VK WorkSpace

Кластерная установка VK WorkMail

Установка VK WorkMail 1.20 на кластер из 8 машин

Оглавление

Описание документа 4

Схема тестового кластера 4

Технические требования 5

Предварительные условия 5

Обязательные предварительные действия 6

- Создание DNS-записей 6
- Подключение дисков 10
- Список портов для установки 10

Этапы установки 12

Действия в командной строке на сервере 12

- 1. Создание пользователя deployer 12
- 2. Распаковка дистрибутива 14
- 3. Запуск установщика как сервиса 15

Действия в веб-интерфейсе установщика 16

- 1. Выбор варианта установки 16
- 2. Выбор продуктов и опций 17
- 3. Добавление лицензионного ключа 20
- 4. Добавление гипервизора 21
- 5. Сетевые настройки 23
- 6. Доменные имена 25
  - 6.1 Добавление SSL-сертификатов 26
- 7. Установка гипервизоров 28
- 8. Распределение контейнеров по гипервизорам 31
  - Порядок действий при распределении контейнеров 32
- 9. Хранилища 36
  - 9.1 Раздел mescalito 38
  - 9.2 fstab 41
- 10. Шардирование и репликация БД 42

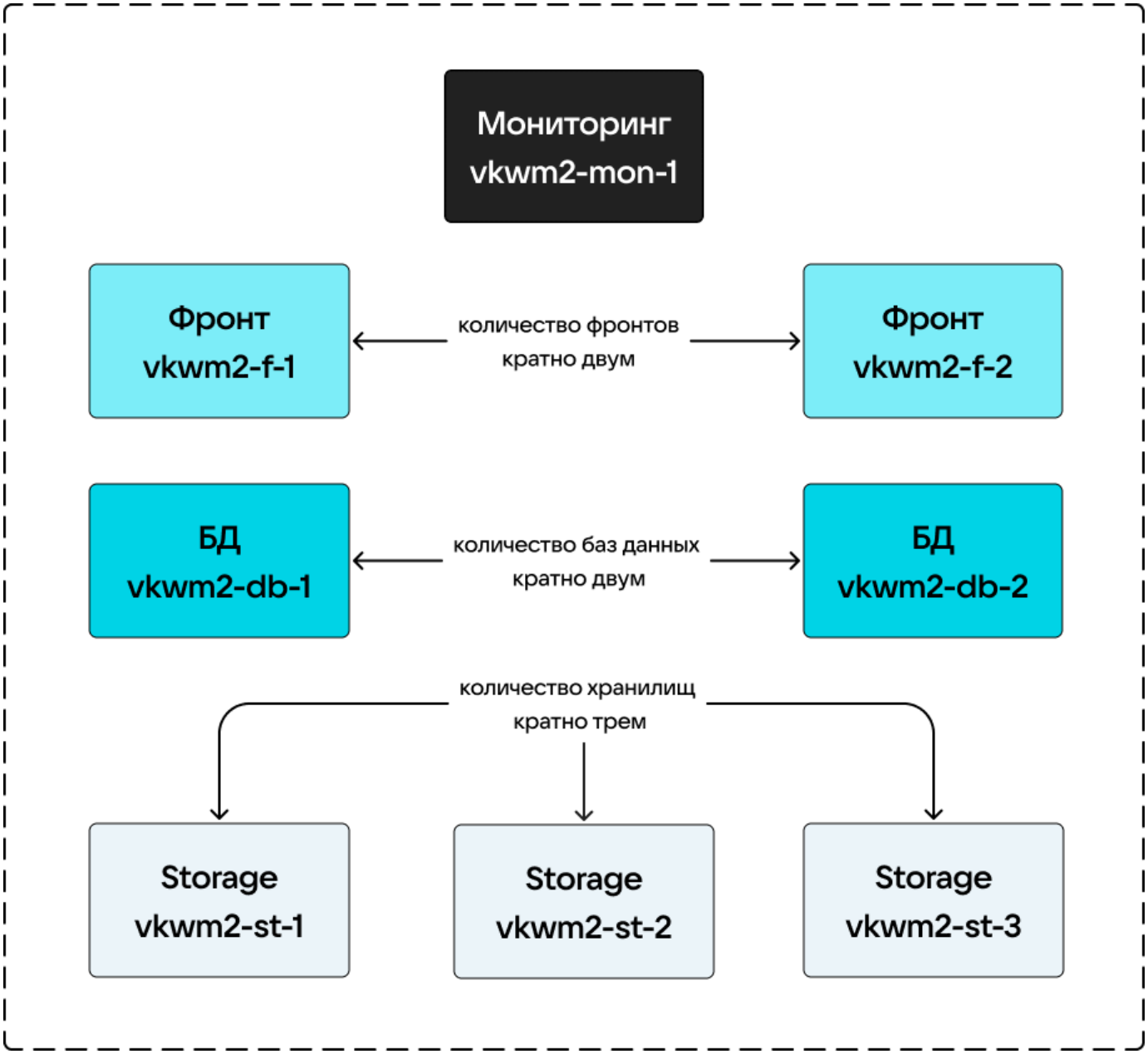
11. Настройки компонентов 43
Авторизация 43
Адресная книга 46
Настройки почты 47
Ограничение доступа к доменам 48
Панель администрирования 50
Политика изменения паролей пользователей 51
Почтовый транспорт 52
Рассыльщики 55
Система расширенных транспортных правил 55
Система учета действий пользователей 56
Мониторинг 57
Настройки HTTP(S)-прокси 59
12. Интеграции 59
Сборщик почты 60
Интеграция с другими инсталляциями VK WorkMail 60
Настройки дублирования действий пользователей во внешнее хранилище 62
Настройки системы BI-аналитики 63
13. Переменные окружения 64
14. Запуск установки всех машин 66
15. Завершение установки, инициализация домена и вход в панель администратора 67
16. Добавление дополнительных доменов 70
Настройка интеграции с Active Directory 71
Дополнительная документация 72
Приложение 1. При входе в панель администратора появляется ошибка «Неверный пароль» 72
Приложение 2. Обновление лицензионного ключа 73
Приложение 3. Логи и полезные команды 74

Описание документа

В документе содержится информация о процедуре кластерной установки **VK WorkMail**. Минимальной отказоустойчивой конфигурацией для установки почтовой системы считается кластер на 8 машин.

Схема тестового кластера

Вне зависимости от размера кластера нужно соблюдать следующее соотношение виртуальных машин:



Минимальная отказоусточивая конфигурация на **8 машин**, которая будет описана в документе, выглядит таким образом:

- **1 ВМ** отводится под мониторинг;

- **2 ВМ** — под фронты;
- **2 ВМ** — под базы данных;
- **3 ВМ** — под хранилища.

> **Примечание**
>
> Дистрибутив VK WorkMail и файл `onpremise-deployer_linux` должны находиться на гипервизоре, отведенном под **мониторинг**.

Технические требования

Рекомендованные операционные системы для установки VK WorkMail:

- **Astra Linux SE Орел** — версии 1.7.3 и выше;
- **РЕД ОС** — версии от 7.3 и выше;
- **CentOS** 7.9.

Минимальные технические параметры для 8 машин в кластере:

- **Установщик + мониторинг**: 8 GB CPU, 16 GB RAM, 200 GB SSD;
- **Фронт №1**: 16 GB CPU, 32 GB RAM, 150 GB SSD;
- **Фронт № 2**: 16 GB CPU, 32 GB RAM, 150 GB SSD;
- **База данных №1**: 8 GB CPU, 12 GB RAM, 150 GB SSD;
- **База данных №2**: 8 GB CPU, 12 GB RAM, 150 GB SSD;
- **Хранилище №1**: 8 GB CPU, 8 GB RAM, 250 GB SSD;
- **Хранилище №2**: 8 GB CPU, 8 GB RAM, 250 GB SSD;
- **Хранилище №3**: 8 GB CPU, 8 GB RAM, 250 GB SSD.

> **Важно**
>
> По вопросам создания сайзинг-модели специально для вашей компании обратитесь к представителям VK.

Предварительные условия

Представители VK предоставили вам следующие данные:

- ссылку на скачивание дистрибутива **VK WorkMail 1.20**;
- пароль от архива с дистрибутивом;
- лицензионный ключ;

- комплект документации.

Также вам потребуется:

- набор **DNS-записей**: A, CNAME, MX, SPF, TXT, NS;
- поддержка процессорами набора инструкций **sse2** и **avx** для каждого гипервизора;
- **DKIM-подпись** с селекторами для каждого домена (или несколько DKIM с разными селекторами для одного домена);
- доступ к серверам по **SSH** с правами администратора (вход по ключу или по паролю);
- локальная сеть **1 GbE** или **10 GbE**;
- отключить **swap**;
- сертификаты **SSL** для каждого **CNAME** или **Wildcard-сертификат** для домена;
- **доступ к портам**: 25, 80, 143, 443, 465, 993, 1025;
- **tar**;
- утилита для распаковки zip-архивов, например **7zip** или **unzip**;
- **Active Directory** или другая служба каталогов, работающая по протоколу **LDAP**.

Используемые протоколы почты:

- **CalDav** для синхронизации календаря;
- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента;
- **HTTPS** для доступа к веб-интерфейсу почты с использованием **TLS**;
- **SMTP** — протокол отправки почтовых сообщений (порт 25/465);
- **IMAP** — протокол получения почтовых сообщений (порт 143/993);
- **IP in IP** — протокол туннелирования IP.

Обязательные предварительные действия

Создание DNS-записей

Для работы почты необходима **MX-запись** (рекомендуемый приоритет — 10), которая обязательно ведет на `mxs.<домен для почты>`.

Помимо этого вам нужно создать два основных домена: **для почты** и **для хранилищ**, а также набор **A-** или **CNAME-записей**.

Для примера в документе будут использоваться следующие **DNS-записи**:

- **Домен для сервисов почты** — `vbastra0mail.onprem.ru`. При создании почтового домена рекомендуется соблюдение структуры: `***mail.***.***` или `***mail.***`.

- **Домен для облачных хранилищ** — `vbastra0st.onprem.ru`. Пример структуры: `***st.***.***` или `***cloud.***`.

Домен для облачных хранилищ должен быть **того же уровня**, что и домен для сервисов почты, и иметь свое уникальное имя.

> ⚠ **Важно**
>
> **Изменять структуру основных доменов запрещено!**
> Несоблюдение структуры и уровня доменов может привести к утечке данных через проброс cookies. Также вы столкнетесь с ошибками на этапе настройки доменных имен.

Далее в таблице представлен список **A-** или **CNAME-записей**, которые нужно создать перед установкой **VK WorkMail**. Домены из таблицы должны являться **поддоменами** для двух основных.

Назначение домена	Имя домена	Основной домен
Веб-интерфейс авторизации	account	Для почты
Скачивание вложений VK WorkMail	af	Для почты
Скачивание исполняемых вложений VK WorkMail	af	Для хранилищ
Проксирование активного контента вложений VK WorkMail	ampproxy	Для хранилищ
Просмотр вложений VK WorkMail	apf	Для почты
Просмотр исполняемых вложений VK WorkMail	apf	Для хранилищ
Доменная авторизация (внутренних запросов браузера)	auth	Для почты
Домен для панели расширенного просмотра действий пользователей	becca	Для почты
Интерфейс администрирования	biz	Для почты
Blobcloud-аттачи	blobcloud.e	Для почты
Домен для BMW gRPC запросов	bmw	Для почты

Назначение домена	Имя домена	Основной домен
Капча	c	Для почты
Календарь	calendar	Для почты
Домен интерфейса календаря для VK Teams	calendarmsg	Для почты
Мобильный календарь	calendartouch	Для почты
Статические данные календаря	calendarx	Для почты
VK WorkDisk	cloud	Для почты
Загрузка файлов в VK WorkDisk	cld-uploader.cloud	Для почты
Скачивание файлов в веб-интерфейсе VK WorkDisk	cloclo.cloud	Для почты
Защита от XSS-атак при скачивании файлов из VK WorkDisk	cloclo	Для хранилищ
Загрузка файлов в VK WorkDisk	cloclo-upload.cloud	Для почты
Интеграция с API VK WorkDisk	openapi.cloud	Для почты
Загрузка файлов в публичные папки в VK WorkDisk	pu.cloud	Для почты
Портальная авторизация VK WorkDisk	sdc.cloud	Для почты
Скачивание больших почтовых вложений из VK WorkDisk	cloclo-stock	Для хранилищ
Загрузка больших почтовых вложений в VK WorkDisk	uploader.e	Для почты
Превью файлов в VK WorkDisk	thumb.cloud	Для почты
Распаковка архивов в интерфейсе VK WorkDisk	cld-unzipper	Для хранилищ
Интеграция с API VK WorkMail	corsapi	Для хранилищ

Назначение домена	Имя домена	Основной домен
Веб-интерфейс VK WorkMail	e	Для почты
Сервис аватарок	filin	Для почты
IMAP VK WorkMail	imap	Для почты
Неисполняемые статические данные	img	Для почты
Исполняемые статические данные	imgs	Для почты
MX VK WorkMail	mxs	Для почты
OAUTH2-авторизация	o2	Для почты
Общепортальные сервисы авторизации	portal	Для почты
Проксирование внешних вложений VK WorkMail	proxy	Для хранилищ
Домен для текстового редактора R7-office	docs	Для хранилищ
Облако, реализующее S3 API	hb	Для хранилищ
SMTP VK WorkMail	smtp	Для почты
Сервер авторизации (межсерверные запросы)	swa	Для почты
Облако временных вложений VK WorkMail	tmpatt	Для хранилищ
Webdav	webdav.cloud	Для почты

Итоговый пример домена: `af` (субдомен из таблицы) + `vbastra0mail.onprem.ru` (основной домен из примера, который вы замените своим) = `af.vbastra0mail.onprem.ru`.

Важно

Изменять доменные имена из таблицы запрещено!
Установщик VK WorkMail использует их при развертывании системы. Если при установке не будет найден соответствующий домен, **может произойти сбой**.

Подключение дисков

К машинам, отведенным под хранилища, рекомендуется заранее подключить диски. Подключенные диски необходимо разбить на разделы, для этого можно использовать любые привычные утилиты, например fdisk.

На разделах дисков необходимо создать файловую систему. Мы рекомендуем **ext4**, также поддерживается **xfs**.

Пример команды для создания файловой системы ext4:

```
mkfs.ext4 <путь к устройству>
```

> **Важно**
>
> **Минимальный размер** раздела диска, используемого под хранилище, составляет **25 GB**.

Список портов для установки

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
TCP	9091	calico-node	Демон динамической маршрутизации	Сбор метрик prometheus	victoria-metrics
TCP	5000	registry	Хранилище docker-образов	Подключение к сервису	Все машины инсталляции
TCP	2379	infraetcd	etcd, которое хранит инфраструктурные данные, например настройки сети	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP	2380	infraetcd	etcd, которое хранит инфраструктурные данные, например настройки сети	Общение между инстансами etcd	Другие infraetcd
TCP	4001	infraetcd	etcd, которое хранит		

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
			инфраструктурные данные, например настройки сети	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP	8080	cadvisor	Инструмент снятия телеметрии с контейнеров	Сбор метрик prometheus	victoria-metrics
TCP	2003	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры
TCP	2004	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры
TCP	22	sshd	Демон операционной системы, предоставляющий консоль пользователю	ssh подключения	Onpremise-deployer
TCP	179	Bird	Calico. Работа BGP сессиий	_	Между всеми серверами системы
TCP	8888	onpremise-deployer	Приложения для установки и начальной настройки VK WorkSpace	Подключение администраторов	Администраторы
UDP	2003	carbclick	Сервис, который принимает метрики и	Прием метрик	Любые контейнеры

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
			передает их в clickhouse		

Этапы установки

Весь процесс установки можно разделить на **два этапа**:

1. В командной строке на сервере выполняются действия для запуска установщика.
2. Последующая установка производится в специальном веб-интерфейсе.

Действия в командной строке на сервере

1. Создание пользователя deployer

В командной строке выполните последовательность команд:

Astra Linux

```
sudo -i

# Задаем пароль и создаем пользователя deployer
DEPLOYER_PASSWORD=mURvnxJ9Jr
useradd -G astra-admin -U -m -s /bin/bash deployer
echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

# Игнорируем ошибку "НЕУДАЧНЫЙ ПАРОЛЬ: error loading dictionary"
# в случае, если она появилась

# Перелогиниваемся под пользователя deployer
sudo -i -u deployer

ssh-keygen -t rsa -N ""
# Нажимаем Enter (согласиться с вариантом по умолчанию)

# Копируем ssh-ключ в нужную директорию
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys

# Опционально: проверяем, что сами к себе можем зайти без пароля
ssh deployer@localhost
exit
```

РЕД ОС

```
sudo -i

# Задаем пароль и создаем пользователя deployer
DEPLOYER_PASSWORD=mURvnxJ9Jr
useradd -G wheel -U -m -s /bin/bash deployer
echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

# Перелогиниваемся под пользователя deployer
sudo -i -u deployer

ssh-keygen -t rsa -N ""
# Нажимаем Enter (согласиться с вариантом по умолчанию)

# Копируем ssh-ключ в нужную директорию
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys

# Опционально: проверяем, что сами к себе можем зайти без пароля
ssh deployer@localhost
exit
```

CentOS

```
# Создаем пользователя
adduser deployer
passwd deployer
usermod -aG wheel deployer

# Авторизовываемся под этим пользователем
su - deployer
# Создаем ключ
ssh-keygen -t rsa
# Прописываем в authorized_key для ssh
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

Важно

Вся дальнейшая установка будет производиться под созданным пользователем **deployer**. Пользователь должен иметь права администратора.

Затем в файле `/etc/sudoers` раскомментируйте строку, следующую после `## Same thing without a password` :

Astra Linux

```
# %astra-admin       ALL=(ALL)       NOPASSWD: ALL
```

РЕД ОС

```
# %wheel        ALL=(ALL)       NOPASSWD: ALL
```

CentOS

```
# %wheel        ALL=(ALL)       NOPASSWD: ALL
```

Для этого нужно выполнить команду `sudo visudo` и убрать **#** в начале приведенной выше строки, после чего выйти из **Vim** с сохранением файла.

То же самое можно сделать с помощью редактора **nano**:

```
sudo EDITOR=nano visudo
# Находим нужную строку, удаляем # в ее начале
# Выходим из nano с сохранением изменений
```

2. Распаковка дистрибутива

Распакуйте дистрибутив под пользователя **deployer**. Нет принципиальной разницы, каким архиватором пользоваться.

Ниже приведен пример для **unzip**:

Astra Linux

```
# В случае если на машину не установлен unzip, скачиваем его:
sudo apt-get install unzip
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P пароль имя_архива
```

РЕД ОС

```
# В случае если на машину не установлен unzip, скачиваем его:
sudo yum install unzip
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P пароль имя_архива
```

CentOS

```
# В случае если на машину не установлен unzip, скачиваем его:
sudo yum install unzip
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P пароль имя_архива
```

> **Важно**
>
> После распаковки **не удаляйте** никакие файлы. По завершении установки допускается только удаление архива, из которого был распакован дистрибутив.

3. Запуск установщика как сервиса

Установщик **onpremise-deployer_linux** рекомендуется запускать как сервис. При таком запуске не придется прибегать к дополнительным мерам (**screen**, **tmux**, **nohup** и т.п.), позволяющим установщику продолжить работу в случае потери соединения по SSH.

Чтобы запустить установщик как сервис, выполните команду (подходит для Astra Linux, РЕД ОС и CentOS):

```
sudo ./onpremise-deployer_linux -concurInstallLimit 5  \
  -serviceEnable -serviceMake -serviceUser deployer
```

По умолчанию выставлен лимит в 5 потоков, при необходимости вы можете увеличить количество потоков до 10, однако это увеличит и нагрузку на систему. Использование более чем 10 потоков **не рекомендуется**.

Ответ в случае успешного запуска установщика выглядит следующим образом:

Astra Linux

```
deployer.service was added/updates
see status: <systemctl status deployer.service>
can`t restart rsyslog services: [exit status 5]
OUT: Failed to restart rsyslog.service: Unit rsyslog.service not found.
deployer.service was enable and started
see status: <systemctl status deployer.service>
```

РЕД ОС

```
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:g8siO32KUsRU9oC/MHro9WaTNKj4R+DkmVnVa7QsYCo.
This key is not known by any other names
# Введите "yes" и нажмите Enter, чтобы подтвердить подключение
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

CentOS

```
deployer.service was added/updates
see status: <systemctl status deployer.service>
deployer service rsyslog config was added/updates
see logs: <less /var/log/deployer.log>
deployer.service was enable and started
see status: <systemctl status deployer.service>
```

Примечание

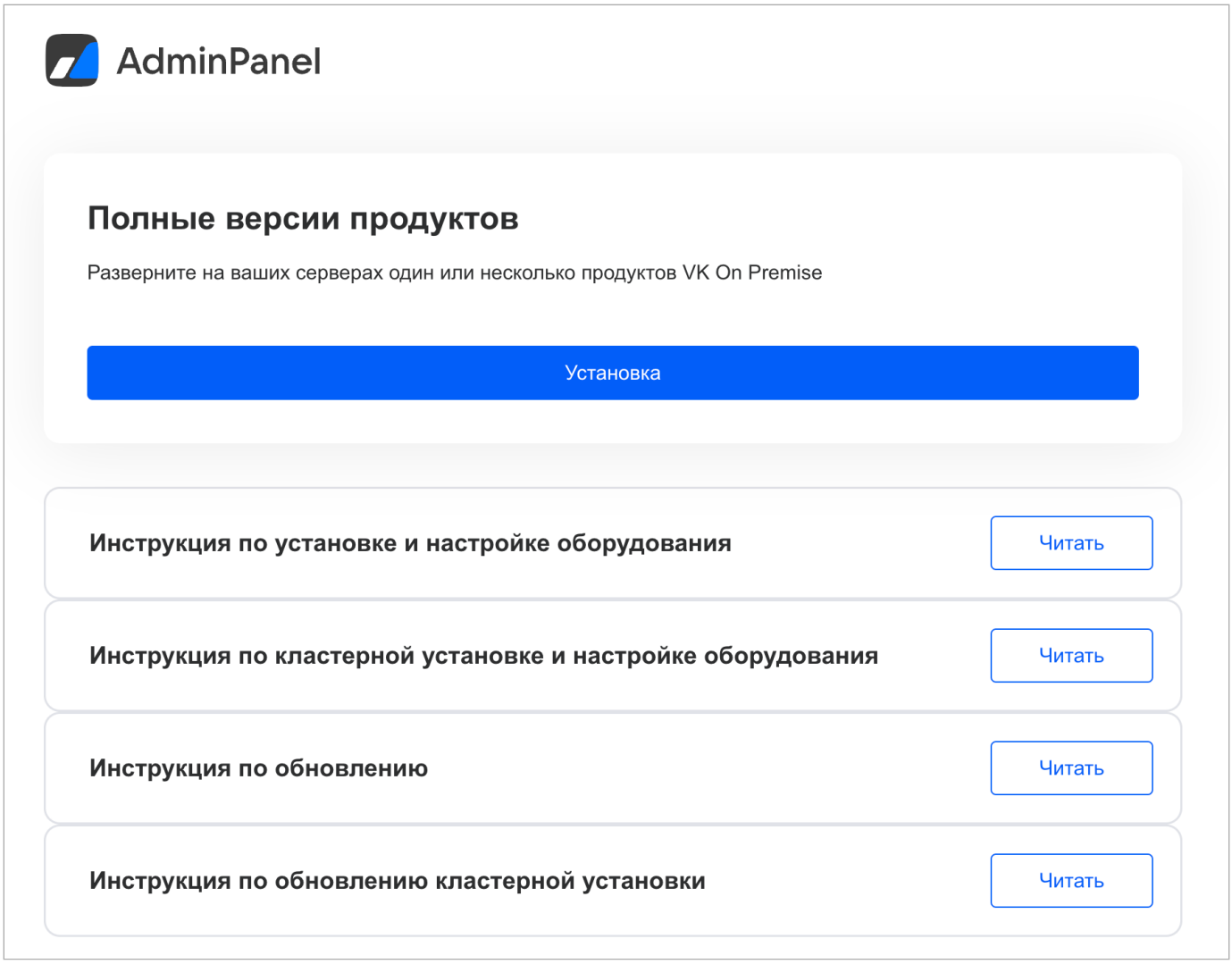
Невозможность включения службы `rsyslog` не повлияет на корректность работы сервиса.

Действия в веб-интерфейсе установщика

Для перехода в веб-интерфейс в адресной строке браузера укажите адрес: `http://server-ip-address:8888`. Если перейти по этому адресу не удается, убедитесь, что **firewall** был отключен.

1. Выбор варианта установки

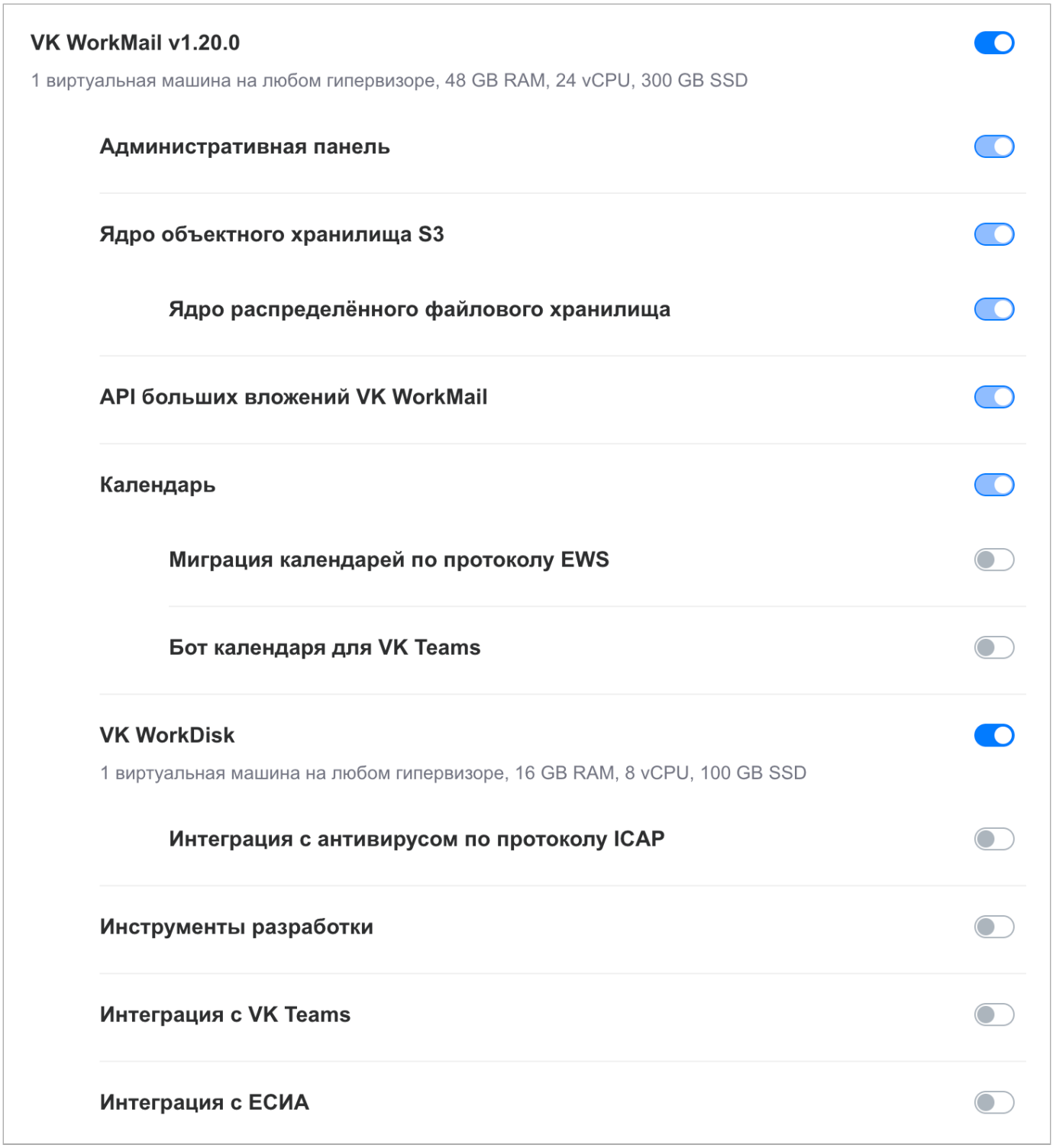
На стартовой странице нажмите на кнопку **Установка**.



2. Выбор продуктов и опций

Включите флаг **VK WorkMail**.

В открывшемся списке отметьте **VK WorkDisk** и нужные вам компоненты. В случае если планируется настройка интеграций, также выберите их в списке продуктов.


VK WorkMail v1.20.0
1 виртуальная машина на любом гипервизоре, 48 GB RAM, 24 vCPU, 300 GB SSD
Административная панель
Ядро объектного хранилища S3
Ядро распределённого файлового хранилища
API больших вложений VK WorkMail
Календарь
Миграция календарей по протоколу EWS
Бот календаря для VK Teams
VK WorkDisk
1 виртуальная машина на любом гипервизоре, 16 GB RAM, 8 vCPU, 100 GB SSD
Интеграция с антивирусом по протоколу ICAP
Инструменты разработки
Интеграция с VK Teams
Интеграция с ЕСИА

Интеграция с другими инсталляциями VK WorkMail Deprecated

Интеграция с Keycloak

Средства резервного копирования почтовых ящиков

Двухфакторная аутентификация

Интеграция с редактором «МойОфис»

Редактор «Р7-Офис» внутри инсталляции

2 GB RAM, 2 vCPU

Интеграция с редактором «Р7-Офис»

Система расширенных транспортных правил

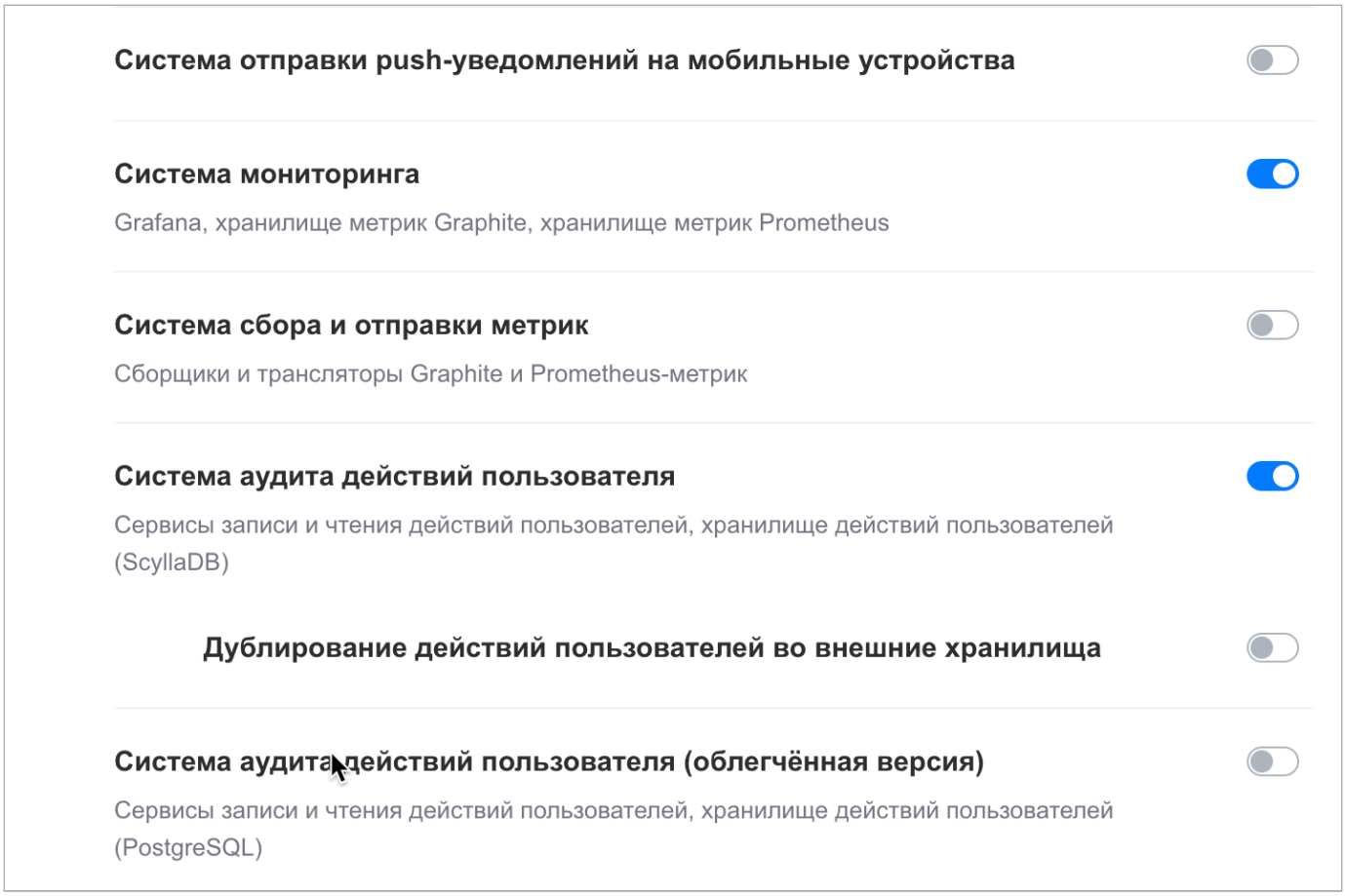
Бот новых почтовых сообщений для VK Teams

Сервис анализа логов доставки почты Beta

16 GB RAM, 16 vCPU

Система групповых политик Beta

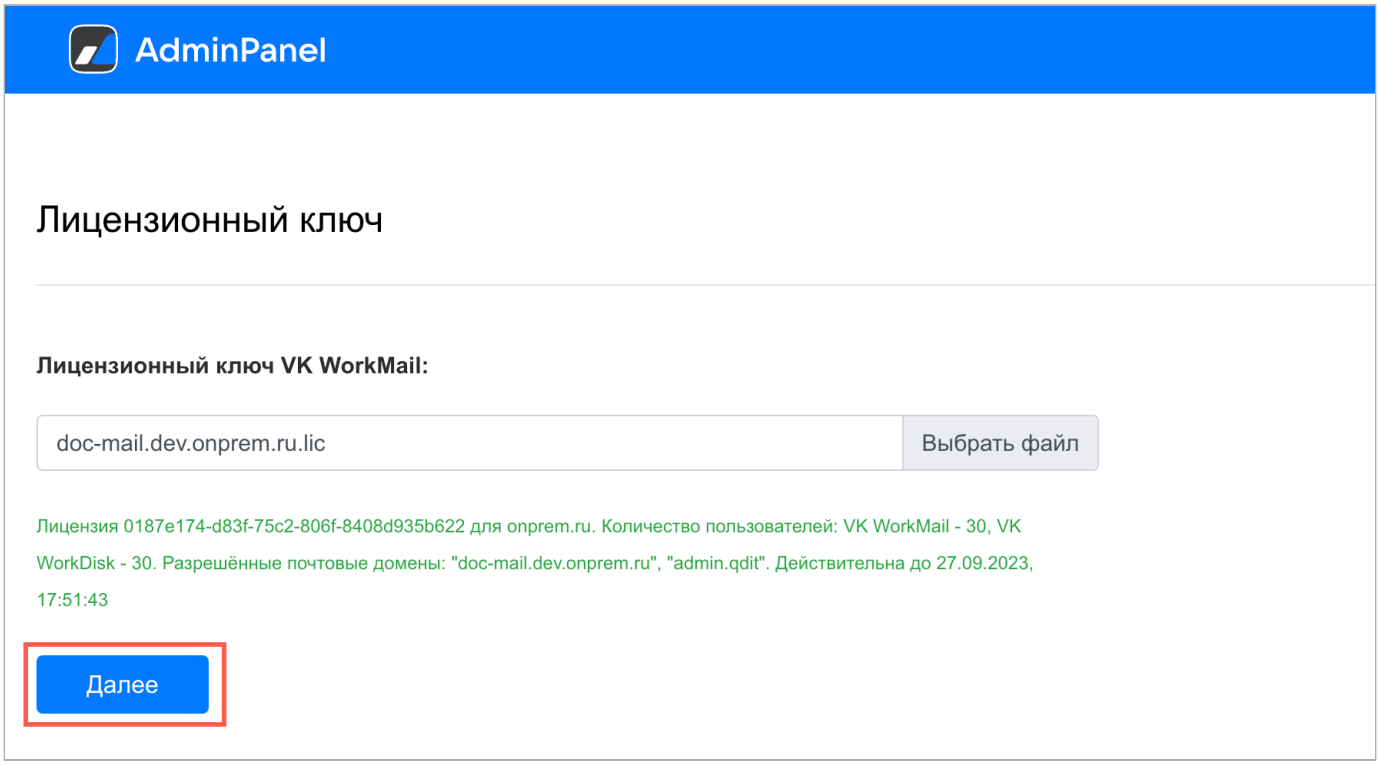
Система BI-аналитики Beta



Нажмите кнопку **Далее** для перехода к следующему шагу.

