

Implementar a reutilização do certificado Multi-SAN Tomcat para CallManager

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Reutilizar certificado Tomcat para CallManager](#)

[Verificar](#)

Introdução

Este documento descreve um processo passo a passo sobre como reutilizar o certificado Multi-SAN Tomcat para CallManager no CUCM.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- Certificados CUCM
- Lista de Confiabilidade de Identidade (ITL)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- CUCM versão 15 SU1

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.

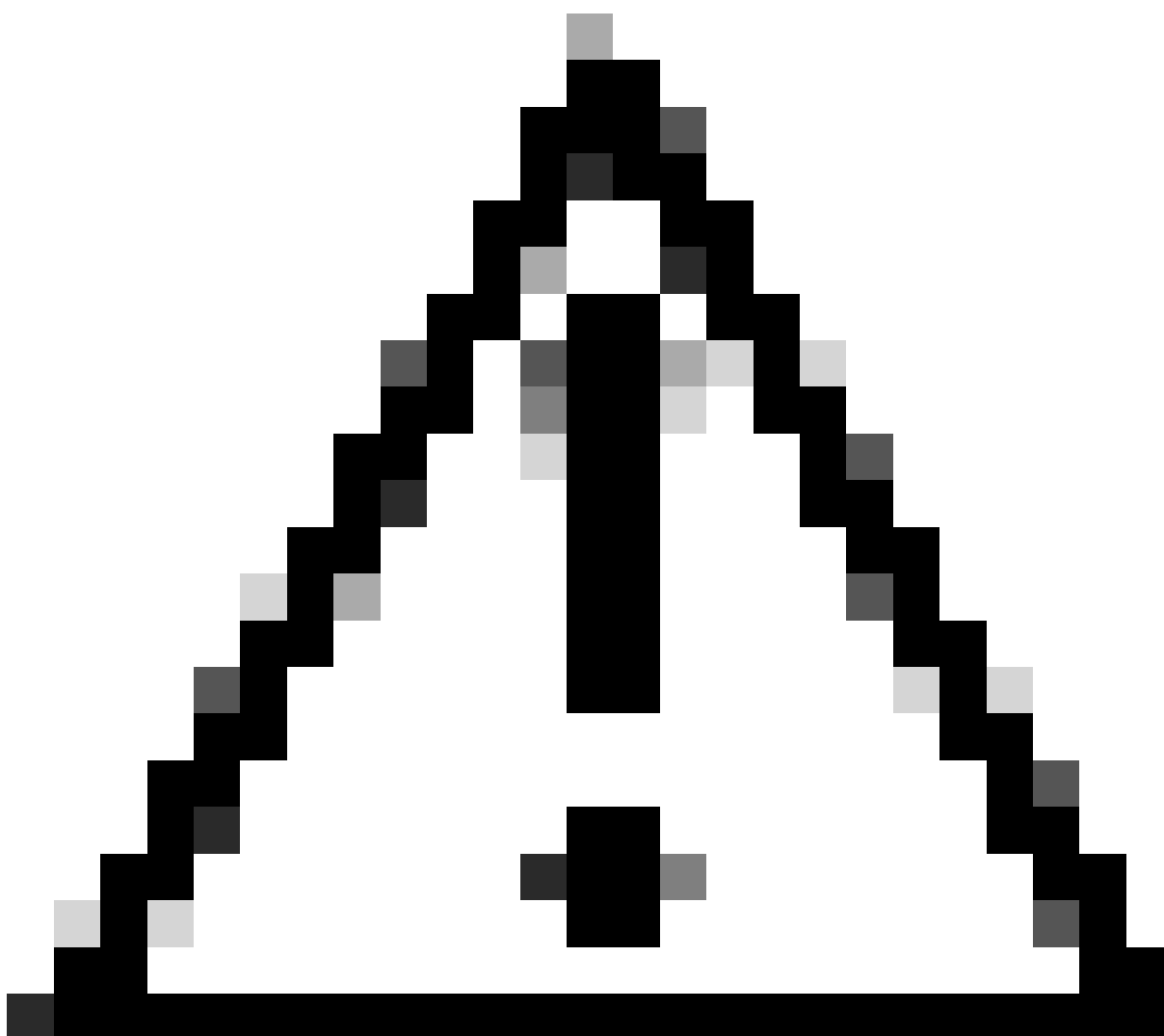
Informações de Apoio

As versões anteriores do CUCM usavam certificados diferentes para cada serviço para o cluster

completo, o que aumentou o número de certificados e o custo. Isso inclui o Cisco Tomcat e o Cisco CallManager, que são serviços críticos executados no CUCM que também têm os respectivos certificados de identidade.

