Configurar a reutilização de certificado Tomcat para CallManager no CUCM 14

Contents

- Introdução
- Pré-requisitos
  - Requisitos
  - Componentes Utilizados
- Informações de Apoio
- Configurar
  - 1. Definir o certificado Tomcat como Multi-SAN
    - Autoassinado
    - Assinado pela CA
  - 2. Reutilizar o certificado Tomcat para CallManager
- Verificar
- Informações Relacionadas

Introdução

Este documento descreve como reutilizar o certificado Multi-SAN Tomcat para CallManager em um servidor Cisco Unified Communications Manager (CUCM).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Certificados CUCM
- Ferramenta de monitoramento em tempo real (RTMT)
- Lista de Confiabilidade de Identidade (ITL)

Componentes Utilizados

As informações neste documento são baseadas no CUCM 14.0.1.13900-155.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os dois principais serviços para o CUCM são Tomcat e CallManager. Nas versões anteriores, certificados diferentes para cada serviço eram necessários para o cluster completo. No CUCM versão 14, um novo recurso foi adicionado para reutilizar o certificado Multi-SAN Tomcat para o serviço CallManager também. Os benefícios de usar esse recurso são:

- Reduz o custo de obter dois certificados assinados por uma autoridade de certificação pública (CA) para um cluster de certificados assinados por CA.
- Esse recurso reduz o tamanho do arquivo ITL, reduzindo assim a sobrecarga.

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	

Configurar

> ⚠ Caution: Antes de carregar um certificado Tomcat, verifique se o SSO (Logon único) está desabilitado. Caso esteja habilitado, o SSO deve ser desabilitado e reabilitado assim que o processo de regeneração do certificado Tomcat for concluído.

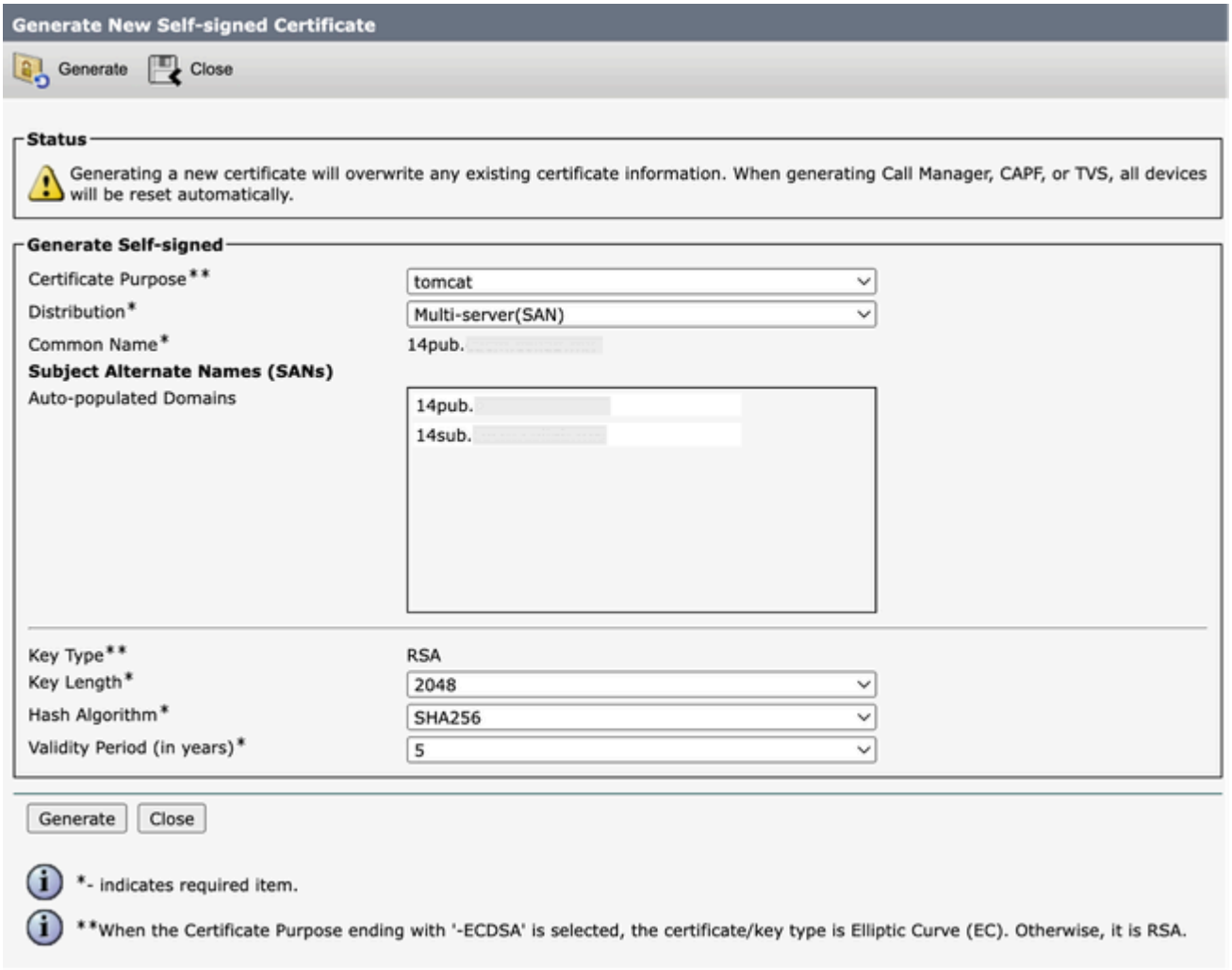
1. Definir o certificado Tomcat como Multi-SAN Low Impact

