Почта VK WorkSpace

Установка версии 26.2 на кластер из 8 машин

Портал с документацией: https://biz.mail.ru/docs/on-premises/

Оглавление

Назначение документа

В документе описана процедура кластерной установки Почты. Минимальной отказоустойчивой конфигурацией для установки почтовой системы считается кластер на 8 машин.

Требования к администраторам

- Знание Linux на уровне системного администратора.
- Знание основ работы Систем управления базами данных (СУБД).
- Знание основ работы служб каталогов (Directory Service).
- Понимание основ контейнеризации.
- Знание основ работы сетей и сетевых протоколов.
- Знание основных инструментов для работы в командной строке: bash, awk, sed.
- Знание основ работы инфраструктуры доставки почты.

Дополнительная документация

Инструкция по установке обновлений на кластер

Что делать, если при входе в панель администратора появляется ошибка «Неверный пароль»

Как обновить лицензионный ключ

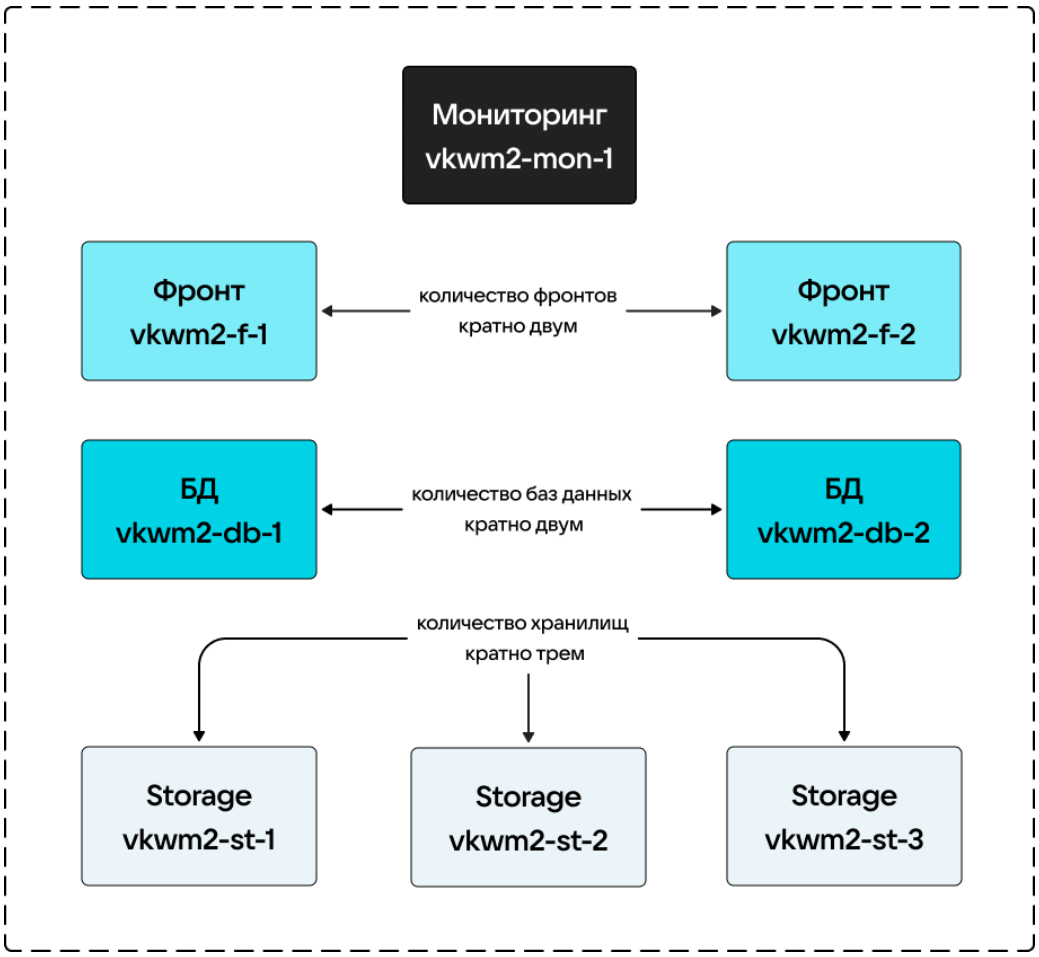
Установщик не может получить доступ до гипервизора

Настройка интеграции с LDAP-каталогами

Как настроить геораспределенную почту

Схема тестового кластера

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



Минимальная отказоустойчивая 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.

Дистрибутив Почты и файл `onpremise-deployer_linux` должны находиться на гипервизоре, отведенном под мониторинг.

Технические требования

Поддерживаемые операционные системы для установки Почты:

- **Astra Linux SE Орел** — версия 1.7.5+, версия ядра — **5.15**.
- **Astra Linux SE Орел** — версия 1.8, версия ядра — **6.1**.
- **РЕД ОС** — версия 7.3.5, версия ядра — **6.1**.
- **РЕД ОС** — версия 7.3c (сертифицированная), версия ядра — **6.1**.
- **РЕД ОС** — версия 8, версия ядра — **6.6** или **6.12**.
- **MosOS Arbat** — версия 15.5, версия ядра — **5.14**.

Архитектура системы — **x86_64**.

Обновлять операционную систему можно только на поддерживаемую версию и только после консультации с представителем VK. Список поддерживаемых ОС может быть уточнен в рамках работ по индивидуальному проекту.

> **Внимание**
>
> Чтобы Почта VK WorkSpace работала корректно, нужно установить оперативное обновление ядра ОС указанной выше версии. Версия должна быть актуальной на момент установки.

Как правильно настроить антивирус на серверах

На всех машинах проверьте антивирусное решение и выполните следующие настройки:

- Добавьте в исключения:
  - `/opt/mailOnPremise` — данные приложений, логи, БД, хранилища. Нельзя детализировать файлы и подкаталоги, нужно добавить весь каталог `/opt/mailOnPremise` в исключения.
  - `/home/deployer/` — данные для инсталлятора, установка обновлений.
  - Диски для хранилища.
  - `/var/lib/docker/`.
- Отключите проверку контейнеров: `ScanContainers: No, ContainerNameMask: *`.
- Не настраивайте firewall на следующие сетевые интерфейсы:
  - cali*
  - docker*
  - wireguard*
  - tun*
- Добавьте в исключения публичные порты из раздела Список портов для установки
- Если вы используете KESL, то на серверах для сервисов контейнеризации отключите задачи по защите от веб-угроз и защите от сетевых угроз.

> **Внимание**
>
> Не вносите изменения в правила iptables.

Пример настройки параметров ОС

> **Важно**
>
> Установка данных параметров возможна только после консультации с вашими системными администраторами.

1. Создайте файл `/etc/sysctl.d/98-vkworkspace.conf` с настройками sysctl:

```
kernel.pid_max=4194304
net.ipv4.tcp_tw_reuse=1
net.netfilter.nf_conntrack_tcp_timeout_time_wait=3
net.netfilter.nf_conntrack_tcp_timeout_fin_wait=5
net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=1
net.netfilter.nf_conntrack_max=4194304
net.ipv4.tcp_syncookies=1
net.ipv4.ip_forward=1
```

2. Создайте файл `/etc/security/limits.d/98-vkworkspace-limits.conf` с настройками лимитов:

```
*    hard nofile 1048576
*    soft nofile 131072
*    hard nproc  257053
*    soft nproc  131072
root hard nofile 1048576
root soft nofile 262144
root hard nproc  514106
root soft nproc  262144
```

Дополнительные настройки для сертифицированной РЕД ОС 7.3

Файл `/etc/sysctl.d/98-vkworkspace.conf` с настройками sysctl для сертифицированной РЕД ОС 7.3 будет отличаться:

```
kernel.pid_max=4194304
net.ipv4.tcp_tw_reuse=1
net.ipv6.conf.all.disable_ipv6=1
net.ipv6.conf.default.disable_ipv6=1
net.ipv6.conf.lo.disable_ipv6=1
net.ipv4.tcp_syncookies = 1
```

До установки Почты VK WorkSpace:

a. Внесите изменение в конфигурации `/etc/systemd/system.conf`:

```
DefaultLimitNOFILE=524288:524288
```

b. Установите следующие пакеты из репозитория РЕД ОС 7.3, поставляемого с операционной системой:

- docker-ce-cli-20.10.24-1.el7.x86_64
- docker-ce-rootless-extras-20.10.24-1.el7.x86_64
- docker-ce-20.10.24-1.el7.x86_64
- docker-ce-20.10.24-1.el7.i686
- docker-compose-2.29.2-1.el7.x86_64
- docker-compose-switch-1.0.5-1.el7.x86_64

Установить пакеты можно с помощью команды:

```
yum install docker-ce-cli-20.10.24-1.el7.x86_64 docker-ce-rootless-
extras-20.10.24-1.el7.x86_64 docker-ce-20.10.24-1.el7.x86_64 docker-
ce-20.10.24-1.el7.i686 docker-compose-2.29.2-1.el7.x86_64 docker-compose-
switch-1.0.5-1.el7.x86_64
```

Дополнительные настройки для MosOS Arbat

Установите docker 20.x и docker-compose из репозитория MosOS:

```
zypper install -y docker docker-compose bind-utils ncat
```

Дополнительные настройки для Astra Linux 1.8

До установки Почты VK WorkSpace:

a. В файле `/etc/default/grub`, в строку параметра `GRUB_CMDLINE_LINUX_DEFAULT` добавьте `parsec.execstack=1`:

```
GRUB_CMDLINE_LINUX_DEFAULT="parsec.mac=0 quiet net.ifnames=0 parsec.execstack=1"
```

b. Выполните команду `sudo update-grub`.

c. Перезагрузите машину.

3. Примените изменения:

```
sysctl -p /etc/sysctl.d/98-vkworkspace.conf
sysctl --system
```

Или перезагрузите операционную систему.

Требования к ресурсам серверов

Внимание

Требования ниже не учитывают работу антивируса, DLP и других дополнительных систем устанавливаемых на сервера. Требования учитывают только базовые функции, если вы хотите включить дополнительные **Продукты**, то предварительно проконсультируйтесь с представителем VK о дополнительных системных требованиях.

По вопросам создания сайзинг-модели специально для вашей компании обратитесь к представителям VK. Минимальные технические параметры для 8 машин:

- Установщик + мониторинг: 8 vCPU, 16 GB RAM, 200 GB SSD;
- Фронт №1: 16 vCPU, 40 GB RAM, 150 GB SSD;
- Фронт № 2: 16 vCPU, 40 GB RAM, 150 GB SSD;
- База данных №1: 16 vCPU, 20 GB RAM, 150 GB SSD;
- База данных №2: 16 vCPU, 20 GB RAM, 150 GB SSD;
- Хранилище №1: 8 vCPU, 16 GB RAM, 250 GB SSD;
- Хранилище №2: 8 vCPU, 16 GB RAM, 250 GB SSD;
- Хранилище №3: 8 vCPU, 16 GB RAM, 250 GB SSD.

Рекомендация

Используйте процессоры Intel Xeon Gold 6140 и новее.

Минимальные требования к SSD-дискам:

Операций чтения, IOPS	Операций записи, IOPS	Максимальная задержка операции, мс
10 000	5 000	< 1

Минимальные требования к локальным HDD-дискам:

Операций чтения, IOPS	Операций записи, IOPS	Максимальная задержка операции, мс
1000 — 2400	500 — 800	< 20

Локальные HDD-диски можно подключать только к некоторым компонентам Почты. Такие компоненты помечены в веб-интерфейсе установщика.

Проверка совместимости с другими типами СХД осуществляется индивидуально. Обратитесь к представителям VK за консультацией.

Как использовать системы виртуализации

Если вы используете системы виртуализации для развертывания серверов VK WorkSpace необходимо учитывать особенности выделения ресурсов:

vCPU

Не допускайте переподписку. Суммарные vCPU на хосте не должны превышать количество физических ядер, выделенных всем виртуальным машинам. При этом не рекомендуется считать Hyper-Threading полноценными ядрами.

Не выделяйте одной виртуальной машине количество ядер больше, чем количество ядер на физическом сокете.

RAM

Не назначайте суммарную vRAM выше физической RAM хоста.

Механизмы экономии памяти

Не включайте механизмы ballooning и сжатия памяти.

swap

Не используйте swap — как на гипервизоре, так и внутри виртуальных машин.

Резервирования ресурсов виртуальных машин

Устанавливайте всю выделенную память и процессоры в резерв для виртуальных машин системы.

Хранилище

Не используйте тонкие диски (диски типа Thin) — диски с отложенным выделением пространства.

Таблица совместимости

Технология	Версия
Мессенджер и ВКС	не старше двух последних версий
MS Exchange Server	2013/2016
Keycloak	17, с использованием OAuth 2.0
Kerberos	5
Р7-Офис	2024.4.2.721

Примечание

Keycloak является внешним провайдером аутентификационной информации (proxy) и не выступает в качестве полноценной IDM системы.

Предварительные условия

Представители VK предоставили вам следующие данные:

- Ссылку на скачивание дистрибутива Почты 26.2.
- Лицензионный ключ.
- Комплект документации.

Также вам потребуется:

- Набор DNS-записей: A, CNAME, MX, SPF, TXT, NS.

- Поддержка процессорами набора инструкций 3DNow, ADX, AES, AVX, AVX2, BMI, BMI2, CMOV, MMX, MODE64, NOT64BITMODE, NOVLX, PCLMUL, SHA, SSE1, SSE2, SSE41, SSE42, SSSE3 и XOP 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 10 GbE.
- Отключить swap.
- Сертификаты SSL для каждого CNAME или Wildcard-сертификат для домена.
- Доступ к портам: 25, 2525, 80, 143, 443, 465, 993, 1025.
- Доступ к административным портам: 22, 8888*.
- tar.
- Утилита для распаковки zip-архивов, например 7zip или unzip.
- Active Directory или другая служба каталогов, работающая по протоколу LDAP.

Чтобы обеспечить безопасность Почты, на ваших серверах должны быть доступны только необходимые порты. Для доступа к веб-интерфейсу: 80 (http), 443 (https). Для отправки и получения почты: 2525 (smtp), 25 (mx), 110 (pop3), 995 (pop3s), 143 (imap), 465(smtps), 993 (imaps). Вы должны сами определить, с каких IP-адресов будут доступны порты.

Порт 8888 используется сервисом deployer (установщик). Рекомендуется применять следующие наложенные средства защиты:

- Отдельный mTLS прокси-сервер с обязательной проверкой клиентских сертификатов. Управление ключами происходит посредством PKI заказчика.
- Использование (меж)сетевых экранов как на операционной системе сервера установщика, так и на активном сетевом оборудовании.
- Прокси-сервера для аутентификации и авторизации посредством простого пароля, Kerberos или доменного пароля.

Можно использовать несколько из перечисленных методов. Выбор метода осуществляется исходя из технических возможностей инфраструктуры и требований информационной безопасности.

Проверьте состояние SELinux

На каждом сервере проверьте текущее состояние SELinux:

```
sestatus
```

Параметр `SELinux status` должен иметь значение `disabled`. Если выводится другое значение:

1. Откройте для редактирования файл `/etc/selinux/config`.
2. Измените значение параметра `SELINUX` на `disabled`.

3. Перезагрузите операционную систему.
4. Повторно проверьте состояние SELinux с помощью команды `sestatus`.
5. Параметр SELinux status должен иметь значение disabled. SELinux будет отключен.

Как работать с Wildcard-сертификатами

Один wildcard-сертификат охватывает только один уровень поддоменов. Это означает, что wildcard-сертификат выпущенный для `domain.ru` будет действительным для всех его субдоменов третьего уровня, но не будет работать для четвертого. Соответственно если необходима защита поддоменов четвертого и далее уровней нужно получить отдельный wildcard-сертификат для родительского домена каждого из них. Например, домен для почты `mail.onprem.ru`, а домен для хранилища `mail-st.onprem.ru`, тогда в сертификат необходимо добавить шесть доменов:

- `*.mail.onprem.ru`
- `*.e.mail.onprem.ru`
- `*.cloud.mail.onprem.ru`
- `*.calendartouch.mail.onprem.ru`
- `*.calendarx.mail.onprem.ru`
- `*.mail-st.onprem.ru`

Какие протоколы использует Почта

- **SMTP**, **ESMTP** — протоколы отправки почтовых сообщений (порт 2525/465).
- **IMAP** — протокол получения почтовых сообщений (порт 143/993).
- **POP3** — протокол получения почтовых сообщений (порт 110/995).
- **HTTPS** для доступа к веб-интерфейсу почты с использованием **TLS**.
- **CalDAV** для синхронизации календаря.
- **CardDAV** для синхронизации и управления контактами.
- **WebDAV** для работы с Диском.
- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента.
- **IP in IP** — протокол туннелирования IP.

Защита сетевых соединений

Для защиты сетевых соединений между серверами, виртуальными машинами и контейнерами почтовой системы используется ПО WireGuard.

Обязательные предварительные действия

Настройте ротацию логов в journald

Выполните шаги из инструкции Как настроить ротацию логов в journald.

Создание DNS-записей

Для работы Почты вам нужны:

- MX-запись (рекомендуемый приоритет — 10), которая обязательно ведет на `mxs.<домен для почты>`
- Два основных домена: для почты и для хранилищ.
- Набор A- или CNAME-записей.

> **Примечание**
>
> В случае кластерной установки есть минимум две виртуальные машиные выделенные под фронт. Поэтому вам нужно обеспечить резолвинг всех доменных имен в IP-адреса машин, выделенных под фронт. Резолвингом называется процесс получения IP-адреса по символическому имени. Например, вы можете создать две A-записи с одинаковыми именем, но разными IP-адресами от машин под фронт.

Для примера в документе будут использоваться следующие DNS-записи:

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

> **Внимание**
>
> 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 таблицах представлен список A- или CNAME-записей, которые нужно создать перед установкой сервиса Почта. Домены из таблиц должны являться поддоменами для двух основных.

Для почты:

Как создается домен: `account` (субдомен из таблицы) + `mail.onprem.ru` (основной домен из примера, который вы замените своим) = `account.mail.onprem.ru`.

Назначение домена	Имя домена	Пример
Веб-интерфейс авторизации	account	account.mail.onprem.ru
Домен для проверки доступа	access	access.mail.onprem.ru
Домен для аккаунт-сервиса	as	as.mail.onprem.ru
Скачивание вложений Почты	af	af.mail.onprem.ru
Просмотр вложений Почты	apf	apf.mail.onprem.ru
Доменная авторизация (внутренних запросов браузера)	auth	auth.mail.onprem.ru
Домен для панели расширенного просмотра действий пользователей	becca	becca.mail.onprem.ru
Интерфейс администрирования	biz	biz.mail.onprem.ru
Blobcloud-аттачи	blobcloud.e	blobcloud.e.mail.onprem.ru
Домен для BMW gRPC запросов	bmw	bmw.mail.onprem.ru
Капча	c	c.mail.onprem.ru
Домен для gRPC-запросов Календаря	calendargrpc	calendargrpc.mail.onprem.ru
Календарь	calendar	calendar.mail.onprem.ru
Домен интерфейса календаря для Супераппа VK WorkSpace	calendarmsg	calendarmsg.mail.onprem.ru
Мобильный календарь	shared.calendartouch	shared.calendartouch.mail.onprem.ru

Назначение домена	Имя домена	Пример
Статические данные календаря	shared.calendarx	shared.calendarx.mail.onprem.ru
VK WorkDisk	cloud	cloud.mail.onprem.ru
Загрузка файлов в VK WorkDisk	cld-uploader.cloud	cld-uploader.cloud.mail.onprem.ru
Скачивание файлов в веб-интерфейсе VK WorkDisk	cloclo.cloud	cloclo.cloud.mail.onprem.ru
Загрузка файлов в VK WorkDisk	cloclo-upload.cloud	cloclo-upload.cloud.mail.onprem.ru
Интеграция с API VK WorkDisk	openapi.cloud	openapi.cloud.mail.onprem.ru
Загрузка файлов в публичные папки в VK WorkDisk	pu.cloud	pu.cloud.mail.onprem.ru
Портальная авторизация VK WorkDisk	sdc.cloud	sdc.cloud.mail.onprem.ru
Загрузка больших почтовых вложений в VK WorkDisk	uploader.e	uploader.e.mail.onprem.ru
Превью файлов в VK WorkDisk	thumb.cloud	thumb.cloud.mail.onprem.ru
Веб-интерфейс Почты	e	e.mail.onprem.ru
Сервис аватарок	filin	filin.mail.onprem.ru
IMAP Почты	imap	imap.mail.onprem.ru
Неисполняемые статические данные	img	img.mail.onprem.ru
Исполняемые статические данные	imgs	imgs.mail.onprem.ru

Назначение домена	Имя домена	Пример
MX Почты	mxs	mxs.mail.onprem.ru
OAUTH2-авторизация	o2	o2.mail.onprem.ru
Общепортальные сервисы авторизации	portal	portal.mail.onprem.ru
POP3 Почты	pop	pop.mail.onprem.ru
Сервер авторизации (межсерверные запросы)	swa	swa.mail.onprem.ru
Webdav	webdav.cloud	webdav.cloud.mail.onprem.ru
Доска VK Workspace	board	board.mail.onprem.ru
Серверное взаимодействие с Диском VK WorkSpace	cloud-serverside-api	cloud-serverside-api.mail.onprem.ru
Серверное взаимодействие с Почтой VK WorkSpace	serverside-api	serverside-api.mail.onprem.ru
Сохранение файлов из Мессенджера и ВКС в Диск VK WorkSpace	cloclo-int	cloclo-int.mail.onprem.ru
Домен для скачивания супераппа VK WorkSpace	dl	dl.mail.onprem.ru
Адрес клиентского API Мессенджера и ВКС	u	u.mail.onprem.ru

Для хранилищ:

Как создается домен: `tmpatt` (субдомен из таблицы) + `mail-st.onprem.ru` (основной домен из примера, который вы замените своим) = `tmpatt.mail-st.onprem.ru`.

Назначение домена	Имя домена	Пример
Скачивание исполняемых вложений Почты	af	af.mail-st.onprem.ru

Назначение домена	Имя домена	Пример
Проксирование активного контента вложений Почты	ampproxy	ampproxy.mail-st.onprem.ru
Просмотр исполняемых вложений Почты	apf	apf.mail-st.onprem.ru
Защита от XSS-атак при скачивании файлов из VK WorkDisk	cloclo	cloclo.mail-st.onprem.ru
Скачивание больших почтовых вложений из VK WorkDisk	cloclo-stock	cloclo-stock.mail-st.onprem.ru
Распаковка архивов в интерфейсе VK WorkDisk	cld-unzipper	cld-unzipper.mail-st.onprem.ru
Интеграция с API Почты	corsapi	corsapi.mail-st.onprem.ru
Проксирование внешних вложений Почты	proxy	proxy.mail-st.onprem.ru
Домен для текстового редактора Р7-Офис	docs	docs.mail-st.onprem.ru
Облако, реализующее S3 API	hb	hb.mail-st.onprem.ru
Облако временных вложений Почты	tmpatt	tmpatt.mail-st.onprem.ru
Домен для Grafana	grafana	grafana.mail-st.onprem.ru

Внимание

Изменять доменные имена из таблицы запрещено! Установщик сервиса Почта 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>
```

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

Список портов для установки

Чтобы обеспечить безопасность Почты, на ваших серверах должны быть доступны только необходимые порты. Для доступа к веб-интерфейсу: 80 (http), 443 (https). Для отправки и получения почты: 2525 (smtp), 25 (mx), 110 (pop3), 995 (pop3s), 143 (imap), 465(smtps), 993 (imaps). Вы должны сами определить, с каких IP-адресов будут доступны порты.

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращаетс
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 инфраструктурные	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращает
			данные, например настройки сети		
TCP	8080	cadvisor	Инструмент снятия телеметрии с контейнеров	Сбор метрик prometheus	victoria-metrics
TCP	9100	node-exporter	Инструмент снятия телеметрии с гипервизоров	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	Установщик (on-premise deployer)
TCP	50051	optimus-agent	Агент отвечающий за автоматизирванную проверку инфраструктуры перед началом установки/ обновления.	Проверка ядра и портов	Установщик (on-premise deployer)
TCP	179	Bird	Calico. Работа BGP сессиий	–	Между всеми серверами системы
TCP	8888		Приложения для установки и		Администратор

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
		onpremise-deployer	начальной настройки VK WorkSpace	Подключение администраторов	
UDP	2003	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры

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

Шаг 1. Создайте пользователя deployer

При кластерной установке вам нужно создать пользователя deployer и скопировать ssh-ключи на всех виртуальных машинах в кластере. Необязательно добавлять один и тот же ssh-ключ, главное, чтобы ВМ с установщиком имела доступ по ssh к другим ВМ в кластере. Ниже алгоритм, который надо выполнить на ВМ с установщиком. На остальных машинах нужно создать пользователя deployer и скопировать ssh-ключи. `/home/deployer/.ssh` и `/home/deployer/.ssh/authorized_keys` должны быть с правами 600

1. 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 пользователем deployer
sudo -i -u deployer

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

# Копируем ssh-ключ в нужную директорию
cat /home/deployer/.ssh/id_rsa.pub >> /home/deployer/.ssh/authorized_keys

chmod 600 /home/deployer/.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 /home/deployer/.ssh/id_rsa.pub >> /home/deployer/.ssh/authorized_keys

chmod 600 /home/deployer/.ssh/authorized_keys

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

exit
```

MosOS Arbat

```
sudo -i

# Задаем пароль и создаем пользователя deployer

DEPLOYER_PASSWORD=xJ9JrmURvn

groupadd deployer
useradd -p "$(openssl passwd -crypt "$DEPLOYER_PASSWORD")" deployer
usermod -aG wheel deployer

# MosOS автоматически не создает группу для нового пользователя
```

```
usermod -aG deployer deployer
mkdir -p /home/deployer/.ssh
chown deployer:deployer /home/deployer/.ssh

ssh-keygen -t rsa -f /home/deployer/.ssh/id_rsa -N ""
# Нажимаем Enter (согласиться с вариантом по умолчанию)

# Копируем ssh-ключ в нужную директорию
cat /home/deployer/.ssh/id_rsa.pub >> /home/deployer/.ssh/authorized_keys

chmod 600 /home/deployer/.ssh/authorized_keys
chown deployer:deployer /home/deployer/.ssh
chown deployer:deployer /home/deployer/.ssh/*


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

exit
```

> **Внимание**
>
> Вся дальнейшая установка будет производиться под созданным пользователем deployer. Если вы планируете устанавливать под другим пользователем, это необходимо учитывать при дальнейшей установке. Также пользователь должен иметь права администратора.

