보호되는 시스템에서 가상 시스템으로 복구 지점 데이터의 연속 내보내기를 위한 가상 대기를 수행할 수 있습니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.
Mount(마운트)	Mount Wizard(마운트 마법사)를 시작합니다. 이 마법사를 사용하면 선택한 보호되는 시스템에서 복구 지점을 마운트할 수 있습니다.
Recovery Points(복구 지점)	Recovery Points Summary(복구 지점 요약) 페이지가 열립니다.
Restore(복원)	Restore Machine Wizard(시스템 보호 마법사)를 시작합니다. 이 프로세스를 사용하면 Core의 복구 지점에서 보호되는 시스템으로 데이터를 복원할 수 있습니다. 자세한 내용은 복구 지점에서 볼륨 복원을(를) 참조하십시오.
Remove Machine(시스템 제거)	Rapid Recovery Core에서 보호로부터 선택한 시스템을 제거하여 Rapid Recovery Core에 이미 있는 복구 지점을 삭제 또는 유지하도록 선택할 수 있습니다. 자세한 내용은 시스템 제거을(를) 참조하십시오.

보호되는 시스템 그리드에 나열된 시스템 중 2개 이상에서 작업을 수행할 수 있습니다. 다중 시스템에서 작업을 수행하려면 각 보호되는 시스템에 대한 확인란을 선택합니다. 그런 다음, 요약 표 위의 메뉴에서 다음 표에 설명되어 있는 작업을 수행할 수 있습니다.

표 222. 시스템이 선택되었을 때 Protected Machines(보호되는 시스템) 창에서 사용할 수 있는 추가 작업

UI 요소	설명
Force Snapshot(스냅샷 강제 적용)	선택한 보호되는 시스템의 보호되는 모든 볼륨에 대한 증분 스냅샷을 강제로 수행할 수 있습니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.
Force Base Image(기본 이미지 강제 적용)	선택한 보호되는 시스템의 모든 보호되는 볼륨에 대한 기본 이미지를 강제로 수행할 수 있습니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.

UI 요소	설명
Protection > Pause or Resume(보호 > 일시 중지 또는 재개)	선택한 시스템에 대한 보호를 일시 중지하거나(보호가 활성화된 경우), 또는 선택한 시스템에 대한 보호를 재개할 수 있습니다(보호가 일시 중지된 경우). 자세한 내용은 보호 일시 중지 및 다시 시작을(를) 참조하십시오.
복제	복제를 활성화, 강제 적용, 복사, 일시 중지 또는 재개할 수 있습니다. 기존 복구 지점을 시드 드라이브에 복사할 수도 있습니다. 자세한 내용은 복제 설정 관리을(를) 참조하십시오.
Cancel(취소)	선택한 시스템에 대해 현재 활성화된 모든 작업을 취소하거나 선택한 시스템에 대해 현재 진행 중인 스냅샷만 취소할 수 있습니다. 이렇게 해도 향후 예약된 작업에 영향을 주지 않습니다.
Remove Machine(시스템 제거)	Rapid Recovery Core에서 보호로부터 선택한 시스템을 제거하여 Rapid Recovery Core에 이미 있는 복구 지점을 삭제 또는 유지하도록 선택할 수 있습니다. 자세한 내용은 시스템 제거을(를) 참조하십시오.

각 보호되는 시스템에 대한 Configuration(구성) 드롭다운 메뉴에서 다음 표에 나와 있는 작업을 수행할 수 있습니다. 일부 옵션은 표시된 대로 Exchange Server 또는 SQL Server의 경우에만 나타납니다.

표 223. Protected Machines(보호되는 시스템) 창에서 사용 가능한 작업

UI 요소	설명
Force Snapshot(스냅샷 강제 적용)	선택한 시스템에서 하나 이상의 볼륨에 대한 증분 스냅샷 또는 기본 이미지를 강제로 수행할 수 있습니다. 자세한 내용은 스냅숏 작성을(를) 참조하십시오.
Force Log Truncation for Exchange(Exchange에 대해 로그 자르기 강제 적용)	보호되는 Exchange Server 시스템의 경우 Exchange Server의 공간을 줄여주는 Exchange 로그의 자르기를 강제로 적용합니다. 자세한 내용은 SQL 시스템에 대한 로그 잘라내기 수행을(를) 참조하십시오.
Force Log Truncation for SQL(SQL에 대해 로그 자르기 강제 적용)	보호되는 SQL Server 시스템의 경우 SQL Server의 공간을 줄여주는 SQL Server 로그의 자르기를 강제로 적용합니다. 자세한 내용은 SQL 시스템에 대한 로그 잘라내기 수행을(를) 참조하십시오.
Export(내보내기)	Export Wizard(내보내기 마법사)를 시작합니다. 이 마법사를 사용하면 모든 지원되는 VM 형식으로 보호되는 시스템에서 가상 시스템으로 복구 지점을 내보낼 수 있습니다. 1회 내보내기를 수행하거나 연속 내보내도록 가상 대기를 설정할 수 있습니다. 자세한 내용은 VM 내보내기을(를) 참조하십시오.
Mount(마운트)	Mount Recovery Point(복구 지점 마운트) 대화 상자가 열리면 특정 복구 지점을 마운트하기 위해 저장된 스냅샷 데이터를 통해 Rapid Recovery Core를 탐색할 수 있습니다. 자세한 내용은 각각 복구 지점 마운트 또는 Linux 시스템에서 복구 지점 볼륨 마운트을(를) 참조하십시오.
Recovery Points(복구 지점)	선택한 에이전트 시스템에 대한 Recovery Points(복구 지점) 탭이 열립니다. 자세한 내용은 스냅숏 및 복구 지점 관리을(를) 참조하십시오.
Restore(복원)	Restore Machine Wizard(시스템 보호 마법사)를 시작합니다. 이 프로세스를 사용하면 Core의 복구 지점에서 보호되는 시스템으로 데이터를 복원할 수 있습니다. 자세한 내용은 복구 지점에서 볼륨 복원을(를) 참조하십시오.
Remove Machine(시스템 제거)	Rapid Recovery Core에서 보호로부터 선택한 시스템을 제거하여 Rapid Recovery Core에 이미 있는 복구 지점을 삭제 또는 유지하도록 선택할 수 있습니다. 자세한 내용은 시스템 제거을(를) 참조하십시오.

보호된 시스템에 대한 이벤트 보기

이벤트 페이지에서는 선택한 보호된 시스템에서 발생했거나 진행 중인 작업을 볼 수 있습니다. 페이지 상단의 단추를 사용하면 세 가지 활동 카테고리 중 하나에서 작업 목록을 탐색할 수 있습니다.

- **작업.** Rapid Recovery가 성공적으로 작동하기 위해 수행해야 하는 작업입니다.

- **경고.** 오류 및 경고가 포함된 작업 또는 이벤트와 관련된 알림입니다.
- **저널.** 모든 보호된 시스템 작업과 경고의 복합체입니다.

다음 표에는 **이벤트** 페이지의 각 요소에 대한 설명이 포함되어 있습니다.

표 224. 이벤트 페이지 요소

UI 요소	설명
키워드 검색	각 범주 내 특정 항목을 검색할 수 있습니다. 작업에만 사용할 수 있습니다.
시작	검색을 시작할 날짜를 입력하여 결과를 좁힐 수 있습니다. 작업에만 사용할 수 있습니다.
종료	검색을 중지할 날짜를 입력하여 결과를 좁힐 수 있습니다. 작업에만 사용할 수 있습니다.
상태 아이콘	각 아이콘은 서로 다른 작업 상태를 나타냅니다. 경고 및 작업의 경우 아이콘 중 하나를 클릭하여 해당 상태를 기준으로 목록을 필터링하고 보고서를 생성할 수 있습니다. 아이콘을 다시 클릭하면 해당 상태에 대한 필터가 제거됩니다. 두 개 이상의 상태를 기준으로 필터링할 수 있습니다. 상태는 다음과 같습니다. • **활성.** 진행 중인 작업입니다. • **대기열에 있음.** 시작하기 위해 다른 작업이 완료되기를 기다리고 있는 작업. • **대기 중.** 시드 드라이브와 같이 사용자의 승인 또는 완료를 대기하는 작업입니다. (시드 드라이브에 대한 자세한 내용은 복제를 참조하십시오.) • **완료.** 성공적으로 완료된 작업입니다. • **실패.** 실패하여 완료되지 못한 작업.
서비스 아이콘	이 단추는 서비스 작업을 작업 목록에 추가합니다. 이 아이콘을 클릭하면 더 작은 서비스 아이콘이 각 상태 아이콘에 나타나며, 이 아이콘을 사용하여 해당 상태(있는 경우)에 있는 서비스 작업을 기준으로 필터링할 수 있습니다. 서비스 작업의 예로는 인덱스 파일 삭제 또는 복제에서 시스템 제거 등이 있습니다.
내보내기 유형 드롭다운 목록	드롭다운 목록에는 이벤트 보고서를 내보낼 수 있는 형식이 포함됩니다. 작업에만 사용할 수 있습니다. 다음과 같은 형식이 포함됩니다. • PDF • HTML • CSV • XLS • XLSX
(내보내기 아이콘)	이벤트 보고서를 사용자가 선택한 형식으로 변환합니다. 작업에만 사용할 수 있습니다.
페이지 선택	이벤트 보고서는 여러 페이지에 걸쳐 여러 작업을 포함할 수 있습니다. **이벤트** 페이지 하단의 숫자와 화살표를 사용하면 보고서의 페이지 사이를 이동할 수 있습니다.

이벤트 페이지에는 모든 이벤트가 표 형태로 표시됩니다. 다음 표는 각 항목에 대해 표시되는 정보를 나열합니다.

표 225. 이벤트 요약 표에 대한 자세한 정보

UI 요소	설명
상태	작업, 경고, 또는 저널 항목의 상태를 보여 줍니다. 경고 또는 저널 항목에 대해 사용 가능하며 상태별로 결과를 필터링하려면 머리글을 클릭합니다.
이름	이름는 작업에만 사용할 수 있습니다. 이 텍스트 필드는 이 보호된 이 시스템에 대해 완료한 작업 유형을 나열합니다. 볼륨 전송, 리포지토리 유지 관리, 롤업, 탑재 가능 검사 수행, 체크섬 검사 수행 등의 예가 있습니다.
시작 시간	작업, 경고 및 저널 항목에 사용 가능합니다. 작업 시작 시 날짜 및 시간을 표시합니다.

UI 요소	설명
종료 시간	작업에만 사용할 수 있습니다. 작업 완료 시 날짜 및 시간을 나타냅니다.
작업 세부 정보	작업에만 사용할 수 있습니다. **진행 중인 작업 모니터** 대화 상자를 열면 특정 작업의 세부 정보를 볼 수 있습니다. 이러한 세부 정보에는 작업 ID, Core의 데이터 전송 속도(관련된 경우), 작업 완료 경과 시간, 총 작업량(기가바이트) 및 해당 작업과 연관된 하위 작업 등이 있습니다.
메시지	경고 및 저널 항목에 사용할 수 있습니다. 이 텍스트 필드는 경고 또는 저널에 대한 설명적 메시지를 제공합니다.

보호되는 시스템의 추가 메뉴 보기

More(추가) 메뉴는 선택한 보호되는 시스템을 관리하기 위한 추가 옵션을 제공합니다. 이러한 도구에 액세스하려면 More(추가) 드롭다운 메뉴를 클릭하고 다음 표에 설명되어 있는 옵션 중 하나를 선택합니다.

표 226. 보호되는 시스템에 대해 More(추가) 옵션에서 액세스할 수 있는 도구

UI 요소	설명
System information(시스템 정보)	보호되는 시스템, 시스템 정보, 볼륨, 프로세서, 네트워크 어댑터 및 이 시스템의 IP 주소에 대한 정보를 보여줍니다. 자세한 내용은 보호된 시스템의 시스템 정보 보기 섹션을 참조하십시오.
Mounts(마운트)	Local Mounts(로컬 마운트) 창에서 로컬로 마운트된 볼륨을 보거나 마운트를 해제할 수 있습니다. Remote Mounts(원격 마운트) 창에서 Local Mount 유틸리티를 사용하여 마운트된 볼륨을 보거나 마운트 해제할 수 있습니다. 볼륨 마운트 해제에 대한 자세한 내용은 복구 지점 분리을(를) 참조하십시오. 복구 지점을 로컬로 마운트하는 자세한 내용은 각각 복구 지점 마운트 또는 Linux 시스템에서 복구 지점 볼륨 마운트을(를) 참조하십시오.
Retention Policy(보존 정책)	선택한 시스템에 대한 보존 정책을 지정할 수 있습니다. Core의 기본 정책을 사용하거나 이 시스템 전용으로 보존 정책을 구별할 수 있습니다. 자세한 내용은 보호되는 시스템에 대한 보존 정책 설정 사용자 지정을(를) 참조하십시오.
Notifications(알림)	선택한 시스템과 관련된 이벤트에 대한 사용자 지정 알림 그룹을 지정할 수 있습니다. 이렇게 해도 이미 Core에 설정된 알림은 변경되지 않습니다. 자세한 내용은 알림 그룹 구성을(를) 참조하십시오.
Agent Log(에이전트 로그)	Rapid Recovery 에이전트 소프트웨어를 사용하여 보호되는 시스템에 대한 로그 파일을 다운로드하여 볼 수 있습니다. 자세한 내용은 보호된 시스템의 로그 파일 다운로드 및 보기을(를) 참조하십시오.

B

Rapid Recovery PowerShell Module 이해

Dell Data Protection | Rapid Recovery에는 여러 가지 소프트웨어 구성 요소가 포함됩니다. 이 항목과 관련된 주요 구성 요소는 다음과 같습니다.

- Rapid Recovery Core는 보호된 시스템 인증, 백업 및 복제를 위한 데이터 전송 일정, 가상 시스템에 내보내기, 보고, 유사 또는 다른 종류의 하드웨어에 대한 BMR(Bare Metal Restore) 등의 작업을 관리합니다.
- Rapid Recovery Agent는 볼륨 스냅숏을 작성하고, 데이터를 Core에서 관리하는 리포지토리로 신속하게 전송하는 작업을 수행합니다.
- Rapid Recovery PowerShell Module은 사용자가 Windows PowerShell® 스크립트를 사용하여 Core 서버와 상호작용할 수 있도록 해주는 Windows 유틸리티입니다. 이 모듈은 Rapid Recovery Core Console 그래픽 사용자 인터페이스(GUI)가 제공하는 일부 동일한 기능을 제공합니다. 예를 들어 Rapid Recovery PowerShell Module은 Rapid Recovery 복구 지점을 마운트하거나 보호된 시스템의 스냅숏을 작성할 수 있습니다.

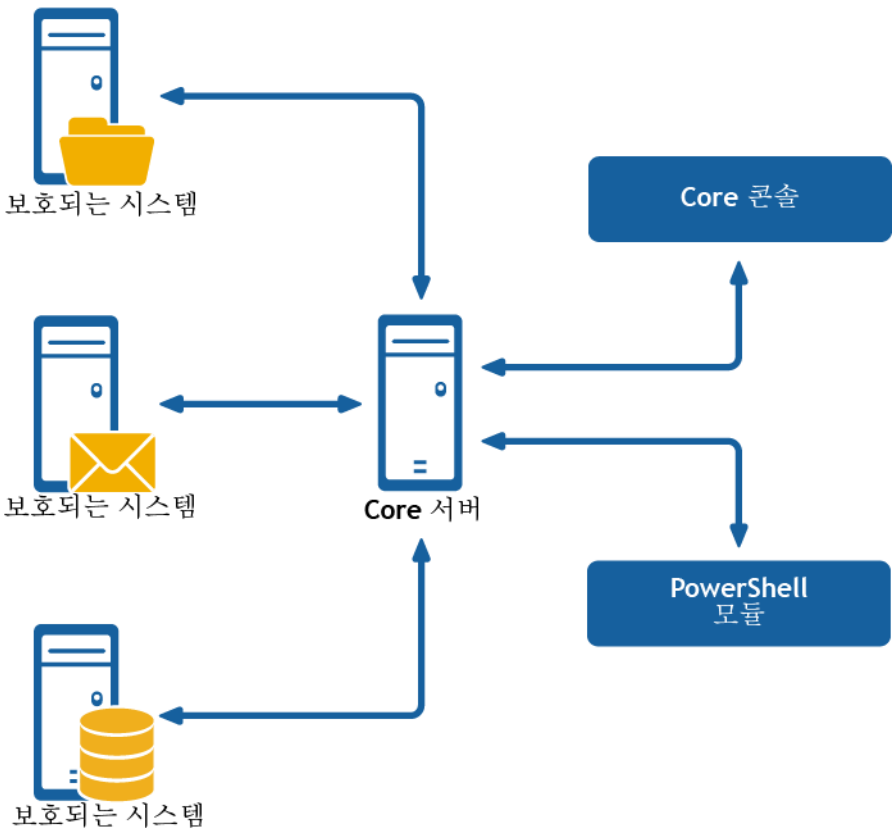


그림 14 . PowerShell Module은 Rapid Recovery Core와 상호 작용

PowerShell은 관리 자동화를 위해 설계된 Microsoft .NET Framework 연결 환경입니다. 이 섹션에서는 관리자가 Rapid Recovery Core GUI와 상호 작용하지 않고 특정 기능을 스크립트하는 데 사용할 수 있는 Rapid Recovery PowerShell Module 및 cmdlets에 대해 설명합니다.

노트: PowerShell 스크립트를 사전 스크립트 또는 사후 스크립트로 실행할 수도 있습니다. 자세한 내용과 샘플 스크립트는 스크립트 작성을 사용하여 Rapid Recovery 작업 확장을(를) 참조하십시오.

주제:

- PowerShell을 사용하기 위한 전제 조건
- 명령 및 cmdlet 사용
- Rapid Recovery PowerShell module cmdlet
- 현지화
- 한정자

PowerShell을 사용하기 위한 전제 조건

Rapid Recovery PowerShell Module을 사용하기 전에 Windows PowerShell 2.0 이상을 설치해야 합니다. PowerShell 3.0에는 더 쉬운 객체 속성 액세스, PowerShell Web 액세스, REST 호출 지원 등 새로운 기능이 포함되어 있으므로 PowerShell 3.0 이상을 사용하는 것이 좋습니다.

노트: PowerShell 홈 디렉터리에 powershell.exe.config 파일을 배치해야 합니다. 예: C:\WindowsPowerShell \powershell.exe.config

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

PowerShell 실행 및 모듈 가져오기

다른 시스템 모듈과 달리 Rapid Recovery PowerShell Module은 기본적으로 로드되지 않습니다. 각 세션에 대해 관리자 권한으로 Windows PowerShell을 연 다음 모듈을 가져올 수 있습니다. PowerShell을 실행하고 Rapid Recovery PowerShell Module을 가져오려면 이 절차에 있는 단계를 완료하십시오.

1 Windows PowerShell에 대한 관리자 권한 명령 프롬프트를 엽니다. 예를 들어, 시작 메뉴에 Windows PowerShell을 입력하고 Windows PowerShell 응용프로그램을 마우스 오른쪽 단추로 클릭한 다음 **관리자 권한으로 실행**을 선택합니다.

Windows PowerShell이 새 명령 창에서 열립니다.

2 다음 명령을 입력한 후 Enter 키를 누릅니다.

```
Import-Module "RapidRecoveryPowerShellModule"
```

현재 세션에 대해 Rapid Recovery PowerShell Module을 가져옵니다. 기존 명령 창에서 cmdlet을 실행할 수 있습니다.

명령 및 cmdlet 사용

cmdlet은 단일 기능을 수행하는 Windows PowerShell 스크립트의 특수 명령입니다. cmdlet은 일반적으로 동사-명사 쌍으로 표현됩니다. cmdlet에 의해 반환되는 결과는 객체입니다.

PowerShell 명령을 파이프라인하여 한 cmdlet 출력을 다른 cmdlet 입력으로 파이프할 수 있습니다. 간단한 예로 Rapid Recovery PowerShell Module의 명령 목록을 요청한 후 이 목록을 이름별로 정렬할 수 있습니다. 이 작업의 스크립트 예는 다음과 같습니다.

```
Get-Command -module rapidrecoverypowershellmodule | sort-object name
```

cmdlet 도움말 및 예제 보기

PowerShell을 열고 Rapid Recovery PowerShell Module을 가져온 후 언제든지 Get-Help <명령_이름> cmdlet을 사용하여 추가 정보를 요청할 수 있습니다. 예를 들어, 가상 시스템 내보내기 cmdlet에 대한 정보를 가져오려면 다음 cmdlet을 입력하고 Enter 키를 입력하십시오.

```
Get-Help Start-VMExport
```

반환되는 객체에는 명령 이름, 개요, 구문 및 명령과 함께 사용할 수 있는 옵션이 포함됩니다.

특정 cmdlet에 대한 도움말을 표시하는 다른 방법은 명령 이름 뒤에 -?를 입력하는 것입니다. 예:

```
Start-VMExport -?
```

다음 명령을 실행하여 cmdlet에 대한 예를 요청할 수도 있습니다.

```
>Get-Help Start-VMExport -examples
```

Rapid Recovery PowerShell module cmdlet

이 섹션에서는 Rapid Recovery PowerShell Module에서 사용 가능한 cmdlet와 옵션을 설명합니다. Rapid Recovery PowerShell Module의 모든 cmdlet는 다음과 같은 일반적인 매개변수를 지원합니다.

- Verbose
- Debug
- ErrorAction
- ErrorVariable
- WarningAction
- WarningVariable
- OutBuffer
- OutVariable

자세한 내용은 `Get-Help about_commonparameters`를 사용하십시오.

다음 표에 사용 가능한 cmdlet이 나열되어 있습니다.

표 227. Rapid Recovery PowerShell Module의 Cmdlet

Cmdlet 이름	설명
Edit esxivirtualstandby	기존의 ESXi 가상 대기 구성을 편집합니다.
Edit-HyperVVirtualStandby	기존의 Hyper-v 가상 대기 구성을 편집합니다.
Edit-VBVirtualStandby	기존의 VirtualBox 가상 대기 구성을 편집합니다.
Edit-VMVirtualStandby	기존의 VMware Workstation 가상 대기 구성을 편집합니다.
Edit-ScheduledArchive	기존의 예약된 아카이브 구성을 편집합니다.
Get-ActiveJobs	활성 작업의 모음을 가져옵니다.
Get-CloudAccounts	Core에 저장된 클라우드 계정에 대한 정보를 가져옵니다.
Get-Clusters	보호된 클러스터의 모음을 가져옵니다.

Cmdlet 이름	설명
Get-CompletedJobs	완료된 작업의 모음을 가져옵니다.
Get-ExchangeMailStores	Exchange 메일 저장소의 모음을 가져옵니다.
Get-Failed	실패한 복구 지점에 대한 정보를 가져옵니다.
Get-FailedJobs	실패한 작업의 모음을 가져옵니다.
Get-Mounts	모든 탑재된 복구 지점을 표시합니다.
Get-Passed	통과한 복구 지점에 대한 정보를 가져옵니다.
Get-ProtectedServers	보호된 서버에 대한 정보를 가져옵니다.
Get-ProtectionGroups	보호 그룹의 모음을 가져옵니다.
Get-QueuedJobs	대기열에 대기 중인 작업의 모음을 가져옵니다.
Get-RecoveryPoints	복구 지점에 대한 정보를 가져옵니다.
Get-ReplicatedServers	복제된 서버에 대한 정보를 가져옵니다.
Get-Repositories	리포지토리에 대한 정보를 가져옵니다.
Get-ScheduledArchive	반복적인 아카이브 작업에 대한 정보를 가져옵니다.
Get-SqlDatabases	SQL 데이터베이스의 모음을 가져옵니다.
Get-UnprotectedVolumes	보호되지 않은 볼륨의 모음을 가져옵니다.
Get-VirtualizedServers	가상화된 서버에 대한 정보를 가져옵니다.
Get-Volumes	볼륨에 대한 정보를 가져옵니다.
New-Base	기본 이미지 스냅숏을 작성합니다.
New-CloudAccount	Core에 새 클라우드 계정을 추가합니다.
New-EncryptionKey	새 암호화 키를 생성합니다.
New-EsxiVirtualStandby	새 ESXi 가상 대기 가상 시스템을 생성합니다.
New-HyperVVirtualStandby	새 Hyper-V 가상 대기 가상 시스템을 생성합니다.
New-Mount	복구 지점 마운트.
New-Replication	복제를 설정하고 적용합니다.
New-Repository	새 DVM 리포지토리를 만듭니다.
New-ScheduledArchive	반복적인 새 아카이브를 예약합니다.
New-Snapshot	스냅숏을 작성합니다.
New-VBVirtualStandby	새 VirtualBox 가상 대기 가상 시스템을 생성합니다.
New-VMVirtualStandby	새 VMware Workstation 가상 대기 가상 시스템을 생성합니다.
Push-Replication	복제 수행.
Push-Rollup	롤업을 수행합니다.
Remove-Agent	시스템 보호를 제거합니다.
Remove-Mount	복구 지점을 분리합니다.

