DDP Enterprise Server - Virtual Edition

빠른 시작 안내서 및 설치 안내서 v9.7

참고, 주의 및 경고

노트: "참고"는 제품을 보다 효율적으로 사용하는 데 도움이 되는 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.

VE 빠른 시작 안내서 및 설치 안내서

2017 - 04

개정 A01

목차

Virtual Edition 빠른 시작 안내서

이 빠른 시작 안내서는 숙련된 사용자가 DDP Enterprise Server - VE를 가동하여 신속하게 실행할 수 있도록 합니다. 일반적으로 DDP Enterprise Server - VE를 먼저 설치한 다음 클라이언트를 설치하는 것이 좋습니다.

자세한 지침은 Virtual Edition 설치 안내서를 참조하십시오.

VE 필수 조건에 대한 자세한 내용은 DDP Enterprise Server - VE 필수 조건, VE Remote Management Console 필수 조건 및 프록시 모드 필수 조건을 참조하십시오.

기존 DDP Enterprise Server - VE를 업데이트하는 방법에 대한 자세한 내용은 Update DDP Enterprise Server - VE를 참조하십시오.

DDP Enterprise Server - VE 설치

1 Dell Data Protection 파일이 저장된 디렉토리를 탐색한 다음 더블 클릭하여 VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**로 가져옵니다.
2 DDP Enterprise Server - VE의 전원을 켭니다.
3 화면의 지침을 따릅니다.

VE 구성

사용자를 활성화하기 전에 DDP Enterprise Server - VE Terminal에서 다음과 같은 구성 작업을 완료해야 합니다.

- 데이터베이스 암호 설정 또는 변경
- SMTP 설정 구성
- 기존 인증서 가져오기 또는 새 서버 인증서 등록
- DDP Enterprise Server - VE 업데이트
- 포트 22에서 SFTP를 지원하는 FTP 클라이언트를 설치하고 파일 전송(FTP) 사용자 설정을 참조하십시오.

  조직에 외부 방향 장치가 있는 경우에는 프록시 모드 설치 및 구성을 참조하십시오.

노트: 출고 시 Enterprise Edition 클라이언트 권한을 부여받거나 라이선스를 구매하는 경우 권한 부여를 사용하도록 도메인 컨트롤러에서 GPO를 설정합니다(Virtual Edition 실행 서버와 다를 수 있음). 아웃바운드 포트 443을 사용하여 서버와 통신할 수 있는지 확인하십시오. 어떠한 이유로든 포트 443이 차단된 경우 권한 부여 기능이 작동하지 않습니다.

VE Remote Management Console 열기

다음에서 VE Remote Management Console 열기

https://server.domain.com:8443/webui/

기본 자격 증명은 **superadmin/changeit**입니다.

지원되는 웹 브라우저의 목록은 E Remote Management Console 필수 조건을 참조하십시오.

관리 작업

VE Remote Management Console을 시작하지 않았으면 바로 시작합니다. 기본 자격 증명은 **superadmin/changeit**입니다.

관리자 역할은 최대한 빨리 할당하는 것이 좋습니다. 이 작업을 지금 완료하려면 Dell 관리자 역할 지정을 참조하십시오.

*Dell Data Protection AdminHelp*를 시작하려면 VE Remote Management Console 오른쪽 상단 모서리에 있는 "?"를 클릭합니다. *시작하기* 페이지가 표시됩니다. **도메인 추가**를 클릭합니다.

고객을 위해 기준 정책이 설정된 상태지만 다음과 같은 특정 요구 사항에 따라 수정이 필요할 수 있습니다(라이선스 및 권한에 따라 활성화 가능).

- Windows 컴퓨터 암호화
- 자체 암호화 드라이브가 포함된 컴퓨터 암호화
- BitLocker 관리를 사용하지 않음
- 고급 위협 차단이 켜지지 않았습니다.
- 위협 차단이 활성화됨
- 외부 미디어를 암호화하지 않음
- 포트에 연결된 장치를 암호화하지 않음
- Dell Data Guardian을 사용함
- Mobile Edition을 사용하지 않음

AdminHelp 주제 *정책 관리*에서 기술 그룹 및 정책 설명으로 가십시오.

빠른 시작 작업이 완료되었습니다.

2

Virtual Edition 설치 안내서

이 설치 안내서는 초보자를 위한 DDP Enterprise Server - VE 설치 및 구성 안내서입니다. 일반적으로 DDP Enterprise Server - VE를 먼저 설치한 다음 클라이언트를 설치하는 것이 좋습니다.

기존 DDP Enterprise Server - VE를 업데이트하는 방법에 대한 자세한 내용은 Update DDP Enterprise Server - VE를 참조하십시오.

DDP Enterprise Server - VE 정보

DDP Enterprise Server - VE는 Dell 솔루션의 보안 관리 제품입니다. VE Remote Management Console을 사용하면 관리자가 기업 전체에 걸쳐 끝점, 정책 적용 및 보호 상태를 모니터링할 수 있습니다. Proxy Mode는 DDP Enterprise Server - VE에서 사용할 수 있는 프론트 엔드 DMZ Mode 옵션을 제공합니다.

DDP Enterprise Server - VE의 특징은 다음과 같습니다.

- 최대 3,500대 장치에 대한 중앙 집중화된 관리
- 역할 기반의 보안 정책 생성 및 관리
- 관리자 지원 장치 복구
- 관리 임무 구분
- 보안 정책 자동 배포
- 구성 요소 간 통신 시 신뢰할 수 있는 경로
- 고유한 암호화 키 생성 및 자동 보안 키 에스크로
- 중앙 집중화된 준수 감사 및 보고
- 자체 서명 인증서의 자동 생성

Dell ProSupport에 문의

877-459-7304(내선번호 4310039)로 전화하면 연중무휴 하루 24시간 Dell Data Protection 제품에 대한 전화 지원을 받을 수 있습니다.

또한, dell.com/support에서 Dell Data Protection 제품에 대한 온라인 지원도 가능합니다. 온라인 지원에는 드라이버, 매뉴얼, 기술 자문, FAQ 및 최근에 나타나는 문제도 포함됩니다.

올바른 기술 전문가에게 신속히 연결될 수 있도록 전화할 때 서비스 코드를 준비하십시오.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

요구 사항

DDP Enterprise Server - VE의 필수 조건

하드웨어

DDP Enterprise Server - VE에 권장되는 디스크 공간은 80GB입니다.

가상 환경

DDP Enterprise Server - VE v9.6은 다음 가상화된 환경을 통해 검증되었습니다.

가상 환경

- VMware Workstation 12.5
  - 64비트 CPU 필요
  - 4GB RAM 권장
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17을 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/workstation-11/index.jsp를 참조하십시오.

- VMware Workstation 11
  - 64비트 CPU 필요
  - 4GB RAM 권장
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17을 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/workstation-11/index.jsp를 참조하십시오.

- VMware ESXi 6.0
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-60/index.jsp를 참조하십시오.

- VMware ESXi 5.5
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 지원되는 호스트 운영 체제의 전체 목록은 http://www.vmware.com/resources/compatibility/search.php를 참조하십시오.
  - 하드웨어가 최소 VMware 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM
  - 자세한 내용은 http://pubs.vmware.com/vsphere-55/index.jsp을 참조하십시오.

- Hyper-V Server(전체 또는 핵심 설치)
  - 64비트 x86 CPU 필요
  - 2코어 이상의 호스트 컴퓨터
  - 8GB 이상의 RAM 권장
  - 운영 체제가 필요 없음
  - 하드웨어가 최소 Hyper-V 요구 사항을 충족해야 함
  - 전용 이미지 리소스를 위한 4GB 이상의 RAM

가상 환경

- 반드시 1세대 가상 시스템으로 실행해야 합니다.
- 자세한 내용은 https://technet.microsoft.com/en-us/library/hh923062.aspx을 참조하십시오.

VE Remote Management Console의 필수 조건

Internet 브라우저

노트:
브라우저에서 쿠키를 허용해야 합니다.

