PCCEソリューションでの自己署名証明書の交換

内容

概要
前提条件
要件
使用するコンポーネント
背景
手順
セクション 1：CVPサーバとADSサーバ間での証明書交換
手順1:CVPサーバ証明書のエクスポート
ステップ2:CVPサーバのWSM証明書をADSサーバにインポートする
ステップ3:ADSサーバ証明書のエクスポート
ステップ4:ADSサーバをCVPサーバおよびレポートサーバにインポートする
セクション 2：VOSプラットフォームアプリケーションとADSサーバ間での証明書交換
手順1:VOSプラットフォームアプリケーションサーバ証明書をエクスポートします。
ステップ2:VOSプラットフォームアプリケーションのADSサーバへのインポート
セクション 3：ロガー、PG、およびADSサーバ間での証明書交換
ステップ1:RoggerサーバとPGサーバからのIIS証明書のエクスポート
ステップ2:RoggerおよびPGサーバからのDiagnostic Framework Portico(DFP)証明書のエクスポート
ステップ3:ADSサーバへの証明書のインポート
セクション 4：CVP CallStudio WEBサービス統合
関連情報

概要

このドキュメントでは、Cisco Packaged Contact Center(PCCE)Enterprise(PCCE)ソリューションで、プリンシパル管理サーバ(ADS/AW)と他のアプリケーションサーバ間で自己署名証明書を交換する方法について説明します。

著者：Cisco TACエンジニア、Anuj Bhatia、Robert Rogier、Ramiro Amaya

前提条件

要件

次の項目に関する知識があることが推奨されます。

- PCCEリリース12.5(1)
- Customer Voice Portal(CVP)リリース12.5(1)

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- PCCE 12.5(1)
- CVP 12.5(1)

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。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景

12.xのPCCEソリューションでは、すべてのデバイスがSingle Pane of Glass(SPOG)を介して制御されます。SPOGはプリンシパルAWサーバでホストされます。PCCE 12.5(1)バージョンのsecurity-management-compliance(SRC)により、SPOGとソリューション内の他のサーバ間のすべての通信は、セキュアHTTPプロトコルを介して厳密に行われます。

証明書は、SPOGと他のデバイス間のシームレスでセキュアな通信を実現するために使用されます。自己署名証明書の環境では、サーバ間の証明書交換が必須になります。この証明書交換は、Smart Licensing、Webex Experience Management(WXM)、Customer Virtual Assistant(CVA)などの12.5(1)バージョンに存在する新機能を有効にするためにも必要です。

手順

これらは、自己署名証明書のエクスポート元のコンポーネントと、自己署名証明書をインポートする必要があるコンポーネントです。

(i)プリンシパルAWサーバ：このサーバーに必要な証明書：

- Windowsプラットフォーム： ICM: ルータとロガー(Rogger){A/B}、ペリフェラルゲートウェイ(PG){A/B}、すべてのADSサーバと電子メールおよびチャット(ECE)サーバ。 注：IISと診断フレームワークの証明書が必要です。CVP:CVPサーバ、CVP Reportingサーバ。 注 1：サーバからのWeb Service Management(WSM)証明書が必要です。注 2：証明書は完全修飾ドメイン名(FQDN)で指定する必要があります。
- VOSプラットフォーム：Cloud Connect、Cisco Virtual Voice Browser(VVB)、Cisco Unified Call Manager(CUCM)、Finesse、Cisco Unified Intelligent Center(CUIC)、ライブデータ(LD)、Identity Server(IDS)、およびその他の該当するサーバ。

ソリューション内の他のADSサーバについても同じです。

(ii) Router \ Logger Server:このサーバーに必要な証明書：

- Windowsプラットフォーム： すべてのADSサーバIIS証明書。

(iii) CUCM PGサーバ：このサーバーに必要な証明書：

- VOSプラットフォーム：CUCMパブリッシャ。 注：これは、CUCMサーバからJTAPIクライアントをダウンロードするために必要です。

(iv) CVPサーバ：このサーバーには次の証明書が必要です：

- Windowsプラットフォーム： すべてのADSサーバIIS証明書
- VOSプラットフォーム：WXM統合用Cloud Connectサーバ、セキュアSIPおよびHTTP通信用