2. Выполните команду `sudo visudo`.
3. В файле `/etc/sudoers` уберите **#** в начале следующей строки:

Astra Linux

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

РЕД ОС

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

MosOS Arbat

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

4. Выйдите 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
```

Шаг 2. Распакуйте дистрибутив

1. Распакуйте дистрибутив под пользователя deployer (в директорию `/home/deployer`). Вы можете распаковать архив с дистрибутивом и в другую папку или создать подпапку. Нет разницы, каким архиватором пользоваться. Ниже приведен пример для **unzip**:

   Astra Linux

   ```
   # Если на машину не установлен unzip, скачиваем его:
   sudo apt-get install unzip

   export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

   unzip -o <имя_архива>
   ```

   РЕД ОС

   ```
   # Если на машину не установлен unzip, скачиваем его:
   sudo yum install unzip

   # Если в вашей версии РЕД ОС нет yum, то используйте dnf

   export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

   unzip -o <имя_архива>
   ```

   MosOS Arbat

   ```
   # Если на машину не установлен unzip, скачиваем его:
   sudo zypper install unzip

   export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

   unzip -o <имя_архива>
   ```

2. Создайте рабочую директорию для установщика:

   ```
   mkdir -p /home/deployer
   cd /home/deployer
   ```

3. Распакуйте основной архив deployer.tar:

   ```
   tar -xf deployer.tar
   ```

4. Создайте директорию для статики и распакуйте архив:

   ```
   tar -xf static.tar.gz
   ```

5. Подготовьте Docker-репозиторий

```
cp registry/mail/dockerRepo.tar source/
cp registry/mail/dockerDMZRepo.tar source/
```

6. Скопируйте файлы md5:

```
cp registry/mail/dockerRepo.md5 source/
cp registry/mail/dockerDMZRepo.md5 source/
```

Шаг 3. Разрешите Port Forwarding

Для корректной работы установщика в настройках SSH на всех машинах должен быть разрешен TCP Forwarding. Чтобы изменить настройку TCP Forwarding, нужно в файле `/etc/ssh/sshd_config` установить следующее значение:

```
AllowTcpForwarding yes
```

Шаг 4. Запустите установщик как сервис

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

> **Важно**
>
> Для подключение администратора к веб-интерфейсу установщика используется порт 8888. Рекомендуется настроить защиту порта через firewall либо наложенными средствами (TLS-proxy).
>
> Не рекомендуется оставлять установщик включенным, если вы не проводите работы по установке и настройке системы. Запустили установщик → Провели установку → Выключили установщик. Если нужна донастройка системы, то снова включите установщик.

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

```
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

```
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>
```

MosOS Arbat

```
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>
```

Примечание

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

Если веб-интерфейс не открывается по адресу `http://server-ip-address:8888`, то проверьте журналы:

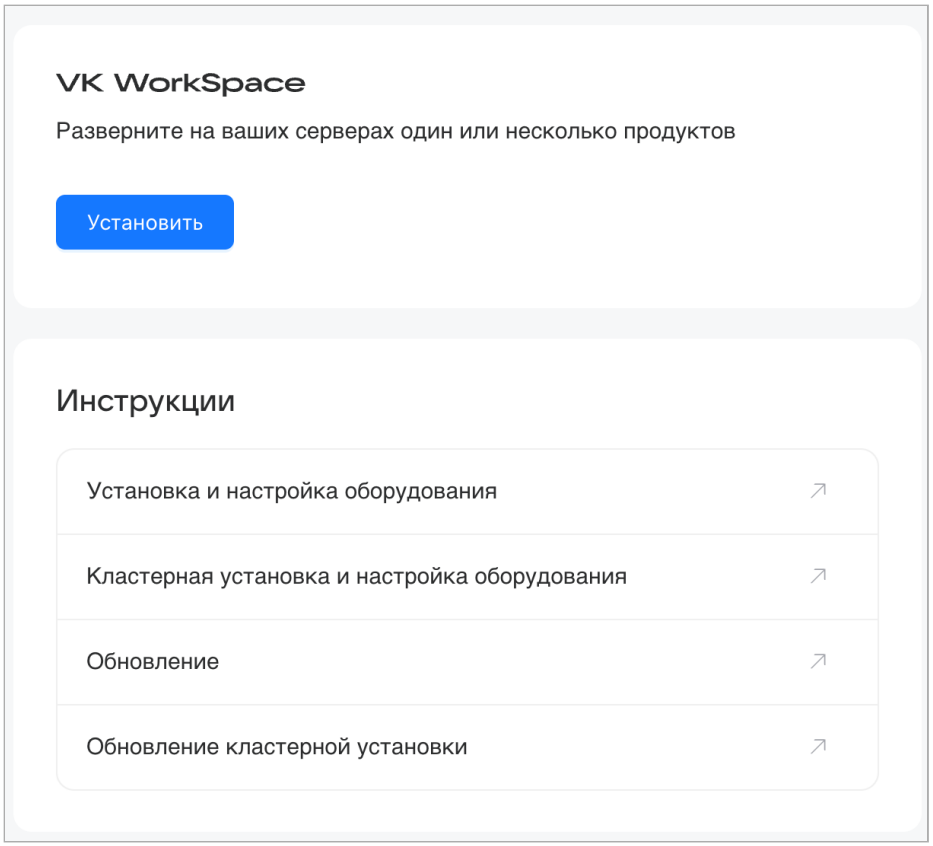
```
journalctl -u deployer
```

И убедитесь, что порт 8888 слушают:

```
ss -lanp|grep :8888
```

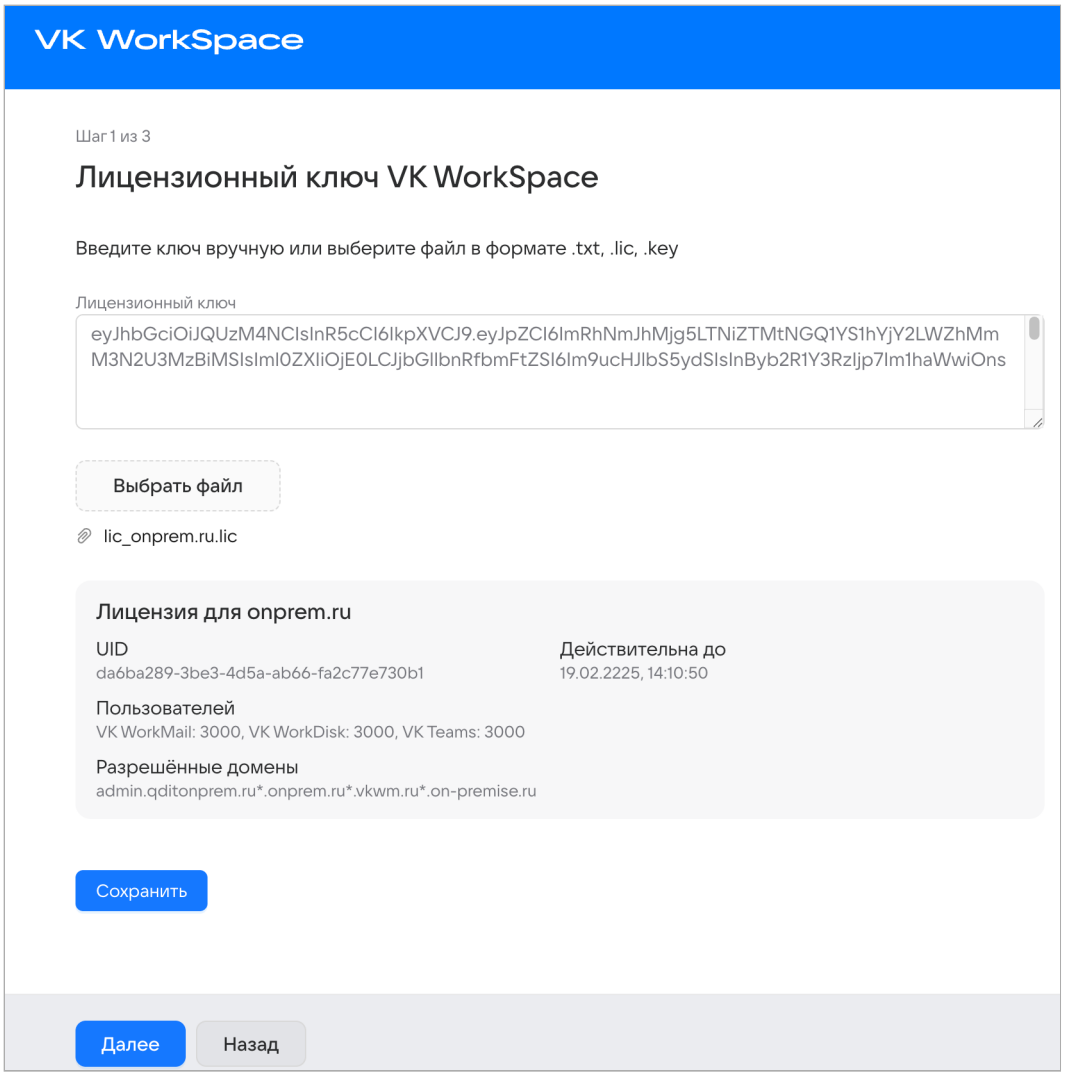
Действия в веб-интерфейсе установщика

1. Перейдите в веб-интерфейс установщика, в адресной строке браузера укажите адрес: `http://server-ip-address:8888`. Если перейти по этому адресу не удается, убедитесь, что firewall был отключен.
2. На стартовой странице нажмите на кнопку **Установить**.



Шаг 1. Добавьте лицензионный ключ

1. Введите лицензионный ключ или укажите путь к файлу лицензии **.lic**.



2. Нажмите кнопку **Сохранить**.
3. Нажмите на кнопку **Далее**.

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

Шаг 2. Выберите продукты и компоненты

1. Включите флаги **Диск VK WorkSpace** и **Почта VK WorkSpace**.
2. Нажмите на кнопку **Далее**.
3. Включите нужные вам компоненты в разделе **Почта VK WorkSpace**.

> **Внимание**
>
> Если вы хотите настроить геораспределенную почту, то обязательно включите ее сразу. При этом одновременно с **Распределённой инсталляцией** нельзя включить продукт **Интеграция с другими инсталляциями VK WorkMail**.

Для функционирования распределенной инсталляции необходимо, чтобы продукт был включен на всех инсталляциях, которые вы хотите объединить. И он должен быть включен при первичной установке. Если вы включите продукт после установки, то инструкция по настройке геораспределенной почты не сработает.

Продукт	**Описание**
Система Antispam	Комплекс сервисов, анализирующих письма и помечающих их как спам. Подробнее: Как включить Антиспам систему
Система доставки обновлений антиспама	Сервис обновления сигнатурных баз Антиспама с серверов VK
Календарь	**Обязательный продукт**. Продукт VK WorkSpace для управления календарями и событиями
Календарь. Миграция календарей по протоколу EWS	Миграция календарей пользователей из внешних систем для работы в VK WorkSpace. Миграция производится по протоколу EWS
Календарь. Интеграция календаря с TrueConf (сервер)	
Календарь. Интеграция календаря с TrueConf (плагин)	Для создания ссылок на звонки TrueConf при планировании встреч
Календарь. Бот календаря для мессенджера VK WorkSpace	Настройки для автоматической отправки уведомлений о событиях Календаря в бот мессенджера VK WorkSpace
Календарь. Планшеты для переговорных комнат Extron	Бронирование и управление переговорными комнатами через планшеты Extron в Календаре VK WorkSpace
Поддержка протокола CardDAV	Синхронизации контактов между почтовой системой и клиентскими приложениями
API больших вложений VK WorkMail	**Обязательный продукт**. Набор сервисов для хранения больших вложений почты
Система расширенных транспортных правил	Настройки для управления потоками входящих и исходящих писем в целях усиления безопасности

Продукт	Описание
Внешняя зона (DMZ)	Опция включает возможность создавать сервера для размещения их в DMZ-зоне. DMZ (Demilitarized Zone) — это изолированный сегмент сети, который находится между внешней (интернет) и внутренней (доверенной) сетью организации. Служит для размещения общедоступных сервисов, таких как веб-серверы, почтовые серверы и DNS-серверы, что позволяет минимизировать риски для внутренних ресурсов и сервисов
Управление размерами ящиков и политиками хранения писем в почтовых ящиках	**Beta**. Назначение групповых политик хранения на отдельные группы пользователей
Импорт данных из Microsoft Exchange	Сервис получения из MS Exchange in-place архивов, пользовательских правил обработки почты из MS Exchange
Распределённая инсталляция	Возможность настройки связей между отдельно развёрнутыми инсталляциями для управления маршрутизацией почты, просмотра занятости пользователей в календарях и объединения контактов в общую адресную книгу. Неприменимо для инсталляции, развёрнутой в минимально рабочей конфигурации на одной виртуальной машине. Подробнее: Геораспределенная Почта VK WorkSpace
Поддержка режима катастрофоустойчивости 2 ЦОД + witness	Дает возможность установить VK WorkSpace в катастрофоустойчивой конфигурации на двух ЦОД и дополнительном сервере, не находящемся в этих двух ЦОД
Экспорт событий во внешний брокер (Kafka)	Позволяет настроить экспорт событий во внешнюю Kafka для дальнейшей аналитики
Редактирование данных в AD	**Beta**. Сервис редактирования данных в Active Directory
Управление автоудалением писем	**Beta**. Настройки управления автоматическим удалением писем

Продукт	Описание
Бот новых почтовых сообщений для для мессенджера VK WorkSpace	Уведомления о новых полученных письмах будут отправляться в бот мессенджера VK WorkSpace
Автоматическое удаление старых писем	**Deprecated**. Дает возможность настраивать автоматическое удаление старых писем. Устаревшая функциональность
Компактная версия некоторых сервисов	Компактная версия сервисов, обрабатывающих почтовые очереди
Интеграция с другими инсталляциями VK WorkSpace	**Deprecated**. Устаревшая версия георасспределенной Почты VK WorkSpace. Не поддерживается и не рекомендуется к включению
Поиск писем во всех ящиках	Опция поиска и удаления писем во всех ящиках в интерфейсе Адмнинпанели
Поддержка протокола POP3	
Система отправки push-уведомлений на мобильные устройства	
Анализ логов доставки почты	**Beta**. Набор сервисов для логирования почты. Хранит в базе данных сведения о получателе, отправителе, теме письма и времени прохождения сообщения через сервера внутри установки

Примечание

Есть компоненты, настройка которых производится в административной панели (`biz.<почтовый домен>`), но включить их нужно при установке. Например, **Система расширенных транспортных правил** и **Система миграции Диска VK WorkSpace из внешних сервисов**.

4. Нажмите на кнопку **Далее**.
5. Включите нужные вам компоненты в разделе **Диск VK WorkSpace**.

Продукт	Описание
Система миграции Диска VK WorkSpace из внешних сервисов	**Beta**. После включения опции появится возможность мигрировать в VK WorkSpace файлы из Microsoft OneDrive, Google Drive, NextCloud
Система проверки файлов Диска через DLP	**Beta**. Настройки дополнительной проверки файлов Диска с помощью внешней DLP-системы для повышения уровня безопасности
Интеграция с антивирусом по протоколу ICAP	Дает возможность интегрировать сторонние антивирусные системы с VK WorkSpace

6. Нажмите на кнопку **Далее**.
7. Включите нужные вам компоненты в разделе **Административная панель**.

> **Внимание**
>
> Для инсталляций до 100000 пользователей необходимо включить облегченную версию аудита на PostgreSQL. По умолчанию в Почте включен продукт **Система аудита действий пользователя** на основе ScyllaDB, она предназначена для инсталляций, где пользователей больше 100000.

Продукт	Описание
Аутентификация v26.2.0	**Обязательный продукт**. Настройка способов входа и защиты аккаунтов
Аутентификация v26.2.0. Единый вход (SSO)	Вход в систему через внешний сервис идентификации (IdP)
Аутентификация v26.2.0. Вход через Kerberos	Вход через Kerberos для пользователей корпоративной сети
Вход через Kerberos. Blitz (внешний)	**Beta**
Вход через Kerberos. Keycloak (внутри инсталляции) v17.0.1	
Вход через Kerberos. Keycloak (внешний)	
	Дополнительная проверка личности при входе

Продукт	Описание
Аутентификация v26.2.0. Двухфакторная аутентификация	
Двухфакторная аутентификация. Коды подтверждения в VK WorkSpace	Получение кодов подтверждения в VK WorkSpace при входе в систему
Аудит действий пользователя	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)
Аудит действий пользователя. Дублирование действий пользователей во внешние хранилища	Нужно, чтобы хранить историю операций пользователей отдельно от почтовой системы
Система BI-аналитики	**Beta**
Система BI-аналитики. Kafka внутри инсталляции	16 GB RAM, 8 vCPU
Консолидация серверов Tarantool	Переключает тарантулы выбранных групп на консолидированные
Базы Данных	Включение обратной совместимости с версиями VK WorkSpace для определенных сервисов, ранее поддерживающих только работу с MySQL.
Базы Данных. Использовать MySQL	
Инструменты разработки	Включает дополнительные сервисы для тестирования системы, например, генерирование аккаунтов
Поддержка Российских криптографических стандартов (ГОСТ TLS)	**Beta**. Позволяет VK WorkSpace работать с российскими криптографическими стандартами: ГОСТ Р 34.12-2015 (шифрование) и ГОСТ Р 34.10-2012 (электронные подписи). Это необходимо для обеспечения безопасного соединения
Система групповых политик	**Beta**

Продукт	Описание
Система групповых политик. Kafka внутри инсталляции	16 GB RAM, 8 vCPU
Встроенное хранилище образов контейнеров	Хранения образов контейнеров почтовой системы внутри вашей инфраструктуры
VK Kubernetes	**Beta**. Возможность развертывания в среде контейнеризации Kubernetes
Резервное копирование (бэкап)	Средства резервного копирования данных диска, почты, календарей, профилей пользователей и адресных книг
Мониторинг	Набор сервисов, обеспечивающих хранение метрик сервисов в базе данных Prometheus и визуализацию данных с помощью Grafana
Мониторинг. Экспортер метрик из Victoria Metrics в Zabbix	Сервис, обеспечивающий отправку данных из Victoria Metrics и Node Exporter в Zabbix
Сбор и отправка метрик	Сборщики и трансляторы Graphite и Prometheus-метрик
Прогноз и контроль объёма почтового хранилища	**Beta**. Мониторинг заполнения хранилища почты
Интеграция с редактором «МойОфис» по протоколу WOPI	
Отменить проверку контейнеров OneDB после запуска	
Редактор «Р7-Офис» внутри инсталляции	Позволяет использовать встроенный в VK WorkSpace редактор «Р7-Офис». Требует дополнительных ресурсов системы
Интеграция с редактором «Р7-Офис» по протоколу WOPI	
Аудит действий пользователя (облегчённая версия)	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (PostgreSQL)

Продукт	Описание
Аудит действий пользователя (облегчённая версия). Дублирование действий пользователей во внешние хранилища	Нужно, чтобы хранить историю операций пользователей отдельно от почтовой системы
Ядро объектного хранилища S3	**Обязательный продукт**. Сервисы, обеспечивающие хранение любых неструктурированных данных по протоколу S3
Ядро объектного хранилища S3. Ядро распределённого файлового хранилища	**Обязательный продукт**. Отвечает за логику распределения данных по узлам, целостность и отказоустойчивость хранилища
Интеграция почты с мессенджером VK WorkSpace	

8. Нажмите на кнопку **Далее**.

Шаг 3. Добавьте гипервизоры (серверы)

В релизе 26.2 появилась возможность использовать готовые шаблоны для создания кластерных инсталляций продуктов VK WorkSpace. Шаблоны позволяют автоматизировать следующие шаги при установке:

- Шаг 6. Установка гипервизоров.
- Шаг 7. Распределение контейнеров по гипервизорам.

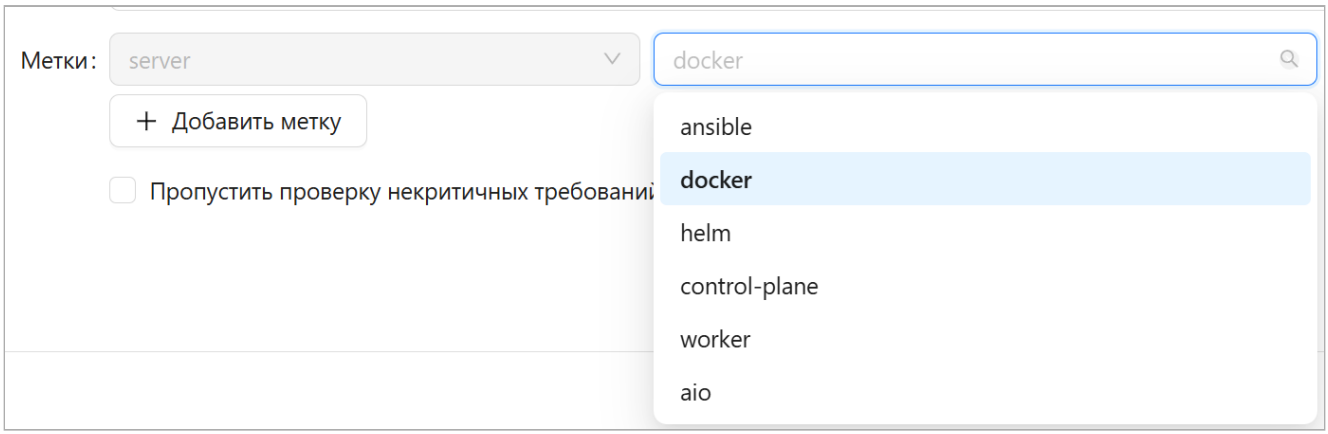
Ниже будут описаны шаги для ручной настройки машин и для шаблонов.

Установка вручную

1. Переключитесь на вкладку **Ручная настройка**.
2. Нажмите на кнопку **Добавить**.
3. Заполните поля:
   - **IP-адрес** — адрес машины, на которую производится установка.
   - **Имя сервера** — укажите имя сервера (гипервизора) или оставьте поле пустым. В случае если вы оставите поле незаполненным, имя гипервизора будет взято из `hostname -s` и добавится автоматически. В документации будет использовано имя **hypervisor1**.

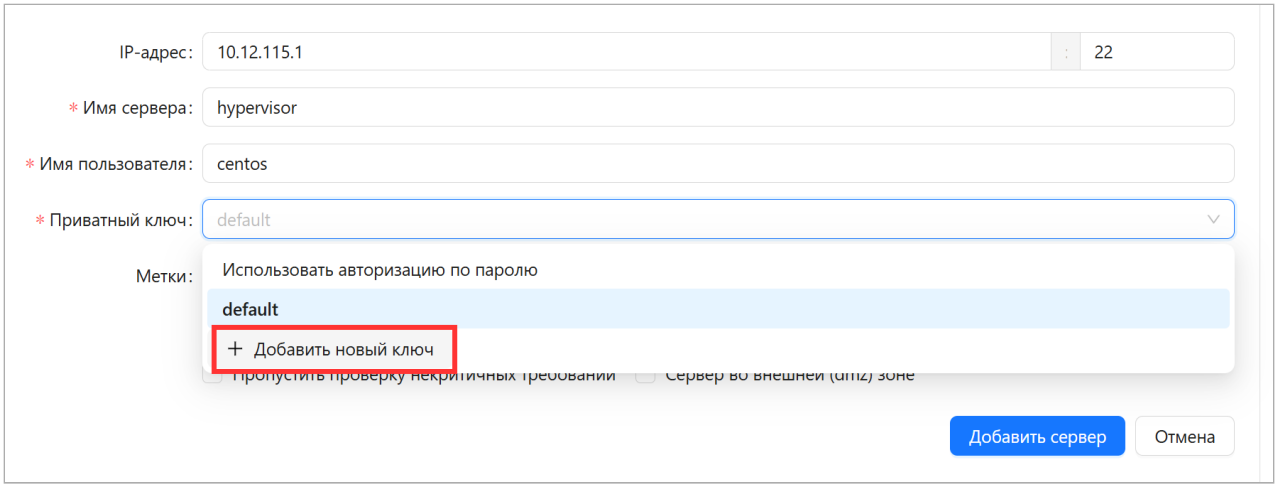
- **Имя пользователя** — укажите имя того пользователя, под которым запущен установщик. В рассматриваемом примере это пользователь deployer.

4. В поле **Метки**, напротив **server**, в выпадающем меню выберите опцию **docker**.



5. Добавьте **SSH-ключ**, сгенерированный на машине с установщиком:

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



   b. В поле **Имя ключа** введите название ключа для его дальнейшей идентификации, например: **deployerRSA**.

   c. Перейдите в консоль.

   d. Выполните команду `cat ~/.ssh/id_rsa` и скопируйте ключ.

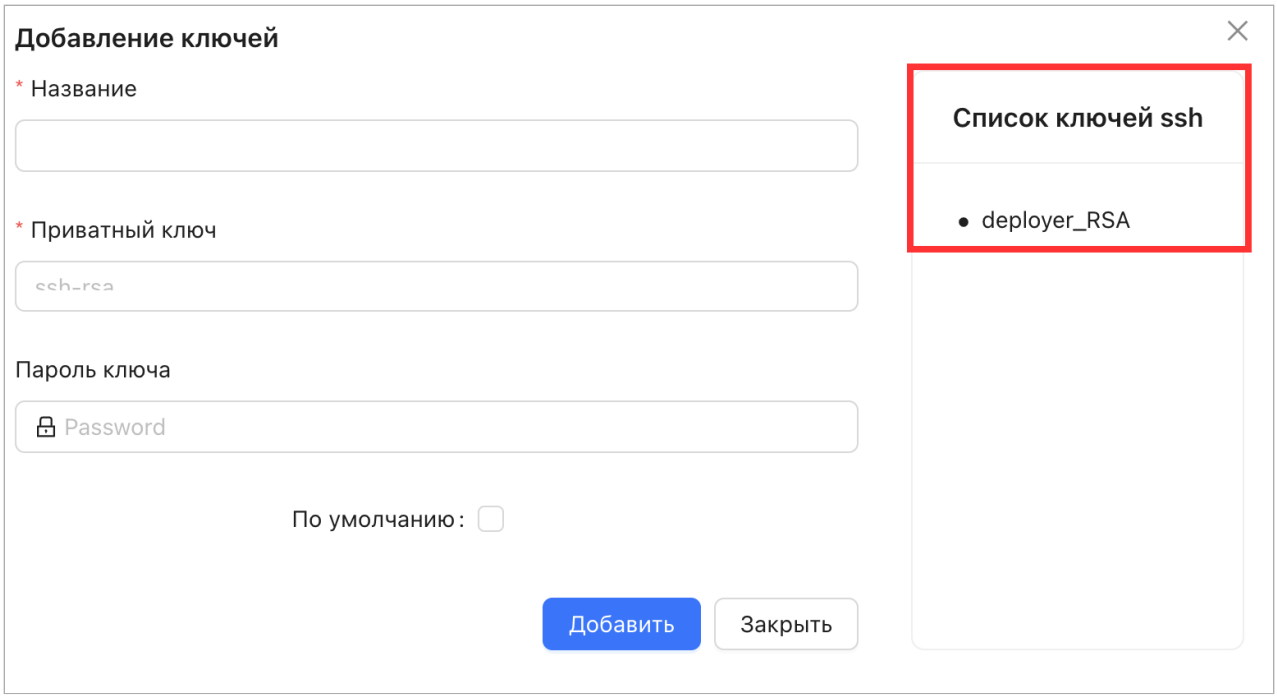
   e. Затем вставьте его в поле **Приватный ключ**. Его нужно указать полностью, включая:

   `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`

   f. Поле **Пароль ключа** оставьте пустым.

   g. Кликните по кнопке **Добавить**.

   h. Новый ключ должен отобразится в панели справа.



i. Нажмите **Закрыть**.

6. Оставьте чекбокс **Сервер во внешней (dmz) зоне** пустым.
7. После заполнения полей нажмите на кнопку **Добавить сервер** — 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.