3. Добавление лицензионного ключа

Введите лицензионный ключ или укажите путь к файлу лицензии **.lic**, затем нажмите на кнопку **Далее**.

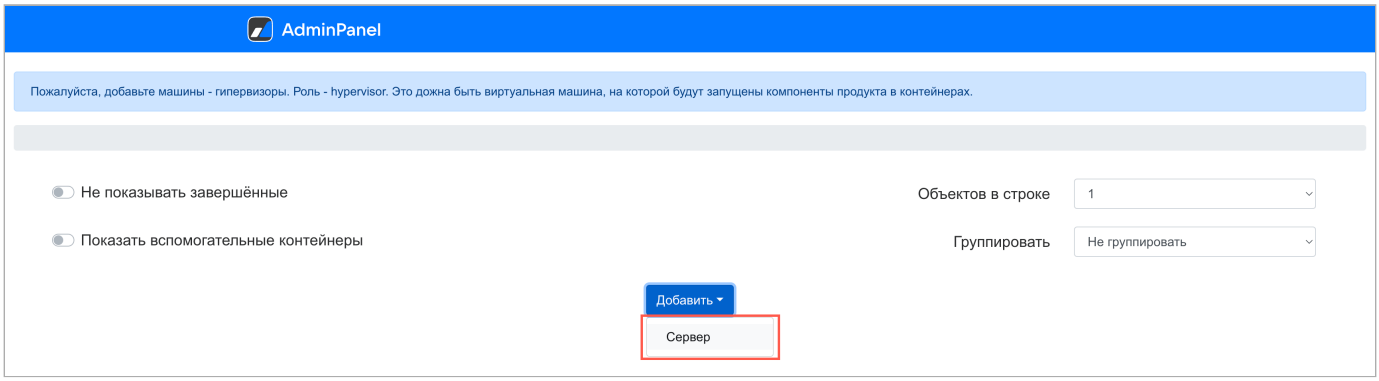


Примечание

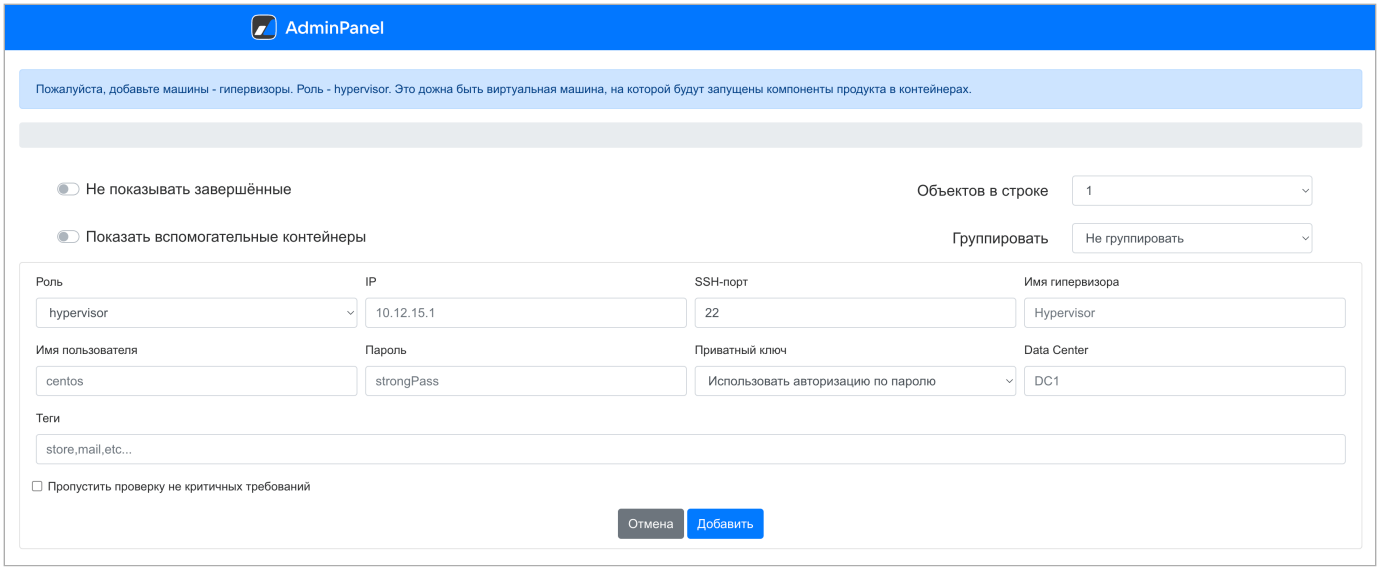
Информацию о том, как обновить лицензионный ключ или проверить сроки действия лицензий по продуктам VK WorkSpace, вы сможете найти в приложении.

4. Добавление гипервизора

Нажмите на кнопку **Добавить**, в выпадающем меню выберите **Сервер**.



Откроется окно добавления гипервизора:



Заполните поля:

Роль — hypervisor.

IP — адрес машины, на которую производится установка.

SSH-порт — стандартный для SSH, выбран по умолчанию, менять его не нужно.

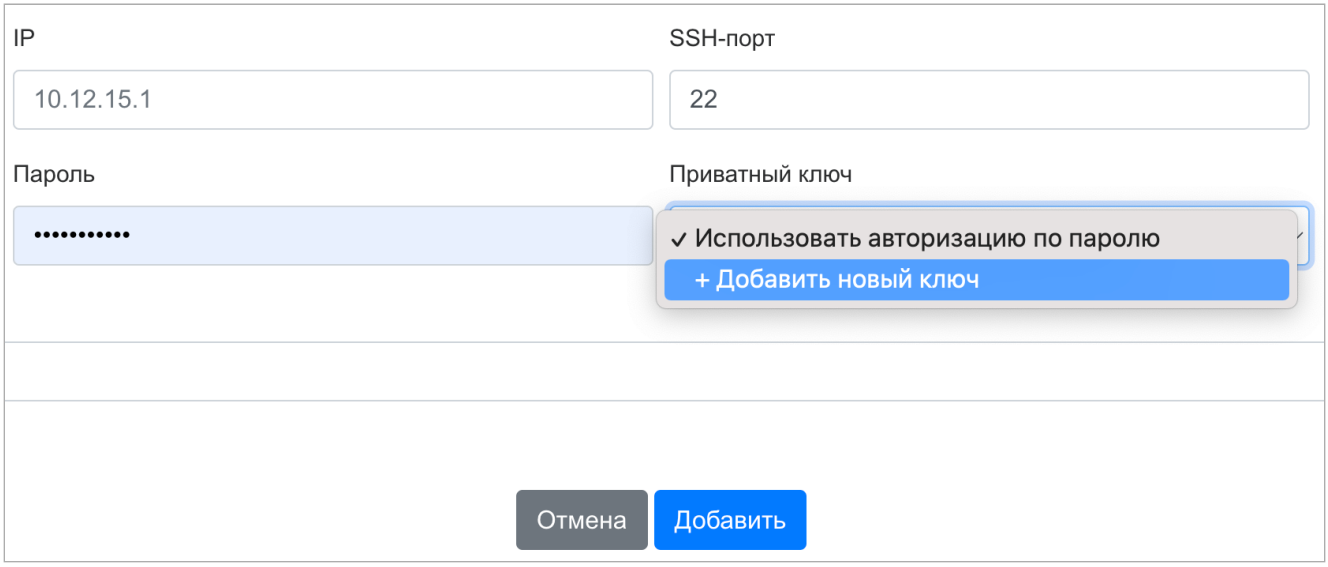
Имя гипервизора — укажите имя гипервизора или оставьте поле пустым. В случае если вы оставите поле незаполненным, имя гипервизора будет взято из `hostname -s` и добавится автоматически. Рекомендуется давать названия гипервизорам в соответствии с их назначением, например: hypervisor-mon или storage1, db1 и т.п.

Имя пользователя — укажите имя того пользователя, под которым запущен установщик. В рассматриваемом примере это пользователь deployer.

Пароль — необходимо ввести пароль пользователя, под которым запущен установщик, если он был задан при создании.

Добавьте **SSH-ключ** (также можно оставить авторизацию по паролю):

- В поле **Приватный ключ** выберите **Добавить новый ключ**.



- Откроется окно добавления ключа. В поле **Имя ключа** укажите любое удобное имяв соответствии с их назначением **deployerRSA**.
- Перейдите в консоль, выполните в ней команду `cat ~/.ssh/id_rsa` и скопируйте ключ.
- Затем вставьте его в поле **Приватный ключ**. Его нужно указать полностью, включая `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`
- Поле **Пароль ключа** оставьте пустым.
- Установите чекбокс **Использовать по умолчанию**, если один ключ используется на всех гипервизорах.
- Кликните по кнопке **Сохранить**.

После добавления приватного ключа вы вернетесь к исходному окну добавления гипервизора.

При необходимости настройте дополнительные поля:

- **Data Center** — тег используется в георасределенной кластерной установке, если вам не требуется пометка о дата-центре, оставьте поле пустым.
- **Теги** — для большей наглядности и простоты поиска вы можете присвоить гипервизорам теги в зависимости от их роли.
- **Пропустить проверку некритичных требований** — если отметить чекбокс, будет пропущена проверка версии ядра и флагов процессора (sse2, avx). В большинстве случаев выбор чекбокса не требуется.

После заполнения полей нажмите на кнопку **Добавить** — гипервизор отобразится в веб-интерфейсе установщика.

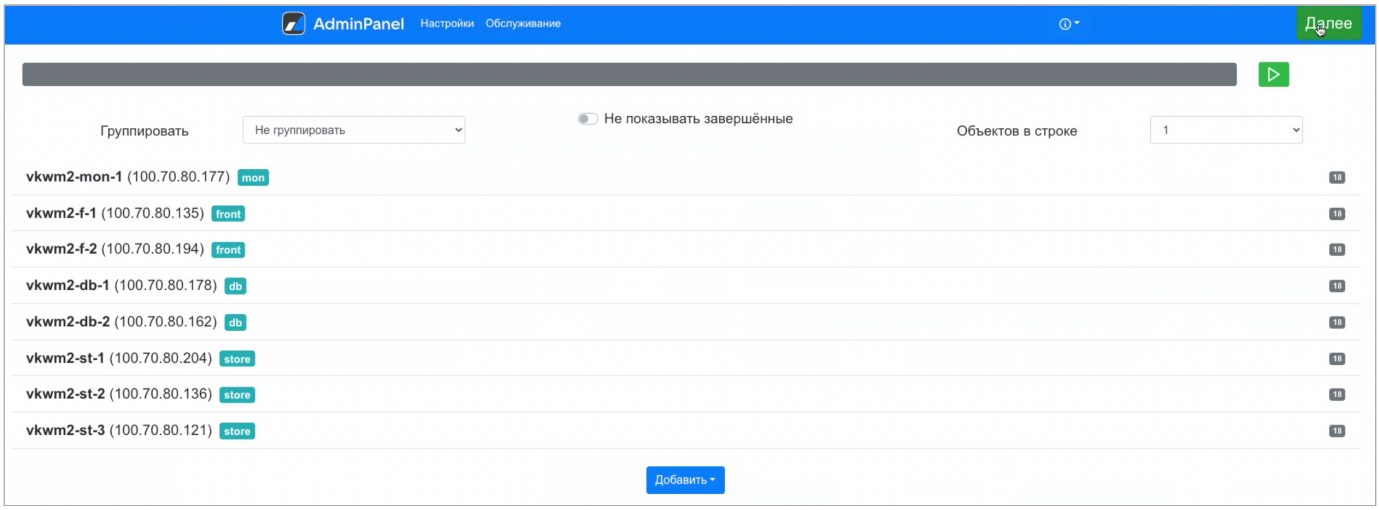
Примечание

При добавлении сервера реализована проверка на наличие команд **tar**, **scp** и необходимых инструкций виртуализации на процессорах. Если при проверке они не будут найдены, то сервер не будет добавлен, а администратор получит сообщение об ошибке.

Аналогичным образом добавьте еще 7 гипервизоров:

- 2 — под фронты,
- 2 — под базы данных,
- 3 — под хранилища.

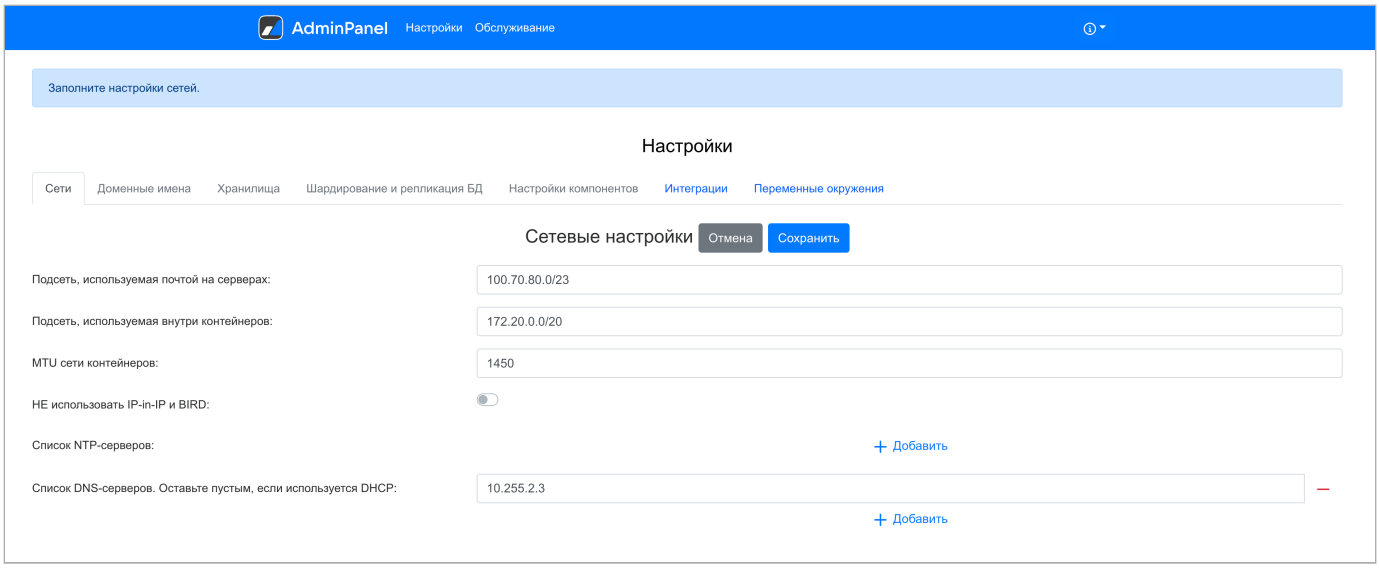
На изображении ниже приведен пример того, как выглядит веб-интерфейс установщика после добавления всех гипервизоров.



Для перехода к следующему шагу нажмите на зеленую кнопку **Далее** в правом верхнем углу.

5. Сетевые настройки

Установщик автоматически вычисляет некоторые сетевые параметры. Эти параметры необходимо проверить и дополнить, если не все из них были определены.



Укажите **NTP-сервер** и **DNS-сервер**.

> **Важно**
>
> Обязательно настройте NTP в соответствии с рекомендациями: для RedOS, для Astra Linux. Не следует указывать белый NTP-сервер.

Убедитесь, что:

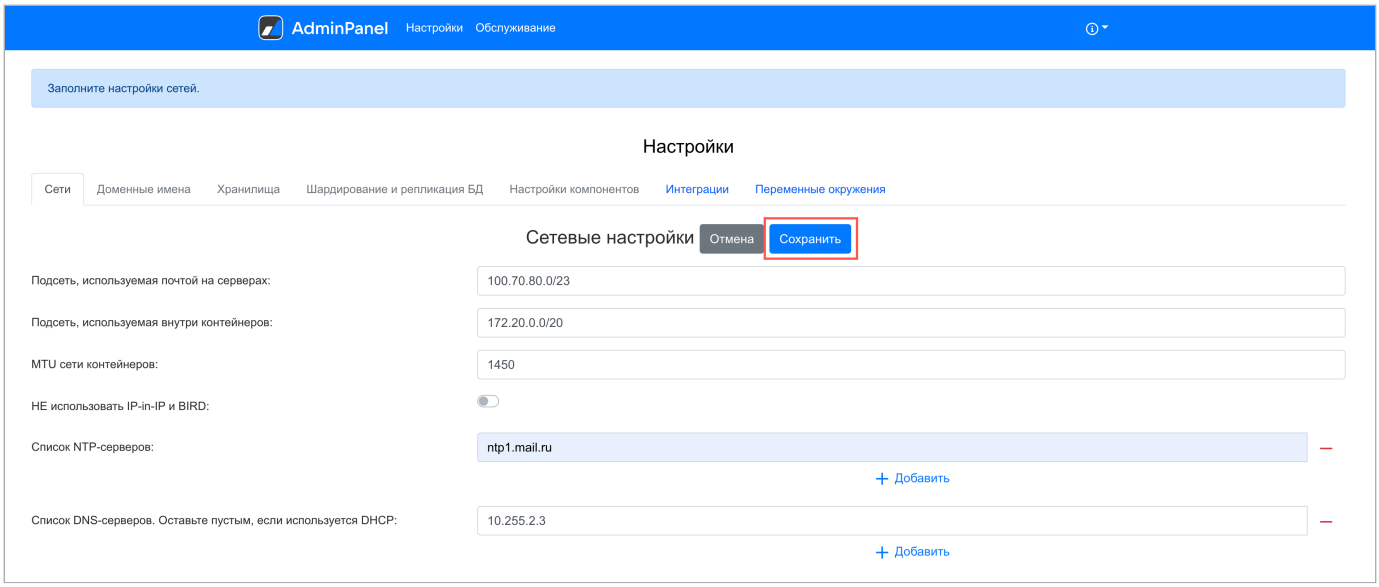
- **Подсеть, используемая почтой на серверах**, имеет доступ на **80-й** или **443-й** порт.
- **Подсеть, используемая внутри контейнеров**, полностью свободна, уникальна и принадлежит только VK WorkMail.

> **Примечание**
>
> Эта подсеть используется только для трафика между контейнерами внутри системы. Если автоматически вычисленная подсеть уникальна и не пересекается с другими подсетями заказчика, значения менять не нужно. По умолчанию используется **20-я подсеть**.

Поле **MTU сети контейнеров** заполняется автоматически. Если вы хотите изменить размер MTU, обратитесь к представителю VK.

Флаг **НЕ использовать IP-in-IP и BIRD** в большинстве случаев должен оставаться неактивным. Если на машине используется динамическая маршрутизация и необходимо включение опции, обратитесь к представителю VK.

После проверки всех настроек нажмите на кнопку **Сохранить** и перейдите к следующему шагу.



6. Доменные имена

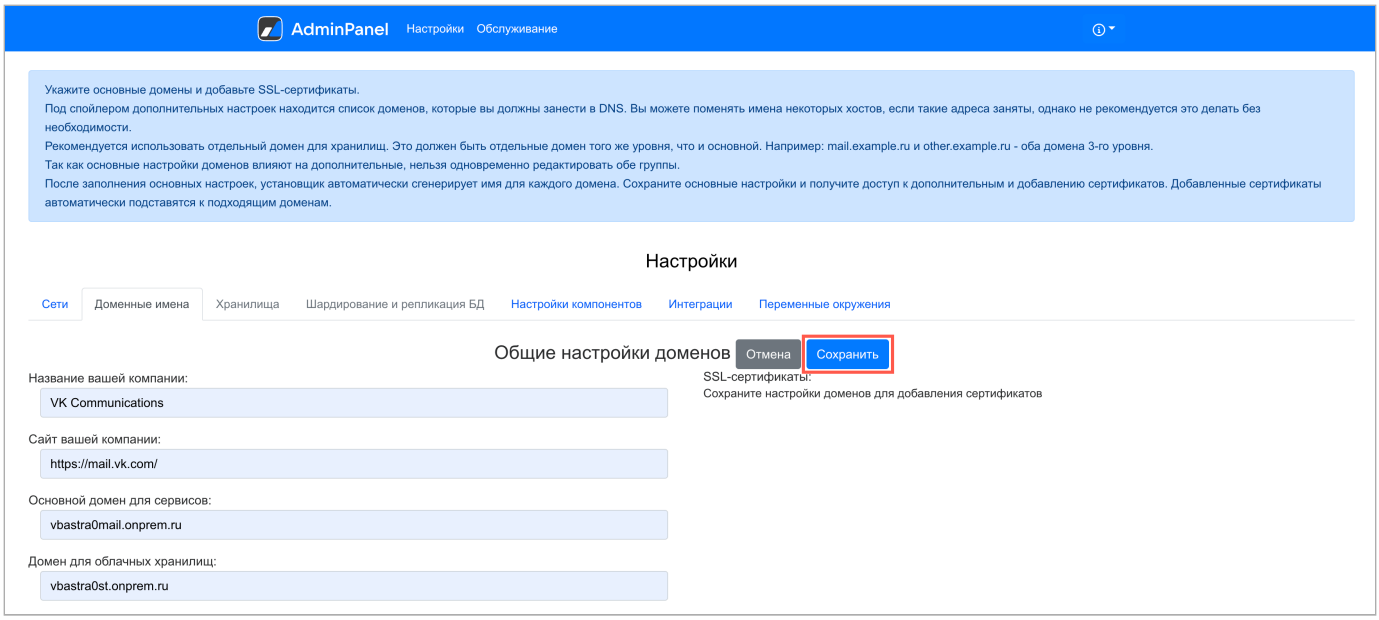
> **Информация**
>
> Подробную информацию о создании доменных имен вы найдете в разделе Создание DNS-записей.

На вкладке **Доменные имена** необходимо заполнить все поля:

- **Название вашей компании** — введите название компании, которое будет отображаться в интерфейсе почты.
- **Сайт вашей компании** — укажите сайт вашей компании.
- **Основной домен для сервисов** — в поле необходимо указать ранее созданный Основной домен для почты.
- **Домен для облачных хранилищ** — в поле введите ранее созданный Домен для облачных хранилищ.

> **Важно**
>
> Для доменных имен нельзя использовать `etc/hosts`.

Когда все поля будут заполнены, нажмите на кнопку **Сохранить** для перехода к следующему шагу.

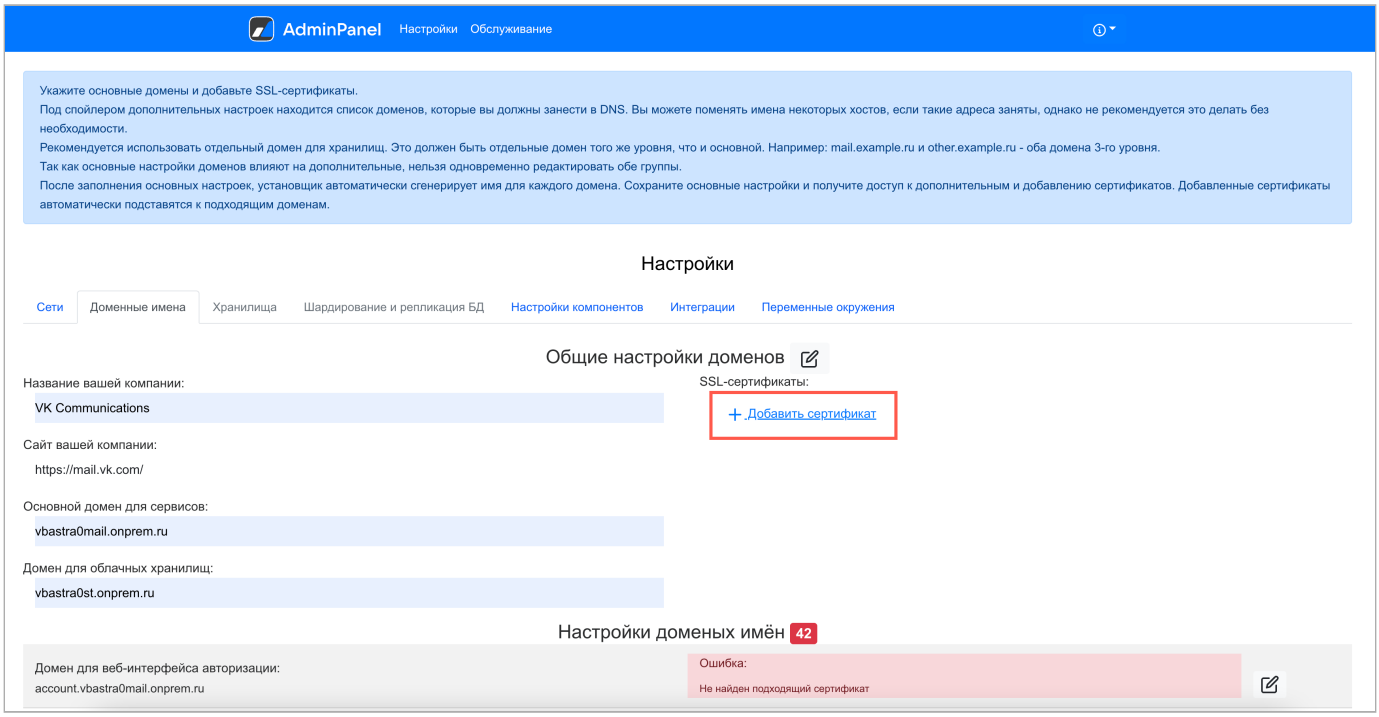


Примечание

После сохранения доменных имен появятся ошибки. Они пропадут после добавления SSL-сертификатов на следующем шаге, но **SMTP**, **MX** и **IMAP** могут остаться красными — это нормально.

6.1 Добавление SSL-сертификатов

Нажмите на кнопку **Добавить сертификат** под заголовком **SSL-сертификаты**.



В открывшейся форме введите сертификат и ключ. Их необходимо указать полностью, включая:

`-----BEGIN CERTIFICATE-----` и `-----END CERTIFICATE-----`

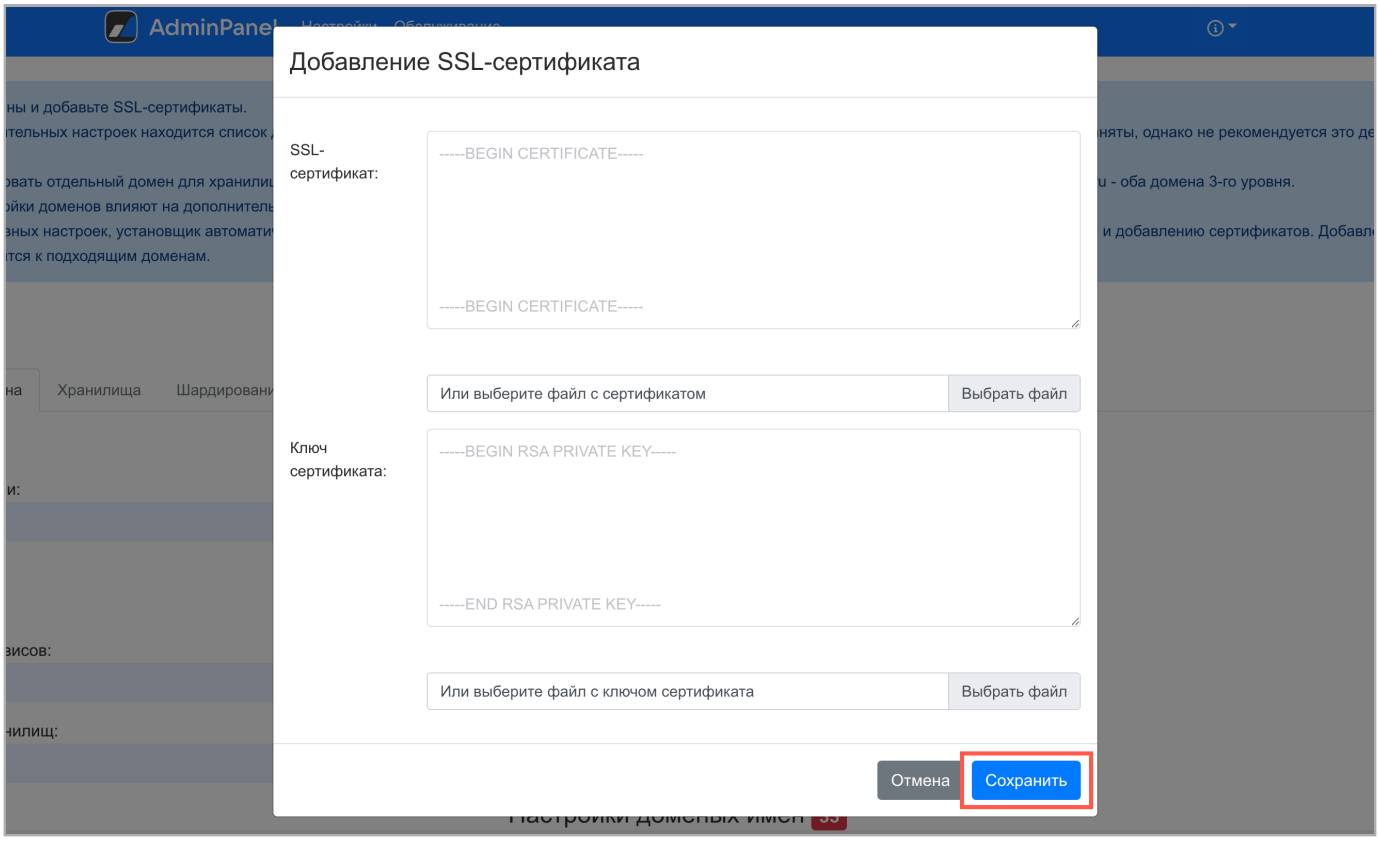
и

`-----BEGIN PRIVATE KEY-----` и `-----END PRIVATE KEY-----`.

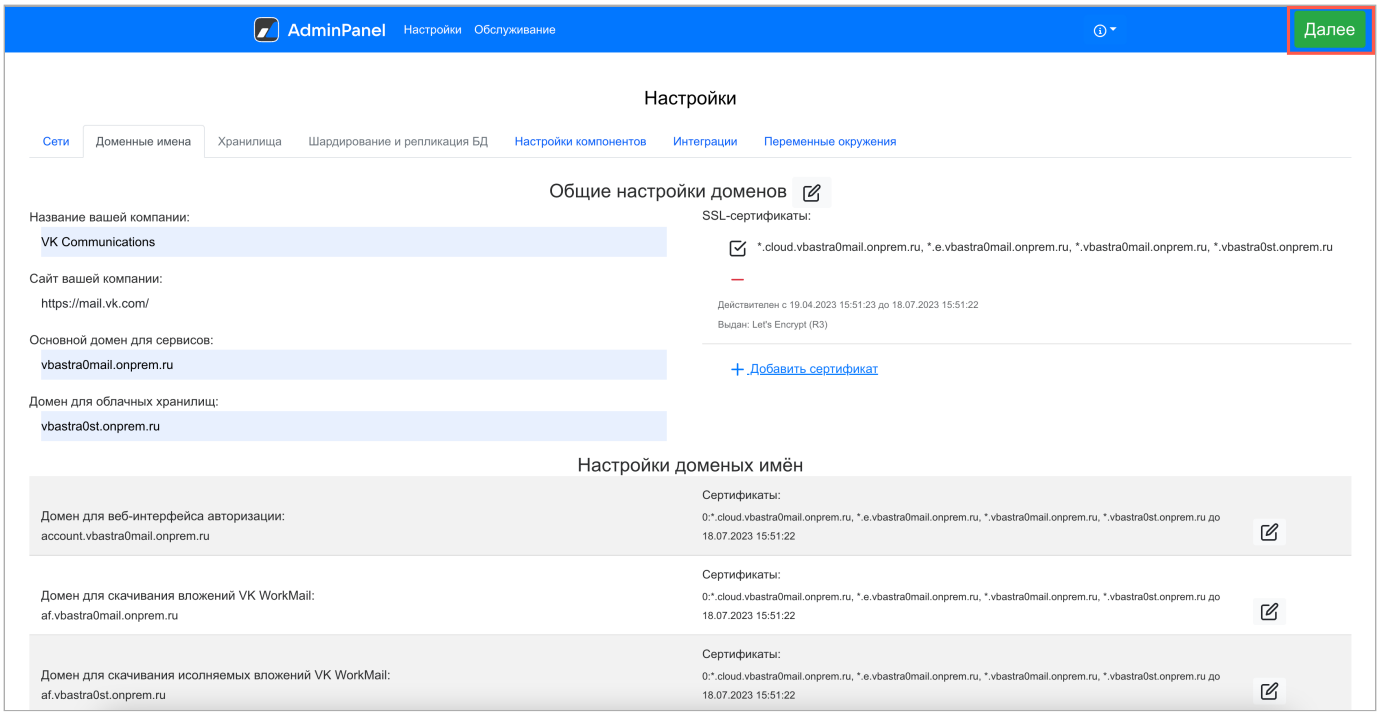
Или нажмите на кнопку **Выбрать файл** и укажите путь к файлу с сертификатом **.crt**, а затем к файлу с ключом **.key**.

