

演示IP電話從安全到非安全CUCM的遷移

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[設定](#)

[網路圖表](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹將電話從安全的思科統一通訊管理器(CUCM)遷移到非安全CUCM的最佳實踐之一。

必要條件

需求

思科建議您瞭解以下主題：

- CUCM
- IP電話

採用元件

本檔案中的資訊是根據以下軟體版本：

- CUCM版本- 12.5.1.16065-1和12.5.1.14900-63
- IP電話型號- 8865和版本- 12.8(1)

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表

IP_Phone > Cisco Switch > Cisco Router > Cisco Switch > CUCM Cluster

組態

這些場景說明了電話從安全CUCM集群遷移到非安全CUCM集群。在每個階段中，記錄電話上的證書信任清單(CTL)和身份信任清單(ITL)檔案的狀態。

1. 向非安全CUCM集群註冊電話。
2. 將非安全群集轉換為安全CUCM群集。
3. 從安全轉換回非安全叢集
4. 將電話遷移到新的非安全CUCM集群。

1. 將電話註冊到非安全CUCM集群。

以下是有關非安全來源叢集的資訊。

- IP地址- 10.201.251.171
- FQDN - cucm1052.domain.com
- 版本：12.5.1.16065-1

向非安全CUCM集群註冊電話。為此，請配置動態主機配置協定(DHCP)選項150 / 66以指向簡單檔案傳輸協定(TFTP) IP地址 (這將是TFTP服務打開的CUCM節點) 。

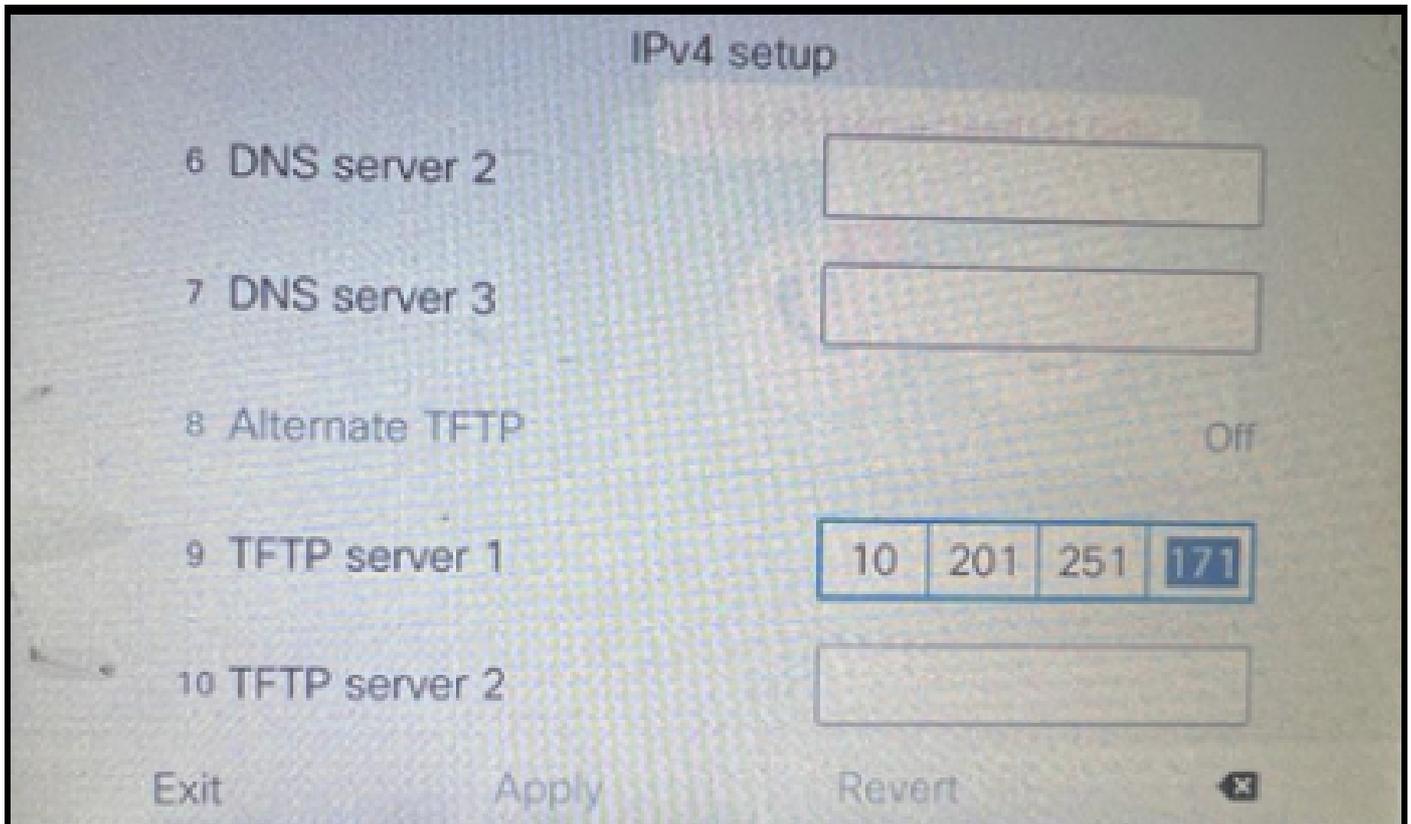
對於沒有DHCP伺服器的基礎設施，您必須在物理電話上手動配置TFTP IP。

在物理電話上，導航到設定>管理設定>網路設定>乙太網設定> IPv4設定。

關閉DHCP並提供網路的靜態IP詳細資訊。之後，在TFTP伺服器1部分中提供非安全CUCM IP，如螢幕截圖所示。

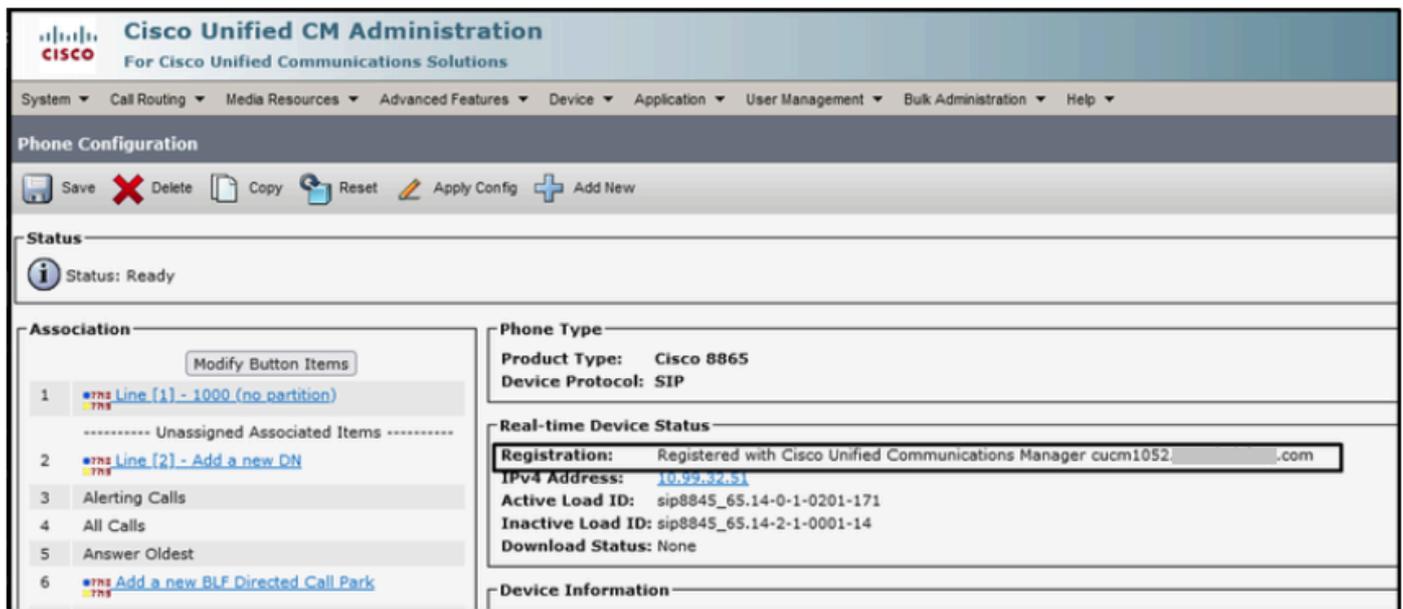


注意：此過程相當於更改DHCP作用域上的TFTP IP (選項150/66)。如果叢集已設定網域名稱，則您也必須在DHCP領域設定適當的網域名稱系統(DNS)伺服器。



