

Лабораторная работа № 16

Тема: Сетевые сервисы на Linux. Email-сервер на linux.

Цель работы: Познакомиться с процессом установки, настройки и администрирования почтового сервера на операционной системе Linux.

Необходимое оборудование и программное обеспечение:

Виртуальная машина под управлением CentOS 7.

Пример настройки серверов.

Меняем имя сервера:

hostnamectl set-hostname mail.nodrop.in

```
[root@localhost ~]# hostnamectl set-hostname mail.nodrop.in
[root@localhost ~]# bash
[root@mail ~]#
```

Проверяем порты:

```
[root@mail ~]# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
1224/master
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
977/sshd
tcp6       0      0 :::25                   :::*                    LISTEN
1224/master
tcp6       0      0 :::22                   :::*                    LISTEN
977/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*
798/dhclient
[root@mail ~]#
```

Порт 25 прослушивается, нам это не нужно, т.к. почта будет в контейнере. Останавливаем postfix:

```
[root@mail ~]# systemctl stop postfix
[root@mail ~]# systemctl disable postfix
Removed symlink /etc/systemd/system/multi-user.target.wants/postfix.service.
[root@mail ~]# netstat -tulpn
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
977/sshd
tcp6       0      0 :::22                   :::*                    LISTEN
977/sshd
udp        0      0 0.0.0.0:68              0.0.0.0:*
798/dhclient
[root@mail ~]#
```

Проверяем и корректируем время:

```
[root@mail ~]# timedatectl list-timezones | grep Almaty
Asia/Almaty
[root@mail ~]# date
C6 map 23 11:48:01 +05 2024
[root@mail ~]# timedatectl list-timezones | grep Almaty
Asia/Almaty
[root@mail ~]# timedatectl set-timezone Asia/Almaty
[root@mail ~]# timedatectl
          Local time: C6 2024-03-23 11:48:53 +05
    Universal time: C6 2024-03-23 06:48:53 UTC
           RTC time: C6 2024-03-23 06:48:53
        Time zone: Asia/Almaty (+05, +0500)
         NTP enabled: n/a
```

Установка docker:

Добавим репозиторий docker:

yum-config-manager --add-repo <https://download.docker.com/linux/centos/docker-ce.repo>

```
[root@mail ~]# yum install yum-utils -y
Загружены модули: fastestmirror
Loading mirror speeds from cached hostfile

Выполнено!
[root@mail ~]# yum-config-manager --add-repo https://download.docker.com/linux/centos/docker-ce.repo
Загружены модули: fastestmirror
adding repo from: https://download.docker.com/linux/centos/docker-ce.repo
grabbing file https://download.docker.com/linux/centos/docker-ce.repo to /etc/yum.repos.d/docker-ce.repo
repo saved to /etc/yum.repos.d/docker-ce.repo
[root@mail ~]#
```

Установим docker:

```
[root@mail ~]# yum -y install docker-ce
Загружены модули: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirror.nsk.ru
```

Добавляем пользователя (если docker будет запускаться от root, можно не делать) в группу Docker и проверяем:

```
[root@mail ~]# id root
uid=0(root) gid=0(root) группы=0(root)
[root@mail ~]# sudo usermod -aG docker $(whoami)
[root@mail ~]# id root
uid=0(root) gid=0(root) группы=0(root),995(docker)
[root@mail ~]#
```

Включаем Docker при загрузке операционной системы:

```
[root@mail ~]# systemctl enable docker.service
Created symlink from /etc/systemd/system/multi-user.target.wants/docker.service to /usr/lib/systemd/system/docker.service.
[root@mail ~]#
```

Устанавливаем docker-compose:

curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-compose-\$(uname -s)-\$(uname -m)" -o /usr/local/bin/docker-compose

```
[root@mail ~]# curl -L "https://github.com/docker/compose/releases/download/1.29.2/docker-compose-$(uname -s)-$(uname -m)" -o /usr/local/bin/docker-compose
% Total % Received % Xferd Average Speed Time Time Time Current
0 0 0 0 0 0 0 0 0:00:00 0:00:00 0:00:00 0
100 12.1M 100 12.1M 0 0 3119k 0 0:00:03 0:00:03 0:00:00 5548k
[root@mail ~]#
```

Делаем файл исполняемым:

```
[root@mail ~]# sudo chmod +x /usr/local/bin/docker-compose
[root@mail ~]#
```

Создадим символическую ссылку. Это позволяет любому пользователю системы запускать **docker-compose** из любого места в командной строке, не указывая полный путь к файлу **docker-compose**:

ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose

```
[root@mail ~]# ln -s /usr/local/bin/docker-compose /usr/bin/docker-compose
[root@mail ~]#
```

Убеждаемся, что docker-compose установлен:

```
[root@mail ~]# docker-compose -v
docker-compose version 1.29.2, build 5becea4c
[root@mail ~]#
```

Установка Mailcow

Для начала убедимся, что umask — 0022, а docker-сервис запущен.

