CVP VXMLサーバのさまざまなインターフェイスでTLS 1.2を有効にする方法

内容

[概要](#)
[前提条件](#)
[要件](#)
[使用するコンポーネント](#)
[背景説明](#)
[VXMLサーバのTLSインターフェイス](#)
[問題：CVP VXMLサーバのさまざまなインターフェイスでTLS 1.2を有効にする方法](#)
[解決方法](#)
[インターフェイス1でTLS 1.2を有効にする手順](#)
[インターフェイス2でTLS 1.2を有効にする手順](#)
[インターフェイス3でTLS 1.2を有効にする手順](#)
[TLS 1.2サポート用JREをアップグレードする手順](#)
[Tomcatをアップグレードする手順](#)

概要

このドキュメントでは、Cisco Customer Voice Portal(CVP)Call ServerおよびVoice Extensible Markup Language(VXML)Server Transport Layer Security(TLS)のHyperText Transfer Protocol(HTTP)サポートを設定する方法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。

- CVP VXMLサーバ
- Cisco Virtual Voice Browser(CVVB)
- VXMLゲートウェイ

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。

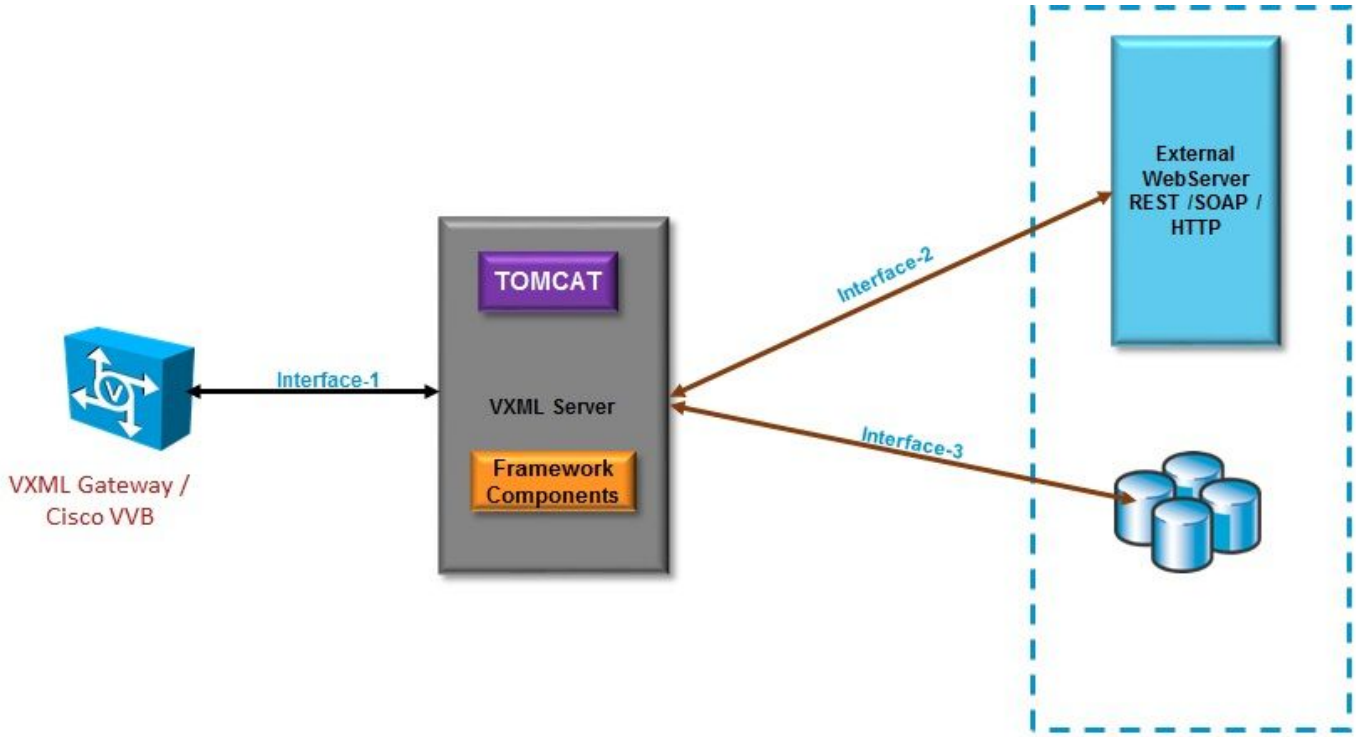
- CVP 11.5(1)
- CVVB 11.5(1)

