Jabber завершенное руководство Инструкции для проверки достоверности сертификата

Содержание

Введение

Этот документ комбинирует несколько Ресурсов Cisco в завершенное, объединил руководство с практическими рекомендациями, которое используется для реализации всех требований для проверки достоверности сертификата в Cisco Jabber. Это необходимо, потому что Cisco Jabber теперь требует использования проверки достоверности сертификата для установления безопасных соединений с серверами. Это требование влечет за собой много изменений, которые могли бы требоваться для пользовательских сред.

> **Примечание:** Это руководство для собственных развертываний только. В настоящее время нет никакого изменения, требуемого для развертываний облачного сервиса, потому что они проверены против Общего Центра сертификации (CA).

На каких Клиентов Jabber влияет это изменение?

Вот таблица, которая перечисляет всех клиентов, которые внедряют проверку достоверности сертификата:

Таблица 1

Клиенты рабочего стола	Мобильный и клиенты планшета
Jabber для версии 9.2 Macintosh (сентябрь 2013) Jabber для Microsoft (MS) версия Windows 9.2.5 (сентябрь 2013)	Jabber для Версии 9.5 iPhone (октябрь 2 Jabber для iPhone и Версии 9.6 iPad (ноя 2013) Jabber для версии 9.6 Android (декабрь 2

Что это означает для среды Jabber?

Когда вы устанавливаете или обновляете любому клиенту, перечисленному в **Таблице 1**, обязательная проверка достоверности сертификата с серверами используется для безопасных соединений. По существу, когда Клиенты Jabber пытаются сделать безопасное соединение теперь, серверы предоставляют Cisco Jabber сертификаты. Cisco Jabber тогда пытается проверить те сертификаты против хранилища сертификата устройства. Если клиент не может проверить сертификат, он побуждает вас подтверждать, что вы хотите принять сертификат и разместить его в его Базу доверенных сертификатов Предприятия.

Какие сертификаты требуются?

Вот список собственных серверов и сертификатов, которые они представляют Cisco Jabber для установления безопасного соединения:

Таблица 2

Сервер	Сертификат
Cisco Unified Presence	HTTP (Tomcat) XMPP
IM Cisco Unified Communications Manager и присутствие	HTTP (Tomcat) XMPP
Cisco Unified Communications Manager	HTTP (Tomcat)
Cisco Unity Connection	HTTP (Tomcat)
Сервер совещаний WebEx Cisco	HTTP (Tomcat)

Вот некоторые важные моменты для замечания:

- Примените новое Сервисное обновление (SU) для Cisco Unified Presence (CUP) или IM Cisco Unified Communications Manager (CUCM) и Присутствия перед началом процесса подписания сертификата.
- Требуемые сертификаты применяются ко всем версиям сервера. Например, и Версия 8.x CUP и IM CUCM и Версия 9.x Присутствия и позже предоставляют клиенту Расширяемый Протокол Обмена сообщениями и Присутствия сертификаты HTTP и (XMPP).
- Каждый узел в кластере, абонентах и издателях, выполняет сервис Tomcat и может предоставить клиенту сертификат HTTP. Запланируйте подписать сертификаты для каждого узла в кластере.
- Для обеспечения Протокола SIP, сигнализирующего между клиентом и CUCM, используйте регистрацию Функции прокси центра сертификации (CAPF).

Какие методы доступны для проверки достоверности сертификата?

В настоящее время существует несколько методов проверки достоверности сертификации, которая может использоваться.

Способ 1: Пользователи просто **нажимают кнопку Принять** ко всем всплывающим окнам сертификата. Это могло бы быть большей частью идеального решения для небольших сред. Если вы **нажимаете кнопку Принять**, сертификаты размещены в Базу доверенных сертификатов Предприятия на устройстве. После того, как сертификаты размещены в Базу доверенных сертификатов Предприятия, пользователям больше не предлагают, когда они входят в Клиента Jabber на том локальном устройстве.

