




Dell DL4300 어플라이언스 배포 안내서



참고, 주의 및 경고

-  **노트:** "주"는 컴퓨터를 보다 효율적으로 사용하는 데 도움을 주는 중요 정보를 제공합니다.
-  **주의:** "주의"는 하드웨어 손상이나 데이터 손실의 가능성을 설명하며, 이러한 문제를 방지할 수 있는 방법을 알려줍니다.
-  **경고:** "경고"는 재산상의 피해나 심각한 부상 또는 사망을 유발할 수 있는 위험이 있음을 알려줍니다.

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

2016 - 05

개정 A02

목차

1 DL4300 어플라이언스 설정	5
소개	5
본 문서에 사용된 용어	5
사용 가능한 구성	5
설치 필수 요소	6
네트워크 요구사항	6
권장되는 네트워크 인프라	6
하드웨어 설정	6
랙에 어플라이언스 설치	7
스토리지 인클로저 구성 스위치 설정	7
DL2xxx 시스템에 스토리지 인클로저 연결	7
케이블 관리대 연결(선택 사항)	9
어플라이언스 케이블 연결	9
기기 켜기	9
DL4300 디스크 구성	9
2 초기 소프트웨어 설치	10
AppAssure 어플라이언스 구성 마법사	10
네트워크 인터페이스 구성	11
호스트 이름 및 도메인 설정 구성	11
SNMP 설정 구성	12
Windows 및 RASR 가상 디스크 생성	13
복구 및 업데이트 유틸리티	13
신속한 어플라이언스 자동 복구	14
RASR USB 키 만들기	14
RASR 실행	15
내장형 듀얼 SD 모듈을 통해 RASR 실행	15
저장소 프로비저닝	16
선택한 저장소 프로비저닝	17
파이버 채널 스토리지를 사용하여 DL4300 구성(선택 사항)	18
3 설치 후 작업	19
Core 콘솔 액세스	19
Internet Explorer에서 신뢰할 수 있는 사이트 업데이트	19
Core 콘솔에 원격으로 액세스하도록 브라우저 구성	19
Internet Explorer 및 Chrome에서 브라우저 설정 구성	20
Mozilla Firefox 브라우저 설정 구성	20
보존 기간 검토	21

에이전트 스냅샷 데이터 암호화.....	21
전자 메일 서버 및 전자 메일 알림 템플릿 구성	21
스트림 수 조정.....	22
컴퓨터 보호 및 클라이언트에 대한 연결 확인.....	23
네트워크 연결 확인.....	23
방화벽 설정 확인.....	23
이름 분석 확인(해당되는 경우).....	24
네트워크 어댑터 타이밍.....	24
Broadcom 고급 구성 제품군 다시 설치	24
NIC 팀 생성.....	25
Hyper-V 가상 스위치 구성.....	25
4 클라이언트에 에이전트 설치.....	26
원격으로 에이전트 설치(푸시).....	26
에이전트를 보호할 때 Agent 소프트웨어 배포.....	27
클라이언트에서 Microsoft Windows 에이전트 설치.....	28
라이센스 포털을 사용하여 에이전트 추가.....	28
Linux 컴퓨터에 에이전트 설치.....	29
Linux 에이전트 파일의 위치.....	29
에이전트 종속성.....	30
Ubuntu에 에이전트 설치.....	31
Red Hat Enterprise Linux 및 CentOS에 에이전트 설치.....	31
SUSE Linux Enterprise Server에 에이전트 설치.....	32
5 도움말 얻기.....	33
설명서 및 소프트웨어 업데이트 찾기.....	33
소프트웨어 업데이트 찾기.....	33
Dell에 문의하기.....	33
설명서에 대한 사용자 의견.....	33

DL4300 어플라이언스 설정

소개

Dell DL4300 어플라이언스는 Dell AppAssure 소프트웨어에 의해 구동되는 디스크 어플라이언스 백업의 최신 세대입니다. 이 어플라이언스를 통해 다음을 사용할 수 있습니다.

- 모든 규모의 조직을 지원하는 확장 가능한 스토리지 기능
- 기존의 테이프 장치 및 백업 방법보다 빠른 백업 및 보다 신속한 복구 시나리오
- 중복 제거 기능(선택 사항)
- 데이터 센터 및 원격 오피스 서버에 대한 연속 데이터 보호
- 중요한 데이터 보호 작업을 시작하는 데 필요한 시간을 줄여주는 빠르고 쉬운 배치 환경
- 옵션으로 제공되는 파이버 채널 구성

본 문서에 사용된 용어

다음 표에 DL4300 어플라이언스의 다양한 하드웨어 및 소프트웨어 구성 요소를 설명하기 위해 본 설명서에 사용된 용어가 나와 있습니다.

표 1. DL4300 어플라이언스 하드웨어 및 소프트웨어 구성 요소

구성 요소	사용된 용어
DL4300 어플라이언스	어플라이언스
Dell Storage MD1400 스토리지 인클로저	스토리지 인클로저
Dell AppAssure 소프트웨어	AppAssure

사용 가능한 구성


DL 어플라이언스는 두 가지 구성으로 제공됩니다: Standard Edition(기본 에디션) 및 High Capacity Edition(고용량 에디션).

표 2. DL4300 Standard Edition 용량 구성

용량	하드웨어 구성
5TB	1TB 드라이브 12개, 1TB 내부 드라이브 4개
10~20TB	2TB 드라이브 12개, 2TB 내부 드라이브 4개
30~40TB	4TB 드라이브 12개, 4TB 내부 드라이브 4개
50~60TB	6TB 드라이브 12개, 6TB 내부 드라이브 4개


표 3. DL4300 High Capacity Edition 용량 구성

용량	하드웨어 구성
40TB, 50TB, 60TB, 70TB, 80TB, 90TB, 100TB, 110TB 및 120TB	6TB 드라이브 12개, 6TB 내부 드라이브 4개

 **노트:** 확장 선반을 통해 추가 스토리지를 추가할 수 있습니다(Dell Storage MD1400). 모든 모델에 추가 스토리지를 추가할 수 있지만, Standard Edition의 경우 최대 40TB 및 High Capacity Edition의 경우 최대 120TB를 추가할 수 있습니다. 두 버전 모두 확장 선반을 최대 4개까지 지원합니다.

또한 각 구성에 다음 하드웨어와 소프트웨어가 포함되어 있습니다.

- Dell DL4300 시스템
- Dell PowerEdge RAID 컨트롤러(PERC)
- 사전 설치된 운영 체제와 Dell OpenManage 시스템 및 스토리지 관리 소프트웨어
- AppAssure 소프트웨어

 **노트:** 어플라이언스 구성에 Dell Storage MD1400 스토리지 인클로저가 포함되어 있지 않은 경우에는 본 설명서에서 Dell Storage MD1400 및 스토리지 인클로저에 대한 참조를 무시하십시오.

설치 필수 요소

네트워크 요구사항

어플라이언스에 필요한 네트워크 환경은 다음과 같습니다.


- 사용 가능한 이더넷 케이블과 연결이 구성된 활성 네트워크
- 정적 IP 주소 및 DNS 서버 IP 주소(동적 호스트 구성 프로토콜 (DHCP)에서 제공하지 않는 경우)
- 관리자 권한이 있는 사용자 이름과 암호

권장되는 네트워크 인프라

Dell은 조직에서 AppAssure에 사용할 경우 효율적인 성능을 제공하는 1 GbE 백본을 사용하고 환경을 크게 강화하려면 10 GbE 네트워크를 사용할 것을 권장합니다.

하드웨어 설정

어플라이언스는 단일 DL4300 시스템과 함께 제공됩니다. 어플라이언스 하드웨어를 설정하기 전에 어플라이언스와 함께 제공된 *Dell DL4300 어플라이언스와 시스템 시작하기* 설명서를 참조하십시오. DL 어플라이언스 하드웨어의 포장을 풀고 설치합니다.

 **노트:** 소프트웨어는 어플라이언스에 미리 설치되어 있습니다. 시스템과 함께 포함된 모든 매체는 시스템 복구가 필요할 경우에만 사용해야 합니다.

DL 어플라이언스 하드웨어를 설치하려면 다음을 수행하십시오:

1. DL4300 시스템과 스토리지 인클로저를 랙에 설치하고 케이블로 연결합니다.
2. 스토리지 인클로저를 켜 다음 DL4300 시스템의 전원을 켭니다.

랙에 어플라이언스 설치

시스템에 레일 키트가 포함되어 있는 경우 랙 키트와 함께 제공되는 **랙 설치 지침**을 찾으십시오. 지침에 따라 랙 장치의 레일, 시스템 및 랙의 스토리지 인클로저를 설치하십시오.

스토리지 인클로저 구성 스위치 설정

다음 그림에 나온 대로 스토리지 인클로저에 대해 스토리지 모드를 통합 모드로 설정합니다.

노트: 스토리지 인클로저를 켜기 전에 먼저 구성 스위치를 설정해야 합니다. 스토리지 인클로저를 켜 후에 구성 모드를 변경하면 시스템의 전원을 껐다 켜야 인클로저 구성에 변경 내용이 적용됩니다. 자세한 내용은 Dell.com/support/home에서 *Dell Storage MD1400 인클로저 하드웨어 소유자 매뉴얼*을 참조하십시오.

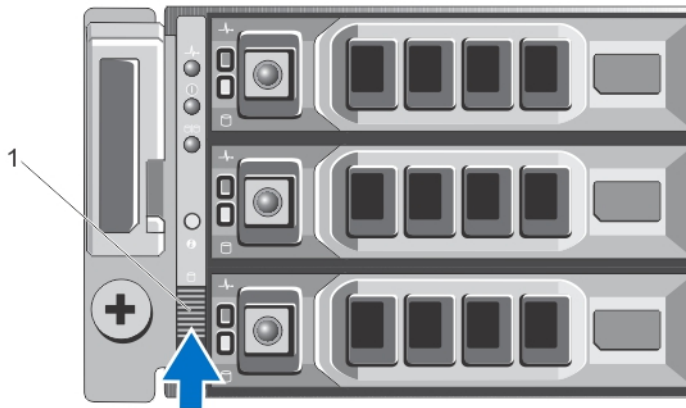


그림 1. PowerVault MD1400 스토리지 인클로저 구성 스위치 설정

1. 구성 스위치

DL2xxx 시스템에 스토리지 인클로저 연결

Dell DL4300 시스템에 설치된 PowerEdge RAID Controller(PERC)의 데이터 케이블을 스토리지 인클로저의 기본 인클로저 관리 모듈(EMM) SAS 포트에 연결합니다.

