# CUCM集群之间的批量证书管理流程,用于电话 迁移

# 目录

简介 <u>先决条件</u> <u>要求</u> 使用的组件 <u>背景信息</u> <u>批量证书管理过程</u> <u>导出目标群集证书</u> <u>导出目标群集证书</u> <u>零合源和目标PKCS12文件</u> <u>将证书导入目标和源集群</u> 使用目标集群TFTP服务器信息配置源集群电话 重置源群集电话以获取目标群集ITL/CTL文件以完成迁移过程 验证 <u>故障排除</u> 配置演练视频

# 简介

本文档提供了在Cisco Unified Communications Manager(CUCM)群集之间进行批量证书管理以进行 电话迁移的操作步骤。

作者:思科TAC工程师Adrian Esquillo。

**注意**:此步骤也在《CUCM版本<u>管理指南》的"管理批量证书"部分中概述</u>

# 先决条件

## 要求

Cisco 建议您了解以下主题: ·安全文件传输协议(SFTP)服务器 ·CUCM证书

## 使用的组件

·本文档中的信息基于CUCM 10.X。

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。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

# 背景信息

批量证书管理允许在CUCM群集之间共享一组证书。此步骤要求需要在各个群集之间建立信任的群 集的系统功能,例如跨群集分机移动(EMCC)以及群集之间的电话迁移。

在此过程中,会创建包含来自集群中所有节点的证书的公钥加密标准#12(PKCS12)文件。每个集群 必须将其证书导出到同一SFTP服务器上的同一SFTP目录。批量证书管理配置必须在源和目标群集 的CUCM发布服务器上手动完成。源和目标群集必须处于启用状态且运行正常,以便要迁移的电话 可以连接到这两个群集。源群集电话将迁移到目标群集。

# 批量证书管理过程

### 导出目标群集证书

步骤1.在目标群集的CUCM发布服务器上为批量证书管理配置SFTP服务器。

在本示例中,目标集群CUCM版本为11.5.1。

·导航**到**Cisco Unified OS Administration > Security > Bulk Certificate Management **,输入SFTP服** 务器详细信息并单击Export,如图所示。

cisco	Cisco Unified Operating System Administration For Cisco Unified Communications Solutions
Show - Set	ings - Security - Software Upgrades - Services - Help -
Bulk Certific	ate Management
Save 2	Export Export
Status Update	successful
SFTP Detai	5
IP Address*	10.24.161.145
Port*	22
User ID*	cisco
Password*	•••••
Directory*	/
Save	ixport

步骤2.将所有证书从目标群集中的所有节点导出到SFTP服务器。

·在后续弹出窗口中,为证书类**型选**择全部,然后单击**导出**,如图所示。

Cisco Unified Operating System Administration For Cisco Unified Communications Solutions	
Show - Settings - Security - Software Upgrades - Services - Help -	
Bulk Certificate Management	
Save Bxport	
Status Update successful	
SFTP Details           IP Address*           10.24.161.145           Port*           22           User ID*           cisco           Password*           •••••           Directory*	Bulk Certificate Export - Mozilla Firefox       Image: Close         Image: Bulk Certificate Export       Image: Bulk Certificate Export         Image: Bulk Certificate Export       Image: Bulk Certificate Export         Image: Bulk Certificate Export       Image: Bulk Certificate Export
Save Export (i) *- indicates required item.	Status         Status: Ready         Export Certificate Type         Certificate Type* All         Export         Close         (i) *- indicates required item.

