



RR Tech

Система RR Tech Service Management

Версия 1

Инструкция по установке

ООО «PP-TECH»

09 июля 2021 г.

Оглавление

1. Предварительные требования	3
2. Настройка и установка веб-сервера Apache	3
2.1 Установка Apache и обновление брандмауэра.....	3
2.2 Настройка .htaccess.....	6
3. Настройка и установка СУБД MySQL.....	6
3.1 Установка MySQL	6
3.2 Настройка безопасности.....	6
3.3 Тестирование работы	8
3.4 Импорт структуры БД и пользователей.....	9
4. Установка PHP	9
5. Создание виртуального хоста для сайта.....	10
5.1 Примечание о DirectoryIndex в Apache.....	12
5.2 Тестирование обработки PHP на веб-сервере	13
5.3 Импорт структуры системы.....	15

1. Предварительные требования

Для установки системы вам потребуется сервер Ubuntu 20.04 с учетной записью пользователя без привилегий root и с привилегиями `sudo`, а также базовым брандмауэром.

2. Настройка и установка веб-сервера Apache

2.1 Установка Apache и обновление брандмауэра

Установите Apache с помощью диспетчера пакетов `apt` в Ubuntu:

- `sudo apt update`
- `sudo apt install apache2`

Если это первое использование `sudo` в этом сеансе, вам нужно будет ввести пароль пользователя для подтверждения прав управления системными пакетами с помощью `apt`. Чтобы подтвердить установку Apache, нажмите `Y`, а затем `ENTER`.

После завершения установки вам нужно будет изменить настройки брандмауэра, чтобы разрешить трафик HTTP и HTTPS. Для этой цели в UFW можно использовать разные профили приложений. Чтобы вывести все доступные профили приложений UFW, запустите следующую команду:

- `sudo ufw app list`

Вывод будет выглядеть следующим образом:

Output

Available applications:

```
Apache
Apache Full
Apache Secure
OpenSSH
```

Вот что означает каждый из этих профилей:

- **Apache:** этот профиль открывает только порт `80` (нормальный веб-трафик без шифрования).

- **Apache Full:** этот профиль открывает порт 80 (нормальный веб-трафик без шифрования) и порт 443 (трафик с шифрованием TLS/SSL).
- **Apache Secure:** этот профиль открывает только порт 443 (трафик с шифрованием TLS/SSL).

Сейчас лучше всего разрешить только соединения на порту 80, поскольку мы только что установили Apache, и у нас еще нет сертификата TLS/SSL, настроенного для разрешения трафика HTTPS на нашем сервере.

Чтобы разрешить только трафик на порту 80, используйте профиль Apache:

```
• sudo ufw allow in "Apache"
```

Проверить изменения можно с помощью следующей команды:

```
• sudo ufw status
```

Output

Status: active

To	Action	From
--	-----	----
OpenSSH	ALLOW	Anywhere
Apache	ALLOW	Anywhere
OpenSSH (v6)	ALLOW	Anywhere (v6)
Apache (v6)	ALLOW	Anywhere (v6)

Теперь брандмауэр пропускает трафик порта 80.

Вы можете провести быструю проверку, открыв в браузере публичный IP-адрес вашего сервера (если вы не знаете свой публичный IP-адрес, следуйте указаниям примечания в следующем разделе):

```
http://your_server_ip
```

Вы увидите веб-страницу по умолчанию Ubuntu 20.04 Apache, предназначенную для информационных целей и целей тестирования. Она должна выглядеть следующим образом:



Apache2 Ubuntu Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in [/usr/share/doc/apache2/README.Debian.gz](#)**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.
- `ports.conf` is always included from the main configuration file. It is used to determine the listening ports for incoming connections, and this file can be customized anytime.
- Configuration files in the `mods-enabled/`, `conf-enabled/` and `sites-enabled/` directories contain particular configuration snippets which manage modules, global configuration fragments, or virtual host configurations, respectively.
- They are activated by symlinking available configuration files from their respective `*-available/` counterparts. These should be managed by using our helpers `a2enmod`, `a2dismod`, `a2ensite`, `a2dissite`, and `a2enconf`, `a2disconf`. See their respective man pages for detailed information.
- The binary is called `apache2`. Due to the use of environment variables, in the default configuration, `apache2` needs to be started/stopped with `/etc/init.d/apache2` or `apache2ctl`. **Calling `/usr/bin/apache2` directly will not work** with the default configuration.

Document Roots

By default, Ubuntu does not allow access through the web browser to *any* file apart of those located in `/var/www`, `public_html` directories (when enabled) and `/usr/share` (for web applications). If your site is using a web document root located elsewhere (such as in `/srv`) you may need to whitelist your document root directory in `/etc/apache2/apache2.conf`.

