

Отчет по лабораторной работе № 5.
Расширенная настройка НТТР-сервера Apache

Данила Стариков
НПИбд-02-22

2024

Содержание

1	Цель работы	3
2	Выполнение работы	4
2.1	Конфигурирование HTTP-сервера для работы через протокол HTTPS	4
2.2	Конфигурирование HTTP-сервера для работы с РНР	8
2.3	Внесение изменений в настройки внутреннего окружения виртуальной машины	9
3	Выводы	11

1 Цель работы

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

2 Выполнение работы

2.1 Конфигурирование HTTP-сервера для работы через протокол HTTPS

1. Загрузили вашу операционную систему и перейдите в рабочий каталог с проектом:

```
cd /var/tmp/dastarikov/vagrant
```

2. Запустили виртуальную машину server:

```
make server-up
```

3. На виртуальной машине server вошли и открыли терминал. Перешли в режим суперпользователя:

```
sudo -i
```

4. В каталоге /etc/ssl создали каталог private:

```
mkdir -p /etc/pki/tls/private  
ln -s /etc/pki/tls/private /etc/ssl/private  
cd /etc/pki/tls/private
```

Сгенерировали ключ и сертификат, используя следующую команду:

```
openssl req -x509 -nodes -newkey rsa:2048 -keyout www.dastarikov.net.key  
→ -out www.dastarikov.net.crt  
mv www.dastarikov.net.crt /etc/pki/tls/certs
```

Далее заполнили сертификат (Рис. 1):

- в строке кода страны укажите RU;
- в строке названия страны укажите Russia;
- в строке названия города укажите Moscow;
- в строке названия организации укажите свой логин;
- в строке названия подразделения укажите свой логин;
- в строке названия хоста должно быть указано доменное имя вашего веб-сервера dastarikov.net;
- в строке e-mail адреса должен быть указан dastarikov@dastarikov.net.

```
Country Name (2 letter code) [XX]:RU  
State or Province Name (full name) []:Russia  
Locality Name (eg, city) [Default City]:Moscow  
Organization Name (eg, company) [Default Company Ltd]:dastarikov  
Organizational Unit Name (eg, section) []:dastarikov  
Common Name (eg, your name or your server's hostname) []:dastarikov.net  
Email Address []:dastarikov@dastarikov.net
```

Рис. 1: Создание SSL-сертификата.

Сгенерированные ключ и сертификат появились в соответствующем каталоге /etc/ssl/private. Скопировали сертификат в каталог /etc/ssl/certs:

```
cp /etc/ssl/private/www.dastarikov.net.crt /etc/ssl/cert/
```

5. Для перехода веб-сервера `www.dastarikov.net` на функционирование через протокол HTTPS изменили его конфигурационный файл. Перешли в каталог с конфигурационными файлами:

```
cd /etc/httpd/conf.d
```

Открыли на редактирование файл `/etc/httpd/conf.d/www.dastarikov.net.conf` и заменили его содержимое на следующее (Рис. 2):

```
<VirtualHost *:80>
ServerAdmin webmaster@dastarikov.net
DocumentRoot /var/www/html/www.dastarikov.net
ServerName www.dastarikov.net
ServerAlias www.dastarikov.net
ErrorLog logs/www.dastarikov.net-error_log
CustomLog logs/www.dastarikov.net-access_log common
RewriteEngine on
RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>
<IfModule mod_ssl.c>
<VirtualHost *:443>
SSLEngine on
ServerAdmin webmaster@dastarikov.net
DocumentRoot /var/www/html/www.dastarikov.net
ServerName www.dastarikov.net
ServerAlias www.dastarikov.net
ErrorLog logs/www.dastarikov.net-error_log
CustomLog logs/www.dastarikov.net-access_log common
SSLCertificateFile /etc/ssl/certs/www.dastarikov.net.crt
SSLCertificateKeyFile /etc/ssl/private/www.dastarikov.net.key
</VirtualHost>
</IfModule>
```

Теперь при попытке подключиться по старому адресу через http будет происходить переадресация на соответствующие адреса https, за что отвечают команды:

```
RewriteEngine on
RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
```

