

从CLI收集Expressway数据包捕获

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[数据包捕获过程](#)

[验证磁盘空间使用情况和捕获位置](#)

[捕获选项](#)

[开始并收集捕获](#)

[相关信息](#)

简介

本文档介绍如何使用Tcpdump功能从Expressway或视频通信服务器(VCS)的CLI收集数据包捕获。

先决条件

要求

Cisco 建议您了解以下主题：

- Cisco Expressway或Cisco VCS
- Tcpdump

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

数据包捕获过程

验证磁盘空间使用情况和捕获位置

1. 使用根用户和相关密码登录Expressway CLI。

```
login as: root
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
```

Expressway根登录

2. 使用命令验证磁盘空间使用情况，以确保有足够的空间来存储数据包捕获。

```
df /mnt/harddisk
```

3. 使用命令为要存储的捕获创建新目录。

```
mkdir /mnt/harddisk/capture
```

4. 定位至新创建的目录。

```
cd /mnt/harddisk/capture
```

捕获选项

可以使用带有各种选项的Tcpdump功能配置数据包捕获。命令可捕获任何接口上的数据包并写入名为Newcapture的文件。您可以指定任何所需的文件名和选项。

```
tcpdump -i any -w Newcapture
```

其他选项在[Tcpdump手册页](#)中进行了说明。

开始并收集捕获

1. 使用命令开始新的数据包捕获。命令中使用的选项可捕获Ethernet 0接口上的数据包，显示完整的数据包，并写入名为Newcapture的文件。

```
tcpdump -i eth0 -s 0 -w Newcapture
```

2. 捕获完所需的数据包后，停止捕获，同时按键盘上的Control (控制) 按钮和C (控制) 按钮。

```
^C15 packets captured
18 packets received by filter
0 packets dropped by kernel
```

Expressway命令行

3. 使用安全文件传输协议(SFTP)客户端将文件从捕获目录传输到本地计算机。

4. 使用命令删除新创建的目录和数据包捕获文件。

```
rm -r /mnt/harddisk/capture
```

相关信息

- [Tcpdump手册页](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。