Настройка кластера объединенных коммуникаций с подписанным CA примером конфигурации альтернативного названия предмета мультисервера

Содержание

Введение

Этот документ описывает, как установить Кластер Объединенных коммуникаций с использованием Центра сертификации (CA) - Подчиненное альтернативное название (SAN) Мультисервера Со знаком.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Cisco Unified Communications Manager (CUCM)
- IM CUCM и версия 10.5 присутствия

Прежде чем вы будете делать попытку этой конфигурации, будете гарантировать, что эти сервисы подключены и функциональны:

- Платформа cisco административный веб-сервис
- Служба Cisco Tomcat

Для проверки этих сервисов на веб-интерфейсе перейдите к **Cisco Unified Serviceability Page Services>, Сетевой сервис> Выбирает сервер**. Для проверки их на CLI введите команду **списка сервиса utils**.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

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.

Общие сведения

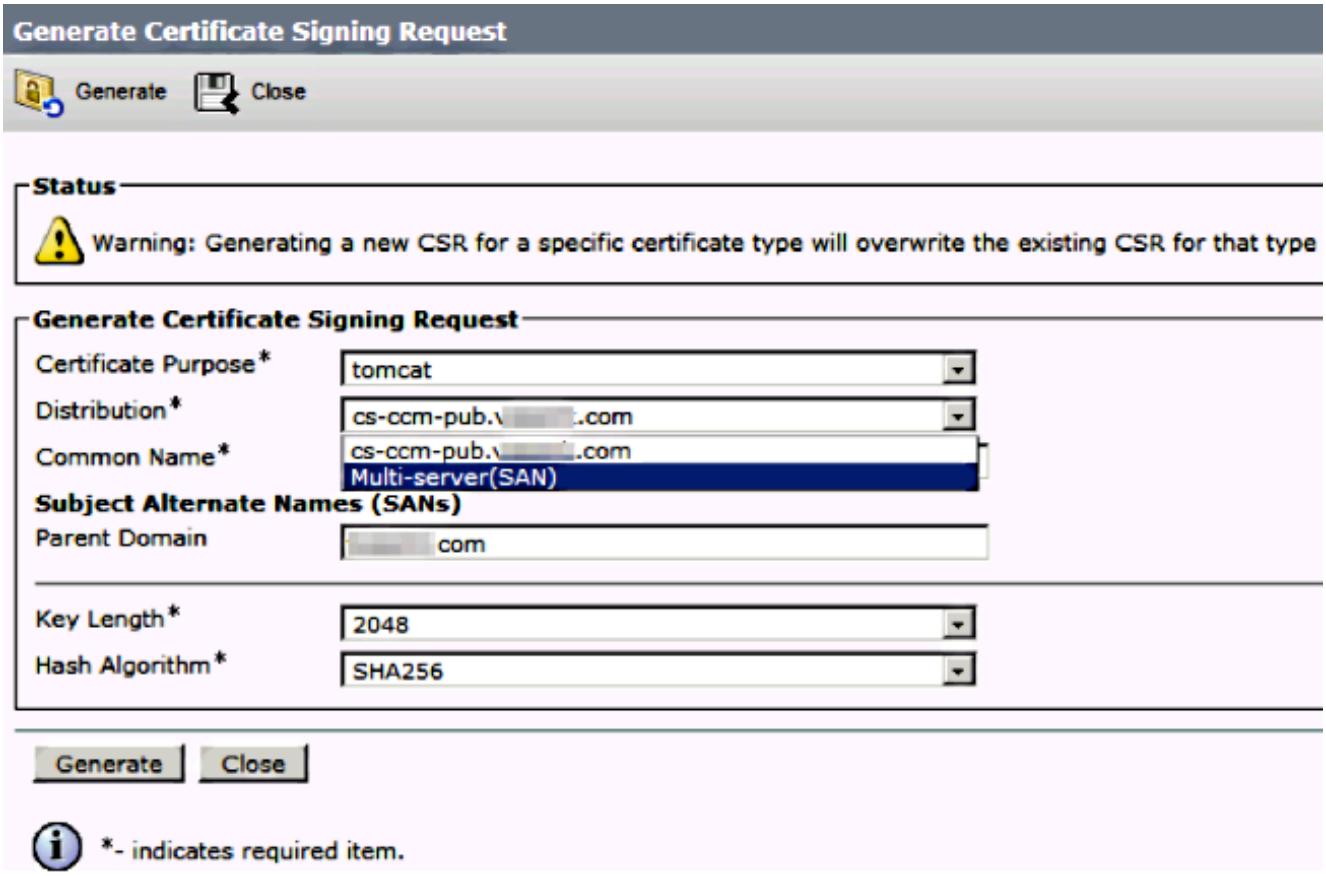
В Версии 10.5 CUCM и позже, эта база доверенных сертификатов запрос Запроса подписи сертификата (CSR) может включать SAN и альтернативные домены.