Для новых файлов устанавливается маска режима создания, которая отключает права на запись для группы и остальных пользователей.

```
[root@mail ~]# umask -S 0022
u=rwx,g=rx,o=rx
[root@mail ~]#
```

```
[root@mail ~]# systemctl start docker
[root@mail ~]# systemctl status docker
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; enabled; vendor prese
  t: disabled)
   Active: active (running) since C6 2024-03-23 12:35:41 +05; 3min 0s ago
     Docs: https://docs.docker.com
    Main PID: 5056 (dockerd)
      Tasks: 7
     Memory: 31.0M
    CGroup: /system.slice/docker.service
            └─5056 /usr/bin/dockerd -H fd:// --containerd=/run/containerd/cont...

map 23 12:35:37 mail.nodrop.in systemd[1]: Starting Docker Application Co....
map 23 12:35:37 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:37.2..."
map 23 12:35:37 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:37.4..."
map 23 12:35:40 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:40.6..."
map 23 12:35:41 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:41.0..."
map 23 12:35:41 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:41.1...0
map 23 12:35:41 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:41.1..."
map 23 12:35:41 mail.nodrop.in dockerd[5056]: time="2024-03-23T12:35:41.3..."
map 23 12:35:41 mail.nodrop.in systemd[1]: Started Docker Application Con....
Hint: Some lines were ellipsized, use -l to show in full.
[root@mail ~]#
```

Клонируем Mailcow из Git:

git clone https://github.com/mailcow/mailcow-dockerized

```
[root@mail ~]# git clone https://github.com/mailcow/mailcow-dockerized
Cloning into 'mailcow-dockerized'...
remote: Enumerating objects: 53159, done.
remote: Counting objects: 100% (3154/3154), done.
remote: Compressing objects: 100% (1310/1310), done.
remote: Total 53159 (delta 2123), reused 2797 (delta 1832), pack-reused 50005
Receiving objects: 100% (53159/53159), 46.14 MiB | 3.49 MiB/s, done.
Resolving deltas: 13% (4717/35117)
```

Переходим в соответствующую папку и запускаем генератор конфига и е отвечаем на вопросы:

```
[root@mail mailcow-dockerized]# ./generate_config.sh
Found Docker Compose Plugin (native).
Setting the DOCKER_COMPOSE_VERSION Variable to native
Notice: You'll have to update this Compose Version via your Package Manager manu
ally!
Press enter to confirm the detected value '[value]' where applicable or enter a
custom value.
Mail server hostname (FQDN) - this is not your mail domain, but your mail server
s hostname mail.nodrop.in
Timezone [Asia/Almaty] y
Installed memory is <= 2.5 GiB. It is recommended to disable ClamAV to prevent o
ut-of-memory situations.
ClamAV can be re-enabled by setting SKIP_CLAMD=n in mailcow.conf.
Do you want to disable ClamAV now? [Y/n] y
Disabling Solr on low-memory system.
Which branch of mailcow do you want to use?

Available Branches:
- master branch (stable updates) | default, recommended [1]
- nightly branch (unstable updates, testing) | not-production ready [2]
Choose the Branch with it's number [1/2] 1
Fetching origin
Already on 'master'
```

В результате должен появиться файл конфигурации:

```
[root@mail mailcow-dockerized]# ls -l
итого 176
-rw-r--r--. 1 root root 3223 map 23 12:42 CODE_OF_CONDUCT.md
-rw-r--r--. 1 root root 5260 map 23 12:42 CONTRIBUTING.md
-rwxr-xr-x. 1 root root 174 map 23 12:42 create_cold_standby.sh
drwxr-xr-x. 7 root root 75 map 23 12:42 data
-rw-r--r--. 1 root root 24363 map 23 12:42 docker-compose.yml
-rwxr-xr-x. 1 root root 22237 map 23 12:42 generate_config.sh
drwxr-xr-x. 3 root root 4096 map 23 12:42 helper-scripts
-rw-r--r--. 1 root root 35141 map 23 12:42 LICENSE
-rw-----. 1 root root 9772 map 23 12:47 mailcow.conf
-rw-r--r--. 1 root root 2157 map 23 12:42 README.md
-rw-r--r--. 1 root root 1737 map 23 12:42 SECURITY.md
-rwxr-xr-x. 1 root root 50459 map 23 12:42 update.sh
[root@mail mailcow-dockerized]#
```

Далее нужно в файле mailcow.conf указать доменные имена, на которые следует выписать сертификат. За это отвечает параметр ADDITIONAL_SAN файла mailcow.conf.

ADDITIONAL_SAN=mail.nodrop.in,smtp.nodrop.in,imap.nodrop.in,www.nodrop.in

```
GNU nano 2.3.1          файл: mailcow.conf          Изменён
#ADDITIONAL_SAN=imap.*,smtp.*
# This will expand the certificate to "imap.example.com", "smtp.example.com", "$
# plus every domain you add in the future.
#
# You can also just add static names...
#ADDITIONAL_SAN=srv1.example.net
# ...or combine wildcard and static names:
#ADDITIONAL_SAN=imap.*,srv1.example.com
#
ADDITIONAL_SAN=mail.nodrop.in,smtp.nodrop.in,imap.nodrop.in,www.nodrop.in
```

После чего скачиваем все контейнеры:

```
[root@mail mailcow-dockerized]# docker-compose pull
Pulling unbound-mailcow    ...
Pulling clamd-mailcow     ... waiting
Pulling sogo-mailcow      ...
Pulling memcached-mailcow ...
Pulling netfilter-mailcow ... done
Pulling redis-mailcow     ...
Pulling php-fpm-mailcow   ...
```

