Endpoint Security Suite Enterprise for Linux

Guia do Administrador v2.1

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

2018 - 11

Rev. A01

Índice

1

Introdução

O Guia do administrador do Endpoint Security Suite Enterprise para Linux fornece as informações necessárias para instalar e implementar o software cliente.

Descrição geral

O Endpoint Security Suite Enterprise para Linux proporciona Advanced Threat Prevention no sistema operativo e nas camadas de memória, tudo isto gerido de forma central a partir do Dell Server. Com uma gestão centralizada, relatórios de conformidade consolidados e alertas de ameaças à consola, as organizações podem facilmente aplicar e comprovar a conformidade dos pontos terminais. Os conhecimentos em termos de segurança estão integrados em funcionalidades como políticas predefinidas e modelos de relatório que ajudam as empresas a reduzir os custos e a complexidade da gestão das TI.

Security Management Server ou Security Management Server Virtual - proporciona uma administração centralizada de políticas de segurança, integra-se nos diretórios existentes na empresa e cria relatórios. Neste documento, ambos os servidores estão assinalados como Dell Server, a não ser que seja necessário indicar uma versão específica (por exemplo, um procedimento que seja diferente ao utilizar o Security Management Server Virtual).

O Advanced Threat Prevention para Linux tem um ficheiro tar.gz, que contém os três RPM.

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

Para números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

2

Requisitos

Os requisitos de hardware e software do cliente são apresentados neste capítulo. Certifique-se de que o ambiente de implementação cumpre os requisitos antes de continuar as tarefas de implementação.

Hardware

A tabela seguinte apresenta o hardware mínimo suportado.

Hardware
• Pelo menos 500 MB de espaço livre em disco • 2 GB de RAM • Placa de rede 10/100/1000 ou Wi-Fi **NOTA: O protocolo IPv6 não é atualmente suportado.**

Software

A tabela seguinte lista os softwares suportados.

Sistemas operativos (kernels de 64 bits)
• CentOS Linux v7.1 - v7.5 • Red Hat Enterprise Linux v7.1 - v7.5

Portas

- A porta 443 (HTTPS) é utilizada para comunicação e deve estar aberta na firewall para que os agentes comuniquem com a consola de gestão. Se, por qualquer motivo, a porta 443 estiver bloqueada, não é possível transferir as atualizações, pelo que os computadores poderão não dispor da proteção mais recente. Certifique-se de que os computadores cliente conseguem aceder ao seguinte:

Utilizar	Protocolo de aplicação	Protocolo de transporte	Número da porta	Destino	Direção
Todas as comunicações	HTTPS	TCP	443	Todo o tráfego https para *.cylance.com	Porta de saída
Comunicação com o Core Server	HTTPS	TCP	8888	Permite a comunicação com o Core Server	Entrada/saída

- Para obter mais informações, consulte SLN303898.

Endpoint Security Suite Enterprise for Linux e dependências

O Endpoint Security Suite Enterprise for Linux utiliza Mono e dependências para instalar e ativar no SO Linux. O instalador irá transferir e instalar as dependências necessárias. Após a extração do pacote, é possível ver que dependências estão a ser utilizadas com o seguinte comando:

```
./showdeps.sh
```

Compatibilidade

A tabela que se segue detalha a compatibilidade com Windows, Mac e Linux.

n/a - a tecnologia não se aplica a esta plataforma.

Campo em branco – a política não é suportada com o Endpoint Security Suite Enterprise.

Funcionalidades	Políticas	Windows	macOS	Linux
Ações do ficheiro				
	Quarentena automática (não seguro)	x	x	x
	Quarentena automática (anormal)	x	x	x
	Carregamento automático	x	x	x
	Lista segura de políticas	x	x	x
Ações da memória				
	Proteção de memória	x	x	x
Exploração				
	Stack Pivot	x	x	x
	Proteção de pilha	x	x	x
	Substituir código	x	n/a	
	Scraping de RAM	x	n/a	
	Payload malicioso	x		
Injeção de processo				
	Alocação remota de memória	x	x	n/a
	Mapeamento remoto de memória	x	x	n/a
	Escrita remota na memória	x	x	n/a
	PE de Escrita remota para memória	x	n/a	n/a
	Substituir código remoto	x	n/a	

