

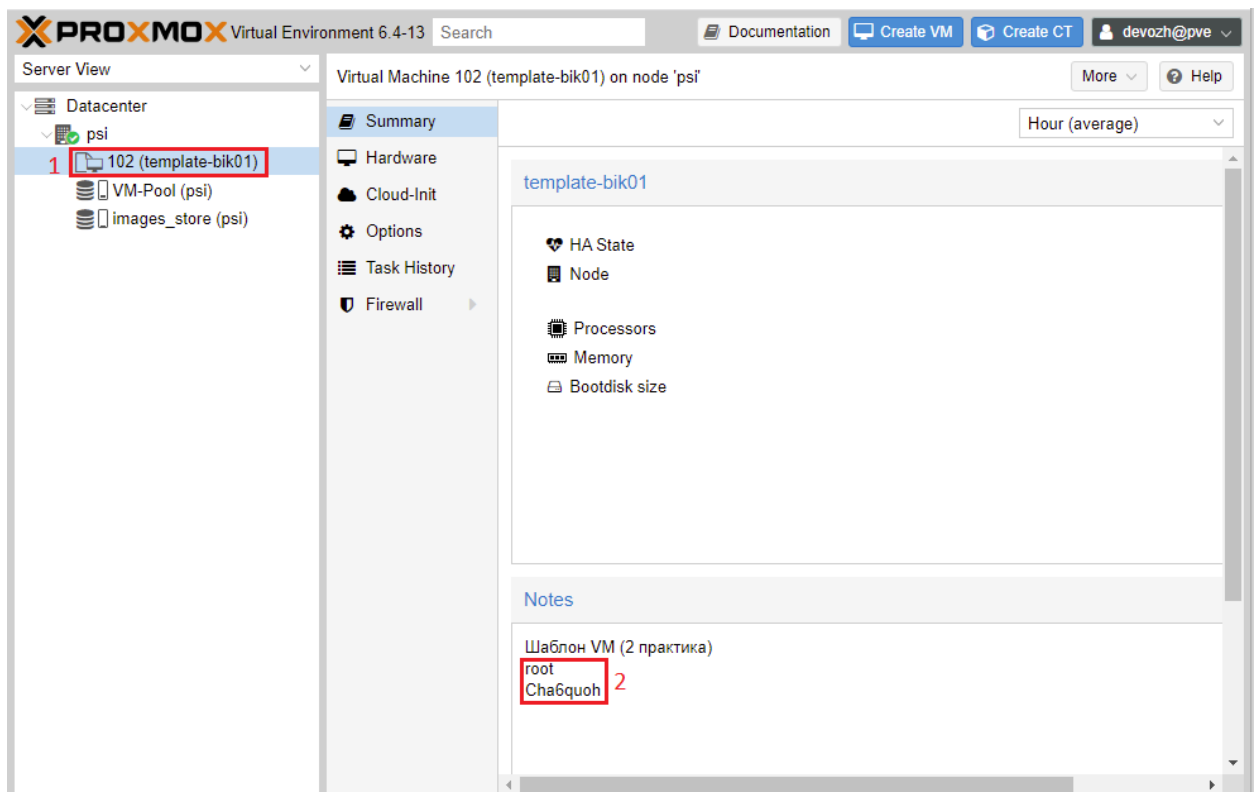
Технологии облачных вычислений

Практическая работа №2

- Подготовка к выполнению практической работы
- Знакомство со снапшотами и их использование.
- Настройка связки nginx + PHP-FPM + mysql
- Установка phpmyadmin.
- Настройка безопасного соединения

