Processo da regeneração do certificado para o gerente das comunicações unificadas de Cisco (CUCM)

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Informações de Apoio
Instale RTMT
Monitore valores-limite com RTMT
Identifique se seu conjunto reage do Misturado-MODE ou o modo NON-seguro
Impacte pela loja do certificado
CallManager.pem
Tomcat.pem
CAPF.pem
IPSec.pem
TVS (Trust Verification Service)
ITL e CTL
Processo da regeneração do certificado
Certificado de Tomcat
  Certificado do IPSEC
Certificado CAPF
Certificado do CallManager
Certificado TV
Certificado de ITLRecovery
A supressão expirou Certificados de confiança
Verificar
Troubleshooting

Introdução

Este documento fornece um procedimento passo a passo recomendado em como regenerar Certificados na liberação 8.X do gerente das comunicações unificadas de Cisco (CUCM) e mais altamente. Este processo não usa a reserva às versões antes da funcionalidade 8.0 e atualiza Certificados pela função. A Segurança caracteriza à revelia é a lista da confiança da identidade (ITL) e a característica Misturado-MODE é o certificate trust list (CTL) é endereçada a fim evitar edições do registro.

Contribuído por Ken Ryder, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta do monitoramento em tempo real (RTMT)
- Certificados CUCM

Componentes Utilizados

- Liberação 8.X CUCM e mais altamente

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

Instale RTMT

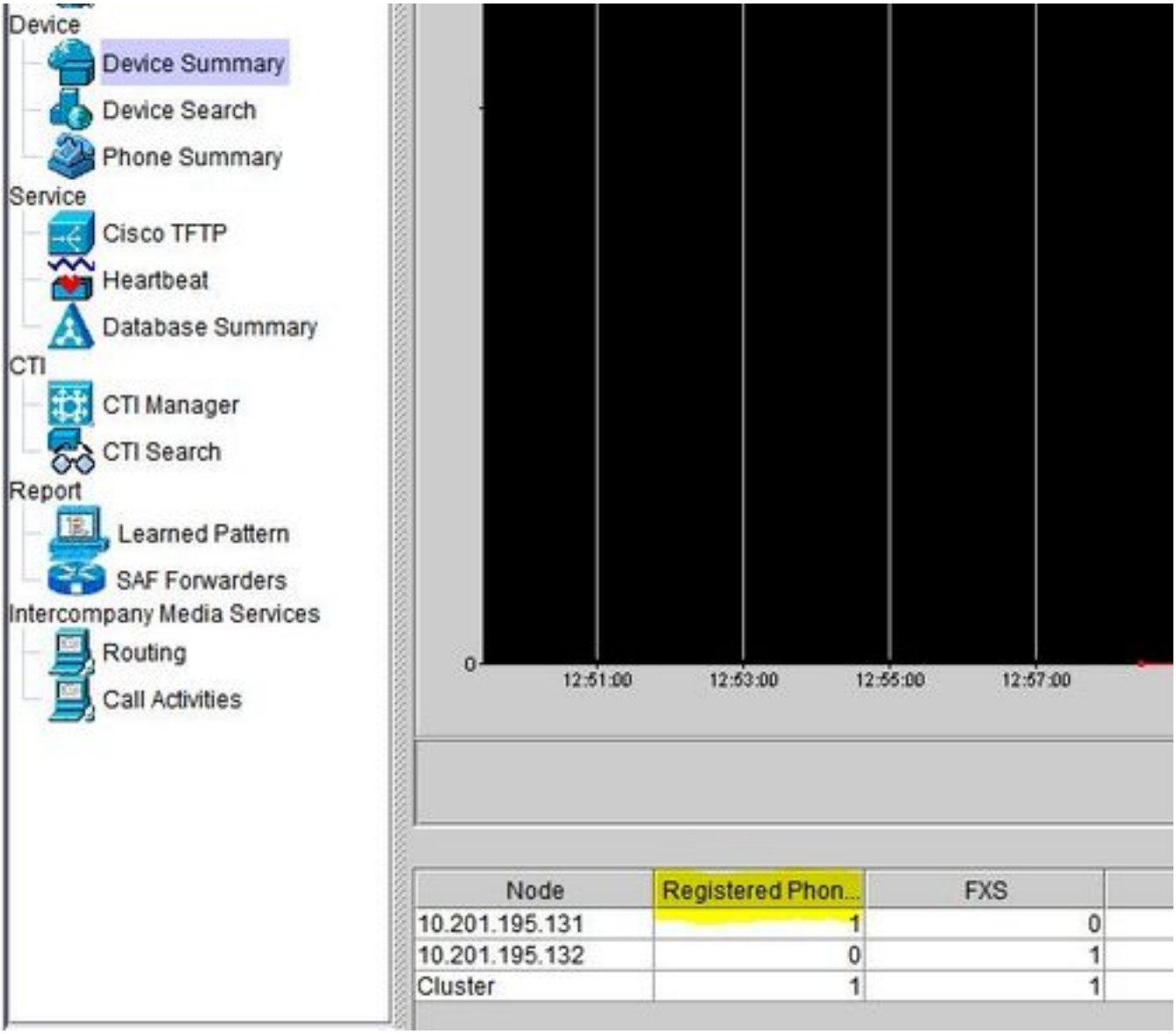
- Transfira e instale a ferramenta RTMT do gerenciador de chamada Navegue à administração do gerenciador de chamada (CM)**O aplicativo > os encaixes > o achado > Cisco unificaram a ferramenta do monitoramento em tempo real - Windows > transferência** Instale e lance