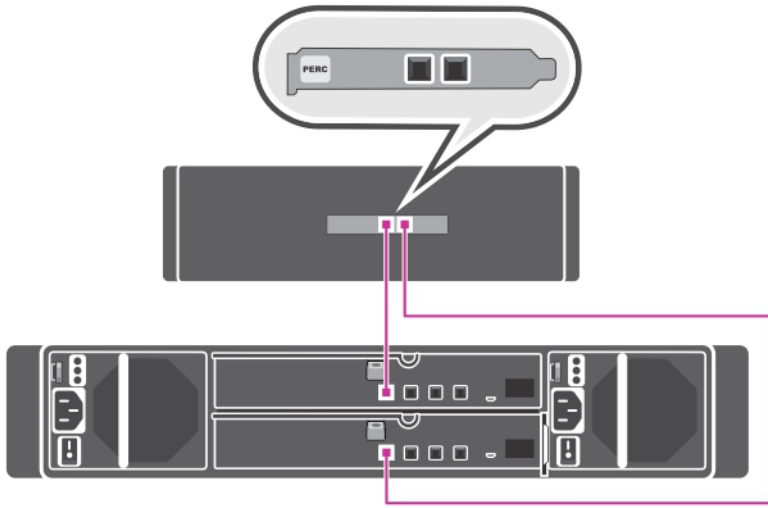


그림 2 . DL4300 시스템을 MD1400 스토리지 인클로저에 연결

중복 포트 구성

중복 포트 구성의 경우 다음을 수행하십시오.

1. 각 SAS 케이블의 한쪽 끝을 DL4300 시스템 PERC 컨트롤러의 포트 0과 포트 1에 연결합니다.
2. 각 SAS 케이블의 다른 쪽 끝을 MD1400 스토리지 인클로저에 있는 각 인클로저 관리 모듈(EMM)의 포트 1에 연결합니다.

단일 포트 구성

단일 포트 구성의 경우 다음을 수행하십시오.

1. 각 SAS 케이블의 한쪽 끝을 DL4300 시스템 PERC 컨트롤러의 포트 0에 연결합니다.
2. SAS 케이블의 다른 쪽 끝을 MD1400 스토리지 인클로저에 있는 인클로저 관리 모듈(EMM)의 포트 1에 연결합니다.

다중 체인 구성

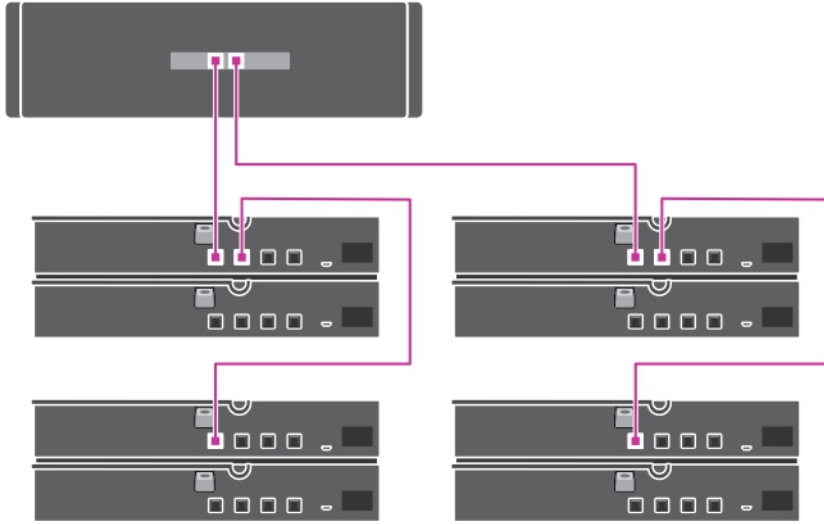


그림 3. 다중 체인 구성

다중 체인 구성에서는 인클로저를 최대 4개까지 지원합니다. 처음 두 개의 인클로저는 컨트롤러 카드의 단일 포트에 인클로저 중 하나가 연결되는 데이지 체인 방식으로 연결되고, 나머지 두 개의 인클로저는 컨트롤러 카드의 두 번째 포트에 인클로저 중 하나가 연결되는 데이지 체인 방식으로 연결됩니다.

케이블 관리대 연결(선택 사항)


어플라이언스에 케이블 관리대(CMA)가 포함된 경우, CMA 키트와 함께 제공되는 CMA 설치 설명서를 찾아 CMA 설치에 대한 지침을 따르십시오.

어플라이언스 케이블 연결

Dell.com/support/home에서 어플라이언스와 함께 제공된 *시스템 시작하기* 설명서를 찾아 키보드, 마우스, 모니터, 전원 및 네트워크 케이블을 어플라이언스에 연결하는 지침을 따릅니다.

기기 켜기

어플라이언스를 케이블로 연결한 후에 MD1400 스토리지 인클로저를 켜고 DL4300 시스템의 전원을 켭니다.

 **노트:** 신뢰성 및 가용성 극대화를 위해 무정전 전원 공급 장치(UPS)에 어플라이언스를 연결할 것을 권장합니다.


DL4300 디스크 구성

DL4300은 니어라인 SAS 드라이브와 SATA 드라이브 모두를 지원합니다. 운영 체제는 슬롯 12와 13에 있는 RAID 1 미러 가상 디스크에 있습니다. 이러한 디스크에 대한 자세한 내용은 Dell.com/support/home에서 *Dell DL4300 어플라이언스 소유자 매뉴얼*을 참조하십시오. 슬롯 0-11 및 14-17에서 사용 가능한 드라이브를 AppAssure 어플라이언스 구성 마법사(권장)를 통해 자동으로 구성할 수 있지만, 필요한 경우 사용자 지정 구성에 맞게 수동으로 구성할 수 있습니다. 디스크는 RAID 6으로 자동으로 프로비저닝되고, MD1400 스토리지 인클로저를 이용한 용량 확장은 선택사항입니다.

초기 소프트웨어 설치


처음 어플라이언스를 켜고 시스템 암호를 변경하면 **AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)**가 자동으로 실행됩니다.

1. 시스템을 켜 후, Windows 언어 옵션에서 운영 체제 언어를 선택합니다.
Microsoft EULA(최종 사용자 라이선스 계약서)가 **Settings(설정)** 페이지에 표시됩니다.
2. EULA를 수락하려면 **I accept(동의함)** 단추를 클릭합니다.
관리자 암호를 변경할 수 있는 페이지가 표시됩니다.
3. 관리자 암호를 변경할 것인지 묻는 메시지가 나타나면 **OK(확인)**를 클릭합니다.
4. 새 암호를 입력하고 확인합니다.
암호가 변경되었음을 확인하는 메시지가 나타납니다.
5. **OK(확인)**를 클릭합니다.
6. **Dell readme.htm** 화면에서 아래로 스크롤하고 **Proceed(진행)**를 클릭합니다.
7. 변경된 관리자 암호를 사용하여 로그인합니다.
Select the language for AppAssure Appliance(AppAssure 어플라이언스 언어 선택) 화면이 표시됩니다.
8. 지원되는 언어 목록에서 어플라이언스에 대한 언어를 선택합니다.
AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사) 시작 화면이 표시됩니다.

 **노트:** **AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)**가 시스템 콘솔에 표시되는 데 최대 30초 정도 걸릴 수 있습니다.

 **노트:** 모든 작업이 완료될 때까지 **AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)**를 닫지 마십시오.

AppAssure 어플라이언스 구성 마법사

 **주의:** 어플라이언스의 설정을 변경하거나 다른 작업을 수행하기 전에 **AppAssure** 어플라이언스 구성 마법사의 모든 단계를 완료했는지 확인하십시오. 마법사가 완료될 때까지 제어판을 통해 변경하거나, **Microsoft Windows Update**를 사용하거나, **AppAssure** 소프트웨어를 업데이트하거나, 라이선스를 설치하지 마십시오.


AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)는 어플라이언스에 소프트웨어를 구성하는 단계를 안내합니다.

- [네트워크 인터페이스 구성](#)
- [호스트 이름 및 도메인 설정 구성](#)
- [SNMP 설정 구성](#)
- [Windows 및 RASR 가상 디스크 생성](#)

마법사를 사용하여 설치를 완료하면 Core 콘솔이 자동으로 시작됩니다.

네트워크 인터페이스 구성

사용 가능한 네트워크 인터페이스를 구성하려면 다음 단계를 따르십시오.

1. **AppAssure Appliance Configuration Wizard Welcome(AppAssure 어플라이언스 구성 마법사 시작)** 화면에서 **Next(다음)**를 클릭합니다.
network interfaces(네트워크 인터페이스) 페이지에 사용 가능한 연결된 네트워크 인터페이스가 표시됩니다.
2. 구성하려는 네트워크 인터페이스를 선택합니다.
 **노트: AppAssure Appliance Configuration(AppAssure 어플라이언스 구성) 마법사가 네트워크 인터페이스를 개별 포트(티밍되지 않음)로 구성합니다. 통합 성능을 높이려면 NIC를 티밍하여 더 큰 통합 채널을 생성하면 됩니다. 그러나 이 작업은 어플라이언스의 초기 구성 후에 수행해야 합니다.**
3. 필요한 경우 추가 네트워크 인터페이스를 연결하고 **Refresh(새로 고침)**를 클릭합니다.
추가로 연결된 네트워크 인터페이스가 표시됩니다.
4. **Next(다음)**를 클릭합니다.
Configure selected network interface(선택한 네트워크 인터페이스 구성) 페이지가 표시됩니다.
5. 선택한 인터페이스에 적절한 인터넷 프로토콜을 선택합니다.
IPv4 또는 **IPv6**을 선택할 수 있습니다.


