CCCSP v15 Conexão de nós CCCSP ao SSM

Contents

Problema

Ao tentar conectar nós CCCSP ao SSM, os usuários podem encontrar problemas de confiança de certificado, o que pode impedir o registro bem-sucedido do Smart Licensing. Isso está relacionado ao bug da Cisco ID CSCwv41814, em que o armazenamento de certificados Java requer atualizações manuais para confiar na cadeia de certificados SSM.

Ambiente

- Cisco Contact Center Solution Platform (CCCSP) versão 15 (anteriormente conhecido como CUSP)
- Conectividade necessária do Smart Software Manager (SSM)
- Servidor SFTP para transferências de arquivos de certificados

Resolução

Resolução de Problemas de Confiança de Certificado SSM (CSCwv41814)

Se encontrar problemas de confiança de certificado ao conectar-se ao SSM, siga estas etapas para resolver o problema do armazenamento de certificados Java.

Passo 1: Habilitar acesso remoto à conta:

```
utils remote_account enable
```

Passo 2: Criar conta remota para solução de problemas:

```
utils remote_account create ciscotac 2
```

Passo 3: Navegue até o diretório de segurança Java:

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

Passo 4: Transferir a raiz SSM e os certificados intermediários para o sistema CCCSP via 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
```

Passo 5: Importe o certificado raiz para o armazenamento de chaves Java:

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

Passo 6: Importe o certificado intermediário para o armazenamento de chaves Java:

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

Passo 7: Reinicialize o sistema CCCSP para aplicar as alterações.

Causa

A limitação do CCCSP v15 CLI existe porque o comando nativo crypto key certreq não fornece um método documentado para adicionar entradas SAN em um CSR. O CCCSP v15 usa a SAN para verificação de pares TLS quando a SAN está presente no certificado; caso contrário, o certificado Nome comum (CN) é usado para verificação. O problema de conectividade do SSM é causado pela ID de bug Cisco CSCwv41814, em que o armazenamento de certificados Java no CCCSP não confia automaticamente na cadeia de certificados SSM, exigindo a importação manual da raiz e dos certificados intermediários.

Conteúdo relacionado

- Guia de configuração da CLI do CCCSP 15.0.1 - Criar e importar um certificado assinado
- 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.