> **Примечание**
>
> Приватный ключ должен быть добавлен в открытом виде, без секретной фразы. Закодированный ключ отличается от открытого наличием слова ENCRYPTED: `BEGIN ENCRYPTED PRIVATE KEY`.

Кликните по кнопке **Сохранить**.



Если всё верно, в интерфейсе не будет отображаться ошибок и красной подсветки (у **SMTP**, **MX** и **IMAP** красная подсветка может остаться). Нажмите на зеленую кнопку **Далее**.



7. Установка гипервизоров

Начала установки необходимо перейти к списку гипервизоров — для этого нажмите на логотип **AdminPanel**.

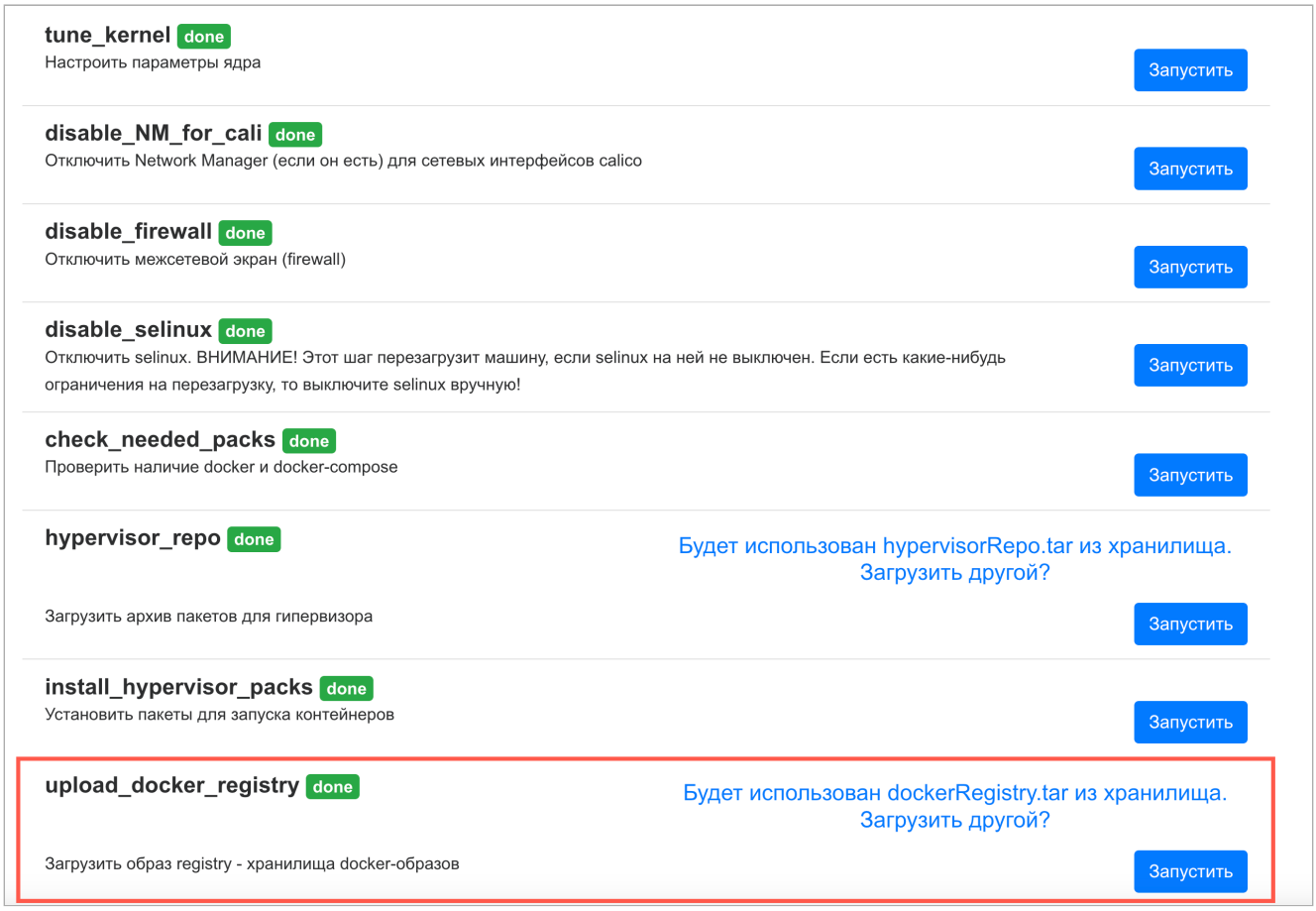
Порядок установки принципиален, так как из них формируется **кластер etcd**. Для кворума кластеру необходимо **N/2+1** экземпляров etcd. В минимальной конфигурации узлы ectd должны быть установлены на **три машины**, две из которых должны быть постоянно доступны. В документе будет описан вариант установки etcd в минимальной конфигурации.

Существует **два варианта** формирования кластера: на три гипервизора, отведенных под хранилища, или на машину мониторинга и два гипервизора под базы данных.

> **Информация**
>
> Если вы выберете первый вариант установки etcd, вам потребуется переход в настройки гипервизоров с помощью кнопки ⚙, ручной запуск отдельных шагов и приостановка установки. Чтобы приостановить установку, нужно нажать на кнопку **Stop** в общей строке состояния.

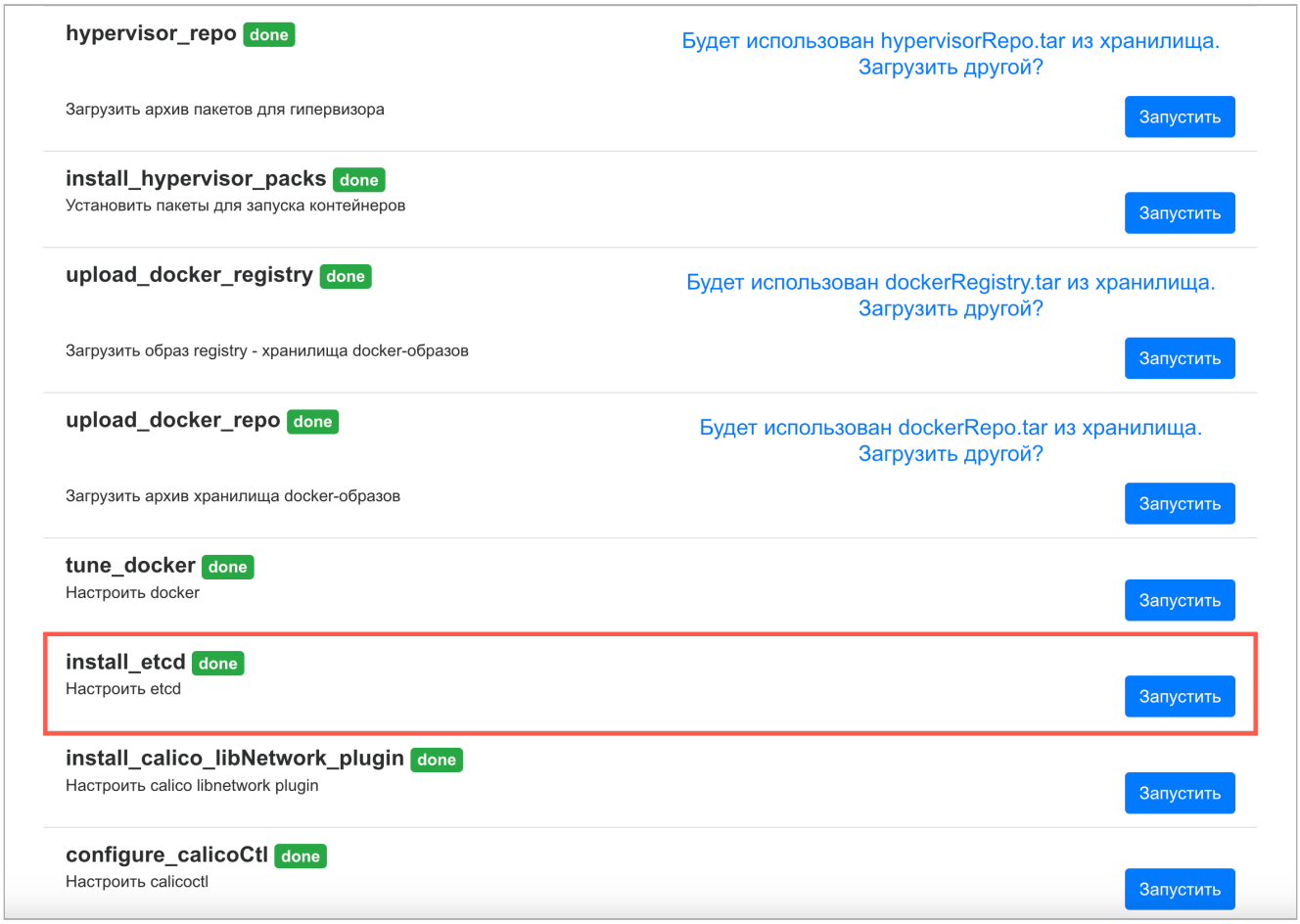
Первый вариант:

1. Перейдите в настройки гипервизора, отведенного под мониторинг. Вручную запустите шаги до **upload_docker_registry** включительно.



2. Вернитесь обратно к списку машин и запустите установку первого гипервизора-стораджа.

3. Перед шагом **install_etcd** приостановите установку.



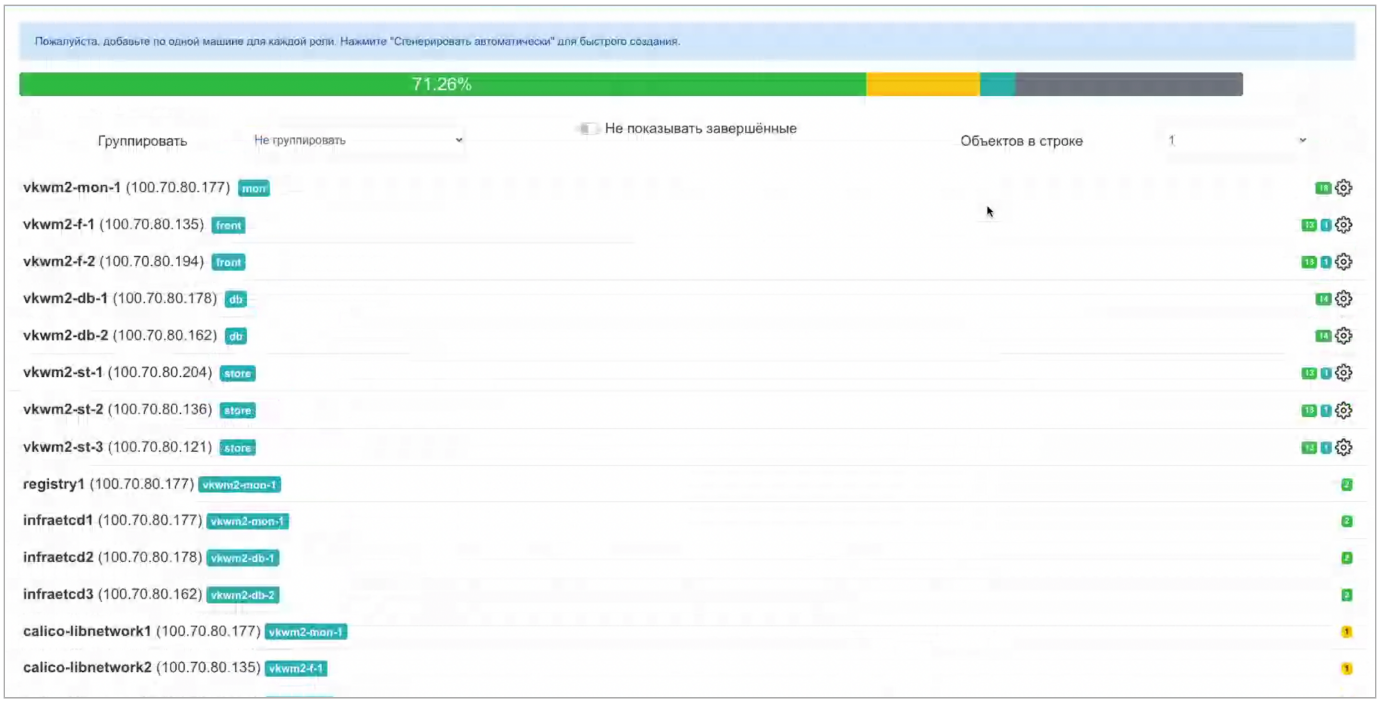
4. Запустите шаг **install_etcd** вручную. По завершении шага первый узел etcd будет установлен.
5. Таким же способом установите etcd на остальные два гипервизора-стораджа.
6. После того, как кластер etcd собран, запустите установку всех гипервизоров по порядку или общую автоматическую установку.

> **Важно**
>
> Не рекомендуется запускать установку нескольких гипервизоров одновременно — это может привести к ошибкам.

Второй вариант выглядит так:

1. Запустите установку первого гипервизора (мониторинг). На этот гипервизор будет автоматически добавлен первый узел etcd.
2. Когда установка первого гипервизора завершится, запустите установку второго гипервизора (БД).
3. Когда установка второго гипервизора завершится, запустить установку третьего (БД).
4. По такому же принципу последовательно установите все оставшиеся гипервизоры.
5. На двух гипервизорах, отведенных под базы данных, вручную в настройках выполните опциональный шаг **install_etcd**.

На изображении ниже приведен пример того, как выглядит веб-интерфейс установщика после завершения установки всех гипервизоров.



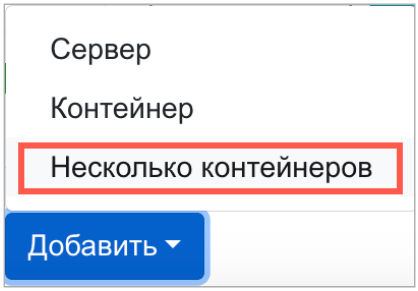
Информация

Развернутую информацию о назначении ролей, их дублируемости, зависимостях и т.п. вы можете найти, кликнув по значку ⓘ и перейдя в раздел **Описание сервисов**. В этом же выпадающем меню вы найдете дополнительную документацию, сможете включить или выключить продукты (внутри раздела **Продукты**) и обновить лицензионный ключ.

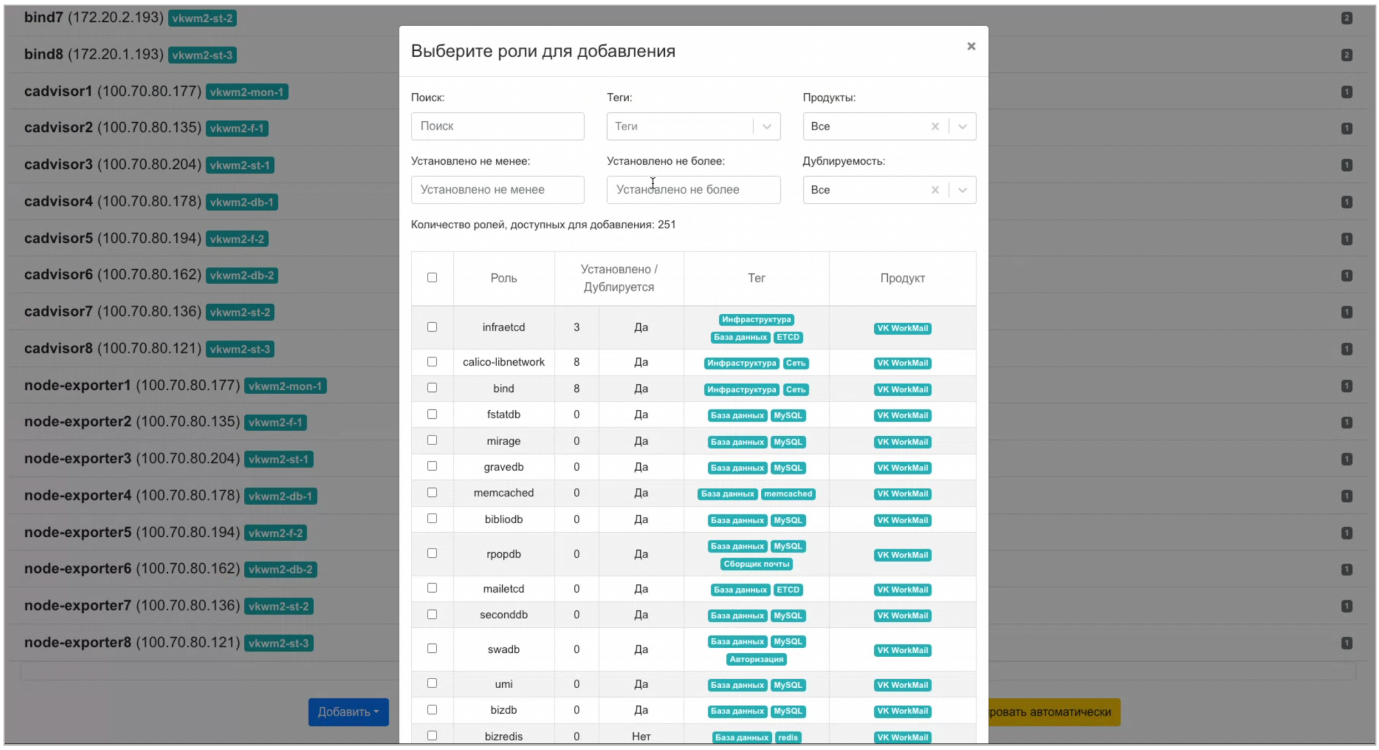
8. Распределение контейнеров по гипервизорам

По завершении установки всех гипервизоров можно приступать к распределению и генерации контейнеров.

В нижней части экрана выберите **Добавить** → **Несколько контейнеров**.



Откроется окно выбора ролей.



При распределении ролей нужно соблюдать такой порядок:

1. Хранилища
2. xtaz
3. raft
4. Базы данных
5. Мониторинг
6. Почтовый транспорт
7. API
8. Все, что осталось (опционально).

> **Важно**
>
> Порядок распределения ролей **принципиально важен**, при его нарушении вы столкнетесь с ошибками.

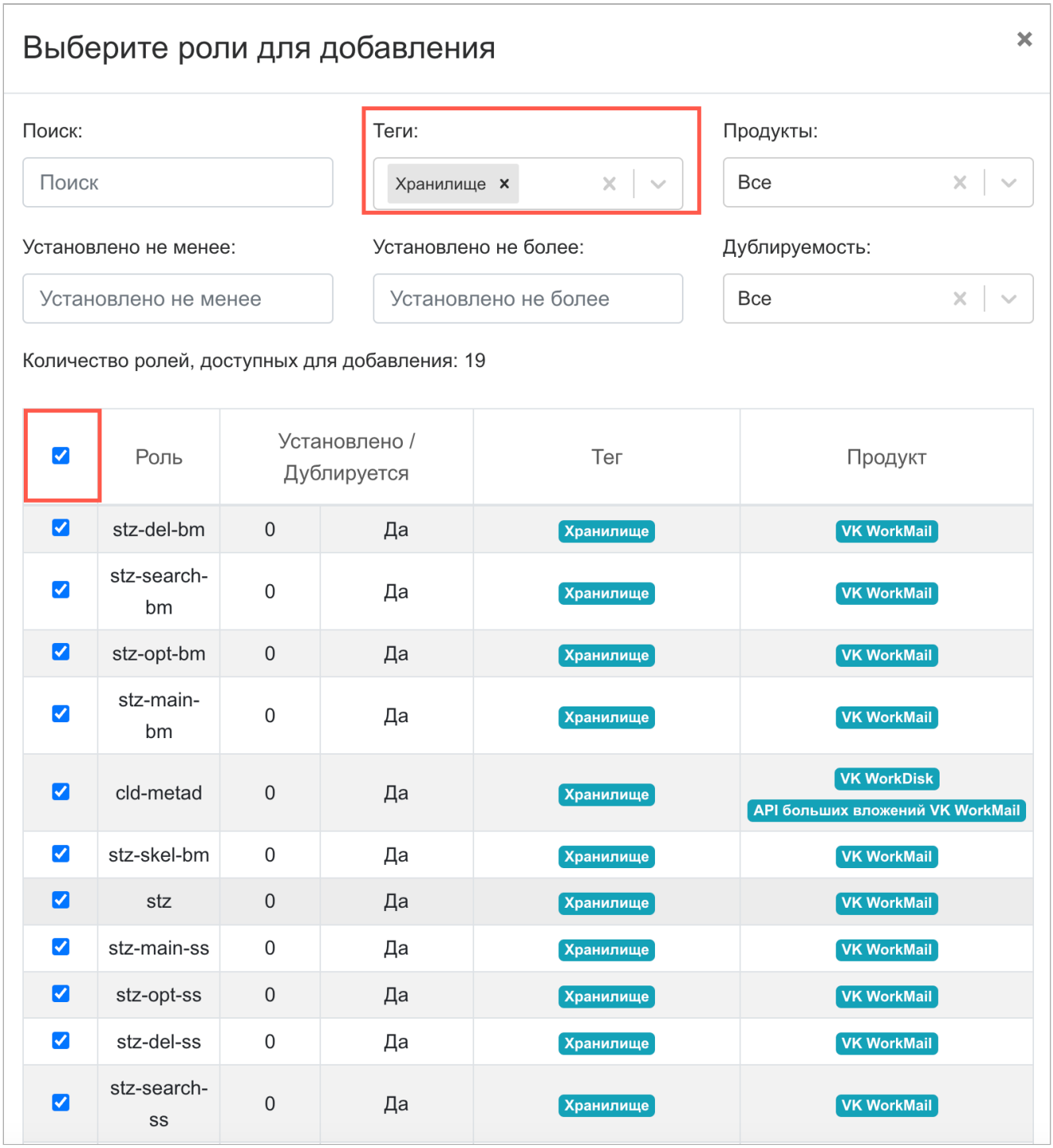
Для выбора ролей используйте поле **Теги** в качестве фильтра.

Порядок действий при распределении контейнеров

Первыми должны быть выбраны роли для хранилищ:

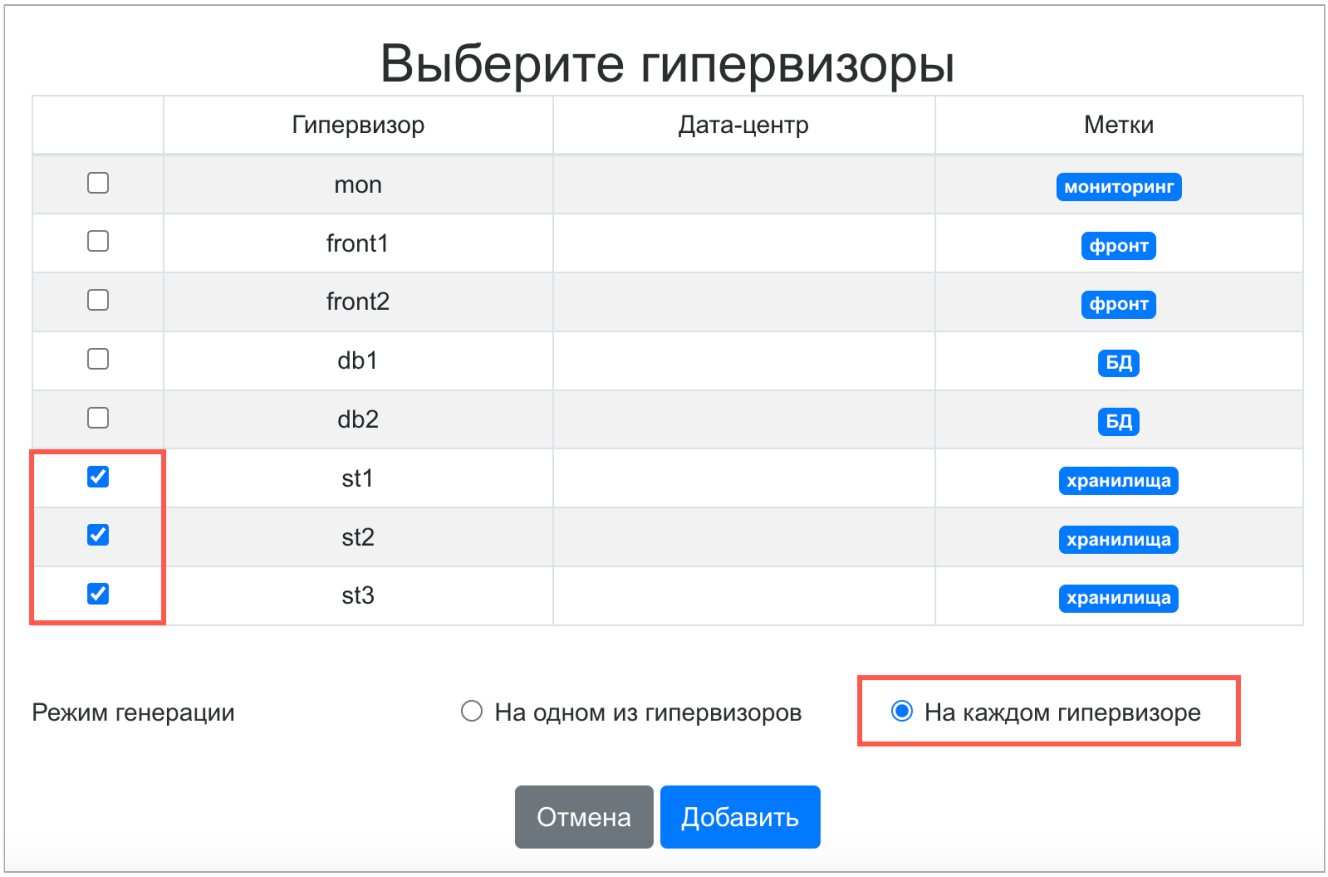
1. В выпадающем меню выберите тег **Хранилище**.

2. Отметьте **Все** доступные для установки роли с помощью чекбокса в таблице.



3. Ниже в списке гипервизоров отметьте те, которые были отведены под стораджи.

4. Режим генерации — **На каждом гипервизоре**.



5. Нажмите на кнопку **Добавить**. Всплывающее окно, в котором выполнялись предыдущие действия, закроется.

На каждом из гипервизоров-хранилищ нужно дополнительно сгенерировать еще по одному контейнеру **xtaz** (они автоматически добавляются по одному на каждый сторадж, теперь для каждого следует добавить пару):

1. В поиске введите **xtaz**.
2. Выберите контейнер с помощью чекбокса.
3. В списке гипервизоров отметьте те, которые были отведены под стораджи.
4. Режим генерации — **На каждом гипервизоре**.
5. Нажмите на кнопку **Добавить**. Всплывающее окно, в котором выполнялись предыдущие действия, закроется.

> **Важно**
>
> Для всех последующих ролей должно быть установлено значение **0** в фильтре **Установлено не более**. Если пропустить этот фильтр, **кластер не соберется**.

Помимо этого на гипервизоры-стораджи необходимо добавить кластер **raft**.

1. Выберите тег **raft**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте **Все** доступные для установки роли.

4. Выберите гипервизоры, отведенные под хранилища.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.

Следующий шаг — распределение ролей для баз данных.

1. Выберите тег **База данных**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте **Все** доступные для установки роли.
4. Ниже выберите гипервизоры, отведенные под базы данных.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.

Чтобы добавить роли для мониторинга, повторно откройте окно выбора ролей.

1. Выберите тег **Мониторинг**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте **Все** доступные для установки роли.
4. Выберите гипервизор-мониторинг.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.

Далее нужно распределить роли для почтового транспорта. Перейдите в окно выбора ролей, нажав **Добавить → Несколько контейнеров**.

1. Выберите тег **Почтовый транспорт**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте **Все** доступные для установки роли.
4. Выберите гипервизоры, отведенные под **фронты**.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.

Завершающий этап — распределить роли для API.

1. Выберите тег **API**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте **Все** доступные для установки роли.
4. Выберите гипервизоры, отведенные под фронты.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.

Финальная проверка для того чтобы убедиться, что все роли распределены:

1. Откройте окно добавления выбора ролей, нажав на **Добавить → Несколько контейнеров**.

2. Для фильтра **Установлено не более:** установите значение **0**.
3. Список ролей, доступных для добавления, должен быть **пустым**. Если это не так, распределите оставшиеся роли по гипевизорам в соответствии с тегами.

После того как все контейнеры сгенерированы, нажмите на зеленую кнопку **Далее** в правом верхнем углу.

9. Хранилища

> **Важно**
>
> **Минимальный размер** раздела диска, используемого под хранилище, составляет **25 GB**.

В разделе формируются дисковые пары для гипервизоров-хранилищ. Разделение на дисковые пары происходит автоматически, если вы **не подключали** дополнительные диски. В таком случае можно переходить в настройке **mescalito**, описанной в следующем шаге.

Ручная настройка дисковых пар требуется в случаях, когда дополнительные диски подключены.

> **Информация**
>
> Под дисковой парой подразумеваются связанные разделы дисков, которые размещены **на двух разных гипервизорах**. Для повышения отказоустойчивости на дисковую пару записываются одни и те же данные.

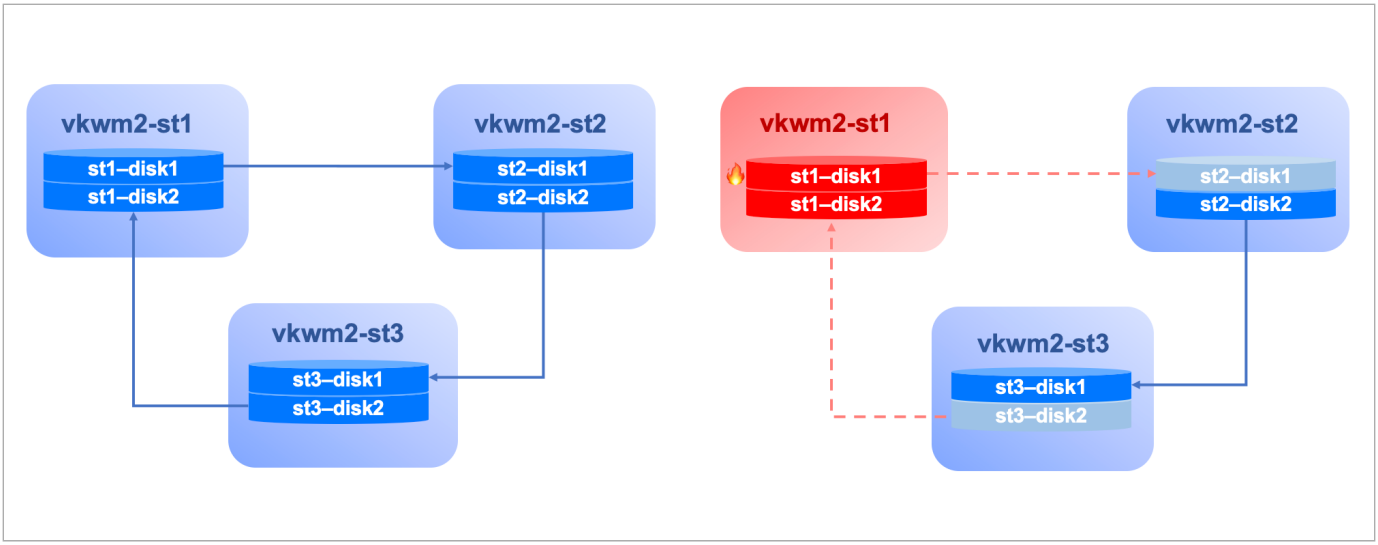
В документе описана процедура **ручного** распределения дисковых пар. При автоматическом формировании дисковых пар настройка не требуется.

Минимальная отказоустойчивая конфигурация: 3 машины, на каждой из которых по 2 дисковых раздела — всего 6 разделов.

При такой конфигурации:

- Всегда есть пара на запись.
- Остальные пары доступны для чтения.

При сборке хранилищ дисковые пары объединяются в «логические треугольники». Объединение происходит по принципу: 1-2, 2-3, 3-1.

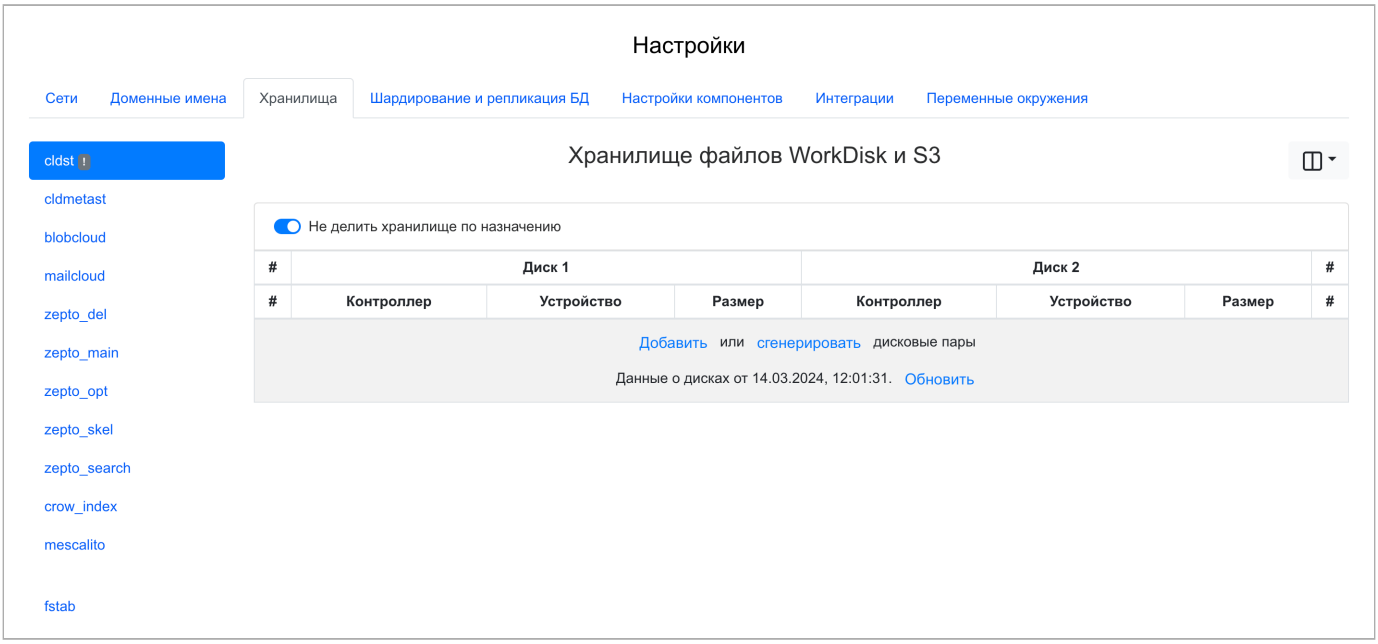


Примечание

vkwm-st – это названия машин-сторажей на тестовом стенде, который рассматривается в качестве примера. **Стрелки** на изображении показывают, какие диски объединены в пару. На правой части изображения демонтрируется ситуация, когда одно из хранилищ вышло из строя.

В списке слева будут отображаться доступные хранилища, отмеченные восклицательными знаками.

Нужно перейти на вкладку каждого хранилища и сформировать дисковые пары.