VVBサーバ。

(v) CVPレポートサーバ：このサーバーに必要な証明書：

- Windowsプラットフォーム： すべてのADSサーバIIS証明書

(vi) VVBサーバ：このサーバーに必要な証明書：

- Windowsプラットフォーム：CVP VXMLサーバ（セキュアHTTP）、CVPコールサーバ（セキュアSIP）

ソリューションで自己署名証明書を効果的に交換するために必要な手順は、3つのセクションに分かれています。

セクション 1：CVPサーバとADSサーバ間での証明書交換。

セクション 2：VOSプラットフォームアプリケーションとADSサーバ間での証明書交換。

セクション 3：Roggers、PG、およびADSサーバ間での証明書交換。

セクション 1：CVPサーバとADSサーバ間での証明書交換

この交換を正常に完了するために必要な手順は次のとおりです。

手順1:CVPサーバのWSM証明書をエクスポートします。

ステップ2:CVPサーバのWSM証明書をADSサーバにインポートします。

ステップ3:ADSサーバ証明書をエクスポートします。

ステップ4:ADSサーバをCVPサーバおよびCVPレポートサーバにインポートします。

手順1:CVPサーバ証明書のエクスポート

証明書をCVPサーバからエクスポートする前に、サーバのFQDNを使用して証明書を再生成する必要があります。そうしないと、Smart Licensing、CVA、およびSPOGとのCVP同期などの機能で問題が発生する可能性があります。

注意：開始する前に、次の操作を行う必要があります。

- キーストアパスワードを取得します。次のコマンドを実行します。%CVP_HOME%\conf\security.propertiesの詳細
- %CVP_HOME%\conf\securityフォルダを別のフォルダにコピーします。
- コマンドウィンドウを管理者として開き、コマンドを実行します。

注：keytoolパラメータ – storepassを使用すると、このドキュメントで使用されているコマンドを合理化できます。すべてのCVPサーバについて、指定したsecurity.propertiesファイルから取得したパスワードを貼り付けます。ADSサーバの場合は、パスワードを入力します。**変更**

CVPサーバで証明書を再生成するには、次の手順を実行します。

(i)サーバ内の証明書の一覧表示

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
list
```

> **注**：CVPサーバには、次の自己署名証明書があります。wsm_certificate , vxml_certificate , callserver_certificateを参照してください。keytoolのパラメータ – vを使用すると、各証明書の詳細情報を確認できます。さらに、keytool.exe listコマンドの最後に「>」記号を追加して、出力をテキストファイルに送信できます。次に例を示します。 > test.txt

二旧自己署名証明書の削除

CVP servers :自己署名証明書を削除するコマンド：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias vxml_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias callserver_certificate
```

