Endpoint Security Suite Enterprise for Linux

관리자 가이드 v2.1

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.

2018 - 11

개정 A01

목차

1

소개

Linux용 Endpoint Security Suite Enterprise 관리자 안내서에서는 클라이언트 소프트웨어 배포와 설치에 필요한 정보를 제공합니다.

개요

Linux용 Endpoint Security Suite Enterprise는 운영 체제 및 메모리 레이어에 Advanced Threat Prevention을 제공하며, Dell Server에서 모두 중앙 집중적으로 관리합니다. 중앙 집중식 관리, 통합 준수 보고, 콘솔 위협 경고를 통해 기업에서 엔드포인트에 대한 준수를 간편하게 적용하고 입증합니다. 보안 전문 기술로 사전 정의된 정책 및 보고서 템플릿과 같은 기능을 구축하여 기업에서 IT 관리 비용을 절감하고 복잡성을 감소시키는 데 도움이 됩니다.

Security Management Server 또는 Security Management Server Virtual - 중앙 집중식 보안 정책 관리 제공, 기존 Enterprise 디렉터리와 통합하고 보고서를 생성함 이 문서의 목적에 알맞게 양쪽 서버가 특정 버전을 언급해야 할 경우(예: Security Management Server Virtual 사용 시 다른 절차 적용)를 제외하고 Dell Server로 지칭됩니다.

Linux용 Advanced Threat Prevention에는 3개의 RPM을 포함한 하나의 tar.gz 파일이 있습니다.

Dell ProSupport에 문의

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

또한, dell.com/support에서 Dell 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 태그 또는 익스프레스 서비스 코드를 준비하십시오.

미국 외부의 전화 번호는 Dell ProSupport 국제 전화 번호를 확인하십시오.

2

요구 사항

이 장에는 클라이언트 하드웨어와 소프트웨어 요구 사항이 나와 있습니다. 배포 작업을 계속하기 전에 배포 환경이 이런 요구 사항을 충족하는지 확인하십시오.

하드웨어

다음 표에 지원되는 최소 하드웨어가 나와 있습니다.

하드웨어

- 최소 500MB의 사용 가능한 디스크 공간
- 2GB RAM
- 10/100/1000 또는 Wi-Fi 네트워크 인터페이스 카드

ⓘ | **노트: 현재 Ipv6이 지원되지 않습니다.**

소프트웨어

다음 표에 지원되는 소프트웨어가 나와 있습니다.

운영 체제(64비트 커널)

- CentOS Linux v7.1 - v7.5
- Red Hat Enterprise Linux v7.1 - v7.5

포트

- 포트 443(HTTPS)은 통신하는 데 사용되며 에이전트가 관리 콘솔과 통신하기 위해 방화벽에서 반드시 열려 있어야 합니다. 어떠한 이유로든 포트 443이 차단되면 업데이트가 다운로드될 수 없기 때문에, 컴퓨터가 가장 최신 보호 기능을 사용할 수 없습니다. 클라이언트 컴퓨터가 다음에 액세스할 수 있어야 합니다.

사용	애플리케이션 프로토콜	전송 프로토콜	포트 번호	대상	방향
모든 통신	HTTPS	TCP	443	*.cylance.com에 모든 https 트래픽 허용	아웃바운드
Dell Core Server와의 통신	HTTPS	TCP	8888	Core Server 통신 허용	인바운드/아웃바운드

- 추가 정보는 SLN303898을 참조하십시오.

Endpoint Security Suite Enterprise for Linux 및 의존성

Endpoint Security Suite Enterprise for Linux는 Mono 및 상관 관계를 사용해 Linux OS에서 설치 및 활성화합니다. 설치 프로그램에서 필수 상관 관계를 다운로드하고 설치합니다. 패키지 추출이 완료되면 어떠한 상관 관계가 활용되는지 다음과 같은 명령을 사용하여 확인할 수 있을 수 있습니다.

```
./showdeps.sh
```

호환성

다음 표에는 Windows, Mac 및 Linux의 호환성이 자세히 나와 있습니다.

해당 없음 - 이 플랫폼에 기술이 적용되지 않습니다.

빈 필드 - 정책이 Endpoint Security Suite Enterprise에서 지원되지 않습니다.

