CCCSP v15将CCCSP节点连接到SSM

目录

问题

尝试将CCCSP节点连接到SSM时，用户可能会遇到证书信任问题，这会阻止智能许可注册成功。这与Cisco Bug ID CSCwv41814相关，其中Java证书存储需要手动更新以信任SSM证书链。

环境

- 思科联系中心解决方案平台(CCCSP)版本15（以前称为CUSP）
- 需要智能软件管理器(SSM)连接
- 用于证书文件传输的SFTP服务器

分辨率

SSM证书信任问题解决方案(CSCwv41814)

如果在连接到SSM时遇到证书信任问题，请按照以下步骤解决Java证书存储问题。

步骤 1：启用远程帐户访问：

```
utils remote_account enable
```

步骤 2：创建远程帐户进行故障排除：

```
utils remote_account create ciscotac 2
```

步骤 3：导航到Java安全目录：

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

步骤 4：通过SFTP将SSM根证书和中间证书传输到CCCSP系统：

```
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
```

步骤 5：将根证书导入Java密钥库：

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

步骤 6：将中间证书导入Java密钥库：

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

步骤 7：重新启动CCCSP系统以应用更改。

原因

CCCSP v15 CLI限制之所以存在，是因为本机crypto key certreq命令未提供将SAN条目添加到

CSR的书面方法。当证书中存在SAN时，CCCSP v15使用SAN进行TLS对等验证；否则，将使用证书公用名(CN)进行验证。SSM连接问题由Cisco Bug ID CSCwv41814引起，其中CCCSP上的Java证书存储不会自动信任SSM证书链，需要手动导入根证书和中间证书。

相关内容

- CCCSP 15.0.1 CLI配置指南 — 创建和导入签名证书
- 思科技术支持和下载

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。