Если docker-compose pull завершается ошибкой вида:

```
[root@mail mailcow-dockerized]# docker-compose pull
ERROR: The Compose file './docker-compose.yml' is invalid because:
services.nginx-mailcow.ports contains an invalid type, it should be a number, or
an object
services.nginx-mailcow.ports contains an invalid type, it should be a number, or
an object
[root@mail mailcow-dockerized]# docker-compose pull
```

То нужно исправить docker-compose.yml, в секции nginx-mailcow нужно исправить раздел портов: ports:

- 80:80
- 443:443

Эта запись определяет проброс порта для контейнера. В данном случае, порт **443** в контейнере будет доступен на порту **443** хоста, то же для порта 80

Переходим в папку data/web (полный путь в нашем случае /root/mailcow-dockerized/data/web), скачиваем и распаковываем RoundCube:

wget -O - https://github.com/roundcube/roundcubemail/releases/download/1.4.9/roundcubemail-1.4.9-complete.tar.gz | tar xfvz -

```
[root@mail web]# wget -O - https://github.com/roundcube/roundcubemail/releases/download/1.4.9/roundcubemail-1.4.9-complete.tar.gz | tar xfvz -
```

Переименовываем полученную папку roundcubemail-1.4.9/ в папку rc и меняем права для папки с roundcube, в нашем случае — на CentOS:

```
[root@mail web]# mv roundcubemail-1.4.9/ rc
[root@mail web]# chown -R root: rc
[root@mail web]#
```

Создаём файл конфига

/root/mailcow-dockerized/data/web/rc/config/config.inc.php

```
GNU nano 2.3.1 Файл: ...dockerized/data/web/rc/config/config.inc.php Изменён
<?php
error_reporting(0);
if (!file_exists('/tmp/mime.types')) {
file_put_contents("/tmp/mime.types",
fopen("http://svn.apache.org/repos/asf/httpd/httpd/trunk/docs/conf/mime.types",
'r'));
}
$config = array();
$config['db_dsnw'] = 'mysql://' . getenv('DBUSER') . ':' . getenv('DBPASS') .
'@mysql/' . getenv('DBNAME');
$config['default_host'] = 'tls://dovecot';
$config['default_port'] = '143';
$config['smtp_server'] = 'tls://postfix';
$config['smtp_port'] = 587;
$config['smtp_user'] = '%u';
$config['smtp_pass'] = '%p';
$config['support_url'] = '';
$config['product_name'] = 'Roundcube Webmail';
$config['des_key'] = 'yourrandomstring_changeme';
$config['log_dir'] = '/dev/null';
```

Запускаем почтовый сервер:

```
[root@mail ~]# cd /root/mailcow-dockerized/
[root@mail mailcow-dockerized]# docker-compose up -d
```



```
[root@mail mailcow-dockerized]# docker-compose up -d
Creating network "mailcowdockerized_mailcow-network" with driver "bridge"
Creating volume "mailcowdockerized_vmail-vol-1" with default driver
Creating volume "mailcowdockerized_vmail-index-vol-1" with default driver
Creating volume "mailcowdockerized_mysql-vol-1" with default driver
Creating volume "mailcowdockerized_mysql-socket-vol-1" with default driver
Creating volume "mailcowdockerized_redis-vol-1" with default driver
Creating volume "mailcowdockerized_rspamd-vol-1" with default driver
Creating volume "mailcowdockerized_solr-vol-1" with default driver
Creating volume "mailcowdockerized_postfix-vol-1" with default driver
Creating volume "mailcowdockerized_crypt-vol-1" with default driver
Creating volume "mailcowdockerized_sogo-web-vol-1" with default driver
Creating volume "mailcowdockerized_sogo-userdata-backup-vol-1" with default driver
Creating volume "mailcowdockerized_clamd-db-vol-1" with default driver
Creating mailcowdockerized_netfilter-mailcow_1 ... done
Creating mailcowdockerized_unbound-mailcow_1 ... done
Creating mailcowdockerized_olefy-mailcow_1 ... done
Creating mailcowdockerized_sogo-mailcow_1 ... done
Creating mailcowdockerized_dockerapi-mailcow_1 ... done
Creating mailcowdockerized_memcached-mailcow_1 ... done
Creating mailcowdockerized_redis-mailcow_1 ... done
Creating mailcowdockerized_solr-mailcow_1 ... done
Creating mailcowdockerized_mysql-mailcow_1 ... done
Creating mailcowdockerized_php-fpm-mailcow_1 ... done
Creating mailcowdockerized_dovecot-mailcow_1 ... done
Creating mailcowdockerized_nginx-mailcow_1 ... done
Creating mailcowdockerized_rspamd-mailcow_1 ... done
Creating mailcowdockerized_ofelia-mailcow_1 ... done
Creating mailcowdockerized_acme-mailcow_1 ... done
Creating mailcowdockerized_clamd-mailcow_1 ... done
Creating mailcowdockerized_postfix-mailcow_1 ... done
Creating mailcowdockerized_watchdog-mailcow_1 ... done
Creating mailcowdockerized_ipv6nat-mailcow_1 ... done
[root@mail mailcow-dockerized]#
```