1. Tomcat
2. Cisco CallManager (CCM)
3. Расширяемый Cisco Unified Presence протокол обмена сообщениями и присутствия (CUP-XMPP)
4. От сервера к серверу CUP-XMPP (S2S)

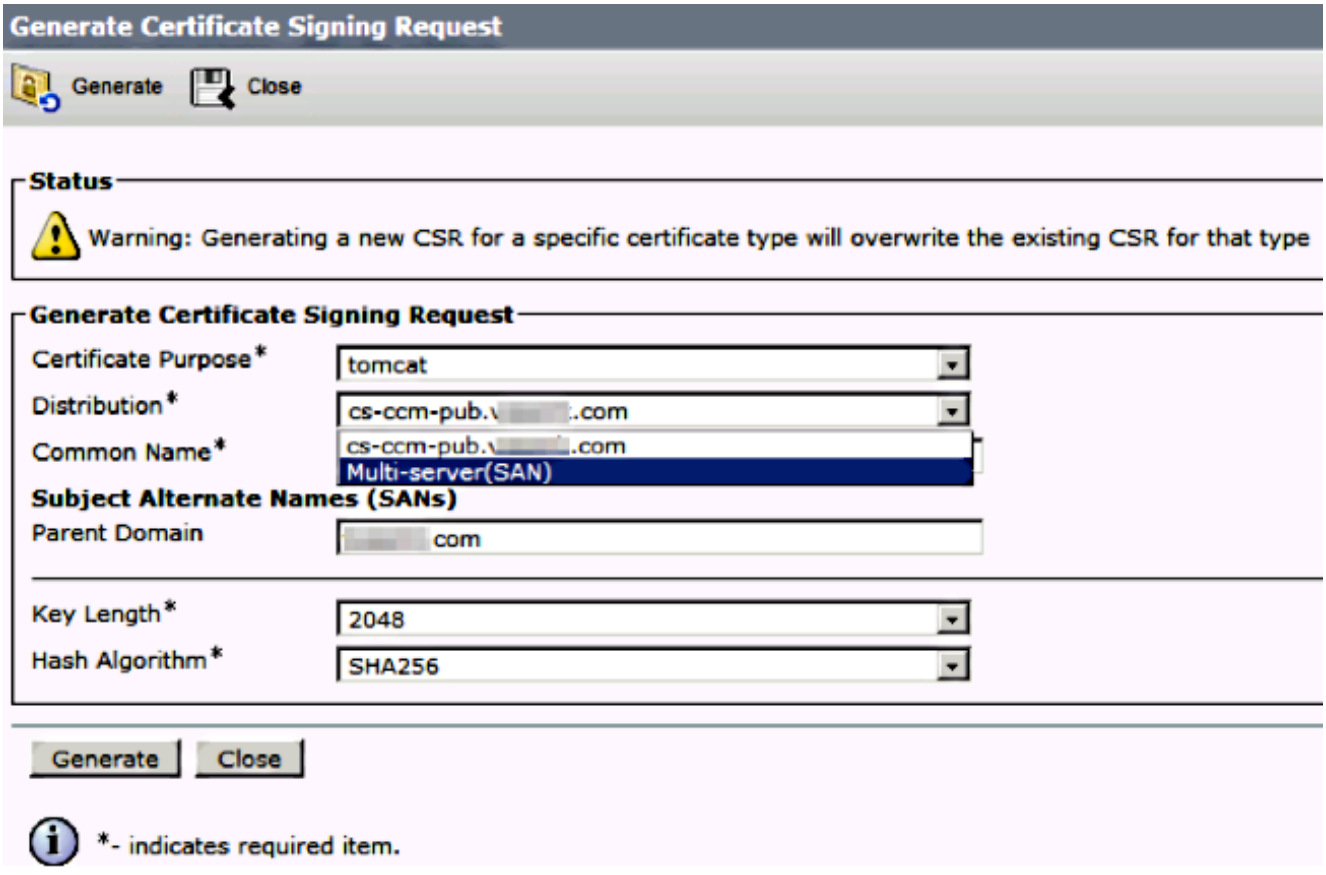
Более просто получить Сертификат подписанный ЦС в этой версии. Только один CSR требуется, чтобы быть подписанным CA, а не требованием, чтобы получить CSR из каждого узла сервера и затем получить Сертификат подписанный ЦС для каждого CSR и управлять ими индивидуально.