Сами настройки подключения по протоколу HTTPS описаны внутри тега `<IfModule mod_ssl.c>`, отличия есть только в наличии команды `SSLEngine on` и указания местоположения файла SSL-сертификата.

```

<VirtualHost *:80>
ServerAdmin webmaster@dastarikov.net
DocumentRoot /var/www/html/www.dastarikov.net
ServerName www.dastarikov.net
ServerAlias www.dastarikov.net
ErrorLog logs/www.dastarikov.net-error_log
CustomLog logs/www.dastarikov.net-access_log common
RewriteEngine on
RewriteRule ^(.*)$ https://%{HTTP_HOST}$1 [R=301,L]
</VirtualHost>
<IfModule mod_ssl.c>
<VirtualHost *:443>
SSLEngine on
ServerAdmin webmaster@dastarikov.net
DocumentRoot /var/www/html/www.dastarikov.net
ServerName www.dastarikov.net
ServerAlias www.dastarikov.net
ErrorLog logs/www.dastarikov.net-error_log
CustomLog logs/www.dastarikov.net-access_log common
SSLCertificateFile /etc/ssl/certs/www.dastarikov.net.crt
SSLCertificateKeyFile /etc/ssl/private/www.dastarikov.net.key
</VirtualHost>
</IfModule>

```

Рис. 2: Изменение конфигурационного файла для работы через протокол HTTPS.

6. Внесли изменения в настройки межсетевого экрана на сервере, разрешив работу с https (Рис. 3):

```

firewall-cmd --list-services
firewall-cmd --get-services
firewall-cmd --add-service=https
firewall-cmd --add-service=https --permanent
firewall-cmd --reload

```

```
[root@server.dastarikov.net conf.d]# firewall-cmd --list-services
firewall-cmd --get-services
firewall-cmd --add-service=https
firewall-cmd --add-service=https --permanent
firewall-cmd --reload
cockpit dhcp dhcpv6-client dns http ssh
RH-Satellite-6 RH-Satellite-6-capsule afp amanda-client amanda-k5-client amqp amqps apcupsd audit ausweisapp2 bacula
acula bacula-client bareos-director bareos-filedaemon bareos-storage bb bgp bitcoin bitcoin-rpc bitcoin-testnet bitcoi
n-testnet-rpc bittorrent-lsd ceph ceph-exporter ceph-mon cfengine checkmk-agent cockpit collectd condor-collector
cratedb ctdb dds dds-multicast dds-unicast dhcp dhcpv6 dhcpv6-client distcc dns dns-over-tls docker-regis
try docker-swarm dropbox-lansync elasticsearch etcd-client etcd-server finger foreman foreman-proxy freeipa-4 freeipa
ldap freeipa-ldaps freeipa-replication freeipa-trust ftp galera ganglia-client ganglia-master git gpsd grafana gre high-
availability http http3 https ident imap imaps ipfs ipp ipp-client ipsec irc ircs iscsi-target isns jenkins kadmin
kdeconnect kerberos kibana klogin kpasswd kprop kshell kube-api kube-apiserver kube-control-plane kube-control-plane-
secure kube-controller-manager kube-controller-manager-secure kube-nodeport-services kube-scheduler kube-scheduler-
secure kube-worker kubelet kubelet-readonly kubelet-worker ldap ldaps libvirt libvirt-tls lightning-network llmnr
llmnr-client llmnr-tcp llmnr-udp managesieve matrix mdns memcache minidlna mongodb mongod mosh mountd mqtt mqtt-tls
ms-wbt mssql murmur mysql nbd nebula netbios-ns netdata-dashboard nfs nfs3 nmap nmap-0183 ntp nut openvpn ovirt-
imageio ovirt-storageconsole ovirt-vmconsole plex pmcd pmpoxy pmwebapi pmwebapis pop3 postgresql privoxy prometheu
s prometheus prometheus-node-exporter proxy-dhcp ps2link ps3netsh ptp pulseaudio puppetmaster quassel radius rdp
redis redis-sentinel rpc-bind rquotad rsh rsyncd rtsp salt-master samba samba-client samba-dc sane sip sips slp smtp
smtp-submission smtps snmp snmptls snmptls-trap snmptrap spideroak-lansync spotify-sync squid sssd ssh steam-stream
ing svdrp svn syncthing syncthing-gui syncthing-relay synergy syslog syslog-tls telnet tentacle tftp tile38 tinc tor-sock
s transmission-client upnp-client vds vnc-server warpinator wbem-http wbm-https wireguard ws-discovery ws-discovery-
client ws-discovery-tcp ws-discovery-udp wsman wsmans xdmcp xmpp-bosh xmpp-client xmpp-local xmpp-server zabbix-agent
zabbix-server zerotier
success
success
success
[root@server.dastarikov.net conf.d]#
```

Рис. 3: Настройка межсетевого экрана.