·关闭弹出窗口并使用为目标集群中的每个节点创建的PKCS12文件进行批量证书管理更新,网页将 刷新此信息,如图所示。

cisco	Cisco Unified Operating System Administration For Cisco Unified Communications Solutions			a	Navigation Cisco Unifie
Show - Se	ttings   Security   Software Upgrades   Services   Help				
Bulk Certifi	icate Management				
Save 1	Export				
Status					
(i) Status	: Ready				
SFTP Deta	ils				
IP Address	10.24.161.145				
Port*	22				
User ID*	cisco				
Password*	•••••				
Directory*	/				
	File Name		Certificate Type		Server Source
CUCM1151P	PUB_capf.pkcs12	STORE		CUCM1151PUB	
CUCM1151P	PUB_tftp.pkcs12	STORE		CUCM1151PUB	
CUCM1151P	PUB_tomcat.pkcs12	STORE		CUCM1151PUB	
0.000					

## 导出源群集证书

步骤1.在源群集的CUCM发布服务器上为批量证书管理配置SFTP服务器。

在本例中,源集群CUCM版本为10.5.2。

·导航**到**Cisco Unified OS Administration > Security > Bulk Certificate Management **,输入SFTP服** 务器详细信息并单击Export,如图所示。

**注意:**从目标集群导出到SFTP服务器的PKCS12文件在访问时显示在源集群CUCM发布者的 批量证书管理网页上。

ultulu. Cisco Unified Operating System Administration CISCO For Cisco Unified Communications Solutions			Navigation Cisco Unified admin Search Documen
Show • Settings • Security • Software Upgrades • Services • Help •			
Bulk Certificate Management			
Save Deport			
Status: Ready			
SFTP Details			
IP Address* 10.24.161.145			
Port* 22			
User ID* cisco			
Password* *****			
Directory* /			
L			
File Name	Certificate Type		Server Source
CUCM1151PUB_capf.pkcs12	STORE	CUCM1151PUB	
CUCM1151PUB_tttp.pkcs12	STORE	CUCM1151PUB	
CUCM1151PUB_tomcat.pkcs12	STORE	CUCM1151PUB	

#### 步骤2.将所有证书从源群集中的所有节点导出到SFTP服务器。

·在后续弹出窗口中,为证书类**型选**择全部,然后单击**导出**,如图所示。

cisco Unified Operating System Administration For Cisco Unified Communications Solutions	
Show - Settings - Security - Software Upgrades - Services - Help -	
Bulk Certificate Management	
Save Export	
Status-	
SFTP Details           IP Address*           IP Address*           Port*           22           User ID*           cisco           Password*           Directory*           /           File Name           CUCM1151PUB_capf.pkcs12           CUCM1151PUB_tappa.tkcs12           CUCM1151PUB_tappa.tkcs12	Bulk Certificate Export - Mozilla Firefox Image: Status - Status: Ready FExport Certificate Type
Save Export	Certificate Type * All

·关闭弹出窗口并使用为源集群中的每个节点创建的PKCS12文件进行批量证书管理更新,网页将刷 新此信息。如图所示,源集群的批量证书管理网页现在显示导出到SFTP的源和目标PKCS12文件。

cisco	Cisco Unified Operating System Administration For Cisco Unified Communications Solutions				Navigation Cisco Unified O admin Search Documents
Show - Se	ettings   Security   Software Upgrades   Services   Help				
Bulk Certifi	icate Management				
Save S	Export 🔒 Consolidate				
-Status					
(i) Status	I: Ready				
-SFTP Deta	ils				
IP Address Port*	* 10.24.161.145				
User ID*	cisco				
Password*	•••••				
Directory*	/				
	File Name		Certificate Tune		Server Source
CUCM1052F	PUB_capf.pkcs12	STORE	Conditione Type	CUCM1052PUB	Server Source
CUCM1151F	FUB_capt.pkcs12	STORE		CUCM1151PUB	
CUCM1052F	PUB_tftp.pkcs12	STORE		CUCM1052PUB	
CUCM1151F	PUB_tftp.pkcs12	STORE		CUCM1151PUB	
CUCM1052F	PUB_tomcat.pkcs12	STORE		CUCM1052PUB	
CUCM1151F	PUB_tomcat.pkcs12	STORE		CUCM1151PUB	
Save	Export Consolidate				

