Como eu certifico conexões de HTTPS a meu Codian MCU?

Índice

Introdução

Este artigo relaciona-se ao Cisco TelePresence MCU 4203, ao Cisco TelePresence MCU MSE 8420, ao Cisco TelePresence MCU 4505, ao Cisco TelePresence MCU MSE 8510 e ao Produtos avançado Cisco TelePresence do gateway de mídia 3610.

Q. Como eu certifico conexões de HTTPS a meu Codian MCU?

A. Da versão 2.3 de Codian MCU avante, se você tem o Gerenciamento seguro (HTTPS) ou a chave dos recursos de criptografia instalado, os apoios MCU fixam as conexões de HTTP (HTTPS) para a interface da WEB. Quando isto permitir todo o tráfego entre o usuário e o MCU a ser cifrado, os administradores que permitem este devem substituir o certificado e a chave privada fornecidos com seus próprias, para permitir que a identidade do MCU esteja autenticada. Note que você pode somente ter um certificado pelo MCU.

A fim criar uma chave privada e um certificado emparelhe, usando o OpenSSL (por exemplo):

1. Instale caso necessário o Gerenciamento seguro (HTTPS) ou a chave dos recursos de criptografia.
2. Vá ao **> serviços da rede** e abra as portas.
3. Conecte ao MCU usando o HTTPS que aceita o certificado temprary emitido por nós.
4. Em seu computador instale OpenSSL*. Isto está disponível à revelia em muitos Unix/sistemas Linux, e pode ser transferido para Windows de (na altura da escrita): http://www.slproweb.com/products/Win32OpenSSL.html
5. Em uma janela de comando, vai ao diretório em que o OpenSSL foi instalado, por exemplo C:\OpenSSL\bin.
6. Gerencia uma chave privada RSA usando o comando abaixo. Este comando gerencie um arquivo chamado “privkey.pem” que é sua chave privada. TANDBERG recomenda este chave seja pelo menos 2048 bit por muito tempo. Se esta chave privada será armazenada em qualquer lugar independentemente no MCU, deve ser protegida por uma frase de passagem: você é alertado entrar duas vezes nesta frase de passagem. > genrsa -des3 do OpenSSL - para fora privkey.pem 2048
7. Crie um certificado baseado nesta chave privada usando um dos comandos abaixo. Para o teste e o uso interno, este certificado pode auto-ser assinado, mas para a segurança

máxima deve ser assinado por um Certificate Authority. Para criar um uso do certificado auto-assinado (um arquivo chamado cert.pem): > req do OpenSSL - -x509 novo - chave privkey.pem - para fora cert.pem - dias 1000 ou para que um pedido do certificado seja enviado a um uso do Certificate Authority: > req do OpenSSL - novo - chave privkey.pem - para fora cert.csr both of these comandos prompt para um número de atributos. O Common Name deve combinar o nome de host ou o endereço IP de Um ou Mais Servidores Cisco ICM NT do MCU em que será instalado.

8. Se você está usando Certificados acorrentados, os Certificados acorrentados, no formato PEM, devem ser adicionados à extremidade do certificado de unidade. Isto pode ser feito em duas maneiras: copiando e colando em um editor de texto, ou usando algo tal como o comando unix do gato (por exemplo gato cert.pem authority.pem > chained.pem). Transfira arquivos pela rede então o arquivo criado.
9. No MCU vá à **rede > aos Certificados SSL**.
10. Para Certificados, o clique **consulta** e encontra o certificado que você criou (este está no diretório você se usou previamente). Se você criou um certificado auto-assinado, o certificado é chamado cert.pem. Para um assinado por um Certificate Authority, escolha o certificado assinado que forneceram.
11. Para a chave privada, selecione o arquivo privkey.pem.
12. Para a senha da criptografia chave privada, entre na frase de passagem usada ao gerar a chave privada (eventualmente).
13. Clique o **certificado e a chave da transferência de arquivo pela rede**. Se a transferência de arquivo pela rede é um sucesso, a informação local do certificado está atualizada àquela do certificado novo, e um aviso parece no encabeçamento da interface da WEB alertá-lo reiniciar o MCU.
14. Vá aos **ajustes > à parada programada** e reinicie o MCU.
15. Depois que reiniciou, conecte à interface da WEB usando o HTTPS. Se você usou um certificado auto-assinado, ignore os mensagens de advertência.
16. Confirme que o certificado correto está sendo usado. Para fazer isso: - Em Firefox: clicar com o botão direito na página, escolha a **informação de página da vista**. Clique sobre a **ABA de segurança**, e clique a **vista**. - No internet explorer: clicar com o botão direito na página, escolha **propriedades**. Clique sobre **Certificados**.

* TANDBERG não é responsável para o índice de sites da terceira parte

Informações Relacionadas

- Suporte Técnico e Documentação - Cisco Systems