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。

背景説明

現在、VXMLサーバは、図に示すように、異なるコンポーネントを持つ3つのセキュアなインターフェイスを持つことができます。



VXMLサーバのTLSインターフェイス

インターフェイス1.これは、VXMLゲートウェイ、Cisco Virtualized Voice Browser(CVVB)、およびVXMLサーバ間のハイパーテキスト転送プロトコル(HTTP)インターフェイスです。ここでは、VXMLサーバがサーバとして動作します。

インターフェイス2。これは、VXMLサーバがHTTP/Simple Object Access Protocol(SOAP)インターフェイスを使用する外部Webサーバと通信する一般的なHTTPインターフェイスです。このインターフェイスは、カスタム要素、WebService要素、またはSOAP要素の一部として定義されます。

インタフェース3。これは、組み込みのDB要素インタフェースまたはカスタム要素インタフェースを使用する外部データベース(DB) (Microsoft Structured Query Language (MSSQL) ServerおよびORACLE DB)です。

このシナリオでは、インターフェイス1.ではVXMLサーバがサーバとして機能し、インターフェイス2.および3.ではVXMLサーバがセキュアクライアントとして機能します。

問題：CVP VXMLサーバのさまざまなインターフェイスでTLS

1.2を有効にする方法

CVP VXMLサーバは、さまざまなインターフェイスを使用してさまざまなデバイスやサーバと通信します。必要なセキュリティレベルを実現するには、すべてのTLS 1.2を有効にする必要があります。

解決方法

インターフェイス1でTLS 1.2を有効にする手順

このインターフェイスでは、前述のように、CVP VXMLサーバがサーバとして機能します。この安全な実装は、Tomcatによって行われます。この構成は、Tomcatの**server.xmlによって制**御されます。

一般的なコネクタ設定：

```
<Connector SSLCertificateFile="C:\Cisco\CVP\conf\security\vxml.crt"
SSLCertificateKeyFile="C:\Cisco\CVP\conf\security\vxml.key" SSLEnabled="true" acceptCount="1500"
ciphers="TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256,TLS_RSA_W
ITH_AES_256_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA256"
clientAuth="false" disableUploadTimeout="true" enableLookups="false" executor="tomcatThreadPool"
keyAlias="vxml_certificate"
keystoreFile="C:\Cisco\CVP\conf\security\.keystore"
keystorePass="3WJ~RH0WjKgyq3CKl$x?7f0?JU*7R3}WW0jE,I*_RC8w2Lf" keystoreType="JCEKS"
maxHttpHeaderSize="8192" port="7443"
protocol="org.apache.coyote.http11.Http11NioProtocol" scheme="https" secure="true"
sslEnabledProtocols="TLSv1, TLSv1.1, TLSv1.2" sslProtocol="TLS"/>
```

この例にはTLS v1.2が含まれているため、設定が必要なパラメータ(sslEnabledProtocolsとcertificate)には、TLS 1.2をサポートするために必要な設定が含まれています。

Java **keytool.exeを使用**して、TLS 1.2証明書を生成します。このツールは、Cisco\CVP\jre\bin\から入手で**きます。**

Keytoolドキュメント

インターフェイス2でTLS 1.2を有効にする手順

これは、最も一般的に使用されるインターフェイスです。ここでは、VXMLサーバがクライアントとして機能し、外部WebServerとのセキュアな通信を開く必要があります。