Настройка

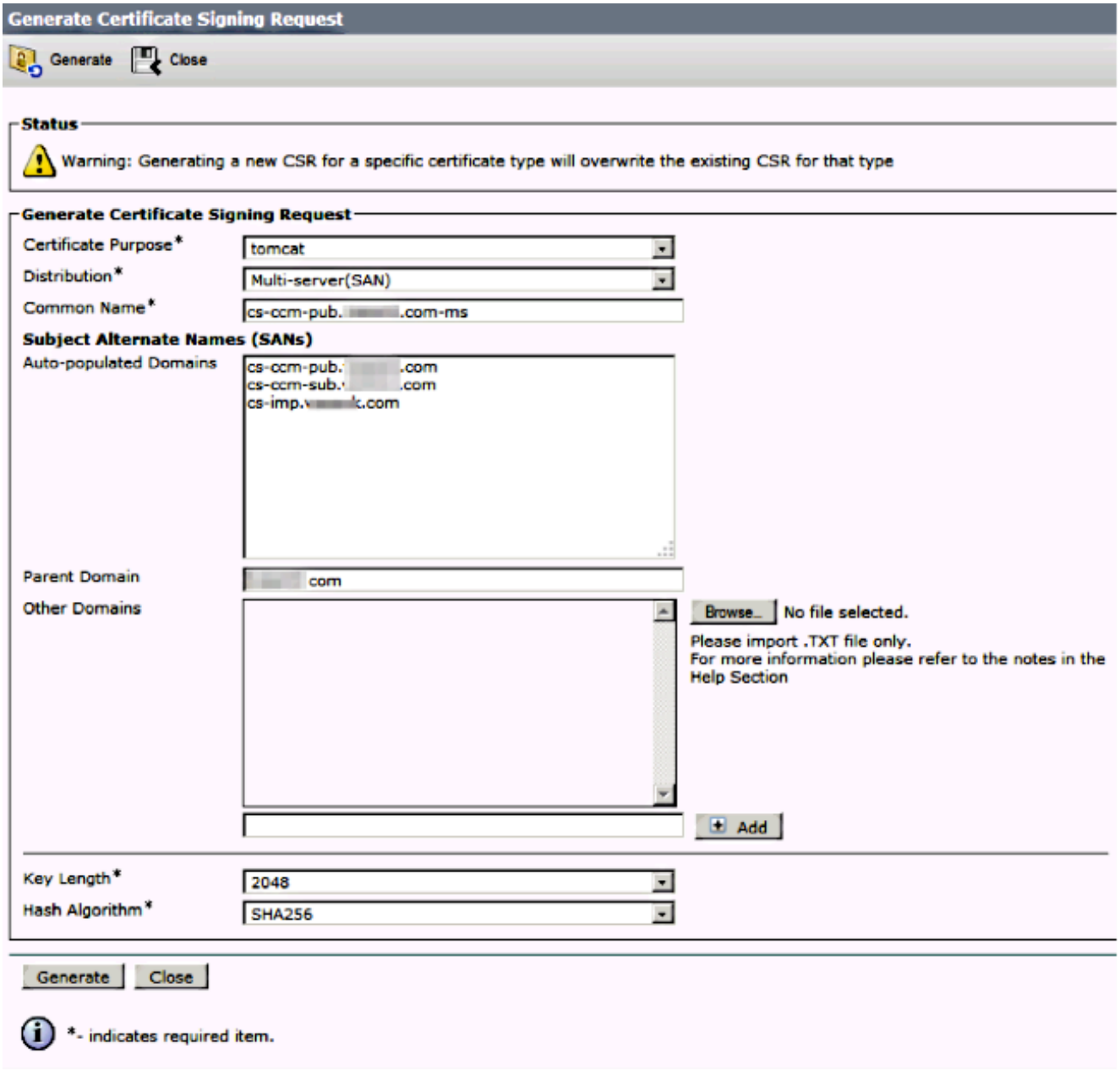
1. Войдите в администрирование Операционной системы (OS) и перейдите к **Безопасности> Управление сертификатами>, Генерируют CSR**.



