

CallManager 認証満了および削除

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[解決策](#)

[CUCM バージョン 8.x および それ 以降のための認証再生](#)

[CAPF](#)

[IPSec](#)

[CM](#)

[TVS](#)

[削除認証](#)

概要

この資料は **CertExpiryEmergency** を受け取る場所 Cisco Unified CallManager (CM) における問題を記述したものです: 実時間監視 ツール (RTMT) クライアントからの**認証終止 EMERGENCY_ALARM** アラーム メッセージは問題に、ソリューションを提供し。

前提条件

要件

Cisco は 9.x によって CM バージョン 6.x の知識があること、そして推奨しますシステムことを:

- Domain Name System (DNS) 設定を持っていません。これは資料の簡単にするためにされますが、多くのシステムに設定される良いそれがあります。
- 期限切れ、再生する必要があるまたは切れることになっている認証を持っています認証。

注: システムの IP アドレスはホスト名が IP アドレスを変更した後生成する新しいですか再生コマンドを入力する場合重要ではありません。

使用するコンポーネント

この文書に記載されている情報は管理 ページとの Cisco CM サーバに基づいています。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

問題

CertExpiryEmergency を受け取ります: CM の RTMT からの**認証終止 EMERGENCY_ALARM** アラーム メッセージ:

```
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
```

解決策

CM アラーム メッセージ問題を解決するためにこのセクションで情報を使用して下さい。

1. CM から統一されたサービスリテイ ページ GUI は **Tools > Control Center** に、**-ネットワークサービス** ナビゲート します。
2. クラスタのサーバすべての **Cisco 認証終止モニタ**および **Cisco 認証 変更通知** サービスを停止して下さい:

Control Center - Network Services Related Links: Service Activation

Start Stop Restart Refresh Page

Status: Ready

Select Server: Server: 10.201.192.238 Go

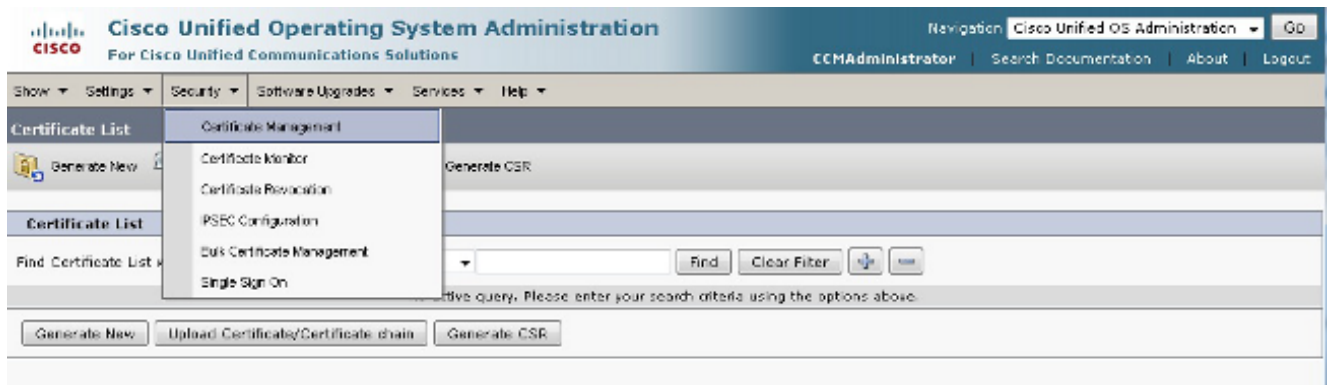
Performance and Monitoring

Service Name	Status	Start Time	Up Time
Cisco CallManager Serviceability RTMT	Running	Wed Nov 6 12:41:03 2013	20 days 12:28:49
Cisco RTMT Reporter Servlet	Running	Wed Nov 6 12:41:01 2013	20 days 12:28:51
Cisco Log Partition Monitoring Tool	Running	Wed Nov 6 12:32:40 2013	20 days 12:37:09
Cisco Tomcat Stats Servlet	Running	Wed Nov 6 12:41:01 2013	20 days 12:28:51
Cisco RJS Data Collector	Running	Wed Nov 6 12:33:00 2013	20 days 12:36:52
Cisco AMC Service	Running	Wed Nov 6 12:33:01 2013	20 days 12:36:51
Cisco Audit Event Service	Running	Wed Nov 6 12:33:05 2013	20 days 12:36:47