7. Перезапустили веб-сервер:

```
systemctl restart httpd
```

8. На виртуальной машине `client` в строке браузера ввели название веб-сервера `www.dastarikov.net` и убедились, что происходит автоматическое переключение на работу по протоколу HTTPS. На открывшейся странице с сообщением о незащищённости соединения нажали кнопку «Дополнительно», затем добавили адрес вашего сервера в постоянные исключения. Затем просмотрели содержание сертификата (нажмите на значок с замком в адресной строке и кнопку «Подробнее») (Рис. 4).

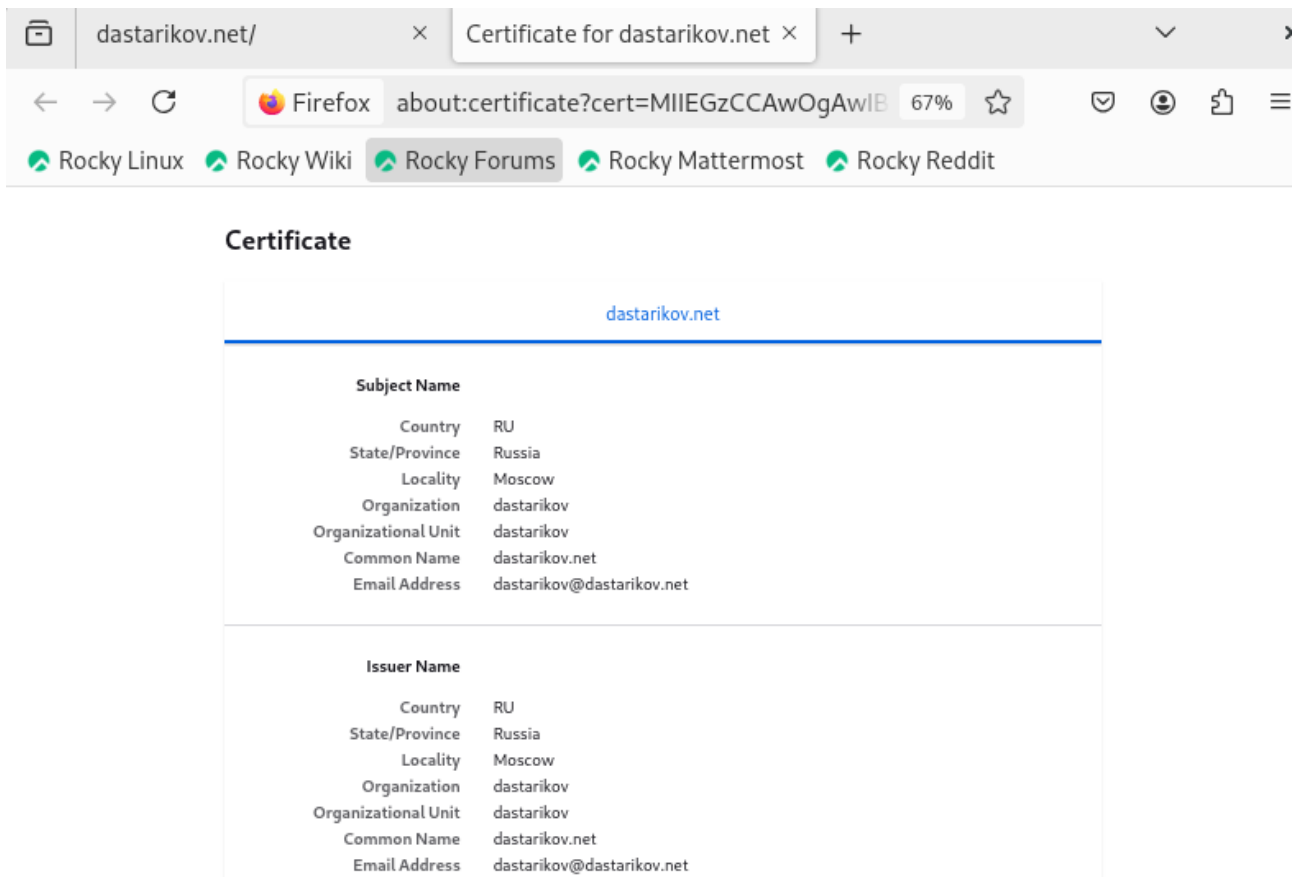


Рис. 4: Просмотр содержания созданного сертификата.

