在CUCM 14中为CallManager配置Tomcat证书重用

目录

简介

本文档介绍如何在Cisco Unified Communications Manager(CUCM)服务器上为CallManager重复使用Multi-SAN Tomcat证书。

先决条件

要求

Cisco 建议您了解以下主题：

- CUCM证书
- 实时监控工具(RTMT)
- 身份信任列表(ITL)

使用的组件

本文档中的信息基于CUCM 14.0.1.13900-155。

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

CUCM的两个主要服务是Tomcat和CallManager。在早期版本中，每个服务都需要不同的证书才能完成整个集群。在CUCM版本14中，添加了一项新功能，以对CallManager服务重复使用Multi-SAN Tomcat证书。使用此功能的优势包括：

- 降低获得一个公共证书颁发机构(CA)签名的证书群集的两个证书的成本。
- 此功能可减小ITL文件的大小，从而降低开销。

Low Impact Medium Impact. High Impact.

Type	Risk	Trust List	Impact	Phone Restart	Service Restart
Tomcat		-	Web services, SSO, EM/EMCC Login	None	Tomcat
IPSec		-	DRS, Ipsec Tunnels	None	DRF Master/Local
CAPF		CTL + ITL	LSC must be updated, secure features	All	CAPF
Callmanager		CTL + ITL	Registration, TL issues, Trunks, CTI	All	CM,CTI,TFTP
TVS		ITL	Verification of TLs, CFG files, https connection	Some	TVS
ITLRecovery		CTL + ITL	Signer or SAST backup for ITL/CTL	All	

