Acronis

acronis.com

Acronis Cyber Protect 15

Update 6

사용자 안내서

수정 버전: 2023-06-15

목차

저작권 설명

Acronis 특허 기술

이 제품에 사용된 기술은 다음과 같이 하나 이상의 미국 특허 번호로 보호됩니다.7,047,380; 7,246,211; 7,275,139; 7,281,104; 7,318,135; 7,353,355; 7,366,859; 7,383,327; 7,475,282; 7,603,533; 7,636,824; 7,650,473; 7,721,138; 7,779,221; 7,831,789; 7,836,053; 7,886,120; 7,895,403; 7,934,064; 7,937,612; 7,941,510; 7,949,635; 7,953,948; 7,979,690; 8,005,797; 8,051,044; 8,069,320; 8,073,815; 8,074,035; 8,074,276; 8,145,607; 8,180,984; 8,225,133; 8,261,035; 8,296,264; 8,312,259; 8,347,137; 8,484,427; 8,645,748; 8,732,121; 8,850,060; 8,856,927; 8,996,830; 9,213,697; 9,400,886; 9,424,678; 9,436,558; 9,471,441; 9,501,234; 및 특허 대기 중인 애플리케이션.

Acronis Cyber Protect 15 버전

다음 버전에서는 Acronis Cyber Protect 15를 사용할 수 없습니다.

- Cyber Protect Essentials
- Cyber Protect Standard
- Cyber Protect Advanced
- Cyber Backup Standard
- Cyber Backup Advanced

각 버전에 포함된 기능에 대한 자세한 내용은 클라우드 디플로이를 포함한 Acronis Cyber Protect 15 버전 비교를 참조하십시오.

Acronis Cyber Protect 15의 모든 버전은 보호되는 워크로드 및 해당 유형(워크스테이션, 서버, 원격 호스트)의 개수에 따라 라이센스가 부여됩니다. Cyber Protect 버전은 구독 라이센스로만 사용할 수 있습니다. 사이버 백업 에디션은 서브스크립션 및 영구 라이센스로 사용할 수 있습니다. 사용 가능한 옵션에 대한 자세한 내용은 "라이센스"(21페이지)을(를) 참조하십시오.

버전 15의 영구 라이센스 키는 Acronis Cyber Backup 12.5의 백업 에이전트에 사용할 수 없습니다. 하지만 이러한 에이전트는 관리 서버가 버전 15로 업그레이드된 경우에도 기존 라이선스 키로 계속해서 작동합니다.

백업 서브스크립션 라이센스는 에이전트가 버전 15로 업그레이드된 경우에도 버전 12.5 에이전트에 사용할 수 있습니다. Cyber Protect 구독 라이센스는 버전 15 에이전트에만 사용할 수 있습니다.

버전 15 관리 서버에 등록된 버전 12.5 백업 에이전트는 백업 복제, 백업 유효성 검사, 정리 또는 가상 머신으로 전환과 같은 오프호스트 데이터 처리 작업을 수행할 수 없습니다.

참고

기능은 버전별로 다릅니다. 이 문서에 설명된 일부 기능은 사용자의 라이선스로 사용하지 못할 수 있습니다. 각 버전에 포함된 기능에 대한 자세한 내용은 클라우드 디플로이를 포함한 Acronis Cyber Protect 15 버전 비교를 참조하십시오.

운영 체제별 지원되는 Cyber Protect 기능

Cyber Protect 기능은 다음과 같은 운영 체제에서 지원됩니다.

- Windows: Windows 7 이상, Windows Server 2008 R2 이상.
  Windows Defender 바이러스 백신 관리는 Windows 8.1 이상에서 지원됩니다.
- Linux: CentOS 7.x, CentOS 8.0, Virtuozzo 7.x, Acronis Cyber Infrastructure 3.x.
  기타 Linux 배포 및 버전도 Cyber Protect 기능을 지원할 수 있지만 테스트는 거치지 않았습니다.
- macOS: 10.13.x 이상(바이러스 백신 및 맬웨어 방지 기능만 지원됨).

중요

Cyber Protect 기능은 보호 에이전트가 설치된 머신에만 지원됩니다. 예를 들어, Agent for Hyper-V, Agent for VMware 또는 Agent for Scale Computing 등의 에이전트가 없는 모드에서 보호되는 가상 머신의 경우 백업만 지원됩니다.

Cyber Protect 기능	Windows	Linux	macOS
포렌직 백업	예	아니요	아니요
지속적인 데이터 보호(CDP)			
파일 및 폴더 CDP	예	아니요	아니요
애플리케이션 추적을 통한 변경된 파일 CDP	예	아니요	아니요
자동 검색 및 원격 설치			
네트워크 기반 검색	예	아니요	아니요
Active Directory 기반 검색	예	아니요	아니요
템플릿 기반 검색(파일에서 머신 가져오기)	예	아니요	아니요
수동 장치 추가	예	아니요	아니요
Acronis 맬웨어 방지 기능			
프로세스 동작 기반(AI 기반) 랜섬웨어 감지	예	아니요	아니요
크립토마이닝 프로세스 감지됨	예	아니요	아니요
실시간 안티맬웨어 보호	예	아니요	예
로컬 캐시에서 영향을 받는 파일 자동 복구	예	아니요	아니요
Acronis 백업 파일 자체 보호	예	아니요	아니요
Acronis 소프트웨어 자체 보호	예	아니요	아니요
이식 가능 파일에 대한 고정 분석	예	아니요	예*
외장 드라이브 보호(HDD, 플래시 드라이브, SD 카드)	예	아니요	아니요
네트워크 폴더 보호	예	아니요	아니요
서버측 보호	예	아니요	아니요
Zoom, WebEx, Microsoft Teams 및 기타 원격 업무	예	아니요	아니요

보호			
온디맨드 맬웨어 방지 스캔	예	아니요	예
아카이브 파일 스캔	예	아니요	예
파일/폴더 제외	예	아니요	예**
프로세스 제외	예	아니요	아니요
기업 전반 허용 목록	예	아니요	예
동작 감지	예	아니요	아니요
격리	예	아니요	예
URL 필터링(http/https)	예	아니요	아니요
Windows Defender 안티바이러스 관리	예	아니요	아니요
Microsoft Security Essentials 관리	예	아니요	아니요
취약성 평가			
운영 체제 및 해당 기본 애플리케이션 취약성 평가	예	예***	아니요
서드 파티 애플리케이션 취약성 평가	예	아니요	아니요
패치 관리			
패치 자동 승인	예	아니요	아니요
수동 패치 설치	예	아니요	아니요
자동 패치 설치 예약	예	아니요	아니요
장애 안전 패치: 보호 계획의 일부로 패치 설치 전 머신 백업	예	아니요	아니요
백업이 실행 중인 경우 머신 다시 시작 취소	예	아니요	아니요
데이터 보호 맵			
보호되지 않은 파일을 찾기 위한 머신 스캔	예	아니요	아니요
보호되지 않은 위치 개요	예	아니요	아니요
데이터 보호 맵의 보호 조치	예	아니요	아니요

디스크 상태			
AI 기반 HDD 및 SDD 상태 제어	예	아니요	아니요
Acronis 사이버 보호 작업 센터(CPOC) 경보에 기반한 스마트 보호 계획			
위협 피드	예	아니요	아니요
수정 마법사	예	아니요	아니요
백업 스캔			
암호화된 백업 스캔	예	아니요	아니요
로컬 스토리지, 네트워크 공유 및 Acronis Cloud Storage에서 디스크 백업 스캔	예	아니요	아니요
안전 복구			
복구 프로세스 중 Acronis 바이러스 백신 및 맬웨어 방지 기능을 사용한 맬웨어 방지 스캔	예	아니요	아니요
원격 데스크톱			
HTML5 기반 클라이언트를 통해 연결	예	아니요	아니요
기본 Windows RDP 클라이언트를 통해 연결	예	아니요	아니요
원격 지우기	예****	아니요	아니요
Cyber Protect 모니터링	예	아니요	예

* macOS에서 이식 가능 파일에 대한 고정 분석은 예약된 스캔에 대해서만 지원됩니다.

** macOS에서는 제외를 사용해야만 실시간 보호 또는 예약된 스캔에 의해 스캔되지 않을 파일 및 폴더를 지정할 수 있습니다.

*** 취약성 평가는 특정 배포에 대한 공식 보안 자문의 가용성에 따라 달라집니다(예: https://lists.centos.org/pipermail/centos-announce, https://lists.centos.org/pipermail/centos-cr-announce 및 기타).

**** 원격 지우기는 Windows 10 이상을 실행 중인 머신에만 이용할 수 있습니다.

라이센스

Acronis Cyber Protect을(를) 사용하여 워크로드를 보호하려면 라이센스가 필요합니다. Acronis Cyber Protect 설치 시 라이센스는 필요하지 않습니다.

라이센스 유형

Acronis Cyber Protect은(는) 서브스크립션 라이센스를 구매하면 사용할 수 있습니다. 라이센스 구매일부터 시작되는 유효 기간 동안에는 업데이트와 무료 기술 지원을 제한 없이 받을 수 있습니다. 유효 기간이 끝나면 기존 보호 계획의 작동이 중지되며 새 보호 계획을 생성할 수 없게 됩니다.

레거시 영구 라이센스는 갱신할 수 있습니다. 영구 라이센스 사용 시에는 클라우드 디플로이, 클라우드 간 백업 등의 일부 기능을 사용할 수 없습니다.

평가판 라이센스도 사용 가능합니다. 평가판 라이센스 사용 시에는 라이센스를 활성화하는 날로부터 30일 동안 모든 제품 기능을 사용할 수 있습니다.

다양한 라이센스 옵션과 관련된 자세한 내용은 지식 베이스에서 Acronis Cyber Protect 15: 라이센싱 및 업그레이드/다운그레이드 FAQ를 참조하십시오. Acronis 라이센스 정책은 https://www.acronis.com/company/licensing.html에서 확인할 수 있습니다.

중요
Acronis Cyber Protect 15 Update 3에는 새로운 라이센스 모델이 도입되었습니다. 이 모델에서는 라이센스 등록 및 온-프레미스 관리 서버 활성화 작업이 필요합니다.

Acronis Cyber Protect 15 Update 3 이상 버전에서 라이센스 관리

Acronis Cyber Protect 15 Update 3 이상 버전에서는 관리 서버(`https://<관리 서버 IP 주소>:<포트>`)의 로컬 콘솔에 라이센스 키가 추가되지 않습니다.

대신 Acronis Customer Portal(`https://account.acronis.com`)에서 계정에 라이센스를 추가한 다음 Acronis Cyber Protect 클라우드 콘솔(`https://cloud.acronis.com`)에서 라이센스를 관리할 수 있습니다.

오프라인 관리 서버의 라이센스를 관리하려면 로컬 콘솔과 클라우드 콘솔 모두에서 작업해야 합니다.

로컬 콘솔 및 클라우드 콘솔에 대해 자세히 알아보려면 "Acronis 계정, 로컬 및 클라우드 콘솔"(23 페이지) 항목을 참조하십시오.

Acronis Cyber Protect 15 Update 3 이상 버전에서 관리 서버 사용을 시작하려면

1. Acronis Customer Portal(`https://account.acronis.com`)에서 계정에 라이센스를 하나 이상 추가합니다.
   온라인에서 구매한 라이센스는 이 계정에 자동 추가됩니다.

2. [온-프레미스 디플로이 모드의 경우] 관리 서버를 활성화합니다.
3. 관리 서버에 라이센스를 할당합니다.

관리 서버의 유형

디플로이 모드에 따라 다음과 같은 관리 서버 유형을 사용할 수 있습니다.

- 클라우드 관리 서버
- 온프레미스 관리 서버
  - 온라인 관리 서버
  - 오프라인 관리 서버

Acronis 계정에 관리 서버가 여러 개 있을 수 있습니다. 클라우드 관리 서버와 온-프레미스 관리 서버에 혼합 디플레이 모델을 사용할 수도 있습니다.

관리 서버를 여러 개 사용한다면 관리 서버 간에 라이센스 할당량을 분할할 수 있습니다. 이 작업을 수행하는 방법에 대한 자세한 내용은 "다른 관리 서버로 라이센스 할당량 전송"(32페이지) 항목을 참조하십시오.

클라우드 관리 서버

클라우드 디플로이 시에는 네트워크에서 관리 서버를 설치 및 유지 관리하지 않습니다. Acronis 데이터 센터에 이미 디플로이된 관리 서버를 사용하면 되므로 워크로드용 보호 에이전트만 설치하면 됩니다.

클라우드 관리 서버는 활성화할 필요가 없습니다. 클라우드 관리 서버는 항상 온라인 상태이며, 라이센스 정보는 Acronis 계정과 서버 간에 자동으로 동기화됩니다.

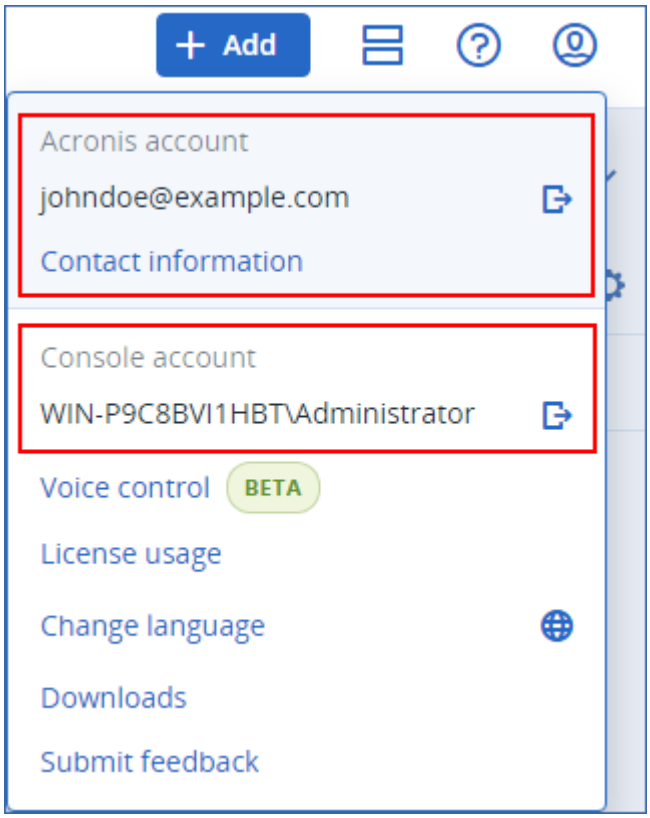
온프레미스 관리 서버

온-프레미스 디플로이 시에는 네트워크에 관리 서버와 보호 에이전트를 모두 설치합니다. 인터넷에 연결되지 않은 오프라인 관리 서버를 사용할 수도 있고, 인터넷에 액세스할 수 있는 온라인 관리 서버를 사용할 수도 있습니다.

온프레미스 관리 서버는 활성화해야 합니다. 활성화에 대한 자세한 내용은 "관리 서버 활성화"(26페이지) 항목을 참조하십시오.

참고

활성화된 온-프레미스 관리 서버의 로컬 콘솔에 두 개의 계정이 표시됩니다. 하나는 라이센스 정보를 동기화하는 데 사용되는 Acronis 계정이고 다른 하나는 로컬 콘솔 자체에 액세스하는 데 사용되는 콘솔 계정입니다.



온라인 온-프레미스 관리 서버

온라인 관리 서버는 인터넷을 통해 활성화합니다. 활성화를 수행하려면 로컬 콘솔에 처음 액세스할 때 Acronis 계정에 로그인합니다.

오프라인 온-프레미스 관리 서버

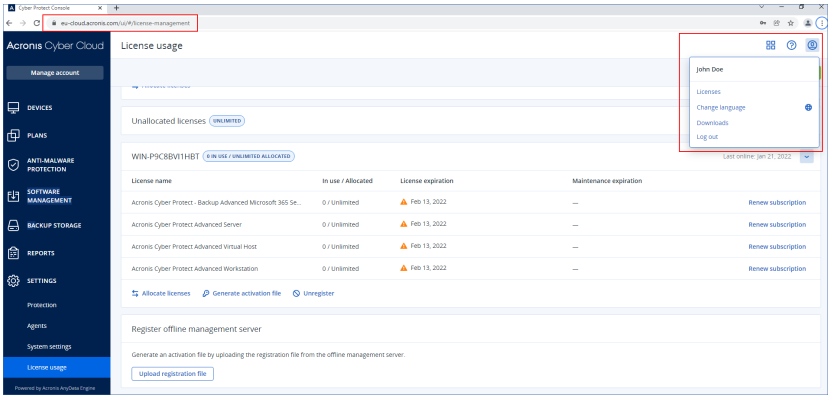
오프라인 관리 서버는 파일을 사용하여 활성화한 후 Acronis 계정과 수동으로 라이센스 정보를 동기화합니다.

Acronis 계정, 로컬 및 클라우드 콘솔

Acronis Cyber Protect을(를) 사용하고 라이센스 및 라이센스 사용을 관리하려면 Acronis 계정이 필요합니다. 모든 라이센스 및 관리 서버는 해당 계정에 등록됩니다.

이 계정을 사용하여 다음 콘솔에 액세스할 수 있습니다.

- 클라우드 콘솔(https://cloud.acronis.com)

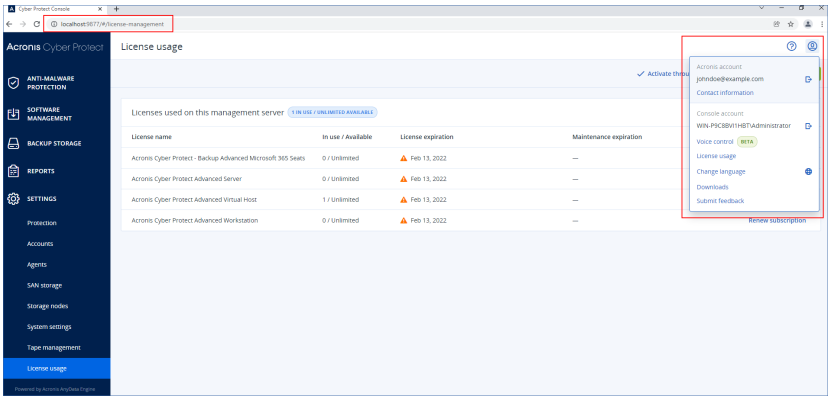


참고

클라우드 콘솔에 로그인하면 해당 URL이 변경되어 계정이 속해 있는 정확한 데이터 센터가 표시됩니다. 예: https://eu-cloud.acronis.com 또는 https://jp-cloud.acronis.com.

클라우드 콘솔은 라이센스를 관리하는 기본 위치입니다. 클라우드 콘솔의 **설정** > **라이센스 사용** 탭에서 특정 관리 서버에 사용 가능한 라이센스 및 라이센스 할당량 할당, 라이센스 할당량을 다른 관리 서버에 재할당, 오프라인 관리 서버 등록 완료 등의 작업을 수행할 수 있습니다.

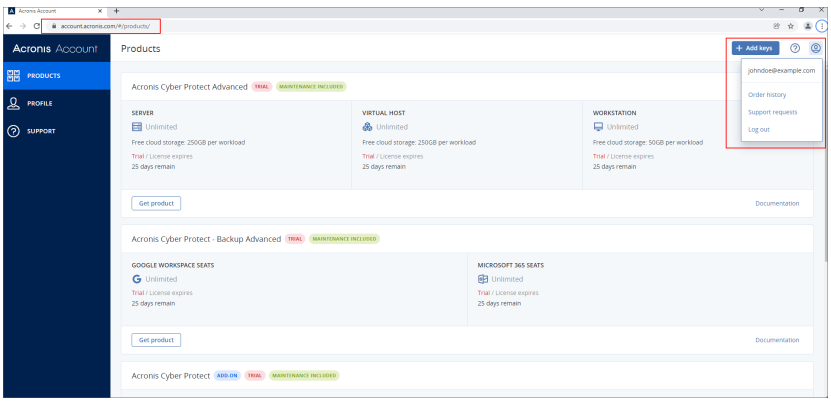
- 온-프레미스 관리 서버(https://<관리 서버 IP 주소>:<포트>)의 로컬 콘솔



이 콘솔에서 할당된 라이센스, 라이센스 할당량 및 사용, 만료 날짜를 확인할 수 있습니다.

오프라인 관리 서버를 활성화하거나 오프라인 관리 서버에 라이센스를 할당할 때 로컬 콘솔을 클라우드 콘솔과 함께 사용할 수 있습니다.

- Acronis Customer Portal(https://account.acronis.com)



Acronis Customer Portal에서는 서브스크립션 만료 날짜 확인, 새 라이센스 키 추가, 라이센스 갱신 등록, 업그레이드 요청 등의 작업을 통해 구매한 제품을 관리할 수 있습니다. 지원 팀에 문의, 제품 설치 파일 다운로드, 제품 설명서 액세스 등의 작업도 가능합니다.

라이센스 관리

아래 표에는 사용 가능한 작업 및 해당 작업을 수행하는 위치가 요약되어 있습니다.

작업	위치
계정에 라이센스 추가	라이센스는 Acronis Customer Portal(https://account.acronis.com)에서 추가합니다. 온라인에서 구매한 라이센스는 자동 추가됩니다.
관리 서버 활성화	관리 서버는 계정에 등록하는 방식으로 활성화합니다. 온라인 관리 서버는 계정에 로그인하여 해당 로컬 콘솔(https://<관리 서버 IP 주소:<포트>)에서 활성화합니다. 오프라인 관리 서버를 활성화하려면 로컬 콘솔과 클라우드 콘솔 모두에서 작업해야 합니다.
관리 서버에 라이센스 할당 기존 라이센스 할당 수정	온라인 관리 서버에서는 클라우드 콘솔(https://cloud.acronis.com)을 사용하여 라이센스를 할당합니다.할당된 라이센스는 관리 서버와 자동으로 동기화됩니다. 오프라인 관리 서버에서는 활성화 파일을 통해 라이센스를 할당합니다. 이 절차를 수행하려면 관리 서버(https://<관리 서버 IP 주소:<포트>)의 로컬 콘솔과 클라우드 콘솔(https://cloud.acronis.com)을 모두 사용해야 합니다.
워크로드에 라이센스 할당	이 작업은 자동으로 수행됩니다.
계정에서 관리 서버 등록 해제	온라인 관리 서버는 클라우드 콘솔(https://cloud.acronis.com)을 사용하여 등록 해제합니다. 오프라인 관리 서버는 비활성화 파일을 통해 등록 해제합니다. 이 절차를 수행하려면 오프라인 관리 서버(https://<관리 서버 IP 주소:<포트>)의 로컬 콘솔과 클라우드 콘솔(https://cloud.acronis.com)을 모두 사용해야 합니다. 액세스할 수 없는 오프라인 관리 서버는 클라우드 콘솔만 사용하여 등록 해제합니다.

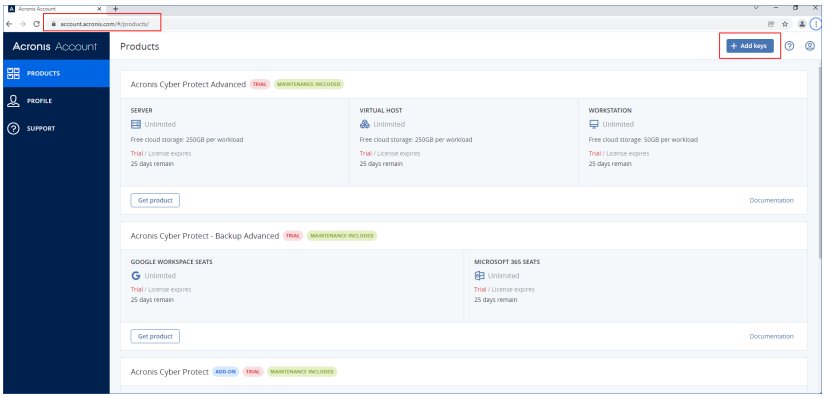
Acronis 계정에 라이센스 추가

라이센스를 사용하려면 Acronis 계정에 추가해야 합니다. 온라인에서 구매한 라이센스는 계정에 자동 추가됩니다. 오프라인에서 구매한 라이센스는 수동으로 추가해야 합니다.

Acronis 계정에 라이센스를 추가하려면

1. 계정 자격 증명을 사용하여 Acronis Customer Portal(https://account.acronis.com)에 로그인합니다.

2. 네비게이션 메뉴에서 **제품**을 클릭합니다.
3. **키 추가**를 클릭합니다.



4. 라이센스 키 하나 이상을 한 줄에 하나씩 입력하고 **추가**를 클릭합니다.

> **참고**
> 라이선스 키는 한 번에 100개까지 입력할 수 있습니다.

라이센스가 계정에 추가됩니다. 그러면 클라우드 콘솔(https://cloud.acronis.com)에서 라이센스 사용을 관리할 수 있습니다.

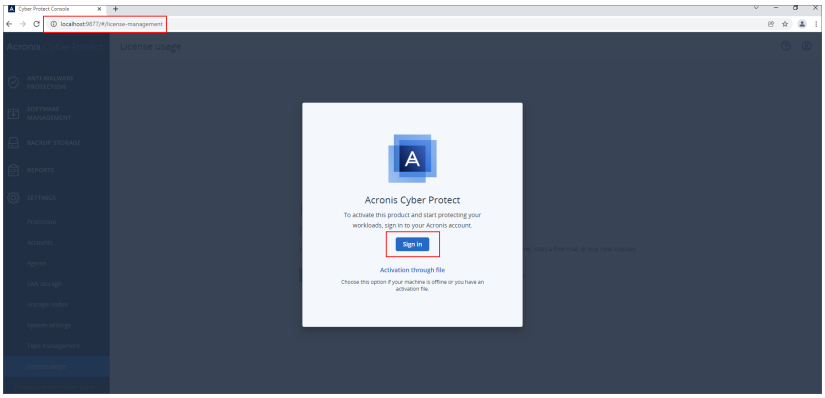
> **중요**
> Acronis Cyber Protect 15 Update 3로 업그레이드하기 전에 로컬에 저장되어 있는 영구 라이센스를 파일로 내보낸 후 Acronis 계정에 추가합니다.
>
> 관리 서버에서 로컬로 입력한 라이센스 키를 확인하려면 `https://<관리 서버 IP 주소>:<포트>/api/account_server/v2/licensing/legacy/license_keys`로 이동합니다.

관리 서버 활성화

관리 서버는 Acronis 계정에 등록하는 방식으로 활성화합니다.

온라인 관리 서버를 활성화하려면

1. Acronis Cyber Protect 관리 서버(`https://<관리 서버 IP 주소>:<포트>`)를 설치한 후 해당 로컬 콘솔을 엽니다.
2. 대화 상자가 열리면 **로그인**을 클릭합니다.



3. Acronis 계정에 로그인합니다.

   이렇게 하면 관리 서버가 자동으로 등록 및 활성화됩니다.

   워크로드 보호를 시작하려면 이 서버에 라이센스를 하나 이상 할당합니다. 라이센스를 할당하는 방법을 자세히 알아보려면 "관리 서버에 라이센스 할당"(30페이지) 항목을 참조하십시오.

참고
온라인 관리 서버에서는 인터넷에 액세스하여 Acronis 계정에 라이센스 정보를 동기화해야 합니다. 이러한 서버의 오프라인 상태가 30일 넘게 유지되면 해당 보호 계획의 작동이 중지되며 워크로드는 보호되지 않는 상태가 됩니다.

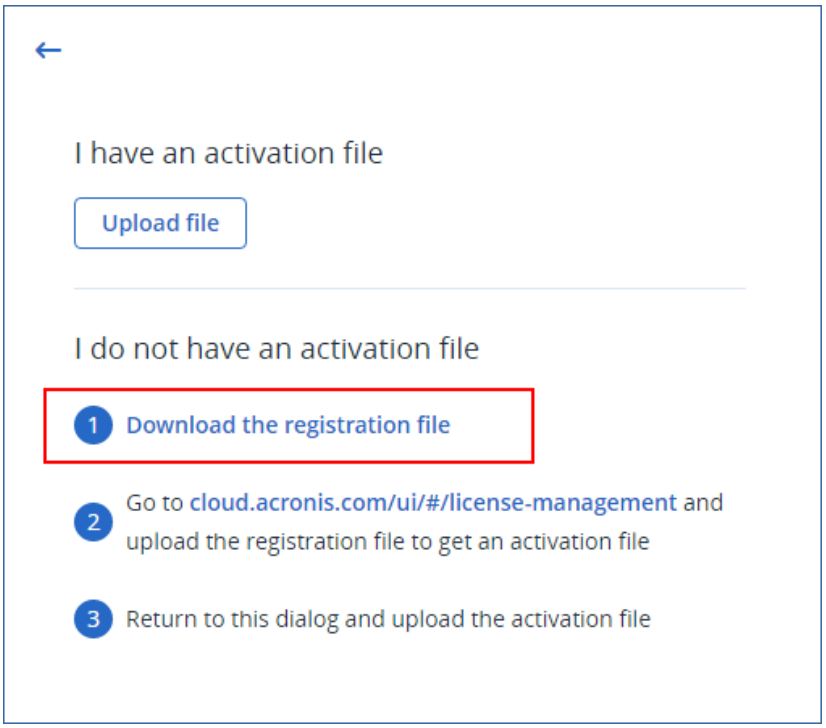
로컬 콘솔에서 Acronis 계정에서 로그아웃하면 라이센스 정보를 동기화할 수 없습니다. 30일 넘게 다시 로그인하지 않으면 보호 계획의 작동이 중지되며 워크로드는 보호되지 않는 상태가 됩니다.

오프라인 관리 서버를 활성화하려면

오프라인 관리 서버를 활성화하려면 로컬 콘솔과 클라우드 콘솔 모두에서 작업해야 합니다.

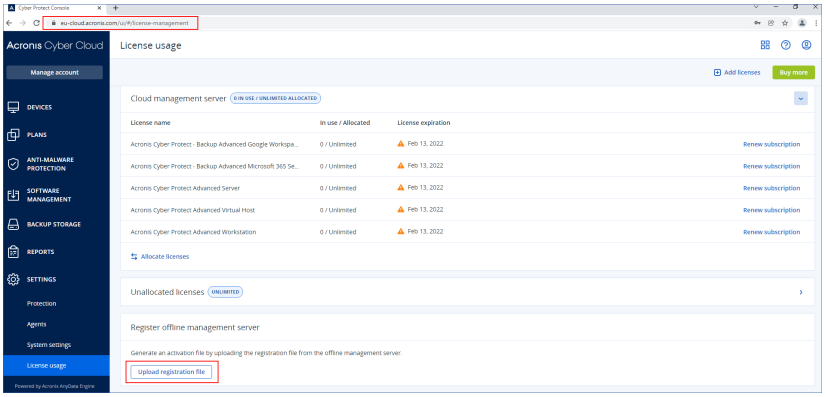
클라우드 콘솔에 액세스하려면 인터넷에 연결된 두 번째 머신이 있어야 합니다.

1. Acronis Cyber Protect 관리 서버(`https://<관리 서버 IP 주소>:<포트>`)를 설치한 후 해당 로컬 콘솔을 엽니다.
2. 대화 상자가 열리면 **파일을 통한 활성화**를 클릭합니다.
3. **활성화 파일이 없습니다.** 아래에서 **등록 파일 다운로드**를 클릭합니다.



머신에 등록 파일이 다운로드됩니다.

4. 인터넷에 액세스할 수 있는 머신에서 클라우드 콘솔(https://cloud.acronis.com)에 로그인한 후 **설정** > **라이센스 사용**으로 이동합니다.
5. **오프라인 관리 서버 등록** 섹션에서 **등록 파일 업로드**를 클릭합니다.



6. 대화 상자가 열리면 **찾아보기**를 클릭한 다음 오프라인 관리 서버에서 다운로드한 등록 파일을 선택합니다.
7. 대화 상자가 열리면 **파일 다운로드**를 클릭합니다.
   머신에 활성화 파일이 다운로드됩니다.

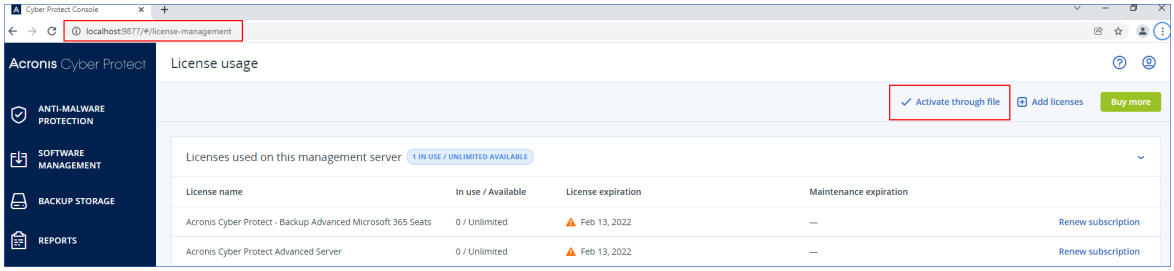
중요

환경 내의 관리 서버가 해당 오프라인 관리 서버뿐이라면 Acronis 계정의 라이센스가 해당 서버에 자동 할당됩니다. 이 정보는 활성화 파일에 포함되어 있으므로 라이센스를 추가로 할당할 필요가 없습니다.

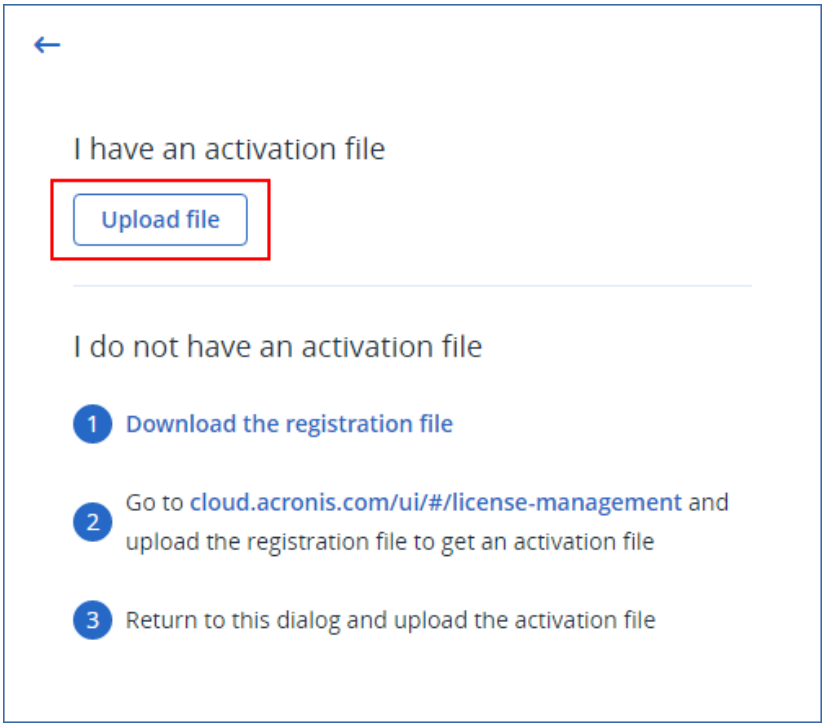
환경 내에 다른 관리 서버도 있다면 활성화 후 "관리 서버에 라이센스 할당"(30페이지)의 절차에 따라 라이센스를 할당해야 합니다.

8. 오프라인 관리 서버(https://<관리 서버 IP 주소>:<포트>)의 로컬 콘솔에서 **파일을 통한 활성화** 대화 상자로 이동합니다.

참고
파일을 통한 활성화 대화 상자가 열리지 않으면 **설정** > **라이센스 사용**으로 이동하여 **파일을 통한 활성화**를 클릭합니다.



9. **활성화 파일이 있습니다.** 아래에서 **파일 업로드**를 클릭하고 클라우드 콘솔에서 다운로드한 활성화 파일을 선택합니다.



그러면 오프라인 관리 서버가 Acronis 계정에 등록되고 활성화됩니다.

참고
고유하지 않은 UUID를 사용하는 가상 머신에서 실행되는 관리 서버는 활성화할 수 없을 수도 있습니다. 예를 들어, VMware vCenter Converter를 사용하여 가상 머신의 UUID를 복제하거나 변환하는 작업을 수행하지 못할 수 있습니다. 이와 유사한 문제가 발생하면 지원 팀에 문의하십시오.

VMware 가상 머신에서 UUID 복제를 방지하는 방법을 자세히 알아보려면 복제 UUID.bios (1002403)를 사용하여 가상 머신 편집을 참조하십시오.

관리 서버에 라이센스 할당

라이센스를 사용하려면 관리 서버에 라이센스 할당량 또는 할당량 중 일부를 할당해야 합니다. 관리 서버 하나에 여러 라이센스를 할당할 수 있습니다. 라이센스 할당량을 분할하여 서로 다른 여러 관리 서버에 할당량 중 일부를 각각 할당할 수도 있습니다.

참고
Acronis 계정에 관리 서버가 하나뿐이면 모든 라이센스가 해당 서버에 자동 할당됩니다. 다른 관리 서버에 라이센스를 재할당하는 방법을 자세히 알아보려면 "다른 관리 서버로 라이센스 할당량 전송"(32페이지) 항목을 참조하십시오.

Acronis 계정에 관리 서버가 여러 개라면 클라우드 콘솔(https://cloud.acronis.com)의 **라이센스가 할당되지 않음**에 새 라이센스가 표시됩니다. 이러한 라이센스는 수동으로 할당해야 합니다.

모든 라이센스 관련 작업은 온라인 관리 서버와 자동으로 동기화됩니다. 할당 변경 사항을 오프라인 관리 서버와 동기화하려면 새 활성화 파일을 생성한 후 할당 절차를 반복합니다. 다양한 관리 서버에 대해 자세히 알아보려면 "관리 서버의 유형"(22페이지) 항목을 참조하십시오.

온라인 관리 서버에 라이센스를 할당하려면

1. 클라우드 콘솔(https://cloud.acronis.com)에서 **설정** > **라이센스 사용**을 클릭합니다.
2. 라이센스를 할당할 관리 서버로 이동합니다.
3. **라이센스 할당**을 클릭합니다.
4. 대화 상자가 열리면 해당 서버에 할당할 라이센스와 라이센스 할당량을 지정합니다.
5. **저장**을 클릭합니다.

그러면 라이센스 정보가 관리 서버와 자동 동기화되므로 할당된 라이센스를 사용하여 워크로드를 보호할 수 있습니다.

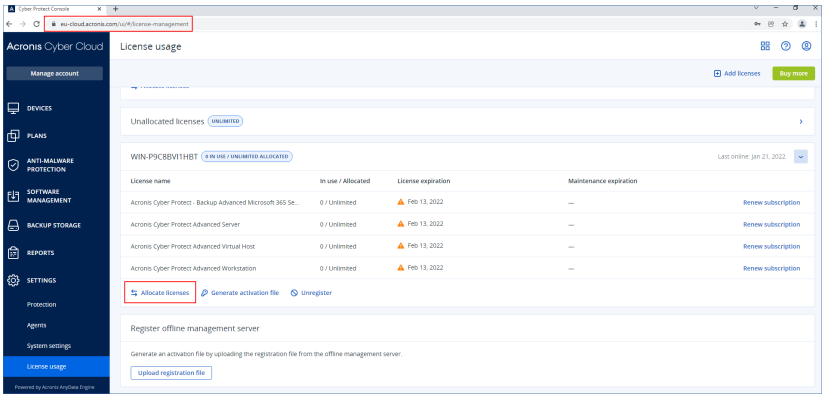
할당을 수정하려면 위 절차를 반복합니다.

중요
수정된 라이센스 할당량이 보호 에이전트 수보다 작으면 로드가 가장 적은 에이전트의 작동이 중지됩니다. 라이센스 할당량은 자동으로 선택됩니다. 자동 선택된 할당량으로는 요구를 충족할 수 없으면 사용 가능한 라이센스를 수동으로 재할당합니다.

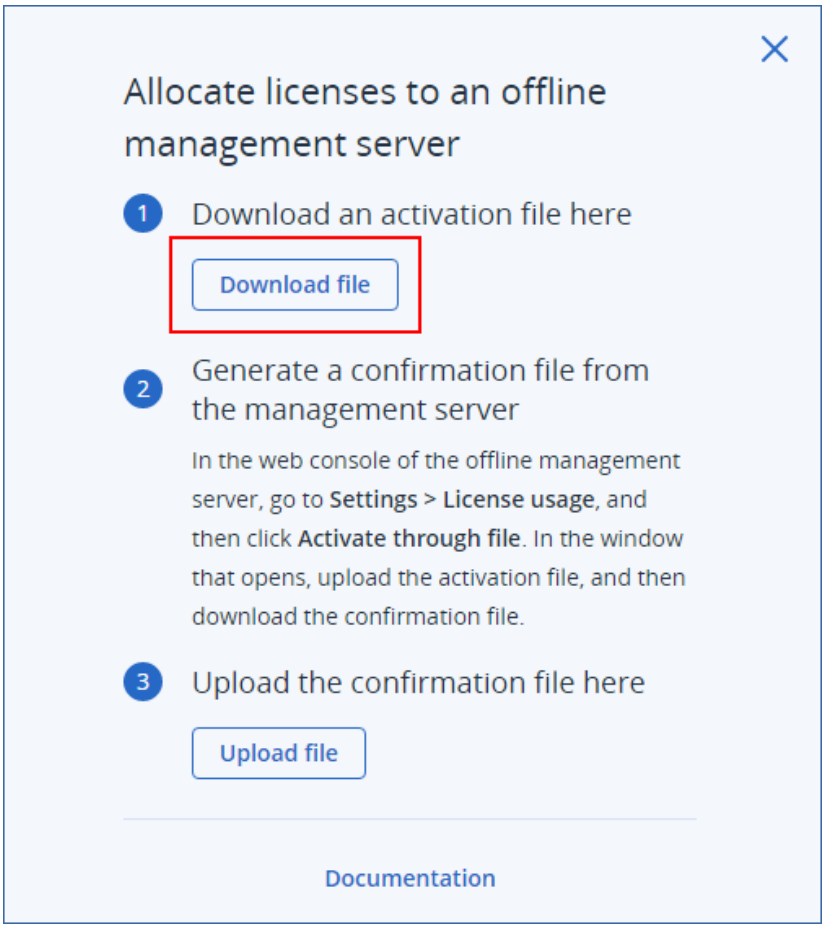
오프라인 관리 서버에 라이센스를 할당하려면

오프라인 관리 서버에 라이센스를 할당하려면 클라우드 콘솔과 로컬 콘솔을 모두 사용해야 합니다. 클라우드 콘솔에 액세스하려면 인터넷에 연결된 두 번째 머신이 있어야 합니다.

1. 인터넷에 액세스할 수 있는 머신에서 클라우드 콘솔(https://cloud.acronis.com)에 로그인한 후 **설정** > **라이센스 사용**을 클릭합니다.
2. 라이센스를 할당할 관리 서버로 이동합니다.
3. **라이센스 할당**을 클릭합니다.

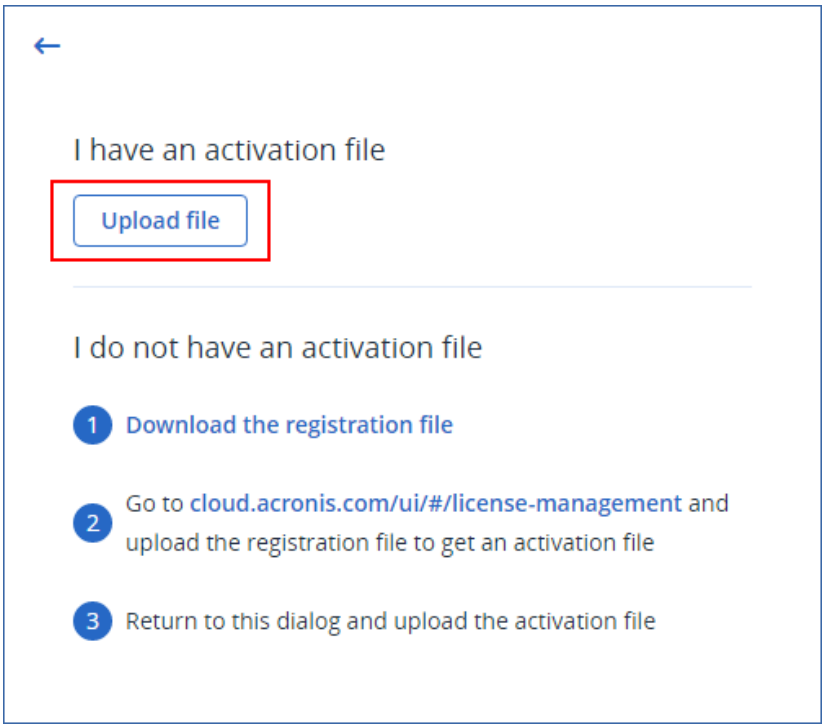


4. 대화 상자가 열리면 해당 서버에 할당할 라이센스와 라이센스 할당량을 지정합니다.
5. **저장**을 클릭합니다.
6. **오프라인 관리 서버에 라이센스 할당** 대화 상자에서 **파일 다운로드**를 클릭합니다.



머신에 활성화 파일이 다운로드됩니다.

7. 오프라인 관리 서버(https://<관리 서버 IP 주소>:<포트>)의 로컬 콘솔에서 **설정** > **라이센스 사용**으로 이동하여 **파일을 통한 활성화**를 클릭합니다.
8. 대화 상자가 열리면 **활성화 파일이 있습니다.** 아래에서 **파일 업로드**를 클릭하고 클라우드 콘솔에서 다운로드한 활성화 파일을 선택합니다.



그러면 오프라인 관리 서버와 Acronis 계정 간에 라이센스 정보가 동기화됩니다.

라이센스 할당량을 늘리려면 위 절차를 반복합니다.

라이센스 할당량을 줄이려면 "오프라인 관리 서버에 할당된 라이센스 할당량 줄이기"(33페이지) 항목을 참조하십시오.

다른 관리 서버로 라이센스 할당량 전송

관리 서버 간에 라이센스 할당량을 전송할 수 있습니다. 특정 관리 서버에 할당된 라이센스를 사용하는 워크로드가 없고 다른 관리 서버에 라이센스가 더 필요한 경우 이 옵션이 유용할 수 있습니다.

참고

Acronis 계정에 관리 서버가 하나뿐이면 모든 라이센스가 해당 서버에 자동 할당됩니다.

Acronis 계정에 관리 서버가 여러 개라면 클라우드 콘솔(https://cloud.acronis.com)의 **라이센스가 할당되지 않음**에 새 라이센스가 표시됩니다. 이러한 라이센스는 수동으로 할당해야 합니다.

다른 관리 서버로 라이센스 할당량을 전송하려면

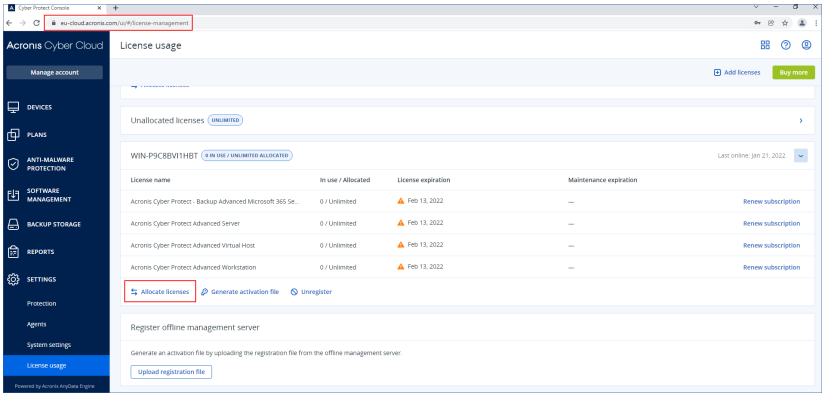
1. "관리 서버에 라이센스 할당"(30페이지)의 절차에 따라 원래 관리 서버에 할당된 라이센스 할당량을 줄입니다.

   점유 해제된 라이센스 할당량은 클라우드 콘솔의 **라이센스가 할당되지 않음** 섹션에 표시됩니다.
2. "관리 서버에 라이센스 할당"(30페이지)의 절차에 따라 두 번째 관리 서버에 라이센스 할당량을 할당합니다.

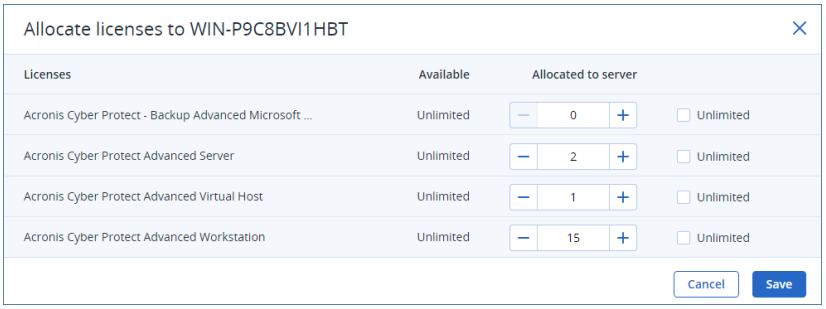
오프라인 관리 서버에 할당된 라이센스 할당량 줄이기

오프라인 관리 서버에 할당된 라이센스 할당량을 줄이려면 클라우드 콘솔과 로컬 콘솔을 모두 사용해야 합니다. 클라우드 콘솔에 액세스하려면 인터넷에 연결된 두 번째 머신이 있어야 합니다.

1. 인터넷에 액세스할 수 있는 머신에서 클라우드 콘솔(https://cloud.acronis.com)에 로그인한 후 **설정** > **라이센스 사용**을 클릭합니다.
2. 라이센스를 할당할 관리 서버로 이동하여 **라이센스 할당**을 클릭합니다.

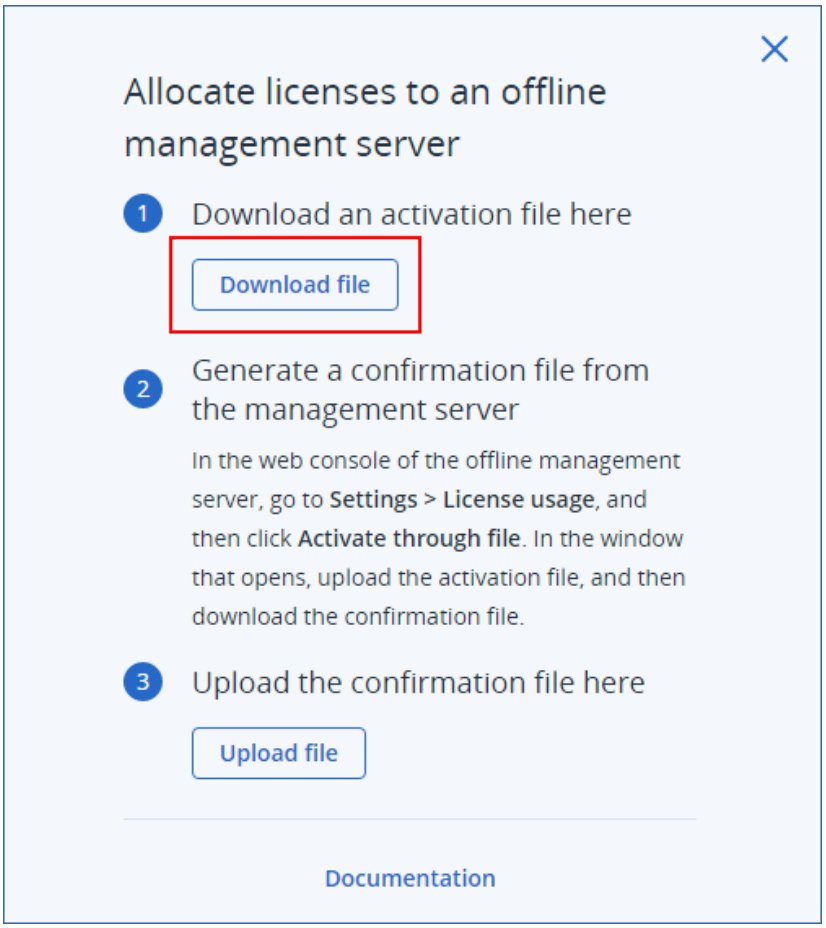


3. 대화 상자가 열리면 해당 서버에 할당된 라이센스와 라이센스 할당량을 수정한 후 **저장**을 클릭합니다.



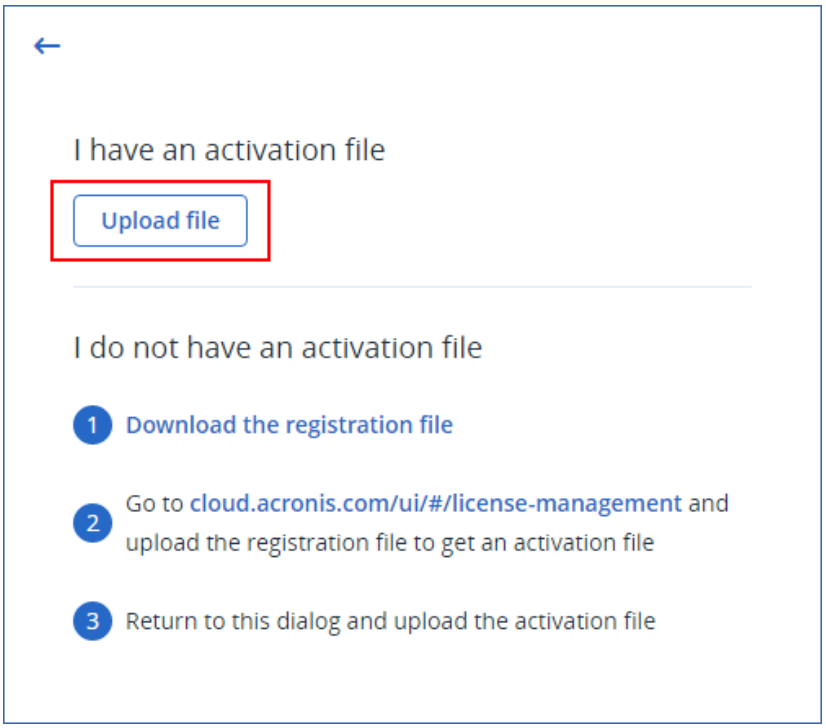
새 할당이 보류 중 상태로 설정됩니다. 새 할당을 취소하려면 **이 할당 제거**를 클릭합니다.

4. **오프라인 관리 서버에 라이센스 할당** 대화 상자에서 **파일 다운로드**를 클릭합니다.

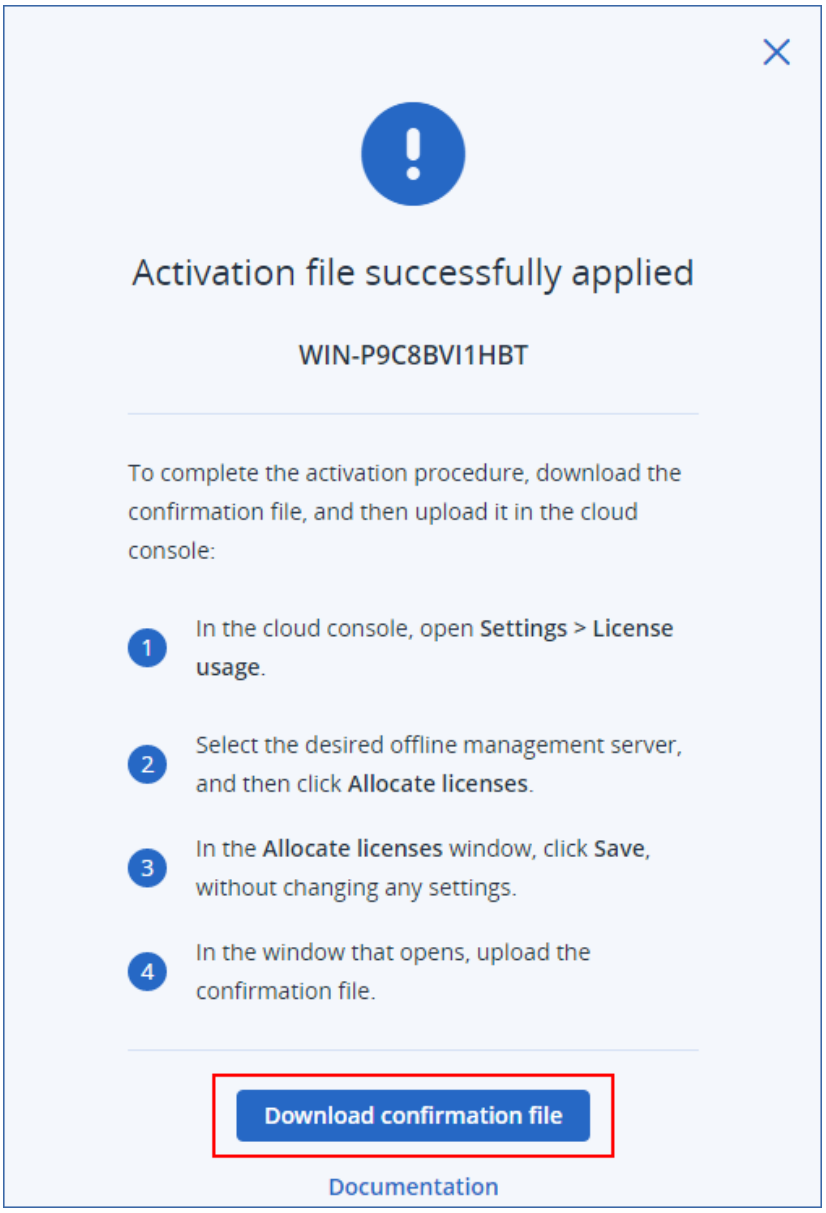


머신에 활성화 파일이 다운로드됩니다.

5. 오프라인 관리 서버(https://<관리 서버 IP 주소>:<포트>)의 로컬 콘솔에서 **설정** > **라이센스 사용**으로 이동하여 **파일을 통한 활성화**를 클릭합니다.
6. 대화 상자가 열리면 **활성화 파일이 있습니다.** 아래에서 **파일 업로드**를 클릭하고 클라우드 콘솔에서 다운로드한 활성화 파일을 선택합니다.

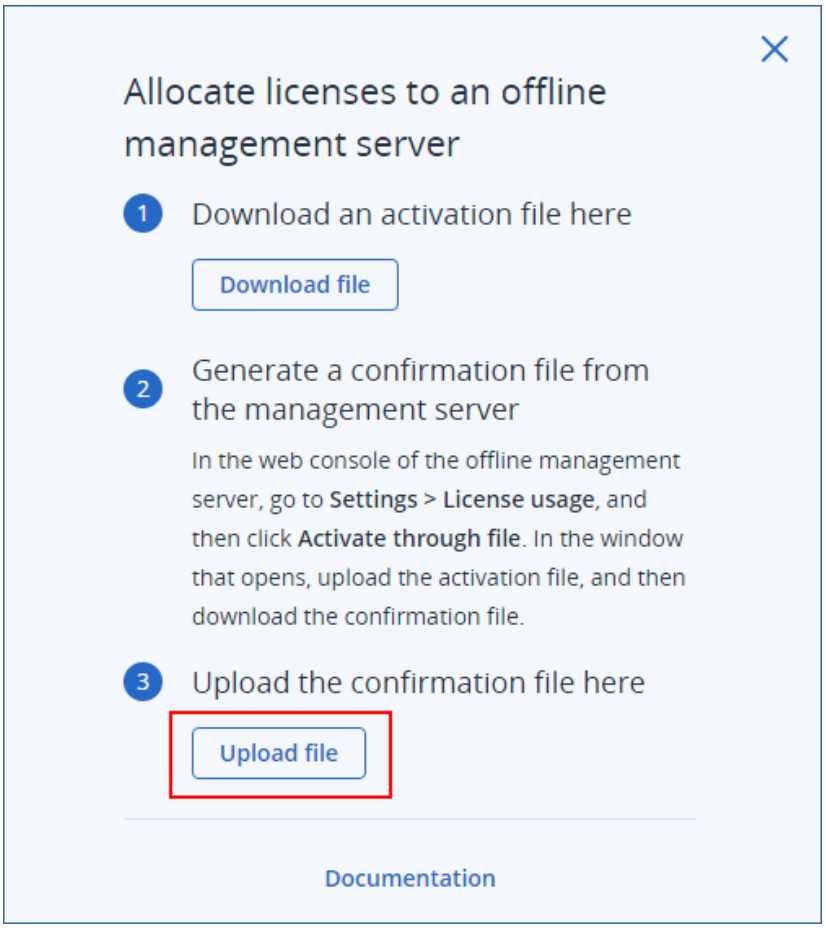


7. 대화 상자가 열리면 **확정 파일 다운로드**를 클릭합니다.



머신에 확정 파일이 다운로드됩니다.

8. 클라우드 콘솔(https://cloud.acronis.com)에서 **설정** > **라이센스 사용**을 클릭합니다.
9. 라이센스를 할당할 관리 서버로 이동하여 **라이센스 할당**을 클릭합니다.
10. 대화 상자가 열리면 설정을 변경하지 않고 **저장**을 클릭합니다.
11. **오프라인 관리 서버에 라이센스 할당** 대화 상자에서 **파일 업로드**를 클릭하고 오프라인 관리 서버에서 다운로드한 확정 파일을 선택합니다.



그러면 오프라인 관리 서버와 Acronis 계정 간에 라이센스 정보가 동기화됩니다.

중요
수정된 라이센스 할당량이 보호 에이전트 수보다 작으면 로드가 가장 적은 에이전트의 작동이 중지됩니다. 라이센스 할당량은 자동으로 선택됩니다. 자동 선택된 할당량으로는 요구를 충족할 수 없으면 사용 가능한 라이센스를 수동으로 재할당합니다.

워크로드에 라이센스 할당

관리 서버는 할당된 라이센스를 해당 서버에 등록되어 있는 워크로드 간에 분배합니다.

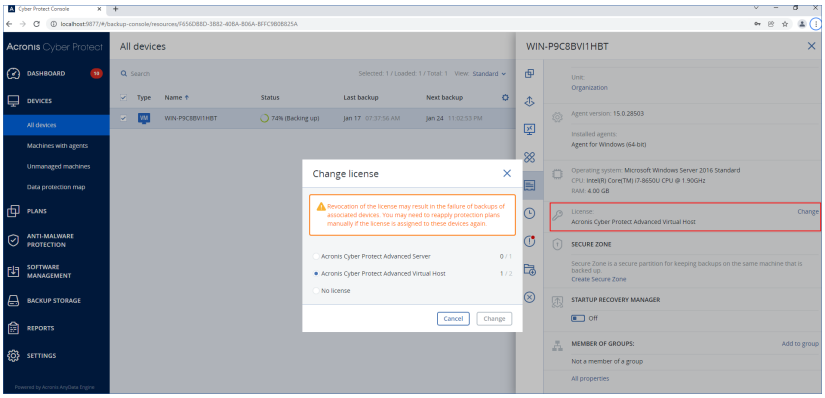
워크로드에 보호 계획을 처음 적용하면 관리 서버가 해당 워크로드에 라이센스를 할당합니다. 라이센스가 여러 개 할당된 관리 서버는 워크로드 유형, 운영 체제 및 필요한 보호 수준에 따라 가장 적절한 라이센스에 워크로드를 할당합니다.

할당된 라이센스를 확인하려면 관리 서버 웹 콘솔에서 원하는 워크로드를 선택하고 **세부 사항**을 클릭합니다.

워크로드에 라이센스를 수동으로 재할당하려면

1. 관리 서버 로컬 웹 콘솔에서 **장치**를 클릭하고 원하는 워크로드를 선택합니다.
2. **상세정보**를 클릭합니다.
3. [온-프레미스 관리 서버의 경우] **라이센스** 섹션으로 이동한 후 **변경**을 클릭합니다.

4. [클라우드 관리 서버의 경우] **서비스 할당량** 섹션으로 이동한 후 **변경**을 클릭합니다.
5. 원하는 라이센스(서비스 할당량)를 선택한 다음 **변경**을 클릭합니다.



제한 사항

오프라인 관리 서버의 경우 로컬 콘솔에만 라이센스 할당량의 현재 사용량이 표시됩니다. 오프라인 관리 서버에서는 이 데이터가 Acronis 계정과 동기화되지 않으므로 클라우드 콘솔에서 사용할 수 없습니다.

알려진 문제

클라우드 콘솔에서 라이센스 사용량 또는 **가상 호스트** 라이센스 할당량이 잘못 표시될 수 있습니다. 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

관리 서버 등록 해제

온라인 관리 서버를 등록 해제하려면

1. 클라우드 콘솔(https://cloud.acronis.com)에서 **설정** > **라이센스 사용**을 클릭합니다.
2. 원하는 관리 서버로 이동하여 **등록 해제**를 클릭합니다.
3. **관리 서버 등록 해제** 창이 표시됩니다.
4. 계정과 연결된 이메일 주소를 입력하여 등록 해제를 확인합니다.
5. **등록 해제**를 클릭합니다.

그러면 등록되지 않은 서버에 할당되었던 모든 라이센스가 점유 해제되어 계정의 다른 관리 서버에 할당할 수 있습니다. 등록되지 않은 관리 서버의 로컬 콘솔에서 라이센스 수가 0으로 재설정됩니다.

오프라인 관리 서버를 등록 해제하려면

두 진입점에서 오프라인 관리 서버를 등록 해제할 수 있습니다.

로컬 콘솔:

1. 로컬 콘솔의 계정이 표시된 줄에서 **등록 해제**를 클릭합니다. **관리 서버 등록 해제** 창이 표시됩니다.
2. 로컬 관리자와 연결된 이메일 주소를 **로그인** 필드에 입력합니다.
3. **등록 해제**를 클릭합니다.

4. **등록 해제에 성공했습니다** 팝업 화면이 표시됩니다.
5. **등록 해제 파일 다운로드**를 클릭합니다.
6. 클라우드 콘솔에서 **등록 해제**를 클릭합니다. **관리 서버 등록 해제** 창이 표시됩니다.
7. **오프라인 관리 서버 등록 해제**를 클릭합니다. **오프라인 관리 서버 등록 해제** 창이 표시됩니다.
8. **찾아보기**를 클릭한 다음 로컬 콘솔에서 다운로드한 등록 해제 파일을 선택합니다.
9. **등록 해제**를 클릭합니다.

클라우드 콘솔:

1. 인터넷에 액세스할 수 있는 머신에서 클라우드 콘솔(https://cloud.acronis.com)에 로그인한 후 **설정** > **라이센스 사용**을 클릭합니다.
2. 원하는 관리 서버로 이동하여 **등록 해제**를 클릭합니다. **관리 서버 등록 해제** 창이 표시됩니다.
3. **오프라인 관리 서버 등록 해제**를 클릭합니다. **오프라인 관리 서버 등록 해제** 창이 표시됩니다.
4. 등록 해제할 관리 서버의 로컬 콘솔(https://<관리 서버 IP 주소>:<포트>)에서 **설정** > **라이선스 사용**으로 이동하여 **등록 해제**를 클릭합니다. 머신에 등록 해제 파일이 다운로드됩니다.
5. 클라우드 콘솔에서 **오프라인 관리 서버 등록 해제** 창으로 다시 이동합니다.
6. **찾아보기**를 클릭한 다음 로컬 콘솔에서 다운로드한 등록 해제 파일을 선택합니다.
7. **등록 해제**를 클릭합니다.
8. 관리 서버가 설치된 머신에 액세스할 수 없으면 **관리 서버가 설치된 머신 액세스 권한 없음**을 클릭해도 됩니다.

경고!
이 머신은 영구적으로 차단되며 계정에서 제거됩니다. 그리고 해당 머신에 관리 서버를 다시 등록할 수도 없습니다.

그러면 등록되지 않은 서버에 할당되었던 모든 라이센스가 점유 해제되어 계정의 다른 관리 서버에 할당할 수 있습니다. 등록되지 않은 관리 서버의 로컬 콘솔에서 라이센스 수가 0으로 재설정됩니다.

Acronis Cyber Protect 15 Update 2 이하 버전에서 라이센스 관리

Acronis Cyber Protect 15 Update 2 이하 버전의 사용을 시작하려면 관리 서버에 라이센스 키를 하나 이상 추가해야 합니다. 라이센스는 보호 계획이 적용될 때 머신에 자동으로 할당됩니다.

라이센스는 수동으로 할당하고 취소할 수도 있습니다. 라이센스 관련 수동 작업은 조직 관리자만 수행할 수 있습니다. 관리자에 대한 자세한 내용은 "단위 및 관리자 계정"(584페이지) 항목을 참조하십시오.

관리 서버에 라이센스 키 추가

Acronis Cyber Protect 15 Update 2 이전 버전에서는 관리 서버에 라이센스 키를 추가합니다.

관리 서버에 라이센스 키를 추가하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **라이센스**로 이동합니다.
2. **키 추가**를 클릭합니다.
3. 라이센스 키 하나 이상을 한 줄에 하나씩 입력합니다.
4. **추가**를 클릭합니다.
5. [서브스크립션 라이센스 키를 추가하는 경우] 서브스크립션 라이센스를 활성화하려면 Acronis 계정에 로그인합니다.
   a. 로그인 양식에 Acronis Customer Portal(https://account.acronis.com)에 사용하는 자격 증명을 입력하고 **로그인**을 클릭합니다.
   b. 계정을 확인하고 **동기화**를 클릭합니다.
   c. 작업이 완료되면 **완료**를 클릭합니다.
6. **라이센스 키 추가** 패널에서 **완료**를 클릭합니다.

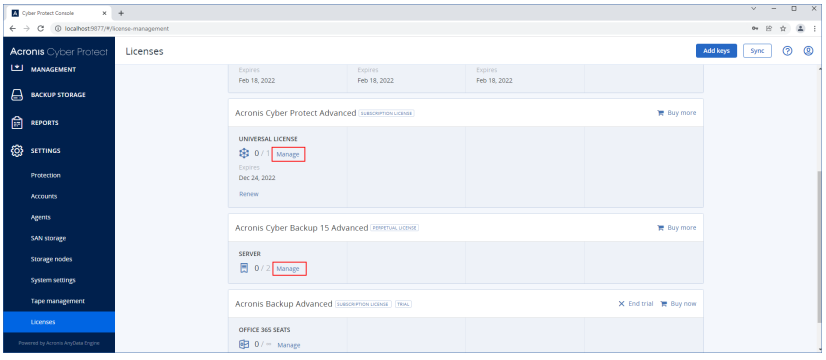
참고
라이센스 키를 관리 서버에 다시 추가하는 대신 Acronis 계정에 등록된 서브스크립션 라이센스 키를 자동으로 가져올 수 있습니다. 라이센스 키를 가져오려면 **라이센스 키 추가** 패널에서 **Acronis 계정 동기화**를 클릭한 다음 Acronis 계정에 로그인합니다.

서브스크립션 라이센스 관리

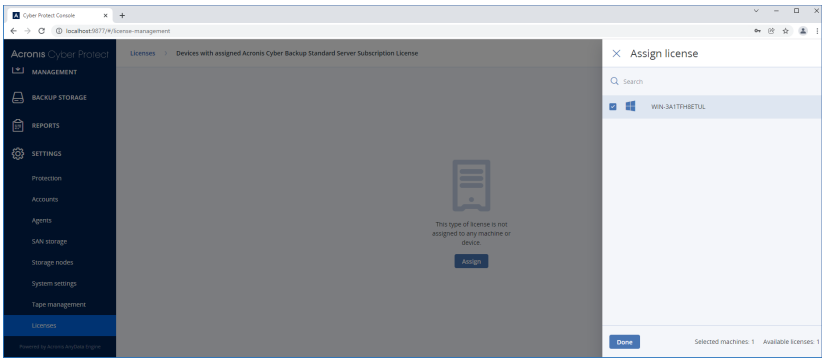
워크로드에 라이센스를 할당하기 전에 관리 서버에 라이센스 키를 추가해야 합니다. 이 작업을 수행하는 방법을 자세히 알아보려면 "관리 서버에 라이센스 키 추가"(39페이지) 항목을 참조하십시오.

워크로드에 서브스크립션 라이센스를 할당하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **라이센스**로 이동합니다.
2. 원하는 라이센스로 이동하여 **관리**를 클릭합니다.



3. **할당**을 클릭합니다.
   해당 라이센스를 할당할 수 있는 워크로드가 표시됩니다.



4. 워크로드를 선택하고 **완료**를 클릭합니다.

서브스크립션 라이센스를 워크로드에서 취소하려면

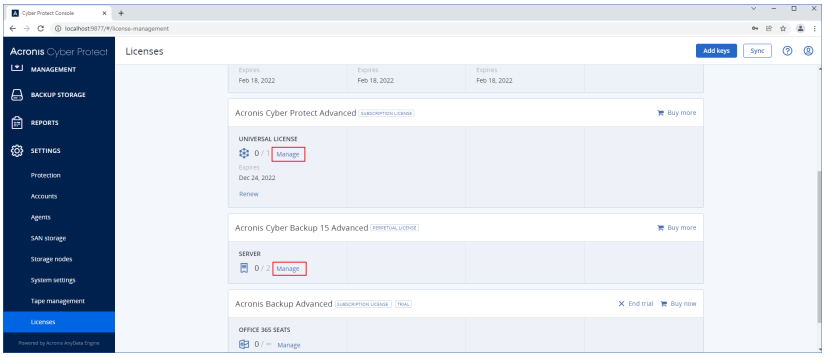
1. Cyber Protect 웹 콘솔에서 **설정** > **라이센스**로 이동합니다.
2. 원하는 라이센스로 이동하여 **관리**를 클릭합니다.
   해당 라이센스가 할당된 모든 워크로드가 표시됩니다.
3. 라이센스를 취소하려는 워크로드를 선택합니다.
4. **취소**를 클릭합니다.
5. 결정을 확인합니다.
   취소한 라이센스는 점유 해제되어 다른 워크로드에 할당할 수 있습니다.

영구 라이센스 관리

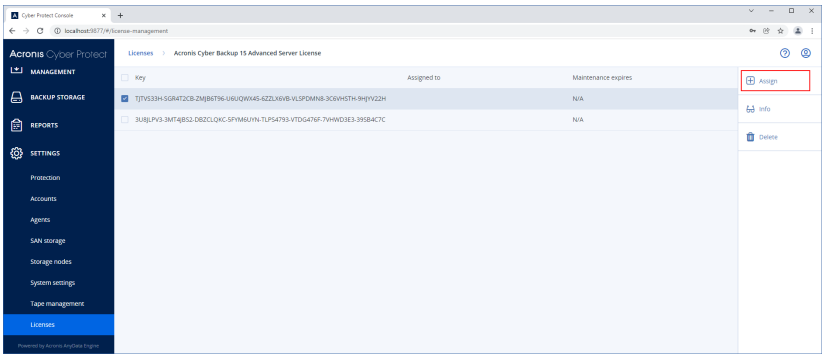
워크로드에 라이센스를 할당하기 전에 관리 서버에 라이센스 키를 추가해야 합니다. 이 작업을 수행하는 방법을 자세히 알아보려면 "관리 서버에 라이센스 키 추가"(39페이지) 항목을 참조하십시오.

워크로드에 영구 라이센스를 할당하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **라이센스**로 이동합니다.
2. 원하는 라이센스로 이동하여 **관리**를 클릭합니다.



   선택한 라이센스에 해당하는 라이센스 키가 표시됩니다.
3. 워크로드에 할당하려는 라이센스 키를 선택합니다.
4. **할당**을 클릭합니다.



해당 라이센스 키를 할당할 수 있는 워크로드가 표시됩니다.

5. 워크로드를 선택하고 **완료**를 클릭합니다.

영구 라이센스를 워크로드에서 취소하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **라이센스**로 이동합니다.
2. 원하는 라이센스를 선택하고 **관리**를 클릭합니다

   선택한 라이센스에 해당하는 라이센스 키가 표시됩니다. **할당 대상** 열에서 이 라이센스 키가 할당된 워크로드를 확인합니다.
3. 취소하려는 라이센스 키를 선택합니다.
4. **취소**를 클릭합니다.
5. 결정을 확인합니다.

   취소한 라이센스 키는 라이센스 목록에 유지되어 다른 워크로드에 할당할 수 있습니다.

설치

설치 개요

Acronis Cyber Protect이(가) 지원하는 두 가지 디플로이 방식은 온-프레미스와 클라우드 방식입니다. 두 방식의 주요 차이점은 Acronis Cyber Protect 관리 서버의 위치입니다.

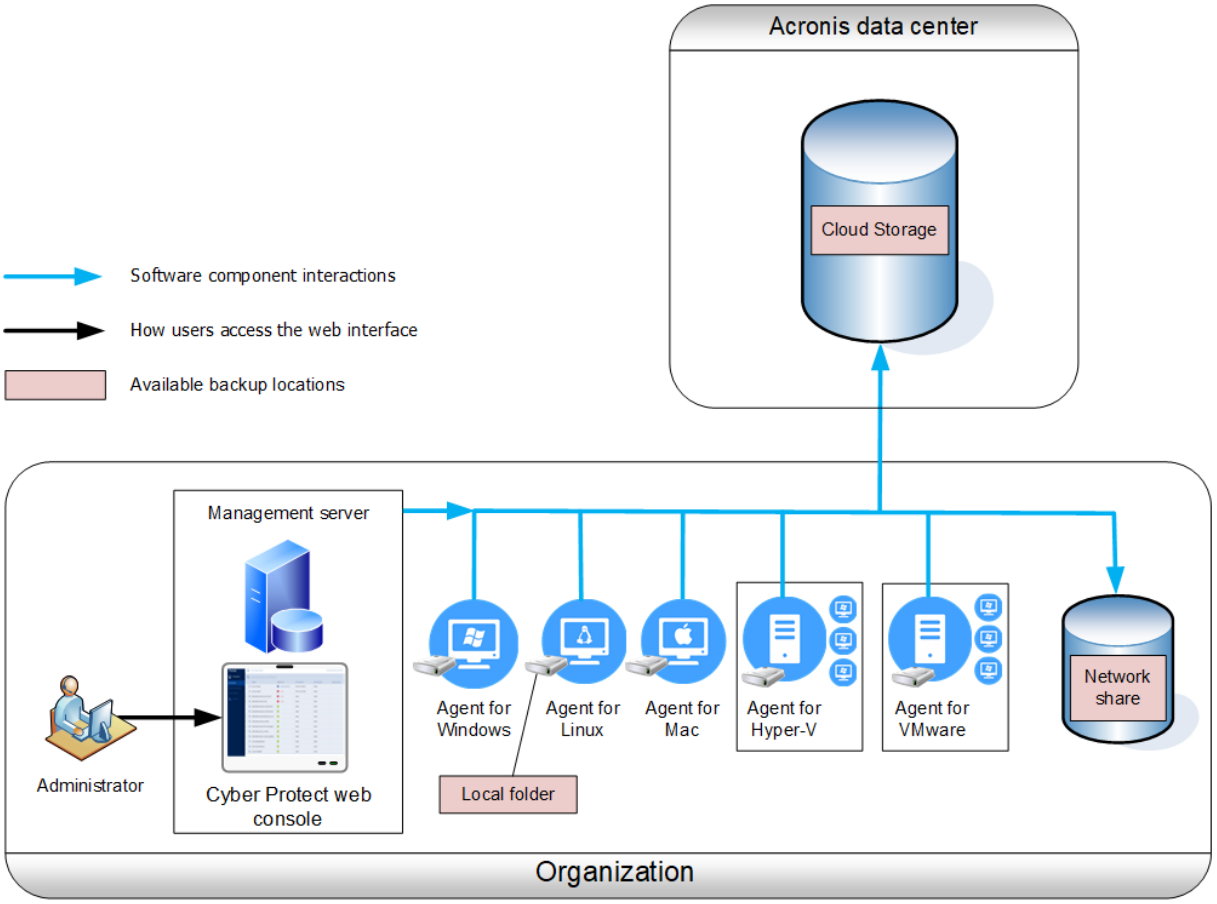
관리 서버는 모든 백업을 관리할 수 있는 중앙 위치입니다. 온-프레미스 디플로이에서는 관리 서버가 사용자의 로컬 네트워크에 설치되며, 클라우드 디플로이에서는 관리 서버가 Acronis 데이터 센터 중 하나에 설치됩니다. 이 서버의 웹 인터페이스는 Cyber Protect 웹 콘솔이라고 합니다.

관리 서버는 보호 에이전트와의 통신을 담당하며 일반적인 계획 관리 기능을 수행합니다. 모든 보호 활동 전에 에이전트는 사전 요구 사항을 확인하기 위해 관리 서버를 참조합니다. 간혹 관리 서버에 대한 연결이 끊길 수 있으며, 이는 새 보호 계획의 디플로이를 방해합니다. 하지만 보호 계획이 이미 머신에 디플로이된 경우, 에이전트는 관리 서버와의 통신이 끊긴 후에도 보호 작업을 30일간 지속합니다.

이 두 가지 디플로이 방식에서 모두 사용자는 백업하려고 하는 모든 머신에 보호 에이전트를 설치해야 합니다. 지원되는 스토리지 유형 역시 동일하며 클라우드 스토리지 공간은 Acronis Cyber Protect 라이센스와 별도로 판매됩니다.

온프레미스 디플로이

온프레미스 디플로이에서는 모든 제품 컴퍼넌트가 사용자의 로컬 네트워크에 설치됩니다. 이는 영구 라이센스가 제공되는 유일한 디플로이 방식입니다. 사용자의 머신이 인터넷에 연결되지 않은 경우에도 이 방식을 사용해야 합니다.



관리 서버 위치

관리 서버는 Windows나 Linux를 실행하는 머신에 설치할 수 있습니다.

Windows에 설치하는 방법이 권장되는데 이 경우 관리 서버를 통해 다른 머신으로 에이전트를 배포할 수 있기 때문입니다. 고급 라이센스가 있으면 조직 단위를 만들고 조직 단위에 관리자를 추가할 수 있습니다. 이 방법을 통해 다른 사용자에게 보호 관리를 위임할 수 있으며, 이렇게 위임받은 사용자의 액세스 권한은 해당 부서로 엄격히 제한됩니다.

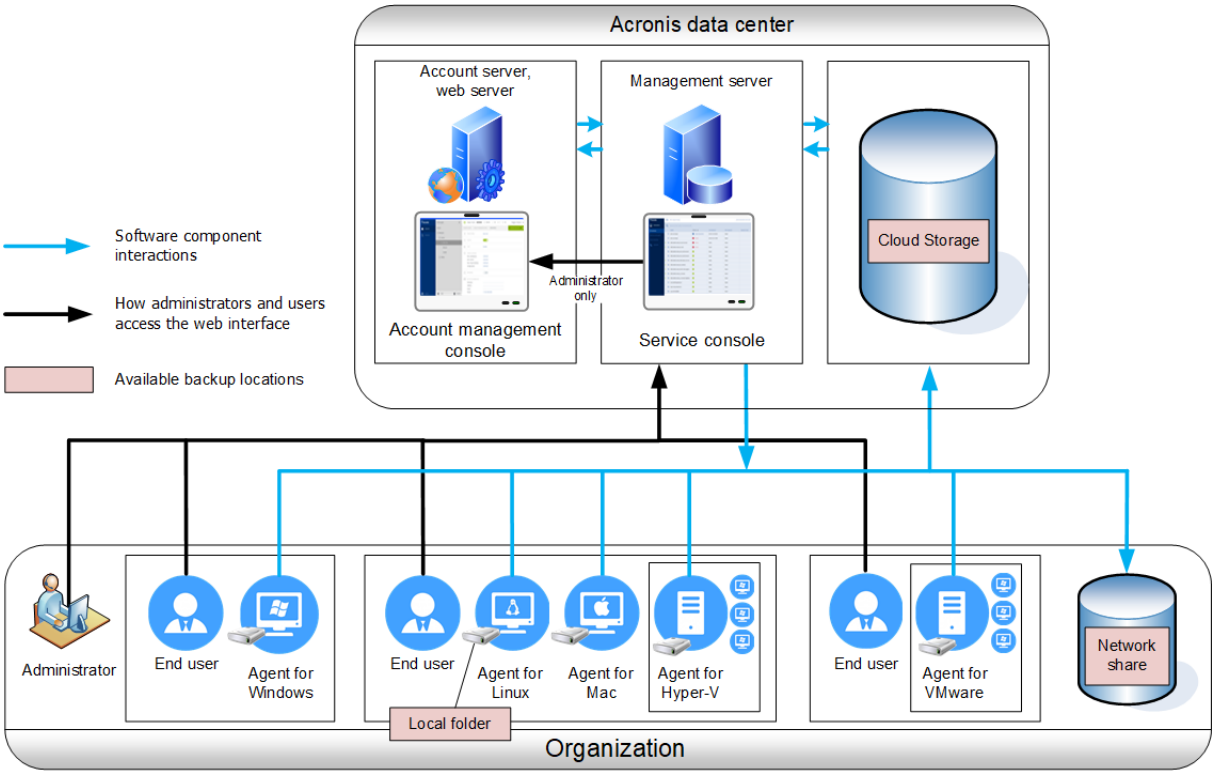
Linux에 설치하는 방식은 Linux 전용 환경에 권장됩니다. 사용자는 백업을 원하는 머신에 에이전트를 로컬로 설치해야 합니다.

클라우드 디플로이

클라우드 디플로이의 경우 관리 서버가 Acronis 데이터 센터 중 하나에 설치됩니다. 이 방식은 사용자가 자신의 로컬 네트워크에서 관리 서버를 유지 관리할 필요가 없다는 것이 장점입니다. Acronis Cyber Protect을(를) Acronis에서 제공하는 사이버 보호 서비스라고 생각하시면 됩니다.

계정 서버에 액세스하여 사용자 계정을 생성하고, 사용자별 서비스 사용 할당량을 설정하고, 사용자 조직을 반영하여 사용자 그룹(단위)을 생성할 수 있습니다. 모든 사용자는 Cyber Protect 웹 콘솔에 액세스하고, 필요한 에이전트를 다운로드하고, 에이전트를 자신의 머신으로 단 몇 분 내에 설치할 수 있습니다.

관리자 계정은 단위 또는 조직 수준으로 생성할 수 있습니다. 각 계정에는 각각의 제어 영역으로 범위가 지정된 보기가 있습니다. 사용자는 자신의 백업에만 액세스할 수 있습니다.



다음 표에는 온프레미스와 클라우드 디플로이 간 차이점이 요약되어 있습니다. 각 열에는 해당 유형의 배포에서만 사용 가능한 기능이 나열되어 있습니다.

온프레미스 디플로이	클라우드 디플로이
• 영구 라이센스 사용 가능 • 에어갭 환경에서 사용 가능한 온프레미스 관리 서버* • 백업 위치로서 SFTP 서버 • 백업 위치로서의 Acronis 사이버 인프라 • 테이프 장치 및 Acronis 스토리지 노드(백업 위치)* • 이전 버전의 Acronis Cyber Protect에서 업그레이드(Acronis Backup for VMware 포함)	• Microsoft 365 데이터의 클라우드 간 백업(그룹, 공용 폴더, OneDrive*** 및 SharePoint Online 데이터에 대한 보호 포함) • Google Workspace 데이터의 클라우드 간 백업 • Agent for Mac은 Apple Silicon M1, M2 등의 ARM 기반 프로세서와 x64 프로세서를 모두 지원합니다 • Agent for Virtuozzo(하이퍼바이저 수준에서 Virtuozzo 가상 머신 백업) • Agent for oVirt(하이퍼바이저 수준에서 oVirt KVM 가상 머신 백업) • Agent for Virtuozzo Hybrid Infrastructure(하이퍼바이저 수준에서 Virtuozzo Hybrid Infrastructure 가상 머신 백업) • 재해 복구(클라우드 서비스)****

* 에어갭 환경에서 관리 서버를 활성화하는 방법에 대한 자세한 내용은 "오프라인 관리 서버를 활성화하려면"(27페이지) 항목을 참조하십시오.

** Standard 에디션에서는 이 기능을 사용할 수 없습니다.

***OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 아카이브에서 유효하지 않은 내용이 포함됩니다.

**** 이 기능은 Disaster Recovery 애드온에서만 사용할 수 있습니다.

컴퍼넌트

에이전트

에이전트란 Acronis Cyber Protect을(를) 통해 관리하는 머신에서 데이터 백업, 복구 및 기타 작업을 수행하는 애플리케이션입니다.

Agent for Windows는 Agent for Exchange, Agent for SQL, Agent for Active Directory 및 Agent for Oracle과 함께 설치됩니다. 예를 들어 Agent for SQL을 설치한 경우 이 에이전트가 설치된 전체 머신을 백업할 수 있습니다.

일부 에이전트는 특정 역할 또는 애플리케이션이 있는 머신에만 설치될 수 있습니다. 예를 들어, Agent for Hyper-V는 Hyper-V 역할을 실행하는 머신에 설치되고, Agent for SQL은 SQL 데이터베이스를 실행하는 머신에 설치되며, Agent for Exchange는 Microsoft Exchange Server의 사서함 역할을 실행하는 머신에 설치되고, Agent for Active Directory는 도메인 컨트롤러에 설치됩니다.

백업하려는 항목에 따라 에이전트를 선택합니다. 다음 표는 결정에 도움이 되는 정보를 요약해서 보여줍니다.

백업 대상	설치할 에이전트	에이전트 설치 위치	에이전트 가용성	
			온-프레미스	클라우드
실제 머신				
Windows를 실행하는 실제 머신의 디스크, 볼륨, 파일	Agent for Windows	백업되는 머신	+	+
Linux를 실행하는 실제 머신의 디스크, 볼륨, 파일	Agent for Linux		+	+
macOS를 실행하는 실제 머신의 디스크, 볼륨, 파일	Agent for Mac		+	+
애플리케이션				
SQL 데이터베이스	Agent for SQL	Microsoft SQL Server를 실행 중인 머신	+	+
Exchange 데이터베이스	Agent for	Microsoft Exchange Server의	+	+

및 사서함	Exchange	사서함 역할을 실행 중인 머신* 사서함 백업만 필요한 경우 Microsoft Exchange Server의 클라이언트 액세스 역할을 실행하는 머신에 대한 네트워크 액세스 권한이 있는 모든 Windows 머신에 에이전트를 설치할 수 있습니다.		사서함 백업 없음
Microsoft 365 사서함	Agent for Office 365	인터넷에 연결된 Windows 머신	+	+
Active Directory 도메인 서비스를 실행 중인 머신	Agent for Active Directory	도메인 컨트롤러.	+	+
Oracle 데이터베이스를 실행 중인 머신	Agent for Oracle	Oracle 데이터베이스를 실행 중인 머신.	+	-
가상 머신				
VMware ESXi 가상 머신	Agent for VMware (Windows)	vCenter Server 및 가상 머신 스토리지에 네트워크를 통해 액세스할 수 있는 Windows 머신**	+	+
	Agent for VMware(가상 어플라이언스)	ESXi 호스트	+	+
Hyper-V 가상 머신	Agent for Hyper-V	Hyper-V 호스트	+	+
Scale Computing HC3 가상 머신	Agent for Scale Computing HC3	Scale Computing HC3 호스트	+	+
Windows Azure에서 호스팅되는 가상 머신	실제 머신에 대해 동일***	백업되는 머신	+	+
Amazon EC2에서 호스팅되는 가상 머신			+	+

Citrix XenServer 가상 머신			+****	+
Red Hat Virtualization (RHV/RHEV) 가상 머신				
커널 기반 가상 머신(KVM)				
Oracle 가상 머신				
Nutanix AHV 가상 머신				
모바일 장치				
Android를 실행하는 모바일 장치	Android용 모바일 앱	백업되는 모바일 장치	-	+
iOS를 실행하는 모바일 장치	iOS용 모바일 앱		-	+

*설치 과정에서 Agent for Exchange는 구동될 머신에 여유 공간이 충분한지 확인합니다. 개별 복구 시 일시적으로 가장 규모가 큰 Exchange 데이터베이스의 15%에 해당하는 여유 공간이 필요하므로 그만큼을 확보해 두어야 합니다.

**ESXi에서 SAN 연결 스토리지를 사용하는 경우 동일한 SAN에 연결된 머신에 에이전트를 설치합니다. 에이전트는 ESXi 호스트 및 LAN을 통해서가 아니라 스토리지에서 가상 머신을 직접 백업합니다. 자세한 지침은 "LAN 프리 백업"을 참조하십시오.

***외부 에이전트에서 가상 머신을 백업하는 경우 가상 머신은 가상으로 간주됩니다. 에이전트가 게스트 시스템에 설치되어 있는 경우 백업 및 복구 작업은 실제 머신과 동일합니다. 그럼에도 불구하고 클라우드 디플로이에서 머신 수 할당량을 설정할 때에는 가상 머신으로 계산됩니다.

****Acronis Cyber Protect Advanced 가상 호스트 라이센스가 있으면 이러한 가상 머신은 가상으로 간주합니다(호스트당 라이센스가 사용됨). Acronis Cyber Protect 가상 호스트 라이센스가 있으면 이러한 머신은 실제로 간주합니다(머신당 라이센스가 사용됨).

기타 구성 요소

구성 요소	기능	에이전트 설치 위치	가용성	
			온-프레미스	클라우드
Management Server	관리 서버는 사용자의 모든 백업을 관리하는 중앙 지점이 됩니다. 온프레미스 디플로이의 경우, 관리 서버가 사용	Windows나 Linux를 실행하는 머신	+	-

	자의 로컬 네트워크에 설치됩니다. 관리 서버는 에이전트를 관리하고 사용자에게 웹 인터페이스를 제공합니다.			
원격 설치 컴퍼넌트	에이전트 설치 패키지를 로컬 폴더에 저장합니다.	관리 서버를 실행하는 Windows 머신.	+	-
검색 서비스	클라우드 스토리지, 로컬 폴더 또는 네트워크 폴더에서 백업의 안티맬웨어 스캔을 활성화하는 선택적 컴포넌트입니다. 검색 서비스를 이용하려면 Microsoft SQL Server 또는 PostgreSQL 데이터베이스가 필요합니다. 검색 서비스는 관리 서버에서 사용하는 기본 SQLite 데이터베이스와 호환되지 않습니다.	관리 서버를 실행하는 Windows 또는 Linux 머신	+	-
Bootable Media Builder	부트 가능한 미디어를 생성합니다.	Windows나 Linux를 실행하는 머신	+	-
명령줄 도구	**acrocmd** 유틸리티의 명령줄 인터페이스를 지원합니다. **acrocmd**에는 명령을 실제로 실행하는 도구가 포함되지 않습니다. 이 유틸리티는 Cyber Protect 컴퍼넌트(에이전트 및 관리 서버)의 명령줄 인터페이스만 제공합니다.	Windows, Linux 또는 macOS를 실행하는 머신.	+	+
Acronis Cyber Protect 15 모니터	Agent for Windows 및 Agent for Mac용 그래픽 사용자 인터페이스를 제공합니다. 모니터에는 에이전트가 설치되어 있는 머신의 보호 상	Windows나 macOS를 실행하는 머신.	+	+

	태에 대한 정보가 표시되며 사용자가 백업 암호화 및 프록시 서버 설정을 구성할 수 있습니다. Windows에서 Acronis Cyber Protect 15 모니터를 사용하려면 동일한 머신에 Agent for Windows가 설치되어 있어야 합니다.			
스토리지 노드	백업을 저장합니다. 백업은 목록화 및 중복 제거에 필요합니다. 스토리지 노드를 사용하려면 동일한 머신에 Agent for Windows가 설치되어 있어야 합니다.	Windows를 실행하는 머신	+	-
카탈로그 서비스	스토리지 노드에서 백업 목록화를 수행합니다.	Windows를 실행하는 머신	+	-
PXE 서버	네트워크를 통한 부트 가능한 미디어로의 머신 부팅을 활성화합니다.	Windows를 실행하는 머신	+	-

Acronis Cyber Protect을(를) 사용자 환경의 다른 보안 솔루션과 함께 사용

Acronis Cyber Protect은(는) 사용자의 환경에서 독립형 안티바이러스 소프트웨어와 같은 다른 보안 솔루션을 사용하거나 사용하지 않고 사용할 수 있습니다.

다른 보안 솔루션이 없으면 라이센스 및 필요에 따라 Acronis Cyber Protect을(를) 완전한 사이버 보호 또는 기존 백업 및 복구에 사용할 수 있습니다. 각 라이센스에 제공되는 기능에 대한 자세한 내용은 "클라우드 디플로이를 포함한 Acronis Cyber Protect 15 버전 비교"를 참조하십시오. 필요한 모듈만 활성화하여 보호 계획의 범위를 조정할 수 있습니다.

사용자의 환경에 이미 다른 보안 솔루션이 있는 경우에도 바이러스 및 기타 맬웨어에 대한 보호를 포함한 완전한 사이버 보호를 위해 Acronis Cyber Protect을(를) 선택할 수 있습니다. 이 경우 충돌을 방지하기 위해 다른 보안 솔루션을 비활성화하거나 제거해야 합니다.

또는 현재 보안 솔루션을 비활성화하거나 제거하지 않고 사이버 보호를 강화할 수도 있습니다. 이를 위해서는 보호 계획에서 안티바이러스 및 맬웨어 방지 모듈을 사용하지 않는지 확인하십시오. 다른 모든 모듈은 자유롭게 사용할 수 있습니다.

제한 사항

- 백업의 맬웨어 방지 스캔을 실행하려면 Cyber Protect Management Server를 설치할 때 스캔 서비스를 설치해야 합니다.
- HTML5 클라이언트를 통한 원격 액세스 권한은 Cyber Protect Management Server가 Linux를 실행 중인 머신에 설치된 경우에만 제공됩니다.

소프트웨어 요구 사항

지원되는 웹 브라우저

웹 인터페이스는 다음 웹 브라우저를 지원합니다.

- Google Chrome 29 이상 버전
- Mozilla Firefox 23 이상 버전
- Opera 16 이상 버전
- Windows Internet Explorer 10 이상 버전

참고
클라우드 디플로이에서는 Internet Explorer가 지원되지 않습니다.

- Microsoft Edge 25 이상 버전
- macOS 및 iOS 운영 체제에서 실행되는 Safari 8 이상

다른 웹 브라우저(다른 운영 체제에서 실행 중인 Safari 포함)에서는 사용자 인터페이스가 제대로 표시되지 않거나 일부 기능을 사용하지 못할 수 있습니다.

지원되는 운영 체제 및 환경

에이전트

Agent for Windows

- Windows XP Professional SP1(x64), SP2(x64), SP3(x86)
- Windows XP Professional SP2(x86) – 특별 버전의 Agent for Windows를 통해 지원. 이 지원에 대한 자세한 사항과 제한에 대해서는 "Agent for Windows XP SP2"를 참조하십시오.
- Windows XP Embedded SP3
- Windows Server 2003 SP1/2003 R2 이상 – Standard 및 Enterprise 에디션(x86, x64)

참고

Acronis Cyber Protect을(를) 사용하려면 Microsoft의 KB940349 업데이트를 설치해야 하는데 이 업데이트는 더 이상 별도로 다운로드할 수 없습니다. 원래 KB940349에서 제공되었던 기능을 머신에서 사용할 수 있는지 확인하려면 Windows Server 2003용으로 현재 제공되는 모든 업데이트를 설치하십시오.

KB940349에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

- Windows Small Business Server 2003/2003 R2
- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x86, x64)
- Windows Small Business Server 2008
- Windows 7 - 모든 버전(x86, x64)

참고

Windows 7에서 AcronisCyber Protect을(를) 사용하려면 Microsoft의 다음 업데이트를 설치해야 합니다.

- Windows 7 ESU(확장 보안 업데이트)
- KB4474419
- KB4490628

필요한 업데이트에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation 및 Web 에디션
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2003/2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise 및 LTSC(이전 LTSB) 버전
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – 모든 설치 옵션, Nano Server는 제외
- Windows 11 – 모든 버전
- Windows Server 2022 – 모든 설치 옵션, Nano Server는 제외

Agent for SQL, Agent for Exchange(데이터베이스 백업 및 애플리케이션 인식 백업용), Agent for Active Directory

이러한 각각의 에이전트는 다음의 예외 사항을 제외하고, 위에 나열된 모든 운영 체제와 각 애플리케이션의 지원 버전을 실행하는 머신에 설치할 수 있습니다.

- Agent for SQL은 Windows 7 Starter 및 Home 버전(x86, x64)의 온프레미스 배포가 지원되지 않습니다

Agent for Exchange(사서함 백업용)

이 에이전트는 Microsoft Exchange Server가 있거나 없는 머신에 설치할 수 있습니다.

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x86, x64)
- Windows Small Business Server 2008
- Windows 7 – 모든 버전
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation 및 Web 에디션
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008/2008 R2/2012/2012 R2
- Windows 10 – Home, Pro, Education 및 Enterprise 버전
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – 모든 설치 옵션, Nano Server는 제외
- Windows 11 – 모든 버전
- Windows Server 2022 – 모든 설치 옵션, Nano Server는 제외

Agent for Office 365

- Windows Server 2008 – Standard, Enterprise, Datacenter, Foundation 및 Web 버전(x64 전용)
- Windows Small Business Server 2008
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter, Foundation 및 Web 에디션
- Windows Home Server 2011
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x64 전용)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016(x64 전용)
- Windows 10 – Home, Pro, Education 및 Enterprise 버전(x64 전용)
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션(x64 전용)
- Windows Server 2019 – Nano Server를 제외한 모든 설치 옵션(x64 전용)
- Windows 11 – 모든 버전
- Windows Server 2022 – 모든 설치 옵션, Nano Server는 제외

Agent for Oracle

- Windows Server 2008R2 – Standard, Enterprise, Datacenter 및 Web 버전(x86, x64)
- Windows Server 2012R2 – Standard, Enterprise, Datacenter 및 Web 버전(x86, x64)
- Linux – Agent for Linux가 지원하는 커널 및 배포(아래 나열)

Agent for Linux

참고
테스트가 완료된 Linux 배포판 및 커널 버전은 다음과 같습니다. 그러나 사용 중인 Linux 배포판이나 커널 버전이 아래 목록에 없더라도 Linux 운영 체제의 특성상 모든 필수 시나리오에서 해당 배포판이나 버전이 정상 작동할 수도 있습니다.

사용 중인 Linux 배포판 및 커널 버전 조합과 함께 Acronis Cyber Protect 사용 시 문제가 발생하면 지원 팀에 추가 조사를 요청하십시오.

커널이 2.6.9~5.19 버전이고 glibc가 2.3.4 이상 버전인 Linux(다음 x86 및 x86_64 배포판 포함):

- Red Hat Enterprise Linux 4.x, 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  중요
  USE Linux Enterprise Server 12 및 SUSE Linux Enterprise Server 15에서는 Btrfs가 포함된 구성이 지원되지 않습니다.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 및 Red Hat Compatible Kernel 모두
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Ubuntu 시스템 같은 RPM 패키지 관리자를 사용하지 않는 시스템에 제품을 설치하려면 먼저 다음 명령을 실행(루트 사용자 자격으로)하는 등의 방법으로 이 관리자를 수동으로 설치해야 합니다.
```
apt-get install rpm
```

Red Hat Enterprise Linux 6.x 또는 CentOS 6.x 등 사용 중인 Linux 배포판에서 D-Bus 메커니즘을 지원하지 않으면 Acronis Cyber Protect에서는 보안 키 저장에 기본 위치를 사용합니다. 운영 체제에서 D-Bus 호환 위치를 제공하지 않기 때문입니다.

* 4.18~5.19 커널에서만 지원됨

Agent for Mac

참고
Apple Silicon M1, M2 등의 ARM 기반 프로세서는 지원되지 않습니다.

- OS X Mavericks 10.9
- OS X Yosemite 10.10
- OS X El Capitan 10.11
- macOS Sierra 10.12
- macOS High Sierra 10.13
- macOS Mojave 10.14
- macOS Catalina 10.15
- macOS Big Sur 11
- macOS Monterey 12
- macOS Ventura 13

Agent for VMware(가상 어플라이언스)

이 에이전트는 ESXi 호스트에서 실행되는 가상 어플라이언스로 제공됩니다.

VMware ESXi 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0

Agent for VMware(Windows)

이 에이전트는 Agent for Windows에 대해 위에 나열된 모든 운영 체제에서 실행할 수 있도록 Windows 애플리케이션으로 제공됩니다. 단, 다음과 같은 예외가 적용됩니다.

- 32비트 운영 체제는 지원되지 않습니다.
- Windows XP, Windows Server 2003/2003 R2, Windows Small Business Server 2003/2003 R2는 지원되지 않습니다.

Agent for Hyper-V

- Windows Server 2008 with Hyper-V role(x64 전용), Server Core 설치 모드 포함
- Windows Server 2008 R2 with Hyper-V role, Server Core 설치 모드 포함
- Microsoft Hyper-V Server 2008/2008 R2
- Windows Server 2012/2012 R2 with Hyper-V role, Server Core 설치 모드 포함
- Microsoft Hyper-V Server 2012/2012 R2
- Windows 8, 8.1 with Hyper-V(x64 전용)
- Windows 10 – Pro, Education 및 Enterprise 버전(Hyper-V 포함)
- Windows Server 2016 with Hyper-V role – Nano Server를 제외한 모든 설치 옵션
- Microsoft Hyper-V Server 2016
- Windows Server 2019 with Hyper-V role – Nano Server를 제외한 모든 설치 옵션

- Microsoft Hyper-V Server 2019
- Windows Server 2022(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션

Agent for Scale Computing HC3(가상 어플라이언스)

이 에이전트는 Cyber Protect 웹 콘솔을 통해 Scale Computing HC3 클러스터에 디플로이된 가상 어플라이언스로 제공됩니다. 이 에이전트의 독립형 설치 프로그램은 없습니다.

Scale Computing Hypercore 8.8, 8.9, 9.0

관리 서버(온프레미스 디플로이에만 해당)

Windows

- Windows 7 - 모든 버전(x86, x64)

  참고
  Windows 7에서 AcronisCyber Protect을(를) 사용하려면 Microsoft의 다음 업데이트를 설치해야 합니다.
  - Windows 7 ESU(확장 보안 업데이트)
  - KB4474419
  - KB4490628

  필요한 업데이트에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

- Windows Server 2008 R2 – Standard, Enterprise, Datacenter 및 Foundation 버전
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x86, x64)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise 및 LTSC(이전 LTSB) 버전
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – 모든 설치 옵션, Nano Server는 제외
- Windows 11 – 모든 버전
- Windows Server 2022 – 모든 설치 옵션, Nano Server는 제외

Linux

참고
테스트가 완료된 Linux 배포판 및 커널 버전은 다음과 같습니다. 그러나 사용 중인 Linux 배포판이나 커널 버전이 아래 목록에 없더라도 Linux 운영 체제의 특성상 모든 필수 시나리오에서 해당 배포판이나 버전이 정상 작동할 수도 있습니다.

사용 중인 Linux 배포판 및 커널 버전 조합과 함께 Acronis Cyber Protect 사용 시 문제가 발생하면 지원 팀에 추가 조사를 요청하십시오.

커널이 2.6.9~5.19 버전이고 glibc가 2.3.4 이상 버전인 Linux(다음 x86_64 배포판 포함):

x86 배포판은 지원되지 않습니다.

- Red Hat Enterprise Linux 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*, 8.6*, 8.7*
- Ubuntu 9.10, 10.04, 10.10, 11.04, 11.10, 12.04, 12.10, 13.04, 13.10, 14.04, 14.10, 15.04, 15.10, 16.04, 16.10, 17.04, 17.10, 18.04, 18.10, 19.04, 19.10, 20.04, 20.10, 21.04, 21.10, 22.04
- Fedora 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31
- SUSE Linux Enterprise Server 10, 11, 12, 15

  중요
  USE Linux Enterprise Server 12 및 SUSE Linux Enterprise Server 15에서는 Btrfs가 포함된 구성이 지원되지 않습니다.

- Debian 4.x, 5.x, 6.x, 7.0, 7.2, 7.4, 7.5, 7.6, 7.7, 8.0, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8, 8.11, 9.0, 9.1, 9.2, 9.3, 9.4, 9.5, 9.6, 9.7, 9.8, 10, 11
- CentOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- CentOS Stream 8
- Oracle Linux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*– Unbreakable Enterprise Kernel 및 Red Hat Compatible Kernel 모두
- CloudLinux 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- ClearOS 5.x, 6.x, 7.x, 8.0, 8.1, 8.2, 8.3, 8.4*, 8.5*
- AlmaLinux 8.4*, 8.5*
- Rocky Linux 8.4*
- ALT Linux 7.0

Ubuntu 시스템 같은 RPM 패키지 관리자를 사용하지 않는 시스템에 제품을 설치하려면 먼저 다음 명령을 실행(루트 사용자 자격으로)하는 등의 방법으로 이 관리자를 수동으로 설치해야 합니다.
`apt-get install rpm`

Red Hat Enterprise Linux 6.x 또는 CentOS 6.x 등 사용 중인 Linux 배포판에서 D-Bus 메커니즘을 지원하지 않으면 Acronis Cyber Protect에서는 보안 키 저장에 기본 위치를 사용합니다. 운영 체제에서 D-Bus 호환 위치를 제공하지 않기 때문입니다.

* 4.18~5.19 커널에서만 지원됨

스토리지 노드(온프레미스 디플로이에만 해당)

- Windows Server 2008 – Standard, Enterprise, Datacenter 및 Foundation 버전(x64 전용)
- Windows Small Business Server 2008
- Windows 7 – 모든 버전(x64 전용)
- Windows Server 2008 R2 – Standard, Enterprise, Datacenter 및 Foundation 버전
- Windows Home Server 2011
- Windows MultiPoint Server 2010/2011/2012
- Windows Small Business Server 2011 – 모든 버전
- Windows 8/8.1 – Windows RT 버전을 제외한 모든 버전(x64 전용)
- Windows Server 2012/2012 R2 – 모든 버전
- Windows Storage Server 2008/2008 R2/2012/2012 R2/2016
- Windows 10 – Home, Pro, Education, Enterprise, IoT Enterprise 에디션
- Windows Server 2016 – Nano Server를 제외한 모든 설치 옵션
- Windows Server 2019 – 모든 설치 옵션, Nano Server는 제외
- Windows Server 2022 – 모든 설치 옵션, Nano Server는 제외

Agent for Windows XP SP2

Agent for Windows XP SP2는 32비트 버전의 Windows XP SP2만 지원합니다.

Windows XP SP1(x64), Windows XP SP2(x64), 또는 Windows XP SP3(x86)를 실행하는 머신을 보호하려면 일반 Agent for Windows를 사용하십시오.

Agent for Windows XP SP2를 실행하려면 Acronis Cyber Backup 12.5 라이센스가 필요합니다. Acronis Cyber Protect 15 라이센스 키는 지원되지 않습니다.

설치

Agent for Windows XP SP2를 사용하려면 최소 550MB의 디스크 공간과 150MB의 RAM이 필요합니다. 백업하는 동안 에이전트는 일반적으로 350MB 메모리를 사용합니다. 처리하는 데이터의 양에 따라 피크 사용량은 2GB까지 오를 수 있습니다.

Agent for Windows XP SP2는 백업하려는 머신에 로컬로만 설치할 수 있습니다. 에이전트 설치 프로그램을 다운로드하려면 우측 상단의 계정 아이콘을 클릭한 다음 **다운로드** > **Agent for Windows XP SP2**를 클릭합니다.

Cyber Protect Monitor 및 Bootable Media Builder는 설치할 수 없습니다. 부트 가능한 미디어 ISO 파일을 다운로드하려면 우측 상단의 계정 아이콘을 클릭하고 **다운로드** > **부트 가능한 미디어**를 클릭합니다.

업데이트

Agent for Windows XP SP2는 원격 업데이트 기능을 지원하지 않습니다. 에이전트를 업데이트하려면 새 버전의 설치 프로그램을 다운로드한 다음 설치를 반복합니다.

Windows XP를 SP2에서 SP3로 업데이트한 경우에는 Agent for Windows XP SP2를 제거한 다음 일반 Agent for Windows를 설치하십시오.

제한 사항

- 디스크 수준 백업만 사용할 수 있습니다. 디스크 또는 볼륨 백업에서 개별 파일을 복구할 수 있습니다.
- 이벤트별 스케줄은 지원되지 않습니다.
- 보호 계획 실행에 대한 조건은 지원되지 않습니다.
- 다음 백업 목적지만 지원됩니다.
  - 클라우드 스토리지
  - 로컬 폴더
  - 네트워크 폴더
  - Secure Zone
- **버전 12** 백업 형식, 그리고 **버전 12** 백업 형식이 필요한 기능은 지원되지 않습니다. 특히, 실제 데이터 전달은 지원되지 않습니다. 활성화한 경우 **성능 및 백업 할당 시간** 옵션은 초록색 수준 설정만 적용합니다.
- 복구 및 복구 중 수동 디스크 매핑을 위한 개발 디스크/볼륨 선택은 웹 인터페이스에서 지원되지 않습니다. 이 기능은 부트 가능한 미디어에서 사용할 수 있습니다.
- 오프호스트 데이터 처리는 지원되지 않습니다.
- Agent for Windows XP SP2는 백업에 대한 다음 작업을 수행할 수 없습니다.
  - 백업을 가상 머신으로 변환
  - 백업에서 볼륨 마운트
  - 백업에서 파일 추출
  - 백업 내보내기 및 수동 유효성 검사.

  이 작업은 다른 에이전트를 사용하여 수행할 수 있습니다.
- Agent for Windows XP SP2가 생성한 백업은 가상 머신으로 실행할 수 없습니다.

지원되는 Microsoft SQL Server 버전

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016
- Microsoft SQL Server 2014
- Microsoft SQL Server 2012

상기한 SQL Server 버전의 SQL Server Express 버전도 지원됩니다.

지원되는 Microsoft Exchange Server 버전

- Microsoft Exchange Server 2019 – 모든 버전.
- Microsoft Exchange Server 2016 – 모든 버전.

- Microsoft Exchange Server 2013 – 모든 버전, CU1(누적 업데이트 1) 이상
- Microsoft Exchange Server 2010 – 모든 버전, 모든 서비스 팩. 사서함 백업 및 데이터베이스 백업에서 개별 복구는 SP1(서비스 팩 1)부터 지원됩니다.
- Microsoft Exchange Server 2007 – 모든 버전, 모든 서비스 팩. 사서함 백업 및 데이터베이스 백업에서 개별 복구는 지원되지 않습니다.

지원되는 Microsoft SharePoint 버전

Acronis Cyber Protect 15에서는 다음 Microsoft SharePoint 버전을 지원합니다.

- Microsoft SharePoint 2013
- Microsoft SharePoint Server 2010 SP1
- Microsoft SharePoint Foundation 2010 SP1
- Microsoft Office SharePoint Server 2007 SP2*
- Microsoft Windows SharePoint Services 3.0 SP2*

*이러한 버전으로 SharePoint Explorer를 사용하려면 데이터베이스를 연결할 SharePoint 복구 팜이 필요합니다.

데이터를 추출한 곳에서 가져온 백업이나 데이터베이스는 SharePoint Explorer가 설치된 곳과 동일한 버전의 SharePoint에서 생성된 것이어야 합니다.

지원되는 Oracle 데이터베이스 버전

- Oracle 데이터베이스 버전 11g, 모든 버전
- Oracle 데이터베이스 버전 12c, 모든 버전.

단일 인스턴스 구성만 지원됩니다.

지원되는 SAP HANA 버전

실제 머신 또는 VMware ESXi 가상 머신에서 실행되는 RHEL 7.6에 HANA 2.0 SPS 03이 설치되었습니다.

SAP HANA는 스토리지 스냅샷을 사용한 멀티테넌트 데이터베이스 컨테이너의 복구를 지원하지 않으므로 이 솔루션은 하나의 테넌트 데이터베이스만 있는 SAP HANA 컨테이너를 지원합니다.

지원되는 가상화 플랫폼

다음 표에는 다양한 가상화 플랫폼이 지원되는 방법이 요약되어 있습니다.

참고

게스트 OS에서 백업 방법을 통해 지원되며 테스트가 완료된 하이퍼바이저 공급업체 및 버전은 다음과 같습니다. 그러나 아래에 나와 있지 않은 버전의 하이퍼바이저나 공급업체의 하이퍼바이저를 실행하더라도 필요한 모든 시나리오에서 **게스트 OS에서 백업** 방법이 정상적으로 작동할 수도 있습니다.

사용 중인 하이퍼바이저 공급업체 및 버전 조합과 함께 Acronis Cyber Protect 사용 시 문제가 발생하면 지원 팀에 추가 조사를 요청하십시오.

플랫폼	하이퍼바이저 수준에서 백업(에이전트 없는 백업)	게스트 OS에서 백업
VMware		
VMware vSphere 버전: 4.1, 5.0, 5.1, 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 **VMware vSphere 버전:** VMware vSphere Essentials* VMware vSphere Essentials Plus* VMware vSphere Standard* VMware vSphere Advanced VMware vSphere Enterprise VMware vSphere Enterprise Plus	+	+
VMware vSphere Hypervisor(Free ESXi)**		+
VMware Server(VMware Virtual 서버) VMware 워크스테이션 VMware ACE VMware Player		+
Microsoft* **		
Windows Server 2008(x64) with Hyper-V Windows Server 2008 R2 with Hyper-V Microsoft Hyper-V Server 2008/2008 R2 Windows Server 2012/2012 R2 with Hyper-V Microsoft Hyper-V Server 2012/2012 R2 Windows 8, 8.1(x64)(Hyper-V 사용)	+	+

Windows 10(Hyper-V 사용) Windows Server 2016(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션 Microsoft Hyper-V Server 2016 Windows Server 2019(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션 Microsoft Hyper-V Server 2019 Windows Server 2022(Hyper-V 사용) – Nano Server를 제외한 모든 설치 옵션		
Microsoft Virtual PC 2004 및 2007 Windows Virtual PC		+
Microsoft Virtual Server 2005		+
Scale Computing		
Scale Computing Hypercore 8.8, 8.9, 9.0	+	+
Citrix		
Citrix XenServer 4.1.5, 5.5, 5.6, 6.0, 6.1, 6.2, 6.5, 7.0, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6		완전 가상화된(즉, HVM) 게스트만 해당. 반가상화된(즉, PV) 게스트는 지원되지 않음.
Red Hat 및 Linux		
Red Hat Enterprise Virtualization(RHEV) 2.2, 3.0, 3.1, 3.2, 3.3, 3.4, 3.5, 3.6 Red Hat Virtualization(RHV) 4.0, 4.1		+
Red Hat Virtualization(oVirt를 통해 관리됨) 4.2, 4.3, 4.4 (클라우드 디플로이 시에만 사용 가능)	+	+
커널 기반 가상 머신(KVM)		+
Red Hat Enterprise Linux 7.6, 7.7 또는 CentOS 7.6, 7.7에서 실행되는 oVirt 4.3을 통해 관리되는 커널 기반 가상 머신(KVM) (고급 라이선스를 활용한 클라우드 디플로이 시에만 사용 가능)	+	+
Red Hat Enterprise Linux 8.x 또는 CentOS Stream 8.x에서 실행되는 oVirt 4.4를 통해 관리되는 커널 기반 가상 머신(KVM)	+	+

(고급 라이선스를 활용한 클라우드 디플로이 시에만 사용 가능)		
Red Hat Enterprise Linux 8.x 또는 CentOS Stream 8.x에서 실행되는 oVirt 4.5를 통해 관리되는 커널 기반 가상 머신(KVM) (고급 라이선스를 활용한 클라우드 디플로이 시에만 사용 가능)	+	+
Parallels		
Parallels Workstation		+
Parallels Server 4 Bare Metal		+
Oracle		
Oracle VM Server 3.0, 3.3, 3.4		완전 가상화된(즉, HVM) 게스트만 해당. 반가상화된(즉, PV) 게스트는 지원되지 않음.
Oracle VM VirtualBox 4.x		+
Nutanix		
Nutanix Acropolis Hypervisor (AHV) 20160925.x ~ 20180425.x		+
Virtuozzo(클라우드 디플로이 시에만 사용 가능)		
Virtuozzo 6.0.10, 6.0.11, 6.0.12	+	가상 머신만 해당. 컨테이너는 지원되지 않음.
Virtuozzo 7.0.13, 7.0.14	Ploop 컨테이너만 해당. 가상 머신은 지원되지 않음.	가상 머신만 해당. 컨테이너는 지원되지 않음.
Virtuozzo Hybrid Server 7.5	+	가상 머신만 해당. 컨테이너는 지원되지 않음.
Virtuozzo Hybrid Infrastructure(클라우드 디플로이 시에만 사용 가능)		
Virtuozzo Hybrid Infrastructure 3.5, 4.0, 4.5	+	+
Amazon		

Amazon EC2 인스턴스		+
Microsoft Azure		
Azure 가상 머신		+

* 이러한 버전의 경우 vSphere 5.0 이상에서 가상 디스크의 HotAdd 전송이 지원됩니다.버전 4.1에서는 백업 실행 속도가 느릴 수 있습니다.

** 이 제품은 RCLI(Remote Command Line Interface)에 대한 액세스가 읽기 전용 모드로 제한되기 때문에 vSphere Hypervisor에 대해 하이퍼바이저 수준의 백업은 지원되지 않습니다. 에이전트는 시리얼 키를 입력하지 않은 상태로 vSphere Hypervisor 평가 기간 동안 작동합니다. 시리얼 키를 입력하면 에이전트가 작동을 멈춥니다.

*** S2D(Storage Spaces Direct)를 사용하는 하이퍼 컨버지드 클러스터에서 실행 중인 Hyper-V 가상 머신이 지원됩니다. Storage Spaces Direct는 백업 스토리지로도 지원됩니다.

제한 사항

- **내결함성 머신**

  Agent for VMware는 VMware vSphere 6.0 이상에서 내결함성이 활성화된 경우에만 내결함성 머신을 백업합니다.이전 vSphere 버전에서 업그레이드한 경우 각 머신에 대해 내결함성을 비활성화하고 활성화하기에 충분합니다. 이전 버전의 vSphere를 사용하는 경우 게스트 운영 체제에 에이전트를 설치하십시오.
- **독립형 디스크 및 RDM**

  Agent for VMware는 물리적 호환성 모드 또는 독립형 디스크에서 RDM(Raw Device Mapping) 디스크를 백업하지 않습니다. 에이전트는 이러한 디스크를 건너뛰며 로그에 경고를 추가합니다. 실제 호환성 모드의 독립형 디스크와 RDM을 보호 계획에서 제외하면 경고를 방지할 수 있습니다. 이러한 디스크 또는 이러한 디스크의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **패스스루 디스크**

  Agent for Hyper-V는 패스스루 디스크를 백업하지 않습니다. 백업 동안 에이전트는 이러한 디스크를 건너뛰며 로그에 경고를 추가합니다. 보호 계획에서 패스스루 디스크를 제외하면 경고를 방지할 수 있습니다. 이러한 디스크 또는 이러한 디스크의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.
- **Hyper-V 게스트 클러스터링**

  Agent for Hyper-V는 Windows Server 장애 조치 클러스터의 노드인 Hyper-V 가상 머신의 백업을 지원하지 않습니다. 호스트 수준의 VSS 스냅샷은 클러스터로부터 외부 쿼럼(quorum) 디스크를 일시적으로 분리할 수도 있습니다. 이러한 머신을 백업하려면 게스트 운영 체제에 에이전트를 설치하십시오.
- **게스트 iSCSI 연결**

  Agent for VMware와 Agent for Hyper-V는 게스트 운영 체제 내에서 작동하는 iSCSI 시작자에 의해 연결된 LUN 볼륨을 백업하지 않습니다. ESXi와 Hyper-V 하이퍼바이저는 이러한 볼륨을 인식하지 않기 때문에, 이러한 볼륨은 하이퍼바이저 수준 스냅샷에 포함되지 않으며 경고 없이 백업

에서 제외됩니다. 이러한 볼륨 또는 이러한 볼륨의 데이터를 백업하려면 게스트 운영 체제에 에이전트를 설치합니다.

- **논리 볼륨을 포함한 Linux 머신(LVM)**

  Agent for VMware와 Agent for Hyper-V는 LVM을 포함한 Linux 머신에서 다음 작업을 지원하지 않습니다.

  - P2V 및 V2P 마이그레이션. Agent for Linux 또는 부트 가능한 미디어를 사용하여 복구를 위한 백업 및 부트 가능한 미디어를 생성합니다.
  - Agent for Linux 또는 부트 가능한 미디어가 생성한 백업으로 가상 머신을 구동합니다.
  - Agent for Linux 또는 부트 가능한 미디어가 생성한 백업을 가상 머신으로 변환합니다.
- **암호화된 가상 머신**(VMware vSphere 6.5에서 소개)
  - 암호화된 가상 머신을 암호화하지 않은 상태로 백업할 수 있습니다. 암호화가 반드시 필요한 경우 보호 계획을 생성할 때 백업 암호화를 활성화합니다.
  - 복구된 가상 머신은 항상 암호 해제됩니다. 복구가 완료된 후에는 수동으로 암호화를 활성화할 수 있습니다.
  - 암호화된 가상 머신을 백업하는 경우 Agent for VMware이 실행 중인 가상 머신도 암호화하는 것이 좋습니다. 그렇지 않으면 암호화된 머신의 작업이 예상보다 느려질 수 있습니다. VSphere Web Client를 사용하여 에이전트의 머신에 **VM 암호화 정책**을 적용하십시오.
  - 에이전트에 대해 SAN 전송 모드를 구성하더라도 암호화된 가상 머신은 LAN을 통해 백업됩니다. VMware가 암호화된 가상 디스크 백업에 SAN 전송을 지원하지 않기 때문에 에이전트가 NBD 전송으로 폴백합니다.
- **보안 부팅**(VMware vSphere 6.5에서 소개)

  가상 머신이 새 가상 머신으로 복구되면 **보안 부팅**은 비활성화됩니다. 복구가 완료된 후에는 수동으로 이 옵션을 활성화할 수 있습니다.
- **ESXi 구성 백업**은 VMware vSphere 7.0에 대해 지원되지 않습니다.

Linux 패키지

Linux 커널에 필요한 모듈을 추가하려면 설치 프로그램에 다음과 같은 Linux 패키지가 필요합니다.

- 커널 헤더 또는 소스가 있는 패키지. 패키지 버전은 커널 버전과 일치해야 합니다.
- GCC(GNU 컴파일러 모음) 컴파일러 시스템. GCC 버전은 커널이 컴파일된 버전이어야 합니다.
- Make 도구.
- Perl 해석기.
- 4.15에서 시작하여 CONFIG_UNWINDER_ORC=y로 구성되는 커널 구축을 위한 `libelf-dev`, `libelf-devel` 또는 `elfutils-libelf-devel` 라이브러리.Fedora28과 같은 일부 배포에 대해서는 커널 헤더와 별도로 설치해야 합니다.

이러한 패키지의 이름은 Linux 배포판에 따라 다릅니다.

Red Hat Enterprise Linux, CentOS, Fedora인 경우 일반적으로 설치 프로그램이 패키지를 설치합니다. 다른 배포판인 경우 패키지가 설치되어 있지 않거나 필요한 버전이 없는 경우 패키지를 설치해야 합니다.

필요한 패키지가 이미 설치되어 있습니까?

패키지가 이미 설치되어 있는지 알아보려면 다음 단계를 수행합니다.

1. 커널 버전과 필요한 GCC 버전을 알아보려면 다음 명령을 실행합니다.

   ```
   cat /proc/version
   ```

   이 명령은 다음과 비슷한 행을 반환합니다. `Linux 버전 2.6.35.6 및 gcc 버전 4.5.1`
2. Make 도구와 GCC 컴파일러가 설치되어 있는지 확인하려면 다음 명령을 실행합니다.

   ```
   make -v
   gcc -v
   ```

   gcc의 경우 명령을 통해 반환되는 버전은 1단계의 `gcc version`과 동일해야 합니다. **make**의 경우 명령이 실행되는지 확인합니다.
3. 커널 모듈 빌드를 위한 올바른 패키지 버전이 설치되어 있는지 알아봅니다.
   - Red Hat Enterprise Linux, CentOS, Fedora의 경우 다음 명령을 실행합니다.

     ```
     yum list installed | grep kernel-devel
     ```

   - Ubuntu의 경우 다음 명령을 실행합니다.

     ```
     dpkg --get-selections | grep linux-headers
     dpkg --get-selections | grep linux-image
     ```

   두 경우 모두 패키지 버전이 1단계의 `Linux` 버전과 동일해야 합니다.
4. Perl 해석기가 설치되었는지 알아보려면 다음 명령을 입력합니다.

   ```
   perl --version
   ```

   Perl 버전에 대한 정보가 보인다면 해석기가 설치되어 있는 것입니다.
5. Red Hat Enterprise Linux, CentOS, Fedora의 경우 다음 명령을 실행하여 `elfutils-libelf-devel`이 설치되었는지 확인합니다.

   ```
   yum list installed | grep elfutils-libelf-devel
   ```

   라이브러리 버전에 대한 정보가 보인다면 라이브러리가 설치되어 있는 것입니다.

리포지토리에서 패키지 설치

다음 표에는 다양한 Linux 배포판에 필수 패키지를 설치하는 방법이 나와 있습니다.

Linux 배포판	패키지 이름	설치 방법
Red Hat Enterprise Linux	**kernel-devel** **gcc** **make**	설치 프로그램이 Red Hat 서브스크립션을 사용하여 패키지를 자동으로 다운로드, 설치합니다.

	elfutils-libelf-devel	
	perl	다음 명령을 실행합니다. `yum install perl`
CentOS Fedora	**kernel-devel** **gcc** **make** **elfutils-libelf-devel**	설치 프로그램이 패키지를 자동으로 다운로드, 설치합니다.
	perl	다음 명령을 실행합니다. `yum install perl`

Ubuntu
Debian
	linux-headers
	linux-image
	gcc
	make
	perl
		다음 명령 실행:
		`sudo apt-get update`
		`sudo apt-get install linux-headers-$(uname -r)`
		`sudo apt-get install linux-image-$(uname -r)`
		`sudo apt-get install gcc-<package version>`
		`sudo apt-get install make`
		`sudo apt-get install perl`

SUSE Linux OpenSUSE	**kernel-source** **gcc** **make** **perl**	sudo zypper install kernel-source sudo zypper install gcc sudo zypper install make sudo zypper install perl

패키지는 배포판 저장소에서 다운로드, 설치됩니다.

다른 Linux 배포판은 필수 패키지의 정확한 이름과 설치 방법에 대한 배포판 문서를 참조하십시오.

수동으로 패키지 설치

다음과 같은 경우 패키지를 **수동으로** 설치해야 합니다.

- 머신에 활성 Red Hat 서브스크립션 또는 인터넷 연결이 없는 경우.
- 설치 프로그램이 커널 버전에 해당하는 **kernel-devel** 또는 **gcc** 버전을 찾을 수 없습니다. 사용 가능한 **kernel-devel**이 기존 커널보다 최신인 경우 커널을 업데이트하거나 일치하는 **kernel-devel** 버전을 수동으로 설치해야 합니다.
- 필수 패키지가 로컬 네트워크에 있고 자동 검색 및 다운로드에 시간을 할애하지 않으려는 경우.

로컬 네트워크 또는 신뢰할 수 있는 타사 웹 사이트에서 패키지를 다운로드하여 다음과 같이 설치합니다.

- Red Hat Enterprise Linux, CentOS, Fedora의 경우 루트 사용자로 다음 명령을 실행합니다.

```
rpm -ivh PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

- Ubuntu의 경우 다음 명령을 실행합니다.

```
sudo dpkg -i PACKAGE_FILE1 PACKAGE_FILE2 PACKAGE_FILE3
```

예: Fedora 14에서 수동으로 패키지 설치

Fedora 14 또는 32비트 머신의 경우 다음 단계에 따라 필수 패키지를 설치합니다.

1. 커널 버전과 필요한 GCC 버전을 확인하려면 다음 명령을 실행합니다.

   ```
   cat /proc/version
   ```

   이 명령의 출력에는 다음이 포함됩니다.

   ```
   Linux version 2.6.35.6-45.fc14.i686
   gcc version 4.5.1
   ```

2. 커널 버전에 해당하는 **kernel-devel**과 **gcc** 패키지를 가져옵니다.

   ```
   kernel-devel-2.6.35.6-45.fc14.i686.rpm
   gcc-4.5.1-4.fc14.i686.rpm
   ```

3. Fedora 14용 **make** 패키지를 가져옵니다.

   ```
   make-3.82-3.fc14.i686
   ```

4. 다음 명령을 루트 사용자로 실행하여 패키지를 설치합니다.

   ```
   rpm -ivh kernel-devel-2.6.35.6-45.fc14.i686.rpm
   rpm -ivh gcc-4.5.1.fc14.i686.rpm
   rpm -ivh make-3.82-3.fc14.i686
   ```

   이 모든 패키지를 단일 `rpm` 명령으로 지정할 수 있습니다. 이러한 패키지를 설치하려면 종속성 해결을 위해 추가 패키지를 설치해야 합니다.

암호화 소프트웨어와의 호환성

파일 수준 암호화 소프트웨어에서 암호화한 데이터를 백업하고 복구하는 작업에는 제한이 없습니다.

디스크 수준 암호화 소프트웨어는 데이터를 즉시 암호화하므로 백업에 포함된 데이터가 암호화되지 않습니다. 디스크 수준 암호화 소프트웨어는 종종 시스템 영역(부트 레코드, 파티션 테이블 또는 파일 시스템 테이블)을 수정합니다. 이러한 요소는 복구된 시스템이 Secure Zone을 부팅하고 액세스할 수 있는 기능인 디스크 수준 백업 및 복구에 영향을 줍니다.

다음 디스크 수준 암호화 소프트웨어에서 암호화한 데이터를 백업할 수 있습니다.

- Microsoft BitLocker Drive Encryption
- CheckPoint Harmony Endpoint

- McAfee Endpoint Encryption
- PGP Whole Disk Encryption

안정적인 디스크 수준 복구를 수행하려면 공통 규칙과 소프트웨어 특정 권장 사항을 따릅니다.

공통 설치 규칙

보호 에이전트를 설치하기 전에 암호화 소프트웨어를 설치하는 것이 좋습니다.

Secure Zone 사용 방법

Secure Zone은 디스크 수준 암호화로 암호화해서는 안 됩니다. Secure Zone의 유일한 사용 방법은 다음과 같습니다.

1. 암호화 소프트웨어를 설치합니다.
2. 보호 에이전트를 설치합니다.
3. Secure Zone을 생성합니다.
4. 디스크 또는 그 볼륨을 암호화할 때 Secure Zone을 제외합니다.

공통 백업 규칙

운영 체제에서 디스크 수준 백업을 수행할 수 있습니다. 부트 가능한 미디어를 사용하여 백업하지 마십시오.

소프트웨어별 복구 절차

Microsoft BitLocker Drive Encryption 및 CheckPoint Harmony Endpoint

복구 및 다시 시작을 진행하거나 부트 가능한 미디어를 사용하여 시스템을 복구할 수 있습니다.

복구 및 다시 시작

암호화된 시스템을 복구하려면 "실제 머신 복구"(287페이지)의 단계를 진행합니다.

"복구 및 다시 시작"(293페이지)의 요구 사항이 충족되었는지 확인합니다.

참고
BitLocker로 암호화된 볼륨의 경우에는 Windows 7 이상 또는 Windows Server 2008 R2 이상을 실행 중인 UEFI 기반 머신에서만 복구 및 다시 시작을 진행할 수 있습니다. CheckPoint로 암호화된 볼륨의 경우에는 Windows 10 및 11을 실행 중인 UEFI 기반 머신에서만 복구 및 다시 시작을 진행할 수 있습니다.

Linux 또는 macOS를 실행 중인 머신이나 BIOS 기반 머신에서는 복구 및 다시 시작을 진행할 수 없습니다.

부트 가능한 미디어를 사용한 복구

1. 부트 가능한 미디어에서 부팅합니다.
2. 시스템을 복구합니다.

중요
백업된 데이터는 암호화되지 않은 상태로 복구됩니다.

3. 복구된 시스템을 재부팅합니다.
4. 암호화 소프트웨어를 켭니다.

멀티 파티션 디스크의 파티션을 하나만 복구해야 하는 경우에는 운영 체제에서 복구를 수행합니다. 부트 가능한 미디어에서 복구하면 Windows에서 복구된 파티션을 감지할 수 없습니다.

McAfee Endpoint Encryption 및 PGP Whole Disk Encryption

암호화된 시스템 파티션은 부트 가능한 미디어를 사용해야 복구 가능합니다.

복구된 시스템이 부팅에 실패하면 다음의 Microsoft 기술 자료 문서의 설명에 따라 마스터 부트 레코드를 다시 빌드합니다. https://support.microsoft.com/kb/2622803

Dell EMC Data Domain 스토리지와의 호환성

Acronis Cyber Protect을(를) 활용하면 Dell EMC Data Domain 장치를 백업 스토리지로 사용할 수 있습니다. 이 경우 보존 잠금(거버넌스 모드)이 지원됩니다.

보존 잠금이 활성화되어 있으면 이 스토리지를 백업 목적지로 사용하는 보호 에이전트가 설치된 머신에 `AR_RETENTION_LOCK_SUPPORT` 환경 변수를 추가해야 합니다.

참고
보존 잠금이 활성화되어 있는 Dell EMC Data Domain 스토리지는 Agent for Mac에서 지원되지 않습니다.

Windows에서 변수를 추가하려면

1. 보호 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. **제어판**에서 **시스템 및 보안** > **시스템** > **고급 시스템 설정**으로 이동합니다.
3. **고급 탭**에서 **환경 변수**를 클릭합니다.
4. **시스템 변수** 패널에서 **새로 만들기**를 클릭합니다.
5. **새 시스템 변수** 창에서 다음과 같이 새 변수를 추가합니다.
   - 변수 이름: `AR_RETENTION_LOCK_SUPPORT`
   - 변수 값: `1`
6. **확인**을 클릭합니다.
7. **환경 변수** 창에서 **확인**을 클릭합니다.
8. 머신을 다시 시작합니다.

Linux에서 변수를 추가하려면

1. 보호 에이전트가 설치된 머신에 관리자로 로그인합니다.
2. `/sbin` 디렉토리로 이동한 후 편집을 위해 `acronis_mms` 파일을 엽니다.
3. `export LD_LIBRARY_PATH` 줄 위에 다음 줄을 추가합니다.

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. acronis_mms 파일을 저장합니다.
5. 머신을 다시 시작합니다.

가상 어플라이언스에서 변수를 추가하려면

1. 가상 어플라이언스 머신에 관리자로 로그인합니다.
2. /bin 디렉토리로 이동한 후 편집을 위해 autostart 파일을 엽니다.
3. export LD_LIBRARY_PATH 줄 아래에 다음 줄을 추가합니다.

```
export AR_RETENTION_LOCK_SUPPORT=1
```

4. autostart 파일을 저장합니다.
5. 가상 어플라이언스 머신을 다시 시작합니다.

시스템 요구 사항

다음 표에는 표준 설치에 대한 디스크 공간 및 메모리 요구 사항이 요약 정리되어 있습니다. 설치는 기본 설정에 따라 수행됩니다.

설치할 컴퍼넌트	설치에 필요한 디스크 공간	최소 메모리 사용량
Agent for Windows	850MB	150MB
Agent for Windows를 설치하려면 다음 에이전트 중 하나가 필요합니다. • Agent for SQL • Agent for Exchange	950MB	170MB
Agent for Windows를 설치하려면 다음 에이전트 중 하나가 필요합니다. • Agent for VMware(Windows) • Agent for Hyper-V	1170MB	180MB
Agent for Office 365	500MB	170MB
Agent for Linux	2.0GB	130MB
Agent for Mac	500MB	150MB
온프레미스 디플로이에만 해당		
Windows 환경의 관리 서버	1.7GB	200MB
Linux 환경의 관리 서버	1.5GB	200MB

관리 서버 및 Agent for Windows	2.4GB	360MB
Windows, Microsoft SQL Server, Microsoft Exchange Server 및 Active Directory 도메인 서비스를 실행 중인 머신의 관리 서버 및 에이전트	3.35GB	400MB
관리 서버 및 Agent for Linux	4.0GB	340MB
스토리지 노드 및 Agent for Windows • 64비트 플랫폼 전용 • 중복 제거를 사용하려면 최소한 8GB RAM이 필요합니다. 자세한 내용은 "중복 제거 우수 사례"(568페이지)을(를) 참조하십시오.	1.1GB	330MB

백업하는 동안 에이전트는 일반적으로 350MB 메모리를 사용합니다(500GB 볼륨의 백업을 진행하는 동안 측정한 결과). 처리하는 데이터의 양 및 유형에 따라 피크 사용량은 2GB까지 오를 수 있습니다.

대용량 백업 세트(600GB 이상)에 백업을 수행하려면 백업 세트 1TB당 약 1GB의 RAM이 필요합니다.

참고
초대형 백업 세트(4TB 이상)로 백업할 때는 RAM 사용량이 늘어날 수 있습니다.

x64 시스템에서는 재부팅 작업을 포함한 부트 가능한 미디어 또는 디스크 복구 작업에 최소한 2GB 메모리가 필요합니다.

등록된 워크로드가 한 대인 관리 서버는 200MB의 메모리를 사용합니다. 워크로드는 실제 머신, 가상 머신, 사서함, 데이터베이스 인스턴스 등 모든 유형의 보호되는 리소스입니다. 워크로드가 하나씩 추가될 때마다 약 2MB의 메모리가 더 필요합니다. 따라서 워크로드 100개가 등록된 서버 한 대는 운영 체제와 실행하는 애플리케이션 이외에 약 400MB의 메모리를 사용합니다.

워크로드는 최대 900~1,000개까지 등록할 수 있으며, 이 수치는 관리 서버 내에 삽입된 SQLite 데이터베이스에서 추출된 것입니다.

관리 서버를 설치하는 동안 외부 Microsoft SQL Server 인스턴스를 지정하여 이 제한 사항을 극복할 수 있습니다. 외부 SQL 데이터베이스를 사용하면 눈에 띄는 성능 저하 없이 최대 8,000개의 워크로드를 관리 서버에 등록할 수 있습니다. 등록된 워크로드가 8,000개일 경우 SQL Server 인스턴스는 약 8GB의 RAM을 사용하게 됩니다.

더 나은 백업 성능을 위해 워크로드를 최대 500개씩 한 그룹으로 묶어서 관리하는 것이 좋습니다.

지원되는 파일 시스템

보호 에이전트는 에이전트가 설치된 운영 체제에서 액세스 가능한 모든 파일 시스템을 백업할 수 있습니다. 예를 들어 Agent for Windows는 Windows에 해당 드라이버가 설치되어 있으면 ext4 파일 시스템을 백업하고 복구할 수 있습니다.

다음 표에는 백업 및 복구할 수 있는 파일 시스템이 요약되어 있습니다. 에이전트 및 부트 가능한 미디어 모두에 제한 사항이 적용됩니다.

파일 시스템	지원				제한 사항
	에이전트	**WinPE** 부트 가능한 미디어	**Linux** 기반 부트 가능한 미디어	**Mac** 부트 가능한 미디어	
FAT16/32	모든 에이전트	+	+	+	제한 없음
NTFS		+	+	+	
ext2/ext3/ext4		+	+	-	
HFS+	Agent for Mac	-	-	+	
APFS		-	-	+	• macOS High Sierra 10.13으로 시작 지원 • 원본 이외 머신 또는 베어 메탈로 복구할 때에는 디스크 구성을 수동으로 재생성해야 합니다.
JFS	Agent for Linux	-	+	-	• 디스크 백업에서 파일을 제외할 수 없음 • 빠른 증분/차등 백업을 활성화할 수 없음
ReiserFS3		-	+	-	

ReiserFS4		-	+	-	• 디스크 백업에서 파일을 제외할 수 없음 • 빠른 증분/차등 백업을 활성화할 수 없음 • 복구 도중 볼륨 크기를 조정할 수 없음
ReFS	모든 에이전트	+	+	+	
XFS		+	+	+	• 디스크 백업에서 파일을 제외할 수 없음 • 빠른 증분/차등 백업을 활성화할 수 없음 • 복구 도중 볼륨 크기를 조정할 수 없음 • 테이프에 저장된 백업의 파일 복구는 지원되지 않음
Linux swap	Agent for Linux	-	+	-	제한 없음
exFAT	모든 에이전트	+	+ 백업이 exFAT에 *저장되어 있*	+	• 디스크/볼륨 백업만 지원 • 백업에서 파일을 제외할 수 없음

			을 경우 부트 가능한 미디어를 복구에 사용할 수 없습니다		• 개별 파일은 백업에서 복구 불가

인식되지 않는 또는 지원되지 않는 파일 시스템이 있는 드라이브를 백업할 때에는 소프트웨어가 섹터 단위 모드로 자동 전환됩니다. 다음과 같은 모든 파일 시스템에서 섹터 단위 백업이 가능합니다.

- 블록 기반
- 단일 디스크에 걸쳐 있음
- 표준 MBR/GPT 파티셔닝 구성표가 있음

파일 시스템이 이 요구 사항을 충족하지 않는 경우 백업이 실패합니다.

데이터 중복 제거

Windows Server 2012 이상에서는 NTFS 볼륨에 대해 데이터 중복 제거 기능을 사용할 수 있습니다. 데이터 중복 제거는 볼륨 파일의 중복된 부분을 한 번만 저장함으로써 볼륨에서 사용 공간을 줄입니다.

디스크 레벨에서 제한 없이 데이터 중복 제거가 활성화된 볼륨을 백업하고 복구할 수 있습니다. Acronis VSS 공급자를 사용할 경우를 제외하고 파일 수준 백업이 지원됩니다. 디스크 백업에서 파일을 복구하려면 백업에서 가상 머신을 실행하거나 Windows Server 2012 이상을 실행 중인 머신에서 백업을 마운트한 다음 마운트된 볼륨에서 파일을 복사합니다.

Windows Server의 데이터 중복 제거 기능은 Acronis Backup 중복 제거 기능과 관련이 없습니다.

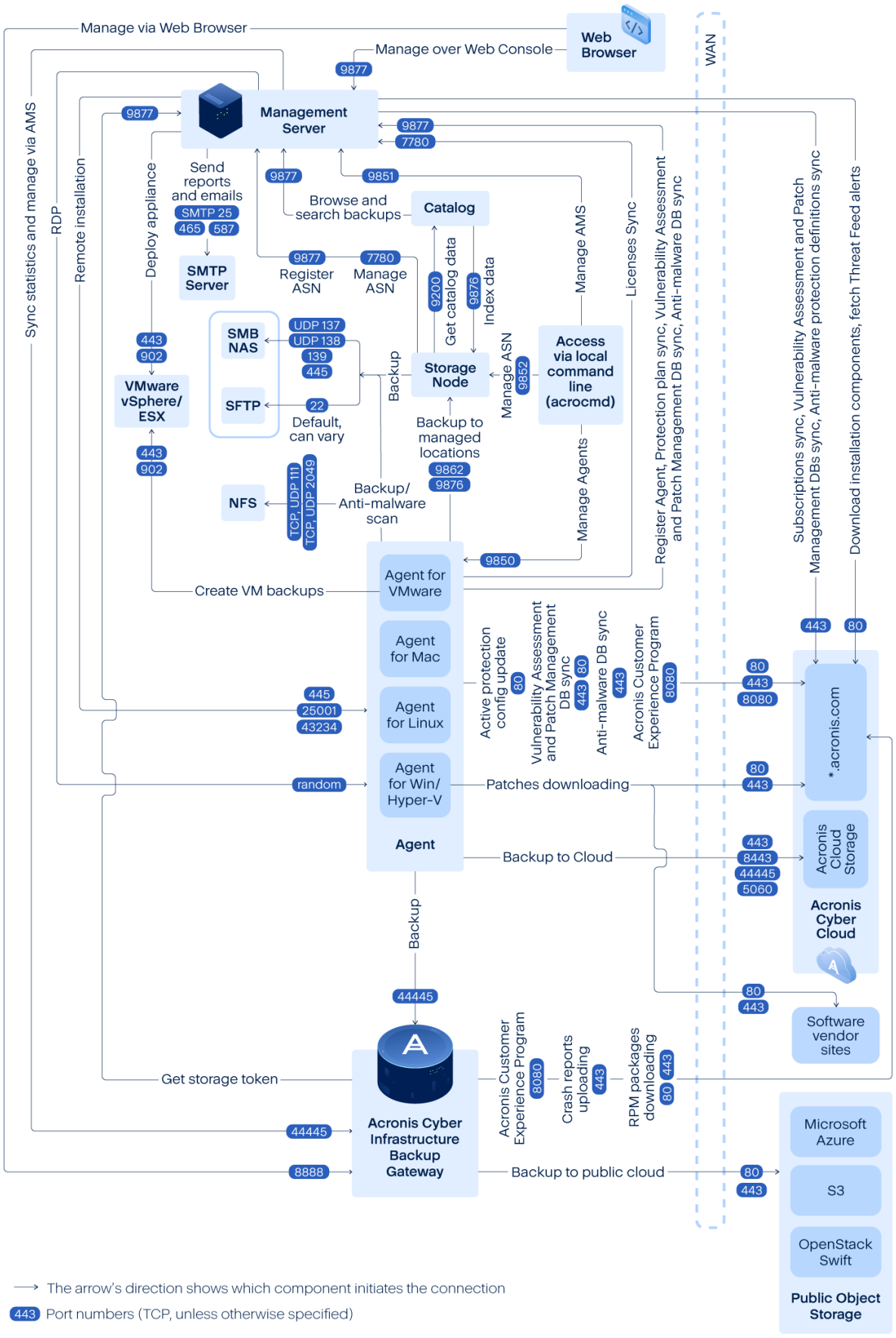
Acronis Cyber Protect에 대한 네트워크 연결 다이어그램

이 항목에는 Acronis Cyber Protect에 대한 연결 다이어그램이 포함되어 있습니다.

Acronis Cyber Protect에서 사용하는 포트, 서비스 및 프로세스의 목록을 확인하려면 지식 베이스를 방문하십시오.

- Windows의 경우 Windows 서비스 및 프로세스(65663)를 참조하십시오.
- Linux의 경우 Linux 컴퍼넌트, 서비스 및 프로세스(67276)를 참조하십시오.

네트워크 연결 다이어그램 - Cyber Protect 프로세스



중요
네트워크 다이어그램의 발신 포트는 동적 포트입니다. 일부 서비스에서는 인바운드 연결에 동적 포트를 사용할 수도 있습니다. 네트워크 문제를 해결할 때는 동적 포트를 통해 트래픽을 전송할 수 있는지 확인하십시오.

동적 포트는 운영 체제에서 관리되며 임의로 할당됩니다. Windows의 기본 동적 포트 범위는 49152 - 65535입니다. 이 범위는 운영 체제에 따라 달라질 수 있으며 수동으로 변경 가능합니다.

관리 서버는 Acronis Cyber Protect의 핵심 컴퍼넌트입니다. 관리 서버는 7780과 9877 두 개의 TCP 포트를 노출합니다. TLS로 보호되는 포트 9877은 REST API 및 웹 기반 사용자 인터페이스를 제공하는 데 사용됩니다. REST API 엔드포인트는 별개의 HTTP 헤더로 표시되거나 HTTP 쿠키로 암호화되는 JWT 토큰을 사용하여 요청을 인증합니다. 포트 7780은 ZMTP CURVE 인증 및 암호화를 사용하여 ZeroMQ 프로토콜을 구현합니다. 포트 7780은 관리 메시지를 관리 서버와 비동기식으로 교환하기 위해 에이전트와 스토리지 노드에서 사용합니다. 또한 관리 서버는 클라우드 서비스와 통신하여 표준 HTTP 및 HTTPS 포트를 통해 업데이트를 다운로드합니다.

스토리지 노드는 Acronis Cyber Protect의 스토리지 컴포넌트입니다. 스토리지 노드는 TCP 포트 9876을 노출합니다. 이 포트는 백업 데이터를 전송하고 수신하는 데 사용됩니다. 전송은 TLS로 보호되고 인증은 상호 TLS를 사용하여 수행됩니다. 애플리케이션 수준 프로토콜은 Acronis 독점입니다. 스토리지 노드는 적절한 프로토콜 및 인증 메커니즘을 사용하여 백엔드 스토리지 시스템과 통신합니다.

카탈로그는 Acronis Cyber Protect의 지원 컴포넌트입니다. 카탈로그는 포트 9876에서 스토리지 노드의 데이터에 액세스하여 데이터를 인덱싱하고 포트 9200에서 색인을 노출합니다.

백업 게이트웨이는 차세대 Acronis 독점 데이터 액세스 프로토콜을 구현합니다. 고객이 클라우드 백업을 선택한 경우 동일한 컴퍼넌트가 Acronis Cyber Cloud에서 사용됩니다. IANA에 등록된 TCP 포트 44445는 게이트웨이에서 사용합니다. 데이터 보호는 TLS를 통해 수행되고 인증은 상호 TLS를 사용하여 수행됩니다. 백업 게이트웨이에서 HTTPS 기반 관리 서비스를 위해 포트 8888을 사용할 수도 있습니다.

에이전트는 위에 설명된 대로 포트를 통해 관리 서버, 스토리지 노드 및 백업 게이트웨이와 통신합니다. 에이전트는 표준 기반 파일 서비스(SMB, NFS)가 백업 대상으로 사용되는 경우 해당 서비스와 통신할 수도 있습니다. 이 경우 표준 포트와 적절한 인증 프로토콜이 사용됩니다. Agent for VMware는 VMware vSphere에서 정의한 포트를 통해 VMware vSphere API를 사용합니다(해당 기능이 구성되어 있는 경우).

Linux에 대한 취약성 평가는 AcronisCyber Cloud에 디플로이된 CVSS 서비스를 통해 구현됩니다. 보호 에이전트는 목록(https://cloud.acronis.com/services.json)에서 ping을 통해 가장 가까운 데이터 센터를 동적으로 선택합니다.

온프레미스 디플로이

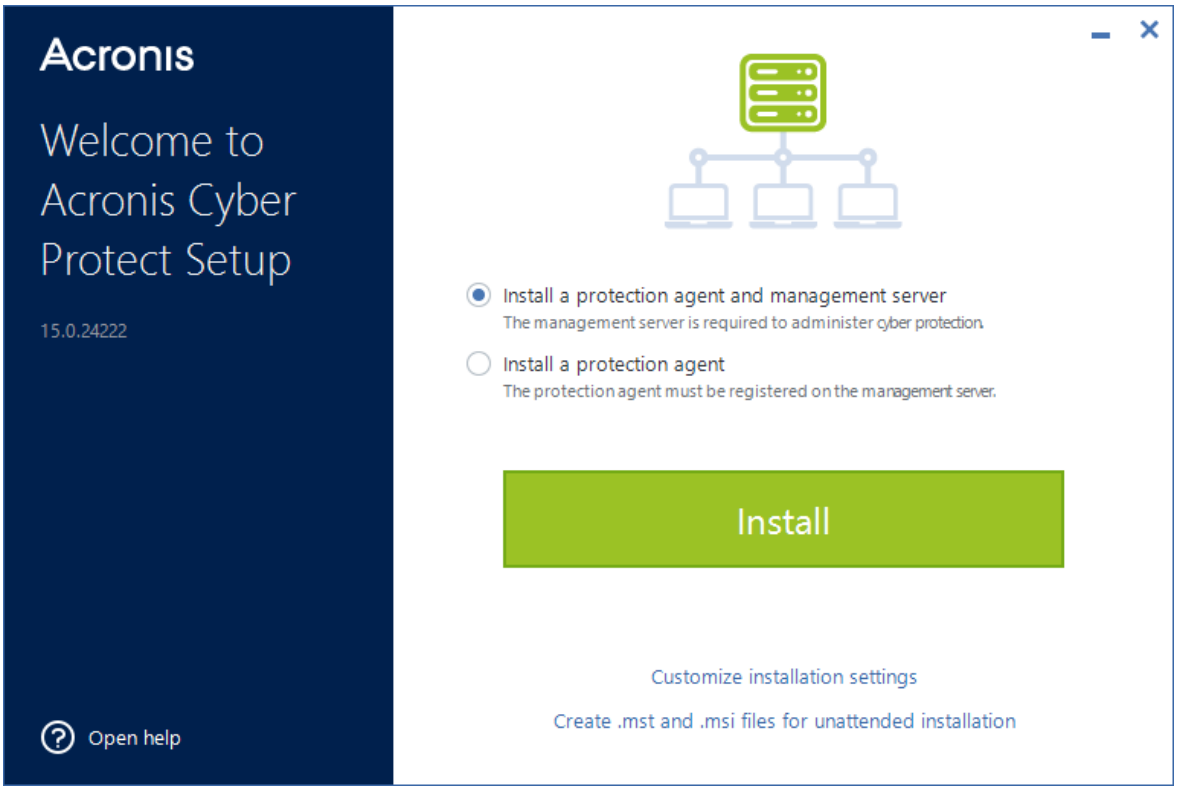
온프레미스 디플로이에는 "컴퍼넌트"(46페이지) 섹션에 설명되어 있는 다수의 소프트웨어 컴퍼넌트가 포함됩니다. 이러한 컴퍼넌트 간의 상호 작용 방식 및 필요한 포트와 관련된 자세한 내용은 "Acronis Cyber Protect에 대한 네트워크 연결 다이어그램"(75페이지)을(를) 참조하십시오.

관리 서버 설치

Windows에 설치

관리 서버를 설치하려면

1. 관리자로 로그온하고 Acronis Cyber Protect 설정 프로그램을 시작합니다.
2. [선택 사항] 설치 프로그램의 언어를 변경하려면 **언어 설정**을 클릭합니다.
3. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
4. **보호 에이전트 및 관리 서버 설치**의 기본 설정을 유지합니다.



5. 다음 중 하나를 수행하십시오.
   - **설치**를 클릭합니다.
     제품을 설치하는 가장 쉬운 방법입니다. 대부분의 설치 매개변수는 기본값으로 설정됩니다. 다음 컴퍼넌트가 설치됩니다.
     - Management Server
     - 원격 설치 컴퍼넌트
     - Agent for Windows
     - 각 하이퍼바이저나 애플리케이션이 머신에서 감지된 경우 다른 에이전트(Agent for Hyper-V, Agent for Exchange, Agent for SQL, Agent for Active Directory)
     - Bootable Media Builder
     - 명령줄 도구
     - Cyber Protect 모니터링

- **설치 설정 사용자 정의**를 클릭하여 설정을 구성합니다.
  설치될 컴퍼넌트를 선택하고 추가 매개변수를 지정할 수 있습니다. 자세한 내용은 "설치 설정 사용자 정의"(80페이지)을(를) 참조하십시오.
- **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭하여 설치 패키지를 추출합니다. .mst 파일에 추가될 설치 설정을 검토하거나 수정한 다음, **생성**을 클릭합니다. 이 절차의 추가 단계는 필수 단계가 아닙니다.
  그룹 정책을 통해 에이전트를 디플로이하려면 "그룹 정책을 통해 에이전트 배포"(165페이지) 항목을 참조하십시오.

6. 설치를 계속 진행합니다.
7. 설치가 완료되면 **닫기**를 클릭합니다.

관리 서버 사용을 시작하려면 Acronis 계정에 로그인하거나 활성화 파일을 사용하여 관리 서버를 활성화합니다.

설치 설정 사용자 정의

이 섹션에서는 설치 중 변경될 수 있는 설정에 대해 설명합니다.

설치할 컴퍼넌트

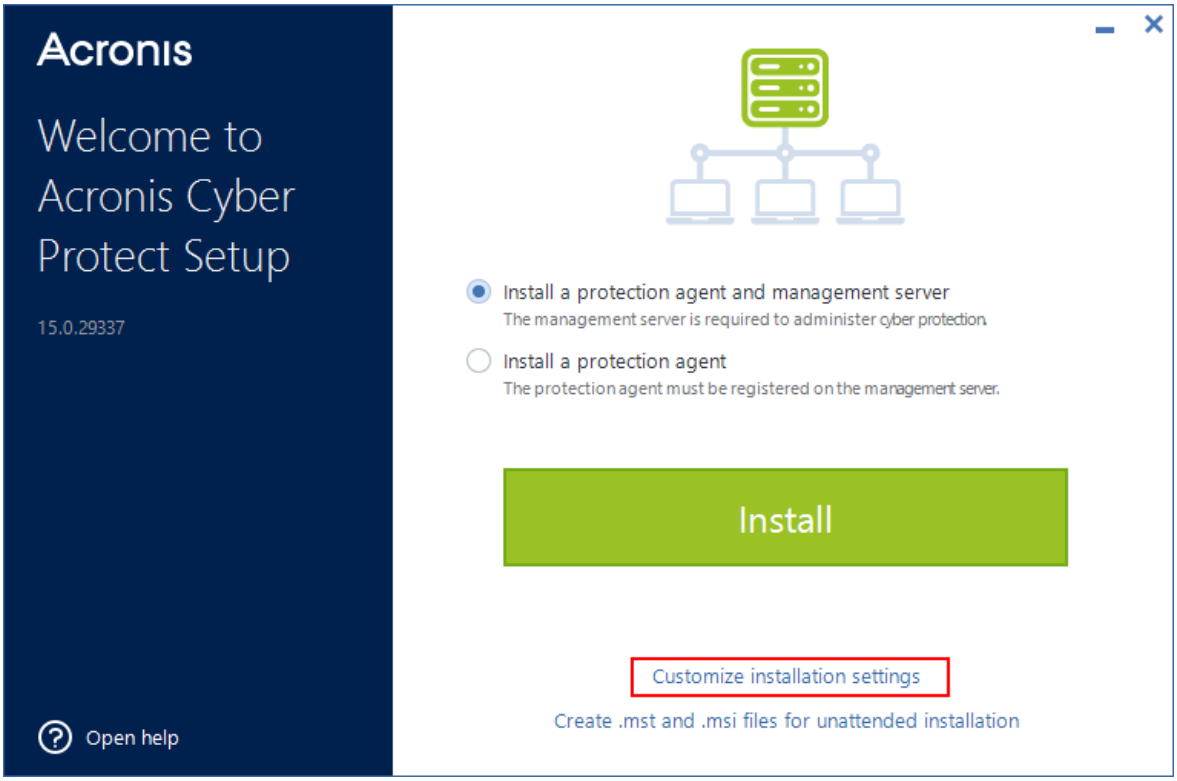
관리 서버 및 보호 에이전트를 모두 설치했는지 아니면 보호 에이전트만 설치했는지에 따라 다음 컴포넌트가 기본적으로 선택됩니다.

관리 서버 및 보호 에이전트	보호 에이전트만
Management Server	Agent for Windows
원격 설치 컴퍼넌트	Bootable Media Builder
Agent for Windows	명령줄 도구
Bootable Media Builder	Cyber Protect 모니터
명령줄 도구	
Cyber Protect 모니터	

사용 가능한 컴포넌트의 전체 목록은 "컴퍼넌트"(46페이지) 항목을 참조하십시오.

선택적 컴포넌트를 설치하려면

1. 설치 마법사에서 **설치 설정 사용자 정의**를 클릭합니다.



2. **설치할 항목**에서 **변경**을 클릭합니다.
3. 원하는 컴포넌트를 선택한 다음 **완료**를 클릭합니다.
4. 메시지가 표시되면 선택한 컴포넌트의 설정을 구성합니다.
5. **설치**를 클릭합니다.

서비스 로그온 계정

각각 **에이전트 서비스를 위한 로그온 계정** 및 **관리 서버 서비스용 로그온 계정** 옵션을 사용하여 에이전트 또는 관리 서비스를 실행할 계정을 변경할 수 있습니다.

다음 옵션 중 하나를 선택할 수 있습니다.

- **서비스 사용자 계정 사용**(에이전트 서비스용 기본값)
  서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 옵션의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다.
- **새 계정 생성**(관리 서버 서비스 및 스토리지 노드 서비스용 기본값)
  에이전트 서비스, 관리 서버 서비스, 스토리지 노드 서비스에 대한 계정의 이름은 각각 **Acronis Agent User**, **AMS User**, **ASN User**로 지정됩니다.
- **다음 계정 사용**
  도메인 컨트롤러에 제품을 설치하는 경우 설치 프로그램에 각 서비스의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

도메인 컨트롤러에서 설치 프로그램을 실행할 때 지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다. 이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

또한 **다음 계정 사용**을 선택하면 SQL 데이터베이스에 관리 서버를 구성한 경우 Microsoft SQL Server에 Windows 인증을 사용할 수 있습니다.

새 계정 생성 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당된 사용자 권한이 박탈되는 경우 관련 컴포넌트가 올바로 작동하지 않거나 아예 작동하지 않을 수 있습니다.

서비스 로그온 계정에 필요한 사용자 권한

보호 에이전트는 Windows 머신에서 **Managed Machine Service**(MMS)로 실행됩니다. 에이전트가 실행되는 계정에는 해당 에이전트가 올바르게 작동할 수 있도록 특정 권한이 있어야 합니다.

1. MMS 사용자가 **Backup Operators** 및 **관리자** 그룹에 포함되어 있어야 합니다. 도메인 컨트롤러에서 사용자가 **도메인 관리자** 그룹에 포함되어 있어야 합니다.
2. MMS 사용자에게 `%PROGRAMDATA%\Acronis`(Windows XP 및 Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) 폴더 및 해당 하위 폴더에 대한 **전체 제어** 권한이 부여되어야 합니다.
3. MMS 사용자에게 다음 키 중 특정 레지스트리 키에 대한 **전체 제어** 권한이 부여되어야 합니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. MMS 사용자에게 Windows에서 다음 사용자 권한이 할당되어야 합니다.
   - **서비스로 로그온**
   - **프로세스에 대한 메모리 할당량 조정**
   - **프로세스 수준 토큰 교체**
   - **펌웨어 환경 값 수정**

ASN 사용자는 Acronis 스토리지 노드가 설치되어 있는 머신에 대한 로컬 관리자 권한이 있어야 합니다.

Windows에서 사용자 권한을 할당하려면

참고

이 절차에서는 **서비스로 로그온** 사용자 권한을 예로 사용합니다. 다른 사용자 권한의 경우도 단계는 동일합니다.

---

1. 관리자로 컴퓨터에 로그인합니다.
2. **제어판**에서 **관리 도구**를 엽니다. 또는 키보드에서 Win+R을 누르고 **control admintools**를 입력한 후 Enter 키를 누릅니다.
3. **로컬 보안 정책**을 엽니다.
4. **로컬 정책**을 확장하고 **사용자 권한 할당**을 클릭합니다.
5. 오른쪽 창에서 **서비스로 로그온**을 마우스 오른쪽으로 클릭하고 **속성**을 선택합니다.

6. **사용자 또는 그룹 추가...**를 클릭하여 새 사용자를 추가합니다.
7. **사용자 또는 그룹 선택** 창에서 추가하려는 사용자를 찾아 **확인**을 클릭합니다.
8. **서비스로 로그온 속성** 창에서 **확인**을 클릭하여 변경 사항을 저장합니다.

참고
서비스로 로그온 사용자 권한에 추가한 사용자가 **로컬 보안 정책**의 **서비스로 로그온 거부** 정책에 포함되어 있지 않아야 합니다.

중요
설치가 완료된 후 수동으로 로그온 계정을 변경하는 것은 권장되지 않습니다.

관리 서버용 데이터베이스

다음 데이터베이스를 사용하여 관리 서버를 구성할 수 있습니다.

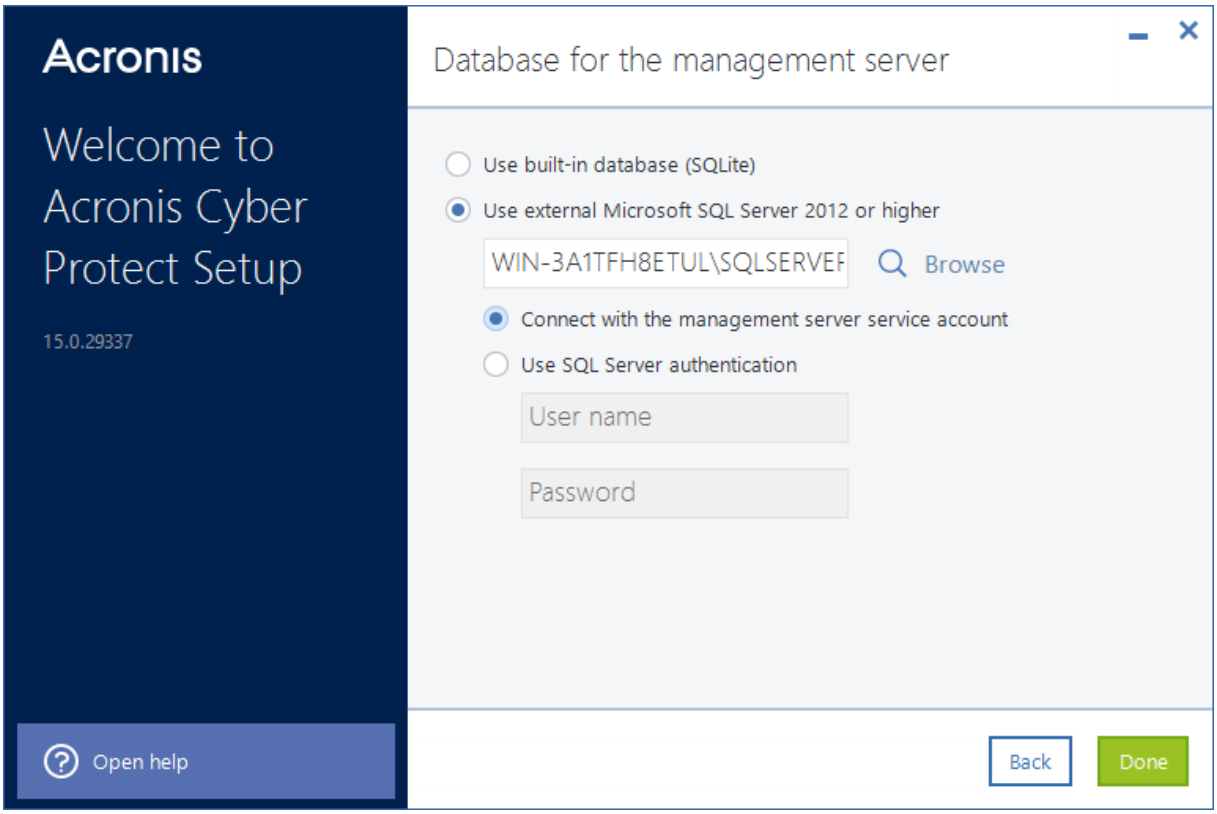
- SQLite

  기본적으로 관리 서버는 기본 제공 SQLite 데이터베이스를 사용합니다. SQLite 데이터베이스를 사용하면 약 900-1,000개의 워크로드를 관리 서버에 등록할 수 있습니다. SQLite는 검색 서비스와 호환되지 않습니다.
- Microsoft SQL

  Microsoft SQL을 사용하면 눈에 띄는 성능 저하 없이 최대 8,000개의 워크로드를 관리 서버에 등록할 수 있습니다. 동일한 Microsoft SQL 인스턴스를 관리 서버, 검색 서비스 및 기타 프로그램에서 사용할 수 있습니다.

  지원되는 MS SQL Server 버전은 다음과 같습니다.
  - Microsoft SQL Server 2019 (Windows에서 실행)
  - Microsoft SQL Server 2017(Windows에서 실행)
  - Microsoft SQL Server 2016
  - Microsoft SQL Server 2014
  - Microsoft SQL Server 2012

Microsoft SQL 인스턴스가 기본 인스턴스인 **MSSQLSERVER**이면 인스턴스가 실행되는 머신의 이름만 지정할 수 있습니다. 인스턴스에 사용자 정의 이름이 있는 경우 `machine name\instance name` 형식으로 이름을 지정해야 합니다.



참고

Microsoft SQL 인스턴스를 실행하는 머신에서 SQL Server Browser 서비스 및 TCP/IP 클라이언트 프로토콜이 활성화되었는지 확인하십시오. SQL Server Browser 서비스 시작 방법에 대한 자세한 내용은 http://msdn.microsoft.com/en-us/library/ms189093.aspx를 참조하십시오.TCP/IP 프로토콜도 비슷한 절차를 통해 활성화할 수 있습니다.

지정한 Microsoft SQL 인스턴스에 연결하려는 경우 다음 인증 방법을 사용할 수 있습니다.

- Windows 인증(**관리 서버 서비스 계정을 사용하여 연결**)
  이 방법은 **다음 계정 사용** 옵션을 사용하여 관리 서버 서비스에 대한 로그온 계정을 구성한 경우(예: `<MACHINE NAME>\Administrator` 지정)에 사용할 수 있습니다. 지정한 계정은 Microsoft SQL Server에서 **dbcreator** 또는 **sysadmin** 역할이 있어야 합니다.
  로그온 계정에 대한 자세한 내용은 "서비스 로그온 계정에 필요한 사용자 권한"(82페이지) 항목을 참조하십시오.
- SQL 서버 인증
  이 방법은 언제든 사용할 수 있습니다. 지정한 계정은 Microsoft SQL Server에서 **dbcreator** 또는 **sysadmin** 역할이 있어야 합니다.

검색 서비스

검색 서비스는 클라우드 스토리지나 로컬 또는 네트워크 폴더에서 백업의 안티맬웨어 스캔을 활성화하는 선택적 컴포넌트입니다. 검색 서비스를 사용하려면 동일한 머신에 관리 서버가 설치되어 있어야 합니다.

설치 서비스를 설치하면 다음 기능을 사용할 수 있습니다.

- 백업 스캔 계획
- 백업 스캔 세부정보 위젯
- 기업 허용 목록
- 안전 복구
- 백업 목록의 **상태** 열

검색 서비스는 관리 서버를 설치하는 동안 설치하거나 나중에 기존 설치를 수정하여 추가할 수 있습니다. 검색 서비스를 선택적 컴포넌트로 설치하는 방법은 "선택적 컴포넌트를 설치하려면"(80 페이지) 항목을 참조하십시오.

중요

검색 서비스는 관리 서버에서 사용하는 기본 SQLite 데이터베이스와 호환되지 않습니다.

Microsoft SQL 또는 PostgerSQL 데이터베이스에 검색 서비스를 구성할 수 있습니다. 데이터베이스 선택 방법에 대한 자세한 내용은 "검색 서비스용 데이터베이스"(86페이지) 항목을 참조하십시오.

검색 서비스용 데이터베이스

검색 서비스는 관리 서버용 기본 데이터베이스인 SQLite와 호환되지 않습니다.

관리 서버에서 SQLite를 사용할 경우 PostgreSQL 데이터베이스에만 검색 서비스를 구성할 수 있습니다. PostgreSQL 9.6 이상이 지원됩니다.

관리 서버에서 Microsoft SQL Server를 사용할 경우 추가 설정 없이 동일한 데이터베이스에 검색 서비스를 구성할 수 있습니다. PostgreSQL 데이터베이스에도 검색 서비스를 구성할 수 있습니다.

PostgreSQL 데이터베이스에 검색 서비스를 구성하려면

1. 설치 마법사의 **검색 서비스용 데이터베이스**에서 **변경**을 클릭합니다.
2. **PostgreSQL Server 데이터베이스**를 선택합니다.
3. PostgreSQL 인스턴스의 호스트 이름 또는 IP 주소와 포트를 지정합니다.
4. **CREATEDB** 권한이 있거나 superuser인 사용자의 자격 증명을 지정합니다.

   참고
   SCRAM-SHA-256 인증 방법은 PostgreSQL 10 이상에서는 지원되지 않습니다.

5. **완료**를 클릭합니다.

포트

관리 서버에 액세스하기 위해 웹 브라우저에서 사용할 포트(기본적으로 9877)와 제품 컴포넌트 간의 통신에 사용할 포트(기본적으로 7780)를 사용자 정의할 수 있습니다. 설치가 완료된 후 제품 컴포넌트 간의 통신에 사용할 포트를 변경하려면 모든 컴포넌트를 다시 등록해야 합니다.

Windows 방화벽은 설치 중 자동으로 구성됩니다. 다른 방화벽을 사용하는 경우 해당 방화벽을 통해 들어오고 나가는 요청 모두에 대해 포트가 열려 있는지 확인하십시오.

프록시 서버

클라우드 스토리지에 백업하고 여기에서 복구할 때 보호 에이전트가 HTTP 프록시 서버를 사용할지 여부를 선택할 수 있습니다.

또한 다양한 Acronis Cyber Protect 컴포넌트 간 통신에 동일한 프록시 서버를 사용하십시오

프록시 서버를 사용하려면 해당 호스트 이름 또는 IP 주소 및 포트 번호를 지정합니다. 프록시 서버를 인증해야 하는 경우 액세스 자격 증명을 지정합니다.

참고
프록시 서버를 사용할 때 보호 정의(안티바이러스 및 안티맬웨어 정의, 고급 감지 정의, 취약점 평가 및 패치 관리 정의)는 업데이트할 수 없습니다.

Linux에 설치

준비

1. 관리 서버와 함께 Agent for Linux를 설치하려면 필요한 Linux 패키지가 머신에 설치되는지 확인하십시오.
2. 관리 서버가 사용할 데이터베이스를 선택합니다.

제한

Linux 머신에서 실행되는 관리 서버에서는 자동 검색 절차 등에 사용되는 보호 에이전트를 원격으로 설치할 수 없습니다. 이러한 경우 사용할 수 있는 해결 방법과 관련된 자세한 내용은 Acronix 지식 베이스 https://kb.acronis.com/content/69553을 참조하십시오.

설치

관리 서버를 설치하려면 4GB 이상의 디스크 여유 공간이 필요합니다.

관리 서버를 설치하려면

1. 루트 사용자로 설치 파일이 있는 디렉토리로 이동하여 파일을 실행 가능하도록 설정한 후에 실행합니다.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

2. 라이센스 계약 조건에 동의합니다.
3. [선택 사항] 설치할 컴퍼넌트를 선택합니다.
   기본적으로 다음 컴퍼넌트가 설치됩니다.
   - Management Server
   - Agent for Linux
   - Bootable Media Builder
4. 관리 서버에 액세스하기 위해 웹 브라우저에서 사용할 포트를 지정하십시오. 기본값은 9877입니다.
5. 제품 컴퍼넌트 간 통신에 사용될 포트를 지정합니다. 기본값은 7780입니다.
6. **다음**을 클릭하여 설치를 계속 진행합니다.
7. 설치가 완료되면 **웹 콘솔 열기**를 선택한 다음 **종료**를 클릭합니다. 사용자의 기본 웹 브라우저에 Cyber Protect 웹 콘솔이 열립니다.

관리 서버 사용을 시작하려면 Acronis 계정에 로그인하거나 활성화 파일을 사용하여 관리 서버를 활성화합니다.

Acronis Cyber Protect 어플라이언스

Acronis Cyber Protect 어플라이언스를 사용하여 다음 소프트웨어가 있는 가상 머신을 쉽게 얻을 수 있습니다.

- CentOS
- Acronis Cyber Protect 컴퍼넌트:
  - Management Server
  - Agent for Linux
  - Agent for VMware(Linux)

이 어플라이언스는 .zip 아카이브로 제공됩니다. 아카이브에는 .ovf 및 .iso 파일이 포함되어 있습니다. .ovf 파일을 ESXi 호스트에 디플로이하거나 .iso 파일을 사용하여 기존 가상 머신을 부팅할 수 있습니다. 아카이브에는 .ovf 파일과 같은 디렉터리에 위치해야 하는 .vmdk 파일도 포함되어 있습니다.

참고
VMware Host Client(독립형 ESXi 6.0+ 관리에 사용되는 웹 클라이언트)는 ISO 이미지가 포함되어 있는 OVF 템플릿의 디플로이를 허용하지 않습니다. 이 경우에는 아래의 요구 사항을 충족하는 가상 머신을 생성하고 .iso 파일을 사용하여 소프트웨어를 설치합니다.

가상 어플라이언스의 요구 사항은 다음과 같습니다.

- 최소 시스템 요구 사항
  - CPU 2개
  - 6GB RAM
  - 10GB 가상 디스크 1개(40GB 권장)
- VMware 가상 머신 설정에서 **옵션** 탭 > **일반** > **구성 매개변수**를 클릭한 다음, `disk.EnableUUID` 매개변수 값이 `true`인지 확인합니다.

제한

Acronis Cyber Protect 어플라이언스를 비롯한 Linux 머신에서 실행되는 관리 서버에서는 자동 검색 절차 등에 사용되는 보호 에이전트를 원격으로 설치할 수 없습니다. 이러한 경우 사용할 수 있는 해결 방법과 관련된 자세한 내용은 Acronix 지식 베이스 https://kb.acronis.com/content/69553을 참조하십시오.

소프트웨어 설치

1. 다음 중 하나를 수행하십시오.
   - .ovf 파일에서 어플라이언스를 배포하십시오. 디플로이가 완료되면 해당 머신을 켭니다.
   - .iso에서 기존 가상 머신을 부팅합니다.
2. **Acronis Cyber Protect 설치 또는 업데이트**를 선택한 후 **Enter** 키를 누릅니다. 초기 설치 창이 나타날 때까지 기다립니다.

3. [선택 사항] 설치 설정을 변경하려면 **설정 변경**을 선택한 다음 **Enter**를 누릅니다. 다음 설정을 지정할 수 있습니다.
   - 어플라이언스의 호스트 이름(기본적으로 `AcronisAppliance-<무작위 부분>`)
   - Cyber Protect 웹 콘솔에 로그인하는 데 사용할 "루트" 계정의 패스워드(기본적으로 **지정되어 있지 않음**)

     기본값을 그대로 두면 Acronis Cyber Protect 설치 후 패스워드를 지정하라는 메시지가 표시됩니다. 이 패스워드가 없으면 Cyber Protect 웹 콘솔 및 Cockpit 웹 콘솔에 로그인할 수 없게 됩니다.
   - 네트워크 인터페이스 카드의 네트워크 설정:
     - **DHCP 사용**(기본값)
     - **고정 IP 주소 설정**

     머신에 네트워크 인터페이스 카드가 여러 개 있는 경우 소프트웨어가 그 중 하나를 무작위로 선택하고 이 설정을 그 카드에 적용합니다.
4. **현재 설정으로 설치**를 선택합니다.

그러면 CentOS 및 Acronis Cyber Protect이(가) 머신에 설치됩니다.

추가 작업

설치가 완료된 후 소프트웨어가 Cyber Protect 웹 콘솔 및 Cockpit 웹 콘솔로 연결되는 링크를 표시합니다. Acronis Cyber Protect을(를) 사용하여 시작할 Cyber Protect 웹 콘솔에 연결합니다(장치 더 추가, 백업 계획 생성 등).

ESXi 가상 머신을 추가하려면 **추가** > **VMware ESXi**를 클릭한 다음 vCenter Server 또는 독립형 ESXi 호스트의 주소 및 자격 증명을 지정합니다.

Cockpit 웹 콘솔에서 구성하는 Acronis Cyber Protect 설정은 없습니다. 이 콘솔은 편의 및 문제 해결용으로 제공됩니다.

소프트웨어 업데이트

1. 새 어플라이언스 버전의 .zip 아카이브를 다운로드하고 압축을 풉니다.
2. 이전 단계에서 압축을 푼 .iso에서 머신을 부팅합니다.
   a. vSphere 데이터 저장소에 .iso를 저장합니다.
   b. 머신의 CD/DVD 드라이브에 .iso을 연결합니다.
   c. 머신을 다시 시작합니다.
   d. [첫 업데이트 시에만 해당] **F2**를 누른 다음 CD/DVD 드라이브가 첫 번째가 되도록 부팅 순서를 변경합니다.
3. **Acronis Cyber Protect 설치 또는 업데이트**를 선택한 후 **Enter** 키를 누릅니다.
4. **업데이트**를 선택하고 **Enter**를 누릅니다.
5. 업데이트가 완료되면 머신의 CD/DVD 드라이브로부터 .iso을 분리합니다.

그러면 Acronis Cyber Protect이(가) 업데이트됩니다. .iso 파일의 CentOS 버전이 디스크에 있는 버전보다 최신인 경우 Acronis Cyber Protect 업데이트 전에 운영 체제가 먼저 업데이트됩니다.

Cyber Protect 웹 콘솔에서 머신 추가

다음 방법 중 하나로 머신을 추가할 수 있습니다.

- 설치 프로그램을 다운로드한 후 대상 머신에서 로컬로 실행.
- 대상 머신에 보호 에이전트를 원격으로 설치.

제한 사항

- 원격 설치는 Windows 머신에서 실행 중인 관리 서버를 통해서만 가능합니다. 대상 머신에서도 Windows를 실행 중이어야 합니다.
- Windows XP를 실행하는 머신에서는 원격 설치가 지원되지 않습니다.
- 도메인 컨트롤러에서는 원격 설치가 지원되지 않습니다. 도메인 컨트롤러에 보호 에이전트를 설치하는 방법을 알아보려면 "Windows에 설치"(98페이지) 항목을 참조하십시오. **에이전트 서비스용 로그온 계정**에서 **다음 계정 사용**을 선택하여 설치 설정을 사용자 지정합니다. 이 옵션에 대해 자세히 알아보려면 "서비스 로그온 계정에 필요한 사용자 권한"(82페이지) 항목을 참조하십시오.

Windows를 실행 중인 머신 추가

Windows 머신은 보호 에이전트를 원격으로 설치하여 추가하거나, Cyber Protect 웹 콘솔에서 추가하거나, 설치 프로그램을 다운로드하여 로컬로 실행하는 방법을 통해 추가할 수 있습니다.

원격으로 에이전트를 설치하려면

중요
설치를 시작하기 전에 원격 설치의 전제조건이 충족되었으며 디플로이먼트 에이전트로 사용 가능한 에이전트가 환경에 하나 이상 있는지 확인합니다. 자세한 내용은 "원격 설치의 전제조건"(91페이지) 및 "디플로이먼트 에이전트"(93페이지) 항목을 참조하십시오.

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **추가**를 클릭합니다.
3. [Agent for Windows를 설치하려면] **Windows**를 클릭합니다.
4. [지원되는 기타 에이전트를 설치하려면] 보호할 애플리케이션에 해당하는 버튼을 클릭합니다. 다음 에이전트를 선택할 수 있습니다.
   - Agent for Hyper-V
   - Agent for SQL + Agent for Windows
   - Agent for Exchange + Agent for Windows

     Microsoft Exchange Server > **Exchange 사서함**을 클릭한 경우 Agent for Exchange가 하나 이상 이미 등록되어 있다면 9단계로 넘어갑니다.
   - Agent for Active Directory + Agent for Windows
   - Agent for Office 365
5. 창이 열리면 디플로이먼트 에이전트를 선택합니다.

6. 대상 머신의 호스트 이름 또는 IP 주소를 지정하고 해당 머신에 대한 관리 권한이 있는 계정의 자격 증명을 지정합니다.

   기본 제공 Administrator 계정을 사용하는 것이 좋습니다. 다른 계정을 사용하려면 관리자 그룹에 해당 계정을 추가하고 https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows 문서에 설명된 대로 대상 머신의 레지스트리를 수정합니다.

7. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다.

   기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경ㄱ우에는 IP 주소를 대신 선택해야 할 수 있습니다.

8. **설치**를 클릭합니다.
9. [4단계에서 **Microsoft Exchange Server** > **Exchange 사서함**을 선택한 경우] Microsoft Exchange Server의 **클라이언트 액세스** 서버 역할(CAS)이 활성화되어 있는 머신을 지정합니다.

   자세한 내용은 "사서함 백업"(415페이지) 항목을 참조하십시오.

에이전트를 다운로드하여 로컬에 설치하려면

1. Cyber Protect 웹 콘솔의 오른쪽 상단에 있는 계정 아이콘을 클릭하고 **다운로드**를 클릭합니다.
2. 필요한 Windows 인스톨러의 이름을 클릭합니다.

   머신에 설정 프로그램이 다운로드됩니다.
3. 보호할 머신에서 설치 프로그램을 실행합니다. 자세한 내용은 "Windows에 설치"(98페이지) 항목을 참조하십시오.

원격 설치의 전제조건

- Windows 7 이상을 실행하는 원격 머신에 설치하려면 해당 머신에서 **제어판** > **폴더 옵션** > **보기** > **공유 마법사 사용** 옵션을 *비활성화*해야 합니다.
- Active Directory 도메인에 속하지 *않는* 원격 머신에 설치를 완료하려면 해당 머신에서 사용자 계정 컨트롤(UAC)을 *비활성화*해야 합니다. 이 옵션을 비활성화하는 방법을 자세히 알아보려면 "UAC를 비활성화하려면"(92페이지) 항목을 참조하십시오.
- 기본적으로는 모든 Windows 머신에서 원격 설치를 수행하려면 기본 제공 Administrator 계정의 자격 증명이 필요합니다. 다른 관리자 계정의 자격 증명을 이용해 원격 설치를 수행하려면, 사용자 계정 컨트롤(UAC) 원격 제한 사항을 반드시 *비활성화*해야 합니다. 해당 제한 사항을 비활성화하는 방법을 자세히 알아보려면 "UAC 원격 제한 사항을 비활성화하려면"(92페이지) 항목을 참조하십시오.
- 원격 머신에서 파일과 프린터 공유를 *활성화*해야 합니다. 이 옵션에 액세스하려면:
  - [Windows 2003 Server를 실행 중인 머신] **제어판** > **Windows 방화벽** > **예외** > **파일 및 프린터 공유**로 이동합니다.
  - [Windows Server 2008, Windows 7 이상을 실행 중인 머신] **제어판** > **Windows 방화벽** > **네트워크 및 공유 센터** > **고급 공유 설정 변경**으로 이동합니다.
- Acronis Cyber Protect에서는 원격 설치 시 TCP 포트 **445**, **25001**, **43234**를 사용합니다.

포트 **445**는 파일 및 프린터 공유를 활성화하면 자동으로 열립니다. 포트 43234 및 25001은 Windows 방화벽에서 자동으로 열립니다. 다른 방화벽을 사용하는 경우에는 수신 및 발신 요청에 모두 이 포트 3개가 열려 있는지(예외에 추가) 확인합니다.

원격 설치가 완료된 후에는 포트 **25001**이 Windows 방화벽에서 자동으로 닫힙니다. 이후 에이전트를 원격으로 업데이트하려면 포트 **445** 및 **43234**를 연 채로 두어야 합니다. 포트 **25001**은 각 업데이트 중에 Windows 방화벽에서 자동으로 열렸다가 닫힙니다. 다른 방화벽을 사용하는 경우 세 개 포트를 모두 연 채로 유지하십시오.

참고
Windows XP를 실행하는 머신에서는 원격 설치가 지원되지 않습니다.

참고
도메인 컨트롤러에서는 원격 설치가 지원되지 않습니다. 도메인 컨트롤러에 보호 에이전트를 설치하는 방법을 알아보려면 "Windows에 설치"(98페이지) 항목을 참조하십시오. **에이전트 서비스용 로그온 계정**에서 **다음 계정 사용**을 선택하여 설치 설정을 사용자 지정합니다. 이 옵션에 대해 자세히 알아보려면 "서비스 로그온 계정에 필요한 사용자 권한"(82페이지) 항목을 참조하십시오.

UAC(User Account Control)에 대한 요구 사항

Windows 7 이상을 실행하고 Active Directory 도메인에 속하지 않는 머신에서 중앙 집중식 관리 작업(원격 설치 포함)을 수행하려면 UAC 및 UAC 원격 제한 사항을 비활성화해야 합니다.

UAC를 비활성화하려면

운영 체제에 따라 다음 중 하나를 수행합니다.

- **Windows 8 이전 Windows 운영 체제:**
  제어판 > 보기 기준: 작은 아이콘 > 사용자 계정 > 사용자 계정 제어 설정 변경으로 이동한 후 슬라이더를 **알리지 않음**으로 이동합니다. 그런 다음 머신을 다시 시작합니다.
- **모든 Windows 운영 체제**:
  1. 레지스트리 편집기를 엽니다.
  2. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System**
  3. **EnableLUA** 값은 설정을 **0**으로 변경합니다.
  4. 머신을 다시 시작합니다.

UAC 원격 제한 사항을 비활성화하려면

1. 레지스트리 편집기를 엽니다.
2. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**
3. **LocalAccountTokenFilterPolicy** 값은 설정을 **1**로 변경합니다.
   LocalAccountTokenFilterPolicy 값이 존재하지 않는 경우 DWORD(32비트)로 생성합니다. 이 값에 대한 자세한 내용은 다음 Microsoft 문서를 참조하십시오.

https://support.microsoft.com/en-us/help/951016/description-of-user-account-control-and-remote-restrictions-in-windows.

참고
보안상의 이유로 원격 설치와 같은 관리 작업을 마친 후에는 두 설정을 모두 원래 상태로 되돌리는 것이 좋습니다. 즉, **EnableLUA=1**로 설정하고 **LocalAccountTokenFilterPolicy=0**으로 설정합니다.

디플로이먼트 에이전트

Cyber Protect 웹 콘솔에서 원격 머신에 보호 에이전트를 설치하려면 환경에 에이전트가 하나 이상 이미 설치되어 있어야 합니다. 이 에이전트가 원격 설치용 디플로이먼트 에이전트로 사용되며 관리 서버와 대상 원격 머신에 연결됩니다.

관리 서버와 함께 설치하는 에이전트는 대개 환경의 첫 번째 보호 에이전트입니다. 그러나 환경의 각 Agent for Windows를 디플로이먼트 에이전트로 선택할 수 있습니다.

참고
자동 검색을 사용해 여러 머신에 보호 에이전트를 설치하는 경우의 디플로이먼트 에이전트는 검색 에이전트입니다.

디플로이먼트 에이전트의 작동 방식

1. 디플로이먼트 에이전트가 관리 서버에 연결하여 `web_installer.exe` 파일을 다운로드합니다.
2. 디플로이먼트 에이전트가 원격 머신의 호스트 이름이나 IP 주소 그리고 사용자가 지정하는 관리자 자격 증명을 사용하여 해당 머신에 연결한 다음 이 머신에 `web_installer.exe` 파일을 업로드합니다.
3. 원격 머신에서 `web_installer.exe` 파일이 무인 모드로 실행됩니다.
4. 필요한 설치의 범위에 따라 웹 인스톨러가 관리 서버의 `installation_files` 폴더에서 추가 설치 패키지를 검색한 다음 `msiexec` 명령을 사용하여 대상 머신에 해당 패키지를 설치합니다.
   `installation_files` 폴더의 위치는 다음과 같습니다.
   - Windows: `\Program Files\Acronis\RemoteInstallationFiles\`
   - Linux: `/usr/lib/Acronis/RemoteInstallationFiles/`
5. 설치가 완료되면 관리 서버에 에이전트가 등록됩니다.

원격 설치 구성 요소

관리 서버를 설치하면 원격 설치 컴포넌트가 기본적으로 설치됩니다.

관리 서버가 실행되는 머신의 운영 체제에 따라 이러한 컴포넌트는 다음 위치에 있습니다.

- Windows: `%Program Files%\Acronis\RemoteInstallationFiles\installation_files`
- Linux: `/usr/lib/Acronis/RemoteInstallationFiles/installation_files`

이전 버전의 Acronis Cyber Protect에서 업그레이드하는 경우 또는 관리 서버를 설치할 때 **원격 설치 컴포넌트**를 명시적으로 제외한 경우에는 이러한 위치를 사용하지 못할 수도 있습니다. 이 경우

에는 기존 Acronis Cyber Protect 설치를 업데이트 및 수정하여 원격 설치 컴포넌트를 수동으로 추가해야 합니다.

기존 설치에 원격 설치 컴포넌트를 추가하려면

1. Acronis 웹 사이트에서 Acronis Cyber Protect의 최신 설치 파일을 다운로드합니다.
   사용 중인 운영 체제의 비트에 해당하는 설치 파일을 선택합니다. 대부분의 경우에는 **Windows 64비트** 설치 파일이 필요합니다. 32비트 머신에서 보호 에이전트를 원격으로 설치해야 한다면 **Windows32/64비트** 설치 파일을 다운로드합니다.
2. 관리 서버가 실행되는 머신에서 설치 파일을 시작하고 **업데이트**를 선택합니다.
3. 업데이트가 완료되면 설치 파일을 다시 시작하고 **현재 설치 수정**을 선택합니다.
4. **원격 설치 컴포넌트**를 선택하고 **완료**를 클릭합니다.

설치가 완료되면 Cyber Protect 웹 콘솔에서 원격 머신에 보호 에이전트를 설치할 수 있습니다.

Linux를 실행 중인 머신 추가

Linux 머신은 보호 에이전트를 로컬에 설치해야 추가할 수 있습니다. 원격 설치는 지원되지 않습니다.

Linux를 실행하는 머신을 추가하려면

1. Cyber Protect 웹 콘솔에서 **모든 장치** > **추가**를 클릭합니다.
2. **Linux**를 클릭합니다.
   머신에 설정 프로그램이 다운로드됩니다.
3. 보호할 머신에서 설치 프로그램을 실행합니다. 자세한 내용은 "Linux에 설치"(100페이지) 항목을 참조하십시오.

macOS를 실행 중인 머신 추가

macOS 머신은 보호 에이전트를 로컬에 설치해야 추가할 수 있습니다. 원격 설치는 지원되지 않습니다.

macOS를 실행하는 머신을 추가하려면

1. Cyber Protect 웹 콘솔에서 **모든 장치** > **추가**를 클릭합니다.
2. **Mac**을 클릭합니다.
   머신에 설정 프로그램이 다운로드됩니다.
3. 보호할 머신에서 설치 프로그램을 실행합니다. 자세한 내용은 "macOS에 설치"(101페이지) 항목을 참조하십시오.

vCenter 또는 ESXi 호스트 추가

vCenter나 독립형 ESXi 호스트를 관리 서버에 추가하는 방법에는 다음과 같은 네 가지가 있습니다.

- Agent for VMware(가상 어플라이언스) 배포

대부분의 경우 이 방법이 권장됩니다. 사용자가 지정한 vCenter에서 관리하는 모든 호스트로 가상 어플라이언스가 자동 배포됩니다. 호스트를 선택하고 가상 어플라이언스 설정을 사용자 정의할 수 있습니다.

- Agent for VMware(Windows) 설치

  오프로드 백업이나 LAN 프리 백업이 목적이라면 Windows를 실행하는 실제 머신에 Agent for VMware를 설치하는 것이 좋습니다.

  - **오프로드 백업**

    운영 ESXi 호스트 부하가 심하여 가상 어플라이언스 실행이 바람직하지 않은 경우 이용합니다.

  - **LAN 프리 백업**

    ESXi에서 SAN 연결 스토리지를 사용하는 경우 동일한 SAN에 연결된 머신에 에이전트를 설치합니다. 에이전트는 ESXi 호스트 및 LAN을 통해서가 아니라 스토리지에서 가상 머신을 직접 백업합니다. 자세한 지침은 "LAN 프리 백업"을 참조하십시오.

  관리 서버가 Windows에서 실행 중인 경우 에이전트는 사용자가 지정하는 머신으로 자동 배포됩니다. 그렇지 않으면 에이전트를 수동으로 설치해야 합니다.

- 이미 설치된 Agent for VMware 등록

  이 단계는 관리 서버를 다시 설치한 이후에 필요한 단계입니다. 또한, OVF 템플릿에서 배포된 Agent for VMware(가상 어플라이언스)를 등록 및 구성할 수 있습니다.

- 이미 등록된 Agent for VMware 구성

  Agent for VMware(Windows)를 수동으로 설치했거나 Acronis Cyber Protect 어플라이언스를 디플로이한 이후에 필요한 단계입니다. 이미 구성된 Agent for VMware를 다른 vCenter Server 또는 독립형 ESXi 호스트에 연결할 수도 있습니다.

웹 인터페이스를 통해 Agent for VMware(가상 어플라이언스) 배포

1. **모든 장치** > **추가**를 클릭합니다.
2. **VMware ESXi**를 클릭합니다.
3. **vCenter의 각 호스트에 가상 어플라이언스로 디플로이**를 선택합니다.
4. vCenter Server 또는 독립형 ESXi 호스트의 주소 및 액세스 자격 증명을 지정합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.
5. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다. 기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경ㄱ우에는 IP 주소를 대신 선택해야 할 수 있습니다.
6. [선택 사항] 배포 설정을 사용자 정의하려면 **설정**을 클릭합니다.
   - 이는 에이전트를 배포할 ESXi 호스트의 설정을 의미합니다(vCenter Server가 이전 단계에서 지정된 경우에만).
   - 가상 어플라이언스 이름
   - 어플라이언스가 저장될 데이터 저장소
   - 어플라이언스를 포함할 리소스 풀 또는 vApp

- 가상 어플라이언스의 네트워크 어댑터가 연결될 네트워크
- 가상 어플라이언스의 네트워크 설정 DHCP 자동 구성을 선택하거나 동적 IP 주소를 포함한 값을 수동으로 지정해도 됩니다.

7. **디플로이**를 클릭합니다.

Agent for VMware(Windows) 설치

준비

"Windows를 실행 중인 머신 추가" 섹션에 설명된 준비 단계를 따릅니다.

설치

1. **모든 장치** > **추가**를 클릭합니다.
2. **VMware ESXi**를 클릭합니다.
3. **Windows를 실행 중인 머신에 원격으로 설치**를 선택합니다.
4. 디플로이 에이전트 선택.
5. 대상 머신의 호스트 이름 또는 IP 주소를 지정하고, 해당 머신에 대한 관리자 권한이 있는 계정의 자격 증명을 지정합니다.
6. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다. 기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경우에는 IP 주소를 대신 선택해야 할 수 있습니다.
7. **연결**을 클릭합니다.
8. vCenter Server 또는 독립형 ESXi 호스트의 주소 및 자격 증명을 지정한 다음, **연결**을 클릭합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.
9. **설치**를 클릭하여 에이전트를 설치합니다.

이미 설치된 Agent for VMware 등록

이 섹션은 웹 인터페이스를 통해 Agent for VMware를 등록하는 방법에 대해 설명합니다.

다른 등록 방법:

- Agent for VMware(가상 어플라이언스)는 가상 어플라이언스 UI에 관리 서버를 지정하는 방법으로 등록할 수 있습니다. "OVF 템플릿에서 Agent for VMware(가상 어플라이언스) 디플로이" 섹션에서 "가상 어플라이언스 구성" 아래에 기술된 3단계를 확인하십시오.
- Agent for VMware(Windows)는 로컬 설치되는 중에 등록됩니다.

Agent for VMware를 등록하려면

1. **모든 장치** > **추가**를 클릭합니다.
2. **VMware ESXi**를 클릭합니다.
3. **이미 설치된 에이전트 등록**을 선택합니다.
4. 디플로이 에이전트 선택.

5. *Agent for VMware(Windows)*를 등록하는 경우 에이전트를 설치할 머신의 호스트 이름 또는 IP 주소를 지정하고, 머신의 관리자 권한을 보유하는 계정의 자격 증명을 지정합니다.

   *Agent for VMware(가상 어플라이언스)*를 등록하는 경우 가상 어플라이언스의 호스트 이름 또는 IP 주소를 지정하고, 어플라이언스를 실행하는 독립형 ESXi 호스트나 vCenter Server의 자격 증명을 지정합니다.

6. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다. 기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경ㄱ우에는 IP 주소를 대신 선택해야 할 수 있습니다.
7. **연결**을 클릭합니다.
8. vCenter Server 또는 ESXi 호스트의 IP 주소 또는 호스트 이름 그리고 액세스 시 사용하는 자격 증명을 지정한 후 **연결**을 클릭합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.
9. **등록**를 클릭하여 에이전트를 등록합니다.

이미 등록된 Agent for VMware 구성

이 섹션은 웹 인터페이스를 통해 Agent for VMware를 vCenter Server 또는 ESXi와 연결하는 방법에 대해 설명합니다. 대안으로 Agent for VMware(가상 어플라이언스) 콘솔에서 수행해도 됩니다.

이 절차를 사용하여 에이전트와 vCenter Server 또는 ESXi의 기존 연결을 변경할 수도 있습니다. 대안으로 Agent for VMware(가상 어플라이언스) 콘솔에서 또는 **설정** > **에이전트** > 해당 에이전트 > **상세정보** > **vCenter/ESXi**를 클릭해 이 작업을 수행할 수도 있습니다.

Agent for VMware를 구성하려면

1. **모든 장치** > **추가**를 클릭합니다.
2. **VMware ESXi**를 클릭합니다.
3. 소프트웨어에 알파벳순으로 가장 먼저 오는 구성되지 않은 Agent for VMware가 표시됩니다. 관리 서버에 등록된 모든 에이전트가 구성되어 있는 경우 **이미 등록된 에이전트 구성**을 클릭하면 소프트웨어에 알파벳순으로 가장 먼저 오는 에이전트가 표시됩니다.
4. 필요한 경우 **에이전트가 있는 머신**을 클릭하고 구성할 에이전트를 선택합니다.
5. vCenter Server 또는 ESXi 호스트의 호스트 이름이나 IP 주소, 그리고 여기에 액세스하기 위한 자격 증명을 지정하거나 변경합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.
6. **구성**을 클릭하여 변경 사항을 저장합니다.

Scale Computing HC3 클러스터 추가

Scale Computing HC3 클러스터를 Cyber Protect 관리 서버에 추가하는 방법

1. 클러스터에 Agent for Scale Computing HC3(가상 어플라이언스) 디플로이.
2. 이 클러스터에 대한 연결과 서버에 대한 연결을 모두 구성합니다.

에이전트를 로컬에 설치

Windows에 설치

Agent for Windows, Agent for Hyper-V, Agent for Exchange, Agent for SQL 또는 Agent for Active Directory를 설치하려면

1. 관리자로 로그온하고 Acronis Cyber Protect 설정 프로그램을 시작합니다.
2. [선택 사항] 설치 프로그램의 언어를 변경하려면 **언어 설정**을 클릭합니다.
3. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
4. **보호 에이전트 설치**를 선택합니다.
5. 다음 중 하나를 수행하십시오.
   - **설치**를 클릭합니다.
     제품을 설치하는 가장 쉬운 방법입니다. 대부분의 설치 매개변수는 기본값으로 설정됩니다. 다음 컴퍼넌트가 설치됩니다.
     - Agent for Windows
     - 각 하이퍼바이저나 애플리케이션이 머신에서 감지된 경우 다른 에이전트(Agent for Hyper-V, Agent for Exchange, Agent for SQL, Agent for Active Directory)
     - Bootable Media Builder
     - 명령줄 도구
     - Cyber Protect 모니터
   - **설치 설정 사용자 정의**를 클릭하여 설정을 구성합니다.
     설치될 컴퍼넌트를 선택하고 추가 매개변수를 지정할 수 있습니다. 자세한 내용은 "설치 설정 사용자 정의"(80페이지)을(를) 참조하십시오.
   - **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭하여 설치 패키지를 추출합니다. .mst 파일에 추가될 설치 설정을 검토하거나 수정한 다음, **생성**을 클릭합니다. 이 절차의 추가 단계는 필수 단계가 아닙니다.
     그룹 정책을 통해 에이전트를 디플로이하려면 "그룹 정책을 통해 에이전트 배포"(165페이지) 항목에 설명되어 있는 대로 진행하십시오.
6. 에이전트와 함께 머신을 등록할 관리 서버를 지정합니다.
   a. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   b. 관리 서버 관리자 또는 등록 토큰의 자격 증명을 지정합니다.
      등록 토큰을 생성하는 방법에 대한 자세한 내용은 "1단계: 등록 토큰 생성"(166페이지)을(를) 참조하십시오.
   c. **완료**를 클릭합니다.
7. 메시지가 표시되면 에이전트가 포함된 머신을 조직에 추가할지, 아니면 부서 중 하나에 추가할지 선택합니다.
   이 메시지는 사용자가 둘 이상의 부서 또는 최소 하나의 부서가 있는 조직을 관리하는 경우에 나타납니다. 그렇지 않으면 머신이 사용자가 관리하는 부서 또는 조직에 자동으로 추가됩니다. 자세한 내용은 "단위 및 관리자 계정"(584페이지) 항목을 참조하십시오.

8. 설치를 계속 진행합니다.
9. 설치가 완료되면 **닫기**를 클릭합니다.
10. Agent for Exchange를 설치한 경우 Exchange 데이터베이스를 백업할 수 있습니다. Exchange 사서함을 백업하려는 경우 Cyber Protect 웹 콘솔을 열고 **추가** > **Microsoft Exchange Server** > **Exchange 사서함**을 클릭한 다음, Microsoft Exchange Server의 **클라이언트 액세스** 서버 역할(CAS)이 활성화되어 있는 머신을 지정합니다. 자세한 내용은 "사서함 백업"(415페이지) 항목을 참조하십시오.

Agent for VMware(Windows), Agent for Office 365, Agent for Oracle 또는 Agent for Exchange를 Microsoft Exchange Server가 없는 머신에 설치하려면

1. 관리자로 로그온하고 Acronis Cyber Protect 설정 프로그램을 시작합니다.
2. [선택 사항] 설치 프로그램의 언어를 변경하려면 **언어 설정**을 클릭합니다.
3. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
4. **보호 에이전트 설치**를 선택한 다음 **설치 설정 사용자 정의**를 클릭합니다.
5. **설치할 항목** 옆에 있는 **변경**을 클릭합니다.
6. 설치할 에이전트에 해당하는 확인란을 선택합니다. 설치하지 않을 컴퍼넌트의 확인란을 선택 해제합니다. **완료**를 클릭하여 계속 진행합니다.
7. 에이전트와 함께 머신을 등록할 관리 서버를 지정합니다.
   a. **Acronis Cyber Protect Management Server** 옆에 있는 **지정**을 클릭합니다.
   b. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   c. 관리 서버 관리자 또는 등록 토큰의 자격 증명을 지정합니다.
      등록 토큰을 생성하는 방법에 대한 자세한 내용은 "1단계: 등록 토큰 생성"(166페이지)을(를) 참조하십시오.
   d. **완료**를 클릭합니다.
8. 메시지가 표시되면 에이전트가 포함된 머신을 조직에 추가할지, 아니면 부서 중 하나에 추가할지 선택합니다.
   이 메시지는 사용자가 둘 이상의 부서 또는 최소 하나의 부서가 있는 조직을 관리하는 경우에 나타납니다. 그렇지 않으면 머신이 사용자가 관리하는 부서 또는 조직에 자동으로 추가됩니다. 자세한 내용은 "단위 및 관리자 계정"(584페이지) 항목을 참조하십시오.
9. [선택 사항] "설치 설정 사용자 정의"(80페이지) 항목에 설명되어 있는 대로 기타 설치 설정을 변경합니다.
10. **설치**를 클릭하여 설치를 계속 진행합니다.
11. 설치가 완료되면 **닫기**를 클릭합니다.
12. [Agent for VMware(Windows)를 설치하는 경우에만] "이미 등록된 Agent for VMware 구성"(97페이지) 항목에 설명되어 있는 절차를 수행합니다.
13. [Agent for Exchange 설치 시에만 해당] Cyber Protect 웹 콘솔을 열고 **추가** > **Microsoft Exchange Server** > **Exchange 사서함**을 클릭한 다음, Microsoft Exchange Server의 **클라이언트 액세스** 서버 역할(CAS)이 활성화되어 있는 머신을 지정합니다. 자세한 내용은 "사서함 백업"(415페이지) 항목을 참조하십시오.

Linux에 설치

준비

1. 필요한 Linux 패키지가 머신에 설치되어 있는지 확인하십시오.
2. SUSE Linux에서 에이전트를 설치할 때는 sudo가 아닌 su를 사용해야 합니다. 이 옵션을 사용하지 않으면 Cyber Protect 웹 콘솔을 통해 에이전트 등록을 시도할 때 다음 오류가 발생합니다. 웹 브라우저를 시작하지 못했습니다. 사용 가능한 디스플레이가 없습니다.

   SUSE 등의 일부 Linux 배포판에서는 sudo 사용 시에 DISPLAY 변수가 전달되지 않으므로 인스톨러가 GUI(그래픽 사용자 인터페이스)에서 브라우저를 열 수 없습니다.

설치

Agent for Linux를 설치하려면 2GB 이상의 디스크 여유 공간이 필요합니다.

Agent for Linux를 설치하려면

1. 루트 사용자로 설치 파일(.i686 또는 .x86_64 파일)이 있는 디렉토리로 이동하여 파일을 실행 가능하도록 설정한 후에 실행합니다.

   ```
   chmod +x <installation file name>
   ```

   ```
   ./<installation file name>
   ```

2. 라이센스 계약 조건에 동의합니다.
3. 설치할 컴퍼넌트를 지정합니다.
   a. **Acronis Cyber Protect Management Server** 확인란의 선택을 해제합니다.
   b. 설치할 에이전트의 확인란을 선택합니다. 다음 에이전트를 선택할 수 있습니다.
      - **Agent for Linux**
      - **Agent for Oracle**

      Agent for Oracle을 설치하려면 Agent for Linux도 설치되어 있어야 합니다.
   c. **다음**을 클릭합니다.
4. 에이전트와 함께 머신을 등록할 관리 서버를 지정합니다.
   a. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   b. 관리 서버 관리자의 사용자 이름과 암호를 지정합니다.
   c. **다음**을 클릭합니다.
5. 메시지가 표시되면 에이전트가 포함된 머신을 조직에 추가할지, 아니면 부서 중 하나에 추가할지 선택한 다음 **Enter**를 누릅니다.

   이 메시지는 이전 단계에서 지정한 계정이 둘 이상의 부서 또는 최소 하나의 부서가 있는 조직을 관리하는 경우에 나타납니다.
6. UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 어느 비밀번호(루트 사용자의 비밀번호 또는 "acronis")를 사용해야 하는지 잘 기억해 두십시오.

참고
설치 시에는 커널 모듈 서명에 사용되는 새 키가 생성됩니다. 머신을 다시 시작하여 MOK (Machine Owner Key) 목록에 이 새 키를 등록해야 합니다. 새 키를 등록하지 않으면 에이전트가 작동하지 않습니다. 에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 에이전트를 다시 설치해야 합니다.

7. 설치가 완료되면 다음 중 하나를 수행하십시오.
   - 이전 단계에서 시스템을 다시 시작하라는 메시지가 표시된 경우 **다시 시작**을 클릭합니다. 시스템 다시 시작 중에 MOK(Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 이전 단계에서 권장된 비밀번호를 사용하여 키를 등록합니다.
   - 그렇지 않은 경우, **종료**를 클릭합니다.

문제 해결 정보가 다음 파일에 제공됩니다.
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

macOS에 설치

Agent for Mac을 설치하려면

1. 설치 파일(.dmg)을 두 번 클릭합니다.
2. 운영 체제가 설치 디스크 이미지를 마운트하는 동안 기다립니다.
3. **설치**를 두 번 클릭한 다음 **계속**을 클릭합니다.
4. [선택 사항] **설치 위치 변경**을 클릭하여 소프트웨어가 설치된 디스크를 변경합니다. 기본적으로 시스템 시작 디스크가 선택됩니다.
5. **설치**를 클릭합니다. 메시지가 표시되면 관리자의 사용자 이름과 비밀번호를 입력합니다.
6. 에이전트와 함께 머신을 등록할 관리 서버를 지정합니다.
   a. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   b. 관리 서버 관리자의 사용자 이름과 암호를 지정합니다.
   c. **등록**을 클릭합니다.
7. 메시지가 표시되면 에이전트가 포함된 머신을 조직에 추가할지, 아니면 부서 중 하나에 추가할지 선택한 다음 **완료**를 클릭합니다.
   이 메시지는 이전 단계에서 지정한 계정이 둘 이상의 부서 또는 최소 하나의 부서가 있는 조직을 관리하는 경우에 나타납니다.
8. 설치가 완료되면 **닫기**를 클릭합니다.

무인 설치 또는 제거

Windows에서 무인 설치 또는 제거

이 섹션에서는 Windows를 실행 중인 머신에서 Windows Installer(`msiexec` 프로그램)를 사용하여 Acronis Cyber Protect을(를) 무인 모드로 설치 또는 설치 제거하는 방법을 설명합니다. Active Directory 도메인에서 무인 설치를 수행하는 또 다른 방법은 그룹 정책을 사용하는 것입니다("그룹 정책을 통해 에이전트 배포"(165페이지) 참조).

설치 중에는 **변환**(.mst 파일)이라는 파일을 사용할 수 있습니다. 변환 파일은 설치 매개변수가 포함된 파일입니다. 대안으로 명령줄에서 직접 설치 매개변수를 지정해도 됩니다.

.mst 변환 생성 및 설치 패키지 추출

1. 관리자 권한으로 로그온하고 설치 프로그램을 시작합니다.
2. **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭합니다.
3. [일부 설치 프로그램에서만 사용 가능] **컴포넌트 비트**에서 **32비트** 또는 **64비트**를 선택합니다.
4. **설치 대상**에서 설치할 컴포넌트를 선택하고 **완료**를 누릅니다.
   해당 컴퍼넌트용 설치 패키지가 설정 프로그램에서 추출됩니다.
5. **Acronis Cyber Protect Management Server**에서 **자격 증명 사용** 또는 **등록 토큰 사용**을 선택합니다. 선택에 따라 자격 증명 또는 등록 토큰을 지정한 다음 **완료**를 클릭합니다.
   등록 토큰을 생성하는 방법에 대한 자세한 내용은 "1단계: 등록 토큰 생성"(166페이지)을(를) 참조하십시오.
6. [도메인 컨트롤러에 설치하는 경우에만 해당] **에이전트 서비스용 로그온 계정**에서 **다음 계정 사용**을 선택합니다. 에이전트 서비스를 실행할 사용자 계정을 지정한 다음 **완료**를 클릭합니다.
   보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

   참고
   지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다.
   이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

   읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.
7. .mst 파일에 추가될 기타 설치 설정을 검토하거나 수정한 다음, **진행**을 클릭합니다.
8. .mst 변환이 생성되고 .msi 및 .cab 설치 패키지가 추출될 폴더를 선택한 다음 **생성**을 클릭합니다.

그러면 .mst 변환이 생성되고 지정한 폴더로 .msi 및 .cab 설치 패키지가 추출됩니다.

.mst 변환을 사용하여 제품 설치

명령줄에서 다음 명령을 실행합니다.

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

위치:

- <패키지 이름>은 .msi 파일의 이름입니다. 이 이름은 운영 체제 비트에 따라 **AB.msi** 또는 **AB64.msi**입니다.
- <변환 이름>은 변환의 이름입니다. 이 이름은 운영 체제 비트에 따라 **AB.msi.mst** 또는 **AB64.msi.mst**입니다.

예: `msiexec /i AB64.msi TRANSFORMS=AB64.msi.mst`

매개변수를 수동으로 지정하여 제품 설치 또는 제거

명령줄에서 다음 명령을 실행합니다.

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

여기에서 <패키지 이름>은 .msi 파일의 이름입니다. 이 이름은 운영 체제 비트에 따라 **AB.msi** 또는 **AB64.msi**입니다.

사용 가능한 매개변수와 해당 값은 "일반 매개변수"(103페이지) 항목에 설명되어 있습니다.

예

- 관리 서버 및 원격 설치용 컴퍼넌트 설치.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,WebConsole,ComponentRegisterFeature
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 AMS_USE_SYSTEM_ACCOUNT=1
  ```

- Agent for Windows, 명령줄 도구, Cyber Protect Monitor 설치. 이전에 설치한 관리 서버에 에이전트와 함께 머신 등록.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AgentsCoreComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
  TARGETDIR="C:\Program Files\Acronis" REBOOT=ReallySuppress CURRENT_LANGUAGE=en ACEP_
  AGREEMENT=1 MMS_CREATE_NEW_ACCOUNT=1 REGISTRATION_ADDRESS=10.10.1.1
  ```

- 관리 서버, 스토리지 노드, 카탈로그 서비스 및 보호 에이전트 업데이트.