Funcionalidades	Políticas	Windows	macOS	Linux
	Anular mapeamento de memória remoto	x	n/a	
	Criação de threads remota	x	x	
	APC remoto agendado	x	n/a	n/a
	Injeção DYLD		x	x
Escalamento				
	Leitura de LSASS	x	n/a	n/a
	Alocação zero	x	x	
Definições de proteção				
	Controlo de execução	x	x	x
	Impedir o encerramento do serviço a partir do dispositivo	x	x	
	Termine processos não seguros em execução e respetivos subprocessos	x	x	x
	Deteção de ameaças em segundo plano	x	x	x
	Monitorizar para ver se há novos ficheiros	x	x	x
	Tamanho máximo de ficheiro de arquivo a verificar	x	x	x
	Excluir pastas específicas	x	x	x
	Copiar amostras de ficheiros	x		
Controlo da aplicação				
	Alterar janela	x		x
	Exclusões de pastas	x		
Definições do agente				
	Ativar o carregamento automático de ficheiros de registo	x	x	x
	Ativar notificações do ambiente de trabalho	x		
Controlo de script				
	Script ativo	x		
	Powershell	x		
	Macros do Office	x		n/a

Funcionalidades	Políticas	Windows	macOS	Linux
	Bloquear a utilização da Consola da Powershell	x		
	Aprovar scripts nestas pastas (e subpastas):	x		
	Nível de registo	x		
	Nível de autoproteção	x		
	Atualização automática	x		
	Executar uma deteção (a partir da IU do Agent)	x		
	Eliminar ficheiros em quarentena (IU do Agent UI e IU do Console)	x		
	Modo Desligado	x		x
	Dados detalhados da ameaça	x		
	Lista segura de certificados	x	x	n/a
	Copiar amostras de malware	x	x	x
	Definições de proxy	x	x	x
	Verificar política manualmente (IU do Agent)	x	x	

3

Tarefas

A instalação

Esta secção orienta-o através do Endpoint Security Suite Enterprise para a instalação do Linux.

Pré-requisitos

A Dell recomenda que sejam seguidas as melhores práticas de TI durante a implementação do software cliente. Estas incluem, entre outras, ambientes de teste controlados para os testes iniciais e a implementação progressiva para os utilizadores.

Antes de iniciar este processo, certifique-se que são observados os seguintes pré-requisitos:

- Certifique-se de que o Dell Server e os seus componentes já estão instalados.

  Se ainda não tiver instalado o Dell Server, siga as instruções apresentadas no respetivo guia abaixo.

  Guia de instalação e migração do Security Management Server

  Guia de instalação e Guia de início rápido do Security Management Server Virtual
- Certifique-se de que tem o nome do anfitrião e a porta do Dell Server. Ambos são necessários para a instalação do software cliente.
- Certifique-se de que o computador alvo dispõe de ligação de rede ao Dell Server.
- Se um certificado do servidor cliente faltar ou estiver autoatribuído, tem de desativar o certificado SSL fidedigno apenas no lado do cliente.

Instalação com linha de comandos

Para instalar o cliente Endpoint Security Suite Enterprise através da linha de comandos, siga os passos abaixo.

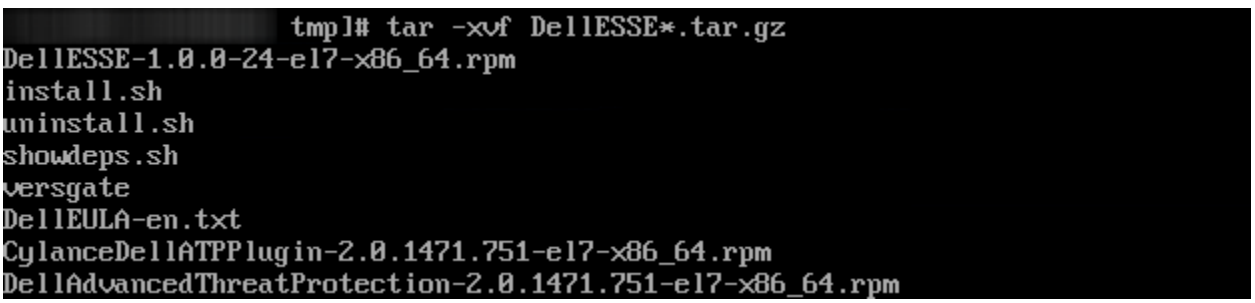
O comando **sudo** tem de ser utilizado para invocar os privilégios administrativos durante a instalação. Quando solicitado, introduza as suas credenciais.