다음 표에 지원되는 Internet 브라우저가 나와 있습니다.

Internet 브라우저

- Internet Explorer 11.x 이상
- Mozilla Firefox 41.x 이상
- Google Chrome 46.x 이상

Proxy Mode 필수 조건

하드웨어

다음 표에는 Proxy Mode의 *최소* 하드웨어 요구 사항이 자세히 나와 있습니다.

프로세서

2GHz Core 2 Duo 이상

RAM

+-2GB 전용 RAM(최소) / 4GB 전용 RAM(권장)

사용 가능한 디스크 공간

약 1.5GB의 사용 가능한 디스크 공간(및 가상 페이징 공간)

네트워크 카드

10/100/1000 네트워크 인터페이스 카드

기타

설치 및 등록된 TCP/IP

소프트웨어

다음 표에는 Proxy Mode보다 먼저 설치해야 하는 소프트웨어에 대해 자세히 나와 있습니다.

필수 조건

- **Windows Installer 4.0 이상**

필수 조건

설치를 수행할 서버에 Windows Installer 4.0 이상이 설치되어 있어야 합니다.

- **Microsoft Visual C++ 2010 재배포 가능 패키지**

  설치되어 있지 않은 경우 설치 프로그램을 통해 자동 설치됩니다.

- **Microsoft .NET Framework 버전 4.5**

  Microsoft는 .NET Framework 버전 4.5용 보안 업데이트를 게시했습니다.

다음 표에는 Proxy Mode 서버의 소프트웨어 요구 사항이 자세하게 나와 있습니다.

노트:

Windows Server 2008을 사용할 경우 항상 UAC를 비활성화하십시오. UAC를 비활성화한 후에는 서버를 재부팅해야 변경사항이 적용됩니다.

Windows Server의 레지스트리 위치: HKLM\SOFTWARE\Dell

운영 체제

- **Windows Server 2008 R2 SP0-SP1 64비트**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2008 SP2 64비트**

  - Standard Edition

  - Enterprise Edition

- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition

- **Windows Server 2016**

  - Standard Edition

  - Datacenter Edition

DDP Enterprise Server - VE 다운로드

초기에 설치할 때 DDP Enterprise Server - VE는 가상 컴퓨터에서 실행되는 소프트웨어를 전달하는 OVA(Open Virtual Application) 파일로 제공됩니다. DDP Enterprise Server - VE OVA 파일은 www.dell.com/support의 다음과 같은 Dell Data Protection 제품의 '제품 지원' 페이지에서 볼 수 있습니다.

암호화

또는

Endpoint Security Suite

또는

Endpoint Security Suite Enterprise

또는

Data Guardian

OVA 파일을 다운로드하려면 다음을 수행하십시오.

1 Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise 또는 Data Guardian의 제품 지원 페이지로 이동합니다.
2 **드라이버 및 다운로드**를 클릭합니다.
3 "<OS 버전>의 사용 가능한 모든 업데이트 보기" 옆의 **OS 변경**을 클릭하고 **VMware ESXi 6.0, VMware ESXi 5.5** 또는 **VMware ESXi 5.1**을 선택합니다.
4 "보기 기준:" 아래에서 **모두 표시**를 선택합니다.
5 Dell Data Protection에서 **다운로드**를 선택합니다.

DDP Enterprise Server - VE 설치

시작하기 전에, 모든 시스템 및 가상 환경의 요구 사항이 충족되었는지 확인하십시오.

1 설치 미디어에서 Dell Data Protection 파일을 찾아 더블 클릭하여 VMware **DDP Enterprise Server - VE v9.x.x Build x.ova**로 가져옵니다.
2 DDP Enterprise Server - VE의 전원을 켭니다.
3 라이선스 계약에 사용되는 언어를 선택한 후 **EULA 표시**를 선택합니다.
4 계약서를 읽고 **EULA 동의**를 선택합니다.
5 사용 가능한 업데이트가 있는 경우 **채택**을 선택합니다.
6 **기본 모드** 또는 **연결되지 않은 모드**를 선택합니다.

> **노트:**
> **연결되지 않은 모드**를 선택하면 VE는 절대로 기본 모드로 변경할 수 없습니다.
>
> 연결되지 않은 모드는 인터넷과 보호되지 않은 LAN 또는 기타 네트워크에서 VE를 격리합니다. 모든 업데이트는 수동으로 수행해야 합니다. 연결되지 않은 모드 기능 및 정책에 대한 자세한 내용은 *AdminHelp*를 참조하십시오.

7 기본 암호 변경 메시지가 표시되면 **예**를 선택합니다.
8 *ddpuser 암호 설정* 화면에서, 현재(기본) 암호인 **ddpuser**를 입력하고 고유한 암호를 입력한 후 다시 한번 입력한 다음 **확인**을 선택합니다.

   암호는 반드시 다음을 포함해야 합니다.

   - 8자 이상의 문자
   - 1자 이상의 대문자
   - 1개 이상의 숫자
   - 1자 이상의 특수 문자

9 *호스트 이름 구성* 대화상자에서 백스페이스 키를 사용하여 기본 호스트 이름을 제거합니다. 고유한 호스트 이름을 입력하고 **확인**을 선택합니다.
10 *네트워크 설정 구성* 대화상자에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.

   - (기본 설정) DHCP 사용
   - (권장 설정) DHCP 사용 필드에서 스페이스바를 눌러 X를 제거하고 해당하는 경우 다음 주소를 수동으로 입력합니다. 고정 IP 네트워크 마스크 기본 게이트웨이 DNS 서버 1 DNS 서버 2 DNS 서버 3

> **노트: 고정 IP를 사용할 경우 DNS 서버에 호스트 항목도 만들어야 합니다.**

11 *시간대* 화면에서, 화살표 키를 사용하여 원하는 시간대를 강조표시하고 **Enter**를 선택합니다.

12 시간대 확인 메시지가 표시되면 **확인**을 선택합니다.
13 초기 구성이 완료되었음을 나타내는 메시지가 표시되면 **확인**을 선택합니다.
14 데이터베이스 암호 설정 또는 변경.
15 SMTP 설정 구성.
16 기존 인증서 가져오기 또는 새 서버 인증서 등록.
17 DDP Enterprise Server - VE 업데이트.
18 포트 22에서 SFTP를 지원하는 FTP 클라이언트를 설치하고 파일 전송(FTP) 사용자 설정을 참조하십시오.

DDP Enterprise Server - VE 설치 작업이 완료됩니다.

VE Remote Management Console 열기

다음에서 VE Remote Management Console 열기

https://server.domain.com:8443/webui/

기본 자격 증명은 **superadmin/changeit**입니다.

지원되는 웹 브라우저의 목록은 E Remote Management Console 필수 조건을 참조하십시오.

프록시 모드 설치 및 구성

프록시 모드에서는 DDP Enterprise Server - VE와 함께 사용하기 위한 프론트 엔드(DMZ 모드) 옵션을 제공합니다. DMZ에 Dell 구성요소를 배포하려면, 구성요소가 공격으로부터 적절히 보호를 받을 수 있는지 확인해야 합니다.

노트: 보호된 Office 모드를 실행할 때 Data Guardian이 보호하는 모든 파일에 콜백 비콘을 삽입하는 Data Guardian 콜백 비콘을 지원하기 위해 이 설치 과정의 일부로 비콘 서비스가 설치됩니다. 이렇게 하면 Dell 프론트 엔드 서버와 모든 위치의 모든 장치 사이에서 통신을 할 수 있습니다. 콜백 비콘을 사용하기 전에 필요한 네트워크 보안이 구성되어 있는지 확인합니다. 기본적으로 콜백 비콘 활성화 정책이 활성화됩니다.

설치를 수행하려면 DMZ 서버의 정규화된 호스트 이름이 필요합니다.

