如何在CVP VXML伺服器的不同介面上啟用TLS 1.2

目錄

簡介

本檔案介紹如何設定對超文字傳輸通訊協定(HTTP)的思科客戶語音入口網站(CVP)通話伺服器和語音可延伸標籤語言(VXML)伺服器傳輸層安全(TLS)支援。

必要條件

需求

思科建議您瞭解以下主題：

- CVP VXML伺服器
- Cisco Virtual Voice Browser(CVVB)
- VXML網關

採用元件

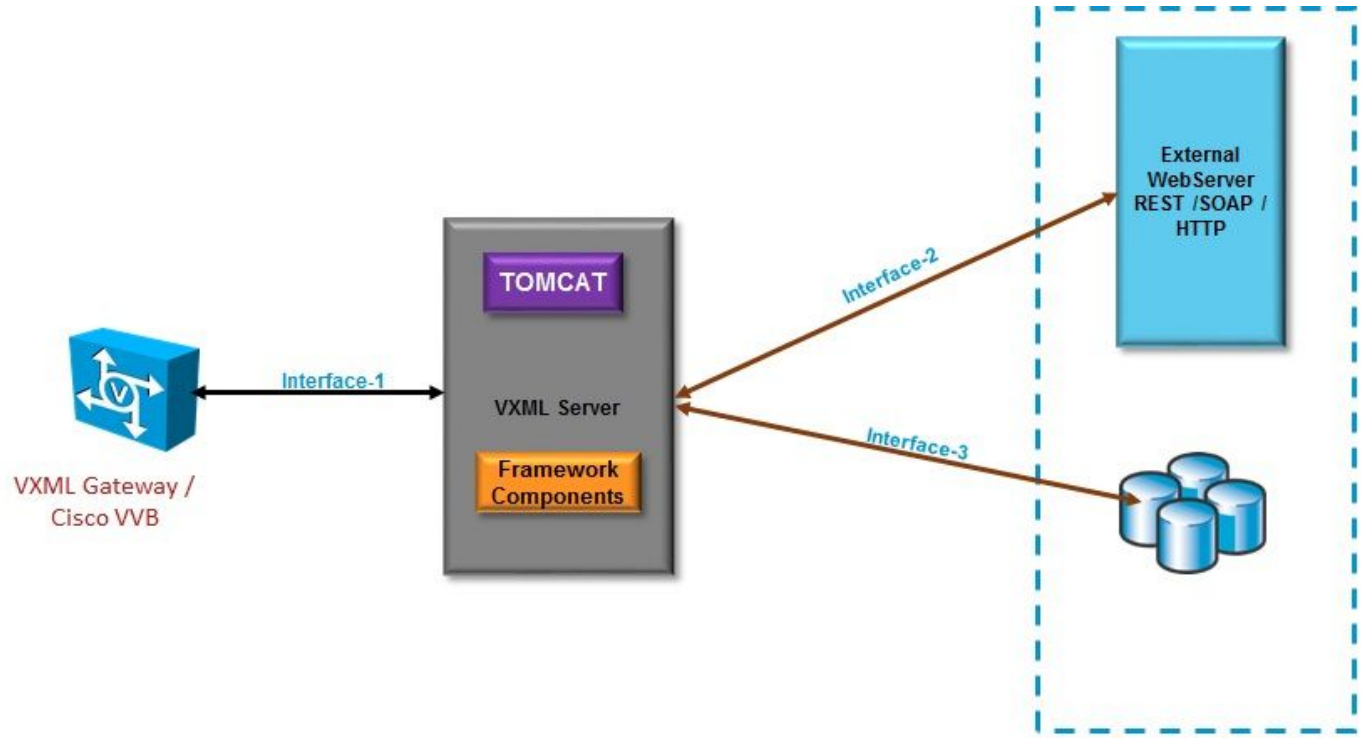
本檔案中的資訊是根據以下軟體版本：

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

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

目前，VXML伺服器可以具有三個具有不同元件的安全介面，如下圖所示。



VXML伺服器的TLS介面

介面1。這是VXML網關、思科虛擬化語音瀏覽器(CVVB)和VXML伺服器之間的超文本傳輸協定(HTTP)介面。在這裡，VXML伺服器充當伺服器。

介面2.這是典型的HTTP介面，其中VXML伺服器與使用HTTP/簡單對象訪問協定(SOAP)介面的外部Web伺服器進行互動。此介面被定義為自定義元素、WebService元素或SOAP元素的一部分。

介面3.這是外部資料庫(DB)(Microsoft Structured Query Language(MSSQL)Server和ORACLE DB)，它使用內建的資料庫元素介面或自定義元素介面。

在此場景中，在介面1.中，VXML伺服器充當伺服器，而在介面2.和3.中，VXML伺服器充當安全客戶端。

問題：如何在CVP VXML伺服器的不同介面上啟用TLS 1.2

CVP VXML伺服器通過不同的介面與各種裝置和伺服器通訊。必須在所有裝置上啟用TLS 1.2才能達到所需的安全級別。

解決方案

在介面1中啟用TLS 1.2的過程

在此介面中，如前所述，CVP VXML伺服器充當伺服器。此安全實現由Tomcat完成。此配置由

Tomcat中的**server.xml**控制。

典型聯結器配置：

```
<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"/>
```

此示例使用TLS v1.2，因此需要配置的引數(sslEnabledProtocols和certificate)具有支援TLS 1.2所需的配置。

使用java **keytool.exe**以生成TLS 1.2證書。此工具位於**Cisco\CVP\jre\bin**。

Keytool文檔

在介面2中啟用TLS 1.2的過程

這是最常用的介面。在這裡，VXML伺服器充當客戶端，需要開啟與外部Web伺服器的安全通訊。

有兩種不同的處理方式。

- 使用自定義代碼。
- 使用CVP框架。

這描述了CVP框架的使用。

自11.6起，預設情況下啟用此功能，對於以前的版本，請檢查此表：

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	

如果安裝了受此缺陷影響的ES版本： CSCvc39129 VXML Server as TLS client，則需要應用以下手動配置：

步驟1.開啟登錄檔編輯器並導航至**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**。

步驟2.開啟**選項鍵**，並在末尾開啟add-**Dhttps.client.protocol=TLSv1.2**。

步驟3.重新啟動Cisco CVP VXMLServer服務。

以下是不同JAVA版本中預設協定支援的快速清單。

	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.
```

此配置要求VXML伺服器使用Java SE開發工具包(JDK)7和JDK6中的TLS 1.2。

> **註**：預設情況下禁用SSL。

在介面3中啟用TLS 1.2的過程

CVP VXML

TLS 1.2TLS 1.2

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

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

CVP3TLS 1.2

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

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

3.Cisco CVP VXMLServer

> **附註**：有關詳細資訊，請檢查此錯誤：CSCvg20831 JNDI資料庫連線失敗，CVP11.6 SQL 2014SP2。

升級JRE以獲得TLS 1.2支援的過程

CVP支援將Java Runtime Environment(JRE)升級到最新版本以發現錯誤。

此表顯示了JAVA版本。

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版本

請按照此連結中介紹的步驟操作。

注意：不支援從32位升級到64位，反之亦然

升級Tomcat的過程

支援Tomcat次要升級。但是，請確保在執行升級之前檢查自定義Jar（AXIS、JDBC等）之間的相容性問題。

有關詳細資訊，請在此處檢查過程。