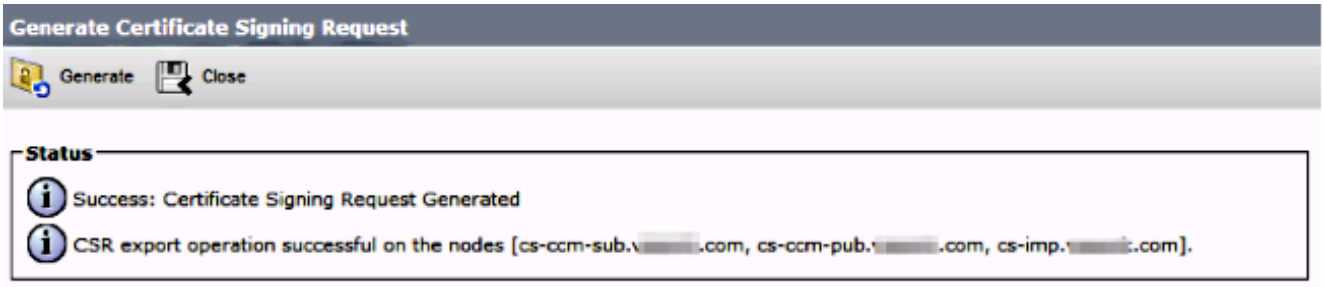
2. Выберите **Multi-Server SAN in Distribution**.



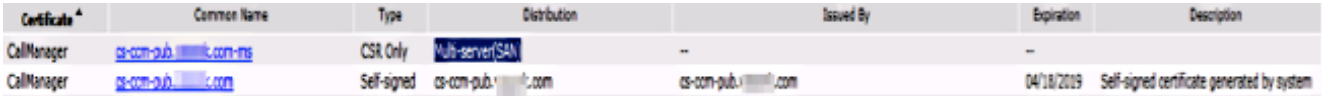
Это автозаполняет SAN домены и родительский домен.



Как только это генерируется, это отображается:



В Управлении сертификатами генерируется SAN Запрос:

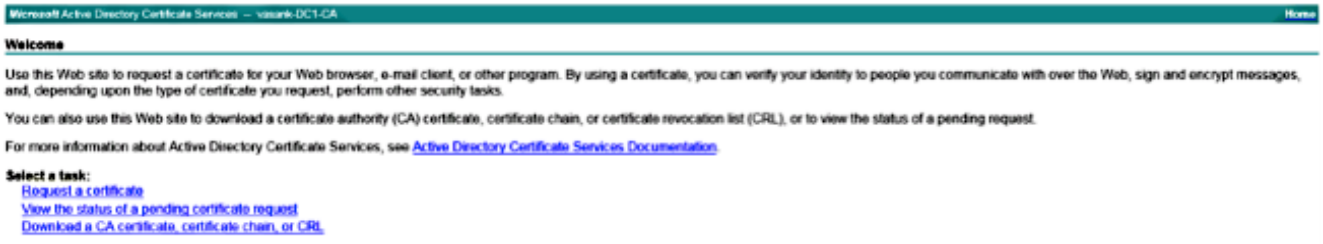


3. Можно использовать локальный CA или Внешний CA как VeriSign для получения подписанного. Данный пример показывает действия настройки для основанного на

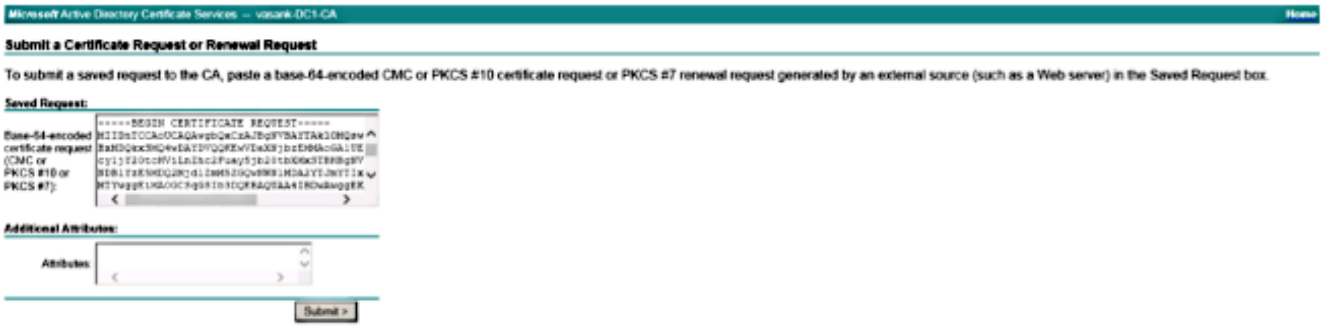
Microsoft Windows server CA.