Cmdlet 이름	설명
Remove-Mounts	모든 마운트된 복구 지점을 분리합니다.
Remove-RecoveryPoints	보호되는 시스템의 복구 지점을 삭제합니다.
Remove-Repository	기존 DVM 리포지토리를 삭제합니다.
Remove-ScheduledArchive	예약된 아카이브를 중단합니다.
Remove-VirtualStandby	Core에서 가상 대기 가상 시스템을 제거합니다.
Resume-Replication	복제를 다시 시작합니다.
Resume-RepositoryActivity	리포지토리 작동을 다시 시작합니다.
Resume-ScheduledArchive	예약된 아카이브를 다시 시작합니다.
Resume-Snapshot	스냅숏을 다시 시작합니다.
Resume-VirtualStandby	가상 대기 가상 시스템으로 데이터 내보내기를 다시 시작합니다.
Start-Archive	복구 지점을 아카이브합니다.
Start-AttachabilityCheck	보호된 MS SQL 데이터베이스에 대한 연결성 검사를 수행합니다.
Start-ChecksumCheck	보호된 Exchange 메일 저장소에 대한 체크섬 검사를 수행합니다.
Start-EsxiExport	ESXi 서버로 내보내기를 수행합니다.
Start-HypervExport	Hyper-V 서버로 내보내기를 수행합니다.
Start-LogTruncation	로그 잘라내기를 수행합니다.
Start-MountabilityCheck	보호된 Exchange 메일 저장소에 대한 마운트 가능성 검사를 수행합니다.
Start-Protect	서버를 보호합니다.
Start-ProtectCluster	클러스터를 보호합니다.
Start-RepositoryCheck	DVM 리포지토리 검사를 수행합니다.
Start-RestoreArchive	복구 지점을 사용하여 아카이브를 복원합니다.
Start-ScheduledArchive	예약된 아카이브에 대한 데이터를 전송을 수행합니다.
Start-VBExport	VirtualBox 서버로 내보내기를 수행합니다.
Start-VirtualStandby	기존의 가상 대기 가상 시스템으로 데이터 전송을 수행합니다.
Start-VMExport	VMWare Workstation 서버로 내보내기를 수행합니다.
Stop-ActiveJobs	활성 작업을 취소합니다.
Suspend-Replication	복제를 일시 중지합니다.
Suspend-RepositoryActivity	리포지토리에 대한 작업을 일시 중지합니다.
Suspend-ScheduledArchive	예약된 아카이브에 대한 데이터 전송을 일시 중지합니다.
Suspend-Snapshot	스냅숏을 일시 중지합니다.

Cmdlet 이름	설명
Suspend-VirtualStandby	가상 대기 가상 시스템에 대한 데이터 전송을 일시 중지합니다.
Update-Repository	DVM 리포지토리에 범위를 추가합니다.

Edit-EsxiVirtualStandby

`Edit-EsxiVirtualStandby` 명령으로 PowerShell을 사용하여 ESXi 가상 시스템(VM)에 대한 기존 가상 내보내기 내용을 변경할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Edit-EsxiVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-
HostPassword <String>] [-DiskProvisioning <String>] [-DiskMapping <String>] [-ProtectedServer
<String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErroAction<ActionPreference>] [-WarningAction<ActionPreference>] [-ErrorVariable String>] [-
WarningVariable <String> [-OutVariable <String>] [-OutBuffer <Int32>]
```

명령 옵션

`Edit-EsxiVirtualStandby` 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 228. Edit-EsxiVirtualStandby 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
`-all`	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
`-number`	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
`-jobtype`	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 `'transfer'`(데이터 전송), `'repository'`(리포지토리 유지 관리), `'replication'`(로컬 및 원격 복제), `'backup'`(백업 및 복원), `'bootcdbuilder'`(부팅 CD 만들기), `'diagnostics'`(로그 업로드), `'exchange'`(Exchange Server 파일

옵션	설명
	검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결 기능 검사), 'mount'(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) "time date 1", "time date 2"(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-activejobs -all
```

Edit-HyperVVirtualStandby

Edit-HyperVVirtualStandby 명령으로 PowerShell을 사용하여 Hyper-V 가상 시스템(VM)에 대한 기존 가상 내보내기 내용을 변경할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Edit-HyperVVirtualStandby [-HostName <String>] [-HostPort <String>] [-HostUserName <String>] [-
HostPassword <String>] [-VMLocation <String>] [-UseLocalMachine] [-gen2] [-UseVhdx] [-
ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram
<String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

명령 옵션

Edit-HyperVVirtualStandby 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 229. Edit-HyperVVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-all	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
-number	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부팅 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결 기능 검사), 'mount'(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-activejobs -all
```

Edit-ScheduledArchive

Edit-ScheduledArchive 명령을 통해 PowerShell을 사용하여 기존 예약된 아카이브에 변경 사항을 적용할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Edit-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -path
[location] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -scheduletype
[type] -dayofweek [name] -dayofmonth [number] -time [time] -initialpause -id [id]
```

명령 옵션

다음 표에서는 Edit-ScheduledArchive 명령에 사용 가능한 옵션에 대해 설명합니다.

표 230. Edit-ScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	아카이브하려는 복구 지점이 있는 보호된 시스템입니다. 여러 시스템 이름을 큰따옴표로 묶고 쉼표로 구분해서 지정할 수 있습니다.
-all	모든 보호된 시스템에 대한 복구 지점을 보관합니다.
-path	아카이브된 데이터를 저장할 위치의 경로입니다. 예: • 로컬 시스템: "d:\work\archive" • 네트워크 경로: "\\servername\sharename" • 클라우드 계정의 폴더: "폴더 이름" **노트: 기호 수는 로컬 및 네트워크 위치의 경우 100, 클라우드 위치의 경우 150보다 커서는 안 됩니다.**
-cloudaccountname	선택 사항. 클라우드 아카이브에만 사용합니다. 아카이브를 저장하려는 클라우드 계정의 이름입니다.
-cloudcontainer	선택 사항. 클라우드 아카이브만 사용합니다. 선택한 클라우드 계정에서 아카이브가 저장될 클라우드 컨테이너의 이름입니다. 이 옵션을 사용하는 경우 "-cloudaccountname" 매개 변수도 지정해야 합니다.
-recycleaction	재활용 작업의 유형입니다. 다음 4개의 값 중 하나를 사용하여 지정됩니다. • "replacethiscore" - 이 Core와 관련된 기존의 아카이브된 데이터를 덮어쓰지만 다른 Core에 대한 데이터는 그대로 둡니다. • "erasecompletely" - 새 아카이브를 쓰기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다. • "incremental" - 기존 아카이브에 복구 지점을 추가할 수 있습니다. 이것은 복구 지점을 비교하여 아카이브에 이미 있는 데이터의 중복 제거를 방지합니다.
-scheduletype	일정 간격의 유형입니다. 다음 4개의 값 중 하나로 옵션을 지정합니다. • "daily" - 매일 자동으로 생성되는 아카이브입니다. • "weekly" - 매주 자동으로 생성되는 아카이브입니다. "-dayofweek" 매개 변수를 지정해야 합니다. • "monthly" - 매월 자동으로 생성된 아카이브입니다. "-dayofmonth" 매개 변수를 지정해야 합니다. 달에 지정된 요일이 없는 경우(예: "31") 해당 달에 대해 아카이브가 발생하지 않습니다. • "lastdayofmonth" - 각 달의 마지막 요일에 아카이브를 자동으로 생성합니다.

옵션	설명
-dayofweek	"-scheduletype" 매개 변수의 "weekly" 옵션에만 사용합니다. 아카이브를 자동으로 생성할 주의 요일입니다(예: "Monday").
-dayofmonth	"-scheduletype" 매개 변수의 "month" 옵션에만 사용합니다. 아카이브를 자동으로 생성할 월의 날짜(숫자)입니다(예: "15").
-time	하루 중 아카이브를 생성할 시간입니다.
-initialpause	선택 사항. 아카이브 예약을 구성한 후 초기에 아카이브를 일시 중지하려는 경우 이 옵션을 지정합니다.
-id	편집하려는 예약된 아카이브의 식별자입니다.

예:

로컬 Core에서 예약된 아카이브를 편집합니다.

```
>Edit-ScheduledArchive -protectedserver protectedserver1 -path d:\work\archive -
cloudaccountname cloud1 -cloudcontainer cloudarchives -recycleaction incremental -scheduletype
daily -time 12:00 AM -initialpause -i
    d archiveid
```

Edit-VBVirtualStandby

Edit-VBVirtualStandby 명령으로 PowerShell을 사용하여 VirtualBox 가상 시스템(VM)에 대한 기존 가상 내보내기 내용을 변경할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Edit-VBVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-LinuxHostName <String>] [-HostPort <UInt32>] [-AccountUserName <String>] [-AccountPassword
<String>] [-ProtectedServer <String>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam]
[-Ram <String>] [-User <String>] [-Core <String>] [-Password <String>] [-Verbose] [-Debug] [-
ErrorAction <ActionPreference>] [-WarningAction <ActionPreference>] [-ErrorVariable <String>] [-
WarningVariable <String>] [-OutVariable <String>] [-OutBuffer <Int32>]
```

명령 옵션

Edit-VBVirtualStandby 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 231. Edit-VBVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다.

옵션	설명
	로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-all	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
-number	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부팅 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결 기능 검사), 'mount'(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-activejobs -all
```

Edit-VMVirtualStandby

Edit-VMVirtualStandby 명령으로 PowerShell을 사용하여 VMware Workstation 가상 시스템(VM)에 대한 기존 가상 내보내기 내용을 변경할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
 Edit-VMVirtualStandby [-TargetPath <String>] [-PathUserName <String>] [-PathPassword <String>]
[-ProtectedServer <S
    tring>] [-Volumes <String[]>] [-VMName <String>] [-UseSourceRam] [-Ram <String>] [-User
<String>] [-Core <String>]
    [-Password <String>] [-Verbose] [-Debug] [-ErrorAction <ActionPreference>] [-WarningAction
<ActionPreference>] [-Er
```

```
    rorVariable <String>] [-WarningVariable <String>] [-OutVariable <String>] [-OutBuffer
<Int32>]
```

명령 옵션

`Edit-VMVirtualStandby` 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 232. Edit-VMVirtualStandby 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
`-all`	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
`-number`	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
`-jobtype`	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 `'transfer'`(데이터 전송), `'repository'`(리포지토리 유지 관리), `'replication'`(로컬 및 원격 복제), `'backup'`(백업 및 복원), `'bootcdbuilder'`(부팅 CD 만들기), `'diagnostics'`(로그 업로드), `'exchange'`(Exchange Server 파일 검사), `'export'`(복구 지점 내보내기), `'pushinstall'`(에이전트 배포), `'rollback'`(복구 지점에서 복원), `'rollup'`(복구 지점 롤업), `'sqlattach'`(에이전트 연결 기능 검사), `'mount'`(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
`-time`	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-activejobs -all
```

Get-ActiveJobs

Get-ActiveJobs 명령으로 Core에서 모든 활성 작업이 반환됩니다. -jobtype 매개 변수를 사용하여 특정 작업을 관찰할 수도 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ActiveJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

명령 옵션

Get-ActiveJobs 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 233. Get-ActiveJobs 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-all	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
-number	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부팅 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결 기능 검사), 'mount'(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다.

옵션	설명
	#d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-activejobs -all
```

Get-Clusters

Get-Clusters 명령은 Core에서 보호되는 서버 클러스터에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Clusters -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 Get-Clusters 명령에 사용 가능한 옵션에 대해 설명합니다.

표 234. Get-Clusters 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core에서 보호되는 서버 클러스터를 나열합니다.

```
>Get-Clusters
```

Get-CompletedJobs

Get-CompletedJobs 명령으로 Core에서 완료된 작업 목록이 반환됩니다. -jobtype 매개 변수를 사용하여 특정 작업을 관찰할 수도 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-CompletedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

명령 옵션

Get-CompletedJobs 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 235. Get-CompletedJobs 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-all	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
-number	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부팅 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결 기능 검사), 'mount'(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다.

옵션	설명
	#d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 활성 작업을 나열합니다.

```
>Get-CompletedJobs -all
```

로컬 Core의 모든 완료된 리포지토리 생성 작업을 나열합니다.

```
>Get-CompletedJobs -jobtype repository
```

Get-ExchangeMailStores

`Get-ExchangeMailStores` 명령은 Core에 의해 보호되는 Exchange Server의 메일 저장소에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ExchangeMailStores -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

명령 옵션

다음 표에서는 `Get-ExchangeMailStores` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 236. Get-ExchangeMailStores 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

로컬 Core의 Exchange Server에 대한 Exchange 메일 저장소를 나열합니다.

```
>Get-ExchangeMailStores -protectedserver 10.10.10.10
```

Get-Failed

Get-Failed 명령은 로컬 Core의 실패한 복구 지점에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Failed -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number]
```

명령 옵션

다음 표에서는 Get-Failed 명령에 사용 가능한 옵션에 대해 설명합니다.

표 237. Get-Failed 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-number	선택 사항. 표시하는 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.

예:

모든 실패한 복구 지점을 나열합니다.

```
>Get-failed -protectedserver 10.10.10.10
```

Get-FailedJobs

`Get-FailedJobs` 명령으로 로컬 Core에서 모든 실패한 작업이 반환됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-FailedJobs -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number] -
jobtype [type] -time [time]
```

명령 옵션

`Get-FailedJobs` 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 238. Get-FailedJobs 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
`-all`	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
`-number`	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
`-jobtype`	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 `'transfer'`(데이터 전송), `'repository'`(리포지토리 유지 관리), `'replication'`(로컬 및 원격 복제), `'backup'`(백업 및 복원), `'bootcdbuilder'`(부팅 CD 만들기), `'diagnostics'`(로그 업로드), `'exchange'`(Exchange Server 파일 검사), `'export'`(복구 지점 내보내기), `'pushinstall'`(에이전트 배포), `'rollback'`(복구 지점에서 복원), `'rollup'`(복구 지점 롤업), `'sqlattach'`(에이전트 연결 기능 검사), `'mount'`(리포지토리 탑재)입니다. 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
`-time`	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.)

옵션	설명
	#h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core의 모든 실패한 작업을 나열합니다.

```
>Get-FailedJobs -all
```

로컬 Core의 모든 실패한 백업 생성 작업을 나열합니다.

```
>Get-FailedJobs -type backup
```

Get-Mounts

`Get-Mounts` 명령은 로컬 Core에 탑재된 모든 복구 지점을 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Mounts -core [host name] -user [user name] -password [password] -protectedserver [server name or IP address]
```

명령 옵션

다음 표에서는 `Get-Mounts` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 239. Get-Mounts 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

모든 마운트된 복구 지점을 표시합니다.

```
>Get-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22
```

Get-Passed

Get-Passed 명령은 Core에서 확인 검사를 통과한 복구 지점에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Passed -core [host name] -user [user name] -password [password] -protectedserver [server
name or IP address] -number [all | f[number] |l[number] | number]
```

명령 옵션

다음 표에서는 Get-Passed 명령에 사용 가능한 옵션에 대해 설명합니다.

표 240. Get-Passed 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core에서 확인 검사를 통과한 모든 복구 지점을 나열합니다.

```
>Get-Passed -protectedserver 10.10.10.10
```

Get-ProtectedServers

Get-ProtectedServers 명령은 로컬 Core에서 보호되는 시스템에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ProtectedServers -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 Get-ProtectedServers 명령에 사용 가능한 옵션에 대해 설명합니다.

표 241. Get-ProtectedServers 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core에서 현재 보호되는 모든 시스템을 나열합니다.

```
>Get-ProtectedServers
```

Get-ProtectionGroups

Get-ProtectionGroups 명령은 로컬 Core의 보호 그룹에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ProtectionGroups -core [host name] -user [user name] -password [password] -all |
-protectedserver [server name or IP address]
```

명령 옵션

다음 표에서는 Get-ProtectionGroups 명령에 사용 가능한 옵션에 대해 설명합니다.

표 242. Get-ProtectionGroups 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

로컬 Core의 보호 그룹을 나열합니다.

```
>Get-ProtectionGroups -protectedserver 10.10.10.10
```

Get-QueuedJobs

Get-QueuedJobs 명령은 Core에서 시작을 기다리는 모든 작업을 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-QueuedJobs -core [host name] -user [login] -password [password] -all | -protectedserver
[name | IP address] -nu
    mber [all | f[number] | l[number] | number] -jobtype [type] -time [time]
```

명령 옵션

다음 표에서는 Get-ActiveJobs 명령에 사용 가능한 옵션에 대해 설명합니다.

표 243. Get-ActiveJobs 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-all	Core 및 모든 보호된 서버에서 수행되는 작업을 포함하여 모든 작업을 표시합니다.
-number	선택 사항. 표시할 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 다음과 같습니다 .'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부트 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(에이전트 배포), 'rollback'(복구 지점에서 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결성 검사), 'mount'(리포지토리 마운트). 기본적으로 지정된 유형의 모든 작업이 반환됩니다.
-time	선택 사항. 작업이 시작된 날짜 및 시간을 기준으로 출력을 필터링합니다. 사용 가능한 입력 유형은 다음과 같습니다. #d 또는 DD(여기서 #은 이전부터 지금까지 기간(일 수)입니다.) #h 또는 #H(여기서 #은 이전부터 지금까지 기간(시간)입니다.) “time date 1”, “time date 2”(쉼표 앞에 표시되는 특정 날짜에서 쉼표 뒤의 특정 날짜까지 사용자 지정 기간 표시).

예:

로컬 Core에서 대기 중인 모든 작업을 표시합니다.

```
>Get-QueuedJobs -all
```

Get-RecoveryPoints

Get-RecoveryPoints 명령은 로컬 Core에서 보호되는 시스템의 복구 지점에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-RecoveryPoints -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address] -number [all | f[number] |l[number] | number]
```

명령 옵션

다음 표에서는 Get-RecoveryPoints 명령에 사용 가능한 옵션에 대해 설명합니다.

표 244. Get-RecoveryPoints 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-number	선택 사항. 표시하는 레코드 수를 결정합니다. 사용 가능한 값은 다음과 같습니다. all(모든 작업 표시), l[number] 또는 [number](실행 및 시간을 기준으로 정렬된 ##개의 최근 작업 가져오기), f[number](실행 및 시간을 기준으로 정렬된 처음 ##개의 복구 작업 표시). 기본적으로 20개의 최근 작업이 표시됩니다.

예:

로컬 Core에서 보호되는 시스템에 대한 복구 지점을 나열합니다.

```
>Get-RecoveryPoints -protectedserver 10.10.10.10
```

Get-ReplicatedServers

Get-ReplicatedServers 명령은 Core에서 복제된 시스템에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ReplicatedServers -core [host name] -user [user name] -password [password]
```

Dell은 명령을 사용하여 값을 반환할 때 보안을 고려할 것을 권장합니다. 예를 들어 이 명령은 각 복제된 서버에 대한 관리자 암호를 반환합니다. 이 명령을 MSP 환경의 대상 Core에서 사용할 경우, 관리자 사용자의 로그인 암호가 노출될 위험이 있습니다. 리포지토리 데이터가 암호화된 환경에서는 잠재적인 보안 문제가 발생하지 않습니다.

명령 옵션

다음 표에서는 Get-ReplicatedServers 명령에 사용 가능한 옵션에 대해 설명합니다.

표 245. Get-ReplicatedServers 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core의 모든 복제된 서버를 나열합니다.

```
>Get-ReplicatedServers
```

Get-Repositories

Get-Repositories 명령은 Core의 리포지토리에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Repositories -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 Get-Repositories 명령에 사용 가능한 옵션에 대해 설명합니다.

표 246. Get-Repositories 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core의 리포지토리를 나열합니다.

```
>Get-Repositories
```

Get-ScheduledArchives

`Get-ScheduledArchives` 명령을 사용하면 PowerShell로 Core와 연관된 기존 Rapid Recovery 예약 아카이브에 대한 정보를 볼 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-ScheduledArchives -core [host name] -user [login] -password [password]
```

명령 옵션

다음 표에서는 `Get-ScheduledArchives` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 247. Get-ScheduledArchives 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

이 Core에서 예약된 아카이브에 대한 정보 얻기:

```
>Get-ScheduledArchives -core 10.10.10.10 -user administrator -password password
```

Get-SqlDatabases

`Get-SqlDatabases` 명령은 지정된 보호된 시스템에서 SQL 데이터베이스 목록을 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-SqlDatabases -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

명령 옵션

다음 표에서는 Get-SqlDatabases 명령에 사용 가능한 옵션에 대해 설명합니다.

표 248. Get-SqlDatabases 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

로컬 Core의 모든 SQL 데이터베이스 작업을 나열합니다.

```
>Get-SqlDatabases -protectedserver 10.10.10.10
```

Get-UnprotectedVolumes

Get-UnprotectedVolumes 명령은 보호할 수 있지만 현재 Core에서 보호되지 않는 볼륨에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-UnprotectedVolumes
-core [host name] -user [user name] -password [password] -protectedserver [server name or IP
address]
```

명령 옵션

다음 표에서는 Get-UnprotectedVolumes 명령에 사용 가능한 옵션에 대해 설명합니다.

표 249. Get-UnprotectedVolumes 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

지정된 에이전트 시스템에서 보호 가능하지만 현재 보호되지 않는 모든 볼륨을 나열합니다.

```
>Get-UnprotectedVolumes -protectedserver 10.10.10.10
```

Get-VirtualizedServers

Get-VirtualizedServers 명령은 가상화된 서버에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-VirtualizedServers -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 Get-VirtualizedServers 명령에 사용 가능한 옵션에 대해 설명합니다.

표 250. Get-VirtualizedServers 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

로컬 Core의 모든 가상화된 서버를 나열합니다.

```
>Get-VirtualizedServers
```

Get-Volumes

Get-Volumes 명령은 Core에 의해 보호되는 지정된 시스템의 볼륨에 대한 정보를 반환합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Get-Volumes -core [host name] -user [user name] -password [password]
-protectedserver [server name or IP address]
```

명령 옵션

다음 표에서는 Get-Volumes 명령에 사용 가능한 옵션에 대해 설명합니다.

표 251. Get-Volumes 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

옵션	설명
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.

예:

지정된 시스템의 모든 볼륨을 나열합니다.

```
>Get-Volumes -protectedserver 10.10.10.10
```

New-Base

New-Base 명령은 현재 보호된 시스템에 데이터를 전송하는 새로운 기본 이미지를 작성합니다. 기본 이미지를 작성하면 전송이 즉시 시작되거나 대기열에 추가됩니다. 이전 복구 지점에서 변경된 데이터만 전송됩니다. 이전 복구 지점이 없을 경우 보호된 볼륨의 모든 데이터가 전송됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-Base [[-all] | -protectedserver [machine name]] -core [host name] -user [user name] -
password [password]
```

명령 옵션

다음 표에서는 New-Base 명령에 사용 가능한 옵션에 대해 설명합니다.

표 252. New-Base 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	모든 에이전트에 대한 기본 이미지.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 시스템의 이름에 대해 적용합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

모든 보호된 시스템에 대해 기본 이미지를 적용합니다.

```
>New-Base -all
```

New-CloudAccount

`New-CloudAccount` 명령을 사용하면 Rapid Recovery Core에 새 클라우드 계정을 추가할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-CloudAccount -core [host name] -user [login] -password [password] -displayname [display
name] -type [cloud acco
    unt type] -username [user name] - key [secret key] -region [region] - tenantid [tenant Id] -
authurl [authorization
    url]
```

명령 옵션

다음 표에서는 `New-CloudAccount` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 253. New-CloudAccount 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-displayname`	표시할 클라우드 계정 이름.
`-type`	추가할 클라우드 계정 유형. 지원되는 값은 다음과 같습니다. • amazon • openstack • rackspace • windowsazure • "windows azure" • azure
`-username`	추가할 클라우드 계정의 사용자 이름. 이 정보는 인증 프로세스에 사용됩니다. 이 속성은 Amazon™ 클라우드에서 "액세스 키", Rackspace 및 OpenStack에서 "사용자 이름", Windows Azure 클라우드 계정에서 "저장소 계정 이름"으로 사용됩니다.
`-key`	추가할 클라우드 계정의 키. 이 정보는 인증 프로세스에 사용됩니다. 이 속성은 Amazon™ 클라우드에서 "비밀 키", Rackspace 및 OpenStack에서 "API 키", Windows Azure 클라우드 계정에서 "액세스 키"로 사용됩니다.
`-region`	추가할 클라우드 계정의 지역. 이 속성은 RackSpace 및 OpenStack 클라우드 계정에서만 필요합니다.

옵션	설명
-tenantid	OpenStack 클라우드 계정의 인증 프로세스에 사용되는 식별자. OpenStack 클라우드 계정에 대해서만 이 옵션이 필요합니다.
-authurl	OpenStack 클라우드 계정의 인증 프로세스에 사용되는 URL. OpenStack 클라우드 계정에 대해서만 이 옵션이 필요합니다.

예:

액세스 키 "akey" 및 비밀 키 "skey"를 사용하여 새 Amazon™ S3 클라우드 계정, "Amazon S3 Account"를 만듭니다.

```
>New-CloudAccount -displayname "Amazon S3 Account" -type Amazon -username akey -key skey
```

New-EncryptionKey

New-EncryptionKey 명령은 Rapid Recovery 백업 데이터를 보호하기 위한 새로운 암호화 키를 생성합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-EncryptionKey -core [host name] -user [login] -password [password] -name [encryption key
name] -passphrase [pas
    sphrase] -comment [comment]
```

명령 옵션

다음 표에서는 New-EncryptionKey 명령에 사용 가능한 옵션에 대해 설명합니다.

표 254. New-EncryptionKey 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-name	생성하려는 암호화 키의 이름입니다.
-passphrase	생성하려는 암호화 키의 암호입니다.
-comment	선택 사항. 암호화 키에 대한 설명입니다.

예:

로컬 Core의 암호화 키를 생성합니다.

