Regeneración del certificado CUCM/proceso de renovación

Contenido

Introducción

Este documento proporciona haber recomendado, procedimiento paso a paso regenerar los Certificados usados en la versión 8.x del administrador de las Comunicaciones unificadas de Cisco (CUCM) y posterior. La Seguridad por abandono ofrece (la ITL) y el Mezclado-MODE (CTL) es también se cubra para evitar cualquier caída del sistema indeseada. Por ejemplo, cómo evitar los problemas o los teléfonos del registro de teléfono que no validan los cambios de configuración o los firmwares.

> **Caution**: Se recomienda siempre para completar la regeneración del certificado en una ventana de mantenimiento.

Información general

Este documento discute el proceso de la regeneración del certificado para estos servicios:

- CallManager

- CAPF (función de proxy del Certificate Authority)
- IPSec
- Tomcat
- TV (servicio de la verificación de la confianza)
- ITLRecovery (solamente para CUCM 10.X y posterior)
- teléfono-VPN-confianza
- teléfono-sast-confianza
- teléfono-confianza
- teléfono-CTL-confianza

Así como estos Certificados del teléfono:

- LSC (localmente - Certificados significativos)
- MIC (Certificados instalados fabricante)

Componentes Utilizados

Todas las salidas y el screenshots mostrados en este documento se basan en la versión 9.1(2)SU2a CUCM, no obstante el actual procedimiento se puede utilizar con la versión 8.x CUCM y posterior. Las diferencias que son específico de la versión se mencionan en las secciones apropiadas.

La información en este documento fue basada en los dispositivos en un ambiente de laboratorio que comenzó con una configuración despejada (predeterminada). Si su red está viva, aseegurese que usted entiende el impacto potencial del comando any y acción realizada.

Cuándo regenerar los Certificados

La mayor parte de los Certificados usados en CUCM después de que una instalación desde el inicio sea certificados autofirmados publicados, por abandono, por cinco años. Observe que el rango de tiempo de cinco años no se puede modificar actualmente para ser un menor alcance del tiempo en CUCM. Sin embargo, un Certificate Authority (CA) puede publicar los Certificados para casi cualquier rango del tiempo.

Hay también algunos certificados confiables (tales como CAPF-confianza y CallManager-confianza) que se cargan y tienen un período de validez más largo. Por ejemplo, “Cisco que fabrica el certificado de CA” se proporciona en los almacenes de la confianza CUCM a las características específicas y no expirará hasta el año 2029.

Los Certificados deben ser regenerados antes de que expiren. Cuando los Certificados están a punto de expirar usted recibirá las advertencias en RTMT (el visor de Syslog) y un correo electrónico con la notificación será enviado si está configurado.

Un ejemplo de una notificación del vencimiento del certificado que detalle el certificado del "CUCM01.der" expirará el “lunes el 19 de mayo el 14:46" en el servidor CUCM02 en el almacén “Tomcat-confianza " de la confianza se muestra aquí:

```
At Fri Sep 05 02:00:56 CEST 2014 on node 192.168.1.2, the following
SyslogSeverityMatchFound events generated:
```

```
SeverityMatch : Critical

MatchedEvent : Sep 5 02:00:06 CUCM02 local7 2 : 864: CUCM02.localdomain:
Sep 05 2014 00:00:06.433 UTC : %UC_CERT-2-CertValidfor7days:
%[Message=Certificate expiration Notification. Certificate name:CUCM01.der
Unit:tomcat-trust Type:own-cert Expiration:Mon May 19 14:46:]
[AppID=Cisco Certificate Monitor][ClusterID=][NodeID=CUCM02]:
Alarm to indicate that Certificate has Expired or Expires in less than seven days

AppID : Cisco Syslog Agent

ClusterID :

NodeID : CUCM02

TimeStamp : Fri Sep 05 02:00:16 CEST 2014
```

Si los Certificados del servicio (los almacenes de certificados con los cuales no se etiquetan "-confianza") se expiran ya es todavía posible regenerarlos. Tenga presente que los certificados vencidos pudieron tener un impacto en sus funciones CUCM, dependiente sobre la configuración del cluster. Las consideraciones se discuten en las siguientes secciones.