1 Dell 설치 미디어에서 Dell Enterprise Server 디렉토리로 이동합니다. Dell Enterprise Server-x64를 VE를 설치할 서버의 루트 디렉토리에 **압축 해제**합니다(복사/붙여넣기 또는 드래그/드롭 불가). ***복사/붙여넣기 또는 드래그/드롭을 실행하면 오류가 발생해 설치가 성공적으로 완료되지 않습니다.***
2 **setup.exe**를 더블 클릭합니다.
3 *InstallShield 마법사* 대화상자에서, 설치 언어를 선택한 후 **확인**을 클릭합니다.
4 필수 구성요소가 아직 설치되어 있지 않으면, 필수 구성요소가 설치된다는 메시지가 표시됩니다. **설치**를 클릭합니다.
5 *시작* 대화상자에서 **다음**을 클릭합니다.
6 라이선스 계약을 읽고 조건을 수락한 후 **다음**을 클릭합니다.
7 제품 키를 입력합니다.
8 **프론트 엔드 설치**를 선택하고 **다음**을 클릭합니다.
9 프론트 엔드 서버를 기본 위치인 C:\Program Files\Dell에 설치하려면 **다음**을 클릭합니다. 그렇지 않으면, **변경**을 클릭하여 다른 위치를 선택하고 **다음**을 클릭합니다.
10 사용할 디지털 인증서 유형을 선택할 수 있습니다. **신뢰할 수 있는 인증 기관의 디지털 인증서를 사용할 것을 권장합니다.** 아래에서 옵션 "a" 또는 "b"를 선택하십시오.

a CA 기관에서 구입한 기존 인증서를 사용하려면 **기존 인증서 가져오기**를 선택하고 **다음**을 클릭합니다.
찾아보기를 클릭하여 인증서 경로를 입력합니다.

이 인증서와 관련된 암호를 입력합니다. 키 저장 파일 확장자는 .p12 또는 pfx일 것입니다.

다음을 클릭합니다.

노트:

이 설정을 사용하려면, 내보내진 CA 인증서 중 가져올 CA 인증서에 최대의 신뢰 체인이 수립되어 있어야 합니다. 확실하지 않을 경우, CA 인증서를 다시 내보내고 "인증서 내보내기 마법사"에서 다음 옵션이 선택되었는지 확인하십시오.

- 개인 정보 교환 - PKCS#12(.PFX)
- 가능한 한 모든 인증서를 인증서 경로에 포함
- 모든 확장 속성을 내보냄

b 자체 서명된 인증서를 만들려면 **자체 서명된 인증서를 생성하여 키 저장소에 가져오기**를 선택하고 **다음**을 클릭합니다. *자체 서명 인증* 대화상자에 다음 정보를 입력합니다.

정규화된 컴퓨터 이름(예: computername.domain.com)

조직

조직 단위(예: 보안 팀)

시

도(전체 이름)

국가: 알파벳 두 글자로 된 국가 약어

다음을 클릭합니다.

노트:

기본적으로 인증서 유효 기간은 1년입니다.

11 *프론트 엔드 서버 설정* 대화상자에서, 백 엔드 서버의 정규화된 호스트 이름이나 DNS 별칭을 입력하고 **Enterprise Edition**을 선택한 후 **다음**을 클릭합니다..

12 *프론트 엔드 서버 설치 설정* 대화상자에서 호스트 이름 및 포트를 보거나 편집할 수 있습니다.

- 기본 호스트 이름 및 포트를 수락하려면 *프론트 엔드 서버 설치 설정* 대화상자에서 **다음**을 클릭합니다.
- 호스트 이름을 보거나 편집하려면 *프론트 엔드 서버 설정* 대화상자에서 **호스트 이름 편집**을 클릭합니다. 필요한 경우에만 호스트 이름을 편집합니다. 기본값 사용을 권장합니다.

노트:

호스트 이름에는 밑줄("_")을 사용할 수 없습니다.

프록시 설치를 구성하지 않으려는 경우에만 프록시를 선택 취소하십시오. 이 대화상자에서 프록시를 선택 취소하면 프록시가 설치되지 않습니다.

작업을 마친 후 **확인**을 클릭합니다.

- 포트를 보거나 편집하려면 *프론트 엔드 서버 설정* 대화상자에서 **외부 연결 포트 편집** 또는 **내부 연결 포트 편집**을 클릭합니다. 필요한 경우에만 포트를 편집합니다. 기본값 사용을 권장합니다.

프론트 엔드 호스트 이름 편집 대화상자에서 프록시를 선택 취소하면 외부 포트 또는 내부 포트 대화상자에 해당 포트가 표시되지 않습니다.

작업을 마친 후 **확인**을 클릭합니다.

13 *프로그램 설치 준비 완료* 대화상자에서 **설치**를 클릭합니다

14 설치가 완료되면 **마침**을 클릭합니다.

VE Terminal - 기본 구성 작업

주 메뉴에서 기본 구성 작업에 액세스합니다.

호스트 이름 변경

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *기본 구성* 메뉴에서 **호스트 이름**을 선택합니다.
2 백스페이스 키를 사용하여 기존 DDP Enterprise Server - VE 호스트 이름을 제거하고 새 호스트 이름으로 바꾼 다음 **확인**을 선택합니다.

네트워크 설정 변경

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *기본 구성* 메뉴에서 **네트워크 설정**을 선택합니다.
2 *네트워크 설정 구성* 화면에서 아래 옵션 중 하나를 선택한 다음 **확인**을 선택합니다.
   - (기본 설정) DHCP 사용
   - (권장 설정) DHCP 사용 필드에서 스페이스바를 눌러 X를 제거한 다음 해당하는 경우 다음 주소를 수동으로 입력합니다.

     고정 IP

     네트워크 마스크

     기본 게이트웨이

     DNS 서버 1

     DNS 서버 2

     DNS 서버 3

     노트: 고정 IP를 사용할 경우 DNS 서버에 호스트 항목을 만들어야 합니다.

DMZ 호스트 이름 설정

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *기본 구성* 메뉴에서 **DMZ 호스트 이름**을 선택합니다.
2 DMZ 서버의 정규화된 도메인 이름을 입력하고 **확인**을 선택합니다.

노트: Proxy Mode(DMZ Mode)를 사용하려면 Proxy Mode를 설치하고 구성해야 합니다.

시간대 변경

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *기본 구성* 메뉴에서 **시간대**를 선택합니다.
2 *시간대* 화면에서, 화살표 키를 사용하여 원하는 시간대를 강조표시하고 **Enter**를 선택합니다.
3 시간대 확인 메시지가 표시되면 **확인**을 선택합니다.

DDP Enterprise Server - VE 업데이트

특정 업데이트에 대한 자세한 내용은 Dell 지원 웹 사이트 http://www.dell.com/support에 있는 VE 기술 자문을 참조하십시오. 이미 적용된 업데이트의 버전 및 설치 날짜를 확인하려면 **기본 구성** 메뉴에서 **DDP Enterprise Server - VE 업데이트** > **마지막 성공된 업데이트 적용**을 선택하십시오.

VE 업데이트의 이메일 알림을 받으려면 SMTP 설정 구성을 참조하십시오.

노트: 기본 모드에서 업데이트는 DDP Enterprise Server - VE의 초기 설치 후, 클라이언트 활성화 전에 수행해야 합니다.

정책이 변경되었으나 Remote Management Console에 적용이 되지 않은 경우, VE를 업데이트하기 전에 정책 변경을 적용합니다.

1 Dell 관리자 계정으로 원격 관리 콘솔에 로그인합니다.
2 왼쪽 메뉴에서 **관리** > **커밋**을 클릭합니다.
3 설명 필드에 변경에 대한 설명을 입력합니다.
4 **정책 커밋**을 클릭합니다.
5 커밋이 완료되면, Remote Management Console에서 로그아웃합니다.

