

# Dell DL4300 어플라이언스 사용 설명서



# 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.

**Copyright © 2015 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.

2015 - 12

개정 A01

# 목차

<b>1 Dell DL4300 어플라이언스 소개.....</b>	<b>10</b>
핵심 기술.....	10
라이브 복구.....	11
검증된 복구.....	11
범용 복구.....	11
트루 글로벌 중복 제거.....	11
True Scale 아키텍처.....	11
배포 아키텍처.....	12
스마트 에이전트.....	13
DL4300 Core.....	14
스냅샷 프로세스.....	14
재난 복구 사이트 또는 서비스 공급자 복제.....	14
복구.....	15
제품 기능 .....	15
리포지토리.....	15
트루 글로벌 중복 제거 .....	16
암호화.....	17
복제.....	17
RaaS(Recovery-as-a-Service).....	18
보존 및 아카이빙.....	18
가상화 및 클라우드.....	19
경고 및 이벤트 관리.....	20
라이센스 포털.....	20
웹 콘솔.....	20
서비스 관리 API.....	20
<b>2 DL4300 Core 작업.....</b>	<b>21</b>
DL4300 Core 콘솔 액세스.....	21
Internet Explorer에서 신뢰할 수 있는 사이트 업데이트.....	21
Core 콘솔에 원격으로 액세스하도록 브라우저 구성.....	21
Core 구성을 위한 로드맵 .....	23
라이센스 관리 .....	23
라이센스 키 변경 .....	23
라이센스 포털 서버 연결 .....	23
수동으로 AppAssure 언어 변경.....	24
설치하는 동안 OS 언어 변경.....	24
Core 설정 관리 .....	25

Core 표시 이름 변경 .....	25
야간 작업 시간 조정 .....	25
전송 큐 설정 수정 .....	26
클라이언트 시간 제한 설정 조정 .....	26
중복 제거 캐시 설정 구성 .....	26
엔진 설정 수정 .....	27
데이터베이스 연결 설정 수정 .....	28
리포지토리 정보 .....	28
리포지토리 관리를 위한 로드맵 .....	29
리포지토리 생성 .....	29
리포지토리 상세정보 보기 .....	32
리포지토리 설정 수정 .....	32
기존 리포지토리 확장 .....	33
기존 리포지토리에 저장소 위치 추가 .....	33
리포지토리 검사 .....	35
리포지토리 삭제 .....	35
볼륨 다시 탑재 .....	35
리포지토리 복구 .....	36
보안 관리 .....	36
암호화 키 추가 .....	36
암호화 키 편집 .....	37
암호화 키 암호 변경 .....	37
암호화 키 가져오기 .....	37
암호화 키 내보내기 .....	38
암호화 키 제거 .....	38
클라우드 계정 관리 .....	38
클라우드 계정 추가 .....	38
클라우드 계정 편집 .....	40
클라우드 계정 설정 구성 .....	40
복제 이해 .....	41
워크스테이션 및 서버 보호 정보 .....	41
복제 정보 .....	41
시드 정보 .....	42
장애 조치 및 장애 복구 정보 .....	43
복제 및 암호화된 복구 지점 정보 .....	43
복제에 대한 보존 정책 정보 .....	43
복제된 데이터 전송에 대한 성능 고려 사항 .....	44
복제 수행을 위한 로드맵 .....	44
자체 관리 Core에 복제 .....	45
타사 관리 Core에 복제 .....	48
복제 모니터링 .....	51
복제 설정 관리 .....	52



복제 제거 .....	52
소스 Core의 복제에서 보호되는 시스템 제거.....	53
대상 Core에서 보호되는 시스템 제거.....	53
복제에서 대상 Core 제거.....	53
복제에서 소스 Core 제거.....	53
복제된 데이터 복구 .....	54
장애 조치 및 장애 복구의 로드맵 .....	54
장애 조치에 대한 환경 설정 .....	54
대상 Core의 장애 조치 수행 .....	55
장애 복구 수행 .....	55
이벤트 관리 .....	56
알림 그룹 구성 .....	57
전자 메일 서버 및 전자 메일 알림 템플릿 구성 .....	58
반복 감소 구성 .....	59
이벤트 보존 구성 .....	59
복구 관리 .....	60
시스템 정보 .....	60
시스템 정보 보기 .....	60
설치 관리자 다운로드 .....	60
에이전트 설치 관리자 정보 .....	60
에이전트 설치 관리자 다운로드 및 설치 .....	61
Local Mount 유틸리티 정보 .....	61
Local Mount 유틸리티 다운로드 및 설치 .....	61
Local Mount 유틸리티에 Core 추가 .....	62
Local Mount 유틸리티를 사용하여 복구 지점 탐색 .....	63
Local Mount 유틸리티를 사용하여 복구 지점 분리 .....	64
Local Mount 유틸리티 트레이 메뉴 정보 .....	64
Core 및 에이전트 옵션 사용.....	65
보존 정책 관리 .....	65
클라우드에 아카이브.....	65
아카이빙 정보 .....	66
아카이브 생성 .....	66
예약된 아카이브 설정 .....	67
예약된 아카이브 일시 중지 또는 재개 .....	68
예약된 아카이브 편집 .....	68
아카이브 확인 .....	69
아카이브 가져오기 .....	70
SQL 연결 기능 관리 .....	70
SQL 연결 기능 설정 구성 .....	71
야간 SQL 연결 기능 검사 및 로그 자르기 구성 .....	72
Exchange 데이터베이스 탐색 기능 검사 및 로그 자르기 관리 .....	72
Exchange 데이터베이스 탐색 기능 및 로그 자르기 구성 .....	72

탐재 기능 검사 강제 적용 .....	73
체크섬 검사 강제 적용 .....	73
로그 자르기 강제 적용 .....	73
복구 지점 상태 표시기 .....	73
<b>3 어플라이언스 관리.....</b>	<b>75</b>
어플라이언스 상태 모니터링.....	75
저장소 프로비저닝.....	75
선택한 저장소 프로비저닝.....	76
가상 디스크의 공간 할당 삭제.....	77
실패한 작업 해결.....	77
어플라이언스 업그레이드.....	77
어플라이언스 복구.....	78
<b>4 워크스테이션 및 서버 보호.....</b>	<b>79</b>
워크스테이션 및 서버 보호 정보 .....	79
시스템 설정 구성 .....	79
구성 설정 보기 및 수정 .....	79
시스템의 시스템 정보 보기 .....	80
시스템 이벤트에 대한 알림 그룹 구성 .....	80
시스템 이벤트에 대한 알림 그룹 편집 .....	82
보존 정책 설정 사용자 지정 .....	84
라이선스 정보 보기 .....	86
보호 일정 수정 .....	86
전송 설정 수정 .....	87
서비스 다시 시작 .....	89
시스템 로그 보기 .....	89
시스템 보호 .....	90
에이전트를 보호할 때 Agent 소프트웨어 배포.....	91
볼륨에 대한 사용자 지정 일정 생성 .....	92
Exchange Server 설정 수정 .....	93
SQL Server 설정 수정 .....	94
에이전트 배포(강제 설치) .....	94
새 에이전트 복제 .....	95
시스템 관리 .....	96
시스템 제거 .....	96
시스템에서 에이전트 데이터 복제 .....	96
에이전트에 대한 복제 우선순위 설정 .....	97
시스템에서 작업 취소 .....	97
시스템 상태 및 기타 상세정보 보기 .....	97
다중 시스템 관리 .....	98
다중 시스템에 배포 .....	99

다중 시스템의 배포 모니터링 .....	103
다중 시스템 보호 .....	103
다중 시스템의 보호 모니터링 .....	104
스냅샷 및 복구 지점 관리 .....	105
복구 지점 보기 .....	105
특정 복구 지점 보기.....	106
Windows 시스템의 복구 지점 탑재 .....	106
선택 복구 지점 분리.....	107
모든 복구 지점 분리.....	107
Linux 시스템의 복구 지점 볼륨 탑재 .....	108
복구 지점 제거 .....	108
분리된 복구 지점망 삭제.....	109
스냅샷 강제 적용 .....	109
보호 일시 중지 및 다시 시작 .....	110
데이터 복원 .....	110
백업.....	110
Windows 시스템에서 가상 시스템으로 보호 데이터 내보내기 정보.....	112
Microsoft Windows 시스템에서 가상 시스템으로 백업 정보 내보내기 .....	113
ESXi 내보내기를 사용하여 Windows 데이터 내보내기 .....	113
VMware 워크스테이션 내보내기를 사용하여 Windows 데이터 내보내기 .....	115
Hyper-V 내보내기를 사용하여 Windows 데이터 내보내기 .....	117
Oracle VirtualBox 내보내기를 사용하여 Microsoft Windows 데이터 내보내기 .....	120
가상 시스템 관리.....	123
롤백 수행 .....	126
명령행을 사용하여 Linux 시스템에 롤백 수행.....	127
Windows 시스템의 운영 체제 미설치 복원 정보 .....	128
Windows 시스템의 운영 체제 미설치 복원 수행을 위한 필수 구성 요소 .....	129
Windows 시스템의 운영 체제 미설치 복원 수행을 위한 로드맵 .....	129
부팅 가능 CD ISO 이미지 생성.....	129
부팅 CD 로드.....	131
Core에서 복원 실행 .....	132
볼륨 매핑 .....	132
복구 진행률 보기 .....	133
복원된 대상 서버 시작 .....	133
시작 문제 복구.....	134
Linux 시스템의 운영 체제 미설치 복원 수행 .....	134
Screen Utility 설치.....	135
Linux 시스템에서 부팅 가능한 파티션 생성.....	135
이벤트 및 경고 보기 .....	136

## 5 서버 클러스터 보호.....137

서버 클러스터 보호 정보 .....	137
---------------------	-----

지원되는 응용프로그램 및 클러스터 유형 .....	137
클러스터 보호 .....	138
클러스터의 노드 보호 .....	139
클러스터 노드 설정 수정 프로세스 .....	140
클러스터 설정 구성을 위한 로드맵 .....	140
클러스터 설정 수정 .....	141
클러스터 이벤트 알림 구성 .....	141
클러스터 보존 정책 수정 .....	142
클러스터 보호 일정 수정 .....	143
클러스터 전송 설정 수정 .....	143
보호된 클러스터 노드를 에이전트로 변환 .....	144
서버 클러스터 정보 보기 .....	144
클러스터 시스템 정보 보기 .....	144
요약 정보 보기 .....	145
클러스터 복구 지점 작업 .....	145
클러스터에 대한 스냅샷 관리 .....	145
클러스터에 대한 스냅샷 강제 적용 .....	146
클러스터 스냅샷 일시 중지 및 다시 시작 .....	146
로컬 복구 지점 분리 .....	146
클러스터 및 클러스터 노드에 대한 롤백 수행 .....	146
CCR(Exchange) 및 Dag 클러스터에 대한 롤백 수행 .....	147
SCC(Exchange, SQL) 클러스터에 대한 롤백 수행 .....	147
클러스터 데이터 복제 .....	147
클러스터 보호 제거 .....	147
클러스터 노드 보호 제거 .....	148
클러스터의 모든 노드 보호 제거 .....	148
클러스터 또는 노드 보고서 보기 .....	148
<b>6 보고 .....</b>	<b>150</b>
보고서 정보 .....	150
보고서 도구 모음 정보 .....	150
호환성 보고서 정보 .....	150
오류 보고서 정보 .....	151
Core 요약 보고서 정보 .....	151
리포지토리 요약 .....	151
에이전트 요약 .....	152
Core 또는 에이전트에 대한 보고서 생성 .....	152
중앙 관리 콘솔 Core 보고서 정보 .....	153
중앙 관리 콘솔에서 보고서 생성 .....	153
<b>7 DL4300 어플라이언스 전체 복구 완료 .....</b>	<b>154</b>
운영 체제에 대한 RAID 1 파티션 생성 .....	154

운영 체제 설치.....	155
복구 및 업데이트 유틸리티 실행.....	155
<b>8 호스트 이름을 수동으로 변경.....</b>	<b>157</b>
Core 서비스 중지.....	157
서버 인증서 삭제.....	157
Core 서버 및 레지스트리 키 삭제.....	157
새 호스트 이름을 사용하여 Core 실행.....	158
표시 이름 변경 .....	158
Internet Explorer에서 신뢰할 수 있는 사이트 업데이트.....	158
<b>9 부록 A - 스크립팅.....</b>	<b>159</b>
Powershell 스크립팅 정보 .....	159
Powershell 스크립팅 필수 구성 요소 .....	159
스크립트 검사 .....	159
입력 매개변수 .....	160
VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage) .....	164
Pretransferscript.ps1 .....	165
Posttransferscript.ps1 .....	165
Preexportscript.ps1 .....	166
Postexportscript.ps1 .....	167
Prenightlyjobscript.ps1 .....	167
Postnightlyjobscript.ps1.....	169
샘플 스크립트 .....	171
<b>10 도움말 얻기.....</b>	<b>172</b>
설명서 및 소프트웨어 업데이트 찾기.....	172
Dell에 문의하기.....	172

## Dell DL4300 어플라이언스 소개

이 장에서는 DL4300\에 대한 소개 및 개요를 제공합니다. 또한, 특징, 기능 및 아키텍처에 대해 설명하며, 다음 항목으로 구성되어 있습니다.

- [핵심 기술](#)
- [True Scale 아키텍처](#)
- [배포 아키텍처](#)
- [제품 기능](#)

가상 시스템(VM), 실제 시스템 및 클라우드 환경을 보호하기 위해 가장 빠르고 신뢰할 수 있는 백업을 수행할 수 있도록 고안된 어플라이언스는 백업, 복제 및 복구를 하나의 솔루션으로 결합함으로써 통합 데이터 보호에 대한 새로운 표준을 수립합니다.

어플라이언스가 모든 개인 또는 공용 클라우드 인프라에 대해 내장된 글로벌 중복 제거, 압축, 암호화 및 복제 기능을 통해 최대 페타바이트 용량의 데이터를 처리할 수 있습니다. 따라서 데이터 보존(DR) 및 호환성을 위해 서버 응용프로그램과 데이터를 몇 분 안에 복구할 수 있습니다.

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

어플라이언스에는 다음과 같은 기술이 결합되어 있습니다.

- [라이브 복구](#)
- [검증된 복구](#)
- [범용 복구](#)
- [트루 글로벌 중복 제거](#)

이러한 기술은 클라우드 재난 복구에 대한 안전한 통합을 통해 구축되며 빠르고 신뢰할 수 있는 복구를 제공합니다. 확장 가능한 개체 저장소가 포함된 어플라이언스에서 모든 개인 또는 공용 클라우드 인프라에 대해 내장된 글로벌 중복 제거, 압축, 암호화 및 복제 기능을 통해 최대 페타바이트 용량의 데이터를 매우 빠르게 처리할 수 있습니다.

개인 및 공용 클라우드가 모두 구성되어 있는 AppAssure는 VMware vSphere 및 Microsoft Hyper-V에서 실행되는 기능을 포함하여 여러 하이퍼바이저 환경의 지원과 핵심 기술을 통해 기존 도구의 복잡성과 비효율성을 해결합니다. AppAssure를 사용하면 IT 관리 및 저장 비용을 크게 줄이면서 이러한 기술을 발전시킬 수 있습니다.

## 핵심 기술

다음 항목에 AppAssure의 핵심 기술에 대해 자세히 설명되어 있습니다.

## 라이브 복구

라이브 복구는 VM 또는 서버에 대한 즉시 복구 기술입니다. 이를 통해 가상 또는 실제 서버의 데이터 볼륨에 거의 지속적으로 액세스할 수 있습니다. 0에 가까운 RTO 및 RPO로 전체 볼륨을 복구할 수 있습니다.

백업 및 복제 기술이 다중 VM 또는 서버의 동시 스냅샷 수를 기록하며, 거의 즉시 데이터와 시스템을 보호합니다. 프로덕션 저장소가 완전히 복원될 때까지 기다리지 않고 백업 파일에서 직접 서버 사용을 다시 시작할 수 있습니다. 사용자의 생산성이 유지되고 갈수록 더욱 엄격해지는 복구 시간 목표(RTO) 및 복구 지점 목표(RPO) 서비스 수준 계약에 맞게 IT 부서의 복구 시간이 감소됩니다.

## 검증된 복구

검증된 복구를 사용하면 자동 복구 검사 및 백업 확인을 수행할 수 있습니다. 대상에는 파일 시스템인 Microsoft Exchange 2007, 2010, 2013 및 여러 버전의 Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014가 포함되지만 이에 제한되지는 않습니다. 검증된 복구에서는 가상 및 실제 환경에서 응용프로그램 및 백업을 복구하고 보관, 복제 및 데이터 시드 작업을 수행하는 동안 백업에서 각 디스크 블록의 정확성을 검사하는 256비트 SHA 키를 기반으로 하는 포괄적인 무결성 검사 알고리즘을 사용합니다. 이를 통해 데이터 손상을 쉽게 식별하고 백업 과정에서 손상된 데이터 블록이 유지되거나 전송되지 않도록 방지할 수 있습니다.

## 범용 복구

범용 복구 기술을 사용하면 시스템을 무제한으로 유연하게 복원할 수 있습니다. 백업을 실제 시스템에서 가상 시스템, 가상 시스템에서 가상 시스템, 가상 시스템에서 실제 시스템 또는 실제 시스템에서 실제 시스템으로 복원하고 다른 하드웨어에 운영 체제 미설치 복원을 수행할 수 있습니다(예: P2V, V2V, V2P, P2P, P2C, V2C, C2P 및 C2V).

또한 범용 복구 기술을 통해 여러 가상 시스템에서 플랫폼 간 이동을 가속화할 수 있습니다. 예를 들어, VMware에서 Hyper-V로 이동하거나 Hyper-V에서 VMware로 이동합니다. 이는 응용프로그램 수준, 항목 수준 및 개체 수준 복구에서 빌드됩니다(파일, 폴더, 전자 메일, 일정 항목, 데이터베이스 및 응용프로그램 포함). AppAssure를 사용하면 실제에서 클라우드 또는 가상에서 클라우드로 복구하거나 내보낼 수 있습니다.

## 트루 글로벌 중복 제거

어플라이언스에서는 데이터 저장소 요구 사항을 충족하면서 50:1을 넘는 공간 축소율을 제공하여 실제 디스크 드라이브 용량 요구 사항을 동적으로 줄이는 트루 글로벌 중복 제거 기능을 제공합니다. 기본 제공 무결성 검사와 함께 회선 속도 성능과 블록 수준 압축 및 중복 제거 기능을 긴밀하게 연결하는 AppAssure True Scale은 데이터 손상으로 인해 백업 품질과 보관 프로세스에 영향을 미치지 않도록 방지합니다.

## True Scale 아키텍처

어플라이언스는 AppAssure True Scale 아키텍처에 구축되어 있습니다. 이를 통해 엔터프라이즈 환경에 강력한 성능을 지속적으로 전달할 수 있도록 최적화된 동적 멀티 코어 파이프라인 아키텍처를 이용할 수 있습니다. True Scale은 연속적으로 확장되도록 완벽하게 설계되어 있어 대량의 데이터를 효율적으로 저장하고 관리하며 성능에 영향을 미치지 않으면서 단시간에 RTO 및 RPO를 전달할 수 있습니다. 이는 통합된 글로벌 중복 제거, 압축, 암호화, 복제 및 보존 기능과 함께 특별히 구축된 개체 및 볼륨 관리자로 구성되어 있습니다. 다음 다이어그램은 AppAssure True Scale 아키텍처에 대해 설명합니다.



그림 1 . AppAssure True Scale 아키텍처

AppAssure 볼륨 관리자 및 확장 가능한 개체 저장소가 AppAssure True Scale 아키텍처의 기초 역할을 수행합니다. 확장 가능한 개체 저장소에 가상 및 물리적 서버에서 수집한 블록 수준 스냅샷이 저장됩니다. 볼륨 관리자가 필요한 항목에 대해서만 일반 리포지토리 또는 시간 적절한 저장소를 제공하여 여러 개체 저장소를 관리합니다. 개체 저장소에서는 최소화된 대기 시간으로 높은 처리량을 제공하고 시스템 사용률을 최대화하는 동기식 I/O를 사용하는 모든 항목을 지속적으로 지원합니다. 리포지토리는 SAN(저장소 영역 네트워크), DAS(직접 연결 저장 장치) 또는 NAS(네트워크 연결 저장 장치)와 같은 여러 저장 기술에 적용됩니다.

AppAssure 볼륨 관리자의 역할은 운영 체제의 볼륨 관리자 역할과 유사합니다. 즉, 스트라이프 또는 순차적 할당 정책을 통해 여러 크기와 유형의 다양한 저장 장치를 사용하고 논리 볼륨에 결합합니다. 개체 저장소는 응용프로그램 인식 스냅샷이 제공하는 개체를 저장, 검색, 유지 보수 및 복제합니다. 볼륨 관리자는 글로벌 데이터 중복 제거, 암호화 및 보존 관리 기능과 함께 확장 가능한 I/O 성능을 제공합니다.

## 배포 아키텍처

어플라이언스는 기업 내에서는 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 AppAssure 에이전트 소프트웨어는 파일 서버, 전자 메일 서버, 데이터베이스 서버 등과 같은 시스템이나 가상 시스템에 설치되어 연결되고 중앙 리포지토리로 구성된 단일 Core를 통해 보호됩니다. 라이선스 포털에서는 사용자 환경에서 보호되는 시스템 및



Core의 라이선스 구독, 그룹 및 사용자를 관리합니다. 사용자 환경에 허용된 라이선스에 따라 라이선스 포털을 통해 사용자가 로그인, 계정 활성화, 소프트웨어 다운로드, 보호되는 시스템 및 Core 배포를 수행할 수 있습니다.

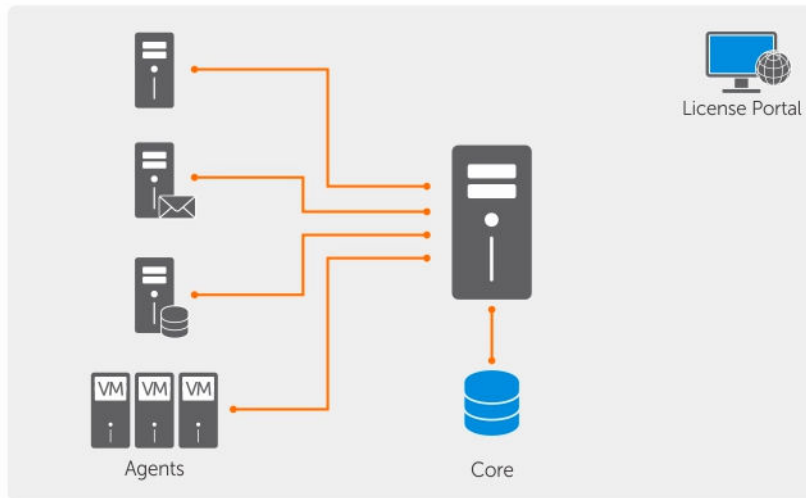


그림 2. 기본 배포 아키텍처

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

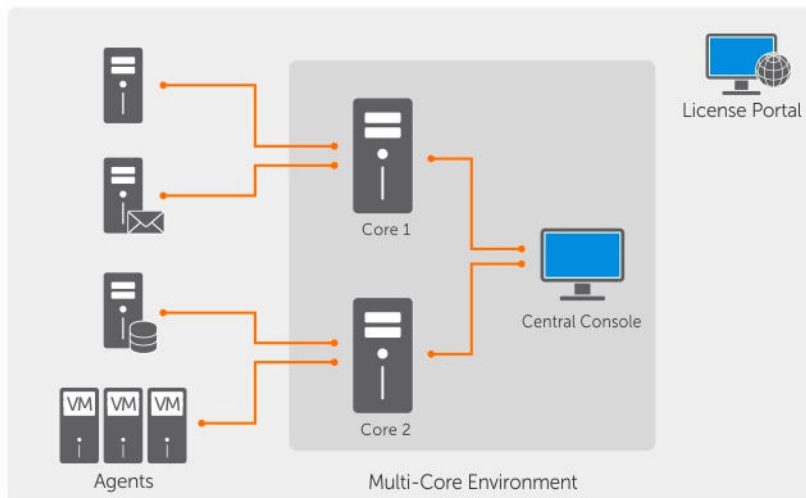


그림 3. 다중 코어 배포 아키텍처

## 스마트 에이전트

스마트 에이전트는 디스크 볼륨에서 변경된 블록을 추적하고 사전 정의된 보호 간격으로 변경된 블록의 이미지를 스냅합니다. 증분 블록 레벨 스냅샷의 영구 접근 방법이 보호된 시스템에서 Core로 동일한 데이터가 반복적으로 복사되지 않도록 합니다. 스마트 에이전트는 시스템에 설치되며, Core에 의해 보호됩니다.

스마트 에이전트는 응용프로그램 인식형이며, 사용하지 않을 때 CPU 사용률이 거의 0%이고 메모리 오버헤드가 20MB 미만인 상태로 유휴 상태가 됩니다. 스마트 에이전트가 활성화되면 Core에 스냅샷 전송을 포함하여 최대 2~4%의 프로세서 사용률과 150MB 미만의 메모리가 사용됩니다.

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. AppAssure 에이전트 소프트웨어가 구성되면 스마트 기술을 사용하여 보호된 디스크 볼륨에서 변경된 블록을 계속해서 추적합니다. 스냅샷이 준비되면 지능형 다중 스트레드 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.

## DL4300 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 버전의 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 전송되는 시점입니다. 이 경우에만 전체 시스템 사본이 정상적으로 작동하는 네트워크 간에 전송된 후 증분 스냅샷이 수행됩니다. Windows용 AppAssure 에이전트 소프트웨어에서는 Microsoft 볼륨 새도 복사본 서비스(VSS)를 사용해 응용프로그램 데이터를 동결하고 디스크에 수신 거부하여 파일-시스템 일치 및 응용프로그램 일치 백업을 수집합니다. 스냅샷이 생성되면 대상 서버의 VSS 기록기에서 콘텐츠가 디스크에 기록되지 않도록 방지합니다. 디스크에 콘텐츠 쓰기가 중지되면 모든 디스크 I/O 작업이 큐에 지정되고 스냅샷이 완료된 후에만 다시 시작됩니다. 반면에 이미 진행 중인 작업은 완료되고 열려 있는 모든 파일은 닫힙니다. 새도 복사본을 생성하는 프로세스는 프로덕션 시스템의 성능에 크게 영향을 미치지 않습니다.

AppAssure에서는 NTFS, 레지스트리 및 Active Directory 등과 같은 모든 Windows 내부 기술에 대한 지원이 내장되어 있으므로 Microsoft VSS를 사용하여 스냅샷 전에 데이터를 디스크에 플러시합니다. 또한 Microsoft Exchange 및 SQL과 같은 기타 엔터프라이즈 응용프로그램에서 VSS 기록기 플러그 인을 사용하여 스냅샷이 준비 중인 경우 및 일관된 트랜잭션 상태로 데이터베이스를 가져오기 위해 사용한 데이터베이스 페이지를 디스크에 플러시해야 하는 경우를 알려줍니다. VSS는 시스템 및 응용프로그램 데이터를 디스크에 정지하는 데 사용되지만 스냅샷을 생성할 때는 사용되지 않습니다. 캡처된 데이터는 즉시 전송되어 Core에 저장됩니다. 백업에 VSS를 사용해도 응용프로그램 서버가 오랫동안 백업 모드로 유지되지 않습니다. 스냅샷을 생성하는 데 걸리는 시간이 몇 시간 단위가 아닌 몇 초 단위이기 때문입니다. 백업에 VSS를 사용하는 또 다른 이점은 스냅샷이 볼륨 수준에서 작동되므로 AppAssure 에이전트 소프트웨어가 대규모 데이터의 스냅샷을 한 번에 만들 수 있다는 점입니다.

## 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 전

송합니다. 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](#)
- [트루 글로벌 중복 제거\(기능\)](#)
- [암호화](#)
- [복제](#)
- [RaaS\(Recovery-as-a-Service\)](#)
- [보존 및 아카이빙](#)
- [가상화 및 클라우드](#)
- [경고 및 이벤트 관리](#)
- [라이선스 포털](#)
- [웹 콘솔](#)
- [서비스 관리 API](#)

## 리포지토리

리포지토리에서는 DVM(중복 제거 볼륨 관리자)을 사용하여 각각 SAN(저장소 영역 네트워크), DAS(직접 연결 저장 장치), NAS(네트워크 연결 저장 장치) 또는 클라우드 저장소와 같이 서로 다른 저장소 기술에 있는 다중 볼륨에 대한 지원을 제공하는 볼륨 관리자를 구현합니다. 각 볼륨은 중복 제거 기능이 있는 확장 가능한 개체 저장소로 구성됩니다. 확장 가능한 개체 저장소는 레코드 기반 파일 시스템으로 작동하며, 이 때 저장소 할당 단위는 레코드라는 고정 크기 데이터 블록입니다. 이 아키텍처에서 압축 및 중복 제거를 위한 블록 크기 지원을 구성할 수 있습니다. 물업에서 더 이상 데이터를 이동하지 않고 레코드만 이동하므로 물업 작업이 디스크 집약 작업으로부터 메타데이터 작업으로 감소됩니다.

DVM이 개체 저장소 세트를 볼륨에 결합할 수 있으며, 추가 파일 시스템을 생성하여 확장할 수 있습니다. 개체 저장소 파일은 미리 할당되어 있으며 저장소 요구 사항이 변경되면 필요에 맞게 추가할 수 있습니다. 단일 Core에 최대 255개의 독립 리포지토리를 생성할 수 있으며, 새 파일 익스텐트를 추가하여 리포지토리의 크기를 더 늘릴 수 있습니다. 확장된 리포지토리에 서로 다른 저장소 기술에 적용되는 익스텐트를 최대 4,096개까지 포함할 수 있습니다. 리포지토리의 최대 크기는 32엑사바이트입니다. 하나의 Core에 여러 리포지토리가 있을 수 있습니다.

## 트루 글로벌 중복 제거

트루 글로벌 중복 제거는 중복되는 데이터를 제거함으로써 필요한 백업 저장소를 줄이는 효과적인 방법입니다. 여러 백업 간에 고유한 하나의 데이터 인스턴스만 리포지토리에 저장되므로 효율적으로 중복 제거됩니다. 중복되는 데이터는 저장되지만 실제로는 저장되지 않습니다. 즉, 리포지토리에 있는 하나의 고유한 데이터 인스턴스를 나타내는 포인터로 교체됩니다.

기존의 백업 응용프로그램은 매주 전체 백업을 반복적으로 수행했지만 어플라이언스는 시스템의 증분 블록 수준의 백업을 수행합니다. 데이터 중복 제거와 동시에 수행되는 이러한 영구적인 증분 방법은 디스크에 사용되는 총 데이터의 양을 대폭 줄이는 데 유용합니다.

서버의 일반적인 디스크 레이아웃은 운영 체제, 응용프로그램 및 데이터로 구성됩니다. 대부분의 환경에서, 관리자는 다중 시스템에서 효율적인 배포와 관리를 수행하기 위해 서버 및 데스크탑 운영 체제의 일반적인 옵션을 사용합니다. 다중 시스템에서 블록 수준의 백업을 동시에 수행하면 소스와 관계 없이 백업에 있는 항목과 백업에 없는 항목을 보다 세부적으로 확인할 수 있습니다. 이 데이터에는 운영 체제, 응용프로그램 및 해당 환경에 있는 응용프로그램 데이터가 포함됩니다.



그림 4. 중복 제거 다이어그램

어플라이언스는 대상 기반 인라인 데이터 중복 제거를 수행합니다. 즉, 중복을 제거하기 전에 스냅샷 데이터가 Core에 전송됩니다. 인라인 데이터 중복 제거는 단순히 데이터가 디스크에 사용되기 전에 중복 제거됨을 의미합니다. 이는 데이터를 저장하기 위해 대상에 전송되기 전에 소스에서 중복되는 원점 중복 제거 또는 데이터가 디스크에 사용된 후 분석되고 중복 제거되어 대상에 원시 상태로 전송되는 사후 처리 중복 제거와는 다릅니다. 원점 중복 제거는 시스템에서 매우 적은 시스템 리소스를 사용하지만, 사후 처리 데이터 중복 제거 방법을 수행하려면 중복 제거 프로세스를 시작하기 전에 디스크에 필수 데이터가 모두 있어야 합니다(초기 용량 오버헤드가 더 큼). 반면에, 인라인 데이터 중복 제거를 수행할 때에는 소스 또는 Core에 중복 제거 프로세스를 위한 추가 디스크 용량 및 CPU 주기가 필요하지 않습니다. 기존의 백업 응용프로그램에서는 매주 반복적으로 전체 백업을 수행하지만 어플라이언스는 시스템의 증분 블록 수준 백업을 영구적으로 수행합니다. 데이터 중복 제거 기능과 함께 이 영구적인 증분 방법을 동시에 사용하면 디스크에 사용되는 전체 데이터 양을 50:1만큼 크게 줄일 수 있습니다.

## 암호화

어플라이언스는 백업 및 비활성 데이터를 무단 액세스 및 무단 사용으로부터 보호하여 데이터의 기밀성을 보장하는 통합된 암호화 기능을 제공합니다. 암호화 키를 사용하는 사용자만 데이터에 액세스하여 암호를 해독할 수 있습니다. 암호화 키는 무제한으로 생성하여 시스템에 저장할 수 있습니다. DVM에서는 256비트 키에 CBC(Cipher Block Chaining) 모드로 AES 256비트 암호화를 사용합니다. 암호화는 성능에 영향을 미치지 않는 회선 속도로 스냅샷 데이터에 대해 즉시 수행됩니다. 이는 DVM 구현이 다중 스레드로 수행되고 배포된 프로세서에 고유한 하드웨어 가속 기능을 사용하기 때문입니다.

암호화는 다중 테넌트를 지원합니다. 특히 중복 제거 기능은 동일한 키로 암호화된 레코드로 제한되므로 서로 다른 키로 암호화된 두 개의 동일한 레코드는 서로 중복 제거되지 않습니다. 이러한 설계로 인해 중복 제거를 사용하여 서로 다른 암호화 도메인 간에 데이터를 유출할 수 없습니다. 이를 통해 관리 서비스 공급자에서 테넌트가 서로의 데이터를 보거나 액세스할 수 없도록 하면서 다중 테넌트(고객)의 백업을 단일 코어에 저장할 수 있습니다. 각 활성 테넌트 암호화 키가 키 소유자만 데이터를 보거나, 액세스하거나, 사용할 수 있는 리포지토리 내에 암호화 도메인을 생성합니다. 다중 테넌트 시나리오에서는 데이터가 암호화 도메인 내에서 파티션화되고 중복 제거됩니다.

복제 시나리오에서는 도청 및 악용을 방지하기 위해 어플라이언스가 SSL 3.0을 사용하여 복제 기술에서 두 Core 간의 연결을 보호합니다.

## 복제

복제는 AppAssure Core에서 복구 지점을 복사하고 재난 복구를 위해 별도의 위치에 있는 다른 AppAssure Core에 전송하는 프로세스입니다. 프로세스를 수행하려면 둘 이상의 Core 간에 소스-대상 쌍으로 지정된 관계가 필요합니다.

소스 Core는 선택한 보호되는 시스템의 복구 지점을 복사하고, 증분 스냅샷 데이터를 원격 재난 복구 사이트의 대상 Core에 비동기적으로 지속적으로 전송합니다. 회사 소유 데이터 센터 또는 원격 재난 복구 사이트(즉, 자체 관리 대상 Core)에 아웃바운드 복제를 구성할 수 있습니다. 또는 타사 관리 서비스 공급자(MSP)나 오픈사이트 백업 및 재난 복구 서비스를 호스팅하는 클라우드에 아웃바운드 복제를 구성할 수 있습니다. 복제할 때 연결을 요청하고 자동 피드백 알림을 받을 수 있는 기본 제공 워크플로를 사용할 수 있습니다.

복제는 보호되는 시스템에서 각각 관리됩니다. 소스 Core에서 보호되거나 복제되는 모든 시스템을 대상 Core에 복제하도록 구성할 수 있습니다.

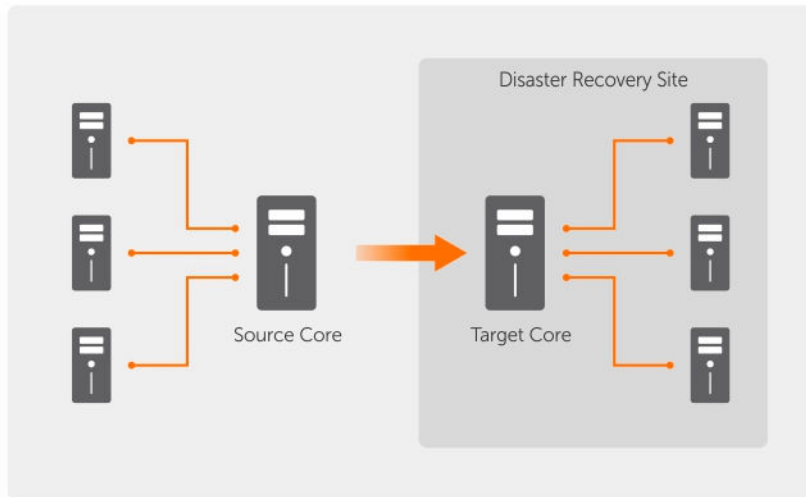


그림 5. 기본 복제 아키텍처

복제는 중복 제거 기능과 밀접하게 연관된 고유한 읽기-일치-쓰기(RMW) 알고리즘을 통해 자체적으로 최적화됩니다. RMW 복제를 사용하면 데이터를 전송하기 전에 소스와 대상 복제 서비스에서 키를 일치시킨 후 WAN 간에 압축, 암호화 및 중복 제거된 데이터만 복제합니다. 이를 통해 필요한 대역폭이 10배 감소됩니다.

복제는 중복 제거된 기본 이미지와 보호된 에이전트의 증분 스냅샷의 초기 전송인 시드를 통해 시작되며, 데이터를 수백 또는 수천 기가바이트까지 추가할 수 있습니다. 외부 미디어를 사용하여 초기 복제를 대상 Core에 시드할 수 있습니다. 이는 일반적으로 링크 속도가 느린 대규모 데이터 세트 또는 사이트에 유용합니다. 시드 아카이브의 데이터는 압축, 암호화 및 중복 제거됩니다. 아카이브의 전체 크기가 외부 미디어에서 사용 가능한 공간보다 큰 경우 아카이브가 여러 장치에 적용됩니다. 시드 과정에서 증분 복구 지점이 대상 사이트에 복제됩니다. 대상 Core에 데이터가 전송되면 새로 복제된 증분 복구 지점이 자동으로 동기화됩니다.

## RaaS(Recovery-as-a-Service)

관리 서비스 공급자(MSP)는 RaaS(Recovery-as-a-Service)를 제공하기 위한 플랫폼으로 어플라이언스를 최대한 활용할 수 있습니다. RaaS를 사용하면 복구 검사 또는 실제 복구 작업을 지원하기 위해 해당 데이터와 함께 고객의 실제 및 가상 서버를 서비스 공급자의 클라우드에 가상 시스템으로 복제하여 클라우드에서 복구를 쉽게 완료할 수 있습니다. 클라우드에서 복구를 수행하려는 고객은 AppAssure 서비스 공급자에 로컬 Core에 있는 보호되는 시스템에서 복제를 구성할 수 있습니다. 재난이 발생하면 MSP가 고객을 위해 가상 시스템을 즉시 스핀업할 수 있습니다.

MSP에서 일반적으로 단일 서버 또는 서버 그룹의 데이터 또는 보안을 공유하지 않는 다중 및 특정 조직이나 사업부(테넌트)를 호스트할 수 있는 다중 테넌트 AppAssure RaaS 인프라를 배포할 수 있습니다. 각 테넌트의 데이터는 다른 테넌트 및 서비스 공급자와 분리되고 보호됩니다.

## 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. 비즈니스에

서는 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.

**Custom Retention Policy**

☒ Enable Roll-up

Keep all Recovery Points for 3 Days ...

☒ ...and then keep one Recovery Point per hour for 3 Days ...

☒ ...and then keep one Recovery Point per day for 2 Days ...

☒ ...and then keep one Recovery Point per week for 4 Weeks ...

☒ ...and then keep one Recovery Point per month for 3 Months ...

☒ ...and then keep one Recovery Point per year for 1 Years ...

Newest Recovery Point: 5/16/2012

**Resulting Retention Period**

5/13/2012	5/10/2012	5/8/2012	4/10/2012	1/11/2012	1/11/2011
-----------	-----------	----------	-----------	-----------	-----------

Oldest Recovery Point will be 1 year, 4 months, 6 days old

그림 6. 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. 폭포수 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 라이선스를 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 이벤트에 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.

## 라이선스 포털

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



## DL4300 Core 작업

### DL4300 Core 콘솔 액세스

Core 콘솔에 액세스하려면 다음을 수행합니다.

1. 브라우저에서 신뢰할 수 있는 사이트를 업데이트 합니다. [Internet Explorer에서 신뢰할 수 있는 사이트 업데이트](#)를 참조하십시오.
2. Core 콘솔에 원격으로 액세스할 수 있도록 브라우저를 구성합니다. [Core 콘솔에 원격으로 액세스하도록 브라우저 구성](#)을 참조하십시오.
3. Core 콘솔에 액세스하려면 다음 중 하나를 수행하십시오.
  - DL4300 Core 서버에 로컬로 로그인하고 **Core Console(Core 콘솔)** 아이콘을 두 번 클릭합니다.
  - 웹 브라우저에 다음 URL 중 하나를 입력합니다.
    - `https://<yourCoreServerName>:8006/apprecovery/admin/core`
    - `https://<yourCoreServerIpAddress>:8006/apprecovery/admin/core`


### Internet Explorer에서 신뢰할 수 있는 사이트 업데이트


Microsoft Internet Explorer에서 신뢰할 수 있는 사이트를 업데이트하려면 다음을 수행하십시오.

1. Internet Explorer를 엽니다.
2. **File(파일)**, **Edit View(보기 편집)** 및 기타 메뉴가 표시되지 않으면 <F10> 키를 누릅니다.
3. **Tools(도구)** 메뉴를 클릭하고 **Internet Options(인터넷 옵션)**을 선택합니다.
4. **Internet Options(인터넷 옵션)** 창에서 **Security(보안)** 탭을 클릭합니다.
5. **Trusted Sites(신뢰할 수 있는 사이트)**를 클릭한 후 **Sites(사이트)**를 클릭합니다.
6. **Add this website to the zone(영역에 웹 사이트 추가)**에서 표시 이름으로 제공한 새 이름을 사용하여 `https://[Display Name]`을 입력합니다.
7. **Add(추가)**를 클릭합니다.
8. **Add this website to the zone(영역에 웹 사이트 추가)**에서 `about:blank`를 입력합니다.
9. **Add(추가)**를 클릭합니다.
10. **Close(닫기)**를 클릭한 후 **OK(확인)**를 클릭합니다.

### Core 콘솔에 원격으로 액세스하도록 브라우저 구성

원격 시스템에서 Core 콘솔에 액세스하려면 브라우저 설정을 수정해야 합니다.

 **노트:** 브라우저 설정을 수정하려면 관리자 권한으로 시스템에 로그인합니다.

 **노트:** Google Chrome에서는 Microsoft Internet Explorer 설정을 사용하므로 Internet Explorer를 사용하여 Chrome의 브라우저 설정을 변경합니다.



**노트:** Core 웹 콘솔에 로컬 또는 원격으로 액세스할 때 **Internet Explorer Enhanced Security Configuration(Internet Explorer 보안 강화형 구성)**이 설정되어 있는지 확인합니다. **Internet Explorer Enhanced Security Configuration(Internet Explorer 보안 강화형 구성)**을 설정하려면 다음을 수행합니다.

1. **Server Manager**를 엽니다.
2. 오른쪽에 표시된 **Local Server IE Enhanced Security Configuration(로컬 서버 IE 보안 강화형 구성)**을 선택하고 **On(설정)**으로 설정되어 있는지 확인합니다.

## Internet Explorer 및 Chrome에서 브라우저 설정 구성

Internet Explorer 및 Chrome에서 브라우저 설정을 수정하려면 다음을 수행합니다.

1. Internet Explorer를 엽니다.
2. **Tools(도구)** 메뉴에서 **Internet Options(인터넷 옵션)**, **Security(보안)** 탭을 선택합니다.
3. **Trusted Sites(신뢰할 수 있는 사이트)**를 클릭한 후 **Sites(사이트)**를 클릭합니다.
4. **Require server verification (https:) for all sites in the zone(이 영역에 있는 모든 사이트에 대해 서버 검증(https:) 필요)** 옵션을 선택 취소하고 **Trusted Sites(신뢰할 수 있는 사이트)**에 `http://<AppAssure Core>`를 호스팅하는 어플라이언스 서버의 IP 주소 또는 호스트 이름을 추가합니다.
5. **Close(닫기)**를 클릭하고 **Trusted Sites(신뢰할 수 있는 사이트)**를 선택한 후 **Custom Level(사용자 지정 수준)**을 클릭합니다.
6. **Miscellaneous(기타)** → **Display Mixed Content(혼합 내용 표시)**로 스크롤하고 **Enable(활성화)**를 선택합니다.
7. 화면 하단의 **User Authentication(사용자 인증)** → **Logon(로그온)**으로 스크롤하고 **Automatic logon with current user name and password(현재 사용자 이름 및 암호로 자동 로그인)**를 선택합니다.
8. **OK(확인)**를 클릭하고 **Advanced(고급)** 탭을 선택합니다.
9. **Multimedia(멀티미디어)**로 스크롤하고 **Play animations in webpages(웹페이지에서 애니메이션 재생)**를 선택합니다.
10. **Security(보안)**로 스크롤하고 **Enable Integrated Windows Authentication(통합된 Windows 인증 활성화)**를 선택하고 **OK(확인)**를 클릭합니다.

## Mozilla Firefox 브라우저 설정 구성



**노트:** 최신 버전의 Firefox에서 Mozilla Firefox 브라우저 설정을 수정하려면 보호를 해제하십시오. URL의 왼쪽에 있는 **Site Identify(사이트 확인)** 단추를 마우스 오른쪽 단추로 클릭하고 **Options(옵션)**로 이동한 후 **Disable protection for now(지금 보호 해제)**를 클릭합니다.

Mozilla Firefox 브라우저 설정을 수정하려면 다음을 수행합니다.


1. Firefox 주소 표시줄에 **about:config**를 입력하고 메시지가 표시되면 **I'll be careful, I promise(주의함)**를 클릭합니다.
2. **ntlm** 용어를 검색합니다.  
3개 이상의 검색 결과가 표시됩니다.
3. **network.automatic-ntlm-auth.trusted-uris**를 두 번 클릭하고 시스템에 맞게 다음과 같은 설정을 입력합니다.
  - 로컬 시스템의 경우 호스트 이름을 입력합니다.
  - 원격 시스템의 경우 AppAssure Core를 호스팅하는 어플라이언스 시스템의 호스트 이름 또는 IP 주소를 점표로 구분하여 입력합니다(예: `IP 주소,호스트 이름`).
4. Firefox를 다시 시작합니다.

## 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

 **노트:** 이 어플라이언스를 사용하는 경우 **Appliance(어플라이언스)** 탭을 사용하여 Core를 구성하는 것이 좋습니다. 초기 설치 후에 Core 구성에 대한 자세한 내용은 [dell.com/support/home](https://dell.com/support/home)에서 *Dell DL4300 어플라이언스 배포 설명서*를 참조하십시오.

## 라이선스 관리

라이선스를 Core 콘솔에서 직접 관리할 수 있습니다. 콘솔에서, 라이선스 키를 변경하고 라이선스 서버에 연결할 수 있습니다. 또한 Core 콘솔의 Licensing(라이선싱) 페이지에서 라이선스 포털에 액세스할 수 있습니다. 라이선싱 페이지에 다음 정보가 포함되어 있습니다.

- 라이선스 유형
- 라이선스 상태
- 라이선스 제약 조건
- 보호된 시스템 수
- 라이선싱 서버의 마지막 응답 상태
- 라이선싱 서버와 마지막으로 연결한 시간
- 다음으로 예약된 라이선싱 서버와의 연결 시도

### 라이선스 키 변경

라이선스 키를 변경하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Licensing(라이선싱)**을 선택합니다.  
**Licensing(라이선싱)** 페이지가 표시됩니다.
3. **License Details(라이선스 상세정보)** 섹션에서 **Change License(라이선스 변경)**를 클릭합니다.  
**Change License(라이선스 변경)** 대화 상자가 표시됩니다.
4. **Change License(라이선스 변경)** 대화 상자에 새 라이선스 키를 입력한 후 **Continue(계속)**를 클릭합니다.

### 라이선스 포털 서버 연결

Core 콘솔은 라이선스 포털에서 변경한 내용으로 최신 상태를 유지하기 위해 포털 서버에 자주 연결합니다. 일반적으로, 지정된 간격으로 포털 서버와 자동으로 통신하지만 요청 시 통신을 시작할 수 있습니다.

포털 서버를 연결하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Licensing(라이선싱)**을 클릭합니다.
3. **License Server(라이선스 서버)** 옵션에서 **Contact Now(지금 연결)**를 클릭합니다.

## 수동으로 AppAssure 언어 변경


AppAssure에서는 AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사) 실행 중에 선택한 언어를 지원되는 언어로 변경할 수 있습니다.  
AppAssure 언어를 원하는 언어로 변경하려면 다음을 수행하십시오.


1. `regdit` 명령을 사용하여 레지스트리 편집기를 실행합니다.
2. **HKEY\_LOCAL\_MACHINE → SOFTWARE → AppRecovery → Core → Localization(지역화)**으로 이동합니다.
3. **Lcid**를 엽니다.
4. **decimal(10진수)**을 선택합니다.
5. Value data (값 데이터) 상자에 필요한 언어 값을 입력합니다. 지원되는 언어 값은 다음과 같습니다.
  - a. 영어: 1033
  - b. 포르투갈어(브라질): 1046
  - c. 스페인어: 1034
  - d. 프랑스어: 1036
  - e. 독일어: 1031
  - f. 중국어(간체): 2052
  - g. 일본어: 1041
  - h. 한국어: 1042
6. 마우스 오른쪽 단추를 클릭하고 지정된 순서로 서비스를 다시 시작합니다.
  - a. Windows Management Instrumentation
  - b. SRM 웹 서비스
  - c. AppAssure 코어
7. 브라우저 캐시를 지웁니다.
8. 브라우저를 닫고 바탕 화면 아이콘에서 Core 콘솔을 다시 시작합니다.

## 설치하는 동안 OS 언어 변경

Windows 설치를 실행하는 동안, 제어판에서 언어 팩을 선택하고 추가적인 국가별 설정을 구성할 수 있습니다.

OS 언어 변경하려면 다음을 수행하십시오.

 **노트:** OS 언어와 AppAssure 언어는 동일하게 설정하는 것이 좋습니다. 그렇지 않으면 일부 메시지가 혼합된 언어로 표시될 수도 있습니다.

 **노트:** AppAssure 언어를 변경하기 전에 OS 언어 변경하는 것이 좋습니다.

1. 시작 페이지에서 언어를 입력하고 검색 범위가 '설정'으로 되어 있는지 확인하십시오.
2. 결과 패널에서 언어를 선택합니다.
3. 언어 기본 설정 변경 창에서 언어 추가를 선택합니다.


4. 설치할 언어를 찾아보거나 검색합니다.  
예를 들어 '카탈로니아어'를 선택한 후 '추가'를 선택합니다. 그러면 '카탈로니아어'가 기본 언어 중 하나로 추가됩니다.
5. '언어 기본 설정 변경' 창에서, 추가한 언어 옆의 **옵션**을 선택합니다.
6. 언어 팩을 해당 언어로 사용할 수 있는 경우에는 언어 팩 다운로드 및 설치를 선택합니다.
7. 언어 팩이 설치되면 Windows 표시 언어에 사용할 수 있는 것으로 표시됩니다.
8. 이 언어를 표시 언어로 사용하려면 해당 언어를 언어 목록 상단으로 이동합니다.
9. Windows에서 로그아웃했다가 다시 로그인해야 변경 사항이 적용됩니다.

## Core 설정 관리

Core 설정은 구성 및 성능에 대한 다양한 설정을 정의하는 데 사용됩니다. 대부분의 설정은 최적의 상태로 사용할 수 있도록 구성되지만, 필요에 따라 다음 설정을 변경할 수 있습니다.

- 일반
- 야간 작업
- 전송 큐
- 클라이언트 시간 제한 설정
- 중복 제거 캐시 구성
- 데이터베이스 연결 설정

## Core 표시 이름 변경

 **노트:** 어플라이언스를 처음 구성할 때 영구 표시 이름을 선택하는 것이 좋습니다. 나중에 변경하려면 몇 가지 단계를 수동으로 수행해야 새 호스트 이름이 적용되고 어플라이언스가 제대로 작동됩니다. 자세한 내용은 [호스트 이름을 수동으로 변경](#)을 참조하십시오.

Core 표시 이름을 변경하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **General(일반)** 창에서 **Change(변경)**를 클릭합니다.  
**General Settings(일반 설정)** 대화 상자가 표시됩니다.
4. **Display name(표시 이름)** 텍스트 상자에 Core에 대한 새 표시 이름을 입력합니다.  
이 이름은 Core 콘솔에 표시되는 이름으로서 최대 길이는 64자입니다.
5. **Web Server Port(웹 서버 포트)** 텍스트 상자에, 웹 서버의 포트 번호를 입력합니다. 기본값은 8006입니다.
6. **Service Port(서비스 포트)**에, 서비스의 포트 번호를 입력합니다. 기본값은 8006입니다.
7. **OK(확인)**를 클릭합니다.

## 야간 작업 시간 조정

야간 작업 시간을 조정하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Nightly Jobs(야간 작업)** 영역에서 **Change(변경)**를 클릭합니다.  
**Nightly Jobs(야간 작업)** 대화 상자가 표시됩니다.

4. **Nightly Jobs Time(야간 작업 시간)** 텍스트 상자에 야간 작업을 수행할 시간을 새로 입력합니다.
5. **OK(확인)**를 클릭합니다.

## 전송 큐 설정 수정

전송 큐 설정은 최대 동시 전송 수와 데이터 전송의 최대 시도 수를 지정하는 코어 수준의 설정입니다.

전송 큐 설정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Transfer Queue(전송 큐)** 창에서 **Change(변경)**를 클릭합니다.  
**Transfer Queue(전송 큐)** 대화 상자가 표시됩니다.
4. **Maximum Concurrent Transfers(최대 동시 전송 횟수)** 텍스트 상자에 값을 입력하여 동시 전송 횟수를 업데이트합니다.  
1 - 60 범위의 값으로 설정합니다. 값이 작을수록 네트워크 및 기타 시스템 리소스에서의 로드가 적습니다. 처리되는 용량이 증가할수록 시스템의 로드도 증가합니다.
5. **Maximum Retries(최대 재시도 횟수)** 텍스트 상자에 값을 입력하여 최대 재시도 횟수를 업데이트합니다.
6. **OK(확인)**를 클릭합니다.

## 클라이언트 시간 제한 설정 조정

클라이언트 시간 제한 설정을 조정하려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Client Timeout Settings Configuration(클라이언트 시간 제한 설정 구성)** 영역에서 **Change(변경)**를 클릭합니다.  
**Client Timeout Settings(클라이언트 시간 제한 설정)** 대화 상자가 표시됩니다.
4. **Connection Timeout(연결 시간 제한)** 텍스트 상자에 연결 시간을 초과하기 전의 시간(분 및 초)을 입력합니다.
5. **Connection UI Timeout(연결 UI 시간 제한)** 텍스트 상자에 연결 UI 시간을 초과하기 전의 시간(분 및 초)을 입력합니다.
6. **Read/Write Timeout(읽기/쓰기 시간 제한)** 대화 상자에 읽기/쓰기 이벤트 동안 시간이 초과되기 전에 경과할 시간(분 및 초)을 입력합니다.
7. **Read/Write UI Timeout(읽기/쓰기 UI 시간 제한)** 텍스트 상자에, 읽기/쓰기 UI 시간을 초과하기 전의 시간(분 및 초)을 입력합니다.
8. **OK(확인)**를 클릭합니다.