네트워크 세부 정보는 선택한 인터넷 프로토콜에 따라 다르게 표시됩니다.

6. 인터넷 프로토콜 세부 정보를 지정하려면 다음 중 하나를 수행합니다.
 - 선택한 인터넷 프로토콜 세부 정보를 자동으로 지정하려면 **Obtain an IPV4 address automatically(자동으로 IPV4 주소 얻기)**를 선택합니다.
 - 네트워크 연결을 수동으로 지정하려면 **Use the following IPv4 address(다음 IPV4 주소 사용)**를 선택하고 다음 세부 정보를 입력합니다.
 - **IPv4 주소 또는 IPv6 주소**
 - **IPV4의 서브넷 마스크 및 IPV6의 서브넷 접두사 길이**
 - **기본 게이트웨이**
7. DNS 서버 세부 정보를 지정하려면 다음 중 하나를 수행합니다.
 - DNS 서버 주소를 자동으로 지정하려면 **Obtain DNS server address automatically(자동으로 DNS 서버 주소 얻기)**를 선택합니다.
 - DNS 서버를 수동으로 지정하려면 **Use the following DNS server address(다음 DNS 서버 주소 사용)**를 선택하고 다음 세부 정보를 입력합니다.
 - **선호하는 DNS 서버**
 - **대체 DNS 서버**
8. **Next(다음)**를 클릭합니다.
Configure hostname and domain setting(호스트 이름 및 도메인 설정 구성) 페이지가 표시됩니다.

NIC 티밍에 대한 자세한 내용은 [네트워크 어댑터 티밍](#)을 참조하십시오.


호스트 이름 및 도메인 설정 구성

어플라이언스의 호스트 이름을 지정해야 합니다. 백업을 시작하기 전에 호스트 이름을 변경하는 것이 좋습니다. 기본적으로 호스트 이름은 운영 체제에서 지정하는 시스템 이름입니다.


-  **노트:** 호스트 이름을 변경하려는 경우 이 단계에서 호스트 이름을 변경하는 것이 좋습니다. **AppAssure Appliance Configuration wizard(어플라이언스 구성 마법사)**를 완료한 후에 호스트 이름을 변경하려면 몇 가지 단계를 수동으로 수행해야 합니다.

호스트 이름과 도메인 설정을 구성하려면 다음을 수행하십시오.

1. **Configure host name and domain setting(호스트 이름 및 도메인 설정 구성)** 페이지에서 어플라이언스의 호스트 이름을 변경하려면 **New host name(새 호스트 이름)**에 올바른 호스트 이름을 입력합니다.
2. 어플라이언스를 도메인에 연결하지 않으려면 **Do you want this appliance to join a domain?(이 어플라이언스를 도메인에 연결하시겠습니까?)**에서 **No(아니요)**를 선택합니다.
기본적으로 **Yes(예)**가 선택되어 있습니다.
3. 도메인에 어플라이언스를 연결하려면 다음 세부 정보를 입력합니다.
 - 도메인 이름
 - 도메인 사용자 이름
4. **Next(다음)**를 클릭합니다.

 **노트:** 도메인 사용자에게 로컬 관리 권한이 있어야 합니다.

- 도메인 사용자 암호


 **노트:** 호스트 이름이나 도메인을 변경하려면 컴퓨터를 다시 시작해야 합니다. 다시 시작한 후에 **AppAssure Appliance Configuration wizard(AppAssure 어플라이언스 구성 마법사)**가 자동으로 시작됩니다. 어플라이언스가 도메인에 연결되면 컴퓨터를 다시 시작한 후에 어플라이언스에 대한 관리 권한을 사용하여 도메인 사용자로 로그인해야 합니다.

Configure SNMP Settings(SNMP 설정 구성) 페이지가 표시됩니다.

SNMP 설정 구성

SNMP(Simple Network Management Protocol)는 장치 검색, 모니터링 및 이벤트 생성과 같은 SNMP 호환 관리 기능을 허용하는 일반적으로 사용되는 네트워크 관리 프로토콜입니다. SNMP는 TCP/IP 프로토콜의 네트워크 관리를 제공합니다.

어플라이언스에 대해 SNMP 경고를 구성하려면 다음 단계를 따르십시오.

1. **Configure SNMP Settings(SNMP 설정 구성)** 페이지에서 **Configure SNMP on this appliance(이 어플라이언스에서 SNMP 구성)**를 선택합니다.
 -  **노트:** 어플라이언스에서 SNMP 세부 정보와 경고를 설정하지 않고 6단계로 건너뛰려면 **Configure SNMP on this appliance(이 어플라이언스에서 SNMP 구성)**를 선택 취소합니다.
2. **Communities(커뮤니티)**에 하나 이상의 SNMP 커뮤니티 이름을 입력합니다.
섬표를 사용하여 여러 개의 커뮤니티 이름을 구분합니다.
3. **Accept SNMP packets from these hosts(이 호스트에서 SNMP 패킷 수락)**에 어플라이언스가 통신할 수 있는 호스트의 이름을 입력합니다.
호스트 이름을 섬표로 구분하거나 모든 호스트와 통신을 허용하려면 이 칸을 비워 둡니다.
4. SNMP 경고를 구성하려면 **Community Name(커뮤니티 이름)**을 입력하고 SNMP 경고의 **Trap destinations(트랩 대상)**를 입력한 다음 **Add(추가)**를 클릭합니다.
더 많은 SNMP 주소를 추가하려면 이 단계를 반복합니다.
5. 구성된 SNMP 주소를 제거하려면 **Configured SNMP addresses(구성된 SNMP 주소)**에서 해당 SNMP 주소를 선택하고 **Remove(제거)**를 클릭합니다.
6. **Next(다음)**를 클릭합니다.

Create Windows 및 RASR virtual disk(s) 페이지가 표시됩니다.


Windows 및 RASR 가상 디스크 생성

DL4300 시스템에서 다음을 지원합니다.

- 운영 체제 드라이브 2개, 데이터 드라이브 12개 및 내장형 하드 드라이브 4개
- BMR(Bare Metal Restore) 정보 저장을 위해 LUNs(Logical Unit Numbers)를 생성하는 옵션
- Windows 백업 RASR 파일을 위해 별도의 공간을 생성하는 옵션.

옵션으로 제공되는 가상 디스크를 생성하려면 다음을 수행합니다.

1. 다음 가상 디스크를 선택합니다.
 - a. Windows 백업 가상 디스크

 **주의: AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)에서 이 옵션을 선택한 경우 Windows Server 백업을 생성하고 백업 정책을 구성할 수 없습니다.**

Windows 백업 가상 디스크는 Windows Server 백업을 생성할 수 있는 대상 공간을 제공합니다. 생성된 Windows 백업 VD에 대해 디스크 용량 75GB가 기본값으로 할당되고 Windows 백업 VD의 크기를 늘릴 수 없습니다. 시간이 지나면 백업된 데이터가 75GB를 초과할 수 있고, 초과한 경우, 백업을 수행하거나 백업 페이지에서 백업 정책을 구성할 수 없고 용량 초과 오류가 표시됩니다. 이 경우, Windows 백업이 네트워크 공유나 DI 어플라이언스의 다른 디스크 볼륨에 재구성될 수 있습니다. 더 자세한 정보는 Dell.com/supportmanuals의 빠른 어플라이언스 자가 복구(RASR)를 사용해 Dell™ DL 백업 및 복구 어플라이언스 복구에서 예정된 공유 네트워크 드라이브 백업 정책 섹션을 참조하십시오.

- b. 부팅 가능한 RASR 가상 디스크

부팅 가능한 RASR 가상 디스크는 RASR 복구를 수행할 수 있도록 중복 복구 볼륨을 제공합니다. POST를 수행하는 동안 <F8> 키를 눌러 중복 복구 볼륨으로 다시 부팅할 수 있습니다. 다시 부팅한 후 [RASR USB 키를 통해 RASR 실행](#)의 단계를 수행하십시오.

2. **Next(다음)**를 클릭합니다.
시스템이 구성되는 동안 감사 화면이 표시됩니다. 구성 완료 메시지가 표시됩니다.
3. **Exit(종료)**를 클릭합니다.
Core 콘솔이 자동으로 시작됩니다.
4. [저장소 프로비저닝](#)을 통해 구성 프로세스를 계속 진행합니다.


복구 및 업데이트 유틸리티


복구 및 업데이트 유틸리티(RUU)는 DL1000, DL1300, DL4000 및 DL4300 등 DL 어플라이언스를 복구 및 업데이트하기 위한 올인원 설치 프로그램 소프트웨어입니다. 여기에는 AppAssure Core 소프트웨어 및 어플라이언스별 구성 요소가 포함되어 있습니다.


RUU는 Windows Server 역할 및 기능, ASP .NET MVC3, LSI Provider, DL 응용프로그램, OpenManage Server Administrator 및 AppAssure Core 소프트웨어의 업데이트된 버전으로 구성되어 있습니다. 추가적으로, 복구 및 업데이트 유틸리티는 빠른 어플라이언스 자가 복구(RASR) 콘텐츠 또한 업데이트합니다.

최신 버전의 RUU를 다운로드하려면 다음을 수행하십시오.

1. 다운로드 섹션 아래의 라이선스 포털로 이동해 RUU 설치 프로그램을 다운로드하거나 support.dell.com으로 이동합니다.
2. RUU 설치 프로그램을 실행합니다.

 **노트:** RUU 업데이트 프로세스 중 시스템이 재부팅될 수 있습니다.

 **노트:** RUU #184를 사용하고 DL 어플라이언스가 5.4.3.106 이전 버전의 AppAssure Core 버전을 사용하는 경우, 코어가 AppAssure Core 5.4.3.106으로 업그레이드됩니다.

 **노트:** RUU #184로 업그레이드하는 경우, RASR을 통해 이미 예약된 Windows 백업의 향후 실행에서 일부 불일치를 보거나 Windows 백업 정책을 생성하지 못할 수 있습니다. 이러한 불일치는 Windows 백업 스토리지 위치의 공간 제한으로 인해 나타납니다.

이러한 오류의 다른 잠재적인 원인은 다음과 같습니다.

