Sichere JMX-Kommunikation zwischen CVP OAMP- und CVP-Komponenten mit gegenseitiger Authentifizierung

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die JMX-Kommunikation (Java Management Extensions) zwischen Customer Voice Portal (CVP) Operation and Management Console (OAMP) und CVP Server und CVP Reporting Server in der Cisco Unified Contact Center Enterprise (UCCE)-Lösung über Zertifikate der Zertifizierungsstelle (Certificate Authority, CA) signierte Zertifikate abgesichert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Hintergrundinformationen

OAMP kommuniziert über das JMX-Protokoll mit dem CVP Call Server, dem CVP VXML-Server und dem CVP Reporting Server. Die sichere Kommunikation zwischen OAMP und diesen CVP-Komponenten verhindert JMX-Sicherheitslücken. Diese sichere Kommunikation ist optional und für den regulären Betrieb zwischen OAMP und den CVP-Komponenten nicht erforderlich.

Sie können die JMX-Kommunikation wie folgt sichern:

- Erstellen Sie die CSR-Anfrage (Certificate Sign Request) für Web Service Manager (WSM) im CVP-Server und im CVP-Reporting-Server.
- Erstellen Sie ein CSR-Client-Zertifikat für WSM im CVP-Server und im CVP-Reporting-Server.
- Erstellen eines CSR-Client-Zertifikats für OAMP (für OAMP erforderlich)
- Signieren Sie die Zertifikate durch eine Zertifizierungsstelle.
- Importieren Sie Zertifikate mit CA-Signatur, Root und Intermediate in CVP Server, CVP Reporting Server und OAMP.
- [Optional] Sichere Anmeldung von JConsole bei OAMP.
- Secure System CLI.

Erstellen von CSR-Zertifikaten für WSM

Schritt 1: Melden Sie sich beim CVP-Server oder Reporting Server an. Rufen Sie das Schlüsselwort aus der Datei **security.properties ab**.

> **Hinweis:** Geben Sie an der Eingabeaufforderung mehr %CVP_HOME%\conf\security.properties ein. Security.keystorePW = <Gibt das Schlüsselwort zurück> Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 2: Navigieren Sie zu %CVP_HOME%\conf\security and delete the WSM certificate. Verwenden Sie diesen Befehl.

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

Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 3: Wiederholen Sie Schritt 2 für Anrufserver- und VXML-Serverzertifikate auf dem CVP-Server und dem Anrufserver-Zertifikat auf dem Reporting Server.

Schritt 4: Generieren Sie ein CA-signiertes Zertifikat für den WSM-Server. Verwenden Sie diesen Befehl:

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

1. Geben Sie in die Eingabeaufforderungen die Details ein, und geben Sie **Yes** to confirm ein.

2. Geben Sie bei Aufforderung das Schlüsselwort ein.

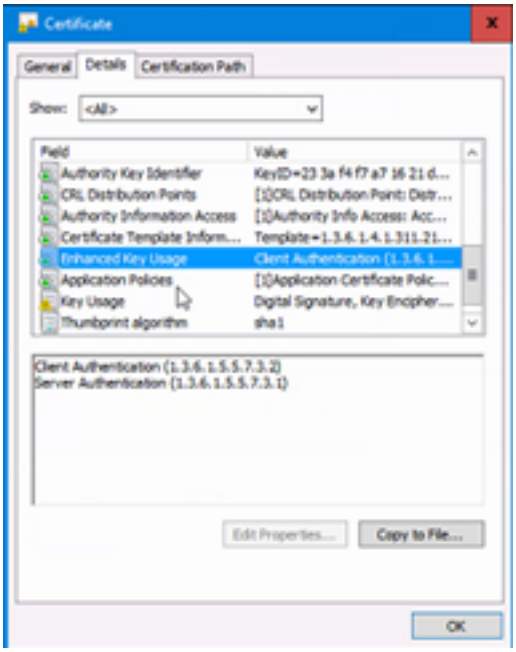
Hinweis: Notieren Sie sich den CN-Namen als Referenz.

Schritt 5: Generieren Sie die Zertifikatsanforderung für den Alias. Führen Sie diesen Befehl aus, und speichern Sie ihn in einer Datei (z. B. **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. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 6: Lassen Sie sich das Zertifikat von einer Zertifizierungsstelle signieren. Gehen Sie wie folgt vor, um ein Zertifikat mit Zertifizierungsstellen zu erstellen, das von einer Zertifizierungsstelle signiert wurde, und stellen Sie sicher, dass beim Generieren des signierten Zertifikats durch die Zertifizierungsstelle eine Authentifizierungsvorlage für Client-Server-Zertifikate verwendet wird.