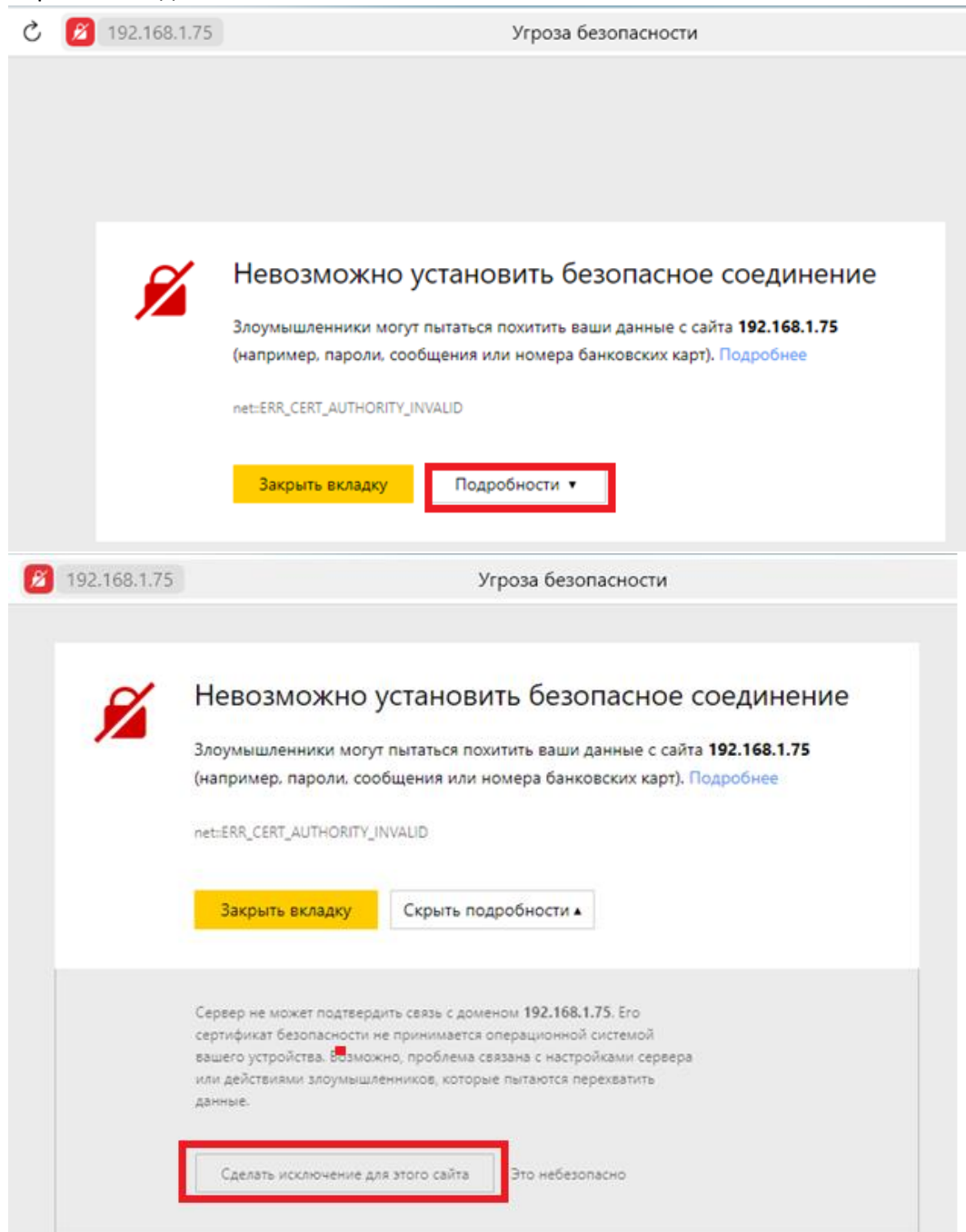
Посмотрим ip-адрес сервера:

```
[root@mail mailcow-dockerized]# ip a s enp0s3
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP
group default qlen 1000
    link/ether 08:00:27:a2:3d:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.75/24 brd 192.168.1.255 scope global noprefixroute dynamic e
p0s3
        valid_lft 77264sec preferred_lft 77264sec
    inet6 fe80::1639:b6b1:2b15:bbc2/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@mail mailcow-dockerized]#
```


На хосте, в браузере, в адресной строке пишем:

https://192.168.1.75

Отрывается админка:



Войти




mailcow UI

Имя пользователя

Пароль

Войти

FIDO2/WebAuthn Login




Приложения

Webmail

Заходим в админку используя логин **admin** и пароль **moohoo**:

Войти




mailcow UI

admin

.....

Пожалуйста, подождите...


FIDO2/WebAuthn Login



192.168.1.75 mailcow UI

Система и контейнеры Журналы

mailcow UI




Hostname	mail.nodrop.in
Architecture	-
IPs	Проверка IP отключена. Вы можете включить его в разделе Система > Конфигурация > Параметры > Настроить.
Version	2024-02 The System is on the latest version
System Time	-
Timezone	y
Время работы	-
Использование дискового пространства	/ ()

Настраиваем почту:

mailcow UI

Система и контейнеры Журналы

Конфигурация
кампейн
Очередь на отправку
Перезапустить SOGo



Hostname	mail.nodrop.in
Architecture	x86_64
IPs	Проверка IP отключена. Вы можете включить его в разделе Система > Конфигурация > Параметры > Настроить.
Version	2024-02 The System is on the latest version
System Time	23.03.2024 09:34:47
Timezone	y

Создаем домен:

Домены Почтовые ящики Ресурсы Псевдонимы Задания синхронизации Фильтры Перезапись адресов Правила TLS