1. 빠른 복구로 업그레이드, 특히 최소 중복 제거 캐시보다 많은 경우.
2. Outlook 등 어플라이언스의 모든 소프트웨어를 설치하거나 업데이트하는 경우.
3. Windows 업데이트를 설치하는 경우.
4. 중복 제거 캐시 등 데이터 파일을 추가하거나 확장하는 경우.
5. 앞 사항의 조합.

신속한 어플라이언스 자동 복구


신속한 어플라이언스 자동 복구(RASR)는 운영 체제 드라이브와 데이터 드라이브를 사용하여 출하 시 설정을 복원하는

- 출하 시 설정 복원
- 어플라이언스를 장애 발생 직전의 상태로 복구

RASR USB 키 만들기

RASR USB 키를 만들려면 다음을 수행합니다.

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

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

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


Prerequisite Check(필수 요소 확인) 메시지가 표시됩니다.

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

4. 대상을 선택하고 **Create(생성)**를 클릭합니다.
경고 대화상자가 표시됩니다.

5. **Yes(예)**를 클릭합니다.

RASR USB 드라이브 키가 생성됩니다.

6.  **노트:** USB 키를 분리할 때에는 그에 앞서 Windows 꺼내기 드라이브 기능을 사용합니다. 그렇지 않으면 USB 키의 콘텐츠가 손상되어 USB 키가 예상대로 작동되지 않을 수 있습니다.

나중에 사용할 수 있도록 키를 분리하고 레이블을 부착하여 보관해 둡니다.


RASR 실행

 **노트:** Dell은 어플라이언스를 설정한 후 RASR USB 키를 생성할 것을 권장합니다. RASR USB 키를 생성하려면 [RASR USB 키 생성](#)을 참조하십시오.

이러한 단계들은 공장 기본 재설정을 수행하는 데 도움을 줍니다.

장애가 발생하기 전의 상태로 어플라이언스를 복구하고 리포지토리, 복구 지점 및 제반 설정을 복구하려면 [Dell.com/support/home](#)에서 **신속한 어플라이언스 자동 복구(RASR)**를 이용해 **Dell™ DL 백업 및 복구 어플라이언스**를 복구 설명서를 참조하십시오.

다음과 같이 RASR을 수행합니다.


1. 생성된 RASR USB 키를 삽입합니다.
2. 어플라이언스를 다시 시작해 **Boot Manager(부팅 관리자)(F11)**를 선택합니다.
3. **Boot Manager(부팅 관리자)** 주 메뉴에서 **One-shot BIOS Boot(단일 BIOS 부팅)** 메뉴를 선택합니다.
4. **Boot Manager Boot(부팅 관리자 부팅)** 메뉴에서 연결된 USB 드라이브를 선택합니다.
5. 키보드 레이아웃을 선택합니다.
6. **Troubleshoot(문제해결) → Rapid Appliance Self Recovery(신속한 어플라이언스 자동 복구)**를 클릭합니다.
7. 대상 운영 체제(OS)를 선택합니다.
RASR가 시작되며 시작 화면이 표시됩니다.
8. **Next(다음)**를 클릭합니다.
Prerequisites(전제조건) 확인 화면이 표시됩니다.
 **노트:** RASR을 수행하기 전 모든 하드웨어 및 기타 전제조건이 체크되도록 확인합니다.
9. **Next(다음)**를 클릭합니다.
세 가지 옵션과 함께 **Recovery Mode Selection(복구 모드 선택)** 화면이 표시됩니다.
 - 시스템 복구
 - Windows 복구 마법사
 - 공장 기본 재설정
10. **Factory Reset(공장 기본 재설정)** 옵션을 선택합니다.
이 옵션을 사용하면 공장 기본 이미지에서 운영 체제 디스크가 복구됩니다.
11. **Next(다음)**를 클릭합니다.
다음과 같은 경고 메시지가 대화 상자에 표시됩니다. This operation will recover the operating system. All OS disk data will be overwritten. (이 작업을 수행하면 운영 체제가 복구됩니다. 모든 OS 디스크 데이터를 덮어씁니다.)
12. **Yes(예)**를 클릭합니다.
운영 체제 디스크가 공장 기본 재설정으로 다시 복원되기 시작합니다.
13. 공장 기본 재설정 복구 프로세스가 완료되면 **RASR Completed(RASR 완료)** 화면에서 **Finish(마침)**를 클릭합니다.

내장형 듀얼 SD 모듈을 통해 RASR 실행

시스템에 내장형 듀얼 SD 모듈 및 용량이 16GB인 SD 카드가 함께 제공됩니다.

내장형 듀얼 SD 모듈(IDSDM)을 사용하여 RASR을 실행하려면 다음을 수행하십시오.

1. IDSDM을 통해 어플라이언스를 다시 부팅합니다.

 **주의: SD 카드가 슬롯 1에 삽입되어 있는지 확인하십시오.**

다음과 같은 메시지가 표시됩니다.

```
The secondary SD card is missing, not responding, or in write-protected mode. Do one of the following: 1) Install a SD card media in the secondary SD card reader. 2) Reseat or replace the SD card media.3) If write-protected mode is expected, then no respose action is required.
```


위의 메시지를 무시하십시오.

2. 계속해서 내장형 듀얼 SD 모듈을 통해 RASR을 실행하려면 [RASR USB 키를 통해 RASR 실행](#) 섹션의 5단계부터 13단계까지 수행합니다.


저장소 프로비저닝

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

- AppAssure 리포지토리

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

- 보호된 컴퓨터의 가상 대기(standby)

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

 **노트:** DL4300 고용량 구성에서는 H830 PERC SAS 어댑터 또는 파이버 채널 HBA가 2개 지원됩니다. 파이버 채널 HBA 구성에 대한 자세한 내용은 Dell.com/support/home에 있는 *DL4xxx - 파이버 채널 구현* 백서를 참조하십시오.

디스크에서 스토리지의 프로비저닝을 시작하기 전에 대기 가상 시스템에 할당할 저장소의 양을 파악해야 합니다. AppAssure 리포지토리를 생성한 뒤 대기 가상 컴퓨터에 사용 가능한 용량의 백분율을 할당할 수 있습니다. 예를 들어, SRM(Storage Resource Management)을 사용하는 경우, AppAssure 리포지토리를 생성한 뒤 가상 컴퓨터를 호스트하기 위해 프로비저닝되는 모든 장치에 최대 100%의 용량을 할당할 수 있습니다. 사용 가능한 공간은 가상 컴퓨터를 호스트하기 위해 프로비저닝된 대기 VM에만 할당될 수 있습니다. AppAssure의 라이브 복구 기능을 사용하면 이러한 가상 컴퓨터를 통해 어플라이언스에서 차단하는 실패한 서버를 모두 신속하게 교체할 수 있습니다.


대기 가상 시스템이 필요하지 않은 중간 규모의 환경에서는, 모든 저장소를 사용하여 상당한 개수의 에이전트를 백업할 수 있습니다. 하지만 대기 가상 시스템에 더 많은 리소스가 필요하고 더 적은 수의 에이전트 시스템을 백업해야 하는 경우에는 규모가 더 큰 VM을 위해 리소스를 추가할 수 있습니다.


Appliance(어플라이언스) 탭을 선택하면 AppAssure Appliance 소프트웨어는 시스템에서 지원되는 모든 컨트롤러에 사용할 수 있는 저장소 공간을 찾고 하드웨어가 요구사항을 충족하는지 유효성을 검사합니다.

사용 가능한 모든 저장소의 디스크 프로비저닝을 완료하려면 다음을 수행합니다.

1. **Appliance(어플라이언스)** 탭에서 **Tasks(작업)** → **Provisioning(프로비저닝)**을 클릭합니다.

Provisioning(프로비저닝) 화면에 프로비저닝을 위한 예상 용량이 표시됩니다. 이 용량은 새 AppAssure 리포지토리를 생성하는 데 사용됩니다.

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

2.  **노트:** 어플라이언스에 초기 리포지토리를 생성하기 위한 내부 RAID 컨트롤러를 프로비저닝합니다.

프로비저닝할 저장소 옆의 Action(작업) 열에서 **Provision(프로비저닝)**을 클릭하여 **Provisioning Storage(저장소 프로비저닝)** 창을 엽니다.

3. **Optional Storage Reserve(선택적 저장소 예약)** 섹션에서, **Allocate a portion of the storage being provisioned for Standby Virtual Machines or other purposes(프로비저닝되는 저장소 일부를 대기 가상 머신 또는 기타 용도로 할당)** 확인란을 선택하고 할당할 저장소 비율을 표시합니다. 그렇지 않으면 **Optional Storage Reserve(선택적 저장소 예약)** 섹션에 표시되는 저장소 비율은 연결된 모든 디스크에서 할당됩니다.

4. **Provision(프로비전)**을 클릭합니다.




리포지토리와 가상 대기 VM을 호스팅할 가상 디스크가 생성됩니다.

선택한 저장소 프로비저닝

선택한 저장소를 프로비저닝하려면 다음을 수행합니다.


1. **Appliance(어플라이언스)** 탭에서 **Tasks(작업)**를 클릭합니다.

Tasks(작업) 화면에 어플라이언스에 사용 가능한 내부 및 외부 저장소 용량과, 프로비저닝에 사용 가능 여부, 이미 프로비저닝되었는지 여부 또는 저장소가 자동으로 프로비저닝될 수 없는 조건이 있는지 여부가 표시됩니다. 이 용량은 AppAssure 리포지토리를 만드는 데 사용됩니다.

2.  **노트:** 외부 인클로저로의 확장을 하기 전에 사용 가능한 내장형 스토리지를 프로비저닝할 것을 권장합니다(MD1400).

사용 가능한 공간 부분만 프로비저닝하려면 프로비저닝할 저장소 공간 옆의 **Action(작업)** 아래에서 **Provision(프로비전)**을 클릭합니다.

