상호 인증을 통해 CVP OAMP와 CVP 구성 요소 간의 보안 JMX 통신

목차

소개

이 문서에서는 CA(Certificate Authority) 서명 인증서를 통해 Cisco Unified Contact Center Enterprise(UCCE) 솔루션에서 CVP(Customer Voice Portal) OAMP(Operation and Management Console)와 CVP 서버 및 CVP 보고 서버 간의 JMX(Java Management Extensions) 통신을 보호하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

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

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

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

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

OAMP는 JMX 프로토콜을 통해 CVP Call Server, CVP VXML Server 및 CVP Reporting Server와

통신합니다.OAMP와 이러한 CVP 구성 요소 간의 보안 통신을 통해 JMX 보안 취약성이 방지됩니다.이러한 보안 통신은 선택 사항이며, OAMP와 CVP 구성 요소 간의 정기적인 작동에는 필요하지 않습니다.

다음을 통해 JMX 통신을 보호할 수 있습니다.

- CVP 서버 및 CVP 보고 서버에서 WSM(Web Service Manager)용 CSR(Certificate Sign Request)을 생성합니다.
- CVP 서버 및 CVP 보고 서버에서 WSM용 CSR 클라이언트 인증서를 생성합니다.
- OAMP용 CSR 클라이언트 인증서 생성(OAMP에서 수행)
- CA에서 인증서를 서명합니다.
- CVP 서버, CVP 보고 서버 및 OAMP에서 CA 서명 인증서, 루트 및 중간 인증서를 가져옵니다.
- [선택 사항] OAMP에 JConsole 로그인 보안
- Secure System CLI.

WSM용 CSR 인증서 생성

1단계. CVP 서버 또는 보고 서버에 로그인합니다.security**.properties** 파일에서 키 저장소 암호를 검색합니다.

> **참고:**명령 프롬프트에서 더 많은 %CVP_HOME%\conf\security.properties을 입력합니다.Security.keystorePW = <키 저장소 암호를 반환합니다.> 메시지가 표시되면 키 저장소 암호를 입력합니다.

2단계. %CVP_HOME%\conf\security and delete the WSM certificate으로 이동합니다.이 명령을 사용합니다.

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

프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

3단계. CVP 서버의 통화 서버 및 VXML 서버 인증서에 대해 2단계를 반복하고 보고 서버의 호출 서버 인증서에 대해 2단계를 반복합니다.

4단계. WSM 서버용 CA 서명 인증서를 생성합니다.다음 명령을 사용합니다.

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

1. 프롬프트에 세부사항을 입력하고 **예**를 입력하여 확인합니다.
2. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

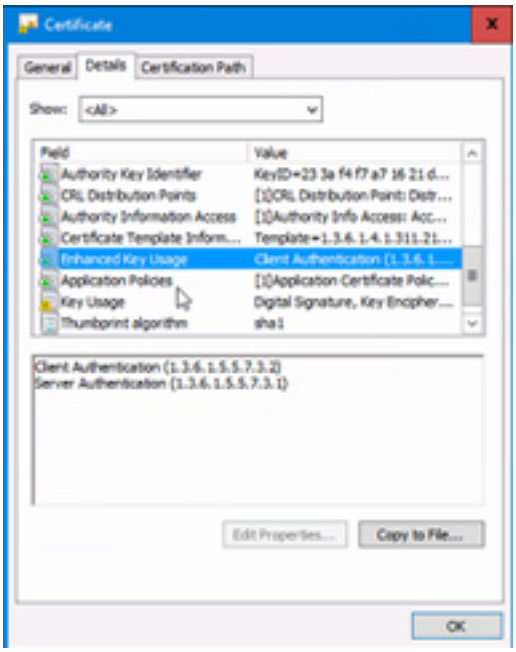
> **참고:**향후 참조를 위해 CN 이름을 확인합니다.

