

Configurar Cluster de Comunicação Unificada

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

[Certificado SAN de vários servidores do CallManager](#)

[Troubleshooting](#)

[Caveats conhecidos](#)

Introdução

Este documento descreve como configurar um Cluster de Comunicações Unificadas com o uso de certificados SAN Multiservidor Assinados por Autoridade de Certificação (CA - Certificate Authority).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Cisco Unified Communications Manager (CUCM)
- CUCM IM e Presence versão 10.5

Antes de tentar essa configuração, verifique se esses serviços estão ativos e funcionais:

- Serviço Web Administrativo de Plataforma da Cisco
- Serviço Cisco Tomcat

Para verificar esses serviços em uma interface da Web, navegue para Cisco Unified Serviceability Page Services > Network Service > Select a server. Para verificá-los na CLI, insira o comando `utils service list`.

Se o SSO estiver habilitado no cluster do CUCM, será necessário desabilitá-lo e habilitá-lo novamente.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

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

No CUCM versão 10.5 e posterior, essa CSR (Certificate Signing Request, solicitação de assinatura de certificado) de armazenamento confiável pode incluir SAN (Subject Alternate Name, nome alternativo do assunto) e domínios alternativos.

1. Tomcat - CUCM e IM&P
2. Cisco CallManager - Somente CUCM
3. Cisco Unified Presence-Extensible Messaging and Presence Protocol (CUP-XMPP) - Somente IM&P
4. CUP-XMPP de servidor para servidor (S2S) - Somente IM&P

É mais simples obter um certificado assinado pela CA nesta versão. Somente um CSR deve ser assinado pela CA, em vez do requisito de obter um CSR de cada nó de servidor e, em seguida, obter um certificado assinado pela CA para cada CSR e gerenciá-lo individualmente.

Configurar

Etapa 1.

Efetue login na Administração do Sistema Operacional (OS) do Publisher e navegue para Segurança > Gerenciamento de Certificado > Gerar CSR.

Generate Certificate Signing Request



Generate



Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com
<hr/>	
Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close



*- indicates required item.

Etapa 2.

Escolha Multi-Server SAN em Distribution (Distribuição).

Generate Certificate Signing Request



Generate



Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose*	tomcat
Distribution*	cs-ccm-pub.v[redacted].com
Common Name*	cs-ccm-pub.v[redacted].com Multi-server(SAN)
Subject Alternate Names (SANs)	
Parent Domain	[redacted].com

Key Length*	2048
Hash Algorithm*	SHA256

Generate

Close



*- indicates required item.

Ele preenche automaticamente os domínios SAN e o domínio pai.

Verifique se todos os nós do cluster estão listados para Tomcat: todos os nós CUCM e IM&P bs para CallManager: somente os nós CUCM foram listados.

Generate Certificate Signing Request

 Generate  Close

Status



Warning: Generating a new CSR for a specific certificate type will overwrite the existing CSR for that type

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* Multi-server(SAN)

Common Name* cs-ccm-pub.com-ms

Subject Alternate Names (SANs)

Auto-populated Domains
cs-ccm-pub.com
cs-ccm-sub.com
cs-imp.com

Parent Domain
....com

Other Domains

 Browse...

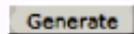
No file selected.

Please import .TXT file only.
For more information please refer to the notes in the Help Section

 Add

Key Length* 2048

Hash Algorithm* SHA256

 Generate  Close

 *- indicates required item.

Etapa 3.

Clique em gerar e, uma vez que o CSR seja gerado, verifique se todos os nós listados no CSR também são exibidos na lista de CSRs exportados Bem-sucedidos.

Generate Certificate Signing Request

 Generate  Close

Status



Success: Certificate Signing Request Generated



CSR export operation successful on the nodes [cs-ccm-sub.com, cs-ccm-pub.com, cs-imp.com].