  ```
  msiexec.exe /i ab64.msi /l*v my_log.txt /qn
  ADDLOCAL=AcronisCentralizedManagementServer,BackupAndRecoveryAgent,AgentsCoreComponen
  ts,StorageServer,CatalogBrowser CATALOG_DATA_MIGRATION_PATH="C:\MyFolder\tmp"
  ```

무인 설치 또는 제거 매개변수

이 섹션에서는 Windows에서 무인 설치 또는 제거 중 사용되는 매개변수에 대해 설명합니다.

이 매개변수 외에 https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx에 설명된 대로 다른 `msiexec` 매개변수도 사용할 수 있습니다.

설치 매개변수

일반 매개변수

`ADDLOCAL=<list of components>`

설치될 컴퍼넌트는 공백 문자 없이 쉼표로 구분됩니다. 지정된 모든 컴퍼넌트가 설치 전에 설정 프로그램에서 추출되어야 합니다.

컴퍼넌트의 전체 목록은 다음과 같습니다.

구성 요소	다음 항목과 함께 설치	비트	컴퍼넌트 이름 / 설명
AcronisCentralizedManagementServer	WebConsole	32비트/64비트	Management Server
WebConsole	AcronisCentralizedManagementServer	32비트/64비트	웹 콘솔
ComponentRegisterFeature	AcronisCentralizedManagementServer	32비트/64비트	원격 설치 컴퍼넌트
AtpScanService	AcronisCentralizedManagementServer	32비트/64비트	검색 서비스
AgentsCoreComponents		32비트/64비트	에이전트용 핵심 컴퍼넌트
BackupAndRecoveryAgent	AgentsCoreComponents	32비트/64비트	Agent for Windows
ArxAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Active Directory
OracleAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Oracle
ArxOnlineAgentFeature	AgentsCoreComponents	32비트/64비트	Agent for Office 365
AcronisESXSupport	AgentsCoreComponents	32비	Agent for

		트/64 비트	VMware (Windows)
HyperVAgent	AgentsCoreComponents	32비트/64비트	Agent for Hyper-V
ESXVirtualAppliance		32비트/64비트	Agent for VMware(가상 어플라이언스)
ScaleVirtualAppliance		32비트/64비트	Agent for Scale Computing HC3(가상 어플라이언스)
CommandLineTool		32비트/64비트	명령줄 도구
TrayMonitor	BackupAndRecoveryAgent	32비트/64비트	Cyber Protect 모니터
BackupAndRecoveryBootableComponents		32비트/64비트	Bootable Media Builder
PXEServer		32비트/64비트	PXE 서버
StorageServer	BackupAndRecoveryAgent	64비트	스토리지 노드
CatalogBrowser	JRE 8 Update 111 이상	64비트	카탈로그 서비스

`TARGETDIR=<path>`

제품을 설치할 폴더.

`REBOOT=ReallySuppress`

이 매개변수가 지정되면 머신 재부팅이 금지됩니다.

`CURRENT_LANGUAGE=<language ID>`

제품 언어. 사용 가능한 값은 en, en_GB, cs, da, de, es_ES, fr, ko, it, hu, nl, ja, pl, pt, pt_BR, ru, tr, zh, zh_TW입니다.

ACEP_AGREEMENT={0,1}

이 값이 1인 경우 머신이 Acronis 고객 체험 프로그램(ACEP)에 참여합니다.

REGISTRATION_ADDRESS=<host name or IP address>:<port>

관리 서버가 설치된 머신의 호스트 이름 또는 IP주소. ADDLOCAL 매개변수에 지정된 에이전트, 스토리지 노드, 카탈로그 서비스가 이 관리 서버에 등록됩니다. 기본값(9877)과 차이가 있는 경우 포트 번호는 필수입니다.

이 매개변수를 사용할 때는 REGISTRATION_TOKEN 매개변수 또는 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수를 지정해야 합니다.

REGISTRATION_TOKEN=<token>

그룹 정책을 통해 에이전트 디플로이에 설명되어 있는 대로 Cyber Protect 웹 콘솔에 생성된 등록 토큰입니다.

REGISTRATION_LOGIN=<user name>, REGISTRATION_PASSWORD=<password>

관리 서버 관리자의 사용자 이름과 비밀번호.

REGISTRATION_TENANT=<unit ID>

조직 내 부서. ADDLOCAL 매개변수에 지정된 에이전트, 스토리지 노드, 카탈로그 서비스가 이 단위에 추가됩니다.

단위 ID를 확인하려면 Cyber Protect 웹 콘솔에서 **설정** > **계정**을 클릭하고 단위를 선택한 다음, **세부정보**를 클릭합니다.

이 매개변수는 REGISTRATION_TOKEN 또는 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 없이 작동하지 않습니다. 이 경우에는 컴퍼넌트가 조직에 추가됩니다.

이 매개변수가 없으면 컴퍼넌트는 조직에 추가됩니다.

REGISTRATION_REQUIRED={0,1}

등록에 실패한 경우의 설치 결과. 값이 1인 경우 설치에 실패합니다. 값이 0인 경우 컴퍼넌트가 등록되지 않았어도 설치가 성공적으로 완료됩니다.

REGISTRATION_CA_SYSTEM={0,1}|REGISTRATION_CA_BUNDLE={0,1}|REGISTRATION_PINNED_PUBLIC_KEY=<public key value>

이 상호 배타적인 매개변수들은 등록 중 관리 서버 인증서 검사 방법을 정의합니다. MITM 공격을 방지하기 위해 관리 서버의 진위를 검증하려면 인증서를 검사하십시오.

값이 1인 경우, 검증 시 상황에 맞게 시스템 CA를 사용하거나 제품과 함께 전달된 CA 번들을 사용합니다. 고정 공개 키가 명시된 경우, 검증 시 해당 키를 사용합니다. 값이 0인 경우 또는 매개변수가 지정되지 않은 경우에는 인증서 검증이 수행되지 않지만 등록 트래픽은 암호화된 상태로 유지됩니다.

/l*v <log file>

이 매개변수를 지정하면 자세한 정보 표시 모드의 설치 로그가 지정된 파일에 저장됩니다. 로그 파일은 설치 문제를 분석하는 데 사용될 수 있습니다.

관리 서버 설치 매개변수

`WEB_SERVER_PORT=<port number>`

관리 서버에 액세스하기 위해 웹 브라우저에서 사용할 포트. 기본값은 9877입니다.

`AMS_ZMQ_PORT=<port number>`

제품 컴퍼넌트 간 통신에 사용될 포트. 기본값은 7780입니다.

`SQL_INSTANCE=<instance>`

관리 서버가 사용할 데이터베이스. Microsoft SQL Server 2012, Microsoft SQL Server 2014 또는 Microsoft SQL Server 2016 버전을 선택할 수 있습니다. 선택한 인스턴스는 다른 프로그램에 의해서도 사용될 수 있습니다.

이 매개변수가 없으면 기본 제공 SQLite 데이터베이스가 사용됩니다.

`SQL_USER_NAME=<user name>` 및 `SQL_PASSWORD=<password>`

Microsoft SQL Server 로그인 계정 자격 증명. 관리 서버가 선택한 SQL 서버 인스턴스에 연결하기 위해 이 자격 증명을 사용합니다. 이 매개변수가 없으면 관리 서버는 관리 서버 서비스 계정(**AMS User**)의 자격 증명을 사용합니다.

관리 서버 서비스를 실행할 계정

다음 매개변수 중 하나를 지정합니다.

- `AMS_USE_SYSTEM_ACCOUNT={0,1}`
  값이 1인 경우 시스템 계정이 사용됩니다.
- `AMS_CREATE_NEW_ACCOUNT={0,1}`
  값이 1인 경우 새 계정이 생성됩니다.
- `AMS_SERVICE_USERNAME=<user name>` 및 `AMS_SERVICE_PASSWORD=<password>`
  지정된 계정이 사용됩니다.

에이전트 설치 매개변수

`HTTP_PROXY_ADDRESS=<IP address>` 및 `HTTP_PROXY_PORT=<port>`

에이전트가 사용하는 HTTP 프록시 서버. 이 매개변수가 없으면 프록시 서버가 사용되지 않습니다.

`HTTP_PROXY_LOGIN=<login>` 및 `HTTP_PROXY_PASSWORD=<password>`

HTTP 프록시 서버의 자격 증명. 서버에 인증이 필요한 경우 이 매개변수를 사용합니다.

`HTTP_PROXY_ONLINE_BACKUP={0,1}`

값이 0인 경우 또는 매개변수가 지정되지 않은 경우에는 에이전트가 클라우드에서의 백업 및 복구에만 프록시 서버를 사용합니다. 또한, 값이 1인 경우에는 에이전트가 프록시 서버를 통해 관리 서버에 연결합니다.

SET_ESX_SERVER={0,1}

값이 0인 경우, 설치 중인 Agent for VMware가 vCenter Server 또는 ESXi 호스트에 연결되지 않습니다. 설치 후 "이미 등록된 Agent for VMware 구성"에 설명된 대로 진행합니다.

값이 1인 경우, 다음 매개변수를 지정합니다.

ESX_HOST=<host name or IP address>

vCenter Server 또는 ESXi 호스트의 호스트 이름 또는 IP 주소.

ESX_USER=<user name> 및 ESX_PASSWORD=<password>

vCenter Server 또는 ESXi 호스트에 액세스하기 위한 자격 증명.

에이전트 서비스가 실행될 계정

다음 매개변수 중 하나를 지정합니다.

- MMS_USE_SYSTEM_ACCOUNT={0,1}
  값이 1인 경우 시스템 계정이 사용됩니다.
- MMS_CREATE_NEW_ACCOUNT={0,1}
  값이 1인 경우 새 계정이 생성됩니다.
- MMS_SERVICE_USERNAME=<user name> 및 MMS_SERVICE_PASSWORD=<password>
  지정된 계정이 사용됩니다.

스토리지 노드 설치 매개변수

스토리지 노드 서비스를 실행할 계정

다음 매개변수 중 하나를 지정합니다.

- ASN_USE_SYSTEM_ACCOUNT={0,1}
  값이 1인 경우 시스템 계정이 사용됩니다.
- ASN_CREATE_NEW_ACCOUNT={0,1}
  값이 1인 경우 새 계정이 생성됩니다.
- ASN_SERVICE_USERNAME=<user name> 및 ASN_SERVICE_PASSWORD=<password>
  지정된 계정이 사용됩니다.

카탈로그 서비스 설치 매개변수

CATALOG_DATA_MIGRATION_PATH=<path>

이 매개변수는 Acronis Cyber Protect 15 Update 4에서 카탈로그 데이터를 새 버전의 카탈로그 서비스로 마이그레이션할 때 사용합니다. 카탈로그 데이터를 내보낼 임시 폴더의 경로를 지정합니다.

`SKIP_CATALOG_DATA_MIGRATION=1`

카탈로그 데이터 마이그레이션을 건너뛰려면 이 매개변수를 사용합니다.

`SKIP_CATALOG_DATA_MIGRATION` 및 `CATALOG_DATA_MIGRATION_PATH` 매개변수는 상호 배타적입니다.

제거 매개변수

`REMOVE={<list of components>|ALL}`

제거될 컴퍼넌트는 공백 문자 없이 쉼표로 구분됩니다.

사용 가능한 컴퍼넌트는 이 섹션 앞부분에 설명되어 있습니다.

값이 `ALL`인 경우 모든 제품 컴퍼넌트가 제거됩니다. 추가로 다음 매개변수를 지정할 수 있습니다.

`DELETE_ALL_SETTINGS={0, 1}`

값이 1인 경우 제품의 로그, 작업 및 구성 설정이 제거됩니다.

Linux에서 무인 설치 또는 제거

이 섹션에서는 Linux를 실행 중인 머신에서 명령줄을 사용하여 Acronis Cyber Protect을(를) 무인 모드로 설치 또는 설치 제거하는 방법을 설명합니다.

제품을 설치 또는 제거하려면

1. 터미널을 엽니다.
2. 다음 명령을 실행합니다.

   ```
   <package name> -a <parameter 1> ... <parameter N>
   ```

   여기서, <패키지 이름>은 설치 패키지(.i686 또는 .x86_64 파일)의 이름입니다.
3. [Agent for Linux 설치에만 해당] UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 어느 비밀번호(루트 사용자의 비밀번호 또는 "acronis")를 사용해야 하는지 잘 기억해 두십시오. 시스템 다시 시작 중에 MOK (Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 권장 비밀번호를 사용하여 키를 등록합니다.

에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 3단계를 포함하는 설치를 반복하십시오. 그렇지 않으면 백업에 실패하게 됩니다.

설치 매개변수

일반 매개변수

`{-i |--id=}<list of components>`

설치될 컴퍼넌트는 공백 문자 없이 쉼표로 구분됩니다.

다음 컴퍼넌트를 설치할 수 있습니다.

구성 요소	컴퍼넌트 설명
AcronisCentralizedManagementServer	Management Server
BackupAndRecoveryAgent	Agent for Linux
BackupAndRecoveryBootableComponents	Bootable Media Builder

이 매개변수가 없으면 위의 모든 컴퍼넌트가 설치됩니다.

`--language=<language ID>`

제품 언어. 사용 가능한 값은 `en`, `en_GB`, `cs`, `da`, `de`, `es_ES`, `fr`, `ko`, `it`, `hu`, `nl`, `ja`, `pl`, `pt`, `pt_BR`, `ru`, `tr`, `zh`, `zh_TW`입니다.

`{-d|--debug}`

이 매개변수를 지정하면 자세한 정보 표시 모드로 설치 로그가 작성됩니다. 로그는 파일 **/var/log/trueimage-setup.log**에 있습니다.

`{-t|--strict}`

이 매개변수를 지정하면 설치 중 발생하는 모든 경고가 설치 실패로 이어집니다. 이 매개변수가 없으면 경고가 발생하더라도 설치가 성공적으로 완료됩니다.

`{-n|--nodeps}`

이 매개변수가 지정되면 설치 중에 필요한 Linux 패키지가 없어도 무시됩니다.

관리 서버 설치 매개변수

`{-W |--web-server-port=}<port number>`

관리 서버에 액세스하기 위해 웹 브라우저에서 사용할 포트. 기본값은 9877입니다.

`--ams-tcp-port=<port number>`

제품 컴퍼넌트 간 통신에 사용될 포트. 기본값은 7780입니다.

에이전트 설치 매개변수

다음 매개변수 중 하나를 지정합니다.

- `--skip-registration`
  - 관리 서버에 에이전트를 등록하지 않습니다.
- `{-C |--ams=}<host name or IP address>`
  - 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소. 에이전트가 이 관리 서버에 등록됩니다.

명령 하나로 에이전트와 관리 서버를 설치하는 경우 `-C` 매개변수에 상관없이 에이전트가 이 관리 서버에 등록됩니다.

이 매개변수를 사용할 때는 `token` 매개변수 또는 `login` 및 `password` 매개변수를 지정해야 합니다.

`--token=<token>`

그룹 정책을 통해 에이전트 디플로이에 설명되어 있는 대로 Cyber Protect 웹 콘솔에 생성된 등록 토큰입니다.

`{-g |--login=}<user name>` 및 `{-w |--password=}<password>`

관리 서버 관리자의 자격 증명.

`--unit=<unit ID>`

조직 내 부서. 에이전트가 이 부서에 추가됩니다.

단위 ID를 확인하려면 Cyber Protect 웹 콘솔에서 **설정** > **계정**을 클릭하고 단위를 선택한 다음, **세부정보**를 클릭합니다.

이 매개변수가 없으면 에이전트가 조직에 추가됩니다.

`--reg-transport={https|https-ca-system|https-ca-bundle|https-pinned-public-key}`

등록 시 관리 서버 인증서 검사 방법. MITM 공격을 방지하기 위해 관리 서버의 진위를 검증하려면 인증서를 검사하십시오.

값이 `https`인 경우 또는 매개변수가 지정되지 않은 경우에는 인증서 검사가 수행되지 않지만 등록 트래픽은 암호화된 상태로 유지됩니다. 값이 `https`가 *아닌* 경우, 검사 시 시스템 CA를 사용하고, 아니면 상황에 따라 제품과 함께 전달된 CA 번들 또는 고정 공개 키를 사용합니다.

`--reg-transport-pinned-public-key=<public key value>`

고정 공개 키 값. 이 매개변수를 `--reg-transport=https-pinned-public-key` 매개변수와 함께, 또는 이를 대신해 지정해야 합니다.

- `--http-proxy-host=<IP address>` 및 `--http-proxy-port=<port>`
  - 에이전트가 클라우드에 백업하고 여기에서 복구할 때, 그리고 관리 서버에 연결할 때 사용하는 HTTP 프록시 서버. 이 매개변수가 없으면 프록시 서버가 사용되지 않습니다.
- `--http-proxy-login=<login>` 및 `--http-proxy-password=<password>`
  - HTTP 프록시 서버의 자격 증명. 서버에 인증이 필요한 경우 이 매개변수를 사용합니다.
- `--no-proxy-to-ams`
  - 보호 에이전트는 `--http-proxy-host` 및 `--http-proxy-port` 매개변수로 지정된 프록시 서버를 사용하지 않고도 관리 서버에 연결합니다.

제거 매개변수

`{-u|--uninstall}`

제품을 제거합니다.

`--purge`

제품 로그, 작업 및 구성 설정을 제거합니다.

정보 매개변수

`{-?|--help}`

매개변수 설명이 표시됩니다.

`--usage`

명령의 용도에 대한 간략한 설명이 표시됩니다.

`{-v|--version}`

설치 패키지 버전을 표시합니다.

`--product-info`

제품 이름 및 설치 패키지 버전을 표시합니다.

예

- 관리 서버 설치.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer
```

- 관리 서버를 설치하고, 사용자 정의 포트 지정.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i AcronisCentralizedManagementServer --
web-server-port 6543 --ams-tcp-port 8123
```

- Agent for Linux를 설치하고, 지정된 관리 서버에 등록.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456
```

- Agent for Linux를 설치하고, 지정된 관리 서버의 지정된 부서에 등록.

```
./AcronisCyberProtect_15_64-bit.x86_64 -a -i BackupAndRecoveryAgent --ams 10.10.1.1 -
-login root --password 123456 -unit 01234567-89AB-CDEF-0123-456789ABCDEF
```

macOS에서 무인 설치 또는 제거

이 섹션에서는 macOS를 실행 중인 머신에서 명령줄을 사용하여 Protection 에이전트를 무인 모드로 설치, 등록 및 설치 제거하는 방법에 대해 설명합니다. 설치 파일(.dmg)을 다운로드하는 방법은 "macOS를 실행하는 머신 추가"를 참조하십시오.

Agent for Mac을 설치하려면

1. 설치 파일(.dmg)을 마운트할 임시 디렉토리를 생성합니다.

   ```
   mkdir <dmg_root>
   ```

   여기에서 `<dmg_root>`은(는) 사용자가 선택한 이름입니다.

2. .dmg 파일을 마운트합니다.

```
hdiutil attach <dmg_file> -mountpoint <dmg_root>
```

여기에서 <dmg_file>은(는) 설치 파일의 이름입니다. 예를 들어 다음과 같습니다. **AcronisCyberProtect_15_MAC.dmg**.

3. 인스톨러를 실행합니다.

```
sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
```

4. 설치 파일(.dmg)을 분리합니다.

```
hdiutil detach <dmg_root>
```

예

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisCyberProtect_15_MAC.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```

Agent for Mac을 등록하려면

다음 중 하나를 수행하십시오.

- 특정 관리자 계정에 에이전트를 등록합니다.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
  <management server address:port> -u <user name> -p <password>
  ```

  <관리 서버 주소:포트>는 Acronis Cyber Protect Management Server가 설치된 머신의 호스트 이름 또는 IP 주소입니다. 기본값(9877)과 차이가 있는 경우 포트 번호는 필수입니다.

  <사용자 이름> 및 <암호>는 에이전트를 등록하는 관리자 계정의 자격 증명입니다.

- 특정 단위에 에이전트를 등록합니다.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent  -o register -a
  <management server address:port> -u <user name> -p <password> --tenant <unit ID>
  ```

  단위 ID를 확인하려면 Cyber Protect 웹 콘솔에서 **설정** > **계정**을 클릭하고 원하는 단위를 선택한 다음, **세부정보**를 클릭합니다.
  ```

중요
관리자는 단위 ID를 해당 조직 계층 수준에서만 지정하여 에이전트를 등록할 수 있습니다. 부서 관리자는 자신의 부서 및 해당 하위 부서에서 머신을 등록할 수 있습니다. 조직 관리자는 모든 부서에서 머신을 등록할 수 있습니다. 여러 관리자 계정에 대한 자세한 내용은 "사용자 계정 및 조직 부서 관리"를 참조하십시오.

- 등록 토큰을 이용하여 에이전트를 등록합니다.

```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
<management server address:port> --token <token>
```

등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. "그룹 정책을 통해 에이전트 디플로이"에 설명되어 있는 대로 Cyber Protect 웹 콘솔에서 생성할 수 있습니다.

중요
macOS 10.14 이상 버전에서는 보호 에이전트에 전체 디스크 액세스 권한을 부여해야 합니다. 이렇게 하려면 **애플리케이션 >유틸리티**로 이동한 다음 **Cyber Protect 에이전트 지원**을 실행하십시오. 그런 다음 애플리케이션 창의 지침을 따릅니다.

예

사용자 이름 및 패스워드로 등록.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

부서 ID 및 관리자 자격 증명으로 등록.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 4dd941c1-c03f-11ea-
86d8-005056bdd3a0
```

토큰으로 등록.

-
```
sudo /Library/Application\
Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -a
https://10.250.144.179:9877 --token D91D-DC46-4F0B
```

Agent for Mac을 제거하려면

다음 명령을 실행합니다.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

Agent for Mac 및 로그, 작업, 구성 설정까지 모두 제거하려면 다음 명령을 실행합니다.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

수동으로 머신 등록

에이전트 설치 중 Cyber Protect 관리 서버에서 머신을 등록하는 것 이외에 명령줄 인터페이스를 사용하여 등록할 수도 있습니다. 에이전트를 설치했지만 자동 등록에 실패한 경우, 또는 새 계정에서 기존 머신을 등록하려는 경우 이 방법을 사용해야 할 수 있습니다.

머신을 등록하려면

에이전트가 설치된 머신의 명령 프롬프트에서 다음 명령 중 하나를 실행합니다.

- 특정 관리자 계정에 머신을 등록하는 방법:

  ```
  <path to the registration tool> -o register -a <management server address:port> -u
  <user name> -p <password>
  ```

  여기서 <등록 도구 경로>는 다음과 같습니다.
  - Windows: `%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe`
  - Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
  - macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`

  <관리 서버 주소:포트>는 Acronis Cyber Protect Management Server가 설치된 머신의 호스트 이름 또는 IP 주소입니다. 기본 포트 9877을 사용하는 경우 명시적으로 지정할 필요는 없습니다.

  <사용자 이름> 및 <암호>는 에이전트를 등록하는 관리자 계정의 자격 증명입니다.
- 특정 부서에 머신을 등록하려면 부서 ID를 지정합니다.

  ```
  <path to the registration tool> -o register -a <management server address:port> u
  <user name> -p <password> --tenant <unit ID>
  ```

  단위 ID를 확인하려면 Cyber Protect 웹 콘솔에서 **설정** > **계정**을 클릭하고 원하는 단위를 선택한 다음, **세부정보**를 클릭합니다.

  중요
  관리자는 해당 조직 계층 수준에서만 에이전트를 등록할 수 있습니다. 부서 관리자는 자신의 부서 및 해당 하위 부서에서 에이전트를 등록할 수 있습니다. 조직 관리자는 모든 부서에서 에이전트를 등록할 수 있습니다. 여러 관리자 계정에 대한 자세한 내용은 "사용자 계정 및 조직 부서 관리"를 참조하십시오.

- 등록 토큰을 사용하여 머신을 등록하는 방법:

```
<path to the registration tool> -o register -a <management server address:port> --
token <token>
```

- 등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. 생성 방법에 대한 자세한 내용은 "그룹 정책을 통해 에이전트 디플로이"를 참조하십시오.

머신 등록을 취소하려면

에이전트가 설치된 머신의 명령 프롬프트에서 다음 명령을 실행합니다.

```
<path to the registration tool> -o unregister
```

예

Windows

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\Acronis\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 --tenant 590b1dd7-8adb-11ea-bf44-0050569deecf
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -a
https://10.250.144.179:9877 -u johndoe -p johnspassword --tenant 590b1dd7-8adb-11ea-
bf44-0050569deecf
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -a https://10.250.144.179:9877 --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

특수 문자 또는 공백이 포함된 비밀번호

패스워드에 특수 문자나 공백이 포함된 경우, 명령줄에 입력할 때 처음과 끝에 인용 부호를 포함하십시오.

```
<path to the registration tool> -o register -a <management server address:port> -u <user
name> -p <"password">
```

예 (Windows용):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -p "johns password"
```

여전히 오류가 발생하는 경우:

1. https://www.base64encode.org/에서 비밀번호를 base64 형식으로 암호화합니다.
2. 명령줄에서 -b 또는 --base64 매개변수를 사용하여 암호화된 비밀번호를 지정합니다.

예 (Windows용):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -a
https://10.250.144.179:9877 -u johndoe -b -p am9obnNwYXNzd29yZA==
```

소프트웨어 업데이트 확인

이 기능은 조직 관리자만 사용할 수 있습니다.

Cyber Protect 웹 콘솔에 로그인할 때마다 Acronis Cyber Protect이(가) Acronis 웹 사이트에서 새로운 버전이 제공되는지 여부를 확인합니다. 제공되는 경우 Cyber Protect 웹 콘솔의 각 페이지 아래쪽에 있는 **장치**, **계획** 및 **백업 스토리지** 탭 아래에 새 버전의 다운로드 링크가 표시됩니다. 링크는 **설정** > **에이전트** 페이지에도 표시됩니다.

업데이트 자동 확인을 활성화하거나 비활성화하려면 **업데이트** 시스템 설정을 변경합니다.

업데이트를 수동으로 확인하려면 오른쪽 상단의 물음표 아이콘 > **정보** > **업데이트 확인**을 클릭하거나 물음표 아이콘 > **업데이트 확인**을 클릭합니다.

관리 서버 마이그레이션

Windows 머신에서 실행 중인 관리 서버를 동일 환경의 다른 Windows 머신으로 마이그레이션할 수 있습니다.

마이그레이션 프로세스에서는 다음 단계를 수행합니다.

1. "원본 머신에서 작업"(118페이지)
   이 단계에서는 마이그레이션을 진행할 수 있도록 원래 관리 서버의 데이터를 준비합니다.
2. "대상 머신에서 작업"(120페이지)
   이 단계에서는 새 관리 서버를 설치 및 구성한 후 원래 관리 서버에서 새 관리 서버로 데이터를 복사합니다.

사전 요구 사항

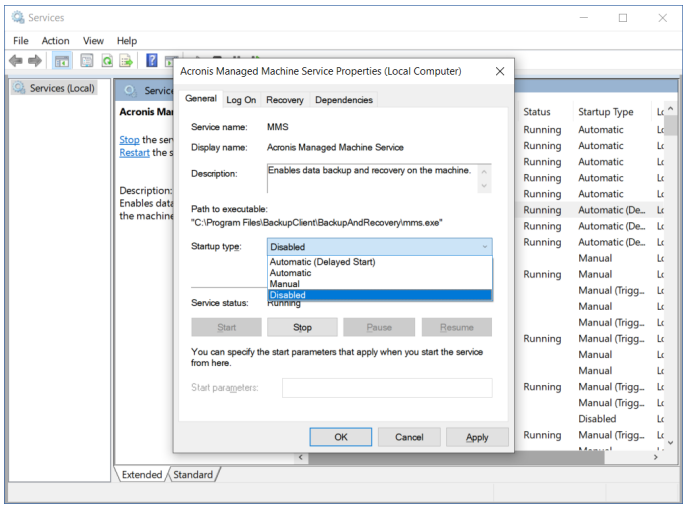
- 관리 서버가 외부 Microsoft SQL Server 데이터베이스를 사용해야 합니다. 전용 머신에서 Microsoft SQL Server 인스턴스를 실행 중이어야 합니다.
- 보호 에이전트가 관리 서버의 IP 주소가 아닌 호스트 이름을 사용하여 관리 서버에 등록되어 있어야 합니다.
- 관리 서버의 버전이 Acronis Cyber Protect 업데이트 4(빌드 29486) 이상이어야 합니다.
- 소스 머신과 대상 머신에 같은 버전의 관리 서버가 설치되어 있어야 합니다.

원본 머신에서 작업

이 단계에서는 마이그레이션을 진행할 수 있도록 원래 관리 서버에서 데이터를 준비합니다.

마이그레이션을 위한 데이터를 준비하려면

1. 원래 관리 서버 머신에서 모든 Acronis 서비스를 중지합니다.
   a. **서비스**를 열고 **Acronis Active Protection 서비스** 및 **Acronis Cyber Protect 서비스**를 제외한 Acronis 서비스 시작을 비활성화합니다.



b. **Regedit**를 열고 **Acronis Active Protection** 서비스 및 **Acronis Cyber Protect** 서비스의 키를 편집하여 해당 서비스를 비활성화합니다.

- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisCyberProtectionService` 키에서 **시작** 값을 열고 값 데이터를 4로 설정합니다.
- `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\AcronisActiveProtectionService` 키에서 **시작** 값을 열고 값 데이터를 4로 설정합니다.

2. 관리 서버 머신을 다시 시작한 후 비활성화된 Acronis 서비스가 실행되지 않음을 확인합니다.

참고
Acronis Scheduler Service Helper 및 **Acronis TIB Mounter Monitor**의 2개 서비스는 계속 실행 중일 수도 있습니다. 이 두 서비스는 무시해도 됩니다.

3. [관리 서버 머신에 Cyber Protect Monitor 컴포넌트가 설치되어 있는 경우] Acronis Cyber Protect Monitor를 종료합니다.
4. Windows 명령 프롬프트에서 다음 명령을 실행하여 `%ProgramData%\Acronis` 및 `%ProgramFiles%\Acronis` 폴더의 소유자를 변경합니다.

```
takeown /f "%ProgramData%\Acronis" /r /d y
```

```
takeown /f "%ProgramFiles%\Acronis" /r /d y
```

5. 다음 명령을 실행하여 이 두 폴더 및 해당 하위 폴더의 액세스 권한을 편집합니다.

```
icacls "%ProgramData%\Acronis" /grant everyone:F /t
```

```
icacls "%ProgramFiles%\Acronis" /grant everyone:F /t
```

6. 새 관리 서버 머신이 액세스할 수 있는 네트워크 공유에 `%ProgramData%\Acronis` 및 `%ProgramFiles%\Acronis` 폴더를 복사합니다.
7. 원래 관리 서버 머신을 종료합니다.

그런 다음 "대상 머신에서 작업"(120페이지)의 절차를 진행합니다.

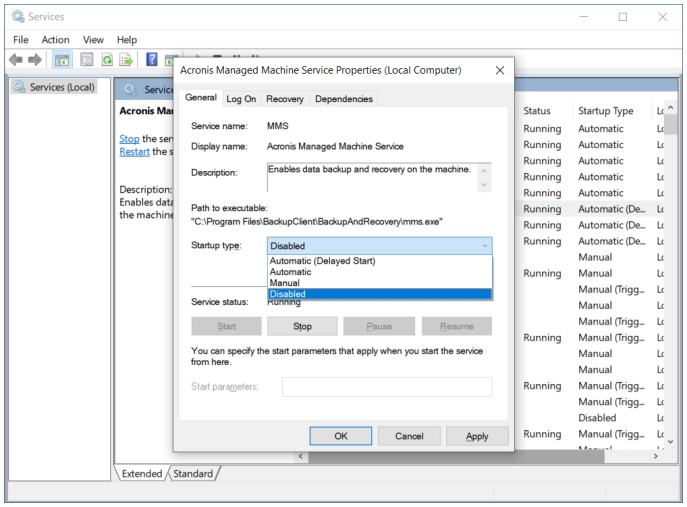
대상 머신에서 작업

이 단계에서는 새 관리 서버를 설치 및 구성한 후 해당 관리 서버로 데이터를 마이그레이션합니다.

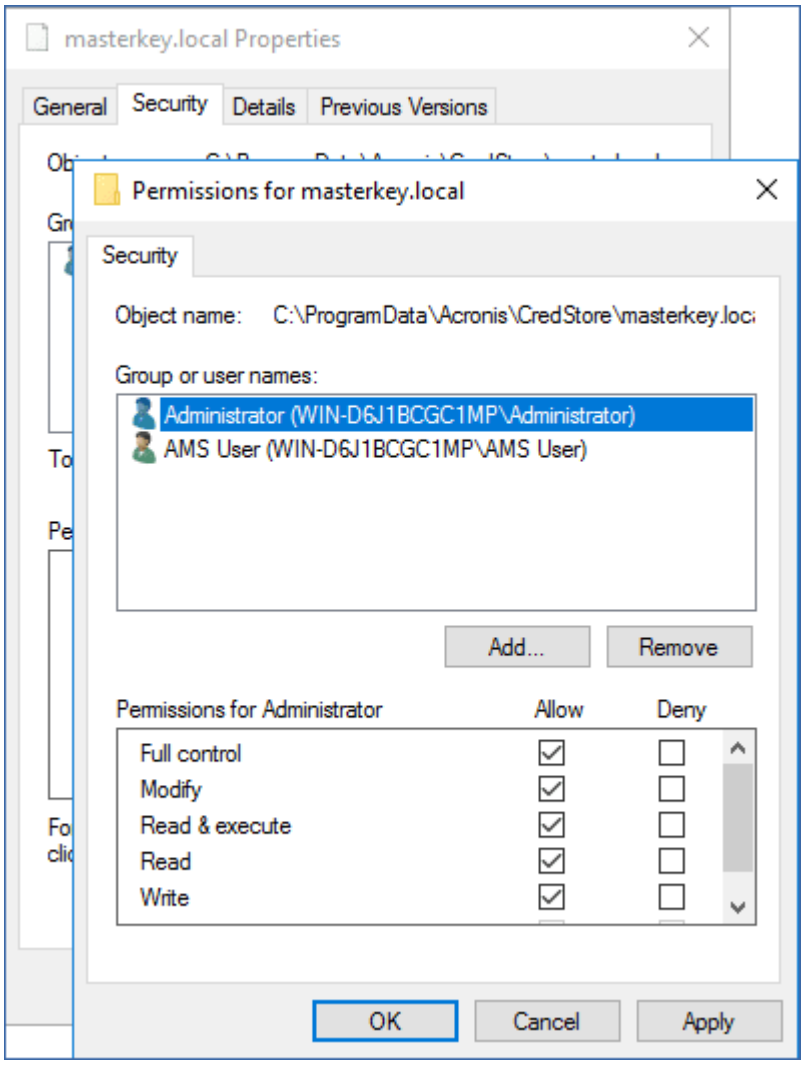
대상 머신에서 작업을 수행하기 전에 "원본 머신에서 작업"(118페이지)의 절차를 완료했는지 확인하십시오.

새 관리 서버로 데이터를 마이그레이션하려면

1. 새 관리 서버를 설치할 머신의 호스트 이름을 설정합니다. 원래 관리 서버가 설치되어 있는 머신의 이름과 같은 이름을 설정해야 합니다.
2. TCP 포트 9877에서 모든 트래픽을 차단하는 방화벽 규칙을 생성합니다.
3. Acronis Cyber Protect 설치 프로그램을 실행합니다.
   a. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
   b. **설치 설정 사용자 정의**를 클릭합니다.
   c. **설치 대상**에서 다음 컴포넌트만 선택하고 **완료**를 클릭합니다.
      - Management Server
      - 원격 설치 컴퍼넌트
      - Bootable Media Builder
      - 명령줄 도구
   d. **관리 서버용 데이터베이스**에서 기본 옵션인 **기본 제공 SQLite 사용**을 선택된 상태로 유지합니다.
   e. **관리 서버 서비스용 로그온 계정**에서는 원래 관리 서버와 같은 옵션을 사용합니다.
4. 모든 Acronis 서비스를 중지합니다.
   a. **서비스**를 열고 모든 Acronis 서비스 시작을 비활성화합니다.



   b. 머신을 다시 시작한 후 비활성화된 Acronis 서비스가 실행되지 않음을 확인합니다.
5. `%ProgramData%\Acronis\CredStore`로 이동한 후 `masterkey.local` 파일에 대한 권한을 다음과 같이 조정합니다.
   a. **Administrator**사용자 계정에 파일 소유권을 부여합니다.
   b. **Administrator**사용자 계정에 **완전한 제어** 권한을 부여합니다.



6. `%ProgramData%\Acronis\AMS\AccessVault\config`로 이동한 후 다음 파일에 대한 **완전한 제어** 권한을 **Administrator**사용자 계정에 부여합니다.
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred`
   - `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json`
7. 다음 폴더를 원래 관리 서버 머신에서 네트워크 공유로 복사한 폴더로 대체합니다.
   - `%ProgramData%\Acronis`
   - `%ProgramFiles%\Acronis`

   중요
   기존 폴더를 먼저 삭제하지 않고 덮어써야 합니다.

   참고
   `%ProgramFiles%\Acronis\ShellExtentions` 폴더를 대체할 수 없다는 메시지가 표시되면 해당 폴더는 건너뛰어도 됩니다.

8. 다음 파일에 대한 권한을 복원합니다.

- `%ProgramData%\Acronis\CredStore\masterkey.local` – 권한이 있는 사용자 목록에서 **Administrator** 사용자 계정을 제거합니다.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred` – **Administrator** 사용자 계정에 **읽기** 권한만 부여합니다.
- `%ProgramData%\Acronis\AMS\AccessVault\config\preferred.json` – **Administrator** 사용자 계정에 **읽기** 권한만 부여합니다.

9. `NGMP\latest` 폴더의 디렉토리 연결을 생성합니다.
   - Windows 명령 프롬프트에서 `%ProgramData%\Acronis\NGMP`로 이동하여 `latest` 폴더를 삭제합니다.

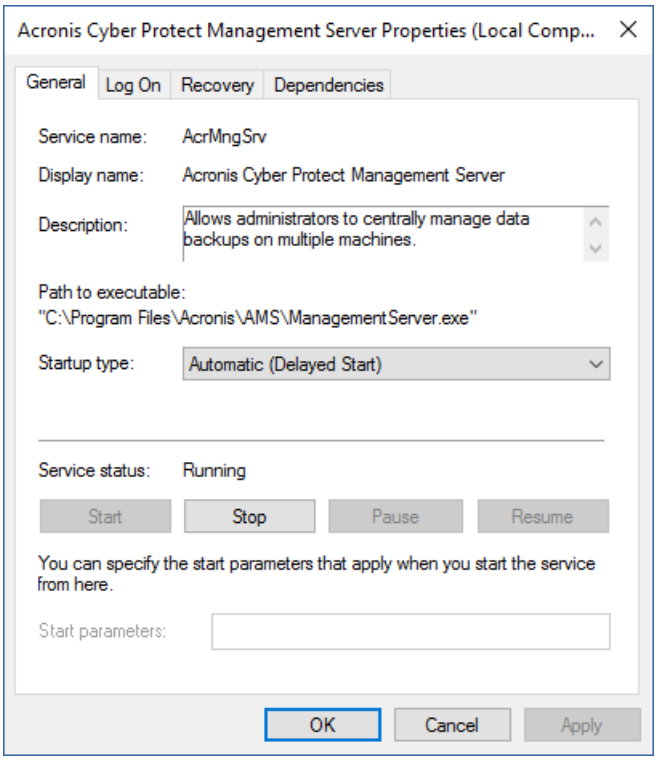
     ```
     cd %ProgramData%\Acronis\NGMP
     ```

     ```
     rmdir latest
     ```

   - 디렉토리 연결 `latest`를 생성한 후 다음과 같이 현재 NGMP 버전에 해당하는 이름이 지정된 폴더를 가리키도록 설정합니다.

     ```
     mklink /j latest C:\ProgramData\Acronis\NGMP\1.0.2653.0
     ```

10. 새 관리 서버가 원래 관리 서버에서 사용했던 Microsoft SQL Server 데이터베이스를 가리키도록 설정합니다.
    a. **Regedit**를 엽니다.
    b. `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\AMS\Settings` 키에서 `AmsDmlDbProtocol` 값을 수정합니다. 이렇게 하려면 해당 데이터를 `config://C:\ProgramData\Acronis\AMS\mssql\dml_mssql.config`로 변경합니다.
11. **서비스**를 열고 비활성화되어 있는 모든 Acronis 서비스를 활성화합니다.
    Acronis Cyber Protect Management Server의 시작 유형을 **자동(지연된 시작)**으로 설정하고, 기타 모든 Acronis 서비스의 시작 유형은 **자동**으로 설정합니다.



12. 방화벽에서 TCP 포트 9877의 모든 트래픽을 허용합니다.
13. 머신을 다시 시작한 후 모든 Acronis 서비스가 실행되고 있음을 확인합니다.
14. Acronis Cyber Protect 설치 프로그램을 실행하여 다음 항목을 설치합니다.
    - Agent for Windows
    - [선택 사항] Cyber Protect 모니터
15. 머신을 다시 시작합니다.

클라우드 디플로이

계정 활성화

관리자가 사용자를 위해 계정을 생성한 경우 사용자의 이메일 주소로 이메일 메시지가 전송됩니다. 이 메시지에는 다음과 같은 정보가 포함되어 있습니다.

- **계정 활성화 링크.** 이 링크를 클릭하여 계정의 패스워드를 설정합니다. 계정 활성화 페이지에 표시된 로그인 정보를 기억해 둡니다.
- **Cyber Protect 웹 콘솔 로그인 페이지 링크** 이후에 이 링크를 사용하여 콘솔에 액세스합니다. 로그인 및 패스워드는 이전 단계와 동일합니다.

준비

1단계

백업하려는 항목에 따라 에이전트를 선택합니다. 에이전트에 대한 정보는 "컴퍼넌트"(46페이지) 항목을 참조하십시오.

2단계

설치 프로그램을 다운로드합니다. 다운로드 링크를 찾으려면 **모든 장치** > **추가**를 클릭합니다.

장치 추가 페이지는 Windows에 설치된 각 에이전트에 대한 웹 인스톨러를 제공합니다. 웹 인스톨러는 인터넷에서 주 설치 프로그램을 다운로드하여 임시 파일에 저장하는 작은 실행 파일입니다. 이 파일은 설치 후 즉시 삭제됩니다.

설치 프로그램을 로컬에 저장하려면 **장치 추가** 페이지 맨 아래에 있는 링크를 사용하여 Windows에 설치하는 데 필요한 모든 에이전트가 포함된 패키지를 다운로드합니다. 32비트 및 64비트 패키지를 둘 다 다운로드할 수 있습니다. 이 패키지에서는 설치할 컴퍼넌트 목록을 사용자 정의할 수 있습니다. 또한 이 패키지는 예를 들어 그룹 정책을 통해 무인 설치를 가능하게 합니다. 이 고급 시나리오는 "그룹 정책을 통해 에이전트 배포"(165페이지)에 설명되어 있습니다.

Agent for Office 365 설치 프로그램을 다운로드하려면 오른쪽 위에 있는 계정 아이콘을 클릭하고 **다운로드** > **Agent for Office 365**를 클릭합니다.

Linux 및 macOS에 설치는 일반적인 설치 프로그램에서 수행됩니다.

머신을 사이버 보호 서비스에 등록하려면 모든 설치 프로그램에 인터넷 연결이 필요합니다. 인터넷에 연결되어 있지 않으면 설치에 실패합니다.

3단계

설치하기 전에 방화벽 및 네트워크 보안 시스템(예: 프록시 서버)의 다른 컴퍼넌트 둘 다가 다음 TCP 포트를 통한 인바운드 및 아웃바운드 연결을 허용하는지 확인합니다.

- 포트 **443** 및 **8443**

  이러한 포트는 Cyber Protect 웹 콘솔에 액세스하고, 에이전트를 등록하고, 인증서 및 사용자 권한을 다운로드하고, 클라우드 스토리지에서 파일을 다운로드하는 데 사용됩니다.
- **7770** – **7800** 범위의 포트

  에이전트에서는 이러한 포트를 사용하여 관리 서버와 통신합니다.
- 포트 **44445** 및 **55556**

  에이전트에서는 백업 및 복구 중 데이터 전송에 이러한 포트를 사용합니다.

네트워크에서 프록시 서버가 활성화되어 있으면 "프록시 서버 설정"(125페이지)을(를) 참조해 보호 에이전트를 실행하는 각 머신에서 프록시 서버 설정을 구성해야 하는지 파악합니다.

클라우드에서 에이전트를 관리하는데 필요한 최소 인터넷 연결 속도는 1Mbit/s입니다(클라우드 백업에 인정되는 데이터 전송 속도와 혼동해서는 안 됩니다). ADSL과 같은 저대역폭 연결 기술을 사용할 경우에는 이 점을 고려합니다.

TCP 포트는 VMware 가상 머신을 백업하고 복제하는 데 필요합니다.

- 포트 **443**

  Agent for VMware(Windows 및 가상 어플라이언스 모두 해당)는 ESXi 호스트/vCenter 서버의 이 포트에 연결되어 백업 및 복구, VM 복제 작업 도중 VSphere에서 VM을 생성하고 업데이트하고 삭제하는 등의 VM 관리 작업을 수행합니다.

- 포트 **902**

  Agent for VMware(Windows 및 가상 어플라이언스 모두 해당)는 ESXi 호스트의 이 포트에 연결되어 백업, 복구, VM 복제 작업 도중 VM 디스크에서 데이크를 읽고 쓸 수 있도록 NFC 연결을 구축합니다.
- 포트 **3333**

  Agent for VMware(가상 어플라이언스)가 VM 복제 대상인 ESXi 호스트/클러스터에서 구동 중인 경우 VM 복제 트래픽은 포트 **902**의 ESXi 호스트로 직접 전달되지 않습니다. 그 대신 해당 트래픽은 소스인 Agent for VMware에서 대상 ESXi 호스트/클러스터에 위치한 Agent for VMware(가상 어플라이언스)에 있는 TCP 포트 **3333**으로 전달됩니다.

  원본 VM 디스크에서 데이터를 읽는 소스 Agent for VMware는 이외 어디에든 존재할 수 있으며 가상 어플라이언스 또는 Windows 유형일 수 있습니다.

  대상 Agent for VMware(가상 어플라이언스)에서 VM 복제 데이터를 허용하도록 담당하는 서비스는 "복제본 디스크 서버"라고 불립니다. 이러한 서비스는 복제본 시딩을 비롯해 VM 복제 작업 도중의 트래픽 압축과 중복 제거 등 WAN 최적화 기술을 담당합니다(초기 복제본 시딩 참조). 대상 ESXi 호스트에서 구동 중인 Agent for VMware(가상 어플라이언스)가 없는 경우 이러한 서비스를 사용할 수 없으며, 이로 인해 복제본 시딩 시나리오도 지원되지 않습니다.

4단계

Protection 에이전트를 설치하려는 머신에서 다음 로컬 포트를 다른 프로세스가 사용하지 않는지 확인합니다.

- 127.0.0.1:**9999**
- 127.0.0.1:**43234**
- 127.0.0.1:**9850**

참고
방화벽에서 해당 로컬 포트를 열 필요가 없습니다.

Active Protection 서비스가 TCP 포트 **6109**에서 수신 대기합니다. 다른 프로세스에서 사용되고 있지 않은지 확인하십시오.

Protection 에이전트가 사용하는 포트 변경

Protection 에이전트가 필요로 하는 일부 포트를 환경 내 다른 애플리케이션이 사용 중일 수 있습니다. 충돌을 피하려면 다음 파일을 수정하여 Protection 에이전트가 사용하는 기본 포트를 변경하면 됩니다.

- Linux: `/opt/Acronis/etc/aakore.yaml`
- Windows: `\ProgramData\Acronis\Agent\etc\aakore.yaml`

프록시 서버 설정

보호 에이전트는 HTTP/HTTPS 프록시 서버를 통해 데이터를 전송할 수 있습니다. 서버는 HTTP 트래픽을 스캔하거나 방해하지 않고 HTTP 터널을 통과해야 합니다. 중간자 프록시는 지원되지 않습니다.

설치 중에 에이전트가 클라우드에 등록되기 때문에 설치하는 동안이나 사전에 프록시 서버 설정이 제공되어야 합니다.

Windows

프록시 서버가 Windows에 구성되어 있는 경우(**제어판 창** > **인터넷 옵션** > **연결**) 설치 프로그램이 레지스트리에서 프록시 서버 설정을 읽어와 자동으로 사용합니다. 또한, 아래 설명된 절차에 따라 설치 중에 프록시 설정을 입력하거나 사전에 설정을 지정할 수 있습니다. 설치 후 프록시 설정을 변경하려면 이와 동일한 절차를 따르십시오.

Windows에서 프록시 설정을 지정하려면

1. 새 텍스트 문서를 생성해 텍스트 편집기(예: 메모장)에서 엽니다.
2. 파일에 다음 행을 복사해 붙여넣습니다.

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\Global\HttpProxy]
"Enabled"=dword:00000001
"Host"="proxy.company.com"
"Port"=dword:000001bb
"Login"="proxy_login"
"Password"="proxy_password"
```

3. `proxy.company.com`을 프록시 서버 호스트 이름/IP 주소로 대체하고 `000001bb`는 포트 번호의 16진수 값으로 대체합니다. 예를 들어, `000001bb`는 포트 443입니다.
4. 프록시 서버에 인증이 필요하다면 `proxy_login`과 `proxy_password`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 이 문서를 **proxy.reg**로 저장합니다.
6. 이 파일을 관리자로 실행합니다.
7. Windows 레지스트리를 편집할 것인지 확인합니다.
8. 보호 에이전트가 아직 설치되지 않았다면 지금 설치할 수 있습니다. 그렇지 않은 경우에는 다음을 수행하여 에이전트를 다시 시작하십시오.
   a. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
   b. **확인**을 클릭합니다.
   c. 다음 명령 실행:

```
net stop mms
net start mms
```

Linux

매개변수 `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`를 사용하여 설치 파일을 실행합니다. 설치 후 프록시 설정을 변경하려면 아래 설명된 절차를 따르십시오.

Linux에서 프록시 설정을 변경하려면

1. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
2. 다음 중 하나를 수행하십시오.
   - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

     ```
     <key name="HttpProxy">
         <value name="Enabled" type="Tdword">"1"</value>
         <value name="Host" type="TString">"ADDRESS"</value>
         <value name="Port" type="Tdword">"PORT"</value>
         <value name="Login" type="TString">"LOGIN"</value>
         <value name="Password" type="TString">"PASSWORD"</value>
     </key>
     ```

   - 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.
3. 주소를 프록시 서버 호스트 이름/IP 주소로 대체하고 포트는 포트 번호의 10진수 값으로 대체합니다.
4. 프록시 서버에 인증이 필요하다면 로그인 및 비밀번호를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 파일을 저장합니다.
6. 아무 디렉터리에서나 다음 명령을 실행하여 에이전트를 다시 시작합니다.

   ```
   sudo service acronis_mms restart
   ```

macOS

아래 설명된 절차에 따라 설치 중에 프록시 설정을 입력하거나 사전에 설정을 지정할 수 있습니다. 설치 후 프록시 설정을 변경하려면 이와 동일한 절차를 따르십시오.

macOS에서 프록시 설정을 지정하려면

1. **/Library/Application Support/Acronis/Registry/Global.config** 파일을 생성해 텍스트 편집기(예: Text Edit)에서 엽니다.
2. 파일에 다음 줄을 복사해 붙여넣습니다.

   ```
   <?xml version="1.0" ?>
   <registry name="Global">
     <key name="HttpProxy">
       <value name="Enabled" type="Tdword">"1"</value>
       <value name="Host" type="TString">"proxy.company.com"</value>
       <value name="Port" type="Tdword">"443"</value>
       <value name="Login" type="TString">"proxy_login"</value>
       <value name="Password" type="TString">"proxy_password"</value>
     </key>
   </registry>
   ```

3. `proxy.company.com`을 프록시 서버 호스트 이름/IP 주소로 대체하고 `443`은 포트 번호의 10진수 값으로 대체합니다.

4. 프록시 서버에 인증이 필요하다면 `proxy_login`과 `proxy_password`를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
5. 파일을 저장합니다.
6. 보호 에이전트가 아직 설치되지 않았다면 지금 설치할 수 있습니다. 그렇지 않은 경우에는 다음을 수행하여 에이전트를 다시 시작하십시오.
   a. **애플리케이션** > **유틸리티** > **터미널**로 이동합니다.
   b. 다음 명령 실행:

```
sudo launchctl stop acronis_mms
sudo launchctl start acronis_mms
```

부트 가능한 미디어에서

부트 가능한 미디어에서 작업할 때 프록시 서버를 통해 클라우드 스토리지에 액세스해야 할 수 있습니다. 프록시 서버 설정을 지정하려면 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 지정합니다.

에이전트 설치

Windows

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 관리자 권한으로 로그온하고 설치 프로그램을 시작합니다.
3. [선택 사항] **설치 설정 사용자 정의**를 클릭하고 원하는 대로 적절하게 변경합니다.
   - 설치할 컴퍼넌트를 변경하려는 경우(특히 Cyber Protect Monitor 및 명령줄 도구의 설치를 비활성화하려는 경우).
   - 사이버 보호 서비스에서 머신 등록 방법을 변경하기 위해. **Cyber Protect 콘솔 사용**(기본값)에서 **자격 증명 사용** 또는 **등록 토큰 사용**으로 전환할 수 있습니다.
   - 설치 경로 변경.
   - 에이전트 서비스용 계정 변경.
   - 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 확인 또는 변경. Windows에서 프록시 서버가 사용하도록 설정되어 있는 경우 자동으로 감지되어 사용됩니다.
4. **설치**를 클릭합니다.
5. [Agent for VMware를 사용하는 경우에만 해당] 에이전트가 가상 머신을 백업할 vCenter Server 또는 독립형 ESXi 호스트에 대한 주소 및 액세스 자격 증명을 지정한 다음, **완료**를 클릭합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.
6. [도메인 컨트롤러에 설치하는 경우에만 해당] 에이전트 서비스를 실행할 사용자 계정을 지한 다음 **완료**를 클릭합니다. 보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

참고

지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다.

이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

7. 3단계에서 **Cyber Protect 콘솔 사용**이라는 기본 등록 방법을 유지한 경우 등록 화면이 나타날 때까지 기다린 후 다음 단계를 진행합니다. 그러지 않으면 추가 작업은 필요하지 않습니다.
8. 다음 중 하나를 수행하십시오.
   - **머신 등록**을 클릭합니다. 열려 있는 브라우저 창에서 Cyber Protect 웹 콘솔에 로그인하고 등록 세부정보를 검토한 다음, **등록 확인**을 클릭합니다.
   - **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 이를 복사하고 다른 머신에서 등록 절차를 수행할 수 있습니다. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.

     또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.
9. **참고**

   등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설치 프로그램을 다시 시작한 다음 **머신 등록**을 클릭해야 합니다.

그러면 Cyber Protect 웹 콘솔에 로그인하는 데 사용된 계정에 머신이 지정됩니다.

Linux

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 루트 사용자로 설치 파일을 실행합니다.

   프록시 서버가 사용자 네트워크에서 활성화된 경우 서버 호스트 이름/IP 주소 및 포트를 다음 형식으로 지정합니다. `--http-proxy-host=ADDRESS --http-proxy-port=PORT --http-proxy-login=LOGIN--http-proxy-password=PASSWORD`.

   사이버 보호 서비스에서 머신을 등록하는 기본 방법을 변경하려면 다음 매개 변수 중 하나로 설치 파일을 실행하십시오.
   - `--register-with-credentials` - 설치 중에 사용자 이름 및 패스워드 요청
   - `--token=STRING` - 등록 토큰 사용
   - `--skip-registration` - 등록 건너뛰기
3. 설치할 에이전트의 확인란을 선택합니다. 다음 에이전트를 선택할 수 있습니다.
   - **Agent for Linux**
   - **Agent for Virtuozzo**

   Agent for Virtuozzo는 Agent for Linux가 없는 경우 설치할 수 없습니다.

4. 2단계에서 기본 등록 방법을 유지한 경우 다음 단계를 진행합니다. 그렇지 않으면 사이버 보호 서비스에 대한 사용자 이름과 비밀번호를 입력하거나 토큰을 사용하여 머신이 등록될 때까지 기다리십시오.
5. 다음 중 하나를 수행하십시오.
   - **머신 등록**을 클릭합니다. 열려 있는 브라우저 창에서 Cyber Protect 웹 콘솔에 로그인하고 등록 세부정보를 검토한 다음, **등록 확인**을 클릭합니다.
   - **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 이를 복사하고 다른 머신에서 등록 절차를 수행할 수 있습니다. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.

     또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.

6. **참고**
   등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설정 프로그램을 다시 시작한 다음, 설치 과정을 반복합니다.

   그러면 Cyber Protect 웹 콘솔에 로그인하는 데 사용된 계정에 머신이 지정됩니다.
7. UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 어느 비밀번호(루트 사용자의 비밀번호 또는 "acronis")를 사용해야 하는지 잘 기억해 두십시오.

   참고
   설치 중 `snapapi` 모듈에 서명하는 데 사용되고, MOK(Machine Owner Key)로 등록되는 새 키가 생성됩니다. 이 키를 등록하려면 다시 시작이 필수입니다. 키를 등록하지 않으면 에이전트가 작동하지 않습니다. 에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 6단계를 포함하는 설치를 반복하십시오.

8. 설치가 완료되면 다음 중 하나를 수행하십시오.
   - 이전 단계에서 시스템을 다시 시작하라는 메시지가 표시된 경우 **다시 시작**을 클릭합니다.

     시스템 다시 시작 중에 MOK(Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 이전 단계에서 권장된 비밀번호를 사용하여 키를 등록합니다.
   - 그렇지 않은 경우, **종료**를 클릭합니다.

문제 해결 정보가 다음 파일에 제공됩니다.
/usr/lib/Acronis/BackupAndRecovery/HOWTO.INSTALL

macOS

1. 머신이 인터넷에 연결되어 있는지 확인합니다.
2. 설치 파일(.dmg)을 두 번 클릭합니다.
3. 운영 체제가 설치 디스크 이미지를 마운트하는 동안 기다립니다.
4. **설치**를 두 번 클릭합니다.

5. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 메뉴 표시줄에서 **보호 에이전트**, **프록시 서버 설정**을 차례로 클릭한 다음 프록시 서버 호스트 이름/IP 주소, 포트 및 자격 증명을 지정합니다.
6. 메시지가 표시되면 관리자 자격 증명을 제공합니다.
7. **계속**을 클릭합니다.
8. 등록 화면이 나타날 때까지 기다립니다.
9. 다음 중 하나를 수행하십시오.
   - **머신 등록**을 클릭합니다. 열려 있는 브라우저 창에서 Cyber Protect 웹 콘솔에 로그인하고 등록 세부정보를 검토한 다음, **등록 확인**을 클릭합니다.
   - **등록 정보 표시**를 클릭합니다. 설치 프로그램에 등록 링크와 등록 코드가 표시됩니다. 이를 복사하고 다른 머신에서 등록 절차를 수행할 수 있습니다. 이 경우 등록 양식에 등록 코드를 입력해야 할 수 있습니다. 등록 코드는 1시간 동안 유효합니다.

     또는, **모든 장치** > **추가**를 클릭하고 **코드를 통한 등록**으로 스크롤을 내린 다음 **등록**을 클릭해 등록 양식에 액세스할 수 있습니다.
10. **팁** 등록을 확인할 때까지 설정 프로그램을 종료하지 마십시오. 등록을 다시 시작하려면 설정 프로그램을 다시 시작한 다음, 설치 과정을 반복합니다.

그러면 Cyber Protect 웹 콘솔에 로그인하는 데 사용된 계정에 머신이 지정됩니다.

Windows 머신에서 로그온 계정 변경

컴퍼넌트 선택 화면에서 **에이전트 서비스를 위한 로그온 계정**을 지정해 서비스를 실행할 계정을 정의합니다. 다음 중 하나를 선택합니다.

- **서비스 사용자 계정 사용**(에이전트 서비스용 기본값)

  서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 설정의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다.
- **새 계정 생성**

  계정 이름은 해당 에이전트에 대해 Agent User로 지정됩니다.
- **다음 계정 사용**

  도메인 컨트롤러에 에이전트를 설치하는 경우 시스템에 각 에이전트의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 시스템은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

  도메인 컨트롤러에서 설치 프로그램을 실행할 때 지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다. 이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

  읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.

새 계정 생성 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당되어 있는 사용자 권한이 박탈되는 경우 컴퍼넌트가 올바로 작동하지 않거나 아예 작동하지 않을 수 있습니다.

로그온 계정에 필요한 권한

보호 에이전트는 Windows 머신에서 관리 대상 머신 서비스(MMS)로 실행됩니다. 에이전트가 실행되는 계정에는 해당 에이전트가 올바르게 작동할 수 있는 특정 권한이 있어야 합니다. 따라서 MMS 사용자에게는 다음과 같은 권한이 할당되어야 합니다.

1. **백업 작업자** 및 **관리자** 그룹에 포함됨. 도메인 컨트롤러에서 사용자는 **도메인 관리자** 그룹에 포함되어 있어야 합니다.
2. **전체 제어** 권한이 `%PROGRAMDATA%\Acronis`(Windows XP 및 Server 2003, `%ALLUSERSPROFILE%\Application Data\Acronis`) 폴더 및 해당 하위 폴더에 대해 부여됩니다.
3. 다음 키 중 특정 레지스트리 키에 대해 **전체 제어** 권한이 부여됩니다. `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis`.
4. 다음의 사용자 권한이 할당됨:
   - 서비스로 로그온
   - 프로세스에 대한 메모리 할당량 조정
   - 프로세스 수준 토큰 교체
   - 펌웨어 환경 값 수정

사용자 권한 할당 방법

아래 지침에 따라 사용자 권한을 할당하십시오(이 예시에서는 **서비스로 로그온** 사용자 권한을 사용하며, 다른 사용자 권한에 대한 단계와 동일합니다).

1. 관리자 권한이 있는 계정을 사용해 컴퓨터에서 로그온합니다.
2. **제어판**에서 **관리 도구**를 열고(또는 Win+R을 클릭하고 **control admintools**를 입력한 후 엔터를 누르고) **로컬 보안 정책**을 엽니다.
3. **로컬 정책**을 확장하고 **사용자 권한 할당**을 클릭합니다.
4. 오른쪽 창에서 **서비스로 로그온**을 마우스 오른쪽으로 클릭하고 **속성**을 선택합니다.
5. **사용자 또는 그룹 추가...** 버튼을 클릭하여 새 사용자를 추가합니다.
6. **사용자, 컴퓨터, 서비스 계정 또는 그룹 선택** 창에서 입력하려는 사용자를 찾아 **확인**을 클릭합니다.
7. **서비스로 로그온 속성**에서 **확인**을 클릭하여 변경 사항을 저장합니다.

중요

서비스로 로그온 사용자 권한에 추가한 사용자가 **로컬 보안 정책**의 **서비스로 로그온 거부** 정책에 포함되어 있지 않은지 확인하십시오.

설치가 완료된 후 수동으로 로그온 계정을 변경하는 것은 권장되지 않습니다.

무인 설치 또는 제거

Windows에서 무인 설치 또는 제거

이 섹션에서는 Windows를 실행하는 머신에서 Windows Installer(`msiexec` 프로그램)를 사용하여 보호 에이전트를 무인 모드로 설치 또는 제거하는 방법에 대해 설명합니다. Active Directory 도메인에서 무인 설치를 수행하는 또 다른 방법은 그룹 정책을 사용하는 것입니다("그룹 정책을 통해 에이전트 배포"(165페이지) 참조).

설치 중에는 **변환**(.mst 파일)이라는 파일을 사용할 수 있습니다. 변환 파일은 설치 매개변수가 포함된 파일입니다. 대안으로 명령줄에서 직접 설치 매개변수를 지정해도 됩니다.

.mst 변환 생성 및 설치 패키지 추출

1. 관리자 권한으로 로그온하고 설치 프로그램을 시작합니다.
2. **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭합니다.
3. **설치 대상**에서 설치할 컴포넌트를 선택하고 **완료**를 누릅니다.
   해당 컴퍼넌트용 설치 패키지가 설정 프로그램에서 추출됩니다.
4. **등록 설정**에서 **자격 증명 사용** 또는 **등록 토큰 사용**을 선택합니다. 등록 토큰을 생성하는 방법에 대한 자세한 내용은 "1단계: 등록 토큰 생성"(166페이지)을(를) 참조하십시오.
5. [도메인 컨트롤러에 설치하는 경우에만 해당] **에이전트 서비스용 로그온 계정**에서 **다음 계정 사용**을 선택합니다. 에이전트 서비스를 실행할 사용자 계정을 지정한 다음 **완료**를 클릭합니다. 보안상의 이유로 설치 프로그램은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

   참고
   지정한 사용자 계정에 서비스로 로그온 권한이 부여되어 있어야 합니다.
   이 계정이 이미 도메인 컨트롤러에 사용 중인 계정이어야 프로필 폴더가 해당 머신에서 생성될 수 있습니다.

   읽기 전용 도메인 컨트롤러에 에이전트를 설치하는 방법에 대한 자세한 내용은 이 기술 자료 문서를 참조하십시오.
6. .mst 파일에 추가될 기타 설치 설정을 검토하거나 수정한 다음, **진행**을 클릭합니다.
7. .mst 변환이 생성되고 .msi 및 .cab 설치 패키지가 추출될 폴더를 선택한 다음 **생성**을 클릭합니다.

.mst 변환을 사용하여 제품 설치

명령줄에서 다음 명령을 실행합니다.

명령 템플릿:

```
msiexec /i <package name> TRANSFORMS=<transform name>
```

위치:

- <패키지 이름>은 .msi 파일의 이름입니다.
- <변환 이름>은 변환의 이름입니다.

명령 예:

```
msiexec /i BackupClient64.msi TRANSFORMS=BackupClient64.msi.mst
```

매개변수를 수동으로 지정하여 제품 설치 또는 제거

명령줄에서 다음 명령을 실행합니다.

명령 템플릿(설치):

```
msiexec /i <package name><PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

여기에서 <패키지 이름>은 .msi 파일의 이름입니다. 사용 가능한 모든 매개변수와 해당 값은 "기본 매개변수"(134페이지) 항목에 설명되어 있습니다.

명령 템플릿(제거):

```
msiexec /x <package name> <PARAMETER 1>=<value 1> ... <PARAMETER N>=<value n>
```

.msi 패키지의 버전은 제거하려는 제품의 버전과 같아야 합니다.

무인 설치 또는 제거 매개변수

이 섹션에서는 Windows에서 무인 설치 또는 제거 중 사용되는 매개변수에 대해 설명합니다. 이 매개변수 외에 https://msdn.microsoft.com/en-us/library/windows/desktop/aa367988(v=vs.85).aspx에 설명된 대로 다른 `msiexec` 매개변수도 사용할 수 있습니다.

설치 매개변수

기본 매개변수

`ADDLOCAL=<list of components>`

설치될 컴퍼넌트는 쉼표로 구분되고 공백 문자가 없습니다. 지정된 모든 컴퍼넌트가 설치 전에 설정 프로그램에서 추출되어야 합니다.

컴퍼넌트의 전체 목록은 다음과 같습니다.

구성 요소	다음 항목과 함께 설치	비트	컴퍼넌트 이름 / 설명
MmsMspComponents		32비트/64비트	에이전트용 핵심 컴퍼넌트
BackupAndRecoveryAgent	MmsMspComponents	32비트/64비트	Agent for Windows

ArxAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Exchange
ArsAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for SQL
ARADAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Active Directory
ArxOnlineAgentFeature	MmsMspComponents	32비트/64비트	Agent for Office 365
OracleAgentFeature	BackupAndRecoveryAgent	32비트/64비트	Agent for Oracle
AcronisESXSupport	MmsMspComponents	64비트	Agent for VMware ESX(i) (Windows)
HyperVAgent	MmsMspComponents	32비트/64비트	Agent for Hyper-V
CommandLineTool		32비트/64비트	명령줄 도구
TrayMonitor	BackupAndRecoveryAgent	32비트/64비트	Cyber Protect 모니터링

`TARGETDIR=<path>`

제품을 설치할 폴더. 기본적으로 이 폴더는 `C:\Program Files\BackupClient`입니다.

`REBOOT=ReallySuppress`

이 매개변수가 지정되면 머신 재부팅이 금지됩니다.

`/l*v <log file>`

이 매개변수를 지정하면 자세한 정보 표시 모드의 설치 로그가 지정된 파일에 저장됩니다. 로그 파일은 설치 문제를 분석하는 데 사용될 수 있습니다.

`CURRENT_LANGUAGE=<language ID>`

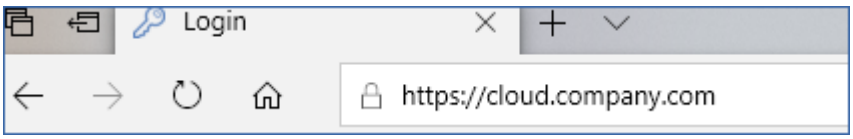
제품 언어. 사용 가능한 값은 다음과 같습니다. `en`, `bg`, `cs`, `da`, `de`, `es`, `fr`, `hu`, `id`, `it`, `ja`, `ko`, `ms`, `nb`, `nl`, `pl`, `pt`, `pt_BR`, `ru`, `fi`, `sr`, `sv`, `tr`, `zh`, `zh_TW`.
이 매개변수가 지정되지 않으면 제품 언어는 시스템 언어로 정의됩니다. 단, 해당 언어가 위 목록에 포함되어 있어야 합니다. 그렇지 않으면 제품 언어는 영어로 설정됩니다(en).

등록 매개변수

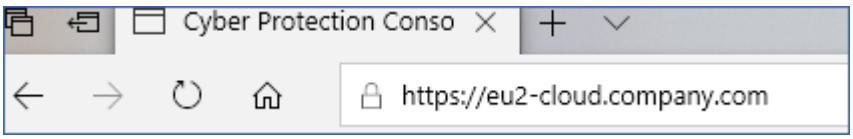
`REGISTRATION_ADDRESS`

Cyber Protect 서비스를 위한 URL입니다. 이 매개변수는 REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수와 함께, 또는 REGISTRATION_TOKEN 매개변수와 함께 사용할 수 있습니다.

- REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD 매개변수와 함께 REGISTRATION_ADDRESS 사용 시, Cyber Protect 서비스에 **로그인**하는 데 사용하는 주소를 지정하십시오. 예: https://cloud.company.com:



- REGISTRATION_TOKEN 매개변수와 함께 REGISTRATION_ADDRESS 사용 시 정확한 데이터센터 주소를 지정하십시오. 이는 Cyber Protect 서비스에 **로그인하면** 표시되는 URL입니다. 예: https://eu2-cloud.company.com.



여기서 https://cloud.company.com을 사용하지 마십시오.

REGISTRATION_LOGIN 및 REGISTRATION_PASSWORD

Cyber Protect 서비스에서 에이전트를 등록할 계정의 자격 증명. 파트너 관리자 계정은 사용할 수 없습니다.

REGISTRATION_PASSWORD_ENCODED

Cyber Protect 서비스에서 에이전트를 등록할 계정의 base64로 암호화된 비밀번호. 비밀번호 암호화 방법에 대한 자세한 내용은 "수동으로 머신 등록"을 참조하십시오.

REGISTRATION_TOKEN

등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. "그룹 정책을 통해 에이전트 디플로이"에 설명되어 있는 대로 웹 콘솔에서 생성할 수 있습니다.

REGISTRATION_REQUIRED={0,1}

등록 실패 시 설치를 종료할 방법을 정의합니다. 값이 1인 경우에도 설치에 실패합니다. 기본값이 0이며 이 매개변수를 지정하지 않은 경우, 에이전트가 등록되어 있지 않아도 설치가 성공적으로 완료됩니다.

추가 매개변수

Windows에서 에이전트 서비스용 로그온 계정을 정의하려면 다음 매개변수 중 하나를 사용하십시오.

- MMS_USE_SYSTEM_ACCOUNT={0,1}

  값이 1인 경우, 에이전트는 **로컬 시스템** 계정에서 실행됩니다.
- MMS_CREATE_NEW_ACCOUNT={0,1}

  값이 1인 경우, 에이전트는 이름이 **Acronis Agent User**인 새롭게 생성된 계정에서 실행됩니다.

- MMS_SERVICE_USERNAME= <user name> 및 MMS_SERVICE_PASSWORD=<password>
  이러한 매개변수를 사용하여 에이전트가 실행될 기존 계정을 지정하십시오.

로그온 계정에 대한 자세한 내용은 "Windows 머신에서 로그온 계정 변경"을 참조하십시오.

SET_ESX_SERVER={0,1}

- 값이 0인 경우, 설치 중인 Agent for VMware가 vCenter Server 또는 ESXi 호스트에 연결되지 않습니다. 값이 1인 경우, 다음 매개변수를 지정합니다.
  - ESX_HOST= <host name>
    vCenter Server 또는 ESXi 호스트의 호스트 이름 또는 IP 주소.
  - ESX_USER= <user name> 및 ESX_PASSWORD=<password>
    vCenter Server 또는 ESXi 호스트에 액세스하기 위한 자격 증명.

HTTP_PROXY_ADDRESS= <IP address> 및 HTTP_PROXY_PORT=<port>

에이전트가 사용하는 HTTP 프록시 서버. 이 매개변수가 없으면 프록시 서버가 사용되지 않습니다.

HTTP_PROXY_LOGIN= <login> 및 HTTP_PROXY_PASSWORD=<password>

HTTP 프록시 서버의 자격 증명. 서버에 인증이 필요한 경우 이 매개변수를 사용합니다.

HTTP_PROXY_ONLINE_BACKUP={0,1}

값이 0인 경우 또는 매개변수가 지정되지 않은 경우에는 에이전트가 클라우드에서의 백업 및 복구에만 프록시 서버를 사용합니다. 또한, 값이 1인 경우에는 에이전트가 프록시 서버를 통해 관리 서버에 연결합니다.

제거 매개변수

REMOVE={ <list of components> |ALL}

제거될 컴퍼넌트는 쉼표로 구분되고 공백 문자가 없습니다. 값이 ALL인 경우 모든 제품 컴퍼넌트가 제거됩니다.

추가로 다음 매개변수를 지정할 수 있습니다.

DELETE_ALL_SETTINGS={0, 1}

값이 1인 경우 제품의 로그, 작업 및 구성 설정이 제거됩니다.

예

- Agent for Windows, 명령줄 도구, Cyber Protection Monitor 설치. 사용자 이름과 비밀번호를 사용하여 Cyber Protect 서비스에서 머신 등록.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_USE_SYSTEM_
ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com REGISTRATION_LOGIN=johndoe
REGISTRATION_PASSWORD=johnspassword
```

- Agent for Windows, 명령줄 도구, Cyber Protection Monitor 설치. Windows에서 에이전트 서비스 용 새 로그온 계정 생성. 토큰을 사용하여 Cyber Protect 서비스에서 머신 등록.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress MMS_CREATE_NEW_
ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com REGISTRATION_TOKEN=34F6-
8C39-4A5C
```

- Agent for Windows, 명령줄 도구, Agent for Oracle, Cyber Protection Monitor 설치. 사용자 이름과 base64로 암호화된 비밀번호를 사용하여 Cyber Protect 서비스에서 머신 등록.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,OracleAgentFeature,T
rayMonitor TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_
LANGUAGE=en MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://cloud.company.com
REGISTRATION_LOGIN=johndoe REGISTRATION_PASSWORD_ENCODED=am9obnNwYXNzd29yZA==
```

- Agent for Windows, 명령줄 도구, Cyber Protection Monitor 설치. 토큰을 사용하여 Cyber Protect 서비스에서 머신 등록. HTTP 프록시 설정.

```
msiexec.exe /i BackupClient64.msi /l*v my_log.txt /qn
ADDLOCAL=MmsMspComponents,BackupAndRecoveryAgent,CommandLineTool,TrayMonitor
TARGETDIR="C:\Program Files\BackupClient" REBOOT=ReallySuppress CURRENT_LANGUAGE=en
MMS_USE_SYSTEM_ACCOUNT=1 REGISTRATION_ADDRESS=https://eu2-cloud.company.com
REGISTRATION_TOKEN=34F6-8C39-4A5C HTTP_PROXY_ADDRESS=https://my-proxy.company.com
HTTP_PROXY_PORT=80 HTTP_PROXY_LOGIN=tomsmith HTTP_PROXY_PASSWORD=tomspassword
```

- 모든 에이전트 제거 및 로그, 작업 및 구성 설정 삭제.

```
msiexec.exe /x BackupClient64.msi /l*v uninstall_log.txt REMOVE=ALL DELETE_ALL_
SETTINGS=1 REBOOT=ReallySuppress
```

Linux에서 무인 설치 또는 제거

이 섹션에서는 Linux를 실행하는 머신에서 명령줄을 사용하여 보호 에이전트를 무인 모드로 설치 또는 제거하는 방법에 대해 설명합니다.

보호 에이전트를 설치 또는 제거하려면

1. 터미널을 엽니다.

2. 다음 중 하나를 수행하십시오.

- 명령줄에서 매개변수를 지정하여 설치를 시작하려면 다음 명령을 실행합니다.

```
<package name> -a <parameter 1> ... <parameter N>
```

여기서, <패키지 이름>은 설치 패키지(.i686 또는 .x86_64 파일)의 이름입니다. 사용 가능한 모든 매개변수와 그 값은 "무인 설치 또는 제거 매개변수"에 설명되어 있습니다.

- 별도의 텍스트 파일에서 지정된 매개변수를 사용해 설치를 시작하려면 다음 명령을 실행합니다.

  ```
  <package name> -a --options-file=<path to the file>
  ```

  이 접근 방식은 명령줄에 민감한 정보를 입력하고 싶지 않을 때 유용할 수 있습니다. 이 경우, 별도의 텍스트 파일에서 구성 설정을 지정하고 사용자만 액세스할 수 있는지 확인할 수 있습니다. 새 행에 각 매개변수를 입력하고 원하는 값을 입력하십시오. 예:

  ```
  --rain=https://cloud.company.com
  --login=johndoe
  --password=johnspassword
  --auto
  ```

  또는

  ```
  -C
  https://cloud.company.com
  -g
  johndoe
  -w
  johnspassword
  -a
  --language
  en
  ```

  명령줄과 텍스트 파일 모두에 동일한 매개변수가 지정된 경우 명령줄 값이 우선합니다.

3. UEFI 보안 부팅이 머신에서 활성화되어 있는 경우에는 설치 후에 시스템을 다시 시작해야 한다는 메시지가 표시됩니다. 어느 비밀번호(루트 사용자의 비밀번호 또는 "acronis")를 사용해야 하는지 잘 기억해 두십시오. 시스템 다시 시작 중에 MOK(Machine Owner Key) 관리를 선택하고, **MOK 등록**을 선택한 다음, 권장 비밀번호를 사용하여 키를 등록합니다.

에이전트 설치 후 UEFI 보안 부팅을 활성화하는 경우에는 3단계를 포함하는 설치를 반복하십시오. 그렇지 않으면 백업에 실패하게 됩니다.

무인 설치 또는 제거 매개변수

이 섹션에서는 Linux에서 무인 설치 또는 제거 중 사용되는 매개변수에 대해 설명합니다.

무인 설치의 최소 구성에는 `-a` 및 등록 매개변수(예: `--login` 및 `--password` 매개변수; `--rain` 및 `--token` 매개변수)가 포함됩니다. 더 많은 매개변수를 사용하여 설치를 사용자 정의할 수 있습니다.

설치 매개변수

기본 매개변수

`{-i |--id=}<list of components>`

설치될 컴퍼넌트는 쉼표로 구분되고 공백 문자가 없습니다. .x86_64 설치 패키지에서는 다음 컴퍼넌트를 사용할 수 있습니다.

구성 요소	컴퍼넌트 설명
BackupAndRecoveryAgent	Agent for Linux
AgentForPCS	Agent for Virtuozzo
OracleAgentFeature	Agent for Oracle

이 매개변수가 없으면 위의 모든 컴퍼넌트가 설치됩니다.

Agent for Virtuozzo 및 Agent for Oracle을 설치하려면 Agent for Linux도 설치되어 있어야 합니다.

.i686 설치 패키지는 BackupAndRecoveryAgent만 포함합니다.

`{-a|--auto}`

설치 및 등록 프로세스는 추가 사용자 상호 작용 없이 완료됩니다. 이 매개변수를 사용할 때 `--token` 매개변수를 사용하거나 `--login` 및 `--password` 매개변수를 사용하여 Cyber Protect 서비스에서 에이전트를 등록할 계정을 지정해야 합니다.

`{-t|--strict}`

이 매개변수를 지정하면 설치 중 발생하는 모든 경고가 설치 실패로 이어집니다. 이 매개변수가 없으면 경고가 발생하더라도 설치가 성공적으로 완료됩니다.

`{-n|--nodeps}`

설치 중에 필요한 Linux 패키지가 없으면 무시됩니다.

`{-d|--debug}`

자세한 정보 표시 모드로 설치 로그를 작성합니다.

`--options-file=<location>`

명령줄 대신 텍스트 파일에서 설치 매개변수를 읽습니다.

`--language=<language ID>`

제품 언어. 사용 가능한 값은 다음과 같습니다. `en, bg, cs, da, de, es, fr, hu, id, it, ja, ko, ms, nb, nl, pl, pt, pt_BR, ru, fi, sr, sv, tr, zh, zh_TW`.
이 매개변수가 지정되지 않으면 제품 언어는 시스템 언어로 정의됩니다. 단, 해당 언어가 위 목록에 포함되어 있어야 합니다. 그렇지 않으면 제품 언어는 영어로 설정됩니다(en).

등록 매개변수

다음 매개변수 중 하나를 지정합니다.

- `{-g|--login=}<user name>` 및 `{-w|--password=}<password>`

Cyber Protect 서비스에서 에이전트를 등록할 계정의 자격 증명. 파트너 관리자 계정은 사용할 수 없습니다.

- `--token=<token>`

  등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. "그룹 정책을 통해 에이전트 디플로이"에 설명되어 있는 대로 웹 콘솔에서 생성할 수 있습니다.

  `--token` 매개변수는 `--login`, `--password` 및 `--register-with-credentials` 매개변수와 함께 사용할 수 없습니다.

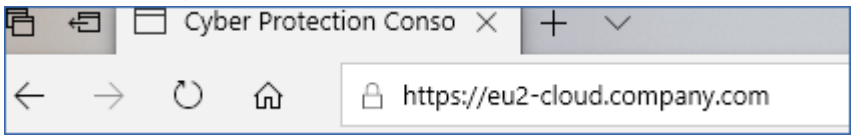
  - `{-C|--rain=}<service address>`

    Cyber Protect 서비스의 URL입니다.

    인스톨러가 기본적으로 올바른 주소(Cyber Protect 서비스에 **로그인하기 위해** 사용하는 주소)를 사용하므로, 등록을 위해 `--login` 및 `--password` 매개변수를 사용할 때 명시적으로 이 매개변수를 포함할 필요는 없습니다. 예:

    하지만 `--token` 매개변수와 함께 `{-C|--rain=}` 사용 시 정확한 데이터센터 주소를 지정해야 합니다. 이는 Cyber Protect 서비스에 **로그인하면** 표시되는 URL입니다. 예:

- `--register-with-credentials`

  이 매개변수가 지정되면 인스톨러의 그래픽 인터페이스가 시작됩니다. 등록을 완료하려면 Cyber Protect 서비스에서 에이전트를 등록할 계정의 사용자 이름과 비밀번호를 입력합니다. 파트너 관리자 계정은 사용할 수 없습니다.

- `--skip-registration`

  에이전트를 설치해야 하지만 나중에 Cyber Protect 서비스에서 등록할 예정인 경우 이 매개변수를 사용하십시오. 작업의 수행 방법에 대한 자세한 내용은 "수동으로 머신 등록"을 참조하십시오.

추가 매개변수

`--http-proxy-host=<IP address>` 및 `--http-proxy-port=<port>`

에이전트가 클라우드에 백업하고 여기에서 복구할 때, 그리고 관리 서버에 연결할 때 사용하는 HTTP 프록시 서버. 이 매개변수가 없으면 프록시 서버가 사용되지 않습니다.

`--http-proxy-login=<login>` 및 `--http-proxy-password=<password>`

HTTP 프록시 서버의 자격 증명. 서버에 인증이 필요한 경우 이 매개변수를 사용합니다.

`--tmp-dir=<location>`

설치 중 임시 파일을 저장할 폴더를 지정합니다. 기본 폴더는 **/var/tmp**입니다.

`{-s|--disable-native-shared}`

이미 시스템에 존재하더라도 설치 중에는 재배포 가능한 라이브러리가 사용됩니다.

`--skip-prereq-check`

snapapi 모듈의 컴파일을 위해 필요한 패키지가 이미 설치되어 있는지는 확인하지 않습니다.

`--force-weak-snapapi`

인스톨러는 snapapi 모듈을 컴파일하지 않습니다. 그 대신 Linux 커널과 정확하게 일치하지 않을 수 있는 이미 생성된 모듈을 사용합니다. 이 옵션을 사용하는 것은 권장되지 않습니다.

`--skip-svc-start`

설치 후 서비스가 자동으로 시작되지 않습니다. 대부분의 경우, 이 매개변수는 `--skip-registration` 매개변수와 함께 사용됩니다.

정보 매개변수

`{-?|--help}`

매개변수 설명이 표시됩니다.

`--usage`

명령의 용도에 대한 간략한 설명이 표시됩니다.

`{-v|--version}`

설치 패키지 버전을 표시합니다.

`--product-info`

제품 이름 및 설치 패키지 버전을 표시합니다.

`--snapapi-list`

이미 생성된 사용 가능 snapapi 모듈을 표시합니다.

`--components-list`

인스톨러 컴퍼넌트를 표시합니다.

레거시 기능에 대한 매개변수

이러한 매개변수는 레거시 컴퍼넌트 agent.exe와 관련이 있습니다.

`{-e|--ssl=}` `<path>`

SSL 통신을 위한 사용자 정의 인증서 파일의 경로를 지정합니다.

`{-p|--port=}` `<port>`

agent.exe가 연결을 수신하는 포트를 지정합니다. 기본 포트는 9876입니다.

제거 매개변수

`{-u|--uninstall}`

제품을 제거합니다.

`--purge`

제품을 제거하고 제품의 로그, 작업 및 구성 설정을 제거합니다. `--purge` 매개변수를 사용할 때 `--uninstall` 매개변수를 명시적으로 지정할 필요가 없습니다.

예

- Agent for Linux를 등록하지 않고 설치.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent -a --skip-registration
```

- Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle을 설치하고 자격 증명을 사용하여 등록.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --login=johndoe --password=johnspassword
```

- Agent for Oracle 및 Agent for Linux를 설치하고 등록 토큰을 사용하여 등록.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -i BackupAndRecoveryAgent,OracleAgentFeature -a --rain=https://eu2-cloud.company.com --token=34F6-8C39-4A5C
```

- 별도의 텍스트 파일에 구성 설정을 포함하여 Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle 설치.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --options-file=/home/mydirectory/configuration_file
```

- Agent for Linux, Agent for Virtuozzo 및 Agent for Oracle을 제거하고 모든 로그, 작업 및 구성 설정 제거.

```
./Cyber_Protection_Agent_for_Linux_x86_64.bin -a --purge
```

macOS에 무인 설치 및 제거

이 섹션에서는 macOS를 실행 중인 머신에서 명령줄을 사용하여 Protection 에이전트를 무인 모드로 설치, 등록 및 설치 제거하는 방법에 대해 설명합니다. 설치 파일(.dmg)을 다운로드하는 방법은 "macOS를 실행하는 머신 추가"를 참조하십시오.

Agent for Mac을 설치하려면

1. 설치 파일(.dmg)을 마운트할 임시 디렉토리를 생성합니다.

   ```
   mkdir <dmg_root>
   ```

   여기에서 `<dmg_root>`은(는) 사용자가 선택한 이름입니다.
2. .dmg 파일을 마운트합니다.

```
hdiutil attach <dmg_file> -mountpoint <dmg_root>
```

여기에서 <dmg_file>은(는) 설치 파일의 이름입니다. 예를 들어, **AcronisAgentMspMacOSX64.dmg**입니다.

3. 인스톨러를 실행합니다.

```
sudo installer -pkg <dmg_root>/Install.pkg -target LocalSystem
```

4. 설치 파일(.dmg)을 분리합니다.

```
hdiutil detach <dmg_root>
```

예

- ```
  mkdir mydirectory
  ```

  ```
  hdiutil attach /Users/JohnDoe/AcronisAgentMspMacOSX64.dmg -mountpoint mydirectory
  ```

  ```
  sudo installer -pkg mydirectory/Install.pkg -target LocalSystem
  ```

  ```
  hdiutil detach mydirectory
  ```

Agent for Mac을 등록하려면

다음 중 하나를 수행하십시오.

- 사용자 이름과 패스워드를 이용하여 특정 계정에 에이전트를 등록합니다.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  <service address> -u <user name> -p <password>
  ```

  여기서,

  <Cyber Protect service address>는 Cyber Protect 서비스에 **로그인**하는 데 사용하는 주소입니다. 예:

  <사용자 이름> 및 <비밀번호> 는 에이전트를 등록하는 계정의 자격 증명입니다. 파트너 관리자 계정은 사용할 수 없습니다.

- 등록 토큰을 이용하여 에이전트를 등록합니다.

  ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  <service address> --token <token>
  ```
  ```

등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. "그룹 정책을 통해 에이전트 디플로이"에 설명되어 있는 대로 Cyber Protect 웹 콘솔에서 생성할 수 있습니다.

등록 토큰을 사용하는 경우 정확한 데이터센터 주소를 지정해야 합니다. 이는 Cyber Protect 서비스에 **로그인하면** 표시되는 URL입니다. 예:

중요

macOS 10.14 이상을 사용 중인 경우 보호 에이전트에 전체 디스크 액세스 권한을 부여해야 합니다.이렇게 하려면 **애플리케이션** >**유틸리티**로 이동한 다음 **Cyber Protect 에이전트 지원**을 실행하십시오. 그런 다음 애플리케이션 창의 지침을 따릅니다.

예

사용자 이름 및 패스워드로 등록.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://cloud.company.com -u johndoe -p johnspassword
  ```

토큰으로 등록.

- ```
  sudo /Library/Application\
  Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent -o register -t cloud -a
  https://eu2-cloud company.com --token D91D-DC46-4F0B
  ```

Agent for Mac을 제거하려면

다음 명령을 실행합니다.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm
  ```

제거 중에 모든 로그, 작업, 구성 설정까지 제거하려면 다음 명령을 실행합니다.

- ```
  sudo /Library/Application\ Support/BackupClient/Acronis/Cyber\ Protect\ Agent\
  Uninstall.app/Contents/MacOS/AgentUninstall /confirm /purge
  ```

수동으로 머신 등록

에이전트 설치 중 Cyber Protect 서비스에서 머신을 등록하는 것 이외에 명령줄 인터페이스를 사용하여 등록할 수도 있습니다. 에이전트를 설치했지만 자동 등록에 실패한 경우, 또는 새 계정에서 기존 머신을 등록하려는 경우 이 방법을 사용해야 할 수 있습니다.

머신을 등록하려면

에이전트가 설치된 머신의 명령 프롬프트에서 다음 명령 중 하나를 실행합니다.

- 현재 계정에서 머신을 등록하는 방법:

```
<path to the registration tool> -o register -s mms -t cloud --update
```

  - 여기서 <등록 도구 경로> 은 다음과 동일합니다.
    - Windows: `%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe`
    - Linux: `/usr/lib/Acronis/RegisterAgentTool/RegisterAgent`
    - macOS: `/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent`
- 다른 계정에서 머신을 등록하는 방법:

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name> -p <password>
```

  - 여기서 <사용자 이름> 및 <비밀번호> 는 에이전트를 등록하는 특정 계정의 자격 증명입니다. 파트너 관리자 계정은 사용할 수 없습니다.

    <서비스 주소>는 Cyber Protect 서비스에 **로그인**하는 데 사용하는 URL입니다. 예: `https://cloud.company.com`

- 등록 토큰으로 머신을 등록하는 방법:

```
<path to the registration tool> -o register -t cloud -a <service address> --token <token>
```

  - 등록 토큰은 12자로 이루어져 있으며 하이픈에 의해 세 개의 세그먼트로 구분됩니다. 생성 방법에 대한 자세한 내용은 "그룹 정책을 통해 에이전트 디플로이"를 참조하십시오.

    등록 토큰을 사용하는 경우, <서비스 주소>처럼 정확한 데이터센터 주소를 지정해야 합니다. 이는 Cyber Protect 서비스에 **로그인하면** 표시되는 URL입니다. 예: `https://eu2-cloud.company.com`.

    여기서 `https://cloud.company.com`을 사용하지 마십시오.

머신 등록을 취소하려면

에이전트가 설치된 머신의 명령 프롬프트에서 다음 명령을 실행합니다.

```
<path to the registration tool> -o unregister
```

예

Windows

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -s mms -t
cloud --update
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p johnspassword
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://au1-cloud.company.com --token 3B4C-E967-4FBD
```

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o unregister
```

Linux

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -s mms -t cloud --
update
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o register -t cloud -a
https://eu2-cloud.company.com --token 34F6-8C39-4A5C
```

```
sudo "/usr/lib/Acronis/RegisterAgentTool/RegisterAgent" -o unregister
```

macOS

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -s mms -t cloud --update
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://cloud.company.com -u johndoe -p johnspassword
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o register -t cloud -a https://us5-cloud.company.com --token 9DBF-3DA9-4DAB
```

```
sudo "/Library/Application Support/BackupClient/Acronis/RegisterAgentTool/RegisterAgent"
-o unregister
```

특수 문자 또는 공백이 포함된 비밀번호

패스워드에 특수 문자나 공백이 포함된 경우, 명령줄에 입력할 때 처음과 끝에 인용 부호를 포함하십시오.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-p <"password">
```

예 (Windows용):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -p "johns password"
```

여전히 오류가 발생하는 경우:

- https://www.base64encode.org/에서 비밀번호를 base64 형식으로 암호화합니다.
- 명령줄에서 -b 또는 --base64 매개변수를 사용하여 암호화된 비밀번호를 지정합니다.

```
<path to the registration tool> -o register -t cloud -a <service address> -u <user name>
-b -p <encoded password>
```

예 (Windows용):

```
"%ProgramFiles%\BackupClient\RegisterAgentTool\register_agent.exe" -o register -t cloud
-a https://cloud.company.com -u johndoe -b -p am9obnNwYXNzd29yZA==
```

Agent for oVirt(가상 어플라이언스) 디플로이 중

Agent for oVirt(가상 어플라이언스)를 디플로이 및 구성하는 방법에 대한 자세한 내용은 Cyber Protection Cloud 설명서를 참조하십시오.

Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스) 디플로이

Agent for Virtuozzo Hybrid Infrastructure(가상 어플라이언스)를 디플로이 및 구성하는 방법에 대한 자세한 내용은 Cyber Protection Cloud 설명서를 참조하십시오.

머신 자동 검색

자동 검색을 사용하면 다음을 수행할 수 있습니다.

- Active Directory 도메인이나 로컬 네트워크의 머신을 감지하여 관리 서버에 머신을 등록하고 보호 에이전트를 설치하는 과정을 자동화할 수 있습니다.
- 여러 머신에서 보호 에이전트를 설치하고 업데이트할 수 있습니다.

- Active Directory와의 동기화를 사용합니다. 그러면 대형 Active Directory 도메인에서 머신을 관리하고 리소스를 프로비저닝하는 작업을 줄일 수 있습니다.

사전 요구 사항

자동 검색을 수행하려면 Active Directory 도메인이나 로컬 네트워크에 보호 에이전트가 설치된 머신이 하나 이상 있어야 합니다. 이 에이전트는 검색 에이전트로 사용됩니다.

중요

Windows 머신에 설치된 에이전트만 검색 에이전트로 사용할 수 있습니다. 환경 내에 검색 에이전트가 없으면 **장치 추가** 패널에서 **여러 장치** 옵션을 사용할 수 없습니다.

에이전트 원격 설치는 Windows를 실행하는 머신에 대해서만 지원됩니다(Windows XP는 지원되지 않음). Windows Server 2012 R2를 실행하는 머신에 에이전트를 원격 설치하려면 해당 머신에 Windows 업데이트 KB2999226이 설치되어 있어야 합니다.

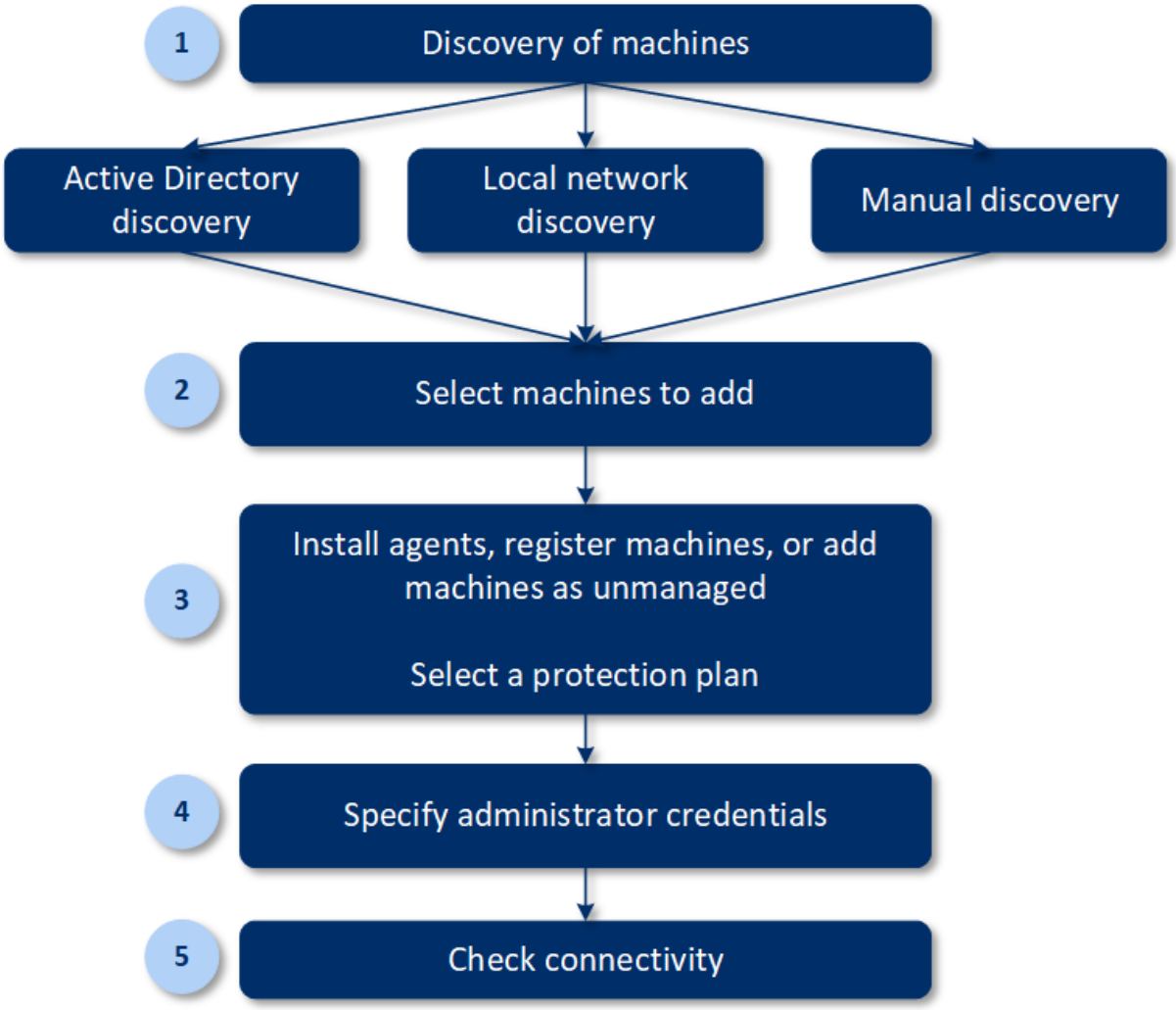
자동 검색의 작동 방식

검색 에이전트는 로컬 네트워크 검색 중에 NetBIOS 검색, WSD(웹 서비스 검색) 및 ARP(주소 확인 프로토콜) 테이블을 사용하여 네트워크 내의 각 머신에 대해 다음 정보를 수집합니다.

- 이름(짧은 이름/NetBIOS 호스트 이름)
- FQDN(정규화된 도메인 이름)
- 도메인/워크그룹
- IPv4/IPv6 주소
- MAC 주소
- 운영 체제(이름/버전/제품군)
- 머신 카테고리(워크스테이션/서버/도메인 컨트롤러)

Active Directory 검색 과정에서는 검색 에이전트가 위의 목록에 나와 있는 정보 외에 머신 OU(조직 구성 단위) 관련 정보, 그리고 머신의 이름과 운영 체제 관련 세부 정보도 수집합니다. 그러나 IP 주소와 MAC 주소는 수집하지 않습니다.

아래 다이어그램에 대략적인 자동 검색 프로세스가 나와 있습니다.



1. 검색 방법 선택:
   - Active Directory 검색
   - 로컬 네트워크 검색
   - 수동 검색 – 머신 IP 주소 또는 호스트 이름을 사용하거나 파일에서 머신 목록 가져오기

   보호 에이전트가 설치된 머신은 Active Directory 검색이나 로컬 네트워크 검색 결과에서 제외됩니다.

   수동 검색 중에는 기존 보호 에이전트가 업데이트 및 재등록됩니다. 에이전트가 등록되어 있는 것과 같은 계정을 사용하여 자동 검색을 수행하면 에이전트는 최신 버전으로 업데이트만 됩니다. 다른 계정을 사용하여 자동 검색을 수행하면 에이전트는 최신 버전으로 업데이트되어 해당 계정이 속한 테넌트에 재등록됩니다.
2. 테넌트에 추가할 머신을 선택합니다.
3. 해당 머신을 추가할 방법을 선택합니다.
   - 보호 에이전트와 추가 컴퍼넌트를 머신에 설치하고 웹 콘솔에서 등록합니다.
   - 보호 에이전트를 이미 설치한 경우에는 웹 콘솔에서 머신을 등록합니다.
   - 보호 에이전트를 설치하지 않고 머신을 **비관리 대상 머신**으로 웹 콘솔에 추가합니다.

보호 에이전트를 설치하거나 웹 콘솔에 등록하는 머신에 기존 보호 계획을 적용할 수도 있습니다.

4. 선택한 머신의 관리자 자격 증명을 입력합니다.
5. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다. 기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경우에는 IP 주소를 대신 선택해야 할 수 있습니다.
6. 입력한 자격 증명을 사용하여 머신에 연결할 수 있는지 확인합니다.

Cyber Protect 웹 콘솔에 표시되는 머신은 다음 카테고리에 속합니다.

- **검색됨** – 검색은 되었지만 보호 에이전트는 설치되지 않은 머신입니다.
- **관리 대상** – 보호 에이전트가 설치된 머신입니다.
- **보호되지 않음** – 보호 계획이 적용되어 있지 않은 머신입니다. 보호되지 않은 머신에는 보호 계획이 적용되지 않은 검색된 머신 및 관리 대상 상태의 머신이 모두 포함됩니다.
- **보호됨** – 보호 계획이 적용된 머신입니다.

자동 검색 및 수동 검색

검색을 시작하기 전 사전 요구 사항이 충족되었는지 확인합니다.

머신을 검색하려면

1. 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. **추가**를 클릭합니다.
3. **여러 개의 장치**에서 **Windows 전용**을 클릭합니다. 검색 마법사가 열립니다.
4. [조직 단위가 있는 경우] 단위를 선택합니다. 그러면 **검색 에이전트**에서 선택한 단위 및 하위 단위와 관련된 에이전트를 선택할 수 있습니다.
5. 머신을 감지하기 위해 스캔을 수행할 검색 에이전트를 선택합니다.
6. 검색 방법 선택:
   - **Active Directory 검색** 검색 에이전트가 설치된 머신이 Active Directory 도메인 멤버여야 합니다.
   - **로컬 네트워크 스캔** 선택한 검색 에이전트에서 머신을 찾지 못한 경우 다른 검색 에이전트를 선택합니다.
   - **수동으로 지정 또는 파일에서 가져오기** 추가할 머신을 수동으로 정의하거나 텍스트 파일에서 가져옵니다.
7. [Active Directory 검색 방법을 선택한 경우] 머신 검색 방법 선택:
   - **조직 단위 목록에서** 추가될 머신 그룹을 선택합니다.
   - **LDAP 언어 쿼리에 따라** LDAP 언어 쿼리를 사용해 머신을 선택합니다. **검색 베이스**는 검색할 곳을 정의하고, **필터**를 사용해 머신 선택의 기준을 지정합니다.
8. [Active Directory 또는 로컬 네트워크 검색 방법을 선택한 경우] 목록을 사용해 추가하려는 머신을 선택합니다.

[수동 검색 방법을 선택한 경우] 머신의 IP 주소 또는 호스트 이름을 지정하거나 텍스트 파일의 머신 목록에서 가져옵니다. 파일은 한 행에 하나씩 IP 주소/호스트 이름을 포함하고 있어야 합니다. 파일 예시:

```
156.85.34.10
156.85.53.32
156.85.53.12
EN-L00000100
EN-L00000101
```

머신 주소를 수동으로 추가하거나 파일에서 가져오면, 에이전트는 추가된 머신을 핑하고 가용성을 정의하려 시도합니다.

9. 검색 후 수행할 작업을 선택합니다.
   - **에이전트 설치 및 머신 등록 컴퍼넌트 선택**을 클릭해 머신에 설치할 컴퍼넌트를 선택할 수 있습니다. 자세한 내용은 "설치할 컴퍼넌트 선택"을 참조하십시오. 에이전트를 동시에 최대 100개까지 설치할 수 있습니다.

     컴퍼넌트 선택 화면에서 **에이전트 서비스를 위한 로그온 계정**을 지정해 서비스를 실행할 계정을 정의합니다. 다음 중 하나를 선택합니다.
     - **서비스 사용자 계정 사용**(에이전트 서비스용 기본값)

       서비스 사용자 계정은 서비스를 실행하는 데 사용되는 Windows 시스템 계정입니다. 이 설정의 이점은 도메인 보안 정책이 이 계정의 사용자 권한에 영향을 미치지 않는다는 점입니다. 기본적으로 에이전트는 **로컬 시스템** 계정 하에서 실행됩니다.
     - **새 계정 생성**

       계정 이름은 해당 에이전트에 대해 Agent User로 지정됩니다.
     - **다음 계정 사용**

       도메인 컨트롤러에 에이전트를 설치하는 경우 시스템에 각 에이전트의 기존 계정(또는 동일한 계정)을 지정하라는 메시지가 표시됩니다. 보안상의 이유로 시스템은 도메인 컨트롤러에서 새 계정을 자동으로 생성하지 않습니다.

     새 계정 생성 또는 **다음 계정 사용** 옵션을 선택하는 경우 도메인 보안 정책이 관련 계정의 권한에 영향을 미치지 않는지 확인하십시오. 설치 중 계정에 할당되어 있는 사용자 권한이 박탈되는 경우 컴퍼넌트가 올바로 작동하지 않거나 아예 작동하지 않을 수 있습니다.
   - **설치된 에이전트로 머신 등록** 에이전트가 이미 머신에 설치되어 있으며 Cyber Protect에 등록하기만 하면 되는 경우 이 옵션을 사용합니다. 머신에서 에이전트를 찾을 수 없으면 **관리되지 않는** 머신으로 추가됩니다.
   - **관리되지 않는 머신으로 추가** 에이전트가 머신에 설치되지 않습니다. 웹 콘솔에서 확인할 수 있으며 나중에 에이전트를 설치 또는 등록할 수 있습니다.

   [**에이전트 설치 및 머신 등록** 검색 후 작업이 선택된 경우] **필요할 때 머신을 자동으로 시작합니다.** – 이 옵션이 활성화되어 있으면 머신이 설치를 완료하기 위해 필요한 만큼 다시 시작됩니다.

   다음의 경우 머신을 다시 시작해야 할 수 있습니다.
   - 사전 요구 사항 설치가 완료되었고 설치를 계속하기 위해 다시 시작해야 하는 경우
   - 설치가 완료되었지만 설치 중 일부 파일이 잠겨 다시 시작해야 하는 경우
   - 설치가 완료되었지만 이전에 설치된 다른 소프트웨어에서 다시 시작을 요구하는 경우

[필요할 때 머신을 자동으로 시작합니다.가 선택된 경우] **사용자 로그인 시 다시 시작하지 않음** – 이 옵션이 활성화되어 있으면 사용자가 시스템에 로그인한 상태에서는 머신이 자동으로 다시 시작되지 않습니다. 예를 들어 사용자가 작업 중이며 설치 과정에서 다시 시작이 필요한 경우 시스템은 다시 시작되지 않습니다.

사전 요구 사항이 설치되었으나 사용자가 로그인한 상태라 재부팅이 이루어지지 않은 경우, 에이전트 설치를 완료하려면 머신을 재부팅하고 설치를 다시 시작해야 합니다.

에이전트가 설치되었으나 재부팅이 이루어지지 않은 경우 머신을 재부팅해야 합니다.

[조직에 부서가 있는 경우] **머신을 등록할 부서** – 머신을 등록할 부서를 선택합니다.

처음에 있는 두 가지의 검색 후 작업 중 하나를 선택한 경우 머신에 보호 계획을 적용하기 위한 옵션도 있습니다. 보호 계획이 여러 개 있는 경우 하나를 선택할 수 있습니다.

10. 모든 머신에 대한 관리자 권한이 있는 사용자의 자격 증명을 지정합니다.

중요

에이전트의 원격 설치는 기본 제공 관리자 계정(운영 체제 설치 시 생성한 첫 번째 계정)의 자격 증명을 지정한 경우에만 아무런 준비 과정 없이 작동합니다. 사용자 정의 관리자 자격 증명을 정의하려는 경우 Windows를 실행 중인 머신 추가 > 준비에 설명되어 있는 대로 추가적인 수동 준비 작업을 수행해야 합니다.

11. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다.

    기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경우에는 IP 주소를 대신 선택해야 할 수 있습니다.

12. 시스템은 모든 머신의 연결을 확인합니다. 연결되지 않는 일부 머신에 대한 자격 증명을 변경할 수 있습니다.

머신 검색이 시작되면 **대시보드** > **활동** > **머신 검색** 활동에서 해당하는 작업을 찾을 수 있습니다.

설치할 컴퍼넌트 선택

아래 표에서 필수 및 추가 컴퍼넌트에 대한 설명을 찾아볼 수 있습니다.

구성 요소	설명
필수 컴퍼넌트	
Agent for Windows	이 에이전트는 디스크, 볼륨, 파일을 백업하며 Windows 머신에 설치됩니다. 언제나 설치되는 항목으로 선택이 가능하지 않습니다.
추가 컴퍼넌트	
Agent for Hyper-V	이 에이전트는 Hyper-V 가상 머신을 백업하며, Hyper-V 호스트에 설치됩니다. 선택되었으며 머신에서 Hyper-V 역할이 감지된 경우 설치됩니다.
Agent for SQL	이 에이전트는 SQL Server 데이터베이스를 백업하며, Microsoft SQL Server를 실행하는 머신에 설치됩니다. 선택되었으며 머신에서 애

	플리케이션이 감지된 경우 설치됩니다.
Agent for Exchange	이 에이전트는 Exchange 데이터베이스를 백업하며, Microsoft Exchange Server의 사서함 역할을 실행하는 머신에 설치됩니다. 선택되었으며 머신에서 애플리케이션이 감지된 경우 설치됩니다.
Agent for Active Directory	이 에이전트는 Active Directory 도메인 서비스의 데이터를 백업하며, 도메인 컨트롤러에 설치됩니다. 선택되었으며 머신에서 애플리케이션이 감지된 경우 설치됩니다.
Agent for VMware(Windows)	이 에이전트는 VMware 가상 머신을 백업하며, vCenter Server에 대한 네트워크 액세스가 있는 Windows 머신에 설치됩니다. 선택된 경우 설치됩니다.
Agent for Office 365	이 에이전트는 Microsoft 365 사서함을 로컬 대상에 백업하며, Windows 머신에 설치됩니다. 선택된 경우 설치됩니다.
Agent for Oracle	이 에이전트는 Oracle 데이터베이스를 백업하며, Oracle 데이터베이스를 실행하는 머신에 설치됩니다. 선택된 경우 설치됩니다.
Cyber Protect 모니터	이 컴퍼넌트는 사용자가 알림 영역에서 실행 중인 작업의 실행을 모니터링할 수 있게 지원하며, Windows 머신에 설치됩니다. 선택된 경우 설치됩니다.
명령줄 도구	Cyber Protect에서는 acrocmd 유틸리티의 명령줄 인터페이스를 지원합니다. acrocmd에는 명령을 실제로 실행하는 도구가 포함되지 않습니다. 이 유틸리티는 Cyber Protect 컴퍼넌트(에이전트 및 관리 서버)의 명령줄 인터페이스만 제공합니다. 선택된 경우 설치됩니다.
Bootable Media Builder	이 컴퍼넌트는 사용자가 부트 가능한 미디어를 생성할 수 있도록 지원하며, Windows 머신에 설치됩니다.

검색된 머신 관리

검색 프로세스를 수행하고 나면 검색된 머신을 모두 **장치** > **관리되지 않는 머신**에서 찾을 수 있습니다.

이 섹션은 사용한 검색 방법에 따라 하위 섹션으로 나누어져 있습니다. 머신 매개변수의 전체 목록은 아래 표시됩니다(검색 방법에 따라 다를 수 있음).

이름	설명
이름	머신의 이름입니다. 머신의 이름을 찾을 수 없는 경우 IP 주소가 표시됩니다.
IP 주소	머신의 IP 주소입니다.
검색 유형	머신을 감지하는 데 사용된 검색 방법입니다.
조직 단위	머신이 속한 Active Directory 내 조직 단위입니다. 이 열은 **관리되지**

	않는 머신 > **Active Directory**에서 머신 목록을 보는 경우 표시됩니다.
운영 체제	머신에 설치된 운영 체제입니다.

예외 섹션에는 검색 프로세스에서 건너뛰어야 할 머신을 추가할 수 있습니다. 검색하지 않아도 될 특정 머신이 있다면 이 목록에 추가하면 됩니다.

머신을 **예외**에 추가하려면 목록에서 해당 머신을 선택한 다음 **예외에 추가**를 클릭합니다. 머신을 **예외**에서 제거하려면 **관리되지 않는 머신** > **예외**로 이동한 다음 해당 머신을 선택하고 **예외에서 제거**를 클릭합니다.

보호 에이전트를 설치하고 검색된 머신 배치를 Cyber Protect에 등록하려면 목록에서 이를 선택한 다음, **설치 및 등록**을 클릭합니다. 보호 계획을 머신 배치에 할당할 수 있게 해주는 마법사가 열립니다.

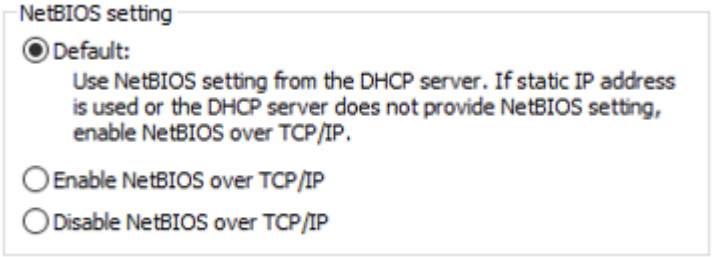
보호 에이전트를 머신에 설치하고 나면 해당 머신이 **장치** > **에이전트가 있는 머신** 섹션에 표시됩니다.

보호 상태를 확인하려면 **대시보드** > **개요**로 이동해 보호 상태 위젯 또는 검색된 머신 위젯을 추가합니다.

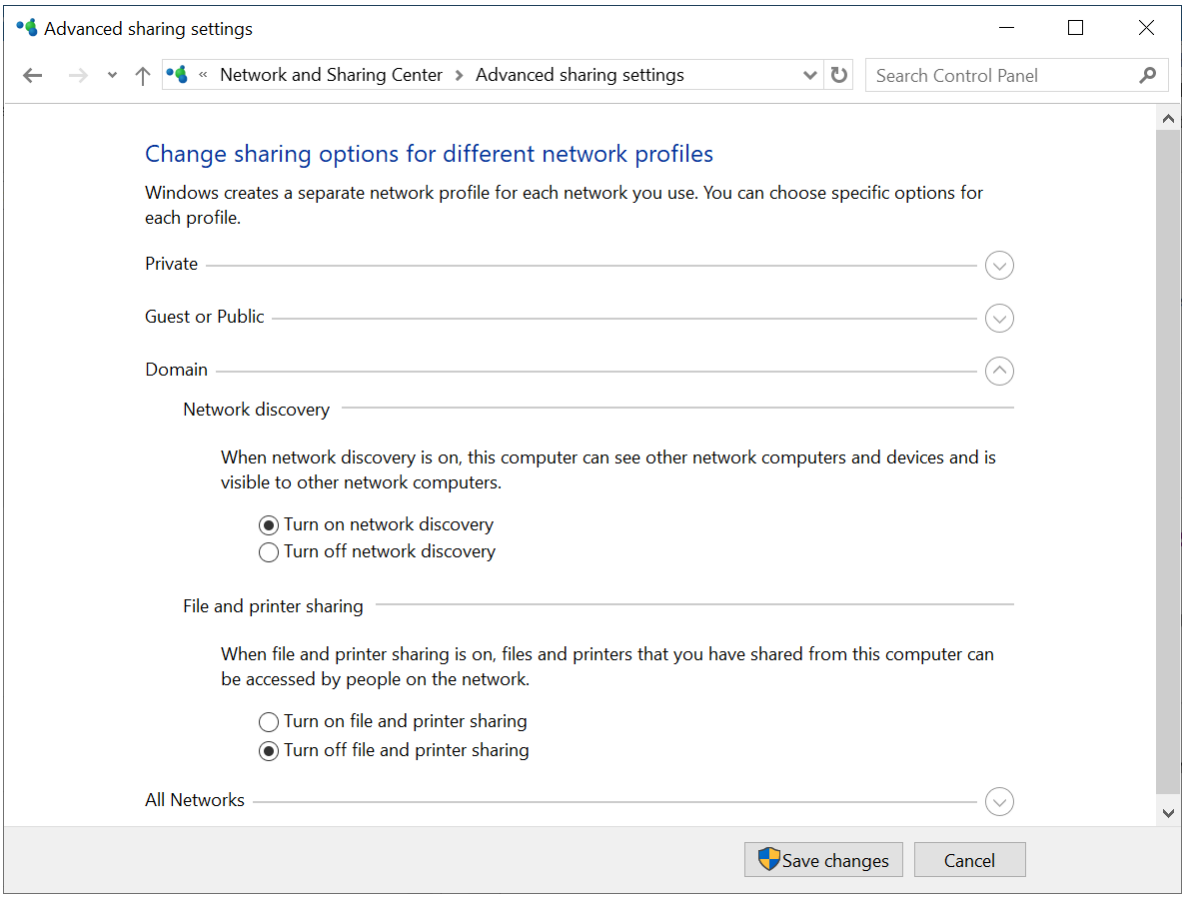
문제 해결

자동 검색 기능에 문제가 있다면 다음을 확인합니다.

- TCP/IP 상에서 NetBIOS 사용이 활성화되어 있거나 기본값으로 설정되어 있는지 확인합니다.



- **제어판** >**네트워크 및 공유 센터** > **고급 공유 설정 변경**에서 네트워크 검색을 켭니다.



- 검색을 수행하는 머신과 검색될 머신에서 **Function Discovery Provider Host** 서비스가 구동되고 있는지 확인합니다.
- 검색될 머신에서 **Function Discovery Resource Publication** 서비스가 구동되고 있는지 확인합니다.

OVF 템플릿으로 Agent for VMware(가상 어플라이언스) 배포

시작하기 전에

에이전트에 대한 시스템 요구사항

가상 어플라이언스는 기본값으로 대다수 작업에 최적의 상태로 실행되는 RAM 4GB, 2vCPU가 할당됩니다. 백업 트래픽 대역폭이 초당 100MB 초과가 예상되는 경우(예, 10 Gbit 네트워크) 백업 성능 개선을 위해 RAM 8GB, 4vCPU로 리소스를 늘리는 방법을 권장합니다.

어플라이언스 자체 가상 디스크가 차지하는 공간은 6GB 이하입니다. 씩 또는 씬 디스크 포맷은 문제가 되지 않습니다. 어플라이언스 성능에 영향을 주지 않습니다.

참고
가상 머신 백업을 활성화하려면 vStorage API를 ESXi 호스트에 설치해야 합니다.
https://kb.acronis.com/content/14931을 참조하십시오.

필요한 에이전트 수는?

가상 어플라이언스 한 대는 전체 vSphere 환경을 보호할 수 있지만, vSphere당(또는 클러스터가 없을 경우 호스트당) 가상 어플라이언스를 한 대 디플로이하는 것이 모범 사례입니다. 이 어플라이언스는 HotAdd 전송을 사용하여 백업된 디스크에 연결할 수 있고, 따라서 백업 트래픽이 하나의 로컬 디스크에서 다른 디스크로 향하기 때문에 이는 신속한 백업을 보장합니다.

동일한 vCenter Server 에 연결되거나 다른 ESXi 호스트에 연결되는 경우 가상 어플라이언스와 Agent for VMware (Windows)를 동시에 사용하는 것이 일반적입니다. 한 에이전트가 ESXi에 직접 연결되고 다른 에이전트가 이 ESXi를 관리하는 vCenter Server에 연결되는 사례를 피합니다.

에이전트가 2명 이상인 경우 로컬로 연결되는 스토리지 사용은 권장하지 않습니다(즉, 가상 어플라이언스에 추가되는 가상 디스크에 백업 저장). 자세한 검토는 "로컬로 연결된 스토리지 사용"를 참조하십시오.

에이전트 자동 DRS 비활성화

가상 어플라이언스가 vSphere 클러스터에 디플로이되면 자동 vMotion을 비활성화해야 합니다. 클러스터 DRS 설정에서 개별 가상 머신 자동화 수준을 활성화하고, **비활성화**할 가상 어플라이언스에 대한 **자동화 수준**을 설정합니다.

OVF 템플릿 디플로이

OVF 템플릿의 위치

OVF 템플릿에는 .ovf 파일 한 개와 .vmdk 파일 두 개가 포함되어 있습니다.

온프레미스 디플로이에서

관리 서버가 설치된 후 가상 어플라이언스의 OVF 패키지가 Windows의 경우에는 **%ProgramFiles%\Acronis\ESXAppliance** 폴더에, Linux의 경우에는 **/usr/lib/Acronis/ESXAppliance** 폴더에 저장됩니다.

클라우드 배포에서는

1. **모든 장치** > **추가** > **VMware ESXi** > **가상 어플라이언스(OVF)**를 클릭합니다.
   .Zip 아카이브가 귀하의 머신에 다운로드됩니다.
2. .zip 아카이브의 압축을 풉니다.

OVF 템플릿 디플로이

1. OVF 템플릿 파일들이 vSphere Client를 실행하는 머신에서 액세스 가능한지 확인하십시오.
2. vSphere Client를 시작하고 vCenter Server에 로그온합니다.
3. OVF 템플릿을 디플로이합니다.
   - 스토리지를 구성할 때 존재하는 경우에는 공유 데이터 저장소를 선택합니다. 씩 또는 씬 디스크 포맷은 어플라이언스 성능에 영향을 주지 않기 때문에 문제가 되지 않습니다.
   - 클라우드 배포에 네트워크 연결을 구성할 때는 에이전트 자체가 클라우드에 제대로 등록될 수 있도록 인터넷 연결이 가능한 네트워크를 선택해야 합니다. 온프레미스 디플로이에 네트워크 연결을 구성할 때는 관리 서버가 포함된 네트워크를 선택하십시오.

가상 어플라이언스 구성

1. **가상 어플라이언스 시작**

   vSphere 클라이언트에서 **인벤토리**를 표시하고 가상 어플라이언스의 이름을 마우스 오른쪽 단추로 클릭한 다음 **전원** > **전원 켜기**를 선택합니다. **콘솔** 탭을 선택합니다.
2. **프록시 서버**

   프록시 서버가 네트워크에서 활성화되면:
   a. 명령 셸을 시작하려면 가상 어플라이언스 UI에서 CTRL+SHIFT+F2를 누르십시오.
   b. 텍스트 편집기에서 **/etc/Acronis/Global.config** 파일을 엽니다.
   c. 다음 중 하나를 수행하십시오.
      - 에이전트 설치 중에 프록시 설정을 지정한 경우 다음 섹션을 참조하십시오.

        ```
        <key name="HttpProxy">
            <value name="Enabled" type="Tdword">"1"</value>
            <value name="Host" type="TString">"ADDRESS"</value>
            <value name="Port" type="Tdword">"PORT"</value>
            <value name="Login" type="TString">"LOGIN"</value>
            <value name="Password" type="TString">"PASSWORD"</value>
        </key>
        ```

      - 그렇지 않으면 위의 행을 복사하고 파일에서 `<registry name="Global">...</registry>` 태그 사이에 붙여넣습니다.
   d. 주소를 프록시 서버 호스트 이름/IP 주소로 대체하고 포트는 포트 번호의 10진수 값으로 대체합니다.
   e. 프록시 서버에 인증이 필요하다면 로그인 및 비밀번호를 프록시 서버 자격 증명으로 대체합니다. 그렇지 않은 경우, 파일에서 이 라인을 삭제합니다.
   f. 파일을 저장합니다.
   g. 텍스트 편집기에서 **/opt/acronis/etc/aakore.yaml** 파일을 엽니다.
   h. **env** 섹션을 찾거나 생성한 후, 다음 행을 추가합니다.

      ```
      env:
       http-proxy: proxy_login:proxy_password@proxy_address:port
       https-proxy: proxy_login:proxy_password@proxy_address:port
      ```

i. `proxy_login`과 `proxy_password`는 프록시 서버 자격 증명으로, `proxy_address:port`는 프록시 서버의 주소와 포트 번호로 대체합니다.

j. **reboot** 명령을 실행합니다.

그렇지 않은 경우 이 단계를 건너뜁니다.

3. **네트워크 설정**

   에이전트의 네트워크 연결은 동적 호스트 구성 프로토콜(DHCP)을 사용하여 자동으로 구성됩니다. 기본 구성을 변경하려면 **에이전트 옵션**의 **eth0**에서 **변경**을 클릭한 후 원하는 네트워크 설정을 지정합니다.

4. **vCenter/ESX(i)**

   에이전트 옵션 아래 **vCenter/ESX(i)**에서 **변경**을 클릭하고 vCenter Server 이름 또는 IP 주소를 지정합니다. 에이전트는 vCenter Server가 관리하는 가상 머신을 백업 및 복구할 수 있습니다.

   vCenter Server를 사용하지 않는 경우에는 가상 머신을 백업 및 복구할 ESXi 호스트의 이름 또는 IP 주소를 지정합니다. 일반적으로 에이전트가 호스트에서 호스팅되는 가상 머신을 백업할 때 백업 실행 속도가 더 빠릅니다.

   에이전트가 vCenter Server 또는 ESXi에 연결하기 위해 사용할 자격 증명을 지정합니다. **관리자** 역할이 할당된 계정을 사용하는 것이 좋습니다. 또는 vCenter Server 또는 ESXi에서 필수 권한이 있는 계정을 제공합니다.

   연결 확인을 클릭하여 액세스 자격 증명이 올바른지 확인할 수 있습니다.

5. **관리 서버**

   a. **에이전트 옵션**의 **관리 서버**에서 **변경**을 클릭합니다.

   b. **서버 이름/IP**에서 다음 중 하나를 수행합니다.

   - 온프레미스 디플로이의 경우 **로컬**을 선택합니다. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   - 클라우드 배포의 경우 **클라우드**를 선택합니다. 소프트웨어에 사이버 보호 서비스 주소가 표시됩니다. 별도의 지시가 없는 한, 이 주소는 변경하지 마십시오.

   c. **사용자 이름** 및 **비밀번호**에서 다음 중 하나를 수행합니다.

   - 온프레미스 디플로이의 경우, 관리 서버 관리자의 사용자 이름과 비밀번호를 지정합니다.
   - 클라우드 디플로이의 경우, 사이버 보호 서비스를 위한 사용자 이름과 비밀번호를 지정합니다. 에이전트와 에이전트가 관리하는 가상 머신은 이 계정에 등록됩니다.

6. **시간대**

   가상 머신의 **시간대**에서 **변경**을 클릭합니다. 예정된 작업이 적절한 시간에 실행될 수 있도록 사용자 지역의 시간대를 선택합니다.

7. **[선택 사항]로컬 스토리지**

   가상 어플라이언스에 추가 디스크를 연결하여 로컬로 연결된 이 스토리지에 Agent for VMware를 백업할 수 있습니다.

   가상 머신의 설정을 편집하여 디스크를 추가하고 **새로 고침**을 클릭합니다. **스토리지 생성** 링크를 사용할 수 있습니다. 이 링크를 클릭하고 디스크를 선택한 다음 디스크 레이블을 지정합니다.

Agent for Scale Computing HC3(가상 어플라이언스) 배포 중

시작하기 전에

이 어플라이언스는 Scale Computing HC3 클러스터에 디플로이하는 미리 구성된 가상 머신입니다. 클러스터의 모든 가상 머신에 대한 사이버 보호를 관리할 수 있게 해주는 보호 에이전트를 포함합니다.

에이전트에 대한 시스템 요구사항

가상 어플라이언스를 디플로이할 때 vCPU 및 RAM 조합 중에 선택할 수 있습니다. vCPU 2개 및 RAM 4GiB가 대다수 작업에 최적의 상태로 실행되는 조합입니다. 백업 트래픽 대역폭이 초당 100MB를 초과할 것으로 예상되는 경우(예: 10GBit 네트워크) 백업 성능 개선을 위해 RAM 8GiB, vCPU 4개로 리소스를 늘리는 방법을 권장합니다.

어플라이언스 자체 가상 디스크가 차지하는 공간은 6GB 이하입니다.

필요한 에이전트 수는?

한 개의 에이전트가 전체 클러스터를 보호할 수 있습니다. 그러나 백업 트래픽 대역폭 로드를 분배해야 할 경우 한 클러스터에 여러 개의 에이전트를 보유할 수 있습니다.

한 클러스터에 여러 개의 에이전트가 있을 경우 가상 머신은 자동으로 에이전트 사이에 동등하게 분배되기 때문에 각 에이전트는 같은 수의 머신을 관리하게 됩니다.

에이전트 간 로드 불균형이 20%에 도달하면 자동 재분배가 수행됩니다. 예를 들어, 머신이나 에이전트가 추가 또는 제거되는 경우 수행될 수 있습니다. 예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 클러스터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. 관리 서버는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다. 관리 서버에서 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 배포됩니다. 그러나 에이전트가 손상되거나 Scale Computing HC3 클러스터에서 수동으로 삭제된 경우에는 수행되지 않습니다. Cyber Protect 웹 인터페이스에서 해당 에이전트를 제거한 후에만 재분배가 시작됩니다.

다음 위치에서 자동 배포의 결과를 볼 수 있습니다.

- **모든 장치** 섹션의 각 가상 머신에 대한 **에이전트** 열
- 에이전트가 **설정** > **에이전트**에서 선택된 경우 **상세정보** 패널의 **할당된 가상 머신** 섹션

가상 어플라이언스 디플로이

1. Cyber Protect 계정에 로그인합니다.
2. **장치** > **모든 장치** > **추가** > **Scale Computing HC3**을 클릭합니다.
3. 디플로이할 가상 어플라이언스 수를 선택합니다.
4. Scale Computing HC3 클러스터의 IP 주소 또는 호스트 이름을 지정합니다.

5. 이 클러스터에 **VM 생성/편집** 역할이 할당된 계정의 자격 증명을 지정합니다.
6. 가상 어플라이언스에 대한 이미지 파일의 임시 스토리지에 사용할 네트워크 공유를 지정합니다. 최고 2GB의 공간이 필요합니다.
7. 이 네트워크 공유에 대해 읽기 및 쓰기 권한이 있는 계정의 자격 증명을 지정합니다.
8. **디플로이**를 클릭합니다.

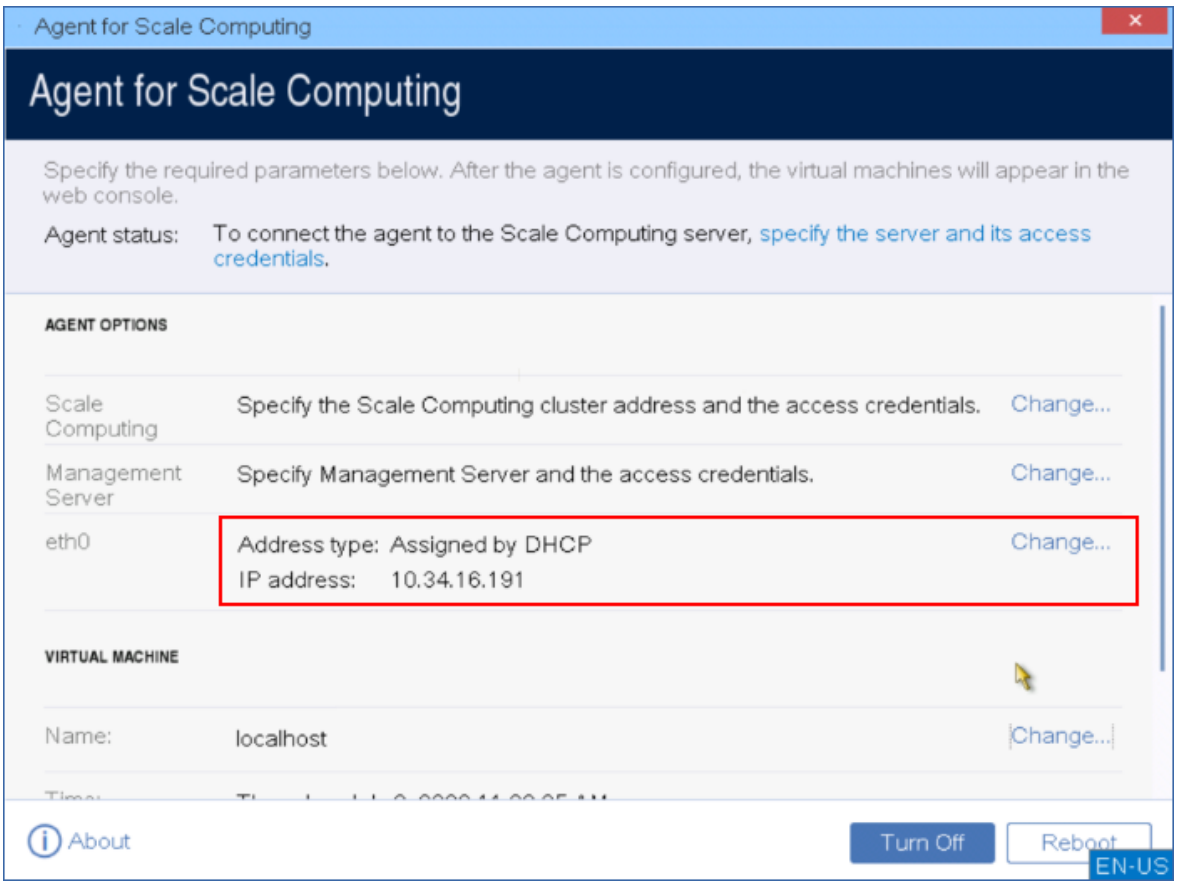
디플로이가 완료되면, 가상 어플라이언스 구성을 합니다.

가상 어플라이언스 구성

가상 어플라이언스를 디플로이한 뒤 어플라이언스가 보호해야 하는 Scale Computing HC3 클러스터와 Cyber Protect 관리 서버에 모두 연결할 수 있도록 어플라이언스를 구성해야 합니다.

가상 어플라이언스을 구성하려면

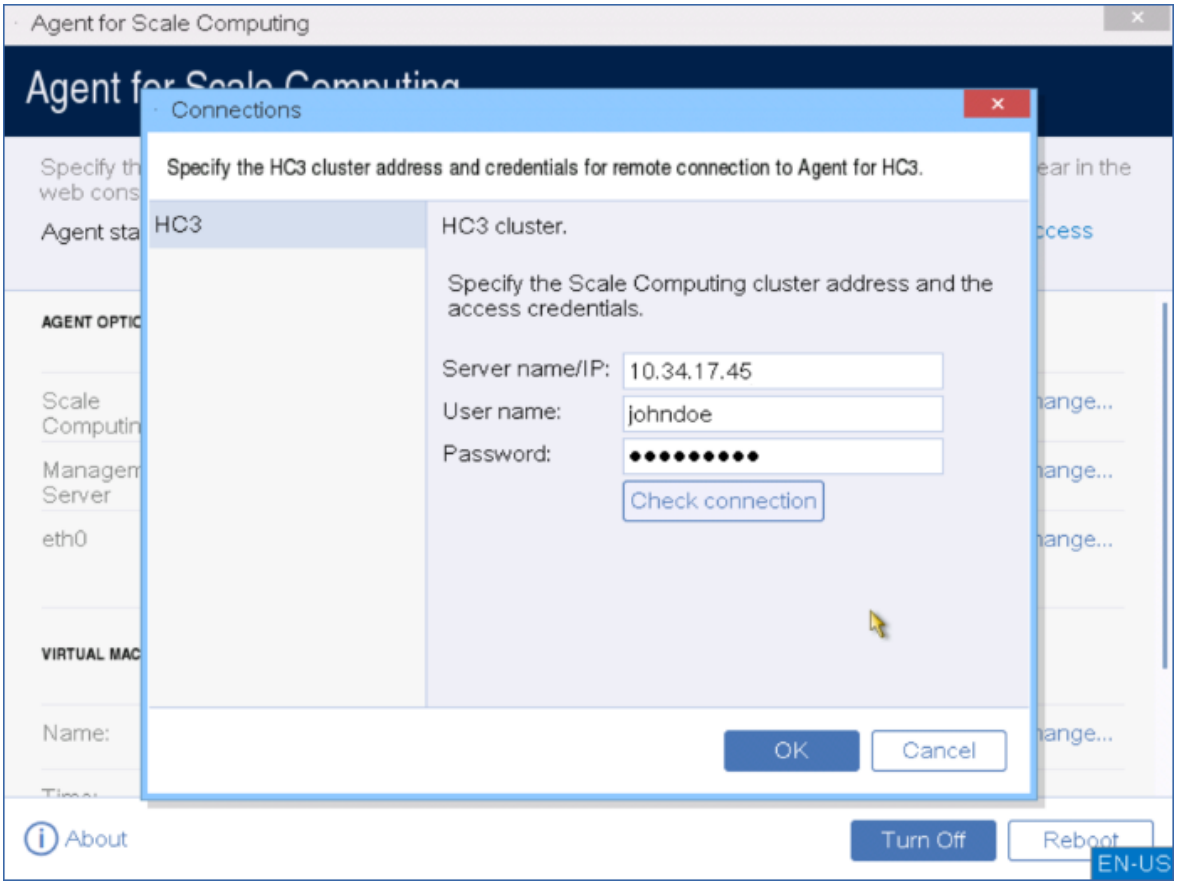
1. Scale Computing HC3 계정에 로그인합니다.
2. 구성해야 할 에이전트가 있는 가상 머신을 선택한 뒤, **콘솔**을 클릭합니다.
3. 어플라이언스의 네트워크 인터페이스를 구성합니다. 어플라이언스가 사용하는 네트워크의 수에 따라 한 개 이상의 인터페이스를 구상해야 할 수 있습니다. 자동으로 할당된 DHCP 주소(있는 경우)가 가상 머신이 사용하는 네트워크 내에서 유효한지 확인하거나 수동으로 할당하십시오.



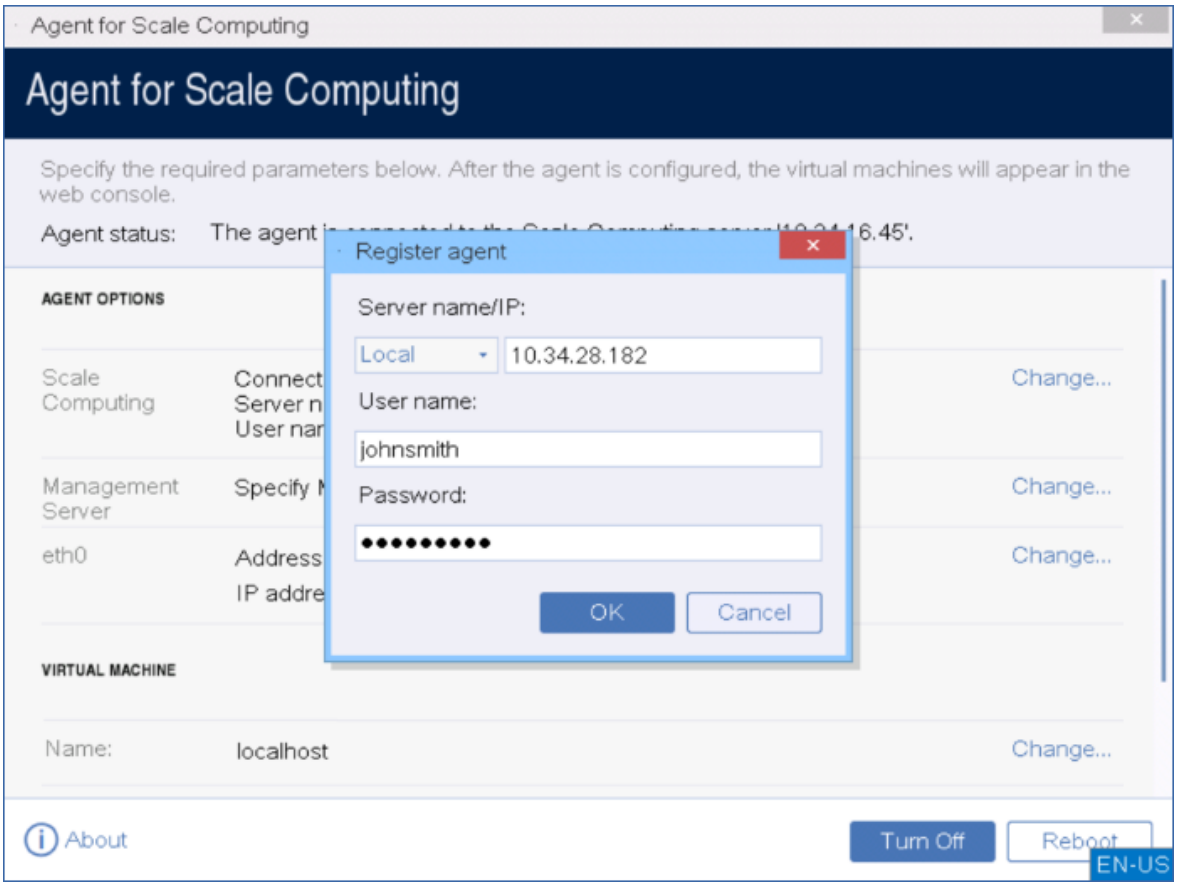
4. Scale Computing HC3 클러스터 주소 및 자격 증명을 지정하십시오.

- 클러스터의 DNS 이름 또는 IP 주소.
- 여기에서 **사용자 이름** 및 **패스워드** 필드에는 적합한 역할이 할당된 Scale Computing HC3 사용자 계정의 자격 증명을 입력합니다.

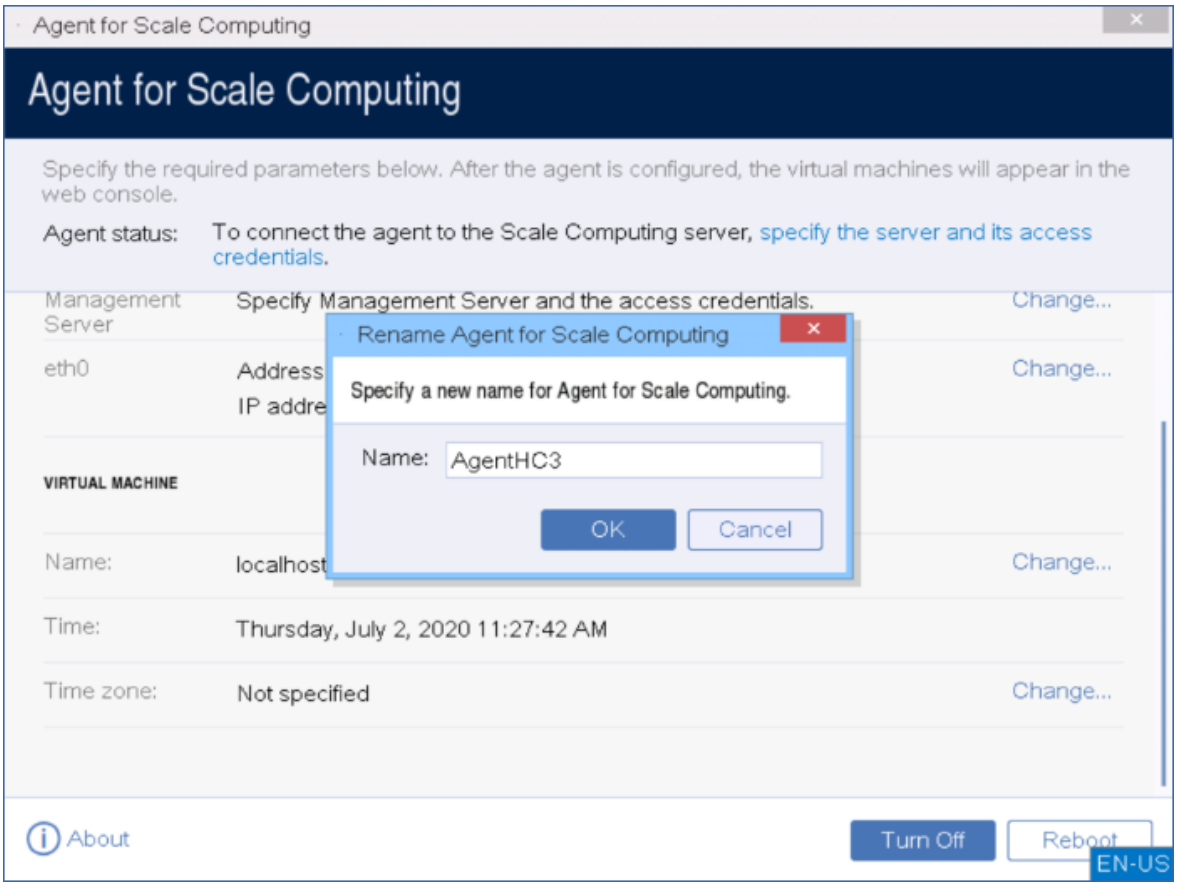
연결 확인을 클릭하여 액세스 자격 증명이 올바른지 확인할 수 있습니다.



5. Cyber Protect 관리 서버 주소와 이를 액세스하기 위한 자격 증명을 지정합니다.



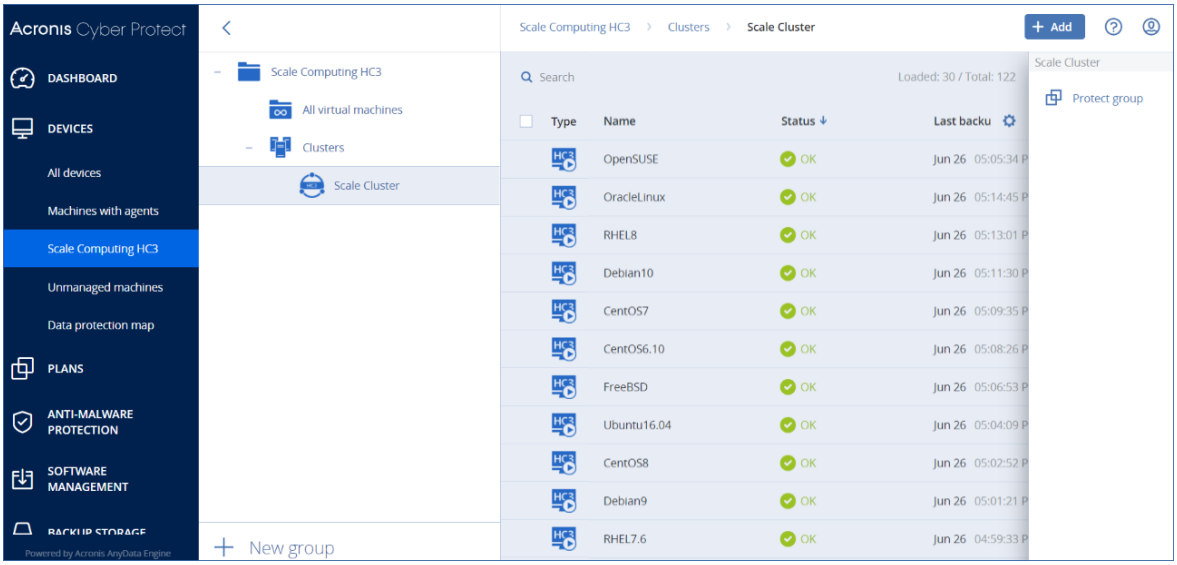
6. [선택 사항] 에이전트의 이름을 지정합니다. 이 이름은 Cyber Protect 웹 콘솔에 표시됩니다.



7. [선택 사항] 예정된 작업이 적절한 시간에 실행될 수 있도록 사용자 지역의 시간대를 선택합니다.

Scale Computing HC3 클러스터의 가상 머신을 보호하는 방법

1. Cyber Protect 계정에 로그인합니다.
2. **장치** > **Scale Computing HC3** > <사용자 클러스터>로 이동하거나 **장치** > **모든 장치**에서 머신을 확인할 수 있습니다.
3. 원하는 머신을 선택하고 보호 계획을 적용합니다.



Agent for Scale Computing HC3 – 필요한 역할

이 섹션은 Scale Computing HC3 가상 머신 작업과 추가적으로 가상 어플라이언스 디플로이에 필요한 역할에 대해 설명합니다.

작업	역할
가상 머신을 백업합니다	백업 VM 생성/편집 VM 삭제
기존 가상 머신으로 복구	백업 VM 생성/편집 VM 전원 제어 VM 삭제 클러스터 설정
새 가상 머신으로 복구	백업 VM 생성/편집 VM 전원 제어 VM 삭제 클러스터 설정
가상 어플라이언스 디플로이	VM 생성/편집

그룹 정책을 통해 에이전트 배포

그룹 정책을 사용하여 Active Directory 도메인의 구성원인 머신에 Agent for Windows를 중앙에서 설치(또는 배포)할 수 있습니다.

이 섹션에서는 전체 도메인 또는 도메인의 조직 단위에서 머신에 에이전트를 배포하도록 그룹 정책 개체를 설정하는 방법에 대해 알아봅니다.

머신이 도메인에 로그온할 때마다 결과적인 그룹 정책 개체는 에이전트가 설치 및 등록되어 있는지 확인합니다.

사전 요구 사항

에이전트 배포를 계속해서 진행하기 전에 다음 내용을 확인합니다.

- Microsoft Windows Server 2003 이상에서 실행 중인 도메인 컨트롤러와 함께 Active Directory 도메인이 있습니다.
- 도메인 내에서 **도메인 관리자** 그룹의 구성원입니다.

- **Windows에 설치할 모든 에이전트** 설치 프로그램을 다운로드했습니다. 웹 콘솔의 **장치 추가** 페이지에서 다운로드 링크를 사용할 수 있습니다.

1단계: 등록 토큰 생성

등록 토큰은 사용자의 로그인 및 패스워드를 Cyber Protect 웹 콘솔에 저장하지 않고 설정 프로그램에 사용자 ID를 전달합니다. 이를 통해 사용자 계정에 개수에 상관없이 여러 머신을 등록할 수 있습니다. 보안 강화를 위해 토큰의 수명이 제한되어 있습니다.

등록 토큰을 생성하려면

1. 머신을 할당해야 하는 계정의 자격 증명을 사용하여 Cyber Protect 웹 콘솔에 로그인합니다.
2. **모든 장치** > **추가**를 클릭합니다.
3. **등록 토큰**으로 스크롤을 내린 다음 **생성**을 클릭합니다.
4. 토큰 수명을 지정한 다음 **토큰 생성**을 클릭합니다.
5. 토큰을 복사하거나 기록해 두십시오. 나중에 필요할 수 있으니 토큰을 저장해 두십시오.
   활성 토큰 관리를 클릭해 이미 생성된 토큰을 보고 관리할 수 있습니다. 보안상 이 표에는 토큰 값 전체가 표시되지는 않습니다.

2단계: .mst 변환 생성 및 설치 패키지 추출

1. 도메인의 머신에서 관리자로 로그인합니다.
2. 설치 패키지를 저장할 공유 폴더를 생성합니다. 도메인 사용자가 공유 폴더에 액세스할 수 있는지 확인합니다. 예를 들어, 기본 공유 설정을 **모든 사람**으로 남겨둘 수 있습니다.
3. 설치 프로그램을 시작합니다.
4. **무인 설치를 위해 .mst 및 .msi 파일 생성**을 클릭합니다.
5. .mst 파일에 추가될 설치 설정을 검토하거나 수정합니다. 관리 서버 연결 방법을 지정할 때에는 **등록 토큰 사용**을 선택한 다음 생성한 토큰을 입력합니다.
6. **진행**을 클릭합니다.
7. **파일 저장 위치**에서 생성된 폴더의 경로를 지정합니다.
8. **생성**을 클릭합니다.

따라서 .mst 변환이 생성되고 생성한 폴더로 .msi 및 .cab 설치 패키지가 추출됩니다.

3단계: 그룹 정책 개체 설정

1. 도메인 관리자로 도메인 컨트롤러에 로그온합니다. 도메인에 도메인 컨트롤러가 두 개 이상인 경우 이 중 하나에 도메인 관리자로 로그온합니다.
2. 조직 단위에서 에이전트를 배포하려는 경우 조직 단위가 도메인에 있는지 확인합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
3. **시작** 메뉴에서 **관리 도구**를 가르킨 후 **Active Directory 사용자 및 컴퓨터**(Windows Server 2003) 또는 **그룹 정책 관리**(Windows Server 2008 이상)를 클릭합니다.
4. Windows Server 2003의 경우:

- 도메인 또는 조직 단위의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 **등록 정보**를 클릭합니다. 대화 상자에서 **그룹 정책** 탭을 클릭한 다음 **새로 만들기**를 클릭합니다.

Windows Server 2008 이상의 경우:

- 도메인 또는 조직 단위의 이름을 마우스 오른쪽 버튼으로 클릭한 다음 **이 도메인에서 GPO 생성 후 여기에 연결**을 클릭합니다.

5. 새 그룹 정책 개체의 이름을 **Agent for Windows**라고 지정합니다.
6. 다음과 같이 편집할 **Agent for Windows** 그룹 정책 개체를 엽니다.
   - Windows Server 2003에서 그룹 정책 개체를 클릭한 다음 **편집**을 클릭합니다.
   - Windows Server 2008 이상의 경우, **그룹 정책 객체**에서 그룹 정책 객체를 마우스 오른쪽 버튼으로 클릭하고 **편집**을 클릭합니다.
7. 그룹 정책 객체 편집기 스냅인에서 **컴퓨터 구성**을 확장합니다.
8. Windows Server 2003 및 Windows Server 2008:
   - **소프트웨어 설정**을 확장합니다.

   Windows Server 2012 이상의 경우:
   - **정책** > **소프트웨어 설정**을 확장합니다.
9. **소프트웨어 설치**를 마우스 오른쪽 버튼으로 클릭한 다음 **새로 만들기**를 가리킨 후 **패키지**를 클릭합니다.
10. 앞에서 만든 공유 폴더에서 에이전트의 .msi 설치 패키지를 선택한 다음 **열기**를 클릭합니다.
11. **소프트웨어 배포** 대화 상자에서 **고급**을 클릭한 다음 **확인**을 클릭합니다.
12. **수정** 탭에서 **추가**를 클릭한 다음 앞에서 만든 .mst 변환을 선택합니다.
13. **확인**을 클릭하여 **소프트웨어 배포** 대화 상자를 닫습니다.

가상 어플라이언스 업데이트

온-프레미스 디플로이

버전 15.24426 미만(2020년 9월 출시)의 가상 어플라이언스(Agent for VMware 또는 Agent for Scale Computing HC3)를 업데이트하려면 "에이전트 업데이트"(168페이지)의 절차를 따르십시오.

가상 어플라이언스 버전 15.24426 이상을 업데이트하려면

1. http://kb.acronis.com/latest에 설명된 대로 업데이트 패키지를 다운로드합니다.
2. 관리 서버 머신의 다음 디렉토리에 `tar.bz` 파일을 저장합니다.
   - Windows: `C:\Program Files\Acronis\VirtualAppliances\va-updates`
   - Linux: `/usr/lib/Acronis/VirtualAppliances/va-updates`
3. Cyber Protect 웹 콘솔에서 **설정** > **에이전트**를 클릭합니다.

   소프트웨어에 머신 목록이 표시됩니다. 가상 어플라이언스 버전이 오래된 머신에는 오렌지색 느낌표가 표시됩니다.
4. 가상 어플라이언스를 업데이트하려는 머신을 선택합니다. 이러한 머신은 온라인 상태여야 합니다.
5. **에이전트 업데이트**를 클릭합니다.
6. 디플로이 에이전트 선택.

7. 타겟 머신에서 관리자 권한을 가진 계정의 자격 증명을 지정합니다.
8. 에이전트가 관리 서버에 액세스하는 데 사용할 이름 또는 IP 주소를 선택합니다.
   기본적으로 서버 이름이 선택됩니다. DNS 서버가 이름을 IP 주소로 확인할 수 없어 가상 어플라이언스 등록 중에 오류가 발생할 경우 이 설정을 변경해야 할 수 있습니다.

업데이트 진행률이 **작업** 탭에 표시됩니다.

참고
업데이트 중에는 진행 중인 모든 백업 작업에 실패하게 됩니다.

클라우드 디플로이

클라우드 디플로이에서 가상 어플라이언스를 업데이트하는 방법에 대한 자세한 내용은 클라우드 설명서에서 에이전트 업데이트를 참조하십시오.

에이전트 업데이트

사전 요구 사항

Windows 머신에서 Cyber Protect 기능을 사용하려면 Microsoft Visual C++ 2017 Redistributable이 필요합니다. 에이전트를 업데이트하기 전에 Microsoft Visual C++ 2017 Redistributable이 머신에 설치되어 있는지 확인하고, 없는 경우 설치합니다. 설치 후에는 다시 시작해야 할 수 있습니다. Microsoft Visual C++ Redistributable 패키지는 https://support.microsoft.com/help/2999226/update-for-universal-c-runtime-in-windows에서 찾을 수 있습니다.

에이전트 버전을 찾으려면 머신을 선택한 다음 **상세정보**를 클릭합니다.

Cyber Protect 웹 콘솔을 사용하거나 가능한 모든 방식으로 설치를 반복해 에이전트를 업데이트할 수 있습니다. 여러 에이전트를 동시에 업데이트하려면 다음 절차대로 수행합니다.

Cyber Protect 웹 콘솔을 이용한 에이전트 업데이트 방법

1. [온프레미스 디플로이에만 해당] 관리 서버를 업데이트합니다.
2. [온프레미스 디플로이에만 해당] 설치 패키지가 관리 서버가 있는 머신에 있는지 확인하십시오. 정확한 단계는 "Windows를 실행 중인 머신 추가" > "설치 패키지"를 참조하십시오.
3. Cyber Protect 웹 콘솔에서 **설정** > **에이전트**를 클릭합니다.
   소프트웨어에 머신 목록이 표시됩니다. 에이전트 버전이 오래된 머신에는 오렌지색 느낌표가 표시됩니다.
4. 에이전트를 업데이트하려는 머신을 선택합니다. 머신이 온라인 상태여야 합니다.
5. **에이전트 업데이트**를 클릭합니다.
6. 디플로이 에이전트 선택.
7. 타겟 머신에서 관리자 권한을 가진 계정의 자격 증명을 지정합니다.
8. 에이전트가 관리 서버에 액세스하는 데 사용할 관리 서버의 이름 또는 IP 주소를 선택합니다.

기본적으로 서버 이름이 선택됩니다. 관리 서버의 네트워크 인터페이스가 여러 개이거나 DNS 문제가 발생하여 에이전트 등록이 실패하는 경우에는 IP 주소를 대신 선택해야 할 수 있습니다.

9. [온프레미스 디플로이에만 해당] 업데이트 진행률이 **작업** 탭에 표시됩니다.

참고
업데이트 중에는 진행 중인 모든 백업 작업에 실패하게 됩니다.

머신에서 Cyber Protect 정의를 업데이트하는 방법

1. **설정** > **에이전트**를 클릭합니다.
2. Cyber Protect 정의를 업데이트할 머신을 선택한 다음 **정의 업데이트**를 클릭합니다. 머신이 온라인 상태여야 합니다.

에이전트에 업데이터 역할을 할당하려면

1. **설정** > **에이전트**를 클릭합니다.
2. 업데이터 역할을 할당할 머신을 선택하고 **세부정보**를 클릭한 다음, **Cyber Protect 정의** 섹션에서 **이 에이전트를 다운로드해 패치 및 업데이트 배포**를 활성화합니다.

에이전트에서 캐시된 데이터를 지우려면

1. **설정** > **에이전트**를 클릭합니다.
2. 캐시된 데이터(오래된 업데이트 파일 및 패치 관리 데이터)를 지우려는 머신을 선택하고 **캐시 지우기**를 클릭합니다.

Acronis Cyber Protect 15로 업그레이드

다음과 같은 방법으로 이전 버전 제품을 Acronis Cyber Protect 15로 업그레이드할 수 있습니다.

- 이전 버전 제품을 제거하지 않고 직접
  이 옵션은 Acronis Backup 12.5 Update 5(빌드 16180) 이상에서만 제공됩니다.
- 이전 버전 제품을 제거하고 Acronis Cyber Protect 15 새로 설치
  이 옵션은 적격한 모든 제품에서 사용할 수 있습니다. 해당 제품에 대한 자세한 내용은 이 지식 베이스 문서를 참조하십시오.

참고
업그레이드하기 전에 시스템을 백업하는 것이 좋습니다. 이렇게 해야 업그레이드 실패 시 원래 구성으로 롤백할 수 있습니다.

업그레이드를 시작하려면 인스톨러를 실행하고 화면에 나타나는 지침을 따릅니다.

Acronis Cyber Protect 15의 관리 서버는 하위 버전과 호환되며, 12.5 버전 에이전트를 지원합니다. 단, 이러한 에이전트는 Cyber Protect 기능을 지원하지 않습니다.

업그레이드 중인 에이전트는 기존 백업 세트 및 설정을 방해하지 않습니다.

제품 제거

머신에서 개별 제품 컴퍼넌트를 제거하려는 경우에는 설치 프로그램을 실행하고 제품 수정을 선택한 다음 제거할 컴퍼넌트의 선택을 해제합니다. 설치 프로그램 링크는 **다운로드** 페이지(오른쪽 상단의 계정 아이콘 > **다운로드** 클릭)에서 찾아볼 수 있습니다.

머신에서 모든 제품 컴퍼넌트를 제거하려면 아래에서 설명하는 단계를 수행합니다.

경고!
온-프레미스 디플로이에서 설치할 컴퍼넌트를 선택할 때는 매우 유의합니다.

관리 서버를 실수로 제거하는 경우 Cyber Protect 웹 콘솔을 사용할 수 없게 될 뿐 아니라, 제거된 관리 서버에 등록된 머신을 더 이상 백업 및 복구할 수 없게 됩니다.

Windows

1. 관리자로 로그온합니다.
2. **제어판**으로 이동한 다음, **프로그램 및 기능**(Windows XP의 경우 **프로그램 추가 또는 제거**) > **Acronis Cyber Protect** > **설치 제거**를 선택합니다.
3. [선택 사항] **로그 및 구성 설정 제거** 확인란을 선택합니다.
   에이전트를 제거하고 다시 설치하려는 경우에는 이 확인란 선택을 해제하십시오. 이 확인란을 선택하면 해당 머신이 Cyber Protect 웹 콘솔에서 중복될 수 있고, 기존 머신의 백업이 새로운 머신과 연결되지 않을 수 있습니다.
4. 결정을 확인합니다.

Linux

1. 루트 사용자로 **/usr/lib/Acronis/BackupAndRecovery/uninstall/uninstall**을 실행합니다.
2. [선택 사항] **모든 제품 추적 정리(제품 로그, 작업, 볼트 및 구성 설정 제거)** 확인란을 선택합니다.
   에이전트를 제거하고 다시 설치하려는 경우에는 이 확인란 선택을 해제하십시오. 이 확인란을 선택하면 해당 머신이 Cyber Protect 웹 콘솔에서 중복될 수 있고, 기존 머신의 백업이 새로운 머신과 연결되지 않을 수 있습니다.
3. 결정을 확인합니다.

macOS

1. 설치 파일(.dmg)을 두 번 클릭합니다.
2. 운영 체제가 설치 디스크 이미지를 마운트하는 동안 기다립니다.
3. 이미지 내에서 **제거**를 두 번 클릭합니다.
4. 메시지가 표시되면 관리자 자격 증명을 제공합니다.
5. 결정을 확인합니다.

Agent for VMware(가상 어플라이언스) 제거

1. vSphere Client를 시작하고 vCenter Server에 로그온합니다.
2. 가상 어플라이언스의 전원이 켜져 있는 경우에는 마우스 오른쪽 버튼으로 클릭한 다음 **전원** > **전원 끄기**를 클릭합니다. 결정을 확인합니다.
3. 가상 어플라이언스가 가상 디스크에서 로컬로 연결된 스토리지를 사용하고 해당 디스크에서 데이터를 보존하려면 다음을 수행하십시오.
   a. 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭한 다음 **설정 편집**을 클릭합니다.
   b. 스토리지가 있는 디스크를 선택한 다음 **제거**를 클릭합니다. **제거 옵션**에서 **가상 머신에서 제거**를 클릭합니다.
   c. **확인**을 클릭합니다.

   결과적으로 디스크는 데이터 저장소에 남아 있습니다. 다른 가상 어플라이언스에 디스크를 연결할 수 있습니다.
4. 가상 어플라이언스를 마우스 오른쪽 버튼으로 클릭한 다음 **디스크에서 삭제**를 클릭합니다. 결정을 확인합니다.

Cyber Protect 웹 콘솔에서 머신 제거

제거한 에이전트는 관리 서버에서 등록 해제되며, 에이전트가 설치되었던 머신은 Cyber Protect 웹 콘솔에서 자동으로 제거됩니다.

그러나 네트워크 문제 등으로 인해 이 작업 중에 관리 서버 연결이 끊기면 에이전트는 제거되더라도 해당 머신이 웹 콘솔에 계속 표시될 수 있습니다. 이 경우에는 웹 콘솔에서 머신을 수동으로 제거해야 합니다.

웹 콘솔에서 머신을 수동 제거하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 에이전트가 설치된 머신을 선택합니다.
3. **삭제**를 클릭합니다.

Cyber Protect 웹 콘솔에 액세스

Cyber Protect 웹 콘솔에 액세스하려면 웹 브라우저의 주소 표시줄에 로그인 페이지 주소를 입력한 후 아래에 설명된 대로 로그인합니다.

온프레미스 디플로이

로그인 페이지 주소는 관리 서버가 설치된 머신의 이름 또는 IP 주소입니다.

관리 서버 설치 중 구성할 수 있는 동일한 TCP 포트에서 HTTP와 HTTPS 프로토콜 모두 지원됩니다. 기본 포트는 9877입니다.

HTTP를 통한 웹 콘솔 액세스를 방지하고 서드 파티 SSL 인증서를 사용하도록 관리 서버를 구성할 수 있습니다.

Windows

관리 서버가 Windows에 설치될 경우 Cyber Protect 웹 콘솔에 로그인하는 두 가지 방법이 있습니다.

- **로그인**을 클릭하여 현재 Windows 사용자로 로그인합니다.
  이것은 관리 서버가 설치되어 있는 같은 머신에서 로그인하는 가장 쉬운 방법입니다.
  관리 서버가 다른 머신에 설치될 경우 이 방법은 다음 조건에서 작동합니다.
  - 로그인 중인 머신은 관리 서버와 같은 Active Directory 도메인에 있습니다.
  - 도메인 사용자로 로그온되어 있습니다.

  통합 Windows 인증을 사용하도록 웹 브라우저를 구성하는 것이 좋습니다. 그러지 않으면 브라우저에 사용자 이름과 비밀번호를 묻는 메시지가 표시됩니다. 하지만 이 옵션을 비활성화할 수 있습니다.
- **사용자 이름 및 비밀번호 입력**을 클릭하고 사용자 이름과 비밀번호를 지정합니다.

해당 계정은 항상 관리 서버 관리자 목록에 있어야 합니다. 기본적으로 이 목록에는 관리 서버를 실행하는 머신의 **관리자** 그룹이 포함됩니다. 자세한 내용은 "관리자 및 단위"를 참조하십시오.

현재 Windows 사용자 옵션으로 로그인을 비활성화하는 방법

1. 관리 서버가 설치되어 있는 머신에서 `C:\Program Files\Acronis\AccountServer`로 이동합니다.
2. 편집하기 위해 **account_server.json** 파일을 엽니다.
3. "connectiors" 섹션으로 이동한 후 다음 줄을 삭제합니다.

   ```
   {
   "type": "sspi",
   "name": "1 Windows Integrated Logon",
   "id": "sspi",
   "config": {}
   },
   ```

4. "checksum" 섹션으로 이동한 다음 "sum" 값을 다음과 같이 변경합니다.