## 整合源和目标PKCS12文件

**注意:**虽然批量证书管理导出在源群集和目标群集上完成,但合并仅通过其中一个群集上的 CUCM发布服务器完成。

步骤1: 返回源群集的CUCM发布者的Bulk Certificate Management页面,然后单**击**Consolidate,如 图所示。

ulud. Cisco Unified Operating System Administration		Navigation Cisco Unifie
CISCO For Cisco Unified Communications Solutions		admin Search Docum
Show * Settings * Security * Software Upgrades * Services * Help *		
Bulk Certificate Management		
🔜 Save 🌇 Export 📵 Consolidate		
- Status		
(i) Status: Ready		
-SFTP Details		
IP Address* 10.24.161.145		
Port* 22		
User ID* cisco		
Password* +++++		
Directory* /		
File Name	Certificate Type	Server Source
CUCM1052PUB_capf.pkcs12	STORE	CUCM1052PUB
CUCM1151PUB_capf.pkcs12	STORE	CUCM1151PUB
CUCM1052PUB_tftp.pkcs12	STORE	CUCM1052PUB
CUCM1151PUB_tftp.pkcs12	STORE	CUCM1151PUB
CUCM1052PUB_tomcat.pkcs12	STORE	CUCM1052PUB
JUCM1151PUB_tomost.pkcs12 STORE CUCM1151PUB		
Save Export Consolidaty		

### ·在后续弹出窗口中,为证书类**型选**择"全部",然后单击**"合**并",如图所示。

Cisco Unified Operating System Administration For Cisco Unified Communications Solutions		
Show - Settings - Security - Software Upgrades - Services - Help -		
Bulk Certificate Management		
Save Prove Consolidate		
Status		
i Status: Ready		
SFTP Details	🍓 Bulk Certificate Consolidate - Mozilla Firefox 🕸 📼 — 🗆 🗙	
IP Address* 10.24.161.145		
Port* 22	https://10.201.194.75/cmplatform/bulkcertmgmtPopUp.do?certaction=consol ***	
User ID* cisco	Bulk Certificate Consolidate	
Password* •••••		
Directory* /		
Eile Name	Status	
CUCM1052PUB_capf.pkcs12	i Status: Ready	
CUCM1151PUB_capf.pkcs12		
CUCM1052PUB_tftp.pkcs12		
CUCM1151PUB_tttp.pkcs12 CUCM1052PUB_tomcat_pkcs12	Certificate Type - [All	
CUCM1151PUB_tomcat.pkcs12	Concolidata Clore	
	Consolution Close	
Save Export Consolidate	(i) *- indicates required item.	
1 * indicates required item		

·您可以随时检查SFTP目录,以验证源和目标集群包含的pkcs12文件。从目标群集和源群集导出所 有证书后,SFTP目录的内容已完成,如图所示。

I     Image: Imag	tificate Export					\$ ⊑	-	
$\leftrightarrow \rightarrow \land \uparrow \square \rightarrow B$	ulk Certificate Export				ٽ ~	Search Bulk	Certificate	Export 🔎
✓ Quick access         ☑ Documents         ✓ Downloads         ✓ Pictures         ✓ Cisco Receipts         CUCM How To         ☑ Desktop	Name pkcs12 10.24.161.145_bulk_tftp.pkcs12 10.24.161.145_bulk_tomcat.pkcs12 CUCM1052PUB_tftp.pkcs12 CUCM1052PUB_tomcat.pkcs12 CUCM1151PUB_tftp.pkcs12 CUCM1151PUB_tomcat.pkcs12	Date modified 4/8/2020 11:19 AM 4/8/2020 11:19 AM 4/8/2020 11:19 AM 4/8/2020 11:18 AM 4/8/2020 11:18 AM 4/8/2020 11:16 AM	Type File folder PKCS12 File PKCS12 File PKCS12 File PKCS12 File PKCS12 File PKCS12 File	Size 8 KB 8 KB 3 KB 3 KB 6 KB 6 KB				
☐   🖓 🔂 🔻   pkcs12 File Home Sha	are View				<	1⊳ ⊑	-	□ × ~ €
← → ~ ↑ 🔒 ›	Bulk Certificate Export > pkcs12				v ₽	Search pkcs	2	م
📌 Quick access	Name	Date modified	Туре	Size				
Documents ;	10.24.161.145_bulk_capf.pkcs12	4/8/2020 11:19 AM	PKCS12 File	13 KB				
Downloads	CUCM1052PUB_capf.pkcs12	4/8/2020 11:18 AM 4/8/2020 11:16 AM	PKCS12 File PKCS12 File	7 KB 6 KB				