Способ 2: Требуемые сертификаты **(Таблица 2)** загружены от индивидуальных серверов (по умолчанию, это подписанные сертификаты), и установленный в Базу доверенных сертификатов Предприятия устройства пользователя. Если ваша среда не имеет доступа к Открытому или закрытому CA для подписания сертификата, это могло бы быть идеальным решением.

Несколько методов могут использоваться для продвижения этих сертификатов пользователям, но один быстрый метод должен использовать использование Реестра Microsoft Windows:

1. От одной из машин примите все сертификаты, которые представлены для Передачи бессмысленных данных в Базу доверенных сертификатов Предприятия.
2. Чтобы проверить, что сертификаты присутствуют, введите команду **Certmgr.msc** и перейдите к **Доверию Предприятия> Сертификаты**.
3. Открытый **Regedit** с **командой выполнения** и перешел к **HKCU> программное обеспечение> Microsoft> SystemCertificates> доверие> Сертификаты**.
4. Щелкните правой кнопкой мыши и экспортируйте папку Certifates в реестре как **.reg** файл.
5. Выставьте этот файл через Объект групповой политики (GPO) всем пользователям (или другой предпочтительный способ).

Это завершает установку Сертификатов Доверия Предприятия для Jabber, и пользователям больше не предлагают.

Метод 3: Общий или Частный CA **(Таблица 2)** подписывает все требуемые сертификаты. Это - рекомендуемый метод Cisco. Этот метод требует, чтобы Запрос подписи сертификата (CSR) генерировался для каждого из сертификатов, был подписан, повторно загружен к серверу, и затем импортирован в Хранилище полномочий Сертификата доверенного корня на устройствах пользователя. Посмотрите **Генерирование CSR** и**, Как я получаю сертификаты к хранилищам сертификата устройств пользователя?** разделы этого документа для получения дополнительной информации.

> **Примечание:** В случае Общественности CA, корневой сертификат должен уже быть в клиентской базе доверенных сертификатов.

Важно помнить, что Общие CAs, как правило, требуют CSR для приспосабливания определенным форматам. Например, общественность CA могла бы только принять CSR

что:

- Закодированы base64
- Не содержите определенные символы, такой как и!, в Организации, Подразделении (OU) или других полях
- Используйте определенные разрядные длины в открытом ключе для сервера

Аналогично при отправке CSR от нескольк узлов общий CAs мог бы потребовать, чтобы информация была последовательна во всех CSR.

Для предотвращения проблем с CSR рассмотрите требования формата от общественности CA, которой вы планируете отправить CSR. Затем гарантируйте, что информация, которую вы вводите при настройке сервера соответствует формату, которого CA требует общественность.

Вот возможное требование, с которым вы могли бы встретиться:

Один Сертификат На FQDN: Некоторые общие CAs подписывают только один сертификат на полное доменное имя (FQDN).

Например, для подписания HTTP и сертификатов XMPP для одиночного IM CUCM и узла Присутствия, вы, возможно, должны были бы отправить каждый CSR другому общему CAs.

Проверьте, самоподписан ли Сертификат или Подписан CA

> **Примечание:** Данный пример для Версии 8 CUCM. x. Процесс мог бы варьироваться между серверами.

1. Переместитесь к **Cisco по унифицированному администрированию ОС**.
2. Выберите **Security> Certificate Management**.
3. Найдите и нажмите **Трастовый Tomcat** файл **.pem Сертификата**.
4. Нажмите **Download** и **Save**.
5. Перейдите к файлу и переименуйте его с **.cer** расширением.
6. Откройте и просмотрите этот файл (пользователи MS Windows).
7. Проверьте **Выполненный** полем. Если это совпадает **с Выполненным к** полю, то сертификат Самоподписан (см. **Пример**).

Пример: Самоподписанный по сравнению с частным сертификатом подписанный ЦС

Самоподписанный	частный подписанный CA

Генерируйте CSR

> **Примечание:** Данный пример для Версии 8 CUCM. x. Процесс мог бы варьироваться между серверами.