2.2 Конфигурирование HTTP-сервера для работы с PHP

1. Установили пакеты для работы с PHP:
`dnf -y install php`
2. В каталоге `/var/www/html/www.dastarikov.net` заменили файл `index.html` на `index.php` следующего содержания:

```
<?php
phpinfo();
?>
```

3. Скорректировали права доступа в каталог с веб-контентом (Рис. 5):
`chown -R apache:apache /var/www`
4. Восстановили контекст безопасности в SELinux (Рис. 5):

```
restorecon -vR /etc
restorecon -vR /var/www
```

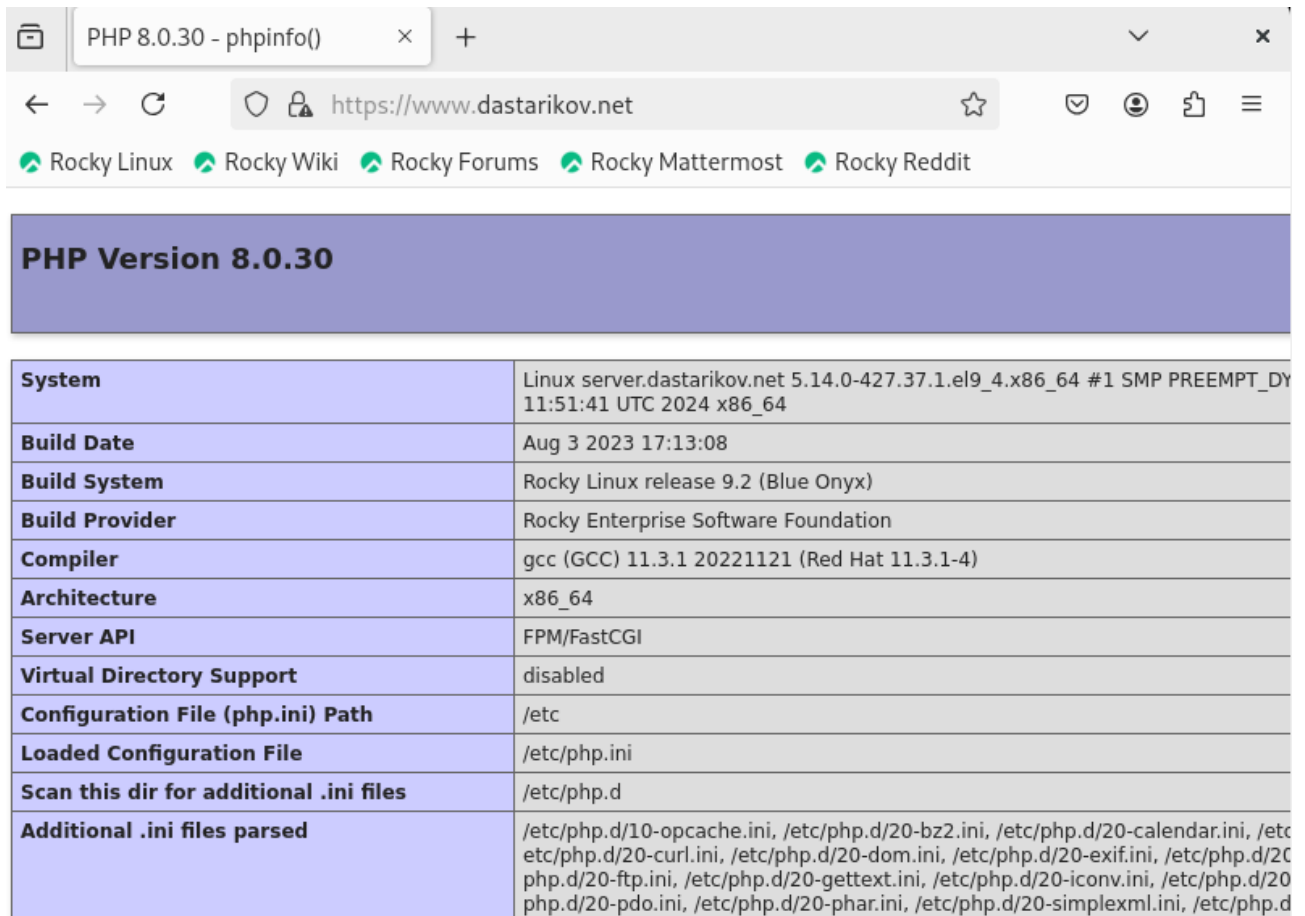
```
[root@server.dastarikov.net www.dastarikov.net]# chown -R apache:apache /var/www
[root@server.dastarikov.net www.dastarikov.net]# restorecon -vR /etc
restorecon -vR /var/www
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
```


Рис. 5: Обновление контекста безопасности в SELinux.

