Endpoint Security Suite Enterprise for Linux

Guia do administrador v2.1

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam você a usar melhor o seu produto.

AVISO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica possíveis danos à propriedade, risco de lesões corporais ou mesmo risco de vida.

2018 - 11

Rev. A01

Índice

1 Introdução....4
Visão geral....4
Entre em contato com o Dell ProSupport....4

2 Requisitos....5
Hardware....5
Software....5
Portas....5
Endpoint Security Suite Enterprise for Linux e dependências....6
Compatibilidade....6

3 Tarefas....9
A instalação....9
Pré-requisitos....9
Instalação por linha de comando....9
Exibir detalhes....11
Verificar instalação....12
Solução de problemas....14
Desativar Certificado de confiança SSL....14
Adicionar Inventário de XML e Alterações nas políticas à pasta Logs....14
Coletar arquivos de log....15
Provisionar um locatário....15
Provisionar um locatário....15
Solução de problemas de provisionamento....15
Provisionamento e comunicação do agente....15

1

Introdução

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

Visão geral

O Endpoint Security Suite Enterprise para Linux oferece o Advanced Threat Prevention no sistema operacional e nas camadas de memória, tudo com gerenciamento centralizado pelo Dell Server. Com gerenciamento centralizado, relatórios de conformidade consolidados e alertas de ameaças ao console, as empresas podem facilmente reforçar e comprovar a conformidade em todos os endpoints. A experiência em segurança está integrada a recursos, como modelos predefinidos de políticas e relatórios, para ajudar as empresas a reduzirem os custos de gerenciamento e a complexidade de TI.

Servidor de gerenciamento de segurança ou Servidor de gerenciamento de segurança virtual - fornece administração centralizada da política de segurança, integra-se a diretórios existentes da empresa e cria relatórios. Para a finalidade deste documento, ambos os servidores são citados como Dell Server, a menos que uma versão específica precise ser citada (por exemplo, um procedimento é diferente ao ser usado o Servidor de gerenciamento de segurança virtual).

O Advanced Threat Prevention para Linux tem um arquivo tar.gz que contém os três RPMs.

Entre em contato com o Dell ProSupport

Ligue para 877-459-7304, extensão 4310039 para obter suporte por telefone, 24 horas por dia, 7 dias na semana, para o seu produto Dell.

Há também disponível o serviço de suporte on-line para os produtos Dell no site dell.com/support. O suporte on-line inclui drivers, manuais, orientações técnicas, perguntas frequentes e problemas emergentes.

Quando telefonar, tenha em mãos a Etiqueta de serviço ou Código de serviço expresso, para nos ajudar a garantir que possamos direcioná-lo rapidamente ao especialista técnico correto.

Para obter os números de telefone fora dos Estados Unidos, veja Números de telefone internacionais do Dell ProSupport.

2

Requisitos

Os requisitos de hardware e software de cliente são apresentados neste capítulo. Verifique se o ambiente de implementação atende aos requisitos antes de continuar com as tarefas de implementação.

Hardware

A tabela a seguir detalha o hardware mínimo suportado.

Hardware

- Ao menos 500 MB de espaço livre em disco
- 2 GB de RAM
- Placa de interface de rede 10/100/1000 ou Wi-Fi

NOTA: IPv6 não é suportado atualmente.

Software

A tabela a seguir detalha os softwares suportados.

Sistemas operacionais (kernels de 64 bits)

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

Portas

- A porta 443 (https) é usada para a comunicação e precisa estar aberta no firewall para que os agentes consigam se comunicar com o Console de gerenciamento. Se a porta 443 estiver bloqueada por algum motivo, não será possível fazer o download das atualizações, de modo que os computadores podem não ter a proteção mais atual. Certifique-se de que os computadores cliente possam acessar:

Uso	Protocolo de aplicativo	Protocolo de transporte	Número da porta	Destino	Direção
Toda a comunicação	HTTPS	TCP	443	Permitir todo o tráfego https para *.cylance.com	Saída
Comunicação com o Dell Core Server	HTTPS	TCP	8888	Permite a comunicação com o Dell Core Server	Entrada/Saída

- Para obter informações adicionais, consulte SLN303898.

