Отчёт по лабораторной работе 5

Расширенная настройка HTTP-сервера Apache

Элсаиед Адел

Содержание

Список иллюстраций

Список таблиц

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 и PHP

1. На виртуальной машине **server** в режиме суперпользователя был создан каталог для хранения закрытых ключей SSL `/etc/pki/tls/private`, а также символьная ссылка `/etc/ssl/private`, обеспечивающая совместимость с принятыми путями размещения SSL-ключей. После этого с использованием утилиты OpenSSL был сгенерирован самоподписанный SSL-сертификат и закрытый ключ длиной 2048 бит для доменного имени `www.elsaiedadel.net`.

   В процессе генерации были заполнены поля Distinguished Name: код страны — RU, страна — Russia, город — Moscow, организация и подразделение — elsaiedadel, общее имя (CN) — elsaiedadel.net, адрес электронной почты — elsaiedadel@elsaiedadel.net. Сгенерированный сертификат был перемещён в каталог `/etc/ssl/certs`.

Рис. 2.1: Генерация SSL-сертификата и ключа OpenSSL

2. После завершения генерации сертификата была выполнена проверка наличия созданных файлов в каталоге `/etc/pki/tls/private`, после чего сертификат `www.elsaiedadel.net.crt` был скопирован в системный каталог сертификатов `/etc/ssl/certs`, предназначенный для использования веб-сервером Apache.

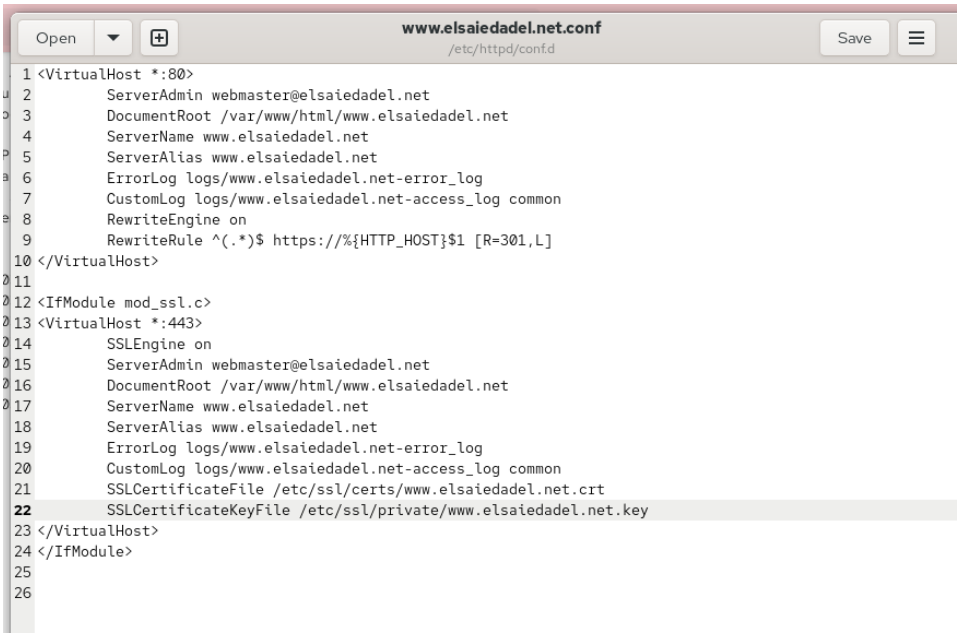

Рис. 2.2: Проверка и копирование SSL-сертификата

3. Для перевода веб-сервера на работу по протоколу HTTPS был отредактирован конфигурационный файл виртуального хоста `/etc/httpd/conf.d/www.elsaiedadel.ne`
   В секции `<VirtualHost *:80>` настроено автоматическое перенаправление всех HTTP-запросов на HTTPS с использованием механизма `RewriteRule`.
   В секции `<VirtualHost *:443>` активирован SSL-модуль, указаны пути к файлам сертификата и закрытого ключа, а также заданы основные параметры виртуального хоста, включая имя сервера, каталог веб-документов и файлы журналов.