В минимальной конфигурации, где к каждому из трех гипервизоров-хранилищ подключено по диску, которые, в свою очередь, разделены на 2 части мы имеем:

- Диск хранилища 1 разделен на 2 части.
- Диск хранилища 2 разделен на 2 части.
- Диск хранилища 3 разделен на 2 части.

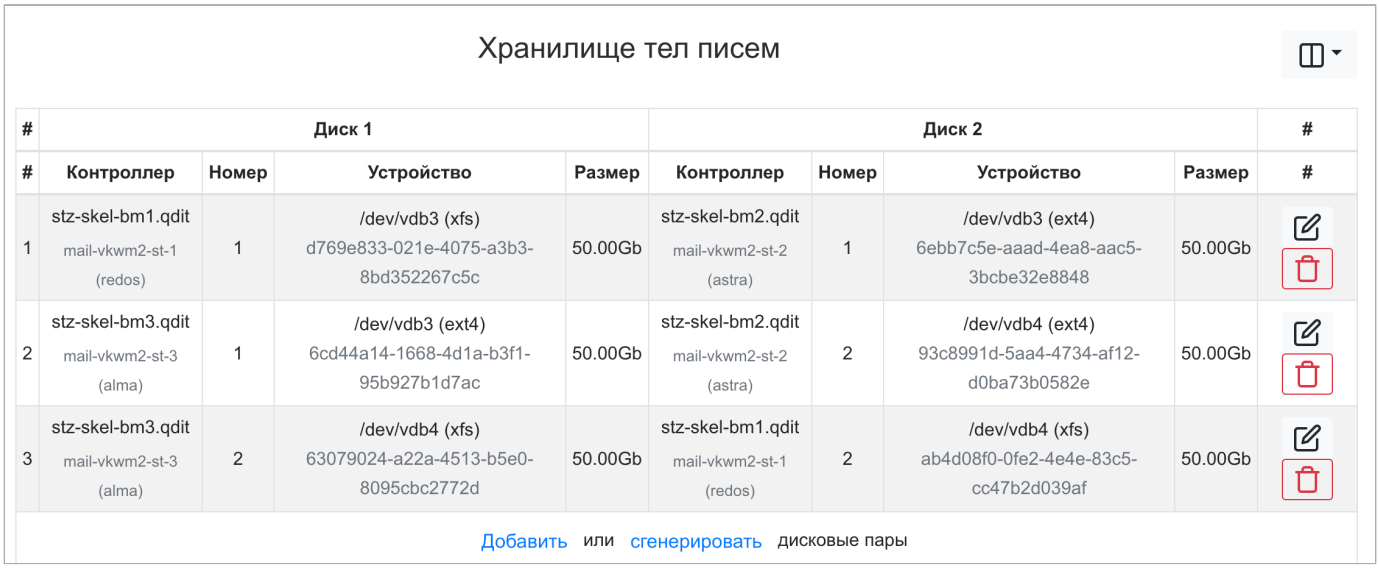
Всего 6 разделов дисков (2 на одном гипервизоре, 2 — на втором, еще 2 — на третьем).

Важно

В интерфейсе под Диском 1 и Диском 2 подразумеваются **разделы** хранилищ. Между собой также нужно будет объединить часть диска, размещенного на **одном хранилище**, с частью диска, размещенного на **другом хранилище**. При увеличении количества разделов дисков и/или подключенных дисков принцип объединения сохраняется.

1. Нажмите на кнопку **Добавить**.
2. В выпадающем меню выберите контроллер и устройство для Диска 1 первой пары.
3. Выберите контроллер и устройство для Диска 2 первой пары.
4. Повторите шаги 2-3 еще для двух пар.

На изображении ниже приведен пример для хранилища **zepto_skel**:

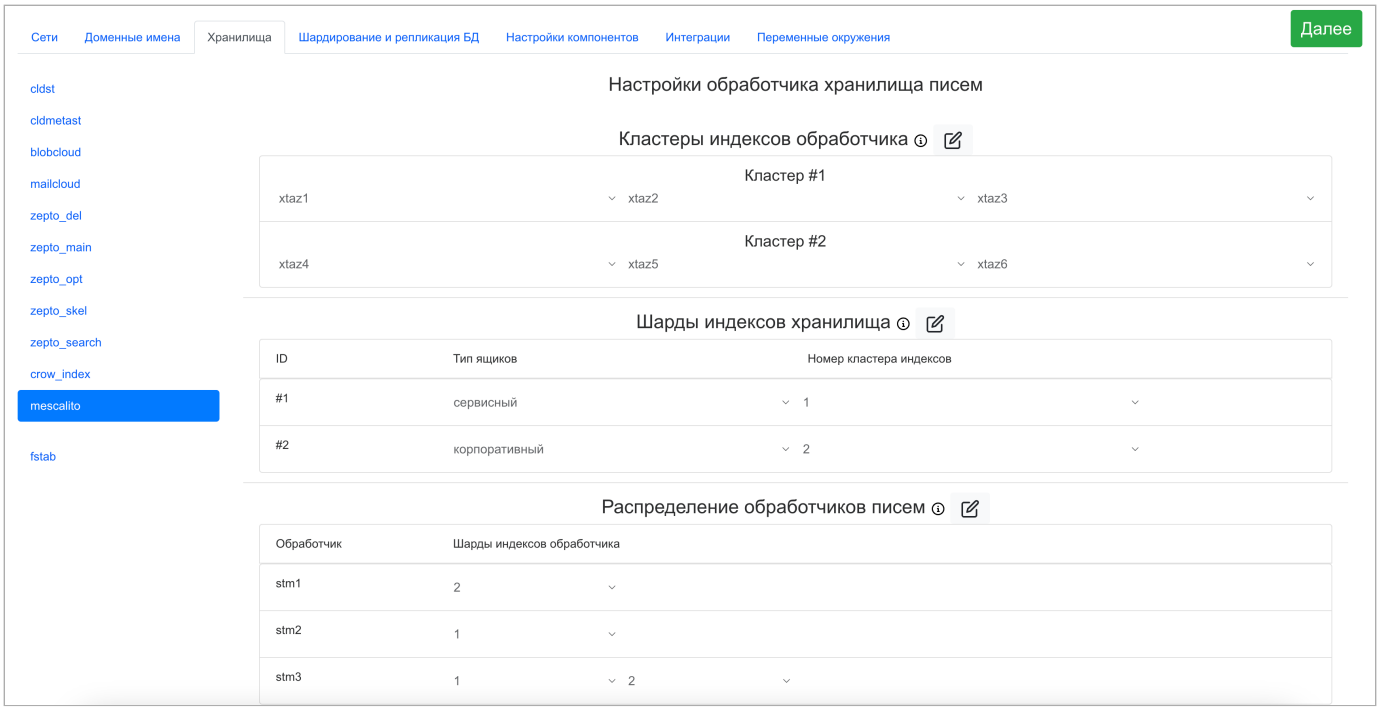


#	Диск 1				Диск 2				#
#	Контроллер	Номер	Устройство	Размер	Контроллер	Номер	Устройство	Размер	#
1	stz-skel-bm1.qdit mail-vkwm2-st-1 (redos)	1	/dev/vdb3 (xfs) d769e833-021e-4075-a3b3-8bd352267c5c	50.00Gb	stz-skel-bm2.qdit mail-vkwm2-st-2 (astra)	1	/dev/vdb3 (ext4) 6ebb7c5e-aaad-4ea8-aac5-3bcbe32e8848	50.00Gb	
2	stz-skel-bm3.qdit mail-vkwm2-st-3 (alma)	1	/dev/vdb3 (ext4) 6cd44a14-1668-4d1a-b3f1-95b927b1d7ac	50.00Gb	stz-skel-bm2.qdit mail-vkwm2-st-2 (astra)	2	/dev/vdb4 (ext4) 93c8991d-5aa4-4734-af12-d0ba73b0582e	50.00Gb	
3	stz-skel-bm3.qdit mail-vkwm2-st-3 (alma)	2	/dev/vdb4 (xfs) 63079024-a22a-4513-b5e0-8095cbc2772d	50.00Gb	stz-skel-bm1.qdit mail-vkwm2-st-1 (redos)	2	/dev/vdb4 (xfs) ab4d08f0-0fe2-4e4e-83c5-cc47b2d039af	50.00Gb	

9.1 Раздел mescalito

В разделе задаются настройки обработчика хранилища писем.

Если на этапе распределения ролей вы добавили по одному контейнеру xtaz и число пользователей вашей системы не будет превышать 100 тысяч человек, можно сразу переходить к настройке fstab.



Индекс обработчика писем (tarantool xtaz) хранит информацию о последних действиях пользователей в их почтовых ящиках (горячий кэш).

Для обеспечения отказоустойчивости формируются кластеры (шарды) обработчиков писем. Почтовые ящики могут обслуживаться разными кластерами таких баз данных в целях масштабирования. Если заканчивается память в одном кластере, добавляется еще один.

> **Информация**
>
> Появление ошибки `failed to allocate X bytes` (или ошибок с подобной формулировкой) при проверке системных логов контейнеров xtaz свидетельствует о недостатке памяти.

Шарды индексов хранилища — распределите типы почтовых ящиков по шардам. Шард индексов обработчика — альтернативное название кластера индексов обработчика.

Существует несколько типов ящиков:

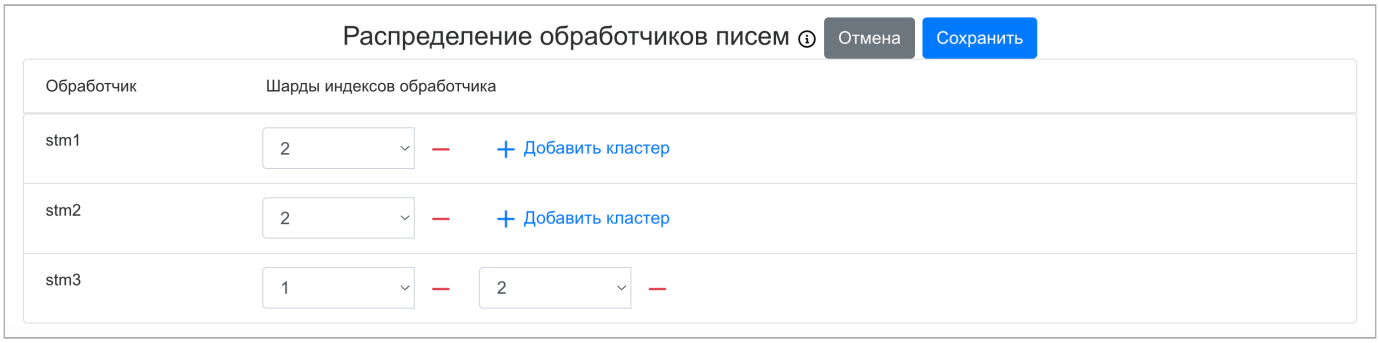
- Сервисный — admin@admin.qdit (администраторы почты).
- Собираемый (**не используется**) — внешние ящики, работа с которыми происходит через наш интерфейс. Распределять этот тип не нужно.
- Корпоративный — все остальные ящики системы, которые администрируются в `biz.<почтовый домен>`.

> **Примечание**
>
> Не рекомендуется назначать более одного типа ящиков на один шард. Если в вашей ситуации невозможно избежать добавления двух типов ящиков на один шард, обратитесь к представителю VK.

Распределение обработчиков писем — каждому шарду необходимо присвоить обработчик писем.

Обработчики писем (mescalito) запускаются в контейнерах **stm**. Их задача — собирать письма из частей, находящихся в разных хранилищах.

По умолчанию нагрузка от кластеров xtaz будет распределяться на тот обработчик, у которого этот кластер первый в списке.



На изображении выше представлен такой порядок распределения по обработчикам:

- **stm1** в первую очередь будет обрабатывать данные, хранящиеся в Кластере №2, который в этом примере соответствует корпоративному типу ящиков.
- **stm2** будет также обрабатывать данные Кластера №2, потому что первым в списке указан именно он.
- **stm3** будет обрабатывать данные, хранящиеся в Кластере №1.

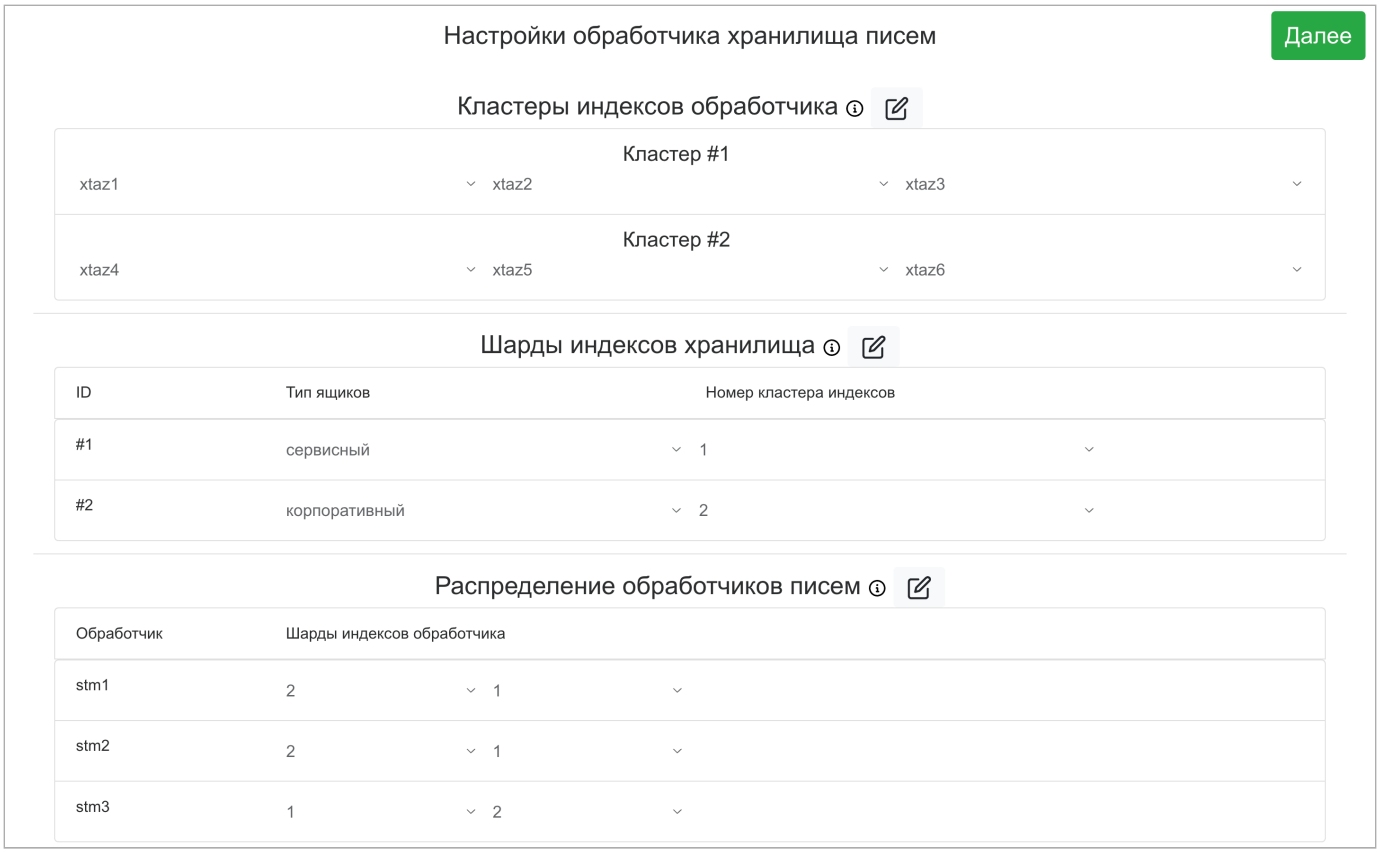
> **Важно**
>
> Обработчики работают в однопоточном режиме. Перенаправление информации на другой обработчик будет производиться только в случае недоступности хранилища, на котором установлен соответствующий stm.

Для обеспечения отказоустойчивости для каждого шарда необходимо назначать по 2-3 обработчика, находящихся на разных машинах или в разных дата-центрах.

> **Информация**
>
> Контейнеры stm устанавливаются на каждый гипервизор-сторадж, поэтому количество обработчиков равно количеству машин, отведенных под хранилища. При необходимости могут быть сгенерированы дополнительные контейнеры stm вручную.

Пример настройки mescalito:

- 6 контейнеров tarantool xtaz.
- 2 кластера индексов обработчика.
- На одном шарде (кластере) хранятся данные сервисного типа ящиков, на втором — корпоративного.
- Каждый шард обрабатывается 3-мя обработчиками.



9.2 fstab

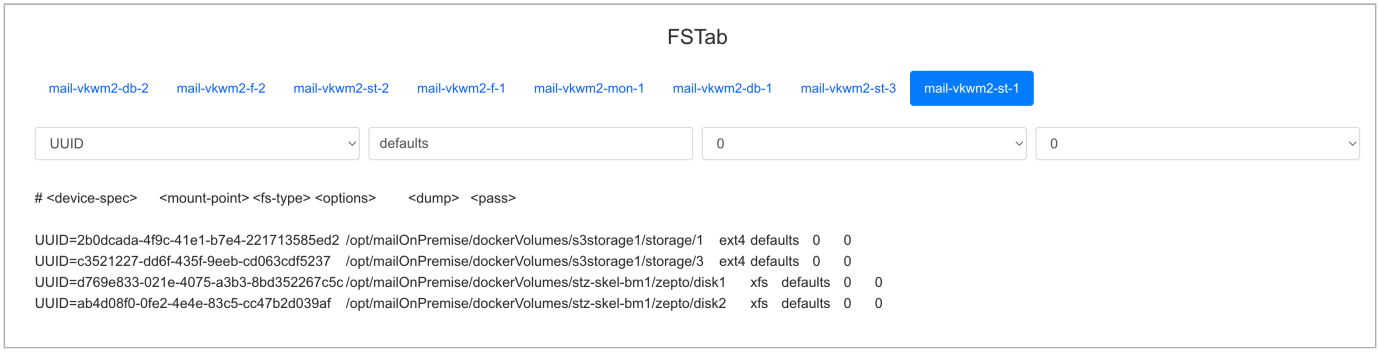
Раздел акуален для ситуаций, когда были подключены дополнительные диски.

Необходимый набор томов для контейнеров хранилища выдается в виде набора записей для `/etc/fstab`.

> **Важно**
>
> Установщик ничего не монтирует и не изменяет в `/etc/fstab`.

Отредактировать fstab и смонтировать разделы нужно самостоятельно в консоли. Монтировать рекомендуется по UUID.

Ниже для примера приведен скриншот с одного из наших тестовых стендов.



Пример команд для монтирования разделов:

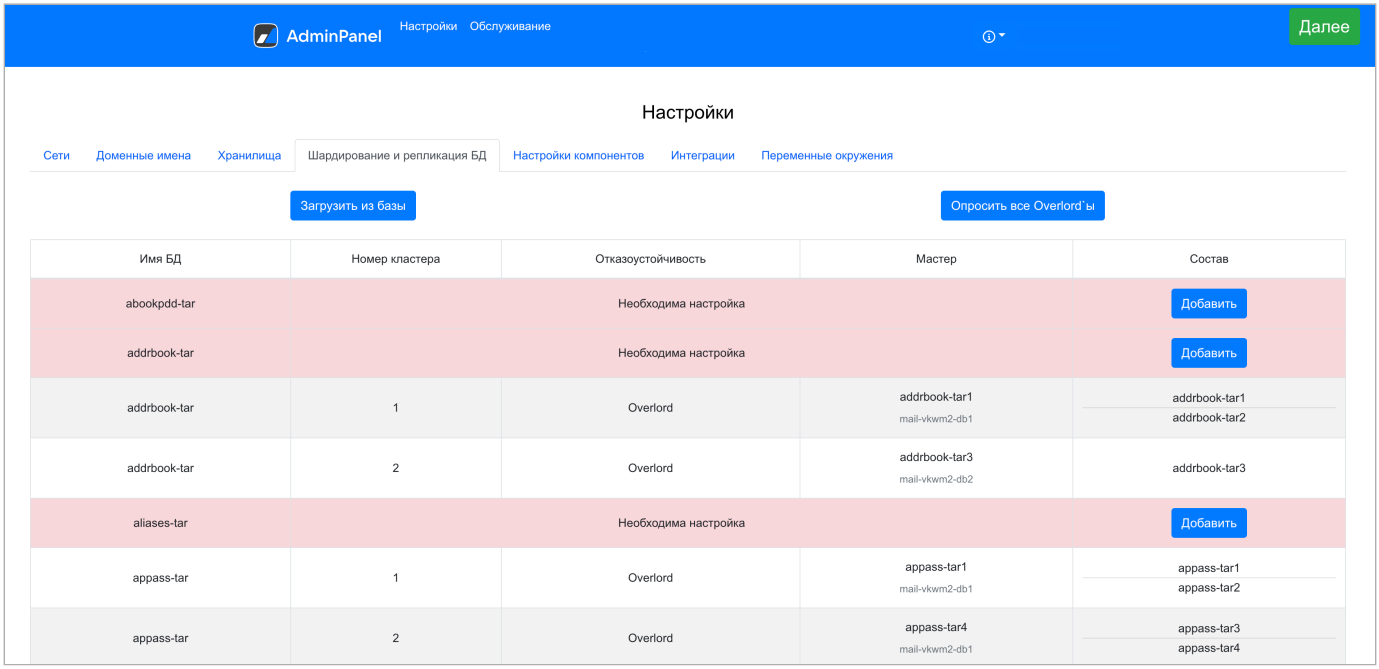
```
vi /etc/fstab

# Вставляем строчки, скопированные из веб-интерфейса установщика.
# Сохраняем изменения.

mount -a

# Получаем набор предупреждений <путь> mount point does not exist

mkdir -p <путь>

# Повторяем для всех путей

mount -a
```

10. Шардирование и репликация БД

Настройка в этом разделе актуальна только для очень крупных инсталляций. В большинстве случаев достаточно настроек по умолчанию, и можно перейти к следующему шагу с помощью кнопки **Далее**.

> **Важно**
>
> Добавлять кластеры БД можно только на этапе **первоначальной** установки!

Чтобы добавить более одного кластера, потребуется сгенерировать дополнительные контейнеры.

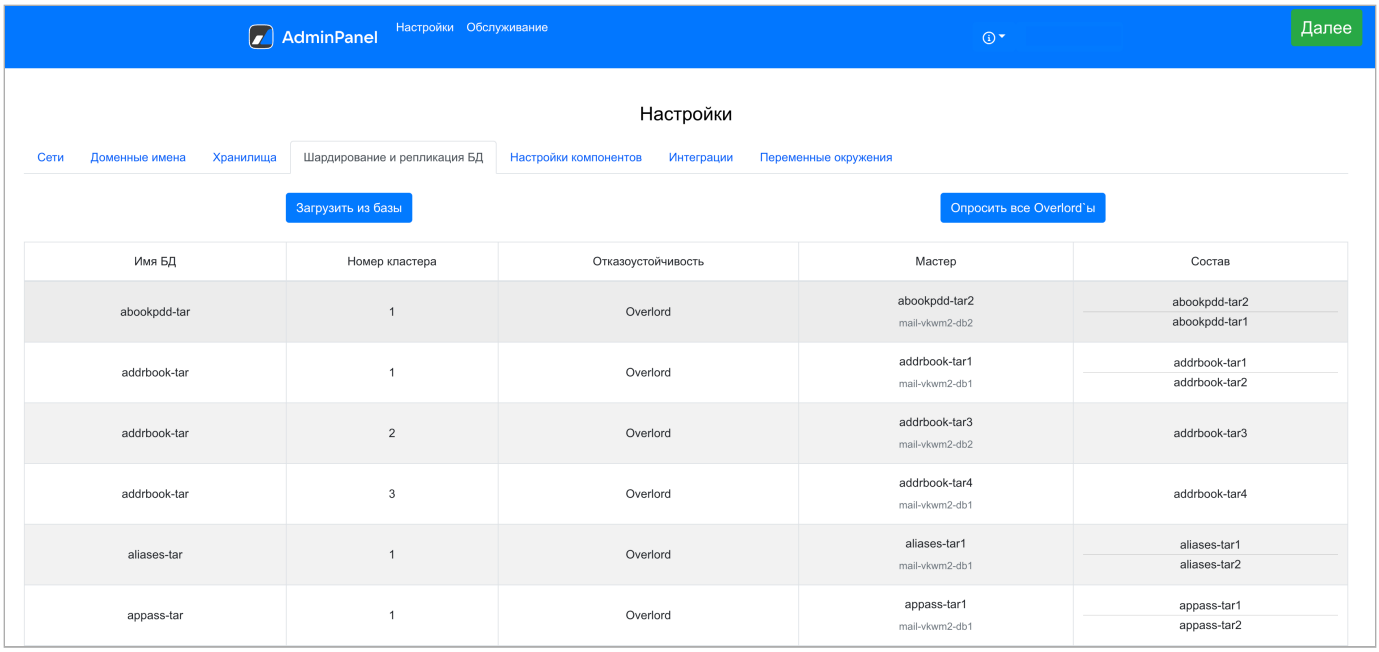


Последовательность действий для добавления кластеров:

1. Нажмите кнопку **Добавить** в первой строке, отмеченной красным.
2. Добавьте контейнеры БД (кнопка **Добавить контейнер БД**). В зависимости от типа базы данных может быть добавлен как один контейнер, так и два.
3. Сохраните изменения.

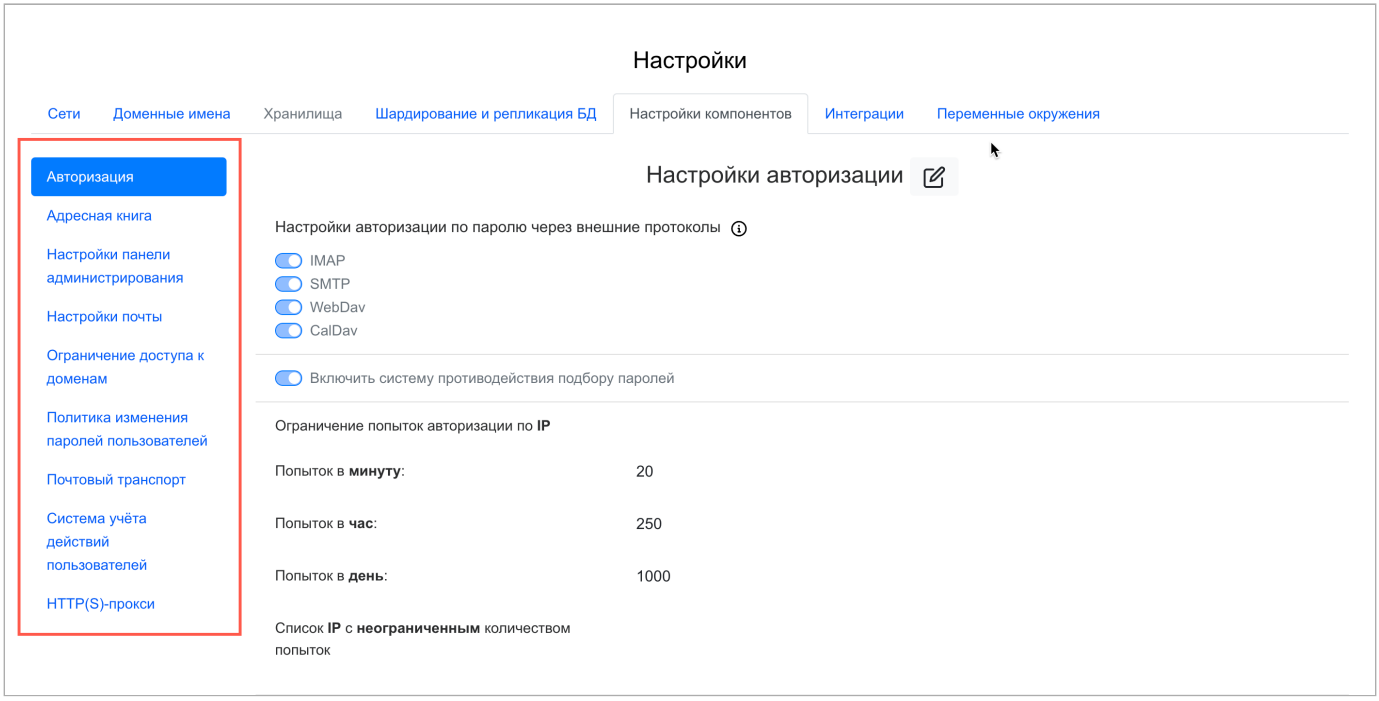
4. Повторите шаги 1-4 для каждой строки, отмеченной красным.

После добавления всех кластеров появится возможность перейти к следующему шагу с помощью кнопки **Далее**.



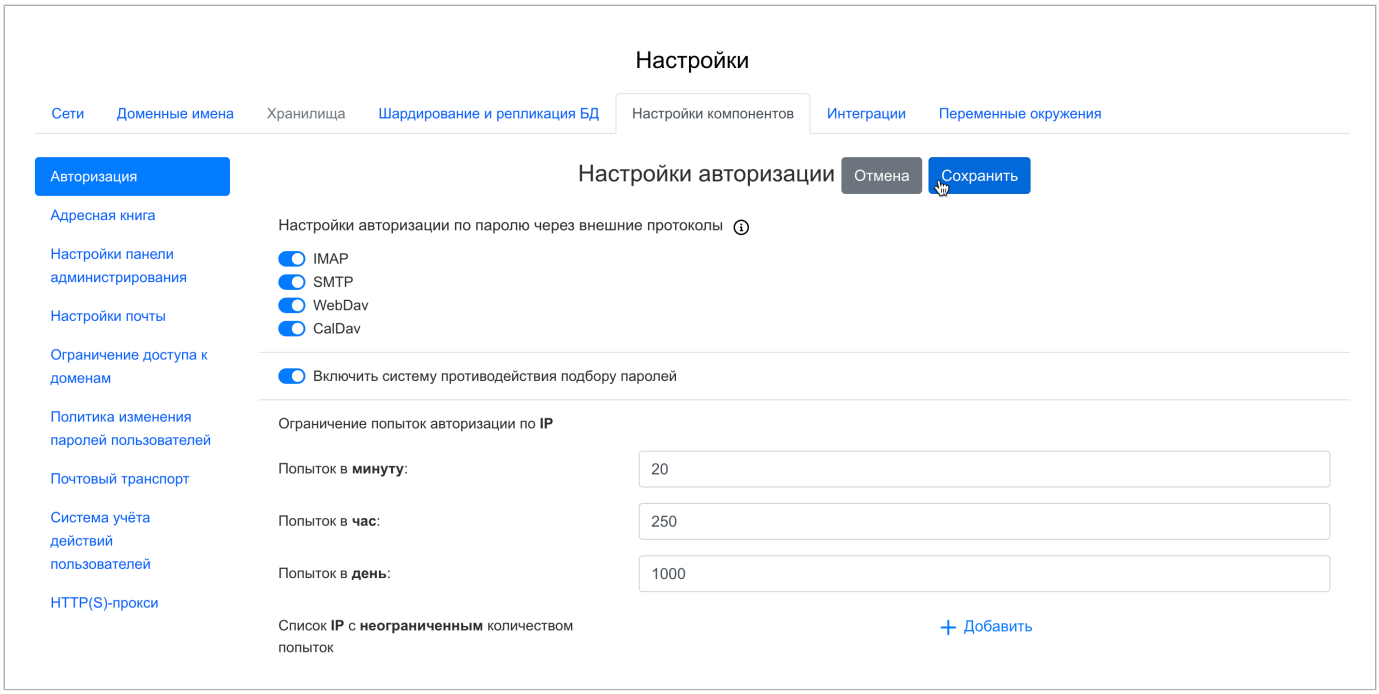
11. Настройки компонентов

В разделе выполняются настройки различных компонентов почтовой системы.