VE 업데이트(기본 모드)

1 Dell은 정규적인 백업을 수행할 것을 권장합니다. 업데이트 전에 백업 과정이 올바르게 진행되는지 확인합니다. 백업 및 복원을 참조하십시오.
2 **기본 구성** 메뉴에서 DDP Enterprise Server - VE 업데이트를 선택합니다.
3 필요한 작업을 선택합니다.
   - 업데이트 서버 설정 - DDP Enterprise Server - VE 업데이트 패키지의 서버 위치를 설정하거나 변경하려면 이 옵션을 선택합니다. *업데이트 서버 설정* 화면에서 백스페이스 키를 사용하여 기존의 서버 호스트 이름 또는 IP 주소를 제거합니다. 새 정규화된 도메인 이름 또는 IP 주소를 입력하고 **확인**을 선택합니다.

     기본 업데이트 서버는 **act.credant.com**입니다.
   - 프록시 설정 - 업데이트를 다운로드하기 위해 프록시 서버를 설정하려면 이 옵션을 선택합니다.

     프록시 설정 구성 화면에서 스페이스바를 눌러 프록시 사용 필드에 **X**를 입력합니다. HTTPS, HTTP 및 FTP 프록시 주소를 입력합니다. 방화벽 인증이 필요한 경우 스페이스바를 눌러 인증 필요 필드에 **X**를 입력합니다. 사용자 이름과 암호를 입력하고 **확인**을 누릅니다.

     노트: FTP 사이트에서 업데이트하려면 FTP 사용자 이름과 암호를 입력한 다음 URL을 입력합니다.
   - 업데이트 확인 - DDP Enterprise Server - VE 업데이트 패키지의 업데이트 서버가 있는지 확인하려면 이 옵션을 선택합니다.
   - 업데이트 다운로드 - 업데이트 확인을 통해 발견한 업데이트를 다운로드하려면 이 옵션을 선택합니다.
   - 업데이트 적용 - 다운로드한 DDP Enterprise Server - VE 업데이트 패키지를 적용하려면 이 옵션을 선택합니다. *업데이트 (.deb) 파일 선택* 화면에서, 설치할 업데이트 패키지를 선택하고 **Enter**를 누릅니다.
   - 마지막 업데이트 적용 - 현재 VE 버전의 버전 번호 및 설치 날짜를 보려면 이 옵션을 선택합니다.

VE 업데이트(연결되지 않은 모드)

1 Dell은 정규적인 백업을 수행할 것을 권장합니다. 업데이트 전에 백업 과정이 올바르게 진행되는지 확인합니다. 백업 및 복원을 참조하십시오.
2 Dell 지원 웹 사이트에서 최신 VE 업데이트가 들어있는 .deb 파일을 가져 오십시오.
   VE 다운로드는 다음에서 **드라이버 및 다운로드** 폴더에 있습니다:

   www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

또는

www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

또는

www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

또는

www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

3 .deb 파일을 VE의 보안 FTP 서버에 있는 /updates 폴더에 저장하십시오.
FTP 클라이언트가 포트 22에서 SFTP를 지원하고 FTP 사용자가 설정되어 있는지 확인하십시오. 파일 전송(FTP) 사용자 설정을 참조하십시오.

4 **기본 구성** 메뉴에서 DDP Enterprise Server - VE 업데이트를 선택합니다.

5 **업데이트 적용**을 선택한 다음 **Enter** 키를 누릅니다.
.deb 파일이 표시되지 않으면 .deb 파일이 올바른 위치에 저장되어 있는지 확인하십시오.

6 설치할 .deb 업데이트 파일을 선택하고 **Enter** 키를 누릅니다.

사용자 암호 변경

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

다음 사용자의 암호를 변경할 수 있습니다.

- ddpuser(DDP Enterprise Server - VE Terminal 관리자) - 이 사용자가 VE Terminal과 목록에 접속했습니다.
- ddpconsole(DDP Enterprise Server - VE 셸 접속) - 이 사용자가 VE 셸 접속 권한을 가지고 있습니다. 네트워크 관리자는 네트워크 연결 확인 및 문제 해결을 위해 셸 접속을 사용할 수 있습니다.
- ddpsupport (Dell ProSupport 관리자) - 이 사용자는 Dell ProSupport 사용만을 위해 존재합니다. 보안 목적을 위해, 이 계정의 암호를 관리할 수 있습니다.

1 *기본 구성* 메뉴에서 **사용자 암호 변경**을 선택합니다.

2 *사용자 암호 변경* 화면에서, 변경할 사용자 암호를 선택하고 **Enter**를 선택합니다.

3 *암호 설정* 화면에서, 현재 암호를 입력하고 새 암호를 입력한 후 다시 한번 새 암호를 입력한 다음 **확인**을 선택합니다.
암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

파일 전송(FTP) 사용자 설정

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

최대 3명의 사용자에게 백업 및 복원 작업을 위해 DDP Enterprise Server - VE의 Secure FTP 서버에 액세스 권한을 부여할 수 있습니다. VE FTP 서버를 사용하여 업데이트를 DDP Enterprise Server - VE에 저장하거나 업로드할 수도 있습니다.

1 *기본 구성* 메뉴에서 **파일 전송(FTP) 사용자**를 선택합니다.

2 *FTP 사용자 구성* 화면에서, FTP 사용자를 활성화하려면 스페이스바를 눌러 해당 사용자의 상태 필드에 **X**를 입력합니다. FTP 사용자를 비활성화하려면, 스페이스바를 눌러 해당 사용자의 상태 필드에서 **X**를 제거합니다.

3 SFTP 사용자의 사용자 이름과 암호를 입력합니다.

암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

4 SFTP 사용자를 입력한 후 **확인**을 선택합니다.

SSH 사용

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

Support 관리자 로그인, DDP Enterprise Server - VE 셸 액세스, VE Terminal 명령줄 인터페이스에 SSH를 사용할 수 있습니다.

1 *기본 구성* 메뉴에서 **SSH 설정**을 선택합니다.
2 SSH를 사용할 사용자를 강조표시하고 스페이스바를 눌러 해당 필드에 **X**를 입력한 후 **확인**을 선택합니다.

VE 서비스 시작 또는 중지

이 작업은 필요할 경우에만 수행합니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 모든 VE 서비스를 동시에 시작하거나 중지하려면 *기본 구성* 메뉴에서 **응용프로그램 시작** 또는 **응용프로그램 중지**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.

노트: 서버 상태 변경은 완료되기까지 최대 2분이 소요될 수 있습니다.

VE 재부팅

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서 **어플라이언스 재부팅**을 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후 DDP Enterprise Server - VE에 로그인합니다.

VE 종료

이 작업은 필요할 경우에만 수행합니다.

1 *기본 구성* 메뉴에서, 아래로 스크롤하여 **어플라이언스 종료**를 선택합니다.
2 확인 메시지가 표시되면 **예**를 선택합니다.
3 재시작 후 DDP Enterprise Server - VE에 로그인합니다.

VE Terminal - 고급 구성 작업

주 메뉴에서 고급 구성 작업에 액세스할 수 있습니다.

데이터베이스 암호 설정 또는 변경

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *고급 구성* 메뉴에서 **데이터베이스 암호**를 선택합니다.
2 데이터베이스에 액세스하기 위한 암호를 입력하고 **확인**을 선택합니다.
암호는 반드시 다음을 포함해야 합니다.

- 8자 이상의 문자
- 1자 이상의 대문자
- 1개 이상의 숫자
- 1자 이상의 특수 문자

노트: 설치가 완료된 후 암호를 백업해두는 것이 좋습니다.

SMTP 설정 구성

DDP Enterprise Server - VE 이메일 알림 수신 **또는** Data Guardian을 사용하려면 다음 단계에 따라 SMTP 설정을 구성하십시오. DDP Enterprise Server - VE 이메일 알림은 DDP Enterprise Server - VE 서버 상태 오류 현황, 암호 업데이트, DDP Enterprise Server - VE 업데이트 사용 가능성 및 클라이언트 라이선스 문제를 수신자에게 알려줍니다.

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

SMTP 설정을 구성하려면 다음 단계를 따르십시오.

