Getting Started

Dell Data Security Implementation Services

December 2023
Rev. A01

참고, 주의 및 경고

노트: 참고는 제품을 보다 효과적으로 사용하는 데 도움이 되는 중요한 정보를 나타냅니다.

주의: 주의는 잠재적 하드웨어 손상이나 데이터 손실을 나타내며, 문제를 방지하는 방법을 알려줍니다.

경고: 경고는 재산 피해, 개인 상해 또는 사망의 위험이 있음을 나타냅니다.

Contents

1

구현 단계

기본 구현 프로세스는 다음과 같은 단계로 구성됩니다.

- 시작 및 요건 검토 수행
- 사전 점검사항 - 초기 구현 또는 사전 점검사항 - 업그레이드/마이그레이션 완료
- 다음 중 ***하나*** 설치 또는 업그레이드/마이그레이션:
  - ***Security Management Server***
    - 중앙 집중식 디바이스 관리
    - 물리적 또는 가상화 환경에서 실행되는 Windows 기반 애플리케이션입니다.
  - ***Security Management Server Virtual***
    - 최대 3,500대 디바이스에 대한 중앙 집중식 관리
    - 가상화된 환경에서 실행

  Dell Server 설치/마이그레이션 지침은 *Security Management Server 설치 및 마이그레이션 가이드* 또는 *Security Management Server Virtual 퀵 스타트 및 설치 가이드*를 참조하십시오. 이 문서를 입수하려면 Dell Data Security Server 문서를 참조하십시오.

- 초기 정책 구성
  - ***Security Management Server*** - *Security Management Server 설치 및 마이그레이션 가이드*, *관리 작업*을 참조하십시오. support.dell.com, *AdminHelp* 및 Management Console에서 이용할 수 있습니다.
  - ***Security Management Server Virtual*** - *Security Management Server Virtual 퀵 스타트 및 설치 가이드*, *Management Console 관리 작업*(support.dell.com에서 이용 가능) 및 *AdminHelp*(Management Console에서 이용 가능)를 참조하십시오.
- 클라이언트 패키징

  클라이언트 요구 사항 및 소프트웨어 설치 지침을 보려면 배포에 따라 해당 문서를 선택합니다.

  - *Encryption Enterprise 기본 설치 가이드* 또는 *Encryption Enterprise 고급 설치 가이드*
  - *Endpoint Security Suite Enterprise 기본 설치 가이드* 또는 *Endpoint Security Suite Enterprise 고급 설치 가이드*
  - *Advanced Threat Prevention 관리자 가이드*
  - *Encryption Personal 설치 가이드*
  - *Mac용 Encryption Enterprise 관리자 가이드*
  - *Mac용 Endpoint Security Suite Enterprise 관리자 가이드*
  - 이 문서를 입수하려면 Dell Data Security 클라이언트 문서를 참조하십시오.
- Dell 보안 관리자 기본 정보 교육 참가
- 모범 사례 이행
- Dell Client Services를 이용한 파일럿 또는 개발 지원 조정

2

시작 및 요건 검토

설치에 앞서 기업 환경과 프로젝트의 비즈니스 및 기술적 목표를 정확히 이해하고 있어야만 Dell Data Security의 성공적인 구현을 통해 해당 목표를 달성할 수 있습니다. 따라서 기업의 전반적인 데이터 보안 요건을 정확하게 파악하고 있어야 합니다.

다음은 Dell Client Services 팀이 기업 환경과 요건을 이해하는 데 도움이 될 수 있는 몇 가지 주요 공통 질문입니다.

1. 기업의 업종은 무엇입니까(의료 등)?
2. 현재 규정 준수 요건은 무엇입니까(HIPAA/HITECH, PCI 등)?
3. 기업 규모는 어떻게 됩니까(사용자 수, 물리적인 위치 수 등)?
4. 배포하고자 하는 끝점 수는 몇 대입니까? 향후 끝점 수를 늘릴 계획이 있습니까?
5. 사용자가 로컬 관리자 권한을 갖고 있습니까?
6. 관리 및 암호화 필요가 있는 데이터나 장치(로컬 고정 디스크, USB 등)는 무엇입니까?
7. 어떤 제품을 배포할 생각입니까?
    - Encryption Enterprise
        - Encryption(DE 자격) - Windows Encryption, Server Encryption, Encryption External Media, SED Management, 전체 디스크 암호화, BitLocker Manager 및 Mac Encryption.
        - Encryption External Media
    - Endpoint Security Suite Enterprise
        - Advanced Threat Prevention - 선택 사항인 클라이언트 방화벽 및 웹 보호(ATP 권한 부여)를 사용하거나 사용하지 않음
        - Encryption(DE 자격) - Windows Encryption, Server Encryption, Encryption External Media, SED Management, 전체 디스크 암호화, BitLocker Manager 및 Mac Encryption.
        - Encryption External Media
8. 기업에서는 어떠한 유형의 사용자 연결을 지원합니까? 사용자 연결은 다음과 같은 유형이 있습니다.
    - 로컬 LAN 연결 전용
    - VPN 기반 및/또는 엔터프라이즈 무선 사용자
    - 원격/미접속 사용자(장기간 직접 또는 VPN을 통해 네트워크에 접속하지 않은 사용자)
    - 도메인에 속하지 않는 워크스테이션
9. 끝점에서 보호해야 할 데이터는 무엇입니까? 일반 사용자가 어떤 유형의 데이터를 끝점에 저장하고 있습니까?
10. 민감한 정보는 어떤 사용자 애플리케이션에 저장합니까? 애플리케이션 파일 형식은 무엇입니까?
11. 기업 환경에서 사용하는 도메인 수는 몇 개입니까? 범위 내에 암호화가 필요한 것은 몇 개입니까?
12. 암호화하려는 운영 체제 및 OS 버전은 무엇입니까?
13. 대안으로서 끝점에 구성해 놓은 부팅 파티션이 있습니까?
    a. 제조사 복구 파티션
    b. 이중 부팅 워크스테이션

클라이언트 문서

배포할 클라이언트의 설치 요구사항, 지원되는 OS 버전, 지원되는 자체 암호화 드라이브 및 지침을 보려면 아래 나열된 해당 문서를 참조하십시오.

Encryption Enterprise(Windows) - www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals에서 문서를 확인하십시오.

- *Encryption Enterprise 고급 설치 가이드* - 맞춤 구성된 설치용 고급 스위치 및 매개변수가 포함된 설치 가이드.
- *Dell Data Security Console 사용자 가이드* - 사용자를 위한 지침.

