Comunicación segura de JMX entre componentes CVP OAMP y CVP con autenticación mutua

Contenido

Introducción

Este documento describe cómo proteger la comunicación de Extensiones de administración de Java (JMX) entre Customer Voice Portal (CVP) Operation and Management Console (OAMP) y CVP Server y CVP Reporting Server en la solución Cisco Unified Contact Center Enterprise (UCCE) a través de certificados firmados por Certificate Authority (CA).

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- UCCE versión 12.5(1)
- Portal de voz del cliente (CVP) versión 12.5 (1)

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- UCCE 12.5(1)
- CVP 12.5(1)

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. If your network is live, make sure that you understand the potential impact of any command.

Antecedentes

OAMP se comunica con CVP Call Server, CVP VXML Server y CVP Reporting Server mediante el protocolo JMX. La comunicación segura entre OAMP y estos componentes de CVP evita las vulnerabilidades de seguridad de JMX. Esta comunicación segura es opcional, no es necesaria para el funcionamiento regular entre OAMP y los componentes CVP.

Puede proteger la comunicación JMX mediante:

- Genere la solicitud de firma de certificado (CSR) para Web Service Manager (WSM) en CVP Server y CVP Reporting Server.
- Genere el certificado de cliente CSR para WSM en el servidor CVP y CVP Reporting Server.
- Genere el certificado de cliente CSR para OAMP (que se realizará en OAMP).
- Firme los certificados por una autoridad certificadora.
- Importe los certificados firmados por CA, raíz e intermedio en CVP Server, CVP Reporting Server y OAMP.
- [Opcional] Conexión segura de JConsole a OAMP.
- Secure System CLI.

Generar certificados CSR para WSM

Paso 1. Inicie sesión en CVP Server o Reporting Server. Recupere la contraseña del almacén de claves del archivo **security.properties**.

> **Nota:** En el símbolo del sistema, introduzca más %CVP_HOME%\conf\security.properties. Security.keystorePW = <Devuelve la contraseña del almacén de claves> Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Vaya a %CVP_HOME%\conf\security and delete the WSM certificate. Utilice este comando.

%CVP_HOME%\jre\bin\keytool.exe -almacén JCEKS -almacén de claves %CVP_HOME%\conf\security\.almacén de claves -delete -alias wsm_certificate.

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

Paso 3. Repita el paso 2 para los certificados de servidor de llamadas y servidor VXML en el servidor CVP y el certificado de servidor de llamadas en el servidor de informes.

Paso 4. Genere un certificado firmado por CA para el servidor WSM. Utilice este comando:

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias wsm_certificate -v -keysize 2048 -keyalg RSA.

1. Ingrese los detalles en las indicaciones y escriba **Sí** para confirmar.
2. Introduzca la contraseña del almacén de claves cuando se le solicite.

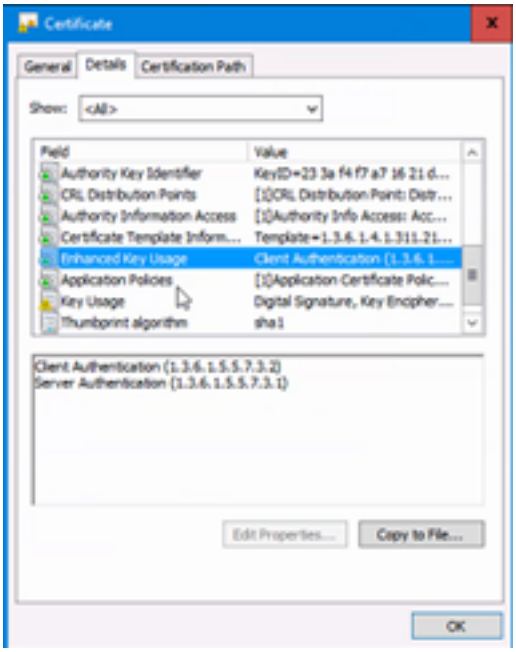
> **Nota:** Anote el nombre CN para referencia futura.

Paso 5. Genere la solicitud de certificado para el alias. Ejecute este comando y guárdelo en un archivo (por ejemplo, **wsm.csr ��**

%CVP_HOME%\jre\bin\keytool.exe -tipo de archivo JCEKS -almacén de claves %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -archivo %CVP_HOME%\conf\security\wsm.csr.