CVP Reporting servers：自己署名証明書を削除するコマンド。

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias wsm_certificate

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
delete -alias callserver_certificate
```

> **注**：CVPレポートサーバには、これらの自己署名証明書wsm_certificate、callserver_certificateがあります。

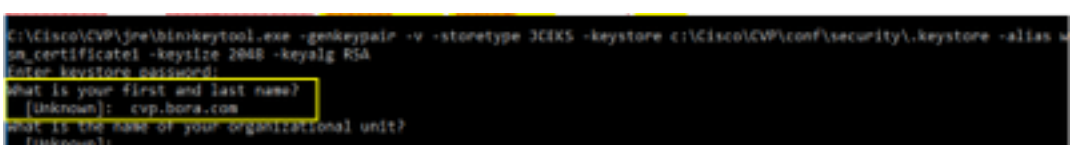
(iii)サーバのFQDNを使用して新しい自己署名証明書を生成します

CVPサーバ

WSMの自己署名証明書を生成するコマンド：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

質問に対してサーバのFQDNを指定します。**最初と最後の名前は何ですか。**



次の質問に答えてください。

組織単位の名前を入力してください。

[不明]:<OUを指定>

組織の名前は何ですか。

[不明]:<組織の名前を指定>

市または地域の名前は何ですか。

[不明]:<市区町村の名前を指定>

州の名前は何ですか。

[不明]:<都道府県の名前を指定>

このユニットの2文字の国コードは何ですか。

[不明]:<2文字の国番号を指定>

次の2つの入力に**yes**を指定します。

vxml_certificateとcallserver_certificateに対して同じ手順を実行します。

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias vxml_certificate -keysize 2048 -keyalg RSA -validity XXXX

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

CVPコールサーバをリブートします。

CVPレポートサーバ

WSMの自己署名証明書を生成するコマンド：

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias wsm_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

クエリのサーバのFQDNを指定します。**最初と最後の名前は何ですか？**CVPサーバと同じ手順に従います。

callserver_certificateについても同じ手順を実行します。

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
genkeypair -alias callserver_certificate -keysize 2048 -keyalg RSA -validity XXXX
```

レポートサーバをリブートします。

> **注：**デフォルトでは、自己署名証明書は2年間生成されます。-validity XXXXを使用して、証明書を再生成する際の有効期限を設定します。そうでない場合、証明書は90日間有効です

。これらの証明書のほとんどでは、3 ~ 5年は妥当な検証期間である必要があります。

次に、標準妥当性入力の一部を示します。

1年	365
2年	730
3年	1095
4年	1460
五年	1895
十年	3650

注意：12.5の証明書は、**SHA 256**、キーサイズ**2048**、および暗号化アルゴリズム**RSA**である必要があります。これらのパラメータを使用して、次の値を設定します。-keyalg RSAおよび – keysize 2048。CVPキーストアコマンドに – storetype JCEKSパラメータを含めることが重要です。これを行わないと、証明書、キー、またはキーストアが破損する可能性があります。

(iv) CVPサーバおよびレポートサーバからのwsm_Certificateのエクスポート

a)各CVPサーバから一時的な場所にWSM証明書をエクスポートし、証明書の名前を目的の名前に変更します。wsmcsX.crtという名前に変更できます。「X」を一意の数字または文字に置き換えます。つまり、wsmcsa.crt、wsmcsb.crtです。

自己署名証明書をエクスポートするコマンド：

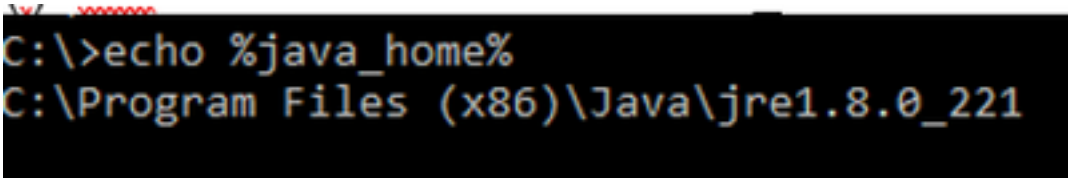
```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
export -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.crt
```

b)パス**C:\Cisco\CVP\conf\security\wsm.crt**から証明書をコピーし、名前をwsmcsX.crtに変更して、ADSサーバの一時フォルダに移動します。