Encryption Enterprise(Mac) - www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals에서 *Mac용 Encryption Enterprise 관리자 가이드*를 참조하십시오. 설치 및 배포 지침이 포함되어 있습니다.

Endpoint Security Suite Enterprise(Windows) - www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals에서 다음 문서를 참조하십시오.

- *Endpoint Security Suite Enterprise 고급 설치 가이드* - 맞춤 구성된 설치용 고급 스위치 및 매개변수가 포함된 설치 가이드.
- *Endpoint Security Suite Enterprise Advanced Threat Prevention 퀵 스타트 가이드* - 정책 권장 사항, 위협 식별과 관리 및 문제 해결이 포함된 관리 지침.
- *Dell Data Security Console 사용자 가이드* - 사용자 지침.

Endpoint Security Suite Enterprise(Mac) - www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals에서 다음 문서를 보십시오.

- *Mac용 Endpoint Security Suite Enterprise 관리자 가이드* - 설치 가이드

지원되는 SED(Self-Encrypting Drive)에 대한 자세한 내용은 https://www.dell.com/support/article/us/en/04/sln296720을 참조하십시오.

서버 문서

배포할 Dell Server의 설치 요구사항, 지원되는 OS 버전, 구성을 보려면 아래 나열된 해당 문서를 참조하십시오.

Security Management Server

- 다음 주소에서 *Security Management Server 설치 및 마이그레이션 가이드*를 참조하십시오.

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

  또는

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

Security Management Server Virtual

- 다음 주소에서 *Security Management Server Virtual 퀵 스타트 및 설치 가이드*를 참조하십시오.

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

  또는

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

3

사전 점검사항 - 초기 구현

배포하는 Dell Server에 따라 Dell Encryption 또는 Endpoint Security Suite Enterprise 설치 전에 해당 점검사항에 따라 모든 구성 요소를 갖추었는지 확인하십시오.

- Security Management Server 점검사항
- Security Management Server Virtual 점검사항

Security Management Server 초기 구현 점검사항

Proof of Concept 환경이 완전히 제거되었습니까(해당되는 경우)?

☐	Dell과 설치 업무 이전에 Proof of Concept 데이터베이스 및 애플리케이션은 백업 후 제거되었습니다(동일 한 서버를 사용하는 경우). 제거 방법에 대한 자세한 내용은 https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us를 참조하십시오.
☐	Proof of Concept 테스트 단계에서 사용되는 프로덕션 엔드포인트은 복호화되었거나 주요 번들로 다운로드 되었습니다. 배포할 클라이언트에 대한 자세한 내용은 클라이언트 문서를 참조하십시오.

ⓘ **노트:**

모든 신규 구현은 새 데이터베이스를 비롯해 Encryption 또는 Endpoint Security Suite Enterprise 소프트웨어의 설치로 시작 되어야 합니다. Dell Client Services는 POC 환경에서는 신규 구현을 수행하지 않습니다. POC 단계에서 암호화된 엔드포인 트은 Dell의 설치 업무 이전에 모두 복호화 또는 재구축되어야 합니다.

서버가 필수 하드웨어 사양을 만족합니까?

☐	Dell Security Management Server 아키텍처 디자인을 참조하십시오.

서버가 필수 소프트웨어 사양을 만족합니까?

☐	Windows Server 2012 R2(Standard 또는 Datacenter), 2016(Standard 또는 Datacenter), Windows Server 2019(Standard 또는 Datacenter) 또는 Windows Server 2022(Standard 또는 Datacenter)가 설치되어 있습니다. 이러한 운영 체제는 물리적 또는 가상 하드웨어에 설치할 수 있습니다.
☐	Windows Installer 4.0 이상이 설치되어 있습니다.
☐	.NET Framework 4.6.1이 설치되어 있습니다.
☐	SQL Server 2012 또는 SQL Server 2016을 사용하는 경우, Microsoft SQL Native Client 2012가 설치되어 있습니다. 가능한 경우, SQL Native Client 2014를 사용할 수 있습니다. ⓘ **노트:** SQL Express는 Security Management Server의 프로덕션 배포가 지원되지 않습니다.
☐	Windows 방화벽이 비활성화되어 있거나, (인바운드) 포트 8000, 8050, 8081, 8888, 61613을 허용하도록 구성되어 있습니다.
☐	Security Management Server와 AD(Active Directory)의 연결은 포트 88, 135, 389, 443, 636, 3268, 3269, 49125+(RPC) (AD까지 인바운드)를 통해 가능합니다.
☐	C:\Program Files에 설치할 때 Windows Server 2012 R2에 설치하기 전에 UAC는 비활성화되어 있습니다. 서버를 재부팅해야만 변경 사항이 적용됩니다. (Windows 제어판 > 사용자 계정 참조).

	• Windows Server 2012 R2 - 설치 프로그램이 UAC를 비활성화합니다. • Windows Server 2016 R2 - 설치 프로그램이 UAC를 비활성화합니다. ⓘ **노트:** 설치 디렉토리에 대해 보호되는 디렉토리를 지정하지 않으면 UAC가 더 이상 사용되지 않습니다.

서비스 계정을 만들었습니까?

☐	AD에 대한 읽기 전용 액세스 권한의 서비스 계정(LDAP) - 기본 사용자/도메인 사용자 계정이면 충분합니다.
☐	서비스 계정에는 Security Management Server 애플리케이션 서버에 대해 로컬 관리자 권한이 있어야 합니다.
☐	데이터베이스에 대한 Windows 인증을 사용하려면, 시스템 관리자 권한이 있는 도메인 서비스 계정이 필요합니다. 사용자 계정은 DOMAIN\\Username 형식이어야 하며 SQL 서버 허가 기본 스키마: dbo 및 데이터베이스 역할 구성원: dbo_owner, public을 가지고 있어야 합니다.
☐	SQL 인증을 사용하려면 사용되는 SQL 계정에 SQL Server에 대한 시스템 관리자 권한이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 데이터베이스 역할 구성원: dbo_owner, public을 가지고 있어야 합니다.

소프트웨어가 다운로드되었습니까?

Dell 지원 웹사이트에서 다운로드합니다.