기능	정책	Windows	macOS	Linux
파일 작업				
	자동 격리(안전하지 않음)	x	x	x
	자동 격리(비정상)	x	x	x
	자동 업로드	x	x	x
	정책 안전 목록	x	x	x
메모리 작업				
	메모리 보호	x	x	x
악용				
	스택 피벗	x	x	x
	스택 보호	x	x	x
	덮어쓰기 코드	x	해당 없음	
	RAM 스크랩	x	해당 없음	
	악성 페이로드	x		
프로세스 주입				
	메모리 원격 할당	x	x	해당 없음
	메모리 원격 매핑	x	x	해당 없음
	메모리에 원격으로 쓰기	x	x	해당 없음
	메모리에 PE를 원격으로 쓰기	x	해당 없음	해당 없음
	원격 덮어쓰기 코드	x	해당 없음	
	메모리 원격 매핑 해제	x	해당 없음	
	원격 스레드 생성	x	x	
	원격 APC 예약됨	x	해당 없음	해당 없음
	DYLD 주입		x	x

기능	정책	Windows	macOS	Linux
에스컬레이션				
	LSASS 읽기	x	해당 없음	해당 없음
	제로 할당	x	x	
보호 설정				
	실행 제어	x	x	x
	장치의 서비스 종료 방지	x	x	
	안전하지 않은 실행 프로세스 및 하위 프로세스 삭제	x	x	x
	백그라운드 위협 감지	x	x	x
	새 파일 감시	x	x	x
	스캔할 최대 아카이브 파일 크기	x	x	x
	특정 폴더 제외	x	x	x
	파일 샘플 복사	x		
응용 프로그램 제어				
	창 변경	x		x
	폴더 제외	x		
에이전트 설정				
	로그 파일 자동 업로드 활성화	x	x	x
	바탕 화면 알림 활성화	x		
스크립트 제어				
	Active Script	x		
	Powershell	x		
	Office 매크로	x		해당 없음
	Powershell 콘솔 사용 차단	x		
	이러한 폴더 및 하위 폴더에서 스크립트 승인	x		
	로깅 수준	x		
	자체 보호 수준	x		
	자동 업데이트	x		
	탐지 실행(에이전트 UI에서)	x		
	격리됨 삭제(에이전트 UI 및 콘솔 UI)	x		
	연결되지 않은 모드	x		x
	상세 위협 데이터	x		

기능	정책	Windows	macOS	Linux
	인증서 안전 목록	x	x	해당 없음
	맬웨어 샘플 복사	x	x	x
	프록시 설정	x	x	x
	수동 정책 확인(에이전트 UI)	x	x	

3

작업

설치

이 섹션에서는 Linux용 Endpoint Security Suite Enterprise의 설치 과정을 안내합니다.

사전 요구 사항

클라이언트 소프트웨어 배포 중에는 IT 모범 사례를 따르는 것이 좋습니다. 예를 들어, 초기 테스트에서 테스트 환경을 통제하고 사용자에 대해 시간별 배포를 수행해야 합니다.

시작하기 전에, 다음과 같은 사전 요구 사항이 충족되어 있는지 확인하십시오.

- Dell Server 및 해당 구성 요소가 이미 설치되어 있는지 확인합니다.

  Dell Server를 아직 설치하지 않은 경우, 아래의 해당 가이드에서 지침을 따릅니다.

  Security Management Server Installation and Migration Guide(Security Management Server 설치 및 마이그레이션 가이드)

  Security Management Server Virtual Quick Start Guide and Installation Guide(Security Management Server Virtual 퀵 스타트 가이드 및 설치 가이드)
- Dell Server 호스트 이름과 포트가 있는지 확인합니다. 클라이언트 소프트웨어 설치를 위해서는 두 가지 모두 필요합니다.
- 대상 컴퓨터가 Dell Server와 네트워크로 연결되어 있어야 합니다.
- 클라이언트의 서버 인증서가 누락되었거나 자체 서명된 경우, 클라이언트 측면에 있는 SSL 인증서만 비활성화해야 합니다.

명령줄 설치

명령줄을 사용하여 Endpoint Security Suite Enterprise 클라이언트를 설치하려면 아래 단계를 따르십시오.

