Endpoint Security Suite Enterprise for Linux

Administratorhandbuch v2.1

Anmerkungen, Vorsichtshinweise und Warnungen

ANMERKUNG: Eine ANMERKUNG macht auf wichtige Informationen aufmerksam, mit denen Sie Ihr Produkt besser einsetzen können.

VORSICHT: Ein VORSICHTSHINWEIS macht darauf aufmerksam, dass bei Nichtbefolgung von Anweisungen eine Beschädigung der Hardware oder ein Verlust von Daten droht, und zeigt auf, wie derartige Probleme vermieden werden können.

WARNUNG: Durch eine WARNUNG werden Sie auf Gefahrenquellen hingewiesen, die materielle Schäden, Verletzungen oder sogar den Tod von Personen zur Folge haben können.

2018 - 11

Rev. A01

Inhaltsverzeichnis

1 Einleitung 4
Übersicht 4
Kontaktaufnahme mit dem Dell ProSupport 4

2 Anforderungen 5
Hardware 5
Software 5
Ports 5
Endpoint Security Enterprise for Linux und Abhängigkeiten 6
Kompatibilität 6

3 Aufgaben 9
Damit ist die Installation 9
Voraussetzungen 9
Installation über die Befehlszeile 9
Details anzeigen 11
Prüfen der Installation 12
Fehlerbehebung 14
SSL Trust Certificate deaktivieren 14
Hinzufügen von XML-Bestandsaufnahme und Richtlinienänderungen zu den Protokollordnern 14
Protokolldateien sammeln 15
Bereitstellung eines Mandanten 15
Bereitstellung eines Mandanten 15
Fehlerbehebung bei Bereitstellung 15
Bereitstellung und Kommunikation mit Agenten 15

1

Einleitung

Im Administratorhandbuch zu Endpoint Security Suite Enterprise for Linux sind die Informationen enthalten, die zum Bereitstellen und Installieren der Client-Software benötigt werden.

Übersicht

Die Endpoint Security Suite Enterprise for Linux bietet Advanced Threat Prevention auf der Betriebssystem- und der Speicherebene. Alles wird dabei zentral über den Dell Server verwaltet. Durch die zentralisierte Verwaltung, konsolidierte Berichterstattung zur Richtlinientreue und Bedrohungsmeldungen in der Konsole können Unternehmen problemlos die Richtlinientreue ihrer Endpunkte durchsetzen und beweisen. Sicherheits-Expertise ist durch Funktionen wie vordefinierten Richtlinien und Berichtsvorlagen integriert, damit Unternehmen Kosten und Komplexität ihrer IT reduzieren können.

Security Management Server oder Security Management Server Virtual – bieten eine zentrale Verwaltung der Sicherheitsrichtlinien, Integration in die vorhandenen Enterprise-Verzeichnisse und das Erstellen von Berichten. Zum Zwecke dieses Dokuments werden beide Server als Dell Server bezeichnet, sofern keine konkrete Version angegeben werden muss (wenn z. B. bei Verwendung von Security Management Server Virtual ein anderes Verfahren notwendig ist).

Advanced Threat Prevention for Linux hat eine tar.gz-Datei, die die drei RPMs enthält.

Kontaktaufnahme mit dem Dell ProSupport

Telefonischen Support rund um die Uhr für Ihr Dell Produkt erhalten Sie unter der Rufnummer 877-459-7304, Durchwahl 4310039.

Zusätzlich steht Ihnen unser Online-Support für Dell Produkte unter dell.com/support zur Verfügung. Der Online-Support enthält Treiber, Handbücher, technische Ratgeber, FAQs und eine Beschreibung festgestellter Probleme.

Halten Sie bei Ihrem Anruf Ihre Service-Tag-Nummer oder Ihren Express-Servicecode bereit, damit wir Sie schneller mit dem richtigen Ansprechpartner für Ihr technisches Problem verbinden können.

Telefonnummern außerhalb der Vereinigten Staaten finden Sie unter Dell ProSupport – Internationale Telefonnummern.