配置

⚠ 警告：在上传Tomcat证书之前，请验证单点登录(SSO)已禁用。如果启用，则必须禁用并在一次Tomcat证书再生过程完成后重新启用SSO。

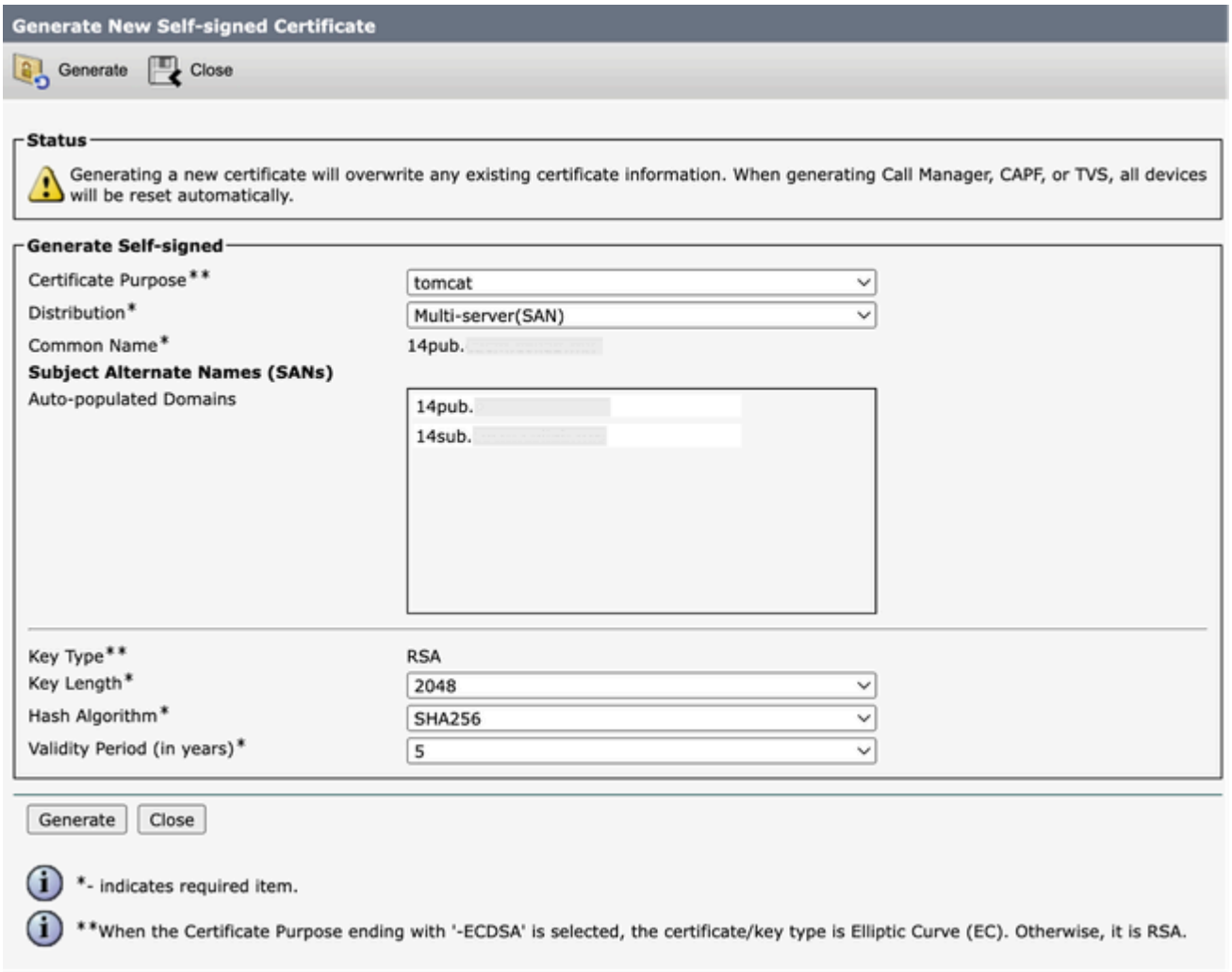
1.将Tomcat证书设置为多SAN Low Impact

在CUCM 14中，Tomcat Multi-SAN证书可以是自签名或CA签名。如果您的Tomcat证书已经是多SAN，请跳过此部分。

自签名

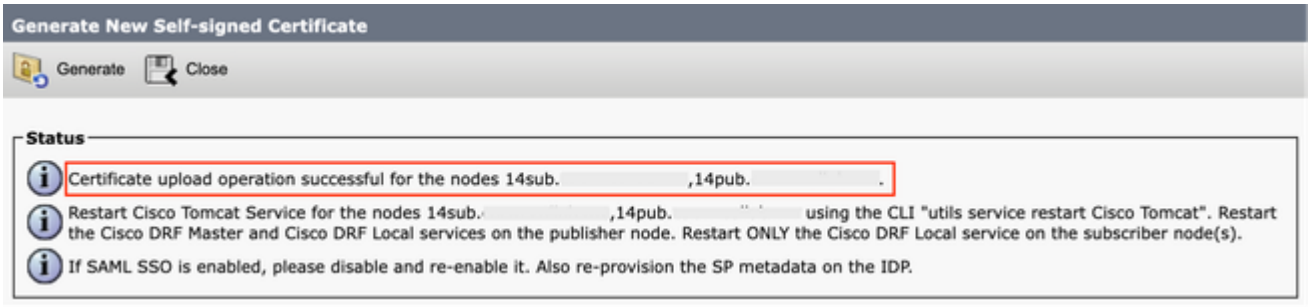
步骤1.登录并导Publisher > Operating System (OS) Administration航至Security > Certificate Management > Generate Self-Signed。

步骤2.选择Certificate Purpose: tomcat > Distribution: Multi-Server SAN。它会自动填充SAN域和父域。



