Problemi SAN con un certificato firmato da terze parti in Finesse

Sommario

Introduzione

In questo documento viene descritto il problema relativo al mancato caricamento del certificato del server applicazioni con il messaggio di errore "CSR SAN and Certificate SAN does not match".

Contributo di Anuj Bhatia, Cisco TAC Engineer.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti

- Processo di generazione CSR (Certificate Signed Request) su piattaforma VOS (Voice Operating System)
- Processo di caricamento del certificato firmato dall'Autorità di certificazione (CA) sulla piattaforma VOS

Componenti usati

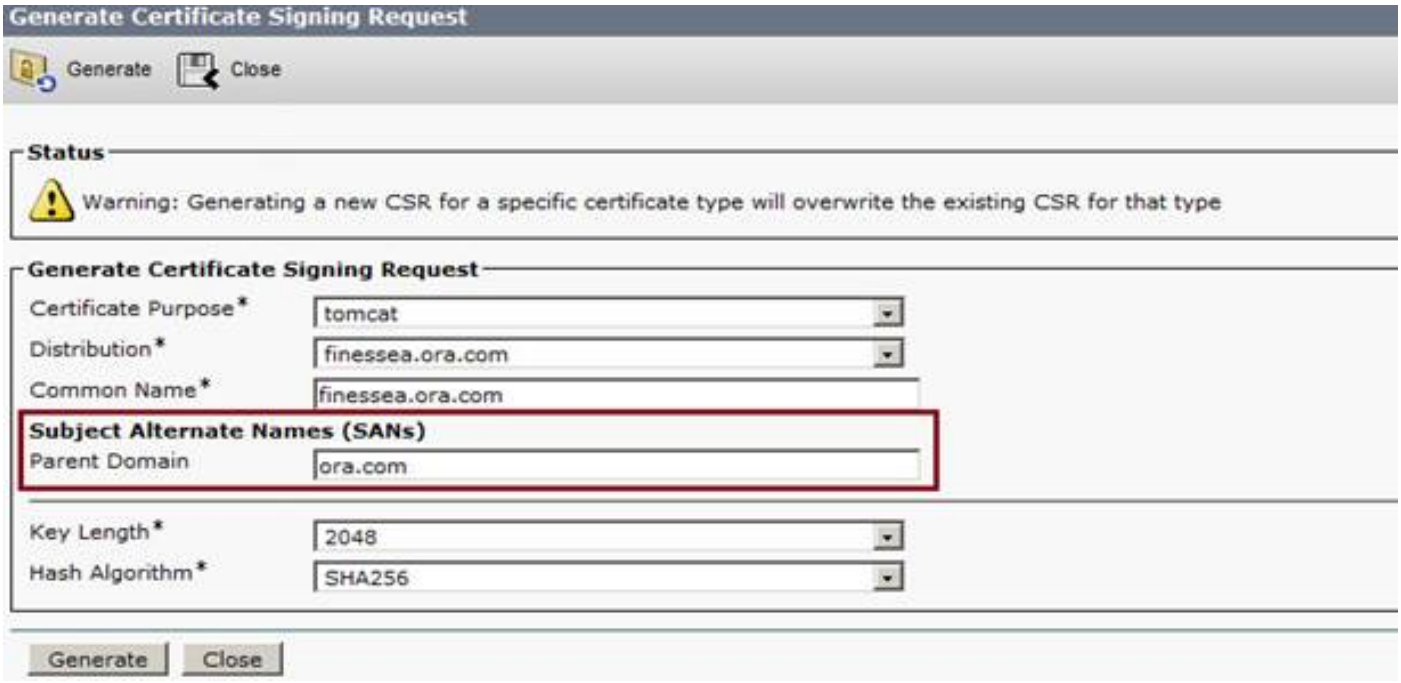
Il riferimento delle informazioni contenute in questo documento è Cisco Finesse 11.0(1) e versioni successive.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema: Problemi SAN con un certificato firmato da terze parti in Finesse

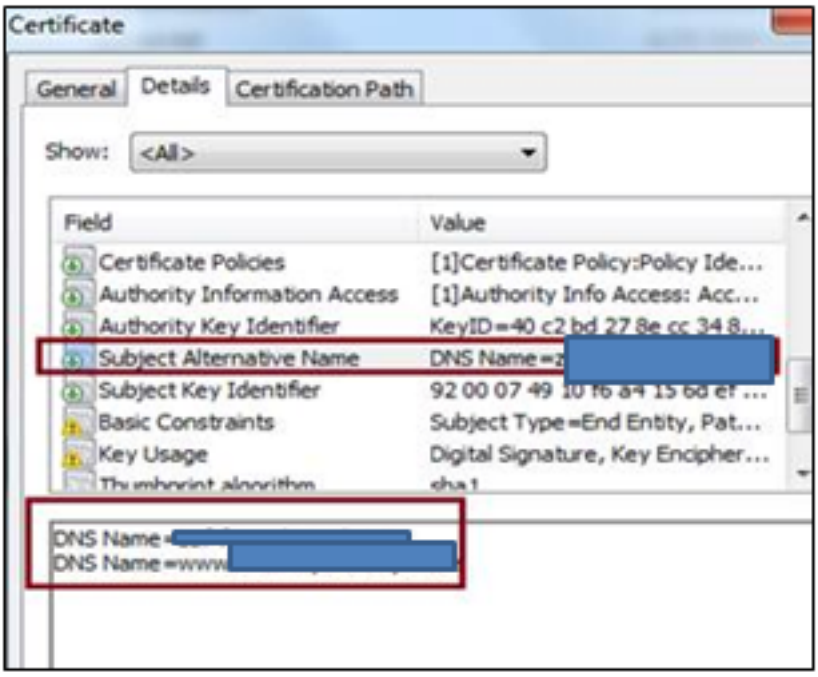
Per utilizzare i certificati firmati dall'autorità di certificazione, il primo passaggio consiste nella

generazione di un CSR. Viene creata dalla pagina Genera CSR, in cui per impostazione predefinita nel campo Nomi alternativi soggetto (SAN) viene inserito il nome di dominio del server.



Dopo la generazione della CSR, le SAN in CSR vengono presentate in questo formato
Nome DNS=ora.com (dNSName)
Nome DNS=finessea.ora.com (dNSName)

Quando l'autorità di certificazione di terze parti crea una catena di certificati da questo CSR, poiché in genere include il nome di queste SAN nel certificato dell'applicazione che non corrisponde al CSR.
Nome DNS= finessea.ora.com
Nome DNS=www. finessea.ora.com
Il certificato dell'applicazione fornito da GoDaddy CA è mostrato nell'immagine:



Questa mancata corrispondenza delle SAN impedisce il caricamento del certificato dell'applicazione nell'archivio di attendibilità Tomcat e genera l'errore "CSR SAN and Certificate

SAN does not match"

> **Nota:** Il problema è relativo alla piattaforma VOS ed è applicabile a tutti i prodotti Contact Center in esecuzione su questo sistema operativo, ad esempio Cisco Live Data, Cisco Unified Intelligence Center (CUIC) e così via.

Soluzione

Esistono due modi per affrontare la questione:

- Il Cliente può consultare l'autorità CA e richiedere di ottenere la catena di certificati con le SAN presenti nel CSR.
- L'opzione più semplice consiste nel lasciare vuoto il campo SAN durante la generazione del CSR.

Non dispone di dati nelle informazioni CSR delle SAN. Quando l'autorità CA fornisce la catena di certificati, le informazioni vengono inserite, ma durante il caricamento il sistema ignora il campo che consente l'installazione del certificato.