CCCSP v15 - Connessione dei nodi CCSP a SSM

Sommario

Problema

Quando si tenta di connettere nodi CCCSP a SSM, gli utenti possono riscontrare problemi di attendibilità del certificato che possono impedire la corretta registrazione delle licenze smart. Questo problema è correlato all'ID bug Cisco CSCwv41814, dove l'archivio certificati Java richiede aggiornamenti manuali per considerare attendibile la catena di certificati SSM.

Ambiente

- Cisco Contact Center Solution Platform (CCSP) versione 15 (in precedenza CUSP)
- Connettività Smart Software Manager (SSM) richiesta
- Server SFTP per i trasferimenti di file di certificato

Risoluzione

Risoluzione dei problemi relativi all'attendibilità dei certificati SSM (CSCwv41814)

Se si verificano problemi di attendibilità del certificato durante la connessione a SSM, eseguire la procedura seguente per risolvere il problema dell'archivio certificati Java.

Passaggio 1: Abilita accesso account remoto:

```
utils remote_account enable
```

Passaggio 2: Crea account remoto per la risoluzione dei problemi:

```
utils remote_account create ciscotac 2
```

Passaggio 3: Passare alla directory Java Security:

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

Passaggio 4: Trasferire i certificati radice e intermedi SSM al sistema CCCSP tramite 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
```

Passaggio 5: Importare il certificato radice nel keystore Java:

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

Passaggio 6: Importare il certificato intermedio nel keystore Java:

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

Passaggio 7: Riavviare il sistema CCSP per applicare le modifiche.

Causa

Il limite CLI di CCCSP v15 esiste perché il comando crypto key nativo certreq non fornisce un metodo documentato per aggiungere voci SAN a un CSR. CCCSP v15 utilizza SAN per la verifica peer TLS quando nel certificato è presente una SAN; in caso contrario, per la verifica viene utilizzato il nome comune (CN) del certificato. Il problema di connettività SSM è causato da Cisco Bug ID CSCwv41814, in cui l'archivio certificati Java su CCCSP non considera automaticamente attendibile la catena di certificati SSM, richiedendo l'importazione manuale dei certificati radice e intermedi.

Contenuto correlato

- Guida alla configurazione della CLI di CCCSP 15.0.1 - Creazione e importazione di un certificato firmato
- Supporto tecnico Cisco e download

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).