A aprovação de impressão digital apenas é apresentada durante a primeira instalação.

1 Localize e faça o download do pacote de instalação (DellESSE-1.x.x-xxx.tar.gz) utilizando a sua conta FTP Dell.

2 Extraia o tar.gz utilizando o seguinte comando:

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



3 O seguinte comando executa o script de instalação para os RPM e as dependências necessários:

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

4 Em *Dell Security Management Server Host?* introduza o nome do anfitrião totalmente qualificado do Dell Server para gerir o utilizador pretendido. Por exemplo, server.organization.com.

5 Em *Dell Security Management Server Port?*, verifique se a porta está definida como 8888.

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

6 Quando solicitado, introduza **y** para instalar o pacote DellESSE e as respetivas dependências.

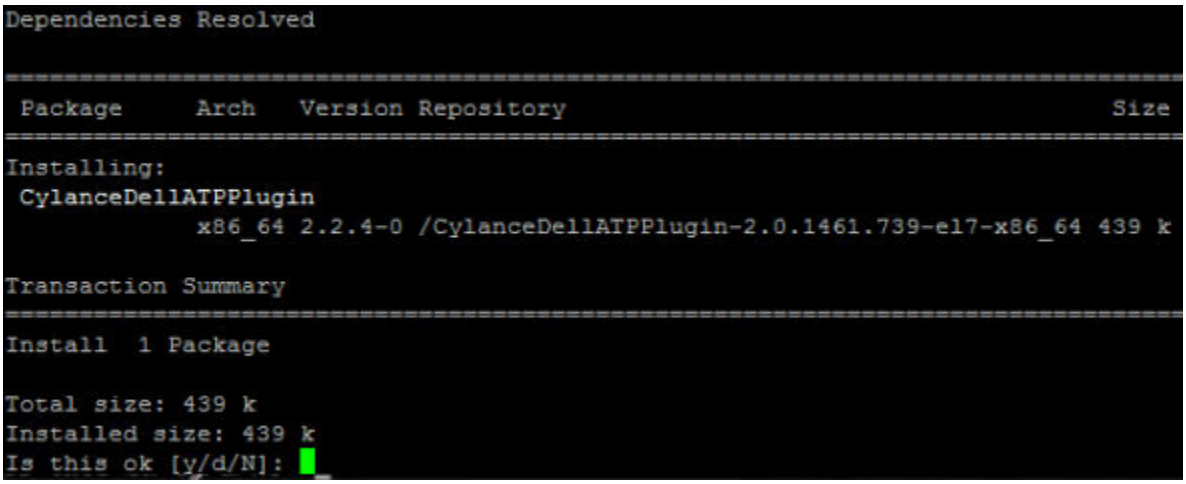
```
 libXfixes      x86_64 5.0.3-1.el7             base                       18
 libXrender     x86_64 0.9.10-1.el7            base                       26
 libXxf86vm     x86_64 1.1.4-1.el7             base                       18
 libexif        x86_64 0.6.21-6.el7            base                      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 Introduza **y** se for solicitada a aprovação por *impressão digital*.

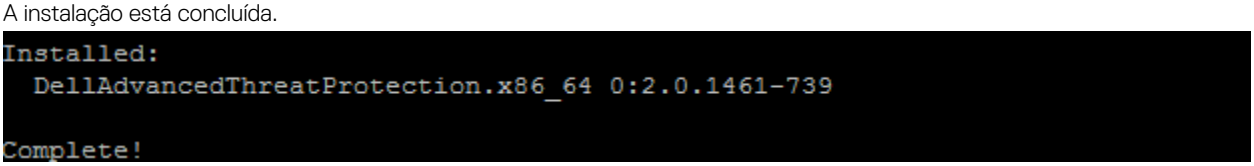
```
Total                                                   452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78 a7c2 7bbl 24c6 a8a7 f4a0 0eb5
 Package        : centos-release-7-3.1611.e17.centos.x86_64 (@anaconda)
 From           : /etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Is this ok [y/N]:
```

8 Quando solicitado, introduza **y** para instalar o pacote *DellAdvancedThreatProtection*.

9 Quando solicitado, introduza **y** para instalar o pacote *CylanceDellATPPlugin*.



10 A instalação está concluída.



11 Consulte Verificar a instalação do Endpoint Security Suite Enterprise para Linux.

Desinstalação por linha de comando

Para desinstalar o Endpoint Security Suite Enterprise para Linux utilizando a linha de comandos, siga os passos abaixo.

1 Aceder uma janela Terminal.

2 Desinstale o pacote utilizando o seguinte comando:

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

3 Prima **Enter**.

O Endpoint Security Suite Enterprise para Linux fica assim desinstalado e o computador pode ser utilizado normalmente.

Ver detalhes

Após instalar o Endpoint Security Suite Enterprise para Linux, este é reconhecido pelo Dell Server como um ponto terminal.

atp -t

O comando **atp - t** apresenta todas as ameaças detetadas no dispositivo e a ação adotada. As ameaças são uma categoria de eventos que são recém-detetados como ficheiros ou programas potencialmente inseguros e requerem uma correção orientada.

