SAN-Probleme mit einem von einem Drittanbieter signierten Zertifikat in Finesse

Inhalt

Einführung

In diesem Dokument wird das Problem beschrieben, bei dem das Anwendungsserverzertifikat nicht geladen werden kann. Hierzu wird die Fehlermeldung "CSR SAN and Certificate SAN does not match" (CSR-SAN und ZertifikatsSAN stimmen nicht überein) angezeigt.

Unterstützt von Anuj Bhatia, Cisco TAC Engineer.

Voraussetzungen

Anforderungen

Cisco empfiehlt, diese Themen zu kennen.

- Generierung von Zertifikatsanforderung (Certificate Signed Request, CSR) auf der VOS-Plattform (Voice Operating System)
- Prozess zum Hochladen eines signierten Zertifikats der Zertifizierungsstelle (Certificate Authority, CA) auf der VOS-Plattform

Verwendete Komponenten

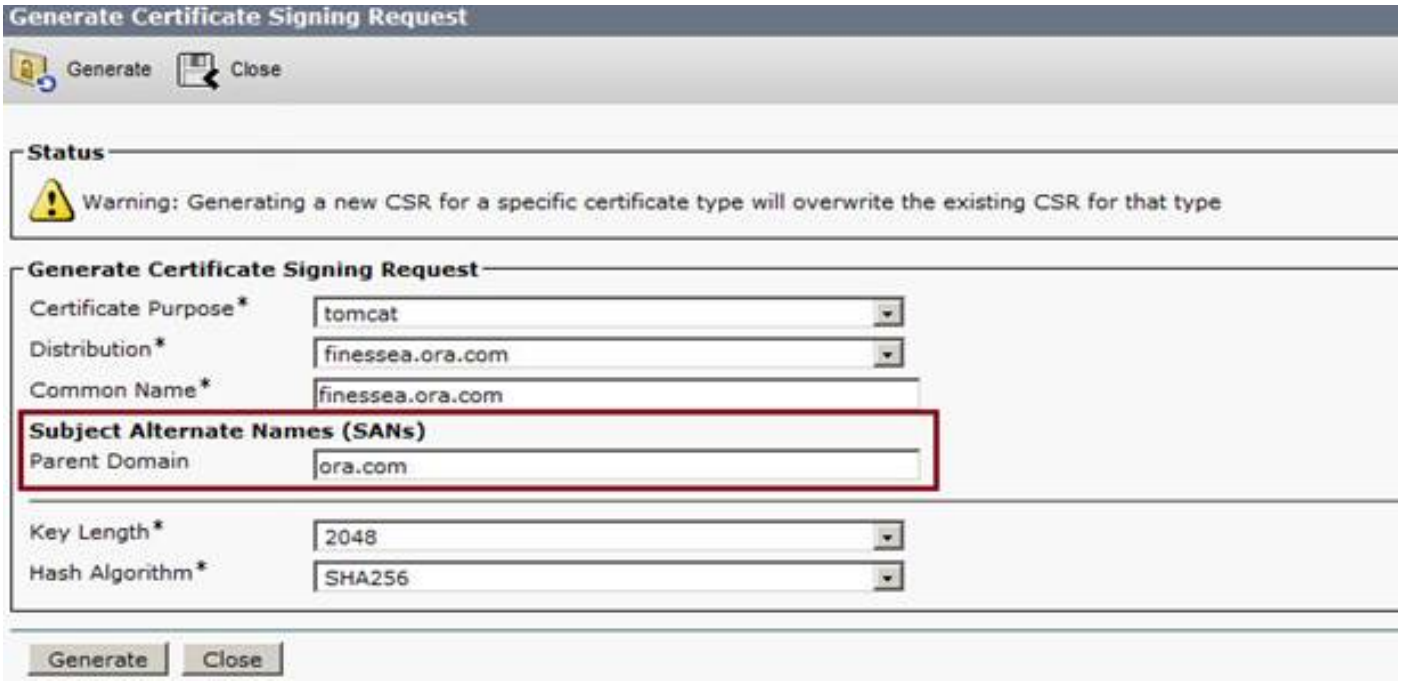
Die Informationen in diesem Dokument basieren auf der Cisco Finesse 11.0(1) und höher.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Problem: SAN-Probleme mit einem von einem Drittanbieter signierten Zertifikat in Finesse