## 중복 제거 캐시 설정 구성

중복 제거 캐시 설정을 구성하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Deduplication Cache Configuration(중복 제거 캐시 구성)** 영역에서 **Change(변경)**를 클릭합니다.  
**Deduplication Cache Configuration(중복 제거 캐시 구성)** 대화 상자가 표시됩니다.
4. **Primary Cache Location(기본 캐시 위치)** 텍스트 상자에 업데이트된 값을 입력하여 기본 캐시 위치를 변경합니다.

5. **Secondary Cache Location(보조 캐시 위치)** 텍스트 상자에 업데이트된 값을 입력하여 보조 캐시 위치를 변경합니다.
6. **Metadata Cache Location(메타데이터 캐시 위치)** 텍스트 상자에 업데이트된 값을 입력하여 메타데이터 캐시 위치를 변경합니다.
7. **Dedupe Cache Size(중복 제거 캐시 크기)** 텍스트 상자에, 중복 제거 캐시에 할당할 공간의 양에 해당하는 값을 입력합니다.  
단위 크기 드롭다운 필드에서, GB(기가바이트) 또는 TB(테라바이트)를 선택하여 Dedupe Cache Size(중복 제거 캐시 크기) 텍스트 상자의 값에 맞는 측정 단위를 지정합니다.
8. **OK(확인)**를 클릭합니다.



**노트:** 변경 내용을 적용하려면 Core 서비스를 다시 시작해야 합니다.

## 엔진 설정 수정

엔진 설정을 수정하려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Replay Engine Configuration(재생 엔진 구성)** 창에서 **Change(변경)**를 클릭합니다.  
**Replay Engine Configuration(재생 엔진 구성)** 대화 상자가 표시됩니다.
4. 다음 설명과 같이 구성 정보를 입력합니다.

### 텍스트 상자 설명

<b>IP 주소</b>	<ul style="list-style-type: none"> <li>TCP/IP에서 기본 IP 주소를 사용하려면 <b>Automatically Determined(자동으로 결정)</b>를 클릭합니다.</li> <li>IP 주소를 수동으로 입력하려면 <b>Use a specific address(특정 주소 사용)</b>를 클릭합니다.</li> </ul>
<b>선호 포트</b>	포트 번호를 입력하거나 기본 설정을 적용합니다. 기본 포트는 8007입니다. 포트는 엔진의 통신 채널을 지정하는 데 사용됩니다.
<b>포트 사용 중</b>	포트가 재생 엔진 구성에 사용되고 있습니다.
<b>포트 자동 지정 허용</b>	TCP 포트 지정을 허용하려면 이 옵션을 클릭합니다.
<b>관리 그룹</b>	관리 그룹에 대한 새 이름을 입력합니다. 기본 이름은 <b>BUILTIN\Administrators</b> 입니다.
<b>최소 비동기 I/O 길이</b>	값을 입력하거나 기본 설정을 선택합니다. 이는 최소 비동기 입력/출력 길이를 나타냅니다. 기본 설정은 65536입니다.
<b>수신 버퍼 크기</b>	인바운드 버퍼 크기를 입력하거나 기본 설정을 선택합니다. 기본 설정은 8192입니다.
<b>보내기 버퍼 크기</b>	아웃바운드 버퍼 크기를 입력하거나 기본 설정을 선택합니다. 기본 설정은 8192입니다.
<b>읽기 시간 제한</b>	읽기 시간 제한 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:00:30입니다.
<b>쓰기 시간 제한</b>	쓰기 시간 제한 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:00:30입니다.

텍스트 상자	설명
--------	----

지연 없음	네트워크 효율성에 영향을 주기 때문에 이 확인란을 선택하지 않는 것이 좋습니다. 이 설정을 수정해야 할 경우에는 Dell 지원팀에 문의하십시오.
-------	---

5. **OK(확인)**를 클릭합니다.

## 데이터베이스 연결 설정 수정

데이터베이스 연결 설정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Database Connection Settings(데이터베이스 연결 설정)** 영역에서 다음 중 하나를 선택합니다.
  - **Apply Default(기본값 적용)**를 클릭합니다.
  - **Change(변경)**를 클릭합니다.

**Database Connection Settings(데이터베이스 연결 설정)** 대화 상자가 표시됩니다.

4. 아래에 설명된 대로 데이터베이스 연결을 수정하기 위한 설정을 입력합니다.

텍스트 상자	설명
--------	----

호스트 이름	데이터베이스 연결을 위한 호스트 이름을 입력합니다.
--------	------------------------------

포트	데이터베이스 연결을 위한 포트 번호를 입력합니다.
----	-----------------------------

사용자 이름(선택사항)	데이터베이스 연결 설정에 액세스하고 관리하기 위한 사용자 이름을 입력합니다. 이는 데이터베이스 연결에 액세스하기 위한 로그인 자격 증명을 지정하는 데 사용됩니다.
--------------	---

암호(선택사항)	데이터베이스 연결 설정에 액세스하고 관리하기 위한 암호를 입력합니다.
----------	--

특정 기간 동안 이벤트 및 작업 기록 보존	데이터베이스 연결에 대한 이벤트 및 작업 기록을 보존할 기간(일)을 입력합니다.
-------------------------	--

최대 연결 풀 크기	동적 재사용을 허용하도록 캐시된 데이터베이스 연결의 최대 개수를 설정합니다. 기본 설정은 100입니다.
------------	--

최소 연결 풀 크기	동적 재사용을 허용하도록 캐시된 데이터베이스 연결의 최소 개수를 설정합니다. 기본 설정은 0입니다.
------------	--

5. **Test Connection(연결 테스트)**을 클릭하여 설정을 확인합니다.

6. **Save(저장)**를 클릭합니다.

## 리포지토리 정보


리포지토리에 보호된 워크스페이스 및 서버에서 수집된 스냅샷이 저장됩니다. 리포지토리는 SAN(저장소 영역 네트워크), DAS(직접 연결 저장소) 또는 NAS(네트워크 연결 저장소)와 같은 여러 저장 기술에 적용됩니다.

리포지토리를 생성하면 Core가 지정된 위치에 데이터 및 메타데이터에 필요한 저장 공간을 미리 할당합니다. 단일 Core에 여러 저장 기술에 적용되는 최대 255개의 독립 리포지토리를 생성할 수 있습니다. 또한 새 파일 범위 또는 사양을 추가하여 리포지토리의 크기를 늘릴 수도 있습니다. 확장된 리포지토리에는 여러 저장 기술에 적용되는 범위를 최대 4096개까지 포함될 수 있습니다.

주요 리포지토리 개념 및 고려 사항은 다음과 같습니다.




- 리포지토리는 AppAssure 확장 가능 개체 파일 시스템을 기반으로 합니다.
- 리포지토리 내에 저장되는 모든 데이터는 전역적으로 중복 제거됩니다.
- 확장 가능 개체 파일 시스템에서 전역 데이터 중복 제거, 암호화 및 보존 관리와 함께 확장 가능한 I/O 성능을 제공할 수 있습니다.

 **노트:** DL4300 리포지토리는 기본 저장 장치에 저장됩니다. 성능 제한으로 인해 데이터 도메인과 같은 보관 저장 장치는 지원되지 않습니다. 마찬가지로, 이러한 장치를 기본 저장소로 사용하면 성능이 제한되므로 클라우드에 계층화되는 NAS 필러에 리포지토리를 저장하지 않아야 합니다.

## 리포지토리 관리를 위한 로드맵

리포지토리 관리를 위한 로드맵은 리포지토리 생성, 구성 및 보기와 같은 작업을 다루며 다음과 같은 항목이 포함됩니다.

- [Core 콘솔 액세스](#)
- [리포지토리 생성](#)
- [리포지토리 상세정보 보기](#)
- [리포지토리 설정 수정](#)
- [기존 리포지토리에 저장소 위치 추가](#)
- [리포지토리 검사](#)
- [리포지토리 삭제](#)
- [리포지토리 복구](#)

 **노트:** Appliance(어플라이언스) 탭을 사용하여 리포지토리를 구성하는 것이 좋습니다.


어플라이언스를 사용하려면 먼저 Core 서버에 하나 이상의 리포지토리를 설정해야 합니다. 리포지토리에는 보호되는 데이터가 저장됩니다. 구체적으로 말하면 사용자 환경에서 보호되는 서버에서 캡처된 스냅샷이 저장됩니다.

리포지토리를 구성할 때 Core 서버에서 데이터 저장소를 배치할 위치, 각 리포지토리에 추가할 수 있는 위치 수, 리포지토리의 이름 및 리포지토리에서 지원하는 동시 작업 수 지정 등과 같은 다양한 작업을 수행할 수 있습니다.

리포지토리를 생성할 때 Core에서 지정된 위치에 데이터와 메타데이터를 저장하는 데 필요한 공간을 미리 할당합니다. 하나의 Core에 최대 255개의 독립된 리포지토리를 생성할 수 있습니다. 단일 리포지토리의 크기를 더 늘리기 위해 새 저장소 위치 또는 볼륨을 추가할 수 있습니다.

Core 콘솔에서 리포지토리를 추가하거나 수정할 수 있습니다.

## 리포지토리 생성

 **노트:** 이 어플라이언스를 SAN으로 사용하는 경우 **Appliance(어플라이언스)** 탭을 사용하여 리포지토리를 생성하는 것이 좋습니다([선택한 저장소 프로비저닝](#) 참조).


리포지토리를 수동으로 생성하려면 다음을 수행하십시오.


1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Repositories(리포지토리)**를 클릭합니다.
3. **Add new(새로 추가)**를 클릭합니다.  
**Add New Repository(새 리포지토리 추가)** 대화 상자가 표시됩니다.

4. 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 Repository 라는 단어와 1부터 시작하여 새 리포지토리에 순차적으로 추가되는 색인 번호로 구성됩니다. 필요한 경우 이름을 변경할 수 있으며 최대 150자를 입력할 수 있습니다.
동시 작업	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다. 기본값은 64입니다.
설명	경우에 따라 이 리포지토리에 대해 설명하는 메모를 입력합니다.

5. 리포지토리의 특정 저장소 위치나 볼륨을 정의하려면 **Add Storage Location(저장소 위치 추가)**을 클릭합니다.

 **주의:** 이 단계에서 만드는 AppAssure 리포지토리를 나중에 제거하는 경우, 리포지토리의 저장소 위치에 있는 모든 파일이 삭제됩니다. 리포지토리 파일을 저장할 전용 폴더를 정의하지 않으면 이 파일이 루트에 저장됩니다. 리포지토리를 삭제하면 루트의 전체 내용도 삭제되어 데이터가 유실됩니다.

 **노트:** 리포지토리는 기본 저장 장치에 저장됩니다. 성능 제한으로 인해 데이터 도메인과 같은 보관 저장 장치는 지원되지 않습니다. 마찬가지로, 이러한 장치를 기본 저장소로 사용하면 성능이 제한되므로 클라우드에 계층화되는 NAS 필러에 리포지토리를 저장하지 않아야 합니다.

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

6. 저장소 위치에 대해 파일을 추가하는 방법을 지정합니다. 로컬 디스크 또는 CIFS 공유에 파일을 추가하도록 선택할 수 있습니다.
- 로컬 시스템을 지정하려면 **Add file on local disk(로컬 디스크에 파일 추가)**를 클릭하고 다음과 같이 정보를 입력합니다.

텍스트 상자	설명
데이터 경로	보호되는 데이터를 저장할 위치를 입력합니다. 예를 들어, X:\Repository\Data를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.
메타데이터 경로	보호되는 메타데이터를 저장할 위치를 입력합니다. 예를 들어, X:\Repository\Metadata를 입력합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름과 도메인을 구분할 때만)만 사용하십시오. a부터 z까지의 문자는 대소문자를 구분합니다. 공백, 기타 기호 또는 문장 부호는 사용할 수 없습니다.

- 네트워크 공유 위치를 지정하려면 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 클릭하고 다음과 같이 정보를 입력합니다.

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다. 이 위치가 루트에 있으면 전용 폴더 이름(예: Repository)을 정의합니다. 경로는 \\로 시작해야 합니다. 경로를 지정할 때는 영숫자, 하이픈, 마침표(호스트 이름

## 텍스트 상자

## 설명

과 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.

7. **Details(상세정보)** 창에서 **Show/Hide Details(상세정보 표시/숨기기)**를 클릭하고 아래에 설명된 대로 저장소 위치에 대한 상세정보를 입력합니다.

## 텍스트 상자

## 설명

### Size(크기)

저장소 위치의 크기 또는 용량을 설정합니다. 기본값은 250MB입니다. 다음을 선택할 수 있습니다.

- MB
- GB
- TB



**노트:** 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.



**노트:** 저장소 위치가 Windows XP 또는 Windows 7을 사용하는 NTFS(New Technology File System) 볼륨일 경우 파일 크기는 16TB로 제한됩니다.

저장소 위치가 Windows 8 또는 Windows Server 2012를 사용하는 NTFS 볼륨일 경우 파일 크기는 256TB로 제한됩니다.



**노트:** 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 설정하면 Windows가 캐싱을 제어합니다.



**노트:** 쓰기 캐싱 정책을 On(켜짐)으로 설정하면 성능이 빨라질 수 있습니다. Windows Server 2012 이전 버전을 사용하는 경우 **Off(꺼짐)**로 설정하는 것이 좋습니다.

**Off(꺼짐)**로 설정하면 AppAssure에서 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.

8. **Save(저장)**를 클릭합니다.

새로 추가된 저장소 위치를 포함할 수 있는 **Repositories(리포지토리)** 화면이 표시됩니다.

9. 리포지토리에 대한 추가 저장소 위치를 추가하려면 4단계에서 7단계를 반복합니다.

10. **Create(생성)**를 클릭하여 리포지토리를 생성합니다.

**Configuration(구성)** 탭에 **Repository(리포지토리)** 정보가 표시됩니다.

## 리포지토리 상세정보 보기

리포지토리 상세정보를 보려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Repositories(리포지토리)**를 클릭합니다.
3. 상세정보를 볼 리포지토리의 **Status(상태)** 열 옆에 있는 >를 클릭합니다.
4. 확장된 보기에서 다음과 같은 작업을 수행할 수 있습니다.
  - 설정 수정
  - 저장소 위치 추가
  - 리포지토리 확인
  - 리포지토리 삭제

리포지토리의 상세정보도 표시되며 저장소 위치 및 통계가 포함되어 있습니다. 저장소 위치 상세정보에는 메타데이터 경로, 데이터 경로 및 크기가 포함됩니다. 통계 정보에는 다음과 같은 사항이 포함됩니다.

- 중복 제거 - 블록 중복 제거 항목 수, 블록 중복 제거 누락 수, 블록 압축 속도로 보고됩니다.
- 레코드 I/O - 속도(MB/초), 읽기 속도(MB/초), 쓰기 속도(MB/초)로 구성됩니다.
- 저장소 엔진 - 속도(MB/초), 읽기 속도(MB/초), 쓰기 속도(MB/초)로 구성됩니다.

## 리포지토리 설정 수정


리포지토리를 추가한 후 설명 또는 최대 동시 작업 수와 같은 리포지토리 설정을 수정할 수 있습니다. 또한 리포지토리에 대한 새 저장소 위치를 생성할 수 있습니다.

리포지토리 설정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Repositories(리포지토리)**를 클릭합니다.
3. **Actions(작업)** 단추 아래의 Compression Ratio(압축 비율) 열 옆에 있는 Settings(설정) 아이콘을 클릭하고 **Settings(설정)**를 클릭합니다.

**Repository Settings(리포지토리 설정)** 대화 상자가 표시됩니다.

4. 아래 설명대로 리포지토리 정보를 편집합니다.

필드	설명
리포지토리 이름	리포지토리의 표시 이름을 입력합니다. 기본적으로 이 텍스트 상자는 리포지토리라는 단어와 리포지토리의 번호에 해당하는 색인 번호로 구성됩니다.  <b>노트:</b> 리포지토리 이름은 편집할 수 없습니다.
설명	경우에 따라 리포지토리에 대해 설명하는 메모를 입력합니다.
최대 동시 작업 수	리포지토리에서 지원할 수 있는 동시 요청 수를 정의합니다.

## 필드

## 설명

### 중복 제거 활성화

중복 제거 기능을 해제하려면 이 확인란을 선택 취소하고, 중복 제거 기능을 활성화하려면 이 확인란을 선택합니다.



**노트:** 이 설정을 변경하면 설정을 지정한 후 수행한 백업에만 적용됩니다. 기존 데이터 또는 다른 Core에서 복제되거나 아카이브에서 가져온 데이터에는 보호되는 시스템에서 데이터가 수집되었을 때의 중복 제거 값이 유지됩니다.

### 압축 활성화

압축 기능을 해제하려면 이 확인란을 선택 취소하고, 압축 기능을 활성화하려면 이 확인란을 선택합니다.



**노트:** 이 설정을 변경하면 설정을 변경한 후 수행한 백업에만 적용됩니다. 기존 데이터 또는 다른 Core에서 복제되거나 아카이브에서 가져온 데이터에는 보호되는 시스템에서 데이터가 수집되었을 때의 압축 값이 유지됩니다.

5. **Save(저장)**를 클릭합니다.

## 기존 리포지토리 확장

어플라이언스에 다른 MD1400 DAS를 추가하는 경우 사용 가능한 저장소를 이용하여 기존 리포지토리를 확장할 수 있습니다.

기존 리포지토리를 확장하려면 다음을 수행합니다.

1. MD1400 DAS를 설치한 후 Core 콘솔을 열고 **Appliance(어플라이언스)** 탭을 선택한 후 **Tasks(작업)**를 클릭합니다.
2. **Tasks(작업)** 화면에서, 새 저장소 옆에 있는 **Provision(프로비전)**을 클릭합니다.
3. **Provisioning Storage(저장소 프로비저닝)** 화면에서 **Expand the existing repository(기존 리포지토리 확장)**를 선택하고 확장할 리포지토리를 선택합니다.
4. **Provision(프로비전)**을 클릭합니다.  
**Tasks(작업)** 화면에 저장소 장치 옆에 있는 **Status Description(상태 설명)**이 **Provisioned(프로비저닝됨)**로 표시됩니다.

## 기존 리포지토리에 저장소 위치 추가

저장소 위치를 추가하면 리포지토리 또는 볼륨을 저장할 위치를 정의할 수 있습니다.

기존 리포지토리에 저장소 위치를 추가하려면 다음을 수행하십시오.

1. 저장소 위치를 추가할 리포지토리의 **Status(상태)** 열 옆에 있는 **>**를 클릭합니다.
2. **Add Storage Location(저장소 위치 추가)**을 클릭합니다.  
**Add Storage Location(저장소 위치 추가)** 대화 상자가 표시됩니다.
3. 저장소 위치의 파일 추가 방법을 지정합니다. 로컬 디스크 또는 CIFS 공유에 파일을 추가하도록 선택할 수 있습니다.
  - 로컬 시스템을 지정하려면 **Add file on local disk(로컬 디스크에 파일 추가)**를 클릭하고 다음과 같이 정보를 입력합니다.

### 텍스트 상자

### 설명

#### 메타데이터 경로

보호된 메타데이터를 저장할 위치를 입력합니다.




#### 데이터 경로

보호된 데이터를 저장할 위치를 입력합니다.

- 네트워크 공유 위치를 지정하려면 **Add file on CIFS share(CIFS 공유에 파일 추가)**를 클릭하고 다음과 같이 정보를 입력합니다.

텍스트 상자	설명
UNC 경로	네트워크 공유 위치에 대한 경로를 입력합니다.
사용자 이름	네트워크 공유 위치에 액세스할 사용자 이름을 지정합니다.
암호	네트워크 공유 위치에 액세스할 암호를 지정합니다.


4. **Details(상세정보)** 섹션에서 **Show/Hide Details(상세정보 표시/숨기기)**를 클릭하고 아래에 설명된 대로 저장소 위치에 대한 상세정보를 입력합니다.

텍스트 상자	설명
Size(크기)	<p>저장소 위치의 크기 또는 용량을 설정합니다. 기본 크기는 250MB입니다. 다음을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• MB</li> <li>• GB</li> <li>• TB</li> </ul> <p> <b>노트:</b> 지정하는 크기는 볼륨 크기를 초과할 수 없습니다.</p> <p> <b>노트:</b> 저장소 위치가 Windows XP 또는 Window 7을 사용하는 NTFS 볼륨일 경우 파일 크기는 16TB로 제한됩니다.</p> <p>저장소 위치가 Windows 8 또는 Windows Server 2012를 사용하는 NTFS 볼륨일 경우 파일 크기는 256TB로 제한됩니다.</p> <p> <b>노트:</b> 운영 체제의 유효성을 검사하려면 사용할 저장소 위치에 WMI가 설치되어 있어야 합니다.</p>

**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 설정하면 Windows에서 캐싱을 제어합니다.

 **노트:** 쓰기 캐싱 정책을 **On(켜짐)**으로 설정하면 성능이 더욱 빨라지지만 권장되는 설정은 **Off(꺼짐)**입니다.

**Off(꺼짐)**로 설정하면 AppAssure에서 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.  
**트**

5. **Save(저장)**를 클릭합니다.  
새로 추가된 저장소 위치를 포함할 수 있는 **Repositories(리포지토리)** 화면이 표시됩니다.
6. 리포지토리에 대한 추가 저장소 위치를 추가하려면 4단계에서 7단계를 반복합니다.
7. **OK(확인)**를 클릭합니다.


## 리포지토리 검사

어플라이언스에서는 오류가 발생한 경우 리포지토리 볼륨의 진단 검사를 수행할 수 있습니다. 비정상적인 종료 또는 하드웨어 오류 등이 발생하는 경우 Core 오류가 발생할 수 있습니다.

 **노트:** 이 절차는 진단용으로만 수행해야 합니다.

리포지토리를 검사하려면 다음을 수행하십시오.


1. **Configuration(구성)** 탭에서 **Repositories(리포지토리)**를 클릭하고 검사할 리포지토리 옆에 있는 >를 선택합니다.
2. **Actions(작업)** 창에서 **Check(검사)**를 클릭합니다.  
**Check Repository(리포지토리 검사)** 대화 상자가 표시됩니다.
3. **Check Repository(리포지토리 검사)** 대화 상자에서 **Check(검사)**를 클릭합니다.

 **노트:** 검사에 실패한 경우에는 아카이브에서 리포지토리를 복원하십시오.

## 리포지토리 삭제

리포지토리를 삭제하려면 다음을 수행하십시오.

1. **Configuration(구성)** 탭에서 **Repositories(리포지토리)**를 클릭하고 삭제할 리포지토리 옆에 있는 >를 선택합니다.
2. **Actions(작업)** 창에서 **Delete(삭제)**를 클릭합니다.
3. **Delete Repository(리포지토리 삭제)** 대화 상자에서 **Delete(삭제)**를 클릭합니다.

 **주의:** 리포지토리가 삭제되면 리포지토리에 포함된 데이터가 삭제되고 복구할 수 없습니다.

리포지토리를 삭제할 때는 Open Manage System Administrator를 통해 리포지토리가 포함된 가상 디스크를 삭제해야 합니다. 가상 디스크를 삭제한 후에 디스크를 다시 프로비저닝하고 리포지토리를 다시 생성할 수 있습니다.

## 볼륨 다시 탑재

볼륨을 다시 탑재하려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.
2. **Appliance(어플라이언스)** → **Tasks(작업)**를 클릭하고
3. **Remount Volumes(볼륨 다시 탑재)**를 클릭합니다.  
볼륨이 다시 탑재됩니다.

### 외부 볼륨 확인

프로비저닝된 MD1400의 전원이 꺼지거나 연결이 끊어졌다가 나중에 다시 전원이 켜진 경우 MD1400이 연결되었음을 보고하는 이벤트가 Core 콘솔에 표시됩니다. 그러나 **Tasks(작업)** 화면의 **Appliance(어플라이언스)** 탭에 이를 복구할 수 있는 작업이 표시되지 않습니다. **Enclosures(인클로저)** 화면에 MD1400이 외부 상태로 보고되고, 외부 가상 디스크의 리포지토리가 오프라인으로 표시됩니다.

외부 볼륨을 해결하려면 다음을 수행합니다.

1. Core 콘솔에서 **Appliance(어플라이언스)** 탭을 선택하고 **Remount Volumes(볼륨 다시 탑재)**를 클릭합니다.

볼륨이 다시 탑재됩니다.

2. **Configuration(구성)** 탭을 선택한 다음 **Repositories(리포지토리)**를 클릭합니다.
3. **Status(상태)** 옆에 있는 >를 클릭하여 빨간색 상태 표시등이 있는 리포지토리를 확장합니다.
4. 리포지토리 무결성을 확인하려면 **Actions(작업)**에서 **Check(검사)**를 클릭합니다.

## 리포지토리 복구

어플라이언스에서 리포지토리 가져오기에 실패하면 빨간색 원으로 작업 실패 상태를 **Tasks(작업)** 화면에 표시하며 상태 설명은 **Error, Completed - Exception(오류, 완료됨 - 예외)**으로 표시됩니다. **Tasks(작업)** 화면에서 오류 상세정보를 보려면 **Status(상태)** 열 옆에 있는 >를 클릭하여 작업 상세정보를 확장하십시오. **Status Details(상태 상세정보)**에 복구 작업 상태가 예외라고 표시되며, **Error Message(오류 메시지)** 열에는 오류 조건에 대한 추가적인 상세정보가 표시됩니다.

가져오기 실패 상태에서 리포지토리를 복구하려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.  
**Repositories(리포지토리)** 화면에 빨간색 상태 표시등이 있는 실패한 리포지토리가 표시됩니다.
2. **Configuration(구성)** → **Repositories(리포지토리)**를 클릭합니다.
3. **Status(상태)** 옆에 있는 >를 클릭하여 실패한 리포지토리를 확장합니다.
4. **Actions(작업)** 섹션에서 **Check(검사), Yes(예)**를 차례로 클릭하여 검사 실행을 확인합니다.  
어플라이언스가 리포지토리를 복구합니다.

## 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.

## 암호화 키 추가


암호화 키를 추가하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Security(보안)**를 클릭합니다.  
**Encryption Keys(암호화 키)** 페이지가 나타납니다.
3. **Actions(작업)**을 클릭한 후 **Add Encryption Key(암호화 키 추가)**를 클릭합니다.  
**Create Encryption Key(암호화 키 생성)** 대화 상자가 표시됩니다.
4. **Create Encryption Key(암호화 키 생성)** 대화 상자에서 아래에 설명된 대로 키에 대한 상세정보를 입력합니다.



텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다.
설명	암호화 키에 대한 설명을 입력합니다. 이는 암호화 키의 추가적인 상세정보를 제공하는 데 사용됩니다.
암호	암호를 입력합니다. 이는 액세스를 제어하는 데 사용됩니다.
암호 확인	암호를 다시 입력합니다. 이는 암호 입력을 확인하는 데 사용됩니다.

5. **OK(확인)**를 클릭합니다.

 주의: 암호를 보호하는 것이 좋습니다. 암호를 분실할 경우 데이터에 액세스할 수 없습니다.

## 암호화 키 편집


암호화 키를 편집하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Security(보안)**를 클릭합니다.  
**Encryption Keys(암호화 키)** 화면이 표시됩니다.
3. 수정할 암호화 키를 선택하고 **Edit(편집)**를 클릭합니다.  
**Edit Encryption Key(암호화 키 편집)** 대화 상자가 표시됩니다.
4. **Edit Encryption Key(암호화 키 편집)** 대화 상자에서 이름을 편집하거나 암호화 키에 대한 설명을 수정합니다.
5. **OK(확인)**를 클릭합니다.

## 암호화 키 암호 변경

암호화 키 암호를 변경하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Security(보안)**를 클릭합니다.  
**Encryption Keys(암호화 키)** 페이지가 나타납니다.
3. 수정할 암호화 키를 선택하고 **Change Passphrase(암호 변경)**를 클릭합니다.  
**Change Passphrase(암호 변경)** 대화 상자가 표시됩니다.
4. **Change Passphrase(암호 변경)** 대화 상자에 암호화에 대한 새 암호를 입력한 후 암호를 다시 입력하여 입력한 내용을 확인합니다.
5. **OK(확인)**를 클릭합니다.

 주의: 암호를 보호하는 것이 좋습니다. 암호를 분실한 경우 시스템 데이터에 액세스할 수 없습니다.

## 암호화 키 가져오기

암호화 키를 가져오려면 다음을 수행합니다.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성) → Security(보안)**를 클릭합니다.
3. **Actions(작업)** 드롭다운 메뉴를 선택하고 **Import(가져오기)**를 클릭합니다.  
**Import Key(키 가져오기)** 대화 상자가 표시됩니다.

4. **Import Key(키 가져오기)** 대화 상자에서 **Browse(찾아보기)**를 클릭하여 가져올 암호화 키를 찾고 **Open(열기)**를 클릭합니다.
5. **OK(확인)**를 클릭합니다.

## 암호화 키 내보내기


암호화 키를 내보내려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Security(보안)**를 클릭합니다.
3. 내보낼 암호화 키의 이름 옆에 있는 >를 클릭한 후 **Export(내보내기)**를 클릭합니다.  
**Export Key(키 내보내기)** 대화 상자가 표시됩니다.
4. **Export Key(키 내보내기)** 대화 상자에서 **Download Key(키 다운로드)**를 클릭하여 안전한 위치에 암호화 키를 저장하고 보관합니다.
5. **OK(확인)**를 클릭합니다.

## 암호화 키 제거

암호화 키를 제거하려면 다음을 수행하십시오.

1. Core 콘솔로 이동합니다.
2. **Configuration(구성)** → **Security(보안)**를 클릭합니다.
3. 제거할 암호화 키의 이름 옆에 있는 >를 클릭한 후 **Remove(제거)**를 클릭합니다.  
**Remove Key(키 제거)** 대화 상자가 표시됩니다.
4. **Remove Key(키 제거)** 대화 상자에서 **OK(확인)**를 클릭하여 암호화 키를 제거합니다.

 **노트:** 암호화 키를 제거하면 데이터의 암호화가 해제됩니다.

## 클라우드 계정 관리

DL 어플라이언스에서는 복구 지점의 백업 아카이브를 클라우드에 생성하여 데이터를 백업할 수 있습니다. DL 어플라이언스를 사용하면 클라우드 저장소 공급자를 통해 클라우드 계정을 생성, 편집, 관리할 수 있습니다. Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage 또는 기타 OpenStack 기반 클라우드 서비스를 사용하여 데이터를 클라우드에 아카이브할 수 있습니다. 클라우드 계정을 관리하려면 다음과 같은 주제를 참조하십시오.

- [클라우드 계정 추가](#)
- [클라우드 계정 편집](#)
- [클라우드 계정 설정 구성](#)
- [클라우드 계정 제거](#)

## 클라우드 계정 추가

아카이브된 데이터를 클라우드에 내보내려면 먼저 Core 콘솔에서 클라우드 공급자의 계정을 추가해야 합니다.

클라우드 계정을 추가하려면 다음을 수행합니다.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. 왼쪽 메뉴에서 **Clouds(클라우드)**를 선택합니다.
3. **Clouds(클라우드)** 페이지에서 **Add New Account(새 계정 추가)**를 클릭합니다.

**Add New Account(새 계정 추가)** 대화 상자가 열립니다.

4. **Cloud Type(클라우드 유형)** 드롭다운 목록에서 호환 가능한 클라우드 공급자를 선택합니다.
5. 4단계에서 선택한 클라우드 유형에 따라 다음 표에 설명된 상세정보를 입력합니다.

**표 1. 클라우드 계정 추가**

클라우드 유형	텍스트 상자	설명
Microsoft Azure	저장소 계정 이름	Windows Azure 저장소 계정의 이름을 입력합니다.
	액세스 키	해당 계정의 액세스 키를 입력합니다.
	표시 이름	AppAssure에서 이 계정의 표시 이름을 만듭니다(예: Windows Azure 1).
Amazon S3	액세스 키	Amazon 클라우드 계정의 액세스 키를 입력합니다.
	암호 키	이 계정의 암호 키를 입력합니다.
	표시 이름	AppAssure에서 이 계정의 표시 이름을 만듭니다(예: Amazon 1).
OpenStack 제공	사용자 이름	OpenStack 기반 클라우드 계정의 사용자 이름을 입력합니다.
	API 키	해당 계정의 API 키를 입력합니다.
	표시 이름	AppAssure에서 이 계정의 표시 이름을 만듭니다(예: OpenStack 1).
	테넌트 ID	이 계정의 테넌트 ID를 입력합니다.
Rackspace Cloud Block Storage	인증 URL	이 계정의 인증 URL을 입력합니다.
	사용자 이름	Rackspace 클라우드 계정의 사용자 이름을 입력합니다.
	API 키	이 계정의 API 키를 입력합니다.
	표시 이름	AppAssure에서 이 계정의 표시 이름을 만듭니다(예: Rackspace 1).

6. **Add(추가)**를 클릭합니다.

대화 상자가 닫히고 Core 콘솔의 **Clouds(클라우드)** 페이지에 계정이 표시됩니다.

## 클라우드 계정 편집

클라우드 계정을 편집하려면 다음 단계를 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. 왼쪽 메뉴에서 **Clouds(클라우드)**를 선택합니다.
3. 편집할 클라우드 계정 옆의 드롭다운 메뉴를 클릭하고 **Edit(편집)**를 클릭합니다.  
**Edit Account(계정 편집)** 창이 열립니다.
4. 필요에 따라 상세정보를 편집한 다음 **Save(저장)**를 클릭합니다.



**노트:** 클라우드 유형은 편집할 수 없습니다.

## 클라우드 계정 설정 구성

클라우드 구성 설정에서는 AppAssure가 클라우드 계정에 연결을 시도하는 횟수와 제한 시간이 초과되기 전에 연결 시도에 소요되는 시간을 결정할 수 있습니다.

클라우드 계정의 연결 설정을 구성하려면 다음을 수행합니다.


1. Core 콘솔에서 **Configuration(구성)** 탭을 클릭합니다.
2. 왼쪽 메뉴에서 **Settings(설정)**를 선택합니다.
3. **Settings(설정)** 페이지에서 **Cloud Configuration(클라우드 구성)**까지 아래로 스크롤합니다.
4. 구성할 클라우드 계정 옆에 있는 드롭다운 메뉴를 클릭하고 다음 중 하나를 수행합니다.
  - **Edit(편집)**를 클릭합니다.  
**Cloud Configuration(클라우드 구성)** 대화 상자가 나타납니다.
    1. 위쪽 및 아래쪽 화살표를 사용하여 다음 옵션 중 하나를 편집합니다.
      - **Request Timeout(요청 시간 제한):** 지연이 발생했을 때 AppAssure가 클라우드 계정에 연결을 한 번 시도하는 데 소요되는 시간으로서 분 및 초로 표시됩니다. 입력된 시간이 초과되면 연결 시도가 중지됩니다.
      - **Retry Count(재시도 횟수):** 클라우드 계정에 연결할 수 없다고 판단될 때까지 AppAssure가 수행해야 할 연결 시도 횟수입니다.
      - **Write Buffer Size(쓰기 버퍼 크기):** 아카이브된 데이터를 클라우드에 쓰기 위해 예약되는 버퍼 크기입니다.
      - **Read Buffer Size(읽기 버퍼 크기):** 클라우드에서 아카이브된 데이터를 읽기 위해 예약되는 블록 크기입니다.
    2. **Next(다음)**를 클릭합니다.
  - **Reset(재설정)**을 클릭합니다. 다음과 같은 기본 설정으로 구성이 다시 설정됩니다.
    - **Request Timeout(요청 시간 제한):** 01:30(분 및 초)
    - **Retry Count(재시도 횟수):** 3(시도 횟수)

## 클라우드 계정 제거

클라우드 계정을 제거하여 클라우드 서비스의 연결을 끊거나 특정 Core에서의 사용을 중지할 수 있습니다. 클라우드 계정을 제거하려면 다음을 수행합니다.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. 왼쪽 메뉴에서 **Clouds(클라우드)**를 선택합니다.
3. 편집할 클라우드 계정 옆의 드롭다운 메뉴를 클릭하고 **Remove(제거)**를 클릭합니다.


4. **Delete Account(계정 삭제)** 창에서 **Yes(예)**를 클릭하여 제거를 확인합니다.
5. 현재 클라우드 계정을 사용하고 있는 경우, 보조 창에 제거할지 묻는 메시지가 나타납니다. **Yes(예)**를 클릭하여 확인합니다.

 **노트:** 현재 사용 중인 계정을 제거하면 이 계정에 예약된 모든 아카이브 작업에 실패합니다.

## 복제 이해

### 워크스테이션 및 서버 보호 정보

데이터를 보호하려면 Core 콘솔에서 보호할 워크스테이션과 서버(예: Exchange Server, SQL Server 또는 Linux 서버)를 추가해야 합니다.


 **노트:** 이 섹션에서는 일반적으로 *시스템*이라는 단어가 해당 시스템에 설치된 AppAssure 에이전트 소프트웨어를 나타냅니다.

Core 콘솔에서 AppAssure 에이전트 소프트웨어가 설치된 시스템 식별, 보호할 볼륨 지정, 보호 일정 정의 및 추가적인 보안 조치 추가(예: 암호화) 등을 수행할 수 있습니다. 워크스테이션 및 서버를 보호하기 위해 Core 콘솔에 액세스하는 방법에 대한 자세한 내용은 [시스템 보호](#)를 참조하십시오.

### 복제 정보

복제는 복구 지점을 복사하고 재난 복구를 위해 보조 위치에 전송하는 프로세스입니다. 이 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. 가능한 복제 시나리오는 다음과 같습니다.

- **로컬 위치에 복사.** 대상 Core가 로컬 데이터 센터 또는 온사이트 위치에 있으며 항상 복제가 유지 보수됩니다. 이 구성에서는 Core가 유실되어도 복구가 가능합니다.
- **오프 사이트 위치에 복사.** 유실이 될 경우 복구할 수 있도록 대상 Core가 오프사이트 재난 복구 시설에 있습니다.
- **Mutual Replication(상호 복제).** 서로 다른 두 위치에 있는 두 데이터 센터에 각각 Core가 포함되어 있으며, 에이전트를 보호하고 서로에 대해 오프사이트 재난 복구 백업 역할을 합니다. 이 시나리오에서는 각 Core가 보호되는 시스템을 다른 데이터 센터에 있는 Core에 복제합니다.
- **호스트 및 클라우드 복제.** AppAssure MSP 파트너가 데이터 센터 또는 공용 클라우드에서 여러 대상 Core를 유지 보수합니다. 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.

- **Point to Point(지점간).** 단일 소스 Core에서 단일 대상 Core로 하나의 보호되는 시스템을 복제합니다.

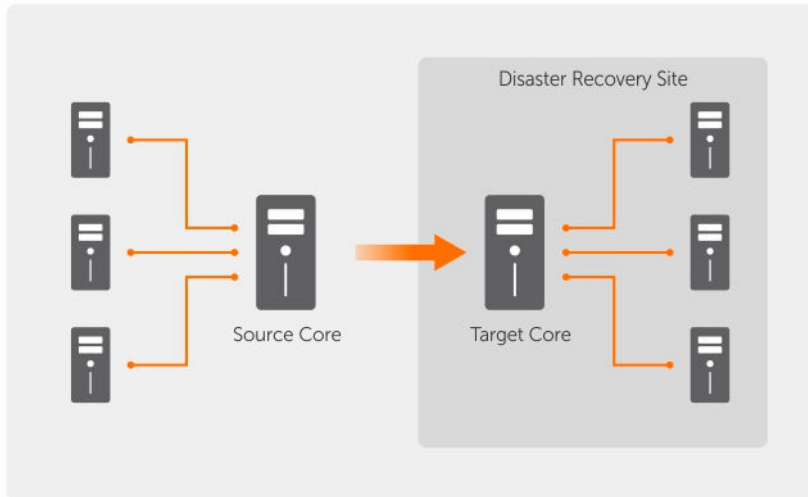


그림 7. 기본 복제 아키텍처 다이어그램

- 다중 지점간: 다중 소스 Core에서 단일 대상 Core로 복제합니다.

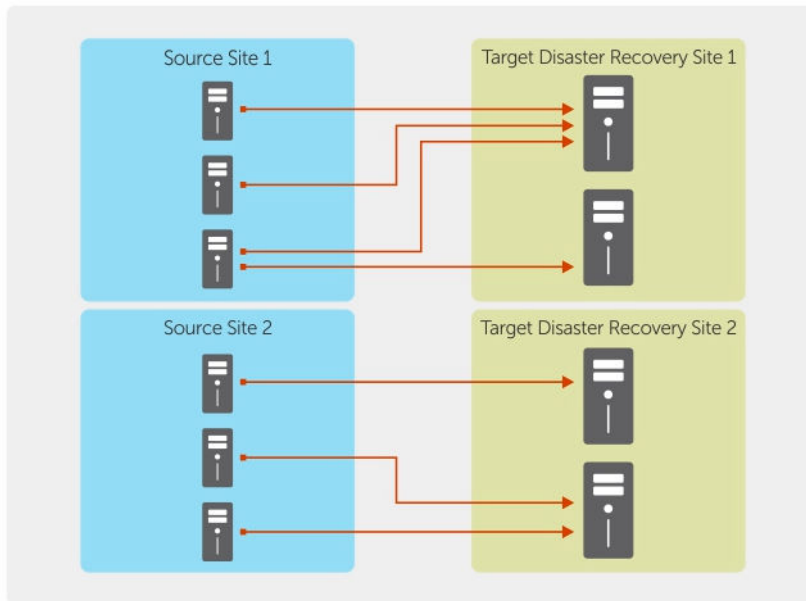


그림 8. 다중 지점 복제 아키텍처 다이어그램

## 시드 정보


복제는 중복 제거된 기본 이미지와 보호되는 시스템의 증분 스냅샷의 초기 전송인 시드를 통해 시작되며, 데이터를 수백 또는 수천 기가바이트까지 추가할 수 있습니다. 초기 데이터를 대상 Core에 전송하기 위해 외부 미디어를 사용하여 초기 복제를 대상 Core에 시드할 수 있습니다. 이는 일반적으로 링크 속도가 느린 대규모 데이터 세트 또는 사이트에 유용합니다.

**노트:** 네트워크 연결을 통해 기본 데이터를 시드할 수 있지만 이는 권장되지 않는 방법입니다. 초기 시드에는 일반 WAN 연결에서 감당할 수 없는 대량 데이터가 잠재적으로 포함됩니다. 예를 들어, 시드 데이터가 10GB이고 WAN 링크가 24Mbps를 전송하는 경우 전송을 완료하는 데 40일 이상 걸릴 수 있습니다.

시드 아카이브의 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. 시드 과정에서 증분 복구 지점이 대상 사이트에 복제됩니다. 대상 Core에서 시드 아카이브를 모두 사용하면 새로 복제된 증분 복구 지점이 자동으로 동기화됩니다.

시드는 다음과 같은 두 개의 부분으로 구성된 프로세스(복사 후 소모라고도 함)로 수행됩니다.

- 첫 번째 부분에서는 초기 복제 데이터를 이동식 미디어 원본에 쓰는 복사가 수행됩니다. 복사하면 소스 Core의 모든 기존 복구 지점이 USB 드라이브와 같은 로컬 이동식 저장 장치에 복제됩니다. 복사가 완료되면 드라이브를 소스 Core 위치에서 원격 대상 Core 위치로 전송해야 합니다.
- 두 번째 부분에서는 대상 Core에서 전송된 드라이브를 수신하고 복제된 데이터를 리포지토리에 복사할 때 발생하는 소모가 수행됩니다. 대상 Core에서 복구 지점을 소모하고 이를 사용하여 복제된 보호되는 시스템 구성합니다.

 **노트:** 시드가 완료되기 전에 소스 Core와 대상 Core 간에 증분 스냅샷의 복제가 발생할 수 있지만 소스에서 대상으로 전송된 복제된 스냅샷은 초기 데이터가 소모될 때까지 "분리"된 상태로 남아 있게 되며, 복제된 기본 이미지와 결합됩니다.

휴대용 저장 장치에 대량 데이터를 복사해야 하므로 휴대용 저장 장치에 eSATA, USB 3.0 또는 기타 고속 연결 장치를 사용하는 것이 좋습니다.

## 장애 조치 및 장애 복구 정보

소스 Core 및 보호되는 시스템이 실패하는 심각한 정전이 발생한 경우 DL 어플라이언스가 복제 환경에서 장애 조치 및 장애 복구를 지원합니다. 장애 조치는 시스템에 오류가 발생하거나 소스 Core 및 연결된 보호되는 시스템이 비정상적으로 종료된 경우 중복 또는 대기 대상 Core로 전환되는 것을 말합니다. 장애 조치의 기본적인 목적은 실패한 소스 Core에 의해 보호된 실패한 에이전트와 동일한 새 에이전트를 시작하는 것입니다. 부수적인 목적은 오류가 발생하기 전에 소스 Core가 초기 에이전트를 보호한 방식과 동일하게 대상 Core가 장애 조치 에이전트를 보호할 수 있도록 대상 Core를 새 모드로 전환하는 것입니다. 대상 Core가 복제된 에이전트로부터 인스턴스를 복구하고 장애 조치된 시스템에서 즉시 보호를 시작할 수 있습니다.


장애 복구는 보호되는 시스템과 Core를 원래 상태(오류 발생 전)로 다시 복원하는 프로세스입니다. 장애 복구의 주요 목적은 보호되는 시스템(대부분의 경우 실패한 에이전트를 대체하는 새 시스템)을 새 임시 에이전트의 최신 상태와 동일한 상태로 복원하는 것입니다. 복원되면 해당 에이전트가 복원된 소스 Core에 의해 보호됩니다. 또한 복제가 복원되고 대상 Core가 다시 복제 대상 역할을 수행합니다.

## 복제 및 암호화된 복구 지점 정보

시드 드라이브에는 소스 Core 레지스트리와 인증서의 백업이 포함되어 있지 않지만, 소스에서 대상으로 복제되는 복구 지점이 암호화된 경우에는 시드 드라이브에 소스 Core의 암호화 키가 포함됩니다. 복제된 복구 지점은 대상 Core에 전송된 후 암호화된 상태로 유지됩니다. 대상 Core의 소유자 또는 관리자가 암호화된 데이터를 복구하려면 암호가 필요합니다.

## 복제에 대한 보존 정책 정보

복제 작업에서 병합된 롤업 또는 임시 삭제로 인해 생성되는 복구 지점을 전송하므로 소스 Core에 대한 보존 정책에 따라 대상 Core에 복제된 데이터에 대한 보존 정책이 결정됩니다.

 **노트:** 대상 Core에서는 복구 지점의 롤업 또는 임시 삭제를 수행할 수 없습니다. 이러한 작업은 소스 Core에서만 수행할 수 있습니다.

## 복제된 데이터 전송에 대한 성능 고려 사항

소스 Core와 대상 Core 간의 대역폭에서 저장된 복구 지점의 전송을 수용할 수 없는 경우 복제 시 소스 Core에서 보호되는 선택한 서버의 기본 이미지 및 복구 지점으로 대상 Core의 시드가 시작됩니다. 시드 프로세스는 정기 예약된 복제에 필요한 기본 역할을 수행하므로 한 번만 수행해야 합니다.

복제를 준비할 때 다음 요소를 고려해야 합니다.

### 변경률

변경률은 보호된 데이터의 용량이 누적되는 비율입니다. 이 비율은 보호된 볼륨 및 해당 볼륨의 보호 간격이 변경되는 데이터 양에 따라 달라집니다. 볼륨에서 블록의 세트가 변경되는 경우 보호 간격을 줄이면 변경률도 감소됩니다.

### 대역폭

대역폭은 소스 Core와 대상 Core 간에 사용 가능한 전송 속도입니다. 스냅샷에서 생성된 복구 지점을 유지하기 위해 복제에 대한 변경률보다 대역폭이 커야 합니다. Core 간에 전송되는 데이터 양으로 인해 최대 1GB의 이더넷 연결 속도까지의 최대 회선 용량에서 작업을 수행하려면 다중 병렬 스트림이 필요할 수 있습니다.



**노트:** ISP에 의해 지정되는 대역폭은 총 사용 가능한 대역폭입니다. 발신 대역폭은 네트워크의 모든 장치에서 공유됩니다. 변경률을 수용하기 위해 복제에 사용 가능한 대역폭이 충분히 있는지 확인하십시오.

### 보호되는 시스템 수

소스 Core당 보호되는 시스템 수와 대상에 복제할 시스템 수를 고려해야 합니다. AppAssure에서는 보호된 서버별로 복제를 수행할 수 있으므로 특정 서버를 복제하도록 선택할 수 있습니다. 이는 보호된 서버를 모두 복제해야 하는 경우 특히, 소스 Core와 대상 Core 간의 대역폭이 복제되는 복구 지점의 양과 크기에 비해 부족한 경우 변경률에 크게 영향을 미칩니다.

네트워크 구성에 따라 복제하는 데 시간이 오래 걸릴 수 있습니다.

다음 표에 적절한 변경률에 필요한 기가바이트당 대역폭의 예가 나와 있습니다.



**노트:** 최적의 결과를 얻을 수 있도록 다음 표에 나열된 권장 사항을 준수하십시오.

## WAN 연결 유형에 대한 최대 변경률

표 2. WAN 연결 유형에 대한 최대 변경률

광대역	대역폭	최대 변경률
DSL	768Kbps 이상	330MB/시간
케이블	1Mbps 이상	429MB/시간
T1	1.5Mbps 이상	644MB/시간
파이버	20Mbps 이상	838GB/시간

데이터를 전송하는 동안 링크가 끊어진 경우 링크 기능이 복원되면 이전에 전송이 실패한 지점에서 계속해서 복제가 다시 시작됩니다.

## 복제 수행을 위한 로드맵

AppAssure를 사용하여 데이터를 복제하려면 복제할 수 있도록 소스 및 대상 Core를 구성해야 합니다. 복제를 구성한 후 보호되는 시스템의 데이터를 복제하고, 복제를 모니터 및 관리하고, 복구를 수행할 수 있습니다.




AppAssure에서 다음과 같은 작업으로 복제를 수행합니다.

- 자체 관리 복제를 구성합니다. 자체 관리 대상 Core에 복제는 [자체 관리 Core에 복제](#)를 참조합니다.
- 타사 복제를 구성합니다. 타사 대상 Core 복제에 대한 자세한 내용은 [타사 관리 Core에 복제](#)를 참조합니다.
- 소스 Core에 첨부된 새 보호되는 시스템을 복제합니다. 보호되는 시스템 복제에 대한 자세한 내용은 [새 보호되는 시스템 복제](#)를 참조하십시오.
- 기존의 보호되는 시스템을 복제합니다. 복제를 위한 에이전트 구성에 대한 자세한 내용은 [시스템에서 에이전트 데이터 복제](#)를 참조하십시오.
- 에이전트의 복제 우선순위를 설정합니다. 에이전트의 복제 우선순위 설정에 대한 자세한 내용은 [에이전트에 대한 복제 우선순위 설정](#)을 참조하십시오.
- 필요한 경우 복제를 모니터링합니다. 복제 모니터링에 대한 자세한 내용은 [복제 모니터링](#)을 참조하십시오.
- 필요에 따라 복제 설정을 관리합니다. 복제 설정 관리에 대한 자세한 내용은 [복제 설정 관리](#)를 참조하십시오.
- 재난 또는 데이터 유실이 발생할 경우 복제된 데이터를 복구합니다. 복제된 데이터 복구에 대한 자세한 내용은 [복제된 데이터 복구](#)를 참조하십시오.

## 자체 관리 Core에 복제

자체 관리 Core는 사용자 회사가 오프사이트 위치에서 관리되므로 사용자가 액세스 권한을 가지는 코어입니다. 데이터를 시드하도록 선택한 경우가 아니라면 소스 Core에서 복제를 완전히 수행할 수 있습니다. 시드를 수행하려면 소스 Core에서 복제를 구성한 후에 대상 Core에서 시드 드라이브를 사용해야 합니다.

 **노트:** 이 구성은 오프사이트 위치에 복제 및 상호 복제에 적용됩니다. 모든 소스 및 대상 시스템에 Core가 설치되어 있어야 합니다. 다중 지점 간 복제를 수행하도록 장치를 구성하는 경우 모든 소스 Core 및 대상 Core에서 이 작업을 수행해야 합니다.

### 자체 관리 대상 Core에 복제하도록 소스 Core 구성

자체 관리 대상 Core에 복제하도록 소스 Core를 구성하려면 다음을 수행합니다.


1. Core에서 **Replication(복제)** 탭을 클릭합니다.
2. **Add Target Core(대상 Core 추가)**를 클릭합니다.  
**Replication(복제)** 마법사가 나타납니다.
3. **I have my own Target Core(고유 대상 Core 있음)**를 선택하고 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
호스트 이름	복제할 Core 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
포트	AppAssure Core가 시스템과 통신하는 포트 번호를 입력합니다. 기본 포트 번호는 8006입니다.
사용자 이름	시스템에 액세스할 사용자 이름을 입력합니다(예: <b>Administrator</b> ).
암호	시스템에 액세스할 암호를 입력합니다.

추가할 Core가 이전에 이 소스 Core와 쌍을 이루고 있었다면 다음을 수행하십시오.

- a. **Use an existing target core(기존 대상 Core 사용)**를 선택합니다.
- b. 드롭다운 목록에서 대상 Core를 선택합니다.
- c. **Next(다음)**를 클릭합니다.

- d. 7단계로 건너뛰니다.
4. **Next(다음)**를 클릭합니다.
  5. **Details(상세정보)** 페이지에서, 이 복제 구성의 이름을 입력합니다(예: SourceCore1). 이전의 복제 구성을 다시 시작하거나 복구하는 경우에는 **My Core has been migrated and I would like to repair replication(내 Core가 마이그레이션 되었으며 복제를 복구함)**을 선택합니다.
  6. **Next(다음)**를 클릭합니다.
  7. **Agents(에이전트)** 페이지에서 복제할 에이전트를 선택하고 **Repository(리포지토리)** 열에 있는 드롭다운 목록에서 각 에이전트의 리포지토리를 선택합니다.
  8. 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. **Agents(에이전트)** 페이지에서 **Use a seed drive to perform initial transfer(시드 드라이브를 사용하여 초기 전송 수행)**를 선택합니다. 현재 대상 Core에 복제할 시스템이 하나 이상 있는 경우에는 **With already replicated(이미 복제된 항목 사용)**를 선택하여 시드 드라이브에서 이러한 보호되는 시스템을 포함할 수 있습니다.
  - b. **Next(다음)**를 클릭합니다.
  - c. **Seed Drive Location(시드 드라이브 위치)** 페이지에서, **Location type(위치 유형)** 드롭다운 목록을 사용하여 다음 중 하나를 선택합니다.
    - 로컬: **Location(위치)** 텍스트 상자에서, 시드 드라이브를 저장할 위치를 입력합니다(예: D:\work\archive).
    - 네트워크: **Location(위치)** 텍스트 상자에서, 시드 드라이브를 저장할 위치를 입력하고 **User name(사용자 이름)** 및 **Password(암호)** 텍스트 상자에 네트워크 공유의 자격 증명을 입력합니다.
    - 클라우드: **계정** 텍스트 상자에서 계정을 선택합니다. 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다. 자세한 내용은 [클라우드 계정 추가](#)를 참조합니다. 계정과 연결된 **컨테이너**를 선택합니다. 아카이브된 데이터가 저장될 **폴더 이름**을 선택합니다.
  - d. 다음을 누릅니다.
9. **Seed Drive Option(시드 드라이브 옵션)** 대화 상자에, 아래에 설명된 정보를 입력합니다.

#### 텍스트 상자      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\archive일 경우 시드 드라이브를 복사할 때 필요하면 D: 드라이브에 있는 모든 사용 가능한 공간이 예약되지만 복사 프로세스가 시작된 후 곧바로 예약되지는 않습니다.
  - 빈 텍스트 상자를 선택하고 공간의 양을 입력한 다음 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다.

**Customer ID(고객 ID) (선택사항)**      선택적으로, 서비스 공급자가 할당한 고객 ID를 입력합니다.

- 재활용 작업**      경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다.
- **Do not reuse(재사용 안 함)** - 위치에서 기존 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있는 경우 시드 드라이브 쓰기가 실패합니다.
  - **Replace this core(이 Core 대체)** - 이 Core와 관련된 기존 데이터를 덮어쓰지만 다른 Core의 데이터는 그대로 남아 있게 됩니다.