2

Anforderungen

In diesem Kapitel werden die Hardware- und Softwareanforderungen für den Client erläutert. Stellen Sie sicher, dass die Implementierungsumgebung die Anforderungen erfüllt, bevor Sie mit der Implementierung fortfahren.

Hardware

Die folgende Tabelle enthält Informationen zur minimal unterstützten Hardware.

Hardware

- Mindestens 500 MB freier Speicherplatz
- 2 GB RAM
- Netzwerkschnittstellenkarte 10/100/1000 oder Wi-Fi

ⓘ | **ANMERKUNG: IPv6 wird derzeit nicht unterstützt.**

Software

Die folgende Tabelle enthält detaillierte Informationen über die unterstützte Software.

Betriebssysteme (64-Bit-Kernel)

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

Ports

- Port 443 (HTTPS) wird für die Kommunikation verwendet und muss auf der Firewall geöffnet sein, damit die Agenten mit der Verwaltungskonsole kommunizieren können. Sollte Port 443 gesperrt sein, können keine Aktualisierungen heruntergeladen werden. In diesem Fall ist ein ordnungsgemäßer Schutz der Computer nicht gewährleistet. Stellen Sie sicher, dass die Client-Computer auf Folgendes zugreifen können:

Verwenden Sie die Datei	Anwendungsprotokoll	Transportprotokoll	Portnummer	Ziel	Richtung
Gesamte Kommunikation	HTTPS	TCP	443	Lassen Sie den gesamten https-Datenverkehr an *.cylance.com zu.	Ausgehend
Core-Server-Kommunikation	HTTPS	TCP	8888	Ermöglicht die Core-Server-Kommunikation	Eingehend/ausgehend

- Weitere Informationen finden Sie unter SLN303898.

Endpoint Security Enterprise for Linux und Abhängigkeiten

Endpoint Security Enterprise for Linux verwendet Mono und Abhängigkeiten zur Installation und Aktivierung auf dem Linux-Betriebssystem. Das Installationsprogramm wird die erforderlichen Abhängigkeiten herunterladen und installieren. Nach der Extraktion des Pakets können Sie anzeigen, welche Abhängigkeiten genutzt werden, indem Sie den folgenden Befehl verwenden:

```
./showdeps.sh
```

Kompatibilität

Die folgende Tabelle zeigt die Kompatibilität mit Windows, Mac und Linux.

Nicht verfügbar – Die Technologie gilt nicht für diese Plattform.

Leeres Feld – Die Richtlinie wird nicht mit Endpoint Security Suite Enterprise unterstützt.

Funktionen	Richtlinien	Windows	macOS	Linux
Dateimaßnahmen				
	Automatische Quarantäne (Unsicher)	x	x	x
	Automatische Quarantäne (Anormal)	x	x	x
	Automatisch hochladen	x	x	x
	Richtlinie „Sichere Liste“	x	x	x
Speichermaßnahmen				
	Speicherschutz	x	x	x
Ausnutzung				
	Stapeldrehung	x	x	x
	Stapelschutz	x	x	x
	Code überschreiben	x	k. A.	
	RAM-Scraping	x	k. A.	
	Schädliche Nutzlast	x		
Vorgangsinjektion				
	Remote-Zuweisung von Speicher	x	x	k. A.
	Remote-Zuordnung von Speicher	x	x	k. A.
	Remote Schreiben in Speicher	x	x	k. A.
	Remote Schreiben von PE in Speicher	x	k. A.	k. A.

