Configuración de la comunicación de Extensiones de administración de Java seguras (JMX) en CVP 12.0

Contenido

Introducción Prerequisites Requirements Componentes Utilizados Configurar Generar certificado firmado por CA para el servicio Web Services Manager (WSM) en servidor de Ilamadas, servidor VoiceXML (VXML) o servidor de informes Generar certificado de cliente firmado por CA para WSM Verificación Troubleshoot

Introducción

Este documento describe los pasos para configurar la comunicación JMX segura en Customer Voice Portal (CVP) versión 12.0.

Colaborado por Balakumar Manimaran, ingeniero del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- CVP
- Certificados

Componentes Utilizados

La información de este documento se basa en la versión 12.0 de CVP.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Generar certificado firmado por CA para el servicio Web Services Manager (WSM) en servidor de llamadas, servidor VoiceXML (VXML) o servidor de informes

1. Inicie sesión en Call Server o VXML Server o Reporting Server o WSM Server. Recuperar la contraseña del almacén de claves de security.properties archivo desde la ubicación,

C:\Cisco\CVP\conf	
<pre>\Cisco\CUP\conf>security.properties</pre>	<pre>Security.keystorePW = i01046ho!\$t5C\$-\$N(({d-0~E~:z03gu</pre>
\Cisco\CUP\conf>	

2. Deliminar el certificado WSM mediante el comando,

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

C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se curity\.keystore -delete -alias wsm_certificate Enter keystore password:	
warning: The JCEKS keystore uses a proprietary format. It is recommended to migrate to PK CS12 which is an industry standard format using "keytool -importkeystore -srckey store c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur ity\.keystore -deststoretype pkcs12".	

Introduzca la contraseña del almacén de claves cuando se le solicite.

Nota: Repita el paso 1 para Call Server, VXML Server y Reporting Server.

3. Genere un certificado firmado por la autoridad de certificación (CA) para el servidor WSM.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -						
genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA						
C:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se surity\.keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA						

Ingrese los detalles en las indicaciones y escribaYesto para confirmar, como se muestra en la imagen;

your first and last name? [CVPA]: CUPA Nhat is the name of your organizational unit? [cisco]: cisco lhat is the name of your organization? [cisco]: cisco That is the name of your City or Locality? [Richardson]: ricĥardson That is the name of your State or Province? [Texas]: texas lhat is the two-letter country code for this unit? [TX]: [TX]: TX CN=CUPA, OU=cisco, V=cisco, L=richardson, ST=texas, C=TX correct? [no]: yes Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) th a validity of 90 days for: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX nter key password for <wsm_certificate> CRETURN if same as keystore password):

Introduzca la contraseña del almacén de claves cuando se le solicite.

Nota: Documentar el nombre común (CN) para referencia futura.

4. Generar la solicitud de certificado para el alias

```
%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -
certreq -alias wsm_certificate -file
%CVP_HOME%\conf\security\wsm_certificate
*CCVP_HOME%\conf\security\wsm_certificate
*CCVP_HOME%\conf\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\security\
```

5. Firme el certificado en una CA.

Nota: siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA.

6. Copie el certificado raíz y el certificado WSM firmado por CA en la ubicación;

C:\Cisco\cvp\conf\security\. 7. Importar el certificado raíz

%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>

Introduzca la contraseña del almacén de claves cuando se le solicite, como se muestra en la imagen;

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se curity\.keystore -import -v -trustcacerts -alias root -file C:\Cisco\cvp\conf\se curity\root.cer Enter keystore password: _____

:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se curity\.keystore -import -v -trustcacerts -alias root -file C:\Cisco\cvp\conf\se curity\CVPA-root.cer Enter keystore password: Dwner: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Serial number: 49000000b96895db4285cda29000000000b Serial number: 49000000096895db4285cda2900000000000 Jalid from: Tue Jun 23 11:22:48 PDT 2020 until: Thu Jun 23 11:22:48 PDT 2022 Certificate fingerprints: MD5: 6D:1E:3B:86:96:32:5B:9F:20:25:47:1C:8E:B0:18:6E SHA1: D0:57:B5:5C:C6:93:82:B9:3D:6C:C8:35:06:40:24:7D:DC:5C:F9:51 SHA256: F5:0C:65:E8:5A:38:1C:90:27:45:B8:B5:67:C8:65:08:95:09:B8:D9:3F: B2:12:53:5D:81:2A:F5:13:67:F4:60 Signature algorithm name: SHA256withRSA Subject Public Key Algorithm: 2048-bit RSA key Lewsion: 3 Jersion: 3 Extensions: ‡1: ObjectId: 1.3.6.1.4.1.311.20.2 Criticality=false 3000: 1E 12 00 57 00 65 00 62 00 53 00 65 00 72 00 76 3010: 00 65 00 72W.e.b.S.e.r.v .e.r 2: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [accessMethod: calssuers accessLocation: URIName: ldap:///CN=UCCE12DOMAINCA,CN=AIA,CN=Public%20Key%20S rvices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?cACertificate?base?objectC lass=certificationAuthority #3: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [(eyldentifier [1000: 78 EF 21 55 BA F9 75 03 3A ØA 1D A8 5A 9E 43 B6 x.!U..u.:...Z.C. 0010: D1 F8 57 3E ..W> t4: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: EURINAME: ldap:///CN=UCCE12DOMAINCA,CN=UCCE12,CN=CDP,CN=Public%20Key%20Serv ices,CN=Services,CN=Configuration,DC=UCCE12,DC=COM?certificateRevocationList?bas ??objectClass=cRLDistributionPoint]

AtTrust this certificateprompt, escriba Sí, como se muestra en la imagen;



8. Importar el certificado WSM firmado por CA

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v trustcacerts

:\Cisco\CVP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se curity\.keystore -import -v -trustcacerts -alias wsm_certificate -file C:\Cisco\ vp\conf\security\CVPA.p7b Enter keystore password: lop-level certificate in reply: Dwner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Serial number: 13988560817c46bf4bb659624cf6209f Jalid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024 Certificate fingerprints: MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97 SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16 SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D: 79-21-05-62-94-45-66-89-98:F5:00 39:31:05:62:84:45:66:89:98:F5:AA Signature algorithm name: SHA256withRSA Subject Public Key Algorithm: 2048-bit RSA key Jersion: 3 Extensions: \$1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 1000: Ö2 01 00 #2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[CAtrue PathLen:2147483647 #3: ObjectId: 2.5.29.15 Criticality=false {eyUsage [
 DigitalSignature Key_CertSign Crl_Sign 44: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: 78 EF 21 55 BA F9 75 03 3A 0A 1D 0010: D1 F8 57 3E x.!U..u.:...Z.C. 3A ØA 1D A8 5A 9E 43 B6 ..W> is not trusted. Install reply anyway? [no]:

9. Repita los pasos 3, 4 y 8 para Call Server, VXML Server y Reporting Server.

10.Configuración de WSM en CVP

Paso 1.

Vaya a

c:\cisco\cvp\conf\jmx_wsm.conf

Agregue o actualice el archivo como se muestra y guárdelo

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
<pre>#com.sun.management.jmxremote.ssl.config.file=</pre>

Paso 2.

Ejecute el regedit (rt. haga clic en Start > Run > Type (Inicio > Ejecutar > Tipo) regedit) comando

Añada lo siguiente a las Opciones clave en



HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun

11. Configuración de JMX de callserver en CVP

c:\cisco\cvp\conf\jmx_callserver.conf

Actualice el archivo como se muestra y guarde el archivo

```
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 = <keystore password>
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
javax.net.ssl.trustStorePassword=< keystore_password >
javax.net.ssl.trustStoreType=JCEKS
#com.sun.management.jmxremote.ssl.config.file=
```

12. Configure JMX de VXMLServer en CVP:

Paso 1.

