相互認証を使用したCVP OAMPとCVPコンポーネント間のセキュアJMX通信

内容

概要

このドキュメントでは、認証局(CA)署名付き証明書を使用して、Customer Voice Portal(CVP)Operation and Management Console(OAMP)とCisco Unified Contact Center Enterprise(UCCE)ソリューションのCVP ServerおよびCVP Reporting server間のJava Management Extensions(JMX)通信をををでで保護するするののの方法についてについて説明します。

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。

- UCCE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。

- UCCE 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。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

OAMPは、JMXプロトコルを介してCVP Call Server、CVP VXML Server、およびCVP Reporting Serverと通信します。OAMPとこれらのCVPコンポーネント間のセキュアな通信により、JMXセキュリティの脆弱性を防止します。このセキュアな通信はオプションであり、OAMPとCVPコンポーネント間の通常の動作には必要ありません。

JMX通信を保護するには、次の方法があります。

- CVPサーバおよびCVPレポートサーバで、Webサービスマネージャ(WSM)の証明書署名要求(CSR)を生成します。
- CVPサーバおよびCVPレポートサーバでWSM用のCSRクライアント証明書を生成します。
- OAMP用のCSRクライアント証明書を生成します（OAMPで実行します）。
- 認証局によって証明書に署名します。
- CA署名付き証明書、ルートおよび中間をCVPサーバ、CVPレポートサーバ、およびOAMPにインポートします。
- [オプション]OAMPへのセキュアJConsoleログイン
- Secure System CLI。

WSMのCSR証明書の生成

ステップ1:CVPサーバまたはレポートサーバにログインします。**security**.propertiesファイルからキーストアのパ**スワードを取得**します。

> **注**：コマンドプロンプトにmore %CVP_HOME%\conf\security.propertiesと入力します。Security.keystorePW = <キーストアのパスワードを返す>プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ 2： %CVP_HOME%\conf\security and delete the WSM certificateに移動します。このコマンドを使用します。

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

プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ3:CVPサーバのCall Server証明書とVXML Server証明書、およびReporting ServerのCall Server証明書について、ステップ2を繰り返します。

ステップ4:WSMサーバのCA署名付き証明書を生成します。コマンド

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

1. プロンプトで詳細を入力し、「**Yes**」と入力して**確認**します。
2. プロンプトが表示されたら、キーストアパスワードを入力します。

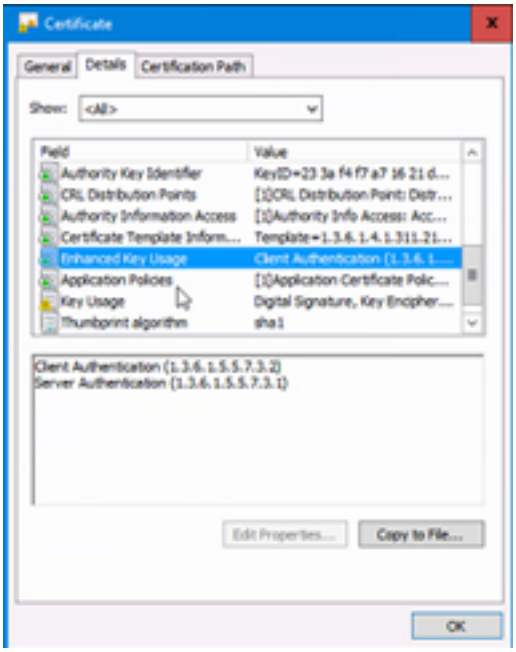
> **注**：今後の参照用にCN名をメモします。

ステップ5：エイリアスの証明書要求を生成します。このコマンドを実行し、ファイルに保存します(例： **wsm.csr**

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr

1.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ6:CAによって署名された証明書を取得します。CA認証局を使用してCA署名付き証明書を作成する手順に従い、CAが署名付き証明書を生成する際にクライアント/サーバ証明書認証テンプレートを使用することを確認します。