☐	Dell Data Security 클라이언트 소프트웨어 및 Security Management Server 다운로드는 아래 URL의 **드라이버 및 다운로드**에 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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research 또는 http://www.dell.com/support 제품 페이지에서 1. **드라이버 및 다운로드**를 선택합니다. 2. 운영 체제 목록에서, 다운로드하는 제품에 해당되는 운영 체제를 선택합니다. 예를 들어 Dell Enterprise Server를 다운로드하려면 **Windows Server 옵션 중 하나**를 선택합니다. 3. 해당 소프트웨어 제목 아래에서 **파일 다운로드**를 선택합니다.
☐	Encryption 또는 Endpoint Security Suite Enterprise를 이미지(on-the-box)로 구매한 경우에는 Dell Digital Delivery를 사용하여 소프트웨어를 타겟 컴퓨터에 전달할 수 있습니다.

또는

Dell Data Security 파일 전송 사이트(CFT)에서 소프트웨어를 다운로드하십시오.

☐	소프트웨어는 **소프트웨어 다운로드** 폴더의 https://ddpe.credant.com에 있습니다.

설치 키와 라이선스 파일이 있습니까?

☐	라이선스 키는 최초 이메일을 통해 FTP 자격 증명과 함께 제공됩니다. 고객 알림 이메일의 예를 참조하십시오. 이 키는 http://www.dell.com/support 및 https://ddpe.credant.com에서 애플리케이션 다운로드에도 포함되어 있습니다.
☐	라이선스 파일은 FTP 사이트의 **클라이언트 라이선스** 폴더에 있는 XML 파일입니다.

노트:

라이선스를 이미지(on-the-box)로 구매한 경우에는 라이선스 파일이 필요 없습니다. 새로운 Encryption Personal, Encryption Enterprise 또는 Endpoint Security Suite Enterprise 클라이언트를 활성화하면 Dell에서 권한이 자동으로 다운로드됩니다.

데이터베이스를 생성하였습니까?

☐	(선택 사항)지원되는 서버에 새 데이터베이스가 생성됩니다. *Security Management Server 설치 및 마이그레이션 가이드*의 요구 사항 및 아키텍처를 참조하십시오. Security Management Server 설치 프로그램이 설치 중 이미 데이터베이스가 생성되지 않은 경우 데이터베이스를 생성합니다.
☐	타겟 데이터베이스 사용자에게 **db_owner** 권한이 부여되었습니다.

Security Management Server 및/또는 내부 및 외부 트래픽에 대한 분할 DNS를 포함한 Policy Proxies에 대한 DNS 별칭이 생성되었습니까?

DNS 별칭은 확장성을 위해 생성하는 것이 좋습니다. 나중에 클라이언트 업데이트 없이도 서버를 비롯해 별도의 애플리케이션 구성요소를 추가할 수 있기 때문입니다.

☐	원한다면 DNS 별칭을 생성합니다. 권장하는 DNS 별칭: ● Security Management Server: dds.<domain.com> ● Front end Server: dds-fe.<domain.com>

노트:

분할 DNS는 내부적 및 외부적으로 동일한 DNS 이름의 사용자를 허용합니다. 즉, 내부적으로 dds.<domain.com>을 내부 c-name으로 제공하고 이를 Dell Security Management Server(백엔드)로 보낼 수 있으며 외부적으로 dds.<domain.com>의 레코드를 제공하고 프런트엔드 서버로 관련 포트(Security Management Server 포트 섹션 참조)를 전달합니다. Dell은 DNS Round-robin(라운드 로빈)이나 로드 밸런서를 사용하여 여러 프런트엔드(여러 개인 경우)에 로드를 분산시킬 수 있습니다.

SSL 인증 계획이 있습니까?

☐	Dell은 인증서 서명에 사용할 뿐만 아니라 기업 환경 내 모든 워크스테이션이 신뢰할 수 있는 내부 CA(Certificate Authority)가 있습니다. **그 밖에도** VeriSign 또는 Entrust 등의 공인 인증 기관을 통해 서명된 인증서를 구매할 계획을 갖고 있습니다. 공인 인증 기관을 사용할 경우에는 Dell Client Services 엔지니어에게 알려주십시오. 인증서는 공용 및 개인 키 서명을 포함한 전체 Chain of Trust(루트 및 중간 단계)를 포함합니다.
☐	인증서 요청의 SAN(Subject Alternate Name)은 Dell Server 설치에 사용되며 모든 서버에 주어진 모든 DNS 별칭과 일치합니다. 와일드 카드 또는 자체 서명된 인증서 요청에는 적용되지 않습니다.
☐	인증서는 .pfx 형식으로 생성됩니다.

Change Control 요구 사항을 Dell에게 알려주었습니까?

☐	Encryption 또는 Endpoint Security Suite Enterprise 설치에 필요한 Change Control의 특정 요구 사항은 설치 업무 이전에 Dell Client Services 팀에 제출하십시오. 애플리케이션 서버, 데이터베이스 및 클라이언트 워크스테이션의 변경 사항 역시 이러한 요구 사항에 포함됩니다.

테스트용 하드웨어가 준비되었습니까?

☐	3대 이상의 컴퓨터에 기업 컴퓨터 이미지를 저장하여 테스트 용도로 준비하십시오. Dell은 운영 컴퓨터는 테스트 용도로 **사용하지 말 것**을 권장합니다. 운영 컴퓨터는 암호화 정책을 정의하고 Dell이 제공하는 테스트 플랜에 따라 테스트를 실시한 후 프로덕션 파일럿 단계에서 사용해야 합니다.

Security Management Server Virtual 초기 구현 점검사항

Proof of Concept 환경이 완전히 제거되었습니까(해당되는 경우)?

☐	Dell과 설치 업무 이전에 Proof of Concept 데이터베이스 및 애플리케이션은 백업 후 제거되었습니다(동일한 서버를 사용하는 경우). 제거 방법에 대한 자세한 내용은 다음을 참조하십시오. https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us
☐	Proof of Concept 테스트 단계에서 사용되는 프로덕션 엔드포인트은 복호화되었거나 주요 번들로 다운로드되었습니다. 배포할 클라이언트에 대한 자세한 내용은 클라이언트 문서를 참조하십시오.

노트:

모든 신규 구현은 새 데이터베이스를 비롯해 Encryption 또는 Endpoint Security Suite Enterprise 소프트웨어의 설치로 시작되어야 합니다. Dell Client Services는 POC 환경에서는 신규 구현을 수행하지 않습니다. POC 단계에서 암호화된 엔드포인트은 Dell의 설치 업무 이전에 모두 복호화 또는 재구축되어야 합니다.

서비스 계정을 만들었습니까?

☐	AD에 대한 읽기 전용 액세스 권한의 서비스 계정(LDAP) - 기본 사용자/도메인 사용자 계정이면 충분합니다.

소프트웨어가 다운로드되었습니까?

