

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Problème : Sans la question avec un certificat signé de tiers dans la finesse](#)

[Solution](#)

Introduction

Ce document décrit le problème où le certificat de serveur d'applications ne charge pas avec le message d'erreur « CSR SAN et le certificat SAN n'apparie pas ».

Contribué par Anuj Bhatia, ingénieur TAC Cisco.

Conditions préalables

Conditions requises

Cisco recommande que vous ayez la connaissance de ces thèmes

- Le certificat a signé le procédé de génération de la demande (CSR) sur la plate-forme du système d'exploitation de Voix (VOS)
- Processus pour télécharger le certificat signé d'Autorité de certification (CA) sur la plate-forme VOS

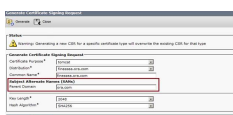
Composants utilisés

Les informations dans ce document sont basées sur le Cisco Finesse 11.0(1) et ci-dessus.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Problème : Sans la question avec un certificat signé de tiers dans la finesse

Pour que le serveur utilise le CA la première étape de Certificats signés est de générer un CSR. Il est créé de la page CSR de générer où par des noms secondaires soumis par défaut (sans) le champ est rempli avec le nom de domaine du serveur.



Après la génération CSR sans dans le CSR sont présentés dans ce format

DN Name=ora.com (dNSName)

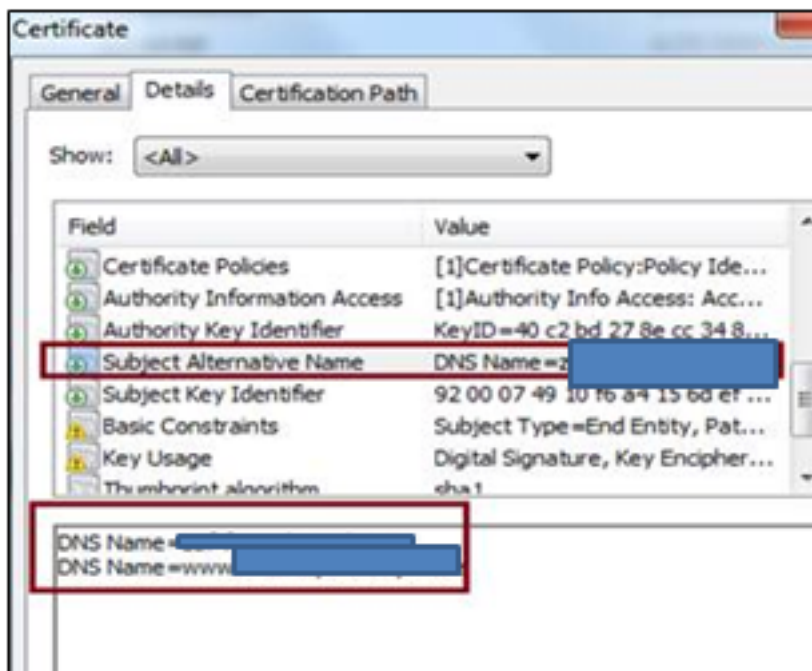
DN Name=finessea.ora.com (dNSName)

Quand le tiers CA crée une chaîne de certificat de ce CSR pendant qu'ils incluent généralement ces derniers sans le nom dans le certificat d'application qui mal adapte du CSR.

DN Name= finessea.ora.com

DN Name=www. finessea.ora.com

Le certificat d'application fourni par GoDaddy CA est affiché dans l'image :



Cette non-concordance de sans gêne le chargement du certificat d'application dans la mémoire de confiance de chat et génère l'erreur « CSR SAN et le certificat SAN n'apparie pas »

Remarque: Le problème s'applique sur le plaform VOS et est à tous les Produits de centre de contact s'exécutant sur ce système d'exploitation tel que les données de Cisco, le centre vivants d'intelligence de Cisco Unified (CUIC) etc.

Solution

Il y a deux manières d'approcher la question :

- Le client peut consulter avec l'autorité CA et peut demander d'obtenir la chaîne de certificat avec sans en tant que présent dans le CSR.
- Une option plus facile est de maintenir sans le champ vide en générant le CSR.

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

Generate Certificate Signing Request

Certificate Purpose* tomcat

Distribution* finessea.ora.com

Common Name* finessea.ora.com

Subject Alternate Names (SANs)
Parent Domain

Key Length* 2048

Hash Algorithm* SHA256

Generate Close

Il n'a aucune donnée dans sans les informations du CSR. Quand l'autorité CA fournit la chaîne de certificat il des popualtes les informations mais pendant le téléchargement, le système ignore le champ qui des allowes le certificat à installer.