- 새 리포지토리를 만들려면 **Create a new repository(새 리포지토리 생성)**를 선택하고 리포지토리의 이름을 제공합니다.
기본적으로 리포지토리 이름은 Repository 1로 표시됩니다. 이 이름을 덮어쓰도록 선택할 수 있습니다.
- 기존 리포지토리에 용량을 추가하려면 **Expand the existing repository(기존 리포지토리 확장)**를 선택하고 **Existing Repositories(기존 리포지토리)** 목록에서 리포지토리를 선택합니다.



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

3. **Optional Storage Reserve(선택적 저장소 예약)**에서, 대기 가상 시스템에 사용할 저장소 부분을 할당하고 VM에 할당할 저장소 비율을 지정할 수 있습니다.

4. 기본적으로 선택되어 있는 **Do this for only one provisioning task when more than one task is being provisioned at a time**(한 번에 둘 이상의 작업을 프로비저닝할 때 하나의 프로비저닝에만 이 작업 수행) 확인란을 선택 취소할 수 있습니다.
이 옵션을 선택 취소하면 선택한 저장소 비율이 선택한 저장소 장치에만 적용됩니다. 이 옵션을 선택하면 선택한 저장소 비율을 내부 저장소 및 외부 인클로저 둘 다에 적용할 수 있습니다.
5. **Provision(프로비전)**을 클릭합니다.
디스크 프로비저닝이 시작되고 **Tasks(작업)** 화면의 **Status(상태)** 영역에 AppAssure 리포지토리 생성 상태가 표시됩니다. **Status Description(상태 설명)**에 **Provisioned(프로비저닝됨)**로 표시됩니다.
6. 디스크 프로비저닝이 완료된 후 상세정보를 보려면 상태 표시등 옆에 >를 클릭합니다.
Tasks(작업) 페이지가 펼쳐지고 상태, 리포지토리 및 가상 디스크 상세정보(할당된 경우)가 표시됩니다.

파이버 채널 스토리지를 사용하여 DL4300 구성(선택 사항)

DL4300 대용량 버전은 파이버 채널 스토리지 어레이를 사용하여 리포지토리를 생성할 수 있는 파이버 채널 HBA 스토리지 옵션을 제공합니다.


-  **노트:** 파이버 채널 구성이 지시된 경우 슬롯이 있는 H830 PERC SAS 어댑터가 대체됩니다.
-  **노트:** 다음 단계에 대한 전제조건, 가정 및 상세정보를 보려면 dell.com/support/home에 있는 *DL4xxx - 파이버 채널 구현* 백서를 참조하십시오.

파이버 채널 스토리지를 사용하여 DL4300을 통합하고 구성하려면 다음을 수행하십시오.

1. DL4300 파이버 채널 HBA를 SAN 스위치에 연결합니다.
2. 시스템과 함께 임의로 주문된 어댑터에 Qlogic 또는 Emulex HBA 관리 소프트웨어를 설치합니다.
3. 저장소 어레이 다중 경로 소프트웨어를 설치합니다.
4. 파이버 채널 조닝(Zoning)을 수행합니다.
5. DL4300 리포지토리로 할당하고 사용할 파이버 채널 LUN을 생성합니다.
6. 파이버 채널 저장소 LUN을 마운트합니다.
7. DL4300 파이버 채널 스토리지를 백업 리포지토리로 구성합니다.

설치 후 작업

AppAssure Appliance Configuration Wizard(AppAssure 어플라이언스 구성 마법사)를 완료한 후 다음 절차에 따라 백업 어플라이언스 및 어플라이언스가 백업 중인 서버가 올바르게 구성되어 있는지 확인합니다.

 **노트:** 어플라이언스는 30일 동안 사용 가능한 임시 AppAssure 소프트웨어 라이선스로 구성됩니다. 영구 라이선스 키를 받으려면 www.dell.com/DLActivation에서 Dell AppAssure 라이선스 포털에 로그인합니다. AppAssure 소프트웨어에서 라이선스 키 변경에 대한 자세한 내용은 dell.com/support/home에서 *Dell DL4300 어플라이언스 사용 설명서*의 '라이선스 키 변경' 항목을 참조하십시오.

Core 콘솔 액세스

주제에서 설명된 대로 신뢰할 수 있는 사이트를 업데이트하고 [Core 콘솔에 원격으로 액세스하도록 브라우저 구성](#), [Configuring Browsers To Remotely Access The Core Console\(Core 콘솔에 원격으로 액세스하도록 브라우저 구성\)](#) 주제에 설명된 대로 브라우저를 구성해야 합니다. Internet Explorer에서 신뢰할 수 있는 사이트를 업데이트하고 브라우저를 구성한 뒤, 다음 중 하나를 수행하여 Core 콘솔에 액세스합니다.

- 로컬에서 AppAssure Core 서버에 로그인하고 **Core Console(Core 콘솔)** 아이콘을 두 번 클릭합니다.
- 웹 브라우저에 다음 URL 중 하나를 입력합니다.
 - <https://<yourCoreServerName>:8006/apprecovery/admin/core>
 - <https://<yourCoreServerIPaddress>:8006/apprecovery/admin/core>




Internet Explorer에서 신뢰할 수 있는 사이트 업데이트

Internet Explorer에서 신뢰할 수 있는 사이트를 업데이트하려면 다음을 수행하십시오.

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

Core 콘솔에 원격으로 액세스하도록 브라우저 구성

원격 시스템에서 Core 콘솔에 액세스하려면 브라우저 설정을 수정해야 합니다.


-  **노트:** 브라우저 설정을 수정하려면 관리자 권한으로 시스템에 로그인합니다.
-  **노트:** Google Chrome에서는 Microsoft Internet Explorer 설정을 사용하므로 Internet Explorer를 사용하여 Chrome의 브라우저 설정을 변경합니다.
-  **노트:** Core 웹 콘솔에 로컬 또는 원격으로 액세스할 때 **Internet Explorer Enhanced Security Configuration(Internet Explorer 보안 강화형 구성)**이 설정되어 있는지 확인합니다. **Internet Explorer Enhanced Security Configuration(Internet Explorer 보안 강화형 구성)**을 설정하려면 다음을 수행합니다.
 1. **Server Manager**를 엽니다.
 2. 오른쪽에 표시된 **Local Server IE Enhanced Security Configuration(로컬 서버 IE 보안 강화형 구성)**을 선택하고 **On(설정)**으로 설정되어 있는지 확인합니다.

Internet Explorer 및 Chrome에서 브라우저 설정 구성

Internet Explorer 및 Chrome에서 브라우저 설정을 수정하려면 다음을 수행합니다.

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

Mozilla Firefox 브라우저 설정 구성

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

Mozilla Firefox 브라우저 설정을 수정하려면 다음을 수행합니다.

1. Firefox 주소 표시줄에 **about:config**를 입력하고 메시지가 표시되면 **I'll be careful, I promise(주의함)**를 클릭합니다.
2. **ntlm** 용어를 검색합니다.
3개 이상의 검색 결과가 표시됩니다.
3. **network.automatic-ntlm-auth.trusted-uris**를 두 번 클릭하고 시스템에 맞게 다음과 같은 설정을 입력합니다.
 - 로컬 시스템의 경우 호스트 이름을 입력합니다.

- 원격 시스템의 경우 AppAssure Core를 호스트하는 어플라이언스 시스템의 호스트 이름 또는 IP 주소를 쉼표로 구분하여 입력합니다(예: IP 주소,호스트 이름).

4. Firefox를 다시 시작합니다.

보존 기간 검토

AppAssure는 스냅샷을 만드는 빈도 및 스냅샷을 보존하는 기간을 결정하는 기본 보존 기간을 설정합니다. 보존 기간은 환경의 요구를 기반으로 해야 합니다. 예를 들어, 자주 변경되며 비즈니스 지속을 위해 업무에 중요한 데이터를 실행하는 서버를 백업하는 경우 스냅샷을 더 자주 만들어야 합니다.

보존 기간을 검토하고 변경하려면 다음을 수행하십시오.

1. Core 콘솔을 엽니다.
2. **Configuration(구성)** 탭을 선택한 후 **Retention Policy(보존 정책)**를 클릭합니다.
3. 조직의 요구에 따라 보존 정책을 조정합니다.
4. **Apply(적용)**를 클릭합니다.


에이전트 스냅샷 데이터 암호화

Core는 리포지토리 내의 에이전트 스냅샷 데이터를 암호화할 수 있습니다. 전체 리포지토리를 암호화하는 대신 리포지토리에서 에이전트가 보호되는 동안 여러 에이전트에 키를 재사용할 수 있도록 허용하는 암호화 키를 지정할 수 있습니다.

에이전트 스냅샷 데이터를 암호화하려면 다음을 수행하십시오.


1. AppAssure Core에서 **Configuration(구성) → Manage(관리) → Security(보안)**를 클릭합니다.
2. **Actions(작업)**을 클릭한 후 **Add Encryption Key(암호화 키 추가)**를 클릭합니다.
Create Encryption Key(암호화 키 생성) 페이지가 표시됩니다.
3. 다음 정보를 작성합니다.

필드	설명
이름	암호화 키의 이름을 입력합니다.
주석	암호화 키에 대한 주석을 입력합니다. 이는 암호화 키에 대한 추가 세부 정보를 제공하는 데 사용됩니다.
암호	암호를 입력합니다. 이는 액세스를 제어하는 데 사용됩니다.
암호 확인	암호를 다시 입력합니다. 이는 암호 입력을 확인하는 데 사용됩니다.

