CallManager证书到期和删除

目录

简介

本文描述一问题用Cisco CallManager (CM)您接收**CertExpiryEmergency的地方：证书**从实时监控工具(RTMT)客户端的**终止EMERGENCY_ALARM**警报信息，和提供解决方案对问题。

先决条件

要求

Cisco建议您有CM版本6.x到9.x知识，并且您的system:

- 没有一域名系统(DNS)配置。这是执行的为了简化本文，但是许多系统有是好的配置的它。
- 有超时并且必须重新生成的一证书，或者安排超时的一证书。

注意：系统的IP地址不重要，如果输入**生成新建的**或**再生**命令，在您更改主机名或IP地址后。

使用的组件

本文档中的信息根据有管理页面的Cisco CM服务器。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

问题

您接收**CertExpiryEmergency ：证书**从RTMT的**终止EMERGENCY_ALARM**警报信息在CM ：

```
Message from syslogd@HOST-CM-PRI at Fri Jul 5 13:00:00 2013 ...
```

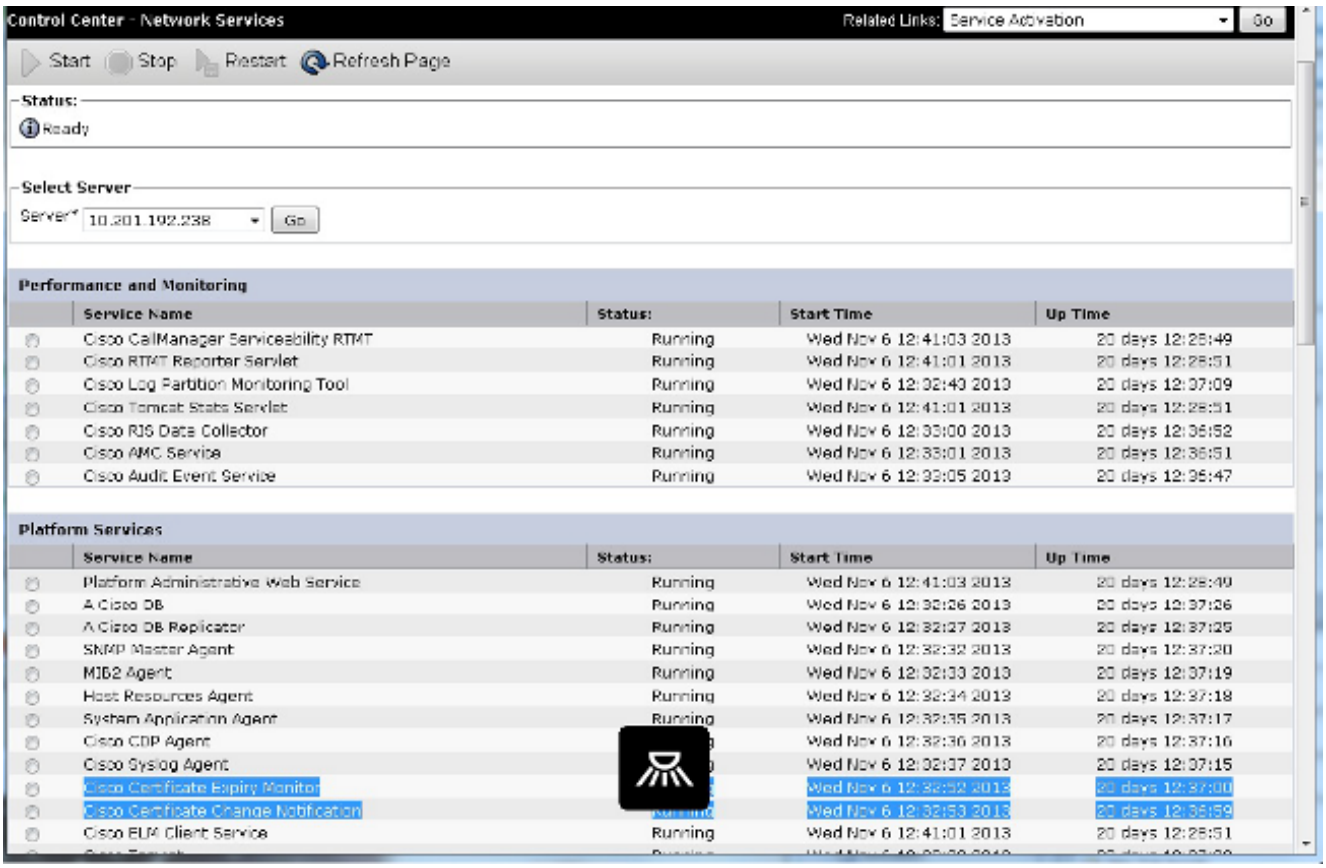
```
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor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

解决方案

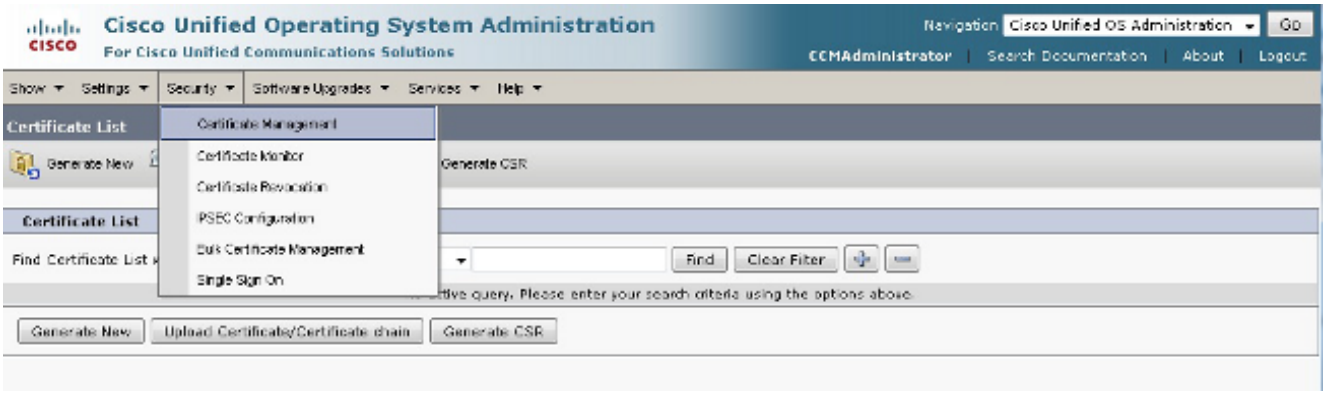
请使用信息在此部分为了解决CM警报信息问题。

1. 从CM统一的维护性页GUI，导航对**Tools > Control Center -网络服务**。

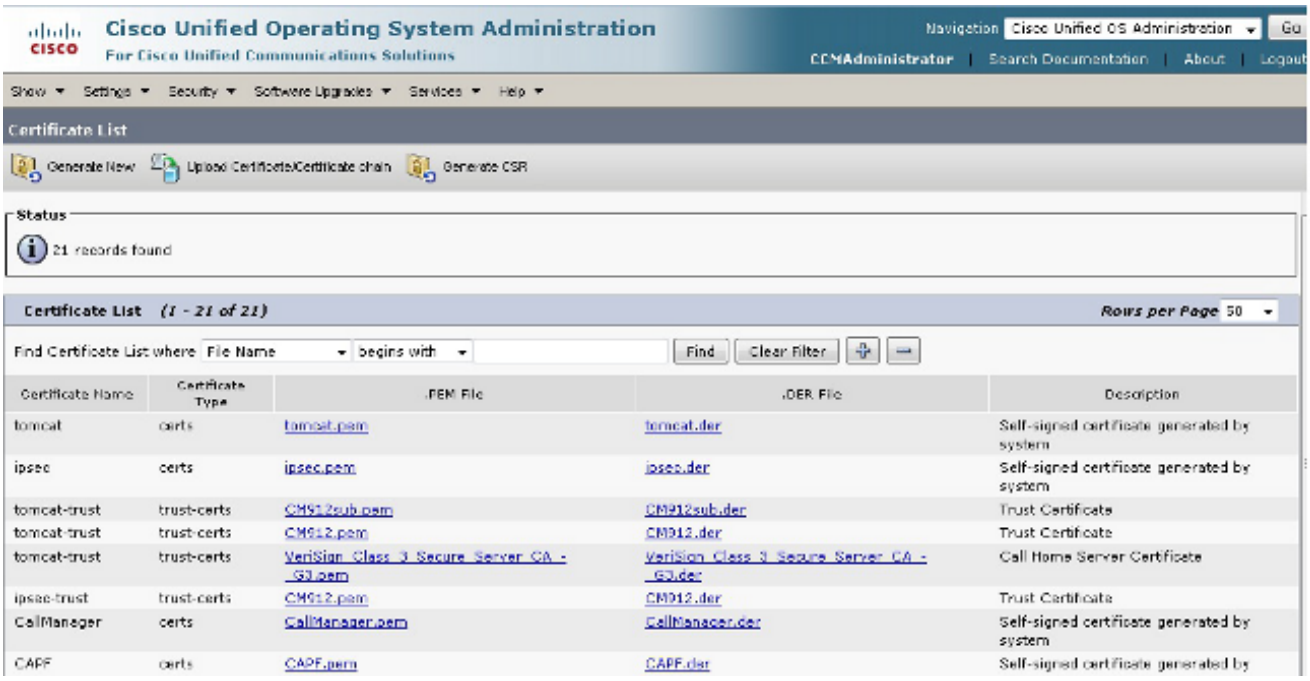
2. 终止**思科证书终止箴言报**和**思科证书**在所有的**修改提示**服务在集群的服务器：



3. 从操作系统(OS)管理GUI，请导航对**安全> Certificate Management**，和此屏幕显示：

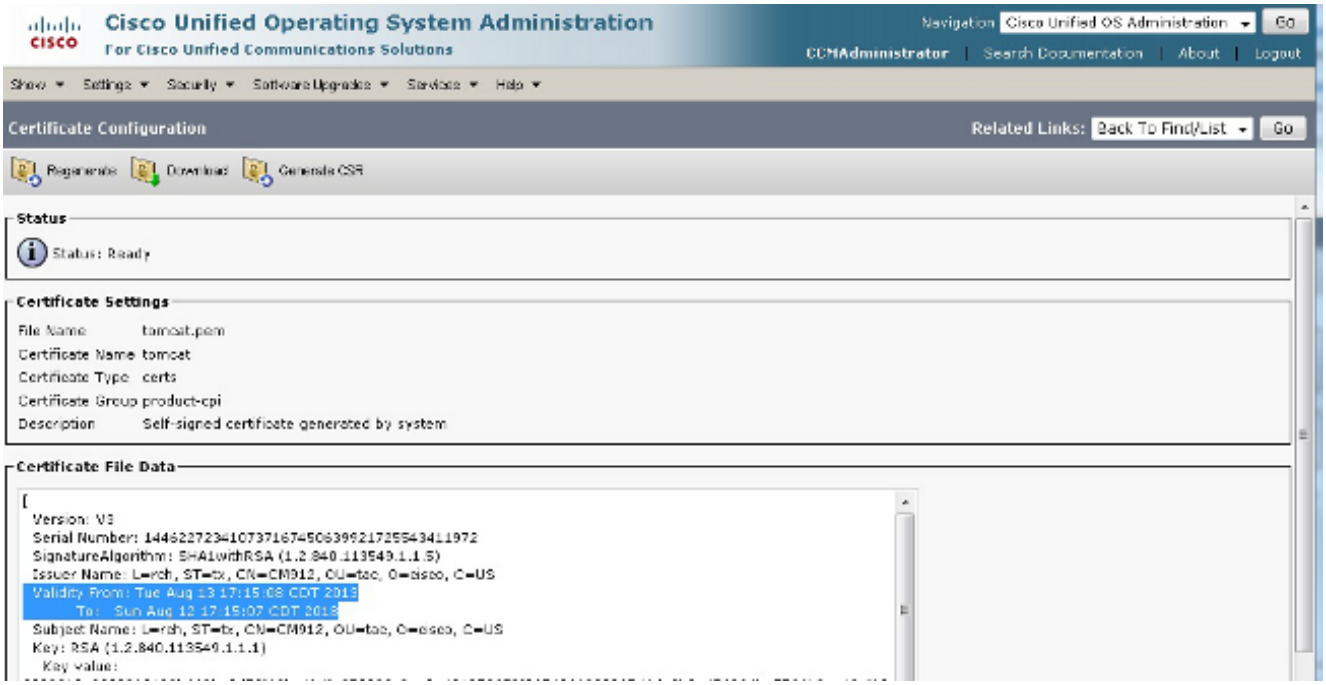


4. 点击**查找**为了显示所有在特定服务器的证书：