Домены Обновить

Выбрать все Действия + Добавить домен

Search: Show 25 entries

Домен	Псевдонимы	Почтовые ящики	Квота	Статистика	Квота по умолчанию	Макс. квота почт. ящика	RL	Активный	Действия
No data available in table									

Showing 0 to 0 of 0 entries

Выбрать все Действия + Добавить домен

Добавить домен

Домен

catec2024.kz

Описание

Template

Default

Теги

Максимум
псевдонимов

400

Максимум почтовых
ящиков

10

Квота почтового
аккаунта по умолчанию

3072

Максимальная квота

Selector

dkim

Длина DKIM ключа
(bits)

2048

Параметры резервного
MX

☐ Ретрансляция этого домена

☐ Ретрансляция всех получателей

↳ Если вы решите не ретранслировать всех получателей, вам нужно будет добавить ("слепой") почт следует ретранслировать.

☐ Ретрансляция только не существующих почтовых ящиков. Почта к существующим почт локально.

Инфо

Вы можете настроить собственный транспорт для домена. Если такой настрой основе MX записей.

Только добавить домен

Добавить домен и перезапустить SOGO

После добавления нового домена вам необходимо перезагрузить контейнер службы SOGO!

И создадим аккаунт:

Домены

Почтовые ящики

Ресурсы

Псевдонимы

Задания синхронизации

Фильтры

Перезапись адресов

Правила TLS

Домены

Почтовые ящики

Templates

Выбрать все

Действия

Добавить домен

Search:

Show 25 entries

Домен	Псевдонимы	Почтовые ящики	Квота	Статистика	Квота по умолчанию	Активный	Действия
<input type="checkbox"/> catec2024.kz	/ 400	0 / 10	0 B / 10.0 GiB	0 / 0 B	3.0 GiB	✓	<div>Изменить</div> <div>Удалить</div> <div>DNS</div>

Showing 1 to 1 of 1 entries

PREVIOUS 1 NEXT

Выбрать все

Действия

Добавить домен

Домены

Почтовые ящики

Ресурсы

Псевдонимы

Задания синхронизации

Фильтры

Перезапись адресов

Правила TLS

Почтовые ящики

Обновить

Выбрать все

Действия

Почтовый аккаунт

TLS

Разрешенные протоколы

Уведомления о спаме

Добавить почтовый аккаунт

Search:

Show 25 entries

Имя пользователя

Квота

Последний вход

Последняя смена пароля

Использовано

Писем

Активный

Действия

Выбрать все

Действия

Почтовый аккаунт

TLS

Разрешенные протоколы

Уведомления о спаме

Добавить почтовый аккаунт

 Version: 2024-02

Добавить почтовый аккаунт

Имя пользователя
(часть адреса
электронной почты
слева)

teacher

Домен

catec2024.kz

Полное имя

Viktor Viktorovich

Пароль
(сгенерировать)

.....

Проверить на утечки в haveibeenpwned.com

Минимальная длина пароля 6 символов

Подтверждение пароля
(повтор)

.....

Template

Template

Теги

Квота (MiB)

3072

так, 10240 MiB

Категория уведомлений о спаме

Отклонённая почта

Нежелательная почта

Все категории

Категория "Отклонённая почта" включает в себя почту, которая была <code>отклонена</code>, тогда как "Нежелательная почта" содержит письма, которые были помещены в папку <code>junk</code>. Для того, чтобы получать уведомления обо всех категориях спама, выберите опцию "Все категории".

Политика шифрования

Принудительный TLS (входящие)

Принудительный TLS (исходящие)

Разрешённые протоколы

Ничего не выбрано

ACL

Временные псевдонимы, Политика шифры

Лимиты отправки

Отключен

сообщений / секунду

Этот лимит применяется к SASL логину пользователя и соответствует любому адресу отправителя, используемому зарегистрированным пользователем. Лимит скорости почтового аккаунта перекрывает лимит скорости для всего домена.

