NAC (CCA): Como fixar erros do certificado no CAM/CAS após a elevação a 4.1.6

Índice

Introdução
Pré-requisitos
Requisitos
Componentes Utilizados
Convenções
Procedimento
Informações Relacionadas

Introdução

Este documento descreve como fixar erros do certificado no servidor de acesso limpo do Access Manager (CAM) /Clean (CAS) com versão 4.1.6.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento do processo de upgrade para o dispositivo do Cisco Network Admission Control (NAC).

Componentes Utilizados

A informação neste documento é baseada na versão 4.1.6 da ferramenta NAC de Cisco com CAM/CAS.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

Procedimento

Estes erros do certificado são encontrados em */perfigo/logs/perfigo-redirect.log0.log.0* ou em */perfigo/logs/perfigo-log0.log.0*.

Está aqui um exemplo de um erro do certificado:

```
SEVERE: RMISocketFactory:Creating RMI socket failed to host
        10.1.20.10:sun.security.validator.ValidatorException:
        Certificate chaining error
Aug 1, 2008 1:41:22 PM com.perfigo.wlan.web.admin.ConnectorClient connect
SEVERE: Communication Exception : java.rmi.ConnectIOException: Exception
        creating connection to: 10.1.20.10; nested exception is:
 javax.net.ssl.SSLHandshakeException:
        sun.security.validator.ValidatorException: Certificate chaining error
```

Estes erros são um resultado dos aprimoramentos de segurança feitos em 4.1.6. Em 4.1.6, CAS e o CAM atuam como o cliente e servidor entre si e devem confiar-se. Cada um exige os Certificados da raiz e do intermediário dos outro. Por exemplo, se CAS tem um certificado Verisign e o CAM têm um certificado (provisório) do perfigo, a necessidade de CAS e CAM a corrente de Verisign (raiz e intermediários) e a raiz do perfigo.

Termine estas etapas a fim fixar os erros do certificado:

1. Suporte todos os Certificados instalados que não forem Certificados provisórios.No CAM, abra a interface da WEB, e vá à **administração > ao gerente CCA > ao certificado SSL > X509**.Em CAS, vá diretamente à interface da WEB através de https:// <CAS IP>/admin, e vá então à **administração > ao certificado SSL > X509**.Escolha a **chave/certificado da exportação CSR/Private da** escolha uma lista de drop-down da ação.Clique a **exportação** situada ao lado do certificado atualmente instalado, e salvar este arquivo.Clique a **exportação** situada ao lado da chave privada atualmente instalada, e salvar este arquivo.
2. Após o backup, se CAS e o CAM já não usam Certificados provisórios, gerencia-os.No CAM, abra a interface da WEB, e vá à **administração > ao gerente CCA > ao certificado SSL > X509**.Em CAS, vá diretamente à interface da WEB através de https:// <CAS IP>/admin, e vá então à **administração > ao certificado SSL > X509**.Escolha **gerenciem o certificado provisório da** lista de drop-down.Complete os campos alistados, e o clique **gerencie**.**Nota:** Isto já não exige uma repartição tomar o efeito.
3. Remova todas as autoridades do certificado confiável de CAS e do CAM. Esta etapa facilita controlar e melhorar a Segurança.No CAM, vá à **administração > ao gerente CCA > ao SSL > às autoridades do certificado confiável**.Em CAS, vá à **administração > ao SSL > às autoridades do certificado confiável**.Crie um filtro para excluir o certificado do perfigo.Escolha o **nome destacado da** lista de drop-down do filtro adicionar.Escolha **contém não da** lista de drop-down que aparece ao lado do nome destacado.Datilografe o perfigo no campo de texto, e clique então o **filtro**.Escolha 100 da lista de drop-down situada ao lado do botão selecionado supressão.Clique a caixa de verificação abaixo da lista de drop-down selecionada supressão a fim selecionar todas as autoridades de certificação (CA) na lista.Clique a **supressão selecionada** a fim suprimir de todos os CA na lista.Continue a clicar a caixa, e clique a **supressão selecionada** até que todos os CA estejam suprimidos.
4. Depois que você remove todos os CA, os Certificados da raiz e do intermediário devem ser importados.No CAM, vá à **administração > ao gerente CCA > ao SSL > às autoridades do certificado confiável**.Em CAS, vá à **administração > ao SSL > às autoridades do certificado confiável**.O clique **consulta**, e escolhe o certificado de raiz primeiramente.**Nota:** O assunto e o expedidor devem ser ajustados ao mesmo valor.Clique a **importação**, e CA deve aparecer na lista abaixo.Execute o mesmo procedimento para todos os Certificados intermediários.

5. Instale os Certificados de CAS e CAM que você suportou na primeira etapa.No CAM, abra a interface da WEB, e vá à **administração > ao gerente CCA > ao certificado SSL > X509**.Em CAS, vá diretamente à interface da WEB através de https:// <CAS IP>/admin, e vá então à **administração > ao certificado SSL > X509**.Escolha o **certificado de importação da** lista de drop-down.O clique **consulta**, e escolhe o certificado salvar de etapa 1.**Transferência de arquivo pela rede do** clique.Clique **consultam** outra vez, e escolhem a chave privada que salvar de etapa 1.Escolha a **chave privada da** lista de drop-down do tipo de arquivo, e clique então a **transferência de arquivo pela rede**.O clique **verifica e instala Certificados transferidos arquivos pela rede**.**Nota:** Este Mensagem de Erro não deve ser fixada por estes procedimentos:
```
SEVERE: SSLFilter:access deniedCN=cas1.domain.com,
        OU=Information Technologies, O=Company, ST=State,
        C=US:Netscape cert type does not permit use for SSL client
```
Se os logs contêm esta mensagem, você deve contactar o fornecedor do certificado. O certificado deve ser reeditado com o tipo conjunto de campo CERT de Netscape ao servidor SSL e ao cliente SSL.

Informações Relacionadas

- Página de suporte da ferramenta NAC de Cisco
- Suporte Técnico e Documentação - Cisco Systems