```
"sum": "FWY/8e8C6c0AgNl0BfCrjgT4v2uj7RQNmaIYbwbjpzU="
```

5. "신뢰할 수 있는 인증 기관에서 발행한 인증서 사용"에 설명된 대로 Acronis Service Manager 서비스를 다시 시작합니다.

Linux

관리 서버가 Linux에 설치된 경우 관리 서버 관리자 목록에 있는 계정의 사용자 이름과 비밀번호를 지정합니다. 기본적으로 이 목록에는 관리 서버를 실행하는 머신의 **루트** 사용자만 포함됩니다. 자세한 내용은 "관리자 및 단위"를 참조하십시오.

클라우드 디플로이

로그인 페이지 주소는 https://backup.acronis.com/입니다. 사용자 이름과 패스워드는 Acronis 계정의 사용자 이름과 패스워드입니다.

계정이 백업 관리자에 의해 생성된 경우에는 계정을 활성화하고 활성화 이메일에 있는 링크를 클릭하여 비밀번호를 설정해야 합니다.

언어 변경

로그인 상태일 때 오른쪽 상단의 계정 아이콘을 클릭하여 웹 인터페이스 언어를 변경할 수 있습니다.

통합 Windows 인증을 사용하도록 웹 브라우저 구성

Windows 및 지원되는 브라우저를 실행 중인 머신에서 Cyber Protect 웹 콘솔에 액세스하면 통합 Windows 인증이 가능합니다.

통합 Windows 인증을 사용하도록 웹 브라우저를 구성하는 것이 좋습니다. 그러지 않으면 브라우저에 사용자 이름과 비밀번호를 묻는 메시지가 표시됩니다.

Internet Explorer, Microsoft Edge, Opera 및 Google Chrome 구성

브라우저를 실행하는 머신이 관리 서버를 실행하는 머신과 같은 Active Directory 도메인에 있으면 콘솔의 로그인 페이지를 **로컬 인트라넷** 사이트에 추가합니다.

그렇지 않으면 콘솔의 로그인 페이지를 **신뢰할 수 있는 사이트** 목록에 추가하고 **현재 사용자 이름 및 암호를 사용하여 자동으로 로그온** 설정을 활성화합니다.

단계별 지침이 이 섹션의 뒷부분에 제공됩니다. 이러한 브라우저에서는 Windows 설정을 사용하므로 Active Directory 도메인에서 그룹 정책을 사용하여 설정을 구성할 수도 있습니다.

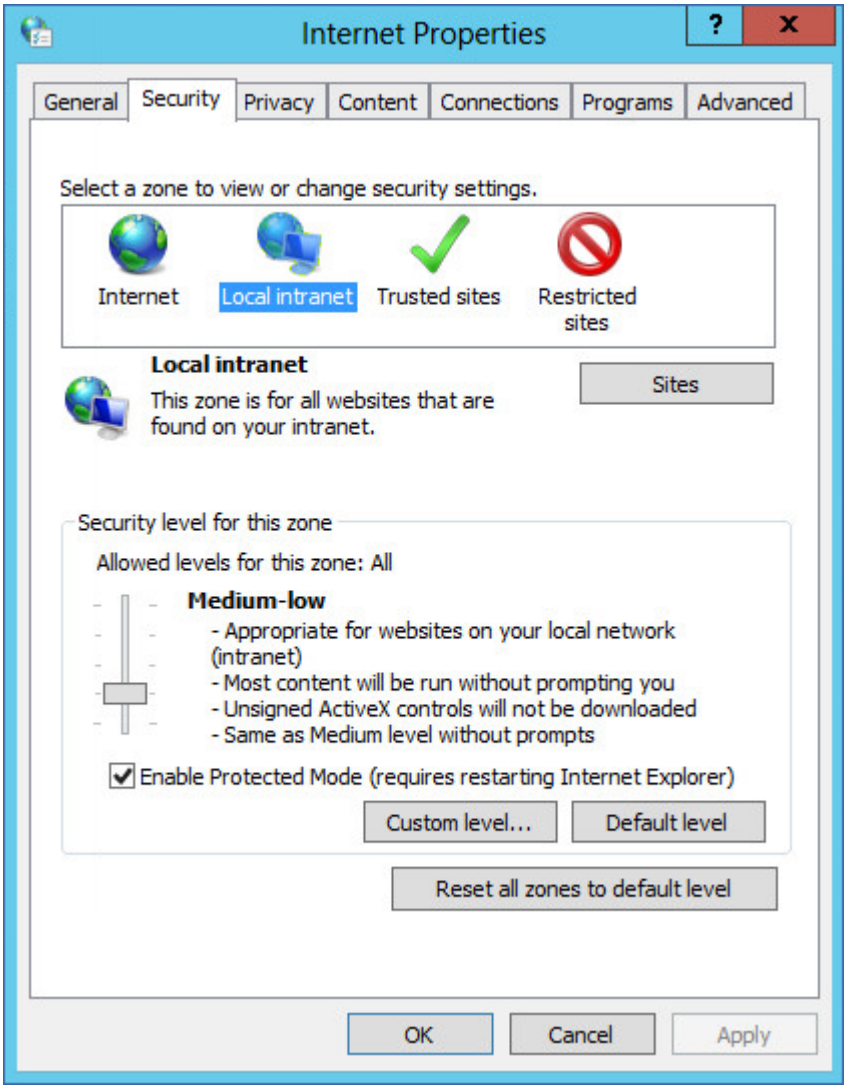
Mozilla Firefox 구성

1. Firefox에서 URL `about:config`로 이동하고 **위험을 감수하겠습니다!** 버튼을 클릭합니다.
2. **검색** 필드에서 `network.negotiate-auth.trusted-uris` 기본 설정을 검색합니다.

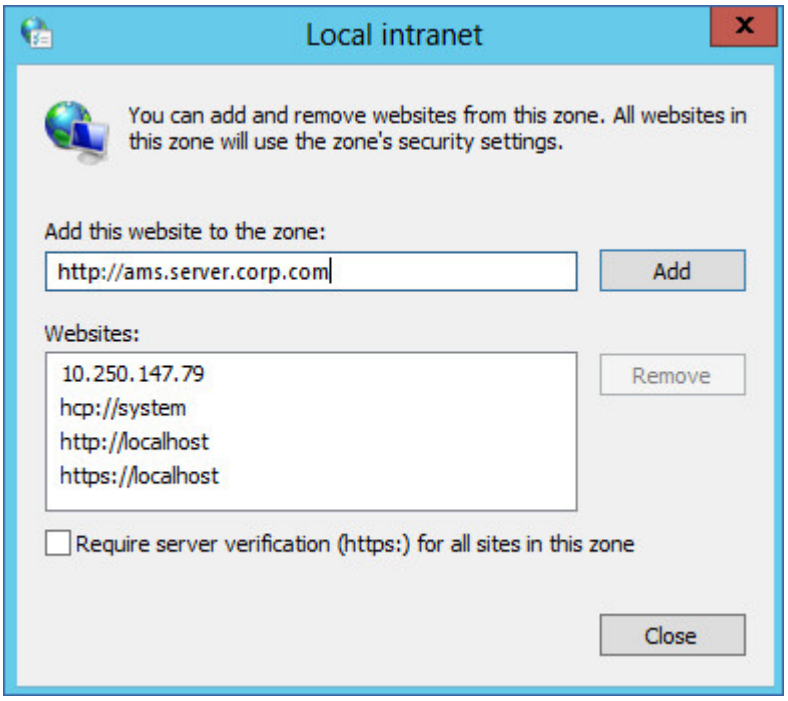
3. 기본 설정을 두 번 클릭하고 Cyber Protect 웹 콘솔 로그인 페이지의 주소를 입력합니다.
4. `network.automatic-ntlm-auth.trusted-uris` 기본 설정에 대해 2~3단계를 반복합니다.
5. `about:config` 창을 닫습니다.

로컬 인트라넷 사이트 목록에 콘솔 추가

1. **제어판** > **인터넷 옵션**으로 이동합니다.
2. **보안** 탭에서 **로컬 인트라넷**을 선택합니다.



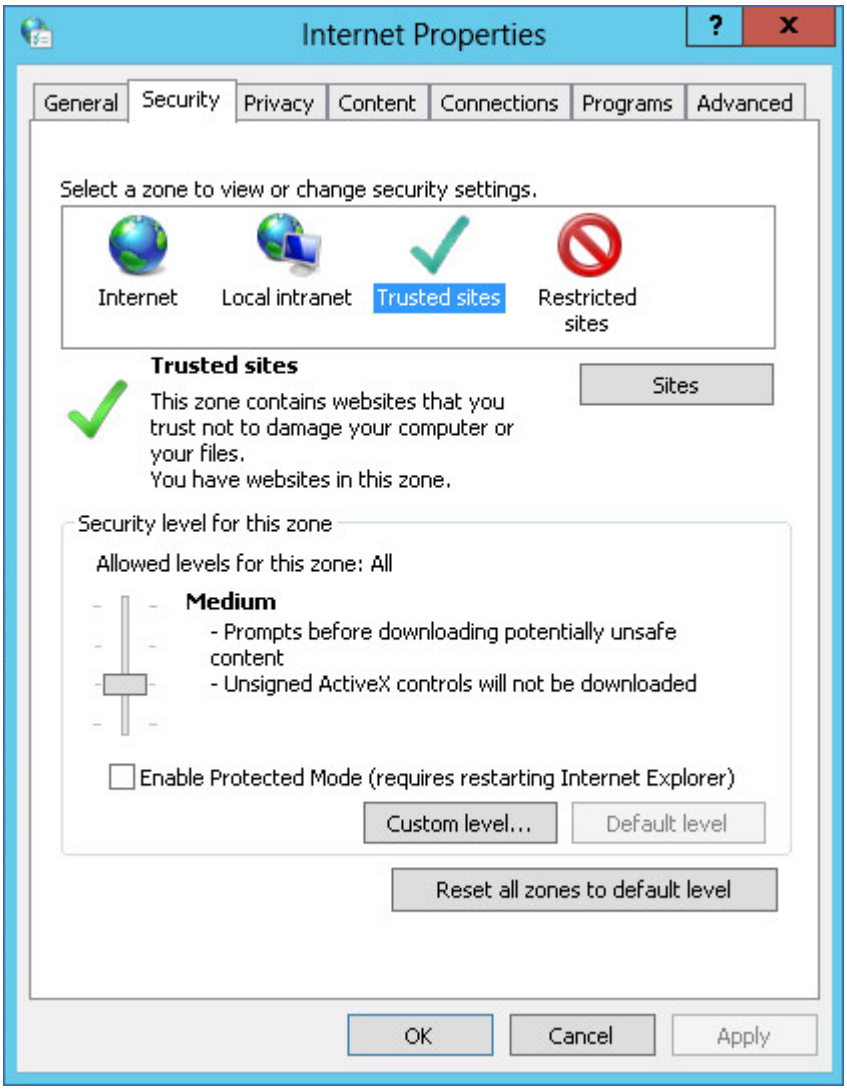
3. **사이트**를 클릭합니다.
4. **영역에 웹 사이트 추가**에서 Cyber Protect 웹 콘솔 로그인 페이지의 주소를 입력하고 **추가**를 클릭합니다.



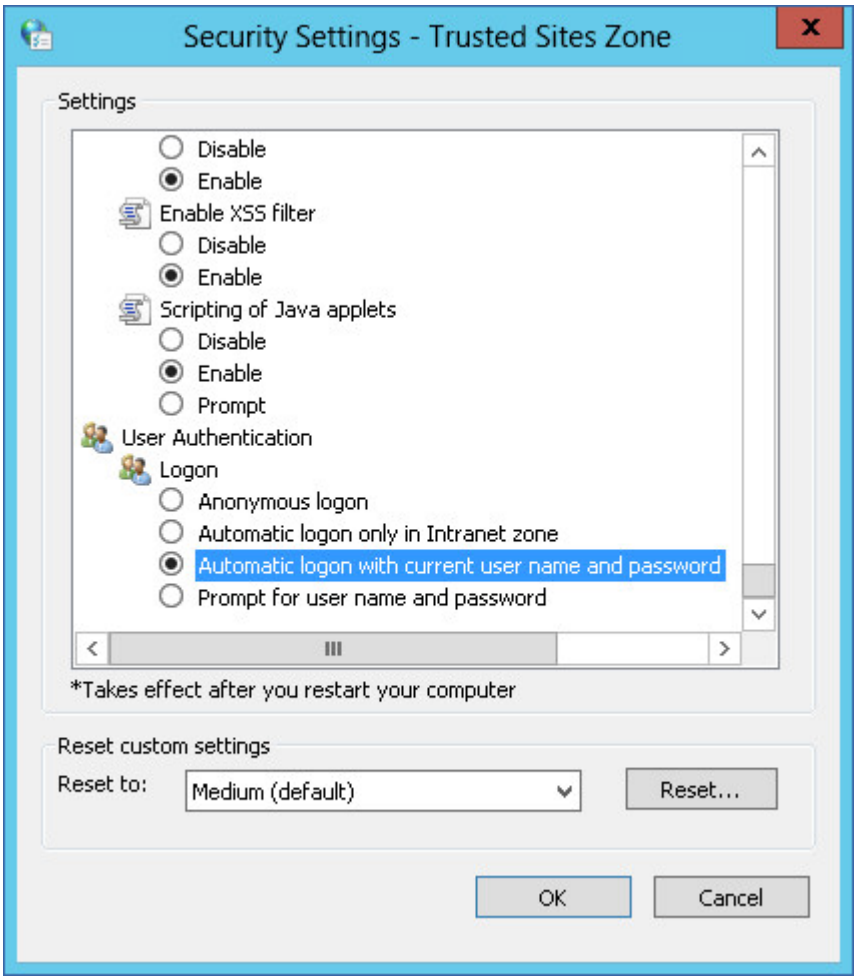
5. **닫기**를 클릭합니다.
6. **확인**을 클릭합니다.

신뢰할 수 있는 사이트 목록에 콘솔 추가

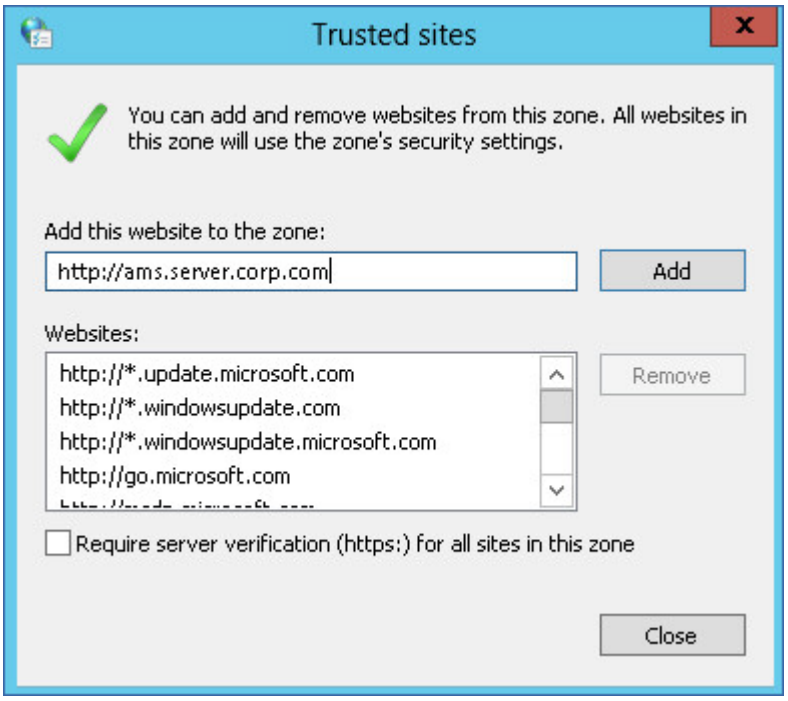
1. **제어판** > **인터넷 옵션**으로 이동합니다.
2. **보안** 탭에서 **신뢰할 수 있는 사이트**를 선택하고 **사용자 지정 수준**을 클릭합니다.



3. **로그온**에서 **현재 사용자 이름 및 암호를 사용하여 자동으로 로그온**을 선택하고 **확인**을 클릭합니다.



4. **보안** 탭에서 **신뢰할 수 있는 사이트**가 선택된 상태로 **사이트**를 클릭합니다.
5. **영역에 웹 사이트 추가**에서 Cyber Protect 웹 콘솔 로그인 페이지의 주소를 입력하고 **추가**를 클릭합니다.



6. **닫기**를 클릭합니다.
7. **확인**을 클릭합니다.

웹 콘솔에 연결할 때 HTTPS 연결만 허용

보안상 사용자가 HTTP 프로토콜을 통해서는 Cyber Protect 웹 콘솔에 액세스하지 못하도록 하고 HTTPS 연결만 허용할 수 있습니다.

웹 콘솔에 연결할 때 HTTPS 연결만 허용하려면

1. 관리 서버를 실행하는 머신에서 텍스트 편집기를 사용하여 다음 구성 파일을 엽니다.
   - Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`
2. 다음 섹션을 찾습니다.

```
"tls": {
  "auto_redirect" : false,
  "cert_file": "cert.pem",
```

3. `"auto_redirect"` 값을 `false`에서 `true`로 변경합니다.

   `"auto_redirect"` 줄이 없으면 수동으로 추가합니다.

```
"auto_redirect": true,
```

4. `api_gateway.json` 파일을 저장합니다.

중요

구성 파일에서 어떠한 쉼표, 괄호, 따옴표도 실수로 삭제하지 않도록 주의하십시오.

5. 아래에 설명된 대로 Acronis Service Manager 서비스를 다시 시작합니다.

Windows에서 Acronis Service Manager 서비스를 다시 시작하려면

Windows

1. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
2. **확인**을 클릭합니다.
3. 다음 명령 실행:

```
net stop asm
net start asm
```

Linux

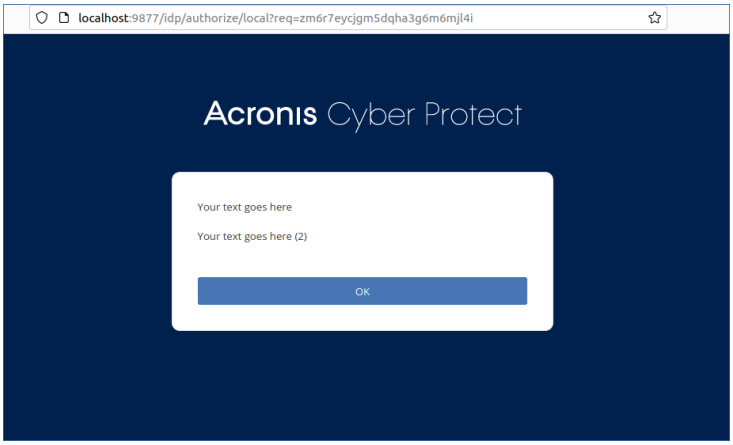
1. **터미널**을 엽니다.
2. 아무 디렉터리에서나 다음 명령을 실행합니다.

```
sudo service acronis_asm restart
```

웹 콘솔에 사용자 정의 메시지 추가

Cyber Protect 웹 콘솔에 사용자 정의 메시지를 추가할 수 있습니다.

해당 메시지는 로그인을 시도하기 전에 항상 표시됩니다.



사전 요구 사항

관리 서버가 실행되는 머신에 보호 계획이 적용되어 있으면 자체 보호 기능이 비활성화되어 있는지 확인하십시오. 자체 보호 기능이 비활성화되어 있지 않으면 구성 파일을 편집할 수 없습니다.

자체 보호 기능을 비활성화하거나 활성화하는 방법에 대한 자세한 내용은 "자체 보호"(472페이지) 항목을 참조하십시오.

웹 콘솔에 사용자 정의 메시지를 추가하려면

Windows

1. 관리 서버가 설치되어 있는 머신에 로그인합니다. 계정에 관리자 권한이 있어야 합니다.
2. %Program Files%\Acronis\AccountServer로 이동합니다.
3. [선택 사항] AccountServer.zip 파일의 백업 사본을 만듭니다.
4. %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale로 이동합니다.
5. Cyber Protect 웹 콘솔에서 사용하는 언어에 해당하는 JSON 파일의 압축을 풉니다. 예를 들어 영어를 사용하는 경우 en.json 파일의 압축을 풉니다.

   참고
   파일은 두 번 클릭하여 여는 것만으로는 편집할 수 없으며 압축을 풀어야 편집할 수 있습니다.

6. 편집을 위해 압축을 푼 파일을 엽니다. 메모장, Notepad++ 등의 텍스트 편집기를 사용할 수 있습니다.
7. 다음 줄로 이동한 후 줄 끝에 쉼표를 추가합니다.

   ```
   "APP_LOGINFORM_LOGIN_BUTTON": "Log in",
   ```

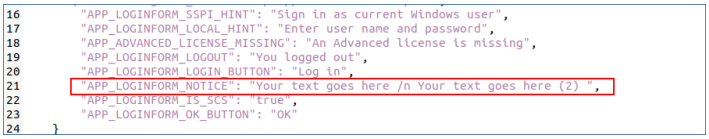
8. "APP_LOGINFORM_LOGIN_BUTTON": "Log in" 줄 아래에 다음 줄을 추가합니다.

   ```
   "APP_LOGINFORM_NOTICE": "<Type your custom message here>",
   ```

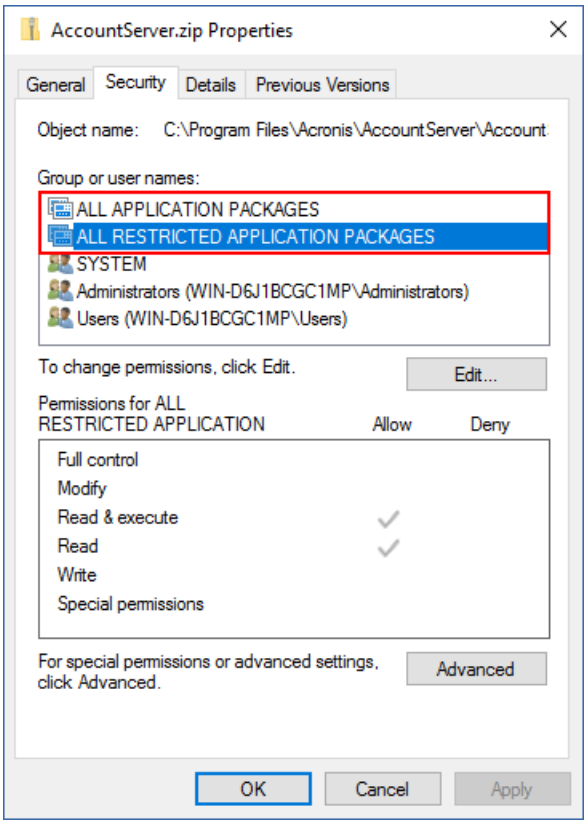
   ```
   "APP_LOGINFORM_IS_SCS": "true",
   ```

   ```
   "APP_LOGINFORM_OK_BUTTON": "OK"
   ```

   예:

9. 변경 사항을 저장한 후 편집한 JSON 파일을 %Program Files%\Acronis\AccountServer\AccountServer.zip\static\locale에 다시 추가합니다.
10. AccountServer.zip 파일을 마우스 오른쪽 버튼으로 클릭하고 **속성** > **보안**으로 이동하여 **그룹 또는 사용자 이름** 아래에 모든 애플리케이션 패키지 및 모든 제한된 애플리케이션 패키지가 각각 **읽기** 권한과 **읽기 및 실행** 권한으로 설정되어 추가되었는지 확인합니다.



참고

모든 제한된 애플리케이션 패키지가 추가되어 있지 않으면 해당 목록에서 모든 애플리케이션 패키지를 제거한 후에 다시 추가합니다. 모든 애플리케이션 패키지를 추가하면 모든 제한된 애플리케이션 패키지가 자동으로 표시됩니다.

11. 에 설명된 대로 **Acronis Service Manager 서비스**를 다시 시작합니다.

Linux

1. 관리 서버가 설치되어 있는 머신에 로그인합니다.
2. `/usr/lib/Acronis/AccountServer`로 이동합니다.
3. `AccountServer.zip` 파일에 대한 쓰기 권한이 있는지 확인합니다.
4. [선택 사항] `AccountServer.zip` 파일의 백업 사본을 만듭니다.
5. `/usr/lib/Acronis/AccountServer/static/locale`로 이동합니다.
6. Cyber Protect 웹 콘솔에서 사용하는 언어에 해당하는 JSON 파일의 압축을 풉니다. 예를 들어 영어를 사용하는 경우 `en.json` 파일의 압축을 풉니다.
7. 편집을 위해 압축을 푼 파일을 엽니다.
8. 다음 줄로 이동한 후 줄 끝에 쉼표를 추가합니다.

```
"APP_LOGINFORM_LOGIN_BUTTON": "Log in",
```

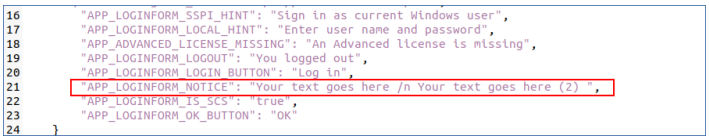
9. `"APP_LOGINFORM_LOGIN_BUTTON": "Log in"` 줄 아래에 다음 줄을 추가합니다.

```
"APP_LOGINFORM_NOTICE": "<Type your custom message here>",
```

```
"APP_LOGINFORM_IS_SCS": "true",
```

```
"APP_LOGINFORM_OK_BUTTON": "OK"
```

예:



10. 변경 사항을 저장한 후 편집한 JSON 파일을 `/usr/lib/Acronis/AccountServer/static/locale`에 다시 추가합니다.
11. 에 설명된 대로 **Acronis Service Manager 서비스**를 다시 시작합니다.

SSL 인증서 설정

이 섹션에서는 다음에 대해 설명합니다.

- 관리 서버가 생성한 자체 서명 SSL(Secure Socket Layer) 인증서를 사용하는 보호 에이전트를 구성하는 방법.
- 관리 서버가 생성한 자체 서명 SSL 인증서를 GoDaddy, Comodo, GlobalSign 같은 신뢰할 수 있는 인증 기관에서 발행한 인증서로 변경하는 방법 이렇게 하면 관리 서버가 사용하는 인증서를 어느 머신에서도 신뢰할 수 있게 됩니다. HTTPS 프로토콜을 사용하여 Cyber Protect 웹 콘솔에 로그인할 때 브라우저 보안 경보가 표시되지 않습니다.

선택적으로 모든 사용자를 HTTPS로 리디렉션함으로써 관리 서버가 HTTP를 통한 Cyber Protect 웹 콘솔 액세스를 방지하도록 구성할 수 있습니다.

자체 서명된 인증서 사용

Windows에서 보호 에이전트를 구성하는 방법

1. 에이전트가 있는 머신에서 레지스트리 편집기를 엽니다.
2. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\Software\Acronis\BackupAndRecovery\Settings\CurlOptions.**
3. **VerifyPeer** 값을 **0**으로 설정합니다.
4. **VerifyHost** 값이 **0**으로 설정되었는지 확인합니다.
5. 관리 대상 머신 서비스(MMS)를 다시 시작합니다.
   a. **시작 메뉴**에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
   b. **확인**을 클릭합니다.
   c. 다음 명령 실행:

```
net stop mms
net start mms
```

Linux에서 보호 에이전트를 구성하는 방법

1. 에이전트가 있는 머신에서 편집하기 위해 **/etc/Acronis/BackupAndRecovery.config** 파일을 엽니다.
2. **CurlOptions** 키로 이동하고 **VerifyPeer** 의 값을 **0**으로 설정합니다. **VerifyHost** 값 역시 **0**으로 설정되었는지 확인합니다.
3. 편집 사항을 저장합니다.
4. 아무 디렉터리에서나 다음 명령을 실행하여 관리 대상 머신 서비스(MMS)를 다시 시작합니다.

```
sudo service acronis_mms restart
```

macOS에서 보호 에이전트를 구성하는 방법

1. 에이전트가 있는 머신에서 관리 대상 머신 서비스(MMS)를 중단합니다.
   a. **애플리케이션** > **유틸리티** > **터미널**로 이동합니다.
   b. 다음 명령을 실행합니다.

```
sudo launchctl stop acronis_mms
```

2. 편집하기 위해 **/Library/Application Support/Acronis/Registry/BackupAndRecovery.config** 파일을 엽니다.
3. **CurlOptions** 키로 이동하고 **VerifyPeer** 의 값을 **0**으로 설정합니다. **VerifyHost** 값 역시 **0**으로 설정되었는지 확인합니다.
4. 편집 사항을 저장합니다.
5. 아무 터미널에서나 다음 명령을 실행하여 관리 대상 머신 서비스(MMS)를 시작합니다.

```
sudo launchctl starts acronis_mms
```

신뢰할 수 있는 인증 기관에서 발행한 인증서 사용

SSL 인증서 설정을 구성하는 방법

1. 다음 항목이 모두 있는지 확인합니다.

인증서 및 키 파일을 사용하는 경우	PFX 파일을 사용하는 경우
인증서 파일 (.pem 형식)	PFX 파일
인증서의 비공개 키가 포함된 파일 (보통 .key 형식)	
비공개 키 암호 (키가 암호로 보호된 경우)	PFX 파일의 암호(파일이 암호로 보호된 경우)

2. 파일을 관리 서버를 실행하는 머신으로 복사합니다.
3. 이 머신에서 텍스트 편집기를 사용하여 다음 구성 파일을 엽니다.
   - Windows: `%ProgramData%\Acronis\ApiGateway\api_gateway.json`
   - Linux: `/var/lib/Acronis/ApiGateway/api_gateway.json`

4. 다음 섹션을 찾습니다.

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "",
```

5. "cert_file" 줄의 물음표 사이에 인증서 파일이나 PFX 파일의 전체 경로를 지정합니다.

   예:

운영 체제	인증서 및 키 쌍을 사용하는 경우	.pfx 파일을 사용하는 경우
Windows (슬래시 주의)	"cert_file": "C:/certificate/local-domain.ams.pem"	"cert_file": "C:/certificate/local-domain.ams.pfx"
Linux	"cert_file": "/home/user/local-domain.ams.pem"	"cert_file": "/home/user/local-domain.ams.pfx"

6. "key_file" 줄의 물음표 사이에 인증서 키가 포함된 PFX 파일이나 비공개 키 파일의 전체 경로를 지정합니다.

   PFX 파일에는 대개 인증서와 해당 키가 모두 포함되어 있습니다. 이 경우 "key_file" 줄에서 이전 단계와 같은 경로를 지정합니다.

   예:

운영 체제	인증서 및 키 쌍을 사용하는 경우	.pfx 파일을 사용하는 경우
Windows (슬래시 주의)	"key_file": "C:/certificate/private.key"	"cert_file": "C:/certificate/local-domain.ams.pfx"
Linux	"key_file": "/home/user/private.key"	"cert_file": "/home/user/local-domain.ams.pfx"

7. [선택 사항] 비공개 키나 PFX 파일이 암호로 보호되어 있는 경우 "passphrase" 줄의 물음표 사이에 암호를 지정합니다.

   예를 들어 "passphrase": "my password"와 같이 지정할 수 있습니다.

   참고

   api_gateway.json 구성 파일에 "passphrase": "", 줄이 없으면 해당 줄을 수동으로 추가합니다.

   예:

```
"tls": {
    "cert_file": "cert.pem",
    "key_file": "key.pem",
    "passphrase": "my password",
}
```

8. api_gateway.json 파일을 저장합니다.

중요
구성 파일에서 어떠한 쉼표, 괄호, 따옴표도 실수로 삭제하지 않도록 주의하십시오.

9. 아래에 설명된 대로 Acronis Service Manager 서비스를 다시 시작합니다.

Acronis Service Manager 서비스를 다시 시작하려면

Windows

1. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
2. **확인**을 클릭합니다.
3. 다음 명령 실행:

```
net stop asm
net start asm
```

Linux

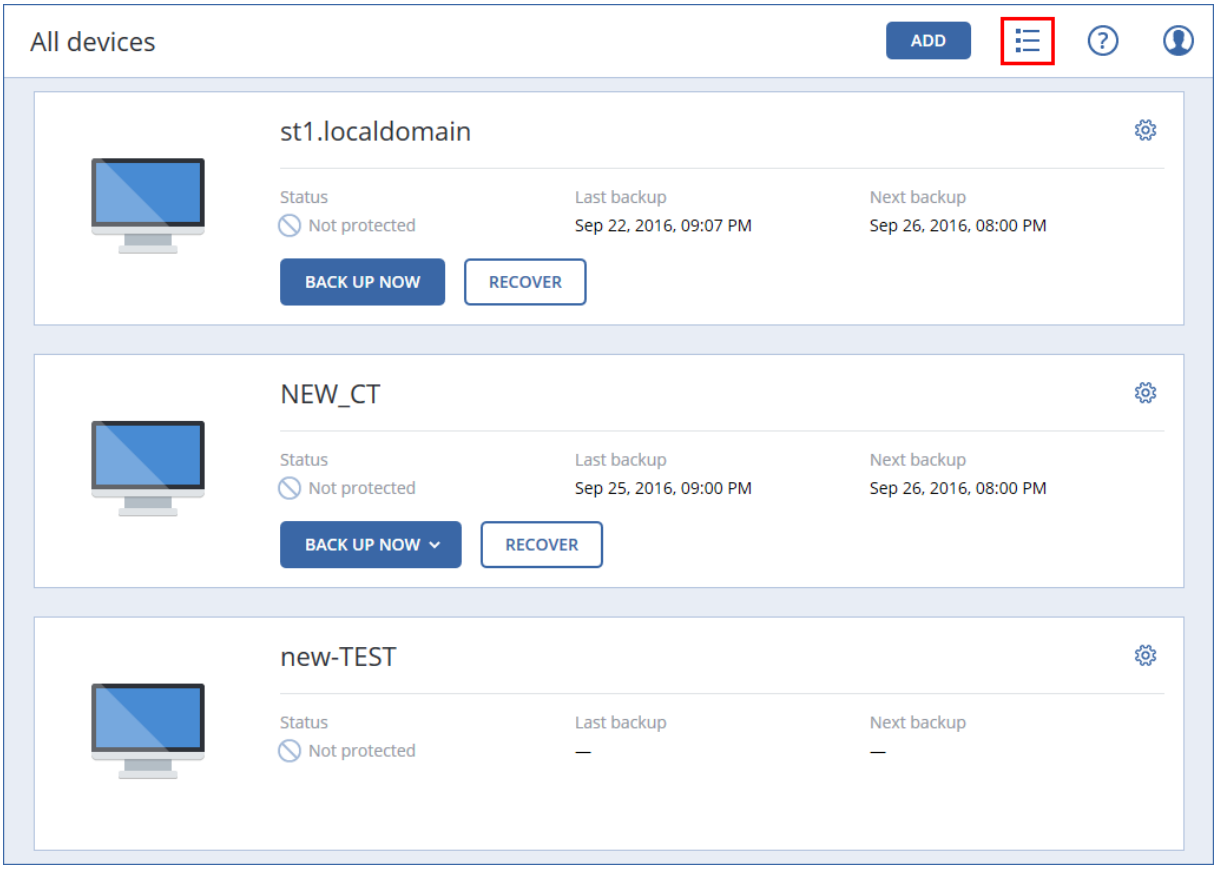
1. **터미널**을 엽니다.
2. 아무 디렉터리에서나 다음 명령을 실행합니다.

```
sudo service acronis_asm restart
```

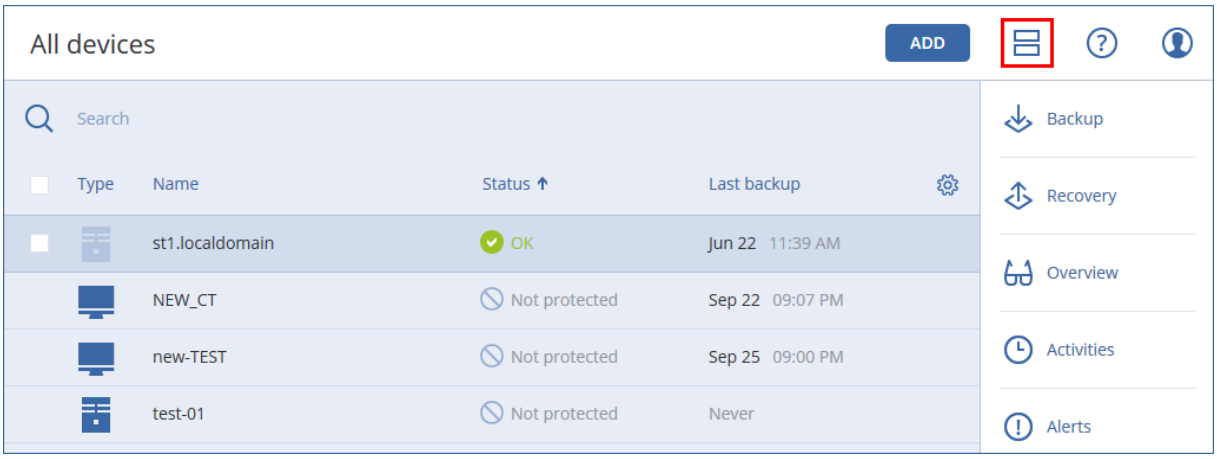
Cyber Protect 웹 콘솔 보기

Cyber Protect 웹 콘솔에는 단순 보기 및 테이블 보기의 두 가지 보기가 있습니다. 이러한 보기 간에 전환하려면 오른쪽 위 구석에서 해당 아이콘을 클릭합니다.

단순 보기에는 적은 수의 머신이 표시됩니다.



머신 수가 많아지면 테이블 보기가 자동으로 활성화됩니다.



두 보기 모두 동일한 기능 및 작업에 대한 액세스를 제공합니다. 이 문서에서는 테이블 보기에서 작업에 액세스하는 방법에 대해 설명합니다.

머신이 온라인 또는 오프라인 상태가 되면 Cyber Protect 웹 콘솔에서 상태가 변경되는 데 시간이 걸립니다.

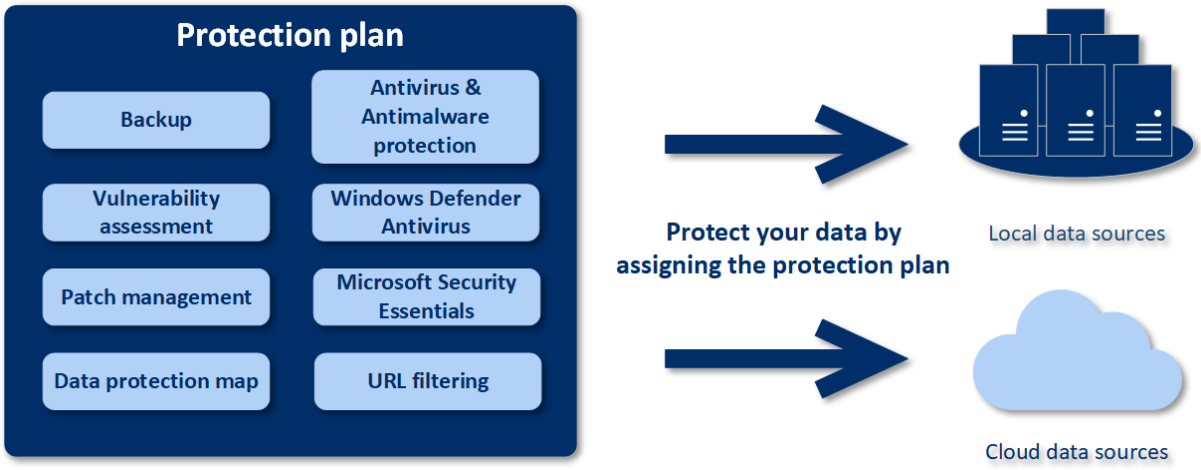
머신 상태는 1분마다 점검됩니다. 이 머신에 설치된 에이전트가 데이터를 전송하지 않고 5회 연속 점검에 응답하지 않으면 머신이 오프라인으로 표시됩니다. 머신이 상태 점검에 응답하거나 데이터 전송을 시작하면 다시 온라인 상태로 표시됩니다.

보호 계획 및 모듈

보호 계획이란 다음을 비롯한 여러 가지 데이터 보호 모듈을 조합한 계획입니다.

- 백업 – 데이터 소스를 로컬 또는 클라우드 스토리지에 백업합니다.
- 바이러스 백신 및 맬웨어 방지 기능 – 내장된 맬웨어 방지 솔루션으로 머신을 확인합니다.
- URL 필터링 – 악성 URL에 대한 액세스와 콘텐츠 다운로드를 차단하여 인터넷을 통한 위협에서 머신을 보호합니다.
- Windows Defender 바이러스 백신 – Windows Defender Antivirus 설정을 관리해 환경을 보호합니다.
- Microsoft Security Essentials – Microsoft Security Essentials 설정을 관리해 환경을 보호합니다.
- 취약성 평가 – 자동으로 머신에 설치된 Microsoft 및 서드 파티 제품의 취약성을 확인하고 결과를 알립니다.
- 패치 관리 – 머신의 Microsoft 및 서드 파티 제품에 대한 패치 및 업데이트를 설치해 발견된 취약성을 해결합니다.
- 데이터 보호 맵 – 중요한 파일의 보호 상태를 모니터링하기 위해 데이터를 검색할 수 있습니다.

보호 계획을 사용해 외부 및 내부 위협으로부터 데이터 소스를 완벽하게 보호할 수 있습니다. 각기 다른 모듈을 활성화/비활성화하고 모듈 설정을 지정하여 다양한 비즈니스 요건에 맞게 유연한 계획을 생성할 수 있습니다.



보호 계획 생성

보호 계획은 생성 시 또는 이후에 여러 머신에 적용할 수 있습니다. 계획을 생성하면 시스템이 운영 체제 및 장치 유형(예: 워크스테이션, 가상 머신 등)을 확인하고, 장치에 해당하는 계획 모듈만 표시합니다.

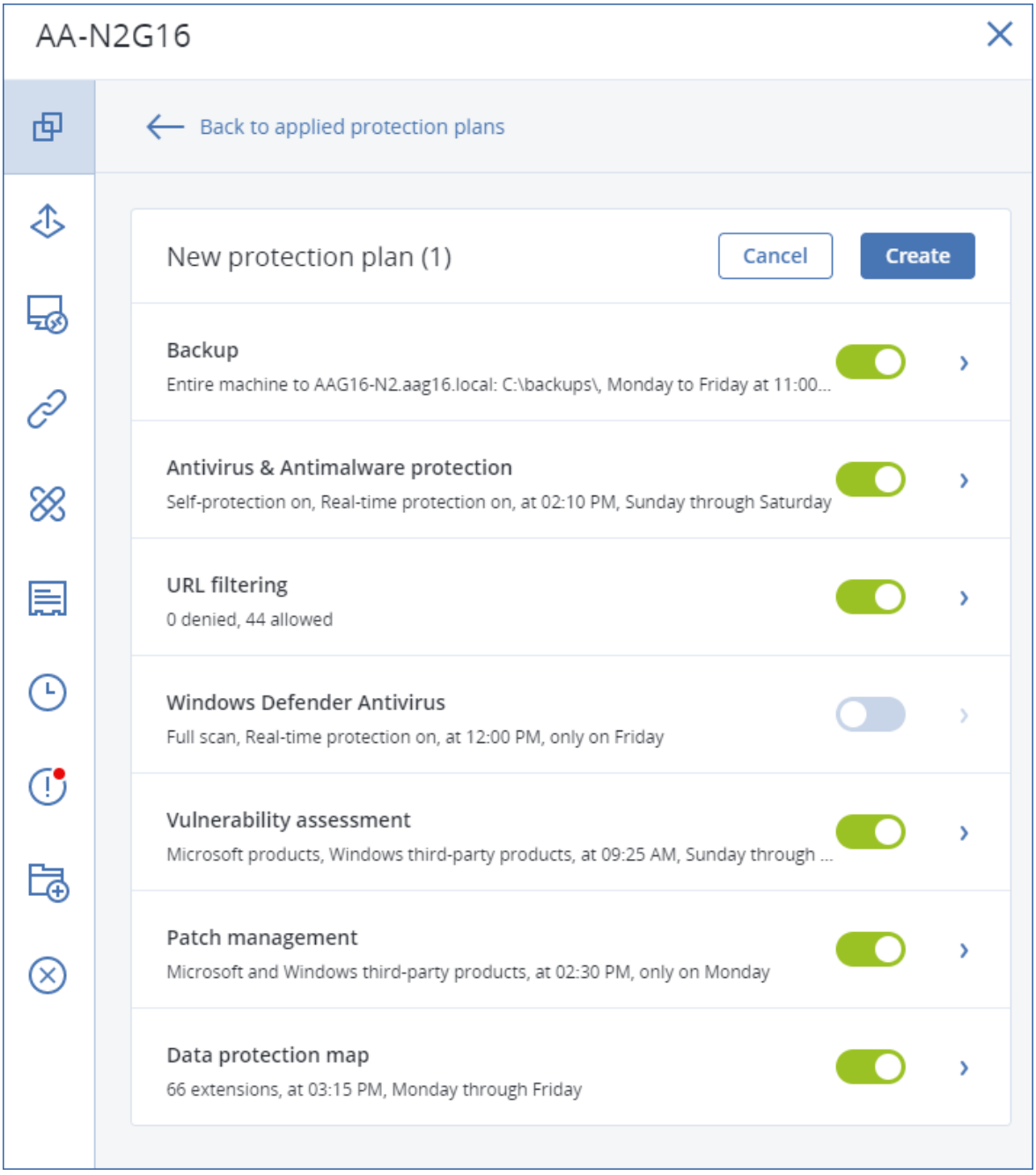
보호 계획은 다음과 같은 2가지 방법으로 생성할 수 있습니다.

- **장치** 섹션에서 보호할 장치 또는 여러 장치를 선택한 다음 이에 대한 계획을 생성합니다.
- **계획** 섹션에서 계획을 생성한 다음 이를 적용할 머신을 선택합니다.

첫 번째 방법을 살펴보겠습니다.

첫 번째 보호 계획을 생성하려면

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 보호하려는 머신을 선택합니다.
3. **보호**를 클릭한 다음, **계획 생성**을 클릭합니다. 그러면 기본 설정의 보호 계획이 표시됩니다.



4. [선택 사항] 보호 계획 이름을 수정하려면 이름 옆의 연필 아이콘을 클릭합니다.
5. [선택 사항] 보호 계획 모듈을 활성화 또는 비활성화하려면 모듈 이름 옆의 스위치를 클릭합니다.
6. [선택 사항] 모듈 매개변수를 구성하려면 보호 계획 패널의 해당 섹션을 클릭합니다.
7. 준비가 되면 **생성**을 클릭합니다.

지금 실행을 클릭해 필요에 따라 백업, 바이러스 백신 및 맬웨어 방지 기능, 취약성 평가, 패치 관리, 데이터 보호 맵 모듈을 수행할 수 있습니다.

계획 충돌 해결

보호 계획은 다음 중 하나로 표시됩니다.

- **활성** – 장치에 할당되어 있으며 실행된 계획입니다.
- **비활성** – 장치에 지정되어 있지만 비활성화되어 있으며 장치에서 실행되지 않은 계획입니다.

장치에 여러 가지 계획 적용

단일 장치에 여러 보호 계획을 적용할 수 있습니다. 결과적으로 단일 장치에 다양한 보호 계획 조합을 할당할 수 있습니다. 예를 들어, 한 계획에는 바이러스 백신 및 맬웨어 방지 기능 모듈만 활성화하고 다른 계획에는 백업 모듈만 활성화하는 계획을 적용할 수 있습니다. 서로 교차하는 모듈이 없는 보호 계획만 조합할 수 있습니다. 하나 이상의 보호 계획에서 같은 모듈이 활성화된 경우, 이들 간의 충돌을 해결해야 합니다.

계획 충돌 해결

새로 생성한 계획이 이미 적용된 계획과 충돌하는 경우

장치 또는 여러 장치에 이미 적용된 계획이 새로 생성한 계획과 충돌하는 경우 다음과 같은 방법으로 해결할 수 있습니다.

- 새로운 계획을 생성해 적용하고 충돌을 일으키는 이전 계획은 모두 비활성화합니다.
- 새로운 계획을 생성하고 비활성화합니다.

이미 계획이 적용된 장치 또는 여러 장치에서 계획을 편집하였으며, 이러한 변경 사항으로 충돌이 발생하는 경우 다음과 같은 방법으로 해결할 수 있습니다.

- 계획에 대한 변경 사항을 저장하고 충돌을 일으키는 이전 계획은 모두 비활성화합니다.
- 계획에 대한 변경 사항을 저장하고 비활성화합니다.

장치 계획이 그룹 계획과 충돌하는 경우

장치가 그룹 계획이 할당된 장치 그룹에 포함되어 있는 상태에서 새로운 계획을 해당 장치에 할당하면, 시스템에서는 다음과 같은 방법으로 충돌을 해결해 달라는 메시지를 표시합니다.

- 그룹에서 장치를 제거하고 해당 장치에 새 계획을 적용합니다.
- 전체 그룹에 새 계획을 적용하거나 현재 그룹 계획을 편집합니다.

라이센스 문제

장치에 지정된 할당량은 수행, 업데이트, 적용될 보호 계획에 적합해야 합니다. 라이센스 문제를 해결하려면 다음 중 하나를 수행합니다.

- 지정된 할당량으로 지원되지 않는 모듈을 비활성화하고 계속 보호 계획을 사용합니다.
- 지정된 할당량을 수동으로 변경합니다. **장치** > **<특정 장치>** > **상세 정보** > **서비스 할당량**으로 이동합니다. 그 다음 기존 할당량을 취소하고 새로운 할당량을 지정합니다.

보호 계획 관련 작업

보호 계획 생성 방법에 대한 자세한 내용은 "보호 계획 생성"을 참조하십시오.

보호 계획으로 가능한 작업

보호 계획으로 다음 작업을 수행할 수 있습니다.

- 계획 이름 바꾸기
- 모듈 활성화/비활성화, 각 모듈 설정 편집
- 계획 활성화/비활성화

  비활성화된 계획은 적용된 장치에 수행되지 않습니다.

  이 작업은 이후에 동일한 계획으로 동일한 장치를 보호하려는 경우 편리합니다. 계획이 장치에서 취소되지 않았으며, 보호를 복구하려면 반드시 관리자가 계획을 재활성화해야만 합니다.
- 장치 또는 장치 그룹에 계획 적용
- 장치에서 계획 취소

  이제 취소된 계획이 장치에 적용되지 않습니다.

  이 작업은 이후에 동일한 계획으로 동일한 장치를 빠르게 보호할 필요가 없는 관리자에게 편리합니다. 취소된 계획의 보호를 복구하려면 관리자가 반드시 해당 계획의 이름을 알고, 사용 가능한 계획 목록에서 선택해 원하는 장치에 해당 계획을 재적용해야 합니다.
- 계획 가져오기/내보내기

  참고

  Acronis Cyber Protect 15에서 생성한 보호 계획만 가져올 수 있습니다. 이전 버전에서 생성한 보호 계획은 Acronis Cyber Protect 15와 호환되지 않습니다.

- 계획 삭제

기존 보호 계획을 적용하려면

1. 보호하려는 머신을 선택합니다.
2. **보호**를 클릭합니다. 선택한 머신에 이미 보호 계획이 적용되어 있는 경우 **계획 추가**를 클릭합니다.
3. 소프트웨어에 이전에 생성한 보호 계획이 표시됩니다.
4. 필요한 보호를 선택한 다음, **적용**을 클릭합니다.

보호 계획을 편집하려면

1. 보호 계획이 적용되는 모든 머신에 대해 보호 계획을 편집하려는 경우 해당 머신 중 하나를 선택합니다. 그렇지 않은 경우 보호 계획을 편집하려는 머신을 선택합니다.
2. **보호**를 클릭합니다.
3. 편집할 보호 계획을 선택합니다.

4. 보호 계획 이름 옆에 있는 말줄임표 아이콘을 클릭한 다음 **편집**을 클릭합니다.
5. 계획 매개변수를 수정하려면 보호 계획 패널의 해당 섹션을 클릭합니다.
6. **변경 사항 저장**을 클릭합니다.
7. 보호 계획이 적용되는 모든 머신의 보호 계획을 변경하려면 **이 보호 계획에 변경 사항을 적용**을 클릭합니다. 그렇지 않으면 **선택한 장치에 대해서만 새 보호 계획 생성**을 클릭합니다.

머신에서 보호 계획을 취소하려면

1. 보호 계획을 취소하려는 머신을 선택합니다.
2. **보호**를 클릭합니다.
3. 머신에 여러 보호 계획이 적용된 경우 취소하려는 보호 계획을 선택합니다.
4. 보호 계획 이름 옆에 있는 말줄임표 아이콘을 클릭한 다음 **취소**를 클릭합니다.

보호 계획을 삭제하려면

1. 삭제하려는 보호 계획이 전용된 모든 머신을 선택합니다.
2. **보호**를 클릭합니다.
3. 머신에 여러 보호 계획이 적용된 경우 삭제하려는 보호 계획을 선택합니다.
4. 보호 계획 이름 옆에 있는 말줄임표 아이콘을 클릭한 다음 **삭제**를 클릭합니다.
   따라서 보호 계획이 모든 머신에서 취소되고 웹 인터페이스에서 완전히 제거됩니다.

백업

백업 모듈이 활성화된 보호 계획은 지정된 데이터를 지정된 머신에서 보호하는 방법에 대한 규칙 세트입니다.

보호 계획은 생성 시 또는 이후에 여러 머신에 적용할 수 있습니다.

참고
온-프레미스 디플로이에서는 표준 라이센스가 관리 서버에 있는 경우 보호 계획을 여러 실제 머신에 적용할 수 없습니다. 각 실제 머신에서 자체 보호 계획을 갖고 있어야 합니다.

처음으로 백업 모듈이 활성화된 보호 계획을 생성하려면

1. 백업하려는 머신을 선택합니다.
2. **보호**를 클릭합니다.

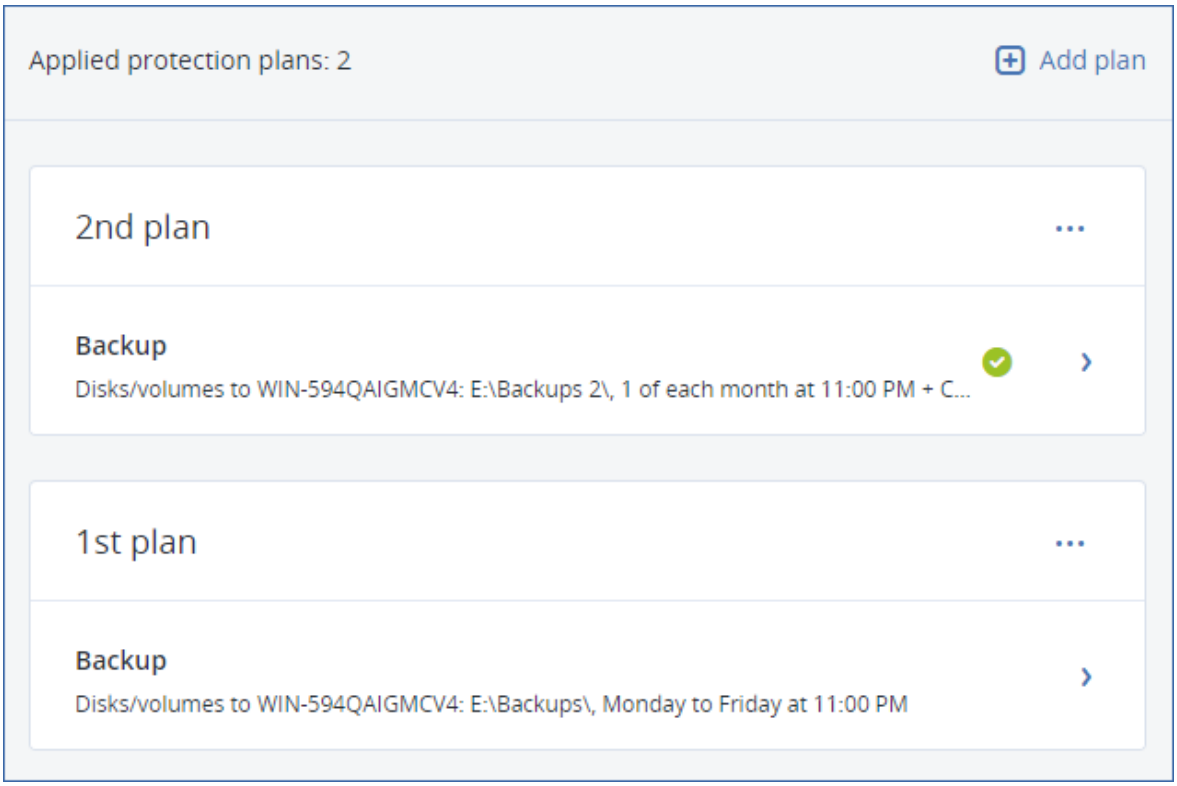
   소프트웨어에서 머신에 적용된 보호 계획을 표시합니다. 머신에 할당된 계획이 없는 경우 적용 가능한 기본 보호 계획이 표시됩니다. 필요한 대로 설정을 조정하고, 이 계획을 적용하거나 새

로운 계획을 생성할 수 있습니다.

3. 새 계획을 만들려면 **계획 생성**을 클릭합니다. **백업** 모듈을 활성화하고 설정을 언롤합니다.
4. [선택 사항] 보호 계획 이름을 수정하려면 기본 이름을 클릭합니다.
5. [선택 사항] 백업 모듈 매개변수를 수정하려면 보호 계획 패널의 해당 섹션을 클릭합니다.
6. [선택 사항] 백업 옵션을 수정하려면 **백업 옵션** 옆에 있는 **변경**을 클릭합니다.
7. **생성**을 클릭합니다.

기존 보호 계획을 적용하려면

1. 백업하려는 머신을 선택합니다.
2. **보호**를 클릭합니다. 선택한 머신에 이미 공통 보호 계획이 적용되어 있는 경우 **계획 추가**를 클릭합니다.
   소프트웨어에 이전에 생성한 보호 계획이 표시됩니다.



3. 적용할 보호 계획을 선택합니다.
4. **적용**을 클릭합니다.

백업 모듈 치트 시트

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

다음 표는 사용 가능한 백업 모듈 매개변수를 요약해서 보여줍니다. 이 표를 사용하여 필요에 가장 잘 맞는 보호 계획을 생성할 수 있습니다.

백업할 대상	백업할 항목 선택 방법	백업할 위치	예약 백업 구성표 (클라우드의 경우 해당 안 됨)	보관 기간
디스크/볼륨	직접 선택	클라우드	항상 증분(단일	백업 기간별(단일 규칙/백

(실제 머신)	정책 규칙 파일 필터	로컬 폴더 네트워크 폴더 SFTP 서버* NFS* Secure Zone* 관리 위치* 테이프 장치*	파일)* 항상 전체 매주 전체, 매일 증분 매월 전체, 매주 차등, 매일 증분 (GFS) 사용자 정의(F-D-I)	업 세트당) 백업 수별 백업의 총 크기 기준* 무기한 보관
디스크/볼륨 (가상 머신)	정책 규칙 파일 필터	클라우드 로컬 폴더 네트워크 폴더 SFTP 서버* NFS* 관리 위치* 테이프 장치*		
파일(실제 머신에만 해당)	직접 선택 정책 규칙 파일 필터	클라우드 로컬 폴더 네트워크 폴더 SFTP 서버* NFS* Secure Zone* 관리 위치* 테이프 장치	항상 전체 매주 전체, 매일 증분 매월 전체, 매주 차등, 매일 증분 (GFS) 항상 증분(단일 파일)* 사용자 정의(F-D-I)	
ESXi 구성	직접 선택	로컬 폴더 네트워크 폴더 SFTP 서버 NFS*		
시스템 상태 (클라우드 디플로이에서만)	직접 선택	클라우드 로컬 폴더 네트워크 폴더	항상 전체 매주 전체, 매일 증분 사용자 정의(F-I)	
SQL 데이터베이스	직접 선택	클라우드 로컬 폴더 네트워크 폴더		

		관리 위치* 테이프 장치		
Exchange 데이터베이스	직접 선택			
Exchange 사서함	직접 선택	클라우드 로컬 폴더 네트워크 폴더 관리 위치*	항상 증분 (단일 파일)	
Microsoft 365 사서함	직접 선택			백업 기간별(단일 규칙/백업 세트당) 백업 수별 무기한 보관

* 아래 제한 사항을 참조하십시오.

제한 사항

SFTP 서버 및 테이프 장치

- 이러한 위치는 macOS를 실행하는 머신의 백업 대상이 될 수 없습니다.
- 이러한 위치는 애플리케이션 인식 백업에 대한 대상이 될 수 없습니다.
- 이러한 위치에 백업할 경우 **항상 증분(단일 파일)** 백업 구성표를 사용할 수 없습니다.
- 이러한 위치에는 **백업의 총 크기 기준** 보관 규칙을 사용할 수 없습니다.

NFS

- NFS 공유로의 백업은 Windows에서 사용할 수 없습니다.
- NFS 공유에 백업할 경우 파일(실제 머신)에 대해 **항상 증분(단일 파일)** 백업 구성표를 사용할 수 없습니다.

Secure Zone

- Secure Zone은 Mac에서 생성할 수 없습니다.

관리되는 위치

- 중복 제거 및 암호화가 활성화된 관리 위치는 대상으로 선택할 수 없습니다.
  - 백업 구성표가 **항상 증분(단일 파일)**으로 설정된 경우
  - 백업 형식이 **버전 12**로 설정된 경우
  - macOS를 실행하는 머신의 디스크 수준 백업의 경우
  - Exchange 사서함 및 Microsoft 365 사서함 백업의 경우
- 중복 제거가 활성화된 관리 위치에는 **백업의 총 크기 기준** 보관 규칙을 사용할 수 없습니다.

항상 증분(단일 파일)

- SFTP 서버 또는 테이프 장치에 백업할 경우 **항상 증분(단일 파일)** 백업 구성표를 사용할 수 없습니다.
- 기본 백업 위치가 Cloud인 경우에만 파일(실제 머신)에 대해 **항상 증분(단일 파일)** 백업 구성표를 사용할 수 있습니다.

백업의 총 크기 기준

- **백업의 총 크기 기준** 보관 규칙을 사용할 수 없습니다.
  - 백업 구성표가 **항상 증분(단일 파일)**으로 설정된 경우
  - SFTP 서버, 테이프 장치 또는 중복 제거가 활성화된 관리 위치에 백업할 경우.

백업할 데이터 선택

전체 머신 선택

전체 머신의 백업은 머신의 제거할 수 없는 모든 디스크 백업입니다.

이러한 백업을 구성하려면 **백업 대상**에서 **전체 머신**을 선택합니다.

중요

USB 플래시 드라이브나 USB 하드 드라이브와 같은 외장형 드라이브는 **전체 머신** 백업에 포함되지 않습니다. 이러한 드라이브를 백업하려면 **디스크/볼륨** 백업을 구성합니다. 디스크 백업에 대한 자세한 내용은 "디스크/볼륨 선택"(198페이지) 항목을 참조하십시오.

디스크/볼륨 선택

디스크 수준 백업에는 디스크 또는 볼륨의 사본이 패키지 형태로 들어 있습니다. 디스크 수준 백업에서 개별 디스크, 볼륨 또는 파일을 복구할 수 있습니다. 전체 머신의 백업은 머신의 제거할 수 없는 모든 디스크 백업입니다.

참고
OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 아카이브에서 유효하지 않은 내용이 포함됩니다.

디스크/볼륨을 선택하는 방법은 각 머신에서 직접 선택하는 방법과 정책 규칙을 사용하는 방법, 두 가지입니다. 파일 필터를 설정하여 디스크 백업에서 파일을 제외할 수 있습니다.

직접 선택

직접 선택은 실제 머신의 경우에만 사용할 수 있습니다. 가상 머신에서 디스크 및 볼륨의 직접 선택을 활성화하려면 해당 게스트 운영 체제에 보호 에이전트를 설치해야 합니다.

1. **백업 대상**에서 **디스크/볼륨**을 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **직접**을 선택합니다.
4. 보호 계획에 포함된 각 머신에 대해 백업할 디스크 또는 볼륨 옆에 있는 확인란을 선택합니다.
5. **완료**를 클릭합니다.

정책 규칙 사용

1. **백업 대상**에서 **디스크/볼륨**을 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **정책 규칙 사용**을 선택합니다.
4. 사전 정의된 규칙 중 하나를 선택하거나, 자체 규칙을 입력하거나 두 가지 방법을 함께 사용합니다.

   정책 규칙이 보호 계획에 포함된 모든 머신에 적용됩니다. 백업 시작 시 하나 이상의 규칙을 충족하는 데이터가 머신에 없으면 해당 머신에서는 백업에 실패합니다.
5. **완료**를 클릭합니다.

Windows, Linux 및 macOS에 대한 규칙

- `[All Volumes]`은 Windows를 실행 중인 머신에 있는 모든 볼륨과 Linux 또는 macOS를 실행 중인 머신에 있는 마운트된 모든 볼륨을 선택합니다.

Windows에 대한 규칙

- 드라이브 문자(예: **C:**)는 지정된 드라이브 문자로 표시되는 볼륨을 선택합니다.
- `[Fixed Volumes(physical machines)]`은 이동식 미디어 이외에 실제 머신의 모든 볼륨을 선택합니다. 고정된 볼륨에는 SCSI, ATAPI, ATA, SSA, SAS 및 SATA 장치와 RAID 어레이의 볼륨이 있습니다.
- `[BOOT+SYSTEM]`에서는 부트 볼륨과 시스템 볼륨을 선택합니다. 이 조합은 백업에서 운영 체제 복구를 보장하는 최소 데이터 집합입니다.

- [BOOT+SYSTEM DISK(physical machines)]에서는 부트 볼륨과 시스템 볼륨이 있는 디스크의 모든 볼륨을 선택합니다. 부트 볼륨과 시스템 볼륨이 같은 디스크에 있지 않으면 아무것도 선택되지 않습니다. 이 규칙은 실제 머신에만 적용됩니다.
- [Disk 1]은 머신의 첫 번째 디스크를 선택합니다(해당 디스크의 모든 볼륨 포함). 다른 디스크를 선택하려면 해당하는 번호를 입력합니다.

Linux에 대한 규칙

- /dev/hda1은 첫 번째 IDE 하드 디스크에서 첫 번째 볼륨을 선택합니다.
- /dev/sda1은 첫 번째 SCSI 하드 디스크에서 첫 번째 볼륨을 선택합니다.
- /dev/md1은 첫 번째 소프트웨어 RAID 하드 디스크를 선택합니다.

다른 기본 볼륨을 선택하려면 /dev/xdyN을 지정합니다. 여기서 각 문자는 다음과 같습니다.

- "x"는 디스크 유형에 해당합니다.
- "y"는 디스크 번호에 해당합니다(첫 번째 디스크의 경우 a, 두 번째 디스크의 경우 b 등).
- "N"은 볼륨 번호입니다.

논리 볼륨을 선택하려면 루트 계정에서 ls /dev/mapper 명령을 실행한 후에 표시되도록 그 경로를 지정합니다. 예:

```
[root@localhost ~]# ls /dev/mapper/
control vg_1-lv1 vg_1-lv2
```

이 출력은 두 가지 논리 볼륨, **lv1** 및 **lv2**를 표시하며, 이 둘은 볼륨 그룹 **vg_1**에 속합니다. 이 볼륨을 백업하려면 다음을 입력합니다.

```
/dev/mapper/vg_1-lv1
/dev/mapper/vg-l-lv2
```

macOS에 대한 규칙

- [Disk 1]은 머신의 첫 번째 디스크를 선택합니다(해당 디스크의 모든 볼륨 포함). 다른 디스크를 선택하려면 해당하는 번호를 입력합니다.

디스크 또는 볼륨 백업은 어떤 항목을 저장합니까?

디스크 또는 볼륨 백업은 운영 체제 부팅에 필요한 모든 정보와 함께 디스크 또는 볼륨 **파일 시스템** 전체를 저장합니다. 해당 백업과 개별 폴더 또는 파일에서 전체 디스크 또는 볼륨을 복구할 수 있습니다.

섹터 단위(원시 모드) 백업 옵션을 활성화하면 디스크 백업 시 모든 디스크 섹터가 저장됩니다. 섹터별 백업은 알 수 없거나 지원되지 않는 파일 시스템 및 기타 독점 데이터 형식을 가진 드라이브를 백업하는 경우 사용할 수 있습니다.

Windows

볼륨 백업은 해당 속성(숨김 파일과 시스템 파일 포함), 부트 레코드, 파일 할당 테이블(FAT)(있는 경우), 마스터 부트 레코드(MBR)가 있는 하드 디스크의 루트 및 제로 트랙과는 별도로 선택된 볼륨의

다른 모든 파일과 폴더를 저장합니다.

디스크 백업은 선택된 디스크의 모든 볼륨(공급업체의 유지보수 파티션과 같은 숨겨진 볼륨 포함)과 마스터 부트 레코드가 있는 제로 트랙을 저장합니다.

다음 항목은 디스크 또는 볼륨 백업(및 파일 수준 백업)에 포함되지 *않습니다*.

- 머신이 최대 절전 모드에 진입할 때 RAM 내용을 보관하는 파일(hiberfil.sys)과 스왑 파일(pagefile.sys). 복구 후에 이 파일이 해당 위치에 0 크기로 다시 생성됩니다.
- 백업이 운영 체제에서 수행되는 경우(부트 가능한 미디어 또는 하이퍼바이저 수준의 가상 머신 백업과 다름):
  - Windows 섀도 스토리지. 해당 경로는 레지스트리 값 **VSS Default Provider**에서 결정됩니다. 이 값은 레지스트리 키 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup**에서 찾을 수 있습니다. 따라서 Windows 7부터는 운영 체제에서 Windows 복원 지점이 백업되지 않습니다.
  - **VSS(Volume Shadow Copy Service)** 백업 옵션이 활성화된 경우 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 레지스트리 키에 지정된 파일 및 폴더.

Linux

볼륨 백업은 해당 속성, 부트 레코드 및 파일 시스템 수퍼 블록과는 별도로 선택된 볼륨의 모든 파일과 디렉토리를 저장합니다.

디스크 백업은 마스터 부트 레코드가 있는 제로 트랙뿐 아니라 모든 디스크 볼륨을 저장합니다.

Mac

디스크 또는 볼륨 백업은 선택한 디스크 또는 볼륨의 모든 파일 및 디렉토리와 함께 볼륨 레이아웃의 설명을 저장합니다.

다음 항목은 제외됩니다.

- 파일 시스템 저널 및 Spotlight 색인과 같은 시스템 메타데이터
- 휴지통
- Time Machine 백업

실제로 Mac의 디스크와 볼륨은 파일 수준에 백업됩니다. 디스크 및 볼륨 백업에서 베어 메탈 복구가 가능하지만 섹터 단위 백업 모드를 사용할 수 없습니다.

파일/폴더 선택

파일 수준 백업은 게스트 시스템에 설치되어 있는 에이전트에 의해 백업되는 실제 머신 및 가상 머신에 사용할 수 있습니다.

파일 수준 백업은 운영 체제를 복구하는 데에는 충분하지 않습니다. 특정 데이터만(예: 현재 프로젝트) 보호하려는 경우에는 파일 백업을 선택합니다. 그러면 백업 크기가 줄어들기 때문에 스토리지 공간이 절약됩니다.

참고

OneDrive 루트 폴더는 백업 작업에서 기본적으로 제외됩니다. 특정 OneDrive 파일 및 폴더를 백업하도록 선택하는 경우 이러한 항목만 백업됩니다. 장치에서 사용할 수 없는 파일에는 아카이브에서 유효하지 않은 내용이 포함됩니다.

파일을 선택하는 방법은 각 머신에서 직접 선택하는 방법과 정책 규칙을 사용하는 방법, 두 가지입니다. 두 방법 모두 파일 필터를 설정하여 선택을 구체화할 수 있습니다.

직접 선택

1. **백업 대상**에서 **파일/폴더**를 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **직접**을 선택합니다.
4. 보호 계획에 포함된 각 머신에 대해 다음을 수행합니다.
   a. **파일 및 폴더 선택**을 클릭합니다.
   b. **로컬 폴더** 또는 **네트워크 폴더**를 클릭합니다.
      선택한 머신에서 공유에 액세스할 수 있어야 합니다.
   c. 필요한 파일/폴더로 이동하거나 경로를 입력한 다음 화살표 버튼을 클릭합니다. 메시지가 표시되면 공유 폴더에 대한 사용자 이름과 비밀번호를 지정합니다.
      익명 액세스를 이용하여 폴더를 백업하는 작업은 지원되지 않습니다.
   d. 필요한 파일/폴더를 선택합니다.
   e. **완료**를 클릭합니다.

정책 규칙 사용

1. **백업 대상**에서 **파일/폴더**를 선택합니다.
2. **백업할 항목**을 클릭합니다.
3. **백업할 항목 선택**에서 **정책 규칙 사용**을 선택합니다.
4. 사전 정의된 규칙 중 하나를 선택하거나, 자체 규칙을 입력하거나 두 가지 방법을 함께 사용합니다.
   정책 규칙이 보호 계획에 포함된 모든 머신에 적용됩니다. 백업 시작 시 하나 이상의 규칙을 충족하는 데이터가 머신에 없으면 해당 머신에서는 백업에 실패합니다.
5. **완료**를 클릭합니다.

Windows에 대한 선택 규칙

- 파일 또는 폴더에 대한 전체 경로(예: **D:\Work\Text.doc** 또는 **C:\Windows**).
- 템플릿:
  - `[All Files]`는 머신의 모든 볼륨에서 모든 파일을 선택합니다.
  - `[All Profiles Folder]`는 모든 사용자 프로필이 위치한 폴더(보통, **C:\Users** 또는 **C:\Documents and Settings**)를 선택합니다.
- 환경 변수:

- %ALLUSERSPROFILE%은 모든 사용자 프로필의 공통 데이터가 위치한 폴더(보통, **C:\ProgramData** 또는 **C:\Documents and Settings\All Users**)를 선택합니다.
- %PROGRAMFILES%는 Program Files 폴더(예: **C:\Program Files**)를 선택합니다.
- %WINDIR%은 Windows가 위치한 폴더(예: **C:\Windows**)를 선택합니다.

다른 환경 변수 또는 환경 변수와 텍스트의 조합을 사용할 수 있습니다. 예를 들어 Program Files 폴더에 있는 Java 폴더를 선택하려는 경우 **%PROGRAMFILES%\Java**를 입력합니다.

Linux에 대한 선택 규칙

- 파일 또는 디렉토리에 대한 전체 경로. 예를 들어, **/home/usr/docs**에 마운트된 **/dev/hda3** 볼륨의 **file.txt**를 백업하려면 **/dev/hda3/file.txt** 또는 **/home/usr/docs/file.txt**를 지정합니다.
  - /home은 일반 사용자의 홈 디렉토리를 선택합니다.
  - /root는 루트 사용자의 홈 디렉토리를 선택합니다.
  - /usr는 모든 사용자 관련 프로그램의 디렉토리를 선택합니다.
  - /etc는 시스템 구성 파일의 디렉토리를 선택합니다.
- 템플릿:
  - [All Profiles Folder]는 **/home**을 선택합니다. 이는 모든 사용자 프로파일이 기본적으로 위치하는 폴더입니다.

macOS에 대한 선택 규칙

- 파일 또는 디렉토리에 대한 전체 경로.
- 템플릿:
  - [All Profiles Folder]는 **/Users**를 선택합니다. 이는 모든 사용자 프로파일이 기본적으로 위치하는 폴더입니다.

예:

- 데스크탑에서 **file.txt**를 백업하려면 **/Users/<username>/Desktop/file.txt**를 지정합니다. 여기서 <username>은 내 사용자 이름입니다.
- 사용자의 모든 홈 디렉토리를 백업하려면 **/Users**를 지정합니다.
- 애플리케이션이 설치된 디렉토리를 백업하려면 **/Applications**를 지정합니다.

시스템 상태 선택

시스템 상태 백업은 Windows 7 이상을 실행 중인 머신에 대해 사용할 수 있습니다.

시스템 상태를 백업하려면 **백업 대상**에서 **시스템 상태**를 선택합니다.

시스템 상태 백업은 다음 파일로 구성됩니다.

- 작업 스케줄러 구성
- VSS 메타데이터 저장소
- 성능 카운터 구성 정보
- MSSearch 서비스
- BITS(Background Intelligent Transfer Service)

- 레지스트리
- WMI(Windows Management Instrumentation)
- 컴퍼넌트 서비스 클래스 등록 데이터베이스

ESXi 구성 선택

ESXi 호스트 구성 백업을 통해 ESXi 호스트를 베어 메탈로 복구할 수 있습니다. 복구는 부트 가능한 미디어에서 수행됩니다.

해당 호스트에서 실행 중인 가상 머신은 백업에 포함되지 않습니다. 가상 머신은 따로 백업 및 복구할 수 있습니다.

ESXi 호스트 구성의 백업에는 다음이 포함됩니다.

- 호스트의 부트로더 및 부트 뱅크 파티션.
- 호스트 상태(가상 네트워킹 및 스토리지 구성, SSL 키, 서버 네트워크 설정, 로컬 사용자 정보).
- 호스트에 설치 또는 스테이징되어 있는 확장 및 패치.
- 로그 파일.

사전 요구 사항

- SSH가 ESXi 호스트 구성의 **보안 프로필**에서 활성화되어 있어야 합니다.
- ESXi 구성을 백업하는 경우 Agent for VMware는 TCP 포트 22에서 SSH 연결을 통해 ESXi 호스트에 연결합니다. 방화벽에서 이 연결을 차단하지 않는지 확인하십시오.
- ESXi 호스트의 '루트' 계정 비밀번호를 알고 있어야 합니다.

제한 사항

- ESXi 구성 백업은 VMware vSphere 7.0에 대해 지원되지 않습니다.
- ESXi 구성을 클라우드 스토리지에 백업할 수 없습니다.

ESXi 구성을 선택하려면

1. **장치** > **모든 장치**를 클릭하고 백업하려는 ESXi 호스트를 선택합니다.
2. **백업**을 클릭합니다.
3. **백업 대상**에서 **ESXi 구성**을 선택합니다.
4. **ESXi '루트' 비밀번호**에서 선택한 각 호스트의 '루트' 계정 비밀번호를 지정하거나 모든 호스트에 동일한 비밀번호를 적용합니다.

지속적인 데이터 보호(CDP)

백업은 주기적으로 수행되지만 성능 관련 이유로 시간 간격은 긴 경우가 일반적입니다. 시스템이 갑자기 손상되면 마지막 백업과 시스템 오류 사이 변경된 데이터가 유실됩니다.

지속적인 데이터 보호 기능을 통해 예약된 백업 사이 선택한 데이터의 변경 사항을 지속적으로 백업할 수 있습니다.

- 지정한 파일/폴더에서 변경 사항 추적
- 지정된 애플리케이션에서 수정한 파일의 변경 사항 추적

백업에 대해 선택한 데이터에서 지속적인 데이터 보호를 위한 특정 파일을 선택할 수 있습니다. 시스템이 이 파일에 대한 변경 사항을 모두 백업합니다. 이러한 파일을 마지막 변경 시간으로 복구할 수 있습니다.

현재 **지속적인 데이터 보호** 기능은 다음 운영 체제에서 지원됩니다.

- Windows 7 이상
- Windows Server 2008 R2 이상

지원되는 파일 시스템: NTFS 전용, 로컬 폴더 전용(공유 폴더는 지원되지 않음)

지속적인 데이터 보호 옵션은 **애플리케이션 백업** 옵션과 호환될 수 없습니다.

참고
기능은 버전별로 다릅니다. 이 문서에 설명된 일부 기능은 사용자의 라이선스로 사용하지 못할 수 있습니다. 각 버전에 포함된 기능에 대한 자세한 내용은 클라우드 디플로이를 포함한 Acronis Cyber Protect 15 버전 비교를 참조하십시오.

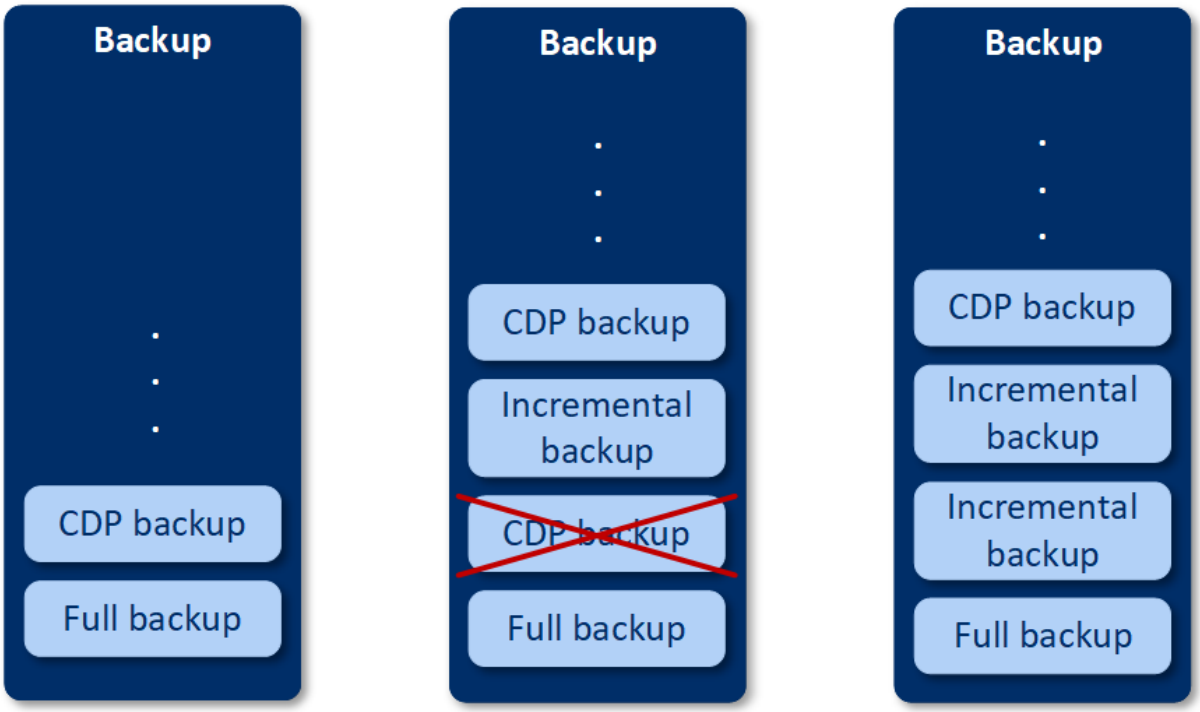
작동법

지속적으로 생성되는 백업을 CDP 백업이라고 부릅니다. CDP 백업을 생성하려면 사전에 전체 백업 또는 증분 백업을 생성해야 합니다.

처음으로 백업 모듈을 사용해 보호 계획을 실행하고 **지속적인 데이터 보호**를 활성화한 경우 전체 백업이 먼저 생성됩니다. 그 후 바로 선택하거나 변경한 파일/폴더에 대한 CDP 백업이 생성됩니다. CDP 백업은 언제나 최신 상태에서 선택한 데이터를 포함합니다. 선택한 파일/폴더를 변경하려 할 때 새로운 CDP 백업이 생성되지 않았다면 모든 변경 사항이 동일한 CDP 백업에 기록됩니다.

예약된 증분 백업 시간이 오면 CDP 백업이 드롭되고 증분 백업이 끝난 후 새로운 CDP 백업이 생성됩니다.

이렇게 CDP 백업은 언제나 백업 체인에서 최신 백업 상태를 유지하며 보호되는 파일/폴더의 실제 최신 상태를 보유합니다.



이미 백업 모듈이 활성화된 보호 계획이 있으며 **지속적인 데이터 보호**를 활성화하기로 선택한 경우, 백업 체인에 이미 전체 백업이 있다면 이 옵션을 활성화한 후 바로 CDP 백업이 생성됩니다.

지속적인 데이터 보호를 지원하는 데이터 소스와 대상

지속적인 데이터 보호가 제대로 작동하려면 다음 데이터 소스에 대해 다음 항목을 지정해야 합니다.

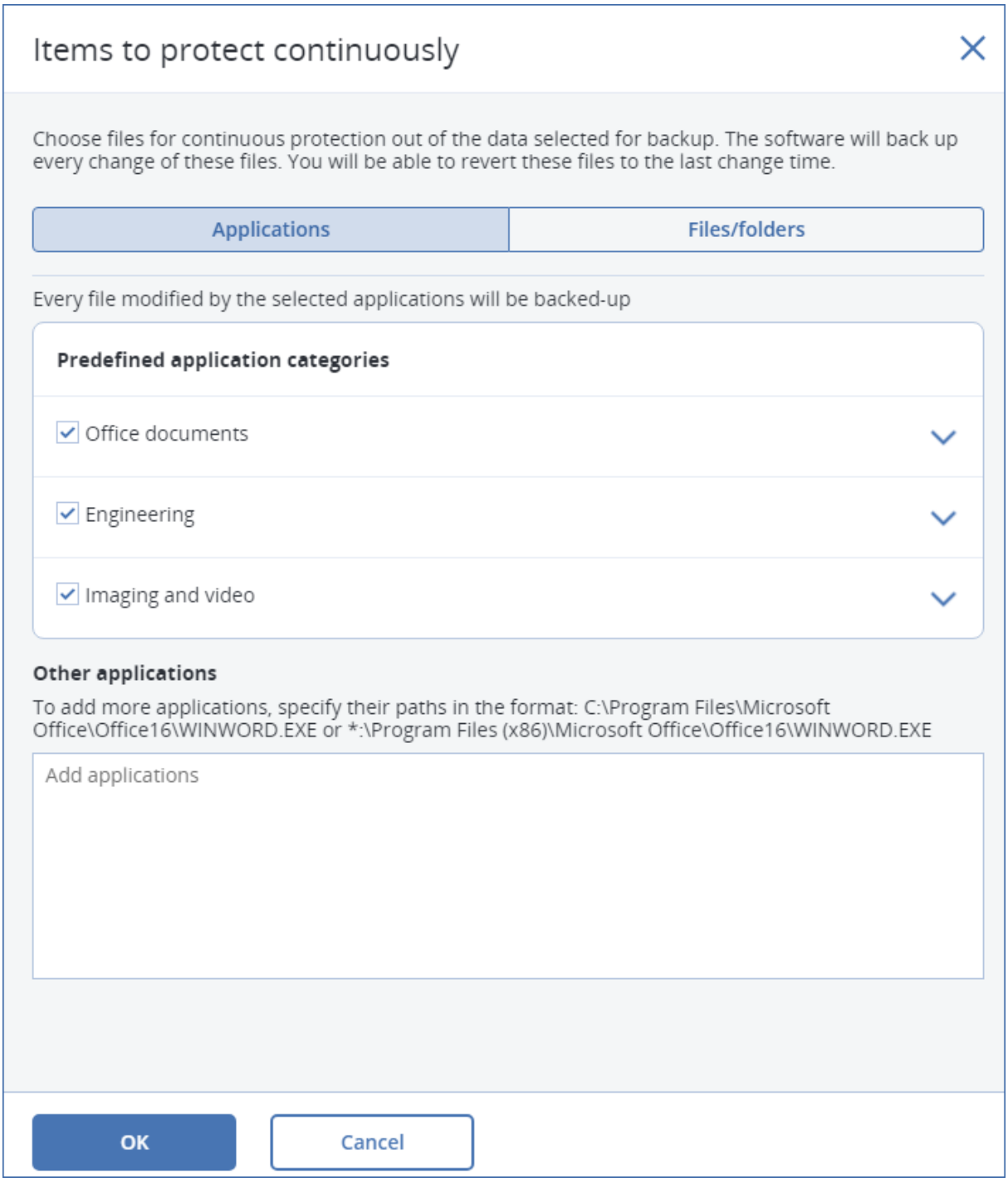
백업 대상	백업할 항목
전체 머신	파일/폴더 또는 애플리케이션을 지정해야 함
디스크/볼륨	디스크/볼륨 및 파일/폴더 또는 애플리케이션 지정 필요
파일/폴더	파일/폴더 지정 필요 애플리케이션을 지정할 수 있음(필수 사항 아님)

지속적인 데이터 보호에 대해 다음 백업 목적지가 지원됩니다.

- 로컬 폴더
- 네트워크 폴더
- 스크립트에서 정의한 위치
- 클라우드 스토리지
- Acronis Cyber Infrastructure

지속적인 데이터 보호로 장치를 보호하려면

1. Cyber Protect 웹 콘솔에서 **백업** 모듈이 활성화된 보호 계획을 생성합니다.
2. **지속적인 데이터 보호(CDP)** 옵션을 활성화합니다.
3. **지속적으로 보호할 항목**을 지정합니다.
   - **애플리케이션**(선택한 애플리케이션에 의해 수정된 모든 파일이 백업됨)이 옵션을 사용해 CDP 백업으로 Office 문서를 보호하는 것이 좋습니다.



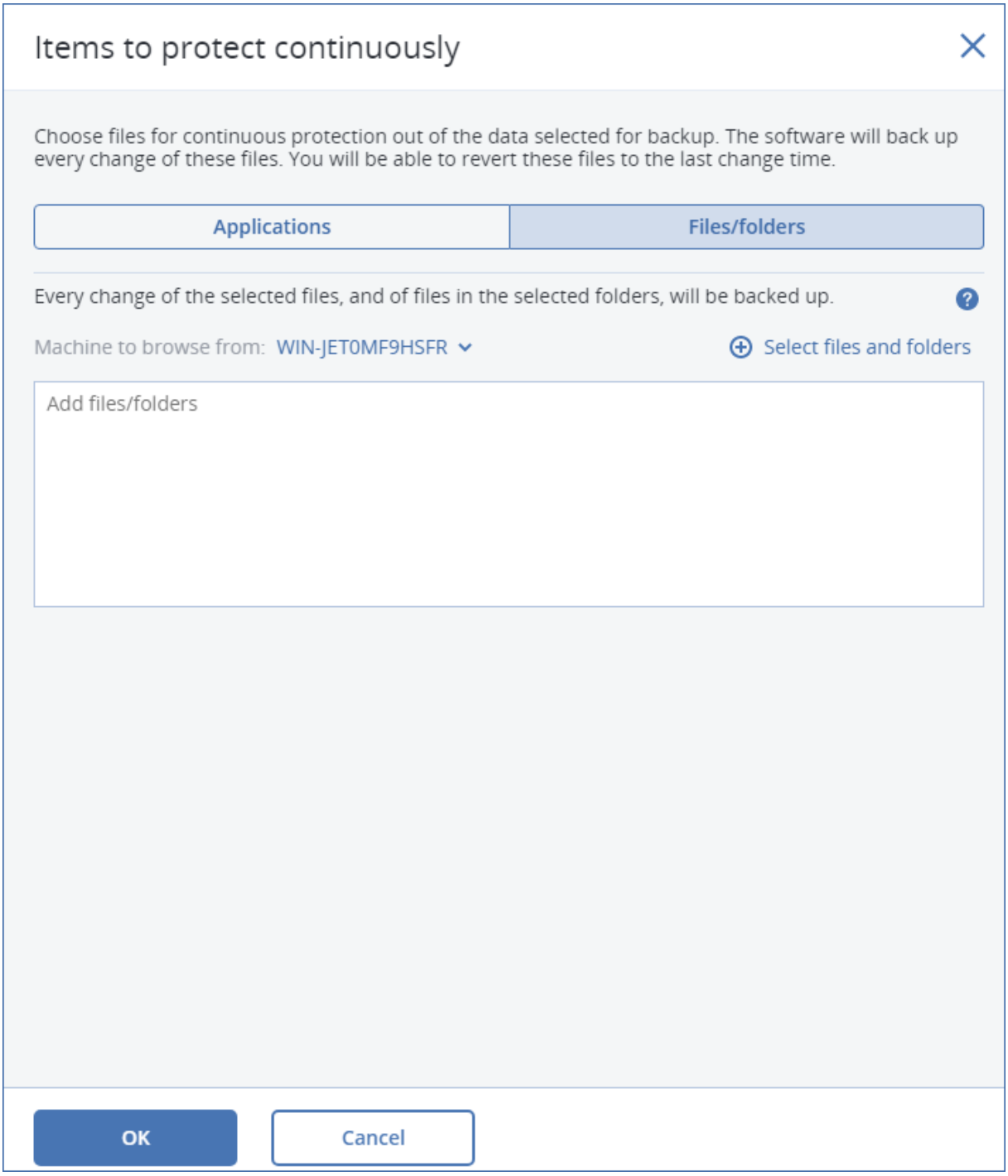
- 사전 정의된 카테고리에서 애플리케이션을 선택하거나 애플리케이션 실행 파일 경로를 정의해 다른 애플리케이션을 지정할 수 있습니다. 다음 형식 중 하나를 사용하십시오.

  `C:\Program Files\Microsoft Office\Office16\WINWORD.EXE`

OR

`*:\Program Files (x86)\Microsoft Office\Office16\WINWORD.EXE`

- **파일/폴더**(지정 위치의 수정된 모든 파일이 백업됨)지속적으로 변경되는 파일과 폴더를 보호하려면 이 옵션을 사용하는 것이 좋습니다.



1. **다음 위치에서 탐색할 머신** – 지속적인 데이터 보호를 위해 파일/폴더를 선택하려는 머신을 지정합니다.

   파일 및 폴더 선택을 클릭해 지정한 머신의 파일/폴더를 선택합니다.

중요
지속적으로 백업할 파일이 있는 전체 폴더를 수동으로 지정하려면 마스크를 사용하십시오. 예를 들면 다음과 같습니다.
올바른 경로:D:\Data*
잘못된 경로: D:\Data\

텍스트 필드에 백업할 파일/폴더를 선택하기 위한 규칙을 지정할 수 있습니다. 규칙 정의에 대한 자세한 내용은 "파일/폴더 선택"을 참고하십시오. 준비가 되면 **완료**를 클릭합니다.

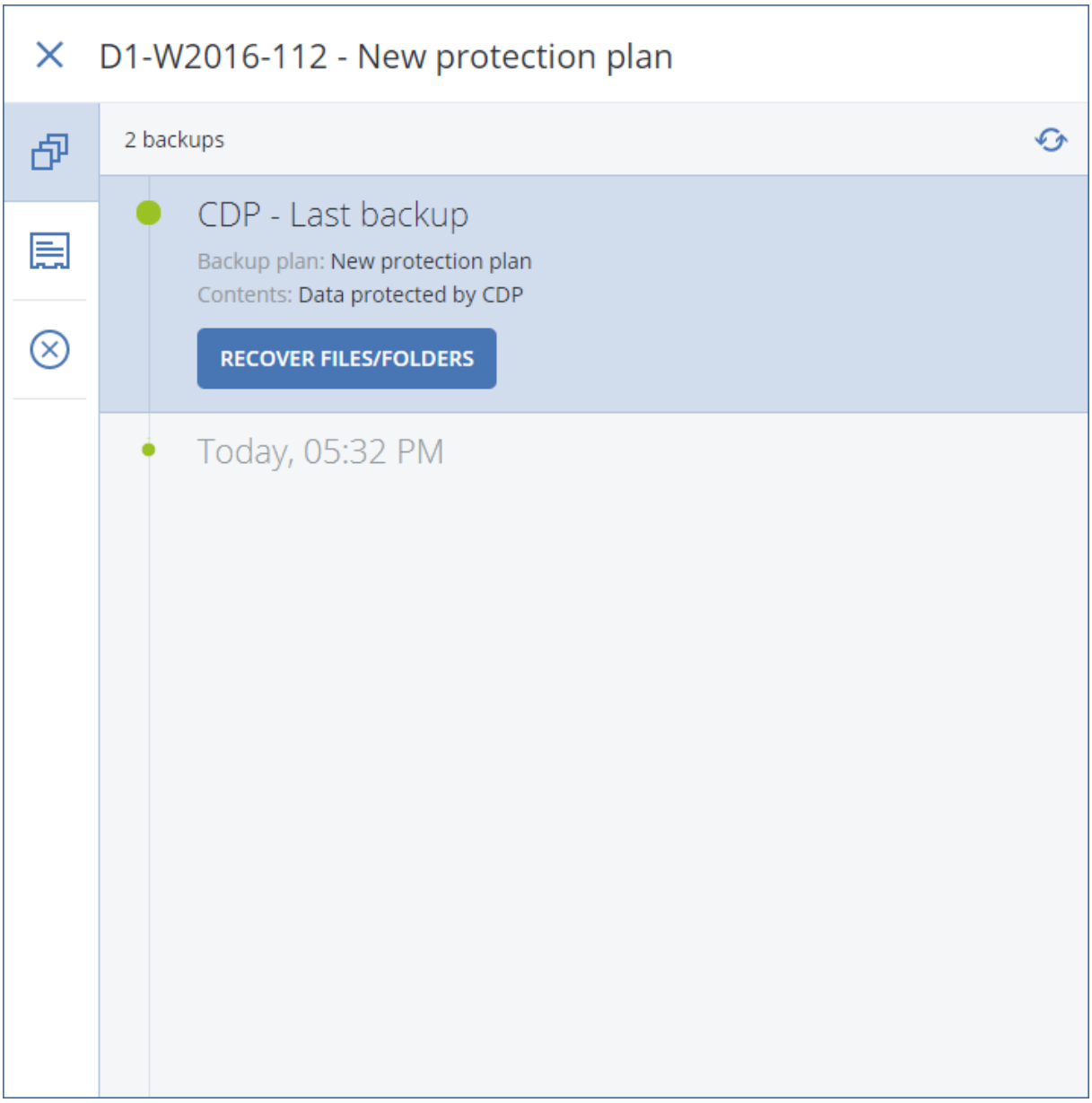
2. **생성**을 클릭합니다.

이렇게 하면 지속적인 데이터 보호가 활성화된 보호 계획이 선택 머신에 할당됩니다. 첫 번째 정규 백업 후 CDP 데이터로 보호되는 최신 복사본을 포함한 백업이 지속적으로 생성됩니다. 애플리케이션과 파일/폴더를 통해 정의된 데이터 모두 백업됩니다.

지속적으로 백업된 데이터는 백업 모듈에서 정의한 보관 정책에 따라 유지됩니다.

지속적인 방식으로 보호되는 백업을 구분하는 방법

지속적인 방식의 백업에는 CDP 접두사가 붙습니다.



전체 머신을 최신 상태로 복구하는 방법

전체 머신을 최신 상태로 복구하려면 보호 계획의 백업 모듈에 있는 **지속적인 데이터 보호(CDP)** 옵션을 사용합니다.

CDP 백업에서 전체 머신 또는 파일/폴더를 복구할 수 있습니다. 전자인 경우 전체 머신을 최신 상태로 복구하고, 후자인 경우 파일/폴더를 최신 상태로 복구합니다.

목적지 선택

중요

이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

백업 위치를 선택하려면

1. **백업할 위치**를 클릭합니다.
2. 다음 중 하나를 수행하십시오.
   - 이전에 사용하거나 미리 정의된 백업 위치 선택
   - **위치 추가**를 클릭하고 새 백업 위치를 지정합니다.

지원되는 위치

- **클라우드 스토리지**

  클라우드 데이터 센터에 백업이 저장됩니다.
- **로컬 폴더**

  단일 머신을 선택한 경우 선택한 머신의 폴더를 찾거나 폴더 경로를 입력합니다.

  여러 머신을 선택한 경우 폴더 경로를 입력합니다. 각 선택한 실제 머신 또는 가상 머신의 에이전트가 설치된 머신에서 백업이 이 폴더에 저장됩니다. 폴더가 없는 경우에는 새로 생성됩니다.
- **네트워크 폴더**

  이 폴더는 SMB/CIFS/DFS를 통해 공유되는 폴더입니다.

  필요한 공유 폴더로 이동하거나 다음 형식으로 경로를 입력합니다.
  - SMB/CIFS 공유의 경우: `\\<호스트 이름>\<경로>>\` 또는 `smb://<호스트 이름>/<경로>/`
  - DFS 공유의 경우: `\\<전체 DNS 도메인 이름>\<DFS 루트>\<경로>`

    예: `\\example.company.com\shared\files`

  그런 다음, 화살표 버튼을 클릭합니다. 메시지가 표시되면 공유 폴더에 대한 사용자 이름과 비밀번호를 지정합니다. 이 자격 증명은 폴더 이름 옆에 있는 열쇠 아이콘을 클릭하여 언제든지 변경할 수 있습니다.

  익명 액세스를 이용하여 폴더에 백업하는 작업은 지원되지 않습니다.
- **Acronis 사이버 인프라**

  Acronis 사이버 인프라은(는) 데이터 중복 기능과 자동 자체 복구 기능이 있는 매우 안정적인 소프트웨어 정의 스토리지로 사용할 수 있습니다. 이 스토리지는 Microsoft Azure 또는 S3나 Swift와 호환되는 여러 스토리지 솔루션 중 하나에 백업을 저장하기 위한 게이트웨이로 구성할 수 있습니다. 또한, 이 스토리지는 NFS 백엔드를 사용할 수도 있습니다. 자세한 내용은 "Acronis 사이버 인프라 정보"를 참조하십시오.

  중요

  macOS 머신에서는 Acronis 사이버 인프라에 백업할 수 없습니다.

- **NFS 폴더**(Linux 또는 macOS를 실행하는 머신에서 사용 가능)

  Linux용 에이전트가 설치되어 있는 Linux 머신에 nfs-utils 패키지가 설치되어 있는지 확인합니다.

  필요한 NFS 폴더로 이동하거나 다음 형식으로 경로를 입력합니다.

  `nfs://<호스트 이름>/<내보낸 폴더>:/<하위 폴더>`

  그런 다음, 화살표 버튼을 클릭합니다.

  비밀번호로 보호되는 NFS 폴더로는 백업할 수 없습니다.
- **Secure Zone**(선택한 각 머신에 있는 경우 사용 가능)

Secure Zone은 백업된 머신의 디스크에 있는 보안 파티션입니다. 백업 구성 전에 이 파티션을 수동으로 생성해야 합니다. Secure Zone을(를) 생성하는 방법, 장점과 제한 사항에 관한 자세한 내용은 "Secure Zone 정보"를 참조하십시오.

- **SFTP**

  SFTP 서버 이름 또는 주소를 입력합니다. 다음 표기법이 지원됩니다.

  `sftp://<서버>`

  `sftp://<서버>/<폴더>`

  사용자 이름과 비밀번호를 입력한 후 서버 폴더를 찾아볼 수 있습니다.

  한쪽 표기법에서 포트, 사용자 이름 및 비밀번호를 지정할 수도 있습니다.

  `sftp://<서버>:<포트>/<폴더>`

  `sftp://<사용자 이름>@<서버>:<포트>/<폴더>`

  `sftp://<사용자 이름>:<패스워드>@<서버>:<포트>/<폴더>`

  포트 번호가 지정되지 않은 경우, 포트 22가 사용됩니다.

  비밀번호 없이 SFTP 액세스를 구성한 사용자는 SFTP에 백업할 수 없습니다.

  FTP 서버에 백업하는 작업은 지원되지 않습니다.

고급 스토리지 옵션

- **스크립트에서 정의**(Windows 실행 머신에 사용 가능)

  스크립트에서 정의한 폴더에 각 머신의 백업을 저장할 수 있습니다. 소프트웨어는 JScript, VBScript 또는 Python 3.5로 작성된 스크립트를 지원합니다.보호 계획을 배포하는 경우 소프트웨어는 각 머신에서 스크립트를 실행합니다. 각 머신에 대한 스크립트 출력은 로컬 또는 네트워크 폴더 경로여야 합니다. 폴더가 없는 경우에는 새로 생성됩니다(제한: Python으로 작성된 스크립트는 공유 네트워크에 폴더를 생성할 수 없습니다). **백업 스토리지** 탭에서 각 폴더가 별도의 백업 위치로 표시됩니다.

  스크립트 유형에서 스크립트 유형(**JScript**, **VBScript**, 또는 **Python**)을 선택한 다음 스크립트를 가져오거나 복사하고 붙여넣습니다. 네트워크 폴더의 경우 읽기/쓰기 권한이 있는 액세스 자격 증명을 지정합니다.

  예:

  - 다음 **JScript** 스크립트는 머신의 백업 위치를 다음과 같이 `\\bkpsrv\<machine name>` 형식으로 출력합니다.

    ```
    WScript.Echo("\\\\bkpsrv\\" + WScript.CreateObject
    ("WScript.Network").ComputerName);
    ```

  - 다음 **JScript** 스크립트 출력은 스크립트가 실행되는 머신 내 폴더의 백업 위치를 출력합니다.

    ```
    WScript.Echo("C:\\Backup");
    ```

    참고

    이러한 스크립트의 위치 경로는 대/소문자를 구분합니다. 즉, `C:\Backup`과 `C:\backup`은 Cyber Protect 웹 콘솔에서 다른 위치로 표시됩니다.그리고 드라이브 문자에는 대문자를 사용해야 합니다.

  - 다음 **VBScript** 스크립트는 머신의 백업 위치를 다음과 같이 \\bkpsrv\<machine name> 형식으로 출력합니다.

    ```
    WScript.Echo("\\bkpsrv\" + WScript.CreateObject("WScript.Network").ComputerName)
    ```

  따라서 각 머신의 백업은 서버 **bkpsrv**의 이름이 동일한 폴더에 저장됩니다..

- **스토리지 노드**

  스토리지 노드는 엔터프라이즈 데이터 보호에 필요한 다양한 리소스(예: 회사 저장 용량, 네트워크 대역폭 및 프로덕션 서버의 CPU 로드)의 사용 최적화를 목표로 하는 서버입니다. 이 목표는 엔터프라이즈 백업(관리 위치)의 전용 스토리지 기능을 수행하는 위치의 구성 및 관리를 통해 달성됩니다.

  이전에 생성한 위치를 선택하거나 **위치 추가** > **스토리지 노드**를 클릭하여 새 위치를 생성할 수 있습니다. 설정에 대한 자세한 내용은 "관리 위치 추가"를 참조하십시오.

  스토리지 노드의 사용자 이름 및 비밀번호를 지정하라는 메시지가 표시될 수 있습니다. 스토리지 노드가 설치된 머신에서 다음 Windows 그룹에 속한 구성원은 스토리지 노드의 모든 관리 위치에 액세스할 수 있습니다.

  - **관리자**
  - **Acronis ASN Remote Users**

    이 그룹은 스토리지 노드가 설치될 때 자동으로 생성됩니다. 기본적으로 이 그룹은 비어 있습니다. 이 그룹에 수동으로 사용자를 추가할 수 있습니다.

- **테이프**

  테이프 장치가 백업된 머신 또는 스토리지 노드에 연결된 경우 위치 목록에는 기본 테이프 풀이 표시됩니다. 이 풀은 자동으로 생성됩니다.

  기본 풀을 선택하거나 **위치 추가** > **테이프**를 클릭하여 새 풀을 생성할 수 있습니다. 풀 설정에 대한 자세한 내용은 "풀 생성"을 참조하십시오.

Secure Zone 정보

Secure Zone은 백업된 머신의 디스크에 있는 보안 파티션입니다. 여기에는 이 머신의 디스크 또는 파일의 백업을 저장할 수 있습니다.

디스크에 물리적 오류가 발생하는 경우 Secure Zone에 위치한 백업이 손실될 수 있습니다. 따라서 Secure Zone이 백업을 저장하는 유일한 위치가 되면 안 됩니다. 엔터프라이즈 환경에서 Secure Zone은 일반 위치를 일시적으로 사용할 수 없거나 느리거나 사용 중인 채널을 통해 연결된 경우 백업에 사용되는 중간 위치로 여겨집니다.

Secure Zone을 사용하는 이유는 무엇일까요?

Secure Zone:

- 디스크 백업이 상주하는 동일한 디스크로 디스크를 복구할 수 있게 해줍니다.
- 소프트웨어 오작동, 바이러스 공격, 사람의 실수로부터 데이터를 보호할 수 있는 비용 효율적이면서 편리한 방법을 제공합니다.

- 데이터 백업 및 복구를 위한 별도의 미디어 또는 네트워크 연결의 필요성을 없애줍니다. 이는 로밍 사용자에게 특히 유용합니다.
- 백업 복제를 사용하는 경우 주 목적지 역할을 할 수 있습니다.

제한 사항

- Secure Zone은 Mac에서 구성할 수 없습니다.
- Secure Zone은 기본 디스크의 파티션입니다. 동적 디스크에 구성하거나 논리 볼륨(LVM으로 관리)으로 생성할 수 없습니다.
- Secure Zone은 FAT32 파일 시스템으로 포맷되어 있습니다. FAT32는 파일 크기 제한이 4GB이기 때문에 이보다 용량이 큰 백업은 Secure Zone에 저장될 때 분할됩니다. 이는 복구 절차와 속도에 영향을 주지 않습니다.

Secure Zone 생성으로 디스크가 변환되는 방식

- Secure Zone은 항상 하드 디스크 끝에 생성됩니다.
- 디스크 끝에는 할당되지 않은 공간이 없거나 부족하지만 볼륨 사이에 할당되지 않은 공간이 있는 경우 해당 볼륨이 디스크 끝으로 이동하여 할당되지 않은 공간을 보충합니다.
- 모든 할당되지 않은 공간이 수집되었지만 여전히 충분하지 않으면 소프트웨어는 사용자가 선택한 볼륨에서 여유 공간을 확보하며 이와 비례하여 볼륨 크기가 줄어듭니다.
- 하지만 볼륨에 여유 공간이 있어야 운영 체제 및 애플리케이션이 임시 파일 생성 등의 작업을 수행할 수 있습니다. 소프트웨어는 어느 한 볼륨의 여유 공간이 총 볼륨 크기의 25% 이하거나, 그 수준까지 떨어질 염려가 있는 경우 볼륨의 크기를 줄이지 않습니다. 디스크의 모든 볼륨에 여유 공간이 25% 이하일 때에만 소프트웨어가 볼륨의 크기를 비례적으로 계속해서 줄여나갑니다.

위 내용에 비추어 Secure Zone 크기를 최대한으로 지정하는 것은 바람직하지 않습니다. 결국 모든 볼륨에 여유 공간이 없어지면 운영 체제나 애플리케이션이 안정적으로 작동하지 못하고, 아예 시작하지 못하는 일이 생길 수도 있습니다.

중요
시스템이 현재 부팅되어 있는 볼륨을 이동하거나 크기 조정하려면 재부팅해야 합니다.

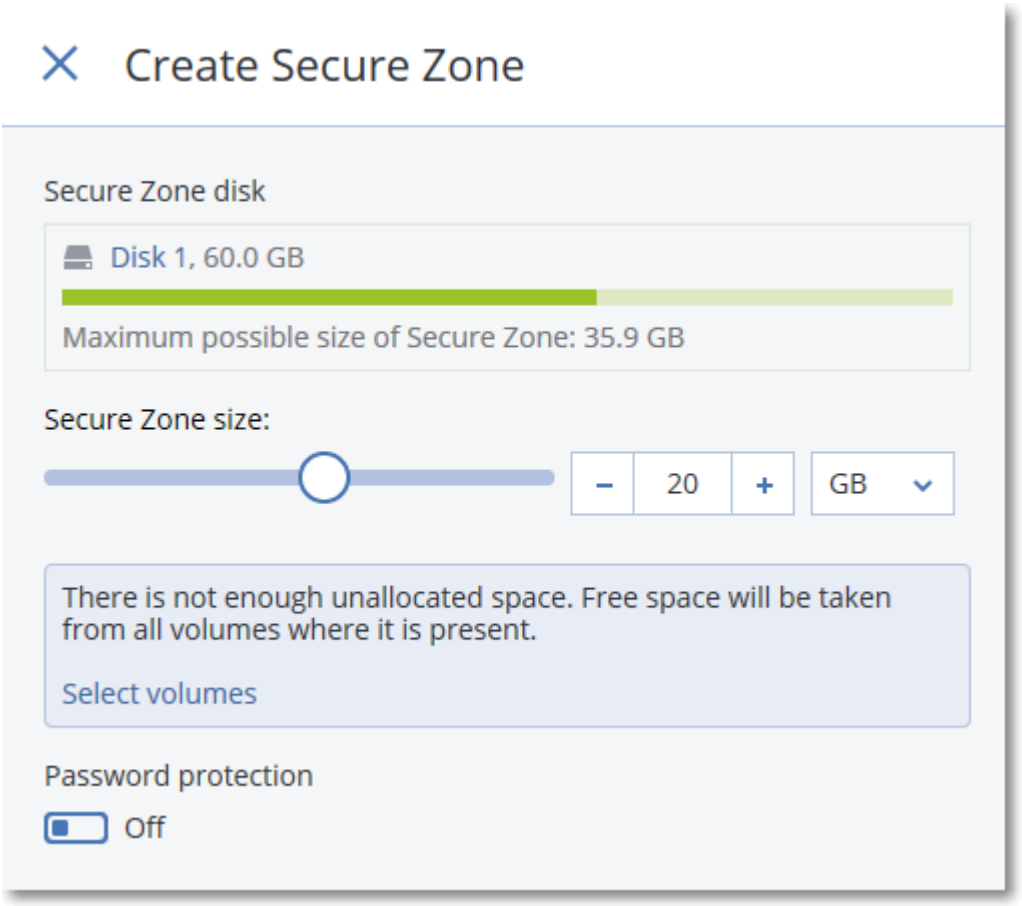
Secure Zone 생성 방법

1. Secure Zone을 생성할 머신을 선택합니다.
2. **상세정보** > **Secure Zone 생성**을 클릭합니다.
3. **Secure Zone 디스크**에서 **선택**을 클릭한 다음, 영역을 생성할 하드 디스크를 선택합니다(여러 개가 있는 경우).

   소프트웨어가 설정 가능한 Secure Zone의 최대 크기를 계산합니다.
4. Secure Zone 크기를 입력하거나 슬라이더를 끌어 최소 크기와 최대 크기 사이의 임의의 크기를 선택합니다.

   최소 크기는 하드 디스크의 구조에 따라 약 50MB 입니다. 최대 크기는 디스크의 할당되지 않은 공간에 모든 디스크 볼륨에 있는 총 여유 공간을 더한 크기와 같습니다.

5. 모든 할당되지 않은 공간이 사용자가 지정한 크기보다 부족한 경우 소프트웨어가 기존 볼륨에서 여유 공간을 확보합니다. 기본적으로 모든 볼륨이 선택되어 있습니다. 일부 볼륨을 제외하려면 **볼륨 선택**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.



6. [선택 사항] **비밀번호 보호** 스위치를 활성화하고 비밀번호를 지정합니다.
   Secure Zone에 위치한 백업에 액세스하려면 비밀번호가 필요합니다. 백업을 부트 가능한 미디어에서 수행하지 않는 한 Secure Zone으로 백업할 때는 비밀번호가 필요하지 않습니다.
7. **생성**을 클릭합니다.
   소프트웨어가 예상 파티션 레이아웃을 표시합니다. **확인**을 클릭합니다.
8. 소프트웨어가 Secure Zone을 생성할 때까지 기다립니다.

이제 보호 계획을 생성할 때 **백업할 위치**로 Secure Zone을 선택할 수 있습니다.

Secure Zone 삭제 방법

1. Secure Zone이 있는 머신을 선택합니다.
2. **상세 정보**를 클릭합니다.
3. **Secure Zone** 옆에 있는 기어 아이콘을 클릭한 다음 **삭제**를 클릭합니다.
4. [선택 사항] 영역에서 사용 가능한 공간을 추가할 볼륨을 지정합니다. 기본적으로 모든 볼륨이 선택되어 있습니다.
   공간은 선택한 볼륨에 균등하게 배분됩니다. 볼륨을 선택하지 않을 경우 확보된 공간은 할당이 취소됩니다.

시스템이 현재 부팅되어 있는 볼륨의 크기를 조정하려면 재부팅해야 합니다.

5. **삭제**를 클릭합니다.

그러면 Secure Zone과 여기에 저장된 모든 백업이 함께 삭제됩니다.

Acronis 사이버 인프라 정보

Acronis Cyber Protect 15는 Acronis 사이버 인프라 3.5 Update 5 이상 버전과의 통합을 지원합니다.

macOS 머신에서는 Acronis 사이버 인프라에 백업할 수 없습니다.

디플로이

Acronis 사이버 인프라을(를) 사용하려면 온-프레미스의 베어 메탈에 디플로이하십시오. 이 제품을 최대한 활용하려면 최소 5대의 실제 서버를 사용하는 것이 좋습니다. 게이트웨이 기능만 필요하다면 실제 서버나 가상 서버 한 대를 사용하거나 원하는 만큼의 서버로 게이트웨이 클러스터를 구성하면 됩니다.

관리 서버와 Acronis 사이버 인프라 간에 시간 설정이 동기화되도록 하십시오. Acronis 사이버 인프라의 시간 설정은 디플로이 중에 구성할 수 있습니다. NTP(네트워크 시간 프로토콜)를 통한 시간 동기화는 기본적으로 활성화되어 있습니다.

Acronis 사이버 인프라 인스턴스를 여러 개 디플로이하고 이를 동일한 관리 서버에 등록할 수 있습니다.

등록

등록은 Acronis 사이버 인프라 웹 인터페이스에서 수행합니다. Acronis 사이버 인프라은(는) 조직 관리자에 의해 조직 내에서만 등록될 수 있습니다. 등록하고 나면 스토리지를 모든 조직 부서가 사용할 수 있습니다. 스토리지는 부서 또는 조직에 백업 위치로 추가할 수 있습니다.

그 반대 작업(등록 취소)은 Acronis Cyber Protect 인터페이스에서 수행합니다. **설정** > **스토리지 노드**를 클릭한 후 필요한 Acronis 사이버 인프라, **삭제**를 차례로 클릭합니다.

백업 위치 추가

각 Acronis 사이버 인프라 인스턴스에 있는 백업 위치 하나만 단위 또는 조직에 추가할 수 있습니다. 부서 수준에서 추가한 위치는 이 부서와 조직 관리자가 사용할 수 있습니다. 조직 수준에서 추가한 위치는 조직 관리자만 사용할 수 있습니다.

위치를 추가할 때 그 이름을 생성하고 입력합니다. 기존 위치를 새 관리 서버 또는 다른 관리 서버에 추가해야 하는 경우 **기존 위치 사용...** 확인란을 선택하고, **찾아보기**를 클릭한 다음 목록에서 해당 위치를 선택합니다.

Acronis 사이버 인프라의 여러 인스턴스가 관리 서버에 등록되어 있는 경우 위치 추가 시 사이버 인프라 인스턴스를 선택할 수 있습니다.

백업 구성표, 작업 및 제한 사항

부트 가능한 미디어에서는 Acronis 사이버 인프라에 직접 액세스할 수 없습니다. Acronis 사이버 인프라(으)로 작업하려면 미디어를 관리 서버에 등록하고 이를 Cyber Protect 웹 콘솔을 통해 관리합니다.

명령줄 인터페이스를 통해서는 Acronis 사이버 인프라에 액세스할 수 없습니다.

사용 가능한 백업 구성표 및 백업 작업은 Acronis 사이버 인프라과(와) 클라우드 스토리지가 유사합니다. 유일한 차이점은 보호 계획의 실행 중에 백업을 Acronis 사이버 인프라*에서* 복제할 수 있다는 점입니다.

문서

Acronis 사이버 인프라 전체 설명서는 Acronis 웹 사이트에서 확인할 수 있습니다.

예약

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

스케줄은 에이전트가 설치되어 있는 운영 체제의 시간 설정(시간대 포함)을 따릅니다. Agent for VMware(가상 어플라이언스)의 시간대는 에이전트의 인터페이스에서 구성할 수 있습니다.

예를 들어 보호 계획이 21:00에 실행되어 각기 다른 시간대의 다양한 머신에 적용되도록 되어 있는 경우, 이러한 백업은 각 머신에서 현지 시간 21:00에 이루어집니다.

예약 매개변수는 백업 목적지에 따라 달라집니다.

클라우드 스토리지에 백업하는 경우

기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다. 백업 실행 시간을 선택할 수 있습니다.

백업 빈도를 변경하려고 하는 경우 슬라이더를 이동한 다음 백업 스케줄을 지정합니다.

시간별이 아닌 이벤트별로 실행할 백업을 예약할 수 있습니다. 이 작업을 수행하려면 스케줄 선택기에서 이벤트 유형을 선택합니다. 자세한 내용은 "이벤트별 예약"을 참조하십시오.

중요
첫 번째 백업은 전체 백업입니다. 즉, 시간이 가장 오래 걸립니다. 이후의 모든 백업은 증분으로 진행되며 시간이 상당히 줄어듭니다.

다른 위치에 백업하는 경우

미리 정의된 백업 구성표 중 하나를 선택하거나 사용자 정의 구성표를 생성할 수 있습니다. 백업 구성표는 백업 스케줄 및 백업 방법을 포함한 보호 계획의 일부입니다.

백업 구성표에서 다음 중 하나를 선택합니다.

- **항상 증분(단일 파일)**

  기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다. 백업 실행 시간을 선택할 수 있습니다.

  백업 빈도를 변경하려고 하는 경우 슬라이더를 이동한 다음 백업 스케줄을 지정합니다.

  이러한 백업은 새로운 단일 파일 백업 형식[1]을 사용합니다.

  테이프 장치나 SFTP 서버에 백업할 때는 이 구성표를 사용할 수 없습니다.
- **항상 전체**

  기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다. 백업 실행 시간을 선택할 수 있습니다.

  백업 빈도를 변경하려고 하는 경우 슬라이더를 이동한 다음 백업 스케줄을 지정합니다.

  모든 백업이 전체 백업입니다.
- **매주 전체, 매일 증분**

  기본적으로 백업이 월요일부터 금요일까지 매일 수행됩니다. 백업을 실행할 요일 및 시간을 변경할 수 있습니다.

  한 주에 한 번 전체 백업을 만듭니다. 그 외의 백업은 모두 증분입니다. 전체 백업이 생성되는 요일은 **주간 백업** 옵션(기어 아이콘을 클릭한 다음 **백업 옵션** > **주간 백업** 클릭)에 따라 다릅니다.
- **매월 전체, 매주 차등, 매일 증분(GFS)**

  기본적으로 증분 백업은 월요일부터 금요일까지 매일 수행되고, 차등 백업은 매주 토요일에 수행되고, 전체 백업은 매월 1일에 수행됩니다. 이러한 스케줄과 백업을 실행할 시간을 수정할 수 있습니다.

  이 백업 구성표는 보호 계획 패널에 **사용자 정의** 구성표로 표시됩니다.
- **사용자 정의**

  전체, 차등 및 증분 백업의 일정을 지정합니다.

  SQL 데이터, Exchange 데이터 또는 시스템 상태를 백업할 때는 차등 백업을 사용할 수 없습니다.

백업 구성표를 사용하면 시간별이 아닌 이벤트별로 실행할 백업을 예약할 수 있습니다. 이 작업을 수행하려면 스케줄 선택기에서 이벤트 유형을 선택합니다. 자세한 내용은 "이벤트별 예약"을 참조하십시오.

추가 예약 옵션

모든 목적지에 대해 다음 작업을 수행할 수 있습니다.

- 조건이 충족되는 경우에만 예약된 백업이 수행되도록 백업 시작 조건을 지정합니다. 자세한 내용은 "시작 조건"을 참조하십시오.

[1]초기 전체 백업 및 이후 증분 백업은 여러 개의 파일이 아니라, 새로운 백업 형식인 단일 .tib 파일에 저장됩니다. 이 형식은 오래된 백업의 삭제가 어렵다는 주요 단점을 피하면서 증분 백업 방식의 빠른 속도를 활용합니다. 이 소프트웨어는 오래된 백업에서 사용하는 블록을 "여유"로 표시하고 이러한 블록에 새 백업을 씁니다. 이를 통해 최소한의 리소스를 사용하여 매우 빠른 정리가 가능합니다. 임의 액세스 읽기 및 쓰기가 지원되지 않는 위치로 백업할 때는 단일 파일 백업 형식을 사용할 수 없습니다(예: SFTP 서버).

- 스케줄이 적용되는 날짜 범위를 설정합니다. **날짜 범위 내에서 계획 실행** 확인란을 선택한 다음 날짜 범위를 지정합니다.
- 스케줄을 비활성화합니다. 스케줄을 사용하지 않도록 설정한 동안에는 백업을 수동으로 시작하지 않는 한 보관 규칙이 적용되지 않습니다.
- 예약된 시간보다 지연되어 시작됩니다. 각 머신에 대한 지연 값은 임의로 선택되며 이 값의 범위는 0에서부터 지정된 최대값까지 입니다. 여러 머신을 네트워크 위치로 백업하는 경우 과도한 네트워크 부하를 피하기 위해 이 설정을 사용할 수 있습니다.

  기어 아이콘을 클릭한 다음 **백업 옵션** > **예약**을 선택합니다. **일정 시간 내에 백업 시작 시간 분배**를 선택하고 최대 지연을 지정합니다. 보호 계획이 머신에 적용될 때 각 머신에 대한 지연 값이 결정되어 보호 계획을 편집하고 최대 지연 값을 변경할 때까지 동일하게 유지됩니다.

  참고
  클라우드 디플로이에서는 이 옵션을 기본적으로 사용하도록 설정되어 있으며 최대 지연은 30분으로 설정되어 있습니다. 온프레미스 디플로이에서는 기본적으로 모든 백업이 스케줄에 따라 정확하게 시작됩니다.

- 다음 옵션에 액세스하려면 **더 많이 표시**를 클릭합니다.
  - **머신이 꺼진 경우에는 머신 시작 시에 누락된 작업을 실행**(기본적으로 비활성화됨)
  - **백업 도중 절전 또는 최대 절전 모드가 되는 것을 방지**(기본적으로 활성화됨)

    이 옵션은 Windows를 실행하는 머신에만 사용할 수 있습니다.
  - **절전 또는 최대 절전 모드에서 깨어나 예약된 백업 시작**(기본적으로 비활성화됨)

    이 옵션은 Windows를 실행하는 머신에만 사용할 수 있습니다. 이 옵션은 머신이 꺼져 있는 경우 사용할 수 없습니다. 즉, 이 옵션은 Wake-on-LAN 기능을 이용하지 않습니다.

이벤트별 스케줄

보호 계획의 스케줄을 설정할 경우 스케줄 선택기에서 이벤트 유형을 선택할 수 있습니다. 이벤트가 발생하면 즉시 백업이 시작됩니다.

다음 이벤트 중 하나를 선택할 수 있습니다.

- **마지막 백업 후 시간**

  동일한 보호 계획 내에서 마지막 백업이 성공적으로 완료된 후 경과된 시간입니다. 시간 길이를 지정할 수 있습니다.

  참고
  스케줄은 성공한 백업 이벤트를 기반으로 하기 때문에 백업이 실패하면 운영자가 계획을 수동으로 실행하고 실행이 성공적으로 완료될 때까지 스케줄러가 작업을 다시 실행하지 않습니다.

- **사용자가 시스템에 로그온할 때**

  기본적으로 사용자가 로그온하면 백업이 시작됩니다. 사용자를 특정 사용자 계정으로 변경할 수 있습니다.
- **사용자가 시스템에서 로그오프할 때**

기본적으로 사용자가 로그오프하면 백업이 시작됩니다. 사용자를 특정 사용자 계정으로 변경할 수 있습니다.

참고
종료는 로그오프와 같지 않으므로 시스템 종료 시에는 백업이 실행되지 않습니다.

- **시스템 시작 시**
- **시스템 종료 시**
- **Windows 이벤트 로그 이벤트 시**
  이벤트 속성을 지정해야 합니다.

아래 표는 Windows, Linux 및 macOS에서 다양한 데이터에 사용할 수 있는 이벤트를 나열합니다.

백업할 대상	마지막 백업 후 시간	사용자가 시스템에 로그온할 때	사용자가 시스템에서 로그오프할 때	시스템 시작 시	시스템 종료 시	Windows 이벤트 로그 이벤트 시
디스크/볼륨 또는 파일(실제 머신)	Windows, Linux, macOS	Windows	Windows	Windows, Linux, macOS	Windows	Windows
디스크/볼륨(가상 머신)	Windows, Linux	–	–	–	–	–
ESXi 구성	Windows, Linux	–	–	–	–	–
Microsoft 365 사서함	Windows	–	–	–	–	Windows
Exchange 데이터베이스 및 사서함	Windows	–	–	–	–	Windows
SQL 데이터베이스	Windows	–	–	–	–	Windows

Windows 이벤트 로그 이벤트 시

특정 Windows 이벤트가 **애플리케이션**, **보안** 또는 **시스템** 로그와 같은 이벤트 로그 중 하나에 기록될 때 백업이 시작되도록 스케줄할 수 있습니다.

예를 들어, Windows에서 하드 디스크 드라이브 고장을 발견하는 즉시 데이터의 응급 전체 백업이 자동으로 수행되도록 보호 계획을 설정할 수 있습니다.

이벤트를 찾아보고 이벤트 속성을 보려면 **컴퓨터 관리** 콘솔에 있는 **이벤트 뷰어** 스냅인을 사용합니다. **보안** 로그를 열려면 **Administrators** 그룹의 구성원이어야 합니다.

이벤트 속성

로그 이름

로그의 이름을 지정합니다. 목록에서 표준 로그(**응용 프로그램**, **보안** 또는 **시스템**)를 선택하거나 로그 이름(예: **Microsoft Office 세션**

이벤트 소스

이벤트 소스를 지정합니다. 이벤트 소스란 예를 들어 **디스크**와 같이 일반적으로 이벤트를 야기하는 프로그램 또는 시스템 컴퍼넌트를 뜻합니다.

특정 문자열이 포함된 모든 이벤트 원본이 예정된 백업을 트리거할 수 있습니다. 이 옵션은 대소문자 구분을 하지 않습니다. 즉 **service**라는 문자열을 지정하면 **Service Control Manager**와 **Time-Service** 이벤트 원본이 모두 백업을 트리거합니다.

이벤트 유형

이벤트 유형, 즉 **오류**, **경고**, **정보**, **감사 성공** 또는 **감사 실패**를 지정합니다.

이벤트 ID

이벤트 번호를 지정합니다. 이벤트 번호는 일반적으로 소스가 동일한 이벤트 중 특정 이벤트 유형을 나타냅니다.

예를 들어, 디스크에 아직 액세스할 준비가 되지 않았다면 이벤트 원본이 **디스크**이고 이벤트 ID가 **15**인 **오류** 이벤트가 발생하지만 Windows가 디스크에서 불량 블록을 발견하면 이벤트 소스가 **디스크**이고 이벤트 ID가 **7**인 **오류** 이벤트가 발생합니다.

예: "불량 블록" 응급 백업

하드 디스크에 갑자기 불량 블록이 하나 이상 나타났다면 이는 대체로 하드 드라이브가 곧 고장 날 것이라는 신호라고 할 수 있습니다. 그러한 상황이 발생할 경우 즉시 하드 디스크 데이터를 백업하는 보호 계획을 생성한다고 가정해 보겠습니다.

Windows가 하드 디스크에서 불량 블록을 발견하면 이벤트 소스가 **디스크**이고 이벤트 번호가 **7**인 이벤트를 **시스템** 로그에 기록합니다. 이 이벤트의 유형은 **오류**입니다.

계획을 생성할 경우 **스케줄** 섹션에서 다음 항목을 입력하거나 선택합니다.

- **로그 이름**: **시스템**
- **이벤트 소스**: **디스크**
- **이벤트 유형**: **오류**
- **이벤트 ID**: **7**

중요
불량 블록이 있는 경우에도 그러한 백업이 완료되도록 하려면 해당 백업이 불량 블록을 무시하도록 설정해야 합니다. 이 작업을 수행하려면 **백업 옵션**에서 **오류 처리**로 이동한 다음 **불량 섹터 무시** 확인란을 선택합니다.

시작 조건

이러한 설정은 스케줄러를 더 유연하게 하며 특정 조건과 관련하여 백업 작업을 실행하도록 합니다. 조건을 여러 개 지정한 경우에는 모든 조건이 동시에 충족되어야만 백업이 시작됩니다. 시작 조건은 백업 계획을 수동으로 시작할 때에는 적용되지 않습니다.

이러한 설정에 액세스하려면 보호 계획에 대한 스케줄을 설정할 때 **더 많이 표시**를 클릭합니다.

해당 조건(또는 여러 조건)이 충족되지 않는 경우에는 백업 시작 조건 백업 옵션에서 스케줄러 동작을 정의합니다. 조건이 너무 오랫동안 충족되지 않고 백업을 더 지연하면 위험하게 되는 상황을 처리하기 위해서는 조건과 관계없이 백업 실행 시간 간격을 설정할 수 있습니다.

아래 표는 Windows, Linux 및 macOS에서 다양한 데이터에 사용할 수 있는 시작 조건을 나열합니다.

백업할 대상	디스크/볼륨 또는 파일(실제 머신)	디스크/볼륨(가상 머신)	ESXi 구성	Microsoft 365 사서함	Exchange 데이터베이스 및 사서함	SQL 데이터베이스
사용자가 유휴 상태인 경우	Windows	-	-	-	-	-
백업 위치의 호스트를 사용할 수 있는 경우	Windows, Linux, macOS	Windows, Linux	Windows, Linux	Windows	Windows	Windows
사용자가 로그오프한 경	Windows	-	-	-	-	-

우						
시간 간격을 맞춘 경우	Windows, Linux, macOS	Windows, Linux	-	-	-	-
배터리 전원 절약	Windows	-	-	-	-	-
데이터 요금제 사용 시 시작하지 않음	Windows	-	-	-	-	-
다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음	Windows	-	-	-	-	-
장치 IP 주소 확인	Windows	-	-	-	-	-

사용자가 유휴 상태임

"사용자가 유휴 상태인 경우"라는 말은 머신에서 화면 보호기가 실행 중이거나 머신이 잠겨 있음을 의미합니다.

예

매일 21시에 머신에서 백업을 실행합니다. 이때 사용자가 유휴 상태인 것이 좋습니다.사용자가 23시에도 여전히 활성 상태인 경우 그대로 백업이 실행됩니다.

- 예약: 일일, 매일 실행. 시작 시간: **21시**.
- 조건: **사용자가 유휴 상태인 경우**.
- 백업 시작 조건: **조건이 충족될 때까지 대기 2시간 후 백업 시작**.

따라서

(1) 사용자가 21시 전에 유휴 상태가 된 경우 21시에 백업이 시작됩니다.

(2) 사용자가 21시에서 23시 사이에 유휴 상태가 된 경우 유휴 상태가 된 직후 백업이 시작됩니다.

(3) 사용자가 23시에도 여전히 활성 상태인 경우 백업이 23시에 시작됩니다.

백업 위치의 호스트를 사용할 수 있음

"백업 위치의 호스트를 사용할 수 있습니다"라는 말은 네트워크를 통해 백업을 저장할 목적지를 호스팅하는 머신을 사용할 수 있음을 의미합니다.

이 조건은 네트워크 폴더, 클라우드 스토리지 및 스토리지 노드에서 관리되는 위치에 적용됩니다.

이 조건은 위치 자체의 가용성을 포함하지 않고 호스트 가용성만 포함합니다. 예를 들어 호스트를 사용할 수 있지만 이 호스트의 네트워크 폴더가 공유되지 않거나 폴더의 자격 증명이 더 이상 유효하지 않을 경우 조건을 충족하는 것으로 간주합니다.

예

데이터가 평일 21시에 네트워크 폴더로 백업됩니다.해당 시점에 유지보수 작업 등으로 인해 폴더를 호스팅하는 머신을 사용할 수 없는 경우 백업을 건너뛰고 다음 평일까지 대기한 후 스케줄에 따라 시작합니다.

- 예약: 일일, 월요일~금요일 실행. 시작 시간: **21시**.
- 조건: **백업 위치의 호스트를 사용할 수 있는 경우**
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

(1) 21시가 되고 호스트를 사용할 수 있는 경우 백업이 즉시 시작됩니다.

(2) 21시가 되었지만 호스트를 사용할 수 없는 경우 백업이 호스트를 사용할 수 있는 다음 평일에 시작됩니다.

(3) 평일 21시에 호스트를 사용할 수 없는 경우 백업이 시작되지 않습니다.

사용자가 로그오프함

모든 사용자가 Windows에서 로그오프할 때까지 백업을 보류할 수 있습니다.

예

금요일마다 20시에 백업을 실행합니다. 이때 모든 사용자가 로그오프하는 것이 좋습니다.23시에 아직 로그온 상태인 사용자가 있을 경우 그대로 백업을 실행합니다.

- 예약: 매주, 금요일. 시작 시간: **20시**.
- 조건: **사용자가 로그오프한 경우**
- 백업 시작 조건: **조건이 충족될 때까지 대기 3시간 후 백업 시작**.

결과:

(1) 모든 사용자가 20시에 로그오프 상태인 경우 백업이 20시에 시작됩니다.

(2) 마지막 사용자가 20시에서 23시 사이에 로그오프할 경우 로그오프하는 즉시 백업이 시작됩니다.

(3) 23시에도 로그온 상태인 사용자가 있을 경우 23시에 백업이 시작됩니다.

시간 간격에 맞음

백업 시작 시간을 지정된 간격으로 제한합니다.

예

한 회사가 동일한 NAS(network-attached storage)에서 다른 위치를 사용하여 사용자 데이터와 서버를 백업하려고 합니다. 평일 업무 시간은 8시부터 17시까지입니다.사용자가 로그오프한 후 곧바로 사용자의 데이터를 백업해야 하지만 16시 30분 이후여야 합니다.매일 23시에 회사의 서버가 백업됩니다. 따라서 네트워크 대역폭의 공간을 늘리려면 이 시간 전에 모든 사용자 데이터를 백업하는 것이 좋습니다.사용자 데이터를 백업하는 데 1시간밖에 걸리지 않는다고 가정하므로 가장 늦은 백업 시작 시간은 22시입니다. 지정된 시간 간격 동안 사용자가 아직 로그온 상태이거나 다른 시간에 로그오프한 경우 백업 실행을 건너뛰는 등 해당 사용자의 데이터를 백업하지 마십시오.

- 이벤트: **사용자가 시스템에서 로그오프할 때**. 사용자 계정 지정: **모든 사용자**.
- 조건: **16시 30분**부터 **22시**까지 **시간 간격을 맞춥니다**.
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

(1) 사용자가 16시 30분과 22시 사이에 로그오프할 경우 로그오프 후 즉시 백업이 시작됩니다.

(2) 사용자가 그 밖의 시간에 로그오프할 경우 백업이 생략됩니다.

배터리 전원 절약

장치(랩톱 또는 태블릿)가 전원에 연결되어 있지 않은 경우 백업을 방지합니다. 백업 시작 조건 백업 옵션의 값에 따라 장치가 전원에 연결된 후에 건너뛴 백업이 시작되거나 시작되지 않습니다. 다음 옵션을 사용할 수 있습니다.

- **배터리 사용 시에는 시작하지 않음**
  장치가 전원에 연결되어 있는 경우에만 백업이 시작됩니다.

- **배터리 레벨이 다음 이상인 경우 배터리 사용 시 시작:**
  장치가 전원에 연결되어 있거나 배터리 수준이 지정된 값보다 높은 경우 백업이 시작됩니다.

예

데이터가 평일 21시마다 백업됩니다.장치가 전원에 연결되어 있지 않은 경우(예: 사용자가 늦은 시간에 열리는 미팅에 참가 중) 백업을 건너뛰어 배터리 전력을 아끼고 사용자가 장치를 전원에 연결할 때까지 기다릴 수 있습니다.

- 예약: 일일, 월요일~금요일 실행. 시작 시간: 21시.
- 조건: **배터리 전원 절약**, **배터리 사용 시에는 시작하지 않음**.
- 백업 시작 조건: **조건이 충족될 때까지 대기**.

결과:

(1) 21시가 되고 장치가 전원에 연결되어 있는 경우 백업이 즉시 시작됩니다.

(2) 21시가 되고 장치가 배터리 전력으로 실행 중인 경우 장치를 전원에 연결하는 대로 백업이 시작됩니다.

데이터 요금제 사용 시 시작하지 않음

장치가 Windows에서 데이터 요금제로 설정되어 있는 연결을 통해 인터넷에 연결되어 있는 경우 백업을 방지합니다(로컬 디스크로의 백업 포함). Windows에서의 데이터 요금제 연결에 대한 자세한 내용은 https://support.microsoft.com/en-us/help/17452/windows-metered-internet-connections-faq를 참조하십시오.

모바일 핫스팟에서의 백업을 방지하기 위한 추가 조치로 **데이터 요금제 사용 시 시작하지 않음** 조건을 활성화하면 **다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음** 조건이 자동으로 활성화됩니다. "android", "phone", "mobile" 및 "modem" 같은 네트워크 이름이 기본적으로 지정됩니다. 이 이름은 X 기호를 클릭해 목록에서 삭제할 수 있습니다.

예

데이터가 평일 21시마다 백업됩니다.장치가 데이터 요금제 연결을 통해 인터넷에 연결된 경우(예: 사용자가 출장 중) 백업을 건너뛰어 네트워크 트래픽을 아끼고 다음 평일에 예약된 백업이 시작될 때까지 기다릴 수 있습니다.

- 예약: 일일, 월요일~금요일 실행. 시작 시간: 21시.
- 조건: **데이터 요금제 사용 시 시작하지 않음**
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

(1) 21시가 되고 장치가 데이터 요금제 연결을 통해 인터넷에 연결되어 있지 않은 경우 백업이 즉시 시작됩니다.

(2) 21시가 되고 장치가 데이터 요금제 연결을 통해 인터넷에 연결되어 있는 경우 백업이 다음 평일에 시작됩니다.

(3) 장치가 평일 21시에 항상 데이터 요금제 연결을 통해 인터넷에 연결되어 있는 경우 백업이 절대 시작되지 않습니다.

다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음

장치가 지정된 무선 네트워크에 연결되어 있는 경우 백업을 방지합니다(로컬 디스크로의 백업 포함). SSID(서비스 세트 식별자)로도 알려진 Wi-Fi 네트워크 이름을 지정할 수 있습니다.

이 제한 사항은 대소문자 구별 없이 이름에 하위 문자열로 지정된 이름을 포함하고 있는 모든 네트워크에 적용됩니다. 예를 들어, 네트워크 이름으로 "phone"을 지정하는 경우 장치가 다음 네트워크 중 어느 것에든 연결되어 있는 경우 백업이 시작되지 않습니다. "John's iPhone", "phone_wifi" 또는 "my_PHONE_wifi".

이 조건은 장치가 휴대폰 핫스팟을 통해 인터넷에 연결되어 있을 때 백업을 방지하는 데 유용합니다.

모바일 핫스팟에서의 백업을 방지하기 위한 추가 조치로 **데이터 요금제 사용 시 시작하지 않음** 조건을 활성화하면 **다음과 같은 Wi-Fi 네트워크에 연결된 경우 시작하지 않음** 조건이 자동으로 활성화됩니다. "android", "phone", "mobile" 및 "modem" 같은 네트워크 이름이 기본적으로 지정됩니다. 이 이름은 X 기호를 클릭해 목록에서 삭제할 수 있습니다.

예

데이터가 평일 21시마다 백업됩니다.장치가 모바일 핫스팟을 통해 인터넷에 연결된 경우(예: 랩톱을 테더링 모드로 연결) 백업을 건너뛰고 다음 평일에 예약된 백업이 시작될 때까지 기다릴 수 있습니다.

- 예약: 일일, 월요일~금요일 실행. 시작 시간: 21시.
- 조건: **다음과 같은 네트워크에 연결된 경우 시작하지 않음**, **네트워크 이름**: <핫스팟 네트워크의 SSID>.
- 백업 시작 조건: **스케줄된 백업 건너뛰기**.

결과:

(1) 21시가 되고 머신이 지정된 네트워크에 연결되어 있지 않은 경우 백업이 즉시 시작됩니다.

(2) 21시가 되고 머신이 지정된 네트워크에 연결되어 있는 경우 백업이 다음 평일에 시작됩니다.

(3) 머신이 평일 21시에 항상 지정된 네트워크에 연결되어 있는 경우 백업이 절대 시작되지 않습니다.

장치 IP 주소 확인

장치 IP 주소가 지정된 IP 주소 범위에 들거나 벗어나는 경우 백업을 방지합니다(로컬 디스크로의 백업도 포함). 다음 옵션을 사용할 수 있습니다.

- **IP 범위 밖인 경우 시작**
- **IP 범위 내인 경우 시작**

어느 옵션에서든 여러 범위를 지정할 수 있습니다. IPv4 주소만 지원됩니다.

이 조건은 해외 사용자가 과도한 데이터 전송 비용을 피하는 데 유용합니다. 또한 VPN(가상 개인 네트워크) 연결을 통한 백업을 방지하는 데에도 유용합니다.

예

데이터가 평일 21시마다 백업됩니다.장치가 VPN 터널을 사용하여 기업 네트워크에 연결된 경우(예: 사용자가 집에서 근무) 백업을 건너뛰고 사용자가 장치를 사무실로 가져올 때까지 기다릴 수 있습니다.

- 예약: 일일, 월요일~금요일 실행. 시작 시간: 21시.
- 조건: **장치 IP 주소 확인**, **IP 주소 밖인 경우 시작**, **시작**: <VPN IP 주소 범위 시작, **끝**: <VPN IP 주소 범위 끝>.
- 백업 시작 조건: **조건이 충족될 때까지 대기**.

결과:

(1) 21시가 되고 머신 IP 주소가 지정된 범위에 없는 경우 백업이 즉시 시작됩니다.

(2) 21시가 되고 머신 IP 주소가 지정된 범위에 있는 경우 장치가 비-VPN IP 주소를 획득하는 대로 백업이 시작됩니다.

(3) 머신 IP 주소가 평일 21시에 항상 지정된 범위에 있는 경우 백업이 절대 시작되지 않습니다.

보관 규칙

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

1. **보관 기간**을 클릭합니다.
2. **정리**에서 다음 중 하나를 선택합니다.
   - **백업 기간별**(기본값)
     보호 계획에 따라 생성된 백업을 보관할 기간을 지정합니다. 기본적으로 보관 규칙은 각 백업 세트[1]에 대해 개별적으로 지정됩니다. 모든 백업에 대해 단일 규칙을 사용하려는 경우 **모든 백업 집합에 대해 단일 규칙으로 전환**을 클릭합니다.
   - **백업 수별**
     보관하려는 최대 백업 수를 지정합니다.
   - **백업의 총 크기 기준**
     보관할 백업의 최대 총 크기를 지정합니다.

[1]개별적인 보관 규칙이 적용되는 백업 그룹입니다. 사용자 정의 백업 구성표의 경우 백업 세트는 백업 방식에 해당합니다(전체, 차등, 증분). 이외의 경우 백업 세트는 월간, 일일, 주간, 매시간입니다. 월간 백업은 한 달이 시작된 후 생성된 첫 번째 백업입니다. 주간 백업은 주간 백업 옵션(기어 아이콘을 클릭한 다음 백업 옵션 > 주간 백업 클릭)에서 선택한 주중 특정일에 생성된 첫 번째 백업입니다. 한 달이 시작된 후 생성된 첫 번째 백업이 주간 백업인 경우 해당 백업은 월간인 것으로 간주됩니다. 이 경우 주간 백업은 다음 주 선택한 요일에 생성됩니다. 일일 백업은 해당 백업이 월간 또는 주간 백업의 정의에 포함되지 않는 한 하루가 시작된 후 생성된 첫 번째 백업입니다. 매시간 백업은 해당 백업이 월간, 주간 또는 일일 백업의 정의에 포함되지 않는 1시간이 시작된 후 생성된 첫 번째 백업입니다.

이 설정은 **항상 증분(단일 파일)** 백업 구성표와 함께 사용하거나 SFTP 서버 또는 테이프 장치에 백업할 경우 사용할 수 없습니다.

- **백업 무기한 보관**

3. 정리를 시작할 시간을 선택합니다.
   - **백업 후**(기본값)

     새 백업이 생성된 후 보관 규칙이 적용됩니다.
   - **백업 전**

     새 백업이 생성되기 전에 보관 규칙이 적용됩니다.

     이 설정은 Microsoft SQL Server 클러스터 또는 Microsoft Exchange Server 클러스터를 백업할 경우 사용할 수 없습니다.

알아야 할 기타 사항

- 새 백업 작업을 시작하기 전에 백업을 정리하는 보존 규칙을 구성하고 유지할 백업의 수를 0으로 설정하지 않으면, 보호 계획으로 생성된 마지막 백업은 항상 유지됩니다.

  경고!
  이런 방법으로 보존 규칙을 적용하여 보유하고 있는 유일한 백업을 삭제하고 백업이 실패하면 사용할 수 있는 백업이 없기 때문에 데이터 복원에 사용할 백업이 없게 됩니다.

- 테이프에 저장된 백업은 테이프를 덮어쓸 때까지 삭제되지 않습니다.
- 백업 구성표 및 백업 형식에 따라 각 백업이 개별 파일로 저장되는 경우 이 파일은 모든 종속(증분 또는 차등) 백업의 수명이 만료될 때까지 삭제할 수 없습니다. 따라서 삭제가 지연된 백업을 저장하기 위해서 추가 공간이 필요합니다. 또한 백업 기간, 백업 수 및 백업 크기가 지정한 값을 초과할 수 있습니다.

  "백업 통합" 백업 옵션을 사용하여 이 동작을 변경할 수 있습니다.
- 보관 규칙은 보호 계획의 일부입니다. 보호 계획이 머신에서 취소 또는 삭제되거나 머신 자체가 관리 서버에서 삭제되는 즉시 머신의 백업에서 이러한 규칙의 작동이 중단됩니다. 계획에서 생성한 백업이 더 이상 필요하지 않은 경우 "백업 삭제"에 설명된 대로 해당 백업을 삭제하십시오.

암호화

특히 회사의 규정 준수에 따라야 하는 경우 클라우드 스토리지에 저장된 모든 백업을 암호화하는 것이 좋습니다.

중요
비밀번호를 잃어버리거나 기억나지 않으면 암호화된 백업을 복구할 방법이 없습니다.

보호 계획 암호화

암호화를 활성화하려면 보호 계획을 생성할 때 암호화 설정을 지정합니다. 보호 계획이 적용된 후에는 암호화 설정을 수정할 수 없습니다. 다른 암호화 설정을 사용하려면 새 보호 계획을 생성해야 합니다.

보호 계획에 암호화 설정을 지정하려면

1. 보호 계획 패널에서 **암호화** 스위치를 활성화합니다.
2. 암호화 비밀번호를 지정한 후 확인합니다.
3. 다음 암호화 알고리즘 중 하나를 선택합니다.
   - **AES 128** – 백업이 128비트 키와 함께 AES(Advanced Encryption Standard) 알고리즘을 사용하여 암호화됩니다.
   - **AES 192** – 백업이 192비트 키와 함께 AES 알고리즘을 사용하여 암호화됩니다.
   - **AES 256** – 백업이 256비트 키와 함께 AES 알고리즘을 사용하여 암호화됩니다.
4. **확인**을 클릭합니다.

머신 속성인 암호화

이 옵션은 여러 머신의 백업을 처리하는 관리자를 위해 마련되었습니다. 각 머신에 대해 고유한 암호화 비밀번호가 필요한 경우 또는 보호 계획 암호화 설정에 상관없이 백업 암호화를 강제해야 하는 경우 각 머신에 대해 개별적으로 암호화 설정을 저장합니다. 백업이 256비트 키와 함께 AES 알고리즘을 사용하여 암호화됩니다.

머신에서 암호화 설정을 저장하면 보호 계획에 다음과 같은 영향을 미칠 수 있습니다.

- **보호 계획이 이미 머신에 적용되었습니다.** 보호 계획의 암호화 설정이 다른 경우 백업에 실패합니다.
- **보호 계획이 나중에 머신에 적용됩니다.** 머신에 저장된 암호화 설정이 보호 계획의 암호화 설정을 오버라이드합니다. 보호 계획 설정에서 암호화가 비활성화된 경우에도 모든 백업이 암호화됩니다.

이 옵션은 Agent for VMware를 실행 중인 머신에서는 사용할 수 있습니다. 그러나 동일한 vCenter Server에 연결된 Agent for VMware가 두 개 이상 있는 경우 주의하십시오. 모든 에이전트 간에는 일종의 부하 분산이 발생하므로 모든 에이전트에 대해 동일한 암호화 설정을 사용해야 합니다.

암호화 설정이 저장된 후 아래 설명된 대로 설정을 변경하거나 재설정할 수 있습니다.

중요
이 머신에서 실행되는 보호 계획이 이미 백업을 생성한 경우 암호화 설정을 변경하면 이 계획이 실패하게 됩니다. 백업을 계속하려면 새 계획을 생성하십시오.

머신에서 암호화 설정을 저장하려면

1. Windows에서는 관리자로, Linux에서는 루트 사용자로 로그온합니다.
2. 다음 스크립트를 실행합니다.
   - Windows: <설치_경로>**\PyShell\bin\acropsh.exe -m manage_creds --set-password** <암호화_비밀번호>

     여기서 <설치_경로>은(는) 보호 에이전트의 설치 경로입니다. 기본 위치는 클라우드 디플로이의 경우 **%ProgramFiles%\BackupClient**이고, 온-프레미스 디플로이의 경우 **%ProgramFiles%\Acronis** 입니다.
   - Linux: **/usr/sbin/acropsh -m manage_creds --set-password** <암호화_비밀번호>

머신에서 암호화 설정을 재설정하려면

1. Windows에서는 관리자로, Linux에서는 루트 사용자로 로그온합니다.
2. 다음 스크립트를 실행합니다.
   - Windows: <설치_경로>**\PyShell\bin\acropsh.exe -m manage_creds --reset**
     여기서 <설치_경로>은(는) 보호 에이전트의 설치 경로입니다. 기본 위치는 클라우드 디플로이의 경우 **%ProgramFiles%\BackupClient**이고, 온-프레미스 디플로이의 경우 **%ProgramFiles%\Acronis** 입니다.
   - Linux: **/usr/sbin/acropsh -m manage_creds --reset**

Cyber Protect Monitor를 사용하여 암호화 설정을 변경하는 방법

1. Windows 또는 macOS에서 관리자로 로그온합니다.
2. 알림 영역(Windows) 또는 메뉴 모음(macOS)에서 **Cyber Protect Monitor** 아이콘을 클릭합니다.
3. 기어 아이콘을 클릭합니다.
4. **암호화**를 클릭합니다.
5. 다음 중 하나를 수행하십시오.
   - **이 머신에 대한 특정 비밀번호 설정**을 선택합니다. 암호화 비밀번호를 지정한 후 확인합니다.
   - **보호 계획에 지정된 암호화 설정 사용**을 선택합니다.
6. **확인**을 클릭합니다.

암호화 작동 방식

AES 암호 알고리즘은 CBC(사이퍼 블록 체이닝) 모드에서 작동하며 128, 192 또는 256비트의 사용자 정의 크기로 임의 생성된 키를 사용합니다. 키 크기가 클수록 프로그램에서 백업을 암호화하는 시간이 길어지고 데이터 보안이 더욱 강화됩니다.

그런 다음 암호화 키는 비밀번호의 SHA-256 해시를 키로 사용하여 AES-256으로 암호화됩니다. 비밀번호 자체는 디스크 또는 백업의 어떤 위치에도 저장되지 않으며 비밀번호 해시가 확인을 위해 사용됩니다. 이 두 가지 수준의 보안을 사용하여 백업 데이터는 무단 액세스로부터 보호되지만 분실한 비밀번호는 복구할 수 없습니다.

공증

공증을 사용하면 파일이 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다. 법적 문서 파일이나 입증된 신뢰성이 필요한 기타 파일을 보호할 때에는 공증을 활성화하는 것이 좋습니다.

공증은 파일 수준 백업에만 사용할 수 있습니다. 디지털 서명이 있는 파일은 공증이 필요하지 않기 때문에 건너뜁니다.

다음과 같은 경우 공증을 사용할 수 *없습니다*.

- 백업 형식이 **버전 11**로 설정된 경우
- 백업 목적지가 Secure Zone인 경우
- 백업 목적지가 중복 제거 또는 암호화가 활성화된 관리 위치인 경우

공증 사용 방법

백업용으로 선택된 모든 파일(디지털 서명이 있는 파일 제외)의 공증을 활성화하려면 보호 계획을 생성할 때 **공증** 스위치를 활성화합니다.

복구를 구성할 때 공증된 파일에 특별한 아이콘이 표시되고, 이를 통해 파일 신뢰성을 확인할 수 있습니다.

작동법

백업 중에 에이전트가 백업된 파일의 해시 코드를 계산하고, 해시 트리(폴더 구조 기반)를 생성하고, 트리를 백업에 저장한 다음 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 Ethereum 블록체인 데이터베이스에 해시 트리 루트를 저장하여 이 값이 변경되지 않도록 합니다.

파일 신뢰성을 확인할 때 에이전트가 파일의 해시를 계산한 다음 이를 백업 내부의 해시 트리에 저장되어 있는 해시와 비교합니다. 두 해시가 일치하지 않으면 파일이 신뢰할 수 없는 것으로 간주됩니다. 그렇지 않으면 해시 트리에 의해 파일 신뢰성이 보증됩니다.

해시 트리 자체가 손상되지 않았는지 확인하기 위해 에이전트는 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 이를 블록체인 데이터베이스에 저장되어 있는 해시 트리 루트와 비교합니다. 해시가 일치하면 선택한 파일은 신뢰할 수 있는 것으로 보증됩니다. 그렇지 않으면 소프트웨어에 파일을 신뢰할 수 없다는 메시지가 표시됩니다.

가상 머신으로 전환

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

가상 머신으로 변환은 디스크 수준 백업에만 사용할 수 있습니다. 백업에 시스템 볼륨과 운영 체제를 시작하는 데 필요한 모든 정보가 포함되어 있는 경우 결과 가상 머신이 자체적으로 시작될 수 있습니다. 그렇지 않으면 가상 디스크를 다른 가상 머신에 추가해도 됩니다.

전환 방법

- **정기적인 변환**
  정기적인 변환을 구성하는 방법은 두 가지입니다.
  - **보호 계획의 일부로 변환 수행**
    변환이 각 백업 이후(주 위치에 대해 구성된 경우) 또는 각 복제 이후(두 번째 이후 위치에 대해 구성된 경우) 수행됩니다.
  - **개별 변환 계획 생성**
    이 방법을 사용하여 개별 변환 스케줄을 지정할 수 있습니다.
- **새 가상 머신으로 복구**
  이 방법을 사용하여 복구 디스크를 선택하고 각 가상 디스크의 설정을 조정할 수 있습니다. 변환을 한 번 또는 가끔(예: 실제-가상 마이그레이션) 수행하려면 이 방법을 사용하십시오.

변환에 대해서 알아야 할 사항

지원되는 가상 머신 유형

가상 머신으로의 백업 변환은 백업을 생성한 같은 에이전트나 다른 에이전트를 통해 수행할 수 있습니다.

VMware ESXi, Hyper-V 또는 Scale Computing HC3로의 변환을 수행하려면 ESXi, Hyper-V 또는 Scale Computing HC3 호스트와 이 호스트를 관리하는 보호 에이전트(Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing HC3)가 필요합니다.

VHDX 파일로의 변환은 파일이 가상 디스크로 Hyper-V 가상 머신에 연결된다고 가정합니다.

다음 표에는 에이전트가 생성할 수 있는 가상 머신 유형이 요약 설명되어 있습니다.

VM 유형	Agent for VMware	Agent for Hyper-V	Agent for Windows	Agent for Linux	Agent for Mac	Agent for Scale Computing HC3
VMware ESXi	+	–	–	–	–	–
Microsoft Hyper-V	–	+	–	–	–	–
VMware 워크스테이션	+	+	+	+	–	–
VHDX 파일	+	+	+	+	–	–
Scale Computing HC3	–	–	–	–	–	+

제한 사항

- Agent for Windows, Agent for VMware(Windows) 및 Agent for Hyper-V는 NFS에 저장되어 있는 백업을 변환할 수 없음
- NFS 또는 SFTP 서버에 저장된 백업은 별도의 변환 계획에서 변환할 수 없습니다.
- Secure Zone에 저장되어 있는 백업은 같은 머신을 실행 중인 에이전트로만 변환할 수 있습니다.
- 별도의 변환 계획에서만 백업을 Scale Computing HC3 가상 머으로 변환할 수 있습니다.
- Linux 논리 볼륨(LVM)을 포함하고 있는 백업은 Agent for VMware, Agent for Hyper-V 및 Agent for Scale Computing HC3에서 생성되었으며 같은 하이퍼바이저로 전송하는 경우에만 변환 가능합니다. 크로스 하이퍼바이저 변환이 지원되지 않습니다.
- Windows 머신의 백업을 VMware Workstation 또는 VHDX 파일로 변환할 때에는 나머지 가상 머신이 변환을 수행하는 머신으로부터 CPU 유형을 상속합니다. 결국, 해당하는 CPU 드라이버가

게스트 운영 체제에 설치됩니다. 다른 CPU 유형의 호스트에서 시작한 경우 게스트 시스템에 드라이버 오류가 표시됩니다. 이 드라이버를 수동으로 업데이트하십시오.

ESXi 및 Hyper-V로의 정기적인 변환과 백업에서 가상 머신 실행 비교

두 가지 방법 모두 원래 머신에 장애가 발생하는 경우 몇 초 내로 가상 머신을 시작할 수 있습니다.

정기적인 변환은 CPU 및 메모리 리소스를 소비합니다. 가상 머신의 파일은 데이터 저장소(스토리지)의 공간을 일정하게 점유합니다. 운영 호스트를 변환에 사용하는 경우에는 이 방법이 실용적이지 않을 수 있습니다. 하지만 가상 머신 성능은 호스트 리소스만큼으로 제한됩니다.

두 번째 경우에는 리소스가 가상 머신을 운영하는 동안에만 소비됩니다. 데이터 저장소(스토리지) 공간은 변경 사항을 가상 디스크에 보관하는 데에만 필요합니다. 하지만 호스트가 가상 디스크에 직접 액세스하지 않고 백업에서 데이터를 읽어오는 에이전트와 통신하기 때문에 가상 머신이 더 느리게 실행됩니다. 또한 가상 머신은 일시적입니다.

보호 계획에서 가상 머신으로 변환

보호 계획에 존재하는 모든 백업 또는 복제 위치에서 가상 머신으로 변환을 구성할 수 있습니다. 각 백업 또는 복제 후에 변환이 수행됩니다.

사전 요구 사항과 제한 사항에 대한 자세한 내용은 "통합에 대해서 알아야 할 사항"을 참조하십시오.

보호 계획에서 가상 머신으로 변환 설정 방법

1. 변환을 수행할 백업 위치를 결정합니다.
2. 보호 계획 패널에서 이 위치 아래의 **VM으로 변환**을 클릭합니다.
3. **변환** 스위치를 활성화합니다.
4. **변환 대상**에서 대상 가상 머신의 유형을 선택합니다. 다음 중 하나를 선택합니다.
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **VMware Workstation**
   - **VHDX 파일**
5. 다음 중 하나를 수행하십시오.
   - VMware ESXi 및 Hyper-V: **호스트**를 클릭하고, 대상 호스트를 선택하고 나서, 새 머신 이름 템플릿을 지정합니다.
   - 기타 가상 머신 유형: **경로**에서 가상 머신 파일 및 파일 이름 템플릿을 저장할 위치를 지정합니다.

   기본 이름은 **[머신 이름]_converted**입니다.
6. [선택 사항] **변환을 수행할 에이전트**를 클릭한 다음 에이전트를 선택합니다.
   해당 에이전트는 백업을 수행할 에이전트(기본값) 또는 다른 머신에 설치된 에이전트입니다. 후자의 경우 다른 머신이 백업에 액세스할 수 있도록 네트워크 폴더 같은 공유 위치에 백업을 저장해야 합니다.
7. [선택 사항] VMware ESXi 및 Hyper-V의 경우 다음 작업도 수행할 수 있습니다.

- ESXi의 경우 **데이터 저장소** 또는 Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
- 디스크 프로비저닝 모드를 변경합니다. 기본 설정은 **씬**(VMware ESXi) 및 **동적 확장**(Hyper-V)입니다.
- **VM 설정**을 클릭해 메모리 크기, 프로세서 수 및 가상 머신의 네트워크 연결을 변경합니다.

8. **완료**를 클릭합니다.

VM으로의 정기적 변환 작동법

정기적인 변환의 작동 방식은 가상 머신 생성 위치에 따라 다릅니다.

- **▸가상 머신을 파일 세트로 저장하도록 선택하는 경우:** 변환할 때마다 가상 머신이 처음부터 다시 생성됩니다.
- **가상 머신을 가상화 서버에 생성하도록 선택하는 경우:** 증분 또는 차등 백업을 변환하는 경우, 소프트웨어는 가상 머신을 다시 생성하지 않고 기존 가상 머신을 업데이트합니다. 일반적으로 이러한 변환이 속도가 더 빠릅니다. 또한 변환을 수행하는 호스트의 CPU 자원과 네트워크 트래픽을 절약할 수 있습니다. 가상 머신을 업데이트할 수 없으면 소프트웨어가 처음부터 다시 생성합니다.

다음은 두 가지 경우 모두에 대한 자세한 설명입니다.

가상 머신을 파일 세트로 저장하도록 선택하는 경우

처음 변환의 결과로 새로운 가상 머신이 생성됩니다. 모든 후속 변환의 결과로 이 머신은 처음부터 다시 생성됩니다. 우선 기존 머신의 이름을 임시로 바꿉니다. 그러면 이전의 기존 머신 이름을 갖는 새 가상 머신이 생성됩니다. 이 작업이 성공하면 기존 머신이 삭제됩니다. 이 작업이 실패하면 새 머신이 삭제되고 기존 머신 이름으로 이전 이름이 지정됩니다. 이러한 방식으로 항상 하나의 머신으로 변환 작업을 끝낼 수 있지만 기존 머신을 유지하기 위해 변환 도중 추가 저장 공간이 필요합니다.

가상 머신을 가상 서버에 생성하도록 선택하는 경우

최초 변환 시 새 가상 머신이 생성됩니다. 이후 변환은 다음과 같이 수행됩니다.

- 마지막 변환 이후 *전체 백업*이 존재하는 경우에는 가상 머신이 처음부터 다시 생성됩니다(이 섹션의 앞부분 참조).
- 그렇지 않은 경우에는 기존 가상 머신이 마지막 변환 이후 변경 내용을 반영하여 업데이트됩니다. 업데이트가 불가능한 경우에는(예를 들어, 아래와 같이 중간 스냅샷을 삭제한 경우) 가상 머신이 처음부터 다시 생성됩니다.

중간 스냅샷

가상 머신을 업데이트해야 하는 경우 소프트웨어는 **백업...**, **복제본...**과 같은 가상 머신의 여러 중간 스냅샷을 저장합니다. 불필요한 스냅샷은 자동으로 삭제됩니다.

최신 **복제본...** 스냅샷은 최신 변환의 결과를 나타냅니다. 이 스냅샷으로 이동하면 머신을 해당 상태로 되돌릴 수 있습니다(예를 들어, 머신 작업을 수행한 후 머신 변경 사항을 취소하려는 경우).

다른 스냅샷은 소프트웨어가 내부적으로 사용합니다.

복제

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

이 섹션에서는 보호 계획의 일부인 백업 복제를 설명합니다. 개별 복제 계획 생성에 대한 자세한 내용은 "오프호스트 데이터 처리"를 참조하십시오.

백업 복제를 사용하도록 설정한 경우 백업 생성 후 즉시 각 백업이 또 다른 위치로 복사됩니다. 이전 백업이 복제되지 않은 경우(예: 네트워크 연결이 끊긴 경우) 성공적인 마지막 복제 후 나타나는 모든 백업이 자동으로 복제됩니다.

복제된 백업은 원래 위치에 남아 있는 백업과 상관이 없으며 그 반대의 경우에도 마찬가지입니다. 다른 위치에 액세스하지 않고 백업에서 데이터를 복구할 수 있습니다.

사용 예제

- **신뢰할 수 있는 재해 복구**
  온사이트(즉시 복구를 위해) 및 오프사이트(로컬 스토리지 오류 또는 자연 재해로부터 백업을 보호하기 위해) 둘 다에 백업을 저장합니다.
- **클라우드 스토리지를 사용하여 자연재해로부터 데이터 보호**
  데이터 변경 사항만 전송하여 클라우드 스토리지로 백업을 복제합니다.
- **최신 복구 지점만 유지**
  값비싼 스토리지 공간을 과도하게 사용하지 않기 위해 보관 규칙에 따라 빠른 스토리지에서 오래된 백업을 삭제합니다.

지원되는 위치

다음 위치*에서* 백업을 복제할 수 있습니다.

- 로컬 폴더
- 네트워크 폴더
- Secure Zone
- SFTP 서버
- 스토리지 노드에서 관리되는 위치

다음 위치*로* 백업을 복제할 수 있습니다.

- 로컬 폴더
- 네트워크 폴더
- 클라우드 스토리지
- SFTP 서버
- 스토리지 노드에서 관리되는 위치
- 테이프 장치

백업 복제를 활성화하려면

1. 보호 계획 패널에서 **위치 추가**를 클릭합니다.
   마지막으로 선택한 백업 혹은 복제 위치*에서* 복제가 지원되는 경우에만 **위치 추가** 제어가 표시됩니다.
2. 백업을 복제할 위치를 지정합니다.
3. [선택 사항] **보관 기간**에서는 "보관 규칙"의 설명에 따라 선택한 위치의 보관 규칙을 변경합니다.
4. [선택 사항] **VM으로 변환**에서 "가상 머신으로 변환"의 설명대로 가상 머신으로 변환에 대한 설정을 지정합니다.
5. [선택 사항] 기어 아이콘 > **성능 및 백업 할당 시간**을 클릭한 다음, "성능 및 백업 할당 시간"에 설명된 대로 선택한 위치의 백업 시간을 설정합니다. 이 설정은 복제 성능을 정의합니다.
6. [선택 사항] 백업을 복제할 모든 위치에 대해 1~5단계를 반복합니다. 기본 위치를 포함하여 최대 5개의 연속 위치가 지원됩니다.

중요
동일한 보호 계획에서 백업 및 복제를 활성화하는 경우 예약된 다음 백업 전에 복제가 완료되어야 합니다. 복제가 여전히 진행 중인 경우 예약된 백업이 시작되지 않습니다. 예를 들어, 복제를 완료하는 데 26시간이 걸리면 24시간마다 한 번씩 실행되는 예약된 백업이 시작되지 않습니다.

이러한 종속성을 방지하려면 별도의 백업 복제 계획을 사용해야 합니다. 이 특정 계획에 대한 자세한 내용은 "백업 복제"(320페이지)을(를) 참조하십시오.

고급 라이센스를 사용하는 사용자에 대한 고려 사항

팁

개별 복제 계획을 생성하여 클라우드 스토리지*에서* 백업 복제를 설정할 수 있습니다. 자세한 내용은 "오프호스트 데이터 처리"를 참조하십시오.

제한 사항

- 스토리지 노드가 관리하는 관리되는 위치*에서* 로컬 폴더로의 백업 복제는 지원되지 않습니다. 로컬 폴더는 머신에서 백업을 생성한 에이전트가 있는 폴더를 의미합니다.
- **버전 12** 백업 형식인 백업의 경우 중복 제거가 활성화된 관리 위치로의 백업 복제는 지원되지 않습니다.

작업은 어떤 머신이 수행합니까?

임의 위치*에서* 백업 복제는 백업을 생성한 에이전트가 시작하고 다음과 같이 수행됩니다.

- 해당 에이전트를 통해 위치가 스토리지 노드에서 관리되지 *않는* 경우.
- 해당 스토리지 노드를 통해 위치가 관리되지 않는 경우. 그러나 관리 위치에서 클라우드 스토리지로의 백업 복제는 백업을 생성한 에이전트가 수행합니다.

위의 설명처럼 작업은 에이전트가 있는 머신에 전원이 켜져 있는 경우에만 수행됩니다.

관리 위치 간 백업 복제

하나의 관리 위치에서 다른 관리 위치로의 백업 복제는 스토리지 노드에서 수행됩니다.

대상 위치(다른 스토리지 노드에 위치 가능)에 대한 중복 제거가 활성화된 경우 소스 스토리지 노드가 대상 위치에 없는 데이터 블록만 보냅니다. 즉, 에이전트와 마찬가지로 스토리지 노드는 소스의 중복 제거를 수행합니다. 이렇게 하면 지리적으로 떨어져 있는 스토리지 노드 사이에 데이터를 복제할 때 네트워크 트래픽을 줄일 수 있습니다.

수동으로 백업 시작

1. 보호 계획이 하나 이상 적용된 머신을 선택합니다.
2. **백업**을 클릭합니다.
3. 보호 계획이 두 개 이상 적용된 경우 원하는 보호 계획을 선택합니다.
4. 다음 중 하나를 수행하십시오.
   - **지금 실행**을 클릭합니다. 증분 백업이 생성됩니다.
   - 백업 구성표에 여러 백업 방법이 포함된 경우, 사용할 방법을 선택할 수 있습니다. **지금 실행** 버튼의 화살표를 클릭한 다음, **전체, 증분** 또는 **차등**을 선택합니다.

보호 계획에서 생성된 첫 번째 백업은 항상 전체 백업입니다.

백업 진행률이 머신의 **상태** 열에 표시됩니다.

백업 옵션

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

백업 옵션을 수정하려면 보호 계획 이름 옆에 있는 기어 아이콘을 클릭한 다음 **백업 옵션**을 클릭합니다.

백업 옵션의 사용 가능성

사용 가능한 백업 옵션은 다음에 따라 다릅니다.

- 에이전트를 운영하는 환경(Windows, Linux, macOS).
- 백업하는 데이터 유형(디스크, 파일, 가상 머신, 애플리케이션 데이터).
- 백업 목적지(클라우드 스토리지, 로컬 또는 네트워크 폴더).

다음 표는 백업 옵션의 사용 가능성을 요약해서 보여줍니다.

	디스크 수준 백업	파일 수준 백업	가상 머신	SQL 및 Exchange

	Windows	Linux	macOS	Windows	Linux	macOS	ESXi	Hyper-V	Scale Computing	Windows
경보	+	+	+	+	+	+	+	+	+	+
백업 통합	+	+	+	+	+	+	+	+	+	-
백업 파일 이름	+	+	+	+	+	+	+	+	+	+
백업 형식	+	+	+	+	+	+	+	+	+	+
백업 유효성 검사	+	+	+	+	+	+	+	+	+	+
CBT (Changed Block Tracking)	+	-	-	-	-	-	+	+	+	+
클러스터 백업 모드	-	-	-	-	-	-	-	-	-	+
압축 수준	+	+	+	+	+	+	+	+	+	+
이메일 알림	+	+	+	+	+	+	+	+	+	+
오류 처리										
오류 발생 시 재시도	+	+	+	+	+	+	+	+	+	+
처리	+	+	+	+	+	+	+	+	+	+

할 동안 메시지 및 대화 상자 표시 안 함(자동 모드)										
불량 섹터 무시	+	-	+	+	-	+	+	+	+	-
VM 스냅샷 생성 도중 오류가 발생하는 경우 재시도	-	-	-	-	-	-	+	+	+	-
빠른 증분/차등 백업	+	+	+	-	-	-	-	-	-	-
파일 필터	+	+	+	+	+	+	+	+	+	-
파일 수준 백업 스냅샷	-	-	-	+	+	+	-	-	-	-
로그 자르기	-	-	-	-	-	-	+	+	-	SQL만 해당
LVM 스냅샷 촬영	-	+	-	-	-	-	-	-	-	-

마운트 포인트	-	-	-	+	-	-	-	-	-	-
다중 볼륨 스냅샷	+	+	-	+	+	-	-	-	-	-
성능 및 백업 할당 시간	+	+	+	+	+	+	+	+	+	+
실제 데이터 전달	+	+	+	+	+	+	+	+	+	-
사전/사후 명령어	+	+	+	+	+	+	+	+	+	+
데이터 캡처 전/후 명령	+	+	+	+	+	+	+	-	-	+
SAN 하드웨어 스냅샷	-	-	-	-	-	-	+	-	-	-
일정 예약										
기간 내에서 시작 시간 분배	+	+	+	+	+	+	+	+	+	+
동시에 실	-	-	-	-	-	-	+	+	+	-

행되는 백업 수 제한										
섹터 단위 백업	+	+	-	-	-	-	+	+	+	-
분할	+	+	+	+	+	+	+	+	+	+
테이프 관리	+	+	+	+	+	+	+	+	+	+
작업 실패 처리	+	+	+	+	+	+	+	+	+	+
작업 시작 조건	+	+	-	+	+	-	+	+	+	+
VSS (Volume Shadow Copy Service)	+	-	-	+	-	-	-	+	-	+
가상 머신용 VSS (Volume Shadow Copy Service)	-	-	-	-	-	-	+	+	+	-
주간 백업	+	+	+	+	+	+	+	+	+	+
Windows	+	-	-	+	-	-	+	+	+	+

이벤트 로그										

경보

지정된 기간(일) 동안 성공적인 백업이 진행되지 않음

사전 설정값이 **비활성화됨**.

이 옵션은 지정된 기간 동안 보호 계획에서 수행한 성공적인 백업이 없는 경우에 대한 경보 생성 여부를 결정합니다. 소프트웨어는 실패한 백업 외에도 스케줄에 따라 실행되지 않은 백업(누락된 백업)의 수도 계산합니다.

경보는 머신당 기준으로 생성되고 **경보** 탭에 표시됩니다.

경보가 생성된 후 백업 없이 연속으로 보낼 수 있는 일 수를 지정할 수 있습니다.

백업 통합

이 옵션은 정리 중에 백업을 통합하거나 전체 백업 체인을 삭제할지 여부를 정의합니다.

사전 설정값이 **비활성화됨**입니다.

통합은 둘 이상의 후속 백업을 단일 백업으로 결합하는 프로세스입니다.

이 옵션이 활성화되어 있으면 정리 중 삭제되어야 하는 백업이 다음 종속 백업(증분 또는 차등)과 통합됩니다.

그렇지 않으면 종속된 모든 백업이 삭제될 때까지 해당 백업이 보관됩니다. 이렇게 하면 시간 소모적인 통합을 피하는 데 도움은 되지만 삭제가 연기되는 백업을 저장해둘 추가 공간이 필요합니다. 백업의 수명 또는 개수가 보관 규칙에 지정되어 있는 값을 초과할 수 있습니다.

중요
통합은 단지 삭제 방법일 뿐 삭제의 대안이 아님을 유의하십시오. 이렇게 생성된 백업에는 삭제된 백업에 있었고, 보관된 증분 또는 차등 백업에 없었던 데이터는 포함되지 않습니다.

다음에 해당하는 경우 이 옵션이 적용되지 *않습니다*.

- 백업 목적지가 테이프 장치 또는 클라우드 스토리지입니다.
- 백업 구성표가 **항상 증분(단일 파일)**으로 설정되어 있습니다.
- 백업 형식이 **버전 12**로 설정되어 있습니다.

테이프에 저장된 백업은 통합할 수 없습니다. 클라우드 스토리지에 저장된 백업과 단일 파일 백업(버전 11 및 12 형식 모두)의 경우 빠르고 간편한 통합을 위해 내부 구조가 생성되므로 항상 통합됩니다.

그러나 버전 12 형식을 사용하고 여러 백업 체인이 있는 경우(모든 체인이 별도의 .tibx 파일에 저장됨) 통합은 마지막 체인 내에서만 작동합니다. 메타 정보(~12KB)를 유지하기 위해 최소 크기로

줄어든 첫 번째 체인을 제외하고 다른 모든 체인은 전체적으로 삭제됩니다 동시 읽기 및 쓰기 작업 중 데이터 일관성을 보장하는 데 이 메타 정보가 필요합니다. 이러한 체인에 포함된 백업은 보관 규칙이 적용되는 즉시 GUI에서 사라지지만 전체 체인이 삭제될 때까지 실제로 존재합니다.

그 밖의 모든 경우에는 삭제가 연기된 백업에 GUI의 휴지통 아이콘()이 표시됩니다. X 기호를 눌러 백업을 삭제하면 통합이 수행됩니다. 테이프에 저장된 백업은 테이프를 덮어쓰거나 지울 때만 GUI에서 사라집니다.

백업 파일 이름

이 옵션은 보호 계획에서 생성된 백업 파일의 이름을 정의합니다.

이러한 이름은 백업 위치를 찾아볼 때 파일 관리자에 표시될 수 있습니다.

백업 파일이란 무엇입니까?

각 보호 계획은 사용되는 백업 구성표 및 백업 형식에 따라 백업 위치에서 하나 이상의 파일을 생성합니다. 다음 표에는 머신 또는 사서함별로 생성될 수 있는 파일이 나와 있습니다.

	항상 증분(단일 파일)	**기타 백업 구성표**
버전 11 백업 형식	TIB 파일 1개 및 XML 메타데이터 파일 1개	TIB 파일 여러 개 및 XML 메타데이터 파일 1개(기존 형식)
버전 12 백업 형식	백업 체인당 TIBX 파일 1개(전체 또는 차등 백업 및 이에 의존하는 모든 증분 백업)	

모든 파일의 이름이 동일하고 타임 스탬프 또는 일련 번호가 추가되거나 추가되지 않습니다. 보호 계획을 생성하거나 편집할 때 이 이름(백업 파일 이름이라고 함)을 정의할 수 있습니다.

참고
타임 스탬프는 버전 11 백업 형식의 백업 파일 이름에만 추가됩니다.

백업 파일 이름을 변경한 후 다음 백업은 전체 백업이 됩니다. 단, 같은 머신에 대한 기존 백업의 파일 이름을 지정하지 않은 경우는 예외입니다. 후자에 해당하는 경우 보호 계획 스케줄에 따라 전체, 증분 또는 차등 백업이 생성됩니다.

클라우드 스토리지 또는 테이프 장치와 같이 파일 관리자를 통해 이동할 수 없는 위치에 대한 백업 파일 이름을 설정할 수 있습니다. **백업 스토리지** 탭에서 사용자 정의 이름을 보려는 경우 이 방법이 유용합니다.

백업 파일 이름은 어디에서 볼 수 있습니까?

백업 스토리지 탭을 선택하고 백업 그룹을 선택합니다.

- 기본 백업 파일 이름이 **상세정보** 패널에 표시됩니다.
- 기본값이 아닌 백업 파일 이름을 설정하면 해당 이름이 바로 **백업 스토리지** 탭, **이름** 열에 표시됩니다.

백업 파일 이름에 대한 제한 사항

- 백업 파일 이름은 숫자로 끝날 수 없습니다.
  기본 백업 파일 이름에는 이름이 숫자로 끝나지 않도록 문자 "A"가 추가됩니다. 사용자 정의 이름을 생성할 경우 항상 숫자로 끝나지 않는지 확인하십시오. 변수를 사용할 경우 변수는 숫자로 끝날 수 있으므로 이름은 변수로 끝나지 않아야 합니다.
- 백업 파일 이름에는 다음 기호가 포함될 수 없습니다. **()&?*$<>":\|/#**, 줄 끝(**\n**) 및 탭(**\t**).

기본 백업 파일 이름

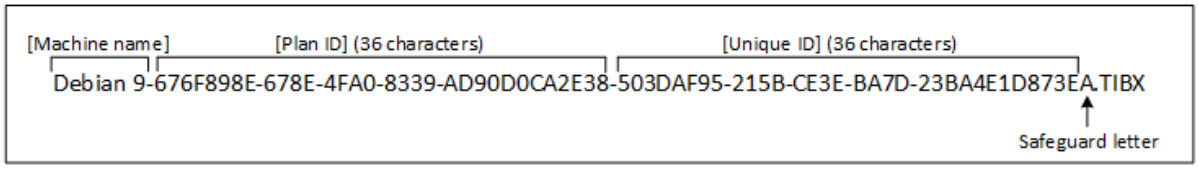
기본 백업 파일 이름은 [머신 이름]-[계획 ID]-[고유 ID]A입니다.

사서함 백업의 기본 백업 파일 이름은 [사서함 ID]_mailbox_[계획 ID]A입니다.

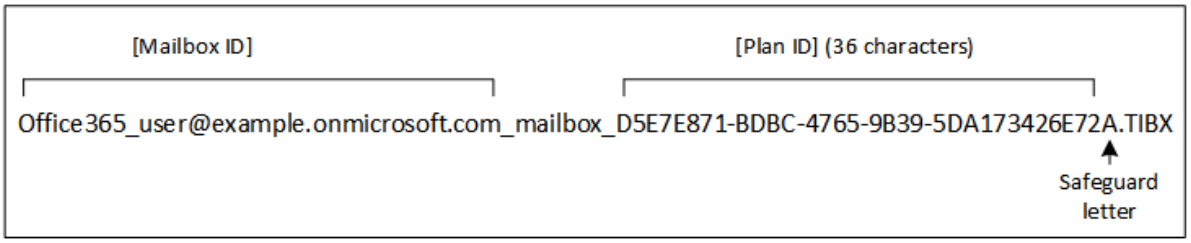
이름은 다음 변수로 구성됩니다.