## 将证书导入目标和源集群

#### 步骤1.将证书导入目标群集

·**在目**标群集的CUCM发布者上,导航至Cisco Unified OS Administration > Security > Bulk Certificate Management,并让页面刷新,然后单击Import,如图所示。

cisco	Cisco Unified Operating System Admin For Cisco Unified Communications Solutions	istration		ad	
Show - Se	ttings • Security • Software Upgrades • Services • Help •				
Bulk Certifi	cate Management				
Save 1	Export 🗿 Consolidate 🗿 Import				
Status					
(i) Status:	: Ready				
SFTP Detai	ils —				
IP Address	10.24.161.145				
Port*	22				
User ID*	cisco				
Password*					
Directory*	/				
				1	
		File Name	Certificate Type		
10.24.161.1	45_bulk_capt.pkcs12		BULK	10.24.161.145	
10.24.161.1	45_bulk_tomcat.nkcs12		BULK	10.24.161.145	
CUCM1052P	UB capf.pkcs12		STORE	CUCM1052PUB	
CUCM1151P	UB_capf.pkcs12		STORE	CUCM1151PUB	
CUCM1052PUB_tftp.pkcs12			STORE	CUCM1052PUB	
CUCM1151PUB_tftp.pkcs12 STORE CUCM1			CUCM1151PUB		
CUCM1052P	UCM1052PUB_tomcat.pkcs12 CUCM1052PUB				
CUCM1151P	CM1151PUB_tomcat.pkcs12 STORE CUCM1151PUB				
Save	Export Consolidate Import				

·在后续弹出窗口中,选择All for Certificate Type,然后单击Import,如图所示。

cisco Unified Operating System Administration For Cisco Unified Communications Solutions		adr
Show - Settings - Security - Software Upgrades - Services - Help -		
Bulk Certificate Management		
Save 🗳 Export 🔋 Consolidate 🔋 Import		
Status		
(i) Status: Ready		
SFTP Details	😝 Bulk Certificate Import - Mozilla Firefox 🛛 🕸 📼 — 🗆 🗙	
IP Address* 10.24.161.145		
Port* 22	Kings://10.201.194.78/cmplatform/bulkcertmgmtPopup.dorcertaction=Import =	
User ID* cisco	Bulk Certificate Import	
Password* •••••	Close	
Directory* /		
File Name	Status	
10.24.161.145_bulk_capf.pkcs12	(i) Status: Ready	10.24.161.145
10.24.161.145_bulk_tftp.pkcs12	- Tunnart Castificata Tunna	10.24.161.145
10.24.161.145_bulk_tomcat.pkcs12	Cartificate Type	10.24.161.145
CUCM1052P05_capf.pkcs12 CUCM1151PUB_capf.pkcs12		CUCM1052PUB
CUCM1052PUB_tftp.pkcs12	Import Close	CUCM1052PUB
CUCM1151PUB_tftp.pkcs12		CUCM1151PUB
CUCM1052PUB_tomcat.pkcs12	<ul> <li>*- indicates required item.</li> </ul>	CUCM1052PUB
		COCHIDIPOD
Save Export Consolidate Import		
• indicates required item.		