<table>
<tr><td>☐</td><td>Dell Data Security 클라이언트 소프트웨어 및 Security Management Server 다운로드는 아래 URL의 드라이버 및 다운로드에 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/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

또는

http://www.dell.com/support 제품 페이지에서

1. 드라이버 및 다운로드를 선택합니다.
2. 운영 체제 목록에서, 다운로드하는 제품에 해당되는 운영 체제를 선택합니다. 예를 들어 Dell Enterprise Server를 다운로드하려면 Windows Server 옵션 중 하나를 선택합니다.
3. 해당 소프트웨어 제목 아래에서 파일 다운로드를 선택합니다.</td></tr>
<tr><td>☐</td><td>Encryption 또는 Endpoint Security Suite Enterprise를 이미지(on-the-box)로 구매한 경우에는 Dell Digital Delivery를 사용하여 소프트웨어를 타겟 컴퓨터에 전달할 수 있습니다.</td></tr>
</table>

라이선스 파일이 있습니까?

☐	라이선스 파일은 ddpe.credant.com 사이트의 **Client Licenses** 폴더에 저장된 XML 파일입니다.

노트:

라이선스를 이미지(on-the-box)로 구매한 경우에는 라이선스 파일이 필요 없습니다. 새로운 Encryption 또는 Endpoint Security Suite Enterprise 클라이언트를 활성화하면 Dell에서 권한이 자동으로 다운로드됩니다.

서버가 필수 하드웨어 사양을 만족합니까?

◻	Security Management Server Virtual 아키텍처 디자인을 참조하십시오.

Security Management Server Virtual 및/또는 내부 및 외부 트래픽에 대한 분할 DNS를 포함한 Policy Proxies에 대한 DNS 별칭이 생성되었습니까?

DNS 별칭은 확장성을 위해 생성하는 것이 좋습니다. 나중에 클라이언트 업데이트 없이도 서버를 비롯해 별도의 애플리케이션 구성요소를 추가할 수 있기 때문입니다.

<table>
<tr><td>◻</td><td>원한다면 DNS 별칭을 생성합니다. 권장하는 DNS 별칭:
Security Management Server: dds.<domain.com>
Front end Server: dds-fe.<domain.com></td></tr>
</table>

노트:

분할 DNS는 내부적 및 외부적으로 동일한 DNS 이름의 사용자를 허용합니다. 즉, 내부적으로 dds.<domain.com>을 내부 c-name으로 제공하고 이를 Dell Security Management Server(백엔드)로 보낼 수 있으며 외부적으로 dds.<domain.com>의 레코드를 제공하고 프런트엔드 서버로 관련 포트(Security Management Server Virtual 포트 섹션 참조)를 전달합니다. Dell은 DNS Round-robin(라운드 로빈)이나 로드 밸런서를 사용하여 여러 프런트엔드(여러 개인 경우)에 로드를 분산시킬 수 있습니다.

SSL 인증 계획이 있습니까?

◻	Dell은 인증서 서명에 사용할 뿐만 아니라 기업 환경 내 모든 워크스테이션이 신뢰할 수 있는 내부 CA(Certificate Authority)가 있습니다. **그 밖에도** VeriSign 또는 Entrust 등의 공인 인증 기관을 통해 서명된 인증서를 구매할 계획을 갖고 있습니다. 공인 인증 기관을 사용할 경우에는 Dell Client Services 엔지니어에게 알려주십시오.

Change Control 요구 사항을 Dell에게 알려주었습니까?

◻	Encryption 또는 Endpoint Security Suite Enterprise 설치에 필요한 Change Control의 특정 요구 사항은 설치 업무 이전에 Dell Client Services 팀에 제출하십시오. 애플리케이션 서버, 데이터베이스 및 클라이언트 워크스테이션의 변경 사항 역시 이러한 요구 사항에 포함됩니다.

테스트용 하드웨어가 준비되었습니까?

◻	3대 이상의 컴퓨터에 기업 컴퓨터 이미지를 저장하여 테스트 용도로 준비하십시오. Dell은 운영 컴퓨터는 테스트 용도로 **사용하지 말 것**을 권장합니다. 운영 컴퓨터는 암호화 정책을 정의하고 Dell이 제공하는 테스트 플랜에 따라 테스트를 실시한 후 프로덕션 파일럿 단계에서 사용해야 합니다.

4

사전 체크리스트 - 업그레이드/마이그레이션

이 체크리스트는 Security Management Server에만 적용됩니다.

노트:

Dell Server 터미널의 기본 구성 메뉴에서 Security Management Server Virtual를 업데이트합니다. 자세한 내용은 *Security Management Server Virtual 빠른 시작 및 설치 가이드*를 참조하십시오.

Encryption 또는 Endpoint Security Suite Enterprise의 업그레이드를 시작하기 전에 다음과 같은 체크리스트를 사용하여 모든 필수 요소를 만족하였는지를 확인합니다.

서버가 필수 소프트웨어 사양을 만족합니까?

☐	Windows Server 2012 R2(Standard 또는 Datacenter), Windows Server 2016(Standard 또는 Datacenter), Windows Server 2019(Standard 또는 Datacenter), 또는 Windows Server 2022(Standard 또는 Datacenter)가 설치되어 있습니다. 또는 가상화된 환경을 설치할 수도 있습니다. **노트:** Dell Server v11.0 이상으로 업데이트하려면 Windows Server 2019 이상이 필요합니다.
☐	Windows Installer 4.0 이상이 설치되어 있습니다.
☐	.NET Framework 4.6.1이 설치되어 있습니다.
☐	SQL Server 2012 또는 SQL Server 2016을 사용하는 경우, Microsoft SQL Native Client 2012가 설치되어 있습니다. 가능한 경우, SQL Native Client 2014를 사용할 수 있습니다. **노트:** SQL Express는 Security Management Server가 지원되지 않습니다.
☐	Windows 방화벽이 비활성화되어 있거나, (인바운드) 포트 8000, 8050, 8081, 8443, 8888, 61613을 허용하도록 구성되어 있습니다.
☐	Security Management Server와 AD(Active Directory)의 연결은 포트 88, 135, 389, 443, 636, 3268, 3269, 49125+(RPC) (AD까지 인바운드)를 통해 가능합니다.
☐	C:\Program Files에 설치할 때 Windows Server 2012 R2에 설치하기 전에 UAC는 비활성화되어 있습니다. 서버를 재부팅해야만 변경 사항이 적용됩니다. (Windows 제어판 > 사용자 계정 참조). ● Windows Server 2012 R2 - 설치 프로그램이 UAC를 비활성화합니다. ● Windows Server 2016 R2 - 설치 프로그램이 UAC를 비활성화합니다.