在電話上配置TFTP IP

IP電話成功註冊到上述非安全CUCM集群。



在CUCM上註冊的電話

登入CUCM管理Web介面並導航至系統>企業引數。

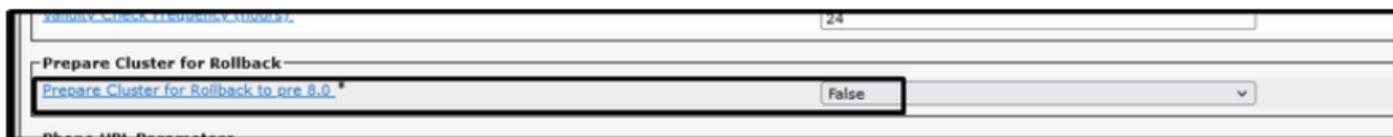
以下是在非安全CUCM集群的Enterprise parameter頁中設定的引數值。

- Cluster Security Mode設定為0，這確認集群不安全。



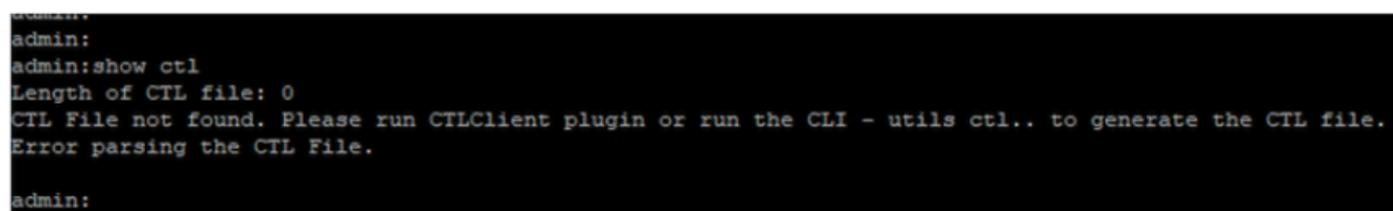
集群安全模式設定為0

- 「準備叢集以便倒回至8.0之前的版本」設為False。因此，ITL和CTL檔案的內容會以適當的值保留。



Prepare Cluster for Rollback to pre 8.0設定為False

由於叢集不安全，因此TFTP伺服器中沒有CTL檔案。要驗證這一點，可以在CUCM節點的安全殼(SSH)會話上運行命令show ctl。



CTL檔案不存在

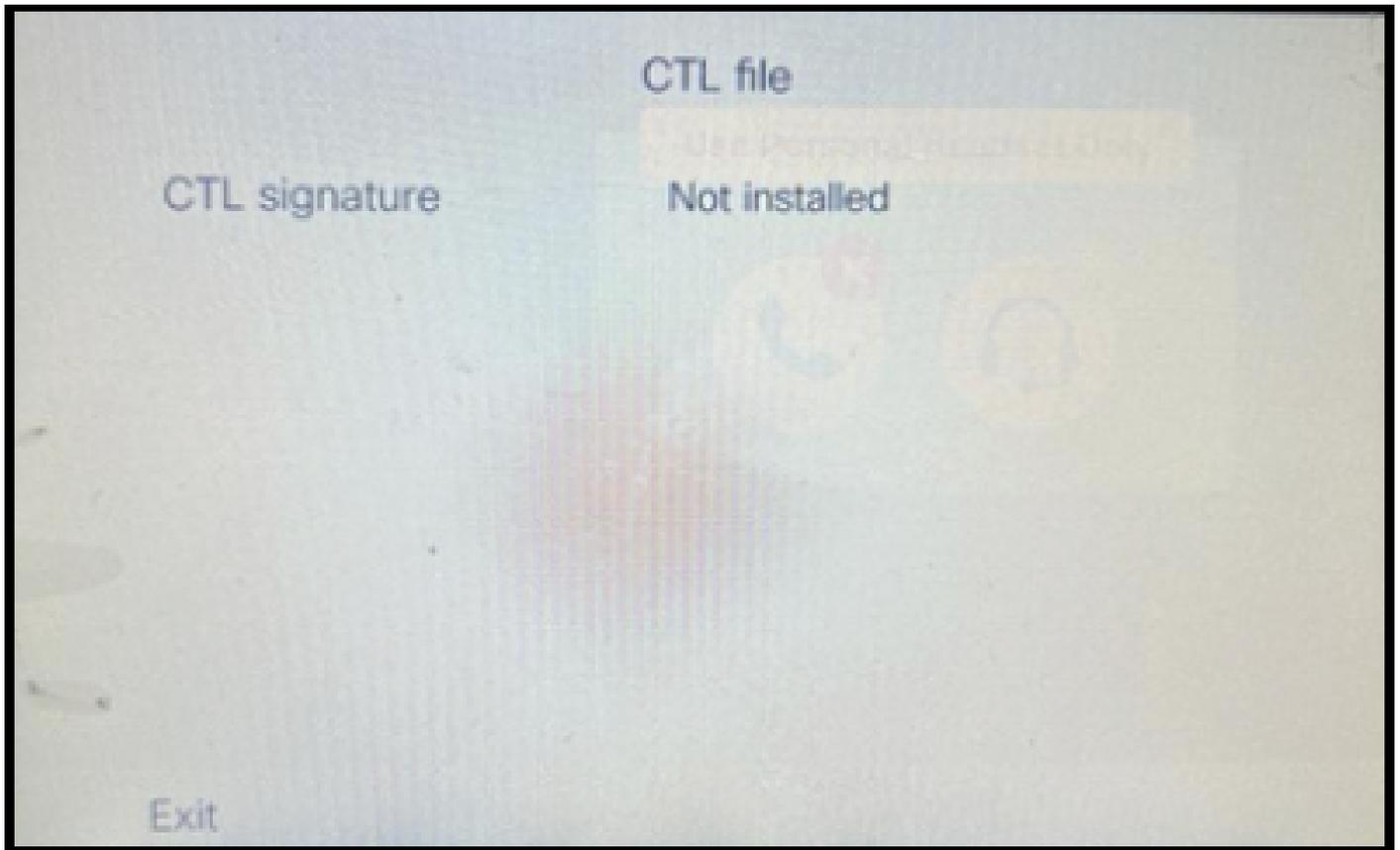
在物理電話上，您可以確認未安裝CTL檔案。但是，您確實會看到國際交易日誌檔案。

由於CUCM中的預設安全(SBD)功能，存在ITL。有關SBD的更多資訊，請點選[這裡](#)。

在物理電話上，導航到設定>管理設定>安全設定>信任清單。

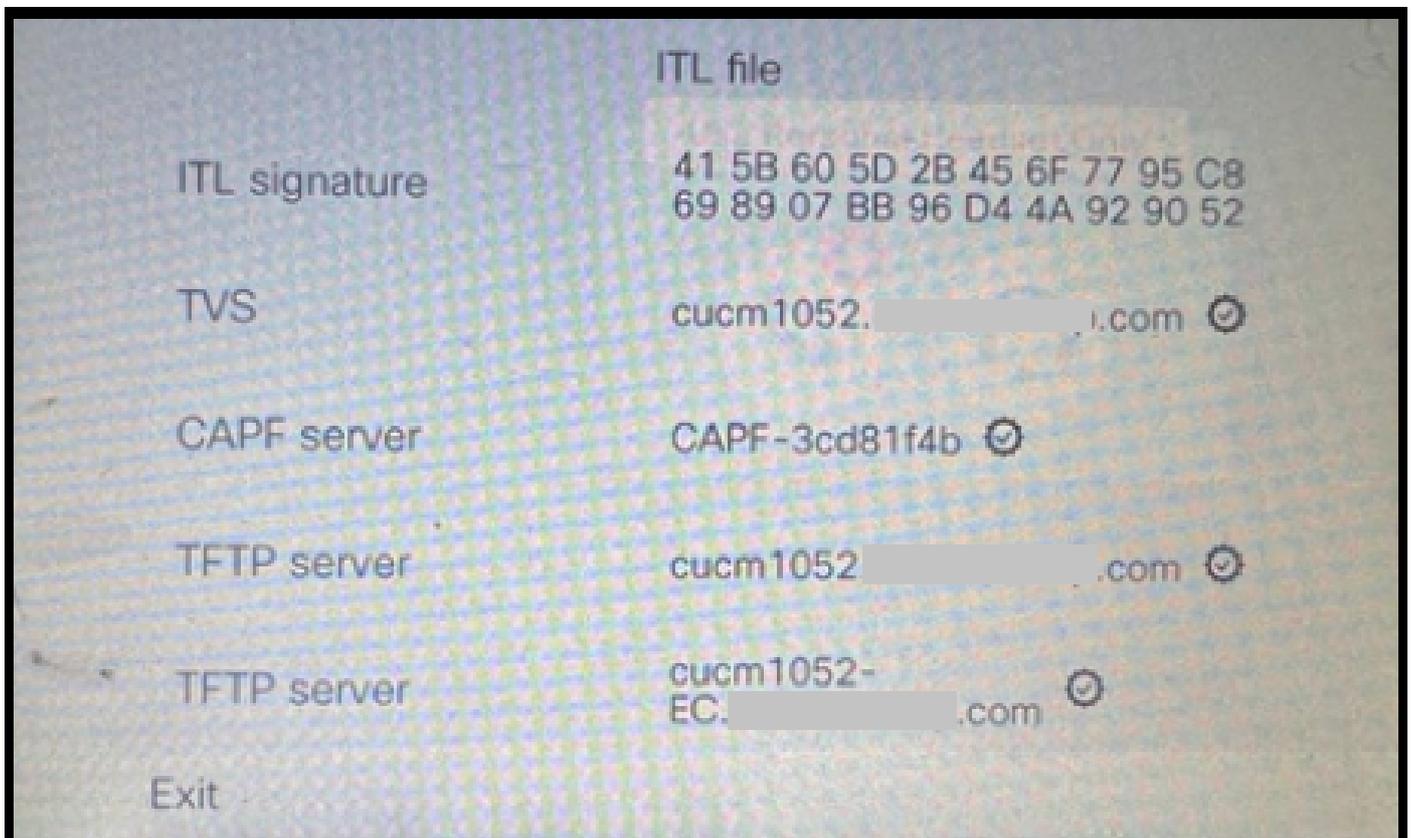
您可以在此處找到CTL和ITL檔案的狀態。

電話上未安裝CTI。



電話上的CTL檔案

電話有國際交易日誌檔案。



電話上的ITL檔案

2. 將非安全集群轉換為安全CUCM集群。

透過在CUCM發佈伺服器的命令列介面(CLI)上運行utils ctl set-cluster mixed-mode命令來啟用混合模式。這會將叢集從非安全轉換為安全。

