

通過CLI收集CCM跟蹤

目錄

[簡介](#)

[背景資訊](#)

[是什麼？](#)

[它對什麼有幫助？](#)

[必要條件](#)

[元件](#)

[收集檔案](#)

簡介

本文檔介紹如何通過任何基於Linux的系統的伺服器作業系統(OS)的命令列介面(CLI)收集Cisco CallManager(CCM)跟蹤，以防無法訪問即時監控工具(RTMT)應用程式。

作者：Christian Nuche(cnuche)，思科TAC工程師。

背景資訊

是什麼？

CCM跟蹤是呼叫控制進程（Cisco CallManager進程）生成的日誌，應將其設定為`detail`，並確保啟用相應的覈取方塊來收集所需的資訊。

它對什麼有幫助？

這有助於排除系統上的各種問題，例如呼叫路由問題、與其他系統的互操作性問題、SIP或SCCP問題、GW相關問題，這些基本將為您顯示CUCM在收到或發出請求時在內部執行的操作。

必要條件

元件

- CUCM的作業系統管理員密碼
- 安全殼層(SSH)客戶端，例如putty(<http://www.putty.org/>)
- 安全檔案傳輸通訊協定(SFTP)伺服器(例如FreeFTPd(<http://www.freesshd.com/?ctt=download>))有關如何設定和使用FreeFTPd的詳細說明，請參閱：[如何為統一通訊配置FreeFTPd](#)

收集檔案

步驟1.開啟Putty並登入到CUCM CLI

附註： 您需要在要從中收集跟蹤的所有伺服器上執行相同的過程

步驟2.若要驗證檔案，需要使用file list 指令。

檔案清單{ activelog | inactivelog |安裝} file-spec [頁 |詳細資訊 |反向] [日期 |大小]

*檔案的位置為：

```
activelog cm/trace/ccm/sdl/SDL*
activelog cm/trace/ccm/calllogs/calllogs*
activelog cm/trace/ccm/sdi/ccm* ( CUCM 7.x及更高版本 )
```

如果您需要下載其他型別的檔案，可以在以下位置找到有用的檔案位置清單： CLI中的 Communications Manager RTMT跟蹤位置

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

範例

file list activelog cm/trace/ccm/sdl/SDL*詳細資訊

```
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
```

這將向您顯示日期、時間、大小和檔名，您可以根據此資訊僅下載所需的檔案，也可以收集資料夾中的所有檔案。

步驟3.使用get指令檔案下載檔案

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

範例

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

此命令將下載資料夾中的所有檔案，系統提示您輸入SFTP伺服器詳細資訊，請記住，要在基於windows的SFTP伺服器上使用SFTP根目錄，您需要使用反斜線(\)，而對於基於Linux的SFTP伺服器，您需要使用轉發線(/)，請參閱下文：

```
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:█
```

如果您獲得了任何.gzo檔案，這些檔案是下載時開啟的檔案，則可能無法開啟它們，但其餘檔案應是.gz，您可以使用7-zip(<http://www.7-zip.org/>)解壓該檔案以備您開啟這些檔案。

```
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
calllogs_00000002.txt.gz
calllogs_00000004.txt.gz
```

如果您需要開啟gzo檔案，可以使用CLI命令file view並使用整個路徑，包括檔名，在這種情況下，您需要複製輸出並將其貼上到支援Unix行尾的文本編輯器中，如記事本++

```
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
```

您還可以使用任何linux框來獲取內容，在這種情況下，請使用`zcat <filename>`命令

```
[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
```

步驟3.收到所需的所有檔案後，建立一個zip檔案，並新增包含剛下載的檔案的所有資料夾，然後透過檔案上傳程式工具將它們上傳到TAC案例：<https://cway.cisco.com/csc>

步驟4.通知您使用的TAC工程師您已上傳檔案。

提示：請記得新增相關裝置的IP、MAC和主機名、測試/事件的日期和時間、源和目標號碼（如果適用）以及所發生情況的詳細說明。如果TAC工程師不知道他/她應該查詢什麼內容，則查詢會比較困難，並且查詢時間會較長，因此請包含此資訊