1 *고급 구성* 메뉴에서 **이메일 알림**을 선택합니다.
2 *이메일 알림 설정* 화면에서 이메일 경고를 사용하려면 스페이스바를 눌러 이메일 경고 사용 필드에 **X**를 입력합니다.
3 SMTP Server의 정규화된 도메인 이름을 입력합니다.
4 SMTP 포트를 입력합니다.
5 '보내는 사용자' 필드에는 이메일 알림을 보내는 이메일 계정 ID를 입력합니다.
6 '사용자 입력' 필드에는 구성된 이메일 알림을 변경할 때 액세스를 위한 이메일 계정 ID를 입력합니다.
7 '암호' 필드에는 구성된 이메일 알림을 변경할 때 액세스를 위한 암호를 입력합니다.
8 VE 상태, 암호 업데이트, 업데이트 가용성에 대한 '메일 ID' 필드에는 각 알림 유형을 받을 수신자 목록을 입력합니다. 수신자 목록을 입력할 때에는 다음 규칙을 따릅니다.
   - 이메일 주소 형식은 recipient@dell.com입니다.
   - 수신자는 쉼표 또는 세미콜론으로 구분합니다.
9 알림을 사용하려면 '서비스 경고 알림' 필드에서 스페이스바를 눌러 필드에 **X**를 입력한 후 알림 간격을 분 단위로 설정합니다. 시스템 상태 문제에 대한 알림이 전송된 후 알림 간격 시간이 경과하면 서비스 경고 알림이 트리거되고, 호스트 또는 서비스는 동일한 상태로 유지됩니다.
10 '보고서 요약' 필드에서 알림 보고서를 활성화하려면 원하는 간격(매일, 매주, 또는 매달)을 선택하고 스페이스바를 눌러 필드에 **X**를 입력합니다.
11 **확인**을 선택합니다.

기존 인증서 가져오기 또는 새 서버 인증서 등록

인증서가 제 위치에 있어야 DDP Enterprise Server - VE에 대해 사용자를 활성화할 수 있습니다.

기존 인증서를 가져오거나 DDP Enterprise Server - VE를 통해 인증서 요청을 생성할 수 있습니다.

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

기존 서버 인증서 가져오기

1 키 저장소에서 기존 인증서와 전체 신뢰 체인을 내보냅니다.

노트: 내보내기 암호는 인증서를 DDP Enterprise Server - VE로 가져올 때 입력해야 하므로 기록해 두십시오.

2 DDP Enterprise Server - VE의 FTP 서버에서 인증서를 **/opt/dell/vsftpd/files/certificates**에 저장합니다.

3 DDP Enterprise Server - VE *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.

4 **기존 인증서 가져오기**를 선택합니다.

5 DDP Enterprise Server - VE에 설치할 인증서 파일을 선택합니다.

6 메시지가 표시되면 인증서 내보내기 암호를 입력하고 **확인**을 선택합니다.

7 가져오기가 완료되면 **확인**을 선택합니다.

새 서버 인증서 등록

1 *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.

2 **새 서버 인증서**를 선택합니다.

3 **인증서 요청 생성**을 선택합니다.

4 *인증서 요청 생성* 화면에서 다음과 같은 필드를 입력합니다.

- 국가 이름: 2문자로 이루어진 국가 코드
- *시 또는 도*: 축약형이 아닌 시 또는 도의 전체 이름을 입력합니다(예: Texas).
- *지역 이름/구/군/시*. 적절한 값을 입력합니다(예: Dallas).
- *조직*: 적절한 값을 입력합니다(예: Dell).
- *부서*: 적절한 값을 입력합니다(예: 보안부).
- *일반 이름*: DDP Enterprise Server - VE가 설치되는 서버의 정규화된 도메인 이름을 입력합니다. 이 정규화된 이름에는 호스트 이름과 도메인 이름이 포함됩니다(예: server.domain.com).
- *이메일 ID*: CSR이 전송될 이메일 주소를 입력합니다.

5 조직이 인증 기관에서 SSL 서버 인증서를 취득하는 데 사용하는 절차를 따르십시오. 서명할 CSR 파일의 내용을 전송합니다.

6 서명된 인증서를 수신하면 인증서를 .p7b 파일로 내보내고 전체 신뢰 체인을 .der 형식으로 다운로드합니다.

7 인증서 및 신뢰 체인의 백업 사본을 만듭니다.

8 인증서 파일과 해당되는 전체 신뢰 체인을 DDP Enterprise Server - VE의 FTP 서버에 업로드합니다.

9 *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.

10 **새 서버 인증서**를 선택합니다.

11 인증서 등록 완료를 선택합니다.

12 DDP Enterprise Server - VE에 설치할 인증서 파일을 선택합니다.

13 메시지가 나타나면 인증서 암호를 입력합니다(**changeit**).

Windows 기반 Encryption 클라이언트에서 신뢰 유효성 검사를 사용하려면 "Manager 신뢰 체인 검사 사용"을 참조하십시오.

자체 서명 인증서 생성 및 설치

1 DDP Enterprise Server - VE *고급 구성* 메뉴에서 **서버 인증서**를 선택합니다.

2 **자체 서명 인증서 생성 및 설치**를 선택합니다.

3 사전 설치된 인증서를 새 인증서로 바꾸도록 확인하려면 **예**를 클릭합니다.

4 인증서 암호를 입력합니다(**changeit**).

5 새로운 인증서를 설치한 후 **확인**을 선택하고 서비스가 다시 시작되도록 기다립니다.

VE 서비스가 자동으로 다시 시작됩니다.

로그 회전 구성

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

기본적으로 매일 로그 회전을 사용하도록 설정되어 있습니다. 기본 로그 회전을 변경하려면 *고급 구성* 메뉴에서 **로그 회전 구성**을 선택합니다.

로그 회전을 사용하지 않으려면 스페이스바를 눌러 '회전 없음' 필드에 **X**를 입력하고 **확인**을 선택합니다.

로그 회전을 사용하도록 설정하려면 다음 단계를 따르십시오.

1 매일, 주별 또는 월별 회전을 사용하려면 스페이스바를 눌러 해당 필드에 **X**를 입력합니다. 주별 또는 월별 회전의 경우 해당 날짜 또는 요일을 숫자로 입력합니다(여기서, 월요일=1).
2 Logrotate 시간 필드에 회전 시간을 입력합니다.
3 **확인**을 선택합니다.

백업 및 복구

백업은 언제든지 구성하거나 수행할 수 있으며 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. Dell은 정규적인 백업 프로세스를 구성하도록 권장합니다.

백업은 외부 보안 FTP 서버(권장) 또는 DDP Enterprise Server - VE에 저장할 수 있습니다. VE 서버에 저장할 경우, 디스크 용량이 90%에 도달하면 새 백업이 저장되지 않습니다. 디스크 할당 공간이 부족하다는 이메일 알림이 수신됩니다.

노트:
디스크 파티션 공간을 보존하고 백업이 자동으로 삭제되지 않도록 하려면 DDP Enterprise Server - VE에서 불필요한 백업을 제거하십시오.

백업은 기본적으로 매일 실행됩니다. 조직에 필요한 백업 및 적절한 스토리지 공간 사용 요구사항에 따라 적절한 빈도로 외부 보안 FTP 서버에 백업을 저장할 것을 권장합니다.

백업 스케줄을 구성하려면, *고급 구성* 메뉴에서 **백업 및 복원 > 구성**을 선택하고 다음 단계를 따르십시오.

1 매일, 주별 또는 월별 백업을 사용하려면 스페이스바를 눌러 해당 필드에 **X**를 입력합니다. 주별 또는 월별 백업의 경우 해당 날짜 또는 요일을 숫자로 입력합니다(여기서, 월요일=1). 백업을 사용하지 않으려면 스페이스바를 눌러 '백업 없음' 필드에 **X**를 입력하고 **확인**을 선택합니다.
2 백업 시간 필드에 백업 시간을 입력합니다.
3 **확인**을 선택합니다.

백업을 즉시 수행하려면, *고급 구성* 메뉴에 **백업 및 복원 > 지금 백업**을 선택합니다. 백업 확인 메시지가 표시되면 **확인**을 선택합니다.

