Лабораторная работа №5

Расширенная настройка HTTP-сервера Apache

Демидова Екатерина Алексеевна

Содержание

# 1 Цель работы

Приобретение практических навыков по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.

# 2 Задание

1. Сгенерируйте криптографический ключ и самоподписанный сертификат безопасности для возможности перехода веб-сервера от работы через протокол HTTP к работе через протокол HTTPS.
2. Настройте веб-сервер для работы с PHP.
3. Напишите (или скорректируйте) скрипт для Vagrant, фиксирующий действия по расширенной настройке HTTP-сервера во внутреннем окружении виртуальной машины server.

# 3 Выполнение лабораторной работы

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

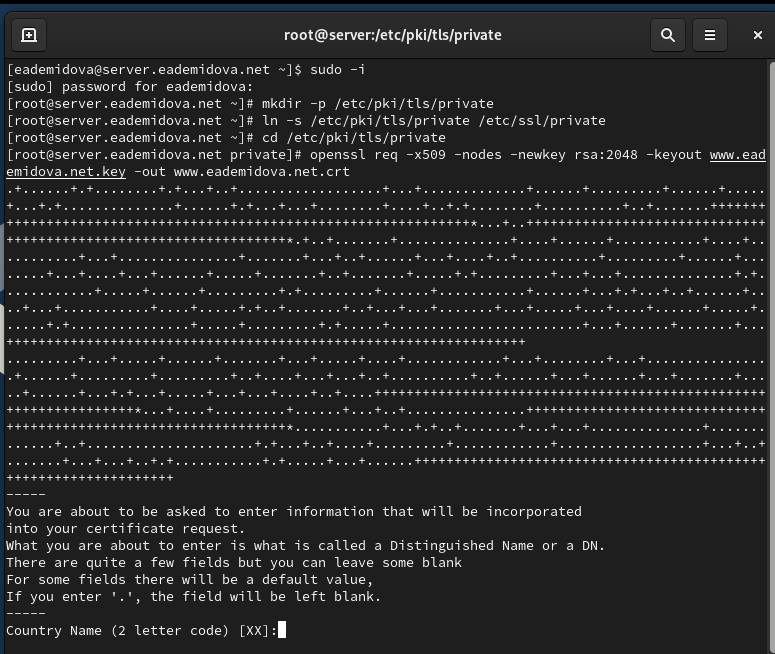
Загрузим нашу операционную систему и перейдем в рабочий каталог с проектом:

cd /var/tmp/eademidova/vagran

Затем запустим виртуальную машину server:

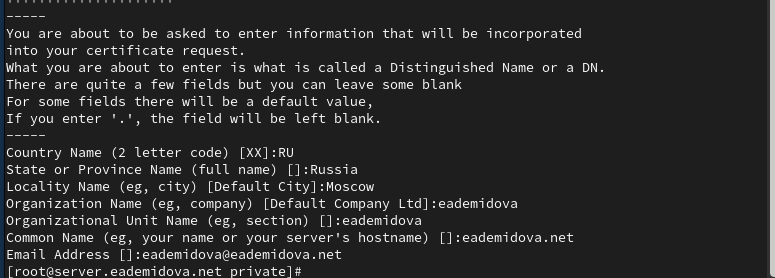
make server-up

На виртуальной машине server войдем под созданным в предыдущей работе пользователем и откроем терминал. Перейдем в режим суперпользователя. В каталоге /etc/ssl создадим каталог private сгенерируем ключ и сертификат, используя следующую команду (рис. ??):