No Gerenciamento de Certificados, a solicitação de SAN é gerada:

Certificate List (1 - 15 of 15)						
Find Certificate List where Certificate begins with tomcat Find Clear Filter + -						
Certificate ^	Common Name	Type	Key Type	Distribution	Issued By	
tomcat	115pub-ms-██████████	CSR Only	RSA	Multi-server(SAN)	--	
tomcat	115pub-ms-██████████	CA-signed	RSA	Multi-server(SAN)	██████████	

Etapa 4.

Clique em Download CSR e escolha a finalidade do certificado e clique em Download CSR.

Cisco Unified Operating System Administration
For Cisco Unified Communications Solutions

Show Settings Security Software Upgrades Services Help

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR **Download CSR**

Download Certificate Signing Request

Download CSR Close

Status

Certificate names not listed below do not have a corresponding CSR

Download Certificate Signing Request

Certificate Purpose* tomcat

Download CSR Close

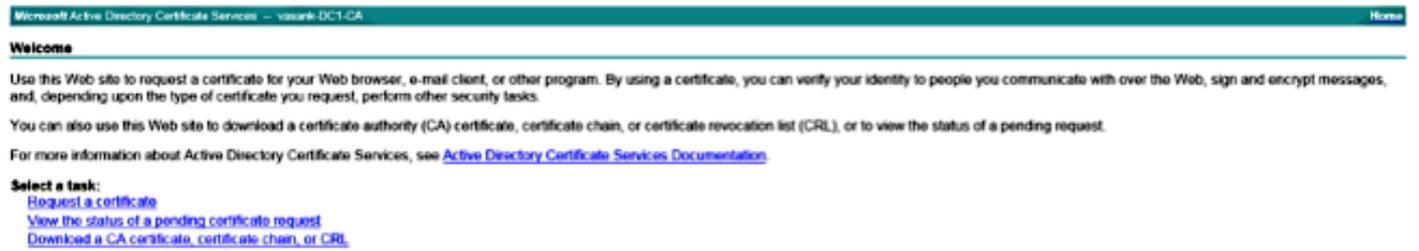
*- indicates required item.

É possível usar a CA local ou uma CA externa, como a VeriSign, para obter a assinatura do CSR (arquivo baixado na etapa anterior).

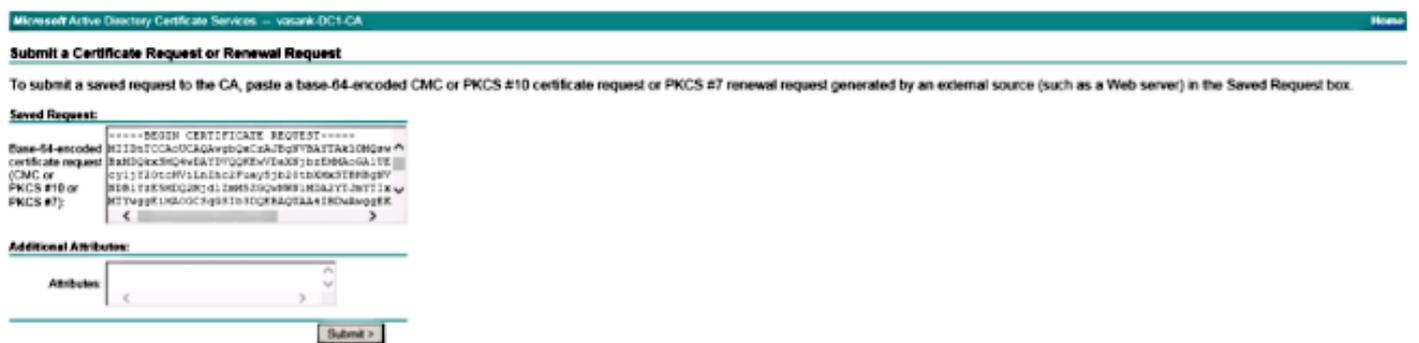
Este exemplo mostra as etapas de configuração para uma CA baseada no Microsoft Windows Server. Se você usar uma CA diferente ou uma CA externa, vá para a Etapa 5.