No CUCM 14, o certificado Tomcat Multi-SAN pode ser autoassinado ou CA-assinado. Se o seu certificado Tomcat já for Multi-SAN, ignore esta seção.

Autoassinado

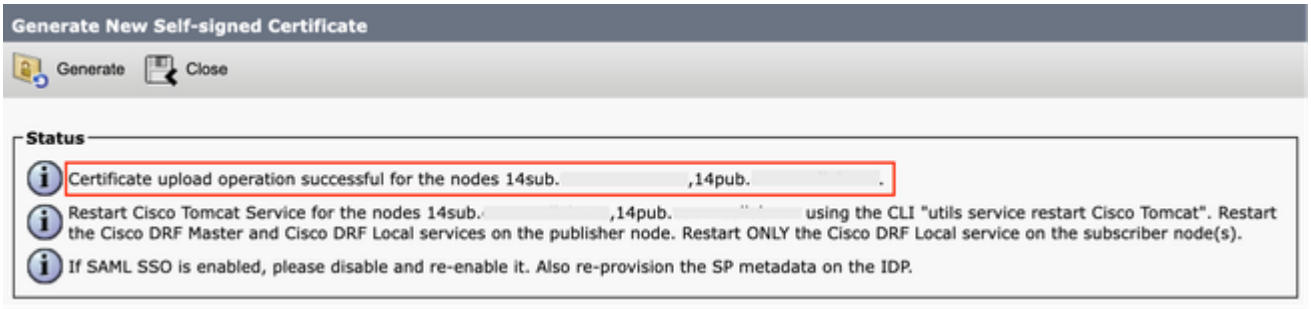
Etapa 1. Efetue login no Publisher > Operating System (OS) Administration e navegue até Security > Certificate Management > Generate Self-Signed.

Etapa 2. Escolha Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Ele preenche automaticamente os domínios SAN e o domínio pai.



Tela Gerar certificado Multi-SAN Tomcat autoassinado

Etapa 3. Clique em Generatee valide se todos os nós estão listados sob a Certificate upload operation successful mensagem. Clique em .Close



Gerar mensagem de êxito do Tomcat de multi-SAN autoassinado

Etapa 4. Reinicie o serviço Tomcat, abra uma sessão CLI para todos os nós do cluster e execute outils service restart Cisco Tomcatcomando.