- [머신 이름]이 변수는 Microsoft 365 사서함을 제외한 모든 백업된 데이터 유형에 대한 머신 이름으로 바뀝니다(Cyber Protect 웹 콘솔에 표시된 동일한 이름). Microsoft 365 사서함의 경우 사서함 사용자의 계정 이름(UPN)으로 바뀝니다.
- [계획 ID]이 변수는 보호 계획의 고유 식별자로 바뀝니다. 계획 이름이 바뀔 경우 이 값은 변경되지 않습니다.
- [고유 ID]이 변수는 선택한 머신 또는 사서함의 고유 식별자로 바뀝니다. 머신 이름이 바뀌거나 사서함 UPN이 변경될 경우 이 값은 변경되지 않습니다.
- [사서함 ID]이 변수는 사서함 UPN으로 바뀝니다.
- "A"는 이름이 숫자로 끝나지 않도록 추가되는 보호 문자입니다.

아래 다이어그램에는 기본 백업 파일 이름이 표시됩니다.



아래 다이어그램에는 사서함의 기본 백업 파일 이름이 표시됩니다.



변수 없는 이름

백업 파일 이름을 MyBackup으로 변경하면 백업 파일이 다음 예제와 같이 표시됩니다. 두 예제에서는 모두 일일 증분 백업이 2016년 9월 13일부터 14시 40분에 스케줄되었다고 가정합니다.

항상 증분(단일 파일) 백업 구성표를 사용한 버전 12 형식의 경우:

```
MyBackup.tibx
```

기타 백업 구성표를 사용한 버전 12 형식의 경우:

```
MyBackup.tibx
MyBackup-0001.tibx
MyBackup-0002.tibx
...
```

항상 증분(단일 파일) 백업 구성표를 사용한 버전 11 형식의 경우:

```
MyBackup.xml
MyBackup.tib
```

기타 백업 구성표를 사용한 버전 11 형식의 경우:

```
MyBackup.xml
MyBackup_2016_9_13_14_49_20_403F.tib
MyBackup_2016_9_14_14_43_00_221F.tib
MyBackup_2016_9_15_14_45_56_300F.tib
...
```

변수 사용

기본적으로 사용되는 변수 이외에 보호 계획 이름으로 바뀌는 [계획 이름]변수를 사용할 수 있습니다.

백업할 머신 또는 사서함을 여러 개 선택할 경우 백업 파일 이름에는 [머신 이름], [사서함 ID] 또는 [고유 ID]변수가 포함되어야 합니다.

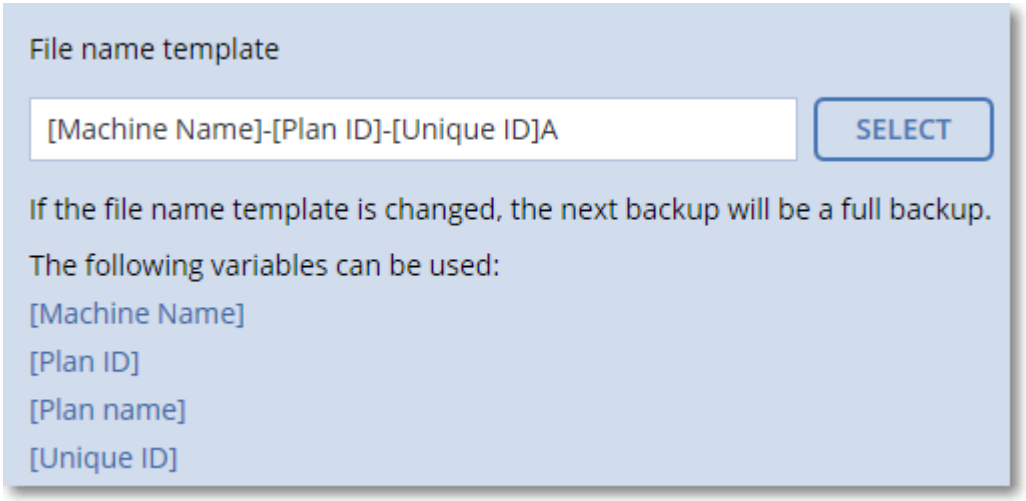
백업 파일 이름 및 간소화된 파일 이름 지정

일반 텍스트 및/또는 변수를 사용하여 이전 Acronis Cyber Protect 버전과 같은 파일 이름을 생성할 수 있습니다. 그러나 간소화된 파일 이름은 재생성할 수 없습니다. 버전 12에서는 단일 파일 형식이 사용되지 않은 경우 파일 이름에 타임 스탬프가 포함됩니다.

사용 예제

- **사용자에게 친숙한 파일 이름 보기**
  파일 관리자를 통해 백업 위치를 찾아볼 때 백업을 쉽게 구별하고 싶습니다.
- **백업의 기존 시퀀스 계속 진행**
  보호 계획이 단일 머신에 적용되고 이 머신을 Cyber Protect 웹 콘솔에서 제거하거나 에이전트를 구성 설정과 함께 설치 제거해야 한다고 가정해보겠습니다. 머신이 다시 추가되거나 에이전트가 다시 설치된 후 보호 계획을 적용하여 같은 백업 또는 백업 시퀀스로의 백업을 계속 진행할 수 있습니다. 이렇게 하려면 보호 계획의 백업 옵션에서 **백업 파일 이름**을 클릭한 다음 **선택**을 클릭하여 원하는 백업을 선택합니다.

찾아보기 버튼을 누르면 보호 계획 패널의 **백업할 위치** 섹션에서 선택된 위치에 백업이 표시됩니다. 이 위치 외부에 있는 항목은 찾아볼 수 없습니다.



- **이전 제품 버전에서 업그레이드**
  업그레이드하는 동안 보호 계획이 자동으로 마이그레이션되지 않은 경우에는 계획을 다시 생성하고 이전 백업 파일을 대상으로 지정합니다. 백업할 머신을 하나만 선택할 경우 **찾아보기**를 클릭하고 필요한 백업을 선택합니다. 백업할 머신을 여러 개 선택할 경우 변수를 사용하여 이전 백업 파일 이름을 다시 생성합니다.

참고
선택 버튼은 생성되어 단일 장치에 적용된 보호 계획에 대해서만 사용할 수 있습니다.

백업 형식

이 옵션은 보호 계획에 따라 생성된 백업의 형식을 정의합니다. 레거시 백업 형식 버전 11을 사용하는 보호 계획에서만 사용할 수 있습니다. 이 경우 새 형식 버전 12로 변경할 수 있습니다. 변경한 이후에는 이 옵션에 엑세스할 수 없게 됩니다.

이 옵션은 사서함 백업에는 효과가 *없습니다*. 사서함 백업에는 항상 새 형식이 지정됩니다.

사전 설정값이 **자동 선택**입니다.

다음 중 하나를 선택합니다.

- **자동 선택**
  보호 계획이 이전 제품 버전에서 생성한 버전에 백업을 추가하지 않는 한 버전 12가 사용됩니다.
- **버전 12**
  빠른 백업과 복구를 위해 대부분의 경우 새 형식이 권장됩니다. 각 백업 체인(전체 또는 차등 백업, 이에 의존하는 증분 백업)은 단일 TIBX 파일에 저장됩니다.
  이 형식을 사용하는 보관 규칙**백업의 총 크기 기준**은 사용할 수 없습니다.
- **버전 11**
  하위 호환성을 위해 보존된 레거시 형식입니다. 이전 제품 버전에서 생성한 버전에 백업을 추가할 수 있게 해줍니다.

또한, 개별 파일에 대한 전체, 증분 및 차등 백업을 원하는 경우 (**항상 증분(단일 파일)**을 제외한 모든 백업 구성표와 함께) 이 형식을 사용합니다.

백업 목적지(또는 복제 목적지)가 중복 제거가 활성화된 관리 위치이거나 암호화가 활성화된 관리 위치인 경우 이 형식이 자동으로 선택됩니다. 형식을 **버전 12**로 변경하면 백업이 실패합니다.

참고

백업 형식 버전 11을 사용하면 데이터베이스 가용성 그룹(DAG)을 백업할 수 없습니다. DAG의 백업은 버전 12 형식에서만 지원됩니다.

백업 형식 및 백업 파일

파일 관리자를 통해 찾아볼 수 있는 백업 위치(예: 로컬 또는 네트워크 폴더)의 경우 백업 형식에 따라 파일 개수와 파일 확장명이 결정됩니다. 백업 파일 이름 옵션을 사용하여 파일 이름을 정의할 수 있습니다. 다음 표에는 머신 또는 사서함별로 생성될 수 있는 파일이 나와 있습니다.

	항상 증분(단일 파일)	**기타 백업 구성표**
버전 11 백업 형식	TIB 파일 1개 및 XML 메타데이터 파일 1개	TIB 파일 여러 개 및 XML 메타데이터 파일 1개(기존 형식)
버전 12 백업 형식	백업 체인당 TIBX 파일 1개(전체 또는 차등 백업 및 이에 의존하는 모든 증분 백업)	

백업 형식을 버전 12(TIBX)로 변경

백업 형식을 버전 11(TIB 형식)에서 버전 12(TIBX 형식)로 변경 시:

- 다음 백업이 전체 백업으로 진행됩니다.
- 파일 관리자를 통해 찾아볼 수 있는 백업 위치(예: 로컬 또는 네트워크 폴더)에 새로운 TIBX 파일이 생성됩니다. 새로운 파일은 원래 파일과 이름이 동일하지만, 접미사 **_v12A**가 추가됩니다.
- 보관 규칙 및 복제는 새로운 백업에만 적용됩니다.
- 이전 백업은 삭제되지 않으며, **백업 스토리지** 탭에서 사용할 수 있습니다. 이전 백업은 수동으로 삭제할 수 있습니다.
- 이전 클라우드 백업은 **클라우드 스토리지** 할당량을 소비하지 않습니다.
- 이전 클라우드 백업은 수동으로 삭제할 때까지 **로컬 백업** 할당량을 소비합니다.
- 백업 목적지(또는 복제 목적지)가 중복 제거가 활성화된 관리 위치인 경우, 백업할 수 없습니다.

아카이브 내 중복 제거

버전 12 형식은 아카이브 내 중복 제거를 지원합니다.

클라이언트측 중복 제거를 사용하는 아카이브 내 중복 제거의 이점은 다음과 같습니다.

- 모든 데이터 유형에 대해 내장된 블록 수준 중복 제거를 통해 백업 크기 대폭 감소
- 하드 링크의 효율적 처리로 스토리지 중복이 없도록 보장
- 해시 기반 청크

참고
아카이브 내 중복 제거는 TIBX 형식의 모든 백업에 대해 기본적으로 활성화되어 있습니다. 백업 옵션에서 따로 활성화할 필요가 없으며, 비활성화할 수 없습니다.

백업 유효성 검사

유효성 검사는 백업에서 데이터를 복구할 수 있는지 그 가능성을 확인하는 작업입니다. 이 옵션을 활성화하면 보호 계획에 따라 생성되는 각 백업의 유효성을 생성 후 즉시 검사합니다. 이 작업은 보호 에이전트를 통해 수행됩니다.

사전 설정값이 **비활성화됨**.

유효성 검사는 백업에서 복구할 수 있는 모든 데이터 블록의 체크섬을 계산합니다. 유일한 예외는 클라우드 스토리지에 위치한 파일 수준 백업의 유효성 검사입니다. 이 백업은 백업에 저장되어 있는 메타데이터의 일관성 확인을 통해 유효성을 검사합니다.

유효성 검사는 크기가 작은 증분 또는 차등 백업의 경우에도 시간이 걸리는 프로세스입니다. 이 작업은 백업에 실제로 포함된 데이터뿐 아니라 백업을 선택하여 복구 가능한 모든 데이터의 유효성을 검사하기 때문입니다. 따라서 이전에 생성한 백업에 대한 액세스 권한이 필요합니다.

성공적인 유효성 검사는 높은 확률의 성공적인 복구를 의미하지만 복구 프로세스에 영향을 미치는 모든 요인을 검사하는 것은 아닙니다. 운영 체제를 백업하는 경우에는 부트 가능한 미디어에서 예비 하드 드라이브로 테스트 복구를 수행하거나 ESXi 또는 Hyper-V 환경에서 백업을 통해 가상 머신을 실행해 보는 것이 좋습니다.

CBT(Changed Block Tracking)

이 옵션은 Windows를 실행하는 가상 머신 및 실제 머신의 디스크 수준 백업에 유효합니다. 이는 Microsoft SQL Server 데이터베이스 및 Microsoft Exchange Server 데이터베이스의 백업에도 적용됩니다.

사전 설정값이 **활성화되었습니다**.

이 옵션은 증분 또는 차등 백업을 수행할 때 CBT(Changed Block Tracking)를 사용할지 결정합니다.

CBT 기술은 백업 프로세스를 가속화합니다. 디스크 또는 데이터베이스 콘텐츠의 변경 사항은 블록 수준에서 지속적으로 추적됩니다. 백업이 시작되면 변경 사항을 백업에 즉시 저장할 수 있습니다.

클러스터 백업 모드

이 옵션은 Microsoft SQL Server 및 Microsoft Exchange Server의 데이터베이스 수준 백업에 적용됩니다.

개별 노드나 개별 노드 내부 데이터베이스가 아닌 클러스터 자체(Microsoft SQL Server AAG(Always On 가용성 그룹) 또는 Microsoft Exchange Server DAG(데이터베이스 가용성 그룹))가 백업을 위해 선택된 경우에만 이 옵션이 적용됩니다. 클러스터 내부의 개별 항목을 선택하면 백업이 클러스터에서 인식되지 않고 항목의 선택한 복사본만 백업됩니다.

Microsoft SQL Server

이 옵션은 SQL Server AAG(Always On 가용성 그룹)에 대한 백업 모드를 결정합니다. 이 옵션을 사용하려면 모든 AAG 노드에 Agent for SQL이 설치되어 있어야 합니다. Always On 가용성 그룹 백업에 대한 자세한 내용은 "AAG(Always On 가용성 그룹) 보호"를 참조하십시오.

사전 설정값이 **가능한 경우 보조 복제본**입니다.

다음 중 하나를 선택할 수 있습니다.

- **가능한 경우 보조 복제본**
  모든 보조 복제본이 오프라인인 경우 주 복제본이 백업됩니다. 주 복제본을 백업하면 SQL Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.
- **보조 복제본**
  모든 보조 복제본이 오프라인인 경우 백업이 실패합니다. 보조 복제본 백업은 SQL Server 성능에 영향을 주지 않으며 백업 할당 시간 연장을 허용합니다. 그러나 수동 복제본은 비동기식으로 (지연) 업데이트되도록 설정되는 경우가 많으므로 최신 정보를 포함하지 않을 수 있습니다.
- **주 복제본**
  주 복제본이 오프라인인 경우 백업이 실패합니다. 주 복제본을 백업하면 SQL Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.

이 옵션의 값에 관계없이 데이터베이스 일관성을 확보하기 위해 소프트웨어에서는 백업이 시작될 때 **동기화됨** 또는 **동기화 중** 상태가 *아닌* 데이터베이스를 건너뜁니다. 모든 데이터베이스를 건너뛰면 백업이 실패합니다.

Microsoft Exchange Server

이 옵션은 Exchange Server DAG(데이터베이스 가용성 그룹)에 대한 백업 모드를 결정합니다. 이 옵션을 사용하려면 모든 DAG 노드에 Agent for Exchange가 설치되어 있어야 합니다. 데이터베이스 가용성 그룹 백업에 대한 자세한 내용은 "DAG(데이터베이스 가용성 그룹) 보호"를 참조하십시오.

사전 설정값이 **가능한 경우 수동 복사본**입니다.

다음 중 하나를 선택할 수 있습니다.

- **가능한 경우 수동 복사본**
  모든 수동 복사본이 오프라인인 경우 활성 복사본이 백업됩니다. 활성 복사본을 백업하면 Exchange Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.
- **수동 복사본**
  모든 수동 복사본이 오프라인인 경우 백업이 실패합니다. 수동 복사본 백업은 Exchange 서버 성능에 영향을 주지 않으며 백업 할당 시간 연장을 허용합니다. 그러나 수동 사본은 비동기식으로 (지연) 업데이트되도록 설정되는 경우가 많으므로 최신 정보를 포함하지 않을 수 있습니다.
- **활성 복사본**
  활성 복사본이 오프라인인 경우 백업이 실패합니다. 활성 복사본을 백업하면 Exchange Server 작업이 느려질 수 있지만 데이터가 가장 최근 상태로 백업됩니다.

이 옵션의 값에 관계없이 데이터베이스 일관성을 확보하기 위해 소프트웨어에서는 백업이 시작될 때 **양호함** 또는 **활성** 상태가 *아닌* 데이터베이스를 건너뜁니다. 모든 데이터베이스를 건너뛰면 백업이 실패합니다.

압축 수준

이 옵션은 백업 중인 데이터에 적용되는 압축 수준을 결정합니다. 사용 가능한 수준은 **없음**, **보통**, **높음**, **최대**입니다.

사전 설정값이 **보통**입니다.

압축 수준이 높아질수록 백업 처리 시간이 더 길어지지만 백업이 차지하는 공간은 줄어듭니다. 현재 높음과 최대는 비슷한 수준을 보입니다.

최적의 데이터 압축 수준은 백업 중인 데이터의 유형에 따라 달라집니다. 백업에 기본적으로 압축된 파일(예: .jpg, .pdf 또는 .mp3)이 포함되어 있으면 최대 압축 수준에서도 백업 크기가 크게 줄어들지 않습니다. 하지만 .doc 또는 .xls 같은 포맷은 압축 효과가 뛰어납니다.

이메일 알림

이 옵션을 사용하여 백업 중에 발생하는 이벤트에 대한 이메일 알림을 설정할 수 있습니다.

이 옵션은 온프레미스 디플로이에서만 사용할 수 있습니다. 클라우드 디플로이에서 설정은 계정을 생성할 때 계정별로 구성됩니다.

사전 설정값이 **시스템 설정 사용**

시스템 설정을 사용하거나 이 계획에만 특정하게 적용되는 사용자 정의 값으로 시스템 설정을 오버라이드할 수 있습니다. 시스템 설정은 "이메일 알림"의 설명대로 구성됩니다.

중요
시스템 설정이 변경되면 시스템 설정을 사용하는 모든 보호 계획이 영향을 받습니다.

이 옵션을 활성화하기 전에 이메일 서버 설정이 구성되었는지 확인하십시오.

보호 계획에 대한 이메일 알림 사용자 정의 방법

1. **이 보호 계획에 대한 설정 사용자 정의하기**를 선택합니다.
2. **받는 사람 이메일 주소** 필드에 목적지 이메일 주소를 입력합니다. 여러 주소를 세미콜론으로 구분하여 입력할 수 있습니다.
3. [선택 사항] **제목**에서 이메일 알림 제목을 변경합니다.
   다음 변수를 사용할 수 있습니다.
   - `[Alert]` - 경보 요약입니다.
   - `[Device]` - 장치 이름입니다.
   - `[Plan]` - 경보를 생성한 계획의 이름입니다.
   - `[ManagementServer]` - 관리 서버가 설치된 머신의 호스트 이름입니다.
   - `[Unit]` - 머신이 속한 단위의 이름입니다.

   기본 제목은 다음과 같습니다. `[Alert]` **장치:** `[Device]` **계획:** `[Plan]`

4. 알림을 받을 이벤트의 확인란을 선택합니다. 백업 중에 발생하는 심각도별로 그룹화된 모든 경보 목록에서 선택할 수 있습니다.

오류 처리

이 옵션을 사용하여 백업 중 발생할 수 있는 오류를 어떻게 처리할지 지정할 수 있습니다.

오류 발생 시 재시도

사전 설정값이 **시도 횟수: 300(기본값에 무관). 불량 섹터 무시 시도 간격: 30초.**

복구 가능 오류가 발생하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

예를 들어, 네트워크 상의 백업 목적지가 사용할 수 없거나 연결할 수 없는 상태가 되면 프로그램이 30초마다 목적지 연결을 시도하지만 30회까지만 시도합니다. 연결 재개 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

클라우드 스토리지

클라우드 스토리지를 백업 목적지로 선택한 경우 옵션 값이 자동으로 **활성화됨**으로 설정됩니다. **시도 횟수: 300**. **시도 간격: 30초.**

이 경우 실제 시도 횟수는 무제한이지만 백업 실패 전의 시간 초과는 다음과 같이 계산됩니다. (300초 + **시도 간격**) * (**시도 횟수** + 1)

예:

- 기본값을 사용하면 (300초 + 30초) * (300 + 1) = 99330초 또는 ~27.6시간 후에 백업이 실패합니다.
- **시도 횟수**를 1로 설정하고 **시도 간격**을 1초로 설정하면 (300초 + 1초) * (1 + 1) = 602초 또는 ~10분 후에 백업이 실패합니다.

계산된 시간 초과가 30분을 초과하고 데이터 전송이 아직 시작되지 않은 경우 실제 시간 초과는 30분으로 설정됩니다.

처리하는 동안 메시지 및 대화 상자 표시 안 함(자동 모드)

사전 설정값이 **활성화됨**입니다.

자동 모드가 활성화되어 있으면 프로그램이 사용자 상호 작용이 필요한 상황을 자동으로 처리합니다(별도의 옵션으로 정의되는 불량 섹터 처리는 예외). 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다. 작업 로그에는 오류(있는 경우)를 포함하여 작업에 대한 자세한 정보가 기록됩니다.

불량 섹터 무시

사전 설정값이 **비활성화됨**.

이 옵션이 비활성화되어 있으면 프로그램이 불량 섹터를 발견할 때마다 백업 작업에 **상호 작용 필요** 상태가 할당됩니다. 사용 기간이 짧은 디스크에서 유효한 정보를 백업하려면 불량 섹터 무시를 활성화하십시오. 그러면 나머지 데이터는 백업되고, 생성된 디스크 백업을 다른 디스크로 마운트하여 유효한 파일을 추출할 수 있습니다.

VM 스냅샷 생성 도중 오류가 발생하는 경우 재시도

사전 설정값이 **시도 횟수: 300(기본값에 무관). 3. 시도 간격: 5분.**

가상 머신 스냅샷 생성에 실패하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

빠른 증분/차등 백업

이 옵션은 증분 및 차등 디스크 수준 백업에 유효합니다.

이 옵션은 JFS, ReiserFS3, ReiserFS4, ReFS, 또는 XFS 파일 시스템으로 포맷된 볼륨에 대해 유효하지 않습니다(항상 비활성화됨).

사전 설정값이 **활성화됨**.

증분 또는 차등 백업은 데이터의 변경 내용만 캡처합니다. 백업 프로세스의 속도를 높이기 위해 프로그램이 파일 크기와 파일이 마지막으로 수정된 날짜/시간을 기준으로 파일의 변경 유무를 판별합니다. 이 기능을 비활성화하면 프로그램이 전체 파일 내용을 백업에 저장되어 있는 내용과 비교합니다.

파일 필터

파일 필터를 사용하여 백업에 특정 파일 및 폴더만 포함하거나 백업에서 특정 파일 및 폴더를 제외할 수 있습니다.

특별히 명시되지 않은 한, 파일 필터는 디스크 수준 및 파일 수준 백업 둘 다에 사용할 수 있습니다.

파일 필터는 에이전트 없는 모드의 Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing을 통해 백업된 가상 머신의 동적 디스크(LVM 또는 LDM 볼륨)에 적용하는 경우 유효하지 않습니다.

파일 필터를 사용하도록 설정하려면

1. 보호 계획에서 **백업** 모듈을 확장합니다.
2. **백업 옵션**에서 **변경**을 클릭합니다.
3. **파일 필터**를 선택합니다.
4. 아래에서 설명하는 옵션 중 하나를 사용합니다.

특정 기준과 일치하는 파일 포함 또는 제외

반대로 동작하는 옵션이 두 개 있습니다.

- **다음 기준과 일치하는 파일만 백업**
  예: 전체 머신을 백업하도록 선택하고 필터 기준에서 **C:\File.exe**를 지정한 경우 이 파일만 백업됩니다.

  참고
  이 필터는 **버전 11**을 **백업 형식**에서 선택하고 백업 목적지가 클라우드 스토리지가 아닌 경우에는 파일 수준 백업에 적용되지 않습니다.

- **다음 기준과 일치하는 파일 백업 안 함**
  예: 전체 머신을 백업하도록 선택하고 필터 기준에서 **C:\File.exe**를 지정한 경우 이 파일만 건너뜁니다.

두 옵션을 동시에 사용할 수도 있습니다. 옵션 중 후자가 전자보다 우선합니다. 즉, 두 필드에 **C:\File.exe**를 지정하면 백업 중 이 파일은 건너뜁니다.

기준

- **전체 경로**
  드라이브 문자(Windows를 백업하는 경우) 또는 루트 디렉토리(Linux 또는 macOS를 백업하는 경우)로 시작하는 파일 또는 폴더의 전체 경로를 지정합니다.
  Windows 및 Linux/macOS 둘 다에서 파일 또는 폴더 경로에 **C:/Temp/File.tmp**처럼 슬래시를 사용할 수 있습니다.Windows에서는 **C:\Temp\File.tmp**처럼 전통적인 백슬래시를 사용할 수도 있습니다.

  중요
  백업된 머신의 운영 체제가 디스크 수준 백업 중에 올바르게 감지되지 않으면 전체 경로 파일 필터가 작동하지 않습니다. 제외 필터인 경우에는 경고가 표시됩니다. 포함 필터가 있으면 백업이 실패합니다.

  전체 경로 필터에는 드라이브 문자(Windows) 또는 루트 디렉토리(Linux 또는 macOS)가 포함됩니다. 예를 들어 파일의 전체 경로는 **C:\Temp\File.tmp**와 같을 수 있습니다. 드라이브 문자나 루트 디렉토리를 포함한 필터(예: **C:\Temp\File.tmp** 또는 **C:\Temp***)는 경고나 실패를 반환하게 됩니다.

  드라이브 문자나 루트 디렉토리를 사용하지 않는 필터(예: **Temp*** 또는 **Temp\File.tmp**) 또는 별표로 시작하는 필터(예: ***C:**)는 경고나 실패를 반환하지 않습니다. 하지만 백업된 머신의 운영 체제가 올바르게 감지되지 않으면 이러한 필터가 작동하지 않습니다.

- **이름**
  파일 또는 폴더의 이름을 지정합니다(예: **Document.txt**). 해당 이름이 포함된 모든 파일 및 폴더가 선택됩니다.

기준은 대/소문자를 구분하지 *않습니다*. 예를 들어 **C:\Temp**를 지정하면 **C:\TEMP**, **C:\temp** 등이 선택됩니다.

기준에 하나 이상의 와일드카드 문자 *, ** 및 ?를 사용할 수 있습니다. 이러한 와일드카드 문자는 전체 경로와 파일 또는 폴더 이름에 둘 다 사용할 수 있습니다.

별표(*)는 파일 이름에서 0개 이상의 문자를 대신하여 사용됩니다. 예를 들어, 기준 **Doc*.txt**는 **Doc.txt**, **Document.txt**와 같은 파일과 일치합니다.

[**버전 12** 형식의 백업에만 해당] 이중 별표(**)는 파일 이름 및 경로에서 슬래시를 포함한 0개 이상의 문자를 대체합니다. 예를 들어, 기준 ****/Docs/**.txt**는 모든 **Docs** 폴더의 모든 하위 폴더에 있는 모든 txt 파일과 일치합니다.

물음표(?)는 파일 이름에서 정확하게 같은 문자를 대신하여 사용됩니다. 예를 들어, 기준 **Doc?.txt**는 **Doc1.txt** 및 **Docs.txt**와 같은 파일과 일치하지만 **Doc.txt** 또는 **Doc11.txt** 파일과는 일치하지 않습니다.

숨겨진 파일 및 폴더 제외

이 확인란을 선택하면 Windows에서 지원하는 파일 시스템의 경우에는 **숨김** 특성이 있는 파일 및 폴더를 건너뛰고 Ext2 및 Ext3과 같은 Linux 파일 시스템의 경우에는 마침표(.)로 시작하는 파일 및 폴더를 건너뜁니다. 폴더가 숨겨진 경우 숨겨지지 않은 파일을 포함하여 폴더에 들어 있는 모든 내용이 제외됩니다.

시스템 파일 및 폴더 제외

이 옵션은 Windows에서 지원하는 파일 시스템의 경우에만 유효합니다. 이 확인란을 선택하면 **시스템** 특성이 포함된 파일 및 폴더를 건너뜁니다. 폴더에 **시스템** 특성이 포함되어 있으면 **시스템** 특성이 없는 파일을 비롯하여 폴더의 모든 내용이 제외됩니다.

참고
파일/폴더 속성 또는 attrib 명령을 사용하여 파일이나 폴더 속성을 볼 수 있습니다. 자세한 내용은 도움말 및 Windows의 지원 센터를 참조하십시오.

파일 수준 백업 스냅샷

이 옵션은 파일 수준 백업에 대해서만 유효합니다.

이 옵션은 파일을 하나씩 백업할지, 인스턴트 데이터 스냅샷을 생성하여 백업할지 정의합니다.

참고
네트워크 공유에 저장되어 있는 파일은 항상 하나씩 백업됩니다.

사전 설정값이

- Linux 실행 머신만 백업하기로 선택한 경우: **스냅샷을 생성하지 않습니다.**
- 그렇지 않은 경우: **가능한 경우 스냅샷을 만듭니다.**

다음 중 하나를 선택합니다.

- **가능한 경우 스냅샷을 만듭니다.**
  스냅샷 생성이 불가능한 경우에는 파일을 직접 백업합니다.

- **항상 스냅샷을 만듭니다.**
  스냅샷을 사용하면 독점적인 액세스 권한으로 열린 파일을 포함하여 모든 파일을 백업할 수 있습니다. 파일은 같은 시점에 백업됩니다. 이 요인들이 결정적으로 중요한 경우, 즉 스냅샷 없이 파일을 백업하는 것을 절대 허용할 수 없는 경우에만 이 설정을 선택하십시오. 스냅샷을 만들 수 없으면 백업이 실패합니다.
- **스냅샷을 생성하지 않습니다.**
  항상 파일을 직접 백업합니다. 독점적인 액세스 권한으로 열린 파일을 백업하려고 하면 읽기 오류가 발생합니다. 백업의 파일 시간이 일관되지 않을 수 있습니다.

포렌직 데이터

머신에서의 악성 활동은 바이러스, 맬웨어 및 랜섬웨어에 의해 발생할 수 있습니다. 다른 프로그램을 통한 머신 데이터의 도난 및 변경 발생 시에도 조사가 필요할 수 있습니다. 이러한 활동은 조사가 필요할 수 있습니다. 단, 조사할 머신에 디지털 증거를 유지하고 있는 경우에만 조사가 가능합니다. 안타깝지만 증거(파일, 추적 등)가 삭제되거나 머신을 사용하지 못하게 될 수 있습니다.

포렌직 데이터라는 백업 옵션을 사용하면 포렌직 조사에 사용될 수 있는 디지털 증거를 수집할 수 있습니다. 디지털 증거로 사용될 수 있는 항목에는 사용되지 않은 디스트 공간의 스냅샷, 메모리 덤프, 실행 중인 프로세스의 스냅샷이 있습니다. **포렌직 데이터** 기능은 전체 머신 백업에만 사용될 수 있습니다.

현재 **포렌직 데이터** 옵션은 다음의 OS 버전을 사용하는 Windows 머신에만 사용할 수 있습니다.

- Windows 8.1, Windows 10
- Windows Server 2012 R2 – Windows Server 2019

참고
• 머신에 백업 모듈이 포함된 보호 계획이 적용된 후에는 포렌식 데이터 설정을 수정할 수 없습니다. 다른 포렌식 데이터 설정을 사용하려면 새 보호 계획을 생성해야 합니다.
• 포렌식 데이터 컬렉션이 포함된 백업은 VPN으로 사용자 네트워크에 연결된 머신을 지원하지 않으며, 인터넷에 직접 연결할 수 없습니다.

포렌직 데이터를 포함하는 백업이 지원되는 위치:

- 클라우드 스토리지
- 로컬 폴더

  참고
  1. 로컬 폴더는 USB를 통해 연결된 외장 하드 디스크에서만 지원됩니다.
  2. 로컬 동적 디스크는 포렌직 백업의 위치로 지원되지 않습니다.

- 네트워크 폴더

포렌직 데이터를 포함하는 백업은 자동으로 공증됩니다. 조사관은 포렌직 백업을 사용하여 일반적으로 정규 백업에 포함되지 않는 디스크 영역을 분석할 수 있습니다.

포렌직 백업 프로세스

시스템은 포렌직 백업 프로세스 중 다음 작업을 수행합니다.

1. 원시 메모리 덤프와 실행 중인 프로세스 목록을 수집합니다.
2. 머신을 부트 가능한 미디어로 자동 재부팅합니다.
3. 사용된 공간과 할당되지 않은 공간을 모두 포함하는 백업을 생성합니다.
4. 백업 디스크를 공증합니다.
5. 라이브 운영 체제로 재부팅하고 계획을 계속 실행합니다(예: 복제, 보관, 유효성 검사 등).

포렌직 데이터 컬렉션을 구성하려면

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다. 또는 **계획** 탭에서 보호 계획을 생성할 수도 있습니다.
2. 장치를 선택하고 **보호**를 클릭합니다.
3. 보호 계획에서 **백업** 모듈을 활성화합니다.
4. **백업 대상**에서 **전체 머신**을 선택합니다.
5. **백업 옵션**에서 **변경**을 클릭합니다.
6. **포렌직 데이터** 옵션을 찾습니다.
7. **포렌직 데이터 수집**을 활성화합니다. 시스템은 자동으로 메모리 덤프를 수집하고 실행 중인 프로세스의 스냅샷을 생성합니다.

   참고
   전체 메모리 덤프에는 비밀번호와 같은 민감한 데이터가 포함될 수 있습니다.

8. 위치를 지정합니다.
9. **지금 실행**을 클릭해 즉시 포렌직 데이터를 포함하는 백업을 수행하거나 스케줄에 따라 백업이 생성될 때까지 기다립니다.
10. **대시보드** > **작업**으로 이동해 포렌직 데이터가 있는 백업이 성공적으로 생성되었는지 확인합니다.

그 결과로 백업에 포렌직 데이터가 포함되며, 해당 데이터를 받아 분석할 수 있습니다. 포렌직 데이터가 있는 백업은 표시가 되어 있으며 **포렌직 데이터가 있는 경우만** 옵션을 사용하여 **백업 스토리지** > **위치**의 여러 백업 중에서 필터링할 수 있습니다.

백업에서 포렌직 데이터를 가져오는 방법은?

1. Cyber Protect 웹 콘솔에서 **백업 스토리지**로 이동해 포렌식 데이터를 포함하는 백업이 있는 위치를 선택합니다.
2. 포렌직 데이터가 있는 백업을 선택하고 **백업 표시**를 클릭합니다.
3. 포렌직 데이터가 있는 백업에 대해 **복구**를 클릭합니다.
   - 포렌직 데이터만 받으려면 **포렌직 데이터**를 클릭합니다.
     시스템이 포렌직 데이터가 있는 폴더를 표시합니다. 메모리 덤프 파일 또는 다른 포렌직 파일을 선택하고 **다운로드**를 클릭합니다.

- 전체 포렌직 백업을 복구하려면 **전체 머신**을 클릭합니다. 시스템이 부트 모드 없이 백업을 복구합니다. 따라서 디스크가 변경되지 않았는지 확인할 수 있습니다.

여러 가지 타사 포렌직 소프트웨어로 제공된 메모리 덤프를 사용할 수 있습니다. 예를 들어, 추가 메모리 분석을 위해 https://www.volatilityfoundation.org에서 Volatility Framework를 사용할 수 있습니다.

포렌직 데이터를 포함하는 백업의 공증

포렌직 데이터가 있는 백업이 정확하게 실행된 이미지이고 손상되지 않았음을 확인하기 위해, 백업 모듈은 포렌직 데이터가 있는 백업의 공증을 제공합니다.

작동법

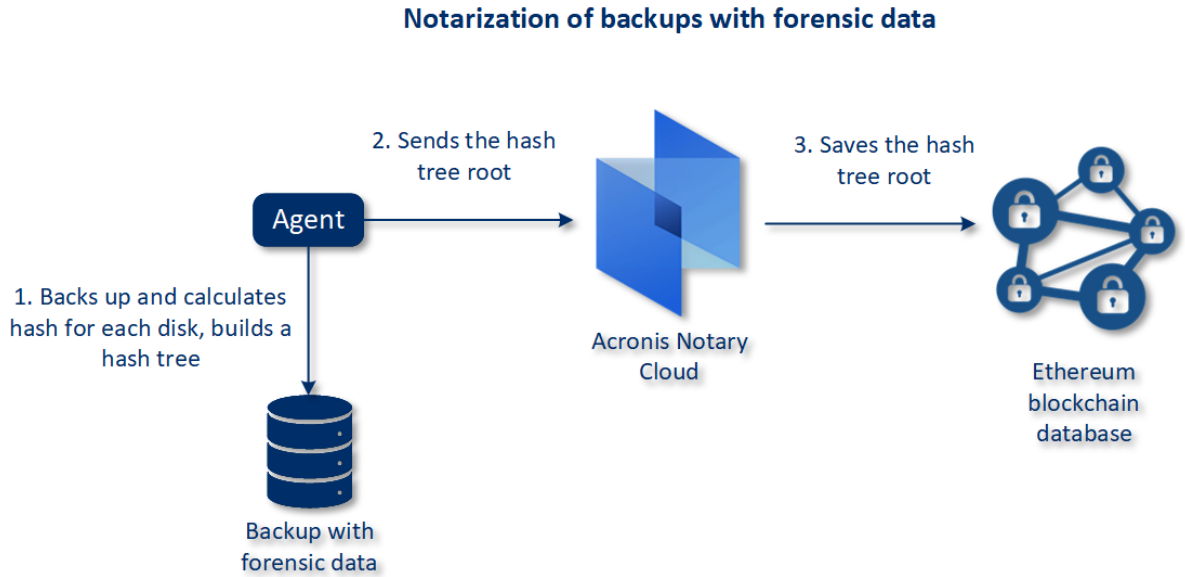
공증을 사용하면 포렌직 데이터가 있는 디스크가 신뢰할 수 있고 백업된 후 변경되지 않았음을 증명할 수 있습니다.

백업 중에 에이전트가 백업된 디스크의 해시 코드를 계산하고, 해시 트리를 생성하고, 트리를 백업에 저장한 다음 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 Ethereum 블록체인 데이터베이스에 해시 트리 루트를 저장하여 이 값이 변경되지 않도록 합니다.

포렌직 데이터가 있는 디스크의 신뢰성을 확인할 때 에이전트가 디스크의 해시를 계산한 다음 이를 백업 내부의 해시 트리에 저장되어 있는 해시와 비교합니다. 두 해시가 일치하지 않으면 디스크가 신뢰할 수 없는 것으로 간주됩니다. 그렇지 않으면 해시 트리에 의해 디스크 신뢰성이 보증됩니다.

해시 트리 자체가 손상되지 않았는지 확인하기 위해 에이전트는 해시 트리 루트를 공증 서비스로 전송합니다. 공증 서비스는 이를 블록체인 데이터베이스에 저장되어 있는 해시 트리 루트와 비교합니다. 해시가 일치하면 선택한 디스크는 신뢰할 수 있는 것으로 보증됩니다. 그렇지 않으면 소프트웨어에 디스크를 신뢰할 수 없다는 메시지가 표시됩니다.

아래의 구성표는 포렌직 데이터를 포함하는 백업의 공증 프로세스를 간략하게 보여줍니다.



공증된 디스크 백업을 수동으로 검증하려면 디스크 백업에 대한 인증서를 받고 tibxread 도구를 사용하여 인증서에 나타난 확인 절차를 수행할 수 있습니다.

포렌직 데이터를 포함하는 백업에 대한 인증서 받기

콘솔에서 포렌직 데이터를 포함하는 백업에 대한 인증서를 받으려면 다음 작업을 수행합니다.

1. **백업 스토리지**로 이동하고 포렌직 데이터가 있는 백업을 선택합니다.
2. 전체 머신을 복구합니다.
3. 시스템에 **디스크 매핑** 보기가 열립니다.
4. 디스크의 **인증서 가져오기** 아이콘을 클릭합니다.
5. 시스템이 인증서를 생성하고 브라우저에서 인증서가 포함된 새 창이 열립니다. 인증서 아래에 공증된 디스크 백업의 수동 검증을 위한 지침이 표시됩니다.

백업 데이터를 받기 위한 "tibxread" 도구

Cyber Protect에서는 백업 디스크 무결성의 수동 확인을 위한 `tibxread`라는 도구를 제공합니다. 이 도구를 사용하면 백업의 데이터를 받고 특정 디스크의 해시를 계산할 수 있습니다. 도구는 자동으로 다음 컴퍼넌트와 함께 설치됩니다: Agent for Windows, Agent for Linux 및 Agent for Mac. 경로 위치: `C:\Program Files\Acronis\BackupAndRecovery`

지원되는 위치:

- 로컬 디스크
- 자격 증명 없이 액세스할 수 있는 네트워크 폴더(CIFS/SMB).
  비밀번호로 보호된 네트워크 폴더의 경우, OS 도구를 사용해 로컬 폴더에 네트워크 폴더를 마운트한 다음 로컬 폴더를 이 도구의 소스로 마운트할 수 있습니다.
- 클라우드 스토리지
  URL, 포트 및 인증서를 제공해야 합니다. URL과 포트는 Windows 레지스트리 키 또는 Linux/Mac 머신의 구성 파일에서 가져올 수 있습니다.
  Windows:

  ```
  HKEY_LOCAL_
  MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Defa
  ult\<tenant_login>\FesUri
  ```

  Linux:

  ```
  /etc/Acronis/BackupAndRecovery.config
  ```

  macOS:

  ```
  /Library/Application Support/Acronis/Registry/BackupAndRecovery.config
  ```

  인증서는 다음 위치에서 찾을 수 있습니다.
  Windows:

```
%allusersprofile%\Acronis\BackupAndRecovery\OnlineBackup\Default
```

Linux:

```
/var/lib/Acronis/BackupAndRecovery/OnlineBackup/Default
```

macOS:

```
/Library/Application Support/Acronis/BackupAndRecovery/OnlineBackup/Default
```

도구에는 다음 명령이 있습니다.

- list backups
- list content
- get content
- calculate hash

list backups

백업에서 복구 지점을 나열합니다.

개요:

```
tibxread list backups --loc=URI --arc=BACKUP_NAME --raw
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--raw
--utc
--log=PATH
```

```
Output template:
```

```
GUID   Date   Date timestamp
----   ------ --------------
<guid> <date> <timestamp>
```

<guid> – 백업 GUID.

<date> – 백업 생성 날짜. 형식은 다음과 같습니다. DD.MM.YYYY HH24:MM:SS. 기본적으로 현지 시간대를 사용합니다(--utc 옵션을 사용해 변경할 수 있습니다).

출력 예:

```
GUID   Date   Date timestamp
----   ------ --------------
```

```
516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865
516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925
```

list content

복구 지점의 콘텐츠를 나열합니다.

개요:

```
tibxread list content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID
--raw --log=PATH
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--raw
--log=PATH
```

출력 템플릿:

```
Disk     Size   Notarization status
-------- ------ --------------------
<number> <size> <notarization_status>
```

<number> – 디스크 식별자.

<size> – 크기(바이트).

<notarization_status> – 가능한 상태: 공증 없음, 공증됨, 다음 백업.

출력 예:

```
Disk     Size   Notary status
-------- ------ --------------
1        123123465798 Notarized
2        123123465798 Notarized
```

get content

복구 지점에서 표준 출력(stdout)으로 지정된 디스크의 콘텐츠를 작성합니다.

개요:

```
tibxread get content --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID -
-disk=DISK_NUMBER --raw --log=PATH --progress
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
--progress
```

calculate hash

SHA-256 알고리즘을 사용하여 복구 지점에서 지정된 디스크의 해시를 계산하고 stdout으로 작성합니다.

개요:

```
tibxread calculate hash --loc=URI --arc=BACKUP_NAME --password --backup=RECOVERY_POINT_ID --disk=DISK_NUMBER --raw --log=PATH --progress
```

옵션

```
--loc=URI
--arc=BACKUP_NAME
--password
--backup=RECOVERY_POINT_ID
--disk=DISK_NUMBER
--raw
--log=PATH
```

옵션 설명

옵션	설명
--arc=BACKUP_NAME	웹 콘솔의 백업 속성에서 가져올 수 있는 백업 파일 이름입니다. 백업 파일은 확장자 .tibx로 지정되어야 합니다.
--backup=RECOVERY_POINT_ID	복구 지점 식별자
--disk=DISK_NUMBER	디스크 번호("get content" 명령의 출력으로 작성된 것과 동일)

--loc=URI	백업 위치 URI입니다. 가능한 "--loc" 옵션 형식:
	• 로컬 경로 이름(Windows)
	`c:/upload/backups`
	• 로컬 경로 이름(Linux)
	`/var/tmp`

	• SMB/CIFS
	`\\server\folder`
	• 클라우드 스토리지
	`--loc=<IP_address>:443 --cert=<path_to_certificate> [--storage_path=/1]`
	`<IP_address>` – Windows의 레지스트리 키에서 찾을 수 있습니다. HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\Settings\OnlineBackup\FesAddressCache\Default\<tenant_login>\FesUri
	`<path_to_certificate>` – Cyber Cloud에 액세스하기 위한 인증서 파일의 경로. 예를 들어, Windows에서 이 인증서는 `C:\ProgramData\Acronis\BackupAndRecovery\OnlineBackup\Default\<username>.crt`에 있습니다. 여기서 <username>은 Cyber Cloud에 액세스하기 위한 계정 이름입니다.

--log=PATH	지정된 경로(로컬 경로만 해당, 형식은 `--loc=URI` 매개변수와 동일)로 로그 작성을 활성화합니다. 로깅 수준은 디버그입니다.
--password=PASSWORD	백업을 위한 암호화 비밀번호입니다. 백업이 암호화되지 않은 경우 이 값을 비워두십시오.

--raw	명령 출력에서 헤더(첫 두 행)을 숨깁니다. 명령 출력 구문을 분석해야 할 때 사용됩니다.
	"`--raw`" 없는 출력 예:
	`GUID Date Date timestamp`
	`---- ------ --------------`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`
	"`--raw`" 있는 출력:
	`516FCE73-5E5A-49EF-B673-A9EACB4093B8 18.12.2019 16:01:05 1576684865`
	`516FCE73-5E5A-49EF-B673-A9EACB4093B9 18.12.2019 16:02:05 1576684925`

--utc	날짜를 UTC로 표시합니다.

--progress	작업의 진행 상태를 표시합니다.
	예:
	`1%`
	`2%`
	`3%`
	`4%`
	`...`
	`100%`

로그 자르기

이 옵션은 Microsoft SQL Server 데이터베이스 백업, 그리고 Microsoft SQL Server 애플리케이션 백업이 활성화되어 있는 상태에서의 디스크 수준 백업에 유효합니다.

이 옵션은 성공적인 백업 후에 SQL Server 트랜잭션 로그를 자를지 결정합니다.

사전 설정값이 **활성화됨**.

이 옵션이 활성화되어 있으면 이 소프트웨어에서 생성한 백업의 시점으로만 데이터베이스를 복구할 수 있습니다. Microsoft SQL Server의 네이티브 백업 엔진을 사용하여 트랜잭션 로그를 백업하는 경우에는 이 옵션을 비활성화하십시오. 트랜잭션 로그를 복구 후에 적용할 수 있기 때문에 결국 데이터베이스를 어느 시점으로든 복구할 수 있습니다.

LVM 스냅샷 촬영

이 옵션은 실제 머신에 대해서만 유효합니다.

이 옵션은 Linux LVM(논리 볼륨 관리자)으로 관리하는 볼륨의 디스크 수준 백업에 대해 유효합니다. 해당 볼륨을 논리 볼륨이라고도 합니다.

이 옵션은 논리 볼륨의 스냅샷을 어떻게 생성할지 결정합니다. 백업 소프트웨어는 자체적으로 결정할 수도 있고, Linux LVM(논리 볼륨 관리자)을 통해 결정할 수도 있습니다.

사전 설정값이 **백업 소프트웨어 사용**.

- **백업 소프트웨어 사용**. 스냅샷 데이터는 주로 RAM에 보관됩니다. 따라서 더 빠르게 백업되고 볼륨 그룹의 할당되지 않은 공간이 필요 없습니다. 결국 논리 볼륨을 백업하는 중 문제가 발생한 경우에만 사전 설정을 변경하는 것이 좋습니다.
- **LVM 사용**. 스냅샷이 볼륨 그룹의 할당되지 않은 공간에 저장됩니다. 할당되지 않은 공간이 누락되면 백업 소프트웨어가 스냅샷을 생성합니다.

마운트 포인트

이 옵션은 Windows에서 마운트된 볼륨 또는 클러스터 공유 볼륨을 포함하는 데이터 소스의 파일 수준 백업에만 유효합니다.

이 옵션은 폴더 계층 구조에서 마운트 포인트보다 상위 폴더를 백업하기 위해 선택하는 경우에만 유효합니다. (마운트 포인트는 추가 볼륨이 논리적으로 연결되는 폴더입니다.)

- 해당 폴더(상위 폴더)가 백업용으로 선택되고 **마운트 포인트** 옵션이 활성화되면 마운트된 볼륨에 있는 모든 파일이 백업에 포함됩니다. **마운트 포인트** 옵션이 비활성화되면 백업의 마운트 포인트가 비워집니다.

  상위 폴더를 복구하는 경우, **복구 시 마운트 포인트** 옵션의 활성화 또는 비활성화 여부에 따라 마운트 포인트 내용이 복구되거나 복구되지 않습니다.
- 마운트 포인트를 직접 선택하거나 마운트된 볼륨 내부의 폴더를 선택하는 경우, 선택한 폴더는 일반 폴더로 간주됩니다. 해당 폴더는 **마운트 포인트** 옵션의 상태에 관계없이 백업되고 **마운트 포인트** 옵션의 상태에 관계 없이 복구됩니다.

사전 설정값이 **비활성화됨**.

참고
파일 수준 백업으로 전체 볼륨 또는 필요한 파일을 백업하여 클러스터 공유 볼륨에 상주하는 Hyper-V 가상 머신을 백업할 수 있습니다. 가상 머신의 전원을 끄면 일관된 상태로 백업할 수 있습니다.

예

C:\Data1 폴더를 마운트된 볼륨의 마운트 포인트로 가정합니다. 볼륨에는 **Folder1** 및 **Folder2** 폴더가 포함됩니다. 파일 수준의 데이터 백업을 위한 보호 계획을 생성합니다.

볼륨 C 확인란을 선택하고 **마운트 포인트** 옵션을 활성화하면 백업의 **C:\Data1** 폴더에 **Folder1**과 **Folder2**가 포함됩니다. 백업된 데이터를 복구할 때는 복구 시 마운트 포인트 옵션을 올바르게 사용해야 합니다.

볼륨 C 확인란을 선택하고 **마운트 포인트** 옵션을 비활성화하면 백업의 **C:\Data1** 폴더가 비워집니다.

Data1, **Folder1** 또는 **Folder2** 폴더 확인란을 선택하면 **마운트 포인트** 옵션의 상태에 관계없이 선택한 폴더가 백업에서 일반 폴더로 포함됩니다.

다중 볼륨 스냅샷

이 옵션은 Windows 또는 Linux를 실행하는 실제 머신의 백업에 유효합니다.

이 옵션은 디스크 수준 백업에 적용됩니다. 또한, 이 옵션은 스냅샷 생성을 통해 파일 수준 백업을 수행할 때 파일 수준 백업에도 적용됩니다. ("파일 수준 백업 스냅샷" 옵션은 파일 수준 백업 중 스냅샷을 생성할지 결정합니다.)

이 옵션은 여러 볼륨의 스냅샷을 동시에 생성할지, 아니면 하나씩 생성할지 결정합니다.

사전 설정값이

- Windows를 실행하는 머신을 최소 하나 백업용으로 선택한 경우: **활성화됨**.
- 머신을 선택하지 않은 경우(**계획 > 백업** 페이지에서 보호 계획 생성을 시작하는 경우): **활성화됨**.
- 그렇지 않은 경우: **비활성화됨**.

이 옵션이 활성화되어 있으면 백업 중인 모든 볼륨의 스냅샷이 동시에 생성됩니다. 여러 볼륨(예: Oracle 데이터베이스)에 분산되어 있는 데이터의 백업을 시간이 일관되게 생성하려면 이 옵션을 사용하십시오.

이 옵션이 비활성화되어 있으면 볼륨의 스냅샷이 하나씩 생성됩니다. 결국, 데이터가 여러 볼륨에 분산되어 있는 경우 생성되는 백업의 시간이 일관되지 않을 수 있습니다.

원클릭 복구

원클릭 복구를 사용하면 사용자가 머신의 최신 디스크 백업을 자동으로 복구할 수 있습니다. 이 백업은 전체 머신의 백업일 수도 있고 특정 디스크 볼륨의 백업일 수도 있습니다.

이 기능은 관리자가 Startup Recovery Manager와 함께 기능을 활성화한 후 사용자의 머신에서 액세스할 수 있습니다. 관리자는 명령줄 인터페이스를 통해서만 이 작업을 수행할 수 있습니다. Startup Recovery Manager 및 원클릭 복구 활성화 방법에 대한 자세한 내용은 명령줄 인터페이스를 참조하십시오.

원클릭 복구는 다음 백업 스토리지를 지원합니다.

1. Secure Zone
2. 네트워크 저장 장치
3. 클라우드 스토리지

특정 스토리지 유형을 사용할 수 없거나 스토리지 유형에 디스크 백업이 없는 경우 다음 스토리지 유형을 사용할지 묻는 메시지가 표시됩니다.

디스크 백업을 포함하는 백업 세트(*아카이브*라고도 함)가 스토리지에 둘 이상 있으면 원클릭 복구는 마지막으로 업데이트된 백업 세트를 선택합니다. 사용자는 다른 백업 세트를 선택할 수 없습니다.

원클릭 복구는 다음 작업을 지원합니다.

- 최신 백업에서 자동 복구
- 자동으로 선택된 백업 세트 내의 특정 백업(*복구 지점*이라고도 함)에서 복구

원클릭 복구를 사용하여 머신 복구

사전 요구 사항

- 관리자가 선택한 머신에서 원클릭 복구를 활성화했습니다.
- 선택한 머신의 디스크 백업이 하나 이상 있습니다.

머신을 복구하려면

1. 복구할 머신을 재부팅합니다.
2. 재부팅 중 F11 키를 눌러 Startup Recovery Manager로 들어갑니다.
3. 원하는 원클릭 복구 옵션을 선택합니다.
   - 자동으로 최신 백업을 복구하려면 키보드에서 1을 누릅니다.
   - 마지막으로 업데이트된 백업 세트 내의 다른 백업을 복구하려면 키보드에서 2를 누릅니다.
     - 원하는 백업(*복구 지점*이라고도 함)을 선택하려면 키보드에서 해당 숫자를 누릅니다.

그래픽 사용자 인터페이스가 시작된 후 사라집니다. 그래픽 사용자 인터페이스 없이 복구 절차가 계속됩니다. 복구가 완료되면 머신이 재부팅됩니다.

성능 및 백업 할당 시간

이 옵션을 사용하면 일주일 동안의 매 시간에 대해 세 가지 백업 성능 수준(높음, 낮음, 금지됨) 중 하나를 설정할 수 있습니다. 이런 식으로 백업이 시작 및 실행될 수 있는 할당 시간을 정의할 수 있습니다. 높음 및 낮음 성능 수준은 프로세스 우선 순위와 출력 속도를 통해 구성 가능합니다.

웹사이트 백업 또는 클라우드 복구 사이트에 위치한 서버의 백업처럼 클라우드 에이전트에 의해 실행되는 백업에는 이 옵션을 사용할 수 없습니다.

이 옵션은 보호 계획에 지정되어 있는 각 위치마다 별도로 구성할 수 있습니다. 복제 위치에 대해 이 옵션을 구성하려면 해당 위치 이름 옆에 있는 기어 아이콘을 클릭한 다음 **성능 및 백업 할당 시간**을 클릭합니다.

이 옵션은 백업 및 백업 복제 프로세스에 대해서만 유효합니다. 보호 계획에 포함된 백업 후 명령 및 기타 작업(유효성 검사, 가상 머신으로 변환)은 이 옵션과 무관하게 실행됩니다.

사전 설정값이 **비활성화됨**입니다.

이 옵션이 비활성화되면 다음 매개변수와 함께 백업이 언제든 실행될 수 있습니다(매개변수가 사전 설정 값과 다르게 변경되어도 무관):

- CPU 우선 순위: **낮음**(Windows에서는 **보통 이하**)입니다.
- 출력 속도: **제한 없음.**

이 옵션이 활성화되면 현재 시간에 대해 지정된 성능 매개변수에 따라 예약된 백업이 허용 또는 차단됩니다. 백업이 차단된 시간이 시작될 때 백업 프로세스가 자동으로 중단되고 경보가 생성됩니다.

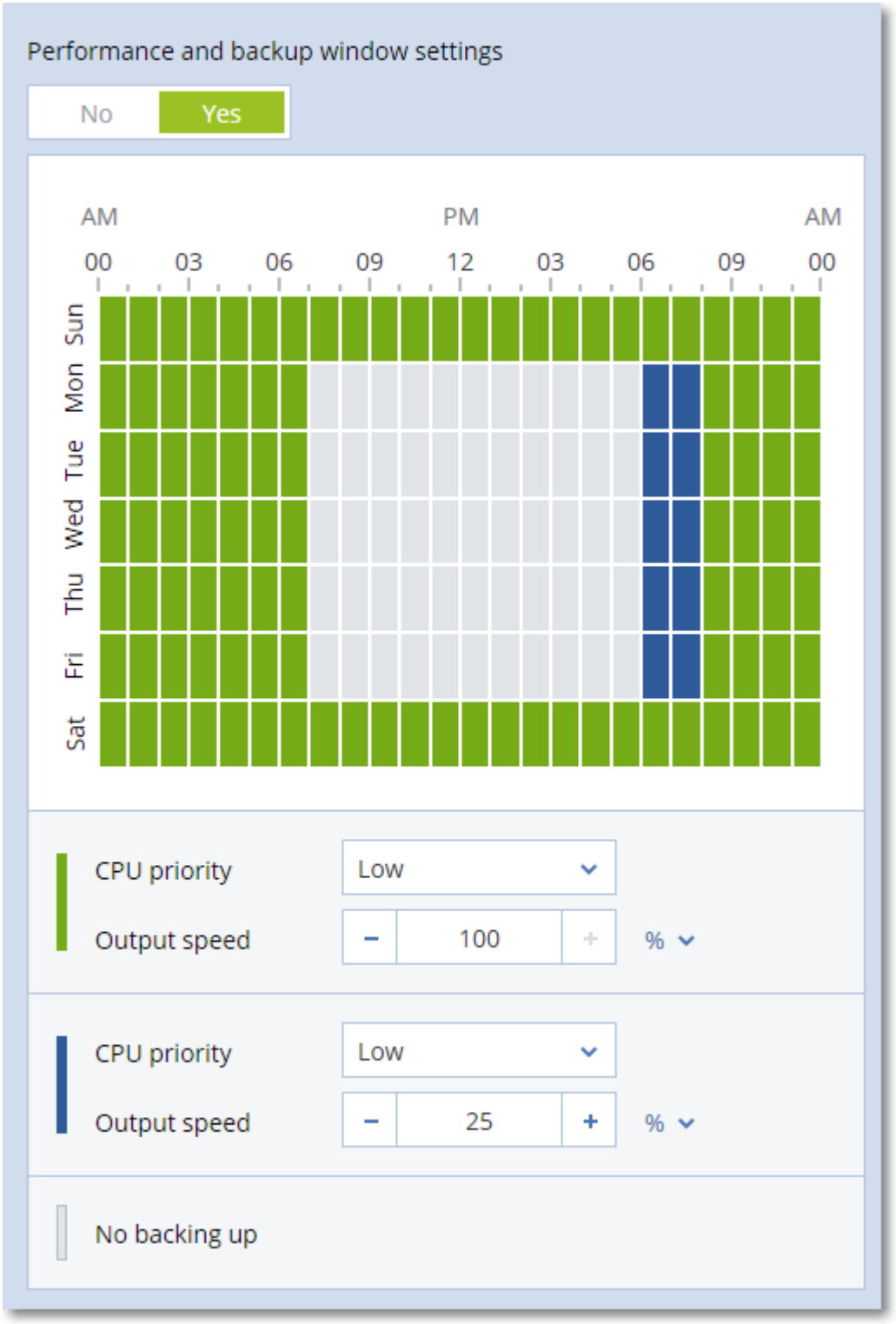
예약된 백업이 차단된다고 해도 백업을 수동으로 시작할 수 있습니다. 이 경우 백업이 허용되었던 가장 최근의 시간에 설정된 성능 매개변수를 사용합니다.

백업 할당 시간

각 직사각형이 평일 내 한 시간을 나타냅니다. 직사각형을 클릭하면 다음 상태를 순환합니다.

- **초록색:** 아래 초록색 섹션에 지정되어 있는 매개변수를 통해 백업이 허용됩니다.
- **파란색:** 아래 파란색 섹션에 지정되어 있는 매개변수를 통해 백업이 허용됩니다.
  백업 형식이 **버전 11**로 설정된 경우에는 이 상태를 사용할 수 없습니다.
- **회색:** 백업이 차단됩니다.

여러 직사각형의 상태를 동시에 변경하려면 클릭 후 드래그하면 됩니다.



CPU 우선 순위

이 매개변수는 운영 체제에서 백업 프로세스의 우선 순위를 정의합니다.

사용 가능한 설정은

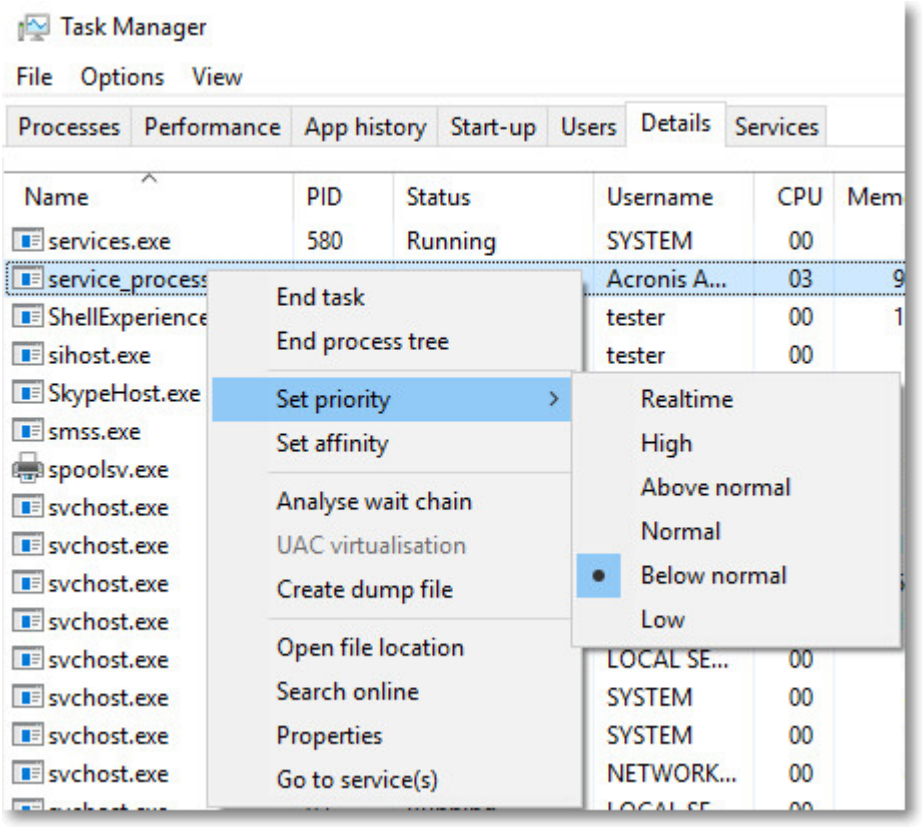
낮음 - Windows에서는 **보통 이하**입니다.

보통 - Windows에서는 **보통**입니다.

높음 - Windows에서는 **높음**입니다.

시스템에서 실행하는 프로세스의 우선 순위는 CPU와 해당 프로세스에 할당된 시스템 리소스를 결정합니다. 백업 우선순위를 낮추면 다른 애플리케이션에 더 많은 리소스를 사용할 수 있게 됩니다. 백업 우선순위를 높이면 CPU 등과 같은 더 많은 리소스를 백업 애플리케이션에 할당하도록 운영 체제에 요청하여 백업 프로세스의 속도를 높일 수 있습니다. 그러나 결과는 전체 CPU 사용량 및 디스크 입/출력 속도 또는 네트워크 트래픽 등과 같은 다른 요인에 따라 달라집니다.

이 옵션은 Windows에서는 백업 프로세스(**service_process.exe**)의 우선 순위를 설정하고, Linux 및 OS X에서는 백업 프로세스(**service_process**) 의 스케줄링 우선 순위를 설정합니다.



백업 중 출력 속도

이 매개변수를 사용하여 하드 드라이브 쓰기 속도(로컬 폴더로 백업하는 경우) 또는 네트워크를 통한 백업 데이터 전송 속도(네트워크 공유 또는 클라우드 스토리지로 백업하는 경우)를 제한할 수 있습니다.

이 옵션이 활성화되어 있으면 다음과 같은 허용되는 최대 출력 속도를 지정할 수 있습니다.

- 대상 하드 디스크의 예상 쓰기 속도(로컬 폴더로 백업하는 경우) 또는 네트워크 연결의 예상 최고 속도(네트워크 공유 또는 클라우드 스토리지로 백업하는 경우)의 비율.
  이 설정은 에이전트가 Windows에서 실행 중인 경우에만 작동합니다.
- KB/초(모든 대상에 대해).

실제 데이터 전달

이 옵션은 백업 목적지가 클라우드 스토리지이고 백업 형식이 **버전 12**로 설정된 경우 효과적입니다.

이 옵션은 Agent for Windows, Agent for Linux, Agent for Mac, Agent for VMware, Agent for Hyper-V, 및 Agent for Virtuozzo에서 생성한 디스크 수준 백업 및 파일 백업에 효과적입니다. 부트 가능한 미디어를 통해 생성된 백업은 지원되지 않습니다.

이 옵션은 보호 계획에서 생성한 첫 번째 전체 백업을 실제 데이터 전달 서비스를 사용하여 하드 디스크 드라이브의 클라우드 스토리지로 보낼지 여부를 결정합니다. 이후 증분 백업은 네트워크를 통해 수행할 수 있습니다.

사전 설정값이 **비활성화됨**.

실제 데이터 전달 서비스 정보

실제 데이터 전달 서비스 웹 인터페이스는 온프레미스 디플로이의 조직 관리자 및 클라우드 디플로이의 관리자만 사용할 수 있습니다.

실제 데이터 전달 서비스 및 주문 생성 도구의 사용에 대한 자세한 지침은 실제 데이터 전달 관리자 안내서를 참조하십시오. 실제 데이터 전달 서비스 웹 인터페이스에서 이 문서에 액세스하려면 물음표 아이콘을 클릭하십시오.

실제 데이터 전달 프로세스 개요

1. 새 보호 계획을 생성합니다. 이 계획에서 **실제 데이터 전달** 백업 옵션을 활성화합니다.
   드라이브로 직접 백업하거나 로컬 또는 네트워크 폴더로 백업한 다음 백업을 드라이브로 복사/이동할 수 있습니다.

   중요
   초기 전체 백업이 완료되면 이후의 백업은 동일한 보호 계획으로 수행해야 합니다. 다른 보호 계획에서는 매개변수와 머신이 동일하더라도 또 다른 실제 데이터 전달 사이클이 필요합니다.

2. 첫 번째 백업이 완료된 후 실제 데이터 전달 서비스 웹 인터페이스를 사용하여 주문 생성 도구를 다운로드하고 주문을 생성합니다.
   이 웹 인터페이스에 액세스하려면 다음 중 하나를 수행합니다.
   - 온-프레미스 디플로이: Acronis 계정에 로그인한 다음, **실제 데이터 전달** 아래의 **콘솔 추적으로 이동**을 클릭합니다.
   - 클라우드 배포: 관리 포털에 로그인하고 **개요** > **사용**을 클릭한 다음 **실제 데이터 전달** 아래의 **서비스 관리**를 클릭합니다.
3. 드라이브를 패키징하고 데이터 센터에 전달합니다.

   중요
   실제 데이터 전달 관리자 안내서에 나온 패키징 지침을 따라야 합니다.

4. 실제 데이터 전달 서비스 웹 인터페이스를 사용하여 주문 상태를 추적하십시오. 이후의 백업은 처음 백업이 클라우드 스토리지에 업로드될 때까지 실패하게 됩니다.

사전/사후 명령어

이 옵션을 사용하여 백업 절차 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다.

다음 도식은 사전/사후 명령어를 언제 실행하는지 보여줍니다.

백업 전 명령	백업	백업 후 명령

사전/사후 명령어를 사용하는 방법의 예:

- 백업을 시작하기 전에 디스크에서 일부 임시 파일을 삭제합니다.
- 백업을 시작하기 전에 매번 서드 파티 안티바이러스 제품을 시작하도록 구성합니다.
- 선택적으로 백업을 다른 위치로 복사합니다. 이 옵션을 활성화하면 보호 계획에 구성되어 있는 복제가 *모든* 백업을 후속 위치로 복사하기 때문에 유용할 수 있습니다.

프로그램은 백업 이후 명령을 실행한 후 복제를 수행합니다.

프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.

백업 전 명령

백업 프로세스가 시작되기 전에 실행할 명령/배치 파일을 지정하려면

1. **백업 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	선택			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨
명령 실행이 완료될 때까지 백업 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				

	사전 설정 명령이 성공적으로 실행된 후에만 백업을 수행합니다. 명령 실행에 실패한 경우 백업 실패.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 백업을 수행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 백업을 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

백업 후 명령

백업이 완료된 후에 실행할 명령/실행 파일을 지정하려면

1. **백업 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 명령 실행이 반드시 성공해야 하는 경우 **명령 실행에 실패한 경우 백업 실패** 확인란을 선택합니다. 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다. 명령 실행에 실패하면 백업 상태가 **오류**로 설정됩니다.
   이 확인란을 선택하지 않으면 명령 실행 결과가 백업 실패 또는 성공에 영향을 주지 않습니다. **작업** 탭을 살펴보면 명령 실행 결과를 추적할 수 있습니다.
6. **완료**를 클릭합니다.

데이터 캡처 전/후 명령

이 옵션을 사용하여 데이터 캡처(즉, 데이터 스냅샷 생성) 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다. 데이터 캡처는 백업 절차 시작 시 수행됩니다.

다음 도식은 데이터 캡처 전/후 명령을 언제 실행하는지 보여줍니다.

	<---------- 백업 ---------->				
백업 전 명령	데이터 캡처 전 명령	데이터 캡처	데이터 캡처 후 명령		백업 후 명령

Volume Shadow Copy Service 옵션이 활성화되어 있으면 명령의 실행과 Microsoft VSS 작업이 다음과 같은 순서로 수행됩니다.

"데이터 캡처 전" 명령 - VSS 일시중지 - 데이터 캡처 - VSS 재개 - "데이터 캡처 후" 명령.

데이터 캡처 전/후 명령을 사용하여 VSS와 호환되지 않는 데이터베이스 또는 애플리케이션을 일시 중지했다가 다시 시작할 수 있습니다. 데이터 캡처는 몇 초 안에 완료되기 때문에 데이터베이스 또는 애플리케이션 유휴 시간은 최소화됩니다.

데이터 캡처 전 명령

데이터 캡처 전에 실행할 명령/배치 파일을 지정하려면

1. **데이터 캡처 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	**선택**			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨
명령 실행이 완료될 때까지 데이터 캡처 수행 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 데이터 캡처를 수행합니다.명령 실행에 실패한 경우 백업 실패.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 데이터 캡처를 수행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 데이터 캡처를 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

데이터 캡처 후 명령

데이터 캡처가 완료된 후에 실행할 명령/배치 파일을 지정하려면

1. **데이터 캡처 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	**선택**			
명령 실행에 실패한 경우 백업 실패	선택됨	선택 해제됨	선택됨	선택 해제됨

명령 실행이 완료될 때까지 백업 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 백업을 계속 진행합니다.	실행 실패 또는 성공에 상관없이 명령이 실행된 후에 백업을 계속 진행합니다.	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 백업을 계속 진행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

SAN 하드웨어 스냅샷

이 옵션은 VMware ESXi 가상 머신의 백업에만 적용됩니다.

사전 설정값이 **비활성화됨**.

이 옵션에 따라 백업을 수행할 때 SAN 스냅샷을 사용할지 여부가 결정됩니다.

이 옵션이 비활성화되면 VMware 스냅샷에서 가상 디스크 내용을 읽습니다. 스냅샷은 전체 백업 기간 동안 보관됩니다.

이 옵션이 활성화되면 SAN 스냅샷에서 가상 디스크 내용을 읽습니다. 가상 디스크를 일관된 상태로 가져오기 위해 VMware 스냅샷이 생성되고 잠시 유지됩니다. SAN 스냅샷에서 읽을 수 없으면 백업이 실패합니다.

이 옵션을 활성화하기 전에 "SAN 하드웨어 스냅샷 사용"에 나열된 요구 사항을 확인하고 수행하십시오.

일정 예약

이 옵션은 백업을 일정대로 시작할지, 지연 후 시작할지를 정의하고, 몇 개의 가상 머신을 동시에 백업할지도 정의합니다.

사전 설정값이

- 온프레미스 디플로이: **예약된 대로 정확하게 모든 백업을 시작합니다.**
- 클라우드 배포: **일정 시간 내에 백업 시작 시간을 분배합니다. 최대 지연: 30분.**

다음 중 하나를 선택합니다.

- **예약된 대로 정확하게 모든 백업 시작**
  실제 머신의 백업이 예약된 대로 정확하게 시작됩니다. 가상 머신은 하나씩 백업됩니다.
- **기간 내에서 시작 시간 분배**

실제 머신의 백업이 예약된 시간보다 지연되어 시작됩니다. 각 머신에 대한 지연 값은 임의로 선택되며 이 값의 범위는 0에서부터 지정된 최대값까지 입니다. 여러 머신을 네트워크 위치로 백업하는 경우 과도한 네트워크 부하를 피하기 위해 이 설정을 사용할 수 있습니다. 보호 계획이 머신에 적용될 때 각 머신에 대한 지연 값이 결정되어 보호 계획을 편집하고 최대 지연 값을 변경할 때까지 동일하게 유지됩니다.

가상 머신은 하나씩 백업됩니다.

- **다음까지 동시에 실행되는 백업 수 제한**

  이 옵션은 하나의 보호 계획이 여러 가상 머신에 적용될 때에만 사용할 수 있습니다. 이 옵션은 정해진 보호 계획을 실행할 때 에이전트가 몇 개의 가상 머신을 동시에 백업할 수 있는지 정의합니다.

  보호 계획에 따라 에이전트가 한 번에 여러 머신의 백업을 시작해야 하는 경우 에이전트는 두 개 머신을 선택합니다. (백업 성능을 최적화하기 위해 에이전트는 서로 다른 스토리지에 저장되어 있는 머신을 매칭하려고 시도합니다.) 두 백업 중 어느 하나가 완료되면 에이전트는 세 번째 머신을 선택하는 식으로 진행합니다.

  에이전트가 동시에 백업하는 가상 머신 수를 변경할 수 있습니다. 최대값은 10입니다. 그러나 에이전트가 시간이 겹치는 여러 보호 계획을 실행하는 경우 각 옵션에 지정된 숫자가 합산됩니다. 실행 중인 보호 계획의 수에 상관없이 에이전트가 동시에 백업할 수 있는 가상 머신의 총 수를 제한할 수 있습니다.

  실제 머신의 백업이 예약된 대로 정확하게 시작됩니다.

섹터 단위 백업

이 옵션은 디스크 수준 백업에 대해서만 유효합니다.

이 옵션은 물리적 수준에서 디스크 또는 볼륨의 똑같은 사본을 생성할지 결정합니다.

사전 설정값이 **비활성화됨**.

이 옵션이 활성화되어 있는 경우 할당되지 않은 공간과 데이터가 없는 섹터를 포함한 디스크 또는 볼륨의 모든 섹터가 백업됩니다. 생성되는 백업은 백업 대상 디스크와 크기가 같아집니다("압축 수준" 옵션이 **없음**으로 설정되어 있는 경우). 인식되지 않는 또는 지원되지 않는 파일 시스템이 있는 드라이브를 백업할 때에는 소프트웨어가 섹터 단위 모드로 자동 전환됩니다.

참고
섹터 단위 모드에서 생성된 백업의 애플리케이션 데이터에 대한 복구를 실행하는 것이 불가능해집니다.

분할

이 옵션은 **항상 전체, 매주 전체, 매일 증분, 매월 전체, 매주 차등, 매일 증분(GFS)** 및 **사용자 정의** 백업 구성표에 적용됩니다.

이 옵션을 통해 대용량 백업을 더 작은 파일들로 분할하는 방법을 선택할 수 있습니다.

사전 설정값이 **자동**입니다.

다음 설정을 사용할 수 있습니다.

- **자동**
  백업이 파일 시스템에서 지원하는 최대 파일 크기를 초과하는 경우 분할됩니다.
- **고정 크기**
  원하는 파일 크기를 입력하거나 드롭다운 목록에서 선택합니다.

테이프 관리

이러한 옵션은 백업 대상이 테이프 장치인 경우에 유효합니다.

테이프에 저장된 디스크 백업에서 파일 복구 활성화

사전 설정값이 **비활성화됨**.

이 확인란을 선택하면 백업할 때마다 테이프 장치가 연결된 머신의 하드 디스크에서 보조 파일이 생성됩니다. 디스크 백업으로부터의 파일 복구는 이러한 보조 파일이 변경되지 않은 경우에만 가능합니다. 각 백업을 저장하는 테이프가 지워지거나, 제거되거나, 테이프를 덮어쓰면 파일이 자동으로 삭제됩니다.

보조 파일의 위치는 다음과 같습니다.

- Windows XP 및 Server 2003: **%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation**.
- Windows 7 이상 버전의 Windows: **%PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation**.
- Linux: **/var/lib/Acronis/BackupAndRecovery/TapeLocation**.

이러한 보조 파일이 점유하는 공간은 각 백업의 파일 수에 따라 다릅니다. 약 20,000개의 파일이 포함된 디스크의 전체 백업(일반 워크스테이션 디스크 백업)의 경우 보조 파일은 약 150MB를 차지합니다. 250,000개 파일이 포함된 서버의 전체 백업은 약 700MB의 보조 파일을 생성할 수 있습니다. 개별 파일을 복구하지 않으려면 디스크 공간을 확보하기 위해 확인란을 해제 상태로 남겨둘 수 있습니다.

보조 파일이 백업 중에 생성되지 않았거나 삭제된 경우에는 백업이 저장된 테이프를 재스캔하여 생성할 수 있습니다.

각 머신의 백업이 성공할 때마다 슬롯으로 다시 테이프 이동

사전 설정값이 **활성화됨**.

이 옵션을 비활성화하면 테이프를 사용한 작업이 완료된 후 드라이브에 테이프가 남아 있습니다. 그렇지 않으면 소프트웨어가 테이프를 작업 전에 테이프가 있던 슬롯으로 다시 이동합니다. 보호 계획에 따라 백업 후에 다른 작업(예: 백업 유효성 검사 또는 다른 위치에 복제)이 수행되면 해당 작업을 완료한 후 테이프가 다시 해당 슬롯으로 이동됩니다.

이 옵션과 **각 머신의 백업이 성공할 때마다 테이프 꺼내기** 옵션이 모두 활성화되면 테이프가 분리됩니다.

각 머신의 백업이 성공할 때마다 테이프 꺼내기

사전 설정값이 **비활성화됨**.

이 확인란을 선택하면 각 머신의 백업 성공 후 테이프가 분리됩니다. 보호 계획에 따라 백업 후에 다른 작업(예: 백업 유효성 검사 또는 다른 위치에 복제)이 수행되면 해당 작업을 완료한 후 테이프가 분리됩니다.

전체 백업을 생성할 때 독립형 테이프 드라이브에 테이프를 덮어쓰기

사전 설정값이 **비활성화됨**.

이 옵션은 독립형 테이프 드라이브에만 적용됩니다. 이 옵션이 활성화되면 전체 백업이 생성될 때마다 드라이브에 삽입된 테이프를 덮어씁니다.

다음 테이프 장치 및 드라이브 사용

이 옵션을 사용하면 보호 계획에서 사용할 테이프 장치 및 테이프 드라이브를 지정할 수 있습니다.

테이프 풀에는 보호 에이전트가 설치되는 스토리지 노드 또는 머신, 또는 둘 모두가 될 머신에 연결된 모든 테이프 장치의 테이프가 포함됩니다. 백업 위치가 될 테이프 풀을 선택할 때에는 테이프 장치가 연결될 머신을 간접적으로 선택하게 됩니다. 기본적으로 백업은 해당 머신에 연결된 테이프 장치의 테이프 드라이브를 통해 테이프에 작성될 수 있습니다. 일부 장치 또는 드라이브가 누락되었거나 작동하지 않는 경우, 사용 가능한 장치나 드라이브가 보호 계획에서 사용됩니다.

선택한 장치 및 드라이브만을 클릭한 다음 목록에서 테이프 장치 및 드라이브를 선택할 수 있습니다. 전체 장치를 선택하면 모든 드라이브를 선택하게 됩니다. 즉, 해당 드라이브는 모두 보호 계획에 의해 사용될 수 있습니다. 선택한 장치 또는 드라이브가 누락되었거나 작동하지 않고, 다른 장치를 선택하지 않는 경우 백업에 실패합니다.

이 옵션을 사용하여 여러 에이전트가 여러 드라이브를 통해 대규모 테이프 라이브러리로 수행하는 백업을 제어할 수 있습니다. 예를 들어, 여러 에이전트가 동일한 백업 할당 시간 동안 머신을 백업하는 경우에는 에이전트가 모든 드라이브를 점유하기 때문에 대규모 파일 서버 또는 파일 공유의 백업이 시작되지 않을 수 있습니다. 에이전트가 드라이브 2 및 3을 사용하도록 하는 경우 드라이브 1은 공유를 백업하는 에이전트용으로 예약됩니다.

멀티스트리밍

사전 설정값이 **비활성화됨**.

멀티스트리밍을 사용하면 한 에이전트의 데이터를 여러 스트림으로 분할한 후 해당 스트림을 다른 테이프에 동시에 작성할 수 있습니다. 그러면 백업 속도가 더 빨라지므로 에이전트의 처리량이 테이프 드라이브보다 높을 때 특히 유용합니다.

멀티스트리밍 확인란은 **선택한 장치 및 드라이브만** 옵션에서 둘 이상의 테이프 드라이브를 선택한 경우에만 사용할 수 있습니다. 선택한 드라이브 수는 에이전트의 동시 스트림 수와 같습니다. 백업이 시작될 때 선택한 드라이브를 사용할 수 없으면 이 백업이 실패합니다.

멀티스트리밍 백업 또는 멀티스트리밍 백업과 멀티플렉싱 백업을 복구하려면 이 백업을 생성하는 데 사용된 것과 동일한 개수 이상의 드라이브가 필요합니다.

기존 보호 계획에서 멀티스트리밍 패스워드 설정은 변경할 수 없습니다. 다른 설정을 사용하거나 선택한 테이프 드라이브를 변경하려면 새 보호 계획을 생성합니다.

멀티스트리밍은 로컬로 연결된 테이프 드라이브와 스토리지 노드에 연결된 테이프 드라이브 모두에서 사용할 수 있습니다.

멀티플렉싱

사전 설정값이 **비활성화됨**.

멀티플렉싱을 사용하면 여러 에이전트의 데이터 스트림을 단일 테이프에 작성할 수 있습니다. 그러면 빠른 테이프 드라이브를 더욱 효과적으로 활용할 수 있습니다. 기본적으로 멀티플렝싱 요소, 즉 데이터를 단일 테이프로 보내는 에이전트 수는 2로 설정됩니다. 에이전트 수는 10개까지 늘릴 수 있습니다.

멀티플렉싱은 백업 작업이 많은 대규모 환경에 유용합니다. 단일 백업의 성능은 향상되지 않습니다.

대규모 환경에서 가장 빠른 백업을 수행하려면 에이전트, 네트워크 및 테이프 드라이브의 처리량을 분석해야 합니다. 그런 다음, 멀티플렉싱 수를 초과하지 않고 멀티플렉싱 요소를 설정합니다. 예를 들어 에이전트가 70Mbit/s에서 데이터를 제공하고 테이프 드라이브는 250Mbit/s에서 작성하며 네트워크에 병목 현상이 없는 경우 멀티플렉싱 요소를 3으로 설정합니다. 멀티플렉싱 요소가 4이면 멀티플렉싱 초과가 발생하고 백업 성능이 저하됩니다. 일반적으로 멀티플렉싱은 2에서 5 사이입니다.

구조상 멀티플렉스 백업은 복구 속도가 더 느립니다. 멀티플렉싱 요소가 클수록 복고 속도는 느려집니다. 단일 멀티플렉싱 테이프에 작성된 여러 백업의 동시 복구는 지원되지 않습니다.

멀티플렉싱을 위해 특정 테이프 드라이브를 하나 이상 선택하거나, 사용 가능한 테이프 드라이브와 함께 멀티플렉싱 옵션을 사용할 수 있습니다. 멀티플렉싱은 첨부된 테이프 드라이브에 로컬로 사용할 수 없습니다.

기존 보호 계획에서 멀티플렉싱 설정은 변경할 수 없습니다. 다른 설정을 사용하려면 새 보호 계획을 생성해야 합니다.

보호 계획에서는 다음과 같은 멀티스트리밍 및 멀티플렉싱 조합이 가능합니다.

- **멀티스트리밍 및 멀티플렉싱 옵션이 모두 지워집니다.**
  모든 에이전트는 데이터를 단일 테이프 드라이브로 보냅니다.
- **멀티스트리밍 옵션만 선택됩니다.**
  모든 에이전트는 2개 이상의 테이프 드라이브로 데이터를 동시에 보냅니다.
- **멀티플렉싱 옵션만 선택됩니다.**
  모든 에이전트는 여러 에이전트의 스트림을 동시에 허용하는 테이프 드라이브로 데이터를 보냅니다. 테이프 드라이브가 허용할 수 있는 최대 스트림 수는 보호 계획에 설정되어 있으며 이를 즉시 변경할 수는 없습니다.

- **멀티스트리밍 및 멀티플렉싱 옵션은 모두 선택됩니다.**
  모든 에이전트는 여러 에이전트의 스트림을 동시에 허용하는 2개 이상의 테이프 드라이브로 데이터를 보냅니다.

테이프 드라이브는 먼저 시작한 보호 계획에 따라 멀티플렉싱 또는 멀티플렉싱이 아닌 한 가지 유형의 백업만 한 번에 작성할 수 있습니다.

백업용으로 선택한 테이프 풀 내에 테이프 세트 사용

사전 설정값이 **비활성화됨**.

하나의 풀 내에 있는 테이프는 **테이프 세트**로 그룹화될 수 있습니다.

이 옵션을 비활성 상태로 유지하면 데이터가 풀에 속하는 모든 테이프에서 백업됩니다. 옵션이 활성화된 경우 미리 정의된 규칙이나 사용자 정의 규칙에 따라 백업을 분리할 수 있습니다.

- **각각에 별도의 테이프 세트 사용**(규칙 선택: **백업 유형**, **장치 유형**, **장치 이름**, **날짜**, **요일**, **월**, **년**, **날짜**)
  이 변형이 선택되면 미리 정의된 규칙에 따라 테이프 세트를 구성할 수 있습니다. 예를 들어 각 요일에 대한 개별 테이프 세트가 있거나 개별 테이프 세트에 각 머신의 백업을 저장할 수 있습니다.
- **테이프 세트에 대한 사용자 정의 규칙 지정**
  이 변형이 선택되면 테이프 세트를 구성하는 자체 규칙을 지정합니다. 규칙에는 다음 변수가 포함됩니다.

변수 구문	변수 설명	사용 가능한 값
[Resource Name]	각 머신의 백업이 개별 테이프 세트에 저장됩니다.	관리 서버에 등록된 머신의 이름.
[Backup Type]	전체, 증분 및 차등 백업이 개별 테이프 세트에 저장됩니다.	full, inc, diff
[Resource Type]	각 유형의 머신 백업이 개별 테이프 세트에 저장됩니다.	Server essentials, Server, Workstation, Physical machine, VMware Virtual Machine, Virtual-PC Virtual Machine, Virtual Server Virtual Machine, Hyper-V Virtual Machine, Parallels Virtual Machine, XEN Virtual Machine, KVM Virtual Machine, RHEV Virtual Machine, Parallels Cloud Virtual Machine
[Day]	해당 월의 각 날짜에 생성된 백업이 개별 테이프 세트에 저장됩니다.	01, 02, 03, ..., 31
[Weekday]	각 요일에 생성된 백업이 개별 테	Sunday, Monday, Tuesday, Wednesday,

	이프 세트에 저장됩니다.	Thursday, Friday, Saturday
[Month]	해당 연도의 각 달에 생성된 백업이 개별 테이프 세트에 저장됩니다.	January, February, March, April, May, June, July, August, September, October, November, December
[Year]	각 연도에 생성된 백업이 개별 테이프 세트에 저장됩니다.	2017, 2018, ...

- 예를 들어 규칙을 [Resource Name]-[Backup Type]으로 지정하면 보호 계획이 적용되는 각 머신의 각 전체, 증분 및 차등 백업에 대해 개별 테이프 세트를 사용합니다.

개별 테이프에 대한 테이프 세트를 지정할 수도 있습니다. 이 경우 소프트웨어에서는 테이프 세트 값이 보호 계획에 지정된 식의 값과 일치하는 테이프에 백업을 기록합니다. 그런 다음 필요한 경우 같은 풀의 다른 테이프를 사용합니다. 이후 풀이 갱신 가능한 경우 **사용 가능 테이프** 풀의 테이프가 사용됩니다.

예를 들어 테이프 1에 대해 테이프 세트 Monday를 지정하고, 테이프 2에 대해 Tuesday를 지정하고, 백업 옵션에서 [Weekday]를 지정하면 각 요일에 해당하는 테이프가 사용됩니다.

작업 실패 처리

이 옵션은 예약된 보호 계획 실행에 실패한 경우의 프로그램 동작을 결정합니다. 이 옵션은 보호 계획을 수동으로 시작할 때에는 적용되지 않습니다.

이 옵션이 활성화되어 있는 경우 프로그램이 보호 계획을 다시 실행하려고 시도합니다. 시도 횟수와 시도 간 시간 간격을 지정할 수 있습니다. 시도가 성공적으로 완료되거나 성공하기 전에 지정된 시도 횟수를 모두 수행하고 나면 프로그램이 시도를 중지합니다.

사전 설정값이 **비활성화됨**.

작업 시작 조건

이 옵션은 Windows 및 Linux 운영 체제에서 유효합니다.

이 옵션은 작업이 시작하려고 하지만(스케줄된 시간이 되었거나 스케줄에 지정된 이벤트가 발생함) 조건(여러 개의 조건 중 하나라도)이 맞지 않는 경우 프로그램의 동작을 결정합니다. 조건에 대한 자세한 내용은 "시작 조건"을 참조하십시오.

사전 설정값이 **스케줄의 조건이 충족될 때까지 대기합니다.**

스케줄의 조건이 충족될 때까지 대기

이 설정을 사용하면 스케줄러는 조건 모니터링을 시작하고 조건이 충족되자마자 작업을 시작합니다. 조건이 절대 충족되지 않는 경우에는 작업이 시작되지 않습니다.

조건이 너무 오랫 동안 충족되지 않고 작업을 더 지연하면 위험하게 되는 상황을 처리하기 위해서는 조건과 관계 없이 작업을 실행하게 할 시간 간격을 설정할 수 있습니다. **다음 시간 후에는 무조건 작업 실행** 확인란을 선택하고 시간 간격을 지정합니다. 작업은 조건 충족 또는 최대 시간 지연 경과 중 하나가 먼저 발생하자마자 즉시 시작됩니다.

작업 실행 건너뛰기

작업을 지연하는 것이 적합하지 않을 수도 있습니다. 예를 들어, 작업을 지정된 시간에 정확하게 실행해야 하는 경우가 있습니다. 특히 작업이 비교적 자주 발생하는 경우에는 조건이 충족되기를 기다리는 대신 작업을 건너뛰는 것이 좋습니다.

VSS(Volume Shadow Copy Service)

이 옵션은 Windows 운영체제에 대해서만 유효합니다.

이 옵션은 VSS(Volume Shadow Copy Service) 제공자가 VSS 인식 애플리케이션에 백업을 곧 시작한다고 알려야 하는지 정의합니다. 이를 통해 애플리케이션이 사용하는 모든 데이터의 상태를 일관되게 유지할 수 있고, 특히 백업 소프트웨어가 데이터 스냅샷을 생성하는 순간에 모든 데이터베이스 트랜잭션이 완료되어 있도록 할 수 있습니다. 데이터 일관성은 또한 애플리케이션이 올바른 상태로 복구되고 복구 후 즉시 작동이 가능하도록 해줍니다.

사전 설정값이 **활성화됨. 자동으로 스냅샷 공급자 선택**입니다.

다음 중 하나를 선택합니다.

- **자동으로 스냅샷 공급자 선택**
  하드웨어 스냅샷 공급자, 소프트웨어 스냅샷 공급자 및 Microsoft Software Shadow Copy Provider 중에서 자동으로 선택합니다.
- **Microsoft Software Shadow Copy Provider 사용**
  애플리케이션 서버(Microsoft Exchange Server, Microsoft SQL Server, Microsoft SharePoint 또는 Active Directory) 백업 시 이 옵션을 선택하는 것이 좋습니다.

데이터베이스가 VSS와 호환되지 않으면 이 옵션을 비활성화하십시오. 스냅샷이 보다 빠르게 생성되지만 스냅샷 생성 시 트랜잭션이 완료되지 않은 애플리케이션의 경우에는 데이터 일관성이 보장되지 않습니다. 데이터 캡처 전/후 명령을 사용하여 데이터가 일관된 상태로 백업되도록 할 수 있습니다. 예를 들어, 데이터베이스를 일시 중단하고 모든 캐시를 플러시하는 데이터 캡처 전 명령을 지정하여 모든 트랜잭션이 완료되도록 할 수 있고, 스냅샷 생성 후 데이터베이스 작업을 다시 시작하도록 하는 데이터 캡처 후 명령을 지정할 수 있습니다.

참고
이 옵션이 활성화되면 **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToSnapshot** 레지스트리 키에 지정된 파일과 폴더가 백업되지 않습니다. 특히 오프라인 Outlook 데이터 파일(.ost)은 이 키의 **OutlookOST** 값에 지정되므로 백업되지 않습니다.

VSS 전체 백업 활성화

이 옵션이 활성화된 경우, 각각의 성공적인 전체, 증분 또는 차등 디스크 수준 백업 후에 Microsoft Exchange Server 및 다른 VSS 인식 애플리케이션의 로그(Microsoft SQL Server 제외)가 잘립니다.

사전 설정값이 **비활성화됨**입니다.

다음과 같은 경우 이 옵션을 비활성화 상태로 두십시오.

- Agent for Exchange 또는 서드 파티 소프트웨어를 사용하여 Exchange Server 데이터를 백업하는 경우. 이 경우 로그 잘림이 연속 트랜잭션 로그 백업을 방해하기 때문입니다.
- 서드 파티 소프트웨어를 사용하여 SQL Server 데이터를 백업하는 경우. 이 경우에는 서드 파티 소프트웨어가 "자체" 전체 백업을 위해 생성된 디스크 수준 백업을 가져가기 때문입니다. 결국, SQL Server 데이터의 다음 번 차등 백업은 실패합니다. 백업은 서드 파티 소프트웨어가 다음 번 "자체" 전체 백업을 생성할 때까지 계속 실패합니다.
- 다른 VSS 인식 애플리케이션이 머신에서 실행 중이고 어떤 이유로 해당 로그를 유지해야 하는 경우.

이 옵션을 활성화하면 Microsoft SQL Server 로그가 잘리지 않습니다. 백업 후 SQL Server 로그를 자르려면 로그 자르기 백업 옵션을 활성화하십시오.

가상 머신용 VSS(Volume Shadow Copy Service)

이 옵션은 가상 머신의 정지 스냅샷을 생성할지 정의합니다. 정지 스냅샷을 생성하기 위해 백업 소프트웨어가 VMware Tools 또는 Hyper-V Integration Services를 사용해 가상 머신 내에서 VSS를 적용합니다.

사전 설정값이 **활성화됨**.

이 옵션이 활성화되어 있으면 가상 머신에서 실행 중인 모든 VSS 인식 애플리케이션의 트랜잭션이 스냅샷 생성 이전에 완료됩니다. "오류 처리" 옵션에 지정된 재시도 횟수 후에도 정지 스냅샷 생성에 실패했고, 애플리케이션 백업이 비활성화되어 있는 경우에는 비정지 스냅샷이 생성됩니다. 애플리케이션 백업이 활성화되어 있는 경우 백업이 실패합니다.

이 옵션이 비활성화되어 있는 경우 비정지 스냅샷이 생성됩니다. 가상 머신이 크래시 일관성 상태에서 백업됩니다. VSS 인식 애플리케이션을 실행하지 않는 가상 머신에 대해서도 이 옵션을 항상 활성화한 상태로 유지하는 것이 좋습니다. 그렇지 않을 경우 캡처한 백업 내부에서 파일 시스템 일관성을 보증할 수 없습니다.

참고
이 옵션은 Scale Computing HC3 가상 머신에는 영향을 주지 않습니다. 이 경우 정지는 Scale 도구가 가상 머신에 설치되었는지 여부에 따라 다릅니다.

주간 백업

이 옵션은 보관 규칙 및 백업 구성표에서 어떤 백업을 "주간"으로 고려할지 결정합니다. "주간" 백업은 한 주가 시작된 후 생성된 첫 번째 백업입니다.

사전 설정값이 **월요일**입니다.

Windows 이벤트 로그

이 옵션은 Windows 운영 체제에서만 유효합니다.

이 옵션은 에이전트가 Windows의 애플리케이션 이벤트 로그에 백업 작업의 이벤트를 기록해야 하는지 정의합니다(이 로그를 보려면 eventvwr.exe를 실행하거나 **제어판** > **관리 도구** > **이벤트 뷰어** 선택). 기록할 이벤트를 필터링할 수 있습니다.

사전 설정값이 **비활성화됨**.

복구

복구 치트 시트

다음 표는 사용 가능한 복구 방법을 요약해서 보여줍니다. 이 표를 사용하여 필요에 가장 잘 맞는 복구 방법을 선택할 수 있습니다.

복구 대상	복구 방법
실제 머신(Windows 또는 Linux)	웹 인터페이스 사용 부트 가능한 미디어 사용
실제 머신(Mac)	부트 가능한 미디어 사용
가상 머신(VMware, Hyper-V 또는 Scale Computing HC3)	웹 인터페이스 사용 부트 가능한 미디어 사용
ESXi 구성	부트 가능한 미디어 사용
파일/폴더	웹 인터페이스 사용 클라우드 스토리지에서 파일 다운로드 부트 가능한 미디어 사용 로컬 백업에서 파일 추출
시스템 상태	웹 인터페이스 사용
SQL 데이터베이스	웹 인터페이스 사용
Exchange 데이터베이스	웹 인터페이스 사용
Exchange 사서함	웹 인터페이스 사용
Microsoft 365 사서함	웹 인터페이스 사용
Oracle 데이터베이스	Oracle Explorer 도구 사용

Mac 사용자 참고 사항

- 10.11 El Capitan으로 시작하는 특정 시스템 파일, 폴더 및 프로세스는 확장된 파일 속성 com.apple.rootless를 사용하여 보호하기 위해 플래그가 지정되어 있습니다.이 기능은 SIP(시스템 무결성 보호)라고 합니다. 보호된 파일에는 사전 설치된 애플리케이션 및 /system, /bin, /sbin, /usr의 대부분의 폴더가 포함되어 있습니다.

  보호된 파일 및 폴더는 운영 체제에서 복구되는 동안 덮어쓸 수 없습니다. 보호된 파일을 덮어써야 하는 경우 부트 가능한 미디어에서 복구를 수행합니다.
- macOS Sierra 10.12부터 자주 사용하지 않는 파일은 클라우드의 저장 기능을 통해 iCloud로 이동될 수 있습니다.이러한 파일의 작은 풋프린트가 파일 시스템에 유지됩니다. 원래 파일 대신 이러한 풋프린트가 백업됩니다.

원래 위치로 폿프린트를 복구하면 iCloud와 동기화하여 원래 파일을 사용할 수 있게 됩니다. 다른 위치로 폿프린트를 복구하면 동기화될 수 없고 원래 파일을 사용할 수 없습니다.

안전 복구

운영 체제의 백업된 이미지는 맬웨어에 감염될 수 있으며 이를 복구하는 머신을 재감염시킬 수 있습니다.

안전 복구 기능은 통합된 맬웨어 방지 스캔 및 맬웨어 삭제를 사용해 복구 프로세스 중 감염이 되풀이되지 않도록 방지합니다.

제한:

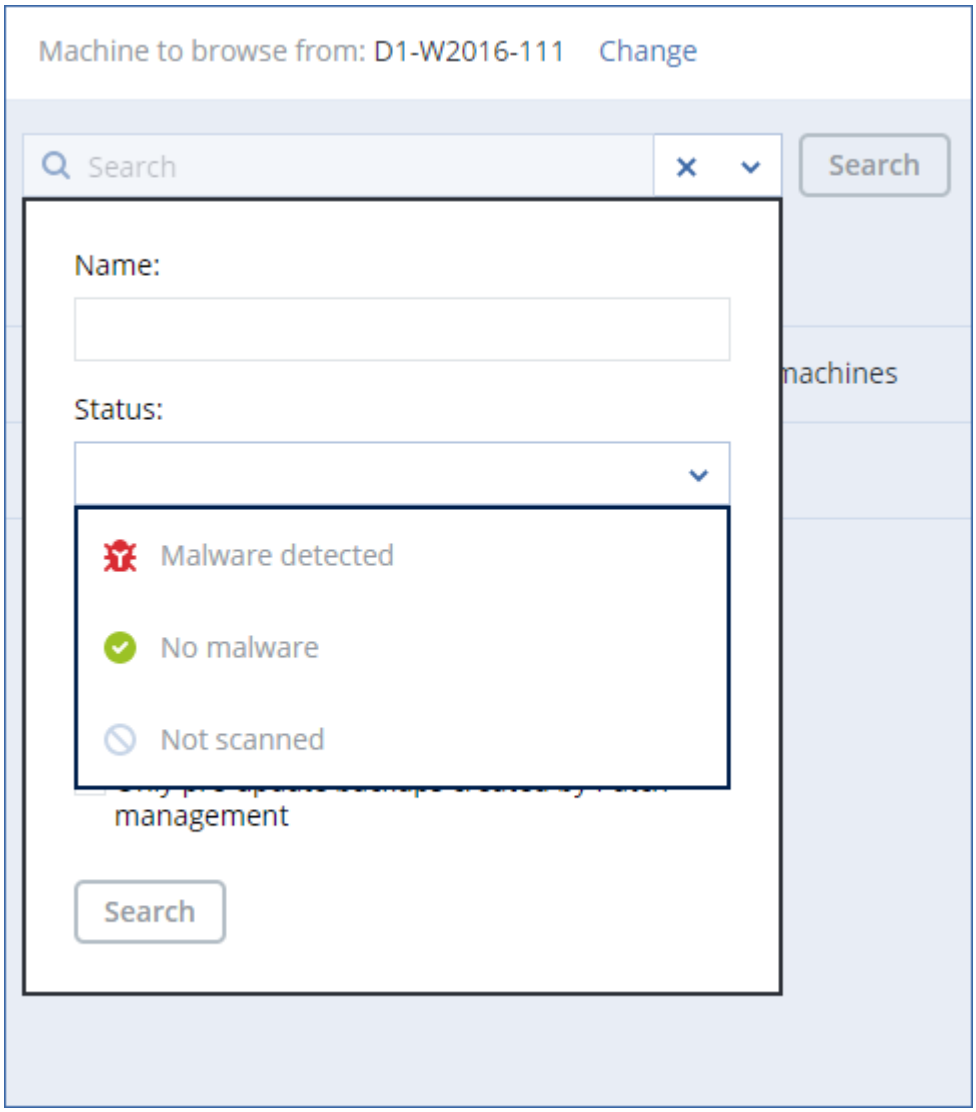
- 안전 복구는 Agent for Windows가 설치된 물리 또는 가상 Windows 머신에 대해서만 지원됩니다.
- **전체 머신** 또는 **디스크/볼륨** 백업 유형만 지원됩니다.
- NTFS 파일 시스템이 있는 볼륨만 지원됩니다. NTFS가 아닌 파티션은 맬웨어에 대한 스캔 없이 복구됩니다.
- CDP(지속적인 데이터 보호) 백업의 경우 안전 복구가 지원되지 않습니다. 머신은 CDP 백업의 데이터 없이 마지막 정규 백업을 기반으로 복구됩니다. CDP 데이터를 복구하려면 **파일/폴더** 복구를 실행하십시오.

작동법

복구 프로세스에서 안전 복구 옵션을 활성화한 경우 시스템은 다음을 수행합니다.

1. 이미지 백업을 스캔해 맬웨어를 찾고 감염된 파일을 표시합니다. 백업에는 다음과 같은 상태가 할당됩니다.
   - **맬웨어 없음** – 백업 스캔 중 발견된 맬웨어가 없습니다.
   - **맬웨어 감지됨** – 백업 스캔 중 맬웨어가 발견되었습니다.
   - **스캔되지 않음** – 백업이 맬웨어에 대해 스캔되지 않았습니다.
2. 선택한 머신에 백업을 복구합니다.
3. 감지된 맬웨어를 삭제합니다.

상태 매개변수를 사용해 백업을 필터링할 수 있습니다.



부트 가능한 미디어 생성

부트 가능한 미디어에는 운영 체제의 도움 없이 에이전트를 실행할 수 있는 CD, DVD, USB 플래시 드라이브 또는 기타 이동식 미디어가 있습니다. 부트 가능한 미디어의 주요 용도는 시작할 수 없는 운영 체제를 복구하는 것입니다.

디스크 수준 백업을 사용하기 시작하면 즉시 부트 가능한 미디어를 생성하여 테스트하는 것이 매우 좋습니다. 또한 보호 에이전트의 주요 업데이트 후에는 항상 부트 가능한 미디어를 다시 생성하는 것이 좋습니다.

동일한 미디어를 사용하여 Windows 또는 Linux를 복구할 수 있습니다. macOS를 복구하려면 macOS를 실행 중인 머신에서 별도의 미디어를 생성합니다.

Windows 또는 Linux에서 부트 가능한 미디어를 생성하려면

1. 부트 가능한 미디어 ISO 파일을 다운로드합니다. 파일을 다운로드하려면 오른쪽 위에 있는 계정 아이콘을 클릭하고 **다운로드** > **부트 가능한 미디어**를 클릭합니다.
2. 다음 중 하나를 수행하십시오.

- ISO 파일을 사용하여 CD/DVD를 굽습니다.
- ISO 파일 및 온라인에서 사용 가능한 무료 도구 중 하나를 사용하여 부트 가능한 USB 플래시 드라이브를 생성합니다.

  UEFI 머신을 부트하려는 경우에는 `ISO-USB` 또는 `RUFUS`를 사용하고 BIOS 머신의 경우에는 `Win32DiskImager`를 사용합니다. Linux에서는 `dd` 유틸리티를 사용합니다.
- ISO 파일을 CD/DVD 드라이브로 복구하려는 가상 머신에 연결합니다.

또는 부트 가능한 미디어 제작기를 사용하여 부트 가능한 미디어를 생성할 수 있습니다.

macOS에서 부트 가능한 미디어를 만들려면

1. Agent for Mac이 설치되어 있는 머신에서 **애플리케이션** > **복구 미디어 제작기**를 클릭합니다.
2. 연결된 이동식 미디어가 표시됩니다. 부트 가능하도록 만들 미디어를 하나 선택합니다.

   경고!
   디스크에 있는 모든 데이터가 지워집니다.
3. **생성**을 클릭합니다.
4. 부트 가능한 미디어가 생성되는 동안 기다립니다.

머신 복구

실제 머신 복구

이 섹션에서는 Cyber Protect 웹 콘솔을 사용하여 실제 머신을 복구하는 방법을 설명합니다.

다음 항목을 복구해야 하는 경우에는 Cyber Protect 웹 콘솔 대신 부트 가능한 미디어를 사용하십시오.

- macOS 운영 체제
- 베어 메탈 또는 오프라인 머신으로 임의의 운영 체제 복구
- 논리 볼륨의 구조(Linux에서는 논리 볼륨 관리자가 생성한 볼륨). 미디어를 사용하여 논리 볼륨 구조를 자동으로 재생성할 수 있습니다.

운영 체제 복구 및 BitLocker 또는 CheckPoint로 암호화된 볼륨 복구 시에는 머신을 다시 시작해야 합니다. 자세한 내용은 "복구 및 다시 시작"(293페이지) 항목을 참조하십시오.

실제 머신을 복구하려면

1. 백업된 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

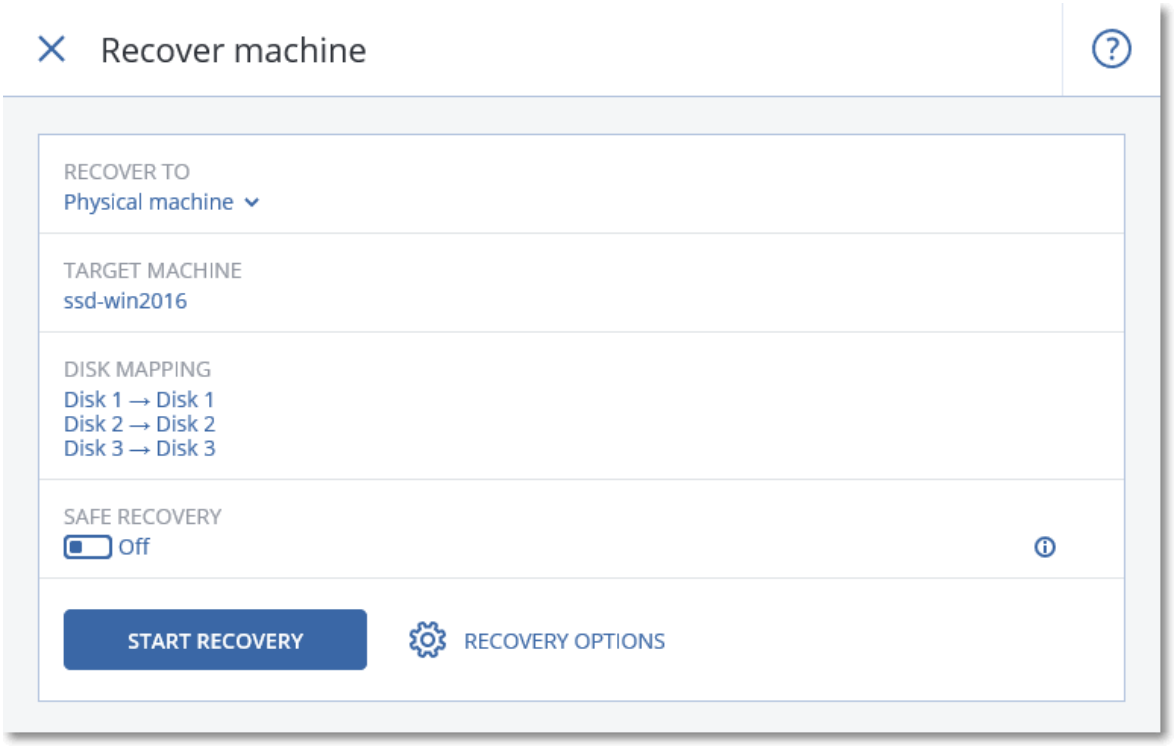
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.

- 백업 스토리지 탭에서 복구 지점을 선택합니다.
- "부트 가능한 미디어를 사용하여 디스크 복구"에서 설명하는 대로 머신을 복구합니다.

4. **복구** > **전체 머신**을 클릭합니다.

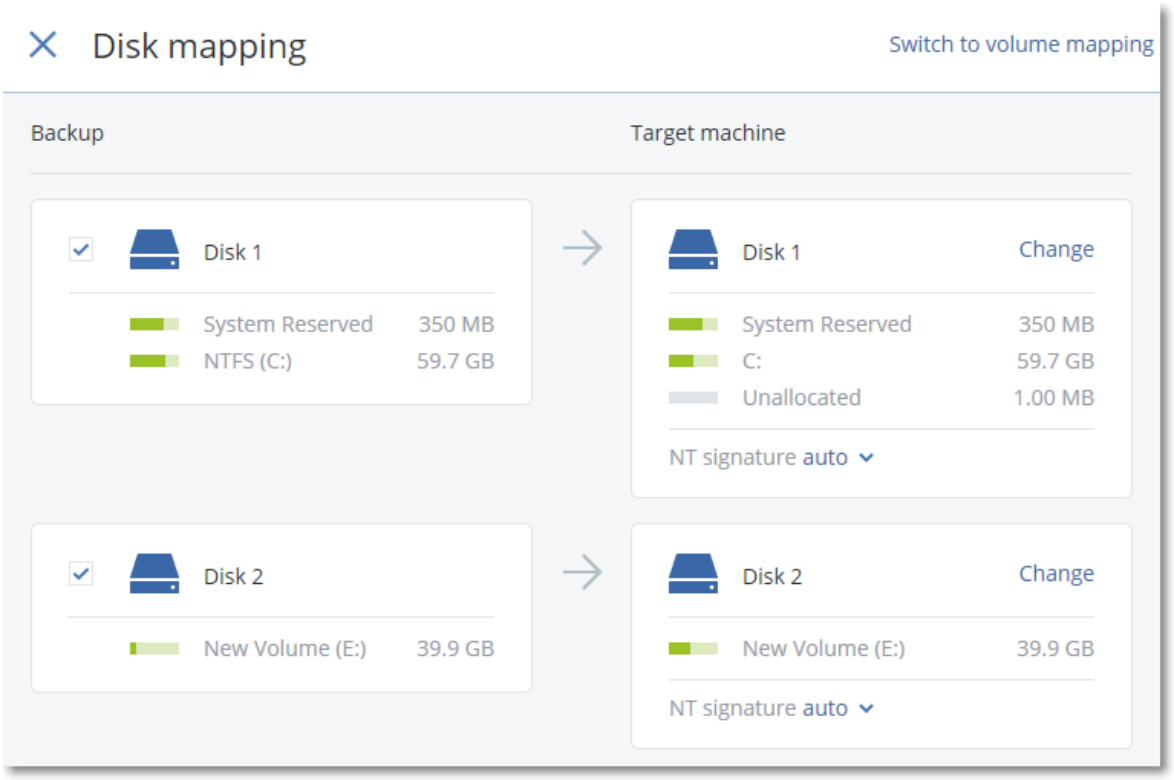
   소프트웨어가 디스크를 백업에서 대상 머신의 디스크로 자동으로 매핑합니다.

   다른 실제 머신으로 복구하려면 **대상 머신**을 클릭한 다음 온라인 상태인 대상 머신을 선택합니다.



5. 매핑 결과가 만족스럽지 않거나 디스크 매핑이 실패할 경우 **디스크 매핑**을 클릭하여 디스크를 수동으로 다시 매핑합니다.

   또한 매핑 섹션에서 복구용 개별 디스크나 볼륨을 선택할 수 있습니다. 오른쪽 위에 있는 **전환...** 링크를 사용하여 디스크 복구와 볼륨 복구 간에 전환할 수 있습니다.



6. [선택 사항] **안전 복구** 스위치를 활성화해 백업에 맬웨어가 있는지 스캔합니다. 맬웨어가 감지되면 백업에 표시되며, 복구 프로세스가 끝난 직후 삭제됩니다.
7. **복구 시작**을 클릭합니다.
8. 백업된 버전으로 디스크를 덮어 쓰려는지 확인합니다. 머신을 자동으로 다시 시작할지 여부를 선택합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

가상 머신에 실제 머신 복구

실제 머신의 백업을 가상 머신에 복구할 수 있습니다.

관련 대상 하이퍼바이저용 에이전트가 환경에 하나 이상 설치되어 있으며 관리 서버에 등록되어 있으면 가상 머신으로의 복구를 수행할 수 있습니다. 예를 들어 VMware ESXi로 복구하려면 Agent for VMware가 환경에 설치되어 있으며 관리 서버에 등록되어 있어야 합니다.

클라우드 디플로이에서만 사용 가능한 옵션도 있습니다.

실제 머신 및 가상 머신 간 마이그레이션(P2V)에 지원되는 경로에 대한 자세한 내용은 "머신 이주" (465페이지) 항목을 참조하십시오.

참고
macOS 실제 머신 백업은 가상 머신으로 복구할 수 없습니다.

실제 머신을 가상 머신처럼 복구하려면

1. 백업된 머신을 선택합니다.
2. **복구**를 클릭합니다.

3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 해당 위치에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
   - "부트 가능한 미디어를 사용하여 디스크 및 볼륨 복구"(294페이지)에 설명된 대로 머신을 복구합니다.
4. **복구** > **전체 머신**을 클릭합니다.
5. **복구 대상**에서 **가상 머신**을 선택합니다.
6. **대상 머신**을 클릭합니다.
   a. 하이퍼바이저를 선택합니다.

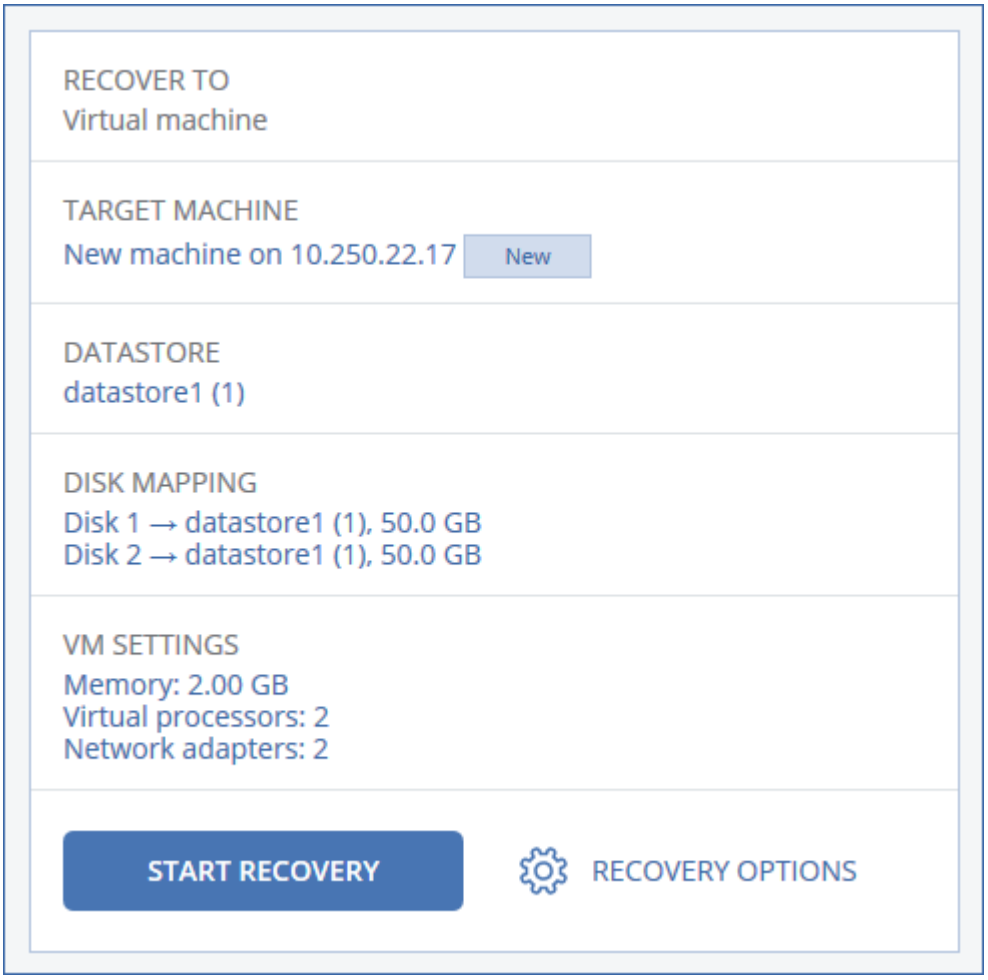
      참고
      해당 하이퍼바이저용 에이전트가 하나 이상 환경에 설치되어 있고 관리 서버에 등록되어 있어야 합니다.

   b. 새 머신 또는 기존 머신으로 복구할지 선택합니다. 새 머신 옵션을 사용하는 것이 좋습니다. 이 옵션을 사용하는 경우 대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치하지 않아도 되기 때문입니다.
   c. 호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.
   d. **확인**을 클릭합니다.
7. [Virtuozzo Hybrid Infrastructure의 경우] **VM 설정**을 클릭하고 **선호 방식**을 선택합니다. 필요한 경우 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경할 수 있습니다.
8. [선택 사항] [새 머신으로 복구하는 경우] 필요한 추가 복구 옵션을 구성합니다.
   - [Virtuozzo Hybrid Infrastructure 및 Scale Computing HC3에서는 사용 불가] 가상 머신의 데이터 저장소를 선택하려면, ESXi의 경우 **데이터 저장소**를, Hyper-V 및 Virtuozzo의 경우 **경로**를, Red Hat Virtualization(oVirt)의 경우에는 **스토리지 도메인**을 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
   - 각 가상 디스크용 데이터 저장소(스토리지), 인터페이스 및 프로비저닝 모드를 선택하려면 **디스크 매핑**을 클릭합니다. 매핑 섹션에서 복구용 개별 디스크를 선택할 수 있습니다.

     참고
     Virtuozzo 컨테이너 또는 Virtuozzo Hybrid Infrastructure 가상 머신을 복구하는 경우에는 이러한 설정을 변경할 수 없습니다. Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 **변경**을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 **완료**를 클릭합니다.

   - [VMware ESXi, Hyper-V, Virtuozzo 및 Red Hat Virtualization/oVirt에 사용 가능] 가상 머신의 메

모리 크기, 프로세서 수 및 네트워크 연결을 변경하려면 **VM 설정**을 클릭합니다.



9. **복구 시작**을 클릭합니다.
10. [기존 가상 머신에 복구하는 경우] 디스크를 덮어쓸 것임을 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

가상 머신 복구

가상 머신의 백업을 실제 머신이나 다른 가상 머신에 복구할 수 있습니다.

관련 대상 하이퍼바이저용 에이전트가 환경에 하나 이상 설치되어 있으며 관리 서버에 등록되어 있으면 가상 머신으로의 복구를 수행할 수 있습니다. 예를 들어 VMware ESXi로 복구하려면 Agent for VMware가 환경에 설치되어 있으며 관리 서버에 등록되어 있어야 합니다.

클라우드 디플로이에서만 사용 가능한 옵션도 있습니다.

가상 머신 및 실제 머신 간 마이그레이션(V2P) 및 가상 머신 간 마이그레이션(V2V)에 지원되는 경로에 대한 자세한 내용은 "머신 이주"(465페이지) 항목을 참조하십시오.

참고
Hyper-V는 macOS를 지원하지 않으므로 macOS 가상 머신을 Hyper-V 호스트에 복구할 수는 없습니다. macOS 가상 머신은 Mac 하드웨어에 설치된 VMware 호스트에 복구할 수 있습니다.

중요
다른 머신을 이 머신에 복구할 때는 가상 머신을 중지해야 합니다. 기본적으로 소프트웨어는 메시지를 표시하지 않고 머신을 중지합니다. 복구가 완료되면 머신을 수동으로 시작해야 합니다. VM 전원 관리 복구 옵션(**복구 옵션** > **VM 전원 관리** 클릭)을 사용하여 기본 동작을 변경할 수 있습니다.

가상 머신을 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 백업된 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
2. **복구** > **전체 머신**을 클릭합니다.
3. [실제 머신에 복구하는 경우] **복구 대상**에서 **실제 머신**을 선택합니다.
   대상 머신의 디스크 구성이 백업의 디스크 구성과 정확하게 일치하는 경우에만 실제 머신으로 복구가 가능합니다. 이 경우 "실제 머신 복구"(287페이지)의 4단계로 계속 진행합니다. 그렇지 않은 경우에는 부트 가능한 미디어를 사용하여 가상 머신 및 실제 머신 간 마이그레이션(V2P)을 수행하는 것이 좋습니다.
4. [선택 사항] 기본적으로는 원래 머신이 대상 머신으로 선택됩니다. 다른 가상 머신으로 복구하려면 **대상 머신**을 클릭한 후 다음을 수행합니다.
   a. 하이퍼바이저를 선택합니다.

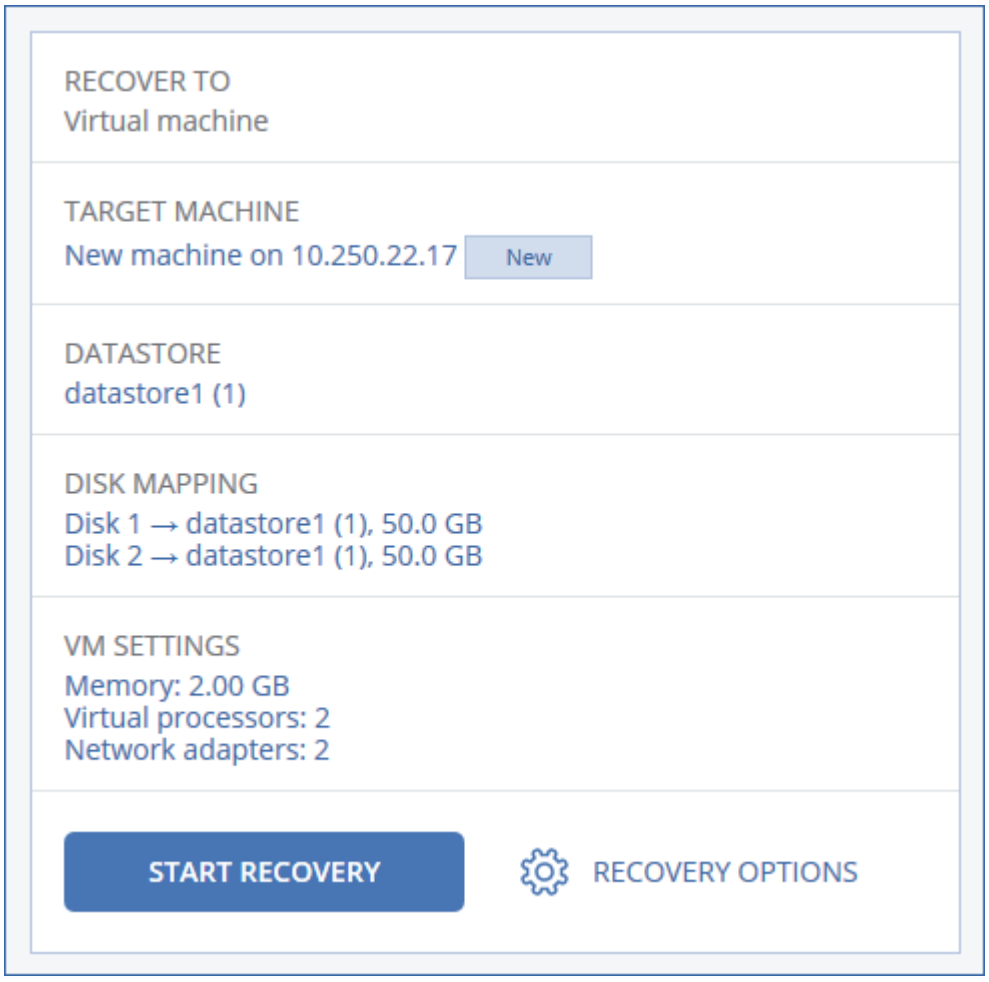
      참고
      해당 하이퍼바이저용 에이전트가 하나 이상 환경에 설치되어 있고 관리 서버에 등록되어 있어야 합니다.

   b. 새 머신 또는 기존 머신으로 복구할지 선택합니다.
   c. 호스트를 선택하고 새 머신 이름을 지정하거나 기존 대상 머신을 선택합니다.
   d. **확인**을 클릭합니다.
5. [Virtuozzo Hybrid Infrastructure의 경우] **VM 설정**을 클릭하고 **선호 방식**을 선택합니다. 필요한 경우 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경할 수 있습니다.
6. [선택 사항] [새 머신으로 복구하는 경우] 필요한 추가 복구 옵션을 구성합니다.
   - [Virtuozzo Hybrid Infrastructure 및 Scale Computing HC3에서는 사용 불가] 가상 머신의 데이터 저장소를 선택하려면, ESXi의 경우 **데이터 저장소**를, Hyper-V 및 Virtuozzo의 경우 **경로**를, Red Hat Virtualization(oVirt)의 경우에는 **스토리지 도메인**을 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
   - 각 가상 디스크용 데이터 저장소(스토리지), 인터페이스 및 프로비저닝 모드를 선택하려면 **디스크 매핑**을 클릭합니다. 매핑 섹션에서 복구용 개별 디스크를 선택할 수 있습니다.

참고

Virtuozzo 컨테이너 또는 Virtuozzo Hybrid Infrastructure 가상 머신을 복구하는 경우에는 이러한 설정을 변경할 수 없습니다. Virtuozzo Hybrid Infrastructure의 경우, 대상 디스크의 스토리지 정책만 선택할 수 있습니다. 이 작업을 수행하려면 대상 디스크를 선택하고 **변경**을 클릭합니다. 날개가 열리면 기어 아이콘을 클릭하고 **완료**를 클릭합니다.

- [VMware ESXi, Hyper-V, Virtuozzo 및 Red Hat Virtualization/oVirt에 사용 가능] 가상 머신의 메모리 크기, 프로세서 수 및 네트워크 연결을 변경하려면 **VM 설정**을 클릭합니다.



7. **복구 시작**을 클릭합니다.
8. [기존 가상 머신에 복구하는 경우] 디스크를 덮어쓸 것임을 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

복구 및 다시 시작

다음 항목을 복구할 때는 머신을 다시 시작해야 합니다.

- 운영 체제
- BitLocker 또는 CheckPoint로 암호화된 볼륨

중요
백업된 암호화 볼륨은 암호화되지 않은 볼륨으로 복구됩니다.

요구 사항

- 암호화된 볼륨을 복구하려면 같은 머신에 암호화되지 않은 볼륨이 있어야 하며, 해당 볼륨의 여유 공간이 1GB 이상이어야 합니다. 그렇지 않으면 복구가 실패합니다.
- 암호화된 시스템 볼륨을 복구할 때는 추가 작업을 수행할 필요가 없습니다. 암호화된 비시스템 볼륨을 복구하려면 먼저 해당 볼륨에 있는 파일을 여는 등의 방식으로 볼륨을 잠가야 합니다. 이렇게 하지 않으면 머신을 다시 시작하지 않고 복구가 계속 진행되므로 Windows에서 복구된 볼륨을 인식하지 못할 수도 있습니다.

문제 해결

복구가 실패하고 머신이 다시 시작된 후 파티션에서 파일을 가져올 수 없음 오류가 발생하면 보안 부팅을 비활성화하십시오. 이 작업을 수행하는 방법을 자세히 알아보려면 Microsoft 설명서에서 보안 부팅 비활성화를 참조하십시오.

부트 가능한 미디어를 사용하여 디스크 및 볼륨 복구

부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "부트 가능한 미디어 생성"(286페이지)을(를) 참조하십시오.

부트 가능한 미디어를 사용하여 디스크 또는 볼륨을 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. [macOS만 해당] APFS 형식의 볼륨을 원본 이외 머신 또는 베어 메탈로 복구하는 경우 원본 디스크 구성을 수동으로 재생성합니다.
   a. **디스크 유틸리티**를 클릭합니다.
   b. 원본 디스크 구성을 재생성합니다. 자세한 내용은 https://support.apple.com/guide/disk-utility/welcome을 참조하십시오.
   c. **디스크 유틸리티** > **디스크 유틸리티 종료**를 클릭합니다.

   참고
   macOS 11 Big Sur부터는 시스템 볼륨을 백업 및 복구할 수 없습니다. 부트 가능한 macOS 시스템을 복구하려면 데이터 볼륨을 복구 한 후 여기에 macOS를 설치해야 합니다.

3. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
4. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소 및 포트를 지정합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
5. 시작 화면에서 **복구**를 클릭합니다.
6. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.

7. 백업 위치 지정:
   - 클라우드 스토리지에서 복구하려면 **클라우드 스토리지**를 선택합니다. 백업된 머신이 할당된 계정의 자격 증명을 입력합니다.
   - 로컬 또는 네트워크 폴더에서 복구하려면 **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.

   확인을 클릭하여 선택 항목을 확인합니다.
8. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
9. **백업 내용**에서 **디스크** 또는 **볼륨**을 선택하고 복구하려는 항목을 선택합니다. **확인**을 클릭하여 선택 항목을 확인합니다.

   중요
   백업한 머신에 동적 디스크 또는 LVM(논리 볼륨)이 있으면 **볼륨**을 선택합니다.
10. **복구 위치**에서 선택한 디스크가 대상 디스크로 자동으로 매핑됩니다.
    매칭에 실패하거나 매핑 결과가 만족스럽지 않은 경우 디스크를 수동으로 다시 매핑할 수 있습니다.

    참고
    디스크 레이아웃을 변경하면 운영 체제 부트 가능성에 영향을 줄 수 있습니다. 확신이 없는 경우 원래 머신의 디스크 레이아웃을 사용하십시오.
11. [macOS만 해당] APFS 형식의 데이터 볼륨을 부트 가능한 macOS 시스템으로 복구하려면 **macOS 설치 섹션**에서 **복구된 macOS 데이터 볼륨에 macOS 설치** 확인란을 선택한 상태로 유지합니다.
    복구 후 시스템이 재부팅되고 macOS 설치가 자동으로 시작됩니다. 인스톨러를 통해 필요한 파일을 다운로드하려면 인터넷이 연결되어 있어야 합니다.
    APFS 형식의 데이터 볼륨을 부트 가능한 시스템으로 복구할 필요가 없는 경우 **복구된 macOS 데이터 볼륨에 macOS 설치** 확인란을 선택 취소합니다. 나중에 수동으로 macOS를 설치하여 이 볼륨을 부트 가능하도록 할 수 있습니다.
12. [Linux에만 해당] 백업한 머신에 LVM(논리 볼륨)이 있고 원래 LVM 구조를 재현하려는 경우:
    a. 대상 머신 디스크의 수 및 각 디스크 용량이 원래 머신의 디스크 수 및 디스크 용량과 일치하거나 초과하는지 확인한 다음 **RAID/LVM 적용**을 클릭합니다.
    b. 볼륨 구조를 검토하고 **RAID/LVM 적용**을 클릭하여 볼륨을 생성합니다.
    c. 선택 내용을 확인합니다.
13. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
14. **확인**을 클릭하여 복구를 시작합니다.

Universal Restore 사용

최신 운영 체제는 VMware 또는 Hyper-V 플랫폼을 포함한 이기종 하드웨어로 복구했을 때에도 부트 가능한 상태로 유지됩니다. 복구한 운영 체제가 부트되지 않는 경우 Universal Restore 도구를 사용해 운영 체제 시작에 핵심적인 드라이버와 모듈을 업데이트하십시오.

Universal Restore는 Windows 및 Linux에 적용할 수 있습니다.

Universal Restore를 적용하려면

1. 부트 가능한 미디어에서 머신을 부트합니다.
2. **Universal Restore 적용**을 클릭합니다.
3. 머신에 여러 운영 체제가 있는 경우 Universal Restore를 적용할 운영 체제를 선택합니다.
4. [Windows에만 해당] 추가 설정을 구성합니다.
5. **확인**을 클릭합니다.

Universal Restore in Windows

준비

드라이버 준비

Universal Restore를 Windows 운영 체제에 적용하기 전에 새로운 HDD 컨트롤러 및 칩셋용 드라이버를 보유하고 있는지 확인하십시오. 이 드라이버는 운영 체제를 시작하는 데 필수적입니다. 하드웨어 공급업체가 제공한 CD 또는 DVD를 사용하거나 공급업체의 웹 사이트에서 드라이버를 다운로드하십시오. 드라이버 파일의 확장자가 *.inf여야 합니다. *.exe, *.cab 또는 *.zip 포맷 드라이버를 다운로드한 경우 서드 파티 애플리케이션을 사용해 추출하십시오.

가장 좋은 방법은 조직에서 사용하는 모든 하드웨어의 드라이버를 장치 유형이나 하드웨어 구성별로 분류한 단일 리포지토리에 저장하는 것입니다. 해당 리포지토리 사본을 DVD 또는 플래시 드라이브에 보관해두면 일부 드라이버를 골라 부트 가능한 미디어에 추가하고, 각 서버에 필요한 드라이버(그리고 필요한 네트워크 구성)로 사용자 지정 부트 가능한 미디어를 생성할 수 있습니다. 아니면 그냥 Universal Restore를 사용할 때마다 해당 리포지토리 경로를 지정해주면 됩니다.

부트 가능한 환경에서 드라이버에 대한 액세스 확인

부트 가능한 미디어에서 작업할 때 해당 드라이버를 포함한 장치에 액세스할 수 있어야 합니다. 장치를 Windows에서는 사용할 수 있지만 Linux 기반 미디어는 이를 감지할 수 없다면 WinPE 기반 미디어를 사용합니다.

Universal Restore 설정

자동 드라이버 검색

다음과 같이 HAL(Hardware Abstraction Layer), HDD 컨트롤러 드라이버 및 네트워크 어댑터 드라이버를 검색할 위치를 지정합니다.

- 드라이버가 공급업체 디스크 또는 다른 이동식 미디어에 있는 경우에는 **이동식 미디어 검색**을 켭니다.
- 드라이버가 네트워크 폴더 또는 부트 가능한 미디어에 있는 경우에는 **폴더 추가**를 클릭하여 폴더의 경로를 지정합니다.

또한, Universal Restore는 Windows 기본 드라이버 저장 폴더를 검색합니다. 그 위치는 레지스트리 값 **DevicePath**에서 정해집니다. 이 값은 레지스트리 키 **HKEY_LOCAL_**

MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion에서 찾을 수 있습니다. 이 저장 폴더는 대개 WINDOWS/inf입니다.

Universal Restore는 지정한 폴더의 모든 하위 폴더에서 재귀 검색을 수행하여, 사용 가능한 모든 드라이버 중에서 가장 적합한 HAL 및 HDD 컨트롤러 드라이버를 찾아 시스템에 설치합니다. Universal Restore는 또한 네트워크 어댑터 드라이버를 검색합니다. 그다음 Universal Restore는 검색한 드라이버의 경로를 운영 체제로 전송합니다. 하드웨어에 네트워크 인터페이스 카드가 여러 개라면 Universal Restore는 모든 카드의 드라이버를 구성하려고 시도합니다.

설치할 대용량 스토리지 드라이버

다음의 경우 이 설정이 필요합니다.

- 하드웨어에 RAID(특히, NVIDIA RAID) 또는 파이버 채널 어댑터와 같은 특정 대용량 스토리지 컨트롤러가 있는 경우.
- SCSI 하드 드라이브 컨트롤러를 사용하는 가상 머신으로 시스템을 마이그레이션한 경우. 가상화 소프트웨어와 함께 묶여진 SCSI 드라이버들을 사용하거나 소프트웨어 제조사 웹 사이트에서 최신 드라이버 버전을 다운로드합니다.
- 자동 드라이버 검색으로 시스템을 부팅할 수 없는 경우.

드라이버 추가를 클릭하여 적절한 드라이버를 지정합니다. 여기에서 정의된 드라이버는 프로그램이 보다 적합한 드라이버를 찾아도 해당 경고와 함께 설치됩니다.

Universal Restore 프로세스

필수 설정을 지정한 후 **확인**을 클릭합니다.

Universal Restore가 지정한 위치에서 호환 가능한 드라이버를 찾지 못하는 경우 문제 장치에 관한 프롬프트가 표시됩니다. 다음 중 하나를 수행하십시오.

- 이전에 지정한 위치에 드라이버를 추가하고 **재시도**를 클릭합니다.
- 위치가 기억나지 않으면 **무시**를 클릭하고 프로세스를 계속 진행합니다. 결과가 만족스럽지 않다면 Universal Restore를 재적용합니다. 작업을 구성할 때 필요한 드라이버를 지정합니다.

Windows는 부팅되고 나면 새 하드웨어 설치를 위한 표준 절차를 시작합니다. 드라이버에 Microsoft Windows 서명이 있으면 네트워크 어댑터 드라이버가 자동으로 설치됩니다. 그렇지 않으면 Windows가 서명 없는 드라이버를 설치할지 확인을 요청합니다.

설치 후 네트워크 연결을 구성하고, 비디오 어댑터, USB 및 기타 장치에 대해 드라이버를 지정할 수 있습니다.

Linux의 Universal Restore

Universal Restore는 커널 버전이 2.6.8 이상인 Linux 운영 체제에 적용할 수 있습니다.

Universal Restore가 Linux 운영 체제에 적용되면 초기 RAM 디스크(initrd)라고 하는 임시 파일 시스템을 업데이트합니다. 이를 통해 새 하드웨어에서 운영 체제를 부팅할 수 있습니다.

Universal Restore는 새 하드웨어(장치 드라이버 포함)의 모듈을 초기 RAM 디스크에 추가합니다. 일반적으로 **/lib/modules** 디렉토리에서 필요한 모듈을 찾습니다. Universal Restore가 필요한 모듈을 찾지 못하면 모듈의 파일 이름을 로그에 기록합니다.

Universal Restore는 GRUB 부트 로더의 구성을 수정할 수 있습니다. 이러한 기능은 예를 들어, 새 머신의 볼륨 레이아웃이 원래 머신과 다른 경우 머신 부트 가능성을 확보하는 데 필요합니다.

Universal Restore는 Linux 커널은 수정하지 않습니다.

원본 초기 RAM 디스크로 되돌리기

필요한 경우 원본 초기 RAM 디스크로 되돌릴 수 있습니다.

초기 RAM 디스크는 머신에 파일로 저장됩니다. 초기 RAM 디스크를 처음 업데이트하기 전에 Universal Restore는 디스크의 사본을 동일한 디렉토리에 저장합니다. 사본의 이름은 파일 이름 뒤에 접미사 **_acronis_backup.img**가 추가됩니다. Universal Restore를 여러 번 실행해도 이 사본은 덮어쓰지 않습니다(예를 들어, 누락된 드라이버를 추가한 후).

원본 초기 RAM 디스크로 되돌리려면 다음 중 아무것이나 수행하십시오.

- 사본의 이름을 그에 따라 변경합니다. 예를 들어, 다음과 유사한 명령을 실행합니다.

  ```
  mv initrd-2.6.16.60-0.21-default_acronis_backup.img initrd-2.6.16.60-0.21-default
  ```

- GRUB 부트 로더 구성의 **initrd** 행에 사본을 지정합니다.

파일 복구

웹 인터페이스를 사용하여 파일 복구

1. 복구하려는 데이터가 원래 포함되어 있는 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   선택한 머신이 실제 머신인데 오프라인 상태인 경우 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [권장 사항] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
   - 클라우드 스토리지에서 파일을 다운로드합니다.
   - 부트 가능한 미디어를 사용합니다.
4. **복구** > **파일/폴더**를 클릭합니다.
5. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
   하나 이상의 와일드 카드 문자(* 및 ?)를 사용할 수 있습니다.와일드카드 사용에 관한 자세한 내용은 "파일 필터"를 참조하십시오.

참고
클라우드 스토리지에 저장된 디스크 수준 백업은 검색할 수 없습니다.

6. 복구할 파일을 선택합니다.
7. 파일을 .zip 파일로 저장하려면 **다운로드**를 클릭하고 데이터를 저장할 위치를 선택한 다음 **저장**을 클릭합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
8. **복구**를 클릭합니다.

   복구 대상에 다음 중 하나가 표시됩니다.
   - 복구할 파일을 원래 포함하고 있던 머신(에이전트가 이 머신에 설치된 경우).
   - Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing HC3가 설치되어 있는 머신(파일의 원래 위치가 ESXi, Hyper-V 또는 Scale Computing HC3 가상 머신인 경우).

   이는 복구를 위한 대상 머신입니다. 필요하다면 다른 머신을 선택할 수 있습니다.
9. **경로**에서 복구 목적지를 선택합니다. 다음 중 하나를 선택합니다.
   - 원래 위치(원래 머신으로 복구하는 경우)
   - 대상 머신의 로컬 폴더

     참고
     심볼 링크는 지원되지 않습니다.

   - 대상 머신에서 액세스할 수 있는 네트워크 폴더.
10. **복구 시작**을 클릭합니다.
11. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 파일 덮어쓰기**
    - **오래된 경우 기존 파일 덮어쓰기**
    - **기존 파일 덮어쓰기 안 함**

복구 진행률이 **작업** 탭에 표시됩니다.

클라우드 스토리지에서 파일 다운로드

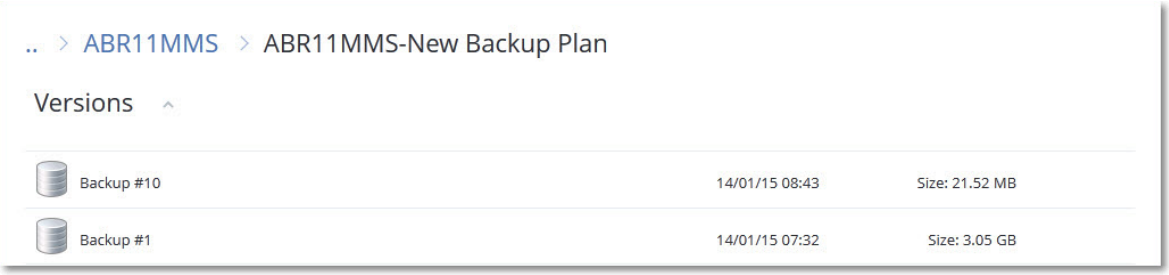
클라우드 스토리지를 찾아 백업 내용을 보고 필요한 파일을 다운로드할 수 있습니다.

제한 사항

- 시스템 상태, SQL 데이터베이스 및 Exchange 데이터베이스 백업은 찾을 수 없습니다.
- 다운로드 경험을 개선하기 위해 한 번에 100MB 이하로 다운로드하십시오. 클라우드에서 더 큰 용량의 데이터를 찾으려면 파일 복구 절차를 따르십시오.

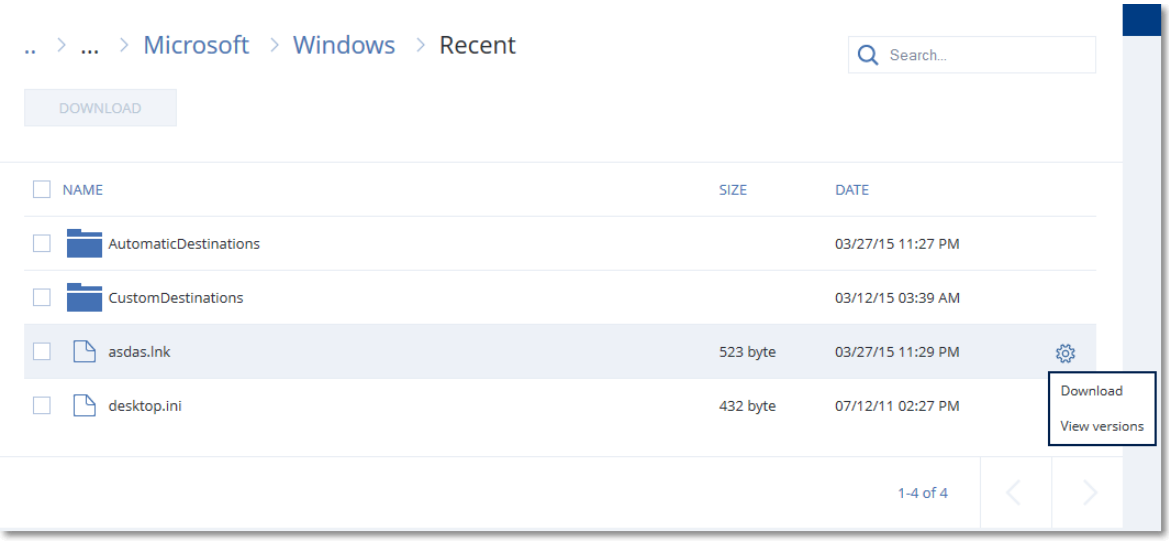
클라우드 스토리지에서 파일을 다운로드하려면

1. 백업한 머신을 선택합니다.
2. **복구** > **추가 복구 방법...** > **다운로드 파일**을 클릭합니다.
3. 백업된 머신이 할당된 계정의 자격 증명을 입력합니다.
4. [디스크 수준 백업을 찾는 경우] **버전**에서 파일을 복구하려는 백업을 클릭합니다.



[파일 수준 백업을 찾는 경우] 다음 단계에서는 선택한 파일의 오른쪽에 있는 기어 아이콘 아래에서 백업 날짜 및 시간을 선택할 수 있습니다. 기본적으로 파일은 최신 백업에서 복구됩니다.

5. 필요한 폴더를 찾거나 검색 기능을 사용하여 필요한 파일을 얻습니다.



6. 복구하려는 항목에 해당하는 확인란을 선택한 다음 **다운로드**를 클릭합니다.
   단일 파일을 선택하면 해당 파일이 있는 그대로 다운로드됩니다. 그렇지 않은 경우 선택한 데이터가 .zip 파일로 아카이브됩니다.
7. 데이터를 저장할 위치를 선택한 다음 **저장**을 클릭합니다.

Notary Service를 통해 파일 신뢰성 확인

백업 중에 공증이 활성화된 경우 백업된 파일의 신뢰성을 확인할 수 있습니다.

파일 신뢰성을 확인하려면

1. "웹 인터페이스를 사용하여 파일 복구" 섹션의 1~6 단계, 또는 "클라우드 스토리지에서 파일 다운로드" 섹션의 1~5 단계에 설명된 대로 파일을 선택합니다.
2. 선택한 파일에 다음 아이콘이 표시되는지 확인합니다.  이는 파일이 공증되었음을 의미합니다.
3. 다음 중 하나를 수행하십시오.
   - **확인**을 클릭합니다.
     소프트웨어에서 파일 신뢰성을 확인하고 결과를 표시합니다.
   - **인증서 가져오기**를 클릭합니다.

파일 공증을 확인하는 인증서가 웹 브라우저 창에서 열립니다. 이 창에는 파일 신뢰성을 수동으로 확인하는 방법도 포함되어 있습니다.

ASign으로 파일에 서명

ASign은 여러 사용자가 백업된 파일에 전자적으로 서명할 수 있도록 하는 서비스입니다. 이 기능은 클라우드 스토리지에 저장된 파일 수준 백업에만 사용할 수 있습니다.

한 번에 하나의 파일 버전에만 서명할 수 있습니다. 파일이 여러 번 백업된 경우 서명할 버전을 선택해야 하고 이 버전에만 서명이 포함됩니다.

예를 들어 다음 파일의 전자 서명에 ASign을 사용할 수 있습니다.

- 대여 또는 임대 계약
- 판매 계약
- 자산 구매 계약
- 대출 계약
- 허가서
- 금융 문서
- 보험 문서
- 책임 포기 각서
- 의료 문서
- 연구 논문
- 제품 정품 인증서
- 비공개 계약
- 제안 문서
- 기밀 유지 계약
- 독립 계약자 계약

파일 버전에 서명하려면

1. "웹 인터페이스를 사용하여 파일 복구" 섹션의 1~6단계에 설명된 대로 파일을 선택합니다.
2. 왼쪽 패널에서 올바른 날짜 및 시간이 선택되었는지 확인합니다.
3. **이 파일 버전에 서명**을 클릭합니다.
4. 백업이 저장된 클라우드 스토리지 계정에 대한 비밀번호를 지정합니다. 프롬프트 창에 계정의 로그인이 표시됩니다.

   ASign 서비스 인터페이스가 웹 브라우저 창에서 열립니다.
5. 이메일 주소를 지정하여 다른 서명인을 추가합니다. 초대를 보낸 후에는 서명인을 추가하거나 제거할 수 없으므로 서명이 필요한 모든 사람이 목록에 포함되었는지 확인하십시오.
6. **서명 초대**를 클릭하여 서명인에게 초대를 보냅니다.

   각 서명인은 서명 요청이 포함된 이메일 메시지를 받습니다. 요청된 모든 서명인이 파일에 서명하면 공증 서비스를 통해 공증되고 서명됩니다.

   각 서명인이 파일에 서명하고 전체 프로세스가 완료되면 알림을 받게 됩니다. 수신한 모든 이메일 메시지에서 **세부정보 보기**를 클릭하여 ASign 웹 페이지에 액세스할 수 있습니다.

7. 프로세스가 완료되면 ASign 웹 페이지로 이동하고 **문서 가져오기**를 클릭하여 다음이 포함된 .pdf 문서를 다운로드하십시오.
   - 수집된 서명이 있는 서명 인증서 페이지.
   - 작업 내역이 있는 감사 추적 페이지: 초대가 서명인에게 전송된 시간, 서명인이 파일에 서명한 시간 등.

부트 가능한 미디어를 사용하여 파일 복구

부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "부트 가능한 미디어 생성"을 참조하십시오.

부트 가능한 미디어를 사용하여 파일을 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
3. 네트워크에서 프록시 서버가 사용하도록 설정되어 있는 경우 **도구** > **프록시 서버**를 클릭한 다음 프록시 서버 호스트 이름/IP 주소 및 포트를 지정합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
4. 시작 화면에서 **복구**를 클릭합니다.
5. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
6. 백업 위치 지정:
   - 클라우드 스토리지에서 복구하려면 **클라우드 스토리지**를 선택합니다. 백업된 머신이 할당된 계정의 자격 증명을 입력합니다.
   - 로컬 또는 네트워크 폴더에서 복구하려면 **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.

   확인을 클릭하여 선택 항목을 확인합니다.
7. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
8. **백업 내용**에서 **폴더/파일**을 선택합니다.
9. 복구할 데이터를 선택합니다. **확인**을 클릭하여 선택 항목을 확인합니다.
10. **복구 위치**에서 폴더를 지정합니다. 또는 새 버전의 파일 덮어쓰기를 금지하거나 복구에서 일부 파일을 제외할 수 있습니다.
11. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
12. **확인**을 클릭하여 복구를 시작합니다.

참고

테이프 위치는 많은 공간을 차지하며 Linux 부트 가능한 미디어 및 WinPE 부트 가능한 미디어에서 재스캔 및 복구할 때 RAM에 충분한 공간이 확보되지 않을 수 있습니다. Linux의 경우 디스크 또는 공유에 데이터를 저장하려면 다른 위치를 마운트해야 합니다. Acronis Cyber Backup Advanced: 테이프 위치 폴더 변경(KB 27445)을 참조하십시오. Windows PE의 경우 현재로서는 방법이 없습니다.

로컬 백업에서 파일 추출

로컬 백업에서 파일 추출백업 내용을 찾아 필요한 파일을 추출할 수 있습니다.

요구 사항

- 이 기능은 파일 탐색기를 사용하여 Windows에서만 이용할 수 있습니다.
- 백업을 찾아보는 머신에 보호 에이전트가 설치되어 있어야 합니다.
- 백업 파일 시스템은 다음 중 하나여야 합니다. FAT16, FAT32, NTFS, ReFS, Ext2, Ext3, Ext4, XFS 또는 HFS+.
- 백업은 로컬 폴더 또는 네트워크 공유(SMB/CIFS)에 저장해야 합니다.

백업에서 파일을 추출하려면

1. 파일 탐색기를 사용하여 백업 위치를 찾습니다.
2. 백업 파일을 두 번 클릭합니다. 파일 이름은 다음 템플릿에 따라 지정되어 있습니다.
   `<머신 이름> - <보호 계획 GUID>`
3. 백업이 암호화되어 있는 경우 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   파일 탐색기가 복구 지점을 표시합니다.
4. 복구 지점을 두 번 클릭합니다.
   파일 탐색기가 백업된 데이터를 표시합니다.
5. 필요한 폴더를 찾습니다.
6. 필요한 파일을 파일 시스템에 있는 폴더에 복사합니다.

시스템 상태 복구

1. 시스템 상태를 복구하려는 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 시스템 상태 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **시스템 상태 복구**를 클릭합니다.
5. 백업된 버전으로 시스템 상태를 덮어 쓰려는지 확인합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

ESXi 구성 복구

ESXi 구성을 복구하려면 Linux 기반 부트 가능한 미디어가 필요합니다. 부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 "부트 가능한 미디어 생성"을 참조하십시오.

ESXi 구성을 원래 호스트가 아닌 호스트로 복구하는 중인데 원래 ESXi 호스트가 여전히 vCenter Server에 연결되어 있는 경우 복구 중 예기치 않은 문제를 방지하려면 이 호스트를 vCenter Server에서 연결 해제하고 제거하십시오. 원래 호스트를 복구된 호스트와 함께 유지하려면 복구가 완료된 후에 원래 호스트를 다시 추가하면 됩니다.

해당 호스트에서 실행 중인 가상 머신은 ESXi 구성 백업에 포함되지 않습니다. 가상 머신은 따로 백업 및 복구할 수 있습니다.

ESXi 구성을 복구하려면

1. 부트 가능한 미디어를 사용하여 대상 머신을 부트합니다.
2. **이 머신을 로컬로 관리**를 클릭합니다.
3. 시작 화면에서 **복구**를 클릭합니다.
4. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
5. 백업 위치 지정:
   - **로컬 폴더** 또는 **네트워크 폴더**에서 폴더를 찾습니다.

   확인을 클릭하여 선택 항목을 확인합니다.
6. **표시**에서 **ESXi 구성**을 선택합니다.
7. 데이터를 복구하려는 백업을 선택합니다. 메시지가 표시되면 백업의 비밀번호를 입력합니다.
8. **확인**을 클릭합니다.
9. **새 데이터 저장소로 사용할 디스크**에서 다음을 수행합니다.
   - **ESXi 복구 대상**에서 호스트 구성을 복구할 디스크를 선택합니다. 구성을 원래 호스트로 복구하는 경우에는 원본 디스크가 자동으로 선택됩니다.
   - [선택 사항] **새 데이터 저장소로 사용**에서 새 데이터 저장소를 생성할 디스크를 선택합니다. 선택하는 디스크의 모든 데이터가 손실되므로 신중하게 선택하십시오. 기존 데이터 저장소의 가상 머신을 유지하려면 아무 데이터도 선택하지 마십시오.
10. 새 데이터 저장소로 사용할 디스크를 선택하는 경우에는 **새 데이터 저장소 생성 방법: 디스크당 하나의 데이터 저장소 생성** 또는 **선택한 모든 HDD에 하나의 데이터 저장소 생성**을 선택합니다.
11. [선택 사항] **네트워크 매핑**에서 백업에 존재하는 가상 스위치의 자동 매핑 결과를 실제 네트워크 어댑터로 변경합니다.
12. [선택 사항] 추가 설정을 지정하려면 **복구 옵션**을 클릭합니다.
13. **확인**을 클릭하여 복구를 시작합니다.

복구 옵션

복구 옵션을 수정하려면 복구를 구성할 때 **복구 옵션**을 클릭합니다.

복구 옵션의 사용 가능성

사용 가능한 복구 옵션은 다음에 따라 다릅니다.

- 복구를 수행하는 에이전트를 운영하는 환경(Windows, Linux, macOS 또는 부트 가능한 미디어).
- 복구하는 데이터 유형(디스크, 파일, 가상 머신, 애플리케이션 데이터).

다음 표는 복구 옵션의 사용 가능성을 요약해서 보여줍니다.

	디스크	파일	가상 머신	SQL 및 Exchan

									ge
	Windows	Linux	부트 가능한 미디어	Windows	Linux	macOS	부트 가능한 미디어	ESXi, Hyper-V, Scale Computing HC3	Windows
백업 유효성 검사	+	+	+	+	+	+	+	+	+
부트 모드	+	-	-	-	-	-	-	+	-
파일의 날짜 및 시간	-	-	-	+	+	+	+	-	-
오류 처리	+	+	+	+	+	+	+	+	+
파일 제외	-	-	-	+	+	+	+	-	-
플래시 백	+	+	+	-	-	-	-	+	-
전체 경로 복구	-	-	-	+	+	+	+	-	-
마운트 포인트	-	-	-	+	-	-	-	-	-
성능	+	+	-	+	+	+	-	+	+
사전/사후 명령어	+	+	-	+	+	+	-	+	+
SID 변경	+	-	-	-	-	-	-	-	-
VM 전원 관리	-	-	-	-	-	-	-	+	-

"데이프 관리" (311페이지) > 빠른 복구를 위해 디스크 캐시 사용	-	-	-	+	+	+	-	-	-
Windows 이벤트 로그	+	-	-	+	-	-	-	Hyper-V만 해당	+
복구 후 전원 켜기	-	-	-	-	-	-	+	-	-

백업 유효성 검사

이 옵션은 데이터가 백업에서 복구되기 전에 백업이 손상되지 않도록 백업의 유효성 검사를 수행할지 여부를 정의합니다. 이 작업은 보호 에이전트를 통해 수행됩니다.

사전 설정값이 **비활성화됨**.

유효성 검사는 백업에 저장되어 있는 모든 데이터 블록의 체크섬을 계산합니다. 유일한 예외는 클라우드 스토리지에 위치한 파일 수준 백업의 유효성 검사입니다. 이 백업은 백업에 저장되어 있는 메타 정보의 일관성 확인을 통해 유효성을 검사합니다.

유효성 검사는 크기가 작은 증분 또는 차등 백업의 경우에도 시간이 걸리는 프로세스입니다. 이 작업은 백업에 실제로 포함된 데이터뿐 아니라 백업을 선택하여 복구 가능한 모든 데이터의 유효성을 검사하기 때문입니다. 따라서 이전에 생성한 백업에 대한 액세스 권한이 필요합니다.

참고
유효성 검사는 Acronis 데이터 센터에 위치하고 Acronis 파트너에서 제공하는 클라우드 스토리지에 대해 가능합니다.

부트 모드

이 옵션은 Windows 운영 체제를 포함하고 있는 디스크 수준 백업에서 실제 머신 또는 가상 머신을 복구하는 경우에 유효합니다.

이 옵션을 사용하면 복구 후 Windows가 사용할 부트 모드(BIOS 또는 UEFI)를 선택할 수 있습니다. 원래 머신의 부트 모드가 선택한 부트 모드와 다른 경우 소프트웨어가 다음 작업을 수행합니다.

- 선택한 부트 모드에 따라 시스템 볼륨을 복구할 디스크(BIOS는 MBR, UEFI는 GPT)를 초기화합니다.
- Windows 운영 체제가 선택한 부트 모드를 사용하여 시작될 수 있도록 조정합니다.

사전 설정값이 **대상 머신에서.**

다음 중 하나를 선택할 수 있습니다.

- **대상 머신에서**
  대상 머신에서 실행 중인 에이전트가 현재 Windows가 사용 중인 부트 모드를 탐지하고, 탐지된 부트 모드에 따라 조정을 수행합니다.
  아래 나열된 제한 사항이 적용되지 않는 한 자동으로 부트 가능한 시스템으로 이어지는 가장 안전한 값입니다. 이 **부트 모드** 옵션이 부트 가능한 미디어 아래에 없기 때문에 해당 미디어의 에이전트는 항상 이 값을 선택한 것처럼 작동합니다.
- **백업된 머신에서**
  대상 머신에서 실행 중인 에이전트가 백업에서 부트 모드를 읽고, 이 부트 모드에 따라 조정을 수행합니다. 이렇게 하면 이 머신이 다른 부트 모드를 사용하는 경우에도 다른 머신의 시스템을 복구한 다음, 백업된 머신의 디스크를 교체할 수 있습니다.
- **BIOS**
  대상 머신에서 실행 중인 에이전트가 BIOS를 사용하도록 조정을 수행합니다.
- **UEFI**
  대상 머신에서 실행 중인 에이전트가 UEFI를 사용하도록 조정을 수행합니다.

설정이 변경되면 디스크 매핑 절차가 반복됩니다. 이 절차는 약간의 시간이 소요됩니다.

권장 사항

UEFI와 BIOS 간에 Windows를 전송해야 하는 경우:

- 시스템 볼륨이 위치한 전체 디스크를 복구합니다. 기존 볼륨 위에 시스템 볼륨만 복구하는 경우 에이전트가 대상 디스크를 올바로 초기화할 수 없습니다.
- BIOS는 2TB를 초과하는 디스크 공간 사용을 허용하지 않습니다.

제한 사항

- 다음에 대한 UEFI와 BIOS 간 전송은 지원되지 않습니다.
  - Windows 7 이상의 64비트 Windows 운영 체제
  - Windows Server 2008 SP1부터 64비트 Windows Server 운영 체제
- 백업이 테이프 장치에 저장되어 있는 경우에는 UEFI와 BIOS 간 전송이 지원되지 않습니다.

UEFI와 BIOS 간 시스템 전송이 지원되지 않으면 에이전트가 **백업된 머신에서** 설정이 선택된 것처럼 작동합니다 대상 머신이 UEFI와 BIOS를 모두 지원하는 경우에는 원본 머신에 따라 부트 모드를 수동으로 활성화해야 합니다. 그렇지 않으면 시스템이 부팅되지 않습니다.

파일의 날짜 및 시간

이 옵션은 파일을 복구할 때에만 유효합니다.

이 옵션은 백업에서 파일의 날짜 및 시간을 복구할지 또는 파일에 현재 날짜 및 시간을 할당할지 정의합니다.

이 옵션이 활성화되어 있으면 파일에 현재 날짜 및 시간이 할당됩니다.

사전 설정값이 **활성화됨**.

오류 처리

이 옵션을 사용하여 복구 중 발생할 수 있는 오류를 어떻게 처리할지 지정할 수 있습니다.

오류 발생 시 재시도

사전 설정값이 **시도 횟수: 300(기본값에 무관). 불량 섹터 무시 시도 간격: 30초.**

복구 가능 오류가 발생하면 프로그램이 성공하지 못한 작업의 수행을 재시도합니다. 시간 간격과 시도 횟수를 설정할 수 있습니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다.

처리하는 동안 메시지 및 대화 상자 표시 안 함(자동 모드)

사전 설정값이 **비활성화됨**.

자동 모드가 활성화되어 있는 경우 가능하면 프로그램이 사용자 상호 작용이 필요한 상황을 자동으로 처리합니다. 작업 성공 또는 지정된 시도 횟수 완료 중 하나가 먼저 발생하면 시도가 중지됩니다. 작업 로그에는 오류(있는 경우)를 포함하여 작업에 대한 자세한 정보가 기록됩니다.

재부팅을 이용한 복구가 실패하는 경우 시스템 정보 저장

이 옵션은 Windows 또는 Linux를 실행하는 실제 머신으로 디스크 또는 볼륨을 복구할 때 유효합니다.

사전 설정값이 **비활성화됨**.

이 옵션이 활성화되어 있으면 로그, 시스템 정보, 크래시 덤프 파일이 저장될 로컬 디스크(대상 머신에 연결된 플래시 또는 HDD 드라이브 포함) 또는 네트워크 공유에서 폴더를 지정할 수 있습니다. 이 파일은 기술 지원 담당자가 문제를 파악하는 데 도움이 됩니다.

파일 제외

이 옵션은 파일을 복구할 때에만 유효합니다.

이 옵션은 복구 프로세스 중 건너뛰으로써 복구된 항목 목록에서 제외시킬 파일 및 폴더를 정의합니다.

참고
제외가 복구할 데이터 항목 선택보다 우선합니다. 예를 들어, MyFile.tmp 파일을 복구하고, 모든 .tmp 파일을 제외하기로 선택하는 경우 MyFile.tmp 파일이 복구되지 않습니다.

파일 수준 보안

이 옵션은 NTFS 형식 볼륨의 디스크 및 파일 수준 백업을 복구하는 경우에만 유효합니다.

이 옵션은 파일과 함께 파일에 대한 NTFS 권한을 복구할지 정의합니다.

사전 설정값이 **활성화됨**.

그 권한을 복구할지 아니면 파일이 복구될 대상 폴더로부터 NTFS 권한을 상속하게 할지 선택할 수 있습니다.

플래시 백

이 옵션은 Mac을 제외한 실제 머신과 가상 머신에서 디스크 및 볼륨을 복구할 때 유효합니다.

이 옵션이 활성화되어 있으면 백업에 있는 데이터와 대상 디스크 데이터 간의 차이만 복구됩니다. 이렇게 하면 특히 디스크의 볼륨 레이아웃이 변경되지 않은 경우 백업에 사용한 동일한 디스크로의 데이터 복구가 가속화됩니다. 데이터는 블록 수준에서 비교됩니다.

실제 머신의 경우 블록 수준에서 데이터를 비교하는 것은 시간 소모적인 작업입니다. 백업 스토리지로의 연결이 빠르다면 데이터 차이를 계산하는 것보다 전체 디스크를 복구하는 것이 시간이 덜 소요됩니다. 따라서 백업 스토리지로의 연결이 느린 경우(예: 백업이 클라우드 스토리지 또는 원격 네트워크 폴더에 저장되어 있는 경우)에만 이 옵션을 활성화하는 것이 좋습니다.

실제 머신을 복구할 때의 사전 설정은 백업 위치에 따라 달라집니다.

- 백업 위치가 클라우드 스토리지라면 사전 설정은 **활성화됨**.
- 다른 백업 위치의 경우 사전 설정은 **비활성화됨**.

가상 머신을 복구할 때의 사전 설정은 **활성화됨**.

전체 경로 복구

이 옵션은 파일 수준 백업에서 데이터를 복구하는 경우에만 유효합니다.

이 옵션이 활성화되어 있으면 대상 위치에서 파일의 전체 경로가 다시 생성됩니다.

사전 설정값이 **비활성화됨**.

마운트 포인트

이 옵션은 Windows의 파일 수준 백업에서 데이터를 복구하는 경우에만 유효합니다.

마운트된 볼륨에 저장되었다가 마운트 포인트 옵션이 활성화된 채로 백업된 파일 및 폴더를 복구하려면 이 옵션을 활성화합니다.

사전 설정값이 **비활성화됨**.

이 옵션은 폴더 계층에서 마운트 포인트보다 상위에 있는 폴더를 복구용으로 선택하는 경우에만 유효합니다. 마운트 포인트 내부의 폴더 또는 마운트 포인트 자체를 복구용으로 선택하는 경우에는 선택한 항목이 **마운트 포인트** 옵션 값에 상관없이 복구됩니다.

참고
볼륨이 복구 시점에 마운트되어 있지 않으면 데이터가 백업 당시 마운트 포인트였던 폴더로 바로 복구됩니다.

성능

이 옵션은 운영 체제에서 복구 프로세스의 우선 순위를 정의합니다.

사용 가능한 설정은 **낮음**, **보통**, **높음**입니다.

사전 설정값이**보통**입니다.

시스템에서 실행하는 프로세스의 우선 순위는 CPU와 해당 프로세스에 할당된 시스템 리소스를 결정합니다. 복구 우선 순위를 낮추면 다른 애플리케이션용으로 추가 여유 리소스가 확보됩니다. 복구 우선 순위를 높이면 운영 체제에게 복구를 수행할 애플리케이션에 더 많은 리소스를 할당하도록 요청함으로써 복구 프로세스 속도가 빨라질 수 있습니다. 하지만 그 효과는 전체 CPU 사용량과 디스크 I/O 속도나 네트워크 트래픽 같은 기타 요인에 따라 달라집니다.

사전/사후 명령어

이 옵션을 사용하여 데이터 복구 전과 후에 자동으로 실행될 명령을 정의할 수 있습니다.

사전/사후 명령어를 사용하는 방법의 예:

- **Checkdisk** 명령을 실행하여 복구를 시작하기 전 또는 복구가 종료된 후 논리적 파일 시스템 오류, 물리적 오류 또는 불량 섹터를 찾아 수정합니다.

프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.

복구로 인해 재부팅이 진행되는 경우에는 복구 후 명령이 실행되지 않습니다.

복구 전 명령

복구 프로세스가 시작되기 전에 실행할 명령/배치 파일을 지정하려면

1. **복구 전 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.프로그램은 대화형 명령, 즉 사용자 입력(예: "pause")이 필요한 명령을 지원하지 않습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 원하는 결과에 따라 아래 표에 설명한 대로 적합한 옵션을 선택합니다.
6. **완료**를 클릭합니다.

확인란	**선택**			
명령 실행이 실패한 경우 복구 실패*	선택됨	선택 해제됨	선택됨	선택 해제됨
명령 실행이 완료될 때까지 복구 안 함	선택됨	선택됨	선택 해제됨	선택 해제됨
결과				
	사전 설정 명령이 성공적으로 실행된 후에만 복구를 수행합니	실행 실패 또는 성공에 상관없이 명령이 실행된 후	해당 없음	명령 실행 결과에 상관없이 명령 실행과 동시에 복

	다. 명령 실행이 실패한 경우 복구 실패.	에 복구를 수행합니다.		구를 수행합니다.

* 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다.

복구 후 명령

복구가 완료된 후에 실행할 명령/실행 파일을 지정하려면

1. **복구 후 명령 실행** 스위치를 활성화합니다.
2. **명령...** 필드에 명령을 입력하거나 배치 파일을 찾습니다.
3. **작업 디렉토리** 필드에 명령/배치 파일을 실행할 디렉토리의 경로를 지정합니다.
4. 필요한 경우 **인수** 필드에 명령 실행 인수를 지정합니다.
5. 명령 실행이 반드시 성공해야 하는 경우 **명령 실행에 실패한 경우 복구 실패** 확인란을 선택합니다. 이 종료 코드가 0과 같지 않다면 명령이 실패한 것으로 간주됩니다. 명령 실행에 실패하면 복구 상태가 **오류**로 설정됩니다.

   이 확인란을 선택하지 않으면 명령 실행 결과가 복구 실패 또는 성공에 영향을 주지 않습니다. **작업** 탭을 살펴보면 명령 실행 결과를 추적할 수 있습니다.
6. **완료**를 클릭합니다.

참고
복구로 인해 재부팅이 진행되는 경우에는 복구 후 명령이 실행되지 않습니다.

테이프 관리

다음 테이프 관리 복구 옵션을 사용할 수 있습니다.

빠른 복구를 위해 디스크 캐시 사용

사전 설정값이 **비활성화됨**.

이미지 아카이브에서 파일을 복구할 때는 **빠른 복구를 위해 디스크 캐시 사용** 옵션을 사용하는 것이 좋습니다. 그렇지 않을 경우 복원 작업에 시간이 많이 걸릴 수 있습니다. 이 옵션을 사용할 경우 중단 및 되감기 없이 테이프가 순차적으로 판독됩니다.

SID 변경

이 옵션은 Windows 8.1/Windows Server 2012 R2 이전 버전을 복구할 때 효과적입니다.

이 옵션은 Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing HC3를 통해 가상 머신으로의 복구를 수행하는 경우 유효하지 않습니다.

사전 설정값이 **비활성화됨**.

소프트웨어는 복구된 운영 체제에 대해 고유한 보안 식별자(컴퓨터 SID)를 생성할 수 있습니다. 이 옵션은 컴퓨터 SID에 의존하는 서드 파티 소프트웨어의 운용 가능성을 보장하는 데에만 필요합니다.

Microsoft는 배포 또는 복구된 시스템에서의 SID 변경을 공식적으로 지원하지는 않습니다. 따라서 이 옵션은 사용자 책임에 따라 사용하십시오.

VM 전원 관리

이 옵션은 Agent for VMware, Agent for Hyper-V 또는 Agent for Scale Computing HC3를 통해 가상 머신으로의 복구를 수행하는 경우에 유효합니다.

복구 시작 시 대상 가상 머신의 전원 끄기

사전 설정값이 **활성화됨**.

머신이 온라인 상태인 경우 결국 복구를 시작하자마자 머신의 전원이 자동으로 꺼지기 때문에 기존 가상 머신으로의 복구가 불가능합니다. 그러면 사용자가 머신에서 연결이 끊기게 되므로 저장되지 않은 데이터가 손실됩니다.

복구 전에 가상 머신의 전원을 수동으로 끄려면 이 옵션의 확인란을 선택 해제하십시오.

복구 완료 시 대상 가상 머신 전원 켜기

사전 설정값이 **비활성화됨**.

머신이 백업에서 다른 머신으로 복구된 후에 기존 머신의 복제본이 네트워크에 표시될 수 있습니다. 안전을 기하기 위해 필요한 예방 조치를 취한 후에 복구된 가상 머신의 전원을 수동으로 켜십시오.

Windows 이벤트 로그

이 옵션은 Windows 운영 체제에서만 유효합니다.

이 옵션은 에이전트가 Windows의 애플리케이션 이벤트 로그에 복구 작업의 이벤트를 기록해야 하는지 정의합니다(이 로그를 보려면 eventvwr.exe를 실행하거나 **제어판** > **관리 도구** > **이벤트 뷰어** 선택). 기록할 이벤트를 필터링할 수 있습니다.

사전 설정값이 **비활성화됨**.

복구 후 전원 켜기

이 옵션은 부트 가능한 미디어에서 작동할 때에만 유효합니다.

사전 설정값이 **비활성화됨**.

이 옵션을 사용하면 사용자 상호 작용 없이 머신을 복구된 운영 체제로 부팅할 수 있습니다.

재해 복구

이 기능은 Acronis Cyber Protect의 클라우드 디플로이에만 제공됩니다. 이 기능에 대한 자세한 설명은 https://www.acronis.com/support/documentation/DisasterRecovery/index.html#43224.html을 참조하십시오.

백업 관련 작업

백업 스토리지 탭

백업 스토리지 탭에는 관리 서버에 등록된 모든 머신의 백업이 표시됩니다. 여기에는 더 이상 등록되지 않은 머신 및 오프라인 머신이 포함됩니다.

공유 위치(예: SMB 또는 NFS 공유)에 저장된 백업은 해당 위치에 대한 읽기 권한을 가진 모든 사용자에게 표시됩니다.

Windows에서는 백업 파일이 해당 상위 폴더의 액세스 권한을 상속받습니다. 따라서 이 폴더에 대한 읽기 권한을 제한하는 것이 좋습니다.

클라우드 스토리지에서 사용자는 자신의 백업에만 액세스할 수 있습니다. 클라우드 디플로이에서 관리자는 동일한 그룹과 그 자식 그룹에 속한 계정을 대신하여 백업을 확인할 수 있습니다. 이 계정은 **다음 위치에서 탐색할 머신**에서 간접적으로 선택됩니다. **백업 스토리지** 탭에는 이 머신이 등록된 것과 동일한 계정에서 등록된 모든 머신의 백업이 표시됩니다.

보호 계획에 사용된 백업 위치가 **백업 스토리지** 탭에 자동으로 추가됩니다. 백업 위치 목록에 사용자 정의 폴더(예: 분리식 USB 장치)를 추가하려면 **찾아보기**를 클릭해 폴더 경로를 지정합니다.

경고!
백업 파일 수동 편집을 시도하지 마십시오. 백업 파일을 수동으로 편집하면 파일이 손상되어 백업을 사용하지 못하게 될 수 있습니다. 또한 백업 파일을 수동으로 이동하는 대신 백업을 내보내거나 백업 복제를 사용하는 것이 좋습니다.

백업 스토리지 탭을 사용하여 복구 지점을 선택하려면

1. **백업 스토리지** 탭에서 백업이 저장된 위치를 선택합니다.
   선택한 위치에서 사용자의 계정이 볼 수 있도록 허용된 모든 백업이 표시됩니다. 백업은 그룹으로 묶여 있습니다. 그룹 이름은 다음 템플릿에 따라 지정되어 있습니다.
   <머신 이름> - <보호 계획 이름>
2. 데이터를 복구하려는 그룹을 선택합니다.
3. [선택 사항] **다음 위치에서 탐색할 머신** 옆에 있는 **변경**을 클릭한 다음 다른 머신을 선택합니다. 일부 백업은 특정 에이전트에서만 찾을 수 있습니다. 예를 들어 Microsoft SQL Server 데이터베이스의 백업을 찾으려면 Agent for SQL을 실행 중인 머신을 선택해야 합니다.

   중요
   실제 머신 백업에서 복구하는 경우 **다음 위치에서 탐색할 머신**이 기본 목적지입니다. 복구 지점을 선택하고 **복구**를 클릭한 후에는 **대상 머신** 설정을 다시 한 번 살펴보고 특정 머신으로 복구할지 확인합니다. 복구 목적지를 변경하려면 **다음 위치에서 탐색할 머신**에서 다른 머신을 지정합니다.

4. **백업 표시**를 클릭합니다.
5. 복구 지점을 선택합니다.

백업에서 볼륨 마운트

디스크 수준 백업에서의 볼륨 마운트를 통해 실제 디스크인 것처럼 볼륨에 액세스할 수 있습니다.

읽기/쓰기 모드에서 볼륨 마운트를 통해 백업 내용을 수정할 수 있습니다. 즉, 파일 또는 폴더를 저장, 이동, 생성, 삭제하고 하나의 파일을 구성하는 실행 파일을 실행합니다. 이 모드에서 소프트웨어는 백업 내용의 변경 사항을 포함한 증분 백업을 생성합니다. 후속 백업에는 이러한 변경 사항이 포함되지 않습니다.

요구 사항

- 이 기능은 파일 탐색기를 사용하여 Windows에서만 이용할 수 있습니다.
- Agent for Windows는 마운트 작업을 수행하는 머신에 설치되어야 합니다.
- 백업된 파일 시스템은 머신이 실행 중인 Windows 버전에서 지원해야 합니다.
- 백업은 로컬 폴더, 네트워크 공유(SMB/CIFS) 또는 Secure Zone에 저장해야 합니다.

사용 시나리오

- **데이터 공유**

  마운팅된 볼륨은 네트워크에서 쉽게 공유할 수 있습니다.
- **"임시 처방" 데이터베이스 복구 솔루션**

  최근 실패한 머신에서 SQL 데이터베이스를 포함하는 볼륨을 마운트합니다. 이 작업은 실패한 머신을 복구할 때까지 데이터베이스에 대한 액세스 권한을 제공합니다. 이 접근법은 SharePoint 탐색기를 사용하여 Microsoft SharePoint 데이터의 개별 복구에 사용할 수도 있습니다.
- **오프라인 바이러스 제거**

  머신이 감염된 경우 백업을 마운트하고 바이러스 백신 프로그램으로 바이러스를 삭제하거나 감염되지 않은 최신 백업을 찾은 다음 이 백업에서 머신을 복구합니다.
- **오류 확인**

  볼륨 크기 조정 복구에 실패한 경우 백업된 파일 시스템에 오류가 발생했기 때문일 수 있습니다. 읽기/쓰기 모드에서 백업을 마운트하십시오. 그런 다음 **chkdsk /r** 명령을 사용하여 마운트된 볼륨에서 오류가 있는지 확인합니다. 오류가 수정되고 새 증분 백업이 생성되면 이 백업에서 시스템을 복구합니다.

백업에서 볼륨을 마운트하려면

1. 파일 탐색기를 사용하여 백업 위치를 찾습니다.
2. 백업 파일을 두 번 클릭합니다. 기본적으로 파일 이름은 다음 템플릿에 따라 지정되어 있습니다.

   <머신 이름> - <보호 계획 GUID>
3. 백업이 암호화되어 있는 경우 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.

   파일 탐색기가 복구 지점을 표시합니다.
4. 복구 지점을 두 번 클릭합니다.

파일 탐색기가 백업된 볼륨을 표시합니다.

참고
내용을 찾으려는 볼륨을 두 번 클릭합니다. 백업에서 파일 및 폴더를 파일 시스템에 있는 폴더에 복사할 수 있습니다.

5. 볼륨을 마우스 오른쪽 버튼으로 클릭하여 마운트한 후 다음 중 하나를 클릭합니다.
   - **마운트**

     참고
     아카이브(백업 체인)의 마지막 백업만 읽기/쓰기 모드로 마운트할 수 있습니다.

   - **읽기 전용 모드로 마운트**
6. 백업이 네트워크 공유에 저장된 경우 액세스 자격 증명을 제공합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   소프트웨어가 선택한 볼륨을 마운트합니다. 사용하지 않은 첫 글자가 볼륨에 할당됩니다.

볼륨을 마운트 해제하려면

1. 파일 탐색기를 사용하여 **컴퓨터**(Windows 8.1 이상에서는 **이 PC**)로 이동합니다.
2. 마운트된 볼륨을 마우스 오른쪽 버튼으로 클릭합니다.
3. **마운트 해제**를 클릭합니다.
4. 볼륨이 읽기/쓰기 모드에서 마운트되고 내용이 수정된 경우 변경 사항을 포함하는 증분 백업을 생성할지 여부를 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   소프트웨어가 선택한 볼륨을 마운트 해제합니다.

백업 유효성 검사

유효성 검사는 백업에서 데이터를 복구할 수 있는지 그 가능성을 확인하는 작업입니다. 이 작업에 대한 자세한 내용은 "유효성 검사"(321페이지)을(를) 참조하십시오.

백업 유효성을 검사하려면

1. 백업된 워크로드를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   워크로드가 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 워크로드를 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다. 클라우드나 공유 스토리지의 백업에 대한 자세한 내용은 "백업 스토리지 탭"(314페이지)을(를) 참조하십시오.
4. 기어 아이콘을 클릭하고 **유효성 검사**를 클릭합니다.
5. 유효성 검사를 수행할 에이전트를 선택합니다.
6. 유효성 검사 방법을 선택합니다.

7. 백업이 암호화되어 있는 경우 암호화 비밀번호를 제공합니다.
8. **시작**을 클릭합니다.

백업 내보내기

내보내기 작업은 사용자가 지정한 위치에 백업의 자급식 사본을 만듭니다. 원본 백업은 그대로 남아 있습니다. 내보내기를 사용하면 빠른 복구를 위해 증분 및 차등 백업의 체인에서 지정한 백업을 분리하고 이동식 또는 분리 가능한 미디어에 또는 다른 목적으로 쓸 수 있습니다.

내보내기 작업의 결과는 항상 전체 백업입니다. 전체 백업 체인을 다른 위치로 복제하고 여러 복구 지점을 유지하려면 백업 복제 계획을 사용하십시오.

내보낸 백업의 백업 파일 이름은 백업 형식 옵션의 값에 따라 정해집니다.

- 백업 구성표에 상관없이 **버전 12** 형식의 경우 백업 파일 이름은 시퀀스 번호만 제외하고 원래 백업의 파일 이름과 동일합니다. 같은 백업 체인의 여러 백업을 같은 위치로 내보낸 경우에는 첫 번째 백업을 제외하고, 모든 백업의 파일 이름에 네 자리 순차 번호가 붙습니다.
- **항상 증분(단일 파일)** 백업 구성표를 사용한 **버전 11** 형식의 경우 백업 파일 이름이 원래 백업의 백업 파일 이름과 똑같습니다. 같은 백업 체인의 여러 백업을 같은 위치로 내보낸 경우에는 모든 내보내기 작업이 이전에 내보낸 백업을 덮어씁니다.
- 다른 백업 구성표를 가진 **버전 11** 형식의 경우 백업 파일 이름은 타임 스탬프만 제외하고 원래 백업의 파일 이름과 동일합니다. 내보낸 백업의 타임스탬프는 내보내기를 수행한 시간과 일치합니다.

내보낸 백업은 원래 백업에서 암호화 설정 및 비밀번호를 상속합니다. 암호화된 백업을 내보낼 때에는 비밀번호를 지정해야 합니다.

백업을 내보내려면

1. 백업된 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 온라인 상태인 대상 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
4. 기어 아이콘을 클릭하고 **내보내기**를 클릭합니다.
5. 내보내기를 수행할 에이전트를 선택합니다.
6. 백업이 암호화되어 있는 경우 암호화 비밀번호를 제공합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
7. 내보내기 대상을 지정합니다.
8. **시작**을 클릭합니다.

백업 삭제

경고!
백업이 삭제되면 해당 백업의 모든 데이터가 영구적으로 삭제됩니다. 삭제된 데이터는 복구할 수 없습니다.

Cyber Protect 웹 콘솔에 있는 온라인 머신의 백업 삭제 방법

1. **모든 장치** 탭에서 백업을 삭제하려는 머신을 선택합니다.
2. **복구**를 클릭합니다.
3. 백업을 삭제하려는 위치를 선택합니다.
4. 다음 중 하나를 수행하십시오.
   - 단일 백업을 삭제하려면 삭제할 백업을 선택한 다음 기어 아이콘을 클릭하고 **삭제**를 클릭합니다.
   - 선택한 위치에 있는 백업을 모두 삭제하려면 **모두 삭제**를 클릭합니다.
5. 결정을 확인합니다.

머신의 백업을 삭제하려면

1. **백업 스토리지** 탭에서 백업을 삭제하려는 위치를 선택합니다.
   선택한 위치에서 사용자의 계정이 볼 수 있도록 허용된 모든 백업이 표시됩니다. 백업은 그룹으로 묶여 있습니다. 그룹 이름은 다음 템플릿에 따라 지정되어 있습니다.
   <머신 이름> - <보호 계획 이름>
2. 그룹을 선택합니다.
3. 다음 중 하나를 수행하십시오.
   - 단일 백업을 삭제하려면 **백업 표시**를 클릭하고 삭제할 백업을 선택한 다음 기어 아이콘을 클릭하고 **삭제**를 클릭합니다.
   - 선택한 그룹을 삭제하려면 **삭제**를 클릭합니다.
4. 결정을 확인합니다.

클라우드 스토리지에서 바로 백업을 삭제하려면

1. "클라우드 스토리지에서 파일 다운로드"에 설명된 대로 클라우드 스토리지에 로그인합니다.
2. 백업을 삭제하고자 하는 머신의 이름을 클릭합니다.
   소프트웨어가 하나 이상의 백업 그룹을 표시합니다.
3. 삭제하려는 백업 그룹 옆의 해당 기어 아이콘을 클릭합니다.
4. **제거**를 클릭합니다.
5. 작업을 확인합니다.

계획 탭

Advanced 라이센스가 있으면 **계획** 탭을 사용하여 보호 계획 및 기타 계획을 관리할 수 있습니다.

계획 탭의 각 섹션에는 특정 유형의 모든 계획이 포함됩니다. 다음 섹션을 사용할 수 있습니다.

