Guia do Cliente do Symantec™ Endpoint Protection 14.3 RU3 for Linux - Portuguese - Brazil

September 2021

Table of Contents

Como proteger dispositivos Linux com o Symantec Endpoint Protection..... 3

- **Sobre o Symantec Agent for Linux.....3**
- **Requisitos de sistema do Symantec Agent for Linux..... 3**
- **Como instalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux.....4**
- **Introdução ao agente do Linux..... 6**
- **Como fazer upgrade do agente do Linux da Symantec..... 7**
- **Como atualizar os módulos de kernel para o agente do Linux da Symantec.....8**
- **Como gerenciar o cliente Linux usando a ferramenta de linha de comando (sav)..... 9**
- **Como solucionar problemas do agente do Linux da Symantec..... 11**
- **Como desinstalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux..... 12**

Como proteger dispositivos Linux com o Symantec Endpoint Protection

Sobre o Symantec Agent for Linux

O Symantec Agent for Linux protege seus dispositivos Linux contra ameaças, riscos e vulnerabilidades decorrentes de malwares. Ele protege seus dispositivos Linux de forma proativa contra malwares conhecidos e desconhecidos.

Os recursos antimalware consistem no **Antimalware** (AMD) que protege os dispositivos Linux contra softwares maliciosos, como vírus, spyware, ransomware, etc., e o **Auto-Protect** (AP), que detecta ameaças maliciosas quando um aplicativo é iniciado.

A Symantec recomenda que o Auto-Protect seja ativado para garantir a proteção em tempo real. Qualquer malware detectado é colocado em quarentena imediatamente. Se você desativar o Auto-Protect, ainda será possível detectar malware executando uma verificação por demanda.

Introdução ao agente do Linux

Requisitos de sistema do Symantec Agent for Linux

Esta seção inclui os requisitos do sistema para a versão mais recente.

Para os requisitos do sistema para versões anteriores do Symantec Endpoint Protection, ou para a versão mais recente desses requisitos do sistema, consulte a seguinte página da Web:

Notas de versão, novas correções e requisitos do sistema para todas as versões do Endpoint Protection

Table 1: Requisitos de sistema do Symantec Agent for Linux

Componente	Requisitos
Hardware	• Processador Intel Pentium 4 (2 GHz) ou posterior • 500 MB de RAM disponível (o recomendado é 4 GB de RAM) • 2 GB de espaço disponível no disco se `/var`, `/opt` e `/tmp` compartilharem o mesmo sistema de arquivos/volume • 500 MB de espaço disponível no disco em cada uma (`/var`, `/opt` e `/tmp`), caso estejam em volumes diferentes
Sistemas operacionais	• Amazon Linux 2 • CentOS 6, 7, 8 • Debian 9, 10 • Oracle Enterprise Linux 6, 7, 8 • Red Hat Enterprise Linux 6, 7, 8 • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 14.04 LTS, 16.04 LTS, 18.04 LTS, 20.04 LTS Para ver uma lista de kernels de sistema operacional aceitos, consulte Supported Linux kernels for Symantec Endpoint Protection (em inglês).

Componente	Requisitos
Outros requisitos ambientais	• Glibc Nenhum sistema operacional que execute uma versão do glibc anterior à 2.6 é compatível. • net-tools ou iproute2 O Symantec Endpoint Protection usa uma dessas duas ferramentas, dependendo do que já está instalado no computador. • OpenSSL 1.0.2k-fips ou posteriores

Como instalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux

(Para 14.3 RU1 e posterior)

Instale o agente do Linux da Symantec diretamente em um dispositivo Linux. É possível implementar remotamente o agente Linux pelo Symantec Endpoint Protection Manager.

Para instalar o agente do Linux da Symantec, crie um pacote de instalação no Symantec Endpoint Protection Manager, transfira esse pacote para um dispositivo Linux e, em seguida, execute o instalador. O instalador configurará o novo agente e o registrará com no Symantec Endpoint Protection Manager.