Подготовка к выполнению практической работы

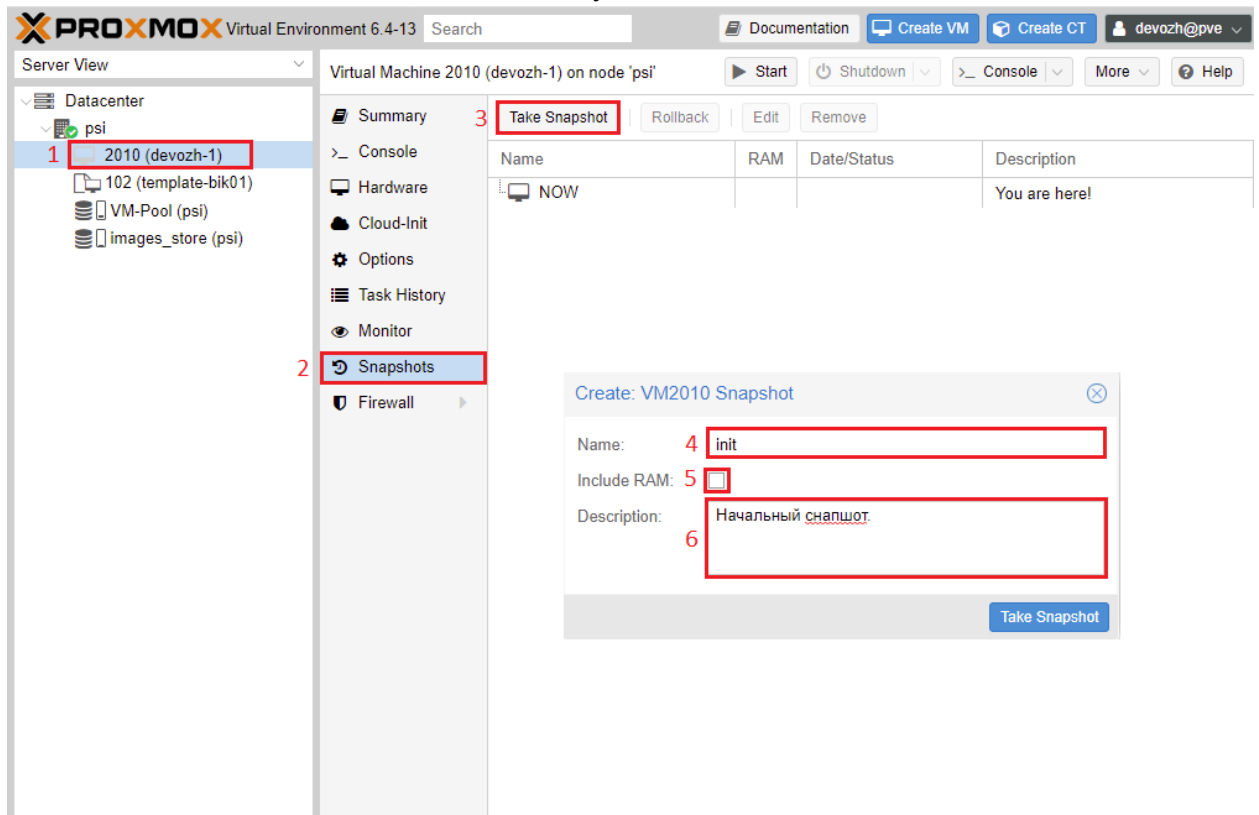
1. Создание VM.
 - 1.1. Создайте связанного клона (Linked Clone) VM из шаблона template-<группа>. Для каждой группы доступен только свой шаблон. Как сделать клона – см. «Практическая работа №1».
 - 1.2. На скриншоте приведен пароль пользователя **root**.
2. Запустите VM.
3. Посмотрите IP адрес в панели управления VM и приступите к настройке SSH соединения (см файл «Настройка доступа через SSH клиент PuTTY» в директории преподавателя).
4. После настройки SSH соединения и успешного логина на VM посмотрите назначенное имя VM командой «**hostname -A**». Оно вам потребуется для выполнения практической работы.



Знакомство со снапшотами и их использование.