生成自签名多SAN Tomcat证书屏幕

步骤3.点击Generate，并验证消息下方是否列出了所有节Certificate upload operation successful点。单击。Close



生成自签名的多SAN Tomcat成功消息

步骤4.重新启动Tomcat服务，打开与群集所有节点的CLI会话，然后运行utils service restart Cisco Tomcat命令。

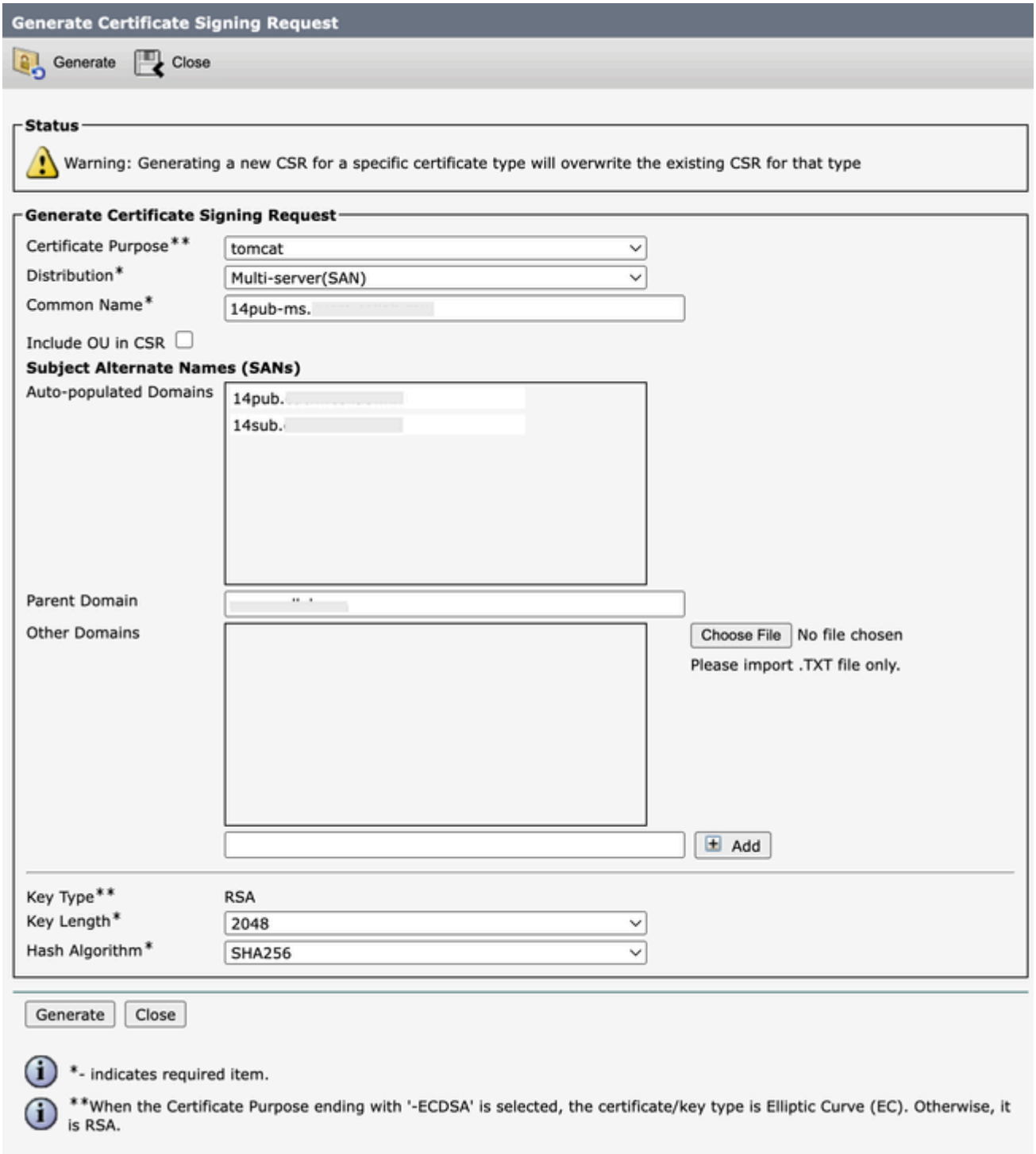
步骤5.导航至，然Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services后重新启动Cisco DRF Master Service和Cisco DRF Local Service。

步骤6.导航到每个并重新启Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network ServicesCisco DRF Local Service们。

CA签名

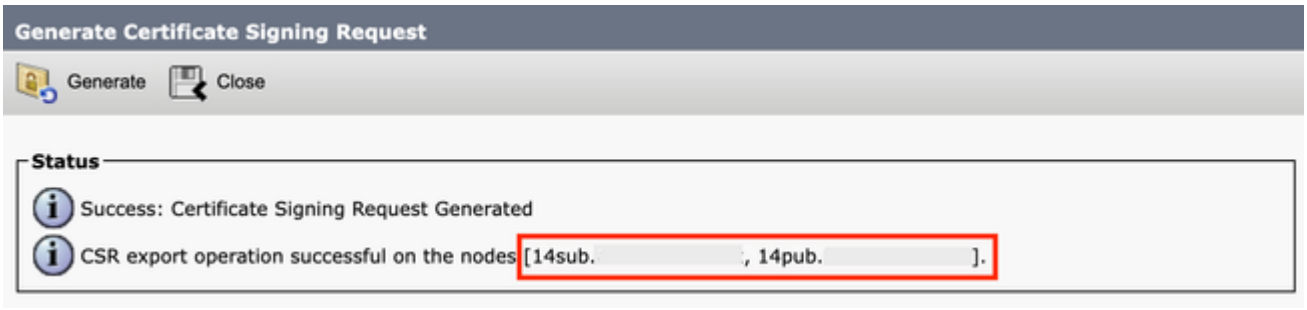
步骤1.登录并导Publisher > Operating System (OS) Administration航至Security > Certificate Management > Generate CSR。