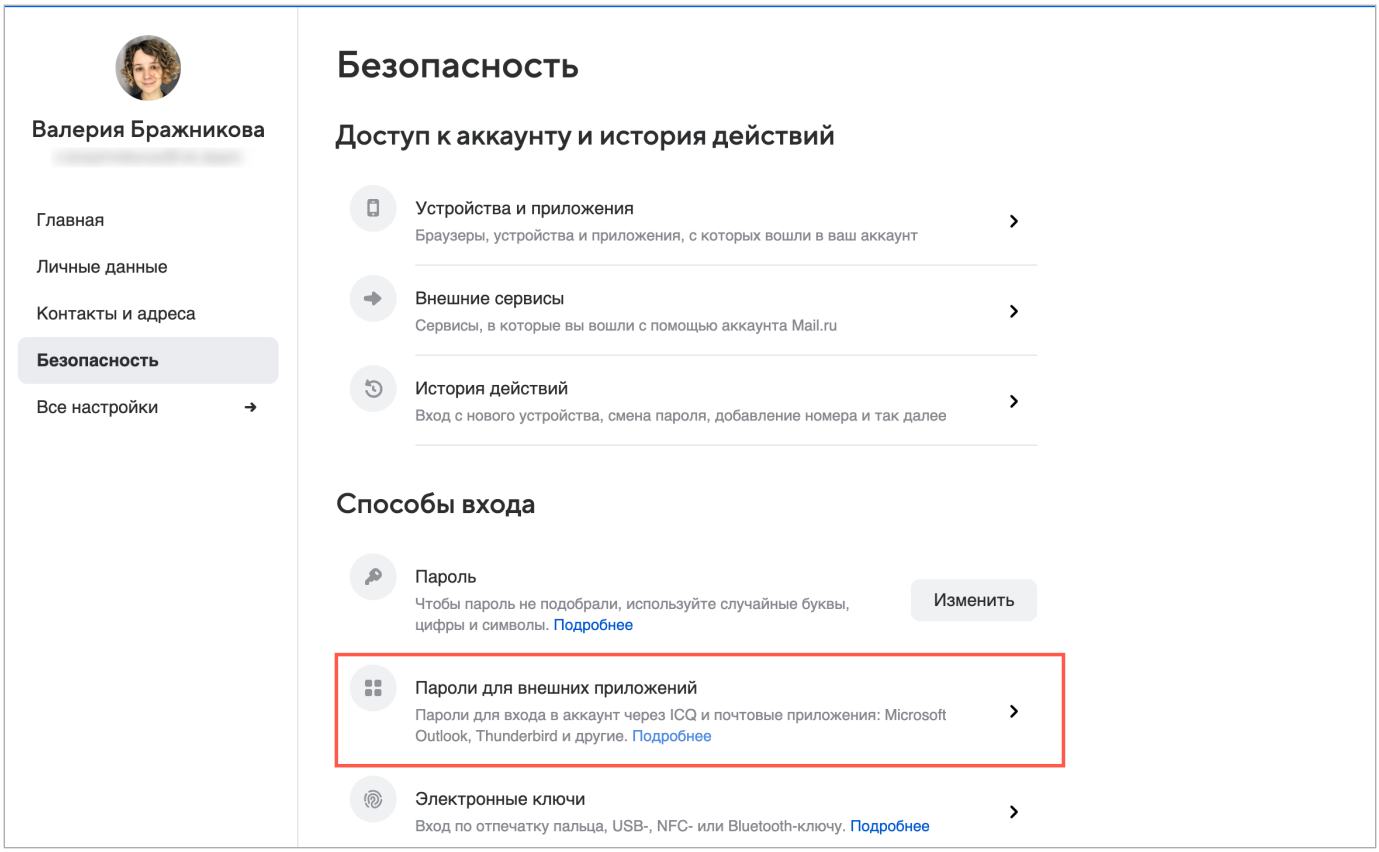
Авторизация

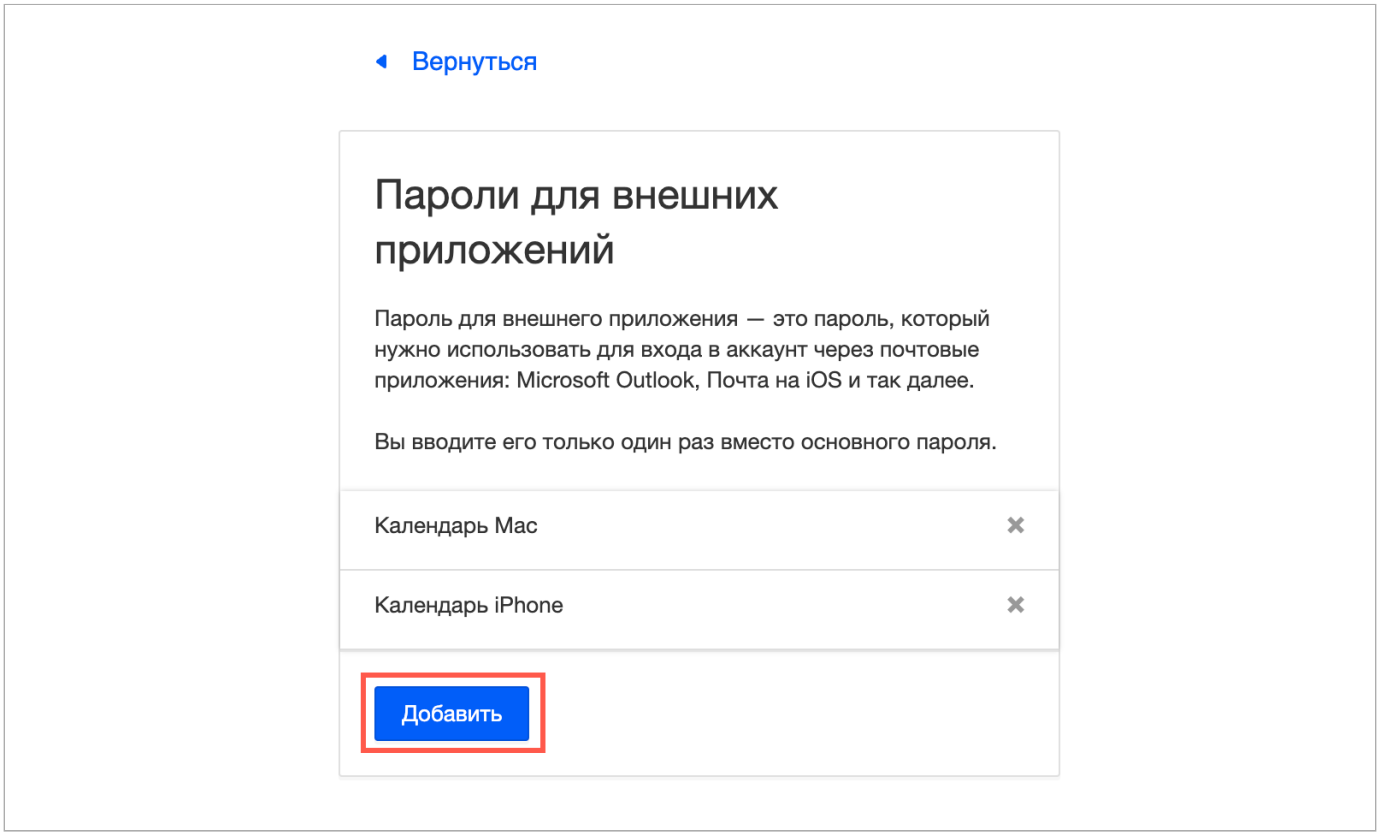
В разделе есть возможность настроить защиту от подбора паролей. Для этого нажмите на кнопку редактирования.



Настройки авторизации по паролю через внешние протоколы — позволяет запретить пользователям авторизовываться во внешних приложениях (MS Outlook, Почта/Календарь на iOS и т.п.) с помощью основного пароля почты.

Если флаг одного или нескольких протоколов включен, для авторизации по этим протоколам пользователю потребуется не пароль от почты , а **одноразовый пароль**, сформированный в разделе **Настройки** → **Безопасность** аккаунта VK WorkMail.





По кнопке **Добавить** пользователю нужно будет ввести название внешнего приложения, для которого нужно сгенерировать пароль, ввести пароль основной пароль аккаунта.

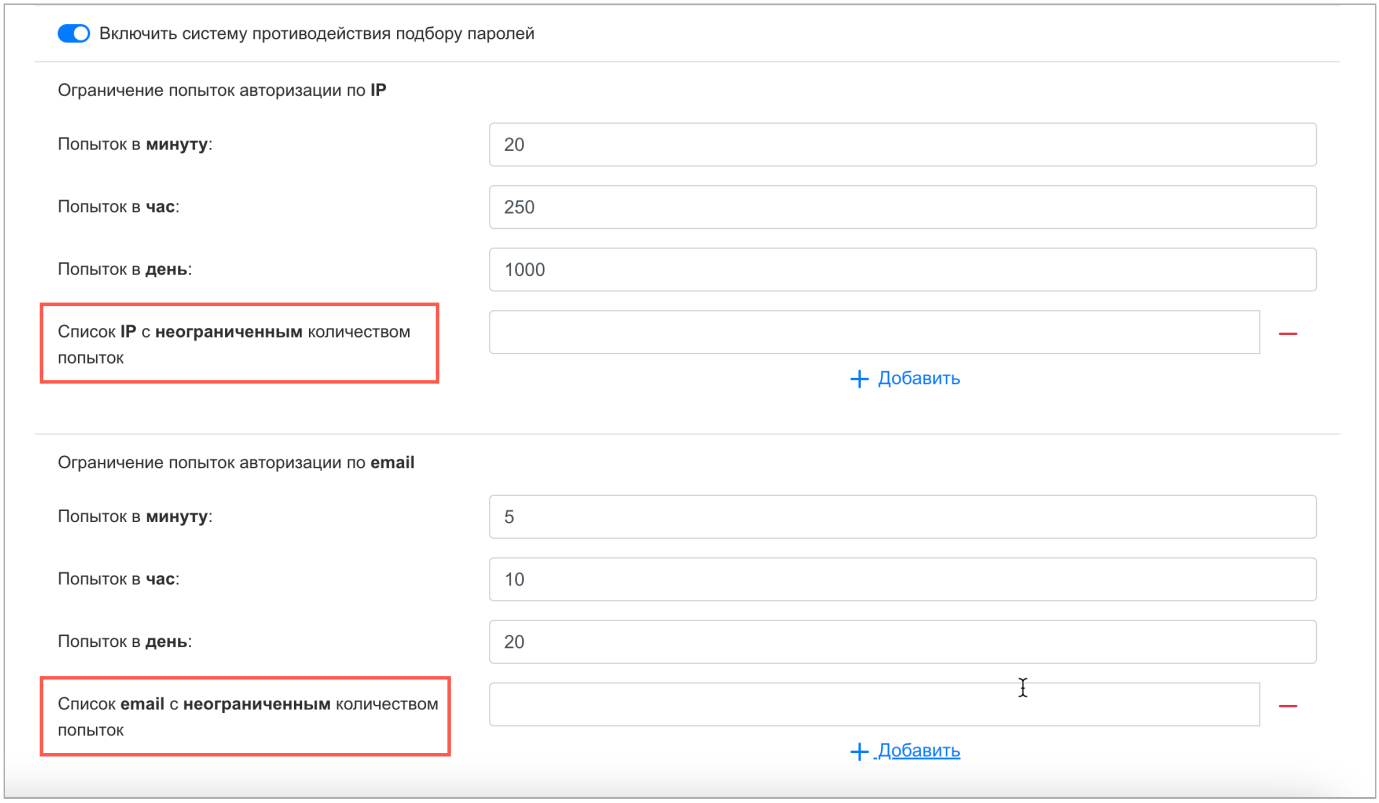
После чего нужно будет скопировать сгенерированный код и ввести его во внешнее приложение **при первом входе** под учетной записью VK WorkMail.

Если флаг протокола **выключен**, для входа во внешнее приложение достаточно будет ввести пароль аккаунта VK WorkMail.

Примечание

Для получения информации о принципе работы системы ограничения SSO-авторизации по IP/группе в ActiveDirectory обратитесь к представителю VK.

Также в разделе вы можете ограничить количество попыток входа в VK WorkMail по IP и по адресу электронной почты и добавить IP и/или адреса в белый список.



Адресная книга

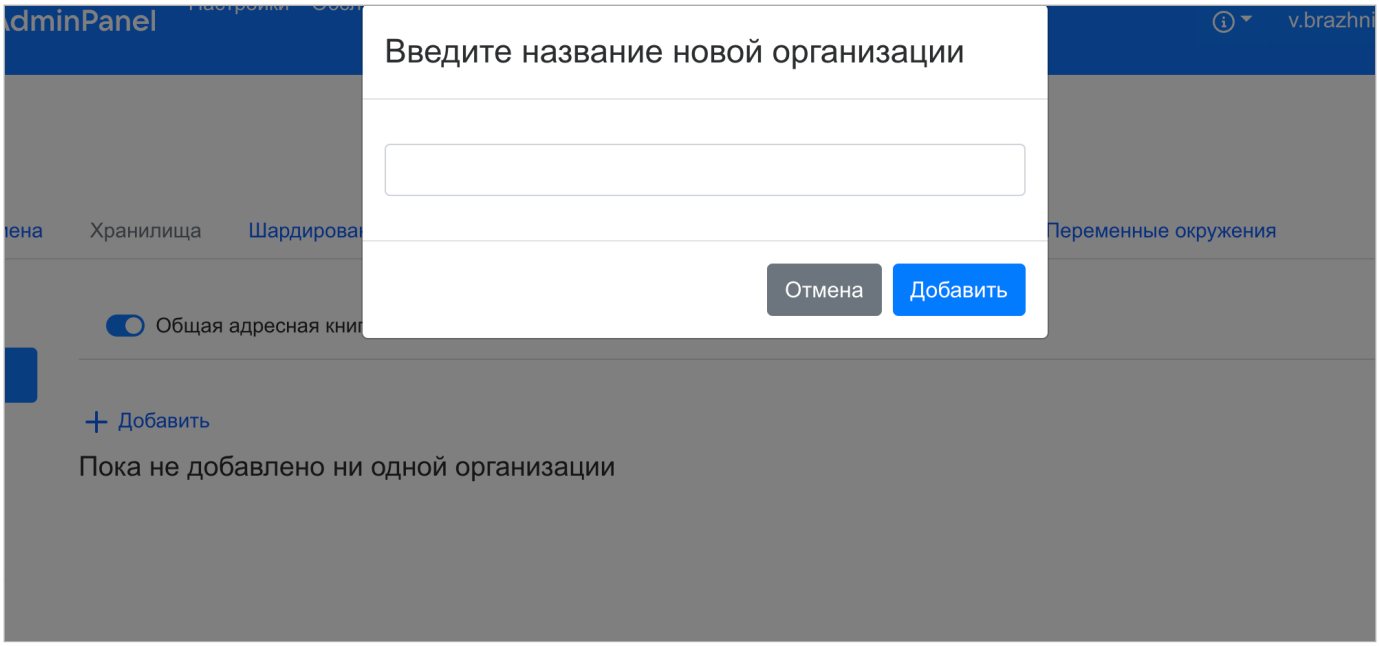
Для случаев, когда необходимо создать общие почтовые ящики для адресов из разных доменов, включите флаг **Общая адресная книга для всех доменов**.

Информация

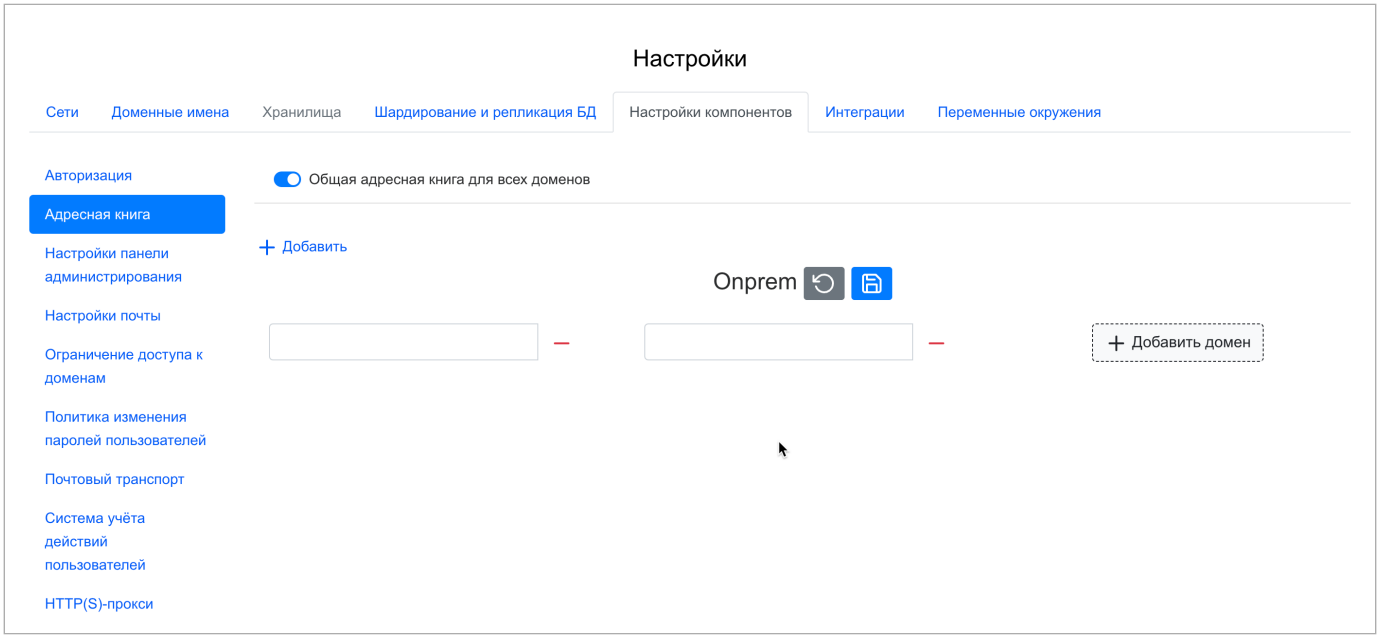
Дальнейшая настройка общих почтовых ящиков производится в административной панели (`biz.<почтовый домен>`).

Чтобы создать организацию, под которой будут объединены домены, кликните по кнопке **Добавить**.

Появится всплывающее окно, куда нужно ввести название организации.



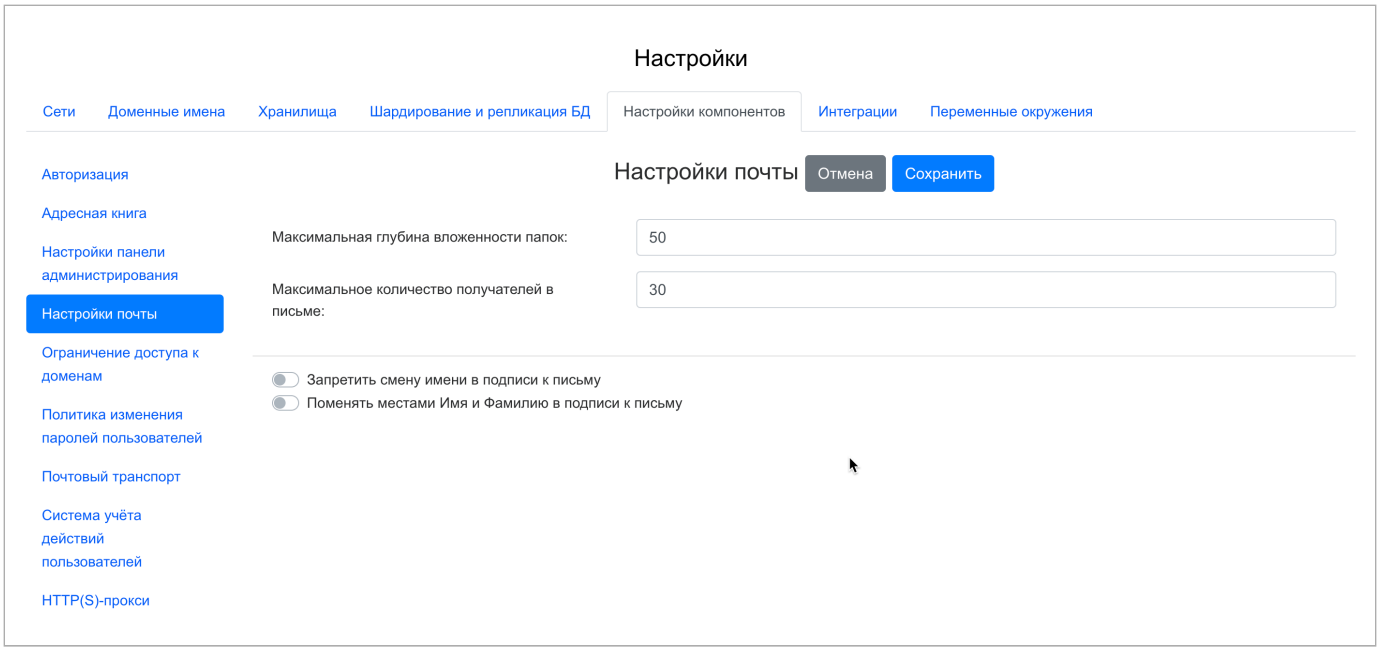
С помощью кнопки **Добавить домен** введите адреса доменов, относящихся к одной организации.



Также есть возможность изменить названия организаций, добавить дополнительные домены и удалить домены/организации. После создания организаций перейдите к списку машин, чтобы повторить нужные шаги.

Настройки почты

Для изменения настроек в разделе нажмите на кнопку редактирования.



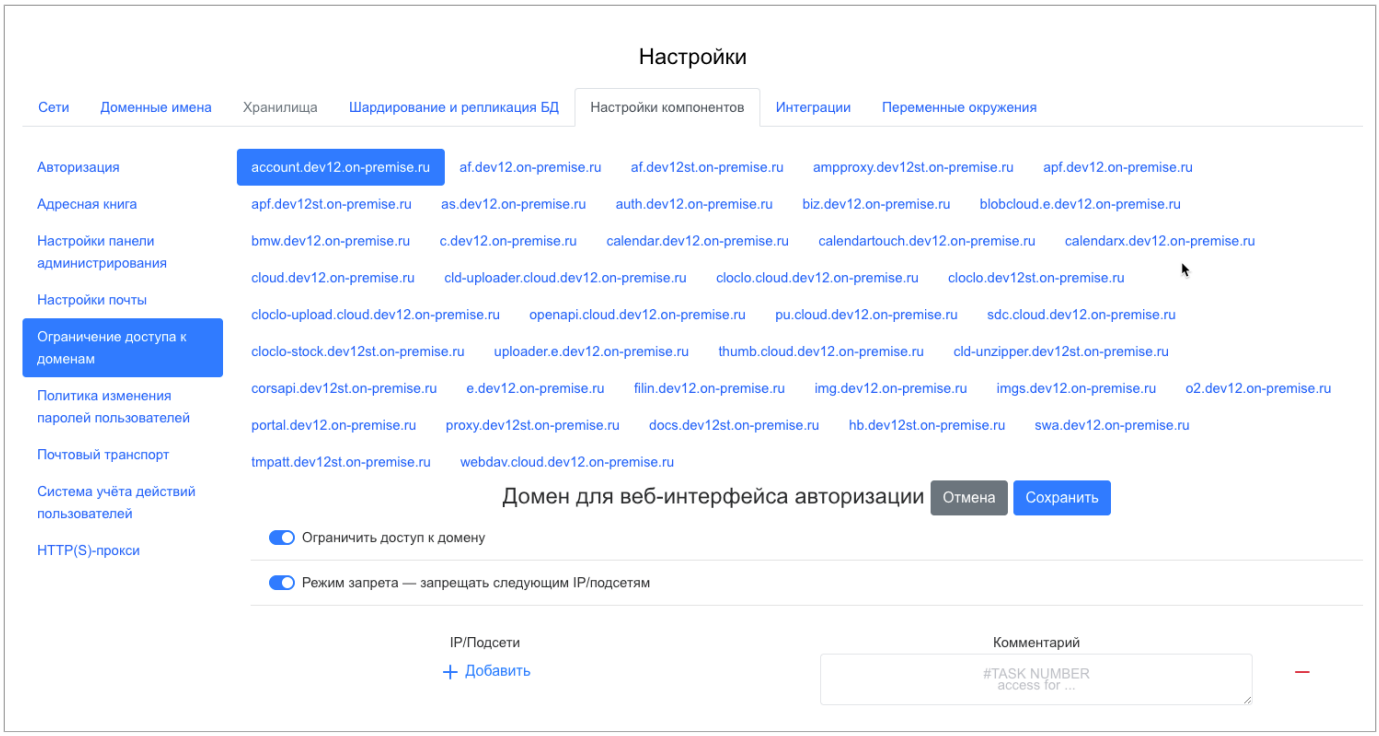
Максимальная глубина вложенности папок — вы можете изменить разрешенную глубину вложенности папок, создаваемых пользователями в своих почтовых ящиках. Значение этого поля также используется при миграции. Если глубина вложенности в исходной системе больше установленного значения, папки будут переноситься в папку с крайней допустимой глубиной.

Максимальное количество получателей в письме — можно ограничить количество пользователей, которым письмо будет отправлено единовременно. Значение по умолчанию — 30 получателей, но, если вы хотите изменить их количество, минимальное значение — 100.

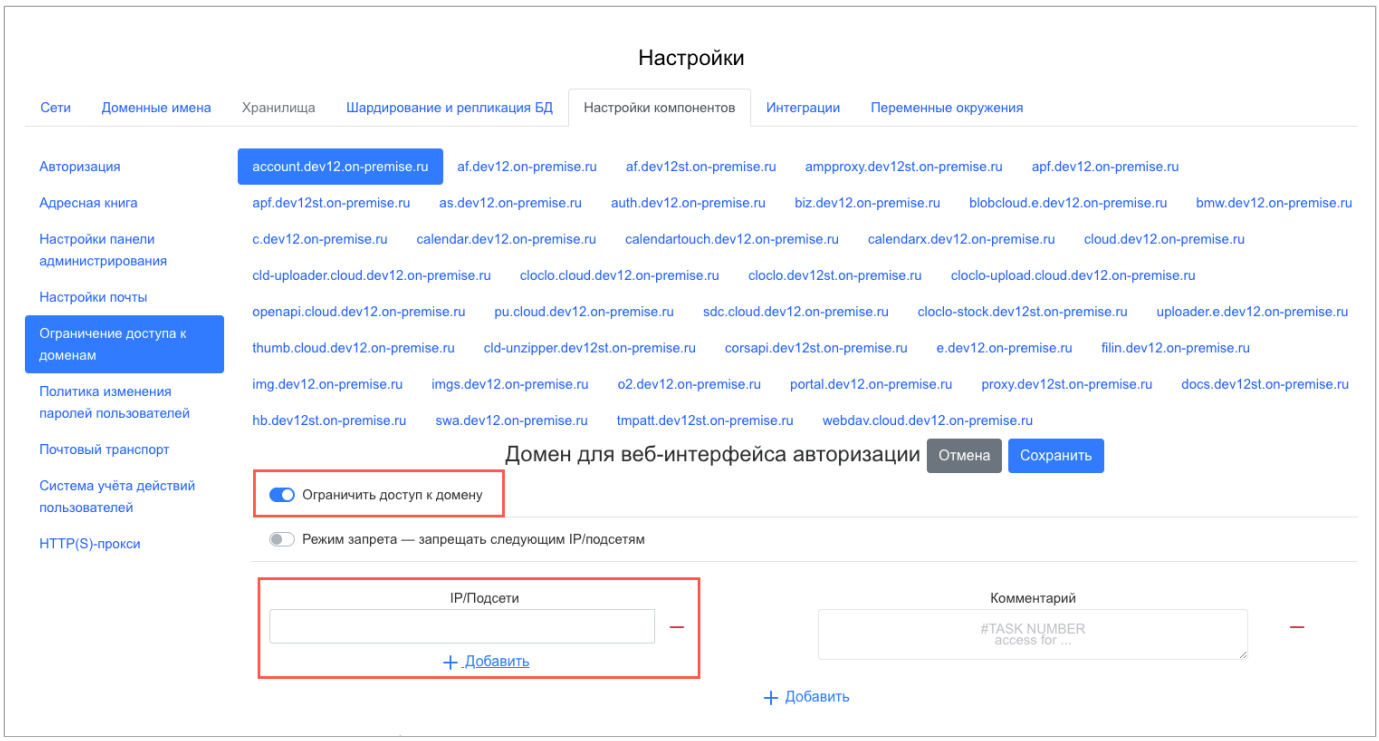
Если необходимо запретить в подписи смену имени или поменять местами имя и фамилию, включите соответствующие флаги.

Ограничение доступа к доменам

Выберите нужный домен и нажмите на кнопку редактирования. После включения флага **Ограничить доступ к домену** появится раздел с более детальными настройками.



Ограничить доступ к домену — если включен только этот флаг, в поле ниже нужно будет ввести IP/подсети, которым будет **разрешен** доступ к домену. Также вы можете добавить комментарии, если это необходимо.



Режим запрета — запрещать следующим IP/подсетям — если включены оба флага (ограничение доступа и режим запрета), доступ к доменам будет **запрещен** IP/подсетям, введенным в поле.

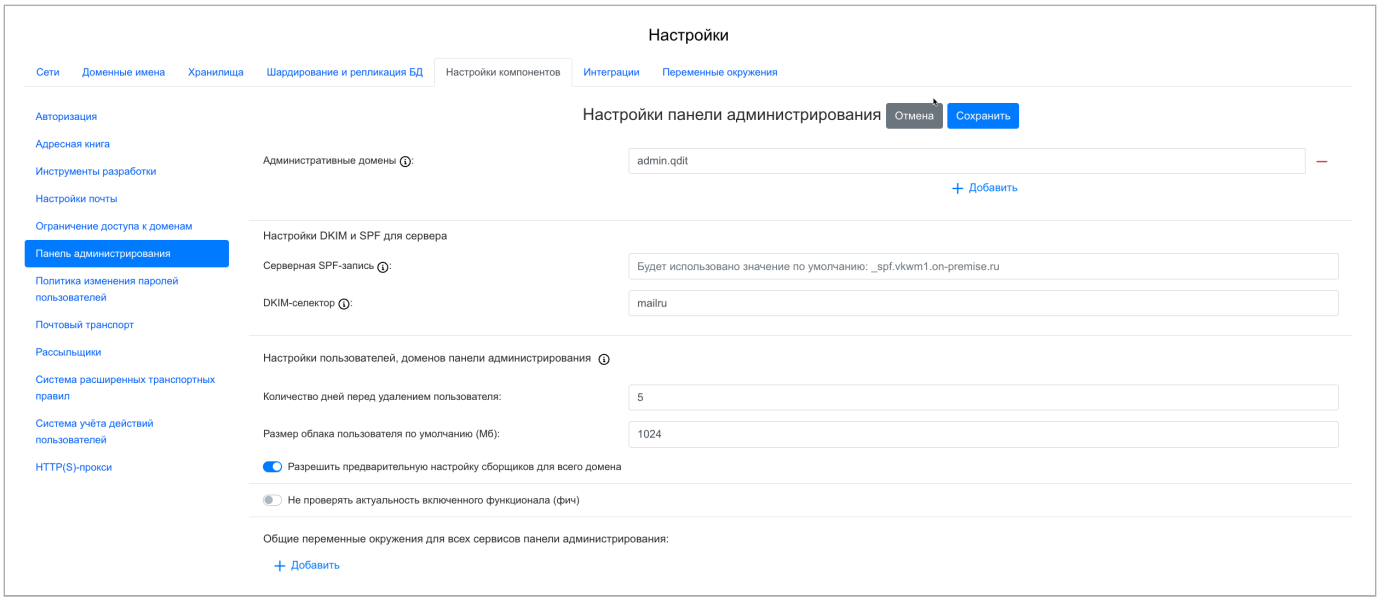
Не забудьте повторить шаги на гипервизоре (нужные шаги уже отмечены желтым). Также можно нажать на кнопку **Play** в общей строке состояния. Для этого перейдите к списку шагов, кликнув по логотипу **AdminPanel**.

Важно

Для доменов `becca.***.***.***` и `bmw.***.***.***` по умолчанию **запрещен** доступ всем IP/подсетям. Чтобы добавить какие-либо IP/подсети в белый список, необходимо **включить** опцию **Ограничить доступ к домену** и добавить в поле IP/подсети. Если включить оба флага, IP/подсети, которые были введены в поле, попадут в черный список.

Панель администрирования

Внутри раздела нужно ввести SPF-запись и DKIM-селектор почтового домена. Так же есть возможность произвести некоторые настройки для административной панели (`biz.<почтовый домен>`). Чтобы начать настройку, нажмите кнопку редактирования .



Административные домены — с помощью кнопки **Добавить** по одному введите домены (до знака @), которым нужно выдать максимальные права.

Серверная SPF-запись — введите в поле SFP почтового домена.

Примечание

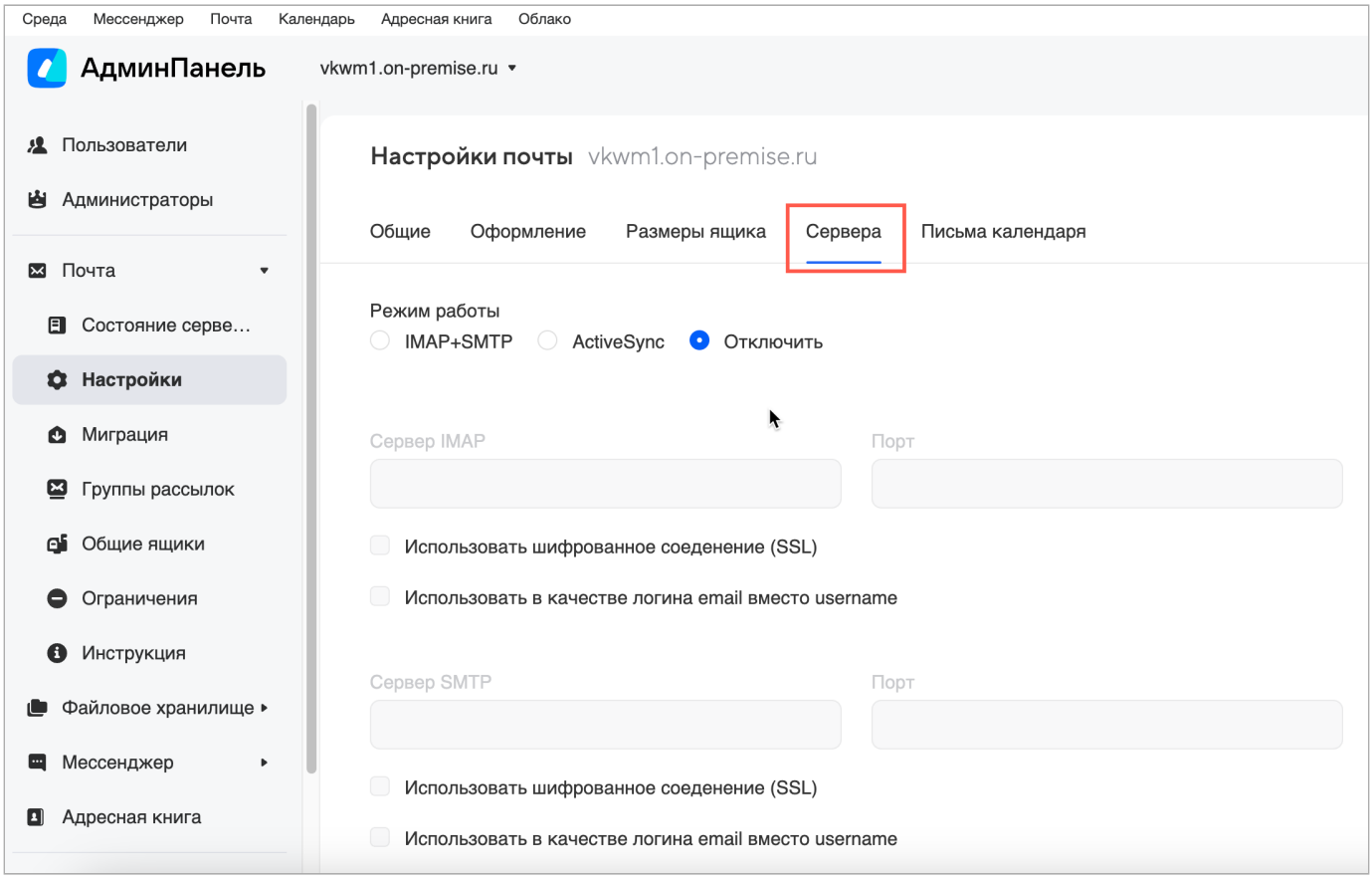
Если оставить поле пустым, будет использована SPF-запись по умолчанию: `v=spf1 a:<почтовый домен> mx -all` .

DKIM-селектор — в поле нужно добавить селектор DKIM-подписи почтового домена.

Количество дней перед удалением пользователя — количество дней, по прошествии которых пользователь будет удален из VK WorkMail. Изменение настройки по умолчанию актуально при одновременном использовании VK WorkMail с Active directory. По умолчанию выставлен срок 5 дней, то есть, пользователь будет удалён из VK WorkMail через 5 дней после его удаления из AD.

Размер облака пользователя по умолчанию (Мб) — при необходимости ограничьте максимальный размер облака для каждого пользователя.

Разрешить предварительную настройку сборщиков для всего домена — включите флаг, если необходимо отобразить окно настроек сборщиков писем в административной панели `biz.<почтовый домен>/domains/`.