Mantenga el impacto por el almacén de certificados

Es crítico para las buenas funciones del sistema tener todos los Certificados actualizados a través del cluster CUCM. Si sus Certificados son expirados o inválido puede ser que afecten perceptiblemente al funcionamiento normal del sistema. Una lista de problemas potenciales que usted puede ser que tenga cuando los Certificados específicos uces de los son inválidos o expirado se muestra aquí. El impacto pudo diferenciar dependiente sobre su configuración del sistema.

CallManager.pem

- Los teléfonos cifrados/autenticados no se registran.
- TFTP no confiado en (los teléfonos no validan los archivos de configuración firmados y/o los archivos ITL).
- Los servicios telefónicos pudieron ser afectados.
- Los trunks o los recursos del medio seguros (Bridge de conferencia, Media Termination Point (MTP) del Session Initiation Protocol (SIP), Xcoders, y así sucesivamente) no se registrarán ni funcionarán.
- La petición AXL falla.

Tomcat.pem

- Los teléfonos no pueden acceder los servicios HTTP recibidos en el nodo CUCM, tal como Corporate Directory (Directorio corporativo).
- Problemas de la red GUI CUCM, tales como incapaz de acceder las páginas del servicio de otros Nodos en el cluster.
- El cluster de la cruz de la movilidad de la extensión o de la movilidad de la extensión publica.

CAPF.pem

- Los teléfonos no autentican para el teléfono VPN, el 802.1x, o el proxy del teléfono.
- No puede publicar los Certificados LSC para los teléfonos.
- Los archivos de configuración cifrados no funcionan.

IPSec.pem

- El marco de la recuperación del sistema de la Recuperación tras desastres (DR) /Disaster (DRF) no pudo funcionar correctamente.
- Los túneles IPsec al gateway (GW) a otros clusteres CUCM no funcionan.

TV (servicio de la verificación de la confianza)

- El teléfono no puede autenticar el servicio HTTPS. El teléfono no puede autenticar los archivos de configuración (éste puede afectar casi todo en CUCM).

teléfono-VPN-confianza

- El teléfono VPN no funcionará, porque el HTTPS URL VPN no puede ser autenticado.

  Note: Si no existe esto no se preocupe. Esto está solamente para las configuraciones específicas.

teléfono-sast-confianza

- CTL/eTokens anterior no podrá poner al día o modificar el CTL.

  Note: Si no existe esto no se preocupe. Esto está solamente para las configuraciones específicas.

teléfono-confianza y teléfono-CTL-confianza

- El Correo de voz visual con el Unity o el Unity Connection no trabajará.

  Note: Si no existe esto no se preocupe. Esto está solamente para las configuraciones específicas.

LSC y MIC

- Los teléfonos no se registran, teléfono no autentican para llamar por teléfono al VPN, al proxy del teléfono, o al 802.1x.

  Note: Los MIC están en la mayoría de los modelos del teléfono por abandono. Los LSC son firmados por el CAPF y duran cinco años por abandono. Los softwares cliente tales como CIPC (Cisco IP Communicator) y Jabber no hacen un MIC instalar.

Cree los DR de reserva

Se recomienda para crear los DR de reserva antes de que usted realice cualquier cambio importante como esto. Los respaldos CUCM DRF sostendrán todos los Certificados en el cluster. Todo el respaldo/los procedimientos de restaurar DR se puede encontrar en Cisco “guía de administración del sistema de la Recuperación tras desastres para el administrador de las Comunicaciones unificadas de Cisco”.

Caution: Tenga en cuenta el Id. de bug Cisco CSCtn50405, respaldo CUCM DRF hace no los Certificados de reserva.

Determine si el cluster está en el Mezclado-MODE

Para determinar si usted ejecuta un cluster CTL/Secure/Mixed-Mode, elija la **administración unificada Cisco CM > el System (Sistema) > Enterprise Parameters (Parámetros Enterprise) > al modo seguro del cluster (0 == NON-seguros; 1 modo mezclado del ==)**.

Si el cluster está en el Mezclado-MODE

Si usted ejecuta un cluster CUCM en el Mezclado-MODE, éste significa que el archivo CTL necesita ser después de todo cambios actualizados del certificado. El procedimiento en cómo hacer esto está dentro de la documentación de la guía de la Seguridad de Cisco. Sin embargo, esté seguro que usted hace que por lo menos uno eToken del lanzamiento original de la característica Mezclado-MODE y la contraseña del eToken está sabida.