步骤2.选择Certificate Purpose: tomcat > Distribution: Multi-Server SAN。它会自动填充SAN域和父域。



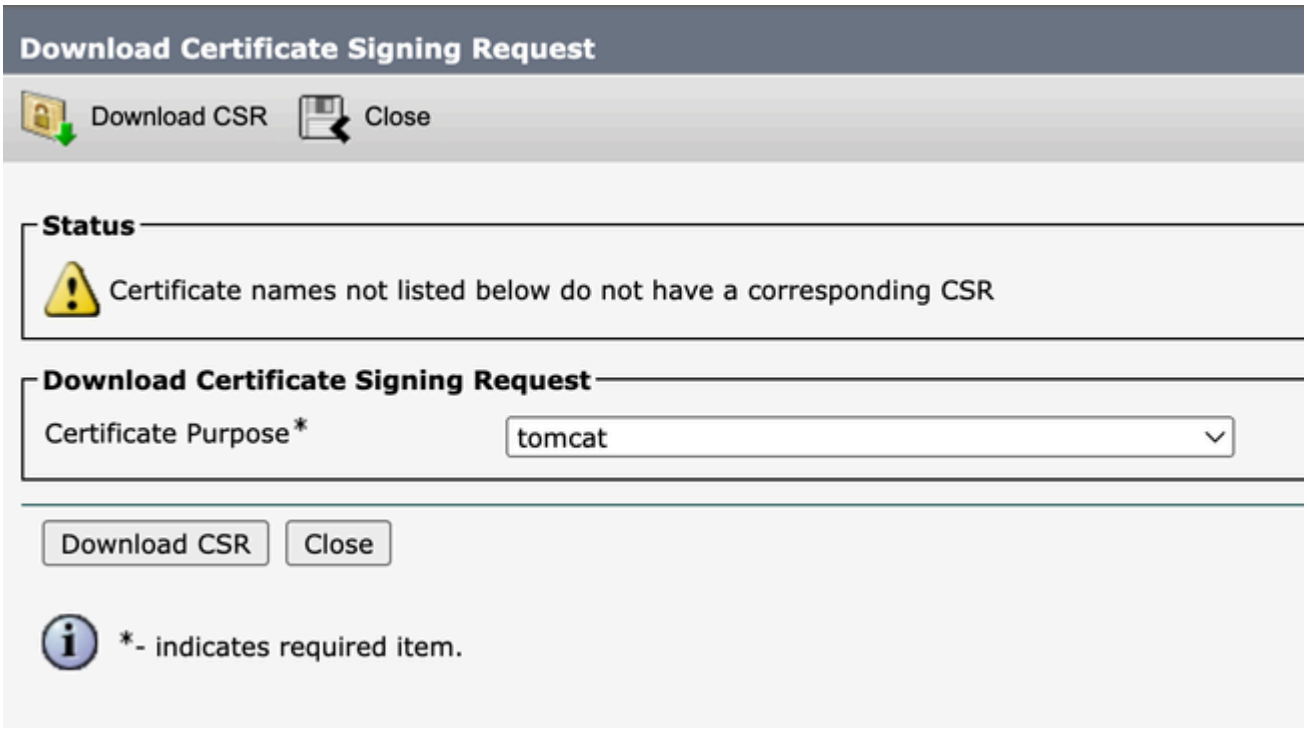
Generate Multi-SAN CSR for Tomcat Certificate屏幕

步骤3.点击Generate，并验证消息下方列出的所有节CSR export operation successful点。单击。Close



生成多SAN CSR Tomcat成功消息

步骤4.单击Download CSR > Certificate Purpose: tomcat > Download。



下载Tomcat CSR屏幕

步骤5.将CSR发送到您的CA进行签名。

步骤6.要上载CA信任链，请导航Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust。 设置证书的说明并浏览信任链文件。

步骤7.上传CA签名的证书，导航至Certificate Management > Upload certificate > Certificate Purpose: tomcat。 设置证书的说明并浏览CA签名的证书文件。

步骤8.重新启动Tomcat服务，打开与集群所有节点的CLI会话，然后运行命令utils service restart Cisco Tomcat。

步骤9.导航至，然Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services后重新启动Cisco DRF Master Service和Cisco DRF Local Service。

步骤10.导航到每个并重新启Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network ServicesCisco DRF Local Service。

2.重用CallManager的Tomcat证书 Medium Impact.

