Dell DL1000 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.

2015 - 12

개정 A01

목차

1

Dell DL1000 소개

Dell DL1000은 백업 및 복제 기능을 갖춘 통합된 데이터 보호 제품입니다. 백업에서 응용프로그램 데이터를 안정적으로 복구함으로써 가상 시스템 및 실제 시스템을 보호할 수 있습니다. 어플라이언스는 기본으로 제공되는 글로벌 중복 제거, 압축, 암호화 및 특정 개인 또는 공용 클라우드 인프라에 복제 기능을 통해 테라바이트 수준까지 데이터를 처리할 수 있습니다. 데이터 보존(DR) 및 호환성을 위해 서버 응용프로그램 및 데이터를 수분 내에 복구할 수 있습니다.

DL1000은 VMware vSphere 및 Microsoft Hyper-V 개인 및 공용 클라우드에서 멀티 하이퍼바이저 환경을 지원합니다.

Dell DL1000 Core 기술

어플라이언스에는 다음과 같은 기술이 결합되어 있습니다.

- 라이브 복구
- 범용 복구
- 트루 글로벌 중복 제거
- 암호화

라이브 복구

라이브 복구는 VM 또는 서버의 즉시 복구 기술입니다. 이 기술을 사용하면 가상 또는 실제 서버에서 데이터 볼륨에 거의 지속적으로 액세스할 수 있습니다.

DL1000 백업 및 복제 기술은 여러 개의 VM 또는 서버의 동시 스냅샷을 기록하므로 데이터 및 시스템을 즉시에 보호할 수 있습니다. 프로덕션 저장소로 완전하게 복원되기를 기다리지 않고도 복구 지점을 탑재하여 서버를 다시 사용할 수 있습니다.

범용 복구

범용 복구는 무제한으로 유연하게 복원할 수 있습니다. 실제 시스템에서 가상 시스템으로, 가상 시스템에서 가상 시스템으로, 가상 시스템에서 실제 시스템으로, 실제 시스템에서 실제 시스템으로 백업을 복원할 수 있으며 종류가 다른 하드웨어에 운영 체제 미설치 복원을 수행할 수 있습니다.

또한 범용 복구 기술은 여러 가상 시스템에서 플랫폼 간 이동을 촉진합니다. 예를 들어, VMware에서 Hyper-V로 또는 Hyper-V에서 VMware로 이동할 수 있습니다. 이 기술은 응용프로그램 수준, 항목 수준, 개체 수준의 복구에서 구축됩니다(개별 파일, 폴더, 전자 메일, 달력 항목, 데이터베이스 및 응용프로그램).

트루 글로벌 중복 제거

트루 글로벌 중복 제거는 블록 수준의 시스템 증분 백업을 수행하여 중복되는 데이터가 없도록 합니다.

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 일반 버전을 사용합니다. 다중 시스템에서 블록 수준의 백업을 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 1. 트루 글로벌 중복 제거 다이어그램

암호화

DL1000의 암호화 기능을 통해 무단 액세스 및 사용으로부터 백업 및 대기 데이터를 보호하여 데이터 기밀성을 유지할 수 있습니다. 암호화 키를 사용하면 데이터에 액세스하고 암호를 해독할 수 있습니다. 암호화는 스냅샷 데이터에서 인라인으로 수행되며 성능에 영향을 주지 않고 회선 속도로 수행됩니다.

Dell DL1000 데이터 보호 기능

Dell DL1000 Core

Core는 DL1000 배포 아키텍처의 중심이 되는 구성요소입니다. Core는 시스템 백업을 저장하고 관리하며 백업, 복구, 보존, 복제, 보관, 관리를 위한 서비스를 제공합니다. Core는 자체적으로 포함된 네트워크로서 Microsoft Windows Server 2012 R2 Foundation 및 Standard 운영 체제의 64비트 변형을 실행하는 주소 지정 가능한 컴퓨터입니다. 이 어플라이언스는 대상 기반의 인라인 압축, 암호화 및 에이전트에서 수신한 데이터의 데이터 중복 제거를 수행합니다. 그런 다음 어플라이언스에 상주하는 리포지토리에 스냅샷 백업을 저장합니다. 복제에 사용되는 Core는 쌍으로 이루어져 있습니다.

리포지토리는 Core 내의 내부 저장소에 상주합니다. Core는 JavaScript가 활성화된 웹 브라우저에서 다음 URL에 액세스하여 관리합니다. **https://CORENAME:8006/apprecovery/admin**

Dell DL1000 Smart Agent

Smart Agent는 Core에서 보호되는 시스템에 설치됩니다. Smart Agent는 디스크 볼륨에서 변경된 블록을 추적하여 미리 정의된 보호 간격에 따라 변경된 블록의 이미지를 생성합니다. 증분 블록 레벨 스냅샷 영구 방법은 보호되는 시스템에서 Core로 동일한 데이터가 반복해서 복사되지 않도록 합니다.

에이전트가 구성되면 에이전트에서 스마트 기술을 사용하여 보호되는 디스크 볼륨에서 변경된 블록을 지속적으로 추적합니다. 스냅샷이 준비되면, 지능형으로 멀티스레드된 소켓 기반 연결을 사용하여 Core에 신속하게 전송됩니다.

스냅샷 프로세스

DL1000 보호 프로세스는 에이전트 시스템에서 Core로 기본 이미지가 전송될 때 시작됩니다. 이 단계에서는 정상적인 작동 상태에서 시스템의 전체 내용이 네트워크를 통해 전송된 다음 영구 증분 스냅샷이 수행됩니다. Windows용 DL1000 Agent에서는 Microsoft VSS(Volume Shadow Copy Service)를 사용하여 디스크에 응용프로그램 데이터를 정지시켜 파일 시스템 일관 백업 및 응용프로그램 일관 백업을 캡처합니다. 스냅샷이 생성되면 대상 서버의 기록기인 VSS가 디스크에 내용이 기록되지 않도록 합니다. 디스크에 내용 쓰기가 중단된 동안 모든 디스크 I/O 작업은 큐에 대기되고 스냅샷이 완료된 후에만 재개되며, 이미 진행 중인 작업은 완료되고 열려 있는 모든 파일은 닫힙니다. 섀도 복사본 생성 프로세스는 프로덕션 시스템의 성능에 심각한 영향을 주지 않습니다.

DL1000에서는 모든 Windows 내부 기술(예: NTFS, 레지스트리, Active Directory)을 기본적으로 지원하므로 Microsoft VSS를 사용하여 스냅샷 생성 전에 데이터를 디스크에 플러시합니다. 또한 Microsoft Exchange 및 SQL 등과 같은 기타 엔터프라이즈 응용프로그램에서는 VSS 기록기 플러그인을 사용하여 스냅샷이 준비되는 시기 및 사용된 데이터베이스 페이지를 디스크에 플러시하여 데이터베이스를 일관된 트랜잭션 상태로 유지해야 할 시기를 알려주는 알림을 받습니다. 캡처된 데이터는 신속하게 전송되어 Core에 저장됩니다.

복제 - 재난 복구 사이트 또는 서비스 공급자

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 오프사이트 백업 및 재난 복구 서비스를 호스팅하는 클라우드 공급자에 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.

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 장치의 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 이동식 미디어에서 사용 가능한 공간보다 큰 경우 미디어에서 사용 가능한 공간을 기반으로 여러 장치 간에 아카이브를 확장할 수 있습니다. 시드 과정에서 증분 복구 지점이 대상 사이트에 복제됩니다. 대상 Core에서 시드 아카이브를 사용하면 새로 복제된 증분 복구 지점이 자동으로 동기화됩니다.

복구

로컬 사이트 또는 복제된 원격 사이트에서 복구를 수행할 수 있습니다. 로컬 보호 및 선택적 복제와 함께 배포가 안정적인 상태가 되면 DL1000 Core를 통해 복구 보증, 범용 복구 또는 라이브 복구를 사용하여 복구를 수행할 수 있습니다.

RaaS(Recovery-as-a-Service)

관리 서비스 공급자(MSP)는 RaaS(Recovery As A Service)를 제공하기 위한 플랫폼으로 DL1000을 최대한 활용할 수 있습니다. RaaS를 사용하면 고객의 실제 및 가상 서버를 복제하여 클라우드에서 복구를 쉽게 완료할 수 있습니다. 서비스 공급자의 클라우드를 가상 시스템으로 사용하여 복구 검사 또는 실제 복구 작업을 지원할 수 있습니다. 클라우드에서 복구를 수행하려는 고객은 로컬 Core에 있는 보호된 시스템에서 AppAssure 서비스 공급자로의 복제를 구성할 수 있습니다. 재난이 발생하면 MSP가 고객을 위해 가상 시스템을 즉시 스핀업할 수 있습니다.

DL1000는 멀티테넌트가 아닙니다. MSP가 DL1000을 여러 사이트에서 사용할 수 있으며 자체 멀티테넌트 환경을 만들 수 있습니다.

가상화 및 클라우드

DL1000 Core에서는 클라우드를 사용할 수 있으며, 이를 통해 복구 및 아카이브할 때 클라우드의 계산 용량을 이용할 수 있습니다.

DL1000에서는 보호되거나 복제된 시스템을 라이센스가 있는 VMware 또는 Hyper-V 버전으로 내보낼 수 있습니다. 연속 내보내기에서는, 스냅샷이 생성된 후마다 가상 시스템이 증분적으로 업데이트됩니다. 증분 업데이트는 속도가 빠르며 단추 하나를 클릭하여 사용 준비가 되는 대기 클론을 제공합니다. 지원되는 가상 시스템 내보내기는 다음과 같습니다.

- 폴더에서 VMware 워크스테이션 또는 서버
- Vsphere 또는 VMware ESXi 호스트에 직접 내보내기
- Oracle VirtualBox에 내보내기
- Windows Server 2008 (x64)의 Microsoft Hyper-V Server
- Windows Server 2008 R2의 Microsoft Hyper-V Server
- Windows Server 2012 R2의 Microsoft Hyper-V Server

Microsoft Azure, Amazon S3, Rackspace Cloud Block Storage 또는 기타 OpenStack 기반의 클라우드 서비스 등과 같은 플랫폼을 사용하여 리포지토리 데이터를 클라우드에 아카이브할 수 있습니다.

Dell DL1000 배포 아키텍처

DL1000 배포 아키텍처는 로컬 및 원격 구성요소로 구성됩니다. 재난 복구 사이트 또는 오프사이트 복구를 위한 관리 서비스 공급자를 이용하지 않아도 되는 환경에서는 원격 구성요소가 선택사항일 수 있습니다. 기본 로컬 배포는 Core라고 하는 백업 서버와 에이전트라고 하는 하나 이상의 보호되는 시스템으로 구성됩니다. 오프사이트 구성요소는 장애 복구 사이트에서 전체 복구 기능을 제공하는 복제를 통해 활성화됩니다. DL1000 Core에서는 기본 이미지 및 증분 스냅샷을 사용하여 보호되는 에이전트의 복구 지점을 컴파일합니다.

또한 DL1000은 Microsoft Exchange 및 SQL과 해당 데이터베이스 및 로그 파일이 있는지 감지할 수 있기 때문에 응용프로그램 인식형입니다. 백업은 응용프로그램에서 인식되는 블록 수준의 스냅샷을 사용하여 수행됩니다. DL1000은 보호되는 Microsoft Exchange 서버의 로그 자르기를 수행합니다.

다음 다이어그램은 간단한 DL1000 배포를 보여줍니다. DL1000 Agent는 중앙 리포지토리로 구성되어 있는 단일 DL1000 Core에 연결되어 여기에서 보호되는 시스템(예: 파일 서버, 전자 메일 서버, 데이터베이스 서버 또는 가상 시스템)에 설치됩니다. Dell 소프트웨어 라이센스 포털에서는 해당 환경에서 에이전트 및 코어에 대한 라이센스 가입, 그룹 및 사용자를 관리합니다. 라이센스 포털을 통해 사용자가 계정에 로그인하고 활성화하며, 소프트웨어를 다운로드하고, 해당 환경의 라이센스에 따라 에이전트 및 코어를 배포할 수 있습니다.

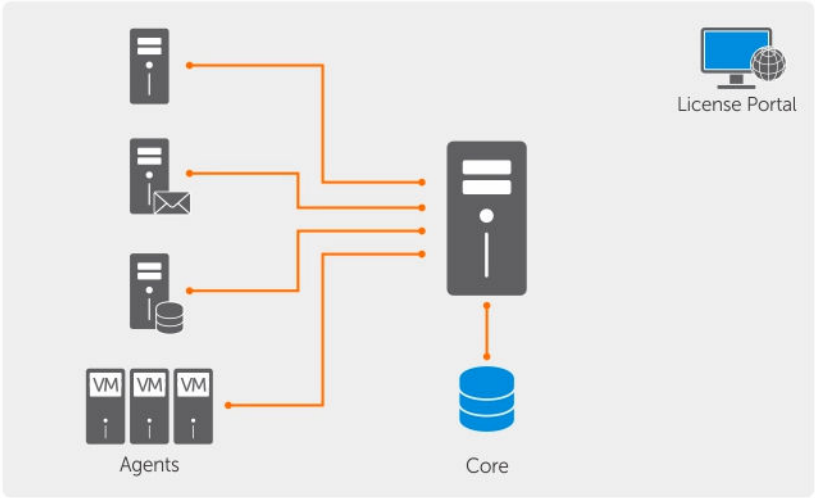

그림 2 . Dell DL1000 배포 아키텍처

다음 다이어그램에서와 같이 여러 개의 DL1000 Core를 배포할 수도 있습니다. 중앙 콘솔에서 여러 개의 코어를 관리합니다.

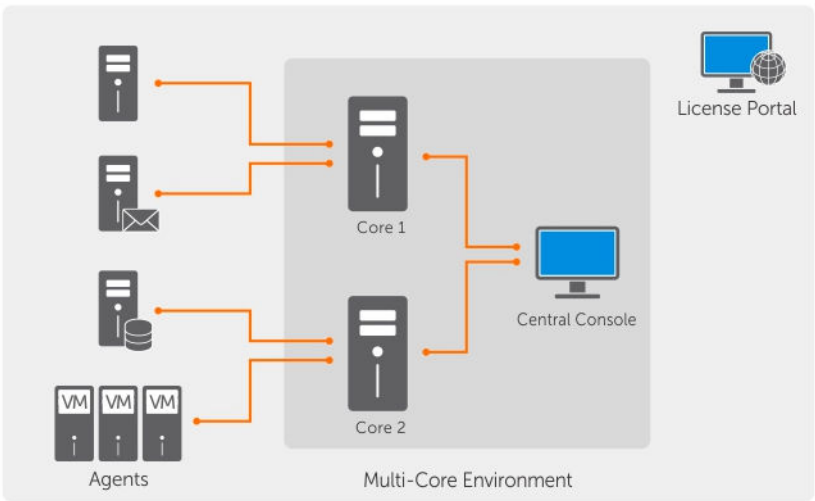

그림 3 . DL1000 다중 코어 배포 아키텍처

기타 필요한 정보

노트: 모든 Dell OpenManage 설명서를 보려면 **dell.com/openmanagemanuals**로 이동하십시오.

노트: 새로운 업데이트가 없는지 **dell.com/support/home**에서 항상 확인하십시오. 업데이트에는 최신 정보가 수록되어 있으므로 다른 문서를 읽기 전에 반드시 먼저 참조하시기 바랍니다.

노트: Dell OpenManage Server Administrator 관련 설명서를 보려면 **dell.com/openmanage/manuals** 를 참조하십시오.

제품 설명서는 다음과 같습니다.

시작 안내서	시스템 기능, 시스템 설정 및 기술 사양의 개요를 제공합니다. 또한 이 문서는 시스템과 함께 제공됩니다.
시스템 플레이스매트	하드웨어를 설정하고 AppAssure 솔루션에 소프트웨어를 설치하는 방법에 대한 정보를 제공합니다.
소유자 매뉴얼	시스템 기능에 대한 정보를 제공하고 시스템 문제 해결 방법 및 시스템 구성 요소 설치 또는 교체 방법을 설명합니다.
배포 안내서	하드웨어 배포 및 어플라이언스의 초기 배포에 대한 정보를 제공합니다.
사용 설명서	시스템의 구성 및 관리에 관한 정보를 제공합니다.
릴리스 정보	Dell DL1000 어플라이언스에서 제품 정보 및 추가 정보를 제공합니다.
상호 운용 안내서	DL1000 어플라이언스의 지원되는 소프트웨어 및 하드웨어는 물론 사용 고려 사항, 권장 사항 및 규칙에 대한 정보를 제공합니다.
OpenManage Server Administrator 사용 설명서	Dell OpenManage Server Administrator를 사용하여 시스템을 관리하는 방법에 대한 정보를 제공합니다.
리소스 미디어	운영 체제, 시스템 관리 소프트웨어, 시스템 업데이트 및 시스템과 함께 구입한 시스템 구성 요소와 관련된 설명서 및 도구를 비롯하여 시스템을 구성 및 관리하는 데 필요한 설명서 및 도구를 제공하는 모든 미디어가 시스템과 함께 제공됩니다.

