混合モードから非セキュア モードに変更された CUCM クラスタの設定例

内容

<u>概要</u>

<u>前提条件</u>

<u>要件</u>

<u>使用するコンポーネント</u>

<u>背景説明</u>

<u>設定</u>

<u>CTL クライアントで CUCM クラスタセキュリティを混合モードから非セキュアモードに変更す</u> る

<u>CLI で CUCM クラスタセキュリティを混合モードから非セキュアモードに変更する</u>

<u>確認</u>

<u>セキュリティ モードに設定された CUCM クラスタ - CTL ファイル チェックサム</u>

<u>非セキュア モードに設定された CUCM クラスタ - CTL ファイルの内容</u>

<u>USB トークン喪失時に CUCM クラスタ セキュリティを混合モードから非セキュア モードへ切り</u> <u>替える</u>

<u>トラブルシュート</u>

概要

このドキュメントでは Cisco Unified Communications Manager(CUCM)のセキュリティモード を混合モードから非セキュア モードへ切り替えるために必要な手順を説明します。また、切り替 えと完了時に証明書信頼リスト(CTL)ファイルの内容がどのように変更されるかも示します。

CUCM セキュリティ モードの変更は主に3つの部分に分けることができます。

1a.CTL クライアントを実行し、必要な種類のセキュリティ モードを選択します。 1b.必要な種類のセキュリティ モードを選択するための CLI コマンドを入力します。 2.これらのサービスを実行するすべてのCUCMサーバでCisco CallManagerおよびCisco TFTPサー ビスを再起動します。 3.すべてのIP Phoneを再起動して、CTLファイルの更新バージョンをダウンロードできるように します。

注: クラスタのセキュリティ モードが混合モードから非セキュア モードに変更されても CTL ファイルは各サーバと電話機に残存しますが、この CTL ファイルには CCM+TFTP(サーバ)証明書は一切含まれません。CTL ファイルに CCM+TFTP(サーバ)証明書は含まれないため、電話機は CUCM に強制的に非セキュアに登録されます。

前提条件

要件

CUCM バージョン 10.0(1) 以降の知識があることが推奨されます。また、次のことを確認してください。

- CTL プロバイダー サービスは、クラスタのすべてのアクティブな TFTP サーバ上で実行され、アップ状態になっていること。このサービスはデフォルトで TCP ポート 2444 で実行され、これは CUCM サービス パラメータ設定で変更できます。
- 認証局プロキシ機能(CAPF)サービスがパブリッシャ ノードで実行され、アップ状態になっていること。
- クラスタ内のデータベース(DB)の複製が正常に動作しており、サーバがデータをリアルタイムに複製していること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- CUCM リリース 10.0.1.11900-2 (2 ノードのクラスタ)
- Cisco 7975 IP フォン (Skinny Client Control Protocol (SCCP)、ファームウェア バージョ ン SCCP75.9-3-1SR3-1S を使用して登録されたもの)
- クラスタを混合モードに設定するには、2つのシスコセキュリティトークンが必要です。
- クラスタを非セキュアモードに設定するには、上記のセキュリティトークンのうち1つが必要です。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このド キュメントで使用するすべてのデバイスは、初期(デフォルト)設定の状態から起動しています 。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的 な影響について確実に理解しておく必要があります。

背景説明

CTL クライアントのプラグインを実行するには、CUCM パブリッシャ サーバに存在する最新の CTL ファイルを作成または更新するために挿入される、少なくとも 1 つのセキュリティ トークン へのアクセスが必要です。つまり、CUCM の現在の CTL ファイルに存在する eToken 証明書の うちの少なくとも 1 つが、セキュリティ モードの変更で使用するセキュリティ トークンにも含 まれている必要があります。

