SANs выходят с Подписанным сертификатом Третьей стороны в Изяществе

Содержание

Введение

Этот документ описывает проблему, где сертификат сервера приложений не в состоянии загружать сообщением об ошибках "SAN CSR, и SAN Сертификата не совпадает".

Внесенный Anuj Bhatia, специалистом службы технической поддержки Cisco.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами

- Процесс генерации Сертификата запроса со знаком (CSR) на платформе голосовой операционной системы (VOS)
- Процесс для загрузки подписанного сертификата Центра сертификации (CA) на платформе VOS

Используемые компоненты

Сведения в этом документе основываются на Изяществе Cisco 11.0 (1) и выше.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

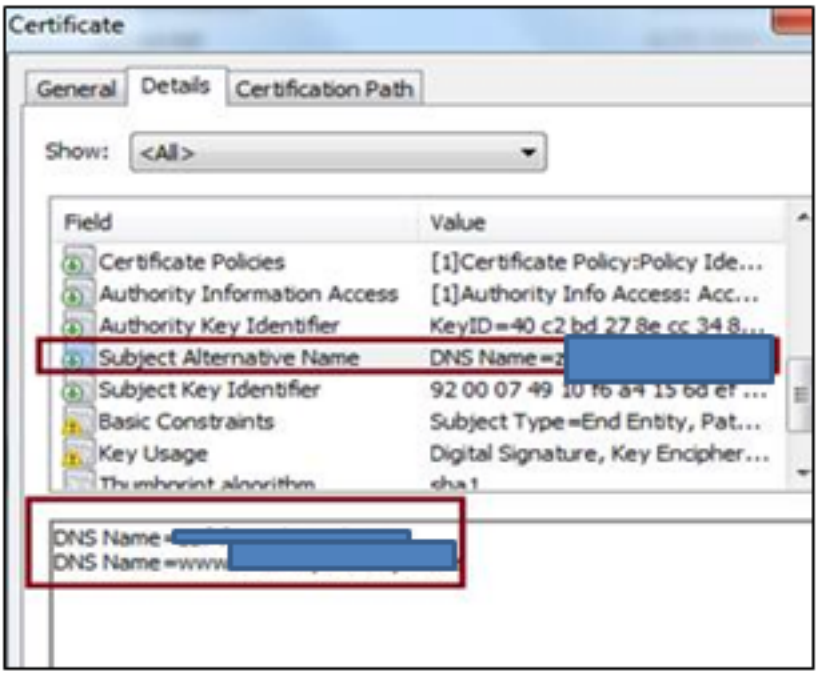
Проблема: SANs выходят с Подписанным сертификатом Третьей стороны в Изяществе

Для сервера для использования первого шага подписанных сертификатов CA должен генерировать CSR. Это создано от страницы Generate CSR, где Subject Alternate Names

(SANs) по умолчанию поле заполнено с доменным именем сервера.

После генерации CSR SANs в CSR представлены в этом формате
DNS Name=ora.com (dNSName)
DNS Name=finessea.ora.com (dNSName)

Когда третья сторона CA создает цепочку сертификатов от этого CSR, поскольку они обычно включают эти SANs название в сертификат приложения, который не сочетается от CSR.
Имя DNS = finessea.ora.com
DNS Name=www. finessea.ora.com
Сертификат приложения, предоставленный GoDaddy CA, показывают в образе:



Это несоответствие SANs препятствует загрузке сертификата приложения в базе доверенных сертификатов tomcat и генерирует ошибку "SAN CSR, и SAN Сертификата не совпадает"

Примечание: Проблема находится на plaform VOS и применима ко всем продуктам Contact Center, работающим на этой операционной системе, таким как Данные Cisco live, Cisco Unified Intelligence Center (CUIC) и т.д.

Решение

Существует два способа приблизиться к проблеме:

- Клиент может консультироваться с полномочиями CA и может запросить получить цепочку сертификатов с SANs как подарок в CSR.
- Более легкая опция должна поддержать пробел поля SANs при генерации CSR.

Это не имеет никаких данных в информации SANs CSR. Когда CA полномочия предоставляют цепочку сертификатов, это заполняет информацию, но во время загрузки, система игнорирует поле, которое позволяет сертификату быть установленным.