노트:
복원 작업을 시작하려면 먼저 모든 VE 서버 서비스를 실행해야 합니다. **서버 상태를 확인**합니다. 서비스가 모두 실행되고 있지 않은 경우 서비스를 다시 시작하십시오. 자세한 내용은 **VE 서비스 시작 또는 중지**를 참조하십시오. ***모든*** 서비스가 실행되는 ***경우에만*** 복원을 시작하십시오.

백업에서 복원하려면, *고급 구성* 메뉴에서 **백업 및 복원 > 복원**을 선택하고 복원할 백업 파일을 선택합니다. 확인 메시지가 나타나면 **예**를 선택합니다.

VE가 재부팅되고 백업이 복원됩니다.

보안 FTP 서버에 백업 저장

FTP 서버에 백업을 저장하려면 FTP 클라이언트가 포트 22에서 SFTP를 지원해야 합니다.

조직의 백업 요구사항에 따라 다음과 같은 방법으로 백업을 다운로드할 수 있습니다.

- 수동
- 자동화된 스크립트
- 조직의 승인된 백업 솔루션

조직의 백업 솔루션을 사용하여 백업을 다운로드하려면 백업 솔루션 벤더로부터 자세한 지침을 받으십시오.

노트:
Virtual Edition은 Linux Debian Ubuntu x64를 기반으로 합니다.

ddpsupport로 VE에 로그인하고 sudo 명령을 사용하여 백업 솔루션을 구성합니다.

`sudo` <백업 솔루션 벤더의 지침>

다음 폴더의 내용을 백업합니다.

/opt/dell/vsftpd/files/backup (필수)

/opt/dell/vsftpd/files/certificates (권장)

/opt/dell/vsftpd/files/support (선택)

sudo 프로세스가 완료되면 **exit**를 입력하고 로그인 프롬프트가 표시될 때까지 **Enter**를 누릅니다.

데이터베이스 원격 액세스 사용

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

노트: 데이터베이스 원격 액세스는 필요할 경우에만 사용하도록 설정하는 것이 좋습니다.

1 *고급 구성* 메뉴에서 **데이터베이스 원격 액세스**를 선택합니다.
2 스페이스바를 눌러 데이터베이스 원격 액세스 사용 필드에 **X**를 입력하고 **확인**을 선택합니다. 데이터베이스 암호를 아직 구성하지 않았다면 데이터베이스 암호 화면이 나타납니다.
3 데이터베이스 암호를 입력합니다.
4 데이터베이스 암호를 다시 입력합니다.
DDP 응용프로그램 구성요소가 자동으로 중지됩니다.

DMZ 서버 지원 사용

이 작업은 언제든지 완료할 수 있습니다. 즉, 이 작업을 수행하지 않아도 DDP Enterprise Server - VE를 사용할 수 있습니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 *고급 구성* 메뉴에서 **DMZ 서버 지원 사용**을 선택합니다.
2 스페이스바를 눌러 DMZ 서버 지원 사용 필드에 **X**를 입력하고 **확인**을 선택합니다.

노트: Proxy Mode(DMZ Mode)를 사용하려면 Proxy Mode를 설치하고 구성해야 합니다.

DDP Enterprise Server - VE 관리자 작업

DDP Enterprise Server - VE Terminal 언어 설정 또는 변경

설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.

1 주 메뉴에서 **언어 설정**을 선택합니다.
2 화살표 키를 사용하여 선호하는 언어를 선택합니다.

서버 상태 확인

DDP Enterprise Server - VE 서비스의 상태를 확인하려면, 주 메뉴에서 **서버 상태**를 선택합니다.

다음 표는 각 서비스 및 기능에 대한 설명입니다.

이름	설명
Dell Message Broker	Enterprise Server 버스
Dell Identity Server	도메인 인증 요청을 처리합니다.
Dell Compatibility Server	엔터프라이즈 아키텍처를 관리하는 서비스입니다.
Dell Security Server	Active Directory와의 통신 및 명령을 제어하는 메커니즘을 제공합니다. Dell Policy Proxy와의 통신에 사용됩니다.
Dell Compliance Reporter	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다.
Dell Core Server	엔터프라이즈 아키텍처를 관리하는 서비스입니다.
Dell Core Server HA (높은 가용성)	엔터프라이즈 아키텍처를 관리할 때 HTTPS 연결에 대한 보안과 성능을 향상시킨 높은 가용성의 서비스입니다.
Dell Inventory Server	인벤토리 대기열을 처리합니다.
Dell Forensic Server	Forensic API를 위한 웹 서비스를 제공합니다.
Dell Policy Proxy	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다.

DDP Enterprise Server - VE는 필요에 따라 서비스를 모니터하고 다시 시작합니다.

노트: 데이터베이스 사용자 지정 프로세스가 실패하면 서버가 실행 실패 상태로 전환됩니다. 데이터베이스 사용자 지정 로그를 확인하려면 주 메뉴에서 로그 보기를 선택합니다.

로그 보기

다음과 같은 로그를 확인하려면, 주 메뉴에서 **로그 보기**를 선택합니다.

Syslog 로그 메일 로그 Auth 로그(SSH) Postgres 로그 모니터 로그

- 시스템 로그

  Syslog 로그

  메일 로그

  Auth 로그(SSH)

  Postgres 로그

  모니터 로그
- 서버 로그

  Compatibility Server

  Security Server

  Message Broker

  Core Server

  Core Server HA

  Compliance Reporter

  Identity Server

  Inventory Server

  Forensic Server

  Policy Proxy
- Databasecustomizer 로그

명령줄 인터페이스 열기

명령줄 인터페이스를 열려면, 주 메뉴에서 **셸 실행**을 선택합니다.

명령줄 인터페이스를 종료하려면, **exit**를 입력하고 **Enter**를 누릅니다.

시스템 스냅샷 로그 생성

Dell ProSupport용 시스템 스냅샷 로그를 생성하려면, 주 메뉴에서 **지원 도구**를 선택합니다.

1 *지원 부서 도구* 메뉴에서 **시스템 스냅샷 로그 생성**을 선택합니다.
2 파일이 생성되었다는 메시지가 표시되면 **확인**을 선택합니다.
ddpsupport 사용자가 활성화되면, Dell ProSupport가 DDP Enterprise Server - VE SFTP 서버에서 로그를 검색할 수 있습니다. ddpsupport 사용자가 활성화되어 있지 않으면 Dell ProSupport에 문의하십시오. 자세한 내용은 Dell ProSupport에 문의를 참조하십시오.

4

DDP Enterprise Server - VE 유지 보수

불필요한 DDP Enterprise Server - VE 백업을 제거해야 합니다.

가장 최근의 백업 10개만 보존됩니다. 디스크 파티션 공간이 10퍼센트 이하인 경우 백업이 더 이상 저장되지 않습니다. 이러한 상태가 발생하면 디스크 할당 공간이 부족하다는 이메일 알림이 수신됩니다.

5

DDP Enterprise Server - VE 문제 해결

이메일 알림이 구성된 상태에서 오류가 발생하면 이메일 알림이 수신됩니다. 이메일 알림의 정보를 기준으로 다음 단계를 따르십시오.

1 해당 로그 파일을 확인합니다.
2 필요하면 서비스를 다시 시작합니다. 설정이 변경될 때마다 서비스를 다시 시작하는 것이 좋습니다.
3 시스템 스냅샷 로그를 생성합니다.
4 Dell ProSupport에 문의하십시오. 자세한 내용은 Dell ProSupport에 문의를 참조하십시오.

6

설치 후 구성 작업

설치 후 조직에서 사용하는 Dell Data Protection 솔루션을 바탕으로 환경의 일부 구성 요소를 구성해야 할 수 있습니다.

Data Guardian용 VE 구성

Data Guardian 지원을 위해 VE를 구성하려면, VE Remote Management Console에서 Cloud Protection 정책을 켜짐으로 설정합니다. Data Guardian Protected Office Documents 모드를 활성화하려면 Protected Office Documents 정책을 켜짐으로 설정합니다.