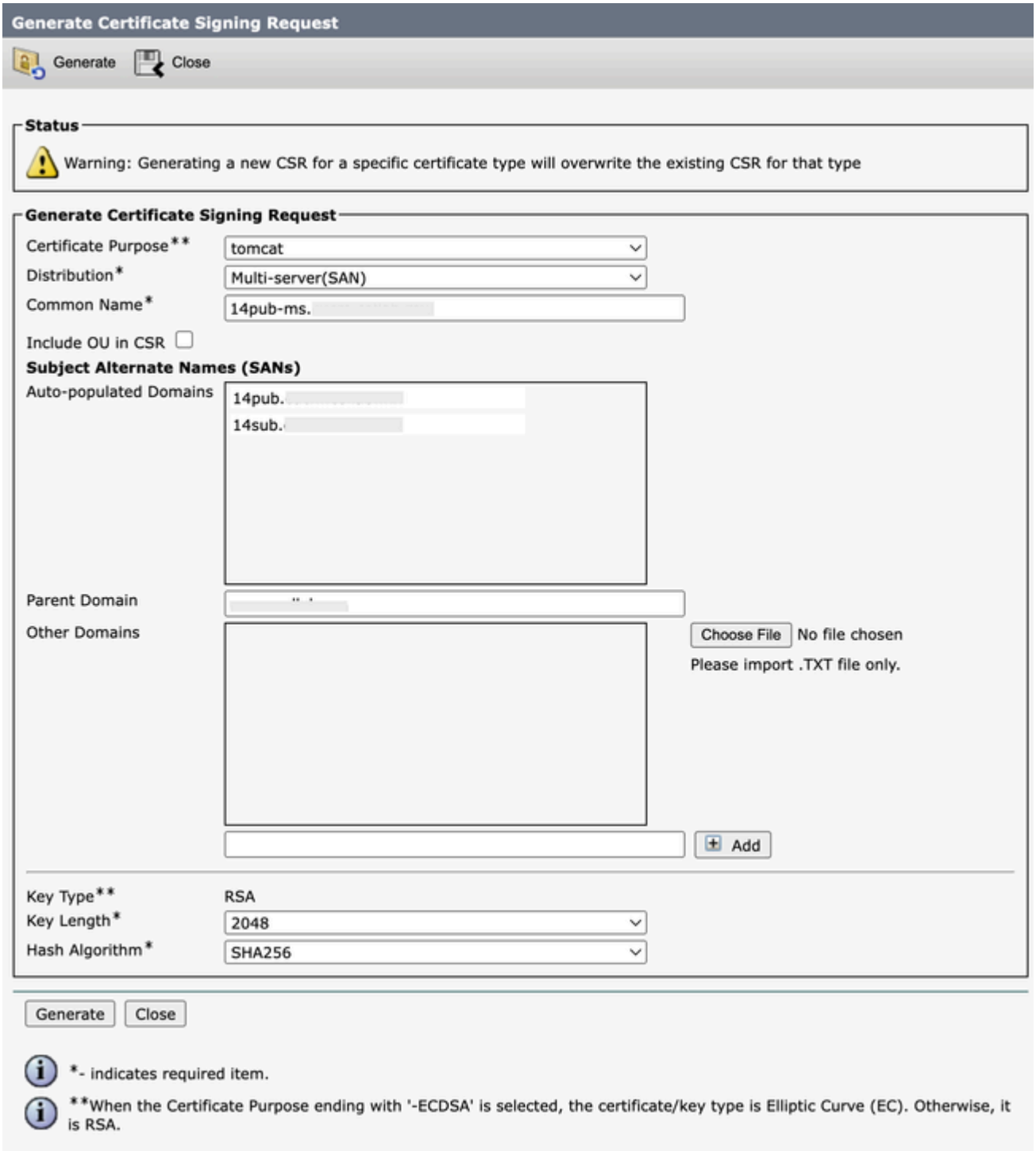
Etapa 5. Navegue até Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services e reinicie o Cisco DRF Master Service e Cisco DRF Local Service.