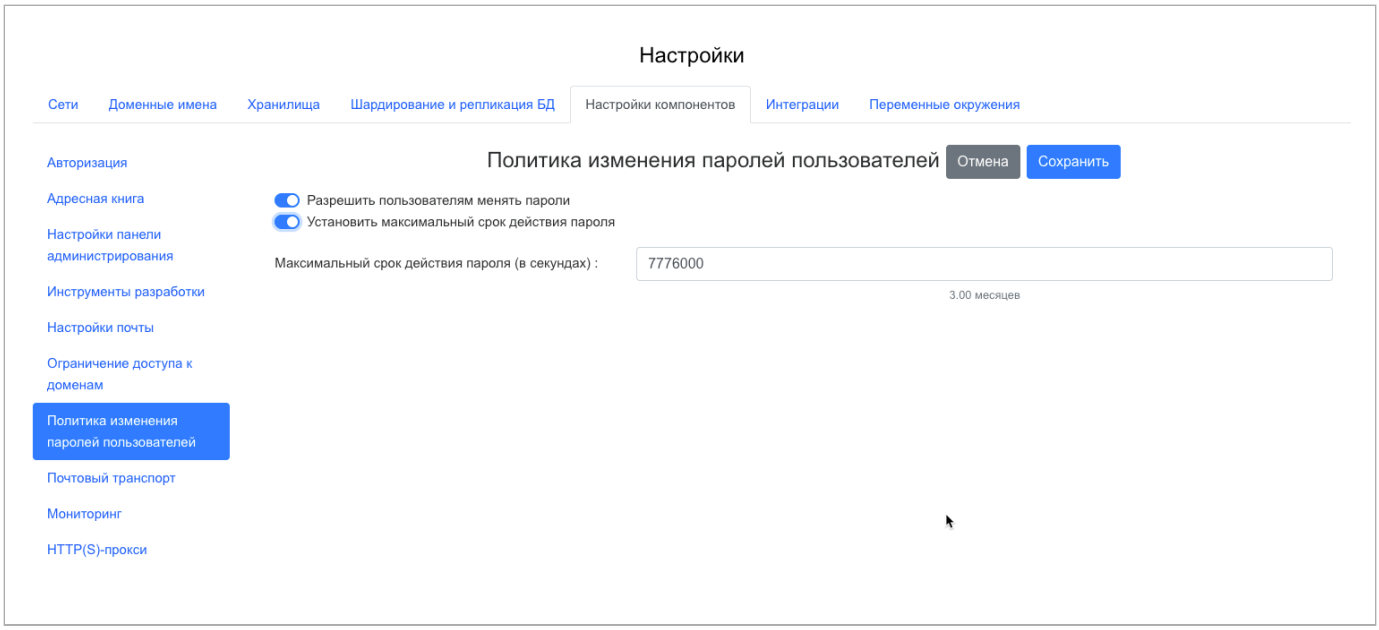
Не проверять актуальность включенного функционала (фич) — при включенном флаге установщик будет пропускать шаг `bizf` → `addBizFeatures`.

Общие переменные окружения для всех сервисов панели администрирования — с помощью кнопки **Добавить** вы можете ввести имя и значение переменных, которые применятся к ролям `bizf`, `biz-celery-worker-*` и `biz-celery-beat`. Вам не нужно будет каждый раз отдельно для всех ролей прописывать переменные, достаточно добавить их в общие переменные окружения.

Политика изменения паролей пользователей

> **Информация**
>
> При интеграции с Active Directory эта вкладка **неактуальна**. С включенной интеграцией пользователи, заведенные внутри VK WorkMail, не смогут совершать никаких действий.

Для изменения настроек во вкладке кликните по кнопке редактирования .

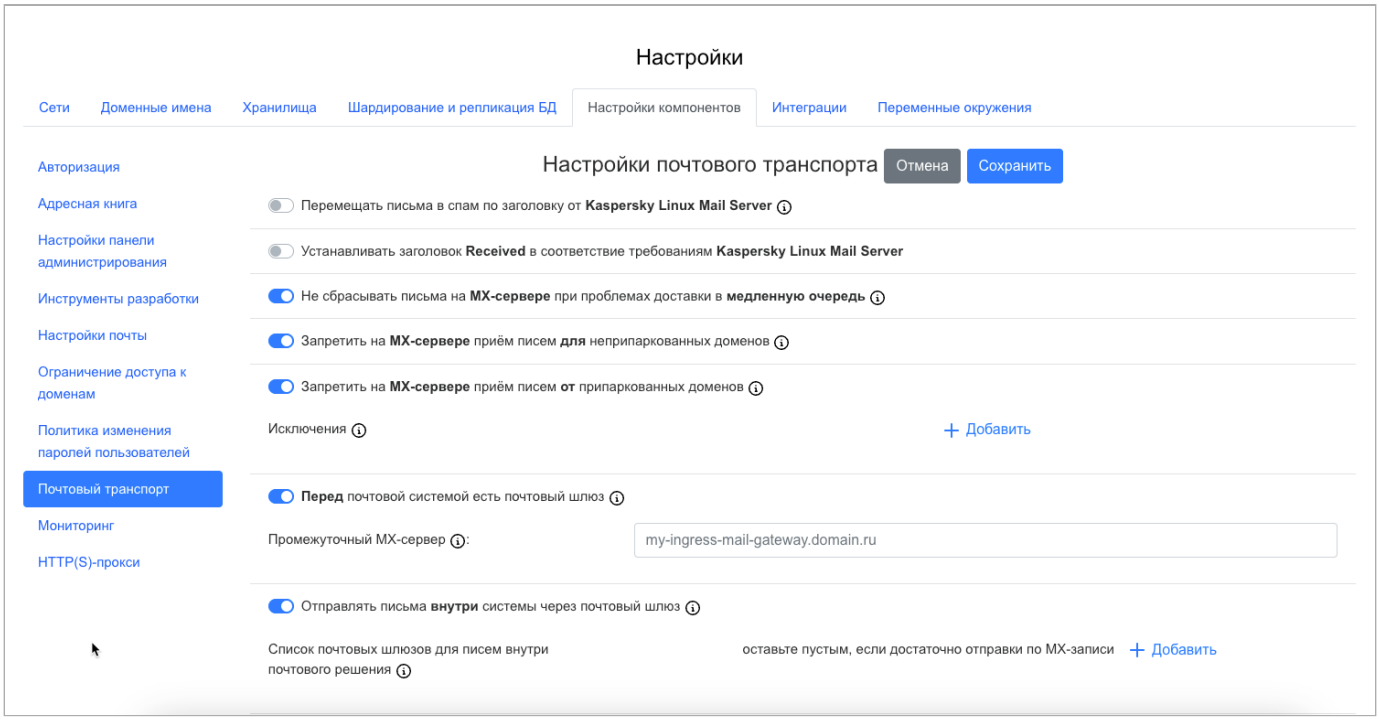


Разрешить пользователям менять пароли — включенный флаг разрешает пользователям менять пароли для своих почтовых ящиков.

Установить максимальный срок действия пароля — при установленном флаге можно установить срок действия пароля. Срок задается в секундах (под полем есть подсказка о том, сколько это будет в более крупных единицах измерения).

Почтовый транспорт

В этой вкладке вы можете изменить нужные вам настройки, нажав на кнопку редактирования .



Перемещать письма в спам по заголовку от Kaspersky Linux Mail Server — включите флаг, если необходима проверка на заголовок X-KLMS-Message-Action. Если у письма присутствует этот заголовок и его значение отличается от **clean**, оно будет автоматически отправляться в папку Спам.

Устанавливать заголовок Received в соответствие требованиям Kaspersky Linux Mail Server — в некоторых случаях Kaspersky Linux Mail Server не может определить последний хоп (расстояние между ближайшими узлами в сетевом протоколе) передаваемого сообщения, из-за этого могут появиться ошибки с валидацией отправителя и проверкой SPF. Чтобы избежать подобных ситуаций, установите этот флаг.

Не сбрасывать письма на MX-сервере в медленную очередь при проблемах доставки — включите флаг, если ваша антиспам/антивирус система не умеет определять сервер отправки почты. Так как медленная почтовая очередь в VK WorkMail реализована отдельным шлюзом, с выключенным флагом могут происходить сбои при проверке подлинности отправителя.

Запретить на MX-сервере прием писем для неприпаркованных доменов — чтобы запретить прием писем для доменов с непроверенной MX-записью, включите этот флаг. При включенной отправке писем внутри системы через почтовый шлюз эта опция также будет включена автоматически.

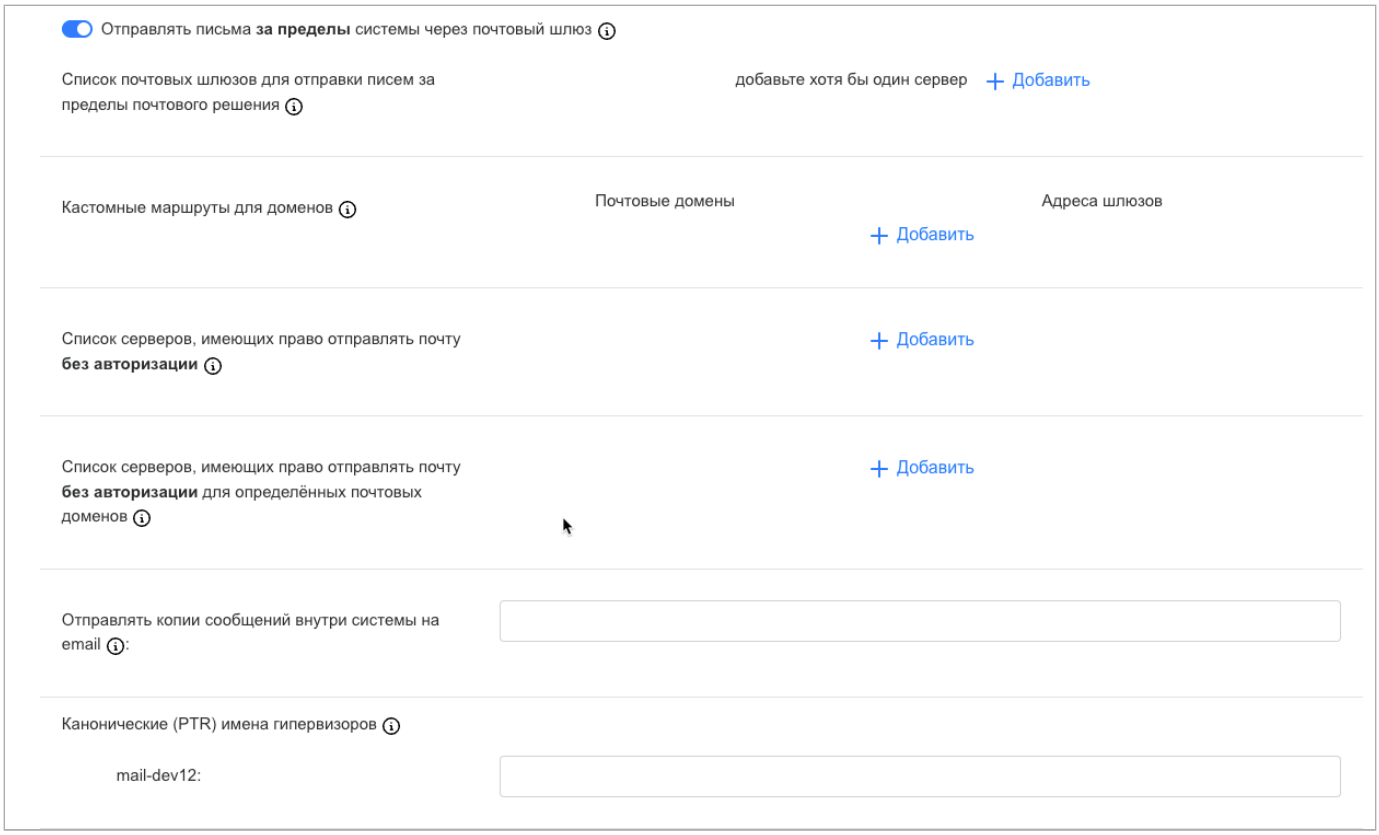
Информация

Чтобы домен считался **припаркованным**, он должен быть добавлен в панель администратора (`biz.<почтовый домен>`); **MX-запись** припаркованного домена должна быть проверена. **Перепиской внутри системы** будет считаться обмен сообщениями между **двумя припаркованными доменами**. Чтобы домен считался **известным**, достаточно добавить его в панель администратора.

Запретить на MX-сервере прием писем от припаркованных доменов — используется для защиты от подделки злоумышленниками писем локальных пользователей. Это неполноценная защита от подделки отправителя, поэтому рекомендуется установка полноценной антиспам-системы.

Перед почтовой системой есть почтовый шлюз — если перед почтовой системой VK WorkMail будет установлен какой-либо почтовый шлюз, включите этот флаг. В поле нужно будет ввести адрес промежуточного MX.

Отправлять письма внутри системы через почтовый шлюз — если необходимо отправлять всю внутреннюю переписку через MX-запись или какой-либо шлюз (антивирус или антиспам), включите эту опцию. Если опция выключена, письма внутри системы доставляются сразу в ящик, минуя MX-сервер.



Отправлять письма за пределы системы через почтовый шлюз — если вы планируете отправлять исходящие письма через шлюз антивируса/DLP-системы, включите эту опцию.

Кастомные маршруты для доменов — вы можете перенаправить домены на заданные шлюзы вместо стандартных. Вы можете внести в раздел «Почтовые домены» несколько доменов и задать для них несколько адресов шлюзов. Если нужно добавить по одному шлюзу для каждого домена, используйте кнопку **Добавить**.

Список серверов, имеющих право отправлять почту без авторизации — добавьте список IP-адресов серверов, почта с которых будет приниматься без авторизации. В список нужно обязательно добавить адреса шлюзов, с которых почта должна возвращаться в VK WorkMail. В этот же список можно внести серверы рассылки почты илив соответствии с их назначением МФУ, отсканированные документы с которых будут отправляться без авторизации. Почта, отправленная в VK WorkMail без авторизации, будет приниматься на порт **1025**.

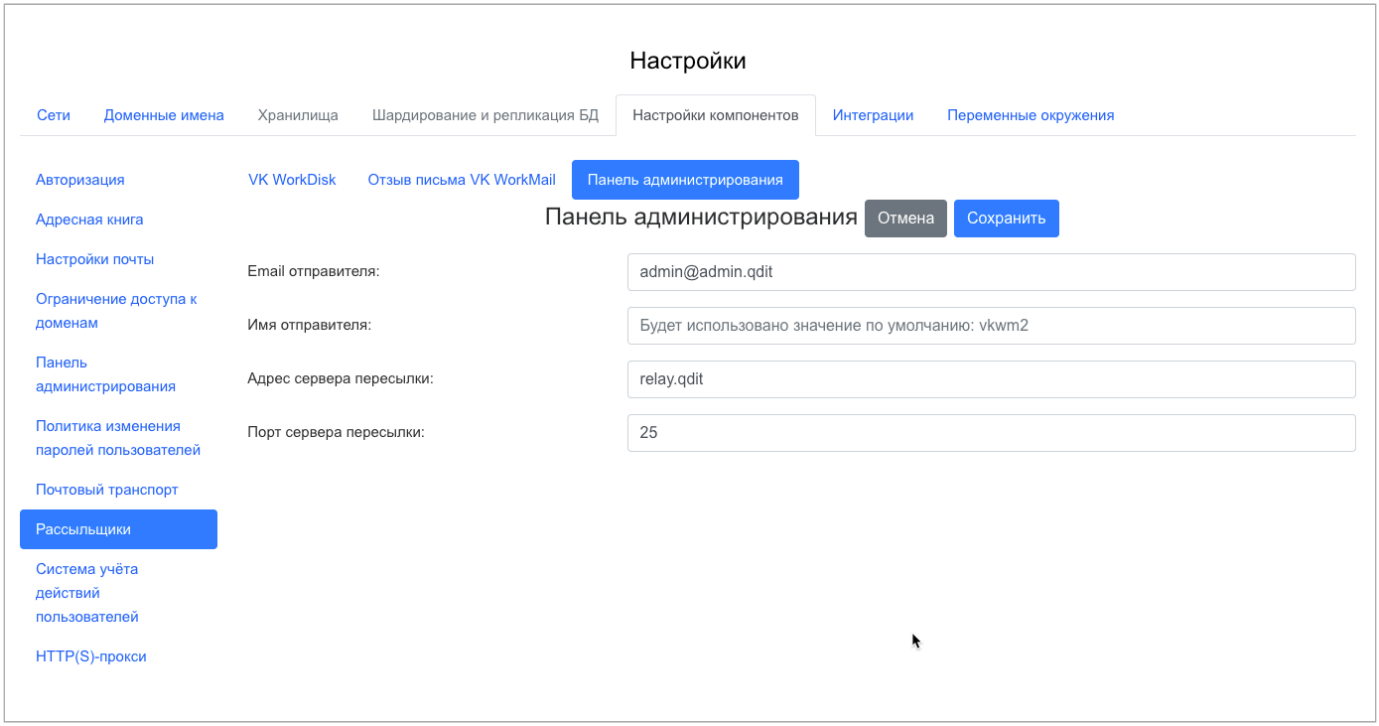
Список серверов, имеющих право отправлять почту без авторизации для определенных почтовых доменов — если вы планируете использовать несколько почтовых доменов, есть возможность добавить для каждого домена свои доверенные IP. Письма с указанных доменов должны отправляться на порт **1025**.

Отправлять копии сообщений внутри системы на email — в почтовой системе VK WorkMail реализована возможность отправки копий внутренней переписки на специальный ящик. В таком случае проверка внутренних писем не будет блокировать потоки почты.

Канонические (PTR) имена гипервизоров — укажите название хоста в PTR-записи. PTR-запись позволяет определить по IP имя хоста, с которого приходит почта. Если при проверке имя хоста будет отличаться, письмо не будет доставлено или попадет в папку Спам.

Рассыльщики

В разделе настраиваются служебные почтовые рассылки для внутренних пользователей. Чтобы перейти к настройкам, нажмите на кнопку редактирования. Есть возможность создать рассылки для VK WorkDisk, административной панели и уведомлений об отзыве письма.

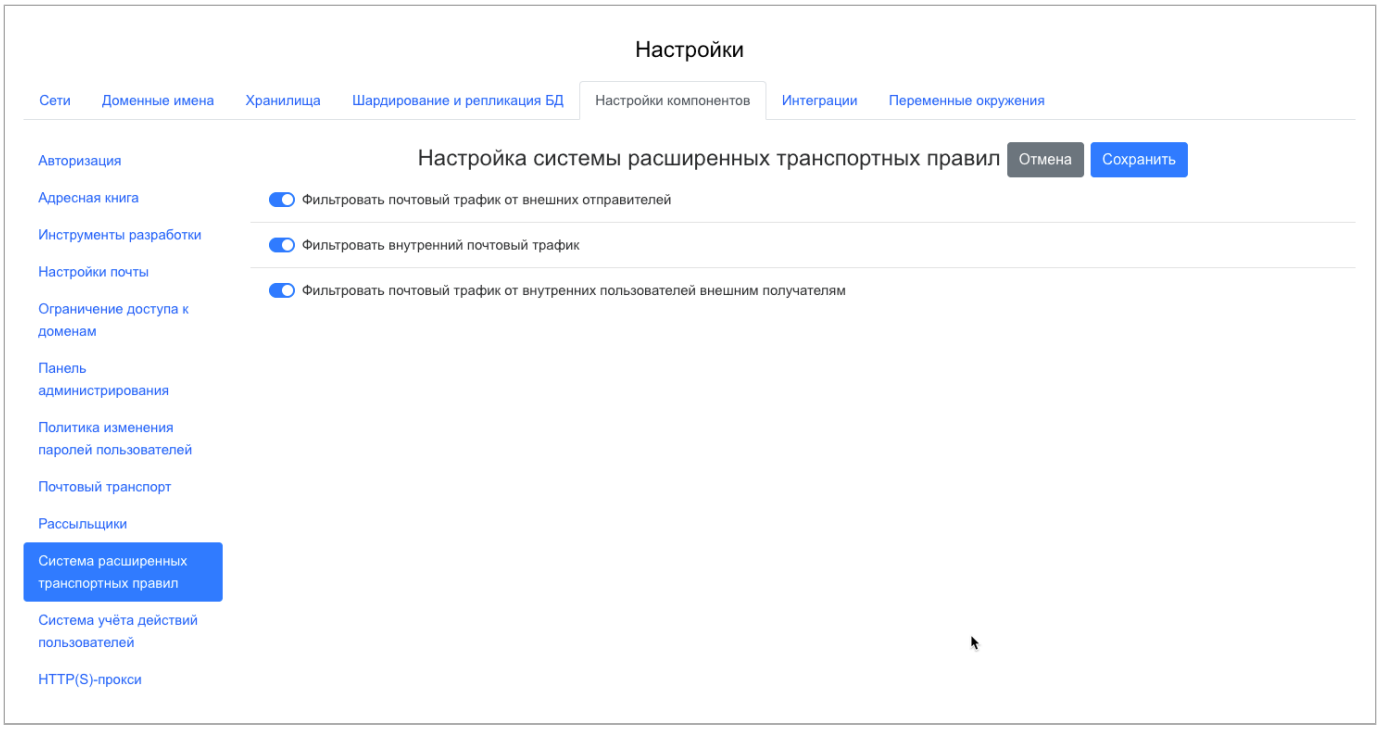


Введите email и имя отправителя, а также адрес и порт сервера рассылки, и сохраните изменения. Затем перейдите к списку ролей и запустите автоматическую установку, чтобы применить настройки.

Система расширенных транспортных правил

Чтобы начать настройку, необходимо нажать на ⓘ, перейти в окно **Продукты** и включить флаг **Система расширенных транспортных правил.**

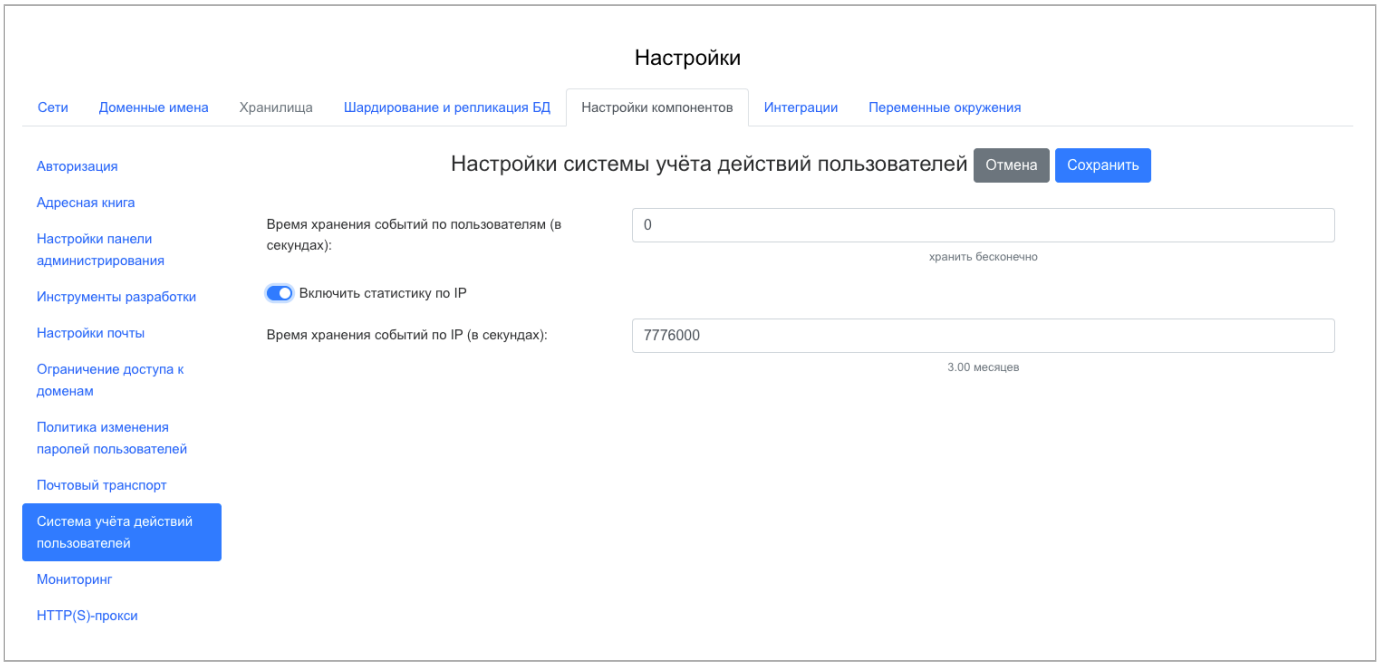
Затем перейдите к списку ролей и запустите автоматическую уставку. Когда нужные роли сгенерируются, перейдите в раздел **Компоненты → Система расширенных транспортных правил** и включите нужные флаги.



Дальнейшая настройка транспортных правил производится в административной панели по завершении установки. Процедура настойки описана по ссылке.

Система учета действий пользователей

Чтобы изменить время хранения логов, кликните по кнопке редактирования.



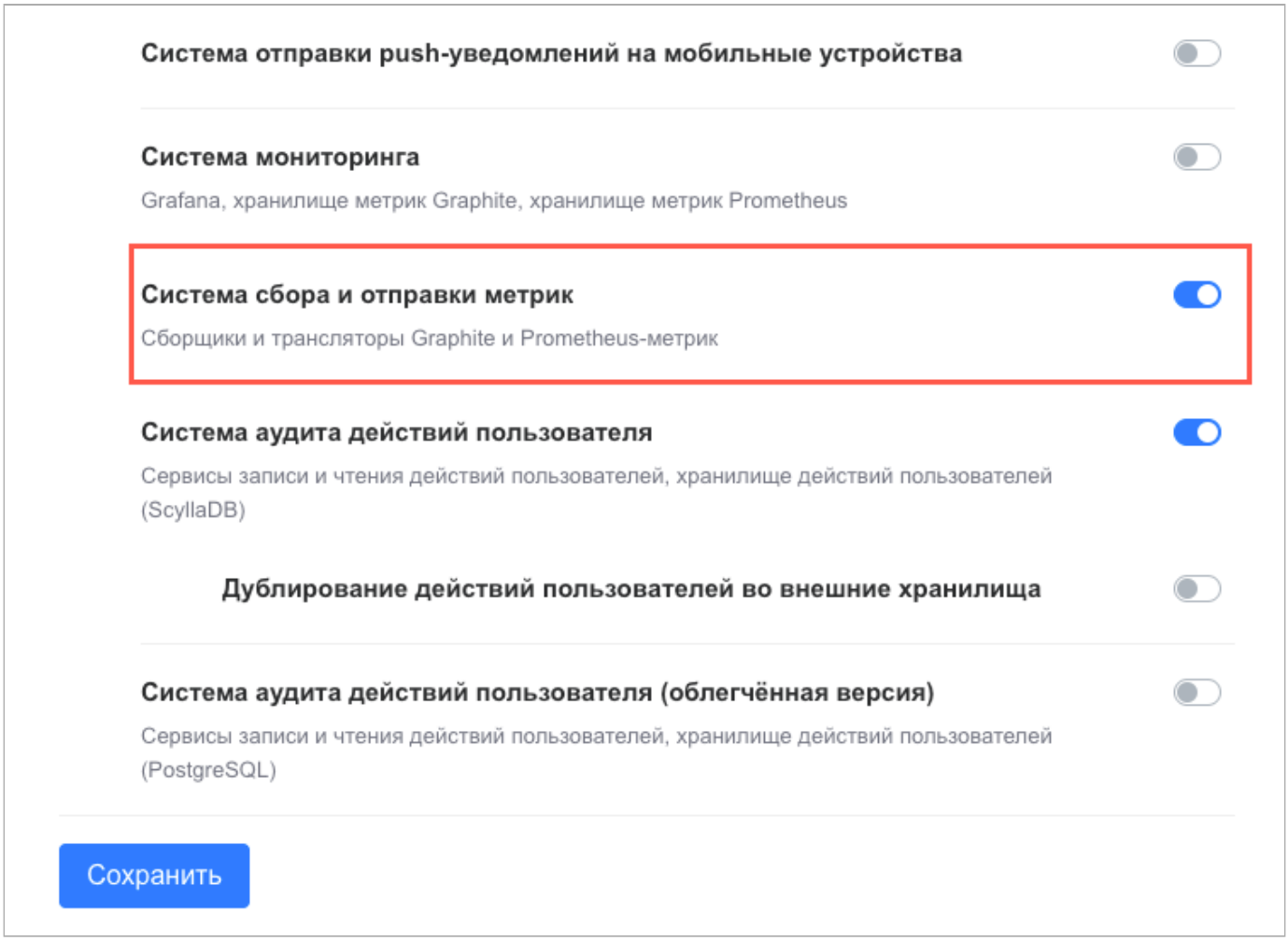
Время хранения событий по пользователям (в секундах) — вы можете установить время хранения логов. При установленном значении 0 срок хранения логов не будет ограничен.

Включить статистику по IP — при включенном флаге появится окно для изменения срока хранения логов по IP.

Мониторинг

Настройки мониторинга актуальны для случаев, когда необходимо переключиться с внутреннего мониторинга VK WorkMail на внешние системы мониторинга (Graphite/Prometheus).

Для включения внешних систем мониторинга необходимо нажать на ⓘ и перейти в окно **Продукты** и включить флаг **Система сбора и отправки метрик.** При этом флаг **Система мониторинга** будет автоматически отключен.



Примечание

Данные, созданные до переключения на внешний мониторинг, продолжат занимать место на диске. Новые данные будут направляться во внешнюю систему мониторинга.

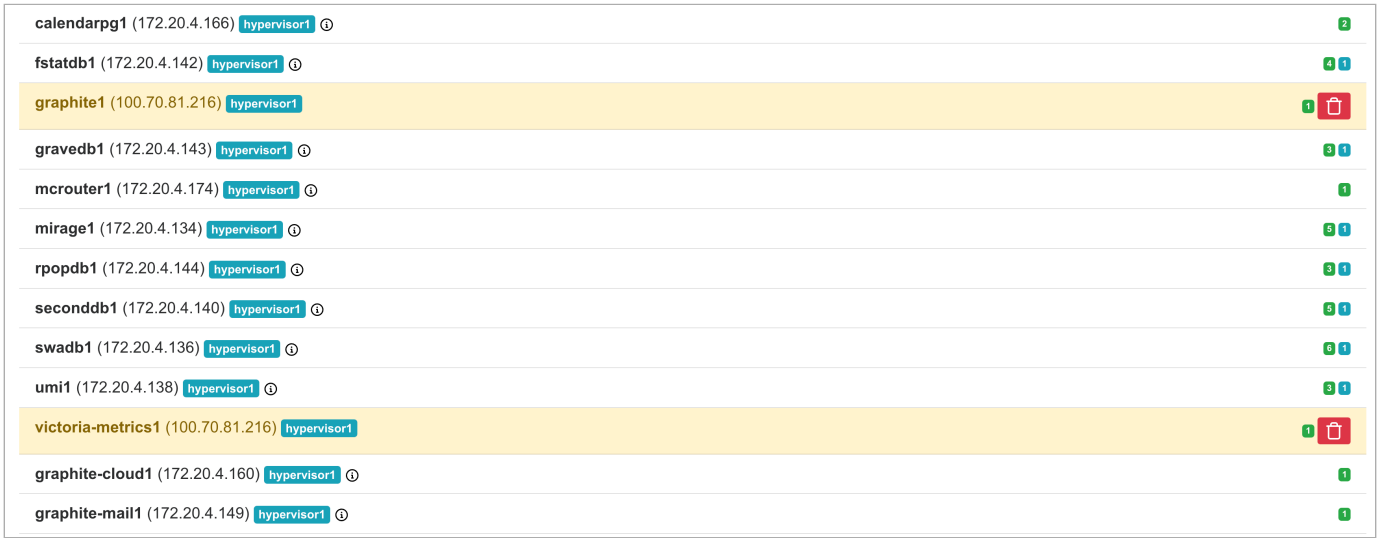
Сохраните изменения и вернитесь к списку ролей.

Внизу страницы нажмите на кнопку **Сгенерировать автоматически**, чтобы установщик сформировал новые роли.

> **Важно**
>
> **Не нужно** запускать автоматическую установку сразу после генерации контейнеров. Сначала необходимо удалить неактуальные роли. Если запустить установку сразу, возникнут сетевые проблемы.

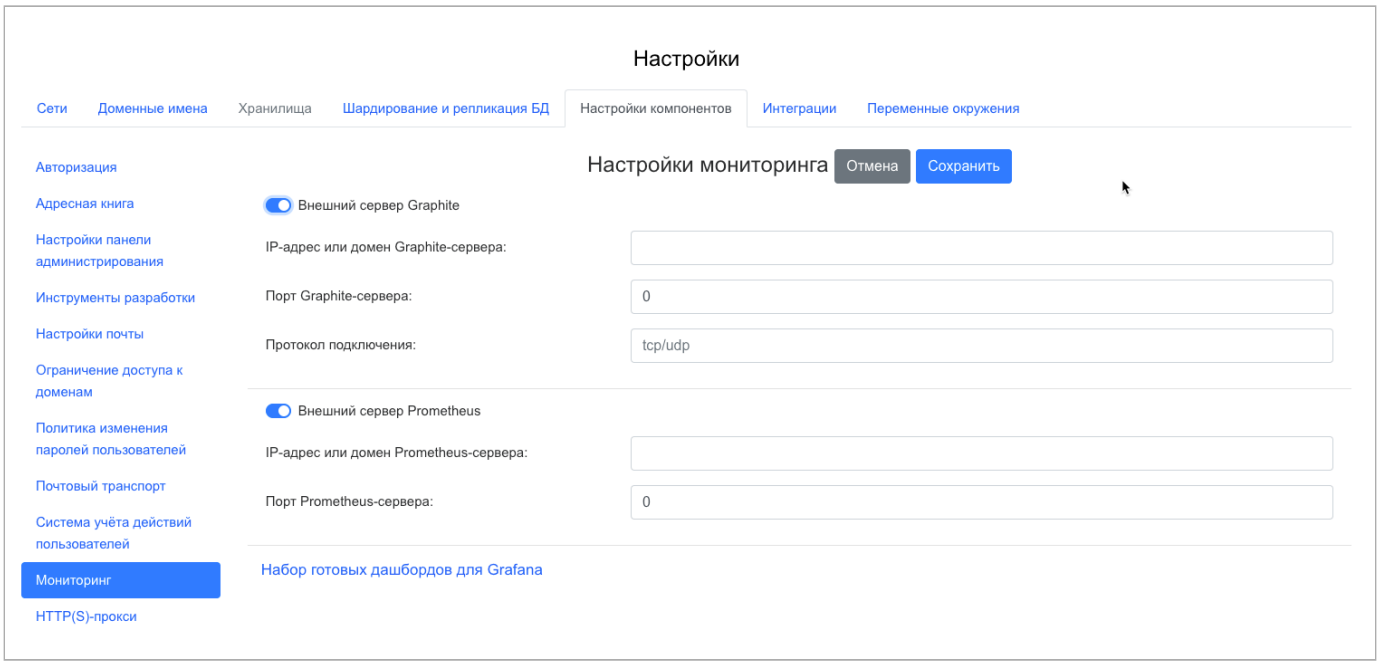
Чтобы предотвратить возможные проблемы, перейдите в консоль и перезапустите установщик с помощью команды: `sudo systemctl restart deployer`.

После перезапуска в списке ролей отобразятся роли, которые нужно удалить. Если в интерфейсе не подсветились роли для удаления, перезагрузите страницу.



