Regenerar certificados autoassinados do serviço CUCM IM/P

Contents

Introdução

Este documento descreve um procedimento passo a passo recomendado sobre como gerar novamente certificados no CUCM IM/P 8.x e posterior.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento dos certificados do Serviço IM & Presence (IM/P).

Componentes Utilizados

As informações neste documento são baseadas no IM/P versão 8.x e posterior.

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

Utilização do Repositório de Certificados

Certificado Cisco Unified Presence (CUP)

Usado para conexões SIP seguras para Federação SIP, Controle de Chamada Remota da Microsoft para Lync/OCS/LCS, conexão segura entre o Cisco Unified Certificate Manager (CUCM) e IM/P e assim por diante.

Cisco Unified Presence - Certificado de Protocolo extensível de mensagens e presença (CUP-XMPP)

Usado para validar conexões seguras para clientes XMPP quando uma sessão XMPP é criada.

Cisco Unified Presence - Protocolo extensível de mensagens e presença - Certificado de servidor para servidor (CUP-XMPP-S2S)

Usado para validar conexões seguras para federações entre domínios XMPP com um sistema XMPP federado externamente.

Certificado de segurança IP (IPSec)

Usado para:
· Validar conexão segura para o Sistema de Recuperação de Desastres (DRS)/Estrutura de Recuperação de Desastres (DRF)
· Validar a conexão segura de túneis IPsec para o Cisco Unified Communications Manager (CUCM) e nós IM/P no cluster

Certificado Tomcat

Usado para:

· Validar vários acessos à Web, como acesso a páginas de serviço de outros nós no cluster e Acesso Jabber.
· Validar conexão segura para SSO (Logon Único SAML).

· Validar conexão segura para o Intercluster Peer.

Cuidado: se você usar o recurso SSO em seus servidores Unified Communication e os certificados Cisco Tomcat forem gerados novamente, o SSO deverá ser reconfigurado com os novos certificados. O link para configurar o SSO no CUCM e no ADFS 2.0 é: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/211302-Configure-Single-Sign-On-using-CUCM-and.html.

Observação: o link para o processo de renovação/regeneração de certificado do CUCM é: https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-callmanager/200199-CUCM-Certificate-Regeneration-Renewal-Pr.html.

Processo de Regeneração de Certificado

Certificado CUP

Etapa 1. Abra uma Interface Gráfica do Usuário (GUI) para cada servidor do cluster. Comece com o editor de IM/P, abra uma GUI para cada servidor de assinantes IM/P e navegue até Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Comece com a GUI do editor e escolha Find mostrar todos os certificados. Escolha o cup.pem certificado. Uma vez aberto, escolha Regenerate e aguarde até que você obtenha êxito antes que o pop-up seja fechado.

Etapa 3. Continue com os assinantes subsequentes, consulte o mesmo procedimento da Etapa 2 e conclua todos os assinantes em seu cluster.

Etapa 4. Depois que o certificado CUP tiver sido gerado novamente em todos os nós, os serviços devem ser reiniciados.

Observação: se a configuração do Grupo de Redundância de Presença tiver Habilitar Alta Disponibilidade marcada, Uncheck ela será exibida antes que os serviços sejam reiniciados. A configuração do Grupo de redundância de presença pode ser acessada em CUCM Pub Administration > System > Presence Redundancy Group. Uma reinicialização dos serviços causa uma interrupção temporária do IM/P e deve ser feita fora das horas de produção.

Reinicie os serviços nesta ordem:

· Faça login no Cisco Unified Serviceability do editor:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Serviço Proxy SIP da Restart Cisco.

c. Quando a reinicialização do serviço for concluída, continue com os assinantes e com o serviço Proxy SIP da CiscoRestart.

d. Comece com o editor e continue com os assinantes. Restart Serviço Cisco SIP Proxy (também, de Cisco Unified Serviceability > Tools > Control Center - Feature Services).

· Faça login no Cisco Unified Serviceability do editor:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart Serviço Cisco Presence Engine.

Restart c. Quando a reinicialização do serviço for concluída, continue com o Cisco Presence Engine Service nos assinantes.

Observação: se configurado para Federação SIP, o serviçoRestart Gerenciador de Conexões de Federação SIP do Cisco XCP (localizado em Cisco Unified Serviceability > Tools > Control Center - Feature Services). Comece com o editor e continue com os assinantes.