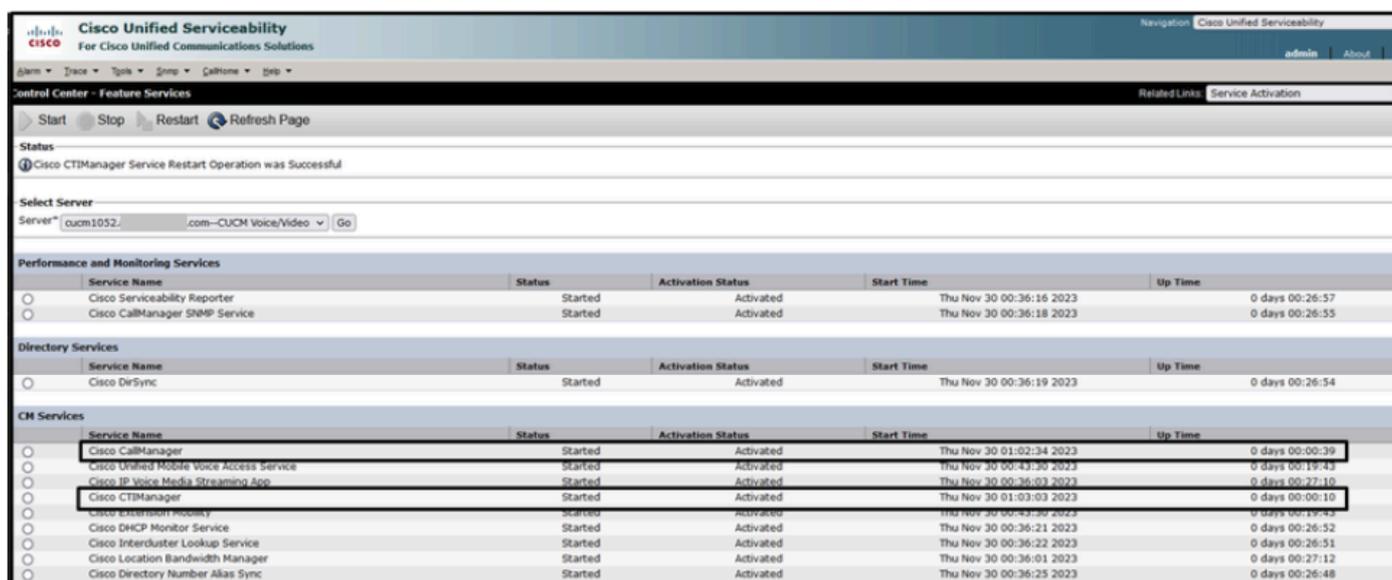
```
admin:
admin:
admin:utils ctl set-cluster mixed-mode
This operation will set the cluster to Mixed mode. Auto-registration is enabled on at least one CM node. Do you want to continue? (y/n): y

Moving Cluster to Mixed Mode
Cluster set to Mixed Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

轉換成安全叢集

運行該命令後，重新啟動集群中所有節點上的Cisco CallManager (CCM)和Cisco CTI管理器服務。



The screenshot shows the Cisco Unified Serviceability Control Center interface. The status indicates that the Cisco CTIManager Service Restart Operation was successful. The 'Performance and Monitoring Services' table shows the following services:

Service Name	Status	Activation Status	Start Time	Up Time
Cisco Serviceability Reporter	Started	Activated	Thu Nov 30 00:36:16 2023	0 days 00:26:57
Cisco CallManager SNMP Service	Started	Activated	Thu Nov 30 00:36:18 2023	0 days 00:26:55

The 'Directory Services' table shows:

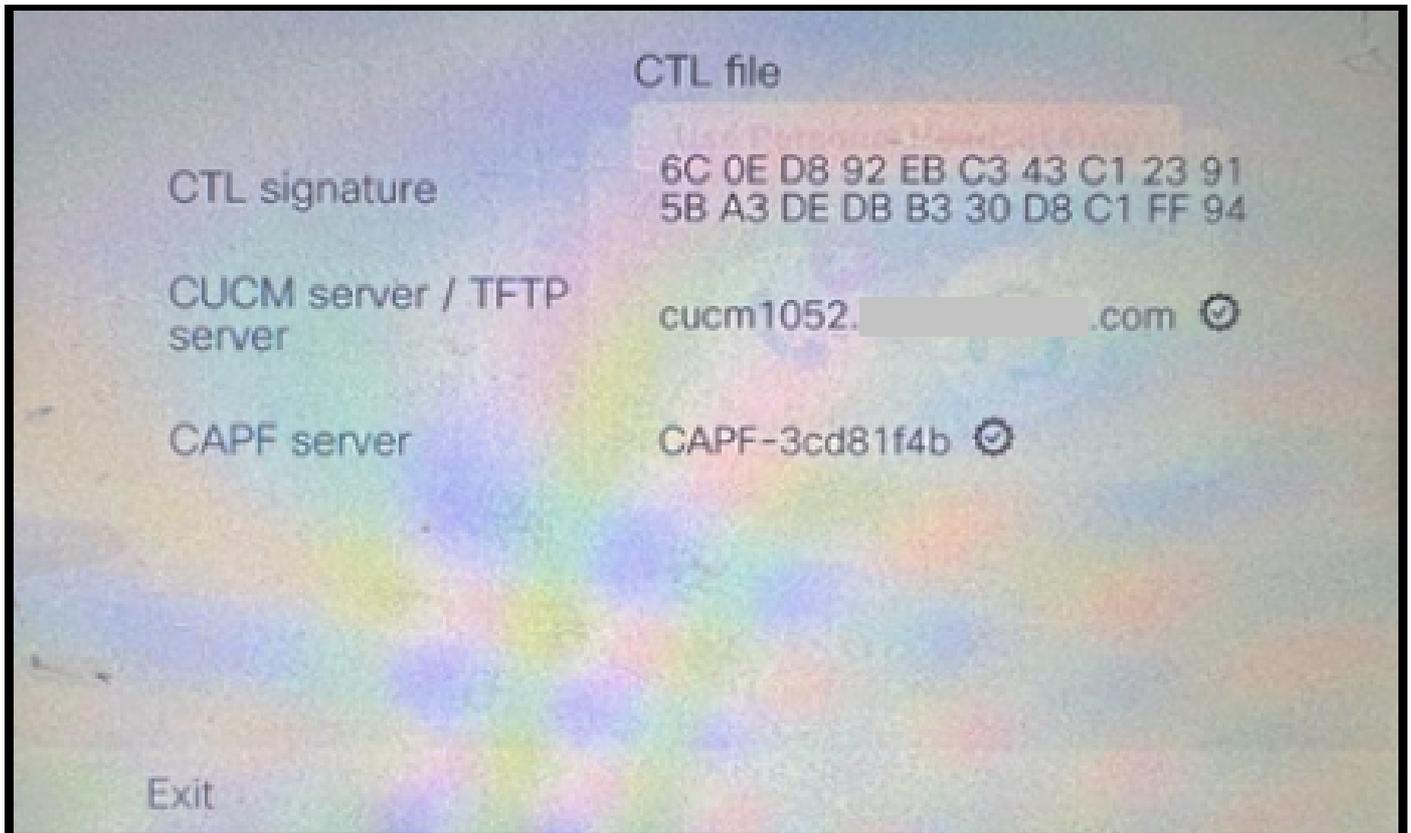
Service Name	Status	Activation Status	Start Time	Up Time
Cisco DirSync	Started	Activated	Thu Nov 30 00:36:19 2023	0 days 00:26:54

