CCCSP v15 Conexión de nodos CCCSP a SSM

Contenido

Problema

Al intentar conectar nodos CCCSP a SSM, los usuarios pueden encontrar problemas de confianza de certificados, que pueden impedir el registro correcto de licencias inteligentes. Esto está relacionado con el ID de bug de Cisco CSCwv41814, donde el almacén de certificados de Java requiere actualizaciones manuales para confiar en la cadena de certificados SSM.

Entorno

- Cisco Contact Center Solution Platform (CCCSP) versión 15 (anteriormente conocido como CUSP)
- Se requiere conectividad con Smart Software Manager (SSM)
- Servidor SFTP para transferencias de archivos de certificados

Resolución

Resolución de problemas de confianza de certificados SSM (CSCwv41814)

Si encuentra problemas de confianza de certificados al conectarse a SSM, siga estos pasos para resolver el problema del almacén de certificados de Java.

Paso 1: Habilitar acceso de cuenta remota:

```
utils remote_account enable
```

Paso 2: Crear cuenta remota para la solución de problemas:

```
utils remote_account create ciscotac 2
```

Paso 3: Navegue hasta el directorio de seguridad de Java:

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

Paso 4: Transfiera la raíz SSM y los certificados intermedios al sistema CCCSP a través de 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
```

Paso 5: Importe el certificado raíz en el almacén de claves Java:

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

Paso 6: Importe el certificado intermedio en el almacén de claves Java:

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

Paso 7: Reinicie el sistema CCCSP para aplicar los cambios.

Causa

La limitación de CLI de CCCSP v15 existe porque el comando nativo crypto key certreq no proporciona un método documentado para agregar entradas SAN a una CSR. CCCSP v15 utiliza SAN para la verificación de pares TLS cuando SAN está presente en el certificado; de lo contrario, se utilizará el certificado de nombre común (NC) para la verificación. El problema de conectividad SSM es causado por el Id. de bug Cisco CSCwv41814, donde el almacén de certificados Java en CCCSP no confía automáticamente en la cadena de certificados SSM, lo que requiere la importación manual de los certificados raíz e intermedios.

Contenido relacionado

- Guía de configuración de CLI de CCCSP 15.0.1: creación e importación de un certificado firmado
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).