```
>New-EncryptionKey -name EncryptionKey1 -passphrase 123456
```

New-EsxiVirtualStandby

`New-EsxiVirtualStandby` PowerShell 명령으로 Rapid Recovery를 사용하여 새 ESXi 가상 대기 시스템을 만들 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-EsxiVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] -hostname [virtual
host name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host password] [-ram [total megabytes] | -usesourceram] -diskprovisioning
[thin | thick] -diskmapping [automatic | manual | withvm] -initialexport
```

명령 옵션

`New-EsxiVirtualStandby` 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 255. New-EsxiVirtualStandby 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
`-volumes`	선택 사항. 내보내려는 볼륨 이름이 나열됩니다. 지정하지 않으면 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다(예: "c:", "d:"). **노트: 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.**
`-vmname`	가상 시스템의 Microsoft Windows 이름.
`-hostname`	가상 서버 호스트 이름.
`-hostport`	가상 서버와 통신하는 데 사용되는 포트 번호.

옵션	설명
-hostusername	가상 서버 호스트에 로그인하는 사용자 이름.
-hostpassword	가상 서버 호스트에 로그인하는 암호.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 보호된 원본 시스템과 같은 RAM 용량을 가상 서버에 할당합니다.
-diskprovisioning	선택 사항. 가상 시스템에 할당할 디스크 공간 용량. 사용 가능한 값은 다음과 같습니다. • Thick - 가상 디스크의 용량을 보호된 서버의 원래 드라이브만큼 할당하려면 'thick'을 지정합니다. • Thin - 원래 드라이브에서 차지하는 실제 디스크 공간 용량에 일부 추가 용량을 더하여 할당하려면 'thin'을 지정합니다. 기본 디스크 프로비저닝은 'thin'입니다.
-diskmappinjg	선택 사항. 디스크를 복구 지점에서 가상 시스템으로 매핑하는 방법이 결정됩니다. 사용 가능한 값은 다음과 같습니다. • 'auto' • 'manual' • 'withvm' 기본 설정은 'auto'입니다.
-initialexport	선택 사항. 가상 대기 모드를 구성한 후 초기 주문형 가상 시스템 내보내기를 시작해야 하는 경우 이 옵션을 지정합니다.

예:

새 ESXi 가상 대기 모드를 다음과 같이 만듭니다.

```
>New-EsxiVirtualStandby -protectedserver 10.10.10.4 -vmname ExportedMachine -hostname
10.10.10.127 -hostport 443 -hostusername root -hostpassword pass123 -usesourceram -
diskprovisioning thin -diskmapping auto
```

New-HyperVVirtualStandby

New-HyperVVirtualStandby PowerShell 명령으로 Rapid Recovery를 사용하여 새 Hyper-V 가상 시스템(VM)를 만들 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

명령 옵션

New-HyperVVirtualStandby 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 256. New-HyperVVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-volumes	선택 사항. 내보내려는 볼륨 이름이 나열됩니다. 지정하지 않으면 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다(예: "c:", "d:"). **노트: 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.**
-vmname	가상 시스템의 Microsoft Windows 이름.
-gen2	선택 사항. 두 번째 VM 생성을 사용하려면 지정합니다. 지정하지 않으면 생성 1이 사용됩니다. Rapid Recovery에서는 Windows 8.1을 통해 Windows Server 2012 R2의 생성 2가 지원됩니다.
-usevhdx	선택 사항. 이 옵션을 지정하면 Rapid Recovery에서 VHDX 디스크 형식을 사용하여 VM을 만듭니다. 지정하지 않으면 VHD 디스크 형식이 사용됩니다. 생성 2에는 VHDX 형식만 사용됩니다.
-uselocalmachine	선택 사항. 로컬 Hyper-V 서버에 연결합니다. 이 값을 무시하면 다음 옵션이 Rapid Recovery에서 무시됩니다. • 호스트 이름 • hostport • hostusername • hostpassword
-hostname	가상 서버 호스트 이름.
-hostport	가상 서버와 통신하는 데 사용되는 포트 번호.
-hostusername	가상 서버 호스트에 로그인하는 사용자 이름.
-hostpassword	가상 서버 호스트에 로그인하는 암호.
-vmlocation	가상 시스템 파일을 저장하려는 폴더에 대한 로컬 또는 네트워크 경로
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 보호된 원본 시스템과 같은 RAM 용량을 가상 서버에 할당합니다.

옵션	설명
-initialexport	선택 사항. 가상 대기 모드를 구성한 후 초기 주문형 가상 시스템 내보내기를 시작해야 하는 경우 이 옵션을 지정합니다.

예:

새 Hyper-V 가상 대기 시스템을 다음과 같이 만듭니다.

```
>New-HyperVVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address]
    -volumes [volumes names] -vmname [virtual machine name] [-gen2] -useVhdx [-uselocalmachine]
| -hostname [virtual ho
    st name] -hostport [virtual host port number] -hostusername [virtual host login] -
hostpassword [virtual host passwo
    rd]] -vmlocation [location] [-ram [total megabytes] | -usesourceram] -initialexport
```

New-Mount

New-Mount 명령으로 드라이브 하나 이상의 스냅숏이 탑재됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-Mount -core [host name] -user [user name] -password [password] -protectedserver [machine
name] -mounttype [read | write | readonlywithpreviouswrites] -drives [drive names] -path
[location] -time [MM/DD/YYYY hh:mm:ss tt | passed | latest] -rpn [number]
```

명령 옵션

New-Mount 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 257. New-Mount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-protectedserver	보호된 서버 IP 주소 또는 시스템 이름(특정 시스템이 보호된 방법에 따라 다름).
-time	선택 사항. 마운트할 복구 지점의 타임스탬프. 현재 PC의 OS에 의해 지정된 형식이어야 합니다. 관리자는 전달된 매개 변수 값에 의해 최근 또는 마지막으로 확인된 복구 지점을 지정하여 최근 복구 지점을 얻을 수 있습니다. 기본적으로 마지막 시간 옵션이 선택됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

옵션	설명
-path	Core 시스템에 복구 지점을 마운트할 경로.
-mounttype	선택 사항. 마운트 모드를 지정합니다. 사용 가능한 옵션은 'read', 'readOnlyWithPreviousWrites'(이전 쓰기가 포함된 읽기 전용), 'write' (쓰기 가능)입니다. 기본 모드는read-only입니다.
-volumes	선택 사항. 공백으로 구분된 마운트할 볼륨 이름 목록. 볼륨 이름에 공백이나 특수 문자가 있을 경우에는 큰따옴표를 사용하여 지정해야 합니다. 이 옵션을 지정하지 않으면 모든 볼륨이 마운트됩니다.
-drivers	선택 사항. 쉼표로 구분된 마운트할 볼륨 이름 목록. 이 옵션을 지정하지 않으면 모든 볼륨이 마운트됩니다. **노트: 이 옵션은 사용되지 않으므로 '-volumes'를 대신 사용합니다.**
-rpn	선택 사항. 마운트 복구 지점 번호. get-mounts 명령으로 이 번호를 가져올 수 있습니다. 단일 명령으로 서로 다른 지점을 탑재하려면 rpn 매개 변수에 여러 번호를 지정합니다. **노트: 마운트할 지점 배열을 설정하면 각 지점이 별도의 하위 디렉터리에 배치됩니다. 이름은 복구 지점이 생성된 시간을 나타냅니다. dismount를 호출하면 모든 하위 디렉터리가 제거됩니다. 수동으로 상위 디렉터리를 제거해야 합니다.**

예:

```
>New-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22 -path C:\MountedRecoveryPoint -mounttype read -volumes c “d, ko”
```

복구 지점 배열을 마운트합니다.

```
>New-Mount -rpn 10 52 41 -protectedserver localhost -path “D:/Folder for mount”
```

특정 시간에 생성된 복구 지점을 마운트합니다.

```
>New-Mount -protectedserver 10.10.5.56 -path “D:/Folder for mount” -time “8/24/2012 11:46 AM”
```

Resume-Replication

New-Replication 명령은 보호된 단일 서버 또는 다중 서버에 대한 복제를 설정 및 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-Replication -core [host name] -user [login] -password [password] -targetserver [host name] -
protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 New-Replication 명령에 사용 가능한 옵션에 대해 설명합니다.

표 258. New-Replication 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-replicationname	대상 Core의 복제 구성 이름입니다.
-targetserver	대상 Core의 호스트 이름과 사용자 이름, 암호입니다.
-protectedserver	복제를 설정하기 위한 대상 Core의 보호된 시스템과 리포지토리 이름입니다.

예:

IP 10.10.10.4 주소를 가진 보호된 시스템에 대한 새로운 복제를 생성합니다.

```
>New-Replication -targetserver 10.10.10.128 -protectedserver 10.10.10.4
```

New-Repository

New-Repository 명령은 Rapid Recovery Core에 새 DVM 리포지토리를 생성합니다. 250MB와 16TB 사이의 크기를 지정해야 합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-Repository | -name [name] -size [size] -datapath [location] -metadatapath [location]
```

명령 옵션

다음 표에서는 New-Repository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 259. New-Repository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-name	리포지토리 이름.
-size	리포지토리 범위 크기. 사용 가능한 단위는 b, Kb, MB, GB, TB, PB입니다.
-datapath	로컬 위치에만 해당. 리포지토리 범위의 데이터 경로를 지정합니다.
-metadatapath	로컬 위치에만 해당. 리포지토리 범위의 메타데이터 경로를 지정합니다.
-uncpath	공유 위치에만 해당. 리포지토리 범위의 데이터 및 메타데이터 경로를 결정합니다.
-shareusername	공유 위치에만 해당. 공유 위치 로그인 ID를 결정합니다.
-sharepassword	공유 위치에만 해당. 공유 위치 암호를 결정합니다.
-comment	선택 사항. 리포지토리 설명.
-concurrent Operations	선택 사항. 동시에 보류 가능한 최대 작업 수. 기본값은 64입니다.

예:

로컬 드라이브 E에 최소 크기의 새 DVM 리포지토리를 만듭니다.

```
>New-Repository -name Repository2 -size 250Mb -datapath e:\Repository\Data -metadatapath e:
\Repository\Metadata
```

New-ScheduledArchive

New-ScheduledArchive 명령으로 PowerShell을 사용하여 기존에 예약한 아카이브를 변경할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-ScheduledArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address] -path [location] -archiveusername [name] -archivepassword
[password] -cloudaccountname [name] -cloudcontainer [name] -recycleaction [type] -schdeuletype
[type] -dayofweek [name] -dayofmonth [number] -time [time]
```

명령 옵션

다음 표에서는 New-ScheduledArchive 명령에서 사용할 수 있는 옵션에 대해 설명합니다.

표 260. New-ScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	아카이브할 복구 지점이 포함된 보호된 시스템. 여러 시스템 이름을 큰따옴표로 묶고 쉼표로 구분해서 지정할 수 있습니다.
-all	모든 보호된 시스템에 대한 복구 지점 아카이브.
-path	아카이브된 데이터를 저장할 경로. 예: • 로컬 시스템: "d:\work\archive" • 네트워크 경로: "\\servername\sharename" • 클라우드 계정에 있는 폴더: "폴더 이름" **노트: 로컬 및 네트워크 위치에 대한 기호 수는 100자 이하여야 하고, 클라우드 위치에 대한 기호 수는 150자 이하여야 합니다.**
-archiveusername	선택 사항. 원격 시스템에 로그인할 사용자 이름. 네트워크 경로에만 필요합니다.
-archivepassword	선택 사항. 원격 시스템에 로그인할 암호. 네트워크 경로에만 필요합니다.
-cloudaccountname	선택 사항. 클라우드 아카이브에만 사용합니다. 아카이브를 저장할 클라우드 계정의 이름.
-cloudcontainer	선택 사항. 클라우드 아카이브에만 사용합니다. 아카이브를 저장할 선택한 클라우드 계정에 있는 클라우드 컨테이너의 이름. 이 옵션을 사용하는 경우 "-cloudaccountname" 매개 변수도 지정해야 합니다.
-recycleaction	재활용 작업 유형. 다음 4개 값 중 하나를 사용하여 지정합니다. • "replacethiscore" - 이 Core와 관련하여 아카이브된 기존 데이터를 덮어쓰지만 다른 Core의 데이터는 그대로 남아 있게 됩니다. • "erasecompletely" - 새 아카이브를 쓰기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다. • "incremental" - 기존 아카이브에 복구 지점을 추가할 수 있습니다. 이것은 복구 지점을 비교하여 아카이브에 이미 있는 데이터의 중복 제거를 방지합니다.
-scheduletype	일정 간격 유형. 다음 4개 값 중 하나로 옵션을 지정합니다. • "daily" - 매일 자동으로 생성된 아카이브. • "weekly" - 매주 자동으로 생성된 아카이브. "-dayofweek" 매개 변수를 지정해야 합니다. • "monthly" - 매월 자동으로 생성된 아카이브. "-dayofmonth" 매개 변수를 지정해야 합니다. 월에 지정된 날짜가 없는 경우(예: "31") 해당 월에는 아카이브가 발생하지 않습니다. • "lastdayofmonth" - 매월 마지막 날 자동으로 아카이브 생성.

옵션	설명
-dayofweek	"-scheduletype" 매개 변수의 "weekly" 옵션에만 사용합니다. 자동으로 아카이브를 생성할 요일(예: "월요일").
-dayofmonth	"-scheduletype" 매개 변수의 "month" 옵션에만 사용합니다. 자동으로 아카이브를 생성할 날짜(숫자)(예: "15").
-time	아카이브를 생성할 시간.
-initialpause	선택 사항. 아카이브 일정을 구성한 후 처음에는 아카이브를 일시 중지하려면 이 옵션을 지정합니다.

예:

Core에 있는 모든 시스템에 대해 2012/04/30 02:55 PM 이후의 생성 날짜가 포함된 모든 복구 지점을 아카이브하고, 이 Core와 관련하여 아카이브된 기존 데이터를 대체합니다.

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path "d:\work
\archive" -s
    tartdate "04/30/2012 02:55 PM" -all -recycleaction replacethiscore
```

두 대의 보호된 시스템에서 날짜 범위 내에 있는 복구 지점을 아카이브하고 새 아카이브를 쓰기 전에 디렉터리에서 아카이브된 데이터를 모두 지웁니다.

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver "10.20.30.40" "20.20.10.1" -path "d:\work\archive" -startdate "04/30/2012 02:55
PM" -enddate "05/31/2012 11:00 AM" -recycleaction erasecompletely
```

Core에 있는 모든 시스템에 대해 2012/04/30 02:55 PM 이후의 생성 날짜가 포함된 모든 복구 지점에 대한 증분 아카이브를 "Amazon S3"라는 이름의 클라우드 계정과 "Container"라는 컨테이너에 생성합니다.

```
>New-ScheduledArchive -core 10.10.10.10 -user administrator -password 23WE@#$sdd -path
"ArchiveOnCloud" -cloudaccountname "Amazon S3" -cloudcontainer "Container" -startdate
"04/30/2012 02:55 PM" -all -recycleaction incremental
```

New-Snapshot

New-Snapshot 명령은 현재 보호된 시스템에 대한 데이터를 전송하게 될 스냅숏을 작성합니다. 스냅숏을 작성하면 전송이 즉시 시작되거나 대기열에 추가됩니다. 이전 복구 지점에서 변경된 데이터만 전송됩니다. 이전 복구 지점이 없을 경우 보호된 볼륨의 모든 데이터가 전송됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-Snapshot [-all] | -protectedserver [machine name]] -core [host name] -user [user name] -
password [password]
```

명령 옵션

다음 표에서는 New-Snapshot 명령에 사용 가능한 옵션에 대해 설명합니다.

표 261. New-Snapshot 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	모든 보호된 컴퓨터의 스냅숏을 작성합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 시스템의 이름에 대해 적용합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

모든 보호된 컴퓨터에 대해 스냅숏을 작성합니다.

```
>New-Snapshot -all
```

New-VBVirtualStandby

New-VBVirtualStandby 명령으로 PowerShell을 사용하여 VirtualBox 가상 시스템(VM)에 대한 새 가상 내보내기를 만들 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-VBVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram]  -linuxhostname [linux hostname] -hostport [linux port] -targetpath
[location] -pathusername [login] -pathpassword [password] -initialexport
```

명령 옵션

New-VBVirtualStandby 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 262. New-VBVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다.

옵션	설명
	로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-volumes	선택 사항. 내보내려는 볼륨 이름이 나열됩니다. 지정하지 않으면 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다(예: "c:", "d:"). **노트: 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.**
-vmname	가상 시스템의 Microsoft Windows 이름.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 보호된 원본 시스템과 같은 RAM 용량을 가상 서버에 할당합니다.
-linuxhostname	Linux VirtualBox 서버 호스트 이름.
-hostport	Linux VirtualBox 서버 포트.
-targetpath	가상 시스템 파일을 저장하려는 폴더에 대한 로컬, 네트워크 또는 Linux 경로
-pathusername	네트워크 시스템에 로그인하는 사용자 이름. 대상 경로의 네트워크 위치를 지정하는 경우에만 필요합니다.
-pathpassword	네트워크 시스템에 로그인하는 암호. 대상 경로의 네트워크 위치를 지정하는 경우에만 필요합니다.
-accountusername	선택 사항. 내보낸 가상 시스템을 등록하는 사용자 계정을 지정할 수 있습니다. 사용자 계정에 로그인하는 사용자 이름입니다. 로컬 또는 네트워크 시스템에만 이 옵션을 사용합니다.
-accountpassword	선택 사항. 내보낸 가상 시스템을 등록하는 사용자 계정을 지정할 수 있습니다. 사용자 계정에 로그인하는 암호입니다. 로컬 또는 네트워크 시스템에만 이 옵션을 사용합니다.
-initialexport	선택 사항. 가상 대기 모드를 구성한 후 초기 주문형 가상 시스템 내보내기를 시작해야 하는 경우 이 옵션을 지정합니다.

예:

ExportedMachine1이라는 이름의 VirtualBox 가상 대기 시스템을 다음 지정된 위치에 만듭니다.

```
>New-VBVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

New-VMVirtualStandby

New-VMVirtualStandby PowerShell 명령을 사용하면 Rapid Recovery를 사용하는 새 VMware Workstation 가상 대기 시스템을 생성할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
New-VMVirtualStandby -core [host name] -user [login] -password [password] -protectedserver
[name | IP address] -volumes [volumes names] -vmname [virtual machine name] [-ram [total
megabytes] | -usesourceram] -targetpath [location] -pathusername [login] -pathpassword
[password] -initialexport
```

명령 옵션

다음 표에서는 New-VMVirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 263. New-VMVirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	IP 주소로 표시되는 특정 보호된 시스템에 대한 작업을 표시합니다.
-volumes	선택 사항. 내보낼 볼륨 이름을 표시합니다. 지정하지 않은 경우 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 예: "c:", "d:". **노트: 볼륨 이름 뒤에 슬래시를 사용하지 마십시오.**
-vmname	가상 시스템의 Microsoft Windows 이름.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 가상 서버에 보호된 소스 시스템과 동일한 RAM 용량을 할당합니다.
-pathusername	네트워크 시스템에 로그인하기 위한 사용자 이름. 대상 경로에 대한 네트워크 위치를 지정하는 경우에만 필요합니다.
-pathpassword	네트워크 시스템에 로그인하기 위한 암호. 대상 경로에 대한 네트워크 위치를 지정하는 경우에만 필요합니다.
-initialexport	선택 사항. 가상 대기를 구성한 후 첫 주문형 가상 시스템 내보내기를 시작해야 하는 경우 이 옵션을 지정합니다.

예:

새 VMware Workstation 가상 대기를 생성합니다.

```
>New-VMVirtualStandby -protectedserver 10.10.10.4 -volumes C:\ -vmname ExportedMachine1 -
usesourceram -targetpath I:\VMExport
```

스크립트를 일시 중지하고 이때 사용자가 적절한 워크스테이션에 대한 색인 번호를 지정해야 합니다. 완료할 스크립트의 색인 번호를 입력합니다(이 경우 2). 다시 예가 계속됩니다.

```
2
Verify location ...
Virtual Standby successfully configured
PS C:\Users\Administrator>
```

Push-Replication

`Push-Replication` 명령은 하나 이상의 보호된 시스템에 대해 복제를 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Push-Replication -core [host name] -user [user name] -password [password] -targetcore [host
name] -all | -protectedserver [machine name | IP address]
```

명령 옵션

다음 표에서는 `Push-Replication` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 264. Push-Replication 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-all`	대상 Core에 복제되는 모든 시스템에 대해 복제를 수행합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	복제를 수행하는 대상 Core의 보호된 시스템 이름.
`-user`	선택 사항. 원격 Core 호스트 시스템의 로그인. 로그인을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

단일 보호된 시스템에 대해 복제를 수행합니다.

```
>Push-Replication -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
-targetcore 10.10.10.20:8006 -protectedserver 10.10.5.22
```

모든 보호된 시스템에 대해 복제를 수행합니다.

```
>Push-Replication -all
```

Push-Rollup

Push-Rollup 명령은 보호된 시스템에 대해 롤업을 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Push-Rollup -core [host name] -user [user name] -password [password] -protectedserver [machine
name | IP address]
```

명령 옵션

다음 표에서는 Push-Rollup 명령에 사용 가능한 옵션에 대해 설명합니다.

표 265. Push-Rollup 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	모든 보호된 컴퓨터의 스냅숏을 작성합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 시스템의 이름에 대해 적용합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 로그인. 로그인을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

단일 보호된 시스템에 대해 롤업을 수행합니다.

```
>Push-Rollup -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -protectedserver
10.10.5.22
```

모든 보호된 시스템에 대해 롤업을 수행합니다.

```
>Push-Rollup -all
```

Remove-Agent

Remove-Agent PowerShell 명령은 Rapid Recovery Core 보호에서 시스템을 제거합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-Agent -core [host name] -user [login] -password [password] -protectedserver [name | IP address] -deleterecoverypoints -all
```

명령 옵션

다음 표에서는 Remove-MountAgent 명령에 사용 가능한 옵션에 대해 설명합니다.

표 266. Remove-Agent 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 시스템에 대해 마운트된 복구 지점을 모두 분리합니다.
-deleterecoverypoints	선택 사항. 이 보호된 시스템의 모든 복구 지점을 삭제합니다.
-all	선택 사항. Core에서 모든 보호된 시스템을 삭제합니다.

예:

모든 보호된 시스템과 해당 복구 지점을 분리합니다.

```
>Remove-Agent -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -deleterecoverypoints -all
```

Remove-Mount

Remove-Mount 명령은 /Path로 지정된 마운트된 복구 지점을 분리합니다. -protectedserver 매개 변수를 사용하여 선택한 시스템에 대해 지점을 분리하거나 -all 매개 변수를 사용하여 모든 마운트된 복구 지점에 대해 지점을 분리합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-Mount -core [host name] -user [user name] -password [password] [-
protectedserver [machine name] | -path [mount path]]
```

명령 옵션

다음 표에서는 Remove-Mount 명령에 사용 가능한 옵션에 대해 설명합니다.

표 267. Remove-Mount 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	모든 마운트된 복구 지점을 분리합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-path	선택한 마운트 지점을 분리합니다.
-protectedserver	현재 보호된 시스템에 대해 마운트된 복구 지점을 모두 분리합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

경로에 의해 지정된 복구 지점을 분리합니다.

```
>Remove-Mount -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -path C:
\mountedRecoveryPoint
```

Remove-Mounts

Remove-Mounts 명령은 모든 마운트된 복구 지점을 분리합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-Mounts -core [host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 Remove-Mounts 명령에 사용 가능한 옵션에 대해 설명합니다.

표 268. Remove-Mounts 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.

예:

지정된 Core의 모든 복구 지점을 분리합니다.

```
>Remove-Mounts -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd
```

Remove-RecoveryPoints

Remove-RecoveryPoints PowerShell 명령을 사용하면 특정 시스템의 복구 지점을 삭제할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-RecoveryPoints -core [host name] -user [login] -password [password] -[range | chain |
all] -protectedserver
    [name | IP address] -rpn [number | numbers] | -time [time string | time interval specified
by two time strings]
```

명령 옵션

다음 표에서는 Remove-RecoveryPoints 명령에 사용 가능한 옵션에 대해 설명합니다.

표 269. Remove-RecoveryPoints 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 시스템에 대해 마운트된 복구 지점을 모두 분리합니다.
-rpn	선택 사항. 체인 삭제의 경우만(증분 또는 분리된 지점의 체인을 포함하는 기본 이미지). 삭제할 복구 지점의 일련 번호(번호를 얻으려면 Get-RecoveryPoints 명령 사용). 여러 번호를 공백으로 구분하여 지정하여 명령 하나로 여러 복구 지점을 삭제할 수 있습니다.
-time	복구 지점의 체인을 삭제하려면 이 옵션을 사용합니다. 선택 사항. 단일 복구 지점을 삭제하려면 해당 생성 시간으로 복구 지점을 선택합니다. 정확한 시간을 “mm/dd/yyyy hh:mm tt” 형식으로 지정합니다(예: “2/24/2012 09:00 AM”). 컴퓨터에 설정된 날짜 및 시간 값을 지정해야 합니다. 필수. 날짜 범위의 경우 쉼표와 공백으로 분리된 두 개의 시간 문자열을 사용하여 시간 간격을 지정하여 삭제할 복구 지점 범위를 선택합니다.
-range	선택 사항. 시간 간격으로 삭제할 복구 지점 범위.
-chain	선택 사항. 복구 지점 생성 시간이나 복구 지점 번호를 통해 삭제하도록 선택한 분리된 지점의 순차 집합 또는 순차 증분 집합을 포함하는 기본 이미지.
-all	선택 사항. Core에서 보호하는 모든 시스템을 삭제합니다.

예:

다음과 같이 날짜로 지정된 복구 지점을 삭제합니다.

```
>Remove-RecoveryPoints -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -time
"2/24/2012 09:00 AM"
```

Remove-Repository

Remove-Repository PowerShell 명령은 Core에서 Rapid Recovery 리포지토리와 해당 내용을 삭제합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-Repository -core [host name] -user [login] -password [password] -name [repository name] -
all
```

명령 옵션

다음 표에서는 Remove-Repository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 270. Remove-Repository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-name	삭제하려는 리포지토리의 이름입니다.
-all	이 Core와 연관된 모든 리포지토리를 삭제합니다.

예:

로컬 Core의 모든 리포지토리를 제거합니다.