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

Paso 6. Obtenga el certificado firmado por una CA. Siga el procedimiento para crear un certificado firmado por CA con la autoridad de CA y asegúrese de utilizar una plantilla de autenticación de certificado cliente-servidor cuando la CA genere el certificado firmado.



Paso 7. Descargue el certificado firmado, el certificado raíz e intermedio de la autoridad de CA.

Paso 8. Copie el certificado WSM raíz, intermedio y firmado por CA en **%CVP_HOME%\conf\security**.

Paso 9. Importe el certificado raíz con este comando.

%CVP_HOME%\jre\bin\keytool.exe -tipo de archivo JCEKS -almacén de claves %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias raíz -archivo %CVP_HOME%\conf\security\<nombre_de_archivo_raíz_cer>.

1. Introduzca la contraseña del almacén de claves cuando se le solicite.
2. En Trust this certificate prompt, escriba **Yes** .

Paso 10. Importe el certificado intermedio con este comando.

%CVP_HOME%\jre\bin\keytool.exe -tipo de archivo JCEKS -almacén de claves %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermedio -archivo %CVP_HOME%\conf\security\<nombre_de_archivo_intermedio_cer>.

1. Introduzca la contraseña del almacén de claves cuando se le solicite.
2. En Trust this certificate prompt, escriba **Yes** .

Paso 11. Importe el certificado WSM firmado por CA con este comando.

%CVP_HOME%\jre\bin\keytool.exe -almacén de claves JCEKS -almacén de claves %CVP_HOME%\conf\security\.almacén de claves -importación -v -trustcacerts -alias wsm_certificate -archivo %CVP_HOME%\conf\security\<nombre_de_archivo_de_su_certificado_firmado_de_CA>.

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

Paso 12. Repita del paso 4 al 11 (los certificados raíz e intermedio no deben importarse dos veces) para los certificados de servidor de llamadas y de servidor VXML en el servidor CVP y el certificado de servidor de llamadas en el servidor de informes.

Paso 13 Configure WSM en CVP.

1. Navegue hasta **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
```

2. Ejecute el comando regedit.

```
Append this to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software
Foundation\Procrun 2.0\WebServicesManager\Parameters\Java:
Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
Djavax.net.ssl.trustStorePassword=
```

Paso 14. Configure JMX de CVP Callserver en CVP Server y servidor de informes.

1. Navegue hasta **c:\cisco\cvp\conf\jmx_callserver.conf.**

Actualice el archivo como se muestra y guárdelo:

```
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 =
```

Paso 15. Configure JMX de VXMLServer en el servidor CVP.

1. Navegue hasta **c:\cisco\cvp\conf\jmx_vxml.conf.**

Edite el archivo como se muestra 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:\Cisco\CVP\conf\security\.keystore javax.net.ssl.keyStorePassword =
```

2. Ejecute el comando regedit.

- ```
  Append theese to the file at HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\VXMLServer\Parameters\Java:
  Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore
  Djavax.net.ssl.trustStorePassword=
  ```

3. Reinicie los servicios de servicio WSM, servidor de llamadas y servidor VXML en el servidor CVP y servicio WSM y servicio de servidor de llamadas en servidor de informes.

> **Nota:** Cuando se habilita la comunicación segura con JMX, fuerza al almacén de claves a ser **%CVP_HOME%\conf\security\.keystore**, en lugar de **%CVP_HOME%\jre\lib\security\cacerts**.
> Por lo tanto, los certificados de **%CVP_HOME%\jre\lib\security\cacerts** deben importarse a **%CVP_HOME%\conf\security\.keystore**.

Generar certificado de cliente firmado por CA para WSM

Paso 1. Inicie sesión en CVP Server o Reporting Server. Recupere la contraseña del almacén de claves del archivo **security.properties**.

> **Nota:** En el símbolo del sistema, introduzca más %CVP_HOME%\conf\security.properties. Security.keystorePW = <Devuelve la contraseña del almacén de claves> Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Vaya a %CVP_HOME%\conf\security and generate a CA-signed certificate for client authentication with callserver with this command.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN de servidor CVP o certificado de servidor de informes WSM> -v -keysize 2048 -keyalg RSA

1. Ingrese los detalles en las indicaciones y escriba **Sí** para confirmar.
2. Introduzca la contraseña del almacén de claves cuando se le solicite.

