Come abilitare TLS 1.2 su diverse interfacce di CVP VXML Server

Sommario

[Introduzione](#)
[Prerequisiti](#)
[Requisiti](#)
[Componenti usati](#)
[Premesse](#)
[Interfaccia TLS del server VXML](#)
[Problema: Come abilitare TLS 1.2 su diverse interfacce di CVP VXML Server](#)
[Soluzione](#)
[Procedura per abilitare TLS 1.2 nell'interfaccia 1](#)
[Procedura per abilitare TLS 1.2 nell'interfaccia 2](#)
[Procedura per abilitare TLS 1.2 nell'interfaccia 3](#)
[Procedura di aggiornamento di JRE per il supporto di TLS 1.2](#)
[Procedura di aggiornamento di Tomcat](#)

Introduzione

In questo documento viene descritto come configurare Cisco Customer Voice Portal (CVP) Call Server e il supporto VXML (Voice Extensible Markup Language) Server Transport Layer Security (TLS) per il protocollo HTTP (HyperText Transfer Protocol).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Server VXML CVP
- Cisco Virtual Voice Browser (CVB)
- Gateway VXML

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

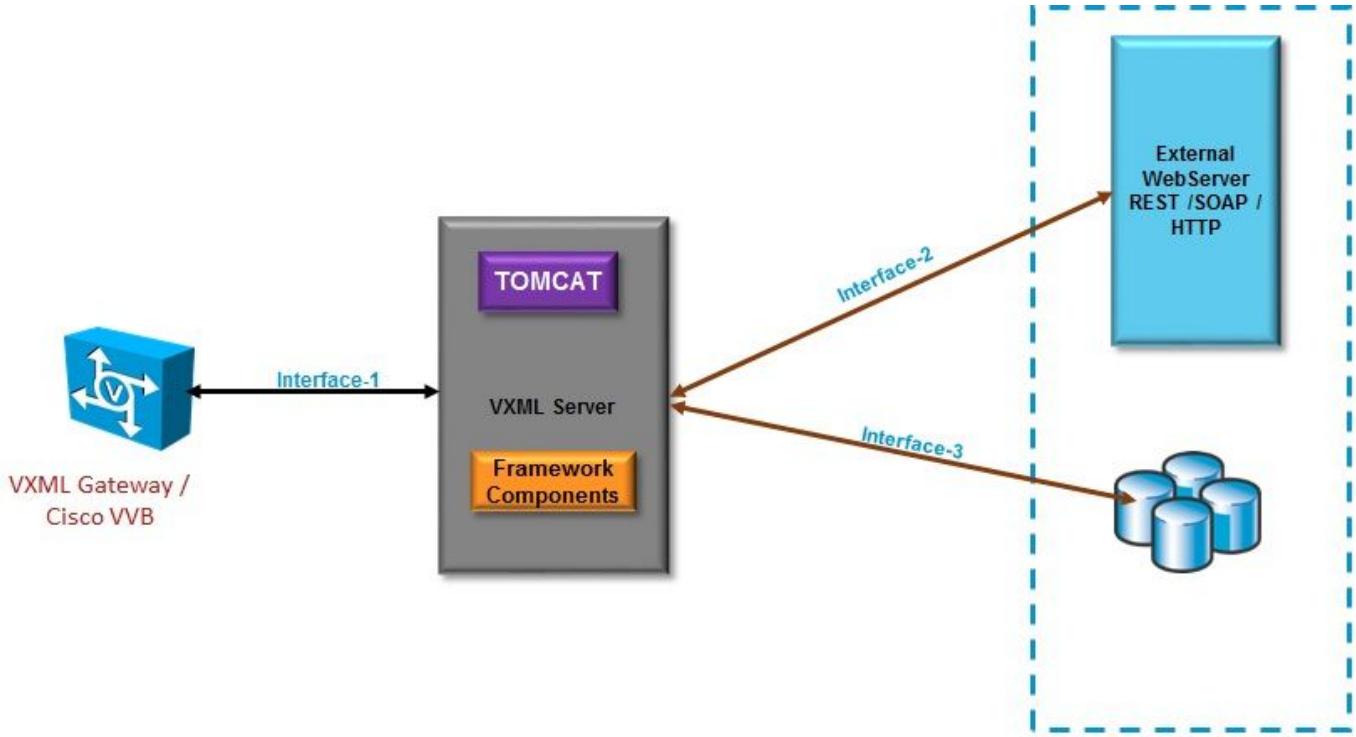
- CVP 11.5(1)
- CVB 11.5(1)

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali

conseguenze derivanti dall'uso dei comandi.

Premesse

Attualmente, il server VXML può avere tre interfacce protette con componenti diversi, come mostrato nell'immagine.



Interfaccia TLS del server VXML

Interfaccia 1. Si tratta dell'interfaccia HTTP (Hypertext Transfer Protocol) tra VXML Gateway, Cisco Virtualized Voice Browser (CVB) e VXML Server. In questo caso, VXML Server funge da server.

