Когда у меня появилась необходимость настроить полноценный прокси сервер на базе CentOS 7, оказалось, что в интернете почти нет актуальной информации на эту тему. Статьи в целом есть, но большинство из них про 6-ю версию, плюс нету полноценной связки с active directory. В своей статье я восполню тематический пробел.

Содержание:

Введение

Существует проверенная временем связка для прокси сервера - squid + sams. Я настраивал ее еще лет 8 назад на Freebsd. Недавно у меня появилась необходимость настроить что-то подобное на CentOS 7, и я с удивлением обнаружил, что ничего принципиально нового с тех пор не появилось. Никакой более удобной и информативной web панели к squid не придумали.

Так что будем настраивать проверенный временем набор программ. Ко всему прочему, удобнее его сразу интегрировать с виндовым доменом, для простой авторизации на прокси с помощью учетных записей домена. Так проще будет смотреть статистику и давать доступ. Особенно это актуально, если у вас есть терминальные пользователи, работающие с одного ip. Здесь у вас вообще нет других вариантов, если вам нужна статистика и ограничение доступа по пользователям.

Приступим к настройке. В своей работе я буду подразумевать, что вы установили и настроили centos по моим рекомендациям. Советую ознакомиться с материалом. Это позволит здесь не тратить время на второстепенные настройки, которые не имеют прямого отношения к теме статьи.

Добавление CentOS 7 в домен Windows

Здесь нужно быть очень внимательным. Это сложный и не любимый мной момент, так как все очень сильно привязано к версиям системы и софта. Порой какой-нибудь точки или регистра достаточно, чтобы ничего не работало. Так вышло и у меня, когда я готовил этот материал.

Я без проблем ввел компьютер в домен, прошел все проверки, но потом в squid напрочь отказывалась работать ntlm авторизация. Все на вид выглядело нормально, но не работало. Я несколько раз восстанавливал виртуалку и начинал все сначала, перечитав практически все, что смог найти по теме в рунете и буржунете. В какой-то момент все заработало. Я зафиксировал результат и несколько раз проверил последовательность действий и отточил ее до каждого шага. Проверил несколько раз на чистой системе. По крайней мере на момент написания статьи конфигурация на 100% рабочая, если аккуратно повторить все мои действия. Приступаем.

Сначала остановим и отключим firewalld:

```
# systemctl stop firewalld && systemctl disable firewalld
```

Это не значит, что его не надо настраивать. Сейчас другая тема статьи, для локализации проблем необходимо убрать все, что теоретически может мешать при неправильной настройке. Firewall нужно настраивать и у меня есть подробная инструкция по настройке iptables. Рекомендую с ней ознакомиться и аккуратно настроить iptables, когда все получится со squid.

Установим софт для добавления сервера в домен windows:

```
# yum -y install samba-winbind samba-winbind-clients pam_krb5 krb5-workstation ntp ntpdate
```

> Для продолжения настройки вам необходимо знать следующие вещи - FQDN имя контроллера домена, его ip адрес и учетную запись с правами на ввод компьютера в домен.

Первым делом вручную синхронизируем часы компьютера с контроллером домена:

```
# ntpdate winsrv.xs.local
```

Добавляем наш контроллер в список серверов для обновления в файле /etc/ntp.conf, запускаем ntp и добавляем в автозагрузку:

```
# systemctl enable ntpd
# systemctl start ntpd
```

> Синхронизация времени с контроллером домена не является обязательным действием. Но в случае расхождения времени более чем на 5 минут, будут возникать проблемы, которые на первый взгляд будут неочевидными и решать их трудно. Поэтому на всякий случай процедуру лучше провести. Очень подробно о настройке времени в CentOS 7 рассказано отдельно.

Выполняем команду для передачи настроек керберосу:

```
# authconfig --enablekrb5 --krb5kdc=winsrv.xs.local --krb5adminserver=winsrv.xs.local --krb5realm=WINSRV.XS.LOCAL --
enablewinbind --enablewinbindauth --smbsecurity=ads --smbrealm=XS.LOCAL --smbservers=winsrv.xs.local --smbworkgroup=XS --
winbindtemplatehomedir=/home/%U --winbindtemplateshell=/bin/bash --enablemkhomedir --enablewinbindusedefaultdomain --
update
```

Команда вся идет в одну строчку. Скопируйте ее сначала в текстовый файл и подредактируйте под свои параметры. Проверьте, что нигде не пропали и не добавились лишние пробелы, либо какие-то еще символы, тире должно быть двойным перед параметром. В данном случае:

- **xs** - название домена
- **winsrv** - имя контроллера домена
- **winsrv.xs.local** - полное имя домена

Вывод после работы команды будет такой:

```
Job for winbind.service failed. See 'systemctl status winbind.service' and 'journalctl -xn' for details.
getsebool: SELinux is disabled
```

Это нормально. Обращаю внимание, что SELinux у меня отключен.

Теперь заводим машину в домен:

```
# net ads join -U administrator
Enter administrators's password:
Using short domain name -- XS
Joined 'PROXY' to dns domain 'xs.local'
```

Вводим пароль, ждем некоторое время. Если ошибки не появилось, значит компьютер успешно включен в домен.

Теперь нужно запустить и добавить в автозагрузку winbind:

```
# systemctl start winbind
# systemctl enable winbind
```

Проверяем, все ли у нас корректно работает. Для начала проверим наличие доверительной учетной записи сервера на КД:

```
# wbinfo -t
checking the trust secret for domain XS via RPC calls succeeded
```

Все в порядке. Теперь проверяем, может ли наш сервер получать списки пользователей и групп. Первая команда выводит список всех групп домена,

вторая - всех пользователей:

```
# wbinfo -g
# wbinfo -u
```

Проверим авторизацию пользователя через winbind:

```
# wbinfo -a XS\\control%'pass'
plaintext password authentication succeeded
challenge/response password authentication succeeded
```

В данном случае **control** - имя пользователя домена, **pass** - его пароль. Успешная проверка выглядит так, как у меня.

Теперь запросим билетик кербероса:

```
# kinit administrator@XS.LOCAL
```

Дальше вводите пароль. Если ошибки не выскочило, значит все в порядке. Проверим билет командой:

```
# klist
Ticket cache: KEYRING:persistent:0:0
Default principal: administrator@XS.LOCAL

Valid starting Expires Service principal
12/04/2015 23:19:33 12/05/2015 09:19:33 krbtgt/XS.LOCAL@XS.LOCAL
renew until 12/11/2015 23:19:29
```

Все в порядке, проверки прошли. Мы полностью подготовили сервер к авторизации пользователей доменными учетными записями.

Настройка SQUID с ntlm авторизацией через домен

Дальше будет попроще. Если на предыдущем этапе вы все сделали правильно, то squid заработает без проблем. Устанавливаем его:

```
# yum -y install squid
```

Открываем файл конфигурации */etc/squid/squid.conf* и добавляем в самое начала следующие параметры:

```
auth_param ntlm program /usr/bin/ntlm_auth --diagnostics --helper-protocol=squid-2.5-ntlmssp --domain=XS
auth_param ntlm children 10
auth_param ntlm keep_alive off
acl auth proxy_auth REQUIRED
```

Не забудьте указать свой домен. Обращаю внимание на первую строку. В большинстве инструкций в интернете она выглядит немного не так, в ней нет дополнительных параметров. Без них у меня ntlm авторизация не хотела работать, я очень долго ее мучал.

Дальше находим в конфиге строку:

```
http_access allow localnet
```

Комментируем ее, она позволяет получить доступ всем компьютерам из локальной сети. После этой строки добавляем новую:

```
http_access allow auth
```

Разрешаем доступ только тем, кто прошел авторизацию. Запускаем squid и добавляем в автозагрузку:

```
# systemctl start squid
# systemctl enable squid
```

Все, можно идти проверять. Открываем браузер у какого-нибудь компьютера и указываем в качестве прокси ip адрес сервера, порт 3128. Пробуйте выйти в интернет.

Как понять, что все работает правильно:

1. Пользователя должно пустить в интернет.
2. В лог файле сквида должна быть информация об имени пользователя, который получает доступ. У меня это выглядит примерно вот так при открытии страницы яндекса:

```
# cat /var/log/squid/access.log | grep control

1449261311.346 9 10.1.4.189 TCP_MISS/304 438 GET http://yastatic.net/islands/_/S1-qWWyv85yFAtoHVvuxJXpOKA4.svg control
HIER_DIRECT/178.154.131.217 -
 1449261311.351 11 10.1.4.189 TCP_MISS/200 622 GET http://yastatic.net/www/_/_/y/ljN5poHcx67T3HSZuHbvf2NNk.png control
HIER_DIRECT/178.154.131.217 image/png
 1449261311.404 9 10.1.4.189 TCP_MISS/304 440 GET http://yastatic.net/morda-logo/i/disaster/metro11072015.png control
HIER_DIRECT/178.154.131.217 -
 1449261311.488 97 10.1.4.189 TCP_MISS/302 355 GET http://kiks.yandex.ru/fu control HIER_DIRECT/213.180.204.143 -
 1449261311.507 9 10.1.4.189 TCP_MISS/304 341 GET http://kiks.yandex.ru/system/fc07.swf control
HIER_DIRECT/213.180.204.143 -
```

В данном случае **control** - доменная учетная запись.

У нас получилась полностью дефолтная конфигурация, в которую мы просто добавили ntlm авторизацию и разрешили доступ в интернет только для тех, кто эту авторизацию прошел. Если компьютер находится не в домене, то при работе через прокси выскочит окно с авторизацией, в которую нужно будет ввести данные от учетной записи домена, чтобы получить доступ в интернет.

В таком виде конфигурация сервера уже вполне рабочая, можно пользоваться, подключать пользователей. Но это неудобно. Нужно средство для удобного управления списками доступа и просмотра статистики пользователей.

Установка и настройка sams2 в CentOS 7

И вот мы подошли самому главному и трудному. Когда я решил написать статью на эту тему, я подозревал, что установить sams2 в CentOS 7 будет тяжело, но не думал, что настолько. Пришлось разбить работу на два этапа. Первый этап мы уже прошли, а со вторым мне пришлось поковыряться не один день, пока все не получилось так, как хотелось.

Трудности тут с тем, что проект sams2 давно заброшен, под CentOS 7 он вообще не планировался, готового пакета нет. Есть только старые пакеты для 6-й версии и исходники. Я буду собирать sams2 из исходников и очень аккуратно опишу все этапы, по которым прошел. Столкнулся с множеством ошибок, пришлось немного править исходники, чтобы собранные версии нормально работали. Потом с настройками много нюансов, которые нигде не описаны, пришлось ковыряться самому.

Если все сделать по инструкции с сайта разработчика, то в CentOS 7 ничего не получится. Там как минимум есть 2 бага, которые не позволят собрать работающие программы и провести нормально установку.

В итоге у меня получилась конфигурация sams2, которая импортирует пользователей из AD, создает списки доступа к сайтам и позволяет отдельным пользователям блокировать различные сайты, плюс ведет статистику по пользователям в удобном виде.

Это тот функционал в sams2, который я настроил у себя и проверил. Возможно работает что-то еще, нужно проверять. Не все заявленные функции самс работают из коробки, их нужно с костылями настраивать и проверять. Я добился удовлетворяющего меня результата и остановился на этом.

Приступаем к работе. Нам нужно настроить web сервер для работы интерфейса sams. Можно воспользоваться моей инструкцией, можно чем-то еще. Не обязательно ставить apache, можно настроить на nginx и php-fpm, либо на lighttpd. Я для простоты все сделаю на апаче. Останавливаться подробно не буду на каждом из этапов, все описание есть в первой ссылке абзаца. Привожу только команды.

Устанавливаем httpd:

```
# yum install -y httpd
```

Добавляем в автозапуск и запускаем:

```
# systemctl enable httpd
# systemctl start httpd
```

Устанавливаем php и некоторые модули:

```
yum install -y php
yum install -y php-mysql php-mbstring php-mcrypt php-devel php-xml php-gd
```

Устанавливаем mariadb

```
yum install -y mariadb mariadb-server mariadb-devel
```

Обращаю внимание на последний пакет. Без него установить sams2 не получится, хотя его наличие в списке необходимых пакетов не очевидно. Я сначала его не установил и при сборке самс не видел у меня установленного сервера mysql.

Добавляем в автозапуск и запускаем:

```
# systemctl enable mariadb.service
# systemctl start mariadb
```

Задаем пароль рута:

```
# /usr/bin/mysql_secure_installation
```

Подключаем репозиторий epel и устанавливаем phpmyadmin. Это не обязательно, но мне с ним удобнее:

```
# yum -y install epel-release
# yum -y install phpmyadmin
```

Все подготовительные работы сделаны. Убедитесь, что у вас нормально работает веб сервер и скрипты php. Я не буду на этом останавливаться. Так удобнее будет для вас. Если сейчас не проверить веб сервер, то потом, если у вас недостаточно опыта в работе, вы не поймете, что у вас не работает - сам самс или что-то другое. Лучше все подготовить и проверить по отдельности.