Vaya a

c:\cisco\cvp\conf\jmx_vxml.conf

Edite el archivo como se muestra en la imagen y guárdelo;

```
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:CiscoCVPconfsecurity.keystore
javax.net.ssl.keyStorePassword = <keystore password>
```

Paso 2.

Ejecute el regedit comando

Añada lo siguiente a las Opciones clave en

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

• 📲 VMware, Inc.	^	Name	lype	Data
1 🔑 Wow6432Node		ab (Default)	REG_SZ	(value not set)
🛛 🌗 Apache Software Foundat		ab Classpath	REG_SZ	C:\Cisco\CVP\VXMLServer\Tomcat\bin\bootstrap
⊿ - 퉲 Procrun 2.0		ab Jvm	REG_SZ	C:\Cisco\CVP\jre\bin\server\jvm.dll
D - CallServer		ab Options	REG_MULTI_SZ	-Djre.home=C:\Cisco\CVP\jre -Dcatalina.base=C:\
⊿ - 퉲 VXMLServer		- Andrewski		, , ,
A - 🎉 Parameters				
Java				
🏄 Log				
Start				
L				
⊿ - WebServicesMana				

 Dcom.sun.management.config.file=C:\Cisco\CVP\conf\jmx_vxm Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore Djavax.net.ssl.trustStorePassword=<keystore_password></keystore_password> Djavax.net.ssl.trustStoreType=JCEKS 				
< 111	>			
OK	Cancel			

Paso 3.

Reinicie el servicio Cisco CVP WebServicesManager.

Generar certificado de cliente firmado por CA para WSM

Inicie sesión en Call Server o VXML Server o Reporting Server o WSM. Recuperar la contraseña del almacén de claves desde el *security.properties* archivo

1. Generar un certificado firmado por CA para la autenticación del cliente

%CVP_HOME%\jre\bin\keytool.exe -st	toretype JCEKS -keystore	%CVP_HOME%\conf\security\.keystore -
genkeypair		
-alias <cn callserver="" cert:<="" of="" td="" wsm=""><td>ificate> -v -keysize 2048</td><td>B -keyalg RSA</td></cn>	ificate> -v -keysize 2048	B -keyalg RSA

c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se curity\.keystore -genkeypair -alias CUPA -v -keysize 2048 -keyalg RSA Enter keystore password:

Ingrese los detalles en las indicaciones y escriba Sí para confirmar.

Introduzca la contraseña del almacén de claves cuando se le solicite , como se muestra en la imagen;

What is your first and last name? [cisco]: CUPA What is the name of your organizational unit? [cisco]: What is the name of your organization? [cisco]: What is the name of your City or Locality? [Richardson]: richardson What is the name of your State or Province? [Tx]: texas What is the two-letter country code for this unit? [US]: TX Is CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX correct? [no]: yes Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) wi th a validity of 90 days for: CN=CUPA, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX Re-enter new password: [Storing c:\cisco\cvp\conf\security\.keystore]

2.Generar la solicitud de certificado para el alias

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore certreq -alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr c:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se curity\.keystore -certreq -alias CUPA -file c:\cisco\cup\conf\security\jmx_clien t.csr Enter keystore password:

3. Firmar el certificado en una CA

Nota: Siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA

4. Copie el certificado raíz y el certificado de cliente JMX firmado por CA en la ubicación;

 $\texttt{C:Cisco}cvp\conf\security\}$

5. Importe el cliente JMX firmado por CA, utilice el comando;

%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 CA-signed JMX Client certificate>

