Procedimento de importação de certificado CSSM de licença inteligente do CVP

Contents

Problema

O Servidor de Chamadas do CVP está experimentando erros de "verificação de assinatura" de licenciamento inteligente nos logs do SmartAgent. O sistema requer que o certificado CSSM (Cisco Smart Software Manager) seja importado para o armazenamento de chaves do CVP para resolver falhas de verificação de assinatura durante processos normais de atualização de status de licenciamento. Sem a cadeia de certificados CSSM apropriada, o CVP não pode validar transações de licenciamento com o Cisco Smart Software Manager, resultando em problemas de conformidade de licenciamento.

Ambiente

- Cisco Customer Voice Portal (CVP) Call Server versão 12.6.2
- Software de central de atendimento - Packaged Contact Center Enterprise (PCCE)
- Serviços CVP: Servidor de chamadas, WSM (Web Service Manager), servidor VXML
- Formato de armazenamento de chaves Java JCEKS para gerenciamento de certificados
- Integração do Smart Licensing com o Cisco Smart Software Manager (CSSM)

Resolução

Siga estas etapas detalhadas para importar o certificado CSSM para o armazenamento de chaves do servidor de chamadas do CVP.

Passo 1: Identificar senha do armazenamento de chaves

Abra uma janela de comando como administrador e navegue até o diretório inicial do CVP para descriptografar a senha do armazenamento de chaves:

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

Registre a senha exibida por este utilitário conforme necessário para todos os comandos keytool subsequentes.

Passo 2: Fazer Backup do Repositório de Chaves Atual

Crie um backup do armazenamento de chaves existente a partir do diretório de segurança:

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

Passo 3: Exportar Conteúdo do Repositório de Chaves Atual

Gere uma lista de todos os certificados atuais no armazenamento de chaves para referência:

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

Revise o arquivo gerado para entender o inventário de certificados atual.

Passo 4: Fazer download de certificados CSSM

Obtenha a cadeia de certificados CSSM necessária na URL de transporte na página de licenciamento do CVP. Os requisitos de certificado dependem do tipo de certificado:

Para certificados assinados por CA: Fazer download dos certificados Raiz e Intermediário individualmente no formato .cer

Para certificados autoassinados: Faça o download do certificado CSSM diretamente

Salve os arquivos de certificado no diretório de segurança do CVP:

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

Passo 5: Importar certificado raiz CSSM (assinado por CA)

Para certificados assinados por CA, importe primeiro o certificado raiz:

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

Passo 6: Importar certificado intermediário CSSM (CA-signed)

Se existir um certificado intermediário, importe-o usando este comando:

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

Passo 7: Importar certificado CSSM autoassinado (alternativo)

Para certificados autoassinados, importe o certificado CSSM diretamente:

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

Passo 8: Verificar Importação de Certificado

Confirme se os novos certificados estão presentes no armazenamento de chaves:

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

Revise a nova lista de certificados para verificar se os certificados CSSM foram importados com êxito.

Etapa 9: Verificação de reinicialização e serviço

Reinicialize o servidor CVP e registre o tempo de reinicialização. Após a reinicialização, confirme se todos os serviços do CVP foram iniciados:

- Servidor de chamadas
- WSM (Gerenciador de serviços da Web)
- Servidor VXML

Aguarde aproximadamente 20 minutos após a inicialização do serviço antes de continuar com a validação.

Etapa 10: Validar Resolução

Execute estas etapas de validação:

Verificar Logs do SmartAgent:

Navegue até C:\Cisco\CVP\logs\WSM e classifique por Data de modificação. Examine os relatórios de status de 15 minutos mais recentes nos logs do SmartAgent. A exceção de

verificação de assinatura não deve mais aparecer após o tempo de reinicialização.

Verificar status do licenciamento:

Acesse a página de licenciamento do CVP e confirme se o sistema mostra o status "registrado" e "em conformidade" sem erros.

Procedimento de reversão (se ocorrerem problemas)

Se forem encontrados problemas durante o processo de importação de certificados, siga estas etapas de reversão:

Passo 1: Interromper todos os serviços CVP (Servidor de chamadas, WSM, VXML)

Passo 2: Navegue até o diretório de segurança:

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

Passo 3: Exclua o armazenamento de chaves modificado:

```
del .keystore
```

Passo 4: Restaurar o armazenamento de chaves de backup:

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

Passo 5: Reiniciar todos os serviços do CVP

Causa

O armazenamento de chaves do servidor de chamadas do CVP não contém a cadeia de certificados CSSM necessária para validar assinaturas digitais do Cisco Smart Software Manager. Durante as operações de licenciamento inteligente, o CVP tenta verificar a autenticidade das comunicações de licenciamento usando a validação de assinatura baseada em certificado. Sem os certificados CSSM apropriados no armazenamento de chaves Java JCEKS, essas tentativas de verificação de assinatura falham, resultando em erros de transação de licenciamento e possíveis problemas de conformidade.

Conteúdo relacionado

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.