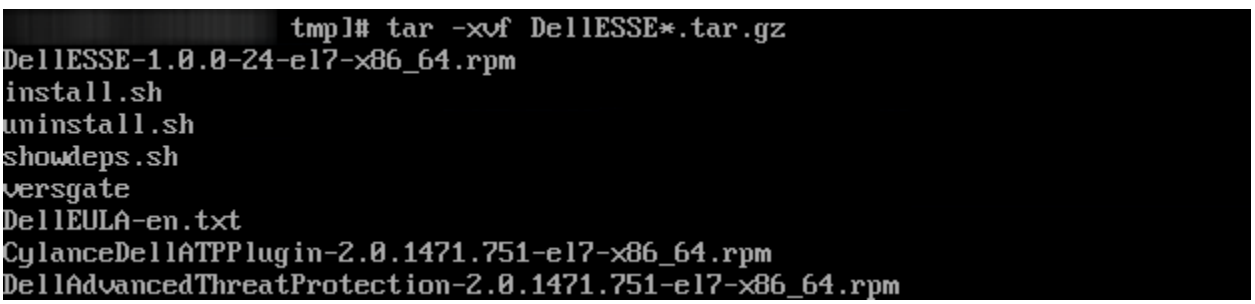
설치 중에 관리 권한을 호출하려면 **sudo** 명령을 사용해야 합니다. 메시지가 표시되면 사용자의 자격 증명을 입력합니다.

지문 판독기 승인은 처음 설치 시에만 표시됩니다.

1 Dell FTP 계정을 사용하여 설치 번들(DellESSE-1.x.x-xxx.tar.gz)을 찾아 다운로드합니다.

2 다음 명령을 사용하여 tar.gz의 압축을 해제합니다:

```
tar -xvf DellESSE*.tar.gz
```



3 다음 명령은 필수 RPM 및 상관 관계의 설치 스크립트를 실행합니다.

```
sudo ./install.sh
```

4 *Dell Security Management Server Host?*에서 대상 사용자 관리를 위한 Dell Server의 정규화된 호스트 이름을 입력합니다. 예를 들어, server.organization.com.

5 *Dell Security Management Server Port?*에서 포트가 8888로 설정되어 있는지 확인합니다.

```
Dell Endpoint Security Suite Enterprise (ESSE) Installation
Dell Security Management Server Host?
Dell Security Management Server Port?
```

6 DellESSE 패키지 및 해당 상관 관계 설치 메시지가 나타나면 **y**를 입력합니다.

```
 libXfixes      x86_64 5.0.3-1.el7             base                      18
 libXrender     x86_64 0.9.10-1.el7            base                      26
 libXxf86vm     x86_64 1.1.4-1.el7             base                      18
 libexif        x86_64 0.6.21-6.el7            base                     347
 libjpeg-turbo x86_64 1.2.90-5.el7             base                     134
 libpng         x86_64 2:1.5.13-7.el7_2        base                     213
 libtiff        x86_64 4.0.3-27.el7_3          base                     170
 libxcb         x86_64 1.12-1.el7              base                     211
 libxshmfence   x86_64 1.2-1.el7               base                     7.2
 lyx-fonts      noarch 2.2.3-1.el7             epel                     159
 mesa-libEGL    x86_64 17.0.1-6.20170307.el7 base                       82
 mesa-libGL     x86_64 17.0.1-6.20170307.el7 base                      155
 mesa-libgbm    x86_64 17.0.1-6.20170307.el7 base                       32
 mesa-libglapi x86_64 17.0.1-6.20170307.el7 base                        41
 pixman         x86_64 0.34.0-1.el7            base                     248

Transaction Summary
================================================================================
Install  1 Package (+27 Dependent packages)

Total size: 96 M
Total download size: 3.8 M
Installed size: 104 M
Is this ok [y/d/N]:
```

7 *지문 판독기* 승인을 묻는 메시지가 나타나면 **y**를 입력합니다.

```
Total                                                452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78 a7c2 7bb1 24c6 a8a7 f4a0 0eb5
 Package        : centos-release-7-3.1611.el7.centos.x86_64 (@anaconda)
 From           : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

8 *DellAdvancedThreatProtection* 패키지를 설치하라는 메시지가 표시되면 **y**를 입력합니다.

