Expiração do certificado e supressão do CallManager

Índice

Introdução

Este documento descreve um problema com CallManager da Cisco (CM) onde você recebe o **CertExpiryEmergency: Certificate o** mensagem de alarme da **expiração EMERGENCY_ALARM do** cliente da ferramenta do monitoramento em tempo real (RTMT), e oferece uma solução ao problema.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento de versões 6.x à 9.x CM, e que seu sistema:

- Não tem uma configuração do Domain Name System (DNS). Isto é feito para a simplicidade do documento, mas muitos sistemas têm-no configurado que é APROVADO.
- Tem um certificado que seja expirado e deva ser regenerado, ou um certificado que seja programado para expirar.

  Nota: O endereço IP de Um ou Mais Servidores Cisco ICM NT do sistema não importa se você incorpora o comando **novo** ou **regenerado da geração** depois que você muda o nome de host ou o endereço IP de Um ou Mais Servidores Cisco ICM NT.

Componentes Utilizados

A informação neste documento é baseada no server do Cisco CM com páginas de administração.

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 sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Problema

Você recebe um **CertExpiryEmergency: Certificate o** mensagem de alarme da **expiração EMERGENCY_ALARM do** RTMT no CM:

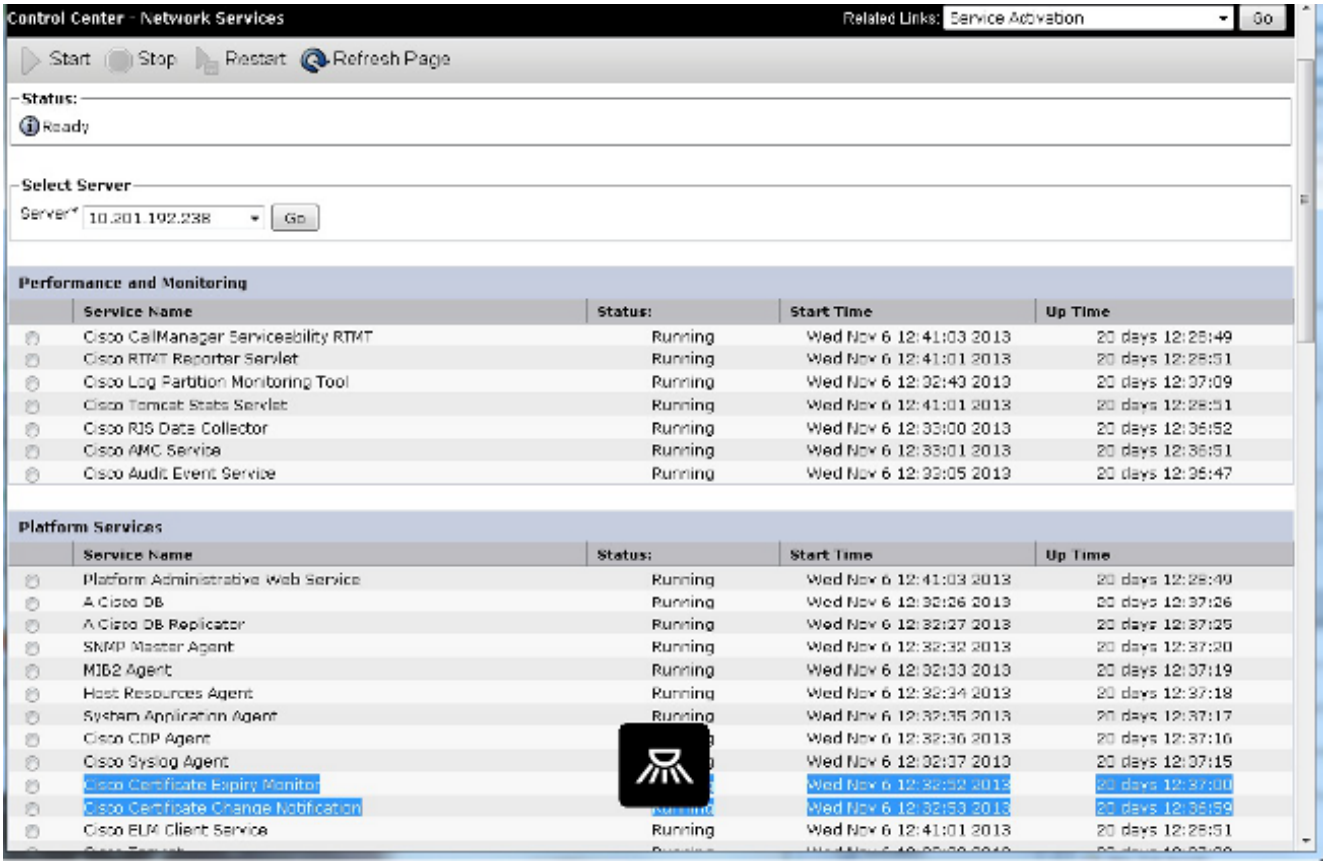
```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor Cluster ID:Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 630: Jul 30 17:00:00.353 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CallManager-trust Type:trust-cert Expiration:Fri Dec 28 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI

Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
HOST-CM912 local7 0 : 631: Jul 30 17:00:00.354 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification. Certificate name:CAPF-5d0a9888
Unit:CAPF-trust Type:trust-cert Expiration:Fri Dec 28 12:14:4 App ID:
 Cisco Certificate
Monitor Cluster ID: Node ID:HOST-CM-PRI
```

