

# Jabber ゲスト サーバでのパケット キャプチャ

## 内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題：Jabber Guestサーバからパケットキャプチャを取得する方法](#)

[解決方法](#)

[関連するシスコ サポート コミュニティ ディスカッション](#)

## 概要

このドキュメントでは、Jabber Guestサーバからパケットキャプチャを取得する方法について説明します。

## 前提条件

### 要件

次の項目に関する知識があることが推奨されます。

- パッケージをダウンロードするには、Jabber Guestがインターネットにアクセスできる必要があります。
- キャプチャを収集するためにPCにインストールされたWinSCPソフトウェア。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Jabber Guestバージョン10.5および10.6
- WinSCPソフトウェア

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

## 問題：Jabber Guestサーバからパケットキャプチャを取得する方法

### 解決方法

## ステップ 1 :

Jabber Guestサーバは、インターネットからパッケージをダウンロードするために、インターネットにアクセスする必要があります。Webプロキシを使用する場合は、Jabber Guest上のCentOSがWebプロキシを使用してパッケージをダウンロードできるようにする手順に従ってください。

手順については、リンク<https://www.centos.org/docs/5/html/yum/sn-yum-proxy-server.html>を参照してください。

Jabber Guest Serverがパッケージをダウンロードできることを確認したら、ステップ2に進みます。

## ステップ 2 :

Secure Socket Host (SSH)ルート資格情報を使用してJabber Guestサーバにログインし、`yum search tcpdump`コマンドを実行して最新バージョンのtcpdumpを検索します。

```
[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 ~]#
```

## ステップ 3 :

`yum install tcpdump`コマンドを実行し、tcpdumpパッケージをJabber Guestサーバにインストールします。

```
[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
```

## ステップ 4 :

いくつかのプロンプトが表示されます。各プロンプトを確認するには、各コンポーネントでyと入力します。

## ステップ 5 :

これで、Jabber Guest Serverからのパケットキャプチャに対してtcpdumpが再度使用可能になりました。

```
Name and Summary matches only, use -s or -S 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を実行し、.pcapファイルにキャプチャを書き込むには、tcpdump -w TAC.pcapコマンドを使用します。

手順 6 :

Jabber Guest ServerからWinSCPを使用してファイルを収集できます。Web GUIからパケットキャプチャを取得するための製品の機能拡張が開かれ、次の場所で追跡されます。

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