Отчёт по лабораторной работе 5

Расширенная настройка HTTP-сервера Apache

Метвалли Ахмед Фарг Набеех

Содержание

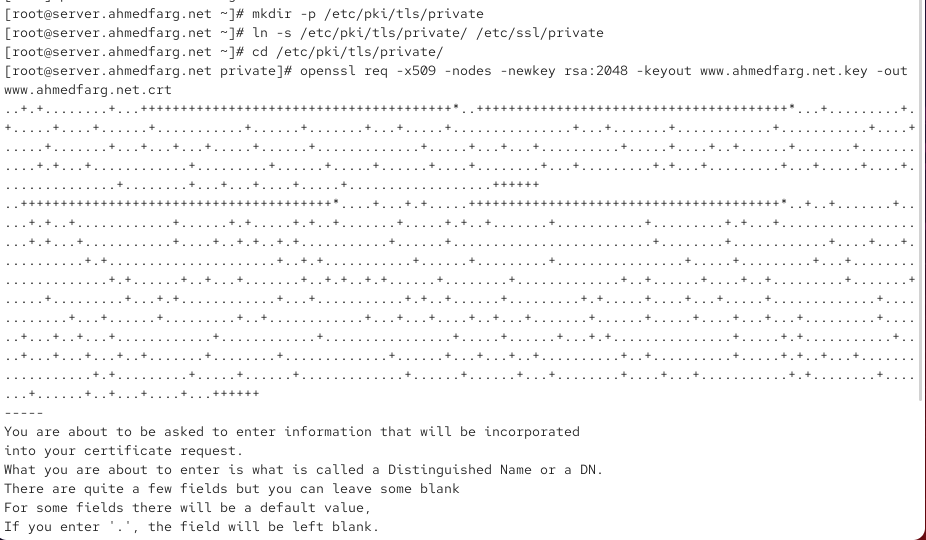
# 1 Цель работы

Приобретение практических навыков по расширенному конфигурированию HTTPсервера Apache в части безопасности и возможности использования PHP.

# 2 Выполнение

## 2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS

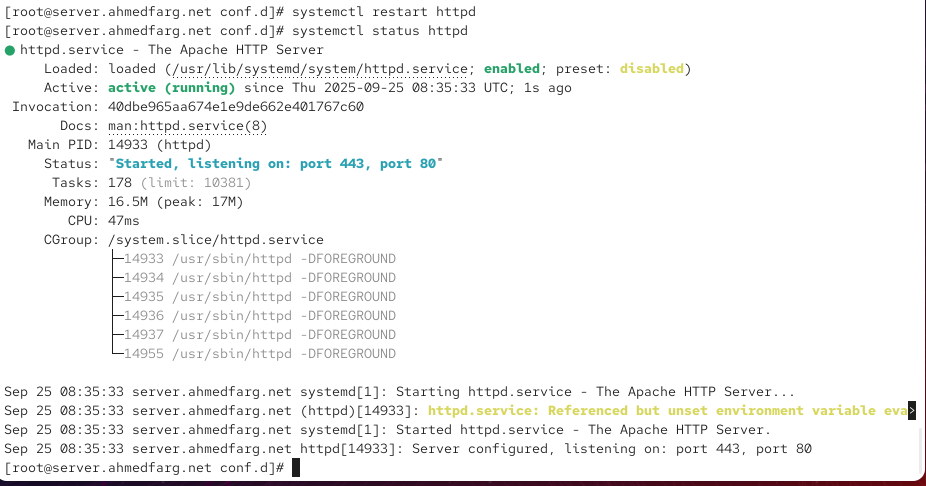
1. На сервере создан каталог для хранения закрытых ключей и сертификатов, а также выполнена генерация самоподписанного сертификата и ключа для домена www.ahmedfarg.net:
   * ключ www.ahmedfarg.net.key сохранён в /etc/ssl/private,
   * сертификат www.ahmedfarg.net.crt помещён в каталог /etc/ssl/certs.