Funktionen	Richtlinien	Windows	macOS	Linux
	Code remote überschreiben	x	k. A.	
	Zuordnung von Speicher remote aufheben	x	k. A.	
	Remote-Thread-Erstellung	x	x	
	Remote-APC geplant	x	k. A.	k. A.
	DYLD-Injektion		x	x
Eskalation				
	LSASS lesen	x	k. A.	k. A.
	Null-Zuweisung	x	x	
Schutzeinstellungen				
	Ausführungssteuerung	x	x	x
	Herunterfahren des Dienstes vom Gerät verhindern	x	x	
	Unsichere Prozesse und ihre Unterprozesse, die gerade ausgeführt werden, beenden	x	x	x
	Entdeckung einer Hintergrundsbedrohung	x	x	x
	Nach neuen Dateien Ausschau halten	x	x	x
	Maximale Größe der zu scannenden Archivdatei	x	x	x
	Bestimmte Ordner ausschließen	x	x	x
	Dateimuster kopieren	x		
Anwendungssteuerung				
	Fenster ändern	x		x
	Ordnerausschlüsse	x		
Agenten-Einstellungen				
	Automatisches Hochladen von Protokolldateien aktivieren	x	x	x
	Desktop-Benachrichtigungen aktivieren	x		
Skriptsteuerung				
	Aktives Skript	x		
	Powershell	x		

Funktionen	Richtlinien	Windows	macOS	Linux
	Office-Makros	x		k. A.
	Powershell-Konsolennutzung blockieren	x		
	Skripte in diesen Ordnern (und Unterordnern) genehmigen	x		
	Protokolliergrad	x		
	Selbstschutzebene	x		
	Automatische Aktualisierung	x		
	Erkennung durchführen (von Agent-UI)	x		
	In Quarantäne löschen (Agent-UI und Konsolen-UI)	x		
	Getrennter Modus	x		x
	Detaillierte Bedrohungsdaten	x		
	Zertifizierte sichere Liste	x	x	k. A.
	Malware-Muster kopieren	x	x	x
	Proxy-Einstellungen	x	x	x
	Manuelle Richtlinienüberprüfung (Agent-UI)	x	x	

3

Aufgaben

Damit ist die Installation

Dieser Abschnitt führt Sie durch die Installation von Endpoint Security Suite Enterprise for Linux.

Voraussetzungen

Dell empfiehlt, bei der Implementierung der Client-Software die Best Practices für IT zu beachten. Dazu zählen u. a. geregelte Testumgebungen für die anfänglichen Tests und die stufenweise Bereitstellung für Benutzer.

Stellen Sie zunächst fest, ob folgende Voraussetzungen erfüllt sind:

- Überprüfen Sie, ob der Dell Server und seine Komponenten bereits installiert sind.

  Wenn Sie den Dell Server noch nicht installiert haben, folgen Sie den Anweisungen in der entsprechenden nachfolgenden Anleitung.

  Security Management Server Installation and Migration Guide (Installations- und Migrationshandbuch für Security Management Server)

  Security Management Server Virtual Quick Start Guide and Installation Guide (Schnellanleitung und Installationshandbuch für Security Management Server Virtual)
- Stellen Sie sicher, dass Sie über den Dell Server-Hostnamen und -Port verfügen. Beides wird für die Installation der Client-Software benötigt.
- Stellen Sie sicher, dass der Zielcomputer über Netzwerkkonnektivität zum Dell Server verfügt.
- Wenn ein Client-Serverzertifikat fehlt oder selbst signiert ist, müssen Sie die Funktion SSL Certificate Trust nur auf der Client-Seite deaktivieren.

Installation über die Befehlszeile

Führen Sie die folgenden Schritte aus, um den Endpoint Security Suite Enterprise Client unter Verwendung der Befehlszeile zu installieren.

Der **sudo**-Befehl muss aufgerufen werden, um die Administratorberechtigungen während der Installation aufzurufen. Wenn Sie dazu aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein.

Die Bestätigung des Fingerabdrucks wird nur während der ersten Installation angezeigt.

1 Suchen Sie das Installationspaket (DellESSE-1.x.x-xxx.tar.gz) und laden Sie es über Ihr Dell FTP-Konto herunter.

2 Extrahieren Sie die Datei tar.gz mithilfe des folgenden Befehls:

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

```
[redacted] tmp]# tar -xvf DellESSE*.tar.gz
DellESSE-1.0.0-24-el7-x86_64.rpm
install.sh
uninstall.sh
showdeps.sh
versgate
DellEULA-en.txt
CylanceDellATPPlugin-2.0.1471.751-el7-x86_64.rpm
DellAdvancedThreatProtection-2.0.1471.751-el7-x86_64.rpm
```

3 Mit dem folgenden Befehl wird das Installationsskript für die erforderlichen RPMs und Abhängigkeiten ausgeführt:

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

4 Geben Sie unter *Dell Security Management Server Host?* den vollständig qualifizierten Hostnamen des Dell Server zum Verwalten des Zielbenutzers ein. Zum Beispiel server.organization.com.