Faça login em <https://<windowsserveripaddress>/certsrv/>
Escolha Solicitar um Certificado > Solicitação Avançada de Certificado.

Copie o conteúdo do arquivo CSR no campo de solicitação de certificado codificado na Base 64 e clique em Submit.



Envie a solicitação CSR como mostrado aqui.



Etapa 5.

 Observação: antes de carregar um certificado Tomcat, verifique se o SSO está desabilitado. Caso esteja habilitado, o SSO deve ser desabilitado e reabilitado depois que todo o processo de regeneração do certificado Tomcat estiver concluído.

Com o certificado assinado, carregue os certificados CA como tomcat-trust. Primeiro, o certificado raiz e, em seguida, o certificado intermediário, se existir.



Show ▾ Settings ▾ Security ▾ Software Upgrades ▾ Services ▾ Help ▾

Certificate List

Generate Self-signed Upload Certificate/Certificate chain Generate CSR Download CSR

Upload Certificate/Certificate chain

Upload Close

Status



Warning: Uploading a cluster-wide certificate will distribute it to all servers in this cluster

Upload Certificate/Certificate chain

Certificate Purpose* ▾

Description(friendly name)

Upload File certchain.p7b

Etapa 6.

Agora carregue o certificado assinado pelo CUCM como Tomcat e verifique se todos os nós do seu cluster estão listados em "Operação de carregamento de certificado bem-sucedida", como mostrado na imagem:

Upload Certificate/Certificate chain

 Upload  Close

Status

-  Certificate upload operation successful for the nodes cs-ccm-pub.v.com,cs-ccm-sub.com,cs-imp.com.
-  Restart Cisco Tomcat Service for the nodes cs-ccm-pub.com,cs-ccm-sub.com,cs-imp.com using the CLI "utils service restart Cisco Tomcat".

Upload Certificate/Certificate chain

Certificate Purpose*

Description(friendly name)

Upload File No file selected.

 *- indicates required item.

A SAN de vários servidores está listada em Gerenciamento de certificados, conforme mostrado na imagem:

psec-trust	cs-ccm-pub.v.com	Self-signed	cs-ccm-pub.com	cs-ccm-pub.com	04/18/2019	Trust Certificate
ITLRecovery	ITLRECOVERY_cs-ccm-pub.vasank.com	Self-signed	ITLRECOVERY_cs-ccm-pub.v.com	ITLRECOVERY_cs-ccm-pub.v.com	04/18/2019	Self-signed certificate generated by system
tomcat	cs-ccm-pub.v.com-ms	CA-signed	Multi-server(SAN)	v.DCI-CA	12/19/2015	Certificate Signed by v.DCI-CA
tomcat-trust	cs-ccm-pub.v.com-ms	CA-signed	Multi-server(SAN)	v.DCI-CA	12/19/2015	Trust Certificate
tomcat-trust	gs-ccm-pub.v.com	Self-signed	gs-ccm-pub.v.com	gs-ccm-pub.v.com	04/21/2019	Trust Certificate
tomcat-trust	VeriSign Class 3 Secure Server CA - G3	CA-signed	VeriSign_Class_3_Secure_Server_CA_-_G3	VeriSign_Class_3_Public_Primary_Certification_Authority_-_G5	02/08/2020	Trust Certificate
tomcat-trust	dcl-ccm-pub.v.com	Self-signed	dcl-ccm-pub.v.com	dcl-ccm-pub.v.com	04/17/2019	Trust Certificate
tomcat-trust	dcl-ccm-sub.v.com	Self-signed	dcl-ccm-sub.v.com	dcl-ccm-sub.v.com	04/18/2019	Trust Certificate
tomcat-trust	v.DCI-CA	Self-signed	v.DCI-CA	v.DCI-CA	04/29/2064	Root CA
TVS	cs-ccm-pub.vasank.com	Self-signed	cs-ccm-pub.v.com	cs-ccm-pub.v.com	04/18/2019	Self-signed certificate generated by system