NOTE
O agente do Linux da Symantec 14.3 RU1 e posterior não podem ser executados como um cliente não gerenciado. Todas as tarefas de gerenciamento devem ser executadas no Symantec Endpoint Protection Manager ou no console da nuvem.

Versão 14.3 RU1 e posterior: para instalar o agente do Linux da Symantec

1. No Symantec Endpoint Protection Manager, crie e baixe o pacote de instalação.
2. Coloque o pacote em um compartilhamento de rede, dispositivo USB ou outro mecanismo de compartilhamento.
   Se os dispositivos em que deseja instalar o agente do Linux estiverem em uma rede isolada ou não tiverem acesso à internet, configure um repositório local.Consulte:
   Como criar um repositório local
3. Instale o agente do Linux usando uma destas opções:

Se você transferiu o pacote para o dispositivo Linux	1. Vá até o local da pasta e execute o seguinte comando para transformar o arquivo **LinuxInstaller** em executável:
	`chmod u+x LinuxInstaller`
	2. Execute o seguinte comando para instalar o agente:
	`./LinuxInstaller`

Se você configurou um repositório local	1. Execute o seguinte comando:
	`./LinuxInstaller – --local-repo <URL do repositório LOCAL>`
	Por exemplo:
	`./LinuxInstaller – --local-repo https://your-domain.com/sep_linux_agent/14_3RU3`

   Você deve executar o comando como raiz.
   Para exibir a lista de opções de instalação, execute `./LinuxInstaller -h`.
4. Para verificar a instalação, vá para `/usr/lib/symantec` e execute o `./status.sh` para confirmar se os módulos estão carregados e se os daemons estão em execução:

```
./status.sh
Versão do Symantec Agent for Linux: 14.3.450.1000
Verificando o status do Symantec Agent for Linux (SEPM)...
Status do daemon:
```

```
cafagent em execução
sisamdagent em execução
sisidsagent em execução
sisipsagent em execução
Status do módulo:
sisevt carregado
sisap carregado
```

Observe que o `status da comunicação` só está disponível para clientes gerenciados na nuvem.

Para as versões 14.3 MP1 e anteriores

Você instala um cliente gerenciado ou não gerenciado do Symantec Endpoint Protection diretamente em um computador Linux. É possível implementar remotamente o cliente Linux através do Symantec Endpoint Protection Manager. As etapas de instalação são similares para clientes gerenciados e não gerenciados.

A única maneira de instalar um cliente gerenciado é com um pacote de instalação criado no Symantec Endpoint Protection Manager. Você pode converter um cliente não gerenciado em cliente gerenciado a qualquer momento importando as configurações de comunicação do servidor-cliente no cliente Linux.

Se o núcleo do sistema operacional do Linux for incompatível com o módulo pré-compilado do núcleo do Auto-Protect, o instalador tentará compilar um módulo compatível do núcleo do Auto-Protect. O processo de compilação automática será iniciado automaticamente se necessário. Contudo, o instalador pode ser incapaz de compilar um módulo compatível do núcleo do Auto-Protect. Neste caso, o Auto-Protect será instalado, mas será desativado. Para obter mais informações, consulte:

Supported Linux kernels for Symantec Endpoint Protection (em inglês)

NOTE

É preciso ter privilégios do superusuário para instalar o cliente do Symantec Endpoint Protection no computador Linux. O procedimento usa `sudo` para demonstrar esta elevação de privilégio.

Para as versões 14.3 MP1 e anteriores: para instalar o cliente do Symantec Endpoint Protection para Linux

1. Copie o pacote de instalação que você criou para o computador Linux. O pacote é um arquivo .zip.
2. No computador Linux, abra uma janela de aplicativo terminal.
3. Navegue até o diretório de instalação com o comando a seguir:

   ```
   cd /diretório/
   ```

   Onde diretório é o nome do diretório no qual você copiou o arquivo .zip.
4. Extraia o conteúdo do arquivo.zip em um diretório chamado `tmp` com o comando a seguir:

   ```
   unzip "Pacote_de_instalação" -d arquivos_do_SEP
   ```

   Onde `Pacote_de_instalação` é o nome completo do arquivo.zip e `arquivos_do_SEP` representa uma pasta de destino na qual o processo de extração colocará os arquivos de instalação.