```
Dependencies Resolved

================================================================================
 Package  Arch   Version      Repository                                   Size
================================================================================
Installing:
 DellAdvancedThreatProtection
         x86_64 2.0.1461-739 /DellAdvancedThreatProtection-2.0.1461.739-el7-x86_64 149 M

Transaction Summary
================================================================================
Install  1 Package

Total size: 149 M
Installed size: 149 M
Is this ok [y/d/N]:
```

9 *CylanceDellATPPlugin* 패키지를 설치하라는 메시지가 표시되면 **y**를 입력합니다.

```
Dependencies Resolved

================================================================================
 Package     Arch   Version Repository                                   Size
================================================================================
Installing:
 CylanceDellATPPlugin
             x86_64 2.2.4-0 /CylanceDellATPPlugin-2.0.1461.739-el7-x86_64 439 k

Transaction Summary
================================================================================
Install  1 Package

Total size: 439 k
Installed size: 439 k
Is this ok [y/d/N]:
```

10 설치가 완료됩니다.

```
Installed:
  DellAdvancedThreatProtection.x86_64 0:2.0.1461-739

Complete!
```

11 Linux용 설치는 Verify Endpoint Security Suite Enterprise를 참조하십시오.

명령줄 설치 제거

명령줄을 사용하여 Linux용 Endpoint Security Suite Enterprise을 제거하려면 아래의 단계를 따릅니다.

1 터미널 창에 액세스합니다.
2 다음 명령을 사용하여 패키지를 제거:
```
sudo ./uninstall.sh
```
3 **Enter** 키를 누릅니다.
이제 Linux 용 Endpoint Security Suite Enterprise가 제거되어 컴퓨터를 정상적으로 사용할 수 있습니다.

세부 정보 보기

Linux용 Endpoint Security Suite Enterprise가 설치된 후에는 Dell Server에 의해 엔드포인트로 인식됩니다.

atp -t

atp - t 명령은 장치에서 발견된 모든 위협 요소와 실시한 조치가 표시됩니다. 위협은 잠재적으로 안전하지 않은 파일 또는 프로그램으로 새로 감지된 이벤트로서 안내에 따른 수정이 필요한 이벤트 범주입니다.

이러한 항목은 수행된 작업, 해시 ID, 위협의 위치를 자세히 나타냅니다.

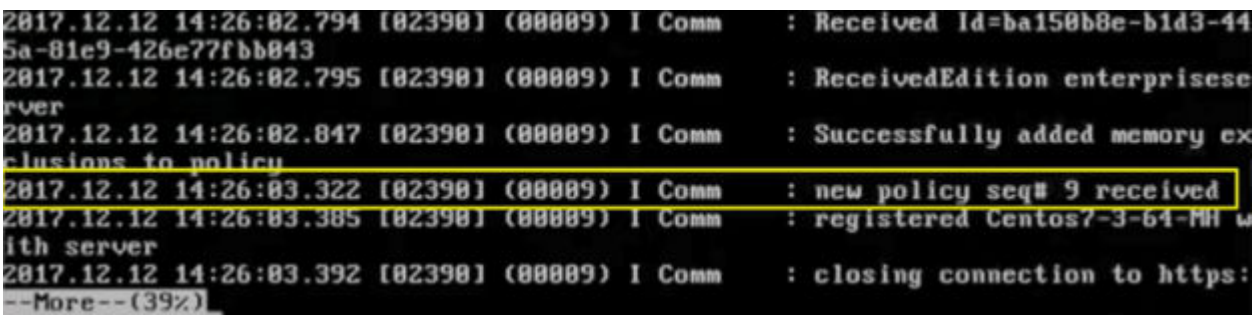
- **안전하지 않음** - 맬웨어일 가능성이 높은 의심스러운 파일
- **비정상** - 맬웨어일 수 있는 의심스러운 파일
- **격리됨** - 장치에서 실행되지 않도록 원래 위치에서 이동되어 격리 폴더에 저장된 파일
- **면제됨** - 장치에서 실행이 허용된 파일.
- **삭제됨** - 조직 내에서 삭제된 파일. 제거된 파일은 면제된 파일, 안전 목록에 추가된 파일 및 장치의 차단된 폴더에서 삭제된 파일을 포함합니다.

Advanced Threat Prevention의 위협 분류에 대한 자세한 내용은 Dell Server Remote Management Console에서 사용 가능한 *관리자 도움말*을 참조하십시오.

설치 확인

경우에 따라 설치가 성공적으로 수행되었는지 확인할 수 있습니다.

- 클라이언트에서 터미널 창에 액세스합니다.
- 정책 순서를 수신하기 전 클라이언트가 Dell Server에 등록합니다.
- */var/log/Dell/ESSE/DellAgent.00.log* 파일에서는 Dell Server와의 통신 및 플러그인/서비스 상호작용에 대해 자세히 설명합니다. 포함된 텍스트는 클라이언트가 Dell Server로부터 정책을 받았음을 확인합니다.



포함된 텍스트는 Dell 서비스가 Advanced Threat Prevention 플러그인을 로드하기 위해 중지되었음을 확인합니다.