* 
* Рис. 1: Генерация ключа и сертификата

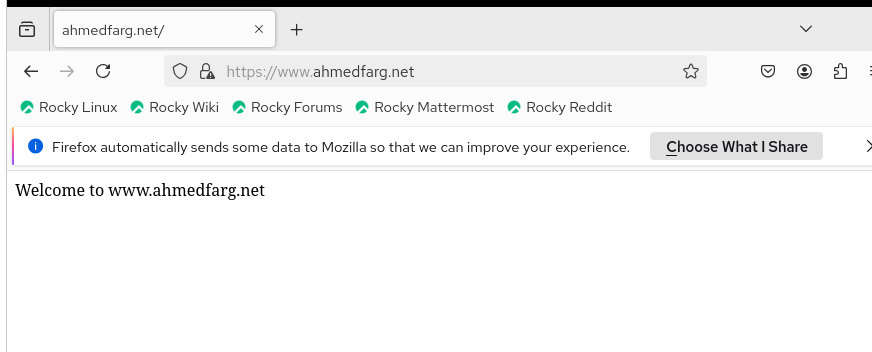
1. В каталоге /etc/httpd/conf.d создан конфигурационный файл www.ahmedfarg.net.conf, где определены два виртуальных хоста:
   * для порта **80** — выполняется перенаправление всех HTTP-запросов на HTTPS,
   * для порта **443** — включено использование SSL с указанием сертификата и закрытого ключа.

* 
* Рис. 2: Конфигурация виртуальных хостов

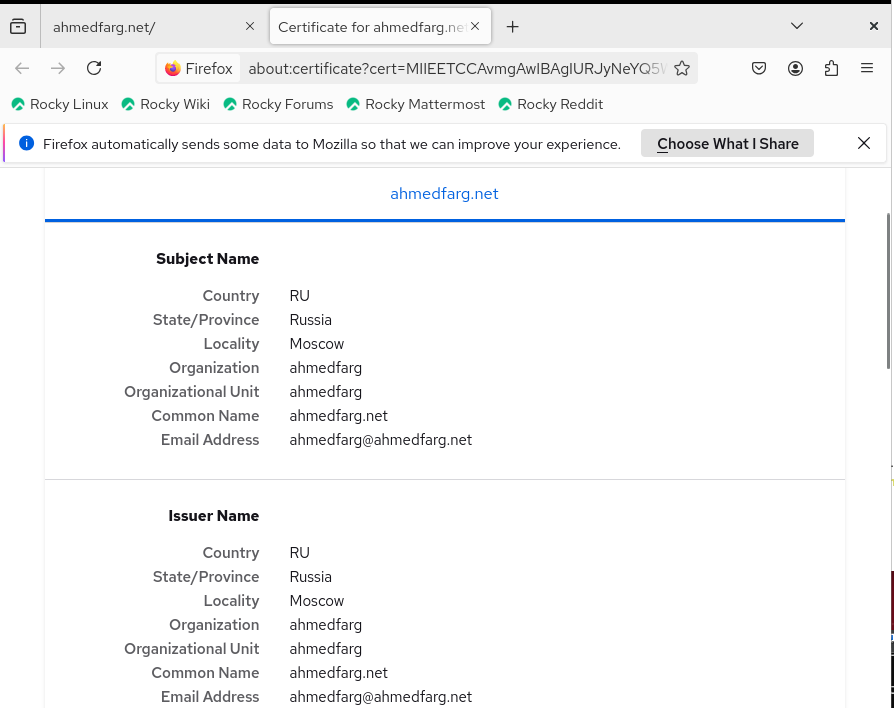
1. После внесения изменений веб-сервер Apache был перезапущен. Его статус показывает успешный запуск и работу на портах 80 и 443.