8. Аналогичным образом добавьте еще 7 гипервизоров:
   - 2 — под фронты,
   - 2 — под базы данных,
   - 3 — под хранилища.
9. Нажмите **Далее** внизу страницы.

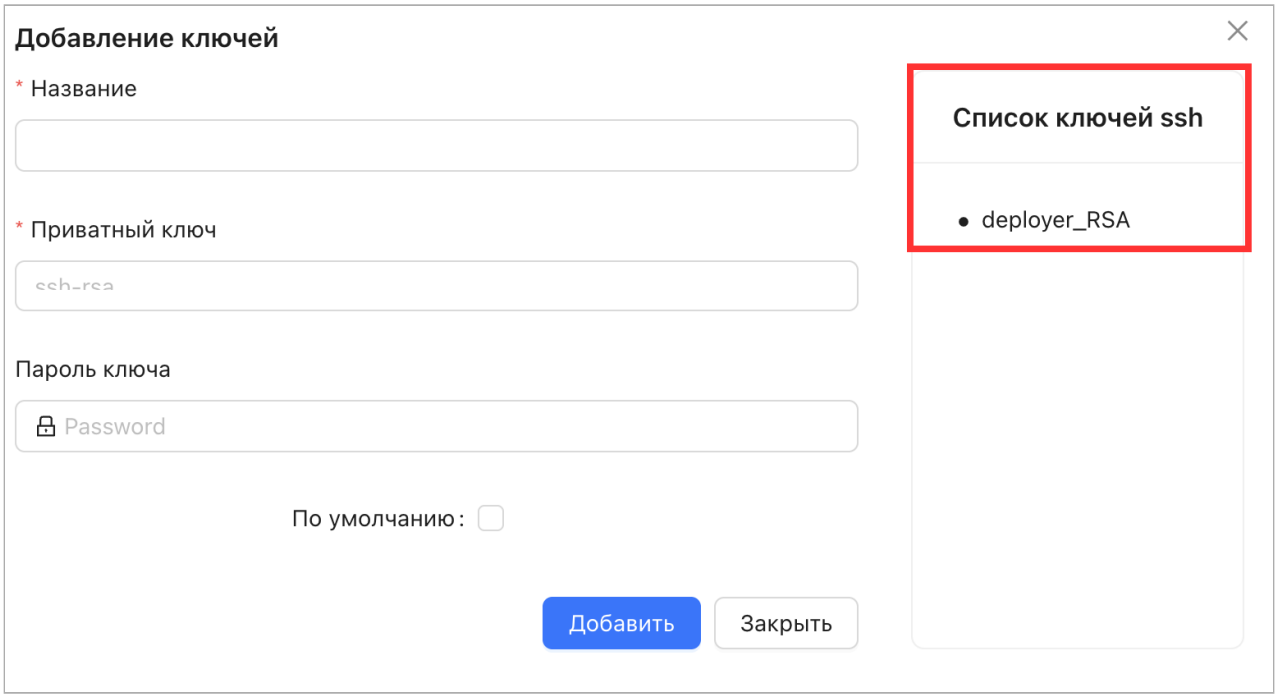
Установка через шаблоны

1. Переключитесь на вкладку **Готовые шаблоны**.
2. Укажите **Количество пользователей** на вашей инсталляции.
3. Укажите **Тип виртуальной машины**. Тип виртуальной машины влияет на количество виртуальных машин. Чем мощнее будут машины, тем меньше их понадобится для инсталляции.
4. Укажите **Лимит почтового ящика (Gb)**. В этом поле указывается ожидаемый максимальный размер почтового ящика пользователей. В зависимости от этого рассчитывается количество необходимого места на дисках.

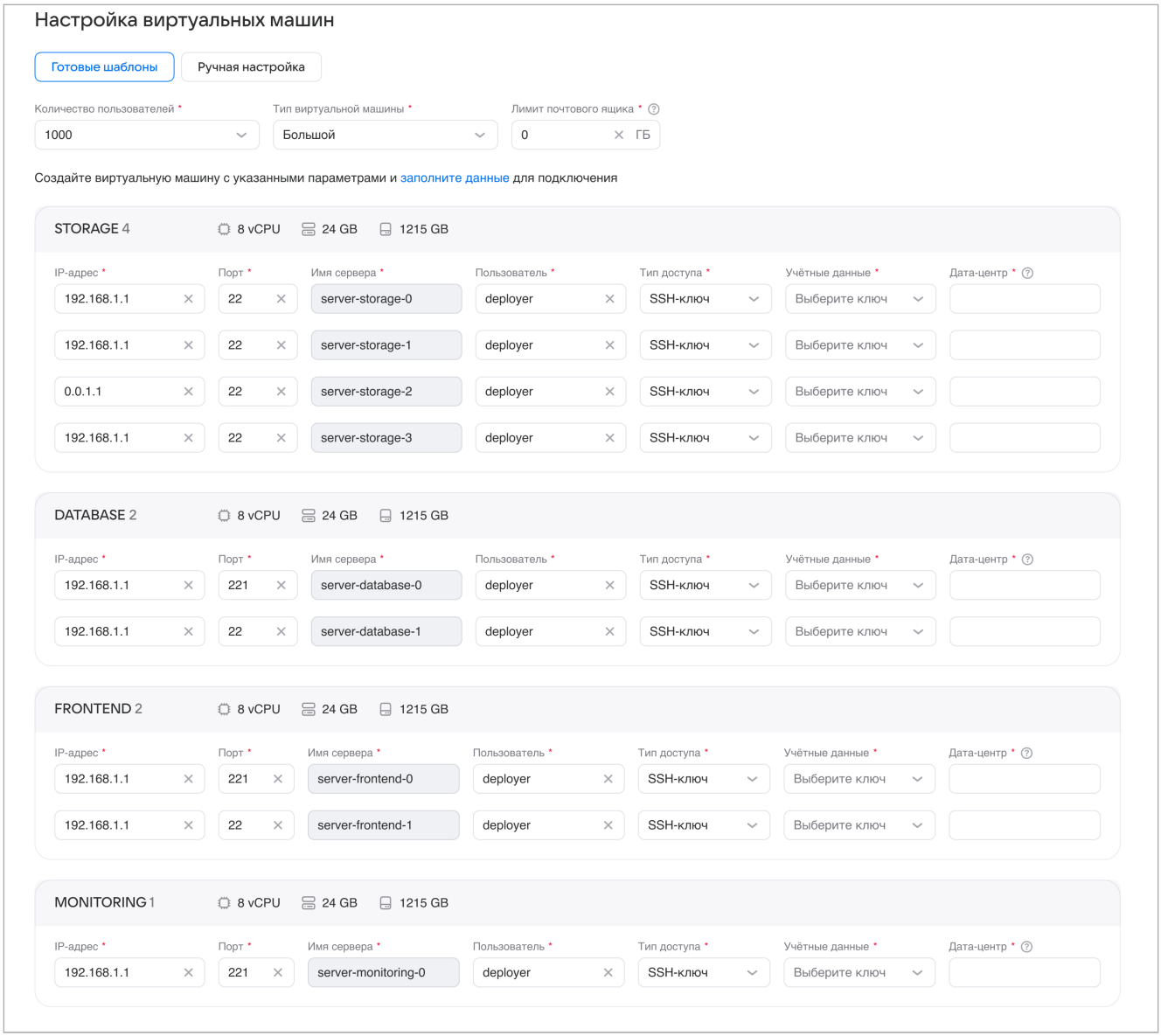
5. Создайте виртуальные машины с указанными параметрами, если не делали этого раньше.
6. Заполните IP-адреса машин.
7. Для каждой машины нажмите на поле **Учетные данные**, нажмите кнопку **Добавить** и добавьте SSH-ключ, сгенерированный на машине с установщиком:
   a. В поле **Имя ключа** введите название ключа для его дальнейшей идентификации, например: **deployerRSA**.
   b. Перейдите в консоль.
   c. Выполните команду `cat ~/.ssh/id_rsa` и скопируйте ключ.
   d. Затем вставьте его в поле **Приватный ключ**. Его нужно указать полностью, включая:

      `-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----`

   e. Поле **Пароль ключа** оставьте пустым.
   f. Кликните по кнопке **Добавить**.
   g. Новый ключ должен отобразится в панели справа.



   h. Нажмите **Закрыть**.
8. Поле **Дата-центр** нужно заполнять только, если на этапе выбора продуктов вы включили **Поддержка режима катастрофоустойчивости 2 ЦОД + witness**.



9. Нажмите **Далее** внизу страницы.

Шаг 4. Проверьте серверы на соответствие требованиям

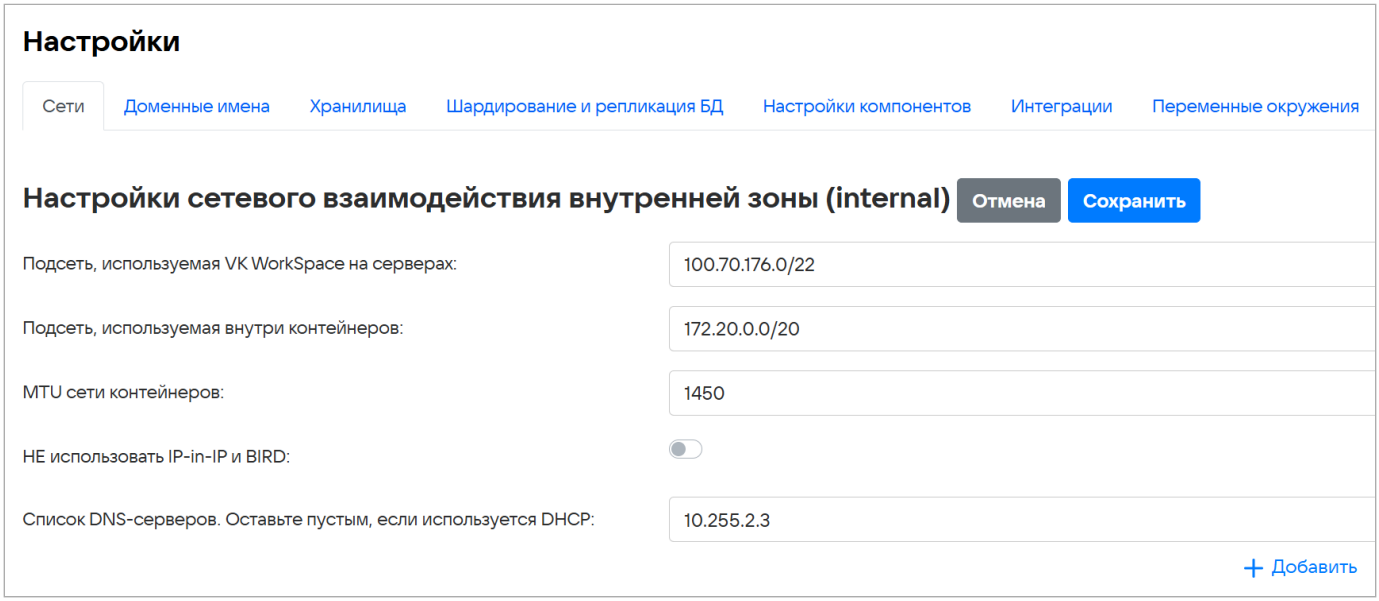
В открывшемся окне нажмите **Запустить проверки**. Будут выполнены следующие проверки:

- Проверка ОС, дистрибутива и параметры ядра.
- Проверка архитектуры CPU, количества ядер и обязательных фич.
- Проверка общего объема и характеристик оперативной памяти.
- Проверка размеров и параметров файловых систем.
- Проверка производительности дисковой подсистемы по IOPS.
- Проверка доступности и состояния обязательных портов.
- Проверка DNS-серверов и записей.
- Проверка активного tuned профиля.
- Проверка наличия и состояния swap.

После успешного выполнения всех проверок нажмите **Далее**.

Шаг 5. Сетевые настройки

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



1. Укажите **DNS-сервер**.

> **Внимание**
>
> Обязательно настройте NTP на BM в соответствии с рекомендациями к используемой ОС: RedOS, Astra Linux или MosOS Arbat.

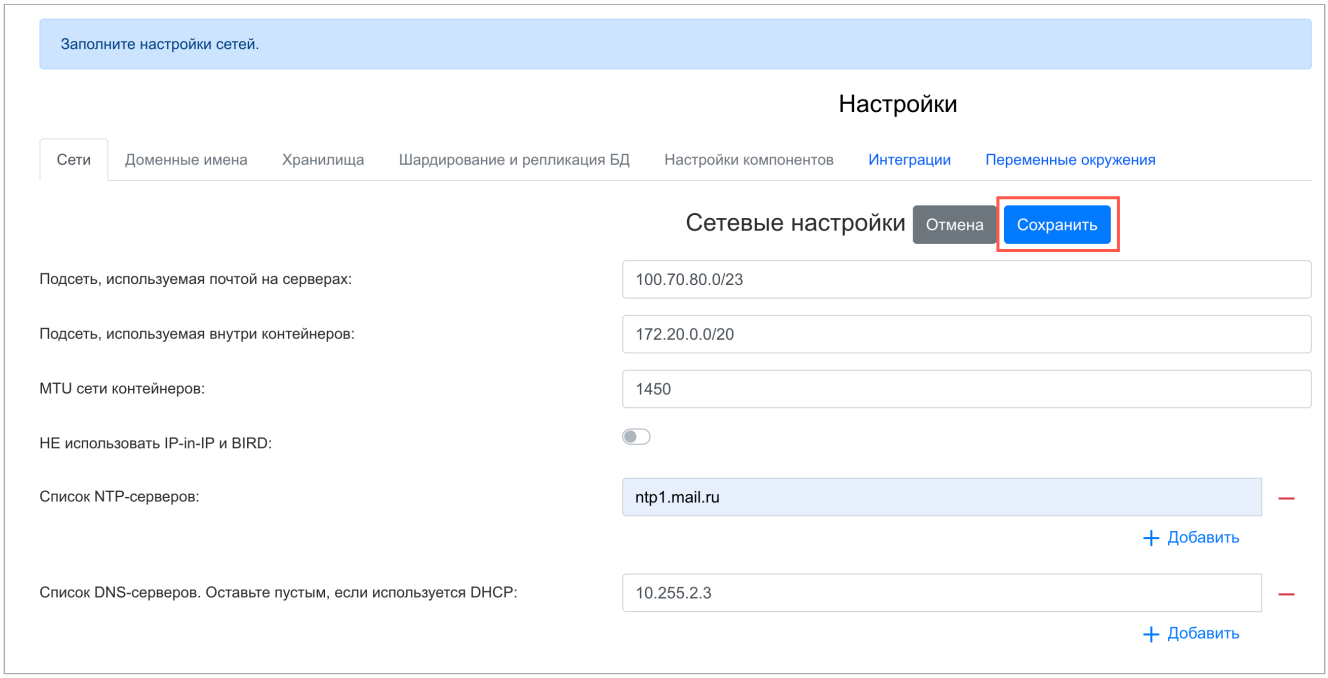
2. Убедитесь, что:
   - **Подсеть, используемая VK WorkSpace на серверах** имеет доступ на **80-й** или **443-й** порт.
   - **Подсеть, используемая внутри контейнеров** полностью свободна, уникальна и принадлежит только Почте.

> **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. При кластерной установке в среднем создается более 1350 контейнеров, поэтому 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.

3. Нажмите на кнопку **Сохранить** и перейдите к следующему шагу.



Шаг 6. Доменные имена

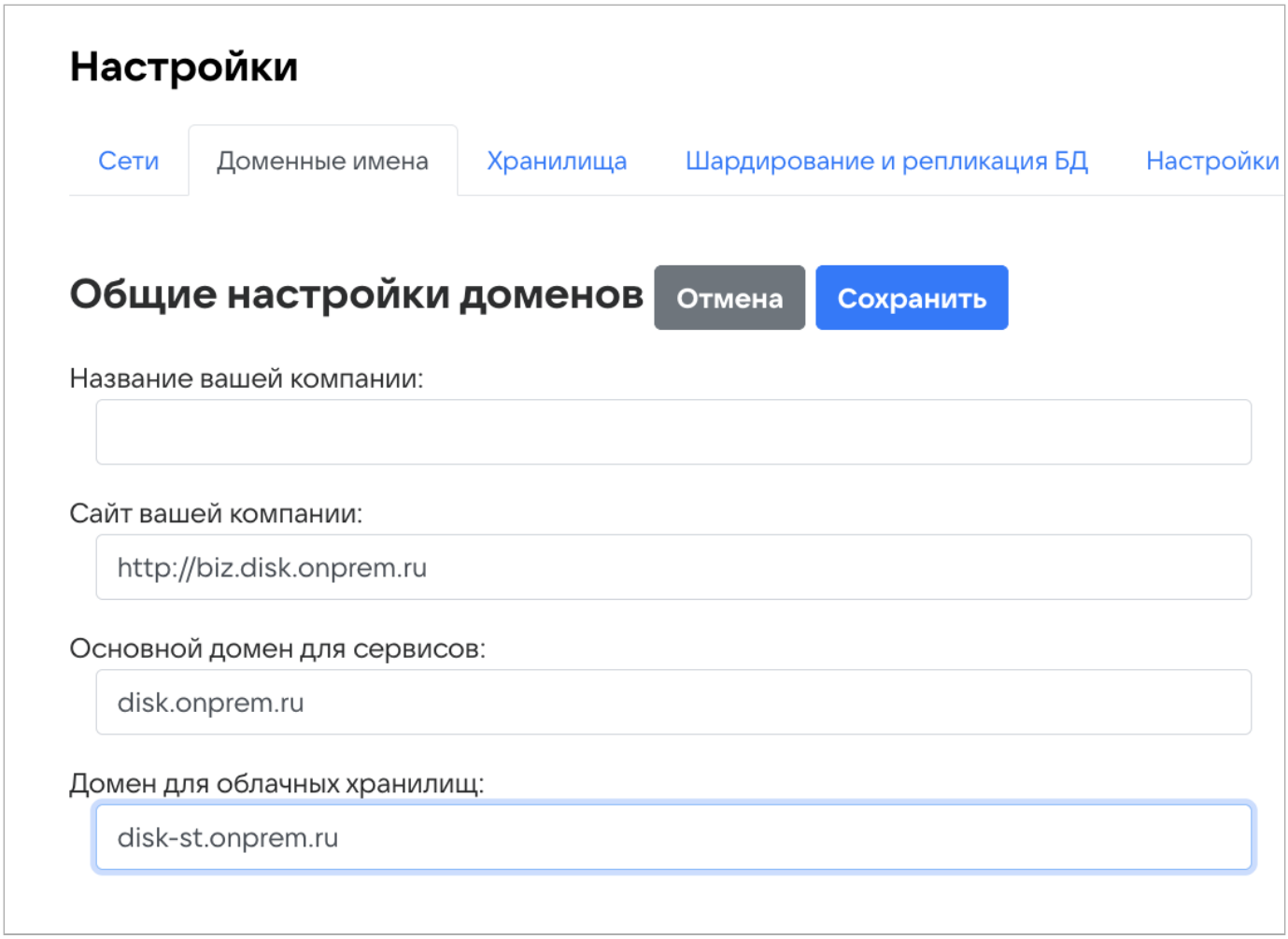
Подробную информацию о создании доменных имен вы найдете в разделе Создание DNS-записей.

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.

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

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



После сохранения доменных имен появятся ошибки. Они пропадут после добавления SSL-сертификатов на следующем шаге.

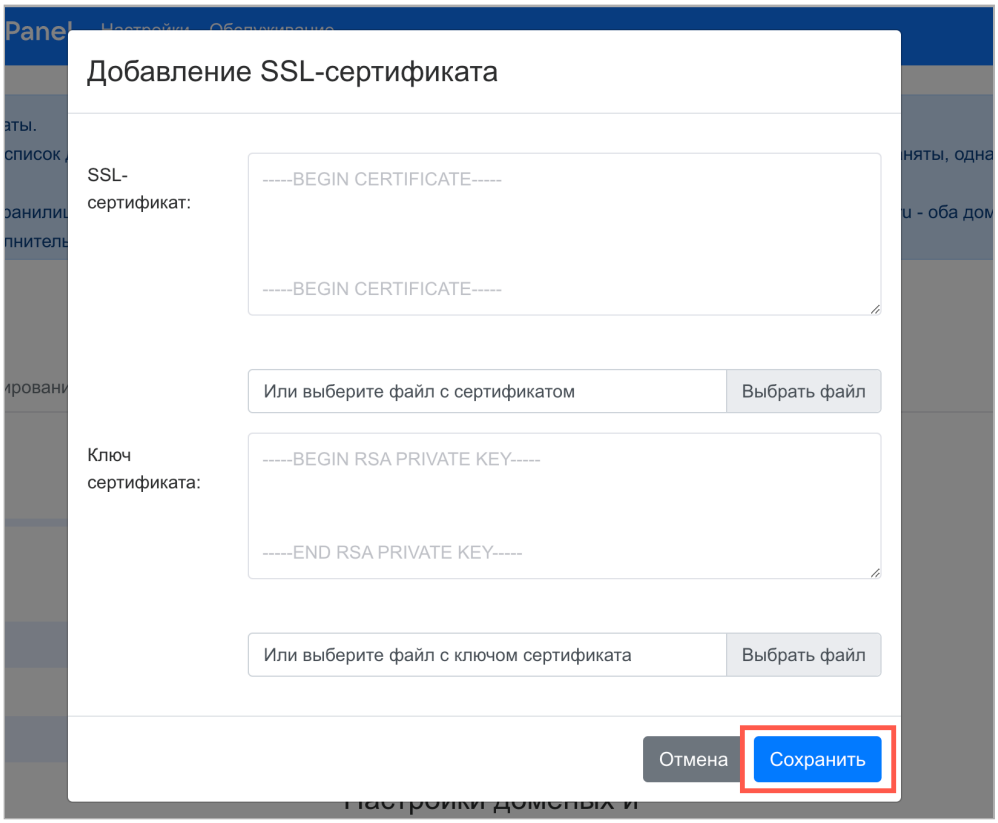
Добавление SSL-сертификатов

1. Нажмите на кнопку **Добавить сертификат** под заголовком **SSL-сертификаты**.
2. 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-----`.
3. Кликните по кнопке **Сохранить**.



Есть второй вариант:

1. Нажмите на кнопку **Выбрать файл**.
2. Укажите путь к файлу с сертификатом **.crt**.
3. Укажите путь к файлу с ключом **.key**.
4. Кликните по кнопке **Сохранить**.

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

Если всё верно, в интерфейсе не будет отображаться ошибок и красной подсветки. Нажмите на зеленую кнопку **Далее**.

Шаг 7. Установка гипервизоров

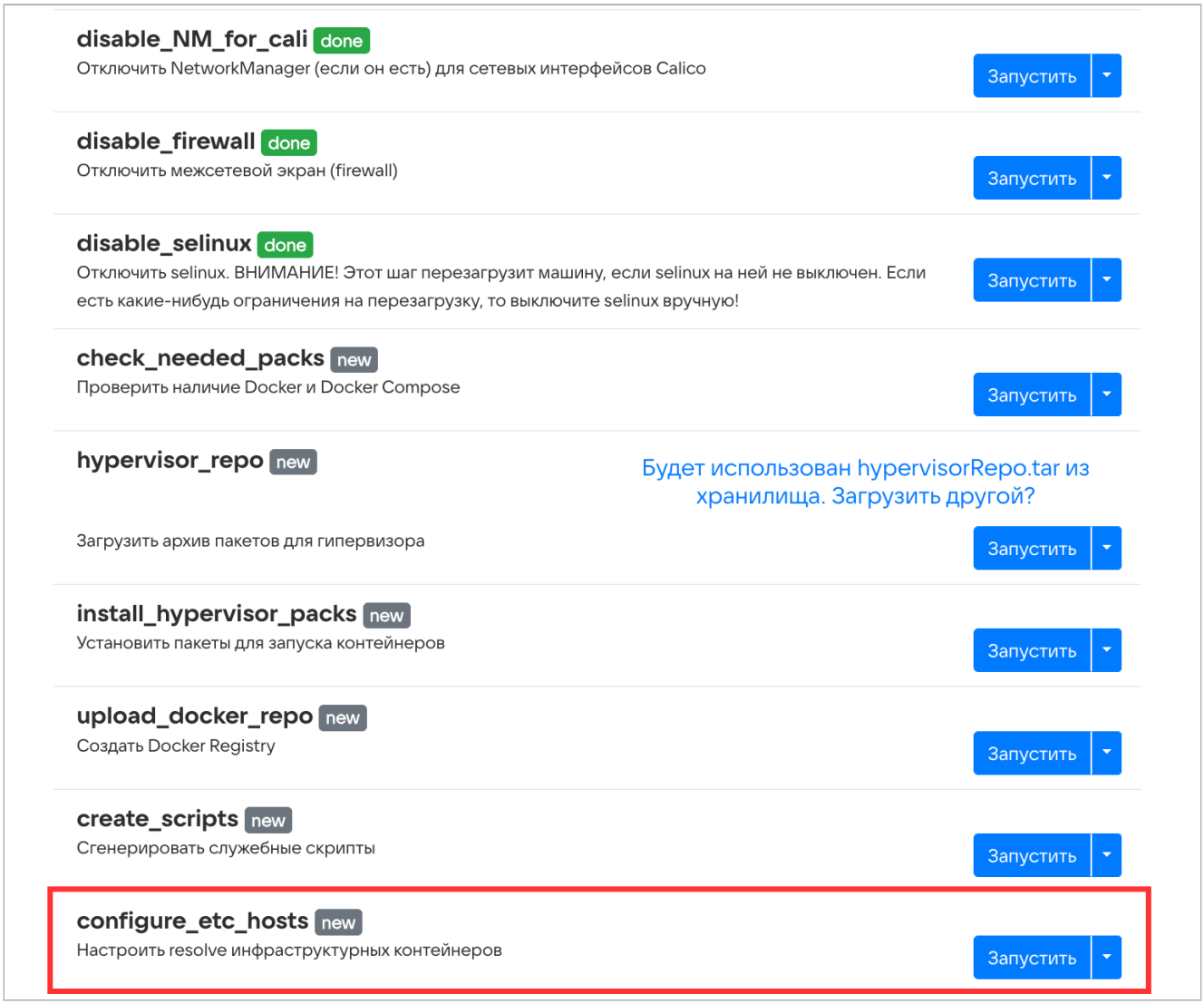
Установка вручную

Для начала установки перейдите к списку гипервизоров — для этого нажмите на логотип в левом верхнем углу веб-интерфейса.

