Esempio di configurazione di un cluster CUCM passato dalla modalità mista alla modalità non protetta

Sommario

Introduzione

Nel documento viene descritta la procedura necessaria per modificare la modalità di protezione di Cisco Unified Communications Manager (CUCM) da modalità mista a non protetta. Viene inoltre illustrato il modo in cui il contenuto di un file dell'elenco di certificati attendibili (CTL) viene modificato al termine dello spostamento.

Per modificare la modalità di protezione CUCM, è necessario eseguire tre operazioni principali:

1 bis. Eseguire il client CTL e selezionare la variante desiderata della modalità di protezione.
1 ter. Immettere il comando CLI per selezionare la variante desiderata della modalità di sicurezza.
2. Riavviare i servizi Cisco CallManager e Cisco TFTP su tutti i server CUCM che eseguono questi servizi.
3. Riavviare tutti i telefoni IP in modo che possano scaricare la versione aggiornata del file CTL.

Nota: se la modalità di protezione del cluster viene modificata da Modalità mista a Non protetta, il file CTL è ancora presente nei server e nei telefoni, ma il file CTL non contiene certificati CCM+TFTP (server). Poiché i certificati CCM+TFTP (server) non esistono nel file CTL, il telefono viene registrato come non protetto con CUCM.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di CUCM versione 10.0(1) o successive. Inoltre, assicurarsi che:

- Il servizio del provider CTL è attivo ed è in esecuzione su tutti i server TFTP attivi nel cluster. Per impostazione predefinita, il servizio viene eseguito sulla porta TCP 2444, ma è possibile modificare questa impostazione nella configurazione dei parametri del servizio CUCM.
- I servizi CAPF (Certificate Authority Proxy Function) sono attivi e in esecuzione nel nodo Publisher.
- La replica del database (DB) nel cluster funziona correttamente e i server replicano i dati in tempo reale.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- CUCM release 10.0.1.1900-2 cluster di due nodi
- Cisco 7975 IP phone (registrato con il protocollo SCCP (Skinny Call Control Protocol), versione firmware SCCP75.9-3-1SR3-1S)
- Per impostare il cluster in modalità mista, sono necessari due token di sicurezza Cisco
- Uno dei token di sicurezza elencati in precedenza è necessario per impostare il cluster in modalità non protetta

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Per eseguire il plug-in del client CTL, è necessario avere accesso ad almeno un token di sicurezza inserito per creare o aggiornare l'ultimo file CTL esistente sul server di pubblicazione CUCM. In altre parole, almeno uno dei certificati eToken presenti nel file CTL corrente in CUCM deve trovarsi nel token di sicurezza utilizzato per modificare la modalità di sicurezza.

Configurazione

Modificare la protezione del cluster CUCM dalla modalità mista alla modalità non protetta con il client CTL

Completare questi passaggi per modificare la sicurezza del cluster CUCM dalla modalità mista

alla modalità non protetta con il client CTL:

1. Ottenere un token di sicurezza inserito per configurare il file CTL più recente.
2. Eseguire il client CTL. Fornire il nome host/indirizzo IP del pub CUCM e le credenziali dell'amministratore CCM. Fare clic su Next (Avanti).
3. Fare clic sul pulsante di opzione Imposta cluster Cisco Unified CallManager in modalità non protetta. Fare clic su Next (Avanti).
4. Inserire un token di sicurezza inserito per configurare il file CTL più recente e fare clic su OK. Questo è uno dei token utilizzati per popolare l'elenco dei certificati in CTLFile.tlv.
5. Vengono visualizzati i dettagli del token di sicurezza. Fare clic su Next (Avanti).
6. Viene visualizzato il contenuto del file CTL. Fare clic su Finish (Fine). Quando viene richiesta la password, immettere Cisco123.
7. Viene visualizzato l'elenco dei server CUCM in cui è presente il file CTL. Selezionate Fatto (Done).
8. Scegliere CUCM Admin Page > Sistema > Parametri enterprise e verificare che il cluster sia stato impostato sulla modalità non protetta (0 indica Non protetto).
9. Riavviare i servizi TFTP e Cisco CallManager su tutti i nodi del cluster che eseguono questi servizi.
10. Riavviare tutti i telefoni IP in modo che possano ottenere la nuova versione del file CTL da CUCM TFTP.

Modificare la protezione del cluster CUCM dalla modalità mista alla modalità non protetta con CLI

Questa configurazione è valida solo per CUCM release 10.X e successive. Per impostare la modalità di protezione del cluster CUCM su Non protetto, immettere il comando utils ctl set-cluster non-secure-mode nella CLI di Publisher. Al termine, riavviare i servizi TFTP e Cisco CallManager su tutti i nodi del cluster che eseguono questi servizi.

Di seguito è riportato un output di esempio della CLI che mostra l'utilizzo del comando.

<#root>

```
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:
```

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Per verificare il file CTLFIle.tlv, è possibile utilizzare uno dei due metodi seguenti:

- Per verificare il contenuto e il checksum MD5 del file CTLFIle.tlv presente sul lato CUCM TFTP, immettere il comando show ctl sulla CLI di CUCM. Il file CTLFIle.tlv deve essere lo stesso in tutti i nodi CUCM.
- Per verificare il checksum MD5 sul telefono IP 7975, scegliere Impostazioni > Configurazione protezione > Elenco di attendibilità > File CTL.