The 'CM Services' table shows the following services, with 'Cisco CallManager' and 'Cisco CTIManager' highlighted:

Service Name	Status	Activation Status	Start Time	Up Time
Cisco CallManager	Started	Activated	Thu Nov 30 01:02:34 2023	0 days 00:00:39
Cisco Unified Mobile Voice Access Service	Started	Activated	Thu Nov 30 00:43:30 2023	0 days 00:19:43
Cisco IP Voice Media Streaming App	Started	Activated	Thu Nov 30 00:36:03 2023	0 days 00:27:10
Cisco CTIManager	Started	Activated	Thu Nov 30 01:03:03 2023	0 days 00:00:10
Cisco CTIManager Proxy	Started	Activated	Thu Nov 30 00:43:30 2023	0 days 00:19:43
Cisco DNCP Monitor Service	Started	Activated	Thu Nov 30 00:36:21 2023	0 days 00:26:52
Cisco Intercluster Lookup Service	Started	Activated	Thu Nov 30 00:36:22 2023	0 days 00:26:51
Cisco Location Bandwidth Manager	Started	Activated	Thu Nov 30 00:36:01 2023	0 days 00:27:12
Cisco Directory Number Alias Sync	Started	Activated	Thu Nov 30 00:36:25 2023	0 days 00:26:48

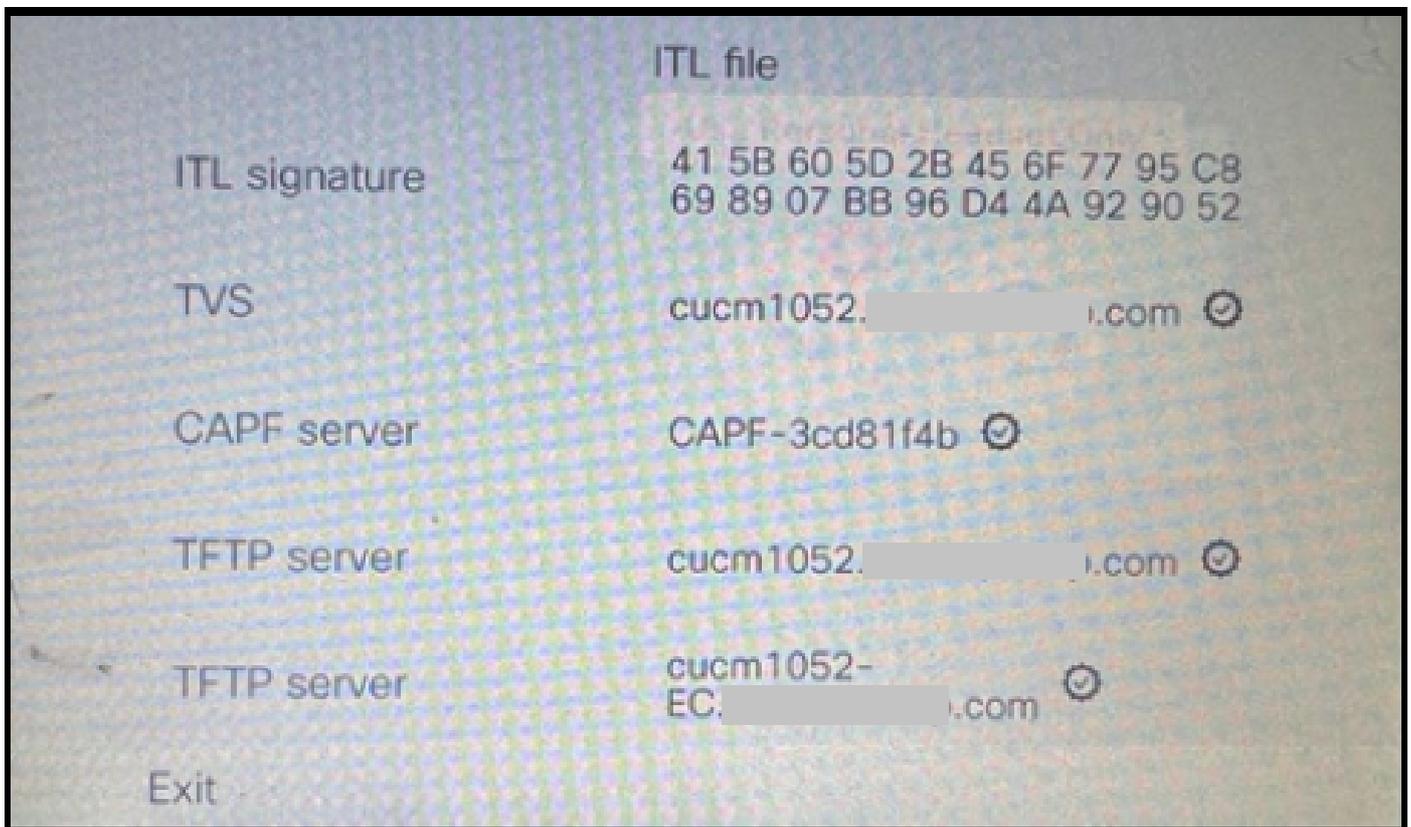
重新啟動CCM和CTI服務

在物理電話上，您可以看到CTL檔案的存在。



電話上的CTL檔案

ITL檔案保持相同的值。



電話上的ITL檔案

3. 從secure轉換回非安全叢集。

為了將集群從安全模式轉換到非安全模式，您需要在CUCM發佈伺服器的CLI上運行utils ctl set-cluster non-secure-mode命令。