   Se a pasta de destino não existir, o processo de extração a criará.
5. Vá para `arquivos_do_SEP` com o comando a seguir:

   ```
   cd arquivos_do_SEP
   ```
6. Para definir corretamente as permissões do arquivo de execução em `install.sh`, use o comando a seguir:

   ```
   chmod u+x install.sh
   ```
7. Use o script incorporado para instalar o Symantec Endpoint Protection com o comando a seguir:

   ```
   sudo ./install.sh -i
   ```

Digite sua senha se solicitado.

Este script inicia a instalação dos componentes do Symantec Endpoint Protection. O diretório de instalação padrão é:

`/opt/Symantec/symantec_antivirus`

O diretório padrão de trabalho do LiveUpdate é:

`/opt/Symantec/LiveUpdate/tmp`

A instalação será concluída quando o prompt de comando retornar. Não é necessário reiniciar o computador para concluir a instalação.

Para as versões 14.3 MP1 e anteriores

Para verificar a instalação do cliente, clique com o botão direito do mouse ou clique no escudo amarelo do Symantec Endpoint Protection e depois clique em **Abrir Symantec Endpoint Protection**. O local do escudo amarelo varia de acordo com a versão do Linux. A interface do usuário do cliente exibe informações sobre a versão do programa, as definições de vírus, o status da conexão do servidor e o gerenciamento.

Mais informações

- Sobre a compilação automática para o cliente do Symantec Endpoint Protection para Linux
- Sobre a interface gráfica do usuário do cliente Linux
- Como importar as configurações de comunicação entre o cliente e o servidor no cliente Linux
- Como preparar a instalação do cliente
- Instalar o Symantec Endpoint Protection 14.x para distribuições baseadas em Red Hat

Introdução ao agente do Linux

O administrador do Symantec Endpoint Protection Manager pode ter permitido que você definisse as configurações no agente do Linux.

Table 2: Etapas para começar a trabalhar com o agente Linux (para a 14.3 RU1 e superior)

Etapa	Tarefa	Descrição
Etapa 1	Instale o Symantec Agent for Linux.	O administrador do fornece a você o pacote de instalação para um cliente gerenciado ou envia um link por email para download.Consulte: Como instalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux
Etapa 2	Verifique se o agente do Linux se comunica com o Symantec Endpoint Protection Manager ou com o console de nuvem.	Para confirmar a conexão com o Symantec Endpoint Protection Manager ou com o console de nuvem, é possível executar o seguinte comando: `/usr/lib/symantec/status.sh`
Etapa 3	Verifique se o Auto-Protect está em execução.	Para verificar o status do Auto-Protect, execute o seguinte comando: `cat /proc/sisap/status`
Etapa 4	Verifique se as definições estão atualizadas.	As definições do LiveUpdate estão disponíveis no seguinte local: `/opt/Symantec/sdcssagent/AMD/sef/definitions/`

Table 3: Etapas para começar a usar o cliente do Linux (14.3 MP1 e anteriores)