Скачиваем исходники sams2 в домашний каталог root. Все работы будут проделываться под этой учетной записью.

```
# yum -y install wget
# cd /root
# wget https://github.com/PavelVinogradov/sams2/archive/master.zip
```

Ставим unzip и распаковываем архив:

```
# yum -y install unzip
# unzip master.zip
```

Исходники программы лежат в папке */root/sams2-master*. В ней ищем папку *src* и файл *proxy.h*. Его нужно будет отредактировать. Открываем редактором, ищем все строчки со значением **enum** и правим их:

```
# mcedit /root/sams2-master/src/proxy.h
```

Было так:

```
enum TrafficType
```

меняем на

```
enum TrafficType: long
```

И так все строчки с этим значением. Их должно быть 5 штук. Сохраняем файл и закрываем. Если не внести эти изменения и собрать исходники как есть, то sams2daemon будет падать с ошибкой:

```
kernel: sams2daemon[27541]: segfault at fffffffffffffe8 ip 00007fc54880944b sp 00007ffc8da37d20 error 5 in
libstdc++.so.6.0.19[7fc54874b000+e9000]
```

Это связано с тем, что CentOS 7 64-х битная система, а из этих исходников программа нормально собирается только на 32-х битных системах.

Теперь установим необходимые для сборки пакеты:

```
# yum -y install autoconf automake libtool pcre-devel libstdc++-devel gcc-c++
```

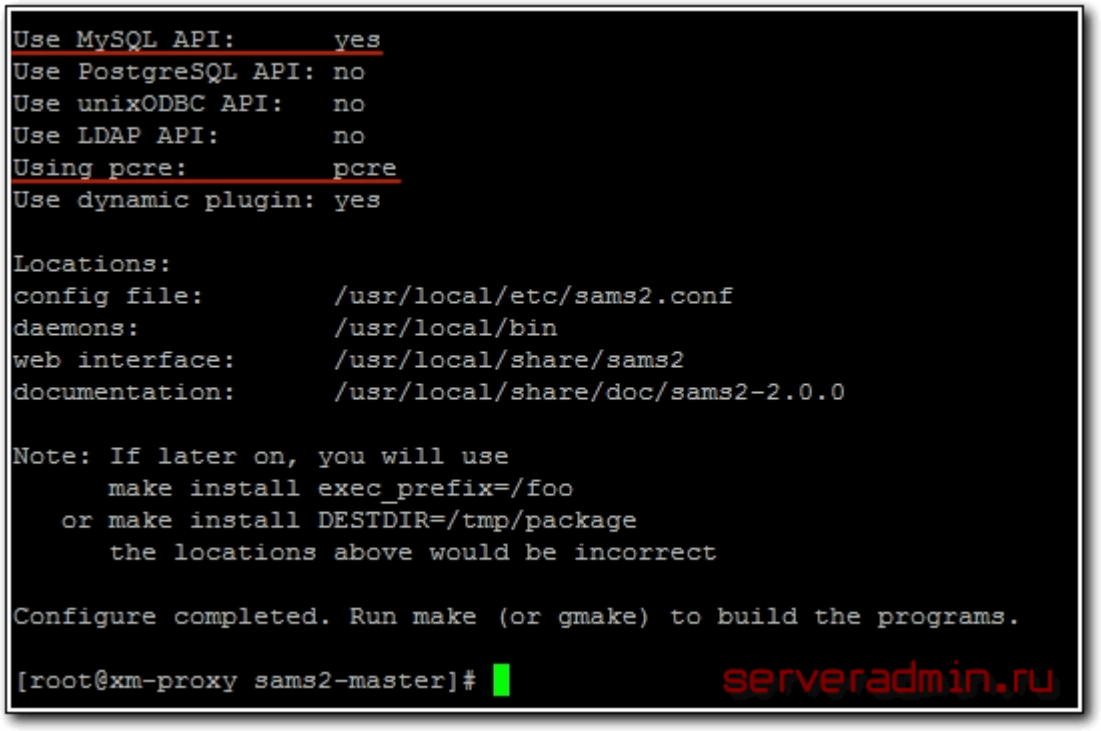
Переходим в каталог с исходниками и начинаем компиляцию:

```
# cd /root/sams2-master
# make -f Makefile.cvs
```

Запускаем скрипт автоматической конфигурации:

```
# sh ./configure
```

Он должен отработать без ошибок и в конце вывести полезную информацию:

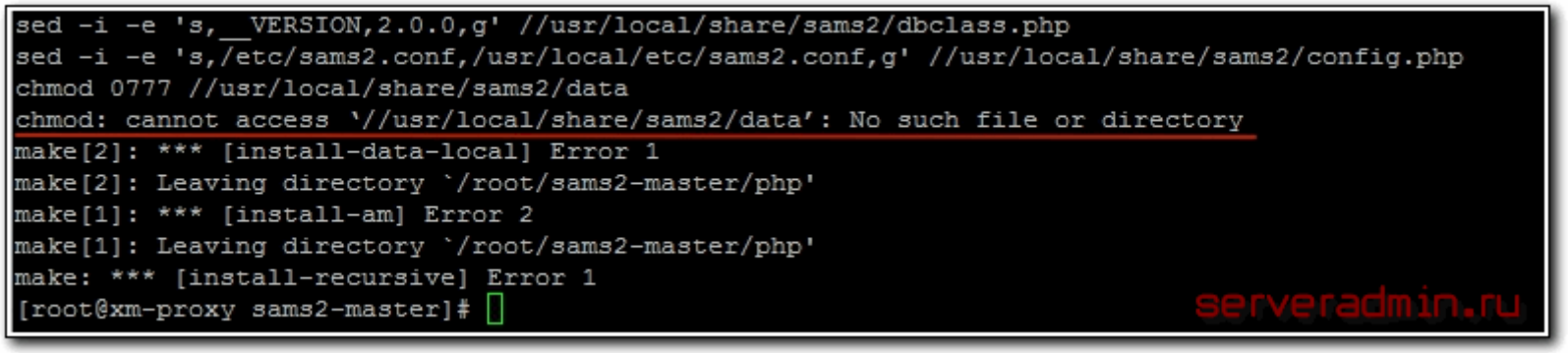


Сохраните пути, они позже пригодятся во время настройки. Обратите внимание на подчеркнутые строки. Без первой строки не будет поддержки mysql, без второй не заработают списки запрета доступа. Убедитесь, что все в порядке с ними.

Выполняем установку sams2:

```
# make install
```

У меня она почему-то проходит с ошибкой:



Суть ошибки в этой строке:

```
chmod: cannot access '//usr/local/share/sams2/data': No such file or directory
```

Я не знаю, почему инсталлятор не может создать эту папку сам. Хотя проблема возможно просто в ошибке в исходниках, в пути почему-то стоят два слеша в начале. Я просто руками создал эту директорию и заново запустил установку:

```
# cd /usr/local/share/sams2/
# mkdir data
# cd /root/sams2-master
# make install
```

Установка прошла успешно. Добавляем директорию с web интерфейсом sams2 в httpd. Для этого идем в директорию с конфигурациями и рисуем следующий файл настроек для самса:

```
# mcedit /etc/httpd/conf.d/sams2.conf
```

```
Alias /sams2 /usr/local/share/sams2
<Directory /usr/local/share/sams2/>
 AddDefaultCharset UTF-8
 <IfModule mod_authz_core.c>
  <RequireAny>
   Require ip 10.1.3.0/24 10.1.4.0/24
  </RequireAny>
 </IfModule>
</Directory>
```

10.1.3.0/24 10.1.4.0/24 - подсети из которых будет доступ к web интерфейсу. Можете просто указать ip адрес администратора, если доступ будет нужен только с его компьютера.

Удаляем те конфиги, которые самс сгенерировал автоматически, я с ними не мог зайти на сайт, не стал разбираться почему, просто сделал быстро сам настройки:

```
# rm /etc/httpd/conf.modules.d/doc4sams2.conf
# rm /etc/httpd/conf.modules.d/sams2.conf
```

Перезапускаем httpd:

```
# systemctl restart httpd
```

Теперь если зайти по адресу *htpp://ip-сервера/sams2* вы увидите сообщение:

```
Invalid query: Access denied for user 'apache'@'localhost' (using password: NO)
```

Это нормально. Пока так и должно быть.

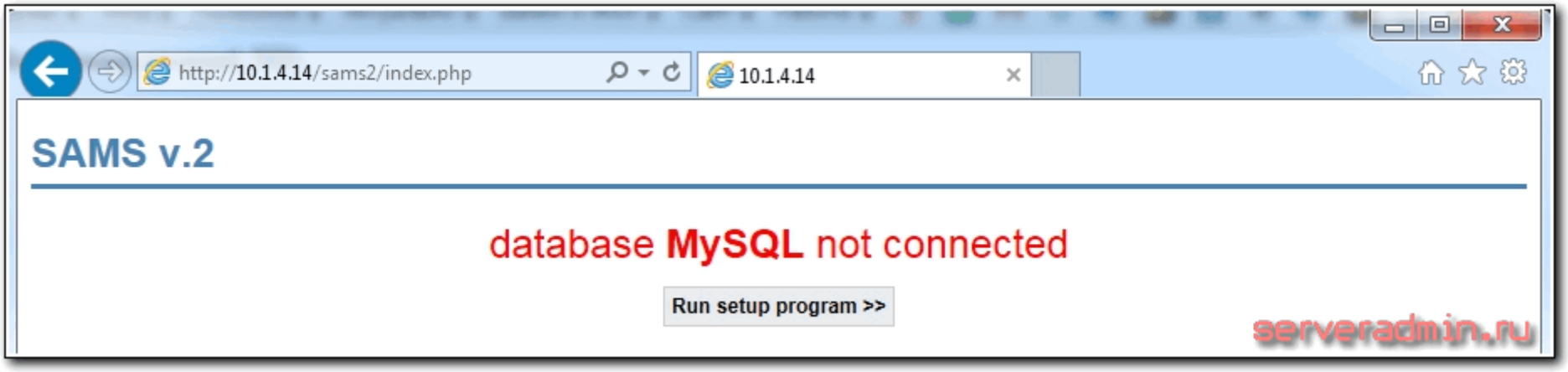
Редактируем конфигурационный файл *sams2.conf*:

```
# mcedit /usr/local/etc/sams2.conf
```

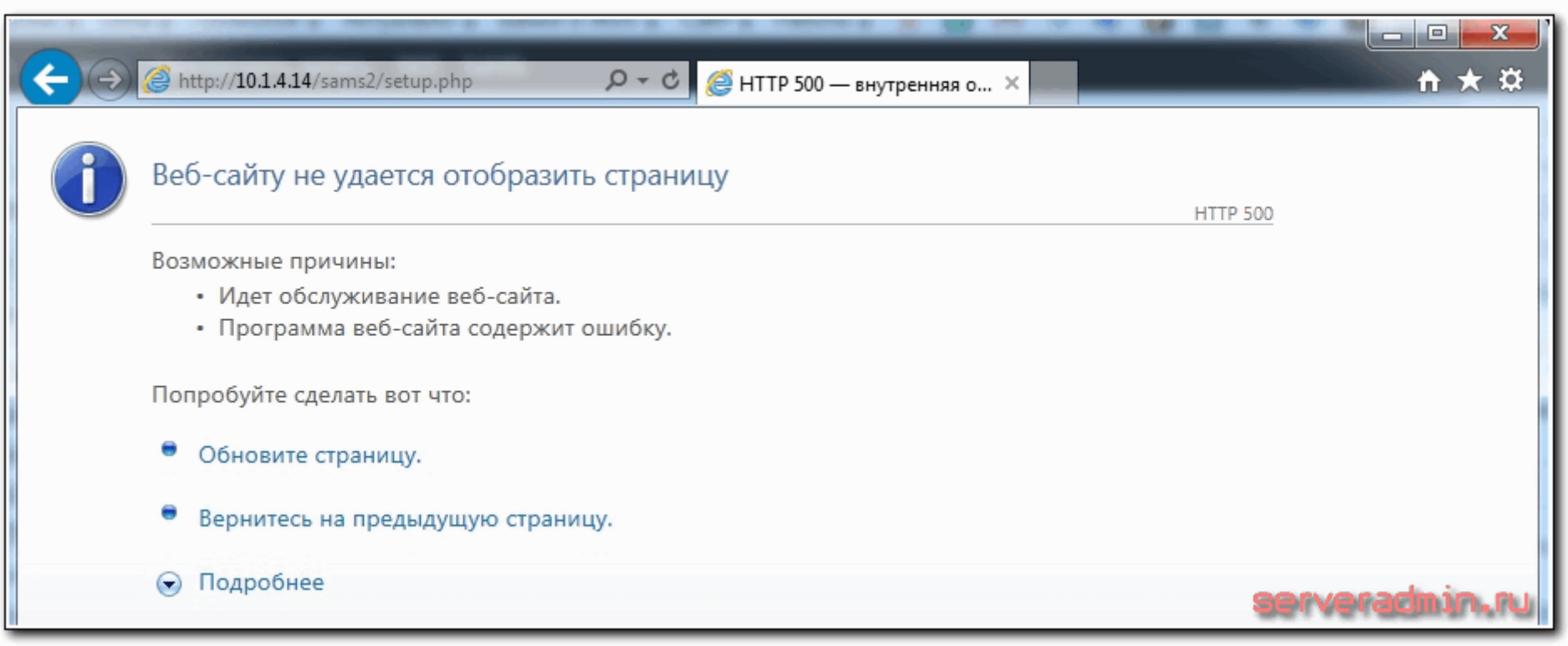
```
DB_ENGINE=MySQL
DB_SERVER=localhost
SAMS_DB=sams2db
ODBC=0
PDO=0
ODBCSOURCE=sams_mysql
DB_USER=root
DB_PASSWORD=rootpass
SQUIDCACHEFILE=access.log
SQUIDROOTDIR=/etc/squid
SQUIDLOGDIR=/var/log/squid
SQUIDCACHEDIR=/var/spool/squid
WBINFOPATH=/usr/local
SAMSPATH=/usr/local
SQUIDPATH=/usr/sbin
```

```
SQUIDGUARDLOGPATH=/var/log
SQUIDGUARDDBPATH=/var/db/squidguard
RECODECOMMAND=iconv -f KOI8-R -t 866 %finp > %fout
REJIKPATH=/usr/local/rejik
SHUTDOWNCOMMAND=shutdown -h now
CACHENUM=1
```