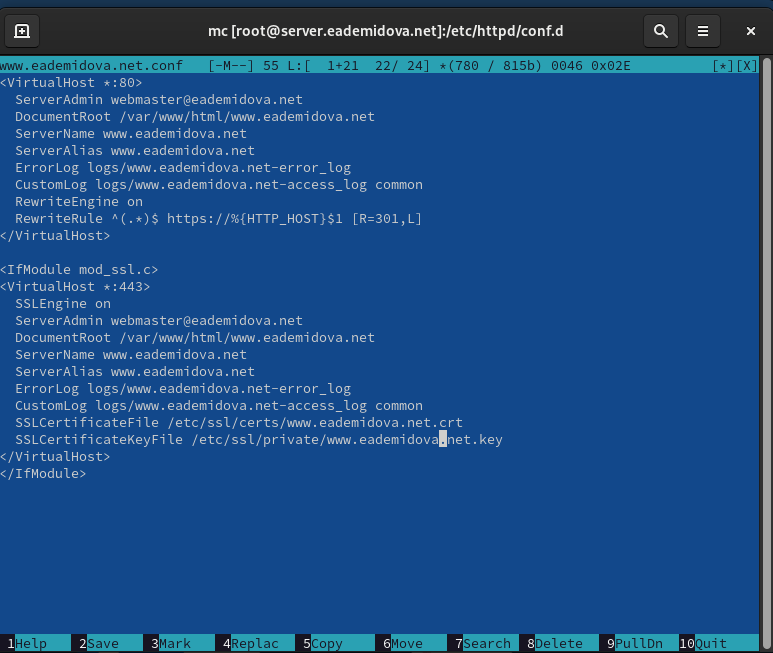
Создание каталога и генерация ключа и сертификата

Далее заполним сертификат(рис. ??):



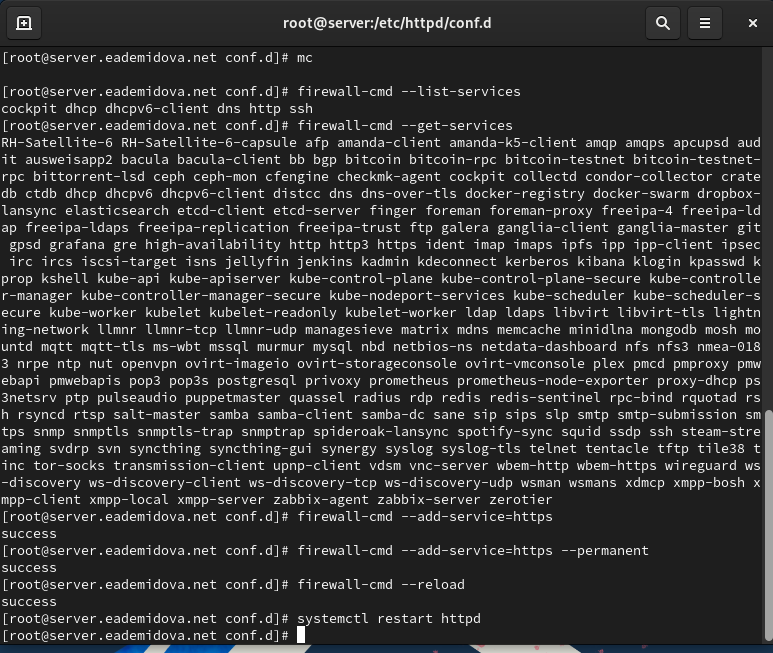
Заполнение сертификата

Для перехода веб-сервера www.eademidova.net на функционирование через протокол HTTPS требуется изменить его конфигурационный файл. Перейдем в каталог с конфигурационными файлами(рис. ??):



Изменение конфигурационного файла www.eademidova.net.conf

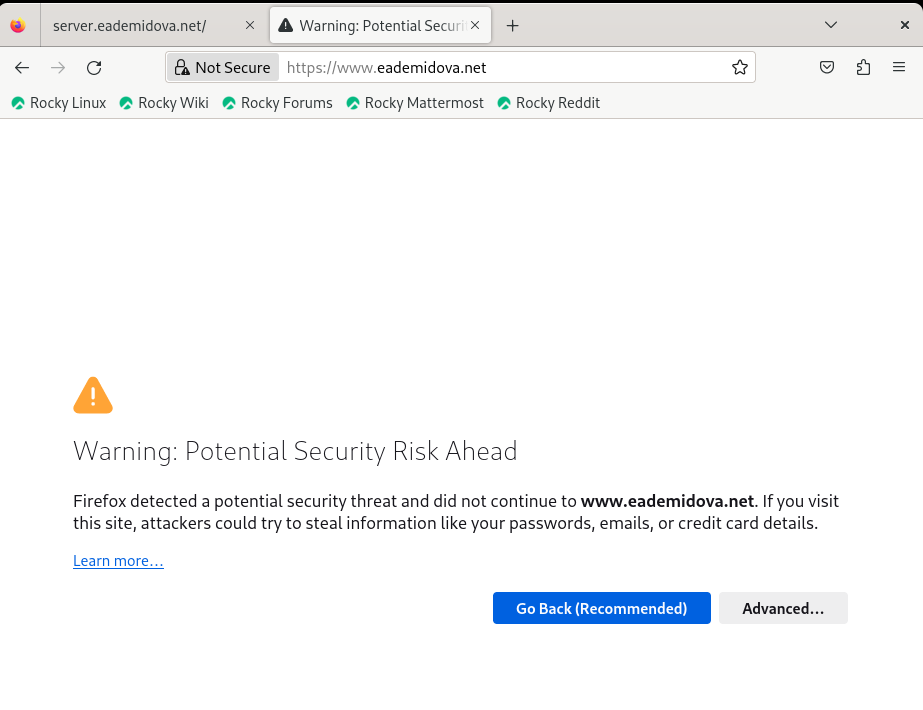
Внесем изменения в настройки межсетевого экрана на сервере, разрешив работу с https и перезапустим веб-сервер(рис. ??):



