CVP OAMP和CVP组件之间的安全JMX通信，带相互身份验证

目录

简介

本文档介绍如何通过证书颁发机构(CA)签名的证书保护客户语音门户(CVP)操作和管理控制台(OAMP)与思科统一联系中心企业(UCCE)解决方案中的CVP服务器和CVP报告服务器之间的Java管理扩展(JMX)通信。

先决条件

要求

Cisco 建议您了解以下主题：

- UCCE版本12.5(1)
- 客户语音门户(CVP)版本12.5(1)

使用的组件

本文档中的信息基于以下软件版本：

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

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

OAMP通过JMX协议与CVP呼叫服务器、CVP VXML服务器和CVP报告服务器通信。OAMP和这些CVP组件之间的安全通信可防止JMX安全漏洞。此安全通信是可选的，OAMP和CVP组件之间的常规操作不需要这种通信。

您可以通过以下方式保护JMX通信：

- 在CVP服务器和CVP报告服务器中为Web服务管理器(WSM)生成证书签名请求(CSR)。
- 在CVP服务器和CVP报告服务器中为WSM生成CSR客户端证书。
- 为OAMP生成CSR客户端证书（将在OAMP上完成）。
- 通过证书颁发机构签名证书。
- 导入CVP服务器、CVP报告服务器和OAMP中的CA签名证书、根证书和中间证书。
- [可选]安全JConsole登录OAMP。
- 安全系统CLI。

为WSM生成CSR证书

步骤1.登录到CVP服务器或报告服务器。从security.properties文件中检**索密钥库**密码。

> **注意：**在命令提示符下，输入更多%CVP_HOME%\conf\security.properties。Security.keystorePW = <Returns the keystore password>出现提示时输入密钥库密码。

第二步： 导航至%CVP_HOME%\conf\security and delete the WSM certificate。使用此命令。

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

出现提示时输入密钥库密码。

步骤3.对CVP服务器上的呼叫服务器和VXML服务器证书以及报告服务器上的呼叫服务器证书重复步骤2。

步骤4.为WSM服务器生成CA签名证书。使用以下命令：

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

1. 在提示符处输入详细信息，然后键入**Yes**进行确认。
2. 出现提示时输入密钥库密码。

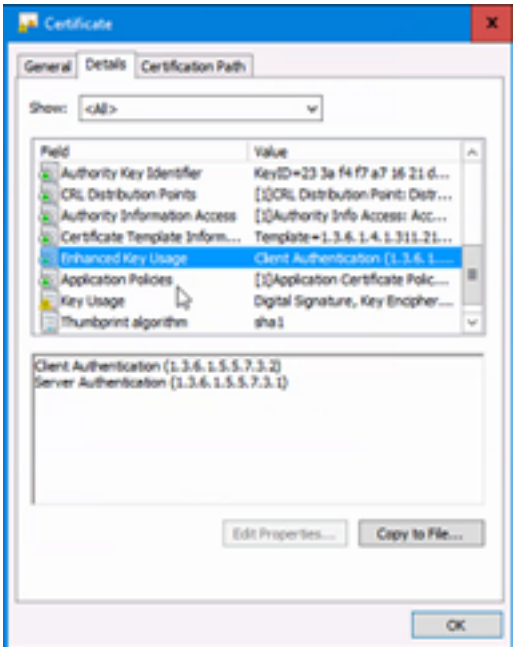
> **注意：**请注意CN名称以备将来参考。

步骤5.生成别名的证书请求。运行此命令并将其保存到文件(例如**wsm.csr**

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias wsm_certificate -file %CVP_HOME%\conf\security\wsm.csr。

1.在出现提示时输入密钥库密码。

步骤6.获取CA签名的证书。按照以下步骤创建具有CA颁发机构的CA签名证书，并确保在CA生成签名证书时使用客户端 — 服务器证书身份验证模板。



步骤7.下载CA颁发机构的签名证书、根证书和中间证书。

步骤8.将根证书、中间证书和CA签名的WSM证书复制**到%CVP_HOME%\conf\security**。

步骤9.使用此命令导入根证书。

%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>。

1. 出现提示时输入密钥库密码。
2. 在信任此证书提示符下，键**入Yes**。

步骤10.使用此命令导入中间证书。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediate -file %CVP_HOME%\conf\security\<filename_of_intermediate_cer>。

1. 出现提示时输入密钥库密码。
2. 在信任此证书提示符下，键**入Yes**。

步骤11.使用此命令导入CA签名的WSM证书。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias wsm_certificate -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>。

1.在出现提示时输入密钥库密码。

步骤12.对CVP服务器上的呼叫服务器和VXML服务器证书以及报告服务器上的呼叫服务器证书重复步骤4到步骤11（根证书和中间证书不需要导入两次）。

第13步在CVP中配置WSM。

1.导航至**c:\cisco\cvp\conf\jmx_wsm.conf**。

添加或更新显示的文件并保存：

```
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.运行regedit命令。

