Cluster CUCM cambiado del ejemplo NON-seguro mezclado de la configuración de modo del modo

Contenido

Introducción

El documento describe los pasos requeridos para cambiar al modo seguro del administrador de las Comunicaciones unificadas de Cisco (CUCM) del modo NON-seguro mezclado del modo. También muestra cómo el contenido del archivo a Certificate Trust List (Lista de confianza del certificado) (CTL) se cambia cuando se completa este movimiento.

Hay tres mayores parte para cambiar al modo seguro CUCM:

1a. Funcione con al cliente CTL y seleccione la variante deseada del modo seguro.
1b. Ingrese el comando CLI para seleccionar la variante deseada del modo seguro.
2. Recomience los servicios del Cisco CallManager y de Cisco TFTP en todos los servidores CUCM que dirijan estos servicios.
3. Recomience todos los Teléfonos IP de modo que puedan descargar la versión actualizada del archivo CTL.

> Nota: Si cambian al modo seguro del cluster del modo NON-seguro mezclado del modo el archivo CTL todavía existe en los servidores y en los teléfonos, pero el archivo CTL no contiene ningunos Certificados CCM+TFTP (servidor). Puesto que los Certificados CCM+TFTP (servidor) no existen en el archivo CTL, éste fuerza el teléfono para registrarse

como NON-seguro con CUCM.

Prerrequisitos

Requisitos

Cisco recomienda que usted tiene conocimiento de la versión 10.0(1) o posterior CUCM. Además, asegure eso:

- El servicio del proveedor CTL es ascendente y se ejecuta en todos los servidores TFTP activos en el cluster. Por abandono el servicio se ejecuta en el puerto TCP 2444, pero esto se puede modificar en la configuración del parámetro de servicio CUCM.
- Los servicios de la función de proxy del Certificate Authority (CAPF) son ascendentes y se ejecutan en el nodo de Publisher.
- La replicación de la base de datos (DB) en el cluster trabaja correctamente y los datos replegados de los servidores en el tiempo real.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Cluster de la versión 10.0.1.11900-2 CUCM de dos Nodos
- Teléfono del IP de Cisco 7975 (registrado con el Skinny Call Control Protocol (SCCP), la versión de firmware SCCP75.9-3-1SR3-1S)
- Dos tokens del Cisco Security son necesarios para fijar el cluster al modo mezclado
- Uno de los tokenes de seguridad enumerados previamente es necesario para fijar el modo NON-seguro del cluster

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Antecedentes

Para funcionar con al plugin del cliente CTL se requiere para tener acceso por lo menos a un token de seguridad que fue insertado para crear o poner al día el último archivo CTL existe en el servidor editor CUCM. Es decir por lo menos uno de los Certificados del eToken que existe en el archivo actual CTL en CUCM debe estar en el token de seguridad que se utiliza para cambiar al modo seguro.

Configurar

Cambie la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo con el cliente CTL

Complete estos pasos para cambiar la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo con el cliente CTL:

1. Obtenga un token de seguridad que usted insertó para configurar el último archivo CTL.
2. Funcione con al cliente CTL. Proporcione el nombre de host IP/el direccionamiento del Pub CUCM y de las credenciales del administrador de CCM. Haga clic en Next (Siguiente).
3. Haga clic el botón de radio NON-**seguro del modo del cluster del Cisco Unified CallManager del conjunto**. Haga clic en Next (Siguiente).
4. Inserte un token de seguridad que fue insertado para configurar el último archivo CTL y para hacer clic la **AUTORIZACIÓN**. Éste es uno de los tokens que fue utilizado para poblar la lista del certificado en CTLFile.tlv.
5. Se visualizan los detalles del token de seguridad. Haga clic en Next (Siguiente).
6. El contenido del archivo CTL se visualiza. Haga clic en Finish (Finalizar). Cuando se le pregunte para la contraseña, ingrese el **cisco123**.
7. La lista de servidores CUCM en los cuales el archivo CTL exista se visualiza. Haga clic en Done (Listo).
8. Elija la **página de administración > el System (Sistema) > Enterprise Parameters (Parámetros Enterprise) CUCM** y verifiquelos que el cluster era modo NON-seguro fijado (el "0" indica NON-seguro).
9. Recomience el TFTP y los servicios del Cisco CallManager en todos los Nodos en el cluster que dirijan estos servicios.
10. Recomience todos los Teléfonos IP de modo que puedan obtener la nueva versión del archivo CTL de CUCM TFTP.

Cambie la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo con el CLI

Esta configuración está solamente para la versión 10.X CUCM y posterior. Para fijar al modo seguro del cluster CUCM NON-seguro, ingrese el comando del conjunto-**cluster NON-seguro-MODE del ctl del utils** en Publisher CLI. Después de que esto sea completo, recomience el TFTP y los servicios del Cisco CallManager en todos los Nodos en el cluster que dirijan estos servicios.