Etapa	Tarefa	Descrição
Etapa 1	Instale o cliente Linux.	O administrador do Symantec Endpoint Protection Manager fornece a você o pacote de instalação para um cliente gerenciado ou envia um link por email para download. Também é possível desinstalar um cliente não gerenciado, que não se comunica com o Symantec Endpoint Protection Manager de nenhuma forma. O usuário do computador principal deve administrar o computador cliente, atualizar o software e atualizar as definições. Você pode converter um cliente não gerenciado em um cliente gerenciado. Consulte: Como instalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux
Etapa 2	Verifique se o cliente Linux se comunica com o Symantec Endpoint Protection Manager.	Clique duas vezes no escudo do Symantec Endpoint Protection. Se o cliente se comunicar com êxito com o Symantec Endpoint Protection Manager, as informações do servidor serão exibidas em **Gerenciamento**, ao lado de **Servidor**. Se você vir **Offline**, entre em contato com o administrador do Symantec Endpoint Protection Manager. Se você vir **Auto-gerenciado**, o cliente não é gerenciado. O ícone de escudo também indica o status de gerenciamento e de comunicação.
Etapa 3	Verifique se o Auto-Protect está em execução.	Clique duas vezes no escudo do Symantec Endpoint Protection. O status do Auto-Protect é exibido em **Status**, ao lado de **Auto-Protect**. Também é possível verificar o status do Auto-Protect pela interface de linha de comando: `sav info -a`
Etapa 4	Verifique se as definições estão atualizadas.	O LiveUpdate é iniciado automaticamente após a conclusão da instalação. É possível verificar se as definições estão atualizadas clicando duas vezes no escudo do Symantec Endpoint Protection. A data das definições é exibida em **Definições**. Por padrão, o LiveUpdate para o cliente Linux é executado a cada quatro horas. Se as definições estiverem desatualizadas, você pode clicar em **LiveUpdate** para executar o LiveUpdate manualmente. Também é possível usar a interface de linha de comando para executar o LiveUpdate: `sav liveupdate -u`
Etapa 5	Execute uma verificação.	Por padrão, o cliente Linux gerenciado verifica todos os arquivos e pastas diariamente ao meio-dia e meia. No entanto, é possível iniciar uma verificação manual usando a interface da linha de comando: sav manualscan -s pathname **Note:** O comando para iniciar uma verificação manual requer privilégios de superusuário.

Mais informações

Perguntas frequentes do Symantec Endpoint Protection for Linux (FAQ do SEP for Linux)

Como fazer upgrade do agente do Linux da Symantec

(Para 14.3 RU1 e posterior)

A partir da versão 14.3 RU1, o instalador do cliente Linux detecta e desinstala o cliente Linux legado (anterior a 14.3 RU1) e, em seguida, executa uma nova instalação. As configurações antigas não serão mantidas.

Para fazer upgrade do agente do Linux da Symantec

1. No Symantec Endpoint Protection Manager, crie e baixe o pacote de instalação.
   Como exportar pacotes de instalação do cliente

2. Copie o pacote obtido por download no dispositivo Linux.
3. Vá até o local da pasta e execute o seguinte comando para transformar o arquivo **LinuxInstaller** em executável:

   ```
   chmod u+x LinuxInstaller
   ```

4. Execute o comando a seguir para desinstalar o agente existente e reinstalar o agente do Linux da Symantec:

   ```
   ./LinuxInstaller
   ```

   Executar o comando como raiz.

5. Para verificar a instalação, vá para `/usr/lib/symantec` e execute o script `./status.sh` para confirmar se os módulos estão carregados e se os daemons estão em execução:

   ```
   ./status.sh
   Versão do Symantec Agent for Linux: 14.3.450.1000
   Verificando o status do Symantec Agent for Linux (SEPM)...
   Status do daemon:
   cafagent em execução
   sisamdagent em execução
   sisidsagent em execução
   sisipsagent em execução
   Status do módulo:
   sisevt carregado
   sisap carregado
   ```

Como atualizar os módulos de kernel para o agente do Linux da Symantec

O agente do Linux da Symantec será o mesmo cliente se você gerenciá-lo no Symantec Endpoint Protection Manager ou no console da nuvem.

(Para 14.3 RU1 e posterior)

Sempre que uma nova atualização do kernel do Linux é lançada, o agente do Linux da Symantec para essa plataforma precisa ser atualizado para oferecer suporte ao novo kernel. Para tornar o processo mais eficiente, os módulos do kernel do agente Linux podem agora ser atualizados usando o repositório do Linux.

> **NOTE**
> Certifique-se de que os agentes possam se conectar ao servidor do repositório do Symantec (https://linux-repo.us.securitycloud.symantec.com/) para fazer download das atualizações do módulo do kernel.

Sempre que você executar o comando `yum update` em um sistema RHEL, Amazon Linux, Oracle Linux ou CentOS, o comando também procura novos pacotes do agente. Se uma atualização estiver disponível, o módulo do kernel mais recente será baixado, e o agente será atualizado automaticamente. Depois que o módulo do kernel for atualizado, você deverá reiniciar a instância para que a atualização entre em vigor.