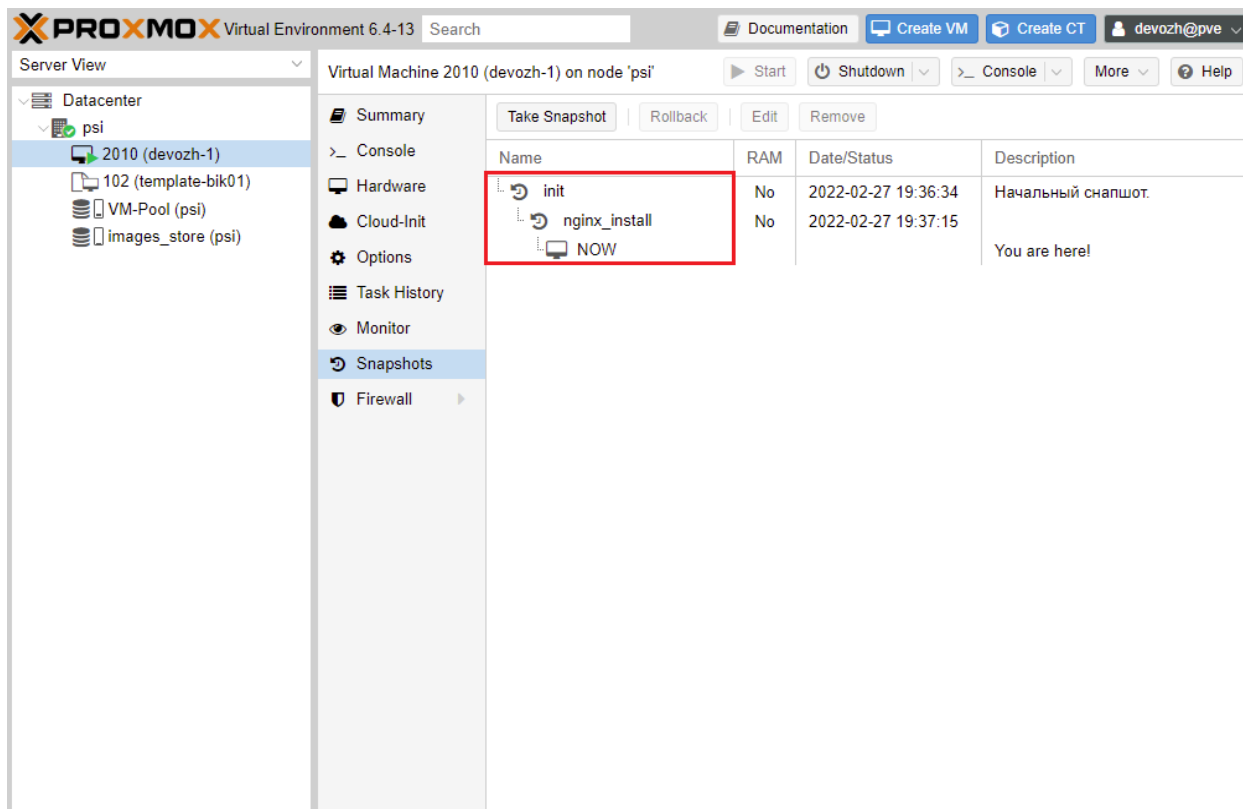
1. Снапшот – это мгновенный снимок состояния, в нашем случае - VM. (Читаем что такое снапшот здесь: https://ru.wikipedia.org/wiki/Снимок_файловой_системы). Цели использования снапшотов могут быть различны. Мы будем использовать снапшоты для сохранения промежуточных результатов выполнения практической работы. Т.е. если вы в результате выполнения работы испортили, что-либо в VM, то при наличии снапшота, можно будет вернуться к рабочему состоянию VM, в котором она находилась на момент создания снапшота.

Снапшоты можно создавать, когда VM запущена и когда она остановлена.



Попробуем создать снапшот.