Monitore valores-limite com RTMT

- Lance RTMT e incorpore o endereço IP de Um ou Mais Servidores Cisco ICM NT ou o nome de domínio totalmente qualificado (FQDN), nome de usuário e senha para alcançar então a ferramenta Selecione a **Voz/aba video**Selecione o **sumário do dispositivo** Esta seção identifica o número total de valores-limite registrados e quanto a cada nóMonitore quando restauração do valor-limite para assegurar o registro antes da regeneração do certificado seguinte

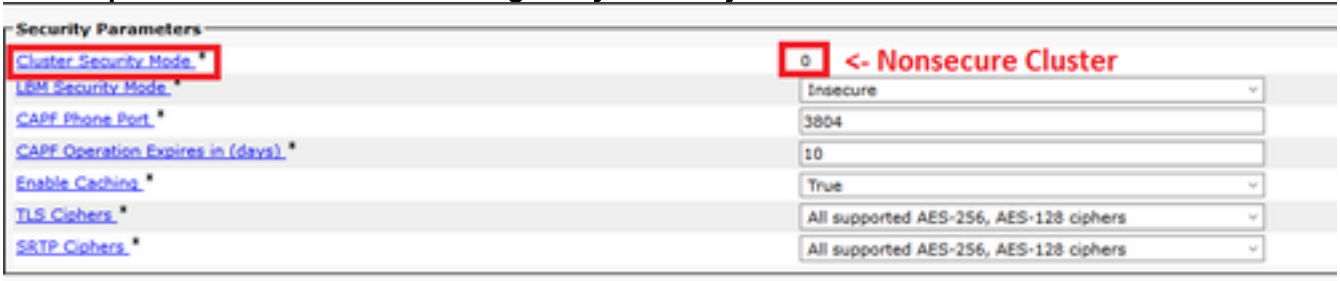
  Dica: O processo da regeneração de alguns Certificados pode impactar o valor-limite. Considere um plano de ação após as horas de negócio regulares devido à exigência reiniciar serviços e recarregar telefones. Monitorar o registro do telefone através de RTMT é altamente recomendado.