Endpoint Security Suite Enterprise for Linux e dependências

O Endpoint Security Suite Enterprise for Linux usa Mono e dependências para instalar e ativar no SO Linux. O instalador irá baixar e instalar as dependências obrigatórias. Após a extração do pacote, você poderá ver quais dependências estão sendo utilizadas usando o seguinte comando:

```
./showdeps.sh
```

Compatibilidade

A tabela a seguir detalha a compatibilidade com Windows, Mac e Linux.

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

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

Recursos	Políticas	Windows	macOS	Linux
Ações de arquivo				
	Quarentena automática (insegura)	x	x	x
	Quarentena automática (anormal)	x	x	x
	Upload automático	x	x	x
	Lista de arquivos seguros da política	x	x	x
Ações de memória				
	Proteção de memória	x	x	x
Vulnerabilidade				
	Stack Pivot	x	x	x
	Proteção de pilha	x	x	x
	Substituir código	x	n/d	
	RAM Scraping	x	n/d	
	Carga mal-intencionada	x		
Injeção de processo				
	Alocação remota de memória	x	x	n/d
	Mapeamento remoto de memória	x	x	n/d
	Gravação remota na memória	x	x	n/d
	Gravação remota de PE na memória	x	n/d	n/d

Recursos	Políticas	Windows	macOS	Linux
	Substituir código remoto	x	n/d	
	Cancelamento remoto de mapeamento de memória	x	n/d	
	Criação remota de thread	x	x	
	APC remoto agendado	x	n/d	n/d
	Injeção DYLD		x	x
Escalonamento				
	Leitura de LSASS	x	n/d	n/d
	Alocamento zero	x	x	
Configurações de proteção				
	Controle de execução	x	x	x
	Prevenção contra desligamento do serviço a partir do dispositivo	x	x	
	Eliminar processos e subprocessos inseguros em execução	x	x	x
	Detecção de ameaças em segundo plano	x	x	x
	Inspecionar se há novos arquivos	x	x	x
	Tamanho máximo do arquivo morto a ser verificado	x	x	x
	Excluir pastas específicas	x	x	x
	Cópia de amostras de arquivo	x		
Controle de aplicativos				
	Alterar janela	x		x
	Exclusões de pasta	x		
Configurações do agente				
	Habilitar upload automático de arquivos de log	x	x	x
	Habilitar notificações da área de trabalho	x		
Controle de scripts				
	Script ativo	x		
	Powershell	x		
	Macros do Office	x		n/d

Recursos	Políticas	Windows	macOS	Linux
	Bloquear uso do console do PowerShell	x		
	Aprovar scripts nessas pastas (e subpastas)	x		
	Nível de registro	x		
	Nível de autoproteção	x		
	Atualização automática	x		
	Executar uma detecção (pela UI do agente)	x		
	Apagar quarentena (UI do agente e UI do console)	x		
	Modo desconectado	x		x
	Dados detalhados de ameaça	x		
	Lista segura de certificados	x	x	n/d
	Copiar amostras de malware	x	x	x
	Configurações do proxy	x	x	x
	Verificação manual de política (UI do agente)	x	x	

3

Tarefas

A instalação

Esta seção irá guiá-lo durante a instalação do Endpoint Security Suite Enterprise para Linux.

Pré-requisitos

A Dell recomenda que as boas práticas de TI sejam seguidas durante a implantação do software cliente. Isso inclui, entre outros, ambientes de teste controlados para testes iniciais e implantações escalonadas para os usuários

Antes de iniciar este processo, confirme que os seguintes pré-requisitos sejam atendidos:

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

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

  Servidor de gerenciamento de segurança Installation and Migration Guide (Guia de instalação e migração do Servidor de gerenciamento de segurança)

  Servidor de gerenciamento de segurança virtual Quick Start Guide and Installation Guide (Guia de instalação e de início rápido do Servidor de gerenciamento de segurança virtual)
- Certifique-se de ter o nome do host e a porta do Dell Server. Os dois serão necessários para a instalação do software cliente.
- Confirme se o computador de destino tem conectividade de rede com o Dell Server.
- Se um certificado do servidor do cliente estiver faltando ou for autoassinado, será preciso desativar o certificado de confiança SSL apenas no lado do cliente.

