

Captures de paquets sur le serveur invité Jabber

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Problème : Comment les captures de paquets peuvent-elles être extraites de Jabber Guest Server ?](#)

[Solution](#)

[Discussions connexes de la communauté d'assistance Cisco](#)

Introduction

Ce document décrit comment les captures de paquets peuvent être prises à partir du serveur invité Jabber.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- L'invité Jabber doit avoir accès à Internet pour télécharger le package.
- Logiciel WinSCP installé sur le PC pour collecter les captures.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Jabber Guest versions 10.5 et 10.6
- Logiciel 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.

Problème : Comment les captures de paquets peuvent-elles être extraites de Jabber Guest Server ?

Solution

Étape 1.

Le serveur Jabber Guest doit avoir accès à Internet pour pouvoir télécharger le package à partir d'Internet. Si un proxy Web est utilisé, suivez la procédure pour permettre à CentOS sur Jabber Guest d'utiliser le proxy Web pour télécharger le package.

Reportez-vous au lien <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html> pour suivre la procédure.

Après vous être assuré que le serveur Jabber Guest Server peut télécharger le package, passez à l'étape 2.

Étape 2.

Connectez-vous au serveur Jabber Guest à l'aide des informations d'identification racine SSH (Secure Socket Host) et exécutez la commande **yum search tcpdump** pour rechercher la dernière version 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 ~]#
```

Étape 3.

Exécutez la commande **yum install tcpdump** pour installer le package tcpdump sur le serveur invité 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
```

Étape 4.

Vous êtes envoyé via plusieurs invites. Entrez **y** sur chaque composant pour vérifier chaque invite.

Étape 5.

Tcpdump est à nouveau disponible pour les captures de paquets à partir du serveur Jabber Guest

Server.

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

Vous pouvez exécuter tcpdump et écrire la capture sur un fichier .pcap à l'aide de la commande `tcpdump -w TAC.pcap`.

Étape 6.

Vous pouvez collecter les fichiers à partir du serveur Jabber Guest Server avec WinSCP. Une amélioration du produit permettant de capturer les paquets à partir de l'interface utilisateur graphique Web est ouverte et est suivie sous :

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