Cisco Secure Endpoint Linux Connector em sistemas baseados em Debian

Contents

Este artigo descreve as alterações e as etapas que os administradores podem tomar para implantar o conector Cisco Secure Endpoint Linux em sistemas baseados em Debian:

- Debian 10 e mais recente.
- Ubuntu 18.04 e mais recente.

Requisitos mínimos do SO

Consulte o artigo Cisco Secure Endpoint Linux Connector OS Compatibility para obter informações sobre compatibilidade de SO.

Configuração do ambiente

O conector Linux em sistemas baseados em Debian usa eBPF para monitoração de arquivos e redes. A máquina deve ter o pacote de software correto de cabeçalhos do linux instalado, caso contrário, o conector aumentará a falha 11 (Dependência do Sistema Ausente) e será executado em um estado degradado sem o monitoramento de arquivos e da rede. As orientações para resolver essa falha podem ser encontradas no artigo Falha de Kernel-Devel do Linux.

Dependências

O conector Linux depende dos pacotes de sistema incluídos na instalação básica de sistemas baseados em Debian, mas se uma dependência estiver faltando, a seguinte mensagem será exibida:

```
ciscoampconnector depends on
```

Use o seguinte comando para instalar todas as dependências ausentes exigidas pelo conector Linux:

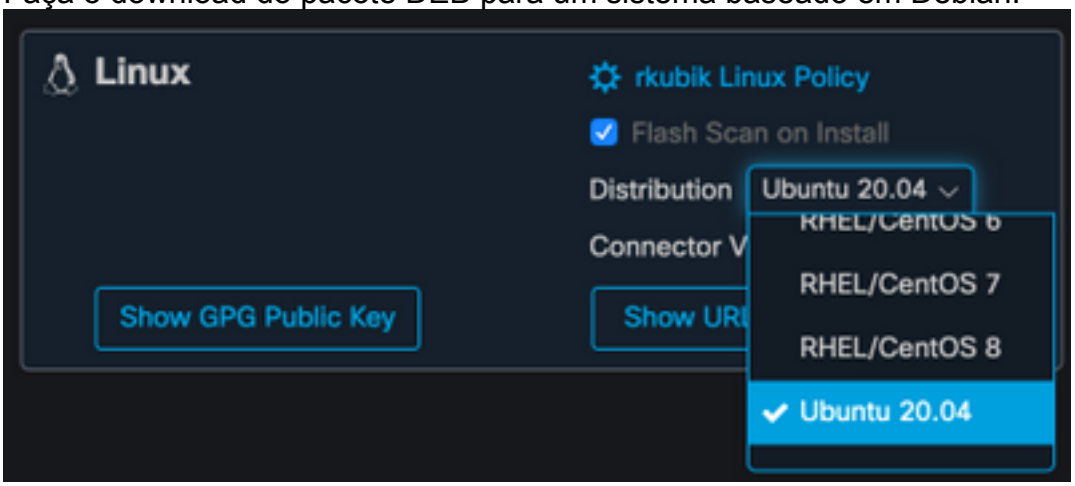
```
sudo apt install
```

Verificação do pacote DEB

O pacote DEB do conector Linux contém uma assinatura para verificar se o pacote de software baixado pertence à Cisco.

Download do pacote DEB

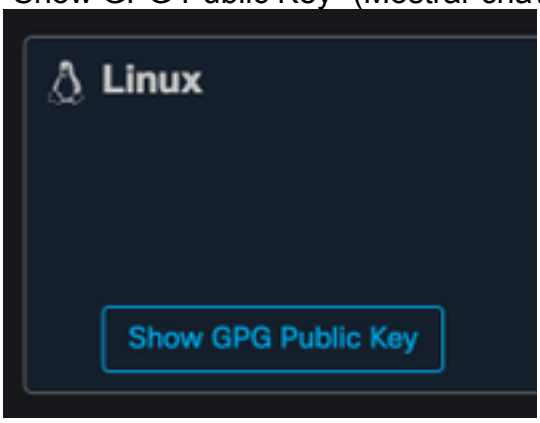
1. Acesse o console do AMP para endpoints.
2. Faça o download do pacote DEB para um sistema baseado em Debian.



3. Transfira o pacote DEB para o sistema baseado em Debian. Por exemplo: amp_ciscoampconnector.deb.

Recuperando a chave pública GPG

1. Clique no botão "Show GPG Public Key" (Mostrar chave pública GPG), como mostrado na imagem abaixo.



2. Se a versão do conector for anterior à 1.17.0, baixe e transfira ou copie a chave pública para a máquina. Por exemplo: cisco.gpg Se a versão do conector for pelo menos 1.17.0, a chave GPG estará disponível em /opt/cisco/amp/etc/dpkg-gpg/DPKG-GPG-KEY-cisco-amp.

Verificação do pacote DEB

O pacote DEB é assinado usando a ferramenta de devoluções e pode ser verificado usando a verificação de débito.

1. Instale a ferramenta de verificação de débito.

```
sudo apt-get install debsig-verify
```

2. Importe a chave pública do Cisco GPG para o teclado do debsigs. **Observação:** a partir da versão 1.17.0, o arquivo debsig.gpg será criado automaticamente para que a etapa 2 possa ser ignorada.
```
sudo mkdir -p /usr/share/debsig/keyrings/914E5BE0F2FD178F sudo gpg --dearmor --output
/usr/share/debsig/keyrings/914E5BE0F2FD178F/debsig.gpg cisco.gpg
```
3. Criar diretório de política.
```
sudo mkdir -p /etc/debsig/policies/914E5BE0F2FD178F
```
4. Copie o conteúdo da política abaixo em um novo arquivo "/etc/debsig/policies/914E5BE0F2FD178F/ciscoampconnector.pol".

5. Verifique a assinatura do DEB com verificação de débito.
```
debsig-verify amp_ciscoampconnector.deb
```
A saída deve ser a seguinte:
```
debsig: Verified package from 'Cisco AMP for Endpoints' (Debsig)
```

Note: A Etapa 5 pode ser repetida para todos os pacotes baseados em Debian baixados do console do AMP for Endpoints.

Instalação

Para instalar o conector, execute o seguinte comando onde [deb package] é o nome do arquivo, por exemplo amp_test.deb:

```
sudo dpkg -i [deb package]
```

IMPORTANTE! Se você estiver executando outros produtos de segurança em seu ambiente, há a possibilidade de que eles detectem o instalador do conector como uma ameaça. Para instalar o conector com êxito, adicione o Cisco Secure a uma lista permitida ou exclua o Cisco Secure nos outros produtos de segurança e tente novamente.

IMPORTANTE! Durante a instalação do conector, um usuário e um grupo chamado cisco-amp-scan-svc são criados no sistema. Se esse usuário ou grupo já existir, mas estiver configurado de forma diferente, o instalador tentará excluí-lo e recriá-lo com a configuração necessária. O instalador falhará se o usuário e o grupo não puderem ser criados com a configuração necessária.

Desinstalação

Consulte o Guia do usuário do Secure Endpointpara obter instruções de desinstalação

Histórico das revisões

10 de dezembro de 2020

- Versão inicial

12 de abril de 2022

- O conteúdo é aplicável a Debian e Ubuntu.