CCCSP v15 CCSP 노드를 SSM에 연결

목차

문제

CCSP 노드를 SSM에 연결하려고 시도할 때 사용자에게 인증서 신뢰 문제가 발생할 수 있으며, 이로 인해 스마트 라이센싱 등록이 실패할 수 있습니다. 이는 Cisco Bug ID CSCwv41814과 관련이 있습니다. 여기서 Java 인증서 저장소는 SSM 인증서 체인을 신뢰하기 위해 수동 업데이트를 필요로 합니다.

환경

- Cisco CCCSP(Contact Center Solution Platform) 버전 15(이전의 CUSP)
- SSM(Smart Software Manager) 연결 필요
- 인증서 파일 전송을 위한 SFTP 서버

해결

SSM 인증서 신뢰 문제 해결(CSCwv41814)

SSM에 연결할 때 인증서 신뢰 문제가 발생하면 다음 단계에 따라 Java 인증서 저장소 문제를 해결합니다.

1단계: 원격 계정 액세스 사용:

```
utils remote_account enable
```

2단계: 문제 해결을 위한 원격 계정 만들기:

```
utils remote_account create ciscotac 2
```

3단계: Java 보안 디렉토리로 이동합니다.

```
cd $JAVA_HOME/jre/lib/security
```

4단계: SFTP를 통해 SSM 루트 및 중간 인증서를 CCCSP 시스템으로 전송합니다.

```
sftp root@X.X.X.X
sftp> get sub-root.cer
sftp> get SSM-Root.cer
sftp> exit

# Check if the certificates are there.

[root@hostname security]# ls -ltr
-rw-r--r--. 1 root root  56050 Aug 17 15:55 java.security
-rw-------. 1 root root   2031 Sep  8 13:43 sub-root.cer
-rw-------. 1 root root   1396 Sep  8 13:43 SSM-Root.cer
```

5단계: 루트 인증서를 Java 키 저장소로 가져옵니다.

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias SSM-Root -keystore $JAVA_HOME/jre/lib/security/cac
```

6단계: 중간 인증서를 Java 키 저장소로 가져옵니다.

```
$JAVA_HOME/bin/keytool -storetype JKS -import -alias sub-root -keystore $JAVA_HOME/jre/lib/security/cac
```

7단계: CCCSP 시스템을 재부팅하여 변경 사항을 적용합니다.

원인

네이티브 crypto key certreq 명령이 SAN 항목을 CSR에 추가하는 문서화된 방법을 제공하지 않기 때문에 CCCSP v15 CLI 제한이 있습니다. CCCSP v15는 SAN이 인증서에 있을 때 TLS 피어 확인에 SAN을 사용합니다. 그렇지 않으면 인증서 CN(Common Name)이 확인에 사용됩니다. SSM 연결 문제는 Cisco 버그 ID CSCwv41814에 의해 발생합니다. CCSP의 Java 인증서 저장소가 SSM 인증서 체인을 자동으로 신뢰하지 않으므로 루트 및 중간 인증서를 수동으로 가져와야 합니다.

관련 콘텐츠

- CCCSP 15.0.1 CLI 컨피그레이션 가이드 - 서명된 인증서 생성 및 가져오기
- Cisco 기술 지원 및 다운로드

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.