Procedimiento de importación de certificados CSSM de licencia inteligente de CVP

Contenido

Problema

CVP Call Server está experimentando errores de "verificación de firma" de licencias inteligentes en los registros de SmartAgent. El sistema requiere que se importe el certificado CSSM (Cisco Smart Software Manager) en el almacén de claves de CVP para resolver los fallos de verificación de firmas durante los procesos normales de actualización del estado de las licencias. Sin la cadena de certificados CSSM adecuada, CVP no puede validar las transacciones de licencias con Cisco Smart Software Manager, lo que da lugar a problemas de cumplimiento de licencias.

Entorno

- Cisco Customer Voice Portal (CVP) Call Server versión 12.6.2
- Software de Contact Center: Packaged Contact Center Enterprise (PCCE)
- Servicios de CVP: Servidor de llamadas, WSM (Administrador de servicios web), servidor VXML
- Formato de almacén de claves Java JCEKS para administración de certificados
- Integración de Smart Licensing con Cisco Smart Software Manager (CSSM)

Resolución

Siga estos pasos detallados para importar el certificado CSSM en el almacén de claves del servidor de llamadas de CVP.

Paso 1: Identificar contraseña del almacén de claves

Abra una ventana de comandos como administrador y navegue hasta el directorio principal de CVP para descifrar la contraseña del almacén de claves:

```
cd %CVP_HOME%\bin
DecryptKeystoreUtil.bat
```

Registre la contraseña mostrada por esta utilidad tal como se requiere para todos los comandos keytool subsiguientes.

Paso 2: Almacén de claves actual de copia de seguridad

Cree una copia de seguridad del almacén de claves existente desde el directorio de seguridad:

```
cd %CVP_HOME%\conf\security
copy .keystore backup.keystore
```

Paso 3: Exportar contenido actual del almacén de claves

Genere una lista de todos los certificados actuales en el almacén de claves como referencia:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp.tx
```

Revise el archivo generado para comprender el inventario de certificados actual.

Paso 4: Descargar certificados CSSM

Obtenga la cadena de certificados CSSM necesaria en la URL de transporte de la página Licencias de CVP. Los requisitos del certificado dependen del tipo de certificado:

Para certificados firmados por CA: Descargue los certificados raíz e intermedio individualmente en formato .cer

Para certificados autofirmados: Descargue el certificado CSSM directamente

Guarde los archivos del certificado en el directorio de seguridad de CVP:

```
%CVP_HOME%\conf\security
```

Paso 5: Importar certificado raíz CSSM (firmado por CA)

Para certificados firmados por CA, importe primero el certificado raíz:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Paso 6: Importar certificado intermedio CSSM (firmado por CA)

Si existe un certificado intermedio, impórtelo utilizando este comando:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Paso 7: Importar certificado CSSM de firma automática (alternativo)

Para los certificados autofirmados, importe el certificado CSSM directamente:

```
"%CVP_HOME%\jre\bin\keytool.exe" -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" -impor
```

Paso 8: Verificar importación de certificados

Confirme que los nuevos certificados estén presentes en el almacén de claves:

```
cd %CVP_HOME%\jre\bin
keytool -list -v -storetype JCEKS -keystore "%CVP_HOME%\conf\security\.keystore" > C:\temp\certs_cvp_ne
```

Revise la nueva lista de certificados para comprobar que los certificados CSSM se han importado correctamente.

Paso 9: Reinicio y verificación del servicio

Reinicie el servidor CVP y registre el tiempo de reinicio. Después del reinicio, confirme que se han iniciado todos los servicios de CVP:

- Servidor de llamadas
- WSM (Administrador de servicios web)
- Servidor VXML

Espere aproximadamente 20 minutos después del inicio del servicio antes de continuar con la validación.

Paso 10: Validar resolución

Realice estos pasos de validación:

Comprobar registros de SmartAgent:

Navegue hasta C:\Cisco\CVP\logs\WSM y ordene por Fecha de modificación. Examine los informes de estado de 15 minutos más recientes en los registros de SmartAgent. La excepción de

verificación de firma ya no debe aparecer después de la hora de reinicio.

Verificar estado de licencia:

Acceda a la página de licencias de CVP y confirme que el sistema muestra el estado "registrado" y "en cumplimiento" sin errores.

Procedimiento de reversión (si se producen problemas)

Si se encuentran problemas durante el proceso de importación de certificados, siga estos pasos de reversión:

Paso 1: Detención de todos los servicios de CVP (Call Server, WSM, VXML)

Paso 2: Vaya al directorio de seguridad:

```
cd %CVP_HOME%\conf\security
```

Paso 3: Eliminar el almacén de claves modificado:

```
del .keystore
```

Paso 4: Restaure el almacén de claves de copia de seguridad:

```
rename backup.keystore .keystore
```

Paso 5: Reinicie todos los servicios de CVP

Causa

El almacén de claves del servidor de llamadas de CVP no contiene la cadena de certificados CSSM necesaria para validar las firmas digitales de Cisco Smart Software Manager. Durante las operaciones de licencias inteligentes, CVP intenta verificar la autenticidad de las comunicaciones de licencias mediante la validación de firmas basada en certificados. Sin los certificados CSSM adecuados en el almacén de claves Java JCEKS, estos intentos de verificación de firmas fallan, lo que provoca errores en las transacciones de licencias y posibles problemas de cumplimiento.

Contenido relacionado

- 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).