1. Переместитесь к **Cisco по унифицированному администрированию ОС**.
2. Выберите **Security> Certificate Management**.

3. Нажмите **Generate CSR** и выберите **Tomcat** из выпадающего списка.
4. Нажмите **Generate CSR** и нажмите **Close**.
5. Нажмите **Download CSR** и выберите **Tomcat** из выпадающего списка.
6. Нажмите **Download CSR** и сохраните файл.
7. Передайте **.csr** файл, который будет подписан вашим Частным Сервером CA или Общим CA.
   Примечание: Как только у вас есть этот файл CSR, процесс варьируется на основе вашей среды.
8. Нажмите **Upload Certificate/Certificate под Безопасностью> Управление сертификатами** , Чтобы повторно загрузить новые подписанные сертификаты, которые были выполнены к вашему серверу.

Как делают меня сертификаты импорта в хранилища сертификата устройства пользователя?

Каждый серверный сертификат должен иметь связанный подарок корневого сертификата в базе доверенных сертификатов на устройстве пользователя. Cisco Jabber проверяет сертификаты, которые серверы представляют против корневых сертификатов в базе доверенных сертификатов.

Корневые сертификаты импорта в сертификат MS Windows хранят если:

- Сертификаты подписаны CA, который уже не существует в базе доверенных сертификатов, такой как частный CA. Если так, необходимо импортировать частный сертификат CA к хранилищу Доверенных корневых центров сертификации.
- Сертификаты самоподписаны. Если так, необходимо импортировать подписанные сертификаты к Базе доверенных сертификатов Предприятия.

Можно использовать любой соответствующий метод чтобы для сертификатов импорта в хранилище сертификата MS Windows, таких как:

- Используйте Мастера Импорта Сертификата чтобы для сертификатов импорта индивидуально.
- Разверните сертификаты на пользователях с программным средством командной строки CertMgr.exe на Сервере MS Windows. (Эта опция требует, чтобы вы использовали Инструментальное средство управления сертификатами, CertMgr.exe, не Консоль управления MS Сертификатов, CertMgr.msc.)
- Разверните сертификаты на пользователях с GPO на Сервере MS Windows.

  Примечание: Для подробных инструкций, о том, как сертификатам импорта, обратитесь к соответствующей документации MS.

Идентичность сервера в сертификатах

Как часть процесса подписания, CA задает идентичность сервера в сертификате. Когда клиент проверяет тот сертификат, он проверяет что:

- Доверяемые полномочия выполнили сертификат.

- Идентичность сервера, который представляет сертификат, совпадает с идентичностью сервера, заданного в сертификате.

  Примечание: Общие CAs обычно требуют FQDN как идентичности сервера, не IP-адреса.

Поля Identifier

Клиент проверяет эти поля identifier в серверных сертификатах для идентификационного соответствия:

Сертификаты XMPP

- SubjectAltName\OtherName\xmppAddr
- SubjectAltName\OtherName\srvName
- SubjectAltName\dnsNames
- Подчиненный CN

Сертификаты HTTP

- SubjectAltName\dnsNames
- Подчиненный CN

  Примечание: Поле Subject CN может содержать подстановочный знак (*) как крайний левый символ; например, *.cisco.com. Ваш CUCM, CUP и серверы Cisco Unity Connection не могли бы поддержать сертификаты подстановочного знака. (См. идентификатор ошибки Cisco усовершенствования CSCta14114).

Предотвратите идентификационное несоответствие

Когда Клиент Jabber пытается соединиться с сервером с IP-адресом, и серверный сертификат определяет сервер с FQDN, клиент не может определить сервер, как доверяется и побуждает пользователя. Так, если ваши серверные сертификаты определяют серверы с FQDNs, необходимо задать имя сервера как FQDN во многих местах на серверах.

Таблица 3 перечисляет все места, которые должны задать имя сервера, как это появляется в сертификате, является ли это IP-адресом или FQDN.