c:\Cisco\CUP\jre<u>\bin>keytool.exe -storetype JCEKS</u> -keystore c:\cisco\cup\conf\se curity\.keystore -import -v -trustcacerts -alias CUPA -file C:\Cisco\cvp\conf\se curity\jmx_client.p Enter keystore password: Top-level certificate in reply: Owner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Serial number: 13988560817c46bf4bb659624cf6209f Valid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024 Certificate fingerprints: MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97 SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16 SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D: E9:31:05:62:84:45:66:89:98:F5:AA Signature algorithm name: SHA256withRSA Subject Public Key Algorithm: 2048-bit RSA key Version: 3 Extensions: #1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 0000: Ö2 01 00 #2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[CA:true PathLen:2147483647 #3: ObjectId: 2.5.29.15 Criticality=false KeyUsage [**DigitalSignature** Key_CertSign Cr1_Sign #4: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: 78 EF 21 55 BA F9 75 03 0010: D1 F8 57 3E 3A ØA 1D A8 5A 9E 43 B6 x.!U..u.:...Z.C. ..W> is not trusted. Install reply anyway? [no]: yes ertificate reply was installed in keystore lStoring c:\cisco\cvp\conf\security\.keystore]

6. Reinicie el servicio Cisco CVP VXMLServer.

Repita el mismo procedimiento para Reporting Server.

Generar certificado de cliente firmado por CA para Operations Console (OAMP)

Inicie sesión en el servidor OAMP. Recuperar la contraseña del almacén de claves desde *elarchivo*de propiedades.security

1. Generar un certificado firmado por CA para la autenticación del cliente con el WSM del servidor de llamadas

genkevpair -alias <CN of Callserver WSM certificate> -v -keysize 2048 -keyalq RSA ::\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cup\conf\se curity\.keystore -genkeypair -alias CVPA -v -keysize 2048 -keyalg RSA Enter keystore password: /hat is your first and last name? CUPOAMP [Unknown]: /hat is the name of your organizational unit? [Unknown]: cisco What is the name of your organization? [Unknown]: cisco What is the name of your City or Locality? [Unknown]: richardson /hat is the name of your State or Province? [Unknown]: texas What is the two-letter country code for this unit? [Unknown]: TX s_CN=CUPOAMP, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX correct? [no]: yes Generating 2,048 bit RSA key pair and self-signed certificate (SHA256withRSA) wi th a validity of 90 days for: CN=CUPOAMP, OU=cisco, O=cisco, L=richardson, ST=texas, C=TX Enter hey rassword for <CUPA> KRETURN II ne as keystore password): Re-enter new password: [Storing c:\cisco\cvp\conf\security\.keystore]

2.Generar la solicitud de certificado para el alias

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore certreq
-alias <CN of Callserver WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr
:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\security\jmx.csr
:\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\security\jmx.csr
:\Cisco\CUP\jre\bin>keytore -certreq -alias CUPA -file c:\cisco\cvp\conf\security\jmx.csr
inter keystore password:
Inter key password for <CUPA>
larning:
he JCEKS keystore uses a proprietary format. It is recommended to migrate to PK
\$12 which is an industry standard format_using "keytool -importkeystore -spckey"

3.Firme el certificado en una CA . Siga el procedimiento para crear un certificado firmado por CA mediante la autoridad de CA. Descargue el certificado y el certificado raíz de la autoridad de CA

4.Copie el certificado raíz y el certificado de cliente JMX firmado por CA en C:\Cisoc\cvp\conf\security\

5.Importe el certificado raíz, utilizando este comando;

 $CVP_HOME \jre\bin\keytool.exe -storetype JCEKS -keystore <math display="inline">CVP_HOME \conf\security\.keystore - import -v -trustcacerts$

-alias root -file %CVP_HOME%\conf\security\<filename_of_root_cert>

Introduzca la contraseña del almacén de claves cuando se le solicite. **AtTrust this** certificate prompt, *escribaYes*, como se muestra en la imagen,