2

DL1000 활용하기

DL1000 Core 콘솔 액세스

DL1000 Core 콘솔에 액세스하려면 다음을 수행합니다.

1. 브라우저에서 신뢰할 수 있는 사이트를 업데이트합니다.
2. DL1000 Core 콘솔에 원격으로 액세스할 수 있도록 브라우저를 구성합니다. Core 콘솔에 원격으로 액세스하도록 브라우저 구성을 참조하십시오.
3. DL1000 Core 콘솔에 액세스하려면 다음 중 하나를 수행하십시오.
   - 로컬에서 DL1000 Core 서버에 로그온하고 **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

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 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 Core를 호스팅하는 어플라이언스 서버의 IP 주소 또는 호스트 이름*>을 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)**을 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 로그온)**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)**을 선택하고 **OK(확인)**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 호스트하는 어플라이언스 시스템의 호스트 이름 또는 IP 주소를 쉼표로 구분하여 입력합니다(예: *IPAddress*,*host name*).
4. Firefox를 다시 시작합니다.

라이센스 관리

DL1000 라이센스를 Core 콘솔에서 직접 관리할 수 있습니다. 콘솔에서, 라이센스 키를 변경하고 라이센스 서버에 연결할 수 있습니다. 또한 Core 콘솔의 **Licensing(라이센싱)** 페이지에서 Dell AppAssure 라이센스 포털에 액세스할 수 있습니다.

Licensing(라이센싱) 페이지에 다음 정보가 포함되어 있습니다.

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

라이센스 키 변경

라이센스 키를 변경하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성)** → **Licensing(라이센싱)**을 선택합니다.
   Licensing(라이센싱) 페이지가 표시됩니다.
2. **License Details(라이센스 상세정보)** 페이지에서 **Change(변경)**를 클릭합니다.
   Change License Key(라이센스 키 변경) 대화 상자가 표시됩니다.
3. **Change License Key(라이센스 키 변경)** 대화 상자에 새 라이센스 키를 입력한 후 **OK(확인)**를 클릭합니다.

라이센스 포털 서버 연결

Core 콘솔은 포털 서버와 연결하여 라이센스 포털의 변경사항을 업데이트합니다. 포털 서버와의 통신은 지정된 간격에서 자동으로 수행되지만 필요에 따라 통신을 시작할 수 있습니다.
포털 서버를 연결하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성)** → **Licensing(라이센싱)**을 클릭합니다.
   Licensing(라이센싱) 페이지가 표시됩니다.
2. **License Server(라이센스 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 **언어**를 선택합니다.
3. **언어 기본 설정 변경** 창에서 **언어 추가**를 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 이 이름을 변경하려면 몇 가지 단계를 수동으로 수행해야 새 호스트 이름이 적용되고 어플라이언스가 제대로 작동됩니다.

Core 표시 이름을 변경하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 클릭합니다.
2. **General(일반)** 섹션에서 **Change(변경)**를 클릭합니다.
   Display Name(표시 이름) 대화 상자가 표시됩니다.
3. **Display name(표시 이름)** 텍스트 상자에 Core에 대한 새 표시 이름을 입력합니다.
4. **OK(확인)**를 클릭합니다.

야간 작업 시간 변경

Nightly Job(야간 작업) 옵션을 사용하면 Core에서 보호되는 에이전트에 대한 작업(예: 롤업, 연결, 자르기)을 예약할 수 있습니다.

야간 작업 시간을 조정하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 선택합니다.
2. **Nightly Jobs(야간 작업)** 섹션에서 **Change(변경)**를 클릭합니다.
   Nightly Jobs(야간 작업) 대화 상자가 표시됩니다.
3. **Nightly Jobs Time(야간 작업 시간)** 텍스트 상자에 새 시작 시간을 입력합니다.
4. **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 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 클릭합니다.
2. **Transfer Queue(전송 큐)** 섹션에서 **Change(변경)**를 클릭합니다.
   Transfer Queue(전송 큐) 대화 상자가 표시됩니다.
3. **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.
4. **Maximum Retries(최대 재시도 횟수)** 텍스트 상자에 값을 입력하여 최대 재시도 횟수를 업데이트합니다.
5. **OK(확인)**를 클릭합니다.

클라이언트 시간 제한 설정 조정

Client Timeout Settings(클라이언트 시간 제한 설정)는 클라이언트에 연결할 때 제한 시간이 초과되기 전에 서버가 대기하는 시간(초 또는 분 단위)을 지정합니다.

클라이언트 시간 제한 설정을 조정하려면 다음을 수행합니다.

1. Core 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 선택합니다.
2. **Client Timeout Settings Configuration(클라이언트 시간 제한 설정 구성)** 섹션에서 **Change(변경)**를 클릭합니다.

   Client Timeout Settings(클라이언트 시간 제한 설정) 대화 상자가 표시됩니다.
3. **Connection Timeout(연결 시간 제한)** 텍스트 상자에 연결 시간을 초과하기 전의 시간(분 및 초)을 입력합니다.
4. **Read/Write Timeout(읽기/쓰기 시간 제한)** 대화 상자에 읽기/쓰기 이벤트 동안 시간이 초과되기 전에 경과할 시간(분 및 초)을 입력합니다.
5. **OK(확인)**를 클릭합니다.

중복 제거 캐시 설정 구성

글로벌 중복 제거 기능을 사용하면 백업된 데이터에 필요한 디스크 저장 공간의 양을 줄일 수 있습니다. DVM(Deduplication Volume Manager)은 일련의 저장소 위치를 하나의 리포지토리에 결합합니다. 중복 캐시에는 고유한 블록에 대한 참조가 포함되어 있습니다. 기본적으로, 중복 캐시의 크기는 1.5 GB입니다. 중복 정보 isso가 크고 중복 제거 캐시가 가득 차 있으면, 리포지토리는 새로 추가된 데이터를 중복 제거할 수 없게 됩니다. 이 경우 Core 콘솔에서 중복 제거 캐시 구성을 변경하여 중복 제거 캐시의 크기를 늘릴 수 있습니다.

중복 제거 캐시 설정을 구성하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 클릭합니다.
2. **Deduplication Cache Configuration(중복 제거 캐시 구성)** 섹션에서 **Change(변경)**를 클릭합니다.

   Deduplication Cache Configuration(중복 제거 캐시 구성) 대화 상자가 표시됩니다.
3. **Primary Cache Location(기본 캐시 위치)** 텍스트 상자에 업데이트된 기본 캐시 위치를 입력합니다.
4. **Secondary Cache Location(보조 캐시 위치)** 텍스트 상자에 업데이트된 보조 캐시 위치를 입력합니다.
5. **Metadata Cache Location(메타데이터 캐시 위치)** 텍스트 상자에 업데이트된 메타데이터 캐시 위치를 입력합니다.
6. **OK(확인)**를 클릭합니다.

   노트: 변경 내용을 적용하려면 Core 서비스를 다시 시작해야 합니다.

엔진 설정 수정

엔진 설정을 수정하려면 다음을 수행합니다.

1. Core 콘솔을 탐색하고 **Configuration(구성) → Settings(설정)**를 클릭합니다.
2. **Replay Engine Configuration(재생 엔진 구성)** 섹션에서 **Change(변경)**를 클릭합니다.

   Replay Engine Configuration(재생 엔진 구성) 대화 상자가 표시됩니다.
3. **Replay Engine Configuration(재생 엔진 구성)** 대화 상자에서 **IP 주소**를 지정합니다. 다음 중 하나를 선택합니다.
   - TCP/IP에서 기본 IP 주소를 사용하려면 **Automatically Determined(자동으로 결정)**를 클릭합니다.
   - IP 주소를 수동으로 입력하려면 **Use a specific IP Address(특정 IP 주소 사용)**를 클릭합니다.
4. 다음 설명과 같이 구성 정보를 입력합니다.

텍스트 상자	설명
선호 포트	포트 번호를 입력하거나 기본 설정을 적용합니다. 기본 포트는 8007입니다. 포트는 엔진의 통신 채널을 지정하는 데 사용됩니다.
관리 그룹	관리 그룹에 대한 새 이름을 입력합니다. 기본 이름은 **BUILTIN\Administrators**입니다.
최소 비동기 I/O 길이	값을 입력하거나 기본 설정을 선택합니다. 이는 최소 비동기 입력/출력 길이를 나타냅니다. 기본 설정은 65536입니다.
수신 버퍼 크기	인바운드 버퍼 크기를 입력하거나 기본 설정을 선택합니다. 기본 설정은 8192입니다.
보내기 버퍼 크기	아웃바운드 버퍼 크기를 입력하거나 기본 설정을 선택합니다. 기본 설정은 8192입니다.
읽기 시간 제한	읽기 시간 제한 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:00:30입니다.
쓰기 시간 제한	쓰기 시간 제한 값을 입력하거나 기본 설정을 선택합니다. 기본 설정은 00:00:30입니다.

5. **No Delay(지연 안 함)**를 선택합니다.
6. **OK(확인)**를 클릭합니다.

배포 설정 수정

배포 설정을 수정하려면 다음을 수행합니다.

1. Core 콘솔을 탐색하고 **Configuration(구성)** 탭을 클릭한 후 **Settings(설정)**를 클릭합니다.
2. **Deploy Settings(배포 설정)** 창에서 **Change(변경)**를 클릭합니다.
   Deploy Settings(배포 설정) 대화 상자가 표시됩니다.
3. **Agent Installer Name(에이전트 설치 프로그램 이름)** 텍스트 상자에 에이전트 실행 파일의 이름을 입력합니다. 기본값은 **Agentweb. exe**입니다.
4. **Core Address(Core 주소)** 텍스트 상자에 코어의 주소를 입력합니다.
5. **Failed Receive Timeout(수신 실패 시간 제한)** 텍스트 상자에 제한 시간이 초과될 때까지 활동 없이 대기하는 시간(분)을 입력합니다.
6. **Max Parallel Installs(최대 병렬 설치)** 텍스트 상자에 병렬로 설치할 수 있는 최대 설치 수를 입력합니다.
7. 다음 설정(선택사항) 중 하나 또는 둘 다 선택합니다.
   - 설치 후 자동 재부팅
   - 배포 후 보호
8. **OK(확인)**를 클릭합니다.

데이터베이스 연결 설정 수정

데이터베이스 연결 설정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔을 탐색하고 **Configuration(구성)** → **Settings(설정)**를 클릭합니다.
2. **Database Connection Settings(데이터베이스 연결 설정)** 섹션에서 다음 중 하나를 수행합니다.
   - 기본 구성을 복원하려면 **Restore Default(기본값 복원)**를 클릭합니다.
   - 데이터베이스 연결 설정을 수정하려면 **Change(변경)**를 클릭합니다.

   변경을 클릭하면 **Database Connection Settings(데이터베이스 연결 설정)** 대화 상자가 나타납니다.

3. 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(선택사양)	데이터베이스 연결 설정에 액세스하고 관리하기 위한 사용자 이름을 입력합니다. 이는 데이터베이스 연결에 액세스하기 위한 로그인 자격 증명을 지정하는 데 사용됩니다.
암호(선택사양)	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.

4. **Test Connection(연결 테스트)**을 클릭하여 설정을 확인합니다.
5. **Save(저장)**를 클릭합니다.

이벤트 관리

Core에는 Core 또는 백업 작업에서 심각한 문제가 발생할 때 관리자에게 알려줄 수 있는 일련의 이벤트가 미리 정의되어 있습니다.

Events(이벤트) 탭에서 알림 그룹, 전자 메일 SMTP 설정, 서버 설정, 활성화된 추적 로그, 클라우드 구성, 반복 감소 및 이벤트 보존을 관리할 수 있습니다.

Notification Groups(알림 그룹) 옵션을 사용하여 다음과 같이 알림 그룹을 관리할 수 있습니다.

- 다음에 대한 경고를 생성할 이벤트를 지정할 수 있습니다.
  - 클러스터
  - 연결 기능
  - 작업
  - 라이센싱
  - 로그 자르기
  - 아카이브
  - Core 서비스
  - 내보내기
  - 보호
  - 복제
  - 롤백
- 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. Core 콘솔에서 **Configuration(구성)** → **Events(이벤트)**를 선택합니다.
2. **Add Group(그룹 추가)**을 클릭합니다.
   Add Notification Group(알림 그룹 추가) 대화 상자가 열리고 다음과 같은 두 개의 패널이 표시됩니다.
   - **경고 활성화**
   - **알림 옵션**

경고 활성화

경고를 활성화하면 보고서를 로그하고 생성하며 경고를 설정할 일련의 시스템 이벤트를 정의할 수 있습니다.

노트: 모든 이벤트에 대한 경고를 생성하려면 **All Alerts(모든 경고)**를 선택합니다.

- 오류, 경고, 정보용 메시지 또는 이러한 항목을 조합하여 관련 경고를 생성하려면 다음 중 하나를 선택합니다.
  - 빨간색 삼각형 아이콘(오류)
  - 노란색 삼각형 아이콘(경고)
  - 파란색 원(정보)
  - 곡선 화살표(기본값 복원)
- 특정 이벤트에 대한 경고를 생성하려면 관련 그룹 옆에 있는 **>** 기호를 클릭하고 해당 확인란을 선택하여 경고를 활성화합니다.

알림 구성 옵션

1. **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. 아래와 같이 참조 및 숨은 참조와 함께 여러 개의 전자 메일 주소를 구분하여 입력할 수 있습니다. • **받는 사람:** • **참조:** • **숨은 참조:**
Windows 이벤트 로그로 알림	Windows 이벤트 로그를 통해 보고되는 경고 알림을 받으려면 이 옵션을 선택합니다.
sys logd로 알림	sys logd를 통해 보고되는 경고를 받으려면 이 옵션을 선택합니다. 다음과 같은 텍스트 상자에 sys logd의 상세정보를 입력합니다. • **호스트 이름:** • **포트: 1**
팝업 경고로 알림	화면 오른쪽 하단에 팝업으로 경고를 받으려면 이 옵션을 선택합니다.

2. **OK(확인)**를 클릭합니다.

다음과 같은 메시지가 표시됩니다. **The Group name cannot be changed after the creation of the Notification Group. are you sure you want to use this name?(알림 그룹이 생성된 후에는 그룹 이름을 변경할 수 없습니다. 이 이름을 사용하시겠습니까?)**

- 그룹 이름을 저장하려면 **Yes(예)**를 클릭합니다.
- 그룹 이름을 변경하려면 **No(아니오)**를 클릭합니다. **Notification Options(알림 옵션)** 창으로 돌아가서, 그룹 이름과 기타 알림 그룹 설정을 업데이트하고 변경된 내용을 저장합니다.

전자 메일 서버 구성

노트: 전자 메일 경고 메시지를 보내기 전에 **Notify by email(전자 메일로 알림)** 옵션을 활성화하고 알림 그룹 설정을 구성해야 합니다.

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

1. Core 콘솔에서 **Configuration(구성)** → **Events(이벤트)**를 클릭합니다.
2. **Email Settings(전자 메일 설정)** 창에서 **SMPT server(SMPT 서버)**를 클릭합니다.
   SMTP Server Settings(SMTP 서버 설정) 대화 상자가 표시됩니다.
3. 다음과 같이 전자 메일 서버의 상세정보를 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**).
보낸 사람	반송 전자 메일 주소를 입력합니다. 이는 전자 메일 알림 템플릿의 반송 전자 메일 주소를 지정하는 데 사용됩니다(예: **noreply@localhost.com**).
사용자 이름	전자 메일 서버의 사용자 이름을 입력합니다.
암호	전자 메일 서버에 액세스하기 위한 암호를 입력합니다.
포트	포트 번호를 입력합니다. 이 번호는 전자 메일 서버의 포트를 식별하는 데 사용됩니다(예: Gmail의 경우 포트 587). 기본값은 25입니다.
시간 제한(초)	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.
TLS	메일 서버에서 TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer)과 같은 보안 연결을 사용하는 경우 이 옵션을 선택합니다.

4. **Send Test Email(테스트 전자 메일 보내기)**을 클릭하여 다음을 수행합니다.
   a. Send Test Email(테스트 전자 메일 보내기) 대화 상자에서, 테스트 메시지의 대상 전자 메일 주소를 입력하고 **Send(보내기)**를 클릭합니다.
   b. 테스트 메시지에 실패할 경우, 오류 대화 상자와 **Send Test Email(테스트 전자 메일 보내기)** 대화 상자를 종료하고 전자 메일 서버 구성 설정을 수정합니다. 4단계를 반복합니다.
   c. **OK(확인)**를 클릭하여 확인합니다.
   d. 테스트 전자 메일 메시지가 전송되었는지 확인합니다.
   e. SMTP Server Settings(SMTP 서버 설정) 대화 상자로 돌아가서 **Save(저장)**를 클릭하여 대화 상자를 닫고 설정을 저장합니다.

전자 메일 알림 템플릿 구성

이벤트에 대한 전자 메일 알림을 받으려면 전자 메일 서버 및 전자 메일 알림 템플릿을 구성해야 합니다.

노트: 전자 메일 경고 메시지를 받으려면, 알림 그룹 설정을 구성하고 **Notify by email(전자 메일로 알림)** 옵션을 활성화합니다.