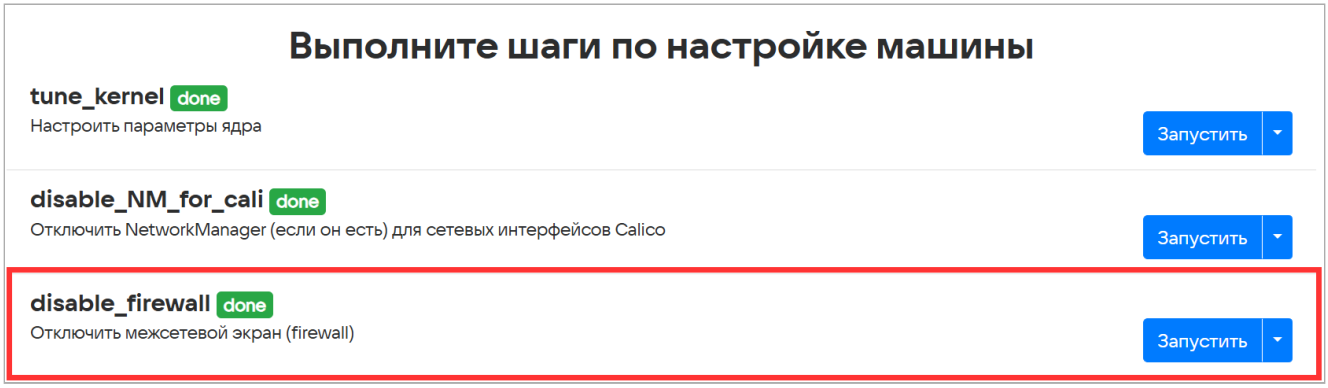
Порядок установки гипервизоров важен, поскольку необходимо сформировать **кластер etcd**. Для кворума кластеру необходимо **N/2+1** экземпляров etcd. В минимальной конфигурации узлы ectd должны

быть установлены на **три машины**, две из которых должны быть постоянно доступны. В документе будет описан вариант установки etcd в минимальной конфигурации.

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

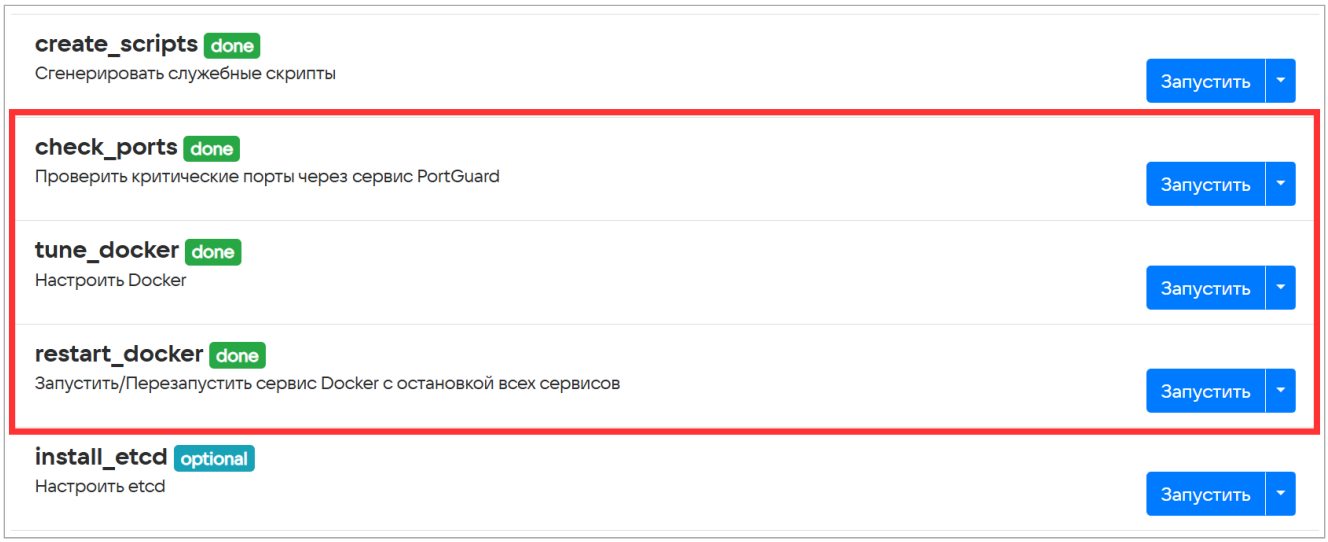


2. Вернитесь к списку машин.
3. Перейдите в настройки любого гипервизора и вручную запустите шаги до **disable_firewall** включительно.

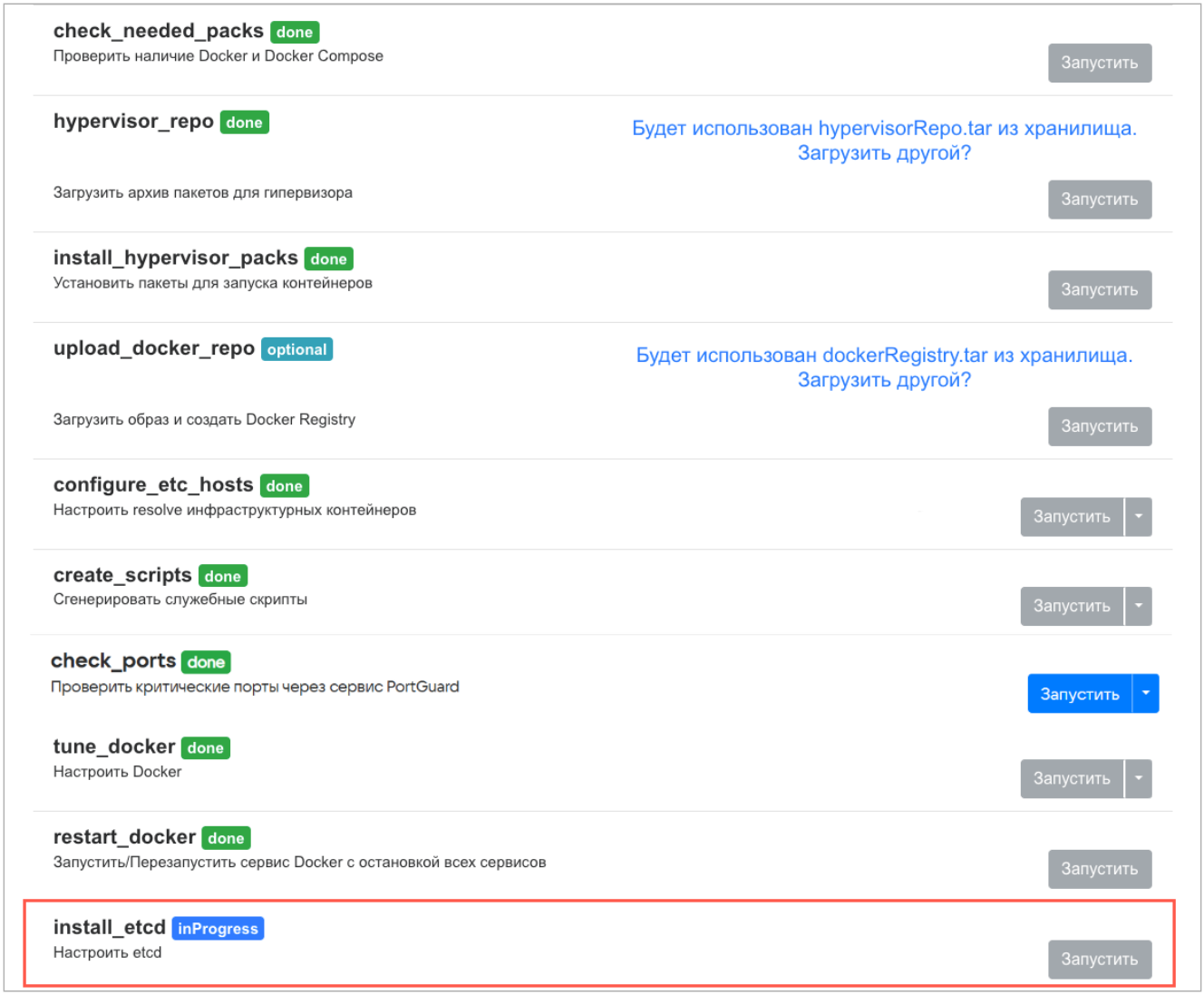


4. Вручную запустите шаги до **disable_firewall** включительно на всех остальных гипервизорах.
5. Вернитесь к списку машин и перейдите в настройки гипервизора, отведенного под мониторинг.

6. Вручную запустите шаги: check_ports, tune_docker и restart_docker.



7. Вернитесь обратно к списку машин и перейдите в настройки первого гипервизора-стораджа.
8. Вручную запустите шаги от **disable_selinux** до **install_etcd** включительно. По завершении шага первый узел etcd будет установлен.

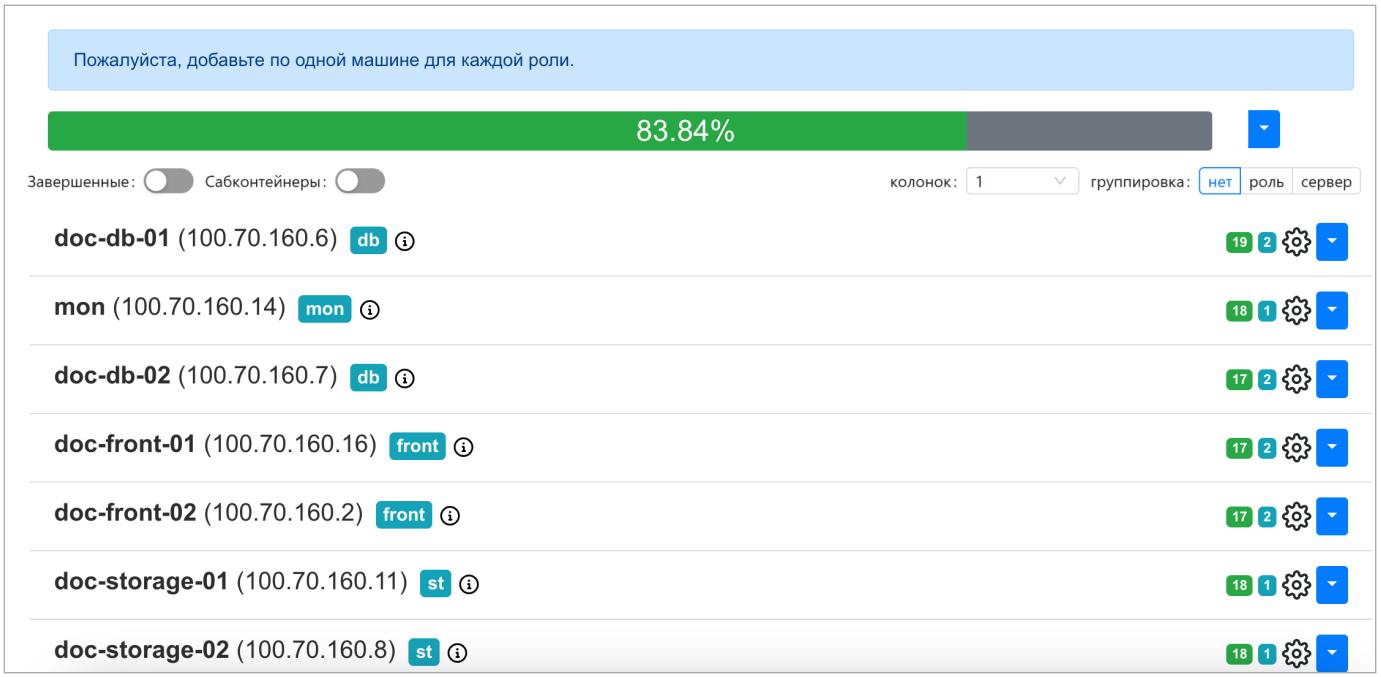


9. Вручную запустите шаги от **disable_selinux** до **install_etcd** включительно на остальных гипервизорах-стораджах.

10. После того, как кластер etcd собран, запустите установку всех гипервизоров по порядку или общую автоматическую установку.

> **Внимание**
>
> Не запускайте установку нескольких гипервизоров одновременно — это может привести к ошибкам.

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



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

Установка через шаблоны

Дополнительных действий не требуется. Переходите к следующему шагу.

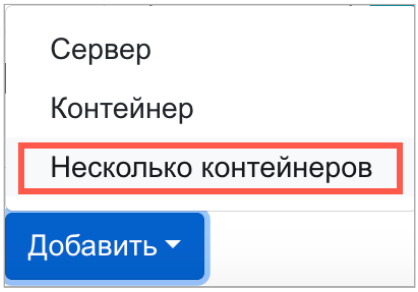
Шаг 8. Распределение контейнеров по гипервизорам

> **Внимание**
>
> Чтобы повысить отказоустойчивость Почты распределяйте одноименные сервисы по разным гипервизорам. Так, в случае выхода из строя одного из гипервизоров, Почта сможет продолжить работу и восстановление гипервизора пройдет быстрее.

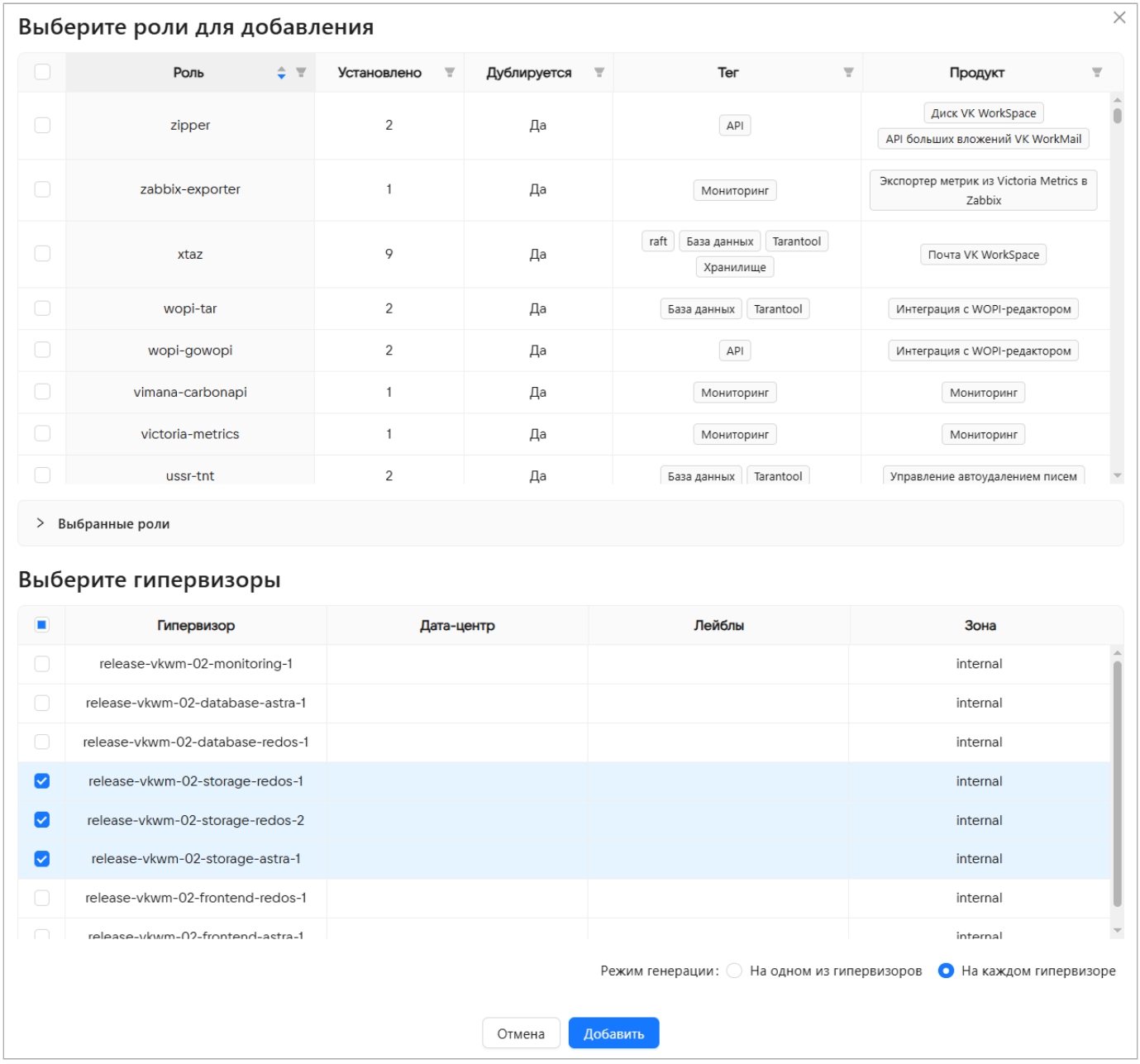
По завершении установки всех гипервизоров можно приступать к распределению и генерации контейнеров.

Установка вручную

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



Откроется окно выбора ролей.



При распределении ролей нужно соблюдать такой порядок:

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

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

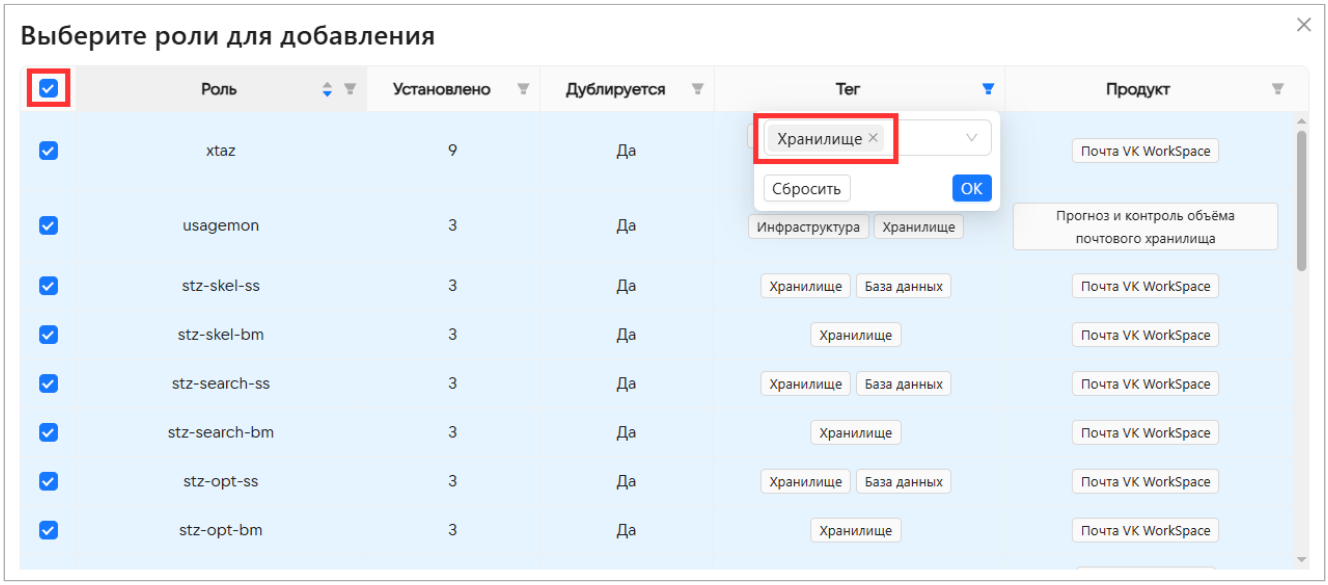
Для выбора ролей используйте поле **Теги** в качестве фильтра.

Порядок действий при распределении контейнеров

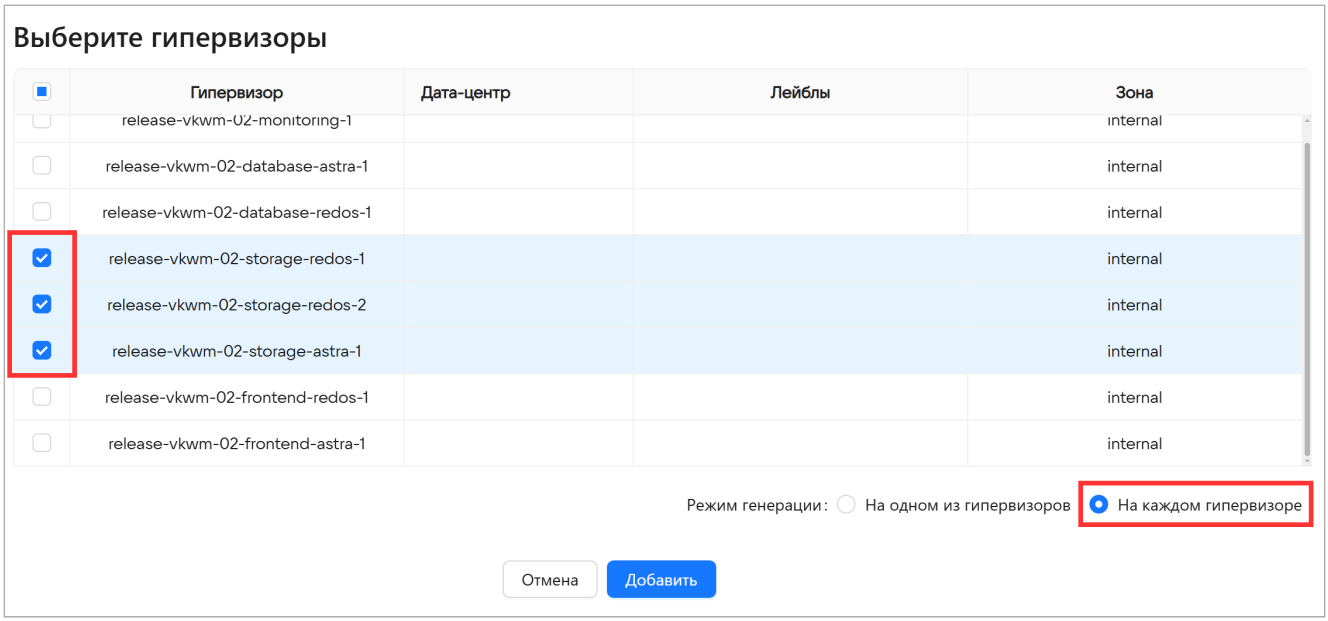
Хранилища

Первыми должны быть выбраны роли для хранилищ:

1. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **Хранилище**.
2. В колонке **Установлено** нажмите на значок и в строке **Не более** установите значение **0**.
3. Отметьте все доступные для установки роли с помощью чекбокса в таблице.



4. Ниже в списке гипервизоров отметьте те, которые были отведены под хранилища.
5. Режим генерации — **На каждом гипервизоре**.



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

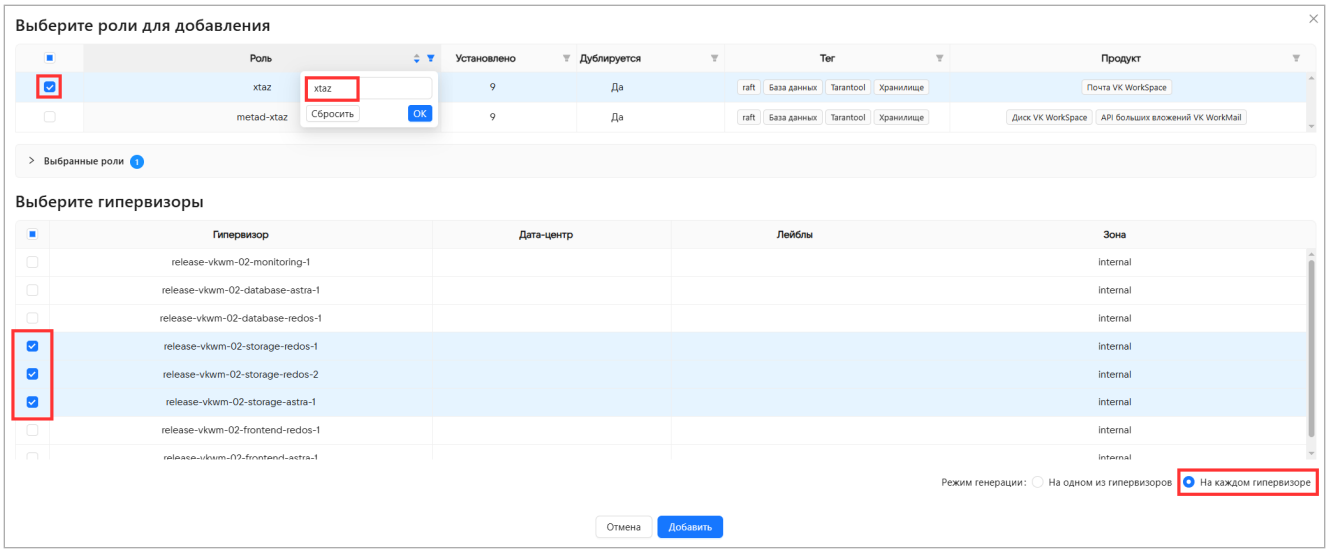
На гипервизоры-хранилища необходимо добавить кластер **raft**.

1. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **raft**.
2. В колонке **Установлено** нажмите на значок и в строке **Не более** установите значение **0**. Если пропустить этот фильтр, кластер не соберется.
3. Отметьте все доступные для установки роли с помощью чекбокса в таблице.
4. Ниже в списке гипервизоров отметьте те, которые были отведены под хранилища.
5. Режим генерации — **На каждом гипервизоре**.
6. 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**.

> **Внимание**
>
> В рассматриваемой конфигурации кластера на 8 машин общее количество контейнеров **xtaz** должно стать равным 6.

1. В колонке **Тег** нажмите на значок и введите **xtaz**.
2. Очистите значение фильтра в колонке **Установлено**.
3. Выберите контейнер **xtaz** с помощью чекбоксов.
4. В списке гипервизоров отметьте те, которые были отведены под хранилища.
5. Режим генерации — **На каждом гипервизоре**.
6. Нажмите на кнопку **Добавить**.



Внимание

Для всех последующих ролей В колонке **Установлено**, при клике на значок , в строке **Не более** должно быть установлено значение 0 в фильтре **Установлено не более**. Если пропустить этот фильтр, кластер не соберется.

Базы данных

Следующий шаг — распределение ролей для баз данных.

1. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **База данных**.
2. В колонке **Установлено** нажмите на значок и в строке **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**.

Мониторинг

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

1. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **Мониторинг**.
2. В колонке **Установлено** нажмите на значок и в строке **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**.

Фронты

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

1. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **Почтовый транспорт**.
2. В колонке **Установлено** нажмите на значок и в строке **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. В колонке **Тег** нажмите на значок и в выпадающем меню выберите **API**.
2. В колонке **Установлено** нажмите на значок и в строке **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**.

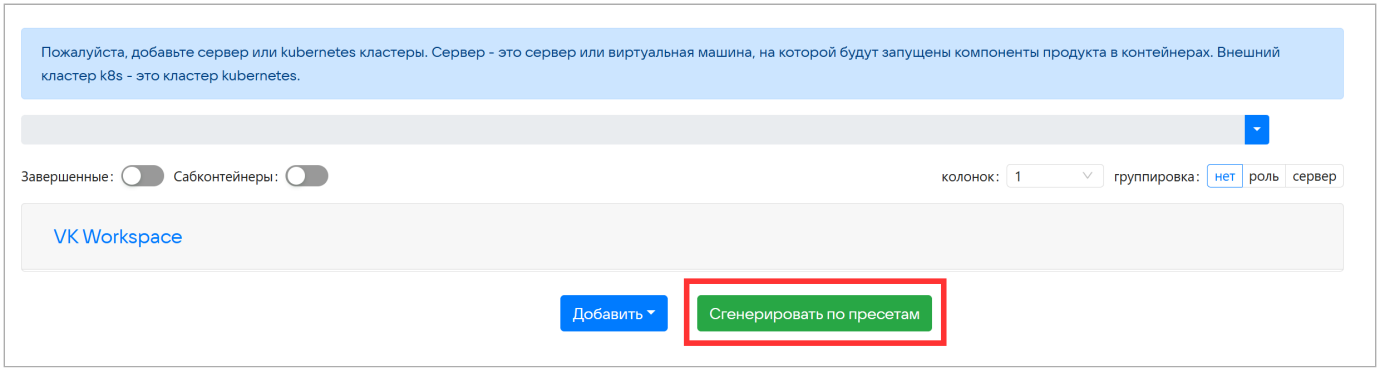
Убедитесь, что все роли распределены

1. Откройте окно добавления выбора ролей, нажав на **Добавить → Несколько контейнеров**.
2. В колонке **Установлено** нажмите на значок и в строке **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.