警告：对于CUCM 14，引入了新的企业参数Phone Interaction on Certificate Update。当更新其中一个TVS、CAPF或TFTP(CallManager/ITLRecovery)证书时，使用此字段手动或自动重置电话（如果适用）。此参数默认设置为reset the phones automatically。在重新生成、删除和更新证书后，确保重新启动适当的服务。

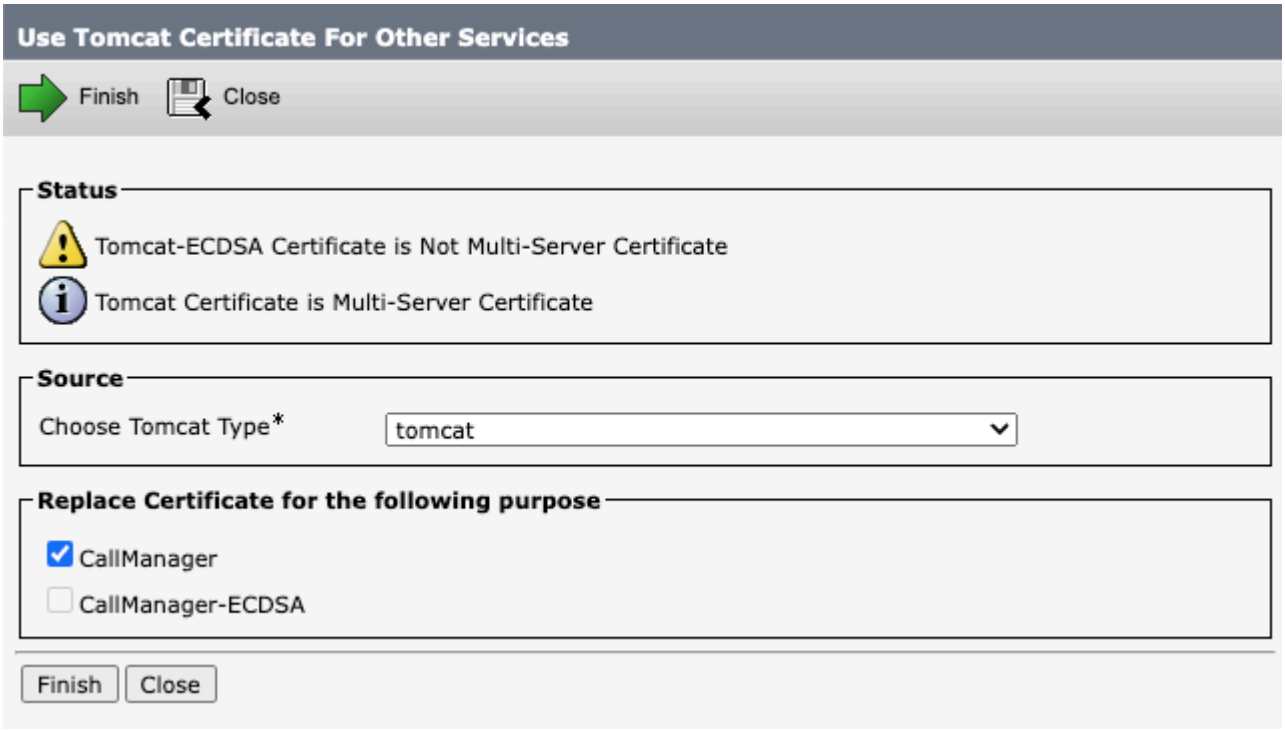
需要重新启动服务以正常的CallManager证书重新生成。选中Regenerate Certificates In Unified Communications Manager。

步骤1.导航到CUCM发布服务器，然后导航到Cisco Unified OS Administration > Security > Certificate Management。