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

1. Core 콘솔에서 **Configuration(구성)** → **Events(이벤트)**를 클릭합니다.
2. **Email Settings(전자 메일 설정)** 창에서 **Change(변경)**를 클릭합니다.
   Edit Email Notification Configuration(전자 메일 알림 구성 편집) 대화 상자가 나타납니다.
3. **Enable email notifications(전자 메일 알림 활성화)**를 선택하고 다음과 같이 전자 메일 서버의 상세정보를 입력합니다.

텍스트 상자	설명
전자 메일 제목	전자 메일 템플릿의 제목을 입력합니다. 이는 전자 메일 알림 템플릿의 제목을 정의하는 데 사용됩니다(예: `<hostname> - <level> <name>`).
Email(이메일)	이벤트가 발생한 경우 해당 이벤트를 설명하는 템플릿의 본문과 심각도에 대한 정보를 입력합니다.

4. **Send Test Email(테스트 전자 메일 보내기)**을 클릭하여 다음을 수행합니다.
   a. Send Test Email(테스트 전자 메일 보내기) 대화 상자에서, 테스트 메시지의 대상 전자 메일 주소를 입력하고 **Send(보내기)**를 클릭합니다.
   b. 테스트 메시지에 실패할 경우, 오류 대화 상자와 Send Test Email(테스트 전자 메일 보내기) 대화 상자를 종료하고 **OK(확인)**를 클릭하여 현재 전자 메일 템플릿 설정을 저장한 후에 전자 메일 서버 설정을 수정합니다. 전자 메일 서버 및 전자 메일 알림 템플릿 구성을 참조하십시오. 전자 메일 계정의 암호를 다시 입력해야 합니다. 설정을 저장하고 4단계로 돌아갑니다.
   c. **OK(확인)**를 클릭하여 확인합니다.
   d. 테스트 전자 메일 메시지가 전송되었는지 확인합니다.
   e. **Edit Email Notification Configuration(전자 메일 알림 구성 편집)** 대화 상자로 돌아가서 **OK(확인)**를 클릭하여 대화 상자를 닫고 설정을 저장합니다.

반복 감소 구성

반복 감소를 구성하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성)** → **Events(이벤트)**를 클릭합니다.
2. **Repetition Reduction(반복 감소)** 섹션에서 **Change(변경)**를 클릭합니다.
   Enable Repetition Reduction(반복 감소 활성화) 대화 상자가 나타납니다.
3. **Enable Repetition Reduction(반복 감소 활성화)**을 선택합니다.
4. **Store events for(이벤트 저장 기간)** 텍스트 상자에서, 반복 감소를 위해 이벤트를 저장할 기간(분)을 입력합니다.
5. **OK(확인)**를 클릭합니다.

이벤트 보존 구성

이벤트 보존을 구성하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Settings(설정)**를 클릭합니다.
2. **Database Connection Settings(데이터베이스 연결 설정)**에서 **Change(변경)**를 클릭합니다.
   Database Connection Settings(데이터베이스 연결 설정) 대화 상자가 표시됩니다.
3. **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.
4. **Save(저장)**를 클릭합니다.

리포지토리 관리

리포지토리는 보호되는 워크스테이션 및 서버에서 캡처되는 스냅샷을 저장합니다. DL1000의 리포지토리는 미리 구성되어 있습니다. 이 리포지토리는 시스템의 내부 저장소에 상주합니다.

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.

리포지토리 상세정보 보기

리포지토리 상세정보를 보려면 다음을 수행합니다.

1. Core 콘솔에서 **Configuration(구성) → Repositories(리포지토리)**를 클릭합니다.
2. 상세정보를 볼 리포지토리의 **Status(상태)** 열 옆에 있는 **>**를 클릭합니다.
3. 리포지토리의 상세정보에는 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 검사

Core 콘솔은 오류가 발생했을 때 리포지토리 볼륨의 진단 검사를 수행할 수 있습니다. Core 오류는 비정상적으로 종료되었거나 하드웨어 장애로 인해 발생할 수 있습니다.

노트: 이 절차는 진단용으로만 수행해야 합니다.

리포지토리를 검사하려면 다음을 수행하십시오.

1. **Configuration(구성) → Repositories(리포지토리)**를 클릭합니다.
2. **Actions(작업)** 단추 아래의 Compression Ratio(압축 비율) 열 옆에 있는 Settings(설정) 아이콘을 클릭합니다.
3. **Check(검사)**를 클릭합니다.
   Check Repository(리포지토리 검사) 대화 상자가 표시됩니다.

4. **Check Repository(리포지토리 검사)** 대화 상자에서 **Check(검사)**를 클릭합니다.

   노트: 검사를 수행하면 이 리포지토리와 연관된 모든 활성 작업은 취소됩니다. 검사가 시작되기 전에, 검사를 계속 진행할지 묻는 메시지가 표시됩니다. 복구 지점 캐시를 다시 작성하는 것이 좋습니다. 검사에 실패하면 아카이브에서 리포지토리를 복원해야 합니다.

보안 관리

DL1000은 보호되는 시스템의 백업에 액세스할 수 없도록 강력한 암호화 기능을 제공합니다. 암호화 키를 보유한 사용자만 데이터에 액세스하여 암호를 해독할 수 있습니다. 암호화 기능은 성능에는 영향을 주지 않습니다. 키 보안 개념 및 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.

암호화 키 추가

암호화 키를 추가하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Add Encryption Key(암호화 키 추가)**를 클릭합니다.
   Create Encryption Key(암호화 키 생성) 대화 상자가 표시됩니다.
3. **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.

4. **OK(확인)**를 클릭합니다.

   주의: 암호를 보호하는 것이 좋습니다. 암호를 분실할 경우 데이터를 복구할 수 없습니다.

암호화 키 편집

암호화 키를 편집하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
   Encryption Keys(암호화 키) 화면이 표시됩니다.
2. 편집할 암호화 키의 이름 옆에 있는 **>**를 클릭한 후 **Edit(편집)**를 클릭합니다.
   Edit Encryption Key(암호화 키 편집) 대화 상자가 표시됩니다.
3. **Edit Encryption Key(암호화 키 편집)** 대화 상자에서 이름을 편집하거나 암호화 키에 대한 설명을 수정합니다.

4. **OK(확인)**를 클릭합니다.

암호화 키 암호 변경

암호화 키 암호를 변경하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
2. 편집할 암호화 키의 이름 옆에 있는 **>**를 클릭한 후 **Change Passphrase(암호 변경)**를 클릭합니다.
   Change Passphrase(암호 변경) 대화 상자가 표시됩니다.
3. **Change Passphrase(암호 변경)** 대화 상자에 암호화에 대한 새 암호를 입력한 후 암호를 다시 입력하여 입력한 내용을 확인합니다.
4. **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 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Import(가져오기)**를 클릭합니다.
   Import Key(키 가져오기) 대화 상자가 표시됩니다.
3. **Import Key(키 가져오기)** 대화 상자에서 **Browse(찾아보기)**를 클릭하여 가져올 암호화 키를 찾고 **Open(열기)**을 클릭합니다.
4. **OK(확인)**를 클릭합니다.

암호화 키 내보내기

암호화 키를 내보내려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
2. 내보낼 암호화 키의 Configuration(구성) 드롭다운 메뉴에서 **Export(내보내기)**를 선택합니다.
   Export Key(키 내보내기) 대화 상자가 표시됩니다.
3. **Export Key(키 내보내기)** 대화 상자에서 **Save File(파일 저장)**을 클릭하여 안전한 위치에 암호화 키를 저장하고 보관합니다.
4. **OK(확인)**를 클릭합니다.

암호화 키 제거

암호화 키를 제거하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Configuration(구성) → Security(보안)**를 클릭합니다.
2. 제거할 암호화 키의 Configuration(구성) 드롭다운 메뉴에서 **Remove(제거)**를 선택합니다.
   Remove Key(키 제거) 대화 상자가 표시됩니다.
3. **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.

클라우드 유형	텍스트 상자	설명
	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.
	인증 URL	이 계정의 인증 URL을 입력합니다.
Rackspace Cloud Block Storage	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.

DL1000 모니터링

Appliance(어플라이언스) 탭의 **Overall Status(전반적인 상태)** 페이지에서 DL1000 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.

또한 Overall Status(전반적인 상태) 페이지는 각 하위 시스템의 세부 정보를 드릴다운하는 도구에 연결할 수 있는 링크를 제공합니다. 이 링크는 경고 또는 오류 문제를 해결할 때 유용합니다. 어플라이언스 하드웨어 및 스토리지 하드웨어 하위 시스템에 있는 **시스템 관리자** 링크를 클릭하면 하드웨어 관리에 사용되는 시스템 관리자 응용프로그램에 로그인하라는 메시지가 표시됩니다. 시스템 관리자 응용프로그램에 대한 자세한 내용은 **dell.com/support/manuals**에서 *OpenManage Server Administrator사용 설명서*를 참조하십시오.

DL1000 업그레이드

노트: Dell 라이센스 활성화 포털에서 사용 가능한 최신 AppAssure 버전을 다운로드하는 것이 좋습니다.

노트: 기타 소프트웨어 업그레이드의 경우 최신 버전으로 업그레이드 알림이 전송됩니다.

DL1000 복구

노트: 복구 프로세스를 시작하기 전에 Core 서비스를 중지해야 합니다.

신속한 어플라이언스 자동 복구

신속한 어플라이언스 자동 복구(RASR)는 운영 체제 드라이브가 공장 기본 이미지로 다시 작성되는 운영 체제 미설치 복원 프로세스입니다.
다음과 같이 RASR을 수행합니다.

노트: Dell은 어플라이언스를 설정한 후 RASR USB 키를 생성할 것을 권장합니다. RASR USB 키를 생성하려면 RASR USB 키 생성을 참조하십시오.

1. 생성된 RASR USB 키를 삽입합니다.
2. RASR USB 키를 통해 어플라이언스를 다시 부팅합니다.
3. **Rapid Appliance Self Recovery(신속한 어플라이언스 자동 복구)**를 클릭합니다.
   시작 화면이 표시됩니다.
4. **Next(다음)**를 클릭합니다.
   Prerequisites(전제조건) 확인 화면이 표시됩니다.

   노트: RASR 수행하기 전에 모든 하드웨어 및 기타 전제조건을 확인합니다.
5. **Next(다음)**를 클릭합니다.
   세 가지 옵션과 함께 **Recovery Mode Selection(복구 모드 선택)** 화면이 표시됩니다.
   - **시스템 복구**
   - **Windows 복구 마법사**
   - **공장 기본 재설정**
6. **Factory Reset(공장 기본 재설정)** 옵션을 선택합니다.
   이 옵션을 사용하면 공장 기본 이미지에서 운영 체제 디스크가 복구됩니다.
7. **Next(다음)**를 클릭합니다.
   Storage Configuration(저장소 구성) 화면이 표시됩니다.
8. **OS Recovery(OS 복구)** 화면에 다음과 같은 경고 메시지가 대화 상자에 표시됩니다. `This operation will recover the operating system. All OS disk data will be overwritten.`(이 작업을 수행하면 운영 체제가 복구됩니다. 모든 OS 디스크 데이터가 덮어써집니다.)
9. **Yes(예)**를 클릭합니다.
   운영 체제 디스크가 공장 기본 재설정으로 다시 복원되기 시작합니다.
10. **Finish(마침)**를 클릭합니다.

RASR USB 키 만들기

노트: 소프트웨어 초기 설치 후에 **AppAssure Appliance Configuration(AppAssure 어플라이언스 구성) 마법사**가 자동으로 시작됩니다. **Appliance(어플라이언스)** 탭의 상태 아이콘은 노란색입니다.

RASR USB 키를 만들려면 다음을 수행합니다.

1. **Appliance(어플라이언스)** 탭으로 이동합니다.
2. 왼쪽 탐색 창에서**Appliance(어플라이언스)** → **Backup(백업)**을 선택합니다.
   Create RASR USB Drive(RASR USB 드라이브 생성) 창이 표시됩니다.

노트: RASR 키 생성을 시도하기 전에 16 GB 이상의 USB 키를 삽입합니다.

3. 16 GB 이상의 USB 키를 삽입한 후에 **Create RASR USB Drive now(RASR USB 드라이브 지금 생성)**를 클릭합니다.

   Prerequisite Check(필수 요소 확인) 메시지가 표시됩니다.

   필수 요소를 확인한 후에는 **Create the RASR USB Drive(RASR USB 드라이브 생성)** 창에 USB 드라이브 생성에 필요한 최소 크기와 **가능한 대상 경로 목록**이 표시됩니다.

4. 대상을 선택하고 **Create(생성)**를 클릭합니다.

   경고 대화상자가 표시됩니다.

5. **Yes(예)**를 클릭합니다.

   RASR USB 드라이브 키가 생성됩니다.

6. **노트:** USB 키를 분리할 시 USB 드라이브 또는 Windows 꺼내기 드라이브 기능을 사용합니다. 그렇지 않은 경우, USB 키의 컨텐츠가 손상되어 USB 키가 예상대로 작동되지 않을 수 있습니다.

   나중에 사용할 수 있도록 키를 분리하고 레이블을 부착하여 보관해 둡니다.

3

워크스테이션 및 서버 보호

워크스테이션 및 서버 보호 정보

DL1000을 사용하여 데이터를 보호하려면 Core 콘솔에서 보호할 워크스테이션과 서버(예: Exchange Server, SQL Server 또는 Linux 서버)를 추가해야 합니다.

노트: 이 장에서는 *시스템*이라는 단어가 해당 시스템에 설치된 AppAssure Agent 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 보호를 참조하십시오.

에이전트 배포(강제 설치)

DL1000을 사용하면 개별 Windows 시스템에 AppAssure Agent 설치 프로그램을 설치하여 시스템을 보호할 수 있습니다. 에이전트에 설치 프로그램을 강제 설치하려면 다음 단계를 완료하십시오. 에이전트를 여러 시스템에 동시에 배포하려면 다중 시스템에 배포를 참조하십시오.

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

에이전트를 배포하려면 다음을 수행하십시오.

1. Core 콘솔의 왼쪽 탐색 영역에서 **Protected Machines(보호되는 시스템)**를 클릭합니다.
2. **Actions(작업)** → **Deploy Agent(에이전트 배포)**를 클릭합니다.
   Deploy Agent(에이전트 배포) 대화 상자가 표시됩니다.
3. **Deploy Agent(에이전트 배포)** 대화 상자에 다음 표에 설명된 대로 로그온 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.

시스템 보호

이 항목에서는 지정하는 시스템에서 데이터를 보호하는 방법을 설명합니다.

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

시스템을 보호하려면 다음을 수행하십시오.

1. AppAssure Agent 소프트웨어가 설치되어 있는 시스템을 다시 부팅합니다(이미 다시 부팅하지 않은 경우).
2. Core 시스템의 Core 콘솔에 있는 단추 모음에서**Protect(보호)** → **Protect Machine(시스템 보호)**을 클릭합니다.

   Protect Machine Wizard(시스템 보호 마법사)가 나타납니다.
3. **Welcome(시작)** 페이지에서 적절한 설치 옵션을 선택합니다.
   - 리포지토리를 정의할 필요가 없거나 암호화를 설정할 필요가 없을 경우에는 **Typical(일반)**을 선택합니다.
   - 나중에 **Protect Machine Wizard(시스템 보호 마법사)**에 **Welcome(시작)** 페이지가 표시되지 않도록 하려면 **Skip this Welcome page the next time the wizard opens(다음에 마법사를 열 때 이 시작 페이지 건너뛰기)** 옵션을 선택합니다.
4. **Next(다음)**를 클릭합니다.
5. **Connection(연결)** 페이지에서, 아래 표에 설명된 대로 연결할 시스템에 대한 정보를 입력합니다.

텍스트 상자	설명
호스트	보호할 시스템의 호스트 이름 또는 IP 주소입니다.
포트	AppAssure 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.

6. **Next(다음)**를 클릭합니다. 다음에 **Protect Machine Wizard(시스템 보호 마법사)**에 **Protection(보호)** 페이지가 나타나면 7단계로 건너뜁니다.

노트: 다음에 **Protect Machine Wizard(시스템 보호 마법사)**에 **Install Agent(에이전트 설치)** 페이지가 나타나면 이는 지정된 시스템에 Agent 소프트웨어가 아직 설치되어 있지 않음을 나타냅니다. **Next(다음)**를 클릭하여 Agent 소프트웨어를 설치합니다. Agent 소프트웨어는 보호할 시스템에 설치하고 다시 시작해야 Core에 백업할 수 있습니다. 설치 프로그램이 에이전트 시스템을 다시 부팅하도록 하려면 **After installation, restart the machine automatically (recommended)(설치 후에 자동으로 시스템 다시 시작(권장))** 옵션을 선택한 후에 **Next(다음)**를 클릭합니다.