서비스 계정을 만들었습니까?

☐	AD에 대한 읽기 전용 액세스 권한의 서비스 계정(LDAP) - 기본 사용자/도메인 사용자 계정이면 충분합니다.
☐	서비스 계정에는 Security Management Server 애플리케이션 서버에 대해 로컬 관리자 권한이 있어야 합니다.
☐	데이터베이스에 대한 Windows 인증을 사용하려면, 시스템 관리자 권한이 있는 도메인 서비스 계정이 필요합니다. 사용자 계정은 DOMAIN\\Username 형식이어야 하며 SQL 서버 허가 기본 스키마: dbo 및 데이터베이스 역할 구성원: dbo_owner, public을 가지고 있어야 합니다.
☐	SQL 인증을 사용하려면 사용되는 SQL 계정에 SQL Server에 대한 시스템 관리자 권한이 있어야 합니다. 사용자 계정은 SQL 서버 허가 기본 스키마: dbo 및 데이터베이스 역할 구성원: dbo_owner, public을 가지고 있어야 합니다.

데이터베이스와 모든 필요한 파일이 백업됩니까?

☐	기존의 모든 설치가 대체 위치에 백업됩니다. 백업해야 할 항목은 SQL 데이터베이스, secretKeyStore, 구성 파일입니다.
☐	데이터베이스에 연결하는데 필요한 정보가 저장되어 있는 이러한 대부분의 중요 파일이 백업되어 있는지 확인합니다. <설치 폴더>\Enterprise Edition\Compatibility Server\conf\server_config.xml <설치 폴더>\Enterprise Edition\Compatibility Server\conf\secretKeyStore <설치 폴더>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

설치 키와 라이선스 파일이 있습니까?

☐	라이선스 키는 최초 이메일을 통해 CFT 자격 증명과 함께 제공됩니다. 고객 알림 이메일의 예를 참조하십시오. 이 키는 http://www.dell.com/support 및 https://ddpe.credant.com에서 애플리케이션 다운로드에도 포함되어 있습니다.
☐	라이선스 파일은 CFT 사이트의 **클라이언트 라이선스** 폴더에 있는 XML 파일입니다.

노트:

라이선스를 이미지(on-the-box)로 구매한 경우에는 라이선스 파일이 필요 없습니다. 새로운 Encryption 또는 Endpoint Security Suite Enterprise 클라이언트를 활성화하면 Dell에서 권한이 자동으로 다운로드됩니다.

새로운 또는 기존의 Dell Data Security 소프트웨어가 다운로드 되나요?

Dell Data Security 파일 전송 사이트(CFT)에서 소프트웨어를 다운로드하십시오.

☐	소프트웨어는 **소프트웨어 다운로드** 폴더의 https://ddpe.credant.com에 있습니다.
☐	Encryption Enterprise 또는 Endpoint Security Suite Enterprise를 이미지(on-the-box, OTB)로 구매한 경우에는 소프트웨어가 Dell Digital Delivery를 사용하여 선택적으로 수행됩니다. 또는, 각각 www.dell.com/support 또는 ddpe.credant.com에서 소프트웨어를 다운로드할 수 있습니다.

엔드포인트 라이선스가 충분합니까?

업그레이드 이전에 기업 환경 내 모든 엔드포인트에 적용할 만큼 클라이언트 라이선스 수가 충분한지 확인하십시오. 현재 설치 수가 라이선스 수를 초과할 경우에는 업그레이드 또는 마이그레이션 전에 Dell 영업 담당자에게 문의하십시오. Dell Data Security는 라이선스 유효성 검사를 실행하여 라이선스가 부족한 경우에는 활성화가 진행되지 않습니다.

☐	기업 환경에 적용할 만큼 라이선스 수가 충분합니다.

DNS 레코드가 문서화되어 있습니까?

☐	하드웨어가 변경된 경우 DNS 레코드가 문서화되고 업데이트용으로 스테이징되는지 확인합니다.

SSL 인증 계획이 있습니까?

☐	Dell은 인증서 서명에 사용할 뿐만 아니라 기업 환경 내 모든 워크스테이션이 신뢰할 수 있는 내부 CA(Certificate Authority)가 있습니다. **그 밖에도** VeriSign 또는 Entrust 등의 공인 인증 기관을 통해 서명된 인증서를 구매할 계획을 갖고 있습니다. 공인 인증 기관을 사용할 경우에는 Dell Client Services 엔지니어에게 알려주십시오. 인증서는 공용 및 개인 키 서명을 포함한 전체 Chain of Trust(루트 및 중간 단계)를 포함합니다.
☐	인증서 요청의 SAN(Subject Alternate Name)은 Dell Enterprise Server 설치에 사용되며 모든 서버에 주어진 모든 DNS 별칭과 일치합니다. 와일드 카드 또는 자체 서명된 인증서 요청에는 적용되지 않습니다.
☐	인증서는 .pfx 형식으로 생성됩니다.

Change Control 요구 사항을 Dell에게 알려주었습니까?

☐	Encryption 또는 Endpoint Security Suite Enterprise 설치에 필요한 Change Control의 특정 요구 사항은 설치 업무 이전에 Dell Client Services 팀에 제출하십시오. 애플리케이션 서버, 데이터베이스 및 클라이언트 워크스테이션의 변경 사항 역시 이러한 요구 사항에 포함됩니다.

테스트용 하드웨어가 준비되었습니까?

☐	3대 이상의 컴퓨터에 기업 컴퓨터 이미지를 저장하여 테스트 용도로 준비하십시오. Dell은 운영 컴퓨터는 테스트 용도로 **사용하지 말 것**을 권장합니다. 운영 컴퓨터는 암호화 정책을 정의하고 Dell이 제공하는 테스트 플랜에 따라 테스트를 실시한 후 프로덕션 파일럿 단계에서 사용해야 합니다.

5

아키텍처

이 섹션에서는 Dell Data Security 구현을 위한 아키텍처 디자인 권장사항에 대해 자세히 설명합니다. 배포할 Dell Server를 선택하십시오.

