

Capturas de paquetes en Jabber Guest Server

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema: ¿Cómo se pueden tomar las capturas de paquetes del servidor invitado Jabber?](#)

[Solución](#)

[Conversaciones relacionadas de la comunidad de soporte de Cisco](#)

Introducción

Este documento describe cómo se pueden tomar las capturas de paquetes del servidor invitado Jabber.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- El invitado Jabber debe tener acceso a Internet para descargar el paquete.
- Software WinSCP instalado en el PC para recopilar las capturas.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Jabber Guest versiones 10.5 y 10.6
- Software WinSCP

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Problema: ¿Cómo se pueden tomar las capturas de paquetes del servidor invitado Jabber?

Solución

Paso 1.

El servidor Jabber Guest debe tener acceso a Internet para poder descargar el paquete desde Internet. En caso de que se utilice un proxy web, siga el procedimiento para permitir que CentOS en Jabber Guest utilice el proxy web para descargar el paquete.

Consulte el enlace <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html> para seguir el procedimiento.

Después de asegurarse de que el servidor de invitados Jabber puede descargar el paquete, vaya al paso 2.

Paso 2.

Inicie sesión en el servidor Jabber Guest con las credenciales raíz de Secure Socket Host (SSH) y ejecute el comando **yum search tcpdump** para encontrar la última versión de tcpdump.

```
[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 ~]#
```

Paso 3.

Ejecute el comando **yum install tcpdump** para instalar el paquete tcpdump en el servidor de invitados Jabber.

```
[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
```

Paso 4.

Se le envía a través de varios avisos. Ingrese y en cada componente para verificar cada mensaje.

Paso 5.

Tcpdump está ahora disponible de nuevo para capturas de paquetes desde el servidor de invitados Jabber.

```
name and summary matches only, use -search all for everything.
[root@jabberquest ~]# 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 jabberquest.havogel.com.ssh > 14.0.25.66.60858: Flags [P.], seq 1089242520:1089242728, ack 1202666623, win 20832, length 208
11:44:54.329007 IP jabberquest.havogel.com.50843 > ad.havogel.com.domain: 15118+ PTR? 66.25.0.14.in-addr.arpa. (41)
11:44:54.384348 IP jabberquest.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 > jabberquest.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
```

Puede ejecutar tcpdump y escribir la captura en un archivo .pcap usando el comando `tcpdump -w TAC.pcap`.

Paso 6.

Puede recopilar los archivos del servidor Jabber Guest con WinSCP. Se abre una mejora en el producto para tomar las capturas de paquetes de la GUI web y se realiza un seguimiento en:

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