## 텍스트 상자 설명

- **Erase completely(완전히 지우기)** - 시드 드라이브를 쓰기 전에 디렉터리에서 모든 데이터를 지웁니다.

**주석** 아카이브에 대한 주석 또는 설명을 입력합니다.

**Add all Agents to Seed Drive(시드 드라이브에 모든 에이전트 추가)** 시드 드라이브를 사용하여 복제할 에이전트를 선택합니다.

**Build RP Chain(RP 망 빌드) (분리 문제 해결)** 전체 복구 지점망을 시드 드라이브에 복제하려면 이 옵션을 선택합니다. 이 옵션은 기본으로 선택되어 있습니다.

AppAssure에서 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 에이전트의 최신 복구 지점을 저장할 수 있는 충분한 공간이 시드 드라이브에 있어야 하며 작업이 완료되는 데 추가적인 시간이 소요될 수 있습니다.

**호환되는 형식 사용** 최신 버전 및 이전 버전의 AppAssure Core와 호환되는 형식으로 시드 드라이브를 생성하려면 이 옵션을 선택합니다.

**10. Agents(에이전트)** 페이지에서, 시드 드라이브를 사용하여 대상 Core에 복제할 에이전트를 선택합니다.

**11. Finish(마침)**를 클릭합니다.

**12.** 시드 드라이브를 생성한 후 대상 Core에 전송합니다.

소스 Core와 대상 Core 쌍이 생성됩니다. 복제가 시작됩니다. 하지만 시드 드라이브가 사용되기 전까지는 대상 Core에 분리된 복구 지점이 생성되며 필요한 기본 이미지가 제공됩니다.

## 대상 Core에서 시드 드라이브 사용

이 절차는 자체 관리 Core의 복제 구성을 수행하는 동안 시드 드라이브를 생성한 경우에만 적용됩니다. 대상 Core에서 시드 드라이브를 사용하려면 다음을 수행합니다.

1. 시드 드라이브가 휴대용 저장소 장치(예: USB)에 저장된 경우 드라이브를 대상 Core에 연결합니다.
2. 소스 Core의 Core 콘솔에서 **Replication(복제)** 탭을 선택합니다.
3. **Incoming Replication(들어오는 복제)**에서, 드롭다운 메뉴를 사용하여 소스 Core를 선택하고 **Consume(사용)**을 클릭합니다.  
Consume(사용) 창이 나타납니다.
4. 드롭다운 목록에서 다음 옵션 중 하나를 **Location Type(위치 유형)**으로 선택합니다.
  - 로컬
  - 네트워크
  - 클라우드
5. 필요에 따라 다음 정보를 입력합니다.

## 텍스트 상자 설명


**위치** USB 드라이브 또는 네트워크 공유와 같은 시드 드라이브가 있는 경로를 입력합니다.(예: D:\).

텍스트 상자	설명
사용자 이름	공유 드라이브 또는 폴더의 사용자 이름을 입력합니다. 사용자 이름은 네트워크 경로에만 필요합니다.
암호	공유 드라이브 또는 폴더의 암호를 입력합니다. 암호는 네트워크 경로에만 필요합니다.
계정	드롭다운 목록에서 계정을 선택합니다. 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다.
컨테이너	드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
폴더 이름	아카이브된 데이터가 저장된 폴더 이름을 입력합니다. 예를 들어, -아카이브 - [생성 날짜] - [생성 시간] 식으로 입력합니다.

6. **Check File(파일 확인)**을 클릭합니다.


Core가 파일을 확인하면 시드 드라이브에 포함된 가장 오래된 복구 지점과 가장 최근의 복구 지점의 날짜로 **Date Range(날짜 범위)**가 자동으로 채워집니다. 또한 자체 관리 Core의 복제 구성 시에 입력된 모든 주석을 가져옵니다.

7. **Consume(사용)** 창의 **Agent Names(에이전트 이름)**에서, 데이터를 사용할 시스템을 선택하고 **Consume(사용)**을 클릭합니다.

 **노트:** 데이터 사용 진행률을 모니터링하려면 **Events(이벤트)** 탭을 선택합니다.

## 대기 중인 시드 드라이브 중단

대상 Core에 사용하기 위해 시드 드라이브를 생성했지만 원격 위치로는 전송하지 않으려고 선택한 경우, 대기 중인 시드 드라이브의 링크가 소스 Core의 **Replication(복제)** 탭에 남아 있습니다. 다른 시드 데이터 또는 최근의 시드 데이터를 위해 대기 중인 시드 드라이브를 중단해야 합니다.


 **노트:** 이 절차를 수행하면 소스 Core의 Core 콘솔에서 대기 중인 시드 드라이브의 링크가 제거됩니다. 이 드라이브가 저장되어 있는 저장소 위치에서는 제거되지 않습니다.

대기 중인 시드 드라이브를 중단하려면 다음을 수행합니다.


1. 소스 Core의 Core 콘솔에서 **Replication(복제)** 탭을 선택합니다.
2. **Outstanding Seed Drive (#)(대기 중인 시드 드라이브 수)**를 클릭합니다.  
**Outstanding seed drives(대기 중인 시드 드라이브)** 섹션이 표시됩니다. 여기에는 원격 대상 Core의 이름, 시드 드라이브가 생성된 날짜 및 시간, 시드 드라이브에 포함된 복구 지점의 데이터 범위가 포함됩니다.
3. 중단할 드라이브의 드롭다운 메뉴를 클릭하고 **Abandon(중단)**을 선택합니다.  
**Outstanding Seed Drive(대기 중인 시드 드라이브)** 창이 표시됩니다.
4. **Yes(예)**를 클릭하여 작업을 확인합니다.  
시드 드라이브가 제거됩니다. 소스 Core에 더 이상 시드 드라이브가 없으면 다음에 **Replication(복제)** 탭을 열 때 **Outstanding Seed Drive (#)(대기 중인 시드 드라이브 수)** 링크 및 **Outstanding seed drives(대기 중인 시드 드라이브)** 섹션이 표시되지 않습니다.

## 타사 관리 Core에 복제

타사 Core는 MSP에서 관리하고 유지하는 대상 Core입니다. 타사에서 관리하는 Core에 복제할 때는 대상 Core에 대한 액세스 권한이 필요하지 않습니다. 고객이 소스 Core에 복제를 구성하면 MSP가 대상 Core에 구성을 완료합니다.

 **노트:** 이 구성은 호스트된 클라우드 복제에 적용됩니다. 모든 소스 Core 시스템에 AppAssure Core를 설치해야 합니다.

### 타사 관리 대상 Core에 대한 복제 구성

 **노트:** 이 구성은 호스트 및 클라우드 복제에 적용됩니다. 다중 지점 간 복제를 수행하도록 AppAssure를 구성하는 경우 모든 소스 Core에서 이 작업을 수행해야 합니다.

타사에서 관리하는 Core에 대한 복제를 구성하려면 다음을 수행하십시오.


1. Core 콘솔로 이동하여 **Replication(복제)** 탭을 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Add Remote Core(원격 Core 추가)**를 클릭합니다.
3. **Select Replication Type(복제 유형 선택)** 대화 상자에서 **I have a subscription to a third-party providing off-site backup and disaster recovery services, and wish to replicate my backups to that service(타사에서 제공하는 오프사이트 백업 및 재난 복구 서비스에 등록되어 있으며 해당 서비스에 내 백업을 복제합니다)** 옵션을 선택한 후 아래에 설명된 대로 정보를 입력합니다.

#### 텍스트 상자      설명

**호스트 이름**      원격 Core 시스템에 대한 호스트 이름, IP 주소 또는 FQDN을 입력합니다.

**포트**      타사 서비스 공급자가 제공한 포트 번호를 입력합니다.  
기본 포트 번호는 8006입니다.

4. **Continue(계속)**를 클릭합니다.
5. **Add Remote Core(원격 Core 추가)** 대화 상자에서 다음을 수행합니다.
  - a. 복제할 보호되는 시스템을 선택합니다.
  - b. 보호되는 시스템 각각에 대한 리포지토리를 선택합니다.
  - c. 구독 전자 메일 주소와 서비스 공급자가 할당한 고객 ID를 입력합니다.
6. 기본 데이터를 전송하기 위해 시드 프로세스를 수행하려면 **Use a seed drive to perform initial transfer(시드 드라이브를 사용하여 초기 전송 수행)**를 선택합니다.
7. **Submit Request(요청 제출)**를 클릭합니다.


 **노트:** **Use a seed drive to perform initial transfer(시드 드라이브를 사용하여 초기 전송 수행)**를 선택하면 **Copy to Seed Drive(시드 드라이브에 복사)** 대화 상자가 표시됩니다.

8. **Copy to Seed Drive(시드 드라이브에 복사)** 대화 상자에서 아래 표에 설명된 대로 시드 드라이브에 대한 정보를 입력합니다.


#### 텍스트 상자      설명

**Location(위치)**      로컬 USB 드라이브와 같이 초기 데이터를 저장할 드라이브에 대한 경로를 입력합니다.

**사용자 이름**      드라이브를 연결할 사용자 이름을 입력합니다.

 **노트:** 시드 드라이브가 네트워크 공유에 있는 경우 이는 필수입니다.

**암호**      드라이브를 연결할 암호를 입력합니다.

 **노트:** 시드 드라이브가 네트워크 공유에 있는 경우 이는 필수입니다.

**최대 크기**      다음 옵션 중 하나를 선택합니다.

- 전체 대상

## 텍스트 상자 설명

- 드라이브의 사용 가능한 공간의 일부입니다.

드라이브의 일부를 지정하려면 다음을 수행합니다.

- a. 텍스트 상자에 원하는 양의 공간을 입력합니다.
- b. 관리를 선택합니다.

## 재활용 작업

경로에 이미 시드 드라이브가 포함되어 있는 경우 다음 옵션 중 하나를 선택합니다.

- **Do not reuse(재사용 안 함)** - 위치에서 기존 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있는 경우 시드 드라이브 쓰기가 실패합니다.
- **Replace this core(이 Core 대체)** - 이 Core와 관련된 기존 데이터를 덮어쓰지만 다른 Core의 데이터는 그대로 남아 있게 됩니다.
- **Erase completely(완전히 지우기)** - 시드 드라이브를 쓰기 전에 디렉터리에서 모든 데이터를 지웁니다.

## 주석

아카이브에 대한 주석 또는 설명을 입력합니다.

## 에이전트

시드 드라이브를 사용하여 복제할 에이전트를 선택합니다.



**노트:** 휴대용 저장 장치에 대량 데이터를 복사해야 하므로 휴대용 저장 장치에 eSATA, USB 3.0 또는 기타 고속 연결 장치를 사용하는 것이 좋습니다.

9. **Start(시작)**를 클릭하여 제공한 경로에 시드 드라이브를 씁니다.

10. 타사 서비스 공급자의 지시에 따라 시드 드라이브를 보냅니다.

## 복제 요청 검토

소스 Core에서 타사 대상 Core로 복제 요청이 전송됩니다. 타사 사용자는 요청을 검토하여 승인한 후 고객을 위해 복제를 시작하거나 복제를 거부할 수 있습니다.

타사 대상 Core에서 복제 요청을 검토하려면 다음을 수행합니다.

1. 대상 Core의 Core 콘솔을 열고 **Replication(복제)** 탭을 선택합니다.

2. **Pending Requests (#)(보류 중인 요청 수)**를 클릭합니다.

**Pending Replication Requests(보류 중인 복제 요청)** 섹션이 표시됩니다.

3. 검토할 요청 옆에 있는 드롭다운 목록에서 **Review(검토)**를 선택합니다.

**Review Replication Request(복제 요청 검토)** 창이 표시됩니다.



**노트:** 고객이 입력한 요청에 따라 **Source Core Identity(소스 Core ID)** 섹션에 나타나는 정보가 결정됩니다.

4. Review Replication Request(복제 요청 검토) 창에서 다음 중 하나를 수행합니다.

- 요청을 거부하려면 **Deny(거부)**를 클릭합니다.
- 요청을 승인하려면 다음을 수행합니다.

1.
  - **Replace an existing replicated Core(복제된 기존 Core 생성)**를 선택하고 드롭다운 목록에서 Core를 선택합니다.
  - **Create a new source Core(새 소스 Core 생성)**를 선택합니다. **Core Name(Core 이름)**, 고객의 **Email Address(전자 메일 주소)**, **Customer ID(고객 ID)**를 식별하고 필요에 따라 정보를 편집합니다.

2. 선택한 **Agents(에이전트)** 아래에서, 승인되는 시스템을 선택하고 드롭다운 목록에서 각 시스템의 적절한 리포지토리를 선택합니다.
3. **Comment(주석)** 상자에 표시할 메모를 입력할 수 있습니다.
4. **Send Response(응답 보내기)**를 클릭합니다.

복제가 수락됩니다.

## 복제 요청 무시

대상 Core의 타사 서비스 공급자는 고객이 보낸 복제 요청을 무시할 수 있습니다. 이 옵션은 고객이 실수로 요청을 보냈거나 요청을 검토하지 않고 거절하려는 경우에 사용할 수 있습니다.

복제 요청을 무시하려면 다음을 수행합니다.

1. 소스 Core의 Core 콘솔에서 **Replication(복제)** 탭을 선택합니다.
2. Replication(복제) 탭에서 **Pending Requests (#)(보류 중인 요청 수)**를 클릭합니다.  
**Pending Replication Requests(보류 중인 복제 요청)** 섹션이 표시됩니다.
3. 무시할 요청 옆에 있는 드롭다운 메뉴를 사용하여 **Ignore(무시)**를 선택합니다.  
대상 Core가 요청이 무시되었다는 알림을 소스 Core에 보냅니다.

## 복제 모니터링

복제가 설정되면 소스 및 대상 Core에 대한 복제 작업의 상태를 모니터링할 수 있습니다. 상태 정보 새로 고침 및 복제 상세정보 보기 등을 수행할 수 있습니다.

복제를 모니터링하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Replication(복제)** 탭을 클릭합니다.
2. 이 탭에서 복제 작업에 대한 정보를 보고 아래에 설명된 대로 복제 작업의 상태를 모니터링할 수 있습니다.

**표 3. 복제 모니터링**

섹션	설명	사용 가능한 조치
보류 중인 복제 요청	복제 요청이 타사 서비스 공급자에게 제출될 때 고객 ID, 전자 메일 주소 및 호스트 이름이 나열됩니다. MSP가 요청을 수락할 때까지 여기에 나열됩니다.	요청을 무시하거나 거부하려면 드롭다운 메뉴에서 <b>Ignore(무시)</b> 를 클릭합니다.
대기 중인 시드 드라이브	기록되었지만 대상 Core에서 사용되지 않은 시드 드라이브를 나열합니다. 여기에는 원격 Core 이름, 생성 날짜 및 날짜 범위가 포함됩니다.	드롭다운 메뉴에서 <b>Abandon(중단)</b> 을 클릭하여 시드 프로세스를 중단하거나 취소합니다.
보내는 복제	소스 Core가 복제되는 대상 Core를 모두 나열합니다. 여기에는 원격 Core 이름, 존재 상태, 복제 중인 보호되는 시스템 수 및 복제 전송의 진행률이 포함됩니다.	소스 Core의 드롭다운 메뉴에서 다음 옵션을 선택할 수 있습니다. <ul style="list-style-type: none"> <li>• <b>Details(상세정보)</b> - ID, URI, 표시 이름, 상태, 고객 ID, 전자 메일 주소 및 복제된 Core에 대한 주석을 나열합니다.</li> </ul>

섹션	설명	사용 가능한 조치
		<ul style="list-style-type: none"> <li>• <b>Change Settings(설정 변경)</b> - 표시 이름을 나열하며, 이를 통해 대상 Core의 호스트와 포트를 편집할 수 있습니다.</li> <li>• <b>Add Agents(에이전트 추가)</b> - 드롭다운 목록에서 호스트를 선택하고, 복제할 보호되는 시스템을 선택하고, 새 보호되는 시스템의 초기 전송에 대한 시드 드라이브를 생성할 수 있습니다.</li> </ul>
들어오는 복제	대상에서 복제된 데이터를 수신하는 모든 원본 시스템을 나열합니다. 여기에는 원격 Core 이름, 상태, 시스템 및 진행률이 포함됩니다.	<p>대상 Core의 드롭다운 메뉴에서 다음 옵션을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• <b>Details(상세정보)</b> - ID, 호스트 이름, 고객 ID, 전자 메일 주소 및 복제된 Core에 대한 주석을 나열합니다.</li> <li>• <b>Consume(사용)</b> - 시드 드라이브의 초기 데이터를 사용하고 해당 데이터를 로컬 리포지토리에 저장합니다.</li> </ul>

3. **Refresh(새로 고침)** 단추를 클릭하여 이 탭의 섹션을 최신 정보로 업데이트합니다.

## 복제 설정 관리

소스 및 대상 Core에서 복제가 실행되는 방법에 대해 여러 가지 설정을 조정할 수 있습니다.

복제 설정을 관리하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Replication(복제)** 탭을 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Settings(설정)**을 클릭합니다.
3. **Replication Settings(복제 설정)** 창에서 아래에 설명된 대로 복제 설정을 편집합니다.

옵션	설명
캐시 수명	소스 Core에서 수행되는 각 대상 Core 상태 요청 간의 시간을 지정합니다.
볼륨 이미지 세션 시간 제한	소스 Core에서 볼륨 이미지를 대상 Core에 전송하도록 시도하는 데 소요되는 시간을 지정합니다.
최대 동시 복제 작업 수	한 번에 대상 Core에 복제할 수 있도록 허용되는 보호되는 시스템 수를 지정합니다.
최대 병렬 스트림 수	단일 보호되는 시스템에서 한 번에 해당 시스템의 데이터를 복제하는 데 사용할 수 있도록 허용되는 네트워크 연결 횟수를 지정합니다.


4. **Save(저장)**를 클릭합니다.

## 복제 제거

복제를 중단한 후 여러 가지 방법으로 복제에서 보호된 시스템을 제거할 수 있습니다. 다음과 같은 옵션을 사용할 수 있습니다.



- [소스 Core의 복제에서 에이전트 제거](#)
- [대상 Core의 에이전트 제거](#)
- [복제에서 대상 Core 제거](#)
- [복제에서 소스 Core 제거](#)

 **노트:** 소스 Core를 제거하면 해당 Core에 의해 보호되는 복제된 시스템이 모두 제거됩니다.

## 소스 Core의 복제에서 보호되는 시스템 제거

소스 Core의 복제에서 보호되는 시스템을 제거하려면 다음을 수행하십시오.

1. 소스 Core에서 Core 콘솔을 열고 **Replication(복제)** 탭을 클릭합니다.
2. **Outgoing Replication(보내는 복제)** 섹션을 확장합니다.
3. 복제에서 제거할 보호되는 시스템의 드롭다운 메뉴에서 **Delete(삭제)**를 클릭합니다.
4. **Outgoing Replication(보내는 복제)** 대화 상자에서 **Yes(예)**를 클릭하여 삭제를 확인합니다.

## 대상 Core에서 보호되는 시스템 제거

대상 Core에서 보호되는 시스템을 제거하려면 다음을 수행하십시오.

1. 대상 Core에서 Core 콘솔을 열고 **Replication(복제)** 탭을 클릭합니다.
2. **Incoming Replication(들어오는 복제)** 섹션을 확장합니다.
3. 복제에서 제거할 보호되는 시스템의 드롭다운 메뉴에서 **Delete(삭제)**를 클릭한 후 다음 옵션 중 하나를 선택합니다.


옵션	설명
<b>Relationship Only(관계만)</b>	복제에서 보호되는 시스템을 제거하지만 복제된 복구 지점은 그대로 유지합니다.
<b>With Recovery Point(복구 지점 포함)</b>	복제에서 보호되는 시스템을 제거하고 해당 시스템에서 받은 모든 복제된 복구 지점을 삭제합니다.

## 복제에서 대상 Core 제거

복제에서 대상 Core를 제거하려면 다음을 수행하십시오.

1. 소스 Core에서 Core 콘솔을 열고 **Replication(복제)** 탭을 클릭합니다.
2. **Outgoing Replication(보내는 복제)** 아래에서 삭제할 원격 Core 옆에 있는 드롭다운 메뉴를 클릭하고 **Delete(삭제)**를 클릭합니다.
3. **Outgoing Replication(보내는 복제)** 대화 상자에서 **Yes(예)**를 클릭하여 삭제를 확인합니다.

## 복제에서 소스 Core 제거

 **노트:** 소스 Core를 제거하면 해당 Core에 의해 보호되는 복제된 에이전트가 모두 제거됩니다.

복제에서 소스 Core를 제거하려면 다음을 수행하십시오.

1. 대상 Core에서 Core 콘솔을 열고 **Replication(복제)** 탭을 클릭합니다.
2. **Incoming Replication(들어오는 복제)**의 드롭다운 메뉴에서 **Delete(삭제)**를 클릭하고 다음 옵션 중 하나를 선택합니다.

옵션	설명
<b>Relationship Only(관계만)</b>	복제에서 소스 Core를 제거하지만 복제된 복구 지점은 그대로 유지됩니다.
<b>With Recovery Points(복구 지점 포함)</b>	복제에서 소스 Core를 제거하고 해당 시스템에서 받은 모든 복제된 복구 지점을 삭제합니다.

3. **Incoming Replication(들어오는 복제)** 대화 상자에서 **Yes(예)**를 클릭하여 삭제를 확인합니다.

## 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 에이전트와 Core를 복구할 수 있습니다.

대상 Core에서 다음 복구 옵션을 수행할 수 있습니다.

- 복구 지점 탐색
- 복구 지점으로 롤백
- 가상 시스템(VM) 내보내기 수행
- 운영 체제 미설치 복원(BMR) 수행
- 장애 복구 수행(장애 조치/장애 복구 복제 환경이 설정된 경우)

## 장애 조치 및 장애 복구의 로드맵

소스 Core 및 연결된 보호되는 시스템이 실패하는 재난 상황이 발생하면 AppAssure에서 장애 복구를 활성화하여 보호를 동일한 장애 복구(대상) Core로 전환하고 실패한 에이전트와 동일한 새 복제 에이전트를 시작할 수 있습니다. 소스 Core와 에이전트가 복구되면 장애 복구를 수행하여 데이터를 장애 조치된 Core와 에이전트에서 소스 Core와 에이전트로 다시 복원할 수 있습니다. AppAssure에서 장애 조치 및 장애 복구를 수행하려면 다음 절차를 수행해야 합니다.

- 장애 조치에 대한 환경을 설정합니다.
- 대상 Core와 연결된 에이전트에 대한 장애 조치를 수행합니다.
- 장애 복구를 수행하여 소스 Core를 복원합니다.

### 장애 조치에 대한 환경 설정

장애 조치에 대한 환경을 설정하려면 소스 및 대상 Core와 복제 가능하도록 설정된 연관 에이전트가 있어야 합니다. 다음 절차를 수행하여 장애 조치를 위한 복제를 설정합니다.

장애 조치에 대한 환경을 설정하려면 다음을 수행하십시오.

1. 소스 및 대상 Core를 각각 설치합니다.
2. 소스 Core에서 보호할 AppAssure Agent를 설치합니다.
3. 소스 Core와 대상 Core에 각각 하나의 리포지토리를 생성합니다.  
자세한 내용은 [리포지토리 생성](#)을 참조하십시오.
4. 소스 Core 아래에 보호할 에이전트를 추가합니다.  
자세한 내용은 [시스템 보호](#)를 참조하십시오.

5. 소스 및 대상 Core에서 복제를 설정하고 모든 복구 지점과 함께 보호된 에이전트를 복제합니다.

[자체 관리 Core에 복제](#)의 단계에 따라 복제할 대상 Core를 추가합니다.

## 대상 Core의 장애 조치 수행

소스 Core 및 연결된 보호되는 시스템이 실패하는 재난 상황이 발생하면 장애 조치를 활성화하여 보호를 동일한 장애 조치(대상) Core로 전환할 수 있습니다. 대상 Core가 해당 환경에서 데이터를 보호하는 유일한 Core가 되며, 새 에이전트를 시작하여 실패한 에이전트를 일시적으로 대체합니다.

대상 Core의 장애 조치를 수행하려면 다음을 수행하십시오.

1. 대상 Core의 Core 콘솔을 탐색하고 **Replication(복제)** 탭을 클릭합니다.
2. **Incoming Replication(들어오는 복제)**에서 소스 Core를 선택하고 개별 에이전트 아래에서 상세정보를 확장합니다.
3. 해당 Core에 대한 **Actions(작업)** 메뉴에서 **Failover(장애 조치)**를 클릭합니다.  
이 테이블에서 이 시스템에 대한 상태가 **Failover(장애 조치)**로 변경됩니다.
4. **Machines(시스템)** 탭을 클릭한 후 AppAssure 에이전트가 복구 지점과 연결되어 있는 시스템을 선택합니다.
5. 해당 에이전트의 백업 복구 지점 정보를 가상 시스템으로 내보냅니다.
6. AppAssure 에이전트가 있는 시스템을 종료합니다.
7. 이제 내보낸 백업 정보가 포함되어 있는 가상 시스템을 시작합니다.  
장치 드라이버 소프트웨어가 설치되는 동안 기다려야 합니다.
8. 가상 시스템을 재부팅하고 에이전트 서비스가 시작될 때까지 기다립니다.
9. 대상 Core의 Core 콘솔로 다시 돌아가 **Protected Machines(보호된 시스템)** 아래의 **Machines(시스템)** 탭과 **Incoming Replication(들어오는 복제)** 아래의 **Replication(복제)** 탭에 새 에이전트가 표시되는지 확인합니다.
10. 여러 개의 스냅샷을 강제 적용하고 올바르게 완료되는지 확인합니다.  
자세한 내용은 [스냅샷 강제 적용](#)을 참조하십시오.
11. 이제 계속해서 장애 복구를 진행할 수 있습니다.  
자세한 내용은 [장애 복구 수행](#)을 참조하십시오.


## 장애 복구 수행

실패한 원래 소스 Core와 보호되는 시스템을 복구하거나 교체한 후 장애 조치된 시스템의 데이터를 이동하여 원본 시스템을 복원해야 합니다.

장애 복구를 수행하려면 다음을 수행하십시오.

1. 대상 Core의 Core 콘솔을 탐색하고 **Replication(복제)** 탭을 클릭합니다.
2. **Incoming Replication(들어오는 복제)** 아래에서 장애 조치 에이전트를 선택하고 상세정보를 확장합니다.
3. **Actions(작업)** 메뉴에서 **Failback(장애 복구)**를 클릭합니다.  
**Start Failback(장애 복구 시작)** 단추를 클릭하기 전에 수행해야 하는 단계를 설명하는 **Failback Warnings(장애 복구 경고)** 대화 상자가 열립니다.
4. **Cancel(취소)**를 클릭합니다.
5. 장애 조치된 시스템에서 Microsoft SQL Server 또는 Microsoft Exchange Server를 실행 중인 경우 해당 서비스를 중지합니다.
6. 대상 Core에 대한 Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
7. 장애 조치된 에이전트의 아카이브를 생성하고 디스크 또는 네트워크 공유 위치에 출력합니다.
8. 아카이브를 생성한 후 새로 복구된 소스 Core의 Core 콘솔을 탐색하고 **Tools(도구)** 탭을 클릭합니다.

9. 7단계에서 생성한 아카이브를 가져옵니다.
10. 대상 Core의 Core 콘솔로 다시 돌아가 **Replication(복제)** 탭을 클릭합니다.
11. **Incoming Replication(들어오는 복제)** 아래에서 장애 조치 에이전트를 선택하고 상세정보를 확장합니다.
12. **Actions(작업)** 메뉴에서 **Failback(장애 복구)**을 클릭합니다.
13. **Failback Warnings(장애 복구 경고)** 대화 상자에서 **Start Failback(장애 복구 시작)**을 클릭합니다.
14. 장애 복구를 수행하는 동안 생성된 내보낸 에이전트가 포함되어 있는 시스템을 종료합니다.
15. 소스 Core와 에이전트에 대해 운영 체제 미설치 복원(BMR)을 수행합니다.
 

 **노트:** 복원을 시작하는 경우 대상 Core에서 가상 시스템의 에이전트로 가져온 복구 지점을 사용해야 합니다.
16. BMR이 재부팅되고 에이전트 서비스가 다시 시작될 때까지 기다린 후 시스템의 네트워크 연결 상세정보를 보고 기록합니다.
17. 소스 Core의 Core 콘솔을 탐색하고 **Machines(시스템)** 탭에서 시스템 보호 설정을 수정하여 새 네트워크 연결 상세정보를 추가합니다.
18. 대상 Core의 Core 콘솔을 탐색하고 **Replication(복제)** 탭에서 에이전트를 삭제합니다.
19. 소스 Core의 Core 콘솔에서 **Replication(복제)** 탭을 클릭하고 복제할 대상 Core를 추가하여 소스와 대상 간의 복제를 다시 설정합니다.

## 이벤트 관리

Core 이벤트 관리를 통해 Core의 상태와 사용량을 모니터링할 수 있습니다. Core에는 관리자에게 Core 또는 백업 작업에 대한 중요한 문제를 알리는 데 사용할 수 있는 사전 정의된 이벤트 집합이 포함되어 있습니다.

**Events(이벤트)** 탭에서 알람 그룹, 전자 메일 SMTP 설정, 반복 감소 및 이벤트 보존을 관리할 수 있습니다. 알람 그룹 옵션을 통해 알람 그룹을 관리할 수 있으며, 다음을 수행할 수 있습니다.

- 다음에 대한 경고를 생성할 이벤트를 지정할 수 있습니다.
  - 클러스터
  - 연결 기능
  - 작업
  - 라이선싱
  - 로그 자르기
  - 아카이브
  - Core 서비스
  - 내보내기
  - 보호
  - 복제
  - 롤백
  - SMTP 서버 설정
  - 추적 로그 활성화
  - 클라우드 구성
- 경고 유형을 지정할 수 있습니다(오류, 경고 및 정보).
- 경고를 보낼 사람과 위치를 지정할 수 있습니다. 옵션은 다음과 같습니다.
  - 이메일 주소
  - Windows 이벤트 로그

- 시스템 로그 서버
- 반복에 대한 시간 임계값을 지정할 수 있습니다.
- 모든 이벤트의 보존 기간을 지정할 수 있습니다.

## 알림 그룹 구성

알림 그룹을 구성하려면 다음을 수행하십시오.

1. Core에서 **Configuration(구성)** 탭을 선택합니다.
2. **Manage(관리)** 옵션에서 **Events(이벤트)**를 클릭합니다.
3. **Add Group(그룹 추가)**를 클릭합니다.

**Add Notification Group(알림 그룹 추가)** 대화 상자가 열리고 다음과 같은 세 가지 패널이 표시됩니다.

- 일반
- 이벤트 활성화
- 알림 옵션

4. **General(일반)** 패널에서 다음에 설명된 대로 알림 그룹의 기본 정보를 입력합니다.

### 텍스트 상자      설명

**이름**                      이벤트 알림 그룹에 대한 이름을 입력합니다. 이는 이벤트 알림 그룹을 식별하는 데 사용됩니다.

**설명**                      이벤트 알림 그룹에 대한 설명을 입력합니다. 이는 이벤트 알림 그룹의 목적을 설명하는 데 사용됩니다.

5. **Enable Events(이벤트 활성화)** 패널에서 생성하고 보고할 이벤트 로고(경고)에 대한 상태를 선택합니다. 다음에 대한 경고를 생성하도록 선택할 수 있습니다.

- 모든 이벤트
- 어플라이언스 이벤트
- 부팅 CD
- 보안
- 데이터베이스 보존
- 로컬 탑재
- 클러스터
- 알림
- Power Shell 스크립팅
- 강제 설치
- 야간 작업
- 연결 기능
- 작업
- 라이선싱
- 로그 자르기
- 아카이브
- Core 서비스
- 내보내기
- 보호
- 복제

- 리포지토리
- 롤백
- 롤업

#### 6. Notification Options(알림 옵션) 패널에서 알림 프로세스를 처리하는 방법을 지정합니다.

알림 옵션은 다음과 같습니다.

##### 텍스트 상자 설명

**전자 메일로 알림** 전자 메일 알림의 받는 사람을 지정합니다. 별도의 전자 메일 주소를 여러 개 지정하고 숨은 참조도 지정하도록 선택할 수 있습니다. 다음과 같은 항목을 선택할 수 있습니다.

- 받는 사람:
- 참조:
- 숨은 참조:

**Windows 이벤트 로그로 알림** Windows 이벤트 로그를 통해 경고를 보고하려면 이 옵션을 선택합니다. 이는 Windows 이벤트 로그를 통해 경고의 알림을 보고해야 하는지 지정하는 데 사용됩니다.


**sys logd로 알림** sys logd를 통해 경고를 수신하려면 이 옵션을 선택합니다. 다음과 같은 텍스트 상자에 sys logd의 상세정보를 지정합니다.

- 호스트 이름:
- 포트: 1

#### 7. OK(확인)를 클릭합니다.

### 전자 메일 서버 및 전자 메일 알림 템플릿 구성

이벤트에 대해 전자 메일 알림을 받으려면 전자 메일 서버 및 전자 메일 알림 템플릿을 구성하십시오.

 **노트:** 전자 메일 경고 메시지가 전송되기 전에 **Notify by email(전자 메일로 알림)** 옵션을 활성화하는 등 알림 그룹 설정도 구성해야 합니다. 전자 메일 경고를 수신할 이벤트 지정에 대한 자세한 내용은 *Dell DL4300 어플라이언스 사용 설명서*에서 '시스템 이벤트에 대한 알림 그룹 구성'을 참조하십시오.

전자 메일 서버 및 전자 메일 알림 템플릿을 구성하려면 다음을 수행합니다.

1. Core에서 **Configuration(구성)** 탭을 선택합니다.
2. **Manage(관리)** 옵션에서 **Events(이벤트)**를 클릭합니다.
3. **Email SMTP Settings(전자 메일 SMTP 설정)** 창에서 **Change(변경)**를 클릭합니다.  
**Email Notification Configuration(전자 메일 알림 구성)** 편집 대화 상자가 나타납니다.
4. **Enable Email Notifications(전자 메일 알림 활성화)**를 선택하고 아래 설명과 같이 전자 메일 서버의 상세 정보를 입력합니다.

##### 텍스트 상자 설명

**SMTP 서버** 전자 메일 알림 템플릿에 사용할 전자 메일 서버의 이름을 입력합니다. 이름 지정 규칙에는 호스트 이름, 도메인 및 접미사가 있습니다(예: **smtp.gmail.com**).

**포트** 포트 번호를 입력합니다. 이 번호는 전자 메일 서버의 포트를 식별하는 데 사용됩니다(예: Gmail의 경우 포트 587).

<b>텍스트 상자</b>	<b>설명</b> 기본값은 25입니다.
<b>시간 제한(초)</b>	정수 값을 입력하여 시간이 초과되기 전에 연결을 시도하는 시간을 지정합니다. 이는 전자 메일 서버에 연결을 시도할 때 시간이 초과되기 전까지의 시간(초)을 설정하는 데 사용됩니다. 기본값은 30초입니다.
<b>TLS</b>	메일 서버에서 TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer)과 같은 보안 연결을 사용하는 경우 이 옵션을 선택합니다.
<b>사용자 이름</b>	전자 메일 서버의 사용자 이름을 입력합니다.
<b>암호</b>	전자 메일 서버에 액세스하기 위한 암호를 입력합니다.
<b>보낸 사람</b>	반송 전자 메일 주소를 입력합니다. 이는 전자 메일 알람 템플릿의 반송 전자 메일 주소를 지정하는 데 사용됩니다(예: <b>noreply@localhost.com</b> ).
<b>전자 메일 제목</b>	전자 메일 템플릿의 제목을 입력합니다. 이는 전자 메일 알람 템플릿의 제목을 정의하는 데 사용됩니다(예: <hostname> - <level> <name>).
<b>Email(이메일)</b>	이벤트가 발생한 경우 해당 이벤트를 설명하는 템플릿의 본문과 심각도에 대한 정보를 입력합니다.

5. **Send Test Email(테스트 전자 메일 보내기)**을 클릭하고 결과를 검토합니다.
6. 테스트 결과에 만족하면 **OK(확인)**를 클릭합니다.

## 반복 감소 구성

반복 감소를 구성하려면 다음을 수행하십시오.

1. Core에서 **Configuration(구성)** 탭을 클릭합니다.
2. **Manage(관리)** 옵션에서 **Events(이벤트)**를 클릭합니다.
3. **Repetition Reduction(반복 감소)** 영역에서 **Change(변경)**를 클릭합니다.  
Repetition Reduction(반복 감소) 대화 상자가 표시됩니다.
4. **Enable Repetition Reduction(반복 감소 활성화)**을 선택합니다.
5. **Store events for X minutes(X분 동안 이벤트 저장)** 텍스트 상자에 반복 감소에 대한 이벤트를 저장할 기간(분)을 입력합니다.
6. **OK(확인)**를 클릭합니다.

## 이벤트 보존 구성

이벤트 보존을 구성하려면 다음을 수행하십시오.

1. Core에서 **Configuration(구성)** 탭을 클릭합니다.
2. **Manage(관리)** 옵션에서 **Events(이벤트)**를 클릭합니다.
3. **Database Connection Settings(데이터베이스 연결 설정)**에서 **Change(변경)**를 클릭합니다.  
**Database Connection Settings(데이터베이스 연결 설정)** 대화 상자가 표시됩니다.
4. **Retain event and job history for(특정 기간 동안 이벤트 및 작업 기록 보존)** 텍스트 상자에 이벤트 정보를 보존할 일수를 입력합니다.

예를 들어 기본값인 30일을 선택할 수 있습니다.

5. **Save(저장)**를 클릭합니다.

## 복구 관리

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

## 시스템 정보

AppAssure에서는 시스템 정보, 로컬 볼륨, 탑재된 볼륨 및 AppAssure 엔진 연결이 포함된 Core에 대한 정보를 제공합니다.

개별적이거나 코어에 로컬로 장착된 모든 복구 지점을 장착 해제하려면 **Tools(도구)** 탭의 **Mount(장착)** 옵션에서 가능합니다.


### 시스템 정보 보기

시스템 정보를 보려면 다음을 수행합니다.

1. Core를 탐색하고 **Tools(도구)** 탭을 선택합니다.
2. **Tools(도구)** 옵션에서 **System Info(시스템 정보)**를 클릭합니다.

## 설치 관리자 다운로드

Core에서 설치 관리자를 다운로드할 수 있습니다. **Tools(도구)** 탭에서 에이전트 설치 관리자 또는 Local Mount 유틸리티를 다운로드하도록 선택할 수 있습니다.

 **노트:** 에이전트 설치 관리자 액세스에 대해서는 [에이전트 설치 관리자 다운로드 및 설치](#)를 참조하십시오. 에이전트 설치 관리자 배포에 대한 자세한 내용은 [Dell.com/support/home](#)에서 *Dell DL4300 어플라이언스 배포 설명서*를 참조하십시오. Local Mount 유틸리티 설치 관리자 액세스에 대해서는 [Local Mount 유틸리티 정보](#)를 참조하고, Local Mount 유틸리티에 대한 자세한 내용은 [Local Mount 유틸리티 다운로드 및 설치](#)를 참조하십시오.

## 에이전트 설치 관리자 정보

에이전트 설치 관리자는 Core를 통해 보호하려는 시스템에 AppAssure Agent 응용프로그램을 설치하는 데 사용됩니다. 에이전트 설치 관리자가 필요한 시스템을 사용하는 경우 Core의 **Tools(도구)** 탭에서 웹 설치 관리자를 다운로드합니다.





**노트:** Core는 라이선스 포털에서 다운로드합니다. Core 설치 관리자를 다운로드하려면 <https://licenseportal.com>을 방문하십시오.

## 에이전트 설치 관리자 다운로드 및 설치

Core에 의해 보호되는 시스템에 에이전트 설치 관리자를 다운로드하고 배포할 수 있습니다.

에이전트 설치 관리자를 다운로드하고 설치하려면 다음을 수행하십시오.

1. 라이선스 포털 또는 Core에서 에이전트 설치 관리자 파일을 다운로드합니다.  
예를 들어, **Agent-X64-5.3.x.xxxx.exe**입니다.
2. **Save File(파일 저장)**을 클릭합니다.  
에이전트 설치에 대한 자세한 내용은 [Dell.com/support/home](https://Dell.com/support/home)에서 *Dell DL4300 어플라이언스 배포 설명서*를 참조하십시오.

## Local Mount 유틸리티 정보

Local Mount 유틸리티(LMU)는 모든 시스템의 원격 Core에 복구 지점을 탑재할 수 있는 다운로드 가능한 응용프로그램입니다. 간단한 유틸리티에 aavdisk 및 aavstor 드라이버가 포함되어 있지만, 서비스로 실행되는 것은 아닙니다. 유틸리티를 설치하면 기본적으로 **C:\Program Files\AppRecovery\Local Mount Utility** 디렉터리에 설치되며 컴퓨터의 바탕화면에 바로 가기가 표시됩니다.


유틸리티는 Core에 대한 원격 액세스를 수행할 수 있도록 고안되어 있지만 Core에 LMU를 설치할 수도 있습니다. Core에서 실행하면 응용프로그램이 AppAssure 5 Core 콘솔을 통해 수행되는 탑재를 포함하여 해당 Core의 모든 탑재를 인식하고 표시합니다. 마찬가지로, LMU에서 수행되는 탑재도 콘솔에 표시됩니다.

## Local Mount 유틸리티 다운로드 및 설치

Local Mount 유틸리티를 다운로드하고 설치하려면 다음을 수행하십시오.

1. LMU를 설치할 시스템에서 브라우저에 콘솔 URL을 입력하고 사용자 이름과 암호를 사용해 로그인하여 Core 콘솔에 액세스합니다.
2. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
3. **Tools(도구)** 탭에서 **Downloads(다운로드)**를 클릭합니다.
4. **Local Mount Utility(Local Mount 유틸리티)** 아래의 **Download web installer(웹 설치 관리자 다운로드)** 링크를 클릭합니다.
5. **Opening LocalMountUtility-Web.exe(LocalMountUtility-Web.exe 열기)** 창에서 **Save File(파일 저장)**을 클릭합니다.  
파일이 로컬 Downloads(다운로드) 폴더에 저장됩니다. 일부 브라우저에서는 폴더가 자동으로 열립니다.
6. **Downloads(다운로드)** 폴더에서 **LocalMountUtility-Web** 실행 파일을 마우스 오른쪽 단추로 클릭하고 **Open(열기)**을 클릭합니다.  
시스템 구성에 따라 **User Account Control(사용자 계정 제어)** 창이 표시될 수도 있습니다.
7. **User Account Control(사용자 계정 제어)** 창이 표시되면 프로그램이 시스템을 변경할 수 있도록 **Yes(예)**를 클릭합니다.  
**AppAssure Local Mount Utility Installation(AppAssure Local Mount 유틸리티 설치)** 마법사가 시작됩니다.
8. **AppAssure Local Mount Utility Installation(AppAssure Local Mount 유틸리티 설치)** 마법사의 **Welcome(시작)** 화면에서 **Next(다음)**를 클릭하여 계속해서 **License Agreement(라이선스 계약)** 페이지를 진행합니다.

9. **License Agreement(라이선스 계약)** 페이지에서 **I accept the terms in the license agreement(라이선스 계약에 동의)**를 선택하고 **Next(다음)**를 클릭하여 계속해서 **Prerequisites(필수 구성 요소)** 페이지를 진행합니다.
10. **Prerequisites(필수 구성 요소)** 페이지에서 필요한 필수 구성 요소를 모두 설치하고 **Next(다음)**를 클릭하여 계속해서 **Installation Options(설치 옵션)** 페이지를 진행합니다.
11. **Installation Options(설치 옵션)** 페이지에서 다음 작업을 완료합니다.
  - a. **Change(변경)** 단추를 클릭하여 LMU에 대한 대상 폴더를 선택합니다.
 

 **노트:** 기본 대상 폴더는 **C:\Program Files\AppRecovery\LocalMountUtility**입니다.
  - b. **Allow Local Mount Utility(Local Mount 유틸리티 허용)**가 AppAssure Software, Inc.에 진단 및 사용 정보를 자동으로 보내도록 허용할 것인지 선택합니다.
  - c. **Next(다음)**를 클릭하여 계속해서 **Progress(진행률)** 페이지로 이동하고 응용프로그램을 다운로드합니다. 응용프로그램이 대상 폴더에 다운로드되고, 진행률 표시줄에 진행률이 표시됩니다. 완료되면 마법사가 자동으로 **Completed(완료)** 페이지로 이동됩니다.
12. **Finish(마침)**를 클릭하여 마법사를 닫습니다.


## Local Mount 유틸리티에 Core 추가

복구 지점을 탑재하려면 LMU에 Core를 추가해야 합니다. 추가할 수 있는 Core의 수는 제한되지 않습니다. Local Mount 유틸리티에 Core를 추가하려면 다음을 수행하십시오.

1. LMU가 설치되어 있는 시스템에서 바탕 화면 아이콘을 두 번 클릭하여 LMU를 시작합니다.
2. **User Account Control(사용자 계정 제어)** 창이 표시되면 프로그램이 시스템을 변경할 수 있도록 **Yes(예)**를 클릭합니다.
3. AppAssure Local Mount 유틸리티 창의 왼쪽 상단에서 **Add core(Core 추가)**를 클릭합니다.
4. **Add Core(Core 추가)** 창에서, 아래에 설명대로 요청된 자격 증명을 입력합니다.

### 텍스트 상자 설명

**호스트 이름** 복구 지점을 탑재할 Core의 이름입니다.


 **노트:** Core에 LMU를 설치하면 LMU가 로컬 호스트 시스템을 자동으로 추가합니다.

**포트** Core와 통신하는 데 사용되는 포트 번호입니다.  
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 사용되는 사용자 이름입니다.

 **노트:** 특정 자격 증명을 사용하도록 선택하는 경우에만 이 옵션을 사용할 수 있습니다.

**암호** Core 시스템에 액세스하는 데 사용되는 암호입니다.

## 텍스트 상자 설명



**노트:** 특정 자격 증명을 사용하도록 선택하는 경우에만 이 옵션을 사용할 수 있습니다.

5. **Connect(연결)**를 클릭합니다.
6. Core를 여러 개 추가하는 경우 필요에 따라 3단계에서 5단계를 반복합니다.

### Local Mount 유틸리티를 사용하여 탑재된 복구 지점 탐색



**노트:** 탑재 절차를 완료하면 복구 지점이 포함되어 있는 폴더가 자동으로 열리므로 탑재 후 바로 복구 지점을 탐색하는 경우에는 이 절차를 수행할 필요가 없습니다.

Local Mount 유틸리티를 사용하여 탑재된 복구 지점을 탐색하려면 다음을 수행하십시오.

1. LMU가 설치되어 있는 시스템에서 바탕 화면 아이콘을 두 번 클릭하여 LMU를 시작합니다.
2. 기본 **Local Mount Recovery(로컬 탑재 복구)** 화면에서 **Active mounts(활성 탑재)**를 클릭합니다.  
**Active Mounts(활성 탑재)** 창이 열리고 탑재된 복구 지점이 모두 표시됩니다.
3. 복구할 복구 지점 옆에 있는 **Explore(탐색)**를 클릭하여 중복 제거된 볼륨의 폴더를 엽니다.

### Local Mount 유틸리티를 사용하여 복구 지점 탑재

복구 지점을 탑재하기 전에 LMU가 복구 지점이 저장되는 Core에 연결해야 합니다. [Local Mount 유틸리티에 Core 추가](#)에 설명된 대로 LMU에 추가할 수 있는 Core의 수는 제한되지 않지만 응용프로그램이 한 번에 하나의 Core에만 연결할 수 있습니다. 예를 들어, 하나의 Core에 의해 보호되는 에이전트의 복구 지점을 탑재한 후 다른 Core에 의해 보호되는 에이전트의 복구 지점을 탑재하는 경우 LMU가 자동으로 첫 번째 Core를 분리하여 두 번째 Core와의 연결을 설정합니다.

Local Mount 유틸리티를 사용하여 복구 지점을 탑재하려면 다음을 수행합니다.

1. LMU가 설치되어 있는 시스템에서 바탕 화면 아이콘을 두 번 클릭하여 LMU를 시작합니다.
2. 기본 **AppAssure Local Mount Utility(AppAssure Local Mount 유틸리티)** 창의 탐색 트리에서 원하는 Core를 확장하여 보호된 에이전트를 표시합니다.
3. 탐색 트리에서 원하는 에이전트를 선택합니다.  
기본 프레임에 복구 지점이 표시됩니다.
4. 탑재할 복구 지점을 확장하여 개별 디스크 볼륨 또는 데이터베이스를 표시합니다.
5. 탑재할 복구 지점을 마우스 오른쪽 단추로 클릭하고 다음 옵션 중 하나를 선택합니다.
  - 탑재
  - 쓰기 가능 탑재
  - 이전 쓰기를 포함하여 탑재
  - 고급 탑재
6. **Advanced Mount(고급 탑재)** 창에서 아래에 설명된 옵션을 완료합니다.

## 텍스트 상자 설명

### 탑재 지점 경로

**Browse(찾아보기)** 단추를 클릭하여 기본 탑재 지점 경로가 아닌 복구 지점에 대한 경로를 선택합니다.

### 탑재 유형

다음 옵션 중 하나를 선택합니다.


- 읽기 전용 탑재
- 쓰기 가능 탑재

## 텍스트 상자 설명

- 이전 쓰기를 포함하여 읽기 전용 탑재

### 7. Mount(탑재)를 클릭합니다.

LMU가 탑재된 복구 지점이 포함되어 있는 폴더를 자동으로 엽니다.

 **노트:** 이미 탑재된 복구 지점을 선택하면 **Mounting(탑재)** 대화 상자에 복구 지점을 분리하라는 메시지가 표시됩니다.

## Local Mount 유틸리티를 사용하여 복구 지점 분리

Local Mount 유틸리티를 사용하여 복구 지점을 분리하려면 다음을 수행하십시오.


1. LMU가 설치되어 있는 시스템에서 바탕 화면 아이콘을 두 번 클릭하여 LMU를 시작합니다.
2. 기본 **Local Mount Recovery(로컬 탑재 복구)** 화면에서 **Active mounts(활성 탑재)**를 클릭합니다.  
**Active Mounts(활성 탑재)** 창이 열리고 탑재된 복구 지점이 모두 표시됩니다.
3. 아래의 표에 설명된 옵션 중 하나를 선택하여 복구 지점을 분리합니다.

옵션	설명
분리	<p>인접한 복구 지점만 분리합니다.</p> <ol style="list-style-type: none"> <li>a. 선택한 복구 지점 옆에 있는 <b>Dismount(분리)</b>를 클릭합니다.</li> <li>b. 창을 닫습니다.</li> </ol>
모두 분리	<p>탑재된 복구 지점을 모두 분리합니다.</p> <ol style="list-style-type: none"> <li>a. <b>Dismount all(모두 분리)</b>을 클릭합니다.</li> <li>b. <b>Dismount All(모두 분리)</b> 창에서 <b>Yes(예)</b>를 클릭하여 확인합니다.</li> <li>c. 창을 닫습니다.</li> </ol>

## Local Mount 유틸리티 트레이 메뉴 정보

LMU 트레이 메뉴는 바탕 화면 작업 표시줄에 있습니다. 아이콘을 마우스 오른쪽 단추로 클릭하여 다음 옵션을 표시합니다.

<b>Browse Recovery Points(복구 지점 찾아보기)</b>	LMU 기본 화면을 엽니다.
<b>Active Mounts(활성 탑재)</b>	Active Mounts(활성 탑재) 화면을 엽니다.
옵션	<b>Default Mount Point Directory(기본 탑재 지점 디렉터리)</b> , <b>Default Core Credentials(기본 Core 자격 증명)</b> 및 LMU 사용자 인터페이스의 <b>Language(언어)</b> 를 변경할 수 있는 <b>Options(옵션)</b> 화면을 엽니다.
정보	라이선스 정보의 시작 화면을 엽니다.
<b>Exit(종료)</b>	응용프로그램을 닫습니다.

 **노트:** 기본 화면의 상단에 있는 X를 사용하면 응용프로그램이 트레이로 최소화됩니다.

## Core 및 에이전트 옵션 사용

기본 LMU 화면에서 Core 또는 에이전트를 마우스 오른쪽 단추로 클릭하여 특정 옵션을 사용할 수 있습니다. 이러한 옵션은 다음과 같습니다.

- 로컬 호스트 옵션
- 원격 Core 옵션
- 에이전트 옵션

### 로컬 호스트 옵션 액세스

로컬 호스트 옵션에 액세스하려면 Core 또는 에이전트를 마우스 오른쪽 단추로 클릭한 후 Core에 **Reconnect(다시 연결)**를 클릭합니다. Core의 정보가 업데이트되고 새로 고쳐집니다(예: 최근에 추가된 에이전트).

### 원격 Core 옵션 액세스

원격 Core 옵션에 액세스하려면 Core 또는 에이전트를 마우스 오른쪽 단추로 클릭한 후 아래에 설명된 대로 원격 Core 옵션 중 하나를 선택합니다.

옵션	설명
<b>Reconnect to core(Core에 다시 연결)</b>	Core에서 정보를 새로 고치고 업데이트합니다(예: 최근에 추가된 에이전트).
<b>Remove core(Core 제거)</b>	Local Mount 유틸리티에서 Core를 삭제합니다.
<b>Edit core(Core 편집)</b>	호스트 이름, 포트 및 자격 증명을 변경할 수 있는 <b>Edit Core(Core 편집)</b> 창을 엽니다.

### 에이전트 옵션 액세스

에이전트 옵션에 액세스하려면 Core 또는 에이전트를 마우스 오른쪽 단추로 클릭한 후 **Refresh recovery points(복구 지점 새로 고침)**를 클릭합니다. 선택한 에이전트에 대한 복구 지점의 목록이 업데이트됩니다.

## 보존 정책 관리

보호되는 모든 서버의 정기적인 백업 스냅샷은 시간이 경과함에 따라 Core에 누적됩니다. 보존 정책은 백업 스냅샷을 장기간 보존하고 이러한 백업 스냅샷을 관리하는 데 사용됩니다. 시간이 지나 오래된 백업을 삭제하는 야간 롤업 프로세스에서 이러한 보존 정책을 적용합니다. 보존 정책 구성에 대한 자세한 내용은 [보존 정책 설정 사용자 지정](#)을 참조하십시오.

## 클라우드에 아카이브

데이터를 직접 Core 콘솔에서 다양한 클라우드 공급자에 업로드하여 클라우드에 데이터를 아카이브할 수 있습니다. 호환 가능한 클라우드로는 Windows Azure, Amazon, Rackspace 및 OpenStack 기반 공급자가 있습니다.

클라우드에 아카이브를 내보내려면 다음을 수행합니다.

- Core 콘솔에 클라우드 계정을 추가합니다. 자세한 내용은 [클라우드 계정 추가](#)를 참조하십시오.
- 클라우드 계정에 데이터를 아카이브하고 내보낼 수 있습니다.
- 클라우드 위치에서 아카이브된 데이터를 가져와 검색합니다.


## 아카이빙 정보

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. AppAssure의 아카이브 기능은 호환 및 비호환 데이터에 대한 연장 보존을 지원하며 복제 데이터를 원격 복제 Core에 시드하는 데에도 사용됩니다.

## 아카이브 생성

아카이브를 생성하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성)** 탭을 클릭합니다.
2. **Manage(관리)** 옵션에서 **Archive(아카이브)**를 클릭합니다.  
**Create Archive(아카이브 생성)** 대화 상자가 표시됩니다.
3. **Create Archive(아카이브 생성)** 대화 상자에서 아래에 설명된 대로 아카이브에 대한 상세정보를 입력합니다.

