Conjunto CUCM mudado de exemplo NON-seguro misturado da configuração de modo do modo

Índice

Introdução

O documento descreve as etapas exigidas a fim mudar o modo de segurança do gerente das comunicações unificadas de Cisco (CUCM) de modo NON-seguro misturado do modo. Igualmente mostra como o índice de um arquivo do certificate trust list (CTL) é mudado quando este movimento é terminado.

Há três maiores parte para mudar o modo de segurança CUCM:

1a. Execute o cliente CTL e selecione a variação desejada do modo de segurança.
1b. Inscreva o comando CLI a fim selecionar a variação desejada do modo de segurança.
2. Reinicie o CallManager da Cisco e os serviços TFTP de Cisco em todos os server CUCM que dirigem estes serviços.
3. Reinicie todos os Telefones IP de modo que possam transferir a versão actualizado do arquivo CTL.

> Nota: Se o modo de segurança do conjunto é mudado de modo NON-seguro misturado do modo o arquivo CTL ainda existe nos server e nos telefones, mas o arquivo CTL não contém nenhuns Certificados CCM+TFTP (server). Desde que os Certificados CCM+TFTP (server) não existem no arquivo CTL, este força o telefone para registrar-se como NON-

seguro com CUCM.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento da versão 10.0(1) ou mais recente CUCM. Adicionalmente, assegure isso:

- O serviço do fornecedor CTL é ascendente e é executado em todos os servidores TFTP ativos no conjunto. À revelia o serviço é executado na porta TCP 2444, mas este pode ser alterado na configuração do parâmetro de serviço CUCM.
- Os serviços da função do proxy do Certificate Authority (CAPF) são ascendentes e são executado no nó do editor.
- A replicação do base de dados (DB) no conjunto trabalha corretamente e os dados replicate server no tempo real.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Conjunto da liberação 10.0.1.11900-2 CUCM de dois Nós
- Telefone IP de Cisco 7975 (registrado com Skinny Call Control Protocol (SCCP), versão de firmware SCCP75.9-3-1SR3-1S)
- Dois tokens do Cisco Security são necessários a fim ajustar o conjunto a modo misturado
- Um dos tokens de segurança alistados previamente é necessário a fim ajustar o modo NON-seguro do conjunto

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

A fim executar o cliente CTL de encaixe exige-se para ter o acesso pelo menos a um token de segurança que foi introduzido a fim criar ou atualizar o arquivo o mais atrasado CTL existe no servidor do publicador CUCM. Ou seja pelo menos um dos Certificados do eToken que existe no arquivo atual CTL em CUCM deve estar no token de segurança que é usado para mudar o modo de segurança.

Configurar

Mude a Segurança do conjunto CUCM de modo NON-seguro misturado do modo com o cliente CTL

Termine estas etapas a fim mudar a Segurança do conjunto CUCM de modo NON-seguro misturado do modo com o cliente CTL:

1. Obtenha um token de segurança que você introduziu para configurar o arquivo o mais atrasado CTL.
2. Execute o cliente CTL. Forneça o hostname IP/endereço do bar CUCM e das credenciais do administrador CCM. Clique em Next.
3. Clique o botão de rádio NON-**seguro do modo do conjunto de Cisco Unified CallManager do grupo**. Clique em Next.
4. Introduza um token de segurança que foi introduzido para configurar o arquivo o mais atrasado CTL e para clicar a **APROVAÇÃO**. Este é um dos tokens que foi usado para povoar a lista do certificado em CTLFile.tlv.
5. Os detalhes do token de segurança são indicados. Clique em Next.
6. O índice do arquivo CTL é indicado. Clique em Finish. Quando alertado para a senha, entre no **cisco123**.
7. A lista de server CUCM em que o arquivo CTL existe é indicada. Clique em Concluído.
8. Escolha a **página de admin > o sistema > parâmetros de empreendimento CUCM** e verifique que o conjunto era modo NON-seguro ajustado ("0" indica NON-seguro).
9. Reinicie o TFTP e os serviços do CallManager da Cisco em todos os Nós no conjunto que dirigem estes serviços.
10. Reinicie todos os Telefones IP de modo que possam obter a nova versão do arquivo CTL de CUCM TFTP.

Mude a Segurança do conjunto CUCM de modo NON-seguro misturado do modo com o CLI

Esta configuração é somente para a liberação 10.X CUCM e mais tarde. A fim ajustar o modo de segurança do conjunto CUCM NON-seguro, incorpore o comando do grupo-**conjunto NON-seguro-MODE do ctl dos utils no** editor CLI. Depois que isto está completo, reinicie o TFTP e os serviços do CallManager da Cisco em todos os Nós no conjunto que dirigem estes serviços.

