Coletar rastreamentos do CCM por meio da CLI

Contents

Introduction

Este documento descreve como coletar rastreamentos do Cisco CallManager (CCM) através da CLI (Command Line Interface, interface de linha de comando) do sistema operacional (OS) do servidor para qualquer sistema baseado em Linux, caso você não possa acessar o aplicativo RTMT (Real-Time Monitoring Tool, ferramenta de monitoramento em tempo real).

Contribuído por Christian Nuche (cnuche), engenheiro do TAC da Cisco.

Informações de Apoio

O que é?

Os rastreamentos do CCM são registros gerados pelo processo de controle de chamadas (processo do Cisco CallManager), que devem ser definidos com *detalhes* e garantir que você tenha as caixas de seleção apropriadas habilitadas para coletar as informações desejadas.

Para que é útil?

Isso é útil para solucionar uma variedade de problemas no sistema, como problemas de rota de chamadas, interoperabilidade com outros sistemas, problemas de SIP ou SCCP, problemas relacionados ao GW, esses problemas basicamente mostrarão o que o CUCM faz internamente quando recebe ou faz uma solicitação.

Prerequisites

Componentes

- Senha do administrador do SO do CUCM
- Um cliente Secure Shell (SSH) como putty, (http://www.putty.org/)
- Um servidor Secure File Transfer Protocol (SFTP) como FreeFTPd (http://www.freesshd.com/?ctt=download) para obter instruções detalhadas sobre como configurar e usar o FreeFTPd consulte: Como configurar o FreeFTPD para Unified Communications

Coletar os arquivos

Etapa 1. Abra o Putty e faça login na CLI do CUCM

> **Note**: Você precisa executar o mesmo procedimento em todos os servidores dos quais deseja coletar rastreamentos

Etapa 2. Para verificar os arquivos necessários, use o comando **file list**.

lista de arquivos { ativelog | inativelog | instalar } *file-spec* **[página | pormenor | reverso] [data | dimensão]**

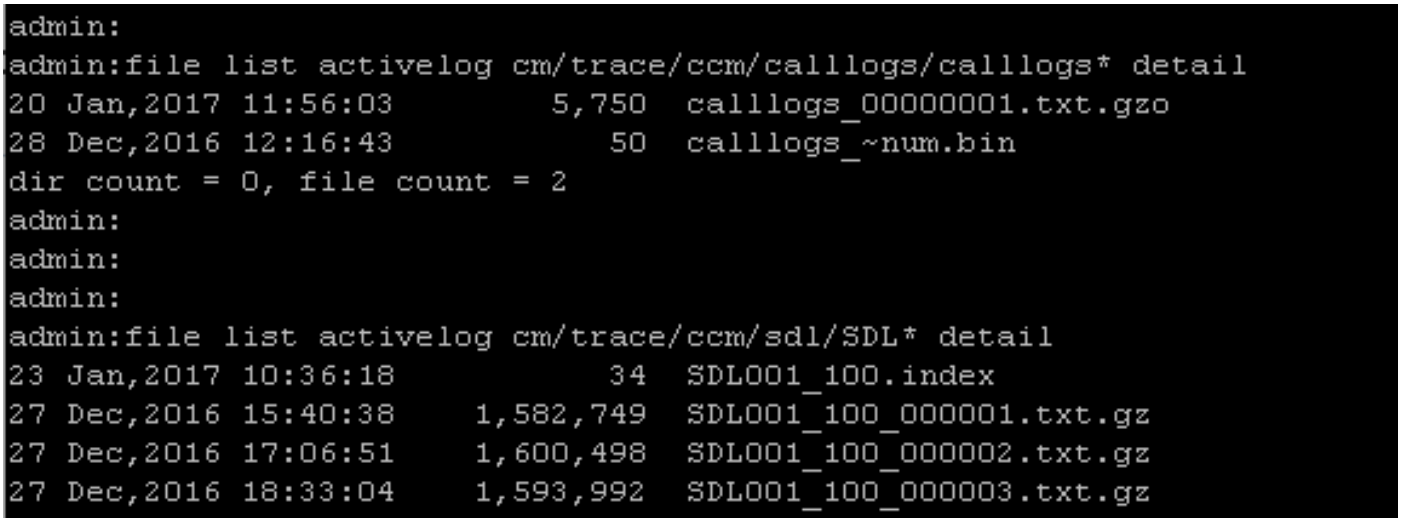
* A localização dos arquivos é:

ativelog cm/trace/ccm/sdl/SDL*
ativelog cm/trace/ccm/calllogs/calllogs*
ativelog cm/trace/ccm/sdi/ccm* (CUCM 7.x e mais recente)

Se precisar fazer o download de outro tipo de arquivo, você pode encontrar uma lista útil de locais de arquivos em: Locais de rastreamento RTMT do Communications Manager na CLI https://supportforums.cisco.com/document/65651/communications-manager-rtmt-trace-locations-cli

Exemplo

detalhe de lista de arquivos ativelog cm/trace/ccm/sdl/SDL*



Isso mostra a data, a hora, o tamanho e o nome do arquivo. Você pode fazer o download somente dos arquivos necessários com base nessas informações ou pode coletar todos os arquivos da pasta.

Etapa 3. Baixe os arquivos com o comando **file get**

arquivo get { **ativelog | inativelog | install** } *file-spec* [*reltime* | *abstime*] [**match** *regex*] [**recurs**] [**compress**]

Exemplo

arquivo get ativelog cm/trace/ccm/calllogs/calllogs*

Este comando baixa todos os arquivos na pasta, o sistema solicita os detalhes do servidor SFTP, lembre-se de que, para usar a raiz SFTP em servidores SFTP baseados em Windows, você usa a barra invertida (\) e, para servidores SFTP baseados em Linux, você usa a barra de encaminhamento (/) veja abaixo:

```
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:
```

Se você obtiver arquivos .gzo que sejam arquivos abertos no momento do download, provavelmente não poderá abri-los, mas o resto dos arquivos deverá ser .gz que você pode extrair com 7-zip (http://www.7-zip.org/) caso queira abrir os arquivos.

```
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
```

Se precisar abrir os arquivos gzo, você poderá usar a **exibição de arquivo de** comando CLI e usar todo o caminho e incluir o nome do arquivo. Nesse caso, você precisará copiar a saída e colá-la em um editor de texto que suporte o fim de linhas Unix, como o Bloco de Notas++

```
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
```

Você também pode usar qualquer caixa do linux para obter o conteúdo. Nesse caso, use o 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|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
```

Etapa 3. Depois de ter todos os arquivos necessários, crie um arquivo zip e adicione todas as pastas que contêm os arquivos que você acabou de fazer o download e, em seguida, carregue-os para seu caso TAC através da ferramenta de upload de arquivo de caso:
https://cway.cisco.com/csc

Etapa 4. Notifique o engenheiro do TAC com o qual você trabalha que carregou os arquivos.

> **Tip**: Lembre-se de adicionar os IPs, MACs e nomes de host dos dispositivos envolvidos, a data e a hora do teste/evento, os números de origem e de destino (se aplicável) e uma descrição detalhada do que aconteceu. Se o engenheiro do TAC não souber o que deve procurar, pode ser mais difícil encontrá-lo e pode levar muito mais tempo para encontrá-lo, então inclua essas informações