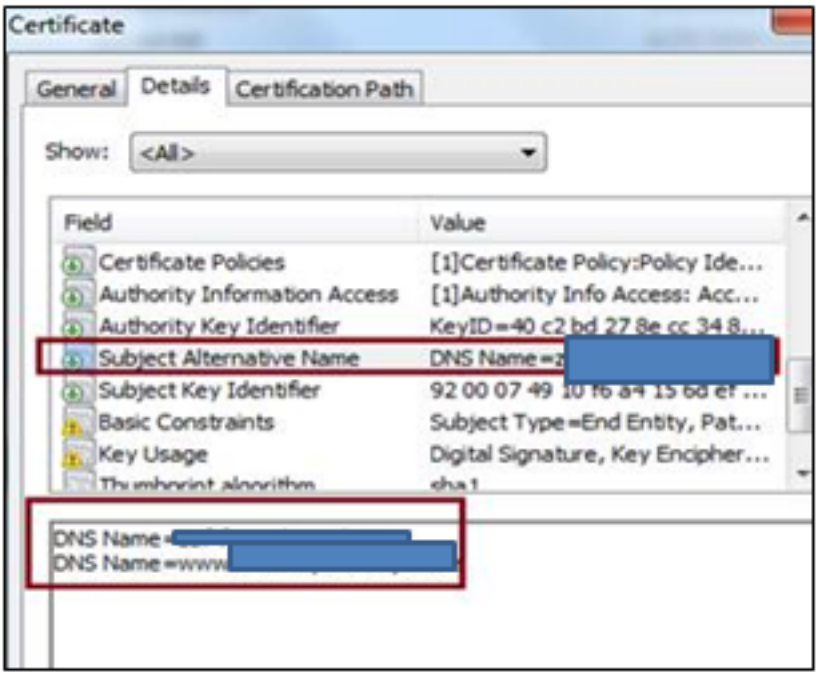
Damit der Server Zertifizierungsstellenzertifikate verwenden kann, muss zunächst ein CSR

generiert werden. Sie wird auf der Seite "CSR erstellen" erstellt, auf der im Standardfeld "SANs" (Subject Alternate Names) der Domänenname des Servers eingetragen wird.



Nach der CSR-Generierung werden die SANs in CSR in diesem Format dargestellt.
DNS Name=ora.com (Name des DNS)
DNS-Name=finessea.ora.com (dNSName)

Wenn die CA eines Drittanbieters eine Zertifikatskette aus diesem CSR erstellt, da diese im Allgemeinen den Namen dieser SANs in das Anwendungszertifikat aufnehmen, der mit dem CSR nicht übereinstimmt.
DNS Name= finessea.ora.com
DNS Name=www. finessea.ora.com
Das von GoDaddy CA bereitgestellte Anwendungszertifikat wird im Bild angezeigt:



Diese Diskrepanz zwischen SANs behindert das Laden von Anwendungszertifikaten im tomcat trust store und generiert den Fehler "CSR SAN and Certificate SAN does not match" (CSR-SAN

und ZertifikatSAN stimmen nicht überein).

> **Hinweis**: Das Problem tritt bei der VOS-Plattform auf und gilt für alle Contact Center-Produkte, die auf diesem Betriebssystem ausgeführt werden, wie z. B. Cisco Live Data, Cisco Unified Intelligence Center (CUIC) usw.

Lösung

Es gibt zwei Möglichkeiten, das Problem anzugehen:

- Der Kunde kann sich an die CA-Behörde wenden und die Zertifikatskette mit den SANs anfordern, wie im CSR vorhanden.
- Einfacher ist es, das Feld SANs bei der Erstellung des CSR leer zu lassen.

Es enthält keine Daten in den SAN-Informationen von CSR. Wenn die Zertifizierungsstellen die Zertifikatskette bereitstellen, werden die Informationen angezeigt, aber während des Uploads ignoriert das System das Feld, in dem das Zertifikat installiert werden kann.