```
>Remove-repository -all
```

Remove-ScheduledArchive

Rapid Recovery에서 정기적으로 특정 시스템의 복구 지점을 아카이브하도록 예약한 경우, Remove-ScheduledArchive PowerShell 명령을 사용하여 예약된 이 아카이브를 Core에서 제거할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id |
id1 id2]
```

명령 옵션

다음 표에서는 Remove-ScheduledArchive 명령에 사용 가능한 옵션에 대해 설명합니다.

표 271. Remove-ScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	이 Core와 관련된 모든 아카이브를 제거합니다.
-id	제거하려는 아카이브의 식별자입니다. 여러 개의 아카이브를 나열합니다(공백으로 각 ID 구분).

예:

여러 개의 예약된 아카이브를 로컬 Core에서 제거합니다.

```
>Remove-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-
dffc49f50e25
```

Remove-VirtualStandby

Rapid Recovery에서 지속적으로 가상 시스템에 데이터 내보내기 작업을 예약한 경우, Remove-VirtualStandby PowerShell 명령을 사용하여 이 예약된 작업을 취소하고 삭제할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Remove-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP ad
    dress]
```

명령 옵션

다음 표에서는 Remove-VirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 272. Remove-VirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	이 Core와 관련된 모든 가상 대기 작업을 제거합니다.
-protectedserver	가상 대기 작업을 제거하려는 보호된 시스템의 이름 또는 IP 주소입니다.

예:

이 Core와 관련된 모든 가상 대기 작업을 제거합니다.

```
>Remove-VirtualStandby -all
```

Resume-Replication

Resume-Replication 명령을 사용하여 복제를 다시 시작할 수 있습니다. 자세한 내용은 Suspend-Replication을(를) 참조하십시오.

용도

이 명령의 사용법은 다음과 같습니다.

```
Resume-Replication -core [host name] -user [user name] -password [password] -all | -
protectedserver [machine name | IP address] -incoming [host name] | -outgoing [host name]
```

명령 옵션

다음 표에서는 Resume-Replication 명령에 사용 가능한 옵션에 대해 설명합니다.

표 273. Resume-Replication 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 보호된 서버.
-protectedserver	지정된 시스템에 대해 복제를 다시 시작합니다.

옵션	설명
-incoming	Core 시스템에 복제하는 원격 Core의 호스트 이름. 원격 Core의 모든 보호된 시스템에 대해 복제가 다시 시작됩니다.
-outgoing	데이터가 복제되는 원격 대상 Core의 호스트 이름. 원격 Core의 모든 보호된 시스템에 대해 복제가 다시 시작됩니다.

예:

로컬 Core의 IP 주소가 10.10.10.128인 보호된 시스템에 대한 복제를 다시 시작하고, 사용되는 리포지토리를 지정합니다.

```
>Resume-Replication replicationname Replication1 -targetserver 10.10.10.128,Administrator,
123asdQ -protectedserver 10.10.10.4

# Repository
- ----------

1 Repository A
2 Repository B
Please, input number of Repository from the list above or type 'exit' to exit:
```

스크립트가 일시 중지되고, 사용자는 해당 리포지토리의 색인 번호를 지정해야 합니다. 스크립트의 색인 번호를 입력하여 작업을 완료합니다(이 경우 2). 예 계속:

```
2
Replication job was started.
True
PS C:\Users\Administrator>
```

Resume-Snapshot

관리자는 스냅숏을 다시 시작하고 가상 시스템으로 내보내거나 복제를 수행할 수 있습니다. 자세한 내용은 Start-VMExport을(를) 참조하십시오.

용도

이 명령의 사용법은 다음과 같습니다.

```
Resume-Snapshot -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 Resume-Snapshot 명령에 사용 가능한 옵션에 대해 설명합니다.

표 274. Resume-Snapshot 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.

옵션	설명
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 보호된 서버.
-protectedserver	지정된 컴퓨터에 대해 스냅숏을 다시 시작합니다.

예:

로컬 Core의 IP가 10.10.10.4인 보호된 컴퓨터의 스냅숏을 다시 시작합니다.

```
>Resume-Snapshot -protectedserver 10.10.10.4
```

Resume- virtualstandby

Resume-VirtualStandby PowerShell 명령은 Rapid Recovery 가상 대기 시스템에 대해 일시 중단된 데이터 내보내기를 다시 시작합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Resume-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

명령 옵션

다음 표에서는 Resume-VirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 275. Resume-VirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 가상 대기 시스템에 대한 내보내기를 다시 시작합니다.

옵션	설명
-protectedserver	다시 시작하려는 가상 대기 시스템이 실행되는 보호된 시스템의 이름(쉼표 및 공백으로 구분)입니다.

예:

보호된 시스템에 대한 가상 대기 내보내기를 다시 시작합니다.

```
>Resume-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Resume-VMExport

Resume-VMExport 명령을 사용하여 관리자가 가상 시스템으로 내보낼 수 있습니다. 자세한 내용은 Suspend-VMExport을(를) 참조하십시오.

용도

이 명령의 사용법은 다음과 같습니다.

```
Resume-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 Resume-VMExport 명령에 사용 가능한 옵션에 대해 설명합니다.

표 276. Resume-VMExport 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 보호된 서버.
-protectedserver	지정된 컴퓨터에 대해 스냅숏을 다시 시작합니다.

예:

로컬 Core의 각 보호된 컴퓨터에 대해 가상 시스템으로 내보내기를 다시 시작합니다.

```
>Resume-VMExport -all
```

Start-Archive

종종 회사에서는 장기 저장 장치를 사용하여 준수 및 비준수 데이터를 모두 아카이브합니다. Rapid Recovery의 아카이브 기능은 준수 및 비준수 데이터의 장기 보존을 지원하는 데 사용됩니다. 관리자는 `/Path` 명령과 자격 증명을 지정하여 로컬 저장 장치 또는 네트워크 위치에 아카이브를 저장할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-Archive -path -startdate -enddate [-all] | -protectedserver [machine name] or [IP]] -core
[host name] -user [user name] -password [password]
```

명령 옵션

다음 표에서는 `Start-Archive` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 277. Start-Archive 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-path`	위치 경로. 경로 예: 'D:\work\archive' 또는 네트워크 경로: '\\servername\sharename'.
`-all`	Core의 모든 시스템에 대한 복구 지점을 아카이브합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-startdate`	복구 지점을 만든 날짜 범위의 시작 날짜. 현재 PC의 OS에 의해 지정된 형식이어야 합니다.
`-enddate`	날짜 범위의 종료 날짜. 기본값은 현재 시간입니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	지정된 시스템에 대해 복구 지점을 아카이브합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-archiveusername`	선택 사항. 네트워크 경로에만 필요합니다.
`-archivepassword`	선택 사항. 네트워크 경로에만 필요합니다.
`-comment`	선택 사항. 예: `-comment 'Before install new application'`.

예:

Core의 모든 시스템에 대한 복구 지점을 아카이브합니다.

```
>Start-Archive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-AttachabilityCheck

`Start-AttachabilityCheck` 명령은 Core에 의해 보호되는 모든 SQL Server 데이터베이스에 대해 연결성 검사를 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-AttachabilityCheck -core [host name] -user [username] - password [password]
- protectedserver [machine name | IP address] -rpn [number | numbers] | -time [time string]
```

명령 옵션

다음 표에서는 `Start-AttachabilityCheck` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 278. Start-AttachabilityCheck 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	SQL 연결성 검사를 수행할 보호된 시스템.
`-rpn`	선택 사항. SQL 연결성 검사를 수행할 복구 지점의 순차적인 번호. `-GetRecoveryPoints` 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다. 공백으로 구분된 여러 번호를 사용하여 명령 하나로 여러 복구 지점을 검사할 수 있습니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점이 연결성 검사에 사용됩니다.**
`-time`	선택 사항. SQL 연결성 검사에 사용할 복구 지점을 지정합니다. "MM/DD/YYYY hh:mm tt"(예: "04/24/2015 09:00 AM") 형식으로 정확한 시간을 지정해야 합니다. 로컬 시스템에 설정된 시간대의 날짜/시간 값을 지정합니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**

예:

지정된 보호된 SQL Server의 가장 최근 복구 지점에 대해 SQL 연결성 검사를 수행합니다.

```
>Start-AttachabilityCheck - protectedserver 10.10.9.120
```

Start- checksumcheck

`Start-ChecksumCheck` PowerShell 명령은 Exchange Server 복구 지점의 체크섬 검사를 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-ChecksumCheck -core [host name] -user [login] -password [password] -protectedserver [name
| IP address] -rpn [number | numbers] | -time [time string]
```

명령 옵션

다음 표에서는 `Start-ChecksumCheck` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 279. Start-ChecksumCheck 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	보호된 시스템의 이름.
`-rpn`	선택 사항. 체인 삭제에만 해당(증분 또는 분리된 지점의 체인이 포함된 기본 이미지). 검사할 복구 지점의 일련 번호(번호를 가져오려면 Get-RecoveryPoints 명령 사용)입니다. 공백으로 구분된 여러 번호를 지정하여 명령 하나로 여러 복구 지점을 삭제할 수 있습니다.
`-time`	선택 사항. 일련 번호 대신 생성 시간을 기준으로 검사할 복구 지점을 선택합니다. 정확한 시간을 “mm/dd/yyyy hh:mm tt” 형식으로 지정합니다(예: “2/24/2012 09:00 AM”). 사용자 컴퓨터에 설정된 표준 시간대의 날짜와 시간 값을 지정해야 합니다.

예:

2개의 복구 지점에서 체크섬 검사를 시작합니다.

```
> Start-ChecksumCheck -core 10.10.10.10 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22 -rpn 5 7
```

Start-EsxiExport

`Start-EsxiExport` PowerShell 명령은 선택된 Rapid Recovery 복구 지점에서 ESX(i) 서버 가상 시스템으로 가상 내보내기 실행을 시작합니다.

필수 매개 변수에는 내보낼 복구 지점이 포함된 보호된 컴퓨터의 이름, 복구 지점을 내보내는 가상 시스템의 이름, 가상 시스템에서 할당될 RAM의 양, Linux 서버 호스트의 호스트 이름 및 포트, 결과 가상 시스템 파일이 저장될 로컬, 네트워크 또는 Linux 폴더의 경로가 포함됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-EsxiExport -core [host name] -user [user name] -password [password] -protectedserver
[machine name | IP address] -volumes [volume names] -rpn [number | numbers] | -time [time
string] -vmname [virtual machine name] -hostname [virtual host name] -hostport [virtual host
port number] -hostusername [virtual host user name] hostpassword [virtual host password] [-ram
[total megabytes] | -usesourceram] -diskprovisioning [thin | thick] -diskmapping [automatic |
manual | withvm]
```

명령 옵션

다음 표에서는 `Start-EsxiExport` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 280. Start-EsxiExport 명령 옵션

옵션	설명
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	내보낼 복구 지점이 있는 보호된 시스템.
`-volumes`	선택 사항. 내보낼 볼륨 이름의 목록. 지정되지 않은 경우 지정된 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 각 값을 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예를 들어, “C:/”가 아니라 “C:”를 지정하십시오.
`-rpn`	선택 사항. 내보낼 복구 지점의 순차적인 번호. `Get-RecoveryPoints` 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다.

옵션	설명
	노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.
-time	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. "MM/DD/YYYY hh:mm tt"(예: "04/24/2015 09:00 AM")" 형식으로 정확한 시간을 지정해야 합니다. 로컬 시스템에 설정된 시간대의 날짜 시간 값을 지정합니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
-vmname	가상 시스템의 Windows 이름.
-hostname	가상 서버 호스트 이름.
-hostport	가상 서버 포트 번호.
-hostusername	가상 서버 호스트의 사용자 이름.
-hostpassword	가상 서버 호스트 암호.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 가상 서버에 보호된 소스 시스템과 동일한 RAM 용량을 할당합니다.
-diskprovisioning	선택 사항. 가상 시스템에 할당할 디스크 공간의 양. 가상 디스크의 크기를 보호된 서버의 원본 드라이브와 동일하게 설정하려면 'thick'으로 지정하고, 원본 드라이브의 실제 사용 디스크 공간에 몇 메가바이트를 더한 용량을 할당하려면 'thin'으로 지정하십시오. 기본적으로 'thin' 프로비저닝이 선택됩니다.
-diskmapping	선택 사항. 'auto', 'manual' 또는 'withvm'을 선택합니다. 기본적으로 auto-mapping이 활성화됩니다.
-resetup	선택 사항. 지정된 위치에 이미 있는 경우 가상 시스템을 재생성합니다.
-datacenter	선택 사항. 사용할 데이터 센터를 지정합니다.
-resourcepool	선택 사항. 사용할 리소스 풀을 지정합니다.
-datastore	선택 사항. 사용할 데이터 저장소를 지정합니다.
-computeresource	선택 사항. 지정합니다는 컴퓨팅 리소스를 사용합니다.
-version	선택 사항. 사용하는 ESXi 버전을 지정합니다.

Start-HypervExport

`Start-HypervExport` PowerShell 명령은 선택된 Rapid Recovery 복구 지점에서 Hyper-V 서버 가상 시스템으로 가상 내보내기 실행을 시작합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-HypervExport -core [host name] -user [user name] -password [password] -protectedserver
[[machine name] or [IP address]] -volumes [volume names] -rpn [number | numbers] | -time [time
string] [-vmname [uselocalmachine] | -hostname [virtual host name] -hostport [virtual host port
```

```
number] -hostusername [virtual host user name] -hostpassword [virtual host password] -
vmlocation [location]] [-ram [total megabytes] | -usesourceram] -diskformat [VHD | VHDX]
```

명령 옵션

다음 표에서는 `Start-HypervExport` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 281. Start-HypervExport 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	내보낼 복구 지점이 있는 보호된 시스템.
`-volumes`	선택 사항. 내보낼 볼륨 이름의 목록. 지정되지 않은 경우 지정된 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 각 값을 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예를 들어, “C:/”가 아니라 “C:”를 지정하십시오.
`-rpn`	선택 사항. 내보낼 복구 지점의 순차적인 번호. `Get-RecoveryPoints` 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다. **노트: 이 명령에서 ‘time’ 또는 ‘rpn’ 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
`-time`	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. “MM/DD/YYYY hh:mm tt”(예: “04/24/2015 09:00 AM”)” 형식으로 정확한 시간을 지정해야 합니다. 로컬 시스템에 설정된 시간대의 날짜 시간 값을 지정합니다. **노트: 이 명령에서 ‘time’ 또는 ‘rpn’ 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
`-vmname`	가상 시스템의 Windows 이름.
`-gen2`	선택 사항. 2세대 VM을 사용합니다. 지정되지 않은 경우 1세대가 사용됩니다. Rapid Recovery는 Windows Server 2012 R2에서 Windows 8.1까지 2세대를 지원합니다.
`-usevhdx`	선택 사항. 이 옵션을 지정할 경우 Rapid Recovery는 VHDX 디스크 형식을 사용하여 VM을 생성합니다. 지정하지 않은 경우 VHD 디스크 형식을 사용합니다. 2세대는 VHDX 형식만 사용합니다.
`-uselocalmachine`	선택 사항. 로컬 Hyper-V 서버를 연결합니다. 이 매개 변수를 사용하는 경우 호스트 이름, 호스트 포트, 호스트 사용자 이름, 호스트 암호 옵션은 무시됩니다.
`-hostname`	가상 서버 호스트 이름.
`-hostport`	가상 서버 포트 번호.
`-hostusername`	가상 서버 호스트의 사용자 이름.
`-hostpassword`	가상 서버 호스트 암호.
`-vmlocation`	가상 시스템 파일을 저장하려는 폴더의 로컬 또는 네트워크 경로입니다.

옵션	설명
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 가상 서버에 보호된 소스 시스템과 동일한 RAM 용량을 할당합니다.

Start-LogTruncation

Start-LogTruncation 명령은 지정된 보호된 SQL Server 또는 Microsoft Exchange Server에 대해 로그 잘라내기를 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-LogTruncation -core [host name] -user [user name] -password [password] -protectedserver
[[machine name] or [IP address]] -target [sql | exchange]
```

명령 옵션

다음 표에서는 Start-LogTruncation 명령에 사용 가능한 옵션에 대해 설명합니다.

표 282. Start-LogTruncation 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	지정된 시스템에 대해 복구 지점을 아카이브합니다.
-target	로그 잘라내기 유형('sql' 또는 'exchange')을 지정합니다 지정되지 않은 경우 모든 데이터베이스에서 로그를 잘라냅니다.

예:

SQL 로그 잘라내기:

```
>Start-LogTruncation -protectedserver SQL1 -target sql
```

Exchange Server 로그, Core의 모든 시스템에 대한 모든 복구 지점을 잘라냅니다.

```
> start-LogTruncation -protectedserver ExServer2 -target exchange
```

Start-MountabilityCheck

`Start-MountabilityCheck` 명령은 보호된 Microsoft Exchange 메일 저장소에 대해 마운트 가능성 검사를 수행합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-MountabilityCheck -core [host name] -user [user name] -password [password] -
protectedserver [[machine name] or [IP address]] -rpn [number | numbers] |
-time [time string]
```

명령 옵션

다음 표에서는 `Start-MountabilityCheck` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 283. Start-MountabilityCheck 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-protectedserver`	지정된 시스템에 대해 복구 지점을 아카이브합니다.
`-rpn`	선택 사항. 내보낼 복구 지점의 순차적인 번호. `-GetRecoveryPoints` 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
`-time`	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. "정확한 시간을 MM/DD/YYYY hh:mm tt" 형식으로 지정해야 합니다(예: "04/24/2015 09:00 AM"). 로컬 시스템에 설정된 표준 시간대의 날짜와 시간 값을 지정합니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**

예:

Core에 있는 모든 시스템의 모든 복구 지점에 대한 마운트 가능성 검사를 시작합니다.

```
> Start-MountabilityCheck -protected EX01
```

Start-Protect

Start-Protect 명령을 사용하여 관리자가 Core의 보호 환경에 서버를 추가할 수 있습니다.

용도

```
Start-Protect -core [host name] -user [user name] -password [password] -repository [repository
name] -agent [name | IP address] -agentusername [user name]
-agentpassword [password] -agentport [port] -volumes [volume names]
```

명령 옵션

다음 표에서는 Start-Protect 명령에 사용 가능한 옵션에 대해 설명합니다.

표 284. Start-Protect 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-repository	보호된 시스템의 데이터가 저장되는 Core의 리포지토리 이름.
-agentname	보호된 시스템 이름 또는 IP 주소.
-agentusername	보호할 서버에 로그온합니다.
-agentpassword	보호할 서버에 대한 암호.
-agentport	보호된 서버 포트 번호.
-volumes	보호할 볼륨 목록. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예: "c:", "d:".

예:

서버의 볼륨을 보호 상태에 둡니다.

```
>Start-Protect -repository "Repository 1" -agentname 10.10.9.120 -agentusername administrator -
agentpassword 12345 -agentport 5002 -volumes "c:" "d:"
```

Start-ProtectCluster

Start-ProtectCluster 명령을 사용하여 관리자가 Core의 보호 환경에 서버 클러스트를 추가할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-ProtectCluster -core [host name] -user [user name] -password [password] -repository [repository name] -clustername [name | IP address] -clusterusername [user name for cluster] -clusterpassword [password for cluster] -clusterport [port] -clustervolumes [volume names] -clusternodes [cluster nodes names and volumes]
```

명령 옵션

다음 표에서는 Start-ProtectCluster 명령에 사용 가능한 옵션에 대해 설명합니다.

표 285. Start-ProtectCluster 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-repository	보호된 시스템의 데이터가 저장되는 Core의 리포지토리 이름. 이름을 큰따옴표로 묶어야 합니다.
-clustername	보호할 클러스터의 이름.
-clusterusername	보호할 클러스터의 사용자 이름.
-clusterpassword	보호할 클러스터의 암호.
-clusterport	보호할 클러스터의 포트 번호.
-clustervolumes	보호할 볼륨 목록. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예: “c:”, “d”.
-clusternodes	보호할 볼륨이 있는 클러스터 노드의 목록. 먼저 “nodename” 레이블을 지정한 다음 노드의 이름을 입력합니다. 그런 다음, “volumes” 레이블을 지정한 다음 노드에 대한 볼륨 목록을 입력합니다. 예: “nodename”, “10.10.10.10”, “volumes”, “c:”, “e:”, “nodename”, “10.10.10.11,” “volumes”, “c:”

예:

서버의 볼륨을 보호 상태에 둡니다.

```
>Start-ProtectCluster -repository "Repository 1" -clustername 10.10.9.120 -clusterusername
administrator -clusterpassword 12345 -clusterport 5002 -clustervolumes "c:" "d:" -clusternodes
nodename 10.10.10.10 volumes “c:” “e:”
```

Start- repositorycheck

`Start-RepositoryCheck` PowerShell 명령을 사용하여 리포지토리의 무결성을 검사할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-RepositoryCheck -name [repository name] | -all [check all repositories] -password
[password] -force
```

명령 옵션

다음 표에서는 `Start-RepositoryCheck` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 286. Start-RepositoryCheck 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-repository`	필수 사항. 검사하려는 리포지토리의 이름입니다.
`-all`	선택 사항. 이 Core와 관련된 모든 리포지토리를 검사합니다.
`-force`	선택 사항. 확인 없이 리포지토리 검사를 수행합니다.

예:

리포지토리 검사를 시작합니다.

```
>Start-RepositoryCheck -repository newRepository1 -core 10.10.10.10:8006 -user administrator -
password 23WE@#$sdd
```

Start-RestoreArchive

종종 회사에서는 장기 저장 장치를 사용하여 준수 및 비준수 데이터를 모두 아카이브합니다. Rapid Recovery의 보관 기능은 호환 및 비호환 데이터의 확장된 보존을 지원하는 데 사용됩니다. 관리자는 -Path 명령과 자격 증명을 지정하여 로컬 저장소 또는 네트워크 위치에 보관함을 저장할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-RestoreArchive -core [host name] -user [login] -password [password] -all | -
protectedserver [name | IP address | "[name1 | IP address1]" "[name2 | IP address2]"] -
repository [name] -archiveusername [name] -archivepassword [password] -path [location]  -
cloudaccountname [name] -cloudcontainer [name]
```

명령 옵션

Start-RestoreArchive 명령에 사용 가능한 옵션이 다음 표에 설명되어 있습니다.

표 287. Start-RestoreArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 보호된 시스템의 보관함 복구 지점.
-protectedserver	보관하려는 복구 지점이 있는 보호된 시스템. 여러 시스템 이름을 큰따옴표로 묶고 쉼표로 구분하여 지정할 수 있습니다.
-repository	복원한 복구 지점을 배치할 리포지토리 이름. 큰따옴표로 이름을 묶어야 합니다(예: "Repository1").
-archiveusername	선택 사항. 원격 시스템에 로그인하는 사용자 이름. 네트워크 경로에만 필요합니다.
-archivepassword	선택 사항. 원격 시스템에 로그인하는 암호. 네트워크 경로에만 필요합니다.
-path	보관된 데이터를 저장할 경로. 예: • 로컬 시스템: "d:\work\archive" • 네트워크 경로: "\\servername\sharename" • 클라우드 계정의 폴더: "폴더 이름"

옵션	설명
	노트: 기호 수는 로컬 및 네트워크 위치에서는 100개를 초과할 수 없으며, 클라우드 위치에서는 150개를 초과할 수 없습니다.
-cloudaccountname	선택 사항. 클라우드 보관용으로만 사용합니다. 보관함을 저장하려는 클라우드 계정 이름.
-cloudcontainer	선택 사항. 클라우드 보관용으로만 사용합니다. 선택한 클라우드 계정에서 보관함이 저장되는 클라우드 컨테이너 이름. 이 옵션을 사용하면 "-cloudaccountname" 매개 변수도 지정해야 합니다.
-manifestcore	선택 사항. 복원된 보관함 매니페스트에서 사용하려는 Core를 지정합니다.

예:

모든 시스템의 모든 복구 지점을 Core에 보관하고 로컬 시스템에 저장합니다.

```
>Start-RestoreArchive -path D:\work\archive -startdate 'Example 04/30/2012' -all
```

Start-ScheduledArchive

Start-ScheduledArchive PowerShell 명령을 사용하여 미리 지정된 일정에 관계 없이 Rapid Recovery 예약 아카이브가 주문형으로 시작되도록 할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

명령 옵션

다음 표에서는 Start-ScheduledArchive 명령에 사용 가능한 옵션에 대해 설명합니다.

표 288. Start-ScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	예약된 모든 아카이브를 강제로 수행합니다.

옵션	설명
-id	식별 번호 또는 강제로 수행하고자 하는 공백으로 구분된 예약 아카이브 식별자입니다.

예:

여러 예약 아카이브 작업 시작:

```
>Start-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Start-VBExport

start-VBExport 명령은 선택한 복구 지점에서 Oracle VirtualBox 서버 가상 시스템으로 가상 내보내기 실행을 시작합니다.