В качестве пользователя mysql указываем пока рута. Сохраняем файл и идем снова в веб-интерфейс, обновляем страничку. У вас должна загрузиться следующая информация:



Нажимаем **Run setup program >>** . И получаем сообщение об ошибке:



При этом в логе httpd следующая информация:

```
# cat /var/log/httpd/error_log

PHP Parse error: syntax error, unexpected '$configbuttom_7_log_2' (T_VARIABLE) in /usr/local/share/sams2/lang/lang.EN on
line 1100, referer: http://10.1.4.14/sams2/index.php
```

Это очередной баг самс2. Чтобы его исправить, открываем на редактирование файл */usr/local/share/sams2/lang/lang.EN* идем на строку 1100 и после нее

убираем все пробелы перед последующими строками:

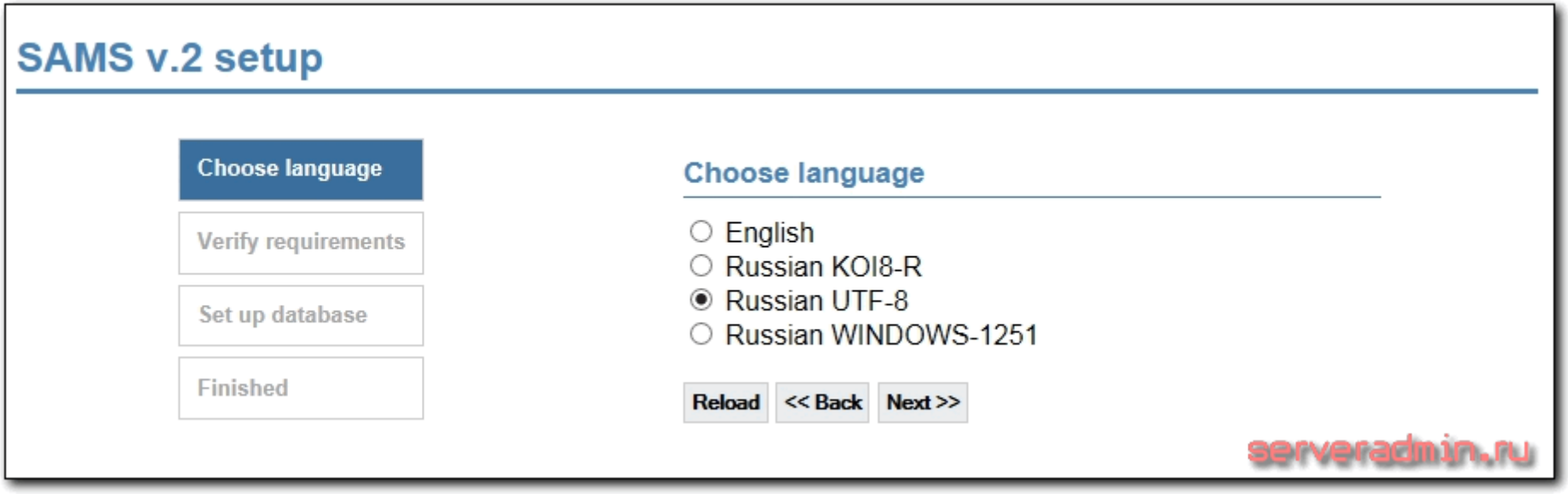
```
# mcedit /usr/local/share/sams2/lang/lang.EN
```

Делаем так:

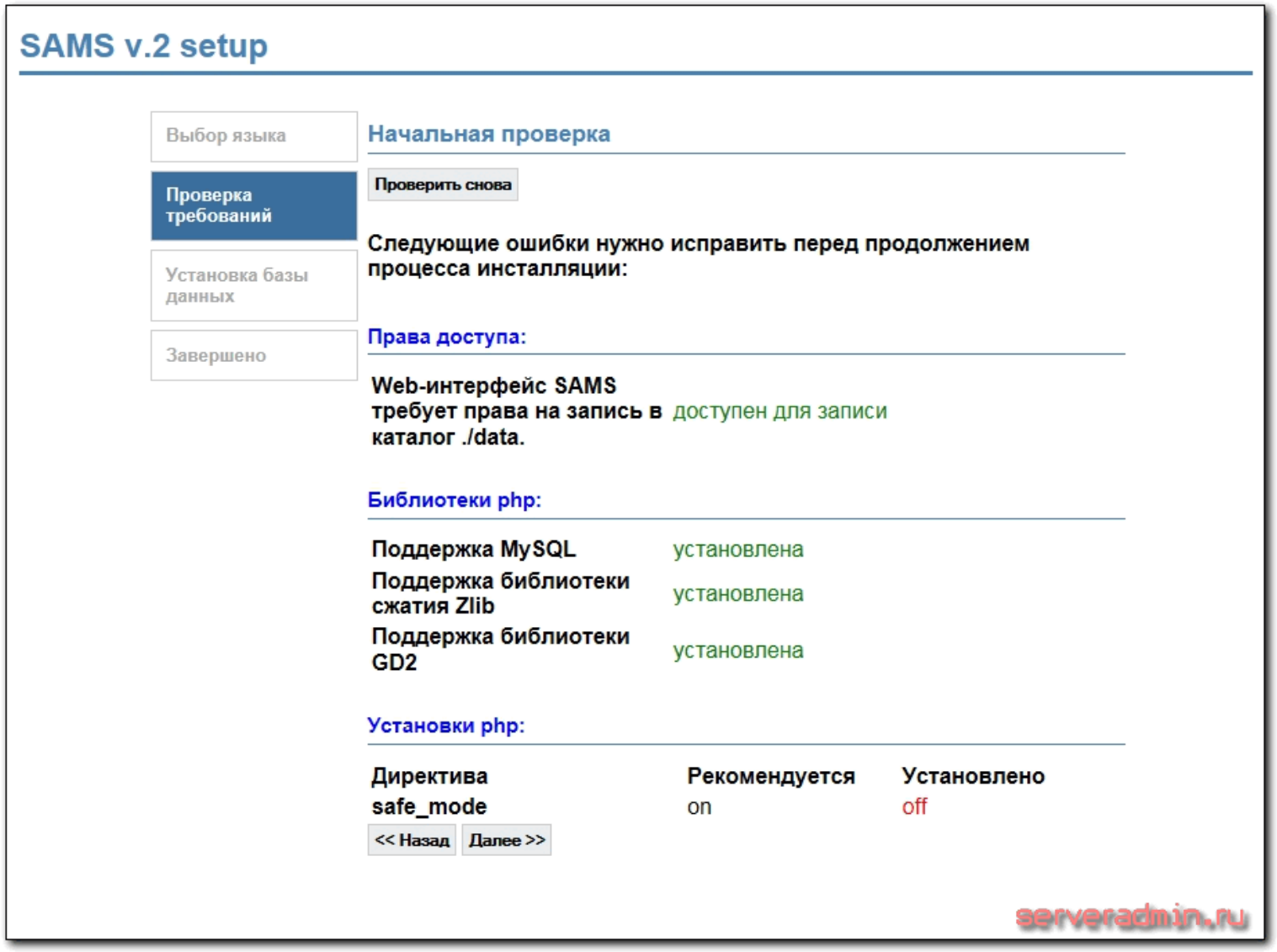
```
    $adminbuttom_1_prop_SamsReConfigForm_54="Displacement from the file beginning access.log (byte)";
    $configbuttom_3_import_ImportProxySettings_1="import proxy settings";
    $usersbuttom_1_domain_AddUsersFromDomainForm_8="Create new group";
    $usersbuttom_1_domain_AddUsersFromDomainForm_9="Group name";
    $admintray_admintray_1="SAMS management interface";
    $configbuttom_7_log_1 = "View SAMS logs";
$configbuttom_7_log_2 = "Item number";
$configbuttom_7_log_3 = "Date";
$configbuttom_7_log_4 = "Time";
$configbuttom_7_log_5 = "Demon";
$configbuttom_7_log_6 = "Value";
$configbuttom_7_log_7 = "Return code";
$configbuttom_7_log_8 = "Clear the logs for the period";
$configbuttom_7_log_9 = "Logs cleaned";
$configbuttom_8_db_1="SAMS Database Maintenance";
$configbuttom_8_db_2="Number of records about the traffic on the SAMS database";
$configbuttom_8_db_3="start date";
$configbuttom_8_db_4="end date";
$configbuttom_8_db_5="Number of log entries ";
$configbuttom_8_db_6="Number of URL in deny access lists";
$configbuttom_8_db_7="Deleting data in the database";
$configbuttom_8_db_8="Clear data";
$configbuttom_8_db_9="Nothing to clean";
$configbuttom_8_db_10="Cleaning of traffic data users";
$configbuttom_8_db_11="Cleaning the SAMS log data";
$configbuttom_8_db_12="Remove of users traffic data";
$configbuttom_8_db_13="The data is deleted";
$configbuttom_8_db_14="Cleaning data";
$configbuttom_8_db_15="Nothing selected";

?>
```