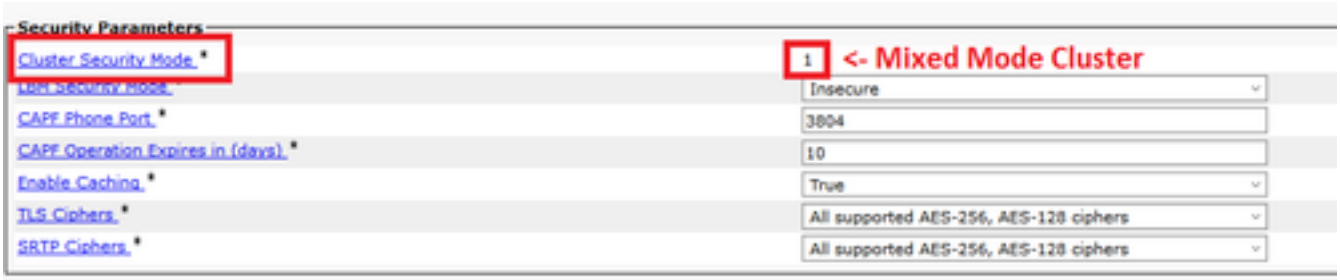
  aviso: Os valores-limite com má combinação atual ITL podem ter edições do registro após este processo. O supressão da ITL no valor-limite é uma solução típica do melhor prática após o processo da regeneração é terminado e todos telefones restantes registraram-se.



Identifique se seu conjunto reage do Misturado-MODE ou o modo NON-seguro

- Navegue à administração CM **Parâmetros do > segurança do sistema > parâmetros de empreendimento > modo de segurança do conjunto**





Impacto pela loja do certificado

Éessencial para uma boa funcionalidade do sistema ter todos os certificados atualizados no cluster CUCM. Se os Certificados são expirados ou inválido puderam significativamente afetar a funcionalidade normal do sistema. Uma lista de serviços para os Certificados específicos que são inválidos ou expirados é mostrada aqui. O impacto pode diferir dependendo da configuração do sistema.

CallManager.pem

- Telefones cifrados/autenticados não se registram
- O Trivial File Transfer Protocol (TFTP) não é confiado (os telefones não aceitam arquivos de configuração assinados e/ou arquivos ITL)
- Os serviços de telefone puderam ser afetados
- Os troncos do Session Initiation Protocol (SIP) ou os recursos de mídia seguros (bridges de conferência, Media Termination Point (MTP), Xcoders, e assim por diante) não se registram nem trabalham-se.
- A solicitação AXL falhará.

Tomcat.pem

- Os telefones não podem alcançar os serviços HTTP hospedados no nó CUCM, tal como o diretório corporativo
- CUCM pode ter várias edições de Web, tais como incapaz de alcançar páginas do serviço de outros Nós no conjunto
- Edições transversais do conjunto da mobilidade de extensão (EM) ou da mobilidade de extensão
- Escolha Sinal-em (o SSO)

CAPF.pem

- Os telefones não autenticam para o telefone VPN, o 802.1x, ou o proxy do telefone
- Não pode emitir localmente - Certificados significativos do certificado (LSC) para os telefones.
- Os arquivos de configuração cifrados não funcionam

IPSec.pem

- A estrutura da recuperação do sistema da Recuperação de desastres (DR) /Disaster (DRF) não pôde funcionar corretamente
- Os túneis de IPsec ao gateway (GW) a outros conjuntos CUCM não funcionam

TVS (Trust Verification Service)

O serviço da verificação da confiança (TV) é o componente principal da Segurança à revelia. Os TV permitem Telefones IP unificados Cisco de autenticar serveres de aplicativo, tais como serviços EM, diretório, e MIDlet, quando o HTTPS é estabelecido.

Os TV fornecem as características como segue:

- Escalabilidade - Cisco unificou recursos do telefone IP não é impactado pelo número de Certificados para confiar
- Flexibilidade - A adição ou a remoção de Certificados de confiança são refletidas automaticamente no sistema
- Segurança à revelia - os recursos de segurança dos NON-media e do sinal são parte da instalação padrão e não exigem a intervenção de usuário

ITL e CTL

- A ITL contém o papel do certificado para o gerenciador de chamada TFTP, todos os Certificados TV no conjunto, e função do proxy do Certificate Authority (CAPF) quando foi executado
- O CTL contém entradas para o token de segurança do administrador de sistema (SAST), CallManager da Cisco e os serviços TFTP de Cisco que são foram executado no mesmo server, em server CAPF, TFTP, e no Firewall adaptável da ferramenta de segurança (ASA). Os TV não são providos no CTL

Processo da regeneração do certificado

Certificado de Tomcat

Identifique se os Certificados da terceira parte estão no uso.

1. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, seguido por cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS** Observe da coluna da descrição se Tomcat indica o certificado auto-assinado gerado pelo sistema. Se Tomcat é terceira parte assinada, siga o link fornecido e execute aquelas etapas após a regeneração de TomcatCertificados assinados da terceira parte - DOC-6119
2. Selecione o **achado** a fim mostrar todos os Certificados Selecione o certificado **PEM de Tomcat**Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
3. Continue com cada subscritor subsequente, siga o mesmo procedimento em etapa 2 e termine-o em todos os assinantes em seu conjunto
4. Afinal os Nós regeneraram o certificado de Tomcat, reiniciam o serviço de TomCat em todos os Nós. Comece com o editor a seguir seguido pelos assinantes. A fim reiniciar Tomcat que você precisa de abrir uma sessão CLI para cada nó e de executar o **reinício Cisco Tomcat do serviço dos utils do** comando

```
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:
```

Certificado do IPSEC

Nota: Mensagem CUCM/Instant e presença (IM&P) antes de version10.X as corridas do agente principal DRF no editor CUCM e no editor IM&P. Corridas do serviço local DRF nos assinantes respectivamente. As versões 10.X e mais recente, do agente principal DRF corridas no editor CUCM somente e serviço local DRF estarão em assinantes CUCM e em publisher e subscriber IM&P.

Nota: O sistema da Recuperação de desastres usa uma comunicação baseada Secure Socket Layer (SSL) entre o agente principal e o agente local para a autenticação e a criptografia dos dados entre os nós de cluster CUCM. Os DR utilizam os Certificados do IPsec para seus público/criptografia chave privada. Esteja ciente que se você suprime do arquivo do truststore do IPSEC (hostname.pem) da página do gerenciamento certificado, a seguir os DR não trabalharão como esperado. Se você suprime do arquivo da IPsec-confiança manualmente, a seguir você deve assegurar-se de que você transfira arquivos pela rede o certificado do IPSEC ao truststore do IPSEC. Para mais detalhes, refira a página da ajuda do gerenciamento certificado nos guias da Segurança do gerente das comunicações unificadas de Cisco.

1. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, seguido por cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS** Selecione o certificado **PEM do IPSEC**.Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
2. Continue com assinantes subsequentes; siga o mesmo procedimento em etapa 1 e termine-o em todos os assinantes em seu conjunto
3. Afinal os Nós regeneraram o certificado do IPSEC a seguir reiniciam serviços. Navegue à **utilidade unificada Cisco do** editor **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de rede**Selecione o **reinício no** serviço do **mestre de Cisco DRF**Uma vez que o reinício do serviço termina, o **reinício** seleto no **serviço local de Cisco DRF no** editor a seguir continua com os assinantes e seleciona o **reinício no serviço local de Cisco DRF**

O certificado IPSEC.pem no editor deve ser válido e deve esta presente em todos os assinantes como truststores do IPSEC. Os assinantes o certificado IPSEC.pem que não estam presente no editor como o truststore do IPSEC em um desenvolvimento padrão. A fim verificar a validez compare os números de série no certificado IPSEC.pem do BAR com o IPSEC - confie nos sub. Devem combinar.

Certificado CAPF

aviso: Assegure-se de que você identifique se seu conjunto está no Misturado-MODE antes que você continue. Refira a seção **identificam se seu conjunto reage do Mistura-MODE ou o modo NON-seguro.**

1. Navegue à **administração unificada Cisco > ao sistema > parâmetros de empreendimento CM**.
   Verifique os parâmetros de segurança da seção e verifique se o modo de segurança do

conjunto é ajustado a 0 ou a 1. Se o valor se 0 então o conjunto reagem do modo NON-seguro. Se é 1 então que o conjunto está no misturado-MODE e você precisará de atualizar o arquivo CTL antes do reinício dos serviços. Veja os links do token e do Tokenless abaixo.

2. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, então cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS**
   Selecione o certificado **PEM CAPF**.Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
3. Continue com assinantes subsequentes; siga o mesmo procedimento em etapa 2 e termine-o em todos os assinantes em seu conjunto Se o conjunto está no Misturado-MODE SOMENTE e o CAPF foi – atualize o CTL antes que você continue um token mais adicional - Tokenless regeneradoSe o conjunto reage de modo misturado então o serviço do gerenciador de chamada igualmente deverá ser reiniciado antes do reinício dos outros serviços
4. Afinal os Nós regeneraram o certificado CAPF, serviços do reinício
   Navegue à **utilidade unificada Cisco do** editor **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços da característica**Comece com o editor e selecione o **reinício no serviço da função do proxy do Certificate Authority de Cisco** somente onde sendo executado
5. Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de rede** Comece com o editor a seguir continue com os assinantes, **reinício** seleto no **serviço da verificação da confiança de Cisco**Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços da característica**Comece com o editor a seguir continue com os assinantes, **serviço TFTP de Cisco do** reinício somente onde sendo executado.
6. Recarregue todos os telefones **Cisco unificou a administração > o sistema > parâmetros de empreendimento CMRestauração** seleta então você verá um PNF-acima com a indicação que **você está a ponto de restaurar todos os dispositivos no sistema. Esta ação não pode ser desabotoada. Continue? ,** selecione **ESTÁ BEM** e selecione então a **restauração**

Os telefones restaurarão agora. Monitore suas ações através da ferramenta RTMT para assegurar-se de que a restauração seja bem sucedida e que os dispositivos se registram de volta a CUCM. Espera para que o registro do telefone termine antes que você continuar ao certificado seguinte. Este processo de registro dos telefones pode tomar alguma hora. Seja recomendado, os dispositivos que tiveram ITLs ruim antes do processo da regeneração não puderam se registrar de volta ao conjunto.

Certificado do CallManager

aviso: Assegure-se de que você identifique se seu conjunto está no Misturado-MODE antes que você continue. Refira a seção **identificam se seu conjunto reage do Mistura-MODE ou o modo NON-seguro.**

aviso: Não regenere Certificados CallManager.PEM e TVS.PEM ao mesmo tempo. Isto causará uma má combinação unrecoverable à ITL instalada nos valores-limite que exigirão a remoção a ITL de TODOS OS valores-limite no conjunto.

1. Navegue à **administração unificada Cisco > ao sistema > parâmetros de empreendimento CM**. Verifique os parâmetros de segurança da seção e verifique se o modo de segurança do

conjunto é ajustado a 0 ou a 1. Se o valor se 0 então o conjunto reagem do modo NON-seguro. Se é 1 então que o conjunto está no misturado-MODE e você precisará de atualizar o arquivo CTL antes do reinício dos serviços. Veja os links do token e do Tokenless abaixo.

2. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, então cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS**
   Selecione o certificado **PEM do CallManager**.Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
3. Continue com assinantes subsequentes; siga o mesmo procedimento em etapa 2 e termine-o em todos os assinantes em seu conjunto. Se o conjunto está no Misturado-MODE SOMENTE e o CAPF foi – atualize o CTL antes que você continue um token mais adicional - Tokenless regenerado
4. O log em Cisco do editor unificou a utilidade Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços da característica**Comece com o editor a seguir continue com os assinantes, **serviço do CallManager da Cisco do** reinício onde sendo executado.
5. Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços da característica**
   Comece com o editor a seguir continue com os assinantes, **serviço do CTIManager de Cisco do** reinício somente onde sendo executado
6. Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de rede**
   Comece com o editor a seguir continue com os assinantes, reinício **Cisco confiam o serviço da verificação**
7. Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços da característica**
   Comece com o editor a seguir continue com os assinantes, **serviço TFTP de Cisco do** reinício somente onde sendo executado
8. Recarregue todos os telefones **Cisco unificou a administração > o sistema > parâmetros de empreendimento CMRestauração** seleta então você verá um PNF-acima com a indicação que **você está a ponto de restaurar todos os dispositivos no sistema. Esta ação não pode ser desabotoada. Continue? ,** selecione **ESTÁ BEM** e selecione então a **restauração**