Всенесение в нстройки межсетевого экрана и перезапуск веб-сервера

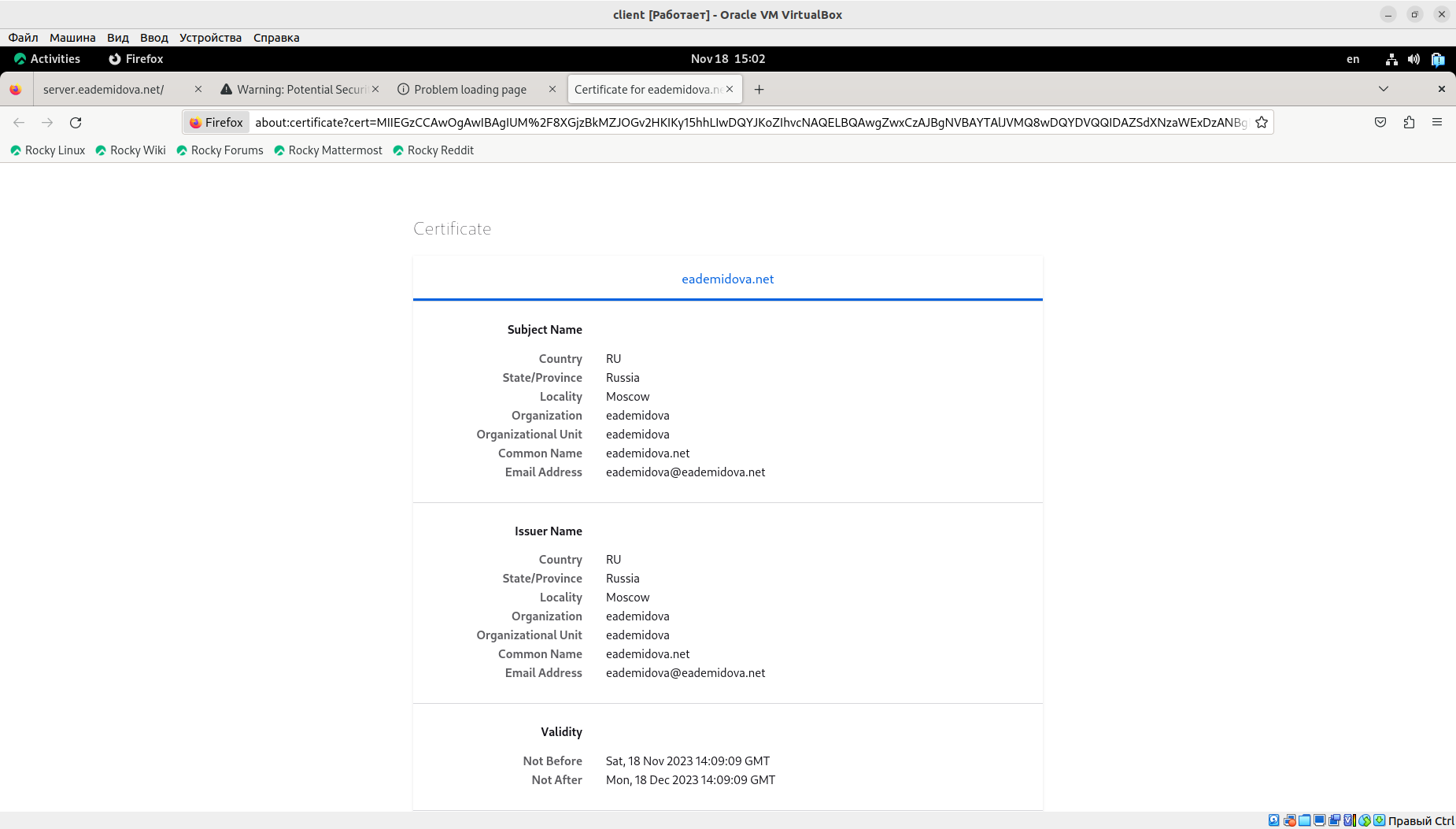
Здесь в первом блоке указывается сервера администратора, указан файл, который используется для запроса, затем имя сервера, альтернативное имя хоста(в нашем случае такое же как основное), лог файл ошибок, лог файл расположения и журнала досутпа, включен механизм перезаписи, запрошенных URL-адресов и правило перезаписи. Во втором блоке настраивается ssl-доступ. Здесь порт 443. Кроме указанных в предыдущем блоке строк, также указан файл ssl-сертификата и его ключ.