Platform Services

Service Name	Status	Start Time	Up Time
Platform Administrative web Service	Running	Wed Nov 6 12:41:03 2013	20 days 12:28:49
A Cisco DB	Running	Wed Nov 6 12:32:26 2013	20 days 12:37:26
A Cisco DB Replicator	Running	Wed Nov 6 12:32:27 2013	20 days 12:37:25
SNMP Master Agent	Running	Wed Nov 6 12:32:32 2013	20 days 12:37:20
MIB2 Agent	Running	Wed Nov 6 12:32:33 2013	20 days 12:37:19
Host Resources Agent	Running	Wed Nov 6 12:32:34 2013	20 days 12:37:18
System Application Agent	Running	Wed Nov 6 12:32:35 2013	20 days 12:37:17
Cisco CDP Agent	Running	Wed Nov 6 12:32:36 2013	20 days 12:37:16
Cisco Syslog Agent	Running	Wed Nov 6 12:32:37 2013	20 days 12:37:15
Cisco Certificate Expiry Monitor	Running	Wed Nov 6 12:32:32 2013	20 days 12:37:20
Cisco Certificate Change Notification	Running	Wed Nov 6 12:32:33 2013	20 days 12:37:19
Cisco ELM Client Service	Running	Wed Nov 6 12:41:01 2013	20 days 12:28:51

3. Operating System (OS) 管理 GUI から、この画面 表示は**セキュリティ > Certificate Management** にナビゲートし:



4. 特定のサーバの認証すべてを表示するために『Find』 をクリックして下さい:

Certificate List (1 - 21 of 21) Rows per Page 50

Certificate Name	Certificate Type	PEM File	.DER File	Description
tomcat	certs	tomcat.pem	tomcat.der	Self-signed certificate generated by system
ipsecc	certs	ipsecc.pem	ipsecc.der	Self-signed certificate generated by system
tomcat-trust	trust-certs	CM912sub.pem	CM912sub.der	Trust Certificate
tomcat-trust	trust-certs	CM912.pem	CM912.der	Trust Certificate
tomcat-trust	trust-certs	VeriSign Class 3 Secure Server CA - G3.pem	VeriSign Class 3 Secure Server CA - G3.der	Call Home Server Certificate
ipsecc-trust	trust-certs	CM912.pem	CM912.der	Trust Certificate
CallManager	certs	CallManager.pem	CallManager.der	Self-signed certificate generated by system
CAPF	certs	CAPF.pem	CAPF.der	Self-signed certificate generated by

5. 認証 (Tomcat 認証この場合) をクリックし、次のイメージで強調表示されるように日付を見て下さい。Tomcat 認証に関しては、サーバが CCMAdmin ページ ログインのためにサードパーティ認証を使用するかどうか確認して下さい。ブラウザからのページにログインするときこれをチェックできます。

注: それがサードパーティ署名入り認証である場合、[CCMAdmin Web GUI 認証](#) Cisco サポート コミュニティ 技術情報を [アップロードする CUCM](#) を参照し、Tomcat 再生成の後でステップを完了して下さい。