Instalação por linha de comando

Para instalar o cliente Endpoint Security Suite Enterprise usando a linha de comando, siga as etapas abaixo.

O comando **sudo** deve ser usado para invocar privilégios administrativos durante a instalação. Quando solicitado, digite suas credenciais.

A aprovação da impressão digital é exibida somente durante a primeira instalação.

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

2 Extraia o tar.gz usando o seguinte comando:

```
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 O comando a seguir executa o script de instalação para os RPMs e dependências obrigatórios:

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

4 Em *Dell Security Management Server Host?* insira o nome completo qualificado do host do Dell Server para gerenciar o usuário de destino. 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? [redacted]
Dell Security Management Server Port?
```

6 Digite **y** quando solicitado para instalar o pacote DellESSE e suas dependências.

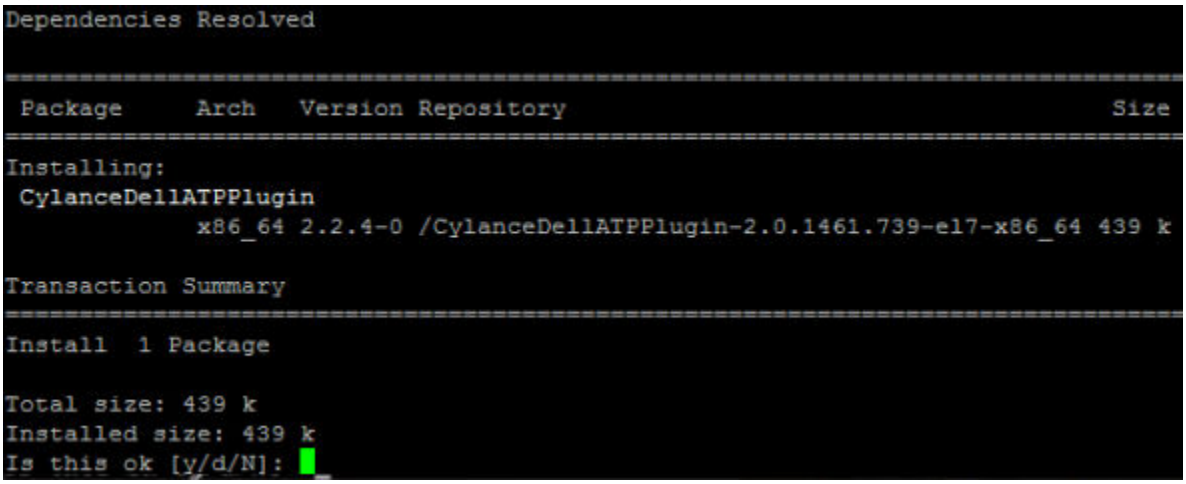
```
 libXfixes      x86_64 5.0.3-1.el7              base                       18 k
 libXrender     x86_64 0.9.10-1.el7             base                       26 k
 libXxf86vm     x86_64 1.1.4-1.el7              base                       18 k
 libexif        x86_64 0.6.21-6.el7             base                      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 Digite **y**, se solicitado, para a aprovação da *Impressão digital*.

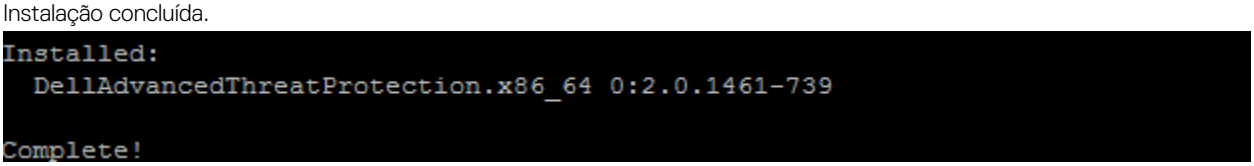
```
Total                                                452 kB/s | 4.9 MB 00:00:11
Retrieving key from file:///etc/pki/rpm-gpg/RPM-GPG-KEY-CentOS-7
Importing GPG key 0xF4A80EB5:
 Userid         : "CentOS-7 Key (CentOS 7 Official Signing Key) <security@centos.org>"
 Fingerprint    : 6341 ab27 53d7 8a78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

