CVP 웹 서비스용 타사 웹 서버 인증서 구성

목차

소개

이 문서에서는 웹 서비스에 액세스하기 위해 Cisco CVP(Customer Voice Portal)의 VXML(Voice Extensible Markup Language) 애플리케이션에 대한 인증서를 업로드하는 절차에 대해 설명합니다.

사전 요구 사항

java keytool 명령 옵션을 참조하십시오.

Keytool 설명서

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Cisco CVP(Unified Customer Voice Portal)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco CVP(Unified Customer Voice Portal) 릴리스 11.X 이상

구성

이 예에서는 webserver.cer라는 인증서를 **설치합니다**.인증서가 인증서 저장소와 동일한 폴더에 복사됩니다.인증서 저장소, 캐시, 키 저장소 암호는 *변경됩니다*.

응용 프로그램을 디버깅하려면 Call Studio에 인증서를 설치합니다.

Call Studio에 대한 인증서 리포지토리는 **%CALLSTUDIO_HOME%\eclipse\jre\lib\security\cacerts입니다**.Keytool.exe 프로그램은

%CALLSTUDIO_**HOME%\eclipse\jre\bin** 폴더 아래에 있습니다.

```
cd %CALLSTUDIO_HOME%\eclipse\jre\lib\security

C:\Cisco\CallStudio\eclipse\jre\lib\security>dir
 Volume in drive C has no label.
 Volume Serial Number is 1800-FBA8

 Directory of C:\Cisco\CallStudio\eclipse\jre\lib\security

07/17/2019  11:03 AM    <DIR>          .
07/17/2019  11:03 AM    <DIR>          ..
12/23/2018  08:33 AM             4,054 blacklist
12/23/2018  08:33 AM             1,253 blacklisted.certs
12/23/2018  08:33 AM           114,757 cacerts
12/23/2018  08:33 AM             2,466 java.policy
12/23/2018  08:33 AM            42,624 java.security
12/23/2018  08:33 AM                98 javaws.policy
02/19/2019  03:38 PM    <DIR>          policy
12/23/2018  08:33 AM                 0 trusted.libraries
03/24/2016  12:45 PM             2,090 webserver.cer
               8 File(s)        167,342 bytes
               3 Dir(s)  54,560,612,352 bytes free

C:\Cisco\CallStudio\eclipse\jre\lib\security>..\..\bin\keytool.exe -importcert -file
webserver.cer -keystore cacerts -alias somewebserver
Enter keystore password:changeit
Trust this certificate? [no]:yes
Certificate was added to keystore
```

CVP VXML 서버에 인증서를 설치합니다.

CVP VXML 서버의 인증서 리포지토리는 %CVP_**HOME%\jre\lib\security\cacerts입니다** .Keytool.exe 프로그램은 %CVP_**HOME%\jre\bin** 폴더 아래에 있습니다.

```
cd %CVP_HOME%\jre\lib\security\

C:\Cisco\CVP\jre\lib\security>dir
 Volume in drive C has no label.
 Volume Serial Number is 1800-FBA8

 Directory of C:\Cisco\CVP\jre\lib\security

07/17/2019  11:46 AM    <DIR>          .
07/17/2019  11:46 AM    <DIR>          ..
12/23/2018  08:37 AM             4,054 blacklist
12/23/2018  08:37 AM             1,253 blacklisted.certs
12/23/2018  08:37 AM           114,757 cacerts
12/23/2018  08:37 AM             2,466 java.policy
12/23/2018  08:37 AM            42,624 java.security
12/23/2018  08:37 AM                98 javaws.policy
02/12/2019  12:45 PM    <DIR>          policy
12/23/2018  08:37 AM                 0 trusted.libraries
03/24/2016  12:45 PM             2,090 webserver.cer
               8 File(s)        167,342 bytes
               3 Dir(s)  54,558,191,616 bytes free

C:\Cisco\CVP\jre\lib\security>..\..\bin\keytool.exe -importcert -file webserver.cer -keystore
cacerts -alias somewebserver
Enter keystore password:changeit
```

```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

다음을 확인합니다.

인증서 저장소 캐시가 있는 폴더 아래에 있는 저장소에 설치된 인증서를 확인하려면 다음 명령을 실행합니다.

```
..\..\bin\keytool.exe -list -keystore cacerts -storepass changeit -v
Keystore type: jks
Keystore provider: SUN

Your keystore contains 106 entries

Alias name: verisignclass2g2ca [jdk]
Creation date: Aug 25, 2016
Entry type: trustedCertEntry

Owner: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only",
OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Issuer: OU=VeriSign Trust Network, OU="(c) 1998 VeriSign, Inc. - For authorized use only",
OU=Class 2 Public Primary Certification Authority - G2, O="VeriSign, Inc.", C=US
Serial number: b92f60cc889fa17a4609b85b706c8aaf
Valid from: Sun May 17 17:00:00 PDT 1998 until: Tue Aug 01 16:59:59 PDT 2028
Certificate fingerprints:
 MD5:  2D:BB:E5:25:D3:D1:65:82:3A:B7:0E:FA:E6:EB:E2:E1
 SHA1: B3:EA:C4:47:76:C9:C8:1C:EA:F2:9D:95:B6:CC:A0:08:1B:67:EC:9D
 SHA256:
3A:43:E2:20:FE:7F:3E:A9:65:3D:1E:21:74:2E:AC:2B:75:C2:0F:D8:98:03:05:BC:50:2C:AF:8C:2D:9B:41:A1
Signature algorithm name: SHA1withRSA
Subject Public Key Algorithm: 1024-bit RSA key
Version: 1


*******************************************
*******************************************


Alias name: digicertassuredidg3 [jdk]
Creation date: Aug 25, 2016
Entry type: trustedCertEntry

Owner: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Issuer: CN=DigiCert Assured ID Root G3, OU=www.digicert.com, O=DigiCert Inc, C=US
Serial number: ba15afa1ddfa0b54944afcd24a06cec
Valid from: Thu Aug 01 05:00:00 PDT 2013 until: Fri Jan 15 04:00:00 PST 2038
Certificate fingerprints:
 MD5:  7C:7F:65:31:0C:81:DF:8D:BA:3E:99:E2:5C:AD:6E:FB
 SHA1: F5:17:A2:4F:9A:48:C6:C9:F8:A2:00:26:9F:DC:0F:48:2C:AB:30:89
 SHA256:
7E:37:CB:8B:4C:47:09:0C:AB:36:55:1B:A6:F4:5D:B8:40:68:0F:BA:16:6A:95:2D:B1:00:71:7F:43:05:3F:C2
Signature algorithm name: SHA384withECDSA
Subject Public Key Algorithm: 384-bit EC key
Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
```

```
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_CertSign
  Crl_Sign
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: CB D0 BD A9 E1 98 05 51   A1 4D 37 A2 83 79 CE 8D  .......Q.M7..y..
0010: 1D 2A E4 84                                        .*..
]
]


......



..\..\bin\keytool.exe -list -keystore cacerts -storepass changeit -alias somewebserver -v
Alias name: somewebserver
Creation date: Jul 17, 2019
Entry type: trustedCertEntry

Owner: CN=......
```