Nota: quando si controlla il checksum del telefono, viene visualizzato MD5 o SHA1, a seconda del tipo di telefono.

Cluster CUCM impostato su Modalità di protezione - Checksum file CTL

<#root>

```
admin:
```

show ctl

```
The checksum value of the CTL file:
```

98784f6f6bcd5019ea165b1d2bc1372e(MD5)

```
9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1)
[...]
```

Sul lato del telefono IP, è possibile vedere che ha lo stesso file CTL installato (il checksum MD5 corrisponde all'output di CUCM).

Cluster CUCM impostato su modalità non protetta - Contenuto file CTL

Di seguito è riportato un esempio di file CTL da un cluster CUCM impostato sulla modalità non protetta. I certificati CCM+TFTP sono vuoti e non contengono alcun contenuto. Gli altri certificati nei file CTL non vengono modificati e sono esattamente gli stessi di quando CUCM è stato impostato sulla modalità mista.

<#root>

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
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
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
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:
```

Sul lato IP Phone, dopo il riavvio e il download della versione aggiornata del file CTL, si nota che il checksum MD5 corrisponde all'output di CUCM.

Passa dalla modalità mista alla modalità non protetta quando i token USB vengono persi

I token di sicurezza per i cluster protetti potrebbero andare perduti. In tale situazione, è necessario considerare i due scenari seguenti:

- Il cluster esegue la versione 10.0.1 o successiva
- Il cluster esegue una versione precedente alla 10.x

Nel primo scenario, completare la procedura descritta nella sezione Modifica della sicurezza del cluster CUCM da modalità mista a modalità non protetta con la CLI per risolvere il problema. Poiché tale comando CLI non richiede un token CTL, potrebbe essere utilizzato anche se il cluster è stato messo in modalità mista con il client CTL.

La situazione diventa più complessa quando viene utilizzata una versione precedente alla 10.x di CUCM. Se si dimentica la password di uno dei token, è comunque possibile utilizzare l'altro per eseguire il client CTL con i file CTL correnti. Si consiglia vivamente di ottenere un altro eToken e di aggiungerlo al file CTL il prima possibile a scopo di ridondanza. Se si perdono o si dimenticano le password per tutti gli eToken elencati nel file CTL, è necessario ottenere una nuova coppia di eToken ed eseguire una procedura manuale come spiegato qui.

1. Immettere il comando file delete tftp CTLFile.tlv per eliminare il file CTL da tutti i server 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. Eseguire il client CTL. Immettere il nome host/indirizzo IP del pub CUCM e le credenziali dell'amministratore CCM. Fare clic su Next (Avanti).

3. Poiché il cluster è in modalità mista, tuttavia in Publisher non esiste alcun file CTL, viene

visualizzato questo avviso. Fare clic su OK per ignorarlo e procedere.

4. Fare clic sul pulsante di opzione Aggiorna file CTL. Fare clic su Next (Avanti).
5. Il client CTL chiede di aggiungere un token di sicurezza. Per continuare, fare clic su Add (Aggiungi).
6. Nella schermata vengono visualizzate tutte le voci nel nuovo elenco di certificati attendibili (CTL). Fare clic su Add Tokens per aggiungere il secondo token dalla nuova coppia.
7. Verrà richiesto di rimuovere il token corrente e di inserirne uno nuovo. Fare clic su OK una volta terminato.
8. Viene visualizzata una schermata che mostra i dettagli del nuovo token. Fare clic su Add (Aggiungi) per confermarli e aggiungere questo token.
9. Verrà visualizzato un nuovo elenco di voci CTL che mostrano entrambi i token aggiunti. Per generare nuovi file CTL, fare clic su Finish (Fine).
10. Nel campo Token Password, immettere Cisco123. Fare clic su OK.
11. Verrà visualizzato un messaggio di conferma del completamento del processo. Fare clic su Done (Fine) per confermare e uscire dal client CTL.
12. Riavviare Cisco TFTP e quindi il servizio CallManager (Cisco Unified Serviceability > Strumenti > Control Center - Feature Services). È necessario generare il nuovo file CTL. Immettere il comando show ctl per la verifica.

```
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. Eliminare il file CTL da ciascun telefono del cluster (questa procedura può variare in base al tipo di telefono. Per ulteriori informazioni, consultare la documentazione, ad esempio la Guida all'amministrazione di Cisco Unified IP Phone 8961, 9951 e 9971).

> Nota: i telefoni potrebbero essere ancora in grado di registrarsi (a seconda delle impostazioni di sicurezza del telefono) e di lavorare senza procedere con il passaggio 13. Tuttavia, avranno installato il vecchio file CTL. Ciò potrebbe causare problemi se i certificati vengono rigenerati, se viene aggiunto un altro server al cluster o se viene sostituito l'hardware del server. Non è consigliabile lasciare il cluster in questo stato.

14. Spostare il cluster in Non protetto. Per ulteriori informazioni, vedere la sezione Modifica della sicurezza del cluster CUCM dalla modalità mista alla modalità non protetta con la sezione Client CTL.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).