```
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 79D8C277F32CD176E4E2DD2198F730C9C79FA00A8F0158E0D519CEC1D860E222 /tmp/threats/LINUXRunni
ngApp
Quarantined B1BC7849F90FB403B9EDE88D40A92769D0AC20640B6A0D310FAF1D6B20E85F8A /tmp/threats/LINUXMaxAr
chive
Quarantined B31D57A77930E60FC151DEED085ED842423A172B4BED7702E33D4D09109BCCB6 /tmp/threats/LINUXGBL1
Quarantined F11C98AADB31D47AD571F6C0FA7F178A6413A8A7E84437098777 11FB1CA6E31F /tmp/threats/LINUXAutoB
lockExecution
```

Estas entradas indicam detalhes sobre as ações tomadas, o ID de hash e a localização da ameaça.

- **Não seguro** - Um ficheiro suspeito com probabilidade de ser malware
- **Anormal** - Um ficheiro suspeito que pode ser malware
- **Em quarentena** - Um ficheiro que foi movido da sua localização original, armazenado na pasta Quarentena e impedido de ser executado no dispositivo.
- **Dispensado** - Um ficheiro que pode ser executado no dispositivo.
- **Limpo** - Um ficheiro que tenha sido apagado dentro da organização. Os ficheiros autorizados incluem ficheiros Dispensados, adicionados à lista Segura e eliminados da pasta Quarentena num dispositivo.

Para mais informações sobre as classificações de ameaças no Advanced Threat Prevention, consulte *AdminHelp*, disponível na Remote Management Console do Dell Server.

Verificar a instalação

Opcionalmente, pode verificar que a instalação foi concluída com êxito.

- No cliente, aceda a uma janela Terminal.
- Antes de receber uma sequência de política, o cliente tem de se registar no Dell Server.
- O ficheiro */var/log/Dell/ESSE/DellAgent.00.log* inclui detalhes sobre a comunicação com o Dell Server e a interação do plug-in/serviço.

  O texto incluído confirma que o cliente recebeu políticas do Dell Server:

```
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%)
```

  O texto incluído confirma que o serviço da Dell foi interrompido para carregar o plug-in Advanced Threat Prevention:

```
//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
```

O texto incluído confirma os três Endpoint Security Suite Enterprise para os plug-ins Linux carregados:

```
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` - Inclui o seguinte:

- Estado de registo
- Número de série - Utilize esta função ao contactar o apoio técnico. Este é o identificador único da instalação.
- Política