> **Note**: Una actualización del CTL no sucede automáticamente (como hace en caso del archivo ITL). Necesita ser completada manualmente por el administrador con el cliente CTL o el comando CLI.

En CUCM 10.X y posterior usted puede poner el cluster en el Mezclado-MODE de dos maneras:

- Comando CLI - si este método se utiliza entonces su archivo CTL se firma con el certificado CallManager.pem del servidor editor.

```
admin:show ctl
The checksum value of the CTL file:
0c05655de63fe2a042cf252d96c6d609(MD5)
8c92d1a569f7263cf4485812366e66e3b503a2f5(SHA1)

Length of CTL file: 4947
The CTL File was last modified on Fri Mar 06 19:45:13 CET 2015

[...]

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1156
2 DNSNAME 16 cucm-1051-a-pub
3 SUBJECTNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 62 CN=cucm-1051-a-pub;OU=TAC;O=Cisco;L=Krakow;
ST=Malopolska;C=PL
6 SERIALNUMBER 16 70:CA:F6:4E:09:07:51:B9:DF:22:F4:9F:75:4F:C5:BB
7 PUBLICKEY 140
8 SIGNATURE 128
9 CERTIFICATE 694 E9 D4 33 64 5B C8 8C ED 51 4D 8F E5 EA 5B 6D 21
A5 A3 8C 9C (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

- Cliente CTL - si este método se utiliza entonces su archivo CTL se firma con uno de los eTokens del hardware.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Note: Usted puede moverse entre el método usado con el modo mezclado CUCM con Tokenless CTL.

El dependiente sobre el método usado para asegurar su cluster, un procedimiento apropiado de la actualización CTL necesita ser utilizado. Vuelva a efectuar al cliente CTL o ingrese el comando de **CTLfile de la actualización del ctl del utils del** CLI.

Verifique la Seguridad por abandono en el cluster

La evitación de los problemas ITL es importante, porque los problemas ITL pueden hacer muchas características fallar o el teléfono rechazará seguir cualquier cambio a las configuraciones. Los problemas ITL se pueden evitar de estas dos maneras.

Utilice “preparan el cluster para la restauración no actualizada a la característica del pre 8.0"

Esta característica “esconde” hacia fuera su ITL en todos los servidores, así que los teléfonos confiarán en a cualquier servidor TFTP. Los servicios telefónicos (por ejemplo, movilidad de la extensión) no trabajarán cuando este parámetro se fija para verdad. Sin embargo, los usuarios podrán continuar haciendo y recibiendo las llamadas telefónicas básicas.

Note: Un cambio a este parámetro hace TODOS LOS TELÉFONOS REAJUSTAR.

Una vez que se fija esta característica, todos los servidores TFTP necesitan ser recomenzados (para suministrar la nueva ITL) y todos los teléfonos necesitan ser reajustar para forzarla a pedir la nueva ITL “en blanco”. Una vez que se completan los cambios del certificado y han recomenzado a todos los servicios necesarios, esta característica se puede fijar de nuevo a “falso”, servicio TFTP recomenzado, y la restauración del teléfono (así que el teléfono puede obtener el archivo válido ITL). Entonces todas las características continuarán trabajando como hicieron previamente.

Certificados regenerados en el orden concreto

Este procedimiento proporciona a un servidor TFTP con un archivo válido/actualizado ITL de un

servidor TFTP de confianza que esté disponible.

1. Pare servicio TFTP en el servidor TFTP primario.
2. Realice los cambios en los Certificados de servidor TFTP primarios (según las necesidades).
3. Reajuste los teléfonos (para conseguir un nuevo archivo ITL del servidor TFTP secundario) - el dependiente sobre quien se regeneran los Certificados, esto pudo suceder automáticamente.
4. Una vez que los teléfonos han vuelto, encienda al servidor TFTP primario servicio TFTP.
5. Realice los cambios del certificado en el servidor TFTP secundario.
6. Reajuste los teléfonos (para conseguir un nuevo archivo ITL del servidor TFTP primario).

> **Caution**: No edite los Certificados en ambos servidores TFTP al mismo tiempo. Esto da a teléfono servidor TFTP para confiar en y requiere al administrador local quitar manualmente la ITL de todos los teléfonos.

Quite y regenere los Certificados en CUCM

Solamente los Certificados del servicio (los almacenes de certificados con los cuales no se etiquetan “- confianza”) pueden ser regenerados. Los Certificados en los almacenes de la confianza (los almacenes de certificados con los cuales se etiquetan “- confianza”) necesitan ser borrados, pues no pueden ser regenerados.

> **Caution**: Sea consciente del Id. de bug Cisco CSCut58407 - Los dispositivos no deben recomenzar cuando se quita el CAPF/CallManager/TV-confianza.