7. **Connect(연결)** 대화 상자에 지정한 호스트 이름이나 IP 주소가 이 텍스트 필드에 나타납니다. 선택적으로, Core 콘솔에 표시할 시스템의 새 이름을 입력할 수도 있습니다.
8. 적절한 보호 일정을 선택합니다.
   - 기본 보호 일정을 사용하려면 **Schedule Settings(일정 설정)** 옵션에서 **Default protection (3 hour snapshots of all volumes)(기본 보호(3시간마다 모든 볼륨의 스냅샷))**를 선택합니다. 기본 보호 일정을 사용하면, Core가 3시간 마다 한 번씩 에이전트 시스템의 스냅샷을 생성합니다. 에이전트 시스템의 스냅샷을 1시간마다(최소) 생성할 수 있습니다. 마법사를 닫은 후에 특정 에이전트 시스템의 Summary(요약) 탭으로 이동하여 보호할 볼륨을 선택하고 언제든지 보호 설정을 변경할 수 있습니다.
   - 다른 보호 일정을 정의하려면 **Schedule Settings(일정 설정)** 옵션에서 **Custom protection(사용자 지정 보호)**을 선택합니다.
9. 다음 중 하나를 선택합니다.
   - **Protect Machine Wizard(시스템 보호 마법사)**에서 Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 **Finish(마침)**를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.
   - 시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 AppAssure Core의 리포지토리에 전송됩니다.
   - **Protect Machine Wizard(시스템 보호 마법사)**에서 Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 사용자 지정 보호 일정을 설정합니다. 사용자 지정 보호 일정을 정의하는 방법에 대해서는 '사용자 지정 보호 일정 생성'을 참조하십시오.
   - **Protect Machine Wizard(시스템 보호 마법사)**에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 12단계를 계속 진행하여 리포지토리 및 암호화 옵션을 확인합니다.
   - **Protect Machine Wizard(시스템 보호 마법사)**에서 Advanced(고급) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하여 10단계를 계속 진행하여 보호할 볼륨을 선택합니다.
10. **Protection Volumes(보호 볼륨)** 페이지에서, 보호할 에이전트 시스템에 있는 볼륨을 선택합니다. 보호하지 않을 볼륨이 나열될 경우 Check(확인) 열을 클릭하여 선택 항목을 지우고 **Next(다음)**를 클릭합니다.

    노트: 시스템 예약 볼륨과 운영 체제가 포함된 볼륨을 보호하는 것이 좋습니다(일반적으로 C 드라이브).
11. **Protection Schedule(보호 일정)** 페이지에서 사용자 지정 보호 일정을 정의합니다.
12. **Repository(리포지토리)** 페이지에서 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
13. **Next(다음)**를 클릭합니다.

    Encryption(암호화) 페이지가 나타납니다.
14. 선택적으로, 암호화를 활성화하려면 **Encryption(암호화)** 페이지에서 **Enable Encryption(암호화 활성화)**을 선택합니다.

    Encryption(암호화) 페이지에 **Encryption key(암호화 키)** 필드가 나타납니다.

    노트: 암호화를 활성화하면 이 에이전트 시스템에서 보호되는 모든 볼륨에 있는 데이터에 적용됩니다. Core 콘솔의 **Configuration(구성)** 탭에서 나중에 이 설정을 변경할 수 있습니다.

주의: AppAssure에서는 CBC(Cipher Block Chaining) 모드에서 256바이트 키와 함께 AES 256비트 암호화를 사용합니다. 암호화 사용은 선택사항이지만, 암호화 키를 설정하고 정의하는 암호를 보호하는 것을 권장합니다. 암호는 데이터 복구에 매우 중요하므로 안전한 위치에 저장해 두십시오. 암호가 없으면 데이터를 복구할 수 없습니다.

15. 다음 표에 설명된 대로 정보를 입력하여 Core의 암호화 키를 추가합니다.

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다.
설명	설명을 입력하여 암호화 키에 대한 추가 세부 정보를 제공합니다.
암호	액세스 제어에 사용되는 암호를 입력합니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

16. **Finish(마침)**를 클릭하여 저장하고 설정을 적용합니다.
    시스템의 보호가 처음 추가되면, 초기에 보호 일시 중지를 지정하지 않은 경우에는 정의된 일정에 따라 기본 이미지(보호되는 볼륨에 있는 모든 데이터의 스냅샷)가 Core의 리포지토리에 전송됩니다.

보호 일시 중지 및 다시 시작

보호를 일시 중지하면 현재 시스템에서의 모든 데이터 전송이 일시적으로 중지됩니다.
보호를 일시 중지하려면 다음을 수행합니다.

1. Core 콘솔의 왼쪽 탐색 영역에서 **Protected Machines(보호되는 시스템)** 드롭다운 메뉴를 클릭합니다.
2. 보호를 일시 중지할 시스템에서 **Pause Protection(보호 일시 중지)**을 선택합니다.
   Pause Protection(보호 일시 중지) 대화 상자가 표시됩니다.
3. 다음 중 하나를 선택하고 **OK(확인)**를 클릭합니다.
   - 보호를 명시적으로 재개할 때까지 일시 중지하려면 **Pause until resumed(재개될 때까지 일시 중지)**를 선택합니다.
   - 특정 기간 동안 보호를 일시 중지하려면 **Pause for(일시 중지 기간)**을 선택하고 Days(일), Hours(시간), Minutes(분) 컨트롤을 사용하여 일시 중지 기간을 적절하게 입력하거나 선택합니다.

   노트: 보호를 재개하려면 **Protected Machines(보호되는 시스템)** 드롭다운 메뉴에서 **Resume Protection(보호 재개)**을 선택합니다.

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. 왼쪽 탐색 창에서 **Protected Machines(보호되는 시스템)**를 클릭합니다.
2. **Actions(작업) → Deploy Agent(에이전트 배포)**를 클릭합니다.
   Deploy Agent(에이전트 배포) 대화 상자가 표시됩니다.
3. 다음과 같이 로그온 및 보호 설정을 입력합니다.
   - **Host name(호스트 이름)** — 보호할 시스템의 호스트 이름이나 IP 주소를 지정합니다.
   - **User name(사용자 이름)** — 이 시스템에 연결하는 데 사용되는 사용자 이름을 지정합니다(예: administrator).

- **Password(암호)** — 이 시스템에 연결하는 데 사용되는 암호를 지정합니다.
- **Protect machine after install(설치 후 시스템 보호)** — 이 옵션을 선택하면 보호할 시스템이 추가된 후에 AppAssure가 데이터의 기본 스냅샷을 만들 수 있습니다. 이 옵션은 기본적으로 선택되지만, 선택 취소할 경우 데이터 보호를 시작할 준비가 될 때 수동으로 스냅샷이 강제 적용되도록 해야 합니다.
- **Display name(표시 이름)** — Core 콘솔에 표시되는 시스템의 이름을 지정합니다. 표시 이름은 호스트 이름과 동일할 수 있습니다.
- **Port(포트)** — Core가 시스템에 있는 Agent와 통신하는 포트 번호를 지정합니다. 기본값은 8006입니다.
- **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.

보호 일정 이해

보호 일정은 보호되는 에이전트 시스템에서 AppAssure Core로 백업이 전송될 때를 정의합니다.

보호 일정은 **Protect Machine Wizard(시스템 보호 마법사)** 또는 **Protect Multiple Machines Wizard(다중 시스템 보호 마법사)**를 사용하여 초기에 정의됩니다. 이후에는 Summary(요약) 탭에서 특정 에이전트 시스템의 기존 일정을 언제든지 수정할 수 있습니다.

AppAssure에서는 2개의 정의된 보호 기간으로 기본 보호 일정이 제공됩니다. 첫 번째 기간은 단일 기간(12:00 AM부터 11:59 PM까지)으로 정의된 평일(월요일-금요일)이며 기본 간격은 3시간입니다. 두 번째 기간은 주말(토요일, 일요일)이며 기본 간격은 3시간입니다.

보호가 처음 사용되면 일정이 활성화됩니다. 따라서 기본 설정을 사용하면 현재 시간과 상관 없이 첫 번째 백업이 3시간마다 발생합니다.

Core에 저장되는 첫 번째 백업 전송을 기본 이미지 스냅샷이라고 합니다. 지정된 모든 볼륨(운영 체제, 응용프로그램 및 설정 포함)에 있는 모든 데이터가 Core에 저장됩니다. 그 후에 증분 스냅샷(마지막 백업 이후에 에이전트에서 변경된 데이터로만 구성된 더 작은 백업)이 정의된 간격에 따라 정기적으로 Core에 저장됩니다.

사용자 지정 일정을 만들어 백업 빈도를 변경할 수 있습니다. 예를 들어, 평일 간격을 60분으로 변경하여 1시간마다 스냅샷이 생성되도록 할 수 있습니다. 또는 주말 간격을 60분에서 180분으로 늘려 트래픽이 낮을 때 3시간마다 스냅샷이 생성되도록 할 수 있습니다.

Protection Schedule Wizard(보호 일정 마법사) 페이지에 있는 기타 옵션에는 일일 보호 시간을 설정하는 옵션이 포함되어 있습니다. 이 옵션을 사용하면 정의된 기간에 일일 단일 백업이 생성됩니다(기본 설정값은 12:00 PM).

초기에 보호를 일시 중지하는 옵션을 사용하면 보호를 명시적으로 재개할 때까지 기본 이미지가 생성되지 않습니다(모든 백업 발생 방지). 설정된 보호 일정을 기준으로 시스템을 보호할 준비가 되면 보호를 명시적으로 재개해야 합니다.

사용자 지정 일정 만들기

1. **Protect Machine(시스템 보호)** 또는 **Protect Multiple Machines Wizard(다중 시스템 보호 마법사)**의 **Protection Schedule(보호 일정)** 페이지에서 원하는 기간의 간격 일정을 변경하려면 다음을 수행합니다.
   a. **Periods(기간)**를 선택합니다.

      기존의 기간이 표시되며 수정할 수 있습니다. 수정 가능한 필드는 각 기간의 시작 시간, 종료 시간, 간격(분)입니다.
   b. 간격 필드를 클릭하고 적절한 간격(분)을 입력합니다.

      예를 들어, 기존의 간격 값을 강조 표시하고 이 값을 **60**으로 바꾸면 이 기간 동안 60분마다 스냅샷이 수행됩니다.
2. 평일에 사용량이 많은 피크 기간과 사용량이 적은 오프 피크 기간을 만들려면 다음과 같이 24시간 기간이 포함되지 않도록 평일의 시간 범위를 변경하고, 피크 기간에 가장 적합한 간격을 설정한 후, **Take snapshots for the remaining time(나머지 시간의 스냅샷 만들기)**을 선택한 다음 사용량이 적은 오프 피크 기간의 간격을 설정하십시오.
   a. **Periods(기간)**를 선택합니다.

      기존의 기간이 표시되며 수정할 수 있습니다.
   b. **From(시작)** 상자를 클릭하여 이 기간의 시작 시간을 변경합니다.

      Choose Time(시간 선택) 대화 상자가 나타납니다.
   c. 시간 및 분 슬라이더를 드래그하여 원하는 시작 시간에 맞게 조정한 후 **Done(완료)**을 클릭합니다. 현재 시간을 지정하려면 **Now(현재)**를 클릭합니다.
   d. **To(종료)** 상자를 클릭하여 이 기간의 종료 시간을 변경합니다.

      Choose Time(시간 선택) 대화 상자가 나타납니다.
   e. 시간 및 분 슬라이더를 드래그하여 원하는 시작 시간에 맞게 조정한 후 **Done(완료)**을 클릭합니다. 현재 시간을 지정하려면 **Now(현재)**를 클릭합니다.
3. 하루에 한 번의 단일 백업이 매일 발생하도록 설정하려면 **Daily protection time(매일 보호 시간)**을 선택하고 HH:MM AM 형식으로 시간을 입력합니다.
4. 백업이 시작되지 않는 일정을 정의하려면 **Initially pause protection(처음에 보호 일시 중지)**을 선택합니다.

   마법사에서 보호를 일시 중지하면 명시적으로 재개할 때까지 일시 중지 상태로 유지됩니다. 보호를 재개하면 설정된 일정에 따라 백업이 발생합니다.
5. **Finish(마침)** 또는 **Next(다음)**를 클릭합니다.

보호 일정 수정

시스템의 특정 볼륨에 대한 보호 일정을 수정할 수 있습니다.

보호 일정을 수정하려면 다음을 수행하십시오.

1. Core 콘솔에서, 변경할 보호 일정이 정의되어 있는 시스템을 선택합니다.

   시스템의 Summary(요약) 탭이 표시됩니다.
2. 변경할 보호 시스템의 볼륨을 선택하고 **Set a schedule(일정 설정)**을 클릭합니다. 한 번에 모든 볼륨을 선택하려면 헤더 행에서 해당 확인란을 클릭합니다.

   처음에는 모든 볼륨에 동일한 보호 일정이 적용됩니다. 대체로 시스템 예약 볼륨과 운영 체제가 포함된 볼륨(일반적으로 C 드라이브)을 보호하는 것이 좋습니다.

   Protection Schedule(보호 일정) 대화 상자가 표시됩니다.

3. **Protection Schedule(보호 일정)** 대화 상자에서, 이전에 보호 일정 템플릿을 만들었고 이 템플릿을 에이전트에 적용하려면, 드롭다운 목록에서 템플릿을 선택하고 9단계로 이동합니다.
4. 새 보호 일정을 템플릿으로 저장하려면 텍스트 상자에 템플릿의 이름을 입력합니다.
5. 일정에서 기존 기간을 제거하려면 각 기간 옵션 옆에 있는 확인란을 선택 취소합니다. 다음과 같은 옵션이 포함됩니다.
   - **Mon - Fri(월 - 금).** 이 시간 범위는 일반적인 평일 5일을 나타냅니다.
   - **Sat - Sun(토 - 일).** 이 시간 범위는 일반적인 주말을 나타냅니다.
6. 평일 시작 및 종료 시간이 12:00 AM부터 11:59 PM까지일 경우 단일 기간이 존재합니다. 정의된 기간의 시작 또는 종료 시간을 변경하려면 다음을 수행하십시오.
   a. 적절한 기간을 선택합니다.
   b. **Start Time(시작 시간)** 상자를 클릭하여 이 기간의 시작 시간을 변경합니다.
   c. 시간 및 분 슬라이더를 드래그하여 원하는 시작 시간에 맞게 조정한 후 **Done(완료)**을 클릭합니다. 현재 시간을 지정하려면 **Now(현재)**를 클릭합니다.
   d. **End Time(종료 시간)** 상자를 클릭하여 이 기간의 종료 시간을 변경합니다.

      Choose Time(시간 선택) 대화 상자가 나타납니다.
   e. 시간 및 분 슬라이더를 드래그하여 원하는 시작 시간에 맞게 조정한 후 **Done(완료)**을 클릭합니다. 현재 시간을 지정하려면 **Now(현재)**를 클릭합니다.
   f. 요구사항에 따라 간격을 변경합니다. 예를 들어, 피크 기간을 정의하는 경우 간격을 60분에서 20분으로 변경하여 1시간에 스냅샷이 세 번 생성되도록 합니다.
7. 6단계에서 12:00 AM부터 11:59 PM까지 이외의 기간을 정의한 경우, 나머지 시간 범위에서 백업이 발생하도록 하려면 다음과 같이 추가적인 기간을 추가하여 보호를 정의해야 합니다.
   a. **+ Add period(+ 기간 추가)**를 클릭합니다.

      해당 범주(평일 또는 주말) 아래에 새 기간이 나타납니다. 첫 번째 기간이 12:00 AM 이후에 시작되면 AppAssure에서 이 기간이 12:00에 자동으로 시작됩니다. 위의 예에 따르면, 두 번째 기간이 12:00 AM에 시작됩니다. 시작 및 종료 시간의 시간 또는 분을 조정해야 하는 경우도 있습니다.
   b. 원하는 시작 및 종료 시간에 맞게 시간 및 분 슬라이더 컨트롤을 드래그합니다.
   c. 요구사항에 따라 간격을 변경합니다. 예를 들어, 오프 피크 기간을 정의하는 경우 간격을 60분에서 120분으로 변경하여 2시간마다 스냅샷이 생성되도록 합니다.
8. 필요한 경우, 시작 및 종료 시간과 간격을 적절하게 설정하여 추가 기간을 생성합니다.

   노트: 추가한 기간을 제거하려면 해당 기간 맨 오른쪽에 있는 **X**를 클릭합니다. 실수로 기간을 제거한 경우에는 **Cancel(취소)**을 클릭하면 됩니다.
9. 보호 일정이 요구사항에 맞으면 **Apply(적용)**을 클릭합니다.

   Protection Schedule(보호 일정) 대화 상자가 닫힙니다.

보호되는 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. Core 콘솔에서, 수정할 시스템으로 이동합니다.
2. **Configuration(구성) → Settings(설정)**를 클릭합니다.
3. **Change(변경)**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. Core에서는 기본 포트 8006을 사용하여 시스템과 통신합니다.
암호화 키	필요한 경우 암호화 키를 편집합니다. 리포지토리에 저장되는 시스템의 모든 볼륨에 대한 데이터에 암호화를 적용할 것인지 지정합니다.
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.

시스템의 시스템 정보 보기

Core 콘솔이 보호 중인 모든 시스템을 표시합니다.
컴퓨터에 대한 시스템 정보를 보려면 다음을 수행하십시오.