5 Stellen Sie unter *Dell Security Management Server Host?* sicher, dass der Port 8888 lautet.

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

6 Geben Sie **y** ein, wenn Sie dazu aufgefordert werden, um das Paket DellESSE und seine Abhängigkeiten zu installieren.

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

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 Geben Sie **y** ein, wenn Sie dazu aufgefordert werden, um die Bestätigung per *Fingerabdruck* zu aktivieren.

```
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 7bbl 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 Geben Sie **y** ein, wenn Sie dazu aufgefordert werden, um das *DellAdvancedThreatProtection*-Paket zu installieren.

```
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 Geben Sie **y** ein, wenn Sie dazu aufgefordert werden, um das *CylanceDellATPPlug*-Paket zu installieren.

```
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 Damit ist die Installation abgeschlossen.

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

Complete!
```

11 Siehe Überprüfen der Installation von Endpunkt Security Enterprise for Linux.

Deinstallation über die Befehlszeile

Um Endpoint Security Suite Enterprise for Linux über die Befehlszeile zu deinstallieren, führen Sie die folgenden Schritte aus.

1 Greifen Sie auf ein Terminalfenster zu.

2 Deinstallieren Sie das Paket unter Verwendung des folgenden Befehls:

```
sudo ./uninstall.sh
```

3 Drücken Sie die **Eingabetaste.**

Endpoint Security Suite Enterprise for Linux ist jetzt deinstalliert und der Computer kann normal verwendet werden.

Details anzeigen

Nach dem Endpoint Security Suite Enterprise for Linux installiert wurde, wird es vom Dell Server als Endpunkt anerkannt.

atp - t

Mit dem Befehl **`atp - t`** werden alle auf dem Gerät erkannten Bedrohungen sowie die durchgeführten Maßnahmen angezeigt. „Bedrohungen“ sind eine Kategorie von Ereignissen, die als potenziell unsichere Dateien oder Programme neu erfasst wurden und eine geführte Fehlerbehebung erfordern.

```
Quarantined 17E76B830F9F30A39F078F5A69AD87B3838DB73A28EC893BD06EAF95D6E464E2 /tmp/threats/LINUXTarGz
Archive
Quarantined 20FBC1FDFCDC96A7E21FB1C700A6517A61711732A0D31FC25A60609710ECBE09 /tmp/threats/LINUXAutoB
lockNoService
Quarantined 2D49A3F81AF3362FE806E417DF2807C960314FF4F271B5B1360964163CB49886 /tmp/threats/LINUXGBL2
Quarantined 52D74BD1555D7C82746112C44F4D9A916B9DA286DD5B14D7665D4167BB1EB5D8 /tmp/threats/LINUXRunni
ngAutoQ
Quarantined 70F193F3C2023A7542338142CA89F1076A238AB7BAAD4202B2DCEDA7286E43D9 /tmp/threats/LINUXTest1
Quarantined 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F8158E0D519CEC1D868E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC28640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED085ED042423A172B4BED7702E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F178A6413A8A7E84437098777711FB1CA6E31F /tmp/threats/LINUXAutoB
lockExecution
```

Diese Einträge beschreiben ergriffene Maßnahmen, Hash-ID und Ort der Gefahr.