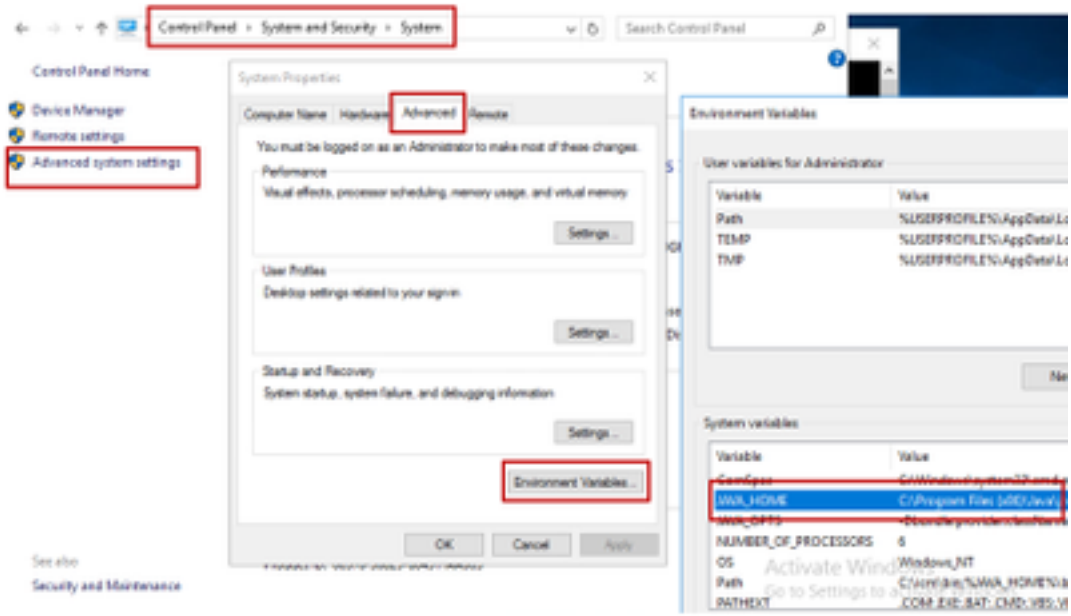
ステップ2:CVPサーバのWSM証明書をADSサーバにインポートする

ADSサーバに証明書をインポートするには、Javaツールセットの一部であるkeytoolを使用する必要があります。このツールがホストされているJavaホームパスを見つける方法がいくつかあります。