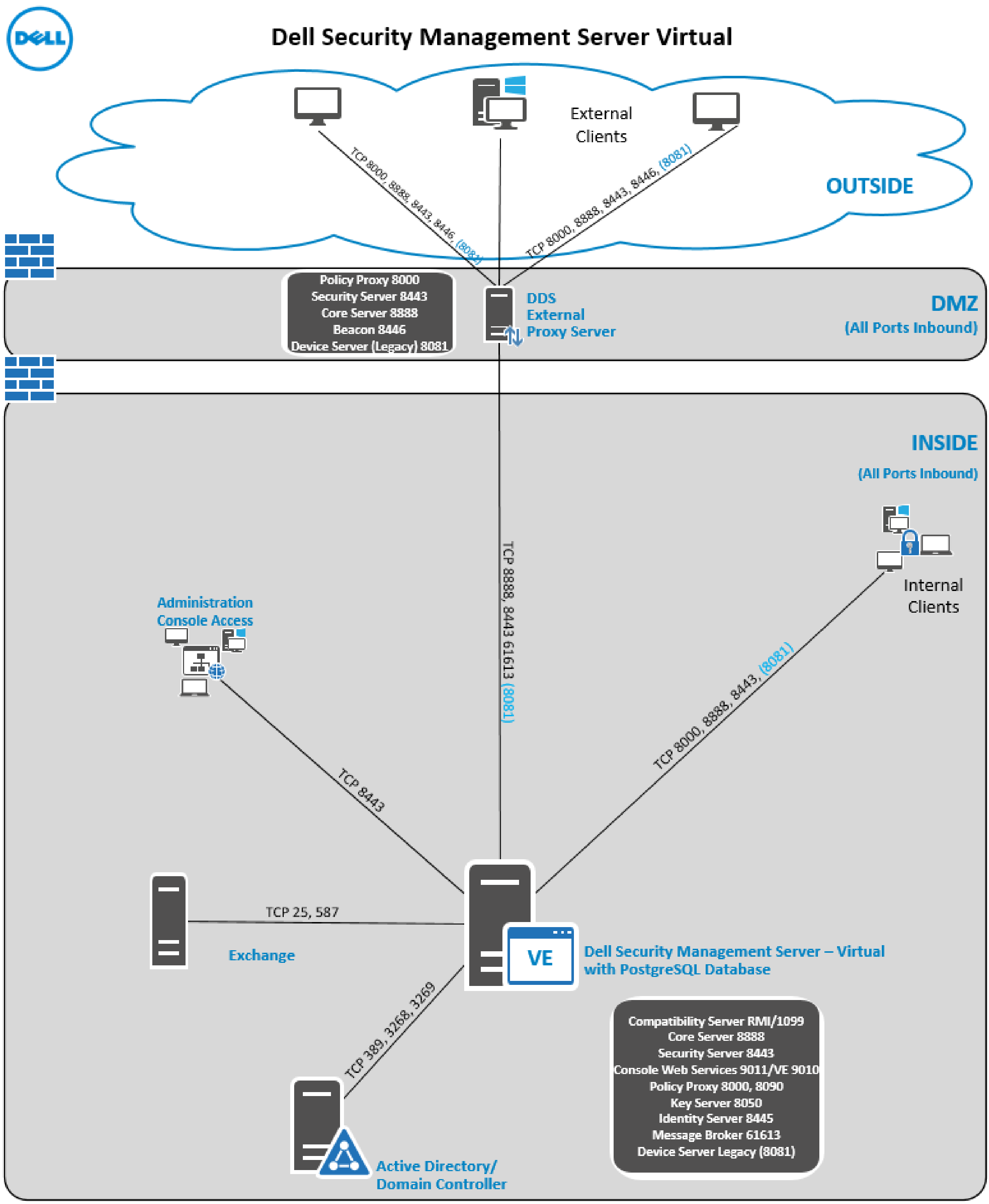
- Security Management Server 아키텍처 디자인
- Security Management Server Virtual 아키텍처 디자인

Security Management Server Virtual 아키텍처 디자인

Encryption Enterprise 및 Endpoint Security Suite Enterprise 솔루션은 확장성이 뛰어난 제품으로서, 조직이 암호화할 엔드포인트 수를 기반으로 합니다.

아키텍처 구성 요소

아래는 Dell Security Management Server Virtual의 Basic Deployment입니다.



포트

다음 표는 각 구성 요소와 그 기능에 대한 설명입니다.

이름	기본 포트	설명
액세스 그룹 서비스	TCP/ 8006	여러 Dell 보안 제품에 대한 다양한 권한과 그룹 액세스를 관리합니다. **노트:** 포트 8006은 현재 보안되지 않습니다. 이 포트가 방화벽을 통해 올바르게 필터링되었는지 확인합니다. 이 포트는 내부 전용입니다.
Management Console	HTTPS/ 8443	전체 Enterprise Deployment를 위한 관리 콘솔 및 제어 센터입니다.
Core Server	HTTPS/ 8887(폐쇄)	정책 흐름, 라이선스 및 사전 부팅 인증을 위한 등록, SED Management, BitLocker Manager, 위협 차단 및 Advanced Threat Prevention을 관리합니다. Management Console을 통해 사용할 인벤토리 데이터를 처리합니다. 인증 데이터를 수집하고 보관합니다. 역할 기반 액세스를 관리합니다.
Core Server HA (고가용성)	HTTPS/ 8888	높은 가용성 서비스가 Management Console, Preboot Authentication, SED Management, BitLocker Manager, Threat Protection, 및 Advanced Threat Prevention에 대한 HTTPS 연결의 증가된 보안 및 성능을 제공합니다.
Security Server	HTTPS/ 8443	포렌식 키 검색, 클라이언트 활성화, SED-PBA 및 전체 디스크 암호화-PBA 통신을 관리하는 Policy Proxy와 통신합니다.
Compatibility Server	TCP/ 1099(폐쇄)	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이터를, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 사용자 그룹에 기반하여 데이터를 처리합니다. **노트:** 포트 1099는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다.
Message Broker 서비스	TCP/ 61616(폐쇄) 및 STOMP/ 61613(폐쇄됨 또는 DMZ에 구성된 경우 61613 개방됨)	Dell Server의 서비스 간 통신을 처리합니다. Policy Proxy 큐에 대한 Compatibility Server가 생성한 정책 정보 단계입니다. **노트:** 포트 61616는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다. **노트:** 포트 61613은 프런트엔드 모드로 구성된 Security Management Server에서만 열어야 합니다.
Identity Server	8445(폐쇄)	SED Management 인증을 포함한 도메인 인증 요구를 관리합니다.