8 Digite **y** quando solicitado para instalar o pacote *DellAdvancedThreatProtection*.

9 Digite **y** quando solicitado para instalar o pacote *CylanceDellATPPlugin*.



10 Instalação concluída.



11 Consulte Verificar Endpoint Security Suite Enterprise para instalação no Linux.

Desinstalação por linha de comando

Para desinstalar o Endpoint Security Suite Enterprise para Linux usando a linha de comando, siga as etapas abaixo.

1 Acesse uma janela de terminal.

2 Desinstale o pacote usando o seguinte comando:

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

3 Pressione **Enter**.

O Endpoint Security Suite Enterprise para Linux agora está desinstalado e o computador pode ser usado normalmente.

Exibir detalhes

Após o Endpoint Security Suite Enterprise para Linux ser instalado, ele é reconhecido pelo Dell Server como um endpoint.

atp -t

O comando **atp - t** exibe todas as ameaças detectadas no dispositivo e a ação tomada. Ameaças são uma categoria de eventos recém-detectados como arquivos ou programas potencialmente inseguros e exigem correção orientada.

Essas entradas detalham a ação tomada, a ID hash e a localização da ameaça.

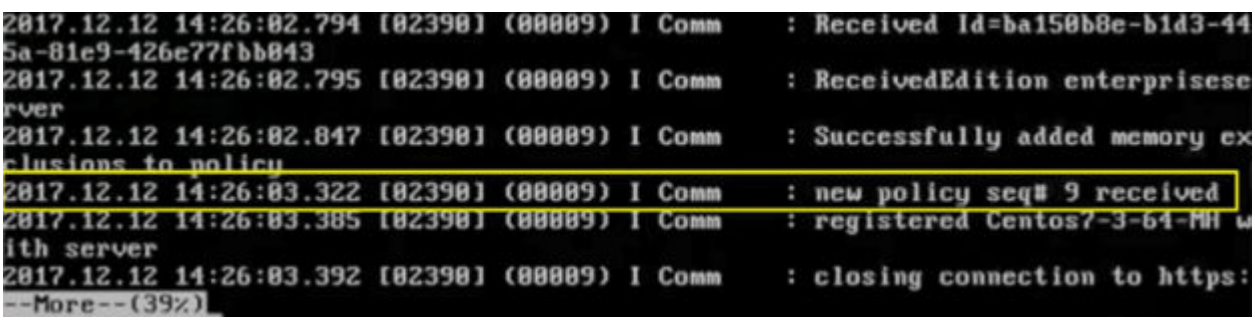
- **Não seguro** - um arquivo suspeito que provavelmente é malware
- **Anormal** - um arquivo suspeito que pode ser malware
- **Em quarentena** - um arquivo movido do seu local original, armazenado na pasta Quarentena e impedido de ser executado no dispositivo.
- **Dispensado** - um arquivo que pode ser executado no dispositivo.
- **Limpo** - Um arquivo que foi limpo dentro da organização. Dentre os arquivos limpos, estão arquivos dispensados, adicionados à lista Segura e excluídos da pasta Quarentena do dispositivo.

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

Verificar instalação

Opcionalmente, você pode verificar se a instalação foi bem-sucedida.

- No cliente, acesse uma janela Terminal.
- Antes de uma sequência de política ser recebida, o cliente registra-se com o Dell Server.
- O arquivo */var/log/Dell/ESSE/DellAgent.00.log* detalha a comunicação com Dell Server e a interação plugin/serviço.
  O texto entre colchetes confirma que o cliente tenha recebido as políticas do Dell Server:



  O texto entre colchetes confirma que o serviço da Dell foi interrompido para carregar o plugin 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 entre colchetes confirma que os três plugins do Endpoint Security Suite Enterprise para Linux foram 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:

- Status do registro
- Número de série - Use quando entrar em contato com o serviço de suporte. Esse é o identificador exclusivo 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 comando a seguir detalha 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 *atp* do Advanced Threat Prevention é adicionado ao diretório */usr/sbin*, que é normalmente incluído em uma variável de CAMINHO da shell, para que ele possa ser usado na maioria dos casos sem um caminho explícito.