Etapa 6. Navegue até cada um Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services e reinicie Cisco DRF Local Service.

Assinado pela CA

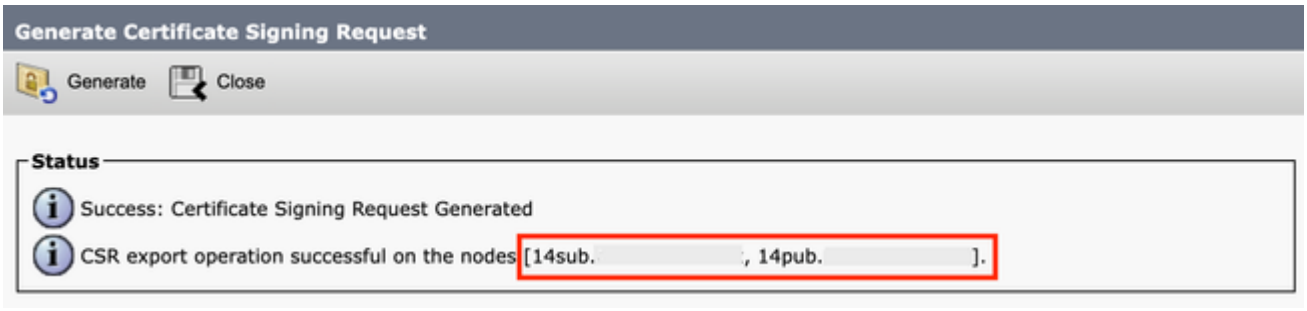
Etapa 1. Efetue login no Publisher > Operating System (OS) Administration e navegue até Security > Certificate Management > Generate CSR.

Etapa 2. Escolha Certificate Purpose: tomcat > Distribution: Multi-Server SAN. Ele preenche automaticamente os domínios SAN e o domínio pai.



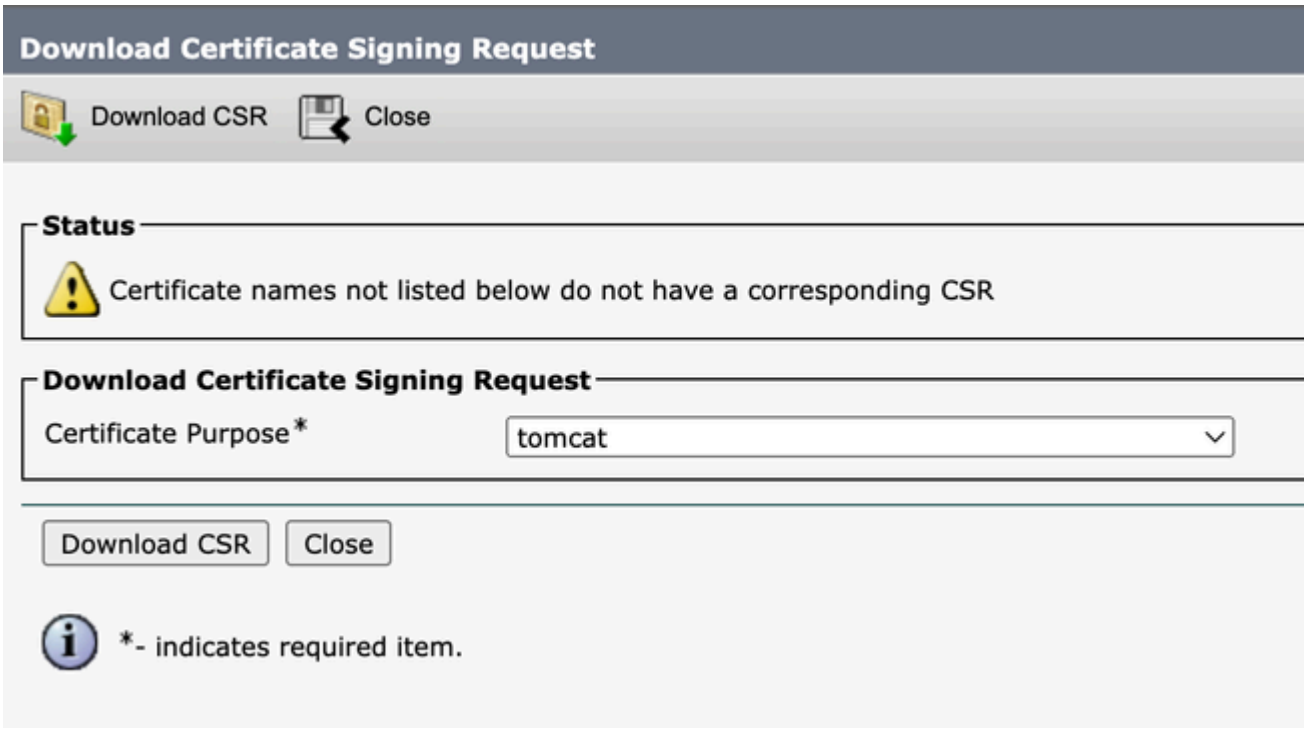
Tela Gerar CSR Multi-SAN para certificado Tomcat

