Criar Certificado Raiz Personalizado Umbrella com Serviços de Certificados AD

Contents

Introdução

Este documento descreve instruções para criar um certificado raiz personalizado usando os Serviços de Certificados do Microsoft Windows Ative Diretory (AD).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Uma versão do Microsoft Windows Server que é atualmente suportada pela Microsoft
- Serviços de Certificados do Ative Diretory instalados no Windows Server
- Uma conta com as funções Serviços de Certificados do Ative Diretory e Serviço Web/Serviço de Registro na Web
- Serviços de Certificados configurados para emitir certificados com codificação UTF-8 ("UTF8STRING")

Componentes Utilizados

As informações neste documento são baseadas no Cisco Umbrella.

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 rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Overview

Este artigo contém instruções para criar um certificado raiz personalizado (que é usado no lugar do certificado Cisco Umbrella Root CA padrão usando os Serviços de Certificados do Microsoft Windows Ative Diretory e, em seguida, usando esse certificado raiz para assinar uma Solicitação de Assinatura de Certificado (CSR) do recurso Certificado CA assinado pelo cliente do Umbrella.

Codificação de Cadeia de Caracteres de Certificado

Se seus serviços de certificado estiverem configurados para usar a codificação padrão ("PRINTABLESTRING"), a cadeia de certificados produzida não será confiável para certos clientes da Web, principalmente o Firefox.

O proxy do Cisco Umbrella Secure Web Gateway usa uma cadeia de certificados que codifica strings com codificação UTF8STRING. Se o certificado de emissão (por exemplo, o certificado raiz) que assina o CSR para criar o certificado intermediário da CA dos clientes do Cisco Umbrella estiver codificado com PRINTABLESTRING, a codificação do campo Assunto do certificado da CA dos clientes do Cisco Umbrella será PRINTABLESTRING. Essa codificação não pode corresponder à codificação UTF8STRING do campo Issuer no certificado intermediário de CA do Cisco Umbrella R1, que é o próximo na cadeia de certificados.

A seção 4.1.2.6 do RFC 5280 requer que uma cadeia de certificados mantenha a mesma codificação de cadeia de caracteres entre o campo Emissor de um certificado emitido e o campo Assunto no certificado emitido:

"Quando o requerente do certificado for uma AC, o campo requerente DEVERÁ ser codificado da mesma forma que no campo emitente (seção 4.1.2.4) em todos os certificados emitidos pela AC requerente."

Muitos navegadores não aplicam esse requisito, mas alguns (principalmente o Firefox) o fazem. Como resultado, os clientes da Web, como o Firefox, podem gerar um erro de site não confiável e não carregar sites ao usar o Secure Web Gateway (SWG) com o recurso de certificado CA assinado pela CA do cliente.

Para contornar esse problema, use um navegador como o Chrome, que não aplica o requisito do RFC 5280.

Passo 1: Preparando Modelo de Serviços de Certificados do AD

1. Abra o MMC da Autoridade de Certificação do Ative Diretory navegando para Iniciar > Executar > MMC.

2. Selecione File > Add/Remove Snap-in e adicione os snap-ins Certificate Templates e Certification Authority. Selecione OK.

3. Expanda Modelos de Certificado e clique com o botão direito do mouse em Autoridade de Certificação Subordinada. Clique em Modelo Duplicado.

Agora você pode criar um modelo de certificado personalizado para atender aos requisitos listados na documentação do Umbrella.

Estes são os requisitos detalhados no momento da criação deste artigo:

- guia Geral
  - Dê ao modelo um nome que tenha significado para você.
  - Defina o Período de validade para 35 meses (3 anos menos um mês).
  - Defina o período de renovação como 20 dias.
- Guia Extensões
  - Clique duas vezes em Restrições básicas.
    - Certifique-se de que Tornar este ramal crítico esteja selecionado.
  - Em Uso de chave:
    - Verifique se Certificate Signing & CRL Signing está selecionado.
    - Desmarque Digital Signature.
    - Certifique-se de que Tornar este ramal crítico também esteja marcado aqui.
- Selecione Aplicar e OK

Passo 2: Emitir o Modelo

1. No MMC configurado na etapa 2 do processo anterior, expanda a seção Autoridade de certificação.

2. Na seção recém-expandida, clique com o botão direito do mouse na pasta Modelos de certificado e selecione Novo > Modelo de certificado a ser emitido.

3. Na nova janela, selecione o nome do modelo de certificado que você criou na última seção e selecione OK.

A CA está pronta para facilitar a solicitação.

Passo 3: Download e assinatura do CSR

1. Faça login no Umbrella Dashboard (https://dashboard.umbrella.com).

2. Navegue até Implantações > Configuração > Certificado Raiz.

3. Selecione o ícone Adicionar (+) no canto e nomeie sua CA na nova janela.

4. Faça o download da CSR (Certificate Signing Request, Solicitação de Assinatura de Certificado).

5. Em uma nova guia do navegador, navegue até os serviços Web para Serviços de Certificados do Ative Diretory. (Se você estiver usando uma máquina local, esse valor será 127.0.0.1/certsrv/ ou similar.)

6. Na nova página, selecione Solicitar um Certificado.

7. Selecione Solicitação Avançada de Certificado.

8. Em Solicitação Salva, copie e cole o conteúdo do CSR que você baixou na etapa 4 (você deve abri-lo com um editor de texto).

9. Em Modelo de Certificado, selecione o nome do modelo de certificado que você criou na seção "Preparando Modelo de Serviços de Certificados do AD" e selecione Enviar.

10. Certifique-se de selecionar Base64 Encoded e selecione Download Certificate e anote o local do arquivo .cer.

Passo 4: Carregar o CSR assinado (e o certificado de raiz pública)

1. No Painel Umbrella, navegue para Implantação > Configuração > Certificado Raiz.

2. Selecione o certificado raiz criado na Etapa 3 da seção anterior.

3. Selecione Carregar CA no canto inferior direito da linha*.

4. Selecione o botão superior Browse (Certificate Authority (Signed CSR)).

5. Navegue até o local do arquivo .cer que você criou na seção anterior e selecione Salvar.

6. Selecione Avançar e selecione os grupos de computadores/usuários com os quais você gostaria que o certificado fosse usado (em vez do Certificado raiz Cisco) e selecione Salvar.

*Você também pode carregar o certificado CA opcionalmente. Ele pode ser recuperado da interface da Web do servidor da autoridade de certificação (http://127.0.0.1/certsrv/) e, em seguida, selecionar Download a CA Certificate, Certificate Chain ou CRL. Preencha os prompts na tela para "Download do certificado CA" na Base 64.

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.