Os telefones restaurarão agora. Monitore suas ações através da ferramenta RTMT para assegurar-se de que a restauração seja bem sucedida e que os dispositivos se registram de volta a CUCM. Espera para que o registro do telefone termine antes que você continuar ao certificado seguinte. Este processo de registro dos telefones pode tomar alguma hora. Seja recomendado, os dispositivos que tiveram ITLs ruim antes do processo da regeneração não puderam se registrar de volta ao conjunto.

Certificado TV

aviso: Não regenere Certificados CallManager.PEM e TVS.PEM ao mesmo tempo. Isto causará uma má combinação unrecoverable à ITL instalada nos valores-limite que exigirão a remoção a ITL de TODOS OS valores-limite no conjunto.

Nota: Os TV autenticam Certificados em nome do gerenciador de chamada. Regenere este último do certificado.

1. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, então cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS**
   Selecione o certificado **PEM TV**.Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
2. Continue com assinantes subsequentes; siga o mesmo procedimento em etapa 1 e termine-o em todos os assinantes em seu conjunto Afinal os Nós regeneraram o certificado TV, reiniciam os serviços: O log em **Cisco do** editor **unificou a utilidade** Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de redeNo reinício** seleto do editor em **Cisco confie o serviço da verificação**.Uma vez que o reinício do serviço termina, continue com os assinantes e reinicie o **serviço da verificação da confiança de Cisco**
3. Comece com o editor a seguir continue com os assinantes, **serviço TFTP de Cisco do** reinício somente onde sendo executado.
4. Recarregue todos os telefones **Cisco unificou a administração > o sistema > parâmetros de empreendimento CMRestauração** seleta então você verá um PNF-acima com a indicação que **você está a ponto de restaurar todos os dispositivos no sistema. Esta ação não pode ser desabotoada. Continue? ,** selecione **ESTÁ BEM** e selecione então a **restauração**

Os telefones restaurarão agora. Monitore suas ações através da ferramenta RTMT para assegurar-se de que a restauração seja bem sucedida e que os dispositivos se registram de volta a CUCM. Espera para que o registro do telefone termine antes que você continuar ao certificado seguinte. Este processo de registro dos telefones pode tomar alguma hora. Seja recomendado, os dispositivos que tiveram ITLs ruim antes do processo da regeneração não puderam se registrar de volta ao conjunto.

Certificado de ITLRecovery

Nota: O certificado de ITLRecovery é usado quando os dispositivos perdem seu estado confiado. O certificado aparece na ITL e no CTL (quando o fornecedor CTL é ativo).
Se os dispositivos perdem seu estado da confiança, você pode usar o **localkey da restauração ITL dos utils do** comando para conjuntos NON-seguros e o **localkey da restauração do ctl dos utils do** comando para os conjuntos mistura-MODE. Leia o guia da Segurança para que sua versão do gerenciador de chamada torne-se familiar com como o certificado de ITLRecovery é usado e o processo exigido para recuperar o estado confiado.
Se o conjunto esteve promovido a uma versão que apoie um comprimento chave de 2048 e os certificados de servidor dos conjuntos esteve regenerado a 2048 e o ITLRecovery não tem sido regenerado e está atualmente a uns 1024 comprimentos chaves, o comando de recuperação ITL falhará e o método de ITLRecovery não poderá ser usado.

