採用相互身份驗證的CVP OAMP和CVP元件之間的安全JMX通訊

目錄

簡介

本文檔介紹如何通過證書頒發機構(CA)簽名的證書，在Cisco Unified Contact Center Enterprise(UCCE)解決方案中保護客戶語音門戶(CVP)操作和管理控制檯(OAMP)與CVP伺服器和CVP報告伺服器之間的Java管理擴展(JMX)通訊。

必要條件

需求

思科建議您瞭解以下主題：

- UCCE版本12.5(1)
- 客戶語音入口網站(CVP)版本12.5(1)

採用元件

本檔案中的資訊是根據以下軟體版本：

- UCCE 12.5(1)
- CVP 12.5(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。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

OAMP通過JMX協定與CVP呼叫伺服器、CVP VXML伺服器和CVP報告伺服器通訊。OAMP和這些CVP元件之間的安全通訊可防止JMX安全漏洞。此安全通訊是可選的，OAMP和CVP元件之間的常規操作不需要此安全通訊。

您可以通過以下方式保護JMX通訊：

- 在CVP伺服器和CVP報告伺服器中為Web服務管理器(WSM)生成證書簽名請求(CSR)。
- 在CVP伺服器和CVP報告伺服器中生成WSM的CSR客戶端證書。
- 為OAMP生成CSR客戶端證書（將在OAMP上完成）。
- 證書頒發機構對證書進行簽名。
- 匯入CVP伺服器、CVP報告伺服器和OAMP中的CA簽名證書、根證書和中間證書。
- [可選]保護JConsole登入OAMP。
- 安全系統CLI。

生成WSM的CSR證書

步驟1.登入到CVP伺服器或報告伺服器。從**security**.properties檔案**檢索keystore密**碼。

> **附註**：在命令提示符下，輸入更多%CVP_HOME%\conf\security.properties。Security.keystorePW = <返回金鑰庫密碼>在提示時輸入金鑰庫密碼。

步驟2. 導航到%CVP_HOME%\conf\security並刪除WSM證書。使用此命令。

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

出現提示時輸入金鑰庫密碼。

步驟3.對CVP伺服器上的呼叫伺服器和VXML伺服器證書和報告伺服器上的呼叫伺服器證書重複步驟2。

步驟4.為WSM伺服器生成CA簽名的證書。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. 在提示中輸入詳細資訊，並鍵入**Yes**進行確認。
2. 出現提示時輸入金鑰庫密碼。

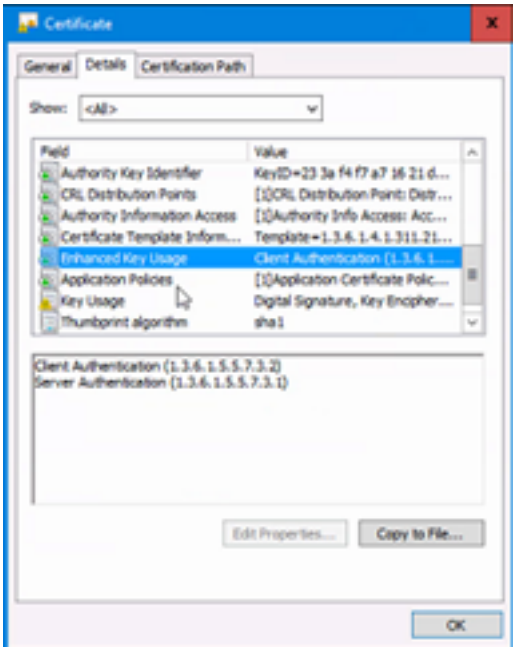
> **附註**：記下將來參照的CN名稱。

步驟5.生成別名的證書請求。運行此命令並將其儲存到檔案(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.在提示時輸入金鑰庫密碼。

步驟6.獲取CA簽署的證書。按照以下步驟建立與CA頒發機構簽署的CA簽名證書，並確保在CA生成簽名證書時使用客戶端 — 伺服器證書身份驗證模板。



步驟7.下載簽名的證書、CA機構的根證書和中間證書。

步驟8.將根、中間和CA簽名的WSM證書複製到**%CVP_HOME%\conf\security**。

步驟9.使用此命令匯入根證書。

%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. 出現提示時輸入金鑰庫密碼。
2. 在Trust this certificate提示符下，鍵入**Yes**。

步驟10.使用此命令匯入中間證書。

%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. 出現提示時輸入金鑰庫密碼。
2. 在Trust this certificate提示符下，鍵入**Yes**。

步驟11.使用此命令匯入CA簽名的WSM證書。

%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.在提示時輸入金鑰庫密碼。

步驟12.對於CVP伺服器上的Call Server和VXML伺服器證書以及報告伺服器上的Call Server證書，重複步驟4至11（無需匯入兩次根證書和中間證書）。

