

Sem a edição com um certificado assinado da terceira parte na fineza

Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Problema: Sem a edição com um certificado assinado da terceira parte na fineza](#)

[Solução](#)

Introdução

Este original descreve o problema onde o certificado de server de aplicativo não carrega com o Mensagem de Erro “CSR SAN e o certificado SAN não combina”.

Contribuído por Anuj Bhatia, engenheiro de TAC da Cisco.

Pré-requisitos

Requisitos

Cisco recomenda que você tem o conhecimento destes assuntos

- O certificado assinou o processo de geração do pedido (CSR) na plataforma do sistema operacional da Voz (VOS)
- Processo para transferir arquivos pela rede o certificado assinado do Certificate Authority (CA) na plataforma VOS

[Componentes Utilizados](#)

A informação neste documento é baseada na fineza de Cisco 11.0(1) e acima.

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.

Problema: Sem a edição com um certificado assinado da terceira parte na fineza

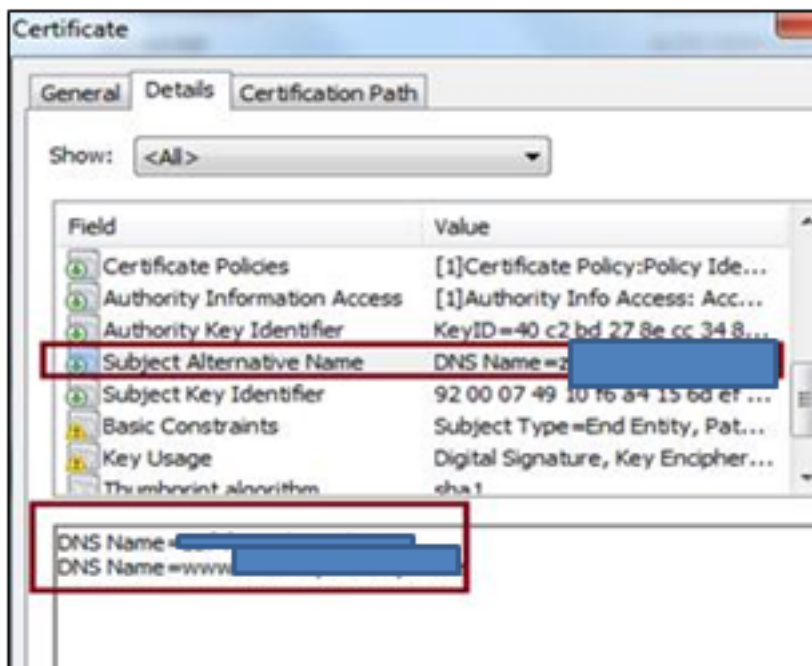
Para que o server use a primeira etapa dos certificados assinados de CA é gerar um CSR. É criado da página da geração CSR onde o campo dos nomes alternativos do assunto (sem) é

povoado à revelia com o Domain Name do server.



Após a geração CSR sem no CSR são apresentados neste formato
DNS Name=ora.com (dNSName)
DNS Name=finessea.ora.com (dNSName)

Quando a terceira parte CA criar um certificate chain deste CSR enquanto incluem geralmente estes sem o nome no certificado do aplicativo que combina mal do CSR.
Name= finessea.ora.com DNS
DNS Name=www. finessea.ora.com
O certificado do aplicativo fornecido por GoDaddy CA é mostrado na imagem:



Esta má combinação de sem impede a carga do certificado do aplicativo na loja da confiança de TomCat e gere o erro "CSR SAN e o certificado SAN não combina"

Note: O problema é no plaform VOS e é aplicável a todo o Produtos do centro de contato que é executado neste sistema operacional tal como dados do cisco live, Cisco unificou o centro da inteligência (CUIC) etc.

Solução

Há duas maneiras de aproximar a edição:

- O cliente pode consultar com a autoridade de CA e pode pedir para obter o certificate chain com sem como o presente no CSR.
- Uma opção mais fácil é manter-se sem a placa do campo ao gerar o CSR.

Status

 Warning: Generating a new CSR for a specific certificate type will overwrite the exist

Generate Certificate Signing Request

Certificate Purpose*

Distribution*

Common Name*

Subject Alternate Names (SANs)

Parent Domain

Key Length*

Hash Algorithm*

Não tem nenhum dados no sem a informação do CSR. Quando a autoridade de CA fornece o certificate chain ele popualtes a informação mas durante a transferência de arquivo pela rede, o sistema ignora o campo que allowes o certificado a ser instalado.