Configurare la VPN client sicura da utilizzare in un contenitore Docker

Sommario

Introduzione

Questo documento descrive come utilizzare la VPN Cisco Secure Client all'interno di un contenitore Docker.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Il pacchetto Cisco Secure Client può essere scaricato sul desktop locale e utilizzato all'interno di un contenitore Docker. (Per scaricare il pacchetto client, consultare la pagina Web Cisco Secure Client).
- Cisco Secure Client è compatibile con Docker a partire dalla versione 5.1.10.
- La distribuzione Docker richiede l'utilizzo dei pacchetti Cisco Secure Client DEB o RPM CLI (i pacchetti sono ottimizzati per l'utilizzo solo CLI, come nel caso di Docker).

Componenti usati

Le informazioni di questo documento si basano su Cisco Secure Client versione 5.1.10 RPM o sul pacchetto DEB CLI.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Informazioni sulla licenza

Per informazioni sulle licenze, consultare la Cisco Secure Client Ordering Guide.

Configurazione

File Docker

1. Installazione del pacchetto da cui dipende Cisco Secure Client.
    - Per RHEL (Red Hat Enterprise Linux):

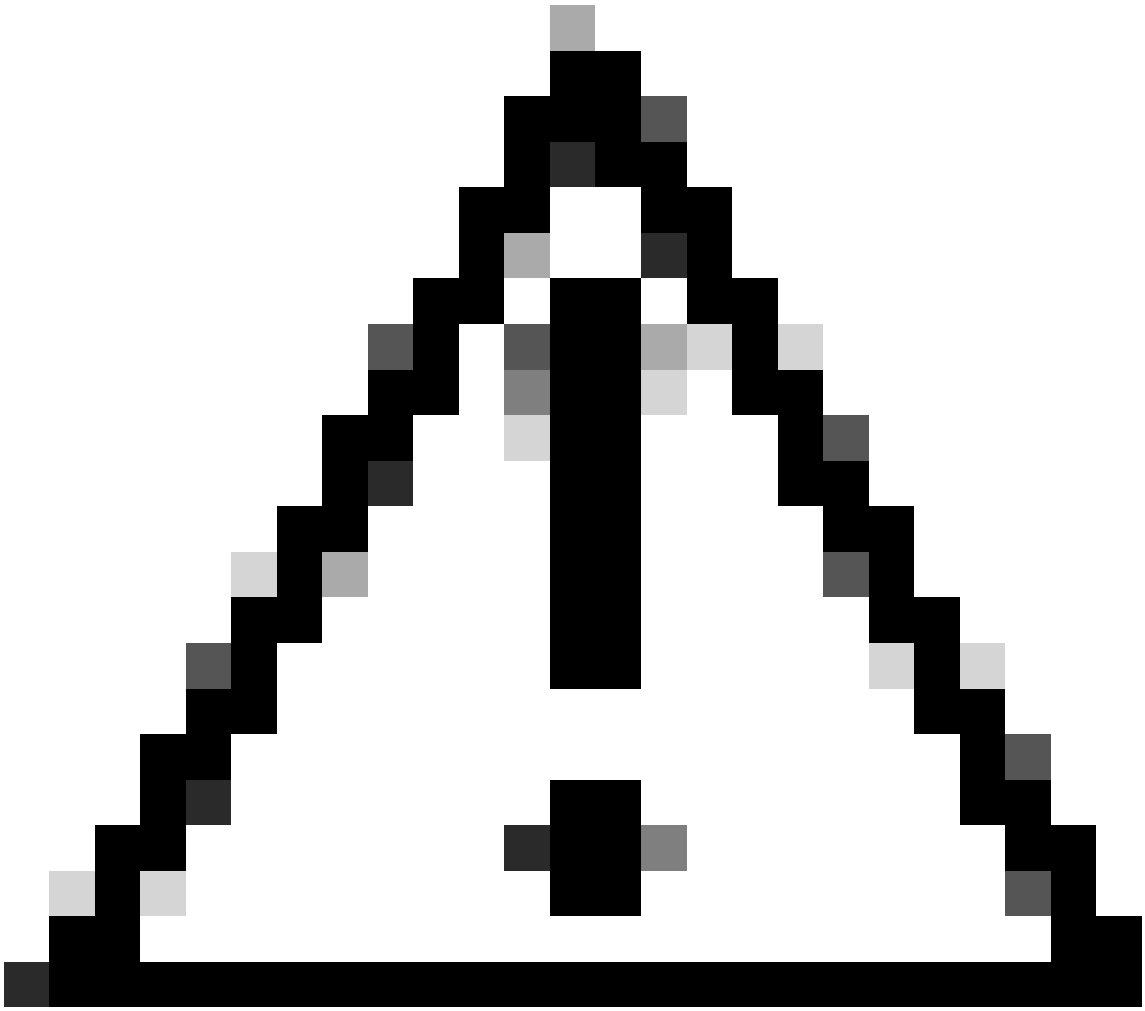
```
RUN yum install -y net-tools iptables
```

    - Per Ubuntu:

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

2. Abilitazione della registrazione.

```
ENV CSC_LOGGING_OUTPUT=STDOUT
```



Attenzione: Se abilitato, i log vengono stampati in linea nella CLI insieme ad altre attività in corso.

3. Copiare il pacchetto DEB/RPM dall'host.
   - Per RHEL:

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

   - Per Ubuntu:

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

4. Per avviare l'agente VPN, mantenerlo in esecuzione e riavviarlo se necessario, viene aggiunto un file denominato entry.sh come punto di ingresso per il contenitore Docker. Lo script deve essere copiato nel contenitore per un utilizzo successivo.

```
#!/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
```

- Sia per RHEL che per Ubuntu:

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

5. Installare il pacchetto.
   - Per RHEL:

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

   - Per Ubuntu:

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

6. Aggiungere entry.sh come punto di ingresso al contenitore Docker.

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

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).