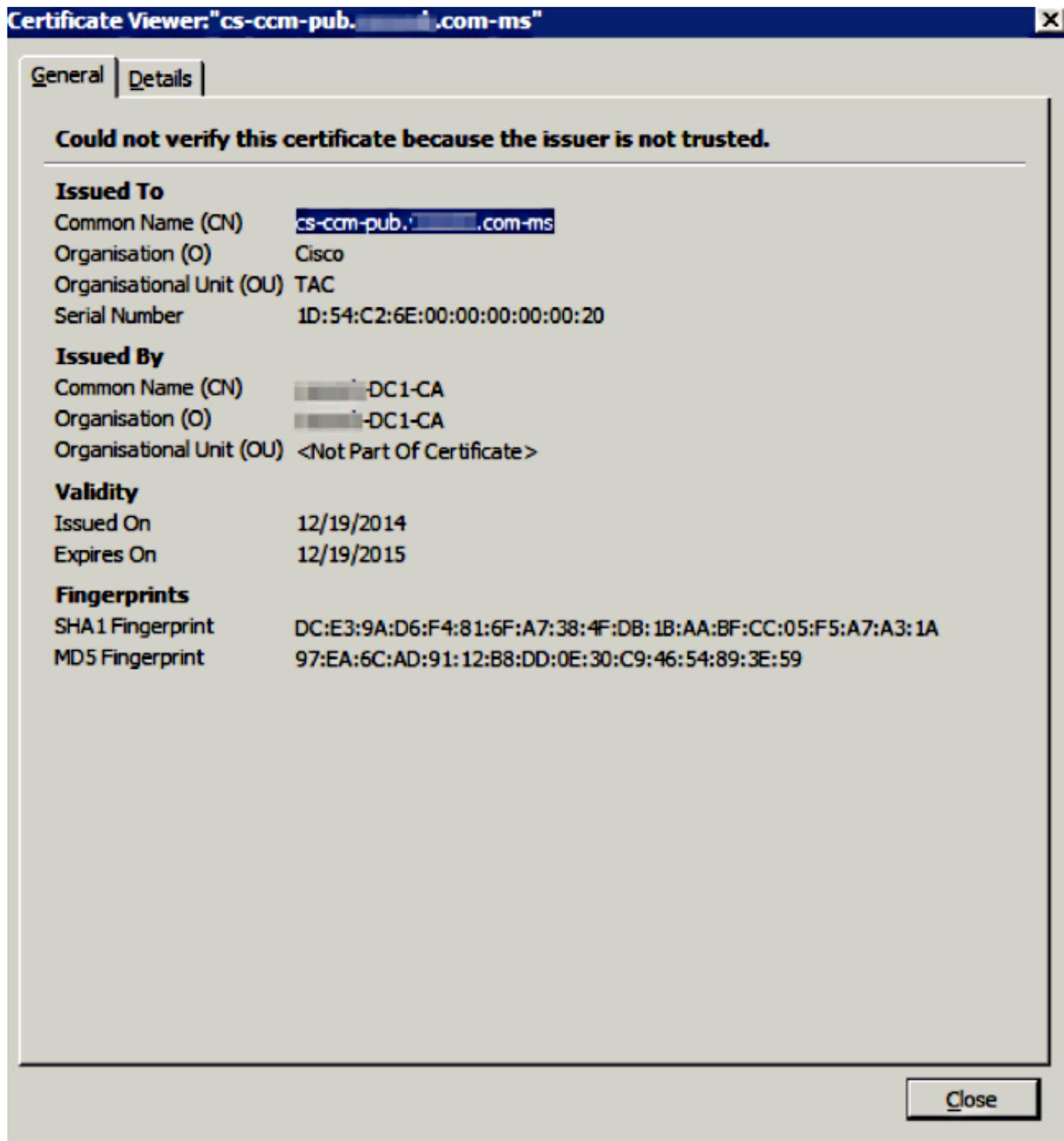
Passo 7.