Solução de problemas

Desativar Certificado de confiança SSL

Se um certificado do servidor do cliente estiver faltando ou for autoassinado, será preciso desativar o certificado de confiança SSL apenas no lado do cliente.

Se você estiver usando um certificado raro, importe o certificado raiz para o Armazenamento de certificados Linux, depois a Suíte Endpoint Security para serviços Linux com o seguinte comando: `/usr/lib/dell/esse/agentservicecmd.sh restart`

1 Acesse uma janela de terminal.
2 Digite o caminho para o aplicativo CsfConfig:
`/usr/lib/dell/esse/CsfConfig`
3 Execute o CsfConfig.app:
`sudo ./CsfConfig`

O seguinte é exibido com as configurações padrão:

Configurações atuais:

ServerHost = deviceserver.company.com

ServerPort = 8888

DisableSSLCertTrust = Falso

DumpXmlInventory = Falso

DumpPolicies = Falso
4 Digite **-help** para listar as opções.
5 Para desativar Certificado de confiança SSL no computador de destino, digite o seguinte comando:

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

Adicionar Inventário de XML e Alterações nas políticas à pasta Logs

Para adicionar os arquivos inventory.xml ou policies.xml à pasta Logs:

1 Execute o CsfConfig.app conforme descrito acima.
2 Para alterar *DumpXmlInventory* para *Verdadeiro*, digite o seguinte comando:

```
sudo /usr/lib/dell/esse/CsfConfig -dumpinventory true
```
3 Para alterar *DumpPolicies* para *Verdadeiro*, digite o seguinte comando:

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

Arquivos de políticas só serão despejados se tiver ocorrido uma alteração na política.
4 Para visualizar os arquivos de log inventory.xml e policies.xml, acesse */var/log/Dell/Dell Data Protection*.

NOTA: Alterações em CsfConfig podem não ser aplicadas imediatamente.

Coletar arquivos de log

Os logs do Endpoint Security Suite Enterprise estão localizados em: */var/log/Dell/ESSE*. Para gerar logs, use o seguinte comando: **./getlogs.sh**

Para obter informações sobre como coletar os logs, consulte SLN303924.

Provisionar um locatário

Um locatário precisa ser provisionado no Dell Server para que a imposição de políticas do Advanced Threat Prevention possa ser ativada.

Pré-requisitos

- Precisa ser realizado por um administrador com a função de administrador do sistema.
- É necessária conectividade com a Internet para provisionar no Dell Server.
- É necessária conectividade do cliente com a Internet para exibir a integração do serviço online do Advanced Threat Prevention no Management Console.
- O provisionamento é baseado em um token gerado a partir de um certificado durante o provisionamento.
- As licenças do Advanced Threat Prevention precisam estar presentes no Dell Server.