設定

CTL クライアントで CUCM クラスタセキュリティを混合モードから非セキュアモ ードに変更する

CTL クライアントで CUCM クラスタセキュリティを混合モードから非セキュアモードに変更す

るには、次の手順を実行します。

- 1. 最新の CTL ファイルを設定するために挿入したセキュリティ トークンのうちの 1 つを取得 します。
- 2. CTL クライアントを実行します。CUCM パブリッシャの IP ホスト名/アドレスと CCM 管理 者のクレデンシャルを入力します。[next] をクリックします。

| \mathcal{C}_n | CTL Client v5.0 | | | | | | x |
|-----------------|--|-------------------|---------------|-------|------|--------------|---|
| | Cisco CTL Cl For IP Telephony Solution | ient | ahah cisco | , | | | |
| | Cisco Unified Communicatio | ns Manager Server | | | | | 1 |
| | Hostname or IP Address: | 10.48.47.153 | | Port: | 2444 | | |
| | Username: | admin | | | | | |
| | Password: | Xokolololok | | | | | |
| | | | | | | | |
| | Help | | <u>C</u> an | icel | 1 | <u>l</u> ext | |

3. [Set Cisco Unified CallManager Cluster to Non-Secure Mode] オプション ボタンをクリック します。[next] をクリックします。

| CTL Client v5.0 | |
|---|------|
| Cisco CTL Client | |
| Cluster Security Mode | |
| C Set Cisco Unified CallManager Cluster to Mixed Mode | |
| Set Cisco Unified CallManager Cluster to Non-Secure Mod | le |
| C Update CTL File | |
| | |
| | |
| Help Cancel | Next |

4. 最新の CTL ファイルの設定で挿入したセキュリティ トークンのうち 1 つを挿入し、[OK] を クリックします。これは CTLFile.tlv 内の証明書のリストを入力するために使用されたトー クンのうちの 1 つです。



5. セキュリティ トークンの詳細が表示されます。[next] をクリックします。

| Crn CTL Client v5.0 | |
|--|--|
| Cisco CTL Ch For IP Telephony Solutions | ent alialia cisco |
| Security Token Information | |
| Subject Name: | cn="SAST-ADN0054f509 ";ou=IPCBU;o="Cisco Sy: |
| Issuer Name: | cn=Cisco Manufacturing CA;o=Cisco Systems |
| Valid From: | 06/09/2010 |
| Expires on: | 06/09/2020 |
| | |
| Help | Cancel Next |

6. CTL ファイルの内容が表示されます。[Finish] をクリックします。パスワードの入力を求め られたら、「Cisco123」と入力します。

| 🧞 CTL Client v5.0 | | | | | | | |
|--|--|---|---|--|---|--|--|
| Cia | sco CTL C · IP Telephony Solutio | hent | ر ا ۲ | haha Isco | | | |
| CTL Entries | | | | | | | |
| Type CAPF CCM+TFTP CCM+TFTP Security T Security T | Hostname/I 10.48.47.153 10.48.47.154 10.48.47.153 — No Hostna — No Hostna | Issuer Name CN=CAPF-e9 — No Issuer N — No Issuer N cn=Cisco Mar cn=Cisco Mar | 037b69;OU lame — lame — lufacturing lufacturing | Subject N CN=CAPF — No Sub — No Sub cn="SAS ⁻ cn="SAS ⁻ | lame F-e9037b69;OU=T bject Name — T-ADN008580ef T-ADN0054f509 | | |
| • | • | | | | | | |
| Help | Add | | Add Fire | wall | | | |
| Cancel | Add | Tokens | Delete Sel | ected | Finish | | |

7. CTL ファイルが存在する CUCM サーバのリストが表示されます。[Done] をクリックします

0

| CTL Client v5.0 | | | |
|----------------------------|------------------------------------|------------------|-----------------------|
| Cisco For IP Tel | CTL Client | ahaha cisco | |
| Contor | File Location | Statua | |
| Server 10.49.47.153 | usr/local.cm/tttp/CTLEilo.tk | | |
| 10.40.47.153 | /usr/local/cm/tttn/CTLFile.tv | Pacco | id id |
| | | | |
| You must resta Cluster. | rt all the Cisco Unified Communica | ations Manager a | and TFTP nodes in the |
| Help | | | Done |