```
//cedmz.credce.com:8888/agent
2017.12.12 14:27:05.883 [02390] (00009) I Comm    : next contact with server sch
eduled for 12/12/2017 8:27:05 PM
2017.12.12 14:27:10.442 [02390] (00005) I Agent   : Dell Data Protection stopped
---date--- ----time---- --pid-- -thrid-   -subsys-  ----------------------------
--message-------------------------------
2017.12.12 14:27:12.968 [02551] (00005) I Agent   : service name is "DellMgmtAge
nt"
2017.12.12 14:27:12.970 [02551] (00005) I Agent   : product name is "Dell Data P
```

포함된 텍스트는 Linux용 Endpoint Security Suite Enterprise 플러그인 3가지가 로드되었음을 확인합니다.

```
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : machine name is "centosvm2.ddsdemos.com"
2018.02.18 10:51:36.951 [01077] (00005) I Agent   : process is 64-bit
2018.02.18 10:51:36.952 [01077] (00005) I Agent   : domain is "(none)"
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Server Communication Manager" 1.
 Id={CAA1A89F-AF21-4C1E-9407-1E185FFEEB5C} in 69 ms
2018.02.18 10:51:37.059 [01077] (00005) I Agent   : loaded plugin "Auditing and Reporting Service"
.0 Id={0E969074-3164-467F-BF3D-D9E695F48240} in <1 ms
2018.02.18 10:51:37.069 [01077] (00005) I AdvATP  : Advanced Threat Prevention Cylance component lo
ging initialized
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded plugin "Advanced Threat Prevention" 1.0
d={96BBD97F-9BF0-4D61-94F8-A9884F8DC287} in 8 ms
2018.02.18 10:51:37.069 [01077] (00005) I Agent   : loaded 3 plugins
2018.02.18 10:51:37.090 [01077] (00010) I Comm    : AgentID 00397403-c05f-4cbf-b6b4-e15dd577186a
2018.02.18 10:51:37.102 [01077] (00011) I AdvATP  : AdvancedAtpManager Starting
2018.02.18 10:51:37.125 [01077] (00011) I AdvATP  : management is active
2018.02.18 10:51:37.129 [01077] (00011) I AdvATP  : processing new policies - Policy list count=1
```

`atp -s` - 다음과 같은 내용이 포함되어 있습니다.

- 등록 상태
- 일련 번호 - 지원 문의 시 사용합니다. 이 번호는 고유한 설치 식별자입니다.
- 정책

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp -s
Registration Status: Registered
Serial Number: 0088ab40-ce18-43fa-a959-85f44e5ff251
Policy:  (Online)
```

다음 명령에서는 Linux용 Endpoint Security Suite Enterprise를 위한 명령줄 변수에 대한 정보를 자세히 설명합니다.

`/opt/cylance/desktop/atp --help`

```
[dell@Centos7-3-64-MH ~]$ /opt/cylance/desktop/atp --help
usage: atp <options>
options:
    -r, --register=token    : register with Dell Data Security servers with the
provided token
    -s, --status            : get status of Advanced Threat Prevention
    -u, --checkupdates      : check for updates
    -b, --start-bg-scan     : start background scan
    -B, --stop-bg-scan      : stop background scan
    -d, --scan-dir=dir      : scan directory
    -l, --getloglevel       : get current log level
    -L, --setloglevel=level : set log level
    -P, --getpolicytime     : get the policy update time
    -p, --checkpolicy       : check for policy updates
    -t, --threats           : list threats
    -q, --quarantine=id     : quarantine a file by id (hash)
    -w, --waive=id          : waive a file by id (hash)
    -v, --version           : print this tools version
    -h, --help              : atp help
```

Advanced Threat Prevention *atp* 명령은 일반적으로 셸의 PATH 변수에 포함된 */usr/sbin* 디렉터리에 추가되어 대부분의 경우 명시적인 경로 없이도 사용 가능합니다.