Como alternativa, é possível atualizar o módulo do kernel do agente executando o comando abaixo na instância. Abra uma janela de terminal com privilégios raiz, vá até `/usr/lib/symantec/` e execute o seguinte comando:

```
/usr/lib/symantec/installagent.sh --update-kmod
```

Como atualizar os módulos do kernel em sistemas Ubuntu

1. Para renovar e atualizar o banco de dados do pacote local, digite os seguintes comandos:
   ```
   sudo apt-get clean
   sudo apt-get update
   ```
2. Para fazer upgrade para o módulo de kernel mais recente, digite os seguintes comandos:
   ```
   /usr/lib/symantec/installagent.sh --update-kmod
   ```

É necessário ter privilégios de superusuário para executar esta ação.

Como atualizar os módulos do kernel em um ambiente restrito sem conexão com a internet

1. Método 1: transfira manualmente o pacote mais recente do KMOD para um sistema sem conexão com a internet, anexe o pacote do KMOD ao LinuxInstaller e, em seguida, execute o LinuxInstaller.
   1. Em um sistema com conexão com a internet, faça download do pacote KMOD.
      `./LinuxInstaller-d`
   2. Copie e cole manualmente o pacote do KMOD no agente que deseja atualizar.
   3. Relacione os pacotes anexados.
      `./LinuxInstaller -l`
   4. Anexe o novo pacote do KMOD ao LinuxInstaller.
      `tar czf - [KMOD-package-name] >> LinuxInstaller`
   5. Certifique-se de que o novo pacote do KMOD esteja incluído na lista de pacotes anexados.
      `./LinuxInstaller -l`
   6. Execute o programa de instalação para atualizar os módulos do kernel.
      `./LinuxInstaller -- --update-kmod`
2. Método 2: configure um repositório local e edite as configurações do repositório, de modo que o agente use o repositório local, em vez do repositório padrão da Symantec.
   1. Configure o repositório local que hospeda os pacotes do KMOD.
      Para obter informações sobre como criar um repositório local, consulte a documentação da distribuição do Linux correspondente que você está usando.
   2. No computador cliente, execute o seguinte comando para redirecioná-lo para usar o repositório local:
      `./LinuxInstaller --local-repo <url_do_repositorio_local>`
      Exemplo do URL: `--local-repo 'http://<ip_ou_nomedehost_do_repositorio:<porta_opcional>/sep_linux'`
   3. Para atualizar o KMOD, execute:
      `./LinuxInstaller -- --update-kmod`

Se você atualizar os módulos do kernel do sistema operacional, deverá fazer também a atualização do módulo do kernel correspondente para o cliente do Symantec Endpoint Protection. Sem os módulos de kernel compatíveis, o cliente do Symantec Endpoint Protection pode não funcionar corretamente, e alguns recursos podem estar desativados.

Mais informações

Como criar e instalar um pacote de instalação do agente do Linux para Symantec

Como gerenciar o cliente Linux usando a ferramenta de linha de comando (sav)

A ferramenta de linha de comando permite controlar e verificar o cliente Linux.

Para gerenciar o cliente Linux usando a ferramenta de linha de comando, consulte:

(para a 14.3 RU2 e superior)

A ferramenta de linha de comando permite controlar e verificar o cliente Linux.

