Collecter les suivis CCM via l'interface de ligne de commande

Contenu

Introduction

Ce document décrit comment collecter les traces de Cisco CallManager (CCM) via l'interface de ligne de commande (CLI) du système d'exploitation (OS) du serveur pour tout système Linux, au cas où vous ne pourriez pas accéder à l'application RTMT (Real-Time Monitoring Tool).

Contribué par Christian Nuche (cnuche), ingénieur du centre d'assistance technique Cisco.

Informations générales

Quel est-il ?

Les traces CCM sont des journaux générés par le processus de contrôle d'appel (processus Cisco CallManager), qui doivent être définis en *détail* et vous assurer que les cases à cocher appropriées sont activées pour collecter les informations souhaitées.

Àquoi cela sert-il ?

Ceci est utile pour résoudre un grand nombre de problèmes sur le système, comme les problèmes de routage des appels, d'interopérabilité avec d'autres systèmes, les problèmes SIP ou SCCP, les problèmes liés à GW, qui vous montreront en gros ce que CUCM fait en interne lorsqu'il reçoit ou fait une demande.

Conditions préalables

Composants

- Mot de passe de l'administrateur du système d'exploitation de CUCM
- Un client Secure Shell (SSH) tel que putty (http://www.putty.org/)
- Un serveur SFTP (Secure File Transfer Protocol) tel que FreeFTPd (http://www.freesshd.com/?ctt=download) pour des instructions détaillées sur la configuration et l'utilisation de FreeFTPd voir : Comment configurer FreeFTPD pour les communications unifiées

Collecter les fichiers

Étape 1. Ouvrez Putty et connectez-vous à l'interface de ligne de commande CUCM

> **Note**: Vous devez effectuer la même procédure sur tous les serveurs à partir desquels vous voulez collecter des traces

Étape 2. Pour vérifier les fichiers, utilisez la commande **file list**.

liste de fichiers { activelog | inactivelog | installer } *file-spec* **[page | détail | inverser] [date | taille]**

* L'emplacement des fichiers est le suivant :

activelog cm/trace/ccm/sdl/SDL*
activelog cm/trace/ccm/calllogs/calllogs*
activelog cm/trace/ccm/sdi/ccm* (CUCM 7.x et versions ultérieures)

Si vous avez besoin de télécharger d'autres types de fichiers, vous pouvez trouver une liste utile d'emplacements de fichiers sur : Communications Manager RTMT Trace Locations dans CLI https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli

Exemple

liste de fichiers détails 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
```

Cela vous montre la date, l'heure, la taille et le nom de fichier, vous pouvez télécharger uniquement les fichiers dont vous avez besoin en fonction de ces informations ou vous pouvez collecter tous les fichiers dans le dossier.

Étape 3. Télécharger les fichiers avec le **fichier** de commande **get**

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

Exemple

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

Cette commande télécharge tous les fichiers du dossier, le système vous invite à entrer les détails du serveur SFTP, souvenez-vous que pour utiliser la racine SFTP sur les serveurs SFTP Windows, vous utilisez la barre oblique inverse (\) et pour les serveurs SFTP Linux, vous utilisez la barre oblique inverse (/) voir ci-dessous :

```
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 vous obtenez des fichiers .gzo qui sont des fichiers ouverts au moment où vous les téléchargez, vous ne pourrez probablement pas les ouvrir mais le reste des fichiers devrait être .gz que vous pouvez extraire avec 7-zip (http://www.7-zip.org/) au cas où vous voulez ouvrir les fichiers.

```
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
```

Si vous devez ouvrir les fichiers gzo, vous pouvez utiliser l'**affichage** du **fichier** de commande CLI et utiliser le chemin d'accès complet, et inclure le nom du fichier. Dans ce cas, vous devez copier le résultat et le coller dans un éditeur de texte prenant en charge les lignes de fin Unix, comme 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
```

Vous pouvez également utiliser n'importe quelle boîte linux pour obtenir le contenu, dans ce cas, utilisez la commande **zcat** *<nom de fichier>*

```
[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
```

Étape 3. Une fois que vous avez tous les fichiers dont vous avez besoin, créez un fichier zip et ajoutez tous les dossiers qui contiennent les fichiers que vous venez de télécharger, puis téléchargez-les dans votre dossier TAC à l'aide de l'outil de téléchargement des fichiers de dossiers : https://cway.cisco.com/csc

Étape 4. Avertissez l'ingénieur TAC avec lequel vous travaillez que vous avez téléchargé les fichiers.

> **Astuce** : N'oubliez pas d'ajouter les adresses IP, les adresses MAC et les noms d'hôte des périphériques concernés, la date et l'heure du test/événement, les numéros d'origine et de destination (le cas échéant) et une description détaillée de ce qui s'est passé. Si l'ingénieur du centre d'assistance technique ne sait pas ce qu'il doit rechercher, cela peut devenir plus difficile à trouver et cela peut prendre beaucoup plus de temps pour le trouver. Veuillez donc inclure ces informations