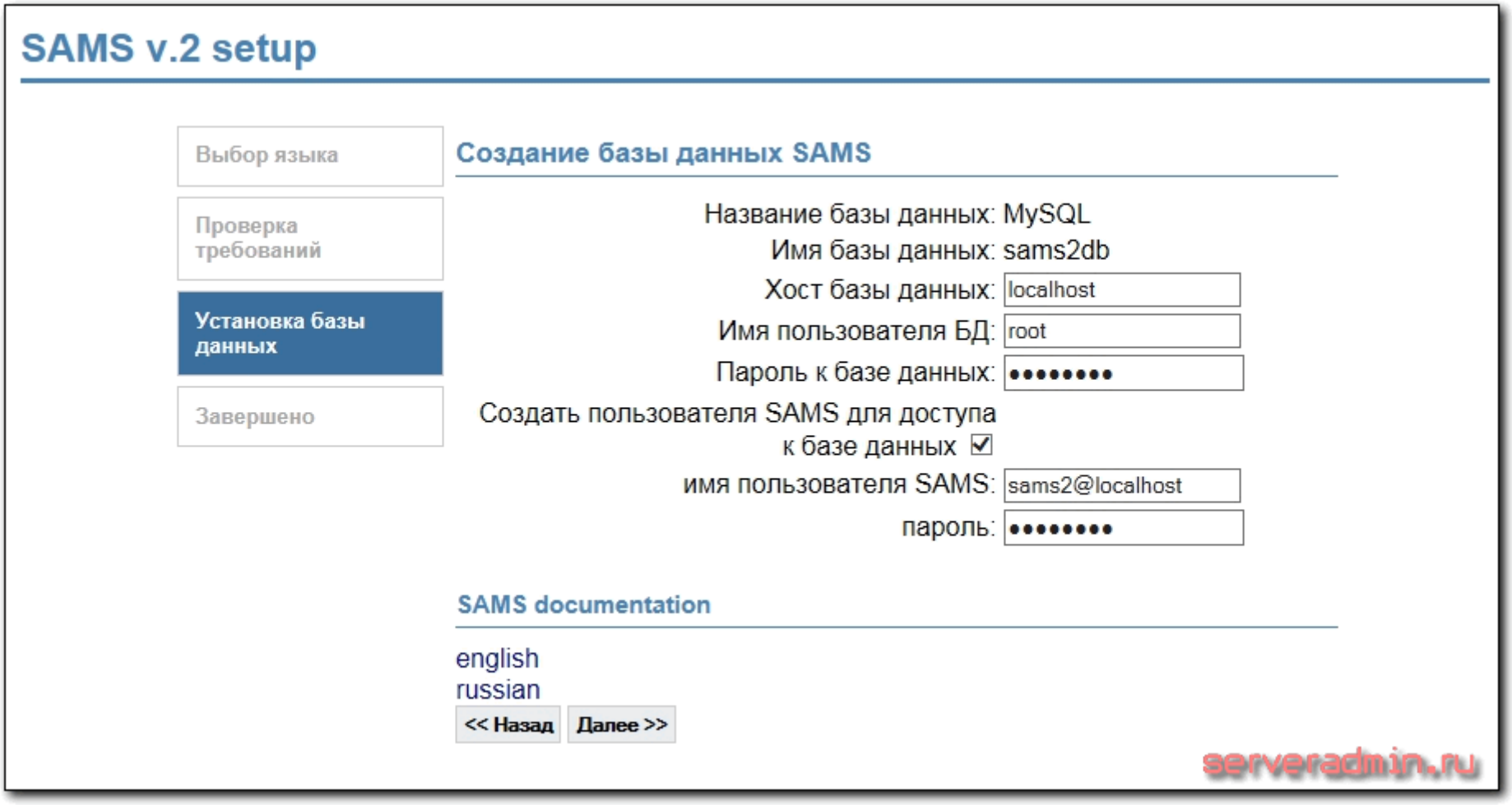

Сохраняем файл, идем в веб интерфейс и перезагружаем страничку. Должны увидеть форму выбора языка. Выбираем русский:



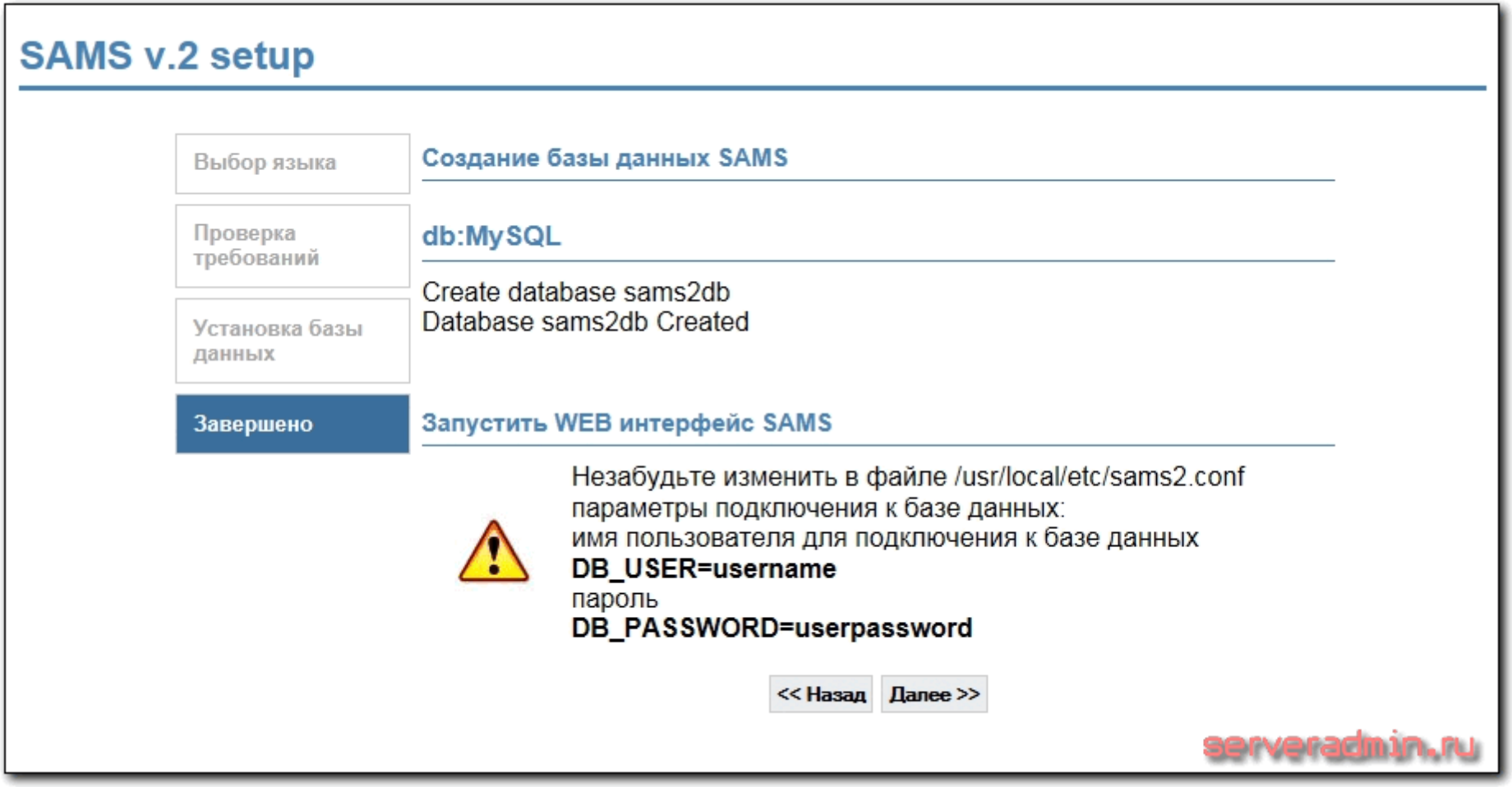
Проходит проверка требований. У меня такие результаты:


SAMS v.2 setup
Выбор языка
Проверка требований
Установка базы данных
Завершено
Начальная проверка
Проверить снова
Следующие ошибки нужно исправить перед продолжением процесса инсталляции:
Права доступа:
Web-интерфейс SAMS требует права на запись в каталог ./data.
доступен для записи
Библиотеки php:
Поддержка MySQL
установлена
Поддержка библиотеки сжатия Zlib
установлена
Поддержка библиотеки GD2
установлена
Установки php:
Директива
Рекомендуется
Установлено
safe_mode
on
off
<< Назад
Далее >>
serveradmin.ru

Создаем базу данных. Убедитесь, что пользователя и базы данных для самс, которые вы будете указывать, у вас еще нет в mysql, иначе получите ошибку. Заполняете данные для root и для нового пользователя:



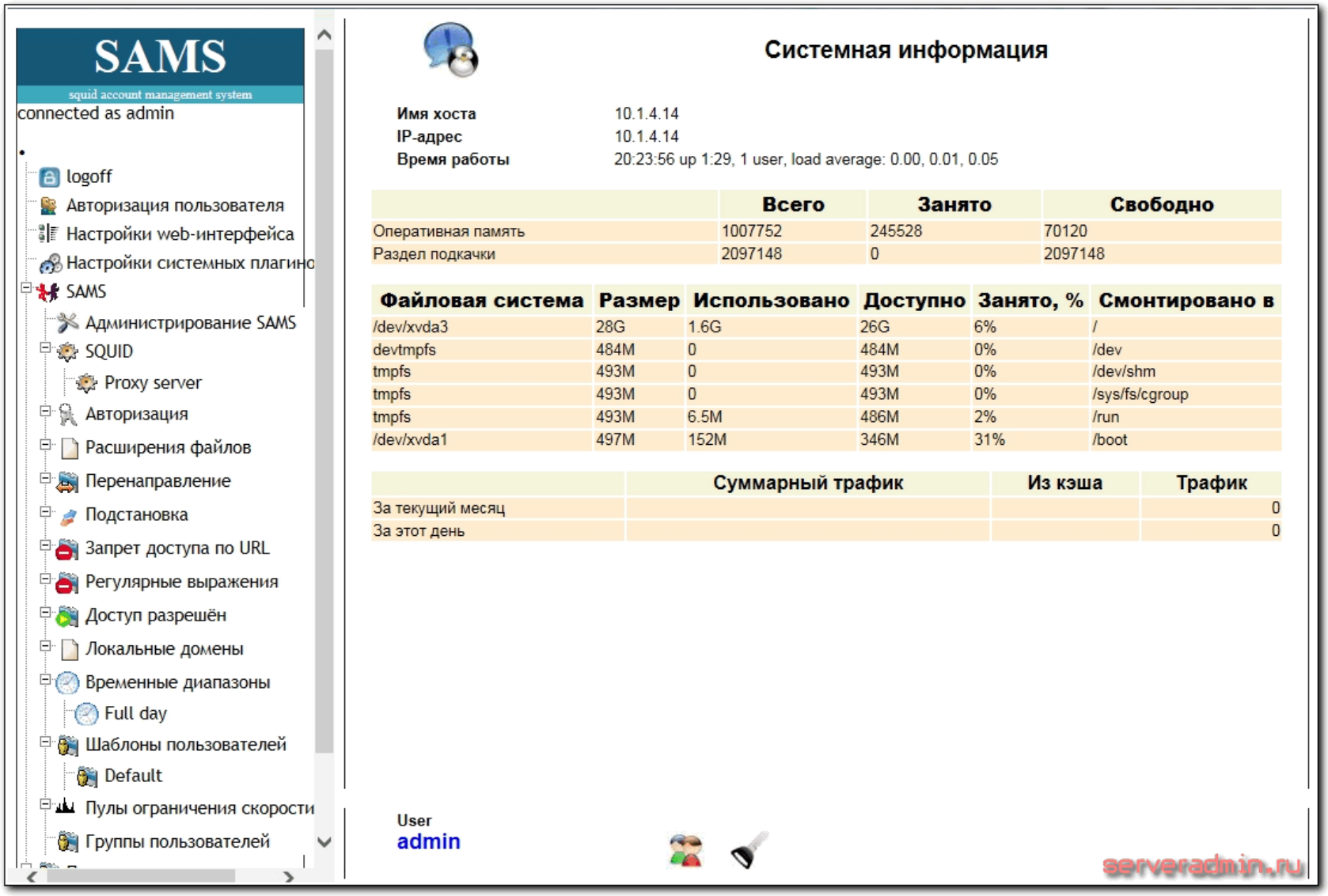
Установка прошла успешно:



Теперь нужно снова отредактировать файл *sams2.conf* и заменить пользователя mysql на только что созданного:

```
# mcedit /usr/local/etc/sams2.conf
```

Проверим работу веб интерфейса. Переходим снова по адресу http://ip-сервера/sams2. Мы должны увидеть окно авторизации. Нажимаем снизу на *Авторизация администратора SAMS* и вводим пользователя **admin**, пароль - **qwerty**. Открывается главное окно системы:


SAMS
squid account management system
connected as admin
logoff
Авторизация пользователя
Настройки web-интерфейса
Настройки системных плагино
SAMS
Администрирование SAMS
SQUID
Proxy server
Авторизация
Расширения файлов
Перенаправление
Подстановка
Запрет доступа по URL
Регулярные выражения
Доступ разрешён
Локальные домены
Временные диапазоны
Full day
Шаблоны пользователей
Default
Пулы ограничения скорости
Группы пользователей
Системная информация
Имя хоста 10.1.4.14
IP-адрес 10.1.4.14
Время работы 20:23:56 up 1:29, 1 user, load average: 0.00, 0.01, 0.05
Всего Занято Свободно
Оперативная память 1007752 245528 70120
Раздел подкачки 2097148 0 2097148
Файловая система Размер Использовано Доступно Занято, % Смонтировано в
/dev/xvda3 28G 1.6G 26G 6% /
devtmpfs 484M 0 484M 0% /dev
tmpfs 493M 0 493M 0% /dev/shm
tmpfs 493M 0 493M 0% /sys/fs/cgroup
tmpfs 493M 6.5M 486M 2% /run
/dev/xvda1 497M 152M 346M 31% /boot
Суммарный трафик Из кэша Трафик
За текущий месяц 0
За этот день 0
User
admin
serveradmin.ru

Теперь нам нужно запустить демон **sams2daemon**. Создадим скрипт запуска. Для этого идем в папку */root/sams2-master/redhat* и редактируем файл **init.d**:

```
# mcedit /root/sams2-master/redhat/init.d
```