이름	기본 포트	설명
Forensic Server	HTTPS/ 8448	적절한 권한을 소유한 관리자가 Management Console에서 데이터 잠금 해제 또는 복호화 작업을 위해 암호화 키를 가져올 수 있습니다. Forensic API에 필요함.
Inventory Server	8887	인벤토리 대기열을 처리합니다.
Policy Proxy	TCP/ 8000	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다. Encryption Enterprise(Windows 및 Mac)에 필요함
PostGres	TCP/ 5432	이벤트 데이터에 사용되는 로컬 데이터베이스입니다. **노트:** 포트 5432는 방화벽을 통해 필터링되어야 합니다. Dell은 이 포트를 내부용으로만 사용할 것을 권장합니다.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	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 애플리케이션에서 이러한 개체에 대한 속성을 모두 가져올 수 있습니다. 예를 들어, 포트 389에 대한 요청을 사용하여 사용자의 부서를 가져올 수 있습니다. 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.
클라이언트 인증	HTTPS/ 8449	클라이언트 서버가 Dell Server를 통해 인증하도록 허용합니다. Server Encryption에 필요함.

Security Management Server 아키텍처 디자인

Encryption Enterprise 및 Endpoint Security Suite Enterprise 솔루션은 확장성이 뛰어난 제품으로서, 조직이 암호화할 엔드포인트 수를 기반으로 합니다.

아키텍처 구성 요소

아래에 환경에 가장 적합한 하드웨어 구성이 제시되어 있습니다.

Security Management Server

- 운영 체제: Windows Server 2012 R2(Standard, Datacenter 64비트), Windows Server 2016(Standard, Datacenter 64비트), Windows Server 2019(Standard, Datacenter), Windows Server 2022(Standard 또는 Datacenter)
- 가상 또는 물리적 시스템
- CPU: 4개 코어
- RAM: 16.00GB
- 드라이브 C: 로그 및 애플리케이션 데이터베이스를 위한 30GB의 사용 가능한 디스크 공간

  노트: PostgreSQL 내에 저장된 로컬 이벤트 데이터베이스에 최대 10GB의 용량이 사용될 수 있습니다.

프록시 서버

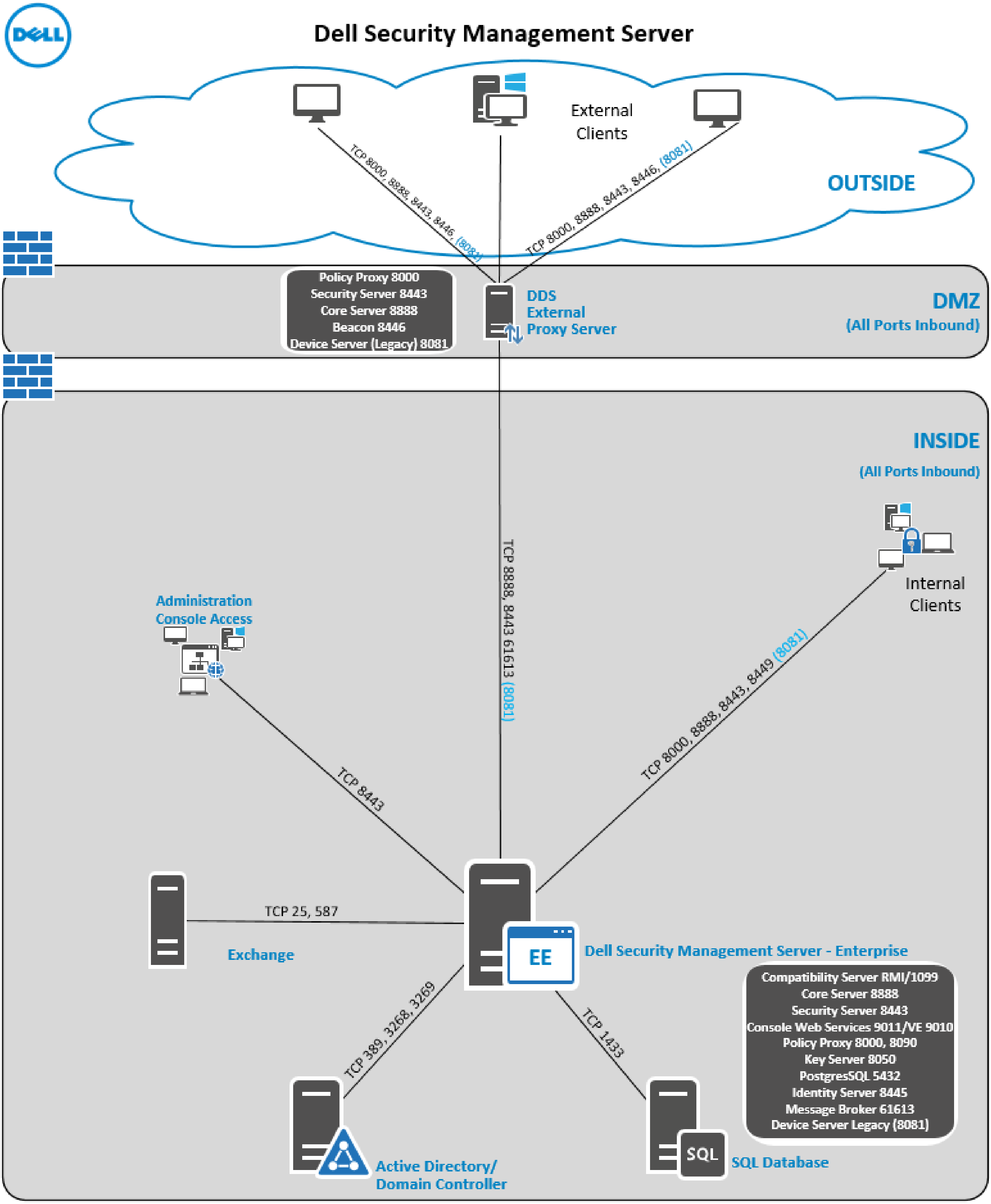
- 운영 체제: Windows Server 2012 R2(Standard, Datacenter 64비트), Windows Server 2016(Standard, Datacenter 64비트), Windows Server 2019(Standard, Datacenter), Windows Server 2022(Standard 또는 Datacenter)
- 가상/ 또는 머신
- CPU: 2개 코어
- RAM: 8.00GB
- 드라이브 C: 로그를 위한 20GB의 사용 가능한 디스크 공간

SQL Server 하드웨어 스펙

- CPU: 4개 코어
- RAM: 24.00GB
- 데이터 드라이브: 100~150GB의 사용 가능한 디스크 공간(이 수치는 환경에 따라 달라질 수 있음)
- 로그 드라이브: 50GB의 사용 가능한 디스크 공간(이 수치는 환경에 따라 달라질 수 있음)

  노트: 위의 정보가 대부분의 환경을 포함하지만 Dell Technologies는 SQL Server 모범 사례를 따르는 것을 권장합니다.