Está aqui a amostra CLI output que mostra o uso do 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:
```

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

A fim verificar o CTLFIle.tlv, você pode usar um de dois métodos:

- A fim verificar o índice e a soma de verificação MD5 do CTLFIle.tlv atual no lado CUCM TFTP, incorpore o **comando do** showctl no CUCM CLI. O arquivo CTLFIle.tlv deve ser o mesmo em todos os Nós CUCM.
- A fim verificar a soma de verificação MD5 no telefone IP 7975, escolha a **configuração do > segurança dos ajustes > a lista da confiança > o arquivo CTL**.

  Nota: Quando você verificar a soma de verificação no telefone que você verá o MD5 ou o SHA1, dependente do tipo de telefone.

Conjunto CUCM ajustado ao modo de segurança - Soma de verificação do arquivo CTL

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

No lado do telefone IP, você pode ver que tem o mesmo arquivo CTL instalado (a soma de verificação MD5 combina quando comparada à saída de CUCM).

O conjunto CUCM ajustou o modo NON-seguro - Conteúdo de arquivo CTL

Está aqui um exemplo de um arquivo CTL de um modo NON-seguro ajustado conjunto CUCM. Você pode ver que os Certificados CCM+TFTP estão vazios e não contém nenhum índice. O resto dos Certificados nos arquivos CTL não é mudado e é exatamente o mesmo que quando CUCM foi ajustado a modo misturado.

```
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:
```

No lado do telefone IP, depois que foi reiniciado e transferiu a versão de arquivo actualizado CTL, você pode ver que a soma de verificação MD5 combina quando comparada à saída de CUCM.

Põe a Segurança do conjunto CUCM de modo NON-seguro misturado do modo quando os tokens USB são perdidos

Os tokens de segurança para conjuntos fixados podiam ser perdidos. Nessa situação, você precisa de considerar estas duas encenações:

- O conjunto executa a versão 10.0.1 ou mais recente
- O conjunto executa uma versão mais cedo do que 10.x

Na primeira encenação, termine o procedimento descrito na mudança a Segurança do conjunto CUCM de modo NON-seguro misturado do modo com a seção CLI a fim recuperar da edição. Desde que esse comando CLI não exige um token CTL, poderia ser usado mesmo se o conjunto foi posto em modo misturado com o cliente CTL.

A situação obtém mais complexa quando uma versão mais cedo do que 10.x de CUCM está no uso. Se você perde ou esquece a senha de um dos tokens, você pode ainda usar outro para executar o cliente CTL com arquivos atuais CTL. É altamente recomendado obter outro eToken e adicionar-lo ao arquivo CTL o mais cedo possível para a Redundância. Se você perde ou esquece as senhas para todos os eTokens alistados em seu arquivo CTL, você precisa de obter um par novo de eTokens e de executar um Procedimento Manual como explicado aqui.

1. Incorpore o **comando de tftp CTLFile.tlv da supressão do arquivo** a fim suprimir do arquivo CTL de todos os 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. Execute o cliente CTL. Incorpore o hostname IP/endereço do bar CUCM e das credenciais do administrador CCM. Clique em Next.
3. Desde que o conjunto reage de modo misturado, porém nenhum arquivo CTL existe no editor, este aviso é indicado. Clique a **APROVAÇÃO** a fim ignorá-la e continuar para a frente.
4. Clique o botão de rádio do **arquivo da atualização CTL**. Clique em Next.
5. O cliente CTL pede para adicionar um token de segurança. O clique **adiciona** a fim continuar.
6. Os displays de tela todas as entradas no CTL novo. O clique **adiciona tokens** a fim adicionar o segundo token dos pares novos.
7. Você será alertado remover o token atual e introduzir um novo. **APROVAÇÃO do** clique feita uma vez.
8. Uma tela que mostre detalhes do token novo é indicada. Clique **adicionam** a fim confirmá-los e adicionar este token.
9. Você é presentado com a lista nova de entradas CTL que mostram ambos os tokens adicionados. **Revestimento do** clique a fim gerar arquivos novos CTL.
10. No campo de senha simbólico, entre no **cisco123**. Clique em **OK**.
11. Você verá a confirmação que o processo era bem sucedido. Clique **feito** a fim confirmar e retirar o cliente CTL.
12. Reinicie Cisco TFTP seguido pelo serviço do CallManager (a utilidade unificada Cisco > utiliza ferramentas > Control Center - caracterize serviços). O arquivo novo CTL deve ser gerado. Incorpore o comando do **ctl da mostra** para a verificação.
```
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. Suprima do arquivo CTL de cada telefone no conjunto (este procedimento poderia variar baseado no tipo de telefone - consulte por favor a documentação para detalhes, tais como o Telefone IP Cisco Unified 8961, o Guia de Administração 9951, e 9971).Nota: Os telefones puderam ainda poder registrar-se (dependente das configurações de segurança do telefone) e trabalhar sem continuar com etapa 13. Contudo, terão o arquivo velho CTL instalado. Poderia causar edições se os Certificados são regenerados, um outro server é adicionado ao conjunto ou o hardware do servidor é substituído. Não se recomenda deixar o conjunto neste estado.
14. Mova o conjunto NON-seguro. Veja a mudança a Segurança do conjunto CUCM de modo NON-seguro misturado do modo com a seção do cliente CTL para detalhes.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.