- 보호
- 백업 스캔
- 백업 복제
- 유효성 검사
- 정리
- VM으로 변환
- VM 복제
- 부트 가능한 미디어. 이 섹션에는 부트 가능한 미디어에서 부팅된 머신에 대해 생성되었고 해당 머신에만 적용할 수 있는 보호 계획이 표시됩니다.

각 섹션에서 계획을 생성, 편집, 비활성화, 활성화, 삭제 및 시작하고 계획의 실행을 모니터링할 수 있습니다.

복제와 중지는 보호 계획에 대해서만 사용할 수 있습니다. **장치** 탭에서 백업을 중지하는 것과 달리 보호 계획을 중지하면 이 계획이 적용된 모든 장치에서 백업이 중지됩니다. 여러 장치의 백업 시작 시간이 시간 창 내에 분산된 경우 보호 계획을 중지하면 실행 중인 백업이 중지되거나 백업이 시작되지 않습니다.

계획을 파일로 내보내고 이전에 내보낸 계획을 가져올 수도 있습니다.

오프호스트 데이터 처리

보호 계획에 포함된 복제, 유효성 검사 및 보관 규칙 적용과 같은 대부분의 작업은 백업을 수행하는 에이전트에서 수행됩니다. 이로 인해 백업 프로세스가 완료된 후에도 에이전트가 실행 중인 머신에 워크로드가 추가됩니다.

맬웨어 방지 스캔, 복제, 유효성 검사, 정리 및 변환 계획을 보호 계획에서 분리하면 다음과 같은 유연성이 제공됩니다:

- 이러한 작업을 수행할 또 다른 에이전트 선택 가능
- 네트워크 대역폭 소비를 최소화하도록 이러한 작업을 사용량이 많지 않은 시간으로 스케줄 가능
- 이러한 작업을 비즈니스 시간 이외의 시간으로 이동 가능(전용 에이전트 설정이 계획에 없는 경우)

스토리지 노드를 사용할 경우 같은 머신에 전용 에이전트를 설치해야 합니다.

에이전트를 구동하는 머신의 시간 설정을 적용하는 백업 및 VM 복제 계획과 다르게, 오프호스트 데이터 프로세싱 계획은 관리 서버 머신의 시간 설정에 따라 실행됩니다.

백업 스캔 계획

지원되는 위치

다음 위치에서 멀웨어 대비 백업을 스캔할 수 있습니다. **클라우드 스토리지**, **로컬 폴더**, **네트워크 폴더**. 스캔된 머신에 설치된 에이전트만 **로컬 폴더** 위치에 액세스할 수 있습니다.

백업 스캔과 그 한계에 대한 자세한 정보는 "백업의 맬웨어 방지 스캔"을 참고하십시오.

백업 스캔 계획을 생성하려면

1. Cyber Protect 웹 콘솔에서 **계획** > **백업 스캔**을 클릭합니다.
2. **계획 생성**을 클릭합니다.
3. [선택 사항] 계획 이름을 수정하려면 연필 아이콘 옆의 기본 이름을 클릭합니다.
4. 스캔 에이전트를 선택합니다.
5. 스캔할 백업 위치 또는 개별 백업을 선택합니다.
   한 번에 여러 백업 위치를 선택할 수 있습니다. 한 계획에 여러 개별 백업을 포함하려면 백업을 하나씩 추가해야 합니다.
6. [**클라우드 스토리지**나 **네트워크 폴더** 선택 시] 메시지가 표시되면 백업 스토리지에 액세스하기 위한 자격 증명을 입력합니다.
7. [암호화된 백업 선택 시] 백업에 액세스하기 위한 비밀번호를 지정하십시오. 볼트 또는 여러 암호화된 백업이 선택된 경우, 단일 비밀번호를 지정할 수 있습니다. 특정 백업에 대한 암호가 틀리면, 알림이 표시됩니다. 암호가 일치하는 백업만 스캔됩니다.
8. 스캔 예약을 구성합니다.
9. 준비가 되면 **생성**을 클릭합니다.

결과적으로 백업 스캔 계획이 생성됩니다.

백업 복제

지원되는 위치

다음 표에는 백업 복제 계획에서 지원되는 백업 위치가 요약되어 있습니다.

위치:	소스로 지원됨	대상으로 지원됨
클라우드 스토리지	+	+
로컬 폴더	+	+
네트워크 폴더	+	+
NFS 폴더	–	–
Secure Zone	–	–

SFTP 서버	–	–
관리 위치*	+	+
테이프 장치	–	+

* "고급 라이센스를 사용하는 사용자에 대한 고려 사항"(237페이지) 항목에 설명된 제한 사항을 확인하십시오.

백업 복제 계획 생성 방법

1. **계획** > **백업 복제**를 클릭합니다.
2. **계획 생성**을 클릭합니다.
   소프트웨어에 새 계획 템플릿이 표시됩니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **에이전트**를 클릭하고 복제를 수행할 에이전트를 선택합니다.
   소스 및 대상 백업 위치에 액세스할 수 있는 모든 에이전트를 선택할 수 있습니다.
5. **복제할 항목**을 클릭한 다음 이 계획에서 복제할 백업을 선택합니다.
   오른쪽 위에 있는 **위치 / 백업** 스위치를 사용하여 백업 선택과 전체 위치 선택 간에 전환할 수 있습니다.
   선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
6. **목적지**를 클릭하고 대상 위치를 지정합니다.
7. [선택 사항] **복제 방법**에서 복제할 백업을 선택합니다. 다음 중 하나를 선택합니다.
   - **모든 백업**(기본값)
   - **전체 백업만**
   - **마지막 백업만**
8. [선택 사항] **스케줄**을 클릭하고 스케줄을 변경합니다.
9. [선택 사항] **보관 규칙**을 클릭한 다음 "보관 규칙"의 설명에 따라 대상 위치에 대한 보관 규칙을 지정합니다.
10. **복제할 항목**에서 선택한 백업이 암호화되면 **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
11. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
12. **생성**을 클릭합니다.

유효성 검사

유효성 검사는 백업에서 데이터를 복구할 수 있는지 그 가능성을 확인하는 작업입니다.

백업 위치의 유효성 검사는 위치에 저장된 모든 백업의 유효성을 검사합니다.

작동법

유효성 검사 계획은 두 가지 유효성 검사 방법을 제공합니다. 두 방법을 모두 선택하는 경우 작업이 연속해서 수행됩니다.

- **백업에 저장되어 있는 모든 데이터 블록의 체크섬 계산**

  체크섬 계산을 통한 유효성 검사에 대한 자세한 내용은 "백업 유효성 검사"를 참조하십시오.
- **백업에서 가상 머신 실행**

  이 방법은 운영 체제가 포함된 디스크 수준 백업에만 적용됩니다. 이 방법을 사용하려면 ESXi 또는 Hyper-V 호스트와 이 호스트를 관리하는 보호 에이전트(Agent for VMware 또는 Agent for Hyper-V)가 필요합니다.

  에이전트가 백업에서 가상 머신을 실행하고 나서 VMware Tools 또는 Hyper-V Heartbeat Service에 연결하여 운영 체제가 성공적으로 시작되었는지 확인합니다. 연결에 실패하는 경우 에이전트는 2분마다 한 번씩, 총 5회까지 연결을 시도합니다. 시도가 모두 실패하는 경우 유효성 검사에 실패합니다.

  유효성 검사 계획 및 유효성을 검사한 백업의 수에 관계없이 유효성 검사를 수행하는 에이전트는 한 번에 가상 머신 한 대를 실행합니다. 유효성 검사 결과가 정상으로 나오는 즉시 에이전트는 해당 가상 머신을 삭제하고 다음 머신을 실행합니다.

유효성 검사에 실패하면 **개요** 탭의 **활동** 탭에서 세부 정보를 살펴볼 수 있습니다.

지원되는 위치

다음 표에는 유효성 검사 계획에서 지원되는 백업 위치가 요약되어 있습니다.

위치:	체크섬 계산	VM 실행
클라우드 스토리지	+	+
로컬 폴더	+	+
네트워크 폴더	+	+
NFS 폴더	–	–
Secure Zone	–	–
SFTP 서버	–	–
관리 위치	+	+
테이프 장치	+	–

새 유효성 검사 계획 생성 방법

1. **계획** > **유효성 검사**를 클릭합니다.
2. **계획 생성**을 클릭합니다.

   소프트웨어에 새 계획 템플릿이 표시됩니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **에이전트**를 클릭하고 유효성 검사를 수행할 에이전트를 선택합니다.

   백업에서 가상 머신을 실행하여 유효성 검사를 수행하려면 Agent for VMware 또는 Agent for Hyper-V를 선택하십시오. 그렇지 않으면 관리 서버에 등록되어 있고 백업 위치에 액세스할 수 있는 에이전트를 선택합니다.

5. **유효성 검사할 항목**을 클릭한 다음 이 계획에서 유효성 검사할 백업을 선택합니다.
   오른쪽 위에 있는 **위치 / 백업** 스위치를 사용하여 백업 선택과 전체 위치 선택 간에 전환할 수 있습니다.
   선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
6. [선택 사항] **유효성 검사 대상**에서 유효성을 검사할 백업을 선택합니다. 다음 중 하나를 선택합니다.
   - **모든 백업**
   - **마지막 백업만**
7. [선택 사항] **유효성 검사 방법**을 클릭하고 다음 방법 중 하나를 선택합니다.
   - **체크섬 확인**
     백업에 저장되어 있는 모든 데이터 블록의 체크섬이 계산됩니다.
   - **가상 머신으로 실행**
     각 백업에서 가상 머신이 실행됩니다.
8. **가상 머신으로 실행**을 선택하는 경우:
   a. **대상 머신**을 클릭하고 가상 머신 유형(ESXi 또는 Hyper-V), 호스트 및 머신 이름 템플릿을 선택합니다.
      기본 이름은 **[머신 이름]_validate**입니다.
   b. ESXi의 경우 **데이터 저장소**를, Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소를 선택합니다.
   c. [선택 사항] 디스크 프로비저닝 모드를 변경합니다.
      기본 설정은 **씬**(VMware ESXi) 및 **동적 확장**(Hyper-V)입니다.
   d. [선택 사항] **VM 설정**을 클릭하여 가상 머신의 메모리 크기 및 네트워크 연결을 변경합니다.
      기본적으로 가상 머신은 네트워크에 연결되지 *않으며* 가상 머신 메모리 크기는 원래 머신의 메모리 크기와 동일합니다.

   참고
   VM 하트비트 스위치는 항상 활성화되어 있습니다. 백업에서 가상 머신을 실행하여 게스트 운영 체제의 하이퍼바이저 도구(VMware Tools 또는 Hyper-V Integration Services)가 보고하는 가상 머신의 하트비트 상태 유효성을 검사해야 하기 때문입니다. 이 스위치는 이후 릴리스에서 제공될 예정이므로 현재는 사용할 수 없습니다.

9. [선택 사항] **스케줄**을 클릭하고 스케줄을 변경합니다.
10. **유효성 검사할 항목**에서 선택한 백업이 암호화되면 **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
11. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
12. **생성**을 클릭합니다.

정리

정리는 보관 규칙에 따라 오래된 백업을 삭제하는 작업입니다.

지원되는 위치

정리 계획은 NFS 폴더, SFTP 서버 및 Secure Zone을(를) 제외한 모든 백업 위치를 지원합니다.

새 정리 계획 생성 방법

1. **계획** > **정리**를 클릭합니다.
2. **계획 생성**을 클릭합니다.
   소프트웨어에 새 계획 템플릿이 표시됩니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **에이전트**를 클릭하고 정리를 수행할 에이전트를 선택합니다.
   백업 위치에 액세스할 수 있는 모든 에이전트를 선택할 수 있습니다.
5. **정리할 항목**을 클릭한 다음 이 계획에서 정리할 백업을 선택합니다.
   오른쪽 위에 있는 **위치 / 백업** 스위치를 사용하여 백업 선택과 전체 위치 선택 간에 전환할 수 있습니다.
   선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
6. [선택 사항] **스케줄**을 클릭하고 스케줄을 변경합니다.
7. [선택 사항] **보관 규칙**을 클릭하고 "보관 규칙"의 설명에 따라 보관 규칙을 지정합니다.
8. **정리할 항목**에서 선택한 백업이 암호화되면 **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
10. **생성**을 클릭합니다.

가상 머신으로 전환

가상 머신으로 전환을 위한 별도의 계획을 생성하고, 이 계획을 수동으로 또는 스케줄에 따라 실행할 수 있습니다.

사전 요구 사항과 제한 사항에 대한 자세한 내용은 "통합에 대해서 알아야 할 사항"을 참조하십시오.

가상 머신으로 전환을 위한 계획 생성

1. **계획** > **VM으로 변환**을 클릭합니다.
2. **계획 생성**을 클릭합니다.
   소프트웨어에 새 계획 템플릿이 표시됩니다.
3. [선택 사항] 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **변환 대상**에서 대상 가상 머신의 유형을 선택합니다. 다음 중 하나를 선택합니다.
   - **VMware ESXi**
   - **Microsoft Hyper-V**
   - **Scale Computing HC3**
   - **VMware Workstation**

- **VHDX 파일**

  참고
  스토리지 공간을 절약하기 위해 VHDX 파일로 변환할 때마다 대상 위치에서 이전 변환 시 생성된 VHDX 파일을 덮어씁니다.

5. 다음 중 하나를 수행하십시오.
   - [VMware ESXi, Hyper-V 및 Scale Computing HC3] **호스트**를 클릭하고 대상 호스트를 선택한 후 새 머신 이름 템플릿을 지정합니다.
   - [기타 가상 머신 유형] **경로**에서 가상 머신 파일 및 파일 이름 템플릿을 저장할 위치를 지정합니다.

   기본 이름은 **[머신 이름]_converted**입니다.
6. **에이전트**를 클릭하고 변환을 수행할 에이전트를 선택합니다.
7. **변환할 항목**을 클릭한 다음 이 계획에서 가상 머신으로 변환할 백업을 선택합니다.
   오른쪽 위에 있는 **위치 / 백업** 스위치를 사용하여 백업 선택과 전체 위치 선택 간에 전환할 수 있습니다.
   선택한 백업이 암호화되어 있는 경우 모든 백업이 같은 암호화 비밀번호를 사용해야 합니다. 다른 암호화 비밀번호를 사용하는 백업의 경우 개별 계획을 생성합니다.
8. [VMware ESXi 및 Hyper-V에만 해당] ESXi의 경우 **데이터 저장소** 또는 Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
9. [VMware ESXi 및 Hyper-V에만 해당됨] 디스크 프로비저닝 모드를 선택합니다. 기본 설정은 **씬**(VMware ESXi) 및 **동적 확장**(Hyper-V)입니다.
10. [선택 사항] [VMware ESXi, Hyper-V 및 Scale Computing HC3] **VM 설정**을 클릭해 메모리 크기, 프로세서 수 또는 가상 머신의 네트워크 연결을 수정합니다.
11. [선택 사항] **스케줄**을 클릭하고 스케줄을 변경합니다.
12. **변환할 항목**에서 선택한 백업이 암호화되면 **백업 비밀번호** 스위치를 활성화하고 암호화 비밀번호를 입력합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
13. [선택 사항] 계획 옵션을 수정하려면 기어 아이콘을 클릭합니다.
14. **생성**을 클릭합니다.

부트 가능한 미디어

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

부트 가능한 미디어

부트 가능한 미디어는 보호 에이전트를 Linux 기반 환경 또는 WinPE(Windows 사전 설치 환경)에서 운영 체제의 도움 없이 실행할 수 있는 물리적 미디어(CD, DVD, USB 플래시 드라이브 또는 머신의 BIOS가 부트 장치로 지원하는 기타 이동식 미디어)입니다.

부트 가능한 미디어는 대부분 다음 작업에 사용됩니다.

- 시작할 수 없는 운영 체제를 복구
- 손상된 시스템에서 살아 남은 데이터에 액세스하고 백업
- 운영 체제를 베어 메탈에 디플로이
- 베어 메탈에 기본 또는 동적 볼륨 만들기
- 지원되지 않는 파일 시스템이 있는 디스크를 섹터별로 백업
- 실행 중인 응용 프로그램에 의해 잠겨 있거나 액세스 제한 등으로 온라인에 백업할 수 없는 데이터를 오프라인으로 백업합니다.

머신은 Acronis PXE Server, WDS(Windows Deployment Services) 또는 RIS(Remote Installation Services)에서 네트워크 부트를 사용하여 부팅할 수도 있습니다. 업로드된 부트 가능한 컴퍼넌트가 있는 이러한 서버 또한 부트 가능한 미디어의 한 유형으로 간주할 수 있습니다. 따라서 동일 마법사를 사용하여 부트 가능한 미디어를 생성하거나 PXE 서버 또는 WDS/RIS를 구성할 수 있습니다.

부트 가능한 미디어를 생성하거나 이미 생성된 미디어를 다운로드하시겠습니까?

Bootable Media Builder를 사용하면 Windows, Linux 또는 macOS 컴퓨터용으로 부트 가능한 자체 미디어(Linux 기반 또는 WinPE 기반)를 생성할 수 있습니다. 완전한 기능의 부트 가능한 미디어를 생성하려면 Acronis Cyber Protect 라이센스 키를 지정해야 합니다. 이 키가 없으면 부트 가능한 미디어가 복구 작업만 수행할 수 있습니다.

참고
부트 가능한 미디어는 하이브리드 드라이브를 지원하지 않습니다.

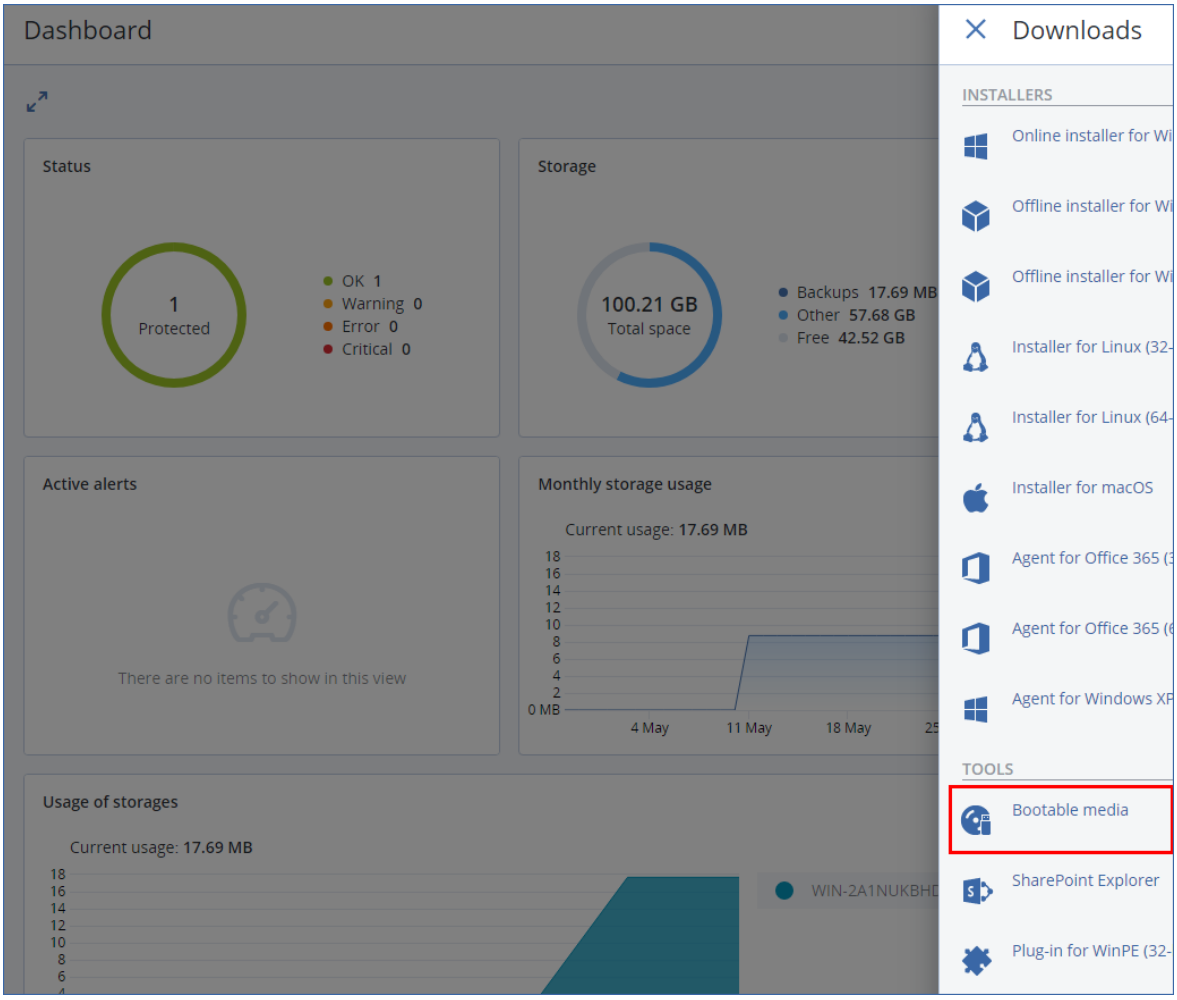
또한 이미 생성된 부트 가능한 미디어(Linux 기반만 해당)를 다운로드할 수 있습니다. 다운로드한 부트 가능한 미디어는 복구 작업이나 Acronis Universal Restore에 대한 액세스에만 사용할 수 있습니다. 이 미디어로 데이터를 백업하거나, 백업 데이터를 확인하고 내보내거나, 디스크를 관리하거나, 스크립트를 사용할 수는 없습니다. 다운로드한 부트 가능한 미디어는 macOS 컴퓨터에 적합하지 않습니다.

참고

이미 생성된 부트 가능한 미디어는 스토리지 노드, 테이프 위치 및 SFTP 위치를 지원하지 않습니다. 온프레미스 디플로이에서 이러한 스토리지 위치를 사용하려는 경우 Bootable Media Builder를 사용하여 부트 가능한 자체 미디어를 생성해야 합니다. https://kb.acronis.com/content/61566을 참조하십시오.

이미 생성된 부트 가능한 미디어를 다운로드하는 방법

1. Cyber Protect 웹 콘솔의 오른쪽 상단에 있는 계정 아이콘을 클릭하고 **다운로드**를 클릭합니다.
2. **부트 가능한 미디어**를 선택합니다.



온라인에서 사용 가능한 무료 도구 중 하나를 사용하여 다운로드한 ISO 파일을 CD/DVD로 굽거나 부트 가능한 USB 플래시 드라이브를 생성할 수 있습니다. UEFI 머신을 부트하려는 경우에는 `ISO-USB` 또는 `RUFUS`를 사용하고 BIOS 머신의 경우에는 `Win32DiskImager`를 사용합니다. Linux에서는 `dd` 유틸리티를 사용합니다.

Cyber Protect 웹 콘솔에 액세스할 수 없는 경우 Acronis Customer Portal의 사용자 계정에서 이미 생성된 부트 가능한 미디어를 다운로드할 수 있습니다.

1. https://account.acronis.com으로 이동합니다.
2. Acronis Cyber Protect을(를) 찾고 **다운로드**를 클릭합니다.
3. 페이지가 열리면 **추가 다운로드**를 찾고 **부트 가능한 미디어 ISO(Windows 및 Linux용)**를 클릭합니다.

Linux 기반 및 WinPE 기반 부트 가능한 미디어의 특징

Linux 기반

Linux 기반 부트 가능한 미디어에는 Linux 커널 기반의 부트 가능한 보호 에이전트가 포함됩니다. 에이전트는 베어 메탈 및 손상되거나 지원되지 않는 파일 머신이 있는 머신을 포함하여 PC와 호환되는 모든 하드웨어에서 부팅 및 작업을 수행할 수 있습니다. 작업은 Cyber Protect 웹 콘솔에서 로컬 또는 원격으로 구성하고 제어할 수 있습니다.

Linux 기반 미디어가 지원하는 하드웨어의 목록은 http://kb.acronis.com/content/55310에서 확인할 수 있습니다.

WinPE 기반

WinPE 기반 부트 가능한 미디어에는 WinPE(Windows 사전 설치 환경) 및 Acronis Plug-in for WinPE라고 하는 최소 Windows 시스템, 즉 사전 설치 환경에서 실행할 수 있는 보호 에이전트의 변형이 포함되어 있습니다.

WinPE는 이종 하드웨어가 있는 대규모 환경에서 가장 편리한 부트 가능한 솔루션으로 증명되었습니다.

장점:

- Windows 사전 설치 환경에서 Acronis Cyber Protect을(를) 사용하는 경우 Linux 기반 부트 가능한 미디어를 사용하는 것보다 더 많은 기능이 제공됩니다. PC 호환 가능 하드웨어를 WinPE로 부팅하면 보호 에이전트뿐만 아니라 PE 명령과 스크립트 및 PE에 추가한 기타 플러그인을 사용할 수도 있습니다.
- PE 기반 부트 가능한 미디어는 특정 RAID 컨트롤러 지원 또는 RAID 어레이의 특정 수준 등과 같은 몇몇 Linux와 관련된 부트 가능한 미디어 문제를 극복하는 데 도움이 됩니다. WinPE 2.x 이상에 기반을 둔 미디어는 필요한 장치 드라이버의 동적 로드를 지원합니다.

제한:

- WinPE 버전 4.0 이전에 기반을 둔 부트 가능한 미디어는 UEFI(Unified Extensible Firmware Interface)를 사용하는 머신에서 부팅되지 않습니다.
- 머신이 PE 기반 부트 가능한 미디어에서 부팅되면 백업 대상으로 CD, DVD 또는 BD(Blu-ray Discs)와 같은 광 미디어를 선택할 수 없습니다.

Bootable Media Builder

Bootable Media Builder는 부트 가능한 미디어를 생성하기 위한 전용 도구입니다. 온프레미스 디플로이에서만 사용할 수 있습니다.

Bootable Media Builder는 관리 서버를 설치할 때 기본적으로 설치됩니다. 이 미디어 제작기는 Windows나 Linux를 실행하는 모든 머신에 별도로 설치할 수 있습니다. 지원되는 운영 체제는 이에 상응하는 에이전트와 동일합니다.

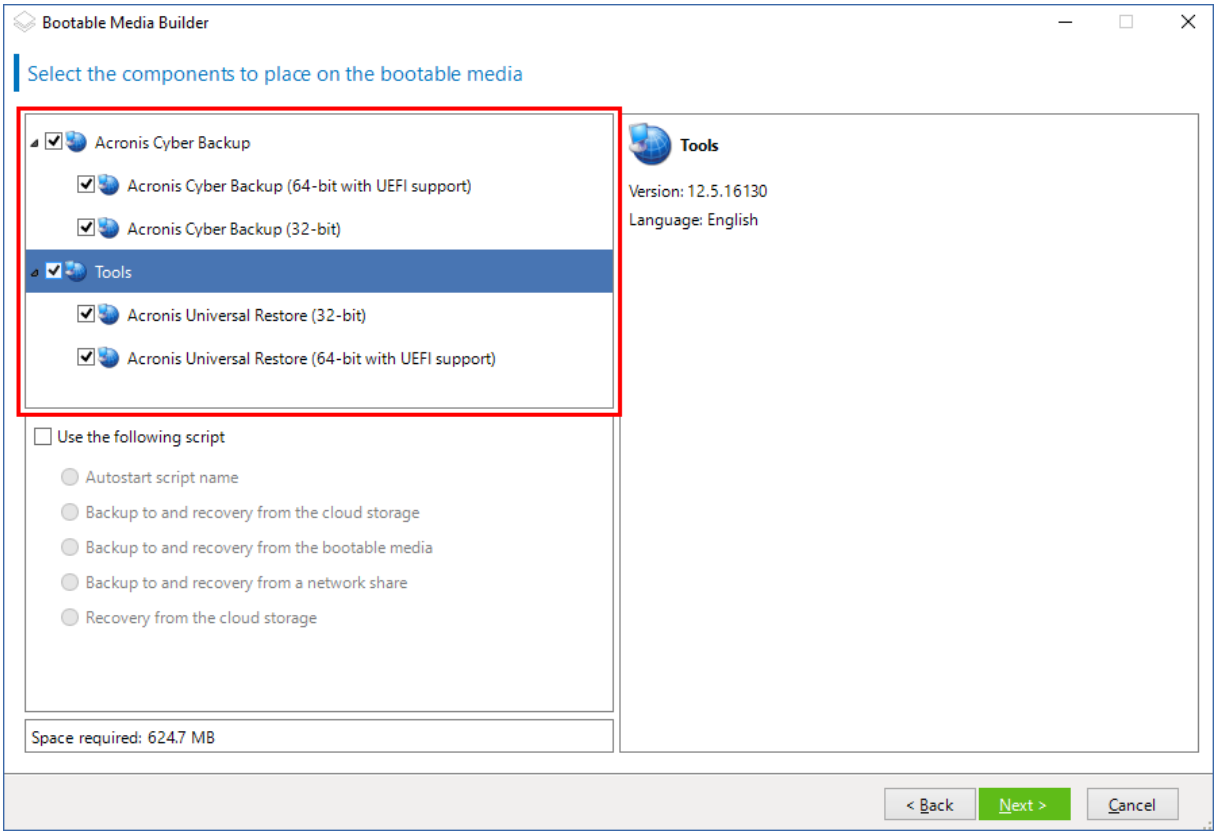
미디어 제작기를 사용하는 이유는 무엇일까요?

Cyber Protect 웹 콘솔에서 다운로드에 사용할 수 있는 이미 생성된 부트 가능한 미디어는 복구 목적으로만 사용할 수 있습니다. 이 미디어는 Linux 커널에 기반을 두고 있습니다. Windows PE와는 달리 여기에는 사용자 정의 드라이버를 쉽게 삽입할 수 없습니다.

- 미디어 제작기는 사용자가 사용자 정의된 완비 Linux 기반 및 WinPE 기반의 부트 가능한 미디어를 백업 기능으로 생성할 수 있게 해줍니다.
- 실제 부트 가능한 미디어와는 별도로 사용자는 Windows Deployment Services(WDS)에 구성 요소를 업로드하고 네트워크 부팅을 사용할 수 있습니다.
- 이미 생성된 부트 가능한 미디어는 스토리지 노드, 테이프 위치 및 SFTP 위치를 지원하지 않습니다. 로컬 온프레미스 디플로이에서 이러한 스토리지 위치를 사용하려는 경우 Bootable Media Builder를 사용하여 부트 가능한 자체 미디어를 생성해야 합니다. https://kb.acronis.com/content/61566을 참조하십시오.

32비트/64비트

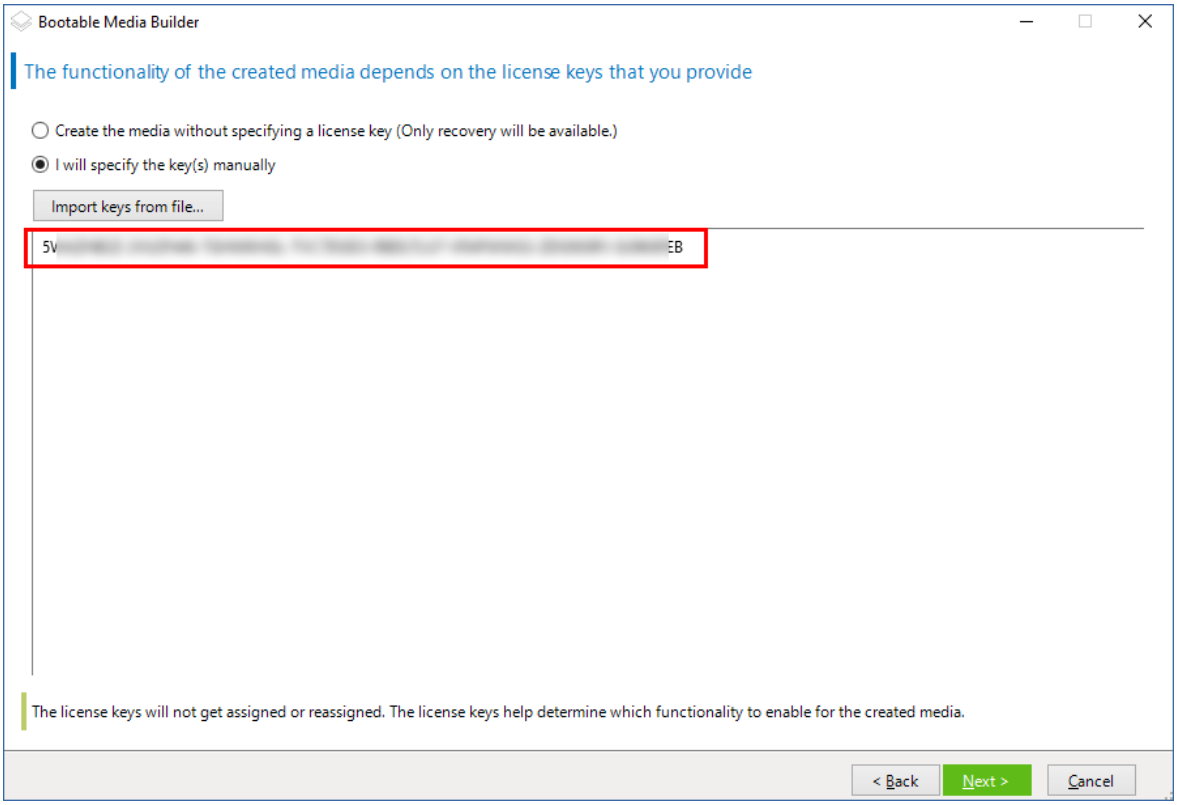
Bootable Media Builder는 32비트 및 64비트 구성 요소로 미디어를 생성합니다. 대부분의 경우 UEFI(통합 확장형 펌웨어 인터페이스)를 사용하는 머신을 부팅하려면 64비트 미디어가 필요합니다.



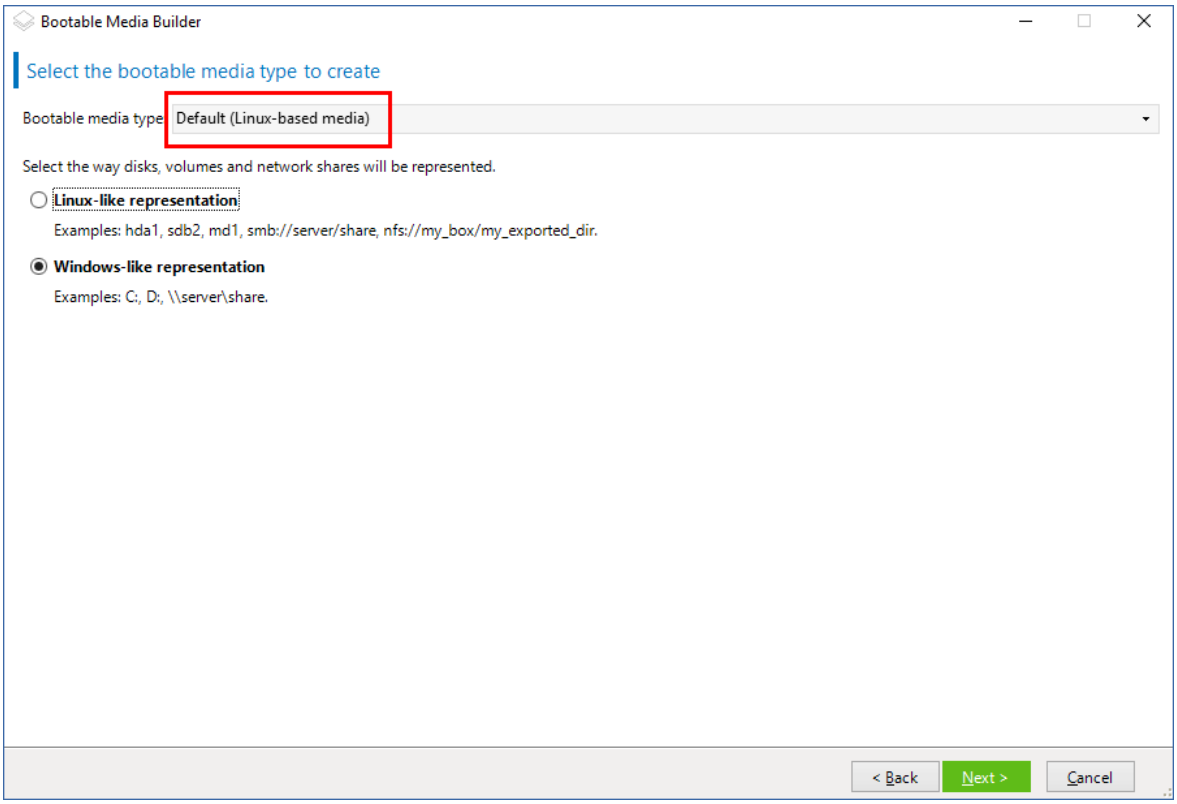
Linux 기반 부트 가능한 미디어

Linux 기반 부트 가능한 미디어를 생성하려면

1. **Bootable Media Builder**를 시작합니다.
2. 완전한 기능의 부트 가능한 미디어를 생성하려면 Acronis Cyber Protect 라이센스 키를 지정합니다. 키는 부트 가능한 미디어에 포함될 기능을 결정합니다. 라이센스는 어떤 머신에서도 철회되지 않습니다.
   라이센스 키를 지정하지 않으면 해당 부트 가능한 미디어는 복구 작업에만 사용할 수 있습니다.



3. **부트 가능한 미디어 유형: 기본값(Linux 기반 미디어)**을 선택합니다.
   볼륨 및 네트워크 리소스가 표시되는 방법을 선택합니다.
   - Linux와 같은 볼륨 표현 방식의 미디어는 볼륨을 예를 들어, hda1 및 sdb2로 표시합니다. 복원을 시작하기 전에 MD 장치 및 논리(LVM) 볼륨을 복구하려고 시도합니다.
   - Windows와 같은 볼륨 표현 방식의 미디어는 볼륨을 예를 들어 C:와 D:으로 표시합니다. 동적(LDM) 볼륨에 대한 액세스를 제공합니다.



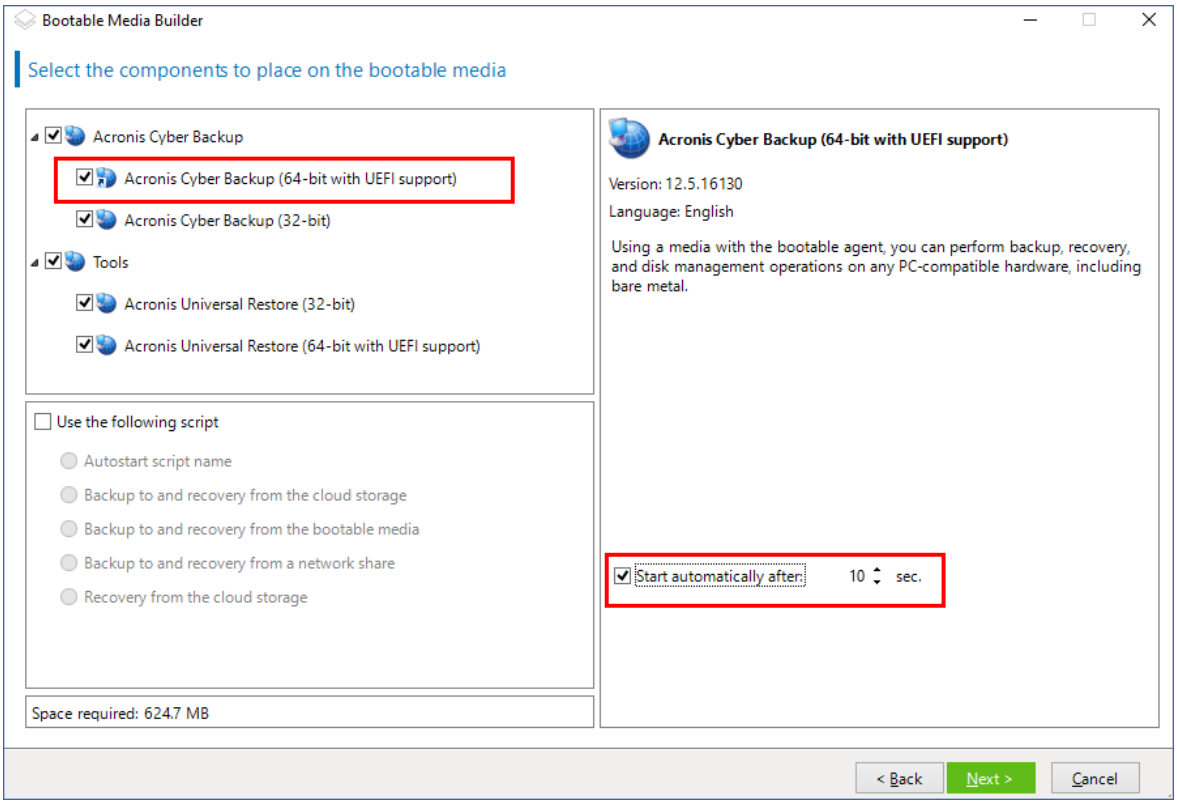
4. [선택 사항] Linux 커널의 매개변수를 지정합니다. 여러 개의 매개변수를 공백으로 구분합니다. 예를 들어 부트 가능한 에이전트에 대한 표시 모드를 선택하려면 미디어가 시작될 때마다 다음을 입력합니다. **vga=ask**

   사용 가능한 매개변수에 대한 자세한 내용은 커널 매개변수를 참고하십시오.
5. [선택 사항] 부트 가능한 미디어에서 사용할 언어를 선택합니다.
6. 미디어에 배치할 컴퍼넌트를 선택하십시오. Acronis Cyber Protect 부트 가능한 에이전트 및/또는 Universal Restore(이기종 하드웨어에서 시스템을 복구하려는 경우)가 해당됩니다.

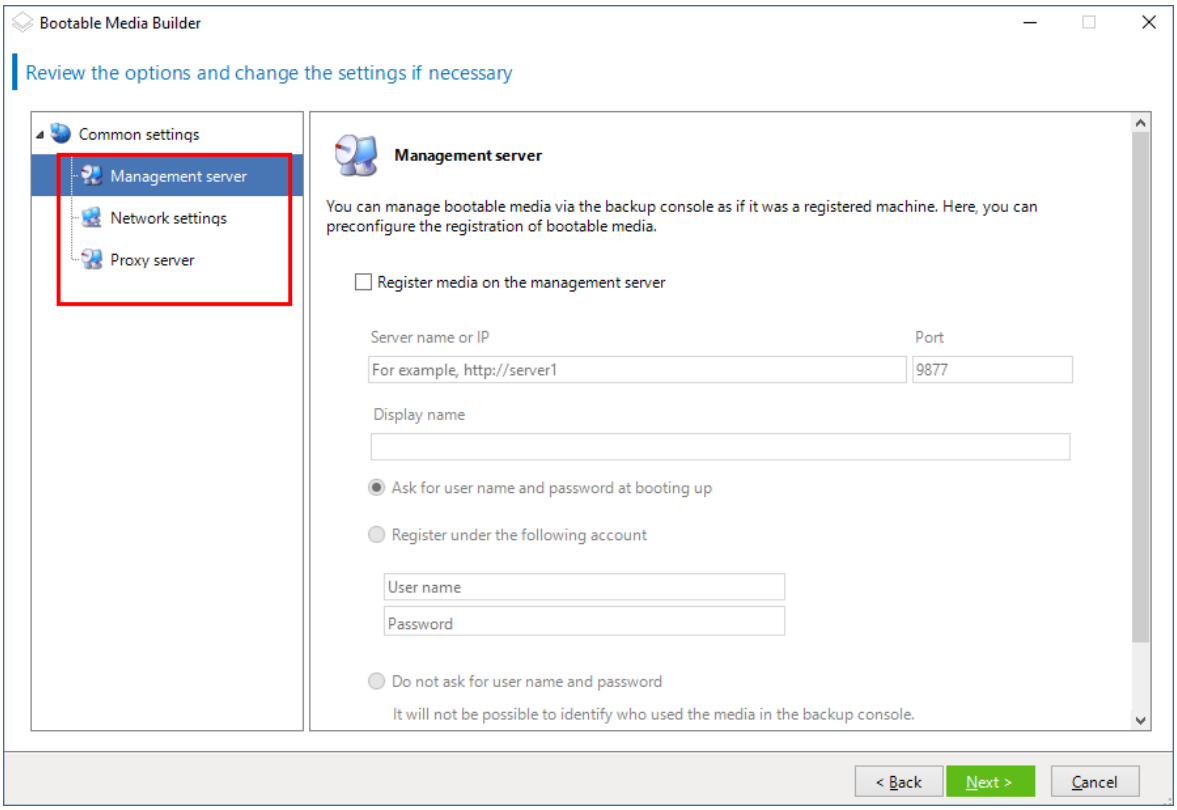
   부트 가능한 에이전트를 사용하면 베어 메탈을 포함한 PC 호환 하드웨어에서 백업, 복구 및 디스크 관리 작업을 수행할 수 있습니다.

   Universal Restore를 사용하면 이기종 하드웨어 또는 가상 머신으로 복구된 운영 체제를 부팅할 수 있습니다. 이 도구는 저장소 컨트롤러, 마더보드, 칩셋 등과 같이 운영 체제 시작에 중요한 장치를 위한 드라이버를 찾고 설치합니다.
7. [선택 사항] 부트 메뉴의 시간 초과 간격과 시간 초과 시 자동으로 시작되는 컴퍼넌트를 지정합니다. 이렇게 하려면 왼쪽 상단 창에서 원하는 컴퍼넌트를 클릭하고 간격을 설정합니다. 이로써 WDS/RIS에서 부팅할 때 무인 온사이트 작업이 가능해집니다.

   이 설정이 구성되지 않은 경우에는 운영 체제(있는 경우)를 부팅할지 또는 컴퍼넌트를 부팅할지 선택할 때까지 로더가 대기합니다.



8. [선택 사항] 부트 가능한 에이전트 작업을 자동화하려면 **다음 스크립트 사용** 확인란을 선택합니다. 그다음에 스크립트 중 하나를 선택하고 스크립트 매개변수를 지정합니다.
9. [선택 사항] 부트 시 관리 서버에 미디어를 등록하는 방법을 선택합니다. 등록 설정에 대한 자세한 내용은 관리 서버를 참조하십시오.



10. [선택 사항] 네트워크 설정 지정: 머신 네트워크 어댑터에 할당할 TCP/IP 설정. 자세한 내용은 "네트워크 설정"(343페이지) 항목을 참조하십시오.
11. [선택 사항] 네트워크 포트 지정: 부트 가능한 에이전트가 수신 연결을 수신 대기하는 TCP 포트.
12. [선택 사항] 프록시 서버가 사용자 네트워크에서 활성화된 경우 해당 호스트 이름/IP 주소 및 포트를 지정합니다.
13. 미디어 유형을 선택합니다. 다음을 수행할 수 있습니다.
    - ISO 이미지를 생성합니다. 그러면 CD/DVD로 구울 수 있습니다. 이를 사용하여 부팅 가능한 USB 플래시 드라이브를 생성하거나 가상 머신에 연결하십시오.
    - ZIP 파일을 생성합니다.
    - 선택한 컴퍼넌트를 Acronis PXE Server에 업로드합니다.
    - 선택한 컴퍼넌트를 WDS/RIS에 업로드
14. [선택 사항] Universal Restore에서 사용할 Windows 시스템 드라이버를 추가합니다. Universal Restore가 미디어에 추가되거나 WDS/RIS이외의 미디어가 선택된 경우에는 이 창이 나타납니다.
15. 메시지가 표시되면 WDS/RIS에 대한 호스트 이름/IP 주소 및 자격 증명 또는 미디어 ISO 파일의 경로를 지정합니다.
16. 요약 화면에서 설정을 확인하고 **진행**을 클릭합니다.

커널 매개변수

이 창을 사용하면 Linux 커널의 하나 이상의 매개변수를 지정할 수 있습니다. 이러한 매개변수는 부트 가능한 미디어를 시작할 때 자동으로 적용됩니다.

또한 일반적으로 부트 가능한 미디어로 작업하는 동안 문제가 발생할 때 사용됩니다. 보통은 이 필드를 비워둘 수 있습니다.

부트 메뉴에서 F11 키를 눌러 이러한 매개변수를 지정할 수도 있습니다.

매개변수

여러 매개변수를 지정할 때는 공백으로 구분합니다.

acpi=off

ACPI(Advanced Configuration and Power Interface)를 비활성화합니다. 특정 하드웨어 구성에 문제가 발생할 때 이 매개변수를 사용할 수 있습니다.

noapic

APIC(Advanced Programmable Interrupt Controller)를 비활성화합니다. 특정 하드웨어 구성에 문제가 발생할 때 이 매개변수를 사용할 수 있습니다.

vga=ask

부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 비디오 모드를 묻습니다. **vga** 매개변수가 없으면 비디오 모드가 자동으로 감지됩니다.

vga= *mode_number*

부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 비디오 모드를 지정합니다. 모드 번호는 16진수 형식으로 *mode_number*에서 제공합니다(예: **vga=0x318**).

모드 번호에 해당하는 화면 해상도와 색상 수는 시스템에 따라 다를 수 있습니다. 먼저 **mode_number**의 값을 선택하려면 *vga=ask* 매개변수를 사용하는 것이 좋습니다.

quiet

Linux 커널을 로딩할 때 시작 메시지 표시를 비활성화하고 커널이 로드된 후에 관리 콘솔을 시작합니다.

이 매개변수는 부트 가능한 이미지를 만들 때 무조건적으로 지정되지만 부트 메뉴에서 이 매개변수를 제거할 수 있습니다.

이 매개변수가 없으면 모든 시작 메시지가 표시된 이후에 명령 프롬프트가 나옵니다. 명령 프롬프트에서 관리 콘솔을 시작하려면 **/bin/product** 명령을 실행합니다.

nousb

USB(Universal Serial Bus) 하위 시스템의 로딩을 비활성화합니다.

nousb2

USB 2.0 지원을 비활성화합니다. USB 1.1 장치는 이 매개변수에서 여전히 작동합니다. 이 매개변수를 사용하면 USB 2.0 모드에서 작동하지 않는 일부 USB 드라이브를 USB 1.1 모드에서 사용할 수 있습니다.

nodma

모든 IDE 하드 디스크 드라이브에 대해 직접 메모리 액세스(DMA)를 비활성화합니다. 커널이 일부 하드웨어에서 고정되는 것을 방지합니다.

nofw

FireWire(IEEE1394) 인터페이스 지원을 비활성화합니다.

nopcmcia

PCMCIA 하드웨어 감지를 비활성화합니다.

nomouse

마우스 지원을 비활성화합니다.

module_name **=off**

*module_name*이 지정한 이름의 모듈을 비활성화합니다. 예를 들어 SATA 모듈 사용을 비활성화하려면 **sata_sis=off**를 지정합니다.

pci=bios

하드웨어 장치를 직접 액세스하는 대신 PCI BIOS를 강제로 사용합니다. 시스템에 표준 이외의 PCI 호스트 브리지가 있는 경우 이 매개변수를 사용할 수 있습니다.

pci=nobios

PCI BIOS의 사용을 비활성화합니다. 직접 하드웨어 액세스 방법만 허용됩니다. BIOS로 인해 부트 가능한 미디어를 시작하지 못할 때 이 매개변수를 사용할 수 있습니다.

pci=biosirq

PCI BIOS 호출을 사용하여 인터럽트 라우팅 테이블을 얻을 수 있습니다. 커널이 인터럽트 요청(IRQ)을 할당할 수 없거나 마더보드에서 보조 PCI 버스를 찾을 수 없는 경우 이 매개변수를 사용할 수 있습니다.

이러한 호출은 일부 시스템에서는 올바로 작동하지 않을 수 있습니다. 그러나 이 방법으로만 인터럽트 라우팅 테이블을 얻을 수 있습니다.

LAYOUTS=en-US, de-DE, fr-FR, ...

부트 가능한 미디어의 그래픽 사용자 인터페이스에서 사용할 키보드 레이아웃을 지정합니다.

이 매개변수가 없으면 두 개의 레이아웃만 사용할 수 있습니다. 영어(미국) 및 미디어의 부트 메뉴에서 선택한 언어에 해당하는 레이아웃.

다음의 레이아웃 중에서 지정 가능:

벨기에어: **be-BE**

체코어: **cz-CZ**

영어: **en-GB**

영어(미국): **en-US**

프랑스어: **fr-FR**

프랑스어(스위스): **fr-CH**

독일어: **de-DE**

독일어(스위스): **de-CH**

이탈리아어: **it-IT**

폴란드어: **pl-PL**

포르투갈어: **pt-PT**

포르투갈어(브라질): **pt-BR**

러시아어: **ru-RU**

세르비아어(키릴): **sr-CR**

세르비아어(라틴): **sr-LT**

스페인어: **es-ES**

부트 가능한 미디어에서 작업할 때에는 CTRL + SHIFT를 사용하여 사용 가능한 레이아웃을 순회합니다.

부트 가능한 미디어의 스크립트

부트 가능한 미디어에서 지정된 일련의 작업을 수행하게 하려면 Bootable Media Builder에서 미디어를 생성하는 동안 스크립트를 지정하면 됩니다. 미디어가 부팅될 때마다 사용자 인터페이스를 표시하지 않고 이 스크립트를 실행합니다.

미리 정의된 스크립트 중 하나를 선택하거나 스크립팅 규칙에 따라 사용자 정의 스크립트를 생성할 수 있습니다.

사전 정의된 스크립트

Bootable Media Builder에서는 다음 사전 정의된 스크립트를 제공합니다.

- 클라우드 스토리지에 백업 및 클라우드 스토리지에서 복구(**entire_pc_cloud**)
- 부트 가능한 미디어에 백업 및 부트 가능한 미디어에서 복구(**entire_pc_local**)
- 네트워크 공유에 백업 및 네트워크 공유에서 복구(**entire_pc_share**)
- 클라우드 스토리지에서 복구(**golden_image**)

스크립트는 Bootable Media Builder가 설치된 머신의 다음 디렉터리에서 찾을 수 있습니다.

- Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

클라우드 스토리지에 백업 및 클라우드 스토리지에서 복구

이 스크립트는 머신을 클라우드 스토리지에 백업하거나 이 스크립트를 통해 클라우드 스토리지에 생성된 가장 최근 백업에서 머신을 복구합니다. 시작 시 이 스크립트는 사용자에게 백업, 복구 및 사용자 인터페이스 시작 중에서 선택할지 묻는 메시지를 표시합니다.

Bootable Media Builder에서 다음 스크립트 매개변수를 지정합니다.

1. 클라우드 스토리지의 사용자 이름 및 비밀번호.
2. [선택 사항] 스크립트가 백업을 암호화하거나 백업에 액세스하는 데 사용할 비밀번호.

부트 가능한 미디어에 백업 및 부트 가능한 미디어에서 복구

이 스크립트는 머신을 부트 가능한 미디어에 백업하거나 동일한 미디어에서 이 스크립트를 통해 생성된 가장 최근 백업에서 머신을 복구합니다. 시작 시 이 스크립트는 사용자에게 백업, 복구 및 사용자 인터페이스 시작 중에서 선택할지 묻는 메시지를 표시합니다.

Bootable Media Builder에서 스크립트가 백업을 암호화하거나 백업에 액세스하는 데 사용할 비밀번호를 지정할 수 있습니다.

네트워크 공유에 백업 및 네트워크 공유에서 복구

이 스크립트는 머신을 네트워크 공유에 백업하거나 네트워크 공유에 있는 가장 최근 백업에서 머신을 복구합니다. 시작 시 이 스크립트는 사용자에게 백업, 복구 및 사용자 인터페이스 시작 중에서 선택할지 묻는 메시지를 표시합니다.

Bootable Media Builder에서 다음 스크립트 매개변수를 지정합니다.

1. 네트워크 공유 경로.
2. 네트워크 공유의 사용자 이름 및 비밀번호.
3. [선택 사항] 백업 파일 이름. 기본값은 **AutoBackup**입니다. 스크립트를 통해 백업을 기존 백업에 추가하거나 기본값이 아닌 이름을 가진 백업에서 복구하려면 기본값을 이 백업의 파일 이름으로 변경합니다.

   백업 파일 이름을 찾으려면

   a. Cyber Protect 웹 콘솔에서 **백업 스토리지** > **위치**로 이동합니다.

   b. 네트워크 공유를 선택합니다(공유가 나열되지 않는 경우 **위치 추가** 클릭).

   c. 백업을 선택합니다.

   d. **상세정보**를 클릭합니다. 파일 이름이 **백업 파일 이름** 아래에 표시됩니다.
4. [선택 사항] 스크립트가 백업을 암호화하거나 백업에 액세스하는 데 사용할 비밀번호.

클라우드 스토리지에서 복구

이 스크립트는 클라우드 스토리지에 있는 가장 최근 백업에서 머신을 복구합니다. 시작 시 이 스크립트는 사용자에게 다음을 지정할지 묻는 메시지를 표시합니다.

1. 클라우드 스토리지의 사용자 이름 및 비밀번호.
2. 백업이 암호화된 경우 비밀번호.

이 클라우드 스토리지 계정으로 머신 하나의 백업만 저장하는 것이 좋습니다. 그렇지 않으면 또 다른 머신의 백업이 현재 머신의 백업보다 더 새로운 경우 스크립트는 해당 머신 백업을 선택합니다.

사용자 정의 스크립트

중요

사용자 지정 스크립트를 생성하려면 Bash 명령 언어 및 JavaScript 객체 표기법(JSON)에 대한 지식이 필요합니다. Bash에 익숙하지 않은 경우 http://www.tldp.org/LDP/abs/html에서 자세히 알아볼 수 있습니다. JSON 사양은 http://www.json.org에서 사용할 수 있습니다.

스크립트 파일

스크립트는 Bootable Media Builder가 설치된 머신의 다음 디렉터리에 있어야 합니다.

- Windows: %**ProgramData%\Acronis\MediaBuilder\scripts**
- Linux: **/var/lib/Acronis/MediaBuilder/scripts/**

스크립트는 3개 이상의 다음 파일로 구성되어야 합니다.

- **<script_file>.sh** - Bash 스크립트가 포함된 파일. 스크립트를 생성할 때 https://busybox.net/downloads/BusyBox.html에서 찾을 수 있는 제한된 셸 명령 집합만 사용하십시오. 다음 명령도 사용할 수 있습니다.
  - `acrocmd` - 백업 및 복구용 명령줄 유틸리티
  - `product` - 부트 가능한 미디어 사용자 인터페이스를 시작하는 명령

  이 파일과 스크립트에 포함된 추가 파일(예: 점 명령 사용)은 **bin** 하위 폴더에 있어야 합니다. 스크립트에서 추가 파일 경로를 **/ConfigurationFiles/bin/<some_file>**로 지정합니다.

- **autostart** - **<script_file>.sh**를 시작하기 위한 파일. 파일 내용은 다음과 같아야 합니다.

```
#!/bin/sh
. /ConfigurationFiles/bin/variables.sh
. /ConfigurationFiles/bin/<script_file>.sh
. /ConfigurationFiles/bin/post_actions.sh
```

- **autostart.json** - 다음이 포함된 JSON 파일.
  - Bootable Media Builder에 표시되는 스크립트 이름 및 설명.
  - Bootable Media Builder를 통해 구성할 스크립트 변수의 이름.
  - 각 변수에 대해 Bootable Media Builder에 표시되는 컨트롤의 매개변수.

autostart.json의 구조

최상위 객체

쌍		필요 사항	설명
이름	값 유형		
displayName	문자열	예	Bootable Media Builder에 표시되는 스크립트 이름.
description	문자열	아니요	Bootable Media Builder에 표시되는 스크립트 설명.
timeout	숫자	아니요	스크립트를 시작하기 전 부트 메뉴에 대한 시간 제한(초). 쌍이 지정되지 않으면 시간 제한은 10초가 됩니다.
variables	객체	아니요	Bootable Media Builder를 통해 구성할 **<script_file>.sh**에 대한 변수. 변수는 변수 문자열 식별자 및 변수 객체의 쌍 집합이어야 합니다(아래 표 참조).

변수 객체

쌍		필요 사항	설명
이름	값 유형		
displayName	문자열	예	**<script_file>.sh**에 사용되는 변수 이름.
type	문자열	예	Bootable Media Builder에 표시되는 컨트롤의 유형. 이 컨트롤은 변수 값을 구성하는 데 사용됩니다. 모든 지원되는 유형에 대해서는 아래 표를 참조하십시오.
description	문자열	예	Bootable Media Builder의 컨트롤 위에 표시되는 컨트롤 레이블.

default	type이 string, multiString, password, 또는 enum인 경우 문자열 type이 number, spinner 또는 checkbox인 경우 숫자	아니요	컨트롤의 기본값. 쌍이 지정되지 않으면 기본값은 컨트롤 유형에 따라 빈 문자열 또는 0이 됩니다. 확인란의 기본값은 0(선택 취소 상태) 또는 1(선택 상태)가 될 수 있습니다.
order	숫자 (음수가 아님)	예	Bootable Media Builder의 컨트롤 순서. 값이 높을수록 컨트롤은 **autostart.json**에 정의된 기타 컨트롤을 기준으로 아래쪽에 배치됩니다. 초기 값은 0이어야 합니다.
min (spinner만 해당)	숫자	아니요	스핀 박스에 있는 스핀 컨트롤의 최소값. 쌍이 지정되지 않으면 값은 0이 됩니다.
max (spinner만 해당)	숫자	아니요	스핀 박스에 있는 스핀 컨트롤의 최대값. 쌍이 지정되지 않으면 값은 100이 됩니다.
step (spinner만 해당)	숫자	아니요	스핀 박스에 있는 스핀 컨트롤의 단계 값. 쌍이 지정되지 않으면 값은 1이 됩니다.
items (enum만 해당)	문자열 배열	예	드롭다운 목록의 값.
required (string, multiString, password, enum만 해당)	숫자	아니요	컨트롤 값이 비어 있을 수 있거나(0) 없는지(1) 여부를 지정합니다. 쌍이 지정되지 않으면 컨트롤 값은 비어 있을 수 있습니다.

컨트롤 유형

이름	설명
string	짧은 문자열을 입력하거나 편집하는 데 사용되는 한 줄의 비제한 텍스트 박스.
multiString	긴 문자열을 입력하거나 편집하는 데 사용되는 여러 줄의 비제한 텍스트 박스.
password	비밀번호를 안전하게 입력하는 데 사용되는 한 줄의 비제한 텍스트 박스.

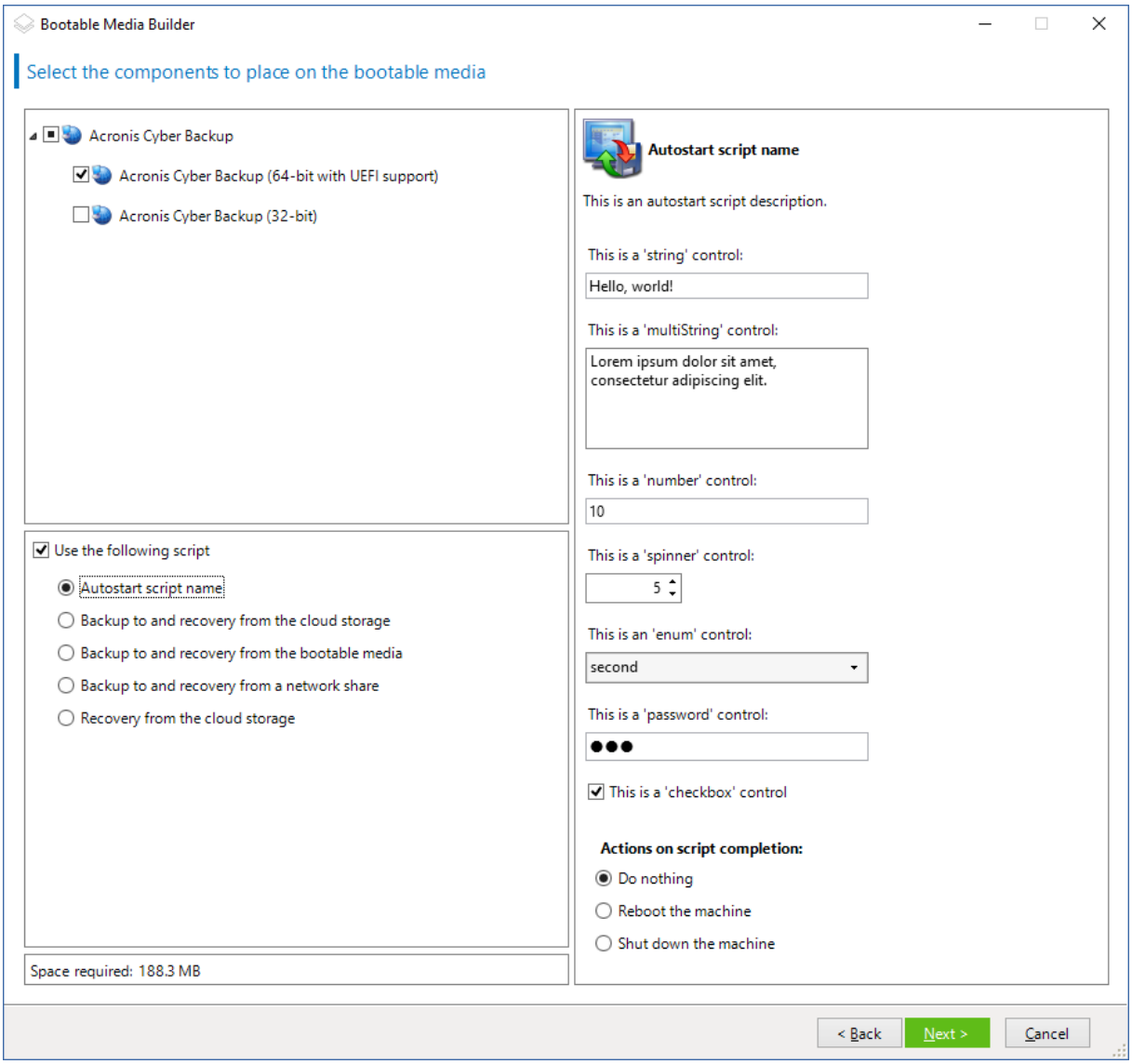
number	숫자를 입력하거나 편집하는 데 사용되는 한 줄의 숫자 전용 텍스트 박스.
spinner	스킨 컨트롤을 통해 숫자를 입력하거나 편집하는 데 사용되는 한 줄의 숫자 전용 텍스트 박스. 스핀 박스라고도 합니다.
enum	미리 결정된 값의 고정된 집합이 있는 표준 드롭다운 목록.
checkbox	선택 취소 상태 또는 선택 상태의 두 가지 상태를 가지는 확인란.

아래 샘플 **autostart.json**에는 **<script_file>.sh**에 대한 변수를 구성하는 데 사용될 수 있는 컨트롤의 모든 가능한 유형이 포함됩니다.

```
{
        "displayName": "Autostart script name",
        "description": "This is an autostart script description.",
        "variables": {
                "var_string": {
                        "displayName": "VAR_STRING",
                        "type": "string", "order": 1,
                        "description": "This is a 'string' control:", "default": "Hello,
world!"
                },
                "var_multistring": {
                        "displayName": "VAR_MULTISTRING",
                        "type": "multiString", "order": 2,
                        "description": "This is a 'multiString' control:",
                        "default": "Lorem ipsum dolor sit amet,\nconsectetur adipiscing elit."
                },
                "var_number": {
                        "displayName": "VAR_NUMBER",
                        "type": "number", "order": 3,
                        "description": "This is a 'number' control:", "default": 10
                },
                "var_spinner": {
                        "displayName": "VAR_SPINNER",
                        "type": "spinner", "order": 4,
```

```
                "description": "This is a 'spinner' control:",
                "min": 1, "max": 10, "step": 1, "default": 5
        },
        "var_enum": {
                "displayName": "VAR_ENUM",
                "type": "enum", "order": 5,
                "description": "This is an 'enum' control:",
                "items": ["first", "second", "third"], "default": "second"
        },
        "var_password": {
                "displayName": "VAR_PASSWORD",
                "type": "password", "order": 6,
                "description": "This is a 'password' control:", "default": "qwe"
        },
        "var_checkbox": {
                "displayName": "VAR_CHECKBOX",
                "type": "checkbox", "order": 7,
                "description": "This is a 'checkbox' control", "default": 1
        }
    }
}
```

Bootable Media Builder에서 이와 같이 표시됩니다.



관리 서버

부트 가능한 미디어를 생성하는 중에 관리 서버에서 미디어 등록을 미리 구성하는 옵션이 있습니다.

미디어를 등록하면 등록된 머신인 것처럼 Cyber Protect 웹 콘솔을 통해 미디어를 관리할 수 있습니다. 원격 액세스의 편리함 외에도 이를 통해 관리자에게 부트 가능한 미디어에서 수행되는 모든 작업을 추적하는 기능이 제공됩니다. 이 작업이 **작업**에 기록되므로 작업을 시작한 사용자와 시간을 확인할 수 있습니다.

등록이 미리 구성되지 않은 경우에도 미디어에서 머신을 부팅한 후 미디어를 등록할 수 있습니다.

관리 서버에서 등록을 미리 구성하려면

1. **관리 서버에 미디어 등록** 확인란을 선택합니다.
2. **서버 이름 또는 IP**에서 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다. 다음 형식 중 하나를 사용할 수 있습니다.

- http://<서버>. 예: http://10.250.10.10 또는 http://server1
- <IP 주소>. 예: 10.250.10.10
- <호스트 이름>. 예: server1 또는 server1.example.com

3. **포트**에서 관리 서버에 액세스하는 데 사용할 포트를 지정합니다. 기본값은 9877입니다.
4. **표시 이름**에 Cyber Protect 웹 콘솔에서 이 머신에 대해 표시할 이름을 지정합니다. 이 필드를 비워 두면 표시 이름이 다음 중 하나로 설정됩니다.
   - 머신이 이전에 관리 서버에 등록된 경우 같은 이름이 사용됩니다.
   - 이외의 경우에는 머신의 FQDN(정규화된 도메인 이름) 또는 IP 주소가 사용됩니다.
5. 관리 서버에서 미디어를 등록하는 데 사용할 계정을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - **부팅 시 사용자 이름과 비밀번호를 물음**

     머신이 미디어에서 부팅될 때마다 자격 증명을 제공해야 합니다.

     등록에 성공하려면 계정이 관리 서버 관리자 목록(**설정** > **계정**)에 있어야 합니다. Cyber Protect 웹 콘솔에서 미디어는 지정된 계정에 부여된 권한에 따라 조직 또는 특정 단위 아래에 제공됩니다.

     부트 가능한 미디어 인터페이스에서 **도구** > **관리 서버에 미디어 등록**을 클릭하여 사용자 이름과 비밀번호를 변경할 수 있습니다.
   - **다음 계정으로 등록**

     머신은 미디어에서 부팅될 때마다 자동으로 등록됩니다.

     지정하는 계정이 관리 서버 관리자 목록(**설정** > **계정**)에 있어야 합니다. Cyber Protect 웹 콘솔에서 미디어는 지정된 계정에 부여된 권한에 따라 조직 또는 특정 단위 아래에 제공됩니다.

     부트 가능한 미디어 인터페이스에서는 등록 매개변수를 변경할 수 *없습니다*.

네트워크 설정

부트 가능한 미디어를 생성하는 중에 부트 가능한 에이전트가 사용할 네트워크 연결을 미리 구성할 수 있습니다. 다음 매개변수를 미리 구성할 수 있습니다.

- IP 주소
- 서브넷 마스크
- 게이트웨이
- DNS 서버
- WINS 서버.

부트 가능한 에이전트가 머신에서 시작된 후 머신의 네트워크 인터페이스 카드(NIC)에 구성이 적용됩니다. 설정이 미리 구성되지 않은 경우에는 에이전트는 DHCP 자동 구성을 사용합니다. 부트 가능한 에이전트가 머신에서 실행 중인 경우에는 네트워크 설정을 수동으로 구성할 수도 있습니다.

여러 네트워크 연결을 미리 구성

최대 10개의 네트워크 인터페이스 카드에 대해 TCP/IP 설정을 미리 구성할 수 있습니다. 각 NIC에 적합한 설정이 할당될 수 있도록 미디어가 사용자 정의된 서버에서 미디어를 생성하십시오. 마법

사 창에서 기존 NIC를 선택한 경우에는 미디어에 저장하기 위한 설정이 선택됩니다. 각 기존 NIC의 MAC 주소 또한 미디어에 저장됩니다.

MAC 주소를 제외하고는 설정을 변경하거나 필요한 경우 존재하지 않는 NIC의 설정을 구성할 수 있습니다.

부트 가능한 에이전트는 서버에서 시작된 후, 사용 가능한 NIC 목록을 검색합니다. 이 목록은 NIC가 사용하고 있는 상단에서 프로세서에 가장 가까운 슬롯으로 정렬되어 있습니다.

부트 가능한 에이전트는 각 알려진 NIC에 적합한 설정을 할당하여 NIC를 MAC 주소로 식별합니다. 알려진 MAC 주소가 있는 NIC를 구성한 후에 나머지 NIC에는, 존재하지 않는 NIC에 대해 작성한 설정이 맨 위의 할당되지 않은 NIC부터 시작하여 할당됩니다.

미디어가 생성된 머신뿐만 아니라 모든 머신에서 부트 가능한 미디어를 사용자 정의할 수 있습니다. 이를 수행하려면 해당 머신에서 슬롯 순서에 따라서 NIC를 구성하십시오. NIC1은 프로세서와 가장 가까운 슬롯을 사용하고, NIC2는 그 다음 슬롯을 사용합니다. 부트 가능한 에이전트는 해당 머신에서 시작할 때 알려진 MAC 주소가 있는 NIC를 찾지 못하고 사용자가 했던 것과 같은 순서로 NIC를 구성합니다.

예

부트 가능한 에이전트는 운영 네트워크를 통한 관리 콘솔과의 통신을 위해 네트워크 어댑터 중 하나를 사용할 수 있습니다. 이 연결을 위해 자동 구성을 수행할 수 있습니다. 복구할 상당량의 데이터를 정적 TCP/IP 설정을 사용하여 전용 백업 네트워크에 포함된 보조 NIC를 통해 전송할 수 있습니다.

네트워크 포트

부트 가능한 미디어를 생성할 때 부트 가능한 에이전트가 acrocmd 유틸리티에서 들어오는 연결을 수신하는 네트워크 포트를 미리 구성할 수 있습니다. 다음 중에서 선택할 수 있습니다.

- 기본 포트
- 현재 사용된 포트
- 새 포트(포트 번호 입력)

포트가 미리 구성되지 않은 경우에는 에이전트가 포트 9876을 사용합니다.

Universal Restore의 드라이버

부트 가능한 미디어를 생성하는 중에 Windows 드라이버를 미디어에 추가할 수 있습니다. Universal Restore가 이 드라이버를 사용하여 이기종 하드웨어로 마이그레이션된 Windows를 부팅합니다.

Universal Restore를 구성하면 다음을 수행할 수 있습니다.

- 대상 하드웨어에 가장 적합한 드라이버의 미디어를 검색할 수 있습니다.
- 미디어에서 명시적으로 지정한 대용량 저장소 드라이버를 가져올 수 있습니다. 대상 하드웨어에 하드 디스크의 특정 대용량 저장소 컨트롤러(예: SCSI, RAID 또는 파이버 채널 어댑터)가 있는 경우에 필요합니다.

이 드라이버는 부트 가능한 미디어에서 표시되는 Drivers 폴더에 배치됩니다. 드라이버는 대상 머신 RAM으로 로드되지 않으므로 Universal Restore 작업 내내 미디어가 삽입 상태에 있거나 연결되어 있어야 합니다.

이동식 미디어 또는 ISO나 플래시 드라이브 등 휴대용 미디어를 생성 중인 경우 드라이버를 부트 가능한 미디어에 추가할 수 있습니다. 드라이버는 WDS/RIS에 업로드할 수 없습니다.

드라이버를 INF 파일 또는 이러한 파일을 포함하는 폴더를 추가하는 방법으로 그룹 내 목록에만 추가할 수 있습니다. INF 파일에서는 개별 드라이버를 선택할 수 없지만 미디어 제작기는 파일 내용을 표시합니다.

드라이버를 추가하려면

1. **추가**를 클릭하고 INF 파일 또는 INF 파일이 포함된 폴더를 찾습니다.
2. INF 파일 또는 폴더를 선택합니다.
3. **확인**을 클릭합니다.

드라이버는 INF 파일을 제거하는 방법으로 그룹 단위로만 목록에서 제거할 수 있습니다.

드라이버를 제거하려면

1. INF 파일을 선택합니다.
2. **제거**를 클릭합니다.

WinPE 기반의 부트 가능한 미디어

Bootable Media Builder는 Acronis Cyber Protect 및 WinPE를 통합하기 위한 2가지 방법을 제공합니다.

- 플러그인으로 PE ISO를 처음부터 생성
- 나중에 사용하기 위해 Acronis Plug-in을 WIM 파일에 추가(수동 ISO 생성, 기타 도구를 이미지에 추가 등)

추가적인 준비 없이 WinRE 기반 PE 이미지를 생성하거나 Windows 자동 설치 키트(AIK) 또는 Windows 평가 및 배포 키트(ADK)를 설치한 후 PE 이미지를 생성할 수 있습니다.

WinRE 기반 PE 이미지

WinRE 기반 이미지 생성은 다음 운영 체제에서 지원됩니다.

- Windows 7(64비트)
- Windows 8, 8.1, 10(32비트 및 64비트)
- Windows Server 2012, 2016, 2019(64비트)

PE 이미지

Windows 자동 설치 키트(AIK) 또는 Windows 평가 및 배포 키트(ADK)를 설치하면 Bootable Media Builder는 다음 커널을 기반으로 하는 WinPE 배포판을 지원합니다.

- Windows Vista(PE 2.0)
- Windows Vista SP1 및 Windows Server 2008(PE 2.1)
- Windows 7(PE 3.0)(Windows 7 SP1(PE 3.1)에 대한 보조 기능 포함 또는 제외)
- Windows 8(PE 4.0)
- Windows 8.1(PE 5.0)
- Windows 10(Windows 10용 PE)

부트 가능한 미디어 제작기는 32비트 및 64비트 WinPE 배포판을 모두 지원합니다. 32비트 WinPE 배포판은 64비트 하드웨어에서도 실행할 수 있습니다. 그러나 UEFI(Unified Extensible Firmware Interface)를 사용하는 머신을 부팅하려면 64비트 배포판이 필요합니다.

WinPE 4 이상 기반 PE 이미지를 실행하려면 약 1GB의 RAM이 필요합니다.

참고
Windows PE 4.0 이상을 기반으로 하는 부트 가능한 미디어에서는 디스크 관리 기능을 사용할 수 없습니다. 따라서 디스크 관리 기능은 Windows 7 이하 운영 체제에서 지원됩니다. Windows 8 이상에서 디스크 관리 작업을 수행하려면 Acronis Disk Director를 설치해야 합니다. 자세한 내용은 다음 KB 문서를 참조하십시오. https://kb.acronis.com/content/47031

준비: WinPE 2.x 및 3.x

PE 2.x 또는 3.x 이미지를 만들거나 수정하려면 먼저 Windows AIK(자동 설치 키트)가 설치된 머신에 부트 가능한 미디어 빌더를 설치합니다. AIK가 있는 머신이 없으면 다음과 같이 준비합니다.

AIK가 있는 머신을 준비하려면

1. Windows 자동 설치 키트를 다운로드하고 설치합니다.
   Windows Vista(PE 2.0)용 AIK(자동 설치 키트):
   http://www.microsoft.com/Downloads/details.aspx?familyid=C7D4BC6D-15F3-4284-9123-679830D629F2&displaylang=ko
   Windows Vista SP1 및 Windows Server 2008(PE 2.1)용 AIK(자동 설치 키트):
   http://www.microsoft.com/downloads/details.aspx?FamilyID=94bb6e34-d890-4932-81a5-5b50c657de08&DisplayLang=ko
   Windows 7(PE 3.0)용 AIK(자동 설치 키트):
   http://www.microsoft.com/downloads/details.aspx?familyid=696DD665-9F76-4177-A811-39C26D3B3B34&displaylang=ko
   Windows 7 SP1(PE 3.1)용 자동 설치 키트(AIK) 보조:
   https://www.microsoft.com/ko-kr/download/details.aspx?id=5188
   상기 링크에는 설치를 위한 시스템 요구사항이 나와 있습니다.
2. [선택 사항] WAIK를 DVD로 제작하거나 플래시 드라이브에 복사합니다.
3. 이 키트(하드웨어에 따라 NETFXx86 또는 NETFXx64)에서 Microsoft .NET Framework를 설치합니다.
4. 이 키트에서 Microsoft Core XML(MSXML) 5.0 또는 6.0 Parser 를 설치합니다.

5. 이 키트에서 Windows AIK를 설치합니다.
6. 같은 머신에 부트 가능한 미디어 제작기를 설치합니다.

Windows AIK와 함께 제공된 도움말 문서를 자세히 읽어보는 것이 좋습니다. 문서에 액세스하려면 시작 메뉴에서 **Microsoft Windows AIK -> 문서**를 선택합니다.

준비: WinPE 4.0 이상

PE 4 또는 이상의 이미지를 생성 또는 수정하려면 Windows 평가 및 배포 키트(ADK)가 설치된 머신에 Bootable Media Builder를 설치합니다. ADK가 있는 머신이 없으면 다음과 같이 준비합니다.

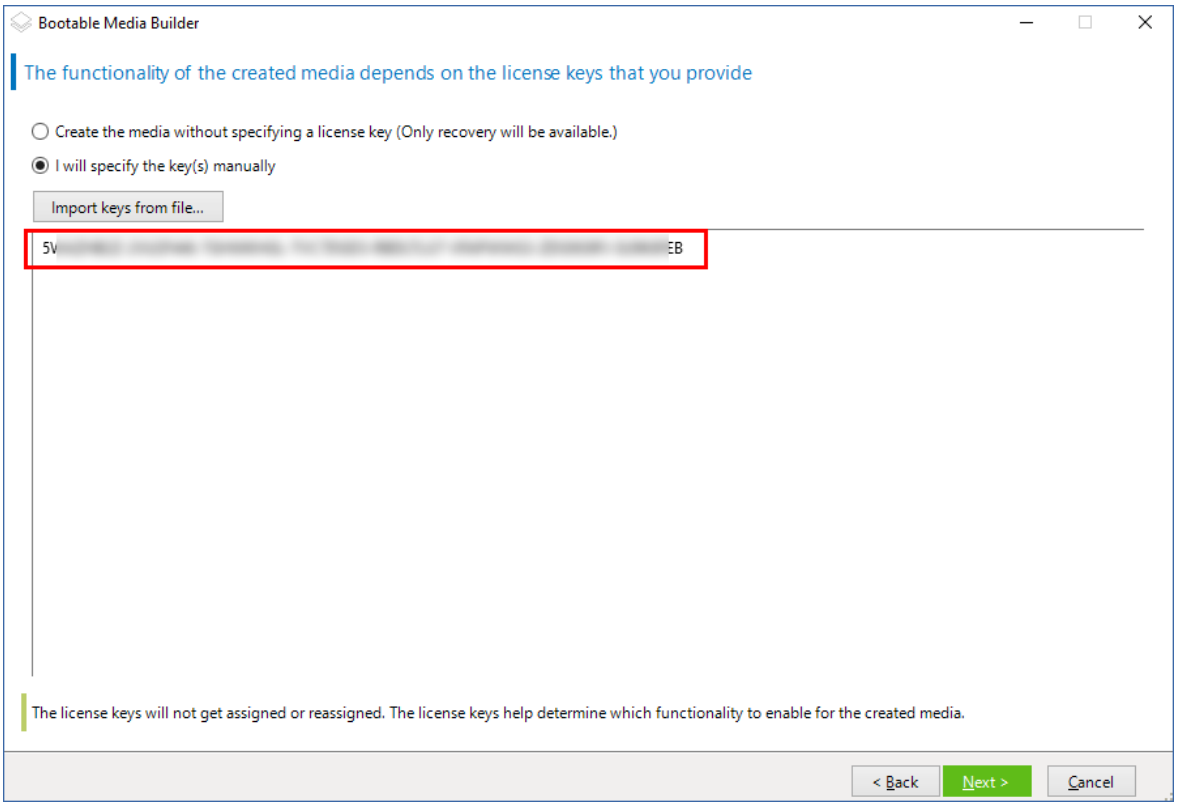
ADK가 있는 머신을 준비하려면

1. 평가 및 배포 키트 설치 프로그램을 다운로드합니다.
   ADK(Assessment and Deployment Kit) for Windows 8(PE 4.0): http://www.microsoft.com/ko-kr/download/details.aspx?id=30652
   ADK(Assessment and Deployment Kit) for Windows 8.1(PE 5.0): http://www.microsoft.com/ko-KR/download/details.aspx?id=39982
   ADK(Assessment and Deployment Kit) for Windows 10(PE for Windows 10): https://msdn.microsoft.com/ko-kr/windows/hardware/dn913721%28v=vs.8.5%29.aspx
   상기 링크에는 설치를 위한 시스템 요구사항이 나와 있습니다.
2. 머신에 평가 및 배포 키트를 설치합니다.
3. 같은 머신에 부트 가능한 미디어 제작기를 설치합니다.

WinPE에 Acronis Plug-in 추가

WinPE에 Acronis Plug-in을 추가하는 방법:

1. Bootable Media Builder를 시작합니다.
2. 완전한 기능의 부트 가능한 미디어를 생성하려면 Acronis Cyber Protect 라이센스 키를 지정합니다. 키는 부트 가능한 미디어에 포함될 기능을 결정합니다. 라이센스는 어떤 머신에서도 철회되지 않습니다.
   라이센스 키를 지정하지 않으면 해당 부트 가능한 미디어는 복구 작업에만 사용할 수 있습니다.



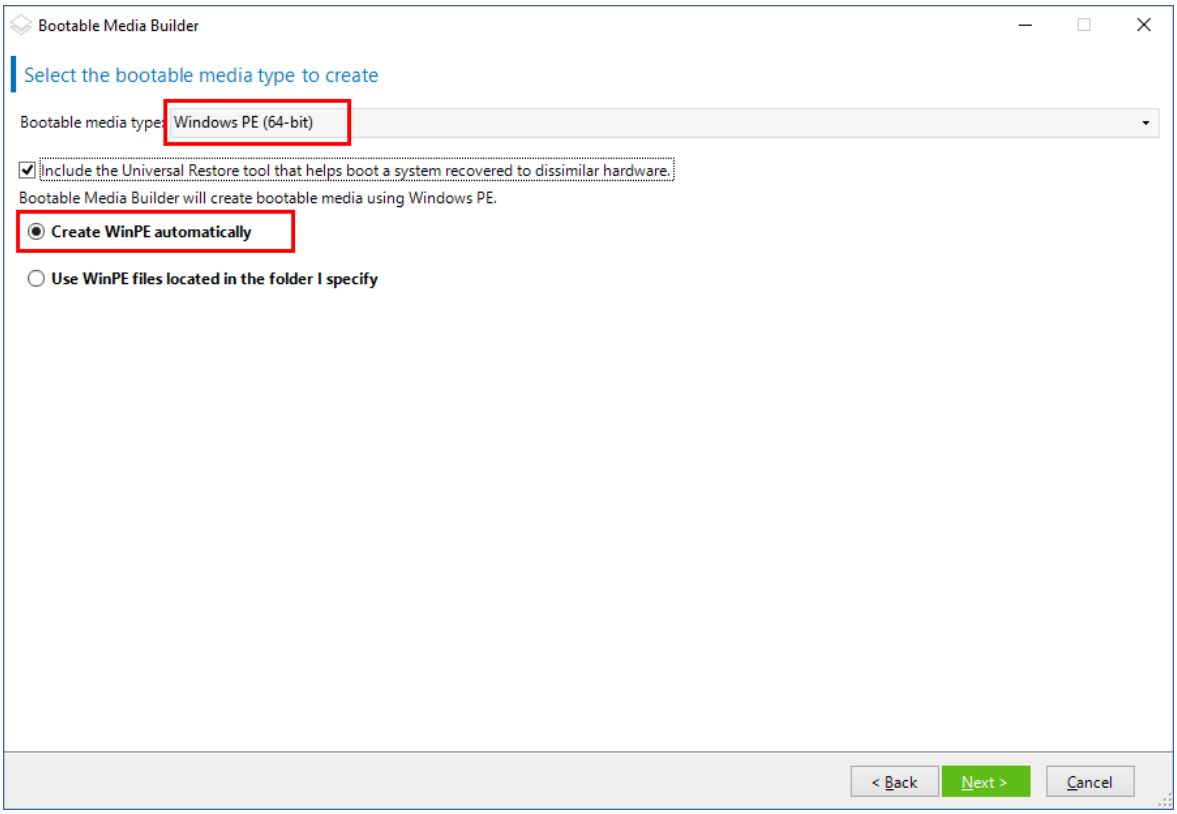
3. **부트 가능한 미디어 유형: Windows PE** 또는 **부트 가능한 미디어 유형: Windows PE(64비트)**를 선택합니다. UEFI(Unified Extensible Firmware Interface)를 사용하는 머신을 부팅하려면 64비트 미디어가 필요합니다.

   부트 가능한 미디어 유형: Windows PE를 선택한 경우 먼저 다음을 수행합니다.

   - **Plug-in for WinPE(32비트) 다운로드**를 클릭합니다.
   - 플러그 인을 **%PROGRAM_FILES%\Acronis\BootableComponents\WinPE32**에 저장합니다.

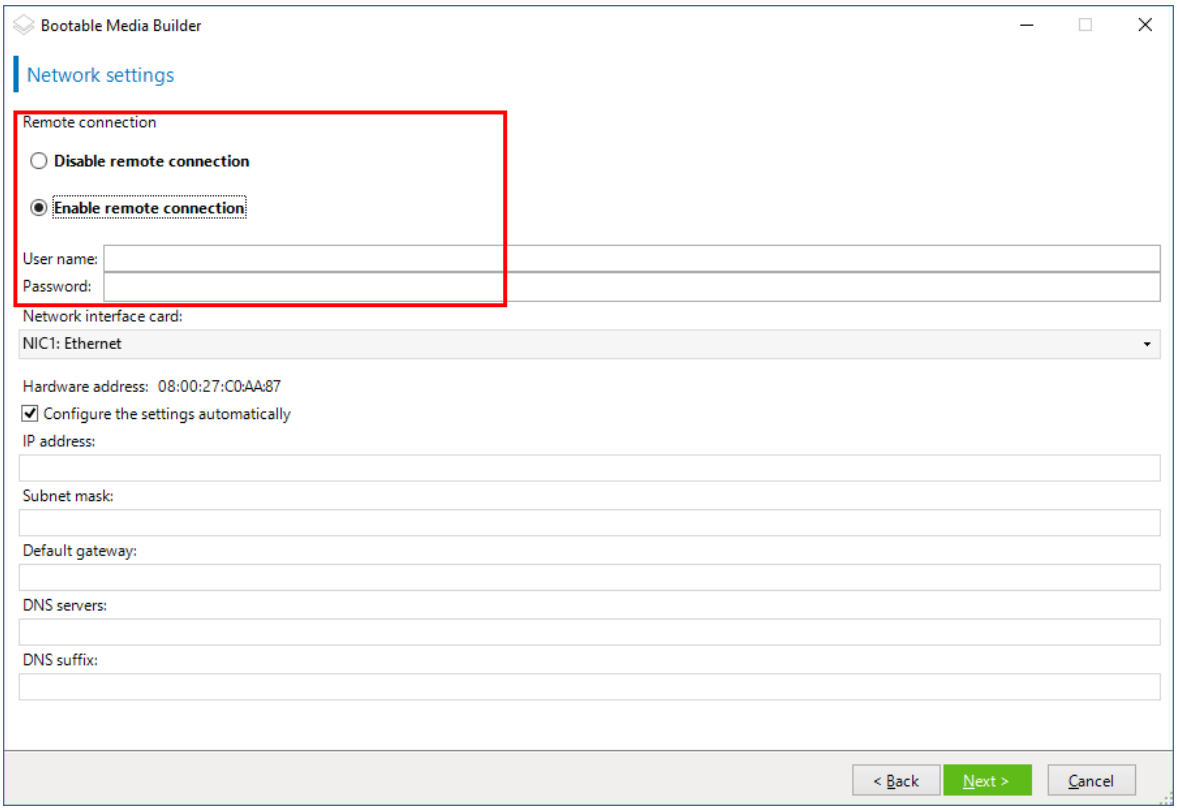
   운영 체제를 이기종 하드웨어 또는 가상 머신으로 복구할 계획이거나 시스템 부트 가능성을 확인하고 싶다면 **Universal Restore 도구 포함...** 확인란을 선택합니다.
4. **자동으로 WinPE 생성**을 선택합니다.

   소프트웨어는 적합한 소프트웨어를 실행하고 다음 창으로 이동합니다.



5. 부트 가능한 미디어에서 사용할 언어를 선택합니다.
6. 미디어에서 부트된 머신에 대한 원격 접속 활성화 여부를 선택합니다. 활성화되면 acrocmd 유틸리티가 다른 머신에서 실행 중인 경우 명령줄에 지정할 사용자 이름과 패스워드를 입력합니다. 이 필드를 비워두면 자격 증명 없이 명령줄 인터페이스를 통해 원격 접속할 수 있습니다.

   Cyber Protect 웹 콘솔에서 관리 서버에 미디어를 등록하는 경우에도 이러한 자격 증명이 필요합니다.



7. 머신 네트워크 어댑터의 네트워크 설정을 지정하거나 DHCP 자동 구성을 선택합니다.

참고
네트워크 설정은 Acronis Cyber Protect 15 Advanced 라이선스와 Acronis Cyber Protect 15 Backup Advanced 라이선스가 있어야 사용 가능합니다. 자세한 기능 비교 정보는 이 기술 자료 문서를 참조하십시오.

8. [선택 사항] 부트 시 관리 서버에 미디어를 등록하는 방법을 선택합니다. 등록 설정에 대한 자세한 내용은 관리 서버를 참조하십시오.
9. [선택 사항] Windows PE에 추가될 Windows 드라이버를 지정합니다.
   머신이 Windows PE로 부팅된 후 사용자는 드라이버를 통해 백업이 위치한 장치에 액세스할 수 있습니다. 32비트 WinPE 배포판을 사용하는 경우에는 32비트 드라이버를 추가하고 64비트 WinPE 배포판을 사용하는 경우에는 64비트 드라이버를 추가합니다.
   또한 Universal Restore for Windows를 구성할 때 추가된 드라이버를 지정할 수 있습니다. Universal Restore를 사용하려면 32비트 또는 64비트 Windows 운영 체제를 복구하려는지 여부에 따라 32비트 또는 64비트 드라이버를 추가합니다.
   드라이버를 추가하려면
   - **추가**를 클릭하고 해당 SCSI, RAID, SATA 컨트롤러, 네트워크 어댑터, 테이프 드라이브 또는 다른 장치에 필요한 .inf 파일의 경로를 지정합니다.
   - 결과로 나오는 WinPE 미디어에 포함시킬 각 드라이버에 대해 이 절차를 반복합니다.
10. ISO 또는 WIM 이미지를 만들거나 서버(WDS 또는 RIS)에서 미디어를 업로드할지 여부를 선택합니다.

11. 파일 이름을 포함한 결과로 나오는 이미지 파일의 전체 경로를 지정하거나 서버를 지정하고 서버에 액세스하기 위한 사용자 이름과 비밀번호를 입력합니다.
12. 요약 화면에서 설정을 확인하고 **진행**을 클릭합니다.
13. 서드 파티 도구를 사용하여 .ISO를 CD 또는 DVD에 굽거나 부트 가능한 플래시 드라이브를 준비합니다.

머신이 WinPE로 부팅된 후에 에이전트가 자동으로 시작됩니다.

결과로 나오는 WIM 파일에서 PE 이미지(ISO 파일)를 만들려면,

- Windows PE 폴더에서 기본 boot.wim 파일을 새로 만든 WIM 파일로 바꿉니다. 위의 예의 경우 다음을 입력합니다.

```
copy c:\AcronisMedia.wim c:\winpe_x86\ISO\sources\boot.wim
```

- **Oscdimg** 도구를 사용합니다. 위의 예의 경우 다음을 입력합니다.

```
oscdimg -n -bc:\winpe_x86\etfsboot.com c:\winpe_x86\ISO c:\winpe_x86\winpe_x86.iso
```

경고!
이 예를 복사하여 붙여 넣지 마십시오. 명령을 직접 입력하지 않으면 작업이 실패합니다.

Windows PE 2.x 및 3.x 사용자 정의에 대한 자세한 내용은 Windows 사전 설치 환경 사용자 안내서(Winpe.chm)를 참조하십시오. Windows PE 4.0 이상 버전에 대한 사용자 정의 정보는 Microsoft TechNet Library에서 참조하실 수 있습니다.

미디어에서 부팅된 머신에 연결

머신이 부트 가능한 미디어에서 부팅되면 머신 터미널은 DHCP로부터 얻거나 사전 구성된 값에 따라 설정된 IP 주소와 함께 시작 창을 표시합니다.

네트워크 설정 구성

현재 세션에 대한 네트워크 설정을 변경하려면, 시작 창에서 **네트워크 구성**을 클릭합니다. 표시되는 **네트워크 설정** 창에서 머신의 각 NIC(네트워크 인터페이스 카드)에 대한 네트워크 설정을 구성할 수 있습니다.

세션 중 실행된 변경 사항은 머신 재부팅 후 소실됩니다.

VLAN 추가

네트워크 설정 창에서 VLAN(가상 로컬 영역 네트워크)을 추가할 수 있습니다. 이 기능은 특정 VLAN에 포함된 백업 위치에 액세스해야 하는 경우에만 사용하십시오.

VLAN은 주로 로컬 영역 네트워크를 세그먼트로 분할하는 데 사용됩니다. 스위치의 *액세스* 포트에 연결된 NIC는 항상 포트 구성에 지정된 VLAN으로 액세스됩니다. 네트워크 설정에 VLAN을 지정한 경우에만 스위치의 *트렁크* 포트에 연결된 NIC가 포트 구성에서 허용된 VLAN으로 액세스할 수 있습니다.

트렁크 포트를 통해 VLAN에 액세스하려면

1. **VLAN 추가**를 클릭합니다.
2. 필요한 VLAN이 포함된 로컬 영역 네트워크에 대한 액세스를 제공하는 NIC를 선택합니다.
3. VLAN 식별자를 지정합니다.

확인을 클릭하면 네트워크 어댑터 목록에 새 입력 항목이 표시됩니다.

VLAN을 삭제하려면, 필수 VLAN 입력 항목을 클릭한 다음 **VLAN 제거**를 클릭합니다.

로컬 연결

부트 가능한 미디어에서 부팅된 머신에서 바로 작업하려면 시작 창에서 **이 머신을 로컬로 관리**를 클릭합니다.

원격 연결

원격으로 미디어에 연결하려면 "관리 서버에 미디어 등록"에 설명된 대로 관리 서버에 미디어를 등록합니다.

관리 서버에 미디어 등록

부트 가능한 미디어를 등록하면 등록된 머신인 것처럼 Cyber Protect 웹 콘솔을 통해 미디어를 관리할 수 있습니다. 이 내용은 부팅 방법에 관계없이 모든 부트 가능한 미디어에 적용됩니다(물리적 미디어, Startup Recovery Manager, Acronis PXE Server, WDS 또는 RIS). 그러나 macOS에서 생성된 부트 가능한 미디어는 등록할 수는 없습니다.

하나 이상의 Acronis Cyber Protect Advanced 라이센스가 관리 서버에 추가된 경우에만 미디어 등록이 가능합니다.

미디어 UI에서 미디어를 등록할 수 있습니다.

등록 매개변수는 Bootable Media Builder의 관리 서버 옵션에 미리 구성되어 있을 수 있습니다. 모든 등록 매개변수가 미리 구성되어 있으면 미디어가 Cyber Protect 웹 콘솔에 자동으로 표시됩니다. 일부 매개변수가 미리 구성된 경우 다음 절차의 일부 단계를 사용할 수 없습니다.

미디어 UI에서 미디어 등록

Bootable Media Builder를 사용하여 미디어를 다운로드하거나 생성할 수 있습니다.

미디어 UI에서 미디어를 등록하려면

1. 미디어에서 머신을 부팅합니다.
2. 다음 중 하나를 수행하십시오.
   - 시작 창의 **관리 서버** 아래에서 **편집**을 클릭합니다.
   - 부트 가능한 미디어 인터페이스에서 **도구 > 관리 서버에 미디어 등록**을 클릭합니다.
3. **다음 위치에 등록:**에서 관리 서버가 설치된 머신의 호스트 이름 또는 IP 주소를 지정합니다. 다음 형식 중 하나를 사용할 수 있습니다.

- http://<서버>. 예: http://10.250.10.10 또는 http://server
- <IP 주소>. 예: 10.250.10.10
- <호스트 이름>. 예: server 또는 server.example.com

4. **사용자 이름** 및 **비밀번호**에서 관리 서버 관리자 목록(**설정** > **계정**)에 있는 계정의 자격 증명을 입력합니다. Cyber Protect 웹 콘솔에서 미디어는 지정된 계정에 부여된 권한에 따라 조직 또는 특정 단위 아래에 제공됩니다.
5. **표시 이름**에 Cyber Protect 웹 콘솔에서 이 머신에 대해 표시할 이름을 지정합니다. 이 필드를 비워 두면 표시 이름이 다음 중 하나로 설정됩니다.
   - 머신이 이전에 관리 서버에 등록된 경우 같은 이름이 사용됩니다.
   - 이외의 경우에는 머신의 FQDN(정규화된 도메인 이름) 또는 IP 주소가 사용됩니다.
6. **확인**을 클릭합니다.

부트 가능한 미디어를 사용한 로컬 작업

부트 가능한 미디어를 사용한 작업은 실행 중인 운영 체제에서 수행되는 백업 및 복구 작업과 비슷합니다. 차이점은 다음과 같습니다.

1. Windows와 같은 볼륨 표현을 지닌 부트 가능한 미디어의 경우 볼륨 드라이브 문자는 Windows의 드라이브 문자와 같습니다. Windows의 드라이브 문자가 없는 볼륨(예: System Reserved 볼륨)에는 사용 가능 문자가 디스크에서의 순서대로 할당됩니다.

   부트 가능한 미디어가 머신에서 Windows를 감지하지 못하거나 여러 개를 감지하는 경우에는 드라이브 문자가 없는 볼륨을 포함한 모든 볼륨에 디스크와 같은 순서대로 문자가 할당됩니다. 따라서 볼륨 문자가 Windows에서와 다르게 표시됩니다. 예를 들어, 부트 가능한 미디어의 D: 드라이브는 Windows의 E: 드라이브와 일치할 수 있습니다.

   참고
   볼륨에 고유한 이름을 할당하는 것이 좋습니다.

2. Linux와 같은 볼륨 표현을 지닌 부트 가능한 미디어는 로컬 디스크와 볼륨을 마운트 해제된 것으로 표시합니다(sda1, sda2...).
3. 부트 가능한 미디어를 사용하여 생성된 백업은 간소화된 파일 이름을 갖습니다. 표준 이름은 표준 파일 이름 지정으로 기존 아카이브에 추가되는 경우 또는 목적지가 간소화된 파일 이름을 지원하지 않는 경우에만 백업에 지정됩니다.
4. Linux와 같은 볼륨 표현을 지닌 부트 가능한 미디어는 백업을 NTFS 포맷 볼륨에 쓸 수 없습니다. 필요할 경우 Windows와 같은 볼륨 표현을 지닌 미디어로 전환하십시오. 부트 가능한 미디어 볼륨 표현을 전환하려면 **도구** > **볼륨 표현 변경**을 클릭하세요.
5. 작업을 예약할 수 없습니다. 작업을 반복해야 하는 경우에는 처음부터 새로 구성하십시오.
6. 로그 수명은 현재 세션으로 제한되어 있습니다. 전체 로그나 필터링된 로그 항목을 파일에 저장할 수 있습니다.
7. 중앙 집중식 볼트는 **아카이브** 창의 폴더 트리에 표시되지 않습니다.

   관리 대상 볼트에 액세스하려면 **경로** 필드에 다음 문자열을 입력하십시오.

   bsp://node_address/vault_name/

관리되지 않는 중앙 집중식 볼트에 액세스하려면 볼트 폴더의 전체 경로를 입력하십시오.
액세스 자격 증명을 입력한 후에는 볼트에 있는 모든 아카이브 목록이 표시됩니다.

디스플레이 모드 설정

Linux 기반 부트 가능한 미디어를 통해 머신을 부팅할 때, 디스플레이 비디오 모드는 하드웨어 구성(모니터 및 그래픽 카드 사양)에 따라 자동으로 감지됩니다. 비디오 모드가 잘못 감지되는 경우에는 다음을 수행하십시오.

1. 부트 메뉴에서 F11을 누릅니다.
2. 명령줄에 **vga=ask**을 입력한 뒤, 부팅을 계속 진행합니다.
3. 지원되는 비디오 모드 목록에서 번호(예: **318**)를 입력하여 적합한 모드를 선택한 다음 **ENTER**를 누릅니다.

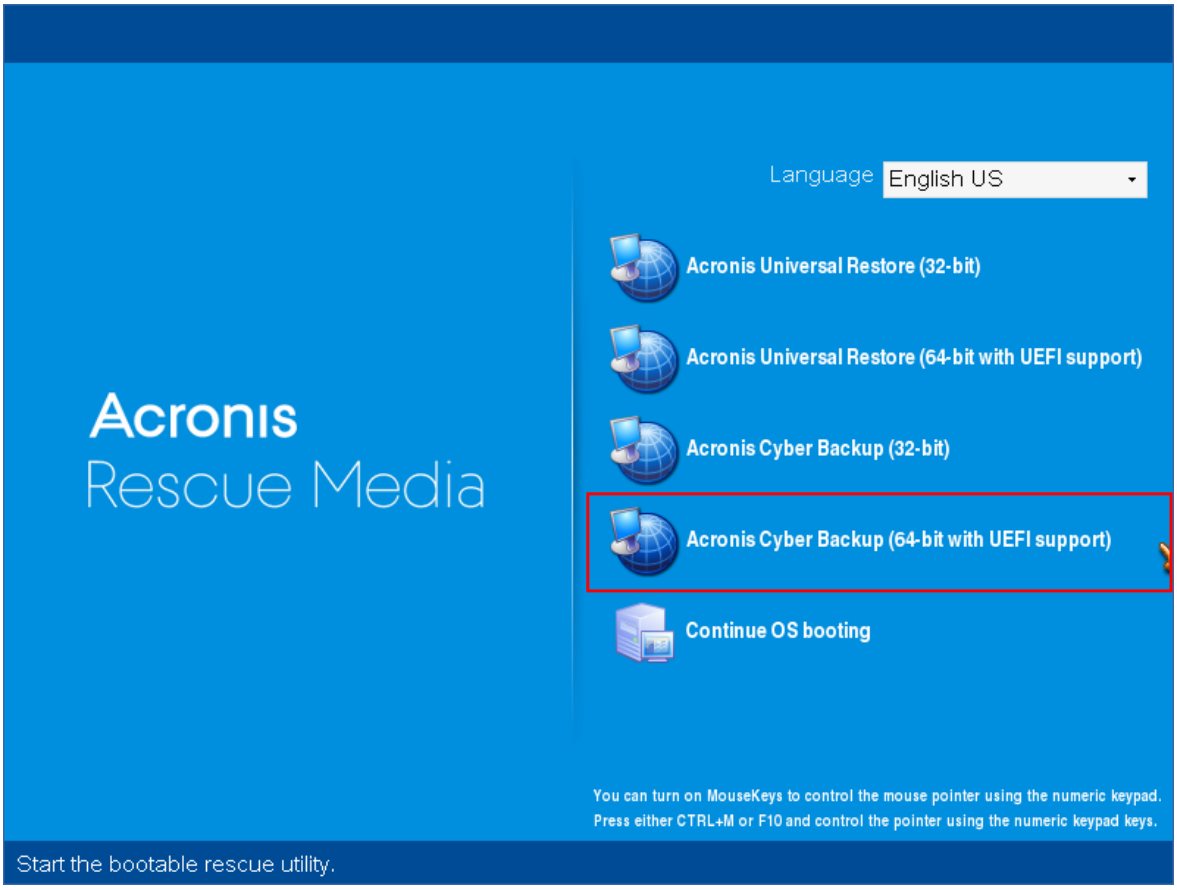
이 절차를 해당 하드웨어 구성에서 부팅할 때마다 반복하지 않으려면 **커널 매개변수** 창에 입력한 해당 모드 번호(이 예제에서는 **vga=0x318**)로 부트 가능한 미디어를 다시 만듭니다.

온프레미스의 부트 가능한 미디어를 사용한 백업

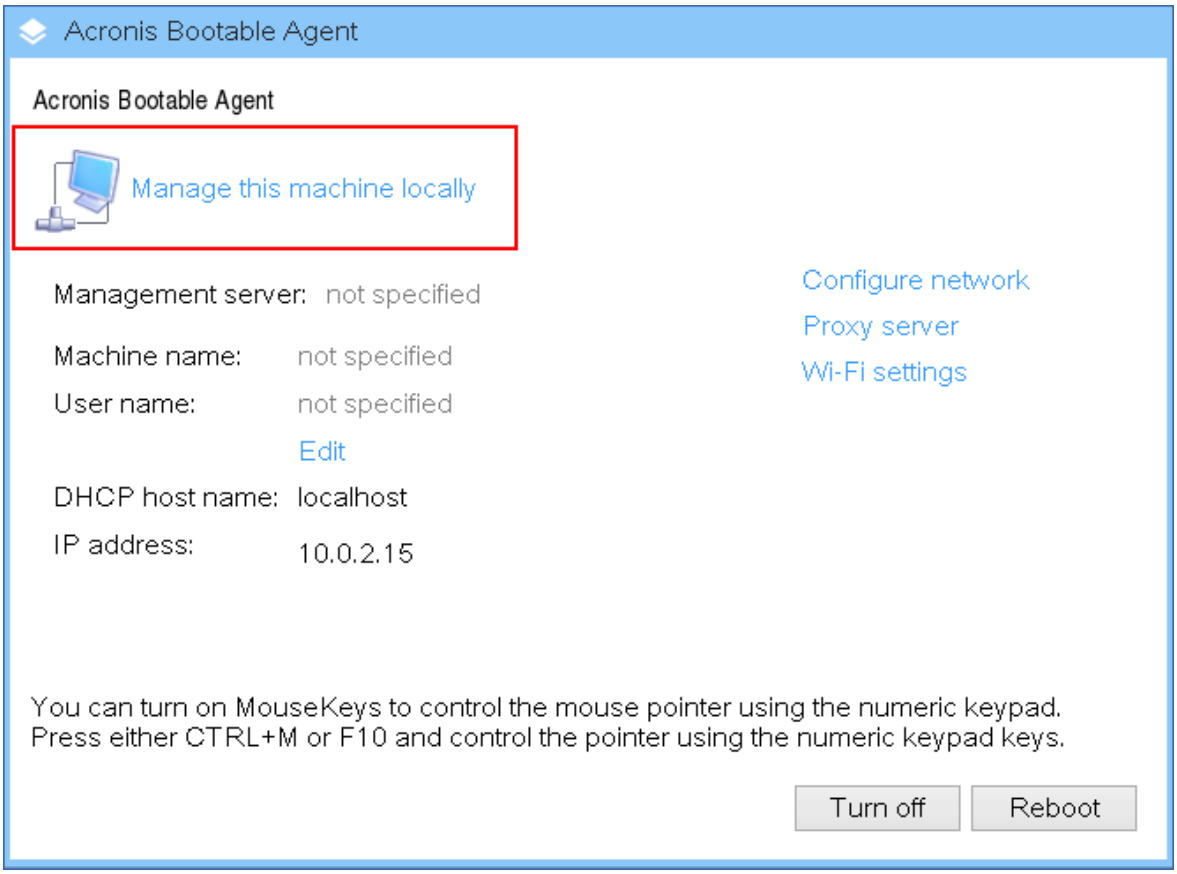
Bootable Media Builder와 Acronis Cyber Protect 라이센스 키를 사용해 생성한 부트 가능한 미디어로만 데이터를 백업할 수 있습니다. 부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 Linux 기반 부트 가능한 미디어 또는 Windows-PE 기반 부트 가능한 미디어를 참조하십시오.

부트 가능한 미디어에서 데이터 백업 작업

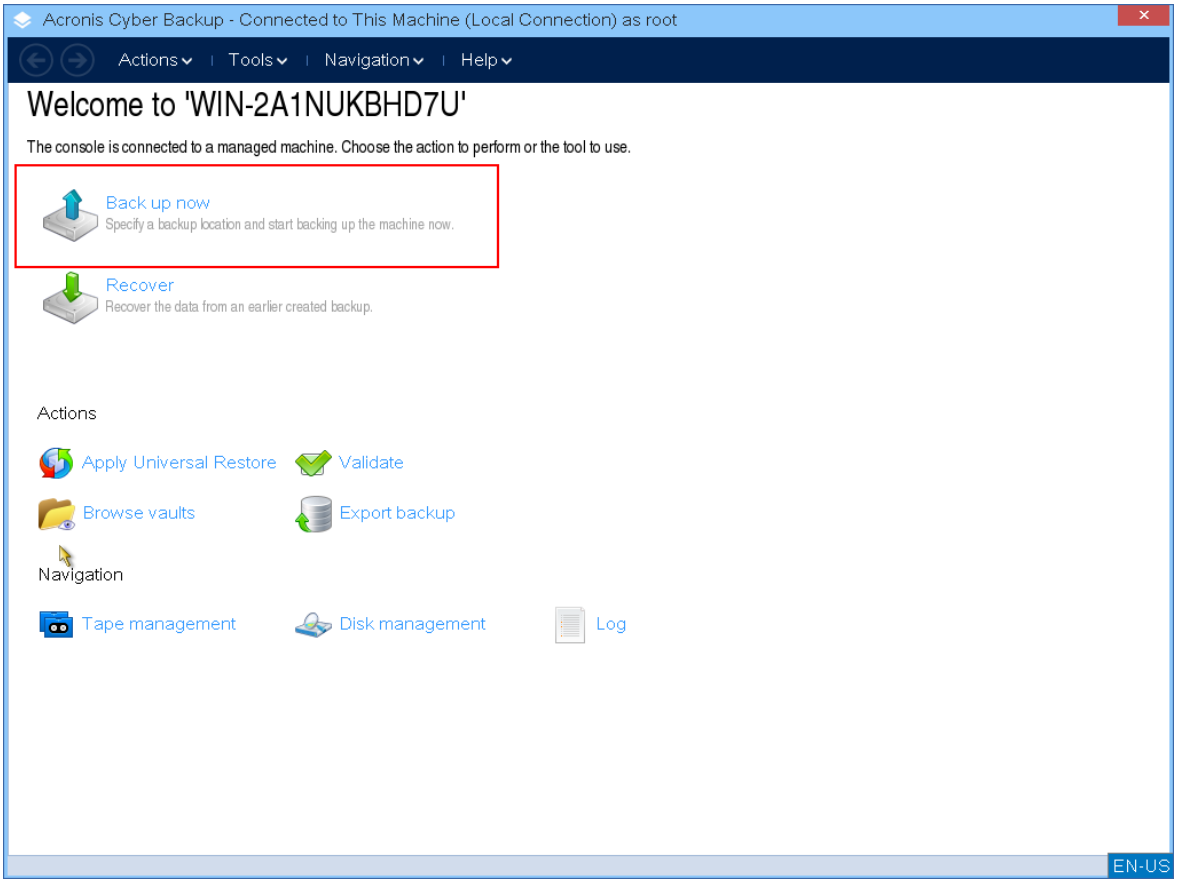
1. Acronis 부트 가능한 복구 미디어에서 부팅합니다.



2. 로컬 머신을 백업하려면 **이 머신을 로컬로 관리**를 클릭합니다. 원격 접속은 관리 서버에 미디어 등록을 참조하십시오.

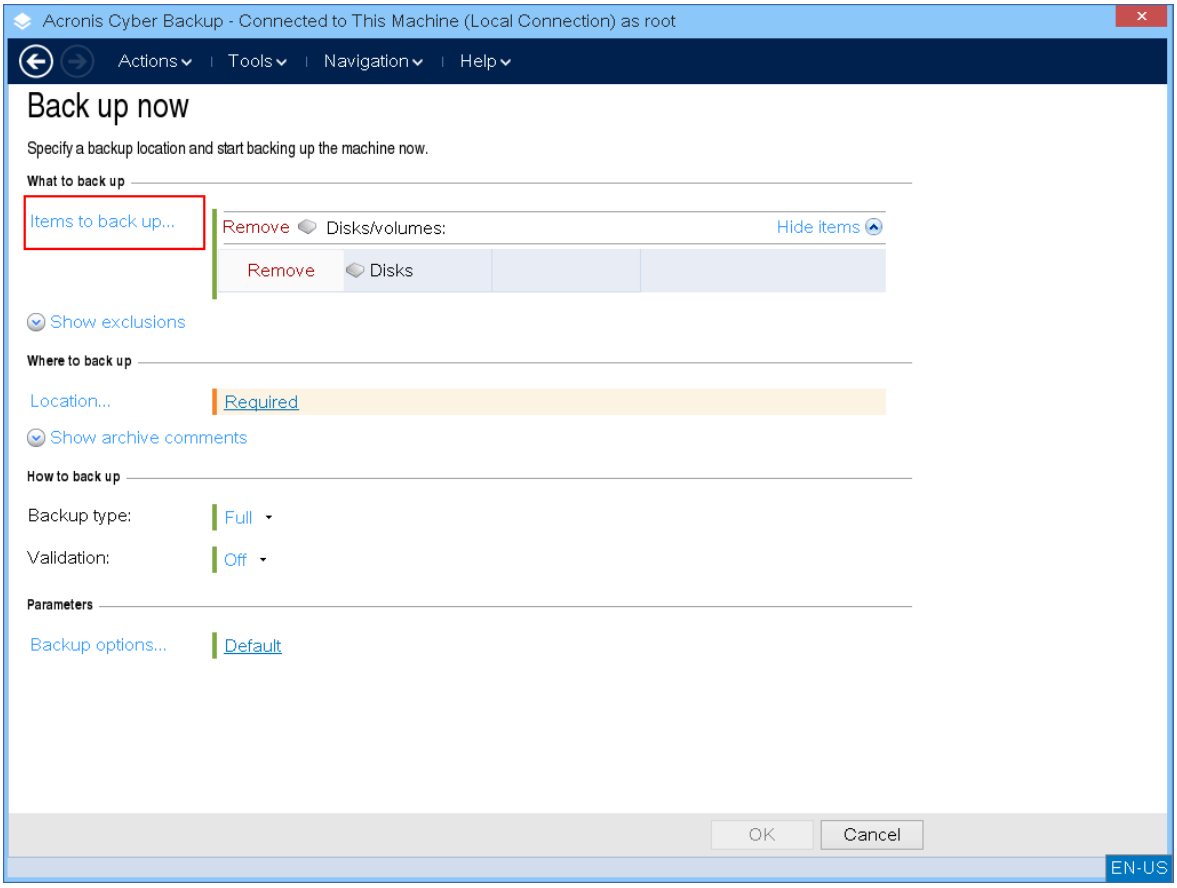


3. **지금 백업**을 클릭합니다.

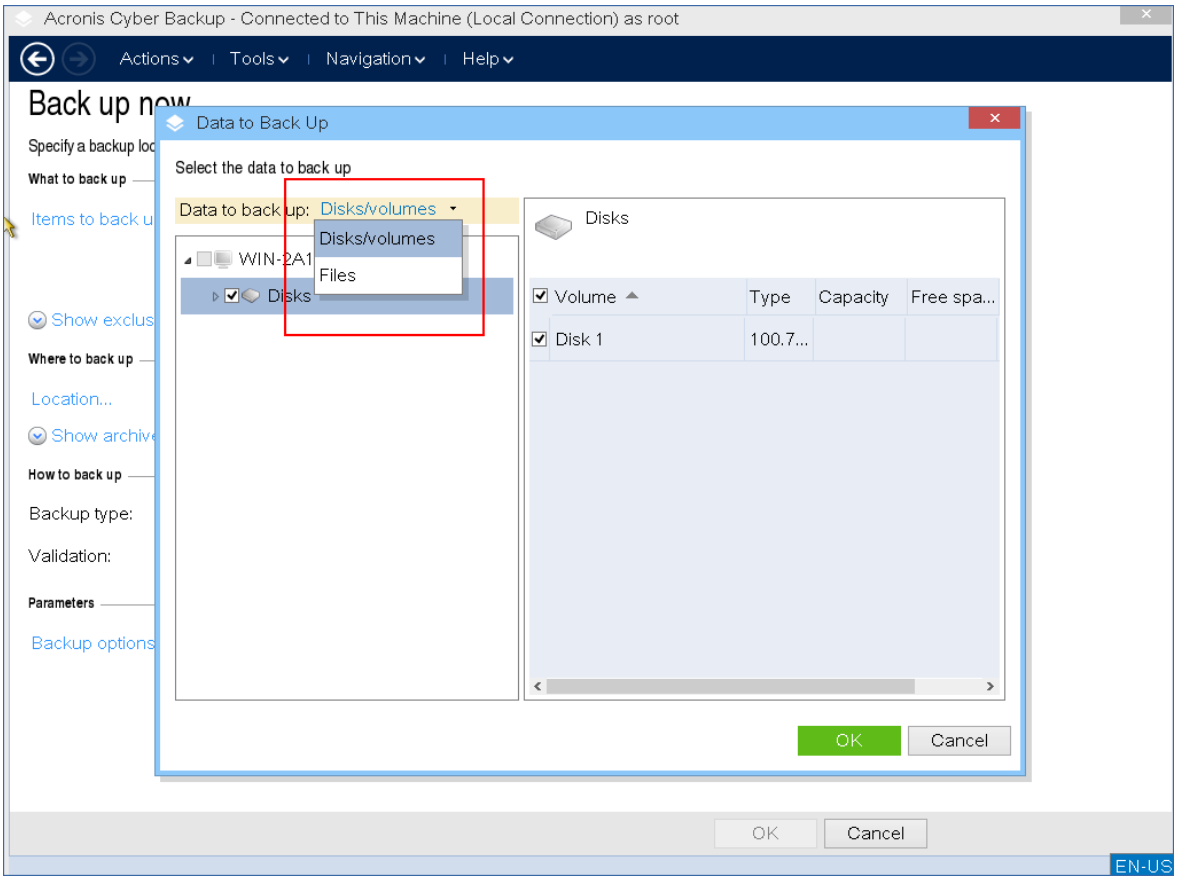


4. 기본적으로 머신의 모든 제거할 수 없는 디스크가 백업 대상으로 선택되어 있습니다. 백업될 데이터를 변경하려면 **백업할 항목**을 클릭한 뒤, 원하는 디스크나 볼륨을 선택하십시오.
   백업할 데이터를 선택할 때, 다음 메시지가 표시될 수도 있습니다. "*이 머신은 직접 선택할 수 없습니다. 머신에 이전 에이전트 버전이 설치되어 있습니다. 정책 규칙을 사용하여 백업에 이 버신을 선택하십시오.*" 이 GUI 이슈는 무시해도 됩니다. 백업하려는 개별 디스크나 볼륨을 선택합니다.

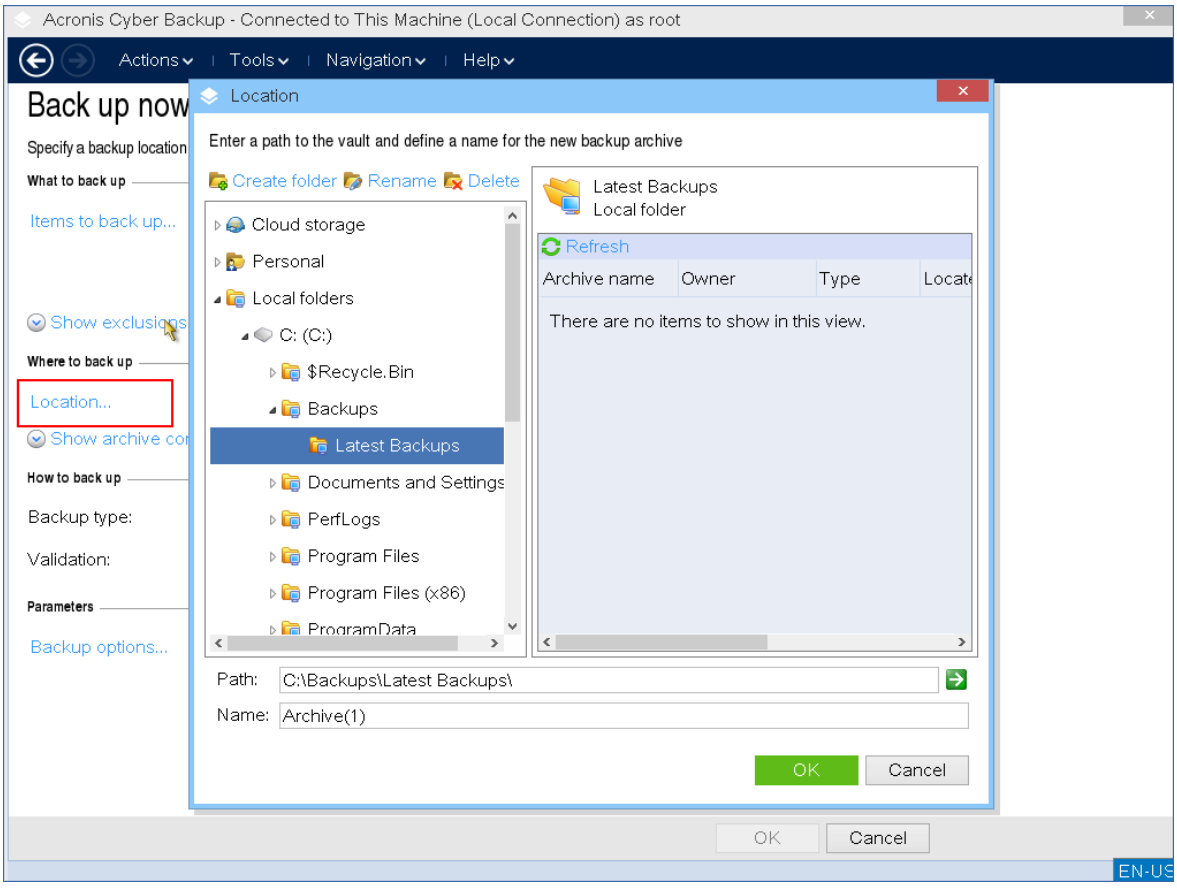
참고
Linux 기반 부트 가능한 미디어는 Windows와 드라이브 문자가 다를 수도 있습니다. 필요한 드라이브나 파티션을 크기나 레이블로 확인하십시오.



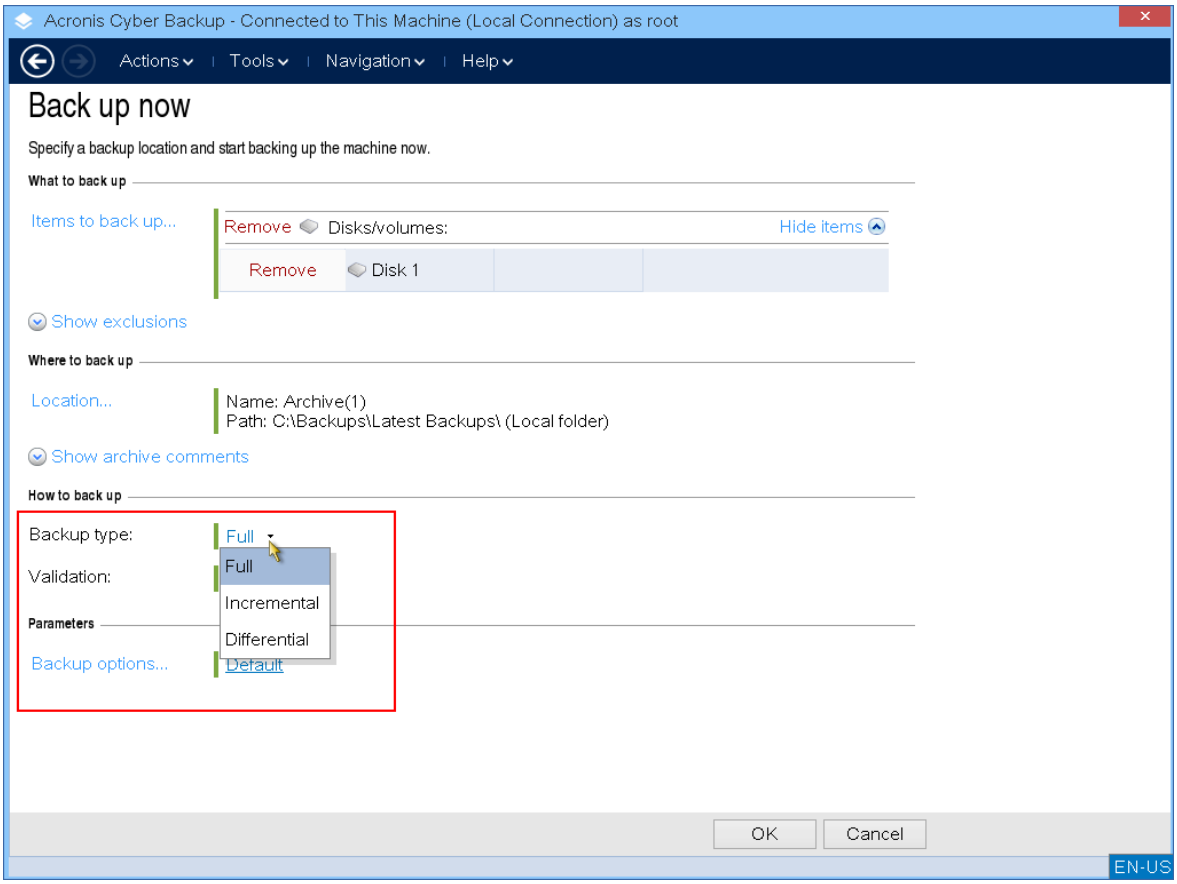
5. 디스크 대신 파일이나 폴더를 백업하려면 **백업할 데이터**에서 **파일**로 변경하십시오.
   부트 가능한 미디어에서는 디스크/파티션과 파일/폴더 백업만 가능합니다. 데이터베이스 백업과 같이 다른 백업 유형은 실행 중인 운영 체제에서만 가능합니다.



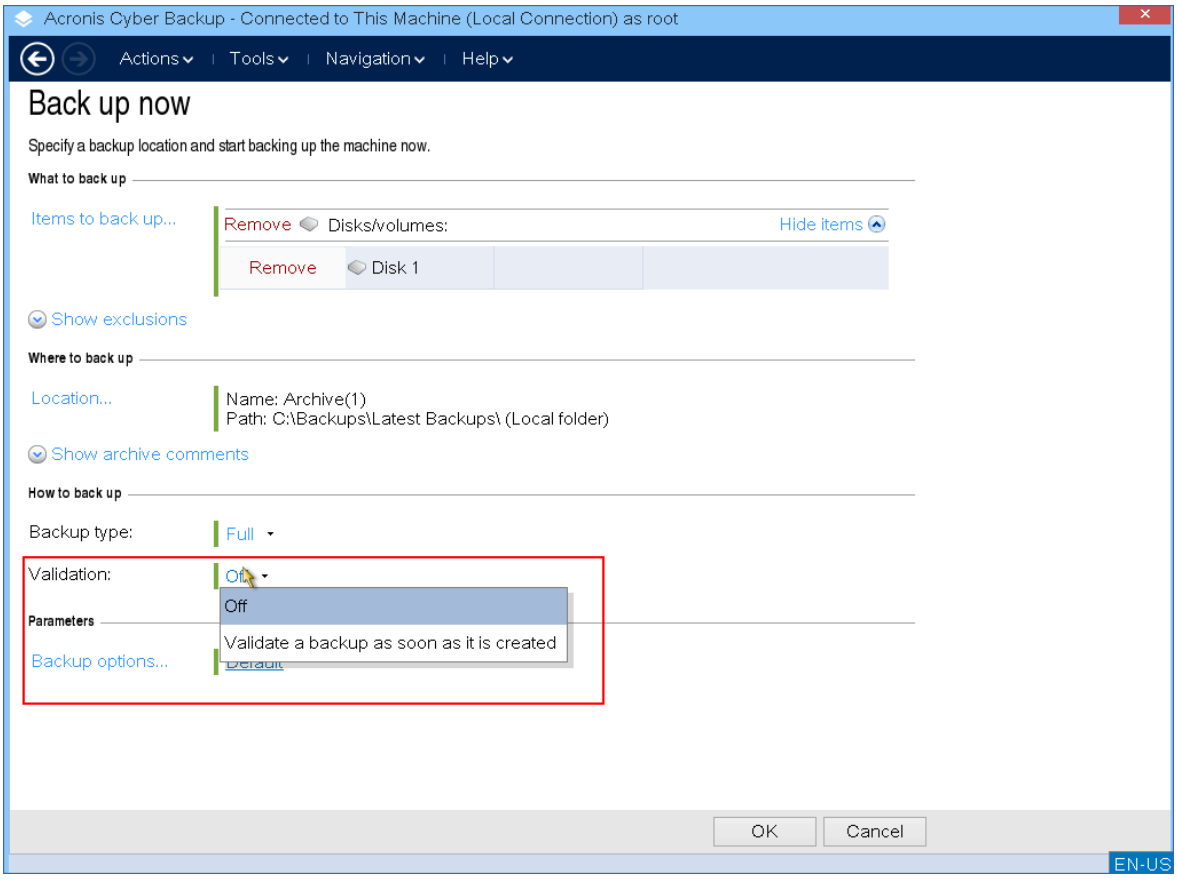
6. 백업 저장 위치를 선택하기 위해 **위치**를 클릭합니다.



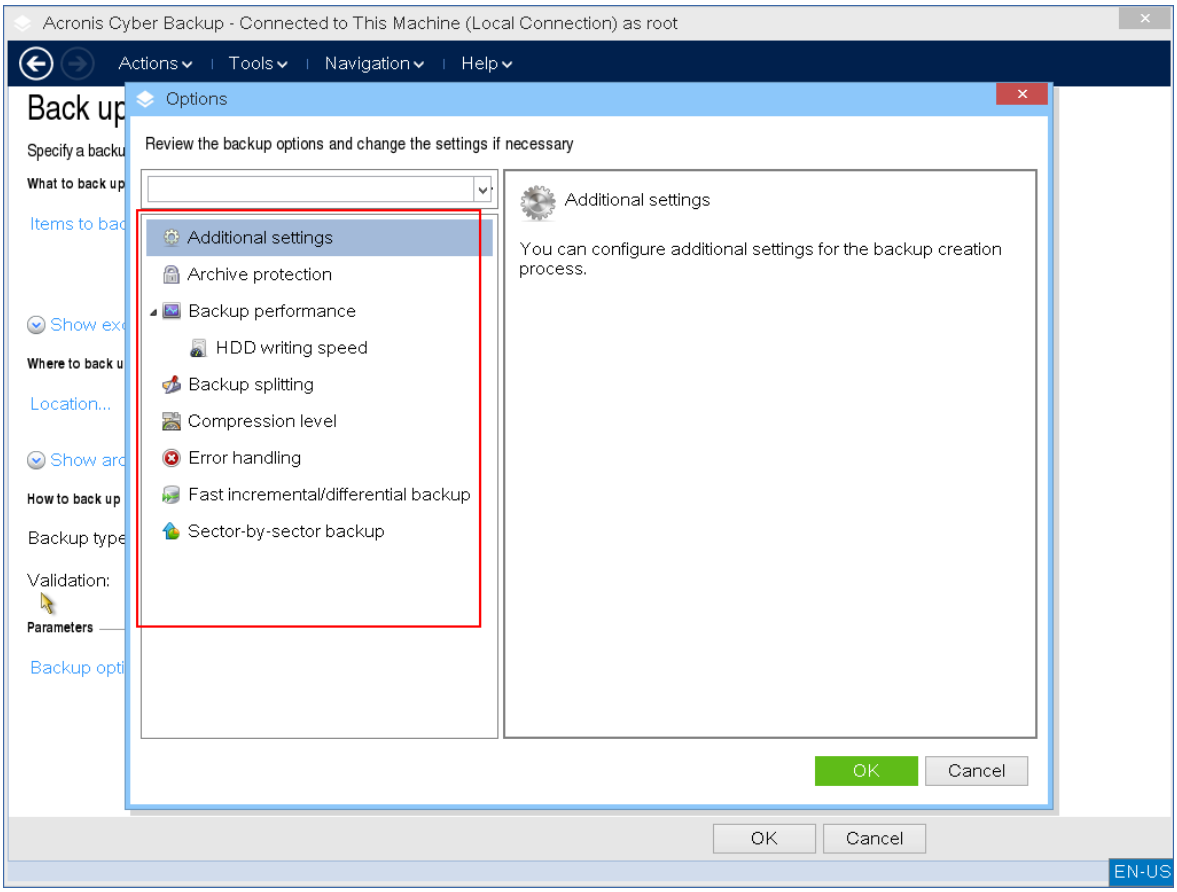
7. 위치와 백업 이름을 지정합니다.
8. 백업 유형을 지정합니다. 해당 위치에 처음 백업하는 경우, 전체 백업이 생성됩니다. 백업 체인을 계속할 경우, **등분** 혹은 **차등**을 선택해 공간을 절약할 수 있습니다. 지원되는 백업 유형에 대한 자세한 내용은 https://kb.acronis.com/content/1536을 참고하십시오.



9. [선택 사항] 백업 파일의 유효성을 검사하려면 **백업 생성 즉시 유효성 검사**를 선택하십시오.



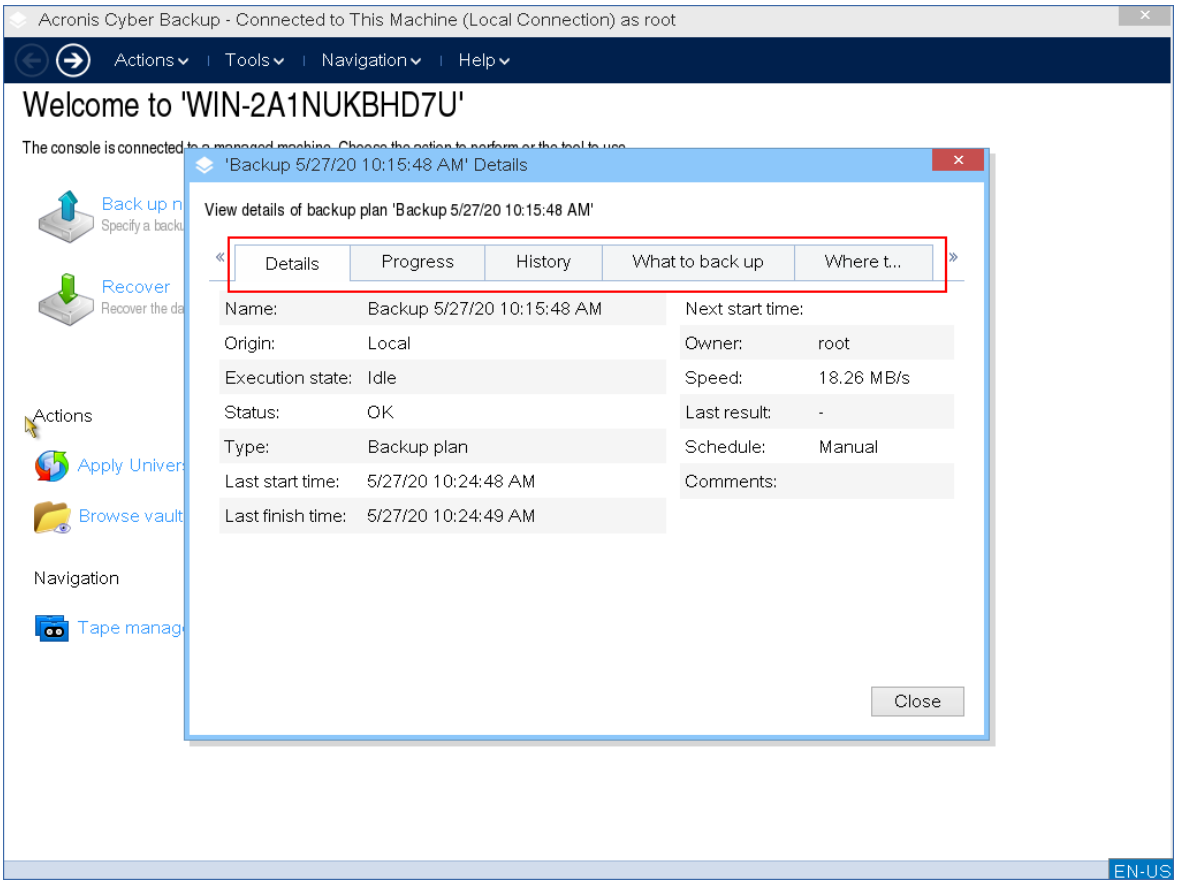
10. [선택 사항] 필요한 백업 옵션을 지정합니다. (예: 백업 파일 비밀번호 설정, 백업 분할, 오류 처리)



11. **확인**을 클릭하여 백업을 시작합니다.

    부트 가능한 미디어가 디스크에서 데이터를 읽고, .tib 파일로 압축하고, 선택한 위치에 파일을 작성합니다. 실행 중인 애플리케이션이 없으므로 디스크 스냅샷을 생성하지 않습니다.

12. 창이 나타나면 백업 작업 상태와 백업 관련 추가 정보를 확인할 수 있습니다.

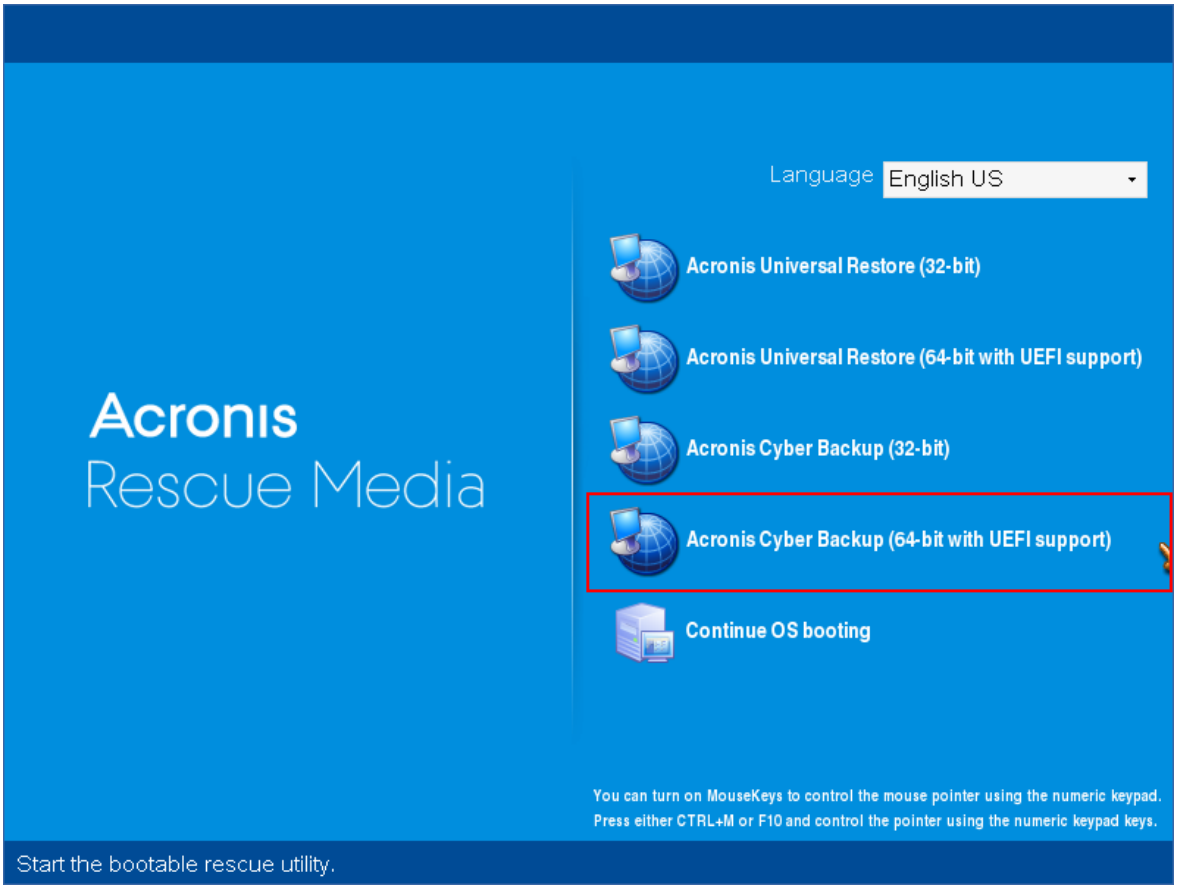


온프레미스의 부트 가능한 미디어를 사용한 복구

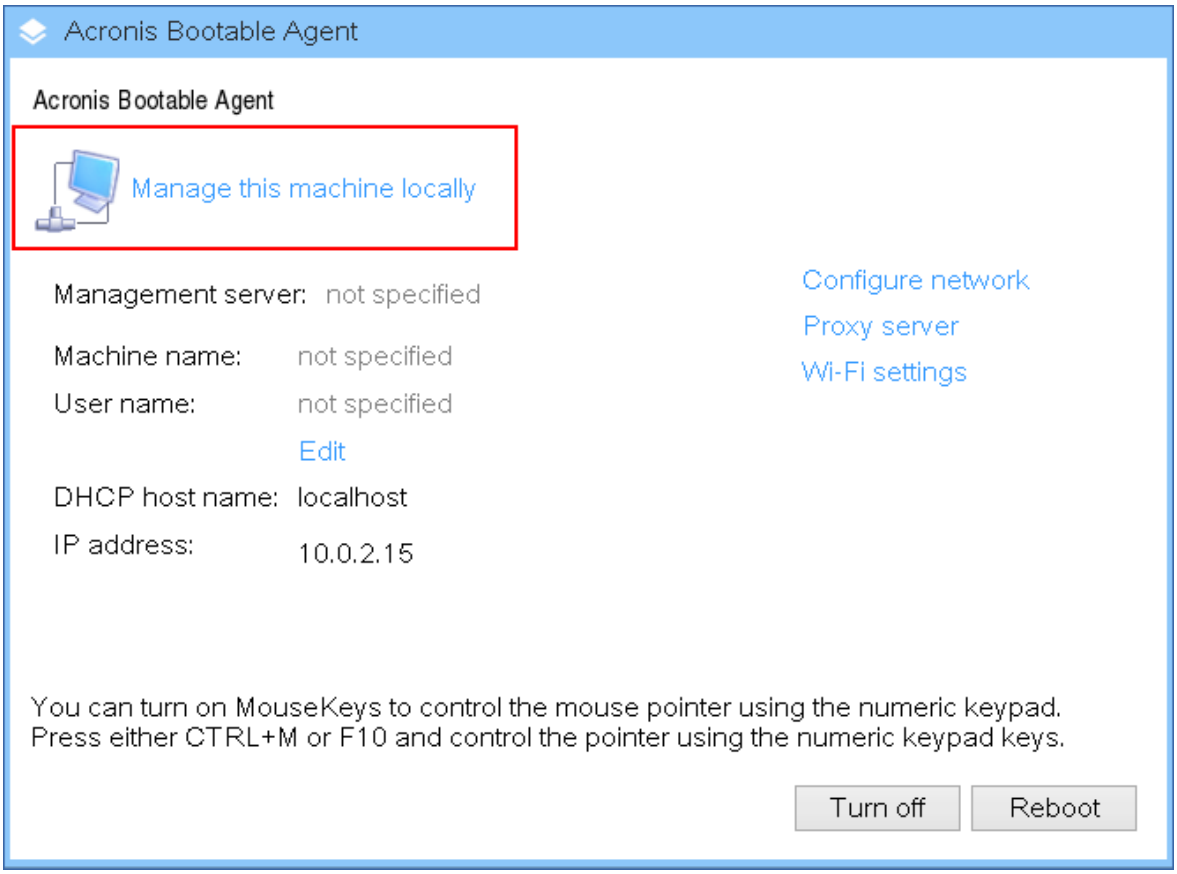
복구 작업은 부트 가능한 미디어 빌더로 생성된 부트 가능한 미디어와 다운로드 받은 이미 생성된 부트 가능한 미디어 모드에서 가능합니다.

부트 가능한 미디어에서 데이터 복구 방법

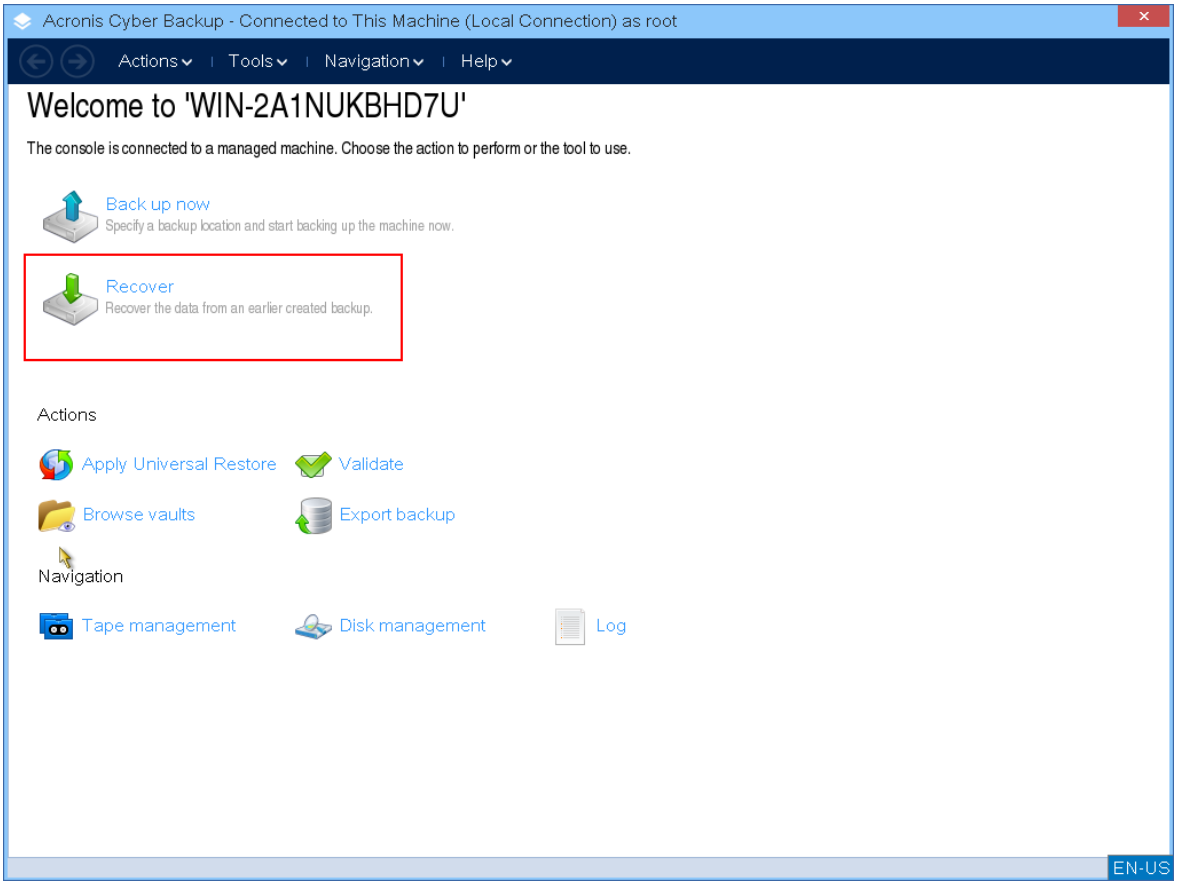
1. Acronis 부트 가능한 복구 미디어에서 부팅합니다.



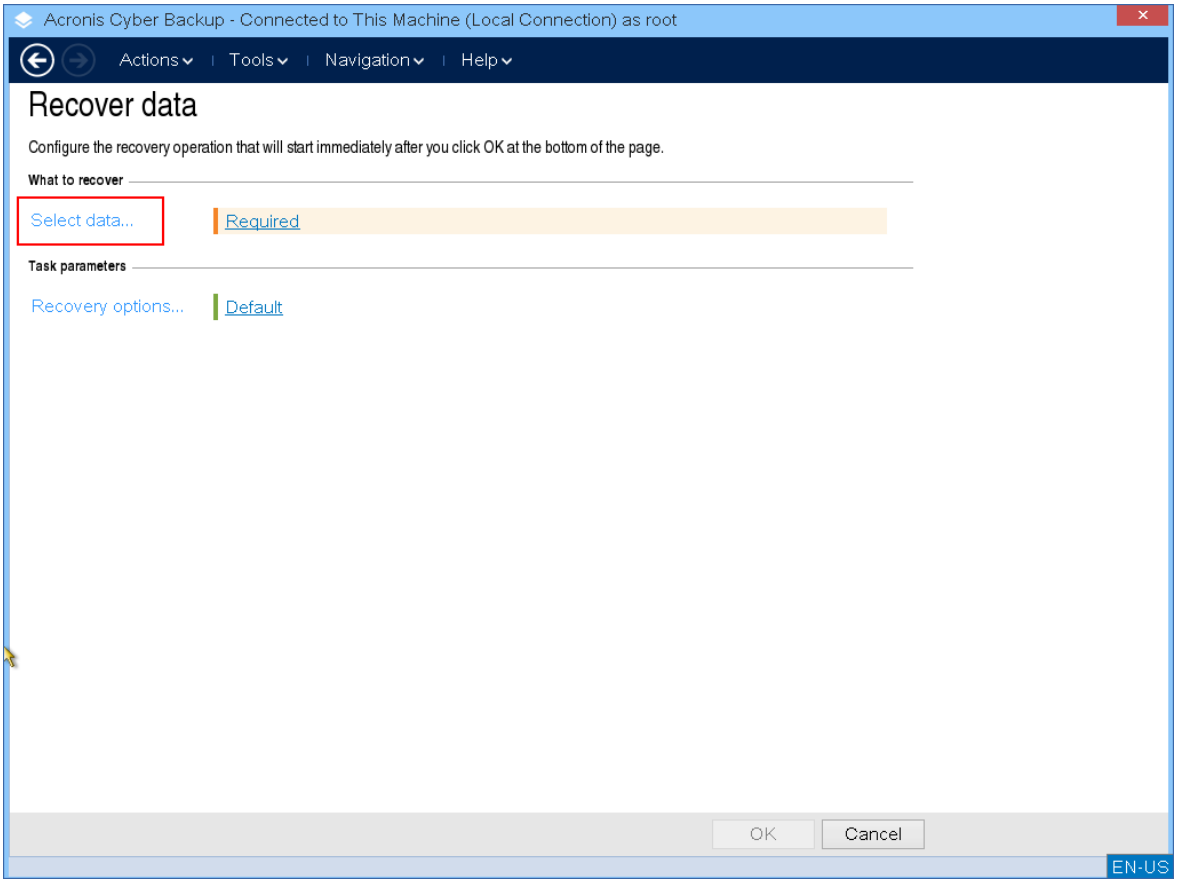
2. 로컬 머신에 데이터를 복구하려면 **이 머신을 로컬로 관리**를 클릭합니다. 원격 접속은 관리 서버에 미디어 등록을 참조하십시오.



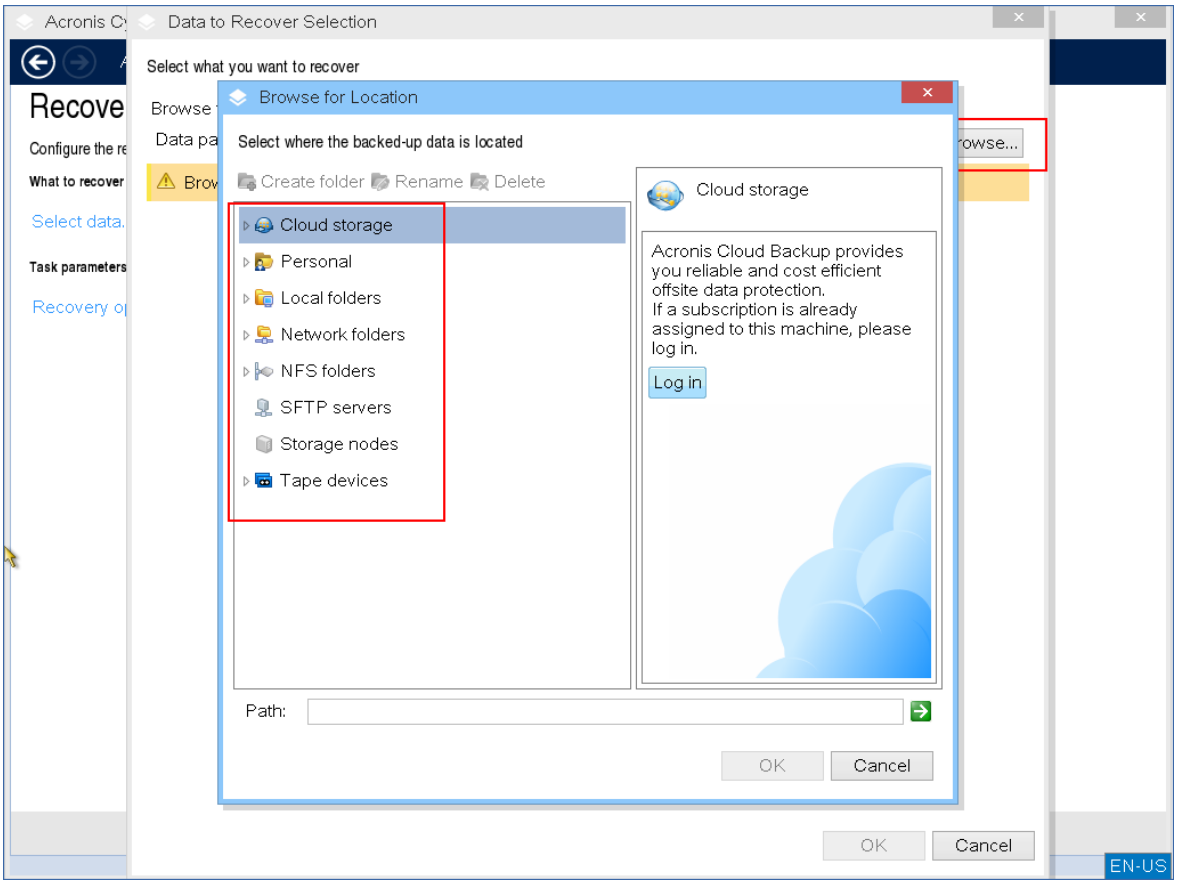
3. **복구**를 클릭합니다.



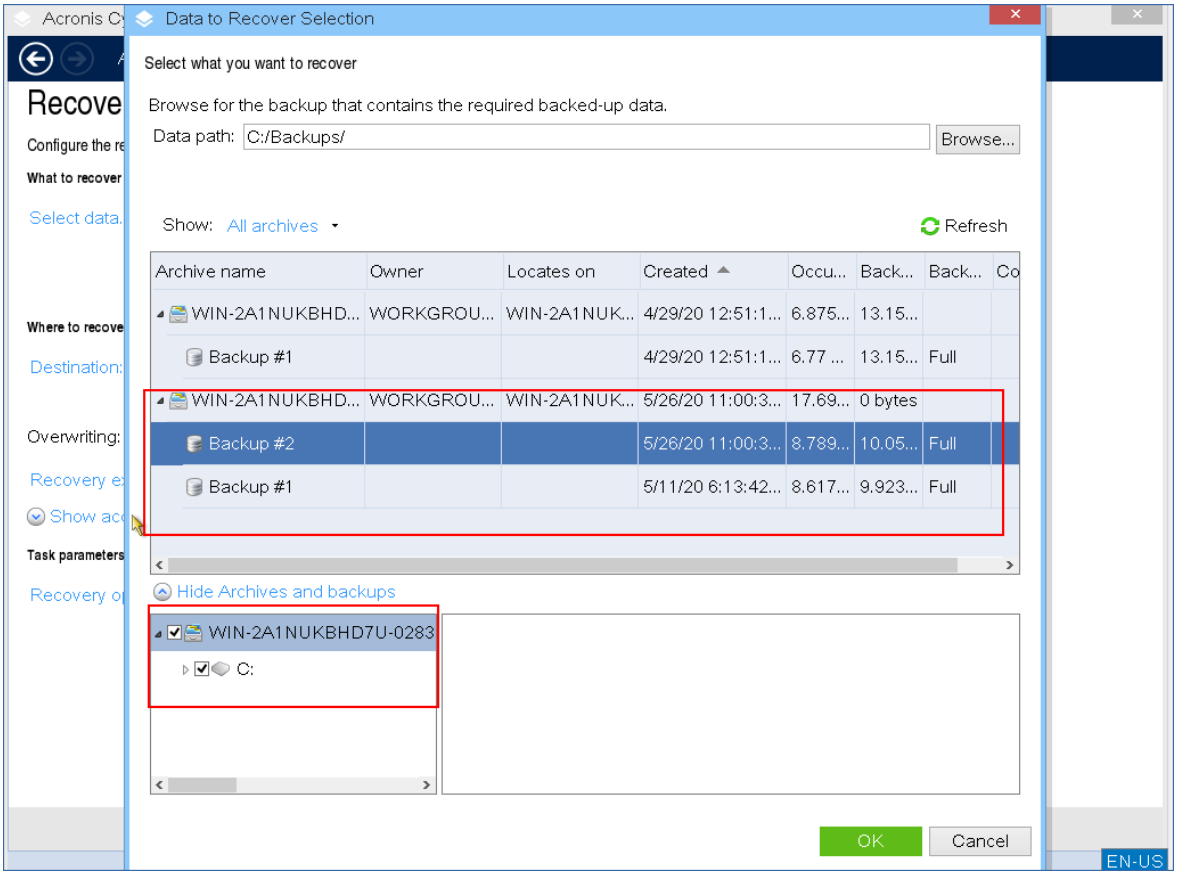
4. **복구 대상**에서 **데이터 선택**을 클릭합니다.



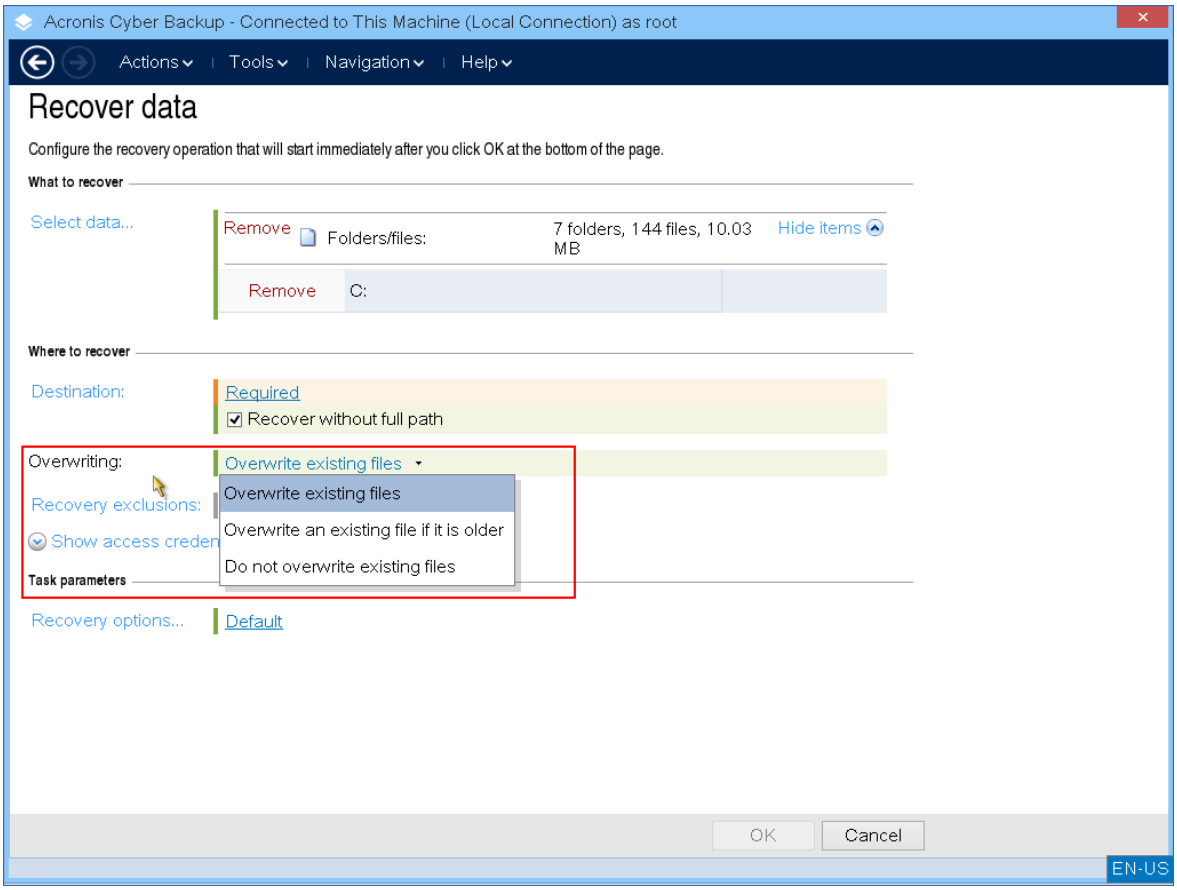
5. **찾아보기**를 클릭한 뒤 백업 위치를 선택합니다.



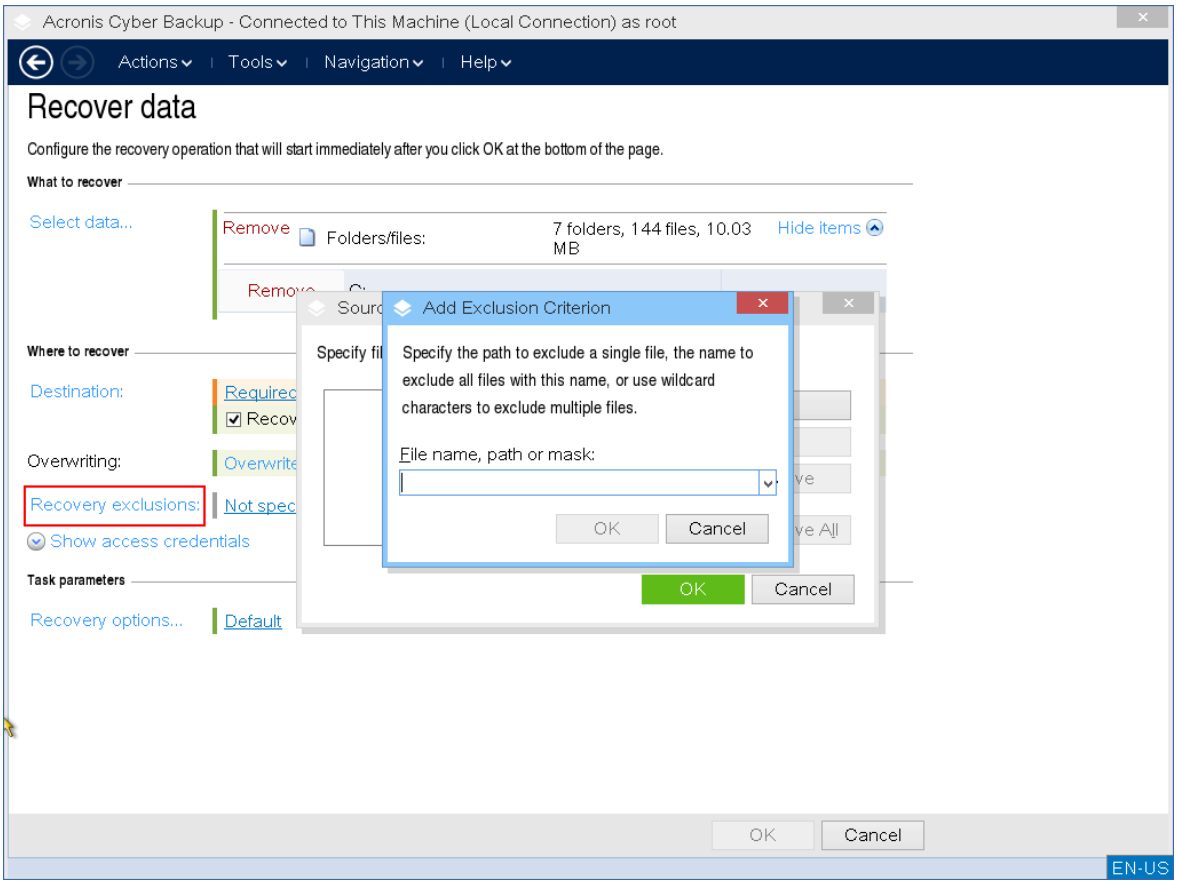
6. 복구할 백업 파일을 선택합니다.



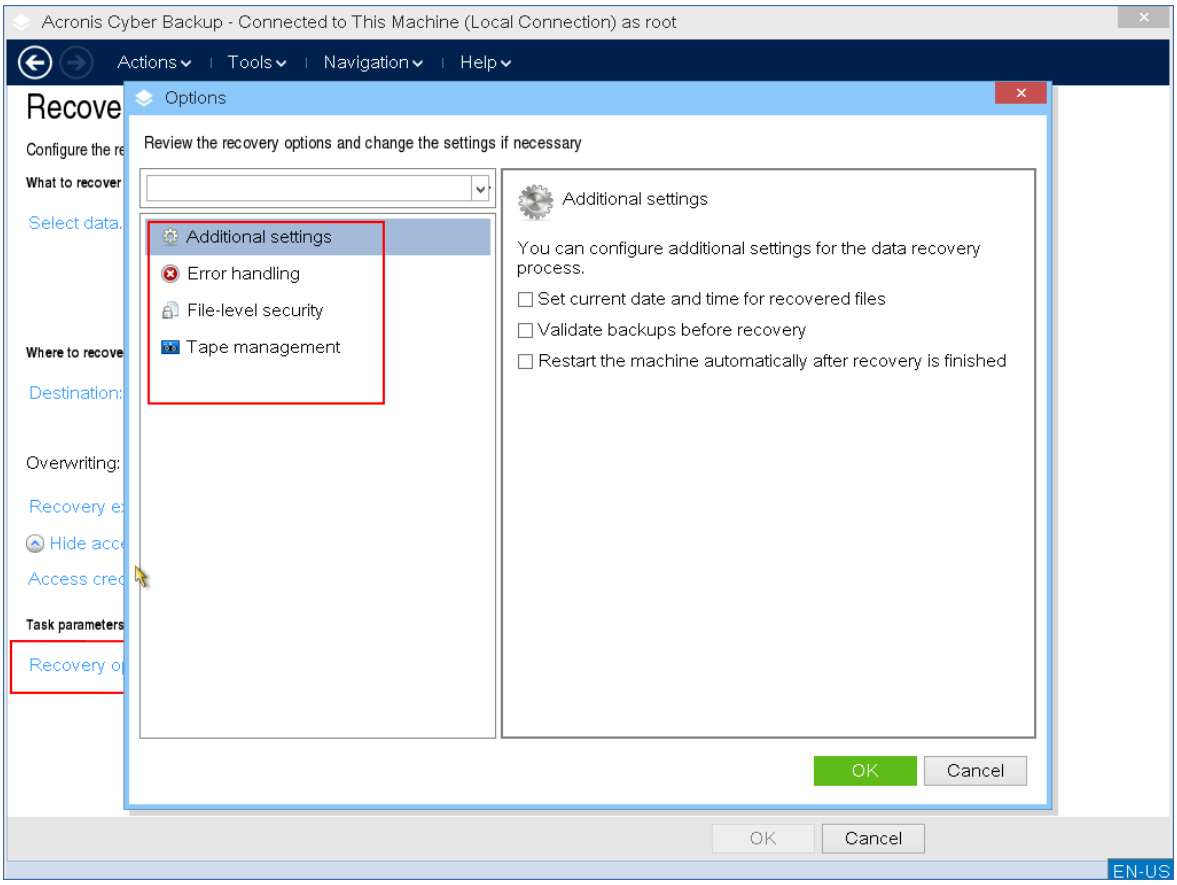
7. 왼쪽 하단 창에서 복구하려는 드라이브/볼륨을 선택한 뒤 **확인**을 클릭합니다.
8. [선택 사항] 덮어쓰기 규칙을 구성합니다.



9. [선택 사항] 복구 예외를 구성합니다.



10. [선택 사항] 복구 옵션을 구성합니다.



11. 설정이 올바른지 살펴본 뒤 **확인**을 클릭합니다.

참고
이기종 하드웨어에 데이터를 복구하려면 Acronis Universal Restore를 사용해야 합니다. 백업이 AcronisSecure Zone에 있는 경우에는
Acronis Universal Restore를 사용할 수 없습니다.

부트 가능한 미디어를 사용한 디스크 관리

Acronis 부트 가능한 미디어를 사용하면 Acronis Cyber Protect(으)로 백업된 볼륨 이미지를 복구하기 위해 디스크/볼륨 구성을 준비할 수 있습니다.

때로는 볼륨이 백업된 후에 해당 이미지가 안전한 스토리지에 배치되면, 머신 디스크 구성이 HDD 교체 또는 하드웨어 유실로 인해 변경될 수도 있습니다. 이러한 경우, 사용자는 볼륨 이미지를 "있는 그대로" 복구하거나 사용자가 필요하다고 생각하는 대로 디스크나 볼륨 구조를 변경한 상태로 볼륨 이미지를 복구할 수 있도록 필요한 디스크 구성을 다시 생성할 수 있습니다.

가능한 데이터 손실을 피하기 위해 필요한 모든 사전 주의 조치를 취하십시오.

중요

디스크와 볼륨에서의 모든 작업은 특정 데이터 손상 위험이 관련됩니다. 시스템, 부트 가능한 볼륨 또는 데이터 볼륨에서의 작업은 부팅 프로세스 또는 하드 디스크 데이터 저장소 관련 문제를 피하기 위해 매우 조심스럽게 수행해야 합니다.

하드 디스크 및 볼륨 관련 작업에는 어느 정도의 시간이 소모되며, 작업 중에 전력 손실이나 의도하지 않은 머신의 전원차단, 또는 실수로 리셋 버튼을 누르게 되면 볼륨 손상 및 데이터 손실을 가져올 수 있습니다.

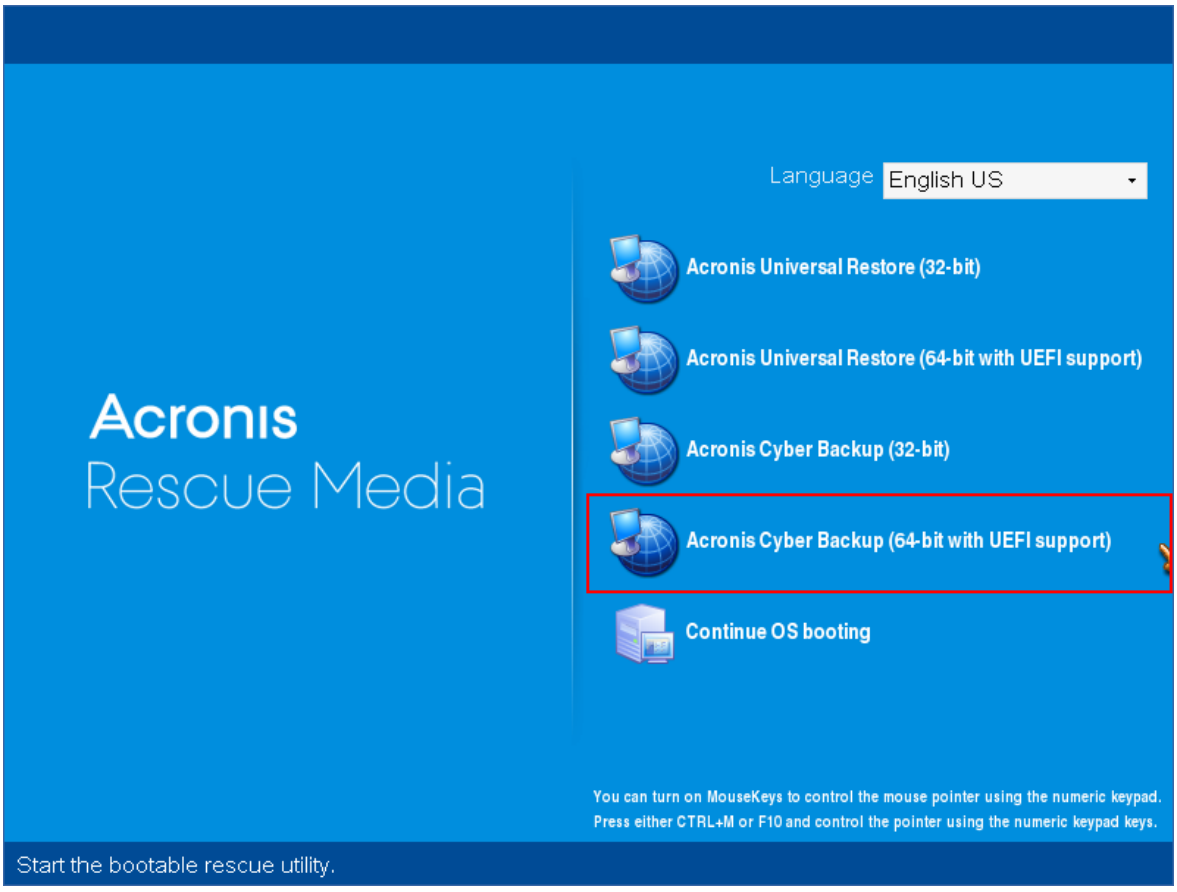
베어 메탈, 부팅할 수 없는 머신 또는 Windows가 아닌 머신에서 디스크 관리를 실행할 수 있습니다. Bootable Media Builder와 Acronis Cyber Protect 라이센스 키를 사용해 생성한 부트 가능한 미디어가 필요합니다. 부트 가능한 미디어를 생성하는 방법에 대한 자세한 내용은 Linux 기반 부트 가능한 미디어 또는 Windows-PE 기반 부트 가능한 미디어를 참조하십시오.

참고

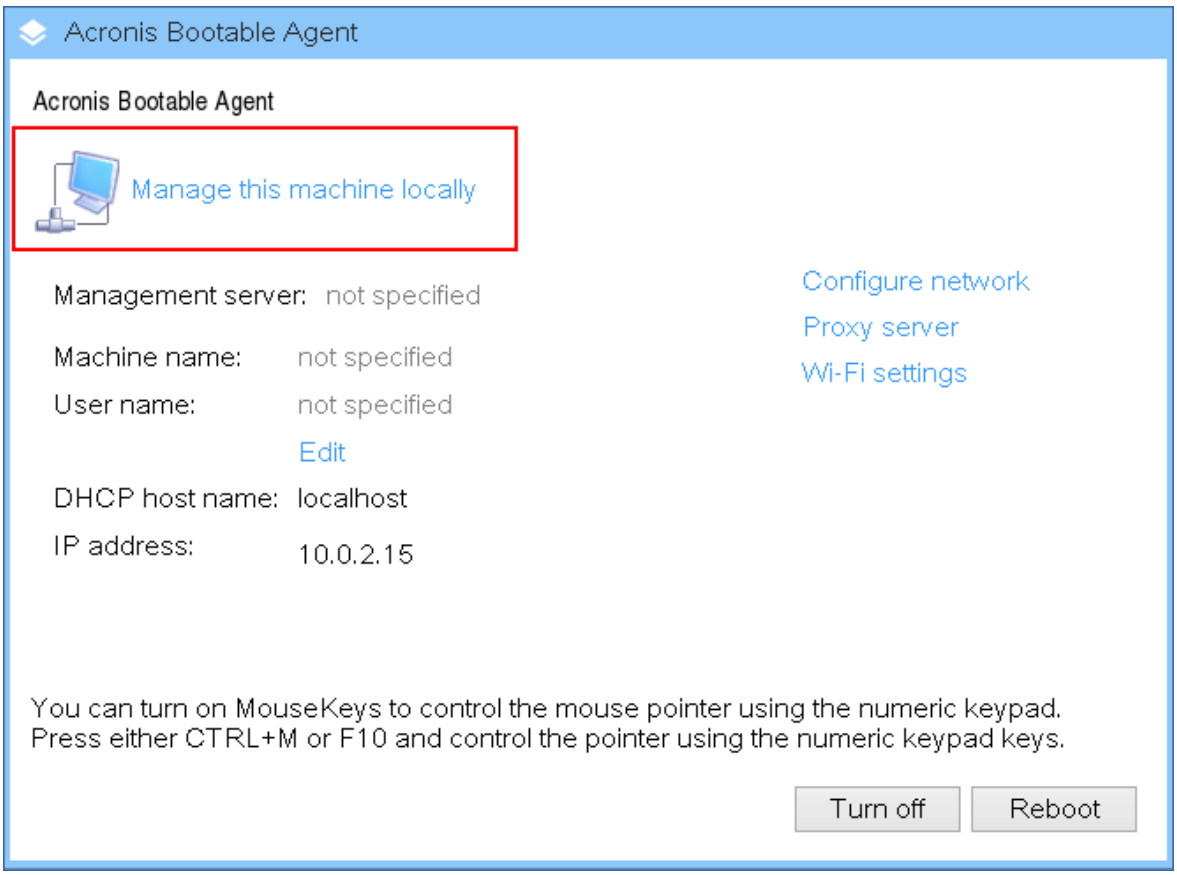
Windows PE 4.0 이상을 기반으로 하는 부트 가능한 미디어에서는 디스크 관리 기능을 사용할 수 없습니다. 따라서 디스크 관리 기능은 Windows 7 이하 운영 체제에서 지원됩니다. Windows 8 이상에서 디스크 관리 작업을 수행하려면 Acronis Disk Director를 설치해야 합니다. 자세한 내용은 다음 KB 문서를 참조하십시오. https://kb.acronis.com/content/47031

디스크 관리 작업 수행 방법

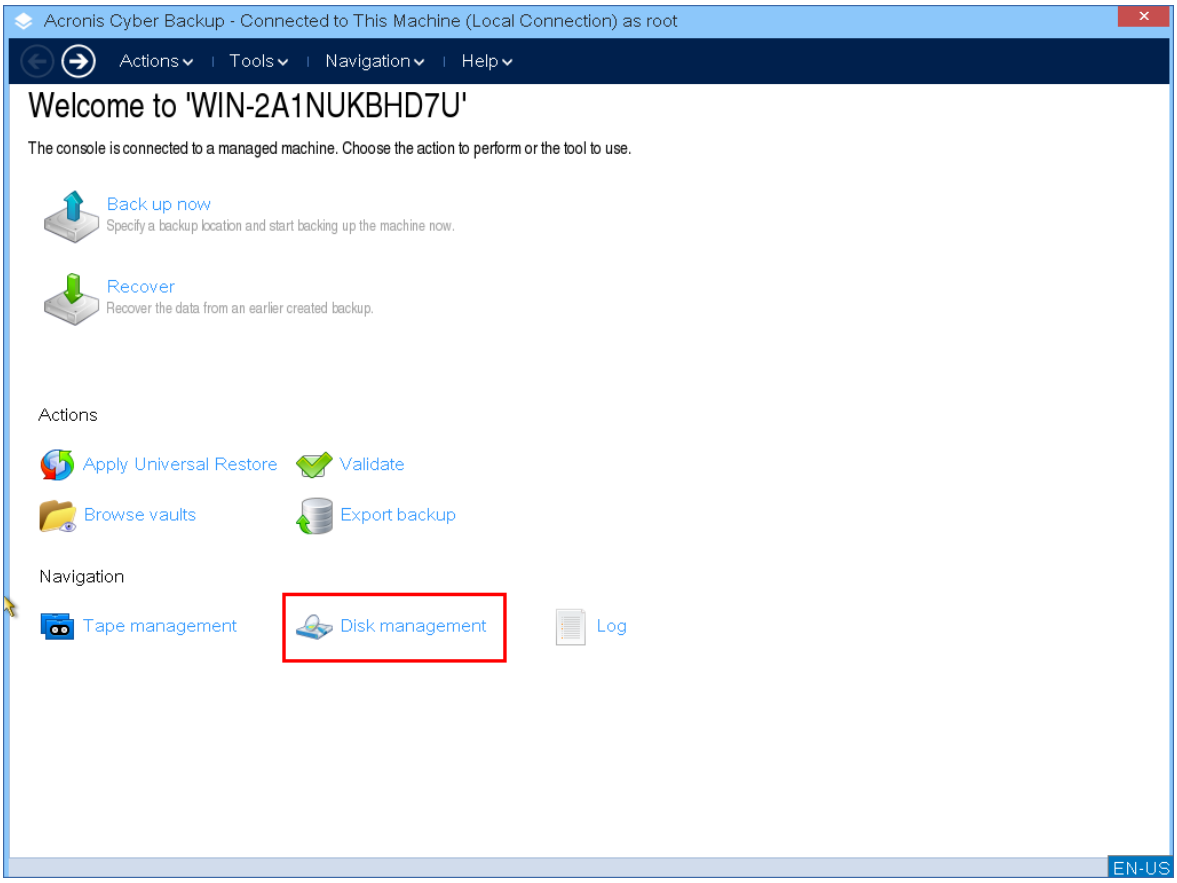
1. Acronis 부트 가능한 복구 미디어에서 부팅합니다.



2. 로컬 머신으로 작업하려면 **이 머신을 로컬로 관리**를 클릭합니다. 원격 접속은 관리 서버에 미디어 등록을 참조하십시오.



3. **디스크 관리**를 클릭합니다.



참고

저장 공간이 머신에 구성된 경우 부트 가능한 미디어의 디스크 관리 작업이 잘못 작동할 수 있습니다.

지원되는 파일 시스템

부트 가능한 미디어는 다음의 파일 시스템 관리 작업을 지원합니다.

- FAT 16/32
- NTFS

파일 시스템이 다른 볼륨에서 작업을 수행해야 하는 경우 정식 버전의 Acronis Disk Director를 사용합니다. 다음 파일 시스템의 경우 이 프로그램에서 디스크와 볼륨을 관리하는 다양한 도구와 유틸리티를 사용할 수 있습니다.

- FAT 16/32
- NTFS
- Ext2
- Ext3
- HFS+
- HFSX
- ReiserFS

- JFS
- Linux SWAP

기본 사전 주의 사항

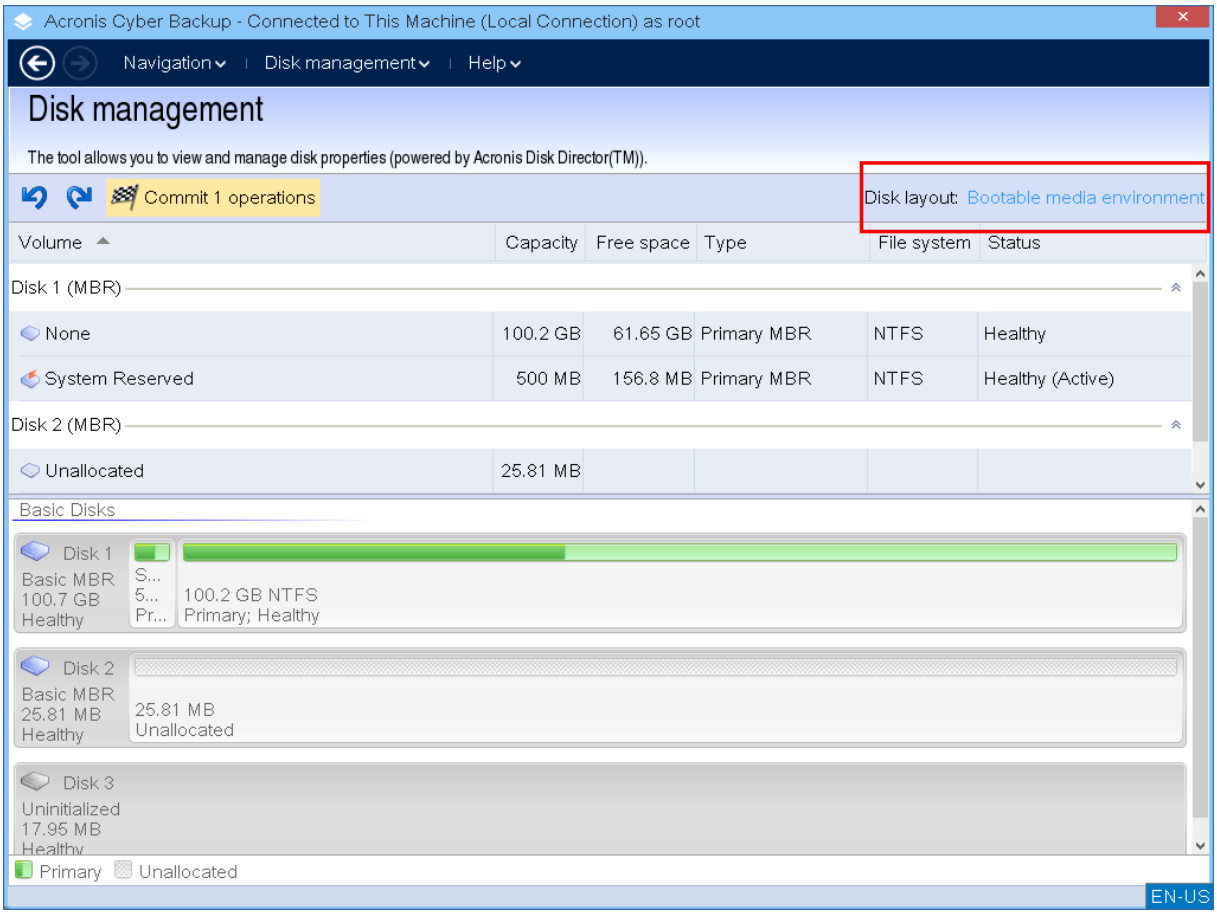
가능한 디스크 및 볼륨 구조 손상 또는 데이터 손상을 피하기 위해서는 필요한 모든 사전 주의 사항을 수행하고 다음 가이드라인을 따르십시오.

1. 볼륨이 만들어지거나 관리되는 디스크를 백업하십시오. 가장 중요한 데이터를 다른 하드 디스크, 네트워크 공유 또는 이동식 미디어에 백업하면 데이터가 안전하다는 것을 알고 디스크 볼륨에서 작업할 수 있습니다.
2. 디스크가 완전한 기능을 하고 손상된 섹터 또는 파일 시스템 오류가 없는지 확인하기 위해 디스크를 테스트합니다.
3. 하위 수준의 디스크 접근을 사용하는 소프트웨어를 실행하는 중에 디스크/볼륨 작업을 수행하지 마십시오.

디스크 관리를 위한 운영 체제 선택

두 개 이상의 운영 체제가 있는 머신에서 디스크 및 볼륨 표시는 현재 실행 중인 운영 체제에 따라 달라집니다. 같은 볼륨이라도 운영 체제가 다르면 문자가 다를 수 있습니다.

디스크 관리 작업을 수행할 경우 운영 체제를 표시할 디스크 레이아웃을 지정해야 합니다. 그러려면 **디스크 레이아웃** 레이블 옆의 운영 체제 이름을 클릭한 뒤 창이 열리면 원하는 운영 체제를 선택하십시오.