:\Cisco\CUP\jre\hin>keytool_exe__storetype_JCEKS__keystore_c:\cisco\cvp\conf\se urity\.keystore__import_v__trustcacerts__alias_root__file_c:\cisco\cvp\conf\se urity\root.cer Inter keystore password: Owner: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Issuer: CN=UCCE12DOMAINCA, DC=UCCE12, DC=COM Serial number: 13988560817c46bf4bb659624cf6209f Valid from: Sat Jun 29 21:30:17 PDT 2019 until: Sat Jun 29 21:40:17 PDT 2024 Certificate fingerprints: MD5: 94:82:AC:3F:59:45:48:A9:D3:4D:2C:D7:E0:38:1C:97 SHA1: 88:75:A7:4B:D3:D5:B2:76:B5:59:96:F1:83:82:C2:BB:97:23:8B:16 SHA256: E6:E3:1F:5A:8E:E2:8F:14:80:59:26:64:25:CA:C0:FD:91:E4:F3:EB:9D: 9:31:05:62:84:45:66:89:98:F5:AA ignature algorithm name: SHA256withRSA ubject Public Key Algorithm: 2048-bit RSA key lersion: 3 xtensions: H: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 1000: 02 01 00 . . . 2: ObjectId: 2.5.29.19 Criticality=true lasicConstraints:[CA:true PathLen:2147483647 3: ObjectId: 2.5.29.15 Criticality=false (eyUsage_l **DigitalSignature** Key_CertSign Cr1_Sign 4: ObjectId: 2.5.29.14 Criticality=false ubjectKeyIdentifier [KeyIdentifier [1000: 78 EF 21 55 BA F9 75 03 3A 0A 1D 1 1010: D1 F8 57 3E x.!U..u.:...Z.C. 3A ØA 1D A8 5A 9E 43 B6 ..W> rust this certificate? [no]: yes ertificate was added to keystore yes Storing c:\cisco\cvp\conf\security\.keystore] larning: The JCEKS keystore uses a proprietary format. It is recommended to migrate to PK S12 which is an industry standard format using "keytool -importkeystore -srckey tore c:\cisco\cvp\conf\security\.keystore -destkeystore c:\cisco\cvp\conf\secur

6. Importar el certificado de cliente JMX firmado por CA de CVP

%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> :\Cisco\CUP\jre\bin>keytool.exe -storetype JCEKS -keystore c:\cisco\cvp\conf\se urity\.keystore -import -v -trustcacerts -alias CUPA -file c:\cisco\cvp\conf\se urity\jmx.p7b nter keystore password: eystore password is too short - must be at least 6 characters inter keystore password: eystore password for <CUPA> ertificate reply was installed in keystore Storing c:\cisco\cvp\conf\security\.keystore] larning: 7. Reinicie el servicio Cisco CVP OPSConsoleServer.

8. Inicie sesión en OAMP. Para habilitar la comunicación segura entre OAMP y Call Server o VXML Server, navegue hasta Device Management > Call Server. Marque la casilla de verificación Habilitar comunicación segura con la consola Ops. Guarde e implemente el servidor de llamadas y el servidor VXML.

Hostname: *	сура
Description:	
Enable secure communication with the Ops console: 1	

9. Ejecute el comando regedit.

 $\label{eq:local_MACHINE\SOFTWARE\Wow6432Node\Apache\ Software\ Foundation\Procrun\ 2.0\OPSConsoleServer\Parameters\Java.$

Añada lo siguiente al archivo y guárdelo

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

Djavax.net.ssl.trustStorePassword= -Djavax.net.ssl.trustStoreType=JCEK					
Djavax.net.ssl.keyStore=C:\Cisco\CVP\cont\secunty\.keystore Djavax.net.ssl.keyStorePassword=)aASYJC*y{4t,17@wyW1VwG1 Djavax.net.ssl.keyStoreType=JCEKS Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore Djavax.net.ssl.trustStorePassword= <keystore_password></keystore_password>					
	N	~			
< 111	>				
	OK Cancel				

Verificación

Conecte CVP Callserver, VXML server y Reporting server desde el servidor OAMP, realice operaciones como guardar&implementar o recuperar detalles de base de datos (servidor de informes) o cualquier acción de OAMP al servidor de llamadas/vxml/informes.

Troubleshoot

Actualmente, no hay información específica de troubleshooting disponible para esta configuración.