```
admin:
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): y

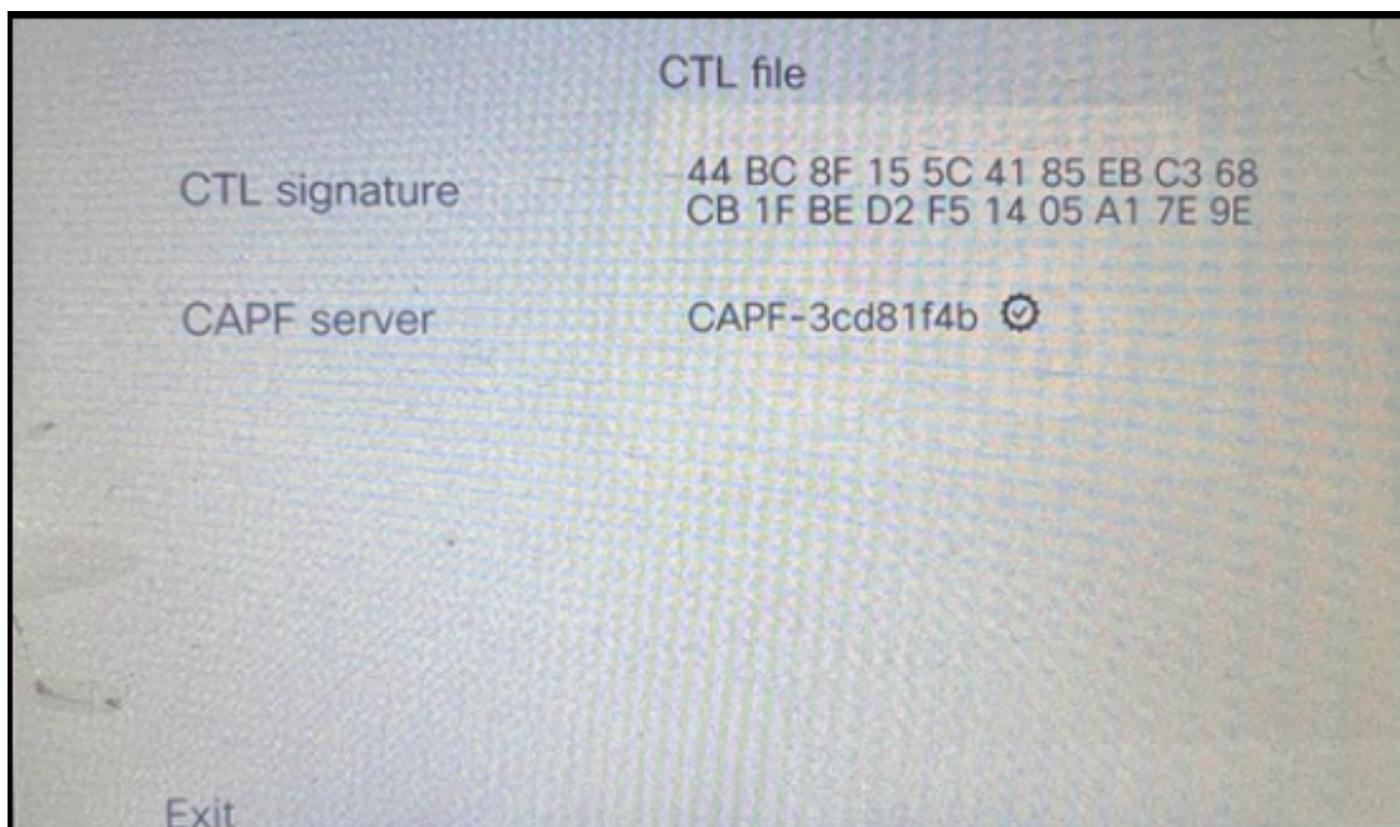
Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please restart Cisco CallManager service and Cisco CTIManager services on all the nodes in the cluster that run these services.