문제 해결

SSL 신뢰 인증서 비활성화

컴퓨터의 서버 인증서가 누락되었거나 자체 서명된 경우, 클라이언트 측면에 있는 SSL 인증서만 비활성화해야 합니다.

흔치 않은 인증서를 사용하는 경우 루트 인증서를 Linux 인증서 저장소에로 가져온 후 다음 명령을 사용하여 Linux 서비스의 Endpoint Security Suite를 다시 시작합니다. `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 터미널 창에 액세스합니다.

2 CsfConfig app에 대한 경로 입력:
```
/usr/lib/dell/esse/CsfConfig
```

3 CsfConfig.app 실행:
```
sudo ./CsfConfig
```

기본 설정 시 다음이 표시됩니다.

현재 설정:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False

4 옵션을 나열하려면 **-help**를 입력합니다.

5 대상 컴퓨터에서 SSL 인증서 신뢰를 비활성화하려면 다음 명령을 입력합니다.
```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

XML 인벤토리 및 정책 변경 사항을 로그 폴더에 추가

inventory.xml 또는 policies.xml 파일을 로그 폴더에 추가하려면 다음 단계를 따르십시오.

1 위에 설명된 대로 *CsfConfig app*을 실행합니다.

2 *DumpXmlInventory*를 *True*로 변경하려면 다음 명령을 입력합니다.
```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 *DumpPolicies*를 *True*로 변경하려면 다음 명령을 입력합니다.
```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

정책이 변경되는 경우에만 정책 파일이 덤프됩니다.

4 inventory.xml 및 policies.xml 로그 파일을 보려면 */var/log/Dell/Dell Data Protection*로 이동합니다.

