Configuración de VPN de cliente seguro para su uso en un contenedor Docker

Contenido

Introducción

Prerequisites

- Requirements
- Componentes Utilizados
- Información de licencia

Configuración

- Archivo Docker

Introducción

Este documento describe cómo utilizar Cisco Secure Client VPN dentro de un contenedor Docker.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- El paquete Cisco Secure Client se puede descargar al escritorio local y utilizarse dentro de un contenedor Docker. (Para descargar el paquete del cliente, consulte la página web de Cisco Secure Client.)
- Cisco Secure Client es compatible con Docker desde la versión 5.1.10.
- La implementación de Docker requiere el uso de los paquetes Cisco Secure Client DEB o RPM CLI (los paquetes están optimizados para el uso exclusivo de CLI, que es el caso de Docker).

Componentes Utilizados

La información de este documento se basa en el paquete Cisco Secure Client versión 5.1.10 RPM o DEB CLI.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Información de licencia

Consulte la Guía para hacer pedidos de Cisco Secure Client para obtener información sobre las licencias.

Configuración

Archivo Docker

1. Instalación del paquete del que depende Cisco Secure Client.
    - Para RHEL (Red Hat Enterprise Linux):

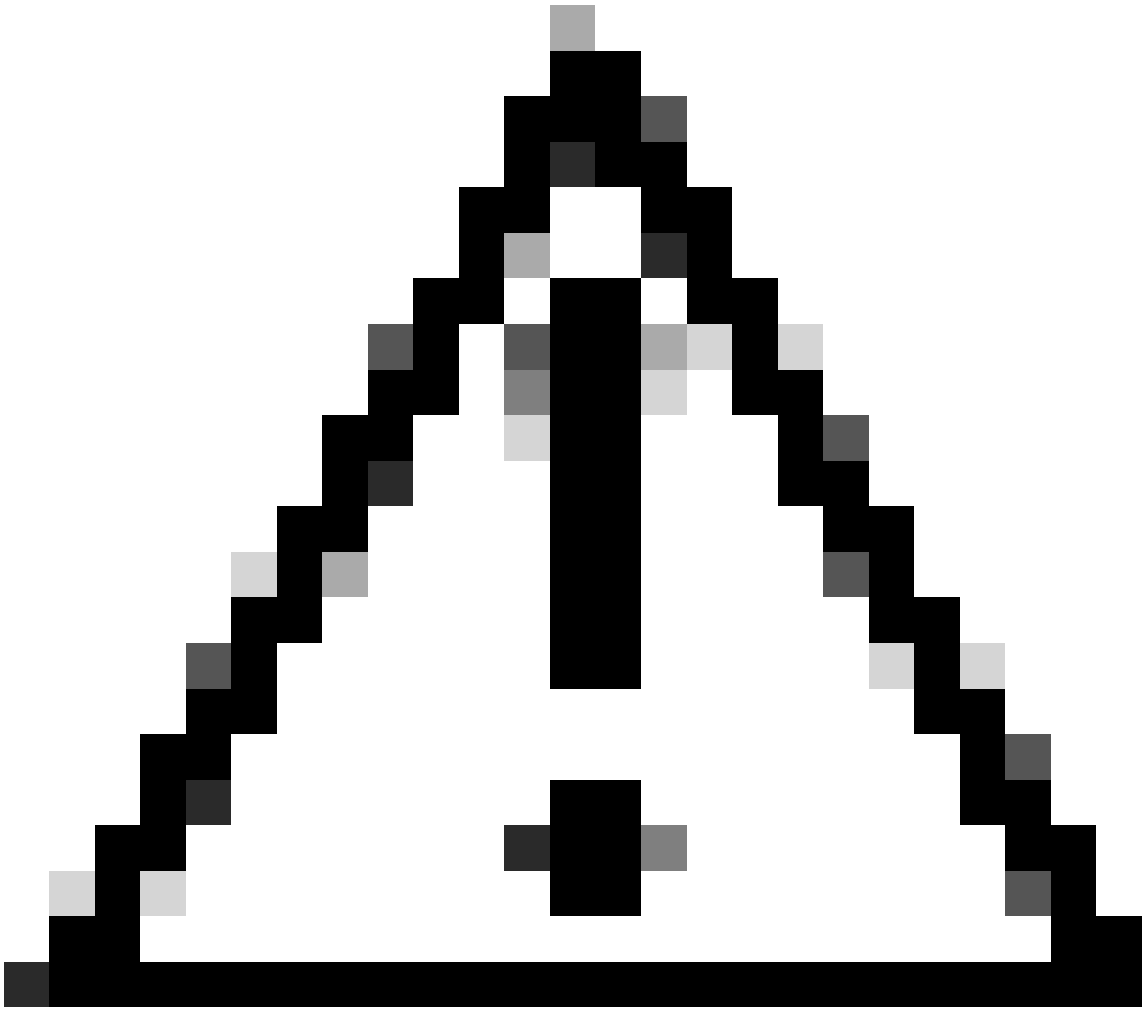
```
RUN yum install -y net-tools iptables
```

    - Para Ubuntu:

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

2. Activación del registro.

```
ENV CSC_LOGGING_OUTPUT=STDOUT
```



Precaución: Si se habilita, los registros se imprimen en línea en la CLI junto con otras actividades en curso.

3. Copie el paquete DEB/RPM del 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 el agente VPN, mantenerlo en ejecución y reiniciarlo si es necesario, se agrega un archivo denominado entry.sh como punto de entrada para el contenedor Docker. Esta secuencia de comandos debe copiarse en el contenedor para su 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 y Ubuntu:

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

5. Instale el paquete.
   - 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. Agregue el archivo entry.sh como el punto de entrada al contenedor Docker.

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

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).