Окончание срока действия сертификата CallManager и удаление

Содержание

Введение

Этот документ описывает проблему с Cisco CallManager (CM), где вы получаете **CertExpiryEmergency: Истечение Сертификата** аварийное сообщение **EMERGENCY_ALARM** от клиента устройства контроля в реальном времени (RTMT) и предложения решение проблемы.

Предварительные условия

Требования

Cisco рекомендует ознакомиться с Версиями CM 6.x через 9.x, и что система:

- Не имеет конфигурации Системы доменных имен (DNS). Это сделано для простоты документа, но многим системам настроили его, который в порядке.
- Действительно имеет сертификат, который истекается и должен быть восстановлен, или сертификат, который планируется для истечения.

Примечание: IP-адрес системы не имеет значения, вводите ли вы **Генерирование Нового** или **команда Regenerate** после изменения имени хоста или IP-адреса.

Используемые компоненты

Сведения в этом документе основываются на сервере Cisco CM со страницами администратора.

Сведения, представленные в этом документе, были получены от устройств, работающих в

специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Проблема

Вы получаете **CertExpiryEmergency: Истечение Сертификата** аварийное сообщение **EMERGENCY_ALARM** от RTMT в CM:

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

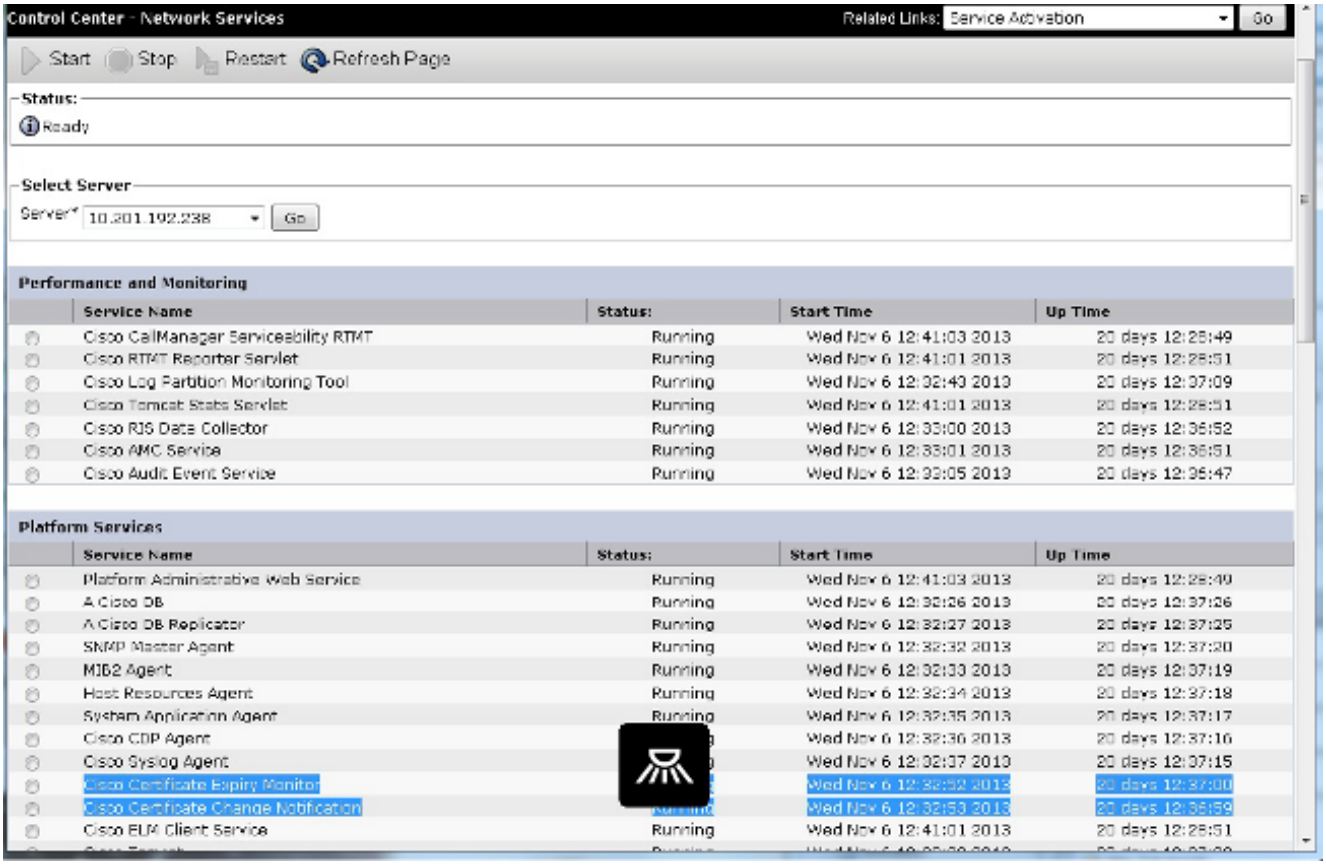
```
HOST-CM912 local7 0 : 629: Jul 30 17:00:00.352 UTC :