Começando com o CUCM versão 14, um novo recurso foi adicionado para reutilizar o certificado Multi-SAN Tomcat para o serviço CallManager.

A vantagem de usar esse recurso é que você pode obter um certificado da CA e usá-lo em vários aplicativos. Isso garante a otimização de custos e uma redução no gerenciamento, além de reduzir o tamanho do arquivo ITL, reduzindo, assim, a sobrecarga.



Cuidado: antes de continuar com a configuração de reutilização, verifique se o Certificado Tomcat é um certificado SAN de vários servidores. O certificado Tomcat Multi-SAN pode ser autoassinado ou CA-assinado.

Configurar

Reutilizar certificado Tomcat para CallManager



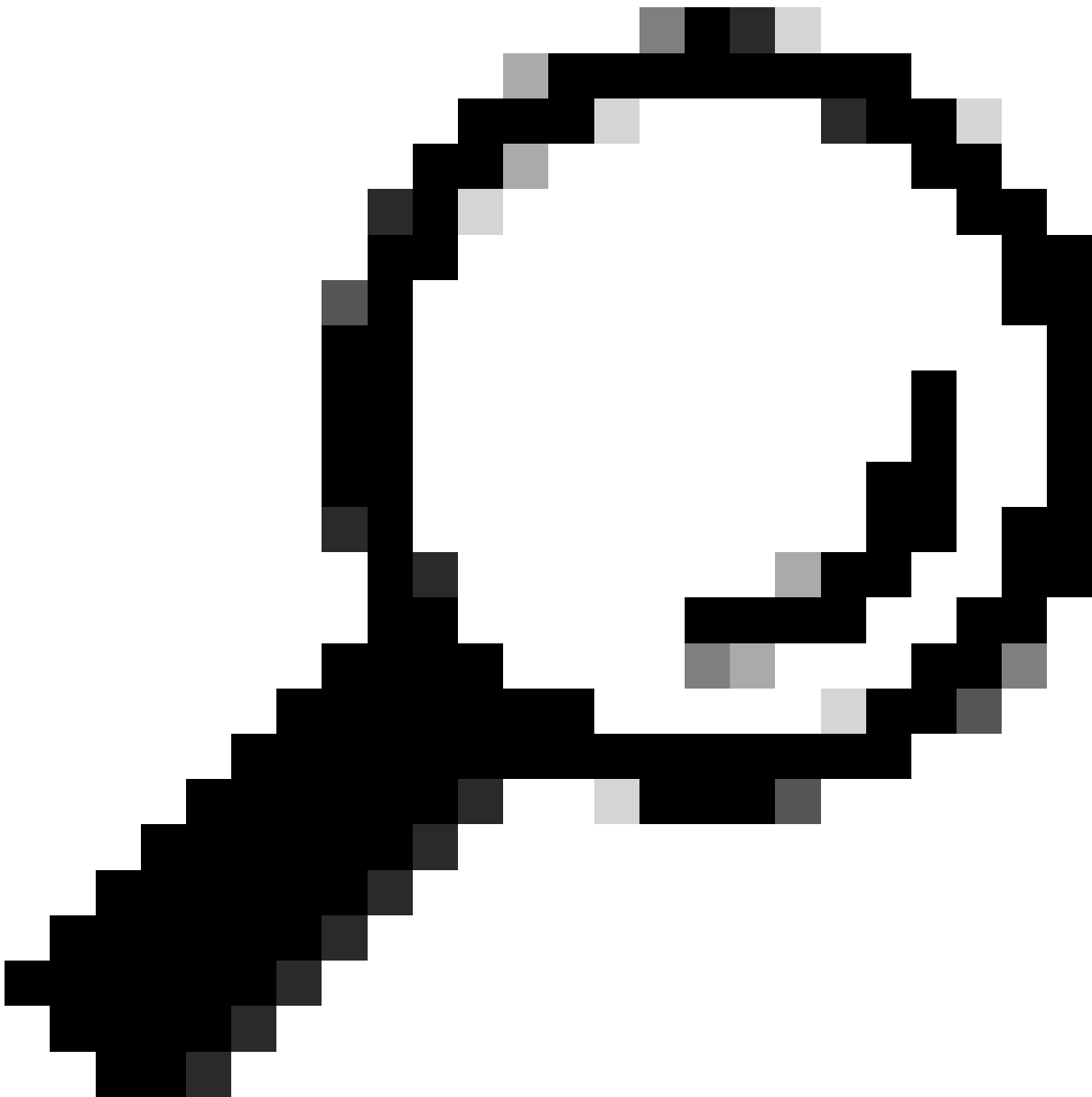
Aviso: antes de continuar, verifique se você identificou se o cluster está no modo misto ou no modo não seguro.