ステップ7：署名付き証明書、CA認証局のルート証明書、中間証明書をダウンロードします。

ステップ8：ルート、中間、およびCA署名付きWSM証明書を**%CVP_HOME%\conf\security\にコピーします**。

ステップ9：このコマンドを使用してルート証明書をインポートします。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cer>。

1. プロンプトが表示されたら、キーストアパスワードを入力します。
2. [この証明書を信頼する]プロンプトで、[はい]と**入力します**。

ステップ10：このコマンドを使用して中間証明書をインポートします。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate -file %CVP_HOME%\conf\security\<filename_of_intermediate_cer>。

1. プロンプトが表示されたら、キーストアパスワードを入力します。
2. [この証明書を信頼する]プロンプトで、[はい]と**入力します**。

ステップ11：このコマンドを使用して、CA署名付きWSM証明書をインポートします。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>。

1.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ12:CVPサーバのCall Server証明書とVXML Server証明書およびReporting ServerのCall Server証明書について、ステップ4 ~ 11（ルート証明書と中間証明書を2回インポートする必要はありません）を繰り返します。

ステップ13 CVPでWSMを設定します。

1. c:\cisco\cvp\conf\jmx_wsm.confに移動します。

次のようにファイルを追加または更新し、保存します。

```
javax.net.debug = all com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 3000
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore javax.net.ssl.keyStorePassword=<
keystore_password > javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password > javax.net.ssl.trustStoreType=JCEKS
```

2. regeditコマンドを実行します。

```
Append this to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
Foundation\Procrun 2.0\WebServicesManager\Parameters\Java:
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=
```

ステップ14:CVPサーバおよびレポートサーバでCVP CallserverのJMXを設定します。

1. c:\cisco\cvp\conf\jmx_callserver.confに移動します。

次のようにファイルを更新し、保存します。

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 2098
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 2097
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore javax.net.ssl.keyStorePassword =
```

ステップ15:CVPサーバでVXMLServerのJMXを設定します。

1. c:\cisco\cvp\conf\jmx_vxml.confに移動します。

次のようにファイルを編集して保存します。

```
com.sun.management.jmxremote.ssl.need.client.auth = true
com.sun.management.jmxremote.authenticate = false com.sun.management.jmxremote.port = 9696
com.sun.management.jmxremote.ssl = true com.sun.management.jmxremote.rmi.port = 9697
javax.net.ssl.keyStore = C:\Cisco\CVP\conf\security\.keystore javax.net.ssl.keyStorePassword =
```

2. regeditコマンドを実行します。

- ```
  Append theese to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
  Foundation\Procrun 2.0\VXMLServer\Parameters\Java:
  Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
  Djavax.net.ssl.trustStorePassword=
  ```

3. CVPサーバのWSMサービス、コールサーバおよびVXMLサーバサービス、およびレポートサーバのWSMサービスとコールサーバサービスを再起動します。

注： JMXでセキュア通信が有効になっている場合、キーストアは%CVP_HOME%\conf\security\.keystoreではなく**%CVP_HOME%\jre\lib\security\cacerts.keystore**になります。したがって、**%CVP_HOME%\jre\lib\security\cacertsからの証明書を%CVP_HOME%\conf\security\.keystoreにインポートします。**

WSM用のCA署名付きクライアント証明書の生成

ステップ1:CVPサーバまたはレポートサーバに口グインします。**security**.propertiesファイルからキーストアのパ**スワードを取得**します。

注：コマンドプロンプトにmore %CVP_HOME%\conf\security.propertiesと入力します。Security.keystorePW = <キーストアのパスワードを返す>プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2:%CVP_HOME%\conf\security and generate a CA-signed certificate for client authentication with callserver with this commandに移動します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of CVP Server or Reporting Server WSM certificate> -v -keysize 2048 -keyalg RSA

1.プロンプトで詳細を入力し、「**Yes**」と入力**して確認**します。
2.プロンプトが表示されたら、キーストアパスワードを入力します。

注：エイリアスは、WSMサーバ証明書の生成に使用されるCNと同じです。

ステップ3：このコマンドを使用してエイリアスの証明書要求を生成し、ファイルに保存します(例：**jmx_client.csr**)。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP Server or Reporting Server WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr

1.プロンプトが表示されたら、キーストアパスワードを入力します。
2.次のコマンドを使用して、CSRが正常に生成されたことを確認します。**dir jmx_client.csr**

ステップ4:CAでJMXクライアント証明書に署名します。

注：CA認証局を使用してCA署名付き証明書を作成する手順に従います。CA署名付きJMXクライアント証明書をダウンロードします（ルート証明書と中間証明書は、以前にダウ
  ```