1. Core 콘솔의 왼쪽 탐색 영역의 **Protected Machines(보호되는 시스템)** 아래에서 시스템 세부 정보를 볼 시스템을 선택합니다.
2. **Tools(도구)** 탭을 클릭합니다.
   System Information(시스템 정보) 탭에는 다음과 같은 정보가 포함되어 있습니다.
   - 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)

   표시되는 기타 시스템 정보는 다음과 같습니다.
   - 프로세서
   - 네트워크 어댑터

- 이 시스템과 연결된 IP 주소

라이센스 정보 보기

시스템에 설치된 AppAssure Agent 소프트웨어에 대한 현재 라이센스 상태 정보를 볼 수 있습니다.
라이센스 정보를 보려면 다음을 수행하십시오.

1. 탐색 창에서 보려는 시스템을 선택합니다.
2. **Configuration(구성)** → **Licensing(라이센싱)**을 클릭합니다.
   Status(상태) 화면에 제품 라이센싱에 대한 상세정보가 표시됩니다.

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 수정을 참조하십시오.

주의: 전송 설정을 변경하면 AppAssure 환경에 상당히 영향을 줄 수 있습니다. 전송 설정값을 수정하기 전에 Dell AppAssure 기술 자료에 있는 전송 성능 조정 안내서를 참조하십시오.

DL1000에는 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.
복원	보호된 시스템에서 백업 정보를 복원하는 프로세스입니다.

DL1000의 데이터 전송은 네트워크를 통해 AppAssure 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, 수정할 시스템으로 이동합니다.
2. **Configuration(구성)** 탭을 클릭하고 **Transfer Settings(전송 설정)**을 클릭합니다.
   현재 **Transfer Settings(전송 설정)** 페이지가 표시됩니다.
3. **Transfer Settings(전송 설정)** 페이지에서 **Change(변경)**를 클릭합니다.
   Transfer Settings(전송 설정) 대화 상자가 표시됩니다.

4. 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.
제외된 기록기	제외할 기록기를 선택합니다. 목록에 표시되는 기록기는 현재 구성하는 시스템과 관련이 있기 때문에 일부 기록기는 목록에 표시되지 않을 수 있습니다. 목록에 표시되는 기록기는 다음과 같습니다. • ASR 기록기 • BITS 기록기 • COM+ REGDB 기록기 • 성능 카운터 기록기 • 레지스트리 기록기 • 섀도 복사본 최적화 기록기 • SQL Server 기록기 • 시스템 기록기 • 작업 스케줄러 기록기 • VSS 메타데이터 저장소 기록기

텍스트 상자	설명
	• WMI 기록기
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.

5. **OK(확인)**를 클릭합니다.

데이터 아카이브

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 수행합니다.

1. Core 콘솔에서 **Tools(도구) → Archive(아카이브) → Create(생성)**를 클릭합니다.
   Add Archive Wizard(아카이브 추가 마법사) 대화 상자가 나타납니다.
2. **Add Archive Wizard(아카이브 추가 마법사)**의 **Create(생성)** 페이지에 있는 **Location Type(위치 유형)** 드롭다운 목록에서 다음 옵션 중 하나를 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드
3. 3단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 아카이브의 세부 정보를 입력합니다.

표 2. 아카이브 생성

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
네트워크	출력 위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경

옵션	텍스트 상자	설명
		로를 정의하는 데 사용됩니다(예: d:\work\archive).
	사용자 이름	사용자 이름을 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트:** 클라우드 계정을 선택하려면 먼저 Core 콘솔에 클라우드 계정을 추가해야 합니다. 클라우드 계정 추가를 참조하십시오.
	컨테이너	드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
	폴더 이름	아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]입니다.

4. **Next(다음)**를 클릭합니다.
5. 마법사의 **Machines(시스템)** 페이지에서, 아카이브할 복구 지점이 포함된 보호 시스템을 선택합니다.
6. **Next(다음)**를 클릭합니다.
7. **Options(옵션)** 페이지에서, 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
최대 크기	대규모 데이터 아카이브는 여러 개의 세그먼트로 나눌 수 있습니다. 다음 중 하나를 수행하여 아카이브 생성을 위해 예약할 최대 공간을 선택합니다. • 4단계에서 제공한 대상에 입력한 경로에서 사용 가능한 모든 공간을 예약하려면 Entire Target(전체 대상)을 선택합니다(예: 위치가 D:\work\archive일 경우 D: 드라이브의 사용 가능한 모든 공간이 예약됨). • 빈 텍스트 상자를 선택하고 위쪽 및 아래쪽 화살표를 사용하여 공간의 양을 입력한 다음 드롭다운 목록에서 측정 단위를 선택하여 예약할 최대 공간을 사용자 지정합니다. **노트:** Amazon 클라우드 아카이브는 50 GB 세그먼트로 자동으로 나뉘고, Windows Azure 클라우드 아카이브는 200 GB 세그먼트로 자동으로 나뉩니다.

텍스트 상자	설명
재활용 작업	다음과 같은 재활용 작업 옵션 중 하나를 선택합니다. • **Do not reuse(재사용 안 함)**: 위치에서 기존의 아카이브된 데이터를 덮어쓰거나 지우지 않습니다. 위치가 비어 있지 않은 경우 아카이브 쓰기에 실패합니다. • **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.
주석	아카이브에 사용하기 위해 캡처해야 하는 추가 정보를 입력합니다. 나중에 아카이브를 가져오면 주석이 표시됩니다.
호환되는 형식 사용	이전 버전의 코어와 호환되는 형식으로 데이터를 아카이브하려면 이 옵션을 선택하십시오. **노트:** 새 형식을 사용하면 성능이 향상되지만 오래된 버전의 코어와는 호환되지 않습니다.

8. **Next(다음)**를 클릭합니다.
9. Date Range(날짜 범위) 페이지에서, 아카이브될 복구 지점의 Start Date(시작 날짜) 및 Expiration Date(만료 날짜)를 입력합니다.
   - 시간을 입력하려면 표시된 시간(기본값 8:00 AM)을 클릭하여 슬라이드 바가 나타나면 시간 및 분을 선택하십시오.
   - 날짜를 입력하려면 텍스트 상자를 클릭하여 달력이 표시되면 원하는 날짜를 선택하십시오.
10. **Finish(마침)**를 클릭합니다.

아카이브 가져오기

아카이브를 가져오려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구) → Archive(아카이브) → Import(가져오기)**를 클릭합니다.
2. 드롭다운 목록에서 다음 옵션 중 하나를 **Location Type(위치 유형)**으로 선택합니다.
   - 로컬
   - 네트워크
   - 클라우드
3. 3단계에서 선택한 위치 유형을 기준으로 다음 표에 설명된 대로 아카이브의 세부 정보를 입력합니다.

표 3. 아카이브 가져오기

옵션	텍스트 상자	설명
로컬	출력 위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경

옵션	텍스트 상자	설명
		로를 정의하는 데 사용됩니다(예: `d:\work\archive`).
네트워크	출력 위치	출력 위치를 입력합니다. 이 위치는 아카이브가 상주하는 위치 경로를 정의하는 데 사용됩니다(예: d:\work\archive).
	사용자 이름	사용자 이름을 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
	암호	네트워크 경로에 대한 암호를 입력합니다. 이는 네트워크 공유에 대한 로그온 자격 증명을 설정하는 데 사용됩니다.
클라우드	계정	드롭다운 목록에서 계정을 선택합니다. **노트:** 클라우드 계정을 선택하려면 먼저 Core 콘솔에 클라우드 계정을 추가해야 합니다. 클라우드 계정 추가를 참조하십시오.
	컨테이너	드롭다운 메뉴에서 계정과 연계된 컨테이너를 선택합니다.
	폴더 이름	아카이브된 데이터가 저장되는 폴더의 이름을 입력합니다. 기본 이름은 AppAssure-5-Archive-[DATE CREATED]-[TIME CREATED]입니다.

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.

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 추가를 참조하십시오.

- 클라우드 계정에 데이터를 아카이브하고 내보낼 수 있습니다.
- 클라우드 위치에서 아카이브된 데이터를 가져와 검색합니다.

시스템 진단 보기

AppAssure에서, 진단 정보를 사용하여 보호되는 시스템의 시스템 로그 데이터를 볼 수 있습니다. 또한 Core의 진단 정보를 보고 업로드할 수 있습니다.

시스템 로그 보기

이 기능은 시스템에 오류 또는 문제가 발생한 경우 로그를 확인하여 문제를 해결할 때 유용합니다.

시스템 로그를 보려면 다음을 수행하십시오.

1. Core 콘솔에서 **Tools(도구) → Diagnostics(진단) → View Log(로그 보기)**를 클릭합니다.
   Download Core Log(Core 로그 다운로드) 페이지가 나타납니다.
2. **Click here to begin the download(다운로드를 시작하려면 여기를 클릭)**를 선택합니다.
   파일을 열거나 저장하라는 경고 메시지가 나타납니다.
3. 로그 파일을 처리하는 기본 방법을 선택합니다.

시스템 로그 업로드

1. Core 콘솔로 이동하여 **Tools(도구) → Diagnostics(진단) → Upload Log(로그 업로드)**를 클릭합니다.
   Upload Log(로그 업로드) 페이지가 표시됩니다.
2. **Click here to begin the upload(업로드를 시작하려면 여기를 클릭)**를 선택합니다.
   Core 및 보호되는 모든 시스템의 로드 정보 업로드 진행 상태를 볼 수 있는 Events(이벤트) 탭이 표시됩니다.

시스템에서 작업 취소

시스템에서 현재 실행 중인 작업을 취소할 수 있습니다. 내보내기 및 복제를 포함하여 현재 모든 작업을 취소하거나 현재 스냅샷을 취소할 수 있습니다.

시스템에서 작업을 취소하려면 다음을 수행하십시오.

1. Core 콘솔에서, 작업을 취소할 시스템을 선택합니다.
2. **Events(이벤트)**에서, 취소할 이벤트 또는 작업의 이벤트 상세정보를 펼칩니다.
3. **Cancel(취소)**을 클릭합니다.

시스템 상태 및 기타 상세정보 보기

시스템 상태 및 기타 상세정보를 보려면 다음을 수행합니다.

1. Core 콘솔에서, 확인할 보호 시스템으로 이동합니다.

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.

- 이름
- 파일 시스템 유형
- 공간 사용량
- 현재 일정
- 다음 스냅샷
- 총 크기
- 사용 중인 공간
- 사용 가능한 공간

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

- 온라인 상태
- 이름
- 설치 경로
- Version(버전)

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

- Version(버전)
- 설치 경로
- 데이터 경로
- Exchange 데이터베이스 경로 이름
- 로그 파일 경로
- 로그 접두사
- 시스템 경로
- 메일 저장소 유형

다중 시스템 관리

이 항목에서는 AppAssure 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 배포를 참조하십시오.
2. 일괄 배포의 작동을 모니터합니다.
   다중 시스템의 배포 모니터링을 참조하십시오.
3. 다중 시스템을 보호합니다.

다중 시스템 보호를 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 모니터링을 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 프로그램을 사용하여 설치 구성요소를 배포하므로, 배포하려는 시스템에서 인터넷에 액세스하여 비트를 다운로드하고 설치할 수 있어야 합니다. 인터넷에 액세스할 수 없을 경우 Core 시스템에서 AppAssure Agent 설치 프로그램을 강제 설치할 수 있습니다. 라이센스 포털에서 Core 및 에이전트 업데이트를 다운로드할 수 있습니다.

다중 시스템의 배포 모니터링

시스템에 AppAssure Agent 소프트웨어 배포에 대한 진행 상태를 볼 수 있습니다.
다중 시스템의 배포를 모니터하려면 다음을 수행하십시오.

1. Core 콘솔에서 **Events(이벤트)** → **Alerts(경고)**를 클릭합니다.
2. AppAssure Core Home(AppAssure Core 홈) 탭으로 이동하여 **Events(이벤트)** 탭을 클릭합니다.
   이벤트가 시작된 시간 및 메시지를 보여주는 경고 이벤트가 나타납니다. Agent 소프트웨어 배포에 성공할 때마다 보호되는 시스템이 추가되었다는 경고가 표시됩니다.
3. 선택적으로, 보호되는 시스템에 연결되는 링크를 클릭합니다.
   선택한 시스템의 Summary(요약) 탭이 나타납니다. 이 탭에는 다음과 같은 관련 정보가 제공됩니다.
   - 보호되는 시스템의 호스트 이름
   - 마지막 스냅샷(해당되는 경우)
   - 선택한 보호 일정을 기준으로 다음 스냅샷의 예약된 시간
   - 남은 시간
   - 보호되는 이 에이전트에 사용되는 암호화 키(있는 경우)
   - Agent 소프트웨어 버전

다중 시스템 보호

Windows 시스템에 AppAssure Agent 소프트웨어를 일괄 배포한 후 데이터를 보호하기 위해 해당 시스템을 보호해야 합니다. 에이전트를 배포할 때 **Protect Machine After Install(설치 후 시스템 보호)**을 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 **Protect(보호)** → **Bulk Protect(일괄 보호)**를 클릭합니다.

   Protect Multiple Machines Wizard(다중 시스템 보호 마법사) 창이 나타납니다.
2. 적절한 설치 옵션을 선택합니다.
   - 리포지토리를 정의할 필요가 없거나 암호화를 설정할 필요가 없을 경우에는 **Typical(일반)**을 선택합니다.
   - 나중에 Protect Machine Wizard(시스템 보호 마법사)에 Welcome(시작) 페이지가 표시되지 않도록 하려면 **Skip this Welcome page the next time the wizard opens(다음에 마법사를 열 때 이 시작 페이지 건너뛰기)**를 선택합니다.
3. **Next(다음)**를 클릭합니다.

   Connection(연결) 페이지가 나타납니다.
4. 다음 옵션 중 하나를 클릭하여 보호하기 원하는 시스템을 추가합니다.
   - Active Directory 도메인에 시스템을 지정하려면 **Active Directory**를 클릭합니다. 아래 표에 설명된 대로 자격 증명을 입력하고 **Next(다음)**를 클릭합니다.
   - vCenter/ESXi 가상 호스트에 가상 시스템을 지정하려면 **vCenter/ESXi**를 클릭합니다. 아래 표에 설명된 대로 자격 증명을 입력하고 **Next(다음)**를 클릭합니다.

텍스트 상자	설명
호스트	Active Directory 도메인 또는 VMware vCenter Server/ESX(i)의 호스트 이름이나 IP 주소입니다.
사용자 이름	이 시스템에 연결하는 데 사용되는 사용자 이름을 입력합니다(예: Administrator).
암호	이 시스템에 연결하는 데 사용되는 안전한 암호를 입력합니다.

   - 시스템을 수동으로 추가하려면 **Add the machines manually(수동으로 시스템 추가)**를 선택합니다. **Next(다음)**를 클릭합니다.
5. **Machines(시스템)** 페이지에서, 수동으로 시스템을 지정하려면 별도의 행에 다음과 같은 각 시스템의 연결 상세정보를 입력하고 **Next(다음)**를 클릭합니다. `hostname::username::password::port`
6. **Machines(시스템)** 페이지에서, Active Directory 도메인 또는 VMware vCenter/ESX(i) 가상 호스트에서 식별된 시스템을 지정하려면 목록에서 보호할 각 시스템을 선택하고 **Next(다음)**를 클릭합니다.

   추가한 각 시스템이 자동으로 식별되고 **Protection(보호)** 페이지가 나타납니다.
7. **Protection(보호)** 페이지에서 적절한 보호 일정을 선택합니다.
   - 기본 보호 일정을 사용하려면 **Schedule Settings(일정 설정)** 옵션에서 **Default protection (hourly snapshots of all volumes)(기본 보호(매시간 모든 볼륨의 스냅샷))**를 선택합니다.
   - 다른 보호 일정을 정의하려면 Schedule Settings(일정 설정) 옵션에서 **Custom protection(사용자 지정 보호)**을 선택하고 **Next(다음)**를 클릭합니다.
8. 다음과 같이 구성을 계속 진행합니다.
   - **Protect Multiple Machines Wizard(다중 시스템 보호 마법사)**에서 Typical(일반) 구성을 선택하고 기본 보호를 지정한 경우 **Finish(마침)**를 클릭하여 선택한 항목을 확인하고 마법사를 닫으십시오. 그러면 지정한 시스템이 보호됩니다.
   - **Protect Multiple Machines Wizard(다중 시스템 보호 마법사)**에서 Typical(일반) 구성을 선택하고 사용자 지정 보호를 지정한 경우 **Next(다음)**를 클릭하고 사용자 지정 일정을 설정합니다.
   - Protect Machine Wizard(시스템 보호 마법사)에서 Advanced(고급 구성) 구성을 선택한 경우 **Next(다음)**를 클릭하고 다음 9단계를 진행하여 리포지토리 및 암호화 옵션을 확인합니다.
9. **Repository(리포지토리)** 페이지에서 **Use an existing repository(기존 리포지토리 사용)**를 선택합니다.
10. **Next(다음)**를 클릭합니다.

    Encryption(암호화) 페이지가 나타납니다.