Data Guardian 클라이언트를 설치하는 지침은 *Enterprise Edition 고급 설치 안내서*, *Enterprise Edition 기본 설치 안내서* 또는 *Data Guardian사용 설명서*를 참조하십시오.

Mobile Edition용 EAS Management 설치 및 구성

Mobile Edition을 사용하려면 EAS Management를 설치하고 구성해야 합니다. Mobile Edition을 사용하지 않으려는 경우 이 절을 건너뛰십시오.

필수 조건

- EAS Mailbox Manager 서비스의 로그온 계정에는 Exchange ActiveSync 정책을 만들거나 수정하고, 사용자 사서함에 정책을 할당하며, ActiveSync 장치에 대한 정보를 쿼리할 권한이 있어야 합니다.
- 파일을 수정하고 서비스를 다시 시작하려면 EAS 구성 유틸리티를 관리자 권한으로 실행해야 합니다.
- DDP Enterprise Server - VE에 대한 네트워크 연결이 필요합니다.
- DDP Enterprise Server - VE의 호스트 이름이나 IP 주소를 확인해 두십시오.
- Exchange 환경을 호스팅하는 서버에 이미 MSMQ(Microsoft Message Queuing)가 설치/구성되어 있어야 합니다. 그렇지 않을 경우 Exchange 환경을 호스팅하는 서버에서 Windows Server 2008 또는 Windows Server 2008 R2에 MSMQ 4.0을 설치하십시오(http://msdn.microsoft.com/en-us/library/aa967729.aspx).

배포 프로세스 중

Exchange ActiveSync를 사용하여 Mobile Edition을 통해 모바일 장치를 관리하려면 Exchange Server 환경을 구성해야 합니다.

EAS Device Manager 설치

1 Mobile Edition 설치 미디어에서 EAS Management 폴더를 찾습니다. EAS Device Manager 폴더에서, setup.exe를 *Exchange Client Access Server*에 복사합니다.

2 **setup.exe**를 더블 클릭하여 설치를 시작합니다. 해당 환경에 *Exchange Client Access Server*가 둘 이상 있을 경우 각 서버에서 이 설치 프로그램을 실행하십시오.

3 설치할 언어를 선택하고 **확인**을 클릭합니다.

4 *시작* 화면이 표시되면 **다음**을 클릭합니다.

5 라이센스 계약을 읽고 약관에 동의한 후 **다음**을 클릭합니다.

6 **다음**을 클릭하여 EAS Device Manager를 기본 위치인 **C:\Inetpub\wwwroot\Dell\EAS Device Manager**에 설치합니다.

7 *설치 시작 준비* 화면에서 **설치**를 클릭합니다.

상태 창에 설치 진행률이 표시됩니다.

8 원하는 경우, 확인란을 선택하여 Windows 설치 프로그램 로그를 표시하고 **마침**을 클릭합니다.

EAS Mailbox Manager 설치

1 Mobile Edition 설치 미디어에서 EAS Management 폴더를 찾습니다. EAS Mailbox Manager 폴더에서 setup.exe를 *Exchange Mailbox Server*에 복사합니다.

2 **setup.exe**를 더블 클릭하여 설치를 시작합니다. 해당 환경에 *Exchange Mailbox Server*가 둘 이상 있을 경우 각 서버에서 이 설치 프로그램을 실행하십시오.

3 설치할 언어를 선택하고 **확인**을 클릭합니다.

4 *시작* 화면이 표시되면 **다음**을 클릭합니다.

5 라이센스 계약을 읽고 약관에 동의한 후 **다음**을 클릭합니다.

6 **다음**을 클릭하여 EAS Mailbox Manager를 기본 위치인 C:\Program Files\Dell\EAS Mailbox Manager\에 설치합니다.

7 *로그온 정보* 화면에서, 이 Service에 로그온할 사용자 계정의 자격 증명을 입력합니다.

   사용자 이름: DOMAIN\Username

   암호: 이 사용자 이름과 연관된 암호

   다음을 클릭합니다.

8 *설치 시작 준비* 화면에서 **설치**를 클릭합니다.

   상태 창에 설치 진행률이 표시됩니다.

9 원하는 경우, 확인란을 선택하여 Windows 설치 프로그램 로그를 표시하고 **마침**을 클릭합니다.

EAS 구성 유틸리티 사용

1 동일한 컴퓨터에서 **시작** > **Dell** > **EAS 구성 유틸리티** > **EAS 구성**으로 이동하여 EAS 구성 유틸리티를 실행합니다.

2 **설정**을 클릭하여 EAS Management 설정을 구성합니다.

3 다음 정보를 입력합니다.

   DDP Enterprise Server - VE 호스트 이름

   Dell Policy Proxy 폴링 간격(기본값은 1분)

   보고 전용 모드에서 EAS Device Manager를 실행하려면 확인란을 선택합니다(배포 중 권장 사항).

   > **노트:**
   > 보고 전용 모드에서는 알려지지 않은 장치/사용자가 Exchange ActiveSync에 액세스할 수 있도록 허용하지만 해당 트래픽을 계속 보고합니다. 배포가 정상적으로 완료되면 이 설정을 변경하여 보안을 강화할 수 있습니다.

   확인을 클릭합니다.

4 확인 메시지가 표시됩니다. **예**를 클릭하여 IIS 및 EAS Mailbox Manager 서비스를 다시 시작합니다.

5 완료되면 **끝내기**를 클릭합니다.

배포 프로세스 후

배포가 정상적으로 완료되고 보안을 강화할 준비가 되면 다음 단계를 따르십시오.

Exchange Mailbox 서버에서

1 **시작** > **Dell** > **EAS 구성 유틸리티** > **EAS 구성**으로 이동하여 EAS 구성 유틸리티를 실행합니다.

2 **설정**을 클릭하여 EAS Management 설정을 구성합니다.

3 다음 정보를 입력합니다.

   DDP Enterprise Server - VE 호스트 이름

   Dell Policy Proxy 폴링 간격(기본값은 1분)

EAS Device Manager를 보고 전용 모드로 실행하려면 확인란을 선택 취소합니다.

확인을 클릭합니다.

4 확인 메시지가 표시됩니다. **예**를 클릭하여 IIS 및 EAS Mailbox Manager 서비스를 다시 시작합니다.

5 완료되면 **끝내기**를 클릭합니다.

Manager 신뢰 체인 검사 사용

SED의 VE Server 또는 BitLocker Manager에 자체 서명 인증서가 사용되는 경우, 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 ***비활성화*** 상태로 유지해야 합니다. 클라이언트 컴퓨터에서 SSL/TLS 신뢰 유효성 검사를 활성화하기 전에 다음 조건을 충족시켜야 합니다.

- Entrust 또는 Verisign 등 루트 인증 기관이 서명한 인증서를 VE Server로 가져와야 합니다. 기존 인증서 가져오기 또는 새 서버 인증서 등록을 참조하십시오.
- 인증서의 전체 신뢰 체인은 클라이언트 컴퓨터의 KeyStore에 저장되어야 합니다.

SSL/TLS 신뢰 유효성을 활성화하려면 클라이언트 컴퓨터에서 다음 레지스트리 항목 값을 0으로 변경하십시오.

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):0

VE Remote Management Console 관리자 작업

Dell 관리자 역할 지정

1 Dell 관리자로 https://server.domain.com:8443/webui/에서 Remote Management Console에 로그인합니다. 기본 자격 증명은 **superadmin/changeit**입니다.
2 왼쪽 창에서 **채우기** > **도메인**을 클릭합니다.
3 사용자를 추가할 도메인을 클릭합니다.
4 도메인 세부 정보 페이지에서 **멤버** 탭을 클릭합니다.
5 **사용자 추가**를 클릭합니다.
6 일반 이름, UPN(Universal Principal Name) 또는 sAMAccountName 중에서 사용자 이름을 검색할 필터를 입력합니다. 와일드카드 문자는 *입니다.