%CCM_UNKNOWN-CERT-0-CertExpiryEmergency: Certificate Expiry EMERGENCY_ALARM
Message:Certificate expiration Notification.
 Certificate name:CAPF Unit:CAPF Type:own-cert
Expiration:Fri Dec 28 12:14:42:000 EST 2012 / App ID:Cisco Certificate
Monitor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

Решение

Используйте информацию в этом разделе для решения проблемы аварийного сообщения CM.

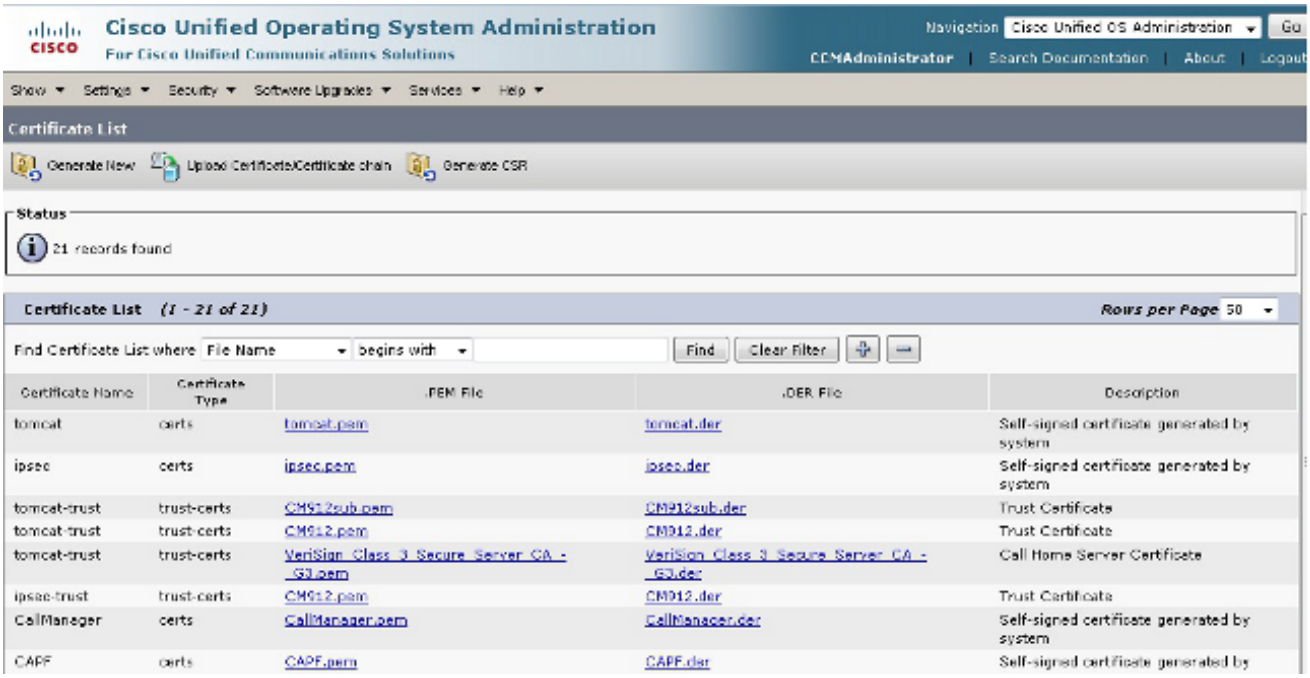
1. От CM Унифицированный GUI страницы Serviceability перейдите к **Tools> Control Center - Сетевые сервисы**.

2. Остановите **Монитор Истечения Сертификата Cisco** и сервисы **Уведомления об изменении Сертификата Cisco** на всех серверах в кластере:



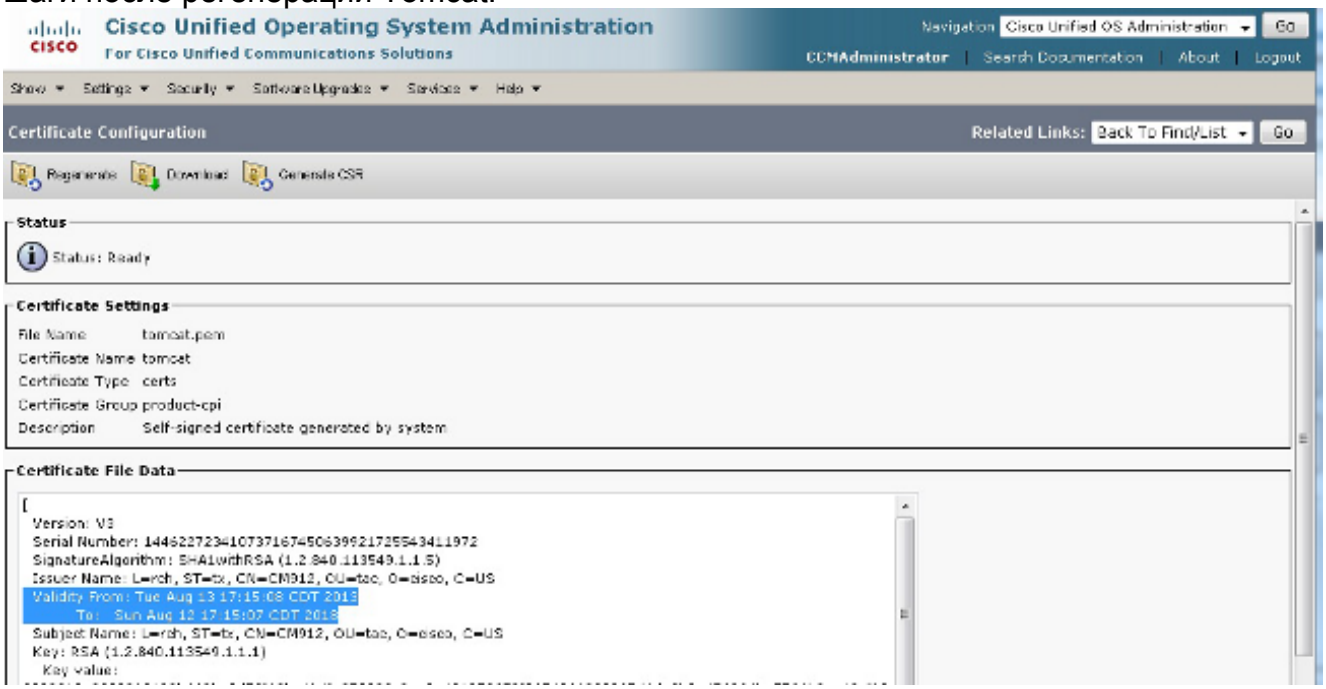
3. От GUI администрирования Операционной системы (OS) перейдите к **Безопасности> Управление сертификатами** и этому изображения на экране:

4. Нажмите **Find** для отображения всех сертификатов на индивидуальном сервере:

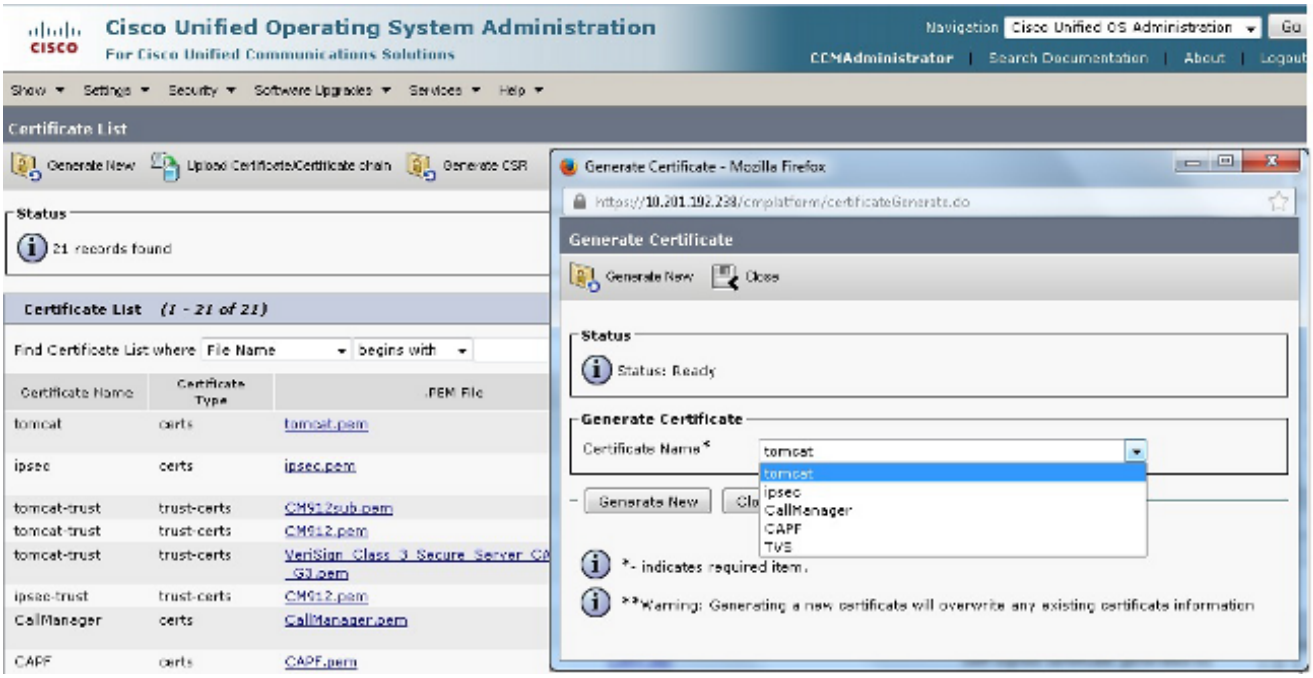


5. Нажмите любой сертификат (сертификат Tomcat в этом случае) и просмотрите дату, как выделено в следующем образе. Для сертификатов Tomcat проверьте, использует ли сервер сторонний сертификат для входа в систему страницы **ccmadmin**. Когда вы входите в страницу от браузера, можно проверить это.