```
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=
```

步骤14.在CVP服务器和报告服务器中配置CVP Callserver的JMX。

1.导航至**c:\cisco\cvp\conf\jmx_callserver.conf。**

如图所示更新文件并保存：

```
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 =
```

步骤15.在CVP服务器中配置VXMLServer的JMX。

1.导航至**c:\cisco\cvp\conf\jmx_vxml.conf。**

按图所示编辑文件并保存：

```
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.运行regedit命令。

- ```
  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.在CVP服务器上重新启动WSM服务、呼叫服务器和VXML服务器服务，在报告服务器上重新启动WSM服务和呼叫服务器服务。

> **注意：** 使用JMX启用安全通信时，它强制密钥库为**%CVP_HOME%\conf\security\.keystore**，而**不是%CVP_HOME%\jre\lib\security\cacerts。**因此，应将%CVP_**HOME%\jre\lib\security\cacerts中的证**书导入到**%CVP_HOME%\conf\security\.keystore。**
  ```

为WSM生成CA签名客户端证书

步骤1.登录到CVP服务器或报告服务器。从security.properties文件中检**索密钥库**密码。

> **注意**：在命令提示符下，输入更多%CVP_HOME%\conf\security.properties。Security.keystorePW = <Returns the keystore password>出现提示时输入密钥库密码。

步骤2.导航至%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 of CVP Server or Reporting Server WSM certificate> -v -keysize 2048 -keyalg RSA

1.在提示符处输入详细信息，然后键入“**是**”进行确认。
2.在出现提示时输入密钥库密码。

> **注意**：别名将与用于生成WSM服务器证书的CN相同。

步骤3.使用此命令生成别名的证书请求并将其保存到文件(例如**jmx_client.csr**)。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP Server or Reporting Server WSM certificate> -file %CVP_HOME%\conf\security\jmx_client.csr

1.在出现提示时输入密钥库密码。
2.使用以下命令验证CSR已成功生成：**dir jmx_client.csr。**

步骤4.在CA上签署JMX客户端证书。

> **注意**：按照以下步骤创建具有CA颁发机构的CA签名证书。下载CA签名的JMX客户端证书（根证书和中间证书之前下载和导入，因此不需要这些证书）。

1.在出现提示时输入密钥库密码。
2.在“信任此证书”提示符下，键入“是”。

步骤5.将CA签名的JMX客户端证书复制**到%CVP_HOME%\conf\security\。**

步骤6.使用此命令导入CA签名的JMX客户端证书。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of CVP Server or Reporting Server WSM certificate> -file %CVP_HOME%\conf\security\<CA签名JMX客户端证书的文件名>

1.在出现提示时输入密钥库密码。

步骤7.重新启动Cisco CVP呼叫服务器、VXML服务器和WSM服务。

步骤8.对Reporting Server重复相同的步骤（如果已实施）。

为OAMP生成CA签名客户端证书（将在OAMP上完成）

步骤1.登录OAMP服务器。从security.properties文件中检**索密钥库**密码。

> **注意**：在命令提示符下，输**入更多%CVP_HOME%\conf\security.properties**。
> Security.keystorePW = <Returns the keystore password>出现提示时输入密钥库密码。

步骤2.导航至**%CVP_HOME%\conf** security并生成CVP服务器WSM用于客户端身份验证的CA签名证书。使用此命令。

%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.在提示符处输入详细信息并键入“是”进行确认。
2.在出现提示时输入密钥库密码。

步骤3.使用此命令生成别名的证书请求并将其保存到文件(例如**jmx.csr**)。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP Server WSM certificate> -file %CVP_HOME%\conf\security\jmx.csr。

1.在出现提示时输入密钥库密码。

步骤4.在CA上签署证书。

> **注意**：请按照步骤使用CA颁发机构创建CA签名证书。下载CA颁发机构的证书和根证书。

步骤5.将根证书和CA签名的JMX客户端证书复制**到%CVP_HOME%\conf\security**。

步骤6.导入CA的根证书。使用此命令。

%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_cert>。

1.在出现提示时输入密钥库密码。
2.在“信任此证书”提示符下，键入“是”。

步骤7.导入CVP的CA签名JMX客户端证书。使用此命令。

%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>。

1.在出现提示时输入密钥库密码。

步骤8.重新启动OAMP服务。

步骤9.登录OAMP，以在OAMP和呼叫服务器或VXML服务器之间实现安全通信。 导航至**Device Management > Call Server**。选中Enable secure communication with the Ops console复选框。保存并部署呼叫服务器和VXML服务器。

步骤10.运行regedit命令。

导航至**HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java。**

将此项附加到文件并保存。

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

> **注意：** 保护JMX的端口后，只有在执行Oracle文档中列出的JConsole的定义步骤后，才能访问JConsole。

相关信息

- CVP安全配置指南
- 技术支持和文档 - Cisco Systems