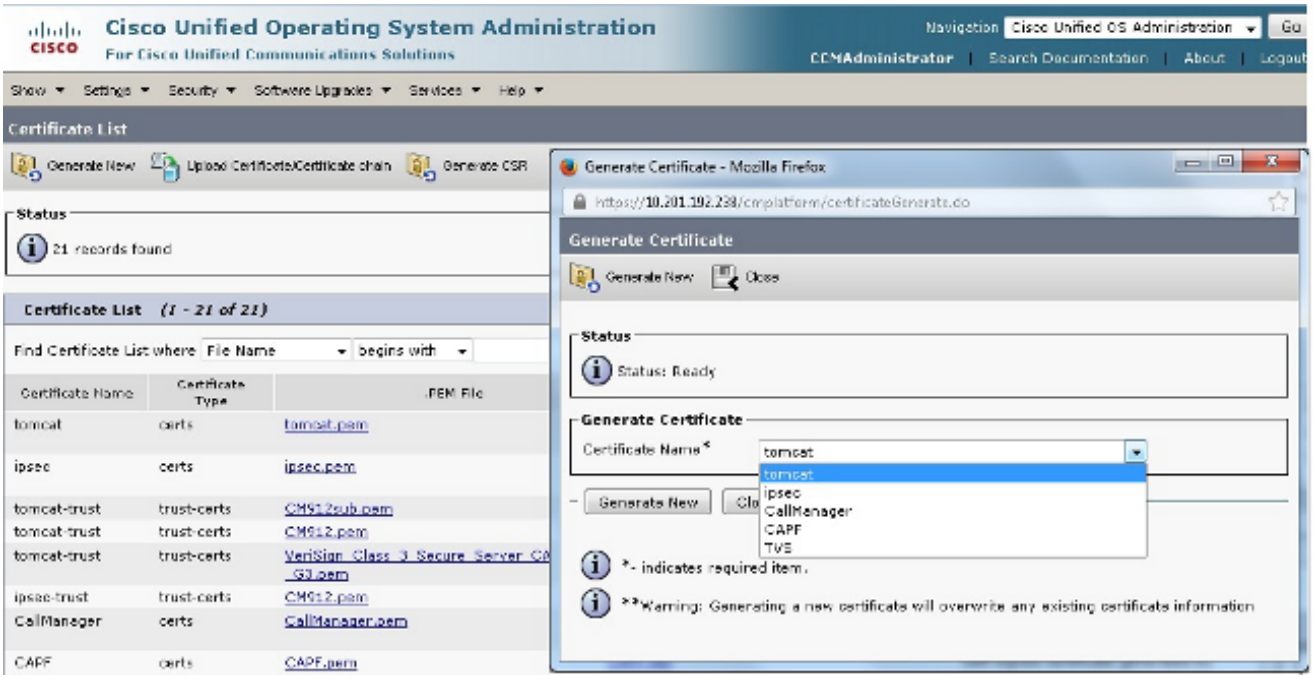


5. 点击所有证书(Tomcat证书在这种情况下)并且观看日期，如用下镜像突出显示。对于Tomcat证书，如果服务器使用一第三方证书**ccmadmin**页登录，请验证。当您登录从浏览器时的页您能检查此。

注意：如果它是一第三方签名证书，请参考上传Ccmadmin Web GUI证书Cisco支持社区条款的CUCM并且在Tomcat重新生成以后完成步骤。

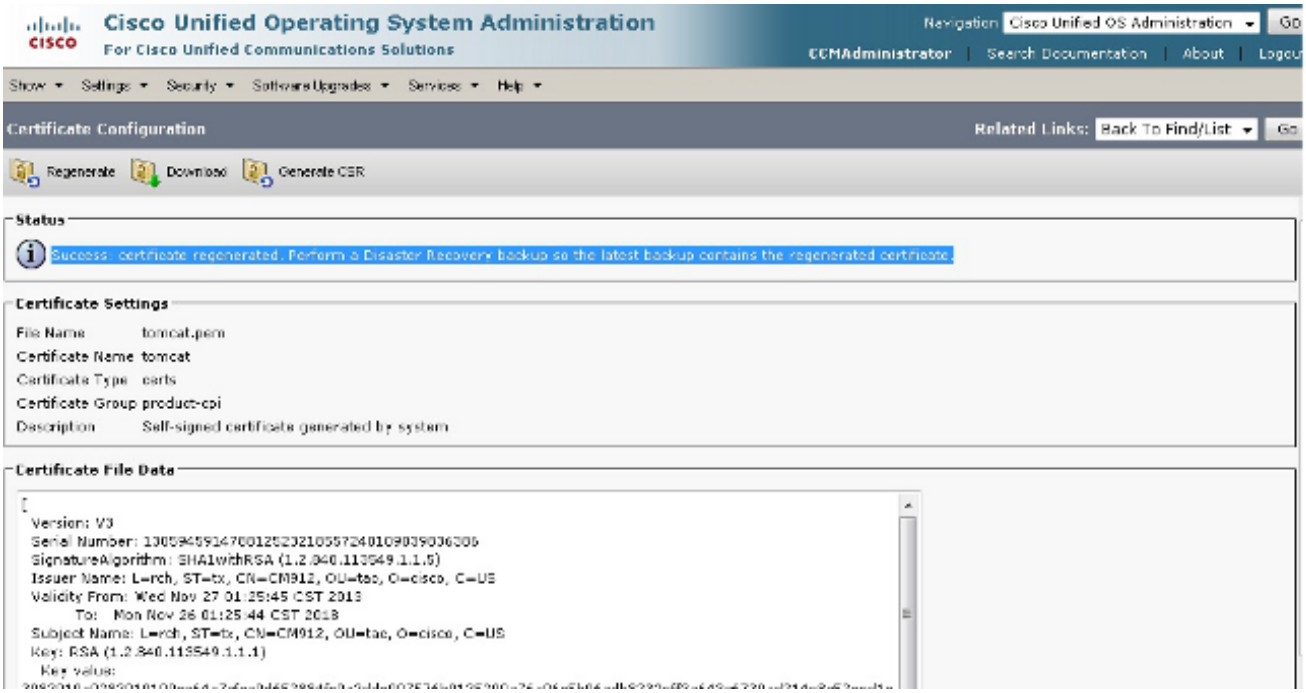


6. 导航对在发行商的**证书管理**页。查找并且点击**tomcat.pem文件**和然后单击重新生成：



7. 为了重新启动在该节点的Tomcat服务，打开CLI到节点和输入**使用情况服务重新启动思科Tomcat**命令。一旦证书生成，消息冒出为了确认证书当前。

注意：证书由在上一个步骤描述的日期信息也验证。



8. 完成其中每一个的此进程集群的用户为了重新生成Tomcat证书。

CUCM版本8.x和以上的证书重新生成

请使用信息在此部分为了重新生成Cisco Unified Communications Manager (CUCM)版本8.x和以上的过期的证书。

