

收集的CCM跟踪通过CLI

目录

[简介](#)

[背景信息](#)

[这是什么？](#)

[什么是这有用为？](#)

[先决条件](#)

[组件](#)

[收集文件](#)

简介

本文描述如何通过服务器的操作系统(OS)的命令行界面(CLI)所有Linux基于系统的收集Cisco CallManager (CCM)跟踪，万一不能访问实时监控工具(RTMT)应用程序。

贡献由基督徒Nuche (cnuche)，Cisco TAC工程师。

背景信息

这是什么？

CCM跟踪是呼叫控制进程的日志(Cisco CallManager进程)生成，这些应该设置选派，并且保证您把适当的复选框启用收集您希望的信息。

什么是这有用为？

这是有用排除故障在系统类似，呼叫路由问题的各种各样的问题，与其他系统，SIP或SCCP问题的互通性，GW相关问题，这些将基本上显示您什么CUCM执行内部地，当收到或做请求。

先决条件

组件

- CUCM的OS管理员密码
- 一个安全壳SSH客户端例如PuTTY，(<http://www.putty.org/>)
- 一个安全文件传输协议(SFTP)服务器类似FreeFTPd (<http://www.freesshd.com/?ctt=download>)关于关于如何的更多的指导信息配置和使用FreeFTPd看到：[如何配置统一通信的FreeFTPd](#)

收集文件

步骤1.打开PuTTY，并且登陆对CUCM CLI

注意：您需要执行在您要收集跟踪从的所有服务器的同一个步骤

步骤2.为了验证文件您需要使用list命令的文件。

文件列表{activelog|inactivelog|安装} FILE规格[页|详细信息|反向] [日期|大小]

文件的*The位置是：

```
activelog cm/trace/ccm/sdl/SDL*
activelog cm/trace/ccm/calllogs/calllogs*
activelog cm/trace/ccm/sdi/ccm* (CUCM 7.x和更加旧有)
```

如果需要下载其他种文件，您能找到文件位置—有用的列表：通信管理器RTMT CLI的Trace位置
<https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli>

示例

文件列表activelog cm/trace/ccm/sdl/SDL*详细信息

```
admin:
admin:file list activelog cm/trace/ccm/calllogs/calllogs* detail
20 Jan,2017 11:56:03      5,750  calllogs_00000001.txt.gz
28 Dec,2016 12:16:43      50    calllogs_~num.bin
dir count = 0, file count = 2
admin:
admin:
admin:
admin:file list activelog cm/trace/ccm/sdl/SDL* detail
23 Jan,2017 10:36:18      34    SDL001_100.index
27 Dec,2016 15:40:38    1,582,749  SDL001_100_000001.txt.gz
27 Dec,2016 17:06:51    1,600,498  SDL001_100_000002.txt.gz
27 Dec,2016 18:33:04    1,593,992  SDL001_100_000003.txt.gz
```

这显示您日期、时间、大小和文件名，您能下载您需要基于此信息仅的文件或您能收集在文件夹的所有文件。

步骤3. 下载有file命令的文件获得

文件获得{activelog|inactivelog|安装} FILE规格[reftime|abstime] [match regex] [recurs] [compress]

示例

文件获得activelog cm/trace/ccm/calllogs/calllogs*

此命令下载在文件夹的所有文件，系统提示您输入SFTP服务器详细信息，记住为了使用在微软视窗SFTP服务器的SFTP根您使用斜线(\)和为Linux根据您使用forwardslash的SFTP服务器(/)如下看到

:

```
admin:
admin:file get activelog cm/trace/ccm/calllogs/calllogs*
Please wait while the system is gathering files info ...
  Get file: /var/log/active/cm/trace/ccm/calllogs/calllogs_00000001.txt.gzo

  Get file: /var/log/active/cm/trace/ccm/calllogs/calllogs_~num.bin
done.
Sub-directories were not traversed.
Number of files affected: 2
Total size in Bytes: 5800
Total size in Kbytes: 5.6640625
Would you like to proceed [y/n]? y
SFTP server IP: 10.152.196.57
SFTP server port [22]:
User ID: cisco
Password: *****
Download directory: \

The authenticity of host '10.152.196.57 (10.152.196.57)' can't be established.
RSA key fingerprint is bf:1c:9e:60:bd:24:aa:fb:21:06:a7:65:16:51:e0:e3.
Are you sure you want to continue connecting (yes/no)? yes
..
Transfer completed.
admin:█
```

如果获得任何.gzo文件那些是开放的您当时下载他们，您很可能不能打开他们的文件，但是文件的其余应该是您能解压缩与7 ZIP的.gz (<http://www.7-zip.org/>)，万一要打开文件。

```
admin:file list activelog cm/trace/ccm/calllogs/calllogs*
calllogs_00000001.txt.gzo ←
calllogs_00000002.txt.gz ←
calllogs_00000003.txt.gz
calllogs_00000004.txt.gz
calllogs_~num.bin
dir count = 0, file count = 5
```

如果需要打开您能使用CLI命令文件视图和使用整个路径的gzo文件，并且包括文件名，在这种情况下您需要复制输出和粘贴它在支持Unix行尾的文本编辑，类似Notepad++

```
admin:
admin:file list activelog cm/trace/ccm/calllogs/calllogs*
calllogs_00000001.txt.gzo          calllogs_~num.bin
dir count = 0, file count = 2
admin:
admin:
admin:
admin:file view activelog cm/trace/ccm/calllogs/calllogs_00000001.txt.gzo

2016/12/28 12:16:43.440|SIPL|0|TCP|IN|10.122.141.60|5060|SEPO0EBD5DA106E|10.88.2
49.90|52925|1,100,14,12.693^10.88.249.90^*|18201|00ebd5da-106e0004-4d7323e2-6966
9318@10.88.249.90|INVITE
```

您能也使用所有Linux方框获得内容，在这种情况下使用命令`zcat <filename>`

```
[root@cmlabmex calllogs]# ls -l
total 12
-rw-r--r--. 1 ccmbase ccmbase 5750 Jan 20 11:56 calllogs_00000001.txt.gzo
-rw-r--r--. 1 ccmbase ccmbase  50 Dec 28 12:16 calllogs_~num.bin
[root@cmlabmex calllogs]# zcat calllogs_00000001.txt.gzo
2016/12/28 12:16:43.440|SIPL|0|TCP|IN|10.122.141.60|5060|SEPO0EBD5DA106E|10.88.2
49.90|52925|1,100,14,12.693^10.88.249.90^*|18201|00ebd5da-106e0004-4d7323e2-6966
9318@10.88.249.90|INVITE
```

第三步：一旦有您需要的所有文件，请创建包含文件您下载的压缩文件并且添加所有文件夹，然后上传他们到您的TAC案例到案件文件uploader工具：<https://cway.cisco.com/csc>

步骤4.通知您工作与那您上传文件的TAC工程师。

提示：切记添加包含的设备的IP、MAC和主机名，测验/事件、源和目的编号，(如果请应用)和发生什么的详细说的日期和时间。如果TAC工程师不了解什么他或她应该寻找能困难获得查找，并且这能更大量需要时间查找它，那么请包括该信息