텍스트 상자	설명
날짜 범위	날짜 범위를 지정하려면 시작 날짜와 종료 날짜를 선택합니다.
아카이브 암호	아카이브에 대한 암호를 입력합니다. 이는 아카이브를 보호하기 위해 로그인 자격 증명을 설정하는 데 사용됩니다.
확인	아카이브를 보호하기 위해 암호를 다시 입력합니다. 이는 <b>Archive Password(아카이브 암호)</b> 텍스트 상자에 입력한 정보에 대한 유효성 검사를 제공하는 데 사용됩니다.
출력 위치	출력에 대한 위치를 입력합니다. 이는 아카이브를 배치할 위치 경로를 정의하는 데 사용되며, 로컬 디스크 또는 네트워크 공유일 수 있습니다. 예를 들어, 네트워크 경로의 경우 <b>d:\work\archive</b> 또는 <b>\\servername\sharename</b> 입니다.  <b>노트:</b> 출력 위치가 네트워크 공유인 경우 공유에 연결할 사용자 이름과 암호를 입력합니다.
사용자 이름	사용자 이름을 입력합니다. 이는 네트워크 공유에 대한 로그인 자격 증명을 설정하는 데 사용됩니다.
암호	네트워크 경로에 대한 암호를 입력합니다. 이는 네트워크 공유에 대한 로그인 자격 증명을 설정하는 데 사용됩니다.
최대 크기	아카이브에 사용할 공간을 입력합니다. 다음을 선택할 수 있습니다. <ul style="list-style-type: none"> <li>• 전체 대상</li> <li>• 공간 지정(MB 또는 GB 단위)</li> </ul>

텍스트 상자	설명
재활용 작업	적절한 재활용 작업을 선택합니다.
주석	아카이브에 대해 수집해야 하는 추가 정보를 입력합니다.

#### 4. Archive(아카이브)를 클릭합니다.

### 예약된 아카이브 설정

예약된 아카이브 기능을 사용하면 선택한 시스템의 아카이브를 자동으로 생성하여 지정된 위치에 저장되도록 시간을 설정할 수 있습니다. 이 기능은 매번 아카이브를 수동으로 생성하는 번거로움 없이 시스템 아카이브를 자주 저장하려는 경우에 유용합니다. 아래 절차의 단계를 수행하여 자동 아카이브를 예약합니다. 예약된 아카이브를 설정하려면 다음을 수행합니다.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. **Archive(아카이브)** 옵션에서 **Scheduled(예약)**을 클릭합니다.
3. Scheduled Archive(예약된 아카이브) 페이지에서 **Add(추가)**를 클릭합니다.  
**Add Archive Wizard(아카이브 추가 마법사)** 대화 상자가 나타납니다.
4. **Add Archive Wizard(아카이브 추가 마법사)**의 **Location(위치)** 페이지에 있는 **Location Type(위치 유형)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
  - Local: Output location(로컬: 출력 위치) - 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.
  - 네트워크
    - Output location(출력 위치): 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.
    - User Name(사용자 이름): 사용자 이름을 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.
    - Password(암호): 네트워크 경로의 암호를 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.
  - 클라우드
    - Account(계정): 드롭다운 목록에서 계정을 선택합니다. 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다.
    - Container(컨테이너): 드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
    - Folder Name(폴더 이름): 아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]입니다.
5. **Next(다음)**를 클릭합니다.
6. 마법사의 **Machines(시스템)** 페이지에서, 아카이브할 복구 지점이 포함된 보호 시스템을 선택합니다.
7. **Next(다음)**를 클릭합니다.
8. **Options(옵션)** 페이지의 드롭다운 목록에서 다음과 같은 재활용 작업 중 하나를 선택합니다.
  - **Replace this Core(이 코어 대체)**: 이 코어와 관련된 기존의 아카이브된 데이터를 덮어쓰지만 다른 코어의 데이터는 그대로 남아 있게 됩니다.
  - **Erase Completely(완전히 지우기)**: 새 아카이브를 작성하기 전에 디렉터리에서 모든 아카이브된 데이터를 지웁니다.
  - **Incremental(증분)**: 기존 아카이브에 복구 지점을 추가할 수 있습니다. 복구 지점을 비교하여 아카이브에 이미 존재하는 데이터의 중복을 방지할 수 있습니다.
9. **Schedule(일정)** 페이지에서, 다음과 같은 데이터 전송 빈도 옵션 중 하나를 선택합니다.
  - Daily: At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.

- 매주
  - At day of week(요일): 아카이브가 자동으로 생성되는 요일을 선택합니다.
  - At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.

- 매월
  - At day of months(날짜): 아카이브가 자동으로 생성되는 날짜를 선택합니다.
  - At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.

10. 나중에 재개할 수 있도록 아카이빙을 일시 중지하려면 **Initial pause archiving(처음에 아카이빙 일시 중지)**을 선택합니다.

아카이빙을 재개하기 전에 대상 위치를 준비할 시간이 필요할 경우 예약된 아카이브를 일시 중지할 수 있습니다. 이 옵션을 선택하지 않으면 예약된 시간에 아카이빙이 시작됩니다.

11. **Finish(마침)**를 클릭합니다.

## 예약된 아카이브 일시 중지 또는 재개

예약된 아카이브 설정 절차를 수행할 때 처음에 아카이빙이 일시 중지되도록 선택한 경우 예약된 아카이브가 나중에 재개되도록 해야 합니다.

예약된 아카이브를 일시 중지하거나 재개하려면 다음을 수행합니다.

1. **Core 콘솔**로 이동하여 **Tools(도구)** 탭을 클릭합니다.
2. **Archive(아카이브)** 옵션에서 **Scheduled(예약)**을 클릭합니다.
3. **Scheduled Archive(예약된 아카이브)** 페이지에서 다음 중 하나를 수행합니다.
  - 원하는 아카이브를 선택하고 다음 작업 중 하나를 클릭합니다.
    - 일시 중지
    - 재개
  - 원하는 아카이브 옆에 있는 드롭다운 메뉴를 클릭하고 다음 작업 중 하나를 클릭합니다.
    - 일시 중지
    - 재개

아카이브 상태가 **Schedule(일정)** 열에 표시됩니다.

## 예약된 아카이브 편집

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. **Archive(아카이브)** 옵션에서 **Scheduled(예약)**을 클릭합니다.
3. **Scheduled Archive(예약된 아카이브)** 페이지에서, 변경할 아카이브 옆에 있는 드롭다운 메뉴를 클릭하고 **Edit(편집)**를 클릭합니다.  
**Add Archive Wizard(아카이브 추가 마법사)** 대화 상자가 나타납니다.
4. **Add Archive Wizard(아카이브 추가 마법사)**의 **Location(위치)** 페이지에 있는 **Location Type(위치 유형)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
  - Local: Output location(로컬: 출력 위치) - 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.
  - 네트워크
    - Output location(출력 위치): 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.



- User Name(사용자 이름): 사용자 이름을 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.
- Password(암호): 네트워크 경로의 암호를 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.
- 클라우드
  - Account(계정): 드롭다운 목록에서 계정을 선택합니다. 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다.
  - Container(컨테이너): 드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
  - Folder Name(폴더 이름): 아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]입니다.
- 5. **Next(다음)**를 클릭합니다.
- 6. 마법사의 **Machines(시스템)** 페이지에서, 아카이브할 복구 지점이 포함된 보호 시스템을 선택합니다.
- 7. **Next(다음)**를 클릭합니다.
- 8. **Schedule(일정)** 페이지에서, 다음과 같은 데이터 전송 빈도 옵션 중 하나를 선택합니다.
  - Daily: At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.
  - 매주
    - At day of week(요일): 아카이브가 자동으로 생성되는 요일을 선택합니다.
    - At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.
  - 매월
    - At day of months(날짜): 아카이브가 자동으로 생성되는 날짜를 선택합니다.
    - At time(매일: 가끔) - 일일 아카이브를 생성할 날의 시간을 선택합니다.
- 9. 나중에 재개할 수 있도록 아카이빙을 일시 중지하려면 **Initial pause archiving(처음에 아카이빙 일시 중지)**을 선택합니다.  
아카이빙을 재개하기 전에 대상 위치를 준비할 시간이 필요할 경우 예약된 아카이브를 일시 중지할 수 있습니다. 이 옵션을 선택하지 않으면 예약된 시간에 아카이빙이 시작됩니다.
- 10. **Finish(마침)**를 클릭합니다.

## 아카이브 확인

아카이브 확인을 수행하여 아카이브의 구조가 완전한 상태인지 검사할 수 있습니다. 아카이브 내에 필요한 파일이 모두 있는지 확인하는 것입니다. 아카이브 확인을 수행하려면 다음 절차의 단계를 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭합니다.
2. **Archive(아카이브)** 옵션에서 **Check Archive(아카이브 확인)**를 클릭합니다.  
**Check Archive(아카이브 확인)** 대화 상자가 표시됩니다.
3. 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
  - Local: Output location(로컬: 출력 위치) - 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.
  - 네트워크
    - Output location(출력 위치): 출력 위치를 입력합니다. 아카이브가 상주할 위치 경로를 나타냅니다.
    - User Name(사용자 이름): 사용자 이름을 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.
    - Password(암호): 네트워크 경로의 암호를 입력합니다. 네트워크 공유에 대한 로그인 자격 증명을 설정합니다.

- 클라우드
  - Account(계정): 드롭다운 목록에서 계정을 선택합니다. 클라우드 계정을 선택하려면 먼저 Core 콘솔에 추가해야 합니다.
  - Container(컨테이너): 드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
  - Folder Name(폴더 이름): 아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]입니다.
- 4. 구조 무결성 검사를 수행하여 **Structure integrity(구조 무결성)**를 선택합니다.
- 5. **Check File(파일 확인)**을 클릭합니다.

## 아카이브 가져오기

아카이브를 가져오려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성)** 탭을 선택합니다.
2. **Manage(관리)** 옵션에서 **Archive(아카이브)**를 클릭한 후 **Import(가져오기)**를 클릭합니다.  
**Import Archive(아카이브 가져오기)** 대화 상자가 표시됩니다.
3. **Import Archive(아카이브 가져오기)** 대화 상자에서 아래에 설명된 대로 아카이브 가져오기에 대한 상세 정보를 입력합니다.

### 텍스트 상자      설명

**입력 위치**      아카이브를 가져올 위치를 선택합니다.

**사용자 이름**      아카이브의 보안을 위해 액세스 권한을 설정하려면 로그인 자격 증명을 입력합니다.

**암호**      아카이브에 액세스하기 위한 암호를 입력합니다.

4. **Check File(파일 확인)**을 클릭하여 가져올 아카이브가 있는지 확인합니다.  
**Restore(복원)** 대화 상자가 표시됩니다.
5. **Restore(복원)** 대화 상자에서 소스 Core의 이름을 확인합니다.
6. 아카이브에서 가져올 에이전트를 선택합니다.
7. 리포지토리를 선택합니다.
8. **Restore(복원)**를 클릭하여 아카이브를 가져옵니다.


## SQL 연결 기능 관리

SQL 연결 기능 구성을 통해 Core가 Microsoft SQL Server의 로컬 인스턴스를 사용하여 SQL Server의 스냅샷에서 SQL 데이터베이스 및 로그 파일을 연결할 수 있습니다. 연결 기능 테스트를 수행하면 Core가 SQL 데이터베이스의 일관성을 검사하고 모든 데이터 파일(MDF 및 LDF 파일)을 백업 스냅샷에서 사용할 수 있도록 합니다. 연결 기능 검사는 특정 복구 지점에 필요할 경우 또는 야간 작업의 일부로 실행할 수 있습니다.

연결 기능을 사용하려면 AppAssure Core 시스템에 Microsoft SQL Server의 로컬 인스턴스가 있어야 합니다. 이 인스턴스는 Microsoft 또는 공인 대리점에서 제공하는 정품 라이선스 버전의 SQL Server여야 합니다. Microsoft에서는 수동적인 SQL 라이선스 사용을 허용하지 않습니다.


연결 기능에서는 SQL Server 2005, 2008, 2008 R2, 2012, 2014를 지원합니다. 테스트 수행에 사용되는 계정은 SQL Server 인스턴스에서 시스템 관리자 역할이 있어야 합니다.

SQL Server의 디스크상 저장소 형식은 64비트와 32비트 환경에서 동일하며, 두 버전 간에 연결 기능이 작동됩니다. 하나의 환경에서 실행되는 서버 인스턴스에서 분리된 데이터베이스를 다른 환경에서 실행되는 서버 인스턴스에서 연결할 수 있습니다.

 **주의:** Core의 SQL Server 버전은 SQL Server가 설치되어 있는 모든 에이전트의 SQL Server 버전과 같거나 이후 버전이어야 합니다.

## SQL 연결 기능 설정 구성

보호되는 SQL 데이터베이스에서 연결 기능 검사를 실행하기 전에, Core 시스템에서 에이전트 시스템에 대해 검사를 수행하는 데 사용할 SQL Server의 로컬 인스턴스를 선택합니다.

 **노트:** 연결 기능을 사용하려면 AppAssure Core 시스템에 Microsoft SQL Server의 로컬 인스턴스가 있어야 합니다. 이 인스턴스는 Microsoft 또는 공인 대리점에서 제공하는 정품 라이선스 버전의 SQL Server 여야 합니다. Microsoft에서는 수동적인 SQL 라이선스 사용을 허용하지 않습니다.

SQL 연결 기능 설정을 구성하려면 다음을 수행하십시오.


1. Core 콘솔로 이동하여 해당 탭을 클릭합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. Nightly Jobs(야간 작업) 창에서 **Change(변경)**를 클릭합니다.  
**Nightly Job(야간 작업)** 대화 상자가 표시됩니다.
4. **Attachability Check Job(연결 기능 검사 작업)**을 클릭한 후 **Settings(설정)**를 클릭합니다.
5. 드롭다운 메뉴의 다음 옵션 중에서 Core에 설치된 SQL Server의 인스턴스를 선택합니다.  
다음에서 선택할 수 있습니다.
  - SQL Server 2005
  - SQL Server 2008
  - SQL Server 2008 R2
  - SQL Server 2012
  - SQL Server 2014
6. 자격 증명 유형을 선택합니다.  
다음에서 선택할 수 있습니다.
  - Windows
  - SQL
7. 아래에 설명된 대로 Windows 또는 SQL Server 인스턴스에 대한 관리 권한이 있는 자격 증명을 지정합니다.

### 텍스트 상자      설명

**사용자 이름**      SQL Server의 로그인 권한에 대한 사용자 이름을 입력합니다.

**암호**      SQL 연결 기능에 대한 암호입니다. 이는 로그인 작업을 제어하는 데 사용됩니다.

8. **Test Connection(연결 테스트)**를 클릭합니다.

 **노트:** 자격 증명을 잘못 입력한 경우 자격 증명 테스트에 실패했음을 경고하는 메시지가 표시됩니다. 자격 증명 정보를 수정하고 연결 테스트를 다시 실행하십시오.

9. **Save(저장)**를 클릭합니다.

이제 보호된 SQL Server 데이터베이스에서 연결 기능 검사를 실행할 수 있습니다.

10. Nightly Jobs(야간 작업) 창에서 **OK(확인)**를 클릭합니다.  
야간 작업 시에 연결 기능 검사가 수행되도록 예약됩니다.

## 야간 SQL 연결 기능 검사 및 로그 자르기 구성

야간 SQL 연결 기능 검사 및 로그 자르기를 구성하려면 다음을 수행하십시오.

1. Core의 왼쪽 탐색 영역에서 야간 연결 기능 검사 및 로그 자르기를 수행할 시스템을 선택하고 **SQL Server Settings(SQL Server 설정)**를 클릭합니다.
2. Core 콘솔로 이동합니다.
3. **Configuration(구성) → Settings(설정)**를 클릭합니다.
4. **Nightly Jobs(야간 작업)** 섹션에서 **Change(변경)**를 클릭합니다.
5. 조직의 필요에 따라 다음 SQL Server 설정을 선택하거나 지웁니다.
  - 연결 기능 검사 작업
  - 로그 자르기 작업(단순 복구 모델에만 해당)
6. **OK(확인)**를 클릭합니다.

보호된 SQL Server에 연결 기능 및 로그 자르기 설정이 적용됩니다.

## Exchange 데이터베이스 탑재 기능 검사 및 로그 자르기 관리

AppAssure를 사용하여 Microsoft Exchange Server를 백업하는 경우 스냅샷을 수행한 후에 항상 모든 Exchange 데이터베이스에 대해 탑재 기능 검사를 수행할 수 있습니다. 이 손상 감지 기능은 관리자에게 잠재적인 오류를 경고하며, 이를 통해 오류가 발생한 경우 Exchange Server의 모든 데이터를 성공적으로 복구할 수 있습니다.

 **노트:** 탑재 기능 검사 및 로그 자르기 기능은 Microsoft Exchange 2007, 2010 및 2013에만 적용됩니다. 또한 Exchange의 조직 관리자 역할에만 AppAssure Agent 서비스 계정을 할당해야 합니다.


### Exchange 데이터베이스 탑재 기능 및 로그 자르기 구성

자동 탑재 기능 검사, 야간 체크섬 검사 또는 야간 로그 자르기를 비롯하여 Exchange 데이터베이스 서버 설정을 보거나, 활성화하거나, 비활성화할 수 있습니다.

Exchange 데이터베이스 탑재 기능 및 로그 자르기를 구성하려면 다음을 수행하십시오.

1. Core의 왼쪽 탐색 영역에서 탑재 기능 검사 및 로그 자르기를 구성할 시스템을 선택합니다. 선택한 시스템에 대한 **Summary(요약)** 탭이 표시됩니다.
2. **Exchange Server Settings(Exchange Server 설정)**를 클릭합니다. **Exchange Server Settings(Exchange Server 설정)** 대화 상자가 표시됩니다.
3. 조직의 필요에 따라 다음 Exchange Server 설정을 선택하거나 지웁니다.
  - 자동 탑재 기능 검사 사용
  - 야간 체크섬 검사 사용
  - 야간 로그 자르기 활성화
4. **OK(확인)**를 클릭합니다.


보호된 Exchange Server에 탑재 기능 및 로그 자르기 설정이 적용됩니다.

 **노트:** 로그 자르기 강제 적용에 대한 자세한 내용은 [로그 자르기 강제 적용](#)을 참조하십시오.

## 탐재 기능 검사 강제 적용

탐재 기능 검사를 강제 적용하려면 다음을 수행하십시오.

1. Core 콘솔의 왼쪽 탐색 영역에서 탐재 기능 검사를 강제로 수행할 시스템을 선택한 후 **Recovery Points(복구 지점)** 탭을 클릭합니다.
2. 목록에서 복구 지점 옆에 있는 >를 클릭하여 보기를 확장합니다.
3. **Force Mountability Check(탐재 기능 검사 강제 적용)**를 클릭합니다.  
탐재 기능 검사를 강제 적용할 것인지 묻는 메시지가 표시됩니다.
4. **Yes(예)**를 클릭합니다.


 **노트:** 연결 기능 검사의 상태를 확인하는 방법에 대한 지침은 [이벤트 및 경고 보기](#)를 참조하십시오.

시스템에서 탐재 기능 검사를 수행합니다.


## 체크섬 검사 강제 적용

체크섬 검사를 강제 적용하려면 다음을 수행하십시오.

1. Core 콘솔의 왼쪽 탐색 영역에서 체크섬 검사를 강제로 수행할 시스템을 선택한 후 **Recovery Points(복구 지점)** 탭을 클릭합니다.
2. 목록에서 복구 지점 옆에 있는 >를 클릭하여 보기를 확장합니다.
3. **Force Checksum Check(체크섬 검사 강제 적용)**를 클릭합니다.  
**Force Attachability Check(연결 기능 체크섬 강제 적용)** 창에 체크섬 검사를 강제 적용할 것인지 나타내는 메시지가 표시됩니다.
4. **Yes(예)**를 클릭합니다.  
시스템에서 체크섬 검사를 수행합니다.

 **노트:** 연결 기능 검사의 상태를 확인하는 방법은 [이벤트 및 경고 보기](#)를 참조하십시오.

## 로그 자르기 강제 적용


 **노트:** 이 옵션은 Exchange 또는 SQL 시스템에서만 사용할 수 있습니다.

로그 자르기를 강제 적용하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하여 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 로그를 자를 시스템의 하이퍼링크를 클릭합니다.
  - 또는 Navigation(탐색) 창에서 로그를 자를 시스템을 선택합니다.
3. 해당 시스템에 대한 **Actions(작업)** 드롭다운 메뉴에서 **Force Log Truncation(로그 자르기 강제 적용)**을 클릭합니다.
4. 계속해서 로그 자르기를 강제 적용할 것인지 확인합니다.

## 복구 지점 상태 표시기

보호된 SQL 또는 Exchange Server에 복구 지점이 생성되면 **Recovery Points(복구 지점)** 테이블에서 응용프로그램에 해당 색상 상태 표시기가 표시됩니다. 표시되는 색상은 보호된 시스템에 대한 검사 설정과 해당 검사의 성공 또는 실패 여부에 따라 다릅니다. 이러한 내용은 다음 표에 설명되어 있습니다.

 **노트:** 복구 지점 보기에 대한 자세한 내용은 [복구 지점 보기](#)를 참조하십시오.


다음 표에 SQL 데이터베이스에 대해 표시되는 상태 표시기가 나열되어 있습니다.


#### SQL 데이터베이스에 대한 복구 상태 지점 색

상태 색	설명
흰색	다음 상태 중 하나가 발생한 경우를 나타냅니다. <ul style="list-style-type: none"><li>• SQL 데이터베이스가 없는 경우</li><li>• 연결 기능 검사가 활성화되지 않은 경우</li><li>• 연결 기능 검사가 실행되지 않은 경우</li></ul>
노란색	SQL 데이터베이스가 오프라인 상태이고 검사를 수행할 수 없음을 나타냅니다.
빨간색	연결 기능 검사가 실패했음을 나타냅니다.
녹색	연결 기능 검사를 통과했음을 나타냅니다.

다음 표에 Exchange 데이터베이스에 대해 표시되는 상태 표시기가 나열되어 있습니다.

#### Exchange 데이터베이스에 대한 복구 상태 지점 색

용어 머리글	설명 머리글
흰색	다음 상태 중 하나가 발생한 경우를 나타냅니다. <ul style="list-style-type: none"><li>• Exchange 데이터베이스가 없는 경우</li><li>• 탑재 기능 검사가 활성화되지 않은 경우</li></ul> <p> <b>노트:</b> 이는 복구 지점 내의 특정 볼륨에 적용될 수 있습니다.</p>
노란색	Exchange 데이터베이스 탑재 기능 검사가 활성화되었지만 검사가 실행되지 않았음을 나타냅니다.
빨간색	하나 이상의 데이터베이스에서 탑재 기능 또는 체크섬 검사가 실패했음을 나타냅니다.
녹색	탑재 기능 검사 또는 체크섬 검사를 통과했음을 나타냅니다.

 **노트:** 연결된 Exchange 또는 SQL 데이터베이스가 없는 복구 지점은 흰색 상태 표시기와 함께 표시됩니다. 복구 지점에 대해 Exchange와 SQL 데이터베이스가 모두 있는 경우 복구 지점에 대해 가장 심각한 상태 표시기가 표시됩니다.

## 어플라이언스 관리

Core 콘솔에는 공간 프로비저닝, 어플라이언스 상태 모니터링, 관리 도구 액세스에 사용할 수 있는 **Appliance(어플라이언스)** 탭이 있습니다.

### 어플라이언스 상태 모니터링


**Appliance(어플라이언스)** 탭의 **Overall Status(전반적인 상태)** 페이지에서 어플라이언스 하위 시스템의 상태를 모니터링할 수 있습니다. **Overall Status(전반적인 상태)** 페이지에는 각 하위 시스템 옆에 상태 표시등과 하위 시스템의 상태를 나타내는 상태 설명이 표시됩니다.

**Overall Status(전반적인 상태)** 페이지에는 각 하위 시스템의 상세정보를 볼 수 있는 도구로 연결되는 링크가 있습니다. 이 링크는 경고나 오류 문제를 해결하는 데 유용합니다. 어플라이언스 하드웨어 및 저장소 하드웨어 하위 시스템에 있는 **System Administrator** 링크를 클릭하면 하드웨어 관리에 사용되는 System Administrator 응용프로그램에 로그인하라는 메시지가 표시됩니다. System Administrator 응용프로그램에 대한 자세한 내용은 [dell.com/support/home](http://dell.com/support/home)에서 *OpenManage Server Administrator 사용 설명서*를 참조하십시오. 저장소 프로비저닝 하위 시스템에 있는 **Provisioning Status(프로비저닝 상태)** 링크를 클릭하면 해당 하위 시스템의 프로비저닝 상태를 보여주는 **Tasks(작업)** 화면이 열립니다. 저장소를 프로비저닝할 수 있는 경우 **Actions(작업)** 아래에서 **Provision(프로비전)** 링크가 프로비전 작업 옆에 표시됩니다.


### 저장소 프로비저닝

어플라이언스는 다음에 대해 사용 가능한 DL4300 내부 스토리지 및 연결된 모든 외부 스토리지 인클로저를 구성합니다.

- AppAssure 리포지토리

 **노트:** 파이버 채널 HBA가 구성되어 있는 경우 리포지토리 생성 프로세스를 수동으로 수행해야 합니다. AppAssure가 루트 디렉터리에 리포지토리를 자동으로 생성하지 않습니다. 자세한 내용은 *Dell DL4300 어플라이언스 배포 설명서*를 참조하십시오.

- 보호된 컴퓨터의 가상 대기(standby)

 **노트:** H830 컨트롤러에 1TB, 2TB, 4TB 또는 6TB(고용량의 경우) 드라이브가 연결된 MD1400s가 지원됩니다. MD 1400s는 최대 4개까지 지원됩니다.

 **노트:** DL4300 고용량 구성에서는 H830 PERC SAS 어댑터 또는 파이버 채널 HBA가 2개 지원됩니다. 파이버 채널 HBA 구성에 대한 자세한 내용은 [dell.com/support/home](http://dell.com/support/home)에 있는 *DL4xxx - 파이버 채널 구현* 백서를 참조하십시오.

디스크에서 스토리지의 프로비저닝을 시작하기 전에 대기 가상 시스템에 사용할 저장소의 양을 파악해야 합니다. 대기 가상 컴퓨터에 사용 가능한 용량의 백분율을 할당할 수 있습니다. 예를 들어, SRM(Storage Resource Management)을 사용하는 경우 가상 컴퓨터를 호스트하기 위해 프로비저닝되는 모든 장치에 최대 100%의 용량을 할당할 수 있습니다. AppAssure의 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(어플라이언스)** 탭을 선택하면 AppAssure Appliance 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(어플라이언스)** 탭에서 **Tasks(작업)** → **Provisioning(프로비저닝)**을 클릭합니다.  
**Provisioning(프로비저닝)** 화면에 프로비저닝을 위한 예상 용량이 표시됩니다. 이 용량은 새 AppAssure 리포지토리를 생성하는 데 사용됩니다.
2. **Provisioning(프로비저닝)** 화면에 프로비저닝을 위한 예상 용량이 표시됩니다. 이 용량은 새 AppAssure 리포지토리를 생성하는 데 사용됩니다.
3. **Optional Storage Reserve(선택적 저장소 예약)** 섹션에서, **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes(대기 가상 시스템에 프로비저닝 또는 기타 용도로 저장소 일부 할당)** 확인란을 선택하고 할당할 저장소 비율을 표시합니다. 그렇지 않으면 **Optional Storage Reserve(선택적 저장소 예약)** 섹션에 표시되는 저장소 비율은 연결된 모든 디스크에서 할당됩니다.
4. **Provision(프로비전)**을 클릭합니다.



주의: 계속 진행하기 전에 이 절차의 2단계부터 4단계까지 수행해야 합니다.

Status	Task Name	State	Action
✓	Provision MD1400 6VFXQ22 Full shelf 0	Verified: Ready for provisioning	Provision
✓	Provision MD1400 6VFYQ22 Full shelf 0	Verified: Ready for provisioning	Provision
✓	Provision PERC H730P Mini(3,0) Full shelf 0, Create repository	Provisioned	

## 선택한 저장소 프로비저닝

선택한 저장소를 프로비저닝하려면 다음을 수행합니다.

1. **Appliance(어플라이언스)** 탭에서 **Tasks(작업)** → **Provisioning(프로비저닝)**을 클릭합니다.  
**Provisioning(프로비저닝)** 화면에 프로비저닝을 위한 예상 용량이 표시됩니다. 이 용량은 새 AppAssure 리포지토리를 생성하는 데 사용됩니다.
2. 사용 가능한 공간 부분만 프로비저닝하려면 프로비저닝할 저장소 공간 옆의 **Action(작업)** 아래에서 **Provision(프로비전)**을 클릭합니다.
  - 새 리포지토리를 만들려면 **Create a new repository(새 리포지토리 생성)**를 선택하고 리포지토리의 이름을 제공합니다.  
기본적으로 리포지토리 이름은 Repository 1로 표시됩니다. 이 이름을 덮어쓰도록 선택할 수 있습니다.
  - 기존 리포지토리에 용량을 추가하려면 **Expand the existing repository(기존 리포지토리 확장)**를 선택하고 **Existing Repositories(기존 리포지토리)** 목록에서 리포지토리를 선택합니다.



**노트:** 용량을 추가하려면 리포지토리를 추가하는 대신 기존 리포지토리를 확장하는 것이 좋습니다. 개별 리포지토리에서는 중복 제거가 발생하지 않기 때문에 용량이 효율적으로 사용되지 않습니다.



3. **Optional Storage Reserve(선택적 저장소 예약)**에서 **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes(대기 가상 시스템 또는 기타 용도로 프로비저닝되는 저장소의 일부 할당)**를 선택한 후 VM에 할당할 저장소 비율을 지정합니다.
4. **Provision(프로비전)**을 클릭합니다.  
디스크 프로비저닝이 시작되고 **Tasks(작업)** 화면의 **Status(상태)** 영역에 AppAssure 리포지토리 생성 상태가 표시됩니다. **State(상태)**에 **Provisioned(프로비저닝됨)**이 표시됩니다.
5. 디스크 프로비저닝이 완료된 후 상세정보를 보려면 상태 표시등 옆에 >를 클릭합니다.  
**Tasks(작업)** 페이지가 펼쳐지고 상태, 리포지토리 및 가상 디스크 상세정보(할당된 경우)가 표시됩니다.

## 가상 디스크의 공간 할당 삭제

이 절차를 시작하기 전에 삭제할 가상 디스크를 판별합니다. Core 콘솔에서 **Appliance(어플라이언스)** 탭을 선택하고 **Tasks(작업)**를 클릭한 후 해당 가상 디스크가 포함된 리포지토리를 확장하여 가상 디스크 상세정보를 봅니다.

가상 디스크의 공간 할당을 삭제하려면 다음을 수행합니다.

1. OpenManage Server Administrator 응용프로그램에서 **Storage(저장소)**를 확장합니다.
2. 가상 디스크가 포함된 컨트롤러를 확장하고 **Virtual Disks(가상 디스크)**를 선택합니다.
3. 제거할 가상 디스크를 선택하고 **Tasks(작업)** 드롭다운 메뉴에서 **Delete(삭제)**를 선택합니다.
4. 삭제를 확인하면, Core 콘솔의 **Appliance(어플라이언스)** 탭, **Tasks(작업)** 화면에 프로비저닝 가능한 공간이 나타납니다.

## 실패한 작업 해결

AppAssure는 Core 콘솔 홈 페이지에 실패한 확인 작업, 프로비전 작업, 복구 작업을 이벤트로 보고하며 **Appliance(어플라이언스)** 탭, **Tasks(작업)** 화면에서도 볼 수 있습니다.

실패한 작업 해결 방법을 이해하려면 **Appliance(어플라이언스)** 탭, **Tasks(작업)**를 차례로 클릭합니다. **Status(상태)** 옆에 있는 >를 클릭하여 실패한 작업을 확장한 다음 오류 메시지와 권장 조치를 검토합니다.

## 어플라이언스 업그레이드

어플라이언스를 업그레이드하려면 다음을 수행하십시오.

1. **dell.com/support**에서 **복구 및 업데이트 유틸리티**를 DL4300 Backup to Disk Appliance에 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, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator 및 AppAssure Core 소프트웨어의 업데이트 버전이 복구 및 업데이트 유틸리티의 일부로 설치됩니다. 또한 복구 및 업데이트 유틸리티를 통해 RASR 내용도 업데이트됩니다.



**노트:** AppAssure Core 소프트웨어 업그레이드 프로세스 중에, 복구 및 업데이트 유틸리티가 현재 설치된 AppAssure 버전을 알려주며 Core 소프트웨어를 유틸리티에 번들된 버전으로 업그레이드할지 확인하는 메시지를 표시합니다. AppAssure Core 소프트웨어 다운그레이드는 지원되지 않습니다.

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. **dell.com/support**에서 **Recovery and Update Utility(복구 및 업데이트 유틸리티)**를 어플라이언스에 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 and Features, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator 및 AppAssure 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. AppAssure Core의 복구 설치가 필요하지 않을 경우에는 이 단계를 생략해도 됩니다.
8. 유틸리티에 번들된 버전이 설치된 버전보다 높으면, 복구 및 업데이트 유틸리티가 AppAssure Core 소프트웨어를 업그레이드하라는 메시지를 표시합니다.



**노트:** AppAssure 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 AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)가 실행되고, 그렇지 않으면 Core 콘솔이 실행됩니다.

# 워크스테이션 및 서버 보호

## 워크스테이션 및 서버 보호 정보

데이터를 보호하려면 Core 콘솔에서 보호할 워크스테이션과 서버(예: Exchange Server, SQL Server 또는 Linux 서버)를 추가해야 합니다.

 **노트:** 이 섹션에서는 일반적으로 *시스템*이라는 단어가 해당 시스템에 설치된 AppAssure 에이전트 소프트웨어를 나타냅니다.

Core 콘솔에서 AppAssure 에이전트 소프트웨어가 설치된 시스템 식별, 보호할 볼륨 지정, 보호 일정 정의 및 추가적인 보안 조치 추가(예: 암호화) 등을 수행할 수 있습니다. 워크스테이션 및 서버를 보호하기 위해 Core 콘솔에 액세스하는 방법에 대한 자세한 내용은 [시스템 보호](#)를 참조하십시오.

## 시스템 설정 구성

AppAssure에서 시스템에 대한 보호를 추가한 후 기본 시스템 구성 설정(이름 및 호스트 이름 등) 및 보호 설정(시스템의 볼륨에 대한 보호 일정 변경, 볼륨 추가/제거, 보호 일시 중지) 등을 수정할 수 있습니다.

### 구성 설정 보기 및 수정

구성 설정을 보고 수정하려면 다음을 수행하십시오.

1. 보호된 시스템을 추가한 후 다음 중 하나를 수행하십시오.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 수정할 시스템의 하이퍼링크를 클릭합니다.
  - **Navigation(탐색)** 창에서 수정할 시스템을 선택합니다.
2. **Configuration(구성)** 탭을 클릭합니다.  
**Settings(설정)** 페이지가 표시됩니다.
3. **Edit(편집)**를 클릭하여 아래 표에 설명된 대로 시스템 설정을 수정합니다.

텍스트 상자	설명
표시 이름	시스템에 대한 표시 이름을 입력합니다. Core 콘솔에 표시되는 이 시스템의 이름입니다. 기본적으로 이 이름은 시스템의 호스트 이름입니다. 필요한 경우 사용자가 사용하기 쉽게 이름을 변경할 수 있습니다.
호스트 이름	시스템에 대한 호스트 이름을 입력합니다.
포트	시스템의 포트 번호를 입력합니다. Core에서 이 포트를 사용하여 시스템과 통신합니다.

## 텍스트 상자      설명

**리포지토리**      복구 지점의 리포지토리를 선택합니다. 이 시스템의 데이터를 저장할 Core의 리포지토리가 표시됩니다.



**노트:** 복구 지점이 없거나 이전 리포지토리가 누락된 경우에만 이 설정을 변경할 수 있습니다.

**암호화 키**      필요한 경우 암호화 키를 편집합니다. 리포지토리에 저장되는 시스템의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.

## 시스템의 시스템 정보 보기

Core 콘솔에 시스템 목록과 각 시스템의 상태를 포함하여 보호되는 시스템이 모두 표시됩니다.

컴퓨터에 대한 시스템 정보를 보려면 다음을 수행하십시오.

1. Core 콘솔의 **Protected Machines(보호된 시스템)** 아래에서, 자세한 시스템 정보를 볼 시스템을 선택합니다.
2. 해당 시스템의 **Tools(도구)** 탭을 클릭합니다.

시스템에 대한 정보가 **System Information(시스템 정보)** 페이지에 표시됩니다. 표시되는 상세정보는 다음과 같습니다.

- 호스트 이름
- OS Version(OS 버전)
- OS 아키텍처
- 메모리(실제)
- 표시 이름
- 정규화된 도메인 이름
- 가상 시스템 유형(해당되는 경우)

이 시스템에 포함된 볼륨에 대한 상세 정보는 다음과 같습니다.

- 이름
- Device ID(장치 ID)
- 파일 시스템
- 용량(원시 용량, 포맷된 용량, 사용된 용량)
- 프로세서
- 프로세서 유형
- 네트워크 어댑터
- 이 시스템과 연결된 IP 주소

## 시스템 이벤트에 대한 알림 그룹 구성

AppAssure에서 알림 그룹을 생성하여 시스템에 대한 시스템 이벤트가 보고되는 방법을 구성할 수 있습니다. 이러한 이벤트는 시스템 경고 및 오류 등일 수 있습니다.

시스템 이벤트에 대한 알림 그룹을 구성하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 수정할 시스템의 하이퍼링크를 클릭합니다.

- 탐색 창에서 수정할 시스템을 선택합니다.

**Summary(요약)** 탭이 나타납니다.

3. **Configuration(구성)** 탭을 클릭한 후 **Events(이벤트)**를 클릭합니다.  
**Notification Groups(알림 그룹)** 페이지가 표시됩니다.
4. **Use custom alert settings(사용자 지정 경고 설정 사용)**을 클릭한 후 **Apply(적용)**를 클릭합니다.  
**Custom Notification Groups(사용자 지정 알림 그룹)** 화면이 표시됩니다.
5. **Add Group(그룹 추가)**을 클릭하여 시스템 이벤트의 목록을 보낼 새 알림 그룹을 추가합니다.  
**Add Notification Group(알림 그룹 추가)** 대화 상자가 표시됩니다.



**노트:** 기본 경고 설정을 사용하려면 **Use Core(Core 사용)** 경고 설정 옵션을 선택합니다.

6. 다음 표에 설명된 대로 알림 옵션을 추가합니다.

텍스트 상자	설명
이름	알림 그룹의 이름을 입력합니다.
설명	알림 그룹에 대한 설명을 입력합니다.
이벤트 활성화	<p>이 알림 그룹과 공유할 이벤트를 선택합니다. <b>All(모두)</b>를 선택하거나 다음을 포함할 이벤트의 하위 집합을 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 부팅 CD</li> <li>• 로컬 탑재</li> <li>• 메타데이터</li> <li>• 클러스터</li> <li>• 알림</li> <li>• PowerShell 스크립팅</li> <li>• 강제 설치</li> <li>• 연결 기능</li> <li>• 작업</li> <li>• 라이선싱</li> <li>• 로그 자르기</li> <li>• 아카이브</li> <li>• Core 서비스</li> <li>• 내보내기</li> <li>• 보호</li> <li>• 복제</li> <li>• 롤백</li> <li>• 롤업</li> </ul> <p>또한 다음과 같은 유형별로 선택하도록 선택할 수 있습니다.</p> <ul style="list-style-type: none"> <li>• 정보</li> <li>• 경고</li> <li>• 오류</li> </ul>

## 텍스트 상자 설명



**노트:** 유형별로 선택하도록 선택하면 기본적으로 적절한 이벤트가 자동으로 활성화됩니다. 예를 들어, 경고를 선택하면 연결 기능, 작업, 라이선싱, 아카이브, Core 서비스, 내보내기, 보호, 복제 및 롤백 이벤트가 활성화됩니다.

### 알림 옵션

알림을 처리할 방법을 지정하는 방법을 선택합니다. 다음 옵션을 선택할 수 있습니다.

- **Notify by Email(전자 메일로 알림)** - 보낸 사람, 참조 및 숨은 참조 텍스트 상자에서 이벤트를 보낼 전자 메일 주소를 지정합니다.



**노트:** 메일을 수신하려면 SMTP가 구성되어 있어야 합니다.

- **Notify by Windows Event log(Windows 이벤트 로그로 알림)** - Windows 이벤트 로그가 알림을 제어합니다.
- **Notify by syslogd(시스템 로그로 알림)** - 이벤트를 보낼 호스트 이름과 포트를 지정합니다.
  - **Host(호스트)** - 서버에 대한 호스트 이름을 입력합니다.
  - **Port(포트)** - 서버와 통신할 포트 번호를 입력합니다.

7. **OK(확인)**를 클릭하여 변경 내용을 저장합니다.

8. 기존 알림 그룹을 편집하려면 편집할 알림 그룹 옆에 있는 **Edit(편집)**를 클릭합니다.

**Edit Notification Group(알림 그룹 편집)** 대화 상자가 열립니다. 여기에서 설정을 편집할 수 있습니다.

## 시스템 이벤트에 대한 알림 그룹 편집

시스템 이벤트에 대한 알림 그룹을 편집하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하여 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 수정할 시스템의 하이퍼링크를 클릭합니다.
  - 또는 탐색 창에서 수정할 시스템을 선택합니다.

**Summary(요약)** 탭이 나타납니다.

3. **Configuration(구성)** 탭을 클릭한 후 **Events(이벤트)**를 클릭합니다.
4. **Use custom alert settings(사용자 지정 경고 설정 사용)**을 클릭한 후 **Apply(적용)**를 클릭합니다.  
**Custom Notification Groups(사용자 지정 알림 그룹)** 화면이 표시됩니다.
5. **Action(작업)** 열 아래에서 **Edit(편집)** 아이콘을 클릭합니다.  
**Edit Notification Group(알림 그룹을 편집)** 대화 상자가 나타납니다.
6. 다음 표에 설명된 대로 알림 옵션을 편집합니다.

### 텍스트 상자 설명

이름

알림 그룹의 이름을 나타냅니다.



**노트:** 알림 그룹의 이름은 편집할 수 없습니다.

설명

알림 그룹에 대한 설명을 입력합니다.

텍스트 상자  
이벤트 활성화

설명

알림 그룹과 공유할 이벤트를 선택합니다. **All(모두)**를 선택하거나 다음을 포함할 이벤트의 하위 집합을 선택할 수 있습니다.

- 부팅 CD
- 로컬 탑재
- 메타데이터
- 클러스터
- 알림
- PowerShell 스크립팅
- 강제 설치
- 연결 기능
- 작업
- 라이선싱
- 로그 자르기
- 아카이브
- Core 서비스
- 내보내기
- 보호
- 복제
- 롤백
- 롤업

또한 다음과 같은 유형별로 선택하도록 선택할 수 있습니다.

- 정보
- 경고
- 오류



**노트:** 유형별로 선택하도록 선택하면 기본적으로 적절한 이벤트가 자동으로 활성화됩니다. 예를 들어, 경고를 선택하면 연결 기능, 작업, 라이선싱, 아카이브, Core 서비스, 내보내기, 보호, 복제 및 롤백 이벤트가 활성화됩니다.

알림 옵션

알림을 처리할 방법을 지정하는 방법을 선택합니다. 다음 옵션을 선택할 수 있습니다.

- **Notify by Email(전자 메일로 알림)** - 보낸 사람, 참조 및 숨은 참조 텍스트 상자에서 이벤트를 보낼 전자 메일 주소를 지정합니다.



**노트:** 전자 메일을 수신하려면 SMTP가 구성되어 있어야 합니다.

- **Notify by Windows Event log(Windows 이벤트 로그로 알림)** - Windows 이벤트 로그가 알림을 제어합니다.
- **Notify by syslogd(시스템 로그로 알림)** - 이벤트를 보낼 호스트 이름과 포트를 지정해야 합니다.
  - **Host(호스트)** - 서버에 대한 호스트 이름을 입력합니다.
  - **Port(포트)** - 서버와 통신할 포트 번호를 입력합니다.

7. **OK(확인)**를 클릭합니다.

## 보존 정책 설정 사용자 지정

시스템의 보존 정책은 에이전트 시스템에 대한 복구 지점이 리포지토리에 저장되는 기간을 지정합니다. 보존 정책은 백업 스냅샷을 장기간 보존하고 이러한 백업 스냅샷을 관리하는 데 사용됩니다. 시간이 지나 오래된 백업을 삭제하는 롤업 프로세스에서 이러한 보존 정책을 적용합니다. 또한 이 작업은 [클러스터 노드 설정 수정 프로세스](#)의 단계에 해당합니다.

보존 정책 설정을 사용자 지정하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 수정할 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 수정할 시스템을 선택합니다.

**Summary(요약)** 탭이 나타납니다.

3. **Configuration(구성)** 탭을 클릭한 후 **Retention Policy(보존 정책)**를 클릭합니다.



**노트:** Core에 구성된 기본 보존 정책을 사용하려면 Use Core default retention policy(Core 기본 보존 정책 사용) 옵션이 선택되어 있는지 확인하십시오.

**Retention Policy(보존 정책)** 화면이 표시됩니다.

4. 사용자 지정 정책을 설정하려면 **Use custom retention policy(사용자 지정 보존 정책 사용)**를 클릭합니다.

**Custom Retention Policy(사용자 지정 보존 정책)** 화면이 표시됩니다.

5. **Enable Rollup(롤업 활성화)**를 선택하고 필요에 맞게 백업 데이터를 보존할 시간 간격을 지정합니다. 아래에 보존 정책 옵션에 대해 설명되어 있습니다.

### 텍스트 상자      설명

**n[보존 기간] 동안**      복구 지점에 대한 보존 기간을 지정합니다.

**모든 복구 지점 유지**      보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 **3**입니다.

다음에서 선택할 수 있습니다.

- 일
- 주
- 월
- 년

**n[보존 기간] 동안 한 시간에 하나의 복구 지점 유지**      보다 세부적인 보존 수준을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있는 기본 설정이 포함된 구성 블록으로 사용됩니다.

**모든 복구 지점 유지**      보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2입니다.

다음에서 선택할 수 있습니다.

- 일
- 주
- 월
- 년



## 텍스트 상자 설명

**n[보존 기간] 동안 하루에 하나의 복구 지점 유지** 보다 세부적인 보존 수준을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있는 구성 블록으로 사용됩니다.  
보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 4입니다.

다음에서 선택할 수 있습니다.

- 일
- 주
- 월
- 년

**n[보존 기간] 동안 한 주에 하나의 복구 지점 유지** 보다 세부적인 보존 수준을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있는 구성 블록으로 사용됩니다.  
보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 3입니다.

다음에서 선택할 수 있습니다.

- 주
- 월
- 년

**n[보존 기간] 동안 한 달에 하나의 복구 지점 유지** 보다 세부적인 보존 수준을 제공합니다. 이는 복구 지점이 유지되는 기간을 더욱 구체적으로 정의할 수 있는 구성 블록으로 사용됩니다.  
보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다. 기본값은 2입니다.

다음에서 선택할 수 있습니다.

- 월
- 년

**n[보존 기간] 동안 일 년에 하나의 복구 지점 유지** 보존 기간을 나타내는 숫자를 입력하고 기간을 선택합니다.

가장 최근 복구 지점을 보여주는 Newest Recovery Point(가장 최근 복구 지점) 텍스트 상자가 표시됩니다. 보존 정책 설정에 따라 가장 오래된 복구 지점이 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

가장 최근 복구 지점이 현재 요일, 달 및 연도로 설정됩니다.

이 예에서 가장 오래된 복구 지점은 1년 4개월 6일이 지난 복구 지점입니다.

6. **Apply(적용)**를 클릭하여 변경 사항을 저장합니다.
7. **Force Rollup(롤업 강제 적용)**을 선택하여 시스템의 현재 보존 정책을 기반으로 롤업을 수행하거나, 매일 밤 롤업이 수행되는 동안 사용자가 정의한 보존 정책이 적용되도록 할 수 있습니다.

## 라이선스 정보 보기

시스템에 설치된 AppAssure Agent 소프트웨어에 대한 현재 라이선스 상태 정보를 볼 수 있습니다.

라이선스 정보를 보려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 보려는 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 보려는 시스템을 선택합니다.
3. **Configuration(구성)** 탭에서 **Licensing(라이선싱)**을 클릭합니다.  
**Status(상태)** 화면에 제품 라이선싱에 대한 상세정보가 표시됩니다.

## 보호 일정 수정

AppAssure에서 시스템의 특정 볼륨에 대한 보호 일정을 수정할 수 있습니다.

보호 일정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 수정할 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 수정할 시스템을 선택합니다.
3. 다음 중 하나를 수행합니다.
  - 시스템의 **Summary(요약)** 탭에 있는 **Volumes(볼륨)** 테이블에서 사용자 지정할 볼륨에 대한 보호 일정의 하이퍼링크를 클릭합니다.
  - **Configuration(구성)** 탭을 클릭한 후 **Protection Settings(보호 설정)**을 클릭합니다. 볼륨 목록에서 사용자 지정할 볼륨 옆에 있는 **Edit(편집)** 아이콘을 클릭합니다.

**Protection Schedule(보호 일정)** 대화 상자가 표시됩니다.

4. **Protection Schedule(보호 일정)** 대화 상자에서 필요에 따라 데이터를 보호하기 위해 다음 일정 옵션을 편집합니다. 다음 표에 옵션에 대해 설명되어 있습니다.

옵션	설명
간격	<b>Weekday(평일)</b> - 특정 시간 간격(예: 15분마다)으로 데이터를 보호하려면 <b>Interval(간격)</b> 을 선택한 후 다음을 수행합니다. <ul style="list-style-type: none"><li>• 최대 사용량 시간 동안 데이터를 보호할 시기를 사용자 지정하려면 드롭다운 메뉴에서 <b>Start Time(시작 시간)</b>, <b>End Time(종료 시간)</b> 및 <b>Interval(간격)</b>을 선택할 수 있습니다.</li><li>• 사용량이 적을 때 데이터를 보호하려면 <b>Protection interval during off-peak times(사용량이 적을 때 보호 간격)</b> 확인란을 선택한 후 드롭다운 메뉴에서 보호할 간격을 선택합니다.</li></ul>

## 옵션

## 설명

**Weekends(주말)** - 주말 동안 데이터를 보호하려면 **Protection interval during weekends(주말 동안 보호 간격)** 확인란을 선택한 후 드롭다운 메뉴에서 간격을 선택합니다.



**노트:** SQL 또는 Exchange 데이터베이스와 로그가 서로 다른 볼륨에 있는 경우 볼륨이 하나의 보호 그룹에 속해야 합니다.

## 매일

데이터를 매일 보호하려면 **Daily(매일)** 옵션을 선택한 후 **Protection Time(보호 시간)** 드롭다운 메뉴에서 데이터 보호를 시작할 시간을 선택합니다.

## 보호 안 함

이 볼륨에서 보호를 제거하려면 **No Protection(보호 안 함)** 옵션을 선택합니다.

이 시스템의 모든 볼륨에 이러한 사용자 지정 설정을 적용하려면 **Apply to All Volumes(모든 볼륨에 적용)**을 선택합니다.

5. 필요한 내용을 모두 변경하면 **OK(확인)**를 클릭합니다.

## 전송 설정 수정

보호되는 시스템의 데이터 전송 프로세스를 관리하는 설정을 수정할 수 있습니다. 이 섹션에 설명된 전송 설정은 에이전트 수준의 설정입니다. 코어 수준의 전송을 적용하려면 [전송 큐 설정 수정](#)을 참조하십시오.



**주의:** 전송 설정을 변경하면 환경에 상당히 영향을 줄 수 있습니다. 전송 설정값을 수정하기 전에 **Dell AppAssure 기술 자료**(<https://support.software.dell.com/appassure/kb>)에 있는 전송 성능 조정 안내서를 참조하십시오.

다음과 같은 세 가지 전송 유형이 있습니다.

### 스냅샷

보호된 시스템에 데이터를 백업하는 전송 유형입니다.

### VM 내보내기

시스템을 보호하도록 정의된 일정에 따라 지정된 대로 백업 정보와 매개변수가 모두 포함된 가상 시스템을 생성하는 전송 유형입니다.

### 롤백

보호된 시스템에서 백업 정보를 복원하는 프로세스입니다.

데이터 전송은 네트워크를 통해 Agent 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 에이전트 시스템 백업, VM 내보내기, 롤백을 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.

전송 설정을 수정하려면 다음을 수행하십시오.


1. Core 콘솔에서 다음 중 하나를 수행합니다.
  - **Machines(시스템)** 탭을 클릭하고 수정할 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 수정할 시스템을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 수정할 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 수정할 시스템을 선택합니다.
3. **Configuration(구성)** 탭을 클릭하고 **Transfer Settings(전송 설정)**을 클릭합니다.  
현재 전송 설정이 표시됩니다.
4. **Transfer Settings(전송 설정)** 페이지에서 **Change(변경)**를 클릭합니다.  
**Transfer Settings(전송 설정)** 대화 상자가 표시됩니다.
5. 다음 표에 설명된 대로 시스템에 대한 **Transfer Settings(전송 설정)** 옵션을 입력합니다.

#### 텍스트 상자      설명


**Priority(우선순위)** 보호되는 시스템 간에 전송 우선순위를 설정합니다. 보호되는 다른 시스템과 비교하여 우선순위를 할당할 수 있습니다. 우선순위가 가장 높은 1부터 가장 낮은 10까지 중에서 선택할 수 있습니다. 기본 설정값은 5입니다.

 **노트:** 큐에 있는 전송에 우선순위가 적용됩니다.

**최대 동시 스트림 수** 에이전트당 동시에 처리하기 위해 Core에 전송되는 최대 TCP 링크 수를 설정합니다.


 **노트:** 이 값은 8로 설정하는 것이 좋습니다. 패킷이 손실된 경우 이 설정을 늘려 보십시오.

**최대 동시 쓰기 수** 에이전트 연결당 최대 동시 디스크 쓰기 작업의 수를 설정합니다.

 **노트:** 이 값은 최대 동시 스트림 수 값과 동일하게 설정하는 것이 좋습니다. 하지만 패킷이 유실된 경우 이 값을 약간 줄이십시오. 예를 들어 최대 동시 스트림 수가 8로 설정되어 있으면 이 옵션을 7로 설정하십시오.


**최대 다시 시도 횟수** 일부 작업을 완료하지 못한 경우 보호된 시스템 각각에 대한 최대 다시 시도 횟수를 설정합니다.

**최대 세그먼트 크기** 컴퓨터에서 단일 TCP 세그먼트로 수신할 수 있는 최대 데이터 양(바이트)을 지정합니다. 기본 설정값은 4194304입니다.

 **주의:** 이 기본 설정값을 변경하지 마십시오.

**최대 전송 큐 크기** 동시에 전송할 수 있는 명령 수를 지정합니다. 시스템에서 동시 입력/출력 작업이 많을 경우에는 이 옵션값을 높게 조정할 수 있습니다.

**스트림당 대기 중인 읽기** 백엔드에 저장되기 위해 큐에 대기 중인 읽기 작업 수를 지정합니다. 이 설정은 에이전트의 큐 대기를 제어하는 데 유용합니다.

 **노트:** 이 값은 24로 설정하는 것이 좋습니다.

텍스트 상자	설명
제외된 기록기	<p>제외할 기록기를 선택합니다. 목록에 표시되는 기록기는 현재 구성하는 시스템과 관련이 있기 때문에 일부 기록기는 목록에 표시되지 않을 수 있습니다. 목록에 표시되는 기록기는 다음과 같습니다.</p> <ul style="list-style-type: none"> <li>• ASR 기록기</li> <li>• BITS 기록기</li> <li>• COM+ REGDB 기록기</li> <li>• 성능 카운터 기록기</li> <li>• 레지스트리 기록기</li> <li>• 새도 복사본 최적화 기록기</li> <li>• SQL Server 기록기</li> <li>• 시스템 기록기</li> <li>• 작업 스케줄러 기록기</li> <li>• VSS 메타데이터 저장소 기록기</li> <li>• WMI 기록기</li> </ul>
데이터 전송 서버 포트	전송에 사용되는 포트를 설정합니다. 기본 설정값은 8009입니다.
전송 시간 제한	패킷을 전송하지 않고 정지할 수 있는 시간을 분 및 초 단위로 지정합니다.
스냅샷 시간 제한	스냅샷 생성을 위해 대기하는 최대 시간을 분 및 초 단위로 지정합니다.
네트워크 읽기 시간 제한	읽기 연결을 위해 대기하는 최대 시간을 분 및 초 단위로 지정합니다. 이 시간 내에 네트워크 읽기가 수행되지 않으면 작업이 반복됩니다.
네트워크 쓰기 시간 제한	쓰기 연결을 위해 대기하는 최대 시간을 초 단위로 지정합니다. 이 시간 내에 네트워크 쓰기가 수행되지 않으면 작업이 반복됩니다.