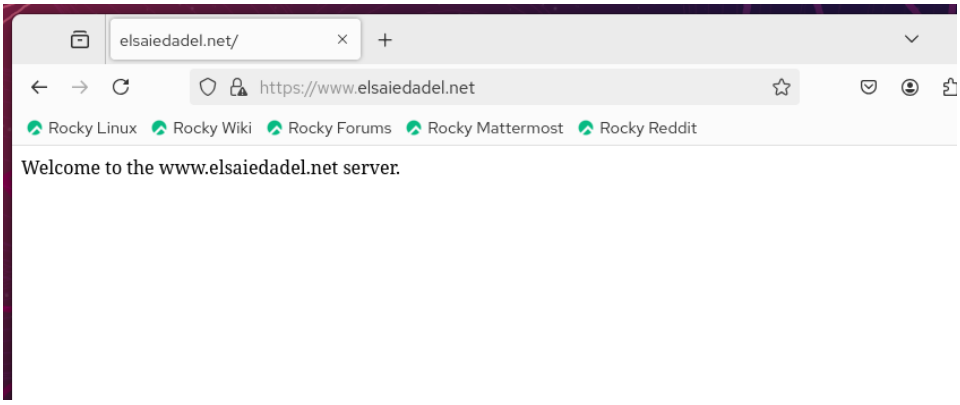

Рис. 2.3: Конфигурация виртуального хоста Apache для HTTPS

4. После применения конфигурации был выполнен доступ к веб-серверу из браузера клиентской виртуальной машины. При обращении к адресу `www.elsaiedadel.net` было зафиксировано автоматическое перенаправление на защищённое соединение HTTPS. Браузер уведомил о том, что сертификат является самоподписанным, после чего адрес сервера был добавлен в список доверенных исключений.

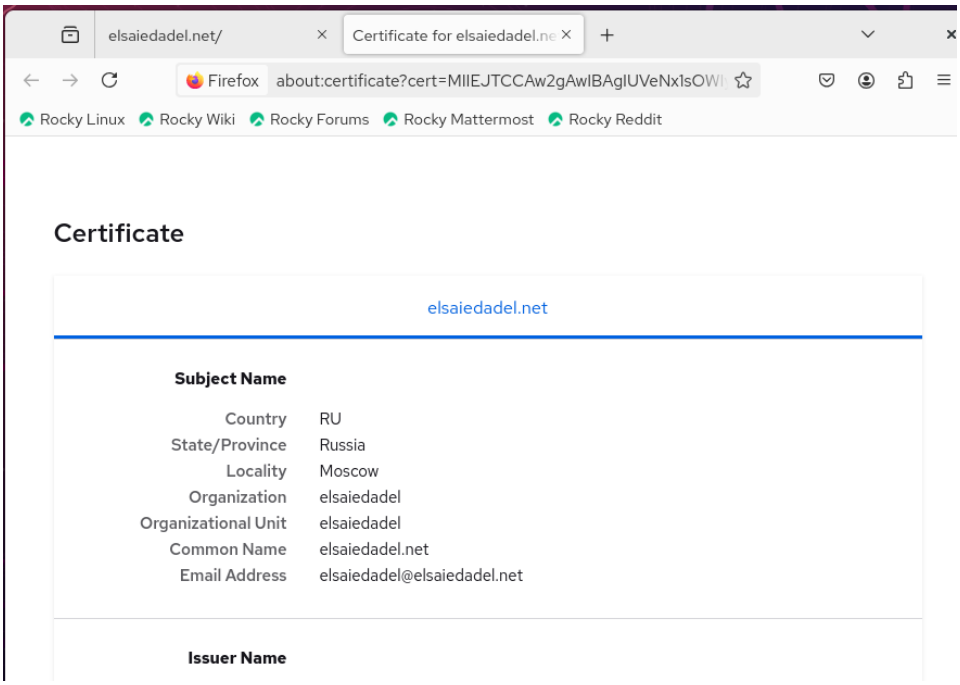

Рис. 2.4: Проверка HTTPS-подключения в браузере

5. В интерфейсе браузера было просмотрено содержимое установленного SSL-сертификата. В сертификате подтверждено соответствие полей Subject Name заданным значениям, включая доменное имя сервера, организацию и адрес электронной почты, что свидетельствует о корректной генерации и применении сертификата.

