Collect CCM Traces Through CLI

Contents

Introduction
Background Information
What is it?
What is it helpful for?
Prerequisites
Components
Collect the files

Introduction

This document describes how to collect Cisco CallManager (CCM) traces through the Command Line Interface (CLI) of the server's Operating System (OS) for any Linux based system, in case you cannot access the Real-Time Monitoring Tool (RTMT) application.

Contributed by Christian Nuche (cnuche), Cisco TAC Engineer.

Background Information

What is it?

CCM traces are logs that the call control process (Cisco CallManager process) generates, these should be set to *detail* and ensure you have the appropriate checkboxes enabled to collect the information you want.

What is it helpful for?

This is helpful to troubleshoot a variety of issues on the system like, call route issues, interoperability with other systems, SIP or SCCP issues, GW related issues, these will basically show you what CUCM does internally when it receives or makes a request.

Prerequisites

Components

- CUCM's OS Administrator password
- A Secure Shell (SSH) client such as putty, (http://www.putty.org/)

- A Secure File Transfer Protocol (SFTP) server like FreeFTPd (http://www.freesshd.com/?ctt=download) for detailed instructions on how to configure and use FreeFTPd see: How to configure FreeFTPD for Unified Communications

Collect the files

Step 1. Open Putty, and log in to the CUCM CLI

Note: You need to perform the same procedure on all servers you want to collect traces from

Step 2. In order to verify the files you need use the **file list** command.

file list { activelog | inactivelog | install } *file-spec* **[page | detail | reverse] [date | size]**

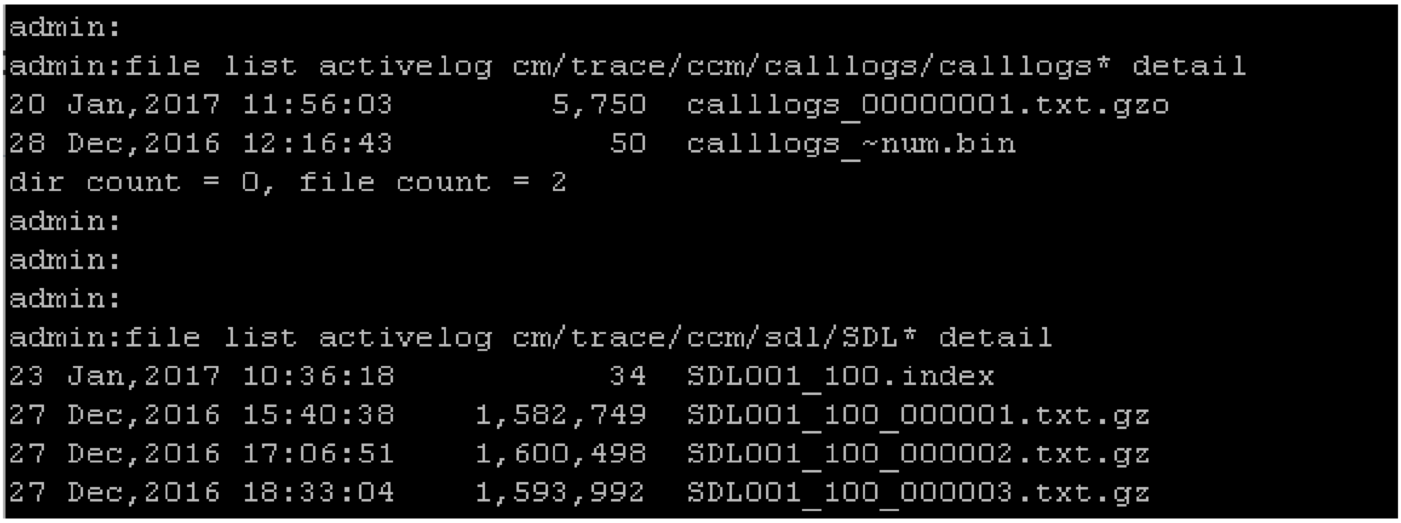
* The location of the files are:

activelog cm/trace/ccm/sdl/SDL*
activelog cm/trace/ccm/calllogs/calllogs*
activelog cm/trace/ccm/sdi/ccm* (CUCM 7.x and older)

If you need to download other type of files, you can find a useful list of file locations on:
Communications Manager RTMT Trace Locations in CLI
https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli

Example

file list activelog cm/trace/ccm/sdl/SDL* detail



```
admin:
admin:file list activelog cm/trace/ccm/calllogs/calllogs* detail
20 Jan,2017 11:56:03         5,750  calllogs_00000001.txt.gzo
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
```

This shows you the date, time, size and filename, you can download only the files you need based on this information or you can collect all the files in the folder.