5단계. 별칭에 대한 인증서 요청을 생성합니다.이 명령을 실행하여 파일(예: **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. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

6단계. CA에서 서명한 인증서를 가져옵니다.CA 인증 기관이 CA 서명 인증서를 생성하고 CA가 서명 인증서를 생성할 때 클라이언트-서버 인증서 인증 템플릿을 사용하도록 하려면 절차를 수행합니다.



7단계. 서명된 인증서, CA 기관의 루트 및 중간 인증서를 다운로드합니다.

8단계. 루트, 중간 및 CA 서명 WSM 인증서를 %CVP_**HOME%\conf\security\에 복사합니다**.

9단계. 이 명령을 사용하여 루트 인증서를 가져옵니다.

%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. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.
2. Trust this certificate 프롬프트에서 **Yes를 입력합니다**.

10단계. 이 명령을 사용하여 중간 인증서를 가져옵니다.

%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. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.
2. Trust this certificate 프롬프트에서 **Yes를 입력합니다**.

11단계. 이 명령을 사용하여 CA 서명 WSM 인증서를 가져옵니다.

%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. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

12단계. CVP 서버의 통화 서버 및 VXML 서버 인증서 및 보고 서버의 통화 서버 인증서에 대해 4단계부터 11단계까지 반복합니다(루트 및 중간 인증서는 두 번 가져올 필요가 없음).

13단계 CVP에서 WSM을 구성합니다.

1. c:\cisco\cvp\conf\jmx_wsm.conf으로 **이동합니다.**

표시된 대로 파일을 추가 또는 업데이트하고 저장합니다.

```
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. regedit 명령을 실행합니다.

```
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=
```

14단계. CVP 서버 및 보고 서버에서 CVP Callserver의 JMX를 구성합니다.

1. c:\cisco\cvp\conf\jmx_callserver.conf으로 **이동합니다.**

표시된 대로 파일을 업데이트하고 저장합니다.

```
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 =
```

15단계. CVP 서버에서 VXMLServer의 JMX를 구성합니다.

1. c:\cisco\cvp\conf\jmx_vxml.conf으로 **이동합니다.**

표시된 대로 파일을 편집하고 저장합니다.

```
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. regedit 명령을 실행합니다.

- ```
  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. CVP 서버에서 WSM 서비스, 통화 서버 및 VXML 서버 서비스를 다시 시작하고 보고 서버에서
  ```

WSM 서비스 및 통화 서버 서비스를 다시 시작합니다.

> **참고:** JMX를 사용하여 보안 통신을 사용하도록 설정하면 키 저장소가 %CVP_HOME%\jre\lib\security\cacerts 대신 **%CVP_HOME%\conf\security\.keystore가 됩니다**.
> 따라서 %CVP_**HOME%\jre\lib\security\cacerts**의 인증서를 %CVP_**HOME%\conf\security\.keystore로 가져와야 합니다**.

WSM용 CA 서명 클라이언트 인증서 생성

1단계. CVP 서버 또는 보고 서버에 로그인합니다.security**.properties** 파일에서 키 저장소 암호를 검색합니다.

> **참고:**명령 프롬프트에서 더 많은 %CVP_HOME%\conf\security.properties을 입력합니다 .Security.keystorePW = <키 저장소 암호를 반환합니다.> 메시지가 표시되면 키 저장소 암호를 입력합니다.

2단계. %CVP_HOME%\conf\security and generate a CA-signed certificate for client authentication with callserver with this command으로 이동합니다.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -genkeypair -alias <CN of CVP 서버 또는 보고 서버 WSM 인증서> -v -keysize 2048 -keyalg RSA

1. 프롬프트에 상세내역을 입력하고 **예**를 입력하여 확인합니다.
2. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

> **참고:**별칭은 WSM 서버 인증서를 생성하는 데 사용된 CN과 동일합니다.

3단계. 이 명령으로 별칭에 대한 인증서 요청을 생성하고 파일(예: jmx_**client.csr**)에 저장합니다.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -certreq -alias <CN of CVP 서버 또는 보고 서버 WSM 인증서> -file %CVP_HOME%\conf\security\jmx_client.csr

1. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.
2. 다음 명령을 사용하여 CSR이 성공적으로 생성되었는지 확인합니다.**dir jmx_client.csr**

4단계. CA에서 JMX 클라이언트 인증서에 서명합니다.

