Comunicazione JMX sicura tra i componenti CVP OAMP e CVP con autenticazione reciproca

Sommario

Introduzione

In questo documento viene descritto come proteggere le comunicazioni JMX (Java Management Extensions) tra OAMP (Customer Voice Portal) e OAMP (Management Console) e CVP Server e CVP Reporting Server in una soluzione Cisco Unified Contact Center Enterprise (UCCE) tramite certificati firmati da CA (Certificate Authority).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- UCCE release 12.5(1)
- Customer Voice Portal (CVP) versione 12.5 (1)

Componenti usati

Le informazioni di questo documento si basano sulle seguenti versioni software:

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

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

OAMP comunica con CVP Call Server, CVP VXML Server e CVP Reporting Server tramite il protocollo JMX. La comunicazione sicura tra OAMP e questi componenti CVP previene le vulnerabilità della sicurezza JMX. Questa comunicazione sicura è facoltativa e non è necessaria per il normale funzionamento tra OAMP e i componenti CVP.

Èpossibile proteggere le comunicazioni JMX nei modi seguenti:

- Generare la richiesta di firma del certificato (CSR) per Web Service Manager (WSM) in CVP Server e CVP Reporting Server.
- Genera certificato client CSR per WSM in CVP Server e CVP Reporting Server.
- Generare un certificato client CSR per OAMP (da eseguire su OAMP).
- Firmare i certificati da un'Autorità di certificazione.
- Importare i certificati firmati dall'autorità di certificazione, radice e intermedio in CVP Server, CVP Reporting Server e OAMP.
- [Facoltativo] Accesso sicuro di JConsole a OAMP.
- Secure System CLI.

Genera certificati CSR per WSM

Passaggio 1. Accedere al server CVP o al server di report. Recuperare la password del keystore dal file **security.properties**.

> **Nota:** Al prompt dei comandi, immettere ulteriori %CVP_HOME%\conf\security.properties. Security.keystorePW = <Restituisce la password del keystore> Quando richiesto, immettere la password del keystore.

Passaggio 2. Passare a %CVP_HOME%\conf\security ed eliminare il certificato WSM. Utilizzare questo comando.

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

Quando richiesto, immettere la password del keystore.

Passaggio 3. Ripetere il passaggio 2 per i certificati del server di chiamata e del server VXML sul server CVP e per il certificato del server di chiamata sul server di report.

Passaggio 4. Generare un certificato firmato dalla CA per il server WSM. Utilizzare questo 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. Immettere i dettagli nei prompt e digitare **Sì** per confermare.
2. Quando richiesto, immettere la password del keystore.

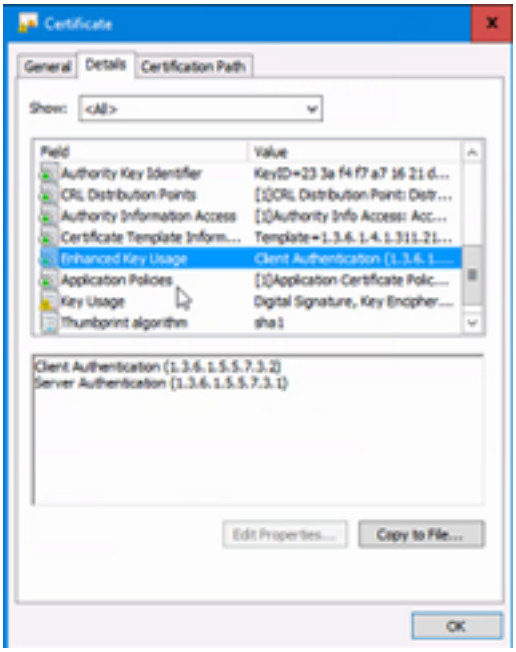
> **Nota:** Annotare il nome CN per riferimento futuro.

Passaggio 5. Generare la richiesta di certificato per l'alias. Eseguire questo comando e salvarlo in un file (ad esempio, **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. Quando richiesto, immettere la password del keystore.

Passaggio 6. Ottenere il certificato firmato da una CA. Seguire la procedura per creare un certificato firmato dalla CA con l'autorità CA e assicurarsi di utilizzare un modello di autenticazione certificato client-server quando la CA genera il certificato firmato.



Passaggio 7. Scaricare il certificato firmato, il certificato radice e intermedio dell'autorità CA.

Passaggio 8. Copiare il certificato WSM radice, intermedio e firmato dalla CA in **%CVP_HOME%\conf\security**.

Passaggio 9. Importare il certificato radice con questo 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\<nomefile_di_root_cer>.

1. Quando richiesto, immettere la password del keystore.
2. Al prompt Considera attendibile il certificato digitare **Sì**.

Passaggio 10. Importare il certificato intermedio con questo comando.

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

1. Quando richiesto, immettere la password del keystore.
2. Al prompt Considera attendibile il certificato digitare **Sì**.

Passaggio 11. Importare il certificato WSM firmato dalla CA con questo 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\<nomefile_del_certificato_firmato_da_CA>.

1. Quando richiesto, immettere la password del keystore.

Passaggio 12. Ripetere i passaggi da 4 a 11 (non è necessario importare due volte i certificati radice e intermedi) per i certificati di server di chiamata e server VXML nel server CVP e per il certificato di server di chiamata nel server di report.

Passaggio 13 Configurare WSM in CVP.

1. Passare a **c:\cisco\cvp\conf\jmx_wsm.conf.**

Aggiungere o aggiornare il file come mostrato e salvarlo:

```
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. Eseguire il 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=
```

Passaggio 14. Configurare JMX di CVP Callserver in CVP Server e Reporting Server.

