CVP(Customer Voice Portal)용 SHA(Secure Hash Algorithm) 256

목차

소개

이 문서에서는 CVP와 함께 SHA256을 사용하는 절차에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- CVP
- 인증서

사용되는 구성 요소

이 문서의 정보는 CVP 10.5를 기반으로 합니다.

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

배경 정보

2016년 1월부터 모든 브라우저에서 SHA1 서명 인증서를 거부했습니다. SHA1에서 SHA256으로 이동하지 않는 한 요청된 서비스가 올바르게 렌더링되지 않았습니다.

폭발적인 연산 능력뿐만 아니라 연산 알고리즘의 최근 발전에 따라, SHA1은 나날이 약해지고 있다.

이는 SHA1의 근본적인 열화 충돌 저항 및 궁극적인 폐기로 이어졌다.

구성

CVP Operations Console(OAMP) 간 인증서 교환 절차:

OAMP

1단계. OAMP 인증서 내보내기

c:\Cisco\CVP\jre\bin\keytool.exe -export -v -keystore .keystore -storetype JCEKS -alias oamp_certificate -file oamp_security_76.cer

2단계. OAMP 인증서를 Callserver에 복사하고 가져옵니다.

c:\Cisco\CVP\jre\bin\keytool.exe -import -trustcacerts -keystore .keystore -storetype JCEKS -alias orm_oamp_certificate -file oamp_security_76.cer

통화 중 서버

1단계. CALLSERVER 인증서 내보내기

c:\Cisco\CVP\jre\bin\keytool.exe -export -v -keystore .ormkeystore -storetype JCEKS -alias orm_certificate -file orm_security_108.cer

2단계. CALLSERVER 인증서를 OAMP에 복사하고 가져옵니다.

c:\Cisco\CVP\jre\bin\keytool.exe -import -trustcacerts -keystore .keystore -storetype JCEKS -alias oamp_orm_certificate -file orm_security_108.cer

3단계. Call Server 키 저장소에서 양식 인증서를 내보냅니다.

C:\Cisco\CVP\conf\security>c:\Cisco\CVP\jre\bin\keytool.exe -import -trustcacerts -keystore .keystore -storetype JCEKS -alias vxml_orm_certificate -file orm_security_108.cer

다음을 확인합니다.

구성 요소 간에 보안 통신이 설정되었는지 확인할 수 있습니다. OAMP Page > Device management > <managed server> > Statistics로 이동합니다.

통계를 표시해야 합니다.

보안이 제대로 설정된 경우 JConsole을 사용하여 연결을 설정할 수 있습니다.

1단계. OAMP의 c: \Cisco\CVP\conf\orm_jmx.conf은 다음과 같습니다.

```
javax.net.debug = all
```

```
com.sun.management.jmxremote.ssl.need.client.auth = false
com.sun.management.jmxremote.authenticate = false
com.sun.management.jmxremote.port = 2099
com.sun.management.jmxremote.ssl = true
javax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.ormkeystore
javax.net.ssl.keyStorePassword=<local security password>
```

2단계. 명령에서 jconsole을 엽니다. 다음 명령을 사용하여:

C:\Cisco\CVP\jre\bin>jconsole.exe -J-Djavax.net.ssl.trustStore=C:\Cisco\CVP\conf\security\.keystore -J-Djavax.net.ssl.trustStorePassword=<oamp 보안 비밀번호/jconsole client> -J-Djavax.net.ssl.keyStore=C:\Cisco\CVP\conf\security\.keystore -J-Djavax.net.ssl.keyStorePassword=<oamp 보안 비밀번호/jconsole client> -J-Djavax.net.ssl.keyStoreType=JCEKS -debug -J-Djavax.netxxx.xxxxxx.ssl.trustStoreType=JCEKS

<managed server ip>:<secure jmx port eg:2099>의 키(Remote Process 필드).

참고: JConsole은 애플리케이션이 보안 방법을 우회하도록 묻는 메시지 없이 연결해야 합니다.

3단계. jconsole 연결이 호출되는 동안 Wireshark. 캡처는 보안 핸드셰이크를 수행하는 동안 협상된 세부 정보에 대한 통찰력을 제공합니다.

JMX의 추적

JMX의 구현에서는 java.util.logging을 사용하여 디버그 추적을 기록합니다. 이러한 흔적들 중 다수는 내부 미공개 클래스에 대한 관심사지만, 이러한 흔적들은 응용 프로그램의 진행 상황을 이해하는 데 도움이 될 수 있습니다.

JMX 구현에는 두 가지 로거 세트가 있습니다.

- **`javax.management.\*`**: jmx API와 관련된 모든 로거
- **`javax.management.remote.\*`**: 특히 JMX Remote API와 관련된 로거

여기서 JMX 로거에 대한 보다 자세한 설명을 확인할 수 있습니다.

두 가지 방법으로 JMX 추적을 활성화할 수 있습니다.

- 정적으로, logging.properties 파일 사용
- JMXTracing MBean을 사용하면 동적으로 작업할 수 있습니다. Java SE 6에서는 JMX 커넥터가 명령줄에서 활성화되지 않은 경우에도 애플리케이션에 대해 이 작업을 수행할 수 있습니다.

logging.properties 파일 사용

다음 플래그로 응용 프로그램을 시작합니다.

```
java -Djava.util.logging.config.file=<logging.properties> ....
```

여기서 logging.properties는 JMX 로거에 대한 추적을 활성화합니다.

```
handlers= java.util.logging.ConsoleHandler
.level=INFO

java.util.logging.FileHandler.pattern = %h/java%u.log
java.util.logging.FileHandler.limit = 50000
java.util.logging.FileHandler.count = 1
java.util.logging.FileHandler.formatter = java.util.logging.XMLFormatter

java.util.logging.ConsoleHandler.level = FINEST
java.util.logging.ConsoleHandler.formatter = java.util.logging.SimpleFormatter

// Use FINER or FINEST for javax.management.remote.level - FINEST is
// very verbose...
//
javax.management.level=FINEST
javax.management.remote.level=FINER
```

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.