11. 암호화를 활성화하려면 **Encryption(암호화)** 페이지에서 **Enable Encryption(암호화 활성화)**을 선택합니다.

    Encryption(암호화) 페이지에 Encryption key(암호화 키) 필드가 나타납니다.

    노트: 암호화를 사용할 경우, 보호를 지정한 시스템의 모든 보호되는 볼륨에 있는 데이터에 적용됩니다. 나중에 Core 콘솔의 **Configuration(구성)** 탭에서 설정을 변경할 수 있습니다. 암호화에 대한 자세한 내용은 보안 관리를 참조하십시오.

12. 다음 표에 설명된 대로 정보를 입력하여 Core의 암호화 키를 추가합니다.

텍스트 상자	설명
이름	암호화 키의 이름을 입력합니다.
설명	설명을 입력하여 암호화 키에 대한 추가 세부 정보를 제공합니다.
암호	액세스 제어에 사용되는 암호를 입력합니다.
암호 확인	방금 입력한 암호를 다시 입력합니다.

13. **Finish(마침)**를 클릭하여 저장하고 설정을 적용합니다.

다중 시스템의 보호 모니터링

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

다중 시스템의 보호를 모니터링하려면 Core Console Home(Core 콘솔 홈) 탭을 탐색하고 **Events(이벤트)**를 클릭합니다.

Events(이벤트) 탭에 Tasks(작업), Alerts(경고) 및 Events(이벤트)가 표시됩니다. 볼륨이 전송되면 Tasks(작업) 창에 상태, 시작 시간, 종료 시간이 표시됩니다. 상태별로(활성, 대기, 완료, 실패) 작업을 필터링할 수도 있습니다.

보호되는 시스템이 추가될 때마다 작업 성공 여부 또는 오류 로그 여부를 설명하는 경고가 로그됩니다.

4

데이터 복구

복구 관리

AppAssure 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

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 섀도 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)**를 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 살펴보십시오.

정보	설명
Actions(조치)	**Actions(조치)** 메뉴에는 선택한 복구 지점에서 수행할 수 있는 다음과 같은 작업이 포함되어 있습니다. **Mount(탑재)** — 선택한 복구 지점을 탑재하려면 이 옵션을 선택합니다. 선택한 복구 지점 탑재에 대한 자세한 내용은 Windows 시스템의 복구 지점 탑재를 참조하십시오. **Export(내보내기)** — Export(내보내기) 옵션에서, 선택한 복구 지점을 ESXi, VMware Workstation 또는 HyperV로 내보낼 수 있습니다. **Restore(복원)** — 선택한 복구 지점에서 지정된 볼륨으로 복원을 수행하려면 이 옵션을 선택합니다.
콘텐츠	Contents(콘텐츠) 영역에는 확장된 복구 지점에 있는 각 볼륨의 행이 포함되어 있으며 이 행에는 각 볼륨의 다음과 같은 정보가 나열됩니다. **Status(상태)**는 복구 지점의 현재 상태를 나타냅니다. **Title(제목)**에는 복구 지점에 있는 특정 볼륨이 나열됩니다. **Size(크기)**는 리포지토리에서 복구 지점이 사용하는 공간의 크기를 표시합니다.

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.

텍스트 상자	설명
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, 로컬 파일 시스템에 탑재할 시스템을 선택합니다.
   선택한 시스템의 **Summary(요약)** 탭이 표시됩니다.
2. **Recovery Points(복구 지점)** 탭을 선택합니다.
3. 복구 지점 목록에서, **>** 부호를 클릭하여 탑재할 복구 지점을 확장합니다.
4. 확장된 복구 지점의 상세정보에서 **Mount(탑재)**를 클릭합니다.
   Mount Recovery Points(복구 지점 탑재) 대화 상자가 표시됩니다.
5. **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. • 읽기 전용 탑재 • 이전 쓰기를 포함하여 읽기 전용 탑재 • 쓰기 가능 탑재
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.

6. **Mount(탑재)**를 클릭하여 복구 지점을 탑재합니다.

선택 복구 지점 분리

선택 복구 지점을 분리하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하여 **Tools(도구)** → **Mounts(탑재)**를 클릭합니다.
2. **Local Mounts(로컬 탑재)** 페이지에서, 탑재를 분리할 복구 지점의 탑재 지점 옆에 있는 **Dismount(분리)**를 클릭합니다.
3. Dismounting the Recovery Point (복구 지점 분리) 창에서 **Yes(예)**를 클릭하여 확인합니다.

모든 복구 지점 분리

모든 복구 지점을 분리하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하여 **Tools(도구)** → **Mounts(탑재)**를 클릭합니다.
2. **Local Mounts(로컬 탑재)** 페이지에서 **Dismount All(모두 분리)**을 클릭합니다.
3. **Dismounting the Recovery Point (복구 지점 분리)** 창에서 **Yes(예)**를 클릭하여 확인합니다.

Linux 시스템의 복구 지점 탑재

Linux 시스템에서 AppAssure의 **aamount** 유틸리티를 사용하면 복구 지점에서 볼륨을 로컬 볼륨으로 원격 탑재할 수 있습니다.

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 수퍼 사용자로 실행합니다. 예: **sudo aamount**
4. AppAssure 탑재 프롬프트에서 **lm** 명령을 입력하여 보호되는 시스템을 나열합니다.
5. 메시지가 표시되면 Core 서버의 IP 주소 또는 호스트 이름을 입력합니다.
6. Core 서버의 로그온 자격 증명(사용자 이름 및 암호)을 입력합니다.

   AppAssure 서버에서 보호되는 시스템의 목록이 표시됩니다. 각 시스템은 라인 항목 번호, 호스트/IP 주소, 시스템의 ID 번호로 식별됩니다. 예: 293cc667-44b4-48ab-91d8-44bc74252a4f
7. 다음 명령을 입력하여 지정된 시스템에 사용할 수 있는 복구 지점을 나열합니다. **lr <line_number_of_machine>**
8. 다음 명령을 입력하여 지정된 탑재 지점/경로에서 지정된 복구 지점을 선택하고 탑재합니다. **m <volume_recovery_point_ID_number> <path>**
9. 탑재 성공 여부를 확인하려면 다음 명령을 입력하여 연결된 원격 볼륨을 나열합니다. **l**

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. 기본 이미지 강제 적용에 대한 자세한 내용은 스냅샷 강제 적용을 참조하십시오.

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.

스냅샷 강제 적용

스냅샷을 강제 적용하면 현재 보호되는 시스템에 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 볼륨의 모든 데이터가 전송니다. 이를 기본 이미지라고 합니다.

스냅샷을 강제 적용하려면 다음을 수행하십시오.

1. Core 콘솔에서, 스냅샷을 강제 적용할 복구 지점이 있는 시스템 또는 클러스터를 선택합니다.
2. **Volumes(볼륨)** 섹션의 **Summary(요약)** 탭을 클릭하고 아래 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.

데이터 복원

AppAssure를 사용하여 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.

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.

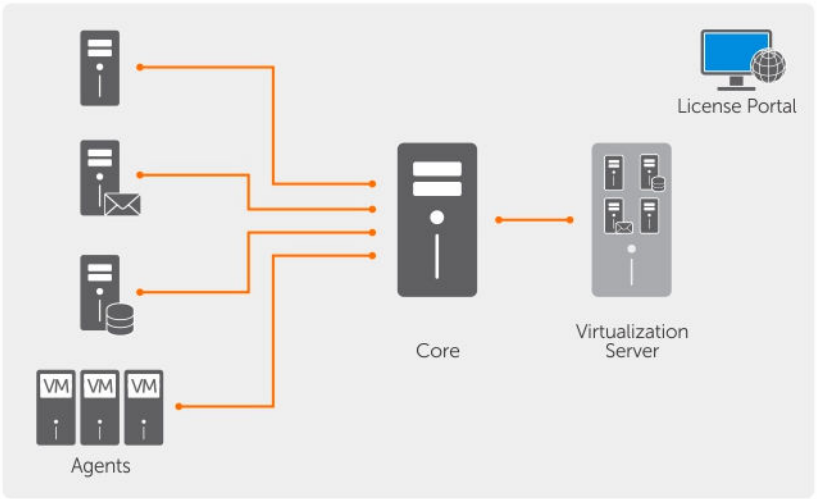

그림 4 . 가상 시스템에 데이터 내보내기

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

Dell AppAssure에서는 모든 동적 및 기본 볼륨의 스냅샷을 만들 수 있습니다. 또한 하나의 실제 디스크에 있는 단순 동적 볼륨을 내보낼 수 있습니다. 단순 동적 볼륨은 스트라이핑, 미러링 또는 스팬되지 않은 볼륨입니다.

동적 디스크(이전에 설명한 단순 동적 디스크 제외)는 Export Wizard(내보내기 마법사)에서 선택할 수 없습니다. 비단순 동적 볼륨에는 완전하게 해석되지 않는 임의 디스크 지오메트리가 있습니다. 따라서 AppAssure에서는 복합 또는 비단순 동적 볼륨의 내보내기를 지원하지 않습니다.

내보내기 관리

Core 콘솔의 **Virtual Standby(가상 대기)** 탭에서, 가상 대기를 위한 1회 내보내기 및 연속 내보내기를 비롯하여 설정된 내보내기 상태를 볼 수 있습니다. 이 탭에서는 내보내기를 일시 중지, 중지, 제거하거나, 다음에 수행될 내보내기 큐를 확인하여 내보내기를 통해 관리할 수 있습니다.

노트: 2 VM 포함 3 TB 구성은 1회 내보내기 및 연속 내보내기(가상 대기) 기능을 지원합니다(Dell DL1000에만 해당).

1. Core 콘솔에서 **Virtual Standby(가상 대기)** 탭으로 이동합니다.

   Virtual Standby(가상 대기) 탭에서, 다음 표에 설명되어 있는 정보가 포함된 저장된 내보내기 설정 표를 볼 수 있습니다.

메뉴	설명
Status(상태)	**노트:** 가상 대기 구성 상태는 아이콘 색상으로 정의됩니다. 녹색 - 가상 대기가 성공적으로 구성되었으며 활성 상태이고 일시 중지되지 않았습니다. 다음 가상 대기 내보내기는 다음 스냅샷 이후에 수행됩니다. 노란색 - 가상 대기가 일시 중지되고 Core에서 여전히 저장됩니다. 하지만 새 전송이 수행된 후에는 내보내기 작업이 자동으로 시작되지 않으며 이 에이전트에 대한 새로운 가상 대기 내보내기가 없습니다.
시스템 이름	소스 시스템의 이름입니다.
대상	데이터를 내보내는 가상 시스템 및 경로입니다.
내보내기 유형	ESXi, VMware, Hyper-V 또는 VirtualBox 등과 같은 내보내기에 사용되는 가상 시스템 플랫폼의 유형입니다.
마지막 내보내기	마지막 내보내기의 날짜 및 시간입니다. 내보내기가 방금 추가되었지만 완료되지 않은 경우 내보내기가 아직 수행되지 않았다는 메시지가 표시됩니다. 내보내기에 실패하거나 취소된 경우 해당 메시지도 표시됩니다.

2. 저장된 내보내기 설정을 관리하려면 내보내기를 선택하고 다음 중 하나를 클릭합니다.
   - **Pause(일시 중지)**: 내보내기를 일시 중지합니다.
   - **Resume(재개)**: 일시 중지된 내보내기를 다시 시작합니다.
   - **Force(강제 적용)**: 새 내보내기를 강제 적용합니다. 이 옵션은 내보내기 작업이 가상 대기가 일시 중지된 다음 재개된 경우(새 전송 이후에만 다시 시작되는 경우)에 유용합니다. 새 전송이 수행될 때까지 기다리지 않고 내보내기를 강제 적용할 수 있습니다.
3. 시스템에서 내보내기를 제거하려면 **Remove(제거)**를 클릭합니다. 내보내기를 제거하면 시스템에서 영구적으로 제거되며 다시 시작할 수 없습니다.
4. 현재 큐에 있고 완료될 활성 상태인 내보내기에 대한 상세정보를 보려면 **Show Export Queue(내보내기 큐 표시)**를 클릭합니다.

   다음과 같은 표가 표시됩니다.

메뉴	설명
시스템 이름	소스 시스템의 이름입니다.

메뉴	설명
대상	가상 대기가 성공적으로 구성되었으며 활성 상태이고 일시 중지되지 않았습니다. 다음 가상 대기 내보내기는 다음 스냅샷 이후에 수행됩니다.
내보내기 유형	가상 대기가 일시 중지되고 Core에서 여전히 저장됩니다. 하지만 새 전송이 수행된 후에는 내보내기 작업이 자동으로 시작되지 않으며 이 에이전트에 대한 새로운 가상 대기 내보내기가 없습니다.
일정 유형	내보내기 유형 중 하나로 1회 또는 연속입니다.
Status(상태)	내보내기 작업의 진행 상태로서 진행률 표시줄에 백분율로 표시됩니다.

Windows 시스템에서 가상 시스템으로 백업 정보 내보내기

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

노트: 2 VM 포함 3 TB 구성은 1회 내보내기 및 연속 내보내기(가상 대기) 기능을 지원합니다(Dell DL1000에만 해당).

Windows 백업 정보를 가상 시스템으로 내보내려면 다음을 수행하십시오.

1. Core 콘솔에서 **Protected Machines(보호되는 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.
   - 1회
   - 가상 대기

   Export Wizard(내보내기 마법사) 대화 상자가 표시됩니다.

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. 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.

ESXi 내보내기 수행을 위한 가상 시스템 정보 정의

ESXi 내보내기 수행을 위한 가상 시스템 정보를 정의하려면 다음을 수행하십시오.

1. **Export Wizard(내보내기 마법사)**의 **Destination(대상)** 페이지에 있는 **Recover to Virtual machine(가상 시스템으로 복구)** 드롭다운 메뉴에서 **ESX(i)**를 선택합니다.
2. 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 로그온 자격 증명을 입력합니다.
암호	호스트 시스템에 대한 로그온 자격 증명을 입력합니다.

3. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
데이터 저장소	드롭다운 목록에서 데이터 저장소를 선택합니다.
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	메모리 사용량을 지정합니다.
디스크 프로비저닝	디스크 프로비저닝의 유형을 선택합니다(씬 프로비저닝 또는 씩 프로비저닝).
디스크 매핑	디스크 매핑의 유형을 지정합니다(자동 또는 수동).
Version(버전)	가상 시스템의 버전을 선택합니다.

4. **Next(다음)**를 클릭합니다.
5. **Volumes(볼륨)** 페이지에서, 내보낼 볼륨을 선택하고 **Next(다음)**를 클릭합니다.
6. **Summary(요약)** 페이지에서, **Finish(완료)**를 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) ESXi 내보내기 수행

지속적(가상 대기) ESXi 내보내기를 수행하려면 다음을 수행하십시오.

1. 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 보호 시스템을 선택하고 **Next(다음)**를 클릭합니다.
   - 내보낼 시스템으로 이동하고**Actions(작업) → Export(내보내기) → Virtual Standby(가상 대기)**를 클릭합니다.
2. **Export Wizard(내보내기 마법사)**의 **Destination(대상)** 페이지에 있는 **Recover to a Virtual machine(가상 시스템으로 복구)** 드롭다운 메뉴에서 **ESXi**를 선택합니다.
3. 다음 표에 설명된 대로 가상 시스템에 액세스하기 위한 정보를 입력하고 **Next(다음)**를 클릭합니다.

텍스트 상자	설명
호스트 이름	호스트 시스템의 이름을 입력합니다.
포트	호스트 시스템의 포트를 입력합니다. 기본값은 443입니다.
사용자 이름	호스트 시스템에 대한 로그온 자격 증명을 입력합니다.
암호	호스트 시스템에 대한 로그온 자격 증명을 입력합니다.

4. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 다음 표에 설명된 대로 정보를 입력합니다.

텍스트 상자	설명
리소스 풀	드롭다운 목록에서 리소스 풀을 선택합니다.
데이터 저장소	드롭다운 목록에서 데이터 저장소를 선택합니다.
가상 시스템 이름	가상 시스템의 이름을 입력합니다.
메모리	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).
디스크 프로비저닝	디스크 프로비저닝의 유형을 선택합니다(씬 프로비저닝 또는 씩 프로비저닝).
디스크 매핑	디스크 매핑의 유형을 지정합니다(자동 또는 수동).
Version(버전)	가상 시스템의 버전을 선택합니다.

5. **Next(다음)**를 클릭합니다.
6. **Volumes(볼륨)** 페이지에서, 내보낼 볼륨을 선택하고 **Next(다음)**를 클릭합니다.
7. **Summary(요약)** 페이지에서, **Finish(완료)**를 클릭하여 마법사를 완료하고 내보내기를 시작합니다.

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

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. Core 콘솔에서, 내보낼 시스템으로 이동합니다.
2. **Summary(요약)**에서**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 VMware 워크스테이션 내보내기를 수행하도록 설정 정의

한 번 VMware 워크스테이션 내보내기를 수행하도록 설정을 정의하려면 다음을 수행하십시오.