* 
* Рис. 3: Перезапуск Apache и проверка статуса

1. На клиентской машине в браузере выполнена проверка доступа к сайту https://www.ahmedfarg.net. Отобразилась стартовая страница веб-сервера с сообщением:

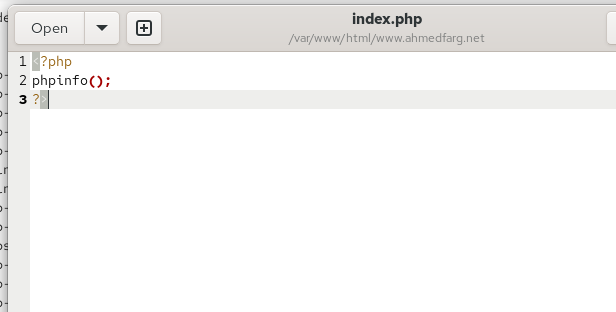
* **Welcome to www.ahmedfarg.net**
* 
* Рис. 4: Доступ к сайту через HTTPS

1. Содержание сертификата подтверждает корректное заполнение полей:
   * страна — RU,
   * регион — Russia,
   * город — Moscow,
   * организация и подразделение — ahmedfarg,
   * CN (Common Name) — www.ahmedfarg.net,
   * email — ahmedfarg@ahmedfarg.net.

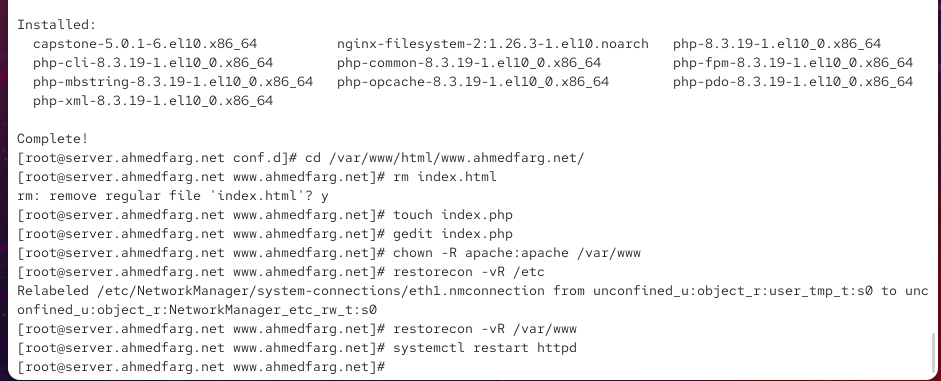
* 
* Рис. 5: Информация о сертификате

## 2.2 Конфигурирование HTTP-сервера для работы с PHP

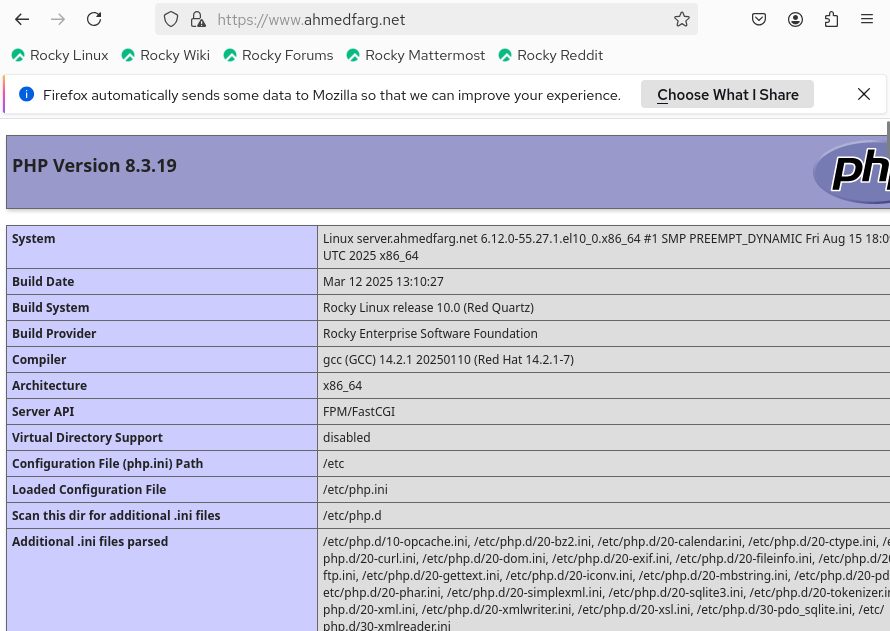
1. На сервер были установлены необходимые пакеты для поддержки PHP.
2. В каталоге /var/www/html/www.ahmedfarg.net файл index.html был заменён на index.php, содержащий вызов функции phpinfo().