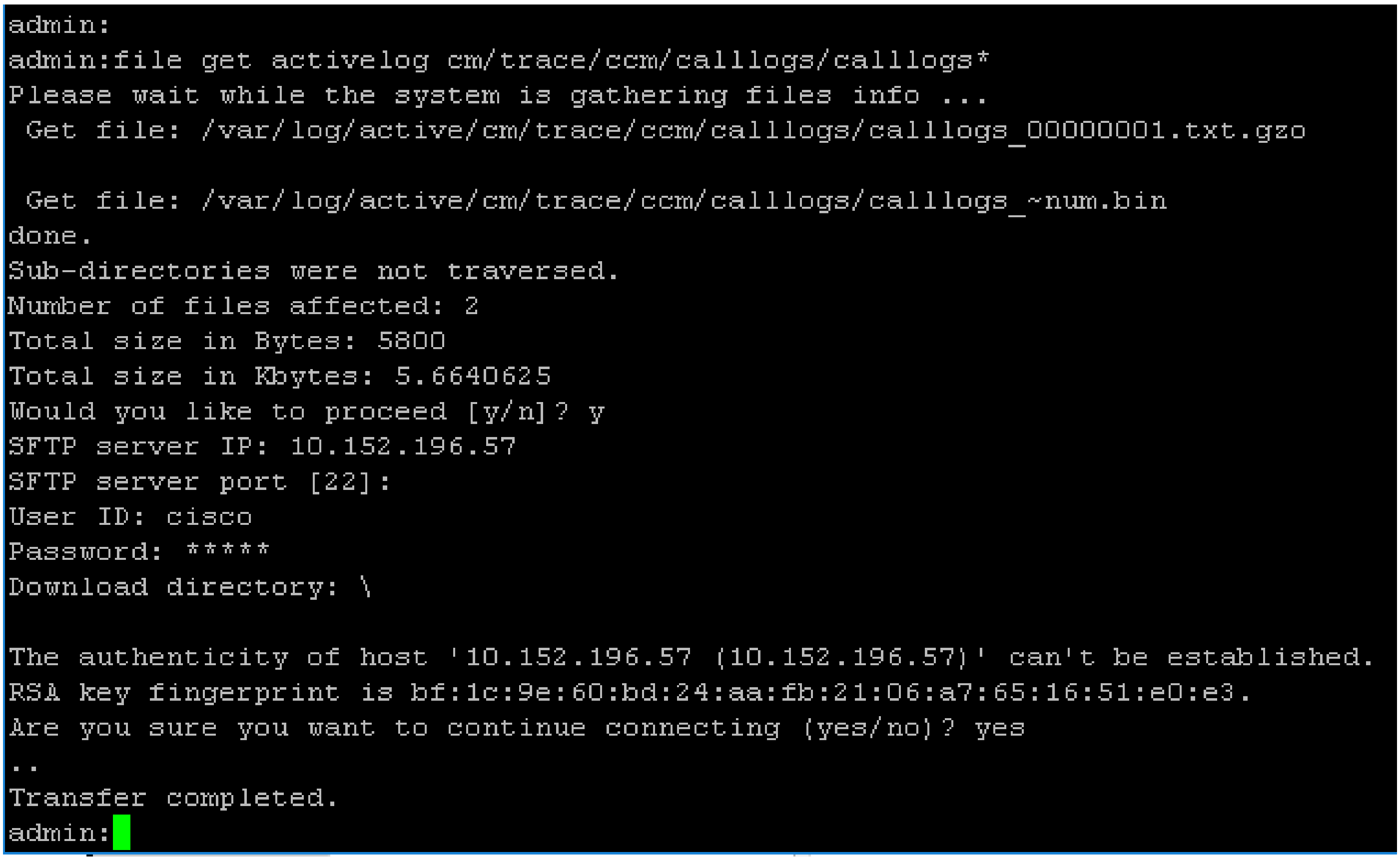
Step 3. Download the files with the command **file get**

file get { **activelog | inactivelog | install** } *file-spec* [*reltime* | *abstime*] [**match** *regex*] [**recurs**] [**compress**]

Example

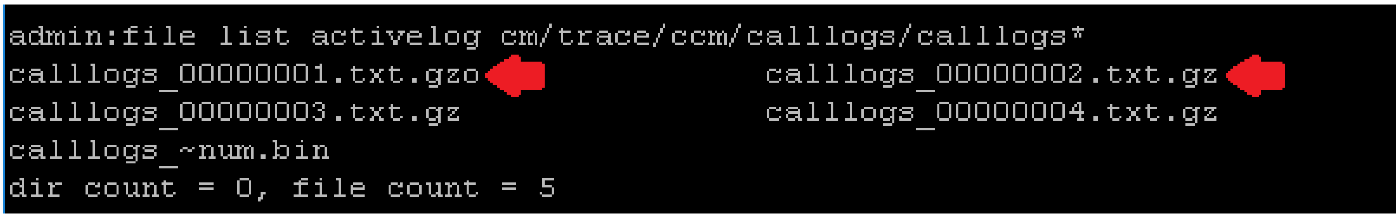
file get activelog cm/trace/ccm/calllogs/calllogs*

This command downloads all files in the folder, the system prompts you for the SFTP server details, remember that in order to use the SFTP root on windows based SFTP servers you use backslash (\), and for Linux based SFTP servers you use forwardslash (/) see below:



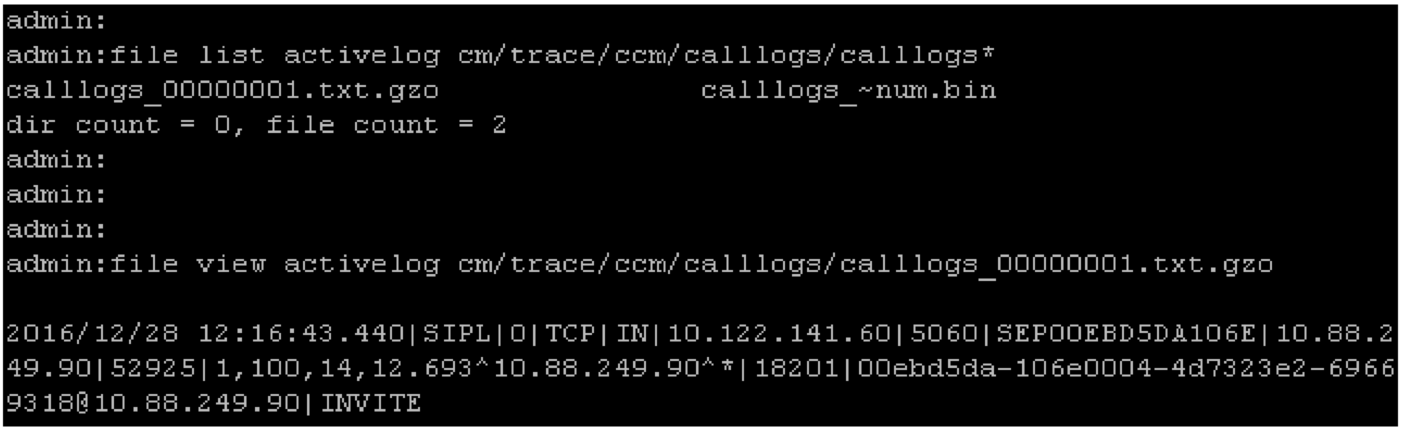
```
admin:
admin:file get activelog cm/trace/ccm/calllogs/calllogs*
Please wait while the system is gathering files info ...
 Get file: /var/log/active/cm/trace/ccm/calllogs/calllogs_00000001.txt.gzo

 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:
```

If you get any .gzo files those are files that were open at the time you download them, you probably wont be able to open them but the rest of the files should be .gz that you can extract with 7-zip (http://www.7-zip.org/) in case you want to open the files.



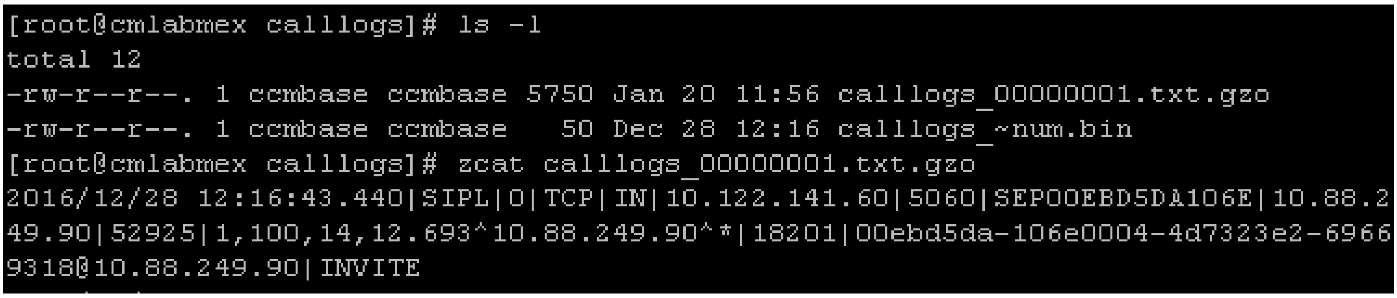
```
admin:file list activelog cm/trace/ccm/calllogs/calllogs*
calllogs_00000001.txt.gzo                calllogs_00000002.txt.gz
calllogs_00000003.txt.gz                 calllogs_00000004.txt.gz
calllogs_~num.bin
dir count = 0, file count = 5
```

If you need to open the gzo files you can use the CLI command **file view** and use the entire path, and include the filename, in this case you need to copy the output and paste it on a text editor that supports Unix end of lines, like 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|SEP00EBD5DA106E|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
```

You can also use any linux box to get the content, in this case use the command **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|SEP00EBD5DA106E|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
```

Step 3. Once you have all the files you need, create a zip file and add all the folders that contains the files you just download, then upload them to your TAC case through the case file uploader tool: https://cway.cisco.com/csc

Step 4. Notify the TAC engineer you work with that you have uploaded the files.

Tip: Remember to add the IPs, MACs, and hostnames of the involved devices, date and time of the test / event, source and destination numbers, (if apply), and a detailed description of what happened. If the TAC engineer does not know what he/she should look for it can get harder to find, and it can take a lot more time to find it, so please include that information