Certificado CUP-XMPP

Nota: como o Jabber utiliza os certificados de servidor CUCM e IM/P Tomcat e CUP-XMPP para validar as conexões para serviços Tomcat e CUP-XMPP, esses certificados CUCM e IM/P são, na maioria dos casos, assinados pela CA. Suponha que o dispositivo Jabber não tenha a raiz e um certificado intermediário que faça parte do certificado CUP-XMPP instalado em seu armazenamento de

---

certificado confiável, nesse caso, o cliente Jabber exibe um pop-up de aviso de segurança para o certificado não confiável. Se ainda não estiver instalado no certificado do armazenamento confiável do dispositivo Jabber, a raiz e qualquer certificado intermediário devem ser enviados para o dispositivo Jabber por meio da política de grupo, MDM, e-mail e assim por diante, que depende do cliente Jabber.

Nota: Se o certificado CUP-XMMP for autoassinado, o cliente Jabber exibirá um pop-up de aviso de segurança para o certificado não confiável se o certificado CUP-XMPP não estiver instalado no armazenamento confiável do certificado do dispositivo Jabber. Se ainda não estiver instalado, o certificado CUP-XMPP autoassinado deve ser enviado para o dispositivo Jabber através da política de grupo, MDM, e-mail, etc, que depende do cliente Jabber.

Etapa 1. Abra uma GUI para cada servidor do cluster. Comece com o editor de IM/P, abra uma GUI para cada servidor de assinantes IM/P e navegue até **Cisco Unified OS Administration > Security > Certificate Management**.

Etapa 2. Comece com a GUI do editor e escolha Find mostrar todos os certificados. Na coluna de tipo do cup-xmpp.pem certificado, determine se ele é autoassinado ou CA-assinado. Se o cup-xmpp.pem certificado for uma multisSAN de distribuição com assinatura de terceiros (tipo com assinatura CA), revise esse link quando gerar um CSR CUP-XMPP multisSAN e envie para a CA para o certificado CUP-XMPP com assinatura CA; Exemplo de Configuração de Cluster de Comunicação Unificada com Nome Alternativo de Entidade de Multiservidor com Assinatura CA.

Se o cup-xmpp.pem certificado for um nó único de distribuição assinado por terceiros (tipo assinado pela CA) (o nome da distribuição é igual ao nome comum do certificado), revise esse link quando gerar um CUP-XMPP CSR de nó único e envie para a CA para o certificado CUP-XMPP assinado pela CA; Guia de Instruções do Jabber para Validação de Certificado. Se o cup-xmpp.pem certificado for autoassinado, continue na etapa 3.

Etapa 3. Escolha Find para mostrar todos os certificados e, em seguida, escolha o certificadocup-xmpp.pem. Uma vez aberto, escolha Regenerate e aguarde até que você obtenha êxito antes que o pop-up seja fechado.

Etapa 4. Continue com os assinantes subsequentes; consulte o mesmo procedimento na Etapa 2 e conclua-o para todos os assinantes em seu cluster.

Etapa 5. Após a regeneração do certificado CUP-XMPP em todos os nós, o serviço do roteador Cisco XCP deve ser reiniciado nos nós IM/P.

Observação: se a Configuração do Grupo de Redundância de Presença tiver Habilitar Alta Disponibilidade marcada, Uncheck isso será feito antes que o serviço seja reiniciado. A Configuração do grupo de redundância de presença pode ser acessada em CUCM Pub Administration > System > Presence Redundancy Group. Uma reinicialização do serviço causa uma interrupção temporária do IM/P e deve ser feita fora das horas de produção.

· Faça login no Cisco Unified Serviceability do editor:

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.

b. Restart o serviço Roteador Cisco XCP.

c. Quando a reinicialização do serviço for concluída, continue com Restart o serviço Cisco XCP Router nos assinantes.

Certificado CUP-XMPP-S2S

Etapa 1. Abra uma GUI para cada servidor do cluster. Comece com o editor de IM/P, abra uma GUI para cada servidor de assinantes de IM/P e

navegue até Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Comece com a GUI do editor, escolha Find mostrar todos os certificados e escolha o certificadocup-xmpp-s2s.pem. Uma vez aberto, escolha Regenerate e aguarde até que você obtenha êxito antes que o pop-up seja fechado.

