

Beveiligde VPN-client configureren voor gebruik in een Docker-container

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Licentie-informatie](#)

[opzet](#)

[Docker-bestand](#)

Inleiding

In dit document wordt beschreven hoe u de Cisco Secure Client VPN in een Docker-container kunt gebruiken.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Het Cisco Secure Client-pakket kan worden gedownload naar het lokale bureaublad en worden gebruikt in een Docker-container. (Als u het clientpakket wilt downloaden, gaat u naar de webpagina [Cisco Secure Client](#).)
- De Cisco Secure Client is compatibel met Docker vanaf versie 5.1.10.
- De Docker-implementatie vereist het gebruik van de Cisco Secure Client DEB- of RPM CLI-pakketten (de pakketten zijn geoptimaliseerd voor alleen CLI-gebruik, wat het geval is voor Docker).

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Client Version 5.1.10 RPM of DEB CLI-pakket.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Licentie-informatie

Raadpleeg de [Cisco Secure Client Ordering Guide](#) voor informatie over licenties.

opzet

Docker-bestand

1. Het pakket installeren waarvan de Cisco Secure Client afhankelijk is.
 - Voor RHEL (Red Hat Enterprise Linux):

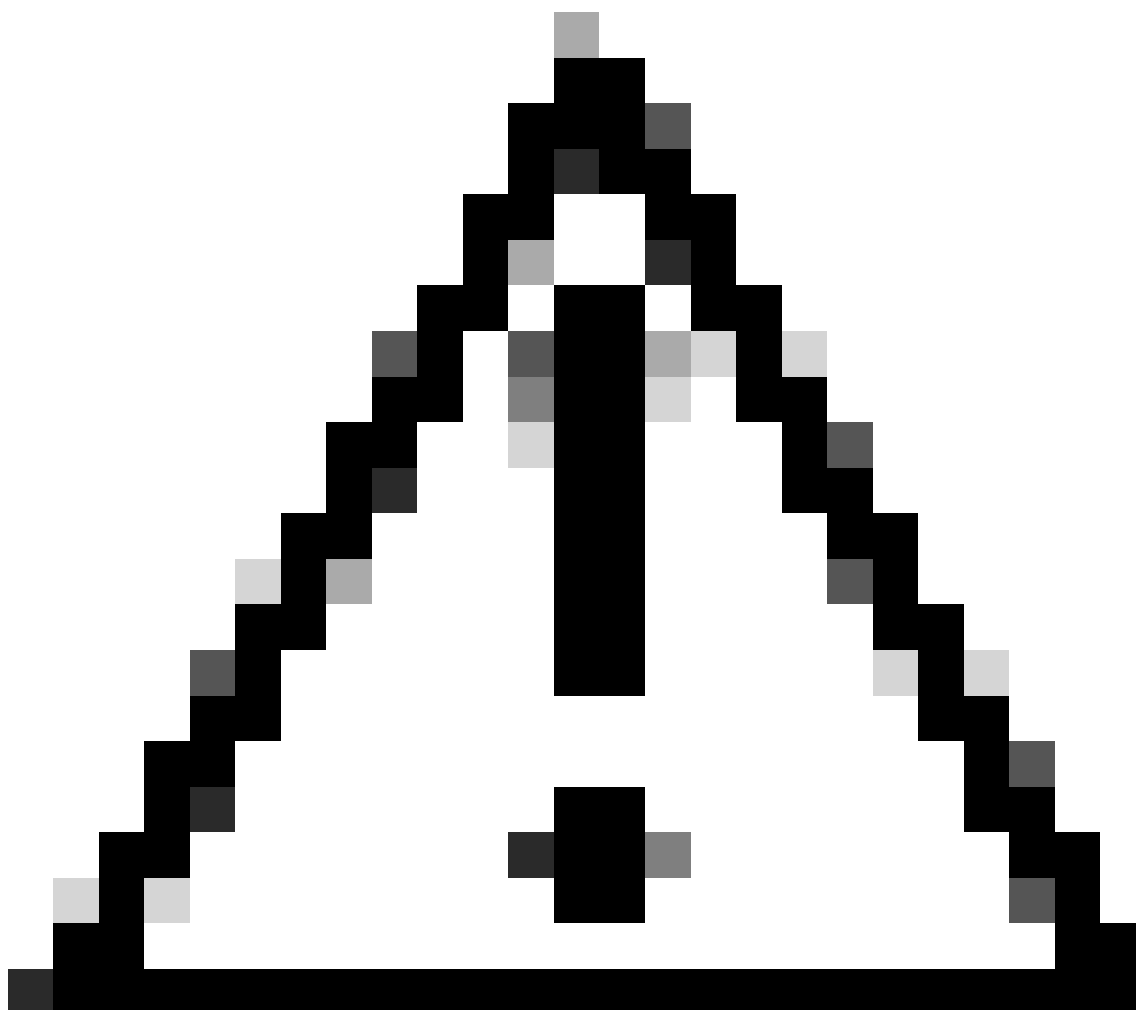
```
RUN yum install -y net-tools iptables
```

- Voor Ubuntu:

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

2. Logboekregistratie inschakelen.

```
ENV CSC_LOGGING_OUTPUT=STDOUT
```



Let op: indien ingeschakeld, worden de logs in de CLI samen met andere lopende activiteiten online afgedrukt.

3. Kopieer het DEB/RPM-pakket van de host.

- Voor RHEL:

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

- Voor Ubuntu:

```
COPY cisco-secure-client-vpn-cli-<VERSION>-amd64.deb /tmp/cisco-secure-client-cli.deb
```

4. Om de VPN-agent te starten, deze actief te houden en indien nodig opnieuw te starten, wordt een bestand met de naam `entry.sh` toegevoegd als ingangspunt voor de Docker-container. Dit script moet in de container worden gekopieerd voor later gebruik.

```
#!/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
```

- Voor zowel RHEL als Ubuntu:

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

5. Installeer het pakket.

- Voor RHEL:

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

- Voor Ubuntu:

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

6. Voeg de entry.sh als het ingangspunt toe aan de Docker-container.

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

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.