6. **OK(확인)**를 클릭합니다.

## 서비스 다시 시작

서비스를 다시 시작하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 다시 시작할 시스템의 하이퍼링크를 클릭합니다.
  - **Navigation(탐색)** 창에서, 다시 시작할 시스템을 선택합니다.
3. **Tools(도구)** 탭을 클릭한 후 **Diagnostics(진단)**을 클릭합니다.
4. **Restart Service(서비스 다시 시작)** 옵션을 선택한 후 **Restart Service(서비스 다시 시작)** 단추를 클릭합니다.

## 시스템 로그 보기


시스템에 오류 또는 문제가 발생한 경우 문제를 해결하기 위해 로그를 확인합니다.

시스템 로그를 보려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 보려는 로그가 포함된 시스템의 하이퍼링크를 클릭합니다.
  - **Navigation(탐색)** 창에서, 보려는 로그가 포함된 시스템을 선택합니다.
3. **Tools(도구)** 탭을 클릭한 후 **Diagnostics(진단)**을 클릭합니다.
4. **View Log(로그 보기)** 링크를 클릭합니다.

## 시스템 보호

이 항목에서는 지정하는 시스템에서 데이터를 보호하는 방법을 설명합니다.

 **노트:** 시스템을 보호하려면 Agent 소프트웨어가 시스템에 설치되어 있어야 합니다. 이 절차를 수행하기 전에 Agent 소프트웨어를 설치하거나 **Connection(연결)** 대화 상자에서 보호를 정의할 때 에이전트에 소프트웨어를 배포할 수 있습니다. 시스템 보호 프로세스 중에 에이전트 소프트웨어 설치 방법에 대해서는 [에이전트를 보호할 때 Agent 소프트웨어 배포](#)를 참조하십시오.

보호를 추가할 때는 보호할 시스템의 이름 또는 IP 주소와 해당 시스템의 볼륨을 지정하고 각 볼륨의 보호 일정을 정의해야 합니다.

여러 시스템을 동시에 보호하려면 [다중 시스템 보호](#)를 참조하십시오.

시스템을 보호하려면 다음을 수행하십시오.

1. Agent 소프트웨어를 설치한 후 Agent 소프트웨어가 설치된 시스템을 다시 부팅합니다(아직 부팅하지 않은 경우).
2. Core 시스템의 Core 콘솔에서 다음 중 하나를 수행합니다.
  - **Home(홈)** 탭의 **Protected machines(보호되는 시스템)**에서 **Protect Machine(시스템 보호)**을 클릭합니다.
  - **Machines(시스템)** 탭을 선택하고 **Actions(작업)** 드롭다운 메뉴에서 **Protect Machine(시스템 보호)**을 클릭합니다.

**Connect(연결)** 대화 상자가 표시됩니다.

3. **Connect(연결)** 대화 상자에 아래 표에 설명된 대로 연결할 시스템에 대한 정보를 입력합니다.

텍스트 상자	설명
--------	----


호스트	보호할 시스템의 호스트 이름 또는 IP 주소입니다.
-----	------------------------------

포트	Core가 시스템의 에이전트와 통신하는 포트 번호입니다. 기본 포트 번호는 8006입니다.
----	--

사용자 이름	이 컴퓨터에 연결하는 데 사용한 사용자 이름입니다(예: administrator).
--------	--

암호	이 시스템에 연결하는 데 사용되는 암호입니다.
----	---------------------------

4. **Connect(연결)**를 클릭하여 이 시스템에 연결합니다.


 **노트:** 해당 시스템에 Agent 소프트웨어가 아직 설치되어 있지 않은 경우 [에이전트를 보호할 때 Agent 소프트웨어 배포](#)에 설명된 절차를 따르십시오. Agent 소프트웨어를 배포한 후 에이전트 시스템을 다시 시작하고 다음 단계를 계속 진행합니다.

5. **Protect(보호)** 대화 상자에서 아래 표에 설명된 대로 필요에 따라 설정을 편집합니다.

필드	설명
표시 이름	<p><b>Connect(연결)</b> 대화 상자에 지정한 호스트 이름이나 IP 주소가 이 텍스트 필드에 나타납니다. 선택적으로, Core 콘솔에 표시할 시스템의 새 이름을 입력할 수도 있습니다.</p> <p> <b>노트: Configuration(구성)</b> 탭에서 기존 시스템의 표시 이름을 변경할 수 있습니다.</p>
리포지토리	Core에서 이 시스템의 데이터를 저장할 리포지토리를 선택합니다.
암호화 키	리포지토리에 저장되는 이 시스템의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.
	<p> <b>노트:</b> 리포지토리에 대한 암호화 설정은 Core 콘솔의 <b>Configuration(구성)</b> 탭에 정의되어 있습니다.</p>
처음에 보호 일시 중지	보호할 시스템을 추가하면 AppAssure에서 데이터의 기본 스냅샷을 만드는 프로세스를 자동으로 시작합니다. 이 확인란을 선택하면 처음에 보호를 일시 중지할 수 있습니다. 그런 다음 데이터 보호를 시작할 때 스냅샷을 수동으로 강제 적용해야 합니다. 자세한 내용은 <a href="#">스냅샷 강제 적용</a> 을 참조하십시오.
볼륨 그룹	<p>Volume Groups(볼륨 그룹)에서, 보호할 볼륨을 정의하고 보호 일정을 설정할 수 있습니다.</p> <p>시스템에 있는 모든 볼륨에 기본 보호 일정인 60분을 설정하려면 <b>Apply Default(기본값 적용)</b>를 클릭합니다.</p> <p>시스템에서 원하는 볼륨을 선택하여 개별적으로 보호 매개변수를 정의할 수도 있습니다.</p> <p>초기 설정에서는 기본 보호 일정인 60분을 적용합니다. 볼륨의 보호 일정을 수정하려면 해당 볼륨에서 <b>Edit(편집)</b>를 클릭합니다. 그런 다음 스냅샷 간의 간격을 추가로 정의하거나(별도의 주말 일정 정의 가능) 매일 스냅샷을 시작할 시간을 지정할 수 있습니다.</p> <p>선택한 볼륨의 보호 일정 편집에 대한 자세한 내용은 <a href="#">볼륨에 대한 사용자 지정 일정 생성</a>을 참조하십시오.</p>


## 6. Protect(보호)를 클릭합니다.

시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 기본 이미지(보호되는 시스템에 있는 모든 데이터의 스냅샷)가 Core의 리포지토리에 즉시 전송됩니다.


 **주의:** Linux 시스템을 보호할 경우 보호되는 볼륨의 탑재를 수동으로 해제하지 않아야 합니다. 탑재를 해제해야 하는 경우 볼륨을 탑재 해제하기 전에 **bsctl -d [path\_to\_volume]** 명령을 실행해야 합니다. 이 명령에서 **[path\_to\_volume]**은 볼륨의 탑재 지점이 아닌 볼륨의 파일 설명자를 나타내며 **/dev/sda1**과 유사한 형식이어야 합니다.


## 에이전트를 보호할 때 Agent 소프트웨어 배포

보호용 에이전트를 추가할 때 에이전트를 다운로드하여 배포할 수 있습니다.

 **노트:** 보호할 시스템에 Agent 소프트웨어가 이미 설치되어 있는 경우에는 이 과정이 필요하지 않습니다.

보호용 에이전트를 추가할 때 에이전트를 배포하려면 다음을 수행합니다.

1. **Protect Machine(시스템 보호) → Connect(연결)** 대화 상자에서, 적절한 연결 설정을 입력한 후 **Connect(연결)**를 클릭합니다.  
**Deploy Agent(에이전트 배포)** 대화 상자가 표시됩니다.
2. **Yes(예)**를 클릭하여 Agent 소프트웨어를 시스템에 원격으로 배포합니다.  
**Deploy Agent(에이전트 배포)** 대화 상자가 표시됩니다.
3. 다음과 같이 로그인 및 보호 설정을 입력합니다.
  - **Host name(호스트 이름)** - 보호할 시스템의 호스트 이름이나 IP 주소를 지정합니다.
  - **Port(포트)** - Core가 시스템에 있는 Agent와 통신하는 포트 번호를 지정합니다. 기본값은 8006입니다.
  - **User name(사용자 이름)** - 이 시스템에 연결하는 데 사용되는 사용자 이름을 지정합니다(예: administrator).
  - **Password(암호)** - 이 시스템에 연결하는 데 사용되는 암호를 지정합니다.
  - **Display name(표시 이름)** - Core 콘솔에 표시되는 시스템의 이름을 지정합니다. 표시 이름은 호스트 이름과 동일할 수 있습니다.
  - **Protect machine after install(설치 후 시스템 보호)** - 이 옵션을 선택하면 보호할 시스템을 추가한 후 AppAssure가 데이터의 기본 스냅샷을 만들 수 있습니다. 이 옵션은 기본적으로 선택되며, 선택을 취소할 경우 데이터 보호를 시작할 때 수동으로 스냅샷을 강제 적용해야 합니다. 수동으로 스냅샷 강제 적용에 대한 자세한 내용은 *Dell DL4300 어플라이언스 사용 설명서*의 '스냅샷 강제 적용' 항목을 참조하십시오.
  - **Repository(리포지토리)** - 이 에이전트의 데이터를 저장할 리포지토리를 선택합니다.  
 **노트:** 여러 에이전트의 데이터를 하나의 리포지토리에 저장할 수 있습니다.
  - **Encryption Key(암호화 키)** - 리포지토리에 저장되는 이 시스템에 있는 모든 볼륨의 데이터에 암호화를 적용할지 여부를 지정합니다.

 **노트:** 리포지토리의 암호화 설정은 Core 콘솔의 **Configuration(구성)** 탭에서 정의합니다.

4. **Deploy(배포)**를 클릭합니다.  
**Deploy Agent(에이전트 배포)** 대화 상자가 닫힙니다. 선택한 에이전트가 보호되는 시스템 목록에 나타나려면 약간의 시간이 걸릴 수도 있습니다.

## 볼륨에 대한 사용자 지정 일정 생성

볼륨에 대한 사용자 지정 일정을 생성하려면 다음을 수행하십시오.

1. **Protect Machine(시스템 보호)** 대화 상자(이 대화 상자에 액세스하는 방법에 대한 자세한 내용은 [시스템 보호](#) 참조)의 **Volume Groups(볼륨 그룹)**에서 보호할 볼륨을 선택하고 **Edit(편집)**를 클릭합니다.  
**Protection Schedule(보호 일정)** 대화 상자가 표시됩니다.
2. **Protection Schedule(보호 일정)** 대화 상자에서 아래에 설명된 대로 데이터를 보호할 일정 옵션 중 하나를 선택합니다.



## 텍스트 상자 설명

### 간격

다음에서 선택할 수 있습니다.

- **Weekday(평일)** - 특정 간격으로 데이터를 보호하려면 **Interval(간격)**을 선택한 후 다음을 수행합니다.
  - 최대 사용량 시간 동안 데이터를 보호할 시기를 사용자 지정하려면 드롭다운 메뉴에서 **Start Time(시작 시간)**, **End Time(종료 시간)** 및 **Interval(간격)**을 지정할 수 있습니다.
  - 사용량이 적을 때 데이터를 보호하려면 **Protection interval during off-peak times(사용량이 적을 때 보호 간격)**을 선택한 후 **Time(시간)** 드롭다운 메뉴에서 보호할 간격을 선택합니다.
- **Weekends(주말)** - 주말 동안에도 데이터를 보호하려면 **Protection interval during weekends(주말 동안 보호 간격)**을 선택한 후 드롭다운 메뉴에서 **Interval(간격)**을 선택합니다.

### 매일

데이터를 매일 보호하려면 **Daily protection(매일 보호)** 옵션을 선택한 후 **Time(시간)** 드롭다운 메뉴에서 데이터 보호를 시작할 시간을 선택합니다.

### 보호 안 함

이 볼륨에서 보호를 제거하려면 **No Protection(보호 안 함)** 옵션을 선택합니다.

이 시스템의 모든 볼륨에 이러한 사용자 지정 설정을 적용하려면 **Apply to All Volumes(모든 볼륨에 적용)**을 선택합니다.

3. 필요한 내용을 모두 변경하면 **OK(확인)**를 클릭합니다.
4. 추가 볼륨을 사용자 지정하려면 2단계와 3단계를 반복하십시오.
5. **Protect Machine(시스템 보호)** 대화 상자에서 **Protect(보호)**를 클릭합니다.

## Exchange Server 설정 수정

Microsoft Exchange Server의 데이터를 보호하는 경우 Core 콘솔에서 추가 설정을 구성해야 합니다.

Exchange Server 설정을 수정하려면 다음을 수행하십시오.

1. 보호할 Exchange Server 시스템을 추가한 후 Core 콘솔의 **Navigation(탐색)** 창에서 해당 시스템을 선택합니다.  
시스템의 **Summary(요약)** 탭이 표시됩니다.
2. **Summary(요약)** 탭에서 **Exchange Server Settings(Exchange Server 설정)** 링크를 클릭합니다.  
**Exchange Server Settings(Exchange Server 설정)** 대화 상자가 표시됩니다.
3. **Exchange Server Settings(Exchange Server 설정)** 대화 상자에서 다음 설정을 선택하거나 지울 수 있습니다.
  - 자동 탑재 기능 검사 사용
  - 야간 체크섬 검사 사용 - 다음을 수행하여 이 설정을 사용자 지정할 수 있습니다.
    - 체크섬 검사 성공 후 자동으로 Exchange 로그 자르기
    - 체크섬 검사를 완료하기 전에 로그 자르기
4. 또한 Exchange Server에 대한 로그인 자격 증명을 수정할 수 있습니다. 수정하려면 **Exchange Server Information(Exchange Server 정보)** 섹션을 아래로 스크롤한 후 **Change Credentials(자격 증명 변경)**을 클릭합니다.  
**Set Exchange Credentials(Exchange 자격 증명 설정)** 대화 상자가 표시됩니다.
5. 새 자격 증명을 입력한 후 **OK(확인)**를 클릭합니다.


## SQL Server 설정 수정

Microsoft SQL Server의 데이터를 보호하는 경우 Core 콘솔에서 추가 설정을 구성해야 합니다.  
SQL Server 설정을 수정하려면 다음을 수행하십시오.

1. 보호할 SQL Server 시스템을 추가한 후 Core 콘솔의 **Navigation(탐색)** 창에서 해당 시스템을 선택합니다.  
시스템의 **Summary(요약)** 탭이 표시됩니다.
2. **Summary(요약)** 탭에서 SQL Server 설정 링크를 클릭합니다.  
**SQL Server Settings(SQL Server 설정)** 대화 상자가 표시됩니다.
3. **SQL Server Settings(SQL Server 설정)** 대화 상자에서 필요에 따라 다음 설정을 편집합니다.
  - 야간 연결 기능 검사 활성화
  - 연결 기능 검사를 완료한 후 로그 자르기(단순 복구 모델에만 해당)
4. 또한 SQL Server에 대한 로그인 자격 증명을 수정할 수 있습니다. 수정하려면 **SQL Server Information(SQL Server 정보)** 테이블을 아래로 스크롤한 후 **Change Credentials(자격 증명 변경)**을 클릭합니다.  
**Set SQL Server Credentials(SQL Server 자격 증명 설정)** 대화 상자가 표시됩니다.
5. 새 자격 증명을 입력한 후 **OK(확인)**를 클릭합니다.

## 에이전트 배포(강제 설치)

에이전트를 설치하려면 AppAssure에 Microsoft.net이 필요합니다. 클라이언트 시스템에 Microsoft.net을 설치해야 수동으로 에이전트를 설치하거나 강제로 설치할 수 있습니다.  
AppAssure 5를 사용하면 보호를 위해 개별 Windows 시스템에 AppAssure 5 Agent 설치 관리자를 배포할 수 있습니다. 다음 절차의 단계를 완료하여 에이전트에 설치 관리자를 강제 적용합니다. 동시에 여러 시스템에 에이전트를 배포하려면 [다중 시스템에 배포](#)를 참조하십시오.

 **노트:** 원격 설치를 수행할 수 있도록 지정하는 보안 정책에 따라 에이전트를 구성해야 합니다.

에이전트를 배포하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Deploy Agent(에이전트 배포)**를 클릭합니다.  
**Deploy Agent(에이전트 배포)** 대화 상자가 표시됩니다.
3. **Deploy Agent(에이전트 배포)** 대화 상자에 다음 표에 설명된 대로 로그인 설정을 입력합니다.

텍스트 상자	설명
시스템	배포할 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
사용자 이름	이 시스템에 연결할 사용자 이름을 입력합니다(예: administrator).
암호	이 시스템에 연결할 암호를 입력합니다.
설치 후 자동 재부팅	AppAssure Agent 설치 프로그램의 배포 및 설치가 완료되면 Core를 시작할 것인지 지정합니다.
4. **Verify(확인)**를 클릭하여 입력한 자격 증명을 유효성 검사합니다.  
유효성 검사가 수행 중이라는 메시지를 보여주는 **Deploy Agent(에이전트 배포)** 대화 상자가 표시됩니다.
5. 유효성 검사 프로세스를 취소하려면 **Abort(중단)**를 클릭합니다.  
유효성 검사 프로세스가 완료되면 유효성 검사가 완료되었다는 메시지가 나타납니다.

6. **Deploy(배포)**를 클릭합니다.  
배포가 시작되었음을 나타내는 메시지가 표시됩니다. **Events(이벤트)** 탭에서 진행 상태를 볼 수 있습니다.
7. 에이전트 배포 상태에 대한 자세한 내용을 보려면 **Show details(상세정보 표시)**를 클릭하십시오.
8. **OK(확인)**를 클릭합니다.

## 새 에이전트 복제

소스 Core에서 보호할 AppAssure Agent를 추가하면 AppAssure에서 새 에이전트를 기존 대상 Core에 복제할 수 있는 옵션을 제공합니다.

새 에이전트를 복제하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하여 **Machines(시스템)** 탭을 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Protect Machine(시스템 보호)**을 클릭합니다.
3. **Protect Machine(시스템 보호)** 대화 상자에 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
호스트	보호할 시스템의 호스트 이름 또는 IP 주소를 입력합니다.
포트	AppAssure Core에서 시스템의 에이전트와 통신하는 데 사용하는 포트 번호를 입력합니다.
사용자 이름	이 시스템에 연결하는 데 사용되는 사용자 이름을 입력합니다(예: Administrator).
암호	이 시스템에 연결하는 데 사용되는 암호를 입력합니다.

4. **Connect(연결)**를 클릭하여 이 시스템에 연결합니다.
5. **Show Advanced Options(고급 옵션 표시)**을 클릭하고 필요에 따라 다음 설정을 편집합니다.

텍스트 상자	설명
표시 이름	Core 콘솔에 표시할 시스템의 이름을 입력합니다.
리포지토리	AppAssure Core에서 이 시스템의 데이터가 저장되는 리포지토리를 선택합니다.
암호화 키	리포지토리에 저장되는 이 시스템의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.



**노트:** 리포지토리에 대한 암호화 설정은 Core 콘솔의 **Configuration(구성)** 탭에 정의되어 있습니다.

원격 Core	에이전트를 복제할 대상 Core를 지정합니다.
원격 리포지토리	대상 Core에서 이 시스템의 복제된 데이터를 저장할 원하는 리포지토리의 이름입니다.
일시 중지	복제를 일시 중지하려면 이 확인란을 선택합니다(예: AppAssure에서 새 에이전트의 기본 이미지를 생성할 때까지 일시 중지).
일정	다음 옵션 중 하나를 선택합니다. <ul style="list-style-type: none"> <li>• 기본 일정을 사용하여 모든 볼륨 보호</li> <li>• 사용자 지정 일정을 사용하여 특정 볼륨 보호</li> </ul>

## 텍스트 상자      설명



**노트:** 기본 일정은 15분 간격입니다.

**처음에 보호 일시 중지** 보호를 일시 중지하려면 이 확인란을 선택합니다(예: 최대 사용 시간이 지날 때까지 AppAssure가 기본 이미지를 생성할 수 없도록 방지).

6. **Protect(보호)**를 클릭합니다.

## 시스템 관리

이 섹션에서는 AppAssure 환경에서 시스템 제거, 복제 설정, 로그 자르기 강제 적용 및 작업 취소 등과 같이 시스템을 관리할 때 수행할 수 있는 여러 작업에 대해 설명합니다.

### 시스템 제거

1. Core 콘솔로 이동하여 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭에서 다음 중 하나를 수행합니다.
  - 제거할 시스템의 하이퍼링크를 클릭합니다.
  - 또는 탐색 창에서 제거할 시스템을 선택합니다.
3. **Actions(작업)** 드롭다운 메뉴에서 **Remove Machines(시스템 제거)**를 클릭한 후 다음 표에 설명된 옵션 중 하나를 선택합니다.

#### 옵션

#### 설명

**Relationship Only(관계만)**

복제에서 소스 Core를 제거하지만 복제된 복구 지점은 그대로 유지됩니다.

**With Recovery Points(복구 지점 포함)**

복제에서 소스 Core를 제거하고 해당 시스템에서 받은 모든 복제된 복구 지점을 삭제합니다.

### 시스템에서 에이전트 데이터 복제

복제는 에이전트별로 링크 속도가 느린 두 사이트 또는 동일한 사이트에 있는 대상 Core와 소스 Core 간의 관계입니다. 두 Core 간에 복제가 설정되면 소스 Core가 선택 에이전트의 증분 스냅샷 데이터를 대상 또는 소스 Core에 비동기적으로 전송합니다. 오프사이트 백업 및 재난 복구 서비스를 제공하는 관리 서비스 공급자 또는 자체 관리 Core에 아웃바운드 복제를 구성할 수 있습니다. 시스템에 에이전트 데이터를 복제하려면 다음을 수행합니다.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. 복제할 시스템을 선택합니다.
3. **Actions(작업)** 드롭다운 메뉴에서 **Replication(복제)**를 클릭한 후 다음 옵션 중 하나를 완료합니다.
  - 복제를 설정하려면 **Enable(사용)**을 클릭합니다.
  - 이미 복제가 설정되어 있는 경우에는 **Copy(복사)**를 클릭합니다.


**Enable Replications(복제 활성화)** 대화 상자가 나타납니다.
4. **Host(호스트)** 텍스트 상자에 호스트 이름을 입력합니다.
5. **Agents(에이전트)** 아래에서 복제할 에이전트와 데이터가 있는 시스템을 선택합니다.
6. 필요한 경우 **Use a seed drive to perform initial transfer(시드 드라이브를 사용하여 초기 전송 수행)** 확인란을 선택합니다.

7. **Add(추가)**를 클릭합니다.
8. 복제를 일시 중지하거나 다시 시작하려면 **Actions(작업)** 드롭다운 메뉴에서 **Replication(복제)**을 클릭한 후 필요에 따라 **Pause(일시 중지)** 또는 **Resume(다시 시작)**을 클릭합니다.

## 에이전트에 대한 복제 우선순위 설정

에이전트에 대한 복제 우선순위를 설정하려면 다음을 수행하십시오.

1. Core 콘솔에서 복제 우선순위를 설정할 보호 시스템을 선택하고 **Configuration(구성)** 탭을 클릭합니다.
2. **Select Transfer Settings(전송 설정 선택)**을 클릭한 후 **Priority(우선순위)** 드롭다운 목록을 사용하여 다음 옵션 중 하나를 선택합니다.
  - **Default(기본값)**
  - **Highest(가장 높음)**
  - **Lowest(가장 낮음)**
  - **1**
  - **2**
  - **3**
  - **4**

 **노트:** 기본 우선순위는 5입니다. 하나의 에이전트에 우선순위가 1로 지정되어 있고 다른 에이전트에 우선순위가 Highest(가장 높음)으로 지정되어 있는 경우 우선순위가 Highest(가장 높음)로 지정된 에이전트가 우선순위가 1로 지정된 에이전트보다 먼저 복제됩니다.

3. **OK(확인)**를 클릭합니다.

## 시스템에서 작업 취소

시스템에 대해 현재 실행 중인 작업을 취소할 수 있습니다. 현재 스냅샷만 취소하거나 내보내기 및 복제 등을 포함하여 현재 작업을 모두 취소하도록 지정할 수 있습니다.

시스템에서 작업을 취소하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. 작업을 취소할 시스템을 선택합니다.
3. **Actions(작업)** 드롭다운 메뉴에서 **Cancel(취소)**을 클릭한 후 아래에 설명된 옵션 중 하나를 선택합니다.

### 텍스트 상자      설명

모든 작업	해당 시스템에 대해 진행 중인 작업을 모두 취소합니다.
스냅샷	현재 진행 중인 스냅샷을 취소합니다.

## 시스템 상태 및 기타 상세정보 보기

시스템 상태 및 기타 상세정보를 보려면 다음을 수행합니다.

1. Core 콘솔의 탐색 창에서 다음 중 하나를 수행합니다.
  - **Machines(시스템)** 탭을 선택하고 보려는 시스템의 하이퍼링크를 클릭합니다.
  - 탐색 창에서 보려는 시스템을 클릭합니다.

**Summary(요약)** 탭이 표시됩니다.

시스템에 대한 정보가 **Summary(요약)** 페이지에 표시됩니다. 표시되는 상세정보는 다음과 같습니다.

- 호스트 이름
- 마지막으로 생성된 스냅샷
- 예약된 다음 스냅샷
- 암호화 상태
- 버전 번호
- 탑재 기능 검사 상태
- 체크섬 검사 상태
- 마지막으로 수행된 로그 자르기

다음과 같이 시스템에 있는 볼륨에 대한 자세한 정보도 나타납니다.

- 총 크기
- 사용 중인 공간
- 사용 가능한 공간

시스템에 SQL Server가 설치되어 있는 경우, 다음과 같은 서버에 대한 자세한 정보도 나타납니다.

- 이름
- 설치 경로
- Version(버전)
- 버전 번호
- 데이터베이스 이름
- 온라인 상태

시스템에 Exchange Server가 설치되어 있는 경우, 다음과 같은 서버 및 메일 저장소에 대한 자세한 정보도 나타납니다.

- 이름
- 설치 경로
- 데이터 경로
- Exchange 데이터베이스 경로 이름
- 로그 파일 경로
- 로그 접두사
- 시스템 경로
- 메일 저장소 유형

## 다중 시스템 관리

이 항목에서는 Agent 소프트웨어를 여러 Windows 시스템에 동시에 배포하기 위해 관리자가 수행하는 작업에 대해 설명합니다.

여러 에이전트를 배포하고 보호하려면 다음 작업을 수행하십시오.

1. 여러 시스템에 AppAssure 배포.  
[다중 시스템에 배포](#)를 참조하십시오.
2. 일괄 배포의 작동을 모니터링합니다.  
[다중 시스템의 배포 모니터링](#)을 참조하십시오.
3. 다중 시스템을 보호합니다.

[다중 시스템 보호](#)를 참조하십시오.



**노트:** 배포하는 동안 Protect Machine After Install(설치 후 시스템 보호) 옵션을 선택한 경우 이 단계를 건너뛸 수 있습니다.

4. 일괄 보호의 작동을 모니터합니다.

[다중 시스템의 보호 모니터링](#)을 참조하십시오.

## 다중 시스템에 배포

AppAssure의 일괄 배포 기능을 사용하여 여러 Windows 시스템에 AppAssure Agent 소프트웨어를 배포하는 작업을 간소화할 수 있습니다. 다음과 같은 시스템에 일괄 배포를 수행할 수 있습니다.

- VMware vCenter/ESXi 가상 호스트의 시스템
- Active Directory 도메인의 시스템
- 기타 호스트의 시스템

일괄 배포 기능을 사용하면 호스트에서 시스템을 자동으로 감지하고, 배포할 시스템을 선택할 수 있습니다. 또는 호스트 및 시스템 정보를 수동으로 입력할 수 있습니다.



**노트:** AppAssure에서는 웹 버전의 AppAssure Agent 설치 관리자를 사용하여 설치 구성요소를 배포하므로 배포하려는 시스템에서 비트를 다운로드하여 설치하려면 인터넷에 액세스할 수 있어야 합니다. 인터넷에 액세스할 수 없으면 Core 시스템에서 AppAssure Agent 설치 프로그램을 강제 실행할 수 있습니다. Core 시스템에서 Agent 설치 프로그램 강제 실행에 대한 자세한 내용은 [Core 시스템에서 에이전트 설치 프로그램 강제 설치](#)를 참조하십시오. 라이선스 포털에서 코어 및 에이전트 업데이트를 다운로드할 수 있습니다.

### Core 시스템에서 에이전트 설치 프로그램 강제 설치

배포되는 서버가 인터넷에 액세스할 수 없는 경우 Core 시스템에서 실제 에이전트 설치 파일을 강제로 설치할 수 있습니다. 어플라이언스에 에이전트 설치 프로그램 파일이 포함되어 있습니다.



**노트:** 라이선스 포털에서 Core 및 에이전트 업그레이드를 다운로드합니다.

Core 시스템에서 에이전트 설치 프로그램을 강제 설치하려면 다음을 수행합니다.

1. Core 시스템에서, 에이전트 설치 프로그램 **Agent-X64-5.x.x.xxxxx.exe**를 C:\Program Files\apprecovery\core\installers 디렉터리에 복사합니다.
2. Core 콘솔에서 **Configuration(구성)** 탭을 선택하고 **Settings(설정)**를 클릭합니다.
3. **Deploy Agent(에이전트 배포)** 섹션에서 **Agent Installer Name(에이전트 설치 관리자 이름)**을 편집합니다.

### Active Directory 도메인에서 시스템에 배포

이 절차를 시작하려면 먼저 Active Directory 서버에 대한 도메인 정보와 로그인 자격 증명이 있어야 합니다.

Active Directory 도메인에서 여러 시스템에 에이전트를 배포하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭한 후 **Bulk Deploy(일괄 배포)**를 클릭합니다.
2. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 **Active Directory**를 클릭합니다.
3. **Connect to Active Directory(Active Directory에 연결)** 대화 상자에서, 아래 표에 설명된 대로 도메인 정보와 로그인 자격 증명을 입력합니다.

## 텍스트 상자 설명

도메인	Active Directory 도메인의 호스트 이름 또는 IP 주소입니다.
사용자 이름	도메인에 연결하는 데 사용되는 사용자 이름입니다(예: Administrator).
암호	도메인에 연결하는 데 사용되는 보안 암호입니다.

4. **Connect(연결)**를 클릭합니다.
5. **Add Machines from Active Directory(Active Directory에서 시스템 추가)** 대화 상자에서, AppAssure Agent를 배포할 시스템을 선택하고 **Add(추가)**를 클릭합니다.  
추가한 시스템이 **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에 나타납니다.
6. 시스템의 암호 입력, 리포지토리 선택, 암호화 키 추가 또는 시스템의 기타 설정 편집을 수행하려면 시스템의 **Edit(편집)** 링크를 클릭하고 다음을 수행합니다.
  - a. **Edit Settings(설정 편집)** 대화 상자에서 아래 표의 설명 대로 설정을 지정합니다.

## 텍스트 상자 설명

호스트 이름	3단계의 암호가 자동으로 제공됩니다.
표시 이름	3단계에서 제공한 호스트 이름을 기반으로 자동으로 할당됩니다.
포트	Core가 시스템의 에이전트와 통신하는 포트 번호입니다.
사용자 이름	3단계의 암호가 자동으로 제공됩니다.
암호	시스템의 암호를 입력합니다.
설치 후 자동 재부팅	배포 후 시스템을 자동으로 재부팅할 것인지 지정합니다.



**노트:** 이 옵션은 **Protect Machine After Install(설치 후 시스템 보호)** 상자를 클릭하여 배포 후 시스템을 자동으로 보호하려는 경우 필수입니다.

**설치 후 시스템 보호** 배포 후 시스템을 자동으로 보호할 것인지 지정합니다. 이 옵션을 선택하면 **Protecting Multiple Machines(다중 시스템 보호)**을 건너뛸 수 있습니다.

**리포지토리** 드롭다운 목록을 사용하여 Core에서 시스템의 데이터가 저장되는 리포지토리를 선택합니다. 선택하는 리포지토리는 보호되는 모든 시스템에 사용됩니다.



**노트:** 이 옵션은 **Protect machine after install(설치 후 시스템 보호)**을 선택한 경우에만 사용할 수 있습니다.

**암호화 키** (선택사항) 드롭다운 목록을 사용하여 리포지토리에 저장되는 시스템의 데이터에 암호화를 적용할지 여부를 지정합니다. 암호화 키는 보호되는 모든 시스템에 할당됩니다.



**노트:** 이 옵션은 **Protect machine after install(설치 후 시스템 보호)**을 선택한 경우에만 사용할 수 있습니다.

- b. **Save(저장)**를 클릭합니다.

7. AppAssure가 각 시스템에 성공적으로 연결할 수 있는지 확인하려면 **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템을 선택하고 **Verify(확인)**를 클릭합니다.
8. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템 옆에 다음과 같이 배포 준비 상태를 나타내는 아이콘이 표시됩니다.



텍스트 상자	설명
--------	----

녹색 아이콘	AppAssure를 시스템에 연결할 수 있으며 배포할 수 있습니다.
--------	---------------------------------------

노란색 아이콘	AppAssure를 시스템에 연결할 수 있지만 에이전트가 Core 시스템과 이미 쌍으로 지정되어 있습니다.
---------	---


빨간색 아이콘	AppAssure를 시스템에 연결할 수 없습니다. 이는 로그인 자격 증명이 올바르지 않거나, 시스템이 종료되거나, 방화벽이 트래픽을 차단하거나, 다른 문제 때문일 수 있습니다. 이 문제를 해결하려면 도구 모음에서 <b>Edit Settings(설정 편집)</b> 를 클릭하거나 시스템 옆에 있는 <b>Edit(편집)</b> 링크를 클릭하십시오.
---------	--

9. 시스템을 성공적으로 확인한 후, AppAssure Agent를 배포할 각 시스템을 선택하고 **Deploy(배포)**를 클릭합니다.

10. **Protect machine after install(설치 후 시스템 보호)** 옵션을 선택한 경우 배포가 완료되면 시스템이 자동으로 재부팅된 후 보호가 활성화됩니다.

### VMware vCenter 또는 ESXi 가상 호스트에서 시스템에 배포

이 절차를 시작하려면 먼저 VMware vCenter/ESXi 가상 호스트에 대한 호스트 위치 정보와 로그인 자격 증명에 있어야 합니다.

 **노트:** 모든 가상 시스템에 VM 도구가 설치되어 있어야 합니다. 그렇지 않으면 AppAssure가 배포할 가상 시스템의 호스트 이름을 감지할 수 없습니다. AppAssure에서 호스트 이름 대신 가상 시스템 이름을 사용하며, 이러한 경우 호스트 이름이 가상 시스템 이름과 다르면 문제가 발생할 수 있습니다.

vCenter/ESXi 가상 호스트에서 여러 시스템을 배포하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭한 후 **Bulk Deploy(일괄 배포)**를 클릭합니다.
2. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 **vCenter/ESXi**를 클릭합니다.
3. **Connect to VMware vCenter Server/ESXi(VMware vCenter 서버/ESXi에 연결)** 대화 상자에 다음과 같이 호스트 정보와 로그인 자격 증명을 입력하고 **OK(확인)**를 클릭합니다.

텍스트 상자	설명
--------	----

호스트	VMware vCenter Server/ESXi(i) 가상 호스트의 이름이나 IP 주소를 입력합니다.
-----	--

사용자 이름	가상 호스트에 연결하는 데 사용할 사용자 이름을 입력합니다(예: administrator).
--------	---

암호	이 가상 호스트에 연결하는 데 사용할 안전한 암호를 입력합니다.
----	-------------------------------------

4. **Add Machines from VMware vCenter Server/ESXi(VMware vCenter 서버/ESXi에서 시스템 추가)** 대화 상자에서 AppAssure Agent를 배포할 시스템 옆에 있는 상자를 선택하고 **Add(추가)**를 클릭합니다.
5. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 추가한 시스템을 확인할 수 있습니다. 리포지토리, 암호화 키 또는 시스템에 대한 기타 설정을 선택하려면 시스템 옆에 있는 확인란을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.

각 설정에 대한 자세한 내용은 [Active Directory 도메인에서 시스템에 배포](#)를 참조하십시오.

6. AppAssure가 각 시스템에 성공적으로 연결할 수 있는지 확인합니다. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템을 선택하고 **Verify(확인)**를 클릭합니다.
7. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템 옆에 다음과 같이 배포 준비 상태를 나타내는 아이콘이 표시됩니다.

텍스트 상자	설명
--------	----

녹색 아이콘	AppAssure를 시스템에 연결할 수 있으며 배포할 수 있습니다.
--------	---------------------------------------

텍스트 상자	설명
노란색 아이콘	AppAssure를 시스템에 연결할 수 있지만 에이전트가 Core 시스템과 이미 쌍으로 지정되어 있습니다.
빨간색 아이콘	AppAssure를 시스템에 연결할 수 없습니다. 이는 로그인 자격 증명이 올바르지 않거나, 시스템이 종료되거나, 방화벽이 트래픽을 차단하거나, 다른 문제 때문일 수 있습니다. 이 문제를 해결하려면 도구 모음에서 <b>Edit Settings(설정 편집)</b> 를 클릭하거나 시스템 옆에 있는 <b>Edit(편집)</b> 링크를 클릭하십시오.

8. 시스템이 확인되면 각 시스템을 선택하고 **Deploy(배포)**를 클릭합니다.
9. **Protect machine after install(설치 후 시스템 보호)** 옵션을 선택한 경우 배포가 완료되면 시스템이 자동으로 재부팅된 후 보호가 활성화됩니다.

### 다른 호스트에서 여러 시스템에 배포

다른 호스트에서 여러 시스템에 배포하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭한 후 **Bulk Deploy(일괄 배포)**를 클릭합니다.
2. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 다음 중 하나를 수행합니다.
  - **New(새로 만들기)**를 클릭하면 나타나는 **Add Machine(시스템 추가)** 대화 상자를 사용하여 여러 개의 시스템을 지정합니다. 여기에서 새 시스템 호스트, 로그인 자격 증명, 리포지토리, 암호화 키 및 기타 정보를 입력할 수 있습니다. 각 설정에 대한 자세한 내용은 [Active Directory 도메인에서 시스템에 배포](#)를 참조하십시오.  
이 정보를 입력한 후 **OK(확인)**를 클릭하여 해당 시스템을 **Deploy Agent on Machines(시스템에 에이전트 배포)** 목록에 추가하거나 **OK & New(확인 후 새로 만들기)**를 클릭하여 다른 시스템을 추가합니다.



**노트:** 배포 후 시스템을 자동으로 보호하려면 **Protect Machine after Install(설치 후 시스템 보호)** 확인란을 선택합니다. 확인란을 선택하면 보호를 활성화하기 전에 시스템이 자동으로 재부팅됩니다.

- 목록에 여러 시스템을 지정하려면 **Manually(수동)**를 클릭합니다. 이를 수행하면 각 행에 배포할 시스템이 표시됩니다. **Add Machines Manually(수동으로 시스템 추가)** 대화 상자에서 다음과 같이 시스템에 대한 IP 주소 또는 이름, 사용자 이름, 이중 콜론 구분 기호로 구분된 암호 및 포트를 입력합니다.  

```
hostname::username::password::port For example:
10.255.255.255::administrator::&1l@yYz90z::8006 abc-
host-00-1::administrator::99!zU$083r::168
```
3. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 추가한 시스템을 확인할 수 있습니다. 리포지토리, 암호화 키 또는 시스템에 대한 기타 설정을 선택하려면 시스템 옆에 있는 확인란을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.  
각 설정에 대한 자세한 내용은 [Active Directory 도메인에서 시스템에 배포](#)를 참조하십시오.
  4. AppAssure가 각 시스템에 성공적으로 연결할 수 있는지 확인합니다. **Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템을 선택하고 **Verify(확인)**를 클릭합니다.  
**Deploy Agent on Machines(시스템에 에이전트 배포)** 창에서 각 시스템 옆에 다음과 같이 배포 준비 상태를 나타내는 아이콘이 표시됩니다.

텍스트 상자	설명
녹색 아이콘	AppAssure를 시스템에 연결할 수 있으며 배포할 수 있습니다.
노란색 아이콘	AppAssure를 시스템에 연결할 수 있지만 에이전트가 Core 시스템과 이미 쌍으로 지정되어 있습니다.

## 텍스트 상자 설명

**빨간색 아이콘** AppAssure를 시스템에 연결할 수 없습니다. 이는 로그인 자격 증명이 올바르지 않거나, 시스템이 종료되거나, 방화벽이 트래픽을 차단하거나, 다른 문제 때문일 수 있습니다. 이 문제를 해결하려면 도구 모음에서 **Edit Settings(설정 편집)**을 클릭하거나 시스템 옆에 있는 **Edit(편집)** 링크를 클릭하십시오.

5. 시스템이 성공적으로 확인되면 각 시스템 옆에 있는 상자를 선택하고 **Deploy(배포)**를 클릭합니다.
6. **Protect machine after install(설치 후 시스템 보호)** 옵션을 선택한 경우 배포가 완료되면 시스템이 자동으로 재부팅된 후 보호가 활성화됩니다.

## 다중 시스템의 배포 모니터링


시스템에 AppAssure Agent 소프트웨어 배포에 대한 진행 상태를 볼 수 있습니다.

다중 시스템의 배포를 모니터링하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Events(이벤트)** 탭을 클릭한 후 목록에서 배포 작업을 찾고 **Details(상세정보)** 옆에 있는 단추를 클릭합니다.  
**Monitor Active Task(진행 중인 작업 모니터링)** 창에 배포 상세정보가 표시됩니다.  
이 창에 각 개별 배포에 대한 상태와 전체 진행률 정보가 포함됩니다. 표시되는 상세정보는 다음과 같습니다.
  - 시작 시간
  - 종료 시간
  - 경과 시간
  - 남은 시간
  - Progress(진행률)
  - 단계
2. 다음 중 하나를 수행합니다.
  - 배포에 대한 진행률을 보려면 **Open in New window(새 창으로 열기)**를 클릭하여 새 창을 시작합니다.
  - **Close(닫기)**를 클릭하면 배포 작업이 배경에서 계속 진행됩니다.

## 다중 시스템 보호

Windows 시스템에 Agent 소프트웨어를 일괄 배포한 후 데이터를 보호하기 위해 해당 시스템을 보호해야 합니다. 에이전트를 배포할 때 **Protect Machine After Install(설치 후 시스템 보호)**를 선택한 경우에는 이 절차를 건너뛸 수 있습니다.

 **노트:** 원격 설치를 수행할 수 있도록 지정하는 보안 정책에 따라 에이전트 시스템을 구성해야 합니다.

다중 시스템을 보호하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 클릭한 후 **Bulk Protect(일괄 보호)**를 클릭합니다.  
**Protect Machines(시스템 보호)** 창이 나타납니다.
2. 다음 옵션 중 하나를 클릭하여 보호하기 원하는 시스템을 추가합니다.  
각 옵션 완료 방법에 대한 자세한 내용은 [다중 시스템에 배포](#)를 참조하십시오.
  - Active Directory 도메인에 시스템을 지정하려면 **Active Directory**를 클릭합니다.
  - vCenter/ESXi 가상 호스트에 가상 시스템을 지정하려면 **vCenter/ESXi**를 클릭합니다.

- Add Machine(시스템 추가) 대화 상자를 사용하여 다중 시스템을 지정하려면 **New(새로 만들기)**를 클릭합니다.
  - 호스트 이름 및 자격 증명을 입력하여 목록에서 다중 시스템을 지정하려면 **Manually(수동)**를 클릭합니다.
3. **Protect Machines(시스템 보호)** 창에서 추가한 시스템을 볼 수 있습니다. 시스템에 대한 리포지토리, 암호화 키 또는 기타 고급 설정을 선택하려면 시스템 옆에 있는 확인란을 선택하고 **Edit Settings(설정 편집)**를 클릭합니다.
4. 다음과 같이 설정을 지정하고 **OK(확인)**를 클릭합니다.

텍스트 상자	설명
사용자 이름	이 시스템에 연결하는 데 사용되는 사용자 이름을 입력합니다(예: Administrator).
암호	이 시스템에 연결하는 데 사용되는 안전한 암호를 입력합니다.
포트	Core가 시스템의 에이전트와 통신하는 포트 번호를 지정합니다.
리포지토리	Core에서 시스템의 데이터가 저장되는 리포지토리를 선택합니다. 선택하는 리포지토리가 보호 중인 모든 시스템에 사용됩니다.
암호화 키	리포지토리에 저장되는 시스템의 에이전트에 암호화를 적용할 것인지 지정합니다. 보호 중인 모든 시스템에 암호화 키가 할당됩니다.
보호 일정	시스템이 보호되는 일정을 지정합니다. 주말 및 작업량이 가장 많은 경우 기본 일정은 60분입니다. 기업의 필요에 맞게 일정을 편집하려면 <b>Edit(편집)</b> 를 클릭합니다.



**노트:** 자세한 내용은 [보호 일정 수정](#)을 참조하십시오.

- 처음에 보호 일시 중지** 경우에 따라 처음 실행할 때 보호를 일시 중지하도록 선택할 수 있습니다. 즉, 수동으로 보호를 다시 시작할 때까지 Core에서 시스템의 스냅샷을 생성하지 않습니다.
5. 각 시스템에 AppAssure를 성공적으로 연결할 수 있는지 확인해야 합니다. 이를 수행하려면 **Protect Machines(시스템 보호)** 창에서 각 시스템 옆에 있는 확인란을 선택하고 **Verify(확인)**를 클릭합니다.
6. **Protect Machines(시스템 보호)** 창에서 각 시스템 옆에 다음과 같이 배포 준비 상태를 나타내는 아이콘이 표시됩니다.

Icon	설명
녹색 아이콘	AppAssure를 시스템에 연결할 수 있으며 보호할 수 있습니다.
노란색 아이콘	AppAssure를 시스템에 연결할 수 있지만 에이전트가 Core 시스템과 이미 쌍으로 지정되어 있습니다.
빨간색 아이콘	AppAssure를 시스템에 연결할 수 없습니다. 이는 로그인 자격 증명이 올바르지 않거나, 시스템이 종료되거나, 방화벽이 트래픽을 차단하거나, 다른 문제 때문일 수 있습니다. 이 문제를 해결하려면 도구 모음에서 <b>Edit Settings(설정 편집)</b> 를 클릭하거나 시스템 옆에 있는 <b>Edit(편집)</b> 링크를 클릭하십시오.

7. 시스템이 성공적으로 확인되면 각 시스템 옆에 있는 확인란을 선택하고 **Protect(보호)**를 클릭합니다.

## 다중 시스템의 보호 모니터링

AppAssure가 시스템에 보호 정책과 일정을 적용할 때 진행률을 모니터링할 수 있습니다.

다중 시스템의 보호를 모니터하려면 다음을 수행하십시오.

1. **Machines(시스템)** 탭을 클릭하여 보호 상태와 진행률을 봅니다.  
**Protected Machines(보호되는 시스템)** 페이지가 표시됩니다.
2. **Events(이벤트)** 탭을 클릭하여 관련 작업, 이벤트 및 경고를 봅니다.  
**Tasks(작업)** 페이지가 나타납니다.

텍스트 상자	설명
--------	----

작업 정보 보기	볼륨이 전송되면 <b>Tasks(작업)</b> 창에 상태, 시작 시간 및 종료 시간이 표시됩니다. 작업에 대한 추가 세부 정보를 보려면 <b>Details(상세정보)</b> 를 클릭하십시오.
----------	--

경고 정보 보기	보호된 시스템이 각각 추가되면 작업이 성공했는지 또는 오류가 로그되었는지 자세히 설명하는 경고가 로그됩니다. 트랜잭션 날짜 및 메시지와 함께 경고 수준이 표시됩니다. 페이지에서 경고를 모두 제거하려면 <b>Dismiss All(모두 해제)</b> 을 클릭합니다.
----------	--

이벤트 정보 보기	전송된 데이터 및 시스템에 대한 상세정보가 <b>Events(이벤트)</b> 창에 나타납니다. 이벤트 수준, 트랜잭션 날짜 및 시간 메시지가 표시됩니다.
-----------	---

## 스냅샷 및 복구 지점 관리

복구 지점은 개별 디스크 볼륨에서 생성되어 리포지토리에 저장되는 스냅샷의 컬렉션이며 리포지토리에 저장됩니다. 스냅샷은 데이터를 생성하는 응용프로그램이 사용되고 있는 동안 지정된 시점(point in time)에서 디스크 볼륨의 상태를 캡처하여 저장합니다. AppAssure에서는 스냅샷을 강제 실행하고, 일시적으로 중단하며, 리포지토리의 현재 복구 지점의 목록을 볼 수 있으며 필요에 따라 삭제할 수도 있습니다. 복구 지점은 보호되는 시스템을 복원하거나 로컬 파일 시스템에 탑재하는 데 사용됩니다.

AppAssure에서 캡처하는 스냅샷은 블록 수준에서 캡처되며 응용프로그램 인식형입니다. 즉, 열려 있는 모든 트랜잭션과 롤링 트랜잭션 로그가 완료되고 스냅샷을 생성하기 전에 캐시가 디스크에 플러시됩니다.

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

## 복구 지점 보기

복구 지점을 보려면 다음을 수행합니다.

1. Core 콘솔의 왼쪽 탐색 영역에서, 복구 지점을 볼 시스템을 선택한 후 **Recovery Points(복구 지점)** 탭을 클릭합니다.

다음 표에 설명된 대로 시스템의 복구 지점에 대한 정보를 볼 수 있습니다.

정보	설명
Status(상태)	복구 지점의 현재 상태를 나타냅니다.
암호화된 상태	복구 지점이 암호화되어 있는지 여부를 나타냅니다.
콘텐츠	복구 지점에 포함된 볼륨을 나열합니다.
Type(유형)	복구 지점을 기준 또는 차등으로 정의합니다.

생성 날짜	복구 지점이 생성된 날짜를 표시합니다.
Size(크기)	리포지토리에서 복구 지점이 사용하는 공간의 크기를 표시합니다.

## 특정 복구 지점 보기

특정 복구 지점을 보려면 다음을 수행합니다.

1. Core 콘솔의 왼쪽 탐색 영역에서, 복구 지점을 볼 시스템을 선택한 후 **Recovery Points(복구 지점)** 탭을 선택합니다.
2. 목록에서 복구 지점 옆에 있는 >를 클릭하여 보기를 확장합니다.  
선택한 시스템의 복구 지점 내용에 대한 자세한 정보를 볼 수 있으며 복구 지점에서 수행할 수 있는 다양한 작업에 액세스할 수 있습니다. 아래 표를 살펴보세요.

정보	설명
Actions(조치)	<p><b>Actions(조치)</b> 메뉴에는 선택한 복구 지점에서 수행할 수 있는 다음과 같은 작업이 포함되어 있습니다.</p> <p><b>Mount(탑재)</b> — 선택한 복구 지점을 탑재하려면 이 옵션을 선택합니다. 선택한 복구 지점 탑재에 대한 자세한 내용은 <a href="#">Windows 시스템의 복구 지점 탑재</a>를 참조하십시오.</p> <p><b>Export(내보내기)</b> - Export (내보내기) 옵션에서, 선택한 복구 지점을 ESXi, VMware 워크스테이션 또는 HyperV로 내보낼 수 있습니다. 선택한 복구 지점 내보내기에 대한 자세한 내용은 <a href="#">Windows 시스템에서 가상 시스템으로 백업 정보 내보내기</a>를 참조하십시오.</p> <p><b>Rollback(롤백)</b> — 선택한 복구 지점에서 지정하는 볼륨으로 복원을 수행하려면 이 옵션을 선택합니다. 선택한 복구 지점에서 복원 수행에 대한 자세한 내용은 <a href="#">Appassure Core에서 복원 시작</a>을 참조하십시오.</p>

3. 선택한 복구 지점에서 볼륨 옆에 있는 >를 클릭하여 보기를 확장합니다.

다음 표에 설명된 대로 확장된 복구 지점에서 선택된 볼륨에 대한 정보를 볼 수 있습니다.

텍스트 상자	설명
Title(직책)	복구 지점에 있는 특정 볼륨을 나타냅니다.
원시 용량	전체 볼륨에서 원시 저장소 공간의 양을 나타냅니다.
포맷된 용량	볼륨이 포맷된 후에 데이터에 사용할 수 있는 볼륨의 저장소 공간 양을 나타냅니다.
사용된 용량	전체 볼륨에서 현재 사용된 저장소 공간의 양을 나타냅니다.

## Windows 시스템의 복구 지점 탑재

AppAssure에서 Windows 시스템의 복구 지점을 탑재하여 로컬 파일 시스템을 통해 저장된 데이터에 액세스할 수 있습니다.

Windows 시스템의 복구 지점을 탑재하려면 다음을 수행하십시오.

1. Core 콘솔에서 다음 중 하나를 수행합니다.

- **Machines(시스템)** 탭을 선택합니다.

- a. 탑재할 복구 지점이 있는 시스템이나 클라이언트 옆에 있는 **Actions(조치)** 드롭다운 메뉴에서 **Mount(탑재)**를 선택합니다.
- b. **Mount Recovery Point(복구 지점 탑재)** 대화 상자의 목록에서 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.

**Mount Recovery Points(복구 지점 탑재)** 대화 상자가 표시됩니다.

- Core 콘솔에서, 로컬 파일 시스템에 탑재할 시스템을 선택합니다.

선택한 시스템의 **Summary(요약)** 탭이 표시됩니다.

- a. **Recovery Points(복구 지점)** 탭을 선택합니다.
- b. 복구 지점 목록에서, 탑재할 복구 지점을 확장합니다.
- c. 확장된 복구 지점의 상세정보에서 **Mount(탑재)**를 클릭합니다.

**Mount Recovery Points(복구 지점 탑재)** 대화 상자가 표시됩니다.

2. **Mount(탑재)** 대화 상자에서 아래 표에 설명된 대로 복구 지점을 탑재하기 위해 텍스트 상자를 편집합니다.

텍스트 상자	설명
탑재 위치: 로컬 파일	탑재된 복구 지점에 액세스하는 데 사용되는 경로를 지정합니다.
볼륨 이미지	탑재할 볼륨 이미지를 지정합니다.
탑재 유형	다음과 같이 탑재된 복구 지점에 대한 데이터에 액세스하는 방법을 지정합니다. <ul style="list-style-type: none"> <li>• 읽기 전용 탑재</li> <li>• 이전 쓰기를 포함하여 읽기 전용 탑재</li> <li>• 쓰기 가능 탑재</li> </ul>
이 탑재의 Windows 공유 생성	경우에 따라 확인란을 선택하여 탑재된 복구 지점의 공유 가능 여부를 지정한 후 공유 이름과 액세스 그룹을 포함하여 해당 복구 지점에 대한 액세스 권한을 설정합니다.

3. **Mount(탑재)**를 클릭하여 복구 지점을 탑재합니다.

## 선택 복구 지점 분리

Core에 로컬로 탑재된 선택 복구 지점을 분리할 수 있습니다.

선택 복구 지점을 분리하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 선택합니다.
2. **Tools(도구)** 옵션에서 **System Info(시스템 정보)**를 클릭합니다.
3. 분리할 복구 지점의 탑재된 디스플레이를 찾아 선택한 후 **Dismount(분리)**를 클릭합니다.

## 모든 복구 지점 분리

Core에 로컬로 탑재된 모든 복구 지점을 분리할 수 있습니다.

모든 복구 지점을 분리하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구)** 탭을 선택합니다.
2. **Tools(도구)** 옵션에서 **System Info(시스템 정보)**를 클릭합니다.
3. **Local Mounts(로컬 탑재)** 섹션에서 **Dismount All(모두 분리)**을 클릭합니다.

## Linux 시스템의 복구 지점 볼륨 탑재

1. 복구 지점을 탑재할 새 디렉터리를 생성합니다(예: `mkdir` 명령 사용).
2. 디렉터리가 있는지 확인합니다(예: `ls` 명령 사용).
3. AppAssure **aamount** 유틸리티를 루트 또는 고급 사용자로 실행합니다. 예를 들어, 다음과 같습니다.

```
sudo aamount
```

4. AppAssure 탑재 지점에 다음 명령을 입력하여 보호된 시스템을 나열합니다.

```
lm
```

5. 메시지가 표시되면 AppAssure Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.