Установка через шаблоны

Нажмите кнопку **Сгенерировать по пресетам**.



Шаг 9. Хранилища

> **Внимание**
>
> 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.

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.

> **Внимание**
>
> Удалять дисковые пары после установки нельзя. Если удалить дисковые пары, то данные будут утеряны.

Особенности работы с хранилищами zepto

Каждому кластеру zepto нужен обособленный диск. Zepto совершает ряд maintenance-операций, помимо чтения и записи с дисков. Например, сверяет контрольные суммы файлов. Такие операции создают дополнительную нагрузку на диск. Поэтому zepto необходим эксклюзивный доступ к диску. Так он сможет корректно планировать онлайн и офлайн задачи по доступу к диску и при этом сохранять допустимый уровень нагрузки на дисковую подсистему.

Не подключайте 2 zepto-кластера на одни и те же диски, диски могут деградировать из-за повышенного уровня нагрузки. Не устанавливайте к уже установленному кластеру zepto любой другой компонент, создающий нагрузку на диск.

Как распределить дисковые пары вручную

Ниже описана процедура ручного распределения дисковых пар. Дисковые пары нужно распределять вручную, если вы подключали дополнительные диски.

Минимальная отказоустойчивая конфигурация состоит из трех машин, на каждой из которых по 2 дисковых раздела:

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

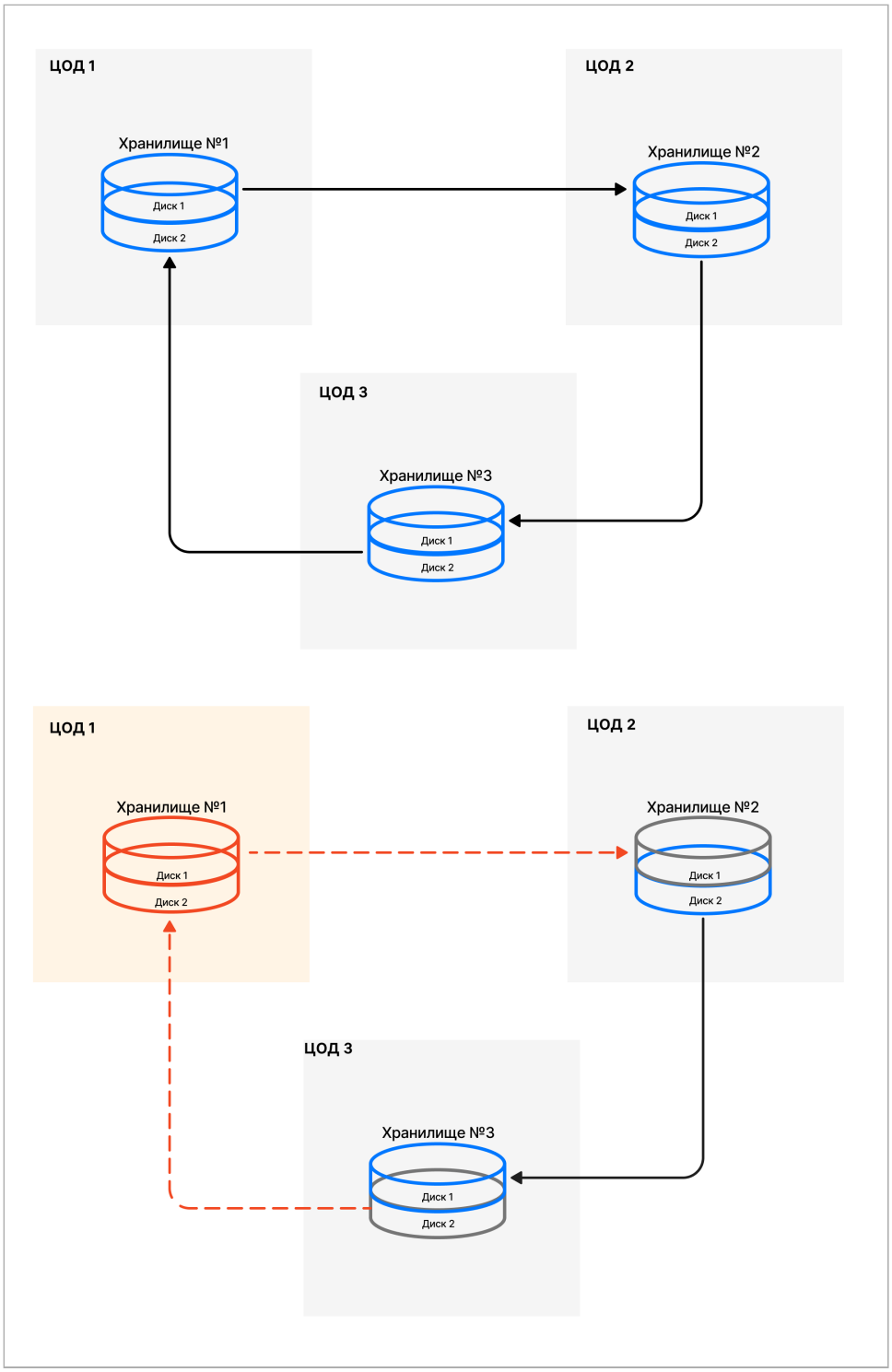
Всего 6 разделов дисков (2 на одном гипервизоре, 2 — на втором, еще 2 — на третьем).

При такой конфигурации:

- Всегда есть пара на запись.

• Остальные пары доступны для чтения.

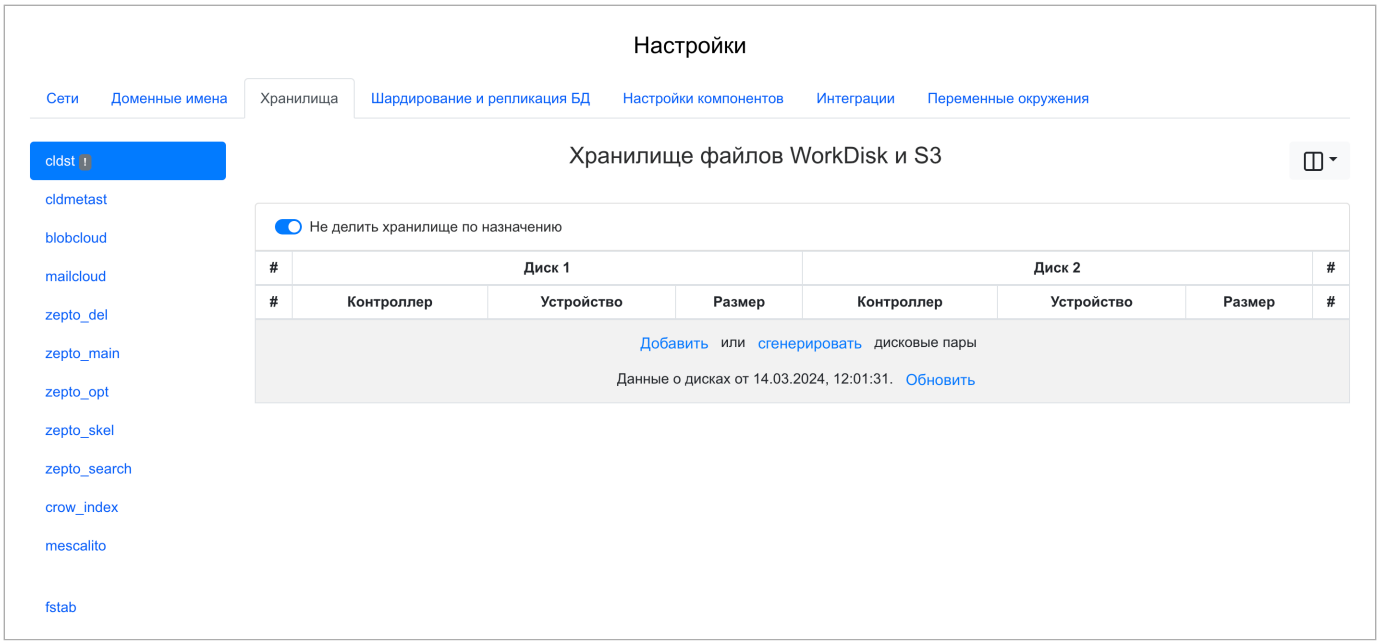
При сборке хранилищ дисковые пары объединяются в «логические треугольники». Объединение происходит по принципу: 1-2, 2-3, 3-1.



Примечание

Стрелки на изображении показывают, какие диски объединены в пару. Нижняя часть изображения иллюстрирует ситуацию, когда одно из хранилищ вышло из строя.

В списке слева доступные хранилища будут отмечены восклицательными знаками. Нужно перейти на вкладку каждого хранилища и сформировать дисковые пары.



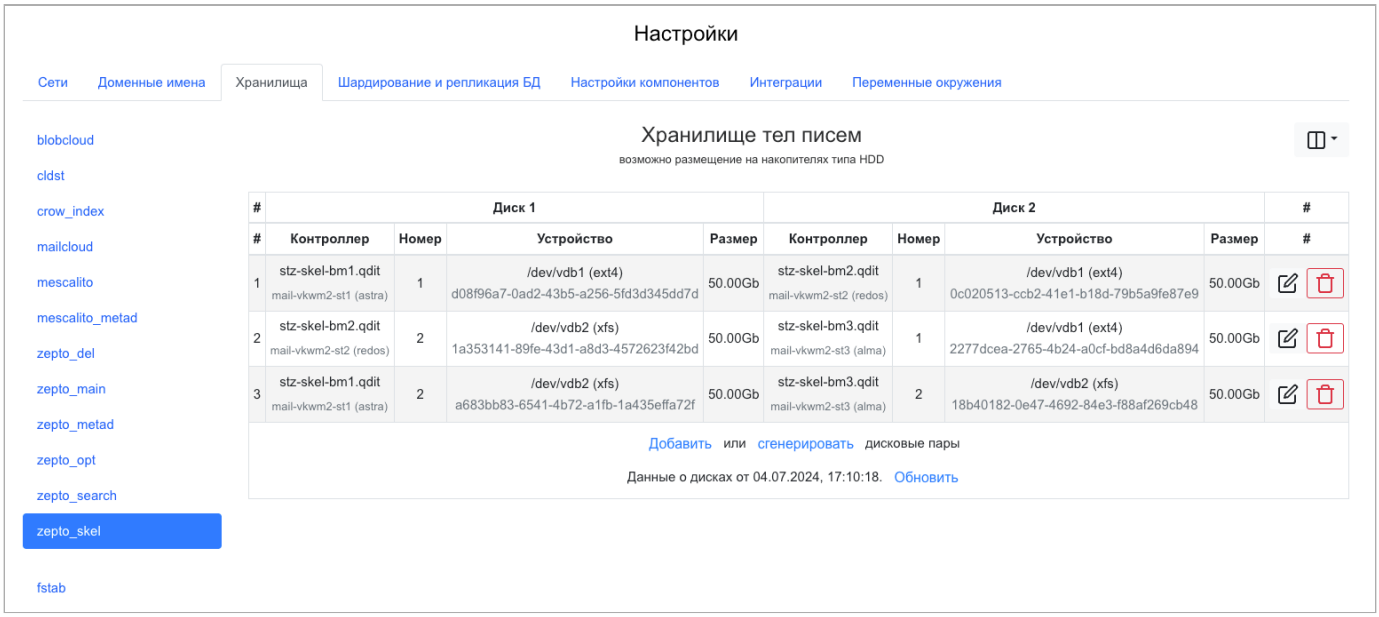
Внимание

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.

Чтобы добавить дисковые пары вручную:

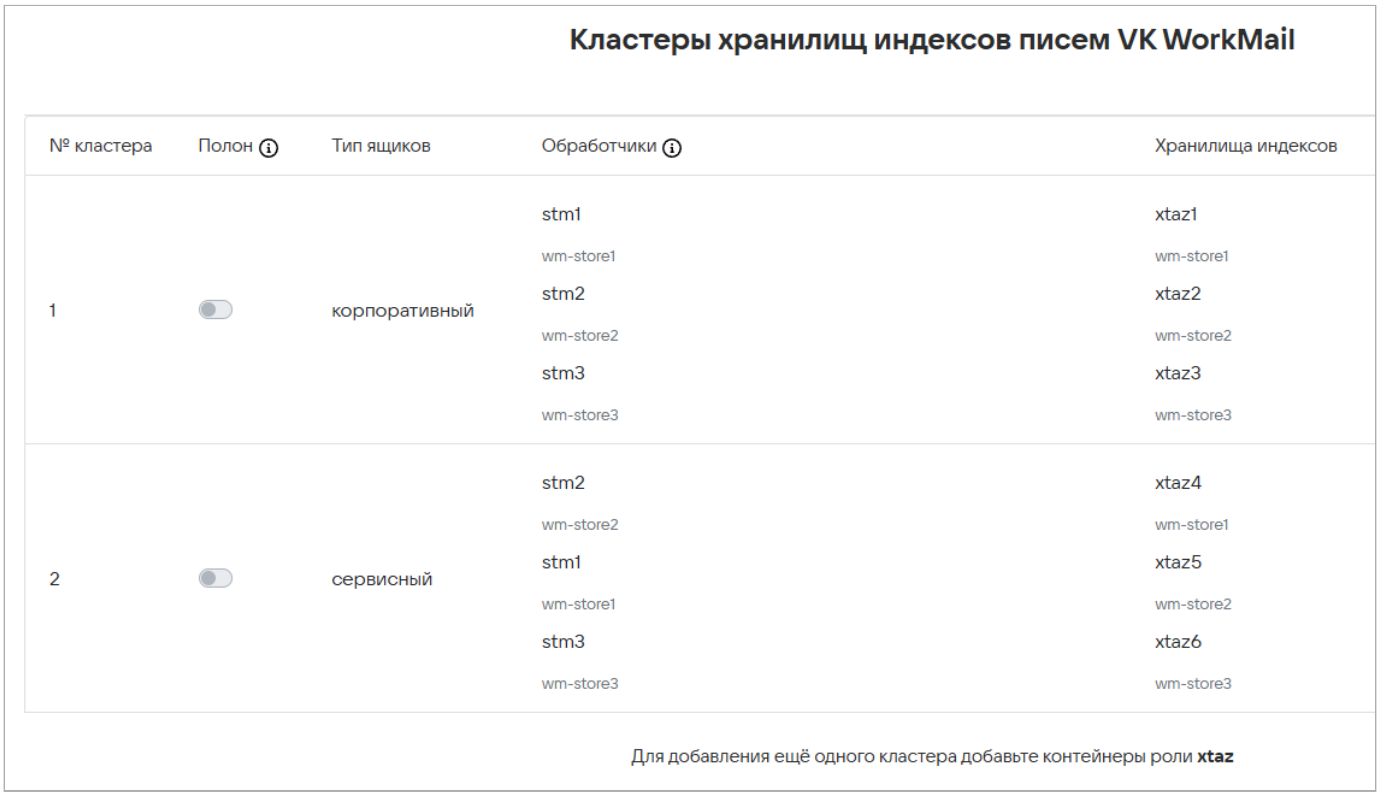
1. Нажмите на кнопку **Добавить**.
2. В выпадающем меню выберите контроллер и устройство для Диска 1 первой пары.
3. Выберите контроллер и устройство для Диска 2 первой пары.
4. Повторите шаги 2-3 еще для двух пар.

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



Раздел Mescalito

Для обеспечения отказоустойчивости в разделе уже заданы автоматические настройки кластеров хранилищ писем.



Кластеры хранилищ индексов писем VK WorkMail

№ кластера	Полон	Тип ящиков	Обработчики	Хранилища индексов
1		корпоративный	stm1 wm-store1 stm2 wm-store2 stm3 wm-store3	xtaz1 wm-store1 xtaz2 wm-store2 xtaz3 wm-store3
2		сервисный	stm2 wm-store2 stm1 wm-store1 stm3 wm-store3	xtaz4 wm-store1 xtaz5 wm-store2 xtaz6 wm-store3

Для добавления ещё одного кластера добавьте контейнеры роли **xtaz**

- Обработчики писем (mescalito) — специальные процессы внутри контейнеров stm. Задача обработчика — собрать письмо из частей, находящихся в разных хранилищах.
- Хранилища индексов (tarantool xtaz) — хранилища «горячих» данных почтовых ящиков.

Информация

Если в логах контейнеров xtaz есть ошибка `failed to allocate X bytes` (или ошибки с подобной формулировкой), то контейнерам не хватает памяти.

Существует 2 типа ящиков:

- Сервисный — admin@admin.qdit (администраторы почты).
- Корпоративный — все остальные ящики системы, которые администрируются в `biz.<почтовый домен>`.

Внимание

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

Чтобы обеспечить отказоустойчивость для каждого кластера необходимо назначать по 2-3 обработчика, которые находятся на разных машинах или в разных дата-центрах.

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

fstab

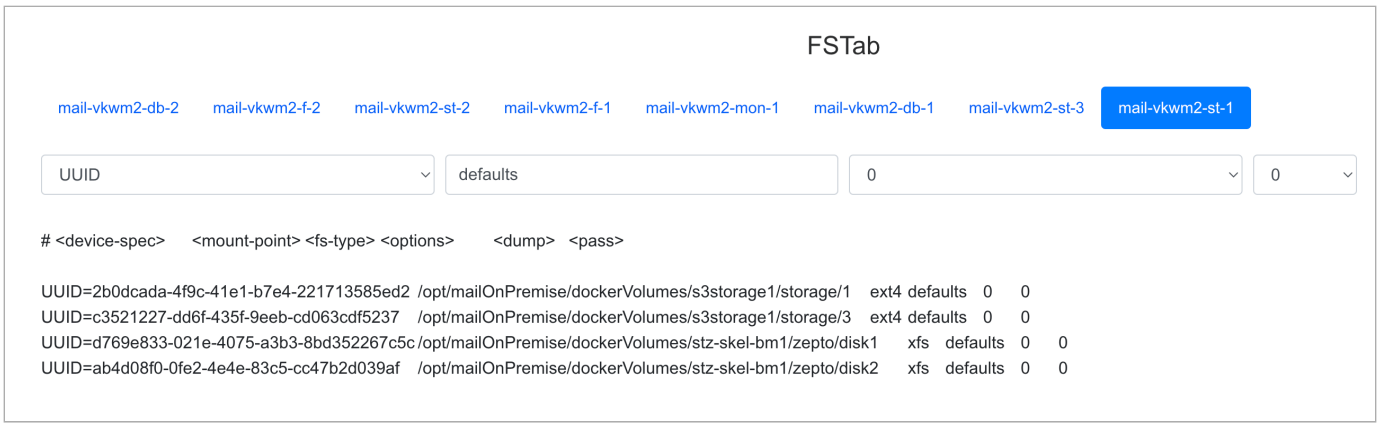
Раздел актуален для ситуаций, когда были подключены дополнительные диски.

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

> **Внимание**
>
> 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:

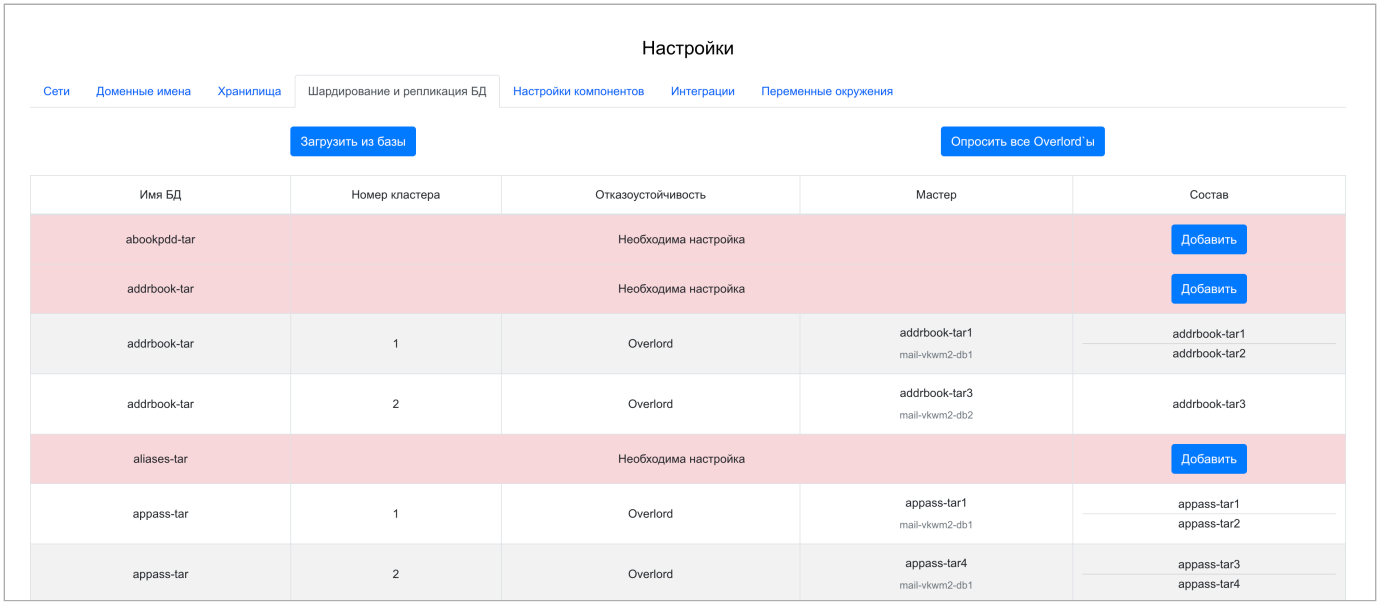
```
vi /etc/fstab

# 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
```

Шаг 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**.

> **Внимание**
>
> Добавлять кластеры БД можно только на этапе первоначальной установки.

Чтобы добавить более одного кластера, потребуется сгенерировать дополнительные контейнеры.



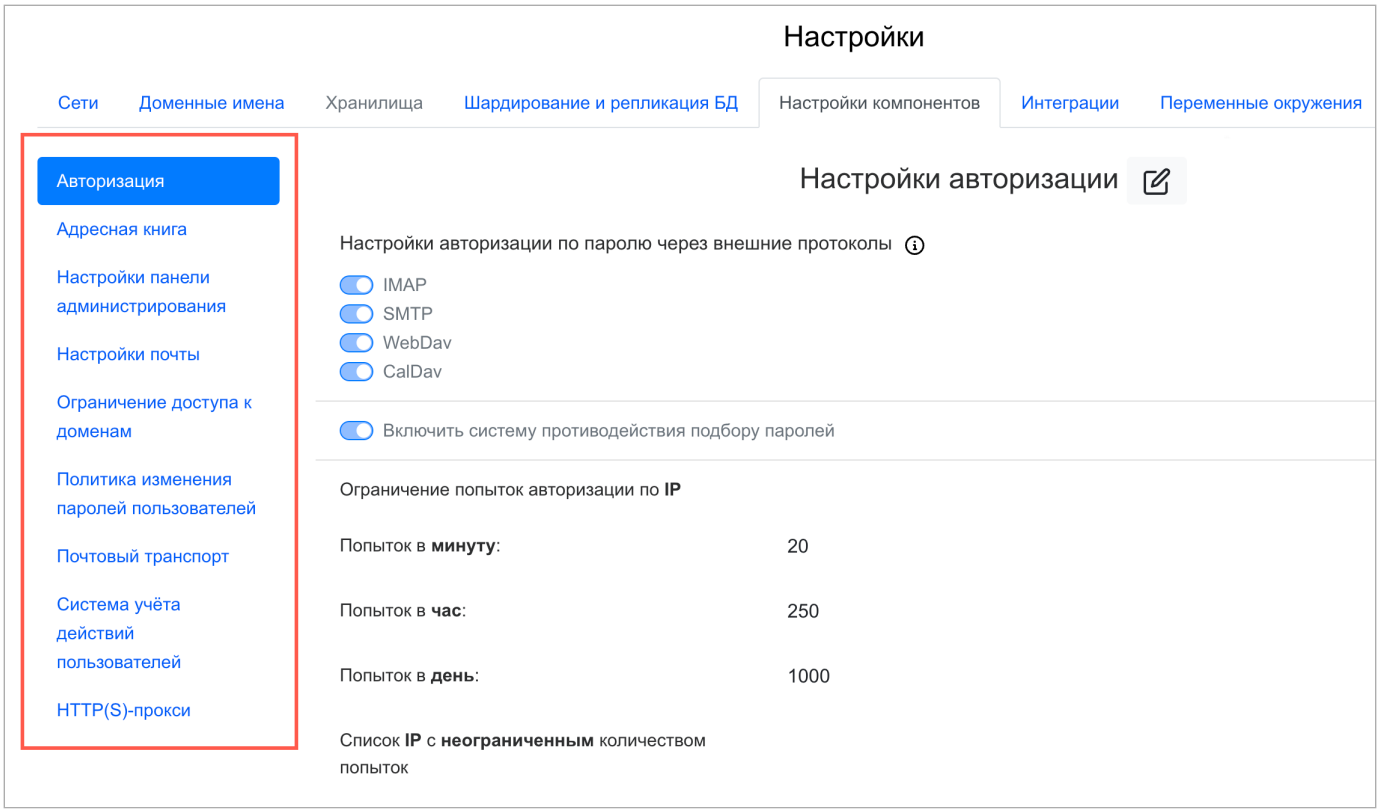
Чтобы добавить кластер:

1. Нажмите кнопку **Добавить** в первой строке, отмеченной красным.
2. Нажмите кнопку **Добавить контейнер БД**. В зависимости от типа базы данных может быть добавлен один или два контейнера.
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**.