- **Unsicher** – Eine verdächtige Datei, die wahrscheinlich Malware enthält
- **Anormal** – Eine verdächtige Datei, die Malware enthalten könnte
- **In Quarantäne** – Eine Datei, die vom ursprünglichen Speicherort in den Quarantäne-Ordner verschoben und daran gehindert wurde, auf dem Gerät ausgeführt zu werden.
- **Freigegeben** – Eine Datei, die auf dem Gerät ausgeführt werden darf.
- **Gelöscht** - Eine Datei, die innerhalb der Organisation gelöscht wurde. Zu den zugelassenen Dateien gehören Dateien mit dem Status „Freigegeben“, Dateien, die zur Liste „Sicher“ hinzugefügt wurden und Dateien, die aus dem Ordner „Quarantäne“ auf dem Gerät gelöscht wurden.

Weitere Informationen zur Klassifizierung von Bedrohungen durch Advanced Threat Prevention finden Sie in der *AdminHelp*, die in der Remote-Verwaltungskonsole des Dell Server verfügbar ist.

Prüfen der Installation

Optional können Sie sicherstellen, dass die Installation erfolgreich war.

- Greifen Sie auf dem Client auf ein Terminalfenster zu.
- Bevor eine Richtliniensequenz empfangen wird, wird der Client beim Dell Server registriert.
- Die Datei */var/log/Dell/ESSE/DellAgent.00.log* enthält Details zur Kommunikation mit dem Dell Server und zur Interaktion von Plug-in/Service.

  Die beigefügte Nachricht bestätigt, dass der Client Richtlinien vom Dell Server erhalten hat:

```
2017.12.12 14:26:02.794 [02390] (00009) I Comm    : Received Id=ba150b8e-b1d3-44
5a-81e9-426e77fbb043
2017.12.12 14:26:02.795 [02390] (00009) I Comm    : ReceivedEdition enterprisese
rver
2017.12.12 14:26:02.847 [02390] (00009) I Comm    : Successfully added memory ex
clusions to policy
2017.12.12 14:26:03.322 [02390] (00009) I Comm    : new policy seq# 9 received
2017.12.12 14:26:03.385 [02390] (00009) I Comm    : registered Centos7-3-64-MH w
ith server
2017.12.12 14:26:03.392 [02390] (00009) I Comm    : closing connection to https:
--More--(39%)
```

  Die beigefügte Nachricht bestätigt, dass der Dell Service gestoppt wurde, um das Advanced Threat Prevention Plug-in zu laden:

```
//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
```

Die beigefügte Nachricht bestätigt die drei geladenen Endpoint Security Suite Enterprise for Linux Plug-ins:

```
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` – Umfasst Folgendes:

- Registrierungsstatus
- Seriennummer – Verwenden Sie diese beim technischen Support. Dies ist die eindeutige Kennung für die Installation.
- Richtlinien

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

Mit dem folgenden Befehl werden die Befehlszeilenvariablen für Endpoint Security Suite Enterprise for Linux angezeigt:

`/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
```

Der *atp*-Befehl von Advanced Threat Prevention wird zum */usr/sbin*-Verzeichnis hinzugefügt, das normalerweise in einer PFAD-Variable einer Shell enthalten ist, sodass es in den meisten Fällen ohne ausdrücklichen Pfad verwendet werden kann.

Fehlerbehebung

SSL Trust Certificate deaktivieren

Wenn das Serverzertifikat eines Computers fehlt oder selbst signiert ist, müssen Sie die Funktion „SSL Certificate Trust“ nur auf der Client-Seite deaktivieren.

Wenn Sie ein unbekanntes Zertifikat verwenden, importieren Sie das Stammzertifikat in den Linux Zertifikatspeicher, und starten Sie anschließend die Endpoint Security Suite for Linux mit dem folgenden Befehl: `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Greifen Sie auf ein Terminalfenster zu.
2 Geben Sie den Pfad zur CsfConfig App ein:
`/usr/lib/dell/esse/CsfConfig`
3 Führen CsfConfig.app aus:
`sudo ./CsfConfig`

Das Folgende stellt die Standardeinstellungen dar:

Aktuelle Einstellungen:

Serverhost = deviceserver.company.com

Serverport = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False

4 Geben Sie **-help** ein, um eine Liste mit den Optionen anzuzeigen.
5 Um das SSL Trust Certificate auf dem Zielcomputer zu deaktivieren, geben Sie den folgenden Befehl ein:

```
sudo /usr/lib/dell/esse/CsfConfig -disablecerttrust true
```

Hinzufügen von XML-Bestandsaufnahme und Richtlinienänderungen zu den Protokollordnern

So fügen Sie die inventory.xml oder polocies.xml-Dateien dem Protokollordner hinzu:

1 Führen Sie die *CsfConfig.app* wie oben beschrieben aus.
2 Zum Ändern von *DumpXmlInventory* auf *True* geben Sie den folgenden Befehl ein:

```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```

3 Zum Ändern von *DumpPolicies* auf *True* geben Sie den folgenden Befehl ein:

```
sudo /usr/lib/dell/esse/CsfConfig -dumppolicies true
```

Die Richtliniendateien werden nur ausgegeben, wenn eine Richtlinienänderung aufgetreten ist.

4 Zum Anzeigen der Protokolldateien inventory.xml und policies.xml gehen Sie zu */var/log/Dell/Dell Data Protection*.

ANMERKUNG: CsfConfig-Änderungen werden möglicherweise nicht sofort angewendet.

Protokolldateien sammeln

Protokolle für Endpoint Security Suite Enterprise for Linux befinden sich an folgendem Speicherort: */var/log/Dell/ESSE*. Zum Generieren von Protokollen verwenden Sie den folgenden Befehl: **./getlogs.sh**

