Erfassung von CCM-Traces über die CLI

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie Cisco CallManager (CCM)-Ablaufverfolgungen über die Befehlszeilenschnittstelle (CLI) des Serverbetriebssystems für ein Linux-basiertes System erfasst werden, falls Sie nicht auf die RTMT-Anwendung (Real-Time Monitoring Tool) zugreifen können.

Mitarbeiter: Christian Nuche (cnuche), Cisco TAC Engineer.

Hintergrundinformationen

Was ist das?

CCM-Ablaufverfolgungen sind Protokolle, die vom Anrufsteuerungsprozess (Cisco CallManager-Prozess) generiert werden. Sie sollten so eingestellt werden, dass *Details* festgelegt werden und sicherstellen, dass die entsprechenden Kontrollkästchen aktiviert sind, um die gewünschten Informationen zu erfassen.

Wofür ist es hilfreich?

Dies ist hilfreich, um eine Reihe von Systemproblemen zu beheben, wie z. B. Probleme bei der Anrufweiterleitung, Interoperabilität mit anderen Systemen, SIP- oder SCCP-Probleme, GW-bezogene Probleme. Diese zeigen Ihnen im Grunde, was CUCM intern tut, wenn er eine Anforderung empfängt oder sendet.

Voraussetzungen

Komponenten

- CUCM-Administratorkennwort
- Ein Secure Shell (SSH)-Client wie putty (http://www.putty.org/)
- Ein Secure File Transfer Protocol (SFTP)-Server wie FreeFTPd (http://www.freesshd.com/?ctt=download) enthält detaillierte Anweisungen zur Konfiguration und Verwendung von FreeFTPd: Konfiguration von FreeFTPD für Unified Communications

Erfassen der Dateien

Schritt 1: Öffnen Sie Putty, und melden Sie sich bei der CUCM-CLI an.

> **Hinweis**: Sie müssen die gleiche Prozedur auf allen Servern ausführen, von denen Sie Traces erfassen möchten.

Schritt 2: Um die erforderlichen Dateien zu überprüfen, verwenden Sie den Befehl **file list**.

file list { activelog | inactivelog | install } *Dateispez.* **[Seite | Details | reverse] [date] | size]**

* Der Speicherort der Dateien ist:

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

Wenn Sie andere Dateitypen herunterladen müssen, finden Sie eine nützliche Liste der Dateispeicherorte unter: Communications Manager RTMT Trace Locations in CLI https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli

Beispiel

Dateiliste 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
```

Hier sehen Sie Datum, Uhrzeit, Größe und Dateiname, Sie können nur die Dateien herunterladen, die Sie aufgrund dieser Informationen benötigen, oder Sie können alle Dateien im Ordner sammeln.

Schritt 3: Laden Sie die Dateien mit dem Befehl **file get herunter**

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

Beispiel

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

Dieser Befehl lädt alle Dateien im Ordner herunter, das System fordert Sie zur Eingabe der SFTP-Serverdetails auf, bedenken Sie, dass Sie für die Verwendung des SFTP-Root auf Windows-basierten SFTP-Servern einen umgekehrten Schrägstrich (\) verwenden, und für Linux-basierte SFTP-Server den Forwardslash (/) wie folgt verwenden:

```
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:
```

Wenn Sie .gzo-Dateien erhalten, die zum Zeitpunkt des Downloads geöffnet waren, können Sie diese möglicherweise nicht öffnen, aber die restlichen Dateien sollten .gz sein, das Sie mit 7-zip (http://www.7-zip.org/) extrahieren können, falls Sie die Dateien öffnen möchten.

```
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
```

Wenn Sie die gzo-Dateien öffnen möchten, können Sie die CLI-Befehlsdateiansicht verwenden und den gesamten Pfad verwenden und den Dateinamen einschließen. In diesem Fall müssen Sie die Ausgabe kopieren und in einen Texteditor einfügen, der Unix-Zeilenende unterstützt, z. B. 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
```

Sie können auch jede Linux-Box verwenden, um den Inhalt zu erhalten, in diesem Fall verwenden

Sie den Befehl 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
```

Schritt 3: Wenn Sie alle erforderlichen Dateien haben, erstellen Sie eine ZIP-Datei, fügen alle Ordner hinzu, die die Dateien enthalten, die Sie gerade herunterladen, und laden Sie sie dann über das Uploader-Tool für Ticket-Dateien in Ihr TAC-Ticket hoch: https://cway.cisco.com/csc

Schritt 4: Benachrichtigen Sie den TAC-Techniker, mit dem Sie zusammenarbeiten, dass Sie die Dateien hochgeladen haben.

> Tipp: Denken Sie daran, die IPs, MACs und Hostnamen der beteiligten Geräte, Datum und Uhrzeit des Tests/Ereignisses, Quell- und Zielnummern (falls zutreffend) sowie eine detaillierte Beschreibung der Ereignisse hinzuzufügen. Wenn der TAC-Techniker nicht weiß, worauf er achten sollte, kann es schwieriger werden, ihn zu finden, und es kann viel mehr Zeit dauern, ihn zu finden. Fügen Sie diese Informationen daher hinzu.