6. Core 서버에 대한 사용자 이름 및 암호와 같은 로그인 자격 증명을 입력합니다.

이 AppAssure 서버에 의해 보호되는 시스템을 보여주는 목록이 표시됩니다. 이 목록에 발견된 시스템이 개별 항목 번호, 호스트/IP 주소 및 시스템의 ID 번호별로 나열됩니다(예: 293cc667-44b4-48ab-91d8-44bc74252a4f).

7. 다음 명령을 입력하여 지정한 시스템에 대해 현재 탑재된 복구 지점을 나열합니다.

```
lr <line_number_of_machine>
```



**노트:** 또한 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템에 대한 기본 및 증분 복구 지점을 보여주는 목록이 표시됩니다. 이 목록에는 개별 항목 번호, 날짜/타임스탬프, 볼륨 위치, 복구 지점 크기 및 끝 부분에 복구 지점을 식별하는 시퀀스 번호가 포함되어 있는 볼륨에 대한 ID 번호가 포함됩니다(예: 293cc667-44b4-48ab-91d8-44bc74252a4f:2).

8. 다음 명령을 입력하여 지정된 복구 지점을 선택하고 지정된 탑재 지점/경로에 탑재합니다.

```
m <volume_recovery_point_ID_number> <path>
```



**노트:** 또한 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 식별할 수 있습니다. 이러한 경우 `lm` 출력의 에이전트/시스템 라인 번호 뒤에 복구 지점 라인 번호와 볼륨 문자를 사용한 후 경로를 사용합니다(예: `m <machine_line_number> <recovery_point_line_number> <volume_letter> <path>`). 예를 들어, `lm` 출력에서 세 개의 에이전트 시스템을 나열하고, 번호 2에 대해 `lr` 명령을 입력하고, 23 복구 지점 볼륨 `b`를 `/tmp/mount_dir`에 탑재하는 경우 명령은 `m 2 23 b /tmp/mount_dir`입니다.



**주의:** 보호된 Linux 볼륨의 탑재를 수동으로 해제하지 않아야 합니다. 탑재를 해제해야 하는 경우 볼륨을 탑재 해제하기 전에 `bsctl -d <path to volume>` 명령을 실행해야 합니다. 이 명령에서 `<path to volume>`은 볼륨의 탑재 지점이 아닌 볼륨의 파일 설명자를 나타내며, `/dev/sda1`과 유사한 형식이어야 합니다.

## 복구 지점 제거


리포지토리에서 특정 시스템에 대한 복구 지점을 쉽게 제거할 수 있습니다. AppAssure에서 복구 지점을 삭제할 때 다음 옵션 중 하나를 지정할 수 있습니다.



## 텍스트 상자 설명

**모든 복구 지점 삭제** 리포지토리에서 선택한 에이전트 시스템에 대한 복구 지점을 모두 제거합니다.

**복구 지점의 범위 삭제** 현재 기본 이미지 이전, 기본 이미지까지 및 기본 이미지 포함과 같이 지정한 범위 내의 모든 복구 지점을 제거합니다. 이렇게 하면 현재 기본 이미지부터 다음 기본 이미지까지의 모든 복구 지점과 시스템의 모든 데이터가 제거됩니다.


 **노트:** 삭제한 복구 지점은 복구할 수 없습니다.

복구 지점을 제거하려면 다음을 수행하십시오.

1. Core 콘솔의 왼쪽 탐색 영역에서, 복구 지점을 볼 시스템을 선택한 후 **Recovery Points(복구 지점)** 탭을 클릭합니다.
2. **Actions(작업)** 메뉴를 클릭합니다.
3. 다음 옵션 중 하나를 선택합니다.
  - 현재 저장된 복구 지점을 모두 삭제하려면 **Delete All(모두 삭제)**을 클릭합니다.
  - 특정 데이터 범위에 속하는 복구 지점의 집합을 삭제하려면 **Delete Range(범위 삭제)**를 클릭합니다. **Delete(삭제)** 대화 상자가 나타납니다. **Delete Range(범위 삭제)** 대화 상자에서 시작 날짜 및 시간과 종료 날짜 및 시간을 사용하여 삭제할 복구 지점의 범위를 지정한 후 **Delete(삭제)**를 클릭합니다.


## 분리된 복구 지점망 삭제

분리된 복구 지점은 기본 이미지와 연관되어 있지 않은 증분 스냅샷입니다. 이후의 스냅샷은 이 복구 지점에 계속해서 생성됩니다. 기본 이미지가 없으면 결과로 나타나는 복구 지점이 불완전하여 복구 완료에 필요한 데이터가 포함되지 않을 수 있습니다. 이러한 복구 지점은 분리된 복구 지점망에 속하는 것으로 간주됩니다. 이러한 상황이 발생하면, 복구 지점망을 삭제하고 기본 이미지를 새로 만드는 것이 가장 좋은 해결책입니다.

 **노트:** 대상 Core에서 복제된 복구 지점에는 분리된 복구 지점망 삭제 기능을 사용할 수 없습니다.

분리된 복구 지점망을 삭제하려면 다음을 수행합니다.

1. Core 콘솔에서, 분리된 복구 지점망을 삭제할 보호되는 시스템을 선택합니다.
2. **Recovery Points(복구 지점)** 탭을 클릭합니다.
3. **Recovery Points(복구 지점)**에서 분리된 복구 지점을 확장합니다.  
이 복구 지점은 **Type(유형)** 열에서 **Incremental Orphaned(증분 분리)**로 표시되어 있습니다.
4. **Actions(작업)** 옆에 있는 **Delete(삭제)**를 클릭합니다.  
**Delete Recovery Points(복구 지점 삭제)** 창이 나타납니다.
5. **Delete Recovery Points(복구 지점 삭제)** 창에서 **Yes(예)**를 클릭합니다.

 **주의:** 복구 지점을 삭제하면 다음 기본 이미지가 생성될 때까지 이 작업의 전후로 발생했던 모든 증분 복구 지점을 비롯하여 복구 지점망 전체가 삭제됩니다. 이 작업은 실행 취소할 수 없습니다.

분리된 복구 지점망이 삭제됩니다.

## 스냅샷 강제 적용

스냅샷을 강제 적용하면 현재 보호된 시스템에 대한 데이터를 강제로 전송할 수 있습니다. 스냅샷을 강제 적용하면 즉시 전송이 시작되고 큐에 추가됩니다. 이전 복구 지점에서 변경한 데이터만 전송됩니다. 이전 복구 지점이 없는 경우에는 기본 이미지라고 하는 보호된 볼륨에 대한 모든 데이터가 전송됩니다.

스냅샷을 강제 적용하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭하고, 보호되는 시스템 목록에서 스냅샷을 강제 적용할 복구 지점이 있는 시스템이나 클러스터를 선택합니다.
2. 해당 시스템에 대한 **Actions(작업)** 드롭다운 메뉴를 클릭하고 **Force Snapshot(스냅샷 강제 적용)**을 클릭한 후 아래에 설명된 옵션 중 하나를 선택합니다.
  - **Force Snapshot(스냅샷 강제 적용)** - 마지막으로 스냅샷을 만든 이후에 업데이트된 데이터의 증분 스냅샷을 만듭니다.
  - **Force Base Image(기본 이미지 강제 적용)** - 시스템의 볼륨에 있는 모든 데이터의 완전한 스냅샷을 만듭니다.
3. **Transfer Status(전송 상태)** 대화 상자에 스냅샷이 큐에 지정되었음을 나타내는 알림이 표시되면 **OK(확인)**를 클릭합니다.  
**Machines(시스템)** 탭에서 시스템 옆에 진행률 표시줄이 나타나고 스냅샷의 진행률이 표시됩니다.

## 보호 일시 중지 및 다시 시작

보호를 일시 중지하면 현재 시스템에서의 모든 데이터 전송이 일시적으로 중지됩니다.


보호를 일시 중지하고 다시 시작하려면 다음을 수행합니다.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. 보호를 일시 중지할 시스템을 선택합니다.  
이 시스템의 **Summary(요약)** 탭이 나타납니다.
3. 해당 시스템에 대한 **Actions(작업)** 드롭다운에서 **Pause(일시 중지)**를 클릭합니다.
4. 보호를 다시 시작하려면 **Actions(작업)** 메뉴에서 **Resume(다시 시작)**을 클릭합니다.

## 데이터 복원

데이터를 Windows 시스템의 저장된 복구 지점에서 가상 시스템 또는 실제 시스템(Windows 또는 Linux 시스템의 경우)으로 즉시 복구하거나 복원할 수 있습니다. 이 섹션에 있는 항목은 Windows 시스템의 특정 복구 지점을 가상 시스템으로 내보내거나 시스템을 이전 복구 지점으로 롤백하는 방법에 대해 설명합니다.

두 Core(소스 Core와 대상 Core) 간에 복제가 설정된 경우 초기 복제가 완료된 후 대상 Core에서만 데이터를 내보낼 수 있습니다. 자세한 내용은 [시스템에서 에이전트 데이터 복제](#)를 참조하십시오.

 **노트:** FAT32 EFI 파티션에서 부팅되는 Windows 8 및 Windows Server 2012 운영 체제는 보호 또는 복구 대상이 아니며 ReFS(Resilient File System) 볼륨이 아닙니다.


## 백업

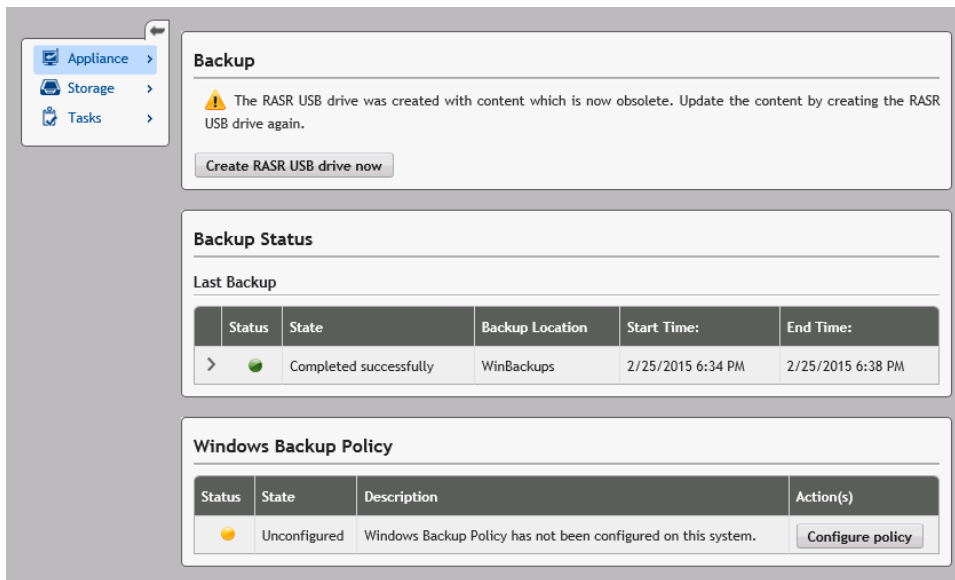
백업 탭에서 백업 정책을 구성하고 RASR USB 키 또는 IDSDM을 통해 시스템을 복구할 수 있습니다. 이 기능을 사용하려면 Windows 백업 가상 디스크가 있어야 합니다. Windows 백업 가상 디스크는 **AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)**를 수행하는 동안 생성됩니다. 자세한 내용은 *Dell DL43000 어플라이언스 배포 설명서*의 신속한 어플라이언스 자동 복구를 참조하십시오. Windows 백업 가상 디스크가 없으면 정책을 구성하거나 Windows 백업을 생성할 수 없습니다.

## 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.
  - Status(상태)
  - 상태
  - 백업 위치
  - 시작 시간
  - 종료 시간
  - 오류 설명
  - 백업된 항목

 **노트:** 위의 정보에 Windows 백업 정책 실행 여부가 표시됩니다.



**Backup**

⚠ The RASR USB drive was created with content which is now obsolete. Update the content by creating the RASR USB drive again.

Create RASR USB drive now

**Backup Status**

Last Backup

Status	State	Backup Location	Start Time:	End Time:
>	Completed successfully	WinBackups	2/25/2015 6:34 PM	2/25/2015 6:38 PM

**Windows Backup Policy**

Status	State	Description	Action(s)
🟡	Unconfigured	Windows Backup Policy has not been configured on this system.	Configure policy

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(C:)
- 복구
- 운영 체제 미설치 복구
- 시스템 상태

위의 항목은 모두 기본적으로 선택되어 있습니다.

백업을 예약할 시간을 선택합니다.

#### 4. Configure(구성)를 클릭합니다.

구성되면 **Windows Backup Policy(Windows 백업)** 창에서 **Backup now(지금 백업)**, **Delete policy(정책 삭제)** 또는 **View policy(정책 보기)** 옵션을 사용할 수 있습니다.

## Windows 시스템에서 가상 시스템으로 보호 데이터 내보내기 정보

AppAssure에서는 Windows 백업 정보를 가상 시스템으로 1회 내보내기 또는 지속적으로 내보내기(가상 대기 지원용) 둘 다 지원됩니다. 데이터를 가상 대기 시스템에 내보내면 가용성이 높은 데이터 사본을 사용할 수 있습니다. 보호되는 시스템이 작동 중지될 경우 가상 시스템을 부팅하여 복구를 수행할 수 있습니다.

다음 다이어그램은 가상 시스템에 데이터 내보내기를 위한 일반적인 배포를 보여줍니다.

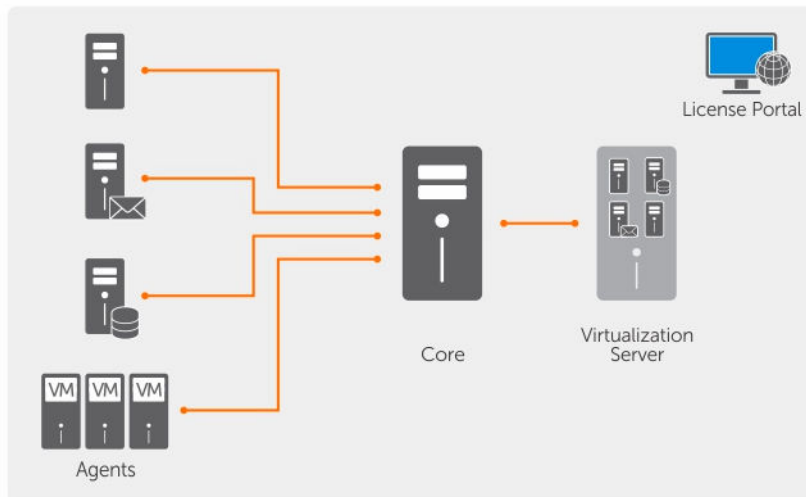




그림 9. 가상 시스템에 데이터 내보내기

보호되는 데이터를 Windows 시스템에서 가상 시스템으로 지속적으로 내보내 가상 대기를 만듭니다. 가상 시스템에 내보낼 때 시스템의 보호 일정에 정의된 매개변수는 물론 복구 지점의 모든 백업 데이터가 내보내집니다.

VMware, ESXi, Hyper-V 및 Oracle VirtualBox에 보호되는 Windows 또는 Linux 시스템에 대한 복구 지점의 가상 내보내기를 수행할 수 있습니다.

 **노트:** 어플라이언스 탭에 가상 시스템이 모두 표시되지만, Hyper-V 및 ESXi 가상 시스템만 관리할 수 있습니다. 다른 가상 시스템을 관리하려면 하이퍼바이저 관리 도구를 사용하십시오.

 **노트:** 내보내는 가상 시스템은 평가판이나 무료 버전이 아닌 사용 허가된 버전의 ESXi, VMWare Workstation 또는 Hyper-V여야 합니다.

### 동적 및 기본 볼륨 지원 제한사항

AppAssure는 모든 동적 및 기본 볼륨의 스냅샷 만들기를 지원합니다. 또한 하나의 실제 디스크에 있는 단순 동적 볼륨 내보내기를 지원합니다. 이름을 통해 알 수 있듯이, 단순 동적 볼륨은 스트라이핑, 미러링 또는 스캔되지 않은 볼륨을 말합니다. 비단순 동적 볼륨에는 완전히 해석할 수 없는 임의의 디스크 지오메트리가 있기 때문에 내보낼 수 없습니다. AppAssure에는 복잡하거나 비단순 동적 볼륨을 내보낼 수 있는 기능이 있습니다.

AppAssure 버전 5.3.1.60393에서는 단순 동적 볼륨만 내보낼 수 있음을 알리는 확인란이 사용자 인터페이스에 추가되었습니다. 이 버전에서 사용자 인터페이스가 이렇게 변경되기 전에는 복잡 또는 비단순 동적 디스크 내보내기 옵션이 표시되었을 수 있습니다. 이러한 디스크를 내보내려고 시도하면 내보내기 작업에 실패합니다.

## Microsoft Windows 시스템에서 가상 시스템으로 백업 정보 내보내기

AppAssure에서는 시스템의 보호 일정에 대해 정의된 매개변수 및 복구 지점의 모든 백업 정보를 내보내 Microsoft Windows 시스템의 데이터를 가상 시스템(VMware, ESXi, Hyper-V 및 Oracle VirtualBox)으로 내보낼 수 있습니다.

Windows 백업 정보를 가상 시스템으로 내보내려면 다음을 수행하십시오.

1. Core 콘솔에서 **Machines(시스템)** 탭을 클릭합니다.
2. 보호된 시스템 목록에서 내보낼 복구 지점이 있는 시스템 또는 클러스터를 선택합니다.
3. 해당 시스템에 대한 **Actions(작업)** 드롭다운 메뉴에서 **Export(내보내기)**를 클릭한 후 수행할 내보내기 유형을 선택합니다. 다음 옵션을 선택할 수 있습니다.
  - ESXi 내보내기
  - VMware 워크스테이션 내보내기
  - Hyper-V 내보내기
  - Oracle VirtualBox 내보내기

**Select Export Type(내보내기 유형 선택)** 대화 상자가 나타납니다.

## ESXi 내보내기를 사용하여 Windows 데이터 내보내기

AppAssure에서는 1회 또는 연속 내보내기를 수행하여 ESXi 내보내기를 통해 데이터를 내보내도록 선택할 수 있습니다.

### 한 번 ESXi 내보내기 수행

한 번 ESXi 내보내기를 수행하려면 다음을 수행하십시오.

1. **Select Export Type(내보내기 유형 선택)** 대화 상자에서 **One-time export(한 번 내보내기)**를 클릭합니다.
2. **Next(다음)**를 클릭합니다.  
**ESXi Export - Select Recovery Point(ESXi 내보내기 - 복구 지점 선택)** 대화 상자가 표시됩니다.
3. 내보낼 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.

Virtual Standby Recovery Point to VMware vCenter Server/ESXi(VMware vCenter 서버/ESXi에 대한 가상 대기 복구 지점) 대화 상자가 표시됩니다.

### ESXi 내보내기 수행을 위한 가상 시스템 정보 정의

ESXi 내보내기 수행을 위한 가상 시스템 정보를 정의하려면 다음을 수행하십시오.

1. **Virtual Standby Recovery Point to VMware vCenter Server/ESXi(VMware vCenter 서버/ESXi에 대한 가상 대기 복구 지점)** 대화 상자에서, 아래에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

텍스트 상자	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본 포트는 443입니다.
사용자 이름	호스트 시스템에 대한 로그인 자격 증명을 입력합니다.
암호	호스트 시스템에 대한 로그인 자격 증명을 입력합니다.

2. **Connect(연결)**를 클릭합니다.

### 지속적(가상 대기) ESXi 내보내기 수행

지속적(가상 대기) ESXi 내보내기를 수행하려면 다음을 수행하십시오.

1. **Select Export Type(내보내기 유형 선택)** 대화 상자에서 **Continuous (Virtual Standby)**(지속적(가상 대기))를 클릭합니다.
2. **Next(다음)**를 클릭합니다.


**Virtual Standby Recovery Point to VMware vCenter Server/ESXi(VMware vCenter 서버/ESXi에 대한 가상 대기 복구 지점)** 대화 상자가 표시됩니다.

3. 아래에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.


텍스트 상자	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본 포트는 443입니다.
사용자 이름	호스트 시스템에 대한 로그인 자격 증명을 입력합니다.
암호	호스트 시스템에 대한 로그인 자격 증명을 입력합니다.

4. **Connect(연결)**를 클릭합니다.
5. **Options(옵션)** 탭에서 설명된 대로 가상 시스템에 대한 정보를 입력합니다.

텍스트 상자	설명
가상 시스템 이름	생성 중인 가상 시스템의 이름을 입력합니다(예: VM-0A1B2C3D4).

 **노트:** 에이전트 이름에서 파생된 이름이나 에이전트 이름과 일치하는 이름을 사용하는 것이 좋습니다. 또한 하이퍼바이저 유형, IP 주소 또는 DNS 이름에서 파생된 이름을 생성할 수도 있습니다.

메모리	메모리 사용량을 지정합니다. 다음과 같은 옵션을 선택할 수 있습니다. <ul style="list-style-type: none"> <li>• 원본 시스템과 동일한 RAM 양 사용</li> </ul>
-----	---

텍스트 상자	<b>설명</b> <ul style="list-style-type: none"> <li>• 사용할 RAM의 크기를 지정하려면 <b>Use a specific amount of RAM(특정 RAM 크기 사용)</b>을 클릭합니다(예: 4096MB). 허용되는 최소 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다(권장됨).</li> </ul>
ESXi 데이터 센터	ESXi 데이터 센터에 대한 이름을 입력합니다.
ESXi 호스트	ESXi 호스트에 대한 자격 증명을 입력합니다.
데이터 저장소	데이터 저장소에 대한 상세정보를 입력합니다.
Version(버전)	가상 시스템의 버전을 선택합니다.
	 <b>노트:</b> vSphere 클라이언트를 사용하여 가상 시스템을 관리하려면 버전 8 이전을 선택하십시오.
리소스 풀	리소스 풀에 대한 이름을 입력합니다.

6. **Start Export(내보내기 시작)**를 클릭합니다.

## VMware 워크스테이션 내보내기를 사용하여 Windows 데이터 내보내기

AppAssure에서는 1회 또는 연속 내보내기를 수행하여 VMware Workstation 내보내기를 통해 데이터를 내보내도록 선택할 수 있습니다. 해당 유형의 내보내기에 맞게 VMware Workstation 내보내기를 사용하여 내보내려면 다음 절차의 단계를 완료하십시오.

### 한 번 VMware 워크스테이션 내보내기 수행


한 번 VMware 워크스테이션 내보내기를 수행하려면 다음을 수행하십시오.

1. **Select Export Type(내보내기 유형 선택)** 대화 상자에서 **One-time export(한 번 내보내기)**를 클릭합니다.
2. **Next(다음)**를 클릭합니다.  
**VM Export - Select Recovery Point(VM 내보내기 - 복구 지점 선택)** 대화 상자가 나타납니다.
3. 내보낼 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.  
**Virtual Standby Recovery Point to VMware Workstation/Server(VMware 워크스테이션/서버에 대한 가상 대기 복구 지점)** 대화 상자가 나타납니다.

### 한 번 VMware 워크스테이션 내보내기를 수행하도록 설정 정의

한 번 VMware 워크스테이션 내보내기를 수행하도록 설정을 정의하려면 다음을 수행하십시오.

1. **Virtual Standby Recovery Point to VMware Workstation/Server(VMware 워크스테이션/서버에 대한 가상 대기 복구 지점)** 대화 상자에서, 아래에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

텍스트 상자	<b>설명</b>
대상 경로	가상 시스템을 생성할 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다.
	 <b>노트:</b> 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그인 자격 증명을 입력합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.

## 텍스트 상자 설명

### 사용자 이름

가상 시스템에 대한 로그인 자격 증명을 입력합니다.

- 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 사용자 이름을 입력해야 합니다.
- 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.

### 암호

가상 시스템에 대한 로그인 자격 증명을 입력합니다.

- 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 암호를 입력해야 합니다.
- 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.

2. **Export Volumes(볼륨 내보내기)** 창에서 내보낼 볼륨을 선택합니다(예: C:\ 및 D:\).

3. **Options(옵션)** 창에서 아래에 설명된 대로 메모리 사용량 및 가상 시스템에 대한 정보를 입력합니다.

## 텍스트 상자 설명

### 가상 시스템

생성 중인 가상 시스템의 이름을 입력합니다(예: VM-0A1B2C3D4).



**노트:** 에이전트 이름에서 파생된 이름이나 에이전트 이름과 일치하는 이름을 사용하는 것이 좋습니다. 또한 하이퍼바이저 유형, IP 주소 또는 DNS 이름에서 파생된 이름을 생성할 수도 있습니다.

### 메모리

가상 시스템의 메모리를 지정합니다.

- RAM 구성을 원본 시스템과 동일하게 지정하려면 **Use the same amount of RAM as the source machine(원본 시스템과 동일한 RAM 크기 사용)**을 클릭합니다.
- 사용할 RAM의 크기를 지정하려면 **Use a specific amount of RAM(특정 RAM 크기 사용)**을 클릭합니다(예: 4096MB). 허용되는 최소 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다(권장됨).

4. **Export(내보내기)**를 클릭합니다.

## 지속적(가상 대기) VMware 워크스테이션 내보내기 수행

지속적(가상 대기) VMware 워크스테이션 내보내기를 수행하려면 다음을 수행하십시오.

1. **Select Export Type(내보내기 유형 선택)** 대화 상자에서 **Continuous (Virtual Standby)(지속적(가상 대기))**를 클릭한 후 **Next(다음)**를 클릭합니다.

**VM Export - Select Recovery Point(VM 내보내기 - 복구 지점 선택)** 대화 상자가 나타납니다.

2. 내보낼 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.

**Virtual Standby Recovery Point to VMware Workstation/Server(VMware 워크스테이션/서버에 대한 가상 대기 복구 지점)** 대화 상자가 나타납니다.

3. 아래에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.


## 텍스트 상자 설명

### 대상 경로

가상 시스템을 생성할 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다.



## 텍스트 상자 설명

 **노트:** 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그인 자격 증명을 입력합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.

**사용자 이름** 가상 시스템에 대한 로그인 자격 증명을 입력합니다.

- 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 사용자 이름을 입력해야 합니다.
- 로컬 경로를 입력한 경우에는 사용자 이름이 필요하지 않습니다.


**암호** 가상 시스템에 대한 로그인 자격 증명을 입력합니다.

- 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 암호를 입력해야 합니다.
- 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.

4. **Export Volumes(볼륨 내보내기)** 창에서 내보낼 볼륨을 선택합니다(예: C:\ 및 D:\).
5. **Options(옵션)** 창에서 아래에 설명된 대로 메모리 사용량 및 가상 시스템에 대한 정보를 입력합니다.

## 텍스트 상자 설명

**가상 시스템** 생성 중인 가상 시스템의 이름을 입력합니다(예: VM-0A1B2C3D4).

 **노트:** 에이전트 이름에서 파생된 이름이나 에이전트 이름과 일치하는 이름을 사용하는 것이 좋습니다. 또한 하이퍼바이저 유형, IP 주소 또는 DNS 이름에서 파생된 이름을 생성할 수도 있습니다.

**메모리** 가상 시스템의 메모리를 지정합니다.

- RAM 구성을 원본 시스템과 동일하게 지정하려면 **Use the same amount of RAM as the source machine(원본 시스템과 동일한 RAM 크기 사용)**을 클릭합니다.
- 사용할 RAM의 크기를 지정하려면 **Use a specific amount of RAM(특정 RAM 크기 사용)**을 클릭합니다(예: 4096MB). 허용되는 최소 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다(권장).

6. **Perform initial ad-hoc export(초기 임시 내보내기 수행)**를 클릭하여 데이터의 내보내기를 테스트합니다.
7. **Save(저장)**를 클릭합니다.

## Hyper-V 내보내기를 사용하여 Windows 데이터 내보내기


1회 또는 연속 내보내기를 수행하여 Hyper-V 내보내기를 통해 데이터를 내보내도록 선택할 수 있습니다. 해당 내보내기 유형에 Hyper-V 내보내기를 사용하여 내보내려면 다음 절차의 단계를 완료하십시오. DL 어플라이언스에서는 다음과 같은 호스트에 1세대 Hyper-V 내보내기가 지원됩니다.

- Windows 8
- Windows 8.1
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

- Windows Server 2012 R2


DL 어플라이언스에서는 다음과 같은 호스트에 2세대 Hyper-V 내보내기가 지원됩니다.

- Windows 8.1
- Windows Server 2012 R2

 **노트:** 보호 시스템 중에서 Hyper-V 2세대 호스트에 내보낼 수 없는 시스템도 있습니다.

다음과 같은 UEFI(Unified Extensible Firmware Interface) 운영 체제가 포함된 보호 시스템에서만 Hyper-V 2세대 호스트에 가상 내보내기가 지원됩니다.

- Windows 8 (UEFI)
- Windows 8.1 (UEFI)
- Windows Server 2012 (UEFI)
- Windows Server 2012R2 (UEFI)

 **노트:** Hyper-V 호스트에 할당된 RAM이 내보내기 수행에 충분하지 않으면 2세대 VM에 Hyper-V 내보내기에 실패합니다.

다음 절차의 단계를 완료하여 적절한 유형의 내보내기를 수행하십시오.

### 한 번 Hyper-V 내보내기 수행

한 번 Hyper-V 내보내기를 수행하려면 다음을 수행하십시오.

1. Core 콘솔에서, 내보낼 시스템으로 이동합니다.
2. Summary(요약) 탭에서 **Actions(작업)** → **Export(내보내기)** → **One-time(1회)**을 클릭합니다.  
**Protected Machines(보호되는 시스템)** 페이지에 **Export Wizard(내보내기 마법사)**가 표시됩니다.
3. 내보내기에 사용할 시스템을 선택하고 **Next(다음)**를 클릭합니다.
4. **Recovery Points(복구 지점)** 페이지에서, 내보낼 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.

### 한 번 Hyper-V 내보내기를 수행하도록 설정 정의

한 번 Hyper-V 내보내기를 수행하도록 설정을 정의하려면 다음을 수행하십시오.


1. Hyper-V 대화 상자에서 **Use local machine(로컬 시스템 사용)**을 클릭하여 Hyper-V 역할이 할당된 로컬 시스템에 Hyper-V 내보내기를 수행합니다.
2. Hyper-V Server가 원격 시스템에 있음을 나타내려면 **Remote host(원격 호스트)** 옵션을 클릭합니다.  
Remote host(원격 호스트) 옵션을 선택한 경우 아래에 설명된 대로 원격 호스트의 매개변수를 입력합니다.

텍스트 상자	설명
호스트 이름	Hyper-V Server에 대한 IP 주소 또는 호스트 이름을 입력합니다. 이는 원격 Hyper-V Server의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. 이는 Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V Server의 워크스테이션에 대한 관리 권한이 있는 사용자의 사용자 이름을 입력합니다. 이는 가상 시스템에 대한 로그인 자격 증명을 지정하는 데 사용됩니다.


## 텍스트 상자 설명

**암호** Hyper-V Server의 워크스테이션에 대한 관리 권한이 있는 사용자 계정의 암호를 입력합니다. 이는 가상 시스템에 대한 로그인 자격 증명을 지정하는 데 사용됩니다.

3. **Next(다음)**를 클릭합니다.
4. **Virtual Machines Options(가상 시스템 옵션)** 페이지의 **VM Machine Location(VM 시스템 위치)** 텍스트 상자에 가상 시스템의 경로 또는 위치를 입력합니다(예: **D:\export**). VM 위치에 가상 시스템에 필요한 가상 드라이브와 VM 메타데이터를 보관할 수 있는 충분한 공간이 있어야 합니다.
5. **Virtual Machine Name(가상 시스템 이름)** 텍스트 상자에 가상 시스템의 이름을 입력합니다.  
입력한 이름이 Hyper-V Manager(Hyper-V 관리자) 콘솔의 가상 시스템 목록에 표시됩니다.
6. 다음 중 하나를 클릭합니다.
  - **Use the same amount of RAM as the source machine(원본 시스템과 동일한 RAM 크기 사용)** - 가상 시스템과 소스 시스템 간에 RAM 크기를 동일하게 지정합니다.
  - **Use a specific amount of RAM(특정 RAM 크기 사용)** - 내보낸 후 가상 시스템에서 보유하는 메모리 양(예: 4096MB)을 지정합니다(권장).
7. 디스크 형식을 지정하려면 **Disk Format(디스크 형식)** 옆에서 다음 중 하나를 클릭합니다.
  - **VHDX**
  - **VHD**

 **노트:** Hyper-V 내보내기에서는, 대상 시스템이 Windows 8(Windows Server 2012) 이상을 실행하고 있는 경우 VHDX 디스크 형식이 지원됩니다. 해당 환경에서 VHDX가 지원되지 않을 경우 이 옵션이 비활성화됩니다.
8. **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다. 가상 시스템을 보호되는 시스템의 효과적인 백업으로 사용하려면 보호되는 시스템의 부팅 드라이브를 포함합니다(예: C:\).  
VHD용으로 선택한 볼륨의 크기는 2040GB를 초과하지 않아야 합니다. 선택한 볼륨이 2040GB보다 크고 VHD 형식을 선택한 경우에는 오류가 발생합니다.
9. **Summary(요약)** 페이지에서, **Finish(마침)**를 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

## 지속적(가상 대기) Hyper-V 내보내기 수행

 **노트:** DL1000에서 2개 VM에 3 TB 구성에서만 1회 내보내기 및 지속적 내보내기(가상 대기) 기능이 지원됩니다.


연속(가상 대기) Hyper-V 내보내기를 수행하려면 다음을 수행하십시오.


1. Core 콘솔의 **Virtual Standby(가상 대기)** 탭에서 **Add(추가)**를 클릭하여 **Export Wizard(내보내기 마법사)**를 실행합니다. **Export Wizard(내보내기 마법사)**의 **Protected Machines(보호되는 시스템)** 페이지에서 다음을 수행합니다.
2. 내보낼 시스템을 선택하고 **Next(다음)**를 클릭합니다.
3. **Summary(요약)** 탭에서 **Export(내보내기)** → **Virtual Standby(가상 대기)**를 클릭합니다.
4. Hyper-V 대화 상자에서 **Use local machine(로컬 시스템 사용)**을 클릭하여 Hyper-V 역할이 할당된 로컬 시스템에 Hyper-V 내보내기를 수행합니다.
5. Hyper-V Server가 원격 시스템에 있음을 나타내려면 **Remote host(원격 호스트)** 옵션을 클릭합니다. **Remote host(원격 호스트)** 옵션을 선택한 경우 아래에 설명된 대로 원격 호스트의 매개변수를 입력합니다.

## 텍스트 상자 설명

호스트 이름	Hyper-V Server에 대한 IP 주소 또는 호스트 이름을 입력합니다. 이는 원격 Hyper-V Server의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. 이는 Core가 이 시스템과 통신하는 포트를 나타냅니다.
사용자 이름	Hyper-V Server의 워크스테이션에 대한 관리 권한이 있는 사용자의 사용자 이름을 입력합니다. 이는 가상 시스템에 대한 로그인 자격 증명을 지정하는 데 사용됩니다.
암호	Hyper-V Server의 워크스테이션에 대한 관리 권한이 있는 사용자 계정의 암호를 입력합니다. 이는 가상 시스템에 대한 로그인 자격 증명을 지정하는 데 사용됩니다.

- Virtual Machines Options(가상 시스템 옵션)** 페이지의 **VM Machine Location(VM 시스템 위치)** 텍스트 상자에 가상 시스템의 경로 또는 위치를 입력합니다(예: D:\export). VM 위치에 가상 시스템에 필요한 가상 드라이브와 VM 메타데이터를 보관할 수 있는 충분한 공간이 있어야 합니다.
- Virtual Machine Name(가상 시스템 이름)** 텍스트 상자에 가상 시스템의 이름을 입력합니다.  
입력한 이름이 Hyper-V Manager(Hyper-V 관리자) 콘솔의 가상 시스템 목록에 표시됩니다.
- 다음 중 하나를 클릭합니다.
  - Use the same amount of RAM as the source machine(원본 시스템과 동일한 RAM 크기 사용)** - 가상 시스템과 소스 시스템 간에 RAM 크기를 동일하게 지정합니다.
  - Use a specific amount of RAM(특정 RAM 크기 사용)** - 내보낸 후 가상 시스템에서 보유하는 메모리 양(예: 4096MB)을 지정합니다(권장됨).
- 세대를 지정하려면 다음 중 하나를 클릭합니다.
  - 1세대(권장됨)
  - 2세대
- 디스크 형식을 지정하려면 **Disk Format(디스크 형식)** 옆에서 다음 중 하나를 클릭합니다.
  - VHDX(기본값)
  - VHD

 **노트:** Hyper-V 내보내기에서는 대상 시스템이 Windows 8(Windows Server 2012) 이상을 실행 중인 경우 VHDX 디스크 형식을 지원합니다. 사용 중인 환경에서 VHDX를 지원하지 않으면 옵션이 비활성화됩니다. 네트워크 어댑터 페이지에서 스위치에 연결할 가상 어댑터를 선택하십시오.
- Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다. 가상 시스템을 보호되는 시스템의 효과적인 백업으로 사용하려면 보호되는 시스템의 부팅 드라이브를 포함합니다(예: C:\).  
VHD용으로 선택한 볼륨의 크기는 2040GB를 초과하지 않아야 합니다. 선택한 볼륨이 2040GB보다 크고 VHD 형식을 선택한 경우에는 오류가 발생합니다.
- Summary(요약)** 페이지에서, **Finish(마침)**를 클릭하여 마법사를 완료하고 내보내기를 시작합니다.
 

 **노트:** **Virtual Standby(가상 대기)** 또는 **Events(이벤트)** 탭을 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

## Oracle VirtualBox 내보내기를 사용하여 Microsoft Windows 데이터 내보내기

AppAssure에서는 한 번 내보내기를 수행하거나 지속적 내보내기를 설정(가상 대기의 경우)하여 Oracle VirtualBox 내보내기를 사용해 데이터를 내보내도록 선택할 수 있습니다.

다음 절차의 단계를 완료하여 적절한 유형의 내보내기를 수행하십시오.



**노트:** 이 유형의 내보내기를 수행하려면 Core 시스템에 Oracle VirtualBox가 설치되어 있어야 합니다. Windows 호스트에 VirtualBox Version 4.2.18 이상이 지원됩니다.

## 1회 Oracle VirtualBox 내보내기 수행

이 절차의 단계를 완료하여 Oracle VirtualBox에 1회 내보내기를 수행할 수 있습니다.

### 1회 Oracle VirtualBox 내보내기를 수행하려면 다음을 수행하십시오.

1. AppAssure Core 콘솔에서 다음 중 하나를 수행합니다.
  - 단추 모음에서 **Export(내보내기)**를 클릭하여 Export Wizard(내보내기 마법사)를 시작하고 다음을 수행합니다.
    1. **Select Export Type(내보내기 유형 선택)** 페이지에서 **One-time export(1회 내보내기)**를 선택한 후 **Next(다음)**를 클릭합니다.
    2. **Protected Machines(보호되는 시스템)**에서 가상 시스템으로 내보낼 보호되는 시스템을 선택하고 **Next(다음)**를 클릭합니다.
  - 내보낼 시스템으로 이동한 다음 **Summary(요약)** 탭에 있는 해당 시스템의 **Actions(작업)** 드롭다운 메뉴에서 **Export(내보내기) > One-time(1회)**을 선택합니다.

**Recovery Points(복구 지점)** 페이지에 Export Wizard(내보내기 마법사)가 나타납니다.

2. **Recovery Points(복구 지점)** 페이지에서 내보낼 AppAssure Core의 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.
3. **Export Wizard(내보내기 마법사)**의 **Destination(대상)** 페이지에 있는 **Recover to Virtual machine(가상 시스템으로 복구)** 드롭다운 메뉴에서 VirtualBox를 선택하고 **Next(다음)**를 클릭합니다.
4. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서 **Use Windows machine(Windows 시스템 사용)**을 선택합니다.
5. 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

#### 옵션

#### 설명

##### 가상 시스템 이름

생성되는 가상 시스템의 이름을 입력합니다.



**노트:** 기본 이름은 원본 시스템의 이름입니다.

##### 대상 경로

가상 시스템을 생성할 로컬 또는 원격 대상 경로를 지정합니다.



**노트:** 대상 경로는 루트 디렉터리가 될 수 없습니다.

네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그인 자격 증명(사용자 이름 및 암호)을 입력해야 합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.

##### 메모리

다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다.

- RAM 구성을 원본 시스템과 동일하게 지정하려면 **Use the same amount of RAM as source machine(원본 시스템과 동일한 RAM 크기 사용)**을 클릭합니다.
- 사용할 RAM의 크기를 지정하려면 **Use a specific amount of RAM(특정 RAM 크기 사용)**을 클릭합니다(예: 4096MB). 허용되는 최소 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다(권장됨).

6. 가상 시스템의 사용자 계정을 지정하려면 **Specify the user account for the exported virtual machine(내보낸 가상 시스템의 사용자 계정 지정)**을 선택하고 다음과 같은 정보를 입력합니다. 이 계정은 가상 시스템에 여러 개의 사용자 계정이 있는 경우 가상 시스템이 등록되는 특정 사용자 계정을 나타냅니다.


다. 이 사용자 계정으로 로그인하면 해당 사용자에게만 VirtualBox 관리자에 가상 시스템이 표시됩니다. 계정이 지정되지 않으면, Oracle VirtualBox를 사용하는 Windows 시스템에 있는 모든 기존 사용자에게 대해 가상 시스템이 등록됩니다.

- **User name(사용자 이름)** - 가상 시스템이 등록되는 사용자 이름을 입력합니다.
- **Password(암호)** - 사용자 계정의 암호를 입력합니다.

7. **Next(다음)**를 클릭합니다.

입력한 이름이 Hyper-V Manager(Hyper-V 관리자) 콘솔의 가상 시스템 목록에 표시됩니다.

8. **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택합니다. 가상 시스템을 보호되는 시스템의 효과적인 백업으로 사용하려면 보호되는 시스템의 부팅 드라이브를 포함합니다(예: C:\).
9. **Summary(요약)** 페이지에서 **Finish(마침)**을 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

 **노트: Virtual Standby(가상 대기)** 또는 **Events(이벤트)** 탭을 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

## 지속적(가상 대기) Oracle VirtualBox 내보내기 수행

이 절차의 단계를 완료하여 가상 대기를 생성하고 Oracle VirtualBox에 지속적 내보내기를 수행할 수 있습니다.

*지속적(가상 대기) VirtualBox 내보내기를 수행하려면 다음을 수행하십시오.*


1. AppAssure Core 콘솔에서 다음 중 하나를 수행합니다.
  - **Virtual Standby(가상 대기)** 탭에서, **Add(추가)**를 클릭하여 Export Wizard(내보내기 마법사)를 실행합니다. Export Wizard(내보내기 마법사)의 **Protected Machines(보호되는 시스템)** 페이지에서 내보낼 보호되는 시스템을 선택하고 **Next(다음)**를 클릭합니다.
  - 내보낼 시스템으로 이동하고, 해당 시스템의 **Actions(작업)** 드롭다운 메뉴에 있는 **Summary(요약)** 탭에서 **Export(내보내기)** > **Virtual Standby(가상 대기)**를 클릭합니다.
2. Export Wizard(내보내기 마법사)의 **Destination(대상)** 페이지에 있는 **Recover to Virtual machine(가상 시스템으로 복구)** 드롭다운 메뉴에서 **VirtualBox**를 선택하고 **Next(다음)**를 클릭합니다.
3. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서 **Use Windows machine(Windows 시스템 사용)**을 선택합니다.
4. 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

### 옵션

### 설명


#### 가상 시스템 이름

생성되는 가상 시스템의 이름을 입력합니다.

 **노트:** 에이전트 이름에서 파생된 이름이나 에이전트 이름과 일치하는 이름을 사용하는 것이 좋습니다. 또한 하이퍼바이저 유형, IP 주소 또는 DNS 이름에서 파생된 이름을 생성할 수도 있습니다.

#### 대상 경로

가상 시스템을 생성할 로컬 또는 원격 대상 경로를 지정합니다.

 **노트:** 대상 경로는 루트 디렉터리가 될 수 없습니다.

네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그인 자격 증명(사용자 이름 및 암호)을 입력해야 합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.

#### 메모리

다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다.

- 가상 시스템과 원본 시스템 간의 RAM 크기를 동일하게 식별하려면 원본 시스템으로 **Use the same amount of RAM(동일한 RAM 크기 사용)**을 클릭합니다.

## 옵션


## 설명

- 사용할 RAM의 크기를 지정하려면 **Use a specific amount of RAM(특정 RAM 크기 사용)**을 클릭합니다(예: 4096MB). 허용되는 최소 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다(권장).

5. 가상 시스템의 사용자 계정을 지정하려면 **Specify the user account for the exported virtual machine(내보낸 가상 시스템의 사용자 계정 지정)**을 선택하고 다음과 같은 정보를 입력합니다. 이 계정은 가상 시스템에 여러 개의 사용자 계정이 있는 경우 가상 시스템이 등록되는 특정 사용자 계정을 나타냅니다. 이 사용자 계정으로 로그인하면 해당 사용자에게만 VirtualBox 관리자에 가상 시스템이 표시됩니다. 계정이 지정되지 않으면, VirtualBox를 사용하는 Windows 시스템에 있는 모든 기존 사용자에 대해 가상 시스템이 등록됩니다.


- **User name(사용자 이름)** - 가상 시스템이 등록되는 사용자 이름을 입력합니다.
- **Password(암호)** - 사용자 계정의 암호를 입력합니다.

6. **Perform initial one-time export(초기 한 번 내보내기 수행)**를 선택하여 다음에 예정된 스냅샷이 생성될 때까지 기다리지 않고 즉시 가상 내보내기를 수행합니다.
7. Volumes(볼륨) 페이지에서 내보낼 볼륨을 선택합니다. 가상 시스템을 보호되는 시스템의 효과적인 백업으로 사용하려면 보호되는 시스템의 부팅 드라이브를 포함합니다(예: C:\).
8. **Summary(요약)** 페이지에서 **Finish(마침)**를 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

 **노트: Virtual Standby(가상 대기)** 또는 **Events(이벤트)** 탭을 확인하여 내보내기의 상태 및 진행률을 모니터링할 수 있습니다.

## 가상 시스템 관리

**VM Management(VM 관리)** 탭에서 보호되는 시스템의 상태가 표시되며, 네트워크 어댑터를 시작, 중지 및 추가할 수 있습니다(Hyper-V and ESXi 가상 시스템에만 해당). VM 관리 탭으로 이동하려면 **Appliance(어플라이언스)** → **VM Management(VM 관리)**를 클릭합니다.

 **노트: Appliance(어플라이언스)** → **VM Management(VM 관리)** 탭을 선택할 때마다 최대 30초 간격으로 네트워크 어댑터 시작, 중지 및 추가 단추가 표시됩니다.

Appliance

Storage

Tasks

Virtual Machine Management

Hyper-V Virtual Standby(s)

Agent / VM Information				Export Status		Hypervisor Information		VM Operations	
Agent Name	VM Name	Status	Location	Status	Last Export	Name	Status		
10.10.101.95	LHyperV-10.10.101.84	Enabled (Running)	C:\V5_SPACE\LocalHV_10.10.101.95\LHyperV-10.10.101.84	Succeeded	3/27/2015 5:02:20 PM	localhost	Online	<div>Start</div> <div>Stop</div> <div>Add Network Adapter</div>	

ESX Virtual Standby(s)

Agent / VM Information				Export Status		Hypervisor Information		VM Operations	
Agent Name	VM Name	Status	Location	Status	Last Export	Name	Status		
10.10.101.84	ESX-10.10.101.84	Disabled (Off)	ESX-10.10.101.84	Failed	4/9/2015 2:45:09 PM	10.10.101.7	Online	<div>Start</div> <div>Stop</div> <div>Add Network Adapter</div>	

Other Virtual Standby(s)

Hypervisor Information		Agent / VM Information		Export Status	
Type	Agent Name	Location	Status	Last Export	
Oracle VirtualBox	Test-10.10.101.96	C:\test	Unknown	Not performed	

## Hyper-V 및 ESXi 가상 대기에 대한 VM 관리

## 필드

## 설명

**Agent / VM Information(에이전트/VM 정보)**

**Agent Name(에이전트 이름):** 가상 대기를 생성한 보호되는 시스템의 이름을 나타냅니다.

**VM Name(VM 이름):** VM의 이름을 나타냅니다.



**노트:** 에이전트 이름에서 파생된 이름이나 에이전트 이름과 일치하는 이름을 사용하는 것이 좋습니다. 또한 하이퍼바이저 유형, IP 주소 또는 DNS 이름에서 파생된 이름을 생성할 수도 있습니다.

**Status(상태):** 가상 시스템 상태를 나타냅니다. 가능한 값은 다음과 같습니다.

- Running(실행)
- Stopped(중지됨)
- Starting(시작)
- Suspended(일시 중지됨)
- Stopping(중지)
- Unknown(알 수 없음)(임시 상태)



**노트:** 위의 상태 값은 하이퍼바이저 유형에 따라 다르며, 일부 하이퍼바이저는 모든 상태 값을 표시하지 않습니다.

**Location(위치):** VM의 위치를 나타냅니다(예: D:\export). VM 위치에 가상 시스템에 필요한 가상 드라이브와 VM 메타데이터를 보관할 수 있는 충분한 공간이 있어야 합니다.

**Export Status(내보내기 상태)**

**Status(상태)**

1. 다음과 같은 내보내기 프로세스의 상태를 나타냅니다.
  - Complete(완료)
  - Failed(실패)
  - In progress(진행 중)
  - Not Performed(수행되지 않음)
2. 현재 내보내기가 진행 중인 경우 내보내기 백분율이 표시됩니다.

**Last Export(마지막 내보내기):** 마지막 내보내기 시간을 나타냅니다.

**Hypervisor Information(하이퍼바이저 정보)**

**Name(이름):** VM이 생성되는 하이퍼바이저의 이름을 나타냅니다.

**Status(상태):** Hyper-V 및 ESXi 하이퍼바이저에 대한 연결 상태를 나타냅니다.

- Online(온라인)
- Offline(오프라인)
- Unknown(알 수 없음)(임시 상태)



**노트:** 상태는 Hyper-V 및 ESXi 하이퍼바이저에 대해서만 표시됩니다.

**VM Operations(VM 작업)**

가상 시스템을 시작하거나 중지하고 네트워크 어댑터를 추가할 수 있습니다.



## 기타 가상 대기의 VM 관리



필드	설명
<b>Hypervisor Information(하이퍼바이저 정보)</b>	<b>Type(유형):</b> 하이퍼바이저 유형을 나타냅니다.
<b>Agent / VM Information(에이전트/VM 정보)</b>	<b>Agent Name(에이전트 이름):</b> 가상 대기를 생성한 보호되는 시스템의 이름을 나타냅니다.  <b>Location(위치):</b> VM의 위치를 나타냅니다(예: D:\export). VM 위치에 가상 시스템에 필요한 가상 드라이브와 VM 메타데이터를 보관할 수 있는 충분한 공간이 있어야 합니다.
<b>Export Status(내보내기 상태)</b>	<b>Status(상태)</b> <ol style="list-style-type: none"> <li>다음과 같은 내보내기 프로세스의 상태를 나타냅니다. <ul style="list-style-type: none"> <li>Complete(완료)</li> <li>Failed(실패)</li> <li>In progress(진행 중)</li> <li>Not Performed(수행되지 않음)</li> </ul> </li> <li>현재 내보내기가 진행 중인 경우 내보내기 백분율이 진행률 표시줄로 표시됩니다.</li> </ol> <p><b>Last Export(마지막 내보내기):</b> 마지막 내보내기 시간을 나타냅니다.</p>

## 가상 네트워크 어댑터 생성

가상 시스템에서 인터넷에 연결하려면 가상 네트워크 어댑터(VNA)가 하나 이상 있어야 합니다. 하나의 VM에 보호되는 시스템에서 실제 네트워크 어댑터(RNA)에 각각 사용할 수 있는 하나의 VNA가 있어야 하며, VNA와 일치하는 RNA의 구성이 유사해야 합니다. 가상 대기를 생성할 때 VM에 VNA를 추가하거나 나중에 VNA를 추가할 수 있습니다.


가상 대기를 생성하면 가상 시스템을 구성할 때 보호되는 시스템에 모든 어댑터에 대해 제안된 어댑터가 있습니다. 이러한 제안된 어댑터를 일부 또는 모두 추가하거나 제거할 수 있습니다. VM당 최대 VNA의 수는 하이퍼바이저 유형에 따라 다릅니다. Hyper-V의 경우 모든 가상 시스템에 대해 어댑터를 최대 8개까지 추가할 수 있습니다.

가상 네트워크 어댑터 생성하려면 다음을 수행하십시오.


- VM Management(VM 관리)** 페이지로 이동합니다.
- VNA를 추가할 VM과 연결된 **Add Network Adapter(네트워크 어댑터 추가)** 단추를 클릭합니다.
  -  **노트:** 보호되는 시스템의 내보내기 또는 백업이 실행 중인 가상 대기의 VM에 어댑터를 추가하지 마십시오. 추가 VNA로 인해 향후 내보내기 작업이 실패할 수 있습니다.
  -  **노트:** 보호되는 시스템을 교체할 때 VM을 시작하기 바로 전에 VNA를 추가하는 것이 좋습니다. 가상 대기 탭을 통해 VM에 대해 대기 중인 내보내기를 중지하거나 일시 중지했는지 확인하십시오.

**Virtual Network Adapters and Switches(가상 네트워크 어댑터 및 스위치)** 창이 나타납니다.

- Create(생성)**를 클릭하여 가상 네트워크 어댑터를 생성합니다.  
**Create Virtual Network Adapter(가상 네트워크 어댑터 생성)** 창이 나타납니다.
- 드롭다운 메뉴에서 기존 가상 스위치를 선택합니다.

 **노트:** ESXi의 가상 스위치를 선택할 때에는 이름에 'VM' 또는 '가상 시스템'이 포함된 스위치만 드롭 다운에 나열됩니다. **Virtual Machine Port Group(가상 시스템 포트 그룹)** 유형의 스위치를 선택해야 ESXi 하이퍼바이저 GUI를 통해 스위치 유형을 확인할 수 있습니다.

5. **Create(생성)**를 클릭합니다.


 **노트:** 가상 네트워크 어댑터를 제거하려면 하이퍼바이저 관리 인터페이스를 사용하십시오.


## VM 작업 시작


VM 작업을 시작하려면 다음을 수행하십시오.

1. **VM Management(VM 관리)** 창으로 이동합니다.

2. 시작할 VM과 연결된 **Start(시작)** 단추를 클릭합니다.

 **노트:** GUI는 시스템의 올바른 상태를 표시하는 데 시간이 오래 걸릴 수 있습니다. 단추를 사용한 후 최대 30초 동안 시작 단추가 비활성 상태로 유지되며, 가상 시스템을 시작할 수 있는 경우에만 시작 단추가 활성화됩니다.

 **노트:** 현재 가상 시스템으로의 내보내기 작업이 실행 중이거나 곧 시작될 예정인 경우에는 시작 단추를 클릭하지 마십시오. **Protected Machines(보호되는 시스템)** 탭 및 **Virtual Standby(가상 대기)** 탭을 확인하여 다음 내보내기 작업의 일정을 확인하십시오. 내보내기 작업이 단기간 내에 예약되어 있는 경우에는 내보내기 작업을 취소 또는 건너뛰거나 가상 시스템을 시작하기 전에 내보내기 작업이 완료될 때까지 기다리십시오. 내보내기 작업이 실행 중일 때 가상 시스템을 시작할 수는 있지만 가상 시스템이 실행 중일 때 시작하면 데이터 내보내기가 실패합니다.


 **노트:** 가상 대기로 유지되는 시스템은 시작하지 않는 것이 좋습니다. 가상 대기 VM은 장애가 있는 보호되는 시스템을 교체할 때 활성화하거나 시작하기 위한 것입니다. 보호되는 시스템이 활성 상태인 경우 VM을 시작하기 전에 먼저 가상 대기를 통해 VM에 대해 대기 중인 내보내기를 중지하거나 일시 중지하십시오.


