

Paketerfassung auf Jabber Guest Server

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem: Wie können Paketerfassungen von Jabber Guest Server übernommen werden?](#)

[Lösung](#)

[Ähnliche Diskussionen in der Cisco Support Community](#)

Einführung

In diesem Dokument wird beschrieben, wie Paketerfassungen vom Jabber Guest Server übernommen werden können.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Der Jabber Guest benötigt Zugriff auf das Internet, um das Paket herunterzuladen.
- WinSCP-Software auf dem PC installiert, um die Aufzeichnungen zu sammeln.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Jabber Guest-Versionen 10.5 und 10.6
- WinSCP-Software

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem: Wie können Paketerfassungen von Jabber Guest Server übernommen werden?

Lösung

Schritt 1:

Der Jabber Guest Server muss über Internetzugang verfügen, damit er das Paket aus dem Internet herunterladen kann. Falls ein Webproxy verwendet wird, befolgen Sie die Schritte, um CentOS auf Jabber Guest die Verwendung des Webproxys zum Herunterladen des Pakets zu ermöglichen.

Lesen Sie den Link <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html>, um das Verfahren zu befolgen.

Wenn Sie sichergestellt haben, dass das Paket von Jabber Guest Server heruntergeladen werden kann, fahren Sie mit Schritt 2 fort.

Schritt 2:

Melden Sie sich mit den SSH-Root-Anmeldeinformationen (Secure Socket Host) beim Jabber Guest-Server an, und führen Sie den Befehl `yum search tcpdump` aus, um die neueste Version von `tcpdump` zu finden.

```
[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 ~]#
```

Schritt 3:

Führen Sie den Befehl `yum install tcpdump` aus, um das `tcpdump`-Paket auf dem Jabber Guest Server zu installieren.

```
[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
```

Schritt 4:

Sie werden über mehrere Aufforderungen gesendet. Geben Sie `y` für jede Komponente ein, um jede Eingabeaufforderung zu überprüfen.

Schritt 5:

Tcpdump ist jetzt wieder für die Paketerfassung vom Jabber Guest Server verfügbar.

```
[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
```

Sie können tcpdump ausführen und die Erfassung in eine .pcap-Datei schreiben, indem Sie den Befehl `tcpdump -w TAC.pcap` verwenden.

Schritt 6:

Sie können die Dateien vom Jabber Guest Server mit WinSCP sammeln. Eine Erweiterung des Produkts zur Übernahme der Paketerfassungen über die Web-GUI wird geöffnet und unter:

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