Находим там значение **__CONFDIR** и меняем его на **/usr/local/etc/**, значение **__PREFIX** меняем на **/usr/local/bin/**. У вас должны получиться 2 измененные строки следующего вида, остальные оставляем как есть:

```
[ -f /usr/local/etc/sams2.conf ] || exit 0
DAEMON=/usr/local/bin/sams2daemon
```

Копируем скрипт запуска в папку /etc/*init.d*:

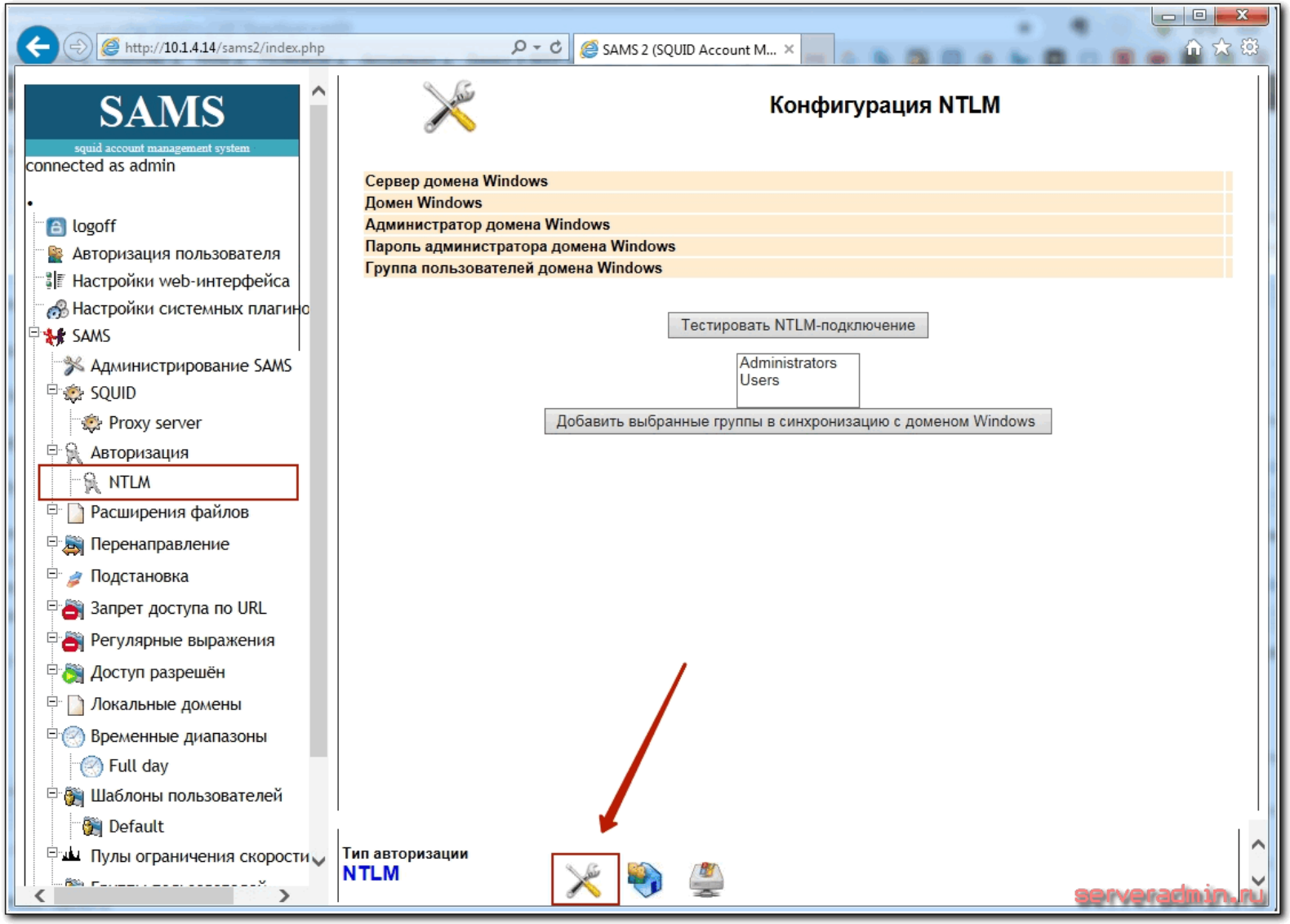
```
# cp /root/sams2-master/redhat/init.d /etc/init.d/sams2
```

Запускаем демон:

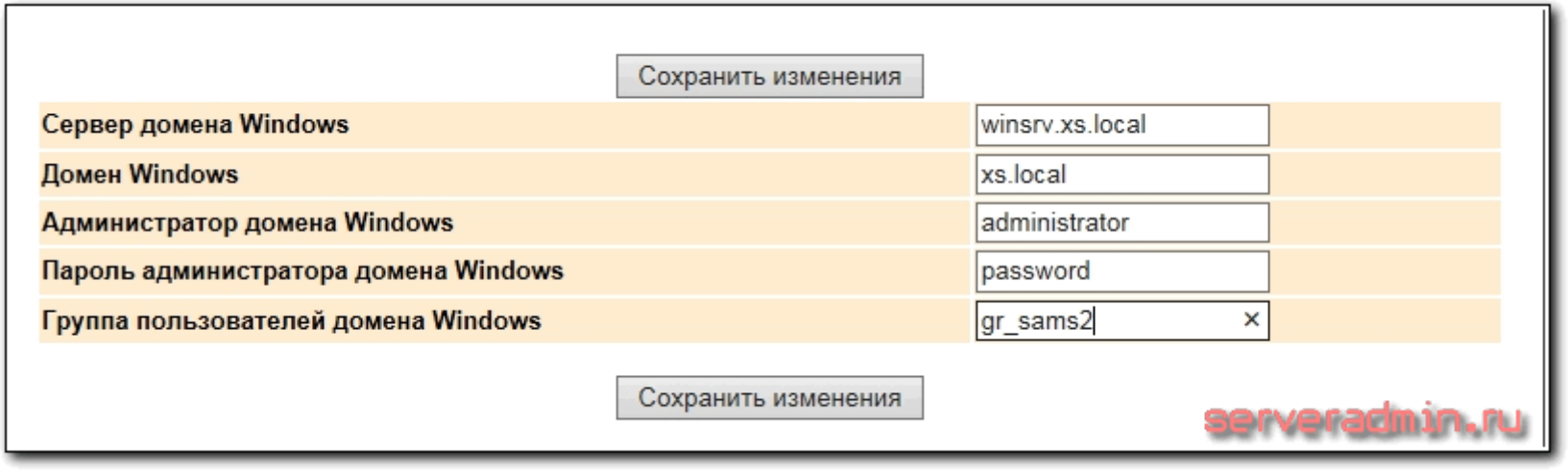
```
# /etc/init.d/sams2 start
Starting sams2 (via systemctl): [ OK ]
```

Если будут какие-то ошибки, то смотрите общий лог messages.

На этом установка sams2 закончена. Можно приступать к настройке. Здесь она может отличаться, в зависимости от того, что вы хотите получить. Добавим в sams пользователей из домена. Для этого заходим в веб интерфейс и идем в раздел **Авторизация**. Убираем все галочки, оставляем только NTLM и жмем Конфигурировать. Появляется новый подпункт NTLM. Заходим в него и нажимаем снизу на отвертку и ключ:

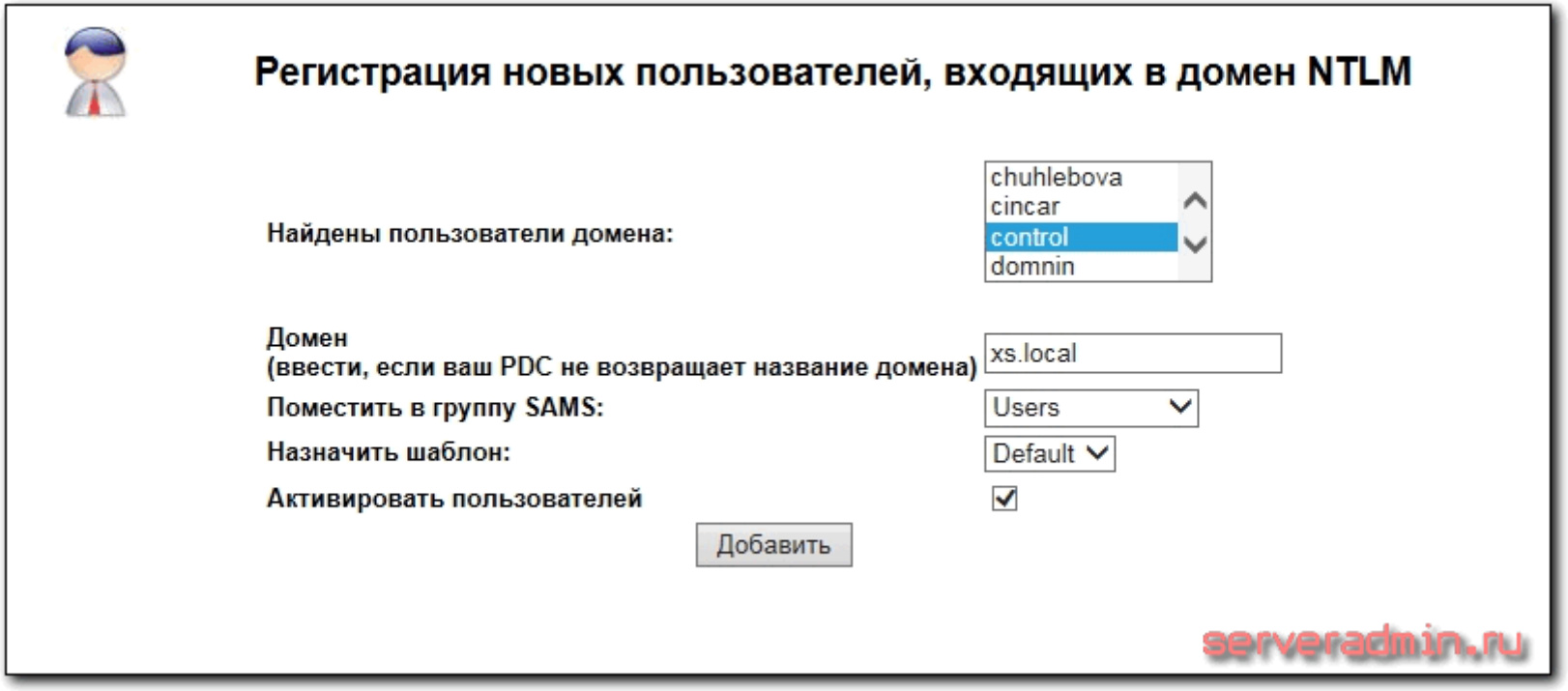

http://10.1.4.14/sams2/index.php
SAMS 2 (SQUID Account M...
SAMS
squid account management system
connected as admin
logoff
Авторизация пользователя
Настройки web-интерфейса
Настройки системных плагино
SAMS
Администрирование SAMS
SQUID
Proxy server
Авторизация
NTLM
Расширения файлов
Перенаправление
Подстановка
Запрет доступа по URL
Регулярные выражения
Доступ разрешён
Локальные домены
Временные диапазоны
Full day
Шаблоны пользователей
Default
Пулы ограничения скорости
Конфигурация NTLM
Сервер домена Windows
Домен Windows
Администратор домена Windows
Пароль администратора домена Windows
Группа пользователей домена Windows
Тестировать NTLM-подключение
Administrators
Users
Добавить выбранные группы в синхронизацию с доменом Windows
Тип авторизации
NTLM
serveradmin.ru

Заполняем настройки. В моем случае они выглядели вот так:

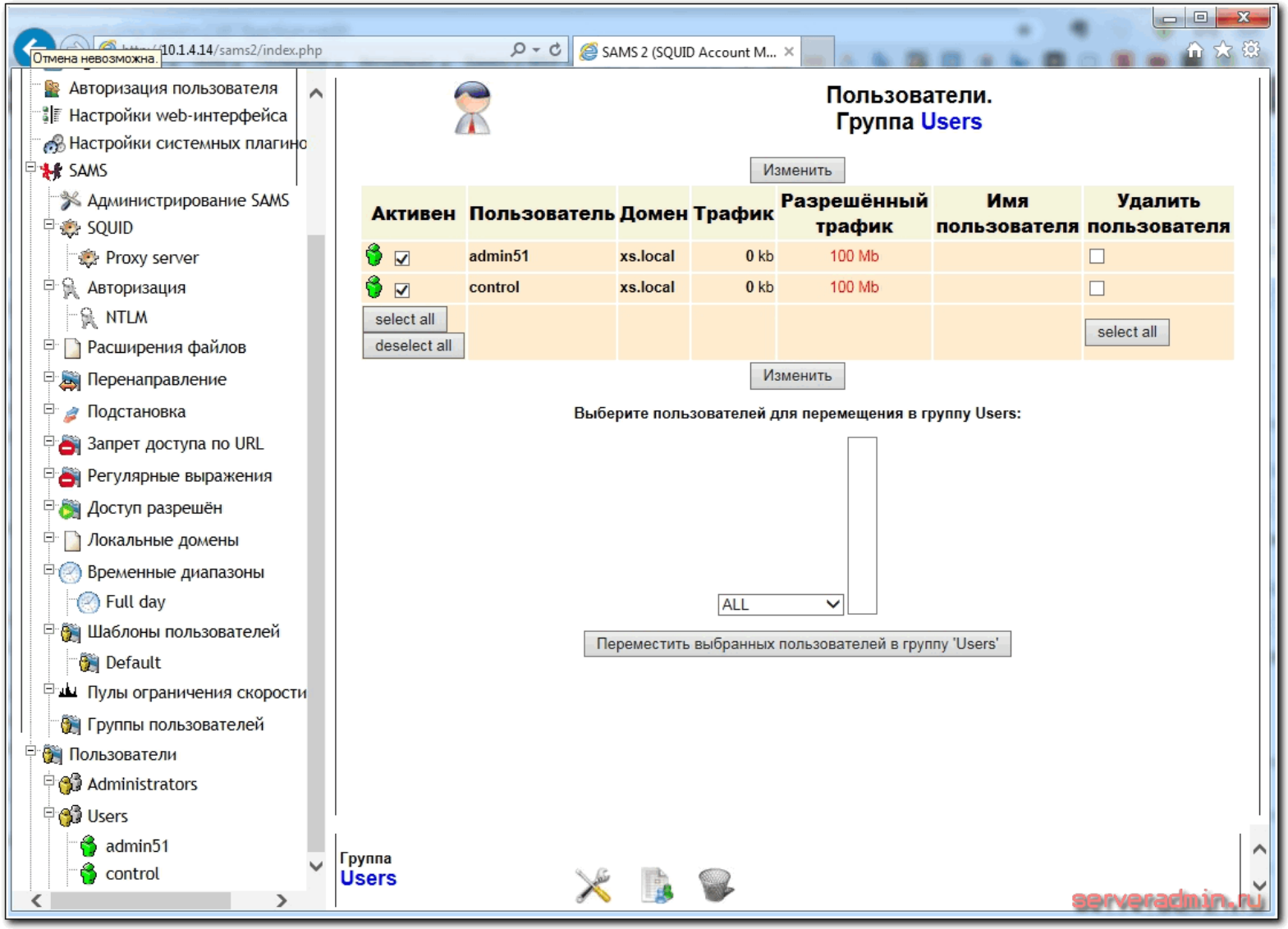


Если все правильно ввели, то при нажатии на кнопку **Тестировать NTLM-подключение** вы увидите список пользователей и групп домена.

Чтобы добавить пользователей домена в качестве пользователей самс, необходимо в разделе NTLM снизу нажать на кнопку с домиком и подписью *Регистрация новых пользователей, входящих в домен Windows*. Выбрать через контрол всех пользователей, которых хотите добавить и нажать **Добавить**.

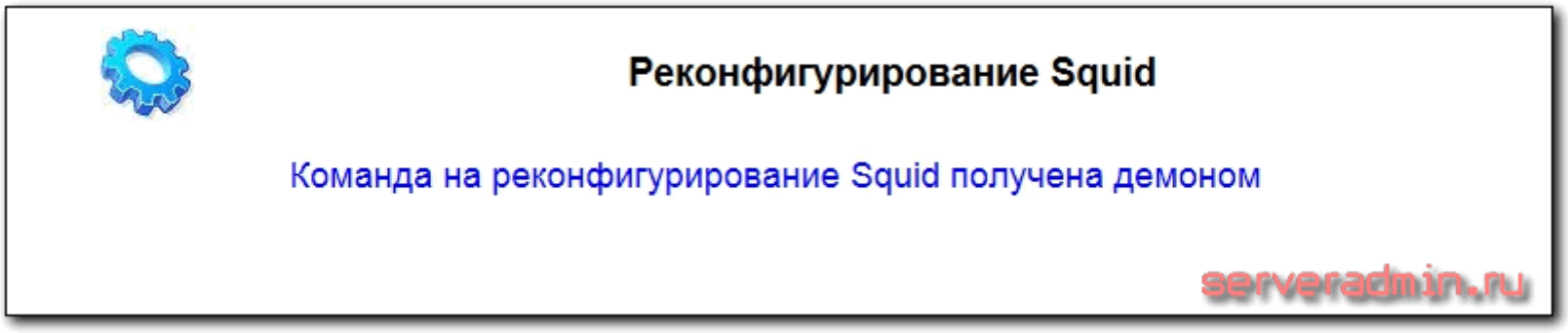


Они появятся в списке пользователей:


Отмена невозможна.
10.1.4.14/sams2/index.php
SAMS 2 (SQUID Account M...
Авторизация пользователя
Настройки web-интерфейса
Настройки системных плагино
SAMS
Администрирование SAMS
SQUID
Proxy server
Авторизация
NTLM
Расширения файлов
Перенаправление
Подстановка
Запрет доступа по URL
Регулярные выражения
Доступ разрешён
Локальные домены
Временные диапазоны
Full day
Шаблоны пользователей
Default
Пулы ограничения скорости
Группы пользователей
Пользователи
Administrators
Users
admin51
control
Пользователи.
Группа Users
Изменить
Активен
Пользователь
Домен
Трафик
Разрешённый трафик
Имя пользователя
Удалить пользователя
admin51
xs.local
0 kb
100 Mb
control
xs.local
0 kb
100 Mb
select all
deselect all
select all
Изменить
Выберите пользователей для перемещения в группу Users:
ALL
Переместить выбранных пользователей в группу 'Users'
Группа
Users
serveradmin.ru

Чтобы не было ограничения по трафику (вряд ли оно кому-то нужно в наше время), необходимо отредактировать соответствующий параметр в шаблоне **Default**.

Теперь нужно применить сделанные настройки. Для этого идем в раздел **SQUID -> Proxy server** и жмем снизу на вторую кнопку слева со стрелочками. Нажимаем на **Реконфигурировать**. В случае успеха увидите надпись:



На всякий случай можно проверить конфиг squid. Там должны появиться только что созданные acl. В моем случае появились следующие строки в конфигурации. Пошел проверять конфиг и обнаружил, что там ничего не появилось. Это связано с тем, что sams редактирует конфиг сквида, ориентируясь на комментарии с метками **TAG:**. В CentOS 7 после установки конфиг сквида очень сокращен, в нем почти нет комментариев, представлена минимальная конфигурация. Указанных меток там тоже нет, нам их нужно добавить самим. Добавляем в */etc/squid/squid.conf* следующие комментарии с метками:

```
# TAG: acl

# TAG: url_rewrite_access

# TAG: url_rewrite_program

# TAG: url_rewrite_children

# TAG: delay_pools
```

```
# TAG: delay_class

# TAG: delay_access

# TAG: delay_parameters

# TAG: http_access

# TAG: http_access2

# TAG: icp_access
```

Обязательно пустая строка после каждой метки. Теперь заново перезапускаем squid через веб интерфейс самса. Должны появиться изменения в конфиге. У меня добавились следующие строки:

```
# TAG: acl
acl Sams2Time1 time MTWHFAS 23:00-23:59
acl Sams2Template1 proxy_auth admin51
acl Sams2Template1 proxy_auth control

# TAG: http_access
# Setup Sams2 HTTP Access here
http_access allow Sams2Template1 Sams2Time1
```

> Обращаю внимание на параметр на acl Sams2Time1. По-умолчанию там указан временной интервал с 23:00 до 23:59. В соответствии с этими настройками доступ в интернет будет предоставлен только в это время. Подозреваю, что это ошибка автора, но мне пришлось потратить некоторое время, чтобы понять, почему правильная на первый взгляд конфигурация не работает. Если вам не нужен этот

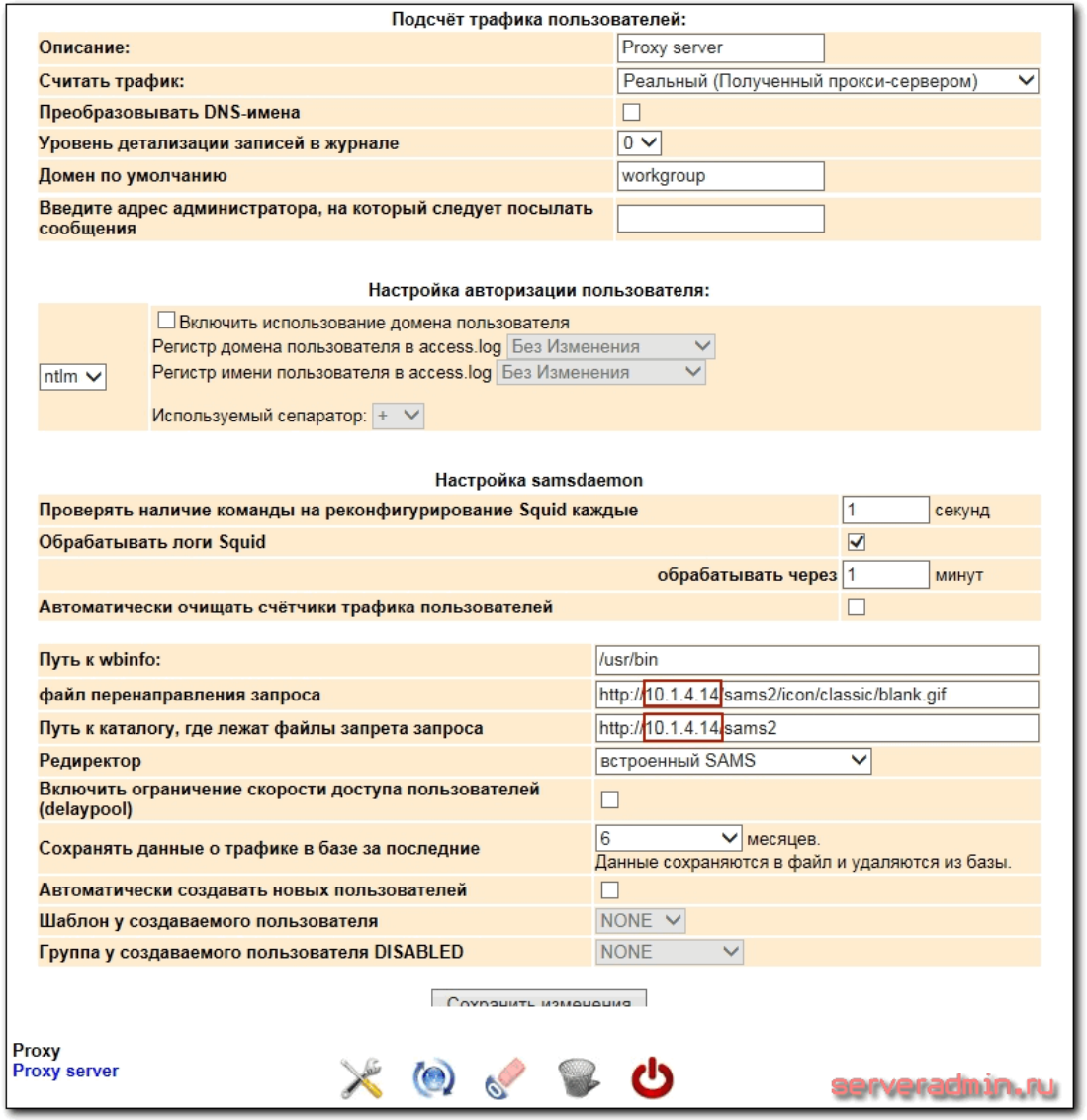
параметр, то уберите вообще временной интервал, либо исправьте его на 00:00-23:59.

Для корректной работы конфигурации необходимо убрать все остальные acl и http_access от предыдущей конфигурации squid, когда самс еще не был установлен.

