CUCM从混合模式更改的团星到不安全的模式配置示例

目录

[简介](#)
[先决条件](#)
[要求](#)
[使用的组件](#)
[背景信息](#)
[配置](#)
[更改从混合模式的CUCM团星安全到与CTL客户端的不安全的模式](#)
[更改从混合模式的CUCM团星安全到与CLI的不安全的模式](#)
[验证](#)
[CUCM团星设置为安全模式- CTL文件校验和](#)
[CUCM团星设置为不安全的模式- CTL文件目录](#)
[当USB令牌丢失时，请放置从混合模式的CUCM团星安全到不安全的模式](#)
[故障排除](#)

简介

本文描述要求的步骤为了更改从混合模式的Cisco Unified Communications Manager (CUCM)安全模式到不安全的模式。它也显示证书信任列表(CTL)文件的内容如何更改，当此移动完成时。

有更改CUCM安全模式的三大部分：

1a. 运行CTL客户端并且选择安全模式希望的变量。
1b. 输入CLI命令为了选择安全模式希望的变量。
2. 重新启动在运行这些服务的所有CUCM服务器的Cisco CallManager和Cisco Tftp服务。
3. 重新启动所有IP电话，以便他们能下载CTL文件的更新版本。

> **注意**：如果集群安全模式从混合模式更改到不安全的模式CTL文件仍然存在服务器和在电话，但是CTL文件不包含任何CCM+TFTP (服务器)证书。因为CCM+TFTP (服务器)证书在CTL文件不存在，这强制电话注册如不安全与CUCM。

先决条件

要求

Cisco建议您有CUCM版本10.0(1)或以上知识。另外，请保证那：

- CTL供应商服务启用并且运作在集群的所有活动TFTP服务器。默认情况下服务在TCP端口2444运作，但是这可以在CUCM服务参数配置里被修改。
- 认证机关代理功能(CAPF)服务启用并且运作在发行商节点。
- 在集群的数据库(DB)复制在实时正确地运作和服务器复制数据。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- CUCM两节点版本10.0.1.11900-2集群
- 思科7975 IP电话(注册与内部呼叫控制协议(SCCP)，固件版本SCCP75.9-3-1SR3-1S)
- 两个Cisco安全令牌是必要为了设置集群到混合模式
- 以前列出的一个安全令牌是必要为了设置集群为不安全的模式

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

为了运行插件CTL的客户端它要求访问插入为了创建或更新最新的CTL文件存在于CUCM发布服务器的至少一安全标记。换句话说，在CUCM的当前CTL文件存在的其中至少一eToken证书必须在用于更改安全模式的安全标记。

配置

更改从混合模式的CUCM团星安全到与CTL客户端的不安全的模式

完成这些步骤为了更改从混合模式的CUCM集群安全到与CTL客户端的不安全的模式：

1. 获取您插入配置最新的CTL文件的一安全标记。
2. 运行CTL客户端。提供CUCM客栈和CCM管理员凭证的Ip hostname /address。单击 **Next**。
3. 单击**集合Cisco Unified CallManager集群到不安全的Mode单选按钮**。单击 **Next**。
4. 插入插入配置最新的CTL文件和点击OK键的一安全标记。这是用于填充在CTLFile.tlv的证书列表的一个令牌。
5. 安全令牌的详细信息显示。单击 **Next**。
6. CTL文件的内容显示。单击 **完成**。系统提示输入口令时，输入 cisco123。
7. 的CUCM服务器列表CTL文件存在显示。点击**完成**。
8. 选择**CUCM管理员页面>System >企业参数**并且验证集群设置为不安全的模式("0"指示不安全)。
9. 重新启动TFTP和Cisco CallManager服务在管理这些服务的所有节点在集群。
10. 重新启动所有IP电话，以便他们能从CUCM TFTP得到CTL文件的新版本。

更改从混合模式的CUCM团星安全到与CLI的不安全的模式

此配置仅是为CUCM版本10.X和以后。为了设置CUCM集群安全模式到不安全，请输入**使用情况ctl设置团星非安全模式**on命令发行商CLI。在这完成后，请重新启动TFTP和Cisco CallManager服务在管理这些服务的所有节点在集群。

这是输出的示例CLI显示使用命令。

```
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n):

Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that
run these services
admin:
```

验证

使用本部分可确认配置能否正常运行。

为了验证CTLFIle.tlv，您能使用两个方法之一：

- 为了验证CTLFIle.tlv的内容和MD5校验和在CUCM TFTP侧，请输入showctl **on命令**CUCM CLI。CTLFIle.tlv文件应该是相同的在所有CUCM节点。
- 为了验证在7975个IP电话的MD5校验和，请选择**设置> Security Configuration>托拉斯列表> CTL文件**。

  注意：当您检查在您将看到MD5或SHA1的电话的校验和，从属在电话类型。

CUCM团星设置为安全模式- CTL文件校验和

```
admin:show ctl
The checksum value of the CTL file:
98784f6f6bcd5019ea165b1d2bc1372e(MD5)
9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1)
[...]
```

在IP电话侧，您能看到安排同一个CTL文件安装(MD5校验和配比，当与从CUCM的输出比较)。

CUCM团星设置为不安全的模式- CTL文件目录

这是CTL文件的示例从CUCM集群的设置为不安全的模式。您能看到CCM+TFTP证书是空的，并且不包含任何内容。当CUCM设置对混合模式，证书的其余在CTL文件的没有正确地更改并且是相同的象。

```
admin:show ctl
The checksum value of the CTL file:
7879e087513d0d6dfe7684388f86ee96(MD5)
be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1)


Length of CTL file: 3746
```

