

Capturas de pacotes no Jabber Guest Server

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema: Como as capturas de pacotes podem ser obtidas do Jabber Guest Server?](#)

[Solução](#)

[Discussões relacionadas da comunidade de suporte da Cisco](#)

Introduction

Este documento descreve como as capturas de pacotes podem ser obtidas do Jabber Guest Server.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- O Convidado Jabber deve ter acesso à Internet para baixar o pacote.
- Software WinSCP instalado no PC para coletar as capturas.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Jabber Guest versões 10.5 e 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: Como as capturas de pacotes podem ser obtidas do Jabber Guest Server?

Solução

Etapa 1.

O servidor Jabber Guest deve ter acesso à Internet para que ele faça o download do pacote da Internet. Caso um proxy da Web seja usado, siga o procedimento para permitir que o CentOS no Jabber Guest use o proxy da Web para baixar o pacote.

Consulte o link <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html> para seguir o procedimento.

Depois de verificar se o Jabber Guest Server pode baixar o pacote, vá para a Etapa 2.

Etapa 2.

Faça login no servidor Jabber Guest usando as credenciais raiz do Secure Socket Host (SSH) e execute o comando **yum search tcpdump** para encontrar a versão mais recente do 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 ~]#
```

Etapa 3.

Execute o comando **yum install tcpdump** para instalar o pacote tcpdump no Jabber Guest Server.

```
[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
```

Etapa 4.

Você é enviado através de vários avisos. Digite **y** em cada componente para verificar cada prompt.

Etapa 5.

O Tcpdump agora está disponível novamente para capturas de pacotes do Jabber Guest Server.

```
name and summary matches only, use -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
```

Você pode executar o tcpdump e gravar a captura em um arquivo .pcap usando o comando `tcpdump -w TAC.pcap`.

Etapa 6.

Você pode coletar os arquivos do Jabber Guest Server com WinSCP. Uma melhoria no produto para capturar as capturas de pacotes da GUI da Web é aberta e controlada em:

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