 **노트:** 암호를 손실하면 데이터에 액세스할 수 없으므로 암호화 암호를 기록하는 것이 좋습니다.

전자 메일 서버 및 전자 메일 알림 템플릿 구성

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

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

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

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

텍스트 상자	설명
SMTP 서버	전자 메일 알림 템플릿에 사용할 전자 메일 서버의 이름을 입력합니다. 이름 지정 규칙에는 호스트 이름, 도메인 및 접미사가 있습니다(예: smtp.gmail.com).
포트	포트 번호를 입력합니다. 이 번호는 전자 메일 서버의 포트를 식별하는 데 사용됩니다(예: Gmail의 경우 포트 587). 기본값은 25입니다.
시간 제한(초)	정수 값을 입력하여 시간이 초과되기 전에 연결을 시도하는 시간을 지정합니다. 이는 전자 메일 서버에 연결을 시도할 때 시간이 초과되기 전까지의 시간(초)을 설정하는 데 사용됩니다. 기본값은 30초입니다.
TLS	메일 서버에서 TLS(Transport Layer Security) 또는 SSL(Secure Sockets Layer)과 같은 보안 연결을 사용하는 경우 이 옵션을 선택합니다.
사용자 이름	전자 메일 서버의 사용자 이름을 입력합니다.
암호	전자 메일 서버에 액세스하기 위한 암호를 입력합니다.
보낸 사람	반송 전자 메일 주소를 입력합니다. 이는 전자 메일 알림 템플릿의 반송 전자 메일 주소를 지정하는 데 사용됩니다(예: noreply@localhost.com).
전자 메일 제목	전자 메일 템플릿의 제목을 입력합니다. 이는 전자 메일 알림 템플릿의 제목을 정의하는 데 사용됩니다(예: <hostname> - <level> <name>).
Email(이메일)	이벤트가 발생한 경우 해당 이벤트를 설명하는 템플릿의 본문과 심각도에 대한 정보를 입력합니다.

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

스트림 수 조정

기본적으로 AppAssure는 어플라이언스에 동시 스트림 3개를 허용하도록 구성되어 있습니다. 스트림의 수는 백업 중인 컴퓨터(에이전트)의 수보다 한 개 더 많습니다. 예를 들어, 6개의 에이전트를 백업 중인 경우 **Maximum Concurrent Transfers(최대 동시 전송)**를 7개로 설정해야 합니다.

동시 스트림의 수를 변경하려면 다음 단계를 따르십시오.

1. **Configuration(구성)** 탭을 선택한 다음 **Settings(설정)**를 클릭합니다.
2. **Transfer Queue(전송 대기열)**에서 **Change(변경)**를 선택합니다.

3. **Maximum Concurrent Transfers(최대 동시 전송)**를 백업 중인 클라이언트의 수보다 하나 더 많은 숫자로 변경합니다.

컴퓨터 보호 및 클라이언트에 대한 연결 확인

DL Appliance 및 Core를 구성한 후에 백업하려는 컴퓨터에 연결할 수 있는지 확인하십시오. 시스템을 보호하려면 다음을 수행하십시오.

1. Core 콘솔로 이동하고 **Machines(시스템)** 탭을 선택합니다.
2. **Actions(작업)** 드롭다운 메뉴에서 **Protect Machine(시스템 보호)**을 클릭합니다. **Connect(연결)** 대화 상자가 표시됩니다.
3. **Connect(연결)** 대화 상자에 아래 표에 설명된 대로 연결할 시스템에 대한 정보를 입력합니다.

호스트	보호할 시스템의 호스트 이름 또는 IP 주소입니다.
포트	AppAssure Core가 시스템의 에이전트와 통신하는 포트 번호입니다.
사용자 이름	이 컴퓨터에 연결하는 데 사용한 사용자 이름입니다(예: administrator).
암호	이 시스템에 연결하는 데 사용되는 암호입니다.

4. **Connect(연결)**를 클릭합니다.
5. 오류 메시지가 나타나면 어플라이언스가 컴퓨터에 연결해 백업할 수 없습니다. 문제를 해결하려면 다음과 같이 하십시오.
 - a. 네트워크 연결을 확인합니다.
 - b. 방화벽 설정을 확인합니다.
 - c. AppAssure 서비스 및 RPC가 실행 중인지 확인합니다.
 - d. 도메인 이름 서비스 조회를 확인합니다(해당되는 경우).

네트워크 연결 확인

네트워크 연결을 확인하려면 다음 단계를 따르십시오.

1. 연결하려는 클라이언트 시스템에서 명령줄 인터페이스를 엽니다.
2. **ipconfig** 명령을 실행하고 클라이언트의 IP 주소를 기록해 둡니다.
3. 어플라이언스에서 명령줄 인터페이스를 엽니다.
4. **ping <IP address of client>** 명령을 실행합니다.
5. 결과에 따라 다음 중 하나를 수행합니다.
 - 클라이언트가 ping에 응답하지 않을 경우 서버 연결과 네트워크 설정을 확인합니다.
 - 클라이언트가 응답할 경우 방화벽 설정이 AppAssure 구성 요소의 실행을 허용하는지 확인합니다.

방화벽 설정 확인

클라이언트가 네트워크에 제대로 연결되어 있지만 Core 콘솔에 표시되지 않으면 방화벽을 확인하여 필요한 인바운드 및 아웃바운드 통신이 허용되고 있는지 확인하십시오.

AppAssure Core와 여기서 백업되는 모든 클라이언트의 방화벽 설정을 확인하려면 다음 단계를 따르십시오.

1. DL1000 어플라이언스에서 **Start(시작)** → **Control Panel(제어판)**을 클릭합니다.
2. **Control Panel(제어판)**에서 **System and Security(시스템 및 보안)**를 클릭하고 **Windows Firewall(Windows 방화벽)** 아래에서 **Check firewall status(방화벽 상태 확인)**를 클릭합니다.

3. **Advanced Settings(고급 설정)**을 클릭합니다.
4. **Windows Firewall with Advanced Security(고급 보안이 포함된 Windows 방화벽)** 화면에서 **Inbound Rules(인바운드 규칙)**를 클릭합니다.
5. AppAssure Core 및 포트가 **Enabled(사용)** 열에 **Yes(예)**로 표시되는지 확인합니다.
6. 규칙이 활성화되어 있지 않으면 AppAssure Core를 마우스 오른쪽 단추로 클릭하고 **Enable Rule(규칙 사용)**을 선택합니다.
7. **Outbound Rules(아웃바운드 규칙)**를 클릭하고 AppAssure Core에 대해 동일한 사항을 확인합니다.

이름 분석 확인(해당되는 경우)

백업하려는 컴퓨터가 DNS를 사용하는 경우 DNS 순방향 조회 및 역방향 조회가 올바른지 확인하십시오. 역방향 조회가 올바른지 확인하려면 다음 단계를 따르십시오.

1. AppAssure 어플라이언스에서 **C:\Windows\system32\drivers\etc** 호스트로 이동합니다.
2. DL4300으로 백업하는 각 클라이언트의 IP 주소를 입력합니다.

네트워크 어댑터 티밍

기본적으로 DL4300 어플라이언스의 네트워크 어댑터(NIC)가 연결되어 있지 않아 시스템의 성능에 영향을 미치므로, NIC를 단일 인터페이스로 티밍하는 것이 좋습니다. NIC를 티밍하려면 다음을 수행해야 합니다.

- Broadcom Advanced Control 제품군 다시 설치
- NIC 탐 생성
- Hyper-V 가상 스위치 구성

Broadcom 고급 구성 제품군 다시 설치

Broadcom 고급 구성 제품군(BACS)을 다시 설치하려면 다음 단계를 따르십시오.

1. 시스템의 NIC를 식별합니다. NIC를 식별하려면 다음 단계를 따르십시오.
 - a. Dell Open Manage Server Administrator(OMSA)에 액세스합니다.
 - b. 기본 페이지에, **System(시스템)** → **Main System Chassis(기본 시스템 새시)** → **Slots(슬롯)**을 클릭합니다.
2. Broadcom 드라이버 및 관리 응용프로그램의 이전 버전을 제거합니다.
3. 알맞은 Broadcom 드라이버 및 BACS를 어플라이언스에 다운로드합니다.


다음 드라이버는 dell.com/support에서 사용할 수 있습니다.

 - QLogic 드라이버

Servers, storage, & Networking(서버, 스토리지 및 네트워킹) → **Dell Software DL 4300(Dell 소프트웨어 DL 4300)** → **Drivers & Downloads(드라이버 및 다운로드)** → **Category(범주)** → **Network(네트워크)** → **QLogic BCM57xx and BCM57xxx(QLogic bcm57xx 및 bcm57xxx)**를 클릭합니다.
 - Broadcom 드라이버


Servers, storage, & Networking(서버, 스토리지 및 네트워킹) → **Dell Software DL 4300(Dell 소프트웨어 DL 4300)** → **Drivers & Downloads(드라이버 및 다운로드)** → **Category(범주)** → **Network(네트워크)** → **Broadcom Windows 64bit driver update for NetXtreme Ethernet adapters(NetXtreme 이더넷 어댑터용 Broadcom Windows 64비트 드라이버 업데이트)**를 클릭합니다.
4. 설치 마법사를 통해 설치를 완료합니다.

NIC 팀 생성


 **노트:** Windows 2012 Server에서는 기본 팀밍 인터페이스를 사용하지 않는 것이 좋습니다. 팀밍 알고리즘은 인바운드 및 트래픽이 아닌 아웃바운드에 대해 최적화되어 있으므로 팀에 추가 네트워크 포트가 있어도 백업 작업부하의 성능이 저하됩니다.

NIC 팀밍을 생성하려면 다음 단계를 따르십시오.

1. **Start(시작)** → **Search(검색)** → **Broadcom Advanced Control Suite(Broadcom Advanced Control 제품군)** 로 이동합니다.

 **노트:** Broadcom Advanced Control Suite(Broadcom Advanced Control 제품군)을 사용하는 경우 Broadcom 네트워크 카드만 선택합니다.

2. **Broadcom Advanced Control Suite(Broadcom Advanced Control 제품군)**에서 **Teams(팀)** → **Go to Team View(팀 보기로 이동)**를 선택합니다.
3. 왼쪽에 있는 **Hosts list(호스트 목록)**에서 DL4300 어플라이언스의 호스트 이름을 마우스 오른쪽 단추로 클릭하고 **Create Team(팀 생성)**을 선택합니다.
Broadcom Teaming Wizard(Broadcom 팀밍 마법사) 창이 표시됩니다.
4. **Next(다음)**를 클릭합니다.
5. 팀의 이름을 입력하고 **Next(다음)**를 클릭합니다.
6. **Team Type(팀 유형)**을 선택하고 **Next(다음)**를 클릭합니다.
7. 팀에 포함시키려는 어댑터를 선택하고 **Add(추가)**를 클릭합니다.
8. 팀에 속한 다른 모든 어댑터에 대해 이 단계를 반복합니다.
9. 팀을 위한 모든 어댑터를 선택했다면 **Next(다음)**를 클릭합니다.
10. 팀에 오류가 발생할 경우 기본값으로 사용할 수 있는 NIC를 사용하려면 대기(standby) NIC를 선택합니다.
11. **LiveLink**를 구성할지 선택한 후 **Next(다음)**를 클릭합니다.
12. **Skip Manage VLAN(VLAN 관리 건너뛰기)**을 선택하고 **Next(다음)**를 클릭합니다.
13. **Commit changes to system(시스템에 변경 사항 커밋)**을 선택하고 **Finish(마침)**를 클릭합니다.
14. 네트워크 연결이 중단되었다는 경고가 나타나면 **Yes(예)**를 클릭합니다.