* 
* Рис. 6: Файл index.php

1. Для корректной работы веб-сервера были изменены права доступа на каталог /var/www и восстановлен контекст безопасности SELinux. После этого HTTP-сервер был перезапущен.

* 
* Рис. 7: Настройка прав доступа и перезапуск Apache

1. На клиентской машине при обращении к сайту https://www.ahmedfarg.net отобразилась информация о конфигурации PHP, что подтверждает успешное подключение модуля.

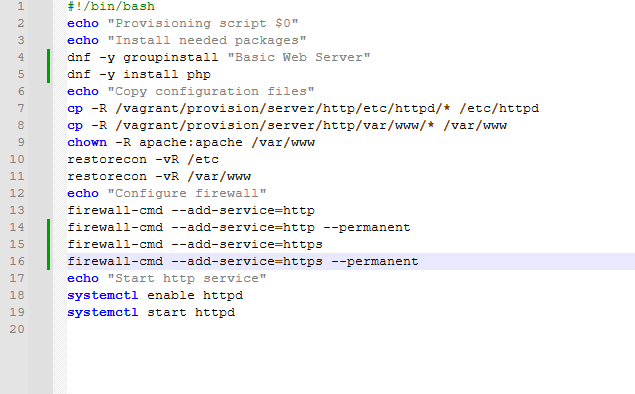
* 
* Рис. 8: Проверка работы PHP в браузере

## 2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. Конфигурационные файлы HTTP-сервера и веб-контента были скопированы в каталог /vagrant/provision/server/http для дальнейшего использования при автоматическом развёртывании.

* 
* Рис. 9: Копирование конфигурационных файлов

1. В скрипт /vagrant/provision/server/http.sh были внесены изменения:
   * добавлена установка PHP,
   * произведена настройка межсетевого экрана с разрешением работы по протоколам HTTP и HTTPS,
   * реализован запуск службы Apache при старте системы.

* 
* Рис. 10: Обновлённый скрипт http.sh

# 3 Заключение

HTTP-сервер был успешно сконфигурирован для работы по протоколу HTTPS, сгенерирован самоподписанный SSL-сертификат и настроено автоматическое перенаправление с порта 80 на 443. Далее сервер был дополнительно настроен для обработки PHP-скриптов, что было подтверждено выводом страницы phpinfo(). Конфигурация и сертификаты сохранены в каталоге Vagrant для последующего автоматического развёртывания.

# 4 Контрольные вопросы

1. **В чём отличие HTTP от HTTPS?**  
   HTTP передаёт данные в открытом виде, а HTTPS использует SSL/TLS для их шифрования, что обеспечивает конфиденциальность и защищает от перехвата.
2. **Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?**  
   Безопасность достигается с помощью шифрования данных, проверки подлинности сервера с использованием SSL-сертификата и защиты от атак типа «man-in-the-middle».
3. **Что такое сертификационный центр? Приведите пример.**  
   Сертификационный центр (CA) — доверенная организация, выпускающая цифровые сертификаты для подтверждения подлинности сайтов и шифрования соединений. Примеры: DigiCert, GlobalSign, Let’s Encrypt.