노트: CsfConfig의 변경 사항은 즉시 적용되지 않을 수 있습니다.

로그 파일 수집

Endpoint Security Suite Enterprise for Linux의 로그는 다음 위치에 있습니다. */var/log/Dell/ESSE*. 로그를 생성하려면 다음 명령을 사용합니다. **./getlogs.sh**

로그를 수집하는 방법에 대한 자세한 내용은 SLN303924를 참조하십시오.

테넌트 프로비저닝

Advanced Threat Prevention의 정책 집행이 활성화되기 전에 테넌트가 Dell Server에서 프로비전되어야 합니다.

사전 요구 사항

- 시스템 관리자 역할의 관리자가 수행해야 합니다.
- Dell Server에서 프로비저닝하려면 인터넷에 연결되어 있어야 합니다.
- Management Console에서 Advanced Threat Prevention 온라인 서비스 통합을 표시하려면 클라이언트에서 인터넷이 연결되어 있어야 합니다.
- 프로비저닝은 프로비저닝 중에 인증서에서 생성되는 토큰을 기반으로 합니다.
- Dell Server에 Advanced Threat Prevention 라이센스가 있어야 합니다.

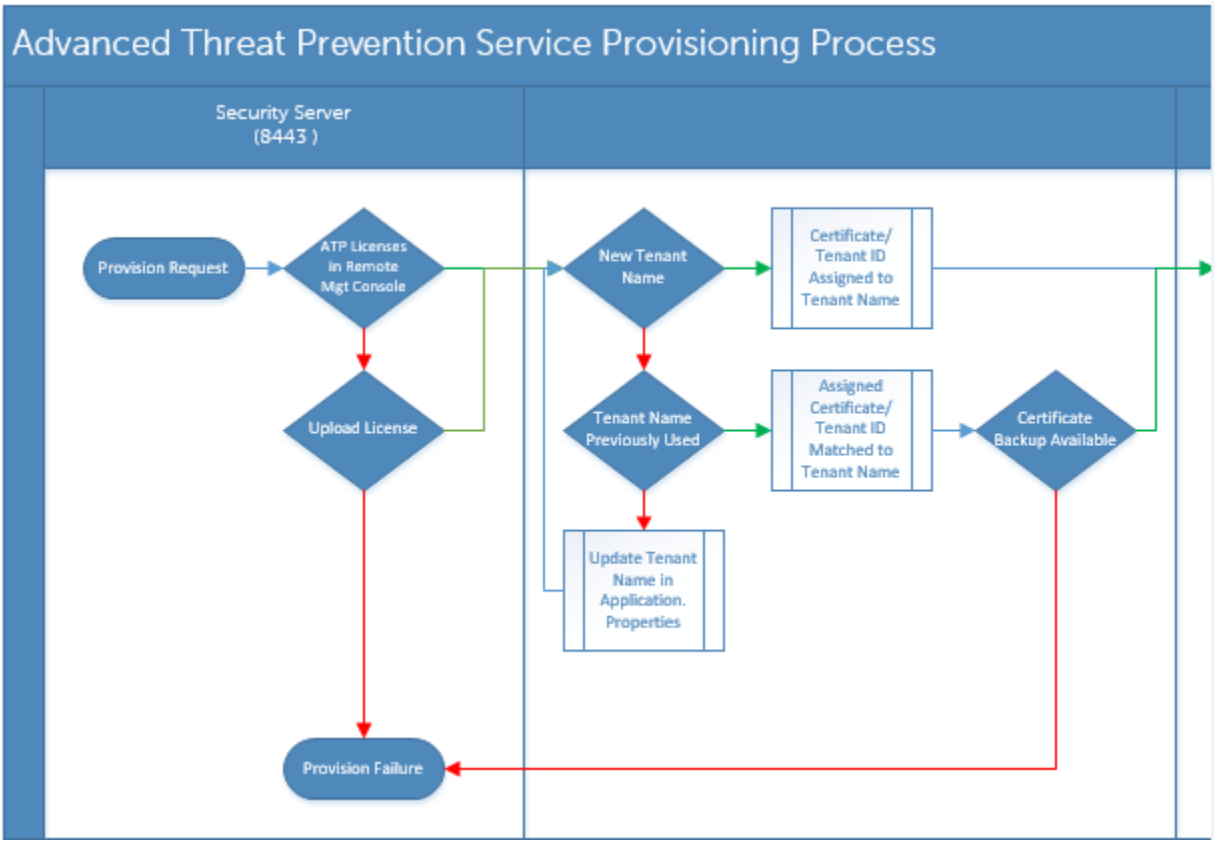
테넌트 프로비저닝

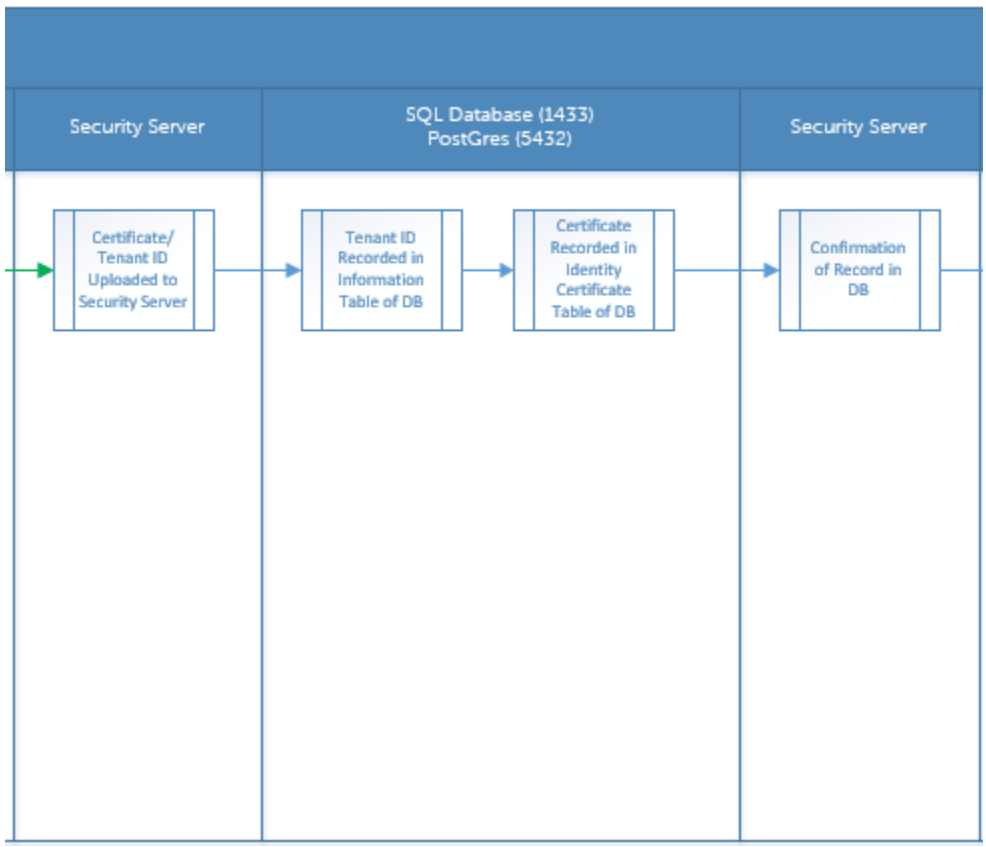
1. Dell 관리자 계정으로 Remote Management Console에 로그인합니다.
2. Management Console의 왼쪽 창에서 **관리 > 서비스 관리**를 클릭합니다.
3. **Advanced Threat Protection 서비스 설정**을 클릭합니다. 이때 오류가 발생하면 Advanced Threat Prevention 라이센스를 가져옵니다.
4. 라이센스를 가져오면 지침 제공되는 설정이 시작됩니다. **다음**을 클릭하여 시작합니다.
5. EULA를 읽고 동의한 후 **다음**을 클릭합니다.
