Comunicação JMX segura entre componentes CVP OAMP e CVP com autenticação mútua

Contents

Introduction

Este documento descreve como proteger a comunicação JMX (Java Management Extensions) entre a operação e o console de gerenciamento (OAMP) do Customer Voice Portal (CVP) e o servidor CVP de relatório e o servidor CVP na solução Cisco Unified Contact Center Enterprise (UCCE) via certificados assinados pela CA (Certificate Authority).

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- UCCE versão 12.5(1)
- Customer Voice Portal (CVP) versão 12.5 (1)

Componentes Utilizados

As informações neste documento são baseadas nestas versões 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.

Informações de Apoio

O OAMP se comunica com o CVP Call Server, CVP VXML Server e CVP Reporting Server por

meio do protocolo JMX. A comunicação segura entre o OAMP e esses componentes do CVP evita vulnerabilidades de segurança do JMX. Essa comunicação segura é opcional, não é necessária para a operação regular entre o OAMP e os componentes do CVP.

Você pode proteger a comunicação JMX:

- Gere a CSR (Certificate Sign Request, solicitação de assinatura de certificado) para o WSM (Web Service Manager) no servidor CVP e no servidor de relatório CVP.
- Gerar Certificado de Cliente CSR para WSM no Servidor CVP e no Servidor de Relatórios CVP.
- Gerar Certificado de Cliente CSR para OAMP (a ser feito em OAMP).
- Assinar os certificados por uma autoridade de certificação.
- Importe os certificados assinados pela CA, raiz e intermediário no servidor CVP, no servidor de relatórios CVP e no OAMP.
- [Opcional] Login do Secure JConsole no OAMP.
- Secure System CLI

Gerar certificados CSR para WSM

Etapa 1. Faça login no CVP Server ou no Reporting Server. Recupere a senha do armazenamento de chaves do arquivo **security.properties**.

> **Note**: No prompt de comando, digite mais %CVP_HOME%\conf\security.properties. Security.keystorePW = <Devolve a senha do keystore> Introduza a senha do keystore quando solicitado.

Etapa 2. Navegue até %CVP_HOME%\conf\security and delete the WSM certificate. Use este comando.

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

Digite a senha do armazenamento de chaves quando solicitado.

Etapa 3. Repita a Etapa 2 para certificados do Servidor de Chamadas e do Servidor VXML no Servidor CVP e no Certificado do Servidor de Chamadas no Servidor de Relatórios.

Etapa 4. Gerar um certificado assinado por CA para o servidor WSM. Use 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. Insira os detalhes nos avisos e digite **Sim** para confirmar.
2. Digite a senha do armazenamento de chaves quando solicitado.

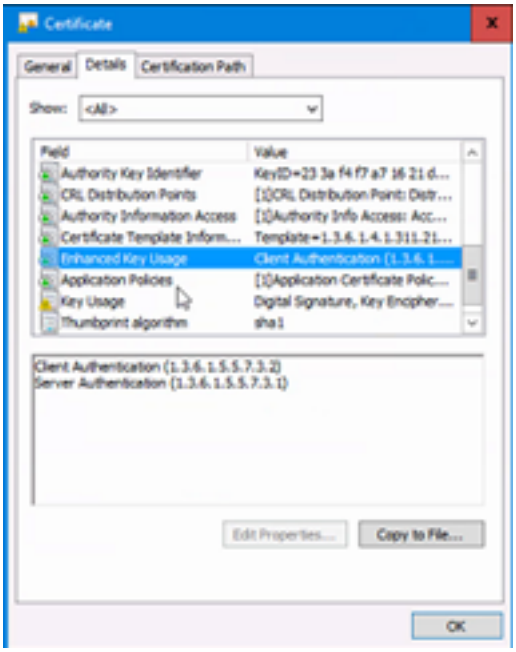
> **Note:** Observe o nome CN para referência futura.

Etapa 5. Gere a solicitação de certificado para o alias. Execute este comando e salve-o em um arquivo (por exemplo, **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. Digite a senha do armazenamento de chaves quando solicitado.

Etapa 6. Obter o certificado assinado por uma AC. Siga o procedimento para criar um certificado assinado pela AC com a autoridade da AC e certifique-se de usar um modelo de autenticação de certificado cliente-servidor quando a AC gerar o certificado assinado.



Passo 7. Baixe o certificado assinado, o certificado raiz e o certificado intermediário da autoridade CA.

Etapa 8. Copie a raiz, o intermediário e o certificado WSM assinado pela CA para **%CVP_HOME%\conf\security**.

Etapa 9. Importe o certificado raiz com este comando.

%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. Digite a senha do armazenamento de chaves quando solicitado.
2. No prompt Confiar neste certificado, digite **Sim**.

Etapa 10. Importe o certificado intermediário com este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediário -arquivo %CVP_HOME%\conf\security\<filename_of_intermediário_cer>.

1. Digite a senha do armazenamento de chaves quando solicitado.
2. No prompt Confiar neste certificado, digite **Sim**.

Etapa 11. Importe o certificado WSM assinado pela CA com este comando.

%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. Digite a senha do armazenamento de chaves quando solicitado.

Etapa 12. Repita as etapas 4 a 11 (os certificados raiz e intermediários não precisam ser importados duas vezes), para os certificados do Servidor de Chamadas e do Servidor VXML no certificado do Servidor CVP e do Servidor de Chamadas no Servidor de Relatórios.

Etapa 13 Configurar WSM no CVP.

1. Navegue até **c:\cisco\cvp\conf\jmx_wsm.conf.**

Adicione ou atualize o arquivo como mostrado e salve-o:

```
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. Execute o 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=
```

Etapa 14. Configure o JMX do CVP Callserver no servidor CVP e no servidor de relatório.

