Получение клиентского сертификата и сертификата сервера

InfoWatch Traffic Monitor knowledge base

Exported on 11/12/2020

1 Table of Contents

2 Версия ТМ: 7.0

3 Выгрузка пользовательского сертификата:

1. Создайте учетную запись пользователя, для которого надо выпустить сертификат. При этом обязательно укажите email в контактных данных.
2. Зайдите в домен под этим пользователем.
3. Запустите приложение-консоль. Для этого в строке поиска Windows введите: `mmc.exe`
4. В консоли выполните **Файл-> Добавить или удалить оснастку** (**File -> Add/Remove snap-in**).
5. Выберите **Сертификаты** (**Certificates**), нажмите **Добавить** (**Add**), укажите оснастку ***Для моей учетной записи пользователя*** (***Certificates - Current user***), нажмите OK.
6. В появившемся дереве выполните **Личное -> Все задачи -> Запросить новый сертификат** (**Personal -> Add task -> Request New Certificate**).
7. В диалоговом окне нажмите **Далее** - в шагах 1-2, затем выберите **Новый Пользователь** (**New User**) и нажмите **Заявка** (**Enroll**).
8. Дождитесь успешного запроса сертификата и нажмите **Готово** (**Finish**).
9. Откройте окно с данными сертификата. На вкладке **Состав** (**Details**) выберите *Серийный номер* сертификата (*Serial Number*) и нажмите **Копировать в файл** (**Copy to File**). Будет загружен Мастер экспорта сертификатов. Нажмите **Далее.**
10. Выберите настройку **Да, экспортировать приватный ключ** (**Yes, export the private key**). Нажмите **Далее**.
11. Выберите, что выгрузить в файл сертификата (***.pfx**) и нажмите **Далее**.
12. Выберите пользователя, для которого выгружается сертификат. Поле *Пароль* не заполняйте. Нажмите **Далее**.
13. Задайте имя и путь для сохранения сертификата и нажмите **Далее**.
14. Будет создан файл с сертификатом. Нажмите **Готово.**

Далее следует переконвертировать файл ***.pfx** в pem-формат, который поддерживается Traffic Monitor.

4 Конвертация файла ***.pfx** в pem-формат:

1. Скопируйте получившийся ***.pfx** на сервер Traffic Monitor, например в `/root/testcert/xxx.pfx`
2. Выполните команду преобразования пользовательского сертификата без ключа:
   `openssl pkcs12 -in /root/testcert/test.pfx -nokeys -out /root/testcert/test.crt.pem`
3. В папке `/root/testcert/` проверьте наличие созданного **test.crt.pem.** Содержимое должно иметь примерно следующий вид:

   Обратите внимание на начало сертификата. Для пользовательского сертификата оно должно быть таким :
   Если у вас по какой-либо причине путей в сертификате будет два или он будет выглядеть подобным образом:

   Это может быть связано с выбором всех пунктов при выгрузке сертификата на шаге 11 предыдущей инструкции:
   В этом случае можно просто удалите первую часть сертификата и сохраните файл. Клиентский сертификат готов.

   
4. Выполните команду преобразования пользовательского ключа без сертификата:

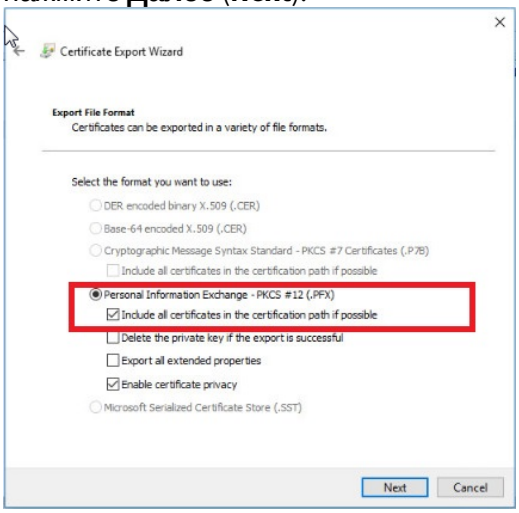
   `openssl pkcs12 -in  /root/testcert/test.pfx -nocerts -out  /root/testcert/test.key.pem`
5. В папке `/root/testcert/` проверьте наличие созданного **test.key.pem** и содержимое примерного вида:
6. Преобразуйте ключ сертификата в RSA командой:
   `openssl rsa -in /root/testcert/test.key.pem -out /root/testcert/test2.key.pem`
7. В итоге вы получите **test2.key.pem** примерного содержания:

Файл **test2.key.pem** будет являться ключом сертификата, файл **test.crt.pem** будет являться пользовательским сертификатом.

Далее нужно выгрузить ранее запрошенный сертификат сервера.

5 Выгрузка сертификата сервера:

1. Выполните шаги 9-10 аналогично выгрузке пользовательского сертификата
2. Отметьте следующим образом, что нужно выгрузить в файл сертификата (***.pfx**) и нажмите **Далее** (**Next**).



3. Выполните шаги 12-14 аналогично выгрузке пользовательского сертификата.

Далее переконвертируйте полученный сертификат в формат Traffic Monitor:

1. Скопируйте получившийся ***.pfx** на сервер Traffic Monitor, например в `/root/testservcert/xxx.pfx`
2. Выполните команду преобразования пользовательского сертификата без ключа: `openssl pkcs12 -in /root/testservcert/testserv.pfx -nokeys -out /root/testservcert/testserv.crt.pem`
3. В папке `/root/testservcert/` проверьте наличие созданного **testserv.crt.pem.** Содержимое должно иметь примерно следующий вид:

   Сертификат сервера готов.