Reinicie o serviço Tomcat em todos os nós na lista SAN (primeiro Publisher e depois subscribers) via CLI com o comando: utils service restart Cisco Tomcat.

```
admin:
admin:utils service restart Cisco Tomcat
Don't press Ctrl-c while the service is getting RESTARTED.If Service has not Restarted Properly, execute the same Command Again
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
admin:
```

Verificar

Faça login em <http://<fqdnofccm>:8443/ccmadmin> para garantir que o novo certificado seja usado.



Certificado SAN de vários servidores do CallManager

Um procedimento semelhante pode ser seguido para o certificado do CallManager. Nesse caso, os domínios preenchidos automaticamente são apenas nós do CallManager. Se o serviço Cisco CallManager não estiver em execução, você poderá optar por mantê-lo na lista de SANs ou

removê-lo.

 Aviso: esse processo afeta o registro e o processamento de chamadas do telefone. Certifique-se de agendar uma janela de manutenção para qualquer trabalho com certificados CUCM/TVS/ITL/CAPF.

Antes do certificado SAN assinado pela CA para o CUCM, verifique se:

- O Telefone IP pode confiar no Serviço de Verificação de Confiança (TVS). Isso pode ser verificado com acesso a qualquer serviço HTTPS do telefone. Por exemplo, se o acesso ao diretório corporativo funcionar, significa que o telefone confia no serviço TVS.
- Verifique se o cluster está no Modo Não Seguro ou no Modo Misto.

Para determinar se é um cluster de modo misto, escolha Cisco Unified CM Administration > System > Enterprise Parameters > Cluster Security Mode (0 == Non-Secure; 1 == Mixed Mode).

 Aviso: se você estiver em um Cluster de Modo Misto antes de os serviços serem reiniciados, a lista de certificados confiáveis deverá ser atualizada: [Token](#) ou [Sem Tokens](#).

Após instalar o certificado emitido pela CA, a próxima lista de serviços deverá ser reiniciada nos nós habilitados:

- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos > Cisco TFTP
- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos > Cisco CallManager
- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de recursos > Cisco CTIManager
- Cisco Unified Serviceability > Ferramentas > Centro de controle - Serviços de rede > Cisco Trust Verification Service

Troubleshooting

Esses registros podem ajudar o Centro de assistência técnica da Cisco a identificar qualquer problema relacionado à geração de CSR SAN de vários servidores e ao upload do certificado assinado pela CA.

- API da plataforma Cisco Unified OS
- Cisco Tomcat
- Logs CertMgr da Plataforma IPT
- [Processo de renovação de certificado](#)

Caveats conhecidos

• ID de bug da Cisco [CSCur97909](#) - O carregamento de certificado de multiservidor não exclui certificados autoassinados no BD

- ID de bug Cisco [CSCus47235](#) - CUCM 10.5.2 não pode ser duplicado em SAN para CSR
- ID de bug da Cisco [CSCup28852](#) - redefinição de telefone a cada 7min devido à atualização de certificado quando você usa o certificado de multiservidor

Se houver um Certificado Multiservidor existente, a regeneração é recomendada nestes cenários:

- Alteração de nome de host ou domínio. Quando uma alteração de nome de host ou domínio é executada, os certificados são gerados novamente automaticamente como Autoassinados. Para alterá-lo para um CA-Signed as etapas anteriores devem ser seguidas.
- Se um novo nó tiver sido adicionado ao cluster, um novo CSR deverá ser gerado para incluir o novo nó.
- Quando um assinante é restaurado e nenhum backup é usado, o nó pode ter novos certificados Autoassinados. Um novo CSR para o cluster completo pode ser exigido para incluir o assinante. (Há uma solicitação de aprimoramentoID de bug da Cisco [CSCuv75957](#) para adicionar esse recurso.)

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.