1. Passare a **c:\cisco\cvp\conf\jmx_callserver.conf.**

Aggiornare il file come mostrato e salvarlo:

```
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 =
```

Passaggio 15. Configurare JMX di VXMLServer in CVP Server.

1. Passare a **c:\cisco\cvp\conf\jmx_vxml.conf.**

Modificare il file come mostrato e salvarlo:

```
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. Eseguire il 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. Riavviare i servizi WSM, Call Server e VXML Server sul server CVP e i servizi WSM e Call Server sul server di report.

> **Nota:** Quando la comunicazione protetta è abilitata con JMX, forza il keystore a **%CVP_HOME%\conf\security\.keystore**, anziché a **%CVP_HOME%\jre\lib\security\cacerts**. I certificati di **%CVP_HOME%\jre\lib\security\cacerts** devono pertanto essere importati in **%CVP_HOME%\conf\security\.keystore**.

Genera certificato client con firma CA per WSM

Passaggio 1. Accedere al server CVP o al server di report. Recuperare la password del keystore dal file **security.properties**.

> **Nota:** Al prompt dei comandi, immettere ulteriori %CVP_HOME%\conf\security.properties. Security.keystorePW = <Restituisce la password del keystore> Quando richiesto, immettere la password del keystore.

Passaggio 2. Passare a %CVP_HOME%\conf\security e generare un certificato firmato dalla CA per l'autenticazione client con callserver con questo comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN del certificato WSM di CVP Server o Reporting Server> -v -keysize 2048 -keyalg RSA

1. Inserire i dettagli nei prompt e digitare **Sì** per confermare.
2. Quando richiesto, immettere la password del keystore.

> **Nota:** L'alias sarà lo stesso utilizzato per generare il certificato del server WSM.

Passaggio 3. Generare la richiesta di certificato per l'alias con questo comando e salvarla in un file (ad esempio, **jmx_client.csr**).

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN del certificato WSM di CVP Server o Reporting Server> -file %CVP_HOME%\conf\security\jmx_client.csr

1. Quando richiesto, immettere la password del keystore.
2. Verificare che il CSR sia stato generato correttamente con questo comando: **dir jmx_client.csr**

Passaggio 4. Firmare il certificato client JMX su una CA.

> **Nota:** Seguire la procedura per creare un certificato firmato dalla CA con l'autorità CA. Scaricare il certificato client JMX firmato dalla CA (i certificati radice e intermedi non sono necessari poiché sono stati scaricati e importati in precedenza).
  ```

1. Quando richiesto, immettere la password del keystore.
2. Al prompt Considera attendibile il certificato, digitare Sì.

Passaggio 5. Copiare il certificato client JMX firmato dalla CA in **%CVP_HOME%\conf\security\.**

Passaggio 6. Importare il certificato client JMX firmato dalla CA con questo comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN del certificato WSM di CVP Server o Reporting Server> -file %CVP_HOME%\conf\security\<nome file del certificato client JMX firmato da CA>

1. Quando richiesto, immettere la password del keystore.

Passaggio 7. Riavviare Cisco CVP Call Server, VXML Server e i servizi WSM.

Passaggio 8. Ripetere la stessa procedura per Reporting Server, se implementata.

Genera certificato client con firma CA per OAMP (da eseguire su OAMP)

Passaggio 1. Accedere al server OAMP. Recuperare la password del keystore dal file **security.properties**.

> **Nota:** Al prompt dei comandi, immettere **%CVP_HOME%\conf\security.properties**. Security.keystorePW = <Restituisce la password del keystore> Quando richiesto, immettere la password del keystore.

Passaggio 2. Passare a **%CVP_HOME%\conf**security e generare un certificato firmato dalla CA per l'autenticazione client con CVP Server WSM. Utilizzare questo comando.

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

1. Inserire i dettagli nei prompt e digitare Sì per confermare.
2. Quando richiesto, immettere la password del keystore.

Passaggio 3. Generare la richiesta di certificato per l'alias con questo comando e salvarla in un file (ad esempio, **jmx.csr**).

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

1. Quando richiesto, immettere la password del keystore.

Passaggio 4. Firmare il certificato su una CA.

> **Nota**: seguire la procedura per creare un certificato firmato dalla CA utilizzando l'autorità CA.

Scaricare il certificato e il certificato radice dell'autorità CA.

Passaggio 5. Copiare il certificato radice e il certificato client JMX firmato dall'autorità di certificazione in **%CVP_HOME%\conf\security**.

Passaggio 6. Importare il certificato radice della CA. Utilizzare questo 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\<nomefile_di_root_cert>.

1. Quando richiesto, immettere la password del keystore.
2. Al prompt Considera attendibile il certificato, digitare Sì.

Passaggio 7. Importare il certificato client JMX firmato dalla CA di CVP. Utilizzare questo comando.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN del certificato WSM del server di chiamata> -file %CVP_HOME%\conf\security\<nomefile_del_certificato_firmato_da_CA>.

1. Quando richiesto, immettere la password del keystore.

Passaggio 8. Riavviare il servizio OAMP.

Passaggio 9. Accedere a OAMP. per abilitare la comunicazione protetta tra OAMP e Call Server o server VXML. Selezionare **Gestione dispositivi > Call Server**. Selezionare la casella di controllo Attiva comunicazione protetta con la console Operazioni. Salvare e distribuire sia Call Server che VXML Server.

Passaggio 10. Eseguire il comando regedit.

Passare a **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java.**

Aggiungere al file e salvarlo.

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

> **Nota:** Dopo aver protetto le porte per JMX, è possibile accedere a JConsole solo dopo aver eseguito i passi definiti per JConsole elencati nei documenti Oracle.

Informazioni correlate

- Guida alla configurazione sicura di CVP
- Documentazione e supporto tecnico – Cisco Systems