Удаление может занять некоторое время. Когда все неактуальные роли будут удалены, запустите автоматическую установку.

Далее передите в раздел **Настройки компонентов → Мониторинг**. Введите необходимые данные для системы мониторинга, которую вы используете.



Сохраните изменения.

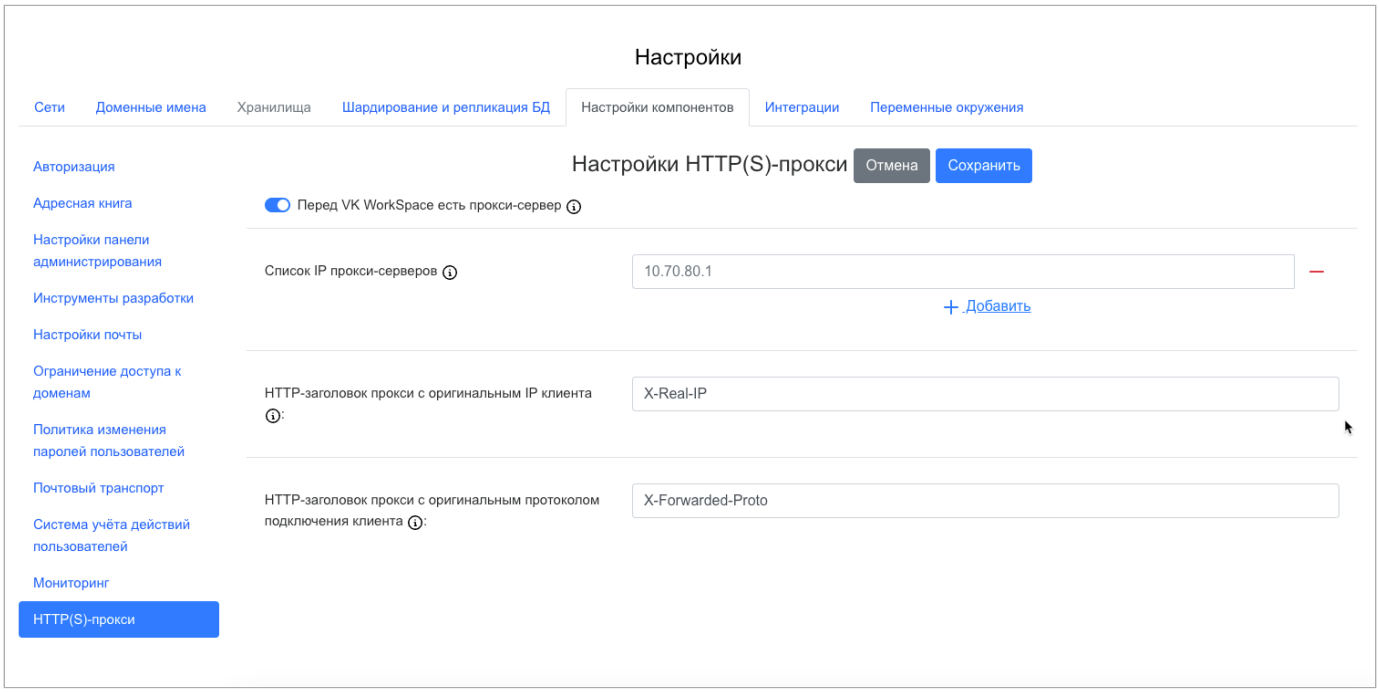
Информация

Также по ссылке **Набор готовых дашбордов для Grafana** вы можете скачать дашборды в формате JSON для добавления их в Grafana.

Перейдите к списку ролей, кликнув по логотипу **AdminPanel**, и при необходимости повторите нужные шаги.

Настройки HTTP(S)-прокси

Если вы используете прокси-сервер при подключении клиентов к системе VK WorkSpace, включите флаг **Перед VK WorkSpace есть прокси-сервер**, чтобы контейнер, отвечающий за HTTPS-соединение, мог принимать трафик без шифрования.



Список IP прокси-серверов — введите в поле список IP-адресов, с которых VK WorkMail будет принимать заголовки с оригинальными IP клиента и оригинальным протоколом подключения.

HTTP-заголовок прокси с оригинальным IP клиента — добавьте в поле заголовок прокси, который передает реальный IP-адрес клиента, иначе сервис будет работать некорректно.

HTTP-заголовок прокси с оригинальным протоколом подключения клиента — для корректной работы почтовых сервисов введите заголовок оригинального протокола подключения.

12. Интеграции

В блоке будут отображаться интеграции, которые вы включили на этапе выбора продуктов и опций (настройки интеграций могут также находиться в верхнем меню).

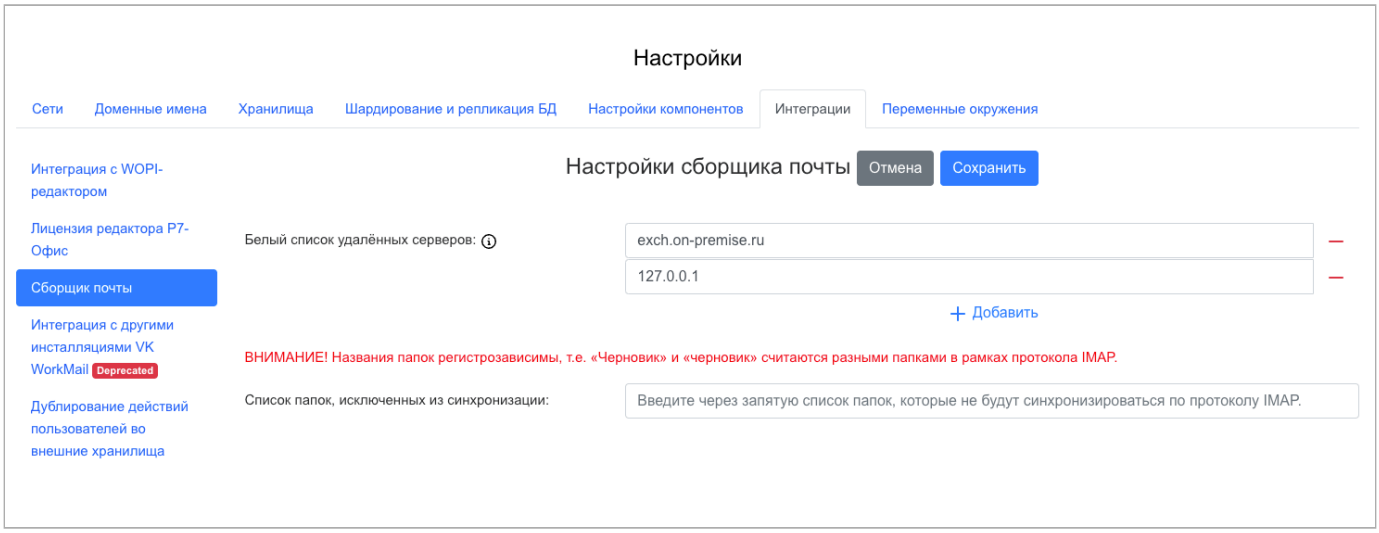
Настройка интеграции VK Teams и VK WorkMail — с помощью документа вы сможете настроить интеграцию между VK Teams и VK WorkMail.

Миграция календарей по протоколу EWS — документ по настройке миграции событий из MS Exchange в VK WorkMail.

Интеграция с Keycloak для SSO-авторизации — в документе содержится инструкция по настройке интеграции с сервисом SSO-авторизации.

Сборщик почты

В разделе есть возможность добавить почтовые серверы для синхронизации/миграции, а также список папок, которые не будут участвовать в синхронизации.



Белый список удалённых серверов — по умолчанию в полях указаны внутренние IP-адреса. Если вы планируете миграцию почты с других почтовых серверов, добавьте их IP-адреса или имена в белый список — VK WorkMail будет определять эти IP/хосты как публичные. При миграции из систем с белым IP/доменом поле можно оставить пустым. При настройке миграции в административной панели вам нужно будет ввести IP/хост, с которого будет производиться миграция.

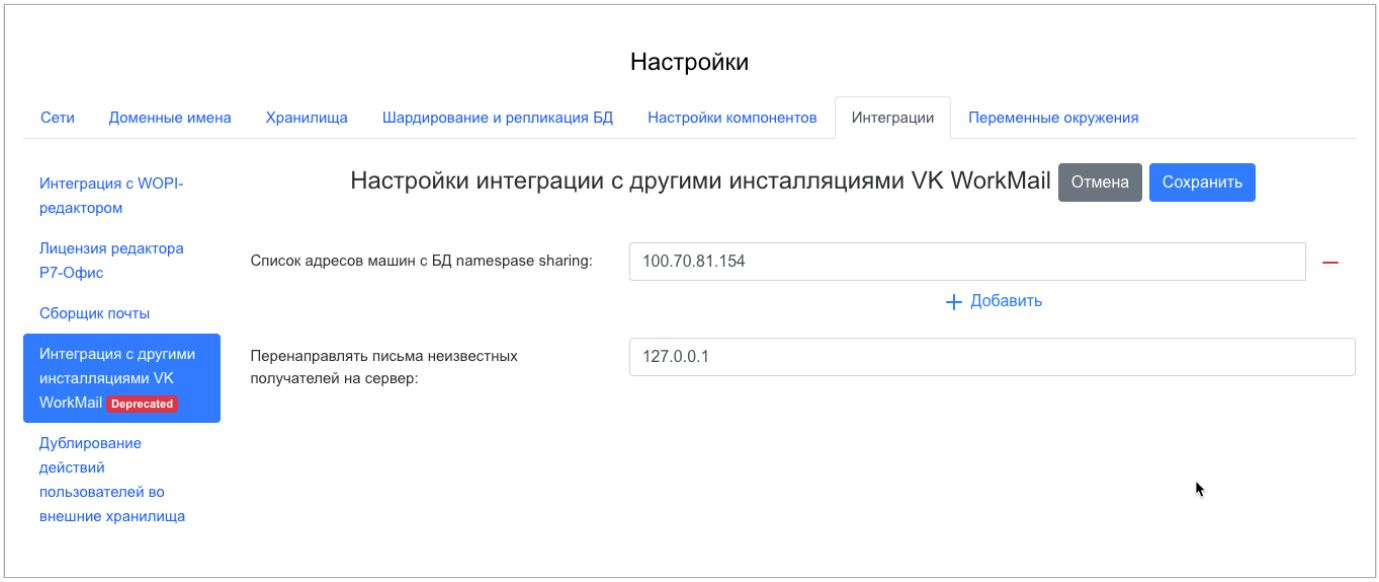
Список папок, исключенных из синхронизации — если у вас есть папки, которые не должны участвовать в синхронизациив соответствии с их назначением «Черновики» и «Удаленные», введите их названия через запятую **в строгом соответствии** с оригинальным названиям из вашей системы (названия папок регистрозависимы).

Интеграция с другими инсталляциями VK WorkMail

> **Информация**
>
> Функциональность устарела и будет в скором времени удалена.

В разделе вы можете настроить интеграции с несколькими инсталляциями VK WorkMail и/или миграции с Exchange и других почтовых серверов.

Чтобы перейти к настройкам, нажмите на кнопку редактирования. Появится возможность изменить значения полей.



Список адресов машин с БД namespase sharing — с помощью кнопки **Добавить** внесите IP-адреса машин с инсталляциями VK WorkMail. При нескольких инсталляциях введите все адреса машин, объединенных в БД namespase sharing.

Каждая из инсталляций получит реплики каталогов пользователей с IP, указанных в поле. При отправке письма система будет знать, на какой почтовый сервер его направить.

По умолчанию в поле указан локальный IP. Если вы пока что не планируете работу с несколькими инталляциями, оставьте значение по умолчанию.

> **Важно**
>
> Если в интеграции участвуют кластерные инсталляции VK WorkMail, в поле нужно ввести IP-адреса контейнеров **tnt-fedman1**.

Также потребуется настройка переменных окружения, описанная в следующем шаге.

Перенаправлять письма неизвестных получателей на сервер — если вы будете проводить миграцию с других почтовых серверов, введите его IP-адрес в поле. В случаях, когда письмо отправляется в адрес пользователей, которые еще не мигрировали в VK WorkMail, система будет автоматически перенаправлять их на указанный IP-адрес. Перенаправление будет работать только для припаркованных доменов.

> **Примечание**
>
> Дальнейшая настройка миграции с Exchange или других почтовых серверов производится в административной панели VK WorkMail по завершении установки.

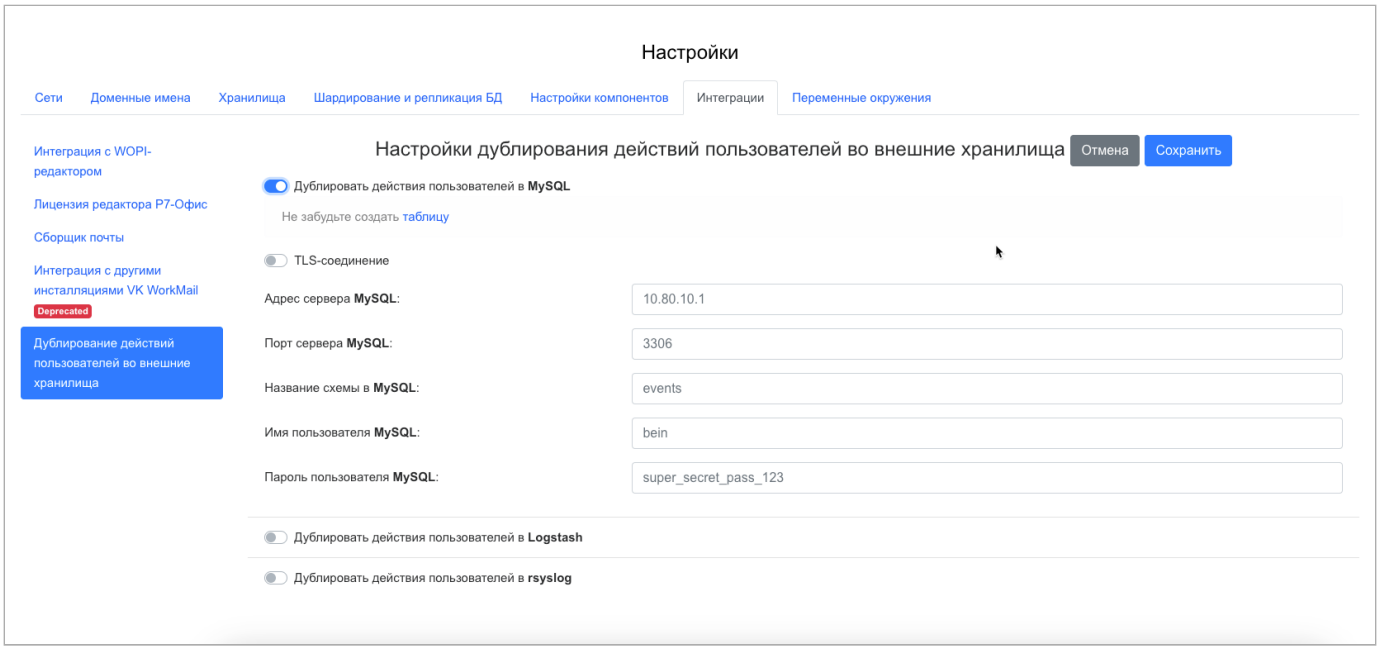
Продублируйте значение по умолчанию из поля выше, если перенаправление писем в данный момент не требуется.

Сохраните изменения и перейдите к следующему шагу, нажав на кнопку **Далее**.

Настройки дублирования действий пользователей во внешнее хранилище

Если на этапе выбора продуктов вы включили опцию дублирования логов, потребуются настройки в этом разделе.

Включите флаг того хранилища, которое вы планируете использовать: **MySQL**, **Logstash** и **rsyslog**. Также есть возможность включения TLS-шифрования.



> **Важно**
>
> Предварительно создайте таблицу, в которую будут сохраняться логи.

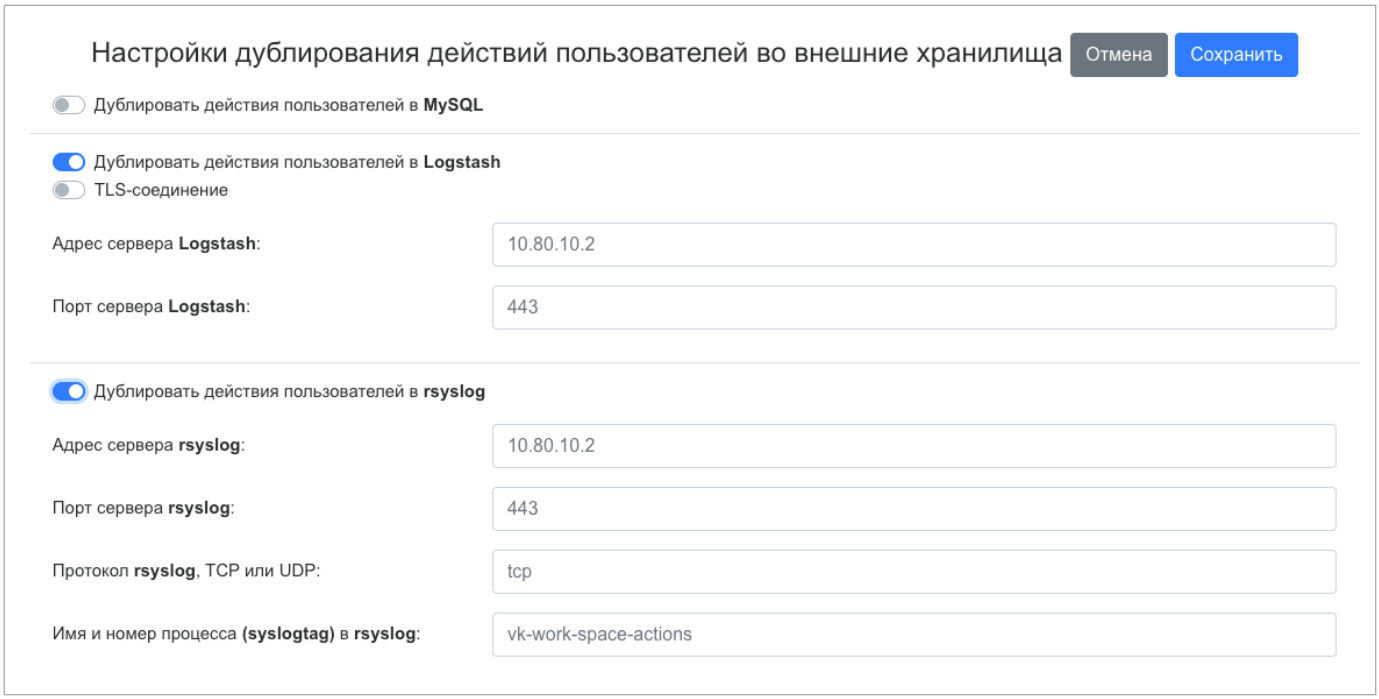
Адрес сервера MySQL — введите адрес сервера MySQL, на котором будут храниться логи.

Порт сервера MySQL — порт, открытый в вашей БД для VK Workspace.

Название схемы в MySQL — тип архитектуры (схемы) вашей БД.

Имя пользователя MySQL — пользователь БД, имеющий права на запись.

Пароль пользователя MySQL — введите пароль пользователя, указанного в поле выше.



Для **Logstash** достаточно ввести адрес сервера и порт.

Чтобы передавать данные в **rsyslog**, введите в поля адрес сервера, его порт, а также протокол подключения и syslogtag.

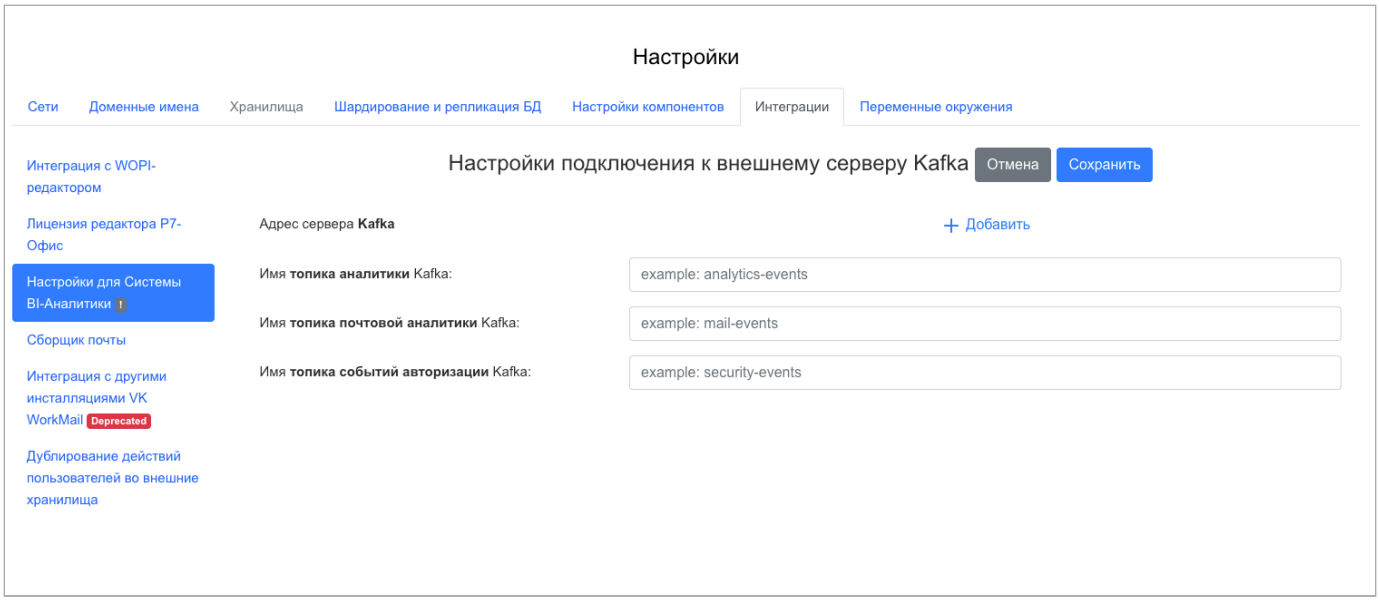
По завершении настроек сохраните изменения.

Настройки системы BI-аналитики

Чтобы получить возможность просматривать статистику использования VK WorkDisk в административной панели (`biz.<почтовый домен>`), в списке продуктов необходимо включить опцию **Система BI-аналитики** и **Kafka внутри инсталяции** и нажать на кнопку **Сохранить**.

> **Примечание**
>
> Если вы используете внешний сервер Kafka, вторую опцию включать не нужно, но потребуется внести данные для подключения. При использовании Kafka внутри инсталляции можно сразу переходить к списку ролей.

Чтобы подключиться к внешнему серверу Kafka, перейдите в раздел **Интеграции** → **Настройки системы BI-аналитики** и заполните соответствующие поля.



Сохраните изменения.

Перейдите к списку ролей, кликнув по логотипу **AdminPanel**. Внизу страницы необходимо создать дополнительные роли. Нажмите на кнопку **Добавить** → **Несколько контейнеров**. В поле **Установлено не более:** введите значение **0**. Появятся контейнеры для распределения. Добавьте контейнеры для Clickhouse на гипервизоры для хранилищ. Если вы используете Kafka внутри инсталяции, распределите контейнеры с Kafka на гипервизоры для баз данных тем же способом (с помощью кнопки **Добавить**).

По окончании генерации контейнеров запустите **автоматическую установку** в общей строке состояния. Когда установка будет завершена, у вас появится возможность просматривать статистику Диска в панели администратора.

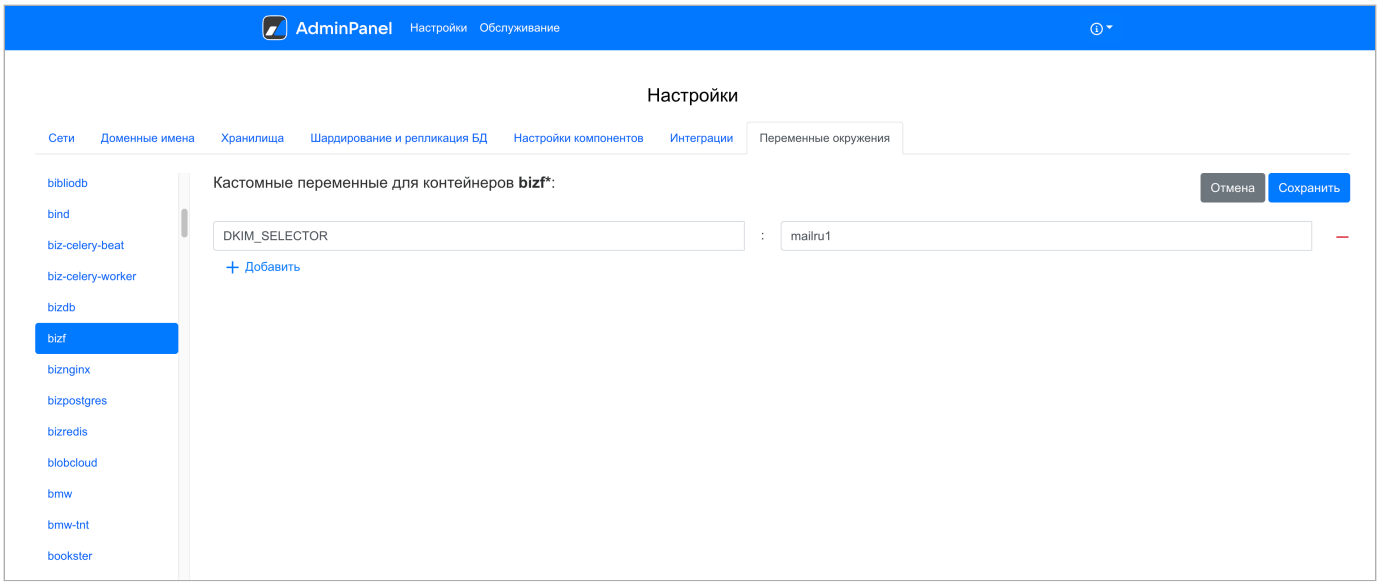
13. Переменные окружения

При работе с несколькими инсталляциями VK WorkMail требуется настройка кастомных переменных для контейнеров **bizf** и **biz-celery-worker**.

> **Примечание**
>
> Если нужна настройка переменных, обратитесь к представителю VK.

В списке контейнеров вам нужно выбрать **bizf**, а затем **biz-celery-worker** и создать для **обоих** контейнеров переменную окружения с названием **DKIM_SELECTOR**. В поле значения переменной вы должны вставить селектор DKIM-подписи домена для текущей инсталляции VK WorkMail.

Для других инсталляций также необходимо создание аналогичной переменной способом, описанным выше. Селекторы разных инсталляций **не должны совпадать**.



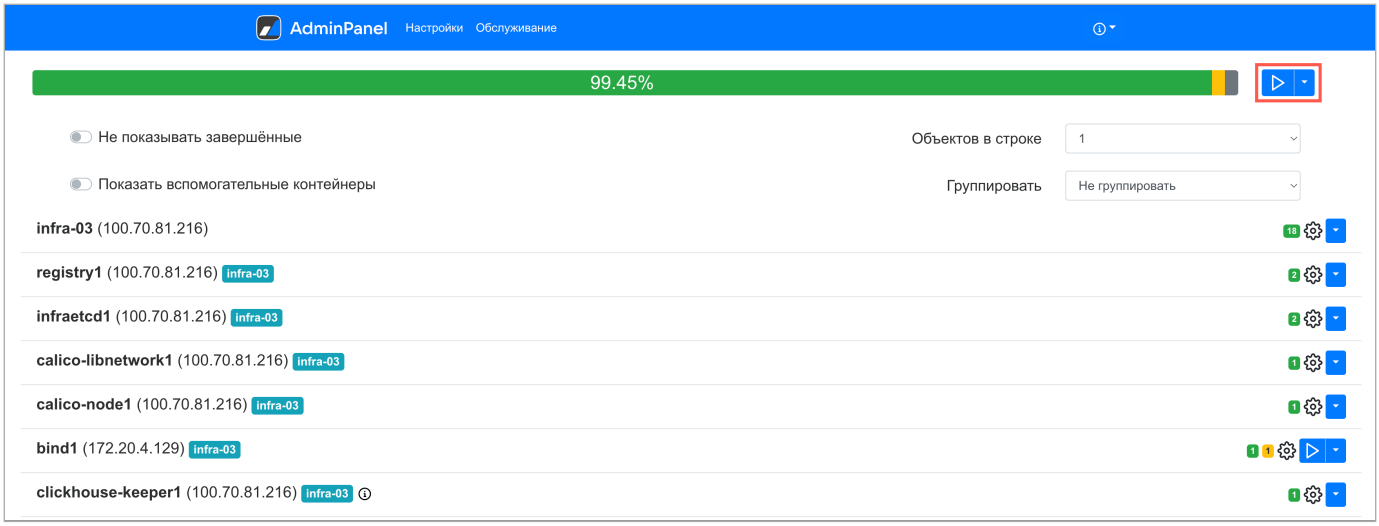
Важно

Если несколько инсталляций VK WorkMail обслуживают один почтовый домен, необходимо создать несколько DKIM-подписей с **разными селекторами** под каждую инсталляцию, обслуживающую этот домен. Не используйте одну DKIM-подпись для нескольких инсталляций, это может привести к ошибкам доставки.

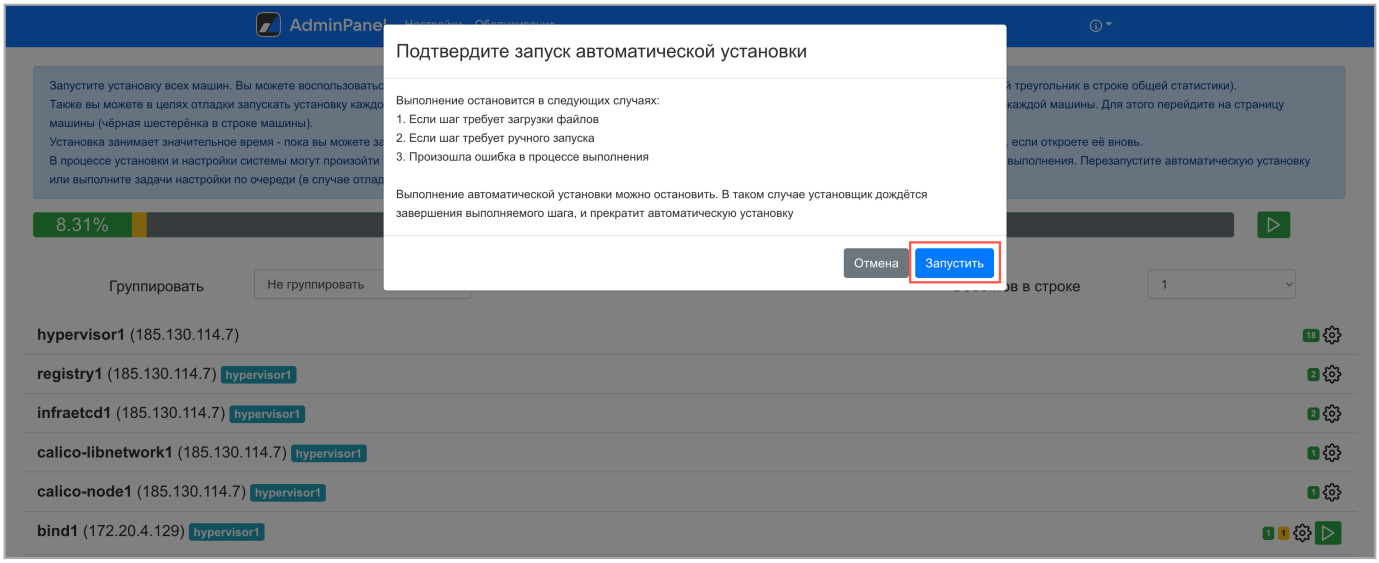
После сохранения изменений нажмите на кнопку **Далее**.

14. Запуск установки всех машин

Кликните по кнопке **Play** рядом с общей строкой состояния в верхней части экрана.



Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**.



В зависимости от этапа установки будет меняться цвет индикатора:

- **Серый** — в ожидании начала генерации;
- **Синий** — в процессе генерации;
- **Желтый** — шаг необходимо повторить (установщик делает это самостоятельно);
- **Красный** — ошибка.

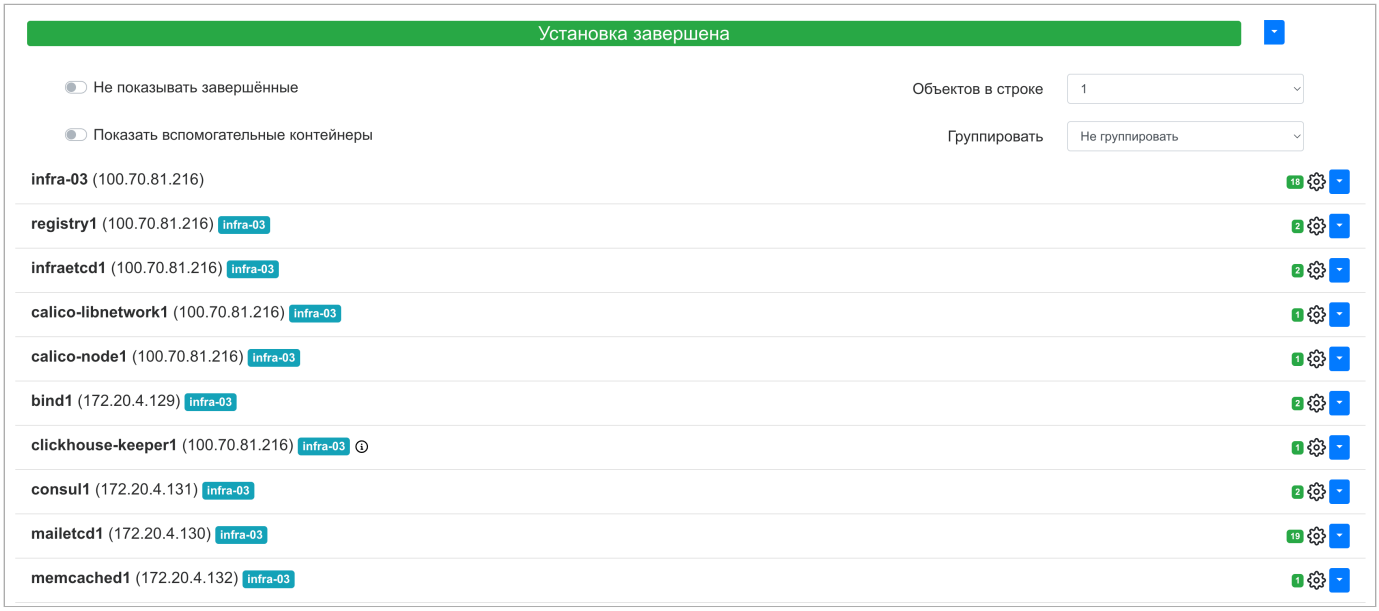
Ожидайте завершения установки. Пока процесс идет, рядом со строкой состояния будет отображаться красная кнопка **Stop**.

