从CUCM linux平台服务器端抓包的方法

目录

硬件平台

在进行思科统一通信管理器(CUCM)相关的排错时，有时有必要抓取CUCM服务器网络接口收发的数据包。本文描述如何在CUCM服务器端进行抓包操作

软件版本

CUCM 6.x/7.x/8.x

操作步骤

1. 登陆CUCM命令行界面
   要进行CUCM服务器端的抓包操作，需要通过SSH登陆进CUCM的命令行(CLI)界面。登陆口令为服务器安装时设定的Administrator用户名/密码。
2. 运行抓包命令
   在命令行界面，抓包操作的命令为"utils network capture"，该命令的相关选项如下：

```
admin:utils network capture ?
Syntax:
utils network capture [options]
options  optional    page,numeric,file fname,count num,size bytes,src addr,dest addr,port
num,host protocol addr
options are:
page                    - pause output
numeric                 - show hosts as dotted IP addresses
file fname              - output the information to a file
    Note: The file will be saved in platform/cli/fname.cap
          fname should not contain the "." character
count num               - a count of the number of packets to capture
    Note: The maximum count for the screen is 1000, for a file is 100000
size bytes              - the number of bytes of the packet to capture
    Note: The maximum number of bytes for the screen is 128
          For a file it can be any number or ALL
src addr                - the source address of the packet as a host name or IPV4 address
dest addr               - the destination address of the packet as a host name or IPV4 address
port num                - the port number of the packet (either src or dest)
host protocol addr      - the protocol should be one of the following: ip/arp/rarp/all. The host
address of the packet as a host name or IPV4 address. This option  will display all packets to
and fro that address.
    Note: If "host" is provided, do not provide "src" or "dest"
verbose                 - The verbose out put
```

由此可见，通过不同参数的选择，"utils network capture"命令可以抓取目标地址、源地址、端口号

、指定包数量等，并将抓取到的包存为.cap文件。

一般来说，我们可以不加限制的抓取服务器网口的全部流量。命令如下：

```
utils network capture eth0 file packets count 100000 size all
```

此命令抓取全部流量，最大10000个包，并将其存为packets.cap文件

```
admin:utils network capture eth0 file packets count 100000 size all
Warning: existing packets.cap was renamed packets_2.cap
Executing command with options:
 size=ALL                count=100000            interface=eth0
 src=                    dest=                   port=
 ip=
```

3. 重现需要排障的问题 以上命令开始运行后，就可以重现需要排障的问题。问题重现的同时，CUCM将相关的流量都抓取下来，以供排错时查看。问题重现结束后，按”ctrl+C”可以停止抓包。CUCM会将刚刚抓取到的文件存至activelog platform/cli/ 路径下。如果该路径下已经存有文件名相同的抓包文件，CUCM会自动重命名已有旧文件。
4. 从服务器端下载抓包文件 4.1 SFTP
   SFTP server