8. [CUCM Admin Page] > [System] > [Enterprise Parameters]を選択し、クラスタが非セキュア モードに設定されていることを確認します(「0」が非セキュアを表示します)。

| Security Farameters | |
|------------------------------------|------------|
| Cluster Security Mode * | 0 |
| LBM Security Mode * | Insecure T |
| CAPF Phone Port * | 3804 |
| CAPF Operation Expires in (days) * | 10 |
| Enable Caching * | True |
| | |

- 9. TFTP サービスおよび Cisco CallManager サービスを実行しているクラスタ内のすべてのノードで、これらのサービスを再起動します。
- 10. IP 電話が CUCM TFTP から新しいバージョンの CTL ファイルを取得できるように、すべての IP 電話を再起動します。

CLI で CUCM クラスタセキュリティを混合モードから非セキュアモードに変更する

これは、CUCM リリース 10.X 以降のみの設定です。CUCM クラスタ セキュリティ モードを非 セキュアに設定するには、パブリッシャの CLI で **utils ctl set-cluster non-secure-mode コマンド** を入力します。完了したら、TFTP サービスおよび Cisco CallManager サービスを実行している

クラスタ内のすべてのノードで、これらのサービスを再起動します。

コマンドを使った場合の CLI の出力のサンプルを以下に示します。

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:

確認

ここでは、設定が正常に機能しているかどうかを確認します。

CTLFIle.tlv を確認するには、次の2つの方法があります。

- CUCM TFTP側にあるCTLFIle.tlvの内容とMD5チェックサムを確認するには、CUCM CLIで show ctlコマンドを入力します。CTLFIle.tlv ファイルは、すべての CUCM ノードで同一のも のでなければなりません。
- 7975 IP Phone で MD5 チェックサムを確認するには、[Settings] > [Security Configuration] > [Trust List] > [CTL File] を選択します。

注:電話のチェックサムを確認すると、電話のタイプに応じて、MD5 または SHA1 が表示 されます。

セキュリティ モードに設定された CUCM クラスタ - CTL ファイル チェックサム

admin:show ctl The checksum value of the CTL file: 98784f6f6bcd5019ea165b1d2bc1372e(MD5) 9c0aa839e5a84b18a43caf9f9ff23d8ebce90419(SHA1) [...] IP フォン側で同一の CTL ファイルがインストールされているか確認できます(同一なら MD5 チ ェックサムは CUCM が出力したものと一致します)。



非セキュア モードに設定された CUCM クラスタ - CTL ファイルの内容

非セキュア モードに設定されている CUCM クラスタからの CTL ファイルの例を示します。 CCM+TFTP 証明書が空で、一切内容が含まれないことが確認できます。CTL ファイルの残りの 証明書は変更されず、CUCM が混合モードに設定されていたときとまったく同じです。

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: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 cl 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: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)

```
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
```

10 IPADDRESS 4

The CTL file was verified successfully.

admin:

IP フォンが再起動し、新しいバージョンの CTL ファイルをダウンロードした後には、IP フォン 側で MD5 チェックサムが CUCM の出力と一致することが確認できます。



USB トークン喪失時に CUCM クラスタ セキュリティを混合モ ードから非セキュア モードへ切り替える

セキュア クラスタのセキュリティ トークンが失われることがあります。この状況では、次の 2 つのシナリオを考慮する必要があります。

・クラスタがバージョン 10.0.1 以降を実行している場合

• クラスタがバージョン 10.x 以前を実行している場合

最初のシナリオでは、問題を解決するため、<u>CLI で CUCM クラスタセキュリティを混合モードから非セキュアモードに変更するセクションの手順を実行してください。</u>CLI コマンドは CTL トークンを必要としないため、このコマンドは CTL クライアントでクラスタを混合モードにしてあっても使用できます。

バージョン 10.x 以前の CUCM が使用されている場合は、状況はより複雑です。いずれかのトー クンのパスワードを紛失または失念した場合でも、他のトークンを使い、現行の CTL ファイルと CTL クライアントを実行できます。冗長性を確保するため、可能な限り、他の eToken を取得し 、CTL ファイルに含めておくことを強く推奨します。CTL ファイルに記載されているすべての eToken のパスワードを紛失または失念した場合は、新しい eToken のペアを取得し、ここで説明 する手順を手作業で実行する必要があります。

