

Configurar VPN de Cliente Seguro para Uso em um Contêiner de Docker

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de licença](#)

[Instalação](#)

[Arquivo Docker](#)

Introdução

Este documento descreve como usar o Cisco Secure Client VPN dentro de um contêiner Docker.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O pacote Cisco Secure Client pode ser baixado para o desktop local e usado dentro de um contêiner Docker. (Para baixar o pacote do cliente, consulte a página da Web do [Cisco Secure Client](#).)
- O Cisco Secure Client é compatível com o Docker a partir da versão 5.1.10.
- A implantação do Docker requer o uso dos pacotes DEB ou RPM CLI do Cisco Secure Client (os pacotes são otimizados somente para uso da CLI, que é o caso do Docker).

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Client versão 5.1.10 RPM ou no pacote DEB CLI.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de licença

Consulte o [Guia de pedidos do Cisco Secure Client](#) para obter informações sobre licenças.

Instalação

Arquivo Docker

1. Instalar o pacote do qual o Cisco Secure Client depende.

- Para RHEL (Red Hat Enterprise Linux):

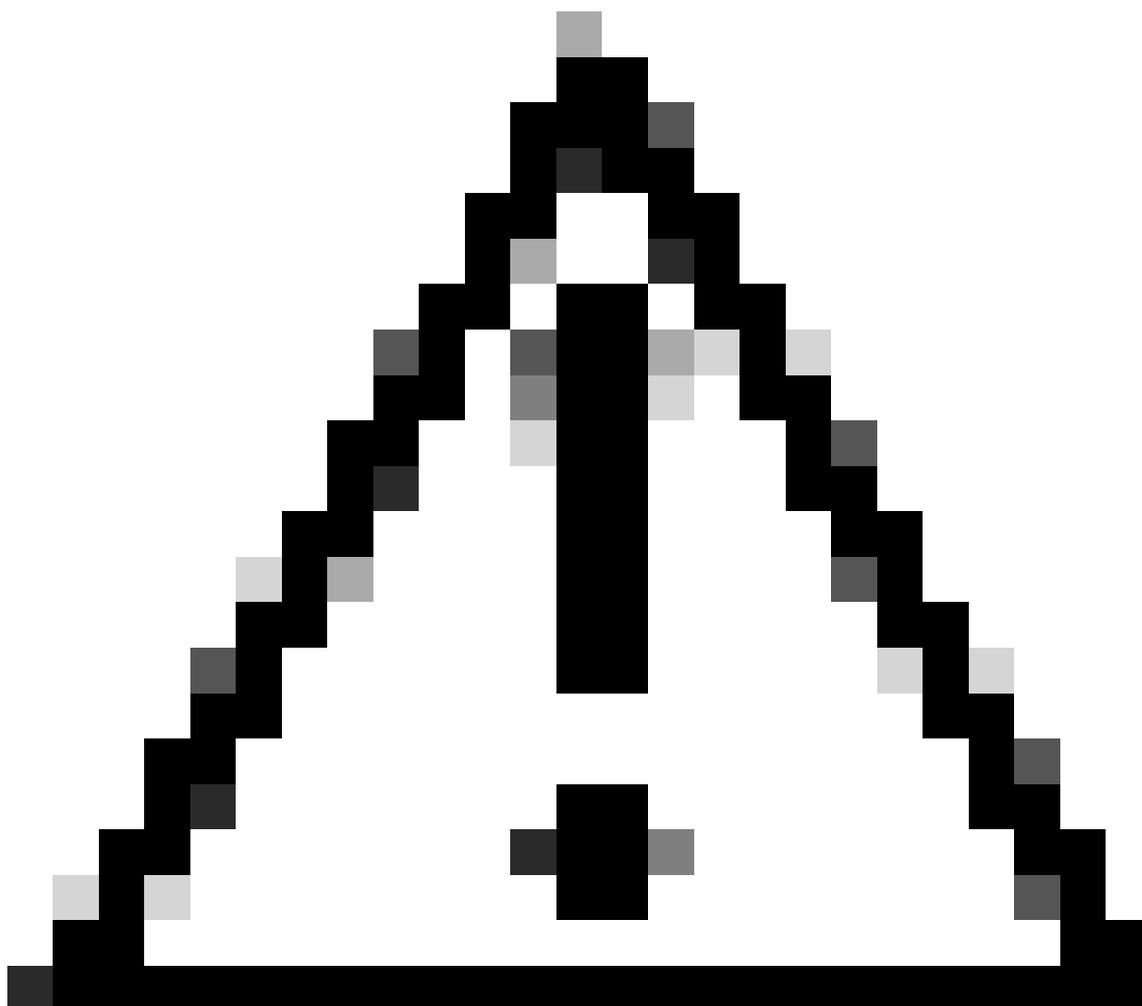
```
RUN yum install -y net-tools iptables
```

- Para Ubuntu:

```
RUN apt-get install -y net-tools iptables
```

2. Habilitando registro.

```
ENV CSC_LOGGING_OUTPUT=STDOUT
```



Caution: Se habilitado, os logs serão impressos em linha na CLI juntamente com outras atividades em andamento.

3. Copie o pacote DEB/RPM do host.

- Para RHEL:

```
COPY cisco-secure-client-vpn-cli-<VERSION>-1.x86_64.rpm /tmp/cisco-secure-client-cli.rpm
```

- Para Ubuntu:

```
COPY cisco-secure-client-vpn-cli_<VERSION>_amd64.deb /tmp/cisco-secure-client-cli.deb
```

4. Para iniciar o agente VPN, mantê-lo em execução e reiniciá-lo se necessário, um arquivo chamado `entry.sh` é adicionado como o ponto de entrada para o contêiner Docker. Este script deve ser copiado no contêiner para uso posterior.

```
#!/bin/bash

wait_forever() {
  while true; do
    sleep infinity &
    wait $!
  done
}

start_service() {
  if [ -f /opt/cisco/secureclient/bin/vpnagentd ]; then
    echo "Starting VPN agent..."
    while true; do
      /opt/cisco/secureclient/bin/vpnagentd -execv_instance &
      SERVICE_PID=$!
      wait $SERVICE_PID
      echo "VPN agent exited. Restarting..."
      sleep 1
    done
  fi
}

start_service
wait_forever
```

- Para RHEL e Ubuntu:

```
COPY entry.sh /entry.sh
RUN chmod +x /entry.sh
```

5. Instale o pacote.

- Para RHEL:

```
RUN cd /tmp && \
  dnf install -y ./cisco-secure-client-cli.rpm && \
  rm -rf /tmp/cisco-secure-client-cli.rpm
```

- Para Ubuntu:

```
RUN cd /tmp && \
  apt-get install -y ./cisco-secure-client-cli.deb && \
  rm -rf /tmp/cisco-secure-client-cli.deb
```

6. Adicione entry.sh como o ponto de entrada para o contêiner Docker.

```
ENTRYPOINT ["/entry.sh"]
```

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.