Etapa 3. Continue com os assinantes subsequentes e consulte o mesmo procedimento na Etapa 2, e complete para todos os assinantes em seu cluster.

Etapa 4. Após a regeneração do certificado CUP-XMPP-S2S em todos os nós, os serviços devem ser reiniciados na ordem mencionada.

Observação: se a Configuração do Grupo de Redundância de Presença tiver a opção Habilitar Alta Disponibilidade marcada,Uncheck esta opção antes que esses serviços sejam reiniciados. A Configuração do Grupo de Redundância de Presença pode ser acessada em CUCM Pub Administration > System > Presence Redundancy Group. Uma reinicialização dos serviços causa uma interrupção temporária do IM/P e deve ser feita fora das horas de produção.

· Faça login no Cisco Unified Serviceability do editor:

a. Cisco Unified Serviceability > Tools > Control Center - Network Services.
b. Restart o serviço Roteador Cisco XCP.
c. Quando a reinicialização do serviço for concluída, continue com Restart o serviço Roteador Cisco XCP nos assinantes.

· Faça login no Cisco Unified Serviceability do editor:

a. Cisco Unified Serviceability > Tools > Control Center - Feature Services.

b. Restart o serviço Cisco XCP XMPP Federation Connection Manager.

c. Quando a reinicialização do serviço for concluída, continue com Restart o serviço Cisco XCP XMPP Federation Connection Manager nos assinantes.

Certificado IPSec

Observação: o ipsec.pem certificado no editor do CUCM deve ser válido e estar presente em todos os assinantes (nós CUCM e IM/P) no armazenamento confiável IPSec. O ipsec.pem certificado do assinante não está presente no publicador como o armazenamento confiável IPSec em uma implantação padrão. Para verificar a validade, compare os números de série no ipsec.pem certificado do CUCM-PUB com o IPSec-trust nos assinantes. Eles devem coincidir.

Observação: o DRS usa uma comunicação baseada em Secure Socket Layer (SSL) entre o Agente de Origem e o Agente Local para autenticação e criptografia de dados entre os nós de cluster CUCM (nós CUCM e IM/P). O DRS usa os certificados IPSec para sua criptografia de chave pública/privada. Lembre-se de que se você excluir o arquivo de armazenamento confiável (hostname.pem) IPSEC da página Gerenciamento de certificados, o DRS não funcionará como esperado. Se você excluir o arquivo de confiança IPSEC manualmente, certifique-se de carregar o certificado IPSEC no armazenamento de confiança IPSEC. Para obter mais detalhes, consulte a página de ajuda do gerenciamento de certificados nos Guias de segurança do CUCM.

Etapa 1. Abra uma GUI para cada servidor do cluster. Comece com o editor de IM/P, abra uma GUI para cada servidor de assinantes de IM/P e navegue até Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Comece com a GUI do editor e escolha Find mostrar todos os certificados.Choose o certificadoipsec.pem. Uma vez aberto, escolha Regenerate e aguarde até que você obtenha êxito antes que o pop-up seja fechado.

Etapa 3. Continue com os assinantes subsequentes e consulte o mesmo procedimento na Etapa 2, e complete para todos os assinantes em seu cluster.

Etapa 4. Depois que todos os nós tiverem gerado novamente o certificado IPSEC, então Restart esses serviços. Navegue até o Cisco Unified Serviceability do editor; Cisco Unified Serviceability > Tools > Control Center - Network Services.
a. Escolha Restart no serviço principal do Cisco DRF.
b. Quando a reinicialização do serviço for concluída, escolha Restart o serviço Cisco DRF Local no editor e continue com Restart o serviço Cisco DRF Local em cada assinante.