Schritt 7: Laden Sie das signierte Zertifikat, das Root- und Zwischenzertifikat der Zertifizierungsstellen herunter.

Schritt 8: Kopieren Sie das Root-, Intermediär- und das CA-signierte WSM-Zertifikat in **%CVP_HOME%\conf\security**.

Schritt 9: Importieren Sie das Stammzertifikat mit diesem Befehl.

%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. Geben Sie bei Aufforderung das Schlüsselwort ein.
2. Geben Sie bei Aufforderung zur Vertrauenswürdigkeit dieses Zertifikats **Yes** ein.

Schritt 10: Importieren Sie das Zwischenzertifikat mit diesem Befehl.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore

%CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias intermediär -file %CVP_HOME%\conf\security\<filename_of_intermediale_cer>.

1. Geben Sie bei Aufforderung das Schlüsselwort ein.
2. Geben Sie bei Aufforderung zur Vertrauenswürdigkeit dieses Zertifikats **Yes** ein.

Schritt 11: Importieren Sie mit diesem Befehl das WSM-Zertifikat mit CA-Vorzeichen.

%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. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 12: Wiederholen Sie die Schritte 4 bis 11 (Root- und Zwischenzertifikate müssen nicht zweimal importiert werden) für Call Server- und VXML-Server-Zertifikate auf dem CVP-Server und dem Call Server-Zertifikat auf dem Reporting Server.

Schritt 13 Konfigurieren von WSM in CVP

1. Navigieren Sie zu **c:\cisco\cvp\conf\jmx_wsm.conf.**

Fügen Sie die Datei wie gezeigt hinzu, oder aktualisieren Sie sie, und speichern Sie sie:

```
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. Führen Sie den Befehl regedit aus.

```
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=
```

Schritt 14: Konfigurieren Sie JMX des CVP-Callservers im CVP-Server und im Reporting-Server.

1. Navigieren Sie zu **c:\cisco\cvp\conf\jmx_callserver.conf.**

Aktualisieren Sie die Datei wie gezeigt, und speichern Sie sie:

```
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 =
```

Schritt 15: Konfigurieren Sie JMX von VXMLServer im CVP-Server.

1. Navigieren Sie zu **c:\cisco\cvp\conf\jmx_vxml.conf.**

Bearbeiten Sie die Datei wie gezeigt, und speichern Sie sie:

```
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. Führen Sie den Befehl regedit aus.

- ```
  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. Starten Sie den WSM-Service, die Call Server- und VXML-Serverdienste auf dem CVP-Server und den WSM-Service sowie den Call Server-Service auf dem Reporting Server neu.

> **Hinweis:** Wenn die sichere Kommunikation mit JMX aktiviert ist, wird der Keystore dazu gezwungen, **%CVP_HOME%\conf\security\.keystore** anstatt **%CVP_HOME%\jre\lib\security\cacerts zu** sein.
> Daher sollten die Zertifikate von **%CVP_HOME%\jre\lib\security\cacerts** nach **%CVP_HOME%\conf\security\.keystore** importiert werden.

Erstellen eines CA-signierten Client-Zertifikats für WSM

Schritt 1: Melden Sie sich beim CVP-Server oder Reporting Server an. Rufen Sie das Schlüsselwort aus der Datei **security.properties ab**.

> **Hinweis:** Geben Sie an der Eingabeaufforderung mehr %CVP_HOME%\conf\security.properties ein. Security.keystorePW = <Gibt das Schlüsselwort zurück> Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 2: Navigieren Sie zu %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 des CVP-Servers oder Reporting Server WSM-Zertifikat> -v -keysize 2048 -keyalg RSA

1. Geben Sie in die Eingabeaufforderungen die Details ein, und geben Sie **Yes** to confirm ein.
2. Geben Sie bei Aufforderung das Schlüsselwort ein.

> **Hinweis:** Der Alias entspricht dem CN, der zum Generieren des WSM-Serverzertifikats verwendet wird.

Schritt 3: Generieren Sie die Zertifikatsanforderung für den Alias mit diesem Befehl, und speichern Sie sie in einer Datei (z. B. **jmx_client.csr**).

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

1. Geben Sie bei Aufforderung das Schlüsselwort ein.
2. Überprüfen Sie, ob der CSR mit dem folgenden Befehl erfolgreich generiert wurde: **dir jmx_client.csr.**

Schritt 4: Signieren Sie das JMX Client-Zertifikat auf einer CA.

> **Hinweis:** Gehen Sie wie folgt vor, um ein Zertifikat mit Zertifizierungsstellen zu erstellen, das von einer Zertifizierungsstelle signiert wurde. Laden Sie das CA-signierte JMX Client-Zertifikat herunter (Stamm- und Zwischenzertifikate sind nicht erforderlich, da sie zuvor heruntergeladen und importiert wurden).

1. Geben Sie bei Aufforderung das Schlüsselwort ein.
2. Geben Sie bei Aufforderung zur Bestätigung die Zeichenfolge Yes (Ja) ein.

Schritt 5: Kopieren Sie das CA-signierte JMX Client-Zertifikat in **%CVP_HOME%\conf\security\.**

Schritt 6: Importieren Sie das CA-signierte JMX Client-Zertifikat mit diesem Befehl.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN des CVP-Servers oder Reporting Server WSM-Zertifikat> -file %CVP_HOME%\conf\security\<filename des CA-signierten JMX-Client-Zertifikats>

1. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 7: Starten Sie den Cisco CVP-Anrufserver, den VXML-Server und die WSM-Dienste neu.

Schritt 8: Wiederholen Sie die gleiche Prozedur für Reporting Server (sofern implementiert).

Erstellen eines CA-signierten Client-Zertifikats für OAMP (auf OAMP)

Schritt 1: Melden Sie sich beim OAMP-Server an. Rufen Sie das Schlüsselwort aus der Datei **security.properties ab**.

> **Hinweis:** Geben Sie an der Eingabeaufforderung more **%CVP_HOME%\conf\security.properties ein**. Security.keystorePW = <Gibt das Schlüsselwort zurück> Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 2: Navigieren Sie zu **%CVP_HOME%\conf**, und generieren Sie ein Zertifikat mit CA-Signatur für die Client-Authentifizierung mit CVP Server WSM. Verwenden Sie diesen Befehl.

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

1. Geben Sie die Details an den Eingabeaufforderungen ein, und geben Sie Yes (Ja) zur Bestätigung ein.
2. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 3: Generieren Sie die Zertifikatsanforderung für den Alias mit diesem Befehl, und speichern Sie sie in einer Datei (z. B. **jmx.csr**).

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

1. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 4: Signieren Sie das Zertifikat auf einer Zertifizierungsstelle.

> **Hinweis**: Befolgen Sie das Verfahren zum Erstellen eines Zertifikats mit CA-Signatur unter Verwendung der Zertifizierungsstellen. Laden Sie das Zertifikat und das Stammzertifikat der Zertifizierungsstelle herunter.

Schritt 5: Kopieren Sie das Stammzertifikat und das CA-signierte JMX Client-Zertifikat in **%CVP_HOME%\conf\security**.

Schritt 6: Importieren Sie das Root-Zertifikat der CA. Verwenden Sie diesen Befehl.

%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. Geben Sie bei Aufforderung das Schlüsselwort ein.
2. Geben Sie bei Aufforderung zur Bestätigung die Zeichenfolge Yes (Ja) ein.

Schritt 7: Importieren Sie das CA-signierte JMX Client-Zertifikat von CVP. Verwenden Sie diesen Befehl.

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

1. Geben Sie bei Aufforderung das Schlüsselwort ein.

Schritt 8: Starten Sie den OAMP-Dienst neu.

Schritt 9: Melden Sie sich bei OAMP an. um eine sichere Kommunikation zwischen OAMP und dem Anrufserver oder dem VXML-Server zu ermöglichen. Navigieren Sie zu **Gerätemanagement > Anrufserver**. Aktivieren Sie das Kontrollkästchen Sichere Kommunikation mit der Betriebskonsole aktivieren. Speichern und Bereitstellen von Anrufserver und VXML-Server.

Schritt 10: Führen Sie den Befehl regedit aus.

Navigieren Sie zu **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java.**

Hängen Sie diese an die Datei an, und speichern Sie sie.

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

```
Djavax.net.ssl.trustStorePassword=
```

Hinweis: Nachdem Sie die Ports für JMX gesichert haben, können Sie auf JConsole nur zugreifen, nachdem Sie die in den Oracle-Dokumenten aufgeführten definierten Schritte für JConsole ausgeführt haben.

Zugehörige Informationen

- CVP Secure Configuration Guide
- Technischer Support und Dokumentation für Cisco Systeme