Como gerenciar o cliente Linux usando a ferramenta de linha de comando

1. Em um computador cliente Linux, vá até o seguinte local:
   `/opt/Symantec/sdcssagent/AMD/tools`
2. Execute o comando sav da seguinte maneira:
   `./sav [opções] command`

Table 4: Opções para sav

Opção	Descrição	Aplica-se a
`-q`	Silencioso	A partir da 14.3 RU2
`-h`	Exibe as opções e comandos disponíveis para sav.	A partir da 14.3 RU2

Table 5: Comandos para sav

Opção	Descrição	Aplica-se a
`autoprotect -e`	Ativa o Auto-Protect. Para verificar o status do Auto-Protect, execute o seguinte comando: `[root@localhost tools]# cat /proc/sisap/status | grep -i MODE` A resposta pode ser uma das seguintes: • `mode=ENA` (se ativado) • `mode=DIS` (se desativado)	A partir da 14.3 RU2
`autoprotect -d`	Desativa o Auto-Protect.	A partir da 14.3 RU2
`info -d`	Mostra a versão e a data das definições atuais de risco à segurança e de vírus em uso no dispositivo.	A partir da versão 14.3 RU3
`info -e`	Mostra a versão do mecanismo de verificação em uso no dispositivo.	A partir da versão 14.3 RU3
`info -p`	Mostra a versão do Symantec Agent em uso no dispositivo.	A partir da versão 14.3 RU3
`info -a`	Mostra o status do Auto-Protect no dispositivo.	A partir da versão 14.3 RU3
`liveupdate -u`	Executa o LiveUpdate imediatamente.	A partir da versão 14.3 RU3
`manage -i <arquivo>`	Importa o arquivo *sylink.xml* para o local especificado.	A partir da 14.3 RU2
`manualscan -s <lista de arquivos>`	Inicia uma verificação manual. <lista de arquivos> especifica a lista de arquivos e diretórios a serem verificados. Para especificar essa lista, digite uma lista de arquivos e diretórios separados por feeds de linha e terminando com um sinal de fim de arquivo, como CTRL-D. Se um diretório for especificado, todos os subdiretórios também serão verificados. Os caracteres curinga são suportados. Por padrão, o número máximo de itens que podem ser adicionados a uma verificação manual iniciada na interface de linha de comando é 100. Você pode usar o **symcfg** para mudar o valor de VirusProtect6MaxInput de DWORD a fim de umentar esse limite. Para remover inteiramente o limite, defina o valor de VirusProtect6MaxInput para 0. Se você especificar um hífen (-) em vez de uma lista de arquivos e diretórios, a lista de nomes de caminho será lida a partir da entrada padrão. É possível usar os comandos que produzem uma lista de arquivos ou nomes de caminho separada por alimentações de linha.Enviar uma lista de itens muito longa a esse comando pode afetar negativamente o desempenho. A Symantec recomenda limitar listas a um máximo de alguns milhares de itens.	A partir da versão 14.3 RU3
`manualscan -t`	Interrompe uma verificação manual em andamento.	A partir da versão 14.3 RU3

Mais informações

Como solucionar problemas do agente do Linux da Symantec

Como solucionar problemas do agente do Linux da Symantec

A tabela a seguir mostra os recursos para a solução de problemas do agente do Linux da Symantec (a partir da versão 14.3 RU1).

Table 6: recursos para solução de problemas do agente do Linux da Symantec

Ação	Descrição
Verificação do status do agente.	Para verificar a versão e o status da conexão do agente e para confirmar se os módulos estão carregados e se os daemons estão em execução, vá para `/usr/lib/symantec` e execute o seguinte comando: `./status.sh`
Verificação das versões dos pacotes de agente.	Vá para `/usr/lib/symantec` e execute o seguinte comando: `./version.sh`

Exibição dos logs.	Você encontra os logs do agente do Linux da Symantec nos seguintes locais:
	• Log AMD - fornece informações relacionadas à verificação.
	`/var/log/sdcsslog/amdlog`
	• Log do CAF - fornece informações relacionadas às atividades do agente, como comunicação com o servidor, registro, comandos, eventos, etc.
	`/var/log/sdcss-caflog/`
	• Log do agente - fornece informações relacionadas às atividades do agente.
	`/var/log/sdcsslog/SISIDSEvents*.csv`
	• Log de CVE - fornece informações relacionadas à comunicação entre o Symantec Endpoint Protection Manager e o agente.
	`/var/log/sdcss-caflog/cve.log`