admin:
admin:
```

轉換成非安全叢集

重新啟動集群中所有節點上的CCM和CTI服務，以便進行更改以反映CUCM集群中的所有節點。

將集群轉換為非安全後，CTL不包含CUCM和TFTP條目。CTL檔案只包含CAPF專案。



電話上的CTL檔案

ITL檔案保留相同的條目。

ITL file

ITL signature

41 5B 60 5D 2B 45 6F 77 95 C8
69 89 07 BB 96 D4 4A 92 90 52

TVS

cucm1052-
EC.
.com ☑

CAPF server

CAPF-3cd81f4b ☑

TFTP server

cucm1052-
EC.
.com ☑

TFTP server

cucm1052-
EC.
.com ☑

Exit

電話上的ITL檔案



註：將電話配置頁面（CUCM管理網頁）中的裝置安全配置檔案更改為安全或非安全對ITL或CTL檔案沒有影響。因此，您可以保持以前的設定，無需更改設定。

4. 將電話遷移到新的非安全CUCM集群。

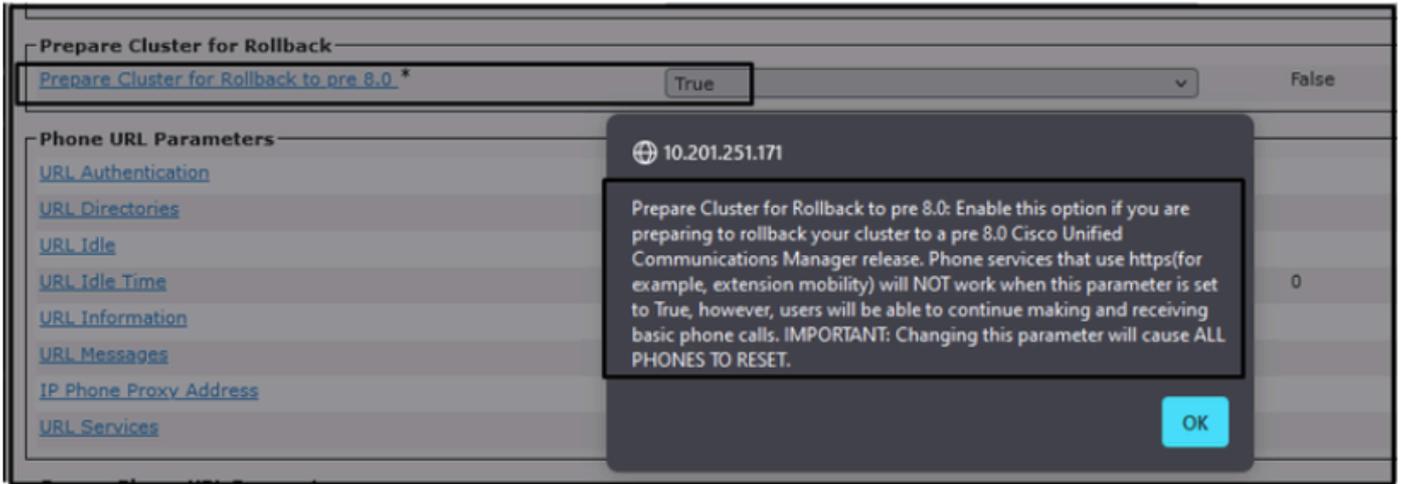


注意：繼續遷移之前，最好在源群集中的所有節點（僅在這些啟用了服務的節點上）上重新啟動信任驗證服務(TVS)和TFTP服務。如此可消除TVS / TFTP服務中的任何掛起或洩漏會話。

登入CUCM管理Web介面並導航至系統>企業引數。