Certificado Tomcat

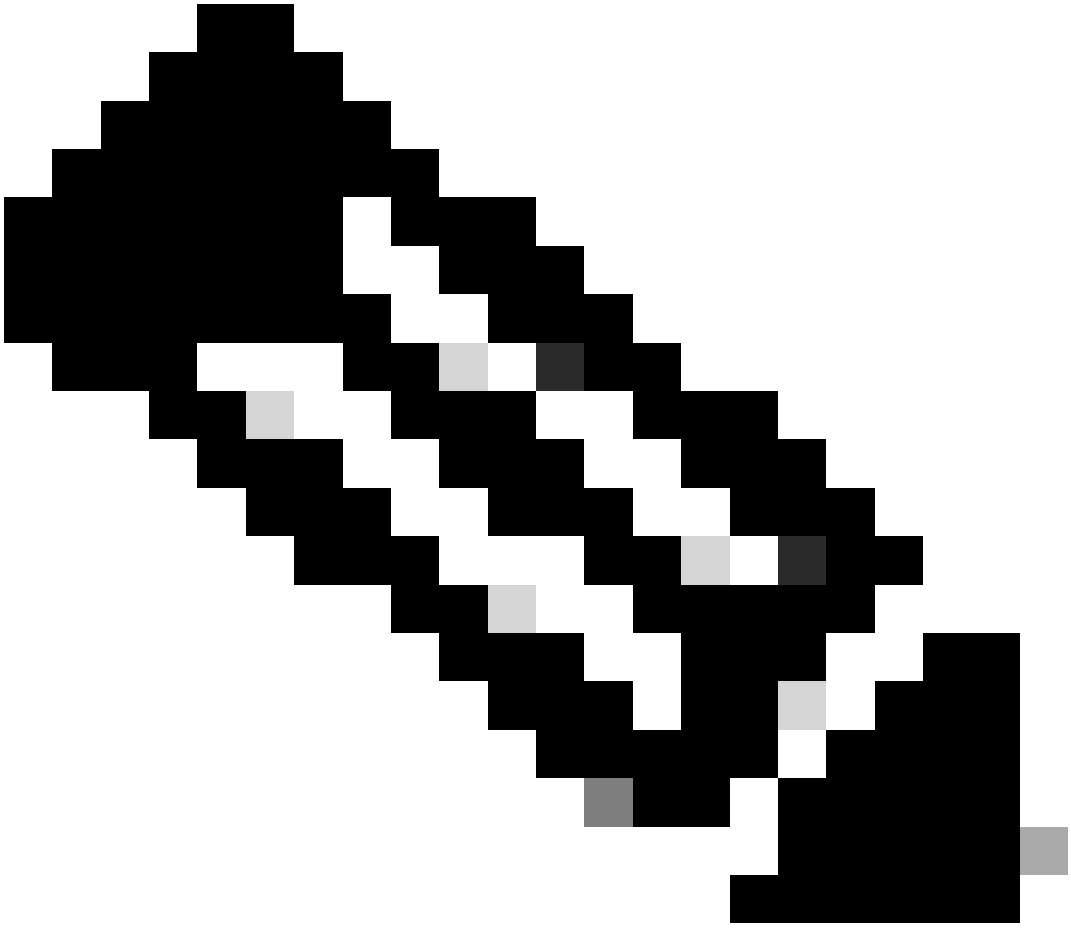
Nota: como o Jabber utiliza os certificados de servidor CUCM Tomcat e IM/P Tomcat e CUP-XMPP para validar as conexões para serviços Tomcat e CUP-XMPP, esses certificados CUCM e IM/P são, na maioria dos casos, assinados pela CA. Suponha que o dispositivo Jabber não tenha a raiz e nenhum certificado intermediário que faça parte do certificado Tomcat instalado em seu armazenamento de confiança de certificado. Nesse caso, o cliente Jabber exibe um pop-up de aviso de segurança para o certificado não confiável. Se ainda não estiver instalado no armazenamento confiável de certificados do dispositivo Jabber, a raiz e qualquer certificado intermediário devem ser enviados para o dispositivo Jabber por meio da política de grupo, MDM, e-mail e assim por diante, que depende do cliente Jabber.

Nota: se o certificado Tomcat for autoassinado, o cliente Jabber exibirá um pop-up de aviso de segurança para o certificado não confiável, se o certificado Tomcat não estiver instalado no armazenamento confiável de certificados do dispositivo Jabber. Se ainda não estiver instalado no armazenamento confiável de certificados do dispositivo Jabber, o certificado CUP-XMPP autoassinado deve ser enviado para o dispositivo Jabber através da política de grupo, MDM, e-mail e assim por diante, que depende do cliente Jabber.

Etapa 1. Abra uma GUI para cada servidor do cluster. Comece com o editor de IM/P, abra uma GUI para cada servidor de assinantes IM/P e navegue até Cisco Unified OS Administration > Security > Certificate Management.