Aquí está la muestra CLI hecha salir que muestra el uso del comando.

```
admin:utils ctl set-cluster non-secure-mode
This operation will set the cluster to non secure mode. Do you want to continue? (y/n):

Moving Cluster to Non Secure Mode
Cluster set to Non Secure Mode
Please Restart the TFTP and Cisco CallManager services on all nodes in the cluster that
run these services
admin:
```

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

Para verificar el CTLFIle.tlv, usted puede utilizar uno de dos métodos:

- Para verificar el contenido y la suma de comprobación MD5 del CTLFIle.tlv presente en el lado CUCM TFTP, ingrese el **comando del** showctl en el CUCM CLI. El archivo CTLFIle.tlv debe ser lo mismo en todos los Nodos CUCM.
- Para verificar la suma de comprobación MD5 en el teléfono del IP 7975, elija la **configuración del > Security (Seguridad) de las configuraciones > la lista de la confianza > el archivo CTL**.

  Nota: Cuando usted marca la suma de comprobación en el teléfono que usted verá el MD5 o el SHA1, dependiente sobre el tipo de teléfono.

Cluster CUCM fijado al modo seguro - Suma de comprobación del archivo CTL

```
admin:show ctl
The checksum value of the CTL file:
98784f6f6bcd5019ea165b1d2bc1372e(MD5)
9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1)
[...]
```

En el lado del teléfono del IP, usted puede ver que hace el mismo archivo CTL instalar (la suma de comprobación MD5 hace juego cuando está comparada a la salida de CUCM).

El cluster CUCM fijó el modo NON-seguro - Contenido del archivo CTL

Aquí está un ejemplo de un archivo CTL de un modo NON-seguro fijado cluster CUCM. Usted puede ver que los Certificados CCM+TFTP están vacíos y no contiene ningún contenido. El resto de los Certificados en los archivos CTL no se cambia y es exactamente lo mismo que cuando CUCM fue fijado al modo mezclado.

```
admin:show ctl
The checksum value of the CTL file:
7879e087513d0d6dfe7684388f86ee96(MD5)
be50e5f3e28e6a8f5b0a5fa90364c839fcc8a3a0(SHA1)


Length of CTL file: 3746
The CTL File was last modified on Tue Feb 24 16:37:45 CET 2015

Parse CTL File
----------------

Version: 1.2
HeaderLength: 304 (BYTES)

BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
3 SIGNERID 2 117
4 SIGNERNAME 56 cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Systems
5 SERIALNUMBER 10 3C:F9:27:00:00:00:AF:A2:DA:45
6 CANAME 42 cn=Cisco Manufacturing CA;o=Cisco Systems
7 SIGNATUREINFO 2 15
8 DIGESTALGORTITHM 1
9 SIGNATUREALGOINFO 2 8
```

```
10 SIGNATUREALGORTITHM 1
11 SIGNATUREMODULUS 1
12 SIGNATURE 128
45 ec 5 c 9e 68 6d e6
5d 4b d3 91 c2 26 cf c1
ee 8c b9 6 95 46 67 9e
19 aa b1 e9 65 af b4 67
36 7e e5 ee 60 10 b 1b
58 c1 6 64 40 cf e2 57
aa 86 73 14 ec 11 b a
3b 98 91 e2 e4 6e 4 50
ba ac 3e 53 33 1 3e a6
b7 30 0 18 ae 68 3 39
d1 41 d6 e3 af 97 55 e0
5b 90 f6 a5 79 3e 23 97
fb b8 b4 ad a8 b8 29 7c
1b 4f 61 6a 67 4d 56 d2
5f 7f 32 66 5c b2 d7 55
d9 ab 7a ba 6d b2 20 6
14 FILENAME 12
15 TIMESTAMP 4

CTL Record #:1
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 1186
2 DNSNAME 1
3 SUBJECTNAME 56 cn="SAST-ADN0054f509 ";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 3C:F9:27:00:00:00:AF:A2:DA:45
7 PUBLICKEY 140
9 CERTIFICATE 902 19 8F 07 C4 99 20 13 51 C5 AE BF 95 03 93 9F F2 CC 6D 93 90 (SHA1 Hash HEX)
10 IPADDRESS 4
This etoken was used to sign the CTL file.

CTL Record #:2
----
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 not used to sign the CTL file.

CTL Record #:3
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.153
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

CTL Record #:4
----
BYTEPOS TAG LENGTH VALUE
```

```
------- --- ------ -----
1 RECORDLENGTH 2 1004
2 DNSNAME 13 10.48.47.153
3 SUBJECTNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
4 FUNCTION 2 CAPF
5 ISSUERNAME 60 CN=CAPF-e9037b69;OU=TAC;O=Cisco;L=Krakow;ST=Malopolska;C=PL
6 SERIALNUMBER 16 79:59:16:C1:54:AF:31:0C:0F:AE:EA:97:2E:08:1B:31
7 PUBLICKEY 140
9 CERTIFICATE 680 A0 A6 FC F5 FE 86 16 C1 DD D5 B7 57 38 9A 03 1C F7 7E FC 07 (SHA1 Hash HEX)
10 IPADDRESS 4

CTL Record #:5
----
BYTEPOS TAG LENGTH VALUE
------- --- ------ -----
1 RECORDLENGTH 2 33
2 DNSNAME 13 10.48.47.154
4 FUNCTION 2 CCM+TFTP
10 IPADDRESS 4

The CTL file was verified successfully.

admin:
```

En el lado del teléfono del IP, después de que fuera recomenzado y descargara la versión del archivo actualizada CTL, usted puede ver que la suma de comprobación MD5 hace juego cuando está comparada a la salida de CUCM.