디스크 작업

부트 가능한 미디어로 다음의 디스크 관리 작업을 실행할 수 있습니다.

- 디스크 초기화 - 시스템에 추가된 새 하드웨어를 초기화합니다
- 기본 디스크 복제 - 원본 기본 MBR 디스크의 전체 데이터를 대상 디스크로 전송합니다
- 디스크 변환: MBR에서 GPT로 - MBR 파티션 테이블을 GPT로 변환합니다
- 디스크 변환: GPT에서 MBR로 - GPT 파티션 테이블을 MBR로 변환합니다
- 디스크 변환: 기본에서 동적으로 - 기본 디스크를 동적으로 변환합니다
- 디스크 변환: 동적에서 기본으로 - 동적 디스크를 기본으로 변환합니다

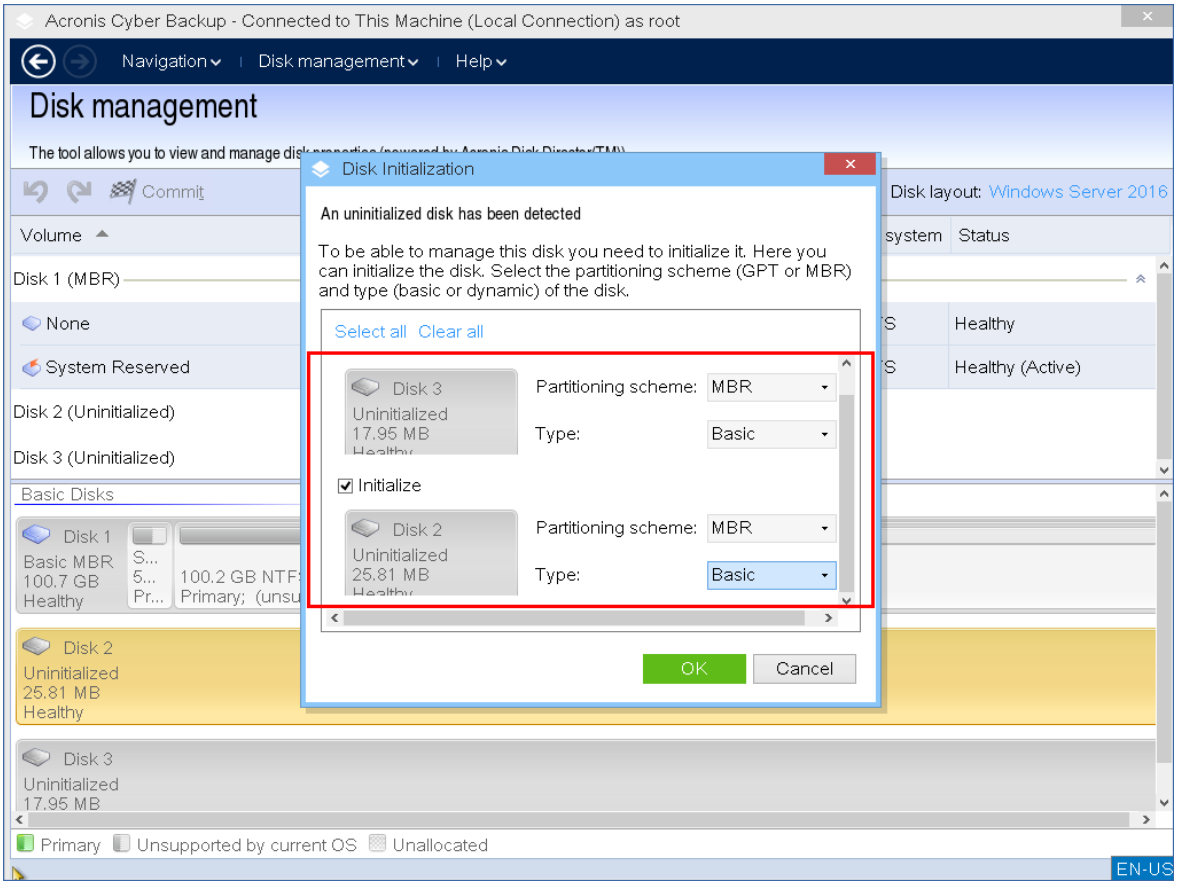
디스크 초기화

부트 가능한 미디어가 초기화되지 않은 디스크가 회색 아이콘과 함께 회색 블록으로 표시되어 시스템이 이 디스크를 사용할 수 없음을 나타냅니다.

디스크 초기화 방법

1. 원하는 디스크를 마우스 오른쪽 버튼으로 클릭한 다음 **초기화**를 클릭합니다.
2. 이 **디스크 초기화** 창에서 디스크 파티셔닝 구성표(MBR 또는 GPT) 및 디스크 유형(기본 또는 동적)을 설정합니다.
3. **확인**을 클릭하면 디스크를 초기화하는 대기 작업이 추가됩니다.

4. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.
5. 초기화 후에 모든 디스크 공간은 비할당된 상태입니다. 볼륨 생성으로 사용할 수 있습니다.



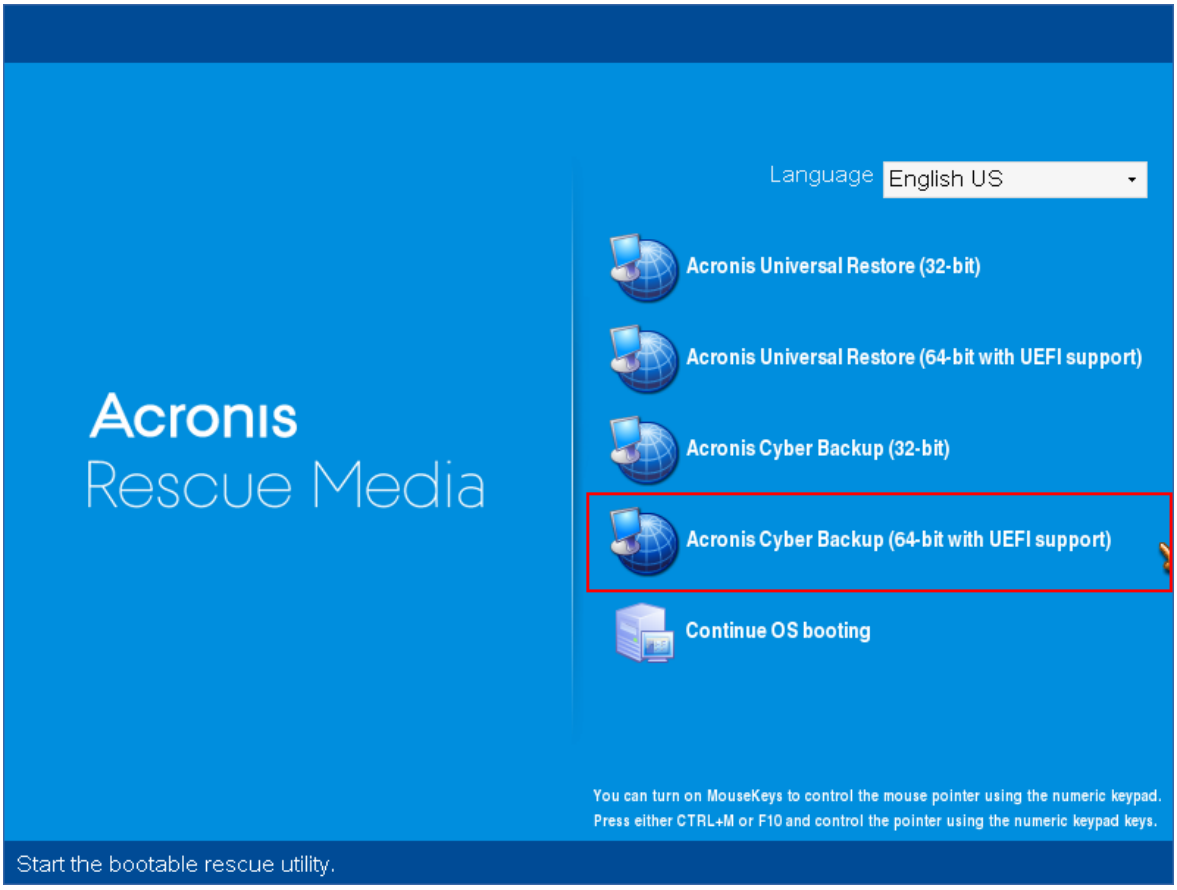
기본 디스크 복제

완비 Linux 기반 부트 가능한 미디어로 기본 MBR 디스크를 복제할 수 있습니다. 다운로드받을 수 있는 이미 생성된 부트 가능한 미디어나 라이센스 키 없이 생성된 부트 가능한 미디어에서는 디스크 복제가 불가능합니다.

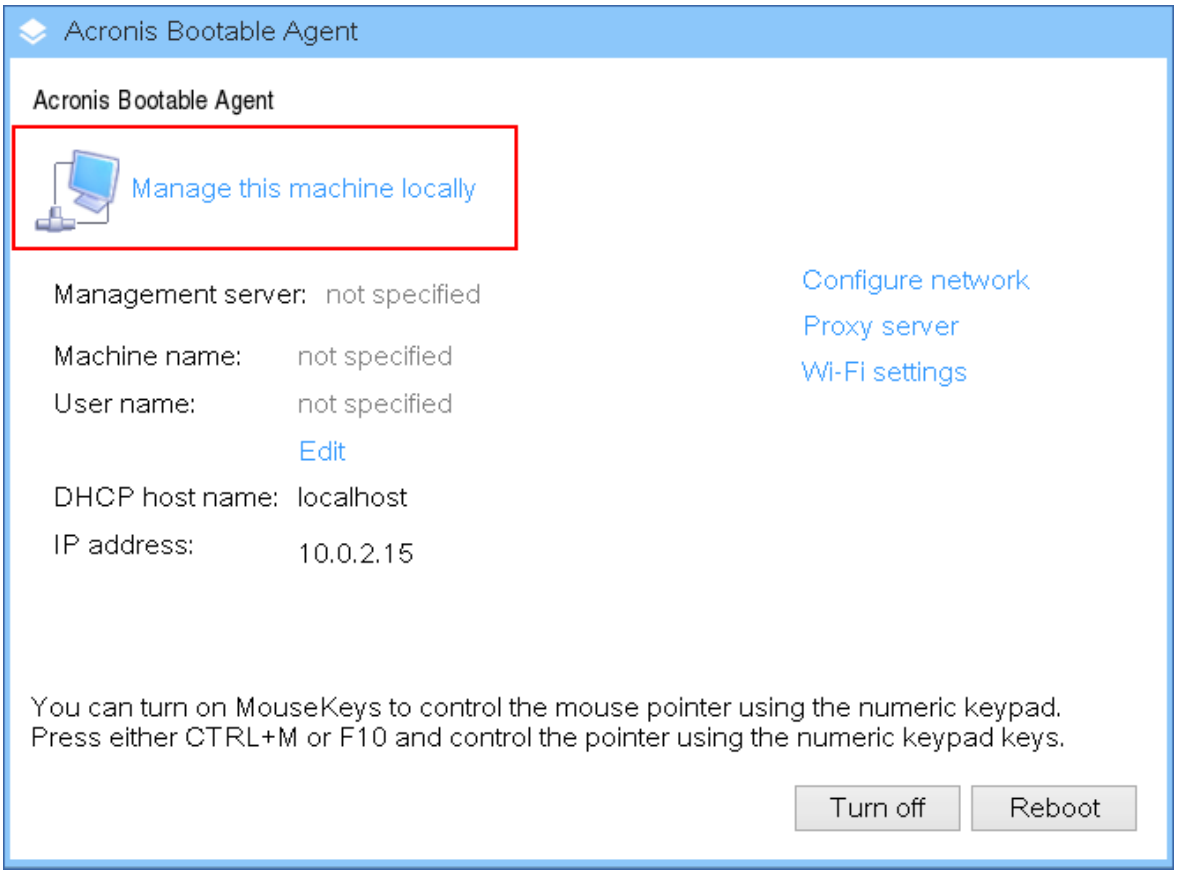
참고
AcronisCyber Protect 명령줄 유틸리티로 디스크를 복제할 수도 있습니다.

부트 가능한 미디어에서 기본 디스크 복제 방법

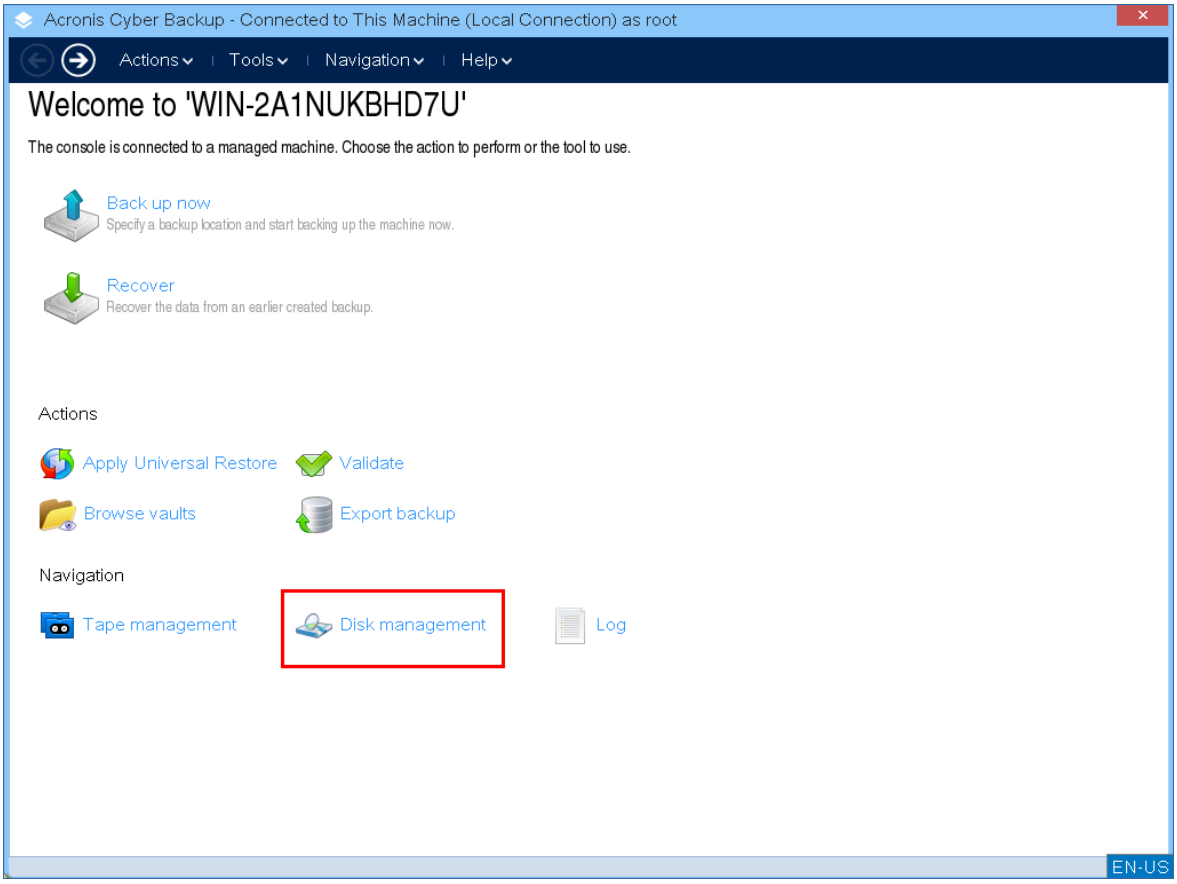
1. Acronis 부트 가능한 복구 미디어에서 부팅합니다.



2. 로컬 머신의 디스크를 복제하려면 **이 머신을 로컬로 관리**를 클릭합니다. 원격 접속은 관리 서버에 미디어 등록을 참조하십시오.

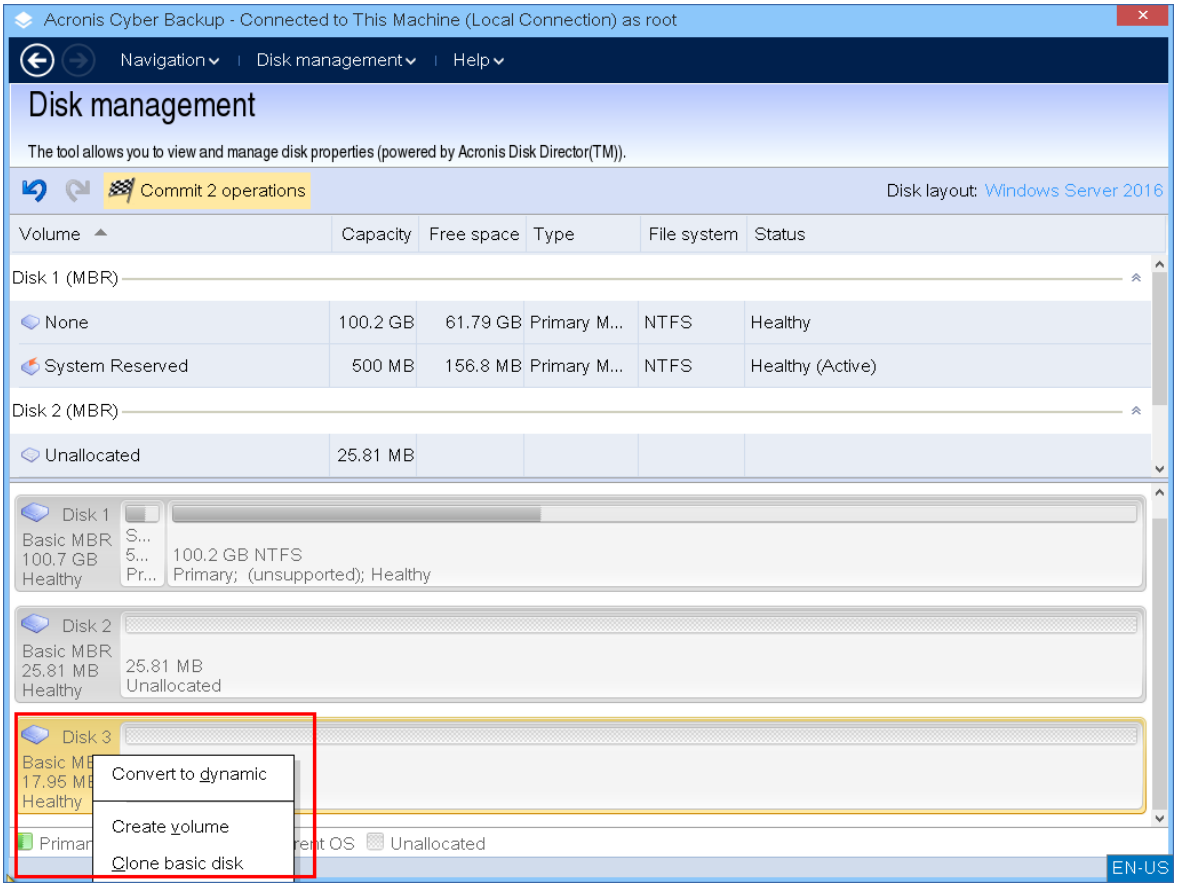


3. **디스크 관리**를 클릭합니다.

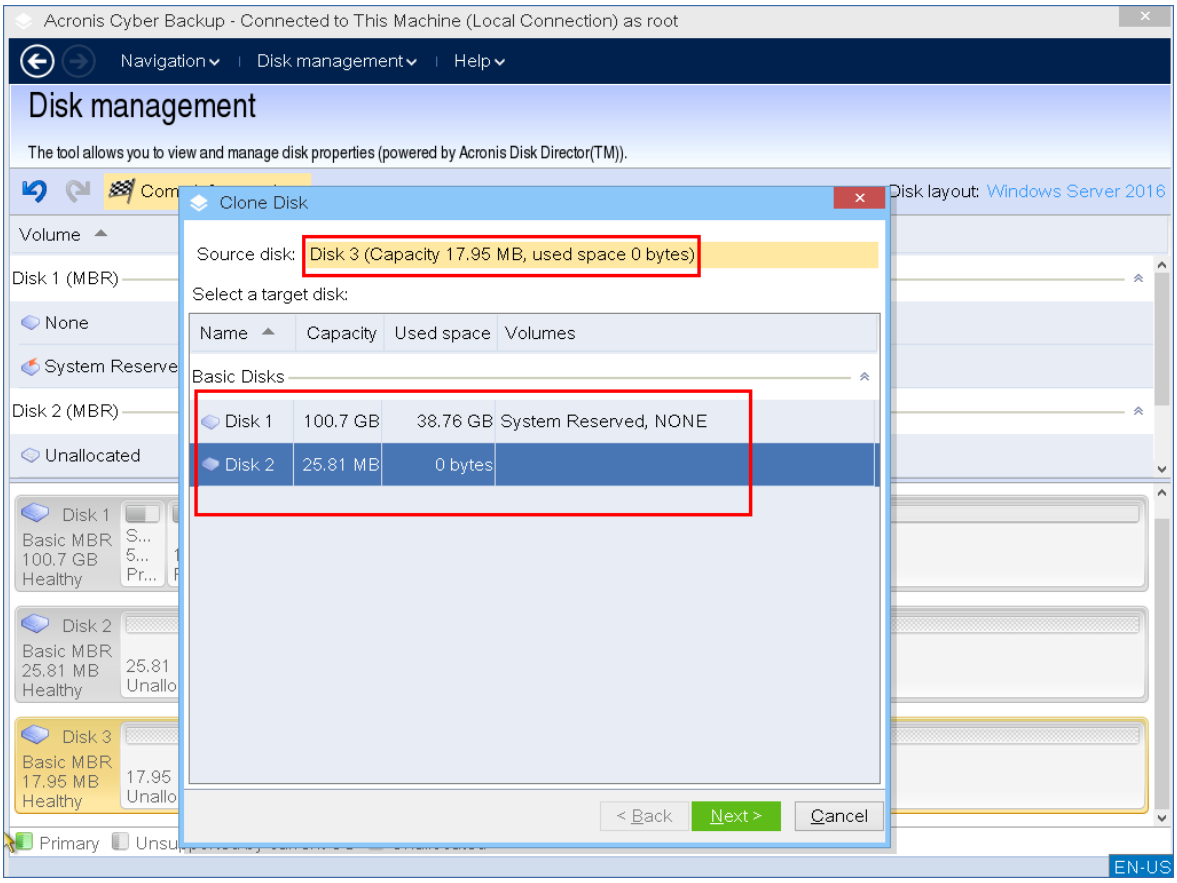


4. 이용 가능한 디스크가 표시됩니다. 복사할 디스크를 오른쪽 버튼으로 클릭한 뒤 **기본 디스크 복제**를 클릭합니다.

참고
전체 디스크만 복제할 수 있습니다. 파티션 복제는 사용할 수 없습니다.

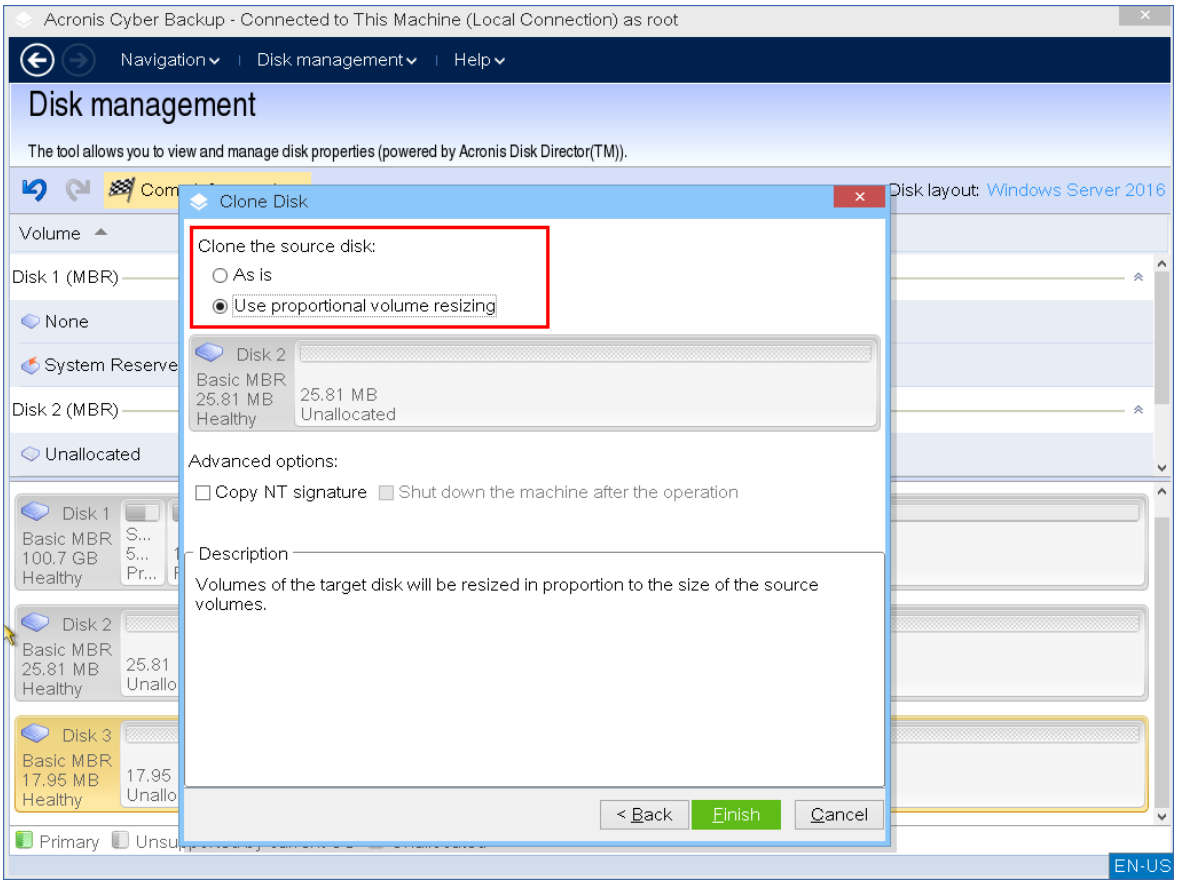


5. 이용 가능한 대상 디스크의 목록이 표시됩니다. 디스크 용량이 원본 디스크의 모든 데이터를 손실 없이 보관할 정도로 충분하다면 프로그램에서 사용자가 대상 디스크를 선택할 수 있습니다. 대상 디스크를 선택한 뒤, **다음**을 클릭합니다.

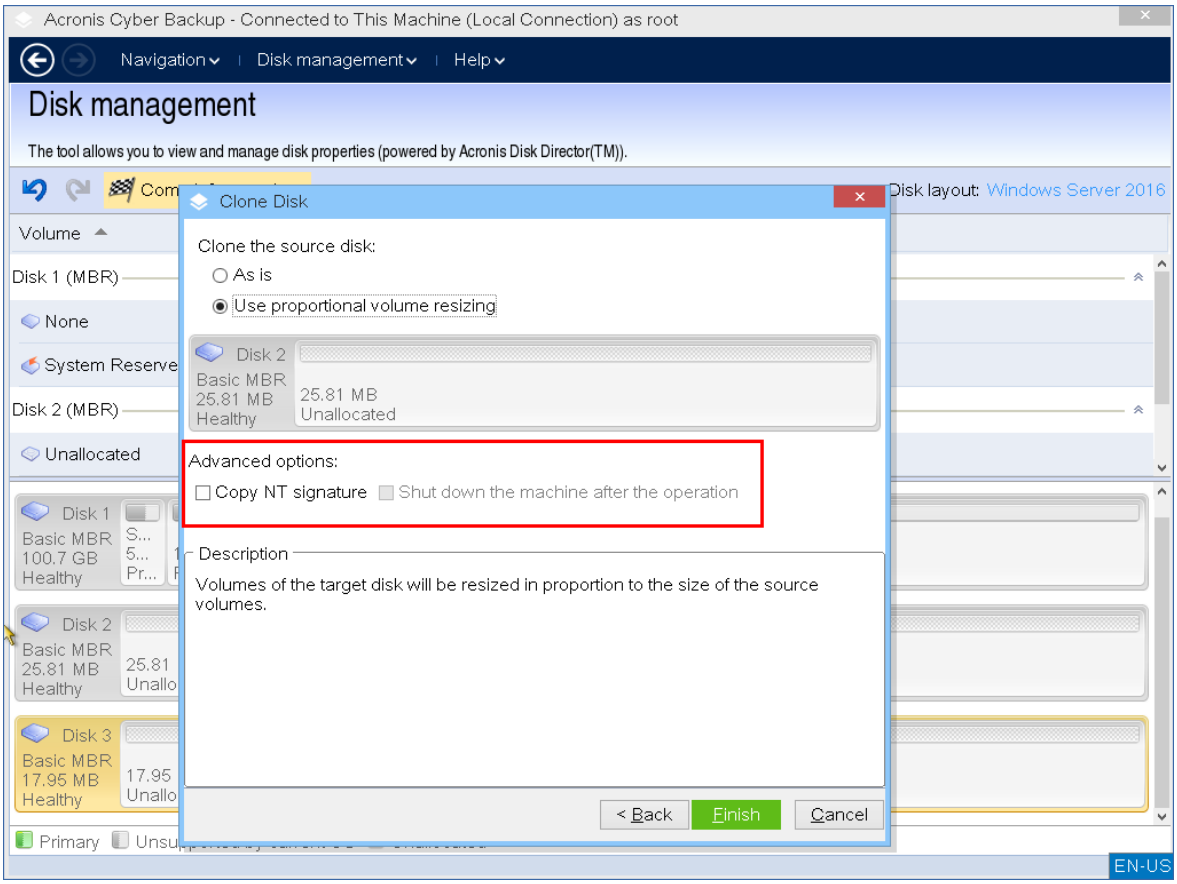


대상 디스크가 더 큰 경우에는 대상 디스크에 할당되지 않은 공간을 남기지 않도록 하기 위해 디스크 자체를 복제하거나 원본 디스크 볼륨의 크기를 조정하는 것이 좋습니다.
대상 디스크의 크기가 작다면, 크기 비례 조정만 가능합니다. 비례 크기 조정 이후에도 안전한 복제가 불가능한 경우 작업을 계속할 수 없습니다.

중요
대상 디스크에 데이터가 있으면 다음과 같은 경고가 표시됩니다. "*선택한 대상 디스크가 비어 있지 않습니다. 볼륨의 데이터를 덮어씁니다.*" 작업을 진행하면 현재 대상 디스크에 있는 모든 데이터가 돌이킬 수 없이 손실됩니다.



6. NT 서명 복사 여부를 선택합니다.



시스템 볼륨을 구성하는 디스크를 복제할 때에는 대상 디스크 볼륨에서 운영 체제 부팅 기능을 가지고 있어야 합니다. 즉 운영 체제에는 MBR 디스크 레코드에 보관되어 있는 디스크 NT 서명과 일치하는 시스템 볼륨 정보(예: 볼륨 문자)가 있어야 합니다. 그러나 NT 서명이 같은 두 개의 디스크는 하나의 운영 체제 아래에서는 제대로 작동할 수 없습니다.

같은 NT 서명이 있고 한 머신에서 머신 볼륨을 구성하는 두 개의 디스크가 있는 경우에는 시작 시에 운영 체제가 첫 번째 디스크에서 실행되고, 두 번째 디스크에서 동일한 서명을 발견하고, 새로운 고유한 NT 서명을 자동으로 생성하고 이를 두 번째 디스크에 할당합니다. 그 결과 두 번째 디스크에 있는 모든 볼륨은 문자를 잃게 되고 디스크에서 모든 경로가 올바르지 않게 되고 프로그램은 파일을 찾지 못하게 됩니다. 해당 디스크의 운영 체제는 부팅할 수 없게 됩니다.

대상 디스크 볼륨에서 시스템 부팅 기능을 유지하는 방법은 다음과 같습니다.

a. **NT 서명 복사** – 대상 디스크에 복사될 레지스트리 키와 일치하는 원본 디스크 NT 서명을 대상 디스크에 제공합니다.

   NT 서명 복사 확인란을 선택합니다.

   다음 경고가 표시됩니다. *"하드 디스크에 운영 체제가 있는 경우에는 머신을 다시 시작하기 전에 머신에서 원본 또는 대상 하드 디스크 드라이브를 설치 제거하십시오. 제거하지 않으면 OS가 둘 중 첫 번째에서 시작되고, 두 번째 디스크의 OS는 부팅할 수 없게 됩니다."*

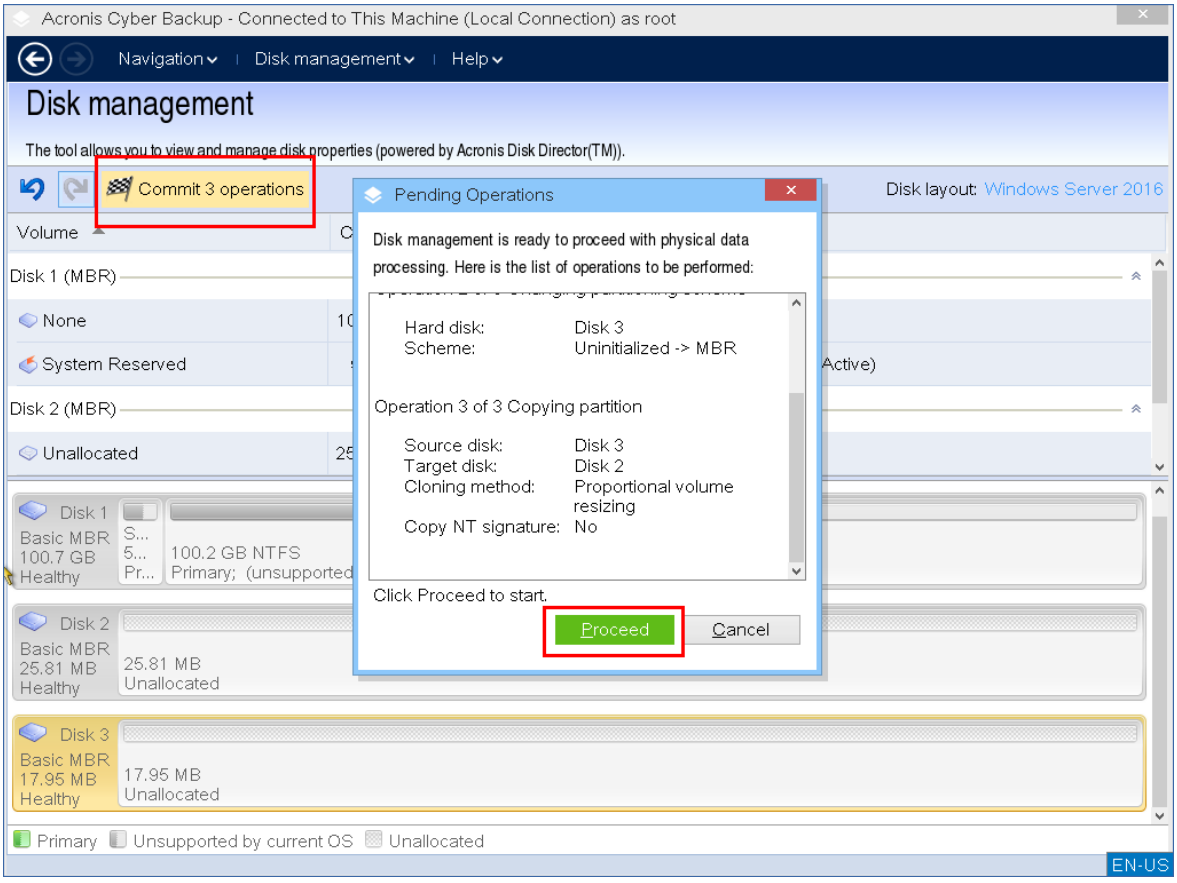
   작업 후에 머신 끄기 확인란이 선택되고 자동으로 비활성화됩니다.

b. **NT 서명 유지** – 이전 대상 디스크 서명을 유지하고 운영 체제를 서명에 따라 업데이트합니다.

   필요한 경우 **NT 서명 복사** 확인란을 클릭해 선택을 지웁니다.

   작업 후에 머신 끄기 확인란이 자동으로 해제됩니다.

7. 대기 작업을 추가하려면 **마침**을 클릭합니다.
8. **대기 작업창**에서 커밋을 클릭한 뒤, **진행**을 클릭합니다. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.



9. NT 서명 복사를 선택한 경우, 작업이 완료되고 컴퓨터가 꺼질 때까지 기다린 다음, 원본 디스크나 대상 하드 디스크 드라이브를 머신에서 연결 해제합니다.

디스크 변환: MBR에서 GPT로

다음과 같은 경우에 MBR 기본 디스크를 GPT 기본 디스크로 변환할 필요가 있습니다.

- 한 디스크에 주 볼륨이 4개 이상 필요한 경우.
- 가능한 모든 데이터 손상으로부터 디스크 안정성을 높여야 하는 경우.

중요
현재 실행 중인 운영 체제의 부트 볼륨을 포함한 기본 MBR 디스크는 GPT로 변환할 수 없습니다.

기본 MBR 디스크를 기본 GPT로 변환하는 방법

1. 복사할 디스크를 오른쪽 버튼으로 클릭한 뒤 **GPT로 변환**을 클릭합니다.
2. **확인**을 클릭하면 MBR을 GPT 디스크로 변환하는 대기 작업이 추가됩니다.
3. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

참고
GPT 파티셔닝된 디스크는 백업 영역에 필요한 파티셔닝된 영역 끝에 공간을 예약합니다. 여기에는 GPT 헤더와 파티션 테이블의 사본을 저장합니다. 디스크가 가득 차고 볼륨 크기를 자동으로 줄일 수 없는 경우에는 MBR 디스크를 GPT로 변환하는 작업이 실패합니다.
이 작업은 되돌릴 수 없습니다. MBR 디스크에 속하는 주 볼륨이 있고, 디스크를 처음에는 GPT로 변환한 후 다시 MBR로 변환하는 경우에는 볼륨은 논리가 되고 시스템 볼륨으로 사용할 수 없게 됩니다.

동적 디스크 변환: MBR에서 GPT로

부트 가능한 미디어는 동적 디스크의 경우 MBR에서 GPT로의 직접 변환은 지원하지 않습니다. 그러나 다음의 변환을 수행하면 목표를 달성할 수 있습니다.

1. MBR 디스크 변환: 동적에서 기본으로 변환하기 위해 **기본으로 변환** 작업 사용.
2. 기본 디스크 변환: **GPT로 변환** 작업을 사용하여 MBR에서 GPT로 변환.
3. GPT 디스크 변환: 기본에서 동적으로 변환하기 위해 **동적으로 변환** 작업 사용.

디스크 변환: GPT에서 MBR로 변환

GPT 디스크를 지원하지 않는 OS를 설치하려는 경우 GPT 디스크를 MBR로 변환할 수 있습니다.

중요
현재 실행 중인 운영 체제의 부트 볼륨을 포함한 기본 GPT 디스크는 MBR로 변환할 수 없습니다.

GPT 디스크를 MBR로 변환하는 방법

1. 복사할 디스크를 오른쪽 버튼으로 클릭한 뒤 **MBR로 변환**을 클릭합니다.
2. **확인**을 클릭하면 GPT를 MBR 디스크로 변환하는 대기 작업이 추가됩니다.
3. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

참고
작업 이후, 디스크의 볼륨은 논리 볼륨이 됩니다. 이 작업은 되돌릴 수 없습니다.

디스크 변환: 기본에서 동적으로

다음과 같은 경우에 기본 디스크를 동적으로 변환할 필요가 있습니다.

- 디스크를 동적 디스크 그룹의 일부로 사용할 계획인 경우
- 데이터 저장소를 위해 디스크 안정성을 높이고 싶은 경우

기본 디스크를 동적 디스크로 변환하는 방법

1. 변환할 디스크를 오른쪽 버튼으로 클릭한 뒤 **동적으로 변환**을 클릭합니다.
2. **확인**을 클릭합니다.

변환이 즉시 수행되고 필요한 경우 머신이 재시작됩니다.

참고
동적 디스크는 각 동적 볼륨에 대한 4가지 수준의 설명(볼륨-구성 요소-파티션-디스크)을 포함하여 데이터베이스를 저장하기 위해 실제 디스크의 마지막 메가바이트를 사용합니다. 동적 디스크로 변환하는 동안 기본 디스크가 가득 차게 되고 볼륨의 크기를 자동으로 줄일 수 없는 경우에는 작업이 실패합니다.
시스템 볼륨을 포함한 디스크 변환에는 어느 정도의 시간과 전력 손실이 있을 수 있으며 절차 중에 머신이 자동으로 꺼지거나 실수로 재설정 버튼을 누르면 부팅 기능을 잃게 될 수 있습니다.

Windows Disk Manager와 반대로 프로그램은 작업 후 디스크에서 **오프라인 운영 체제**의 부트 가능성을 보장합니다.

디스크 변환: 동적에서 기본으로

동적 디스크를 다시 기본 디스크로 변환하고 싶은 경우(예: 동적 디스크를 지원하지 않는 운영 체제를 이용하고 싶은 경우).

동적 디스크를 기본 디스크로 변환하는 방법

1. 변환할 디스크를 오른쪽 버튼으로 클릭한 뒤 **기본으로 변환**을 클릭합니다.
2. **확인**을 클릭합니다.

변환이 즉시 수행되고 필요한 경우 머신이 재시작됩니다.

참고
이 작업은 스팬, 스트라이프 또는 RAID-5 볼륨을 포함하는 동적 디스크에서 사용할 수 없습니다.

변환 후에는 나중에 기본 디스크에서 동적 디스크로 변환할 수 있도록 마지막 8Mb의 디스크 공간이 예약됩니다. 어떤 경우에는 할당되지 않은 공간과 제안된 최대 볼륨 크기가 다를 수 있습니다. 예를 들어, 한 미러의 크기가 다른 미러의 크기를 설정할 때나 마지막 8Mb의 디스크 공간이 나중에 기본에서 동적 디스크로 변환 시에 사용하기 위해 예약되어 있는 경우입니다.

참고
시스템 볼륨을 포함한 디스크 변환 시에는 어느 정도의 전력 손실이 있을 수 있으며, 절차 중에 머신을 무심코 끄거나 실수로 재설정 버튼을 누르면 부트 가능성이 손실될 수 있습니다.

Windows Disk Manager와는 반대로 이 프로그램은 다음을 보장합니다.

- 단순 및 미러 볼륨의 경우 **데이터가 있는** 볼륨이 있을 때 동적 디스크를 기본으로 안전하게 변환
- 다중 부트 시스템에서 작업 중에 **오프라인** 상태였던 시스템의 부트 가능성

볼륨 작업

부트 가능한 미디어로 다음의 작업을 볼륨에 실행할 수 있습니다.

- 볼륨 생성 - 새 볼륨을 생성합니다
- 볼륨 삭제 - 선택한 볼륨을 삭제합니다

- 활성으로 설정 - 머신이 여기에 설치된 OS로 부팅할 수 있도록 선택한 볼륨을 활성으로 설정합니다
- 문자 변경 - 선택한 볼륨 문자를 변경합니다
- 레이블 변경 - 선택한 볼륨 레이블을 변경합니다
- 볼륨 포맷 - 파일 시스템과 함께 볼륨을 포맷합니다

동적 볼륨 유형

단순 볼륨

단일 실제 디스크의 여유 공간에서 생성한 볼륨. 이는 디스크의 한 영역 또는 여러 영역으로 구성할 수 있으며 사실상 LDM(Logical Disk Manager)에 의해 통합됩니다. 이는 추가적인 안정성, 속도 향상 또는 별도의 크기를 제공하지는 않습니다.

스팬 볼륨

디스크 여유 공간에서 생성한 볼륨은 사실상 실제 여러 디스크에서 LDM에 의해 서로 링크되어 있습니다. 한 볼륨에 최대 32개의 디스크를 포함할 수 있으므로 하드웨어 크기 제한을 극복할 수 있습니다. 하지만 디스크가 하나만 고장나도 모든 데이터가 유실될 수 있습니다. 또한, 스팬 볼륨을 제거하려면 전체 볼륨을 파괴해야 합니다. 따라서 스팬 볼륨은 추가적인 안정성이나 더 나은 I/O 속도를 제공하지 않습니다.

스트립 볼륨

볼륨의 각 디스크에 작성된 동일 크기의 데이터 스트립으로 구성되고 RAID 0으로도 불리는 볼륨. 즉, 스트립 볼륨을 만들기 위해서는 둘 이상의 동적 디스크가 필요합니다. 스트립 볼륨의 디스크는 동일할 필요는 없지만 볼륨에 포함하고자 하는 각 디스크에는 사용하지 않은 공간이 있어야 합니다. 볼륨의 크기는 가장 작은 공간의 크기에 따라 다릅니다. 스트립 볼륨에서 데이터에 액세스하는 것은 단일 실제 디스크에서 동일 데이터에 액세스하는 것보다 빠릅니다. I/O는 둘 이상의 디스크에 걸쳐 있기 때문입니다.

스트립 볼륨은 안정성 향상이 아니라 성능 향상을 위해 생성된 것입니다. 중복 정보는 들어 있지 않습니다.

미러링된 볼륨

데이터가 두 개의 동일한 실제 디스크에 중복되어 있고 RAID 1이라고도 불리는 장애 허용 볼륨. 한 디스크에 있는 모든 데이터는 데이터 중복을 제공하기 위해 다른 디스크로 복사됩니다. 시스템 및 부트 볼륨을 포함하여 거의 대부분의 볼륨은 미러링할 수 있으며 디스크 중 하나가 고장나도 데이터를 나머지 디스크에서 액세스할 수 있습니다. 유감스럽게도 미러링된 볼륨을 사용할 때에 크기와 성능에 대한 하드웨어 제한 사항이 더욱 엄격합니다.

미러링된 스트립 볼륨

스트립 레이아웃의 높은 I/O 속도와 미러 유형의 중복 장점을 결합한 RAID 1+0이라고도 불리는 고장 방지 볼륨. 디스크 대비 볼륨 크기 비율이 낮은 단점은 미러 아키텍처에 내재되어 남아 있습니다.

RAID-5

데이터가 세 개 이상의 디스크 어레이에 스트라이프되는 고장 방지 볼륨입니다. 디스크는 동일할 필요는 없지만, 볼륨의 각 디스크에 동일한 크기의 할당되지 않은 공간 블럭이 있어야 합니다. 패리티(고장 시 데이터를 복원하는 데 사용할 수 있는 계산된 값)는 디스크 어레이에서도 스트라이프되며, 항상 데이터 자체와는 다른 디스크에 저장됩니다. 물리적 디스크가 고장나는 경우 고장 난 디스크에 있던 RAID-5 볼륨의 일부를 나머지 데이터와 패리티로부터 다시 만들 수 있습니다. RAID-5 볼륨은 안정성을 제공하며 미러링된 디스크 대 볼륨 크기 비율보다 높은 비율로 실제 디스크 크기 제한을 극복할 수 있습니다.

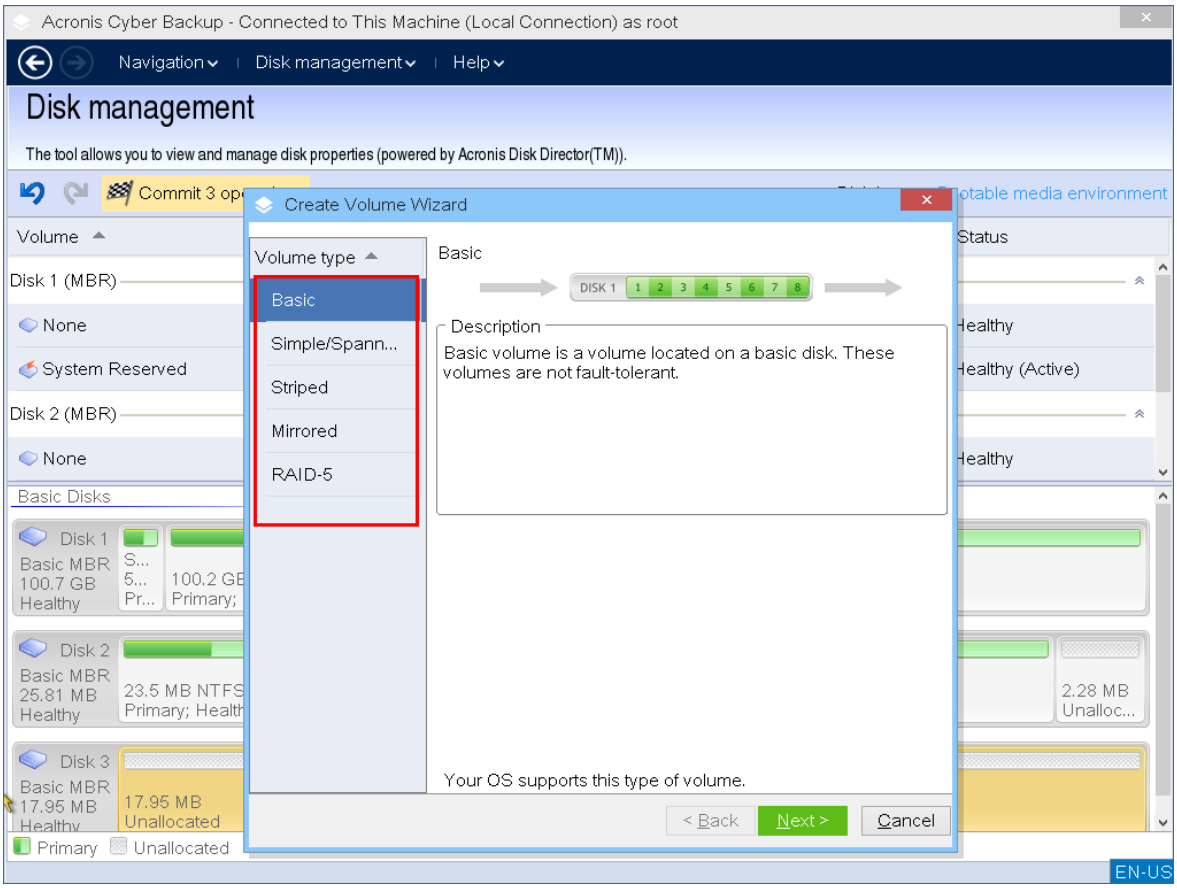
볼륨 생성

다음 작업을 위해 새 볼륨이 필요할 수도 있습니다.

- 이전에 저장한 백업 사본을 "예전 그대로" 구성으로 복구합니다
- 유사한 파일 모음을 별도로 저장합니다. 예를 들어, MP3 모음 또는 비디오 파일을 별도의 볼륨에 저장합니다.
- 다른 볼륨/디스크의 백업(이미지)을 특수 볼륨에 저장합니다
- 새 운영 체제(또는 스왑 파일)를 새 볼륨에 설치합니다
- 새 하드웨어를 머신에 추가합니다

볼륨 생성 방법

1. 디스크의 할당되지 않은 공간을 오른쪽 버튼으로 클릭한 다음, **볼륨 생성**을 클릭합니다. **볼륨 생성 마법사**가 열립니다.



2. 볼륨 유형을 선택합니다. 다음 옵션을 사용할 수 있습니다.
   - 기본
   - 단순/스팬
   - 스트라이프형
   - 미러형
   - RAID-5

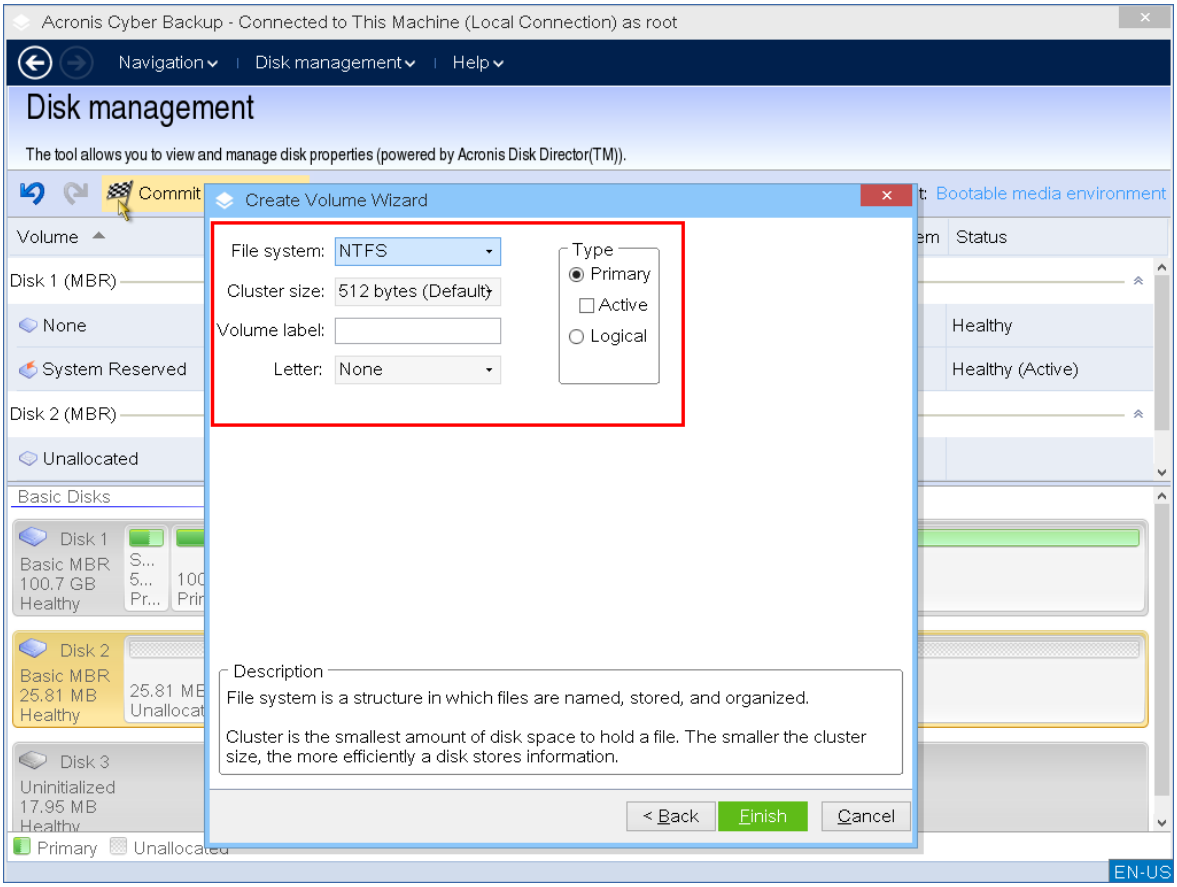
   현재 운영 체제가 선택한 볼륨 유형을 지원하지 않으면 경고가 나타나고 **다음** 버튼이 비활성화됩니다. 계속 진행하기 위해서는 다른 볼륨 유형을 선택해야 합니다.
3. 할당되지 않은 공간을 지정하거나 목적지 디스크를 선택합니다.
   - 기본 볼륨에 대해서는 선택된 디스크의 할당되지 않은 공간을 지정합니다.
   - 단순/스팬 볼륨의 경우, 하나 이상의 목적지 디스크를 선택합니다.
   - 미러 볼륨의 경우, 두 개의 목적지 디스크를 선택합니다.
   - 스트라이프 볼륨의 경우, 하나 이상의 목적지 디스크를 선택합니다.
   - RAID-5 볼륨의 경우, 두 개의 목적지 디스크를 선택합니다.

   동적 볼륨을 생성하고 하나 이상의 **기본** 디스크를 대상으로 선택하면 선택한 디스크가 동적으로 자동 변환된다는 경고를 받게 됩니다.
4. 볼륨 크기 설정으로 이동합니다.

   최대값은 일반적으로 할당되지 않은 최대 공간을 나타냅니다. 어떤 경우에는 최대값이 다를 수 있습니다. 예를 들어, 한 미러의 크기가 다른 미러의 크기를 설정할 때나 마지막 8Mb의 디스크 공간이 나중에 기본에서 동적 디스크로 변환 시에 사용하기 위해 예약되어 있는 경우입니다.

디스크의 할당되지 않은 공간이 볼륨보다 큰 경우, 디스크에서 새 기본 볼륨의 위치를 선택할 수 있습니다.

5. 볼륨 옵션 설정으로 이동합니다.



볼륨 **문자**(기본적으로 알파벳 중 첫 번째 사용가능 문자)를 할당하고 선택적으로 **레이블**(기본적으로 없음)을 할당할 수 있습니다. **파일 시스템**과 **클러스터 크기**도 지정해야 합니다.

가능한 파일 시스템 옵션은 다음과 같습니다.

- FAT16 (볼륨 크기가 2GB보다 크게 설정된 경우 비활성화됨)
- FAT32(볼륨 크기가 2TB보다 크게 설정된 경우 비활성화됨)
- NTFS
- 볼륨을 포맷하지 않은 채로 둡니다.

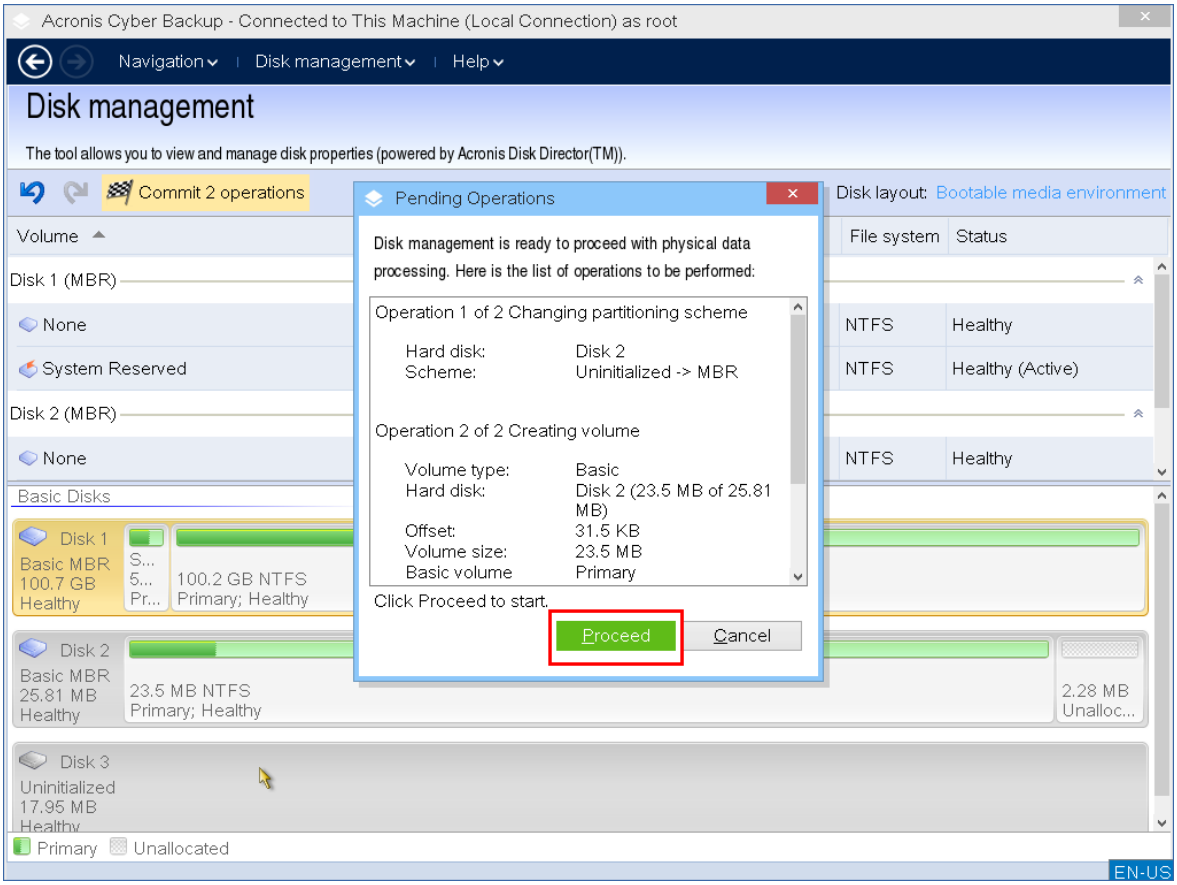
클러스터 크기를 설정할 때에는 각 파일 시스템에 대해 사전 정의된 양의 임의의 숫자 중에서 선택할 수 있습니다. 프로그램은 선택한 파일 시스템이 있는 볼륨에 가장 잘 맞는 클러스터 크기를 제안해줍니다. FAT16/FAT32에 64K 클러스터 크기를 설정하거나 NTFS에 8KB-64KB 클러스터 크기를 설정하면, Windows는 볼륨을 마운트할 수 있지만 몇몇 프로그램(예: 설치 프로그램)은 디스크 공간을 잘못 계산할 수도 있습니다.

시스템 볼륨으로 만들 수 있는 기본 볼륨을 생성하는 경우, **주 (활성 주 볼륨)** 또는 **논리 볼륨** 중 볼륨 유형을 선택할 수 있습니다. 일반적으로 운영 체제를 볼륨에 설치할 때 **주 볼륨**이 선택됩니다. 머신 시작 시에 부팅되도록 이 볼륨에 운영 체제를 설치하려면 **활성** (기본값) 값을 선택합니다. **기본** 버튼을 선택하지 않으면 **활성** 옵션이 비활성화됩니다. 볼륨의 용도가 데이터 저장인 경우에는 **논리**를 선택합니다.

참고

기본 디스크에는 최대 4개의 주 볼륨을 포함할 수 있습니다. 이미 있는 경우에는 디스크를 동적으로 변환해야 합니다. 그렇지 않으면 **활성** 및 **주** 옵션은 사용 불가능하게 되고 **논리** 볼륨 유형만 선택할 수 있습니다.

6. **대기 작업창**에서 커밋을 클릭한 뒤, **진행**을 클릭합니다. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.



볼륨 삭제

볼륨 삭제 방법

1. 삭제할 스토리지를 오른쪽 버튼으로 클릭합니다.
2. **볼륨 삭제**를 클릭합니다.

참고

이 볼륨에 있는 모든 정보는 손실되면 되돌릴 수 없습니다.

3. **확인**을 클릭하면 볼륨을 삭제하는 대기 작업이 추가됩니다.
4. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

볼륨을 삭제한 후에는 공간이 할당되지 않은 디스크 공간에 추가됩니다. 새 볼륨을 생성하거나 다른 볼륨의 유형을 변경하는 데 사용할 수 있습니다.

활성 볼륨 설정

여러 개의 기본 볼륨이 있는 경우에는 하나를 부트 볼륨으로 지정해야 합니다. 이를 위해서 볼륨을 활성으로 설정할 수 있습니다. 디스크마다 하나의 활성 볼륨만 생성될 수 있습니다.

볼륨을 활성으로 설정하는 방법

1. 기본 MBR에서 활성으로 설정할 주 볼륨을 오른쪽 버튼으로 클릭한 뒤 **활성으로 표시**를 클릭합니다.
   시스템에 다른 활성 볼륨이 없으면 보류 중인 활성 설정 작업이 추가됩니다. 시스템에 또 다른 활성 볼륨이 있으면 먼저 이전의 활성 볼륨을 수동으로 설정해야 한다는 경고를 받게 됩니다.

   참고
   새 활성 볼륨을 설정하게 되면 이전의 활성 볼륨 문자가 변경되고 설치된 프로그램의 일부가 실행을 중지할 수도 있음을 유의하십시오.

2. **확인**을 클릭하면 활성 볼륨을 설정하는 대기 작업이 추가됩니다.

   참고
   새 활성 볼륨에 운영 체제가 있더라도 머신이 여기에서 부팅하지 못하는 경우도 있습니다. 새 볼륨을 활성으로 설정하려면 결정을 확정해야 합니다.

3. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

볼륨 문자 변경

Windows 운영 체제는 시작 시 하드 디스크 볼륨에 문자(C:, D: 등)를 할당합니다. 이러한 문자는 애플리케이션과 운영 체제가 볼륨에서 파일 및 폴더를 찾는 데 사용됩니다. 추가 디스크를 연결하고, 볼륨을 생성하거나 기존 디스크에서 볼륨을 삭제하는 작업이 시스템 구성을 변경할 수도 있습니다. 그 결과 몇몇 응용 프로그램은 작동을 멈추거나 사용자 파일을 자동으로 찾거나 열지 못하게 될 수도 있습니다. 이를 막기 위해서 운영 체제가 볼륨에 자동으로 할당한 문자를 수동으로 변경할 수 있습니다.

운영 체제가 볼륨에 할당한 문자를 변경하는 방법

1. 원하는 볼륨을 마우스 오른쪽 버튼으로 클릭한 다음 **문자 변경**을 클릭합니다.
2. **문자 변경** 창에서 새 문자를 선택합니다.
3. **확인**을 클릭하면 볼륨 문자를 할당하는 대기 작업이 추가됩니다.
4. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

볼륨 레이블 변경

볼륨 레이블은 선택적 속성입니다. 이는 인식을 쉽게 하기 위해 볼륨에 할당되는 이름입니다.

볼륨 레이블 변경 방법

1. 원하는 볼륨을 마우스 오른쪽 버튼으로 클릭한 다음 **레이블 변경**을 클릭합니다.
2. **레이블 변경** 창 텍스트 필드에 새 레이블을 입력합니다.
3. **확인**을 클릭하면 볼륨 레이블을 변경하는 대기 작업이 추가됩니다.
4. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

볼륨 포맷

다음 목적을 위해 파일 시스템을 변경하려는 경우에는 볼륨을 포맷할 필요가 있습니다.

- FAT16 또는 FAT32 파일 시스템에서 클러스터 크기로 인해 손실된 추가 공간을 절약하는 방법
- 이 볼륨에 상주하는 데이터를 파괴하는 보다 빠르고 안정적인 방법으로서

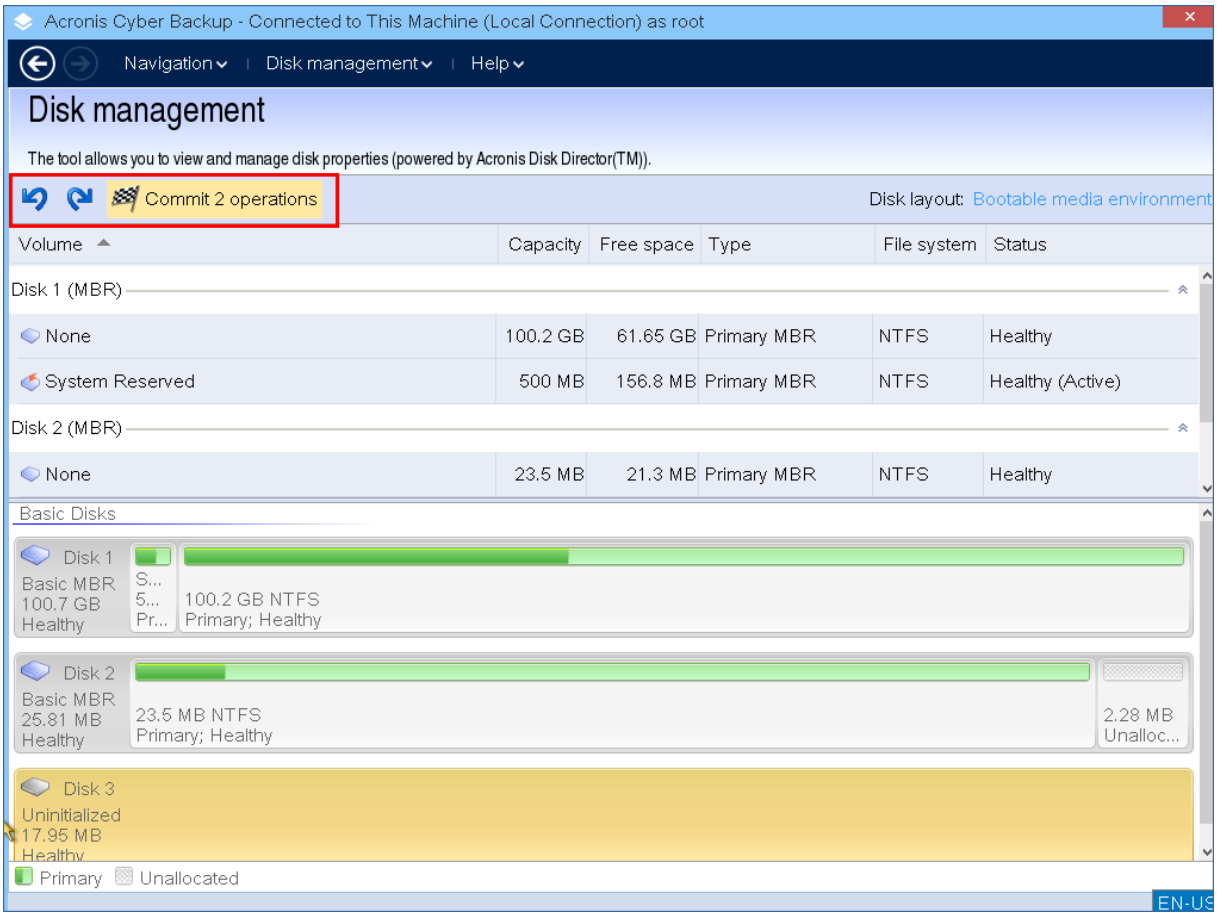
볼륨 삭제 방법

1. 원하는 볼륨을 마우스 오른쪽 버튼으로 클릭한 다음 **포맷**을 클릭합니다.
2. 클러스터 크기와 파일 시스템을 선택합니다. 가능한 파일 시스템 옵션은 다음과 같습니다.
   - FAT16 (볼륨 크기가 2GB보다 크게 설정된 경우 비활성화됨)
   - FAT32(볼륨 크기가 2TB보다 크게 설정된 경우 비활성화됨)
   - NTFS
3. **확인**을 클릭하면 볼륨을 포맷하는 대기 작업이 추가됩니다.
4. 추가 작업을 완료하려면 커밋하십시오. 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.

보류 중인 작업

모든 작업은 사용자가 **커밋** 명령을 내릴 때까지 대기합니다. 그러면 계획된 모든 작업을 제어하고, 원하는 변경 사항을 이중 확인하고, 필요한 경우 작업을 실행하기 전에 취소할 수 있습니다.

디스크 관리 보기에는 대기 작업의 **실행 취소**, **다시 실행** 및 **커밋** 아이콘이 있는 툴바가 있습니다. 이러한 작업은 **디스크 관리** 메뉴에서 실행할 수도 있습니다.



계획한 모든 작업은 보류 중인 작업 목록에 추가됩니다.

실행 취소 작업을 사용하면 목록에 있는 마지막 작업을 실행 취소할 수 있습니다. 이 목록이 비어 있지 않으면 이 조치를 사용 가능합니다.

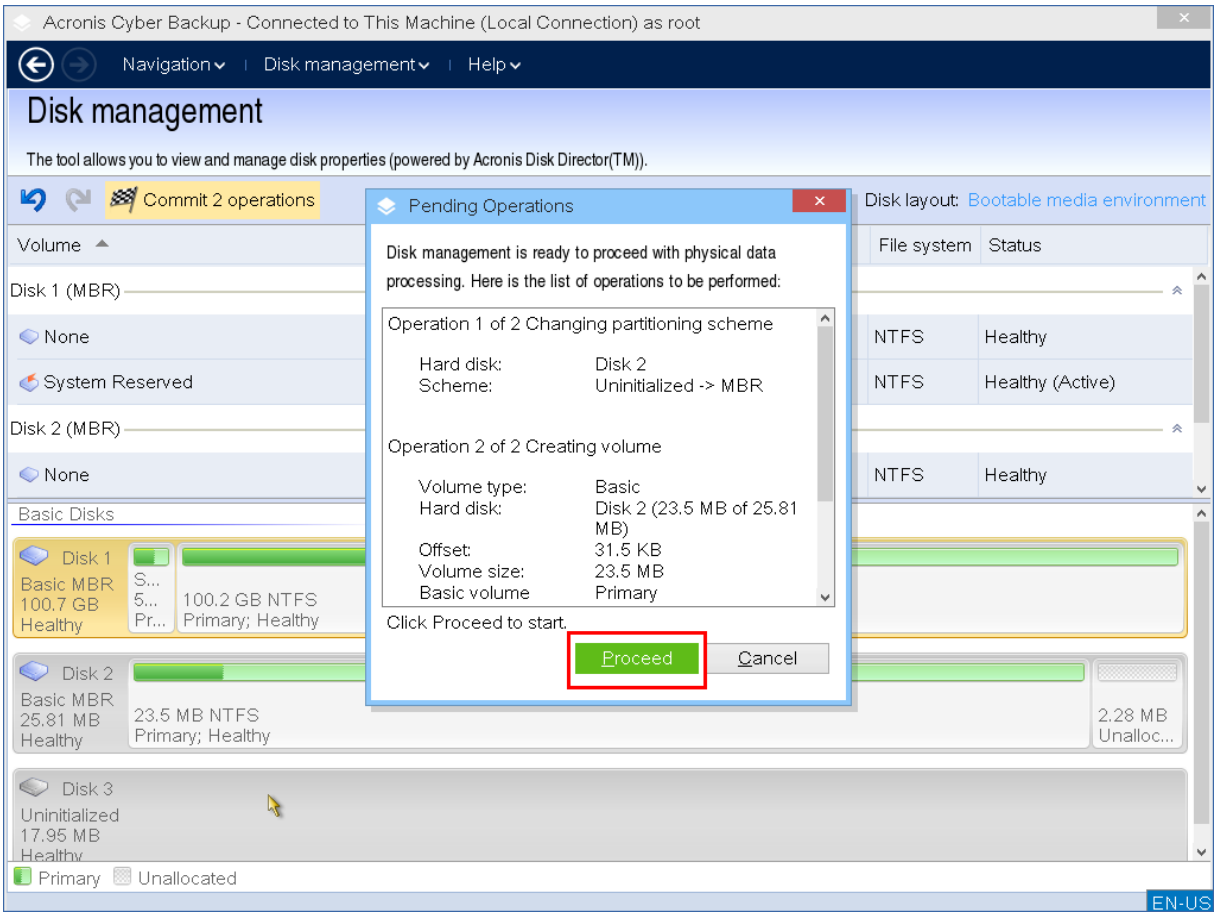
다시 실행 작업을 사용하면 실행 취소된 마지막 대기 작업을 원상태로 되돌릴 수 있습니다.

커밋하면 대기 중인 작업 목록을 볼 수 있는 **대기 작업** 창으로 이동합니다.

작업을 실행하려면 **진행**을 클릭합니다.

참고
진행 작업을 선택한 후에는 어떠한 조치나 작업도 실행 취소할 수 없습니다.

약정을 진행하지 않으려면 **취소**를 클릭합니다. 그러면 보류 중인 작업 목록에 아무런 변경이 수행되지 않습니다. 대기 작업을 확인하지 않고 프로그램을 종료하면 작업은 사실상 취소됩니다.



부트 가능한 미디어를 사용한 원격 작업

Cyber Protect 콘솔에서 부트 가능한 미디어를 확인하려면 먼저 "관리 서버에 미디어 등록"(352페이지)의 설명에 따라 해당 미디어를 등록해야 합니다.

Cyber Protect 콘솔에서 등록한 미디어는 **장치** > **부트 가능한 미디어**에 표시됩니다.

웹 인터페이스를 사용하면 미디어를 원격으로 관리할 수 있습니다. 예를 들어 데이터 복구, 미디어로 부팅한 머신 다시 시작/종료, 미디어 관련 정보/활동/경보 확인 등의 작업을 수행할 수 있습니다.

부트 가능한 미디어를 사용하여 원격으로 파일이나 폴더를 복구하려면

1. Cyber Protect 콘솔에서 **장치** > **부트 가능한 미디어**로 이동합니다.
1. 데이터 복구에 사용할 미디어를 선택합니다.
2. **복구**를 클릭합니다.
3. 위치를 선택하고 필요한 백업을 선택합니다. 백업은 위치별로 필터링됩니다.
4. 복구 지점을 선택한 다음 **파일/폴더 복구**를 클릭합니다.
5. 필요한 폴더를 찾거나 검색 창을 사용하여 필요한 파일 및 폴더 목록을 얻습니다.
   하나 이상의 와일드 카드 문자(* 및 ?)를 사용할 수 있습니다. 와일드카드 사용에 관한 자세한 내용은 "파일 필터"(253페이지) 항목을 참조하십시오.
6. 복구할 파일을 클릭하여 선택한 다음 **복구**를 클릭합니다.

7. **경로**에서 복구 목적지를 선택합니다.
8. [선택 사항] 고급 복구 구성을 설정하려면 **복구 옵션**을 클릭합니다. 자세한 내용은 "복구 옵션" (304페이지) 항목을 참조하십시오.
9. **복구 시작**을 클릭합니다.
10. 다음 파일 덮어쓰기 옵션 중 하나를 선택합니다.
    - **기존 파일 덮어쓰기**
    - **오래된 경우 기존 파일 덮어쓰기**
    - **기존 파일 덮어쓰기 안 함**

    머신을 자동으로 다시 시작할지 여부를 선택합니다.
11. 복구를 시작하려면 **진행**을 클릭합니다. 복구 진행률이 **작업** 탭에 표시됩니다.

부트 가능한 미디어를 사용하여 원격으로 디스크, 볼륨 또는 전체 머신을 복구하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **복구**를 클릭합니다.
3. 위치를 선택하고 필요한 백업을 선택합니다. 백업은 위치별로 필터링됩니다.
4. 복구 지점을 선택한 다음 **복구** > **전체 머신**을 클릭합니다.
   필요한 경우 "실제 머신 복구"(287페이지)의 설명에 따라 대상 머신 및 볼륨 매핑을 구성합니다.
5. 고급 복구 구성을 설정하려면 **복구 옵션**을 클릭합니다. 자세한 내용은 "복구 옵션"(304페이지) 항목을 참조하십시오.
6. **복구 시작**을 클릭합니다.
7. 백업된 버전으로 디스크를 덮어 쓰려는지 확인합니다. 머신을 자동으로 다시 시작할지 여부를 선택합니다.
8. 복구 진행률이 **작업** 탭에 표시됩니다.

부팅한 머신을 원격으로 다시 시작하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **재부팅**을 클릭합니다.
3. 미디어로 부팅한 머신을 다시 시작할 것임을 확인합니다.

부팅한 머신을 원격으로 종료하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **종료**를 클릭합니다.
3. 미디어로 부팅한 머신을 종료할 것임을 확인합니다.

부트 가능한 미디어 관련 정보를 확인하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **상세 정보**, **활동** 또는 **경보**를 클릭하여 해당 정보를 확인합니다.

부트 가능한 미디어를 원격으로 삭제하려면

1. **장치** 탭에서 **부트 가능한 미디어** 그룹으로 이동한 다음 데이터 복구에 사용할 미디어를 선택합니다.
2. **삭제**를 클릭하여 Cyber Protect 콘솔에서 부트 가능한 미디어를 삭제합니다.
3. 부트 가능한 미디어를 삭제할 것임을 확인합니다.

iSCSI 장치 구성

이 섹션에서는 부트 가능한 미디어에서 iSCSI(Internet Small Computer System Interface) 장치를 구성하는 방법을 설명합니다. 아래 단계를 수행한 후 부트 가능한 미디어로 부트된 머신에 로컬로 연결된 것처럼 이러한 장치를 사용할 수 있습니다.

iSCSI 대상 서버(또는 **대상 포털**)는 iSCSI 장치를 호스트하는 서버입니다. **iSCSI 대상**은 대상 서버의 컴퍼넌트입니다. 이 컴퍼넌트는 장치를 공유하고 장치 액세스가 허용된 iSCSI 초기자를 나열합니다. **iSCSI 초기자**는 머신의 컴퍼넌트입니다. 이 컴퍼넌트는 머신과 iSCSI 대상 간에 상호 작용하도록 해줍니다. 부트 가능한 미디어로 부트된 머신에서 iSCSI 장치 액세스를 구성할 경우 장치의 iSCSI 대상 포털 및 대상에 나열된 iSCSI 초기자 중 하나를 지정해야 합니다. 대상이 여러 장치를 공유하는 경우 모든 장치에 액세스할 수 있습니다.

Linux 기반 부트 가능한 미디어에서 iSCSI 장치를 추가하려면

1. **도구** > **iSCSI/NDAS 장치 구성**을 클릭합니다.
2. **호스트 추가**를 클릭합니다.
3. iSCSI 대상 포털의 IP 주소와 포트 및 장치에 액세스할 수 있는 iSCSI 초기자의 이름을 지정합니다.
4. 호스트를 인증해야 하는 경우 사용자 이름과 그에 대한 비밀번호를 지정합니다.
5. **확인**을 클릭합니다.
6. 목록에서 iSCSI 대상을 선택한 다음 **연결**을 클릭합니다.
7. CHAP 인증이 iSCSI 대상 설정에 활성화되어 있는 경우 iSCSI 대상에 액세스하기 위한 자격 증명을 입력하라는 메시지가 표시됩니다. iSCSI 대상 설정과 동일한 사용자 이름 및 대상 비밀번호를 지정합니다. **확인**을 클릭합니다.
8. **닫기**를 클릭하여 창을 닫습니다.

PE 기반 부트 가능한 미디어에서 iSCSI 장치를 추가하려면

1. **도구** > **iSCSI 설정 실행**을 클릭합니다.
2. **검색** 탭을 클릭합니다.
3. **대상 포털**에서 **추가**를 클릭하고 iSCSI 대상 포털의 IP 주소와 포트를 지정합니다. **확인**을 클릭합니다.
4. **일반** 탭을 클릭하고 **변경**을 클릭한 다음 장치에 액세스할 수 있는 iSCSI 초기자의 이름을 지정합니다.
5. **대상** 탭을 클릭하고 **새로 고침**을 클릭한 후 목록에서 iSCSI 대상을 선택하고 나서, **연결**을 클릭합니다. **확인**을 클릭하여 iSCSI 대상에 연결합니다.
6. CHAP 인증이 iSCSI 대상 설정에 활성화되어 있는 경우 **인증 실패** 오류가 표시됩니다. 이 경우 **연결**을 클릭하고, **고급**을 클릭하고, **CHAP 로그온 활성화** 확인란을 선택한 다음 iSCSI 대상 설정

과 동일한 사용자 이름 및 대상 비밀번호를 지정합니다. **확인**을 클릭하여 창을 닫고, **확인**을 클릭하여 iSCSI 대상에 연결합니다.

7. **확인**을 클릭하여 창을 닫습니다.

Startup Recovery Manager

Startup Recovery Manager은(는) 하드 드라이브에 있는 부트 가능한 컴포넌트입니다. Startup Recovery Manager을(를) 사용하면 별도의 부트 가능한 미디어를 사용하지 않고도 부트 가능한 복구 유틸리티를 시작할 수 있습니다.

Startup Recovery Manager는 특히 이동 중인 사용자에게 유용합니다. 장애가 발생하면 머신을 재부팅하고 **Acronis Startup Recovery Manager를 사용하려면 F11 키를 누르십시오.** 프롬프트가 나타나면 F11 키를 누릅니다. 프로그램이 시작되고 복구를 수행할 수 있습니다. GRUB 부트 로더가 설치되어 있는 머신에서는 재부팅 중에 F11 키를 누르는 대신 부트 메뉴에서 Startup Recovery Manager를 선택합니다.

이동 중에 Startup Recovery Manager를 사용하여 백업할 수도 있습니다.

Startup Recovery Manager는 먼저 활성화해야 사용 가능합니다. 그러므로 부팅 시에 표시되는 프롬프트인 **Acronis Startup Recovery Manager를 사용하려면 F11 키를 누르십시오.**를 활성화하거나, GRUB 부트 로더를 사용하는 경우에는 GRUB 메뉴에 **Startup Recovery Manager** 항목을 추가해야 합니다.

참고

암호화되지 않은 시스템 볼륨이 있는 머신에서 Startup Recovery Manager를 활성화하려면 100MB 이상의 여유 공간이 있어야 합니다. 머신을 다시 시작해야 하는 복구 작업의 경우 여유 공간 100MB가 추가로 필요합니다.

BitLocker로 암호화된 볼륨이 있으며 암호화되지 않은 다른 볼륨이 하나 이상 있는 머신에서 Startup Recovery Manager를 활성화할 수 있습니다. 암호화되지 않은 볼륨에는 500MB 이상의 여유 공간이 있어야 합니다. 머신을 다시 시작해야 하는 복구 작업의 경우 머신에 추가 여유 공간 500MB가 있어야 합니다.

중요

Startup Recovery Manager 활성화가 불가능한 경우에는 원클릭 복구 백업을 생성하는 백업 작업이 실패합니다.

GRUB 부트 로더를 사용하고 마스터 부트 레코드(MBR)에 설치되어 있지 않는 한, Startup Recovery Manager 활성화는 MBR을 자체 부트 코드로 덮어씁니다. 따라서 타사 부트 로더가 설치되어 있는 경우 해당 부트 로더를 재활성화해야 할 수도 있습니다.

Linux에서는 GRUB(예: LILO) 이외의 부트 로더를 사용하는 경우 Startup Recovery Manager을(를) 활성화하기 전에 MBR 대신 Linux 루트(또는 부트) 파티션 부트 레코드에 설치하는 것이 좋습니다. 그렇지 않은 경우에는 활성화 후에 부트 로더를 수동으로 재구성해야 합니다.

Startup Recovery Manager 활성화

Agent for Windows 또는 Agent for Linux를 실행 중인 머신에서는 Cyber Protect 웹 콘솔에서 Startup Recovery Manager를 활성화할 수 있습니다.

Cyber Protect 웹 콘솔에서 Startup Recovery Manager을(를) 활성화하는 방법

1. Startup Recovery Manager를 활성화할 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
3. **Startup Recovery Manager** 스위치를 활성화합니다.
4. 소프트웨어에서 Startup Recovery Manager를 활성화하는 동안 기다려 주십시오.

에이전트가 없는 머신에서 Startup Recovery Manager를 활성화하려면

1. 부트 가능한 미디어에서 머신을 부팅합니다.
2. **도구** > **활성화 Startup Recovery Manager**를 클릭합니다.
3. 소프트웨어에서 Startup Recovery Manager를 활성화하는 동안 기다려 주십시오.

Startup Recovery Manager 비활성화

Startup Recovery Manager를 비활성화하려면 활성화 절차를 반복하고 각 단계에서 활성화와 반대 작업을 선택합니다. 비활성화를 완료하면 부팅 시에 표시되는 프롬프트인 **Acronis Startup Recovery Manager를 사용하려면 F11 키를 누르십시오.** 또는 GRUB의 메뉴 항목이 비활성화됩니다.

Startup Recovery Manager가 활성화되지 않은 경우 부팅이 실패할 때 시스템을 복구하기 위해 다음 중 하나를 수행해야 합니다.

- 별도의 부트 가능한 미디어에서 머신을 부팅
- PXE Server 또는 Microsoft RIS(원격 설치 서비스)에서 네트워크 부팅 사용

Acronis PXE Server

Acronis PXE Server는 네트워크를 통해 머신을 Acronis 부트 가능한 컴퍼넌트로 부팅할 수 있습니다.

네트워크 부팅:

- 부팅해야 하는 시스템에 부트 가능한 미디어를 설치하기 위해 기술 담당자가 현장에 상주할 필요도 없습니다.
- 그룹 작업 중에는 실제 부트 가능한 미디어를 사용하는 것과 비교하여 여러 개의 머신을 부팅하기 위해 필요한 시간을 줄일 수 있습니다.

부트 가능한 컴퍼넌트는 Acronis Bootable Media Builder를 사용하여 Acronis PXE Server에 업로드됩니다. 부트 가능한 컴퍼넌트를 업로드하려면 Bootable Media Builder를 시작하고 "Linux 기반 부트 가능한 미디어"에 설명된 단계별 지침을 따릅니다.

Acronis PXE Server에서 여러 개의 머신을 부팅하는 것은 네트워크에 DHCP(Dynamic Host Control Protocol) 서버가 있는 경우에 가능합니다. 그런 다음에는 부팅된 머신의 네트워크 인터페이스는 자동으로 IP 주소를 확보합니다.

제한 사항:

Acronis PXE Server는 UEFI 부트 로더를 지원하지 않습니다.

Acronis PXE Server 설치

Acronis PXE Server를 설치하는 방법

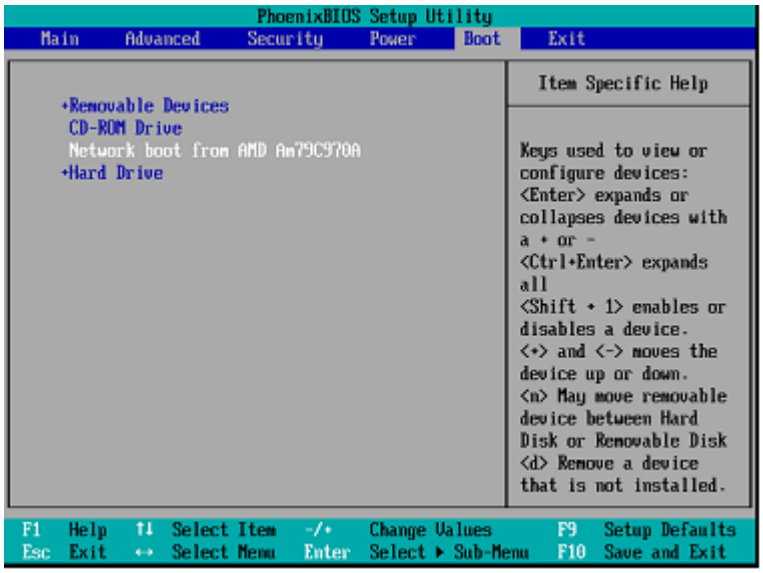
1. 관리자로 로그온하고 Acronis Cyber Protect 설정 프로그램을 시작합니다.
2. [선택 사항] 설치 프로그램의 언어를 변경하려면 **언어 설정**을 클릭합니다.
3. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
4. **설치 설정 사용자 정의**를 클릭합니다.
5. **설치할 항목** 옆에 있는 **변경**을 클릭합니다.
6. **PXE Server** 확인란을 선택합니다. 다른 컴퍼넌트를 이 머신에 설치하지 않으려면 해당하는 확인란의 선택을 해제합니다. **완료**를 클릭하여 계속 진행합니다.
7. [선택 사항] 기타 설치 설정을 변경합니다.
8. **설치**를 클릭하여 설치를 계속 진행합니다.
9. 설치가 완료되면 **닫기**를 클릭합니다.

Acronis PXE Server는 설치 후 즉시 서비스로 실행됩니다. 나중에 시스템이 다시 시작될 때마다 자동으로 시작됩니다. Acronis PXE Server를 다른 Windows 서비스와 같은 방법으로 중지 및 시작할 수 있습니다.

PXE에서 부팅하도록 머신 설정

베어 메탈의 경우 시스템의 BIOS가 네트워크 부팅만 지원하면 됩니다.

운영 체제가 하드 디스크에 있는 머신의 경우 네트워크 인터페이스 카드가 첫 번째 부트 장치이거나 적어도 하드 드라이브 장치보다 먼저 부팅되도록 BIOS를 구성해야 합니다. 아래 예제는 바람직한 BIOS 구성을 보여줍니다. 부트 가능 미디어를 삽입하지 않으면 머신이 네트워크에서 부팅됩니다.



일부 BIOS 버전의 경우 네트워크 인터페이스 카드를 활성화한 후 BIOS에 변경 내용을 저장하여 부트 장치 목록에 카드가 나타나도록 해야 합니다.

하드웨어에 여러 개의 네트워크 인터페이스 카드가 있는 경우 BIOS가 지원하는 카드에 네트워크 케이블이 연결되어 있어야 합니다.

서브넷에서 작업

Acronis PXE Server가 스위치를 통해 다른 서브넷에서 작동하도록 설정하려면 PXE 트래픽을 중계하도록 스위치를 구성합니다. PXE 서버 IP 주소는 DHCP 서버 주소와 같은 방식으로 IP 도우미 기능을 사용하여 인터페이스마다 구성됩니다. 자세한 내용은 다음 페이지를 참조하십시오. https://docs.microsoft.com/en-us/troubleshoot/mem/configmgr/boot-from-pxe-server.

모바일 장치 보호

백업 앱을 사용하면 모바일 데이터를 클라우드 스토리지에 백업한 다음 데이터 손실 또는 손상 발생 시 복구할 수 있습니다. 클라우드 스토리지로 백업하려면 계정 및 클라우드 가입이 필요합니다.

지원되는 모바일 장치

다음과 같은 운영 체제 중 하나를 실행하는 모바일 장치에 백업 앱을 설치할 수 있습니다.

- iOS 10.3 이상(iPhone, iPod, iPads)
- Android 5.0 이상

백업할 수 있는 항목

- 연락처
- 사진
- 비디오
- 일정표
- 미리 알림(iOS 장치만 해당)

알아야 할 사항

- 클라우드 스토리지에만 데이터를 백업할 수 있습니다.
- 앱을 열 때마다 데이터 변경 사항의 요약을 확인할 수 있으며 백업을 수동으로 시작할 수 있습니다.
- **지속 백업** 기능은 기본적으로 활성화됩니다. 이 설정이 활성화된 경우:
  - Android 7.0 이상에서는 백업 앱이 사용 중인 새 데이터를 자동으로 감지하고 이를 클라우드에 업로드합니다.
  - Android 5 및 6에서는 3시간마다 변경 사항을 확인합니다. 앱 설정에서 지속 백업 기능을 끌 수 있습니다.
- 앱 설정에서 기본적으로 **Wi-Fi만 사용** 옵션이 활성화되어 있습니다. 이 설정이 활성화되면, Wi-Fi 연결을 사용할 수 있는 경우에만 백업 앱이 데이터를 백업합니다. Wi-Fi 연결이 끊어지면 백업 프로세스가 시작되지 않습니다. 앱에서 셀룰러 연결도 사용할 수 있도록 하려면 이 옵션을 끕니다.
- 에너지를 절약하는 두 가지 방법이 있습니다.
  - **충전하는 동안 백업** 기능은 기본적으로 비활성화되어 있습니다. 이 설정이 활성화되면, 장치가 전원에 연결된 경우에만 백업 앱이 데이터를 백업합니다. 지속적인 백업 프로세스 동안 장치가 전원에서 분리되면 백업이 일시 중지됩니다.
  - **절전 모드**는 기본적으로 활성화되어 있습니다. 이 설정이 활성화되면, 장치의 배터리 잔량이 낮지 않은 경우에만 백업 앱이 데이터를 백업합니다. 장치의 배터리 잔량이 낮아지면 지속적인 백업이 일시 중지됩니다. 이 옵션은 Android 8 이상에서 사용할 수 있습니다.

- 해당 계정으로 등록한 모바일 장치에서 백업된 데이터에 액세스할 수 있습니다. 이를 통해 이전 모바일 장치에서 새로운 장치로 데이터를 전송할 수 있습니다. Android 장치의 연락처 및 사진을 iOS 장치로 복구하거나 이와 반대로 복구할 수 있습니다. 또한 Cyber Protect 웹 콘솔을 사용하여 사진, 비디오 또는 연락처를 모든 장치에 다운로드할 수도 있습니다.
- 본인 계정으로 등록한 모바일 장치에서 백업한 데이터는 이 계정으로만 사용할 수 있습니다. 다른 누구도 해당 데이터를 보거나 복구할 수 없습니다.
- 백업 앱에서 최신 데이터 버전만 복구할 수 있습니다. 특정 백업 버전에서 복구해야 하는 경우 태블릿 또는 컴퓨터에서 Cyber Protect 웹 콘솔을 사용합니다.
- [Android 장치만 해당] 백업하는 동안 SD 카드가 있는 경우 이 카드에 저장된 데이터도 백업됩니다. 복구하는 동안 SD 카드가 있는 경우 데이터가 이 SD 카드의 **백업에서 복구됨** 폴더에 복구되거나, 앱에서 데이터를 복구할 다른 위치를 묻습니다.

백업 앱 다운로드 방법

1. 모바일 장치에서 브라우저를 열고 https://backup.acronis.com/으로 이동합니다.
2. 사용자 계정으로 로그인합니다.
3. **모든 장치** > **추가**를 클릭합니다.
4. **모바일 장치**에서 장치 유형을 선택합니다.
   장치 유형에 따라 App Store 또는 Google Play Store로 이동하게 됩니다.
5. [iOS 장치만 해당] **가져오기**를 클릭합니다.
6. **설치**를 클릭하여 백업 앱을 설치합니다.

데이터 백업 시작 방법

1. 앱을 엽니다.
2. 사용자 계정으로 로그인합니다.

설정을 탭해서 첫 백업을 생성합니다.

1. 백업하려는 데이터 카테고리를 선택합니다. 기본적으로 모든 범주가 선택되어 있습니다.
2. [선택 단계] 백업을 암호화로 보호하려면 **백업 암호화**를 활성화합니다. 이 경우 다음 작업도 필요합니다.
   a. 암호화 비밀번호를 두 번 입력합니다.

      참고
      비밀번호를 잊어버리면 복구하거나 변경할 수 없으므로 비밀번호를 잘 기억해 두십시오.

   b. **암호화**를 탭합니다.
3. **백업**을 누릅니다.
4. 앱에서 개인용 데이터에 액세스하도록 허용합니다. 일부 데이터 카테고리에 대한 액세스를 거부하면 해당 데이터는 백업되지 않습니다.

백업이 시작됩니다.

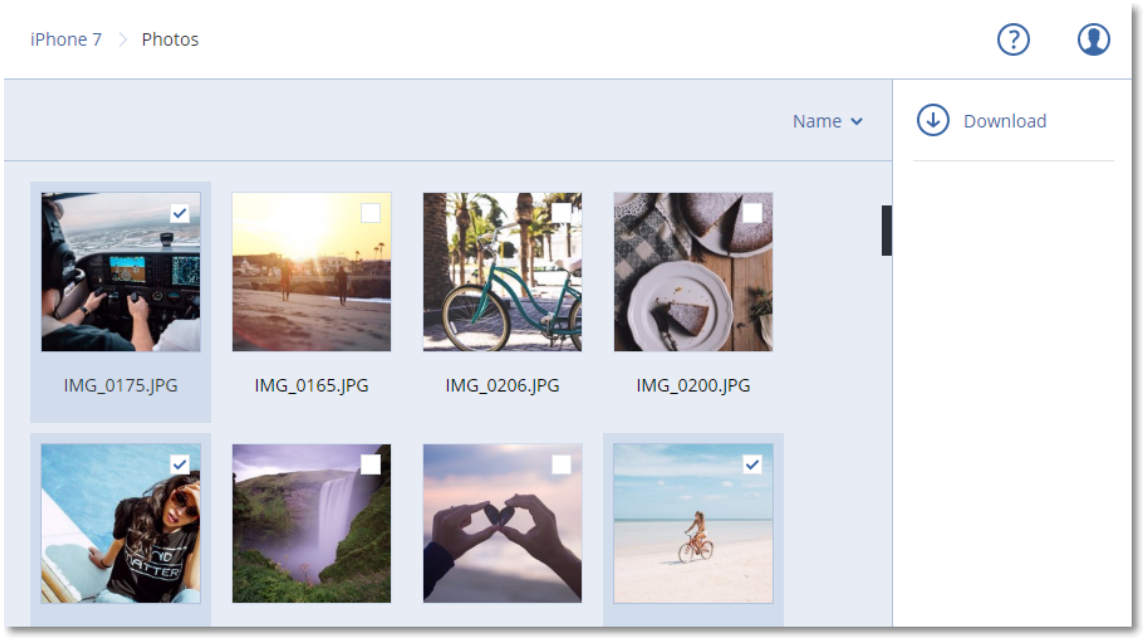
데이터를 모바일 장치로 복구하는 방법

1. 백업 앱을 엽니다.
2. **찾아보기**를 탭합니다.
3. 장치 이름을 누릅니다.
4. 다음 중 하나를 수행하십시오.
   - 백업한 데이터를 모두 복구하려면 **모두 복구**를 누릅니다. 추가 작업은 필요하지 않습니다.
   - 하나 이상의 데이터 카테고리를 복구하려면 **선택**을 누른 다음 필요한 데이터 카테고리의 확인란을 누릅니다. **복구**를 누릅니다. 추가 작업은 필요하지 않습니다.
   - 동일한 데이터 카테고리에 속한 하나 이상의 데이터 항목을 복구하려면 데이터 카테고리를 누릅니다. 추가 단계를 진행합니다.
5. 다음 중 하나를 수행하십시오.
   - 단일 데이터 항목을 복구하려면 해당 항목을 누릅니다.
   - 여러 데이터 항목을 복구하려면 **선택**을 누른 다음 필요한 데이터 항목의 확인란을 누릅니다.
6. **복구**를 누릅니다.

Cyber Protect 웹 콘솔을 통해 데이터를 검토하는 방법

1. 컴퓨터에서 브라우저를 열고 Cyber Protect 웹 콘솔 URL을 입력합니다.
2. 사용자 계정으로 로그인합니다.
3. **모든 장치**에서 모바일 장치 이름 아래의 **복구**를 클릭합니다.
4. 다음 중 하나를 수행하십시오.
   - 모든 사진, 비디오, 연락처, 달력 또는 미리 알림을 다운로드하려면 해당 데이터 카테고리를 선택합니다. **다운로드**를 클릭합니다.

- 개별 사진, 비디오, 연락처, 달력 또는 미리 알림을 다운로드하려면 해당 데이터 카테고리 이름을 클릭한 다음 필요한 데이터 항목의 확인란을 선택합니다. **다운로드**를 클릭합니다.



- 사진 또는 연락처를 미리 보려면 해당 데이터 카테고리 이름을 클릭한 다음 필요한 데이터 항목을 클릭합니다.

Microsoft 애플리케이션 보호

중요
이 섹션에 설명된 일부 기능은 온-프레미스 디플로이에만 제공됩니다.

Microsoft SQL Server 및 Microsoft Exchange Server 보호

이 애플리케이션을 보호하는 방법은 두 가지입니다.

- **데이터베이스 백업**
  이는 데이터베이스와 여기에 관련된 메타데이터의 파일 수준 백업을 말합니다. 데이터베이스는 라이브 애플리케이션으로 복구하거나 파일로 복구할 수 있습니다.
- **애플리케이션 인식 백업**
  이는 애플리케이션의 메타데이터도 수집하는 디스크 수준 백업을 말합니다. 이 메타데이터를 통해 전체 디스크 또는 볼륨을 복구하지 않고도 애플리케이션 데이터를 찾아 복구할 수 있습니다. 디스크나 볼륨을 전체적으로 복구할 수도 있습니다. 이는 단일 솔루션과 단일 보호 계획으로 재해 복구와 데이터 보호라는 두 가지 목적을 모두 충족할 수 있다는 의미입니다.

Microsoft Exchange Server의 경우 **사서함 백업**을 선택할 수 있습니다. 이는 Exchange 웹 서비스 프로토콜을 통해 수행된 개별 사서함의 백업입니다. 사서함 또는 사서함 항목은 라이브 Exchange Server 또는 Microsoft 365로 복구할 수 있습니다. 사서함 백업은 Microsoft Exchange Server 2010 SP1(서비스 팩 1) 이상에서 지원됩니다.

Microsoft SharePoint 보호

Microsoft SharePoint 팜은 SharePoint 서비스를 실행하는 프런트 엔드 서버, Microsoft SQL Server를 실행하는 데이터베이스 서버, 그리고 (선택적으로) 프런트 엔드 서버로부터 일부 SharePoint 서비스를 오프로드하는 애플리케이션 서버로 구성됩니다. 일부 프런트 엔드 서버 및 애플리케이션 서버는 서로 동일할 수도 있습니다.

전체 SharePoint 팜을 보호하려면

- 애플리케이션 인식 백업을 통해 모든 데이터베이스 서버를 백업합니다.
- 일반 디스크 수준 백업을 통해 고유한 프런트 엔드 서버 및 애플리케이션 서버를-모두 백업합니다.

모든 서버의 백업이 같은 스케줄에 완료되어야 합니다.

그 내용만 보호하려면 콘텐츠 데이터베이스를 따로 백업하면 됩니다.

도메인 컨트롤러 보호

Active Directory 도메인 서비스를 실행 중인 머신은 애플리케이션 인식 백업을 통해 보호할 수 있습니다. 도메인에 도메인 컨트롤러가 두 개 이상 포함되어 있고 이러한 도메인 컨트롤러 중 하나를 복구하는 경우 신뢰할 수 없는 복원이 수행되고 복구 후 USN 롤백이 발생하지 않습니다.

애플리케이션 복구

다음 표는 사용 가능한 애플리케이션 복구 방법을 요약해서 보여줍니다.

	데이터베이스 백업에서 복구	애플리케이션 인식 백업에서 복구	디스크 백업에서 복구
Microsoft SQL Server	데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로	전체 머신 데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로	전체 머신
Microsoft Exchange Server	데이터베이스를 라이브 Exchange로 데이터베이스를 파일로 라이브 Exchange 또는 Microsoft 365로 세부 복구*	전체 머신 데이터베이스를 라이브 Exchange로 데이터베이스를 파일로 라이브 Exchange 또는 Microsoft 365로 세부 복구*	전체 머신
Microsoft SharePoint 데이터베이스 서버	데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로 SharePoint 탐색기를 사용하여 개별 복구	전체 머신 데이터베이스를 라이브 SQL Server 인스턴스로 데이터베이스를 파일로 SharePoint 탐색기를 사용하여 개별 복구	전체 머신
Microsoft SharePoint 프런트엔드 웹 서버	-	-	전체 머신
Active Directory 도메인 서비스	-	전체 머신	-

* 개별 복구는 사서함 백업에서도 사용할 수 있습니다.

사전 요구 사항

애플리케이션 백업을 구성하기 전에 아래 나열된 요구 사항이 충족되었는지 확인하십시오.

VSS 작성자 상태를 확인하려면 `vssadmin list writers` 명령을 사용합니다.

공통 요구 사항

Microsoft SQL Server의 경우 다음을 확인합니다.

- 최소 하나의 Microsoft SQL Server 인스턴스를 시작했습니다.
- SQL VSS 작성자가 켜져 있습니다.

Microsoft Exchange Server의 경우 다음을 확인합니다.

- Microsoft Exchange 정보 저장소 서비스를 시작했습니다.
- Windows PowerShell이 설치되어 있습니다. Exchange 2010 이상에서는 Windows PowerShell 버전이 2.0 이상이어야 합니다.
- Microsoft .NET Framework가 설치되어 있습니다.
  Exchange 2007에서는 Microsoft .NET Framework 버전이 2.0 이상이어야 합니다.
  Exchange 2010 이상에서는 Microsoft .NET Framework 버전이 3.5 이상이어야 합니다.
- VSS용 Exchange 작성기가 켜집니다.

참고

Agent for Exchange를 작동하려면 임시 스토리지가 필요합니다. 임시 파일은 기본적으로 `%ProgramData%\Acronis\Temp`에 저장됩니다. `%ProgramData%` 폴더가 있는 볼륨에 적어도 Exchange 데이터베이스 크기의 15% 여유 공간이 있는지 확인하십시오. 또는 https://kb.acronis.com/content/40040.에 설명된 대로 Exchange 백업을 만들기 전에 임시 파일 위치를 변경할 수 있습니다.

도메인 컨트롤러에서 다음을 확인합니다.

- Active Directory VSS 작성자가 켜져 있습니다.

보호 계획을 생성할 때에는 다음을 확인합니다.

- 실제 머신에서 VSS(Volume Shadow Copy Service) 백업 옵션이 활성화되어 있습니다.
- 가상 머신에서 가상 머신용 VSS(Volume Shadow Copy Service) 백업 옵션이 활성화되어 있습니다.

애플리케이션 인식 백업을 위한 추가 요구 사항

보호 계획을 생성할 때 **전체 머신**을 백업하도록 선택되어 있는지 확인합니다. 보호 계획에서 **섹터 단위** 백업 옵션이 비활성화되어 있어야 합니다. 비활성화되지 않은 경우 해당 백업으로부터 애플리케이션 데이터를 복구하는 것이 불가능합니다. **섹터 단위** 모드로 자동 전환되어 백업 계획이 실행된 경우에도 애플리케이션 데이터는 복구할 수 없습니다.

ESXi 가상 머신의 시스템 요구사항

Agent for VMware를 통해 백업되는 가상 머신에서 애플리케이션을 실행 중인 경우 다음을 확인합니다.

- 백업 중인 가상 머신이 VMware 설명서의 "Windows 백업 구현" 문서에 나열된 애플리케이션의 일관성을 보장하는 백업 및 복구를 위한 요구 사항을 충족합니다.
  https://code.vmware.com/docs/1674/virtual-disk-programming-guide/doc/vddkBkupVadp.9.6.html
- VMware Tools가 머신에 설치되어 있고 최신 상태입니다.

- 머신에서 사용자 계정 컨트롤(UAC)이 사용하지 않도록 설정되어 있습니다. UAC를 사용하지 않도록 설정하지 않으려는 경우 애플리케이션 백업을 사용하도록 설정할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

Hyper-V 가상 머신의 시스템 요구사항

Agent for Hyper-V를 통해 백업되는 가상 머신에서 애플리케이션을 실행 중인 경우 다음을 확인합니다.

- 게스트 운영 체제는 Windows Server 2008 이상입니다.
- Hyper-V 2008 R2: 게스트 운영 체제는 Windows Server 2008/2008 R2/2012입니다.
- 가상 머신에 동적 디스크가 없습니다.
- Hyper-V 호스트와 게스트 운영 체제 사이에 네트워크 연결이 있습니다. 이는 가상 머신 내에서 원격 WMI 쿼리를 실행하는 데 필요합니다.
- 머신에서 사용자 계정 컨트롤(UAC)이 사용하지 않도록 설정되어 있습니다. UAC를 사용하지 않도록 설정하지 않으려는 경우 애플리케이션 백업을 사용하도록 설정할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.
- 가상 머신 구성이 다음 조건과 일치합니다.
  - Hyper-V 통합 서비스가 설치되어 있고 최신 상태입니다. 중대한 업데이트는 https://support.microsoft.com/en-us/help/3063109/hyper-v-integration-components-update-for-windows-virtual-machines입니다.
  - 가상 머신 설정에서 **관리** > **통합 서비스** > **백업(볼륨 체크포인트)** 옵션이 활성화되어 있습니다.
  - Hyper-V 2012 이상: 가상 머신에 체크포인트가 없습니다.
  - Hyper-V 2012 R2 이상: 가상 머신에 SCSI 컨트롤러가 있습니다(**설정** > **하드웨어** 확인).

데이터베이스 백업

데이터베이스를 백업하기 전에 "사전 요구 사항"에 나열되어 있는 요구 사항이 충족되었는지 확인하십시오.

아래 설명에 따라 데이터베이스를 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

SQL 데이터베이스 선택

SQL 데이터베이스 백업에는 데이터베이스 파일(.mdf, .ndf), 로그 파일(.ldf) 및 기타 관련 파일이 들어 있습니다. 이러한 파일은 SQL 기록기 서비스를 통해 백업합니다. 이 서비스는 VSS(Volume Shadow Copy Service)가 백업 또는 복구를 요청할 당시 실행 중이어야 합니다.

성공적인 각각의 백업 후 SQL 트랜잭션 로그 파일이 잘립니다. SQL 로그 자르기는 보호 계획 옵션에서 비활성화할 수 있습니다.

SQL 데이터베이스를 선택하려면

1. **장치** > **Microsoft SQL**을 클릭합니다.

   SQL Server AAG(Always On 가용성 그룹), Microsoft SQL Server를 실행하는 머신, SQL Server 인스턴스 및 데이터베이스의 트리가 표시됩니다.
2. 백업하려는 데이터로 이동합니다.

   트리 노드를 확장하거나 트리 오른쪽에 있는 목록에서 항목을 두 번 클릭합니다.
3. 백업하려는 데이터를 선택합니다. AAG, SQL Server를 실행하는 머신, SQL Server 인스턴스 또는 개별 데이터베이스를 선택할 수 있습니다.
   - AAG를 선택하면 선택한 AAG에 포함된 모든 데이터베이스가 백업됩니다. AAG 또는 개별 AAG 데이터베이스 백업에 대한 자세한 내용은 "AAG(Always On 가용성 그룹) 보호"를 참조하십시오.
   - SQL Server를 실행하는 머신을 선택하면 선택한 머신에서 실행되는 모든 SQL Server 인스턴스에 연결된 모든 데이터베이스가 백업됩니다.
   - SQL Server 인스턴스를 선택하면 선택한 인스턴스에 연결된 모든 데이터베이스가 백업됩니다.
   - 데이터베이스를 직접 선택하면 선택한 데이터베이스만 백업됩니다.
4. **보호**를 클릭합니다. 메시지가 표시되면 SQL Server 데이터에 액세스하기 위한 자격 증명을 입력합니다.

   Windows 인증을 사용하는 경우 해당 계정은 머신의 **Backup Operators** 또는 **Administrators** 그룹 구성원이자 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다.

   SQL Server 인증을 사용하는 경우 해당 계정은 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다.

Exchange Server 데이터 선택

다음 표는 백업하려고 선택할 수 있는 Microsoft Exchange Server 데이터와 이러한 데이터를 백업하는 데 필요한 최소 사용자 권한을 요약해서 보여줍니다.

Exchange 버전	데이터 항목	사용자 권한
2007	스토리지 그룹	**Exchange 조직 관리자** 역할 그룹의 구성원 자격
2010/2013/2016/2019	데이터베이스, DAG(데이터베이스 가용성 그룹)	**서버 관리** 역할 그룹의 구성원 자격.

전체 백업에는 선택한 Exchange Server 데이터가 모두 포함되어 있습니다.

증분 백업에는 해당하는 데이터베이스 체크포인트보다 최신인 데이터베이스 파일의 변경된 블록, 체크포인트 파일 및 소수의 로그 파일이 포함되어 있습니다. 백업에 데이터베이스 파일에 대한 변경 사항이 포함되므로 이전 백업 이후 모든 트랜잭션 로그 레코드를 백업할 필요가 없습니다. 복구 후 해당 체크포인트보다 최신인 로그만 재생해야 합니다. 따라서 복구 속도가 더 빠르고 순환 로깅이 활성화되어 있는 경우에도 성공적인 데이터베이스 백업을 보장합니다.

성공적인 각각의 백업 후 트랜잭션 로그 파일이 잘립니다.

Exchange Server 데이터를 선택하려면

1. **장치** > **Microsoft Exchange**를 클릭합니다.

   소프트웨어에 Exchange Server DAG(데이터베이스 가용성 그룹), Microsoft Exchange Server를 실행하는 머신, Exchange Server 데이터베이스의 트리가 표시됩니다. "사서함 백업"에 설명된 대로 Agent for Exchange를 구성하면 사서함 역시 이 트리에 표시됩니다.
2. 백업하려는 데이터로 이동합니다.

   트리 노드를 확장하거나 트리 오른쪽에 있는 목록에서 항목을 두 번 클릭합니다.
3. 백업하려는 데이터를 선택합니다.
   - DAG를 선택하면 각 클러스터 데이터베이스마다 사본이 하나씩 백업됩니다. DAG 백업에 대한 자세한 내용은 "DAG(데이터베이스 가용성 그룹) 보호"를 참조하십시오.
   - Microsoft Exchange Server를 실행하는 머신을 선택하면 선택한 머신에서 실행되는 Exchange Server에 마운트된 모든 데이터베이스가 백업됩니다.
   - 데이터베이스를 직접 선택하면 선택한 데이터베이스만 백업됩니다.
   - "사서함 백업"에 설명된 대로 Agent for Exchange를 구성한 경우 백업용 사서함을 선택할 수 있습니다.
4. 메시지가 표시되면 데이터에 액세스하기 위한 자격 증명을 입력합니다.
5. **보호**를 클릭합니다.

AAG(Always On 가용성 그룹) 보호

SQL Server 고가용성 솔루션 개요

WSFC(Windows Server 장애 조치 클러스터링) 기능을 사용하면 인스턴스 수준(장애 조치 클러스터 인스턴스, FCI) 또는 데이터베이스 수준(AlwaysOn 가용성 그룹, AAG)에서 이중화를 통해 고가용성 SQL Server를 구성할 수 있습니다. 두 방법 모두 결합시킬 수도 있습니다.

장애 조치 클러스터 인스턴스에서 SQL 데이터베이스는 공유 스토리지에 위치합니다. 이 스토리지는 활성 클러스터 노드에서만 액세스할 수 있습니다. 활성 노드에 장애가 생기면 장애 조치가 발생하고 다른 노드가 활성 노드가 됩니다.

가용성 그룹에서 각 데이터베이스 복제본은 다른 노드에 상주합니다. 주 복제본을 사용할 수 없게 되면 다른 노드에 있는 보조 복제본에 주 역할이 할당됩니다.

따라서 이미 클러스터 자체로 재해 복구 솔루션의 서비스를 제공하고 있습니다. 그러나 예를 들어 데이터베이스 논리 손상이 발생하거나 전체 클러스터가 가동 중단된 경우에는 클러스터가 데이터를 보호하지 못할 수 있습니다. 클러스터 솔루션이 유해한 내용 변경도 차단하지 못하는데, 그 이유는 변경 사항이 즉시 모든 클러스터 노드에 복제되기 때문입니다.

지원되는 클러스터 구성

이 백업 소프트웨어서는 SQL Server 2012 이상의 경우 AAG(Always On 가용성 그룹)*만* 지원합니다. 장애 조치 클러스터 인스턴스, 데이터베이스 미러링 및 로그 전달과 같은 기타 클러스터 구성은 지원되지 *않습니다*.

클러스터 데이터 백업 및 복구에 필요한 에이전트 수는?

클러스터 데이터의 성공적인 백업 및 복구를 위해서는 WSFC 클러스터의 각 노드에 Agent for SQL을 설치해야 합니다.

AAG에 포함된 데이터베이스 백업

1. WSFC 클러스터의 각 노드에 Agent for SQL을 설치합니다.

   참고
   노드 중 하나에서 에이전트를 설치한 후 **장치** > **Microsoft SQL** > **데이터베이스** 아래에 AAG 및 해당 노드가 표시됩니다. 나머지 노드에 Agent for SQL을 설치하려면 AAG를 선택하고, **상세정보**를 클릭하고 나서, 각 노드 옆에 있는 **에이전트 설치**를 클릭합니다.

2. "SQL 데이터베이스 선택"의 설명대로 백업할 AAG 또는 데이터베이스를 선택합니다.
   모든 AAG 데이터베이스를 백업할 AAG를 선택해야 합니다. 데이터베이스 세트를 백업하려면 이 데이터베이스 세트를 AAG의 모든 노드에 정의하십시오.

   경고!
   데이터베이스는 모든 노드에서 동일해야 합니다. 하나의 세트라도 다르거나 모든 노드에서 정의되지 않은 경우 클러스터 백업이 올바르게 작동하지 않습니다.

3. "클러스터 백업 모드" 백업 옵션을 구성합니다.

AAG에 포함된 데이터베이스 복구

1. 복구할 데이터베이스를 선택하고 데이터베이스를 복구할 복구 지점을 선택합니다.
   장치 > **Microsoft SQL** > **데이터베이스**에서 클러스터 데이터베이스를 선택하고 **복구**를 클릭하면 데이터베이스의 선택한 복사본이 백업된 시간에 해당하는 복구 지점만 표시됩니다.
   클러스터 데이터베이스의 모든 복구 지점을 보는 가장 쉬운 방법은 백업 스토리지 탭에서 전체 AAG의 백업을 선택하는 것입니다. AAG 백업의 이름은 <AAG 이름> - <보호 계획 이름> 템플릿에 따라 결정되고 특수 아이콘을 포함합니다.
2. 복구를 구성하려면 "SQL 데이터베이스 복구"에 설명된 단계를 5단계부터 따릅니다.
   데이터가 복구될 클러스터 노드가 자동으로 정의됩니다. 노드 이름은 **복구 대상** 필드에 표시됩니다. 대상 노드를 수동으로 변경할 수 있습니다.

   중요
   Always On 가용성 그룹에 포함된 데이터베이스는 복구 과정에서 덮어쓸 수 없습니다. Microsoft SQL Server가 이를 금지하기 때문입니다. 복구 전에 AAG에서 대상 데이터베이스를 제외해야 합니다. 또는 간단히 AAG가 아닌 새 데이터베이스로 데이터베이스를 복구하면 됩니다. 복구가 완료되면 원래 AAG 구성을 재구성할 수 있습니다.

DAG(데이터베이스 가용성 그룹) 보호

Exchange Server 클러스터 개요

Exchange 클러스터의 기본 개념은 신속한 장애 조치 및 데이터 손실 방지와 함께 높은 데이터베이스 가용성을 제공하는 것입니다. 보통 데이터베이스 또는 스토리지 그룹의 복사본을 한 개 이상 클러스터 구성 요소(클러스터 노드)에 보유하면 됩니다. 활성 데이터베이스 복사본을 호스팅하는 클러스터 노드 또는 활성 데이터베이스 복사본 자체가 실패하는 경우, 수동 복사본을 호스팅하는 나머지 노드가 실패한 노드의 작업을 자동으로 인계 받아서 최소한의 가동 중단으로 Exchange 서비스에 액세스를 지원합니다. 따라서 이미 클러스터 자체로 재해 복구 솔루션의 서비스를 제공하고 있습니다.

그러나 장애 조치 클러스터 솔루션이 데이터 보호 기능을 제공할 수 없는 경우가 있는데, 예를 들면 데이터베이스 논리 손상 또는 클러스터의 특정 데이터베이스에 복사본(복제본)이 없는 경우 또는 전체 클러스터가 가동 중단된 경우입니다. 클러스터 솔루션이 유해한 내용 변경도 차단하지 못하는데, 그 이유는 변경 사항이 즉시 모든 클러스터 노드에 복제되기 때문입니다.

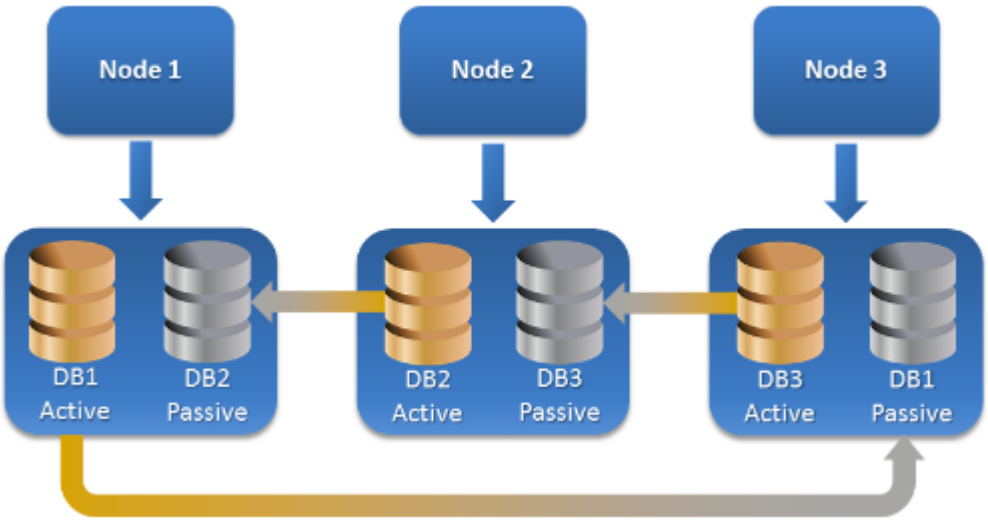
클러스터 인식 백업

클러스터 인식 백업을 사용하면 클러스터 데이터의 복사본 하나만 백업됩니다. 데이터 위치가 클러스터 내에서 변경되는 경우(예: 전환 또는 장애 조치로 인해) 소프트웨어는 이 데이터의 모든 변경 위치를 추적하여 안전하게 백업합니다.

지원되는 클러스터 구성

클러스터 인식 백업은 Exchange Server 2010 이상에서 DAG(Database Availability Group)에 *대해서만* 지원됩니다. SCC(단일 복사본 클러스터) 및 Exchange 2007용 CCR(클러스터 연속 복제)과 같은 기타 클러스터 구성은 지원되지 *않습니다*.

DAG는 최대 16대의 Exchange 사서함 서버로 구성되는 그룹입니다. 모든 노드가 다른 노드로부터 사서함 데이터베이스 복사본을 호스팅할 수 있습니다. 각 노드가 수동 및 활성 데이터베이스 복사본을 호스팅할 수 있습니다. 각 데이터베이스의 복사본을 16개까지 생성할 수 있습니다.



클러스터 인식 백업 및 복구에 필요한 에이전트 수는?

클러스터 데이터베이스의 성공적인 백업 및 복구를 위해서는 Exchange 클러스터의 각 노드에 Agent for Exchange를 설치해야 합니다

참고
노드 중 하나에 에이전트를 설치하고 나면 Cyber Protect 웹 콘솔의 **장치** > **Microsoft Exchange** > **데이터베이스** 아래에 DAG 및 해당 노드가 표시됩니다. 나머지 노드에 Agent for Exchange를 설치하려면 DAG를 선택하고, **상세정보**를 클릭하고 나서, 각 노드 옆에 있는 **에이전트 설치**를 클릭합니다.

Exchange 클러스터 데이터 백업

1. 보호 계획을 생성할 때에는 "Exchange Server 데이터 선택"의 설명대로 DAG를 선택합니다.
2. "클러스터 백업 모드" 백업 옵션을 구성합니다.
3. 보호 계획의 기타 설정을 적합하게 지정합니다.

중요
클러스터 인식 백업의 경우 DAG 자체를 선택하십시오. DAG 내부의 개별 노드 또는 데이터베이스를 선택하면 선택한 항목만 백업되고 **클러스터 백업 모드** 옵션이 무시됩니다.

Exchange 클러스터 데이터 복구

1. 복구할 데이터베이스의 복구 지점을 선택합니다. 전체 클러스터 복구는 선택할 수 없습니다.
   장치 > **Microsoft Exchange** > **데이터베이스** > <클러스터 이름> > <노드 이름 >에서 클러스터 데이터베이스 사본을 선택하고 **복구**를 클릭하면 이 사본이 백업된 시간에 해당하는 복구 지점만 표시됩니다.
   클러스터 데이터베이스의 모든 복구 지점을 보는 가장 쉬운 방법은 백업 스토리지 탭에서 백업을 선택하는 것입니다.
2. "Exchange 데이터베이스 복구"에 설명된 단계를 5단계부터 따릅니다.
   데이터가 복구될 클러스터 노드가 자동으로 정의됩니다. 노드 이름은 **복구 대상** 필드에 표시됩니다. 대상 노드를 수동으로 변경할 수 있습니다.

Aware 인식→인지

애플리케이션 인식 디스크 수준 백업은 실제 머신, ESXi 가상 머신 및 Hyper-V 가상 머신에 대해 사용할 수 있습니다.

Microsoft SQL Server, Microsoft Exchange Server 또는 Active Directory 도메인 서비스를 실행 중인 머신을 백업하는 경우 이러한 애플리케이션 데이터를 추가로 보호하려면 **애플리케이션 백업**을 사용하도록 설정합니다.

애플리케이션 인식 백업을 사용해야 하는 이유는 무엇입니까?

애플리케이션 인식 백업을 사용하면 다음과 같은 이점을 얻을 수 있습니다.

1. 애플리케이션이 일관된 상태에서 백업되므로 머신 복구 후 즉시 사용할 수 있습니다.
2. 전체 머신을 복구하지 않고 SQL 및 Exchange 데이터베이스, 사서함 및 사서함 항목을 복구할 수 있습니다.
3. 성공적인 각각의 백업 후 SQL 트랜잭션 로그 파일이 잘립니다. SQL 로그 자르기는 보호 계획 옵션에서 비활성화할 수 있습니다. Exchange 트랜잭션 로그는 가상 머신에서만 잘립니다. 실제 머신에서 Exchange 트랜잭션 로그를 자르려면 VSS 전체 백업 옵션을 사용하도록 설정하면 됩니다.
4. 도메인에 도메인 컨트롤러가 두 개 이상 포함되어 있고 이러한 도메인 컨트롤러 중 하나를 복구하는 경우 신뢰할 수 없는 복원이 수행되고 복구 후 USN 롤백이 발생하지 않습니다.

애플리케이션 인식 백업을 사용하려면 무엇이 필요합니까?

실제 머신에 Agent for SQL 및/또는 Agent for Exchange, 그리고 Agent for Windows가 설치되어 있어야 합니다.

가상 머신에서는 에이전트 설치가 필요 없습니다. 이 경우에는 머신이 Agent for VMware(Windows) 또는 Agent for Hyper-V에 의해 백업되는 것으로 간주됩니다.

참고
Windows Server 2022를 실행하는 Hyper-V 가상 머신의 경우 비에이전트 모드에서(Agent for Hyper-V가 백업을 수행할 때) 애플리케이션 인식 백업이 지원되지 않습니다. 이러한 머신에서 Microsoft 애플리케이션을 보호하려면 게스트 운영 체제 내에 Windows용 Agent를 설치하십시오.

Agent for VMware(가상 어플라이언스) 및 Agent for VMware(Linux)는 응용 프로그램 인식 백업을 생성할 수 있지만 여기에서 응용 프로그램 데이터를 복구할 수는 없습니다. 해당 에이전트를 통해 생성된 백업에서 응용 프로그램 데이터를 복구하려면 백업이 저장되어 있는 위치에 액세스할 수 있는 머신에 Agent for VMware(Windows), Agent for SQL 또는 Agent for Exchange가 있어야 합니다. 응용 프로그램 데이터 복구를 구성할 때에는 **백업 스토리지** 탭에서 복구 지점을 선택하고 **다음 위치에서 탐색할 머신**에서 이 머신을 선택합니다.

다른 요구 사항은 "사전 요구 사항"(406페이지) 및 "애플리케이션 인식 백업에 필요한 사용자 권한"(414페이지)에 나열되어 있습니다.

애플리케이션 인식 백업에 필요한 사용자 권한

애플리케이션 인식 백업에는 디스크에 있는 VSS 인식 애플리케이션의 메타데이터가 포함되어 있습니다. 이 메타데이터에 액세스하려면 아래 나열된 해당 권한이 있는 계정이 에이전트에 필요합

니다. 애플리케이션 백업을 사용하도록 설정하는 경우 이러한 계정을 지정하라는 메시지가 표시됩니다.

- SQL Server의 경우:
  Windows 인증을 사용하는 경우 해당 계정은 머신의 **Backup Operators** 또는 **Administrators** 그룹 구성원이자 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다. SQL Server 인증을 사용하는 경우 해당 계정은 백업하려는 각 인스턴스의 **sysadmin**역할 구성원이어야 합니다.
- Exchange Server의 경우:
  Exchange 2007: 계정이 머신의 **관리자** 그룹 및 **Exchange 조직 관리자** 역할 그룹의 구성원이어야 합니다.
  Exchange 2010 이상: 계정이 머신의 **관리자** 그룹 및 **조직 관리** 역할 그룹의 구성원이어야 합니다.
- Active Directory의 경우:
  계정이 도메인 관리자여야 합니다.

가상 머신의 추가 시스템 요구사항

애플리케이션이 Agent for VMware 또는 Agent for Hyper-V에 의해 백업되는 가상 머신에서 실행되는 경우 머신에서 사용자 계정 컨트롤(UAC)이 비활성화되어 있는지 확인하십시오. UAC를 사용하지 않도록 설정하지 않으려는 경우 애플리케이션 백업을 사용하도록 설정할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

Windows를 실행하는 머신에 대한 추가 요구 사항

모든 Windows 버전의 경우 애플리케이션 인식 백업을 허용하려면 사용자 계정 컨트롤(UAC) 정책을 비활성화해야 합니다. UAC 정책을 비활성화하지 않으려는 경우 애플리케이션 인식 백업을 구성할 때 기본 제공 도메인 관리자(DOMAIN\Administrator)의 자격 증명을 제공해야 합니다.

Windows에서 UAC 정책을 비활성화하려면

1. 레지스트리 편집기에서 다음 레지스트리 키를 찾습니다.
   `HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System`
2. **EnableLUA** 값을 **0**으로 변경합니다.
3. 머신을 다시 시작합니다.

사서함 백업

사서함 백업은 Microsoft Exchange Server 2010 SP1(서비스 팩 1) 이상에서 지원됩니다.

하나 이상의 Agent for Exchange가 관리 서버에 등록된 경우 사서함 백업을 사용할 수 있습니다. 에이전트는 Microsoft Exchange Server와 동일한 Active Directory 포리스트에 속한 머신에 설치되어야 합니다.

사서함을 백업하기 전에 Agent for Exchange를 Microsoft Exchange Server의 **클라이언트 액세스** 서버 역할(CAS)을 실행 중인 머신에 연결해야 합니다. Exchange 2016 이상에서 CAS 역할은 별도 설치

옵션으로 사용할 수 없습니다. 이는 사서함 서버 역할의 일부로 자동 설치됩니다. 따라서 에이전트를 **사서함 역할**을 실행하는 어느 서버로든 연결할 수 있습니다.

Agent for Exchange를 CAS에 연결하려면

1. **장치** > **추가**를 클릭합니다.
2. **Microsoft Exchange Server**를 클릭합니다.
3. **Exchange 사서함**을 클릭합니다.

   관리 서버에 등록된 Agent for Exchange가 없는 경우 에이전트를 설치할지 묻는 메시지가 표시됩니다. 설치 후에 이 절차를 1단계부터 반복합니다.
4. [선택 사항] 관리 서버에 여러 Agent for Exchange가 등록되어 있는 경우에는 **에이전트**를 클릭한 다음 백업을 수행할 에이전트를 변경합니다.
5. **클라이언트 액세스 서버**에서 Microsoft Exchange Server의 **클라이언트 액세스** 역할이 활성화된 머신의 FQDN(정규화된 도메인 이름)을 지정합니다.

   Exchange 2016 이상에서는 클라이언트 액세스 서비스가 사서함 서버 역할의 일부로 자동 설치됩니다. 따라서 **사서함 역할**을 실행하는 어느 서버든 지정할 수 있습니다. 이 섹션 뒷부분에서는 이 서버를 CAS로 언급합니다.
6. **인증 유형**에서 CAS에 사용되는 인증 유형을 선택합니다. **Kerberos**(기본값) 또는 **기본**을 선택할 수 있습니다.
7. [기본 인증만 해당] 사용할 프로토콜을 선택합니다. **HTTPS**(기본값) 또는 **HTTP**를 선택할 수 있습니다.
8. [HTTPS 프로토콜을 사용한 기본 인증만 해당] CAS가 인증 기관에서 얻은 SSL 인증서를 사용할 때 소프트웨어를 통해 CAS에 연결할 때 인증서를 확인하려는 경우 **SSL 인증서 확인** 확인란을 선택합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
9. 계정의 자격 증명이 제공되며 CAS에 액세스할 때 이 자격 증명을 사용합니다. 이 계정에 대한 요구사항이 "필수 사용자 권한"에 나열됩니다.
10. **추가**를 클릭합니다.

그러면 사서함이 **장치** > **Microsoft Exchange** > **사서함** 아래에 표시됩니다.

Exchange 서버 사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

MS Exchange 사서함을 선택하려면

1. **장치** > **Microsoft Exchange**를 클릭합니다.

   Exchange 데이터베이스 및 사서함의 트리가 표시됩니다.
2. **사서함**을 클릭하고 백업할 사서함을 선택합니다.
3. **백업**을 클릭합니다.

필수 사용자 권한

사서함에 액세스하려면 Agent for Exchange에 적절한 권한이 있는 계정이 있어야 합니다. 사서함을 사용하여 다양한 작업을 구성할 때 이 계정을 지정하라는 메시지가 나타납니다.

조직 관리 역할 그룹의 계정 구성원은 미래에 생성될 사서함을 포함하여 모든 사서함에 대한 액세스를 허용합니다.

필요한 최소 사용자 권한은 다음과 같습니다.

- 계정이 **서버 관리** 및 **수신자 관리** 역할 그룹의 구성원이어야 합니다.
- 에이전트가 액세스하는 사서함의 모든 사용자 또는 사용자 그룹에 대해 계정의 **ApplicationImpersonation** 관리 역할이 활성화되어 있어야 합니다.
  ApplicationImpersonation 관리 역할의 구성에 대한 자세한 내용은 다음 Microsoft 지식 기반 기사를 참조하십시오. https://msdn.microsoft.com/en-us/library/office/dn722376.aspx.

SQL 데이터베이스 복구

이 섹션에서는 데이터베이스 백업과 애플리케이션 인식 백업 모두에서 복구하는 방법에 대해 설명합니다.

Agent for SQL이 SQL 서버 인스턴스를 실행 중인 머신에 설치되어 있는 경우 SQL 데이터베이스를 SQL 서버 인스턴스로 복구할 수 있습니다.

Windows 인증을 사용하는 경우 머신의 **Backup Operators** 또는 **Administrators** 그룹 구성원이자 대상 인스턴스의 **sysadmin** 역할 구성원인 계정의 자격 증명을 입력해야 합니다. SQL Server 인증을 사용하는 경우에는 대상 인스턴스의 **sysadmin** 역할 구성원인 계정의 자격 증명을 입력해야 합니다.

또는 데이터베이스를 파일로 복구할 수 있습니다. 이 기능은 서드 파티 도구를 사용한 데이터 마이닝, 감사 또는 추가 처리를 위해 데이터를 추출해야 하는 경우 유용할 수 있습니다. "SQL Server 데이터베이스 연결"에서 설명하는 것처럼 SQL 데이터베이스 파일을 SQL 서버 인스턴스에 연결할 수 있습니다.

Agent for VMware(Windows)만 사용하는 경우에는 데이터베이스를 파일로 복구하는 것이 유일하게 사용 가능한 복구 방법입니다. Agent for VMware(가상 어플라이언스)를 이용한 데이터 복구는 불가능합니다.

시스템 데이터베이스는 기본적으로 사용자 데이터베이스와 같은 방식으로 복구됩니다. 시스템 데이터베이스 복구의 특성은 "시스템 데이터베이스 복구"에 설명되어 있습니다.

SQL 데이터베이스를 SQL Server 인스턴스로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft SQL**을 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.

- [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for SQL이 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
- 백업 스토리지 탭에서 복구 지점을 선택합니다.

위 작업 중 하나에서 찾기 위해 선택한 머신이 SQL 데이터베이스 복구의 대상 머신이 됩니다.

4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **SQL 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 인스턴스로**를 클릭합니다.
5. 기본적으로 데이터베이스는 원본 데이터베이스로 복구됩니다. 원본 데이터베이스가 없으면 재생성됩니다. 데이터베이스를 복구하려는 다른 SQL Server 인스턴스(동일한 머신에서 실행 중인 인스턴스)를 선택할 수 있습니다.

   데이터베이스를 동일한 인스턴스에 대해 다른 데이터베이스로 복구하려면:

   a. 데이터베이스 이름을 클릭합니다.
   b. **복구 대상**에서 **새 데이터베이스**를 선택합니다.
   c. 새 데이터베이스 이름을 지정합니다.
   d. 새 데이터베이스 경로 및 로그인 경로를 지정합니다. 지정한 폴더에는 원본 데이터베이스 및 로그 파일이 들어 있으면 안 됩니다.
6. [선택 사항] [원본 인스턴스로 복구된 데이터베이스를 새로운 데이터베이스로 사용할 수 없음] 복구 후 데이터베이스 상태를 변경하려면 데이터베이스 이름을 클릭한 후 다음 상태 중 하나를 선택합니다.
   - **사용 준비(복구를 통해 복원)**(기본값)

     복구가 완료되면 데이터베이스를 사용할 준비가 끝납니다. 사용자는 이 데이터베이스에 대한 전체 액세스 권한을 갖습니다. 소프트웨어는 트랜잭션 로그에 저장되어 있는 복구된 데이터베이스에서 커밋하지 않은 모든 트랜잭션을 롤백합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 없습니다.
   - **비실행(복구가 없는 복원)**

     복구가 완료되면 데이터베이스가 비실행 상태가 됩니다. 사용자는 여기에 액세스할 수 없습니다. 소프트웨어는 복구된 데이터베이스의 커밋하지 않은 모든 트랜잭션을 유지합니다. 네이티브 Microsoft SQL 백업에서 추가 트랜잭션 로그를 복구할 수 있으며, 따라서 필요한 복구 지점에 도달할 수 있습니다.
   - **읽기 전용(대기로 복원)**

     복구가 완료된 후 사용자는 데이터베이스에 읽기 전용으로 액세스할 수 있습니다. 소프트웨어는 커밋하지 않은 모든 트랜잭션을 실행 취소합니다. 그러나 임시 대기 파일에 실행 취소 동작을 저장하므로 복구 효과를 되돌릴 수 있습니다.

     이 값은 주로 SQL Server 오류가 발생한 시점을 찾기 위해 사용됩니다.
7. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

SQL 데이터베이스를 파일로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft SQL**을 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for SQL 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 SQL 데이터베이스 복구의 대상 머신이 됩니다.
4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **SQL 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **파일로 복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 파일로**를 클릭합니다.
5. **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택합니다.
6. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

시스템 데이터베이스 복구

인스턴스의 모든 시스템 데이터베이스는 한 번에 복구됩니다. 시스템 데이터베이스를 복구하는 경우 단일 사용자 모드에서 목적지 인스턴스가 자동으로 다시 시작됩니다. 복구가 완료된 후, 소프트웨어가 인스턴스를 다시 시작하고 다른 데이터베이스(있는 경우)를 복구합니다.

시스템 데이터베이스를 복구하는 경우 고려할 기타 사항:

- 시스템 데이터베이스는 원본 인스턴스와 동일한 버전의 인스턴스로만 복구할 수 있습니다.
- 시스템 데이터베이스는 항상 "사용 준비" 상태에서 복구됩니다.

마스터 데이터베이스 복구

시스템 데이터베이스에는 **마스터** 데이터베이스가 포함되어 있습니다. **마스터** 데이터베이스는 인스턴스의 모든 데이터베이스에 대한 정보를 기록합니다. 따라서 백업의 **마스터** 데이터베이스에는 백업 당시 인스턴스에 있었던 데이터베이스에 대한 정보가 포함되어 있습니다. **마스터** 데이터베이스를 복구한 후 다음 작업을 수행해야 할 수 있습니다.

- 백업이 완료된 후 인스턴스에 나타난 데이터베이스는 인스턴스별로 표시되지 않습니다. 이러한 데이터베이스를 프로덕션 모드로 전환하려면 SQL Server Management Studio를 사용하여 인스턴스에 수동으로 연결합니다.
- 백업 완료 후 삭제된 데이터베이스는 인스턴스에 오프라인으로 표시됩니다. SQL Server Management Studio를 사용하여 이러한 데이터베이스를 삭제합니다.

SQL Server 데이터베이스 연결

이 섹션에서는 SQL Server Management Studio를 사용하여 SQL Server에서 데이터베이스를 연결하는 방법에 대해 설명합니다. 한 번에 하나의 데이터베이스만 연결할 수 있습니다.

데이터베이스를 연결하려면 다음 권한이 필요합니다. **데이터베이스 생성**, **모든 데이터베이스 생성** 또는 **모든 데이터베이스 변경**. 일반적으로 이러한 권한은 인스턴스의 **sysadmin** 역할에 부여됩니다.

데이터베이스를 연결하려면

1. Microsoft SQL Server Management Studio를 실행합니다.
2. 필수 SQL Server 인스턴스에 연결한 다음 인스턴스를 확장합니다.
3. **데이터베이스**를 마우스 오른쪽 버튼으로 클릭하고 **연결**을 클릭합니다.
4. **추가**를 클릭합니다.
5. **데이터베이스 파일 찾기** 대화 상자에서 데이터베이스의 .mdf 파일을 찾아서 선택합니다.
6. **데이터베이스 세부정보** 섹션에서 나머지 데이터베이스 파일(.ndf 및 .ldf 파일)을 찾았는지 확인합니다.

   상세정보. 다음과 같은 경우 SQL Server 데이터베이스 파일을 자동으로 찾지 못할 수 있습니다.
   - 데이터베이스 파일이 기본 위치에 있지 않거나 기본 데이터베이스 파일(.mdf)과 동일한 폴더에 있지 않은 경우 해결 방법: **현재 파일 경로** 열에서 경로를 필수 파일로 수동으로 지정합니다.
   - 데이터베이스를 구성하는 불완전한 파일 세트를 복구한 경우 해결 방법: 백업에서 누락된 SQL Server 데이터베이스를 복구합니다.
7. 모든 파일을 찾으면 **확인**을 클릭합니다.

Exchange 데이터베이스 복구

이 섹션에서는 데이터베이스 백업과 애플리케이션 인식 백업 모두에서 복구하는 방법에 대해 설명합니다.

Exchange Server 데이터를 라이브 Exchange Server로 복구할 수 있습니다. 라이브 Exchange Server는 원래 Exchange Server일 수도 있고, FQDN(정규화된 도메인 이름)이 동일한 머신에서 실행 중인 동일한 버전의 Exchange Server일 수도 있습니다. Agent for Exchange가 대상 머신에 설치되어 있어야 합니다.

다음 표는 복구하려고 선택할 수 있는 Exchange Server 데이터와 이러한 데이터를 복구하는 데 필요한 최소 사용자 권한을 요약해서 보여줍니다.

Exchange 버전	데이터 항목	사용자 권한
2007	스토리지 그룹	**Exchange 조직 관리자** 역할 그룹의 구성원 자격.
2010/2013/2016/2019	데이터베이스	**서버 관리** 역할 그룹의 구성원 자격.

또는 데이터베이스(스토리지 그룹)를 파일로 복구할 수 있습니다. 트랜잭션 로그 파일과 함께 데이터베이스 파일은 백업에서 지정한 폴더로 추출됩니다. 감사 또는 서드 파티 도구로 추가 처리를 위해 데이터를 추출해야 하는 경우 또는 어떤 이유로든 복구에 실패하여 데이터베이스를 수동으로 마운트하는 방법을 찾고 있는 경우 이러한 기능이 유용할 수 있습니다.

Agent for VMware(Windows)만 사용하는 경우에는 데이터베이스를 파일로 복구하는 것이 유일하게 사용 가능한 복구 방법입니다. Agent for VMware(가상 어플라이언스)를 이용한 데이터 복구는 불가능합니다.

아래 절차 전체에서는 데이터베이스와 스토리지 그룹 둘 다를 "데이터베이스"라고 지칭할 것입니다.

Exchange 데이터베이스를 라이브 Exchange Server로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 Exchange 데이터 복구의 대상 머신이 됩니다.
4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **Exchange 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 Exchange Server로**를 클릭합니다.
5. 기본적으로 데이터베이스는 원본 데이터베이스로 복구됩니다. 원본 데이터베이스가 없으면 재생성됩니다.

   데이터베이스를 다른 데이터베이스로 복구하려면:
   a. 데이터베이스 이름을 클릭합니다.
   b. **복구 대상**에서 **새 데이터베이스**를 선택합니다.
   c. 새 데이터베이스 이름을 지정합니다.
   d. 새 데이터베이스 경로 및 로그인 경로를 지정합니다. 지정한 폴더에는 원본 데이터베이스 및 로그 파일이 들어 있으면 안 됩니다.
6. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

Exchange 데이터베이스를 파일로 복구하려면

1. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터베이스를 선택합니다.
2. **복구**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 중 하나를 수행하십시오.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 Exchange 데이터 복구의 대상 머신이 됩니다.
4. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **복구** > **Exchange 데이터베이스**를 클릭하고, 복구할 데이터베이스를 선택하고 나서, **파일로 복구**를 클릭합니다.
   - 데이터베이스 백업에서 복구할 경우 **복구** > **데이터베이스를 파일로**를 클릭합니다.
5. **찾아보기**를 클릭하고 파일을 저장할 로컬 또는 네트워크 폴더를 선택합니다.
6. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

Exchange Server 데이터베이스 마운트

데이터베이스 파일을 복구한 다음 마운팅하여 온라인으로 데이터베이스를 가져올 수 있습니다. 마운팅은 Exchange Management Console, Exchange System Manager 또는 Exchange Management Shell을 사용하여 수행됩니다.

복구된 데이터베이스는 부적절한 종료 상태가 됩니다. 부적절한 종료 상태에 있는 데이터베이스는 원래 위치로 복구되는 경우(즉, 원본 데이터베이스 정보가 Active Directory에 있는 경우) 시스템에서 마운팅할 수 있습니다. 다른 위치(예: 새 데이터베이스 또는 복구 데이터베이스)에 데이터베이스를 복구하는 경우에는 `Eseutil /r <Enn>` 명령을 사용하여 정상 종료 상태로 전환할 때까지 데이터베이스를 마운트할 수 없습니다. `<Enn>`은 트랜잭션 로그 파일을 적용해야 하는 데이터베이스(또는 데이터베이스를 포함하는 스토리지 그룹)에 대한 로그 파일 접두사를 지정합니다.

데이터베이스를 첨부하는 데 사용하는 계정은 대상 서버에 Exchange Server 관리자 역할 및 로컬 관리자 그룹으로 위임해야 합니다.

데이터베이스를 마운트하는 방법에 대한 자세한 사항은 다음 문서를 참고하십시오.

- Exchange 2010 이상: http://technet.microsoft.com/en-us/library/aa998871.aspx
- Exchange 2007: http://technet.microsoft.com/en-us/library/aa998871(v=EXCHG.80).aspx

Exchange 사서함 및 사서함 항목 복구

이 섹션에서는 데이터베이스 백업과 애플리케이션 인식 백업 및 사서함 백업에서 Exchange 사서함 및 사서함 항목을 복구하는 방법을 설명합니다. 사서함 또는 사서함 항목은 라이브 Exchange Server 또는 Microsoft 365로 복구할 수 있습니다.

다음 항목을 복구할 수 있습니다.

- 사서함(아카이브 사서함 제외)
- 공용 폴더

> **참고**
> 데이터베이스 백업에서만 사용 가능합니다. "Exchange Server 데이터 선택"(409페이지)을(를) 참조하십시오.

- 공용 폴더 항목
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

검색 기능을 사용해 항목을 찾을 수 있습니다.

Exchange Server로 복구

개별 복구는 Microsoft Exchange Server 2010 서비스 팩 1(SP1)이상에서 수행할 수 있습니다. 소스 백업은 지원되는 모든 Exchange 버전의 데이터베이스 또는 사서함을 포함할 수 있습니다.

개별 복구는 Agent for Exchange 또는 Agent for VMware(Windows)를 통해 수행할 수 있습니다. 대상 Exchange Server 및 에이전트를 실행하는 머신은 동일한 Active Directory 포리스트에 속해 있어야 합니다.

기존 사서함으로 사서함을 복구하면 일치하는 ID의 기존 항목이 덮어써집니다.

사서함 항목 복구 시에는 무엇도 덮어쓰지 않습니다. 대신, 사서함 항목의 전체 경로가 대상 폴더에 재생성됩니다.

사용자 계정에 대한 요구 사항

백업에서 복구하는 사서함은 Active Directory에 연결된 사용자 계정이 있어야 합니다.

사용자 사서함 및 그 내용은 연결된 사용자 계정이 *활성화됨* 상태인 경우에만 복구할 수 있습니다. 공유, 대화방 및 장비 사서함은 연결된 사용자 계정이 *비활성화됨* 상태인 경우에만 복구할 수 있습니다.

위의 조건을 충족하지 않는 사서함은 복구 중 건너뜁니다.

일부 사서함을 건너뛴 경우에는 경고가 표시되지만 복구는 성공합니다. 모든 사서함을 건너뛰면 복구가 실패합니다.

Microsoft 365로 복구

복구는 Microsoft Exchange Server 2010 이상의 백업에서 수행할 수 있습니다.

기존 Microsoft 365 사서함으로 사서함을 복구하면 기존 항목은 그대로 유지되고, 복구된 항목이 기존 항목 옆에 위치합니다.

단일 사서함을 복구할 때에는 대상 Microsoft 365 사서함을 선택해야 합니다. 하나의 복구 작업으로 여러 사서함을 복구할 때에는 사용자 이름이 같은 사용자의 사서함으로 각 사서함을 복구합니다. 사용자 이름이 같은 사용자가 없는 사서함은 건너뜁니다. 일부 사서함을 건너뛴 경우에는 경고가 표시되지만 복구는 성공합니다. 모든 사서함을 건너뛰면 복구가 실패합니다.

Microsoft 365로 복구에 대한 자세한 내용은 "Microsoft 365 사서함 보호"(430페이지) 항목을 참조하십시오.

사서함 복구

애플리케이션 인식 백업 또는 데이터베이스 백업에서 사서함을 복구하려면

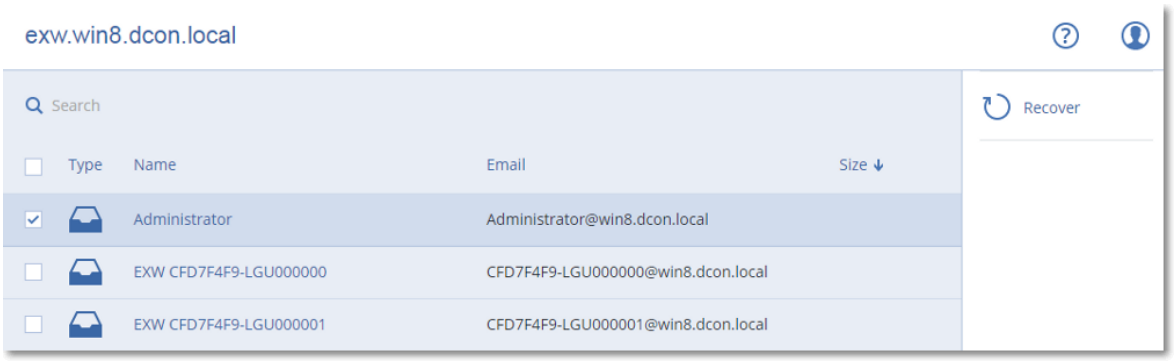
1. [데이터베이스 백업을 Microsoft 365로 복구하는 경우에만 해당] Agent for Office 365가 백업한 Exchange Server를 실행하는 머신에 설치되어 있지 않다면 다음 중 하나를 수행합니다.
   - 조직에 Agent for Office 365가 없는 경우 백업한 머신에 Agent for Office 365를 설치합니다(또는 같은 Microsoft Exchange Server 버전을 가진 다른 머신에 설치).
   - 조직에 Agent for Office 365가 이미 있는 경우에는 "Microsoft Exchange 라이브러리 복사"에 설명되어 있는 대로 백업한 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Office 365가 있는 머신으로 라이브러리를 복사합니다.
2. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터가 원래 포함된 데이터베이스를 선택합니다.
3. **복구**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 두 가지 방법으로 복구합니다.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 오프라인인 원래 머신 대신 복구를 수행합니다.

5. **복구** > **Exchange 사서함**을 클릭합니다.
6. 복구할 사서함을 선택합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.



7. **복구**를 클릭합니다.
8. [Microsoft 365로 복구하는 경우만 해당]:
   a. **복구 대상**에서 **Microsoft Office 365**를 선택합니다.
   b. [6단계에서 사서함 하나만 선택한 경우] **대상 사서함**에서 대상 사서함을 지정합니다.
   c. **복구 시작**을 클릭합니다.

   이 절차의 추가 단계는 필수 단계가 아닙니다.
9. 대상 머신을 선택하거나 변경하려면 **Microsoft Exchange Server가 포함된 대상 머신**을 클릭합니다. 이 단계를 통해 Agent for Exchange를 실행 중이지 않은 머신으로 복구할 수 있습니다.

   클라이언트 액세스 역할(Microsoft Exchange Server 2010/2013) 또는 **사서함 역할**(Microsoft Exchange Server 2016 이상)이 활성화되어 있는 머신의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 머신은 복구를 수행하는 머신과 같은 Active Directory 포리스트에 속해 있어야 합니다.

   메시지가 표시되면 시스템에 액세스하는 데 사용될 계정의 자격 증명을 제공합니다. 이 계정의 요구사항은 "필수 사용자 권한"(416페이지) 항목에 나와 있습니다.
10. [선택 사항] 자동으로 선택된 데이터베이스를 변경하려면 **누락된 사서함을 재생성할 데이터베이스**를 클릭합니다.
11. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

사서함 백업에서 사서함을 복구하려면

1. **장치** > **Microsoft Exchange** > **사서함**을 클릭합니다.
2. 복구할 사서함을 선택한 다음 **복구**를 클릭합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **복구** > **사서함**을 클릭합니다.
5. 위 절차의 8-11단계를 수행합니다.

사서함 항목 복구

애플리케이션 인식 백업 또는 데이터베이스 백업에서 사서함 항목을 복구하려면

1. [데이터베이스 백업을 Microsoft 365로 복구하는 경우에만 해당] Agent for Office 365가 백업한 Exchange Server를 실행하는 머신에 설치되어 있지 않다면 다음 중 하나를 수행합니다.
   - 조직에 Agent for Office 365가 없는 경우 백업한 머신에 Agent for Office 365를 설치합니다(또는 같은 Microsoft Exchange Server 버전을 가진 다른 머신에 설치).
   - 조직에 Agent for Office 365가 이미 있는 경우에는 "Microsoft Exchange 라이브러리 복사"에 설명되어 있는 대로 백업한 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Office 365가 있는 머신으로 라이브러리를 복사합니다.
2. 다음 중 하나를 수행하십시오.
   - 애플리케이션 인식 백업에서 복구할 경우 **장치** 아래에서 복구할 데이터가 원래 포함된 머신을 선택합니다.
   - 데이터베이스 백업에서 복구할 경우 **장치** > **Microsoft Exchange** > **데이터베이스**를 클릭하고 복구할 데이터가 원래 포함된 데이터베이스를 선택합니다.
3. **복구**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.

   머신이 오프라인 상태이면 복구 지점이 표시되지 않습니다. 다음 두 가지 방법으로 복구합니다.
   - [애플리케이션 인식 백업에서 복구할 경우만 해당] 백업 위치가 클라우드 또는 공유 스토리지인 경우(즉, 다른 에이전트가 여기에 액세스할 수 있는 경우) **머신 선택**을 클릭하고 Agent for Exchange 또는 Agent for VMware가 있는 온라인 머신을 선택한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.

   위 작업 중 하나에서 찾기 위해 선택한 머신이 오프라인인 원래 머신 대신 복구를 수행합니다.
5. **복구** > **Exchange 사서함**을 클릭합니다.
6. 복구하려는 항목이 원래 포함되어 있는 사서함을 클릭합니다.
7. 복구할 항목을 선택합니다.

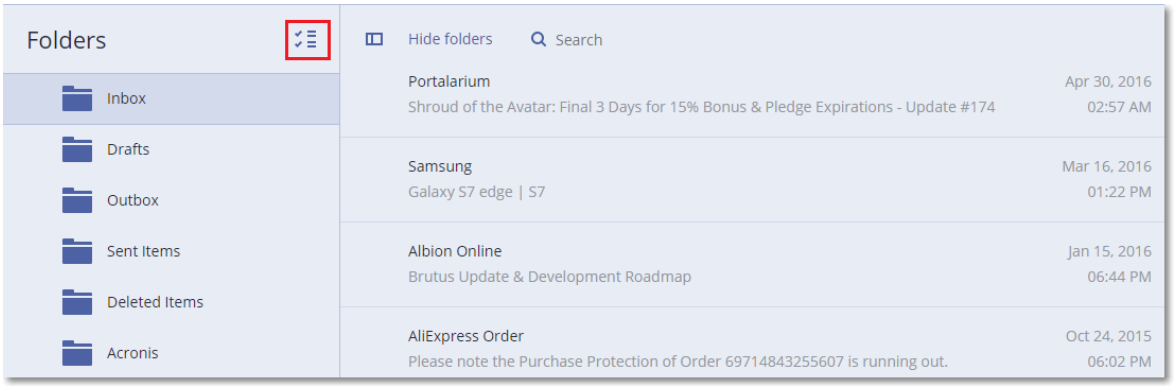
   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.
   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

   이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

   참고

   첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

   폴더를 선택하려면 폴더 복구 아이콘을 클릭하십시오.



8. **복구**를 클릭합니다.
9. Microsoft 365로 복구하려면 **복구 대상**에서 **Microsoft Office 365**를 선택합니다.

   Exchange Server를 복구하려면 **복구 대상**에서 기본값인 **Microsoft Exchange** 값을 유지합니다.
10. [Exchange Server로 복구하는 경우에만 해당] 대상 머신을 선택하거나 변경하려면 **Microsoft Exchange Server가 포함된 대상 머신**을 클릭합니다. 이 단계를 통해 Agent for Exchange를 실행 중이지 않은 머신으로 복구할 수 있습니다.

    클라이언트 액세스 역할(Microsoft Exchange Server 2010/2013) 또는 **사서함 역할**(Microsoft Exchange Server 2016 이상)이 활성화되어 있는 머신의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 머신은 복구를 수행하는 머신과 같은 Active Directory 포리스트에 속해 있어야 합니다.

    메시지가 표시되면 시스템에 액세스하는 데 사용될 계정의 자격 증명을 제공합니다. 이 계정의 요구사항은 "필수 사용자 권한"(416페이지) 항목에 나와 있습니다.
11. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.

    기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않거나 원래 대상 머신이 아닌 머신을 선택한 경우에는 대상 사서함을 지정해야 합니다.
12. [이메일 메시지를 복구할 경우만 해당] **대상 폴더**에서 대상 사서함의 대상 폴더를 보거나 변경합니다. 기본적으로 **복구 항목** 폴더가 선택되어 있습니다. Microsoft Exchange 제한으로 인해 이벤트, 작업, 메모 및 연락처는 다른 **대상 폴더** 지정하지 않은 원래 위치에 복원됩니다.
13. **복구 시작**을 클릭합니다.

복구 진행률이 **작업** 탭에 표시됩니다.

사서함 백업에서 사서함 항목을 복구하려면

1. **장치** > **Microsoft Exchange** > **사서함**을 클릭합니다.
2. 복구하려는 항목이 원래 포함되어 있는 사서함을 선택한 다음 **복구**를 클릭합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
3. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
4. **복구** > **이메일 메시지**를 클릭합니다.
5. 복구할 항목을 선택합니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.

   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.

- 작업: 제목 및 날짜로 검색합니다.
- 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

  이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

  참고
  첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

  이메일 메시지를 선택한 경우 **이메일로 보내기**를 클릭해 해당 메시지를 지정한 이메일 주소로 보낼 수 있습니다. 관리자 계정의 이메일 주소에서 메시지가 전송됩니다.

  폴더를 선택하려면 폴더 복구 아이콘  을 클릭하십시오.

6. **복구**를 클릭합니다.
7. 위 절차의 9-13단계를 수행합니다.

Microsoft Exchange Server 라이브러리 복사

Exchange 사서함 또는 사서함 항목을 Microsoft 365로 복구할 때는 백업된 머신에서(또는 같은 Microsoft Exchange Server 버전이 있는 다른 머신에서) Agent for Office 365가 있는 머신으로 다음 라이브러리를 복사해야 할 수 있습니다.

백업된 Microsoft Exchange Server 버전에 따라 다음 파일을 복사합니다.

Microsoft Exchange Server 버전	라이브러리	기본 위치
Microsoft Exchange Server 2010	ese.dll esebcli2.dll store.exe	%ProgramFiles%\Microsoft\Exchange Server\V14\bin
Microsoft Exchange Server 2013	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll	%WINDIR%\system32
Microsoft Exchange Server 2016, 2019	ese.dll	%ProgramFiles%\Microsoft\Exchange Server\V15\bin
	msvcr110.dll msvcp110.dll	%WINDIR%\system32

라이브러리는 **%ProgramData%\Acronis\ese** 폴더에 위치해야 합니다. 이 폴더가 존재하지 않는 경우 수동으로 생성하십시오.

SQL Server 또는 Exchange Server 액세스 자격 증명 변경

에이전트를 다시 설치하지 않고 SQL Server 또는 Exchange Server에 대한 액세스 자격 증명을 변경할 수 있습니다.

SQL Server 또는 Exchange Server 액세스 자격 증명을 변경하려면

1. **장치**를 클릭하고 **Microsoft SQL** 또는 **Microsoft Exchange**를 클릭합니다.
2. 액세스 자격 증명을 변경할 Always On 가용성 그룹, 데이터베이스 가용성 그룹, SQL Server 인스턴스 또는 Exchange Server를 선택합니다.
3. **자격 증명 지정**을 클릭합니다.
4. 새 액세스 자격 증명을 지정한 다음 **확인**을 클릭합니다.

사서함 백업을 위해 Exchange Server 액세스 자격 증명을 변경하려면

1. **장치** > **Microsoft Exchange**를 클릭한 다음, **사서함**을 확장합니다.
2. 액세스 자격 증명을 변경할 Exchange Server를 선택합니다.
3. **설정**을 클릭합니다.
4. **Exchange 관리자 계정**에서 새 액세스 자격 증명을 지정한 다음 **저장**을 클릭합니다.

Microsoft 365 사서함 보호

중요

이 섹션은 Acronis Cyber Protect의 온-프레미스 디플로이에 유효합니다. 클라우드 디플로이를 사용하는 경우에는 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-microsoft-365-data.html을 참조하십시오.

라이센싱 옵션에 대한 자세한 내용은 Microsoft 365용 Acronis Cyber Backup 라이센싱을 참조하십시오.

Microsoft 365 사서함을 백업하는 이유

Microsoft 365는 클라우드 서비스이지만 정기적으로 백업을 하면 사용자 오류 및 의도적인 악성 동작으로부터 한층 더 보호할 수 있습니다. Microsoft 365 보관 기간이 만료된 후에도 백업으로부터 삭제된 항목을 복구할 수 있습니다. 또한, 규정 준수를 위해 필요한 경우 Microsoft 365 사서함의 로컬 사본을 유지할 수 있습니다.

복구

다음과 같은 항목을 사서함 백업에서 복구할 수 있습니다.

- 사서함
- 이메일 폴더
- 이메일 메시지
- 달력 이벤트
- 작업
- 연락처
- 업무 일지
- 메모

검색 기능을 사용해 항목을 찾을 수 있습니다.

복구는 Microsoft 365 또는 라이브 Exchange Server로 수행할 수 있습니다.

기존 Microsoft 365 사서함으로 사서함을 복구하면 일치하는 ID의 기존 항목이 덮어써집니다. 기존 Exchange Server 사서함으로 사서함을 복구하면 기존 항목이 그대로 유지됩니다. 복구된 항목은 기존 항목 옆에 위치합니다.

사서함 항목 복구 시에는 무엇도 덮어쓰지 않습니다. 대신, 사서함 항목의 전체 경로가 대상 폴더에 재생성됩니다.

제한 사항

- 보호 계획을 사서함 500개 이상에 적용하는 경우 백업 성능이 저하될 수도 있습니다. 대량의 사서함을 보호하려면, 다양한 시간에 실행되도록 여러 개의 보호 계획과 스케줄을 생성합니다.
- 아카이브 사서함(**내부 아카이브**)은 백업할 수 없습니다.
- 사서함 백업에는 사용자에게 보이는 폴더만 포함됩니다. **복구 가능 항목** 폴더 및 해당 하위 폴더(**삭제**, **버전**, **제거**, **감사**, **DiscoveryHold**, **일정 로깅**)는 사서함 백업에 포함되지 않습니다.
- 새 Microsoft 365 사서함으로의 복구는 불가능합니다. 먼저 수동으로 Microsoft 365 사용자를 생성한 다음 이 사용자 사서함으로 항목을 복구해야 합니다.
- 다른 Microsoft 365 조직으로의 복구는 지원되지 않습니다.
- Microsoft 365가 지원하는 일부 항목 유형 또는 속성이 Exchange Server에서는 지원되지 않을 수 있습니다. 해당 항목 유형 또는 속성은 Exchange Server로의 복구 도중 건너뜁니다.

Microsoft 365 조직 추가

Microsoft 조직을 추가하려면 애플리케이션 ID, 애플리케이션 암호, Microsoft 365 테넌트 ID를 알고 있어야 합니다. 이를 찾는 방법은 애플리케이션 ID와 애플리케이션 암호 가져오기를 참조하십시오.

Microsoft 365 조직을 추가하려면

1. 인터넷에 연결된 Windows 머신에 Agent for Office 365를 설치합니다. 한 조직에 하나의 Agent for Office 365만 있어야 합니다.
2. Cyber Protect 웹 콘솔에서 **Microsoft Office 365**를 클릭합니다.
3. 창이 열리면 애플리케이션 ID, 애플리케이션 암호, Microsoft 365 테넌트 ID를 입력합니다.
4. **로그인**을 클릭합니다.

따라서 조직의 데이터 항목은 Cyber Protect 웹 콘솔의 **Microsoft Office 365** 탭에 표시됩니다.

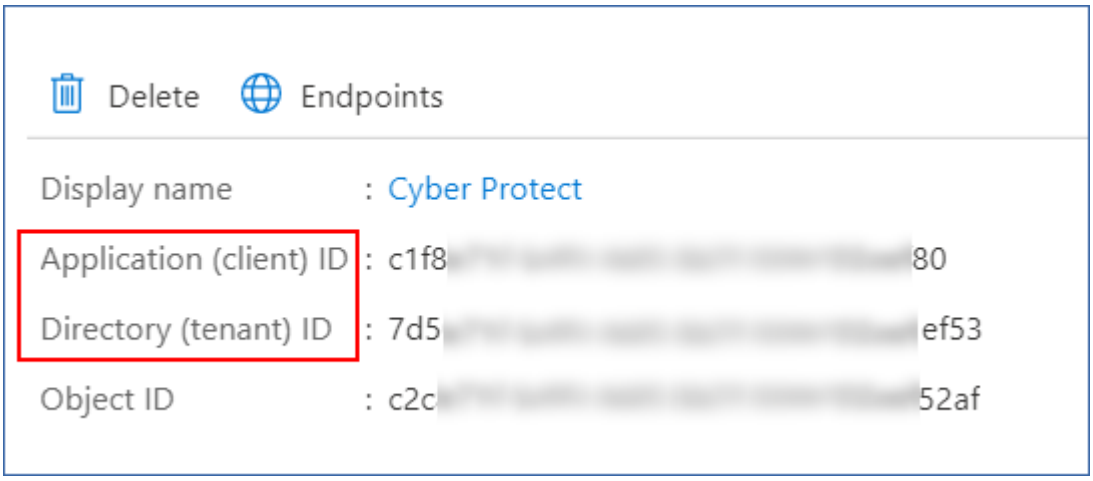
애플리케이션 ID 및 암호를 가져오는 방법

Microsoft 365에 대한 최신 인증을 사용하려면 Azure Active Directory에 사용자 지정 애플리케이션을 생성하고 특정 API 권한을 부여해야 합니다. 그러면 웹 콘솔에 입력해야 하는 **애플리케이션 ID**, **애플리케이션 암호** 및 **디렉토리(테넌트) ID**를 얻게 됩니다.

Azure Active Directory에 애플리케이션을 생성하는 방법

1. Azure portal에 관리자로 로그인합니다.
2. **Azure Active Directory** > **App 등록**으로 이동한 뒤, **새로운 등록**을 클릭합니다.
3. 사용자 지정 애플리케이션의 이름을 지정합니다(예: Cyber Protect).
4. **지원 계정 유형**에서 **이 조직 디렉토리 내 계정**을 선택합니다.
5. **등록**을 클릭합니다.

애플리케이션이 생성되었습니다. Azure portal에서 애플리케이션의 **Overview** 페이지로 이동하여 애플리케이션(클라이언트) ID 및 디렉토리(테넌트 ID)를 확인합니다.



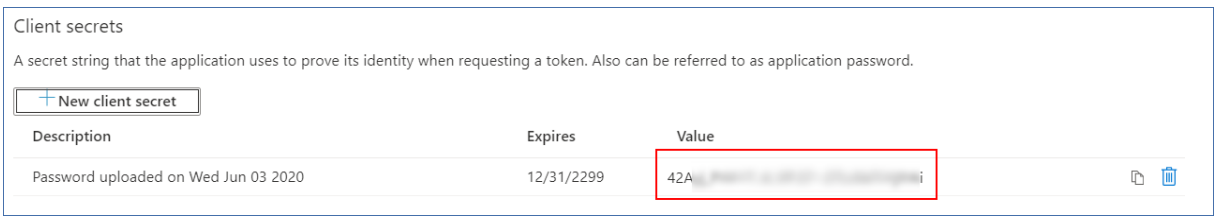
Azure portal에서 애플리케이션을 생성하는 방법에 대한 자세한 정보는 Microsoft 설명서를 참조합니다.

애플리케이션에 필요한 API 권한을 부여하는 방법

1. Azure portal에서 애플리케이션의 **API 권한**으로 이동한 뒤, **권한 추가**를 클릭합니다.
2. **조직에서 사용하는 API** 탭을 선택한 다음, **Office 365 Exchange Online**을 검색합니다.
3. **Office 365 Exchange Online**, **애플리케이션 권한**을 차례로 클릭합니다.
4. **App으로_전체_액세스** 확인란을 선택하고, **권한 추가**를 클릭하십시오.
5. **API 권한**에서 **권한 추가**를 클릭합니다.
6. **Microsoft Graph**를 선택합니다.
7. **애플리케이션 권한**을 선택합니다.
8. **디렉토리** 탭을 확장한 후 **디렉토리.모두.읽기** 확인란을 선택합니다. **권한 추가**를 클릭합니다.
9. 모든 권한을 확인한 뒤, **<사용자 애플리케이션 이름>에 대한 관리자 동의**를 클릭합니다.
10. **예**를 클릭하여 선택을 확인합니다.

애플리케이션 암호 생성 방법

1. Azure portal에서 사용자 애플리케이션의 **인증서&암호** > **새로운 클라이언트 암호**로 이동합니다.
2. 대화 상자가 열리면 만료 기한을 선택합니다. **해당 없음**을 선택한 뒤, **추가**를 클릭합니다.
3. **값** 필드에서 애플리케이션 암호를 확인하고 기억하십시오.



애플리케이션 암호에 대한 자세한 내용은 Microsoft 문서를 참고하십시오.

Microsoft 365 액세스 자격 증명 변경

에이전트를 다시 설치하지 않고 Microsoft 365에 대한 액세스 자격 증명을 변경할 수 있습니다.

Microsoft 365 액세스 자격 증명을 변경하려면

1. Cyber Protect 웹 콘솔에서 **장치** > **Microsoft Office 365**로 이동합니다.
2. Microsoft 365 조직을 선택합니다.
3. **자격 증명 지정**을 클릭합니다.
4. 애플리케이션 ID, 애플리케이션 암호, Microsoft 365 테넌트 ID를 입력합니다. 이를 찾는 방법은 애플리케이션 ID와 애플리케이션 암호 가져오기를 참조하십시오.
5. **로그인**을 클릭합니다.

사서함 선택

아래 설명에 따라 사서함을 선택한 다음, 보호 계획의 기타 설정을 적절하게 지정합니다.

사서함을 선택하려면

1. Cyber Protect 웹 콘솔에서 **장치** > **Microsoft Office 365**로 이동합니다.
2. 백업할 사서함을 선택합니다.
3. **백업**을 클릭합니다.

사서함 및 사서함 항목 복구

사서함 복구

1. [Exchange Server로 복구하는 경우에만 해당] 사서함을 복구 중인 사용자의 사용자 이름과 로그온 이름이 같은 Exchange 사용자가 있는지 확인합니다. 없으면 사용자를 생성합니다. 이 사용자에 대한 전체 요구 사항 목록은 "사용자 계정에 대한 요구 사항"(423페이지) 항목을 참조하십시오.
2. Cyber Protect 웹 콘솔에서 **장치** > **Microsoft Office 365**로 이동합니다.
3. 복구할 사서함을 선택한 다음 **복구**를 클릭합니다.
   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.
   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
5. **복구** > **사서함**을 클릭합니다.
6. Exchange Server로 복구하려면 **복구 대상**에서 **Microsoft Exchange**를 선택합니다. "사서함 복구"(424페이지) 항목의 설명대로 복구를 9단계부터 계속합니다. 이 절차의 추가 단계는 필수 단계가 아닙니다.
   Microsoft 365로 복구하려면 **복구 대상**에서 기본값인 **Microsoft Office 365** 값을 유지합니다.
7. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.
   기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않는 경우 대상 사서함을 지정해야 합니다.
8. **복구 시작**을 클릭합니다.

사서함 항목 복구

1. [Exchange Server로 복구하는 경우에만 해당] 사서함을 복구 중인 사용자의 사용자 이름과 로그온 이름이 같은 Exchange 사용자가 있는지 확인합니다. 없으면 사용자를 생성합니다. 이 사용자에 대한 전체 요구 사항 목록은 "사용자 계정에 대한 요구 사항"(423페이지) 항목을 참조하십시오.
2. Cyber Protect 웹 콘솔에서 **장치** > **Microsoft Office 365**로 이동합니다.
3. 복구하려는 항목이 원래 포함되어 있는 사서함을 선택한 다음 **복구**를 클릭합니다.

   사서함을 이름으로 검색할 수 있습니다. 와일드카드는 지원되지 않습니다.

   사서함이 삭제된 경우 백업 스토리지 탭에서 이를 선택한 다음 **백업 표시**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
5. **복구** > **이메일 메시지**를 클릭합니다.
6. 복구할 항목을 선택합니다.

   다음 검색 옵션을 사용할 수 있습니다. 와일드카드는 지원되지 않습니다.

   - 이메일 메시지: 제목, 보낸 사람, 받는 사람, 날짜로 검색합니다.
   - 이벤트: 제목 및 날짜로 검색합니다.
   - 작업: 제목 및 날짜로 검색합니다.
   - 연락처: 이름, 이메일 주소, 전화번호로 검색합니다.

   이메일 메시지를 선택한 경우 **내용 표시**를 클릭해 첨부 파일을 포함한 내용을 볼 수 있습니다.

   참고
   첨부 파일을 다운로드하려면 그 이름을 클릭하십시오.

   이메일 메시지를 선택한 경우 **이메일로 보내기**를 클릭해 해당 메시지를 지정한 이메일 주소로 보낼 수 있습니다. 관리자 계정의 이메일 주소에서 메시지가 전송됩니다.

   폴더를 선택하려면 "폴더 복구" 아이콘  을 클릭하십시오.
7. **복구**를 클릭합니다.
8. Exchange Server로 복구하려면 **복구 대상**에서 **Microsoft Exchange**를 선택합니다.

   Microsoft 365로 복구하려면 **복구 대상**에서 기본값인 **Microsoft Office 365** 값을 유지합니다.
9. [Exchange Server로 복구하는 경우에만 해당] 대상 머신을 선택하거나 변경하려면 **Microsoft Exchange Server가 포함된 대상 머신**을 클릭합니다. 이 단계를 통해 Agent for Exchange를 실행 중이지 않은 머신으로 복구할 수 있습니다.

   Microsoft Exchange Server의 **클라이언트 액세스** 역할이 활성화된 머신의 FQDN(정규화된 도메인 이름)을 지정합니다. 이 머신은 복구를 수행하는 머신과 같은 Active Directory 포리스트에 속해 있어야 합니다.

   메시지가 표시되면 시스템에 액세스하는 데 사용될 계정의 자격 증명을 제공합니다. 이 계정의 요구사항은 "필수 사용자 권한"(416페이지) 항목에 나와 있습니다.
10. **대상 사서함**에서 대상 사서함을 보고, 변경하거나 지정합니다.

    기본적으로 원래 사서함이 선택됩니다. 이 사서함이 존재하지 않는 경우 대상 사서함을 지정해야 합니다.

11. [이메일 메시지를 복구할 경우만 해당] **대상 폴더**에서 대상 사서함의 대상 폴더를 보거나 변경합니다. 기본적으로 **복구 항목** 폴더가 선택되어 있습니다.
12. **복구 시작**을 클릭합니다.

Google Workspace 데이터 보호

이 기능은 Acronis Cyber Protect의 클라우드 디플로이에만 제공됩니다. 이 기능에 대한 자세한 설명은 https://www.acronis.com/support/documentation/CyberProtectionService/#protecting-google-workspace-data.html을 참조하십시오.

Oracle 데이터베이스 보호

Oracle 데이터베이스 보호는 별도 문서(https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_OracleBackup_whitepaper.pdf)에 설명되어 있습니다.

가상 머신을 사용한 특수 작업

백업에서 가상 머신 실행(즉시 복원)

운영 체제가 포함된 디스크 수준 백업에서 가상 머신을 실행할 수 있습니다. 즉시 복구라고도 하는 이 작업을 통해 가상 서버를 스핀업할 수 있습니다. 가상 디스크가 백업에서 직접 열거되므로 데이터 저장소(스토리지)의 공간을 사용하지 않습니다. 스토리지 공간은 변경 사항을 가상 디스크에 보관하는 데에만 필요합니다.

이러한 임시 가상 머신은 최대 3일 동안 실행하는 것이 좋습니다. 그런 다음 완전히 제거하거나 가동 중지 없이 일반 가상 머신으로 변환(완료)할 수 있습니다.

임시 가상 머신이 존재하는 한 해당 머신에서 사용 중인 백업에는 보관 규칙을 적용할 수 없습니다. 원래 머신의 백업은 계속해서 실행할 수 있습니다.

사용 예제

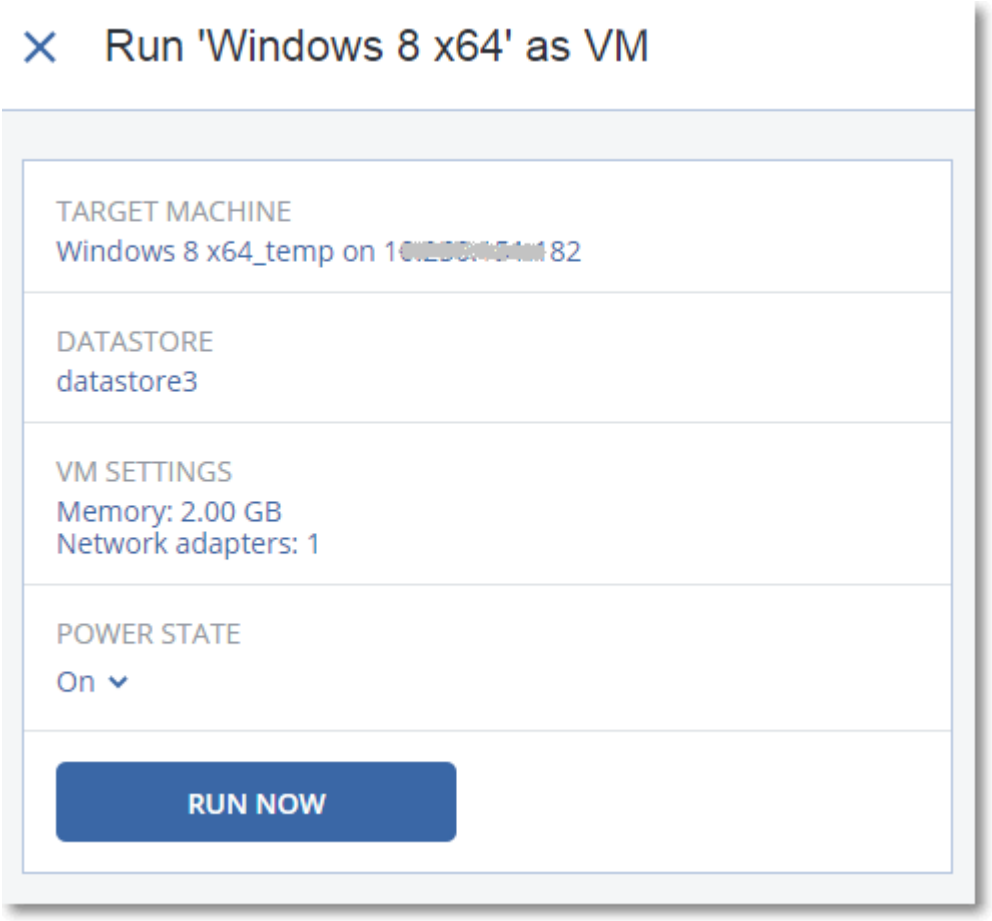
- **재해 복구**
  실패한 머신의 사본을 온라인으로 즉시 가져옵니다.
- **백업 테스트**
  백업에서 머신을 실행하고 게스트 OS 및 애플리케이션이 제대로 작동하는지 확인합니다.
- **애플리케이션 데이터에 액세스**
  머신 실행 중 애플리케이션의 기본 관리 도구를 사용하여 필수 데이터에 액세스하고 필수 데이터를 추출합니다.

사전 요구 사항

- 사이버 보호 서비스에 Agent for VMware 또는 Agent for Hyper-V가 하나 이상 등록되어 있어야 합니다.
- Agent for VMware 또는 Agent for Hyper-V가 설치된 머신의 네트워크 폴더, 스토리지 노드 또는 로컬 폴더에 백업이 저장될 수 있습니다. 네트워크 폴더를 선택하면 머신에서 액세스할 수 있습니다. 가상 머신을 클라우드 스토리지에 저장되어 있는 백업에서 실행할 수 있지만 이 작업에는 백업으로부터 집중적인 임의 액세스 읽기가 필요하기 때문에 속도가 느려집니다. 가상 머신을 SFTP 서버, 테이프 장치 또는 Secure Zone에 저장된 백업에서 실행할 수 없습니다.
- 백업에는 전체 머신이 포함되어 있거나 운영 체제를 시작하는 데 필요한 모든 볼륨이 포함되어 있어야 합니다.
- 실제 머신 및 가상 머신 둘 다의 백업을 사용할 수 있습니다. Virtuozzo *컨테이너*의 백업은 사용할 수 없습니다.
- Linux 논리 볼륨(LVM)을 포함하고 있는 백업은 Agent for VMware 또는 Agent for Hyper-V에서 생성된 것이어야 합니다. 가상 머신은 원래 머신과 동일한 유형이어야 합니다(ESXi 또는 Hyper-V).

머신 실행

1. 다음 중 하나를 수행하십시오.
   - 백업된 머신을 선택하고 **복구**를 클릭한 다음 복구 지점을 선택합니다.
   - 백업 스토리지 탭에서 복구 지점을 선택합니다.
2. **VM으로 실행**을 클릭합니다.
   호스트 및 기타 필수 매개변수가 자동으로 선택됩니다.



3. [선택 사항] **대상 머신**을 클릭한 다음 가상 머신 유형(ESXi 또는 Hyper-V), 호스트 또는 가상 머신 이름을 변경합니다.
4. [선택 사항] ESXi의 경우 **데이터 저장소**를, Hyper-V의 경우 **경로**를 클릭한 다음 가상 머신의 데이터 저장소(스토리지)를 선택합니다.
   머신 실행 중에는 가상 디스크에 대한 변경 사항이 누적됩니다. 선택한 데이터 저장소에 여유 공간이 충분한지 확인합니다. 가상 머신을 영구적으로 설정하여 이 변경 사항을 유지할 계획인 경우, 운영 중인 머신을 실행하는 데 적합한 데이터 저장소를 선택합니다.
5. [선택 사항] **VM 설정**을 클릭하여 가상 머신의 메모리 크기 및 네트워크 연결을 변경합니다.
6. [선택 사항] VM 전원 상태(**켜짐**/**꺼짐**)를 선택합니다.
7. **지금 실행**을 클릭합니다.

따라서 머신이 웹 인터페이스에 아이콘  또는  중 하나와 함께 나타납니다. 이러한 가상 머신은 백업 대상으로 선택할 수 없습니다.

머신 삭제

vSphere/Hyper-V에서 임시 가상 머신을 직접 삭제하는 것은 좋은 방법이 아닙니다. 이렇게 하면 웹 인터페이스에서 불필요한 부분이 생길 수 있습니다. 또한 머신이 실행 중이었던 백업은 한 동안 잠금 상태로 남아 있을 수 있습니다. 이러한 백업은 보관 규칙에 따라 삭제할 수 없습니다.

백업에서 실행 중인 가상 머신을 삭제하려면

1. **모든 장치** 탭에서 백업에서 실행 중인 머신을 선택합니다.
2. **삭제**를 클릭합니다.

웹 인터페이스에서 해당 머신이 제거됩니다. vSphere 또는 Hyper-V 인벤토리 및 데이터 저장소(스토리지)에서도 제거됩니다. 머신 실행 중 데이터에 대해 변경된 모든 사항이 손실됩니다.

머신 완료

가상 머신이 백업에서 실행 중인 경우 가상 디스크의 내용은 해당 백업에서 직접 가져옵니다. 따라서 백업 위치 또는 보호 에이전트에 대한 연결이 끊기면 해당 머신에 액세스할 수 없게 되거나 해당 머신이 손상됩니다.

이 머신을 영구적으로 만들 수 있습니다. 즉, 머신 실행 중 변경된 사항과 함께 모든 가상 디스크를 이러한 변경 사항이 저장된 데이터 저장소로 복구합니다. 이러한 프로세스를 완료라고 합니다.

완료는 가동 중지 없이 수행됩니다. 가상 머신은 완료 중 전원이 꺼지지 *않습니다*.

최종 가상 디스크의 위치는 **VM으로 실행** 작업의 매개변수(ESXi용 **데이터 저장소** 또는 Hyper-V용 **경로**)에 정의되어 있습니다. 완료를 시작하기 전에 여유 공간, 공유 기능, 이 데이터 저장소의 성능이 운영 중 머신 실행에 적합한지 여부 등을 확인하십시오.

참고
Windows Server 2008/2008 R2 및 Microsoft Hyper-V Server 2008/2008 R2에서 실행 중인 Hyper-V의 경우 해당 Hyper-V 버전에는 필요한 API가 누락되어 있기 때문에 완료가 지원되지 않습니다.

백업에서 실행 중인 머신을 완료하려면

1. **모든 장치** 탭에서 백업에서 실행 중인 머신을 선택합니다.
2. **완료**를 클릭합니다.
3. [선택 사항] 머신의 새 이름을 지정합니다.
4. [선택 사항] 디스크 프로비저닝 모드를 변경합니다. 기본 설정은 **씬**입니다.
5. **완료**를 클릭합니다.

머신 이름이 즉시 변경됩니다. 복구 진행률이 **작업** 탭에 표시됩니다. 복구가 완료되면 머신 아이콘이 일반적인 가상 머신 아이콘을 바뀝니다.

완료에 대해서 알아야 할 사항

완료와 일반 복구 비교

다음과 같은 이유로 완료 프로세스는 일반 복구보다 속도가 느립니다.

- 완료를 진행하는 동안 에이전트는 백업의 다른 부분에 임의 액세스를 수행합니다. 전체 머신이 복구되는 동안 에이전트가 백업에서 가져온 데이터를 순차적으로 읽습니다.
- 완료 작업 동안 가상 머신이 실행되는 경우 에이전트는 두 프로세스를 동시에 유지 관리하기 위해 백업에서 가져온 데이터를 더 자주 읽습니다. 일반 복구 시에는 가상 머신이 정지됩니다.

클라우드 백업에서 실행 중인 머신의 완료

백업 데이터에 대한 집중적인 액세스로 인해 완료 속도는 백업 위치와 에이전트 사이의 연결 대역폭에에 따라 크게 달라집니다. 로컬 백업과 비교할 때 클라우드에 있는 백업의 완료 속도가 더 느립니다. 인터넷 연결이 매우 느리거나 불안정한 경우 클라우드 백업에서 실행 중인 머신의 완료 작업이 실패할 수 있습니다. 완료를 수행할 계획인 경우 가능하면 로컬 백업의 가상 머신을 실행하는 것이 좋습니다.

VMware vSphere에서 작업

이 섹션에서는 VMware vSphere 환경에만 관련된 작업을 설명합니다.

가상 머신 복제

복제는 VMware ESXi 가상 머신에 대해서만 가능합니다.

