

# Jabber 게스트 서버의 패킷 캡처

## 목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[문제/장애: Jabber Guest Server에서 패킷 캡처를 가져오는 방법](#)

[솔루션](#)

[관련 Cisco 지원 커뮤니티 토론](#)

## 소개

이 문서에서는 Jabber 게스트 서버에서 패킷 캡처를 가져오는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 패키지를 다운로드하려면 Jabber 게스트가 인터넷에 액세스할 수 있어야 합니다.
- 캡처를 수집하기 위해 PC에 WinSCP 소프트웨어가 설치되어 있습니다.

### 사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Jabber 게스트 버전 10.5 및 10.6
- WinSCP 소프트웨어

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 문제/장애: Jabber Guest Server에서 패킷 캡처를 가져오는 방법

## 솔루션

### 1단계.

인터넷에서 패키지를 다운로드하려면 Jabber 게스트 서버가 인터넷에 액세스할 수 있어야 합니다. 웹 프록시가 사용되는 경우 절차를 따라 Jabber Guest의 CentOS가 웹 프록시를 사용하여 패키지

를 다운로드하도록 허용합니다.

절차를 수행하려면 <https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html> 링크를 참조하십시오.

Jabber Guest Server가 패키지를 다운로드할 수 있는지 확인한 후 2단계로 진행합니다.

## 2단계.

SSH(Secure Socket Host) 루트 자격 증명을 사용하여 Jabber Guest 서버에 로그인하고 yum search tcpdump 명령을 실행하여 tcpdump의 최신 버전을 찾습니다.

```
[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 ~]#
```

## 3단계.

yum install tcpdump 명령을 실행하여 Jabber Guest Server에 tcpdump 패키지를 설치합니다.

```
[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
```

## 4단계.

여러 프롬프트를 통해 전송됩니다. 각 구성 요소에 y를 입력하여 각 프롬프트를 확인합니다.

## 5단계.

이제 Jabber 게스트 서버의 패킷 캡처에 대해 Tcpdump를 다시 사용할 수 있습니다.

```
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
```

tcpdump -w TAC.pcap 명령을 사용하여 tcpdump를 실행하고 .pcap 파일에 캡처를 쓸 수 있습니다.

## 6단계.

WinSCP를 사용하여 Jabber 게스트 서버에서 파일을 수집할 수 있습니다. 웹 GUI에서 패킷 캡처를 가져오는 제품에 대한 개선 사항이 열리며 다음 아래에서 추적됩니다.

[https://tools.cisco.com/bugsearch/bug/CSCuu99856/?referring\\_site=dumpcr](https://tools.cisco.com/bugsearch/bug/CSCuu99856/?referring_site=dumpcr)