   Примечание: Если это - сторонний подписанный сертификат, сошлитесь на статью [CUCM Uploading CCMAdmin Web GUI Certificates Cisco Support Community] и выполните шаги после регенерации Tomcat.

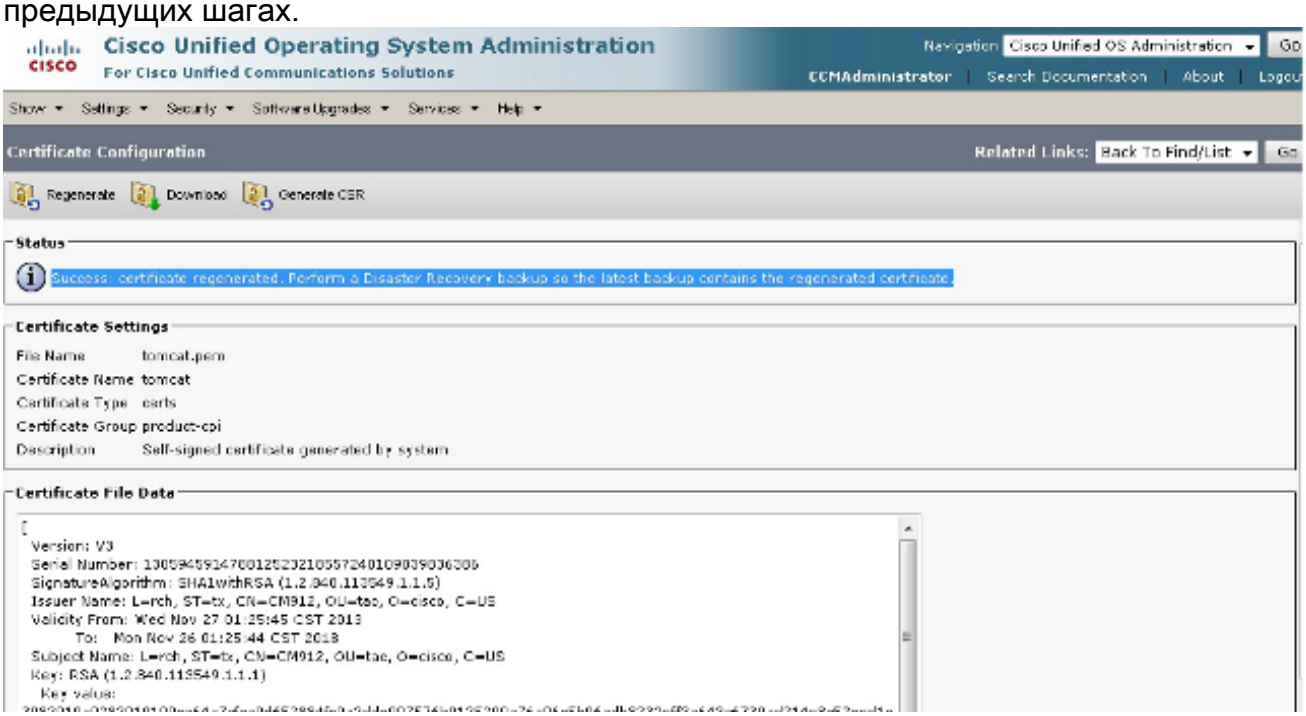


6. Перейдите к странице **Certificate Management** на Издателе. Найдите и нажмите **tomcat.pem** файл, и затем нажмите **Regenerate**:



7. Для перезапуска сервиса Tomcat на том узле откройте CLI для узла и введите **команду utils service restart Cisco Tomcat**. Как только сертификат генерируется, сообщение появляется, чтобы подтвердить, что сертификат является текущим.

   Примечание: Сертификат также проверен информацией о дате, описанной в предыдущих шагах.



8. Завершите этот процесс для каждого из абонентов в кластере для регенерации сертификатов tomcat.

Регенерация сертификата для версий CUCM 8.x и позже

Используйте информацию в этом разделе для регенерации просроченных сертификатов для Версий Cisco Unified Communications Manager (CUCM) 8.x и позже.

Примечание: Восстановите сертификаты после обычных рабочих часов, потому что необходимо перезапустить сервисы и перезагрузить телефоны в процессе.

CAPF

Для регенерации функции представительства сертифицирующей организации (CAPF) гарантируйте, что кластер не находится в безопасном кластерном режиме: перейдите к **Системе> Параметры предприятия** от Административной веб - страницы CM, и поиск **Кластера Защищает Режим**. Если значение **0**, то кластер не находится в безопасном