Interfaccia 2. Si tratta della tipica interfaccia HTTP in cui il server VXML interagisce con un server Web esterno che utilizza l'interfaccia HTTP/SOAP (Simple Object Access Protocol). Questa interfaccia viene definita come parte dell'elemento personalizzato, dell'elemento WebService o dell'elemento SOAP.

Interfaccia 3. Si tratta di un database esterno (DB) (server Microsoft Structured Query Language (MSSQL) e ORACLE DB) che utilizza l'interfaccia elemento DB incorporata o l'interfaccia elemento personalizzata.

In questo scenario, nell'interfaccia 1., il server VXML funge da server e nell'interfaccia 2. e 3., il server VXML funge da client sicuri.

Problema: Come abilitare TLS 1.2 su diverse interfacce di CVP

VXML Server

CVP VXML Server comunica a vari dispositivi e server con l'aiuto di diverse interfacce. TLS 1.2 deve essere abilitato su tutti i dispositivi per raggiungere il livello di sicurezza desiderato.

Soluzione

Procedura per abilitare TLS 1.2 nell'interfaccia 1

Come descritto in precedenza, in questa interfaccia CVP VXML Server funge da server. Questa implementazione sicura viene eseguita da Tomcat. Questa configurazione è controllata da **server.xml** in Tomcat.

Configurazione connettore tipica:

```
<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"/>
```

Questo esempio ha TLS v1.2, quindi i parametri da configurare (sslEnabledProtocols e certificato) hanno la configurazione richiesta per avere il supporto di TLS 1.2.

Utilizzare java **keytool.exe** per generare certificati TLS 1.2. Questo strumento è disponibile in **Cisco\CVP\jre\bin\.**

Documentazione Keytool

Procedura per abilitare TLS 1.2 nell'interfaccia 2

Si tratta dell'interfaccia più comune utilizzata. In questo caso, il server VXML funge da client e deve aprire una comunicazione protetta con un server Web esterno.

Ci sono due modi diversi per gestire questo.

- Utilizzare codice personalizzato.
- Utilizzare CVP Framework.

Viene descritto l'utilizzo di CVP Framework.

Dalla versione 11.6 è attivata per default. Per le versioni precedenti, controllare questa tabella:

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	

Se è installata una versione di ESX interessata da questo problema: CSCvc39129 VXML Server come client TLS, è necessario applicare la seguente configurazione manuale:

Passaggio 1. Aprire l'editor del Registro di sistema e passare a **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Passaggio 2. Aprire **Options Key** e add **-Dhttps.client.protocol=TLSv1.2** alla fine.

Passaggio 3. Riavviare il servizio Cisco CVP VXMLServer.

Di seguito è riportato un breve elenco del supporto del protocollo predefinito nelle diverse versioni JAVA.

	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.
```

Questa configurazione impone al server VXML di utilizzare TLS 1.2 in Java SE Development Kit (JDK) 7 e JDK6.

> **Nota**: SSL è disabilitato per impostazione predefinita.

Procedura per abilitare TLS 1.2 nell'interfaccia 3

Come descritto in precedenza, in questa interfaccia CVP VXML Server funge da client e da server di database di terze parti che funge da server.

Verificare che il server di database di terze parti supporti TLS 1.2 e che TLS 1.2 sia abilitato su tale server.

Ad esempio, se si utilizza SQL Server 2014 con Service Pack (SP) 2, è supportato TLS 1.2 e si

conferma che Il protocollo TLS 1.2 è abilitato nel Registro di sistema come indicato di seguito in SQL Server:

SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols

Per abilitare TLS 1.2 per l'interfaccia 3 sul lato CVP:

Passaggio 1. Aprire l'editor del Registro di sistema e passare a **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java**.

Passaggio 2. Aprire **Options Key** e add **-Djdk.tls.client.protocols=TLSv1.2** alla fine.

Passaggio 3. Riavviare il servizio Cisco CVP VXMLServer.

> **Nota:** Controllare questo bug per ulteriori dettagli: la connessione al database JNDI CSCvg20831 non riesce con CVP11.6 SQL 2014SP2.

Procedura di aggiornamento di JRE per il supporto di TLS 1.2

CVP Supporta l'aggiornamento di Java Runtime Environment (JRE) alla versione più recente per i difetti di bug.

Questa tabella mostra le versioni JAVA.

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

Versioni JAVA

Attenersi alla procedura descritta in questo collegamento.

> **Attenzione:** L'aggiornamento da 32 bit a 64 bit e viceversa non è supportato

Procedura di aggiornamento di Tomcat

L'aggiornamento di Tomcat Minor è supportato. Tuttavia, prima di eseguire l'aggiornamento, accertarsi di controllare i problemi di compatibilità tra i jar personalizzati (AXIS, JDBC e così via).

Per ulteriori informazioni, fare riferimento alla procedura qui.