Шаг 11. Настройка компонентов

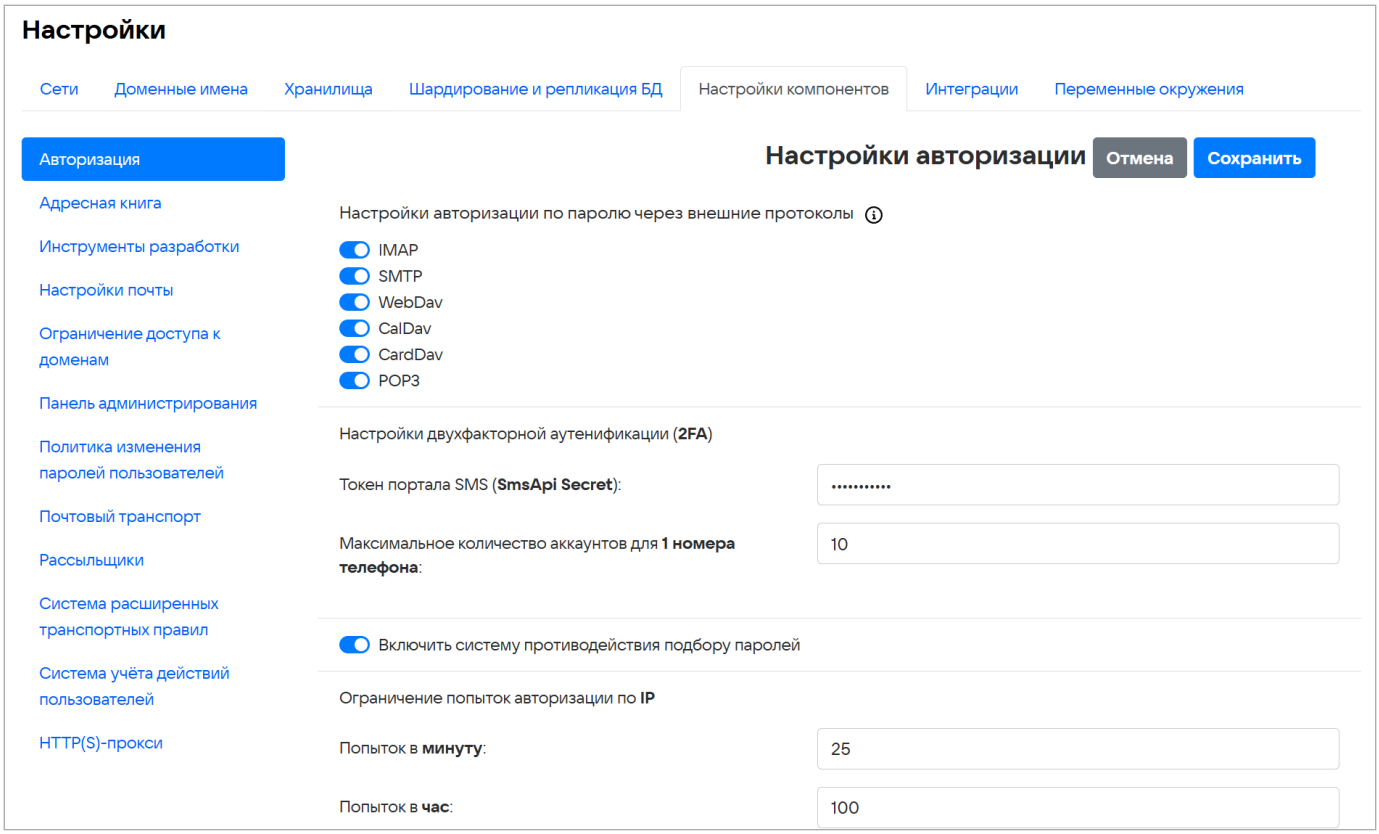
В разделе выполняются настройки различных компонентов почтовой системы.



Авторизация

В разделе можно настроить следующие параметры:

- Защита от подбора паролей.
- Количество попыток входа в Почту по IP и адресу электронной почты.
- Указать IP-адреса с неограниченным количеством попыток авторизации.
- Настроить авторизацию по паролю через внешние протоколы.



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 по инструкции Пароль и безопасность из руководства пользователя Почты.

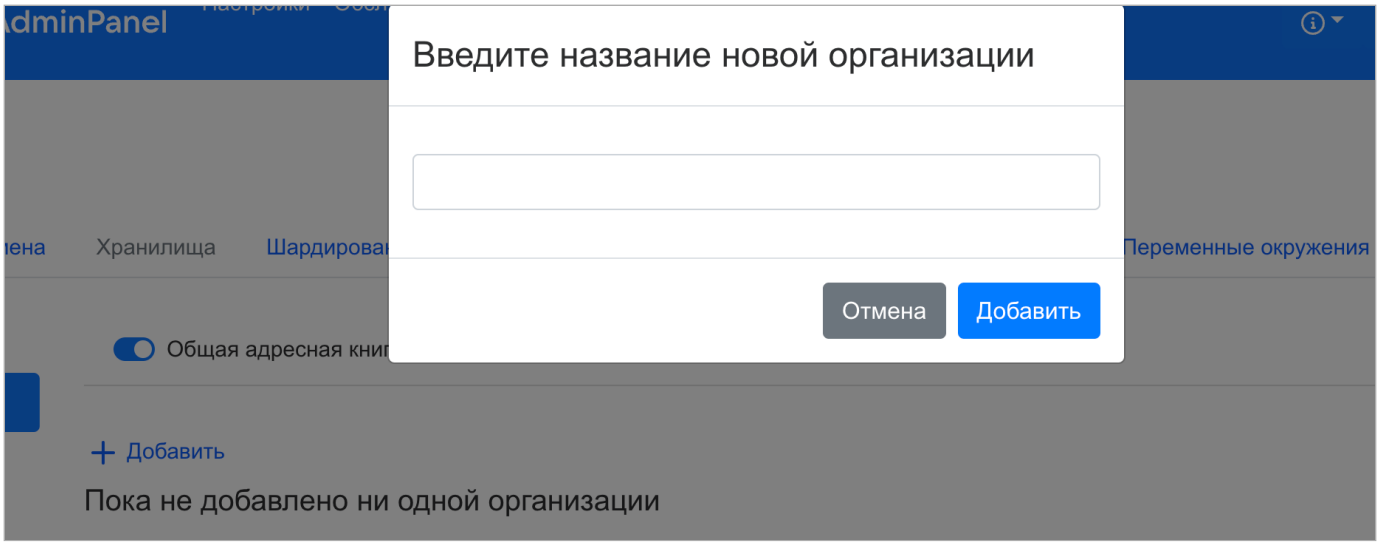
Если флаг протокола выключен, для входа во внешнее приложение достаточно будет ввести пароль аккаунта Почты.

> **Примечание**
>
> За информацией о принципе работы системы ограничения SSO-авторизации по IP/группе в ActiveDirectory обратитесь к представителю VK.

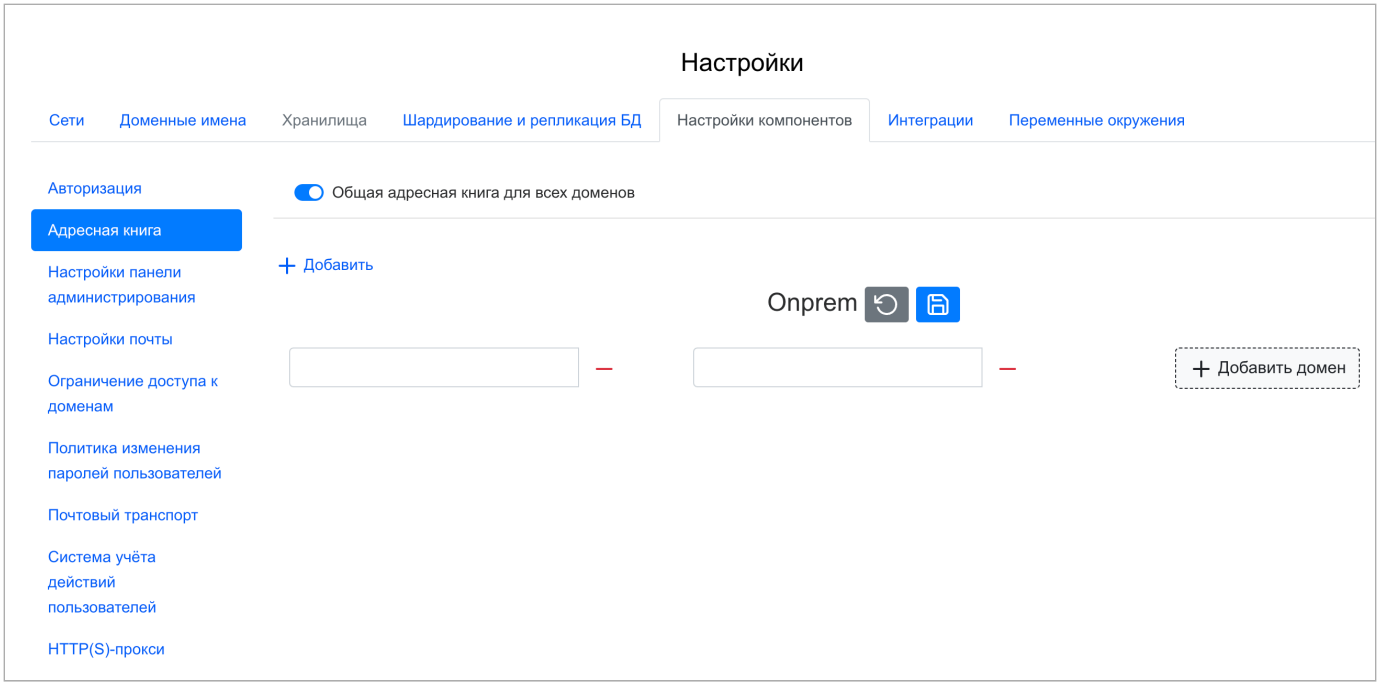
Адресная книга

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

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.

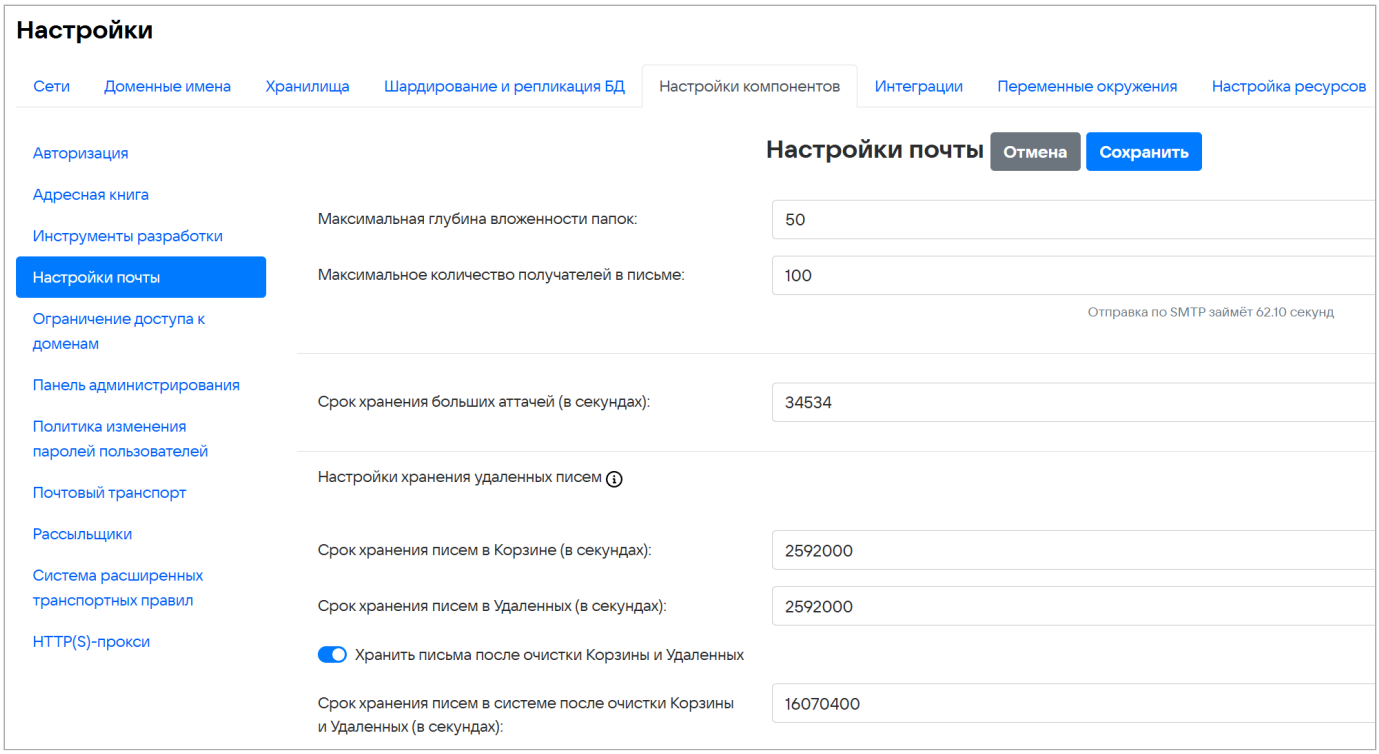


Также есть возможность изменить названия организаций, добавить дополнительные домены и удалить домены/организации. После создания организаций перейдите к списку машин, чтобы повторить нужные шаги.

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

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.

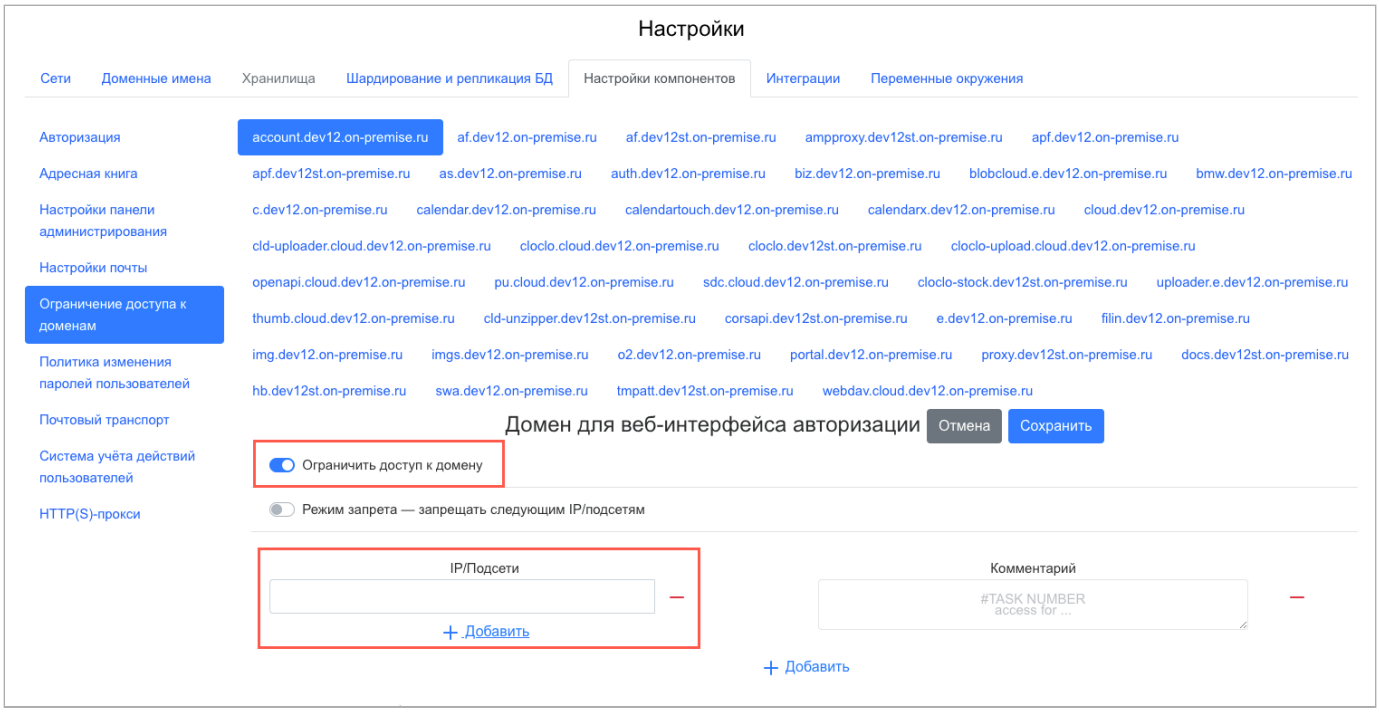
> **Важно**
>
> Максимальная глубина вложенности папок и максимальное количество получателей в письме меняются только вместе. Если вы зададите новое значение для глубины вложенности, система не даст сохранить его без изменения максимального числа получателей. Количество получателей в письме, устанавливаемое вручную, не может быть меньше 100.

Срок хранения больших аттачей (в секундах) — срок хранения больших вложений.

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.



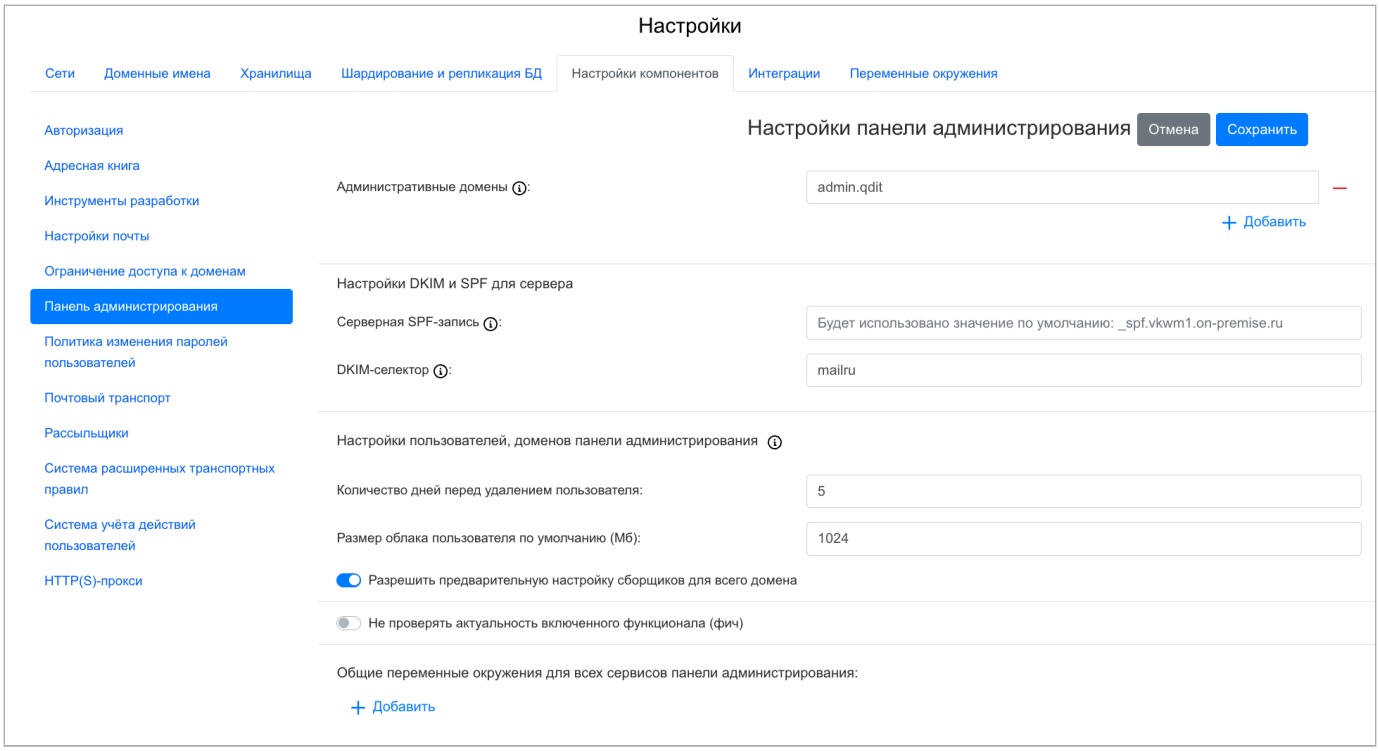
Режим запрета — запрещать следующим IP/подсетям — если включены оба флага (ограничение доступа и режим запрета), доступ к доменам будет **запрещен** IP/подсетям, введенным в поле.

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 в левом верхнем углу веб-интерфейса.

> **Внимание**
>
> 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.

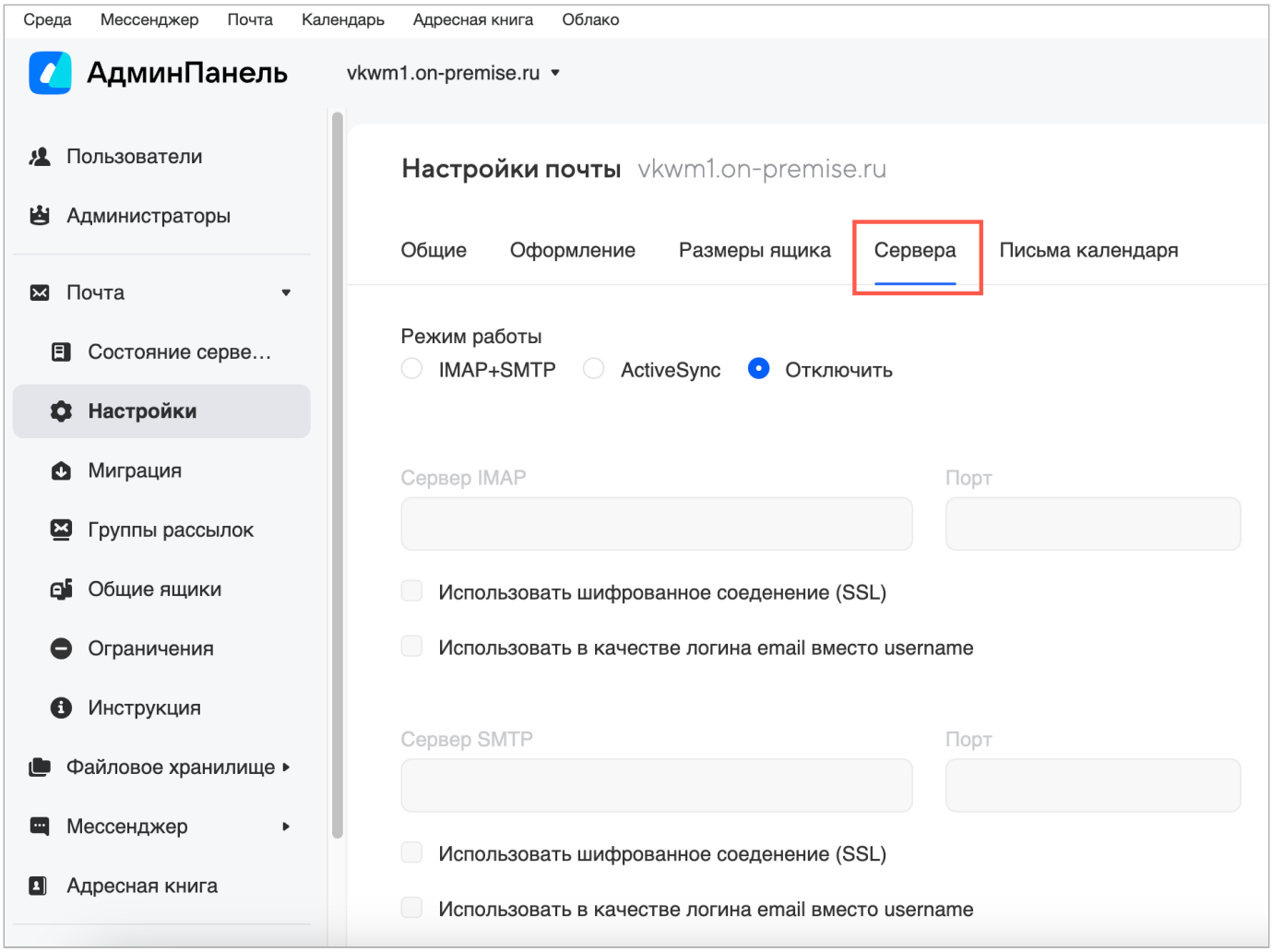
Серверная SPF-запись — введите в поле имя SPF-записи в DNS вашего домена, например: `my_spf_record.onprem.ru`. По умолчанию в SPF-запись ищется по следующему имени: `_spf.<почтовый домен>`. Подробнее про SPF-запись можно прочитать в статье Настройка SPF.

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

Количество дней перед удалением пользователя — количество дней, через которое пользователь будет удален из Почты. Изменение настройки по умолчанию актуально при одновременном использовании Почты с Active directory. По умолчанию выставлен срок 5 дней, то есть пользователь будет удалён из Почты 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/`.



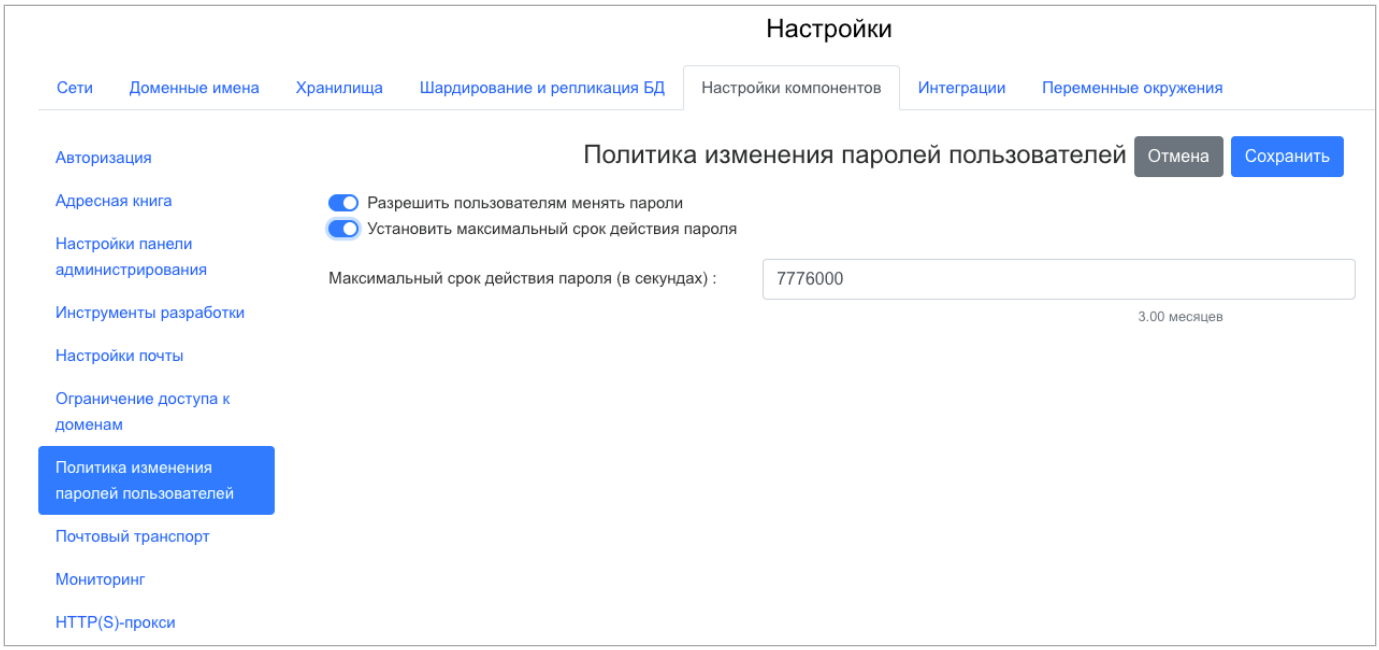
Не проверять актуальность включенного функционала (фич) — при включенном флаге установщик будет пропускать шаг `bizf` → `addBizFeatures`.

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

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

Для изменения настроек во вкладке кликните по кнопке редактирования .