Еще у меня были добавлены следующие строки:

```
# TAG: url_rewrite_access
acl Sams2Proxy dst your.ip.address
url_rewrite_access deny Sams2Proxy
```

Из-за значения **your.ip.address** сквид писал об ошибке конфигурации. Чтобы самс писал сюда нормальное значение в виде ip адреса сервера, необходимо изменить его настройки. Делается это в разделе **SQUID -> Proxy server**, снизу кнопочка с отверткой и ключом. Нажимаем на нее и изменяем снизу 2 настройки, указывая свой ip адрес:

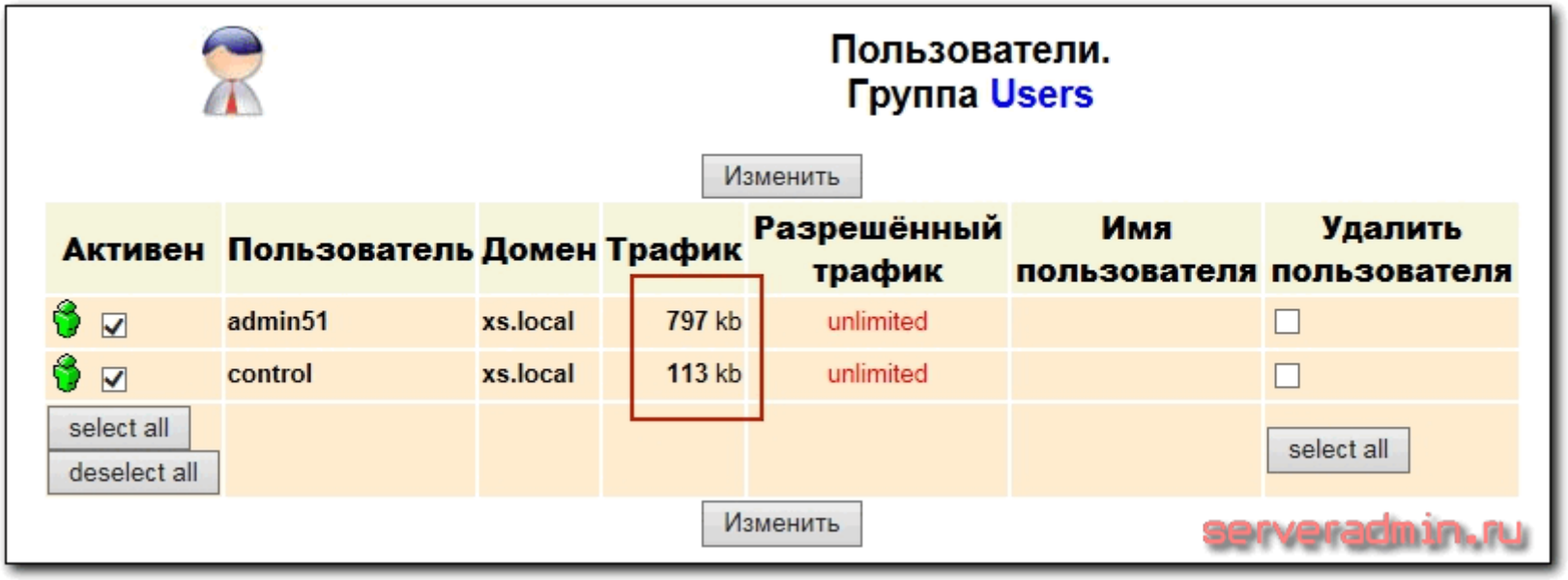

Подсчёт трафика пользователей:
Описание:
Proxy server
Считать трафик:
Реальный (Полученный прокси-сервером)
Преобразовывать DNS-имена
Уровень детализации записей в журнале
0
Домен по умолчанию
workgroup
Введите адрес администратора, на который следует посылать сообщения
Настройка авторизации пользователя:
Включить использование домена пользователя
Регистр домена пользователя в access.log
Без Изменения
ntlm
Регистр имени пользователя в access.log
Без Изменения
Используемый сепаратор:
+
Настройка samsdaemon
Проверять наличие команды на реконфигурирование Squid каждые
1
секунд
Обрабатывать логи Squid
обрабатывать через
1
минут
Автоматически очищать счётчики трафика пользователей
Путь к wbinfo:
/usr/bin
файл перенаправления запроса
http://10.1.4.14/sams2/icon/classic/blank.gif
Путь к каталогу, где лежат файлы запрета запроса
http://10.1.4.14/sams2
Редиректор
встроенный SAMS
Включить ограничение скорости доступа пользователей (delaypool)
Сохранять данные о трафике в базе за последние
6
месяцев.
Данные сохраняются в файл и удаляются из базы.
Автоматически создавать новых пользователей
Шаблон у создаваемого пользователя
NONE
Группа у создаваемого пользователя DISABLED
NONE
Proxy
Proxy server
serveradmin.ru

Попутно на всякий случай проверьте остальные настройки. Я кое-что подредактировал под свои нужды. Сохраняете настройки и снова перезапускаете сквид через самс. Проверяем файл конфигурации squid.conf:

```
# cat squid.conf | grep Sams2Proxy
acl Sams2Proxy dst 10.1.4.14
```

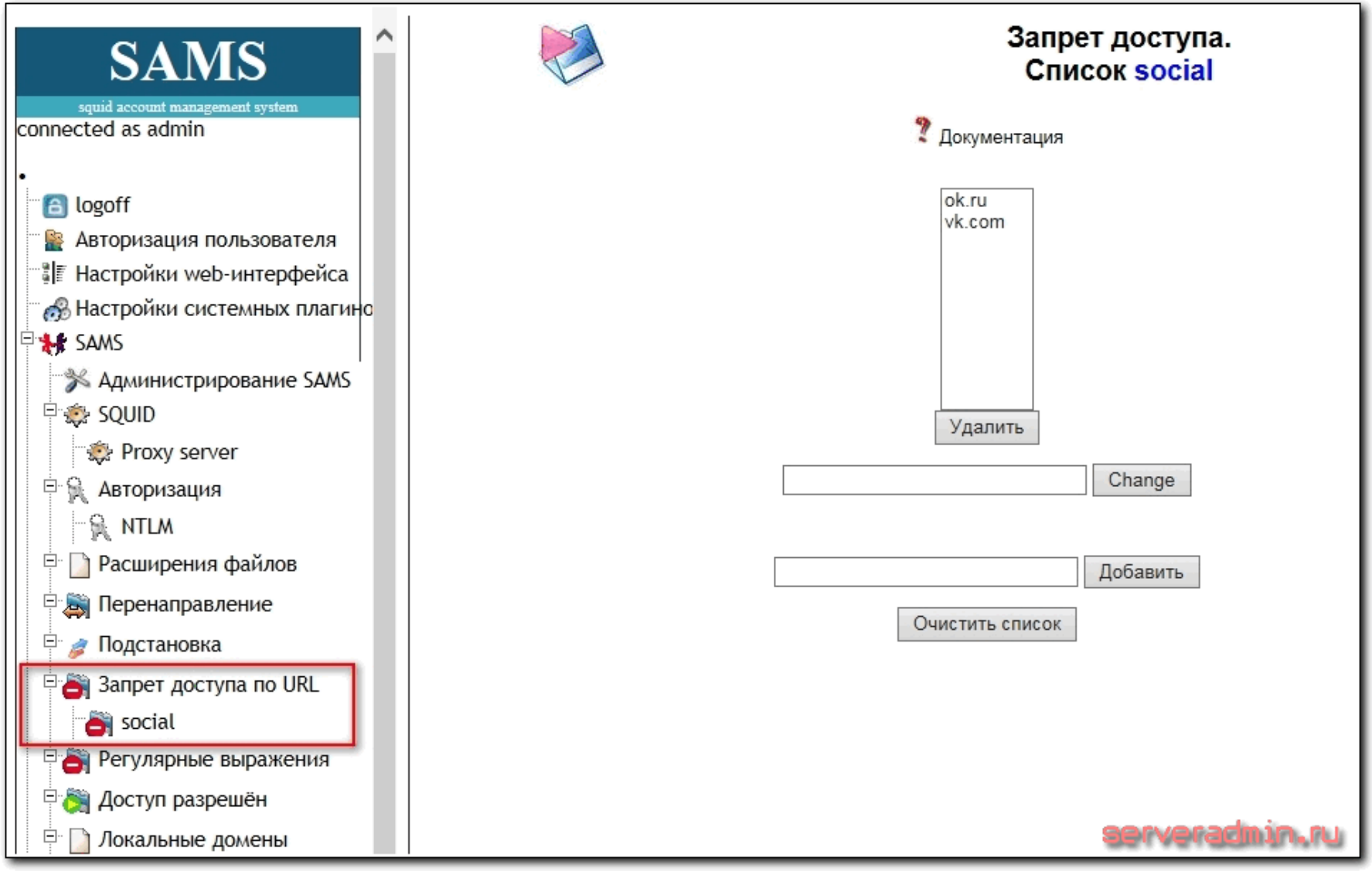
В строке появился реальный адрес и сквид больше не ругается на ошибку конфигурации.

Сейчас можно проверять работу. Заходим добавленными пользователями на компьютеры домена, указываем настроенный прокси сервер и серфим. Через некоторое время проверяем статистику в sams. Должны побежать килобайты:

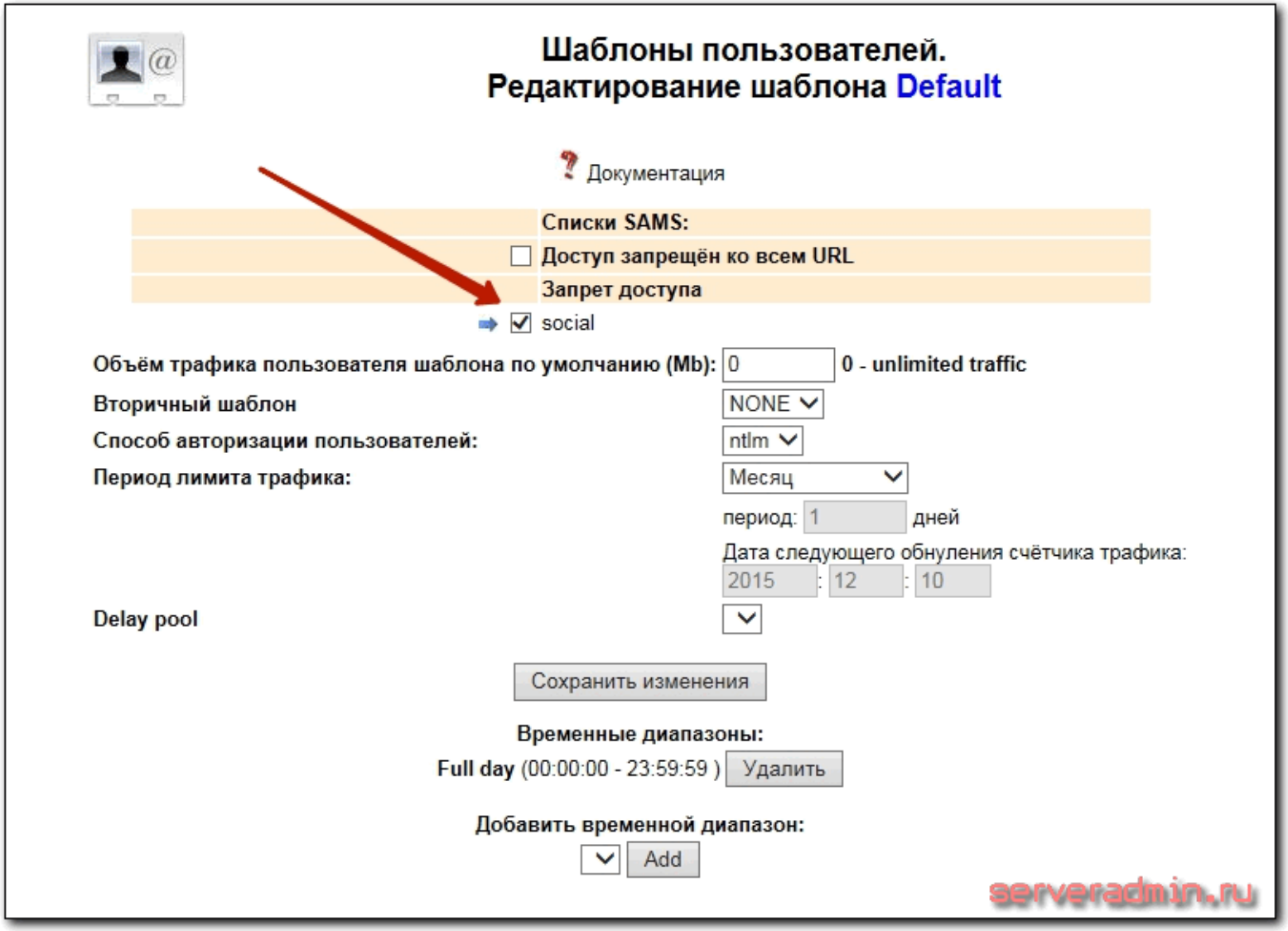


Теперь добавим ограничение для доступа к некоторым сайтам. Для этого идем в раздел **Запрет доступа по URL** и создаем новый список. Я создал список