Solução

Use a informação nesta seção a fim resolver o problema do mensagem de alarme CM.

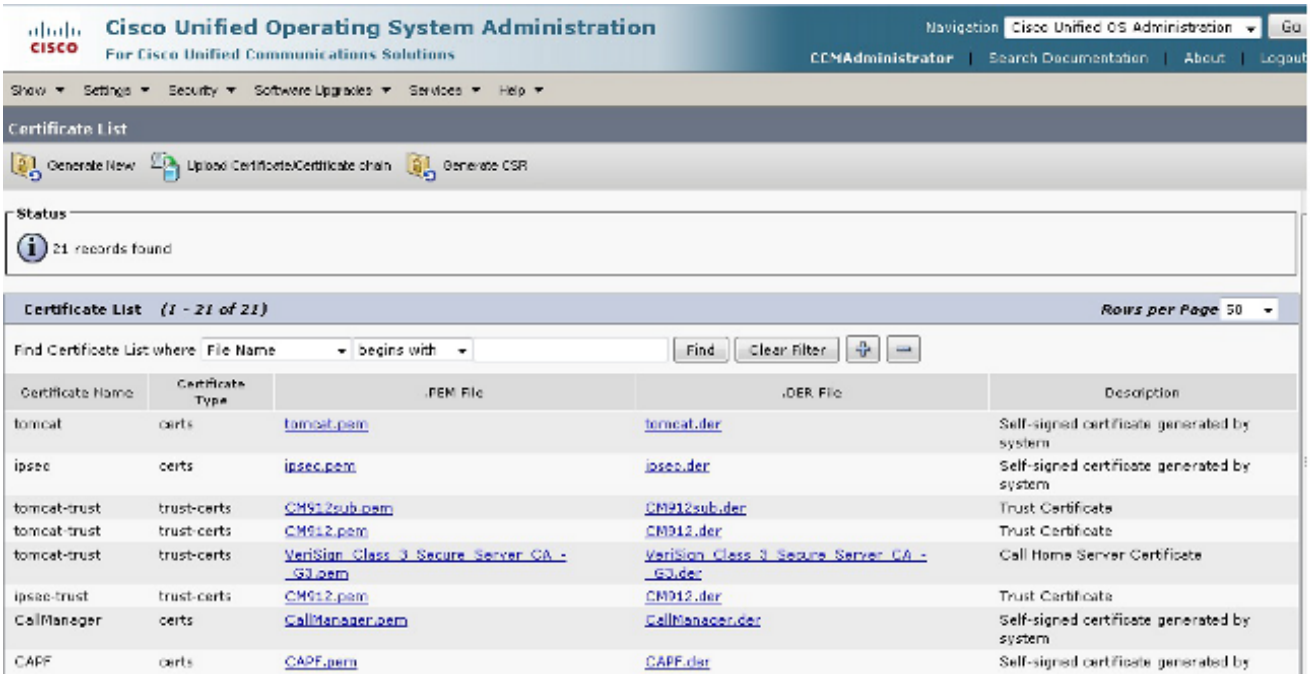
1. Do CM a página unificada GUI da utilidade, navega às **ferramentas > ao Control Center - serviços de rede**.

