

Packet Capture op Jabber Guest Server

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Probleem: Hoe Packet Capture kan worden genomen van Jabber Guest Server?](#)

[Oplossing](#)

[Gerelateerde Cisco Support Community-discussies](#)

Inleiding

Dit document beschrijft hoe pakketvastlegging kunt worden gegenereerd vanaf de Jabber Guest Server.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- De Jabber Guest moet toegang hebben tot internet om het pakket te kunnen downloaden.
- WinSCP-software die op de PC is geïnstalleerd om de opnamekaarten te verzamelen.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Jabber Guest versies 10.5 en 10.6
- WinSCP-software

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 de potentiële impact van elke opdracht begrijpen.

Probleem: Hoe Packet Capture kan worden genomen van Jabber Guest Server?

Oplossing

Stap 1.

De Jabber Guest server moet toegang hebben tot internet, anders kan het de verpakking van internet downloaden. Indien een webproxy wordt gebruikt, volgt u de procedure om CentOS op Jabber Guest toe te staan om de webproxy te gebruiken om het pakket te downloaden.

Raadpleeg de link <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html> om de procedure te volgen.

Nadat u ervoor hebt gezorgd dat de Jabber Guest Server het pakket kan downloaden, gaat u naar Stap 2.

Stap 2.

Meld u aan bij de Jabber Guest-server met Secure Socket Host (SSH) wortelgeloofsbrieven en voer het opdracht **yum** Zoompomp uit om de laatste versie van de TCAB te vinden.

```
[root@jabberguest ~]# yum search tcpdump
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: centos.host-engine.com
 * extras: centos.mirror.nac.net
 * updates: centos.arvixe.com
===== N/S Matched: tcpdump =====
tcpdump.x86_64 : A network traffic monitoring tool

Name and summary matches only, use "search all" for everything.
[root@jabberguest ~]#
```

Stap 3.

Start het geprogrammeerde opdracht om de pomp op de Jabber Guest Server te installeren.

```
[root@jabberguest ~]# yum install tcpdump
Loaded plugins: fastestmirror
Setting up Install Process
Determining fastest mirrors
 * base: centos.aol.com
 * extras: centos.mirror.ndchost.com
 * updates: centos.mirror.nac.net
base | 3.7 kB | 00:00
extras | 3.4 kB | 00:00
extras/primary_db | 31 kB | 00:00
updates | 3.4 kB | 00:00
updates/primary_db 50% [===== ] 0.0 B/s | 2.0 MB --:-- ETA
```

Stap 4.

U wordt via verschillende aanwijzingen verzonden. Voer **y in** op elk onderdeel om elke melding te controleren.

Stap 5.

TcPa is nu opnieuw beschikbaar voor pakketvastlegging vanaf de Jabber Guest Server.

```
name and summary matches only, use -s search all for everything.
[root@jabberguest ~]# tcpdump
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
11:44:54.328431 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 1089242520:1089242728, ack 1202666623, win 20832, length 208
11:44:54.329007 IP jabberguest.havogel.com.50843 > ad.havogel.com.domain: 15118+ PTR? 66.25.0.14.in-addr.arpa. (41)
11:44:54.384348 IP jabberguest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 4294967232:208, ack 1, win 20832, length 272
11:44:54.388191 IP 14.0.25.66.60858 > jabberguest.havogel.com.ssh: Flags [.] , ack 208, win 64384, options [nop,nop,sack 1 {4294967232:208}], length 0
11:44:54.579286 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:54.656970 ARP, Request who-has 14.80.94.11 tell 14.80.94.1, length 46
11:44:54.660995 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.237405 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:55.579320 ARP, Request who-has 14.80.94.10 tell 14.80.94.15, length 46
11:44:55.660815 ARP, Request who-has 14.80.94.235 tell 14.80.94.232, length 46
11:44:55.915532 ARP, Request who-has 14.80.94.104 tell 14.80.94.1, length 46
11:44:55.921206 ARP, Request who-has 14.80.94.150 tell 14.80.94.1, length 46
11:44:56.102066 ARP, Request who-has 14.80.94.66 tell 14.80.94.56, length 46
11:44:56.113541 ARP, Request who-has 14.80.94.48 tell 14.80.94.220, length 46
11:44:56.234761 ARP, Request who-has 14.80.94.17 tell 14.80.94.16, length 46
11:44:56.281613 ARP, Request who-has 14.80.94.101 tell 14.80.94.1, length 46
```

U kunt de tcpdump uitvoeren en de opname in een .pcap-bestand schrijven met de opdracht **tcpdump -w TAC.pcap**.

Step 6.

U kunt de bestanden van de Jabber Guest Server met WinSCP verzamelen. Er wordt een productverbetering geopend om de pakketvastlegging van de web GUI af te nemen. Deze verbetering wordt onder:

https://tools.cisco.com/bugsearch/bug/CSCuu99856/?reffering_site=dumpcr