Coleta dos logs em um arquivo ZIP.	É possível usar o script `GetAgentInfo` para coletar todos os arquivos de log em um arquivo ZIP que pode ser enviado ao suporte ao cliente. 1. Faça login no sistema do agente do Linux da Symantec. 2. Vá para `/opt/Symantec/sdcssagent/IPS/tools/`. 3. Execute `./getagentinfo.sh` como raiz. 4. Um arquivo ZIP será criado no diretório `/tmp/`. O nome do arquivo será semelhante a `20201208_184935_0001_CU_mihsan-rhel8.zip` `-out <diretório>` permite alterar o local e o nome do arquivo ZIP gerado.
Alteração do nível de log de CVE.	Por padrão, o nível de registo em log do CVE é `info`. Você pode alterar o nível de registro em log para `debug` no arquivo `/opt/Symantec/cafagent/bin/log4j.properties`. Após alterar o arquivo, será necessário reiniciar o serviço `cafagent`.

Alteração do nível de registro em log do AMD.	Por padrão, o nível de registro em log do AMD é `info`.
	Você pode alterar o nível de registro em log para `trace`, `warning` ou `error` no arquivo `/opt/Symantec/sdcssagent/AMD/system/AntiMalware.ini`.
	Note: Antes de modificar o arquivo AntiMalware.ini, interrompa o sisamdagent:
	`service sisamdagent stop`
	Note: Depois de modificar o arquivo, reinicie o serviço:
	`service sisamdagent start`

Como desinstalar o agente do Linux da Symantec ou o cliente do Symantec Endpoint Protection para Linux

Você desinstala o cliente do Symantec Endpoint Protection para Linux com o script fornecido pela instalação.

NOTE

Você deve ter privilégios de superusuário para desinstalar o cliente do Symantec Endpoint Protection no computador Linux. O procedimento usa `sudo` para demonstrar esta elevação de privilégio.

Versão 14.3 RU1 e posterior: como desinstalar o agente do Linux da Symantec

1. No computador Linux, abra uma janela de aplicativo terminal.
2. Vá para o seguinte diretório:
   `/usr/lib/symantec/`
3. Execute o seguinte script integrado para desinstalar o Symantec Agent for Linux:
   `./uninstall.sh`
4. Reinicialize o computador depois que a desinstalação for concluída e que o prompt de reinicialização for exibido. Observe que o script `uninstall.sh` removerá todos os componentes do Symantec Agent for Linux (`sdcss-caf`, `sdcss-sepagent` e `sdcss-kmod`).

```
[root@localhost symantec]# ./uninstall.sh
Executando ./uninstall.sh (PWD /usr/lib/symantec; versão 2.2.4.41)
Desinstalando o Symantec Agent for Linux (SEPM) ...
Removendo os pacotes sdcss-caf, sdcss-sepagent, sdcss-kmod, sdcss-scripts
Symantec Agent for Linux (SEPM) desinstalado com êxito.
É necessário reinicializar para concluir a desinstalação.
Reinicialize sua máquina assim que possível.
```

Versão 14.3 MP1 e anterior: como desinstalar o cliente do Symantec Endpoint Protection para Linux

1. No computador Linux, abra uma janela de aplicativo terminal.
2. Navegue até a pasta de instalação do Symantec Endpoint Protection com o comando:

   ```
   cd /opt/Symantec/symantec_antivirus
   ```

   O caminho é o caminho de instalação do padrão.
3. Use o script incorporado para desinstalar o Symantec Endpoint Protection com o comando a seguir:

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

   Digite sua senha se solicitado.

   Este script inicia a desinstalação dos componentes do Symantec Endpoint Protection.
4. No prompt, digite `S` e pressione **Enter**.

   A desinstalação será concluída quando o prompt de comando retornar.

   NOTE

   Em alguns sistemas operacionais, se os arquivos do cliente do Symantec Endpoint Protection forem o único conteúdo da pasta `/opt`, o script do desinstalador excluirá também `/opt`. Para recriar esta pasta, digite o comando a seguir: `sudo mkdir /opt`

Para desinstalar usando um gerenciador de pacotes ou de software, consulte a documentação específica a sua distribuição Linux.


Symantec
A Division of Broadcom