Активный

Требуется смена пароля при следующем входе в систему

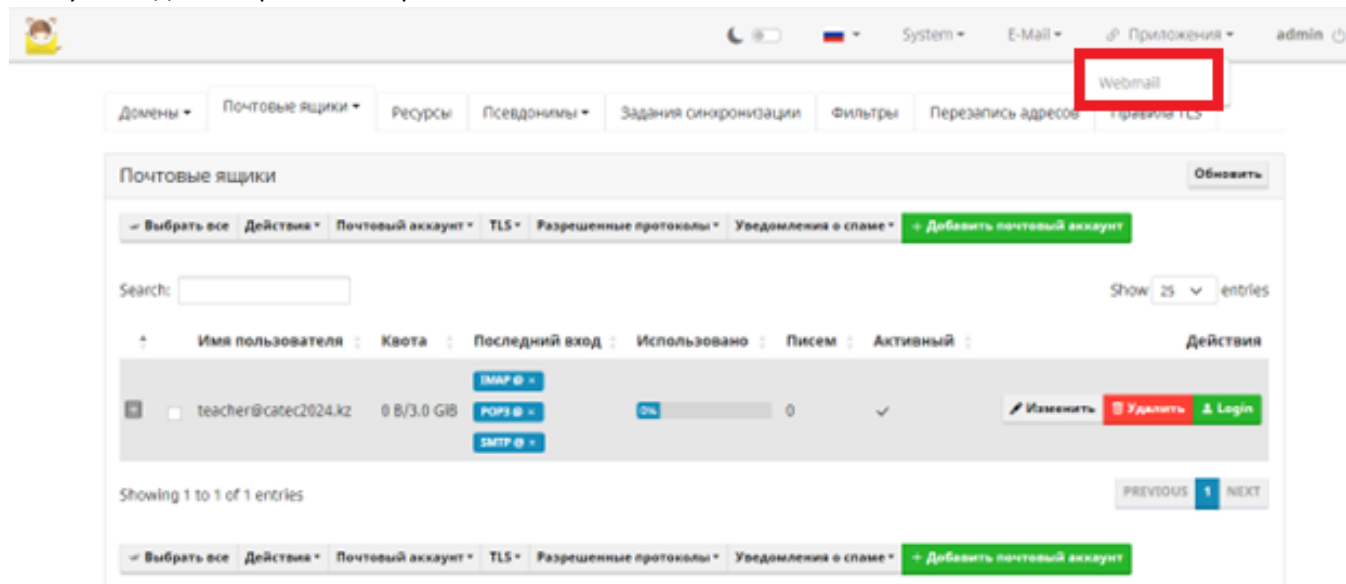
Пользователь должен будет войти в mailcow UI и сменить свой пароль. mailcow OAuth2, SOGo, EAS, IMAP/POP3 и SMTP будут не доступны до смены пароля.

Grant direct login access to SOGo

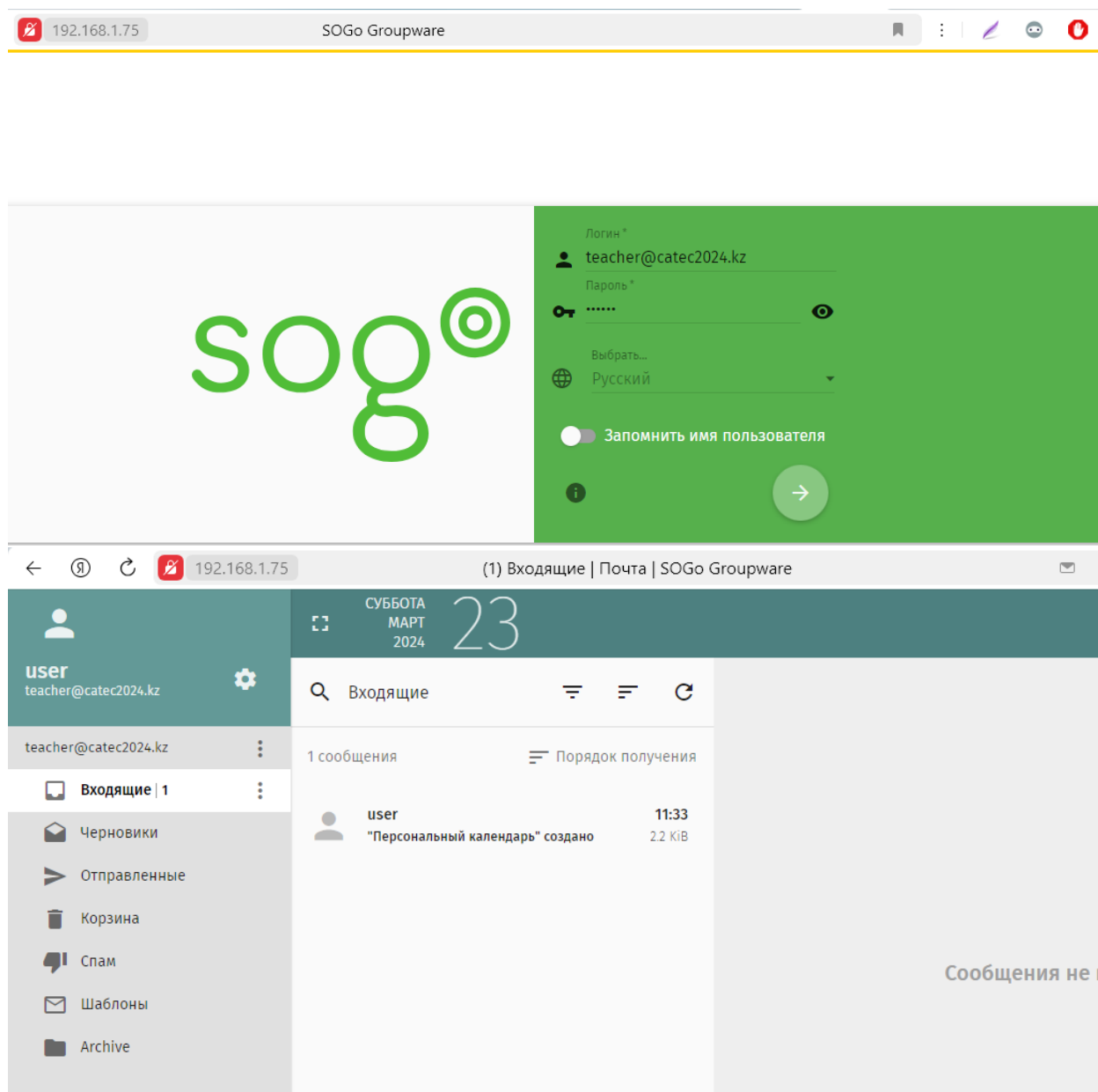
Единый вход из интерфейса почты продолжает работать. Эта настройка не влияет на доступ ко всем другим службам, а также не удаляет или изменяет существующий профиль пользователя SOGo.