將Prepare Cluster for Rollback的值設定為Pre 8.0到True。然後，繼續按一下Apply Config和Reset按鈕。

此螢幕截圖提供了此引數的幫助部分。

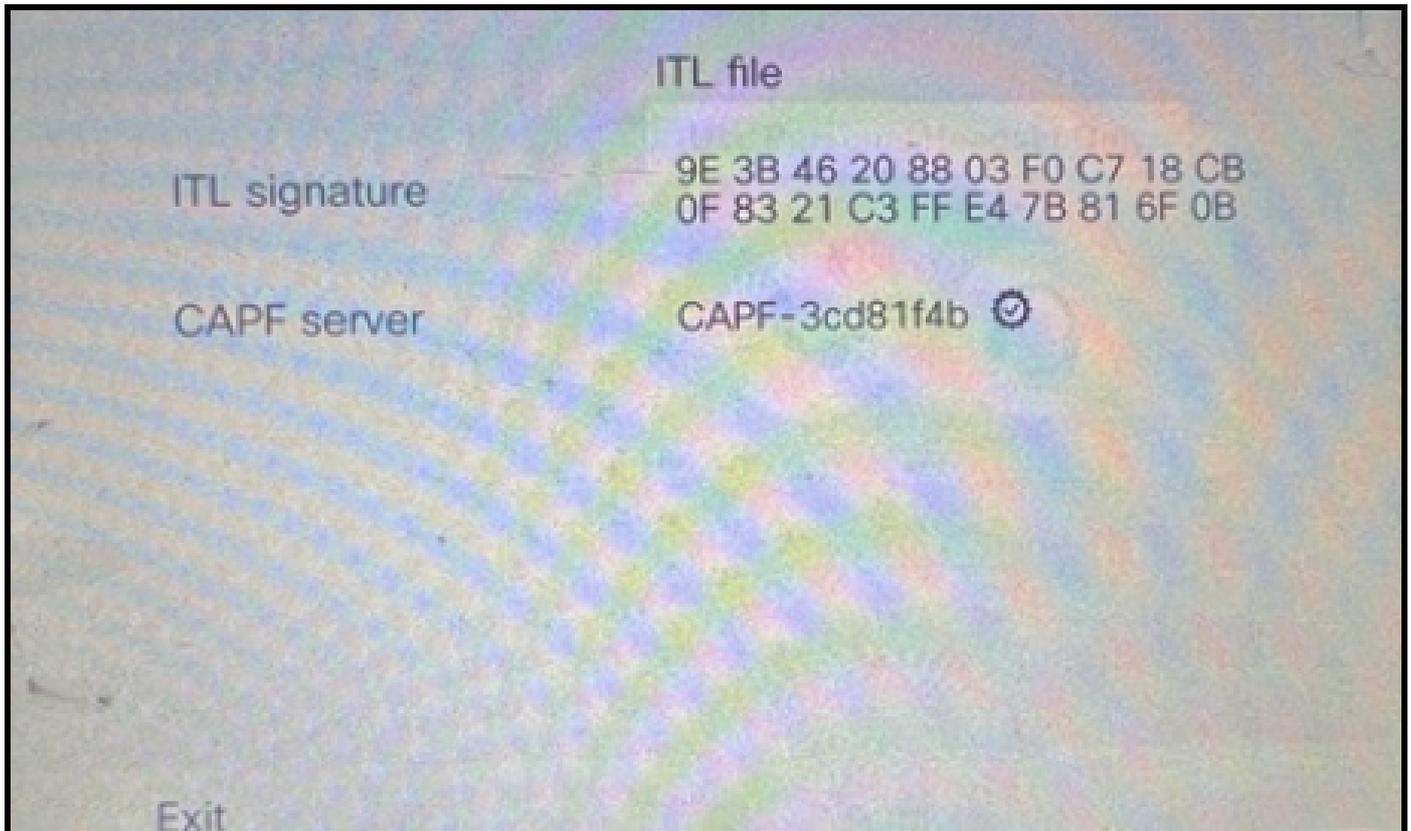


有關準備集群以便回滾到8.0之前的引數的資訊

在更改引數值前後對集群上的電話註冊計數(透過即時監控工具- RTMT)進行監控。這樣可以驗證這些變更是否套用至叢集中的所有裝置。

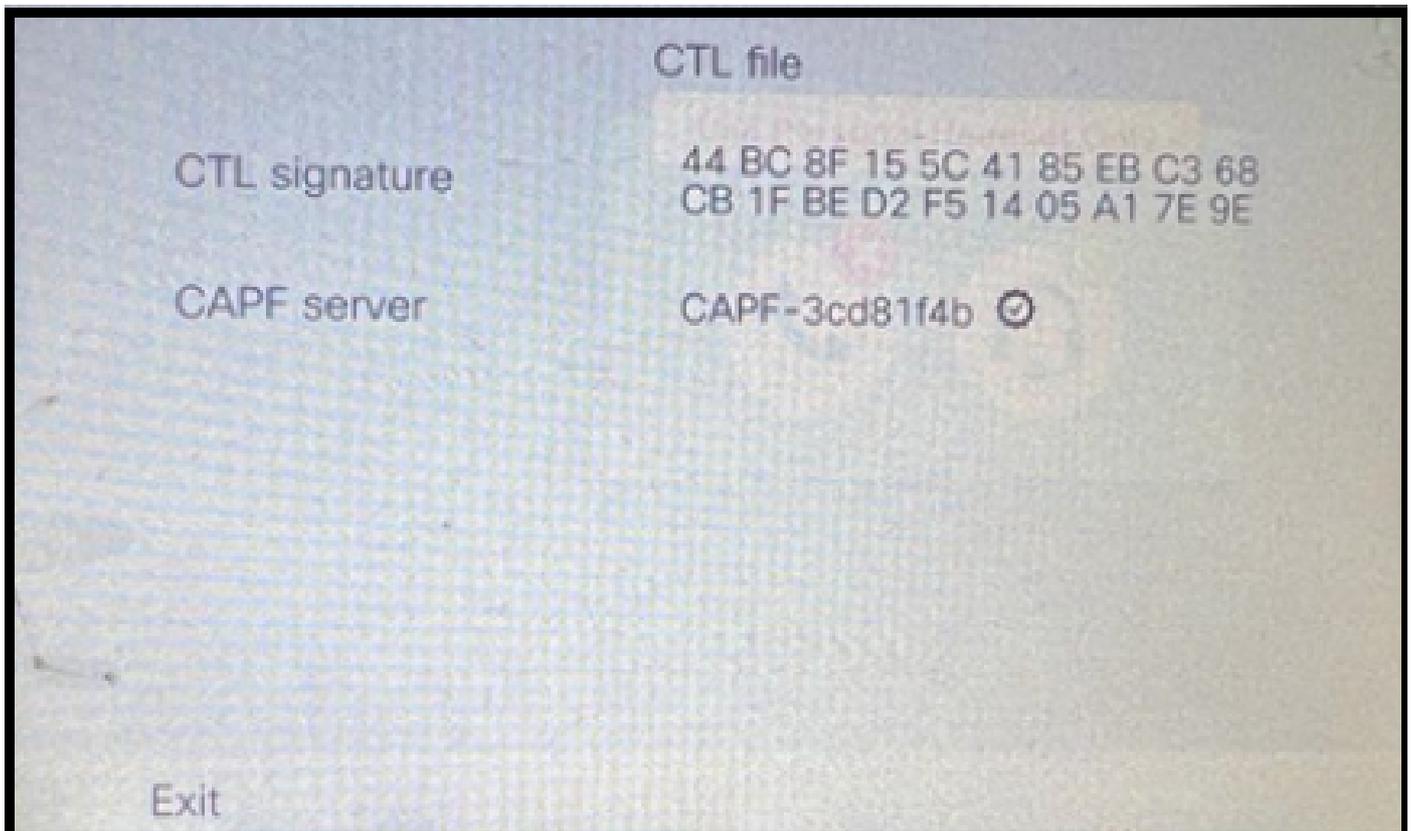
在物理電話上，您只能在ITL和CTL檔案中看到CAPF條目。您也可以透過在Web瀏覽器中打開電話網頁來觀察這一點。

ITL檔案



電話上的ITL檔案

CTL檔案



電話上的CTL檔案

在開始遷移之前，最好在少數電話上驗證ITL和CTL檔案，以確保已發生更改。

現在，電話已準備好進行遷移。

將電話從源群集遷移到目標群集。目前，這兩個群集都不安全。

來源叢集：

- IP地址- 10.201.251.171
- FQDN - cucm1052.domain.com
- 版本：12.5.1.16065-1

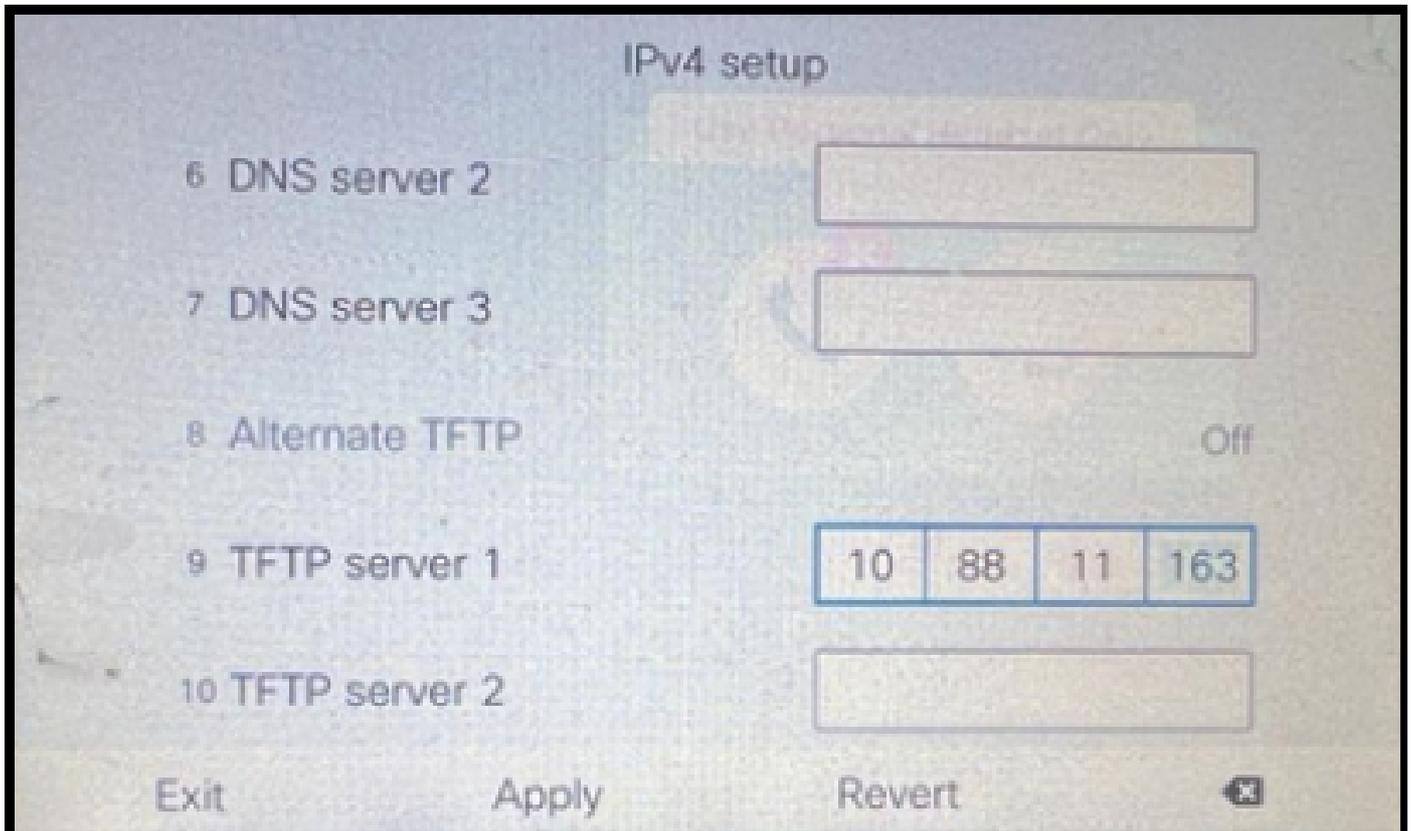
目的地叢集：

- IP地址- 10.88.11.163
- FQDN - cucmpub.domain.com
