Contenido

Introducción

Este documento describe cómo prevenir una situación con la versión 8.0(1) del administrador de las Comunicaciones unificadas de Cisco (CUCM) donde los millares de teléfonos deben tener sus archivos iniciales de la lista de la confianza (ITL) borrados manualmente.

Antecedentes

Con la versión 8.0(1) CUCM, la nueva Seguridad por abandono (SBD) ofrece y el uso de los archivos ITL fue introducida. Con esta nueva función, el cuidado debe ser tomado cuando usted mueve los teléfonos entre diversos clusteres CUCM. Si usted no completa los pasos apropiados, es posible encontrar una situación donde los millares de teléfonos deben manualmente tener sus archivos ITL borrados. Los teléfonos que soportan los nuevos archivos ITL descargan un archivo especial de su servidor TFTP CUCM. Una vez que un archivo ITL está instalado en un teléfono, todos los archivos de configuración futuros y las actualizaciones del archivo ITL deben ser cualquiera:

- Firmado por el certificado de servidor CCM+TFTP que está instalado actualmente en Certificate Trust List (Lista de confianza del certificado) el archivo (CTL) del teléfono (si la Seguridad del cluster con los CTL se habilita).

- Firmado por el certificado de servidor CCM+TFTP que está instalado en el archivo ITL del teléfono.

- Firmado por un certificado que exista en uno de la verificación de la confianza del servidor CUCM mantiene los almacenes de certificados (TV) que se enumeran en el archivo ITL.

Con las nuevas funciones de la Seguridad, aquí están los tres problemas que usted puede encontrar cuando usted mueve un teléfono a partir de un cluster a otro cluster:

- El archivo ITL del nuevo cluster no es firmado por el certificado actual ITL CCM+TFTP del teléfono, así que el teléfono no valida el nuevo archivo o los archivos de configuración ITL.

- Los servidores TV que se enumeran en el archivo actual ITL del teléfono no pudieron ser

accesibles cuando los teléfonos se mueven al nuevo cluster.

- Incluso si los servidores TV son accesibles para la verificación del certificado, los servidores viejos del cluster TV no pudieron tener los Certificados para el nuevo servidor.

Si se encuentran estos tres problemas, una opción posible es borrar el archivo ITL manualmente de todos los teléfonos que se muevan entre los clusteres. Esto no es una solución deseable, pues requiere esfuerzo masivo mientras que el número de teléfonos afectados aumenta.

> Consejo: Para la información adicional, refiera a la Seguridad por abandono seccionan de la guía de la Seguridad del administrador de las Comunicaciones unificadas de Cisco, la versión 8.5(1).

Problema

Ninguna cambios que un teléfono recibe con el TFTP o el HTTP de los archivos de configuración no se honran. Las opciones de configuración que son pasadas por los archivos de configuración incluyen parcialmente:

- URL (tales como la autenticación URL, directorios URL, y servicios URL, incluir la configuración interna y externa de los directorios)
- Características de la escena
- Grupos de CallManager para el registro primario y secundario

El teléfono se registra probablemente al servidor TFTP configurado por abandono, pero no se registra muy probablemente si el nuevo servidor TFTP no dirige el servicio de CallManager. Cuando un teléfono tiene un archivo incorrecto ITL para el servidor TFTP actual, los registros de la consola del teléfono muestran un mensaje similar a esto:

```
1715: ERR 16:59:35.170584 SECD: EROR:verifyFile: sgn verify file failed
</usr/ram/SEP00260BD749E9.cnf.xml>, errclass 8, errcode 19 (signer not in CTL)
1716: ERR 16:59:35.171327 SECD: EROR:verifyFile: verify FAILED,
</usr/ram/SEP00260BD749E9.cnf.xml>
```

Solución

Esta sección describe cómo emigrar el seamlessly de los teléfonos a partir de un cluster al siguiente, así como cómo borrar manualmente los archivos ITL de los teléfonos en un escenario del malo-caso.

Exportación a granel del certificado

> Nota: Este método a granel de la exportación del certificado trabaja solamente si ambos clusteres están en línea con la conectividad de red mientras que se emigran los teléfonos.

Una Solución posible, si los viejos y nuevos clusteres están en línea al mismo tiempo, es utilizar el

método a granel de la migración del certificado.

Es importante entender que los Teléfonos IP verifican cada archivo descargado contra el archivo ITL o contra un servidor TV que exista en el archivo ITL. Si el teléfono debe moverse a un nuevo cluster, el archivo ITL que los nuevos presentes del cluster se deben confiar en por el almacén de certificados TV del viejo cluster.

Complete estos pasos para implementar el método a granel de la exportación del certificado:

1. Navegue al **> Security (Seguridad) de la administración OS > al certificado del bulto**.

2. Exporte los Certificados del nuevo clúster de destino (TFTP solamente) y del cluster original a un servidor central del protocolo FTP del Secure Shell (SSH) (SFTP).

3. Funcione con el servicio de los **Certificados de la consolidación del** cluster original (TFTP solamente) en el servidor SFTP que utiliza la interfaz a granel del certificado.

4. Utilice la función **a granel del certificado del** viejo cluster de las creaciones para importar los Certificados TFTP del servidor SFTP central.

5. Recomience los servicios TV en el viejo cluster de las creaciones.

6. Utilice la opción DHCP 150, o un cierto otro método, para señalar los teléfonos al nuevo clúster de destino.

Después de que usted complete estos pasos, los teléfonos descargan el nuevo archivo ITL del clúster de destino e intentan verificarlo contra el archivo actual ITL. Puesto que el certificado no está presente en el archivo actual ITL, los teléfonos piden que el servidor viejo TV verifique la firma del nuevo archivo ITL. Los teléfonos envían una interrogación TV al viejo cluster de las creaciones en el puerto TCP 2445 para hacer esta petición.