1. file delete tftp CTLFile.tlv コマンドを入力し、すべての TFTP サーバから CTL ファイルを削 除します。

| 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. CTL クライアントを実行します。CUCM パブリッシャの IP ホスト名/アドレスと CCM 管理 者のクレデンシャルを入力します。[next] をクリックします。

| \mathcal{C}_n | CTL Client v5.0 | | | |
|-----------------|--|-------------------|----------------|------|
| | Cisco CTL Cl For IP Telephony Solution | ient | ahaha cisco | |
| | Cisco Unified Communicatio | ns Manager Server | | |
| | Hostname or IP Address: | 10.48.47.153 | Port: | 2444 |
| | Username: | admin | | |
| | Password: | Xolololololok | | |
| | | | | |
| | Help | | <u>C</u> ancel | Next |

3. クラスタは混合モードになっており、CTL ファイルは存在しないため、このことを示す警告 が表示されます。[OK] をクリックしてこれを無視し、[proceed forward] で次へ進みます。

| CTLClient | × |
|-----------|---|
| 8 | No CTL File exists on the server but the Call Manager Cluster Security Mode is in Secure Mode. For the system to function, you must create the CTL File and set Call Manager Cluster to Secure Mode. |
| | OK |

| [Update CTL File] オプション ボタンをクリックします。 | [next] をクリックします |
|---|-------------------|
| CTL Client v5.0 | |
| Cisco CTL Chent For IP Telephony Solutions | ahaha cisco |
| Cluster Security Mode | 1 |
| C Set Cisco Unified CallManager Cluster to <u>M</u> i | ixed Mode |
| C Set Cisco Unified CallManager Cluster to Ng | on-Secure Mode |
| Update CTL File | |
| | |
| | |
| | ncel <u>N</u> ext |

5. CTL クライアントは、セキュリティ トークンを追加のための表示を行います。[Add] をクリ ックして続行します。

| CTL Client v5.0 | | |
|-------------------------------------|------------------------------|--------------------|
| Cisco CT For IP Telephony | L Client Solutions | ahaha cisco |
| Security Token Information |] | 1 |
| Subject Name: | cn=''SAST-ADN0054f50a | ";ou=IPCBU;o="Cisi |
| Issuer Name: | cn=Cisco Manufacturing CA; | o=Cisco Systems |
| Valid From: | 06/08/2010 | |
| Expires on: | 06/08/2020 | |
| | | |
| <u>H</u> elp | <u>C</u> ar | icel Add |

6. 新しい CTL のすべてエントリが表示されます。[Add Tokens] をクリックし、新しいペアの 2 つ目のトークンを追加します。

| 🧞 CTL Client v5.0 | |
|--|--|
| Cisco CTL Client For IP Telephony Solutions | cisco |
| CTL Entries | 1 |
| Type Hostname/ Issuer Name CAPF 10.48.47.153 CN=CAPF-e9037b69;0U= CCM+TFTP 10.48.47.154 CN=cucm-1001-a-sub1;0 CCM+TFTP 10.48.47.153 CN=cucm-1001-a-pub;0U Security To No Host cn=Cisco Manufacturing C | Subject Name CN=CAPF-e9037t CN=cucm-1001-a CN=cucm-1001-a cn=''SAST-ADN0 |
| Help Add TFTP Add Firewall Cancel Add Tokens Delete Selected | Finish |
| | |

7. 現在のトークンを削除し、新しいユーザを挿入するか、確認が表示されます。完了したら [OK]をクリックします。

| CTLClient | × |
|-----------|--|
| | Please remove any Security Tokens already inserted and insert another Security Token. Click Ok when done. |
| | OK Cancel |