Etapa 3. Clique em Generatee valide se todos os nós estão listados sob a CSR export operation successful mensagem. Clique em . Close



Gerar mensagem de êxito do Tomcat CSR de várias SANs

Etapa 4. Clique em Download CSR > Certificate Purpose: tomcat > Download.



Tela Baixar Tomcat CSR

Etapa 5. Envie o CSR à sua CA para assinatura.

Etapa 6. Para carregar a cadeia de confiança da autoridade de certificação, navegue Certificate Management > Upload certificate > Certificate Purpose: tomcat-trust. Defina a descrição do certificado e procure os arquivos da cadeia de confiança.

Etapa 7. Carregue o certificado assinado pela CA, navegue até Certificate Management > Upload certificate > Certificate Purpose: tomcat. Defina a descrição do certificado e procure o arquivo de certificado assinado pela CA.

Etapa 8. Reinicie o serviço Tomcat, abra uma sessão CLI para todos os nós do cluster e execute o utils service restart Cisco Tomcat comando.

Etapa 9. Navegue até Publisher > Cisco Unified Serviceability > Tools > Control Center - Network Services e reinicie o Cisco

DRF Master Service e Cisco DRF Local Service.

Etapa 10. Navegue até cada um Subscriber > Cisco Unified Serviceability > Tools > Control Center - Network Services e reinicie Cisco DRF Local Service.

2. Reutilizar o certificado Tomcat para CallManager

Medium Impact.

⚠ Caution: Para o CUCM 14, um novo parâmetro Phone Interaction on Certificate Update empresarial é apresentado. Use este campo para redefinir telefones manual ou automaticamente, conforme aplicável, quando um dos certificados TVS, CAPF ou TFTP (CallManager/ITLRecovery) for atualizado. Por padrão, esse parâmetro é definido como reset the phones automatically. Após a regeneração, exclusão e atualização de certificados, assegure-se de que os serviços apropriados sejam reiniciados.