2. Pare o **monitor da expiração do certificado de Cisco** e os serviços da **notificação de alteração do certificado de Cisco em** todos os server no conjunto:



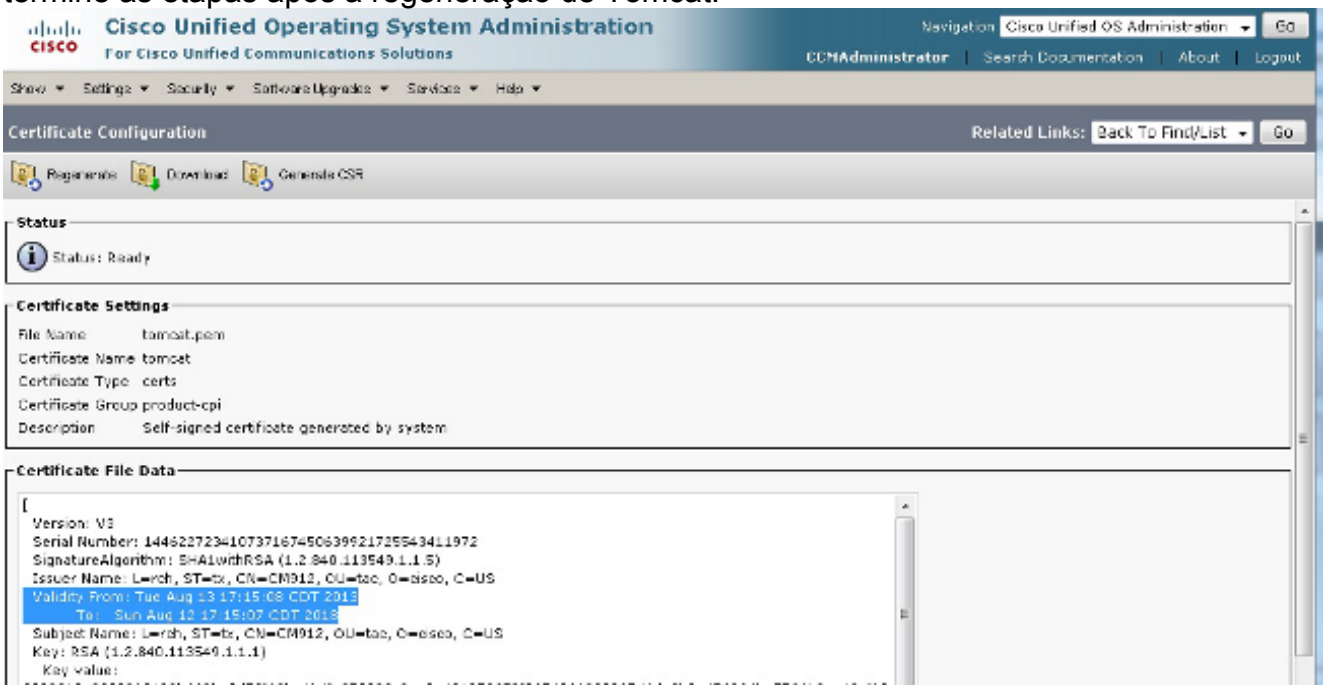
3. Da administração GUI do operating system (OS), navegue ao **> gerenciamento de certificado da Segurança**, e este displays de tela:

4. Clique o **achado** a fim indicar todos os Certificados em um servidor particular:

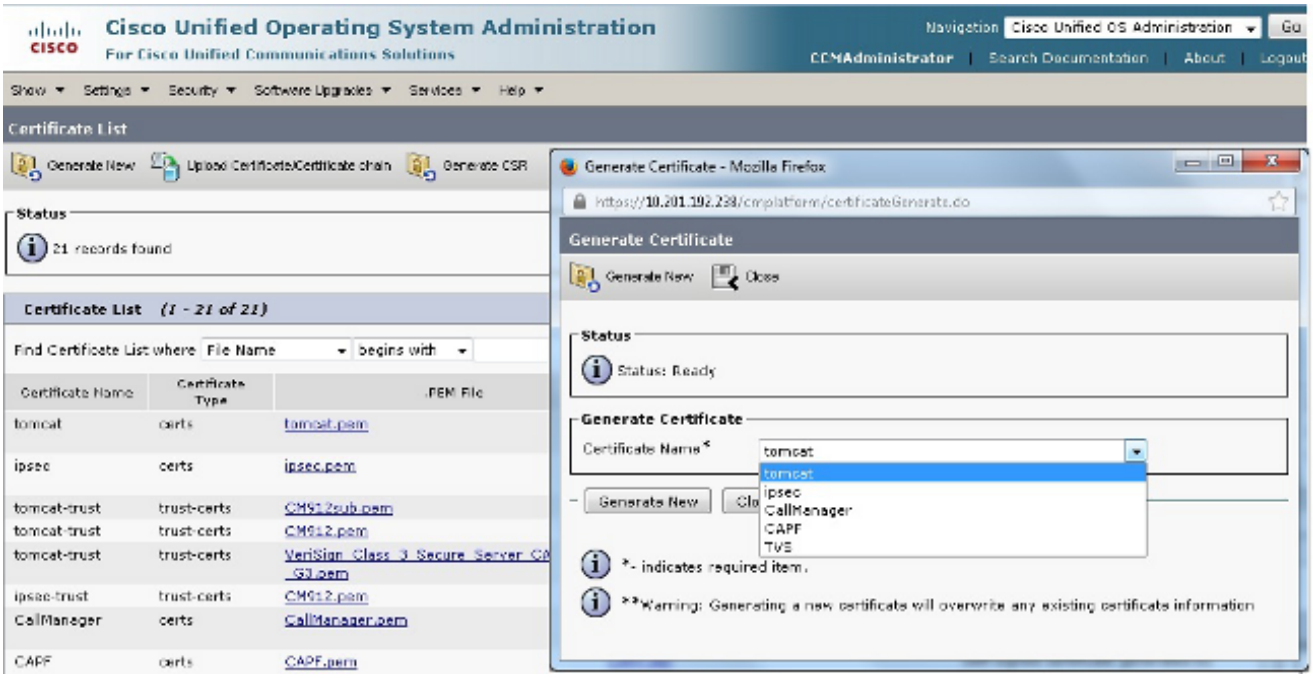


5. Clique todo o certificado (um certificado de Tomcat neste caso) e veja a data, como destacada na imagem seguinte. Para Certificados de Tomcat, verifique se o server usa um certificado da terceira para o início de uma sessão da página do **ccmadmin**. Você pode verificar este quando você registra na página de um navegador.

   Nota: Se é um certificado assinado da terceira, proveja o artigo transferindo arquivos pela rede da comunidade do apoio de Cisco dos Certificados da Web GUI do ccmadmin CUCM e termine as etapas após a regeneração de Tomcat.