6. 테넌트 프로비저닝을 위해 Dell Server에 유효한 자격 증명을 제공합니다. **다음**을 클릭합니다. *Cylance 상표의 기존 테넌트의 프로비저닝은 지원되지 않습니다.*
7. 인증서를 다운로드합니다. 이 인증서는 Dell Server에서 재해가 발생할 경우 복구에 필요합니다. 이 인증서는 자동으로 백업되지 않습니다. 인증서를 다른 컴퓨터의 안전한 위치에 백업합니다. 인증서를 백업한다는 옵션의 확인란을 선택하고 **다음**을 클릭합니다.
8. 설정이 완료됩니다. **확인**을 클릭합니다.

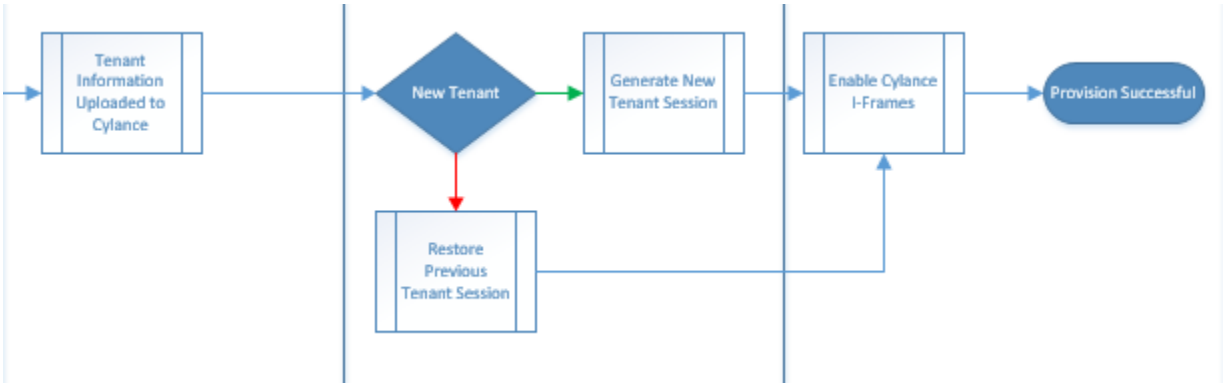
프로비저닝 문제 해결

프로비저닝 및 에이전트 통신

다음 다이어그램은 Advanced Threat Prevention 서비스 프로비저닝 프로세스를 보여 줍니다.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
Provision Failure
New Tenant Name
Certificate/ Tenant ID Assigned to Tenant Name
Tenant Name Previously Used
Assigned Certificate/ Tenant ID Matched to Tenant Name
Certificate Backup Available
Update Tenant Name in Application. Properties


Security Server
SQL Database (1433)
PostGres (5432)
Security Server
Certificate/ Tenant ID Uploaded to Security Server
Tenant ID Recorded in Information Table of DB
Certificate Recorded in Identity Certificate Table of DB
Confirmation of Record in DB



다음 그림은 Advanced Threat Prevention 에이전트 통신 프로세스를 보여 줍니다.