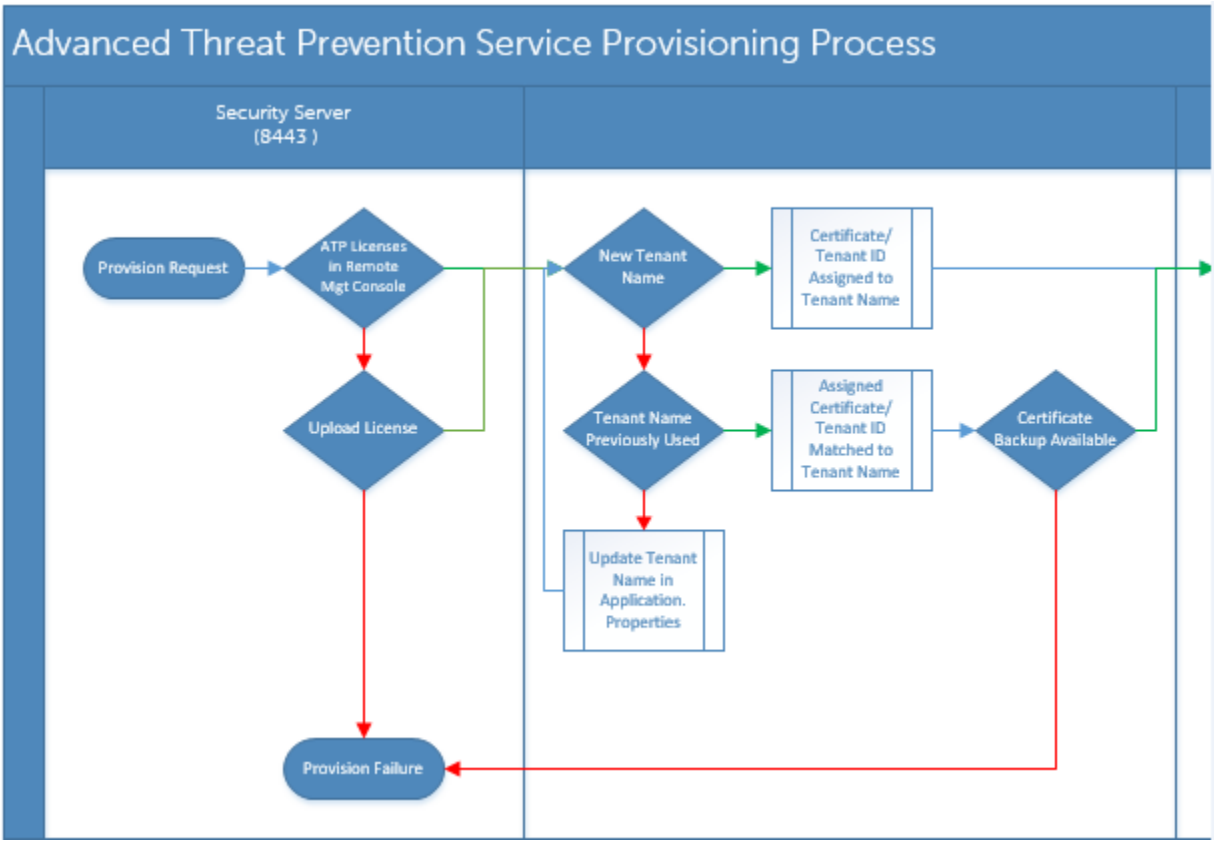
Provisionar um locatário

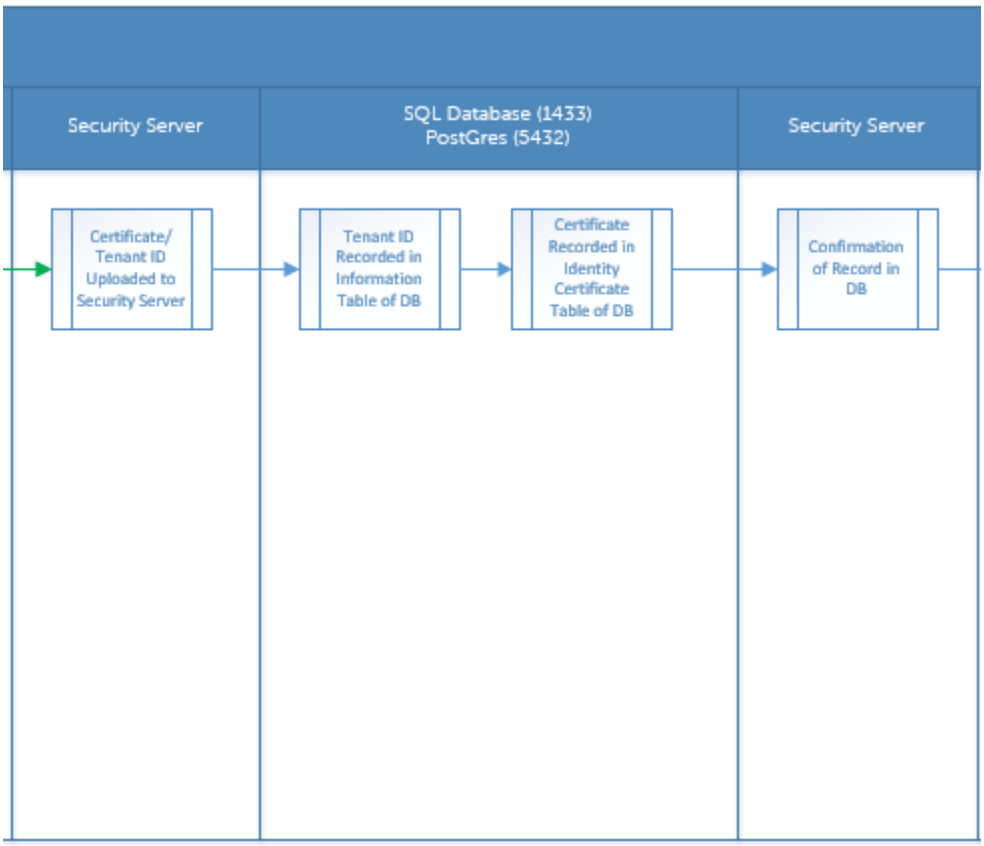
1. Como um administrador Dell, faça login no Remote Management Console.
2. No painel esquerdo do Management Console, clique em **GerenciamentoGerenciamento de serviços**.
3. Clique em **Configurar o serviço Advanced Threat Protection**. Importe as licenças do Advanced Threat Prevention, caso ocorra uma falha nesse ponto.
4. A instalação guiada começa logo após a importação das licenças. Clique em **Avançar** para começar.
5. Leia e concorde com o EULA e clique em **Avançar**.
6. Forneça credenciais de identificação ao Dell Server para provisionamento do Usuário. Clique em **Avançar**. *Não há suporte para o provisionamento de um usuário existente da marca Cylance.*