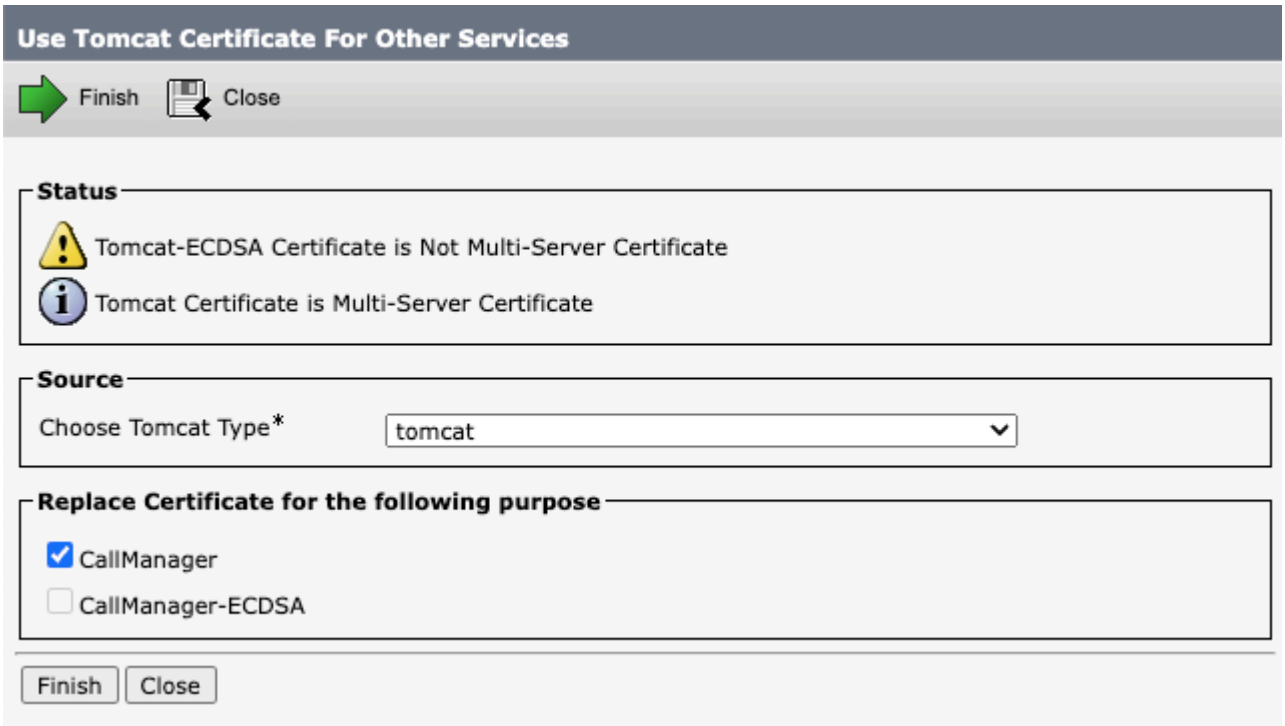
É necessário reiniciar os serviços para uma regeneração de certificado normal do CallManager. Marque Regenerar Certificados No Unified Communications Manager.

Etapa 1. Navegue até o editor do CUCM e, em seguida, para Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Clique em Reuse Certificate.

Etapa 3. Na lista choose **Tomcat type** suspensa, escolha tomcat.

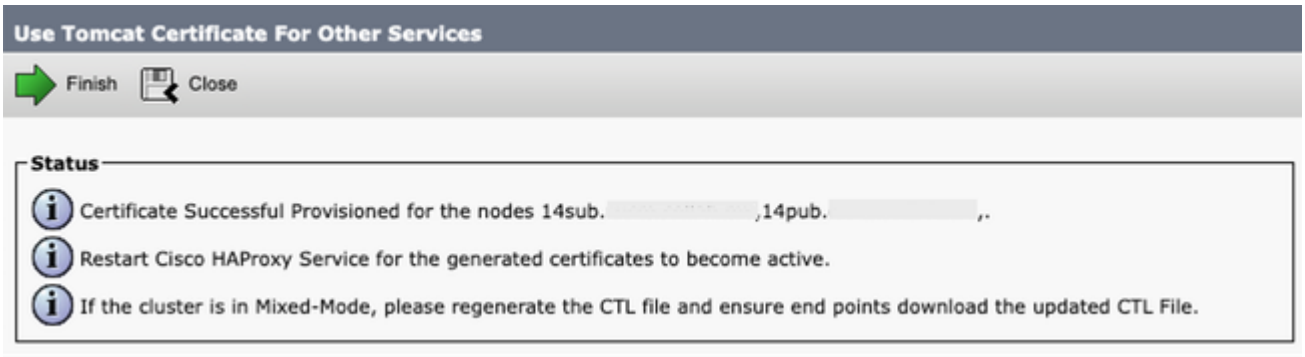
Etapa 4. No painel Replace Certificate for the following purpose, marque a caixa CallManager de seleção.