Certificate Configuration Related Links: [Back To Find/List](#) Go

Status: Ready

Certificate Settings

File Name: tomcat.pem
 Certificate Name: tomcat
 Certificate Type: certs
 Certificate Group: product-cpi
 Description: Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 144622723=10737167=50639921725543411972
  Signature Algorithm: SHA1withRSA (1.2.840.113549.1.1.5)
  Issuer Name: L=roh, ST=tx, CN=CM912, OU=tao, O=cisco, C=US
  Validity From: Tue Aug 13 17:15:08 CDT 2013
  To: Sun Aug 12 17:15:07 CDT 2013
  Subject Name: L=roh, ST=tx, CN=CM912, OU=tao, O=cisco, C=US
  Key: RSA (1.2.840.113549.1.1.1)
  Key value:
]
```

6. パブリッシャの証明書管理 ページにナビゲートして下さい。見つけ、tomcat.pem ファイルをクリックし、それから再生をクリックして下さい:

The screenshot shows the Cisco Unified Operating System Administration interface. On the left, the 'Certificate List' page displays a table of certificates. On the right, a 'Generate Certificate' dialog box is open, showing a dropdown menu for 'Certificate Name' with 'tomcat' selected.

Certificate Name	Certificate Type	PEM File
tomcat	certs	tomcat.pem
ipsec	certs	ipsec.pem
tomcat-trust	trust-certs	CM912sub.pem
tomcat-trust	trust-certs	CM912.pem
tomcat-trust	trust-certs	Version: Class 3 Secure Server Certificate.pem
ipsec-trust	trust-certs	CM912.pem
CallManager	certs	CallManager.pem
CAPF	certs	CAPF.pem

7. そのノードの Tomcat サービスを再開し、CLI をノードに開き、utils サービス再始動 Cisco Tomcat コマンドを入力するため。認証が生成されれば認証が現在であることを確認するために、メッセージはポップアップします。

注: 認証はまた前の手順に説明がある日付情報によって確認されます。

The screenshot shows the 'Certificate Configuration' page in the Cisco Unified Operating System Administration interface. It displays the status of a certificate regeneration and the details of the certificate settings and file data.

Status: Success: certificate regenerated. Perform a Disaster Recovery backup so the latest backup contains the regenerated certificate.

Certificate Settings:

- File Name: tomcat.pem
- Certificate Name: tomcat
- Certificate Type: certs
- Certificate Group: product-cpi
- Description: Self-signed certificate generated by system

Certificate File Data:

```
[
Version: V3
Serial Number: 130594591470012523210557240109039036305
Signature Algorithm: SHA1withRSA (1.2.840.113549.1.1.5)
Issuer Name: L=rch, ST=tx, CN=CM912, OU=tao, O=cisco, C=US
Validity From: Wed Nov 27 01:25:45 CST 2013
To: Mon Nov 26 01:25:44 CST 2018
Subject Name: L=rch, ST=tx, CN=CM912, OU=tao, O=cisco, C=US
Key: RSA (1.2.840.113549.1.1.1)
Key usage:
criticality: true
usage: digital signature, key encipherment, key agreement, data encipherment, data signature, key
exchange, key transport, non-repudiation, non-repudiation of origin, non-repudiation of receipt, non-repudiation of
signature
]
```

8. Tomcat 認証を再生するためにクラスタのサブスクリバのそれぞれのためのこのプロセスを完了して下さい。

CUCM バージョン 8.x および それ 以降のための認証再生

Cisco Unified Communications Manager (CUCM) バージョン 8.x および それ 以降のための期限の切れた 認証を再生するためにこのセクションで情報を使用して下さい。

注: サービスを再開し、プロセスの電話をリポートする必要がありますので、正常な営業時間後

に認証を再生して下さい。

CAPF

認証局 (CA) プロキシ 機能 (CAPF) 再生成に関しては、クラスタがセキュア クラスタ モードにないようにして下さい: **クラスタ セキュア モード**のための CM 管理Webページおよび検索からの **System > Enterprise Parameters** にナビゲートして下さい。値が 0 である場合、クラスタはセキュア クラスタ モードにありません。値がゼロ以外数である場合、クラスタはセキュア モードにあり、CTL ファイルをアップデートするために Certificate trust list (CTL) クライアントを使用して下さい。

注: 詳細については [IP Phone セキュリティおよび CTL \(証明書信頼リスト \)](#) Cisco サポート コミュニティ技術情報を参照して下さい。

1. パブリッシャから、証明書管理 ページにナビゲート して下さい。
2. **CAPF.pem** ファイルを開き、再生をクリックして下さい。これは認証を更新し、2 つの新しい信頼ファイルを作成します: 1 つは CM 信頼であり、他は CAPF 信頼です。
3. サービスビリティ ページから、**ツール > 機能 サービス**へのナビゲート。
4. CAPF サービスが**機能 サービス**の下でアクティブになる場合、サービスを再開して下さい。CAPF サービスがアクティブにならない場合、再始動は必要ではありません。
5. **ツール > サービスビリティ** ページからの**ネットワークサービス**にナビゲートし、信頼確認サービス (TV) サービスを再開して下さい。
6. **ツール > サービスビリティ** ページからの**機能 サービス**にナビゲートし、ノードを規定し、TFTPサービスを再起動して下さい。
7. サービスが再開されたら、更新済識別信頼リスト (ITL) ファイルを取得できるように電話をリポートして下さい。
8. 証明書管理 ページに戻り、2 つの古い信頼ファイルを削除して下さい。これらはエラー出力から受け取った 2 つの切らされた信頼ファイルです。新しい認証に **CAPF.pem** ファイルと一致するシリアル番号があります。
9. 各サブスクリバのための前の手順を完了して下さい。

IPSec

インターネット プロトコル セキュリティ (IPSec) 認証はディザスタ リカバリ失敗 (DRF) マスターおよびローカルに影響を与えます、バックアップと復元機能を取扱う。

1. パブリッシャの OS 管理 ページへのナビゲート。
2. **セキュリティ > Certificate Management** にナビゲートし、**IPSEC.pem** ファイルをクリック

して下さい。

3. 信頼ファイルをアップデートするために再生をクリックして下さい。
4. 認証が再生したことサーバをリブートして下さい。各サービスが後あらゆる認証のあらゆる再生成/アップデート再開する必要があったのでこれが必要となります。ただし全体のノードをリブートする、IPSec にサービス再始動機能が以外ありません。他の認証がアップデートされることを/再生する必要のある場合すべてのステップを完了し、次にノードをリブートして下さい結局認証が処理された。これはサーバが truststore でアップデートされるすべての認証を持つようにおよびきちんと読取るようにします。

CM

1. パブリッシャの OS 管理 ページへのナビゲート。
2. 証明書管理 ページにナビゲートし、『Find』をクリックし、CallManager.pem ファイルをクリックし、それから再生をクリックして下さい。
3. ツール > サービスビリティ ページの機能サービスにナビゲートし、指定されたノードを見つけ、Cisco CM サービスを再開して下さい。
4. サービスビリティ ページから、ツール > ネットワークサービスにナビゲートし、TV サービスを再開して下さい。
5. サービスビリティ ページから、ツール > 機能 サービスにナビゲートし、ノードを規定し、CM および CTI サービスを再開して下さい。
6. 更新済 ITL ファイルを取得できるように電話をリブートして下さい。
7. 各サブスクリバのための前の手順を完了して下さい。

TVS

1. パブリッシャの OS 管理 ページへのナビゲート。
2. セキュリティ > Certificate Management にナビゲートし、『Find』をクリックし、TVS.pem ファイルをクリックし、それから再生をクリックして下さい。
3. サービスビリティ ページから、ツール > ネットワークサービスにナビゲートし、TV サービスを再開して下さい。
4. サービスビリティ ページから、ツール > 機能 サービスにナビゲートし、ノードを規定し、TFTPサービスを再起動して下さい。
5. 更新済 ITL ファイルを取得できるように電話をリブートして下さい。
6. 各サブスクリバのための前の手順を完了して下さい。

認証を削除して下さい

認証を削除するとき、以前に述べられたサービスが停止すること、そして確認して下さい現在実際に期限切れ使用されないし、ではないことを削除する認証ことを。

また削除の後でそれを保存することができないので、認証内の情報すべてを常にチェックして下さい。