步骤2.单击Reuse Certificate。

步骤3.从choose **Tomcat type**下拉列表中选择tomcat。

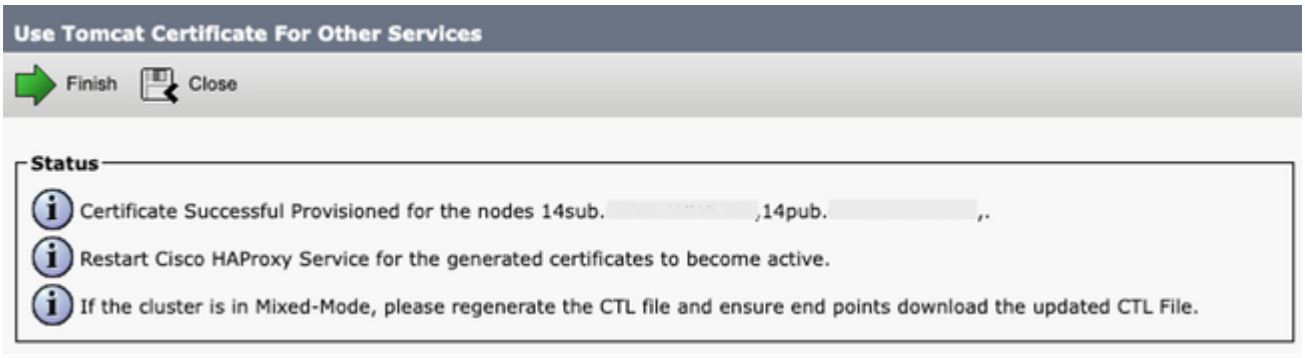
步骤4.在窗Replace Certificate for the following purpose格中，选中CallManager复选框。



Reuse Tomcat Certificate for Other Services屏幕

注意：如果选择Tomcat作为证书类型，则会启用CallManager作为替换。如果选择tomcat-ECDSA作为证书类型，则会启用CallManager-ECDSA作为替换。

步骤5.单击Finish，以便使用Tomcat Multi-SAN证书替换CallManager证书。



重新使用Tomcat证书成功消息

步骤6.重新启动Cisco HAProxy服务，打开与集群所有节点的CLI会话，然后运行该utils service restart Cisco HAProxy命令。

注意：要确定集群是否处于混合模式，请导航至Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode(0 == Non-Secure;1 == 混合模式）。

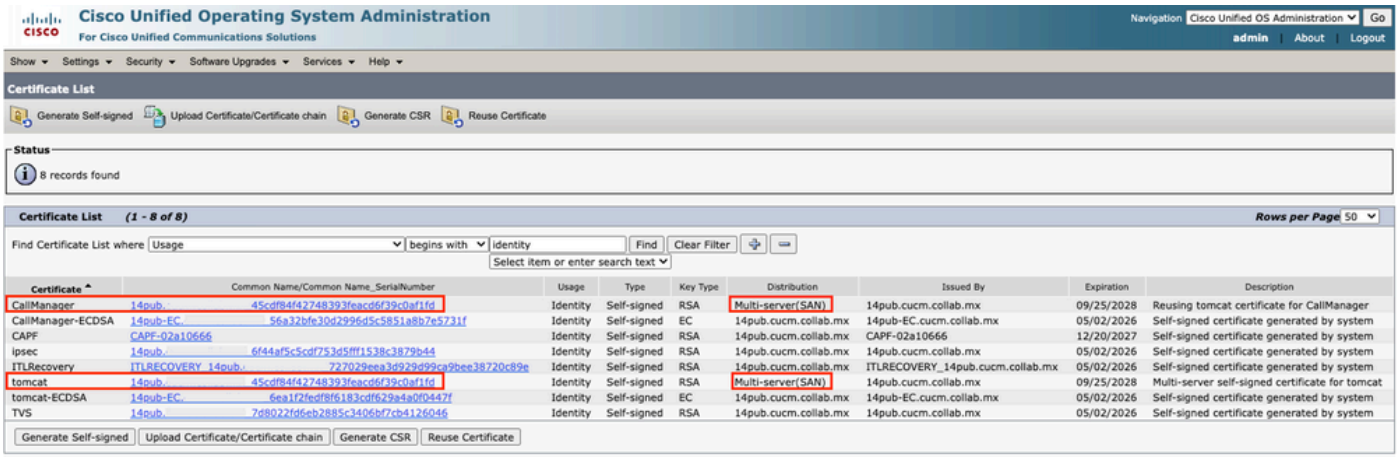
步骤7.如果集群处于混合模式，请打开与发布服务器节点的CLI会话，并运行命**utils ctl update CTLFile**令，然后重置集群的所有电话以使CTL文件更新生效。

验证

步骤1.导航到CUCM发布服务器，然后导航到Cisco Unified OS Administration > Security > Certificate Management。

步骤2.按过滤条件Find Certificate List where: Usage > begins with: identity ，然后单Find击。

步骤3. CallManager和Tomcat证书必须以相同的值结Common Name_Serial Number尾。



验证CallManager的Tomcat证书重复使用

注意：从SU4开始，在启用证书重用后，Call Manager证书不会显示在GUI上，而两个证书在SU2和SU3中均可见。

相关信息

- Cisco Unified Communications Manager安全指南14
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。