(i) CLIコマンド**> echo %JAVA_HOME%**



(ii)図に示すように、**高度なシステム設**定を使用して手動で行う。



PCCE 12.5のデフォルトパスは**C:\Program Files (x86)\Java\jre1.8.0_221\bin**です。

自己署名証明書をインポートするコマンド：

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_cvp} -file c:\temp\certs\wsmcsX.crt
```

> **注**：導入環境内の各CVPに対してコマンドを繰り返し、他のADSサーバで同じタスクを実行します

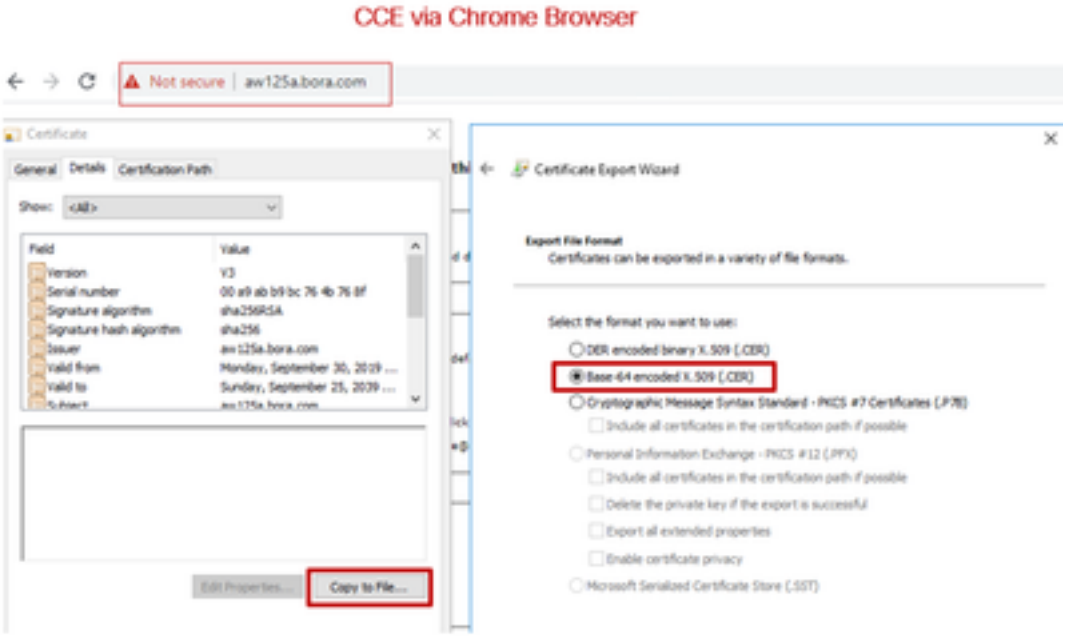
d) ADSサーバでApache Tomcatサービスを再起動します。

ステップ3:ADSサーバ証明書のエクスポート

CVP Reportingサーバの場合は、ADS証明書をエクスポートし、Reportingサーバにインポートする必要があります。内容は次のとおりです。

(i) ADSサーバで、ブラウザからサーバURL(https://{servername})に**移動します。**

(ii)証明書を一時フォルダに保存します。次に例を示します。**c:\temp\certsと入力**し、証明書に**ADS{svr}[ab].cerという名前を付けます。**



注：オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ4:ADSサーバをCVPサーバおよびレポートサーバにインポートする

(i)**C:\Cisco\CVP\conf\security**ディレクトリのCVPサーバおよびCVPレポートサーバに証明書をコピーします。

(ii)CVPサーバおよびCVPレポートサーバに証明書をインポートする。

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
import -trustcacerts -alias {fqdn_of_ads} -file %CVP_HOME%\conf\security\ICM{svr}[ab].cer
```