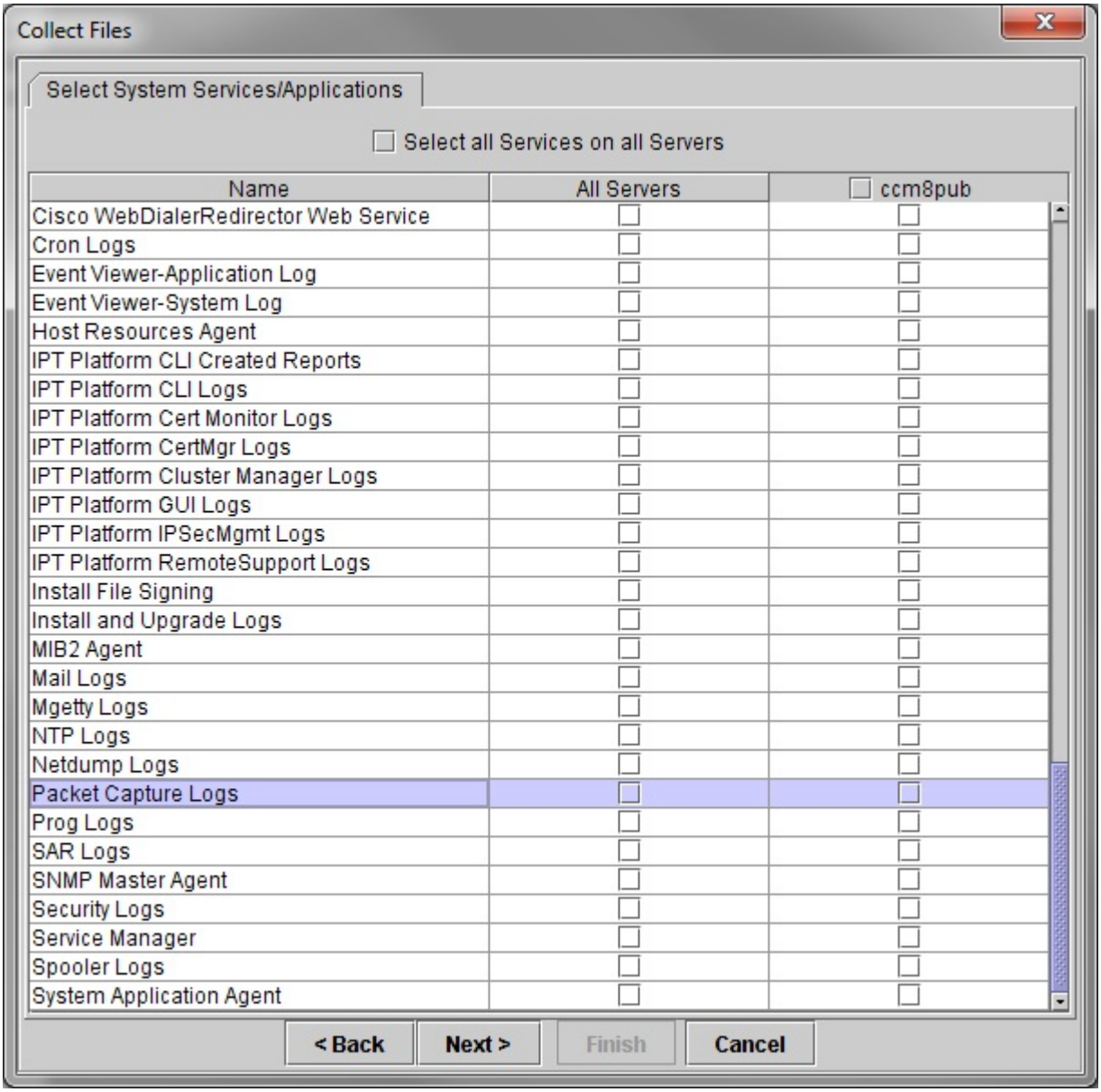
```
file get activelog platform/cli/packets.cap
```

```
admin:file get activelog platform/cli/packets.cap
Please wait while the system is gathering files info ...done.
Sub-directories were not traversed.
Number of files affected: 1
Total size in Bytes: 3428397
Total size in Kbytes: 3348.044
Would you like to proceed [y/n]? y
SFTP server IP: 10.125.30.233
SFTP server port [22]:
User ID: cisco
Password: *****

Download directory: /

The authenticity of host '10.125.30.233 (10.125.30.233)' can't be established.
RSA key fingerprint is cf:8f:3c:b4:75:aa:48:56:57:9b:62:a0:aa:48:a0:97.
Are you sure you want to continue connecting (yes/no)? yes
```

- 4.2 RTMT
  Real Time Monitoring Tool RTMT
  RTMTCUCMApplications->Plugins
  RTMTSystem->Trace & Log Centralcollect filesNext” Packet Capture Logs”



- 选择这一项，点击Next，在最后一页选择抓包操作的时间段和本地保存位置。点击Finish就可以将其下载到本地了。

经验总结

从CUCM服务器端抓包常用于抓取以下信息：

- IP 电话或其他终端在建立通话时和CUCM间进行的信令交互。
- CUCM提供MTP或transcoder资源时，终端与CUCM间的RTP流交互。
- CUCM集群服务器间以及CUCM和其他与其整合的服务器(Unity,UCCX等)间的信息交互。
- CUCM与网络中其他设备间的信息交互

相关命令

- utils network capture eth0 file packets count 100000 size all
- file get activelog platform/cli/packets.cap

参考文档

- Set Up Cisco CallManager Traces for Cisco Technical Support
- Command Line Interface Reference Guide for Cisco Unified Communications Solutions

Release 8.6(1)