1. **Export Wizard(내보내기 마법사)**의 **Destination(대상)** 페이지에 있는 **Recover to Virtual machine(가상 시스템으로 복구)** 드롭다운 메뉴에서 **VMware Workstation**을 선택하고 **Next(다음)**를 클릭합니다.
2. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

텍스트 상자	설명
Location(위치)	가상 시스템을 생성할 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다.

텍스트 상자	설명
	노트: 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그온 자격 증명을 입력해야 합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.
사용자 이름	가상 시스템에 대한 로그온 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 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 암호를 입력해야 합니다. • 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
가상 시스템 이름	생성할 가상 시스템의 이름을 입력합니다(예: VM-0A1B2C3D4). **노트:** 기본 이름은 원본 시스템의 이름입니다.
Version(버전)	가상 시스템으로 사용할 VMware Workstation의 버전을 지정합니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리 사용량을 지정합니다. • Use the same amount of RAM as the source machine(소스 시스템과 동일한 RAM 크기 사용) - RAM 구성을 소스 시스템과 동일하게 지정합니다. • Use a specific amount of RAM(특정 RAM 크기 사용) - 사용할 RAM의 크기를 지정합니다(예: 4096MB). 최소 허용 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다.

3. **Next(다음)**를 클릭합니다.
4. **Summary(요약)** 페이지에서, **Finish(완료)**를 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) VMware 워크스테이션 내보내기 수행

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

1. 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 보호 시스템을 선택하고 **Next(다음)**를 클릭합니다.
   - 내보낼 시스템으로 이동하고, 이 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)** 페이지에서 **Recover to a Virtual Machine(가상 시스템에 복구) → VMware Workstation**을 클릭합니다.

3. **Next(다음)**를 클릭합니다.
4. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서, 아래 표에 설명된 대로 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

텍스트 상자	설명
대상 경로	가상 시스템을 생성할 로컬 폴더 또는 네트워크 공유의 경로를 지정합니다. **노트:** 네트워크 공유 경로를 지정한 경우 대상 시스템에 등록된 계정의 유효한 로그온 자격 증명을 입력합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.
사용자 이름	가상 시스템에 대한 로그온 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 로그온 자격 증명을 입력합니다. • 네트워크 공유 경로를 지정한 경우, 대상 시스템에 등록된 계정의 유효한 암호를 입력해야 합니다. • 로컬 경로를 입력한 경우에는 암호가 필요하지 않습니다.
가상 시스템	생성할 가상 시스템의 이름을 입력합니다(예: VM-0A1B2C3D4). **노트:** 기본 이름은 원본 시스템의 이름입니다.
Version(버전)	가상 시스템으로 사용할 VMware Workstation의 버전을 지정합니다. • VMware Workstation 7.0 • VMware Workstation 8.0 • VMware Workstation 9.0
메모리	다음 중 하나를 클릭하여 가상 시스템의 메모리를 지정합니다. • Use the same amount of RAM as the source machine(소스 시스템과 동일한 RAM 크기 사용) - RAM 구성을 소스 시스템과 동일하게 지정합니다. • Use a specific amount of RAM(특정 RAM 크기 사용) - 사용할 RAM의 크기를 지정합니다(예: 4096MB). 최소 허용 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다.

5. 다음에 예정된 스냅샷이 생성될 때까지 기다리지 않고 즉시 가상 내보내기를 수행하려면 **Perform initial ad-hoc export(초기 임시 내보내기 수행)**를 선택합니다.
6. **Next(다음)**를 클릭합니다.
7. **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택하고(예: C:\ 및 D:\) **Next(다음)**를 클릭합니다.
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.

Hyper-V 내보내기를 사용하여 Windows 데이터 내보내기

AppAssure에서는 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.

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

6. **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.
7. **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.
8. 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).

9. 세대를 지정하려면 다음 중 하나를 클릭합니다.
   - 1세대(권장됨)
   - 2세대
10. 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.
11. **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.
12. **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 Windows 데이터 내보내기

AppAssure에서 VirtualBox 내보내기를 통해 한 번 또는 지속적 내보내기를 수행하거나 지속적으로 내보내기(가상 대기)를 구축하여 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

1회 Oracle VirtualBox 내보내기를 수행하려면 다음을 수행하십시오.

1. Core 콘솔에서, 내보낼 Linux 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.
5. **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.
6. **Virtual Machine Options(가상 시스템 옵션)** 페이지에서 **Remote Linux Machine(원격 Linux 시스템)**을 선택합니다.
7. 다음과 같이 가상 시스템에 액세스하기 위한 매개변수를 입력합니다.

텍스트 상자	설명
VirtualBox 호스트 이름	VirtualBox 서버의 IP 주소 또는 호스트 이름을 입력합니다. 이 필드는 원격 VirtualBox 서버의 IP 주소 또는 호스트 이름을 나타냅니다.
포트	시스템의 포트 번호를 입력합니다. 이 번호는 Core가 이 시스템과 통신하는 포트를 나타냅니다.
가상 시스템 이름	가상 시스템을 생성할 대상 경로를 지정합니다.
사용자 이름	대상 컴퓨터에 사용되는 계정의 사용자 이름입니다(예: 루트).
암호	호스트 시스템에 대한 로그온 자격 증명을 입력합니다.
메모리	가상 시스템의 메모리를 지정합니다.

8. **Volumes(볼륨)** 페이지에서, 내보낼 데이터의 볼륨을 선택하고 **Next(다음)**를 클릭합니다.
9. **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.

지속적(가상 대기) Oracle VirtualBox 내보내기 수행

지속적(가상 대기) VirtualBox 내보내기를 수행하려면 다음을 수행하십시오.

1. 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 보호 시스템을 선택하고 **Next(다음)**를 클릭합니다.
   - 내보낼 시스템으로 이동하고, 이 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.

텍스트 상자	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 로그온 자격 증명(사용자 이름 및 암호)을 입력해야 합니다. 해당 계정에 네트워크 공유에 대한 읽기 및 쓰기 권한이 있어야 합니다.
메모리	가상 시스템의 메모리를 지정합니다.

텍스트 상자	설명
	• 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). 최소 허용 크기는 512MB이고 최대값은 호스트 시스템의 용량 및 제한에 따라 결정됩니다.

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 로그온하면 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. 다음에 예정된 스냅샷이 생성될 때까지 기다리지 않고 즉시 가상 내보내기를 수행하려면 **Perform initial ad-hoc export(초기 임시 내보내기 수행)**를 선택합니다.
7. **Next(다음)**를 클릭합니다.
8. **Volumes(볼륨)** 페이지에서 내보낼 볼륨을 선택하고(예: C:\ 및 D:\) **Next(다음)**를 클릭합니다.
9. **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.

복구 지점에서 볼륨 복원

AppAssure Core에 저장된 복구 지점에서 보호 시스템의 볼륨을 복원할 수 있습니다. 복구 지점에서 볼륨을 복원하려면 다음을 수행합니다.

1. Core 콘솔에서 **Restore(복원)** 탭을 클릭합니다.

   Restore Machine Wizard(시스템 복원 마법사)가 나타납니다.
2. **Protected Machines(시스템 보호)** 페이지에서, 데이터를 복원할 보호 시스템을 선택하고 **Next(다음)**를 클릭합니다.

   노트: 보호 시스템에는 Agent 소프트웨어가 설치되어 있어야 하며 복원 작업을 수행할 복구 지점이 있어야 합니다.

   Recovery Points(복구 지점) 페이지가 나타납니다.
3. 복구 지점 목록에서, 에이전트 시스템에 복원할 스냅샷을 검색합니다.

   노트: 필요한 경우, 페이지 하단에 있는 탐색 단추를 사용하여 추가 복구 지점을 표시합니다. 또는 마법사의 Recovery Points(복구 지점) 페이지에 표시되는 복구 지점의 양을 제한하려면 볼륨(정의된 경우)이나 복구 지점 생성 날짜를 기준으로 필터링할 수 있습니다.
4. 복구 지점을 클릭하여 선택한 후 **Next(다음)**를 클릭합니다.

   Destination(대상) 페이지가 나타납니다.
5. **Destination(대상)** 페이지에서, 데이터를 복원하려는 시스템을 다음과 같이 선택합니다.
   - 선택한 복구 지점에서 동일한 에이전트 시스템(예: Machine1)으로 데이터를 복원하려 하고 복원할 볼륨에 시스템 볼륨이 포함되어 있지 않을 경우 **Recover to a protected machine (only non-system**

volumes)(보호 시스템에 복구(시스템 이외 볼륨만 해당)) 옵션을 선택하고 대상 시스템(Machine1)이 선택되어 있는지 확인한 후 **Next(다음)**를 클릭합니다. **Volume Mapping(볼륨 매핑)** 페이지가 나타나면 7단계를 계속 진행합니다.

- 선택한 복구 지점에서 다른 보호 시스템으로 데이터를 복원하려면(예: Machine2의 콘텐츠를 Machine1의 데이터로 대체) **Recover to a protected machine (only non-system volumes)(보호 시스템에 복구(시스템 이외 볼륨만 해당))** 옵션을 선택하고 목록에서 대상 시스템(예: Machine2)을 선택한 후 **Next(다음)**를 클릭합니다. **Volume Mapping(볼륨 매핑)** 페이지가 나타나면 7단계를 계속 진행합니다.
- 부팅 CD를 사용하여 선택한 복구 지점에서 동일한 시스템 또는 다른 시스템으로 복원하려 하고 복원할 볼륨에 시스템 볼륨이 포함되어 있지 않을 경우 **Recover to any target machine using a boot CD(부팅 CD를 사용하여 대상 시스템에 복구)**를 선택합니다.
- 계속해서 선택한 복구 지점의 정보를 사용하여 부팅 CD를 만들려면 **Next(다음)**를 클릭하고 10단계로 진행합니다.
- 부팅 CD를 이미 생성했고 대상 시스템이 부팅 CD를 통해 시작된 경우 17단계를 계속 진행합니다.
- 복구 지점에서 시스템 볼륨(예: 이름이 Machine1인 에이전트 시스템의 C 드라이브)으로 복원하려는 경우에는 BMR을 수행해야 합니다. Windows에서 BMR 수행에 대한 자세한 내용은 Windows 시스템의 운영 체제 미설치 복원 실행을 참조하십시오.
- Linux에서 BMR 수행에 대한 자세한 내용은 Linux 시스템의 운영 체제 미설치 복원 실행의 Linux 시스템의 운영 체제 미설치 복원 수행을 위한 로드맵을 참조하십시오.

6. 대상 시스템의 범용 복구 콘솔(URC)에 연결하려면 다음을 수행합니다.
   a. **I already have a boot CD running on the target machine(대상 시스템에서 실행 중인 부팅 CD 있음)**을 선택합니다.
   b. IP address(IP 주소) 텍스트 상자에 부팅 CD가 포함된 대상 시스템의 IP 주소를 입력합니다.
   c. Authentication Key(인증 키) 텍스트 상자에 대상 시스템에 있는 URC의 인증 키를 입력하고 **Next(다음)**를 클릭합니다.

   Disk Mapping(디스크 맵핑) 페이지가 나타납니다. 20단계를 진행합니다.
7. **Volume Mapping(볼륨 매핑)** 페이지에서, 복원할 복구 지점의 각 볼륨에 대해 적절한 대상 볼륨을 선택합니다. 볼륨을 복원하지 않으려면 Destination Volumes(대상 볼륨) 열에서 **Do not restore(복원하지 않음)**를 선택합니다.
8. **Show advanced options(고급 옵션 표시)**를 선택하고 다음을 수행합니다.
   - Windows 시스템에 복원할 때 라이브 복구를 사용하려면 **Live Recovery(라이브 복구)**를 선택합니다.
     AppAssure의 라이브 복구라고 하는 인스턴트 복구 기술을 사용하면 Microsoft Windows Storage Spaces가 포함된 Windows 시스템의 저장된 복구 지점에서 실제 시스템 또는 가상 시스템에 데이터를 즉시 복구하거나 복원할 수 있습니다. Linux 시스템에서는 라이브 복구를 사용할 수 없습니다.
   - 복구 지점을 강제로 분리하려면 **Force Dismount(강제 분리)**를 선택합니다.
     데이터를 복원하기 전에 복구 지점을 강제로 분리하지 않으면 복원에 실패하고 볼륨 사용 중 오류가 표시될 수 있습니다.
9. 20단계로 이동합니다.
10. Boot CD(부팅 CD) 페이지에서 다음을 수행합니다.
    a. **Output path(출력 경로)** 텍스트 필드에 부팅 CD ISO 이미지가 저장되는 경로를 입력합니다.
    b. **Environment(환경)**에서, 복원할 하드웨어에 가장 적합한 아키텍처를 선택합니다.
       - 64비트 아키텍처를 사용하는 Windows 시스템에 복원하려면 **Windows 8 64-bit(Windows 8 64비트)**를 선택합니다.
       - 32비트(x86) 아키텍처를 사용하는 시스템에 복원하려면 **Windows 7 32-bit(Windows 7 32비트)**를 선택합니다.
11. 선택적으로, 복원되는 에이전트의 네트워크 매개변수를 설정하거나 UltraVNC를 사용하려면 **Show advanced options(고급 옵션 표시)**를 선택하고 다음 중 하나를 수행합니다.

- 복원되는 시스템의 네트워크 연결을 설정하려면 다음 표에 설명된 대로 **Use the following IP address(다음 IP 주소 사용)**을 선택합니다.

옵션	설명
IP Address(IP 주소)	복원되는 시스템의 IP 주소 또는 호스트 이름을 지정합니다.
Subnet Mask(서브넷 마스크)	복원되는 시스템의 서브넷 마스크를 지정합니다.
Default Gateway(기본 게이트웨이)	복원되는 시스템의 기본 게이트웨이를 지정합니다.
DNS Server(DNS 서버)	복원되는 시스템의 도메인 이름 서버를 지정합니다.

- UltraVNC 정보를 정의하려면 다음 표에 설명된 **Add UltraVNC(UltraVNC 추가)**를 선택합니다. 복구 콘솔에 원격으로 액세스해야 할 경우에는 이 옵션을 사용하십시오. 부팅 CD를 사용하는 동안에는 Microsoft 터미널 서비스를 사용하여 로그온할 수 없습니다.

옵션	설명
Password(암호)	이 UltraVNC 연결에 사용할 암호를 지정합니다.
Port(포트)	이 UltraVNC 연결에 사용되는 포트를 지정합니다. 기본 포트는 5900입니다.

12. **Next(다음)**를 클릭합니다.
13. 드라이버를 삽입하려면 다음을 수행합니다.
    a. **Add an archive of drivers(드라이버의 아카이브 추가)**를 선택합니다.
    b. 아카이브가 포함된 ZIP 파일을 탐색하여 선택하고 **Open(열기)**을 클릭합니다. 아카이브가 업로드되고 Driver Injection(드라이버 삽입) 페이지에 나타납니다.
    c. **Next(다음)**를 클릭합니다.
14. ISO Image(ISO 이미지) 페이지에서, 부팅 CD ISO 이미지가 생성될 때의 상태를 확인할 수 있습니다. 부팅 CD에 성공하면 **Next(다음)**를 클릭합니다.

    Connection(연결) 페이지가 나타납니다.
15. 부팅 CD에서 데이터를 복원할 에이전트 시스템을 시작합니다.
    - ISO 이미지에서 에이전트 시스템을 부팅합니다(가능한 경우).
    - 그렇지 않은 경우 ISO 이미지를 실제 미디어(CD 또는 DVD)에 복사하고, 에이전트 시스템의 디스크에 로드하고, 부팅 CD에서 로드하도록 시스템을 구성한 후, 부팅 CD에서 다시 시작합니다.

    노트: 가장 먼저 로드되는 볼륨이 부팅 CD가 되도록 하려면 에이전트 시스템의 BIOS 설정을 변경해야 하는 경우도 있습니다.

    부팅 CD에서 에이전트 시스템이 시작되면 범용 복구 콘솔(URC) 인터페이스가 표시됩니다. 이 환경은 시스템 드라이브나 선택된 볼륨을 AppAssure Core에서 직접 복원하는 데 사용됩니다. URC의 IP 주소와 인증 키 인증서는 부팅 CD에서 시작할 때마다 새로 고쳐지므로 기록해 두십시오.
16. **Connection(연결)** 페이지의 Core 콘솔에서, 다음과 같이 복원할 시스템의 URC 인스턴스에 대한 인증 정보를 입력합니다.
    a. IP address(IP 주소) 텍스트 상자에 복구 지점에서 복원하는 시스템의 IP 주소를 입력합니다.
    b. Authentication Key(인증 키) 텍스트 상자에 URC의 정보를 입력합니다.
    c. **Next(다음)**를 클릭합니다.

    Disk Mapping(디스크 맵핑) 페이지가 나타납니다.

17. 볼륨을 수동으로 매핑하려면 18단계로 이동합니다. 볼륨을 자동으로 매핑하려면 다음을 수행하십시오.
    a. **Automatic volume mapping(자동 볼륨 매핑)**을 선택합니다.
    b. **Automatic volume mapping(자동 볼륨 매핑)** 영역에서 복원할 볼륨을 선택합니다. 나열되는 볼륨을 복원하지 않으려면 해당 옵션을 선택 취소합니다.