これを処理する方法は2つあります。

- カスタムコードを使用します。
- CVPフレームワークを使用します。

ここでは、CVPフレームワークの使用について説明します。

11.6以降では、デフォルトで有効になっています。以前のバージョンでは、次の表を確認してください。

CVP Version	ES release	JAVA Version	Support
9.0	NA	JRE 1.6	Upgrade JAVA to 111 and above for 1.2 support and customer has to implement custom java code to handle TLS1.2 (Refer to the example)
10.0	NA	JRE 1.6	Customer has to implement TLS 1.2 in Customer code (Refer to the example).Upgrade to JRE111 or upgrade to 1.7.
10.5	ES-26	JAVA 1.7 32 bit	JAVA In built support for TLS1.2, no update of JAVA required
11.0	ES-23	JAVA 1.7 32 Bit	JAVA In built support for TLS1.2, no update of JAVA required
11.5	ES-12	JAVA 1.7 64 Bit	JAVA In built support for TLS1.2, no update of JAVA required
11.6	NA	JRE 1.7 64 bit	

この不具合の影響を受けるESリリース(CSCvc39129 VXML Server as TLS client)がインストールされている場合は、次の手動設定を適用する必要があります。

ステップ1：レジストリエディタを開き、HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Javaに移動します。

ステップ2：オプションキーを開き、最後に-Dhtps.client.protocol=TLSv1.2を追加します。

ステップ3:Cisco CVP VXMLServerサービスを再起動します。

異なるJAVAバージョンでのデフォルトのプロトコルサポートのクイックリストを次に示します。

	JDK 8 (March 2014 to present)	JDK 7 (July 2011 to present)	JDK 6 (2006 to end of public updates 2013)
TLS Protocols	TLSv1.2 (default) TLSv1.1 TLSv1 SSLv3	TLSv1.2 TLSv1.1 TLSv1 (default) SSLv3	TLS v1.1, TLS v1.2 (JDK 6 update 111 and above) TLSv1 (default) SSLv3

```
-Djdk.tls.client.protocols=TLSv1.2.
```

この設定では、VXMLサーバがJava SE Development Kit(JDK)7およびJDK6でTLS 1.2を使用することを義務付けています。

注:SSLはデフォルトで無効になっています。

インターフェイス3でTLS 1.2を有効にする手順

CVP VXML

TLS 1.2TLS 1.2

SQL Server 2014 with Service Pack (SP) 2SQL Server 2014TLS 1.2TLS 1.2 TLS 1.2SQL

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

CVP3TLS 1.2

1HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java

2**-Djdk.tls.client.protocols=TLSv1.2**

3:Cisco CVP VXMLServer

> **注**：詳細については、このバグを確認してくださいい：CSCvg20831 JNDIデータベース接続がCVP11.6 SQL 2014SP2で失敗します。

TLS 1.2サポート用JREをアップグレードする手順

CVPは、バグ不具合の最新バージョンへのJava Runtime Environment(JRE)のアップグレードをサポートしています。

次の表に、JAVAのバージョンを示します。

CVP Version	JRE	TOMCAT
9.0	java version "1.6.0_67" 32 –Bit Server	Apache Tomcat/6.0
10.0	java version "1.6.0_67" 32 –Bit Server	Apache Tomcat/7.0
10.5	java version "1.7.0_45" 32 –Bit Server	Apache Tomcat/7.0
11.0	java version "1.7.0_67" 32 –Bit Server	Apache Tomcat/7.0
11.5	java version "1.7.0_67" 64 –Bit Server	Apache Tomcat/8.0
11.6	java version "1.8.0_67" 64 –Bit Server	Apache Tomcat/8.0

JAVAバージョン

このリンクで説明する手順に従います。

> **注意**：32ビットから64ビットへのアップグレードはサポートされていません

Tomcatをアップグレードする手順

Tomcatマイナーアップグレードがサポートされます。ただし、アップグレードを実行する前に、カスタムjar（AXIS、JDBCなど）間の互換性の問題を確認してください。

詳細については、この手順を参照してください。