ンロードおよびインポートされているため、必要ありません）。

1.プロンプトが表示されたら、キーストアパスワードを入力します。
2. Trust this certificateプロンプトで、Yesと入力します。

ステップ5:CA署名付きJMXクライアント証明書を**%CVP_HOME%\conf\security\にコピーします。**

ステップ6：このコマンドを使用して、CA署名付きJMXクライアント証明書をインポートします。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of CVP Server or Reporting Server WSM certificate> -file %CVP_HOME%\conf\security\<filename of CA-signed JMX Client certificate>

1.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ7:Cisco CVP Call Server、VXML Server、およびWSMサービスを再起動します。

ステップ8:Reporting Serverを実装している場合は、同じ手順を繰り返します。

OAMP用のCA署名付きクライアント証明書の生成（OAMPで実行）

ステップ1:OAMPサーバにログインします。**security**.propertiesファイルからキーストアの**パスワードを取得**します。

> **注：**コマンドプロンプトにmore **%CVP_HOME%\conf\security.propertiesと入力します。**
> Security.keystorePW = <キーストアのパスワードを返す>プロンプトが表示されたら、キーストアのパスワードを入力します。

ステップ2: **%CVP_HOME%\conf**セキュリティに移動し、CVPサーバWSMを使用したクライアント認証用のCA署名付き証明書を生成します。このコマンドを使用します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of OAMP Server WSM certificate> -v -keysize 2048 -keyalg RSA.

1.プロンプトで詳細を入力し、「Yes」と入力して確認します。
2.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ3：このコマンドを使用してエイリアスの証明書要求を生成し、ファイル(例：**jmx.csr**)に保存します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP Server WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr

1.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ4:CAで証明書に署名します。

> **注**：手順に従って、CA認証局を使用してCA署名付き証明書を作成します。CA認証局の証明書とルート証明書をダウンロードします。

ステップ5：ルート証明書とCA署名付きJMXクライアント証明書を**%CVP_HOME%\conf\security\にコピーします。**

ステップ6:CAのルート証明書をインポートします。このコマンドを使用します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>。

1.プロンプトが表示されたら、キーストアパスワードを入力します。
2. Trust this certificateプロンプトで、Yesと入力します。

ステップ7:CVPのCA署名付きJMXクライアント証明書をインポートします。このコマンドを使用します。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>。

1.プロンプトが表示されたら、キーストアパスワードを入力します。

ステップ8:OAMPサービスを再起動します。

ステップ9:OAMPにログインして、OAMPとコールサーバまたはVXMLサーバ間のセキュアな通信を有効にします。 [**Device Management**] > [**Call Server**]**に移動します。**[Enable secure communication with the Ops console]チェックボックスをオンにします。Call ServerとVXML Serverの両方を保存して導入します。

ステップ10:regeditコマンドを実行します。

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Javaに移動**します。**

これをファイルに追加して保存します。

```
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=
```

> **注：** JMXのポートを保護した後、JConsoleにアクセスできるのは、Oracleドキュメントに記載されているJConsoleに対して定義された手順を実行した後だけです。

関連情報

- CVPセキュア設定ガイド
- テクニカル サポートとドキュメント – Cisco Systems