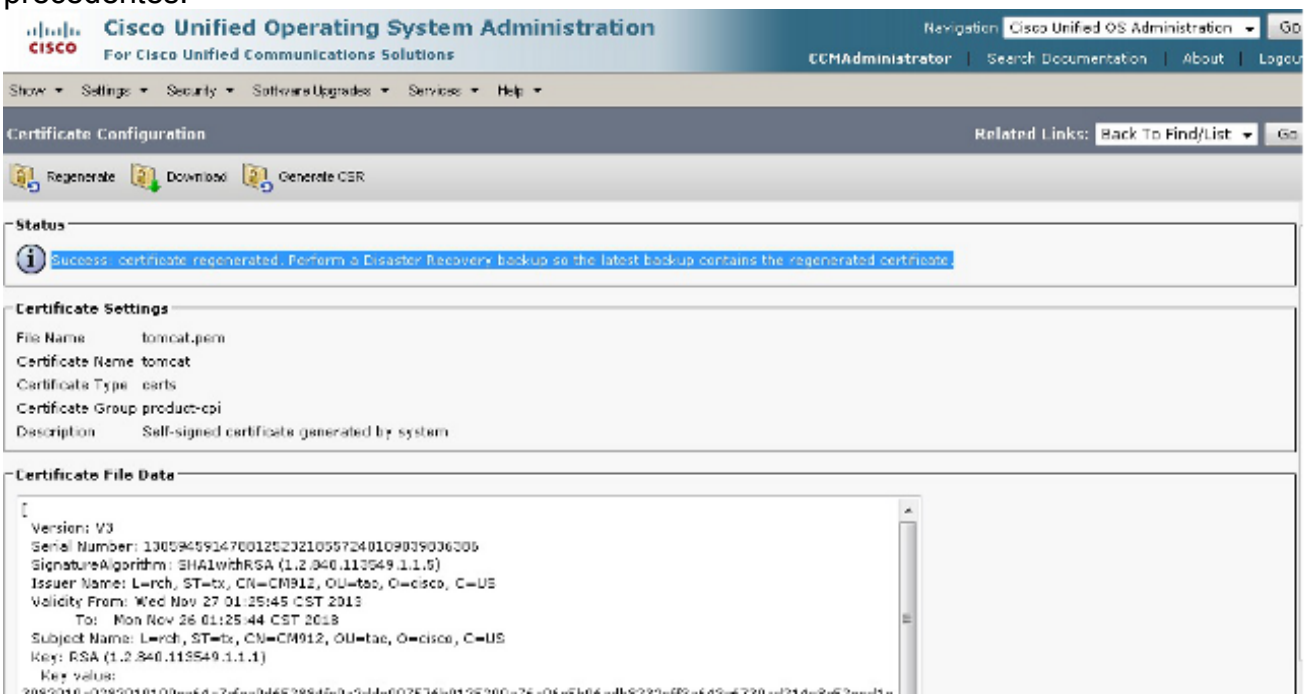


6. Navegue à página do **gerenciamento certificado no** editor. Encontre e clique o **arquivo tomcat.pem**, e clique então o regenerado:



7. A fim reiniciar o serviço de Tomcat nesse nó, abrir um CLI ao nó e incorporar o comando de **Cisco Tomcat do reinício do serviço dos utils**. Uma vez que o certificado é gerado, uma mensagem estala acima a fim confirmar que o certificado é atual.

   Nota: O certificado é verificado igualmente pela informação da data descrita nas etapas precedentes.



8. Termine este processo para cada um dos assinantes no conjunto a fim regenerar os Certificados de TomCat.

Certificate a regeneração para versões 8.x e mais recente CUCM

Use a informação nesta seção a fim regenerar certificados expirados para versões 8.x e mais recente do gerente das comunicações unificadas de Cisco (CUCM).

Nota: Regenere os Certificados após horas de negócio normais, porque você deve reiniciar serviços e recarregar os telefones no processo.

CAPF

Para a regeneração da função do proxy do Certificate Authority (CAPF), assegure-se de que o conjunto não reaja de um modo seguro do conjunto: navegue ao **sistema > parâmetros de empreendimento da** página da web de administração CM, e da busca para o **modo seguro do conjunto**. Se o valor é **0**, a seguir o conjunto não reage de um modo seguro do conjunto. Se o valor é qualquer número a não ser zero, a seguir o conjunto reage de um modo seguro, e você deve usar o cliente do certificate trust list (CTL) a fim atualizar o arquivo CTL.