кластерном режиме. Если значение является каким-либо номером кроме нуля, то кластер находится в безопасном режиме, и необходимо использовать клиента Списка надежных сертификатов (CTL) для обновления файла CTL.

Примечание: Сошлитесь на статью IP Phone Security и CTL (Certificate Trust List) Cisco Support Community для получения дополнительной информации.

1. От Издателя перейдите к странице Certificate Management.
2. Откройте файл **CAPF.pem** и нажмите **Regenerate**. Это возобновляет сертификат и создает два новых трастовых файла: каждый - доверие CM, и другой доверие CAPF.
3. От страница Serviceability, перейдите к **Программным средствам> Feature Services**.
4. Если сервис CAPF активирован под **Feature Services**, то перезапустите сервис. Если сервис CAPF не активирован, то перезапуск не необходим.
5. Перейдите к **Программным средствам> Сетевые сервисы** от страницы Serviceability и перезапустите сервис службы проверки доверия (TVS).
6. Перейдите к **Программным средствам> Feature Services** от страницы Serviceability, задайте узел и перезапустите Сервис TFTP.
7. Как только сервисы перезапущены, перезагружают телефоны так, чтобы они могли получить обновленный файл Идентификационного списка доверия (ITL).
8. Возвратитесь к странице Certificate Management и удалите два старых трастовых файла. Это два трастовых файла с истекшим сроком, которые вы получили от ошибки вывода. Новые сертификаты имеют серийный номер, который совпадает с файлом **CAPF.pem**.