> **Nota:** El alias será el mismo que el CN utilizado para generar el certificado de servidor WSM.

Paso 3. Genere la solicitud de certificado para el alias con este comando y guárdelo en un archivo (por ejemplo, **jmx_client.csr**).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN de servidor CVP o certificado WSM del servidor de informes> -archivo %CVP_HOME%\conf\security\jmx_client.csr

1. Introduzca la contraseña del almacén de claves cuando se le solicite.
2. Verifique que el CSR se generó correctamente con este comando: **dir jmx_client.csr.**

Paso 4. Firme el certificado de cliente JMX en una CA.

> **Nota:** Siga el procedimiento para crear un certificado firmado por CA con la autoridad de CA.
  ```

Descargue el certificado de cliente JMX firmado por CA (los certificados raíz e intermedio no son obligatorios, ya que se descargaron e importaron anteriormente).

1. Introduzca la contraseña del almacén de claves cuando se le solicite.
2. En Trust this certificate prompt (Confiar en este mensaje de certificado), escriba Yes (Sí).

Paso 5. Copie el certificado de cliente JMX firmado por CA en **%CVP_HOME%\conf\security\.**

Paso 6. Importe el certificado de cliente JMX firmado por CA con este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN de servidor CVP o certificado WSM de servidor de informes> -archivo %CVP_HOME%\conf\security\<nombre de archivo del certificado de cliente JMX firmado por CA>

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

Paso 7. Reinicie los servicios Cisco CVP Call Server, VXML Server y WSM.

Paso 8. Repita el mismo procedimiento para Reporting Server, si se implementa.

Generar certificado de cliente firmado por CA para OAMP (se realizará en OAMP)

Paso 1. Inicie sesión en el servidor OAMP. Recupere la contraseña del almacén de claves del archivo **security.properties**.

> **Nota:** En el símbolo del sistema, ingrese más **%CVP_HOME%\conf\security.properties**. Security.keystorePW = <Devuelve la contraseña del almacén de claves> Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 2. Navegue hasta la seguridad **%CVP_HOME%\conf** y genere un certificado firmado por CA para la autenticación del cliente con el servidor CVP WSM. Utilice este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of OAMP Server WSM certificate> -v -keysize 2048 -keyalg RSA.

1. Introduzca los detalles en las indicaciones y escriba Sí para confirmarlo.
2. Introduzca la contraseña del almacén de claves cuando se le solicite.

Paso 3. Genere la solicitud de certificado para el alias con este comando y guárdelo en un archivo (por ejemplo, **jmx.csr**).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN de certificado WSM del servidor CVP> -archivo %CVP_HOME%\conf\security\jmx.csr.

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

Paso 4. 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.

Paso 5. Copie el certificado raíz y el certificado de cliente JMX firmado por CA en **%CVP_HOME%\conf\security**.

Paso 6. Importe el certificado raíz de la CA. Utilice este comando.

%CVP_HOME%\jre\bin\keytool.exe -tipo de archivo JCEKS -almacén de claves %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias raíz -archivo %CVP_HOME%\conf\security\<nombre_de_archivo_raíz_cert>.

1. Introduzca la contraseña del almacén de claves cuando se le solicite.
2. En Trust this certificate prompt (Confiar en este mensaje de certificado), escriba Yes (Sí).

Paso 7. Importe el certificado de cliente JMX firmado por CA de CVP. Utilice este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN del certificado WSM del servidor de llamadas> -archivo %CVP_HOME%\conf\security\<nombre_de_archivo_de_su_certificado_firmado_de_CA>.

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

Paso 8. Reinicie el servicio OAMP.

Paso 9. Inicie sesión en OAMP. para habilitar la comunicación segura entre OAMP y Call Server o VXML Server. Vaya a **Administración de dispositivos > Servidor de llamadas**. Marque la casilla de verificación Habilitar comunicación segura con la consola de operaciones. Guarde e implemente el servidor de llamadas y el servidor VXML.

Paso 10. Ejecute el comando regedit.

Navegue hasta **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java.**

Añada esto al archivo y guárdelo.

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

> **Nota**: Después de proteger los puertos para JMX, sólo se puede acceder a JConsole después de realizar los pasos definidos para JConsole enumerados en los documentos de Oracle.

Información Relacionada

- Guía de configuración segura de CVP

- Soporte Técnico y Documentación - Cisco Systems