Таблица 3

Сервер	**Местоположение (Установка должна Совпасть с Сертификатом),**
Клиенты Cisco Jabber	Адрес Сервера входа в систему (Отличается для клиентов, обычно при **Настройках соединения),**
CUP (Версия 8.x и ранее)	** Все Имена узлов (**Система> Топология кластера)** **Внимание. :** Удостоверьтесь, что при изменении этого на FQDN можно решить это через DNS, или серверы остаются в начальном состоянии!

IM CUCM и Присутствие (Версия 9.x и позже)	Серверы TFTP (**Приложение> Cisco Jabber> Параметры настройки)** Основной и Вторичный Cisco IP Phone Cisco Call Manager (CCMCIP) (**Приложение> Cisco Jabber> Профиль CCMCIP)** Имя хоста голосовой почты (**Приложение> Cisco Jabber> Сервер голосов почты)** Название хранилища почты **(Приложение> Cisco Jabber> Хранилище поч** Имя хоста конференц-связи (**Приложение> Cisco Jabber> Сервер Конфер связи)** (Только Meeting Place) Домен XMPP (См. **Предоставление Домена XMPP к** разделу **Клиентов**), ** Все Имена узлов **(Система> Топология кластера**) **Внимание. :** Удостоверьтесь, что при изменении этого на FQDN можно решить это через DNS, или серверы остаются в начальном состоянии!
CUCM (Версия 8.x и ранее)	Серверы TFTP (**Приложение> Устаревшие Клиенты> Параметры настрой** Основной и Вторичный CCMCIP **(Приложение> Устаревшие Клиенты> Профиль CCMCIP)** Домен XMPP (См. **Предоставление Домена XMPP к** разделу **Клиентов**), Имя сервера **(System> Server)**
CUCM (Версия 9.x и позже)	Имя сервера **(System> Server)** IM и Сервер Присутствия (**Управление пользователями> Параметры пользователя> Сервис UC> IM и Присутствие)** Имя хоста голосовой почты **(Управление пользователями> Параметры пользователя> Сервис UC> Голосовая почта)** Название хранилища почты **(Управление пользователями> Параметры пользователя> Сервис UC> Хранилище почты)** Имя хоста конференц-связи (**(Управление пользователями> Параметры пользователя> Сервис UC> Конференц-связь)** (Только Meeting Place)
Cisco Unity Connection (Все версии)	**Никакое Изменение не необходимо**

Предоставьте домен XMPP клиентам

Клиент определяет сертификаты XMPP с доменом XMPP, а не с FQDN. Сертификаты XMPP должны содержать домен XMPP в поле identifier.

Когда клиент пытается соединиться с сервером присутствия, сервер присутствия предоставляет домен XMPP клиенту. Клиент может тогда проверить идентичность сервера присутствия против сертификата XMPP.

Выполните эти шаги, чтобы гарантировать, что сервер присутствия предоставляет домен XMPP клиенту:

1. Откройте интерфейс администрирования для своего сервера присутствия, или **Cisco Унифицированный IM CM и Интерфейс администрирования Присутствия** или **Интерфейс администрирования Cisco Unified Presence**.
2. Перейдите к **Системному> Security> Параметры настройки**.
3. Найдите раздел **Параметров настройки Сертификата XMPP**.
4. Задайте домен сервера присутствия в **Доменном имени для** поля **Subject Alternative Name Сервера к серверному сертификату XMPP**.
5. Проверьте флажок **Use Domain Name for XMPP Certificate Subject Alternative Name**.

6. **Нажмите Save.**
7. После того, как вы сохраните это изменение, необходимо восстановить сертификат **чашки-xmpp** на сервере.
8. Перезапустите **маршрутизатор XCP** для изменения для вступления в силу.

Внимание. : Перезапуск маршрутизатора XCP влияет на сервис.

Проверка достоверности сертификата теперь завершена!

Дополнительные сведения

- Cisco Jabber 9.2.5 Комментария к выпуску
- Cisco Jabber: обязательная проверка серверного сертификата TechNote
- Cisco Systems – техническая поддержка и документация