Después de todo certifique las modificaciones, el servicio respectivo necesita ser recomenzado para adquirir el cambio. Esto se cubre en después de la regeneración/del retiro de la sección de los Certificados.

> **Caution**: Sea consciente del Id. de bug Cisco CSCto86463 - Los Certificados borrados reaparecen, incapaz de quitar los Certificados de CUCM. Esto es un problema donde los Certificados borrados continúan reapareciendo después del retiro. Siga la solución alternativa en el defecto.

Regenere los Certificados vía el CLI

> **Caution**: Las regeneraciones de los Certificados accionan una actualización automática de los archivos ITL dentro del cluster, que acciona una restauración cluster-ancha del Soft Phone para permitir que los teléfonos accionen una actualización de su ITL local. Esto se centra en el CAPF y las regeneraciones del certificado del CallManager, pero puede ocurrir con otros almacenes de certificados dentro de CUCM, tal como Tomcat.

CAPF regenerado

Sobre la regeneración, el certificado del CAPF se carga automáticamente CAPF-confianza y

CallManager-confianza. También, el CAPF tiene siempre una encabezado única del asunto, así los Certificados previamente usados del CAPF serán conservados y utilizados para la autenticación.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

> **Note**: Si un certificado del CAPF consigue expirado, los teléfonos que utilizan el LSC no podrán registrarse a CUCM porque CUCM rechaza su certificado. Sin embargo, usted puede todavía generar un nuevo LSC para el teléfono con el nuevo certificado del CAPF. Cuando usted reinicia el teléfono que descarga la configuración y entonces entra en contacto el CAPF para poner al día el LSC. Después de que el LSC sea actualizado, el teléfono se registra como él deba. Esto trabaja mientras un nuevo certificado del CAPF esté en el archivo ITL y el teléfono descargados y confiara en el certificado que lo firmó (callmanager.pem).

CallManager regenerado

Sobre la regeneración, el CallManager se carga automáticamente CallManager-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
```

```
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPSec regenerado

Sobre la regeneración, el certificado del IPSec se carga automáticamente IPSec-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat regenerado

Sobre la regeneración, el certificado de Tomcat se carga automáticamente Tomcat-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
```

```
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TV regenerados

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Qué a esperar

Cuando usted regenera los Certificados vía el CLI, le piden verificar este cambio. Tipo **sí** y Presione ENTER.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```

This etoken was used to sign the CTL file.

Quite los Certificados vía el CLI

Quite los Certificados de la CAPF-confianza

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Quite los Certificados de la CallManager-confianza

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Quite los Certificados de la IPSec-confianza

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Quite los Certificados de la Tomcat-confianza

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Quite los Certificados de la TV-confianza

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Regenere los Certificados vía la red GUI

Regenere el CAPF

Sobre la regeneración, el certificado del CAPF se carga automáticamente CAPF-confianza y CallManager-confianza. También, el certificado del CAPF tiene siempre una encabezado única del asunto, así los Certificados previamente usados del CAPF se conservan y se utilizan para la autenticación.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

CallManager regenerado

Sobre la regeneración, el certificado del CAPF se carga automáticamente CallManager-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)
```

```
Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

IPSec regenerado

Sobre la regeneración, el certificado del IPSec se carga automáticamente IPSec-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Tomcat regenerado

Sobre la regeneración, el certificado de Tomcat se carga automáticamente Tomcat-confianza.

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015
```

```
[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

TV regenerados

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.
```