아래는 Dell Security Management Server의 Basic Deployment입니다.



노트: 조직의 엔드포인트 수가 20,000개 이상일 경우에는 Dell ProSupport에 문의하십시오.

포트

다음 표는 각 구성 요소와 그 기능에 대한 설명입니다.

이름	기본 포트	설명
ACL 서비스	TCP/ 8006	여러 Dell 보안 제품에 대한 다양한 권한과 그룹 액세스를 관리합니다. **노트:** 포트 8006에는 보안이 설정되어 있지 않습니다. 이 포트가 방화벽을 통해 올바르게 필터링되는지 확인합니다. 이 포트는 내부 전용입니다.
Management Console	HTTP(S)/ 8443	전체 Enterprise Deployment를 위한 관리 콘솔 및 제어 센터입니다.
Core Server	HTTPS/ 8888	정책 흐름, 라이선스 및 사전 부팅 인증을 위한 등록, SED Management, BitLocker Manager, 위협 차단 및 Advanced Threat Prevention을 관리합니다. Management Console을 통해 사용할 인벤토리 데이터를 처리합니다. 인증 데이터를 수집하고 보관합니다. 역할 기반 액세스를 관리합니다.
Device Server	HTTPS/ 8081	활성화 및 비밀번호 복구를 지원합니다. Security Management Server의 구성 요소입니다. Encryption Enterprise(Windows 및 Mac)에 필요함
Security Server	HTTPS/ 8443	포렌식 키 검색, 클라이언트 활성화, SED-PBA 및 전체 디스크 암호화-PBA 통신을 관리하는 Policy Proxy 및 인증 또는 조정을 위한 Active Directory와 통신합니다. 여기에는 Management Console에 대한 인증을 위한 ID 유효성 검사가 포함됩니다. SQL 데이터베이스 액세스가 필요합니다.
Compatibility Server	TCP/ 1099	엔터프라이즈 아키텍처를 관리하는 서비스입니다. 활성화 도중 초기 인벤토리 데이터를, 그리고 마이그레이션 중 정책 데이터를 수집하고 보관합니다. 사용자 그룹에 기반하여 데이터를 처리합니다. **노트:** 포트 1099는 방화벽을 통해 필터링되어야 합니다. Dell Technologies는 이 포트를 내부용으로만 사용할 것을 권장합니다.
Message Broker 서비스	TCP/ 61616 및 STOMP/	Dell Server의 서비스 간 통신을 처리합니다. Compatibility Server가 정책 프록시 대기열을 위해 만드는 정책 정보를 스테이징합니다.

이름	기본 포트	설명
	61613	SQL 데이터베이스 액세스가 필요합니다. **노트:** 포트 61616는 방화벽을 통해 필터링되어야 합니다. Dell Technologies는 이 포트를 내부용으로만 사용할 것을 권장합니다. **노트:** 프론트엔드 모드로 구성된 보안 관리 서버에 대해 포트 61613만 엽니다.
Key Server	TCP/ 8050	Kerberos API를 사용하여 클라이언트 연결을 협상, 인증 및 암호화합니다. 주요 데이터를 가져오기 위해 SQL 데이터베이스 액세스가 필요합니다.
Policy Proxy	TCP/ 8000	네트워크 기반 통신 경로를 제공하여 보안 정책 업데이트 및 인벤토리 업데이트를 제공합니다.
PostGres	TCP/ 5432	이벤트 데이터에 사용되는 로컬 데이터베이스입니다. **노트:** 포트 5432는 방화벽을 통해 필터링되어야 합니다. Dell Technologies는 이 포트를 내부용으로만 사용할 것을 권장합니다.
LDAP	TCP/ 389/636(로컬 도메인 컨트롤러), 3268/3269(글로벌 카탈로그) TCP/ 135/ 49125+ (RPC)	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 애플리케이션은 이러한 개체에 대한 속성을 모두 가져올 수 있습니다. 예를 들어, 포트 389에 대한 요청을 사용하여 사용자의 부서를 가져올 수 있습니다. 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.
Microsoft SQL 데이터베이스	TCP/ 1433	기본 SQL Server 포트는 1433이며, 클라이언트 포트에는 1024 ~ 5000 범위 내의 임의 값이 할당됩니다.
클라이언트 인증	HTTPS/ 8449	클라이언트 서버가 Dell Server를 통해 인증하도록 허용합니다. Server Encryption에 필요합니다.

6

SQL Server 모범 사례

다음 목록은 SQL Server 모범 사례로서 Dell Security 설치 시 구현하지 않았다면 반드시 구현해야 합니다.

1. 데이터 파일 및 로그 파일이 저장되는 NTFS 블록 크기가 64KB인지 확인하십시오. SQL Server 익스텐트(SQL Storage 기본 단위)는 64KB입니다.

   자세한 내용은 Microsoft의 TechNet 게시글에서 “페이지 및 익스텐트에 대한 이해”를 검색하여 확인하시기 바랍니다.
2. 일반 지침으로서 SQL Server 메모리의 최대 용량을 설치된 메모리의 80%로 설정하십시오.

   자세한 내용은 Microsoft의 TechNet 게시글에서 *서버 메모리 서버 구성 옵션*을 검색하여 확인하시기 바랍니다.

   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
   - Microsoft SQL Server 2017 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)
3. 교착 상태 발생 시 관련 정보를 수집할 수 있도록 인스턴스 시작 속성에서 -t1222를 설정합니다.

   자세한 내용은 Microsoft의 TechNet 게시글에서 “트레이스 플래그(Transact-SQL)”를 검색하여 확인하시기 바랍니다.

   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2017 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
4. 매주 유지 보수 작업을 통해 인덱스를 재작성하면서 모든 인덱스가 적용되어 있는지 확인하십시오.
5. Security Management Server가 활용하는 데이터베이스에 대한 사용 권한 및 기능이 적합한지 확인하십시오. 자세한 내용은 KB 문서 124909를 참조하십시오.

7

고객 알림 이메일의 예

Dell Data Security를 구입하면 DellDataSecurity@Dell.com으로부터 이메일을 받게 됩니다. 다음은 CFT 자격 증명 및 라이센스 키 정보가 포함된 이메일의 예입니다.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - **U.S. & Canada Only**
- Outside the U.S., click here for a list of numbers

Need Support?
CHAT NOW!
Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options