CCCSP v15 Connexion des noeuds CCCSP à SSM

Table des matières

Problème

Lors de la tentative de connexion des noeuds CCCSP à SSM, les utilisateurs peuvent rencontrer des problèmes d'approbation de certificat, ce qui peut empêcher l'enregistrement réussi de la licence Smart. Ceci est lié à l'ID de bogue Cisco CSCwv41814, où le magasin de certificats Java nécessite des mises à jour manuelles pour faire confiance à la chaîne de certificats SSM.

Environnement

- Cisco Contact Center Solution Platform (CCCSP) version 15 (anciennement CUSP)
- Connectivité SSM (Smart Software Manager) requise
- Serveur SFTP pour les transferts de fichiers de certificats

Résolution

Résolution des problèmes d'approbation de certificat SSM (CSCwv41814)

Si vous rencontrez des problèmes d'approbation de certificat lors de la connexion à SSM, procédez comme suit pour résoudre le problème du magasin de certificats Java.

Étape 1: Activer l'accès au compte distant :

```
utils remote_account enable
```

Étape 2: Créer un compte distant pour le dépannage :

```
utils remote_account create ciscotac 2
```

Étape 3: Accédez au répertoire de sécurité Java :

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

Étape 4: Transférez les certificats SSM racine et intermédiaires vers le système CCCSP via SFTP :

```
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
```

Étape 5: Importez le certificat racine dans le keystore Java :

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

Étape 6: Importez le certificat intermédiaire dans le keystore Java :

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

Étape 7: Redémarrez le système CSP pour appliquer les modifications.

Motif

La limitation CLI CCCSP v15 existe parce que la commande certreq de clé de chiffrement native ne fournit pas de méthode documentée pour ajouter des entrées SAN dans un CSR. CCCSP v15 utilise le SAN pour la vérification TLS par homologue lorsque le SAN est présent dans le certificat ; sinon, le certificat Nom commun (CN) est utilisé à des fins de vérification. Le problème de connectivité SSM est causé par le bogue Cisco ayant l'ID CSCwv41814, où le magasin de certificats Java sur CCCSP ne fait pas automatiquement confiance à la chaîne de certificats SSM, ce qui nécessite l'importation manuelle des certificats racine et intermédiaire.

Autres informations utiles

- CCCSP 15.0.1 Guide de configuration CLI - Création et importation d'un certificat signé
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.