CVPスマートライセンスCSSM証明書のインポート手順

内容

問題

CVP Call Serverで、SmartAgentログにスマートライセンスの「署名の確認」エラーが記録される。通常のライセンスステータスの更新プロセスで署名検証エラーが発生した場合、システムでCSSM(Cisco Smart Software Manager)証明書をCVPキーストアにインポートして解決する必要があります。適切なCSSM証明書チェーンがないと、CVPはCisco Smart Software Managerとのライセンストランザクションを検証できないため、ライセンスコンプライアンスの問題が発生します。

環境

- Cisco Customer Voice Portal(CVP)Call Serverバージョン12.6.2
- Contact Center Software - Packaged Contact Center Enterprise(PCCE)
- CVPサービス：Call Server、WSM(Web Service Manager)、VXML Server
- 証明書管理用のJava JCEKSキーストア形式
- Smart LicensingとCisco Smart Software Manager(CSSM)の統合

解決方法

次の詳細な手順に従って、CSSM証明書をCVP Call Serverキーストアにインポートします。

ステップ1：キーストアパスワードの識別

管理者としてコマンドウィンドウを開き、CVPホームディレクトリに移動してキーストアパスワードを復号化します。

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

このユーティリティで表示されるパスワードを、以降のすべてのkeytoolコマンドで必要になるとおりに記録します。

ステップ2：現在のキーストアのバックアップ

セキュリティディレクトリから既存のキーストアのバックアップを作成します。

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

ステップ3：現在のキーストアの内容の工クスポート

参照用にキーストア内の現在のすべての証明書のリストを生成します。

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

生成されたファイルを確認して、現在の証明書インベントリを理解します。

ステップ4:CSSM証明書のダウンロード

CVP Licensingページのトランスポートから、必要なCSSM証明書チェーンを取得します。証明書の要件は、証明書のタイプによって異なります。

CA署名付き証明書：ルート証明書と中間証明書を.cer形式で個別にダウンロードします。

自己署名証明書：CSSM証明書を直接ダウンロードします。

証明書ファイルをCVPセキュリティディレクトリに保存します。

```
%CVP_HOME%\conf\security
```

ステップ5:CSSMルート証明書（CA署名付き）をインポートする

CA署名付き証明書の場合は、最初に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" -impor
```

ステップ6:CSSM中間証明書（CA署名付き）のインポート

中間証明書が存在する場合は、次のコマンドを使用してインポートします。

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

ステップ7：自己署名CSSM証明書のインポート（代替）

自己署名証明書の場合は、CSSM証明書を直接インポートします。

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

ステップ8：証明書インポートの確認

キーストアに新しい証明書が存在することを確認します。

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

新しい証明書リストを確認して、CSSM証明書が正常にインポートされたことを確認します。

ステップ9：リブートとサービスの検証

CVPサーバをリブートし、再起動時間を記録します。リブート後、すべてのCVPサービスが起動していることを確認します。

- コールサーバ
- WSM（Webサービスマネージャ）
- VXMLサーバ

サービスの起動後、約20分待ってから検証に進みます。

ステップ10：解決の検証

次の検証手順を実行します。

SmartAgentログの確認：

C:\Cisco\CVP\logs\WSMに移動し、更新日でソートします。SmartAgentログで最新の15分間のステータスレポートを確認します。再起動後は、シグニチャの検証例外が表示されなくなっている必要があります。

ライセンスのステータスを確認します。

CVPライセンスページにアクセスし、システムに「登録済み」と「コンプライアンス中」のステータスがエラーなしで表示されていることを確認します。

ロールバック手順（問題が発生した場合）

証明書のインポートプロセス中に問題が発生した場合は、次のロールバックステップに従います。

ステップ1：すべてのCVPサービス(Call Server、WSM、VXML)を停止します。

ステップ2：セキュリティディレクトリに移動します。

```
cd %CVP_HOME%\conf\security
```

ステップ3：変更したキーストアを削除します。

```
del .keystore
```

ステップ4：バックアップキーストアを復元します。

```
rename backup.keystore .keystore
```

ステップ5：すべてのCVPサービスを再起動します。

原因

CVP Call Serverキーストアに、Cisco Smart Software Managerからのデジタル署名の検証に必要なCSSM証明書チェーンが含まれていません。Smart Licensingの操作中に、CVPは証明書ベースの署名検証を使用して、ライセンス通信の信頼性を検証しようとします。Java JCEKSキーストアに適切なCSSM証明書がないと、これらの署名検証の試行が失敗し、ライセンストランザクションエラーとコンプライアンスの問題が発生する可能性があります。

関連コンテンツ

- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。