- 1.1. Выбираете **VM**
- 1.2. Переходим в раздел «**Snapshots**»
- 1.3. Нажимаем кнопку «**Take Snapshot**»
- 1.4. Вводим имя снапшота. (Только английские символы, без пробелов).
- 1.5. Снимаем галочку «**Include RAM**».
- 1.6. Добавляем описание снапшота. (Можете добавить заметку для себя. Например, что уже сделано.)
- 1.7. Нажимаем на кнопку «**Take Snapshot**».
- 1.8. В результате в окне появляется запись о созданном снапшоте.



2. Откат к снимкту.

2.1. Выбираем раздел «**Snapshots**»

2.2. Выбираем снимкту. Чем выше снимкту находится в списке, тем раньше он создан. Например, мы хотим откатить все изменения, которые произошли с момента создания снимкту «**nginx_install**».

2.3. Нажимаем кнопку «**Rollback**».

2.4. Подтверждаем откат к снимкту.

2.5. Ждем пока завершится откат. Теперь можете проверять.

Замечание: В Proxmox есть ограничение на откат снимктов. Откатиться можно только на самый последний снимкту. Если вы хотите откатиться до более раннего снимкту, то вам придется удалить все снимкты, которые находятся между ним и состоянием «**NOW**».

PROXMOX Virtual Environment 6.4-13

Search

Documentation

Create VM

Create CT

devozh@pve

Server View

Datacenter

psi

2010 (devozh-1)

102 (template-bik01)

VM-Pool (psi)

images_store (psi)

Virtual Machine 2010 (devozh-1) on node 'psi'

Start

Shutdown

Console

More

Help

Summary

Console

Hardware

Cloud-Init

Options

Task History

Monitor

1 Snapshots

Firewall

Take Snapshot

3 Rollback

Edit

Remove

Name	RAM	Date/Status	Description
init	No	2022-02-27 19:36:34	Начальный снимшот.
2 nginx_install	No	2022-02-27 19:37:15	
NOW			You are here!

Confirm

VM 2010 - Rollback 'nginx_install'

4 Yes No

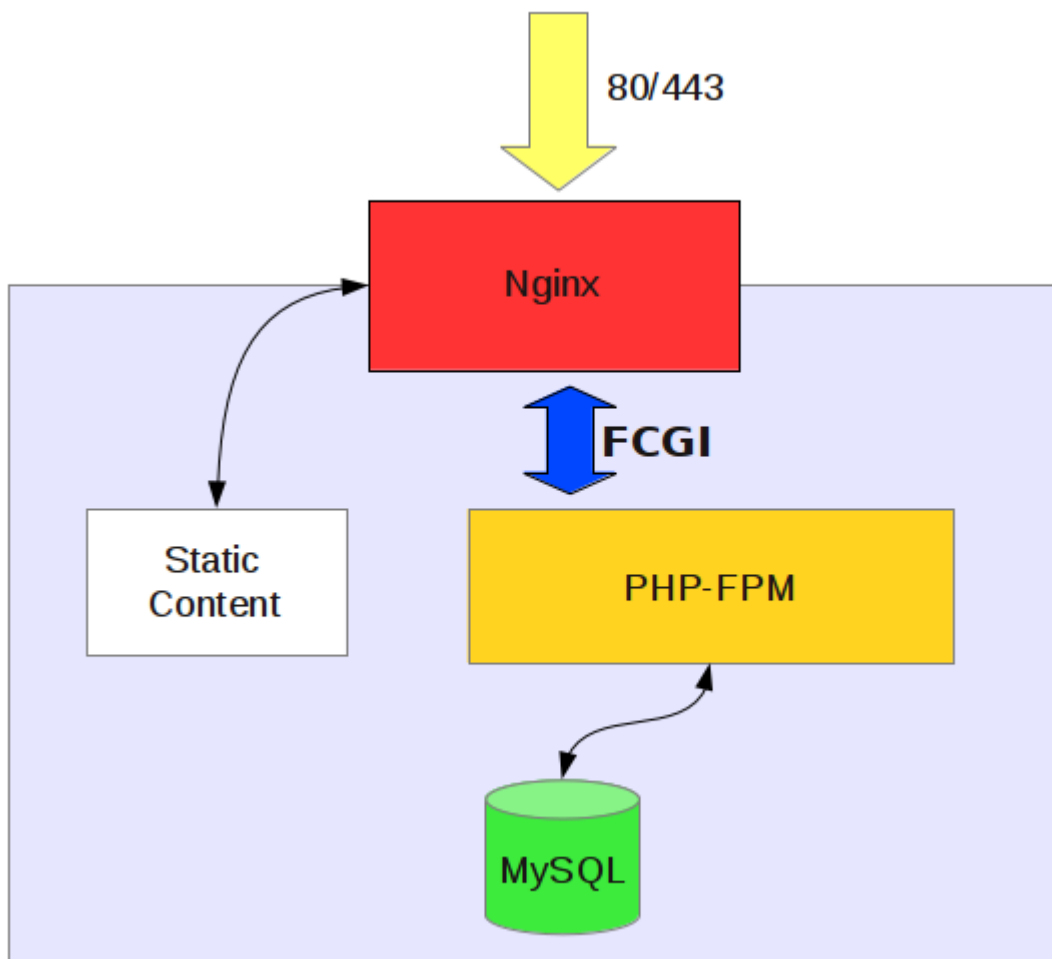
Настройка связки nginx + PHP-FPM + mysql