Informationen über das Sammeln der Protokolle finden Sie unter SLN303924.

Bereitstellung eines Mandanten

Ein Tenant muss im Dell Server bereitgestellt werden, bevor die Durchsetzung von Advanced Threat Prevention-Richtlinien aktiv wird.

Voraussetzungen

- Muss durch einen Administrator mit der Systemadministratorrolle durchgeführt werden.
- Muss über eine Verbindung mit dem Internet verfügen, um auf dem Dell Server bereitgestellt zu werden.
- Muss über eine Verbindung mit dem Internet auf dem Client verfügen, um die Online-Dienst-Integration von Advanced Threat Prevention in der Verwaltungskonsole anzuzeigen.
- Die Bereitstellung basiert auf einem Token, das im Rahmen der Bereitstellung aus einem Zertifikat generiert wird.
- Die Lizenzen für Advanced Threat Prevention müssen auf dem Dell Server vorhanden sein.

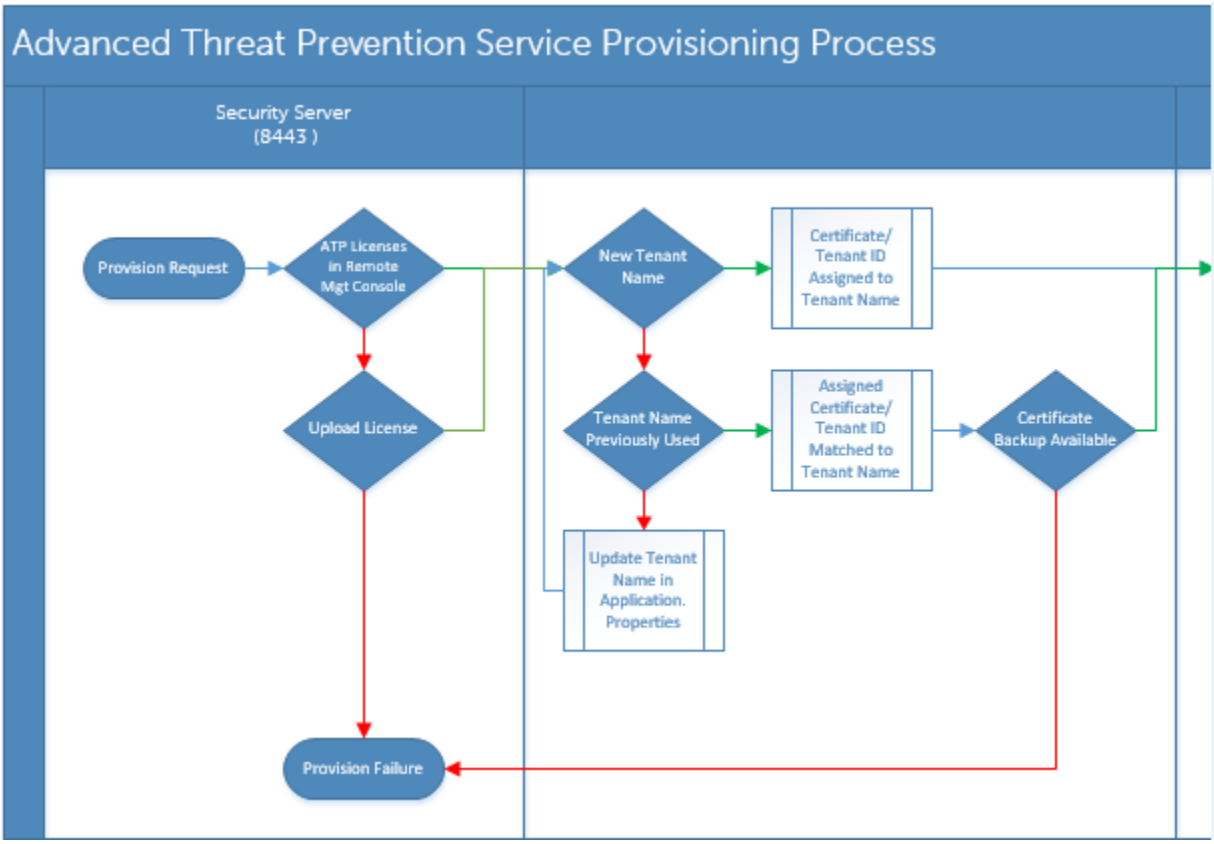
Bereitstellung eines Mandanten

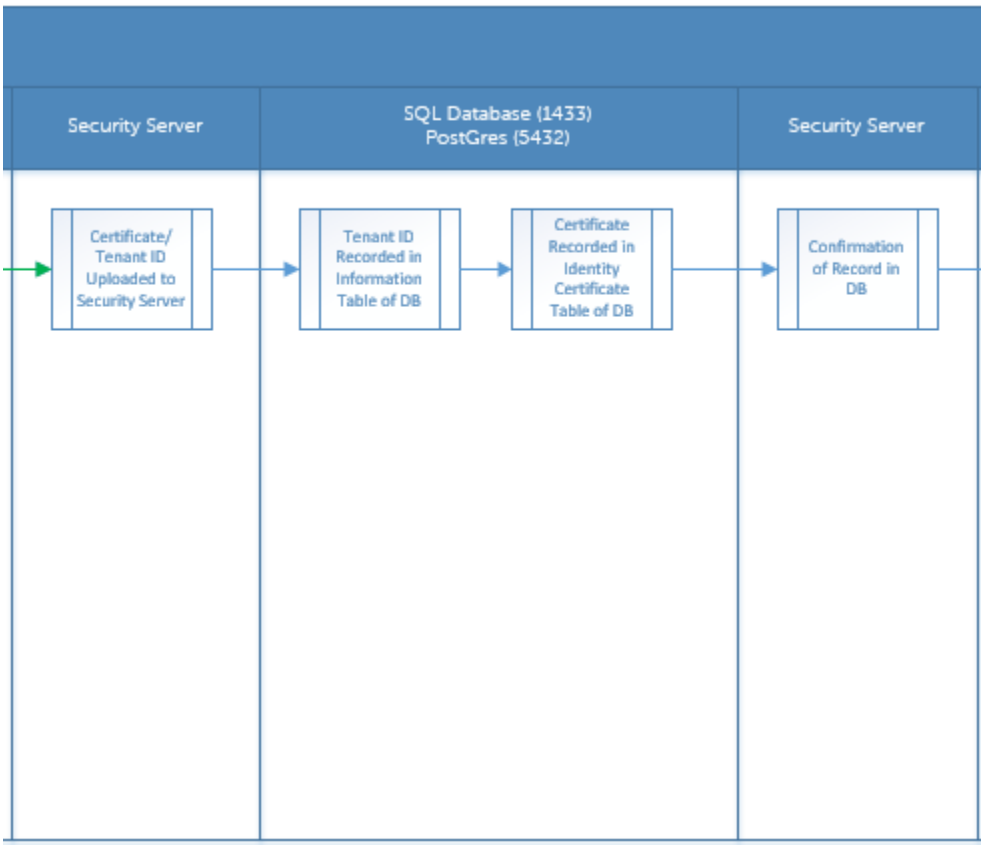
1 Melden Sie sich als Dell Administrator bei der Remote Management Console an.
2 Klicken Sie im linken Bereich der Verwaltungskonsole auf Verwaltung > Servicemanagement.
3 Klicken Sie auf **Advanced Threat Protection-Dienst einrichten**. Importieren Sie Ihre Advanced Threat Prevention Lizenzen, wenn zu diesem Zeitpunkt ein Fehler auftritt.