他のADSサーバーでも同じ手順を実行します。

(iii) CVPサーバとレポートサーバの再起動

セクション 2：VOSプラットフォームアプリケーションとADSサーバ間での証明書交換

この交換を正常に完了するために必要な手順は次のとおりです。

手順1:VOSプラットフォームアプリケーションサーバ証明書をエクスポートします。

ステップ2:VOSプラットフォームアプリケーション証明書をADSサーバにインポートします。

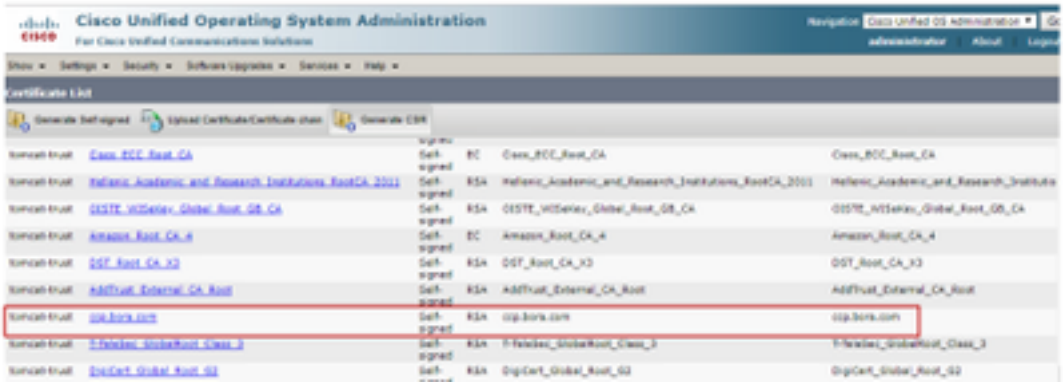
このプロセスは、次のようなすべてのVOSアプリケーションに適用されます。

- CUCM
- VVB
- Finesse
- CUIC \ LD \ IDS
- Cloud Connect

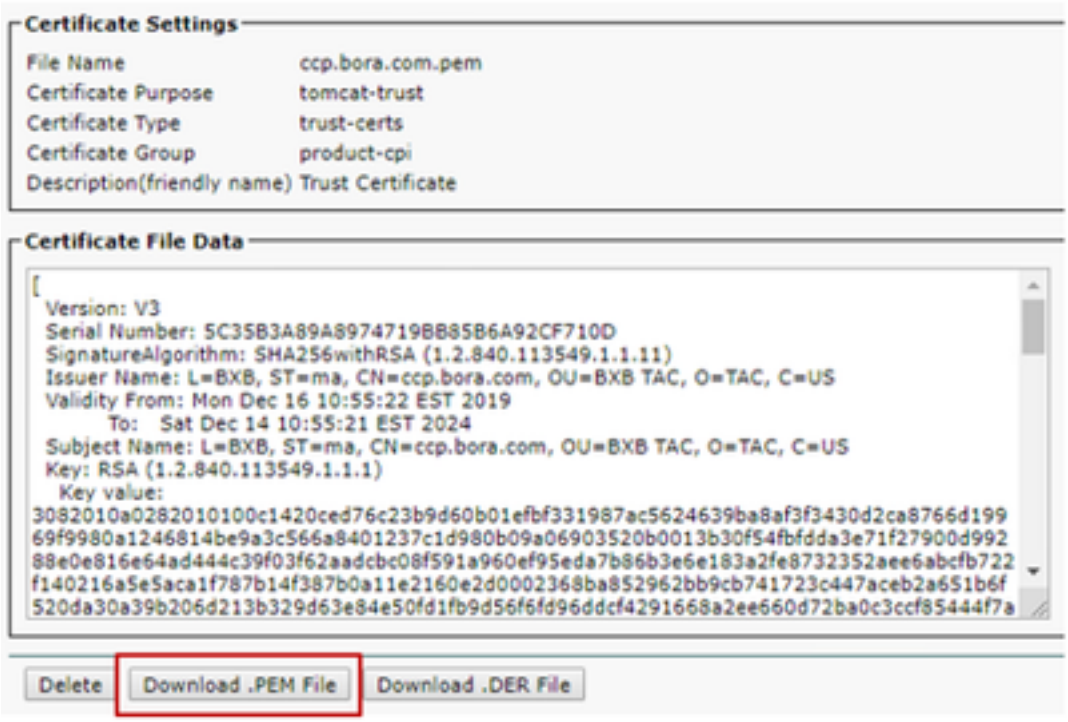
手順1:VOSプラットフォームアプリケーションサーバ証明書をエクスポートします。

(i)[Cisco Unified Communications Operating System Administration]ページに移動します。
https://FQDN:8443/cmplatform

(ii) [Security] > [Certificate Management] に移動し、**tomcat-trust**フォルダにあるアプリケーションプライマリサーバ証明書を見つけます。