Ponga la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo cuando se pierden los Token USB

Los tokenes de seguridad para los clusteres asegurados podían ser perdidos. En esa situación, usted necesita considerar estos dos escenarios:

- El cluster funciona con la versión 10.0.1 o posterior
- El cluster funciona con una versión anterior que 10.x

En el primer escenario, complete el procedimiento descrito en el cambio la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo con la sección CLI para recuperarse del problema. Puesto que ese comando CLI no requiere un token CTL, podría ser utilizado incluso si el cluster fue puesto en el modo mezclado con el cliente CTL.

La situación consigue más compleja cuando una versión que 10.x de CUCM es anterior funcionando. Si usted pierde u olvida la contraseña de uno de los tokens, usted puede todavía utilizar el otro para funcionar con al cliente CTL con los archivos actuales CTL. Se recomienda altamente para obtener otro eToken y lo agrega al archivo CTL cuanto antes por la Redundancia. Si usted pierde u olvida las contraseñas para todos los eTokens enumerados en su archivo CTL, usted necesita conseguir un nuevo par de eTokens y funcionar con un procedimiento manual según lo explicado aquí.

1. Ingrese el **comando del tftp CTLFile.tlv de la cancelación del archivo** para borrar el archivo CTL de todos los servidores TFTP.
```
admin:file delete tftp CTLFile.tlv
Delete the File CTLFile.tlv?
Enter "y" followed by return to continue: y
files: found = 1, deleted = 1

admin:show ctl
```

```
Length of CTL file: 0
CTL File not found. Please run CTLClient plugin or run the CLI - utils ctl..
to generate the CTL file.
Error parsing the CTL File.
```

2. Funcione con al cliente CTL. Ingrese el nombre de host IP/el direccionamiento del Pub CUCM y de las credenciales del administrador CCM. Haga clic en Next (Siguiente).
3. Puesto que el cluster está en el modo mezclado, no obstante ningún archivo CTL existe en Publisher, se visualiza esta advertencia. Haga Click en OK para ignorarlo y proceder adelante.
4. Haga clic el botón de radio del **archivo de la actualización CTL**. Haga clic en Next (Siguiente).
5. El cliente CTL pide agregar un token de seguridad. El tecleo **agrega** para proceder.
6. Las visualizaciones de la pantalla todas las entradas en el nuevo CTL. El tecleo **agrega los tokens** para agregar el segundo token de los nuevos pares.
7. A le indicarán que quite el token actual e inserte un nuevo. Haga Click en OK hecho una vez.
8. Se visualiza una pantalla que muestra los detalles del nuevo token. Haga clic **agregan** para confirmarlos y agregar este token.
9. Le presentarán con la nueva lista de entradas CTL que muestren ambos tokens agregados. Clic en Finalizar para generar los nuevos archivos CTL.
10. En el campo de contraseña simbólico, ingrese el **cisco123**. Haga clic en OK.
11. Usted verá la confirmación que el proceso era acertado. Haga clic **hecho** para confirmar y salir al cliente CTL.
12. Recomience Cisco TFTP seguido por el servicio de CallManager (utilidad unificada Cisco > Tools (Herramientas) > Control Center (Centro de control) - ofrezca los servicios). El nuevo archivo CTL debe ser generado. Ingrese el comando del **ctl de la demostración** para la verificación.
```
admin:show ctl
The checksum value of the CTL file:
68a954fba070bbcc3ff036e18716e351(MD5)
4f7a02b60bb5083baac46110f0c61eac2dceb0f7(SHA1)


Length of CTL file: 5728
The CTL File was last modified on Mon Mar 09 11:38:50 CET 2015
```
13. Borre el archivo CTL de cada teléfono en el cluster (este procedimiento podría variar basado en el tipo de teléfono - consulte por favor la documentación para los detalles, tales como el Cisco Unified IP Phone 8961, la guía de administración 9951, y 9971).Nota: Los teléfonos pudieron todavía poder registrarse (dependiente sobre los ajustes de seguridad en el teléfono) y trabajar sin el procedimiento con el paso 13. Sin embargo, tendrán el viejo archivo CTL instalado. Podría causar los problemas si se regeneran los Certificados, otro servidor se agrega al cluster o se substituye el hardware del servidor. No se recomienda para dejar el cluster en este estatus.
14. Mueva el cluster NON-seguro. Vea el cambio la Seguridad del cluster CUCM del modo NON-seguro mezclado del modo con la sección del cliente CTL para los detalles.

Troubleshooting

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.