На виртуальной машине client в строке браузера введем название веб-сервера www.eademidova.net и убедимся, что произойдёт автоматическое переключение на работу по протоколу HTTPS(рис. ??):



Сообщение о незащищенности соединения

На открывшейся странице с сообщением о незащищённости соединения нажмем кнопку «Дополнительно», затем добавим адрес нашего сервера в постоянные исключения. Затем просмотрим содержание сертификата (нажав на значок с замком в адресной строке и кнопку «Подробнее»)(??):



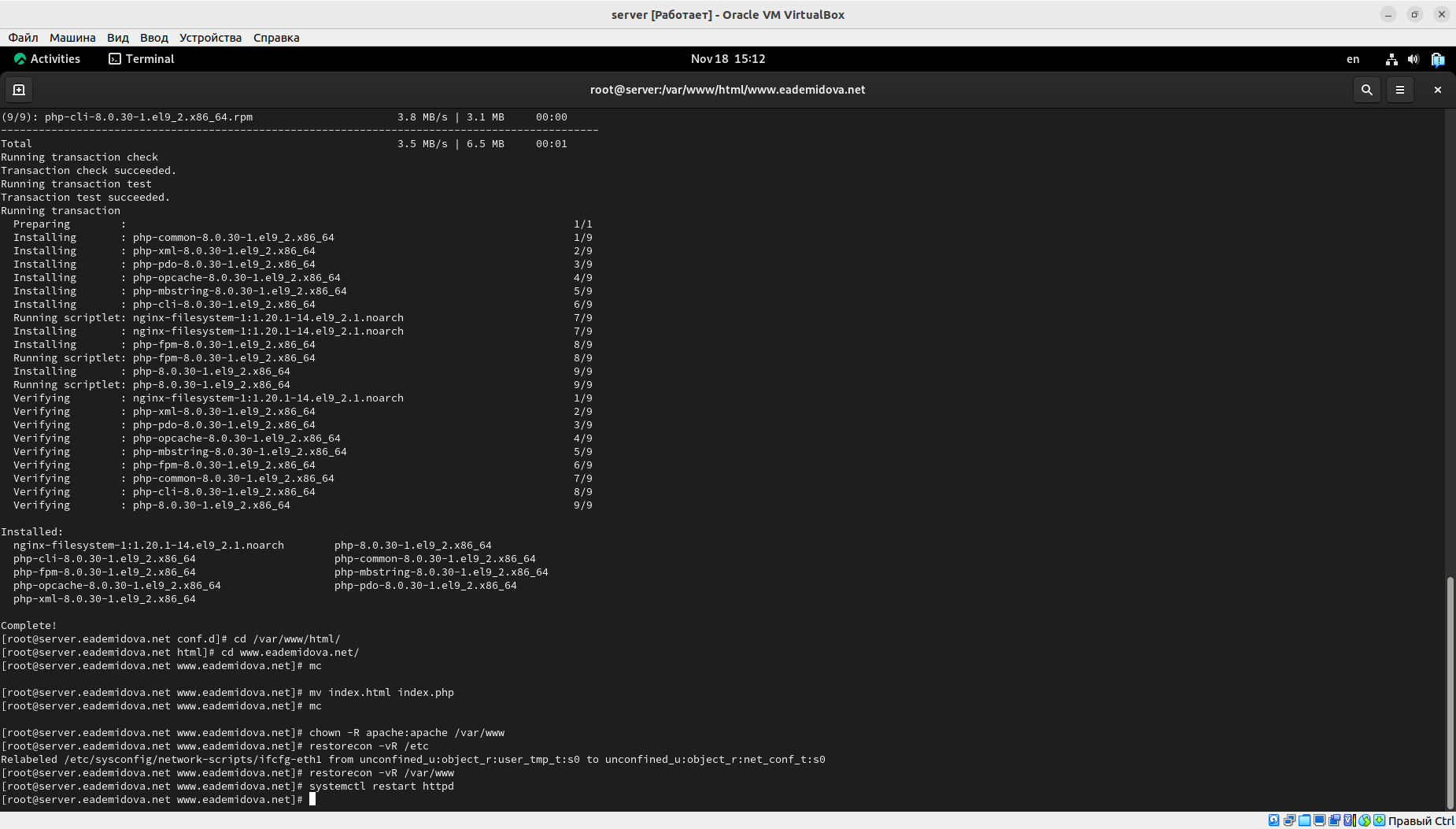
Просмотр содержания сертификата

## 3.2 Конфигурирование HTTP-сервера для работы с PHP

Установим пакеты для работы с PHP, затем в каталоге /var/www/html/www.eademidova.net заменим файл index.html на index.php следующего содержания:

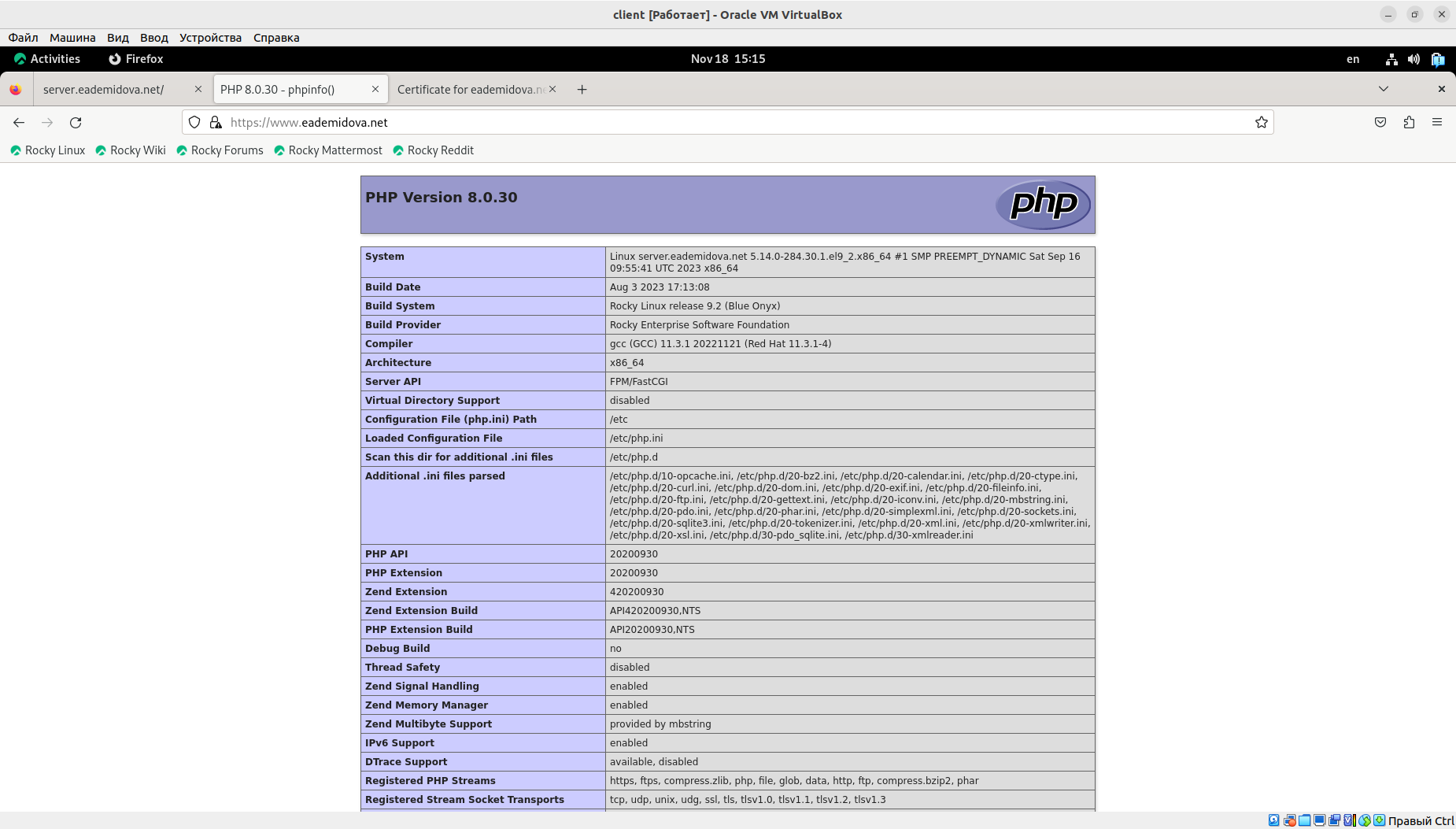
<?php  
phpinfo();  
?>

Cкорректируем права доступа в каталог с веб-контентом, восстановим контекст безопасности в SELinux и перезапустим HTTP-сервер(??):



Конфигурирование HTTP-сервера для работы с PHP