В общем виде web-сервер представляет собой связку nginx + PHP-FPM + mysql. Любая часть этой связки может быть расширена, изменена или настроена альтернативным способом. В практической работе будут даны указания, какой вариант конфигурации нужно использовать.

Все системные настройки производятся из-под пользователя **root**. Если вы произвели логин под обычным пользователем выполните команду «**sudo su**».

При обращении к сайту проверяйте, что адрес начинается с «http» иначе работать ничего не будет. Браузер Chrome постоянно пытается перекинуть на https, поэтому либо используйте приватный режим, либо браузер FireFox.

Помните о владельце и правах доступа к файлам. «www-data» - пользователь из-под которого работает web-сервер. Если владелец будет другим – будут возникать проблемы.



Информация по nginx:

<https://selectel.ru/blog/install-nginx/>

<https://www.cs-cart.ru/docs/4.3.x/install/vps/nginx/>

<https://www.digitalocean.com/community/tutorials/how-to-install-linux-nginx-mysql-php-lemp-stack-on-ubuntu-20-04-ru>

<https://www.digitalocean.com/community/tutorials/how-to-configure-nginx-to-use-custom-error-pages-on-ubuntu-14-04>

<https://serveradmin.ru/ustanovka-i-nastroyka-nginx/>

<https://habr.com/ru/post/130511/>

http://nginx.org/en/docs/http_access_module.html

NGINX Задание:


1. Установить nginx.
2. Проверить работу (обратиться по имени через браузер. Должна быть выдана надпись «Welcome to nginx!»).
3. Найти конфигурационные файлы (главный файл nginx.conf) и узнать из конфигурационных файлов расположение «root» (корневой директории web-сервера). Найти расположение файла index.html (название может немного отличаться).
4. Добавить в файл свою строку любого содержимого и проверить изменения через браузер.
5. Попробовать получить доступ к несуществующей странице (404) через браузер на вашем «сайте».
6. Создать страницу альтернативную страницу 404 и добавить ее в конфигурацию nginx. Проверить.
7. Создать location «phpmyadmin» в nginx. Проверить доступность. Ограничить доступ средствами nginx по ip адресу ВГУЭС (получить адрес ВГУЭС можно на myip.ru). С адреса ВГУЭС доступ должен работать, а с других адресов нет. (Проверить можете с помощью мобильного телефона). Далее мы будем устанавливать в данную директорию phpmyadmin (web-интерфейс для управления СУБД) и ограничение доступа необходимо для безопасности.
8. Создать в директории «phpmyadmin» файл и попробовать получить к нему доступ из ВГУЭС (должен открываться) и с мобильного телефона (должны получить ошибку 403 Forbidden).