(iii)証明書を選択し、[download .PEM file]をクリックしてADSサーバの一時フォルダに保存します。



注：サブスクライバに対して同じ手順を実行します。

ステップ2:VOSプラットフォームアプリケーションのADSサーバへのインポート

キーツールを実行するパス：**C:\Programファイル(x86)\Java\jre1.8.0_221\bin**

自己署名証明書をインポートするコマンド：

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
```

```
storepass changeit -alias {fqdn_of_vos}  -file c:\temp\certs\vosapplicationX.cer
```

ADSサーバでApache Tomcatサービスを再起動します。

注：他のADSサーバーでも同じタスクを実行します

セクション 3：ロガー、PG、およびADSサーバ間での証明書交換

この交換を正常に完了するために必要な手順は次のとおりです。

ステップ 1：RoggerおよびPGサーバからのIIS証明書のエクスポート

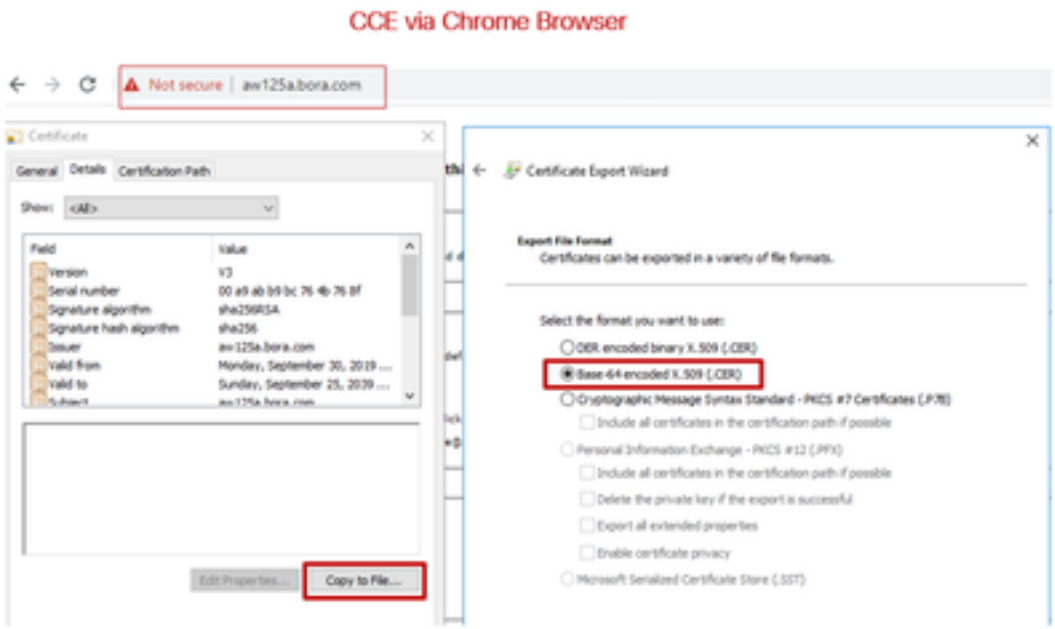
ステップ 2：RoggerおよびPGサーバからのDiagnostic Framework Portico(DFP)証明書のエクスポート

ステップ 3：ADSサーバへの証明書のインポート

ステップ1:RoggerサーバとPGサーバからのIIS証明書のエクスポート

(i)ブラウザからADSサーバ上で、サーバ(Roggers、PG)のURL:**https://{servername}に移動します。**

(ii)証明書を一時フォルダ(**c:\temp\certsなど)に保存し、証明書にICM{svr}[ab].cerという名前を付けます**

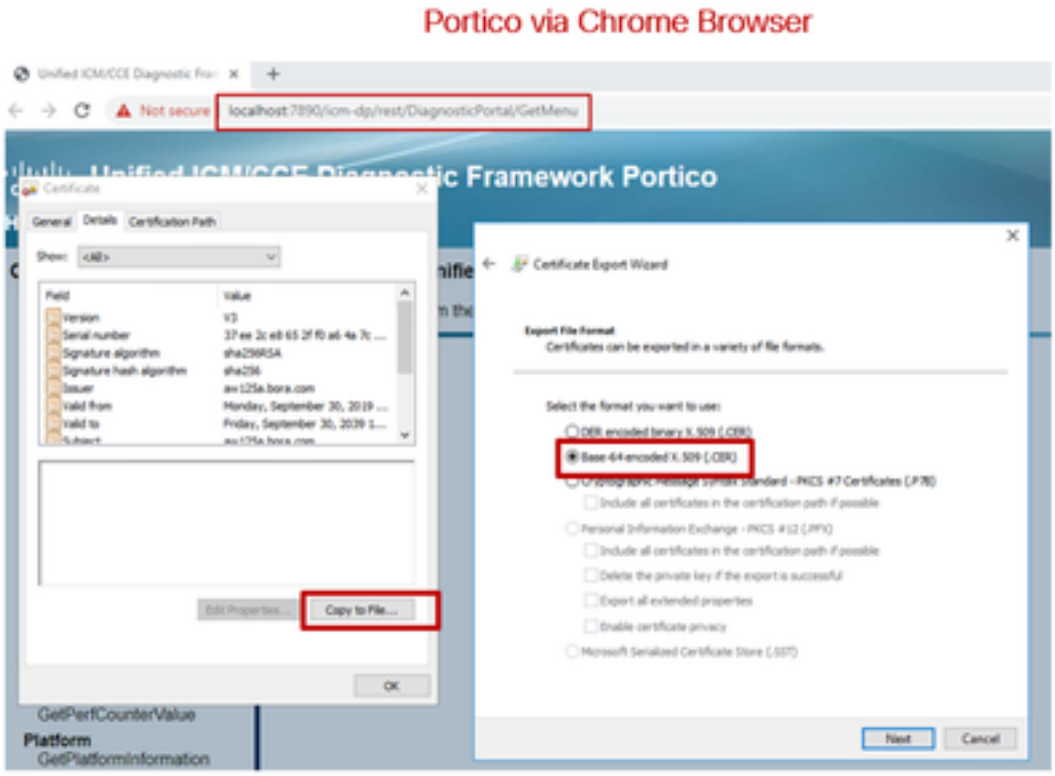


注：オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ2:RoggerおよびPGサーバからのDiagnostic Framework Portico(DFP)証明書のエクスポート

(i)ブラウザからADSサーバで、サーバ(Roggers、PG) DFPのURL:***https://{servername}:7890/icm-dp/rest/DiagnosticPortal/GetProductVersionに移動します。***

(ii)証明書をフォルダexample c:\temp\certsに保存し、証明書にdfp{svr}[ab].cerという名前を付けます



注：オプションBase-64 encoded X.509 (.CER)を選択します。

ステップ3:ADSサーバへの証明書のインポート

IIS自己署名証明書をADSサーバにインポートするコマンド。キーツールを実行するパス：**C:\Program Files (x86)\Java\jre1.8.0_221\bin**

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_IIS -file c:\temp\certs\ ICM{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_IIS -file c:\temp\certs\ICMrgra.cer
```

