SAN在Finesse中頒發第三方簽名的證書

目錄

簡介

本檔案將說明應用伺服器憑證無法載入的問題，並出現錯誤「CSR SAN and Certificate SAN does not match」。

作者：Anuj Bhatia，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題

- 語音作業系統(VOS)平台上的憑證簽署請求(CSR)產生程式
- 在VOS平台上上傳證書頒發機構(CA)簽名證書的流程

採用元件

本文檔中的資訊基於Cisco Finesse 11.0(1)及更高版本。

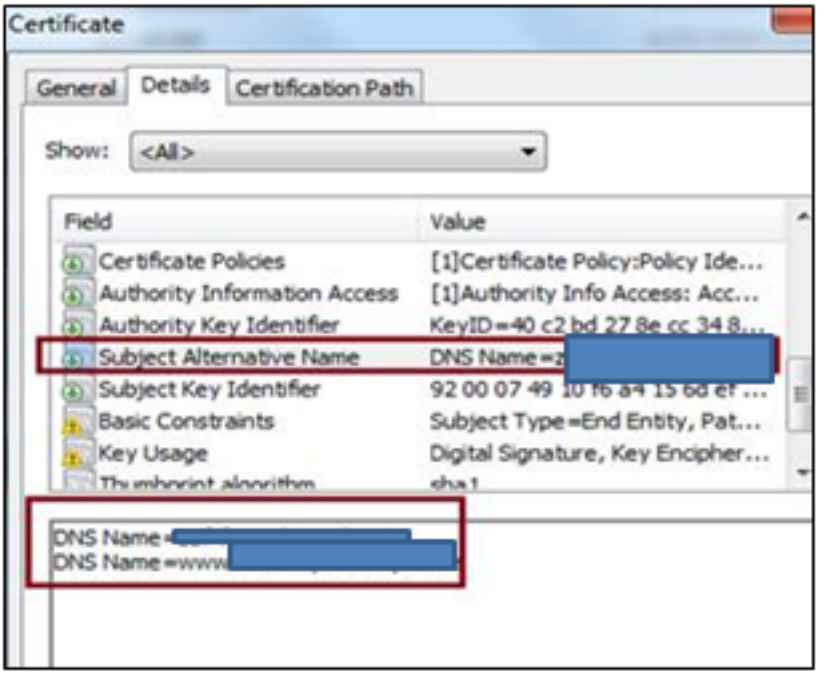
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

問題：SAN在Finesse中頒發第三方簽名的證書

對於伺服器使用CA簽名的證書，第一步是生成CSR。它從Generate CSR（生成CSR）頁面建立，其中預設的Subject Alternate Names(SAN)欄位填充有伺服器的域名。

產生CSR後，CSR中的SAN會以此格式顯示
DNS Name=ora.com(dNSName)
DNS Name=finessea.ora.com(dNSName)

當第三方CA從此CSR建立憑證鏈結時，因為它們通常會在來自CSR的不相符的應用憑證中包含這些SAN名稱。
DNS名稱= finessea.ora.com
DNS名稱=www.finessea.ora.com
GoDaddy CA提供的應用證書如下圖所示：



此SAN不匹配會妨礙在tomcat信任儲存中載入應用程式證書，並生成錯誤「CSR SAN和證書SAN不匹配」

附註：問題出在VOS平台上，適用於在此作業系統上運行的所有聯絡中心產品，例如Cisco Live Data、Cisco Unified Intelligence Center(CUIC)等。

解決方案

有兩種方法可以解決此問題：

- 客戶可諮詢CA主管機構，並可要求取得具有CSR中存在SAN的憑證鏈結。
- 更簡單的選項是在生成CSR時將SAN欄位留空。

在CSR的SAN資訊中沒有資料。當CA授權機構提供憑證鏈結時，系統會提供資訊，但在上傳期間，系統會忽略允許安裝憑證的欄位。