1. Navegue a cada server em seu conjunto (em abas separadas de seu navegador da Web) começam com o editor, então cada subscritor. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS**
   Selecione o certificado **PEM de ITLRecovery**.Uma vez abra **regenerado** seleto e espere até que você ver o PNF-acima do sucesso a seguir o PNF-acima próximo ou vá para trás e selecione o **achado/lista**
2. Continue com assinantes subsequentes; siga o mesmo procedimento em etapa 2 e termine-o em todos os assinantes em seu conjunto
3. Afinal os Nós regeneraram o certificado de ITLRecovery, serviços deverão ser reiniciados na

ordem como segue: Se você reage de modo misturado – Atualize o CTL antes que você continue token - TokenlessO log em **Cisco do** editor **unificou a utilidade** Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de redeNo reinício** seleto do editor em **Cisco confie o serviço da verificação**. Uma vez que o reinício do serviço termina, continue com os assinantes e reinicie o **serviço da verificação da confiança de Cisco**

4. Recarregue todos os telefones **Cisco unificou a administração > o sistema > parâmetros de empreendimento CMRestauração** seleta então você verá um PNF-acima com a indicação que **você está a ponto de restaurar todos os dispositivos no sistema. Esta ação não pode ser desabotoada. Continue? ,** selecione **ESTÁ BEM** e selecione então a **restauração**
5. Os telefones transferirão arquivos pela rede agora o ITL/CTL novo quando restaurarem.

A supressão expirou Certificados de confiança

Nota: Identifique os Certificados de confiança que precisam de ser suprimidos, já não exigido, ou expiraram. Não suprima dos cinco Certificados baixos que incluem o CallManager.pem, o tomcat.pem, o ipsec.pem, o CAPF.pem e o TVS.pem. Os Certificados de confiança podem ser suprimidos quando apropriados. Os reinícios do serviço abaixo são projetados cancelar alguns na informação de memória de Certificados do legado dentro daqueles serviços.

1. Navegue a **Cisco unificou a utilidade > as ferramentas > o Control Center - serviços de rede** Da gota selecione para baixo o editor CUCMSelecione a **notificação de alteração do certificado da parada**Repita para cada nó do gerenciador de chamada em seu conjuntoSe você tem um server IMP Do menu de gota para baixo selecione seus server IMP um de cada vez e selecione **serviços de Web da administração da plataforma da parada e agente de sincronização do intercluster de Cisco**
2. Navegue a **Cisco unificou o > gerenciamento de certificado > o achado do > segurança da administração do OS**
   Encontre os Certificados de confiança expirados. (Para versões 10.X e mais recente que você pode filtrar pela expiração. Versões franco abaixo de 10.0 que você precisará de identificar os Certificados específicos manualmente ou através dos alertas RTMT se recebido)O mesmo certificado de confiança pode aparecer nos nós múltiplos. Deve ser suprimido individualmente de cada nó.Selecione o certificado de confiança para ser suprimido (dependente de sua versão você ou obterá um PNF-acima ou você será navegado ao certificado na mesma página) **Supressão** seleta (você obterá um PNF-acima que comece com você esteja a ponto de suprimir permanentemente deste certificado…*)*Selecione **ESTÁ BEM**
3. Repita o processo para que cada certificado de confiança seja suprimido
4. Em cima da conclusão, os serviços deverão ser reiniciados que são relacionados diretamente aos Certificados suprimidos. Você não precisa de recarregar telefones nesta seção. O gerenciador de chamada e o CAPF serão impacto do valor-limite. Tomcat-confiança: serviço de Tomcat do reinício através da linha de comando (veja a seção de Tomcat)CAPF-confiança: a função do proxy do Certificate Authority de Cisco do reinício (veja a seção CAPF) não recarrega valores-limiteCallManager-confiança: O serviço do CallManager/CTIManager (veja a seção do CallManager) não recarrega valores-limite Impacta valores-limite e reinícios das causasIPsec-confiança: Local DRF Master/DRF (veja a

seção do IPSEC)Os TV (Auto-assinados) não têm Certificados de confiança
5. Serviços do reinício parados previamente em 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.