 **노트:** 팀을 구성하는 데 5분 정도 걸릴 수 있습니다.

Hyper-V 가상 스위치 구성

가상 대기 시스템이 프로덕션 환경 내에서 통신할 수 있도록 가상 스위치를 생성합니다. 외부 가상 스위치를 생성하려면 www.technet.microsoft.com에서 **가상 네트워크 구성** 섹션을 참조하십시오.

클라이언트에 에이전트 설치

AppAssure 어플라이언스에 의해 백업되는 각 클라이언트에 AppAssure 에이전트가 설치되어 있어야 합니다. AppAssure Core 콘솔을 사용하면 컴퓨터에 에이전트를 배포할 수 있습니다. 컴퓨터에 에이전트를 배포하려면 클라이언트로 푸시할 에이전트 유형 하나를 선택하도록 설정을 미리 구성해야 합니다. 이 방법은 모든 클라이언트가 같은 운영 체제를 실행 중인 경우에 효과적이지만 운영 체제의 버전이 다르면 컴퓨터에 에이전트를 설치하는 것이 더 쉬울 수 있습니다.

또한 컴퓨터 보호 프로세스를 수행하는 동안 에이전트 컴퓨터에 Agent 소프트웨어를 배포할 수 있습니다. 이 옵션은 Agent 소프트웨어가 아직 설치되어 있지 않은 컴퓨터에 사용할 수 있습니다. 컴퓨터를 보호하면서 Agent 소프트웨어를 배포하는 방법에 대한 자세한 내용은 dell.com/support/home에서 *Dell DL4300 어플라이언스 사용 설명서*를 참조하십시오.

원격으로 에이전트 설치(푸시)

원격으로 에이전트를 설치(푸시)하려면 다음과 같이 하십시오.

1. 클라이언트가 Windows Server 2012 이전 운영 체제 버전을 실행 중인 경우 클라이언트에 Microsoft.NET4 Framework가 설치되어 있는지 확인합니다.
 - a. 클라이언트에서 **Windows Server Manager**를 시작합니다.
 - b. **Configuration(구성) → Services(서비스)**를 클릭합니다.
 - c. Microsoft .NET Framework가 서비스 목록에 표시되는지 확인합니다.
설치되어 있지 않으면 microsoft.com에서 설치할 사본을 다운로드할 수 있습니다.
2. 다음과 같이 에이전트 설치 패키지 경로를 확인하거나 변경합니다.
 - a. AppAssure Core 콘솔에서 **Configuration(구성)** 탭을 클릭한 다음 왼쪽 패널에서 **Settings(설정)**를 클릭합니다.
 - b. **Deploy Settings(배포 설정)** 영역에서 **Change(변경)**를 클릭합니다.
 - c. 에이전트 위치에 대해 다음 정보를 작성합니다.

필드

설명

**에이전트 설치 프로
그램 이름** 에이전트에 대한 folder\file의 정확한 경로를 지정합니다.


Core 주소

AppAssure Core를 실행 중인 어플라이언스의 IP 주소를 지정합니다.



노트: 기본적으로 **Core Address(Core 주소)**는 비어 있습니다. 어플라이언스에 설치 파일이 설치되어 있으므로 **Core Address(Core 주소)** 필드에는 IP 주소가 필요하지 않습니다.


- d. **OK(확인)**를 클릭합니다.
3. **Tools(도구)** 탭을 클릭한 다음 왼쪽 패널에서 **Bulk Deploy(대량 배포)**를 클릭합니다.

 **노트:** 클라이언트에 에이전트가 이미 설치되어 있는 경우 설치 프로그램이 에이전트의 버전을 확인합니다. 무시하도록 시도하는 에이전트가 설치된 버전보다 최신인 경우 설치 프로그램에서 에이전트를 업그레이드하도록 제안합니다. 호스트에 현재 에이전트 버전이 설치되어 있는 경우 대량 배포에서 AppAssure Core와 에이전트 간의 보호를 시작합니다.



4. 클라이언트 목록에서 모든 클라이언트를 설치하고 **Verify(확인)**를 클릭하여 컴퓨터가 활성 상태이고 에이전트를 배포할 수 있는지 확인합니다.
5. **Message(메시지)** 열에서 컴퓨터가 준비되어 있다고 확인되면 **Deploy(배포)**를 클릭합니다.
6. 배포의 상태를 모니터링하려면 **Events(이벤트)** 탭을 선택합니다.
에이전트가 배포된 후에 클라이언트의 백업이 자동으로 시작합니다.

에이전트를 보호할 때 Agent 소프트웨어 배포

보호용 에이전트를 추가할 때 에이전트를 다운로드하여 배포할 수 있습니다.

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

보호용 에이전트를 추가할 때 에이전트를 배포하려면 다음을 수행합니다.

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


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

클라이언트에서 Microsoft Windows 에이전트 설치

에이전트를 설치하려면 다음 단계를 따르십시오.


1. 클라이언트에 Microsoft .NET4 Framework가 설치되어 있는지 확인합니다.
 - a. 클라이언트에서 **Windows Server Manager**를 시작합니다.
 - b. **Configuration(구성) → Services(서비스)**를 클릭합니다.
 - c. Microsoft .NET Framework가 서비스 목록에 표시되는지 확인합니다.
설치되어 있지 않으면 **microsoft.com**에서 사본을 다운로드할 수 있습니다.
2. 다음과 같이 에이전트를 설치합니다.
 - a. AppAssure 어플라이언스에서 백업하려는 클라이언트에 **C:\install\AppAssure** 디렉터리를 공유합니다.
 - b. 클라이언트 시스템에서 AppAssure 어플라이언스의 **C:\install\AppAssure**로 드라이브를 매핑합니다.
 - c. 클라이언트 시스템에서 **C:\install\AppAssure** 디렉터리를 열고 클라이언트 시스템에 맞는 에이전트를 두 번 클릭하여 설치를 시작합니다.


라이선스 포털을 사용하여 에이전트 추가

 **노트:** 에이전트를 다운로드하고 추가하려면 관리 권한이 있어야 합니다.

에이전트를 추가하려면 다음 단계를 따르십시오.


1. **AppAssure License Portal Home(AppAssure 라이선스 포털 홈)** 페이지에서 그룹을 선택한 다음 **Download Agent(에이전트 다운로드)**를 클릭합니다.
Download Agent(에이전트 다운로드) 대화 상자가 표시됩니다.
2. 다운로드하려는 설치 프로그램 버전 옆에서 **Download(다운로드)**를 클릭합니다.
다음에서 선택할 수 있습니다.
 - 32비트 Windows 설치 프로그램
 - 64비트 Windows 설치 프로그램
 - 32비트 Red Hat Enterprise Linux 6.3, 6.4 설치 프로그램
 - 64비트 Red Hat Enterprise Linux 6.3, 6.4 설치 프로그램
 - 32비트 CentOS 6.3, 6.4 설치 프로그램
 - 64비트 CentOS 6.3, 6.4 설치 프로그램
 - 32비트 Ubuntu 12.04 LTS, 13.04 설치 프로그램
 - 64비트 Ubuntu 12.04 LTS, 13.04 설치 프로그램
 - 32비트 SUSE Linux Enterprise Server 11 SP2, SP3 설치 프로그램
 - 64비트 SUSE Linux Enterprise Server 11 SP2, SP3 설치 프로그램
 - Microsoft Hyper-V Server 2012

 **노트:** Dell은 이러한 Linux 배포를 지원하며 릴리스된 커널 버전 대부분에서 테스트를 마쳤습니다.

 **노트:** Microsoft Hyper-V Server 2012에 설치된 에이전트는 Windows Server 2012의 Core 버전 모드로 작동됩니다.


Agent(에이전트) 파일이 다운로드됩니다.

3. **Installer(설치 프로그램)** 대화 상자에서 **Run(실행)**을 클릭합니다.

 **노트:** Core 컴퓨터를 사용하여 에이전트를 추가하는 방법에 대한 자세한 내용은 dell.com/support/home에서 *Dell DL4300 어플라이언스 사용 설명서*의 '에이전트 배포(강제 설치)' 항목을 참조하십시오.

Linux 컴퓨터에 에이전트 설치

분산을 위한 32비트 또는 64비트 설치 프로그램을 AppAssure Core를 사용하여 보호하려는 모든 Linux 서버에 다운로드하십시오. 설치 프로그램은 <https://licenseportal.com>의 AppAssure 라이선스 포털에서 다운로드할 수 있습니다. 자세한 내용은 [라이선스 포털을 사용하여 에이전트 추가](#)을(를) 참조하십시오.


 **노트:** 컴퓨터 보호와 관련된 보안은 Linux의 PAM(Pluggable Authentication Module)을 기반으로 합니다. **libpam**을 사용하여 인증된 사용자는 다음 그룹 중 하나에 속하는 경우에만 컴퓨터를 보호할 수 있는 권한을 갖습니다.


- sudo
- admin
- appassure
- wheel

컴퓨터를 보호하는 방법에 대한 자세한 내용은 dell.com/support/home에서 *Dell DL4300 어플라이언스 사용 설명서*의 '컴퓨터 보호' 섹션을 참조하십시오.

설치 지침은 사용 중인 Linux 분산에 따라 다릅니다. 분산에 Linux 에이전트를 설치하는 방법에 대한 자세한 내용은 다음을 참조하십시오.