步驟13在CVP中配置WSM。

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

按所示新增或更新檔案並儲存：

```
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.運行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=
```

步驟14.在CVP伺服器和報告伺服器中配置CVP Callserver的JMX。

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

按所示更新檔案並儲存：

```
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 =
```

步驟15.在CVP伺服器中配置VXMLServer的JMX。

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

按所示編輯檔案並儲存：

```
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.運行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.重新啟動CVP伺服器上的WSM服務、呼叫伺服器和VXML伺服器服務以及報告伺服器上的WSM服務和呼叫伺服器服務。

附註： 當通過JMX啟用安全通訊時，它將強制金鑰庫為%CVP_HOME%\conf\security\.keystore，而不是**%CVP_HOME%\jre\lib\security\cacerts。**因此，應將**%CVP_HOME%\jre\lib\security\cacerts**的證書匯入**%CVP_HOME%\conf\security\.keystore。**
  ```

為WSM生成CA簽名的客戶端證書

步驟1.登入到CVP伺服器或報告伺服器。從**security**.properties檔案**檢索keystore密**碼。

> **附註**：在命令提示符下，輸入更多%CVP_HOME%\conf\security.properties。Security.keystorePW = <返回金鑰庫密碼>在提示時輸入金鑰庫密碼。

步驟2.使用此命令導航到%CVP_HOME%\conf\security，並生成用於callserver客戶端身份驗證的CA簽名證書。

%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.在提示中輸入詳細資訊，並鍵入**Yes**進行確認。
2.在提示時輸入金鑰庫密碼。

> **附註**：別名將與用於生成WSM伺服器證書的CN相同。

步驟3.使用此命令生成別名的證書請求並將其儲存到檔案(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.在提示時輸入金鑰庫密碼。
2.使用以下命令驗證是否成功產生CSR:**dir jmx_client.csr。**

步驟4.在CA上簽署JMX客戶端證書。

> **附註**：按照以下步驟建立具有CA頒發機構的CA簽名證書。下載CA簽名的JMX客戶端證書（根證書和中間證書不是必需的，因為它們之前已經下載和匯入）。

1.在提示時輸入金鑰庫密碼。
2.在「信任此證書」提示符下，鍵入Yes。

步驟5.將CA簽名的JMX客戶端證書複製到**%CVP_HOME%\conf\security\。**

步驟6.使用此命令匯入CA簽名的JMX客戶端證書。

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CVP Server或Reporting Server WSM證書的CN> -file %CVP_HOME%\conf\security\<CA簽名的JMX客戶端證書的檔名>

1.在提示時輸入金鑰庫密碼。

步驟7.重新啟動Cisco CVP呼叫伺服器、VXML伺服器和WSM服務。

步驟8.對報告伺服器重複相同過程（如果已實施）。

為OAMP生成CA簽名的客戶端證書（將在OAMP上完成）

步驟1.登入OAMP伺服器。從**security**.properties檔案**檢索keystore密**碼。

> **附註**：在命令提示符下，輸入更多**%CVP_HOME%\conf\security.properties**。
> Security.keystorePW = <返回金鑰庫密碼>在提示時輸入金鑰庫密碼。

步驟2.導航到**%CVP_HOME%\conf**安全，並生成用於CVP伺服器WSM的客戶端身份驗證的CA簽名證書。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.在提示中輸入詳細資訊，然後鍵入「是」進行確認。
2.在提示時輸入金鑰庫密碼。

步驟3.使用此指令產生別名的憑證請求，並將其儲存到檔案(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.在提示時輸入金鑰庫密碼。

步驟4.在CA上簽署憑證。

> **注意**：按照以下步驟使用CA頒發機構建立CA簽名的證書。下載CA頒發機構的證書和根證書。

步驟5.將根證書和CA簽名的JMX客戶端證書複製到**%CVP_HOME%\conf\security**。

步驟6.匯入CA的根證書。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.在提示時輸入金鑰庫密碼。
2.在「信任此證書」提示符下，鍵入Yes。

步驟7.匯入CVP的CA簽名的JMX客戶端證書。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.在提示時輸入金鑰庫密碼。

步驟8.重新啟動OAMP服務。

步驟9.登入OAMP。啟用OAMP與呼叫伺服器或VXML伺服器之間的安全通訊。 導航到**Device Management > Call Server**。選中Enable secure communication with the Ops console覈取方塊。儲存並部署呼叫伺服器和VXML伺服器。

步驟10.運行regedit命令。

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

將此項附加到檔案並儲存。

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

> **附註**： 保護JMX的埠後，只有在執行Oracle文檔中列出的JConsole的已定義步驟後，才能訪問JConsole。

相關資訊

- CVP安全配置指南
- 技術支援與文件 - Cisco Systems