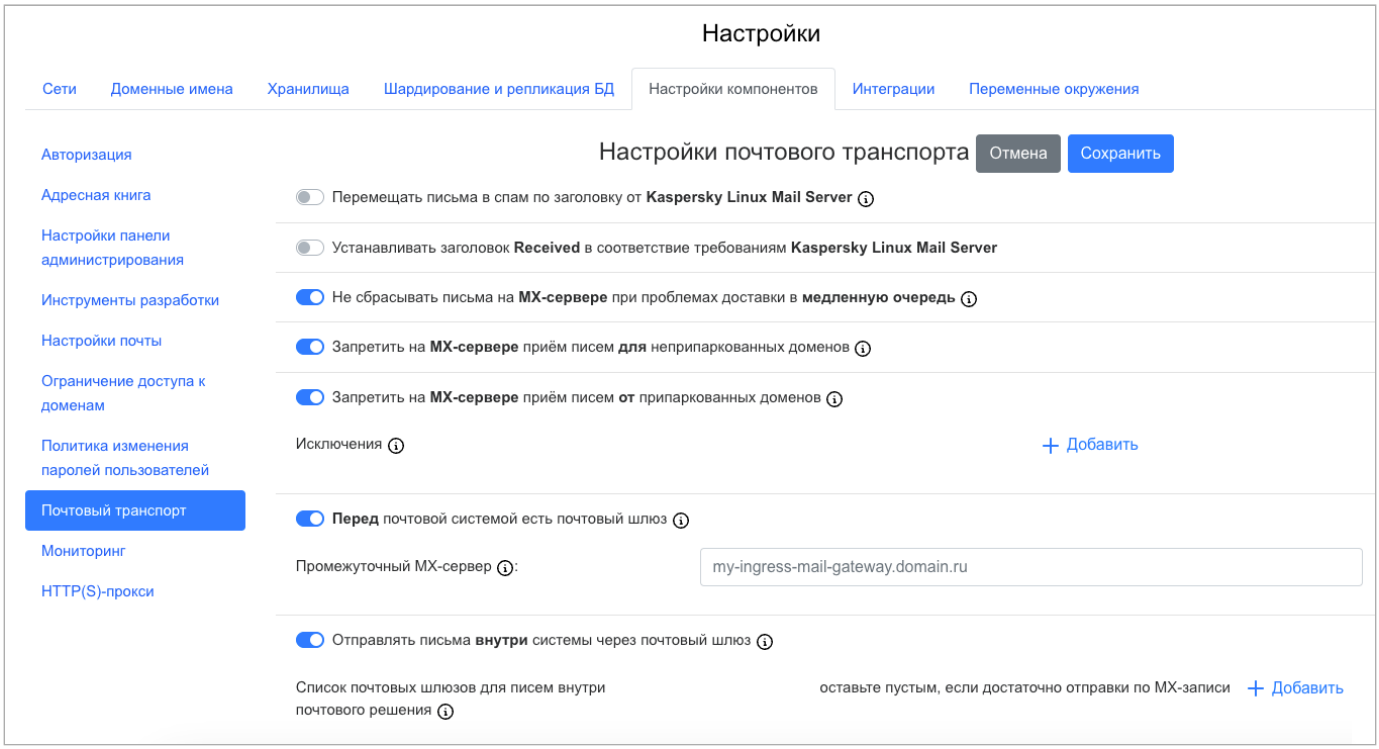


Разрешить пользователям менять пароли — включенный флаг разрешает пользователям менять пароли для своих почтовых ящиков.

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 .



> **Внимание**
>
> Нельзя указывать одинаковые роли пограничного MX-шлюза, DLP и шлюзов антивируса для внутренних писем.

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 Почте 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 WorkSpace 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 в вашей инфраструктуре есть система DLP или система антивирусной проверки и вы хотите отправлять всю исходящую переписку через них, включите эту опцию. Письмо от внутреннего отправителя будет перенаправляться в DLP/антивирус для проверки, а затем возвращаться в Почту для доставки отправителю. DLP/антивирус при этом должны работать в режиме SMTP relay. Если опция выключена, письма внутри системы доставляются сразу в почтовый ящик получателя.

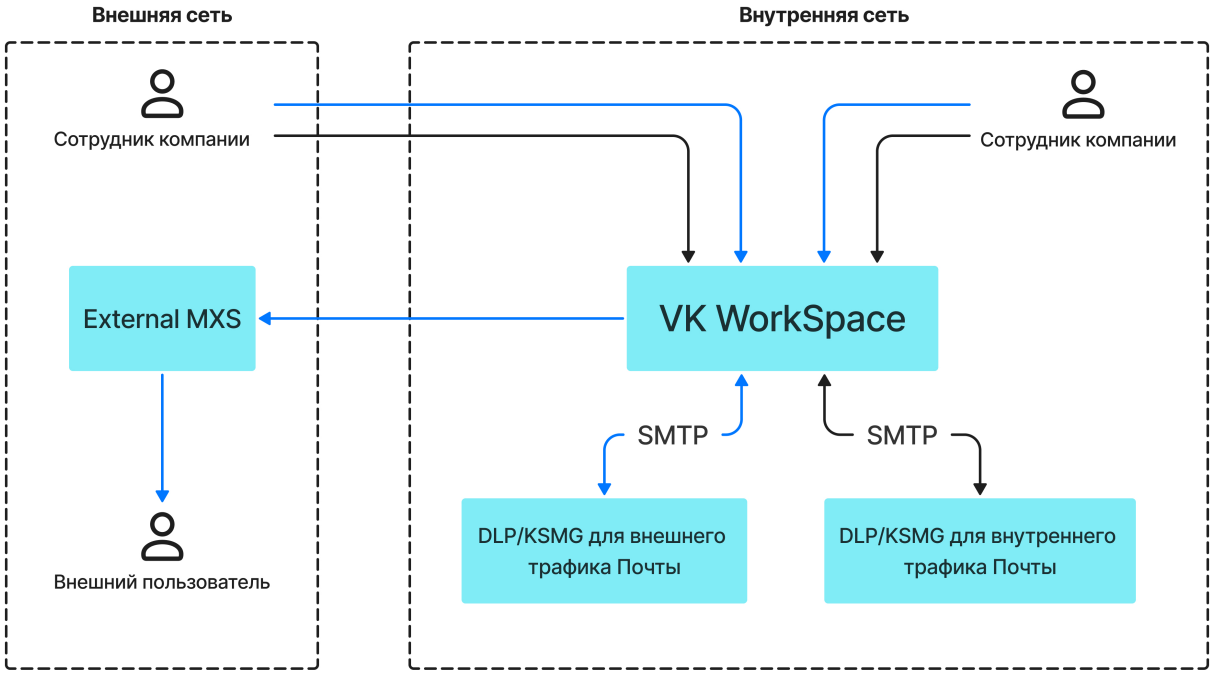
Отправлять письма за пределы системы через почтовый шлюз — если в вашей инфраструктуре есть система DLP или система антивирусной проверки и вы хотите отправлять всю исходящую переписку ко

внешним отправителям через них, включите эту опцию. Письмо от внутреннего отправителя будет перенаправляться в DLP/антивирус для проверки, а затем отправляться во внешний контур для доставки отправителю. DLP/антивирус при этом должны работать в режиме SMTP relay. Если опция выключена, письма внутри системы доставляются сразу в почтовый ящик получателя.

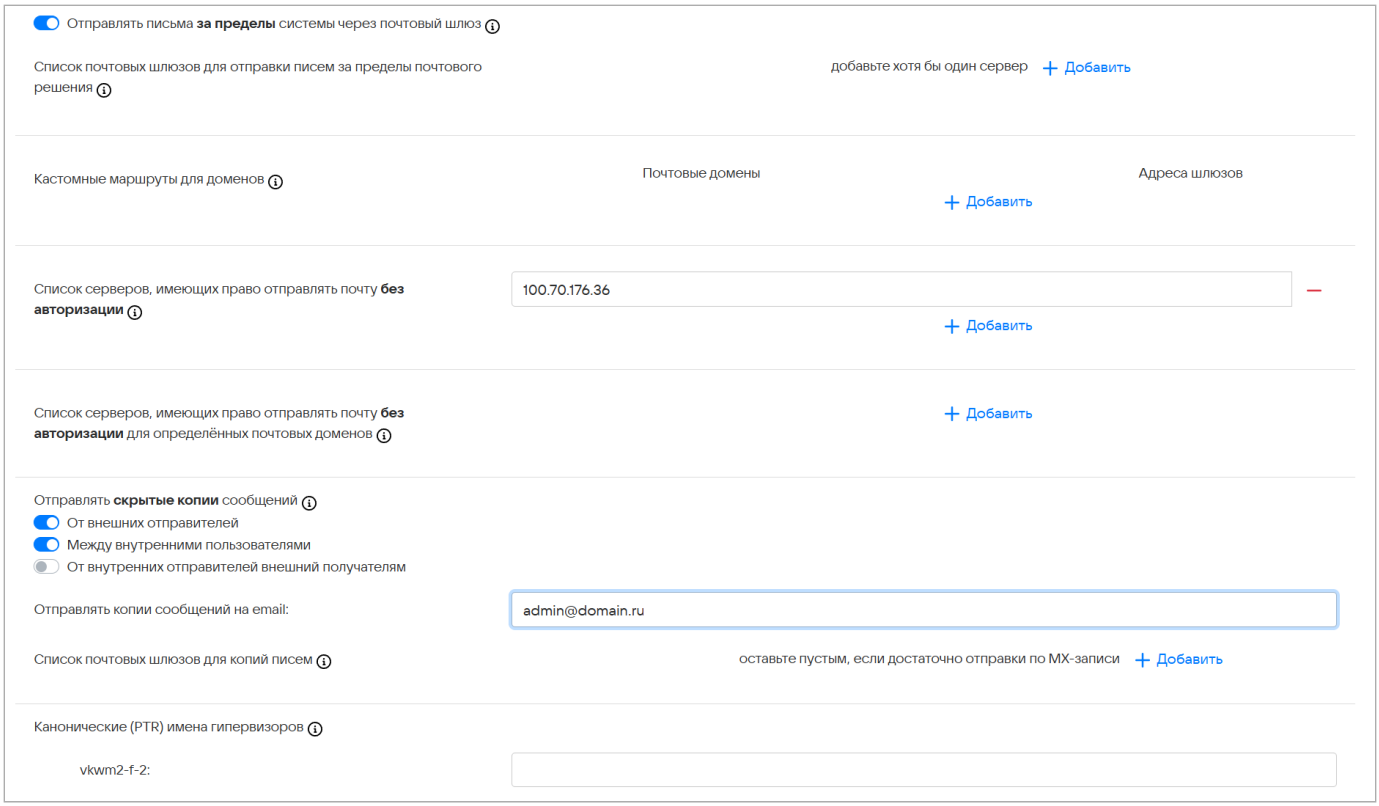
Внимание

Система расширенных транспортных правил при интеграции с внешними DLP системами может привести к дублированию исходящего почтового трафика и другим непредвиденным эффектам.

Ниже представлена схема движения трафика Почты при интеграции с системой DLP:



Черный — внутренний трафик Почты
Синий — внешний трафик Почты



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 сервис Почта. В этот же список можно внести серверы рассылки почты или в соответствии с их назначением МФУ, отсканированные документы с которых будут отправляться без авторизации. Почта, отправленная в Почту VK WorkSpace без авторизации, будет приниматься на порту **1025**.

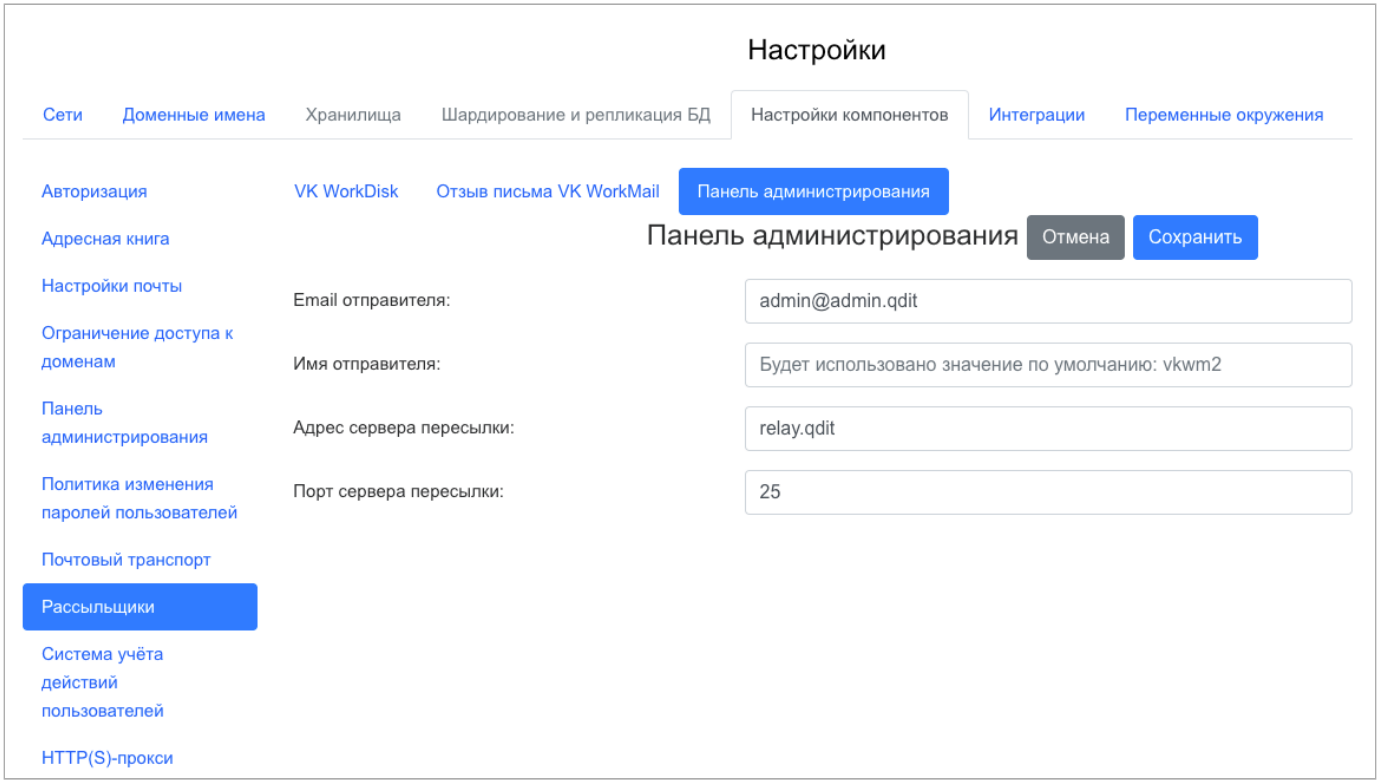
Список серверов, имеющих право отправлять почту без авторизации для определенных почтовых доменов — если вы планируете использовать несколько почтовых доменов, есть возможность добавить для каждого домена свои доверенные IP. Письма с указанных доменов должны отправляться на порт **1025**.

Отправлять скрытые копии сообщений — в почтовой системе VK WorkSpace реализована возможность отправки скрытых копий сообщений на специальный ящик: от внешних отправителей, сообщений между внутренними пользователями и от внутренних пользователей внешним. 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.

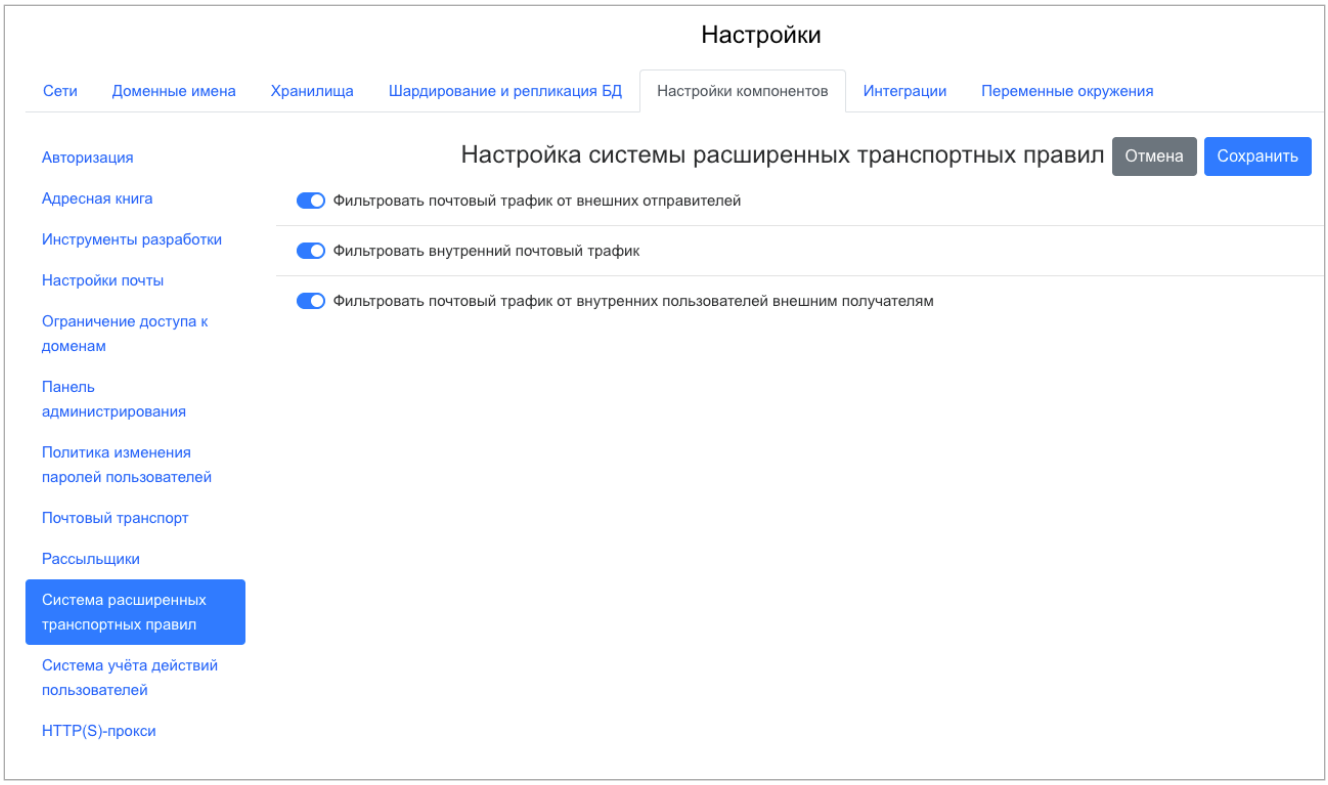


1. Введите email и имя отправителя.
2. Введите адрес и порт сервера рассылки.
3. Сохраните изменения.
4. Перейдите к списку ролей и запустите автоматическую установку, чтобы применить настройки.

Система расширенных транспортных правил

> **Внимание**
>
> Система расширенных транспортных правил при интеграции с внешними DLP системами может привести к дублированию исходящего почтового трафика и другим непредвиденным эффектам.

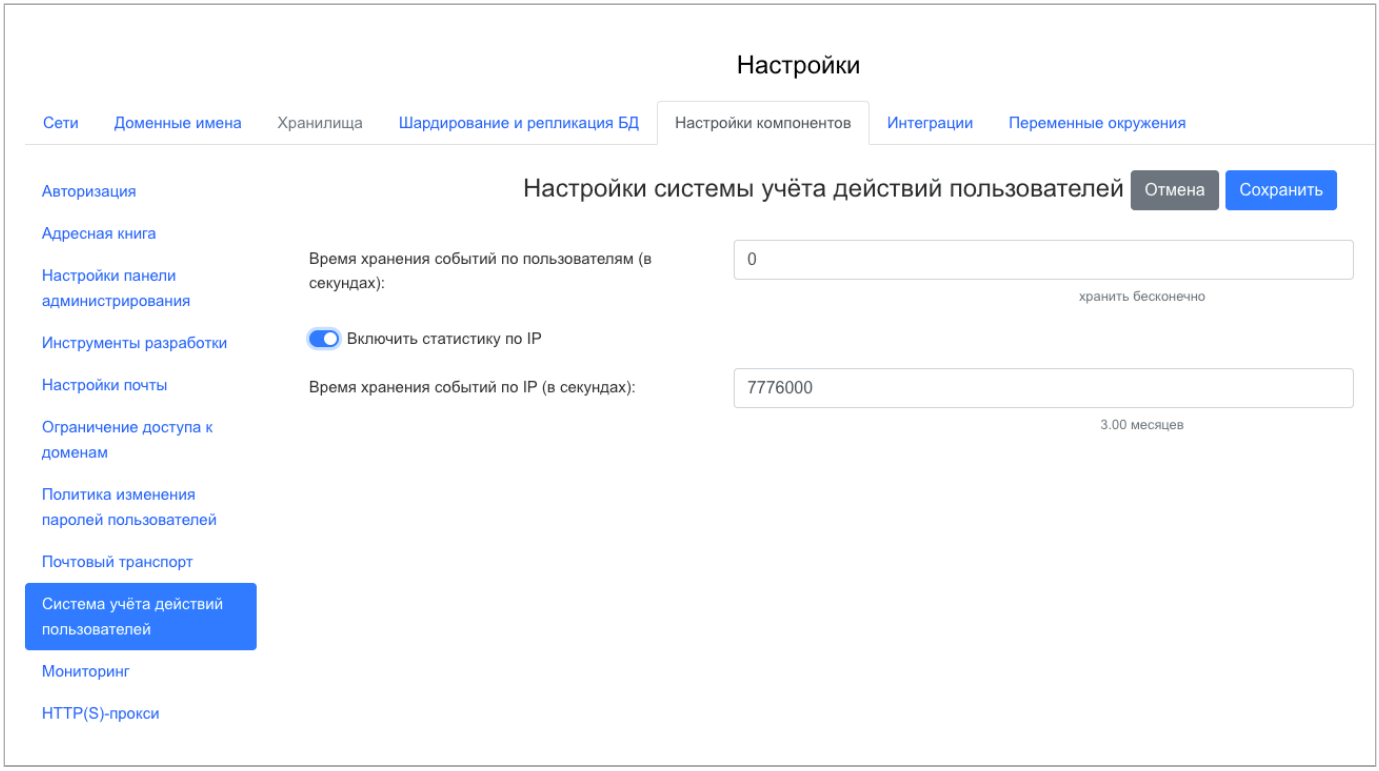
1. Нажмите на и перейдите в раздел **Продукты**.
2. Перейдите на вкладку **Почта**.
3. Включите флаг **Система расширенных транспортных правил**.
4. Перейдите к списку ролей и запустите автоматическую уставку.
5. Когда нужные роли сгенерируются, перейдите в раздел **Компоненты** → **Система расширенных транспортных правил** и включите нужные флаги.



Дальнейшая настройка транспортных правил производится в административной панели по завершении установки.

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.

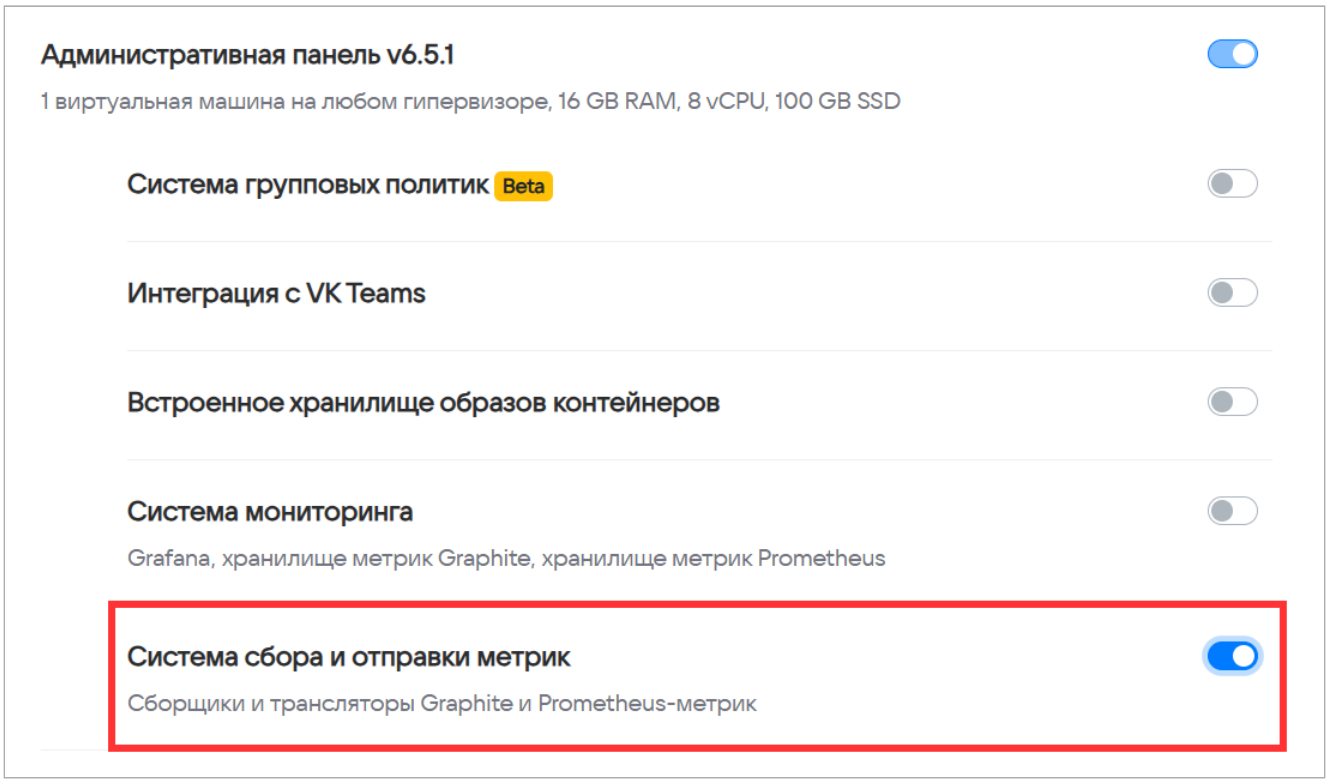
Включить статистику по IP — при включенном флаге появится окно для изменения срока хранения логов по IP.

Мониторинг

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

Чтобы включить внешнюю систему мониторинга:

1. Нажмите на  и перейдите в раздел **Продукты**.
2. Перейдите на вкладку **Администрирование**.
3. Включите 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.

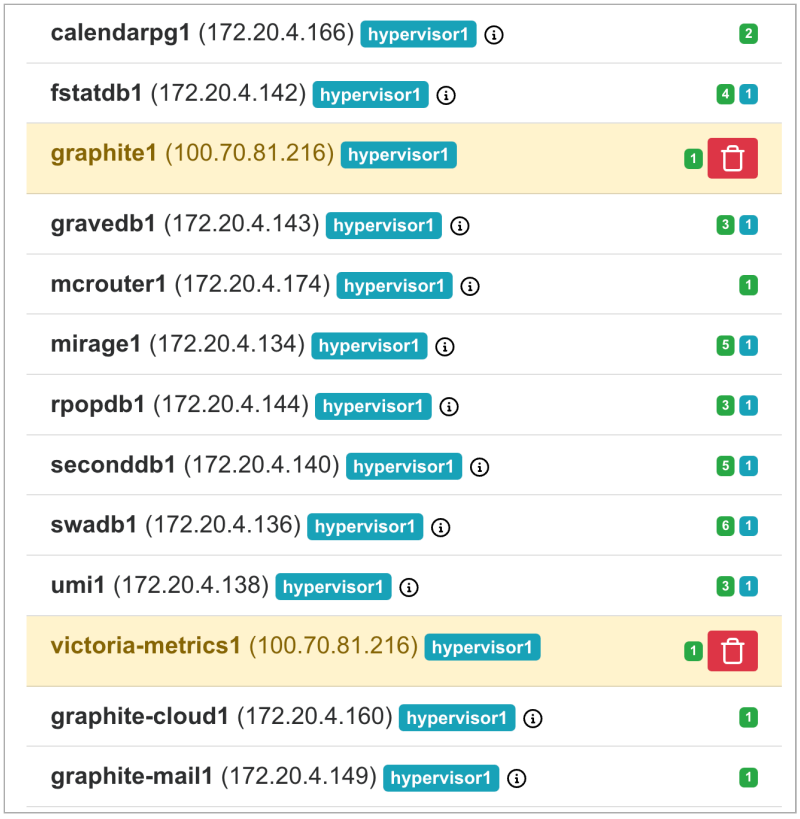
4. Сохраните изменения и вернитесь к списку ролей.
5. Внизу страницы нажмите на кнопку **Сгенерировать автоматически**, чтобы установщик сформировал новые роли.