Добавить

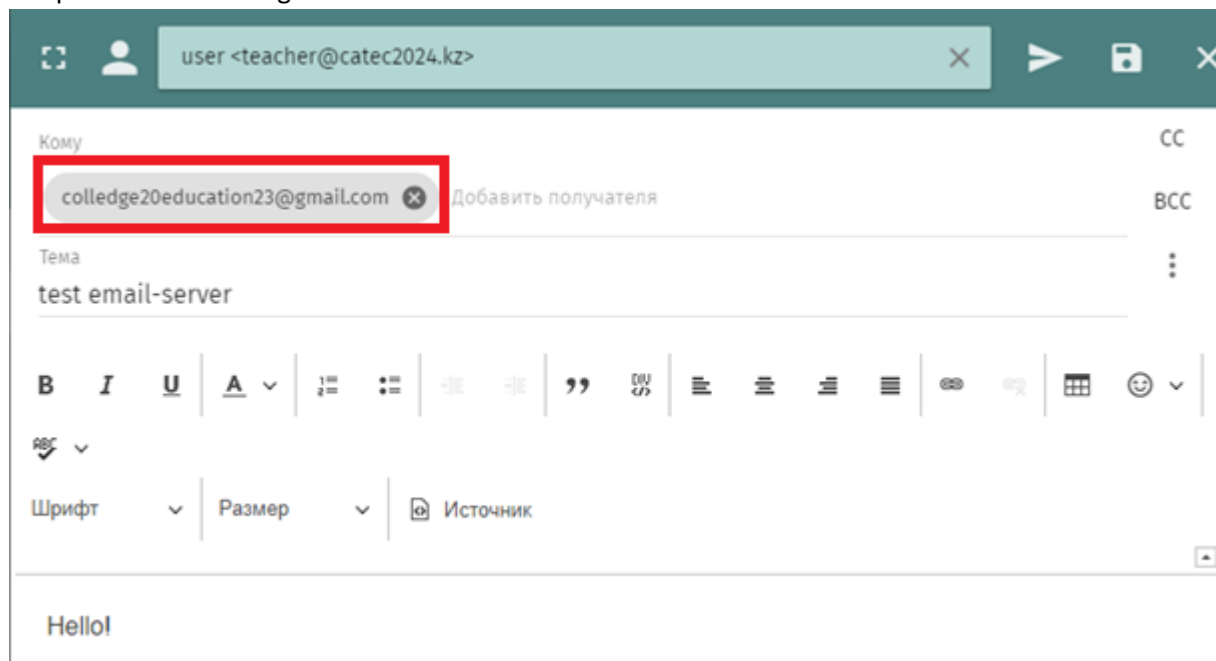
Аккаунт создан. Открываем встроенный почтовый клиент:



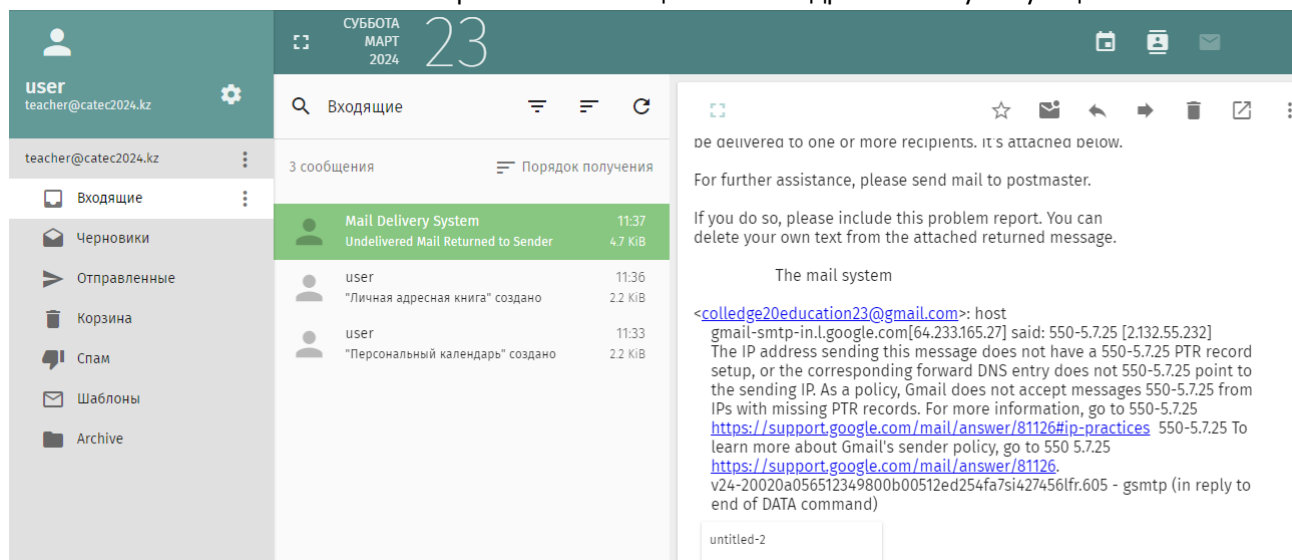
Логинимся:



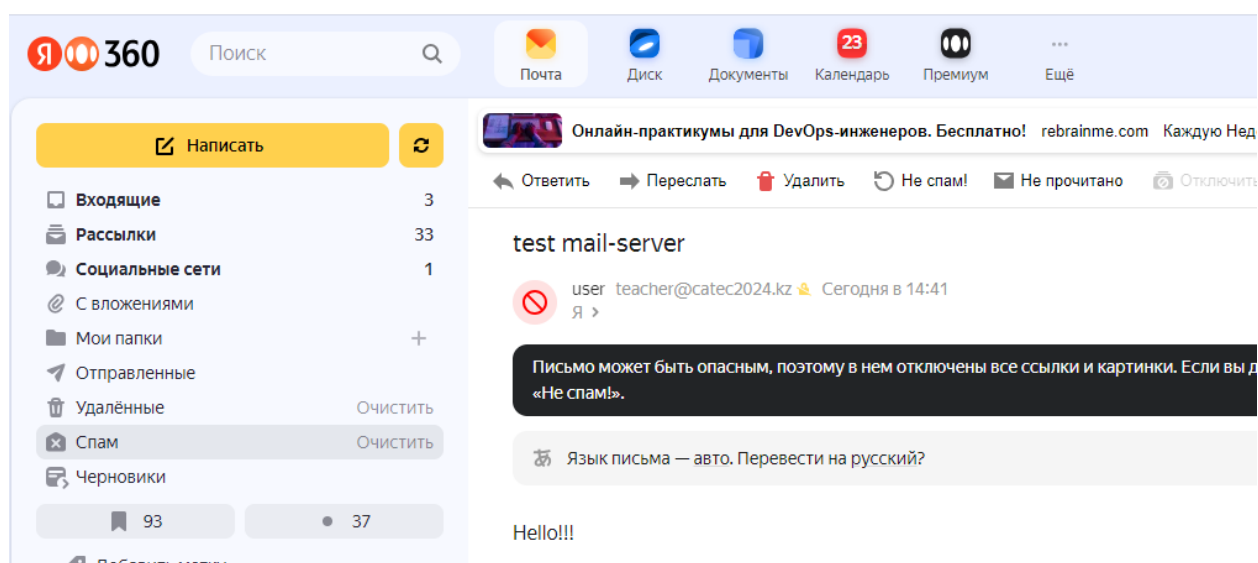
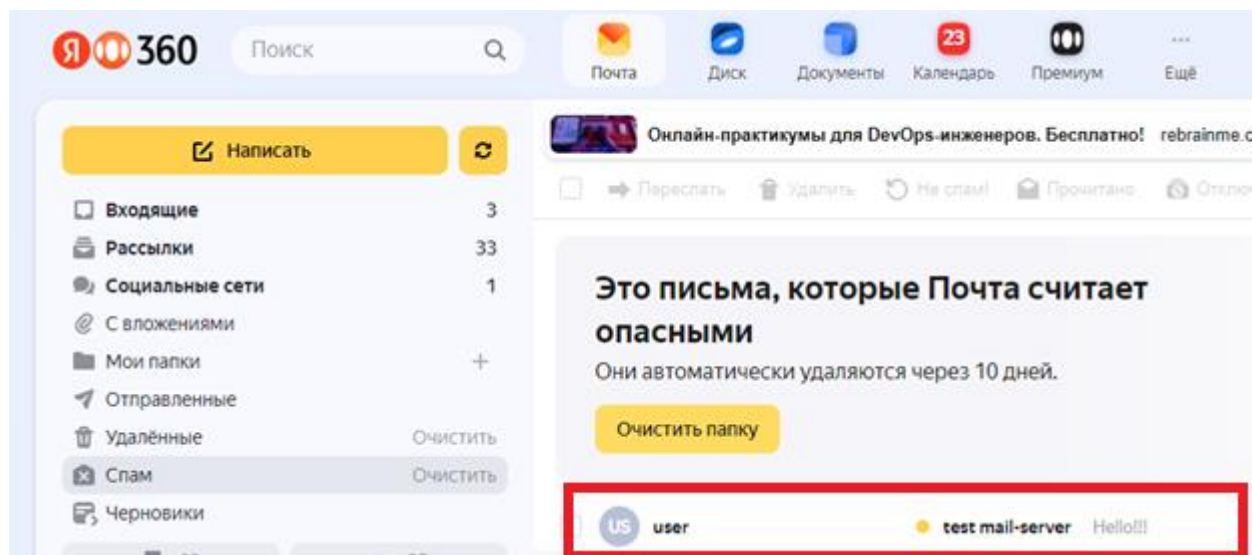
Отправим письмо на gmail.com



Письмо не доставлено. Получаем сообщение, что IP-адрес, отправляющий это сообщение, не имеет записи PTR. Политика Gmail не позволяет принимать сообщения от IP-адресов с отсутствующими записями PTR.



Пробуем отправить на яндекс почту. Письмо дошло, но помещено в папку «Спам»



Настройка почтового сервера завершена!

Задание:

1. В VM на базе CentOS 7 установите Docker и Docker Compose. Установите, настройте и запустите почтовый сервер Mailcow.
2. В браузере откройте админ. панель.
3. *Создайте домен вида: catec<номер варианта>.kz
4. *Создайте аккаунт вида: <ваше имя на латинице>@<домен>
5. *Проверьте работоспособность почтового сервера.