Nota: Proveja o artigo da comunidade da Segurança do telefone IP e do apoio CTL (certificate trust list) Cisco para mais informação.

1. Do editor, navegue à página do gerenciamento certificado.
2. Abra o **arquivo CAPF.pem** e clique o regenerado**. Isto** renova o certificado e cria dois arquivos novos da confiança: um é a CM-confiança e a outro é a CAPF-confiança.
3. O da página da utilidade, navegue às **ferramentas > aos serviços da característica**.
4. Se o serviço CAPF é ativado sob **serviços da característica**, a seguir reinicie o serviço. Se o serviço CAPF não é ativado, a seguir um reinício não é necessário.
5. Navegue às **ferramentas > aos serviços de rede da** página da utilidade, e reinicie o serviço do serviço da verificação da confiança (TV).
6. Navegue às **ferramentas > aos serviços da característica da** página da utilidade, especifique o nó, e reinicie o serviço TFTP.
7. Uma vez que os serviços são reiniciados, recarregue os telefones de modo que possam recuperar o arquivo actualizado da lista da confiança da identidade (ITL).
8. Retorne à página do gerenciamento certificado e suprima dos dois arquivos velhos da confiança. Estes são os dois arquivos expirados da confiança que você recebeu das saídas de erro. Os Certificados novos têm um número de série que combine o **arquivo CAPF.pem**.
9. Termine as etapas precedentes para cada subscritor.

IPSec

Os Certificados da segurança de protocolo do Internet (IPsec) afetam o mestre da falha da Recuperação de desastres (DRF) e locais, que trata as funções alternativas e da restauração.

1. Navegue à página de administração do OS no editor.
2. Navegue ao **> gerenciamento de certificado da Segurança** e clique o **arquivo IPSEC.pem**.

3. Clique o **regenerado** a fim atualizar o arquivo da confiança.

4. Recarregue o server que o certificado esteve regenerado sobre. Isto é exigido porque cada serviço deve ser reiniciado após toda a regeneração/atualização de qualquer certificado. Contudo, o IPsec não tem uma capacidade do reinício do serviço a não ser para recarregar o nó inteiro. Se outros Certificados precisam de ser atualizados/regenerado, termine todas as etapas e recarregue então o nó os Certificados foram processados afinal que completamente. Isto permite que o server tenha todos os Certificados actualizados no truststore e leia-os dentro corretamente.

CM

1. Navegue à página de administração do OS no editor.

2. Navegue à página do gerenciamento certificado, clique o **achado**, clique o **arquivo CallManager.pem**, e clique então o regenerado**.**

3. Navegue às **ferramentas > ao serviço da característica na** página da utilidade, encontre o nó especificado, e reinicie o serviço do Cisco CM.

4. Da página da utilidade, navegue às **ferramentas > aos serviços de rede**, e reinicie o serviço TV.

5. Da página da utilidade, navegue às **ferramentas > aos serviços da característica**, especifique o nó, e reinicie os serviços CM e CTI.

6. Recarregue os telefones de modo que possam recuperar o arquivo actualizado ITL.

7. Termine as etapas precedentes para cada subscritor.

TV

1. Navegue à página de administração do OS no editor.

2. Navegue ao **> gerenciamento de certificado da Segurança**, clique o **achado**, clique o **arquivo TVS.pem**, e clique então o regenerado**.**

3. Da página da utilidade, navegue às **ferramentas > aos serviços de rede**, e reinicie o serviço TV.

4. Da página da utilidade, navegue às **ferramentas > aos serviços da característica**, especifique o nó, e reinicie o serviço TFTP.

5. Recarregue os telefones de modo que possam recuperar o arquivo actualizado ITL.

6. Termine as etapas precedentes para cada subscritor.

Suprima de Certificados

Quando você suprime de Certificados, assegure-se de que os serviços previamente mencionados estejam parados, e que os Certificados que você suprime não estão usados atualmente nem estão expirados realmente.

Também, verifique sempre toda a informação dentro do certificado, porque você não pode o salvar após o supressão.