       노트: 복원할 수행할 볼륨을 하나 이상 선택해야 합니다.
    c. 복원 대상 디스크를 선택합니다.
    d. **Next(다음)**를 클릭하고 19단계를 계속 진행합니다.
18. 볼륨을 수동으로 매핑하려면 다음을 수행합니다.
    a. **Manual volume mapping(수동 볼륨 매핑)**을 선택합니다.
    b. **Manual volume mapping(수동 볼륨 매핑)** 영역에 있는 각 볼륨의 **Destination Volumes(대상 볼륨)** 드롭다운 목록에서 복원할 볼륨을 선택합니다. 나열되는 볼륨을 복원하지 않으려면 해당 옵션을 선택 취소합니다.

       노트: 복원할 수행할 볼륨을 하나 이상 선택해야 합니다.
    c. **Finish(마침)**을 클릭합니다.

    주의: Finish(마침)를 선택하면 대상 드라이브에 있는 기존의 모든 파티션과 데이터가 영구적으로 제거되며, 운영 체제 및 모든 데이터를 비롯하여 선택한 복구 지점의 내용으로 대체됩니다.

    Restore Machine Wizard(시스템 복원 마법사)가 닫히고 복구 지점의 선택한 볼륨에서 대상 시스템으로 데이터가 복원됩니다. 22단계를 계속 진행합니다.
19. **Disk Mapping Preview(디스크 매핑 미리보기)** 페이지에서, 선택한 복원 작업의 매개변수를 검토할 수 있습니다. 복원을 수행하려면 **Finish(마침)**를 클릭합니다.

    주의: Finish(마침)를 선택하면 대상 드라이브에 있는 기존의 모든 파티션과 데이터가 영구적으로 제거되며, 운영 체제 및 모든 데이터를 비롯하여 선택한 복구 지점의 내용으로 대체됩니다.

    Restore Machine Wizard(시스템 복원 마법사)가 닫히고 복구 지점의 선택한 볼륨에서 대상 시스템으로 데이터가 복원됩니다. 22단계를 계속 진행합니다.
20. 복원하려는 볼륨에 SQL 또는 Microsoft Exchange 데이터베이스가 포함되어 있는 경우, **Dismount Databases(데이터베이스 분리)** 페이지에 데이터베이스를 분리할지 묻는 메시지가 표시됩니다. 복원이 완료된 후 이러한 데이터베이스를 분리하려는 경우 **Automatically remount all databases after the recovery point is restored(복구 지점이 복원된 후 모든 데이터베이스 자동으로 분리)**를 선택하고(선택사항) **Finish(마침)**를 클릭합니다.
21. **OK(확인)**를 클릭하여 복원 프로세스가 시작되었다는 상태 메시지를 확인합니다.
22. 복원 작업 진행 상태를 모니터링하려면 Core 콘솔에서 **Events(이벤트)**를 클릭합니다.

명령행을 사용하여 Linux 시스템의 볼륨 복원

AppAssure에서, `aamount` 명령행 유틸리티를 사용하여 보호되는 Linux 시스템의 볼륨을 복원할 수 있습니다. 명령행을 사용하여 Linux 시스템의 볼륨을 복원하려면 다음을 수행합니다.

주의: 시스템 또는 루트(/) 볼륨은 복원하지 않아야 합니다.

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

   `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 b를 `/mnt/data` 디렉터리에 탑재된 볼륨에 롤백하려는 경우 명령은 `r2 23 b /mnt/data`입니다.

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.

Windows 시스템의 운영 체제 미설치 복원 실행

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 실행을 참조하십시오.

Windows 시스템의 운영 체제 미설치 복원 수행을 위한 로드맵

Windows 시스템에 대한 BMR을 수행하려면 다음을 수행하십시오.

1. 부팅 CD를 생성합니다.
2. 이미지를 디스크에 굽습니다.
3. 부팅 CD에서 대상 서버를 부팅합니다.
4. 복구 디스크에 연결합니다.
5. 볼륨을 매핑합니다.
6. 복구를 시작합니다.
7. 진행 상태를 모니터링합니다.

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 삽입을 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.

부팅CD 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 로그온할 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 로그온합니다.
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)**을 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 로딩을 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.

볼륨을 매핑하려면 다음을 수행하십시오.

1. 볼륨을 자동으로 매핑하려면 다음을 수행합니다.
   a. **Restore Machine Wizard(시스템 복원 마법사)**의 **Disk Mapping(디스크 매핑)** 페이지에서 **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. **Restore(복원)**를 클릭하고 3단계를 계속 진행합니다.
2. 볼륨을 수동으로 매핑하려면 다음을 수행합니다.
   a. **Restore Machine Wizard(시스템 복원 마법사)**의 **Disk Mapping(디스크 매핑)** 페이지에서 **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 **Restore(복원)**를 클릭합니다.

   주의: 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 로그온합니다.

   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

DL1000에서는 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.com의 라이센스 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.

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 탑재 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 로그온 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 `y`를 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.

5

복구 지점 복제

복제

복제는 재난 복구를 위해 복구 지점을 복사하여 보조 위치에 전송하는 프로세스입니다. 이러한 프로세스를 수행하려면 두 Core 간의 관계가 소스-대상 쌍으로 지정되어 있어야 합니다. 복제는 보호된 시스템에서 각각 관리됩니다. 즉, 보호된 시스템의 백업 스냅샷이 대상 복제 Core에 복제됩니다. 복제가 설정되면 소스 Core가 증분 스냅샷 데이터를 대상 Core에 비동기적으로 지속적으로 전송합니다. 회사의 자체 데이터 센터나 원격 재난 복구 사이트(즉, "자체 관리" 대상 Core) 또는 외부 백업과 재난 복구 서비스를 제공하는 관리 서비스 공급자(MSP)에 이 아웃바운드 복제를 구성할 수 있습니다. MSP에 복제하는 경우 연결을 요청하고 자동 피드백 알림을 받을 수 있는 기본 제공 워크플로를 사용할 수 있습니다.

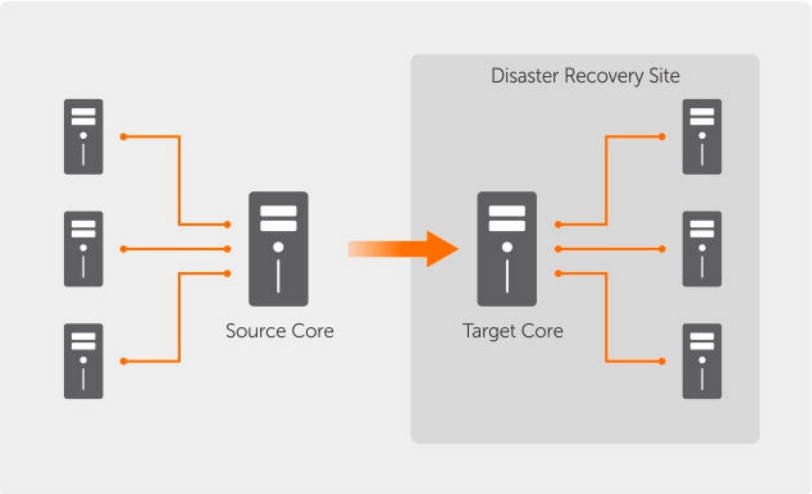

그림 5 . 기본 복제 아키텍처

복제는 중복 제거된 기본 이미지와 보호되는 에이전트의 증분 스냅샷의 초기 전송인 시드를 통해 시작되며, 데이터를 수백 또는 수천 기가바이트까지 추가할 수 있습니다. 외부 미디어를 사용하여 초기 복제를 대상 코어에 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 이동식 미디어에서 사용 가능한 공간보다 큰 경우 미디어에서 사용 가능한 공간을 기반으로 여러 장치 간에 아카이브를 확장할 수 있습니다. 시드 과정에서 증분 복구 지점이 대상 사이트에 복제됩니다. 대상 코어에서 시드 아카이브를 사용하면 새로 복제된 증분 복구 지점이 자동으로 동기화됩니다.

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 복제를 참조합니다.
- 타사 복제를 구성합니다. 타사 대상 Core 복제에 대한 자세한 내용은 타사 관리 Core에 복제를 참조합니다.
- 소스 Core에 첨부된 새 보호되는 시스템을 복제합니다. 보호되는 시스템 복제에 대한 자세한 내용은 새 보호되는 시스템 복제를 참조하십시오.
- 기존의 보호되는 시스템을 복제합니다. 복제를 위한 에이전트 구성에 대한 자세한 내용은 시스템에서 에이전트 데이터 복제를 참조하십시오.
- 에이전트의 복제 우선순위를 설정합니다. 에이전트의 복제 우선순위 설정에 대한 자세한 내용은 에이전트에 대한 복제 우선순위 설정을 참조하십시오.
- 필요한 경우 복제를 모니터합니다. 복제 모니터링에 대한 자세한 내용은 복제 모니터링을 참조하십시오.
- 필요에 따라 복제 설정을 관리합니다. 복제 설정 관리에 대한 자세한 내용은 복제 설정 관리를 참조하십시오.
- 재난 또는 데이터 유실이 발생할 경우 복제된 데이터를 복구합니다. 복제된 데이터 복구에 대한 자세한 내용은 복제된 데이터 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: **Administrator**).
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 건너뜁니다.

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 추가를 참조합니다. 계정과 연결된 **컨테이너**를 선택합니다. 아카이브된 데이터가 저장될 **폴더 이름**을 선택합니다.
   d. **다음**을 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.

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. • 기본 일정을 사용하여 모든 볼륨 보호 • 사용자 지정 일정을 사용하여 특정 볼륨 보호 **노트:** 기본 일정은 15분 간격입니다.

텍스트 상자	설명
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.

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)**을 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.

복제 모니터링

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

복제를 모니터하려면 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 4. 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 **Ignore(무시)**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 **Abandon(중단)**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. • **Details(상세정보)** - ID, URI, 표시 이름, 상태, 고객 ID, 전자 메일 주소 및 복제된 Core에 대한 주석을 나열합니다. • **Change Settings(설정 변경)** - 표시 이름을 나열하며, 이를 통해 대상 Core의 호스트와 포트를 편집할 수 있습니다. • **Add Agents(에이전트 추가)** - 드롭다운 목록에서 호스트를 선택하고, 복제할 보호되는 시스템을 선택하고, 새 보호되는 시스템의 초기 전송에 대한 시드 드라이브를 생성할 수 있습니다.
들어오는 복제	대상에서 복제된 데이터를 수신하는 모든 원본 시스템을 나열합니다. 여기에는 원격 Core 이름, 상태, 시스템 및 진행률이 포함됩니다.	대상 Core의 드롭다운 메뉴에서 다음 옵션을 선택할 수 있습니다. • **Details(상세정보)** - ID, 호스트 이름, 고객 ID, 전자 메일 주소 및 복제된 Core에 대한 주석을 나열합니다. • **Consume(사용)** — 시드 드라이브의 초기 데이터를 사용하

섹션	설명	사용 가능한 조치
		고 해당 데이터를 로컬 리포지토리에 저장합니다.

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
Relationship Only(관계만)	복제에서 보호되는 시스템을 제거하지만 복제된 복구 지점은 그대로 유지합니다.
With Recovery Point(복구 지점 포함)	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
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.

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 탑재
- 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 복구 이해

AppAssure에서는 서버 중지로 인해 소스 Core와 에이전트에 오류가 발생하는 경우에 복제된 환경에서 장애 조치 및 장애 복구를 지원합니다. 장애 조치는 시스템에 장애가 발생하거나 소스 Core와 해당 에이전트가 비정상적으로 종료될 때 중복 또는 대기 대상(AppAssure Core)으로 전환하는 것을 말합니다. 장애 조치의 기본 목적은 장애가 발생한 에이전트와 동일한 새 에이전트를 실행하는 것입니다. 그런 다음, 장애가 발생하기 전에 소스 Core가 초기 에이전트를 보호했던 방법과 동일한 방법으로 대상 Core에서 장애 조치 에이전트를 보호할 수 있도록 대상 Core를 새 모드로 전환하는 것입니다. 따라서 대상 Core는 복제된 에이전트에서 인스턴스를 복구하고 장애 조치된 시스템에서 즉시 보호를 시작할 수 있습니다.

장애 복구는 에이전트와 Core를 원래 상태(오류 발생 전)로 다시 복원하는 프로세스입니다. 장애 복구의 주요 목적은 에이전트(대부분의 경우 실패한 에이전트를 대체하는 새 시스템)를 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.

장애 조치 수행

소스 Core 및 연결된 에이전트가 실패하는 재난 상황이 발생하면 AppAssure에서 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.

   Fail Over(장애 조치) 대화 상자가 나타나고 장애 조치를 완료하는 데 필요한 단계가 나열됩니다.
4. **Continue(계속)**를 클릭합니다.
5. **Protected Machines(보호되는 시스템)** 아래의 왼쪽 탐색 영역에서, 복구 지점이 있는 AppAssure 에이전트 소프트웨어가 연결되어 있는 시스템을 선택합니다.
6. 해당 에이전트의 백업 복구 지점 정보를 가상 시스템으로 내보냅니다.
7. 해당 에이전트의 백업 복구 지점 정보를 가상 시스템으로 내보냅니다.
8. 이제 내보낸 백업 정보가 포함되어 있는 가상 시스템을 시작합니다.

   장치 드라이버 소프트웨어가 설치되는 동안 기다려야 합니다.
9. 가상 시스템을 재부팅하고 에이전트 서비스가 시작될 때까지 기다립니다.
10. 대상 Core의 Core 콘솔로 다시 돌아가 **Protected Machines(보호되는 시스템)** 아래 및 **Incoming Replication(들어오는 복제)** 아래의 **Replication(복제)** 탭에 새 에이전트가 표시되는지 확인합니다.

11. 여러 개의 스냅샷을 강제 적용하고 올바르게 완료되는지 확인합니다.
    자세한 내용은 스냅샷 강제 적용을 참조하십시오.
12. 이제 계속해서 장애 복구를 진행할 수 있습니다.
    자세한 내용은 장애 복구 수행을 참조하십시오.

장애 복구 수행

실패한 원래 소스 Core와 에이전트를 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)**을 클릭합니다.
   Continue(계속) 단추를 클릭하여 장애 복구를 완료하기 전에 수행해야 하는 단계를 설명하는 **Fail Back(장애 복구)** 대화 상자가 열립니다.
4. **Cancel(취소)**을 클릭합니다.
5. 장애 조치된 시스템에서 Microsoft SQL Server 또는 Microsoft Exchange Server를 실행 중인 경우 해당 서비스를 중지합니다.
6. 시스템의 스냅샷을 강제 적용합니다. 자세한 내용은 스냅샷 강제 적용을 참조하십시오.
7. 장애 조치된 시스템을 종료합니다.
8. 장애 조치된 에이전트의 아카이브를 생성하고 디스크 또는 네트워크 공유 위치에 출력합니다.
   아카이브 생성에 대한 자세한 내용은 아카이브 생성을 참조하십시오.
9. 아카이브를 생성한 후 새로 복구된 소스 Core의 Core 콘솔을 탐색하고 **Tools(도구)** 탭을 클릭합니다.
10. 8단계에서 생성한 아카이브를 가져옵니다.
    자세한 내용은 아카이브 가져오기를 참조하십시오.
11. 대상 Core의 Core 콘솔로 다시 돌아가 **Replication(복제)** 탭을 클릭합니다.
12. **Incoming Replication**(들어오는 복제) 아래에서 장애 조치 에이전트를 선택하고 상세정보를 확장합니다.
13. **Failback(장애 복구)** 대화 상자에서 **Continue(계속)**를 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.
    자세한 내용은 시스템 설정 구성을 참조하십시오.
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.

6

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.

7

도움말 얻기

설명서 및 소프트웨어 업데이트 찾기

Core 콘솔에서 AppAssure 및 DL1000 어플라이언스 설명서 및 소프트웨어 업데이트에 직접 연결할 수 있는 링크를 사용할 수 있습니다.

설명서

설명서의 링크에 액세스하려면 다음을 수행합니다.

1. Core 콘솔에서 **Appliance(어플라이언스)** 탭을 클릭합니다.
2. 왼쪽 창에서 **Appliance(어플라이언스)** → **Documentation(설명서)** 링크를 탐색합니다.

Software updates(소프트웨어 업데이트)

소프트웨어 업데이트의 링크에 액세스하려면 다음을 수행합니다.

1. Core 콘솔에서 **Appliance(어플라이언스)** 탭을 클릭합니다.
2. 왼쪽 창에서 **Appliance(어플라이언스)** → **Software Updates(소프트웨어 업데이트)** 링크를 탐색합니다.

Dell에 문의하기

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.

판매, 기술 지원 또는 고객 서비스 문제에 대해서는 **software.dell.com/support**를 통해 Dell에 문의하십시오.

설명서에 대한 사용자 의견

Dell 설명서의 모든 페이지에 있는 **Feedback(피드백)** 링크를 클릭해 양식을 작성한 다음 **Submit(제출)**을 클릭하여 의견을 보낼 수 있습니다.