Информация по PHP-FPM:

<https://selectel.ru/blog/install-nginx/>

PHP-FPM Задание:

1. Установить PHP-FPM
2. Найти конфигурационные файлы PHP (php-fpm.conf). Найти конфигурационные файлы пулов.
3. Настроить пул для конкретного сайта (можете настраивать файл по умолчанию). Использовать способ подключения к PHP серверу через сокет.
4. Сделать тестовый файл (см пример 1 здесь <https://www.php.net/manual/en/function.phpinfo.php>) и положить его в директорию phpmyadmin. Проверьте что он у вас открывается, либо скачивается.
5. Настроить связку nginx и php
6. Проверить работу связки. Должно получиться как на скриншоте (см. ниже).

PHP Version 7.4.28 	
System	Linux devozh-1 5.10.0-11-amd64 #1 SMP Debian 5.10.92-1 (2022-01-18) x86_64
Build Date	Feb 17 2022 16:17:19
Server API	FM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php/7.4/fpm
Loaded Configuration File	/etc/php/7.4/fpm/php.ini
Scan this dir for additional .ini files	/etc/php/7.4/fpm/conf.d
Additional .ini files parsed	/etc/php/7.4/fpm/conf.d/10-mysqlnd.ini, /etc/php/7.4/fpm/conf.d/10-opcache.ini, /etc/php/7.4/fpm/conf.d/10-pdo.ini, /etc/php/7.4/fpm/conf.d/20-calendar.ini, /etc/php/7.4/fpm/conf.d/20-ctype.ini, /etc/php/7.4/fpm/conf.d/20-exif.ini, /etc/php/7.4/fpm/conf.d/20-fileinfo.ini, /etc/php/7.4/fpm/conf.d/20-ftp.ini, /etc/php/7.4/fpm/conf.d/20-gettext.ini, /etc/php/7.4/fpm/conf.d/20-iconv.ini, /etc/php/7.4/fpm/conf.d/20-ldap.ini, /etc/php/7.4/fpm/conf.d/20-mbstring.ini, /etc/php/7.4/fpm/conf.d/20-mysqli.ini, /etc/php/7.4/fpm/conf.d/20-pdo_mysql.ini, /etc/php/7.4/fpm/conf.d/20-phar.ini, /etc/php/7.4/fpm/conf.d/20-posix.ini, /etc/php/7.4/fpm/conf.d/20-readline.ini, /etc/php/7.4/fpm/conf.d/20-shmop.ini, /etc/php/7.4/fpm/conf.d/20-sockets.ini, /etc/php/7.4/fpm/conf.d/20-sysmsg.ini, /etc/php/7.4/fpm/conf.d/20-sysvsem.ini, /etc/php/7.4/fpm/conf.d/20-sysvshm.ini, /etc/php/7.4/fpm/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 v7.4.28, Copyright (c), by Zend Technologies	