Tela Reutilizar certificado Tomcat para outros serviços

Note: Se você escolher Tomcat como o tipo de certificado, o CallManager será ativado como o substituto. Se você escolher tomcat-ECDSA como o tipo de certificado, CallManager-ECDSA será ativado como o substituto.

Etapa 5. Clique Finish para substituir o certificado CallManager pelo certificado Tomcat Multi-SAN.



Mensagem de reutilização do certificado do Tomcat com êxito

Etapa 6. Reinicie o serviço Cisco HAProxy, abra uma sessão CLI para todos os nós do cluster e execute o utils service restart Cisco HAProxy comando.

Note: Para determinar se o cluster está no modo misto, navegue para Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Não seguro; 1 == Mixed Mode).

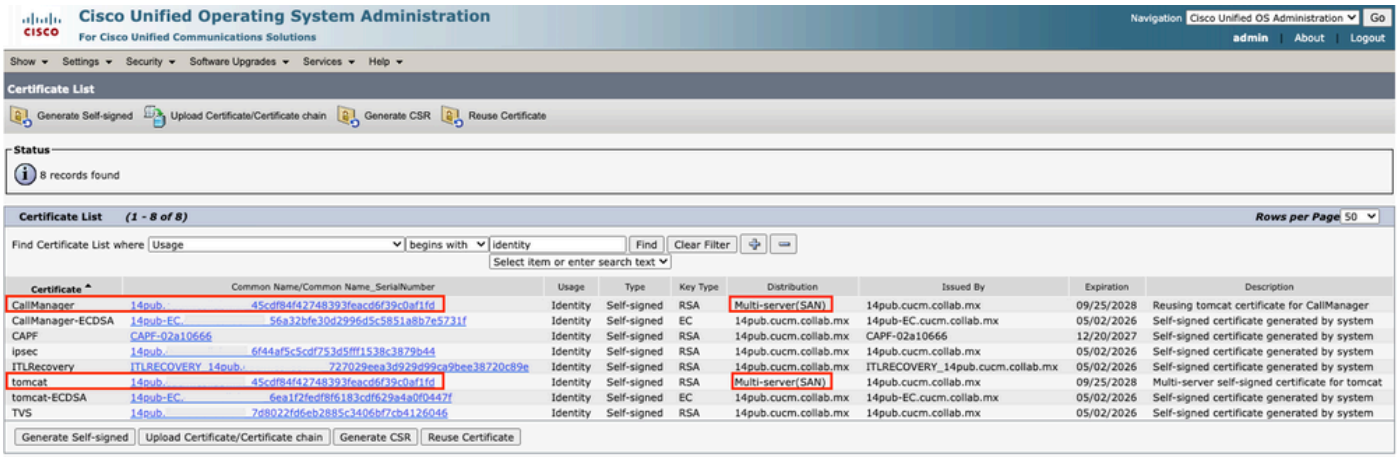
Etapa 7. Se o cluster estiver no Modo Misto, abra uma sessão CLI no nó do Publisher, execute o **utils ctl update CTLFile** comando e redefina todos os telefones do cluster para que as atualizações do arquivo CTL entrem em vigor.

Verificar

Etapa 1. Navegue até o editor do CUCM e, em seguida, para Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Filtre por Find Certificate List where: Usage > begins with: identity e clique em Find.

Etapa 3. Os certificados CallManager e Tomcat devem terminar com o mesmo Common Name_Serial Number valor.



Verifique a reutilização do certificado Tomcat para CallManager

Note: A partir do SU4, com a reutilização de certificado ativada, o certificado do Call Manager não é exibido na GUI, enquanto ambos os certificados são visíveis no SU2 e no SU3.

Informações Relacionadas

- Guia de segurança do Cisco Unified Communications Manager 14
- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.