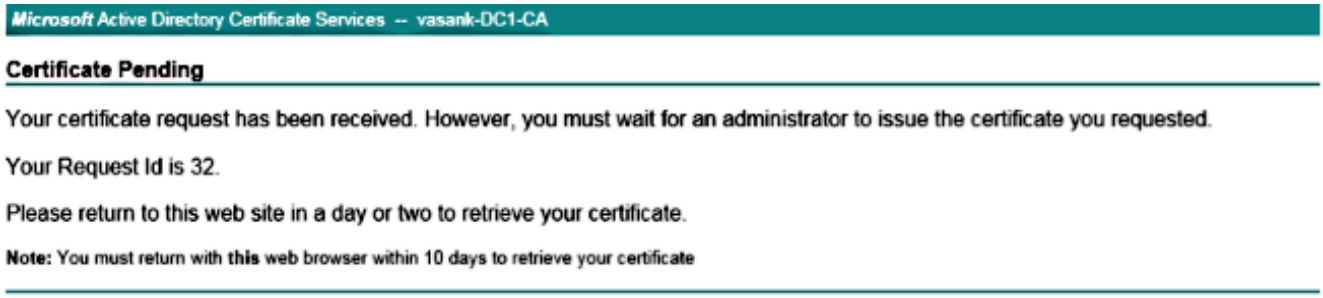
Войдите в https://<windowsserveripaddress>/certsrv/

Выберите **Request a Certificate> Advanced Certificate Request**.