Etapa 2. Comece com a GUI do editor e escolha Find mostrar todos os certificados.
· Na coluna Tipo do certificadotomcat.pem, determine se ele é autoassinado ou CA-assinado.

· Se o certificadotomcat.pem for uma multisSAN de distribuição assinada por terceiros (tipo assinado pela CA), revise este link sobre como gerar um CSR Tomcat multisSAN e envie para a CA um certificado Tomcat assinado pela CA, Exemplo de Configuração de Cluster de Comunicação Unificada com Nome Alternativo de Entidade de Multiservidor Assinado pela CA



Observação: o CSR do Tomcat de várias SANs é gerado no editor do CUCM e é distribuído para todos os nós do CUCM e IM/P no cluster.

· Se o tomcat.pem certificado for um nó único de distribuição assinado por terceiros (tipo assinado pela CA) (o nome da distribuição é igual ao nome comum do certificado), revise este link para gerar um CSR CUP-XMPP de nó único e envie-o à CA para o certificado CUP-XMPP assinado pela CA, Guia de Instruções do Jabber para Validação de Certificado

· Se o tomcat.pem certificado for autoassinado, continue na Etapa 3

Etapa 3. Escolha Find para mostrar todos os certificados:

· Escolha o tomcat.pem certificado.

· Uma vez aberto, escolha Regenerate e aguarde até ver o pop-up de sucesso antes de fechar o pop-up.

Etapa 4. Continue com cada assinante subsequente, consulte o procedimento na Etapa 2 e conclua todos os assinantes em seu cluster.

Etapa 5. Depois que todos os nós tiverem gerado novamente o certificado Tomcat, Restart o serviço Tomcat em todos os nós. Comece com o editor, seguido pelos assinantes.

· ParaRestart executar o serviço Tomcat, você deve abrir uma sessão CLI para cada nó e executar o comando até que o serviço reinicie o Cisco Tomcat, como mostrado na imagem:

```
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:
```

Excluir Certificados de Confiança Expirados

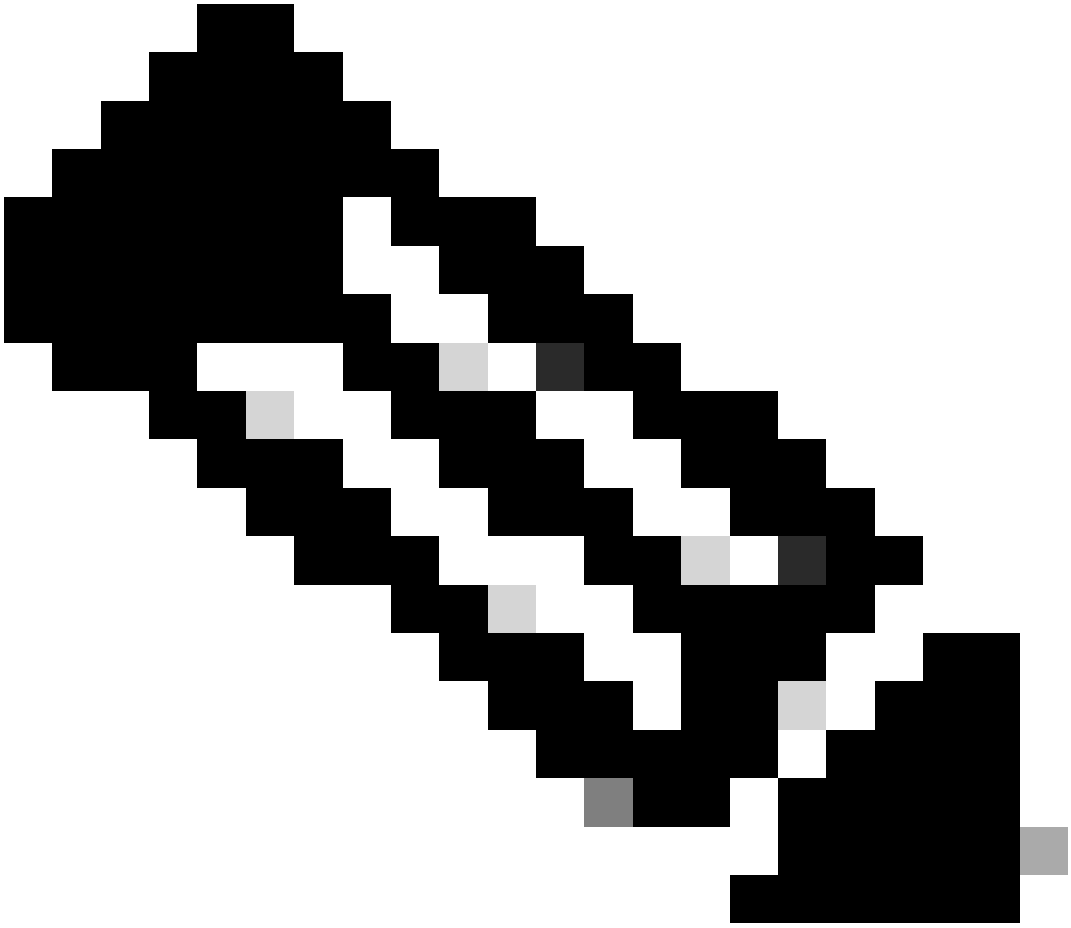
Observação: certificados confiáveis (que terminam em confiança) podem ser excluídos quando apropriado. Os certificados confiáveis que podem ser excluídos são aqueles que não são mais necessários, expiraram ou estão obsoletos. Não exclua os cinco certificados de identidade: cup.pem , cup-xmpp.pem , cup-xmpp-s2s.pem , ipsec.pem e tomcat.pem certificados. As reinicializações do serviço, como mostrado, são projetadas para limpar qualquer informação na memória desses certificados herdados dentro desses serviços.