- 版本：12.5.1.14900-63

在物理電話上，將TFTP Server 1值設定為目標新集群IP地址，然後按一下Apply按鈕。

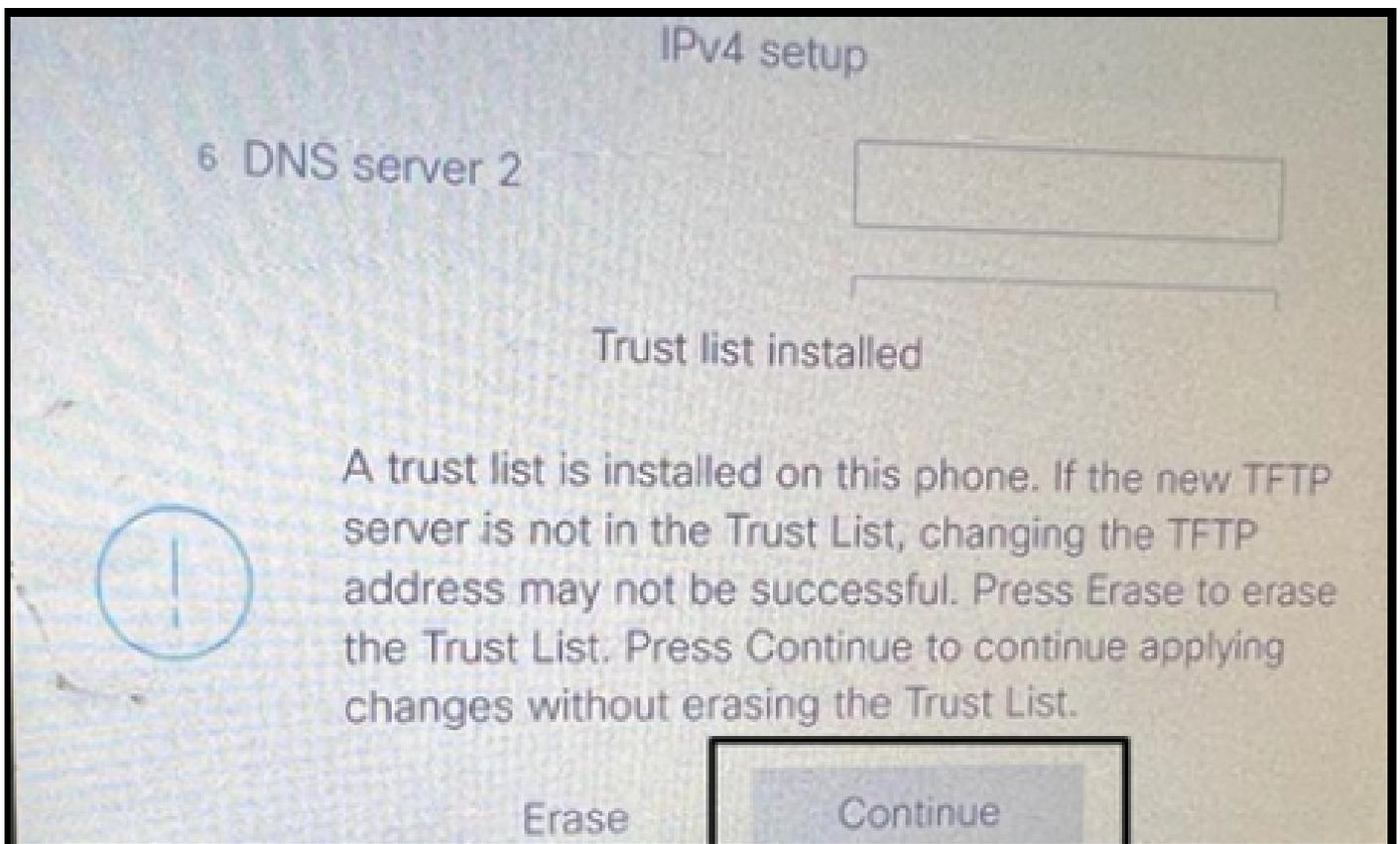


注意：此過程相當於更改DHCP作用域上的TFTP IP（選項150/66）。如果目的地叢集位於不同的網域中，則您也必須在DHCP領域設定適當的DNS伺服器。



在電話上配置TFTP IP

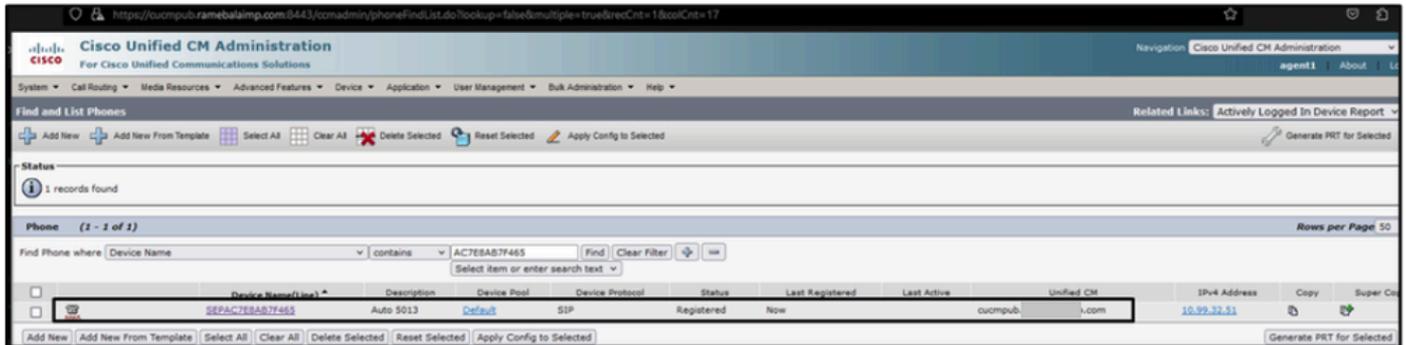
按一下Continue按鈕，這樣將保留源集群的舊CTL和ITL檔案（僅包含CAPF條目）。



按「繼續」按鈕可以保留舊的CTL和ITL檔案

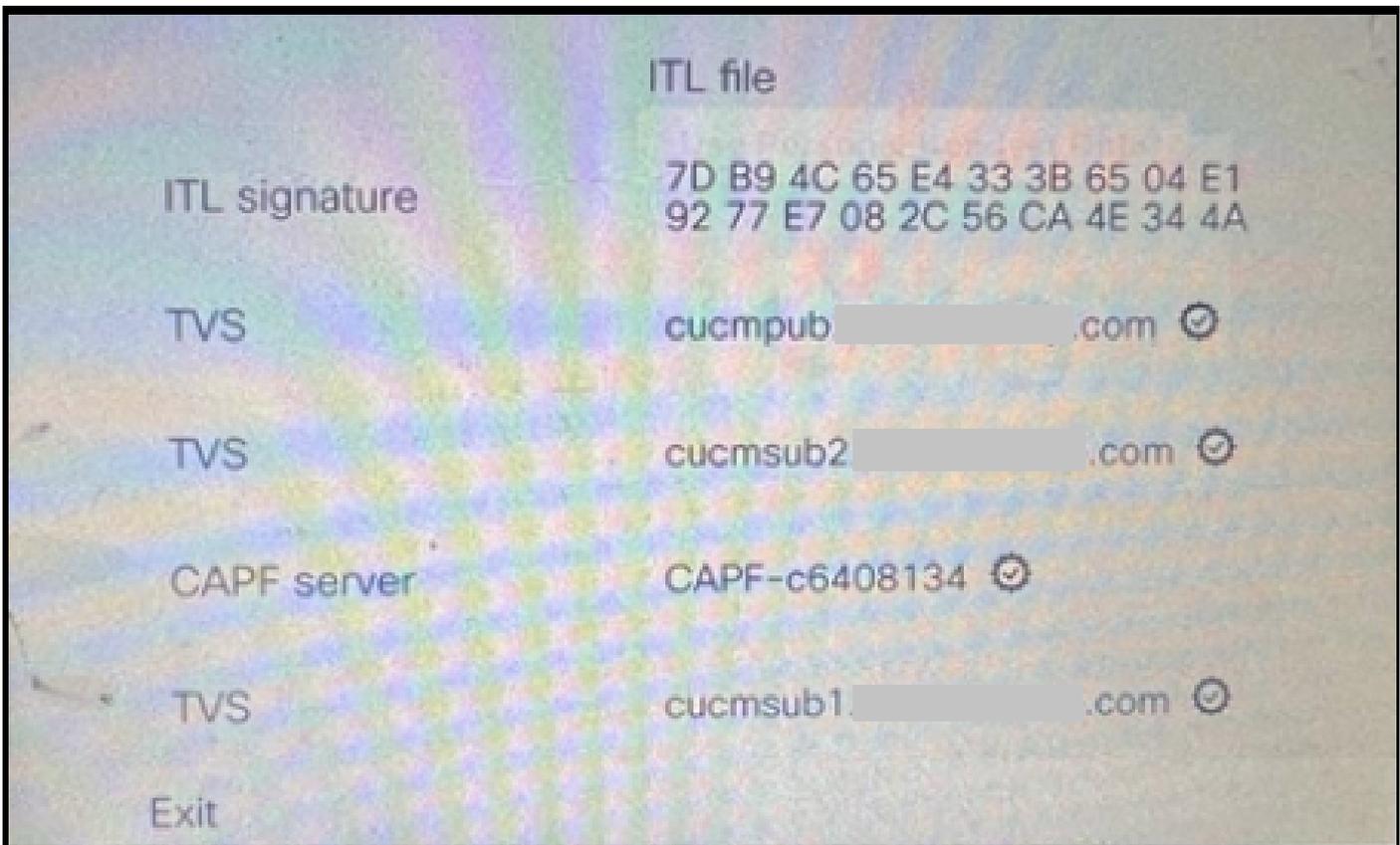
驗證

電話已成功註冊到目標群集。



在CUCM上註冊的電話

電話包含目標群集信任清單條目。



電話上的ITL檔案

疑難排解

目前尚無適用於此組態的具體疑難排解資訊。

相關資訊

- [瞭解預設情況下的CUCM安全以及ITL運行和故障排除](#)
- [帶無令牌CTL的CUCM混合模式](#)
- [Cisco Unified Communications Manager版本12.5\(1\)安全指南](#)
- [思科技術支援與下載](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。