- [Ubuntu에 에이전트 설치](#)
- [Red Hat Enterprise Linux 및 CentOS에 에이전트 설치](#)
- [SUSE Linux Enterprise Server에 에이전트 설치](#)

 **노트:** Dell은 이러한 Linux 배포를 지원하며 릴리스된 커널 버전 대부분에서 테스트를 마쳤습니다.

 **노트:** Linux 에이전트 설치에는 UFW, Yast2 또는 **system-config-firewall**을 통해 적용되지 않은 방화벽 규칙을 덮어씁니다.

방화벽 규칙을 수동으로 추가한 경우 설치 후 AppAssure 포트를 수동으로 추가해야 합니다. 기존 규칙의 백업이 `/var/lib/appassure/backup.fwl`에 기록됩니다.

에이전트에 액세스하려면 AppAssure Core용 TCP 포트 8006 및 8009에 대해 AppAssure 에이전트를 실행하는 모든 서버에 방화벽 예외를 추가해야 합니다.

Linux 에이전트 파일의 위치

Linux 에이전트 파일은 모든 분산에 대해 다음 디렉터리에 위치합니다.

구성 요소	위치/경로
mono	/opt/appassure/mono
에이전트	/opt/appassure/aagent
aamount	/opt/appassure/amount
aavdisk and aavdctl	/usr/bin

구성 요소	위치/경로
aavdisk를 위한 구성 파일	/etc/appassure/aavdisk.conf
aamount 및 에이전트를 위한 래퍼(wrapper)	<ul style="list-style-type: none"> • /usr/bin/aamount • /usr/bin/aagent
aavdisk 및 에이전트를 위한 자동 실행 스크립트	<ul style="list-style-type: none"> • /etc/init.d/appassure-agent • /etc/init.d/appassure-vdisk

에이전트 종속성

에이전트 설치 프로그램 패키지의 일부로 필요한 다음 종속성이 설치됩니다.

Ubuntu의 경우 종속성

appassure-vss에서 다음이 필요합니다.

dkms, gcc, make, linux-headers-`uname-r`

appassure-aavdisk에서 다음이 필요합니다.

libc6 (>=2.7-18), libblkid1, libpam0g, libpcre3

appassure-mono에서 다음이 필요합니다.

libc6 (>=2.7-18)

Red Hat Enterprise Linux 및 CentOS의 경우 종속성

nbd-dkms에서 다음이 필요합니다.

dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`

appassure-vss에서 다음이 필요합니다.

dkms, gcc, make, kernel-headers-`uname-r` kernel-devel-`uname-r`

appassure-aavdisk에서 다음이 필요합니다.

nbd-dkms, libblkid, pam, pcre

appassure-mono에서 다음이 필요합니다.

glibc >=2.11

SUSE Linux Enterprise Server의 경우 종속성


nbd-dkms에서 다음이 필요합니다. dkms, gcc, make, kernel-syms

appassure-vss에서 다음이 필요합니다. dkms, kernel-syms, gcc, make

appassure-aavdisk에서 다음이 필요합니다. libblkid1, pam, pcre

appassure-mono에서 다음이 필요합니다. glibc >= 2.11

Ubuntu에 에이전트 설치

 **노트:** 이 단계를 수행하기 전에 Ubuntu 고유의 설치 프로그램 패키지를 `/home/system directory`에 다운로드했는지 확인합니다.


Ubuntu에 AppAssure 에이전트를 설치하려면 다음을 수행하십시오.

1. 루트에 액세스하여 터미널 세션을 엽니다.

2. AppAssure Agent 설치 프로그램을 실행 가능하게 만들려면 다음 명령을 입력합니다.

`chmod +x appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.


파일을 실행할 수 있게 됩니다.

 **노트:** 32비트 환경의 경우 설치 프로그램의 이름이 `appassureinstaller_ubuntu_i386_5.x.x.xxxxx.sh`가 됩니다.

3. AppAssure Agent의 압축을 해제하고 설치하려면 다음 명령을 입력합니다.


`/appassure-installer_ubuntu_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.

Linux 에이전트가 압축 해제 및 설치 프로세스를 시작합니다. 에이전트에 필요한 누락된 패키지나 파일이 스크립트의 일부로 자동으로 다운로드되고 설치됩니다.

 **노트:** 에이전트에서 필요한 파일에 대한 자세한 내용은 [에이전트 종속성](#)(를) 참조하십시오.


설치 프로그램이 완료되면 컴퓨터에서 에이전트가 실행됩니다. Core로 이 컴퓨터를 보호하는 방법에 대한 자세한 내용은 dell.com/support/home에서 *Dell DL4300 어플라이언스 사용 설명서*의 워크스테이션 및 서버 보호 섹션을 참조하십시오.

Red Hat Enterprise Linux 및 CentOS에 에이전트 설치

 **노트:** 이 단계를 수행하기 전에 `/home/system directory`에 Red Hat 또는 CentOS 설치 프로그램 패키지를 다운로드했는지 확인하십시오. 다음 단계는 32비트 및 64비트 환경에서 모두 동일합니다.

Red Hat Enterprise Linux 및 CentOS에 에이전트를 설치하려면 다음을 수행하십시오.

1. 루트에 액세스하여 터미널 세션을 엽니다.
2. AppAssure Agent 설치 프로그램을 실행 가능하게 만들려면 다음 명령을 입력합니다.
`chmod +x appassure-installer__rhel_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.

 **노트:** 32비트 환경의 경우 설치 프로그램의 이름이 `appassureinstaller__rhel_i386_5.x.x.xxxxx.sh`가 됩니다.

파일을 실행할 수 있게 됩니다.

3. AppAssure Agent의 압축을 해제하고 설치하려면 다음 명령을 입력합니다.
`/appassure-installer__rhel_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.

Linux 에이전트가 압축 해제 및 설치 프로세스를 시작합니다. 에이전트에서 필요한 누락된 패키지나 파일은 스크립트의 일부로 자동 다운로드 및 설치됩니다.

에이전트에서 필요한 파일에 대한 자세한 내용은 [에이전트 종속성](#)(를) 참조하십시오.


설치 프로그램이 완료되면 컴퓨터에서 에이전트가 실행됩니다. Core로 이 컴퓨터를 보호하는 방법에 대한 자세한 내용은 [dell.com/support/home](#)에서 *Dell DL4300 어플라이언스 사용 설명서*의 '워크스테이션 및 서버 보호' 섹션을 참조하십시오.

SUSE Linux Enterprise Server에 에이전트 설치

 **노트:** 이 단계를 수행하기 전에 `/home/system directory`에 SLES(SUSE Linux Enterprise Server) 설치 프로그램 패키지를 다운로드했는지 확인하십시오. 다음 단계는 32비트 및 64비트 환경에서 모두 동일합니다.

SLES에 에이전트를 설치하려면 다음을 수행하십시오.

1. 루트에 액세스하여 터미널 세션을 엽니다.
2. AppAssure Agent 설치 프로그램을 실행 가능하게 만들려면 다음 명령을 입력합니다.
`chmod +x appassure-installer__sles_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.

 **노트:** 32비트 환경의 경우 설치 프로그램의 이름이 `appassureinstaller__sles_i386_5.x.x.xxxxx.sh`가 됩니다.

파일을 실행할 수 있게 됩니다.

3. AppAssure Agent의 압축을 해제하고 설치하려면 다음 명령을 입력합니다.
`/appassure-installer__sles_amd64_5.x.x.xxxxx.sh`를 입력한 후 <Enter> 키를 누릅니다.

Linux 에이전트가 압축 해제 및 설치 프로세스를 시작합니다. 에이전트에 필요한 누락된 패키지나 파일은 스크립트의 일부로 자동으로 다운로드되고 설치됩니다.

에이전트에서 필요한 파일에 대한 자세한 내용은 [에이전트 종속성](#)(를) 참조하십시오.

4. 새 패키지를 설치하라는 메시지가 나타나면 `y`를 입력한 후 <Enter> 키를 누릅니다.

시스템이 설치 프로세스를 마칩니다.

설치 프로그램이 완료되면 컴퓨터에서 에이전트가 실행됩니다. Core로 이 컴퓨터를 보호하는 방법에 대한 자세한 내용은 [dell.com/support/home](#)에서 *Dell DL4300 어플라이언스 사용 설명서*의 '워크스테이션 및 서버 보호' 섹션을 참조하십시오.

도움말 얻기


설명서 및 소프트웨어 업데이트 찾기

AppAssure Core 콘솔에 AppAssure, 어플라이언스 설명서 및 소프트웨어 업데이트로 직접 이동되는 링크가 있습니다. 링크에 액세스하려면 **Appliance(어플라이언스)** 탭을 클릭한 후 **Overall Status(전체 상태)**를 클릭합니다. 소프트웨어 업데이트 및 설명서에 대한 링크는 **Documentation(설명서)** 섹션에 있습니다.

소프트웨어 업데이트 찾기

AppAssure 5 Core 콘솔에서 AppAssure 및 DL4300 어플라이언스 소프트웨어 업데이트로 직접 이동되는 링크를 사용할 수 있습니다. 소프트웨어 업데이트에 대한 링크에 액세스하려면 **Appliance(어플라이언스)** 탭을 선택한 후 **Overall Status(전체 상태)**를 클릭합니다. 소프트웨어 업데이트에 대한 링크는 **Documentation(설명서)** 섹션에 있습니다.

Dell에 문의하기

 **노트:** 인터넷 연결을 사용할 수 없는 경우에는 제품 구매서, 포장 명세서, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 찾을 수 있습니다.

Dell은 다양한 온라인 및 전화 기반 지원과 서비스 옵션을 제공합니다. 인터넷에 연결되어 있지 않은 경우 구매 송장, 포장 명세서, 청구서 또는 Dell 제품 카탈로그에서 연락처 정보를 확인할 수 있습니다. 가용성은 국가 및 제품에 따라 다르며, 해당 지역에서 일부 서비스를 이용하지 못할 수도 있습니다. Dell의 영업, 기술 지원 또는 고객 지원 문제는 [software.dell.com/support](https://www.dell.com/support)를 참조하십시오.

설명서에 대한 사용자 의견

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