Etapa 1. Navegue até Cisco Unified CM Administration > System > Enterprise Parameters:

Verifique a seção Parâmetros de Segurança e verifique se o Modo de Segurança de Cluster está definido como 0 ou 1. Se o valor for 0, o cluster estará no Modo Não Seguro. Se for 1, o cluster estará no modo misto e você precisará atualizar o arquivo CTL antes da reinicialização dos serviços.

Etapa 2. Navegue para o editor do CUCM e, em seguida, para Cisco Unified OS Administration > Security > Certificate Management.

Etapa 3. Carregue a cadeia de certificados da autoridade de certificação Multi-SAN Tomcat para o armazenamento de confiança do CallManager.



Dica: se estiver usando o certificado SAN multiservidor autoassinado para Tomcat, você poderá ignorar esta etapa.

Antes de reutilizar os certificados, certifique-se de carregar manualmente a cadeia de certificados da autoridade de certificação (que assinou o certificado de identidade tomcat) para o armazenamento confiável do CallManager.



Reinicie esses serviços quando carregar a cadeia de certificados tomcat para a confiança do CallManager.

- CallManager: serviço Cisco HAProxy
- CallManager-ECDSA: Cisco CallManager Service e Cisco HAProxy Service



Etapa 4. Clique em Reutilizar certificado. A página Usar certificados Tomcat para outros serviços

é exibida.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

 Tomcat-ECDSA Certificate is Not Multi-Server Certificate
 Tomcat Certificate is Multi-Server Certificate

Source

Choose Tomcat Type*

Replace Certificate for the following purpose

CallManager
 CallManager-ECDSA

Etapa 5. Na lista suspensa Tipo de Tomcat, escolha Tomcat ou Tomcat-ECDSA.



Etapa 6. No painel Replace Certificate for the following purpose, marque a caixa de seleção CallManager ou CallManager-ECDSA com base no certificado selecionado na etapa anterior.






Observação: 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.

Passo 7. Clique em Finish para substituir o certificado do CallManager pelo certificado de SAN de vários servidores tomcat.

Use Tomcat Certificate For Other Services

 Finish  Close

Status

-  Certificate Successful Provisioned for the nodes cucmpub15. , cucmsub15. .
-  Restart Cisco HAProxy Service for the generated certificates to become active.
-  If the cluster is in Mixed-Mode, please regenerate the CTL file and ensure end points download the updated CTL File.

Etapa 8. Reinicie o serviço Cisco HAProxy em todos os nós do cluster executando o comando `utils service restart Cisco HAProxy` via CLI.

```
admin:utils service restart Cisco HAProxy
Stopping Cisco HAProxy...

Cisco HAProxy [STOPPED] Service Activated
Starting Cisco HAProxy...
Cisco HAProxy [STARTED]
admin: █
```

Etapa 9. Se o cluster estiver no modo misto, atualize o arquivo CTL executando o comando `utils ctl update CTLFile` via CLI do CUCM Publisher e continue a redefinir os telefones para obter o novo arquivo CTL.

Verificar

Observação: o certificado do CallManager não é exibido na GUI quando você reutiliza o certificado.

Você pode executar o comando a partir da CLI para confirmar se o CallManager reutiliza o certificado Tomcat.

- show cert list own

```
admin:show cert list own  
  
tomcat/tomcat.pem: Certificate Signed by AKASH-WINSERVLAB-CA  
tomcat-ECDSA/tomcat-ECDSA.pem: Self-signed certificate generated by system  
ipsec/ipsec.pem: Self-signed certificate generated by system  
ITLRecovery/ITLRecovery.pem:  
CallManager-ECDSA/CallManager-ECDSA.pem: Self-signed certificate generated by system  
CallManager/CallManager.pem: Reusing tomcat certificate for CallManager  
TVS/TVS.pem: Self-signed certificate generated by system  
  
admin:█
```


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.