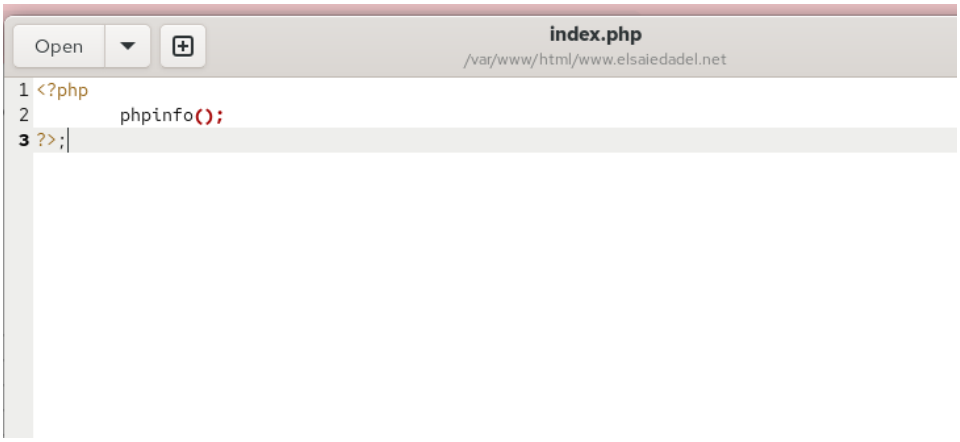

Рис. 2.5: Просмотр сведений SSL-сертификата

6. Для проверки работы PHP на веб-сервере в каталоге `/var/www/html/www.elsaiedadel.net` был создан файл `index.php`, содержащий вызов функции `phpinfo()`. После этого при обращении к серверу через браузер была успешно отображена страница с информацией о версии PHP и параметрах окружения.

