Exemplo de configuração do Certificate Authority do server de comunicação de vídeo

Índice

Introdução

Este documento descreve o certificado de autenticação no server de comunicação de vídeo (VC). Um certificado identifica os VC e contém os nomes por que se sabe e a pelo que tráfego é distribuído. Se os VC são sabidos por nomes múltiplos para estas finalidades, como se é parte de um conjunto, este deve ser representado nos dados do assunto X.509. O certificado deve conter o nome de domínio totalmente qualificado (FQDN) de ambos os VC próprio e do conjunto. Se um certificado é compartilhado através dos pares do conjunto, deve alistar todo o par possível FQDNs.

Os VC precisam Certificados para:

- Fixe o HTTP com Transport Layer Security (TLS) (HTTPS) Conectividade
- Conectividade TLS para a sinalização do Session Initiation Protocol (SIP), os valores-limite, e zonas vizinhas
- Conexões a outros sistemas tais como o gerente das comunicações unificadas de Cisco (CUCM), os server da suite de gerenciamento do Cisco TelePresence (TMS), do Lightweight Directory Access Protocol (LDAP), e os servidores de SYSLOG

Usa sua lista dos Certificados confiados do Certificate Authority (CA) e das listas de revogação de certificado associadas (CRL) a fim validar os outros dispositivos que lhe conectam.

Pré-requisitos

Requisitos

Não existem requisitos específicos para este documento.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- VC - Liberações 8.1 e 8.1.1
- Certificate Authority - Empresa R2 de Microsoft Windows 2008

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.

Informações de Apoio

A liberação 8.1.1 VC apoia a característica móvel do Acesso remoto da borda de Collab (MRA) e exige uma conexão TLS entre o VC-controle e a VC-via expressa.

A fim estabelecer o TLS, você precisa de transferir arquivos pela rede Certificados necessários nos VC. Você pode terminar este com estes três métodos:

- OpenSSL
- Empresa CA
- CA da terceira

A conexão TLS entre o VC-controle e a VC-via expressa exige estes dois atributos:

- Authenticação do cliente TLS
- Autenticação do servidor de Web TLS

Este documento concentra-se no método de CA da empresa enquanto o OpenSSL é discutido já no guia de distribuição do certificado VC.

Quando você instala CA, o certificado do servidor de Web vem à revelia. Contudo, este molde não pode ser usado para gerar o certificado para a conexão TLS entre o VC-controle e a VC-via expressa. Se você tenta transferir arquivos pela rede o certificado aos VC, que está gerado com apenas o atributo do servidor de Web, você recebe este erro.

A fim verificar isto, selecione a **manutenção > o certificado de servidor**. O clique **descodifica o certificado**. Verifique a seção “estendeu o uso chave”.

Configurar

Como indicado mais cedo, porque a conexão TLS você precisa um atributo do cliente e do servidor de Web. Desde que não há um molde do padrão, você pode criar um. Termine estas etapas a fim gerar o molde novo com os atributos da autenticação da authenticação do cliente TLS e do servidor de Web TLS:

1. Abra o Certificate Authority ou vá ao console do Microsoft Management Console (MMC). O clique **adiciona/remove o Certificate Authority Snapin** e seleto. Expanda CA no painel

esquerdo e selecione **moldes de certificado**. Clicar com o botão direito o molde de certificado e seleto **controle**.
2. Clicar com o botão direito o molde de certificado do **servidor de Web** e selecione o **molde duplicado**.
3. Clique o botão de rádio da **empresa de Windows Server 2003** (se você quer o molde estar disponível para o registro da Web). Clique em **OK**.
4. Dê entrada com o nome de molde no campo de nome do indicador do molde. Nomeie o molde conforme suas exigências, por exemplo do “cliente servidor de Web 2003".
5. Clique os **Ramais** aba e selecione a política do aplicativo. O clique **edita**.
6. Na caixa de diálogo da política do aplicativo adicionar, selecione a **authenticação do cliente**. Clique em **OK**.
7. Na caixa de diálogo da extensão de políticas do aplicativo da edição, clique a **APROVAÇÃO**.
8. Do console MMC ou do indicador de CA, clicar com o botão direito o **molde de certificado**. Selecione **novo > molde de certificado a emitir**.
9. Selecione seu molde recém-criado na caixa de diálogo dos moldes de certificado da possibilidade. Verifique o molde na coluna **pretendida da finalidade**. Clique em **OK**.

Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Conclua estes passos:

1. Verifique que seu molde de certificado pedido está disponível a fim emitir Certificados novos.Nota: O molde estará disponível para o registro da Web somente se você selecionou o molde como Windows 2003 quando você criou o molde de certificado.
2. Siga o procedimento para gerar a solicitação de assinatura de certificado (CSR) dos VC e para obter o certificado assinado com o molde novo.
3. Verifique que o certificado tem o cliente e o atributo do servidor de Web disponíveis.

Troubleshooting

Esta seção fornece a informação que você pode se usar a fim pesquisar defeitos sua configuração.

Se o molde não está disponível para o registro da Web, determine se o usuário que alcança o **certsrv** tem as permissões necessárias.

Como indicado previamente, o molde de Windows 2008 não estará disponível para o registro da Web. Para mais detalhes, veja moldes do registro 2008 e da versão 3 da Web.