필수 매개 변수에는 내보낼 복구 지점이 포함된 보호된 컴퓨터의 이름, 복구 지점을 내보내는 가상 시스템의 이름, 가상 시스템에서 할당될 RAM의 양, Linux 서버 호스트의 호스트 이름 및 포트, 결과 가상 시스템 파일이 저장될 로컬, 네트워크 또는 Linux 폴더의 경로가 포함됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-VBExport -core -user [user name] -password [password] -protectedserver [machine name] or
[IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostname [linux hostname] -hostport [linux port] -targetpath [location]
pathusername [user name] - pathpassword [password]
```

명령 옵션

다음 표에서는 Start-VBExport 명령에 사용 가능한 옵션에 대해 설명합니다.

표 289. Start-VBExport 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	내보낼 복구 지점이 있는 보호된 시스템.
-volumes	선택 사항. 내보낼 볼륨 이름의 목록. 지정되지 않은 경우 지정된 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 각 값을 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예를 들어, “C:/”가 아니라 “C:”를 지정하십시오.

옵션	설명
-rpn	선택 사항. 내보낼 복구 지점의 순차적인 번호. Get-RecoveryPoints 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
-time	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. "MM/DD/YYYY hh:mm tt"(예: "04/24/2015 09:00 AM")" 형식으로 정확한 시간을 지정해야 합니다. 로컬 시스템에 설정된 시간대의 날짜 시간 값을 지정합니다. **노트: 이 명령에서 'time' 또는 'rpn' 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
-vmname	가상 시스템의 Windows 이름.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 가상 서버에 보호된 소스 시스템과 동일한 RAM 용량을 할당합니다.
-linuxhostname	Linux VirtualBox 서버 호스트 이름.
-hostport	Linux VirtualBox 서버 포트.
-targetpath	가상 시스템 파일이 저장될 폴더의 로컬, 네트워크 또는 Linux 경로.
-pathusername	네트워크 시스템의 사용자 이름. -targetpath 매개 변수에서 네트워크 경로를 지정할 경우에만 필요합니다.
-pathpassword	네트워크 시스템 암호. -targetpath 매개 변수에서 네트워크 경로를 지정할 경우에만 필요합니다.
-accountusername	선택 사항. 내보낸 가상 시스템을 등록하기 위해 사용자 계정을 지정할 수 있는 경우 이 옵션을 사용합니다. 로컬 또는 네트워크 시스템에만 해당됩니다.
-accountpassword	선택 사항. -accountusername. 매개 변수를 사용하여 내보낸 가상 시스템을 등록하기 위해 사용자 계정을 지정하는 경우에만 이 옵션을 사용합니다(로컬 또는 네트워크 시스템만 해당).

예:

모든 볼륨을 10.10.12.97 시스템의 최신 복구 지점에서 NewVirtualBoxVM이라는 VM으로 내보냅니다.

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVirtualBoxVM -ram usesourceram -
targetpath D:/exports
```

Start- virtualstandby

Start-VirtualStandby PowerShell 명령을 사용하여 Rapid Recovery에서 가상 대기 시스템으로 데이터 내보내기를 실행할 수 있습니다. 이 주문형 내보내기는 정기적으로 예약된 가상 대기 내보내기 작업 외에 수행이 가능합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

명령 옵션

다음 표에서는 Start-VirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 290. Start-VirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 가상 대기 시스템에 대해 내보내기를 수행합니다.
-protectedserver	내보내려는 보호된 시스템의 이름(쉼표 및 공백으로 구분)입니다.

예:

보호된 시스템에 대해 가상 대기 내보내기를 수행합니다.

```
>Start-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Start-VMExport

Start-VMExport 명령은 선택된 복구 지점에서 VMware Workstation 서버 가상 시스템으로 가상 내보내기 실행을 시작합니다.

필요한 매개 변수에는 내보낼 복구 지점이 포함된 보호된 컴퓨터의 이름, 복구 지점을 내보내는 가상 시스템의 이름, 가상 시스템에서 할당될 RAM의 양, 결과 가상 시스템 파일이 저장될 로컬 또는 네트워크 폴더의 경로가 포함됩니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Start-VMExport -core -user [user name] -password [password] -protectedserver [machine name] or
[IP address]] -volumes [volume names] -rpn [number | numbers] |
-time [time string] -vmname [virtual machine name] [-ram [total megabytes] |
-usesourceram] -linuxhostnme [linux hostname] -hostport [linux port] -targetpath [location]
pathusername [user name] - pathpassword [password]
```

명령 옵션

다음 표에서는 Start-VMExport 명령에 사용 가능한 옵션에 대해 설명합니다.

표 291. Start-VMExport 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	내보낼 복구 지점이 있는 보호된 시스템.
-volumes	선택 사항. 내보낼 볼륨 이름의 목록. 지정되지 않은 경우 지정된 복구 지점의 모든 볼륨을 내보냅니다. 값을 큰따옴표로 묶고 공백으로 구분해야 합니다. 볼륨 이름 뒤에 슬래시를 사용하지 마십시오. 예를 들어, “C:/”가 아니라 “C:”를 지정하십시오.
-rpn	선택 사항. 내보낼 복구 지점의 순차적인 번호. Get-RecoveryPoints 명령을 사용하여 복구 지점 번호를 가져올 수 있습니다. **노트: 이 명령에서 ‘time’ 또는 ‘rpn’ 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
-time	선택 사항. 내보내기 위해 선택할 복구 지점을 결정합니다. "MM/DD/YYYY hh:mm tt"(예: "04/24/2015 09:00 AM")" 형식으로 정확한 시간을 지정해야 합니다. 로컬 시스템에 설정된 시간대의 날짜 시간 값을 지정합니다. **노트: 이 명령에서 ‘time’ 또는 ‘rpn’ 옵션을 지정하지 않은 경우 가장 최근의 복구 지점을 내보냅니다.**
-vmname	가상 시스템의 Windows 이름.
-ram	특정 용량의 RAM을 가상 서버에 할당합니다.
-usesourceram	선택 사항. 가상 서버에 보호된 소스 시스템과 동일한 RAM 용량을 할당합니다.
-targetpath	가상 시스템 파일이 저장될 폴더의 로컬, 네트워크 또는 Linux 경로.
-pathusername	네트워크 시스템의 사용자 이름. -targetpath 매개 변수에서 네트워크 경로를 지정할 경우에만 필요합니다.
-pathpassword	네트워크 시스템 암호. -targetpath 매개 변수에서 네트워크 경로를 지정할 경우에만 필요합니다.
-version	사용할 VMware Tools 버전. 유효한 버전은 7, 8, 9 및 10입니다.

예:

모든 볼륨을 10.10.12.97 시스템의 최신 복구 지점에서 NewVMwareVM이라는 VM으로 내보냅니다.

```
>Start-VBExport -protectedserver 10.10.12.97 -vmname NewVMWareVM -ram usesourceram -targetpath
D:/exports
```

Stop-ActiveJobs

Stop-ActiveJobs는 지정된 보호된 시스템에 대한 활성 작업을 취소합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Stop-ActiveJobs [-protectedserver [machine name | IP address] | -core [host name]] -user [user name] -password [password] -jobtype [jobtype]
```

명령 옵션

다음 표에서는 Stop-ActiveJobs 명령에 사용 가능한 옵션에 대해 설명합니다.

표 292. Stop-ActiveJobs 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	모든 보호된 시스템에 대해 지정된 유형의 이벤트를 선택 및 취소합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	작업을 취소해야 하는 보호된 시스템을 확인합니다.
-jobtype	선택 사항. 작업 유형 필터를 지정합니다. 사용 가능한 값은 다음과 같습니다. 'transfer'(데이터 전송), 'repository'(리포지토리 유지 관리), 'replication'(로컬 및 원격 복제), 'backup'(백업 및 복원), 'bootcdbuilder'(부트 CD 만들기), 'diagnostics'(로그 업로드), 'exchange'(Exchange Server 파일 검사), 'export'(복구 지점 내보내기), 'pushinstall'(보호된 시스템에 Agent 소프트웨어 배포), 'rollback'(복구 지점에서 데이터 복원), 'rollup'(복구 지점 롤업), 'sqlattach'(에이전트 연결성 검사), 'mount'(리포지토리 아님). 기본적으로 지정된 유형의 모든 작업이 취소됩니다.

예:

보호된 시스템에서 전송 작업을 중지합니다.

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -jobtype transfer
```

특정 보호된 시스템에 대해 모든 작업을 중지합니다.

```
>Stop-ActiveJobs -protectedserver 10.10.1.76 -all
```

Suspend-Replication

Suspend-Replication 명령을 사용하여 관리자가 복제를 일시 중지할 수 있습니다.

사용자는 다음 세 가지 방법으로 복제를 일시 중지할 수 있습니다.

- 모든 보호된 시스템의 마스터 Core에서 복제 일시 중지(-outgoing parameter)
  관리자가 마스터 Core에서 발신 복제를 일시 중지하려면 원격 시스템 이름을 발신 복제 연결과 함께 지정해야 합니다.

  ```
  >Suspend-replication -outgoing 10.10.12.10
  ```
- 단일 보호된 시스템의 마스터 Core에서 복제 일시 중지(-protectedserver 매개 변수)

  ```
  >Suspend-replication -protectedserver 10.10.12.97
  ```
- 대상 Core에서 복제 일시 중지(-incoming parameter)
  로컬 Core가 대상 Core일 경우 관리자는 수신 매개 변수를 사용하여 마스터 Core를 지정함으로써 복제를 일시 중지할 수 있습니다.

명령 옵션

다음 표에서는 Suspend-Replication 명령에 사용 가능한 옵션에 대해 설명합니다.

표 293. Suspend-Replication 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	선택된 Core의 모든 보호된 시스템을 일시 중지합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-pause	[snapshots],[replication] 또는[vmexport].
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-protectedserver	현재 보호된 서버를 일시 중지합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-incoming	Core 시스템에 복제하는 원격 Core의 호스트 이름. 원격 Core의 모든 보호된 시스템에 대해 복제가 일시 중지됩니다.
-outgoing	데이터가 복제되는 원격 대상 Core의 호스트 이름. 원격 Core의 모든 보호된 시스템에 대해 복제가 일시 중지됩니다.

예:

단일 보호된 시스템(IP 주소 10.10.1.76)에 대해 원격 Core(IP 주소 10.10.1.15)에서 보내는 복제를 일시 중지합니다.

```
>Suspend-replication -core 10.10.1.15 -protectedserver 10.10.1.76
```

모든 보호된 시스템에 대해 로컬 Core에서 원격 대상(IP 주소 10.10.1.63)으로 보내는 복제를 일시 중지합니다.

```
>Suspend-replication -outgoing 10.10.1.63
```

원격 Core(IP 주소 10.10.1.15)에서 10.10.1.82로부터 들어오는 복제를 일시 중지합니다(관리자는 전체 시스템에서만 들어오는 복제를 일시 중지할 수 있음).

```
>Suspend-replication -core 10.10.1.15 -incoming 10.10.1.82
```

Suspend- repositoryactivity

`Suspend-RepositoryActivity` PowerShell 명령을 사용하여 Rapid Recovery 리포지토리의 활동을 일시 중지할 수 있습니다. 일시 중단된 활동은 데이터 입력이나 누락을 막기 위해 리포지토리에 잠금 상태로 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Suspend-RepositoryActivity -core [host name] -user [login] -password [password] -all | -
repository ["name" | "name1 " "name2"]
```

명령 옵션

다음 표에서는 `Suspend-RepositoryActivity` 명령에 사용 가능한 옵션에 대해 설명합니다.

표 294. Suspend-RepositoryActivity 명령 옵션

옵션	설명
`-?`	이 도움말 메시지를 표시합니다.
`-core`	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
`-password`	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-user`	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
`-all`	이 Core와 연관된 모든 리포지토리의 활동을 일시 중단합니다.
`-repository`	잠그려는 리포지토리의 이름. 이름을 큰따옴표로 묶어야 합니다. 여러 개의 리포지토리(공백으로 구분)를 지정할 수 있습니다.

예:

다수의 리포지토리에 대한 활동을 일시 중단합니다.

```
>Suspend-RepositoryActivity -repository "repository1" "repository2"
```

모든 리포지토리의 활동을 일시 중단합니다.

```
>Suspend-RepositoryActivity -all
```

Suspend-ScheduledArchive

Suspend-ScheduledArchive PowerShell 명령을 사용하면 Rapid Recovery 예약 아카이브를 일시 중지할 수 있습니다. 이 명령은 다시 활성화할 때까지 예약된 대로 아카이브가 진행되는 것을 방지합니다..

용도

이 명령의 사용법은 다음과 같습니다.

```
Suspend-ScheduledArchive -core [host name] -user [login] -password [password] -all -ids [id | id1 id2]
```

명령 옵션

다음 표에서는 Suspend-ScheduledArchive 명령에 사용 가능한 옵션에 대해 설명합니다.

표 295. Suspend-ScheduledArchive 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	예약된 모든 아카이브를 일시 중지합니다.
-id	식별 번호를 또는 공백으로 구분된 예약 아카이브 번호를 일시 중지합니다.

예:

여러 개의 예약된 아카이브를 일시 중지합니다.

```
>Suspend-ScheduledArchive -ids 799138c8-3dfc-4398-9711-1823733c2a31, 26c29bb7-b320-47f5-b5a8-dffc49f50e25
```

Suspend-Snapshot

Suspend-Snapshot 명령을 사용하여 관리자가 스냅숏을 일시 중지할 수 있습니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Suspend-Snapshot -core [host name] -user [user name] -password [password] -all |
-protectedserver [name | IP address] -time [time string]
```

명령 옵션

다음 표에서는 Suspend-Snapshot 명령에 사용 가능한 옵션에 대해 설명합니다.

표 296. Suspend-Snapshot 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-all	선택된 Core의 모든 보호된 시스템을 일시 중지합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-time	스냅숏이 다시 시작되는 때를 나타내는 'Day-Hours-Minutes' 형식의 시간(스냅숏 일시 중지에만 해당).

예:

로컬 Core의 IP가 10.10.10.4이고 일정 시간 동안 다시 시작하는 보호된 컴퓨터의 스냅숏을 일시 중지합니다.

```
>Suspend-Snapshot -protectedserver 10.10.10.4 -time 3-20-50
```

Suspend- virtualstandby

Suspend-VirtualStandby PowerShell 명령은 Rapid Recovery 가상 대기 시스템에 대한 데이터 내보내기를 일시 중지합니다.

용도

이 명령의 사용법은 다음과 같습니다.

```
Suspend-VirtualStandby -core [host name] -user [login] -password [password] -all | -
protectedserver [name(s) | IP address]
```

명령 옵션

다음 표에서는 Suspend-VirtualStandby 명령에 사용 가능한 옵션에 대해 설명합니다.

표 297. Suspend-VirtualStandby 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 로그온 ID도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	모든 가상 대기 시스템에 대한 내보내기를 일시 중지합니다.
-protectedserver	일시 중단할 가상 대기 시스템이 실행되는 보호된 시스템의 이름(쉼표 및 공백으로 구분)입니다.

예:

보호된 시스템에 대한 가상 대기 내보내기를 일시 중단합니다.

```
>Suspend-VirtualStandby -core 10.10.10.10:8006 -user administrator -password 23WE@#$sdd -
protectedserver 10.10.5.22
```

Suspend-VMExport

Suspend-VMExport 명령을 사용하여 관리자가 가상 시스템으로 내보내기를 일시 중지할 수 있습니다.

용도

```
Suspend-VMExport -core [host name] -user [user name] -password [password] -all | -
protectedserver [name | IP address]
```

명령 옵션

다음 표에서는 Suspend-VMExport 명령에 사용 가능한 옵션에 대해 설명합니다.

표 298. Suspend-VMExport 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-all	선택된 Core의 모든 보호된 시스템을 일시 중지합니다.
-protectedserver	현재 보호된 서버를 일시 중지합니다.

예:

로컬 Core의 IP가 10.10.10.4인 보호된 시스템의 VM 내보내기를 일시 중지합니다.

```
>Suspend-VMExport -protectedserver 10.10.12.25
```

Update-Repository

Update-Repository 명령은 기존 DVM 리포지토리에 범위를 추가합니다. 250MB와 16TB 사이의 크기를 지정해야 합니다.

용도

```
Update-Repository -name [repository name] -size [size] [[[-datapath [datapath]
-metadatapath [metadata path]] | [-uncpath [UNC path] -shareusername [share user name] -
sharepassword [share password]]] -core [host name] -user [user name]
-password [password]
```

명령 옵션

다음 표에서는 Update-Repository 명령에 사용 가능한 옵션에 대해 설명합니다.

표 299. Update-Repository 명령 옵션

옵션	설명
-?	이 도움말 메시지를 표시합니다.
-core	선택 사항. 원격 Core 호스트 시스템 IP 주소(선택적 포트 번호 포함). 기본적으로 로컬 시스템에 설치된 Core에 연결합니다.
-user	선택 사항. 원격 Core 호스트 시스템의 사용자 이름. 사용자 이름을 지정하면 암호도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-password	선택 사항. 원격 Core 호스트 시스템 암호. 암호를 지정하면 사용자 이름도 입력해야 합니다. 로그온 ID를 입력하지 않으면 로그온한 사용자의 자격 증명이 사용됩니다.
-name	DVM 리포지토리 이름입니다.
-size	DVM 리포지토리 범위의 크기입니다. 사용 가능한 단위는 b, Kb, MB, GB, TB, PB입니다.
-datapath	로컬 위치에만 해당. DVM 리포지토리 범위의 데이터 경로를 결정합니다.
-metadatapath	로컬 위치에만 해당. DVM 리포지토리 범위의 메타데이터 경로를 결정합니다.
-uncpath	공유 위치에만 해당. DVM 리포지토리 범위의 데이터 및 메타데이터 경로를 결정합니다.
-shareusername	공유 위치에만 해당. 공유 위치 로그인 ID를 결정합니다.
-sharepassword	공유 위치에만 해당. 공유 위치 암호를 결정합니다.

예:

최소 크기의 DVM 리포지토리에 범위를 추가합니다.

```
>Update-Repository -name Repository1 -size 250Mb -datapath C:\Repository\Data -metadatapath C:
\repository\Metadata
```

현지화

Rapid Recovery Core가 설치된 같은 시스템에서 실행할 경우 Rapid Recovery PowerShell 모듈에서는 Core용으로 설정된 언어를 표시 언어로 사용합니다. 영어, 중국어(간체), 프랑스어, 한국어, 독일어, 일본어, 포르투갈어(브라질), 스페인어와 같은 언어를 지원하는 현지화된 Rapid Recovery 버전입니다.

Rapid Recovery PowerShell Module이 별도의 시스템에 설치된 경우에는 영어만 지원됩니다.

한정자

다음 표에서는 Rapid Recovery PowerShell Module에 대해 사용 가능한 한정자를 설명합니다.

표 300. Rapid Recovery PowerShell Module 한정자

한정자	용도
-core <Rapid Recovery Core Name>	Core의 호스트 이름.

한정자	용도
	기본값: Localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent의 호스트 이름/IP 주소. 기본값: 보호되는 서버가 여러 대일 경우 Localhost, 그렇지 않으면 하나가 보호됩니다.
-Mode <READ, READWRITE, WRITE>	복구 지점 마운트 모드. 기본값: Read.
-Volumes <Snapshot Volume Letter>	Rapid Recovery Agent의 스냅숏 볼륨 문자. 기본값: All.
-User <User Name>	Rapid Recovery Core에 연결하는 데 사용된 사용자 이름. 일반적으로 서비스 사용자입니다.
-Domain <Domain Name>	/User에서 정의한 사용자의 도메인.
-Password <Password>	/User에서 정의한 사용자의 암호.
-Path <Target path to mount, dismount recovery points or archive location>	예: C:\RapidRecoveryMount.

C

스크립트 작성을 사용하여 Rapid Recovery 작업 확장

관리자는 Rapid Recovery를 사용하여 경우에 따라 명령과 스크립트 실행을 통해 리소스 관리를 자동화할 수 있습니다. Rapid Recovery 소프트웨어는 Windows용 PowerShell scripting 및 Linux용 Bourne Shell 스크립트 작성을 지원합니다.

Rapid Recovery Core에서 복제, 가상 내보내기 또는 백업 스냅숏과 같은 작업을 시작할 때마다 Core 작업이 자동으로 작성됩니다. 이러한 작업 전 또는 후에 스크립트를 실행하여 작업을 확장할 수 있습니다. 이들은 사전 스크립트와 사후 스크립트로 알려져 있습니다.

이 섹션에서는 Windows 및 Linux용 Rapid Recovery에서 관리자가 지정된 경우 사용할 수 있는 스크립트에 대해 설명합니다.

주의: 이 문서에 제공된 샘플 PowerShell 및 Bourne 스크립트는 자격을 갖춘 관리자가 설계한 대로 실행할 때 작동합니다. 사용 중인 버전을 유지하기 위해 작동 중인 스크립트를 수정할 때는 주의를 기울이십시오. 여기에 포함된 스크립트 샘플 또는 사용자가 수정한 스크립트는 사용자 지정 사항으로 간주되어, 일반적으로 Dell 고객 지원 부서에서 다루지 않습니다.

주제:

- Rapid Recovery에서 PowerShell 스크립트 사용
- PowerShell 스크립트 작성을 위한 입력 매개 변수
- 샘플 PowerShell 스크립트
- Rapid Recovery에서 Bourne Shell 스크립팅 사용
- Bourne Shell 스크립트 작성을 위한 입력 매개 변수
- 샘플 Bourne Shell 스크립트

Rapid Recovery에서 PowerShell 스크립트 사용

Windows PowerShell은 관리 자동화를 위해 설계된 Microsoft .NET Framework 연결 환경입니다. Rapid Recovery에는 지정된 발생 빈도(예: 스냅숏, 연결 기능 및 탑재 기능 검사 등 전후)에서 관리 사용자가 사용자 제공 PowerShell 스크립트를 실행할 수 있는 포괄적인 PowerShell 스크립트 작성용 클라이언트 소프트웨어 개발 키트(SDK)가 포함되어 있습니다. 관리자는 Rapid Recovery Core와 보호된 시스템에서 모두 스크립트를 실행할 수 있습니다. 스크립트에는 매개 변수를 입력할 수 있으며 스크립트 출력은 Core 및 보호된 시스템 로그 파일에 기록됩니다.

노트: 야간 작업의 경우 야간 작업을 구별하려면 스크립트 파일 한 개와 JobType 입력 매개 변수를 유지하십시오.

스크립트 파일은 **%ALLUSERSPROFILE%\AppRecovery\Scripts** 폴더에 있습니다.

- Windows 7에서 %ALLUSERSPROFILE% 폴더를 찾는 경로는 **C:\ProgramData**입니다.
- Windows 2003의 경우 폴더가 있는 경로는 **Documents and Settings\All Users\Application Data**입니다.

노트: Windows PowerShell은 필수이며 Rapid Recovery 스크립트를 실행하기 전에 설치 및 구성해야 합니다.

PowerShell 스크립트 사용 방법에 대한 자세한 내용은 샘플 PowerShell 스크립트, PowerShell 스크립트 작성을 위한 입력 매개 변수, Bourne Shell 스크립트 작성을 위한 입력 매개 변수 및 샘플 Bourne Shell 스크립트을(를) 참조하십시오.

PowerShell 스크립트 작성을 위한 전제 조건

Rapid Recovery의 PowerShell 스크립트를 실행하려면 Windows PowerShell 2.0 이상이 설치되어 있어야 합니다. PowerShell 3.0에는 더 쉬운 객체 속성 액세스, PowerShell Web 액세스, REST 호출 지원 등 새로운 기능이 포함되어 있으므로 PowerShell 3.0 이상을 사용하는 것이 좋습니다.