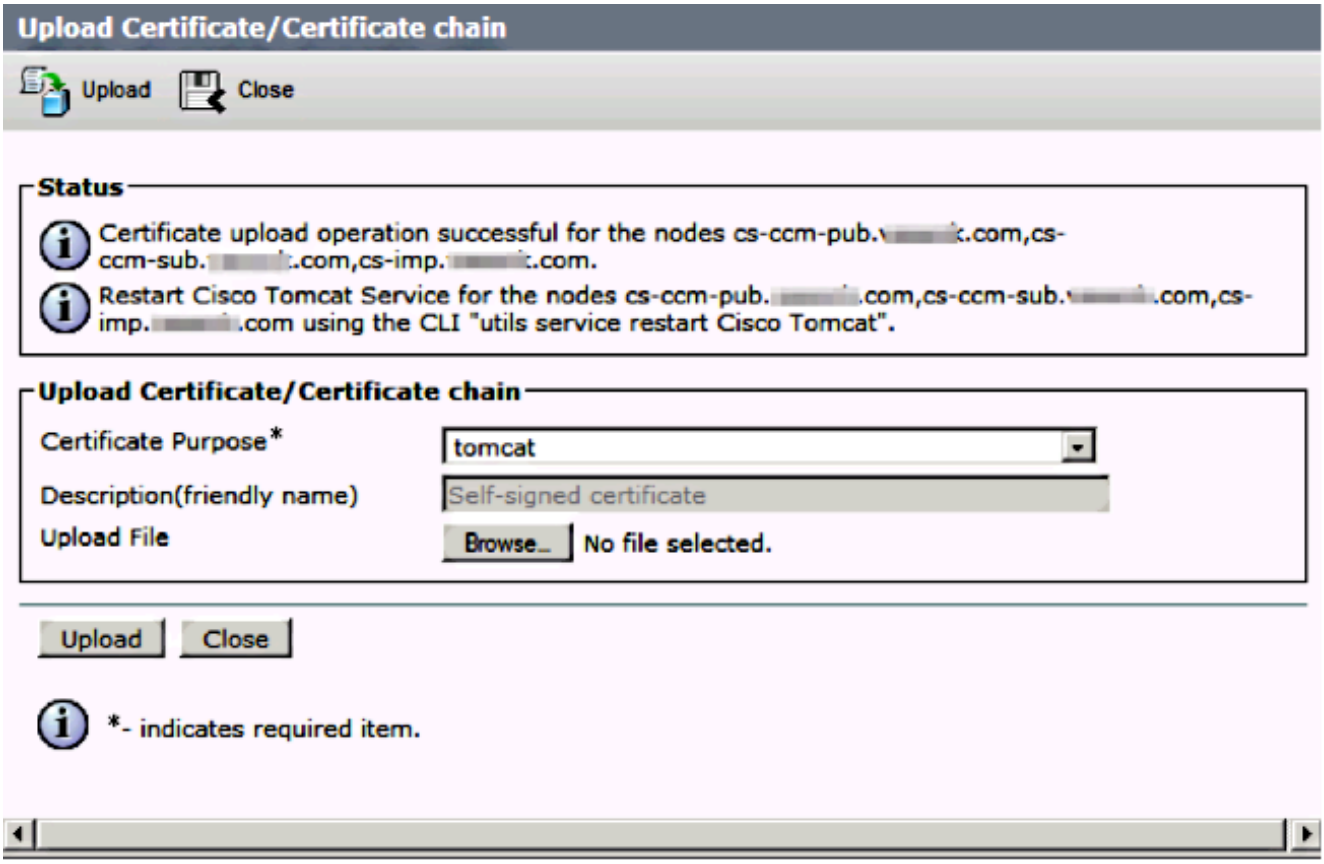


4. Отправьте запрос CSR как показано здесь.

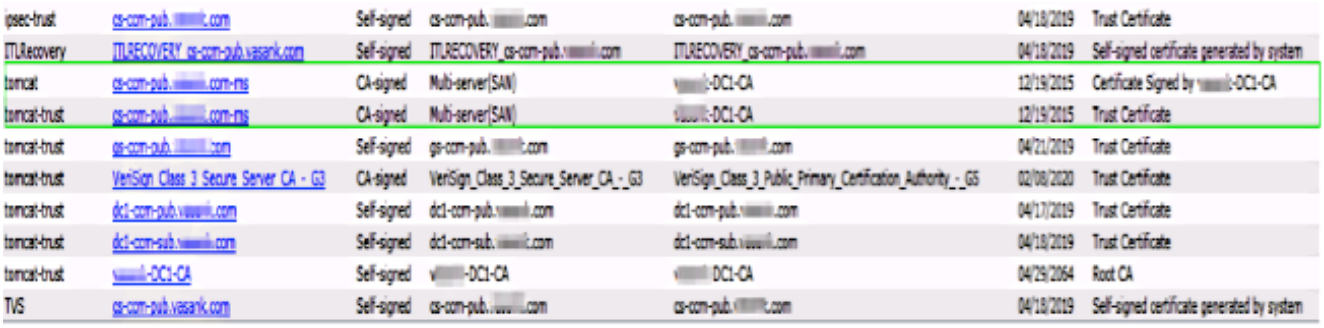




5. Как только вы получаете сертификат, необходимо загрузить сертификат CA, столь же трастовый tomcat, и затем загрузить Сертификат подписанный ЦС как tomcat.