## VM 작업 중지


VM 작업을 중지하려면 다음을 수행하십시오.

1. **VM Management(VM 관리)** 창으로 이동합니다.

2. 중지할 VM과 연결된 **Stop(중지)** 단추를 클릭합니다.


 **노트:** 현재 가상 시스템이 실행되고 VM을 시작한 후 약 30초 내에 새로 고칠 수 있는 경우에만 중지 단추가 활성화됩니다.

 **노트:** 시작 단추는 VM을 중지한 후 약 30초 내에 활성화됩니다.

 **노트:** 보호된 VM이 복원되면 하이퍼바이저 및 해당 가상 대기에서 VM을 제거하고 복원된 보호되는 시스템에 대한 가상 대기를 다시 생성하십시오. 이렇게 하면 가상 대기 VM이 보호되는 시스템을 정확하게 미러링합니다.

## 롤백 수행

AppAssure에서 롤백은 복구 지점에서 시스템에 대한 볼륨을 복원하는 프로세스입니다.

 **노트:** 보호되는 Linux 시스템에서 명령행 `aamount` 유틸리티를 사용하여 롤백 기능을 수행할 수 있습니다. 자세한 내용은 [명령행을 사용하여 Linux 시스템에 롤백 수행](#)을 참조하십시오.



롤백을 수행하려면 다음을 수행합니다.

1. Core 콘솔에서 다음 중 하나를 수행합니다.

- **Machines(시스템)** 탭을 클릭하고 다음을 수행합니다.
  - a. 보호되는 시스템 목록에서 내보낼 시스템 옆에 있는 확인란을 선택합니다.
  - b. 해당 시스템에 대한 **Actions(작업)** 드롭다운 메뉴에서 **Rollback(롤백)**을 클릭합니다.
  - c. **Rollback – Select Recovery Point(롤백 - 복구 지점 선택)** 대화 상자에서, 내보낼 복구 지점을 선택하고 **Next(다음)**를 클릭합니다.
    - AppAssure Core 콘솔의 왼쪽 탐색 영역에서 롤백할 시스템을 선택합니다. 이렇게 하면 해당 시스템의 **Summary(요약)** 탭이 시작됩니다.
  - d. **Recovery Points(복구 지점)** 탭을 클릭하고 목록에서 복구 지점을 선택합니다.
  - e. 복구 지점의 상세정보를 확장하고 **Rollback(롤백)**을 클릭합니다.
- 2. 다음 표에 설명된 대로 롤백 옵션을 편집합니다.


#### 텍스트 상자 설명


<b>보호되는 시스템</b>	원래 에이전트 시스템을 롤백 대상으로 지정합니다. 소스는 롤백에 사용되는 복구 지점이 생성된 에이전트를 의미합니다.
<b>복구 콘솔 인스턴스</b>	URC 모드에서 부팅된 시스템으로 복구 지점을 복원하려면 사용자 이름과 암호를 입력합니다.

3. **Load Volumes(볼륨 로드)**를 클릭합니다.  
**Volume Mapping(볼륨 매핑)** 대화 상자가 표시됩니다.
  -  **노트:** Core 콘솔은 Linux 볼륨을 자동으로 매핑하지 않습니다. Linux 볼륨을 찾으려면 롤백할 볼륨을 찾으십시오.
4. 롤백을 수행할 볼륨을 선택합니다.
5. **Destination(대상)** 옵션을 사용하여 선택한 볼륨을 롤백할 대상 볼륨을 선택합니다.
6. 다음 옵션을 선택합니다.
  - **Live Recovery(라이브 복구).** 이 옵션을 선택하면 Windows 볼륨의 롤백이 즉시 수행됩니다. 이 옵션은 기본적으로 선택되어 있습니다.
    -  **노트:** Live Recovery(라이브 복구) 옵션은 Linux 볼륨에 사용할 수 없습니다.
  - **Force Dismount(강제 분리).** 이 옵션을 선택하면 롤백을 수행하기 전에 탑재된 모든 복구 지점을 강제로 분리합니다. 이 옵션은 기본적으로 선택되어 있습니다.
7. **Rollback(롤백)**을 클릭합니다.  
 선택한 복구 지점으로 롤백이 시작됩니다.

## 명령행을 사용하여 Linux 시스템에 롤백 수행

롤백은 복구 지점으로부터 시스템의 볼륨을 복원하는 프로세스입니다. AppAssure에서는 명령행 `aamount` 유틸리티를 사용하여 보호된 Linux 시스템의 볼륨에 대한 롤백을 수행할 수 있습니다.

 **주의:** 시스템 또는 루트(/) 볼륨에 대해 롤백을 수행하도록 시도하지 마십시오.

 **노트:** Core 콘솔 내에서 보호된 Windows 시스템에 대해 롤백 기능이 지원됩니다. 자세한 내용은 [롤백 수행](#)을 참조하십시오.

Linux 시스템의 볼륨에 대한 롤백을 수행하려면 다음을 수행하십시오.

1. AppAssure `aamount` 유틸리티를 루트로 실행합니다. 예를 들어, 다음과 같습니다.  
`sudo aamount`
2. AppAssure 탑재 프롬프트에 다음 명령을 입력하여 보호된 시스템을 나열합니다.  
`lm`

3. 메시지가 표시되면 AppAssure Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.

4. 이 서버에 대한 사용자 이름 및 암호와 같은 로그인 자격 증명을 입력합니다.

이 AppAssure 서버가 보호하는 시스템을 보여주는 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 호스트/IP 주소 및 시스템의 ID 번호별로 에이전트 시스템이 나열됩니다(예: 293cc667-44b4-48ab-91d8-44bc74252a4f).

5. 지정된 시스템의 현재 탑재된 복구 지점을 나열하려면 다음 명령을 입력하십시오.

```
lr <machine_line_item_number>
```



**노트:** 또한 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.

해당 시스템에 대한 기본 및 증분 복구 지점을 보여주는 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 날짜/타임스탬프, 볼륨 위치, 복구 지점 크기 및 끝 부분에 복구 지점을 식별하는 시퀀스 번호가 포함되어 있는 볼륨에 대한 ID 번호가 포함됩니다(예: "293cc667-44b4-48ab-91d8-44bc74252a4f:2").

6. 롤백의 복구 지점을 선택하려면 다음 명령을 입력하십시오.

```
r [volume_recovery_point_ID_number] [path]
```

이 명령은 ID로 지정된 볼륨 이미지를 Core에서 지정된 경로로 롤백합니다. 롤백의 경로는 탑재되는 디렉터리가 아닌 장치 파일 설명자의 경로입니다.



**노트:** 또한 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 식별할 수 있습니다.

이러한 경우 `lm` 출력의 에이전트/시스템 라인 번호 뒤에 복구 지점 라인 번호와 볼륨 문자를 사용한 후 경로를 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 에이전트 시스템이 나열되고 2번에 대해 `lr` 명령을 입력한 후 23 복구 지점 볼륨 `b`를 `/mnt/data` 디렉터리에 탑재된 볼륨에 롤백하려는 경우 명령은 `r2 23 b /mnt/data`입니다.



**노트:** /로 롤백할 수는 있지만 라이브 CD로 부팅하는 동안 운영 체제 미설치 복원을 수행하는 경우에만 가능합니다. 자세한 내용은 [Linux 시스템의 운영 체제 미설치 복원 수행](#)을 참조하십시오.

7. 계속할 것인지 묻는 메시지가 표시되면 예를 의미하는 `y`를 입력합니다.

롤백이 진행된 후 상태를 알리는 일련의 메시지가 나타납니다.

8. 롤백이 완료되면 대상이 이전에 보호되고 탑재된 경우 `aamount` 유틸리티가 커널 모듈을 자동으로 탑재하고 롤백된 볼륨에 다시 연결합니다. 그렇지 않은 경우에는 롤백 볼륨을 로컬 디스크에 탑재한 후 파일이 복원되었는지 확인합니다.

예를 들어, `sudo mount` 명령을 사용한 후 `ls` 명령을 사용할 수 있습니다.



**주의:** 보호된 Linux 볼륨을 수동으로 탑재 해제하지 마십시오. 수동으로 탑재를 해제해야 하는 경우에는 볼륨의 탑재를 해제하기 전에 `bsctl -d [path to volume]` 명령을 실행해야 합니다.

이 명령에서 `[path to volume]`은 볼륨의 탑재 지점이 아닌 볼륨의 파일 설명자를 나타냅니다. 이는 `/dev/sda1`과 유사한 형식이어야 합니다.

## Windows 시스템의 운영 체제 미설치 복원 정보

서버가 예상대로 작동되면 수행하도록 구성된 작업이 실행되고 수행됩니다. 서버가 제대로 작동하지 않도록 렌더링하는 치명적인 오류 이벤트가 발생하면 서버를 이전 작동 상태로 복원하기 위해 즉시 단계를 수행해야 합니다. 일반적으로 프로세스에서 시스템을 다시 포맷하고, 운영 체제를 다시 설치하고, 백업을 통해 데이터를 복구하고, 소프트웨어 응용프로그램을 다시 설치합니다.

AppAssure에서는 하드웨어가 유사하거나 다른 Windows 시스템의 운영 체제 미설치 복원(BMR)을 수행하는 기능을 제공합니다. 이 프로세스에서 부팅 CD 이미지 생성, 이미지를 디스크에 굽기, 디스크에서 대상 서버 부팅, 복구 콘솔 인스턴스에 연결, 볼륨 매핑, 복구 시작 및 프로세스 모니터링이 수행됩니다. 운영 체제 미설치 복원이 완료되면 고유한 설정 및 구성에 따라 계속해서 복원된 서버에서 운영 체제 및 소프트웨어 응용프로그램의 로딩 작업을 수행할 수 있습니다.


운영 체제 미설치 복원을 수행하도록 선택할 수 있는 기타 환경으로는 하드웨어 업그레이드 또는 서버 대체가 있습니다.

보호되는 Linux 시스템에서 aamount 명령행 유틸리티를 사용하여 BMR 기능을 사용할 수도 있습니다. 자세한 내용은 [Linux 시스템의 운영 체제 미설치 복원 수행](#)을 참조하십시오.

## Windows 시스템의 운영 체제 미설치 복원 수행을 위한 필수 구성 요소

Windows 시스템의 운영 체제 미설치 복원을 수행하는 프로세스를 시작하기 전에 먼저 다음 조건과 기준을 충족하는지 확인해야 합니다.

- 서버 및 작동 중인 Core의 백업
- 복원할 하드웨어(기존 또는 새 하드웨어인지 및 유사하거나 다른 하드웨어인지 여부)
- 빈 CD 및 CD 굽기 소프트웨어
- VNC 뷰어(선택사항)
- Windows 7 PE(32비트) 호환 드라이버 저장소 및 대상 시스템에 대한 네트워크 어댑터 드라이버
- 저장소 컨트롤러, RAID, AHCI 및 대상 운영 체제의 칩셋 드라이버

 **노트:** 저장소 컨트롤러 드라이버는 다른 하드웨어에 복원을 수행 중인 경우에만 필요합니다.

## Windows 시스템의 운영 체제 미설치 복원 수행을 위한 로드맵


Windows 시스템에 대한 BMR을 수행하려면 다음을 수행하십시오.

1. 부팅 CD를 생성합니다. [부팅 가능 CD ISO 이미지 생성](#)을 참조하십시오.
2. 이미지를 디스크에 굽습니다.
3. 부팅 CD에서 대상 서버를 부팅합니다. [부팅 CD 로드](#)를 참조하십시오.
4. 복구 디스크에 연결합니다.
5. 볼륨을 매핑합니다. [볼륨 매핑](#)을 참조하십시오.
6. 복구를 시작합니다. [AppAssure Core에서 복원 시작](#)을 참조하십시오.
7. 진행 상태를 모니터링합니다. [복구 진행률 보기](#)를 참조하십시오.

### 부팅 가능 CD ISO 이미지 생성

Windows 시스템의 BMR을 수행하려면 Core 콘솔에서 AppAssure 범용 복구 콘솔 인터페이스가 포함된 부팅 가능한 CD/ISO 이미지를 만들어야 합니다. AppAssure 범용 복구 콘솔은 시스템 드라이브나 전체 서버를 AppAssure Core에서 직접 복원할 수 있는 환경입니다.

생성하는 ISO 이미지는 복원되는 시스템에 맞게 조정되어 있기 때문에 올바른 네트워크 및 대용량 저장소 드라이버가 포함되어야 합니다. 부팅 CD를 만드는 시스템과 다른 유형의 하드웨어로 복원하는 경우에는 부팅 CD에 저장소 컨트롤러 및 기타 드라이브를 포함해야 합니다. [부팅 CD에 드라이버 삽입](#)을 참조합니다.

 **노트:** ISO(국제 표준화 기구)는 파일 시스템 표준을 결정하고 설정하는 다양한 국가 기관의 대표자로 구성된 국제 단체입니다. ISO 9660은 데이터 교환을 위해 광 디스크 미디어에 사용되는 파일 시스템 표준으로, Windows와 같은 다양한 운영 체제를 지원합니다. ISO 이미지는 디스크의 모든 섹터와 디스크 파일 시스템에 대한 데이터가 포함되어 있는 보관 파일 또는 디스크 이미지입니다.

부팅 가능 CD ISO 이미지를 생성하려면 다음을 수행하십시오.


1. 복원할 서버가 있는 Core 콘솔에서 **Core**를 선택한 후 **Tools(도구)** 탭을 클릭합니다.
2. **Boot CDs(부팅 CD)**를 클릭합니다.
3. **Actions(작업)**을 선택한 후 **Create Boot ISO(부팅 ISO 생성)**를 클릭합니다.  
**Create Boot CD(부팅 CD 생성)** 대화 상자가 표시됩니다. 대화 상자를 완료하려면 다음 절차를 따르십시오.

### 부팅 CD 파일 이름 지정 및 경로 설정

부팅 CD 파일의 이름을 지정하고 경로를 설정하려면 다음을 수행합니다.


**Create Boot CD(부팅 CD 생성)** 대화 상자에서, Core 서버에 부팅 이미지를 저장할 ISO 경로를 입력합니다.

이미지를 저장할 공유의 공간이 디스크 공간보다 적으면 필요에 따라 경로를 설정할 수 있습니다(예: D:\filename.iso).

 **노트:** 파일 확장명은 .iso여야 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.

### 연결 생성


연결을 생성하려면 다음을 수행하십시오.

1. **Connection Options(연결 옵션)**에서 다음 중 하나를 수행합니다.
  - DHCP(Dynamic Host Configuration Protocol)를 사용하여 동적으로 IP 주소를 가져오려면 **Obtain IP address automatically(자동으로 IP 주소 가져오기)**를 선택합니다.
  - 복구 콘솔의 정적 IP 주소를 지정하려면 **Use the following IP address(다음 IP 주소 사용)**를 선택하고 해당 필드에 IP 주소, 서브넷 마스크, 기본 게이트웨이 및 DNS 서버를 입력합니다. 이러한 필드는 모두 입력해야 합니다.
2. 필요한 경우, **UltraVNC Options(UltraVNC 옵션)**에서 **Add UltraVNC(UltraVNC 추가)**를 선택하고 UltraVNC 옵션을 입력합니다. UltraVNC 설정을 사용하면 복구 콘솔을 사용하는 동안 원격으로 관리할 수 있습니다.  
 **노트:** 이 단계는 선택사항입니다. 복구 콘솔에 대한 원격 액세스가 필요한 경우 UltraVNC를 구성하여 사용해야 합니다. 부팅 CD를 사용하는 동안에는 Microsoft Terminal Service를 사용하여 로그인할 수 없습니다.

### 부팅 CD에 드라이버 삽입

드라이버 추가는 복구 콘솔, 네트워크 어댑터 및 대상 서버의 저장소 간에 쉽게 작동하기 위해 사용됩니다.

다른 종류의 하드웨어로 복원하는 경우 저장소 컨트롤러, RAID, AHCI, 칩셋 및 기타 드라이버를 부팅 CD에 삽입해야 합니다. 이러한 드라이버를 통해 운영 체제가 감지되고 대상 서버에서 모든 장치를 올바르게 작동시킬 수 있습니다.

 **노트:** 부팅 CD에는 Windows 7 PE 32비트 드라이버가 자동으로 포함됩니다.

부팅 CD에 드라이버를 추가하려면 다음을 수행하십시오.

1. 제조업체의 웹 사이트에서 해당 서버용 드라이버를 다운로드하고 압축을 풉니다.
2. 파일 압축 유틸리티(예: Win Zip)를 사용하여 드라이버가 포함된 폴더를 압축합니다.
3. **Create Boot CD(부팅 CD 생성)** 대화 상자의 **Drivers(드라이버)** 창에서 **Add a Driver(드라이버 추가)**를 클릭합니다.
4. 압축된 드라이버 파일을 찾으려면 파일 정리 시스템을 탐색합니다. 파일을 선택하고 **Open(열기)**을 클릭합니다.


**Drivers(드라이버)** 창에 추가된 드라이버가 강조표시된 상태로 나타납니다.

## 부팅 CD 생성

부팅 CD를 생성하려면, **Create Boot CD(부팅 CD 생성)** 화면에서 부팅 CD의 이름 지정, 경로 지정, 연결 생성, 드라이버 삽입(선택사항)을 마친 후 **Create Boot CD(부팅 CD 생성)**를 클릭합니다. 그러면 ISO 이미지가 생성됩니다.

## ISO 이미지 생성 진행률 보기

ISO 이미지 생성 진행률을 보려면 **Events(이벤트)** 탭을 선택한 후 **Tasks(작업)** 아래에서 ISO 이미지 작성에 대한 진행 상태를 모니터할 수 있습니다.

 **노트:** 또한 **Monitor Active Task(진행 중인 작업 모니터)** 대화 상자에서 ISO 이미지 생성에 대한 진행 상태를 확인할 수도 있습니다.


ISO 이미지 생성이 완료되면 **Boot CDs(부팅 CD)** 페이지의 **Tools(도구)** 메뉴에서 해당 이미지를 사용할 수 있습니다.

## ISO 이미지 액세스

ISO 이미지에 액세스하려면 지정한 출력 경로를 탐색하거나 링크를 클릭하여 새 시스템에서 해당 이미지를 로드할 수 있는 위치에 다운로드할 수 있습니다(예: 네트워크 드라이브).

## 부팅 CD 로드

부팅 CD 이미지를 생성한 경우 새로 생성된 부팅 CD를 사용하여 대상 서버를 부팅합니다.


 **노트:** DHCP를 사용하여 부팅 CD를 생성한 경우에는 IP 주소와 암호를 기록해 둡니다.

부팅 CD를 로드하려면 다음을 수행하십시오.

1. 새 서버를 탐색하고 부팅 CD를 로드한 후 시스템을 시작합니다.
2. **Boot from CD-ROM(CD-ROM에서 부팅)** 옵션을 선택합니다. 그러면 다음과 같은 항목이 로드됩니다.
  - Windows 7 PE
  - AppAssure 에이전트 소프트웨어

AppAssure 범용 복구 콘솔이 시작되고 시스템의 IP 주소와 인증 암호가 표시됩니다.


3. **Network Adapter settings(네트워크 어댑터 설정)** 창에 표시된 IP 주소와 **Authentication(인증)** 창에 표시된 인증 암호를 기록합니다. 나중에 데이터를 복구하는 동안 이 정보를 사용하여 콘솔에 다시 로그인합니다.
4. IP 주소를 변경하려면 해당 IP 주소를 선택하고 **Change(변경)**를 클릭합니다.

 **노트:** Create Boot CD(부팅 CD 생성) 대화 상자에서 IP 주소를 지정한 경우 범용 복구 콘솔에서 해당 주소를 사용하고 이를 **Network Adapter settings(네트워크 어댑터 설정)** 화면에 표시합니다.

## 대상 서버에 드라이버 삽입

다른 종류의 하드웨어로 복원하는 경우 저장소 컨트롤러, RAID, AHCI, 칩셋 및 기타 드라이버를 삽입해야 합니다(부팅 CD에 없는 경우). 이러한 드라이버를 통해 운영 체제가 대상 서버에서 모든 장치를 올바르게 작동시킬 수 있습니다.

대상 서버에 필요한 드라이버를 잘 모를 경우, 범용 복구 콘솔에서 System Info(시스템 정보) 탭을 클릭하십시오. 이 탭에는 복원 대상 서버에 필요한 모든 장치 유형 및 시스템 하드웨어가 표시됩니다.


 **노트:** 대상 서버에는 Windows 7 PE 32비트 드라이버가 자동으로 포함됩니다.


대상 서버에 드라이버를 삽입하려면 다음을 수행합니다.

1. 제조업체의 웹 사이트에서 해당 서버용 드라이버를 다운로드하고 압축을 풉니다.
2. 파일 압축 유틸리티(예: Win Zip)를 사용하여 드라이버가 포함된 폴더를 압축하여 대상 서버에 복사합니다.
3. 범용 복구 콘솔에서 **Driver Injection(드라이버 삽입)**을 클릭합니다.
4. 압축된 드라이버 파일을 찾으려면 파일 정리 시스템을 탐색하여 파일을 선택합니다.
5. 3단계에서 **Driver Injection(드라이버 삽입)**을 클릭한 경우 **Add Driver(드라이버 추가)**를 클릭합니다. 3단계에서 **Load driver(드라이버 로드)**를 클릭한 경우 **Open(열기)**를 클릭합니다.  
선택한 드라이버가 삽입되고 대상 서버가 다시 부팅되면 운영 체제에 로드됩니다.

## Core에서 복원 실행

Core에서 복원을 실행하려면 다음을 수행하십시오.

1. 복원 중인 시스템의 NIC가 티밍(연결)되어 있는 경우 네트워크 케이블 중 하나를 제외하고 나머지를 모두 제거합니다.  
 **노트:** AppAssure 복원에서는 티밍된 NIC를 인식하지 않습니다. 프로세스에서 둘 이상의 연결이 활성화되어 있는 경우 사용할 NIC를 확인하지 못합니다.
2. 다시 Core 서버로 이동하여 Core 콘솔을 엽니다.
3. **Machines(시스템)** 탭에서 데이터를 복원할 시스템을 선택합니다.
4. 시스템에 대한 **Actions(작업)** 메뉴를 클릭하고 **Recovery Points(복구 지점)**를 클릭하여 해당 시스템에 대한 모든 복구 지점의 목록을 봅니다.
5. 복원할 복구 지점을 확장한 후 **Rollback(롤백)**을 클릭합니다.
6. **Rollback(롤백)** 대화 상자의 **Choose Destination(대상 선택)** 아래에서 **Recovery Console Instance(복구 콘솔 인스턴스)**를 선택합니다.
7. **Host(호스트)** 및 **Password(암호)** 텍스트 상자에 데이터를 복원할 새 서버에 대한 IP 주소와 인증 암호를 입력합니다.

 **노트:** 호스트 및 암호 값은 이전 작업에서 기록한 자격 증명입니다. 자세한 내용은 [부팅 CD 로딩](#)을 참조하십시오.

8. **Load Volumes(볼륨 로드)**를 클릭하여 대상 볼륨을 새 시스템에 로드합니다.

## 볼륨 매핑

대상 서버의 디스크에 볼륨을 수동 또는 자동으로 매핑하도록 선택할 수 있습니다. 자동 디스크 정렬의 경우, 디스크가 정리되어 다시 파티션되고 모든 데이터가 삭제됩니다. 정렬은 볼륨 나열 순서대로 수행되며 볼륨은



크기 등에 따라 적절히 디스크에 할당됩니다. 여러 볼륨에 하나의 디스크를 사용할 수 있습니다. 드라이브를 수동으로 매핑하는 경우에는 동일한 디스크를 두 번 사용할 수 없습니다.

수동 매핑의 경우, 새 시스템이 올바르게 포맷되어 있어야 복원할 수 있습니다. 자세한 내용은 [Appassure Core에서 복원 시작](#)을 참조하십시오.

볼륨을 매핑하려면 다음을 수행하십시오.

1. 볼륨을 자동으로 매핑하려면 다음을 수행합니다.
  - a. **RollbackURC** 대화 상자에서 **Automatically Map Volumes(자동으로 볼륨 매핑)** 탭을 선택합니다.
  - b. **Disk Mapping(디스크 매핑)** 영역의 **Source Volume(소스 볼륨)**에서 소스 볼륨이 선택되어 있고 해당 볼륨이 그 아래 나열되어 있고 선택되어 있는지 확인합니다.
  - c. 자동으로 매핑되는 대상 디스크가 올바른 대상 볼륨일 경우 **Destination Disk(대상 디스크)**를 선택합니다.
  - d. **Rollback(롤백)**을 클릭하고 3단계를 계속 진행합니다.
2. 볼륨을 수동으로 매핑하려면 다음을 수행합니다.
  - a. **RollbackURC** 대화 상자에서 **Manually Map Volumes(수동으로 볼륨 매핑)** 탭을 선택합니다.
  - b. **Volume Mapping(볼륨 매핑)** 영역의 **Source Volume(소스 볼륨)**에서 소스 볼륨이 선택되어 있고 해당 볼륨이 그 아래 나열되어 있고 선택되어 있는지 확인합니다.
  - c. **Destination(대상)**의 드롭다운 메뉴에서, 선택한 복원 지점의 운영 체제 미설치 복원을 수행할 대상 볼륨인 대상을 선택하고 **Rollback(롤백)**을 클릭합니다.
3. **RollbackURC** 확인 대화 상자에서, 복구 지점의 소스 매핑과 롤백의 대상 볼륨을 검토합니다. 롤백을 수행하려면 **Begin Rollback(롤백 시작)**을 클릭합니다.



**경고:** **Begin Rollback(롤백 시작)**을 선택하면 대상 드라이브에 있는 기존의 모든 파티션과 데이터가 영구적으로 제거되며, 운영 체제 및 모든 데이터를 비롯하여 선택한 복구 지점의 내용으로 대체됩니다.

## 복구 진행률 보기

복구 진행률을 보려면 다음을 수행합니다.

1. 롤백 프로세스를 시작하면 롤백 작업이 시작되었음을 보여주는 **Active Task(진행 중인 작업)** 대화 상자가 표시됩니다.



**노트:** 이 **Active Task(진행 중인 작업)** 대화 상자가 표시되어도 작업이 성공적으로 완료된다는 의미는 아닙니다.

2. 롤백 작업 진행 상태를 모니터링하려면, **Active Task(진행 중인 작업)** 대화 상자에서 **Open Monitor Window(모니터 창 열기)**를 클릭합니다. **Monitor Open Task(진행 중인 작업 모니터링)** 창에서 복구 상태, 시작 및 종료 시간을 볼 수 있습니다.



**노트:** **Active Task(진행 중인 작업)** 대화 상자에서 소스 시스템의 복구 지점으로 되돌아 가려면 **Close(닫기)**를 클릭합니다.

## 복원된 대상 서버 시작

복원된 대상 서버를 시작하려면 다음을 수행합니다.

1. 대상 서버를 다시 탐색한 후 **AppAssure Universal Recovery Console(AppAssure 범용 복구 콘솔)** 인터페이스에서 **Reboot(재부팅)**를 클릭하여 시스템을 시작합니다.
2. Windows를 정상적으로 시작하도록 지정합니다.
3. 시스템에 로그인합니다.  
시스템이 운영 체제 미설치 복원 이전의 상태로 복원됩니다.

## 시작 문제 복구

다른 종류의 하드웨어로 복원하는 경우 스토리지 컨트롤러, RAID, AHCI, 칩셋 및 기타 드라이버를 삽입해야 합니다(부팅 CD에 없는 경우). 이러한 드라이버를 통해 운영 체제가 대상 서버에서 모든 장치를 올바르게 작동시킬 수 있습니다.

시작 문제를 복구하려면 다음을 수행합니다.

1. 복원된 대상 서버를 시작할 때 문제가 발생하면 부팅 CD를 다시 로드하여 범용 복구 콘솔을 엽니다.
2. 범용 복구 콘솔에서 **Driver Injection(드라이버 삽입)**을 클릭합니다.
3. Driver Injection(드라이버 삽입) 대화 상자에서 **Repair Boot Problems(부팅 문제 복구)**를 클릭합니다.  
대상 서버 부팅 레코드의 시작 매개변수가 자동으로 복구됩니다.
4. 범용 복구 콘솔에서 **Reboot(재부팅)**를 클릭합니다.

## Linux 시스템의 운영 체제 미설치 복원 수행

시스템 볼륨의 롤백을 포함하여 Linux 시스템의 운영 체제 미설치 복원(BMR)을 수행할 수 있습니다.

AppAssure 명령행 유틸리티인 `aamount`를 사용하여 부팅 볼륨 기본 이미지로 롤백합니다. Linux 시스템의 BMR을 수행하기 전에 먼저 다음을 수행해야 합니다.

- AppAssure 지원 센터에서 부팅 가능한 버전의 Linux가 포함되어 있는 BMR 라이브 CD 파일을 가져옵니다.



**노트:** <https://licenseportal.com>의 라이선스 포털에서 Linux 라이브 CD 파일을 다운로드할 수도 있습니다.


- 소스 볼륨을 포함할 대상 파티션을 대상 시스템에 만들 수 있는 충분한 공간이 하드 드라이브에 있어야 합니다. 모든 대상 파티션의 크기는 원래 소스 파티션과 같거나 커야 합니다.
- 롤백 경로가 장치 파일 설명자 경로인지 확인합니다. 장치 파일 설명자의 경로를 식별하려면 터미널 창에서 `fdisk` 명령을 사용하십시오.



**노트:** AppAssure 명령을 사용하기 전에 Screen Utility를 설치할 수 있습니다. Screen Utility를 사용하면 화면을 스크롤하여 규모가 큰 데이터(예: 복구 지점 목록)를 볼 수 있습니다. Screen Utility 설치에 대한 내용은 [Screen Utility 설치](#)를 참조하십시오.

Linux 시스템의 운영 체제 미설치 복원을 수행하려면 다음을 수행하십시오.


1. AppAssure에서 받은 라이브 CD 파일을 사용하여 Linux 시스템을 부팅하고 터미널 창을 엽니다.
2. 필요한 경우 새 디스크 파티션을 생성합니다. 예를 들어, `fdisk` 명령을 루트로 실행하고 `a` 명령을 사용하여 이 파티션을 부팅 가능하도록 지정합니다.
3. AppAssure `aamount` 유틸리티를 루트로 실행합니다. 예를 들어, 다음과 같습니다.  
`sudo aamount`
4. AppAssure 탐색 프롬프트에 다음 명령을 입력하여 보호된 시스템을 나열합니다.  
`lm`
5. 메시지가 표시되면 AppAssure Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.
6. 이 서버에 대한 사용자 이름 및 암호와 같은 로그인 자격 증명을 입력합니다.  
이 AppAssure Core 서버에 의해 보호되는 시스템을 보여주는 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 호스트/IP 주소 및 시스템의 ID 번호별로 시스템이 나열됩니다(예:  
`293cc667-44b4-48ab-91d8-44bc74252a4f`).
7. 복원할 시스템의 현재 탑재된 복구 지점을 나열하려면 다음 명령을 입력하십시오.  
`lr <machine_line_item_number>`

 **노트:** 또한 이 명령에 라인 항목 번호 대신 시스템 ID 번호를 입력할 수도 있습니다.


해당 시스템에 대한 기본 및 증분 복구 지점을 보여주는 목록이 표시됩니다. 이 목록에는 라인 항목 번호, 날짜/타임스탬프, 볼륨 위치, 복구 지점 크기 및 끝 부분에 복구 지점을 식별하는 시퀀스 번호가 포함되어 있는 볼륨에 대한 ID 번호가 포함됩니다(예: "293cc667-44b4-48ab-91d8-44bc74252a4f:2").

8. 롤백에 사용할 기본 이미지 복구 지점을 선택하려면 다음 명령을 입력하십시오.

```
r <volume_base_image_recovery_point_ID_number> <path>
```

 **주의:** 시스템 볼륨이 탑재되어 있지 않은지 확인해야 합니다.


이 명령은 ID로 지정된 볼륨 이미지를 Core에서 지정된 경로로 롤백합니다. 롤백의 경로는 탑재되는 디렉터리가 아닌 장치 파일 설명자의 경로입니다.


 **노트:** 또한 명령에 복구 지점 ID 번호 대신 라인 번호를 지정하여 복구 지점을 식별할 수 있습니다. lm 출력의 에이전트/시스템 라인 번호 뒤에 복구 지점 라인 번호와 볼륨 문자를 사용한 후 경로를 사용합니다(예: `r <machine_line_item_number> <base_image_recovery_point_line_number> <volume_letter> <path>`). 이 명령에서 `<path>`는 실제 볼륨에 대한 파일 설명자입니다.

9. 계속할 것인지 묻는 메시지가 표시되면 예를 의미하는 y를 입력합니다.

롤백이 진행된 후 상태를 알리는 일련의 메시지가 나타납니다.

10. 롤백이 완료되면 필요한 경우 기본 부팅 레코드를 복원된 부팅 로더로 업데이트합니다.

 **노트:** 이 디스크가 새 디스크인 경우에만 부팅 로더 복구 또는 설정을 수행해야 합니다. 동일한 디스크에 대한 단순 롤백인 경우에는 부팅 로더를 설정할 필요가 없습니다.

 **주의:** 보호되는 Linux 볼륨을 수동으로 탑재 해제하지 마십시오. 수동으로 탑재를 해제해야 하는 경우에는 볼륨의 탑재를 해제하기 전에 `bsctl -d <path to volume>` 명령을 실행해야 합니다.

이 명령에서 `<path to volume>`은 볼륨의 탑재 지점이 아닌 볼륨의 파일 설명자를 나타냅니다. 이는 `/dev/sda1`과 유사한 형식이어야 합니다.

## Screen Utility 설치

AppAssure 명령을 사용하기 전에 Screen Utility를 설치할 수 있습니다. Screen Utility를 사용하면 화면을 스크롤하여 규모가 큰 데이터(예: 복구 지점 목록)를 볼 수 있습니다.


Screen Utility를 설치하려면 다음을 수행합니다.

1. 라이브 CD 파일을 사용하여 Linux 시스템을 시작합니다.  
터미널 창이 열립니다.
2. 다음 명령을 입력합니다. `sudo apt-get install screen`.
3. Screen Utility를 시작하려면 명령 프롬프트에 `screen`을 입력합니다.

## Linux 시스템에서 부팅 가능한 파티션 생성

명령행을 사용하여 Linux 시스템에서 부팅 가능한 파티션을 생성하려면 다음을 수행합니다.

1. `sudo bsctl --attach-to-device /dev/<restored volume>` 명령을 루트로 사용하여 `bsctl` 유틸리티를 통해 모든 장치에 추가합니다.

 **노트:** 복원된 각 볼륨에 대해 이 단계를 반복합니다.

2. 다음 명령을 사용하여 복원된 각 볼륨을 탑재합니다.

```
mount /dev/<restored volume> /mnt
```

```
mount /dev/<restored volume> /mnt
```



**노트:** 일부 시스템 구성에는 루트 볼륨에 속하는 부팅 디렉터리가 포함될 수 있습니다.

3. 다음 명령을 사용하여 복원된 각 볼륨의 스냅샷 메타데이터를 탑재합니다.

```
sudo bsctl --reset-bitmap-store /dev/<restored volume>
```

```
sudo bsctl --map-bitmap-store /dev/<restored volume>
```

4. `blkid` 명령 또는 `ll /dev/disk/by-uuid` 명령을 사용하여 UUID(Universally Unique Identifier)에 새 볼륨이 포함되어 있는지 확인합니다.
5. `/etc/fstab`에 루트 및 부팅 볼륨에 사용되는 올바른 UUID가 포함되어 있는지 확인합니다.
6. 다음 명령을 사용하여 GRUB(Grand Unified Bootloader)를 설치합니다.

```
mount --bind /dev/ /mnt/dev
```

```
mount --bind /proc/ /mnt/proc
```

```
chroot/mnt/bin/bash
```

```
grub-install/dev/sda
```

7. `/boot/grub/grub.conf` 파일에 루트 볼륨에 사용되는 올바른 UUID가 포함되어 있는지 확인하거나, 텍스트 편집기를 사용하여 필요에 따라 업데이트합니다.
8. CD-ROM 드라이브에서 라이브 CD를 제거하고 Linux 시스템을 다시 시작합니다.

## 이벤트 및 경고 보기

이벤트 및 경고를 보려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔의 Machines(시스템) 탭에서 이벤트를 볼 시스템의 하이퍼링크를 클릭합니다.
  - Core 콘솔의 왼쪽 **탐색** 영역에서 이벤트를 볼 시스템을 선택합니다.
2. **Events(이벤트)** 탭을 클릭합니다.  
현재 작업에 대한 모든 이벤트와 경고의 로그가 나타납니다.

# 서버 클러스터 보호

## 서버 클러스터 보호 정보

AppAssure에서는 서버 클러스터 보호가 개별 클러스터 노드(즉, 클러스터의 개별 시스템)에 설치된 AppAssure 에이전트 및 Core와 연결되어 있어, 하나의 복합 시스템인 것처럼 에이전트를 보호합니다.

클러스터를 보호하고 관리하도록 Core를 쉽게 구성할 수 있습니다. Core 콘솔에서 클러스터가 관련 노드를 포함하는 '컨테이너' 역할을 수행하는 별도의 엔터티로 구성되어 있습니다. 예를 들어, 왼쪽 탐색 영역에서 탐색 트리의 맨 위에 Core가 나열되고 클러스터가 Core 아래에 나열되며 AppAssure 에이전트가 설치된 관련 개별 노드가 포함되어 있습니다.

Core 및 클러스터 수준에서 관련 노드의 목록 및 공유 볼륨과 같은 클러스터에 대한 정보를 볼 수 있습니다. Core 콘솔의 시스템 탭에 클러스터가 표시되고, 표시/숨기기를 사용해 보기를 전환하여 클러스터에 포함된 노드를 봅니다. 또한 클러스터 수준에서 클러스터에 있는 노드에 대한 해당 Exchange 및 SQL 클러스터 메타데이터를 볼 수 있습니다. 해당 클러스터의 공유 볼륨 및 전체 클러스터에 대한 설정을 지정하거나 클러스터의 개별 노드(시스템)를 탐색하여 해당 노드 및 연결된 로컬 볼륨에 대한 설정만 구성할 수 있습니다.

## 지원되는 응용프로그램 및 클러스터 유형

클러스터를 적절하게 보호하려면 클러스터의 노드 또는 각 시스템에 AppAssure 에이전트 소프트웨어가 설치되어 있어야 합니다. AppAssure에서는 다음 표에 나열된 응용프로그램 버전과 클러스터 구성을 지원합니다.

**표 4. 지원되는 응용프로그램 및 클러스터 유형**

응용프로그램	응용프로그램 버전 및 관련 클러스터 구성	Windows 장애 조치 클러스터
Microsoft Exchange	2007 SCC(단일 복사본 클러스터)	2003, 2008, 2008 R2
	2007 CCR(클러스터 연속 복제)	
	2010 DAG(데이터베이스 사용 가능 그룹)	2008, 2008 R2
Microsoft SQL	2005, 2008, 2008 R2 SCC(단일 복사본 클러스터)	2003, 2008, 2008 R2
	2012 SCC(단일 복사본 클러스터)	2008, 2008 R2, 2012

지원되는 디스크 유형은 다음과 같습니다.


- 2TB보다 큰 GUID 파티션 테이블(GPT) 디스크
- 동적 디스크
- 기본 디스크

지원되는 탑재 유형은 다음과 같습니다.

- 드라이브 문자로 연결되는 공유 드라이브(예: D:)
- 단일 실제 디스크의 단순 동적 볼륨(스트라이핑, 미러링 또는 스펠되지 않은 볼륨)
- 탑재 지점으로 연결되는 공유 드라이브

## 클러스터 보호

이 항목에서는 AppAssure에서 보호할 클러스터를 추가하는 방법에 대해 설명합니다. 보호할 클러스터를 추가할 때 클러스터, 클러스터 응용프로그램 또는 AppAssure 에이전트가 포함되어 있는 클러스터 노드나 시스템 중 하나의 호스트 이름이나 IP 주소를 지정해야 합니다.

 **노트:** 리포지토리는 보호된 노드에서 캡처되는 데이터의 스냅샷을 저장하는 데 사용됩니다. 클러스터에서 데이터 보호를 시작하기 전에 AppAssure Core와 연결되는 리포지토리를 하나 이상 설정하십시오.


리포지토리 설정에 대한 자세한 내용은 [리포지토리 정보](#)를 참조하십시오.

클러스터를 보호하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Home(홈)** 탭을 탐색한 후 **Protect Cluster(클러스터 보호)** 단추를 클릭합니다.
  - Core 콘솔의 **Machines(시스템)** 탭에서 **Actions(작업)**을 클릭한 후 **Protect Cluster(클러스터 보호)**를 클릭합니다.
2. **Connect to Cluster(클러스터에 연결)** 대화 상자에 다음 정보를 입력합니다.


### 텍스트 상자 설명

**호스트** 클러스터, 클러스터 응용프로그램 또는 보호할 클러스터 노드 중 하나의 호스트 이름이나 IP 주소입니다.

 **노트:** 노드 중 하나의 IP 주소를 사용하는 경우 이 노드에 AppAssure 에이전트가 설치되어 있고 시작되어야 합니다.


**포트** AppAssure Core가 에이전트와 통신하는 시스템의 포트 번호입니다.

**사용자 이름** 이 시스템에 연결하는 데 사용되는 도메인 관리자의 사용자 이름입니다(예: **domain\_name\administrator** 또는 **administrator@domain\_name.com**).

 **노트:** 도메인 이름은 필수입니다. 로컬 관리자 사용자 이름을 사용하는 경우에는 클러스터에 연결할 수 없습니다.

**암호** 이 시스템에 연결하는 데 사용되는 암호입니다.

3. **Protect Cluster(클러스터 보호)** 대화 상자에서 이 클러스터에 대한 리포지토리를 선택합니다.
4. 기본 설정을 기반으로 클러스터를 보호하려면 기본 보호를 적용할 노드를 선택하고 **Protect(보호)**를 클릭합니다.

 **노트:** 기본 설정을 사용하면 60분마다 모든 볼륨이 보호됩니다.

5. 클러스터에 대한 사용자 지정 설정을 입력(예: 공유 볼륨에 대한 보호 일정 사용자 지정)하려면 다음을 수행합니다.
  - a. **Settings(설정)**를 클릭합니다.
  - b. **Volumes(볼륨)** 대화 상자에서 보호할 볼륨을 선택하고 **Edit(편집)**를 클릭합니다.
  - c. **Protection Schedule(보호 일정)** 대화 상자에서 다음 표에 설명된 대로 데이터를 보호할 일정 옵션 중 하나를 선택합니다.

## 텍스트 상자

## 설명

### 간격

다음에서 선택할 수 있습니다.

- **Weekday(평일)** - 특정 간격으로 데이터를 보호하려면 **Interval(간격)**을 선택한 후 다음을 수행합니다.
  - 최대 사용량 시간 동안 데이터를 보호할 시기를 사용자 지정하려면 **Start Time(시작 시간)**, **End Time(종료 시간)** 및 **Interval(간격)**을 지정할 수 있습니다.
  - 사용량이 적을 때 데이터를 보호하려면 **Protect during off-peak times(사용량이 적을 때 보호)** 확인란을 선택한 후 보호할 간격을 선택합니다.
- **Weekends(주말)** - 주말 동안에도 데이터를 보호하려면 **Protect during weekends(주말 동안 보호)** 확인란을 선택한 후 간격을 선택합니다.

### 매일

데이터를 매일 보호하려면 **Daily(매일)** 옵션을 선택한 후 **Protection Time(보호 시간)**에 대해 데이터 보호를 시작할 시간을 선택합니다.

### 보호 안 함

이 볼륨에서 보호를 제거하려면 **No Protection(보호 안 함)** 옵션을 선택합니다.

6. 필요한 내용을 모두 변경하면 **Save(저장)**를 클릭합니다.
7. 클러스터에 있는 노드의 사용자 지정 설정을 입력하고 노드를 선택한 다음 노드 옆에 있는 **Settings(설정)** 링크를 클릭합니다.
  - 5단계를 반복하여 보호 일정을 편집합니다.

노드 사용자 지정에 대한 자세한 내용은 [클러스터의 노드 보호](#)를 참조하십시오.

8. **Protect Cluster(클러스터 보호)** 대화 상자에서 **Protect(보호)**를 클릭합니다.

## 클러스터의 노드 보호

이 항목에서는 AppAssure 에이전트가 설치되어 있는 클러스터 노드 또는 시스템에서 데이터를 보호하는 방법에 대해 설명합니다. 보호를 추가할 때 사용 가능한 노드의 목록에서 노드를 선택하고 도메인 관리자의 호스트 이름과 사용자 이름 및 암호를 지정해야 합니다.

클러스터에서 노드를 보호하려면 다음을 수행하십시오.

1. 클러스터를 추가한 후 해당 클러스터를 탐색하고 **Machines(시스템)** 탭을 클릭합니다.
2. **Actions(작업)** 메뉴를 클릭한 후 **Protect Cluster Node(클러스터 노드 보호)**를 클릭합니다.
3. **Protect Cluster Node(클러스터 노드 보호)** 대화 상자에서 다음 정보를 적절하게 선택하거나 입력한 후 **Connect(연결)**를 클릭하여 시스템 또는 노드를 추가합니다.

## 텍스트 상자

## 설명

### 호스트

클러스터에서 보호할 수 있는 노드의 드롭다운 목록입니다.

### 포트

Core가 노드의 에이전트와 통신하는 포트 번호입니다.


### 사용자 이름

이 노드에 연결하는 데 사용되는 도메인 관리자의 사용자 이름입니다(예: **example\_domain\administrator** 또는 **administrator@example\_domain.com**).

### 암호

이 시스템에 연결하는 데 사용되는 암호입니다.

4. **Protect(보호)**를 클릭하여 기본 보호 설정으로 이 시스템의 보호를 시작합니다.

 **노트:** 기본 설정을 사용하면 60분마다 시스템의 모든 볼륨이 보호됩니다.


- 이 시스템에 대한 사용자 지정 설정을 입력(예: 표시 이름 변경, 암호화 추가 또는 보호 일정 사용자 지정)하려면 **Show Advanced Options(고급 옵션 표시)**을 클릭합니다.
- 필요에 따라 아래에 설명된 대로 다음 설정을 편집합니다.

#### 텍스트 상자      설명

**표시 이름**      Core 콘솔에 표시할 시스템에 대한 새 이름을 입력합니다.

**리포지토리**      Core에서 이 시스템의 데이터를 저장할 리포지토리를 선택합니다.

**암호화**      리포지토리에 저장되는 이 시스템의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.

 **노트:** 리포지토리에 대한 암호화 설정은 Core 콘솔의 **Configuration(구성)** 탭에 정의되어 있습니다.

**일정**      다음 옵션 중 하나를 선택합니다.

- 기본 일정을 사용하여 모든 볼륨을 보호합니다.
- 사용자 지정 일정이 포함된 특정 볼륨을 보호합니다. 그런 다음 **Volumes(볼륨)** 아래에서 볼륨을 선택하고 **Edit(편집)**를 클릭합니다. 사용자 지정 간격 설정에 대한 자세한 내용은 [클러스터 보호](#)를 참조하십시오.

## 클러스터 노드 설정 수정 프로세스

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.

- 다음 중 하나를 수행합니다.
  - 수정할 노드가 포함되어 있는 클러스터를 탐색하고 **Machines(시스템)** 탭을 클릭한 후 수정할 시스템 또는 노드를 선택합니다.
  - 또는 **Navigation(탐색)** 창의 **Cluster(클러스터)** 머릿글 아래에서 수정할 시스템 또는 노드를 선택합니다.
- 구성 설정을 수정하고 보려면 [구성 설정 보기 및 수정](#)을 참조하십시오.
- 시스템 이벤트에 대한 알림 그룹을 구성하려면 [시스템 이벤트에 대한 알림 그룹 구성](#)을 참조하십시오.
- 보존 정책 설정을 사용자 지정하려면 [보존 정책 설정 사용자 지정](#)을 참조하십시오.
- 보호 일정을 수정하려면 [보호 일정 수정](#)을 참조하십시오.
- 전송 설정을 수정하려면 [전송 설정 수정](#)을 참조하십시오.

## 클러스터 설정 구성을 위한 로드맵

클러스터 설정 구성을 위한 로드맵에서는 다음 작업이 수행됩니다.

- 클러스터 설정 수정
- 클러스터 이벤트 알림 구성
- 클러스터 보존 정책 수정
- 클러스터 보호 일정 수정



- 클러스터 전송 설정 수정

## 클러스터 설정 수정

클러스터를 추가한 후 기본 설정(예: 표시 이름) 및 보호 설정(예: 보호 일정, 볼륨 추가 또는 제거, 보호 일시 중지) 등을 쉽게 수정할 수 있습니다.

클러스터 설정을 수정하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core Console(Core 콘솔)에서 **Machines(시스템)** 탭을 클릭하고 수정하기 원하는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 수정하기 원하는 클러스터를 선택합니다.
2. **Configuration(구성)** 탭을 클릭합니다.  
**Settings(설정)** 페이지가 나타납니다.
3. **Edit(편집)**를 클릭하여 다음에 설명된 대로 이 페이지에서 클러스터에 대한 설정을 수정합니다.

### 텍스트 상자 설명

**표시 이름** 클러스터의 표시 이름을 입력합니다.  
이 클러스터의 이름이 Core 콘솔에 표시됩니다. 기본적으로 이는 클러스터의 호스트 이름입니다. 필요한 경우 이 이름을 더욱 설명적으로 변경할 수 있습니다.

**호스트 이름** 이 설정은 클러스터의 호스트 이름을 나타냅니다. 이는 정보 제공을 위해서만 여기에 나열되며 수정할 수 없습니다.

**리포지토리** 클러스터와 연결된 Core 리포지토리를 입력합니다.



**노트:** 이 클러스터에 대한 스냅샷을 이미 만든 경우 이 설정이 정보 제공을 위해서만 여기에 나열되며 수정할 수 없습니다.

**암호화 키** 필요한 경우 암호화 키를 입력하고 선택합니다.  
이는 리포지토리에 저장되는 이 클러스터의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.

## 클러스터 이벤트 알림 구성

알림 그룹을 생성하여 클러스터에 대한 시스템 이벤트가 보고되는 방법을 구성할 수 있습니다. 이러한 이벤트는 시스템 알림 또는 오류일 수 있습니다.

클러스터 이벤트 알림을 구성하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core Console(Core 콘솔)에서 **Machines(시스템)** 탭을 클릭하고 수정하기 원하는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 수정하기 원하는 클러스터를 선택합니다.
2. **Configuration(구성)** 탭을 클릭한 후 **Events(이벤트)**를 클릭합니다.
3. 다음 표에 설명되어 있는 옵션 중 하나를 선택합니다.

## 텍스트 상자      설명

**Core 경고 설정 사용** 이 옵션을 선택하면 연결된 Core에서 사용하는 설정이 사용됩니다.

- a. **Apply(적용)**를 클릭합니다.
- b. 5단계를 완료합니다.

**사용자 지정 경고 설정 사용** 이 옵션을 선택하면 사용자 지정 설정을 구성할 수 있습니다. 계속해서 4단계를 수행합니다.

4. **Custom alert settings(사용자 지정 경고 설정)**을 선택하는 경우 **Add Group(그룹 추가)**을 클릭하여 시스템 이벤트의 목록을 보내기 위한 새 알림 그룹을 추가합니다.

**Add Notification Group(알림 그룹 추가)** 대화 상자가 열립니다.

5. 다음 표에 설명된 대로 알림 옵션을 추가합니다.

## 텍스트 상자      설명

**이름** 알림 그룹의 이름을 입력합니다.

**설명** 알림 그룹에 대한 설명을 입력합니다.

**이벤트 활성화** 알림에 대한 이벤트를 선택합니다(예: 클러스터). 유형별로 선택할 수도 있습니다.

- 오류
- 경고
- 정보



**노트:** 유형별로 선택하도록 선택하면 기본적으로 적절한 이벤트가 자동으로 활성화됩니다. 예를 들어, 경고를 선택하면 연결 기능, 작업, 라이선싱, 아카이브, Core 서비스, 내보내기, 보호, 복제 및 롤백 이벤트가 활성화됩니다.

**알림 옵션** 알림을 처리할 방법을 지정하는 방법을 선택합니다. 다음 옵션을 선택할 수 있습니다.

- **Notify by Email(전자 메일로 알림)** - 보낸 사람, 참조 및 숨은 참조 텍스트 상자에서 이벤트를 보낼 전자 메일 주소를 지정합니다.
- **Notify by Windows Event log(Windows 이벤트 로그로 알림)** - Windows 이벤트 로그가 알림을 제어합니다.
- **Notify by syslogd(시스템 로그로 알림)** - 이벤트를 보낼 호스트 이름과 포트를 지정합니다.

6. **OK(확인)**를 클릭하여 변경 내용을 저장한 후 **Apply(적용)**를 클릭합니다.

7. 기존 알림 그룹을 편집하려면 목록에서 알림 그룹 옆에 있는 **Edit(편집)**를 클릭합니다.

설정을 편집할 수 있도록 **Edit Notification Group(알림 그룹 편집)** 대화 상자가 나타납니다.

## 클러스터 보존 정책 수정

클러스터에 대한 보존 정책이 클러스터의 공유 볼륨에 대한 복구 지점이 리포지토리에 보관되는 기간을 지정합니다. 보존 정책은 장기간 백업 스냅샷을 보존하는 데 사용되며, 이러한 백업 스냅샷을 관리하는 데 도움을 줍니다. 오래된 백업을 에이징 및 삭제할 때 유용한 롤업 프로세스에서 보존 정책이 강제 적용됩니다.

1. 다음 중 하나를 수행합니다.


- **Core 콘솔**에서 **Machines(시스템)** 탭을 클릭하고 수정할 클러스터를 선택합니다.

- 왼쪽 탐색 영역에서 수정하기 원하는 클러스터를 선택합니다.
2. **Configuration(구성)** 탭을 클릭한 후 **Retention Policy(보존 정책)**를 클릭합니다.
  3. 다음 표에 있는 옵션 중 하나를 선택합니다.

텍스트 상자	설명
--------	----

<b>Core 기본 보존 정책 사용</b>	이 옵션을 선택하면 연결된 Core에서 사용하는 설정이 사용됩니다. <b>Apply(적용)</b> 를 클릭하십시오.
-------------------------	--

<b>사용자 지정 보존 정책 사용</b>	사용자 지정 설정을 구성할 수 있습니다.
------------------------	------------------------

 **노트:** **Custom alert settings(사용자 지정 경고 설정)**를 선택한 경우, [보존 정책 설정 사용자 지정](#)에 설명된 대로 4단계를 시작으로 사용자 지정 보존 정책 설정에 대한 지침을 따르십시오.

## 클러스터 보호 일정 수정


클러스터에 공유 볼륨이 있는 경우에만 보호 일정을 수정할 수 있습니다.

클러스터 보호 일정을 수정하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core Console(Core 콘솔)에서 **Machines(시스템)** 탭을 클릭하고 수정하기 원하는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 수정하기 원하는 클러스터를 선택합니다.
2. **Configuration(구성)** 탭을 클릭하고 **Protection Settings(보호 설정)**을 클릭합니다.
3. [보호 일정 수정](#)에 설명된 대로 2단계를 시작으로 보호 설정 수정에 대한 지침을 따릅니다.

## 클러스터 전송 설정 수정

AppAssure에서 설정을 수정하여 보호된 클러스터에 대한 데이터 전송 프로세스를 관리할 수 있습니다.

 **노트:** 클러스터에 공유 볼륨이 있는 경우에만 클러스터 전송 설정을 수정할 수 있습니다.

AppAssure에는 다음과 같은 세 가지 전송 유형이 있습니다.

텍스트 상자	설명
--------	----

<b>스냅샷</b>	보호된 클러스터에 데이터를 백업합니다.
------------	-----------------------

<b>VM 내보내기</b>	클러스터를 보호하도록 정의된 일정에 따라 지정된 대로 백업 정보와 매개변수가 모두 포함된 가상 시스템을 생성합니다.
----------------	--

<b>롤백</b>	보호된 클러스터에 대한 백업 정보를 복원합니다.
-----------	----------------------------

클러스터 전송 설정을 수정하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core Console(Core 콘솔)에서 **Machines(시스템)** 탭을 클릭하고 수정하기 원하는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 수정하기 원하는 클러스터를 선택합니다.
2. **Configuration(구성)** 탭을 클릭하고 **Transfer Settings(전송 설정)**을 클릭합니다.
3. [보호 일정 수정](#)에 설명된 대로 2단계를 시작으로 보호 설정을 수정합니다.