#### 第二步: 对源集群重复步骤1。

**注意:**执行批量证书导入时,证书将按如下方式上传到远程群集:

- ·证书颁发机构代理功能(CAPF)证书作为CallManager-trust上传
- ·Tomcat证书作为tomcat-trust上传
- ·CallManager证书上传为Phone-SAST-trust和CallManager-trust
- ·身份信任列表恢复(ITLRecovery)证书上传为Phone-SAST-trust和CallManager-trust

#### 使用目标集群TFTP服务器信息配置源集群电话

为具有简单文件传输协议(TFTP)选项150的源集群电话配置DHCP范围,以指向目的集群CUCM TFTP服务器。

#### 重置源群集电话以获取目标群集ITL/CTL文件以完成迁移过程

作为迁移过程的一部分,源群集电话尝试建立到源群集的思科信任验证服务(TVS)的安全连接,以 验证目标群集的CallManager或ITLRecovery证书。

**注意:**源群集的CallManager证书来自运行TFTP服务(也称为TFTP证书)的CUCM服务器 ,或者其ITLRecovery证书签署源群集CUCM节点的证书信任列表(CTL)和/或身份信任列表 (ITL)文件。同样,目标群集的CallManager证书来自运行TFTP服务的CUCM服务器,或者其 ITLRecovery证书签署目标群集CUCM节点的CTL和/或ITL文件。CTL和ITL文件是在运行 TFTP服务的CUCM节点上创建的。如果源群集TVS未验证目标群集的CTL和/或ITL文件,则电 话迁移到目标群集失败。

**注意:**在启动源群集电话迁移过程之前,请确认这些电话已安装有效的CTL和/或ITL文件。另 外,确保对于源群集,企业功能"准备群集以回滚到8.0之前版本"设置为False。此外,验证运 行TFTP服务的目标集群CUCM节点是否安装了有效的CTL和/或ITL文件。

在非安全集群中,源电话获取目标集群ITL文件以完成电话迁移的流程:

步骤1. CallManager和目标群集的ITL文件中包含的ITLRecovery证书(重置时提供给源群集电话 )均不能用于验证当前安装的ITL文件。这会导致源群集电话与源群集的TVS建立连接,以验证目标 群集的ITL文件。

步骤2.电话在tcp端口2445上建立到源集群TVS的连接。

步骤3.源群集的TVS向电话提供其证书。电话验证连接并请求源群集TVS验证目标群集的

CallManager或ITLRecovery证书,以允许电话下载目标群集的ITL文件。

步骤4.验证和安装目标群集ITL文件后,源群集电话现在可以从目标群集验证和下载签名的配置文件。

在安全集群中,源电话获取目标集群CTL文件以完成电话迁移的过程:

步骤1.电话引导并尝试从目标群集下载CTL文件。

步骤2. CTL文件由目标群集的CallManager或ITLRecovery证书签名,该证书不在电话的当前CTL或 ITL文件中。

步骤3.因此,电话会到达源群集上的TVS,以验证CallManager或ITLRecovery证书。

**注意:**此时,电话仍有其旧配置,其中包含源集群TVS服务的IP地址。在电话配置中指定的 TVS服务器与电话Callmanager组相同。

步骤4.电话在源群集上建立到TVS的传输层安全(TLS)连接。

步骤5.当源群集TVS向电话提供其证书时,电话会根据其当前ITL文件中的证书验证此TVS证书。 步骤6.如果它们相同,则握手成功完成。

步骤7.源电话请求源群集TVS从目标群集CTL文件验证CallManager或ITLRecovery证书。

步骤8.源TVS服务在其证书存储中找到目标群集CallManager或ITLRecovery,验证它,并且源群集 电话继续使用目标群集CTL文件进行更新。

步骤9.源电话下载目标群集的ITL文件,该文件已根据目标群集当前包含的CTL文件进行验证。由于 源电话的CTL文件现在包含目标群集的CallManager或ITLRecovery证书,因此源电话现在可以验证 CallManager或ITLRecovery证书,而无需与源群集的TVS联系。

# 验证

当前没有可用于此配置的验证过程。

## 故障排除

目前没有针对此配置的故障排除信息。

## 配置演练视频

此链接提供对视频的访问,该视频在CUCM集群之间通过批量证书管理:

<u>CUCM群集之间的批量证书管理</u>