

# Recopilación de seguimientos de CCM a través de CLI

## Contenido

[Introducción](#)

[Antecedentes](#)

[¿Qué es?](#)

[¿Para qué sirve?](#)

[Prerequisites](#)

[Componentes](#)

[Recopilar los archivos](#)

## Introducción

Este documento describe cómo recopilar seguimientos de Cisco CallManager (CCM) a través de la interfaz de línea de comandos (CLI) del sistema operativo (OS) del servidor para cualquier sistema basado en Linux, en caso de que no pueda acceder a la aplicación Real-Time Monitoring Tool (RTMT).

Contribuido por Christian Nuche (cnuche), ingeniero del TAC de Cisco.

## Antecedentes

### ¿Qué es?

Los seguimientos de CCM son registros que genera el proceso de control de llamadas (proceso de Cisco CallManager), deben configurarse en *detalle* y asegurarse de que tiene habilitadas las casillas de verificación adecuadas para recopilar la información que desea.

### ¿Para qué sirve?

Esto es útil para solucionar una variedad de problemas en el sistema como problemas de ruta de llamada, interoperabilidad con otros sistemas, problemas de SIP o SCCP, problemas relacionados con GW, que básicamente le mostrarán lo que CUCM hace internamente cuando recibe o realiza una solicitud.

## Prerequisites

## Componentes

- Contraseña del administrador del sistema operativo de CUCM
- Un cliente Secure Shell (SSH) como putty (<http://www.putty.org/>)
- Un servidor de protocolo seguro de transferencia de archivos (SFTP) como FreeFTPd (<http://www.freesshd.com/?ctt=download>) para obtener instrucciones detalladas sobre cómo configurar y utilizar FreeFTPd, consulte: [Cómo configurar FreeFTPd para Unified Communications](#)

## Recopilar los archivos

Paso 1. Abra Putty e inicie sesión en CUCM CLI

**Nota:** Debe realizar el mismo procedimiento en todos los servidores de los que desea recopilar seguimientos

Paso 2. Para verificar los archivos que necesita utilice el comando **file list**.

**file list { activelog | inactivelog | install } file-spec [ página | detalle | revertir ] [ fecha | tamaño**

\* La ubicación de los archivos es:

activelog cm/trace/ccm/sdl/SDL\*

activelog cm/trace/ccm/calllogs/calllogs\*

activelog cm/trace/ccm/sdi/ccm\* (CUCM 7.x y posterior)

Si necesita descargar otro tipo de archivos, puede encontrar una lista útil de ubicaciones de archivos en: Communications Manager RTMT Trace Locations en CLI

<https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli>

Ejemplo:

detalle de la lista de archivos activelog cm/trace/ccm/sdl/SDL\*

```
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
```

Esto le muestra la fecha, hora, tamaño y nombre de archivo, sólo puede descargar los archivos que necesita en función de esta información o puede recopilar todos los archivos de la carpeta.

Paso 3. Descargue los archivos con el comando **file get**

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

Ejemplo:

```
archivo get activelog cm/trace/ccm/calllogs/calllogs*
```

Este comando descarga todos los archivos de la carpeta, el sistema le solicita los detalles del servidor SFTP, recuerde que para utilizar la raíz SFTP en los servidores SFTP basados en Windows se utiliza la barra invertida (\) y para los servidores SFTP basados en Linux se utiliza la barra invertida (/), consulte a continuación:

```

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:

```

Si obtiene archivos .gzo que son archivos que estaban abiertos en el momento de descargarlos, probablemente no podrá abrirlos, pero el resto de los archivos debe ser .gz que puede extraer con [7-zip](http://www.7-zip.org/) (<http://www.7-zip.org/>) en caso de que desee abrir los archivos.

```

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

```

Si necesita abrir los archivos gzo puede utilizar el comando CLI **file view** y utilizar la ruta completa, e incluir el nombre del archivo, en este caso debe copiar el resultado y pegarlo en un editor de texto que soporte el fin de las líneas Unix, como 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

```

También puede utilizar cualquier cuadro linux para obtener el contenido, en este caso utilice el comando **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|SEP00EBD5D&106E|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
```

Paso 3. Una vez que tenga todos los archivos que necesita, cree un archivo zip y agregue todas las carpetas que contienen los archivos que acaba de descargar y, a continuación, cárguelos en su caso TAC a través de la herramienta de carga de archivos de casos:

<https://cway.cisco.com/csc>

Paso 4. Notifique al ingeniero del TAC con el que trabaja que ha cargado los archivos.

**Consejo:** Recuerde agregar las IP, los MAC y los nombres de host de los dispositivos involucrados, la fecha y hora de la prueba/evento, los números de origen y de destino (si procede) y una descripción detallada de lo que ocurrió. Si el ingeniero del TAC no sabe lo que debe buscar, puede ser más difícil de encontrar, y puede llevar mucho más tiempo encontrarlo, por lo que incluya esa información