SANs第三方签名的证书的问题在精良

Contents

Introduction

本文描述应用服务器认证不能用错误信息“CSR SAN装载和认证SAN不匹配”的问题。

贡献用Anuj Bhatia， Cisco TAC工程师。

Prerequisites

Requirements

Cisco建议您有这些题目知识

- 认证签署了请求(CSR)在语音操作系统的(VOS)平台的生成过程
- 加载在VOS平台的Certificate Authority (CA)签名的证书的进程

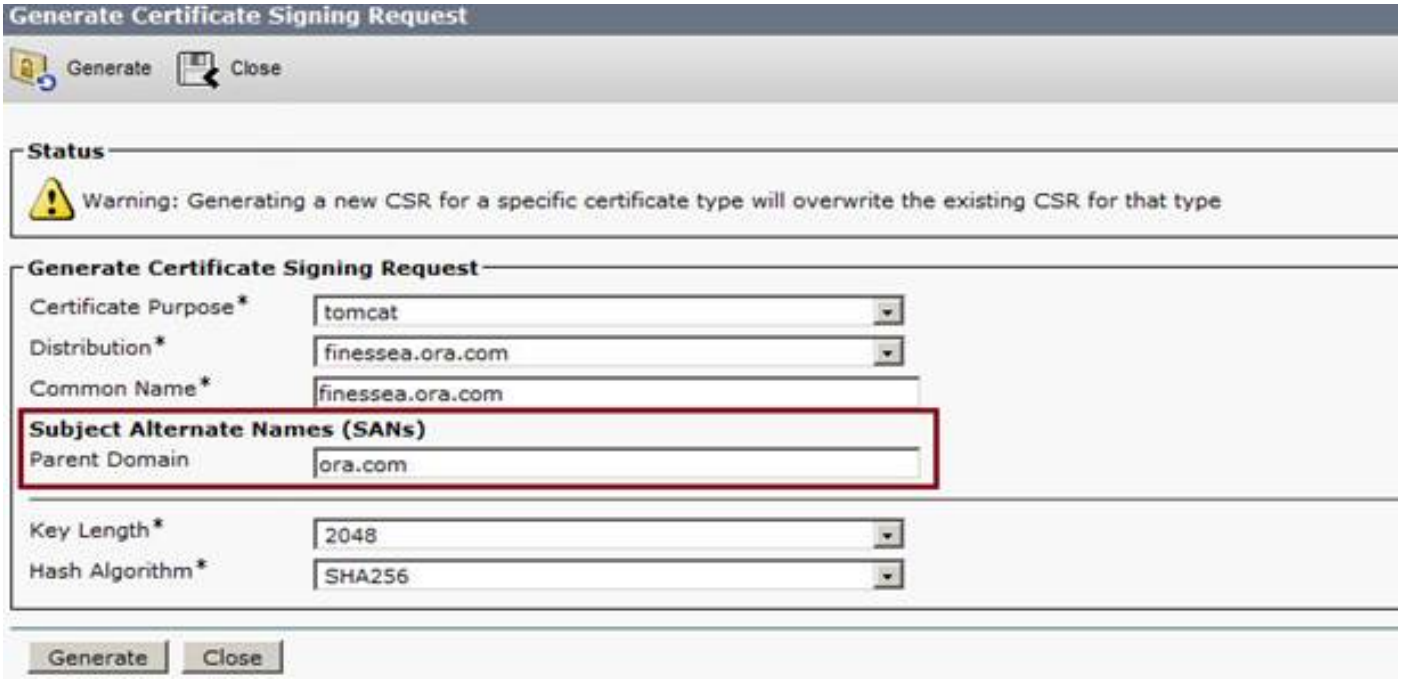
Components Used

本文的信息根据Cisco精良11.0(1)以上。

The information in this document was created from the devices in a specific lab environment.All of the devices used in this document started with a cleared (default) configuration.If your network is live, make sure that you understand the potential impact of any command.

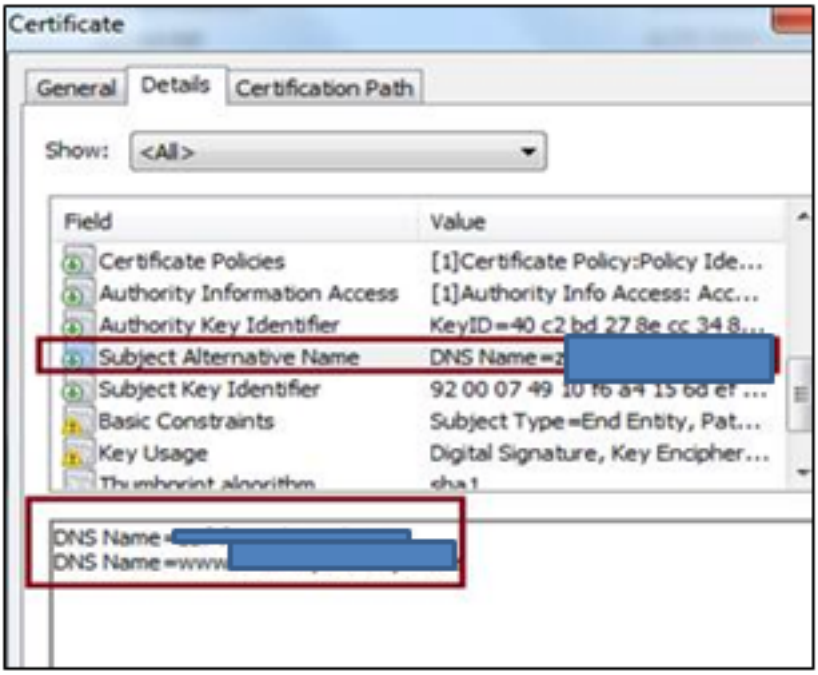
问题：SANs第三方签名的证书的问题在精良

为了使服务器使用CA签名的证书第一步是生成CSR。它从默认情况下主题替代名称的生成CSR页被创建(SANs)字段带有服务器的域名。



在CSR生成以后SANs在CSR被提交以此格式
DNS Name=ora.com (dNSName)
DNS Name=finessea.ora.com (dNSName)

当第三方CA创建从此CSR的一条证书链，当他们通常包括这些SANs名字在从CSR配错的应用程序认证。
DNS Name= finessea.ora.com
DNS Name=www。finessea.ora.com
GoDaddy CA提供的应用程序认证在镜像显示：



此不匹配SANs在Tomcat信任存储妨害应用程序认证加载并且生成错误“CSR SAN和认证SAN不匹配”

Note:问题是在VOS plaform并且是可适用的对运行在此的所有联系中心产品操作系统例如Cisco Live数据， Cisco Unified智力中心(CUIC)等。

解决方案

有两种方式看待问题：

- 用户与CA权限咨询，并且能请求获得有的证书链SANs作为在CSR的存在。
- 当生成CSR时，更加容易的选项是保持SANs字段空白。

它没有数据在SANs CSR的信息。在加载期间时，当CA权限提供证书链它popualtes信息，但是，系统忽略allowes将安装的认证的字段。