The default Ubuntu document root is `/var/www/html`. You can make your own virtual hosts under `/var/www`. This is different to previous releases which provides better security out of the box.

Reporting Problems

Please use the `ubuntu-bug` tool to report bugs in the Apache2 package with Ubuntu. However, check **existing bug reports** before reporting a new bug.

Please report bugs specific to modules (such as PHP and others) to respective packages, not to the web server itself.

Если вы видите эту страницу, ваш веб-сервер правильно установлен и доступен через ваш брандмауэр.

2.2 Настройка .htaccess

Для того, чтобы, Apache обрабатывал файлы .htaccess, необходимо включить поддержку htaccess в настройках Apache.

Откройте файл конфигурации сервера Apache /etc/apache2/httpd.conf

```
sudo nano -w /etc/apache2/httpd.conf
```

В Ubuntu 14.04 откройте файл конфигурации сервера Apache /etc/apache2/apache2.conf

```
sudo nano -w /etc/apache2/apache2.conf
```

Добавьте в файл /etc/apache2/httpd.conf или apache2.conf следующие строки

```
AccessFileName .htaccess
<Directory "/var/www/*">
AllowOverride All
</Directory>
```

Перезагрузите Apache

```
sudo /etc/init.d/apache2 restart
```

3. Настройка и установка СУБД MySQL

3.1 Установка MySQL

Мы запустили веб-сервер, и теперь нам нужно установить СУБД, которая может хранить данные вашего сайта и управлять ими. MySQL — популярная СУБД, используемая в средах PHP.

Используйте `apt` для получения и установки этого программного обеспечения:

```
• sudo apt install mysql-server
```

Для подтверждения установки введите `Y`, а затем нажмите `ENTER`.

3.2 Настройка безопасности

После завершения установки рекомендуется запустить скрипт безопасности, предустановленный в MySQL. Этот скрипт будет удалять некоторые небезопасные настройки по умолчанию и блокировать доступ к системе управления базы данных. Для запуска интерактивного скрипта введите следующую команду:

```
• sudo mysql_secure_installation
```

Скрипт предложит настроить плагин `VALIDATE PASSWORD PLUGIN`.

Примечание. Эту функцию следует активировать при наличии разумных оснований. Если она активирована, MySQL будет отклонять пароли, не соответствующие определенным критериям, и выводить сообщение об ошибке. Оставить проверку отключенной достаточно безопасно, но для входа в базу данных всегда нужно использовать надежные уникальные пароли.

Выберите `Y` для активации или любой другой вариант, чтобы продолжить без активации этой функции.

```
VALIDATE PASSWORD PLUGIN can be used to test passwords
and improve security. It checks the strength of password
and allows the users to set only those passwords which are
secure enough. Would you like to setup VALIDATE PASSWORD plugin?
```

```
Press y|Y for Yes, any other key for No:
```

Если вы ответите утвердительно, вам будет предложено выбрать уровень проверки пароля. Если вы укажете самый высокий уровень `2`, система будет выводить сообщения об ошибке при попытке установки пароля, который не будет содержать цифры, буквы в верхнем и нижнем регистре и специальные символы, или будет содержать распространенные словарные слова.

```
There are three levels of password validation policy:
```

```
LOW    Length >= 8
```

```
MEDIUM Length >= 8, numeric, mixed case, and special characters
```

```
STRONG Length >= 8, numeric, mixed case, special characters and dictionary
file
```

```
Please enter 0 = LOW, 1 = MEDIUM and 2 = STRONG: 1
```

Вне зависимости от того, будете ли вы использовать плагин `VALIDATE PASSWORD PLUGIN`, ваш сервер предложит вам выбрать и подтвердить пароль для **root** user в MySQL.

Если вы включили использование паролей, вы увидите уровень надежности введенного пароля для пользователя `root`, и ваш сервер запросит у вас подтверждение дальнейшего использования этого пароля. Если вас устраивает текущий пароль, введите `Y` в диалоге для подтверждения:

```
Estimated strength of the password: 100
```

```
Do you wish to continue with the password provided?(Press y|Y for Yes, any other key for No) : y
```

Для всех остальных вопросов нужно выбирать **Y** и нажимать **ENTER** в каждом диалоге. Выбрав эти ответы, вы удалите ряд анонимных пользователей и тестовую базу данных, отключите возможность удаленного входа пользователя **root** и загрузите новые правила, чтобы внесенные изменения немедленно активировались в MySQL.