5. Перезапустили HTTP-сервер:

```
systemctl restart httpd
```

6. На виртуальной машине `client` в строке браузера ввели название веб-сервера `www.dastarikov.net` и убедились, что выведена страница с информацией об используемой на веб-сервере версии PHP (Рис. 6).



System	Linux server.dastarikov.net 5.14.0-427.37.1.el9_4.x86_64 #1 SMP PREEMPT_DY 11:51:41 UTC 2024 x86_64
Build Date	Aug 3 2023 17:13:08
Build System	Rocky Linux release 9.2 (Blue Onyx)
Build Provider	Rocky Enterprise Software Foundation
Compiler	gcc (GCC) 11.3.1 20221121 (Red Hat 11.3.1-4)
Architecture	x86_64
Server API	FPM/FastCGI
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc
Loaded Configuration File	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
Additional .ini files parsed	/etc/php.d/10-opcache.ini, /etc/php.d/20-bz2.ini, /etc/php.d/20-calendar.ini, /etc/php.d/20-curl.ini, /etc/php.d/20-dom.ini, /etc/php.d/20-exif.ini, /etc/php.d/20-ftp.ini, /etc/php.d/20-gettext.ini, /etc/php.d/20-iconv.ini, /etc/php.d/20-pdo.ini, /etc/php.d/20-phar.ini, /etc/php.d/20-simplexml.ini, /etc/php.d

Рис. 6: Информация об оспользуемой на веб-сервере версии PHP.

2.3 Внесение изменений в настройки внутреннего окружения виртуальной машины

1. На виртуальной машине `server` перешли в каталог для внесения изменений в настройки внутреннего окружения `/vagrant/provision/server/http` и в соответствующие каталоги скопировали конфигурационные файлы (Рис. 7):

```
cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/conf.d
cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html
mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
```

```

mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
cp -R /etc/pki/tls/private/www.dastarikov.net.key
↪ /vagrant/provision/server/http/etc/pki/tls/private
cp -R /etc/pki/tls/certs/www.dastarikov.net.crt
↪ /vagrant/provision/server/http/etc/pki/tls/certs

```

```

[root@server.dastarikov.net www.dastarikov.net]# cp -R /etc/httpd/conf.d/* /vagrant/provision/server/http/etc/httpd/conf.d
cp -R /var/www/html/* /vagrant/provision/server/http/var/www/html
mkdir -p /vagrant/provision/server/http/etc/pki/tls/private
mkdir -p /vagrant/provision/server/http/etc/pki/tls/certs
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.dastarikov.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.dastarikov.net.conf'? y
cp: overwrite '/vagrant/provision/server/http/var/www/html/server.dastarikov.net/index.html'? y
[root@server.dastarikov.net www.dastarikov.net]# y
bash: y: command not found...
[root@server.dastarikov.net www.dastarikov.net]# cp -R /etc/pki/tls/private/www.user.net.key /vagrant/provision/server/http/etc/pki/tls/private
cp: cannot stat '/etc/pki/tls/private/www.user.net.key': No such file or directory
[root@server.dastarikov.net www.dastarikov.net]# cp -R /etc/pki/tls/private/www.dastarikov.net.key /vagrant/provision/server/http/etc/pki/tls/private
[root@server.dastarikov.net www.dastarikov.net]# cp -R /etc/pki/tls/certs/www.dastarikov.net.crt /vagrant/provision/server/http/etc/pki/tls/certs
[root@server.dastarikov.net www.dastarikov.net]#

```

Рис. 7: Копирование конфигурационных файлов для настройки внутреннего окружения.

2. В имеющийся скрипт `/vagrant/provision/server/http.sh` внесли изменения, добавив установку PHP и настройку межсетевого экрана, позволяющую работать с https.

```

#!/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
```

3 Выводы

В результате выполнения лабораторной работы приобрели практические навыки по расширенному конфигурированию HTTP-сервера Apache в части безопасности и возможности использования РНР.