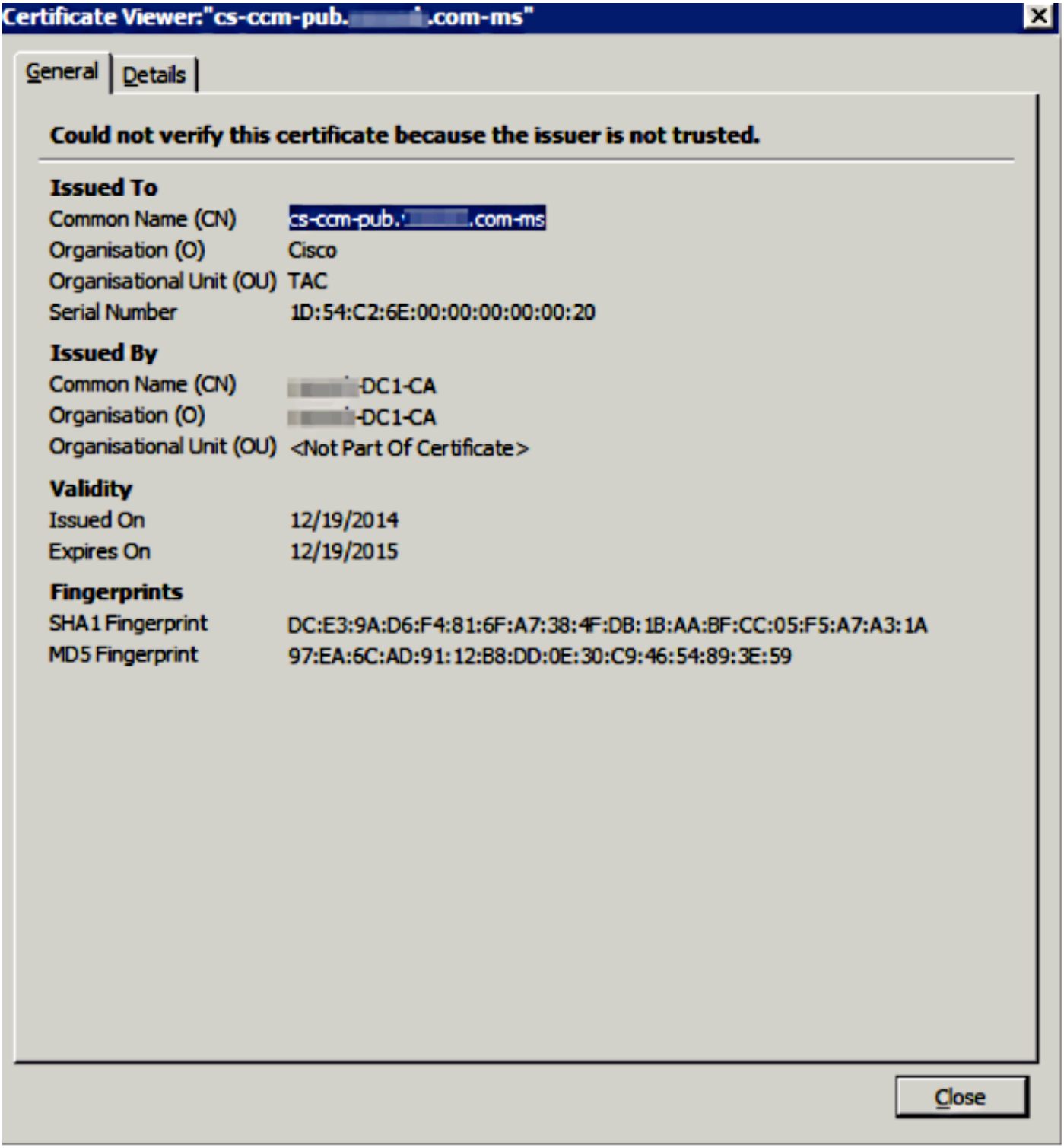


6. Гарантируйте, что сервис перезапущен на всех узлах в SAN списке, который включает узел, где это загружено. Вы видите SAN Мультисервера, перечисленный в Управлении сертификатами.



Проверка

Войдите в http://<fqdnofccm>:8443/ccmadmin, чтобы гарантировать, что используется новый сертификат.



Сертификат SAN мультисервера CallManager

Подобная процедура может быть выполнена для сертификата CallManager. В этом случае автозаполненные домены являются всеми узлами CallManager. Если это не работает, можно принять решение поддержать его от SAN списка или удалить его оттуда.

После установки сертификата, выполненного CA необходимо перезапустить Сервис CallManager на всех узлах.

Прежде чем вы получите подписанный CA SAN сертификат для CUCM, гарантируете что:

- IP-телефон в состоянии доверять службе проверки доверия (TVS). Это может быть

проверено при доступе к какому-либо сервису HTTPS с телефона. Например, если доступ Корпоративного каталога работает, то это означает, что телефон доверяет сервису TVS.
- Если это - безопасный кластер, гарантируйте, что клиент Списка надежных сертификатов (CTL) повторно выполнен так, чтобы новый файл CTL был создан, и кластер перезагружен.

Устранение неполадок

Эти журналы должны помочь Центру технической поддержки Cisco определять любые проблемы, отнесенные к генерации CSR SAN Мультисервера и загрузке Подписанного CA Certficate.

- Cisco унифицированный API платформы операционной системы
- Cisco Tomcat
- Платформа IPT журналы CertMgr

В существующем Мультисервере Certifcate CUCM, если имя хоста изменений сервера, рекомендуется генерировать запрос CSR SAN мультисервера, как объяснено ранее для подписывания сертификата CA.