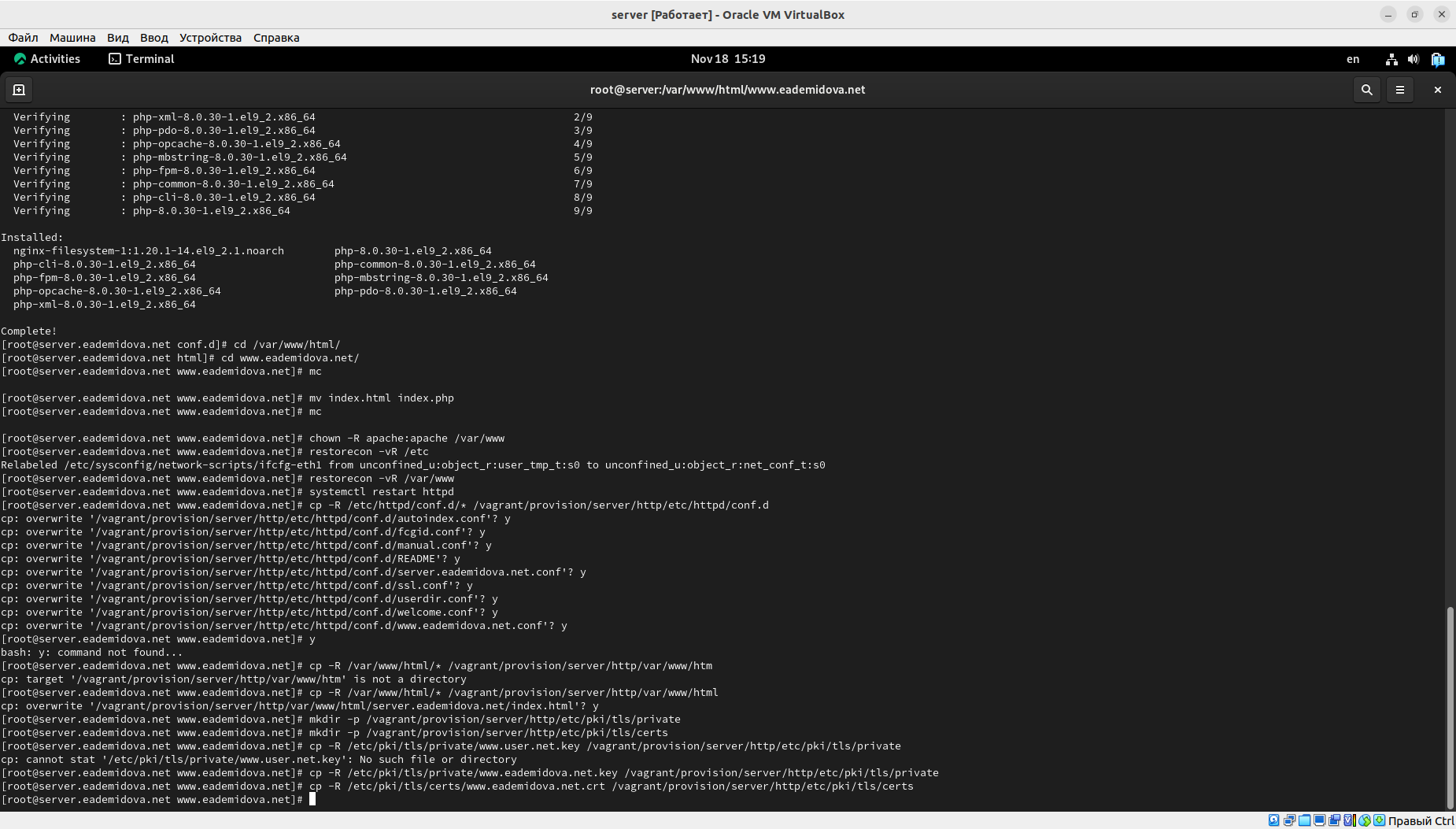
На виртуальной машине client в строке браузера введем название веб-сервера www.eademidova.net и убедимся, что будет выведена страница с информацией об используемой на веб-сервере версии PHP(??):



