CCCSP v15 SSMへのCCCSPノードの接続

内容

問題

CCCSPノードをSSMに接続しようとすると、証明書の信頼に関する問題が発生し、スマートライセンスの登録が失敗する可能性があります。これは、Cisco Bug ID CSCwv41814に関連しています。このバグでは、Java証明書ストアがSSM証明書チェーンを信頼するために手動アップデートを必要とします。

環境

- Cisco Contact Center Solution Platform(CCCSP)バージョン15（旧称CUSP）
- Smart Software Manager(SSM)への接続が必要
- 証明書ファイル転送用のSFTPサーバ

解決方法

SSM証明書信頼の問題の解決(CSCwv41814)

SSMへの接続時に証明書信頼の問題が発生した場合は、次の手順に従ってJava証明書ストアの問題を解決します。

ステップ1：リモートアカウントアクセスを有効にします。

```
utils remote_account enable
```

ステップ2：トラブルシューティング用のリモートアカウントを作成します。

```
utils remote_account create ciscotac 2
```

ステップ3: Javaセキュリティディレクトリに移動します。

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

ステップ4:SSMルート証明書および中間証明書をSFTP経由でCCCSPシステムに転送します。

```
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
```

ステップ5：ルート証明書をJavaキーストアにインポートします。

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

ステップ6：中間証明書をJavaキーストアにインポートします。

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

ステップ7:CCCSPシステムを再起動して変更を適用します。

原因

CCCSP v15 CLIの制限が存在するのは、native crypto key certreqコマンドが、CSRにSANエントリを追加するための文書化された方法を提供しないためです。CCCSP v15では、SANが証明書に存在する場合、TLSピアの検証にSANを使用します。それ以外の場合は、証明書の共通名(CN)が検証に使用されます。SSM接続の問題は、Cisco Bug ID CSCwv41814が原因で発生します。このバグIDでは、CCCSP上のJava証明書ストアがSSM証明書チェーンを自動的に信頼しないため、ルート証明書と中間証明書の手動インポートが必要になります。

関連コンテンツ

- CCCSP 15.0.1 CLIコンフィギュレーションガイド – 署名付き証明書の作成およびインポート
- シスコのテクニカルサポートとダウンロード

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。