Примечание

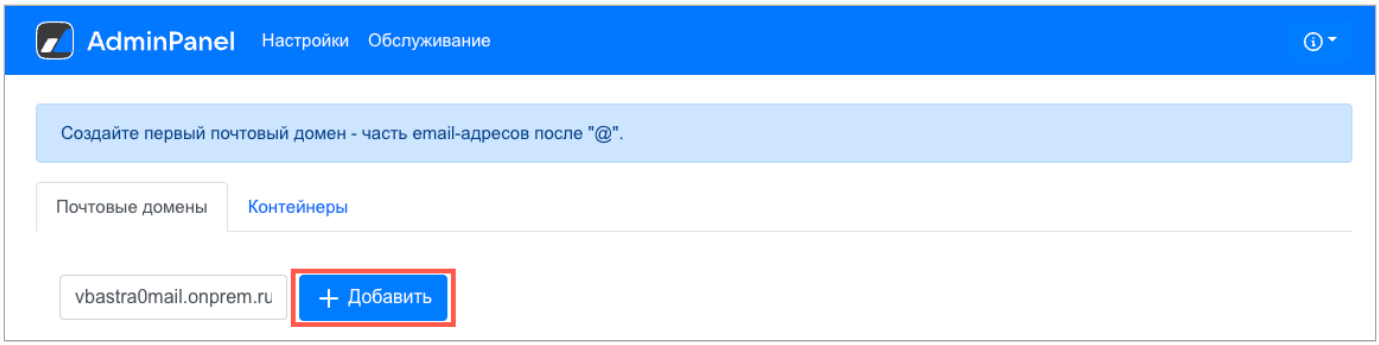
Если в процессе установки и настройки системы происходят изменения конфигурации, некоторые задачи могут потребовать повторного выполнения. Для повторного запуска необходимо нажать на кнопку **Play** в общей строке состояния в верхней части экрана или рядом с названием конкретного контейнера.

15. Завершение установки, инициализация домена и вход в панель администратора

Когда установка будет завершена, соответствующий статус отобразится в строке состояния. Для перехода к следующему шагу нажмите на кнопку **Далее**.

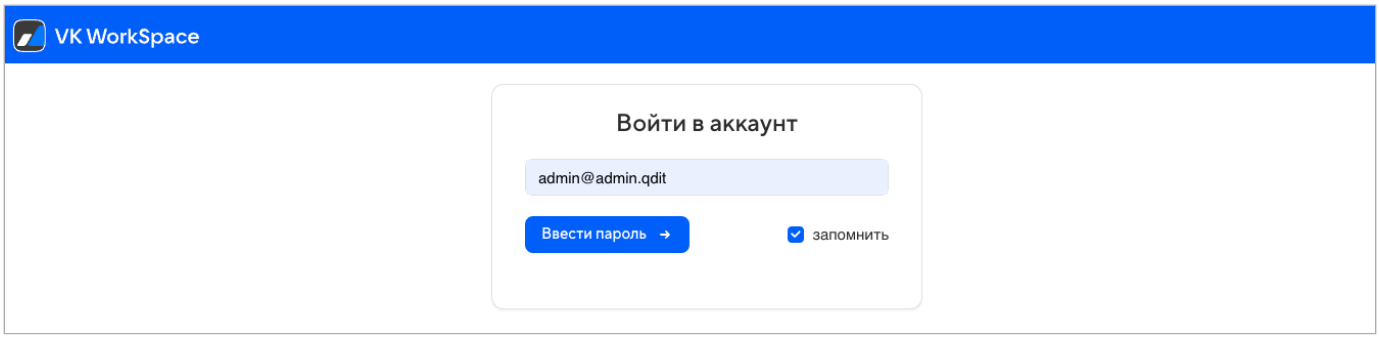


Введите имя почтового домена и нажмите на кнопку **Добавить**.

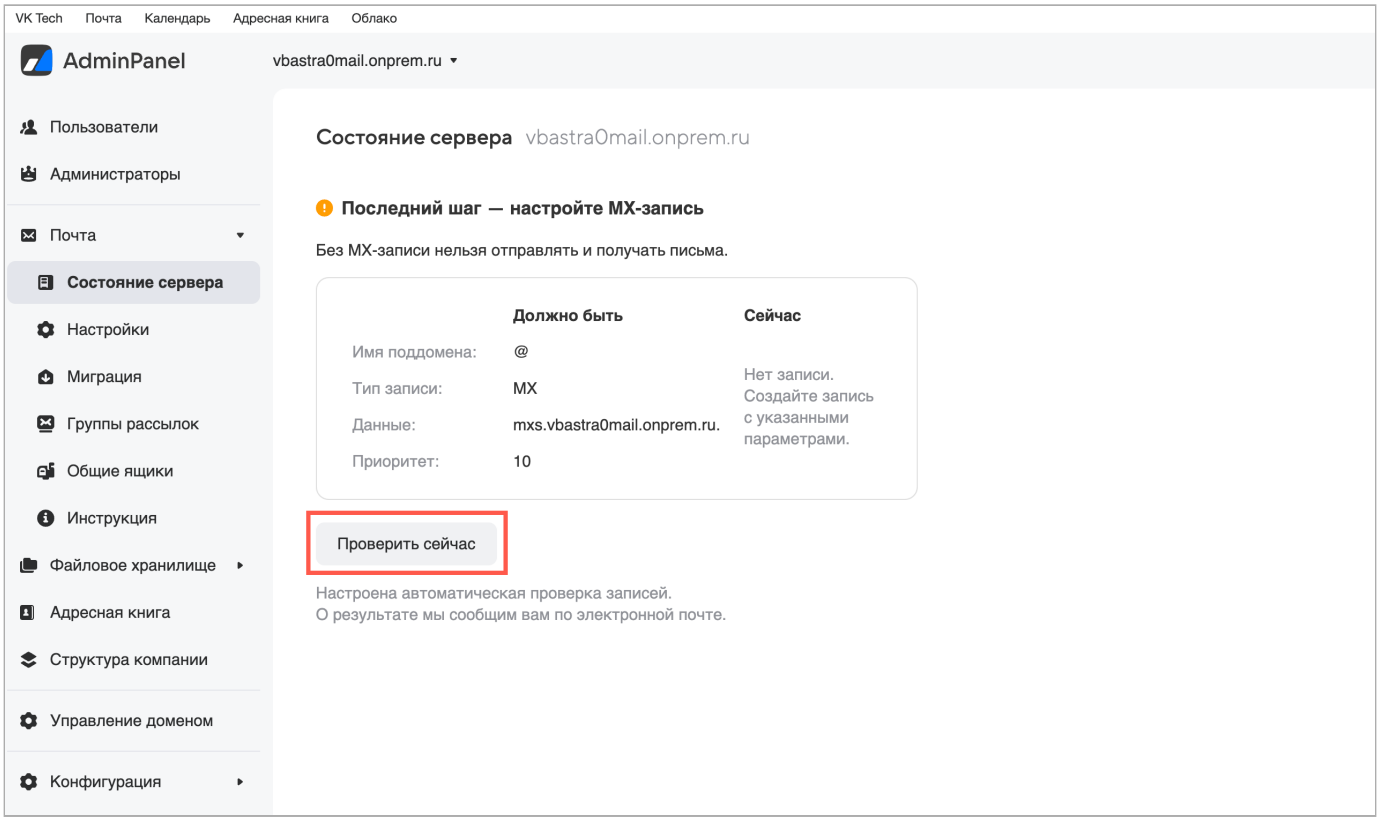


Откроется новая вкладка, на которой необходимо авторизоваться:

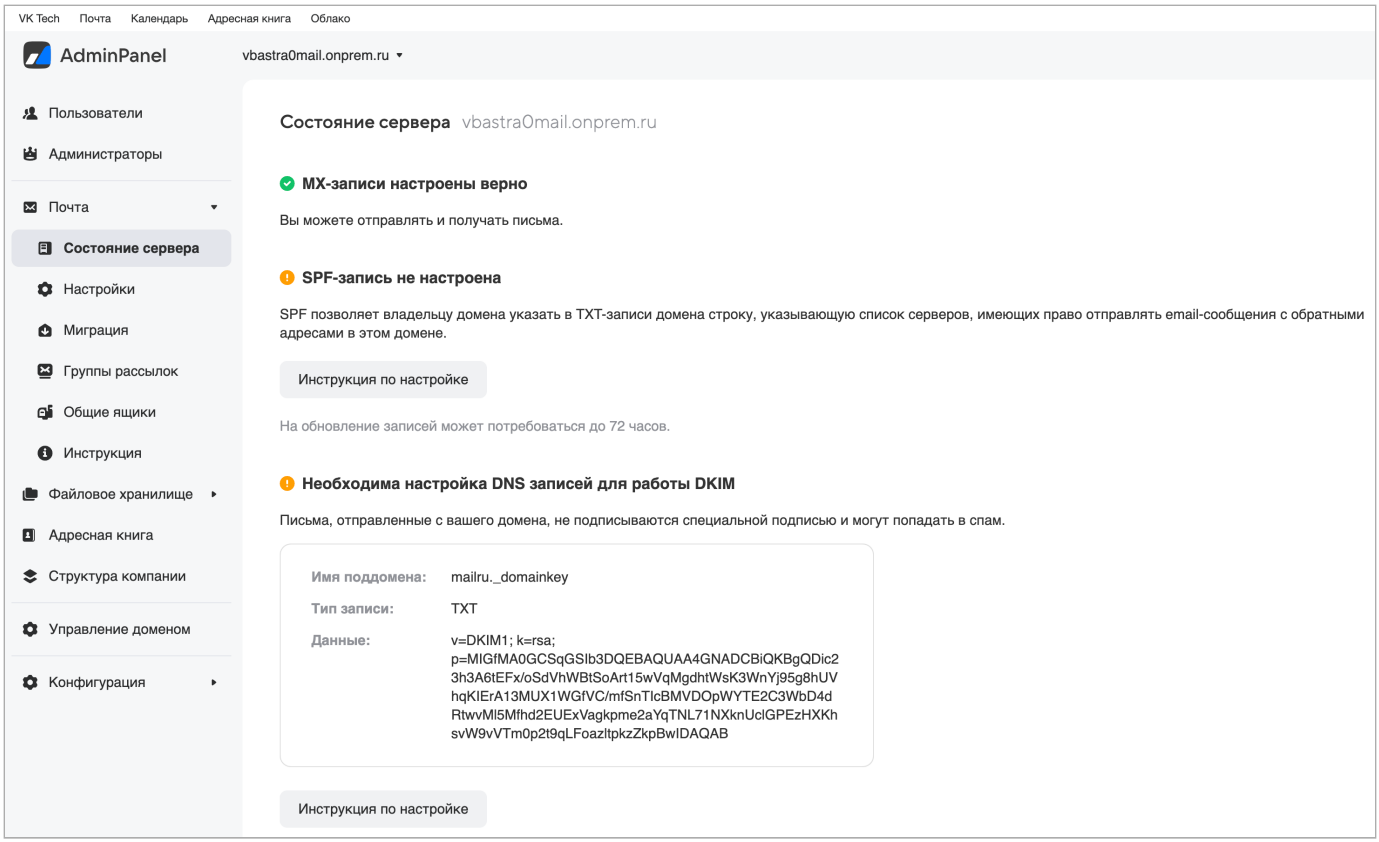
- Имя пользователя — **admin@admin.qdit**.
- Пароль находится в файле — **bizOwner.pass**, для его просмотра введите в консоли команду: `cat /home/deployer/bizOwner.pass`.



Если логин и пароль были введены правильно, вы попадете в панель администратора. Для проверки **MX-записи** нажмите на кнопку **Проверить сейчас**.



При успешно пройденной проверке появится уведомление о том, что **MX-запись** настроена верно.

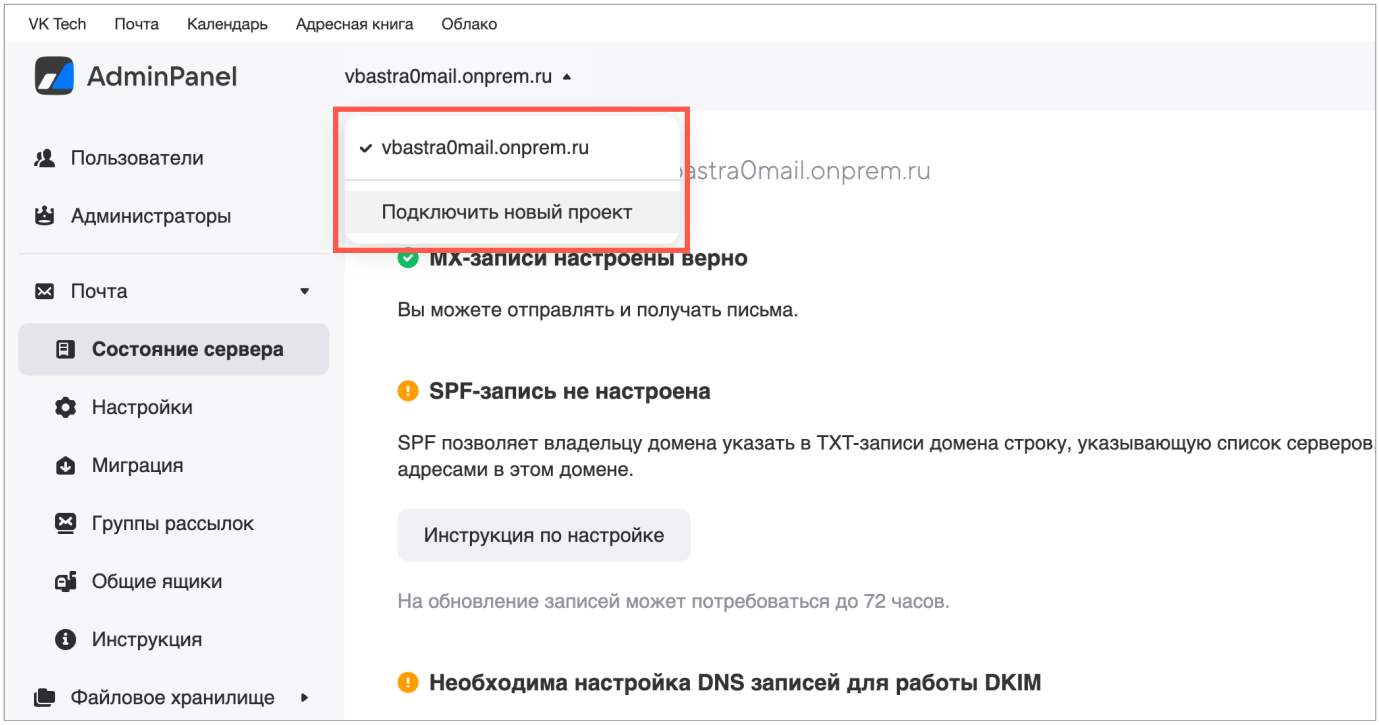


После проверки MX-записи установку можно считать оконченной. Также потребуется настройка **SPF-записи** и **DKIM-подписи**. Инструкции по их настройке вы найдете по ссылке.

> **Важно**
>
> По завершении установки допускается только удаление архива, из которого был распакован дистрибутив в начале установки. Все остальные файлы должны оставаться в папке с файлом **onpremise-deployer_linux**. **Не удаляйте пользователя deployer** — эта учетная запись потребуется для обновления и дальнейшей эксплуатации сервиса почты.

16. Добавление дополнительных доменов

Если вы планируете использовать несколько доменов, добавьте их с помощью кнопки **Подключить новый проект**. Для этого нужно открыть выпадающее меню рядом с вашим доменом и ввести адрес домена.

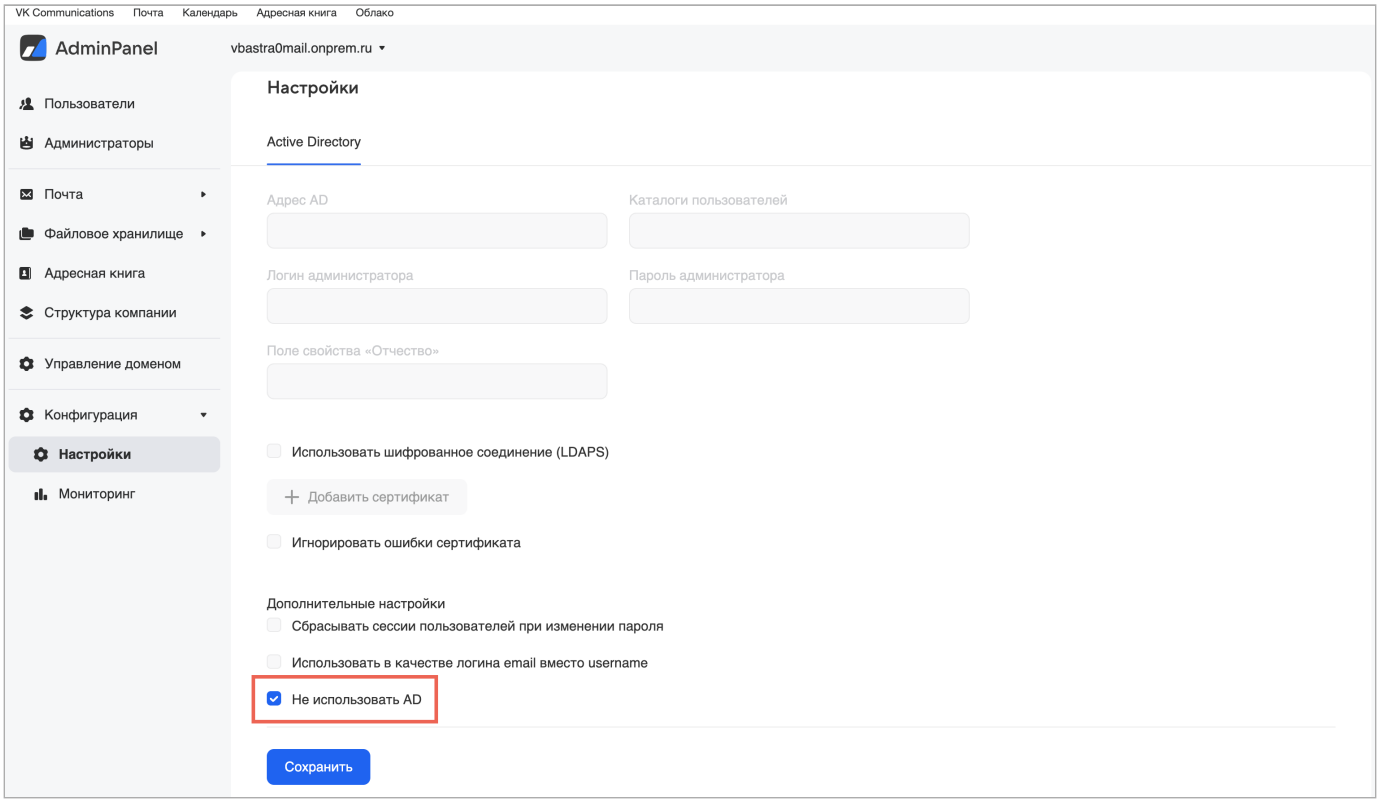


Если хотите сделать домен **припаркованным**, необходимо пройти проверку MX-записи способом, описанным выше. Чтобы сделать домен **известным** для системы VK WorkMail, достаточно просто добавить домен в список.

Настройка интеграции с Active Directory

Для настройки интеграции с **Active Directory** перейдите в раздел административной панели **Конфигурация → Настройки**.

Чтобы начать настройку, уберите чекбокс **Не использовать AD**.



Адрес AD — введите в поле адрес вашего каталога Active Directory.

Каталоги пользователей — введите значение поля **distinguishedName** из списка атрибутов каталога. Например, `OU=demoapp.DC=presale.DC=local` .

> **Примечание**
>
> Если вам нужно указать больше одного каталога пользователей, обратитесь к представителю VK.

Логин администратора — введите в поле логин пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

Пароль администратора — вставьте в поле пароль пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

Поле свойства «Отчество» — если вы используете свойство **Отчество**, введите его значение в это поле.

Использовать шифрованное соединение (LDAPS) — есть возможность добавления сертификата LDAPS с помощью кнопки **Добавить сертификат**.

Игнорировать ошибки сертификата — если у вас самоподписанный SSL-сертификат, отметьте этот чекбокс.

Сбрасывать сессии пользователей при изменении пароля — если чекбокс отмечен, при изменении пароля пользователя в Active Directory будет сбрасываться сессия в VK WorkMail.

Использовать в качестве логина email вместо username — в текущей версии поле не используется.

Для применения настроек нажмите на кнопку **Сохранить**.

Если пользователи не появились в VK WorkMail, нужно проверить корректность настроек синхронизации с Active Directory с помощью консольной команды:

```
sudo journalctl -fu onpremise-container-adloader1.service
```

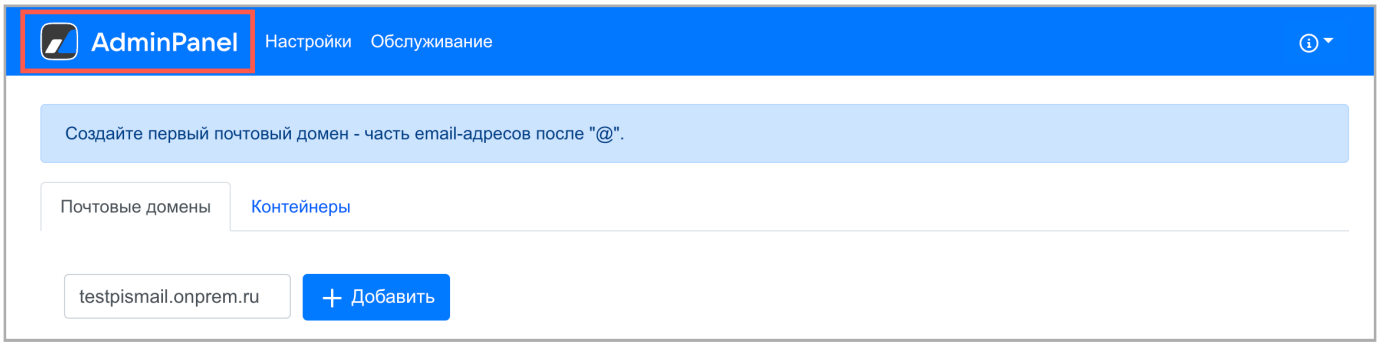
Дополнительная документация

Инструкция по установке обновлений на кластер — в документе содержится информация по обновлению VK WorkMail.

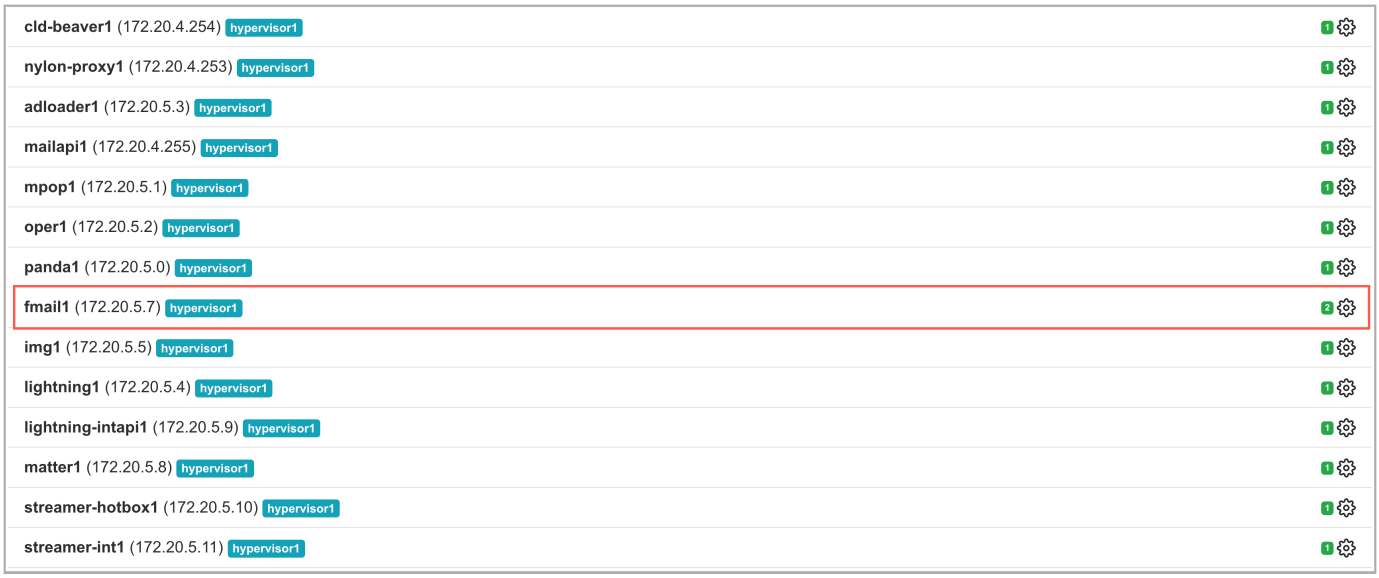
Приложение 1. При входе в панель администратора появляется ошибка «Неверный пароль»

Перепроверьте, что пароль скопирован верно. Чтобы просмотреть пароль, введите в консоли команду: `cat /home/deployer/VKWorkMail/bizOwner.pass`. Если пароль был правильным, а ошибка всё равно появилась, также необходимо сгенерировать новый пароль.

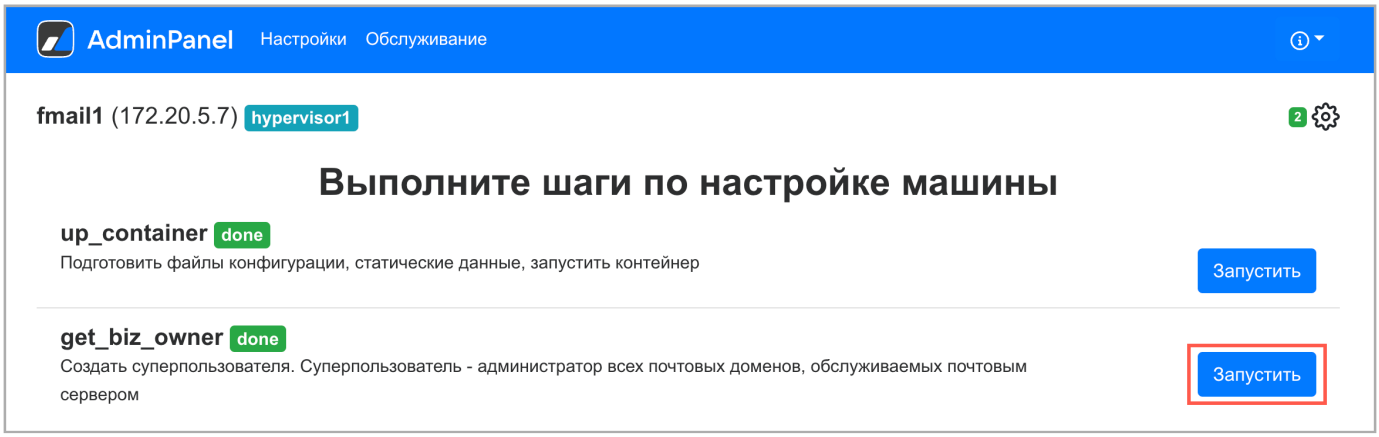
В веб-интерфейсе установщика перейдите к списку контейнеров, кликнув по логотипу **Admin Panel**



Найдите в списке контейнеров **fmail1** и нажмите на значок шестеренки справа от названия контейнера.



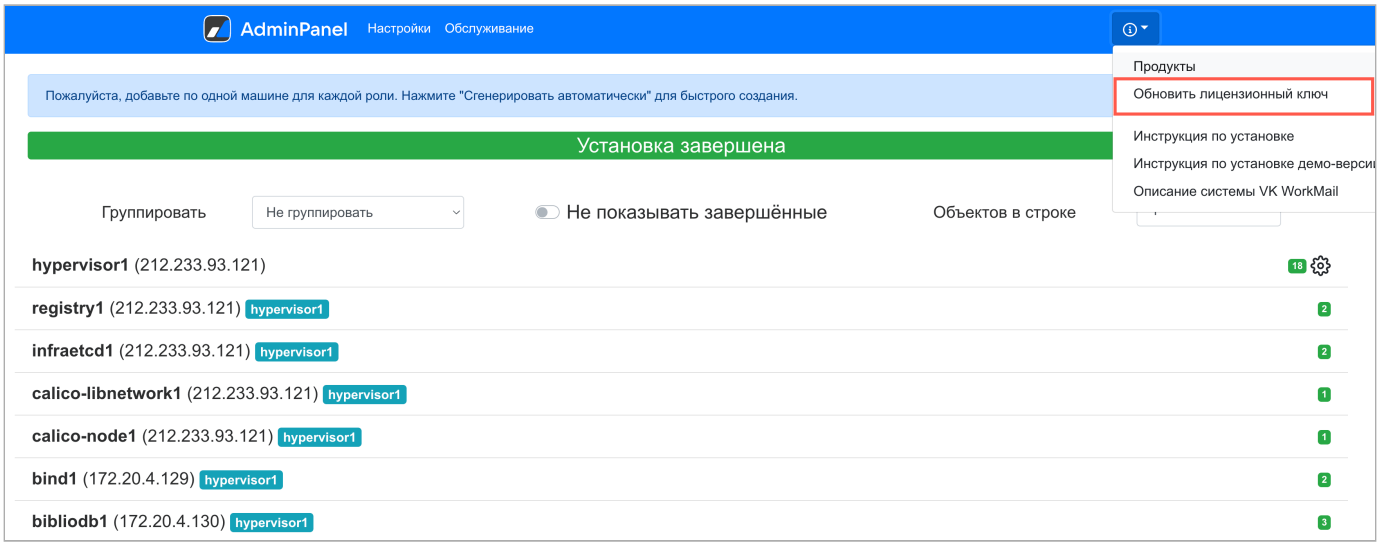
Запустите выполнение шага **get_biz_owner**.



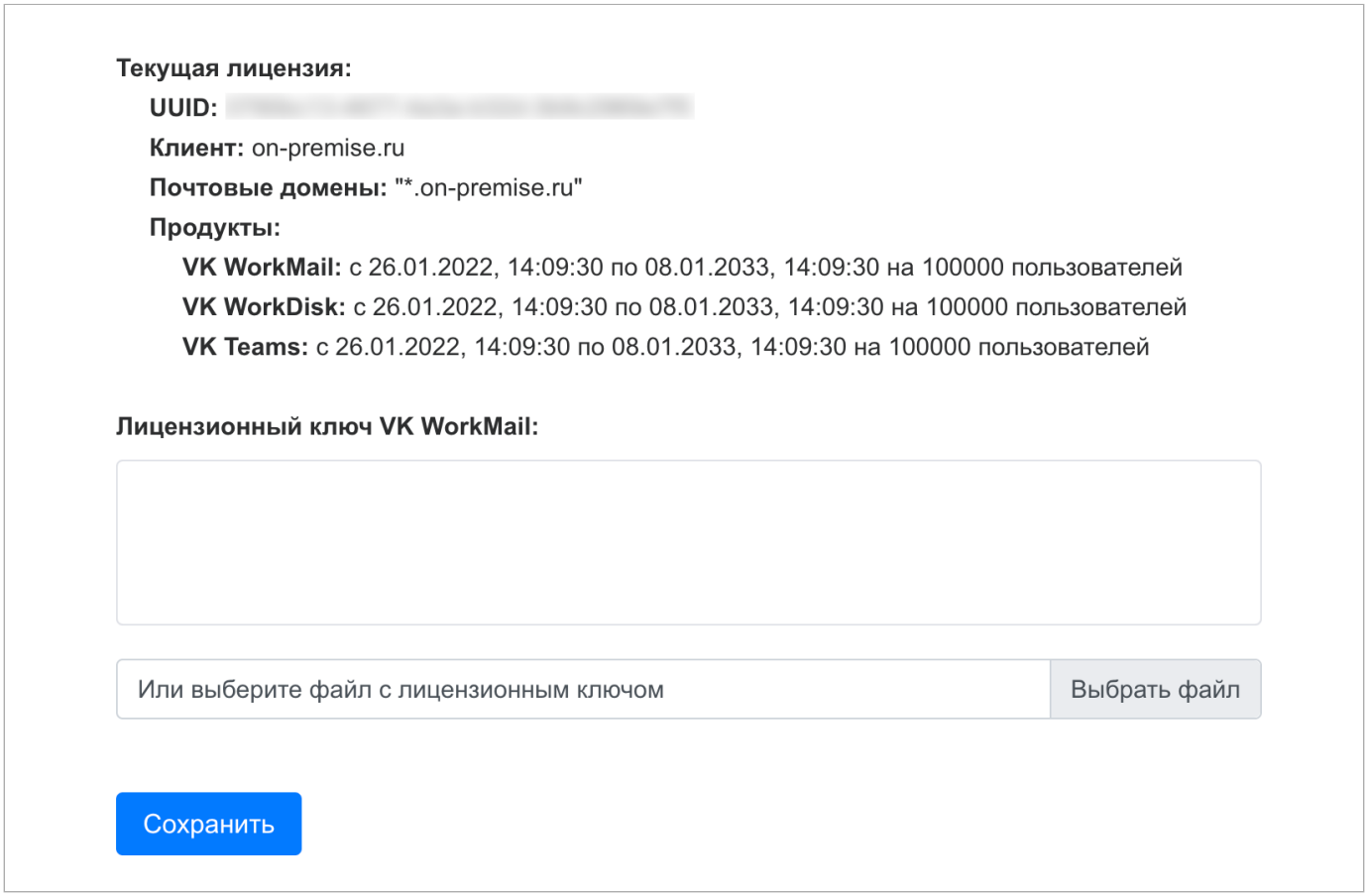
Дождитесь окончания выполнения шага, затем скопируйте новый пароль.

Приложение 2. Обновление лицензионного ключа

Если вам нужно обновить лицензионный ключ, нажмите на значок ⓘ и в выпадающем меню выберите **Обновить лицензионный ключ**.



В открывшемся окне вы сможете просмотреть информацию о текущих лицензиях, а также обновить лицензионный ключ.



Если вы вносили какие-либо изменения, кликните по кнопке **Сохранить**.

Приложение 3. Логи и полезные команды

Все команды, перечисленные ниже, следует выполнять в консоли машины-мониторинга.

1. Перезапуск установщика:

```
sudo systemctl restart deployer
```

2. Логи установщика:

```
sudo journalctl -fu deployer
```

3. Список запущенных контейнеров:

```
docker ps
```

4. Логи конкретного контейнера:

```
sudo journalctl -eu имя_контейнера
```

5. Статус контейнера:

```
systemctl status имя_контейнера
```

6. Посмотреть список «сломанных» контейнеров:

```
docker ps -a|grep Exit
```

7. Посмотреть список всех не запустившихся контейнеров:

```
sudo systemctl | grep onpremise | grep -v running
```

8. Удалить контейнер:

```
sudo docker rm имя_контейнера
```

Дата обновления документа: 18.03.2024