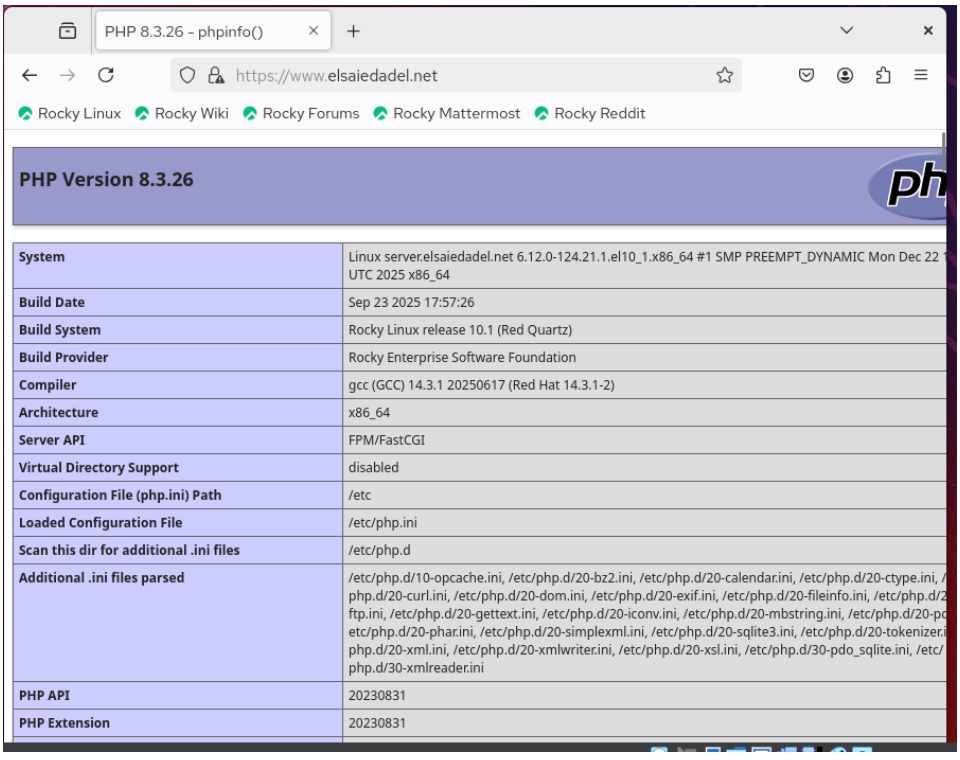

Рис. 2.6: Создание PHP-файла index.php

7. В результате загрузки страницы `index.php` в браузере была выведена информация о версии PHP 8.3.26, конфигурации PHP-FPM, параметрах сборки и используемых расширениях, что подтверждает корректную установку и функционирование PHP на веб-сервере Apache.

```
[root@server.elsaiedadel.net www.elsaiedadel.net]#
[root@server.elsaiedadel.net www.elsaiedadel.net]# cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/conf.d/
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/autoindex.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/fcgid.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/manual.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/README'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/server.elsaiedadel.net.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/ssl.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/userdir.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/welcome.conf'? y
cp: overwrite '/vagrant/provision/server/http/etc/httpd/conf.d/www.elsaiedadel.net.conf'? y
[root@server.elsaiedadel.net www.elsaiedadel.net]# cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html/
cp: overwrite '/vagrant/provision/server/http/var/www/html/server.elsaiedadel.net/index.html'? y
[root@server.elsaiedadel.net www.elsaiedadel.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
[root@server.elsaiedadel.net www.elsaiedadel.net]# mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
[root@server.elsaiedadel.net www.elsaiedadel.net]#
[root@server.elsaiedadel.net www.elsaiedadel.net]# cp -R /etc/pki/tls/private/www.elsaiedadel.net.key /vagrant/provision/server/http
/etc/pki/tls/private
[root@server.elsaiedadel.net www.elsaiedadel.net]# cp -R /etc/pki/tls/private/www.elsaiedadel.net.crt /vagrant/provision/server/http
/etc/pki/tls/certs/
[root@server.elsaiedadel.net www.elsaiedadel.net]#
```

Рис. 2.7: Отображение страницы phpinfo()

8. Для сохранения внесённых изменений в систему автоматического развёртывания были скопированы конфигурационные файлы Apache, содержимое каталога веб-документов, а также файлы SSL-сертификата и закрытого ключа в каталог `/vagrant/provision/server/http`.
   Дополнительно был модифицирован provisioning-скрипт `http.sh`, в который добавлены установка PHP, настройка межсетевого экрана для разрешения HTTPS-трафика, восстановление контекста SELinux и автоматический запуск сервиса httpd при старте системы.

Vagrantfile | dhcp.sh | http.sh

```
#!/bin/bash
echo "Provisioning script $0"
echo "Install needed packages"
dnf -y groupinstall "Basic Web Server"
dnf -y install php
echo "Copy configuration files"
cp -R /vagrant/provision/server/http/etc/httpd/* /etc/httpd
cp -R /vagrant/provision/server/http/var/www/* /var/www
chown -R apache:apache /var/www
restorecon -vR /etc
restorecon -vR /var/www
echo "Configure firewall"
firewall-cmd --add-service=http
firewall-cmd --add-service=http --permanent
firewall-cmd --add-service=https
firewall-cmd --add-service=https --permanent
echo "Start http service"
systemctl enable httpd
systemctl start httpd
```

Рис. 2.8: Обновление provisioning-скрипта и копирование конфигураций

3 Вывод

В ходе выполнения лабораторной работы было выполнено конфигурирование HTTP-сервера для работы через защищённый протокол HTTPS. На сервере был сгенерирован самоподписанный SSL-сертификат и настроен виртуальный хост Apache с поддержкой шифрованного соединения и автоматическим перенаправлением HTTP-запросов на HTTPS. Произведена настройка межсетевого экрана, разрешающая работу сервиса HTTPS, а также выполнена установка и проверка корректного функционирования PHP. Дополнительно были внесены изменения в provisioning-скрипты Vagrant, обеспечивающие автоматическое развёртывание веб-сервера с поддержкой HTTPS и PHP. Результаты проверки подтвердили корректную работу защищённого веб-доступа и серверной обработки PHP-скриптов.

4 Контрольные вопросы

1. В чём отличие HTTP от HTTPS?

HTTP — это протокол передачи данных прикладного уровня, обеспечивающий обмен информацией между клиентом и сервером в открытом виде без механизмов шифрования и проверки подлинности. HTTPS является расширением HTTP, использующим протокол TLS/SSL, который обеспечивает шифрование передаваемых данных, аутентификацию сервера и контроль целостности информации, что позволяет защитить соединение от перехвата и подмены данных.

2. Каким образом обеспечивается безопасность контента веб-сервера при работе через HTTPS?

Безопасность при использовании HTTPS обеспечивается за счёт применения криптографических алгоритмов протокола TLS/SSL. В процессе установки соединения происходит обмен ключами, после чего весь передаваемый трафик шифруется симметричными алгоритмами. Цифровой сертификат сервера позволяет клиенту убедиться в подлинности веб-сайта, а механизмы контроля целостности данных предотвращают незаметное изменение информации в процессе передачи.

3. Что такое сертификационный центр? Приведите пример.

Сертификационный центр — это доверенная организация, занимающаяся выпуском, подписанием и управлением цифровыми сертификатами, используемыми для подтверждения подлинности серверов и шифрования соединений. Сертификационный центр удостоверяет соответствие доменного имени владельцу сертификата и формирует цепочку доверия между клиентом и сервером. При-

мером сертификационного центра является Let’s Encrypt, предоставляющий бесплатные SSL/TLS-сертификаты для веб-сайтов.