노트: PowerShell 홈 디렉터리에 powershell.exe.config 파일을 배치하십시오. 예를 들면, C:\WindowsPowerShell\powershell.exe.config입니다.

powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
    <startup useLegacyV2RuntimeActivationPolicy="true">
        <supportedRuntime version="v4.0.30319"/>
        <supportedRuntime version="v2.0.50727"/>
    </startup>
</configuration>
```

PowerShell 스크립트 테스트

실행할 스크립트를 테스트하려면 PowerShell 그래픽 편집기 powershell_is를 사용하면 됩니다. 또한 구성 파일 powershell_ise.exe.config를 구성 파일 powershell.exe.config와 같은 폴더에 추가해야 합니다.

노트: powershell_ise.exe.config 구성 파일의 내용은 powershell.exe.config 파일의 내용과 같아야 합니다.

주의: 사전 PowerShell 또는 사후 PowerShell 스크립트가 실패하면 작업도 실패합니다.

현지화

Rapid Recovery Core가 설치된 같은 시스템에서 실행할 경우 Rapid Recovery PowerShell 모듈에서는 Core용으로 설정된 언어를 표시 언어로 사용합니다. 이와 같이 지역화된 Rapid Recovery 버전에서는 영어, 중국어(간체), 프랑스어, 한국어, 독일어, 일본어, 포르투갈어(브라질), 스페인어가 지원됩니다.

Rapid Recovery PowerShell 모듈이 별도의 시스템에 설치되어 있으면 영어가 유일한 지원되는 언어입니다.

한정자

다음 표에서는 Rapid Recovery PowerShell Module에 대해 사용 가능한 한정자를 설명합니다.

표 301. Rapid Recovery PowerShell Module 한정자

한정자	용도
`-core <Rapid Recovery Core Name>`	Core의 호스트 이름.

한정자	용도
	기본값: Localhost
-ProtectedServer <Protected Server Name>	Rapid Recovery Agent의 호스트 이름/IP 주소. 기본값: 보호되는 서버가 여러 대일 경우 Localhost, 그렇지 않으면 하나가 보호됩니다.
-Mode <READ, READWRITE, WRITE>	복구 지점 마운트 모드. 기본값: Read.
-Volumes <Snapshot Volume Letter>	Rapid Recovery Agent의 스냅숏 볼륨 문자. 기본값: All.
-User <User Name>	Rapid Recovery Core에 연결하는 데 사용된 사용자 이름. 일반적으로 서비스 사용자입니다.
-Domain <Domain Name>	/User에서 정의한 사용자의 도메인.
-Password <Password>	/User에서 정의한 사용자의 암호.
-Path <Target path to mount, dismount recovery points or archive location>	예: C:\RapidRecoveryMount.

PowerShell 스크립트 작성을 위한 입력 매개 변수

사용 가능한 모든 입력 매개 변수가 샘플 스크립트에 사용되었습니다. 매개 변수는 다음 표에 설명되어 있습니다.

노트: 스크립트 파일의 이름은 샘플 스크립트 파일 이름과 같아야 합니다.

AgentProtectionStorageConfiguration(Replay.Common.Contracts.Agents 네임스페이스)

다음 표에는 AgentProtectionStorageConfiguration 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 302. AgentProtectionStorageConfiguration 매개 변수에 대한 객체

메서드	설명
public Guid RepositoryId { get; set; }	에이전트 복구 지점이 저장된 리포지토리의 ID를 가져오거나 설정합니다.
public string EncryptionKeyId { get; set; }	이 에이전트의 복구 지점에 대한 암호화 키의 ID를 가져오거나 설정합니다. 빈 문자열은 암호화하지 않음을 의미합니다.

AgentTransferConfiguration(Replay.Common.Contracts.Transfer 네임스페이스)

다음 표에는 AgentTransferConfiguration 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 303. AgentTransferConfiguration 매개 변수에 대한 객체

메서드	설명
public uint MaxConcurrentStreams { get; set; }	Core가 데이터를 전송하기 위해 에이전트에 대해 설정하는 동시 TCP 연결의 최대 수를 가져오거나 설정합니다.
public uint MaxTransferQueueDepth { get; set; }	쓰기를 위해 대기할 수 있는 블록 범위의 최대 수를 가져오거나 설정합니다. 전송 스트림에서 한 범위의 블록을 읽을 때 해당 범위는 생산자 또는 소비자 대기열에 배치되며, 이 대기열에서 소비자 스레드가 범위를 읽고 epoch 객체에 씁니다. 리포지토리가 쓰는 속도가 네트워크가 읽은 속도보다 느리면 이 대기열이 가득차게 됩니다. 대기열이 가득차고 읽기가 중단되는 시점이 최대 전송 대기열 깊이입니다.
public uint MaxConcurrentWrites { get; set; }	지정된 시간에 한 epoch의 해결되지 않은 블록 쓰기 작업의 최대 수를 가져오거나 설정합니다. 이 매개 변수에 지정된 최대 개수의 쓰기 작업을 수행한 이후에 추가 블록이 수신되는 경우 이 추가 블록은 해결되지 않은 쓰기 중 하나가 완료될 때까지 무시됩니다.
public ulong MaxSegmentSize { get; set; }	단일 요청으로 전송될 인접 블록의 최대 수를 가져오거나 설정합니다. 테스트를 통해 더 높거나 더 낮은 최적 값을 찾을 수 있습니다.
public Priority Priority { get; set; }	전송 요청의 우선 순위를 가져오거나 설정합니다.
public uint GetChangedBlocksRetries { get; set; }	에이전트에서 변경된 블록의 초기 검색에 실패한 경우 재시도 횟수를 가져오거나 설정합니다.
public int MaxRetries { get; set; }	실패한 전송이 실패한 것으로 간주되기 전에 재시도해야 하는 최대 횟수를 가져오거나 설정합니다.
public bool UseDefaultMaxRetries { get; set; }	포함된 경우 전송 구성에 지정된 기본 최대 재시도 횟수를 사용합니다.
public Guid ProviderId{ get; set; }	이 호스트에서 스냅숏에 사용하는 VSS 공급자의 GUID를 가져오거나 설정합니다. 관리자들은 일반적으로 기본값을 사용합니다.
public Collection<ExcludedWriter> ExcludedWriterIds { get; set; }	이 스냅숏에서 제외해야 하는 VSS 작성기 ID 컬렉션을 가져오거나 설정합니다. 작성기 ID는 작성기 이름으로 지정됩니다. 이 이름은 문서 작성용으로만 제공되며, 작성기 이름과 정확히 일치하지 않아도 됩니다.
public ushort TransferDataServerPort { get; set; }	보호된 시스템에서 Core로의 실제 데이터 전송을 위해 Core에서 연결을 수락하는 TCP 포트가 포함된 값을 가져오거나 설정합니다. 에이전트는 이 포트를 수신하려고 시도하지만, 포트가 사용 중인 경우 보호된 시스템은 다른 포트를 대신 사용할 수 있습니다. Core는 스냅된 각 볼륨에 대해 VolumeSnapshotInfo 객체의 BlockHashesUri 및 BlockDataUri 속성에 지정된 포트 번호를 사용해야 합니다.
public TimeSpan CleanSnapshotTimeout { get; set; }	전송을 마치고 스냅숏을 정리하기 전에 기다리는 시간을 가져오거나 지정합니다.
public TimeSpan SnapshotTimeout { get; set; }	중단 및 시간 초과 전에 VSS 스냅숏 작업이 완료되기까지 대기해야 하는 시간을 가져오거나 설정합니다.
public TimeSpan TransferTimeout { get; set; }	스냅숏을 중단하기 전에 Core로부터 추가 연결을 대기해야 하는 시간을 가져오거나 설정합니다.
public TimeSpan NetworkReadTimeout { get; set; }	이 전송과 관련된 네트워크 읽기 작업의 시간 초과를 가져오거나 설정합니다.
public TimeSpan NetworkWriteTimeout { get; set; }	이 전송과 관련된 네트워크 쓰기 작업의 시간 초과를 가져오거나 설정합니다.
public uint InitialQueueSize { get; set; }	초기 대기열 또는 요청의 크기를 가져오거나 설정합니다.

메서드	설명
public uint MinVolumeFreeSpacePercents { get; set; }	볼륨에서 사용 가능한 최소 여유 공간(퍼센트)을 가져오거나 설정합니다. 여유 공간이 이 매개 변수에 지정된 크기보다 작으면 모든 변경 로그를 삭제하고 기본 이미지를 적용합니다.
public uint MaxChangeLogsSizePercents { get; set; }	볼륨 용량의 일부로 측정되는 드라이버 변경 로그의 최대 크기(퍼센트)를 가져오거나 설정합니다. 변경 로그 일부가 이 값보다 크면 모든 변경 로그를 삭제하고 기본 이미지를 적용합니다.
public bool EnableVerification { get; set; }	Core로 전송되는 각 블록의 진단 확인을 수행해야 하는지 여부를 나타내는 값을 가져오거나 설정합니다.

BackgroundJobRequest(Replay.Core.Contracts.BackgroundJobs 네임스페이스)

다음 표에는 BackgroundJobRequest 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 304. BackgroundJobRequest 매개 변수에 대한 객체

메서드	설명
public AgentIdsCollection AgentIds { get; set; }	보호된 시스템의 ID를 가져오거나 설정합니다.
public bool IsNightlyJob { get; set; }	백그라운드 작업이 야간 작업인지 여부를 나타내는 값을 가져오거나 설정합니다.
public Guid NightlyJobTransactionId { get; set; }	야간 작업 트랜잭션의 ID를 가져오거나 설정합니다.
public Guid JobId { get; set; }	백그라운드 작업의 ID를 가져오거나 설정합니다.
public bool Force { get; set; }	작업을 강제 적용하는지 여부를 나타내는 값을 가져오거나 설정합니다.
public uint JobStartsCount { get; set; }	작업을 시작하는 횟수를 가져오거나 설정합니다.
public virtual bool InvolvesAgentId(Guid agentId)	특정 에이전트가 작업에 포함되어 있는지 여부를 나타내는 값을 지정합니다.

ChecksumCheckJobRequest(Replay.Core.Contracts.Exchange.ChecksumChecks 네임스페이스)

DatabaseCheckJobRequestBase 매개 변수에서 값을 상속합니다.

DatabaseCheckJobRequestBase(Replay.Core.Contracts.Exchange 네임스페이스)

BackgroundJobRequest 매개 변수에서 값을 상속합니다.

표 305. DatabaseCheckJobRequestBase 매개 변수에 대한 객체

메서드	설명
public string RecoveryPointId { get; set; }	데이터베이스가 선택된 복구 지점의 ID를 가져오거나 설정합니다.

ExportJobRequest(Replay.Core.Contracts.Export 네임스페이스)

BackgroundJobRequest 매개 변수에서 값을 상속합니다.

다음 표에는 ExportJobRequest 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 306. ExportJobRequest 매개 변수에 대한 객체

메서드	설명
public uint RamInMegabytes { get; set; }	내보낸 VM에 대한 메모리 크기를 가져오거나 설정합니다. 원본 시스템의 메모리 크기를 사용하려면 0으로 설정하십시오.
public ushort CpuCount { get; set; }	내보낸 VM에 대한 CPU 수를 가져오거나 설정합니다. 원본 시스템의 CPU 수를 사용하려면 0으로 설정합니다.
public ushort CoresPerCpu { get; set; }	내보낸 VM에 대한 CPU마다 Cores를 가져오거나 설정합니다. 원본 시스템의 CPU마다 Cores를 사용하려면 0으로 설정합니다.
public VirtualMachineLocation Location { get; set; }	이 내보내기의 대상 위치를 가져오거나 설정합니다. 이는 추상 기본 클래스입니다.
public VolumeImageIdsCollection VolumeImageIds { get; private set; }	VM 내보내기에 포함할 볼륨 이미지를 가져오거나 설정합니다.
public ExportJobPriority Priority { get; set; }	내보내기 요청의 우선 순위를 가져오거나 설정합니다.

NightlyAttachabilityJobRequest(Replay.Core.Contracts.Sql 네임스페이스)

BackgroundJobRequest 매개 변수에서 값을 상속합니다.

표 307. NightlyAttachabilityJobRequest 매개 변수에 대한 객체

메서드	설명
public int SimultaneousJobsCount { get; set; }	동시에 실행할 수 있는 작업 개수를 가져오거나 설정합니다.

RollupJobRequest(Replay.Core.Contracts.Rollup 네임스페이스)

BackgroundJobRequest 매개 변수에서 값을 상속합니다.

TakeSnapshotResponse(Replay.Agent.Contracts.Transfer 네임스페이스)

다음 표에는 TakeSnapshotResponse 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 308. TakeSnapshotResponse 매개 변수에 대한 객체

메서드	설명
public Guid SnapshotSetId { get; set; }	VSS에 의해 이 스냅숏에 할당된 GUID를 가져오거나 설정합니다.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	스냅에 포함된 각 볼륨에 대한 스냅숏 모음을 가져오거나 설정합니다.

TransferJobRequest(Replay.Core.Contracts.Transfer 네임스페이스)

BackgroundJobRequest 매개 변수에서 값을 상속합니다.

다음 표에는 TransferJobRequest 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 309. TransferJobRequest 매개 변수에 대한 객체

메서드	설명
public VolumeNameCollection VolumeNames { get; set; }	전송에 대한 이름 모음을 가져오거나 설정합니다. VolumeNames는 다음 데이터가 포함된 데이터 구조입니다. · GuidName. DisplayName가 설정되지 않은 경우 이름으로 사용되고 볼륨과 연관된 GUID. · DisplayName. 볼륨의 표시 이름.
public VolumeNameCollection TransferredVolumes { get; set; }	전송된 볼륨의 컬렉션을 가져오거나 설정합니다.
public VolumeNameCollection DependentVolumeNames { get; set; }	종속 볼륨의 컬렉션을 가져오거나 설정합니다.
public QuotaSettingsCollection EnabledDiskQuotas { get; set; }	볼륨에서 활성화된 할당량을 가져오거나 설정합니다.
public ShadowCopyType ShadowCopyType { get }	전송에 대한 복사 유형을 가져옵니다. 사용 가능한 값: · 복사 · 전체
public AgentTransferConfiguration TransferConfiguration { get; set; }	전송 구성을 가져오거나 설정합니다. AgentTransferConfiguration은 다음 데이터가 포함된 객체입니다. · MaxConcurrentStreams. Core가 데이터를 전송하기 위해 에이전트에 대해 설정하는 동시 TCP 연결의 최대 수 · MaxTransferQueueDepth. 쓰기를 위해 대기할 수 있는 블록 범위의 최대 수

메서드	설명

	• MaxConcurrentWrites. 지정된 시간에 epoch에서 해결되지 않은 블록 쓰기 작업의 최대 수. 이 개수의 블록 쓰기 작업이 해결되지 않은 상태에서 추가 블록이 수신되는 경우 추가 블록은 해결되지 않은 블록 중 하나가 작성될 때까지 무시됩니다.
	• MaxSegmentSize. 단일 요청으로 전송될 인접 블록의 최대 수
	• Priority. 다음 데이터가 포함된 객체입니다.
	  • 정의되지 않음
	  • 1
	  • 2
	  • 3
	  • 4
	  • 5
	  • 6
	  • 7
	  • 8
	  • 9
	  • 10
	  • 가장 높음(1과 같음)
	  • 가장 낮음(10과 같음)
	  • 기본값(5와 같음)
	• MaxRetries. 실패한 전송이 실패한 것으로 간주되기 전에 재시도해야 하는 최대 횟수
	• UseDefaultMaxRetries. 최대 재시도 횟수가 기본값임을 나타내는 값
	• ProviderId. 이 호스트에서 스냅숏에 사용하는 VSS 공급자의 GUID. 사용자는 일반적으로 기본 설정을 사용합니다.

public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	저장소 구성을 가져오거나 설정합니다.
public string Key { get; set; }	전송 요청을 인증하기 위해 1회용 암호로 사용할 수 있는 의사 난수(단, 암호 표기 상 안전한) 키를 생성합니다.
public bool IsBaseImage { get; set; }	기본 이미지를 가져오는지 여부를 나타내는 값을 가져오거나 설정합니다.
public bool IsForced { get; set; }	정송을 강제 적용하는지 여부를 나타내는 값을 가져오거나 설정합니다.
public Guid ProtectionGroupId { get; set; }	보호 그룹의 ID를 가져오거나 설정합니다.
public TargetComponentTypes LogTruncationTargets { get; set; }	데이터베이스 로그 자르기를 수행할 위치(SQL 또는 Exchange)를 나타내는 값을 가져오거나 설정합니다.
public bool ForceBaseImage { get }	기본 이미지가 적용되었는지 여부를 나타내는 값을 가져옵니다.
public bool IsLogTruncation { get }	로그 자르기 작업을 수행하는지 여부를 나타내는 값을 가져옵니다.

TransferPrescriptParameter(Replay.Common.Contracts.PowerShellExecution 네임스페이스)

TransferScriptParameterBase 매개 변수에서 값을 상속합니다.

TransferPostscriptParameter(Replay.Common.Contracts.PowerShellExecution 네임스페이스)

다음 표에는 TransferPostscript 매개 변수에 대해 사용 가능한 객체가 나와 있습니다. TransferScriptParameterBase 매개 변수에서 값을 상속합니다.

표 310. TransferPostscript 매개 변수에 대한 객체

메서드	설명
public VolumeNameCollection VolumeNames (get; set;)	전송에 대한 볼륨 이름 모음을 가져오거나 설정합니다. VolumeNames는 다음 데이터가 포함된 데이터 구조입니다. · GuidName. DisplayName가 설정되지 않은 경우 이름으로 사용되고 볼륨과 연관된 GUID. · DisplayName. 볼륨의 표시 이름.
public ShadowCopyType ShadowCopyType { get; set; }	전송에 대한 복사 유형을 가져오거나 설정합니다. ShadowCopyType는 값의 목록입니다. 사용 가능한 값: · 알 수 없음 · 복사 · 전체
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	저장소 구성을 가져오거나 설정합니다.
public AgentTransferConfiguration TransferConfiguration { get; set; }	전송 구성을 가져오거나 설정합니다. AgentTransferConfiguration은 다음 데이터가 포함된 객체입니다. · MaxConcurrentStreams. Core가 데이터를 전송하기 위해 에이전트에 대해 설정하는 동시 TCP 연결의 최대 수 · MaxTransferQueueDepth. 쓰기를 위해 대기할 수 있는 블록 범위의 최대 수 · MaxConcurrentWrites. 지정된 시간에 epoch에서 해결되지 않은 블록 쓰기 작업의 최대 수. 이 개수의 블록 쓰기 작업이 해결되지 않은 상태에서 추가 블록이 수신되는 경우 추가 블록은 해결되지 않은 블록 중 하나가 작성될 때까지 무시됩니다. · MaxSegmentSize. 단일 요청으로 전송될 인접 블록의 최대 수 · Priority. 다음 데이터가 포함된 객체입니다. · "정의되지 않음 · "1 · "2 · "3 · "4 · "5 · "6 · "7 · "8 · "9 · "10 · "가장 높음(1과 같음) · "가장 낮음(10과 같음)

메서드	설명
	• "기본값(5와 같음) • MaxRetries. 실패한 전송이 실패한 것으로 간주되기 전에 재시도해야 하는 최대 횟수 • UseDefaultMaxRetries. 최대 재시도 횟수가 기본값임을 나타내는 값 • ProviderId. 이 호스트에서 스냅숏에 사용하는 VSS 공급자의 GUID. 관리자들은 일반적으로 기본값을 사용합니다.
public AgentTransferConfiguration TransferConfiguration { get; set; } (계속)	• ExcludedWriterIds. 이 스냅숏에서 제외해야 하는 VSS 작성기 ID 모음. 작성기 ID는 작성기 이름으로 입력됩니다. 이 이름은 설명서 작성 목적으로만 사용되며 작성기의 실제 이름과 정확히 일치할 필요가 없습니다. • TransferDataServerPort. 에이전트에서 Core로의 실제 데이터 전송을 위해 Core에서 연결을 수락하는 TCP 포트가 포함된 값. • SnapshotTimeout. 중단 및 시간 초과 전에 VSS 스냅숏 작업이 완료되기까지 대기해야 하는 시간. • TransferTimeout. 스냅숏을 중단하기 전에 Core로부터 추가 연결을 대기해야 하는 시간. • NetworkReadTimeout. 이 전송과 관련된 네트워크 읽기 작업의 시간 초과. • NetworkWriteTimeout. 이 전송과 관련된 네트워크 쓰기 작업의 시간 초과. • InitialQueueSize. 초기 요청 대기열의 크기. • MinVolumeFreeSpacePercents. 볼륨의 최소 사용 가능한 공간(퍼센트). • MaxChangeLogsSizePercents. 볼륨 용량의 일부로 측정되는 드라이버 변경 로그의 최대 크기(퍼센트). • EnableVerification. Core로 전송되는 각 블록의 진단 확인을 수행해야 하는지 여부를 나타내는 값.
public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }	저장소 구성을 가져오거나 설정합니다. AgentProtectionStorageConfiguration 객체에는 다음 데이터가 포함됩니다. • RepositoryId. 이 에이전트의 복구 지점이 저장될 리포지토리의 이름 • EncryptionKeyId. 이 에이전트의 복구 지점에 대한 암호화 키의 ID. 빈 문자열은 암호화하지 않음을 의미합니다.
public string Key { get; set; }	Key 메서드는 전송 요청을 인증하기 위해 1회용 암호로 사용할 수 있는 의사 난수(단, 암호 표기 상 안전한) 키를 생성합니다.
public bool ForceBaseImage { get; set; }	전송이 강제 기본 이미지 캡처였는지 여부를 나타내는 값을 가져오거나 설정합니다.
public bool IsLogTruncation { get; set; }	로깅이 잘라내기되는지 여부를 나타내는 값을 가져오거나 설정합니다.
public uint LatestEpochSeenByCore { get; set; }	최신 epoch 값을 가져오거나 설정합니다. LatestEpochSeenByCore 메서드는 Core가 가장 최근에 작성한 스냅숏의 서수입니다. 이 숫자는 VSS가 스냅숏을 작성할 때 필터 드라이버가 특정 스냅숏에 할당하는 'epoch 번호'입니다.
public Guid SnapshotSetId { get; set; }	VSS에 의해 이 스냅숏에 할당된 GUID를 가져오거나 설정합니다.
public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }	스냅숏에 포함된 각 볼륨에 대한 스냅숏 모음을 가져오거나 설정합니다.

TransferScriptParameterBase(Replay.Common.Contracts.PowerShellExecution 네임스페이스)

다음 표에는 TransferScriptParameterBase 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 311. TransferScriptParameterBase 매개 변수에 대한 객체

메서드	설명
public AgentTransferConfiguration TransferConfiguration { get; set; }	전송 구성을 가져오거나 설정합니다.
public AgentProtectionStorageConfigurationCommon StorageConfiguration { get; set; }	저장소 구성을 가져오거나 설정합니다.

VirtualMachineLocation(Replay.Common.Contracts.Virtualization 네임스페이스)

다음 표에는 VirtualMachineLocation 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 312. VirtualMachineLocation 매개 변수에 대한 객체

메서드	설명
public string Description { get; set;}	이 위치에 대해 사람이 읽을 수 있는 형태의 설명을 가져오거나 설정합니다.
public string Name { get; set;}	VM의 이름을 가져오거나 설정합니다.

VolumeImageIdsCollection(Replay.Core.Contracts.RecoveryPoints 네임스페이스)

System.Collections.ObjectModel.Collection<string> 매개 변수에서 값을 상속합니다.

VolumeName(Replay.Common.Contracts.Metadata.Storage 네임스페이스)

다음 표에는 VolumeName 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 313. VolumeName 매개 변수에 대한 객체

메서드	설명
public string GuidName { get; set;}	볼륨의 ID를 가져오거나 설정합니다.
public string DisplayName { get; set;}	볼륨의 이름을 가져오거나 설정합니다.

메서드	설명
public string UrlEncode()	URL에서 명확하게 전달할 수 있는 이름의 URL 인코딩 버전을 가져옵니다. **노트: .NET 4.0 WCF에는 URI 템플릿에서 경로 이스케이프 문자가 제대로 작동하지 않는 알려진 문제가 있습니다(https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312). 볼륨 이름에 '\' 및 '?'가 모두 포함되어 있기 때문에 특수 문자 '\' 및 '?'를 다른 특수 문자로 변경해야 합니다.**
public string GetMountName()	볼륨 이미지를 일부 폴더에 마운트하는 데 유효한 이 볼륨의 이름을 반환합니다.

VolumeNameCollection(Replay.Common.Contracts.Metadata.Storage 네임스페이스)

System.Collections.ObjectModel.Collection<VolumeName> 매개 변수에서 값을 상속합니다.

다음 표에는 VolumeNameCollection 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 314. VolumeNameCollection 매개 변수에 대한 객체

메서드	설명
public override bool Equals(object obj)	이 인스턴스 및 지정된 객체(VolumeNameCollection 객체이기도 해야 함)의 값이 같은지 여부를 지정합니다. (Object.Equals(Object)를 재정의합니다.)
public override int GetHashCode()	이 VolumeNameCollection에 대한 해시 코드를 반환합니다. (Object.GetHashCode()를 재정의합니다.)

VolumeSnapshotInfo(Replay.Common.Contracts.Transfer 네임스페이스)

다음 표에는 VolumeSnapshotInfo 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 315. VolumeSnapshotInfo 매개 변수에 대한 객체

메서드	설명
public Uri BlockHashesUri { get; set;}	볼륨 블록의 MD5 해시를 읽을 수 있는 URI를 가져오거나 설정합니다.
public Uri BlockDataUri { get; set;}	볼륨 데이터 블록을 읽을 수 있는 URI를 가져오거나 설정합니다.

VolumeSnapshotInfoDictionary(Replay.Common.Contracts.Transfer 네임스페이스)

System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo> 매개 변수에서 값을 상속합니다.

샘플 PowerShell 스크립트

다음 샘플 스크립트는 PowerShell 스크립트를 실행하는 관리자를 지원하기 위해 제공됩니다.

관련 링크

PreTransferScript.sh
PostTransferScript.ps1
PreExportScript.ps1
PostExportScript.ps1
PreNightlyJobScript.ps1
PostNightlyJobScript.ps1

PreTransferScript.ps1

PreTransferScript는 스냅숏을 전송하기 전 보호된 컴퓨터에서 실행됩니다.

샘플 PreTransferScript

```
# receiving parameter from transfer job
param([object]$TransferPrescriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
$TransferPrescriptParameterObject = $TransferPrescriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPrescriptParameter];
# Working with input object. All echo's are logged
if($TransferPrescriptParameterObject -eq $null) {
        echo 'TransferPrescriptParameterObject parameter is null'
}
else {
        echo 'TransferConfiguration:'$TransferPrescriptParameterObject.TransferConfiguration
        echo 'StorageConfiguration:' $TransferPrescriptParameterObject.StorageConfiguration
}
```

PostTransferScript.ps1

PostTransferScript는 스냅숏을 전송한 후 보호된 컴퓨터에서 실행됩니다.

샘플 PostTransferScript

```
# receiving parameter from transfer job
param([object] $TransferPostscriptParameter)
# building path to Agent's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Agent 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
```

```
$TransferPostscriptParameterObject = $TransferPostscriptParameter -as
[Replay.Common.Contracts.PowerShellExecution.TransferPostscriptParameter];
# Working with input object. All echo's are logged
if($TransferPostscriptParameterObject -eq $null) {
            echo 'TransferPostscriptParameterObject parameter is null'
}
else {
echo 'VolumeNames:' $TransferPostscriptParameterObject.VolumeNames
            echo 'ShadowCopyType:' $TransferPostscriptParameterObject.ShadowCopyType
        echo 'ForceBaseImage:' $TransferPostscriptParameterObject.ForceBaseImage
        echo 'IsLogTruncation:' $TransferPostscriptParameterObject.IsLogTruncation
}
```

PreExportScript.ps1

PreExportScript는 내보내기 작업 전 Core에서 실행됩니다.

샘플 PreExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
        echo 'ExportJobRequestObject parameter is null'
}
else {
        echo 'Location:' $ExportJobRequestObject.Location
        echo 'Priority:' $ExportJobRequestObject.Priority
}
```

PostExportScript.ps1

PostExportScript는 내보내기 작업 후 Core에서 실행됩니다.