복제는 가상 머신과 똑같은 복사본(복제본)을 생성하고, 이 복제본을 원래 머신과 동기화된 상태로 유지하는 프로세스입니다. 필수 가상 머신을 복제해두면 이 머신의 복사본을 언제든 시작할 준비가 되어 있는 상태로 항상 보유하고 있는 셈입니다.

복제본은 수동으로 또는 지정한 일정에 따라 시작할 수 있습니다. 첫 번째 복제는 전체 복제(전체 머신 복사)입니다. 이후의 모든 복제는 증분 복제로, 이 옵션을 비활성화하지 않는 한, Changed Block Tracking 옵션에 따라 수행됩니다.

복제 대 백업 비교

스케줄대로 이루어지는 백업과 달리 복제본은 가상 머신의 마지막 상태만 유지합니다. 복제본은 데이터 저장소 공간을 사용하는 데 반해, 백업은 더 저렴한 스토리지에 유지할 수 있습니다.

하지만 복제본의 전원을 켜는 것이 복구보다는 훨씬 빠르고, 백업에서 가상 머신을 실행하는 것보다도 빠릅니다. 전원이 켜지면 복제본이 백업에서 실행되는 VM보다 빠르게 작동하고, Agent for VMware를 로드하지 않습니다.

사용 예제

- **가상 머신을 원격 사이트로 복제합니다.**

  복제를 통해 주 사이트에서 보조 사이트로 가상 머신을 복제해두면 부분 또는 전체 데이터 센터 장애 시 대처할 수 있습니다. 대개 보조 사이트는 원격 주 사이트 장애를 유발할 수 있는 환경, 인프라 또는 기타 요인의 영향을 받을 가능성이 거의 없는 원격 설비에 위치합니다.
- **단일 사이트 내에서 가상 머신을 복제합니다(한 호스트/데이터 저장소에서 다른 호스트/데이터 저장소로 복제).**

  온사이트 복제는 고가용성과 재해 복구 시나리오 용도로 사용할 수 있습니다.

복제본으로 할 수 있는 작업

- **복제본 테스트**

  테스트를 위해 복제본의 전원이 꺼집니다. vSphere Client 또는 기타 도구를 사용해 복제본이 올바로 작동하는지 확인합니다. 테스트를 진행하는 동안 복제본은 일시 중지됩니다.
- **복제본으로 장애 조치**

  장애 조치는 원래 가상 머신의 워크로드를 복제본으로 이전하는 작업입니다. 장애 조치를 진행하는 동안 복제본은 일시 중지됩니다.
- **복제본 백업**

  백업과 복제 모두 가상 디스크 액세스가 필요하므로 가상 머신을 실행 중인 호스트의 성능에 영향을 미치게 됩니다. 가상 머신의 복제본과 백업을 모두 확보하고 싶지만 프로덕션 호스트에 추가 로드를 주고 싶지 않다면 머신을 다른 호스트로 복제한 다음, 해당 복제본의 백업을 설정하십시오.

제한 사항

다음 유형의 가상 머신은 복제할 수 없습니다.

- ESXi 5.5 이하에서 실행 중인 내결함성 머신.
- 백업에서 실행하는 머신.
- 가상 머신의 복제본.

복제 계획 생성

복제 계획은 각 머신마다 개별적으로 생성해야 합니다. 기존 계획을 다른 머신에 적용할 수는 없습니다.

복제 계획을 생성하려면

1. 복제할 가상 머신을 선택합니다.
2. **복제**를 클릭합니다.

   소프트웨어에 새 복제 계획 템플릿이 표시됩니다.
3. [선택 사항] 복제 계획 이름을 수정하려면 기본 이름을 클릭합니다.
4. **대상 머신**을 클릭한 후 다음 작업을 수행합니다.

a. 새 복제본을 생성할지, 아니면 원래 머신의 기존 복제본을 사용할지 선택합니다.
b. ESXi 호스트를 선택하고, 새 복제본 이름을 지정하거나 기존 복제본을 선택합니다.
새 복제본의 기본 이름은 **[원래 머신 이름]_replica**입니다.
c. **확인**을 클릭합니다.

5. [새 머신으로 복제하는 경우에만 해당] **데이터 저장소**를 클릭한 다음 가상 머신의 데이터 저장소를 선택합니다.
6. [선택 사항] 복제 스케줄을 변경하려면 **스케줄**을 클릭합니다.
기본적으로 복제는 월요일부터 금요일까지 매일 수행됩니다. 복제를 실행할 시간을 선택할 수 있습니다.
복제 빈도를 변경하려고 하는 경우 슬라이더를 이동한 다음 스케줄을 지정합니다.
다음 작업도 수행할 수 있습니다.
- 스케줄이 적용되는 날짜 범위를 설정합니다. **날짜 범위 내에서 계획 실행** 확인란을 선택한 다음 날짜 범위를 지정합니다.
- 스케줄을 비활성화합니다. 이 경우에는 복제를 수동으로 시작할 수 있습니다.

7. [선택 사항] 복제 옵션을 수정하려면 기어 아이콘을 클릭합니다.
8. **적용**을 클릭합니다.
9. [선택 사항] 계획을 수동으로 실행하려면 계획 패널에서 **지금 실행**을 클릭합니다.

복제 계획을 실행하고 나면 가상 머신 복제본이 **모든 장치** 목록에 다음 아이콘과 함께 나타납니다.

복제본 테스트

복제본 테스트를 준비하려면

1. 테스트할 복제본을 선택합니다.
2. **복제본 테스트**를 클릭합니다.
3. **테스트 시작**을 클릭합니다.
4. 전원이 켜진 복제본을 네트워크에 연결할지 선택합니다. 기본적으로 복제본은 네트워크에 연결되지 않습니다.
5. [선택 사항] 복제본을 네트워크에 연결하기로 선택한 경우 복제본의 전원을 켜기 전에 먼저 **원래 가상 머신 중지** 확인란을 선택하여 원래 머신을 중지합니다.
6. **시작**을 클릭합니다.

복제본 테스트를 중지하려면

1. 테스트가 진행 중인 복제본을 선택합니다.
2. **복제본 테스트**를 클릭합니다.
3. **테스트 중지**를 클릭합니다.
4. 결정을 확인합니다.

복제본으로 장애 조치

머신을 복제본으로 장애 조치하려면

1. 장애 조치할 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **장애 조치**를 클릭합니다.
4. 전원이 켜진 복제본을 네트워크에 연결할지 선택합니다. 기본적으로 복제본은 원래 머신과 같은 네트워크에 연결됩니다.
5. [선택 사항] 복제본을 네트워크에 연결하기로 선택한 경우 **원래 가상 머신 중지** 확인란을 선택 취소하여 원래 머신을 온라인 상태로 유지합니다.
6. **시작**을 클릭합니다.

복제본이 장애 조치 상태에 있는 동안 다음 작업 중 하나를 선택할 수 있습니다.

- **장애 조치 중지**

  원래 머신이 고쳐진 경우 장애 조치를 중지합니다. 복제본의 전원이 꺼집니다. 복제가 다시 시작됩니다.
- **복제본으로 영구 장애 조치 수행**

  이 즉각적인 작업은 가상 머신에서 '복제본' 플래그를 제거하여 이에 대한 복제가 더 이상 가능하지 않도록 합니다. 복제를 다시 시작하려면 복제 계획을 편집하여 이 머신을 소스로 선택하십시오.
- **장애 복구**

  연속 작업을 위해 마련되지 않은 사이트로 장애 조치한 경우에는 장애 복구를 수행합니다. 복제본이 원래 머신 또는 새 가상 머신으로 복구됩니다. 원래 머신으로의 복구가 완료되고 나면 복제본의 전원이 켜지고, 복제가 다시 시작됩니다. 새 머신으로 복구하기로 선택한 경우 복제 계획을 편집하여 이 머신을 소스로 선택하십시오.

장애 조치 중지

장애 조치를 중지하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **장애 조치 중지**를 클릭합니다.
4. 결정을 확인합니다.

영구 장애 조치 수행

영구 장애 조치를 수행하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **영구 장애 조치**를 클릭합니다.
4. [선택 사항] 가상 머신의 이름을 변경합니다.
5. [선택 사항] **원래 가상 머신 중지** 확인란을 선택합니다.
6. **시작**을 클릭합니다.

장애 복구

복제본에서 장애를 복구하려면

1. 장애 조치 상태에 있는 복제본을 선택합니다.
2. **복제본 작업**을 클릭합니다.
3. **복제본에서 장애 복구**를 클릭합니다.
   원래 머신이 대상 머신으로 자동으로 선택됩니다.
4. [선택 사항] **대상 머신**을 클릭한 후 다음 작업을 수행합니다.
   a. 새 머신 또는 기존 머신으로 장애 복구할지 선택합니다.
   b. ESXi 호스트를 선택하고, 새 머신 이름을 지정하거나 기존 머신을 선택합니다.
   c. **확인**을 클릭합니다.
5. [선택 사항] 새 머신으로 장애 복구하는 경우 다음 작업을 수행할 수도 있습니다.
   - **데이터 저장소**를 클릭하여 가상 머신의 데이터 저장소를 선택합니다.
   - **VM 설정**을 클릭해 메모리 크기, 프로세서 수 및 가상 머신의 네트워크 연결을 변경합니다.
6. [선택 사항] **장애 복구 옵션**을 수정하려면 복구 옵션을 클릭합니다.
7. **복구 시작**을 클릭합니다.
8. 결정을 확인합니다.

복제 옵션

복제 옵션을 수정하려면 복제 계획 이름 옆에 있는 기어 아이콘을 클릭한 다음 **복제 옵션**을 클릭합니다.

CBT(Changed Block Tracking)

이 옵션은 백업 옵션 "CBT(Changed Block Tracking)"와 유사합니다.

디스크 프로비저닝

이 옵션은 복제본에 대한 디스크 프로비저닝 설정을 정의합니다.

사전 설정값이 **씬 프로비저닝**입니다.

다음 값을 선택할 수 있습니다. **씬 프로비저닝**, **씩 프로비저닝**, **원래 설정 유지**.

오류 처리

이 옵션은 백업 옵션 "오류 처리"와 유사합니다.

사전/사후 명령어

이 옵션은 백업 옵션 "사전/사후 명령어"와 유사합니다.

가상 머신용 VSS(Volume Shadow Copy Service)

이 옵션은 백업 옵션 "가상 머신용 VSS(Volume Shadow Copy Service)"와 유사합니다.

장애 복구 옵션

장애 복구 옵션을 수정하려면 장애 복구를 구성할 때 **복구 옵션**을 클릭합니다.

오류 처리

이 옵션은 복구 옵션 "오류 처리"와 유사합니다.

성능

이 옵션은 복구 옵션 "성능"과 유사합니다.

사전/사후 명령어

이 옵션은 복구 옵션 "사전/사후 명령어"와 유사합니다.

VM 전원 관리

이 옵션은 복구 옵션 "VM 전원 관리"와 유사합니다.

초기 복제본 시딩

원격 위치로의 복제 속도를 높이고 네트워크 대역폭을 저장하기 위해 복제본 시딩을 수행할 수 있습니다.

중요
복제본 시딩을 수행하려면 Agent for VMware(가상 어플라이언스)가 대상 ESXi에서 실행되어야 합니다.

초기 복제본을 시딩하려면

1. 다음 중 하나를 수행하십시오.
   - 원본 가상 머신의 전원을 끌 수 있다면, 전원을 끈 다음 4단계로 건너뛰십시오.
   - 원본 가상 머신의 전원을 끌 수 없다면 다음 단계를 계속 수행하십시오.
2. 복제 계획을 생성합니다.
   계획을 생성할 때 **대상 머신**에서 **새 복제본** 및 원본 머신을 호스팅하는 ESXi를 선택합니다.
3. 계획을 한 번 실행합니다.
   복제본이 원본 ESXi에 생성됩니다.
4. 가상 머신(또는 복제본) 파일을 외장 하드 드라이브로 내보냅니다.
   a. 외장 하드 드라이브를 vSphere Client가 실행 중인 머신과 연결합니다.
   b. vSphere Client를 원본 vCenter\ESXi로 연결합니다.
   c. 새롭게 생성된 복제본을 인벤토리에서 선택합니다.
   d. **파일** > **내보내기** > **OVF 템플릿 내보내기**를 클릭합니다.
   e. **디렉토리**에서 외장 하드 드라이브의 폴더를 지정합니다.
   f. **확인**을 클릭합니다.
5. 하드 드라이브를 원격 위치로 전송합니다.

6. 복제본을 대상 ESXi로 가져옵니다.
   a. 외장 하드 드라이브를 vSphere Client가 실행 중인 머신과 연결합니다.
   b. vSphere Client를 대상 vCenter\ESXi로 연결합니다.
   c. **파일** > **OVF 템플릿 디플로이**를 클릭합니다.
   d. **파일 또는 URL의 디플로이**에서 앞서 4단계에서 내보낸 템플릿을 지정합니다.
   e. 가져오기 절차를 완료합니다.
7. 2단계에서 생성한 복제 계획을 편집합니다. **대상 머신**에서 **기존 복제본**을 선택한 다음, 가져온 복제본을 선택합니다.

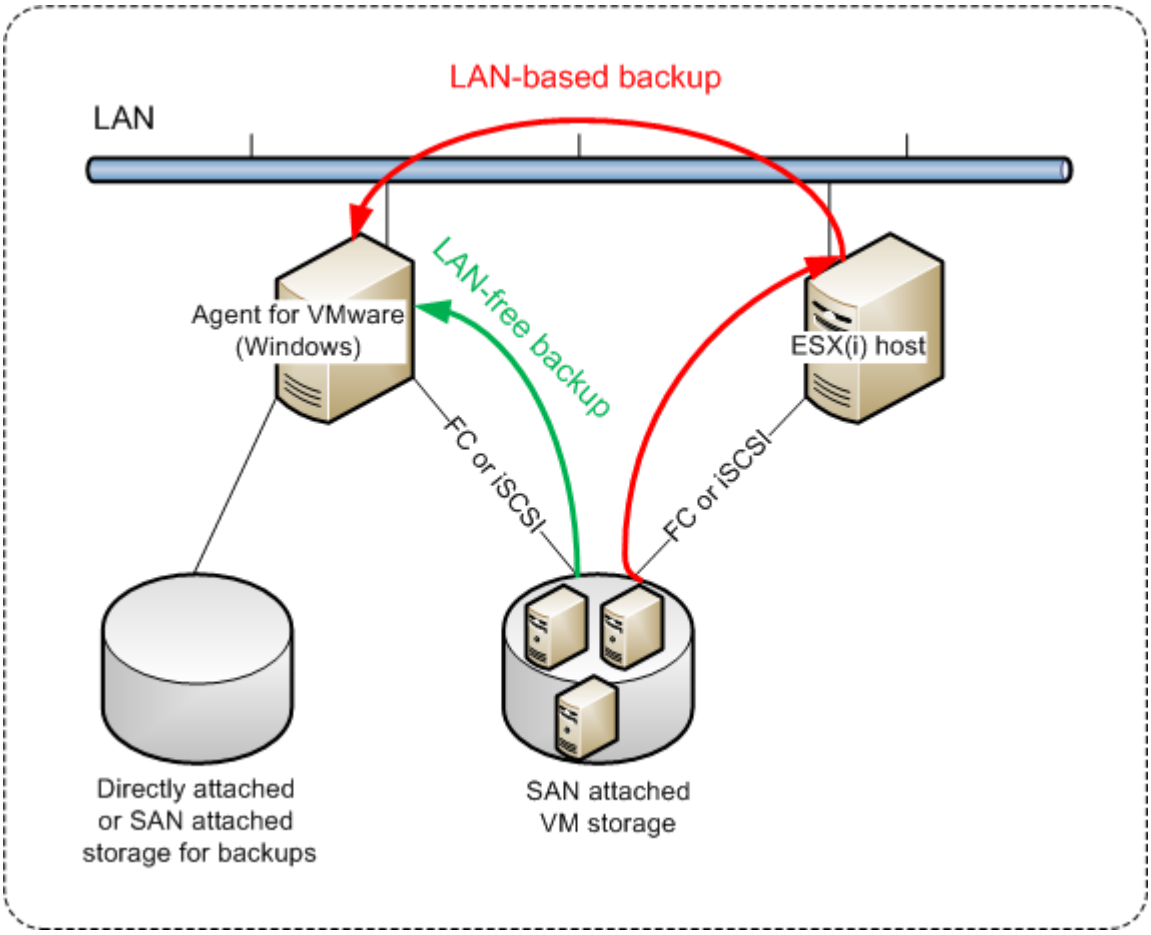
결과적으로 소프트웨어에서 복제본 업데이트를 지속합니다. 모든 복제는 증분식입니다.

LAN 프리 백업

운영 ESXi 호스트 로드가 크게 증가하여 가상 어플라이언스의 실행이 만족스럽지 않은 경우, ESXi 인프라 외부의 실제 머신에 Agent for VMware(Windows) 설치를 고려하십시오.

ESXi에서 SAN 연결 스토리지를 사용하는 경우 동일한 SAN에 연결된 머신에 에이전트를 설치합니다. 에이전트는 ESXi 호스트 및 LAN을 통해서가 아니라 스토리지에서 가상 머신을 직접 백업합니다. 이 기능을 LAN 프리 백업이라고 부릅니다.

아래 다이어그램은 LAN 기반 및 LAN 프리 백업을 보여줍니다. FC(광채널) 또는 iSCSI Storage Area Network가 있는 경우 가상 머신에 대한 LAN 프리 액세스가 가능합니다. LAN을 통한 백업된 데이터 전송을 완전히 제거하기 위해서는 에이전트 머신의 로컬 디스크 또는 SAN 연결 스토리지에 백업을 저장합니다.



에이전트가 데이터 저장소에 직접 액세스할 수 있도록 하려면

1. vCenter Server에 네트워크를 통해 액세스할 수 있는 Windows 머신에 Agent for VMware를 설치합니다.
2. 머신에 데이터 저장소를 호스팅하는 LUN(Logical Unit Number)을 연결합니다. 다음을 고려하십시오.
   - ESXi로의 데이터 저장소 연결에 사용된 동일한 프로토콜(즉, iSCSI 또는 FC)을 사용합니다.
   - LUN은 초기화되지 *말아야* 하며 **디스크 관리**에 "오프라인" 디스크로 표시되어야 합니다. Windows가 LUN을 초기화하면 손상되고 VMware vSphere에서 읽지 못하게 될 수 있습니다. LUN 초기화를 피하기 위해 Agent for VMware(Windows) 설치 중에 **SAN 정책**이 자동으로 **모두 오프라인**으로 설정됩니다.

따라서 에이전트는 SAN 전송 모드를 사용하여 가상 디스크에 액세스합니다. 즉, Windows에서 인식하지 않는 VMFS 파일 시스템을 식별하지 않고 iSCSI/FC에서 LUN 섹터를 읽습니다.

제한 사항

- VSphere 6.0 이상에서, VM 디스크 중 일부는 VVol(VMware Virtual Volume)에 위치하고 일부는 여기에 위치하지 않는 경우 에이전트가 SAN 전송 모드를 사용할 수 없습니다.이러한 가상 머신으로의 백업이 실패합니다.

- 에이전트에 대해 SAN 전송 모드를 구성하더라도 VMware vSphere 6.5에서 소개된 암호화된 가상 머신은 LAN을 통해 백업됩니다.VMware가 암호화된 가상 디스크 백업에 SAN 전송을 지원하지 않기 때문에 에이전트가 NBD 전송으로 폴백합니다.

예

ISCSI SAN을 사용하고 있는 경우 Agent for VMware가 설치된 Windows를 실행 중인 머신에 iSCSI 초기자를 구성합니다.

SAN 정책을 구성하려면

1. 관리자로 로그온하고 명령 프롬프트를 열고 `diskpart`를 입력한 다음, **Enter**를 누릅니다.
2. `san`을 입력한 다음, **Enter**를 누릅니다. **SAN 정책 : 모두 오프라인**이 표시됩니다.
3. SAN 정책의 다른 값이 설정된 경우:
   a. `san policy=offlineall`을 입력합니다.
   b. **Enter** 키를 누릅니다.
   c. 설정이 올바르게 적용되었는지 확인하려면 2단계를 수행합니다.
   d. 머신을 다시 시작합니다.

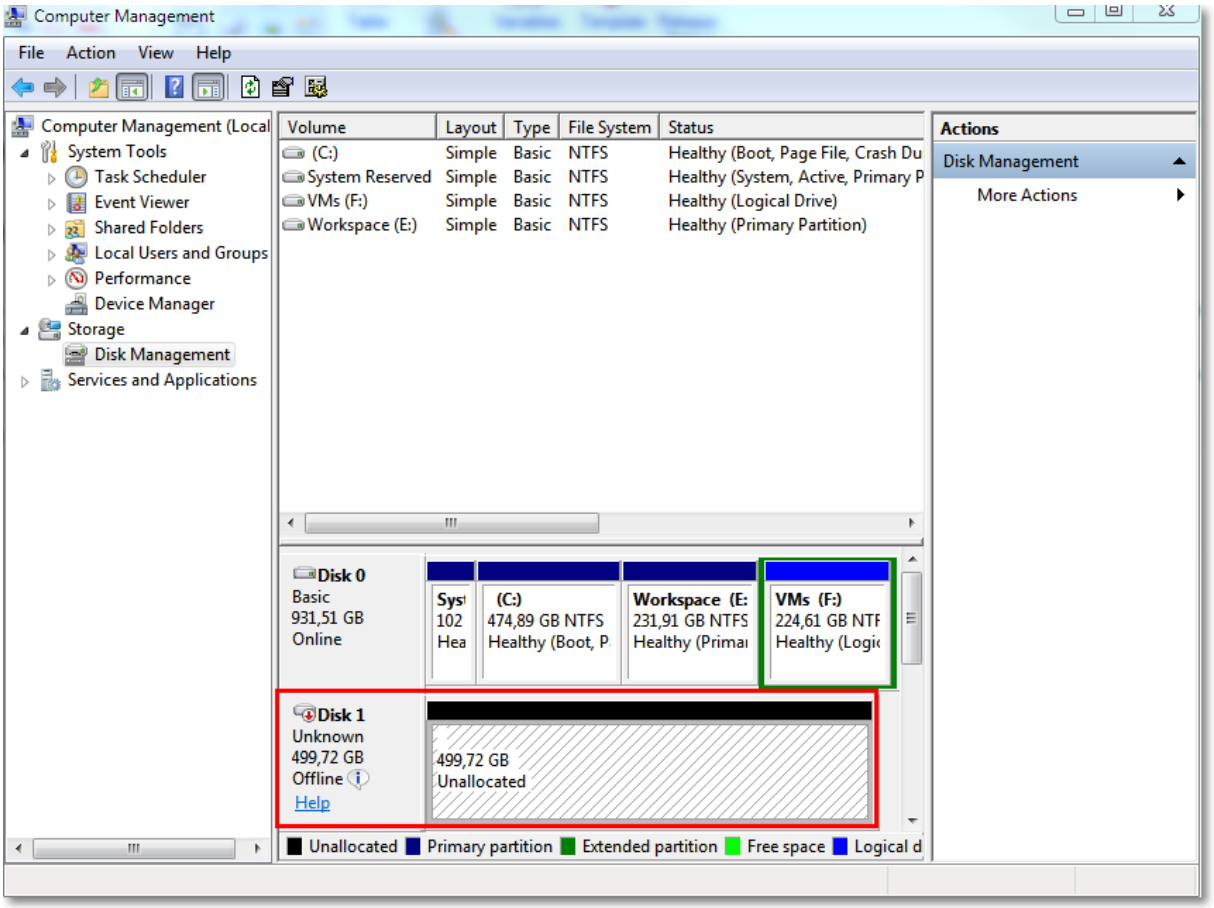
iSCSI 초기자를 구성하려면

1. **제어판** > **관리 도구** > **iSCSI 초기자**로 이동합니다.

   참고
   관리 도구 애플릿을 찾으려면 **제어판** 보기를 **홈** 또는 **카테고리**가 아닌 다른 것으로 변경하거나 검색을 사용해야 할 수 있습니다.

2. Microsoft iSCSI 초기자를 처음 실행하는 경우라면 Microsoft iSCSI 초기자 서비스를 시작하길 원한다고 확인하십시오.
3. **대상** 탭에서 대상 SAN 장치의 FQDN(정규화된 도메인 이름) 또는 IP 주소를 입력한 다음 **빠른 연결**을 클릭합니다.
4. 데이터 저장소를 호스팅하는 LUN을 선택한 다음 **연결**을 클릭합니다.
   LUN이 표시되지 않는 경우 iSCSI 대상의 조닝(zoning)이 에이전트를 실행 중인 머신에서 LUN에 액세스할 수 있도록 활성화되어 있는지 확인하십시오. 해당 머신이 이 대상에 대해 허용된 iSCSI 초기자 목록에 추가되어야 합니다.
5. **확인**을 클릭합니다.

아래 스크린샷에 표시된 바와 같이 준비된 SAN LUN이 **디스크 관리**에 나타납니다.



SAN 하드웨어 스냅샷 사용

VMware vSphere에서 SAN(Storage Area Network) 스토리지 시스템을 데이터 저장소로 사용하는 경우 Agent for VMware(Windows)를 통해 백업을 수행할 때 SAN 하드웨어 스냅샷을 사용할 수 있습니다.

중요

NetApp SAN 스토리지만 지원됩니다.

SAN 하드웨어 스냅샷을 사용하는 이유는 무엇입니까?

일관된 백업을 생성하려면 Agent for VMware에 가상 머신 스냅샷이 필요합니다. 에이전트는 스냅샷에서 가상 디스크 내용을 읽기 때문에 스냅샷은 전체 백업 프로세스 기간 동안 보관되어야 합니다.

기본적으로 에이전트는 ESXi 호스트에서 생성된 기본 VMware 스냅샷을 사용합니다. 스냅샷이 보관되는 동안 가상 디스크 파일은 읽기 전용 상태로 있고 호스트는 디스크에 대한 모든 변경 사항을 개별 델타 파일에 씁니다. 백업 프로세스가 완료되면 호스트는 스냅샷을 삭제합니다. 즉, 델타 파일을 가상 디스크 파일과 병합합니다.

스냅샷 유지보수 및 삭제는 둘 다 가상 머신 성능에 영향을 미칩니다. 큰 가상 디스크와 빠른 데이터 변경이 있으면 이러한 작업에 시간이 오래 걸리고 이 기간에 성능이 저하될 수 있습니다. 극단

적인 경우에는 여러 머신이 동시에 백업될 경우 증가하는 델타 파일이 데이터 저장소를 거의 채우기 때문에 모든 가상 머신의 전원이 꺼집니다.

스냅샷을 SAN으로 오프로드하여 하이퍼바이저 리소스 사용을 줄일 수 있습니다. 이 경우 작업 순서는 다음과 같습니다.

1. ESXi는 백업 프로세스 시작 시 VMware 스냅샷을 사용하여 가상 디스크를 일관된 상태로 유지합니다.
2. SAN에서는 가상 머신과 해당 VMware 스냅샷이 포함된 볼륨 또는 LUN의 하드웨어 스냅샷을 생성합니다. 일반적으로 이 작업에는 몇 초가 걸립니다.
3. ESXi가 VMware 스냅샷을 삭제합니다. Agent for VMware는 SAN 하드웨어 스냅샷에서 가상 디스크 내용을 읽습니다.

VMware 스냅샷이 몇 초 동안만 유지되므로 가상 머신 성능 저하가 최소화됩니다.

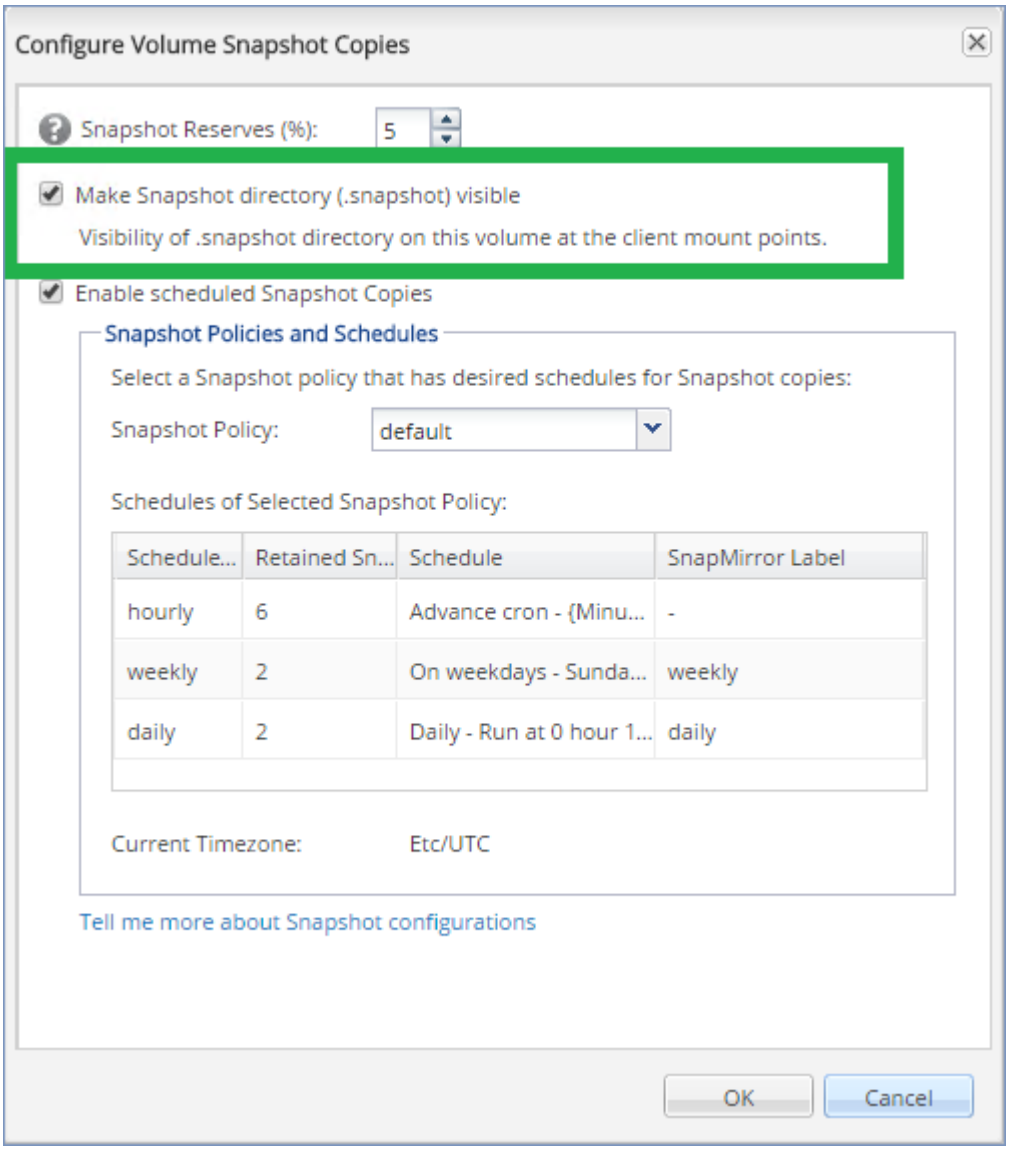
SAN 하드웨어 스냅샷을 사용하려면 무엇이 필요합니까?

가상 머신을 백업할 때 SAN 하드웨어 스냅샷을 사용하려면 다음 조건을 모두 충족해야 합니다.

- NetApp SAN 스토리지가 "NetApp SAN 스토리지 요구 사항"에 설명된 요구 사항을 충족합니다.
- Agent for VMware(Windows)를 실행하는 머신이 "Agent for VMware를 실행하는 머신 구성"의 설명대로 구성되어 있습니다.
- SAN 스토리지가 관리 서버에 등록되어 있습니다.
- [위의 등록에 참여하지 않은 Agent for VMware가 있는 경우] SAN 스토리지에 상주하는 가상 머신이 "가상 머신 결합"에 설명된 대로 SAN 지원 에이전트에 할당되어 있습니다.
- "SAN 하드웨어 스냅샷" 백업 옵션이 보호 계획 옵션에서 활성화되어 있습니다.

NetApp SAN 스토리지 요구 사항

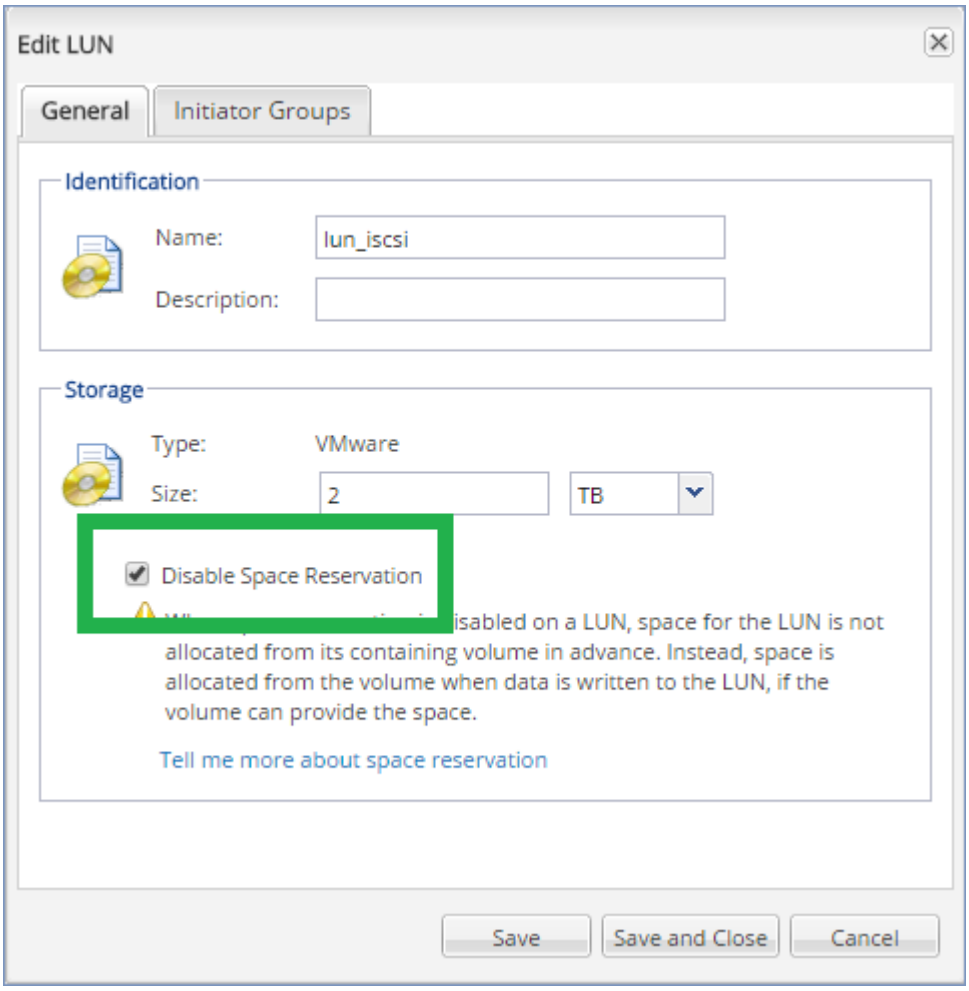
- SAN 스토리지는 NFS 또는 iSCSI 데이터 저장소로 사용되어야 합니다.
- SAN은 **cDOT(Clustered Data ONTAP)**모드에서 Data ONTAP 8.1 이상 버전을 실행해야 합니다. **7-모드** 모드는 지원되지 않습니다.
- 데이터 저장소가 있는 볼륨의 경우 NetApp OnCommand System Manager에서 **스냅샷 복사본** > **구성** > **스냅샷 디렉토리(.snapshot) 표시** 확인란을 선택해야 합니다.



- [NFS 데이터 저장소에 해당] Windows NFSv3 클라이언트에서 NFS 공유 액세스는 데이터 저장소를 생성할 때 지정된 SVM(Storage Virtual Machine)에서 활성화되어야 합니다. 다음 명령으로 액세스를 활성화해야 합니다.

  ```
  vserver nfs modify -vserver [SVM name] -v3-ms-dos-client enable
  ```

  자세한 내용은 NetApp 모범 사례 문서 (https://kb.netapp.com/support/s/article/ka21A0000000k89QAA/top-windows-nfsv3-0-issues-workarounds-and-best-practices)를 참조하십시오.
- [iSCSI 데이터 저장소에 해당] 데이터 저장소가 있는 iSCSI LUN의 경우 NetApp OnCommand System Manager에서 **공간 예약 비활성화** 확인란을 선택해야 합니다.



Agent for VMware를 실행하는 머신 구성

SAN 스토리지를 NFS 또는 iSCSI 데이터 저장소로 사용하는지 여부에 따라 아래 해당하는 섹션을 참조하십시오.

iSCSI 초기자 구성

다음 조건을 모두 충족하는지 확인합니다.

- Microsoft iSCSI 초기자가 설치되어 있습니다.
- Microsoft iSCSI 초기자 서비스 시작 유형이 **자동** 또는 **수동**으로 설정되어 있습니다. 이 작업은 **서비스** 스냅인에서 수행할 수 있습니다.
- "LAN 프리 백업"의 예제 섹션에 설명된 대로 iSCSI 초기자가 구성되어 있습니다.

NFS 클라이언트 구성

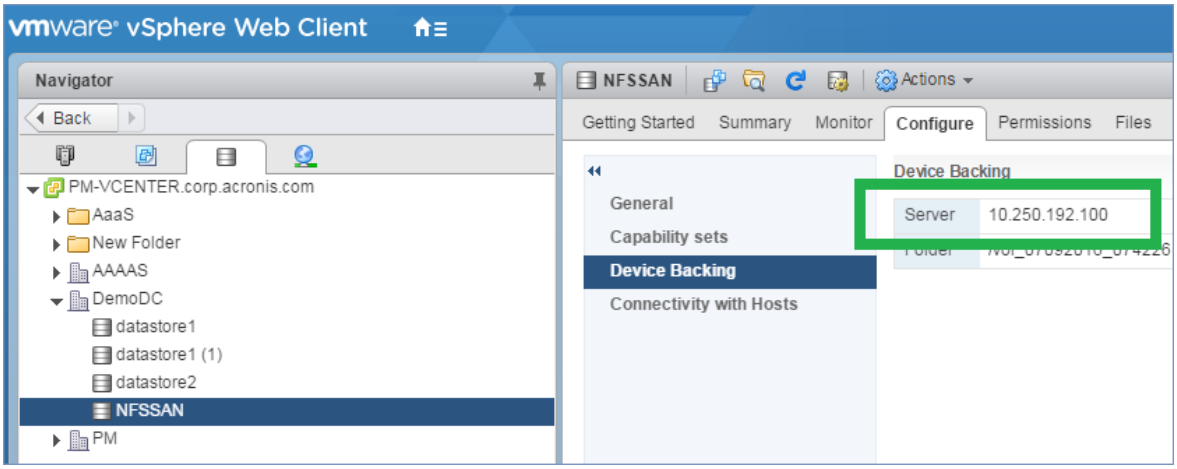
다음 조건을 모두 충족하는지 확인합니다.

- Microsoft **NFS용 서비스**(Windows Server 2008) 또는 **NFS용 클라이언트**(Windows Server 2012 이상)가 설치되어 있습니다.
- NFS 클라이언트가 익명 액세스를 사용하도록 구성되어 있습니다. 예를 들면 다음과 같습니다.

a. 레지스트리 편집기를 엽니다.
b. 다음 레지스트리 키를 찾습니다. **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\ClientForNFS\CurrentVersion\Default**
c. 이 키에서 새 **AnonymousUID**라는 **DWORD** 값을 생성하고 값 데이터를 0으로 설정합니다.
d. 이 키에서 새 **AnonymousGID**라는 **DWORD** 값을 생성하고 값 데이터를 0으로 설정합니다.
e. 머신을 다시 시작합니다.

관리 서버에 SAN 스토리지 등록

1. **설정** > **SAN 스토리지**를 클릭합니다.
2. **스토리지 추가**를 클릭합니다.
3. [선택 사항] **이름**에서 스토리지 이름을 변경합니다.
   이 이름이 **SAN 스토리지** 탭에 표시됩니다.
4. **호스트 이름 또는 IP 주소**에서 데이터 저장소를 생성할 때 지정된 NetApp SVM(스토리지 가상 머신, 파일러라고도 함)을 지정합니다.
   VMware vSphere 웹 클라이언트에서 필요한 정보를 찾으려면 데이터 저장소를 선택하고 **구성** > **장치 지원**을 클릭합니다. 호스트 이름 또는 IP 주소는 **서버** 필드에 표시됩니다.



5. **사용자 이름** 및 **비밀번호**에서 SVM 관리자 자격 증명을 지정합니다.

중요
지정된 계정은 전체 NetApp 시스템 관리 관리자가 아니라 SVM의 로컬 관리자여야 합니다.

기존 사용자를 지정하거나 새 사용자를 생성할 수 있습니다. 새 사용자를 생성하려면 NetApp OnCommand System Manager에서 **구성** > **보안** > **사용자**로 이동하고 새 사용자를 생성합니다.

6. SAN 장치에 대한 읽기 권한이 있는 Agent for VMware(Windows)를 한 개 이상 선택하십시오.
7. **추가**를 클릭합니다.

로컬로 연결된 스토리지 사용

Agent for VMware(가상 어플라이언스)에 추가 디스크를 연결하여 로컬로 연결된 이 스토리지에 에이전트를 백업할 수 있습니다. 이 접근법은 에이전트와 백업 위치 간 네트워크 트래픽을 없애줍니다.

백업된 가상 머신과 같은 호스트 또는 클러스터에서 실행 중인 가상 어플라이언스는 해당 머신이 존재하는 데이터 저장소에 대한 직접 액세스 권한을 가집니다. 즉, 이 어플라이언스는 HotAdd 전송을 사용하여 백업된 디스크에 연결할 수 있고, 따라서 백업 트래픽이 하나의 로컬 디스크에서 다른 디스크로 향하게 됩니다. 데이터 저장소가 **NFS**가 아닌 **Disk/LUN**으로 연결되어 있는 경우 백업은 완전한 LAN 프리 백업이 됩니다. NFS 데이터 저장소의 경우에는 데이터 저장소와 호스트 간에 네트워크 트래픽이 발생합니다.

로컬로 연결된 스토리지를 사용하는 경우에는 에이전트가 항상 동일한 머신을 백업하는 것으로 가정합니다. vSphere에서 여러 에이전트가 작동하고 그중 하나 이상이 로컬로 연결된 스토리지를 사용하는 경우에는 각 에이전트를 백업해야 하는 모든 머신을 수동으로 결합해야 합니다. 그렇지 않고 관리 서버가 에이전트에 머신을 다시 배포하면 머신 백업이 여러 스토리지에 분산될 수 있습니다.

스토리지는 이미 작동 중인 에이전트에 추가할 수도 있고, OVF 템플릿에서 가져온 에이전트를 디플로이할 때 추가할 수도 있습니다.

스토리지를 이미 작동 중인 에이전트에 연결하려면

1. VMware vSphere 인벤토리에서 Agent for VMware(가상 어플라이언스)를 마우스 오른쪽 버튼으로 클릭합니다.
2. 가상 머신의 설정을 편집하여 디스크를 추가합니다. 디스크 크기는 10GB 이상이어야 합니다.

   경고!
   기존 디스크는 조심스럽게 추가합니다. 스토리지가 생성되면 이전에 이 디스크에 포함된 모든 데이터를 잃게 됩니다.

3. 가상 어플라이언스 콘솔로 이동합니다. 화면 하단에 **스토리지 생성** 링크가 나타납니다. 링크가 나타나지 않으면 **새로 고침**을 클릭합니다.
4. **스토리지 생성** 링크를 클릭하고 디스크를 선택한 다음 디스크 레이블을 지정합니다. 레이블 길이는 파일 시스템 제한에 따라 16자로 제한됩니다.

로컬로 연결된 스토리지를 백업 대상으로 선택하려면

보호 계획을 생성할 경우 **백업할 위치**에서 **로컬 폴더**를 선택하고 로컬로 연결된 스토리지에 해당하는 문자(예: **D:**)를 입력합니다.

가상 머신 결합

이 섹션은 관리 서버가 VMware vCenter에서 여러 에이전트의 작업을 구성하는 방법에 대한 개요 정보를 제공합니다.

아래 배포 알고리즘은 Windows에 설치된 가상 어플라이언스와 에이전트에 모두 적용됩니다.

배포 알고리즘

가상 머신이 Agent for VMware 간에 균일하게 배포됩니다. 균일이란 각 에이전트가 동일한 수의 머신을 관리함을 의미합니다. 가상 머신이 점유하는 저장 공간의 크기는 계산하지 않습니다.

그러나 머신의 에이전트를 선택하는 경우 소프트웨어는 전체 시스템 성능을 최적화하려고 시도합니다. 특히 소프트웨어는 에이전트와 가상 머신 위치를 고려합니다. 동일한 호스트에서 호스팅되는 에이전트를 선호합니다. 동일한 호스트에 에이전트가 없는 경우에는 동일한 클러스터의 에이전트를 선호합니다.

가상 머신이 에이전트에 할당되면 이 머신의 모든 백업이 해당 에이전트에 위임됩니다.

재배포

재배포는 설정된 균형이 깨질 때마다 또는 보다 정확하게는 에이전트 간 로드 불균형이 20%에 도달할 때마다 수행됩니다. 이는 머신 또는 에이전트가 추가 또는 제거되거나 머신이 다른 호스트 또는 클러스터로 마이그레이션되거나 머신을 에이전트에 수동으로 결합하는 경우 해당됩니다. 이러한 경우에는 관리 서버가 동일한 알고리즘을 사용하여 머신을 재배포합니다.

예를 들어, 처리량 문제로 에이전트가 더 필요하다고 판단하여 클러스터에 추가 가상 어플라이언스를 디플로이할 수 있습니다. 관리 서버는 새 에이전트에 가장 적합한 머신을 할당합니다. 이전 에이전트의 로드는 감소합니다.

관리 서버에서 에이전트를 제거하는 경우 에이전트에 할당된 머신은 나머지 에이전트에 배포됩니다. 그러나 에이전트가 손상되거나 vSphere에서 수동으로 삭제된 경우는 이에 해당되지 않습니다. 재배포는 웹 인터페이스에서 해당 에이전트를 제거한 후에만 시작됩니다.

배포 결과 보기

다음 위치에서 자동 배포의 결과를 볼 수 있습니다.

- **모든 장치** 섹션의 각 가상 머신에 대한 **에이전트** 열
- 에이전트가 **설정** > **에이전트** 섹션에서 선택된 경우 **상세정보** 패널의 **할당된 가상 머신** 섹션

수동 결합

Agent for VMware 결합을 사용하면 이 머신을 항상 백업해야 하는 에이전트를 지정하여 이 배포 프로세스에서 가상 머신을 제외할 수 있습니다. 전체적인 균형은 유지되지만 이 특정 머신은 원래 에이전트가 제거된 경우에만 다른 에이전트로 전달될 수 있습니다.

머신과 에이전트를 결합하려면

1. 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
   할당된 에이전트 섹션에는 선택한 머신을 현재 관리하는 에이전트가 표시됩니다.
3. **변경**을 클릭합니다.
4. **수동**을 선택합니다.
5. 머신을 결합할 에이전트를 선택합니다.
6. **저장**을 클릭합니다.

머신과 에이전트의 결합을 해제하려면

1. 머신을 선택합니다.
2. **상세정보**를 클릭합니다.
   할당된 에이전트 섹션에는 선택한 머신을 현재 관리하는 에이전트가 표시됩니다.
3. **변경**을 클릭합니다.
4. **자동**을 선택합니다.
5. **저장**을 클릭합니다.

에이전트에 대한 자동 할당 비활성화

Agent for VMware가 백업해야 하는 머신 목록을 지정하는 방식으로 이 에이전트에 대한 자동 할당을 비활성화하여 배포 프로세스에서 제외할 수 있습니다. 다른 에이전트 간에 전체적인 균형이 유지됩니다.

다른 등록된 에이전트가 없거나 다른 모든 에이전트에 대한 자동 할당이 비활성화된 경우에는 에이전트에 대한 자동 할당을 비활성화할 수 없습니다.

에이전트에 대한 자동 할당을 비활성화하려면

1. **설정** > **에이전트**를 클릭합니다.
2. 자동 할당을 비활성화할 Agent for VMware를 선택합니다.
3. **상세정보**를 클릭합니다.
4. **자동 할당** 스위치를 비활성화합니다.

사용 예제

- 특정(대규모) 머신을 Agent for VMware(Windows)에서 파이버 채널을 통해 백업하고 다른 머신은 가상 어플라이언스에서 백업하는 경우 수동 결합이 유용합니다.
- SAN 하드웨어 스냅샷을 사용할 경우 수동 결합이 필요합니다. SAN 하드웨어 스냅샷이 구성된 Agent for VMware(Windows)를 SAN 데이터 저장소에 상주하는 머신과 결합합니다.
- 에이전트에 로컬로 연결된 스토리지가 있는 경우 VM을 에이전트에 결합해야 합니다.
- 자동 할당을 비활성화하면 특정 머신을 지정한 스케줄에 따라 예상대로 백업할 수 있습니다. VM을 하나만 백업하는 에이전트는 스케줄된 시간이 되면 다른 VM을 백업하는 데 사용할 수 없습니다.
- 지리적으로 떨어진 여러 ESXi 호스트가 있는 경우 자동 할당을 비활성화하는 것이 좋습니다. 자동 할당을 비활성화하고 각 호스트의 VM을 같은 호스트에서 실행 중인 에이전트에 결합하면, 에이전트가 원격 ESXi 호스트에서 실행 중인 머신을 백업하지 않으므로 네트워크 트래픽을 절약할 수 있습니다.

VM 이주 지원

이 섹션은 vSphere 클러스터의 일부인 ESXi 호스트 간의 마이그레이션을 포함하여 vSphere 환경에서 가상 머신을 마이그레이션할 때 예상되는 점에 대해 설명합니다.

vMotion

vMotion은 머신의 디스크는 공유 스토리지의 동일한 장소에 유지되는 반면 가상 머신의 상태와 구성을 다른 호스트로 이동합니다.

- Agent for VMware(가상 어플라이언스)의 vMotion은 지원되지 않으므로 비활성화됩니다.
- 백업 중 가상 머신의 vMotion이 비활성화됩니다. 마이그레이션이 완료된 후에도 백업이 계속 실행됩니다.

Storage vMotion

Storage vMotion은 가상 머신 디스크를 데이터 저장소에서 다른 곳으로 이동합니다.

- Agent for VMware(가상 어플라이언스)의 Storage vMotion은 지원되지 않으므로 비활성화됩니다.
- 백업 중 가상 머신의 Storage vMotion이 비활성화됩니다. 이주 후에도 백업이 계속 실행됩니다.

가상화 환경 관리

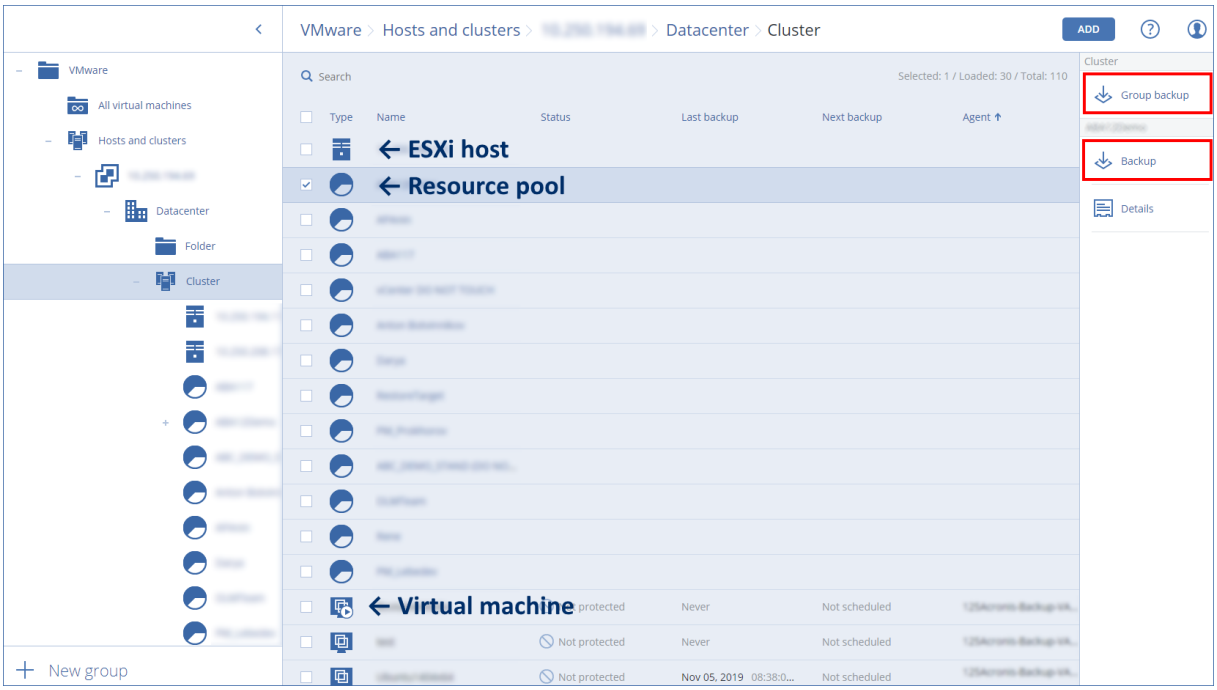
vSphere, Hyper-V 및 Virtuozzo 환경을 각각의 네이티브 표시로 볼 수 있습니다. 해당 에이전트가 설치 및 등록되어 있으면 **VMware**, **Hyper-V** 또는 **Virtuozzo** 탭이 **장치** 아래에 표시됩니다.

VMware 탭에서 다음과 같은 vSphere 인프라 개체를 백업할 수 있습니다.

- 데이터 센터
- 폴더
- 클러스터
- ESXi 호스트
- 리소스 풀

이러한 인프라 객체 각각은 가상 머신에 대한 그룹 객체로 작동합니다. 이러한 그룹 객체에 보호 계획을 적용할 때 그 안에 포함된 모든 가상 머신이 백업됩니다. **백업**을 클릭하여 선택된 그룹 머신을 백업하거나 **그룹 백업**을 클릭하여 선택된 그룹이 포함된 부모 그룹 머신을 백업할 수 있습니다.

예를 들어 해당 클러스터를 선택한 후 그 안의 리소스 풀을 선택했다고 가정해 보겠습니다. **백업**을 클릭하면 선택된 리소스 풀에 포함된 모든 가상 머신이 백업됩니다. **그룹 백업**을 클릭하면 클러스터에 포함된 모든 가상 머신이 백업됩니다.



에이전트를 다시 설치하지 않고 vCenter Server 또는 독립형 ESXi 호스트에 대한 액세스 자격 증명을 변경할 수 있습니다.

vCenter Server 또는 ESXi 호스트 액세스 자격 증명을 변경하려면

1. **장치**에서 **VMware**를 클릭합니다.
2. **호스트 및 클러스터**를 클릭합니다.
3. **호스트 및 클러스터** 트리의 오른쪽에 있는 **호스트 및 클러스터** 목록에서 Agent for VMware 설치 중 지정한 vCenter Server 또는 독립형 ESXi 호스트를 선택합니다.
4. **상세정보**를 클릭합니다.
5. **자격 증명**에서 사용자 이름을 클릭합니다.
6. 새 액세스 자격 증명을 지정한 다음 **확인**을 클릭합니다.

vSphere Client에서 백업 상태 보기

vSphere Client에서 가상 머신의 마지막 백업 시간과 백업 상태를 볼 수 있습니다.

이 정보는 가상 머신 요약(**요약** > **사용자 정의 속성/주석/메모**, 클라이언트 유형 및 vSphere 버전에 따라 달라짐)에 나타납니다. 모든 호스트, 데이터센터, 폴더, 리소스 풀 또는 전체 vCenter Server의 **가상 머신** 탭에서 **마지막 백업** 및 **백업 상태** 열을 활성화할 수도 있습니다.

이러한 속성을 제공하려면 Agent for VMware에는 "Agent for VMware - 필수 권한"에 설명된 권한 외에 다음과 같은 권한이 있어야 합니다.

- **글로벌** > **사용자 정의 속성 관리**
- **글로벌** > **사용자 정의 속성 설정**

Agent for VMware - 필수 권한

이 섹션은 ESXi 가상 머신 작업과 추가적으로 가상 어플라이언스 배포에 필요한 권한에 대해 설명합니다.

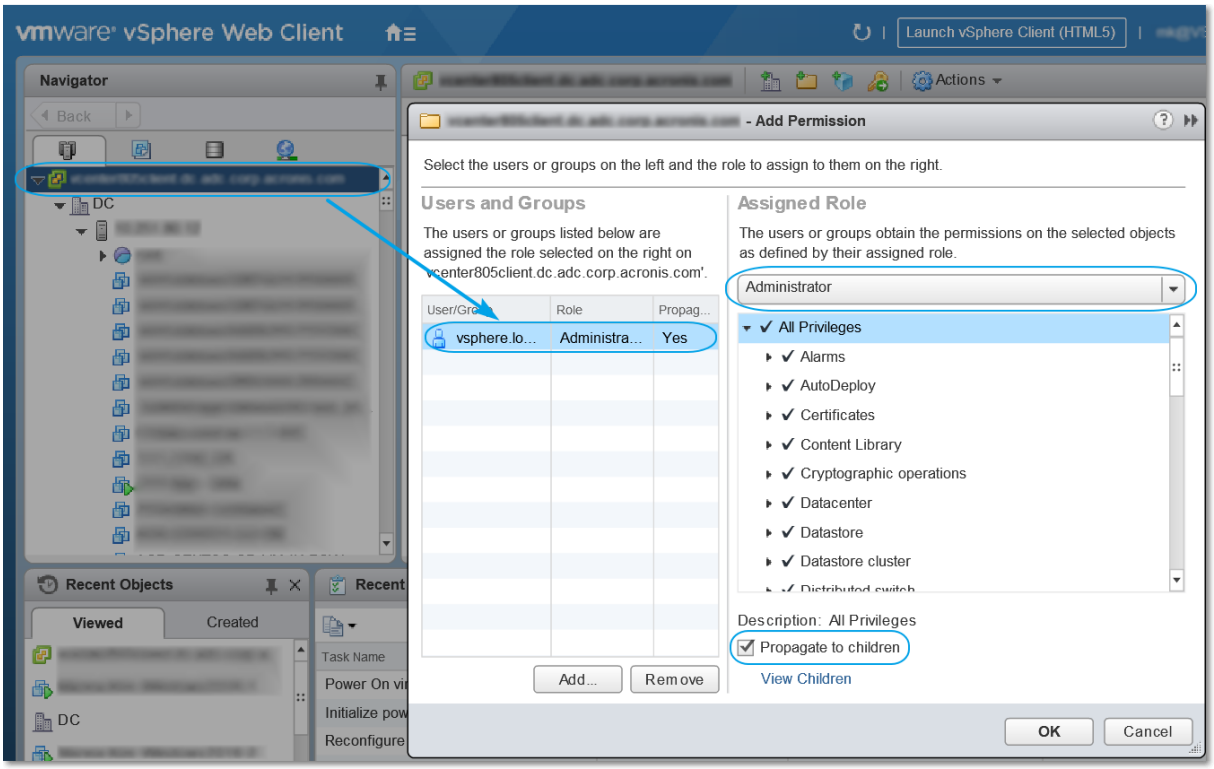
참고
가상 머신 백업을 활성화하려면 vStorage API를 ESXi 호스트에 설치해야 합니다. https://kb.acronis.com/content/14931을 참조하십시오.

가상 머신, ESXi 호스트, 클러스터, vCenter 같은 vCenter 객체를 사용하여 작업을 수행하기 위해, VMware용 에이전트는 사용자가 제공한 vSphere 자격 증명을 사용하여 vCenter 또는 ESXi 호스트에서 인증합니다. VMware용 에이전트에 의한 vSphere로의 연결에 사용된 vSphere 계정에는 vCenter 수준부터 모든 vSphere 인프라 수준에 대해 필요한 권한이 있어야 합니다.

Agent for VMware를 설치하거나 구성하는 동안 vSphere 계정에 필수 권한을 지정합니다. 나중에 계정을 변경해야 하는 경우 "가상화 환경 관리" 섹션을 참조하십시오.

vCenter 수준에서 vSphere 사용자에게 권한을 할당하려면 다음을 수행하십시오.

1. vSphere 웹 클라이언트에 로그인합니다.
2. vCenter를 마우스 오른쪽 버튼으로 클릭한 다음, **권한 추가**를 클릭합니다.
3. 필요한 역할을 가진 새 사용자를 선택하거나 추가합니다(역할은 아래 표의 모든 필수 권한을 포함해야 합니다).
4. **자식에 전파** 옵션을 선택합니다.



객체	권한	작업				
		VM 백업	머신 추가	기존의 VM으로 복구	백업에서 VM 실행	VA 디플로이
암호화 동작 (vSphere 6.5 부터 시작)	디스크 추가	+*				
	직접 액세스	+*				
데이터 저장소	공간 할당		+	+	+	+
	데이터 저장소 찾기				+	+
	데이터 저장소 구성	+	+	+	+	+
	낮은 수준의 파일 작업				+	+
글로벌	라이센스	+	+	+	+	
	방법 비활성화	+	+	+		
	방법 활성화	+	+	+		
	사용자 정의 속성 관리	+	+	+		
	사용자 정의 속성 설정	+	+	+		
호스트 > 구성	VM 자동 시작 구성					+
	저장소 파티션 구성				+	
호스트 > 인벤토리	클러스터 수정					+
호스트 > 로컬 작업	VM 생성				+	+
	VM 삭제				+	+
	VM 재구성				+	+
네트워크	네트워크 할당		+	+	+	+
리소스	VM을 리소스 풀로 할당		+	+	+	+
	가져오기					+
가상 머신 > 구성	기존의 디스크 추가	+	+		+	

	새 디스크 추가		+	+	+	+
	장치 추가 또는 제거		+		+	+
	고급	+	+	+		+
	CPU 개수 변경		+			
	디스크 변경 추적	+		+		
	디스크 임대	+		+		
	메모리		+			
	디스크 제거	+	+	+	+	
	이름 변경		+			
	주석 설정				+	
	설정		+	+	+	
가상 머신 > 게스트 작업	게스트 작업 프로그램 실행	+**				+
	게스트 작업 쿼리	+**				+
	게스트 작업 수정	+**				
가상 머신 > 상호 작용	게스트 제어 티켓 획득 (vSphere 4.1 및 5.0)				+	+
	CD 미디어 구성		+	+		
	콘솔 상호 작용					+
	VIX API의 게스트 운영 체제 관리(vSphere 5.1 이상)				+	+
	전원 끄기			+	+	+
	전원 켜기		+	+	+	+
가상 머신 > 인벤토리	기존 항목에서 생성		+	+	+	
	새로 만들기		+	+	+	+
	이동					+
	등록				+	
	제거		+	+	+	+
	등록 해제				+	

가상 머신 > 프로비저닝	**디스크 액세스 허용**		+	+	+	
	읽기 전용 디스크 액세스 허용	+		+		
	가상 머신 다운로드 허용	+	+	+	+	
가상 머신 > 상태 **가상 머신 > 스냅샷 관리** (vSphere 6.5 이상)	**스냅샷 생성**	+		+	+	+
	스냅샷 제거	+		+	+	+
vApp	**가상 머신 추가**				+	

***** 암호화된 머신 백업에만 이 권한이 필요합니다.

****** 애플리케이션 인식 백업에만 이 권한이 필요합니다.

클러스터 Hyper-V 머신 백업

Hyper-V 클러스터에서는 가상 머신이 클러스터 노드 간에 마이그레이션될 수 있습니다. 클러스터 Hyper-V 머신의 올바른 백업을 설정하려면 이 권장 사항을 따릅니다.

1. 어떤 노드로 마이그레이션되었는지에 상관없이 머신을 백업에 사용할 수 있어야 합니다. Agent for Hyper-V가 모든 노드에 있는 머신에 액세스할 수 있도록 보장하려면 에이전트 서비스가 각각의 클러스터 노드에서 관리자 권한을 가진 도메인 사용자 계정에서 실행되어야 합니다. Agent for Hyper-V 설치 중 에이전트 서비스에 대해 그러한 계정을 지정하는 것이 권장됩니다.
2. 클러스터의 각 노드에 Agent for Hyper-V를 설치합니다.
3. 관리 서버에 모든 에이전트를 등록합니다.

복구된 머신의 고가용성

백업된 디스크를 *기존* Hyper-V 가상 머신에 복구하는 경우 머신의 고가용성 특성은 그대로 유지됩니다.

백업된 디스크를 *새로운* Hyper-V 가상 머신으로 복구하거나 보호 계획 내에서 Hyper-V 가상 머신으로의 변환을 수행하는 경우, 해당 머신의 가용성이 높지 않게 됩니다. 해당 머신은 예비 머신으로 간주되며 일반적으로 전원이 꺼져 있습니다. 머신을 운영 환경에서 사용해야 하는 경우에는 **장애 조치 클러스터 관리** 스냅인에서 고가용성에 맞게 구성할 수 있습니다.

동시 백업되는 가상 머신의 총 수를 제한합니다.

예약 백업 옵션은 정해진 보호 계획을 실행할 때 에이전트가 몇 개의 가상 머신을 동시에 백업할 수 있는지 정의합니다.

여러 보호 계획의 시간이 겹치는 경우 각 백업 옵션에 지정된 숫자가 합산됩니다. 총 숫자 결과가 프로그램에서 10으로 제한되더라도 계획이 겹치면 백업 성능에 영향을 주고 호스트와 가상 머신 스토리지 모두에 과부하가 발생할 수 있습니다.

Agent for VMware 또는 Agent for Hyper-V가 동시에 백업할 수 있는 가상 머신의 총 수를 더 줄일 수 있습니다.

Agent for VMware(Windows) 또는 Agent for Hyper-V가 백업할 수 있는 가상 머신의 총 수를 제한하려면

1. 에이전트를 실행 중인 머신에서 새 텍스트 문서를 생성해 텍스트 편집기(예: 메모장)에서 엽니다.
2. 파일에 다음 행을 복사해 붙여넣습니다.

   ```
   Windows Registry Editor Version 5.00

   [HKEY_LOCAL_
   MACHINE\SOFTWARE\Acronis\MMS\Configuration\ManagedMachine\SimultaneousBackupsLimits]
   "MaxNumberOfSimultaneousBackups"=dword:00000001
   ```

3. `00000001`을 설정하려는 제한의 16진수 값으로 대체합니다. 예를 들어, `00000001`은 1이고 `0000000A`는 10입니다.
4. 문서를 **limit.reg**로 저장합니다.
5. 이 파일을 관리자로 실행합니다.
6. Windows 레지스트리를 편집할 것인지 확인합니다.
7. 다음을 수행하여 에이전트를 다시 시작하십시오.
   a. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
   b. **확인**을 클릭합니다.
   c. 다음 명령 실행:

   ```
   net stop mms
   net start mms
   ```

Agent for VMware(가상 어플라이언스) 또는 Agent for VMware(Linux)가 백업할 수 있는 가상 머신의 총 수를 제한하려면

1. 에이전트를 실행 중인 머신에서 다음 명령 셸을 시작합니다.
   - **Agent for VMware(가상 어플라이언스):** 가상 어플라이언스 UI에서 CTRL+SHIFT+F2를 누릅니다.
   - **Agent for VMware(Linux):** Acronis Cyber Protect 어플라이언스를 실행 중인 머신에 루트 사용자로 로그인합니다. 패스워드는 Cyber Protect 웹 콘솔의 패스워드와 동일합니다.

2. **vi** 등의 텍스트 편집기에서 **/etc/Acronis/MMS.config** 파일을 엽니다.
3. 다음 섹션을 찾습니다.

```
<key name="SimultaneousBackupsLimits">
    <value name="MaxNumberOfSimultaneousBackups" type="Tdword">"10"</value>
</key>
```

4. 10을 설정하려는 제한의 10진수 값으로 대체합니다.
5. 파일을 저장합니다.
6. 에이전트를 다시 시작합니다.
   - **Agent for VMware(가상 어플라이언스):** 재부팅 명령을 실행합니다.
   - **Agent for VMware(Linux):** 다음 명령을 실행합니다.

```
sudo service acronis_mms restart
```

머신 이주

머신의 백업을 원래 머신이 아닌 머신으로 복구하여 머신 이주를 수행할 수 있습니다.

다음 표가 이용 가능한 마이그레이션 방법을 요약하고 있습니다.

백업된 머신 유형	이용 가능한 복구 목적지							
	실제 머신	ESXi 가상 머신	Hyper-V 가상 머신	Virtuozzo 가상 머신*	Virtuozzo 컨테이너*	Virtuozzo Hybrid Infrastructure 가상 머신*	Scale Computing HC3 가상 머신	RHV/oVirt 가상 머신*
실제 머신	+	+	+	-	-	+	+	+
VMware ESXi 가상 머신	+	+	+	-	-	+	+	+
Hyper-V 가상 머신	+	+	+	-	-	+	+	+
Virtuozzo 가상 머신*	+	+	+	+	-	+	+	+
Virtuozzo 컨테이너*	-	-	-	-	+	-	-	-
Virtuozzo Hybrid Infrastructure 가상 머신*	+	+	+	-	-	+	+	+
Scale	+	+	+	-	-	+	+	+

Computing HC3 가상 머신								
Red Hat Virtualization /oVirt 가상 머신*	+	+	+	-	-	+	+	+

* 클라우드 디플로이 시에만 사용 가능합니다.

이주 수행 방법에 대한 지침은 다음 섹션을 참조하십시오.

- 물리-가상(P2V) – "가상 머신에 실제 머신 복구"(289페이지)
- 가상-가상(V2V) – "가상 머신 복구"(291페이지)
- 가상-물리(V2P) – "가상 머신 복구"(291페이지) 또는 "부트 가능한 미디어를 사용하여 디스크 및 볼륨 복구"(294페이지)

웹 인터페이스에서 V2P 이주를 수행할 수 있더라도 특정한 경우 부트 가능한 미디어를 사용하는 것이 좋습니다. 때때로 ESXi 또는 Hyper-V로 이주에 미디어를 사용하려고 할 수 있습니다.

미디어를 사용하면 다음 작업을 수행할 수 있습니다.

- 논리 볼륨을 포함한 Linux 머신(LVM)의 P2V 마이그레이션 또는 V2P 마이그레이션을 수행합니다. Agent for Linux 또는 부트 가능한 미디어를 사용하여 복구를 위한 백업 및 부트 가능한 미디어를 생성합니다.
- 시스템 부팅 기능에 중요한 특성 하드웨어에 드라이버를 제공합니다.

Windows Azure 및 Amazon EC2 가상 머신

Windows Azure 또는 Amazon EC2 가상 머신을 백업하려면 머신에 보호 에이전트를 설치합니다. 백업 및 복구 작업은 실제 머신과 동일합니다. 그럼에도 불구하고 클라우드 디플로이에서 머신 수 할당량을 설정할 때에는 가상 머신으로 계산됩니다.

실제 머신과의 차이점은 Windows Azure와 Amazon EC2 가상 머신을 부트 가능한 미디어에서 부팅할 수 없다는 것입니다. 새 Windows Azure 또는 Amazon EC2 가상 머신으로 복구해야 하는 경우 아래의 절차를 따르십시오.

머신을 Windows Azure 또는 Amazon EC2 가상 머신으로 복구하려면

1. Windows Azure 또는 Amazon Ec2의 이미지/템플릿에서 새 가상 머신을 생성합니다. 새 머신에는 복구하려는 머신과 동일한 디스크 구성이 있어야 합니다.
2. 새 머신에 Agent for Windows 또는 Agent for Linux를 설치합니다.
3. "실제 머신"에 설명된 대로 백업된 머신을 복구합니다. 복구를 구성할 때 새 머신을 대상 머신으로 선택합니다.

네트워크 요구사항

백업한 머신에 설치된 에이전트는 네트워크를 통해 관리 서버와 통신할 수 있어야 합니다.

온프레미스 디플로이

- 에이전트와 관리 서버가 모두 Azure/EC2 클라우드에 설치되어 있는 경우 모든 머신은 이미 동일한 네트워크에 위치합니다. 추가 작업은 필요하지 않습니다.
- 관리 서버가 Azure/EC2 클라우드 외부에 있는 경우, 클라우드에 있는 머신은 관리 서버가 설치되어 있는 로컬 네트워크에 네트워크 액세스할 수 없습니다. 이러한 머신에 설치된 에이전트가 관리 서버와 통신하도록 하려면 로컬(온-프레미스)과 클라우드(Azure/EC2) 네트워크 간에 VPN(가상 개인 네트워크) 연결이 생성되어야 합니다. VPN 연결을 생성하는 방법에 대한 자세한 내용은 다음 문서를 참조하십시오.

  Amazon EC2: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_VPN.html#vpn-create-cgw

  Windows Azure: https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal

클라우드 디플로이

클라우드 디플로이에서는 관리 서버가 Acronis 데이터 센터 중 하나에 위치하고 에이전트에 의해 연결 가능합니다. 추가 작업은 필요하지 않습니다.

SAP HANA 보호

SAP HANA의 보호는 별도 문서(https://dl.managed-protection.com/u/pdf/AcronisCyberProtect_15_SAP_HANA_whitepaper_en-US.pdf)에 설명되어 있습니다.

맬웨어 방지 및 웹 보호

Cyber Protect의 맬웨어 방지 기능에는 다음과 같은 이점이 있습니다.

- 사전 보호, 능동 보호, 사후 보호의 모든 단계에서 최고의 보호를 제공합니다.
- 내장된 4가지 맬웨어 방지 기술이 동종 최고 수준의 다중 계층 보호를 제공합니다.
- Microsoft Security Essentials와 Windows Defender 바이러스 백신을 관리합니다.

바이러스 백신 및 맬웨어 방지 기능

바이러스 백신 및 맬웨어 방지 기능 모듈은 모든 최신 맬웨어 위협에서 Windows 및 macOS 머신을 보호합니다. 맬웨어 방지의 일부인 Active Protection 기능은 macOS 머신에서 지원되지 않는다는 점에 유의하십시오. 지원되는 맬웨어 방지 기능의 전체 목록을 아래에서 확인하십시오. 운영 체제별 지원되는 기능.

Acronis Cyber Protect은(는) Windows 보안 센터에서 지원 및 등록됩니다.

안티바이러스 및 맬웨어 방지 기능 모듈을 적용하는 시점에 머신이 이미 서드 파티 안티바이러스 솔루션으로 보호되고 있는 경우, 잠재적인 호환성 및 성능 문제를 방지하기 위해 시스템에서 경보를 생성하고 실시간 보호를 중지합니다. 완전히 작동하는 Acronis Cyber Protect의 안티바이러스 및 맬웨어 방지 기능을 활성화하려면 서드 파티 안티바이러스 솔루션을 비활성화 또는 설치 제거해야 합니다.

다음 맬웨어 방지 기능을 사용할 수 있습니다.

- 실시간 보호 및 온디맨드 모드에서 파일의 맬웨어 감지(Windows, macOS)
- 프로세스에서 악성 동작 감지(Windows)
- 악성 URL에 대한 액세스 차단(Windows)
- 위험 파일 격리
- 신뢰하는 기업 애플리케이션을 허용 목록에 추가

바이러스 백신 및 맬웨어 방지 기능 모듈은 두 가지 유형의 스캔을 제공합니다.

- 실시간 보호 스캔
- 온디맨드 맬웨어 스캔

실시간 보호 스캔

실시간 보호는 머신에서 실행되거나 열리는 모든 파일을 확인해 맬웨어 위협을 방지합니다.

다음 스캔 유형 중 하나를 선택할 수 있습니다.

- 온액세스 감지는 맬웨어 방지 프로그램이 백그라운드에서 실행되며, 시스템이 켜져 있는 내내 머신 시스템을 능동적이고 지속적으로 스캔하며 바이러스와 기타 악성 위협을 찾아냅니다. 맬웨어는 파일이 실행될 때, 그리고 파일을 읽거나 편집하기 위해 여는 등의 다양한 작업 중에 감지됩니다.

- 온엑시큐션 감지는 실행 파일에 대해서만 실행 시 자동으로 스캔하여 파일에 문제가 없으며 머신 또는 데이터에 손상을 야기하지 않는지 확인합니다. 감염된 파일의 사본은 감지되지 않은 채 유지됩니다.

온디맨드 맬웨어 스캔

맬웨어 방지 스캔은 스케줄에 따라 수행됩니다.

대시보드 > **개요** > 최근 영향 받은 항목 위젯에서 맬웨어 방지 스캔 결과를 모니터링할 수 있습니다.

바이러스 백신 및 맬웨어 방지 기능 설정

바이러스 백신 및 맬웨어 방지 기능 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"을 참고하십시오.

바이러스 백신 및 맬웨어 방지 기능 모듈에 대해 다음 설정을 지정할 수 있습니다.

Active Protection

Active Protection은 랜덤웨어와 암호화폐 채굴 맬웨어로부터 시스템을 보호합니다. 랜섬웨어는 파일을 암호화하고 암호화 키에 대한 몸값을 요구합니다. 암호화폐 채굴 맬웨어는 백그라운드에서 수학 계산을 실행하면서 프로세싱 파워와 네트워크 트래픽을 훔칩니다.

Acronis Cyber Protect의 Cyber Backup 버전에서 Active Protection은 보호 계획 내 별도의 모듈입니다. 따라서 장치와 장치 그룹마다 다르게 구성하고 적용할 수 있습니다. Acronis Cyber Protect의 Protect 버전에서 Active Protection은 안티바이러스 및 맬웨어 방지 기능 모듈의 일부입니다.

Active Protection은 다음 운영 체제를 실행 중인 머신에서 사용할 수 있습니다.

- 데스크톱 운영 체제: Windows 7 서비스 팩 1 이상 버전

  Windows 7을 실행하는 머신에서 Windows 7용 업데이트(KB2533623)가 설치되어 있는지 확인합니다.
- 서버 운영 체제: Windows Server 2008 R2 이상

Agent for Windows가 머신에 설치되어 있어야 합니다.

작동법

Active Protection은 보호된 머신에서 실행 중인 프로세스를 모니터링합니다. 서드 파티 프로세스에서 파일 암호화 또는 암호화폐 채굴을 시도하면 Active Protection은 경보를 생성하고 구성에 지정된 추가 작업을 수행합니다.

또한, 로컬 폴더에 위치하는 소프트웨어 고유 프로세스, 레지스트리 기록, 실행 가능한 구성 파일, 백업의 무단 변경을 방지합니다.

악성 프로세스를 식별하기 위해 Active Protection에는 동작 추론이 사용됩니다. Active Protection은 프로세스에서 수행한 작업 체인을 악의적인 동작 패턴의 데이터베이스에 기록된 이벤트 체인과 비교합니다. 이 방법을 사용하면 Active Protection이 일반적인 동작에 따라 새로운 맬웨어를 탐지할 수 있습니다.

기본 설정: **활성화됨**.

Active Protection 설정

감지에 대한 작업에서 랜섬웨어를 감지할 때 소프트웨어에서 수행할 작업을 선택하고 **완료**를 클릭합니다.

다음 중 하나를 선택합니다.

- **알리기만 함**
  소프트웨어에서 프로세스에 대한 경보를 생성합니다.
- **프로세스 중지**
  소프트웨어에서 경보를 생성하고 프로세스를 중지합니다.
- **캐시를 사용해 되돌림**
  소프트웨어에서 경보를 생성하고 프로세스를 중지하고 서비스 캐시를 사용해 파일 변경 사항을 되돌립니다.

기본 설정: **캐시를 사용해 되돌림**.

네트워크 폴더 보호

로컬 드라이브로 매핑된 네트워크 폴더 보호 옵션은 로컬 악성 프로세스에서 바이러스 백신 및 맬웨어 방지 기능이 로컬 드라이브로 매핑된 네트워크 폴더를 보호하는지 정의합니다.

이 옵션은 SMB나 NFS 프로토콜을 통해 공유된 폴더에 적용됩니다.

파일이 원래 매핑된 드라이브에 위치할 경우에는 **캐시를 사용하여 되돌리기** 작업을 통해 캐시에서 추출할 때 원래 위치에 저장할 수 없습니다. 그 대신 파일은 이 옵션의 설정에 지정되는 폴더에 저장됩니다. 기본 폴더는 **C:\ProgramData\Acronis\Restored Network Files**입니다.이 폴더가 없는 경우에는 새로 생성됩니다. 이 경로의 변경을 원할 경우에는 로컬 폴더를 지정해야 합니다. 매핑된 드라이브의 폴더를 포함하여 네트워크 폴더는 지원되지 않습니다.

기본 설정: **활성화됨**.

서버측 보호

이 옵션은 위협을 가져올 가능성이 있는 네트워크의 다른 서버에서 들어오는 외부 연결로 공유된 네트워크 폴더를 바이러스 백신 및 맬웨어 방지 기능이 보호하는지 정의합니다.

기본 설정: **비활성화됨**.

신뢰하는 연결 및 차단된 연결 설정

신뢰함 탭에서 어떤 데이터든 수정하도록 허용할 연결을 지정할 수 있습니다. 사용자 이름과 IP 주소를 정의해야 합니다.

차단됨 탭에서 어떤 데이터도 수정하지 못하도록 차단할 연결을 지정할 수 있습니다. 사용자 이름과 IP 주소를 정의해야 합니다.

자체 보호

자체 보호는 로컬 폴더에 있는 소프트웨어 고유 프로세스, 레지스트리 기록, 실행 파일과 구성 파일, Secure Zone 및 백업의 무단 변경을 방지합니다. 이 기능을 비활성화하지 않는 것이 좋습니다.

기본 설정: **활성화됨**.

프로세스가 백업을 수정할 수 있도록 허용

특정 프로세스가 백업을 수정할 수 있도록 허용 옵션은 **자체 보호**가 활성화되어 있을 때 유효합니다.

확장자가 .tibx, .tib, .tia이고 로컬 폴더에 위치한 파일에 적용됩니다.

이 옵션을 이용하면 백업 파일이 자체 보호로 보호되더라도 백업 파일을 수정할 수 있습니다. 예를 들면 이 옵션은 스크립트를 사용하여 백업 파일을 제거하거나 다른 위치로 이동할 때 유용합니다.

이 옵션을 비활성화할 경우, 백업 파일은 백업 소프트웨어 벤더가 서명하는 프로세스로만 수정할 수 있습니다. 이 상태에서 소프트웨어는 사용자가 웹 인터페이스에서 이를 요청할 때 보관 규칙을 적용하고 백업을 삭제할 수 있습니다. 다른 프로세스는 아무리 의심스러워도 백업을 수정할 수 없습니다.

이 옵션을 활성화할 경우, 다른 프로세스에 백업을 수정하도록 허용할 수 있습니다. 드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다.

기본 설정: **비활성화됨**.

크립토마이닝 프로세스 감지됨

이 옵션은 바이러스 백신 및 맬웨어 방지 기능으로 잠재적인 크립토마이닝 맬웨어를 감지할지 여부를 정의합니다.

암호화폐 채굴 맬웨어는 유용한 애플리케이션의 성능을 저하시키고, 전기세를 증가시키고, 남용으로 인한 시스템 크래시 및 하드웨어 손상을 발생시킵니다. 크립토마이닝 맬웨어를 **해로운** 프로세스 목록에 추가해 실행을 방지하는 것이 좋습니다.

기본 설정: **활성화됨**.

크립토마이닝 프로세스 감지 설정

크립토마이닝 활동이 감지되었을 때 소프트웨어에서 수행할 작업을 선택하고 **완료**를 클릭합니다. 다음 중 하나를 선택합니다.

- **알리기만 함**
  소프트웨어가 크립토마이닝 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
- **프로세스 중지**
  소프트웨어가 크립토마이닝 활동이 의심되는 프로세스에 대해 경보를 생성하고 프로세스를 중지합니다.

기본 설정: **프로세스 중지**.

격리

격리는 감염 가능성이 있는 의심스러운 파일 또는 잠재적으로 위험한 파일을 격리하는 폴더입니다.

다음 후에 격리된 파일을 제거 – 격리된 파일을 제거하기까지 며칠을 보관할지 정의합니다.

기본 설정: **30일**.

동작 감지

Acronis Cyber Protect에서는 악의적인 프로세스를 식별하기 위해 행동 휴리스틱을 사용하여 시스템을 보호하며 프로세스에서 수행한 작업 체인을 악의적인 동작 패턴의 데이터베이스에 기록된 작업 체인과 비교합니다. 따라서 새로운 맬웨어는 그 전형적인 동작으로 감지할 수 있습니다.

기본 설정: **활성화됨**.

동작 감지 설정

감지에 대한 작업에서 맬웨어를 감지할 때 소프트웨어에서 수행할 작업을 선택하고 **완료**를 클릭합니다.

다음 중 하나를 선택합니다.

- **알리기만 함**
  소프트웨어가 맬웨어 활동이 의심되는 프로세스에 대해 경보를 생성합니다.
- **프로세스 중지**
  소프트웨어가 맬웨어 활동이 의심되는 프로세스에 대해 경보를 생성하고 프로세스를 중지합니다.
- **격리**
  소프트웨어가 경보를 생성하고, 프로세스를 중지하고, 실행 파일을 격리 폴더로 이동합니다.

기본 설정: **격리**.

실시간 보호

실시간 보호는 시스템이 켜져 있는 동안 지속적으로 머신 시스템의 바이러스 및 기타 위협을 검사합니다.

기본 설정: **활성화됨**.

실시간 보호의 감지 시 작업 구성

감지에 대한 작업에서 바이러스나 기타 맬웨어 위협이 감지되었을 때 소프트웨어에서 수행할 작업을 선택하고 **완료**를 클릭합니다.

다음 중 하나를 선택합니다.

- **차단 및 알림**
  소프트웨어가 맬웨어 활동이 의심되는 프로세스를 차단하고 경보를 생성합니다.

- **격리**
  소프트웨어가 경보를 생성하고, 프로세스를 중지하고, 실행 파일을 격리 폴더로 이동합니다.

기본 설정: **격리**.

실시간 보호의 스캔 모드 구성

스캔 모드에서 바이러스나 기타 맬웨어 위협이 감지되었을 때 소프트웨어에서 수행할 작업을 선택하고 **완료**를 클릭합니다.

다음 중 하나를 선택합니다.

- **스마트 온액세스** – 모든 시스템 활동을 모니터링하면서 읽기 또는 쓰기를 위한 액세스가 발생할 경우 또는 프로그램이 실행될 경우 자동으로 파일을 스캔합니다.
- **온엑시큐션** – 실행 파일에 대해서만 실행 시 자동으로 스캔하여 파일에 문제가 없으며 컴퓨터 또는 데이터에 손상을 야기하지 않는지 확인합니다.

기본 설정: **스마트 온액세스**.

스캔 예약

스캔 예약 설정을 활성화하여 맬웨어를 확인할 머신에 따라 스케줄을 정의할 수 있습니다.

감지에 대한 작업:

- **격리**
  소프트웨어가 경보를 생성하고 실행 파일을 격리 폴더로 이동합니다.
- **알리기만 함**
  소프트웨어가 맬웨어가 의심되는 프로세스에 대해 경보를 생성합니다.

기본 설정: **격리**.

스캔 유형:

- **전체**
  전체 스캔은 모든 파일을 확인하므로 빠른 스캔에 비해 완료되기까지 훨씬 많은 시간이 걸립니다.
- **빠른 스캔**
  빠른 스캔은 일반적으로 머신에 맬웨어가 위치하는 영역만 스캔합니다.
- **사용자 정의**
  사용자 정의 스캔은 관리자가 보호 계획에서 선택한 파일/폴더를 확인합니다.

하나의 보호 계획에 **빠른 스캔**, **전체**, **사용자 정의** 스캔 세 가지를 모두 예약할 수 있습니다.

기본 설정:

- **신속한 전체** 스캔이 예약됩니다.
- **사용자 정의** 스캔은 기본적으로 비활성화됩니다.

다음 이벤트를 사용해 작업 실행 예약:

- **시간 기준 예약** – 지정 시간에 따라 작업을 실행합니다.
- **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.
- **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

참고
작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다.

- **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다.
- **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.

기본 설정: **시간 기준 예약**.

예약 유형:

- **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다.
- **일일** – 작업을 실행할 요일을 선택합니다.
- **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.

기본 설정: **일일**.

시작 시간 – 작업을 실행할 정확한 시간을 선택합니다.

날짜 범위 내에 실행 – 구성된 예약이 실행될 기간의 범위를 설정합니다.

시작 조건 – 작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다.

맬웨어 방지 스캔용 시작 조건은 "시작 조건"(222페이지)에 설명되어 있는 백업 모듈용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다.

- **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다.
- **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행**
- **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다.
- **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다.

새 파일 및 변경된 파일만 스캔 – 새로 생성되었거나 수정된 파일만 스캔됩니다.

기본 설정: **활성화됨**.

전체 스캔을 예약할 때는 두 가지 추가 옵션이 있습니다.

- **아카이브 파일 스캔**
  기본 설정: **활성화됨**.

- **최대 재귀 깊이**
  스캔할 임베디드된 아카이브의 수준입니다. 예: MIME 문서 > ZIP 아카이브 > Office 아카이브 > 문서 콘텐츠
  기본 설정: **16**.
- **최대 크기**
  스캔할 아카이브 파일의 최대 크기입니다.
  기본 설정: **무제한**.

- **이동식 드라이브 스캔**
  기본 설정: **비활성화됨**.
  - **매핑된 (원격) 네트워크 드라이브**
  - **USB 스토리지 장치**(예: 플래시 드라이브 및 외장 하드 드라이브)
  - **CD/DVD**

제외

추정 분석에 사용되는 리소스를 최소화하고 가양성을 제거하려면 신뢰할 수 있는 프로그램이 랜섬웨어로 간주할 경우 다음 설정을 정의합니다.

신뢰함 탭에서 지정할 수 있는 부분은 다음과 같습니다.

- 절대 맬웨어로 간주되지 않을 프로세스. Microsoft에서 서명한 프로세스는 항상 신뢰됩니다.
- 파일 변경이 모니터링되지 않을 폴더.
- 예약된 스캔이 수행되지 않을 파일 및 폴더.

차단됨 탭에서 지정할 수 있는 부분은 다음과 같습니다.

- 언제나 차단할 프로세스. Active Protection이 머신에서 활성화되어 있는 한 이 프로세스는 시작될 수 없습니다.
- 어떤 프로세스든 차단되는 폴더입니다.

드라이브 문자로 시작하는 프로세스 실행 파일의 전체 경로를 지정합니다. 예:
`C:\Windows\Temp\er76s7sdkh.exe`.

폴더를 지정하는 데는 와일드카드 문자 * 및 ?를 사용할 수 있습니다. 별표(*)는 0개 이상의 문자를 대체합니다. 물음표(?)는 정확히 하나의 문자를 대체합니다. `%AppData%` 등의 환경 변수는 사용할 수 없습니다.

기본 설정: 기본적으로 제외가 정의되어 있지 않습니다.

URL 필터링

자세한 내용은 URL 필터링을 참조하십시오.

Active Protection

Acronis Cyber Protect의 Cyber Backup 버전에서 Active Protection은 보호 계획 내 별도의 모듈입니다. 이 모듈에는 다음 설정이 있습니다.

- 감지에 대한 작업
- 자체 보호
- 네트워크 폴더 보호
- 서버측 보호
- 크립토마이닝 프로세스 감지됨
- 제외

Acronis Cyber Protect의 Protect 버전에서 Active Protection은 안티바이러스 및 맬웨어 방지 기능 모듈의 일부입니다.

Active Protection은 다음 운영 체제를 실행 중인 머신에서 사용할 수 있습니다.

- 데스크톱 운영 체제: Windows 7 서비스 팩 1 이상 버전
  Windows 7을 실행하는 머신에서 Windows 7용 업데이트(KB2533623)가 설치되어 있는지 확인합니다.
- 서버 운영 체제: Windows Server 2008 R2 이상

Agent for Windows가 머신에 설치되어 있어야 합니다.

Active Protection 및 해당 설정에 대해 자세히 알아보려면 "바이러스 백신 및 맬웨어 방지 기능 설정"(470페이지)을(를) 참조하십시오.

Windows Defender 바이러스 백신

Windows Defender 안티바이러스는 Windows 8부터 제공된 Microsoft Windows의 기본 맬웨어 방지 컴퍼넌트입니다.

Windows Defender 안티바이러스 모듈을 사용하면 Windows Defender 안티바이러스 보안 정책을 구성하고 Cyber Protect 웹 콘솔을 통해 상태를 추적할 수 있습니다.

이 모듈은 Windows Defender 바이러스 백신이 설치된 머신에 대해 적용 가능합니다.

스캔 예약

예약된 스캔의 스케줄을 지정합니다.

스캔 모드:

- **전체** – 빠른 스캔으로 스캔되는 항목을 비롯한 모든 파일과 폴더를 전체 검사합니다. 빠른 스캔에 비해 더 많은 머신 리소스가 필요합니다.
- **빠른 스캔** – 일반적으로 맬웨어가 발견되는 메모리 내 프로세스와 폴더를 빠르게 검사합니다. 머신 리소스를 적게 사용합니다.

스캔이 실행될 시간과 요일을 정의합니다.

일일 빠른 스캔 – 매일 빠른 스캔을 수행할 시간을 정의합니다.

필요에 따라 다음 옵션을 설정할 수 있습니다.

머신이 켜져 있지만 사용 중이 아닐 때 예약된 스캔을 시작

예약된 스캔을 실행하기 전에 최신 바이러스 및 스파이웨어 정의를 확인합니다

스캔 중 CPU 사용을 다음으로 제한

Windows Defender 바이러스 백신 예약 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#scheduled-scans-settings를 참고하십시오.

기본 작업

다양한 보안 수준의 감지된 위협에 대해 수행할 기본 작업을 정의합니다.

- **정리** – 머신에서 감지된 맬웨어를 정리합니다.
- **격리** – 감지된 맬웨어를 격리 폴더로 이동하지만 제거하지는 않습니다.
- **제거** – 머신에서 감지된 맬웨어를 제거합니다.
- **허용** – 감지된 맬웨어를 제거하거나 격리하지 않습니다.
- **사용자 정의** – 감지된 맬웨어에 대해 수행할 작업을 지정해 달라는 메시지가 표시됩니다.
- **작업 없음** – 아무런 작업도 수행하지 않습니다.
- **차단** – 감지된 맬에어를 차단합니다.

Windows Defender 바이러스 백신 기본 작업 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#default-actions-settings를 참고하십시오.

실시간 보호

실시간 보호를 활성화해 맬웨어를 감지하고 머신에서 설치 또는 실행되지 않도록 방지합니다.

모든 다운로드 스캔 – 이 옵션을 선택한 경우 다운로드된 모든 파일과 첨부 파일을 스캔합니다.

행동 모니터링 활성화 – 이 옵션을 선택한 경우 행동 모니터링이 활성화됩니다.

네트워크 파일 스캔 – 이 옵션을 선택한 경우 네트워크 파일이 스캔됩니다.

매핑된 네트워크 드라이브에서 전체 스캔 허용 – 이 옵션을 선택한 경우 매핑된 네트워크 드라이브 전체가 스캔됩니다.

이메일 스캔 허용 – 활성화된 경우 메일 본문과 첨부 파일을 분석하기 위해 엔진이 사서함과 메일 파일을 특정 형식에 따라 구문 분석합니다.

Windows Defender 바이러스 백신 실시간 보호 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#real-time-protection-settings를 참고하십시오.

Advanced

고급 스캔 설정 지정:

- **아카이브 파일 스캔** – .zip 또는 .rar 파일과 같은 아카이브 파일을 스캔에 포함합니다.
- **이동식 드라이브 스캔** – 전체 스캔 중 이동식 드라이브를 스캔합니다.

- **시스템 복원 지점 생성** – 중요 파일 또는 레지스트리 항목을 "감지 오류"로 제거할 수 없는 경우 복원 지점에서 복구할 수 있습니다.
- **다음 후에 격리된 파일을 제거** – 격리된 파일을 제거하기까지 보관할 기간을 정의합니다.
- **추가 분석이 필요할 경우 자동으로 파일 샘플 전송:**
  - **항상 메시지 표시** – 파일을 전송하기 전 확인 메시지가 표시됩니다.
  - **자동으로 안전한 샘플 전송** – 개인 정보를 포함할 가능성이 있는 파일을 제외하고 대부분의 경우 자동으로 샘플이 전송됩니다. 개인 정보를 포함할 가능성이 있는 파일의 경우 추가 확인이 필요합니다.
  - **자동으로 모든 샘플 전송** – 모든 샘플이 자동으로 전송됩니다.
- **Windows Defender 바이러스 백신 GUI 비활성화** – 이 옵션을 선택한 경우 사용자는 Windows Defender 바이러스 백신 사용자 인터페이스를 사용할 수 없습니다. Cyber Protect 웹 콘솔을 통해 Windows Defender 안티바이러스 정책을 관리할 수 있습니다.
- **MAPS(Microsoft Active Protection Service)** – 잠재적 위협에 대해 어떤 대응을 선택할지 지원하는 온라인 커뮤니티입니다.
  - **MAPS에 참여하지 않겠습니다** – 감지된 소프트웨어에 대한 그 어떤 정보도 Microsoft에 전송하지 않습니다.
  - **기본 구성원 자격** – 감지된 소프트웨어에 대한 기본 정보만 Microsoft에 전송합니다.
  - **고급 구성원 자격** – 감지된 소프트웨어에 대한 보다 상세한 정보를 Microsoft에 전송합니다.

  자세한 내용은 https://www.microsoft.com/security/blog/2015/01/14/maps-in-the-cloud-how-can-it-help-your-enterprise를 참고하십시오.

Windows Defender 바이러스 백신 고급 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#advanced-settings를 참고하십시오.

제외

다음과 같이 스캔에서 제외될 파일과 폴더를 정의할 수 있습니다.

- **프로세스** – 여기에서 정의한 프로세스가 읽거나 쓰는 모든 파일이 스캔에서 제외됩니다. 프로세스의 실행 파일에 대한 전체 경로를 정의해야 합니다.
- **파일 및 폴더** – 지정한 파일과 폴더가 스캔에서 제외됩니다. 폴더 또는 파일에 대한 전체 경로나 파일 확장자를 정의해야 합니다.

Windows Defender 바이러스 백신 제외 설정에 대한 자세한 내용은 https://docs.microsoft.com/en-us/sccm/protect/deploy-use/endpoint-antimalware-policies#exclusion-settings를 참고하십시오.

Microsoft Security Essentials

Microsoft Security Essentials는 Windows 8 이전 버전에서 제공된 Microsoft Windows의 기본 맬웨어 방지 컴퍼넌트입니다.

Microsoft Security Essentials 모듈을 사용하면 Microsoft Security Essentials 보안 정책을 구성하고 Cyber Protect 웹 콘솔을 통해 상태를 추적할 수 있습니다.

이 모듈은 Microsoft Security Essentials가 설치된 머신에 대해 적용 가능합니다.

Microsoft Security Essentials 설정은 Microsoft Windows Defender 안티바이러스와 거의 유사하지만 실시간 보호 설정이 없으며 Cyber Protect 웹 콘솔을 통한 제외 항목도 정의할 수 없습니다.

URL 필터링

맬웨어는 악성 또는 감염된 사이트에서 배포되는 경우가 많으며 드라이브 바이 다운로드라는 감염 방법을 사용합니다. URL 필터링은 인터넷의 맬웨어와 피싱 같은 위협에서 머신을 보호합니다. 사용자가 악성 콘텐츠를 포함할 가능성이 있는 웹사이트에 액세스하지 못하도록 차단할 수 있습니다.

또 이 URL 필터링으로 외부 규정 및 회사 내부 정책을 준수하기 위해 웹을 사용하도록 제어할 수 있습니다. 40개 이상의 웹 사이트 카테고리에 대해 서로 다른 액세스 정책을 구성할 수 있습니다.

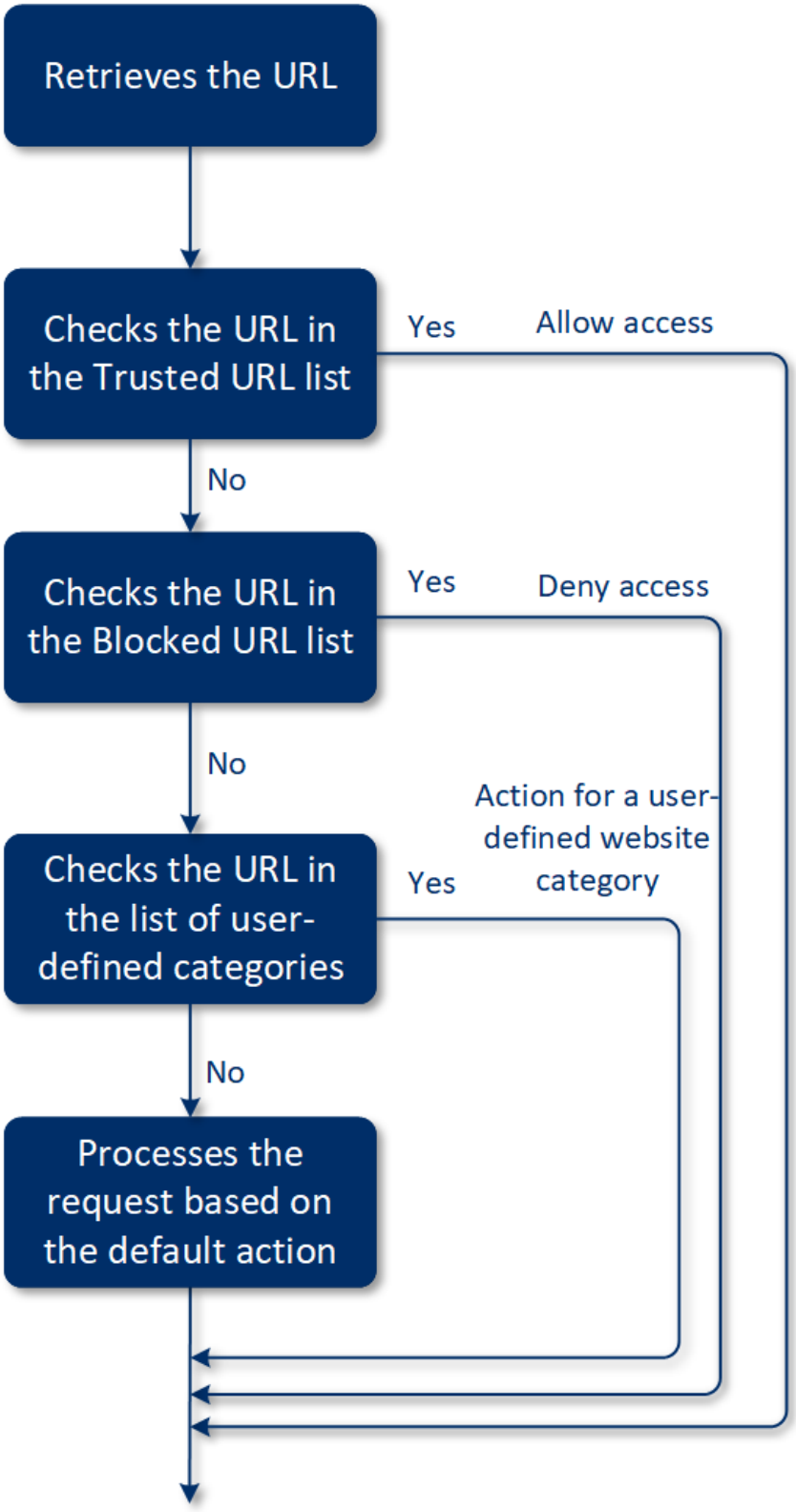
현재 보호 에이전트는 Windows 머신의 HTTP와 HTTPS 연결을 검사합니다.

URL 필터링 기능을 사용하려면 기능이 인터넷에 연결할 수 있어야 합니다.

참고
URL 필터링 기능을 사용하는 타사 안티바이러스 솔루션과 URL 필터링을 함께 사용하면 충돌이 발생할 수도 있습니다. 설치되어 있는 다른 안티바이러스 솔루션의 상태는 Windows 보안 센터를 통해 확인할 수 있습니다.
호환성 또는 성능 문제가 발생하면 타사 솔루션을 제거하거나 보호 계획에서 URL 필터링 모듈을 비활성화하십시오.

작동법

사용자가 링크를 누르거나 브라우저의 주소 표시줄에 URL을 입력합니다. 인터셉터가 URL을 가져와 보호 에이전트로 전송합니다. 보호 에이전트는 URL을 분석하고 데이터베이스를 확인한 다음 의견을 인터셉터에 전달합니다. URL이 금지된 경우, 인터셉터는 액세스를 차단한 뒤 사용자에게 이 콘텐츠를 볼 수 없다고 알립니다.



URL 필터링 구성 방법

1. URL 필터링 모듈이 활성화된 보호 계획을 생성합니다.
2. URL 필터링 설정을 구성합니다 (아래 참고).
3. 원하는 머신에 보호 계획을 할당합니다.

차단된 URL을 확인하려면 **대시보드** > **경보**로 이동합니다.

URL 필터링 설정

URL 필터링 모듈에 대해 다음 설정을 구성할 수 있습니다.

악성 웹사이트 액세스

사용자가 악성 웹사이트 접속을 시도할 경우 수행할 작업을 지정합니다.

- **차단** – 악성 웹 사이트에 대한 액세스가 차단되고 경고가 생성됩니다.
- **항상 사용자에게 묻기** – 사용자에게 웹사이트로 계속 접속할지 아니면 다시 돌아갈지를 묻습니다.

필터링할 카테고리

다음과 같이 액세스 정책을 구성할 수 있는 44개의 웹사이트 카테고리가 있습니다. 기본적으로 모든 범주의 웹 사이트에 대한 액세스가 허용됩니다.

	웹사이트 카테고리	설명
1	**광고**	이 카테고리에는 주 목적이 광고인 도메인이 포함됩니다.
2	**메시지 게시판**	이 카테고리에는 포럼, 토론 게시판, 질의 응답형 웹사이트가 포함됩니다. 이 카테고리에 고객이 질문을 게시하는 기업 웹 사이트의 특정 섹션은 포함되지 않습니다.
3	**개인용 웹사이트**	이 카테고리에는 개인 웹사이트와 모든 유형의 블로그(개인, 그룹, 회사 블로그 등)가 포함됩니다. '블로그'란 WWW(World Wide Web)에 게시된 저널입니다. 게시글('포스팅')로 이루어져 있으며, 일반적으로 가장 최근 포스팅이 가장 먼저 보이도록 역순으로 배열됩니다.
4	**기업/비즈니스 웹사이트**	이 카테고리는 보통 다른 어떤 카테고리에도 속하지 않는 기업 웹사이트가 포함되는 광범위한 카테고리입니다.
5	**컴퓨터 소프트웨어**	이 카테고리에는 보통 오픈 소스, 프리웨어 또는 쉐어웨어 같은 컴퓨터 소프트웨어를 제공하는 웹사이트가 포함됩니다. 일부 온라인 소프트웨어 스토어도 포함될 수 있습니다.
6	**의약품**	이 카테고리에는 의약품/주류/담배와 관련되어 (합법) 의약용품, 주류, 담배 제품의 사용이나 판매에 관해 토론하는 웹사이트가 포함됩니다. 불법 약물은 마약 카테고리에 포함됩니다.
7	**교육**	이 카테고리에는 .edu 도메인 이외의 웹사이트까지 포함하여 공식 교육 기관이 소유한 웹사이트가 포함됩니다. 백과사전과 같은 교육적인 웹사이트도 포함됩니다.

8	**엔터테인먼트**	이 카테고리에는 예술 활동 및 박물관에 관한 정보를 제공하는 웹사이트와 영화, 음악, 미술 등의 콘텐츠를 리뷰하거나 평가하는 웹사이트가 포함됩니다.
9	**파일 공유**	이 카테고리에는 사용자가 파일을 업로드하고 다른 사람과 공유할 수 있는 파일 공유 웹사이트가 포함됩니다. 토렌트 공유 웹사이트 및 토렌트 트래커도 포함됩니다.
10	**금융**	이 카테고리에는 온라인 액세스를 제공하는 전 세계 모든 은행의 웹사이트가 포함됩니다. 일부 신용 조합과 기타 금융 기관도 포함됩니다. 그러나 일부 지방 은행은 포함되지 않을 수 있습니다.
11	**도박**	이 카테고리에는 도박 웹사이트가 포함됩니다. 이는 일반적으로 사용자가 온라인 룰렛, 포커, 블랙잭 등의 게임에 돈을 걸기 전에 결제를 해야 하는 '온라인 카지노' 또는 '온라인 복권' 유형의 웹사이트를 의미합니다. 이런 웹사이트 중 일부는 합법적이고 이길 확률도 있지만, 일부는 사기 행위이며, 이길 확률이 없음을 의미합니다. 이 외에 도박 및 온라인 복권 웹사이트에서 이익을 얻는 방법을 알려주는 '이기는 팁과 치트' 웹사이트까지 감지합니다.
12	**게임**	이 카테고리에는 보통 Adobe Flash 또는 JAVA 애플릿 기반의 온라인 게임 웹사이트가 포함됩니다. 게임이 무료인지, 구독을 필요로 하는지의 여부는 웹사이트 감지에 영향을 주지 않지만, 카지노 식 웹 사이트는 도박 카테고리로 감지됩니다. 이 카테고리에는 다음이 포함되지 않습니다. • 비디오 게임을 개발하는 기업의 공식 웹사이트(온라인 게임을 제작하는 경우 제외) • 게임을 논의하는 토론 웹사이트 • 비온라인 게임을 다운로드할 수 있는 웹 사이트(일부는 불법 카테고리에 포함) • World of Warcraft와 같이 사용자가 실행 파일을 다운로드하고 실행해야 하는 게임(이런 유형은 방화벽 등의 다른 수단에 의해 차단될 수 있음)
13	**정부**	이 카테고리에는 정부 기관, 대사관, 사무소 웹사이트 등의 정부 웹사이트가 포함됩니다.
14	**해킹**	이 카테고리에는 해커들을 위한 해킹 도구, 문서, 토론 플랫폼을 제공하는 웹사이트가 포함됩니다. 일반적인 플랫폼에 대한 악용 수단을 제공해 Facebook 또는 Gmail 계정 해킹을 용이하게 하는 웹사이트도 포함됩니다.
15	**불법 활동**	이 카테고리는 혐오, 폭력, 인종차별과 관련된 광범위한 카테고리이며, 다음 카테고리의 웹사이트를 차단하려는 목적을 가지고 있습니다. • 테러리스트 조직이 소유한 웹사이트 • 인종차별 또는 외국인 혐오적인 콘텐츠가 포함된 웹사이트 • 격렬한 스포츠를 논의하고/논의하거나 폭력을 조장하는 웹사이트
16	**건강 및 피트니스**	이 카테고리에는 의료기관 웹사이트, 질병 예방 및 치료 관련 웹사이트, 체중 감량, 다이어트, 스테로이드, 아나볼릭 또는 HGH 제품 관련 정보나 제품을 제공하는 웹사이트 및 성형 수술 관련 정보를 제공하는 웹사이트가 포함됩니다.
17	**취미**	이 카테고리에는 수집, 예술 및 공예, 자전거 타기 등 보통 개인의 여가 시간에 이루어지는 활동과 관련한 자료를 제공하는 웹사이트가 포함됩니다.
18	**웹 호스팅**	이 카테고리에는 개인 사용자와 조직이 웹페이지를 만들어 공개할 수 있도록 지원하는 무료 및 상용 웹사이트 호스팅 서비스가 포함됩니다.

19	**불법 다운로드**	이 카테고리에는 소프트웨어 프라이버시와 관련된 다음 웹사이트가 포함됩니다. • 저작권자의 동의 없이 저작권이 있는 콘텐츠를 배포하는 데 일조하는 것으로 알려진 P2P(BitTorrent, emule, DC++) 트래커 웹사이트 • Warez(해적판 상업용 소프트웨어) 웹사이트 및 토론 게시판 • 사용자에게 크랙, 키 생성기, 시리얼 번호를 제공해 불법적인 소프트웨어 사용을 조장하는 웹 사이트 이중 일부 웹 사이트는 포르노 또는 주류 광고를 사용해 이익을 창출하기 때문에 포르노 또는 주류/담배로도 감지될 수 있습니다.
20	**인스턴트 메시징**	이 카테고리에는 실시간 채팅 서비스를 제공하는 인스턴트 메시징 및 채팅 웹사이트가 포함됩니다. 이 외에도 임베디드 인스턴트 메신저 서비스가 있는 yahoo.com 및 gmail.com도 감지할 것입니다.
21	**구직/구인**	이 카테고리에는 구직 게시판, 구직 관련 광고, 커리어 기회를 제공하는 웹사이트와 이러한 서비스를 종합하여 제공하는 웹사이트가 포함됩니다. 채용 기관 웹사이트 또는 일반 기업의 '채용' 페이지는 포함되지 않습니다.
22	**성인 콘텐츠**	이 카테고리에는 웹사이트 제작자가 성인용이라고 명시한 콘텐츠가 포함됩니다. 카마 수트라 책 및 성교육 웹사이트부터 노골적인 포르노까지 넓은 범위의 웹사이트를 감지합니다.
23	**마약**	이 카테고리에는 오락용 불법 약물에 관한 정보를 공유하는 웹사이트가 포함됩니다. 이 카테고리에는 마약 재배 및 개발과 관련된 웹사이트도 포함됩니다.
24	**뉴스**	이 카테고리에는 텍스트 및 동영상 뉴스를 제공하는 뉴스 웹사이트가 포함됩니다. 세계 및 지역 뉴스 웹사이트를 모두 포함하기 위해 노력합니다. 그러나 일부 소규모 지역 뉴스 웹사이트는 포함되지 않을 수 있습니다.
25	**온라인 데이트**	이 카테고리에는 사용자가 몇 가지 조건을 기준으로 다른 사람을 검색해 볼 수 있는 유료 및 무료 온라인 데이트 웹사이트가 포함됩니다. 사용자는 프로필을 게시해 다른 사람이 검색하도록 할 수 있습니다. 이 카테고리에는 유무료 온라인 데이트 웹사이트가 모두 포함됩니다. 대부분의 유명 소셜 네트워크가 온라인 데이트 웹사이트로 사용될 수 있기 때문에, Facebook과 같은 일부 인기 웹사이트도 이 카테고리에 감지됩니다. 이 카테고리를 소셜 네트워크 카테고리와 함께 사용할 것을 권장합니다.
26	**온라인 결제**	이 카테고리에는 온라인 결제 또는 자금 이체 서비스를 제공하는 웹사이트가 포함됩니다. PayPal 또는 Moneybookers와 같은 인기 결제 웹사이트를 감지합니다. 또, 이 카테고리는 일반 웹사이트 중 신용 카드 정보를 요청하는 페이지를 스스로 감지해 숨겨지거나 알려지지 않거나 불법적인 온라인 스토어를 감지합니다.
27	**사진 공유**	이 카테고리에는 주 목적이 사진 업로드 및 공유인 사진 공유 웹사이트가 포함됩니다.
28	**온라인 스토어**	이 카테고리에는 알려진 온라인 스토어가 포함됩니다. 상품이나 서비스를 온라인으로 판매하는 웹사이트는 온라인 스토어로 간주됩니다.
29	**포르노**	이 카테고리에는 성적 콘텐츠와 포르노를 다루는 웹사이트가 포함됩니다. 유료 및 무료 웹사이트가 모두 포함됩니다. 사진, 이야기, 동영상을 제공하는 웹사이트가 포함되

		고, 여러 종류의 콘텐츠를 담고 있는 웹사이트에 포함된 포르노 콘텐츠도 감지합니다.
30	**포털**	이 카테고리에는 여러 출처 및 다양한 도메인에서 정보를 수집하고, 보통 검색 엔진, 이메일, 뉴스, 엔터테인먼트 정보 등의 기능을 제공하는 웹사이트가 포함됩니다.
31	**라디오**	이 카테고리에는 온라인 라디오 방송국부터 주문형(무료 또는 유료) 오디오 콘텐츠를 제공하는 웹사이트까지, 인터넷 음악 스트리밍 서비스를 제공하는 다양한 웹사이트가 포함됩니다.
32	**종교**	이 카테고리에는 종교 또는 종파를 홍보하는 웹사이트가 포함됩니다. 한 종교 또는 여러 종교에 관한 토론 포럼도 다룹니다.
33	**검색 엔진**	이 카테고리에는 Google, Yahoo, Bing 같은 검색 엔진 웹사이트가 포함됩니다.
34	**소셜 네트워크**	이 카테고리에는 MySpace.com, Facebook.com, Bebo.com 등의 소셜 네트워크 웹사이트가 포함됩니다. YouTube.com과 같은 특별한 유형의 소셜 네트워크는 비디오/사진 카테고리에 나열됩니다.
35	**스포츠**	이 카테고리에는 스포츠 정보, 뉴스, 튜토리얼을 제공하는 웹사이트가 포함됩니다.
36	**자살**	이 카테고리에는 자살을 홍보, 조장, 옹호하는 웹사이트가 포함됩니다. 자살 방지 클리닉은 포함되지 않습니다.
37	**타블로이드**	이 카테고리에는 보통 소프트 포르노 및 셀럽 가십 웹사이트가 포함됩니다. 상당수의 타블로이드 뉴스가 여기에 해당하는 하위 카테고리를 갖고 있을 수 있습니다. 또한,이 카테고리의 감지는 휴리스틱을 기반으로 합니다.
38	**시간 낭비**	이 카테고리에는 사람들이 많은 시간을 소비하게 되는 웹사이트가 포함됩니다. 여기에는 소셜 네트워크나 엔터테인먼트와 같은 다른 카테고리의 웹사이트도 포함될 수 있습니다.
39	**여행**	이 카테고리에는 여행 상품과 여행 장비, 여행지 소개와 평가 등의 정보를 제공하는 웹사이트가 포함됩니다.
40	**비디오**	이 카테고리에는 사용자가 업로드하거나 다양한 콘텐츠 제공업체가 제공하는 동영상과 사진을 호스팅하는 웹사이트가 포함됩니다. 여기에는 YouTube, Metacafe, Google Video와 같은 웹사이트 및 Picasa나 Flickr와 같은 사진 웹사이트가 포함됩니다. 또한, 다른 웹사이트나 블로그에 포함된 비디오도 감지합니다.
41	**폭력적인 만화**	이 카테고리에는 폭력성, 외설적 언어, 성적 콘텐츠가 담겨 있어 미성년자에게 부적절한 폭력적인 만화나 애니메이션을 이야기하고, 공유하고, 제공하는 웹사이트가 포함됩니다. "톰과 제리"와 같은 대중적인 만화를 제공하는 웹사이트는 이 카테고리에 포함되지 않습니다.
42	**무기**	이 카테고리에는 판매 또는 교환, 제조, 사용을 목적으로 무기를 제공하는 웹사이트가 포함됩니다. 여기에는 사냥 도구, 공기총 및 BB총의 사용은 물론 근거리 무기도 포함됩니다.
43	**이메일**	이 카테고리에는 웹 응용 프로그램처럼 이메일 기능을 제공하는 웹사이트가 포함됩니다.

44	**웹 프록시**	이 카테고리에는 웹 프록시 서비스를 제공하는 웹사이트가 포함됩니다. 사용자가 웹 페이지를 열고 양식에 요청된 URL을 입력한 다음 "제출"을 클릭할 때 연결되는 "브라우저 내 브라우저" 유형의 웹사이트입니다. 웹 프록시 사이트는 실제 페이지를 다운로드한 다음 사용자 브라우저 내에 표시합니다. 이러한 유형을 감지하는 이유는 다음과 같습니다(또한 이런 이유로 차단이 필요할 수 있습니다). • 익명 브라우징. 대상 웹 서버가 프록시 웹 서버로부터 요청을 받으면 IP 주소만 표시되고, 서버 관리자가 사용자를 추적할 때 웹 프록시에서 추적이 끝나게 됩니다. 원래 사용자의 위치를 확인하는 데 필요한 로그가 남을 수도, 남지 않을 수도 있습니다. • 위치 스푸핑. 소스 위치에서 서비스 정보를 수집할 때 종종 사용자 IP 주소가 사용되며(일부 국내 정부 웹사이트는 로컬 IP 주소로만 이용할 수 있음), 사용자가 실제 위치를 기만하는 데 이러한 서비스가 이용될 수도 있습니다. • 금지되는 콘텐츠에 액세스. 간단한 URL 필터를 사용하는 경우에는 웹 프록시 URL만 확인할 수 있고 사용자가 방문하는 실제 서버는 확인하지 못합니다. • 회사의 모니터링 회피. 기업 정책상 직원의 인터넷 사용을 모니터링 해야 하는 경우가 있습니다. 웹 프록시를 통해 액세스하게 되면 사용자가 올바른 정보를 제공하지 않으며 모니터링에서 벗어날 수 있습니다. SDK는 URL만이 아니라 HTML 페이지(제공된 경우)도 분석하므로, 일부 카테고리의 경우 여전히 SDK가 콘텐츠를 감지할 수 있습니다. 하지만 SDK를 사용하는 것만으로 그 외의 경우에 해당하는 문제를 방지할 수는 없습니다.

차단된 URL에 대한 모든 알림을 카테고리별로 표시를 활성화하면, 차단된 URL에 대한 모든 알림이 카테고리별로 트레이에 표시됩니다. 웹사이트에 하위 도메인이 여러 개 있으면 시스템에서 그에 대한 알림 역시 생성하기 때문에 알림 수가 많을 수 있습니다.

제외

안전하다고 알려진 URL을 신뢰할 수 있는 URL 목록에 추가할 수 있습니다. 위협으로 표시되는 URL을 차단된 URL 목록에 추가할 수 있습니다.

URL을 목록에 추가하는 방법

1. 보호 계획의 URL 필터링 모듈에서 **제외**를 클릭합니다.
2. 원하는 목록을 선택합니다. **신뢰됨** 혹은 **차단됨**
3. **추가**를 클릭합니다.
4. URL 또는 IP 주소를 지정한 뒤, 확인 표시를 클릭합니다.

URL 제외의 예:

- xyz.com을 신뢰할 수 있는 URL 또는 신뢰할 수 없는 URL로 추가하면 xyz.com 도메인의 모든 주소가 추가 대상 위치에 따라 신뢰할 수 있는 URL 또는 신뢰할 수 없는 URL로 간주됩니다.
- 특정 하위 도메인을 추가하려는 경우 **mail.xyz.com**을 신뢰할 수 있는 URL 또는 신뢰할 수 없는 URL로 추가할 수 있습니다. 이 경우 모든 **xyz.com** 주소가 신뢰할 수 있는 주소나 신뢰할 수 없는 주소로 설정되지 않습니다.

- IPv4를 신뢰할 수 있는 주소나 신뢰할 수 없는 주소로 추가하려는 경우에는 **20.53.203.50**과 같은 형식을 사용해야 해당 주소가 유효한 항목으로 추가됩니다.
- 여러 URL 제외를 동시에 추가하려면 다음과 같이 각 항목을 새 줄에 추가해야 합니다.

  acronis.com

  mail.xyz.com

  20.53.203.50

격리

격리는 머신의 하드 디스크에 특별히 격리된 폴더로, 위협이 확산되지 않도록 바이러스 백신 및 맬웨어 방지 보호 기능이 의심스럽다고 감지한 파일이 위치하는 곳입니다.

격리를 통해 모든 머신에서 의심스럽거나 잠재적으로 위험한 파일을 검토하고 이러한 파일을 제거 또는 복원할지 선택할 수 있습니다. 격리된 파일은 머신이 시스템에서 제거되는 경우 자동으로 제거됩니다.

파일은 어떻게 격리 폴더로 이동합니까?

1. 보호 계획을 구성해 감염된 파일을 격리 폴더로 이동하기 위한 기본 작업을 정의합니다.
2. 시스템은 예약 또는 온액세스 스캔 도중 악성 파일을 감지하여 격리라는 보안 폴더로 이동합니다.
3. 시스템은 머신의 격리 목록을 업데이트합니다.
4. 파일은 보호 계획의 **다음 후의 격리된 파일을 제거** 설정에서 정의한 기간 후 격리 폴더에서 자동으로 정리됩니다.

격리된 파일 관리

격리된 파일을 관리하려면 **맬웨어 방지 기능** > **격리**로 이동합니다. 모든 머신에서 격리된 파일 목록을 확인할 수 있습니다.

이름	설명
파일	파일 이름입니다.
격리된 날짜	파일이 격리 폴더로 이동된 날짜와 시간입니다.
장치	감염된 파일이 발견된 장치입니다.
위협 이름	위협 이름.
보호 계획	의심스러운 파일을 격리 폴더에 보관한 보호 계획입니다.

격리된 파일에 가능한 작업은 2가지입니다.

- **삭제** – 모든 머신에서 격리된 파일을 영구적으로 제거합니다.
- **복원** – 아무 수정 없이 원래 위치로 격리된 파일을 복원합니다. 원래 위치에 동일한 이름의 파일이 존재하면 복원된 파일이 해당 파일을 덮어씁니다.

머신의 격리 위치

격리된 파일의 기본 위치는 다음과 같습니다.

Windows 머신: `%ProgramData%\%product_name%\Quarantine`

Mac/Linux 머신: `/usr/local/share/%product_name%/quarantine`

기업 허용 목록

중요
기업 허용 목록을 사용하려면 관리 서버에 검색 서비스가 설치되어 있어야 합니다.

안티바이러스 솔루션에서 합법적인 회사 관련 애플리케이션을 의심스러운 항목으로 식별할 수도 있습니다. 이러한 감지 오류를 방지하기 위해 신뢰할 수 있는 애플리케이션을 허용 목록에 수동으로 추가하는데, 이렇게 하려면 많은 시간이 소요됩니다.

Cyber Protect에서는 이 프로세스를 자동화할 수 있습니다. 즉, 안티바이러스 및 맬웨어 방지 모듈이 백업을 스캔한 후 스캔한 데이터가 분석되며, 이를 통해 신뢰할 수 있는 애플리케이션이 허용 목록으로 이동하고 감지 오류가 방지됩니다. 또한 전사적 허용 목록을 통해 스캔 성능이 추가로 개선됩니다.

허용 목록은 활성화 및 비활성화할 수 있습니다. 비활성화되어 있을 때는 허용 목록에 추가된 파일이 일시적으로 숨겨집니다.

허용 목록에 자동 추가

1. 최소 2개의 머신에서 백업의 클라우드 스캔을 실행합니다. 이렇게 하려면 "백업 스캔 계획"(320 페이지)을(를) 사용합니다.
2. 허용 목록 설정에서 **허용 목록 자동 생성** 스위치를 활성화합니다.

허용 목록에 수동 추가

허용 목록 자동 생성 스위치가 비활성화되어 있더라도 허용 목록에 파일을 수동으로 추가할 수 있습니다.

1. Cyber Protect 웹 콘솔에서 **맬웨어 방지 기능** > **허용 목록**으로 이동합니다.
2. **파일 추가**를 클릭합니다.
3. 파일 경로를 지정한 다음 **추가**를 클릭합니다.

허용 목록에 격리된 파일 추가

격리된 파일을 허용 목록에 추가할 수 있습니다.

1. Cyber Protect 웹 콘솔에서 **맬웨어 방지 기능** > **격리**로 이동합니다.
2. 격리된 파일을 선택한 다음 **허용 목록에 추가**를 클릭합니다.

허용 목록 설정

허용 목록 자동 생성 스위치를 활성화하는 경우 다음 휴리스틱 보호 수준 중 하나를 지정해야 합니다.

- **낮음**
  상당한 시간이 지나고 확인이 완료된 후에만 기업 애플리케이션을 허용 목록에 추가합니다. 이러한 애플리케이션은 신뢰도가 높습니다. 하지만 이 방식을 사용하면 감지 오류의 가능성이 커집니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 높습니다.
- **기본**
  잠재적인 감지 오류를 줄이기 위해 권장 보호 수준에 따라 기업 애플리케이션을 허용 목록에 추가합니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 중간 수준입니다.
- **높음**
  잠재적인 감지 오류를 줄이기 위해 더욱 빠르게 기업 애플리케이션을 화이트리스트에 추가합니다. 하지만 이 방식은 소프트웨어가 안전하다는 것을 보장하지 않으며 추후 소프트웨어가 의심스러운 소프트웨어나 맬웨어로 인식될 수도 있습니다. 안전하며 신뢰할 수 있는 파일이라고 판단하기까지의 기준이 낮습니다.

허용 목록의 항목 관련 상세 정보 확인

허용 목록의 항목을 클릭하면 해당 항목과 관련된 추가 정보를 확인하고 온라인에서 항목을 분석할 수 있습니다.

추가한 항목을 모르는 경우 VirtusTotal 분석기에서 항목을 확인할 수 있습니다. **VirusTotal에서 확인**을 클릭하면 해당 사이트에서는 사용자가 추가한 항목의 파일 해시를 사용하여 의심스러운 파일과 URL을 분석해 맬웨어 유형을 감지합니다. **파일 해시(MD5)** 문자열에서 해시를 확인할 수 있습니다.

머신 값은 백업 스캔 중에 해당 해시가 확인된 머신의 수를 나타냅니다. 백업 스캔 또는 격리에 포함되어 있었던 항목의 경우에만 이 값이 입력됩니다. 허용 목록에 파일을 수동으로 추가한 경우 이 필드는 비어 있는 상태로 유지됩니다.

백업 맬웨어 방지 스캔

감염된 파일이 백업에서 복원되지 않도록 방지하기 위해 맬웨어 대비 백업을 스캔할 수 있습니다. 백업 스캔은 Windows 운영 체제에 대해서만 지원됩니다. 이 기능은 스캔 서비스가 Cyber Protect Management Server에 설치된 경우에만 사용할 수 있습니다.

맬웨어 대비 백업을 스캔하려면 백업 스캔 계획을 생성하십시오.

참고
보안 및 성능상의 이유로 스캔용으로 지정된 머신을 사용하는 것을 권장합니다. 이 머신은 스캔되는 모든 백업에 대한 액세스를 보유합니다.

스캔 결과는 대시보드에 있는 "백업 스캔 세부정보" 위젯에서 확인할 수 있습니다. 또한 **백업 스토리지** > **위치** > **<백업 이름>**에서 백업 상태를 확인할 수 있습니다. 백업 스캔이 수행되지 않은 경우 백업은 **스캔되지 않음** 상태를 유지합니다. 백업 스캔이 수행된 후에는 백업 상태가 다음 중 하나로 업데이트됩니다.

- **맬웨어 없음**
- **맬웨어 감지됨**

제한 사항

- **전체 머신** 또는 **디스크/볼륨** 백업 유형만 맬웨어에 대해 스캔할 수 있습니다.
- GPT 및 MBR 파티셔닝이 있는 NTFS 파일 시스템이 존재하는 볼륨만 스캔됩니다.
- 지원되는 백업 위치: **클라우드 스토리지**, **로컬 폴더**, **네트워크 폴더**.
- 지속적인 데이터 보호(CDP) 복구 지점이 있는 백업은 스캔 대상으로 선택할 수는 있지만 이러한 복구 지점은 스캔에서 제외됩니다. 일반 복구 지점만 스캔됩니다.
- 전체 머신에 대한 안전 복구로 CDP 백업이 선택된 경우 머신은 CDP 복구 지점의 데이터 없이 안전하게 복구됩니다. CDP 데이터를 복구하려면 **파일/폴더** 복구를 실행하십시오.

협업 및 커뮤니케이션 애플리케이션 보호

Zoom, Cisco Webex Meetings, Microsoft Teams는 현재 널리 사용되고 있는 화상/웹 컨퍼런스 및 커뮤니케이션 솔루션입니다. Cyber Protect을(를) 이용하면 공동 작업 도구를 보호할 수 있습니다.

Zoom, Cisco Webex Meetings, Microsoft Teams에 대한 보호 구성은 비슷합니다. 아래 예에서는 Zoom 구성을 살펴보겠습니다.

Zoom 보호를 설정하려면

1. 협업 애플리케이션이 설치되어 있는 머신에 보호 에이전트를 설치합니다.
2. Cyber Protect 웹 콘솔에 로그인하고, 다음 중 하나의 모듈이 활성화되어 있는 보호 계획을 적용합니다.
   - 안티바이러스 및 맬웨어 방지 기능(**Self-Protection** 및 **Active Protection** 설정이 활성화되어 있음) - Cyber Protect 버전 중 하나를 사용하는 경우.
   - **Active Protection**(**Self-Protection** 설정이 활성화되어 있음) - Cyber Backup 버전 중 하나를 사용하는 경우.
3. [선택 사항] 자동 업데이트 설치의 경우 보호 계획에서 **패치 관리** 모듈을 구성합니다.

그러면 Zoom 애플리케이션이 다음 작업을 포함하는 보호 상태에 놓이게 됩니다.

- Zoom 클라이언트 업데이트 자동 설치
- 코드 주입으로부터 Zoom 프로세스 보호
- Zoom 프로세스에 의한 의심스러운 작업 방지
- Zoom 관련 도메인이 추가되지 않도록 "호스트" 파일 보호

취약성 평가 및 패치 관리

취약성 평가(VA)는 시스템에서 발견한 취약성을 식별하고, 수량화하고, 우선순위를 지정하는 프로세스입니다. 보호 계획의 취약성 평가 모듈을 사용하면 머신의 취약성을 스캔하고, 운영 체제 및 설치된 애플리케이션이 최신 상태이며 제대로 작동하는지 확인할 수 있습니다.

취약성 평가 스캔은 다음 운영 체제를 실행하는 머신에서 지원됩니다.

- Windows 자세한 내용은 "지원되는 Microsoft 및 서드 파티 제품"(492페이지)을(를) 참조하십시오.
- Linux(CentOS 7/Virtuozzo/Acronis Cyber Infrastructure) 머신 자세한 내용은 "지원되는 Linux 제품"(494페이지)을(를) 참조하십시오.

패치 관리(PM) 기능을 사용하면 머신에 설치된 애플리케이션 및 운영 체제에 대한 패치(업데이트)를 관리하고, 시스템을 최신 상태로 유지할 수 있습니다. 패치 관리 모듈에서 머신에 대한 업데이트 설치를 자동 또는 수동으로 승인할 수 있습니다.

패치 관리는 Windows를 실행하는 머신에서 지원됩니다. 자세한 내용은 "지원되는 Microsoft 및 서드 파티 제품"(492페이지)을(를) 참조하십시오.

취약성 평가

취약성 평가 프로세스에서는 다음 단계를 수행합니다.

1. 취약성 평가 모듈이 활성화된 보호 계획을 생성하고 취약성 평가 설정을 지정하고 머신에 계획을 할당합니다.
2. 시스템은 스케줄에 따르거나 온디맨드로 취약성 평가 스캔 실행 명령을 보호 에이전트로 전송합니다.
3. 에이전트는 명령을 수신해 머신에서 취약성 스캔을 시작하고, 스캔 활동을 생성합니다.
4. 취약성 평가 스캔이 완료되면 에이전트에서 결과를 생성해 모니터링 서비스로 전송합니다.
5. 모니터링 서비스는 에이전트의 데이터를 처리해 취약성 평가 위젯에 결과와 발견된 취약성 목록을 표시합니다.
6. 이 정보를 사용하면 발견된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

대시보드 > **개요** > **취약성/기존 취약성** 위젯에서 취약성 평가 스캔 결과를 모니터링할 수 있습니다.

지원되는 Microsoft 및 서드 파티 제품

취약성 평가에서 지원되는 Microsoft 제품 및 Windows 운영 체제용 서드 파티 제품은 다음과 같습니다.

지원되는 Microsoft 제품

데스크톱 운영 체제

- Windows 7(Enterprise, Professional, Ultimate)
- Windows 8
- Windows 8.1
- Windows 10

서버 운영 체제

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

Microsoft Office 및 관련 컴퍼넌트

- Microsoft Office 2019(x64, x86)
- Microsoft Office 2016(x64, x86)
- Microsoft Office 2013(x64, x86)
- Microsoft Office 2010(x64, x86)

Windows 관련 컴퍼넌트

- Internet Explorer
- Microsoft Edge
- Windows Media Player
- .NET Framework
- Visual Studio 및 애플리케이션
- 운영 체제 컴퍼넌트

서버 애플리케이션

- Microsoft SQL Server 2008 R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2019
- Microsoft Exchange Server 2013
- Microsoft Sharepoint Server 2016
- Microsoft Sharepoint Server 2016

지원되는 Windows용 서드 파티 제품

Cyber Protect에서는 원격 업무 환경에서 필수적인 협업 도구와 VPN 클라이언트를 포함하여 다양한 서드 파티 앱에 대한 취약성 평가 및 패치를 지원합니다.

지원되는 Windows용 서드 파티 제품의 전체 목록은 https://kb.acronis.com/content/62853을 참조하십시오.

지원되는 Linux 제품

취약성 평가에서 지원되는 Linux 배포판 및 버전은 다음과 같습니다.

- Virtuozzo 7.0.11
- Virtuozzo 7.0.10(320)
- Virtuozzo 7.0.9(539)
- Virtuozzo 7.0.8(524)
- CentOS 7.x
- Acronis Cyber Infrastructure 3.x
- Acronis Storage 2.4.0
- Acronis Storage 2.2.0

취약성 평가 설정

취약성 평가 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"(188페이지)을(를) 참조하십시오. 취약성 평가 스캔은 스케줄에 따라 또는 온디맨드로 수행할 수 있습니다(보호 계획에서 **지금 실행** 작업 사용).

취약성 평가 모듈에서는 다음 설정을 지정할 수 있습니다.

스캔 대상

취약성을 스캔할 소프트웨어 제품을 정의합니다.

- Windows 머신:
  - **Microsoft 제품**
  - **Windows 서드 파티 제품**
    (지원되는 Windows용 서드 파티 제품에 대한 자세한 내용은 https://kb.acronis.com/content/62853을 참조하십시오.)
- Linux 머신:
  - **Linux 패키지 스캔**

예약

선택한 머신에서 수행될 취약성 평가 스캔 스케줄을 정의합니다.

다음 이벤트를 사용해 작업 실행 예약:

- **시간 기준 예약** – 지정 시간에 따라 작업을 실행합니다.
- **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

- **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

  참고
  작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다.

- **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다.
- **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.

기본 설정: **시간 기준 예약**.

예약 유형:

- **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다.
- **일일** – 작업을 실행할 요일을 선택합니다.
- **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.

기본 설정: **일일**.

시작 시간 – 작업을 실행할 정확한 시간을 선택합니다.

날짜 범위 내에 실행 – 구성된 예약이 실행될 기간의 범위를 설정합니다.

시작 조건 – 작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다.

맬웨어 방지 스캔용 시작 조건은 "시작 조건"(222페이지)에 설명되어 있는 백업 모듈용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다.

- **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다.
- **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행**
- **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다.
- **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다.

참고
Linux에서는 시작 조건이 지원되지 않습니다.

Windows 머신 취약성 평가

Windows 머신 및 Windows용 서드 파티 제품을 스캔하여 취약성을 확인할 수 있습니다.

1. Cyber Protect 웹 콘솔에서 보호 계획을 생성하고 **취약성 평가** 모듈을 활성화합니다.
2. 취약성 평가 설정을 지정합니다.

- **스캔 대상** - **Microsoft 제품**이나 **Windows 서드 파티 제품** 중 하나를 선택하거나 두 제품을 모두 선택합니다.
- **스케줄** – 취약성 평가를 수행할 스케줄을 정의합니다.

  예약 옵션에 대한 자세한 내용은 "취약성 평가 설정"(494페이지)을(를) 참조하십시오.

3. Windows 머신에 계획을 할당합니다.

취약성 평가 스캔을 완료하면 검색된 취약성 목록을 확인할 수 있습니다. 정보를 처리하고 검색된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

취약성 평가 결과를 모니터링하려면 **대시보드** > **개요** > **취약성/기존 취약성** 위젯을 확인합니다.

Linux 머신 취약성 평가

Linux 머신의 애플리케이션 수준 취약성과 커널 수준 취약성을 스캔할 수 있습니다.

Linux 머신에 대한 취약성 평가 구성하기

1. Cyber Protect 웹 콘솔에서 보호 계획을 생성하고 **취약성 평가** 모듈을 활성화합니다.
2. 취약성 평가 설정을 지정합니다.
   - **스캔 대상** – **Linux 패키지 스캔**을 선택합니다.
   - **스케줄** – 취약성 평가를 수행할 스케줄을 정의합니다.

     예약 옵션에 대한 자세한 내용은 "취약성 평가 설정"(494페이지)을(를) 참조하십시오.
3. Linux 머신에 계획을 할당합니다.

취약성 평가 스캔을 완료하면 검색된 취약성 목록을 확인할 수 있습니다. 정보를 처리하고 검색된 취약성 중 수정해야 할 항목을 결정할 수 있습니다.

취약성 평가 결과를 모니터링하려면 **대시보드** > **개요** > **취약성/기존 취약성** 위젯을 확인합니다.

발견된 취약성 관리

취약성 평가를 한 번 이상 수행했으며 취약성이 검색되었다면 **소프트웨어 관리** > **취약성**에서 취약성을 확인할 수 있습니다. 취약성 목록에는 패치가 있는 취약성과 제안된 패치가 없는 취약성이 모두 표시됩니다. 필터를 사용해 패치가 있는 취약성만 표시할 수 있습니다.

이름	설명
이름	취약성의 이름입니다.
영향을 받은 제품	취약성이 발견된 소프트웨어 제품입니다.
머신	영향을 받는 머신의 개수입니다.
심각도	발견된 취약성의 심각도입니다. CVSS(일반 취약성 점수 시스템)에 따라 취약성의 심각도 수준은 다음으로 나누어집니다. • **심각**: CVSS 9~10점 • **높음**: CVSS 7~9점

	• **중간**: CVSS 3~7점 • **낮음**: CVSS 0~3점 • **없음**
패치	해당 패치의 개수입니다.
게시됨	취약성이 CVE(일반 취약성 및 노출)에 게시된 날짜와 시간입니다.
감지됨	머신에서 기존 취약성이 최초로 감지된 날짜입니다.

목록에서 이름을 클릭해 발견된 취약성에 대한 설명을 찾을 수 있습니다.

취약성 수정 프로세스를 시작하려면

1. Cyber Protect 웹 콘솔에서 **소프트웨어 관리** > **취약성**으로 이동합니다.
2. 목록에서 취약성을 선택한 후 **패치 설치**를 클릭합니다. 취약성 수정 마법사가 열립니다.
3. 설치할 패치를 선택합니다. **다음**을 클릭합니다.
4. 패치를 설치하려는 머신을 선택합니다.
5. 패치 설치 후 머신을 재부팅할지 선택합니다.
   - **아니요** – 패치 설치 후 재부팅이 시작되지 않습니다.
   - **필요 시** – 업데이트 적용에 필요한 경우에만 재부팅이 시작됩니다.
   - **예** – 패치 설치 후 언제나 재부팅이 시작됩니다. 하지만 지연을 지정할 수 있습니다.

   백업이 끝날 때까지 재부팅하지 마십시오 – 백업 절차가 실행 중인 경우, 백업이 완료될 때까지 머신 재부팅이 지연됩니다.
6. **패치 설치**를 클릭합니다.

그러면 선택한 머신에 선택한 패치가 설치됩니다.

패치 관리

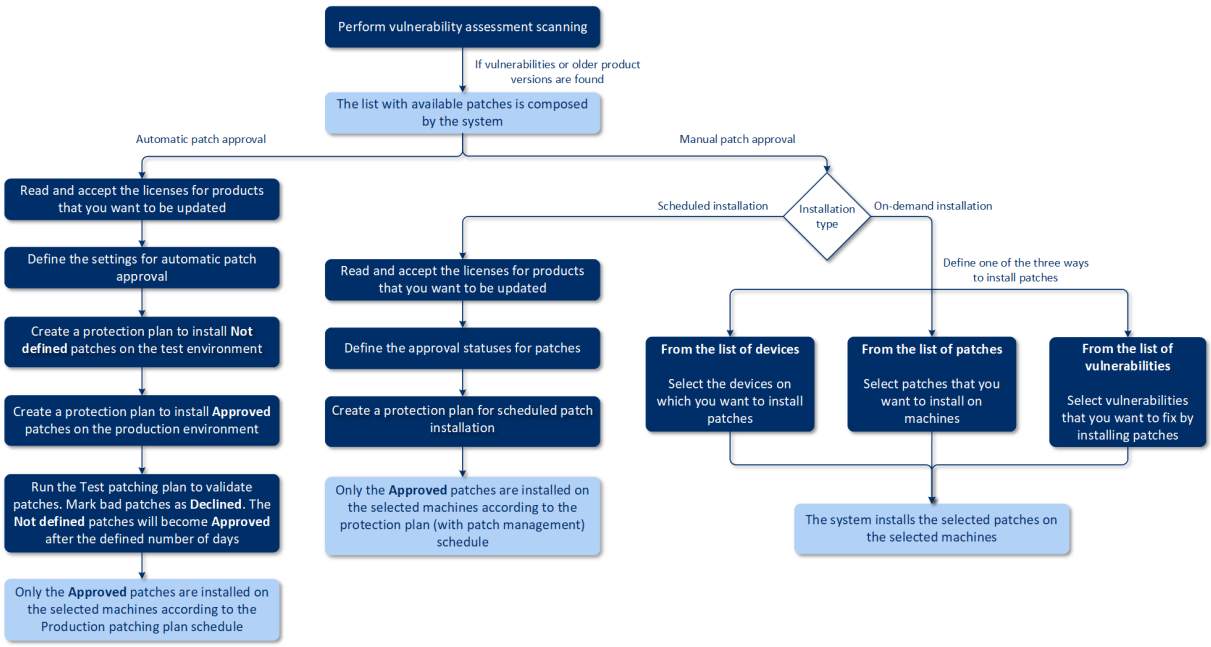
패치 관리 기능을 사용하면 다음 작업을 수행할 수 있습니다.

- OS 수준 및 애플리케이션 수준 업데이트 설치
- 패치 수동 또는 자동 승인
- 온디맨드로 또는 스케줄에 따라 패치 설치
- 심각도, 카테고리, 승인 상태 등 각기 다른 조건에 따라 어떤 패치를 적용할지 정확하게 정의
- 사전 업데이트 백업을 수행해 업데이트 실패 방지
- 패치 설치 후 적용할 재부팅 옵션 정의

Cyber Protect에서는 피어 투 피어 기술을 사용해 네트워크 대역폭 트래픽을 최소화합니다. 인터넷에서 업데이트를 다운로드할 전용 에이전트를 하나 이상 선택하여 네트워크의 다른 에이전트 사이에 분산시킬 수 있습니다. 또한 모든 에이전트는 피어 투 피어 에이전트로 서로 업데이트를 공유합니다.

작동법

자동 또는 수동 패치 승인을 구성할 수 있습니다. 아래 구성표에서 자동 및 수동 패치 승인 작업 흐름을 확인할 수 있습니다.



1. 먼저 **취약성 평가** 모듈이 활성화된 보호 계획을 사용해 취약성 평가 스캔을 최소 1번 수행해야 합니다. 스캔이 완료되면 시스템에서 발견된 취약점 및 사용 가능한 패치의 목록을 구성합니다.
2. 그러면 자동 패치 승인을 구성하거나 수동 패치 승인 접근 방식을 사용할 수 있습니다.
3. 패치를 온디맨드로 설치할지 스케줄에 따라 설치할지 정의합니다. 온디맨드 패치 설치는 세 가지 방식으로 수행할 수 있습니다.
   - 패치 목록으로 이동(**소프트웨어 관리** > **패치**)하여 필수 패치를 설치합니다.
   - 취약성 목록(**소프트웨어 관리** > **취약성**)으로 이동해 패치 설치를 포함한 수정 프로세스를 시작합니다.
   - 장치 목록(**장치** > **모든 장치**)으로 이동해 업데이트하려는 특정 장치를 선택하고 해당 장치에 패치를 설치합니다.

대시보드 > **개요** > **패치 설치 내역** 위젯에서 패치 설치 결과를 모니터링할 수 있습니다.

패치 관리 설정

패치 관리 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"을 참고하십시오. 보호 계획을 사용해 정의된 머신에 자동으로 설치할 Microsoft 제품 및 기타 Windows OS용 서드 파티 제품에 대한 업데이트를 지정할 수 있습니다.

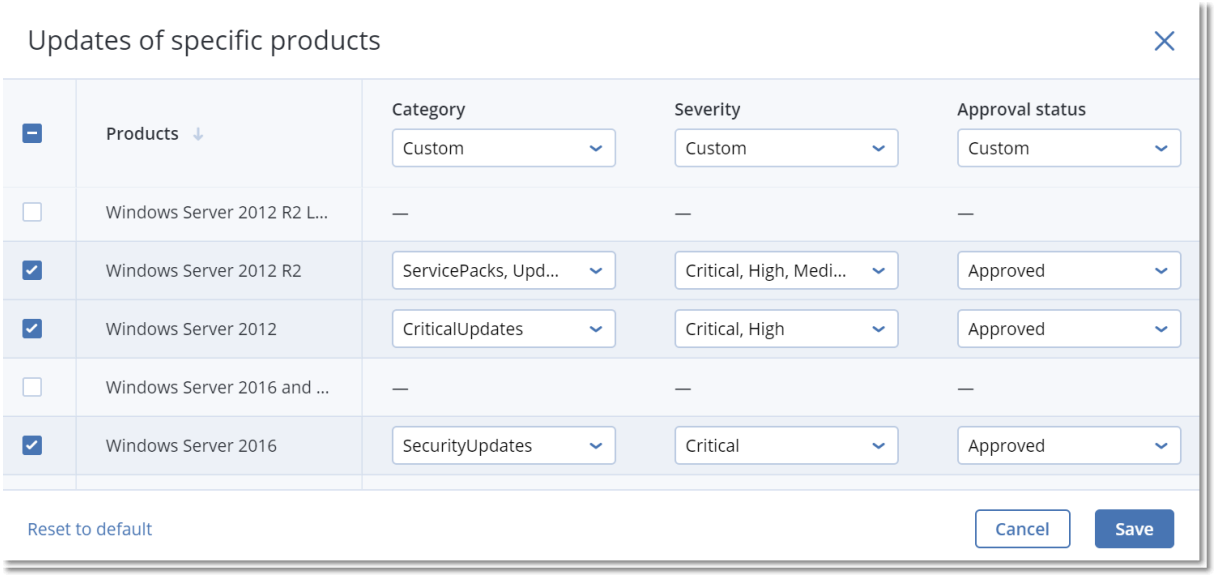
패치 관리 모듈에 대해 다음 설정을 지정할 수 있습니다.

Microsoft 제품

선택한 머신에 Microsoft 업데이트를 설치하려면 **Microsoft 제품 업데이트** 옵션을 활성화합니다.

설치할 업데이트를 선택합니다.

- **모두 업데이트**
- **보안 및 중요 업데이트만**
- **특정 제품의 업데이트**: 다른 제품에 대한 사용자 정의 설정을 정의할 수 있습니다. 특정 제품을 업데이트하려는 경우 각 제품에 대해 설치할 업데이트를 카테고리, 심각도, 승인 상태별로 정의할 수 있습니다.

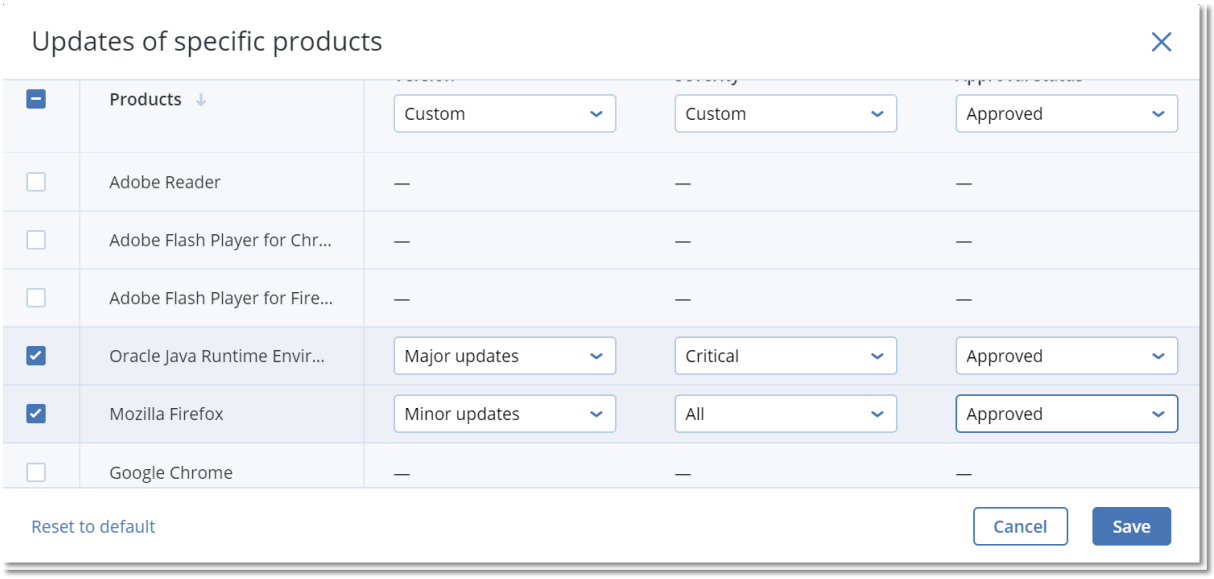


Windows 서드 파티 제품

선택한 머신에 Windows OS용 서드 파티 업데이트를 설치하려면 **Windows 서드 파티 제품** 옵션을 활성화합니다.

설치할 업데이트를 선택합니다.

- **대규모 업데이트만**을 선택하면 업데이트의 사용 가능한 최신 버전을 설치합니다.
- **마이너 업데이트만**을 선택하면 업데이트의 마이너 버전을 설치합니다.
- **특정 제품의 업데이트**: 다른 제품에 대한 사용자 정의 설정을 정의할 수 있습니다. 특정 제품을 업데이트하려는 경우 각 제품에 대해 설치할 업데이트를 카테고리, 심각도, 승인 상태별로 정의할 수 있습니다.



예약

선택한 머신에 설치될 업데이트 스케줄을 정의합니다.

다음 이벤트를 사용해 작업 실행 예약:

- **시간 기준 예약** – 지정 시간에 따라 작업을 실행합니다.
- **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.
- **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

> **참고**
> 작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다.

- **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다.
- **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.

기본 설정: **시간 기준 예약**.

예약 유형:

- **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다.
- **일일** – 작업을 실행할 요일을 선택합니다.
- **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.

기본 설정: **일일**.

시작 시간 – 작업을 실행할 정확한 시간을 선택합니다.

날짜 범위 내에 실행 – 구성된 예약이 실행될 기간의 범위를 설정합니다.

시작 조건 – 작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다.

맬웨어 방지 스캔용 시작 조건은 "시작 조건"(222페이지)에 설명되어 있는 백업 모듈용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다.

- **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다.
- **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행**
- **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다.
- **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다.

업데이트 전 백업

소프트웨어 업데이트 설치 전에 백업 실행 – 시스템에서 업데이트를 설치하기 전에 머신의 증분 백업을 생성합니다. 이전에 생성한 백업이 없는 경우에는 머신의 전체 백업이 생성됩니다. 그러면 패치 설치 실패 시 이전 상태로 롤백할 수 있습니다. **업데이트 전 백업** 옵션이 작동하려면 해당 머신에 패치 관리 및 백업 모듈이 활성화된 보호 계획과 백업될 항목(전체 머신 또는 부팅 + 시스템 볼륨)이 있어야 합니다. 백업에 적절하지 않은 항목을 선택한 경우에는 시스템이 **업데이트 전 백업** 옵션의 활성화를 허용하지 않습니다.

패치 목록 관리

취약성 평가 완료 후 **소프트웨어 관리** > **패치**에서 사용 가능한 패치를 찾아볼 수 있습니다.

이름	설명
이름	패치의 이름
심각도	패치의 심각도: • **심각** • **높음** • **중간** • **낮음** • **없음**
벤더	패치의 벤더
제품	패치를 적용할 수 있는 제품
설치된 버전	이미 설치된 제품 버전
버전	패치 버전
카테고리	패치가 속한 카테고리: • **중대한 업데이트** – 심각하며 보안과 관련되지 않은 버

	그를 해결하고자 특정 문제에 대해 광범위하게 릴리스된 수정 항목입니다. • **보안 업데이트** – 보안 문제를 해결하고자 특정 제품에 대해 광범위하게 릴리스된 수정 항목입니다. • **정의 업데이트** – 바이러스 또는 기타 정의 파일을 업데이트합니다. • **업데이트 롤업** – 핫픽스, 보안 업데이트, 중대한 업데이트, 손쉬운 디플로이를 위해 패키징된 업데이트의 누적입니다. 롤업은 일반적으로 보안과 같은 특정 영역이나 인터넷 정보 서비스(IIS)와 같은 특정 컴퍼넌트를 대상으로 합니다. • **서비스 팩** – 모든 핫픽스, 보안 업데이트, 중대한 업데이트, 제품 출시 후 생성된 업데이트의 누적입니다. 서비스 팩에는 고객이 요청한 제한된 수의 설계 변경 또는 기능이 포함될 수도 있습니다. • **도구** – 작업 또는 일련의 작업을 완료할 수 있도록 지원하는 유틸리티 또는 기능입니다. • **기능 팩** – 새로운 기능 릴리스로, 일반적으로 다음 릴리스에서 제품에 적용됩니다. • **업데이트** – 심각하지 않으며 보안과 관련되지 않은 버그를 해결하고자 특정 문제에 대해 광범위하게 릴리스된 수정 항목입니다. • **애플리케이션** – 애플리케이션용 패치.
Microsoft KB	Microsoft 제품에 대한 패치인 경우 KB 문서 ID가 제공됩니다.
릴리스 날짜	패치가 릴리스된 날짜입니다.
머신	영향을 받는 머신의 개수입니다.
승인 상태	승인 상태는 주로 자동 승인 시나리오와 상태별로 어떤 업데이트가 설치되어야 하는지 보호 계획에서 정의하는 데 필요합니다. 패치에 대해 다음 상태 중 하나를 정의할 수 있습니다. • **승인됨** – 패치가 최소 1개의 머신에 설치되어 있으며 유효성이 검증되었습니다. • **거절됨** – 패치가 안전하지 않으며 머신 시스템을 손상시킬 수 있습니다. • **정의되지 않음** – 패치 상태를 알 수 없으며 유효성 검증이 필요합니다.
라이센스 계약	• 읽고 수락 • 동의하지 않음. 라이센스 계약에 동의하지 않은 경우 패치 상태는 **거절됨**으로 설정되며 설치되지 않습니다.
취약성	취약성의 개수입니다. 클릭하면 취약성 목록으로 리디렉

	션됩니다.
크기	패치의 평균 크기
언어	패치가 지원하는 언어
벤더 사이트	벤더의 공식 사이트

자동 패치 승인

자동 패치 승인을 통해 머신에 업데이트를 설치하는 프로세스를 손쉽게 만들 수 있습니다. 예시를 통해 작동 방법을 살펴보겠습니다.

작동법

테스트 및 운영이라는 두 개의 환경이 있어야 합니다. 테스트 환경은 패치 설치를 테스트하여 문제가 없는지 확인하는 데 사용합니다. 테스트 환경에서 패치 설치를 테스트한 후 운영 환경에 안전한 패치를 자동 설치할 수 있습니다.

자동 패치 승인 구성

자동 패치 승인을 구성하려면

1. 업데이트하려는 제품의 각 벤더에 대해 라이센스 계약을 읽고 동의합니다. 그렇지 않으면 자동 패치 설치가 불가능합니다.
2. 자동 승인에 대한 설정을 구성합니다.
3. **패치 관리** 모듈이 활성화된 보호 계획을 준비(예: "테스트 패치")해 테스트 환경의 머신에 적용합니다. 다음과 같이 패치 설치 조건을 지정합니다. 패치 승인 상태는 **정의되지 않음**이어야 합니다. 이 단계는 패치를 검증하고 머신이 패치 설치 후에도 제대로 작동하는지 확인하는 데 필요합니다.
4. **패치 관리** 모듈이 활성화된 보호 계획을 준비(예: "운영 패치")해 운영 환경의 머신에 적용합니다. 다음과 같이 패치 설치 조건을 지정합니다. 패치 상태가 **승인됨**이어야 합니다.
5. 테스트 패치 계획을 실행하고 결과를 확인합니다. 이러한 머신에 대해 아무런 문제가 없는 승인 상태를 **정의되지 않음**으로 보존하고 제대로 작동하지 않는 머신 상태는 **거절됨**으로 설정합니다.
6. **자동 승인** 옵션에 설정된 일 수가 지나면 **정의되지 않음** 상태의 패치가 **승인됨**으로 변경됩니다.
7. 운영 패치 계획이 시작되면 **승인됨** 상태의 패치만 운영 머신에 설치됩니다.

수동 단계는 다음과 같습니다.

1단계 업데이트하려는 제품에 대한 라이센스 계약을 읽고 수락

1. Cyber Protect 웹 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. 패치를 선택한 다음 라이센스 계약을 읽고 수락합니다.

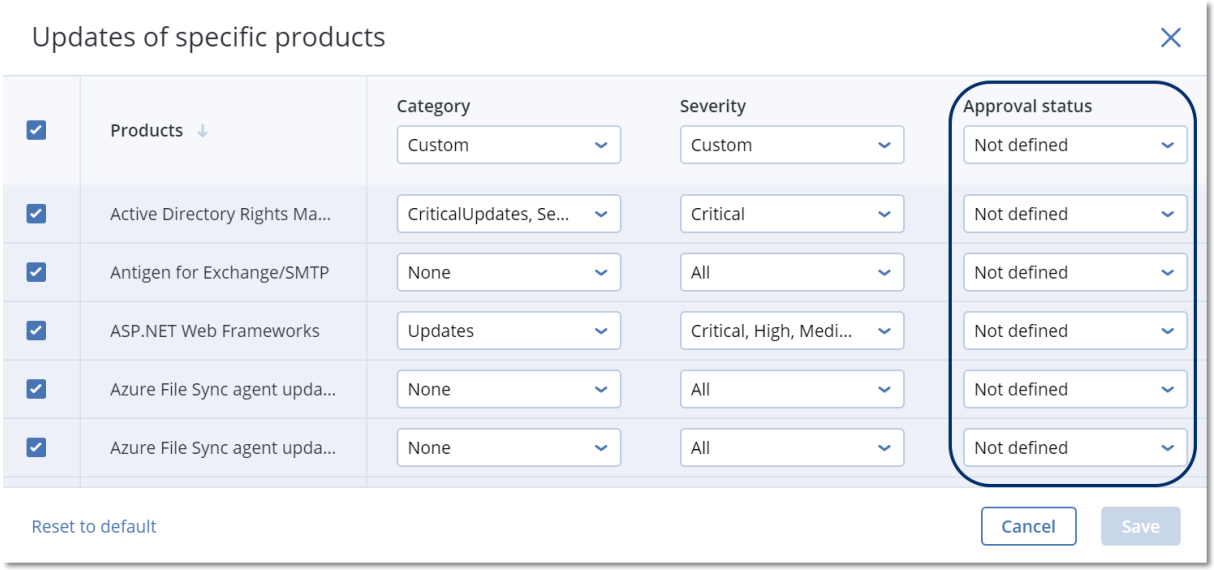
2단계 자동 승인 설정 구성

1. Cyber Protect 웹 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. **설정**을 클릭합니다.
3. **자동 승인** 옵션을 활성화하고 일 수를 지정합니다. 이렇게 하면 첫 번째 패치 시도부터 시작해 지정한 일 수가 지나면 **정의되지 않음** 상태의 패치가 **승인됨**으로 자동 변경됩니다.
   10일을 지정했다고 가정해 보겠습니다. 테스트 머신에 테스트 패치 계획을 수행하고 패치를 설치합니다. 머신에 손상을 주는 패치는 **거절됨**으로 표시하고 나머지 패치는 **정의되지 않음** 상태를 유지합니다. 10일이 지나면 **정의되지 않음** 상태의 패치는 **승인됨**으로 자동 전환됩니다.
4. **라이센스 계약을 자동으로 수락** 옵션을 활성화합니다. 이는 사용자의 확인을 받지 않고 패치 설치 시 라이센스를 자동으로 수락하려고 할 때 필요합니다.

3단계 테스트 패치 보호 계획 준비

1. Cyber Protect 웹 콘솔에서 **계획** > **보호**로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. **패치 관리** 모듈을 활성화합니다.
4. Microsoft 및 서드 파티 제품, 스케줄, 사전 업데이트 백업에 대해 설치할 업데이트를 정의합니다. 이러한 설정에 대한 자세한 내용은 "패치 관리 설정"을 참고하십시오.

중요
업데이트될 모든 제품에 대해 **승인 상태**를 **정의되지 않음**으로 정의합니다. 업데이트 시점이 오면 에이전트는 선택한 머신에 대해 **정의되지 않음** 상태의 패치만 테스트 환경에 설치합니다.



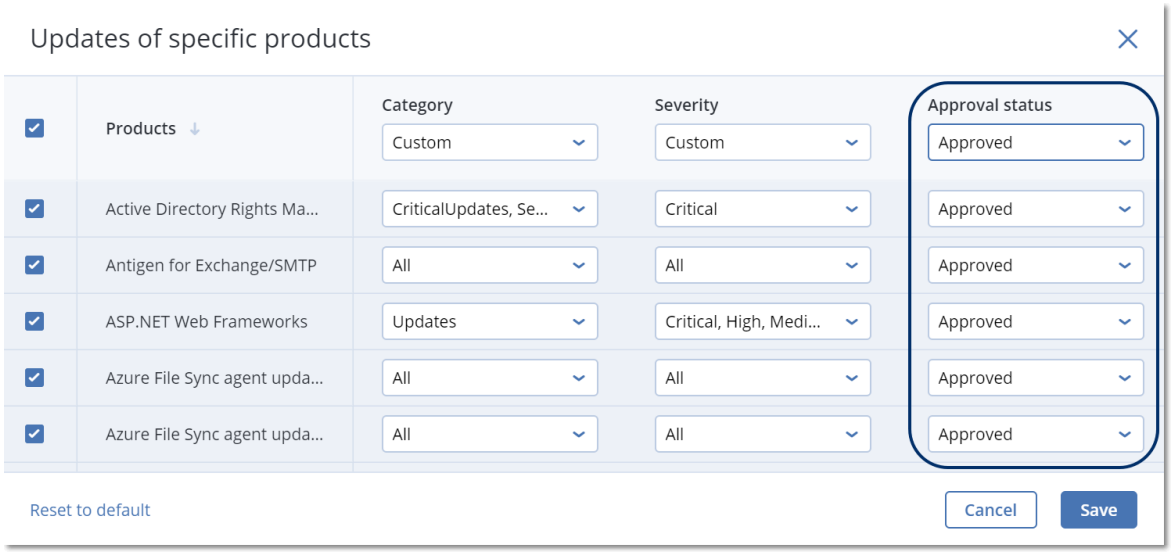
4단계. 운영 패치 보호 계획 준비

1. Cyber Protect 웹 콘솔에서 **계획** > **보호**로 이동합니다.
2. **계획 생성**을 클릭합니다.
3. **패치 관리** 모듈을 활성화합니다.
4. Microsoft 및 서드 파티 제품, 스케줄, 사전 업데이트 백업에 대해 설치할 업데이트를 정의합니다. 이러한 설정에 대한 자세한 내용은 "패치 관리 설정"을 참고하십시오.

중요

업데이트될 모든 제품에 대해 **승인 상태**를 **승인됨**으로 정의합니다. 업데이트 시점이 오면 에이전트는 선택한 머신에 대해 **승인됨** 상태의 패치만 운영 환경에 설치합니다.

참고



5단계. 테스트 패치 보호 계획 실행 및 결과 확인

1. 테스트 패치 보호 계획을 실행합니다(스케줄에 따르거나 온디맨드로).
2. 그 다음 설치된 패치 중 무엇이 안전하고 위험한지 확인합니다.
3. **소프트웨어 관리** > **패치**로 이동해 안전하지 않은 패치의 **승인 상태**를 **거절됨**으로 지정합니다.

수동 패치 승인

수동 패치 승인 프로세스는 다음과 같습니다.

1. Cyber Protect 웹 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. 설치하려는 패치를 선택한 다음 라이센스 계약을 읽고 수락합니다.
3. 설치를 승인하려는 패치의 **승인 상태**를 **승인됨**으로 설정합니다.
4. 패치 관리 모듈이 활성화된 보호 계획을 생성합니다. 스케줄을 구성하거나 패치 관리 모듈 설정에서 **지금 실행**을 클릭해 온디맨드로 계획을 실행할 수 있습니다.

그 결과 승인된 패치만 선택한 머신에 설치됩니다.

온디맨드 패치 설치

온디맨드 패치 설치는 세 가지 방식으로 수행할 수 있습니다.

- 패치 목록으로 이동(**소프트웨어 관리** > **패치**)하여 필수 패치를 설치합니다.
- 취약성 목록(**소프트웨어 관리** > **취약성**)으로 이동해 패치 설치를 포함한 수정 프로세스를 시작합니다.
- 장치 목록(**장치** > **모든 장치**)으로 이동해 업데이트하려는 특정 장치를 선택하고 해당 장치에 패치를 설치합니다.

패치 목록의 패치를 설치한다고 가정해 보겠습니다.

1. Cyber Protect 웹 콘솔에서 **소프트웨어 관리** > **패치**로 이동합니다.
2. 설치하려는 패치에 대한 라이센스 계약을 수락합니다.
3. 설치하려는 패치를 선택한 다음 **설치**를 클릭합니다.
4. 패치를 설치해야 할 머신을 선택합니다.
5. 패치 설치 후 재부팅 여부를 정의합니다.
   - **해당 없음** – 패치 후 절대 재부팅이 시작되지 않습니다.
   - **필요 시** – 패치 적용에 필요한 경우에만 재부팅합니다.
   - **항상** – 패치 후 항상 재부팅합니다. 언제나 재부팅 지연을 지정할 수 있습니다.

   백업이 끝날 때까지 재부팅하지 마십시오 – 백업 절차가 실행 중인 경우, 백업이 완료될 때까지 머신 재부팅이 지연됩니다.
6. **패치 설치**를 클릭합니다.

선택한 머신에 선택한 패치가 설치됩니다.

패치 목록 수명

패치 목록을 최신 상태로 유지하려면 **소프트웨어 관리** > **패치** > **설정**으로 이동해 **목록 수명** 옵션을 지정합니다.

목록 수명 옵션은 사용 가능한 상태로 감지된 패치를 패치 목록에 보관한 기간을 정의합니다. 일반적으로 패치는 패치가 없는 것으로 감지되거나 정의한 시간이 경과한 모든 머신에 성공적으로 적용된 경우 목록에서 제거됩니다.

- **영구** – 패치가 항상 목록에 유지됩니다.
- **7일** – 초기 설치 후 7일이 경과하면 패치가 제거됩니다.

  패치가 설치되어야 하는 머신이 2개 있다고 가정해보겠습니다. 머신 하나는 온라인이고, 하나는 오프라인입니다. 첫 번째 머신에 패치가 설치되었습니다. 7일 후 해당 패치는 오프라인인 두 번째 머신에 설치되지 않았다고 해도 목록에서 제거됩니다.
- **30일** – 초기 설치 후 30일이 경과하면 패치가 제거됩니다.

스마트 보호

위협 피드

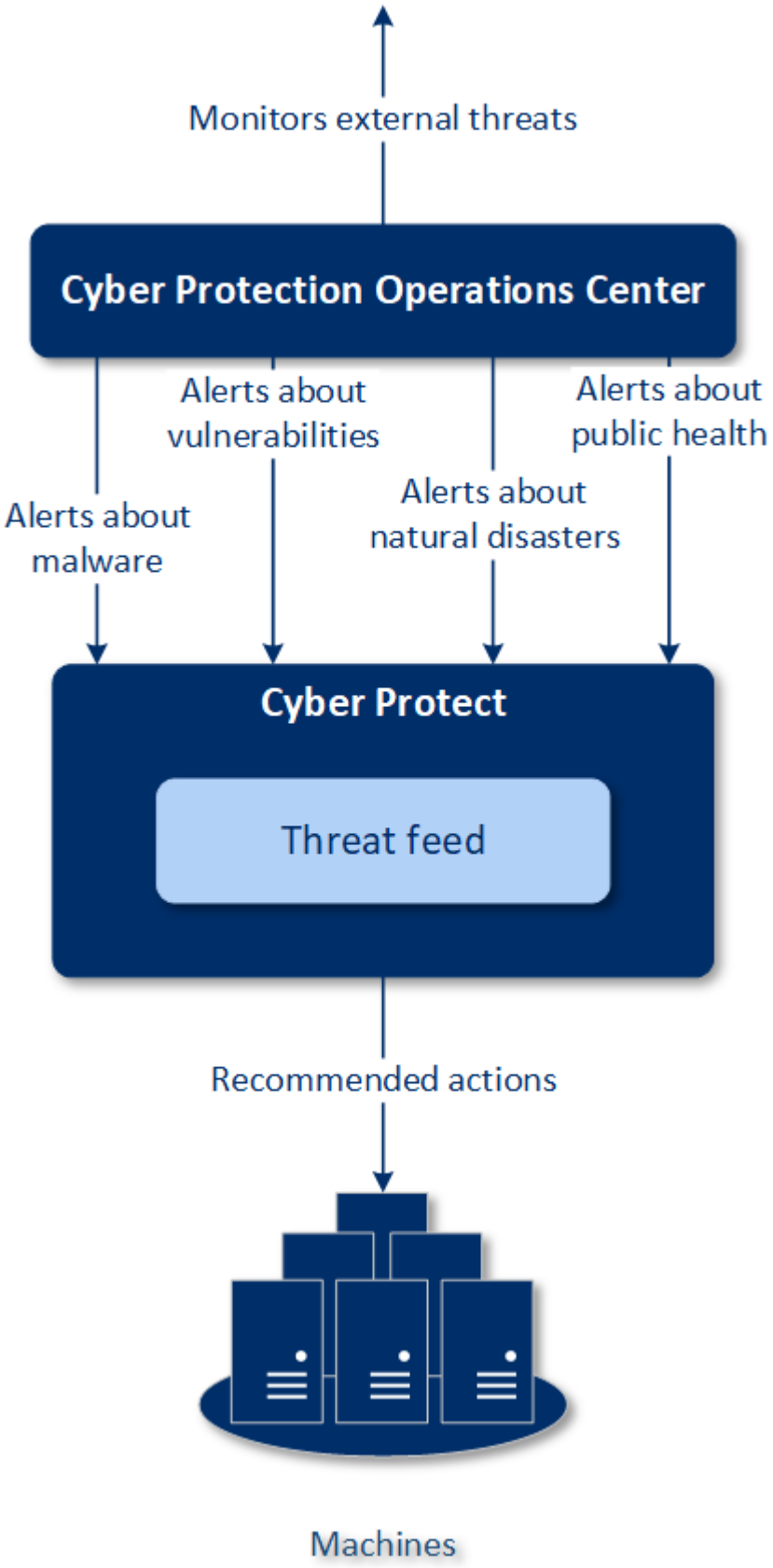
Acronis 사이버 보호 작업 센터(CPOC)에서는 관련된 지역으로만 전송되는 보안 경보를 생성합니다. 이러한 보안 경보는 맬웨어, 취약성, 자연 재해, 공공 보건을 비롯해 데이터 보호에 영향을 미칠 수 있는 글로벌 이벤트에 대한 정보를 제공합니다. 위협 피드에는 모든 잠재적인 위협이 표시되어 이를 방지할 수 있도록 해줍니다.

보안 경보는 보안 전문가가 제공하는 특정 작업을 통해 해결할 수 있습니다. 일부 경보는 이후 발생할 가능성이 있지만 사용 가능한 권장 작업이 없는 위협을 알리기 위한 것일 수도 있습니다.

작동법

Acronis 사이버 보호 작업 센터는 외부 위협을 모니터링하고 맬웨어, 취약성, 자연 재해 위협, 공공 보건에 대한 경보를 생성합니다. **위협 피드** 섹션의 Cyber Protect 웹 콘솔에서 이러한 모든 경보를 확인할 수 있습니다. 경보 유형에 따라 해당하는 권장 작업을 수행할 수 있습니다.

위협 피드의 주요 작업 흐름은 아래 다이어그램에 설명되어 있습니다.



Acronis 사이버 보호 작업 센터에서 수신한 경보에 대한 권장 작업을 실행하려면 다음을 수행하십시오.

1. Cyber Protect 웹 콘솔에서 **대시보드** > **위협 피드**로 이동해 기존 보안 경보가 있는지 검토합니다.

2. 목록의 경보를 선택한 다음 제공된 상세 정보를 검토합니다.

3. **시작**을 클릭해 마법사를 실행합니다.

4. 수행하려는 작업을 활성화하고 이러한 작업이 적용될 머신을 선택합니다. 다음 작업이 제안될 수 있습니다.

- **취약성 평가** – 선택된 머신의 취약성 스캔
- **패치 관리** –선택한 머신에 패치 설치
- **맬웨어 방지 기능** – 선택한 머신에 대한 전체 스캔 실행
- **보호 또는 보호되지 않는 머신 백업** – 보호/보호되지 않는 머신 백업

5. **시작**을 클릭합니다.

6. **작업** 페이지에서 작업이 성공적으로 수행되었는지 확인합니다.

모든 경보 삭제

위협 피드 알림은 다음 시간이 지나면 자동으로 정리됩니다.

- 자연 재해 – 1주
- 취약성 – 1개월
- 맬웨어 – 1개월
- 공공 보건 - 1주

데이터 보호 맵

데이터 보호 맵 기능으로 다음이 가능합니다.

- 머신에 저장된 데이터에 대한 상세한 정보(분류, 위치, 보호 상태, 기타 추가 정보)를 파악합니다.
- 데이터의 보호 여부를 감지합니다. 데이터는 백업으로 보호될 때 보호 상태로 간주됩니다(백업 모듈이 활성화된 보호 계획 사용).
- 데이터 보호를 위한 작업을 수행합니다.

작동법

1. 먼저 데이터 보호 맵 모듈이 활성화된 보호 계획을 생성합니다.
2. 계획이 수행되어 데이터의 발견 및 분석이 끝나면 데이터 보호 맵 위젯에 데이터 보호 상태가 시각적으로 표시됩니다.
3. 또한 **장치** > **데이터 보호 맵**으로 이동해 장치별로 보호되지 않는 파일에 대한 정보를 확인할 수도 있습니다.
4. 장치에서 보호되지 않는 것으로 감지된 파일을 보호하기 위한 작업을 수행할 수 있습니다.

보호되지 않는 것으로 감지된 파일 관리

보호되지 않는 것으로 감지된 중요 파일을 보호하려면 다음을 수행하십시오.

1. Cyber Protect 웹 콘솔에서 **장치** > **데이터 보호 맵**으로 이동합니다.
   장치 목록에서 장치별로 보호되지 않는 파일의 수, 해당 파일의 크기, 마지막 데이터 검색 등과 같은 일반적인 정보를 확인할 수 있습니다.
   특정 머신의 파일을 보호하려면 말줄임표 아이콘(...)과 **모든 파일 보호**를 차례로 클릭합니다.
   백업 모듈이 활성화된 보호 계획을 생성할 수 있는 계획 목록으로 리디렉션됩니다.
   목록에서 보호되지 않는 파일이 있는 특정 장치를 삭제하려면 **다음 데이터 검색 시까지 숨김**을 클릭합니다.
2. 특정 장치에서 보호되지 않는 파일에 대한 자세한 정보를 확인하려면 해당 장치의 이름을 클릭합니다.
   확장자 및 위치별로 보호되지 않는 파일의 목록을 확인할 수 있습니다. 파일 확장자별로 목록을 필터링할 수 있습니다.
3. 보호되지 않는 파일을 모두 보호하려면 **모든 파일 보호**를 클릭합니다. 백업 모듈이 활성화된 보호 계획을 생성할 수 있는 계획 목록으로 리디렉션됩니다.

보고서 형식으로 보호되지 않는 파일에 대한 정보를 받아보려면 **상세 보고서를 CSV로 다운로드**를 클릭합니다.

데이터 보호 맵 설정

데이터 보호 맵 모듈이 있는 보호 계획을 생성하는 방법을 알아보려면 "보호 계획 생성"을 참고하십시오.

데이터 보호 맵 모듈에 대해 다음 설정을 지정할 수 있습니다.

예약

다른 설정을 정의해 데이터 보호 맵이 수행될 작업에 따라 스케줄을 생성할 수 있습니다.

다음 이벤트를 사용해 작업 실행 예약:

- **시간 기준 예약** – 지정 시간에 따라 작업을 실행합니다.
- **사용자가 시스템에 로그인할 때** – 기본적으로 사용자가 로그인하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.
- **사용자가 시스템에서 로그오프할 때** – 기본적으로 사용자가 로그오프하면 작업이 시작됩니다. 특정 사용자 계정만 작업을 트리거할 수 있도록 이 설정을 수정할 수 있습니다.

  참고
  작업은 시스템 종료 시 실행되지 않습니다. 일정 예약 구성에서 시스템 종료와 로그오프는 다른 작업입니다.

- **시스템 시작 시** – 운영 체제가 시작될 때 작업을 실행합니다.
- **시스템 종료 시** – 운영 체제가 종료될 때 작업을 실행합니다.

기본 설정: **시간 기준 예약**.

예약 유형:

- **월간** – 작업을 실행할 월과 주 또는 일을 선택합니다.
- **일일** – 작업을 실행할 요일을 선택합니다.
- **매시간** – 작업을 실행할 요일, 반복 횟수, 시간 간격을 선택합니다.

기본 설정: **일일**.

시작 시간 – 작업을 실행할 정확한 시간을 선택합니다.

날짜 범위 내에 실행 – 구성된 예약이 실행될 기간의 범위를 설정합니다.

시작 조건 – 작업을 시작하기 위해 동시에 충족되어야 하는 모든 조건을 정의합니다.

맬웨어 방지 스캔용 시작 조건은 "시작 조건"(222페이지)에 설명되어 있는 백업 모듈용 시작 조건과 유사합니다. 다음과 같이 추가적인 시작 조건을 정의할 수 있습니다.

- **기간 내에서 작업 시작 시간 분배** – 이 옵션을 사용하면 작업을 수행해야 하는 기간을 정의할 수 있습니다. 이 옵션을 사용해 작업 시간대를 설정하여 네트워크 병목현상을 피할 수 있습니다. 지연 시간은 시간 또는 분 단위로 지정할 수 있습니다. 예를 들어 기본 시작 시간이 오전 10시이고 지연 시간이 60분인 경우 작업은 오전 10시~오전 11시 사이에 시작됩니다.
- **머신이 꺼진 경우 머신 시작 시 누락된 작업 실행**
- **작업 실행 중 절전 또는 최대 절전 모드가 되는 것을 방지** – 이 옵션은 Windows를 구동 중인 머신에서만 유효합니다.
- **시작 조건이 충족되지 않아도 다음 후에 작업 실행** - 다른 시작 조건에 관계없이 지정한 기간이 지나면 작업이 시작됩니다.

확장자 및 예외 규칙

확장자 탭에서 데이터 검색 시 중요하다고 간주하여 보호 여부를 확인할 파일 확장자 목록을 정의할 수 있습니다. 확장자 정의에는 다음 형식을 사용하십시오.

```
.html, .7z, .docx, .zip, .pptx, .xml
```

예외 규칙 탭에서 데이터 검색 시 보호 상태를 확인하지 않을 파일과 폴더를 정의할 수 있습니다.

- **숨겨진 파일 및 폴더** – 이 옵션을 선택하는 경우 데이터 검사 시 숨겨진 파일과 폴더를 건너뜁니다.
- **시스템 파일 및 폴더** – 이 옵션을 선택하는 경우 데이터 검사 시 시스템 파일과 폴더를 건너뜁니다.

원격 데스크톱 액세스

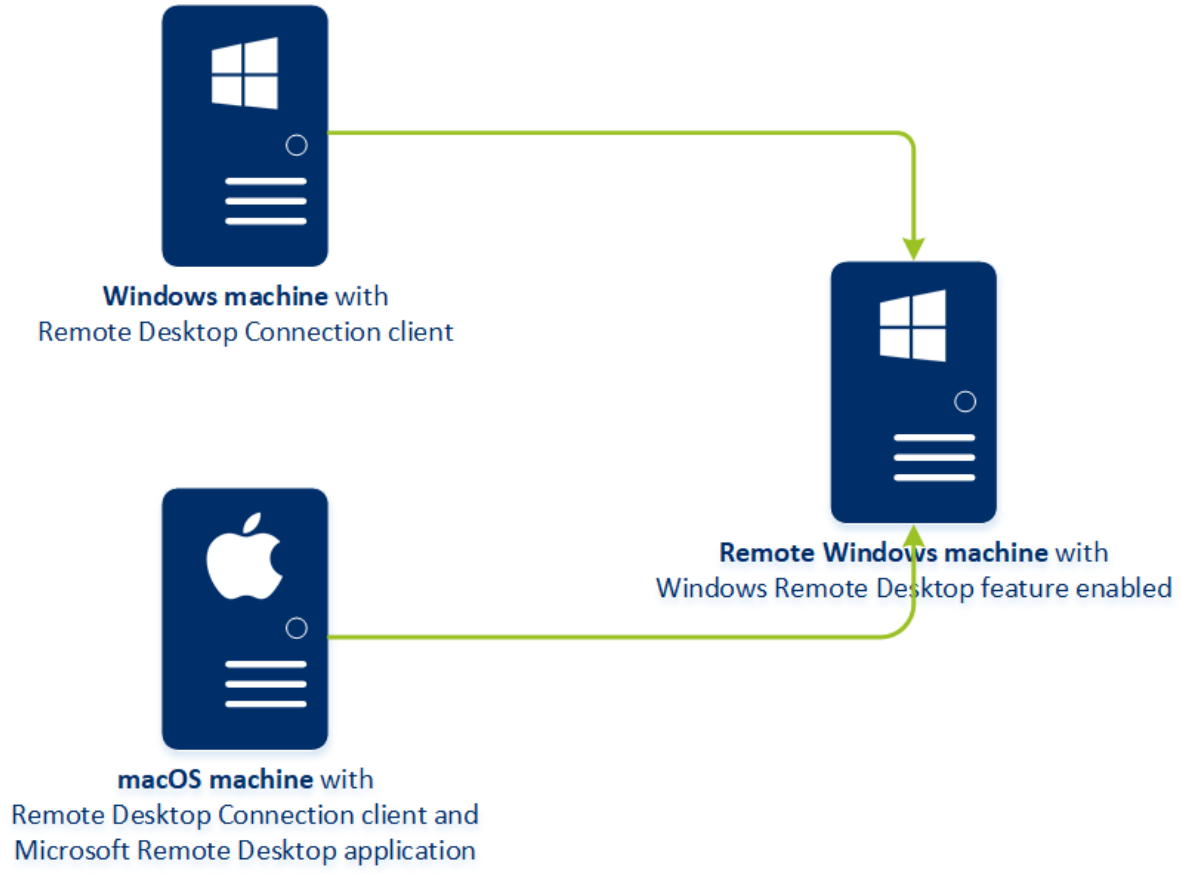
원격 액세스(RDP 및 HTML5 클라이언트)

Cyber Protect에서는 원격 액세스 기능을 제공합니다. 웹 콘솔에서 바로 사용자 머신에 원격으로 연결하고 관리할 수 있습니다. 이를 통해 사용자의 머신에 발생한 문제를 해결하도록 손쉽게 지원할 수 있습니다.

전제조건:

- 보호 에이전트는 원격 머신에 설치되고 관리 서버에 등록됩니다.
- 머신에는 적절한 Cyber Protect 라이센스가 할당되어 있습니다.
- 연결을 시작하는 머신에 원격 데스크톱 연결 클라이언트가 설치되어 있습니다.
- RDP 연결이 시작되는 머신은 해당 호스트 이름으로 관리 서버에 액세스할 수 있어야 합니다. DNS 설정은 적절하게 구성되어야 하며, 그렇지 않은 경우 관리 서버 호스트 이름이 호스트 파일에 포함되어야 합니다.

원격 연결은 Windows 머신과 macOS 머신 모두에서 설정할 수 있습니다.



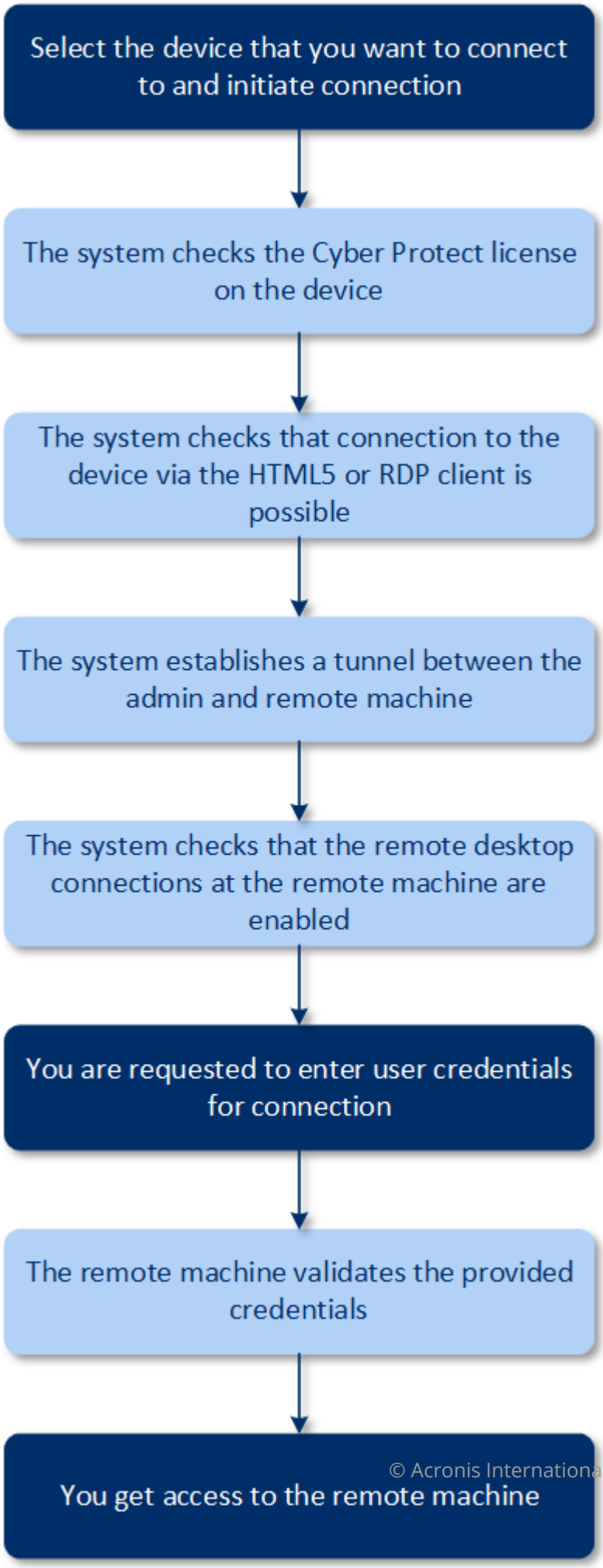
원격 액세스 기능은 Windows 원격 데스크톱 기능을 사용할 수 있는 Windows 머신에 연결할 때 사용할 수 있습니다. 이것이 바로 Windows 10 Home 또는 macOS 시스템 등에 대해 원격 액세스가 불가능한 이유입니다.

macOS 머신에서 원격 머신으로 연결을 설정하려면 다음 애플리케이션이 macOS 머신에 설치되어 있는지 확인하십시오.