8. 新しいトークンの詳細を示す画面が表示されます。[Add] をクリックして、トークンの詳細 を確認し、トークンを追加します。

| CTL Client v5.0 | | | | |
|-----------------------------|---|--|--|--|
| L Chent Solutions | ahaha cisco | | | |
|] | | | | |
| cn="SAST-ADN008580ef | ";ou=IPCBU;o="Cisi | | | |
| cn=Cisco Manufacturing CA; | o=Cisco Systems | | | |
| 05/17/2012 | | | | |
| 05/17/2022 | | | | |
| | | | | |
| <u>C</u> an | cel Add | | | |
| | L Client Solutions cn=''SAST-ADN008580ef cn=Cisco Manufacturing CA; 05/17/2012 05/17/2022 <u>C</u> an | | | |

9. 両方のトークンが追加された新しい CTL エントリのリストが表示されます。[Finish] をクリ ックして、新しい CTL ファイルを生成します。

| C_n CTL Client v5.0 | |
|---|--|
| Cisco CTL Client For IP Telephony Solutions | ahaha cisco |
| CTL Entries | |
| TypeHostname/IIssuer NameCAPF10.48.47.153CN=CAPF-e9037b69;0UCCM+TFTP10.48.47.154CN=cucm-1001-a-sub1;0CCM+TFTP10.48.47.153CN=cucm-1001-a-pub;0Security To No Hostncn=Cisco ManufacturingSecurity To No Hostncn=Cisco Manufacturing | Subject Name I= CN=CAPF-e9037 DU CN=cucm-1001-a U= CN=cucm-1001-a C cn=''SAST-ADNC C cn=''SAST-ADNC |
| Help Add TFTP Add Firew Cancel Add Tokens Delete Selev | all cted <u>F</u> inish |

10. <u>[Token Password]フィールドに**Cisco123**と入力し、[OK] をクリックします。____</u>

| 🤶 Token Logon | × | | | | |
|---|---------------------------------------|--|--|--|--|
| SafeNet S | SafeNet SafeNet Authentication Client | | | | |
| Enter the Token Passw | vord. | | | | |
| Token Name: | eToken PRO | | | | |
| Token Password: | •••••• | | | | |
| Current Language: EN This is an unlicensed copy for evaluation use only. | | | | | |
| | OK Cancel | | | | |

11. プロセスが成功したことを示す確認が表示されます。[Done] をクリックし、以上を確認し て CTL クライアントを終了します。

| 🧞 CTL Client v5.0 | | × | | | |
|---|-------------------------------------|--------|--|--|--|
| Cisc For IP | o CTL Client Telephony Solutions | cisco | | | |
| Server | File Location | Status | | | |
| 10.48.47.153 | /usr/local/cm/tftp/CTLFile.tlv | Passed | | | |
| 10.48.47.154 | /usr/local/cm/tftp/CTLFile.tlv | Passed | | | |
| | TIT | | | | |
| | | | | | |
| You must restart all the Cisco Unified Communications Manager and TFTP nodes in the Cluster. | | | | | |
| <u>H</u> elp | | Done | | | |

12. CallManager サービスに続いて Cisco TFTP を再起動します([Cisco Unified Serviceability] > [Tools] > [Control Center - Feature Services])。 新しい CTL ファイルが生成されます。 確認のために show ctl コマンドを入力します。

```
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. クラスタの各電話機から CTL ファイルを削除します(この手順は電話の種類により異なる ことがあります - 詳細は <u>Cisco Unified IP Phone 8961、9951、9971 アドミニストレーショ ンガイド</u>などのドキュメンテーションを参照してください)。注:電話機は(電話機のセ キュリティ設定に応じて)引き続き登録でき、手順13に進まなくても動作する場合があり ます。ただし、古いCTLファイルがインストールされます。このことにより、証明書を再 生成した場合、クラスタに他のサービスが追加された場合、サーバのハードウェアが交換 された場合に問題が発生することがあります。クラスタをこの状態で放置することは推奨 されません。
- 14. クラスタを非セキュアに変更してください。詳細は <u>CTL クライアントで CUCM クラスタ</u> <u>セキュリティを混合モードから非セキュアモードに変更するセクションを参照してくださ</u> <u>い。</u>

トラブルシュート

現在、この設定に関する特定のトラブルシューティング情報はありません。