> **참고:**절차에 따라 CA 인증 기관과 함께 CA 서명 인증서를 생성합니다.CA 서명 JMX 클라이언트 인증서를 다운로드합니다(루트 및 중간 인증서는 이전에 다운로드 및 가져오기되었으므로 필요하지 않습니다).

1. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.
2. Trust this certificate 프롬프트에서 Yes를 입력합니다.

5단계. CA 서명 JMX 클라이언트 인증서를 %CVP_**HOME%\conf\security\에 복사합니다.**

6단계. 이 명령을 사용하여 CA 서명 JMX 클라이언트 인증서를 가져옵니다.

%CVP_HOME%\jre\bin\keytool.exe -storetype JCEKS -keystore %CVP_HOME%\conf\security\.keystore -import -v -trustcacerts -alias <CN of CVP Server 또는 Reporting Server WSM 인증서> -file %CVP_HOME%\conf\security\<CA 서명 JMX 클라이언트 인증서의 파일 이름>

1. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

7단계. Cisco CVP Call Server, VXML Server 및 WSM 서비스를 다시 시작합니다.

8단계. 구현된 경우 Reporting Server에 대해 동일한 절차를 반복합니다.

OAMP용 CA 서명 클라이언트 인증서 생성(OAMP에서 수행)

1단계. OAMP 서버에 로그인합니다.security.**properties** 파일에서 키 저장소 암호를 검색합니다.

> **참고:**명령 프롬프트에서 more%CVP_**HOME%\conf\security.properties을 입력합니다** .Security.keystorePW = <키 저장소 암호를 반환합니다.> 메시지가 표시되면 키 저장소 암호를 입력합니다.

2단계. %CVP_**HOME%\conf**security로 이동하여 CVP 서버 WSM을 사용하여 클라이언트 인증을 위한 CA 서명 인증서를 생성합니다.이 명령을 사용합니다.

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

1. 프롬프트에 상세내역을 입력하고 확인을 위해 예를 입력합니다.
2. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

3단계. 이 명령으로 별칭에 대한 인증서 요청을 생성하고 파일(예: jmx.csr)**에** 저장합니다.

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

1. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

4단계. CA에 인증서를 서명합니다.

> **참고**: CA 권한을 사용하여 CA 서명 인증서를 생성하려면 절차를 수행합니다.CA 기관의 인증서 및 루트 인증서를 다운로드합니다.

5단계. 루트 인증서 및 CA 서명 JMX 클라이언트 인증서를 %CVP_**HOME%\conf\security\에 복사합니다**.

6단계. CA의 루트 인증서를 가져옵니다.이 명령을 사용합니다.

%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. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.
2. Trust this certificate 프롬프트에서 Yes를 입력합니다.

7단계. CVP의 CA 서명 JMX 클라이언트 인증서를 가져옵니다.이 명령을 사용합니다.

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

1. 프롬프트가 표시되면 키 저장소 비밀번호를 입력합니다.

8단계. OAMP 서비스를 다시 시작합니다.

9단계. OAMP에 로그인하여 OAMP와 Call Server 또는 VXML Server 간 보안 통신을 활성화합니다. Device **Management > Call Server로 이동합니다**.Enable secure communication with the Ops console(운영 콘솔과의 보안 통신 활성화) 확인란을 선택합니다.통화 서버와 VXML 서버를 모두 저장하고 배포합니다.

10단계. regedit 명령을 실행합니다.

HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Apache Software Foundation\Procrun 2.0\OPSConsoleServer\Parameters\Java으로 **이동합니다.**

이 파일을 파일에 추가하고 저장합니다.

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

> **참고:** JMX용 포트를 보호한 후 Oracle 문서에 나열된 JConsole에 대해 정의된 단계를 수행한 후에만 JConsole에 액세스할 수 있습니다.

관련 정보

- CVP 보안 구성 가이드
- 기술 지원 및 문서 – Cisco Systems