3.3 Тестирование работы

Завершив настройку, проверьте возможность входа в консоль MySQL, набрав следующую команду:

- `sudo mysql`

В результате будет установлено подключение к серверу MySQL с помощью пользователя **root** базы данных с правами администратора, который логически выводится в результате использования `sudo` при запуске данной команды. Результат должен выглядеть следующим образом:

Output

```
Welcome to the MySQL monitor.  Commands end with ; or \g.
```

```
Your MySQL connection id is 22
```

```
Server version: 8.0.19-0ubuntu5 (Ubuntu)
```

```
Copyright (c) 2000, 2020, Oracle and/or its affiliates. All rights reserved.
```

```
Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.
```

```
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

```
mysql>
```

Для выхода из консоли MySQL введите следующую команду:

- `exit`

Обратите внимание, что для подключения под именем пользователя **root** не требуется вводить пароль, хотя вы и задали его при запуске скрипта `mysql_secure_installation`. Это работает, поскольку используемый по умолчанию метод аутентификации для пользователя MariaDB с правами

администратора — `unix_socket`, а не `пароль`. Хотя это может выглядеть как проблема безопасности, это делает сервер БД более безопасным, поскольку вход с правами `root` в MySQL доступен только системным пользователям с привилегиями `sudo`, которые подключаются через консоль или через приложение с тем же уровнем прав. На практике это означает, что вы не сможете использовать пользователя `root` базы данных с правами администратора для подключения из вашего приложения PHP. Настройка пароля учетной записи `root` MySQL работает как гарантия, если метод аутентификации по умолчанию меняется с `unix_socket` на `password`.

Для дополнительной безопасности рекомендуется иметь специальные учетные записи пользователей с менее обширными привилегиями, особенно если вы планируете использовать несколько баз данных на сервере.

3.4 Импорт структуры БД и пользователей

Теперь необходимо создать БД и пользователя и выполнить импорт структуры таблиц для работы системы.

Запускаем MySQL

- `sudo mysql`

Далее выполняем команды ниже (пароль можно изменить)

- `CREATE DATABASE RR_ITSM;`
- `CREATE USER 'itsm_admin' IDENTIFIED BY 'Aa123456';`
- `GRANT ALL PRIVILEGES ON RR_ITSM.* TO 'itsm_admin';`

Выполняем импорт структуры БД:

- `mysql -u root -p RR_ITSM < DATABASE.sql`

4. Установка PHP

Мы установили Apache для обслуживания вашего контента и MySQL для хранения и управления вашими данными. PHP — это элемент нашей настройки, который будет обрабатывать код для отображения динамического контента конечному пользователю. Помимо пакета `php` вам потребуется `php-mysql`, модуль PHP, который позволяет PHP взаимодействовать с базами данных MySQL. Также вам потребуется `libapache2-mod-php` для активации Apache для обработки файлов PHP. Ключевые пакеты PHP автоматически будут установлены в качестве зависимостей.

Чтобы установить эти пакеты, выполните команду:

```
• sudo apt install php libapache2-mod-php php-mysql php-mbstring -y
```

После завершения установки вы можете использовать следующую команду для подтверждения вашей версии PHP:

```
• php -v
```

Output

```
PHP 7.4.3 (cli) (built: Mar 26 2020 20:24:23) ( NTS )
```

```
Copyright (c) The PHP Group
```

```
Zend Engine v3.4.0, Copyright (c) Zend Technologies
```

```
with Zend OPcache v7.4.3, Copyright (c), by Zend Technologies
```

Теперь комплект LAMP полностью работоспособен. Однако, прежде чем тестировать настройку с помощью скрипта PHP, лучше всего настроить виртуальный хост Apache для хранения файлов и папок вашего сайта. Мы сделаем это на следующем шаге.

5. Создание виртуального хоста для сайта

При использовании веб-сервера Apache вы можете создать *виртуальные хосты* (аналогичные серверным блокам в Nginx) для инкапсуляции данных конфигурации и размещения на одном сервере нескольких доменов. Мы настроим домен **itsm**, но вы должны **заменить это имя собственным доменным именем**.

В Apache в Ubuntu 20.04 по умолчанию включен один серверный блок, настроенный на обслуживание документов из директории `/var/www/html`. Хотя это хорошо работает для отдельного сайта, при хостинге нескольких сайтов это неудобно. Вместо изменения `/var/www/html` мы создадим внутри `/var/www` структуру каталогов для нашего сайта **itsm**, оставив `/var/www/html` в качестве каталога по умолчанию для вывода в случае, если запросу клиента не соответствуют никакие другие сайты.

Создайте следующий каталог для **itsm**:

```
• sudo mkdir /var/www/itsm
```

Затем необходимо назначить права владения для директории с помощью переменной среды `$USER`, которая будет использоваться для текущего системного пользователя:

```
• sudo chown -R $USER:$USER /var/www/itsm
```

После этого откройте новый файл конфигурации в директории Apache `sites-available` с помощью любого редактора командной строки. Мы будем использовать `nano`:

```
• sudo nano /etc/apache2/sites-available/itsm.conf
```

В результате будет создан новый пустой файл. Вставьте следующую пустую конфигурацию:

```
                                /etc/apache2/sites-available/itsm.conf
<VirtualHost *:80>
    ServerName itsm
    ServerAlias www.itsm
    ServerAdmin webmaster@localhost
    DocumentRoot /var/www/itsm
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined
</VirtualHost>
```

Эта конфигурация `VirtualHost` указывает Apache обслуживать `itsm`, используя `/var/www/itsm` в качестве корневого каталога. Если вы хотите протестировать Apache без доменного имени, вы можете удалить или закомментировать опции `ServerName` и `ServerAlias`, добавляя символ `#` в начале строк опций.

Теперь вы можете использовать `a2ensite` для активации нового виртуального хоста:

```
• sudo a2ensite itsm
```

Возможно, вы захотите отключить сайт по умолчанию, устанавливаемый с Apache. Это требуется, если вы не используете собственное доменное имя, поскольку в таком случае конфигурация Apache по умолчанию перезаписывает ваш виртуальный хост. Чтобы отключить сайт Apache по умолчанию, введите следующую команду:

```
• sudo a2dissite 000-default
```

Чтобы убедиться в отсутствии ошибок синтаксиса в вашем файле конфигурации, выполните команду:

```
• sudo apache2ctl configtest
```

В заключение перезагрузите Apache, чтобы эти изменения вступили в силу:

- `sudo systemctl reload apache2`

Теперь ваш новый сайт активен, но корневой веб-каталог `/var/www/itsm` все еще пуст. Создайте файл `index.html` в этом расположении, чтобы убедиться, что виртуальный хост работает, как ожидалось:

- `nano /var/www/itsm/index.html`

Внесите в файл следующее:

```
/var/www/itsm/index.html
<h1>It works!</h1>
<p>This is the landing page of <strong>itsm</strong>.</p>
```

Откройте браузер и введите в адресную строку доменное имя вашего сервера или IP-адрес:

```
http://server_domain_or_IP
```

Страница будет выглядеть следующим образом:

It works!

This is the landing page of **your_domain**.

Если вы видите эту страницу, это означает, что виртуальный хост Apache работает, как и ожидалось.

Вы можете оставить этот файл в качестве временной начальной страницы для вашего приложения, пока не настроите файл `index.php` для его замены. Как только вы сделаете это, не забудьте удалить или переименовать файл `index.html` из корневого каталога документов, так как он будет иметь приоритет перед файлом `index.php` по умолчанию.

5.1 Примечание о `DirectoryIndex` в Apache

Если в Apache используются настройки `DirectoryIndex` по умолчанию, файл `index.html` всегда будет иметь приоритет по сравнению с файлом `index.php`. Это полезно при настройке страниц техобслуживания приложений PHP посредством создания временного файла `index.html` с информационным сообщением для посетителей. Поскольку эта страница будет иметь приоритет

перед страницей `index.php`, она станет начальной страницей приложения. После завершения обслуживания файл `index.html` можно переименовать или удалить из корневого каталога документов, в результате чего восстановится обычная начальная страница приложения.

Если вы хотите изменить это поведение, отредактируйте файл `/etc/apache2/mods-enabled/dir.conf` и измените порядковое расположение файла `index.php` в директиве `DirectoryIndex`:

- `sudo nano /etc/apache2/mods-enabled/dir.conf`

```
                                /etc/apache2/mods-enabled/dir.conf
<IfModule mod_dir.c>
    DirectoryIndex index.php index.html index.cgi index.pl index.xhtml index.htm
</IfModule>
```

После сохранения и закрытия файла вам нужно будет перезагрузить Apache, чтобы изменения вступили в силу:

- `sudo systemctl reload apache2`

На следующем шаге мы создадим скрипт PHP для тестирования правильности установки и настройки PHP на вашем сервере.

5.2 Тестирование обработки PHP на веб-сервере

Мы указали персонализированное расположение для хостинга файлов и папок сайта и теперь можем создать тестовый скрипт PHP, чтобы подтвердить способность Apache обрабатывать запросы для файлов PHP.

Создайте новый файл с именем `info.php` в корневой папке сайта:

- `nano /var/www/itsm/info.php`

В результате откроется пустой файл. Вставьте в файл следующий код PHP:


```
                                /var/www/itsm/info.php
<?php
phpinfo();
```

После завершения редактирования сохраните и закройте файл.

Чтобы протестировать этот скрипт, откройте браузер и введите доменное имя или IP-адрес вашего сервера, а затем название скрипта, в данном случае `info.php`:


http://server_domain_or_IP/info.php

Вы увидите приблизительно следующую страницу:

PHP Version 7.4.3 

System	Linux sassy-starfish 5.4.0-26-generic #30-Ubuntu SMP Mon Apr 20 16:58:30 UTC 2020 x86_64
Build Date	Mar 26 2020 20:24:23
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/apache2
Loaded Configuration File	/etc/php/7.4/apache2/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/apache2/conf.d
Additional .ini files parsed	/etc/php/7.4/apache2/conf.d/10-mysqlnd.ini, /etc/php/7.4/apache2/conf.d/10-opcache.ini, /etc/php/7.4/apache2/conf.d/10-pdo.ini, /etc/php/7.4/apache2/conf.d/20-calendar.ini, /etc/php/7.4/apache2/conf.d/20-ctype.ini, /etc/php/7.4/apache2/conf.d/20-exif.ini, /etc/php/7.4/apache2/conf.d/20-ffi.ini, /etc/php/7.4/apache2/conf.d/20-fileinfo.ini, /etc/php/7.4/apache2/conf.d/20-ftp.ini, /etc/php/7.4/apache2/conf.d/20-gettext.ini, /etc/php/7.4/apache2/conf.d/20-iconv.ini, /etc/php/7.4/apache2/conf.d/20-json.ini, /etc/php/7.4/apache2/conf.d/20-mysqli.ini, /etc/php/7.4/apache2/conf.d/20-pdo_mysql.ini, /etc/php/7.4/apache2/conf.d/20-phar.ini, /etc/php/7.4/apache2/conf.d/20-posix.ini, /etc/php/7.4/apache2/conf.d/20-readline.ini, /etc/php/7.4/apache2/conf.d/20-shmop.ini, /etc/php/7.4/apache2/conf.d/20-sockets.ini, /etc/php/7.4/apache2/conf.d/20-sysmsg.ini, /etc/php/7.4/apache2/conf.d/20-syssem.ini, /etc/php/7.4/apache2/conf.d/20-sysvshm.ini, /etc/php/7.4/apache2/conf.d/20-tokenizer.ini
PHP API	20190902
PHP Extension	20190902
Zend Extension	320190902
Zend Extension Build	API320190902,NTS
PHP Extension Build	API20190902,NTS
Debug Build	no
Thread Safety	disabled
Zend Signal Handling	enabled
Zend Memory Manager	enabled
Zend Multibyte Support	disabled
IPv6 Support	enabled
DTrace Support	available, disabled
Registered PHP Streams	https, ftps, compress.zlib, php, file, glob, data, http, ftp, phar
Registered Stream Socket Transports	tcp, udp, unix, udg, ssl, tls, tlsv1.0, tlsv1.1, tlsv1.2, tlsv1.3
Registered Stream Filters	zlib.*, string.rot13, string.toupper, string.tolower, string.strip_tags, convert.*, consumed, dechunk, convert.iconv.*

This program makes use of the Zend Scripting Language Engine:
Zend Engine v3.4.0, Copyright (c) Zend Technologies
with Zend OPcache v7.4.3, Copyright (c), by Zend Technologies



На этой странице содержится информация о вашем сервере с точки зрения PHP. Эта информация полезна для отладки и обеспечения правильного применения настроек.

Если вы видите эту страницу в своем браузере, ваша система PHP работает надлежащим образом.

После проверки соответствующей информации о вашем сервере PHP с помощью данной страницы рекомендуется удалить созданный вами файл, поскольку он содержит конфиденциальную информацию о вашей среде PHP и о вашем сервере Ubuntu. Для этого можно использовать `rm`:

- `sudo rm /var/www/itsm/info.php`

Если впоследствии вам снова потребуется эта информация, вы всегда можете воссоздать эту страницу.

5.3 Импорт структуры системы

Следующим этапом необходимо поместить файловую структуру нашего приложения в каталог `/var/www/itsm/`

После размещения файлов необходимо перезапустить службу Apache

```
• sudo service apache2 restart
```

Чтобы протестировать изменения, откройте браузер и введите доменное имя или IP-адрес вашего сервера, вы должны увидеть страницу авторизации.

Логин и пароль служебной УЗ `admin/admin` (изменяется после ввода системы в эксплуатацию)