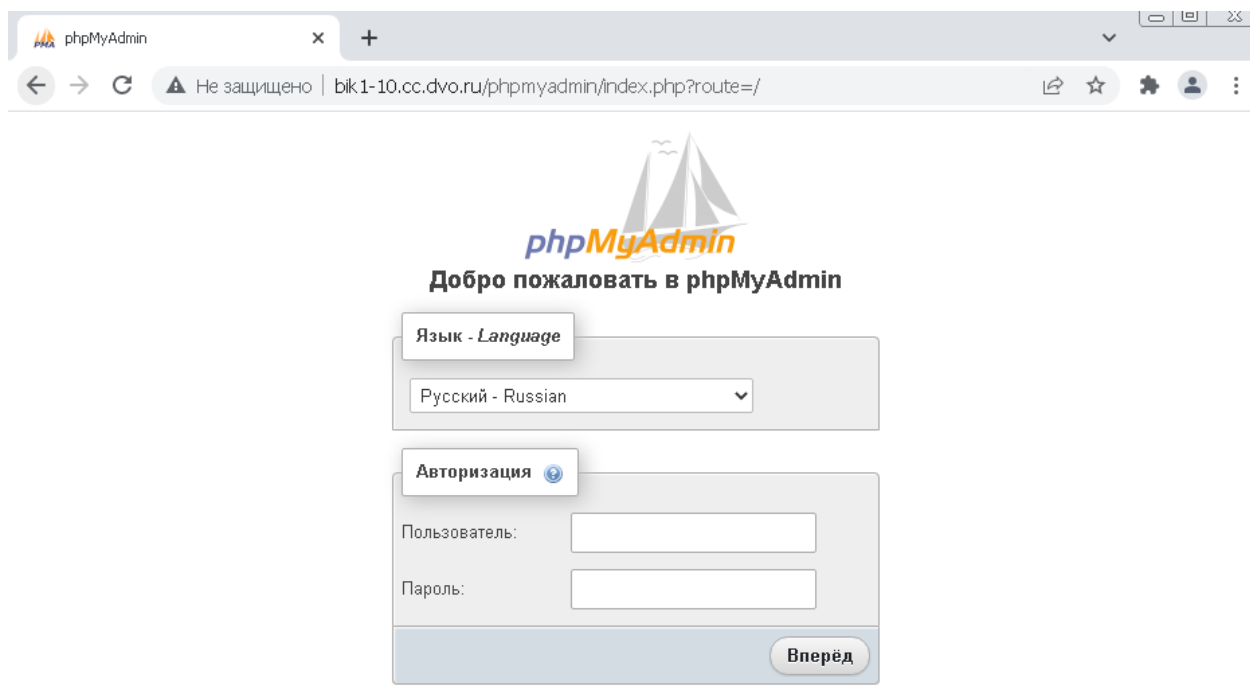
Confiuration

MYSQL Задание:

Установите mariadb. (<https://infoit.com.ua/databases/mariadb/kak-ustanovit-mariadb-na-debian-11/>).

Задание Установка phpmyadmin

1. Установите модули php
apt install php-cgi php-mysqli php-pear php-mbstring libapache2-mod-php php-common php-phpseclib php-mysql
2. Загрузите исходники phpmyadmin
wget <https://files.phpmyadmin.net/phpMyAdmin/5.1.3/phpMyAdmin-5.1.3-all-languages.zip>
3. Распакуйте архив.
4. Поместите файлы из распакованной директории в директорию «phpmyadmin» в корне web-сервера, которую создавали ранее.
5. Проверьте результат в браузере. Должно получиться окно как на скриншоте ниже.
6. Выполните логин. Пользователь **root**. Пароль от базы, который вы задали при установке.



Настройка SSL

Сейчас доступ к вашим сайтам происходит через не безопасное соединение (http). С точки зрения безопасности — это не только плохо, но и опасно. На текущий момент вы настроили web-сервер и phpmyadmin. При этом с помощью phpmyadmin вы можете получать доступ к базам данных. Перехватить ваш пароль не составляет труда. Поэтому предлагаю вам произвести настройку SSL соединения. Среди вышеприведенных ссылок достаточно информации для настройки SSL. <https://ru.wikipedia.org/wiki/HTTPS>

Как получить сертификат

1. Выключаем nginx **systemctl stop nginx .**
2. Устанавливаем CertBot **apt install certbot .**
3. Выполняем команду
`certbot certonly --standalone --agree-tos --email <ваш mail> -d <ваш домен>`
Данные в скобках заменить вашими.

После получения сертификата будет выдан путь к его месту расположению

Теперь можете приступать к настройке web-сервера.

После успешной настройки вам необходимо будет сделать перенаправление всего трафика с 80 порта (http) на 443 (https).