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

O seguinte comando indica detalhes sobre as variáveis da linha de comando para o Endpoint Security Suite Enterprise para Linux:

`/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
```

O comando Advanced Threat Prevention *atp* é adicionado ao diretório */usr/sbin*, o qual é normalmente incluído numa variável PATH de shell, para que possa ser utilizado na maioria dos casos sem um caminho explícito.

Resolução de problemas

Desativar o certificado fidedigno SSL

Se um certificado do servidor do computador faltar ou estiver autoatribuído, tem de desativar o certificado SSL fidedigno apenas no lado do cliente.

Se estiver a utilizar um certificado invulgar, importe o certificado de raiz para o Arquivo de Certificados do Linux e, em seguida, reinicie o Endpoint Security Suite para serviços Linux com o seguinte comando: `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Aceder uma janela Terminal.

2 Introduza o caminho para CsfConfig.app:
```
/usr/lib/dell/esse/CsfConfig
```

3 Execute o ficheiro CsfConfig.app:
```
sudo ./CsfConfig
```

São apresentadas as seguintes predefinições:

Definições atuais:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = False

DumpXmlInventory = False

DumpPolicies = False

4 Digite **-help** para ver a lista das opções.

5 Para desativar o certificado fidedigno SSL no computador de destino, introduza o seguinte comando:

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

Adicionar inventário XML e alterações de políticas à pasta de registos

Para adicionar os ficheiros inventory.xml ou policies.xml à pasta Registos:

1 Execute a *CsfConfig.app* conforme descrito acima.

2 Para alterar *DumpXmlInventory* para *True*, introduza o seguinte comando:

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

3 Para alterar *DumpPolicies* para *True*, introduza o seguinte comando:

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

Os ficheiros de políticas só são descartados se tiver ocorrido uma alteração à política.

4 Para ver os ficheiros de registos inventory.xml e policies.xml, aceda a */var/log/Dell/Dell Data Protection*.

NOTA: As alterações a CsfConfig podem não ser aplicadas imediatamente.

Recolher ficheiros de registo

Os registos do Endpoint Security Suite Enterprise for Linux encontram-se na seguinte localização: */var/log/Dell/ESSE*. Para gerar registos, utilize o seguinte comando: **./getlogs.sh**

Para obter mais informações sobre como recolher os registos, consulte SLN303924.

Configurar um inquilino

Deve ser aprovisionado um inquilino no Dell Server antes da ativação da aplicação de políticas do Advanced Threat Prevention.

Pré-requisitos

- Tem de ser efetuado por um administrador com função de administrador de sistema.
- Deve ter ligação à Internet para configuração no Dell Server.
- Tem de ter ligação à Internet no cliente para visualizar a integração do serviço online do Advanced Threat Prevention na Management Console.
- A configuração tem como base um token que é gerado a partir de um certificado durante a configuração.
- As licenças do Advanced Threat Prevention devem estar presentes no Dell Server.

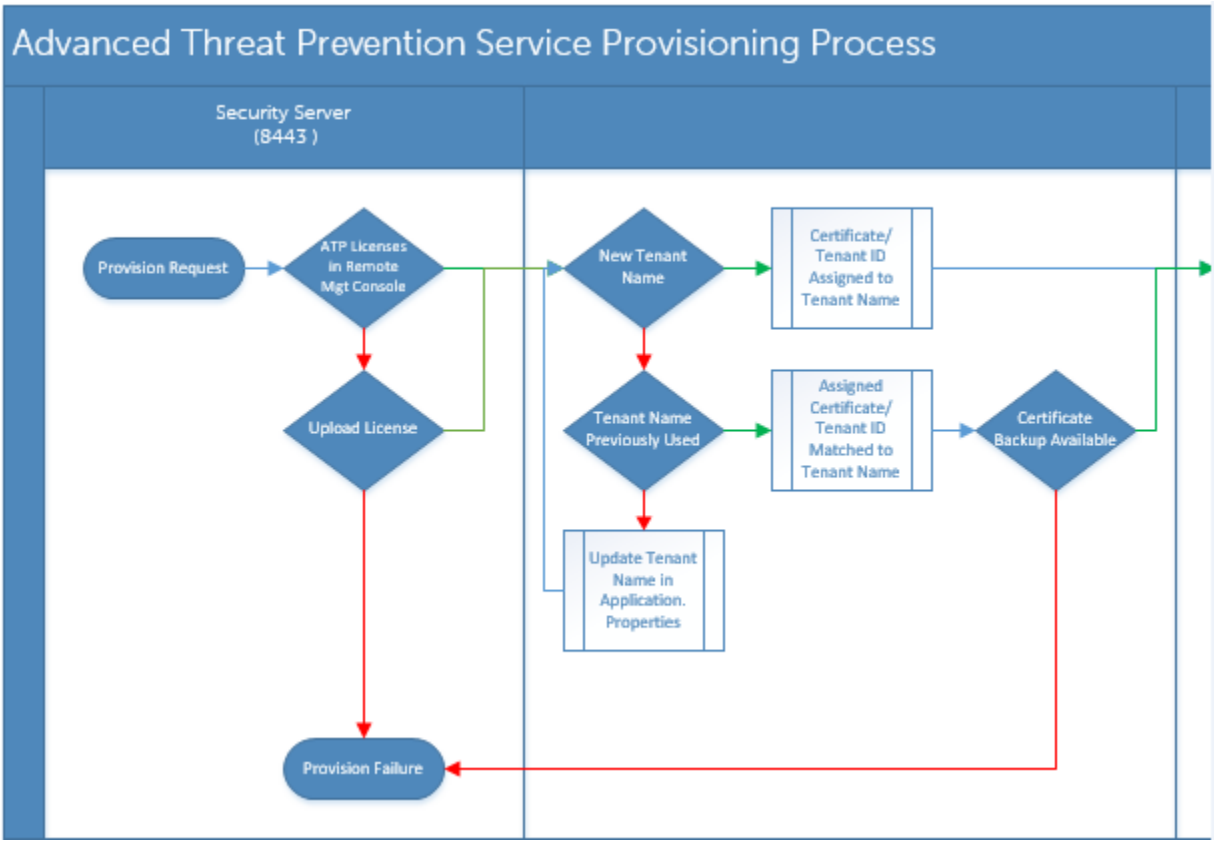
Configurar um inquilino

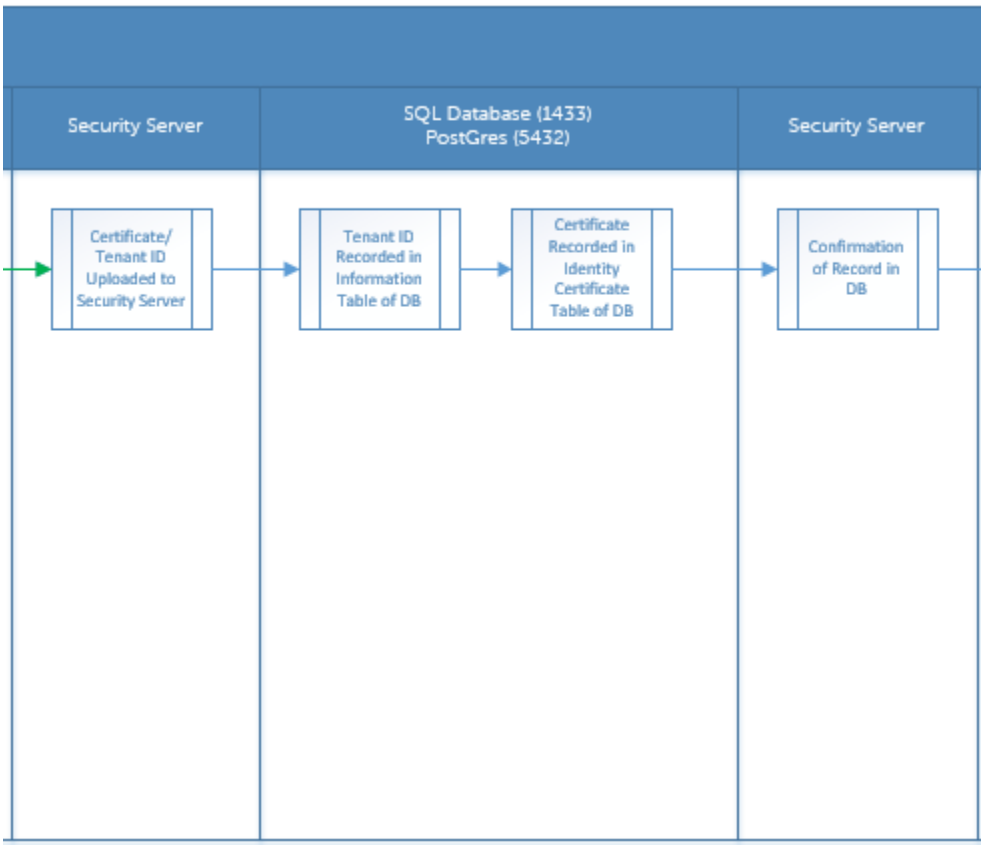
1 Como Administrador Dell, inicie sessão na Remote Management Console.