- 원격 데스크톱 연결 클라이언트
- Microsoft 원격 데스크톱 애플리케이션

작동법

원격 머신 연결을 시도할 때 시스템에서는 먼저 이러한 머신에 Cyber Protect 라이센스가 있는지 확인하고 HTML5 또는 RDP 클라이언트를 통한 연결이 가능한지 확인합니다. 사용자가 RDP 또는 HTML5 클라이트를 통한 연결을 시작하면 시스템에서 원격 머신에 대한 터널을 구축하고 원격 머신에 원격 데스크톱 연결이 활성화되어 있는지 확인합니다. 그런 다음 자격 증명을 입력하고 유효성 검사가 완료되면 원격 머신에 액세스할 수 있습니다.



원격 머신 연결 방법

원격 머신에 연결하려면 다음을 수행합니다.

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원격으로 연결하려는 머신을 클릭한 다음 **사이버 보호 데스크톱** > **RDP 클라이언트를 통해 연결** 또는 **HTML5 클라이언트를 통해 연결**을 클릭합니다.

   참고
   HTML5 클라이언트를 통한 연결은 Linux 머신에 관리 서버가 설치된 경우에만 사용할 수 있습니다.

3. [선택 사항, RDP 클라이언트를 통해 연결하는 경우에만 해당] 원격 데스크톱 연결 클라이언트를 다운로드하여 설치합니다. 원격 머신 연결을 시작합니다.
4. 원격 머신에 액세스하기 위한 로그인 및 비밀번호를 지정하고 **연결**을 클릭합니다.

그러면 원격 머신에 연결해 관리할 수 있습니다.

원격 연결 공유

재택 근무 중인 직원이 사무실 컴퓨터에 액세스해야 하는데 조직에 VPN 또는 원격 접속을 위한 기타 도구가 구성되어 있지 않을 수 있습니다. Cyber Protect 서비스를 이용하면 사용자와 RDP 링크를 공유하여 머신에 대한 원격 액세스를 제공할 수 있습니다.

원격 연결 공유 기능을 활성화하는 방법

1. Cyber Protect 웹 콘솔에서 **설정** > **보호** > **원격 접속**으로 이동합니다.
2. **원격 데스크톱 연결 공유** 확인란을 선택합니다.

Cyber Protect 웹 콘솔에서 장치를 선택했을 때 **원격 접속 공유**라는 새 옵션이 표시됩니다.

사용자와 원격 연결을 공유하는 방법

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 원격 연결을 제공하려는 장치를 선택합니다.
3. **원격 연결 공유**를 클릭합니다.
4. **링크 가져오기**를 클릭합니다. 창이 열리면 생성된 링크를 복사합니다. 이 링크를 장치에 대한 원격 액세스가 필요한 사용자와 공유할 수 있습니다. 이 링크는 10시간 동안 유효합니다.

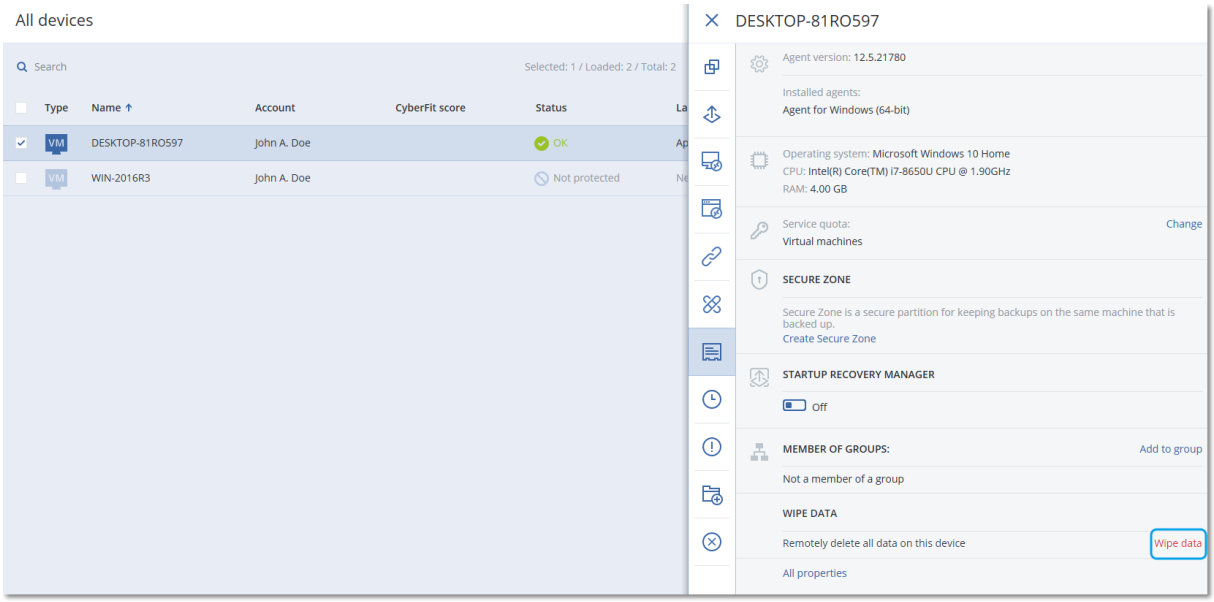
링크를 가져온 후에는 이메일이나 기타 커뮤니케이션 수단을 통해 공유할 수 있습니다. 링크를 공유 받은 사용자는 링크를 클릭한 다음 연결 유형을 선택해야 합니다.

- RDP 클라이언트를 통해 연결.
  이 연결에서는 원격 연결 클라이언트를 다운로드하고 설치하라는 메시지가 표시됩니다.
- HTML5 클라이언트를 통해 연결.
  이 연결에서는 사용자 머신에 RDP 클라이언트를 설치할 필요가 없습니다. 사용자는 로그인 화면으로 리디렉션되며 머신에 액세스하기 위한 자격 증명을 입력해야 합니다.

원격 지우기

머신을 분실 또는 도난당한 경우, Cyber Protect 서비스 관리자 및 머신 소유자는 원격 지우기를 통해 관리 대상 머신에서 데이터를 삭제할 수 있습니다. 이를 통해 민감한 정보에 대한 무단 액세스를 방지할 수 있습니다.

원격 지우기는 Windows 10을 실행 중인 머신에만 이용할 수 있습니다. 지우기 명령을 수신하려면 머신이 켜져 있고, 인터넷에 연결된 상태여야 합니다.



머신에서 데이터를 지우려면

1. Cyber Protect 웹 콘솔에서 **장치** > **모든 장치**로 이동합니다.
2. 데이터를 지우려는 머신을 선택합니다.

   참고
   한 번에 하나의 머신에서만 데이터를 지울 수 있습니다.

3. **상세 정보**를 클릭한 다음, **데이터 지우기**를 클릭합니다.
   선택한 머신이 오프라인이면 **데이터 지우기** 옵션에 액세스할 수 없습니다.
4. 선택 내용을 확인합니다.
5. 이 머신의 로컬 관리자의 자격 증명을 입력한 다음, **데이터 지우기**를 클릭합니다.

   참고
   소거 프로세스와 이 프로세스를 시작한 사람에 관한 상세 정보를 **대시보드** > **활동**에서 확인할 수 있습니다.

장치 그룹

장치 그룹은 등록된 많은 장치를 쉽게 관리할 수 있도록 설계되었습니다.

그룹에 보호 계획을 적용할 수 있습니다. 새 장치가 그룹에 나타나면 해당 장치는 계획으로 보호됩니다. 장치가 그룹에서 제거되면 해당 장치는 더 이상 계획으로 보호되지 않습니다. 그룹에 적용된 계획은 그룹 구성원에서 취소할 수 없고 그룹 자체에서만 취소할 수 있습니다.

같은 유형의 장치만 그룹에 추가할 수 있습니다. 예를 들어 **Hyper-V**에서 Hyper-V 가상 머신 그룹을 생성할 수 있습니다. **에이전트가 있는 머신** 아래에서 설치된 에이전트가 있는 머신 그룹을 생성할 수 있습니다. **모든 장치**에서는 그룹을 생성할 수 없습니다.

단일 장치는 두 개 이상 그룹의 구성원일 수 있습니다.

기본 제공 그룹

장치가 등록되면 해당 장치는 **장치** 탭의 기본 제공 루트 그룹 중 하나에 나타납니다.

루트 그룹은 편집하거나 삭제*할 수 없습니다*. 루트 그룹에는 계획을 적용*할 수 없습니다*.

일부 루트 그룹에는 기본 제공 하위 루트 그룹이 포함됩니다. 이러한 그룹은 편집하거나 삭제*할 수 없습니다*. 그러나 하위 루트 기본 제공 그룹에는 계획을 적용*할 수 있습니다*.

사용자 정의 그룹

머신의 다양한 역할로 인해 단일 보호 계획이 있는 기본 제공 그룹의 모든 장치를 보호하는 작업이 만족스럽지 않을 수 있습니다. 백업된 데이터는 각 부서에 특정하며 일부 데이터는 자주, 다른 데이터는 일 년에 두 번 백업해야 하므로 각기 다른 머신 집합에 적용할 수 있는 다양한 보호 계획을 생성하고 싶을 수 있습니다. 이 경우 사용자 정의 그룹을 만드는 것을 고려하십시오.

하나의 사용자 그룹에 하나 이상의 중첩된 그룹이 포함될 수 있습니다. 모든 사용자 정의 그룹은 편집 또는 삭제할 수 있습니다. 다음과 같은 유형의 사용자 정의 그룹이 있습니다.

- **정적 그룹**

  정적 그룹에는 수동으로 추가된 머신이 포함됩니다. 정적 그룹 내용은 머신을 명시적으로 추가 또는 삭제하는 경우에만 변경됩니다.

  예: 회계 부서의 사용자 정의 그룹을 만들고 이 그룹에 회계원의 머신을 수동으로 추가합니다. 보호 계획이 그룹에 적용되면 회계원의 머신은 보호됩니다. 새 회계원을 고용하는 경우 새 머신을 그룹에 수동으로 추가해야 합니다.
- **동적 그룹**

  동적 그룹에는 그룹을 생성할 때 지정한 검색 조건에 따라 자동으로 추가된 머신이 포함됩니다. 동적 그룹 내용은 자동으로 변경됩니다. 머신은 지정된 기준에 부합하는 동안 그룹에 남아 있습니다.

  예 1: 회계 부서에 속한 머신의 호스트 이름에는 단어 "accounting"이 포함됩니다. 부분 머신 이름을 그룹 구성원 자격 기준으로 지정하고 보호 계획을 이 그룹에 적용하면 됩니다. 새 회계원을 고용하는 경우 등록되는 즉시 새 머신이 그룹에 추가되므로 자동으로 보호됩니다.

예 2: 회계 부서는 별도의 Active Directory 조직 단위(OU)를 만듭니다. 회계 OU를 그룹 구성원 자격 기준으로 지정하고 보호 계획을 이 그룹에 적용하면 됩니다. 새 회계원을 고용하는 경우 등록되는 즉시 새 머신이 그룹과 OU(순서는 상관없음)에 추가되므로 자동으로 보호됩니다.

정적 그룹 생성

1. **장치**를 클릭하고 정적 그룹을 생성할 장치가 포함된 기본 제공 그룹을 선택합니다.
2. 그룹을 생성하려는 그룹 옆의 기어 아이콘을 클릭합니다.
3. **새 그룹**을 클릭합니다.
4. 그룹 이름을 지정하고 **확인**을 클릭합니다.
   새 그룹이 그룹 트리에 나타납니다.

정적 그룹에 장치 추가

1. **장치**를 클릭하고 그룹에 추가할 장치를 선택합니다.
2. **그룹에 추가**를 클릭합니다.
   소프트웨어에서 선택된 장치를 추가할 수 있는 그룹 트리를 표시합니다.
3. 새 그룹을 생성하려면 다음을 수행합니다. 그렇지 않은 경우 이 단계를 건너뜁니다.
   a. 그룹을 생성하려는 그룹을 선택합니다.
   b. **새 그룹**을 클릭합니다.
   c. 그룹 이름을 지정하고 **확인**을 클릭합니다.
4. 장치를 추가할 그룹을 선택하고 **완료**를 클릭합니다.

그룹을 선택하여 **장치 추가**를 클릭하여 정적 그룹에 장치를 추가하는 방법도 있습니다.

동적 그룹 생성

1. **장치**를 클릭하고 동적 그룹을 생성할 장치가 포함된 그룹을 선택합니다.
2. 검색 필드를 사용하여 장치를 검색합니다. 아래 설명된 여러 속성 및 연산자를 사용할 수 있습니다.
3. 검색 필드 옆의 **다른 이름으로 저장**을 클릭합니다.

   참고
   일부 속성은 그룹 생성에 대해 지원되지 않습니다. 아래 검색 쿼리 섹션의 표를 참조하십시오.

4. 그룹 이름을 지정하고 **확인**을 클릭합니다.

검색 쿼리

다음 표에는 검색 쿼리에서 사용 가능한 속성이 요약되어 있습니다.

속성	의미	검색 쿼리 예제	그룹 생성 지원
name	• 실제 머신의 호스트 이름 • 가상 머신의 이름 • 데이터베이스 이름 • 사서함의 이메일 주소	name = 'en-00'	예
parameters.MacAddress	MAC 주소.	parameters.MacAddress LIKE '00-22-4D-50-25-E5'	예

comment	장치에 대한 주석. 자동이나 수동으로 지정할 수 있습니다.
	기본값:
	• Windows를 실행하는 실제 머신의 경우 Windows의 컴퓨터 설명이 주석으로 자동 복사됩니다. 이 값은 15분마다 동기화됩니다.
	• 다른 장치의 경우 비어 있습니다.
	참고
	주석 필드에 수동으로 텍스트를 추가한 경우 Windows 설명과의 자동 동기화는 비활성화됩니다. 자동 동기화를 다시 활성화하려면 추가한 주석을 지우십시오.
	장치의 자동 동기화된 주석 필드를 새로 고치려면 **Windows 서비스**에서 Managed Machine Service를 다시 시작하거나 명령 프롬프트에서 다음 명령을 실행합니다.
	`net stop mms`
	`net start mms`
		comment = 'important machine'
		comment = ''(주석 없는 모든 머신)
			예

속성	의미	검색 쿼리 예제	그룹 생성 지원
	주석을 보려면 **장치**에서 해당 장치를 선택하고 **상세정보**를 클릭한 다음 **주석** 섹션으로 이동합니다. 주석을 추가하거나 변경하려면 **추가** 또는 **편집**을 클릭합니다. 보호 에이전트가 설치된 장치에는 주석 필드 2개가 있습니다. • 에이전트 주석 ◦ Windows를 실행하는 실제 머신의 경우 Windows의 컴퓨터 설명이 주석으로 자동 복사됩니다. 이 값은 15분마다 동기화됩니다. ◦ 다른 장치의 경우 비어 있습니다. **참고** 주석 필드에 수동으로 텍스트를 추가한 경우 Windows 설명과의 자동 동기화는 비활성화됩니다. 자동 동기화를 다시 활성화하려면 추가한 주석을 지우십시오. • 장치 주석 ◦ 자동으로 지정된 에이전트 주석은 장치 주석으로 복사됩니다. 수동으로 추가한 에이전트 주석은 장치 주석으로 복사되지 않습니다. ◦ 장치 주석은 에이전트 주석으로 복사되지 않습니다.		

속성	의미	검색 쿼리 예제	그룹 생성 지원
	각 장치에서는 두 주석 중 하나 이상을 지정할 수도 있고 두 주석을 모두 비워 둘 수도 있습니다. 두 주석을 모두 지정하면 장치 주석이 우선적으로 사용됩니다. 에이전트 주석을 보려면 **장치** > **에이전트**에서 에이전트가 설치된 장치를 선택하고 **세부 사항**을 클릭한 다음 **주석** 섹션을 찾습니다. 장치 주석을 보려면 **장치**에서 해당 장치를 선택하고 **상세정보**를 클릭한 다음 **주석** 섹션을 찾습니다. 주석을 수동으로 추가하거나 변경하려면 **추가** 또는 **편집**을 클릭합니다.		
ip	IP 주소(물리적인 머신만 해당).	ip RANGE ('10.250.176.1','10.250.176.50')	예
cpuArch	CPU 아키텍처. 가능한 값: • 'x64' • 'x86'	cpuArch = 'x64'	예
memorySize	RAM 크기(MiB(메가바이트) 단위).	memorySize < 1024	예
cpuName	CPU 이름.	cpuName LIKE '%XEON%'	예
insideVm	에이전트가 포함된 가상 머신. 가능한 값: • true • false	insideVm = true	예
tzOffset	머신 시간대 오프셋(분).	tzOffset = 120	예

속성	의미	검색 쿼리 예제	그룹 생성 지원
parameters.Architecture	운영 체제 아키텍처. 가능한 값: • 'x86' • 'x64'	parameters.Architecture = 'x86'	예
osName	운영 체제 이름.	osName LIKE '%Windows XP%'	예
osType	운영 체제 유형. 가능한 값: • 'windows' • 'linux' • 'macosx'	osType IN ('linux', 'macosx')	예
osProductType	운영 체제 제품 유형. 가능한 값: • 'dc' 도메인 컨트롤러를 나타냅니다. • 'server' • 'workstation'	osProductType = 'server'	예
virtualType	가상 머신 유형. 가능한 값: • 'vmwesx' VMware 가상 머신. • 'mshyperv' Hyper-V 가상 머신. • 'pcs' Virtuozzo 가상 머신. • 'hci' Virtuozzo Hybrid Infrastructure 가상 머신. • 'scale' Scale Computing HC3 가상 머신. • 'ovirt' oVirt 가상 머신	virtualType = 'vmwesx'	예

속성	의미	검색 쿼리 예제	그룹 생성 지원
osSp	운영 체제 서비스 팩.	osSp = 1	예
osVersionMajor	운영 체제의 주 버전.	osVersionMajor = 1	예
osVersionMinor	운영 체제의 부 버전.	osVersionMminor = 1	예
isOnline	머신 가용성. 가능한 값: • true • false	isOnline = true	아니요
tenant	장치가 속한 단위의 이름.	tenant = 'Unit 1'	예
tenantId	장치가 속한 단위의 식별자. 단위 ID를 확인하려면 **장치**에서 장치를 선택하고 **상세정보** > **모든 속성**을 클릭합니다. ID가 ownerId 필드에 표시됩니다.	tenantId = '3bfe6ca9-9c6a-4953-9cb2-a1323f454fc9'	예
state	장치 상태. 가능한 값: • 'idle' • 'interactionRequired' • 'canceling' • 'backup' • 'recover' • 'install' • 'reboot' • 'failback' • 'testReplica' • 'run_from_image' • 'finalize' • 'failover' • 'replicate' • 'createAsz' • 'deleteAsz' • 'resizeAsz'	state = 'backup'	아니요
status	리소스 상태.	status = 'ok'	아니요

속성	의미	검색 쿼리 예제	그룹 생성 지원
	가능한 값: • 'notProtected' • 'ok' • 'warning' • 'error' • 'critical'		
protectedByPlan	제공된 ID를 가진 보호 계획으로 보호되는 장치입니다. 계획 ID를 확인하려면 **계획** > **백업**을 클릭하고, 계획을 선택하고, **상태** 열에서 다이어그램을 클릭하고, 상태를 클릭합니다. 계획 ID를 가진 새 검색이 생성됩니다.	protectedByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
okByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **정상** 상태인 장치입니다.	okByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
errorByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **오류** 상태인 장치입니다.	errorByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
warningByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **경고** 상태인 장치입니다.	warningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
runningByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **실행 중** 상태인 장치입니다.	runningByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
interactionByPlan	제공된 ID를 가진 보호 계획으로 보호되며 **상호 작용 필요** 상태인 장치입니다.	interactionByPlan = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	아니요
ou	지정된 Active Directory 조직 단위에 속한 머신	ou IN ('RnD', 'Computers')	예
id	장치 ID. 장치 ID를 확인하려면 **장치**	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'	예

속성	의미	검색 쿼리 예제	그룹 생성 지원
	에서 장치를 선택하고 **상세정보** > **모든 속성**을 클릭합니다. ID가 `id` 필드에 표시됩니다.		

`lastBackupTime`	마지막으로 성공한 백업의 날짜 및 시간.
	형식은 `'YYYY-MM-DD HH:MM'` 입니다.
		`lastBackupTime > '2022-03-11'`
		`lastBackupTime <= '2022-03-11 00:15'`
		`lastBackupTime is null`
			아니요

`lastBackupTryTime`	마지막 백업 시도 시간. 형식은 `'YYYY-MM-DD HH:MM'` 입니다.	`lastBackupTryTime >= '2022-03-11'`	아니요
`nextBackupTime`	다음 백업 시간. 형식은 `'YYYY-MM-DD HH:MM'` 입니다.	`nextBackupTime >= '2022-08-11'`	아니요
`agentVersion`	설치된 보호 에이전트의 버전입니다.	`agentVersion LIKE '12.0.*'`	예
`hostId`	보호 에이전트의 내부 ID입니다. 보호 에이전트 ID를 확인하려면 **장치**에서 머신을 선택하고 **상세 정보** > **모든 속성**을 클릭합니다. `agent` 속성의 `"id"` 값을 사용합니다.	`hostId = '4B2A7A93-A44F-4155-BDE3-A023C57C9431'`	예
`resourceType`	리소스 유형. 가능한 값: • `'machine'` • `'virtual_machine.vmwesx'` • `'virtual_machine.mshyperv'` • `'virtual_machine.rhev'` • `'virtual_machine.kvm'` • `'virtual_machine.xen'`	`resourceType = 'machine'` `resourceType in ('mssql_aag_database', 'mssql_database')`	예
`hasAsz`	AcronisSecure Zone이(가)	`hasAsz=true`	예

속성	의미	검색 쿼리 예제	그룹 생성 지원
	설치된 실제 머신의 보호 에이전트. 가능한 값: • true • false		
chassis	머신 섀시 유형. 가능한 값: • unknown • laptop • desktop • server • other	chassis='laptop'	예

참고
시간 및 분 값을 건너뛸 경우, 시작 시간은 YYYY-MM-DD 00:00, 종료 시간은 YYYY-MM-DD 23:59:59인 것으로 간주됩니다.예를 들어, lastBackupTime = 2020-02-20은 검색 결과에 lastBackupTime >= 2020-02-20 00:00 및
lastBackup time <= 2020-02-20 23:59:59 사이의 백업을 모두 포함한다는 의미입니다.

연산자

다음 표에는 사용 가능한 연산자가 요약되어 있습니다.

연산자	의미	예
AND	논리적 결합 연산자.	name like 'en-00' AND tenant = 'Unit 1'
OR	논리적 분리 연산자.	state = 'backup' OR state = 'interactionRequired'
IN (<value1>,... <valueN>)	이 연산자는 식이 값 목록의 값과 일치하는지 테스트하는 데 사용됩니다.	osType IN ('windows', 'linux')
NOT	논리적 부정 연산자.	NOT(osProductType = 'workstation')
NOT IN (<value1>,... <valueN>)	IN 연산자와 반대의 연산자.	NOT osType IN ('windows', 'linux')
LIKE 'wildcard pattern'	이 연산자는 식이 와일드카드 패턴과 일치하는지 테스트하는 데 사용됩니다.	name LIKE 'en-00' name LIKE '*en-00'

연산자	의미	예
	다음 와일드카드 연산자를 사용할 수 있습니다. • * 또는 % 별표 및 퍼센트 기호는 0, 1 또는 여러 문자를 나타냅니다. • _ 밑줄은 단일 문자를 나타냅니다.	name LIKE '*en-00*' name LIKE 'en-00_'
RANGE(<starting_value>, <ending_value>)	이 연산자는 식이 값 범위 내에 있는지(포함) 테스트하는 데 사용됩니다.	ip RANGE ('10.250.176.1','10.250.176.50')
= or ==	*같음* 연산자.	osProductType = 'server'
!= 또는 <>	*같지 않음* 연산자.	id != '4B2A7A93-A44F-4155-BDE3-A023C57C9431'
<	*보다 작음* 연산자.	memorySize < 1024
>	*보다 큼* 연산자.	diskSize > 300GB
<=	*보다 작음 또는 같음* 연산자.	lastBackupTime <= '2022-05-11 00:15'
>=	*보다 큼 또는 같음* 연산자.	nextBackupTime >= '2022-09-11'

그룹에 보호 계획 적용

1. **장치**를 클릭하고 보호 계획을 적용할 그룹이 포함된 기본 제공 그룹을 선택합니다.
   소프트웨어에 자식 그룹 목록이 표시됩니다.
2. 보호 계획을 적용할 그룹을 선택합니다.
3. **그룹 백업**을 클릭합니다.
   소프트웨어에 그룹에 적용할 수 있는 보호 계획 목록이 표시됩니다.
4. 다음 중 하나를 수행하십시오.
   - 기존 보호 계획을 확장하고 **적용**을 클릭합니다.
   - **새로 만들기**를 클릭한 다음, "백업"에 설명된 대로 새 보호 계획을 생성합니다.

모니터링 및 보고

개요 대시보드에서는 보호 인프라의 현재 상태를 모니터링할 수 있습니다.

보고서 섹션에서는 보호 인프라에 대한 주문형 및 스케줄된 보고서를 생성할 수 있습니다. 이 섹션은 고급 라이센스가 있어야 사용 가능합니다.

개요 대시보드

개요 대시보드에서는 보호 인프라의 개요를 제공하는 많은 사용자 정의 가능한 위젯을 제공합니다. 원형 차트, 표, 그래프, 막대 차트 및 목록으로 제공되는 20개 넘는 위젯 중에서 선택할 수 있습니다. 위젯에는 문제를 조사하고 해결하는 데 사용되는 클릭 가능한 요소가 있습니다. 위젯 내 정보는 5분마다 업데이트됩니다.

고급 라이센스를 사용하면 대시보드의 현재 상태를 다운로드하거나 이메일을 통해 .pdf 및/또는 .xlsx 형식으로 보낼 수도 있습니다. 이메일을 통해 대시보드를 보내려면 이메일 서버 설정이 구성되었는지 확인하십시오.

사용 가능한 위젯은 Cyber Protect 버전에 따라 다릅니다. 기본 위젯에 포함되어 있는 항목:

위젯	가용성	설명
사이버 보호	Cyber Backup 에디션에서 사용할 수 없음	백업 크기, 차단된 맬웨어, 차단된 URL, 발견한 취약성, 설치된 패치 등의 전반적인 정보를 보여줍니다.
보호 상태	모든 에디션에서 사용 가능	모든 머신에 대한 현재 보호 상태를 표시합니다.
작업	모든 에디션에서 사용 가능	지정된 기간 동안 수행된 테이프 작업에 대한 요약 정보를 표시합니다.
활성 경보 요약	모든 에디션에서 사용 가능	경보 유형과 심각도에 따라 활성 경보에 대한 요약 정보를 표시합니다.
패치 설치 상태	Cyber Backup 에디션에서 사용할 수 없음	패치 설치 상태에 따라 그룹으로 지정된 머신의 수를 표시합니다.
카테고리별 누락 업데이트	Cyber Backup 에디션에서 사용할 수 없음	누락된 업데이트 수를 카테고리에 따라 표시합니다.
디스크 상태	Cyber Backup 에디션에서 사용할 수 없음	상태별 디스크의 개수를 보여줍니다.
장치	모든 에디션에서 사용 가능	사용자 환경의 장치에 대한 자세한 정보를 보여줍니다.
활성 경보 세부 정보	모든 에디션에서 사용 가능	활성 경보에 대한 자세한 정보를 표시합니다.
기존 취약성	모든 에디션에서 사용	사용자 환경 및 영향을 받는 머신에서 운영체제와 애플리케이

	가능	션에 이미 존재하는 취약성의 목록을 보여줍니다.
패치 설치 내역	Cyber Backup 에디션에서 사용할 수 없음	설치된 패치에 대한 자세한 정보를 표시합니다.
최근 영향 받은 항목	모든 에디션에서 사용 가능	최근 감염된 머신에 대한 자세한 정보를 표시합니다.
위치 요약	모든 에디션에서 사용 가능	백업 위치에 대한 자세한 정보를 표시합니다.

위젯을 추가하려면:

위젯 추가를 클릭한 다음, 다음 중 하나를 수행합니다.

- 추가할 위젯을 클릭합니다. 위젯이 기본 설정으로 추가됩니다.
- 추가하기 전에 위젯을 편집하려면 위젯이 선택된 상태에서 연필 아이콘을 클릭합니다. 위젯을 편집한 후 **완료**를 클릭합니다.

대시보드에서 위젯을 재정렬하려면:

이름을 클릭하여 위젯을 끌어서 놓습니다.

위젯을 편집하려면:

위젯 이름 옆의 연필 아이콘을 클릭합니다. 위젯을 편집하면 이름 바꾸기, 시간 범위 변경 및 필터 및 그룹 행 설정이 가능합니다.

위젯을 제거하려면:

위젯 이름 옆의 X 기호를 클릭합니다.

Cyber Protection

이 위젯은 백업 크기, 차단된 맬웨어, 차단된 URL, 발견한 취약성, 설치된 패치 등의 전반적인 정보를 보여줍니다.

상단 행에는 현재 통계가 표시됩니다.

- **오늘 백업됨** – 지난 24시간에 해당하는 복구 지점의 전체 크기
- **맬웨어 차단됨** – 차단된 맬웨어에 대한 현재 활성 경보의 수
- **차단된 URL** – 차단된 URL에 대한 현재 활성 경보의 수
- **기존 취약성** – 현재 존재하는 취약성의 수
- **패치 설치 준비 완료** – 현재 설치 가능한 패치의 수

하단 행에는 전체 통계가 표시됩니다.

- 모든 백업의 압축된 크기
- 모든 머신 전반에서 차단된 맬웨어의 누적 수
- 모든 머신 전반에서 차단된 URL의 누적 수

- 모든 머신 전반에서 검색된 취약성의 누적 수
- 모든 머신 전반에서 설치된 업데이트/패치의 누적 수

보호 상태

보호 상태

이 위젯은 모든 머신에 대한 현재 보호 상태를 표시합니다.

머신은 다음과 같은 상태일 수 있습니다.

- **보호됨** – 보호 계획이 적용되어 있는 머신입니다.
- **보호되지 않음** – 보호 계획이 적용되어 있지 않은 머신입니다. 여기에는 보호 계획이 적용되지 않은 검색된 머신 및 관리 대상 상태의 머신이 모두 포함됩니다.
- **관리 대상** – 보호 에이전트가 설치되어 있는 머신입니다.
- **검색됨** – 보호 에이전트가 설치되어 있지 않은 머신입니다.

머신 상태를 클릭하면 해당 상태의 머신 목록으로 리디렉션되어 자세한 정보를 확인할 수 있습니다.

검색된 머신

이 위젯은 지정한 기간 동안 검색된 머신 목록을 표시합니다.

디스크 상태 모니터링

디스크 상태 모니터링에서는 현재 디스크 상태 관련 정보 및 상태 예측 정보를 제공합니다. 따라서 디스크 오류와 관련하여 발생할 수 있는 데이터 손실을 방지할 수 있습니다. HDD 및 SSD 디스크가 모두 지원됩니다.

제한:

- 디스크 상태 예측은 Windows를 실행하는 머신에 대해서만 지원됩니다.
- 실제 머신의 디스크만 모니터링됩니다. 가상 머신의 디스크는 모니터링할 수 없으며 디스크 상태 위젯에 표시되지 않습니다.
- RAID 구성은 지원되지 않습니다.
- NVMe 드라이브에서는 Windows API를 통해 SMART 데이터를 전송하는 드라이브에 대해서만 디스크 상태 모니터링이 지원됩니다. 드라이브에서 SMART 데이터를 직접 읽어야 하는 NVMe 드라이브에서는 디스크 상태 모니터링이 지원되지 않습니다.

디스크 상태는 다음 중 하나로 표시됩니다.

- **정상**
  디스크 상태가 70~100%입니다.
- **경고**
  디스크 상태가 30~70% 사이입니다.
- **심각**
  디스크 상태가 0~30%입니다.

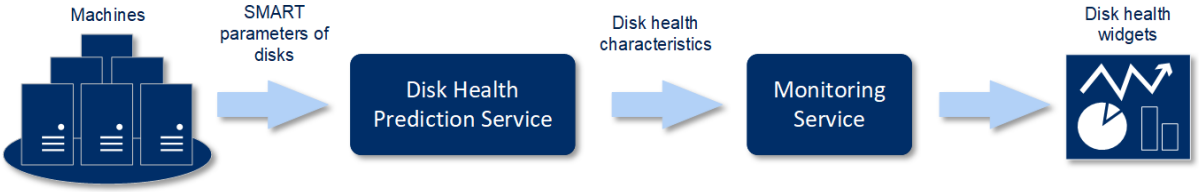
- **디스크 데이터 계산 중**
  현재 및 예측 디스크 상태를 계산하는 중입니다.

작동법

디스크 상태 예측 서비스는 AI 기반 예측 모델을 사용합니다.

1. 보호 에이전트는 디스크의 SMART 매개변수를 수집해 해당 데이터를 디스크 상태 예측 서비스로 전달합니다.
   - SMART 5 – 재할당된 섹터 수입니다.
   - SMART 9 – 가동 시간입니다.
   - SMART 187 – 수정할 수 없는 오류가 보고되었습니다.
   - SMART 188 – 명령 시간이 초과되었습니다.
   - SMART 197 – 현재 보류 중인 섹터 수입니다.
   - SMART 198 – 수정할 수 없는 오프라인 섹터 수입니다.
   - SMART 200 – 쓰기 오류 비율입니다.
2. 디스크 상태 예측 서비스는 수신한 SMART 매개변수를 처리하고, 예측하며, 다음과 같은 디스크 상태 특성을 제공합니다.
   - 디스크 현재 상태: 정상, 경고, 심각.
   - 디스크 상태 예측: 부정적, 안정적, 긍정적
   - 디스크 상태 예측 가능성을 백분율로 표시합니다.

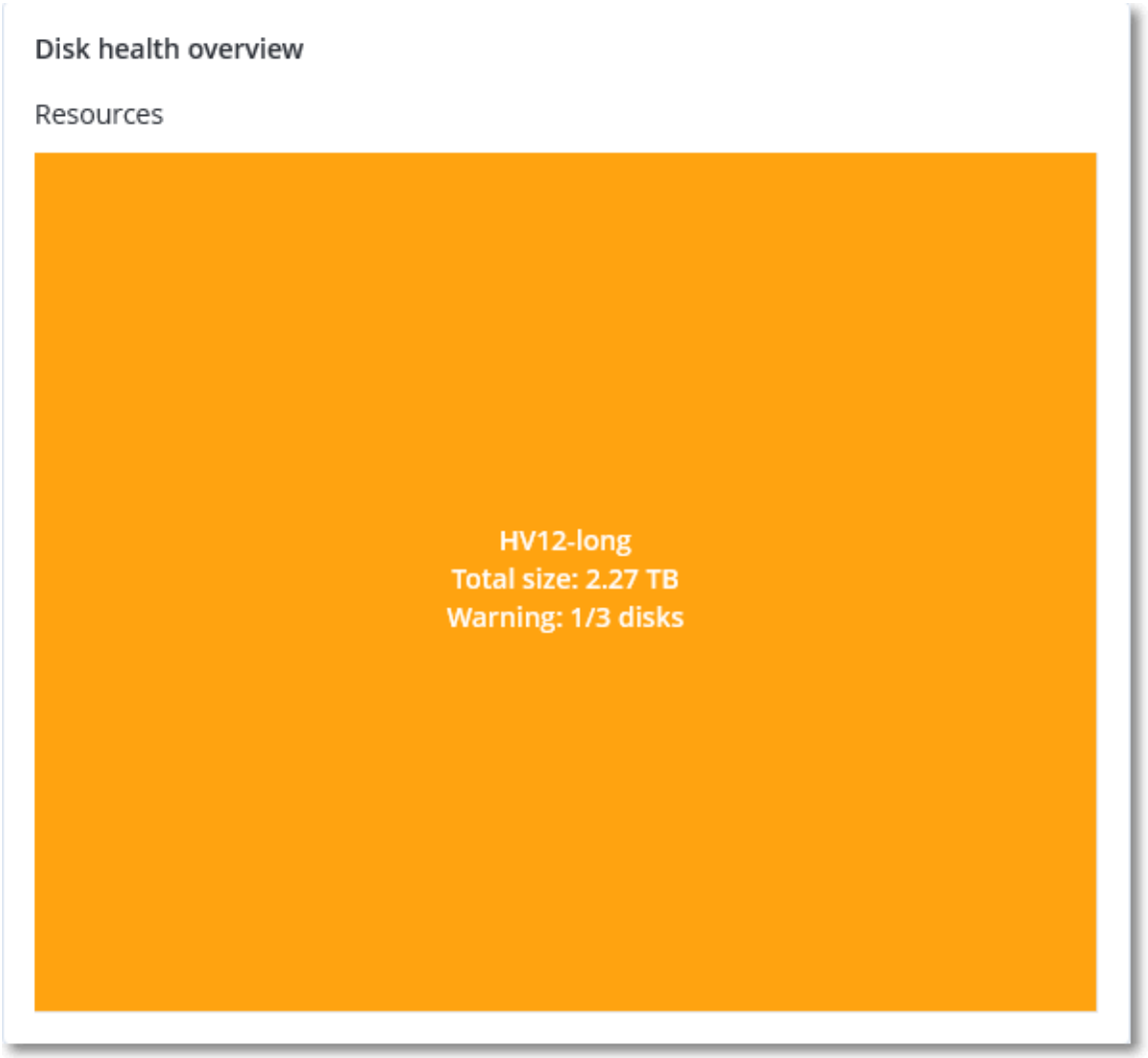
   예측 기간은 항상 1개월입니다.
3. 모니터링 서비스에서는 이러한 특성을 수신한 다음 Cyber Protect 웹 콘솔의 디스크 상태 위젯에 관련 정보를 표시합니다.



디스크 상태 위젯

디스크 상태 모니터링의 결과는 Cyber Protect 웹 콘솔에서 사용 가능한 다음 위젯에 표시됩니다.

- **디스크 상태 개요** – 트리맵 구조의 위젯으로, 드릴다운을 통해 두 수준의 세부 정보를 전환하며 확인할 수 있습니다.
  - 머신 수준
    선택한 조직 단위에 있는 모든 머신의 디스크 상태에 대한 요약 정보를 표시합니다. 가장 심각한 디스크 상태만 표시됩니다. 다른 상태는 특정 블록을 마우스로 가리켰을 때 도구 설명으로 표시됩니다. 머신 블록 크기는 머신의 총 디스크 크기에 따라 달라집니다. 머신 블록 색상은 발견된 중요 디스크 상태가 무엇인지에 따라 달라집니다.

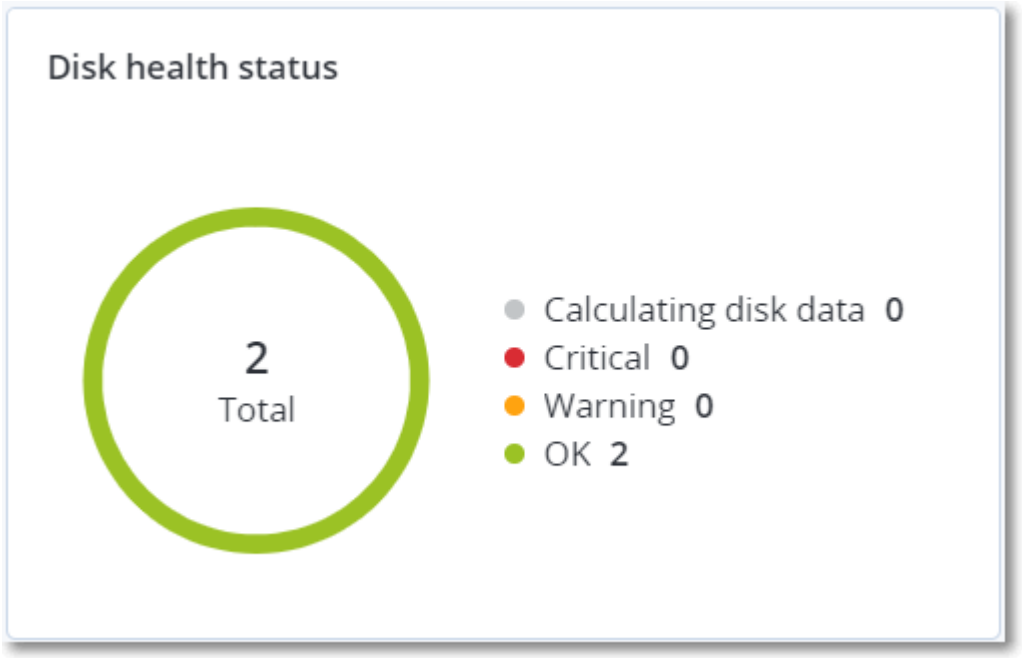


◦ 디스크 수준
선택한 머신에 있는 모든 디스크의 현재 상태를 표시합니다. 각 디스크 블록에는 다음 디스크 상태 예측 항목 중 하나와 해당 상태가 표시될 확률(비율)이 표시됩니다.

- 열화될 것으로 예측
- 안정적으로 유지될 것으로 예측

- 개선될 것으로 예측

- **디스크 상태** – 각 상태에 해당하는 디스크의 수를 원 그래프에 표시한 위젯입니다.



디스크 상태 경보

디스크 상태 확인은 30분마다 실행되고 해당 경보는 하루에 한 번 생성됩니다. 디스크 상태가 **경고**에서 **심각**으로 변경되면 항상 경보가 생성됩니다.

경보 이름	심각도	디스크 상태	설명
잠재적인 디스크 장애	경고	(30 – 70)	나중에 이 머신의 <디스크 이름> 디스크에 장애가 발생할 가능성이 높습니다. 가능한 한 빨리 이 디스크에 대한 전체 이미지 백업을 실행하고 디스크를 교체한 후, 새로운 디스크에 이미지를 복구하십시오.
디스크 장애 임박	심각	(0 – 30)	이 머신의 <디스크 이름> 디스크가 심각한 상태이며, 곧 장애가 발생할 가능성이 매우 높습니다. 추가적인 부담은 디스크 장애를 유발할 수 있으므로 현재 시점에서는 이 디스크에 대한 이미지 백업이 권장되지 않습니다. 즉시 이 디스크에서 가장 중요한 파일들을 백업한 후 디스크를 교체하십시오.

데이터 보호 맵

사용자는 데이터 보호 맵 기능을 통해 자신에게 중요한 모든 데이터를 발견하고 모든 중요 파일의 수, 크기, 위치, 보호 상태와 같은 자세한 정보를 확장 가능한 트리맵 보기로 확인할 수 있습니다.

각 블록 크기는 조직 단위/머신에 속한 모든 중요 파일의 총 수/크기에 따라 달라집니다.

파일의 보호 상태는 다음 중 하나로 표시됩니다.

- **심각** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 51~100%인 경우
- **낮음** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 21~50%인 경우
- **중간** – 선택한 머신/위치에 대해 기존 백업 설정으로 현재 또는 이후 백업되지 않도록 사용자가 지정한 확장자를 가진 파일 중 보호되지 않는 파일이 1~20%인 경우
- **높음** – 선택한 머신/위치에 대해 백업되지 않도록 사용자가 지정한 확장자를 가진 모든 파일이 보호되고 있는 경우

데이터 보호 조사 결과는 머신 수준의 세부 정보를 트리맵 구조로 표시하는 데이터 보호 맵 위젯의 대시보드에서 확인할 수 있습니다.

색깔 블록 위로 마우스를 가져가면 보호되지 않는 파일 수와 해당 파일의 위치와 같은 자세한 정보를 볼 수 있습니다. 이러한 파일을 보호하려면 **모든 파일 보호**를 클릭합니다.

취약성 평가 위젯

취약한 머신

이 위젯은 취약한 머신을 취약성 심각도에 따라 표시합니다.

CVSS(일반 취약성 점수 시스템) v3.0에 따라 취약성의 심각도 수준은 다음으로 나누어집니다.

- 보안됨: 발견된 취약성 없음
- 심각: 9.0 - 10.0 CVSS
- 높음: 7.0 - 8.9 CVSS
- 중간: 4.0 - 6.9 CVSS
- 낮음: 0.1 - 3.9 CVSS
- 없음: 0.0 CVSS

기존 취약성

이 위젯은 머신에 현재 존재하는 취약성을 표시합니다. **기존 취약성** 위젯에는 타임 스탬프를 보여주는 두 개의 열이 있습니다.

- **첫 번째로 감지됨** – 머신에서 처음으로 취약성이 감지된 날짜와 시간입니다.
- **마지막으로 감지됨** – 머신에서 마지막으로 취약성이 감지된 날짜와 시간입니다.

패치 설치 위젯

패치 설치 기능과 관련된 위젯은 4개입니다.

패치 설치 상태

이 위젯은 패치 설치 상태별로 그룹화된 머신 수를 표시합니다.

- **설치됨** – 사용 가능한 모든 패치가 머신에 설치되어 있음
- **재부팅 필요** – 패치 설치 후 재부팅이 필요한 머신
- **실패** – 머신에 패치 설치 실패

패치 설치 요약

이 위젯은 패치 내역을 패치 설치 상태로 요약하여 표시합니다.

패치 설치 내역

이 위젯은 머신에 설치된 패치에 대한 자세한 정보를 표시합니다.

카테고리별 누락 업데이트

이 위젯은 카테고리별 누락 업데이트의 수를 표시합니다. 다음과 같은 카테고리가 표시됩니다.

- 보안 업데이트
- 중요 업데이트
- 기타

백업 스캔 세부 정보

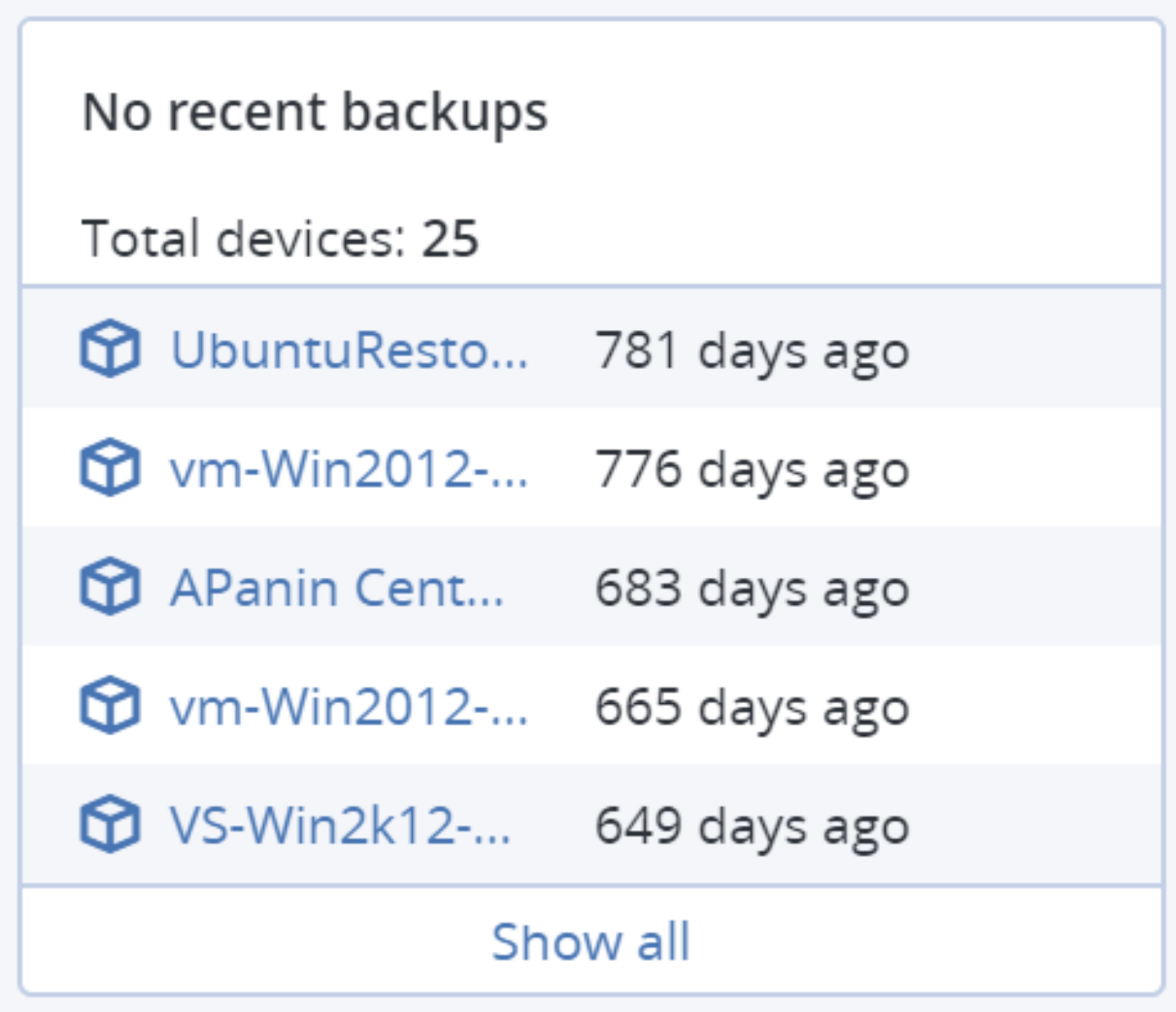
이 위젯은 스캔 서비스가 관리 서버에 설치된 경우에만 사용할 수 있습니다. 이 위젯은 백업에서 탐지된 위협에 대한 자세한 정보를 표시합니다.

최근 영향 받은 항목

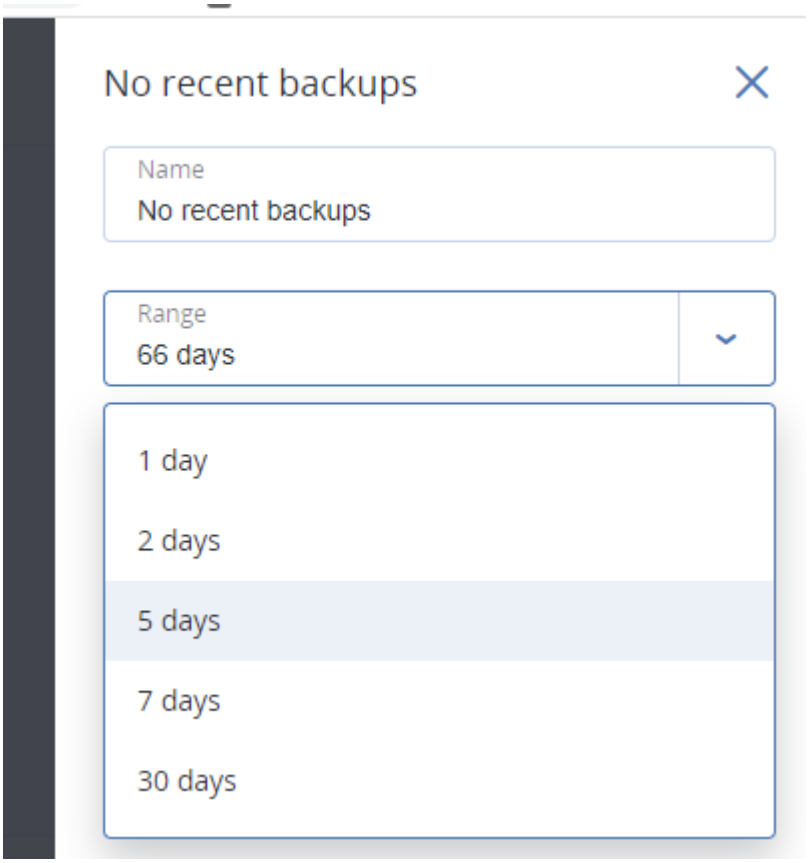
이 위젯은 최근 감염된 머신에 대한 자세한 정보를 표시합니다. 여기서 감지된 위협과 감염된 파일 개수에 대한 정보를 확인할 수 있습니다.

최근 백업 없음

이 위젯에는 보호 계획이 적용된 워크로드가 표시됩니다. 마지막으로 성공한 백업이 위젯 설정에 지정된 시간 범위보다 이전이었습니다.



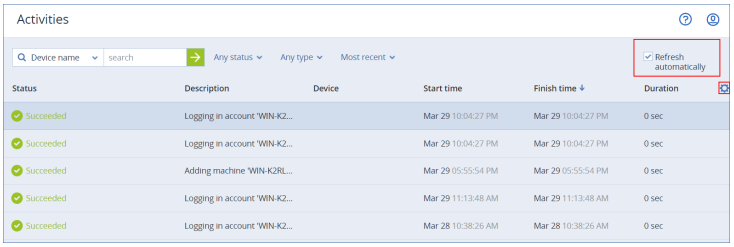
기본적으로 이 위젯을 추가하면 지난 5일 동안의 정보가 표시됩니다. 드롭다운 메뉴를 사용하여 다른 기간을 선택할 수도 있고, 일수를 직접 입력할 수도 있습니다. 입력할 수 있는 최대 일수는 180일입니다.



활동 탭

활동 탭에는 지난 90일 동안 활동의 개요가 나와 있습니다.

활동 탭의 보기를 사용자 지정하려면 기어 아이콘을 클릭하고 확인하려는 열을 선택합니다. 활동 진행률을 실시간으로 확인하려면 **자동 새로 고침** 확인란을 선택합니다. 여러 활동을 자주 업데이트하면 관리 서버의 성능이 저하될 수 있습니다.



나열된 활동은 다음 기준으로 검색할 수 있습니다.

- **장치 이름**
  활동이 수행되는 머신입니다.
- **시작한 사람**
  활동을 시작한 계정입니다.

다음 속성을 기준으로 작업을 필터링할 수도 있습니다.

- **상태**
  성공, 실패, 진행 중, 취소 등의 상태가 설정됩니다.
- **유형**
  계획 적용, 백업 삭제, 소프트웨어 업데이트 설치 등의 유형이 적용됩니다.
- **시간**
  예: 최신 활동, 24시간 전부터 발생한 활동 또는 기본 보관 기간 내 특정 기간 동안의 활동

기본 보존 기간을 변경하려면 task_manager.yaml 구성 파일을 편집합니다.

보관 기간을 변경하려면

1. 관리 서버를 실행하는 머신의 텍스트 편집기에서 다음 구성 파일을 엽니다.
   - Windows: `%Program Files%\Acronis\TaskManager\task_manager.yaml`
   - Linux: `/usr/lib/Acronis/TaskManager/task_manager.yaml`
2. 다음 섹션을 찾습니다.

```
database:
  connection-string: ""
  run-cleanup-at: "23:59"
  cleanup-batch-size: 10
  max-cleanup-retries: 10
  log-queries: false
  max-transaction-retries: 10
  shards:
   - connection-string: sqlite://task-manager.sqlite
     days-to-keep: 90
     space: "default"
     key: "00000000-0000-0000-0000-000000000000"
```

3. `days-to-keep` 행을 원하는 대로 편집합니다.
   예:

```
days-to-keep: 30
```

   참고
   필요에 따라 보존 기간을 변경할 수 있습니다. 보관 기간을 늘리면 관리 서버의 성능이 저하됩니다.

4. 에 설명된 대로 **Acronis Service Manager 서비스**를 다시 시작합니다.

보고

미리 정의된 보고서를 사용하거나 사용자 정의 보고서를 생성할 수 있습니다. 보고서에는 모든 대시보드 위젯 집합을 포함할 수 있습니다.

사용자가 관리하는 단위에 대한 보고서만 구성할 수 있습니다.

보고서는 이메일을 통해 보내거나 스케줄에 따라 다운로드할 수 있습니다. 이메일을 통해 보고서를 보내려면 **이메일 서버** 설정이 구성되었는지 확인하십시오. 서드 파티 소프트웨어를 사용하여 보고서를 처리하려면 보고서를 .xlsx 형식으로 특정 폴더에 저장하도록 스케줄하십시오.

사용 가능한 보고서는 Cyber Protect 버전에 따라 다릅니다. 기본 보고서에 포함되어 있는 항목:

보고서 이름	가용성	설명
경보	Cyber Backup Advanced Cyber Protect Advanced	지정된 기간 동안 발생한 경보를 표시합니다.
백업 스캔 세부 정보	Cyber Protect Advanced	백업에서 감지된 위협에 대한 자세한 정보를 표시합니다.
백업	Cyber Backup Advanced Cyber Protect Advanced	현재 백업 및 복구 지점에 대한 세부정보를 표시합니다.
현재 상태	Cyber Backup Advanced Cyber Protect Advanced	사용자 환경의 현재 상태를 표시합니다.
일일 작업	Cyber Backup Advanced Cyber Protect Advanced	지정된 기간 동안 수행된 테이프 작업에 대한 요약 정보를 표시합니다.
데이터 보호 맵	Cyber Protect Advanced	머신에 있는 모든 중요 파일의 수, 크기, 위치, 보호 상태에 대한 자세한 정보를 표시합니다.
감지된 위협	Cyber Backup Advanced Cyber Protect Advanced	차단된 위협의 수, 양호한 머신 및 취약한 머신에 대한 정보를 통해 감염된 머신에 대한 자세한 정보를 표시합니다.
검색된 머신	Cyber Backup Advanced Cyber Protect Advanced	조직 네트워크에서 발견된 모든 머신을 표시합니다.
디스크 상태 예측	Cyber Protect Advanced	HDD/SDD가 고장 나게 되는 시기에 대한 예측 정보와 현재 디스크 상태를 표시합니다.
기존 취약성	Cyber Backup	사용자 환경 및 영향을 받는 머신에서 운영체제와 애플리

	Advanced Cyber Protect Advanced	케이션에 이미 존재하는 취약성의 목록을 보여줍니다.
라이센스	Cyber Backup Advanced Cyber Protect Advanced	사용 가능한 라이센스의 요약 정보를 표시합니다.
위치	Cyber Backup Advanced Cyber Protect Advanced	지정된 시간 동안 백업 위치의 사용 통계를 표시합니다.
패치 관리 요약	Cyber Protect Advanced	누락된 패치, 설치된 패치, 적용 가능한 패치의 수를 목록으로 보여줍니다. 이 보고서를 자세히 살펴보면 모든 시스템의 세부정보 및 누락/설치된 패치 정보를 확인할 수 있습니다.
요약	Cyber Backup Advanced Cyber Protect Advanced	지정된 기간 동안 보호되는 장치에 대한 요약 정보를 표시합니다.
테이프 작업	Cyber Backup Advanced Cyber Protect Advanced	지난 24시간 동안 사용된 테이프 목록을 표시합니다.
주간 작업	Cyber Backup Advanced Cyber Protect Advanced	지정된 기간 동안 수행된 테이프 작업에 대한 요약 정보를 표시합니다.

보고서 관련 기본 작업

- 보고서를 보려면 보고서 이름을 클릭합니다.
- 보고서가 있는 추가 작업을 보려면 말줄임표 아이콘(...)을 클릭합니다.
  동일한 작업을 보고서 내에서 사용할 수 있습니다.

보고서를 추가하는 방법

1. **보고서 추가**를 클릭합니다.
2. 다음 중 하나를 수행하십시오.

- 미리 정의된 보고서를 추가하려면 보고서 이름을 클릭합니다.
- 사용자 정의 보고서를 추가하려면 **사용자 정의**를 클릭합니다. 이름이 **사용자 정의**인 새 보고서가 보고서 목록에 추가됩니다. 이 보고서를 열고 여기에 위젯을 추가합니다.

3. [선택 사항] 위젯을 끌어서 놓아서 재정렬합니다.
4. [선택 사항] 아래에 설명된 대로 보고서를 편집합니다.

보고서를 편집하는 방법

1. 보고서 이름 옆에 있는 말줄임표 아이콘(...)을 클릭한 다음 **설정**을 클릭합니다.
2. 보고서를 편집합니다. 다음을 수행할 수 있습니다.
   - 보고서 이름 변경
   - 보고서에 포함된 모든 위젯의 시간 범위 변경
   - .pdf 및/또는 .xlsx 형식으로 이메일을 통해 보고서를 전송하도록 예약
3. **저장**을 클릭합니다.

보고서를 예약하는 방법

1. 보고서를 선택하고 **스케줄**을 클릭합니다.
2. **스케줄된 보고서 보내기** 스위치를 활성화합니다.
3. 이메일을 통해 보고서를 보낼지, 폴더에 저장할지 또는 둘 다 수행할지 선택합니다. 선택에 따라 이메일 주소, 폴더 경로 또는 두 항목을 모두 지정합니다.
4. 보고서 형식을 선택합니다. .pdf, .xlsx 또는 둘 다.
5. 보고 기간을 선택합니다. 1일, 7일 또는 30일.
6. 보고서를 보내거나 저장할 일수 및 시간을 선택합니다.
7. **저장**을 클릭합니다.

보고서 구조 내보내기 및 가져오기

보고서 구조(위젯 집합 및 스케줄 설정)를 .json 파일로 내보내거나 가져올 수 있습니다. 관리 서버를 다시 설치하거나 보고서 구조를 다른 관리 서버로 복사하는 경우 이 방법이 유용할 수 있습니다.

보고서 구조를 내보내려면 보고서를 선택하고 **내보내기**를 클릭합니다.

보고서 구조를 가져오려면 **보고서 생성**을 클릭하고 **가져오기**를 클릭합니다.

보고서 데이터 덤프

보고서 데이터의 덤프를 .csv 파일로 저장할 수 있습니다. 덤프에는 사용자 정의 시간 범위에 대한 모든 보고서 데이터(필터링 없음)가 포함됩니다.

데이터 덤프가 즉시 생성됩니다. 긴 기간을 지정하면 이 작업에 시간이 오래 걸릴 수 있습니다.

보고서 데이터를 덤프하려면

1. 보고서를 선택하고 **열기**를 클릭합니다.
2. 오른쪽 위에서 말줄임표 아이콘(...)을 클릭하고 **데이터 덤프**를 클릭합니다.
3. **위치**에 .csv 파일의 폴더 경로를 지정합니다.

4. **시간 범위**에서 시간 범위를 지정합니다.
5. **저장**을 클릭합니다.

경보의 심각도 구성

경보는 실제 또는 잠재적 문제를 경고하는 메시지입니다. 경보는 다양한 방법으로 사용할 수 있습니다.

- **개요** 탭의 **경보** 섹션에서 현재 경보를 모니터링하여 문제를 빠르게 식별하고 해결할 수 있습니다.
- **장치** 아래에서 장치 상태는 경보에서 파생됩니다. **상태** 열을 사용하여 문제가 있는 장치를 필터링할 수 있습니다.
- 이메일 알림을 구성할 경우 알림을 트리거할 경보를 선택할 수 있습니다.

경보의 심각도는 다음 중 하나에 해당할 수 있습니다.

- **심각**
- **오류**
- **경고**

아래 설명된 대로 경보 구성 파일을 사용하여 경보의 심각도를 변경하거나 경보를 완전히 비활성화할 수 있습니다. 이 작업을 수행하려면 관리 서버를 다시 시작해야 합니다.

경보의 심각도를 변경해도 이미 생성된 경보에는 영향을 미치지 않습니다.

경보 구성 파일

구성 파일은 관리 서버를 실행하는 머신에 있습니다.

- Windows: `<installation_path>`**\AlertManager\alert_manager.yaml**
  여기서 `<installation_path>`는 관리 서버 설치 경로입니다. 기본 위치는 **%ProgramFiles%\Acronis**입니다.
- Linux: **/usr/lib/Acronis/AlertManager/alert_manager.yaml**

파일은 YAML 문서로 구조화됩니다. 각 경보는 `alertTypes` 목록에 있는 요소입니다.

`name` 키는 경보를 식별합니다.

`severity` 키는 경보 심각도를 정의합니다. 값은 `critical`, `error`, `warning` 중 하나여야 합니다.

선택 사항인 `enabled` 키는 경보가 활성화 또는 비활성화되는지 여부를 정의합니다. 해당 값은 `true` 또는 `false` 중 하나여야 합니다. 기본적으로(이 키 없음) 모든 경보가 활성화됩니다.

경보 심각도를 변경하거나 경보를 비활성화하려면

1. 관리 서버가 설치된 머신의 텍스트 편집기에서 **alert_manager.yaml** 파일을 엽니다.
2. 변경하거나 비활성화할 경보를 찾습니다.
3. 다음 중 하나를 수행하십시오.

- 경보 심각도를 변경하려면 `severity` 키의 값을 변경합니다.
- 경보를 비활성화하려면 `enabled` 키를 추가한 후 해당 값을 `false`로 설정합니다.

4. 파일을 저장합니다.
5. 아래 설명된 대로 관리 서버 서비스를 다시 시작합니다.

***Windows*에서 관리 서버 서비스를 다시 시작하려면**

1. **시작** 메뉴에서 **실행**을 클릭한 다음 **cmd**를 입력합니다.
2. **확인**을 클릭합니다.
3. 다음 명령 실행:

```
net stop acrmngsrv
net start acrmngsrv
```

***Linux*에서 관리 서버 서비스를 다시 시작하려면**

1. **터미널**을 엽니다.
2. 아무 디렉터리에서나 다음 명령을 실행합니다.

```
sudo service acronis_ams restart
```

고급 스토리지 옵션

테이프 장치

다음 섹션에서는 테이프 장치를 사용하여 백업을 저장하는 방법에 대해 자세히 설명합니다.

테이프 장치란 무엇입니까?

테이프 장치는 테이프 라이브러리 또는 독립형 테이프 드라이브를 의미하는 일반 용어입니다.

테이프 라이브러리(로봇 라이브러리)는 다음이 포함된 대용량 저장 장치입니다.

- 하나 이상의 테이프 드라이브
- 테이프를 수용하는 여러(최대 수천 개) 슬롯
- 슬롯과 테이프 드라이브 간에 테이프를 이동시키기 위한 하나 이상의 변경자(로봇 메커니즘).

바코드 판독기 또는 바코드 프린터와 같은 다른 컴퍼넌트도 포함될 수 있습니다.

오토로더는 특별한 형태의 테이프 라이브러리로, 하나의 드라이브, 여러 슬롯, 변경자 및 바코드 판독기(선택 사항)로 구성됩니다.

독립형 테이프 드라이브(**스트리머**라고도 함)에는 하나의 슬롯이 포함되며 한 번에 하나의 테이프만 보관할 수 있습니다.

테이프 지원 개요

보호 에이전트는 테이프 장치에 직접 또는 스토리지 노드를 통해 데이터를 백업할 수 있습니다. 두 가지 방법 모두 테이프 장치의 완전 자동 작업이 보장됩니다. 드라이브가 여러 개인 테이프 장치를 스토리지 노드에 연결하면 여러 에이전트를 동시에 테이프에 백업할 수 있습니다.

RSM 및 타사 소프트웨어와의 호환성

타사 소프트웨어와 함께 사용

독점 테이프 관리 도구를 사용하는 서드 파티 소프트웨어가 설치된 머신에서는 테이프를 사용할 수 없습니다. 그러한 머신에서 테이프를 사용하려면 서드 파티 관리 소프트웨어를 제거하거나 비활성화해야 합니다.

Windows RSM(이동식 저장소 관리자)과의 상호 작용

보호 에이전트와 스토리지 노드에서는 RSM을 사용하지 않습니다. 테이프 장치가 감지되면 백업 에이전트와 스토리지 노드가 RSM에서 해당 장치를 비활성화합니다(다른 소프트웨어에서 사용되지 않는 경우). 테이프 장치를 사용하려면 사용자 또는 서드 파티 소프트웨어가 RSM에서 장치를 활성화하지 않도록 하십시오. RSM에서 테이프 장치가 활성화된 경우 테이프 장치 검색을 반복하십시오.

지원되는 하드웨어

Acronis Cyber Protect은(는) 외장 SCSI 장치를 지원합니다. 이러한 장치는 파이버 채널(FC)에 연결되거나 SCSI, iSCSI, SAS(Serial Attached SCSI) 인터페이스를 사용하는 장치에 해당합니다. 또한 Acronis Cyber Protect은(는) USB 연결 테이프 장치를 지원합니다.

Windows에서는 장치 체인저 드라이버가 설치되지 않은 경우에도 Acronis Cyber Protect이(가) 테이프 장치에 백업할 수 있습니다. 이러한 테이프 장치는 **장치 관리자**에서 **알 수 없는 미디어 체인저**로 표시됩니다. 그러나 장치 드라이브의 드라이버는 설치해야 합니다. Linux 및 부트 가능한 미디어에서는 드라이버가 없는 테이프 장치에 백업할 수 없습니다.

IDE 또는 SATA 연결 장치의 인식은 보장할 수 없으며 운영 체제에 적절한 드라이브가 설치되었는지 여부에 따라 달라집니다.

특정 장치가 지원되는지 알아보려면 http://kb.acronis.com/content/57237의 설명에 따라 하드웨어 호환성 도구를 사용하십시오. Acronis(으)로 테스트 결과에 대한 보고서를 보내주시면 많은 도움이 됩니다. 지원이 확인된 하드웨어는 다음 하드웨어 호환성 목록에 나와 있습니다.
https://go.acronis.com/acronis-cyber-protect-advanced-tape-hcl

테이프 관리 데이터베이스

머신에 연결된 모든 테이프 장치에 대한 정보는 테이프 관리 데이터베이스에 저장됩니다. 기본 데이터베이스 경로는 다음과 같습니다.

- Windows XP/Server 2003: `%ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\ARSM\Database`
- Windows 7 이상 버전의 Windows: `%PROGRAMDATA%\Acronis\BackupAndRecovery\ARSM\Database`
- Linux: `/var/lib/Acronis/BackupAndRecovery/ARSM/Database`

데이터베이스 크기는 테이프에 저장된 백업의 수에 따라 다르며 100개 백업당 약 10MB입니다. 테이프 라이브러리에 수천 개의 백업이 포함되는 경우에는 데이터베이스 크기가 커질 수 있습니다. 이 경우 다른 볼륨에 테이프 데이터베이스를 저장할 수 있습니다.

Windows에서 데이터베이스 위치를 변경하려면:

1. Removable Storage Management 서비스를 중지합니다.
2. 모든 파일을 기본 위치에서 새 위치로 이동합니다.
3. 레지스트리 키 `HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\ARSM\Settings`를 찾습니다.
4. 레지스트리 값 `ArsmDmlDbProtocol`에 새 위치 경로를 지정합니다. 문자열에는 최대 32765자가 포함될 수 있습니다.
5. Removable Storage Management 서비스를 시작합니다.

Linux에서 데이터베이스 위치를 변경하려면:

1. `acronis_rsm` 서비스를 중지합니다.
2. 모든 파일을 기본 위치에서 새 위치로 이동합니다.
3. 텍스트 편집기에서 구성 파일 `/etc/Acronis/ARSM.config`를 엽니다.

4. <value name="ArsmDmlDbProtocol" type="TString"> 줄을 찾습니다.
5. 이 행 아래 경로를 변경합니다.
6. 파일을 저장합니다.
7. acronis_rsm 서비스를 시작합니다.

TapeLocation 폴더

TapeLocation 폴더에는 테이프에 백업된 모든 볼륨의 파일 시스템 메타데이터 캐시가 포함되어 있습니다.

기본 TapeLocation 폴더 경로는 다음과 같습니다.

- Windows XP/Server 2003: %ALLUSERSPROFILE%\Application Data\Acronis\BackupAndRecovery\TapeLocation
- Windows 7 이상: %PROGRAMDATA%\Acronis\BackupAndRecovery\TapeLocation
- Linux: /var/lib/Acronis/BackupAndRecovery/TapeLocation

TapeLocation 폴더 크기는 테이프에 저장된 모든 백업 크기의 0.5-1% 정도입니다. 파일 복구 옵션이 활성화된 디스크 수준 백업의 경우에는 백업된 파일 수에 따라 TapeLocation 폴더 크기가 약간 더 클 수도 있습니다.

테이프에 쓰기 위해 필요한 매개변수

테이프 쓰기 매개변수(블록 크기 및 캐시 크기)를 사용하면 최대 성능에 도달하도록 소프트웨어를 미세 조정할 수 있습니다. 테이프에 쓰려면 두 매개변수가 모두 필요하지만 일반적으로 블록 크기만 조정하면 됩니다. 가장 적절한 값은 테이프 장치 유형과 백업되는 데이터(예: 파일 수 및 파일 크기)에 따라 달라집니다.

참고
소프트웨어가 테이프에서 읽는 경우 테이프에 작성할 때 사용했던 것과 동일한 블록 크기를 사용합니다. 테이프 장치가 해당하는 블록 크기를 지원하지 않는 경우 읽기에 실패합니다.

이러한 매개변수는 연결된 테이프 장치가 있는 각 머신에서 설정됩니다. 이러한 머신은 에이전트 또는 스토리지 노드가 설치된 머신일 수 있습니다. Windows를 실행 중인 머신에서는 구성이 레지스트리에서 수행되며 Linux 머신에서는 구성 파일 **/etc/Acronis/BackupAndRecovery.config**에서 구성이 수행됩니다.

Windows에서 각 레지스트리 키와 해당하는 DWORD 값을 생성합니다. Linux에서는 구성 파일 끝 부분에 있는 </registry> 태그 바로 앞에 다음 텍스트를 추가합니다.

```
<key name="TapeLocation">
     <value name="WriteCacheSize" type="Dword">
          "value"
     </value>
     <value name=DefaultBlockSize" type="Dword">
          "value"
     </value>
</key>
```

DefaultBlockSize

테이프에 쓰는 경우 사용되는 블록 크기(단위: 바이트)입니다.

가능한 값: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576.

이 값이 0이거나 매개변수가 없는 경우 블록 크기는 다음과 같이 결정됩니다.

- Windows에서는 이 값을 테이프 장치 드라이버에서 가져옵니다.
- Linux에서는 이 값이 **64KB**입니다.

레지스트리 키(Windows를 실행 중인 머신): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\DefaultBlockSize**

/etc/Acronis/BackupAndRecovery.config의 행(Linux를 실행 중인 머신):

```
<value name=DefaultBlockSize" type="Dword">
     "value"
</value>
```

지정된 값을 테이프 드라이브에서 수락하지 않는 경우 소프트웨어에서는 적용 가능한 값이 되거나 32바이트가 될 때까지 이 값을 2로 나눕니다. 적용 가능한 값이 없는 경우 소프트웨어에서는 적용 가능한 값이 되거나 1MB가 될 때까지 지정된 값에 2를 곱합니다. 드라이버에서 값을 수락하지 않으면 백업에 실패합니다.

WriteCacheSize

테이프에 쓰는 경우 사용되는 버퍼 크기(단위: 바이트)입니다.

가능한 값: 0, 32, 64, 128, 256, 512, 1024, 2048, 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288, 1048576. 하지만 **DefaultBlockSize** 매개변수 값 미만일 수는 없습니다.

이 값이 0이거나 해당 매개변수가 없는 경우 버퍼 크기는 **1MB**입니다. 운영 체제에서 이 값을 지원하지 않으면 적용 가능한 값을 찾거나 **DefaultBlockSize** 매개변수 값에 도달할 때까지 이 값을 2로 나눕니다. 운영 체제에서 지원하는 값이 없으면 백업에 실패합니다.

레지스트리 키(Windows를 실행 중인 머신): **HKEY_LOCAL_MACHINE\SOFTWARE\Acronis\BackupAndRecovery\TapeLocation\WriteCacheSize**

/etc/Acronis/BackupAndRecovery.config의 행(Linux를 실행 중인 머신):

```
<value name="WriteCacheSize" type="Dword">
     "value"
</value>
```

운영 체제에서 지원하지 않는 0이 아닌 값을 지정하면 백업에 실패합니다.

테이프 관련 백업 옵션

테이프 관리 백업 옵션을 구성하여 다음을 결정할 수 있습니다.

- 테이프에 저장된 디스크 수준 백업으로부터의 파일 복구 활성화 여부.
- 보호 계획이 완료된 후 테이프를 다시 슬롯으로 반환할지 여부.
- 백업이 완료된 후 테이프를 꺼낼지 여부.
- 각 전체 백업에 대해 사용 가능 테이프를 사용할지 여부.
- 전체 백업 생성 시 테이프 덮어쓰기 여부(독립형 테이프 장치만 해당).
- 예를 들어 서로 다른 요일에 생성된 백업 또는 다양한 머신 유형의 백업에 사용되는 테이프를 구별하는 데 테이프 세트를 사용할지 여부.

병렬 작업

Acronis Cyber Protect은(는) 테이프 장치의 여러 컴퍼넌트에 대한 작업을 동시에 수행할 수 있습니다. 드라이브를 사용하는 작업(백업, 복구, 재스캐닝 또는 지우기) 중에 체인저를 사용하는 작업(다른 슬롯으로 테이프 이동 또는 테이프 꺼내기)을 시작할 수 있으며, 그 반대로 할 수도 있습니다. 테이프 라이브러리에 드라이브가 여러 개 있는 경우, 드라이브 중 하나를 사용하는 작업 도중 다른 드라이브를 사용하는 작업을 시작할 수도 있습니다. 예를 들어, 동일한 테이프 라이브러리의 다른 드라이브를 사용하여 여러 머신을 동시에 백업 또는 복구할 수 있습니다.

새 테이프 장치 감지 작업과 다른 작업을 동시에 수행할 수 있습니다. 인벤토리 작업 중에는 새 테이프 장치 감지 이외의 다른 작업을 수행할 수 없습니다.

동시에 수행할 수 없는 작업은 대기 상태가 됩니다.

제한 사항

테이프 장치 사용에 대한 제한 사항은 다음과 같습니다.

1. 머신을 32비트 Linux 기반 부트 가능한 미디어에서 부팅하는 경우 테이프 장치가 지원되지 않습니다.
2. 다음 데이터 유형은 테이프에 백업할 수 없습니다. Microsoft 365 사서함, Microsoft Exchange 사서함.
3. 실제 및 가상 머신의 애플리케이션 인식 백업을 생성할 수 없습니다.
4. macOS에서는 관리 테이프 기반 위치로의 파일 수준 백업만 지원됩니다.
5. 테이프에 있는 백업은 통합할 수 없습니다. 따라서 테이프에 백업할 경우 **항상 증분** 백업 구성표를 사용할 수 없습니다.
6. 테이프에 있는 백업은 중복을 제거할 수 없습니다.
7. 삭제되지 않은 백업이 포함되어 있거나 다른 테이프에 종속 백업이 있는 경우 소프트웨어는 테이프를 자동으로 덮어쓸 수 없습니다.

   이 규칙의 유일한 예외는 "전체 백업을 생성할 때 독립형 테이프 드라이브에 테이프를 덮어쓰기" 옵션이 활성화된 경우입니다.
8. 복구 시 재부팅이 필요한 운영 체제에서는 테이프에 저장된 백업에서의 복구를 수행할 수 없습니다. 이러한 복구를 수행하려면 부트 가능한 미디어를 사용해야 합니다.

9. 테이프에 저장된 모든 백업의 유효성을 검사할 수 있지만, 전체 테이프 기반 위치 또는 테이프 장치의 유효성 검사를 선택할 수는 없습니다.
10. 테이프 기반 관리 위치는 암호화로 보호할 수 없습니다. 대신 백업을 암호화합니다.
11. 소프트웨어는 하나의 백업을 여러 테이프에 동시에 쓰거나 여러 백업을 동일한 드라이브를 통해 동일한 테이프에 동시에 쓸 수 없습니다.
12. NDMP(Network Data Management Protocol)를 사용하는 장치는 지원되지 않습니다.
13. 바코드 프린터는 지원되지 않습니다.
14. LTFS(Linear Tape File System) 형식의 테이프는 지원되지 않습니다.

이전 Acronis 제품에서 작성한 테이프의 판독 가능성

다음 표에는 Acronis Cyber Protect의 Acronis True Image Echo, Acronis True Image 9.1, Acronis Backup & Recovery 10, Acronis Backup & Recovery 11, Acronis Backup 11.5/11.7/12.5 제품군에서 작성된 테이프의 판독 가능성이 요약되어 있습니다. 또한 이 표에는 Acronis Cyber Protect의 다양한 컴퍼넌트가 작성한 테이프의 호환성도 나와 있습니다.

Acronis Backup 11.5/11.7/12.5에서 생성된 재스캔된 백업에 증분 및 차등 백업을 추가할 수 있습니다.

	...머신에 연결된 테이프 장치에서 판독 가능...			
	Acronis Cyber Protect 부트 가능한 미디어	Acronis Cyber Protect Agent for Windows	Acronis Cyber Protect Agent for Linux	Acronis Cyber Protect 스토리지 노드

다음에 의해 로컬에 연결된 테이프 장치에 작성된 테이프(테이프 드라이브 또는 테이프 라이브러리)	부트 가능한 미디어	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agent for Windows	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
	Agent for Linux	9.1	+	+	+	+
		Echo	+	+	+	+
		ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	-
다음을 통해 테이프 장치에 작성된 테이프	백업 서버	9.1	-	-	-	-
		Echo	-	-	-	-
	스토리지 노드	ABR10	+	+	+	+
		ABR11/ Acronis Backup 11.5/11.7/12.5	+	+	+	+

테이프 장치 시작하기

로컬 연결 테이프 장치에 머신 백업

사전 요구 사항

- 테이프 장치가 제조사의 지시사항에 따라 머신에 연결되어 있습니다.
- 보호 에이전트가 머신에 설치되어 있습니다.

백업 전

1. 테이프 장치에 테이프를 로드합니다.
2. Cyber Protect 웹 콘솔에 로그인합니다.
3. **설정** > **테이프 관리**에서 머신 노드를 확장하고 **테이프 장치**를 클릭합니다.
4. 연결된 테이프 장치가 표시되는지 확인합니다. 표시되지 않으면 **장치 감지**를 클릭합니다.
5. 테이프 인벤토리 수행:
   a. 테이프 장치 이름을 클릭합니다.
   b. **인벤토리**를 클릭하여 로드된 테이프를 감지합니다. **전체 인벤토리**를 활성 상태로 유지합니다. **인식되지 않거나 가져온 테이프를 '사용 가능 테이프' 풀로 이동**을 활성화하지 마십시오. **지금 인벤토리 시작**을 클릭합니다.
   결과. 로드된 테이프는 "인벤토리 작업" 섹션에 지정된 올바른 풀로 이동되었습니다.

   참고
   전체 테이프 장치의 전체 인벤토리 작업은 시간이 오래 소요될 수 있습니다.

   c. 로드된 테이프를 **인식되지 않은 테이프** 또는 **가져온 테이프** 풀로 보내고 백업 시 사용하려는 경우에는 해당 테이프를 **사용 가능 테이프** 풀로 수동으로 이동합니다.

   참고
   가져온 테이프 풀로 보낸 테이프에는 Acronis 소프트웨어로 작성한 백업이 포함됩니다. 해당 테이프를 **사용 가능 테이프** 풀로 이동하려면 먼저 이러한 백업이 필요하지 않은지 확인합니다.

백업

"보호" 섹션에 설명된 대로 보호 계획을 생성합니다. 백업 위치를 지정할 경우 **테이프 풀 'Acronis'**를 선택합니다.

결과

- 백업을 생성할 위치에 액세스하려면 **백업 스토리지** > **테이프 풀 'Acronis'**를 클릭합니다.
- 백업이 포함된 테이프는 **Acronis** 풀로 이동합니다.

스토리지 노드에 연결된 테이프 장치에 백업

사전 요구 사항

- 스토리지 노드는 관리 서버에 등록되어 있습니다.
- 테이프 장치가 제조사의 지시사항에 따라 스토리지 노드에 연결되어 있습니다.

백업 전

1. 테이프 장치에 테이프를 로드합니다.
2. Cyber Protect 웹 콘솔에 로그인합니다.

3. **설정** > **테이프 관리**를 클릭하고, 스토리지 노드 이름을 가진 노드를 확장하고 나서, **테이프 장치**를 클릭합니다.
4. 연결된 테이프 장치가 표시되는지 확인합니다. 표시되지 않으면 **장치 감지**를 클릭합니다.
5. 테이프 인벤토리 수행:
   a. 테이프 장치 이름을 클릭합니다.
   b. **인벤토리**를 클릭하여 로드된 테이프를 감지합니다. **전체 인벤토리**를 활성 상태로 유지합니다. **인식되지 않거나 가져온 테이프 풀을 '사용 가능 테이프' 풀로 이동**을 활성화하지 마십시오. **지금 인벤토리 시작**을 클릭합니다.
      결과. 로드된 테이프는 "인벤토리 작업" 섹션에 지정된 올바른 풀로 이동되었습니다.

      참고
      전체 테이프 장치의 전체 인벤토리 작업은 시간이 오래 소요될 수 있습니다.

   c. 로드된 테이프를 **인식되지 않은 테이프** 또는 **가져온 테이프** 풀로 보내고 백업 시 사용하려는 경우에는 해당 테이프를 **사용 가능 테이프** 풀로 수동으로 이동합니다.

      참고
      가져온 테이프 풀로 보낸 테이프에는 Acronis 소프트웨어로 작성한 백업이 포함됩니다. 해당 테이프를 **사용 가능 테이프** 풀로 이동하려면 먼저 이러한 백업이 필요하지 않은지 확인합니다.

   d. **Acronis** 풀로 백업하거나 새 풀을 생성할지 여부를 결정합니다.
      상세정보. 풀이 여러 개 있으면 각 머신 또는 회사의 각 부서마다 별도의 테이프 세트를 사용할 수 있습니다. 여러 개의 풀을 사용하면 다른 보호 계획을 통해 생성된 백업이 하나의 테이프에서 혼합되는 것을 방지할 수 있습니다.
   e. 선택한 풀이 **사용 가능 테이프** 풀의 테이프를 사용할 수 있는 경우 필요하면 이 단계를 건너뜁니다.
      그렇지 않으면 **사용 가능 테이프** 풀의 테이프를 선택한 풀로 이동합니다.
      팁. 풀이 **사용 가능 테이프** 풀의 테이프를 사용할 수 있는지 알아보려면 풀을 클릭하고 **정보**를 클릭합니다.

백업

"보호" 섹션에 설명된 대로 보호 계획을 생성합니다. 백업 위치를 지정할 경우 생성된 테이프 풀을 선택합니다.

결과

- 백업을 생성할 위치에 액세스하려면 **백업**을 클릭하고 생성된 테이프 풀의 이름을 클릭합니다.
- 백업이 포함된 테이프는 선택한 풀로 이동합니다.

테이프 라이브러리 추가 사용을 위한 팁

- 새 테이프를 로드할 때마다 전체 인벤토리 작업을 수행할 필요는 없습니다. 시간을 절약하려면 "빠른 인벤토리 작업과 전체 인벤토리 작업의 결합" 아래 "인벤토리 작업" 섹션에 설명된 절차를

따릅니다.

- 동일한 테이프 라이브러리에서 다른 풀을 생성하고 원하는 풀을 백업 대상으로 선택할 수 있습니다.

테이프 장치에서 운영 체제 복구

테이프 장치에서 운영 체제를 복구하려면:

1. Cyber Protect 웹 콘솔에 로그인합니다.
2. **장치**를 클릭하고 백업된 머신을 선택합니다.
3. **복구**를 클릭합니다.
4. 복구 지점을 선택합니다. 복구 지점은 위치별로 필터링됩니다.
5. 복구에 필요한 테이프 목록이 표시됩니다. 누락된 테이프는 회색으로 표시됩니다. 테이프 장치에 비어 있는 슬롯이 있으면 해당 테이프가 장치에 로드됩니다.
6. 기타 복구 설정을 구성합니다.
7. **복구 시작**을 클릭하여 복구 작업을 시작합니다.
8. 필요한 테이프가 어떠한 이유로 로드되지 않으면 소프트웨어가 필요한 테이프의 ID가 포함된 메시지를 표시합니다. 다음을 수행합니다.
   a. 테이프를 로드합니다.
   b. 빠른 인벤토리 작업을 수행합니다.
   c. **개요** > **작업**을 클릭하고 **사용자 입력이 필요함** 상태의 복구 작업을 클릭합니다.
   d. **상세정보 표시**를 클릭하고 **재시도**를 클릭하여 복구를 계속 진행합니다.

테이프에 저장된 백업이 나타나지 않을 때 필요한 조치는 무엇입니까?

어떠한 이유로 인해 테이프 내용이 있는 데이터베이스가 유실 또는 손상되었음을 의미할 수 있습니다.

데이터베이스를 복원하려면 다음을 수행하십시오.

1. 빠른 인벤토리 작업을 수행합니다.

   경고!
   인벤토리 작업 중에 *인식되지 않거나 가져온 테이프를 '사용 가능 테이프' 풀로 이동*을 활성화하지 **마십시오**. 이 스위치를 활성화하면 모든 백업을 잃을 수 있습니다.

2. **인식되지 않는 테이프** 풀을 재스캔합니다. 결과적으로 로드된 테이프의 내용이 나타납니다.
3. 감지된 백업이 아직 재스캔되지 않은 다른 테이프에 계속 남아 있는 경우에는 메시지에 따라 해당 테이프를 로드하고 재스캔합니다.

로컬로 연결된 테이프 장치의 부트 가능한 미디어에서 복구

로컬로 연결된 테이프 장치의 부트 가능한 미디어에서 복구하려면:

1. 복구에 필요한 테이프를 테이프 장치에 로드합니다.
2. 부트 가능한 미디어에서 머신을 부트합니다.

3. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
4. iSCSI 인터페이스를 사용하여 테이프 장치를 연결한 경우에는 "iSCSI 및 NDAS 장치 구성"의 설명대로 장치를 구성합니다.
5. **테이프 관리**를 클릭합니다.
6. **인벤토리**를 클릭합니다.
7. **인벤토리 작업을 수행할 객체**에서 테이프 장치를 선택합니다.
8. **시작**을 클릭하여 인벤토리 작업을 시작합니다.
9. 인벤토리 작업이 완료되면 **닫기**를 클릭합니다.
10. **작업** > **복구**를 클릭합니다.
11. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
12. **테이프 장치**를 확장하고 필요한 장치를 선택합니다. 재검색을 확인하는 메시지가 표시됩니다. **예**를 클릭합니다.
13. **인식되지 않는 테이프** 풀을 선택합니다.
14. 재스캔할 테이프를 선택합니다. 풀의 모든 테이프를 선택하려면 **테이프 이름** 열 머리글 옆에 있는 확인란을 선택합니다.
15. 테이프에 비밀번호로 보호되는 백업이 포함되어 있는 경우에는 해당 확인란을 선택하고 **비밀번호** 박스에 백업의 비밀번호를 지정합니다. 비밀번호를 지정하지 않거나 비밀번호가 올바르지 않으면 백업이 감지되지 않습니다. 이러한 경우 재스캐닝 후 백업이 나타나지 않습니다.
    팁. 테이프에 다양한 비밀번호로 보호되는 여러 백업이 포함되는 경우에는 각각의 비밀번호를 차례로 지정하여 재스캐닝을 여러 번 반복해야 합니다.
16. **시작**을 클릭하여 재스캔을 시작합니다. 결과적으로 로드된 테이프의 내용이 나타납니다.
17. 감지된 백업이 아직 재스캔되지 않은 다른 테이프에 계속 남아 있는 경우에는 메시지에 따라 해당 테이프를 로드하고 재스캔합니다.
18. 재스캔이 완료되면 **확인**을 클릭합니다.
19. **아카이브 보기**에서 데이터를 복구할 백업을 선택한 다음 복구할 데이터를 선택합니다. **확인**을 클릭하면 **데이터 복구** 페이지에 복구에 필요한 테이프 목록이 표시됩니다. 누락된 테이프는 회색으로 표시됩니다. 테이프 장치에 비어 있는 슬롯이 있으면 해당 테이프가 장치에 로드됩니다.
20. 기타 복구 설정을 구성합니다.
21. **확인**을 클릭하여 복구를 시작합니다.
22. 필요한 테이프가 어떠한 이유로 로드되지 않으면 소프트웨어가 필요한 테이프의 ID가 포함된 메시지를 표시합니다. 다음을 수행합니다.
    a. 테이프를 로드합니다.
    b. 빠른 인벤토리 작업을 수행합니다.
    c. **개요** > **작업**을 클릭하고 **사용자 입력이 필요함** 상태의 복구 작업을 클릭합니다.
    d. **상세정보 표시**를 클릭하고 **재시도**를 클릭하여 복구를 계속 진행합니다.

스토리지 노드에 연결된 테이프 장치의 부트 가능한 미디어에서 복구

스토리지 노드에 연결된 테이프 장치의 부트 가능한 미디어에서 복구하려면:

1. 복구에 필요한 테이프를 테이프 장치에 로드합니다.
2. 부트 가능한 미디어에서 머신을 부트합니다.
3. 사용 중인 미디어 유형에 따라 **이 머신을 로컬로 관리**를 클릭하거나 **부트 가능한 미디어 복구**를 두 번 클릭합니다.
4. **복구**를 클릭합니다.
5. **데이터 선택**을 클릭한 다음 **찾아보기**를 클릭합니다.
6. **경로** 박스에 bsp://<스토리지 노드 주소>/<풀 이름>/을 입력합니다. 여기서 <스토리지 노드 주소>는 필요한 백업이 포함된 스토리지 노드의 IP 주소이고, <풀 이름>은 테이프 풀의 이름입니다. **확인**을 클릭하고 풀의 자격 증명을 지정합니다.
7. 백업을 선택한 다음 복구할 데이터를 선택합니다. **확인**을 클릭하면 **데이터 복구** 페이지에 복구에 필요한 테이프 목록이 표시됩니다. 누락된 테이프는 회색으로 표시됩니다. 테이프 장치에 비어 있는 슬롯이 있으면 해당 테이프가 장치에 로드됩니다.
8. 기타 복구 설정을 구성합니다.
9. **확인**을 클릭하여 복구를 시작합니다.
10. 필요한 테이프가 어떠한 이유로 로드되지 않으면 소프트웨어가 필요한 테이프의 ID가 포함된 메시지를 표시합니다. 다음을 수행합니다.
    a. 테이프를 로드합니다.
    b. 빠른 인벤토리 작업을 수행합니다.
    c. **개요** > **작업**을 클릭하고 **사용자 입력이 필요함** 상태의 복구 작업을 클릭합니다.
    d. **상세정보 표시**를 클릭하고 **재시도**를 클릭하여 복구를 계속 진행합니다.

테이프 관리

테이프 장치 감지

백업 소프트웨어는 테이프 장치 감지 중 머신에 연결된 테이프 장치를 찾고 해당 정보를 테이프 관리 데이터베이스에 저장합니다. 감지된 테이프 장치는 RSM에서 비활성화됩니다.

일반적으로 테이프 장치는 제품이 설치된 머신에 연결된 직후에 자동으로 감지됩니다. 그러나 다음 경우에는 테이프 장치를 감지해야 할 수 있습니다.

- 테이프 장치를 연결 또는 다시 연결한 후.
- 테이프 장치가 연결된 머신에 백업 소프트웨어를 설치했거나 다시 설치한 후

테이프 장치를 감지하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치가 연결되는 머신을 선택합니다.
3. **장치 감지**를 클릭합니다. 연결된 테이프 장치와 해당 드라이브 및 슬롯이 표시됩니다.

테이프 풀

백업 소프트웨어는 테이프의 논리 그룹인 테이프 풀을 사용합니다. 소프트웨어에는 **인식되지 않는 테이프**, **가져온 테이프**, **사용 가능 테이프** 및 **Acronis** 테이프 풀이 사전 정의되어 있습니다. 또한 고유 사용자 정의 풀을 생성할 수 있습니다.

Acronis 풀과 사용자 정의 풀은 백업 위치로도 사용됩니다.

사전 정의된 풀

인식되지 않는 테이프

풀에는 타사 애플리케이션으로 기록한 테이프가 포함됩니다. 이러한 테이프에 쓰려면 **사용 가능 테이프** 풀로 테이프를 명시적으로 이동해야 합니다. **사용 가능 테이프** 풀을 제외하고는 이 풀의 테이프를 다른 풀로 이동할 수 없습니다.

가져온 테이프

풀에는 다른 스토리지 노드 또는 에이전트에 연결된 테이프 장치에 있는 Acronis Cyber Protect(으)로 기록된 테이프가 포함됩니다. 이러한 테이프에 쓰려면 **사용 가능 테이프** 풀로 테이프를 명시적으로 이동해야 합니다. **사용 가능 테이프** 풀을 제외하고는 이 풀의 테이프를 다른 풀로 이동할 수 없습니다.

사용 가능 테이프

풀에는 여유 공간이 있는(비어 있는) 테이프가 포함됩니다. 다른 풀에서 이 풀로 테이프를 수동으로 이동할 수 있습니다.

사용 가능 테이프 풀로 테이프를 이동하는 경우 소프트웨어는 해당 테이프를 비어 있는 것으로 표시합니다. 테이프에 백업이 포함되는 경우 아이콘이 함께 표시됩니다. 소프트웨어가 테이프 덮어쓰기를 시작하면 백업과 관련된 데이터가 데이터베이스에서 제거됩니다.

Acronis

풀은 자체 풀을 생성하지 않으려는 경우 기본적으로 백업 대상으로 사용됩니다. 일반적으로 테이프가 적은 하나의 테이프 드라이브에 적용됩니다.

사용자 정의 풀

다른 데이터의 백업을 구분하려면 별도의 풀을 생성해야 합니다. 예를 들어, 다음을 구분하기 위해 사용자 정의 풀을 만들 수 있습니다.

- 회사의 다른 부서에서 백업
- 다른 머신의 백업
- 시스템 볼륨 및 사용자 데이터의 백업

풀 작업

풀 생성

풀을 생성하려면:

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. **풀 생성**을 클릭합니다.

4. 풀 이름을 지정합니다.
5. [선택 사항] **'사용 가능 테이프' 풀에서 자동으로 테이프 가져오기...** 확인란의 선택을 취소합니다. 확인란을 지우면 특정 시점에 새 풀에 포함되는 테이프만 백업에 사용됩니다.
6. **생성**을 클릭합니다.

풀 편집

Acronis 풀 또는 사용자 정의 풀의 매개변수를 편집할 수 있습니다.

풀을 편집하려면:

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 풀을 선택한 다음 **풀 편집**을 클릭합니다.
4. 풀 이름 또는 설정을 변경할 수 있습니다. 풀 설정에 대한 자세한 내용은 "풀 생성" 섹션을 참조하십시오.
5. **저장**을 클릭하여 변경 사항을 저장합니다.

풀 삭제

사용자 정의 풀만 삭제할 수 있습니다. 사전 정의된 테이프 풀(**인식되지 않는 테이프**, **가져온 테이프**, **사용 가능 테이프** 및 **Acronis**)은 삭제할 수 없습니다.

참고
풀이 삭제된 후에는 풀이 백업 위치로 사용되는 보호 계획을 편집해야 합니다. 그렇지 않으면 이러한 보호 계획이 실패합니다.

풀을 삭제하려면:

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 풀을 선택하고 **삭제**를 클릭합니다.
4. 삭제 후 삭제되는 풀의 테이프가 제거될 풀을 선택합니다.
5. **확인**을 클릭하여 풀을 삭제합니다.

테이프 작업

다른 슬롯으로 이동

이 작업은 다음과 같은 경우에 사용합니다.

- 테이프 장치에서 동시에 여러 개의 테이프를 꺼내야 하는 경우.
- 테이프 장치에 메일 슬롯이 없고 꺼내려는 테이프가 고정식 저장소의 슬롯에 있는 경우.

테이프를 특정 슬롯 저장소의 슬롯으로 이동한 다음 해당 저장소를 수동으로 꺼내야 하는 경우.

테이프를 다른 슬롯으로 이동하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **슬롯으로 이동**을 클릭합니다.
5. 선택한 테이프를 이동할 새 슬롯을 선택합니다.
6. **이동**을 클릭하여 작업을 시작합니다.

다른 풀로 이동

이 작업을 수행하면 특정 풀에서 다른 풀로 하나 이상의 테이프를 이동할 수 있습니다.

사용 가능 테이프 풀로 테이프를 이동하는 경우 소프트웨어는 해당 테이프를 비어 있는 것으로 표시합니다. 테이프에 백업이 포함되는 경우  아이콘이 함께 표시됩니다. 소프트웨어가 테이프 덮어쓰기를 시작하면 백업과 관련된 데이터가 데이터베이스에서 제거됩니다.

특정 테이프 유형에 대한 참고 사항

- 쓰기 방지가 되어 있거나 레코딩 기록이 있는 WORM(Write-Once-Read-Many) 테이프는 **사용 가능 테이프** 풀로 이동할 수 없습니다.
- 정리 테이프는 항상 **인식되지 않는 테이프** 풀에 표시됩니다. 이러한 테이프는 다른 풀로 이동할 수 없습니다.

테이프를 다른 풀로 이동하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **풀로 이동**을 클릭합니다.
5. [선택 사항] 선택한 테이프의 다른 풀을 생성하려면 **새 풀 생성**을 클릭합니다. "풀 생성" 섹션에 설명된 작업을 수행합니다.
6. 테이프를 이동할 대상 풀을 선택합니다.
7. **이동**을 클릭하여 변경 사항을 저장합니다.

참고
복원 가능 백업이 저장되어 있는 테이프를 다른 풀로 이동할 때는 이동 작업을 완료한 후 백업 스토리지에서 볼트를 새로 고쳐야 합니다. 그러면 원래 백업 대상이 아닌 두 번째 풀에서 백업을 사용할 수 있습니다.

인벤토리 작업 중

인벤토리 작업은 테이프 장치에 로드된 테이프를 감지하며 이름이 없는 테이프에 이름을 할당합니다.

인벤토리 방법

인벤토리 작업 방법에는 두 가지가 있습니다.

빠른 인벤토리 작업

에이전트나 스토리지 노드가 테이프의 바코드를 스캔합니다. 바코드를 사용하면 소프트웨어가 테이프를 이전 풀로 빠르게 되돌릴 수 있습니다.

이 방법을 선택하면 동일한 머신에 연결된 동일한 테이프 장치가 사용하는 테이프를 인식합니다. 다른 테이프는 **인식되지 않는 테이프** 풀로 보냅니다.

테이프 라이브러리에 바코드 판독기가 없는 경우에는 모든 테이프를 **인식되지 않는 테이프** 풀로 보냅니다. 테이프를 인식하려면 전체 인벤토리 작업을 수행하거나 이 섹션에서 아래에 설명된 대로 빠른 인벤토리 작업과 전체 인벤토리 작업을 결합합니다.

전체 인벤토리 작업

에이전트나 스토리지 노드가 이전에 기록된 태그를 읽고 로드된 테이프 내용에 대한 다른 정보를 분석합니다. 이 방법을 선택하면 비어 있는 테이프와 테이프 장치 및 머신에서 같은 소프트웨어로 작성된 테이프를 인식합니다.

다음 표에는 전체 인벤토리 작업에 따라 테이프를 보내는 풀이 나와 있습니다.

테이프 사용...	테이프 읽기...	테이프를 풀로 보냄...
에이전트	동일한 에이전트	테이프의 이전 위치
	다른 에이전트	**가져온 테이프**
	저장소 노드	**가져온 테이프**
저장소 노드	동일한 스토리지 노드	테이프의 이전 위치
	다른 스토리지 노드	**가져온 테이프**
	에이전트	**가져온 테이프**
타사 백업 애플리케이션	에이전트 또는 스토리지 노드	**인식되지 않는 테이프**

특정 유형의 테이프를 특정 풀로 보냅니다.

테이프 유형	테이프를 풀로 보냄...
비어 있는 테이프	**사용 가능 테이프**
비어 있는 쓰기 방지된 테이프	**인식되지 않는 테이프**
정리 테이프	**인식되지 않는 테이프**

빠른 인벤토리 작업은 전체 테이프 장치에 적용될 수 있습니다. 전체 인벤토리 작업은 전체 테이프 장치, 개별 드라이브 또는 슬롯에 적용될 수 있습니다. 독립형 테이프 드라이브의 경우 빠른 인벤토리 작업이 선택된 경우에도 항상 전체 인벤토리 작업이 수행됩니다.

빠른 인벤토리 작업과 전체 인벤토리 작업의 결합

전체 테이프 장치의 전체 인벤토리 작업은 시간이 오래 소요될 수 있습니다. 몇몇 테이프에만 인벤토리 작업을 수행해야 하는 경우에는 다음을 수행합니다.

1. 테이프 장치의 빠른 인벤토리 작업을 수행합니다.
2. **인식되지 않는 테이프** 풀을 클릭합니다. 인벤토리 작업을 수행할 테이프를 찾고 테이프에 있는 슬롯을 기록합니다.
3. 해당 슬롯의 전체 인벤토리 작업을 수행합니다.

인벤토리 작업 후 수행 작업

인식되지 않는 테이프 또는 **가져온 테이프** 풀에 저장된 테이프에 백업하려는 경우에는 테이프를 사용 가능 테이프 풀로 **이동**한 다음 **Acronis** 풀 또는 사용자 정의 풀로 이동합니다. 백업하려는 풀을 갱신할 수 있는 경우에는 테이프를 **사용 가능 테이프** 풀에 남겨둘 수 있습니다.

인식되지 않는 테이프 또는 **가져온 테이프** 풀에 저장된 테이프에서 복구하려면 테이프를 재스캐닝해야 합니다. 재스캐닝 중에 선택한 볼트와 연관된 풀로 테이프가 이동되며 테이프에 저장된 백업은 위치에 나타납니다.

작업 순서

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치가 연결되는 머신을 선택하고 인벤토리 작업을 수행할 테이프 장치를 선택합니다.
3. **인벤토리**를 클릭합니다.
4. [선택 사항] 빠른 인벤토리 작업을 선택하려면 **전체 인벤토리**를 비활성화합니다.
5. [선택 사항] **인식되지 않거나 가져온 테이프를 '사용 가능 테이프' 풀로 이동**을 활성화합니다.

   경고!
   테이프에 저장한 데이터를 덮어써도 되는 경우에만 이 스위치를 활성화합니다.

6. **지금 인벤토리 시작**을 클릭하여 인벤토리를 시작합니다.

재스캐닝

테이프 내용에 대한 정보는 전용 데이터베이스에 저장됩니다. 재스캔 작업은 테이프 내용을 읽고 데이터베이스의 정보가 테이프에 저장된 데이터와 일치하지 않는 경우 데이터베이스를 업데이트합니다. 작업을 수행하여 감지된 백업은 지정된 풀에 저장됩니다.

하나의 작업으로 단일 풀의 테이프를 재스캔할 수 있습니다. 작업에는 온라인 테이프만 선택할 수 있습니다.

멀티스트리밍 백업 또는 멀티스트리밍 백업과 멀티플렉싱 백업으로 테이프를 재스캔하려면 이 백업을 생성하는 데 사용된 것과 동일한 개수 이상의 드라이브가 필요합니다. 이러한 백업은 독립형 테이프 드라이브를 통해 재스캔할 수 없습니다.

재스캔 실행:

- 스토리지 노드 또는 관리 대상 머신의 데이터베이스가 손실되거나 손상된 경우
- 데이터베이스의 테이프에 대한 정보가 오래된 경우(예를 들어, 다른 스토리지 노드 또는 에이전트가 테이프 내용을 수정한 경우)
- 부트 가능한 미디어에서 작업할 때 테이프에 저장된 백업에 대한 액세스 권한을 얻으려면
- 테이프에 대한 정보를 실수로 데이터베이스에서 제거한 경우 제거된 테이프를 재스캔하는 경우 테이프에 저장된 백업이 데이터베이스에 다시 나타나며 데이터 복구에 사용할 수 있습니다.
- 테이프에서 수동으로 또는 보관 규칙에 따라 백업이 삭제되었지만 데이터 복구 시 액세스 가능하게 만들려는 경우 그러한 테이프를 재스캔하기 전에 테이프를 꺼내고 데이터베이스에서 테이프에 대한 정보를 제거한 다음 테이프 장치에 다시 테이프를 넣습니다.

테이프를 재스캔하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 장치**를 클릭합니다.
3. 테이프를 로드한 테이프 장치를 선택합니다.
4. 빠른 인벤토리 작업을 수행합니다.

   참고
   인벤토리 작업 중에는 **인식되지 않거나 가져온 테이프를 '사용 가능 테이프' 풀로 이동** 스위치를 활성화하지 *마십시오*.

5. **인식되지 않는 테이프** 풀을 선택합니다. 빠른 인벤토리 작업의 결과로 생성된 대부분의 테이프를 이 풀로 보냅니다. 다른 모든 풀도 재스캔할 수 있습니다.
6. [선택 사항] 개별 테이프만 재스캔하려면 해당 테이프를 선택합니다.
7. **재스캔**을 클릭합니다.
8. 새로 감지된 백업이 배치될 풀을 선택합니다.
9. 필요한 경우 **테이프에 저장된 디스크 백업으로부터 파일 복구 사용** 확인란을 선택합니다.

   상세정보. 이 확인란을 선택하면 테이프 장치가 연결된 머신의 특후 하드 디스크에서 보조 파일이 생성됩니다. 디스크 백업으로부터의 파일 복구는 이러한 보조 파일이 변경되지 않은 경우에만 가능합니다. 테이프에 애플리케이션 인식 백업이 포함된 경우 확인란을 선택해야 합니다. 그렇지 않으면, 이 백업에서 애플리케이션 데이터를 복구할 수 없습니다.
10. 테이프에 비밀번호로 보호되는 백업이 포함되어 있는 경우에는 해당 확인란을 선택하고 백업의 비밀번호를 지정합니다. 비밀번호를 지정하지 않거나 비밀번호가 올바르지 않으면 백업이 감지되지 않습니다. 이러한 경우 재스캐닝 후 백업이 나타나지 않습니다.

    팁. 테이프에 다양한 비밀번호로 보호되는 백업이 포함되는 경우에는 각각의 비밀번호를 차례로 지정하여 재스캐닝을 여러 번 반복해야 합니다.
11. **재스캔 시작**을 클릭하여 재스캐닝을 시작합니다.

결과. 선택한 테이프는 선택한 풀로 이동됩니다. 테이프에 저장된 백업은 이 풀에서 찾을 수 있습니다. 여러 테이프에 분산된 백업은 해당 테이프를 모드 재스캔해야 풀에 나타납니다.

이름 변경

소프트웨어가 새 테이프를 감지하면 자동으로 **Tape XXX** 형식의 이름을 할당합니다. 여기서 **XXX**는 고유한 숫자입니다. 테이프 번호는 순차적으로 지정됩니다. 이름 변경 작업을 수행하면 테이프의 이름을 수동으로 변경할 수 있습니다.

테이프 이름을 변경하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **이름 변경**을 클릭합니다.
5. 선택한 테이프의 새 이름을 입력합니다.
6. **이름 변경**을 클릭하여 변경 사항을 저장합니다.

지우기

테이프를 지우면 테이프에 저장된 모든 백업이 실제로 삭제되며 데이터베이스에서 해당 백업에 대한 정보가 제거됩니다. 그러나 테이프 자체에 대한 정보는 데이터베이스에 남아 있습니다.

테이프를 지우면 **인식되지 않는 테이프** 또는 **가져온 테이프** 풀에 있는 테이프가 **사용 가능 테이프** 풀로 이동합니다. 다른 풀에 있는 테이프는 이동되지 않습니다.

테이프를 지우려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **지우기**를 클릭합니다. 작업을 확인하는 메시지가 표시됩니다.
5. 지우기 방법 빠른 또는 전체 중에서 선택합니다.
6. **지우기**를 클릭하여 작업을 시작합니다.

   상세정보. 지우기 작업은 취소할 수 없습니다.

꺼내기

테이프 라이브러리에서 테이프를 꺼내려면 테이프 라이브러리에 메일 슬롯이 필요하며 사용자 또는 다른 소프트웨어가 해당 슬롯을 잠그지 않아야 합니다.

테이프를 꺼내려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.

4. **꺼내기**를 클릭합니다. 테이프 설명을 입력해야 합니다. 테이프를 보관할 실제 위치를 설명하는 것이 좋습니다. 복구 중에 이 설명이 표시되어 테이프를 쉽게 찾을 수 있습니다.
5. **꺼내기**를 클릭하여 작업을 시작합니다.

테이프를 수동 또는 자동으로 꺼낸 후에는 테이프에 이름을 쓰는 것이 좋습니다.

제거 중

제거 작업은 선택한 테이프에 저장된 백업과 테이프 자체에 대한 정보를 데이터베이스에서 삭제합니다.

오프라인(꺼낸) 테이프만 제거할 수 있습니다.

테이프를 제거하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **제거**를 클릭합니다. 작업을 확인하는 메시지가 표시됩니다.
5. **제거**를 클릭하여 테이프를 제거합니다.

실수로 테이프를 제거한 경우 필요한 조치는 무엇입니까?

지워진 테이프와 달리 제거된 테이프의 데이터는 실제로 삭제되지 않습니다. 따라서 해당 테이프에 저장된 백업을 다시 사용할 수 있습니다. 이 작업을 수행하려면:

1. 테이프 장치에 테이프를 로드합니다.
2. 빠른 인벤토리 작업을 수행하여 테이프를 감지합니다.

> **참고**
> 인벤토리 작업 중에는 **인식되지 않거나 가져온 테이프를 '사용 가능 테이프' 풀로 이동** 스위치를 활성화하지 *마십시오*.

3. 재스캐닝을 수행하여 테이프에 저장된 데이터와 데이터베이스를 비교합니다.

테이프 세트 지정

이 작업을 통해 테이프에 테이프 세트를 지정할 수 있습니다.

테이프 세트는 하나의 풀 내에 있는 테이프 그룹입니다.

변수를 사용할 수 있는 백업 옵션에서 테이프 세트를 지정하는 경우와 달리 여기서는 문자열 값만 지정할 수 있습니다.

특정 규칙에 따라 *특정* 테이프에 백업하게 소프트웨어를 설정하려면 이 작업을 수행합니다(예: 월요일 백업을 테이프 1에 저장하고, 화요일 백업을 테이프 2에 저장하는 방식으로 진행하려는 경우). 필요한 각 테이프에 대해 특정 테이프 세트를 지정하고 백업 옵션에서 동일한 테이프 세트를 지정하거나 적절한 변수를 사용합니다.

위의 예시에서는 테이프 1에 대해 테이프 세트 Monday를 지정하고, 테이프 2에 대해 Tuesday를 지정합니다. 백업 옵션에서 [Weekday]를 지정합니다. 이 경우 적절한 테이프가 해당 주의 개별 날짜에 사용됩니다.

하나 이상의 테이프에 대한 테이프 세트를 지정하려면

1. **설정** > **테이프 관리**를 클릭합니다.
2. 테이프 장치를 연결할 머신 또는 스토리지 노드를 선택하고 이 머신에서 **테이프 풀**을 클릭합니다.
3. 필요한 테이프가 있는 풀을 클릭한 다음 필요한 테이프를 선택합니다.
4. **테이프 세트**를 클릭합니다.
5. 테이프 세트 이름을 입력합니다. 선택한 테이프에 대해 또 다른 테이프 세트를 이미 지정한 경우 이 테이프 세트가 대체됩니다. 다른 테이프 세트를 지정하지 않고 테이프 세트에서 테이프를 제외하려면 기존 테이프 세트 이름을 삭제합니다.
6. **저장**을 클릭하여 변경 사항을 저장합니다.

스토리지 노드

스토리지 노드는 엔터프라이즈 데이터 보호에 필요한 다양한 리소스(예: 회사 저장 용량, 네트워크 대역폭 및 프로덕션 서버의 CPU 로드)의 사용 최적화를 목표로 하는 서버입니다. 이 목표는 엔터프라이즈 백업(관리 위치)의 전용 스토리지 위치 기능을 수행하는 위치의 구성 및 관리를 통해 달성됩니다.

Acronis 스토리지 노드의 주요 용도는 테이프 드라이브 또는 라이브러리에 대한 중앙 집중식 액세스를 가능하게 하는 것입니다(예: 여러 장치의 데이터를 동일한 테이프 드라이브 또는 라이브러리(테이프의 관리 대상 볼트)에 백업 및 복구).

또 다른 사용 사례는 여러 장치의 데이터를 서로 중복 제거하고 단일 위치(중복 제거가 활성화되어 있는 관리 대상 볼트)에 저장해야 하는 경우 고급 중복 제거 기능을 활성화하는 것입니다.

스토리지 노드 및 카탈로그 서비스 설치

스토리지 노드를 설치하기 전에 머신이 시스템 요구 사항을 충족하는지 확인합니다.

스토리지 노드와 카탈로그 서비스를 개별 머신에 설치하는 것이 좋습니다. 카탈로그 서비스를 실행하는 머신의 시스템 요구 사항은 "모범 사례 목록화"(572페이지)에 설명되어 있습니다.

스토리지 노드 및/또는 카탈로그 서비스를 설치하려면

1. 관리자로 로그온하고 Acronis Cyber Protect 설정 프로그램을 시작합니다.
2. [선택 사항] 설치 프로그램의 언어를 변경하려면 **언어 설정**을 클릭합니다.
3. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
4. **보호 에이전트 설치**를 클릭합니다.
5. **설치 설정 사용자 정의**를 클릭합니다.
6. **설치할 항목** 옆에 있는 **변경**을 클릭합니다.
7. 설치할 컴퍼넌트를 선택합니다.

- 스토리지 노드를 설치하려면 **스토리지 노드** 확인란을 선택합니다. **Agent for Windows** 확인란이 자동으로 선택됩니다.
- 카탈로그 서비스를 설치하려면 **카탈로그 서비스** 확인란을 선택합니다.
- 다른 컴퍼넌트를 이 머신에 설치하지 않으려면 해당하는 확인란의 선택을 해제합니다.

완료를 클릭하여 계속 진행합니다.

8. 컴퍼넌트를 등록할 관리 서버를 지정합니다.
   a. **Acronis Cyber Protect Management Server** 옆에 있는 **지정**을 클릭합니다.
   b. 관리 서버가 설치된 머신의 호스트 이름 또는 IP주소를 지정합니다.
   c. 관리 서버 관리자 또는 등록 토큰의 자격 증명을 지정합니다.
      등록 토큰을 생성하는 방법에 대한 자세한 내용은 "1단계: 등록 토큰 생성"(166페이지)을(를) 참조하십시오.
   d. **완료**를 클릭합니다.
9. 메시지가 표시되면 스토리지 노드 및/또는 카탈로그 서비스가 설치된 머신을 조직에 추가할지, 아니면 부서 중 하나에 추가할지 선택합니다.
   이 메시지는 사용자가 둘 이상의 부서 또는 최소 하나의 부서가 있는 조직을 관리하는 경우에 나타납니다. 그렇지 않으면 머신이 사용자가 관리하는 부서 또는 조직에 자동으로 추가됩니다. 자세한 내용은 "관리자 및 단위"를 참조하십시오.
10. [선택 사항] "설치 설정 사용자 정의"에 설명되어 있는 대로 기타 설치 설정을 변경합니다.
11. **설치**를 클릭하여 설치를 계속 진행합니다.
12. 설치가 완료되면 **닫기**를 클릭합니다.

Acronis Cyber Protect 15 Update 4로 카탈로그 서비스 업데이트

Acronis Cyber Protect 15 Update 4는 새 버전의 카탈로그 서비스를 사용합니다. 새 버전은 이전 버전에서 생성된 카탈로그 데이터와 직접 호환되지 않습니다.

업데이트Acronis Cyber Protect 15 Update 4로 업데이트하는 동안 이 데이터를 새 버전의 카탈로그 서비스로 수동으로 마이그레이션할 수 있습니다. 마이그레이션을 건너뛰고 나중에 카탈로그 데이터를 다시 생성할 수도 있습니다. 카탈로그 데이터 재생성 작업은 해당 데이터를 마이그레이션하는 것보다 오래 걸립니다.

카탈로그 데이터를 마이그레이션하려면

1. 카탈로그 서비스가 설치되어 있는 머신에서 Acronis Cyber Protect 설치 프로그램을 실행합니다.
2. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
3. **다음 사항을 이해합니다.** 확인란을 선택한 후 **업데이트**를 클릭합니다.
4. **임시 폴더 지정** 확인란을 선택합니다.
5. 카탈로그 데이터를 내보낼 폴더를 지정합니다.
   내보낸 데이터는 암호화됩니다. 마이그레이션이 완료되면 임시 폴더가 자동으로 삭제됩니다.
6. **완료**를 클릭합니다.

카탈로그 데이터 마이그레이션을 건너뛰려면

1. 카탈로그 서비스가 설치되어 있는 머신에서 Acronis Cyber Protect 설치 프로그램을 실행합니다.
2. 라이센스 계약 조건 및 개인 정보 보호 정책에 동의하고 **진행**을 클릭합니다.
3. **다음 사항을 이해합니다.** 확인란을 선택한 후 **업데이트**를 클릭합니다.
4. **임시 폴더 지정** 확인란을 선택 취소합니다.
5. **완료**를 클릭합니다.
6. 선택 내용을 확인합니다.

그러면 Acronis Cyber Protect 15 Update 4로 업데이트한 후 기존 카탈로그 데이터를 사용할 수 없게 됩니다. 카탈로그 데이터를 다시 생성하려면 백업을 실행합니다.

참고
카탈로그 서비스, 스토리지 노드 및 관리 서버가 각각 서로 다른 머신에서 실행되는 경우 다음 순서에 따라 모두 Acronis Cyber Protect 15 Update 4로 업데이트해야 합니다.

1. 관리 서버
2. 저장소 노드
3. 카탈로그 서비스

관리 위치 추가

관리 위치를 구성할 수 있습니다.

- 로컬 폴더:
  - 스토리지 노드에 로컬인 하드 드라이브
  - 운영 체제에 로컬 연결 장치로 나타나는 SAN 스토리지
- 네트워크 폴더:
  - SMB/CIFS 공유
  - 운영 체제에 네트워크 폴더로 나타나는 SAN 스토리지
  - NAS
- 스토리지 노드에 로컬로 연결된 테이프 장치.
  테이프 기반 위치는 테이프 풀 형식으로 생성됩니다. 기본적으로 하나의 테이프 풀이 제공됩니다. 필요한 경우 이 섹션에서 이후에 설명하는 대로 다른 테이프 풀을 생성할 수 있습니다.

로컬 또는 네트워크 폴더에서 관리 위치를 생성하려면

1. 다음 중 하나를 수행하십시오.
   - **백업 스토리지** > **위치 추가**를 클릭한 다음 **스토리지 노드**를 클릭합니다.
   - 보호 계획을 생성할 때에는 **백업 위치** > **위치 추가**를 클릭한 다음, **스토리지 노드**를 클릭합니다.
   - **설정** > **스토리지 노드**를 클릭하고 위치를 관리할 스토리지 노드를 선택한 다음 **위치 추가**를 클릭합니다.
2. **이름**에 위치의 고유한 이름을 지정합니다. "고유"하다는 것은 동일한 스토리지 노드로 관리하는 같은 이름의 또 다른 위치가 없어야 한다는 의미입니다.

3. [선택 사항] 위치를 관리할 스토리지 노드를 선택합니다. 1단계에서 마지막 옵션을 선택한 경우 스토리지 노드를 변경할 수 없습니다.
4. 스토리지 노드 이름 또는 에이전트가 위치에 액세스하는 데 사용할 IP 주소를 선택합니다.
   기본적으로 스토리지 노드 이름이 선택됩니다. DNS 서버가 이름을 IP 주소로 확인할 수 없어 액세스에 실패할 경우 이 설정을 변경해야 할 수 있습니다. 이후에 이 설정을 변경하려면 **백업 스토리지** > 위치 > **편집**을 클릭한 다음 **주소** 필드 값을 변경합니다.
5. 폴더 경로를 입력하거나 원하는 폴더를 찾습니다.
6. **완료**를 클릭합니다. 소프트웨어에서 지정된 폴더에 대한 액세스를 확인합니다.
7. [선택 사항] 위치에서 백업 중복 제거를 활성화합니다.
   중복 제거는 중복 디스크 블록을 제거함으로써 백업 트래픽을 최소화하고, 해당 위치에 저장되는 백업 크기를 줄여줍니다.
   중복 제거 제한 사항에 대한 자세한 내용은 "중복 제거 제한 사항"을 참조하십시오.
8. [중복 제거가 활성화된 경우에만 해당] **중복 제거 데이터베이스 경로** 필드 값을 지정하거나 변경합니다.
   이 경로는 스토리지 노드에 로컬인 하드 드라이브의 폴더여야 합니다. 시스템 성능을 향상하려면 중복 제거 데이터베이스와 관리 위치를 다른 디스크에 생성하는 것이 좋습니다.
   중복 제거 데이터베이스에 대한 자세한 내용은 "중복 제거 모범 사례"를 참조하십시오.
9. [선택 사항] 암호화로 위치를 보호할지 여부를 선택합니다. 위치에 작성된 모든 내용은 암호화되고 여기에서 읽는 모든 내용은 스토리지 노드에 저장된 위치 기준 암호화 키를 사용하여 스토리지 노드에 의해 투명하게 암호 해독됩니다.
   암호화에 대한 자세한 내용은 "위치 암호화"를 참조하십시오.
10. [선택 사항] 위치에 저장된 백업의 목록화 여부를 선택합니다. 데이터 카탈로그를 사용하면 필요한 데이터 버전을 쉽게 찾고 복구 대상으로 선택할 수 있습니다.
    관리 서버에 여러 목록화 서비스가 등록되는 경우에는 해당 위치에 저장된 백업을 목록화하는 서비스를 선택할 수 있습니다.
    목록화는 이후에 "목록화 활성화 또는 비활성화 방법"에 설명된 대로 활성화하거나 비활성화할 수 있습니다.
11. **완료**를 클릭하여 위치를 생성합니다.

테이프 장치에서 관리 위치를 생성하려면

1. **백업 스토리지** > **위치 추가**를 클릭하거나, 보호 계획을 생성 중이라면 **백업 위치** > **위치 추가**를 클릭합니다.
2. **테이프**를 클릭합니다.
3. [선택 사항] 위치를 관리할 스토리지 노드를 선택합니다.
4. "풀 생성"에 설명된 단계를 4단계부터 따릅니다.

참고
기본적으로 에이전트는 스토리지 노드 이름을 사용하여 관리 테이프 기반 위치에 액세스합니다. 에이전트가 스토리지 노드 IP 주소를 사용하도록 하려면 **백업 스토리지** > 위치 > **편집**을 클릭한 다음 **주소** 필드 값을 변경합니다.

중복 제거

중복 제거 제한

공통 제한 사항

암호화된 백업을 중복 제거할 수 없습니다. 중복 제거와 암호화를 동시에 사용하려면 백업을 암호화되지 않은 채로 유지하고, 중복 제거와 암호화가 모두 활성화되어 있는 위치로 지정하십시오.

디스크 수준 백업

볼륨의 할당 단위 크기(클러스터 크기 또는 블록 크기라고도 함)를 4KB로 나눌 수 없으면 디스크 블록 중복 제거가 수행되지 않습니다.

참고
대부분의 NTFS 및 ext3 볼륨의 할당 단위 크기는 4KB입니다. 따라서 블록 수준 중복 제거가 가능합니다. 블록 수준 중복 제거에 허용되는 할당 단위 크기의 다른 예로 8KB, 16KB 및 64KB가 있습니다.

파일 수준 백업

파일이 암호화되어 있으면 파일 중복 제거가 수행되지 않습니다.

중복 제거 및 NTFS 데이터 스트림

NTFS 파일 시스템에서는 *대체 데이터 스트림*이라고도 하는 관련 데이터의 하나 이상의 추가 집합이 파일에 포함될 수 있습니다.

이런 파일이 백업되면 이는 모두 대체 데이터 스트림입니다. 그러나 파일 자체는 중복 제거되더라도 이러한 스트림은 중복 제거되지 않습니다.

중복 제거 우수 사례

중복 제거는 여러 요소에 따라 달라지는 복잡한 프로세스입니다.

중복 제거 속도에 영향을 주는 가장 중요한 요소는 다음과 같습니다.

- 중복 제거 데이터베이스에 대한 액세스 속도
- 스토리지 노드의 RAM 용량
- 스토리지 노드에 생성된 중복 제거 위치의 수.

중복 제거 성능을 높이려면 다음의 권장 사항을 따르십시오.

중복 제거 데이터베이스와 중복 제거 위치를 별도의 실제 장치에 놓습니다.

중복 제거 데이터베이스는 위치에 저장된 모든 항목의 해시 값을 저장합니다(암호화된 파일과 같이 중복을 제거할 수 없는 항목은 제외).

중복 제거 데이터베이스에 대한 액세스 속도를 높이려면 데이터베이스와 위치가 별도의 실제 장치에 배치되어야 합니다.

가장 좋은 방법은 위치와 데이터베이스에 대해 전용 장치를 할당하는 것입니다. 이것이 가능하지 않으면 최소한 운영 체제가 있는 동일한 디스크에 위치 또는 데이터베이스를 저장하지 않도록 하십시오. 그 이유는 운영 체제가 다수의 하드 디스크 읽기/쓰기 작업을 수행하기 때문에 중복 제거 속도가 크게 저하될 수 있기 때문입니다.

중복 제거 데이터베이스의 디스크 선택

- 데이터베이스는 고정된 디스크에 상주해야 합니다. 분리식 외장 드라이브에 중복 제거 데이터베이스를 저장하지 마십시오.
- 데이터베이스에 대한 액세스 시간을 최소화하려면 이를 마운트된 네트워크 볼륨이 아닌 직접 연결된 드라이브에 저장합니다. 네트워크 대기 시간은 중복 제거 성능을 크게 줄일 수 있습니다.
- 다음 공식을 사용해서 중복 제거 데이터베이스에 필요한 디스크 공간을 예측할 수 있습니다.

$$S = U * 90 / 65536 + 10$$

여기서,

S는 디스크 크기(단위: GB)이며

U는 중복 제거 데이터 저장소에서 계획된 고유한 데이터 양(단위: GB)입니다.

예를 들어 중복 제거 데이터 저장소에서 계획된 고유한 데이터 양이 U=5TB인 경우, 중복 제거 데이터베이스에는 다음과 같이 최소 여유 공간이 필요합니다.

$$S = 5000 * 90 / 65536 +10 = 17 GB$$

중복 제거 위치의 디스크 선택

데이터 손실 방지 목적으로 RAID 10, 5 또는 6을 사용하는 것을 권장합니다. RAID 0에는 내결함성이 없으므로 권장되지 않습니다. RAID 1은 상대적으로 속도가 느리므로 권장되지 않습니다. 로컬 디스크나 SAN 모두 양호한 성능을 제공하므로 특별한 선호도는 없습니다.

고유 데이터 1TB당 40~160MB의 RAM

한계에 도달하면 중복 제거가 중지되지만 백업 및 복구는 계속 작동합니다. 스토리지 노드에 더 많은 RAM을 추가하는 경우, 다음 백업 이후에 중복 제거가 재개됩니다. 일반적으로 RAM이 많을수록 더 많은 용량의 고유 데이터를 저장할 수 있습니다.

각 스토리지 노드에서 하나의 중복 제거 위치만

스토리지 노드에 하나의 중복 제거 위치만 생성하는 경우 권장됩니다. 그렇지 않으면 위치 수에 비례하여 전체 사용 가능한 RAM 볼륨이 분배될 수 있습니다.

리소스를 경쟁하는 애플리케이션이 없음

스토리지 노드가 있는 머신은 많은 시스템 리소스를 필요로 하는 애플리케이션을 실행해서는 안 됩니다(예: 데이터베이스 관리 시스템(DBMS) 또는 전사적 자원 관리(ERP) 시스템).

최소 2.5GHz 클럭 속도를 지원하는 멀티코어 프로세서

코어 수가 4개 이상이고 클럭 속도가 2.5GHz 이상인 프로세서를 사용하는 것이 권장됩니다.

위치의 충분한 여유 공간

대상에서의 중복 제거 작업에는 데이터를 위치에 저장한 직후 백업한 데이터가 차지하는 것만큼 많은 여유 공간이 필요합니다. 소스에서의 압축 또는 중복 제거가 없을 경우, 지정된 백업 작업 동안 이 값은 백업된 원본 데이터의 크기와 같습니다.

고속 LAN

1Gbit LAN이 권장됩니다. 소프트웨어가 중복 제거를 포함한 5-6개의 백업을 병렬로 수행할 수 있으며, 속도가 크게 저하되지 않습니다.

유사한 내용이 포함된 여러 개의 머신을 백업하기 전에 표준 머신 백업

유사한 내용이 포함된 여러 개의 머신을 백업할 경우, 먼저 하나의 머신을 백업하고 백업된 데이터의 인덱싱 작업이 완료될 때까지 기다리는 것이 좋습니다. 이후 효율적인 중복 제거 덕분에 나머지 머신이 보다 빠르게 백업됩니다. 첫 번째 머신의 백업에 대한 인덱싱이 완료되었기 때문에 대부분의 데이터가 이미 중복 제거 데이터 저장소에 포함됩니다.

서로 다른 시간에 여러 머신 백업

다수의 머신을 백업하는 경우 시간에 따라 백업 작업을 분산시킵니다. 이렇게 하려면 다양한 스케줄로 여러 개의 보호 계획을 생성합니다.

위치 암호화

암호화로 위치를 보호할 경우 위치에 작성된 모든 내용은 암호화되고 여기에서 읽는 모든 내용은 노드에 저장된 위치 기준 암호화 키를 사용하여 스토리지 노드에 의해 투명하게 암호 해독됩니다. 저장소 미디어를 도난당했거나 인증되지 않은 사용자가 무단 액세스하는 경우, 스토리지 노드에 액세스하지 않고 위반자가 위치 내용을 암호 해독할 수 없습니다.

이 암호화는 보호 계획에서 지정하고 에이전트에서 수행하는 백업 암호화와 아무런 관련이 없습니다. 백업이 이미 암호화된 경우 스토리지 노드 측 암호화가 에이전트에서 수행하는 암호화에 우선하여 적용됩니다.

암호화로 위치를 보호하려면

1. 암호화 키를 생성하는 데 사용할 단어(비밀번호)를 지정하고 확인합니다.
   단어는 대/소문자를 구분합니다. 다른 스토리지 노드에 위치를 연결하는 경우에만 이 단어를 물어봅니다.
2. 다음 암화화 알고리즘 중 하나를 선택합니다.
   - **AES 128** – 위치 내용이 128비트 키와 함께 AES(Advanced Encryption Standard) 알고리즘을 사용하여 암호화됩니다.
   - **AES 192** – 위치 내용이 192비트 키와 함께 AES 알고리즘을 사용하여 암호화됩니다.
   - **AES 256** – 위치 내용이 256비트 키와 함께 AES 알고리즘을 사용하여 암호화됩니다.
3. **확인**을 클릭합니다.

AES 암호 알고리즘은 CBC(사이퍼 블록 체이닝) 모드에서 작동하며 128, 192 또는 256비트의 사용자 정의 크기로 임의 생성된 키를 사용합니다. 키 크기가 클수록 프로그램이 위치에 저장된 백업을 암호화하는 시간이 오래 걸리며 백업이 더욱 안전해집니다.

그런 다음 암호화 키는 SHA-256 해시의 선택한 단어를 키로 사용하여 AES-256으로 암호화됩니다. 단어 자체는 디스크의 어디에도 저장되지 않고, 단어 해시는 확인 용도로 사용됩니다. 이 두 가지 수준의 보안을 사용하여 백업은 무단 액세스로부터 보호되지만 분실한 단어는 복구할 수 없습니다.

목록화

데이터 카탈로그

데이터 카탈로그를 사용하면 필요한 데이터 버전을 쉽게 찾고 복구 대상으로 선택할 수 있습니다. 데이터 카탈로그에는 목록화가 활성화되어 있거나 활성화되었던 관리 위치에 저장된 데이터가 표시됩니다.

카탈로그 섹션은 하나 이상의 카탈로그 서비스가 관리 서버에 등록된 경우에만 **백업 스토리지** 탭 아래에 표시됩니다. 카탈로그 서비스 설치에 대한 자세한 내용은 "스토리지 노드 및 카탈로그 서비스 설치"를 참조하십시오.

카탈로그 섹션은 조직 관리자에게만 표시됩니다.

제한 사항

목록화는 실제 머신의 디스크 및 파일 수준 백업과 가상 머신의 백업에 대해서만 지원됩니다.

다음 데이터는 카탈로그에 표시할 수 없습니다.

- 암호화된 백업의 데이터
- 테이프 장치에 백업된 데이터
- 클라우드 스토리지에 백업된 데이터
- Acronis Cyber Protect 12.5 이하 제품 버전으로 백업된 데이터

복구할 백업 데이터 선택

1. **백업 스토리지** > **카탈로그**를 클릭합니다.
2. 관리 서버에 여러 목록화 서비스가 등록되는 경우에는 해당 위치에 저장된 백업을 목록화하는 서비스를 선택합니다.

   참고
   위치를 목록화하는 서비스를 확인하려면 **백업** > **스토리지** > **위치** > **위치**에서 위치를 선택한 후 **세부정보**를 클릭합니다.

3. 그러면 선택한 카탈로그 서비스를 통해 목록화된 관리 위치에 백업된 머신이 표시됩니다. 찾아보기 또는 검색을 통해 복구할 데이터를 선택합니다.

- **찾아보기**

  머신을 두 번 클릭하면 백업된 디스크, 볼륨, 폴더 및 파일을 확인할 수 있습니다.

  디스크를 복구하려면  아이콘이 표시되어 있는 디스크를 선택합니다.

  볼륨을 복구하려면 해당 볼륨이 포함된 디스크를 두 번 클릭하고 볼륨을 선택합니다.

  파일 및 폴더를 복구하려면 파일 및 폴더가 위치한 볼륨을 찾습니다.  폴더 아이콘이 표시되어 있는 볼륨을 찾으면 됩니다.
- **검색**

  검색 필드에, 필요한 데이터 항목 식별에 도움이 되는 정보(예를 들어, 머신 이름, 파일 또는 폴더 이름, 디스크 레이블)를 입력한 다음 **검색**을 클릭합니다.

  별표(*) 및 물음표(?)를 와일드카드로 사용할 수 있습니다.

  검색 결과로 입력된 값과 이름이 전체 또는 일부가 일치하는 백업된 데이터 항목의 목록이 표시됩니다.

4. 데이터는 기본적으로 최신 시점으로 되돌아갑니다. 단일 항목을 선택한 경우 **버전** 버튼을 사용하여 복구 지점을 선택할 수 있습니다.
5. 필요한 데이터를 선택한 경우 다음 중 하나를 수행하십시오.
   - **복구**를 클릭하고 "복구"의 설명대로 복구 작업의 매개변수를 구성합니다.
   - [파일/폴더만 해당] 파일을 .zip 파일로 저장하려면 **다운로드**를 클릭하고 데이터를 저장할 위치를 선택한 다음 **저장**을 클릭합니다.

모범 사례 목록화

목록화 성능을 높이려면 다음의 권장 사항을 따르십시오.

설치

카탈로그 서비스와 스토리지 노드를 개별 머신에 설치하는 것이 좋습니다. 그렇지 않으면 이러한 컴퍼넌트가 CPU 및 RAM 리소스를 얻기 위해 경쟁합니다.

관리 서버에 여러 스토리지 노드가 등록된 경우에는 인덱싱 또는 검색 성능이 저하되지 않는 한 하나의 카탈로그 서비스로 충분합니다. 예를 들어 목록화가 연중 무휴 작동 중인 것(목록화 활동 간에 일시 정지가 없다는 것)을 인식하면 별도의 머신에 카탈로그 서비스를 하나 더 설치합니다. 그 다음에 일부 관리 위치를 제거하고 새 카탈로그 서비스를 사용하여 관리 위치를 다시 만듭니다. 이러한 위치에 저장된 백업은 그대로 유지됩니다.

시스템 요구 사항

매개변수	최소값	권장 값
CPU 코어 수	2	4개 이상
RAM	8GB	16GB 이상

하드 디스크	7200rpm HDD	SSD
스토리지 노드가 있는 머신과 카탈로그 서비스가 있는 머신 간 네트워크 연결	100Mbps	1Gbps

목록화를 활성화하거나 비활성화하려면

관리되는 위치에 대해 목록화가 활성화되어 있으면 해당 위치로의 각 백업 콘텐츠가 백업이 생성되는 즉시 데이터 카탈로그에 추가됩니다.

관리되는 위치를 추가할 때 또는 이후에 목록화를 활성화할 수 있습니다. 목록화를 활성화하면 해당 위치에 저장되어 있고 이전에 목록화되지 않았던 모든 백업이 해당 위치로의 다음 백업 후 목록화됩니다.

목록화 프로세스는 특히 같은 위치로 많은 머신을 백업하는 경우 오래 걸릴 수 있습니다. 목록화는 언제든 비활성화할 수 있습니다. 비활성화 이전에 생성된 백업의 목록화는 완료됩니다. 새로 생성된 백업은 목록화되지 않습니다.

기존 위치에 대해 목록화를 구성하려면

1. **백업 스토리지** > **위치**를 클릭합니다.
2. **위치**를 클릭한 다음 목록화를 구성하려는 관리되는 위치를 선택합니다.
3. **편집**을 클릭합니다.
4. **카탈로그 서비스** 스위치를 활성화 또는 비활성화합니다.
5. **완료**를 클릭합니다.

시스템 설정

이러한 설정은 온프레미스 디플로이에서만 사용 가능합니다.

이러한 설정에 액세스하려면 **설정** > **시스템 설정**을 클릭합니다.

시스템 설정 섹션은 조직 관리자에게만 표시됩니다.

이메일 알림

관리 서버에서 전송되는 모든 이메일 알림에 공통으로 적용되는 전역 설정을 구성할 수 있습니다.

기본 백업 옵션에서 백업 중에 발생하는 이벤트에 대해서만 이러한 설정을 오버라이드할 수 있습니다. 이 경우 전역 설정은 백업 이외의 작업에 대해서 유효합니다.

보호 계획을 생성할 때, 사용할 설정을 전역 설정 또는 기본 백업 옵션에 지정된 설정 중에서 선택할 수 있습니다. 이 설정은 계획에만 특정하게 적용되는 사용자 정의 값으로 오버라이드할 수도 있습니다.

중요
전역 이메일 알림 설정이 변경되면 전역 설정을 사용하는 모든 보호 계획이 영향을 받습니다.

이러한 설정을 구성하기 전에 이메일 서버 설정이 구성되었는지 확인하십시오.

전역 이메일 알림 설정을 구성하려면

1. **설정** > **시스템 설정** > **이메일 알림**을 클릭합니다.
2. **받는 사람 이메일 주소** 필드에 목적지 이메일 주소를 입력합니다. 여러 주소를 세미콜론으로 구분하여 입력할 수 있습니다.
3. [선택 사항] **제목**에서 이메일 알림 제목을 변경합니다.
   다음 변수를 사용할 수 있습니다.
   - [Alert] - 경보 요약입니다.
   - [Device] - 장치 이름입니다.
   - [Plan] - 경보를 생성한 계획의 이름입니다.
   - [ManagementServer] - 관리 서버가 설치된 머신의 호스트 이름입니다.
   - [Unit] - 머신이 속한 단위의 이름입니다.

   기본 제목은 다음과 같습니다. [Alert] **장치:** [Device] **계획:** [Plan]
4. [선택 사항] **활성 경보에 대한 일일 확인** 확인란을 선택하고 다음을 수행합니다.
   a. 확인이 전송되는 시간을 지정합니다.
   b. [선택 사항] **'활성 경보 없음' 메시지는 전송 안 함** 확인란을 선택합니다.
5. [선택 사항] 이메일 알림에서 사용할 언어를 선택합니다.
6. 알림을 받을 이벤트의 확인란을 선택합니다. 심각도별로 그룹화된 모든 가능한 경보 목록에서 선택할 수 있습니다.
7. **저장**을 클릭합니다.

이메일 서버

관리 서버에서 이메일 알림을 보내는 데 사용할 이메일 서버를 지정할 수 있습니다.

이메일 서버를 지정하려면

1. **설정** > **시스템 설정** > **이메일 서버**를 클릭합니다.
2. **이메일 서비스**에서 다음 중 하나를 선택합니다.
   - **사용자 정의**
   - **Gmail**
   - **Yahoo Mail**
   - **Outlook.com**
3. [사용자 정의 이메일 서비스에만 해당] 다음 설정을 지정합니다.
   - **SMTP 서버**에 보내는 메일 서버(SMTP)의 이름을 입력합니다.
   - **SMTP 포트**에 보내는 메일 서버 포트를 설정합니다. 기본적으로 포트는 25로 설정됩니다.
   - SSL 또는 TLS 암호화를 사용할지 여부를 선택합니다. 암호화를 비활성화하려면 **없음**을 선택하십시오.
   - SMTP 서버에서 인증을 요구하는 경우 **SMTP 서버에 인증이 필요** 확인란을 선택한 다음 메시지를 보내는 데 사용될 계정의 자격 증명을 지정합니다. SMTP 서버에 인증이 필요한지 여부를 알 수 없는 경우에는 네트워크 관리자 또는 이메일 서비스 공급자에게 도움을 요청하십시오.
4. [Gmail, Yahoo Mail, Outlook.com만 해당] 메시지를 보내는 데 사용될 계정의 자격 증명을 지정합니다.
5. [사용자 정의 이메일 서비스에만 해당] **보내는 사람**에 보내는 사람의 이름을 입력합니다. 이 이름은 이메일 알림에서 **발신** 필드에 표시됩니다. 이 필드를 비워두면 3 또는 4단계에서 지정한 계정이 메시지에 포함됩니다.
6. [선택 사항] 이메일 알림이 지정된 설정으로 올바르게 작동하는지 여부를 확인하려면 **테스트 메시지 보내기**를 클릭합니다. 테스트 메시지를 보낼 이메일 주소를 입력합니다.

보안

이 옵션을 사용하여 Acronis Cyber Protect 온-프레미스 디플로이의 보안을 강화합니다.

다음 시간 후 작업 중이지 않은 사용자 로그아웃

이 옵션을 사용하여 사용자 비활성으로 인한 자동 로그아웃 시간 초과 값을 지정할 수 있습니다. 설정된 시간 초과 값이 1분 남으면 사용자에게 로그인을 유지할지 묻습니다. 그렇지 않으면 사용자가 로그아웃되고 저장되지 않은 변경 사항은 모두 손실됩니다.

사전 설정값이 **활성화됨. 시간 초과: 10분.**

현재 사용자의 최근 로그인에 대한 알림 표시

이 옵션을 사용하면 사용자의 최근 로그인 날짜 및 시간, 마지막 로그인 이후 인증 실패 횟수, 마지막 로그인의 IP 주소가 표시되도록 할 수 있습니다. 이 정보는 사용자가 로그인할 때마다 화면 맨 아래에 표시됩니다.

사전 설정값이 **비활성화됨**.

로컬 또는 도메인 비밀번호 만료 경고

이 옵션을 사용하면 Acronis Cyber Protect Management Server에 액세스하기 위한 사용자의 패스워드가 만료되는 시간을 표시할 수 있습니다. 이 비밀번호는 사용자가 관리 서버가 설치되어 있는 머신에 로그온하는 데 사용할 로컬 또는 도메인 비밀번호입니다. 암호 만료까지 남은 시간은 화면 맨 아래, 그리고 오른쪽 상단 구석의 계정 메뉴에 표시됩니다.

사전 설정값이 **비활성화됨**.

업데이트

이 옵션은 조직 관리자가 웹 콘솔에 로그인할 때마다 Acronis Cyber Protect에서 새 버전을 확인하는지 여부를 정의합니다.

사전 설정값이 **활성화됨**.

이 옵션을 비활성화하면 관리자가 "소프트웨어 업데이트 확인"의 설명처럼 업데이트를 수동으로 확인할 수 있습니다.

기본 백업 옵션

백업 옵션의 기본값은 관리 서버의 모든 보호 계획에 대해 공통적입니다. 조직 관리자는 기본 옵션 값을 미리 정의된 값으로 변경할 수 있습니다. 변경을 수행한 후 생성된 모든 보호 계획에서 기본적으로 새 값이 사용됩니다.

보호 계획을 생성할 때 이 계획에만 적용되는 사용자 정의 값으로 기본값을 오버라이드할 수 있습니다.

기본 옵션 값을 변경하려면

1. 조직 관리자로 Cyber Protect 웹 콘솔에 로그인합니다.
2. **설정** > **시스템 설정**을 클릭합니다.
3. **기본 백업 옵션** 섹션을 확장합니다.
4. 옵션을 선택하고 필요한 변경 작업을 수행합니다.
5. **저장**을 클릭합니다.

보호 설정

보호 설정을 구성하려면 Cyber Protect 웹 콘솔에서 **설정** > **보호**로 이동합니다.

구체적인 설정과 절차에 대한 자세한 내용은 이 섹션의 개별 항목을 참조하십시오.

보호 정의 업데이트

기본적으로 모든 보호 에이전트는 인터넷에 연결하여 다음 컴포넌트의 업데이트를 다운로드할 수 있습니다.

- 맬웨어 방지
- 취약성 평가
- 패치 관리

업데이터 역할이 설정된 에이전트

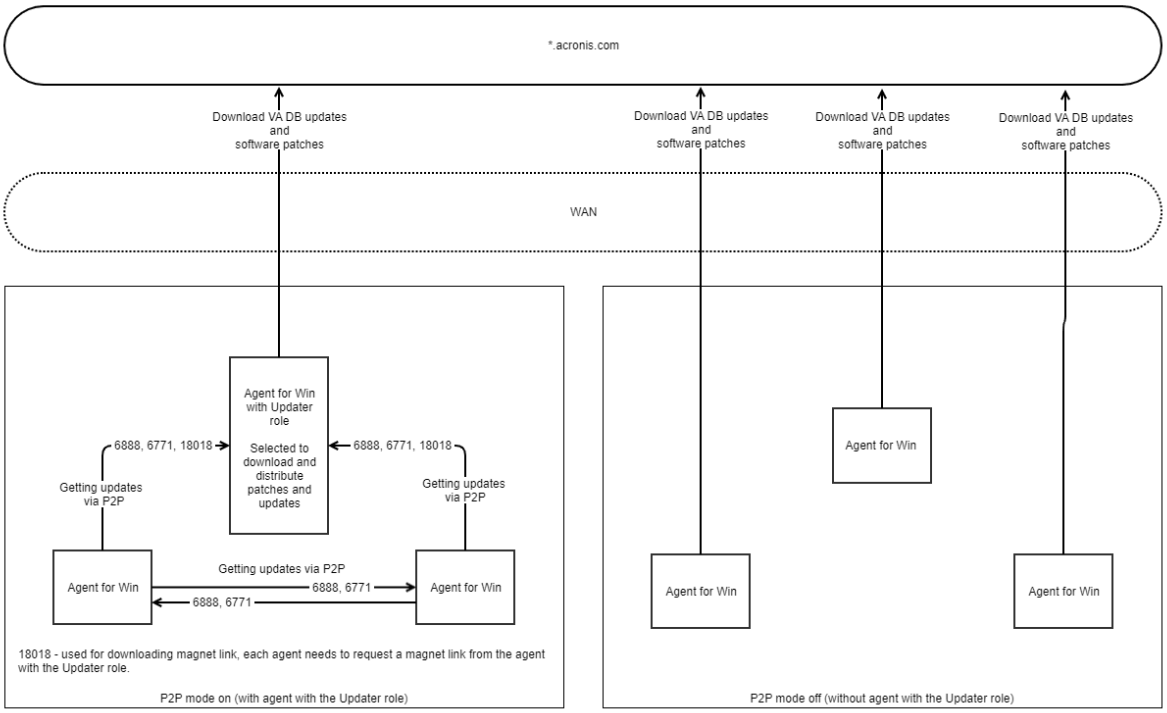
관리자는 환경에서 보호 에이전트를 하나 이상 선택한 다음 업데이터 역할을 할당하는 방식으로 네트워크 대역폭 트래픽을 최소화할 수 있습니다. 그러면 전용 에이전트가 인터넷에 연결하여 업데이트를 다운로드합니다. 기타 모든 에이전트는 피어 투 피어 기술을 사용하여 전용 업데이터 에이전트에 연결한 다음 해당 에이전트에서 업데이트를 다운로드합니다.

업데이터 역할이 지정되지 않은 에이전트는 환경 내에 전용 업데이터 에이전트가 없거나 약 5분 동안 전용 업데이트 에이전트 연결을 설정할 수 없으면 인터넷에 연결합니다.

에이전트에 업데이터 역할을 할당하기 전에 에이전트가 실행되는 머신의 성능이 업데이트 역할을 수행하기에 충분하고, 머신의 고속 인터넷 연결 상태가 안정적이며, 디스크 공간이 충분한지 확인하십시오.

환경 내의 여러 에이전트에 업데이터 역할을 할당할 수 있습니다. 그러면 업데이터 역할이 할당된 에이전트 하나가 오프라인 상태로 전환되는 경우 해당 역할의 다른 에이전트가 업데이트된 보호 정의의 소스 역할을 할 수 있습니다.

다음 다이어그램에서는 보호 업데이트를 다운로드하기 위한 옵션을 설명합니다. 왼쪽에는 에이전트에 업데이터 역할이 할당되어 있습니다. 이 에이전트는 보호 업데이트 다운로드를 위해 인터넷에 연결하며, 해당 피어 에이전트는 업데이터 에이전트에 연결하여 최신 업데이트를 가져옵니다. 오른쪽에는 에이전트에 업데이터 역할이 할당되어 있지 않으므로 모든 에이전트가 보호 업데이트 다운로드를 위해 인터넷에 연결합니다.



업데이트 역할용으로 머신을 준비하려면

1. 업데이터 역할이 설정된 에이전트를 실행할 머신에서 다음 방화벽 규칙을 적용합니다.
   - 인바운드(들어옴) "updater_incoming_tcp_ports": 모든 방화벽 프로필(공개, 비공개, 도메인)에 대해 TCP 포트 18018 및 6888로의 연결을 허용합니다.
   - 인바운드(들어옴) "updater_incoming_udp_ports": 모든 방화벽 프로필(공개, 비공개, 도메인)에 대해 UDP 포트 6888로의 연결을 허용합니다.
2. Acronis Agent Core 서비스를 다시 시작합니다.
3. 방화벽 서비스를 다시 시작합니다.

이러한 규칙을 적용하지 않고 방화벽을 활성화하면 피어 에이전트가 클라우드에서 업데이트를 다운로드합니다.

에이전트에 업데이터 역할을 할당하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 업데이터 역할을 할당할 에이전트가 있는 머신을 선택합니다.
3. **세부정보**를 클릭하고 **이 에이전트를 다운로드해 패치 및 업데이트 배포** 스위치를 활성화합니다.

업데이트 예약

모든 에이전트에서 보호 정의 자동 업데이트를 예약할 수도 있고 선택한 에이전트에서 보호 정의를 수동으로 업데이트할 수도 있습니다.

자동 업데이트를 예약하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **보호** > **보호 정의 업데이트**로 이동합니다.
2. **예약**을 선택합니다.
3. **예약 유형**에서 다음 중 하나를 선택합니다.
   - **일일**

     보호 정의를 업데이트할 요일을 선택합니다.

     시작 시간에서 업데이트를 시작할 시간을 선택합니다.
   - **매시간**

     업데이트의 개별 스케줄을 설정합니다.

     실행 빈도에서 업데이트 주기를 설정합니다.

     시작...종료에서 업데이트의 구체적인 시간 범위를 설정합니다.

보호 정의를 수동으로 업데이트하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **에이전트**로 이동합니다.
2. 에이전트의 보호 정의를 업데이트할 머신을 선택한 다음 **정의 업데이트**를 클릭합니다.

다운로드 위치 변경

보호 정의는 머신의 기본 임시 폴더에 다운로드된 후 Acronis 프로그램 폴더에 저장됩니다.

다운로드용 임시 폴더를 변경하려면

1. 관리 서버 머신에서 편집을 위해 `atp-database-mirror.json` 파일을 엽니다.

   이 파일의 위치는 다음과 같습니다.
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
2. `"enable_user_config"`의 값을 `true`로 변경합니다.

   ```
   {
   "sysconfig":
   {
   ...
   "enable_user_config": true
   }
   ...
   }
   ```
3. 관리 서버 머신에서 편집을 위해 `config.json` 파일을 엽니다.

   이 파일의 위치는 다음과 같습니다.
   - Windows: `%programdata%\Acronis\AtpDatabaseMirror\`
   - Linux: `/var/lib/Acronis/AtpDatabaseMirror/`
4. `"mirror_temp_dir": "<새 다운로드 위치의 경로>"` 줄을 추가합니다.

   예:

   ```
   {
           "mirror_temp_dir": "C:\\temp"
   }
   ```

AppData 폴더의 절대 경로나 상대 경로를 추가할 수 있습니다.
폴더를 생성할 수 없거나 관리 서버가 해당 폴더에 쓸 수 없는 경우 기본 위치가 사용됩니다.

캐시 스토리지 옵션

캐시된 데이터는 다음 위치에 저장됩니다.

- Windows: `C:\ProgramData\Acronis\Agent\var\atp-downloader\Cache`
- Linux: `/opt/acronis/var/atp-downloader/Cache`
- macOS: `/Library/Application Support/Acronis/Agent/var/atp-downloader/Cache`

오래된 캐시된 데이터를 지울 스케줄을 구성하고 캐시된 데이터 크기의 제한을 설정할 수 있습니다. 업데이터가 아닌 에이전트가 설치되어 있는 머신과 업데이터 에이전트가 설치되어 있는 머신에 각기 다른 제한을 설정할 수 있습니다.

최신 보호 정의를 다운로드할 소스

다음 위치에서 최신 보호 정의를 다운로드할 수 있습니다.

- **Cloud**
  보호 에이전트가 인터넷에 연결하고 Acronis Cloud에서 최신 보호 정의를 다운로드합니다. 기본적으로 관리 서버에 등록된 모든 에이전트가 업데이트를 확인하고 이를 배포합니다. 업데이터 역할이 설정된 에이전트에 대한 자세한 내용은 "보호 정의 업데이트"(577페이지) 항목을 참조하십시오.
- **Cyber Protect Management Server**
  이 옵션을 사용하는 경우 에이전트가 인터넷에 접속할 필요가 없습니다. 에이전트는 보호 정의가 저장된 관리 서버에만 연결합니다. 하지만 최신 보호 정의를 다운로드하기 위해서는 관리 서버가 인터넷에 연결되어야 합니다.
- **사용자 지정 웹 서버**
  이 옵션은 문제 해결 및 테스트에 사용하거나 에어갭 환경에서 사용하기 위해 고안되었습니다. 자세한 내용은 "에어갭 환경의 보호 정의 업데이트"(581페이지) 항목을 참조하십시오. 일반적으로 이 옵션은 Acronis 지원 팀에서 선택하도록 요청한 경우에만 선택해야 합니다.

원격 연결

원격 연결을 활성화하면 Cyber Protect 웹 콘솔 오른쪽 메뉴의 **Cyber Protection Desktop** 아래에 **RDP 클라이언트를 통해 연결** 및 **HTML5 클라이언트를 통해 연결** 옵션이 표시됩니다. **장치** 탭에서 워크로드를 선택하면 오른쪽 메뉴가 열립니다.

원격 연결 활성화나 비활성화는 조직의 모든 사용자에게 적용됩니다.

원격 연결을 활성화하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **보호**로 이동합니다.
2. **원격 연결**을 클릭한 다음 **원격 데스크톱 연결** 스위치를 활성화합니다.

그리고 원격 연결 공유도 활성화할 수 있습니다. 이 옵션을 사용하면 선택한 워크로드에 원격으로 액세스하는 데 사용 가능한 링크를 생성할 수 있습니다. 이러한 링크를 다른 사용자들과 공유할 수 있습니다.

원격 연결 공유를 활성화하려면

1. Cyber Protect 웹 콘솔에서 **설정** > **보호**로 이동합니다.
2. **원격 데스크톱 연결 공유** 확인란을 선택합니다.

그러면 Cyber Protect 웹 콘솔 오른쪽 메뉴의 **Cyber Protection Desktop** 아래에 **원격 연결 공유** 옵션이 표시됩니다.

에어갭 환경의 보호 정의 업데이트

Acronis Cyber Protect에서는 에어갭 환경의 보호 정의를 업데이트할 수 있습니다.

에어갭 환경의 보호 정의를 업데이트하려면

1. 에어갭 환경 외부에 인터넷에 액세스할 수 있는 두 번째 관리 서버를 설치합니다.
   이 작업을 수행하는 방법에 대한 자세한 내용은 "관리 서버 설치"(79페이지) 항목을 참조하십시오.
2. 온라인 관리 서버에서 이동식 드라이브로 보호 정의를 복사한 다음 에어갭 환경의 HTTP 서버로 정의를 전송합니다.
   이 단계에 대한 자세한 내용은 "온라인 관리 서버에 정의 다운로드"(581페이지) 및 "HTTP 서버로 정의 전송"(582페이지) 항목을 참조하십시오.
3. 에어갭 관리 서버에서 HTTP 서버를 업데이트된 보호 정의의 소스로 구성합니다.
   이 단계에 대한 자세한 내용은 "에어갭 관리 서버에서 정의의 소스 구성"(583페이지) 항목을 참조하십시오.

온라인 관리 서버에 정의 다운로드

인터넷에 액세스할 수 있는 두 번째 관리 서버를 설치한 후에는 최신 보호 정의를 다운로드한 후 USB 플래시 메모리나 외부 하드 드라이브와 같은 이동식 드라이브에 복사합니다.

보호 정의를 다운로드 및 복사하려면

1. 온라인 관리 서버가 설치되어 있는 머신의 선택한 위치에 `AtpDatabaseMirror` 폴더를 복사합니다. 예를 들어 바탕 화면이나 `Temp` 폴더를 선택할 수 있습니다.

   `AtpDatabaseMirror` 폴더의 위치는 다음과 같습니다.
   - Windows: `%ProgramData%\Acronis\`
   - Linux: `/usr/lib/Acronis/`
2. 편집을 위해 `atp_database_mirror.json` 파일을 엽니다. 이 파일의 위치는 다음과 같습니다.
   - Windows: `%Program Files%\Acronis\AtpDatabaseMirror`

   참고
   Windows에서 이 폴더는 이전 단계에서 사용한 폴더와 다릅니다.

- Linux: `/usr/lib/Acronis/AppDatabaseMonitor`

3. `atp_database_mirror.json` 파일을 다음과 같이 편집합니다.
   a. `"enable_appdata_as_root"`의 값을 `false`로 변경합니다.
   b. 모든 `"local_path"` 항목의 값을 보호 정의를 저장할 위치의 절대 경로로 변경합니다.
4. `atp_database_mirror.json` 파일의 변경 사항을 저장합니다.
5. 온라인 관리 서버가 설치된 머신에서 다음 명령을 사용하여 **Acronis Management Server Service**를 중지합니다.
   - Windows(명령 프롬프트):

     ```
     sc stop AcrMngSrv
     ```

   - Linux(터미널):

     ```
     sudo systemctl stop acronis_ams.service
     ```

6. 선택한 위치에 복사한 `AtpDatabaseMirror` 폴더에서 다음 명령을 사용하여 `AtpDatabaseMirror` 도구를 시작합니다.
   - Windows(명령 프롬프트):

     ```
     atp_database_mirror.exe -config atp_database_mirror.json
     ```

   - Linux(터미널):

     ```
     sudo ./atp_database_mirror -config atp_database_mirror.json
     ```

   `"local_path"`에 지정한 폴더에 모든 업데이트가 다운로드되면 명령 프롬프트 또는 터미널 창에 다음 줄이 표시됩니다.

   ```
   standing by for 1m0s
   ```

7. Ctrl+C를 눌러 `AtpDatabaseMirror` 도구를 중지합니다.
8. `"local_path"`에 지정한 폴더의 파일을 이동식 드라이브에 복사합니다.

다음으로는 이동식 드라이브에서 에어갭 환경의 HTTP 서버로 파일을 복사해야 합니다. 에어갭 관리 서버를 HTTP 서버로 사용할 수 있습니다. 자세한 내용은 "HTTP 서버로 정의 전송"(582페이지) 항목을 참조하십시오.

HTTP 서버로 정의 전송

에어갭 환경에서 보호 정의를 배포하려면 전용 HTTP 서버가 필요합니다. 에어갭 관리 서버를 HTTP 서버로 사용할 수 있습니다.

HTTP 서버로 보호 정의를 전송하려면

1. HTTP 서버를 실행할 머신에서 선택한 폴더에 보호 정의를 복사합니다.
2. 보호 정의를 복사한 폴더에서 HTTP 서버를 시작합니다.
   예를 들어 Python을 사용하여 다음 명령을 실행할 수 있습니다.


```
python -m http.server 8080
```

참고
원하는 어떤 HTTP 서버나 사용 가능합니다.

3. 보호 정의를 복사한 폴더에서 편집을 위해 다음 update-index.json 파일을 엽니다.
   - ./ngmp/update-index.json
   - ./vapm/update-index.json
4. 두 update-index.json 파일에서 모든 products > os > arch > components > versions > url 필드를 다음과 같이 편집합니다.
   a. IP 및 포트 값으로는 HTTP 서버의 IP 주소와 포트를 설정합니다.
   b. 경로의 다른 부분은 변경하지 마십시오.
   예를 들어 "url": "http://192.168.1.10:8080/ngmp/win64/ngmp.zip"과 같이 편집할 수 있습니다. 여기서 192.168.1.10은 HTTP 서버의 IP 주소이고 8080은 해당 서버의 포트입니다. /ngmp/win64/ngmp.zip 부분은 변경하지 마십시오.
5. 두 update-index.json 파일에서 편집 사항을 저장합니다.

다음으로는 에어갭 관리 서버에서 보호 정의의 소스를 구성해야 합니다. 자세한 내용은 "에어갭 관리 서버에서 정의의 소스 구성"(583페이지) 항목을 참조하십시오.

에어갭 관리 서버에서 정의의 소스 구성

HTTP 서버를 구성한 후에는 에어갭 관리 서버에서 해당 서버를 보호 정의의 소스로 구성해야 합니다.

에어갭 관리 서버에서 보호 정의의 소스를 구성하려면

1. 에어갭 관리 서버의 Cyber Protect 웹 콘솔에서 **설정** > **보호** > **보호 정의 업데이트**로 이동합니다.
2. **정의**를 선택합니다.
3. **사용자 정의**를 선택한 후 다음 경로를 지정합니다.

- **안티바이러스 및 안티맬웨어 정의**:
  `http://<IP address of your HTTP server>:8080/scanner`
- **고급 감지 정의**:
  `http://<IP address of your HTTP server>:8080/ngmp`
- **취약점 평가 및 패치 관리 정의**:
  `http://<IP address of your HTTP server>:8080/vapm`

따라서 에어갭 환경의 에이전트가 HTTP 서버에서 보호 정의를 다운로드합니다.

사용자 계정 및 조직 단위 관리

온프레미스 디플로이

이 섹션에서 설명하는 기능은 조직 관리자만 사용할 수 있습니다.

이러한 설정에 액세스하려면 **설정** > **계정**을 클릭합니다.

단위 및 관리자 계정

단위 및 관리자 계정을 관리하려면 Cyber Protect 웹 콘솔에서 **설정** > **계정**으로 이동합니다. **계정** 패널에는 **Organization** 그룹과 함께 단위 트리(있는 경우) 및 선택한 계층 구조 수준의 관리자 계정 목록이 표시됩니다.

부서

관리 서버를 설치하면 **Organization** 그룹이 자동으로 생성됩니다. Acronis Cyber Protect Advanced 라이센스를 사용하면 일반적으로 조직의 단위 또는 부서에 해당하는 단위라는 자식 그룹을 생성하고 관리자 계정을 단위에 추가할 수 있습니다. 이 방법을 통해 다른 사용자에게 보호 관리를 위임할 수 있으며, 이렇게 위임받은 사용자의 액세스 권한은 해당 부서로 엄격히 제한됩니다. 단위 생성 방법에 대한 자세한 내용은 "단위 생성"(588페이지) 항목을 참조하십시오.

모든 단위에는 하위 단위가 있을 수 있습니다. 부모 단위의 관리자 계정은 모든 자식 단위에서도 동일한 권한을 보유합니다. **Organization** 그룹은 가장 높은 수준의 부모 단위이며 이 수준의 관리자 계정은 모든 단위에서 동일한 권한을 보유합니다.

관리자 계정

Cyber Protect 웹 콘솔에 로그인할 수 있는 계정은 관리자 계정입니다.

Cyber Protect 웹 콘솔에서 관리자 계정은 해당 단위의 계층 구조 수준에 있거나 그 아래에 있는 모든 항목을 보거나 관리할 수 있습니다. 예를 들어 *조직*의 관리자 계정은 가장 높은 수준에 액세스할 수 있으므로 이 조직의 모든 단위에 액세스할 수 있지만 특정 *단위*의 관리자 계정은 해당 단위와 그 자식 단위에만 액세스할 수 있습니다.

어떤 계정이 관리자 계정일 수 있습니까?

관리 서버가 Active Directory 도메인에 포함된 Windows 머신에 설치된 경우 로컬 사용자나 Active Directory 도메인 포리스트 내의 사용자 또는 사용자 그룹에 관리자 권한을 부여할 수 있습니다.

기본적으로 관리 서버는 Active Directory 도메인 컨트롤러에 대해 SSL/TLS로 보호되는 연결을 설정합니다. SSL/TLS로 보호되는 연결을 설정할 수 없으면 연결이 설정되지 않습니다. 하지만 `auth-connector.json5` 파일을 편집하여 비보안 연결을 허용할 수 있습니다.

보안 연결을 사용하려면 Active Directory에 대해 LDAPS(LDAP over SSL)가 구성되어 있는지 확인하십시오.

Active Directory에 대해 LDAPS를 구성하려면

1. 도메인 컨트롤러에서 Microsoft 요구 사항을 충족하는 LDAPS 인증서를 만들고 설치합니다.
   이 작업을 수행하는 방법은 Microsoft 설명서에서 타사 인증 기관을 통해 LDAP over SSL 활성화를 참조하십시오.
2. 도메인 컨트롤러에서 **Microsoft 관리 콘솔**을 열고 **인증서(로컬 컴퓨터)** > **개인** > **인증서** 아래에 인증서가 있는지 확인합니다.
3. 도메인 컨트롤러를 다시 시작합니다.
4. LDAPS가 활성화되어 있는지 확인합니다.

도메인 컨트롤러에 대한 비보안 연결을 허용하려면

1. 관리 서버가 설치되어 있는 머신에 로그인합니다.
2. 편집을 위해 `auth-connector.json5` 파일을 엽니다.
   `auth-connector.json5` 파일은 `%APPDATA%\Acronis\AuthConnector`에 있습니다.
3. **sync** 섹션으로 이동하여 **"connectionMode"** 줄에서 **"ssl_only"**를 **"auto"**로 바꿉니다.
   auto 모드에서는 TLS로 연결할 수 없는 경우 비보안 연결이 설정됩니다.
4. 에 설명된 대로 **Acronis Service Manager 서비스**를 다시 시작합니다.

참고
관리 서버가 Active Directory 도메인에 포함되어 있지 않거나 Linux 머신에 설치된 경우 로컬 사용자 및 그룹에 관리자 권한을 부여할 수 있습니다.

관리 서버에 관리자 계정을 추가하는 방법을 자세히 알아보려면 "관리자 계정 추가"(587페이지) 항목을 참조하십시오.

관리자 계정 역할

각각의 관리자 계정에는 특정 작업을 수행하는 데 필요한 사전 정의된 권한이 있는 역할이 할당됩니다. 관리자 계정 역할은 다음과 같습니다.

- **관리자**
  이 역할은 조직 또는 단위에 전체 관리자 권한으로 액세스할 수 있습니다.
- **읽기 전용**
  이 역할은 Cyber Protect 웹 콘솔에 읽기 전용으로 액세스할 수 있습니다. 이 역할로는 시스템 보고서와 같은 진단 데이터를 수집할 수만 있습니다. 읽기 전용 역할로는 백업을 검색하거나 백업된 사서함의 내용을 검색할 수 없습니다.
- **감사인**
  이 역할은 Cyber Protect 웹 콘솔의 **활동** 탭에 읽기 전용으로 액세스할 수 있습니다. 이 탭에 대한 자세한 내용은 "활동 탭"(537페이지) 항목을 참조하십시오. 이 역할로는 관리 서버의 시스템 정보를 포함하여 어떤 데이터도 수집하거나 내보낼 수 없습니다.

역할과 관련한 모든 변경 사항은 **작업** 탭에 표시됩니다.

역할의 상속

상위 단위의 역할은 해당 하위 단위에 상속됩니다. 하나의 사용자 계정에 대해 상위 단위와 하위 단위에서 서로 다른 역할이 할당된 경우 두 역할을 모두 보유하게 됩니다.

또한 역할은 특정 사용자 계정에 명시적으로 할당되거나 사용자 그룹으로부터 상속될 수 있습니다. 따라서 사용자 계정은 특별히 할당된 역할과 상속된 역할을 모두 보유할 수 있습니다.

하나의 사용자 계정에 서로 다른 역할(할당 및/또는 상속된 역할)이 있는 경우 객체에 액세스하고 이러한 역할이 허용하는 작업을 수행할 수 있습니다. 예를 들어 읽기 전용 역할 및 상속된 관리자 역할이 할당된 사용자 계정은 관리자 권한을 보유하게 됩니다.

중요
Cyber Protect 웹 콘솔에는 현재 단위에 대해 명시적으로 할당된 역할만 표시됩니다. 상속된 역할과의 불일치 항목은 표시되지 않습니다. 상속된 역할과 관련하여 잠재적으로 발생할 수 있는 문제를 피하기 위해 관리자, 읽기 전용 및 감사인 역할을 별도의 계정 또는 그룹에 할당하는 것이 좋습니다.

기본 관리자

Windows

관리 서버가 머신에 설치되는 동안 다음 작업이 수행됩니다.

- **Acronis Centralized Admins** 사용자 그룹이 머신에서 생성됩니다.
  도메인 컨트롤러에서 이 그룹의 이름은 *DCNAME* **$ Acronis Centralized Admins**입니다. 여기서 *DCNAME*은 도메인 컨트롤러의 NetBIOS 이름을 나타냅니다.
- **Administrators** 그룹의 모든 멤버가 **Acronis Centralized Admins** 그룹에 추가됩니다. 머신이 도메인이지만 도메인 컨트롤러는 아닐 경우 로컬(비도메인) 사용자들은 제외됩니다. 도메인 컨트롤러에 비도메인 사용자는 없습니다.
- **Acronis Centralized Admins** 및 **Administrators** 그룹은 관리 서버에 **조직 관리자**로 추가됩니다. 머신이 도메인이지만 도메인 컨트롤러가 아닐 경우 로컬(비도메인) 사용자들이 조직 관리자가 될 수 없도록 **Administrators** 그룹이 추가되지 않습니다.

조직 관리자 목록에서 **Administrators** 그룹을 삭제할 수 있습니다. 그러나 **Acronis Centralized Admins** 그룹은 삭제할 수 없습니다. 가능성은 거의 없지만 모든 조직 관리자가 삭제된 경우 Windows의 **Acronis Centralized Admins** 그룹에 계정을 추가하고 이 계정으로 Cyber Protect 웹 콘솔에 로그인할 수 있습니다.

Linux

관리 서버가 머신에 설치될 때 **루트** 사용자가 관리 서버에 **조직 관리자**로 추가됩니다.

이후의 설명에 따라 다른 Linux 사용자를 관리 서버 관리자 목록에 추가한 다음, 이 목록에서 **루트** 사용자를 삭제할 수 있습니다. 가능성은 거의 없지만 모든 조직 관리자가 삭제된 경우 `acronis_asm` 서비스를 다시 시작하면 됩니다. 그러면 **루트** 사용자가 조직 관리자로 자동으로 다시 추가됩니다.

여러 단위의 관리자 계정

계정 하나에 많은 단위의 관리자 권한이 부여될 수 있습니다. 이런 계정과 조직 수준 관리자 계정의 경우 Cyber Protect 웹 콘솔에 단위 선택기가 표시됩니다. 이 계정은 단위 선택기를 사용하여 각 단위를 개별적으로 보고 관리할 수 있습니다.

조직의 모든 단위에 대한 권한이 있는 계정에는 조직에 대한 권한이 없습니다. 조직 수준의 관리자 계정은 **Organization** 그룹에 명시적으로 추가해야 합니다.

단위를 머신으로 채우는 방법

관리자가 웹 인터페이스를 통해 머신을 추가하면 관리자가 관리하는 단위에 머신이 추가됩니다. 관리자가 여러 단위를 관리할 경우 단위 선택기에서 선택한 단위에 머신이 추가됩니다. 따라서 관리자는 **추가**를 클릭하기 전에 단위를 선택해야 합니다.

에이전트를 로컬로 설치할 경우 관리자는 자신의 자격 증명을 제공합니다. 관리자가 관리하는 단위에 머신이 추가됩니다. 관리자가 여러 단위를 관리할 경우 인스톨러에서는 머신을 추가할 단위를 선택할지 묻는 프롬프트를 표시합니다.

관리자 계정 추가

참고
Standard 및 Essentials 버전에서는 이 기능을 사용할 수 없습니다.

계정을 추가하는 방법

1. **설정** > **계정**을 클릭합니다.
   소프트웨어에서 관리 서버 관리자 목록 및 단위 트리(있는 경우)를 표시합니다.
2. **조직**을 선택하거나 관리자를 추가할 단위를 선택합니다.
3. **계정 추가**를 클릭합니다.
4. **도메인**에서 추가할 사용자 계정이 포함된 도메인을 선택합니다. 관리 서버가 Active Directory 도메인에 포함되어 있지 않거나 Linux에 설치되어 있는 경우에는 로컬 사용자만 추가할 수 있습니다.
5. 사용자 이름 또는 사용자 그룹 이름을 검색합니다.
6. 사용자 또는 그룹 이름 옆에 있는 "+"를 클릭합니다.
7. 계정의 역할을 선택합니다.
8. 추가할 모든 사용자 또는 그룹에 대해 4~6단계를 반복합니다.
9. 작업을 마치면 **완료**를 클릭합니다.
10. [Linux만 해당] 아래에 설명된 대로 Acronis 모듈용 PAM(Pluggable Authentication Module) 구성에 사용자 이름을 추가합니다.

Acronis용 PAM 구성에 사용자 이름을 추가하려면

이 절차는 Linux 머신 및 Acronis Cyber Protect 일체형 어플라이언스에서 실행 중인 관리 서버에 적용됩니다.

1. 관리 서버를 실행하는 머신에서 루트 사용자로 텍스트 편집기를 사용하여 **/etc/security/acronisagent.conf** 파일을 엽니다.
2. 이 파일에서 한 라인에 한 번씩 관리 서버 관리자로 추가한 사용자 이름을 입력합니다.
3. 파일을 저장 후 닫습니다.

단위 생성

1. **설정** > **계정**을 클릭합니다.
2. 소프트웨어에서 관리 서버 관리자 목록 및 단위 트리(있는 경우)를 표시합니다.
3. **조직**을 선택하거나 새 단위의 부모 단위를 선택합니다.
4. **단위 생성**을 클릭합니다.
5. 새 단위의 이름을 지정하고 **생성**을 클릭합니다.

클라우드 디플로이

사용자 계정 및 조직 단위 관리는 관리 포털에서 수행할 수 있습니다. 관리 포털에 액세스하려면 사이버 보호 서비스에 로그인할 때 **관리 포털**을 클릭하거나 오른쪽 상단의  아이콘을 클릭한 후 **관리 포털**을 클릭하십시오. 관리 권한이 있는 사용자만 이 포털에 액세스할 수 있습니다.

사용자 계정 및 조직 부서 관리에 대한 자세한 내용은 관리 포털 관리자 안내서를 참조하십시오. 이 문서에 액세스하려면 관리 포털의 물음표 아이콘을 클릭하십시오.

이 섹션에는 사이버 보호 서비스 관리와 관련한 추가 정보가 나와 있습니다.

할당량

할당량을 사용하면 사용자가 서비스를 사용할 수 있는 기능을 제한할 수 있습니다. 할당량을 설정하려면 **사용자** 탭에서 사용자를 선택한 다음 **할당량** 섹션의 연필 아이콘을 클릭합니다.

할당량을 초과하면 사용자의 이메일 주소로 알림이 전송됩니다. 할당량 초과분을 설정하지 않는 경우 "소프트" 할당량으로 간주됩니다. 즉, 사이버 보호 서비스 사용에 대한 제한 사항이 적용되지 않습니다.

할당량 초과분을 지정할 수도 있습니다. 초과분은 사용자가 지정된 값까지 할당량을 초과하도록 허용합니다. 초과분까지 초과되면 사이버 보호 서비스 사용에 대한 제한이 적용됩니다.

백업

클라우드 스토리지 할당량, 로컬 백업용 할당량, 사용자가 보호할 수 있는 최대 머신/장치/사서함 수를 지정할 수 있습니다. 다음 할당량을 사용할 수 있습니다.

- **클라우드 스토리지**
- **워크스테이션**
- **서버**
- **Windows Server Essentials**
- **가상 호스트**

- **범용성**
  이 할당량은 위에 나열된 네 가지 할당량을 대신해 사용될 수 있습니다. 워크스테이션, 서버, Windows Server Essentials, 가상 호스트.
- **모바일 장치**
- **Microsoft 365 사서함**
- **로컬 백업**

하나 이상의 보호 계획이 적용된 경우 해당 머신/장치/사서함은 보호된 것으로 간주합니다. 모바일 장치는 첫 번째 백업 후에 보호됩니다.

클라우드 스토리지 할당량 초과분을 초과하면 백업에 실패합니다. 장치 수 초과분을 넘어선 경우 사용자는 더 이상 추가 장치에 대한 보호 계획을 적용할 수 없습니다.

로컬 백업 할당량은 클라우드 인프라를 사용하여 생성된 로컬 백업의 총 크기를 제한합니다. 이 할당량에 대한 초과분을 설정할 수 없습니다.

재해 복구

이 할당량은 서비스 제공업체가 전체 회사에 적용합니다. 회사 관리자는 관리 포털에서 할당량 및 사용량을 볼 수 있지만 사용자에 대한 할당량을 설정할 수는 없습니다.

- **재해 복구 스토리지**
  이 스토리지는 기본 및 복구 서버에서 사용됩니다. 이 할당량 초과분에 도달한 경우 기본 및 복구 서버를 만들거나, 기존 기본 서버에 디스크를 추가/확장할 수 없습니다. 이 할당량 초과분이 초과된 경우 장애 조치를 시작하거나, 중지된 서버를 시작할 수 없습니다. 실행 중인 서버는 계속 실행됩니다.
  할당량이 비활성화된 경우 모든 서버가 삭제됩니다. **클라우드 복구 사이트** 탭이 Cyber Protect 웹 콘솔에서 사라집니다.
- **컴퓨팅 포인트**
  이 할당량은 청구 기간 동안 기본 및 복구 서버에서 사용되는 CPU 및 RAM 리소스를 제한합니다. 이 할당량 초과분에 도달한 경우 모든 기본 서버 및 복구 서버가 중단됩니다. 다음 청구 기간이 시작될 때까지 이러한 서버를 사용할 수 없습니다. 기본 청구 기간은 1개월입니다.
  할당량을 비활성화하면 청구 기간에 관계없이 서버를 사용할 수 없습니다.
- **공용 IP 주소**
  이 할당량은 기본 및 복구 서버에 할당할 수 있는 공용 IP 주소 수를 제한합니다. 이 할당량 초과분에 도달한 경우 더 많은 서버에 대해 공용 IP 주소를 활성화할 수 없습니다. 서버 설정에서 **공용 IP 주소** 확인란의 선택을 취소하여 서버가 공용 IP 주소를 사용하지 못하게 할 수 있습니다. 그런 다음 다른 서버가 공용 IP 주소를 사용할 수 있도록 허용할 수 있습니다. 공용 IP 주소는 일반적으로 같은 주소가 아닙니다.
  할당량을 비활성화하면 모든 서버가 공용 IP 주소 사용을 중지하므로 인터넷에서 연결할 수 없게 됩니다.
- **클라우드 서버**
  이 할당량은 기본 및 복구 서버의 총 수를 제한합니다. 이 할당량 초과분에 도달한 경우, 기본 및 복구 서버를 생성할 수 없습니다.

할당량을 사용하지 않으면 Cyber Protect 웹 콘솔에 서버가 표시되지만 사용 가능한 작업은 **삭제**뿐입니다.

- **인터넷 액세스**

  이 할당량은 기본 및 복구 서버에서 인터넷 액세스를 활성화하거나 비활성화합니다.

  할당량을 비활성화하면 기본 서버와 복구 서버가 즉시 인터넷 연결이 끊어집니다. 서버 속성의 **인터넷 액세스** 스위치가 지워지고 비활성화됩니다.

공지

사용자에 대한 알림 설정을 변경하려면 **사용자** 탭에서 사용자를 선택한 다음 **설정** 섹션의 연필 아이콘을 클릭합니다. 다음 알림 설정을 사용할 수 있습니다.

- **할당량 초과 사용 알림** (기본적으로 활성화됨)

  초과된 할당량에 대한 알림.
- **예약된 사용 보고서**

  아래에 설명하는 대로 매월 첫 째날 전송되는 사용 보고서.
- **실패 알림**, **경고 알림...** 및 **성공 알림** (기본적으로 비활성화됨)

  보호 계획의 실행 결과와 각 장치별 재해 복구 작업 결과에 대한 알림입니다.
- **활성 경보에 대한 일일 확인**(기본적으로 활성화됨)

  이 확인은 실패한 백업, 누락된 백업 및 기타 문제를 알립니다. 확인은 10시(데이터 센터 시간)에 전송됩니다. 그 당시 문제가 없다면 확인이 전송되지 않습니다.

모든 알림은 사용자의 이메일 주소로 전송됩니다.

보고

사이버 보호 서비스 사용 보고서에는 조직 또는 부서에 대한 다음 데이터가 포함됩니다.

- 부서, 사용자 및 장치 유형별 백업 크기.
- 부서, 사용자 및 장치 유형별 보호되는 장치 수.
- 부서, 사용자 및 장치 유형별 가격.
- 백업의 총 크기
- 보호되는 장치의 총 수.
- 총 가격

명령줄 참조

명령줄 참조는 https://www.acronis.com/en-us/support/documentation/AcronisCyberProtect_15_Command_Line_Reference/index.html에서 제공되는 별도의 문서입니다.

문제 해결

이 섹션에서는 에이전트 로그를 .zip 파일로 저장하는 방법을 설명합니다. 불확실한 이유 때문에 백업에 실패한 경우 기술 지원 담당자가 문제를 파악하는 데 이 파일이 도움이 됩니다.

로그를 수집하려면

1. 다음 중 하나를 수행하십시오.
   - **장치**에서 로그를 수집하려는 머신을 선택한 다음 **작업**을 클릭합니다.
   - **설정** > **에이전트**에서 로그를 수집하려는 머신을 선택한 다음 **상세정보**를 클릭합니다.
2. **시스템 정보 수집**을 클릭합니다.
3. 웹 브라우저에서 메시지가 표시되면 파일을 저장할 위치를 지정합니다.

용어 설명

S

Startup Recovery Manager

부트 가능한 에이전트의 수정 내용은 시스템 디스크에 상주하며 부팅 시에 F11을 누를 때 시작되도록 구성할 수 있습니다. Startup Recovery Manager는 부트 가능한 구조 유틸리티를 시작하기 위해 구조 미디어나 네트워크 연결이 필요하지 않습니다. Startup Recovery Manager는 특히 모바일 사용자에게 유용합니다. 장애가 발생하면 사용자는 머신을 재부팅하고, "Press F11 for Startup Recovery Manager..." 프롬프트가 나타나면 F11 키를 누르고 일반적인 부트 가능한 미디어에서와 같은 방법으로 데이터 복구를 수행합니다. 제한 사항: Windows 로더 및 GRUB 이외의 다른 로더를 재활성화해야 합니다.

관

관리되는 위치

스토리지 노드에서 관리되는 백업 위치. 실제로, 관리 위치는 네트워크 공유, SAN, NAS, 스토리지 노드에 로컬인 하드 드라이브 또는 스토리지 노드에 로컬로 연결된 테이프 라이브러리에 상주할 수 있습니다. 스토리지 노드는 관리 위치에 저장된 각 백업에 대해 정리 및 유효성 검사(보호 계획에 포함된 경우)를 수행합니다. 스토리지 노드가 수행할 추가 작업을 지정할 수 있습니다(중복 제거, 암호화).

단

단일 파일 백업 형식

초기 전체 백업 및 이후 증분 백업은 여러 개의 파일이 아니라, 새로운 백업 형식인 단일 .tib 파일에 저장됩니다. 이 형식은 오래된 백업의 삭제가 어렵다는 주요 단점을 피하면서 증분 백업 방식의 빠른 속도를 활용합니다. 이 소프트웨어는 오래된 백업에서 사용하는 블록을 "여유"로 표시하고 이러한 블록에 새 백업을 씁니다. 이를 통해 최소한의 리소스를 사용하여 매우 빠른 정리가 가능합니다. 임의 액세스 읽기 및 쓰기가 지원되지 않는 위치로 백업할 때는 단일 파일 백업 형식을 사용할 수 없습니다(예: SFTP 서버).

백

백업 세트

개별적인 보관 규칙이 적용되는 백업 그룹입니다. 사용자 정의 백업 구성표의 경우 백업 세트는 백업 방식에 해당합니다(전체, 차등, 증분). 이외의 경우 백업 세트는 월간, 일일, 주간, 매시간입니다. 월간 백업은 한 달이 시작된 후 생성된 첫 번째 백업입니다. 주간 백업은 주간 백업 옵션(기어 아이콘을 클릭한 다음 백업 옵션 > 주간 백업 클릭)에서 선택한 주중 특정일에 생성된 첫 번째 백업입니다. 한 달이 시작된 후 생성된 첫 번째 백업이 주간 백업인 경우 해당 백업은 월간인 것으로 간주됩니다. 이 경우 주간 백업은 다음 주 선택한 요일에 생성됩니다. 일일 백업은 해당 백업이 월간 또는 주간 백업의 정의에 포함되지 않는 한 하루가 시작된 후 생성된 첫 번째 백업입니다. 매시간 백업은 해당 백업이 월간, 주간 또는 일일 백업의 정의에 포함되지 않는 1시간이 시작된 후 생성된 첫 번째 백업입니다.

전

전체 백업

업에 선택된 모든 데이터를 포함하는 자급식 백업. 데이터를 전체 백업에서 복구하기 위해서 다른 백업에 액세스할 필요가 없습니다.

증

증분 백업

백업은 가장 최근의 백업 이후 데이터에 대한 변경 내용을 저장합니다. 증분 백업에서 데이터를 복구하려면 다른 백업에 액세스해야 합니다.

차

차등 백업

차등 백업은 최신 전체 백업 이후 데이터 변경 사항을 저장합니다. 차등 백업에서 데이터를 복구하기 위해서는 해당하는 전체 백업에 액세스해야 합니다.

색인

O

P

R

S

T

U

V

W

가

각

도

동

드

등

디

라

레

로

웹

위

유

이

인

일

자

작

장

재

저

전

정

제

주

준

중

지

타

테

통

특

팁

파

패