Проверка работы сервера с PHP

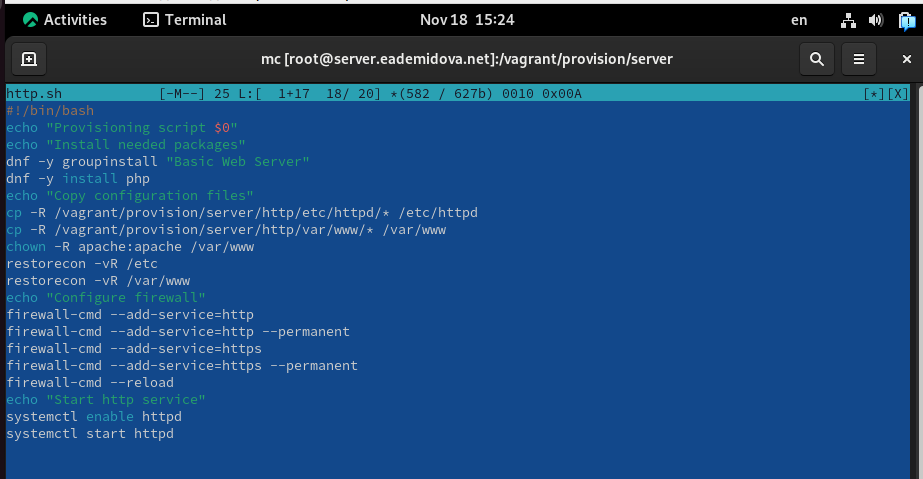
## 3.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

На виртуальной машине server перейдем в каталог для внесения изменений в настройки внутреннего окружения /vagrant/provision/server/http и в соответствующие каталоги скопируем конфигурационные файлы(рис. ??)



Создание окружения для внесения изменений в настройки окружающей среды

Открыв http.sh на редактирование, добавим в него следующие строки(??):



Содержание http.sh

# 4 Контрольные вопросы

1. В чём отличие HTTP от HTTPS?

Основное отличие между HTTP и HTTPS заключается в том, что HTTPS использует шифрование для обеспечения безопасной передачи данных, в то время как HTTP передает информацию в открытом виде.

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

Безопасность контента веб-сервера при работе через HTTPS обеспечивается с помощью шифрования данных, используя SSL/TLS протоколы, что позволяет защитить информацию от несанкционированного доступа.

1. Что такое сертификационный центр? Приведите пример.

Сертификационный центр (Certification authority, CA) представляет собой компонент глобальной службы каталогов, отвечающий за управление криптографическими ключами пользователей. Примеры: Let’s Encrypt, Comodo, Symantec.

# 5 Выводы

В результате выполнения данной работы были приобретены практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования PHP.