注意：因为您必须重新启动服务和重新启动在进程的电话在正常工作时间之后重新生成证书。

CAPF

对于认证机关代理功能(CAPF)重新生成，请保证集群不在一个安全集群模式：导航对从CM管理网页和搜索的**System > Enterprise Parameters团星安全模式的**。如果值是**0**，则集群不在一个安全集群模式。除零之外，如果值是任何编号，则集群在安全模式，并且您必须使用证书信任列表(CTL)客户端为了更新CTL文件。

注意：参考IP电话安全和CTL (证书信任列表) Cisco支持社区条款欲知更多信息。

1. 从发行商，请导航对证书管理页。
2. 打开**CAPF.pem文件**并且点击重新生成。**这**更新证书并且创建两个新的信任文件：一个是CM托拉斯，并且其他是CAPF托拉斯。
3. 从维护性页，请导航对**Tools>功能服务**。
4. 如果CAPF服务被启动在**功能服务下**，则请重新启动服务。如果CAPF服务没有被启动，则重新启动不是必要的。
5. 导航对从维护性页的**Tools>网络服务**，并且重新启动托拉斯验证服务(TV)服务。

6. 导航对**Tools>**从维护性页的**功能服务**，指定节点，并且重新启动TFTP服务。

7. 一旦服务被重新启动，请重新启动电话，以便他们能检索更新标识托拉斯列表(ITL)文件。

8. 返回到证书管理页并且删除两个旧有信任文件。这些是该两个超时的信任的文件您从错误输出接收。新的证书有匹配**CAPF.pem文件的**一序列号。

9. 完成每个用户的上一个步骤。

IPsec

Internet协议安全性(IPSec)证书影响灾难恢复失败(DRF)主控和本地，处理备份和恢复功能。

1. 导航对在发行商的OS管理页面。

2. 导航对**安全> Certificate Management**并且点击**IPSEC.pem文件**。

3. 点击**重新生成**为了更新信任文件。

4. 重新启动服务器证书被重新生成了。因为必须重新启动每服务，在任何证书后，所有重新生成/更新这要求。然而， IPSec没有一个服务重新启动能力除之外重新启动整个节点。如果其他证书需要更新/被重新生成，请完成所有步骤然后重新启动节点，在所有证书通过后处理。这允许服务器有在truststore更新的所有证书和适当地写入。

CM

1. 导航对在发行商的OS管理页面。

2. 导航对证书管理页，点击**查找**，点击**CallManager.pem文件**和然后单击重新生成**。**

3. 导航对**Tools>**在维护性页的**功能服务**，查找指定的节点，并且重新启动Cisco CM服务。

4. 从维护性页，请导航对**Tools>网络服务**，并且重新启动TV服务。

5. 从维护性页，请导航对**Tools>功能服务**，指定节点，并且重新启动CM和CTI服务。

6. 重新启动电话，以便他们能检索更新ITL文件。

7. 完成每个用户的上一个步骤。

TV

1. 导航对在发行商的OS管理页面。

2. 导航对**安全> Certificate Management**，点击**查找**，点击**TVS.pem文件**和然后单击重新生成**。**

3. 从维护性页，请导航对**Tools>网络服务**，并且重新启动TV服务。

4. 从维护性页，请导航对**Tools>功能服务**，指定节点，并且重新启动TFTP服务。

5. 重新启动电话，以便他们能检索更新ITL文件。

6. 完成每个用户的上一个步骤。

删除证书

当您删除证书时，请保证以前被提及的服务被终止，并且您删除的证书当前没有使用也实际上没有超时。

并且，因为您不能在删除以后，保存它总是请检查所有在证书内的信息。