Quite los Certificados vía la red GUI

```
admin:show ctl
The checksum value of the CTL file:
256a661f4630cd86ef460db5aad4e91c(MD5)
3d56cc01476000686f007aac6c278ed9059fc124(SHA1)

Length of CTL file: 5728
The CTL File was last modified on Fri Mar 06 21:48:48 CET 2015

[...]
CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
```

```
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN008580ef ";ou=IPCBU;o="Cisco Systems
4 FUNCTION 2 System Administrator Security Token
5 ISSUERNAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
6 SERIALNUMBER 10 83:E9:08:00:00:00:55:45:AF:31
7 PUBLICKEY 140
9 CERTIFICATE 902 85 CD 5D AD EA FC 34 B8 3E 2F F2 CB 9C 76 B0 93
3E 8B 3A 4F (SHA1 Hash HEX)
10 IPADDRESS 4
```

This etoken was used to sign the CTL file.

Después de la regeneración/del retiro de los Certificados

Después de que usted quite o regenere un certificado de un almacén de certificados, el servicio respectivo necesita ser recomenzado para adquirir el cambio.

Salve	Mantenga para recomenzar	Cómo (== CLI del C; Red GUI del == W)
Tomcat	Tomcat	C: utils service restart Cisco Tomcat G: Cisco unificó la utilidad > el Tools (Herramientas) > Contro Center (Centro de control) - La característica mantiene > (serv selecto) > “Cisco CallManager selecto” > reinicio
CallManager	CallManager; TFTP	Y G: Cisco unificó la utilidad > el Tools (Herramientas) > Contro Center (Centro de control) - La característica mantiene > (serv selecto) > “Cisco selecto Tftp” > reinicio
CAPF	CAPF (en Publisher solamente)	G: Cisco unificó la utilidad > el Tools (Herramientas) > Contro Center (Centro de control) - La característica mantiene > (serv selecto) > “función de proxy selecta del Certificate Authority de Cisco” > reinicio
TV	Servicio de la verificación de la confianza (en el servidor correspondiente)	G: Cisco unificó la utilidad > el Tools (Herramientas) > Control Center (Centro de control) - Servicios de red > (servidor select “servicio selecto de la verificación de la confianza de Cisco” > reinicio
IPSec	Local de Cisco DRF (en todos los Nodos); Master de Cisco DRF (en Publisher)	C: Local de Cisco DRF del reinicio del servicio del utils Y C: master de Cisco DRF del reinicio del servicio del utils

Instale/la actualización LSC en el teléfono

Si se ha regenerado el certificado del CAPF, después los Certificados LSC para todos los teléfonos en el cluster necesitan ser puestos al día con el LSC firmado por el nuevo certificado del CAPF.

1. Elija la **utilidad CUCM > la activación del servicio**. Active el proveedor de Cisco CTL y la función de proxy del Certificate Authority de Cisco en el servidor editor.
2. Del ccmadmin CUCM, elija el **Device (Dispositivo) > Phone (Teléfono).** Escoja el teléfono del IP que usted quiere provision un LSC encendido.
3. En la página de la configuración del dispositivo bajo la operación del certificado, elija **instalan/actualización > por la cadena nula**.
4. Salve la Configuración del teléfono en el ccmadmin y elija **aplican los Config**.

Si el teléfono tiene problema con la instalación del LSC, complete estas acciones en el teléfono:

Cuando el teléfono reajusta, va al teléfono físico y elige las **configuraciones > (6) la Configuración**

de seguridad > (4) LSC > ** # (esta operación desbloquea el GUI y permite que continuemos al siguiente paso) **> la actualización** (la actualización no será visible hasta que usted realice el paso anterior) **> somete**.

No asigne ningunos Certificados a un teléfono a menos que sea un teléfono inalámbrico (7921/25). Los teléfonos inalámbricos utilizan las autoridades de certificación de las de otras compañías para autenticarse.

Conclusión

Si usted se ejecuta en un problema o necesita la ayuda con este procedimiento, entre en contacto el Centro de Asistencia Técnica de Cisco (TAC) para la ayuda. En este caso, mantenga su respaldo DRF disponible pues será utilizado como último recurso para restablecer el servicio si TAC no puede hacer tan con otros métodos.