4 Die geführte Einrichtung beginnt, sobald die Lizenzen importiert wurden. Klicken Sie zum Starten auf **Weiter**.
5 Lesen Sie die EULA, stimmen Sie ihr zu und klicken Sie dann auf **Weiter**.
6 Geben Sie die Anmeldeinformationen für den Dell Server ein, um den Mandanten bereitzustellen. Klicken Sie auf **Weiter**. *Die Bereitstellung eines vorhandenen Mandanten der Marke Cylance wird nicht unterstützt.*
7 Laden Sie das Zertifikat herunter. Dies ist erforderlich, um eine Wiederherstellung im Falle von Notfallszenarien mit dem Dell Server durchzuführen. Dieses Zertifikat wird nicht automatisch gesichert. Sichern Sie das Zertifikat auf einem sicheren Speicherplatz auf einem anderen Computer. Aktivieren Sie das Kontrollkästchen, um zu bestätigen, dass Sie das Zertifikat gesichert haben, und klicken dann Sie auf **Weiter**.
8 Die Einrichtung ist abgeschlossen. Klicken Sie auf **OK**.

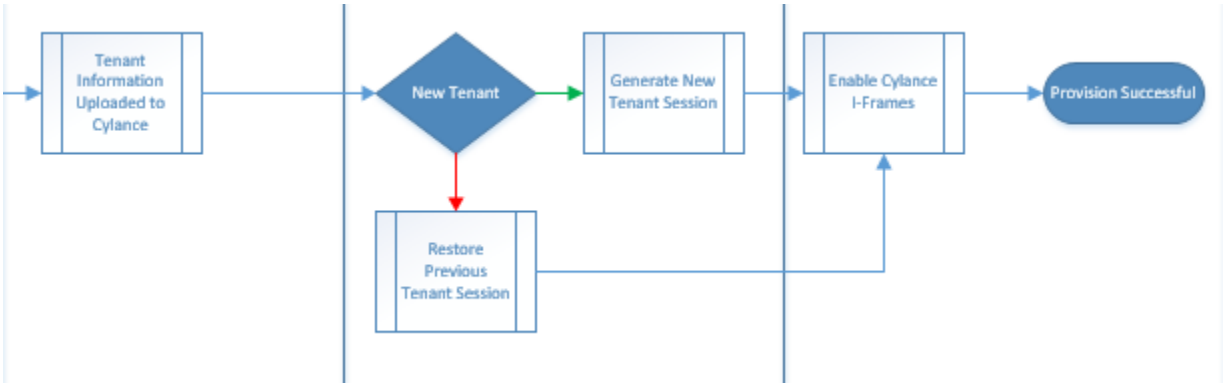
Fehlerbehebung bei Bereitstellung

Bereitstellung und Kommunikation mit Agenten

Die folgenden Diagramme veranschaulichen die Bereitstellung des Advanced Threat Prevention Dienstes.


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



Das folgende Diagramm veranschaulicht die Agentenkommunikation für Advanced Threat Prevention.