노트: 처음 시작 후 내보낸 보호된 시스템에서 한 번 실행하기 위해 사용되는 경우 PostExportScript에 대한 입력 매개 변수는 없습니다. 보호된 일반 시스템는 이 스크립트를 PowerShell 스크립트 폴더에 PostExportScript.ps1로 포함해야 합니다.

샘플 PostExportScript

```
# receiving parameter from export job
param([object]$ExportJobRequest)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2 = $regVal2 + 'CoreService\Common.Contracts.dll'
```

```
# Converting input parameter into specific object
$ExportJobRequestObject = $ExportJobRequest -as [Replay.Core.Contracts.Export.ExportJobRequest]
# Working with input object. All echo's are logged
if($ExportJobRequestObject -eq $null) {
        echo 'ExportJobRequestObject parameter is null'
}
else {
        echo 'VolumeImageIds:' $ExportJobRequestObject.VolumeImageIds
        echo 'RamInMegabytes:' $ExportJobRequestObject.RamInMegabytes
}
```

PreNightlyJobScript.ps1

PreNightlyJobScript는 모든 야간 작업 전에 Core에서 실행됩니다. 이 스크립트는 해당 하위 작업을 별도로 처리하는 데 사용할 수 있는 $JobClassName 매개 변수를 포함합니다.

샘플 PreNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
            if($NightlyAttachabilityJobRequestObject -eq $null) {
                echo 'NightlyAttachabilityJobRequestObject parameter is null';
            }
            else {
                echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
                echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
            }
            break;
        }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
            if($RollupJobRequestObject -eq $null) {
                    echo 'RollupJobRequestObject parameter is null';
            }
            else {
                echo 'SimultaneousJobsCount:' $RollupJobRequestObject.SimultaneousJobsCount;
                    echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
                    echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
            }
            $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System.Guid]"
            if($AgentsCollection -eq $null) {
                echo 'AgentsCollection parameter is null';
            }
```

```
            else {
                echo 'Agents GUIDs:'
                foreach ($a in $AgentsCollection) {
                    echo $a
                }
            }
            break;
        }
# working with Checksum Check Job
            ChecksumCheckJob {
                $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
                echo 'Exchange checksumcheck job results:';
                if($ChecksumCheckJobRequestObject -eq $null) {
                    echo 'ChecksumCheckJobRequestObject parameter is null';
            }
            else {
                    echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
                    echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
                    echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
                }
                break;
            }
# working with Log Truncation Job
        TransferJob {
            $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
            echo 'Transfer job results:';
            if($TransferJobRequestObject -eq $null) {
                    echo 'TransferJobRequestObject parameter is null';
            }
            else {
                    echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
                    echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
                }
                echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
                break;
            }
}
```

PostNightlyJobScript.ps1

PostNightlyJobScript는 모든 야간 작업 후에 Core에서 실행됩니다. 이 스크립트는 해당 하위 작업을 별도로 처리하는 데 사용할 수 있는 $JobClassName 매개 변수를 포함합니다.

샘플 PostNightlyJobScript

```
# receiving parameters from Nightlyjob
param([System.String]$JobClassMethod , [object]$NightlyAttachabilityJobRequest, [object]
$RollupJobRequest, [object]$Agents, [object]$ChecksumCheckJobRequest, [object]
$TransferJobRequest, [int]$LatestEpochSeenByCore, [object]$TakeSnapshotResponse)
# building path to Core's Common.Contracts.dll and loading this assembly
$regLM = [Microsoft.Win32.Registry]::LocalMachine
$regLM = $regLM.OpenSubKey('SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\AppRecovery
Core 5')
$regVal = $regLM.GetValue('InstallLocation')
$regVal = $regVal + 'CoreService\Common.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal)  |  out-null
$regVal2 = $regLM.GetValue('InstallLocation')
$regVal2= $regVal2 + 'CoreService\Core.Contracts.dll'
[System.Reflection.Assembly]::LoadFrom($regVal2) | out-null
# Nightlyjob has four child jobs: NightlyAttachability Job, Rollup Job, Checksum Check Job and
Log Truncation Job. All of them are triggering the script, and $JobClassMethod (contain job
name that calls the script) helps to handle those child jobs separately
```

```
switch ($JobClassMethod) {
# working with NightlyAttachability Job
    NightlyAttachabilityJob {
        $NightlyAttachabilityJobRequestObject = $NightlyAttachabilityJobRequest -as
[Replay.Core.Contracts.Sql.NightlyAttachabilityJobRequest];
        echo 'Nightly Attachability job results:';
        if($NightlyAttachabilityJobRequestObject -eq $null) {
            echo 'NightlyAttachabilityJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $NightlyAttachabilityJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $NightlyAttachabilityJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Rollup Job
    RollupJob {
        $RollupJobRequestObject = $RollupJobRequest -as
[Replay.Core.Contracts.Rollup.RollupJobRequest];
        echo 'Rollup job results:';
        if($RollupJobRequestObject -eq $null) {
            echo 'RollupJobRequestObject parameter is null';
        }
        else {
            echo 'AgentIds:' $RollupJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $RollupJobRequestObject.IsNightlyJob;
        }
        $AgentsCollection = $Agents -as "System.Collections.Generic.List``1[System.Guid]"
        if($AgentsCollection -eq $null) {
            echo 'AgentsCollection parameter is null';
        }
        else {
        echo 'Agents GUIDs:'
            foreach ($a in $AgentsCollection) {
                echo $a
                }
            }
            break;
        }
# working with Checksum Check Job
    ChecksumCheckJob {
        $ChecksumCheckJobRequestObject = $ChecksumCheckJobRequest -as
[Replay.Core.Contracts.Exchange.ChecksumChecks.ChecksumCheckJobRequest];
        echo 'Exchange checksumcheck job results:';
        if($ChecksumCheckJobRequestObject -eq $null) {
            echo 'ChecksumCheckJobRequestObject parameter is null';
        }
        else {
            echo 'RecoveryPointId:' $ChecksumCheckJobRequestObject.RecoveryPointId;
            echo 'AgentIds:' $ChecksumCheckJobRequestObject.AgentIds;
            echo 'IsNightlyJob:' $ChecksumCheckJobRequestObject.IsNightlyJob;
        }
        break;
    }
# working with Log Truncation Job
    TransferJob {
        $TransferJobRequestObject = $TransferJobRequest -as
[Replay.Core.Contracts.Transfer.TransferJobRequest];
        echo 'Transfer job results:';
        if($TransferJobRequestObject -eq $null) {
            echo 'TransferJobRequestObject parameter is null';
        }
        else {
             echo 'TransferConfiguration:' $TransferJobRequestObject.TransferConfiguration;
            echo 'StorageConfiguration:' $TransferJobRequestObject.StorageConfiguration;
        }
        echo 'LatestEpochSeenByCore:' $LatestEpochSeenByCore;
        $TakeSnapshotResponseObject = $TakeSnapshotResponse -as
[Replay.Agent.Contracts.Transfer.TakeSnapshotResponse];
```

```
        if($TakeSnapshotResponseObject -eq $null) {
            echo 'TakeSnapshotResponseObject parameter is null';
        }
        else {
            echo 'ID of this transfer session:' $TakeSnapshotResponseObject.SnapshotSetId;
            echo 'Volumes:' $TakeSnapshotResponseObject.VolumeSnapshots;
        }
        break;
    }
}
```

Rapid Recovery에서 Bourne Shell 스크립팅 사용

Bourne shell(sh)은 Unix 기반 운영 체제용 셸 언어 또는 명령줄 인터프리터입니다. Bourne Shell은 Linux가 설치된 Rapid Recovery에서 사용되어 환경을 사용자 지정하고 특정 작업이 미리 결정된 순서로 발생하도록 지정합니다. .sh는 Bourne Shell 파일의 파일 확장명이면서 명명 규칙입니다.

Bourne Again Shell(BASH)은 동일한 문법, 매개 변수 및 가변 확장, 리디렉션 및 쿼우팅(quoting)을 구현하는 유사 셸 언어입니다. 또한 BASH는 동일한 .sh 파일 확장자를 사용합니다. 여기에 있는 정보는 BASH에 동일하게 적용됩니다.

사전 전송, 사후 전송 및 내보내기 스크립트 후크를 사용하여 전송 또는 내보내기 전후에 시스템 작업을 수행할 수 있습니다. 예를 들어, 전송이 수행되는 동안 특정 cronjob을 비활성화했다가 전송이 완료된 후 활성화할 수 있습니다. 또 다른 예로, 응용프로그램 관련 데이터를 디스크로 플러시하는 명령을 실행해야 할 경우도 있습니다. 콘텐츠가 임시 파일에 기록되고 exec를 사용하여 실행됩니다. 그런 다음 스크립트는 스크립트의 첫 번째 행에 정의된 인터프리터를 사용하여 실행됩니다(`#!/usr/bin/env bash`). 지정된 인터프리터를 사용할 수 없는 경우 스크립트는 $SHELL 환경 변수에 정의된 기본 셸을 사용합니다.

인터프리터를 대체 및 사용할 수 있습니다. 예를 들어, 스크립트의 `#!` 행에서 환경 설정을 기준으로 “bash”를 “zsh”(Z shell), "tcsh"(tee shell) 등으로 바꿀 수 있습니다.

TransferPrescript 매개 변수에서 사용 가능한 객체를 추가하거나 명령을 PreTransferScript.sh 및 PostTransfer.sh 스크립트에 직접 추가하여 사용자 지정할 수 있습니다.

이 섹션에서는 Windows 및 Linux용 Rapid Recovery에서 지정된 발생 상황에서 관리자가 사용할 수 있는 스크립트에 대해 설명합니다. 이 장은 다음 항목으로 구성되어 있습니다.

- Bourne Shell 스크립트 작성을 위한 입력 매개 변수
- 샘플 Bourne Shell 스크립트

Bourne Shell 스크립트 작성을 위한 전제 조건

Rapid Recovery는 전송 전과 후에 Linux Agent 시스템에서 Bourne Shell 스크립트를 실행하는 기능을 제공합니다. Rapid Recovery Agent 소프트웨어로 보호되는 Linux 시스템에서 지원되는 스크립트는 다음과 같습니다.

노트: 스크립트가 실행 파일이 아닌 경우 전송 작업이 실패합니다.

- PreTransferScript.sh
- PostTransferScript.sh
- PostExportScript.sh

이러한 스크립트를 사용하려면 해당 스크립트가 `/opt/apprecovery/scripts/` 디렉터리에 있는지 확인하십시오.

지원되는 전송 및 사후 전송 스크립트 매개 변수

전송 스크립트에 대해 Linux에서 다음 매개 변수가 지원됩니다. 자세한 내용은 샘플 Bourne Shell 스크립트을(를) 참조하십시오.

- TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
- TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
- TransferPrescriptParameter_TransferConfiguration=$TransferPrescriptParameter_TransferConfiguration
- TransferPrescriptParameter_StorageConfiguration=$TransferPrescriptParameter_StorageConfiguration
- TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
- TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
- TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
- TransferPrescriptParameter_LatestEpochSeenByCore=$TransferPrescriptParameter_LatestEpochSeenByCore

사후 전송 스크립트에 대해 Linux에서 다음 매개 변수가 지원됩니다.

- TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
- TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
- TransferPostscriptParameter_TransferConfiguration=$TransferPostscriptParameter_TransferConfiguration
- TransferPostscriptParameter_StorageConfiguration=$TransferPostscriptParameter_StorageConfiguration
- TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
- TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
- TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
- TransferPostscriptParameter_LatestEpochSeenByCore=$TransferPostscriptParameter_LatestEpochSeenByCore

Bourne Shell 스크립트 작성 테스트

스크립트(.sh) 파일에 대해 편집기를 사용하여 실행하려는 스크립트를 테스트할 수 있습니다.

노트: 사전 Bourne Shell 스크립트 또는 사후 Bourne Shell 스크립트가 실패하면 작업도 실패합니다. 작업에 대한 정보는 /var/log/apprecovery/apprecovery.log 파일에서 확인할 수 있습니다.
성공적인 스크립트는 종료 코드 0을 반환합니다.

Bourne Shell 스크립트 작성을 위한 입력 매개 변수

Rapid Recovery의 Bourne Shell 스크립트 작성용 매개 변수가 다음 표에 설명되어 있습니다.

TransferPrescriptParameters_VolumeNames

다음 표에는 TransferPrescript 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 316. TransferPrescript 객체

메서드	설명
public VolumeNameCollection VolumeNames (get; set;)	전송에 대한 볼륨 이름 모음을 가져오거나 설정합니다.

메서드	설명
	VolumeNames는 다음 데이터가 포함된 데이터 구조입니다. • GuidName. DisplayName가 설정되지 않은 경우 이름으로 사용되고 볼륨과 연관된 GUID. • DisplayName. 볼륨의 표시 이름.
public ShadowCopyType ShadowCopyType { get; set; }	전송에 대한 복사 유형을 가져오거나 설정합니다. ShadowCopyType은 값의 목록입니다. 사용 가능한 값: • 알 수 없음 • 복사 • 전체
public string Key { get; set; }	Key 메서드는 전송 요청을 인증하기 위해 1회용 암호로 사용할 수 있는 의사 난수(단, 암호 표기 상 안전한) 키를 생성합니다.
public bool ForceBaseImage { get; set; }	전송이 강제 기본 이미지 캡처였는지 여부를 나타내는 값을 가져오거나 설정합니다.
public bool IsLogTruncation { get; set; }	로깅이 잘라내기되는지 여부를 나타내는 값을 가져오거나 설정합니다.
public uint LatestEpochSeenByCore { get; set; }	최신 epoch 값을 가져오거나 설정합니다. LatestEpochSeenByCore 메서드는 Core가 가장 최근에 작성한 스냅숏의 서수입니다. 이 숫자는 VSS가 스냅숏을 작성할 때 필터 드라이버가 특정 스냅숏에 할당하는 'epoch 번호'입니다.

TransferPostscriptParameter

다음 표에는 TransferPostscript 매개 변수에 대해 사용 가능한 객체가 나와 있습니다.

표 317. TransferPostscript 객체

메서드	설명
public VolumeNameCollection VolumeNames (get; set;)	전송에 대한 볼륨 이름 모음을 가져오거나 설정합니다. VolumeNames는 다음 데이터가 포함된 데이터 구조입니다. • GuidName. DisplayName가 설정되지 않은 경우 이름으로 사용되고 볼륨과 연관된 GUID. • DisplayName. 볼륨의 표시 이름.
public ShadowCopyType ShadowCopyType { get; set; }	전송에 대한 복사 유형을 가져오거나 설정합니다. ShadowCopyType은 값의 목록입니다. 사용 가능한 값: • 알 수 없음 • 복사 • 전체
public string Key { get; set; }	Key 메서드는 전송 요청을 인증하기 위해 1회용 암호로 사용할 수 있는 의사 난수(단, 암호 표기 상 안전한) 키를 생성합니다.
public bool ForceBaseImage { get; set; }	전송이 강제 기본 이미지 캡처였는지 여부를 나타내는 값을 가져오거나 설정합니다.
public bool IsLogTruncation { get; set; }	로깅이 잘라내기되는지 여부를 나타내는 값을 가져오거나 설정합니다.

메서드	설명
public uint LatestEpochSeenByCore { get; set; }	최신 epoch 값을 가져오거나 설정합니다. LatestEpochSeenByCore 메서드는 Core가 가장 최근에 작성한 스냅숏의 서수입니다. 이 숫자는 VSS가 스냅숏을 작성할 때 필터 드라이버가 특정 스냅숏에 할당하는 'epoch 번호'입니다.

샘플 Bourne Shell 스크립트

이 섹션에서는 보호된 시스템에서 관리자가 실행할 수 있는 샘플 Bourne Shell 스크립트를 설명합니다.

△ 주의: **이 문서에 제공된 샘플 Bourne 스크립트는 자격을 갖춘 관리자가 설계한 대로 실행할 때 작동합니다. 사용 중인 버전을 유지하기 위해 작동 중인 스크립트를 수정할 때는 주의를 기울이십시오. 여기에 포함된 스크립트 샘플 또는 사용자가 수정한 스크립트는 사용자 지정 사항으로 간주되어, 일반적으로 Dell 고객 지원 부서에서 다루지 않습니다.**

ⓘ 노트: **보호된 시스템는 'exec' 셸 명령을 사용하여 스크립트를 실행합니다. 스크립트의 첫 번째 행에 해당 정보를 정의하여 스크립트를 실행해야 하는 인터프리터를 나타낼 수 있습니다. 인터프리터를 지정하지 않은 경우 기본 셸이 스크립트를 해석합니다. 기본 셸이 아닌 다른 셸을 선택하는 경우 모든 보호된 시스템에서 지정된 인터프리터를 사용할 수 있는지 확인해야 합니다.**

보호된 시스템용 샘플 스크립트에는 다음 항목이 포함됩니다.

PreTransferScript.sh

PreTransferScript는 스냅숏을 전송하기 전 보호된 컴퓨터에서 실행됩니다.

다음 스크립트는 루트 홈 디렉터리에 저장되는 Pre(Post)TransferScriptResult.txt의 입력 매개 변수에서 값을 저장합니다.

샘플 PreTransferScript

```
#!/bin/bash
echo "TransferPrescriptParameter_VolumeNames=$TransferPrescriptParameter_VolumeNames
TransferPrescriptParameter_ShadowCopyType=$TransferPrescriptParameter_ShadowCopyType
TransferPrescriptParameter_Key=$TransferPrescriptParameter_Key
TransferPrescriptParameter_ForceBaseImage=$TransferPrescriptParameter_ForceBaseImage
TransferPrescriptParameter_IsLogTruncation=$TransferPrescriptParameter_IsLogTruncation
TransferPrescriptParameter_LatestEpochSeenByCore=
$TransferPrescriptParameter_LatestEpochSeenByCore" > ~/PreTransferScriptResult.txt
exit 0
```

PostTransferScript.sh

PostTransferScript는 스냅숏을 전송한 후 보호된 컴퓨터에서 실행됩니다.

다음 스크립트는 루트 홈 디렉터리에 저장되는 Pre(Post)TransferScriptResult.txt의 입력 매개 변수에서 값을 저장합니다.

샘플 PostTransferScript

```
#!/bin/bash
echo "TransferPostscriptParameter_VolumeNames=$TransferPostscriptParameter_VolumeNames
TransferPostscriptParameter_ShadowCopyType=$TransferPostscriptParameter_ShadowCopyType
TransferPostscriptParameter_Key=$TransferPostscriptParameter_Key
TransferPostscriptParameter_ForceBaseImage=$TransferPostscriptParameter_ForceBaseImage
TransferPostscriptParameter_IsLogTruncation=$TransferPostscriptParameter_IsLogTruncation
TransferPostscriptParameter_LatestEpochSeenByCore=
```

```
$TransferPostscriptParameter_LatestEpochSeenByCore" > ~/PostTransferScriptResult.txt
exit 0
```

PostExportScript.sh

PostExportScript는 전송 후 보호된 시스템에서 실행됩니다.

다음 스크립트는 루트 홈 디렉터리에 저장되는 Pre(Post)ExportScriptResult.txt의 입력 매개 변수에서 값을 저장합니다.

샘플 PostExportScript