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

Atualize o arquivo como mostrado e salve-o:

```
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 =
```

Etapa 15. Configure o JMX do VXMLServer no servidor CVP.

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

Edite o arquivo como mostrado e salve-o:

```
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. Execute o 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 o serviço WSM, o servidor de chamadas e os serviços do servidor VXML no servidor CVP e o serviço de serviço e servidor de chamadas WSM no Servidor de relatórios.

> **Observação:** quando a comunicação segura está habilitada com JMX, ela força o armazenamento de chaves a ser **%CVP_HOME%\conf\security\.keystore**, em vez de **%CVP_HOME%\jre\lib\security\cacerts**.
> Portanto, os certificados de **%CVP_HOME%\jre\lib\security\cacerts** devem ser importados para **%CVP_HOME%\conf\security\.keystore**.

Gerar certificado de cliente assinado por CA para WSM

Etapa 1. Faça login no CVP Server ou no Reporting Server. Recupere a senha do armazenamento de chaves do arquivo **security.properties**.

> **Note**: No prompt de comando, digite mais %CVP_HOME%\conf\security.properties. Security.keystorePW = <Devolve a senha do keystore> Introduza a senha do keystore quando solicitado.

Etapa 2. Navegue até %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. Insira os detalhes nos avisos e digite **Sim** para confirmar.
2. Digite a senha do armazenamento de chaves quando solicitado.

> **Note**: O alias será igual ao CN usado para gerar certificado de servidor WSM.

Etapa 3. Gere a solicitação de certificado para o alias com este comando e salve-a em um arquivo (por exemplo, **jmx_client.csr**).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN do servidor CVP ou do certificado WSM do servidor de relatórios> -arquivo %CVP_HOME%\conf\security\jmx_client.csr

1. Digite a senha do armazenamento de chaves quando solicitado.
2. Verifique se o CSR foi gerado com êxito com este comando: **dir jmx_client.csr.**

Etapa 4. Assine o certificado do cliente JMX em uma CA.
  ```

> **Note**: Siga o procedimento para criar um certificado assinado pela CA com a autoridade da AC. Faça o download do certificado do cliente JMX assinado pela CA (os certificados raiz e intermediários não são necessários, pois eles foram baixados e importados anteriormente).

1. Digite a senha do armazenamento de chaves quando solicitado.
2. No prompt Confiar neste certificado, digite Sim.

Etapa 5. Copie o certificado do cliente JMX assinado pela CA para **%CVP_HOME%\conf\security\.**

Etapa 6. Importe o certificado do cliente JMX assinado pela CA com este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN do servidor CVP ou certificado WSM do servidor de relatórios> -arquivo %CVP_HOME%\conf\security\<nome do arquivo do certificado do cliente JMX assinado pela CA>

1. Digite a senha do armazenamento de chaves quando solicitado.

Passo 7. Reinicie os serviços Cisco CVP Call Server, VXML Server e WSM.

Etapa 8. Repita o mesmo procedimento para o Servidor de Relatórios, se implementado.

Gerar certificado de cliente assinado pela CA para OAMP (a ser feito em OAMP)

Etapa 1. Faça login no servidor OAMP. Recupere a senha do armazenamento de chaves do arquivo **security.properties**.

> **Note**: No prompt de comando, digite mais **%CVP_HOME%\conf\security.properties**. Security.keystorePW = <Devolve a senha do keystore> Introduza a senha do keystore quando solicitado.

Etapa 2. Navegue até **%CVP_HOME%\conf**segurança e gere um certificado assinado por CA para autenticação de cliente com o servidor CVP WSM. Use este comando.

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

1. Insira os detalhes nos avisos e digite Sim para confirmar.
2. Digite a senha do armazenamento de chaves quando solicitado.

Etapa 3. Gere a solicitação de certificado para o alias com este comando e salve-a em um arquivo (por exemplo, **jmx.csr**).

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

1. Digite a senha do armazenamento de chaves quando solicitado.

Etapa 4. Assine o certificado em uma CA.

> **Nota**: Siga o procedimento para criar um certificado assinado pela AC usando a autoridade da AC. Baixe o certificado e o certificado raiz da autoridade CA.

Etapa 5. Copie o certificado raiz e o certificado do cliente JMX assinado pela AC para **%CVP_HOME%\conf\security**.

Etapa 6. Importar o certificado raiz da AC. Use este comando.

%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. Digite a senha do armazenamento de chaves quando solicitado.
2. No prompt Confiar neste certificado, digite Sim.

Passo 7. Importar o certificado do cliente JMX assinado pela CA do CVP. Use este comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN do certificado Callserver WSM> -file %CVP_HOME%\conf\security\<filename_of_your_signed_cert_from_CA>.

1. Digite a senha do armazenamento de chaves quando solicitado.

Etapa 8. Reinicie o serviço OAMP.

Etapa 9. Faça login no OAMP. para permitir a comunicação segura entre o OAMP e o Call Server ou o VXML Server. Navegue até **Gerenciamento de dispositivos > Servidor de chamadas**. Marque a caixa de seleção Habilitar comunicação segura com o console Ops. Salve e implante o servidor de chamadas e o servidor VXML.

Etapa 10. Execute o comando regedit.

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

Acrescente isso ao arquivo e salve-o.

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

> **Observação**: depois de proteger as portas do JMX, o JConsole pode ser acessado somente depois que você executar as etapas definidas para o JConsole listadas nos documentos Oracle.

Informações Relacionadas

- Guia de configuração segura do CVP
- Suporte Técnico e Documentação - Cisco Systems