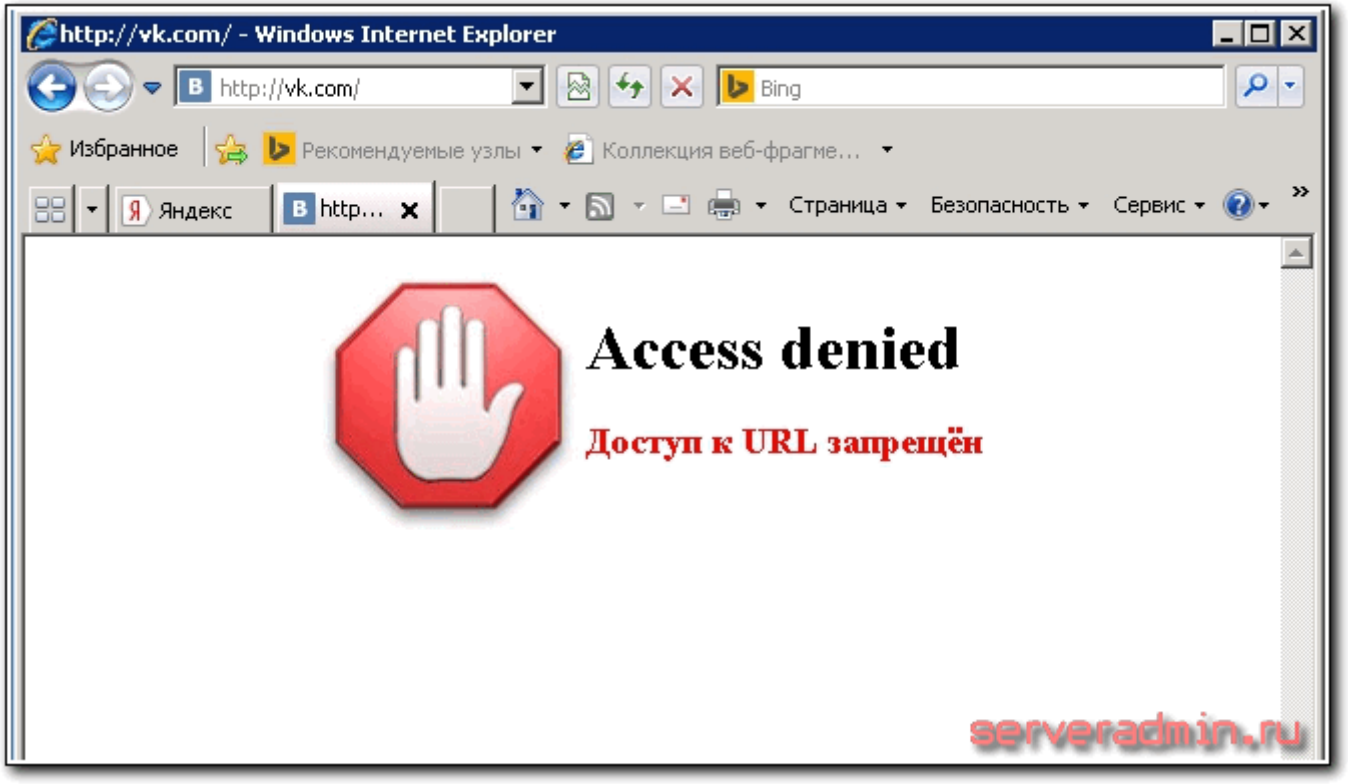
social и добавил в него адрес социальных сетей для теста: vk.com и ok.ru:


SAMS
squid account management system
connected as admin
logoff
Авторизация пользователя
Настройки web-интерфейса
Настройки системных плагино
SAMS
Администрирование SAMS
SQUID
Proxy server
Авторизация
NTLM
Расширения файлов
Перенаправление
Подстановка
Запрет доступа по URL
social
Регулярные выражения
Доступ разрешён
Локальные домены
Запрет доступа.
Список social
Документация
ok.ru
vk.com
Удалить
Change
Добавить
Очистить список
serveradmin.ru

Теперь нужно подключить этот список шаблону по-умолчанию. Идем в шаблон Default, заходим в редактирование и ставим галочку напротив списка social:

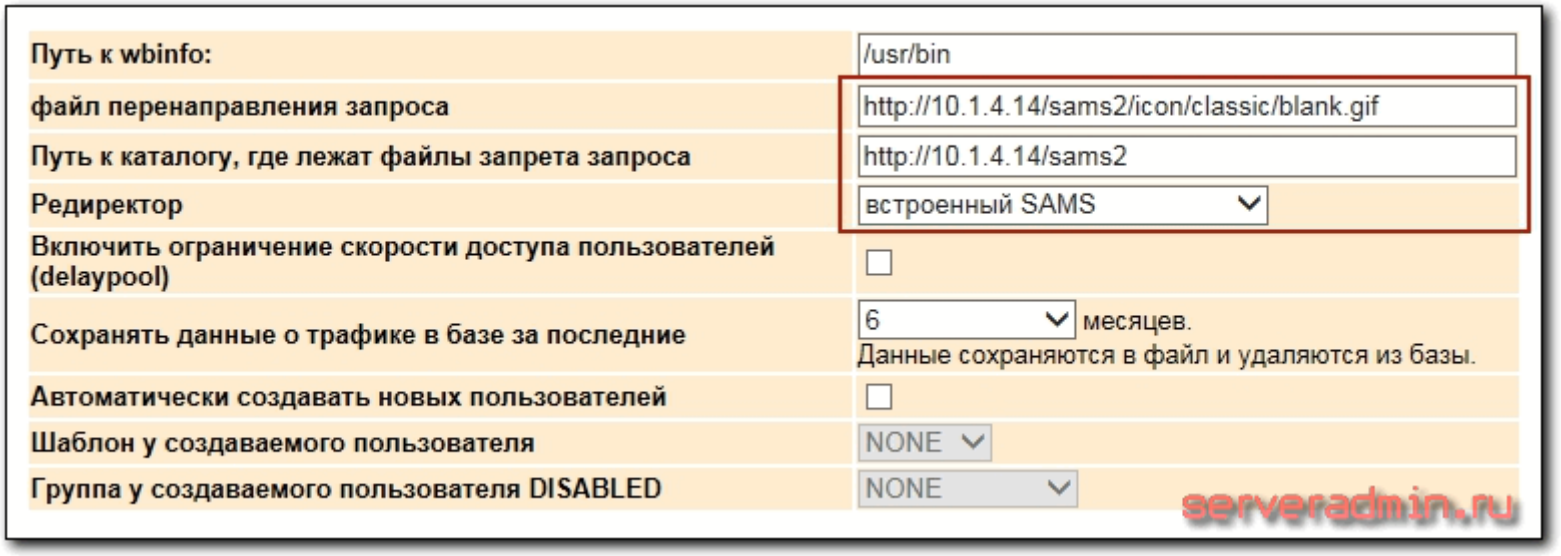

Шаблоны пользователей.
Редактирование шаблона Default
Документация
Списки SAMS:
Доступ запрещён ко всем URL
Запрет доступа
social
Объём трафика пользователя шаблона по умолчанию (Mb): 0 0 - unlimited traffic
Вторичный шаблон
NONE
Способ авторизации пользователей:
ntlm
Период лимита трафика:
Месяц
период: 1 дней
Дата следующего обнуления счётчика трафика:
2015 : 12 : 10
Delay pool
Сохранить изменения
Временные диапазоны:
Full day (00:00:00 - 23:59:59) Удалить
Добавить временной диапазон:
Add
serveradmin.ru

Сохраняем изменения шаблона и перезапускаем конфигурацию сквида. Идем к пользователям и проверяем запрет:



При попытке открыть запрещенный сайт, пользователь получит сообщение о запрете. Реализован этот функционал с помощью встроенного в самс редиректора. Никакие другие редиректоры в sams2 не работают. Но как по мне, так и этого достаточно. Что делать если у вас по какой-то причине не работает запрет доступа, как это было у меня?

В первую очередь надо проверить настройки прокси сервера в самс, там где мы указывали ip адрес сервера. Должен быть выбран редиректор **встроенный в SAMS**. Путь к каталогу, где лежат файлы запрета запроса у меня указан **http://10.1.4.14/sams2**:



Я не знаю, почему именно такой путь должен быть, я указал наугад, так как по-умолчанию там стоял вообще не существующий адрес. И у меня заработало. Некоторое время я проковырялся с этим параметром, потому что в настройках httpd разрешил доступ к алиасу /sams2 только с машины администратора. А при запрете адреса пользователя редиректит на этот же алиас, и если он не имеет к нему доступа, то просто получает ошибку соединения в браузере и не понятно, то ли сработал запрет, то ли сайт недоступен, то ли с интернетом какие-то проблемы. В общем, было неудобно.

Дальше у меня были проблемы с тем, что сам редиректор не запускался. Я сначала скомпилировал исходники без редактирования под 64 бита, и демон не стартовал. Проверить, запущен ли он можно просто по списку процессов. Если все в порядке, то должен быть запущен **sams2daemon** и несколько **sams2redir**. Проверить можно просто:

```
# ps ax | grep sams
22721 ? S 0:01 /usr/local/bin/sams2daemon -l syslog
28498 ? S 0:00 (sams2redir)
28667 ? S 0:00 (sams2redir)
```

```
28860 pts/1 R+ 0:00 grep --color=auto sams
```

Если у вас по какой-то причине сам редиректор не запускаются, запустить его можно вручную:

```
# /usr/local/bin/sams2redir
```

После запуска у вас будет доступен терминал для ввода. Тут же можно проверить, как отрабатываются запреты. Вводите адрес сайта, пользователя, запрос GET и смотрите результат. Вот как выглядит реакция на нормальный сайт, доступ к которому разрешен:

```
http://ya.ru 10.1.4.189 control - GET
http://ya.ru 10.1.4.189 control - GET
```

То есть вы вводите первую строку и редиректор тут же выводит точно такую же сам. А вот какая реакция должна быть на сайт под запретом:

```
http://vk.com 10.1.4.189 control - GET
http://10.1.4.14/sams2/blocked.php?action=urldenied&id=control 10.1.4.189 control -
```

Идет редирект на страничку **blocked.php**. Для разбора ситуации можно пойти в логи апача и посмотреть, что там есть на эту тему. Я так заметил, что у пользователей нет доступа к этому адресу, так как он был закрыт настройкой веб сервера. Отмечу еще для справки, что список заблокированных сайтов sams2 хранит в своей базе в таблице url. Возможно вам пригодится эта информация во время отладки.

Вот все, что касается настройки sams2 под CentOS 7. Надеюсь вам будет полезна эта информация. Бесплатных продуктов, аналогичных самсу я лично не знаю, поэтому ничего лучше не нашел, как использовать в очередной раз его, хоть и с такими большими трудностями пришлось столкнуться во время настройки. Но на выходе получился вполне рабочий вариант.

Заключение

Пришло время подвести итог того, что мы сделали. Проведена большая работа по настройке прокси сервера на базе CentOS 7. Были выполнены следующие шаги:

1. Сервер был введен в домен Windows для настройки авторизации доменных пользователей на прокси сервере.
2. Настроен прокси сервер squid для работы с доменными учетными записями.
3. Собран из исходников многофункциональный web интерфейс для управления squid - sams2 самой последней на текущий момент версии.

Первые два этапа сами по себе позволяют полноценно пользоваться прокси сервером, но не дают удобства и гибкости настройки. Иногда это и не нужно и можно не заморачиваться с установкой и настройкой sams. Как ни крути, но установка достаточно хлопотная и нет гарантии, что через некоторое время после смены версий каких-нибудь пакетов или исходников, не появятся новые нюансы, которые не будут отражены в этой статье. С ними придется разбираться заново.

Уровень данной статьи получился чуть выше, чем может рассчитывать новичок в линуксе, но тем не менее я постарался расписать все максимально подробно. Все этапы проверены на чистой системе, чтобы убедиться в достоверности данных и отсутствии ошибок. То есть сначала была исследована тема, настроена конфигурация на тестовой машине. После того, как я убедился, что все работает так, как мне нужно, я на чистой системе еще раз с нуля провел всю конфигурацию по своей шпаргалке и зафиксировал эту чистую настройку в статье.

- Умение подбирать конфигурацию под необходимые задачи, управлять процессами и обеспечивать безопасность системы.
- Владение основными рабочими инструментами системного администратора.
- Понимание особенностей развертывания, настройки и обслуживания сетей, построенных на базе Linux.
- Способность быстро решать возникающие проблемы и обеспечивать стабильную и бесперебойную работу системы.

Проверьте себя на вступительном тесте и смотрите подробнее программу по .