```
#!/bin/bash
echo
"$curr_name-exported" > /etc/hostname
exit 0
```

D

Rapid Recovery API

이 섹션의 목적은 Rapid Recovery REST(Representational State Transfer) API(Application Program Interface) 소개 및 개요, 사용 용도, 기능을 제공하는 것입니다.

Rapid Recovery 웹 서비스 API는 RESTful로, 이 웹 서비스 API를 사용하면 Rapid Recovery 소프트웨어 솔루션 내 특정 기능 및 작업을 자동화하고 사용자 지정하여 비즈니스 목적을 충족할 수 있습니다.

이러한 API는 Dell Data Protection | Rapid Recovery License Portal의 **다운로드** 페이지에서 접근할 수 있습니다.

주제:

- 대상 사용자
- Rapid Recovery REST API로 작업
- Core 및 Agent API 다운로드 및 보기
- 권장된 추가 문서

대상 사용자

Rapid Recovery API는 해당 응용프로그램에서 Rapid Recovery를 통합하고 확장하려는 응용프로그램 개발자뿐만 아니라 Rapid Recovery Core Server와의 상호 작용을 스크립트로 작성하려는 관리자도 사용할 수 있습니다.

Rapid Recovery REST API로 작업

Rapid Recovery API는 REST 형식 API로, HTTP 요청을 사용하여 URI 경로를 통해 리소스(데이터 엔터티)에 액세스할 수 있습니다. Rapid Recovery API는 GET, PUT, POST 및 DELETE와 같은 표준 HTTP 메서드를 사용합니다. REST API는 개방형 표준에 기반하므로, HTTP 호출을 지원하는 모든 언어나 도구를 사용할 수 있습니다.

응용 프로그램 개발자 및 관리자가 Rapid Recovery API로 작업할 수 있는 두 가지 방법은 다음과 같습니다.

- C# 또는 기타 .NET 언어를 사용하여 Rapid Recovery .NET 클라이언트 DLL 파일을 직접 사용.
- HTTP 엔드포인트와 직접 통신하여 XML을 직접 생성.

첫 번째 접근방식이 권장됩니다. 클라이언트 DLL은 Rapid Recovery SDK에 포함됩니다. Rapid Recovery API를 호출하는 방법은 .NET 4.5X WCF(Windows Communication Foundation) 서비스를 사용하는 방법과 같습니다.

Core 및 Agent API 다운로드 및 보기

*Dell Data Protection | Rapid Recovery 소프트웨어 개발자 키트(SDK)*에는 Rapid Recovery Core 및 Rapid Recovery Agent 구성 요소, 샘플 그리고 지원 파일이 포함되어 있습니다. 이러한 내용물을 다음 폴더에 포함시킨 후 다음 구성 요소를 포함하는 아카이브로 압축됩니다.

표 318. SDK 아카이브에 포함된 구성 요소

폴더 이름	콘텐츠	설명
Core.계약	Rapid Recovery Core API	Rapid Recovery Core에서 개발자 또는 관리자의 스크립트 기능을 지원하기 위한 API가 포함되어 있습니다. 두 세트의 서비 계약이 있습니다. 1 일반 REST 표준에 대한 정보를 보려면 웹 브라우저에서 CoreWeb.Client HTML 파일을 엽니다. 서비스 계약이 나열됩니다. 해당하는 하이퍼링크된 URI(Uniform Resource Identifier)를 클릭하면 브라우저가 **Core.Contracts/docWeb/** 디렉터리에서 정보를 엽니다. 결과 페이지는 메서드 및 설명을 포함해 일반 REST 서비스 작업에 대한 정보를 표시합니다. 2 자세한 C# 정보를 보려면 웹 브라우저에서 Core.Client HTML 파일을 엽니다. 하이퍼링크된 서비스 계약(클래스)를 클릭하면 브라우저는 **Core.Contracts/doc/** 디렉터리에서 정보를 엽니다. 결과 페이지는 선택한 클래스에서 모든 C# 메서드에 대한 자세한 정보를 보여줍니다.
Agent.Contracts	Rapid Recovery Agent API(사용 안 함)	개발자 또는 관리자가 보호된 시스템에서 Rapid Recovery Agent를 조작하기 위해 사용할 수 있는 API가 포함되어 있습니다. **주의: Agent API는 더 이상 사용되지 않으며 이후 버전의 SDK에서 제거될 예정입니다. Agent API를 직접 조작하지 않는 것이 좋습니다. 이러한 API를 사용하는 것은 사용자 지정으로 간주되어 지원되지 않습니다. 이 정보는 기록을 위해 문서에 제공됩니다.** 1 일반 REST 표준에 대한 정보를 보려면 웹 브라우저에서 AgentWeb.Client HTML 파일을 엽니다. 2 자세한 C# 정보를 보려면 웹 브라우저에서 Agent.Client HTML 파일을 엽니다.
AppRecoveryAPI Samples	코드 샘플 및 동적 링크 라이브러리	**AppRecoveryAPISamples**에는 C# 프로그래밍 언어로 작성된 코드 샘플이 포함되어 있습니다. 이러한 파일은 GUI, 관리 시스템 등을 사용자 지정하기 위해 API를 사용할 경우 코드 조각을 보기 위한 좋은 시작점을 나타냅니다. **AppRecoveryAPISamples\Dependencies**에는 Rapid Recovery Core에서 사용하는 동적 링크 라이브러리(DLL)가 포함되어 있습니다. DLL에는 데이터 계약(Core가 익숙한 유형)과 서비스 계약(Core의 작업 수행을 강제하는 데 사용할 수 있는 관리 메소드 및 작업)이 포함되어 있습니다. 사용자가 직접 그래픽 사용자 인터페이스를 사용자 지정하거나 Rapid Recovery Core와 사용할 관리 시스템을 사용하는 경우 이러한 DLL이 필요합니다. **노트: 사용된 DLL 버전은 Core 버전과 일치해야 합니다.**

SDK를 아카이브로 다운로드할 수 있습니다(API-Reference-x.x.x-xxxx). 각 x는 관련 릴리스에 대한 빌드 번호의 숫자를 나타냅니다.

Core 및 Agent API 사용을 준비하면서 SDK를 획득하고 지정한 위치로 다운로드하며 해당 파일의 압축을 해제하려면 이 절차의 단계를 완료합니다.

1 Dell Data Protection | Rapid Recovery License Portal(https://licenseportal.com)에 로그인합니다.
2 라이센스 포털의 왼쪽 탐색 메뉴에서 **다운로드**를 클릭합니다.
라이센스 포털의 **다운로드** 페이지가 나타납니다.
3 **다운로드** 페이지의 Windows 기반 응용 프로그램 섹션에서 해당 SDK에 대한 설명까지 아래로 스크롤하여 **다운로드**를 클릭합니다.
4 다운로드한 아카이브을 원하는 위치에 저장합니다.
5 아카이브의 압축을 풉니다.
새로운 API-Reference-x.x.x-xxxx 폴더에 이전 표에서 설명한 별도의 파일 세트가 있습니다.
6 해당 API에 대한 지침을 확인하려면 웹 브라우저에서 이전 표에 설명된 주요 HTML 파일을 엽니다.

권장된 추가 문서

*Dell Data Protection | Rapid Recovery 설치 및 업그레이드 안내서*는 Rapid Recovery 아키텍처의 개요를 제공하고, Rapid Recovery 구성 요소 설치 및 이전 버전에서 Core 또는 Agent 구성요소를 업그레이드하는 데 필요한 단계를 설명합니다.

https://support.software.dell.com/rapid-recovery/release-notes-guides/에서 이 안내서를 다운로드할 수 있습니다.

Dell 정보

Dell은 고객의 말에 귀를 기울이고 고객이 신뢰하면서 가치를 인정하는 혁신 기술과 비즈니스 솔루션 및 서비스를 전 세계에 제공합니다. 자세한 내용은 http://software.dell.com을 방문하십시오.

Dell에 문의하기

판매 또는 기타 질의 사항은 http://software.dell.com/company/contact-us.aspx 또는 + 1-949-754-8000으로 연락하십시오.

기술 지원 리소스

유효한 유지보수 계약을 보유한 Dell 소프트웨어 구입 고객과 평가판을 보유한 고객에게 기술 지원이 제공됩니다. Support Portal을 이용하려면 https://support.software.dell.com로 이동하십시오.

Support Portal에서는 문제를 직접 신속하게 해결하기 위해 사용할 수 있는 자체 헬프 도구를 연중무휴로 하루 24시간 제공합니다. 또한 Support Portal에서는 온라인 서비스 요청 시스템을 통해 제품 지원 엔지니어와 직접 연락할 수도 있습니다.

지원 포털을 사용하면 다음을 수행할 수 있습니다.

- 서비스 요청(사안) 작성, 수정 및 관리
- 기술 문서 보기
- 제품 알림 받기
- 소프트웨어 다운로드. 평가판 소프트웨어는 http://software.dell.com/trials를 참조하십시오.
- 커뮤니티 토론 참여

용어 해설

Agent

Rapid Recovery Agent는 Rapid Recovery Core의 보호에 추가될 수 있는 실제 또는 가상 시스템에 설치된 소프트웨어입니다.

CCR(Cluster Continuous Replication)

기본 제공된 비동기식 로그 제공 기술을 사용하여 각 저장소 그룹의 복사본을 장애 조치 클러스터의 두 번째 서버에 만들고 유지 관리하는 비공유 저장소 장애 조치 클러스터 솔루션입니다. CCR는 한 두개의 데이터 센터 솔루션으로 제공되어, 고가용성과 사이트 복구성을 모두 제공하도록 설계되었습니다. 이것은 Exchange 2007에서 사용할 수 있는 두 가지 유형의 CMS(Clustered Mailbox Server) 배포 중 하나입니다.

Central Management Console

Rapid Recovery Central Management Console은 둘 이상의 Rapid Recovery Core를 사용하는 환경에 알맞은 선택적 구성 요소입니다. 이 구성 요소는 하나의 웹 기반 인터페이스를 사용하는 여러 Core에 대한 보고서를 그룹화, 관리 및 생성할 수 있는 중앙 인터페이스를 제공하는 웹 포털입니다.

Core

Rapid Recovery Core는 Rapid Recovery 아키텍처의 중앙 구성요소입니다. Core는 백업, 복구, 보존, 복제, 아카이브 및 관리에 필요한 서비스를 제공합니다. 복제 맥락에서 Core를 소스 Core라고도 합니다. 소스 Core는 원본 Core이고 대상 Core는 목적지(보호된 시스템 또는 클러스터가 복제된 자체 전용 서버의 또 다른 Rapid Recovery Core)입니다.

Core Console

Rapid Recovery Core Console은 Rapid Recovery Core를 완전히 관리할 수 있는 웹 기반 인터페이스입니다.

DAG(Database Availability Group)

데이터베이스, 서버 또는 네트워크 오류에서 자동 데이터베이스 수준 복구를 제공하는 최대 16개의 Microsoft Exchange Server 2010 Mailbox 서버 집합입니다. DAG는 연속 복제와 Windows 장애 조치 클러스터링 기술 하위 집합을 사용하여 높은 가용성과 사이트 복구성을 제공합니다. DAG의 Mailbox 서버는 각자의 오류를 모니터링합니다. Mailbox 서버가 DAG에 추가될 때 이것은 DAG의 다른 서버와 함께 작동하여 데이터베이스 오류에서 자동 데이터베이스 수준 복구를 제공합니다.

global deduplication

SNIA(Storage Networking Industry Association)는 공유 복사본을 참조하여 다양한 세분화 수준에서 여러 데이터 복사본의 대체로 데이터 중복 제거를 정의하여 저장소 공간이나 대역폭을 절약합니다. Rapid Recovery 볼륨 관리자가 논리적 볼륨 내에서 전역 데이터 중복 제거를 수행합니다. 중복 제거 세분화 수준은 8KB입니다. Rapid Recovery에서 중복 제거 범위는 동일한 리포지토리 및 암호화 키를 사용하는 보호된 시스템으로 제한됩니다.

License Portal

Dell Data Protection | Rapid Recovery License Portal은 사용자와 파트너가 소프트웨어를 다운로드하고, Rapid Recovery 어플라이언스를 등록하며, 라이센스 구독을 관리할 수 있는 웹 인터페이스입니다. License Portal 사용자는 계정 등록, Rapid Recovery Core 및 Agent 소프트웨어 다운로드, 그룹 관리, 그룹 작업 추적, 시스템 등록, 어플라이언스 등록, 사용자 초대, 보고서 생성 작업을 수행할 수 있습니다. 자세한 내용은 *Dell Data Protection | Rapid Recovery License Portal 사용자 안내서*를 참조하십시오.

Live Recovery

Rapid Recovery Live Recovery는 VM 및 서버용 인스턴트 복구 기술입니다. 이 기술을 사용하면 가상 또는 실제 서버의 데이터 볼륨에 계속 액세스할 수 있으므로, 0분에 가까운 RTO 및 RPO로 전체 볼륨을 복구할 수 있습니다.

Local Mount Utility

LMU(Local Mount Utility)는 모든 시스템에서 원격 Rapid Recovery Core에 복구 지점을 마운트하기 위해 사용할 수 있는 다운로드 가능한 응용 프로그램입니다.

PowerShell 스크립트 작성

Windows PowerShell은 관리 자동화를 위해 설계된 Microsoft .NET Framework 연결 환경입니다. Rapid Recovery에는 관리자가 직접 또는 스크립트를 통해 명령을 실행하여 Rapid Recovery 리소스 운영 및 관리를 자동화할 수 있는 PowerShell 스크립트 작성을 위한 포괄적인 클라이언트 SDK가 포함되어 있습니다.

Rapid Recovery

Rapid Recovery는 백업, 복제 및 복구를 가상 시스템(VM)뿐만 아니라 실제 및 클라우드 환경을 보호하기 위한 가장 빠르고 신뢰할 수 있는 백업이 되도록 설계된 단일 솔루션으로 결합하여 통합 데이터 보호의 새로운 기준을 제시합니다.

REST API

REST(Representational State Transfer)는 확장용으로 설계된 상태가 없는 단순 소프트웨어 아키텍처입니다. Rapid Recovery는 이 아키텍처를 해당 API(Application Program Interface)가 특정 기능과 작업을 자동화하고 사용자 지정하는 데 사용합니다. Core 기능과 보호된 시스템 기능에 각각 다른 REST API 세트가 있습니다.

SharePoint 백업

SharePoint 백업은 시스템 오류 후 SharePoint 서버에 해당 데이터를 복원 및 복구하는 데 사용되는 데이터 사본입니다. SharePoint 백업에서 전체 SharePoint 팜 또는 하나 이상의 팜 구성 요소를 복구할 수 있습니다.

Single Copy Cluster

클러스터의 노드 간에 공유되는 저장소에서 저장소 그룹의 단일 복사본을 사용하는 공유 저장소 장애 조치 클러스터 솔루션입니다. 이것은 Exchange 2007에서 사용할 수 있는 두 가지 유형의 CMS(Clustered Mailbox Server) 배포 중 하나입니다.

Smart Agent

Rapid Recovery Smart Agent는 Rapid Recovery Core로 보호되는 시스템에 설치됩니다. Smart Agent는 디스크 볼륨에서 변경된 블록을 추적하고 미리 정의된 보호 간격으로 변경된 블록의 스냅숏을 작성합니다.

SQL 백업

SQL 백업은 시스템 오류 후 SQL Server에 해당 데이터를 복원 및 복구하는 데 사용되는 데이터 사본입니다. SQL 백업에서 전체 SQL 데이터베이스 또는 SQL 데이터베이스의 하나 이상의 구성 요소를 복구할 수 있습니다.

SQL 연결성

SQL 연결성은 Rapid Recovery Core 내에서 실행되는 테스트로, 모든 SQL 복구 지점에 오류가 없고 장애가 발생할 경우 백업을 위해 이러한 SQL 복구 지점을 모두 사용할 수 있도록 합니다.

SQL 차등 백업

차등 데이터베이스 백업은 SQL 데이터베이스의 마지막 전체 백업 이후 모든 데이터 변경사항의 누적 복사본입니다. 일반적으로 차등 백업은 전체 데이터베이스 백업을 만드는 것보다 더 빠르고, 데이터베이스를 복구하는 데 필요한 트랜잭션 로그 수를 줄입니다.

Transport Layer Security

TLS(Transport Layer Security)는 인터넷에서 통신을 보안하기 위해 설계된 최신 암호화 네트워크 프로토콜입니다. Internet Engineering Task Force에 의해 정의된 이 프로토콜은 SSL(Secure Sockets Layer)의 후속 프로토콜입니다. SSL 용어가 일반적으로 계속 사용되며, 프로토콜을 모두 사용할 수 있습니다(TLS 클라이언트가 SSL 서버와 통신하기 위해 다운그레이드할 수 있음).

True Scale

True Scale은 Rapid Recovery의 확장형 아키텍처입니다.

Universal Recovery

Rapid Recovery Universal Recovery 기술은 무제한의 시스템 복원 유연성을 제공합니다. 이 기술을 사용하여 선택한 물리적 또는 플랫폼 간에 획일적인 복구를 수행할 뿐만 아니라 물리적 또는 가상 원본에서 가상 시스템에 증분 복구 업데이트를 수행할 수 있습니다. 또한 이 기술을 통해 개별 파일, 폴더, 이메일, 달력 항목, 데이터베이스 및 응용프로그램의 응용프로그램 수준, 항목 수준 및 객체 수준 복구를 수행할 수 있습니다.

Verified Recovery

Verified Recovery 기술은 백업의 자동 복구 테스트 및 확인을 수행하는 데 사용됩니다. 이 기술은 다양한 파일 시스템 및 서버를 지원합니다.

Windows 장애 조치 클러스터

응용 프로그램 및 서비스의 가용성을 증가시키기 위해 함께 작동하는 독립적 컴퓨터 그룹입니다. 클러스터된 서버(노드라고 함)는 실제 케이블과 소프트웨어로 연결됩니다. 클러스터 노드 중 하나가 실패할 경우 다른 노드가 서비스를 제공하기 시작합니다(장애 조치로 알려진 프로세스). 따라서 서비스 중단이 최소화됩니다. Rapid Recovery에서는 다양한 SQL Server 및 Exchange Server 클러스터 유형의 보호를 지원합니다.

가상 대기

가상 대기는 보호된 시스템의 클론 가상 시스템을 만드는 프로세스입니다. 기존 소스 시스템은 실제 또는 가상 시스템이 가능하지만 제품은 항상 가상 시스템입니다. 한 번 주문으로 가상 대기를 만들거나 부팅 가능한 VM을 만들기 위한 요구 사항을 정의할 수 있으며, 보호된 기존 시스템에서 각 스냅숏이 캡처된 후에 계속 업데이트할 수 있습니다.

객체 파일 시스템

Rapid Recovery 확장형 객체 저장소는 객체 파일 시스템 구성 요소입니다. 이것은 스냅숏이 파생되는 모든 데이터 블록을 객체로 처리하고, 해당 객체를 저장하고 검색 및 유지관리하고 복제합니다. 객체 파일 시스템은 글로벌 데이터 중복 제거, 암호화 및 보존 관리와 함께 확장형 입력 및 출력(I/O) 성능을 제공하도록 설계되었습니다. 객체 파일 시스템은 업계 표준 저장소 기술과 호환됩니다.

관리 역할

Rapid Recovery Central Management Console은 신뢰할 수 있는 데이터 및 서비스 관리자들 간에 관리 책임을 분배할 수 있는 새로운 개념의 관리 역할뿐만 아니라 보안되고 효율적인 관리 위임을 지원하는 액세스 제어도 소개합니다.

금지된 구

금지된 구는 운영 체제 사용을 위해 예약되었기 때문에 Rapid Recovery Core Console에서 객체 이름으로 사용하면 안 되는 구(또는 문자 집합)입니다. 가능하면 이러한 구를 사용하지 않는 것이 가장 좋습니다. 예를 들어, 보호된 시스템에 대한 표시 이름을 정의할 때 다음 구를 사용하지 마십시오.

표 319. 금지된 구

구	일반적인 사용	금지 위치
con	콘솔	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
prn	프린터 포트	시스템 표시 이름, 암호화 키
aux	보조 포트	시스템 표시 이름, 암호화 키
nul	null 값	시스템 표시 이름, 암호화 키
com1, com2... Com9*까지*	통신 포트	시스템 표시 이름, 암호화 키
lpt1, lpt2... lpt9 *까지*	라인 인쇄 터미널 포트	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명

금지된 문자

금지된 문자는 Rapid Recovery Core Console에서 객체의 이름을 지정할 때 사용하면 안 되는 문자입니다. 예를 들어, 보호된 시스템에 대한 표시 이름을 정의할 때 다음 특수 문자를 사용하지 마십시오.

표 320. 금지된 문자

문자	문자 이름	금지 위치
?	물음표	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
|	파이프	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명

문자	문자 이름	금지 위치
:	콜론	시스템 표시 이름, 암호화 키, 리포지토리 경로를 지정할 때 이 기호를 사용할 수 있습니다(예: **c:\data**).
/	슬래시	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
\	백슬래시	시스템 표시 이름, 암호화 키, 리포지토리 로컬 또는 네트워크 경로를 지정할 때 이 기호를 사용할 수 있습니다(예: **c:\data** 또는 **\\ComputerName\SharedFolder**).
*	별표	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
“	따옴표	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
<	여는 꺾쇠 괄호	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명
>	닫는 꺾쇠 괄호	시스템 표시 이름, 암호화 키, 리포지토리, 경로 설명

기본 이미지

Core에 저장된 최초 백업 전송을 기본 이미지 스냅숏이라고 합니다. 지정된 모든 볼륨의 모든 데이터(운영 체제, 응용프로그램, 설정 포함)는 Core에 저장됩니다. 자세한 내용은 스냅숏을 참조하십시오.

대상 Core

때때로 복제 Core라고도 하는 대상 Core는 소스 Core에서 복제된 데이터를 수신하는 Rapid Recovery Core입니다.

라이센스 키

라이센스 키는 Rapid Recovery 소프트웨어 또는 어플라이언스를 등록하는 데 사용하는 한 가지 방법입니다. (라이센스 파일을 사용할 수도 있습니다.) 계정에 맞게 Dell Data Protection | Rapid Recovery License Portal에서 등록할 때 라이센스 키 또는 파일을 얻을 수 있습니다. 자세한 내용은 License Portal을 참조하십시오.

로그 잘라내기

로그 잘라내기는 트랜잭션 로그에서 로그 레코드를 제거하는 기능입니다. SQL Server 시스템의 경우 SQL Server 로그 잘라내기를 수행할 때 이 프로세스는 SQL Server에서 여유 공간을 식별합니다. Exchange Server 시스템의 경우 Exchange Server 로그 잘라내기를 수행할 때 이 작업은 Exchange Server에서 사용 가능한 공간을 늘립니다.

롤업

롤업 프로세스는 과거 복구 지점을 축소 및 제거하여 보존 정책을 적용하는 내부의 야간 유지관리 절차입니다. Rapid Recovery에서는 롤업을 메타데이터 작업으로만 줄입니다.

리포지토리

리포지토리는 기본 이미지 컬렉션이며 Rapid Recovery Core의 보호된 시스템에서 캡처된 증분 스냅숏입니다. 리포지토리는 빠른 기본 저장소 장치에 저장해야 합니다. DVM 리포지토리의 저장소 위치는 Core 시스템에 대한 로컬일 수 있습니다(지원되는 Windows 운영 체제에서 호스팅되는 경우만 해당). 직접 연결 저장소, 저장소 영역 네트워크 또는 적절하게 관련된 네트워크 연결 서버를 사용할 수 있습니다.

마운트 가능성

Exchange 마운트 가능성은 관리자에게 잠재적 실패를 경고하고, 장애 발생 시 Exchange Server의 모든 데이터를 성공적으로 복구하는 손상 탐지 기능입니다.

보존

보존은 Rapid Recovery Core에 보호된 시스템의 백업 스냅숏이 저장되는 기간을 정의합니다. 보존 정책은 롤업 프로세스를 통해 복구 지점에서 수행됩니다.

보호된 시스템

"에이전트"라고도 하는 보호된 시스템은 Rapid Recovery Core에서 보호하는 실제 컴퓨터 또는 가상 시스템입니다. Core에서 미리 정의된 보호 간격을 사용하여 보호된 시스템에서 리포지토리로 백업 데이터가 전송됩니다. 기본 이미지가 복구 지점(운영 체제, 응용 프로그램 및 설정 포함)으로 모든 데이터를 전송합니다. 이후의 각 증분 스냅숏은 보호된 시스템의 지정된 디스크 볼륨에서 변경된 블록만 적용됩니다. 소프트웨어 기반 보호된 시스템에는 Rapid Recovery Agent 소프트웨어가 설치되어 있습니다. 또한 일부 가상 시스템도 몇 가지 제한 사항이 있지만 에이전트 없이 보호될 수 있습니다.

복구 지점

복구 지점은 다양한 디스크 볼륨의 스냅숏 모음입니다. 예: C:, D: 및 E:

복구 지점 전용 시스템

복구 지점 전용 시스템은 이전에 Core에서 보호되는 시스템의 복구 지점의 Core를 나타냈지만 이후에 제거되었습니다. 복제를 제거하지만 복구 지점은 유지하려는 경우 결과적으로 복구 지점 전용 시스템이 됩니다. 정보는 파일 수준에서 보고 복구할 수 있습니다. BMR을 수행하거나 전체 볼륨을 복원하기 위해 복구 지점 전용 시스템을 사용할 수 있으며 복구 지점 전용 시스템에 더 많은 데이터를 추가할 수도 없습니다.

복원

Rapid Recovery Core에 저장된 복구 지점에서 시스템에 있는 하나 이상의 저장소 볼륨을 복원하는 프로세스가 복원을 수행하는 작업으로 알려져 있습니다. 복원은 이전에 롤백으로 알려져 있었습니다.

복제

복제는 한 Rapid Recovery Core에서 복구 지점을 복사하고 재해 복구를 목적으로 다른 Rapid Recovery Core로 전송하는 프로세스입니다. 이 프로세스를 수행하려면 두 개 이상의 Core 간에 페어링된 소스-대상 관계가 설정되어야 합니다. 복제는 보호된 시스템을 기준으로 관리됩니다. 소스 Core에서 보호되거나 복제된 모든 시스템은 대상 Core로 복제되도록 구성할 수 있습니다. 이는 대상 Core에 복사되는 복구 지점입니다.

볼륨 관리자

Rapid Recovery 볼륨 관리자는 객체를 관리한 다음 객체를 저장하고 논리적 볼륨으로 나타냅니다. 이것은 동적 파이프라인 아키텍처를 활용하여 I/O 대기 시간을 최소화하고 처리 속도를 개선하기 위해 TruScale 확장성, 병렬화 및 비동기식 입출력(I/O) 모델을 제공합니다.

서버 클러스터

Windows 장애 조치 클러스터를 참조하십시오.

스냅숏

스냅숏은 응용프로그램이 실행되고 있는 동안 지정된 지점에서 디스크 볼륨의 상태를 캡처 및 저장하는 기능을 정의하는 일반 산업 용어입니다. 스냅숏은 정전 또는 시스템 장애로 인해 시스템 복구가 필요한 경우 중요합니다. Rapid Recovery 스냅숏은 응용프로그램 인식형으로, 열려있는 모든 트랜잭션 및 롤링 트랜잭션 로그가 완료되고 스냅숏을 만들기 전에 캐시가 플러시됨을 의미합니다. Rapid Recovery는 Microsoft VSS(볼륨 섀도 서비스)를 사용하여 응용 프로그램 크래쉬에 대비한 백업 스냅숏 작성(application crash consistent snapshots)을 수행합니다.

시딩

복제에서 처음에는 보호된 에이전트의 중복 제거된 기본 이미지 및 증분 스냅숏을 전송하고 수백 또는 수천 기가바이트의 데이터까지 추가할 수 있습니다. 초기 복제는 외부 미디어를 사용하여 대상 Core에 시딩할 수 있으므로, 대규모 데이터 집합 또는 느린 링크를 포함하는 사이트에 유용합니다.

암호

암호는 데이터 암호화에 사용된 키입니다. 암호를 분실하면 데이터를 복구할 수 없습니다.

암호화

데이터는 해당 암호 해독 키를 가지는 인증된 사용자만 액세스할 수 있도록 암호화되었습니다. 데이터는 CBC(Cipher Block Chaining) 모드에서 256-bit AES를 사용하여 암호화됩니다. CBC에서 각 데이터 블록은 암호화되기 전에 이전 암호 텍스트 블록으로 XOR화되므로, 각 새 암호 텍스트 블록은 모든 선행 일반 텍스트 블록에 따라 달라집니다. 암호는 초기화 벡터로 사용됩니다.

압축

SNIA(Storage Networking Industry Association)는 데이터를 인코딩하여 데이터의 크기를 줄이는 프로세스로 압축을 정의합니다.

원격 Core

원격 Core는 Local Mount Utility 또는 Central Management Console을 사용하여 Core가 아닌 시스템이 액세스하는 Rapid Recovery를 나타냅니다.

이벤트

이벤트는 Core에서 로그하는 프로세스입니다. 아이콘 표시줄에서 (이벤트) 아이콘을 클릭하면 Core Console에서 이벤트를 볼 수 있습니다. (이벤트) 아이콘을 클릭할 때 기본 보기는 **작업** 페이지입니다. 이 보기에서는 작업과 관련된 이벤트를 표시합니다. 알림을 받은 이벤트 우선 순위는 **경고** 페이지에서 볼 수 있습니다. 모든 이벤트 로그가 **저널** 페이지에 나타납니다. 기존 알림 그룹을 설정하거나 수정하여 이벤트에 대한 알림을 사용자 지정할 수 있습니다. 이 과정을 통해 **경고** 페이지에 표시하여 이벤트 우선 순위를 나타낼 수 있습니다. 알림 그룹의 구성원은 그룹의 알림 옵션에 설정된 알림 방법을 사용하여 이벤트에 대한 알림을 받게 됩니다.

증분 스냅숏

증분 스냅숏은 마지막 백업 이후 보호된 컴퓨터에서 변경된 데이터로만 구성된 백업입니다. 증분 스냅숏은 정기적으로 정의된 간격에 따라(예: 60분마다) Core에 저장됩니다. 자세한 내용은 스냅숏을 참조하십시오.

체크섬

체크섬은 전송 또는 저장 도중 발생한 우발적인 오류를 탐지하기 위해 사용되는 데이터 블록을 만드는 기능입니다.

쿼럼

장애 조치 클러스터의 경우 지정된 클러스터가 실행을 계속하려면 온라인 상태여야 하는 요소 수입니다. 이 맥락에서 관련된 요소는 클러스터 노드입니다. 또한 이 용어는 클러스터를 복구하는 데 필요한 구성 데이터를 유지관리하기 위해 선택된 쿼럼 지원 리소스를 나타낼 수 있습니다. 이 데이터는 클러스터 데이터베이스에 적용된 모든 변경 사항의 세부정보를 포함합니다. 일반적으로 쿼럼 리소스는 다른 클러스터 리소스에 액세스하여 모든 클러스터 노드 또는 최신 데이터베이스 변경 사항에 액세스할 수 있도록 합니다. 기본적으로 서버 클러스터당 쿼럼 리소스는 하나만 있습니다. 특정 쿼럼 구성(장애 조치 클러스터에 대한 설정)으로 너무 많은 오류가 발생하여 클러스터가 실행을 중지하는 지점이 결정됩니다.

클러스터

Windows 장애 조치 클러스터를 참조하십시오.

클러스터 노드

Windows 장애 조치 클러스터에 속하는 개별 시스템입니다.

화이트 레이블링

Rapid Recovery에서는 백업 및 재해 복구 서비스 공급자가 자신의 ID로 Rapid Recovery에 화이트 레이블링 또는 리브랜딩한 다음 판매하거나 자신의 제품 또는 서비스로 분배할 수 있습니다.