9. Выполните предыдущие шаги для каждого абонента.

IPSec

Протокол IPSEC (Internet Protocol Security) (IPSec), сертификаты влияют на ведущее устройство Сбоя восстановления после отказа (DRF) и локальную переменную, которая имеет дело с функциями восстановления и резервной копией.

1. Перейдите к Странице администрирования операционной системы на Издателе.

2. Перейдите к **Безопасности> Управление сертификатами** и нажмите файл **IPSEC.pem**.

3. Нажмите **Regenerate** для обновления трастового файла.

4. Перезагрузите сервер, на котором был восстановлен сертификат. Это требуется, потому что каждый сервис должен быть перезапущен после любой регенерации / обновление любого сертификата. Однако IPSec не имеет сервисной способности к перезапуску кроме перезагрузить весь узел. Если другие сертификаты должны быть обновлены / восстановленный, выполнить все шаги и затем перезагрузить узел после того, как все сертификаты были обработаны через. Это позволяет серверу иметь все сертификаты, обновленные в базе доверенных сертификатов и чтении в должным образом.

CM

1. Перейдите к Странице администрирования операционной системы на Издателе.

2. Перейдите к странице Certificate Management, нажмите **Find**, нажмите файл **CallManager.pem**, и затем нажмите **Regenerate**.