## 보호된 클러스터 노드를 에이전트로 변환

AppAssure에서는 보호된 클러스터 노드가 Core에서 계속해서 관리되지만 더 이상 클러스터에 속하지 않도록 해당 클러스터 노드를 AppAssure 에이전트로 변환할 수 있습니다. 예를 들어, 클러스터에서 클러스터 노드를 제거하지만 계속해서 보호된 상태로 유지하려는 경우 유용합니다.

보호된 클러스터 노드를 에이전트로 변환하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭하고 변환하기 원하는 시스템이 포함되어 있는 클러스터를 선택합니다. 클러스터의 **Machines(시스템)** 탭을 클릭합니다.
  - 왼쪽 탐색 영역에서 변환하기 원하는 시스템이 포함되어 있는 클러스터를 선택한 후 **Machines(시스템)** 탭을 클릭합니다.
2. 변환할 시스템을 선택하고 Machines(시스템) 탭의 맨 위에 있는 **Actions(작업)** 드롭다운 메뉴를 클릭한 후 **Convert to Agent(에이전트로 변환)**를 클릭합니다.
3. 시스템을 클러스터에 다시 추가하려면 시스템을 선택한 후 **Summary(요약)** 탭, **Actions(작업)** 메뉴 및 **Convert to Node(노드로 변환)**를 차례로 클릭합니다.

## 서버 클러스터 정보 보기

### 클러스터 시스템 정보 보기

클러스터 시스템 정보를 보려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 보려는 클러스터를 선택합니다.
2. **Tools(도구)** 탭을 클릭합니다.

이름, 연관된 상태 및 Windows 버전과 함께 포함된 노드, 네트워크 인터페이스 정보 및 볼륨 용량 정보와 같이 클러스터에 대한 시스템 상세정보를 보여주는 **System Information(시스템 정보)** 페이지가 표시됩니다.

### 클러스터 이벤트 및 경고 보기

클러스터의 개별 시스템 또는 노드에 대한 이벤트 및 경고 보기에 대한 자세한 내용은 [이벤트 및 경고 보기](#)를 참조하십시오.

클러스터 이벤트 및 경고를 보려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역의 **Clusters(클러스터)**에서 보려는 클러스터를 선택합니다.
2. **Events(이벤트)** 탭을 클릭합니다.

로그에 현재 작업에 대한 모든 이벤트와 클러스터에 대한 경고가 표시됩니다.
3. **Active(활성)**, **Complete(완료)** 또는 **Failed(실패)** 확인란을 적절하게 선택하거나 지워 이벤트 목록을 필터링할 수 있습니다.
4. **Alerts(경고)** 테이블에서 **Dismiss All(모두 해제)**을 클릭하여 목록에 있는 경고를 모두 해제합니다.


## 요약 정보 보기

요약 정보를 보려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역의 **Clusters(클러스터)**에서 보려는 클러스터를 선택합니다.
2. **Summary(요약)** 탭에서 클러스터 이름, 클러스터 유형, 쿼럼 유형(해당되는 경우) 및 쿼럼 경로(해당되는 경우)와 같은 정보를 볼 수 있습니다.  
또한 이 탭에서 크기 및 보호 일정을 포함하여 이 클러스터의 볼륨에 대한 정보를 한 눈에 볼 수 있습니다.
3. 이 정보를 최신 상태로 새로 고치려면 **Actions(작업)** 드롭다운 메뉴를 클릭하고 **Refresh Metadata(메타데이터 새로 고침)**를 클릭합니다.  
클러스터의 노드 또는 개별 시스템에 대한 요약 및 상태 정보에 대해서는 [시스템 상태 및 기타 상세정보 보기](#)를 참조하십시오.

## 클러스터 복구 지점 작업

복구 지점을 스냅샷이라고도 하며, 이는 리포지토리에 저장되는 클러스터의 공유 볼륨에 대한 폴더 및 파일의 지정 시간 복사입니다. 복구 지점은 보호되는 시스템을 복구하거나 로컬 파일 시스템에 탑재하는 데 사용됩니다. AppAssure에서는 리포지토리에 있는 복구 지점의 목록을 볼 수 있습니다. 복구 지점을 보려면 다음 절차의 단계를 완료하십시오.

 **노트:** DAG 또는 CCR 서버 클러스터에서 데이터를 보호하는 경우에는 연결된 복구 지점이 클러스터 수준에서 표시되지 않습니다. 이러한 복구 지점은 노드 또는 시스템 수준에서만 볼 수 있습니다.

클러스터에서 개별 시스템의 복구 지점 보기에 대한 자세한 내용은 [복구 지점 보기](#)를 참조하십시오.

클러스터 복구 지점에 대해 작업하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 복구 지점을 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역의 **Clusters(클러스터)**에서 복구 지점을 보려는 클러스터를 선택합니다.
2. **Recovery Points(복구 지점)** 탭을 클릭합니다.
3. 특정 복구 지점에 대한 자세한 내용을 보려면 목록에서 복구 지점 옆에 있는 > 기호를 클릭하여 보기를 확장합니다.  
복구 지점에서 수행할 수 있는 작업에 대해서는 [특정 복구 지점 보기](#)를 참조하십시오.
4. 탑재할 복구 지점을 선택합니다.  
복구 지점 탑재에 대한 자세한 내용은 2단계를 시작으로 [Windows 시스템의 복구 지점 탑재](#)를 참조하십시오.
5. 복구 지점을 삭제하려면 [복구 지점 제거](#)를 참조하십시오.

## 클러스터에 대한 스냅샷 관리

스냅샷을 강제 적용하거나 현재 스냅샷을 일시 중지하여 스냅샷을 관리할 수 있습니다. 스냅샷을 강제 적용하면 현재 보호된 클러스터에 대한 데이터를 강제로 전송할 수 있습니다. 스냅샷을 강제 적용하면 전송이 즉시 시작되거나 큐에 추가됩니다. 이전 복구 지점에서 변경된 데이터만 전송됩니다. 이전 복구 지점이 없는 경우에는 보호된 볼륨에 대한 모든 데이터(기본 이미지)가 전송됩니다. 스냅샷을 일시 중지하면 현재 시스템에서의 모든 데이터 전송이 일시적으로 중지됩니다.

클러스터의 개별 시스템에 대한 스냅샷 강제 적용에 대한 자세한 내용은 [스냅샷 강제 적용](#)을 참조하십시오. 클러스터의 개별 시스템에 대한 스냅샷 일시 중지 및 다시 시작에 대한 자세한 내용은 [보호 일시 중지 및 다시 시작](#)을 참조하십시오.

## 클러스터에 대한 스냅샷 강제 적용

클러스터에 대한 스냅샷을 강제 적용하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 복구 지점을 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역의 **Clusters(클러스터)**에서 복구 지점을 보려는 클러스터를 선택합니다.
2. **Summary(요약)** 탭에서 **Actions(작업)** 드롭다운 메뉴를 클릭한 후 **Force Snapshot(스냅샷 강제 적용)**을 클릭합니다.

## 클러스터 스냅샷 일시 중지 및 다시 시작

클러스터 스냅샷을 일시 중지하고 다시 시작하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 복구 지점을 보려는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역의 **Clusters(클러스터)**에서 복구 지점을 보려는 클러스터를 선택합니다.
2. **Summary(요약)** 탭에서 **Actions(작업)** 드롭다운 메뉴를 클릭한 후 **Pause Snapshots(스냅샷 일시 중지)**을 클릭합니다.
3. **Pause Protection(보호 일시 중지)** 대화 상자에서 다음에 설명된 옵션 중 하나를 선택합니다.

### 텍스트 상자      설명

**다시 시작될 때까지 일시 중지**      보호를 수동으로 다시 시작할 때까지 스냅샷을 일시 중지합니다. 보호를 다시 시작하려면 **Actions(작업)** 메뉴를 클릭한 후 **Resume(다시 시작)**을 클릭합니다.

**다음 기간 동안 일시 중지**      스냅샷을 일시 중지할 기간을 일, 시간 및 분 단위로 지정할 수 있습니다.

## 로컬 복구 지점 분리

로컬 복구 지점을 분리하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 복구 지점을 분리하기 원하는 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 복구 지점을 분리하기 원하는 클러스터를 선택합니다.
2. **Tools(도구)** 탭의 **Tools(도구)** 메뉴 아래에서 **Mounts(탑재)**를 클릭합니다.
3. 로컬 탑재 목록에서 다음 중 하나를 수행합니다.
  - 단일 로컬 탑재를 분리하려면 분리할 복구 지점에 대한 탑재를 찾아 선택한 후 **Dismount(분리)**를 클릭합니다.
  - 모든 로컬 탑재를 분리하려면 **Dismount All(모두 분리)** 단추를 클릭합니다.

## 클러스터 및 클러스터 노드에 대한 롤백 수행

롤백은 복구 지점으로부터 시스템의 볼륨을 복원하는 프로세스입니다. 서버 클러스터에 대해 노드 또는 시스템 수준에서 롤백을 수행합니다. 이 섹션에서는 클러스터 볼륨의 롤백 수행에 대한 지침을 제공합니다.

## CCR(Exchange) 및 Dag 클러스터에 대한 롤백 수행

SCC(Exchange, SQL) 클러스터에 대한 롤백을 수행하려면 다음을 수행하십시오.

1. 하나를 제외한 나머지 노드를 모두 끕니다.
2. [롤백 수행 및 명령행을 사용하여 Linux 시스템에 롤백 수행](#)에 설명된 대로 시스템의 표준 AppAssure 절차에 따라 롤백을 수행합니다.
3. 롤백이 완료되면 클러스터 볼륨에서 모든 데이터베이스를 탑재합니다.
4. 기타 모든 노드를 해제합니다.
5. Exchange의 경우, Exchange Management 콘솔을 탐색하여 각 데이터베이스에 **데이터베이스 복사 업데이트** 작업을 수행합니다.

## SCC(Exchange, SQL) 클러스터에 대한 롤백 수행

SCC(Exchange, SQL) 클러스터에 대한 롤백을 수행하려면 다음을 수행하십시오.

1. 하나를 제외한 나머지 노드를 모두 끕니다.
2. [롤백 수행 및 명령행을 사용하여 Linux 시스템에 롤백 수행](#)에 설명된 대로 시스템의 표준 AppAssure 절차에 따라 롤백을 수행합니다.
3. 롤백이 완료되면 클러스터 볼륨에서 모든 데이터베이스를 탑재합니다.
4. 나머지 모든 노드를 하나씩 켵니다.



**노트:** 쿼럼 디스크는 롤백할 필요가 없습니다. 쿼럼 디스크는 자동으로 다시 생성되거나 클러스터 서비스 기능을 사용하여 다시 생성할 수 있습니다.

## 클러스터 데이터 복제

클러스터에 대한 데이터를 복제할 때 해당 클러스터의 개별 시스템에 대한 시스템 수준에서 복제를 구성합니다. 또한 복제를 구성하여 공유 볼륨에 대한 복구 지점을 복제할 수 있습니다(예: 원본에서 대상으로 복제할 에이전트가 5개 있는 경우).

데이터 복제에 대한 자세한 내용 및 지침은 [시스템에서 에이전트 데이터 복제](#)를 참조하십시오.

## 클러스터 보호 제거

클러스터의 보호를 제거하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭하고 제거할 클러스터를 선택합니다.
  - 왼쪽 탐색 영역에서 제거할 클러스터를 선택하여 **Summary(요약)** 탭을 봅니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Remove Machine(시스템 제거)**를 클릭합니다.
3. 다음 옵션 중 하나를 선택합니다.

### 옵션

### 설명

#### 복구 지점 유지

이 클러스터에 대해 현재 저장된 모든 복구 지점을 유지하려면 선택합니다.

#### 복구 지점 제거

이 클러스터에 대해 현재 저장된 모든 복구 지점을 리포지토리에서 제거하려면 선택합니다.

## 클러스터 노드 보호 제거

다음 절차의 단계를 완료하여 클러스터 노드의 보호를 제거합니다. 클러스터에서 노드 제거만 수행하려면 [보호된 클러스터 노드를 에이전트로 변환](#)을 참조하십시오. 클러스터 노드의 보호를 제거하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 제거하기 원하는 노드가 포함되어 있는 클러스터를 선택합니다. 클러스터에 대한 **Machines(시스템)** 탭에서 제거하기 원하는 노드를 선택합니다.
  - 왼쪽 탐색 영역의 관련 클러스터 아래에서 제거하기 원하는 노드를 선택합니다.
2. **Actions(작업)** 드롭다운 메뉴를 클릭하고 **Remove Machine(시스템 제거)**을 클릭합니다.
3. 다음 표에 설명되어 있는 옵션 중 하나를 선택합니다.

옵션	설명
<b>Relationship Only(관계만)</b>	복제에서 소스 Core를 제거하지만 복제된 복구 지점은 그대로 유지됩니다.
<b>With Recovery Points(복구 지점 포함)</b>	복제에서 소스 Core를 제거하고 해당 시스템에서 받은 모든 복제된 복구 지점을 삭제합니다.

## 클러스터의 모든 노드 보호 제거

클러스터의 모든 노드에 대한 보호를 제거하려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭하고 제거하기 원하는 노드가 포함되어 있는 클러스터를 선택한 다음 클러스터의 **Machines(시스템)** 탭을 클릭합니다.
  - 왼쪽 탐색 영역에서 제거하기 원하는 노드가 포함되어 있는 클러스터를 선택한 후 **Machines(시스템)** 탭을 클릭합니다.
2. **Machines(시스템)** 탭의 맨 위에 있는 **Actions(작업)** 드롭다운 메뉴를 클릭하고 **Remove Machines(시스템 제거)**을 클릭합니다.
3. 다음 표에 설명되어 있는 옵션 중 하나를 선택합니다.

옵션	설명
<b>Relationship Only(관계만)</b>	복제에서 소스 Core를 제거하지만 복제된 복구 지점은 그대로 유지됩니다.
<b>With Recovery Points(복구 지점 포함)</b>	복제에서 소스 Core를 제거하고 해당 시스템에서 받은 모든 복제된 복구 지점을 삭제합니다.


## 클러스터 또는 노드 보고서 보기

클러스터 및 개별 노드의 AppAssure 작업에 대한 호환성 및 오류 보고서를 생성하고 볼 수 있습니다. 보고서에 클러스터, 노드 및 공유 볼륨에 대한 AppAssure 작업 정보가 포함되어 있습니다. AppAssure 보고에 대한 자세한 내용은 [보고서 정보](#)를 참조하십시오.



보고서 도구 모음에 있는 내보내기 및 인쇄 옵션에 대한 자세한 내용은 [보고서 도구 모음 정보](#)를 참조하십시오.

클러스터 또는 노드 보고서를 보려면 다음을 수행하십시오.

1. 다음 중 하나를 수행합니다.
  - Core 콘솔에서 **Machines(시스템)** 탭을 클릭한 후 보고서를 생성하기 원하는 클러스터 또는 노드를 선택합니다.
  - 왼쪽 **탐색** 영역에서 보고서를 생성하기 원하는 클러스터 또는 노드를 선택합니다.
2. **Tools(도구)** 탭을 클릭하고 **Reports(보고서)** 메뉴에서 다음 옵션 중 하나를 선택합니다.
  - **호환성 보고서**
  - **오류 보고서**
3. **Start Time(시작 시간)** 드롭다운 달력에서 시작 날짜를 선택한 후 보고서의 시작 시간을 입력합니다.  
 **노트:** AppAssure Core 또는 AppAssure 에이전트 소프트웨어가 배포되기 이전의 데이터는 사용할 수 없습니다.
4. **End Time(종료 시간)** 드롭다운 달력에서 종료 날짜를 선택한 후 보고서의 종료 시간을 입력합니다.
5. **Generate Report(보고서 생성)**를 클릭합니다.  
보고서에 여러 페이지가 포함되어 있는 경우 페이지 번호를 클릭하거나 보고서 결과의 맨 위에 있는 화살표 단추를 클릭하여 결과 페이지를 넘겨 볼 수 있습니다.  
  
페이지에 보고서 결과가 나타납니다.
6. 보고서 결과를 PDF, XLS, XLSX, RTF, MHT, HTML, TXT, CSV 또는 이미지와 같은 사용 가능한 형식 중 하나로 내보내려면 드롭다운 목록에서 내보낼 형식을 선택한 후 다음 중 하나를 수행하십시오.
  - 보고서를 내보내고 디스크에 저장하려면 첫 번째 **Save(저장)** 아이콘을 클릭합니다.
  - 보고서를 내보내고 새 웹 브라우저 창에 표시하려면 두 번째 **Save(저장)** 아이콘을 클릭합니다.
7. 보고서 결과를 인쇄하려면 다음 중 하나를 수행하십시오.
  - 전체 보고서를 인쇄하려면 첫 번째 **Printer(프린터)** 아이콘을 클릭합니다.
  - 보고서의 현재 페이지를 인쇄하려면 두 번째 **Printer(프린터)** 아이콘을 클릭합니다.

## 보고

### 보고서 정보





DL 어플라이언스에서는 여러 Core 및 에이전트 시스템에 대한 호환성, 오류 및 요약 정보를 생성하고 볼 수 있습니다.

보고서를 온라인으로 보거나, 보고서를 인쇄하거나, 지원되는 여러 형식 중 하나로 해당 보고서를 내보내고 저장하도록 선택할 수 있습니다. 선택할 수 있는 형식은 다음과 같습니다.

- PDF
- XLS
- XLSX
- RTF
- MHT
- HTML
- TXT
- CSV
- 이미지

### 보고서 도구 모음 정보

모든 보고서에 사용 가능한 도구 모음에서 두 가지 다른 방식으로 보고서를 인쇄하고 저장할 수 있습니다. 다음 표에 인쇄 및 저장 옵션이 설명되어 있습니다.

Icon	설명
	보고서 인쇄
	현재 페이지 인쇄
	보고서를 내보내고 디스크에 저장
	보고서를 내보내고 새 창에 표시 다른 사용자가 웹 브라우저에서 보고서를 볼 수 있도록 URL을 복사하고, 붙여 넣고, 전자 메일로 보내려면 이 옵션을 사용합니다.

### 호환성 보고서 정보

Core 및 AppAssure Agent에 대한 호환성 보고서를 사용할 수 있습니다. 이 보고서에서는 선택한 Core 또는 에이전트에서 수행한 작업의 상태를 확인할 수 있습니다. 실패한 작업은 빨간색으로 표시됩니다. 에이전트와 연결되어 있지 않은 Core 호환성 보고서의 정보는 비어 있습니다.

다음 범주가 포함되어 있는 열 보기에 작업에 대한 상세정보가 표시됩니다.

- Core
- 보호된 에이전트
- Type(유형)
- Summary(요약)
- Status(상태)
- 오류
- 시작 시간
- 종료 시간
- 시간
- 총 작업 시간

## 오류 보고서 정보

오류 보고서는 호환성 보고서의 하위 집합으로, Core 및 AppAssure Agent에서 사용할 수 있습니다. 오류 보고서에는 호환성 보고서에 나열된 실패한 작업만 포함되며, 해당 작업을 인쇄하고 내보낼 수 있는 단일 보고서로 편집합니다.

다음 범주가 포함되어 있는 열 보기에 오류에 대한 상세정보가 표시됩니다.

- Core
- 에이전트
- Type(유형)
- Summary(요약)
- 오류
- 시작 시간
- 종료 시간
- 경과 시간
- 총 작업 시간

## Core 요약 보고서 정보

**Core Summary Report(Core 요약 보고서)**에는 선택한 Core에 있는 리포지토리 및 해당 Core에서 보호되는 에이전트에 대한 정보가 포함됩니다. 이러한 정보는 단일 보고서 내에서 두 가지 요약으로 표시됩니다.

### 리포지토리 요약

**Core Summary Report(Core 요약 보고서)**의 **Repositories(리포지토리)** 옵션에 선택한 Core에 있는 리포지토리에 대한 데이터가 포함되어 있습니다. 다음 범주가 포함되어 있는 열 보기에 리포지토리에 대한 상세정보가 표시됩니다.

- 이름
- 데이터 경로
- 메타데이터 경로
- 할당된 공간
- 사용 중인 공간

- 사용 가능한 공간
- 압축/중복 제거 비율

## 에이전트 요약

**Core Summary Report(Core 요약 보고서)**의 **Agents(에이전트)** 옵션에 선택한 Core에 의해 보호되는 모든 에이전트에 대한 데이터가 포함되어 있습니다.

다음 범주가 포함되어 있는 열 보기에 에이전트에 대한 상세정보가 표시됩니다.

- 이름
- 보호된 볼륨
- 총 보호된 공간
- 현재 보호된 공간
- 일일 변경률(평균, 중간)
- 작업 통계(통과, 실패 및 취소)

## Core 또는 에이전트에 대한 보고서 생성

Core 또는 에이전트에 대한 보고서를 생성하려면 다음을 수행하십시오.

1. Core 콘솔로 이동해서 보고서를 실행할 Core 또는 에이전트를 선택합니다.
2. **Tools(도구)** 탭을 클릭합니다.
3. **Tools(도구)** 탭에서 왼쪽 탐색 영역에 있는 **Reports(보고서)**를 확장합니다.
4. 왼쪽 탐색 영역에서 실행할 보고서를 선택합니다. 사용 가능한 보고서는 1단계에서 선택한 항목에 따라 다르며, 아래에 설명되어 있습니다.

시스템	사용 가능한 보고서
Core	호환성 보고서 요약 보고서  오류 보고서
에이전트	호환성 보고서 오류 보고서

5. **Start Time(시작 시간)** 드롭다운 달력에서 시작 날짜를 선택한 후 보고서의 시작 시간을 입력합니다.



**노트:** Core 또는 에이전트가 배포되기 이전의 데이터는 사용할 수 없습니다.

6. **End Time(종료 시간)** 드롭다운 달력에서 종료 날짜를 선택한 후 보고서의 종료 시간을 입력합니다.
7. **Core Summary Report(Core 요약 보고서)**의 경우 **Start Time(시작 시간)** 및 **End Time(종료 시간)**에 Core의 수명을 포함하려면 **All Time(모든 시간)** 확인란을 선택합니다.
8. **Core Compliance Report(Core 호환성 보고서)** 또는 **Core Errors Report(Core 오류 보고서)**의 경우 **Target Cores(대상 Core)** 드롭다운 목록을 사용하여 데이터를 볼 Core를 선택합니다.
9. **Generate Report(보고서 생성)**를 클릭합니다.


보고서가 생성되면 도구 모음을 사용하여 보고서를 인쇄하거나 내보낼 수 있습니다.

## 중앙 관리 콘솔 Core 보고서 정보

DL 어플라이언스를 사용하여 여러 Core의 호환성, 오류, 요약 정보를 생성하고 확인할 수 있습니다. Core에 대한 상세정보는 이 섹션에 설명된 동일한 범주와 함께 열 보기에 제공되어 있습니다.

## 중앙 관리 콘솔에서 보고서 생성

중앙 관리 콘솔에서 보고서를 생성하려면 다음을 수행하십시오.


1. **Central Management Console Welcome(중앙 관리 콘솔 시작)** 화면에서 오른쪽 상단에 있는 드롭다운 메뉴를 클릭합니다.
2. 드롭다운 메뉴에서 **Reports(보고서)**를 클릭한 후 다음 옵션 중 하나를 선택합니다.
  - 호환성 보고서
  - 요약 보고서
  - 오류 보고서
3. 왼쪽 탐색 영역에서 보고서를 실행할 Core를 선택합니다.
4. **Start Time(시작 시간)** 드롭다운 달력에서 시작 날짜를 선택한 후 보고서의 시작 시간을 입력합니다.  
 **노트:** Cores가 배포되기 이전의 데이터는 사용할 수 없습니다.
5. **End Time(종료 시간)** 드롭다운 달력에서 종료 날짜를 선택한 후 보고서의 종료 시간을 입력합니다.
6. **Generate Report(보고서 생성)**를 클릭합니다.  
보고서가 생성되면 도구 모음을 사용하여 보고서를 인쇄하거나 내보낼 수 있습니다.

## DL4300 어플라이언스 전체 복구 완료




DL4300 Backup To Disk Appliance의 데이터 드라이브는 슬롯 0-11 및 14-17에 RAID 6 형식으로 있습니다. 즉, 데이터 손실 없이 최대 두 개의 드라이브 오류까지 수용할 수 있습니다. 운영 체제는 드라이브 12와 13에 있으며, RAID 1 가상 디스크 형식으로 지정되어 있습니다. 이러한 두 디스크에 모두 오류가 발생하면 드라이브를 교체하고 다시 작동되도록 어플라이언스에 필요한 소프트웨어를 다시 설치해야 합니다. 어플라이언스의 전체 복구를 완료하려면 다음을 수행해야 합니다.

- 운영 체제에 대한 RAID 1 파티션 생성
- 운영 체제 설치
- 복구 및 업데이트 유틸리티 실행
- 볼륨 탑재

### 운영 체제에 대한 RAID 1 파티션 생성

 주의: 운영 체제가 포함되어 있는 RAID 1 가상 디스크에서만 이러한 작업을 수행해야 합니다. 데이터가 포함되어 있는 RAID 6 가상 디스크에서는 이러한 작업을 수행하지 마십시오.




RAID 1 파티션을 생성하려면 다음을 수행하십시오.

1. 슬롯 12와 13에 있는 디스크가 정상적으로 작동하는 디스크인지 확인합니다.
2. DL4300 Backup to Disk Appliance를 부팅합니다.
3. 부팅 프로세스를 수행하는 동안 메시지가 표시되면 <Ctrl><R>을 누릅니다.  
**PERC BIOS Configuration Utility(PERC BIOS 구성 유틸리티)** 화면이 표시됩니다.
4. **VD Management(VD 관리)** 탭의 맨 위에 있는 컨트롤러를 강조표시하고 <F2> 키를 누른 후 **Create New VD(새 VD 생성)**를 선택합니다.  
 **노트:** RAID-1 OS VD가 이미 있는 경우 RAID-1 OS VD를 빠른 초기화합니다.
5. **Virtual Disk Management(가상 디스크 관리)** 페이지에서 RAID 수준에 대해 RAID 1을 선택합니다.
6. **Physical Disks(실제 디스크)** 상자에서 두 디스크를 모두 선택합니다.  
 **노트:** 가상 디스크 크기는 278.87GB를 초과하지 않아야 합니다.
7. 운영 체제가 포함되어 있는 디스크로 가상 디스크를 식별하는 VD 이름을 입력합니다(예: "OS").
8. <Tab> 키를 눌러 커서를 Initialize(초기화)로 이동하고 <Enter> 키를 누릅니다.  
 **노트:** 이 단계에서 수행되는 초기화는 빠른 초기화입니다.
9. **OK(확인)**를 클릭하여 선택을 완료하거나 <Ctrl><N>을 두 번 누릅니다.  
**Ctrl Mgt(관리 제어)** 페이지가 표시됩니다.
10. **Select boot device(부팅 장치 선택)** 필드를 탐색하고 운영 체제가 포함되어 있는 가상 디스크를 선택합니다.  
이 디스크의 용량은 약 278GB입니다.

11. **Apply(적용)**를 선택하고 <Enter> 키를 누릅니다.
12. **PERC BIOS Configuration(PERC BIOS 구성)** 유틸리티를 종료하고 <Ctrl><Alt><Del>를 눌러 시스템을 재부팅합니다.

## 운영 체제 설치

다음과 같이 어플라이언스에서 USC-LCE(Unified Server Configurator-Lifecycle Controller Enabled)를 사용하여 운영 체제를 복구할 수 있습니다.

1. 운영 체제 설치 미디어를 찾습니다.
2. 미디어를 실행할 드라이버가 있는지 확인합니다.  
USB 광 드라이브 또는 가상 미디어 장치를 사용할 수 있습니다. 가상 미디어는 iDRAC를 통해 지원됩니다. iDRAC를 통한 가상 미디어 설정에 대한 자세한 내용은 시스템의 iDRAC 장치에 대한 사용 설명서를 참조하십시오.  
설치 미디어가 손상되었거나 읽을 수 없는 경우 USC가 지원되는 광 드라이브의 유무를 감지하지 못할 수 있습니다. 이 경우 사용 가능한 광 드라이브가 없다는 오류 메시지가 표시될 수 있습니다. 미디어가 유효하지 않은 경우(예: 잘못된 CD 또는 DVD인 경우) 올바른 설치 미디어를 삽입하라는 메시지가 표시됩니다.
3. 시스템을 부팅하고 Dell 로고가 표시되면 10초 내에 <F10> 키를 눌러 USC를 시작합니다.
4. 왼쪽 창에서 **OS Deployment(OS 배치)**를 클릭합니다.
5. 오른쪽 창에서 **Deploy OS(OS 배치)**를 클릭합니다.
6. 관련 운영 체제를 선택하고 **Next(다음)**를 클릭합니다.  
USC가 사용자가 선택한 운영 체제에 필요한 드라이버를 추출합니다. **OEMDRV**라는 내부 USB 드라이브에 드라이버가 추출됩니다.  
 **노트:** 드라이버를 추출하는 프로세스는 몇 분 정도 걸릴 수 있습니다.  
 **노트:** OS 배포 마법사에서 복사된 모든 드라이버는 18시간 후에 제거됩니다. 복사한 드라이버를 사용하려면 18시간 내에 운영 체제 설치를 완료해야 합니다. 18시간이 지나기 전에 드라이버를 제거하려면 시스템을 재부팅한 후 <F10> 키를 눌러 USC를 다시 시작합니다. 재부팅 시 USC를 다시 시작하거나 운영 체제 설치를 취소하기 위해 <F10> 키를 사용하면 18시간 동안 드라이버가 제거됩니다.
7. 드라이버가 추출되고 USC가 메시지를 표시하면 운영 체제 설치 미디어를 삽입합니다.  
 **노트:** Microsoft Windows 운영 체제를 설치할 때 운영 체제를 설치하는 동안 추출된 드라이버가 자동으로 설치됩니다.

## 복구 및 업데이트 유틸리티 실행

복구 및 업데이트 유틸리티를 실행하려면 다음을 수행하십시오.

1. [dell.com/support](http://dell.com/support)에서 **Recovery and Update Utility(복구 및 업데이트 유틸리티)**를 다운로드합니다.
2. DL4300 Backup To Disk Appliance의 데스크탑에 유틸리티를 복사하고 파일을 추출합니다.
3. **launchRUU**를 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 and Features, ASP .NET MVC3, LSI Provider, DL Applications, OpenManage Server Administrator 및 AppAssure Core 소프트웨어가 복구 및 업데이트 유틸리티의 일부로 설치됩니다.

7. 메시지가 다시 표시되면 시스템을 재부팅합니다.
8. 모든 서비스와 응용프로그램이 설치되면 **Proceed(계속)**를 클릭합니다.  
**AppAssure Appliance Recovery(AppAssure 어플라이언스 복구)** 마법사가 시작됩니다.
9. AppAssure Appliance Recovery(AppAssure 어플라이언스 복구) 마법사의 **Collecting Information and Configuring(정보 수집 및 구성)** 단계에 있는 단계를 완료한 후 **Next(다음)**를 클릭합니다.  
**Disk Recovery(디스크 복구)** 단계가 시작됩니다.
10. 종료되는 AppAssure 서비스에 대한 경고를 본 후 **Next(다음)**를 클릭합니다.  
리포지토리에 대한 가상 디스크 및 모든 가상 대기 시스템이 복원되고 AppAssure 서비스가 다시 시작됩니다. 복구가 완료됩니다.



## 호스트 이름을 수동으로 변경

DL4300 Backup to Disk Appliance를 처음 구성할 때 호스트 이름을 선택하는 것이 좋습니다. 나중에 **Windows System Properties(Windows 시스템 등록 정보)**를 사용하여 호스트 이름을 변경하는 경우 새 호스트 이름이 적용되고 어플라이언스 가 제대로 작동되도록 다음 단계를 수동으로 수행해야 합니다.

1. AppAssure Core 서비스 중지
2. AppAssure 서버 인증서 삭제
3. Core 서버 및 레지스트리 키 삭제
4. AppAssure에서 표시 이름 변경
5. Internet Explorer에서 신뢰할 수 있는 사이트 업데이트

### Core 서비스 중지

AppAssure Core 서비스를 중지하려면 다음을 수행하십시오.

1. **Windows Server Manager**를 엽니다.
2. 왼쪽에 있는 트리에서 **Configuration** → **Services**를 선택합니다.
3. **AppAssure Core Service(AppAssure Core 서비스)**를 마우스 오른쪽 단추로 클릭하고 **Stop(중지)**을 선택합니다.

### 서버 인증서 삭제

AppAssure 서버 인증서를 삭제하려면 다음을 수행하십시오.

1. 명령행 인터페이스를 엽니다.
2. **Certmgr**를 입력하고 <Enter> 키를 누릅니다.
3. **Certificate Manager(인증서 관리자)** 창에서 **Trusted Root Certification Authorities(신뢰할 수 있는 루트 인증 기관)** → **Certificates(인증서)**를 선택합니다.
4. **Issue To(발급 대상)** 열에 이전 호스트 이름이 표시되고 **Intended Purpose(용도)** 열에 **Server Authentication(서버 인증)**이 표시되도록 인증서를 삭제합니다.

### Core 서버 및 레지스트리 키 삭제

Core 서버 및 레지스트리 키를 삭제하려면 다음을 수행하십시오.

1. 명령행 인터페이스를 엽니다.
2. **regedit**를 입력하고 <Enter> 키를 눌러 레지스트리 편집기를 엽니다.
3. 트리에서 **HKEY\_LOCAL\_MACHINE** → **SOFTWARE** → **AppRecovery**를 탐색하고 Core 디렉터리를 엽니다.

4. **webServer** 및 **serviceHost** 디렉터리를 삭제합니다.

## 새 호스트 이름을 사용하여 Core 실행

수동으로 생성한 새 호스트 이름을 사용하여 Core를 시작하려면 다음을 수행합니다.

1. AppAssure Core 서비스를 시작합니다.
2. 바탕화면에서 **AppAssure 5 Core** 아이콘을 마우스 오른쪽 단추로 클릭하고 **Properties(속성)**를 클릭합니다.
3. 기존 서버 이름을 새 <server name:8006>으로 바꿉니다.  
예를 들어, **https://<servername>:8006/apprecovery/admin/Core**입니다.
4. **OK(확인)**를 클릭하고 **AppAssure 5 Core** 아이콘을 사용하여 AppAssure Core 콘솔을 시작합니다.

## 표시 이름 변경

표시 이름을 변경하려면 다음을 수행하십시오.

1. **AppAssure Console(AppAssure 콘솔)**에 관리자로 로그인합니다.
2. **Configuration(구성)** 탭을 선택한 후 **General(일반)** 모음에서 **Change(변경)** 단추를 클릭합니다.
3. 새 표시 이름을 입력하고 **OK(확인)**를 클릭합니다.

## Internet Explorer에서 신뢰할 수 있는 사이트 업데이트

Internet Explorer에서 신뢰할 수 있는 사이트를 업데이트하려면 다음을 수행하십시오.


1. Internet Explorer를 엽니다.
2. **File(파일)**, **Edit View(보기 편집)** 및 기타 메뉴가 표시되지 않으면 <F10> 키를 누릅니다.
3. **Tools(도구)** 메뉴를 클릭하고 **Internet Options(인터넷 옵션)**을 선택합니다.
4. **Internet Options(인터넷 옵션)** 창에서 **Security(보안)** 탭을 클릭합니다.
5. **Trusted Sites(신뢰할 수 있는 사이트)**를 클릭한 후 **Sites(사이트)**를 클릭합니다.
6. **Add this website to the zone(영역에 웹 사이트 추가)**에서 표시 이름으로 제공한 새 이름을 사용하여 **https://[Display Name]**을 입력합니다.
7. **Add(추가)**를 클릭합니다.
8. **Add this website to the zone(영역에 웹 사이트 추가)**에서 **about:blank**를 입력합니다.
9. **Add(추가)**를 클릭합니다.
10. **Close(닫기)**를 클릭한 후 **OK(확인)**를 클릭합니다.

## 부록 A - 스크립팅

### Powershell 스크립팅 정보


Windows PowerShell은 관리 자동화를 위해 설계된 Microsoft .NET Framework 연결 환경입니다. AppAssure에는 관리자가 스크립트를 통해 명령을 실행하여 AppAssure 리소스의 운영 및 관리를 자동화할 수 있는 PowerShell 스크립팅에 대한 통합 클라이언트 소프트웨어 개발 키트(SDK)가 포함되어 있습니다.

이를 통해 관리 사용자가 지정된 어커런스에서 사용자 제공 PowerShell 스크립트를 실행할 수 있습니다. 예를 들어, 스냅샷 전 또는 후에 연결 기능 및 탑재 기능 검사 등을 수행할 수 있습니다. 관리자가 AppAssure Core와 에이전트에서 모두 스크립트를 실행할 수 있습니다. 스크립트에서 Core 및 에이전트 로그 파일에 기록된 스크립트의 출력과 매개변수를 허용합니다.

 **노트:** 야간 작업의 경우 하나의 스크립트 파일 및 JobType 입력 매개변수를 유지하여 야간 작업을 구분합니다.


스크립트 파일은 다음과 같이 **%ALLUSERSPROFILE%\AppRecovery\Scripts** 폴더에 있습니다.

- Windows 7의 경우 **%ALLUSERSPROFILE%** 폴더가 있는 경로는 **C:\ProgramData**입니다.
- Windows 2003의 경우 폴더가 있는 경로는 **Documents and Settings\All Users\Application Data**입니다.

 **노트:** Windows PowerShell이 필요하며, AppAssure 스크립트를 사용하고 실행하기 전에 설치 및 구성해야 합니다.

### Powershell 스크립팅 필수 구성 요소

AppAssure용 PowerShell 스크립트를 사용하고 실행하려면 먼저 Windows PowerShell 2.0이 설치되어 있어야 합니다.


 **노트:** PowerShell 홈 디렉터리에 **powershell.exe.config** 파일을 배치해야 합니다(예: **C:\WindowsPowerShell\powershell.exe**).

#### powershell.exe.config

```
<?xml version="1.0"?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0.30319"/>
  </startup>
  <supportedRuntime version="v2.0.50727"/>
</configuration>
```

### 스크립트 검사


실행할 스크립트를 검사하려면 PowerShell 그래픽 편집기인 **powershell\_ise**를 사용하여 검사할 수 있습니다. 또한 **powershell\_ise.exe.config** 구성 파일을 **powershell.exe.config** 구성 파일과 동일한 폴더에 추가해야 합니다.

 **노트:** powershell\_ise.exe.config 구성 파일에 powershell.exe.config 파일과 동일한 내용이 있어야 합니다.

 **주의:** 사전 PowerShell 또는 사후 PowerShell 스크립트가 실패하면 작업도 실패합니다.

## 입력 매개변수

사용 가능한 모든 입력 매개변수가 샘플 스크립트에서 사용됩니다. 해당 매개변수는 다음 표에 설명되어 있습니다.

 **노트:** 스크립트 파일에 샘플 스크립트 파일과 동일한 이름을 사용해야 합니다.

**표 5. AgentTransferConfiguration (namespace Replay.Common.Contracts.Transfer)**

방법	설명
<pre>public uint MaxConcurrentStreams { get; set; }</pre>	Core에서 데이터를 전송하기 위해 에이전트에 설정하는 최대 동시 TCP 연결 수를 가져오거나 설정합니다.
<pre>public uint MaxTransferQueueDepth { get; set; }</pre>	전송 스트림에서 블록의 범위를 관독하면 해당 범위가 생산자 또는 소비자 큐에 배치되며, 여기에서 소비자 스레드가 범위를 읽고 epoch 개체에 씁니다. 리포지토리 쓰기의 속도가 네트워크 읽기보다 느린 경우 이 큐가 채워집니다. 큐가 채워지고 읽기가 중지되는 시점이 최대 전송 큐 크기입니다.
<pre>public uint MaxConcurrentWrites { get; set; }</pre>	지정한 시간에 언제든지 epoch에서 대기하는 최대 블록 쓰기 작업의 수를 가져오거나 설정합니다. 이러한 여러 블록 쓰기가 대기 중인 때 추가 블록을 수신하면 대기 중인 쓰기 중 하나가 완료될 때까지 해당 추가 블록이 무시됩니다.
<pre>public ulong MaxSegmentSize { get; set; }</pre>	단일 요청에서 전송에 대한 최대 연속 블록의 수를 가져오거나 설정합니다. 검사에 따라 더 높거나 더 낮은 값이 적합할 수 있습니다.
<pre>public Priority Priority { get; set; }</pre>	전송 요청에 대한 우선순위를 가져오거나 설정합니다.
<pre>public int MaxRetries { get; set; }</pre>	추정이 실패하기 전에 실패한 전송이 다시 시도되는 최대 횟수를 가져오거나 설정합니다.
<pre>public Guid ProviderId { get; set; }</pre>	이 호스트의 스냅샷에 사용할 VSS 공급자의 GUID를 가져오거나 설정합니다. 일반적으로 관리자가 기본값을 사용합니다.
<pre>public Collection&lt;ExcludedWriter&gt;ExcludedWriterIds { get; set; }</pre>	이 스냅샷에서 제외되는 VSS 기록기 ID의 컬렉션을 가져오거나 설정합니다. 기록기 ID는 기록기의 이름에 따라 결정됩니다. 이 이름은 문서 작성용으로만 사용되며 작성기의 이름과 정확하게 일치할 필요가 없습니다.

방법	설명
<code>public ushort TransferDataServerPort { get; set; }</code>	에이전트에서 Core로 데이터를 실제로 전송할 수 있도록 Core에서의 연결을 수용할 TCP 포트가 포함되어 있는 값을 가져오거나 설정합니다. 에이전트가 이 포트에서 수신하도록 시도하지만 포트가 사용 중인 경우에는 에이전트가 다른 포트를 대신 사용할 수 있습니다. Core에서 각 스냅 볼륨에 대해 VolumeSnapshotInfo 개체의 BlockHashesUri 및 BlockDataUri 속성에 지정된 포트 번호를 사용합니다.
<code>public TimeSpan SnapshotTimeout { get; set; }</code>	중지하고 시간이 초과되기 전에 VSS 스냅샷 작업이 완료될 때까지 대기하는 시간을 가져오거나 설정합니다.
<code>public TimeSpan TransferTimeout { get; set; }</code>	스냅샷을 중단하기 전에 Core에서의 추가 연결을 대기하는 시간을 가져오거나 지정합니다.
<code>public TimeSpan NetworkReadTimeout { get; set; }</code>	이 전송과 관련된 네트워크 읽기 작업에 대한 시간 제한을 가져오거나 설정합니다.
<code>public TimeSpan NetworkWriteTimeout { get; set; }</code>	이 전송과 관련된 네트워크 쓰기 작업에 대한 시간 제한을 가져오거나 설정합니다.

**표 6. BackgroundJobRequest (namespace Replay.Core.Contracts.BackgroundJobs)**

방법	설명
<code>public Guid AgentId { get; set; }</code>	에이전트의 ID를 가져오거나 설정합니다.
<code>public bool IsNightlyJob { get; set; }</code>	백그라운드 작업이 야간 작업인지 나타내는 값을 가져오거나 설정합니다.
<code>public virtual bool InvolvesAgentId(Guid agentId)</code>	작업에 구체적인 에이전트가 포함되어 있는지 나타내는 값을 결정합니다.

#### **ChecksumCheckJobRequest (namespace Replay.Core.Contracts.Exchange.ChecksumChecks)**

매개변수 DatabaseCheckJobRequestBase에서 해당 값을 상속합니다.

#### **DatabaseCheckJobRequestBase (namespace Replay.Core.Contracts.Exchange)**

매개변수 BackgroundJobRequest에서 해당 값을 상속합니다.

#### **ExportJobRequest(네임스페이스 Replay.Core.Contracts.Export)**

매개변수 BackgroundJobRequest에서 해당 값을 상속합니다.

방법	설명
<code>public uint RamInMegabytes { get; set; }</code>	내보낸 VM의 메모리 크기를 가져오거나 설정합니다. 원본 시스템의 메모리 크기를 사용하려면 0으로 설정하십시오.
<code>public VirtualMachineLocation Location { get; set; }</code>	이 내보내기에 대한 대상 위치를 가져오거나 설정합니다. 이는 추상 기본 클래스입니다.

방법	설명
<code>public VolumeImageIdsCollection VolumeImageIds { get; private set; }</code>	VM 내보내기에 포함할 볼륨 이미지를 가져오거나 설정합니다.
<code>public ExportJobPriority Priority { get; set; }</code>	내보내기 요청에 대한 우선순위를 가져오거나 설정합니다.

#### **NightlyAttachabilityJobRequest (namespace Replay.Core.Contracts.Sql)**

매개변수 `BackgroundJobRequest`에서 해당 값을 상속합니다.

#### **RollupJobRequest (namespace Replay.Core.Contracts.Rollup)**

매개변수 `BackgroundJobRequest`에서 해당 값을 상속합니다.

#### **TakeSnapshotResponse (namespace Replay.Agent.Contracts.Transfer)**

방법	설명
<code>public Guid SnapshotSetId { get; set; }</code>	VSS에 의해 이 스냅샷에 할당된 GUID를 가져오거나 설정합니다.
<code>public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }</code>	스냅에 포함된 각 볼륨에 대한 스냅샷 정보의 컬렉션을 가져오거나 설정합니다.

#### **TransferJobRequest (namespace Replay.Core.Contracts.Transfer)**

매개변수 `BackgroundJobRequest`에서 해당 값을 상속합니다.

방법	설명
<code>public VolumeNameCollection VolumeNames { get; set; }</code>	전송할 볼륨 이름의 컬렉션을 가져오거나 설정합니다.
<code>public ShadowCopyType ShadowCopyType { get; set; }</code>	전송에 사용할 복사 유형을 가져오거나 설정합니다. 사용 가능한 값은 <code>Unknown</code> (알 수 없음), <code>Copy</code> (복사), <code>Full</code> (전체) 입니다.
<code>Public AgentTransferConfiguration TransferConfiguration { get; set; }</code>	전송 구성을 가져오거나 설정합니다.
<code>public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }</code>	저장소 구성을 가져오거나 설정합니다.
<code>public string Key { get; set; }</code>	전송 요청을 인증하기 위한 일회용 암호로 사용할 수 있는 의사 난수(암호화로 보안되지 않음) 키를 생성합니다.
<code>public bool ForceBaseImage { get; set; }</code>	기본 이미지가 강제 적용되는지 여부를 나타내는 값을 가져오거나 설정합니다.
<code>public bool IsLogTruncation { get; set; }</code>	작업이 로그 자르기인지를 나타내는 값을 가져오거나 설정합니다.

**표 7. TransferPostscriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)**

방법	설명
<code>public VolumeNameCollection VolumeNames { get; set; }</code>	전송할 볼륨 이름의 컬렉션을 가져오거나 설정합니다.
<code>public ShadowCopyType ShadowCopyType { get; set; }</code>	전송에 사용할 복사 유형을 가져오거나 설정합니다. 사용 가능한 값은 Unknown (알 수 없음), Copy (복사), Full (전체) 입니다.
<code>public AgentTransferConfiguration TransferConfiguration { get; set; }</code>	전송 구성을 가져오거나 설정합니다.
<code>public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }</code>	저장소 구성을 가져오거나 설정합니다.
<code>public string Key { get; set; }</code>	전송 요청을 인증하기 위한 일회용 암호로 사용할 수 있는 의사 난수(암호화로 보안되지 않음) 키를 생성합니다.
<code>public bool ForceBaseImage { get; set; }</code>	기본 이미지가 강제 적용되는지 여부를 나타내는 값을 가져오거나 설정합니다.
<code>public bool IsLogTruncation { get; set; }</code>	작업이 로그 자르기인지를 나타내는 값을 가져오거나 설정합니다.
<code>public uint LatestEpochSeenByCore { get; set; }</code>	최신 epoch 값을 가져오거나 설정합니다.
<code>public Guid SnapshotSetId { get; set; }</code>	VSS에 의해 이 스냅샷에 할당된 GUID를 가져오거나 설정합니다.
<code>public VolumeSnapshotInfoDictionary VolumeSnapshots { get; set; }</code>	스냅에 포함된 각 볼륨에 대한 스냅샷 정보의 컬렉션을 가져오거나 설정합니다.

**표 8. TransferPrescriptParameter (namespace Replay.Common.Contracts.PowerShellExecution)**

방법	설명
<code>public VolumeNameCollection VolumeNames { get; set; }</code>	전송할 볼륨 이름의 컬렉션을 가져오거나 설정합니다.
<code>public ShadowCopyType ShadowCopyType { get; set; }</code>	전송에 사용할 복사 유형을 가져오거나 설정합니다. 사용 가능한 값은 Unknown (알 수 없음), Copy (복사), Full (전체) 입니다.
<code>public AgentTransferConfiguration TransferConfiguration { get; set; }</code>	전송 구성을 가져오거나 설정합니다.
<code>public AgentProtectionStorageConfiguration StorageConfiguration { get; set; }</code>	저장소 구성을 가져오거나 설정합니다.
<code>public string Key { get; set; }</code>	전송 요청을 인증하기 위한 일회용 암호로 사용할 수 있는 의사 난수(암호화로 보안되지 않음) 키를 생성합니다.

방법	설명
<code>public bool ForceBaseImage { get; set; }</code>	기본 이미지가 강제 적용되는지 여부를 나타내는 값을 가져오거나 설정합니다.
<code>public bool IsLogTruncation { get; set; }</code>	작업이 로그 자르기인지를 나타내는 값을 가져오거나 설정합니다.
<code>public uint LatestEpochSeenByCore { get; set; }</code>	최신 epoch 값을 가져오거나 설정합니다.

#### 표 9. VirtualMachineLocation (namespace Replay.Common.Contracts.Virtualization)

방법	설명
<code>public string Description { get; set; }</code>	이 위치에 대해 사용자가 읽을 수 있는 설명을 가져오거나 설정합니다.
<code>public string Method { get; set; }</code>	VM의 이름을 가져오거나 설정합니다.

#### VolumImageldsCollection (namespace Replay.Core.Contracts.RecoveryPoints)

매개변수 `System.Collections.ObjectModel.Collection<string>`에서 해당 값을 상속합니다.

#### 표 10. VolumeName (namespace Replay.Common.Contracts.Metadata.Storage)

방법	설명
<code>public string GuidName { get; set; }</code>	볼륨의 ID를 가져오거나 설정합니다.
<code>public string DisplayName { get; set; }</code>	볼륨의 이름을 가져오거나 설정합니다.
<code>public string UrlEncode()</code>	URL에서 올바르게 전달할 수 있는 URL로 인코딩된 버전의 이름을 가져옵니다.



**노트:** .NET 4.0 WCF(<https://connect.microsoft.com/VisualStudio/feedback/ViewFeedback.aspx?FeedbackID=413312>)에 경로 이스케이프 문자가 URI 템플릿에서 올바르게 작동하지 않도록 하는 알려진 문제가 있습니다. 볼륨 이름에 '\'와 '?'가 모두 포함되어 있으므로 특수 문자인 '\' 및 '?'를 다른 특수 문자로 대체해야 합니다.

`public string GetMountName()` 볼륨 이미지를 일부 폴더에 탑재할 수 있도록 유효한 이 볼륨의 이름을 반환합니다.

#### VolumeNameCollection (namespace Replay.Common.Contracts.Metadata.Storage)

매개변수 `System.Collections.ObjectModel.Collection<VolumeName>`에서 해당 값을 상속합니다.

방법	설명
<code>public override bool Equals(object obj)</code>	이 인스턴스와 지정된 개체 (VolumeNameCollection 개체여야 함)에 동일한



방법	설명
	값이 있는지 확인합니다 (Object.Equals(Object) 재정의).
public override int GetHashCode()	이 VolumeNameCollection에 대한 해시 코드를 반환합니다(Object.GetHashCode() 재정의).

**표 11. VolumeSnapshotInfo (namespace Replay.Common.Contracts.Transfer)**

방법	설명
public Uri BlockHashesUri { get; set; }	블록 블록의 MD5 해시를 읽을 수 있는 URI를 가져오거나 설정합니다.
public Uri BlockDataUri { get; set; }	블록 데이터 블록을 읽을 수 있는 URI를 가져오거나 설정합니다.

### VolumeSnapshotInfoDictionary (namespace Replay.Common.Contracts.Transfer)

매개변수 System.Collections.Generic.Dictionary<VolumeName, VolumeSnapshotInfo>에서 해당 값을 상속합니다.

## Pretransferscript.ps1

**PreTransferScript**는 스냅샷을 전송하기 전에 에이전트 쪽에서 실행됩니다.

```
# 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

**PostTransferScript**는 스냅샷을 전송한 후 에이전트 쪽에서 실행됩니다.

```
# 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

**PreExportScript**는 내보내기 작업을 수행하기 전에 Core 쪽에서 실행됩니다.

```

# 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.StorageConfiguration
}

```

## Postexportscript.ps1

**PostExportScript**는 내보내기 작업을 수행한 후에 Core 쪽에서 실행됩니다.

 **노트:** 처음 시작한 후 내보낸 에이전트에서 한 번 실행하는 데 사용된 경우 **PostExportScript**에 대한 입력 매개변수가 없습니다. 일반 에이전트에서는 PowerShell 스크립트 폴더에 이 스크립트가 **PostExportScript.ps1**로 포함되어 있습니다.

```
# 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

**PreNightlyJobScript**는 Core 쪽에서 모든 야간 작업 전에 실행되며, 해당 하위 작업을 개별적으로 처리할 수 있는 **\$JobClassName** 매개변수를 사용합니다.

```
# 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 'AgentId:'
$NightlyAttachabilityJobRequestObject.AgentId;
            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 'AgentId:' $RollupJobRequestObject.AgentId;
            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 'AgentId:'
$ChecksumCheckJobRequestObject.AgentId;
        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

**PostNightlyJobScript**는 Core 쪽에서 모든 야간 작업 후에 실행되며, 해당 하위 작업을 개별적으로 처리할 수 있는 **\$JobClassName** 매개변수를 사용합니다.

```

# 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 'AgentId:' $NightlyAttachabilityJobRequestObject.AgentId;
    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 'AgentId:' $RollupJobRequestObject.AgentId;
    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 'AgentId:' $ChecksumCheckJobRequestObject.AgentId;
    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.Id;
        echo 'Volumes: ' $TakeSnapshotResponseObject.Volumes;
    }
    break;
}
}
```

## 샘플 스크립트

PowerShell 스크립트를 실행할 때 관리 사용자를 지원하기 위해 다음 샘플 스크립트가 제공됩니다.  
샘플 스크립트는 다음과 같습니다.


- PreTransferScript.ps1
- PostTransferScript.ps1
- PreExportScript.ps1
- PostExportScript.ps1
- PreNightlyJobScript.ps1
- PostNightlyJobScript.ps1

## 도움말 얻기

### 설명서 및 소프트웨어 업데이트 찾기

AppAssure Core 콘솔에 AppAssure, 어플라이언스 설명서 및 소프트웨어 업데이트로 직접 이동되는 링크가 있습니다. 링크에 액세스하려면 **Appliance(어플라이언스)** 탭을 클릭한 후 **Overall Status(전체 상태)**를 클릭합니다. 소프트웨어 업데이트 및 설명서에 대한 링크는 **Documentation(설명서)** 섹션에 있습니다.

### Dell에 문의하기

 **노트:** 인터넷 연결을 사용할 수 없는 경우에는 제품 구매서, 포장 명세서, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 찾을 수 있습니다.

Dell은 다양한 온라인 및 전화 기반 지원과 서비스 옵션을 제공합니다. 인터넷에 연결되어 있지 않은 경우 구매 송장, 포장 명세서, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 확인할 수 있습니다. 가용성은 국가 및 제품에 따라 다르며, 해당 지역에서 일부 서비스를 이용하지 못할 수도 있습니다. Dell의 영업, 기술 지원 또는 고객 지원 문제는 [software.dell.com/support](https://software.dell.com/support)를 참조하십시오.