2 No painel esquerdo da Management Console, clique em **Gestão > Gestão de serviços**.
3 Clique em **Configurar serviço Advanced Threat Protection**. Se ocorrer qualquer falha neste momento, importe as suas licenças Advanced Threat Prevention.
4 A configuração com assistente é iniciada imediatamente após as licenças serem importadas. Clique em **Seguinte** para começar.
5 Leia e aceite o EULA e clique em **Seguinte**.
6 Disponibilize credenciais de identificação no Dell Server para configuração do Inquilino. Clique em **Seguinte**. *A configuração de um Inquilino existente da marca Cylance não é suportada.*
7 Transfira o Certificado. Este é necessário para recuperação em caso de desastres no Dell Server. Não é efetuada uma cópia de segurança deste Certificado. Efetue uma cópia de segurança do Certificado numa localização segura num computador diferente. Selecione a caixa de verificação para confirmar que efetuou uma cópia de segurança do Certificado e clique em **Seguinte**.
8 A configuração está concluída. Clique em **OK**.

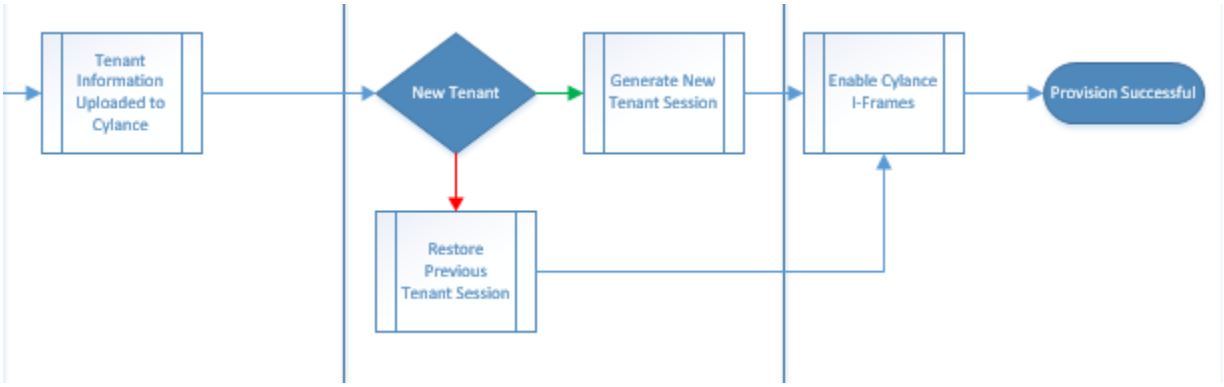
Solução de problemas de aprovisionamento

Aprovisionamento e comunicação do agente

Os diagramas seguintes ilustram o processo de aprovisionamento do serviço do Advanced Threat Prevention.


Advanced Threat Prevention Service Provisioning Process
Security Server
(8443)
Provision Request
ATP Licenses in Remote Mgt Console
Upload License
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
Provision Failure


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



O diagrama seguinte ilustra o processo de comunicação do agente do Advanced Threat Prevention.