Si el proceso del certificado trabajó correctamente, los TV mantienen las devoluciones con éxito y los teléfonos substituyen el archivo ITL del en memory por el archivo nuevamente descargado ITL. Los teléfonos pueden ahora descargar y verificar los archivos de configuración firmados del nuevo cluster.

Parámetro Enterprise de la restauración no actualizada

> Nota: Este método es solamente válido si está completado antes de que la migración del teléfono se intente y no pueda ser utilizada una vez los teléfonos esté en el *estado fallido del archivo del verificar*. Los teléfonos que soportan el servicio TV pueden potencialmente perder el acceso a los servicios seguros URL tales como Corporate Directory (Directorio corporativo) antes de que se emigren al nuevo cluster y después de que el *cluster de la preparación para la restauración no actualizada al* parámetro *pre-8.0* se fija *para verdad* en el cluster original. Emigrado una vez al nuevo cluster, los teléfonos descargan los nuevos archivos ITL, y la operación segura URL debe volver a normal.

Esta solución hace uso del *cluster de la preparación para la restauración no actualizada al* parámetro Enterprise *pre-8.0* CUCM. Una vez que este parámetro se fija *para verdad*, los teléfonos descargan un archivo especial ITL que contenga las secciones del certificado vacío TV

y TFTP.

Cuando un teléfono tiene un archivo vacío ITL, valida cualquier archivo de configuración sin signo (para las migraciones a los clusteres que funcionan con las versiones CUCM anterior que la versión 8.x) y cualquier nuevo archivo ITL (para las migraciones a los clústeres diferentes que funcionan con la versión 8.X CUCM). Para verificar el archivo vacío ITL, navegue al **> Security (Seguridad) de las configuraciones > a la lista de la confianza > a la ITL**. Las entradas vacías aparecen donde estaban los viejos TV y servidores TFTP.

Los teléfonos deben tener acceso a los servidores viejos CUCM solamente mientras los toma para descargar la nueva, vacía ITL clasifían. Una vez que el teléfono tiene un archivo vacío ITL, los servidores viejos pueden ser desarmados, ser accionados abajo, o ser reconstruidos (dependiente sobre sus requisitos comerciales).

> Consejo: Para la información adicional, refiera a rodar detrás el cluster a una sección de la versión Pre-8.0 de la guía de la Seguridad del administrador de las Comunicaciones unificadas de Cisco, la versión 8.5(1).

Tokenes de seguridad del hardware (KEY-CCM-ADMIN-K9=)

Si los tokenes de seguridad del hardware (número de producto **KEY-CCM-ADMIN-K9=**) se han utilizado para generar un CTL en los viejos y nuevos clusteres, los teléfonos pueden emigrar libremente entre los clusteres, mientras por lo menos uno de los mismos tokens del hardware fuera utilizado en los viejos y nuevos clusteres.

Cuando un teléfono que tiene un CTL del viejo cluster se mueve al nuevo cluster, valida el CTL del nuevo cluster, pues el nuevo CTL contiene un certificado del token de seguridad que haga juego el del CTL actual. Porque el CTL también contiene el certificado para el servidor CCM+TFTP, los archivos ITL del nuevo cluster también son validados por el teléfono, tan allí no son ningún problema cuando usted intenta mover el teléfono entre los clusteres.

Para los teléfonos que no utilizan la característica SBD (ITLs), por ejemplo los 7960 y 7940 modelos, usted debe funcionar con al cliente CTL otra vez en el cluster original primero para agregar las nuevas entradas TFTP para los servidores TFTP del nuevo cluster antes de que usted mueva los teléfonos al nuevo cluster. Esto es porque estos modelos del teléfono no alcanzan hacia fuera para los archivos TFTP para un servidor que no esté en el CTL.

Este método requiere el hardware simbólico de la seguridad complementaria y se debe configurar en el viejo cluster. Normalmente, los tokenes de seguridad se utilizan para permitir el protocolo Real-Time Transport seguro (SRTP) en un cluster y los archivos de configuración cifrados/autenticados. Un cluster tiene una vez Seguridad habilitada con los tokenes de seguridad, usted debe quitar manualmente el CTL de cada teléfono en ese cluster (del teléfono sí mismo) para inhabilitar la Seguridad en ese cluster.

Cancelacíon manual del archivo ITL

Si sucede una cierta Falla catastrófica y la clave/el certificado TFTP es no más disponible desde el viejo cluster (esto se mantiene en un respaldo del marco de la Recuperación tras desastres (DRF)), después la única opción disponible para emigrar un teléfono a un nuevo cluster es borrar

manualmente el archivo ITL de los teléfonos.

> Nota: Este proceso diferencia para cada modelo del teléfono. Los pasos que se requieren borrar la ITL clasifían en los modelos mas comunes del teléfono se describen en esta sección, pero los pasos para otros modelos se pueden encontrar en las guías de administración del teléfono.

Complete estos pasos para borrar manualmente los archivos ITL en los teléfonos de las 7900 Series:

1. Navegue al **> Security (Seguridad) de las configuraciones > a la lista de la confianza > al archivo ITL**.
2. Ingrese **** #** para abrir las configuraciones.
3. Haga clic el **borrado**.

Para borrar manualmente los archivos ITL en los teléfonos de las 8900 o 9900 Series, navegue a las **configuraciones > a las configuraciones del administrador > las configuraciones reajustadas del > Security (Seguridad) de las configuraciones**.