The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015

Parse CTL File

Version: 1.2
HeaderLength: 304 (BYTES)

BYTEPOS TAG LENGTH VALUE
--- --- --- ---
3 SIGNERID 2 117
4 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
6 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
45 ec 5 c 9e 68 6d e6
5d 4b d3 91 c2 26 cf c1
ee 8c b9 6 95 46 67 9e
19 aa b1 e9 65 af b4 67
36 7e e5 ee 60 10 b 1b
58 c1 6 64 40 cf e2 57
aa 86 73 14 ec 11 b a
3b 98 91 e2 e4 6e 4 50
ba ac 3e 53 33 1 3e a6
b7 30 0 18 ae 68 3 39
d1 41 d6 e3 af 97 55 e0
5b 90 f6 a5 79 3e 23 97
fb b8 b4 ad a8 b8 29 7c
1b 4f 61 6a 67 4d 56 d2
5f 7f 32 66 5c b2 d7 55
d9 ab 7a ba 6d b2 20 6
14 FILENAME 12
15 TIMESTAMP 4

CTL Record #:1

BYTEPOS TAG LENGTH VALUE
--- --- --- ---
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
7 PUBLICKEY 140
9 CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2 CC 6D 93 90 (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.

CTL Record #:2

BYTEPOS TAG LENGTH VALUE
--- --- --- ---
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31

```
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93 3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was not used to sign the CTL file.

CTL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.153
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

CTL Record #:4
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1004
2 DNSNAME 13 10.48.47.153
3 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
6 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
10 IPADDRESS 4

CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.154
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

在IP电话侧，在重新启动并且下载更新CTL文件版本后，您能看到MD5校验和配比，当与从CUCM的输出比较。

当USB令牌丢失时，请放置从混合模式的CUCM团星安全到不安全的模式

被巩固的集群的安全令牌能丢失。在该情况下，您需要考虑这两个方案：

- 集群运行版本10.0.1或以上
- 集群早于10.x运行版本

在第一个方案中，请完成在崔凡吉莱描述的步骤从混合模式的CUCM团星安全到不安全的模式以CLI部分为了从问题恢复。因为该CLI命令不要求CTL标记，可能使用，即使集群在混合模式放置与CTL客户端。

当版本早于CUCM 10.x是在使用中的时，情况变得更加复杂。如果丢失或忘记密码一个令牌，您能仍然使用人一个运行CTL客户端以当前CTL文件。它是高度推荐的获取另一eToken和尽快添加它到CTL文件为冗余。如果丢失或忘记在您的CTL文件列出的所有eTokens的密码，您需要获得一个新

的对eTokens和运行手工的步骤如解释此处。

1. 输入**文件删除tftp CTLFile.tlv命令**为了删除从所有TFTP服务器的CTL文件。`admin:file delete tftp CTLFile.tlv`
   ```
   Delete the File CTLFile.tlv?
   Enter "y" followed by return to continue: y
   files: found = 1, deleted = 1

   admin:show ctl
   Length of CTL file: 0
   CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl..
   to generate the CTL file.
   Error parsing the CTL File.
   ```
2. 运行CTL客户端。进入CUCM客栈和CCM管理员凭证的Ip hostname /address。单击 **Next**。
3. 因为集群在混合模式，然而CTL文件在发行商不存在，此警告显示。点击OK键为了忽略它和继续转发。
4. 点击**更新CTL File单选按钮**。单击 **Next**。
5. CTL客户端请求添加安全标记。单击**添加**为了继续。
6. 屏幕显示在新的CTL的所有条目。单击**添加令牌**为了从新的对添加第二标记。
7. 将提示您去除当前标记和插入新的。点击OK键一次完成的。
8. 显示新的标记的详细信息的屏幕显示。单击**添加**为了确认他们和添加此标记。
9. 您将提交与的CTL条目新的列表显示两个已添加令牌。点击**芬通社**为了生成新建的CTL文件。
10. 在令牌的密码字段，请输入**Cisco123**。单击 **Ok**。
11. 您将看到确认进程是成功的。单击**完成**为了确认和退出CTL客户端。
12. 重新启动CallManager服务跟随的Cisco Tftp (Cisco Unified维护性> Tools > Control Center - 功能服务)。应该生成新的CTL文件。输入验证的**显示ctl**命令。`admin:show ctl`
    ```
    The checksum value of the CTL file:
    68a954fba070bbcc3ff036e18716e351(MD5)
    4f7a02b60bb5083baac46110f0c61eac2dceb0f7(SHA1)


    Length of CTL file: 5728
    The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015
    ```
13. 删除从每个电话的CTL文件在集群(此步骤可能变化基于电话类型-请参考文档关于详细信息，例如思科统一IP电话8961， 9951和9971管理指南)。**注意**：电话也许仍然能注册(从属在安全设置于电话)和工作，无需继续进行步骤13。然而，他们把旧有CTL文件安装。它可能导致问题，如果证书被重新生成，另一个服务器被添加到集群或服务器硬件被更换。没有推荐离开在此状态的集群。
14. 移动集群向不安全。请参阅崔凡吉莱从混合模式的CUCM团星安全到与CTL客户端部分的不安全的模式关于详细信息。

故障排除

目前没有针对此配置的故障排除信息。