CCSP v15 Verbinden von CCSP-Knoten mit SSM

Inhalt

Problem

Beim Versuch, CCSP-Knoten mit SSM zu verbinden, können Benutzer auf Probleme mit der Zertifikatsvertrauensstellung stoßen, die eine erfolgreiche Smart Licensing-Registrierung verhindern können. Dies bezieht sich auf die Cisco Bug-ID CSCwv41814, bei der für den Java-Zertifikatspeicher manuelle Updates erforderlich sind, um der SSM-Zertifikatkette zu vertrauen.

Umwelt

- Cisco Contact Center Solution Platform (CCSP) Version 15 (ehemals CUSP)
- Smart Software Manager (SSM)-Verbindung erforderlich
- SFTP-Server für die Übertragung von Zertifikatsdateien

Auflösung

Problemlösung bei der SSM-Zertifikatvertrauensstellung (CSCwv41814)

Wenn bei der Verbindung mit SSM Zertifikatvertrauensprobleme auftreten, befolgen Sie diese Schritte, um das Problem mit dem Java-Zertifikatspeicher zu beheben.

Schritt 1: Remote-Kontozugriff aktivieren:

```
utils remote_account enable
```

Phase 2: Remote-Konto für die Fehlerbehebung erstellen:

```
utils remote_account create ciscotac 2
```

Schritt 3: Navigieren Sie zum Java-Sicherheitsverzeichnis:

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

Schritt 4: Übertragen Sie die SSM-Root- und Zwischenzertifikate über SFTP an das CCSP-System:

```
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
```

Schritt 5: Importieren Sie das Stammzertifikat in den Java-Schlüsselspeicher:

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

Schritt 6: Zwischenzertifikat in den Java-Schlüsselspeicher importieren:

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

Schritt 7: Starten Sie das CCSP-System neu, um die Änderungen zu übernehmen.

Ursache

Die CLI-Einschränkung in CCSP v15 liegt vor, da der Befehl certreq für den nativen Kryptografieschlüssel keine dokumentierte Methode zum Hinzufügen von SAN-Einträgen zu einem CSR bietet. CCCSP v15 verwendet SAN für TLS-Peer-Verifizierung, wenn SAN im Zertifikat vorhanden ist. Andernfalls wird der Common Name (CN) des Zertifikats für die Überprüfung verwendet. Das SSM-Verbindungsproblem wird durch die Cisco Bug-ID CSCwv41814 verursacht, bei der der Java-Zertifikatspeicher auf dem CCSP nicht automatisch der SSM-Zertifikatkette vertraut, sodass das Root- und Zwischenzertifikat manuell importiert werden müssen.

Verwandte Inhalte

- CCSP 15.0.1 CLI-Konfigurationsanleitung - Erstellen und Importieren eines signierten Zertifikats
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.