엔터프라이즈 디렉토리 서버에서 모든 사용자마다 일반 이름, UPN(Universal Principal Name) 및 sAMAccountName이 정의되어 있어야 합니다. 사용자가 도메인 또는 그룹의 멤버이지만 Management의 도메인 또는 그룹 멤버 목록에 표시되지 않으면, 엔터프라이즈 디렉토리 서버에 해당 사용자에 대해 3개 이름 모두가 올바르게 정의되어 있는지 확인하십시오.

쿼리는 일치하는 항목을 찾을 때까지 자동으로 일반 이름, UPN, sAMAccount 이름순으로 검색합니다.

7 *디렉토리 사용자 목록*에서 도메인에 추가할 사용자를 선택합니다. 여러 사용자를 선택하려면 <Shift><클릭> 또는 <Ctrl><클릭>을 사용합니다.
8 **추가**를 클릭합니다.
9 메뉴 표시줄에서, 지정된 사용자의 **세부 정보 및 작업** 탭을 클릭합니다.
10 메뉴 표시줄을 스크롤하여 **관리자** 탭을 선택합니다.
11 이 사용자에 추가할 관리자 역할을 선택합니다.
12 **저장**을 클릭합니다.

Dell 관리자 역할로 로그인

1 Remote Management ConsoleEnterprise Server에서 로그아웃합니다.
2 Remote Management ConsoleEnterprise Server에 로그인하고 도메인 사용자 자격 증명으로 로그인합니다.

*Dell Data Protection AdminHelp*를 시작하려면 Remote Management Console 오른쪽 상단 모서리에 있는 "?"를 클릭합니다. *시작하기* 페이지가 표시됩니다. **도메인 추가**를 클릭합니다.

고객을 위해 기준 정책이 설정된 상태지만 다음과 같은 특정 요구 사항에 따라 수정이 필요할 수 있습니다(라이선스 및 권한에 따라 활성화 가능).

- Windows 컴퓨터 암호화
- 자체 암호화 드라이브가 포함된 컴퓨터 암호화
- Hardware Crypto Accelerator가 설치된 Windows 컴퓨터 암호화
- BitLocker 관리를 사용하지 않음
- 고급 위협 차단이 켜지지 않았습니다.
- 위협 차단이 활성화됨
- 외부 미디어를 암호화하지 않음
- 포트에 연결된 장치를 암호화하지 않음
- Data Guardian을 사용함
- Mobile Edition을 사용하지 않음

AdminHelp 주제 *정책 관리*에서 기술 그룹 및 정책 설명으로 가십시오.

정책 커밋

설치가 완료되면 정책을 커밋합니다.

설치 이후 또는 나중에 정책 수정이 저장된 이후에 정책을 커밋하려면 다음 단계를 수행합니다.

1 왼쪽 창에서 **관리** > **커밋**을 클릭합니다.
2 설명 필드에 변경에 대한 설명을 입력합니다.
3 **정책 커밋**을 클릭합니다.

8

솔루션 포트

다음 표는 각 구성요소와 그 기능에 대한 설명입니다.

이름	기본 포트	설명	필요한 분야
Compliance Reporter	HTTP(S)/8084	감사 및 준수 보고를 위한 환경을 포괄적으로 볼 수 있습니다. DDP Enterprise Server - VE의 구성 요소	보고
Remote Management Console	HTTPS/8443	전체 엔터프라이즈 배포를 위한 관리 콘솔 및 제어 센터입니다. DDP Enterprise Server - VE의 구성 요소	모두
Core Server	HTTPS/8888	정책 흐름, 라이선스 및 사전 부팅 인증을 위한 등록, SED 관리, BitLocker Manager, 위협 차단 및 고급 위협 차단을 관리합니다. Compliance Reporter 및 Remote Management Console을 통해 사용할 인벤토리 데이터를 처리합니다. 인증 데이터를 수집하고 보관합니다. 역할 기반 액세스를 관리합니다. DDP Enterprise Server - VE의 구성 요소	모두
Core Server HA (높은 가용성)	HTTPS/8888	높은 가용성 서비스가 Remote Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, 및 Advanced Threat Protection에 대한 HTTPS 연결의 증가된 보안 및 성능을 제공합니다. DDP Enterprise Server - VE의 구성 요소	모두
Security Server	HTTPS/8443	Policy Proxy와 통신합니다. 포렌직 키 검색, 클라이언트 활성화, Data Guardian 제품 및 SED-PBA 통신을 관리합니다. DDP Enterprise Server - VE의 구성 요소	모두
Compatibility Server	TCP/1099(폐쇄)	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이터를, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 이 서비스의 사용자 그룹에 기반하여 데이터를 처리합니다. DDP Enterprise Server - VE의 구성 요소	모두
Message Broker 서비스	TCP/61616 및 STOMP/61613(폐쇄 또는 DMZ용으로 구성된 경우 61613이 개방됨)	DDP Enterprise Server - VE의 서비스 간 통신을 처리합니다. Policy Proxy 큐에 대한 Compatibility Server가 생성한 정책 정보 단계입니다. DDP Enterprise Server - VE의 구성 요소	모두

이름	기본 포트	설명	필요한 분야
Identity Server	HTTPS/8445	SED Manager 인증을 포함한 도메인 인증 요구를 관리합니다. Active Directory 계정이 필요합니다. DDP Enterprise Server - VE의 구성 요소	모두
Forensic Server	HTTPS/8448	적절한 권한을 소유한 관리자가 Remote Management Console에서 데이터 잠금 해제 또는 복호화 작업을 위해 암호화 키를 가져올 수 있습니다. DDP Enterprise Server - VE의 구성 요소	Forensic API
Inventory Server	8887	인벤토리 대기열을 처리합니다. DDP Enterprise Server - VE의 구성 요소	모두
Policy Proxy	TCP/ 8000/8090	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다. DDP Enterprise Server - VE의 구성 요소	Mac용 Enterprise Edition Windows용 Enterprise Edition Mobile Edition
LDAP	389/636, 3268/3269 RPC - 135, 49125+	**포트 3268** - 이 포트는 특별히 글로벌 카탈로그에 대한 대상으로 지정된 쿼리에 사용됩니다. 포트 3268에 전송된 LDAP 요청을 사용하여 전체 포리스트에서 개체를 검색할 수 있습니다. 그러나 글로벌 카탈로그에 복제하도록 표시된 속성만 반환될 수 있습니다. 예를 들어, 이 속성이 글로벌 카탈로그에 복제되지 않으므로 포트 3268을 사용하여 사용자의 부서를 반환할 수 없습니다. **포트 389** - 이 포트는 로컬 도메인 컨트롤러에서 정보를 요청하는 데 사용됩니다. 포트 389에 전송된 LDAP 요청을 사용하여 글로벌 카탈로그의 홈 도메인 내에 속하는 개체만 검색할 수 있습니다. 그러나 요청하는 응용 프로그램에서 이러한 개체에 대한 속성을 모두 가져올 수 있습니다. 예를 들어, 포트 389에 대한 요청을 사용하여 사용자의 부서를 가져올 수 있습니다.	모두
클라이언트 인증	HTTPS/8449	클라이언트 서버가 DDP Enterprise Server - VE를 통해 인증하도록 허용합니다.	Server Encryption
콜백 신호	HTTP/8446	Data Guardian Protected Office 모드를 실행할 때 각각의 보호된 Office 파일에 콜백 신호를 삽입할 수 있습니다.	Data Guardian
고급 위협 방지	HTTPS/TCP/443	고급 위협 방지를 사용하는 경우 클라이언트 통신	고급 위협 방지
EAS Device Manager	N/A(해당 없음)	무선 기능을 가능하게 해줍니다. Exchange Client Access Server에 설치됩니다.	모바일 장치의 Exchange ActiveSync를 관리합니다.
EAS Mailbox Manager	N/A(해당 없음)	Exchange Mailbox Server에 설치되는 메일박스 에이전트입니다.	모바일 장치의 Exchange ActiveSync를 관리합니다.

NTP 시간 동기화: TCP 및 UDP/123(자세한 내용은 https://help.ubuntu.com/lts/serverguide/NTP.html 참조)