3. Перейдите к **Программным средствам> Сервис Функции** на странице Serviceability, найдите указанный узел и перезапустите сервис Cisco CM.

4. От страницы Serviceability перейдите к **Программным средствам> Сетевые сервисы** и перезапустите сервис TVS.

5. От страницы Serviceability перейдите к **Программным средствам> Feature Services**, задайте узел и перезапустите сервисы CTI и CM.

6. Перезагрузите телефоны так, чтобы они могли получить обновленный файл ITL.

7. Выполните предыдущие шаги для каждого абонента.

TVS

1. Перейдите к Странице администрирования операционной системы на Издателе.

2. Перейдите к **Безопасности> Управление сертификатами**, нажмите **Find**, нажмите файл **TVS.pem**, и затем нажмите **Regenerate**.

3. От страницы Serviceability перейдите к **Программным средствам> Сетевые сервисы** и перезапустите сервис TVS.

4. От страницы Serviceability перейдите к **Программным средствам> Feature Services**, задайте узел и перезапустите Сервис TFTP.

5. Перезагрузите телефоны так, чтобы они могли получить обновленный файл ITL.

6. Выполните предыдущие шаги для каждого абонента.

Удалите сертификаты

Когда вы удаляете сертификаты, гарантируете, что ранее упомянутые сервисы остановлены, и что сертификаты, которые вы удаляете, в настоящее время не используются или фактически истекаются.

Кроме того, всегда проверяйте всю информацию в сертификате, потому что вы не можете сохранить его после удаления.