Observação: se a Configuração do Grupo de Redundância de Presença tiver Habilitar Alta Disponibilidade marcada, Uncheck isso antes de um serviço ser Stopped/Started ou Restarted. A Configuração do grupo de redundância de presença pode ser acessada em CUCM Pub Administration > System > Presence Redundancy Group. A reinicialização de alguns dos serviços, como mostrado, causa uma interrupção temporária do IM/P e deve ser feita fora das horas de produção.

Etapa 1. Navegue até:Cisco Unified Serviceability > Tools > Control Center - Network Services

· No menu suspenso, escolha seu editor de IM/P, escolha Stop no Cisco Certificate Expiry Monitor, seguido por Stop no Cisco Intercluster Sync Agent.

· RepitaStop esses serviços para cada nó IM/P no cluster.



Observação: se o certificado Tomcat-trust precisar ser excluído, navegue até Cisco Unified Serviceability > Tools > Control Center - Network Services o editor do CUCM.

· No menu suspenso, escolha o editor do CUCM.

· Escolha Stop no Cisco Certificate Expiry Monitor, seguido por Stop em Cisco Certificate Change Notification.

· Repita o procedimento para cada nó do CUCM no cluster.

Etapa 2. Navegue até Cisco Unified OS Administration > Security > Certificate Management > Find.

· Localizar os certificados confiáveis expirados (para versões 10.x e posteriores, você pode filtrar por Expiração. Nas versões anteriores à 10.0, você deve identificar os certificados específicos manualmente ou por meio dos alertas RTMT (se recebidos).

· O mesmo certificado confiável pode aparecer em vários nós, ele deve ser excluído individualmente de cada nó.

· Escolha o certificado confiável a ser excluído (com base na versão, você receberá um pop-up ou será direcionado para o certificado na mesma página).

· Escolha Delete (você receberá um pop-up que começa com "você está prestes a excluir permanentemente este certificado...").
· Clique OK.

Etapa 3. Repita o processo para cada certificado de confiança a ser excluído.

Etapa 4. Após a conclusão, os serviços que estão diretamente relacionados aos certificados devem ser reiniciados e excluídos.

· CUP-trust: Cisco SIP Proxy, Cisco Presence Engine e, se configurado para Federação SIP, Cisco XCP SIP Federation Connection Manager (consulte a seção Certificado CUP)
· CUP-XMPP-trust: Roteador Cisco XCP (consulte a seção do certificado CUP-XMPP)
· CUP-XMPP-S2S-trust: roteador Cisco XCP e Cisco XCP XMPP Federation Connection Manager
· IPSec-trust: DRF Source/DRF Local (consulte a seção Certificado IPSec)
· Tomcat-trust: reinicie o serviço Tomcat por meio da linha de comando (consulte a seção Certificado Tomcat)

Etapa 5. Reinicie os serviços interrompidos na Etapa 1.

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

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.