7. Baixe o certificado. Isso é necessário para a recuperação se ocorrer um desastre com o Dell Server. O backup deste certificado não é feito automaticamente. Faça backup do certificado em um local seguro em outro computador. Marque a caixa de seleção para confirmar que você fez o backup do Certificado e clique em **Avançar**.
8. A configuração foi concluída. Clique em **OK**.

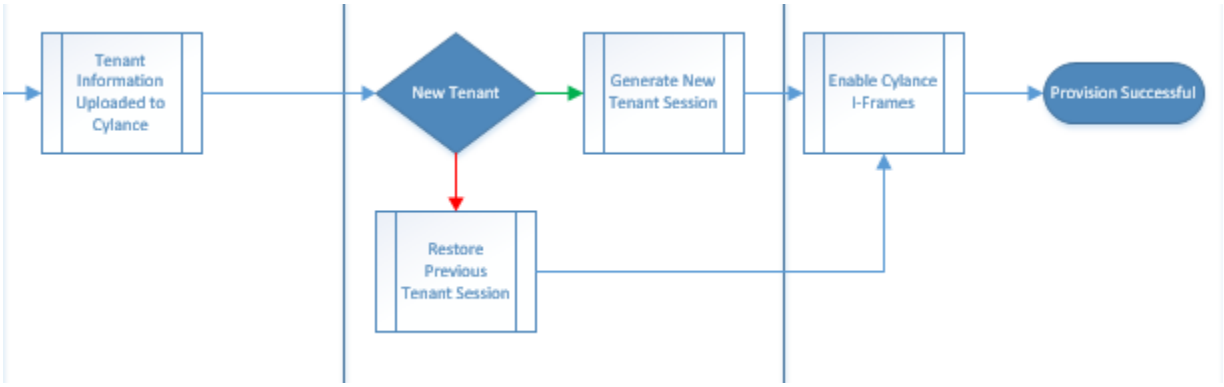
Solução de problemas de provisionamento

Provisionamento e comunicação do agente

Os diagramas a seguir ilustram o processo de provisionamento do serviço 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 a seguir ilustra o processo de comunicação do agente do Advanced Threat Prevention.