注： すべてのADSサーバにエクスポートされたすべてのサーバ証明書をインポートします。

診断の自己署名証明書をADSサーバにインポートするコマンド

```
keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -import -
storepass changeit -alias {fqdn_of_server}_DFP -file c:\temp\certs\ dfp{svr}[ab].cer

Example: keytool -keystore "C:\Program Files (x86)\Java\jre1.8.0_221\lib\security\cacerts"  -
import -storepass changeit -alias myrgra.domain.com_DFP -file c:\temp\certs\dfprgra.cer
```

注：すべてのADSサーバにエクスポートされたすべてのサーバ証明書をインポートします。

ADSサーバでApache Tomcatサービスを再起動します。

セクション 4：CVP CallStudio WEBサービス統合

Web Services ElementおよびRest_Client要素のセキュアな通信を確立する方法の詳細については、

『Cisco Unified CVP VXML ServerおよびCisco Unified Call Studioリリース12.5(1)のユーザガイド – Webサービス統合[Cisco Unified Customer Voice Portal] - Cisco

関連情報

- CVP設定ガイド：CVPコンフィギュレーションガイド – セキュリティ
- UCCE設定ガイド：UCCEコンフィギュレーションガイド：セキュリティ
- 『PCCE Administration Guide:PCE管理ガイド：セキュリティ
- UCCE自己署名証明書：Exchange UCCE自己署名証明書
- CCE 12.5(1)でのOpenJDKのインストールと移行：CCE OpenJDKの移行
- CVP 12.5(1)でのOpenJDKのインストールと移行：CVP OpenJDKの移行