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

6. Чтобы предотвратить возможные проблемы, перейдите в консоль и перезапустите установщик с помощью команды:

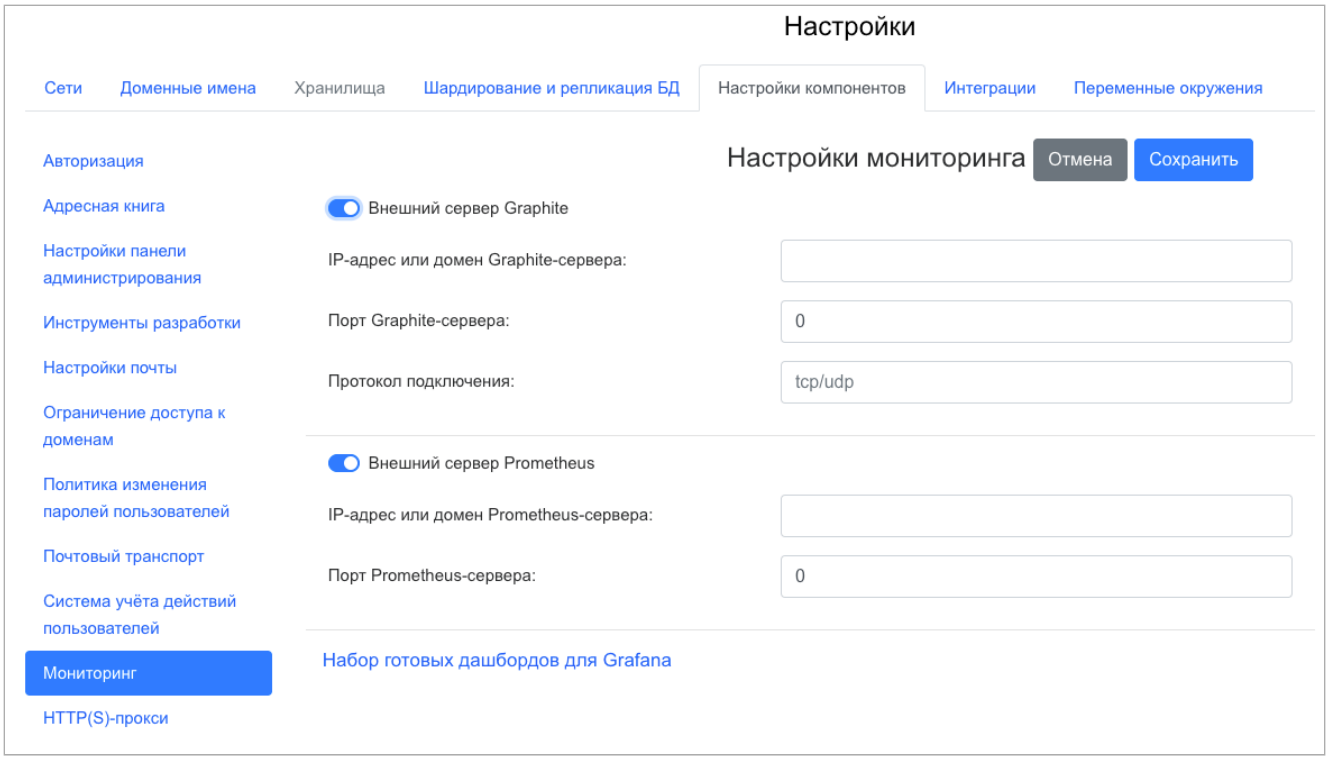
```
sudo systemctl restart deployer
```

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



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

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

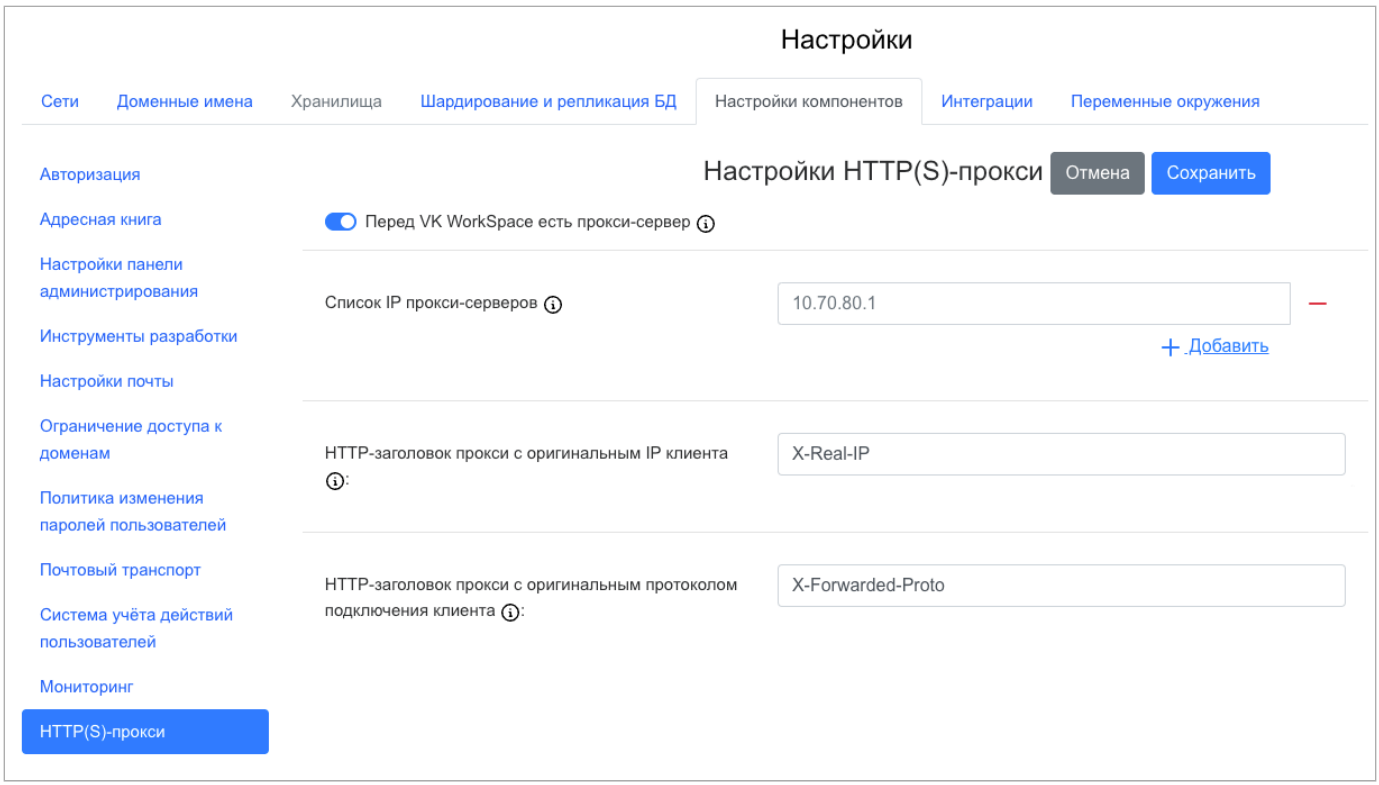


10. Сохраните изменения.

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

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 Почта 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.

Шаг 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 Мессенджер и ВКС и Почты — с помощью документа вы сможете настроить интеграцию между Мессенджер и ВКС и Почтой.

Миграция календарей по протоколу EWS — документ по настройке миграции событий из MS Exchange в сервис Почта.

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

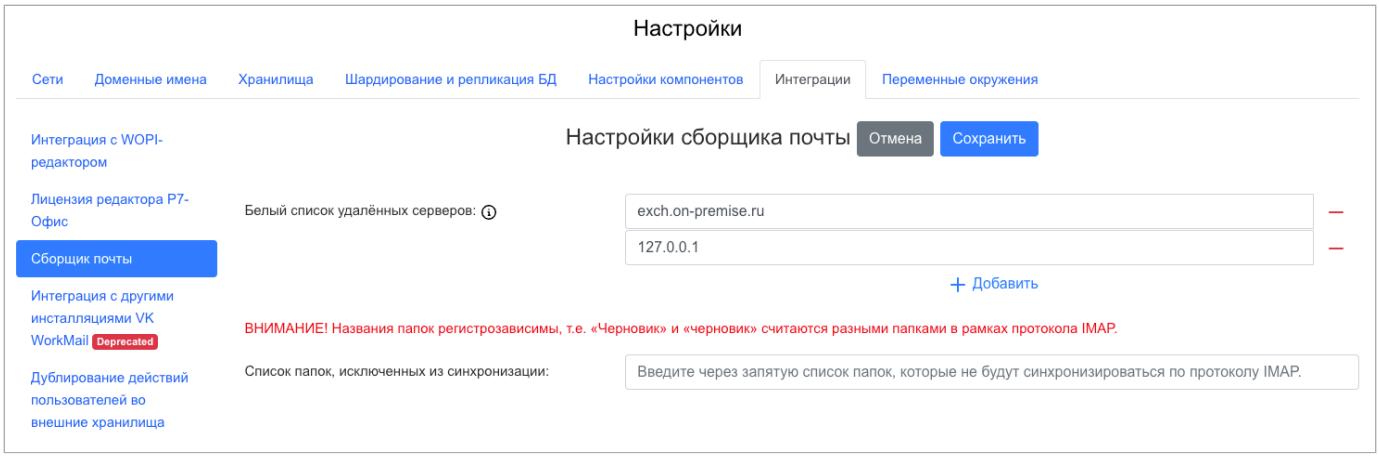
Аудит действий пользователей – в документе описаны предусмотренные в Почте системы аудита действий пользователя и их отличия. Описано, как включить сбор статистики по IP и настроить отправку событий во внешние хранилища.

Настроить дублирование действий пользователей во внешние хранилища

Сборщик почты

> **Внимание**
>
> Если планируется одновременная миграция более 100 почтовых ящиков, то выделите отдельные серверы для сборщиков. Минимальные требования к серверам из расчета не более чем на 2000 запущенных сборщиков: 8 vCPU и 32 GB RAM. После миграции ресурсы серверов освободятся.

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 — Почта 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.

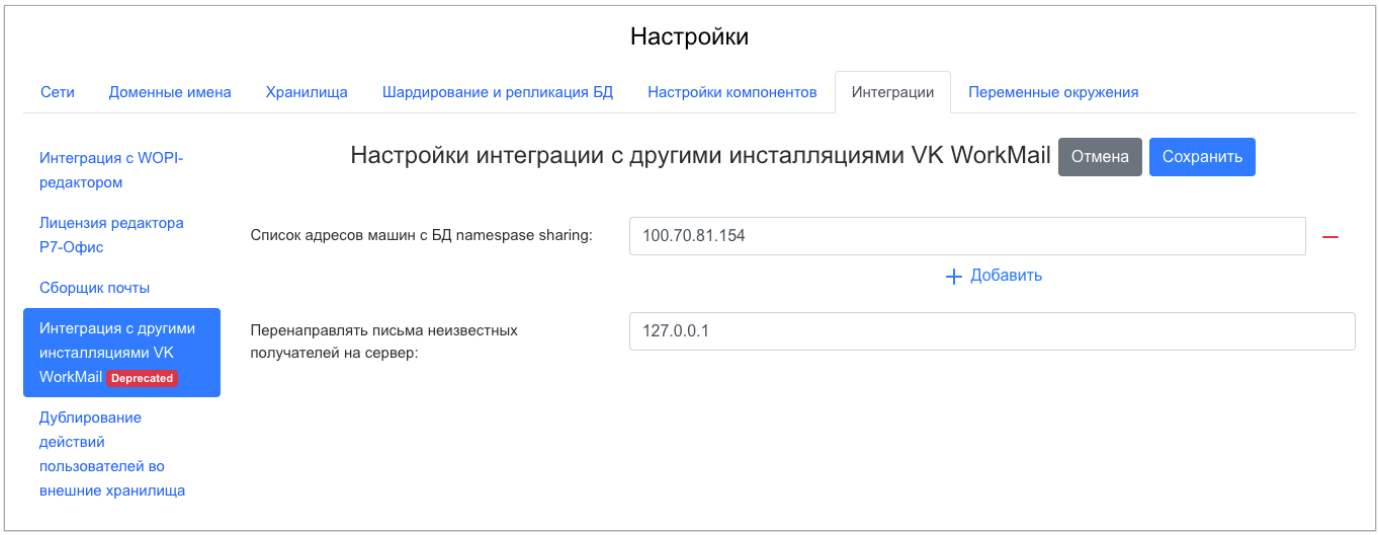
Список папок, исключенных из синхронизации — если у вас есть папки, которые не должны участвовать в синхронизациив соответствии с их назначением «Черновики» и «Удаленные», введите их названия через запятую **в строгом соответствии** с оригинальным названиям из вашей системы (названия папок регистрозависимы).

Интеграция с другими инсталляциями Почты

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

В разделе вы можете настроить интеграции с несколькими инсталляциями Почты 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 Почты. 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 инсталляциями, оставьте значение по умолчанию.

> **Внимание**
>
> Если в интеграции участвуют кластерные инсталляции Почты, 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 Почту, 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 Почты VK WorkSpace по завершении установки.

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

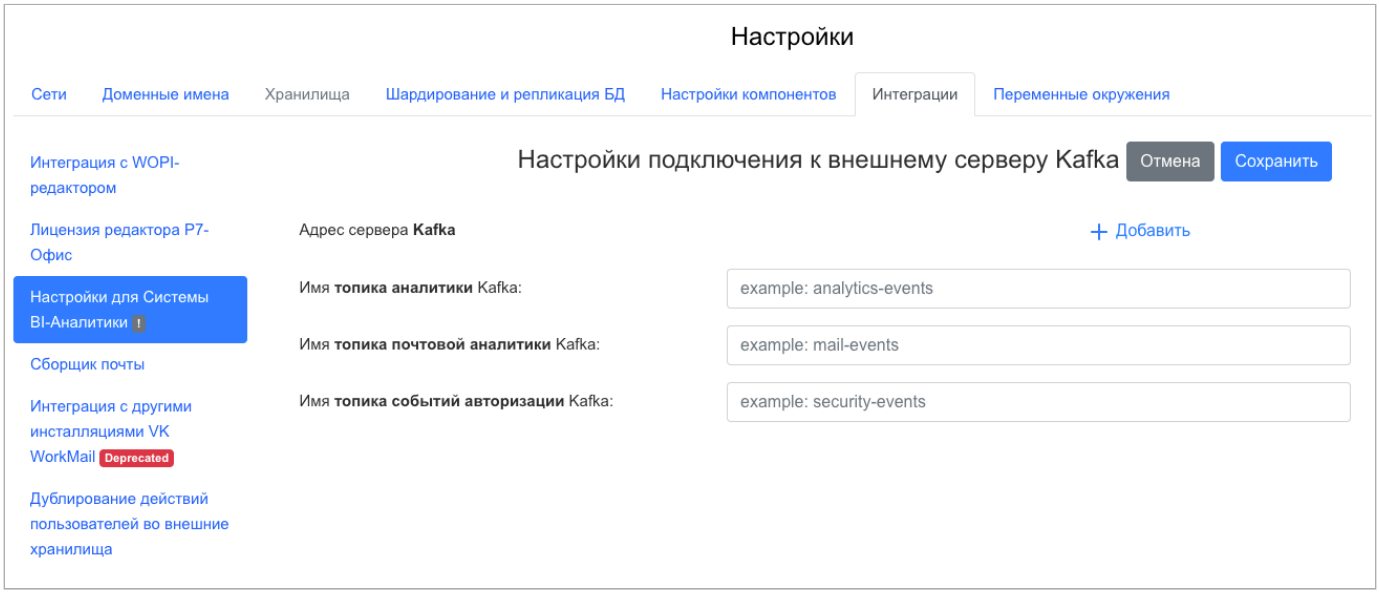
Сохраните изменения и перейдите к следующему шагу, нажав на кнопку **Далее**.

Настройки системы BI-аналитики

Чтобы получить возможность просматривать статистику использования Диска VK WorkSpace 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 в левом верхнем углу веб-интерфейса. Внизу страницы необходимо создать дополнительные роли.

1. Нажмите на кнопку **Добавить → Несколько контейнеров**.
2. В поле **Установлено не более:** введите значение **0**. Появятся контейнеры для распредления.
3. Добавьте контейнеры для Clickhouse на гипервизоры для хранилищ.
4. Если вы используете Kafka внутри инсталяции, распределите контейнеры с Kafka на гипервизоры для баз данных тем же способом (с помощью кнопки **Добавить**).
5. По окончании генерации контейнеров запустите **автоматическую установку** в общей строке состояния.

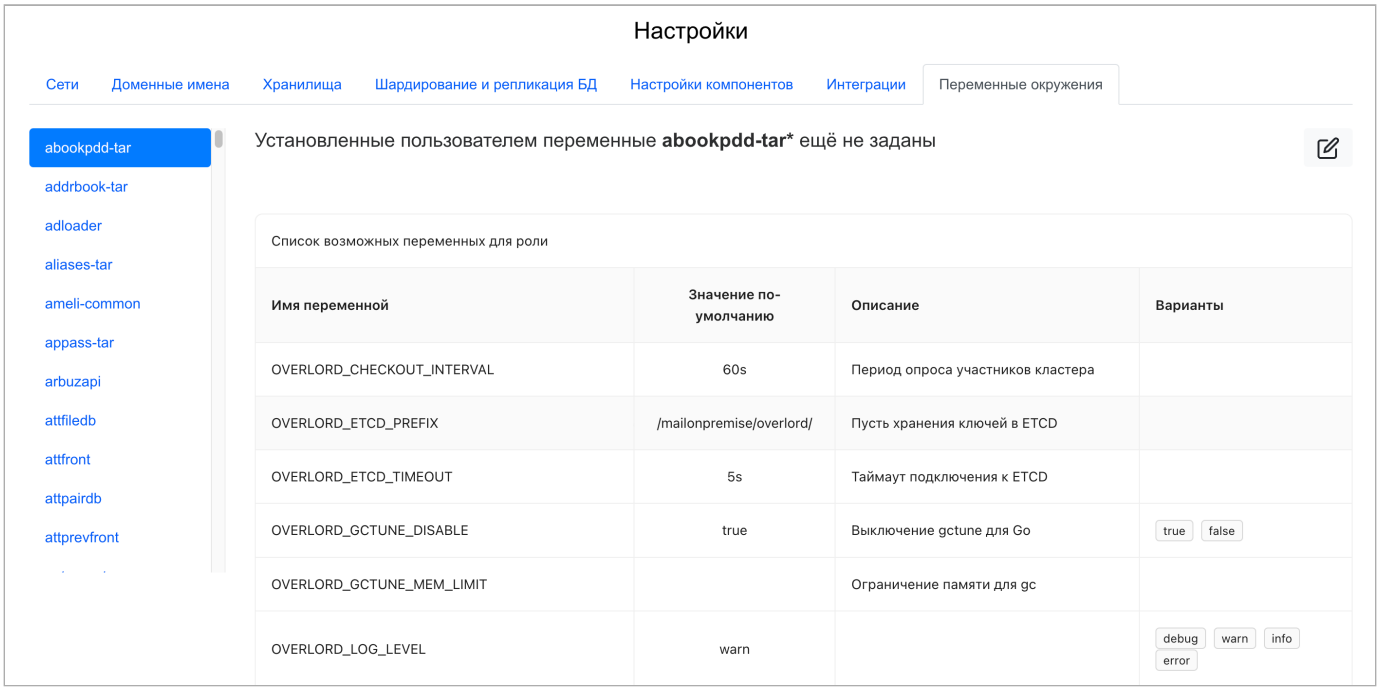
> **Рекомендация**
>
> Перед запуском автоматической установки оставьте включенными все проверки. Подробнее о работе проверок можно прочитать здесь: Диагностика системы в веб-интерфейсе установщика

Когда установка будет завершена, у вас появится возможность просматривать статистику Диска в панели администратора.

Шаг 13. Переменные окружения

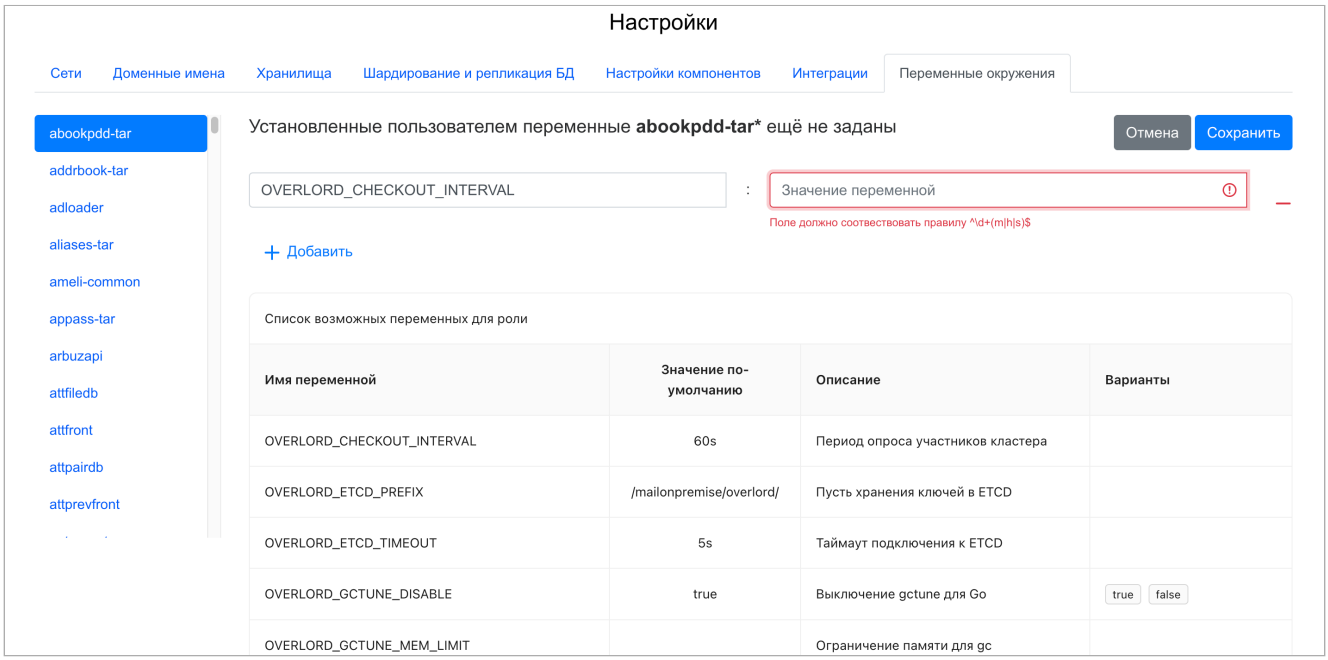
В разделе производится настройка кастомных переменных почтовой системы.

> **Внимание**
>
> Настройка переменных окружения возможна только после консультации с представителем VK.



Чтобы добавить кастомную переменную:

1. Нажмите на кнопку редактирования.
2. Нажмите кнопку **Добавить**.
3. В выпадающем меню выберите название переменной.
4. Введите значение переменной. Значение переменной должно быть введено корректно, иначе установщик не позволит создать переменную.



5. Нажмите на кнопку **Сохранить**.
6. Нажмите на кнопку **Далее** для перехода к следующему шагу.

Какие переменные рекомендуется установить для 5000 пользователей

Для сервиса **xtaz** установите следующую переменную:

Название переменной	Значение переменной
MEMTX_MEMORY	3

Для сервиса **mpop** установите следующие переменные:

Название переменной	Значение переменной
HTTPD_KEEP_ALIVE_TIMEOUT	5
HTTPD_LISTEN_BACKLOG	1024
HTTPD_MAX_CLIENTS	150
HTTPD_MAX_KEEP_ALIVE_REQUESTS	100
HTTPD_MAX_REQUESTS_PER_CHILD	25
HTTPD_MAX_SPARE_SERVERS	30
HTTPD_MIN_SPARE_SERVERS	20
HTTPD_SERVER_LIMIT	150
HTTPD_START_SERVERS	20

Для сервиса **crow-index** установите следующие переменные:

Название переменной	Значение переменной
CROW_INDEX_DATABASE_BLOCK_CACHE_SIZE	5368709120
CROW_INDEX_DATABASE_CONTENT_MEM_TABLE	536870912
CROW_INDEX_DATABASE_COUNT_MEM_TABLE	104857600
CROW_INDEX_DATABASE_DOCUMENT_MEM_TABLE	268435456

Название переменной	Значение переменной
CROW_INDEX_DATABASE_MAILBOX_MEM_TABLE	104857600
CROW_INDEX_DATABASE_MESCALITO_MEM_TABLE	268435456
CROW_INDEX_DATABASE_SEARCH_MEM_TABLE	536870912
CROW_INDEX_DATABASE_SUGGEST_MEM_TABLE	268435456

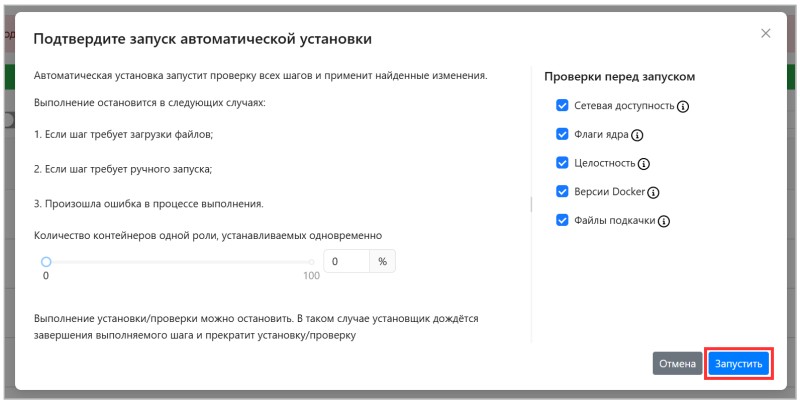
Для сервиса **crow-frontend** установите следующие переменные:

Название переменной	Значение переменной
CROW_FRONTEND_ASYNC_MAX_INFLIGHT_PER_WATCHER	10
CROW_FRONTEND_ASYNC_USER_DELAY	5m
CROW_FRONTEND_REBUS_EMAIL_FETCHER_WORKERS_COUNT	200
CROW_FRONTEND_REINDEX_MAX_FETCH_ATTACHES	10
CROW_FRONTEND_REINDEX_MAX_FETCH_TOTAL	25

Шаг 14. Запуск установки всех машин

1. Кликните по кнопке **Play** рядом с общей строкой состояния в верхней части экрана.
2. Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**.

> **Рекомендация**
>
> Перед запуском автоматической установки оставьте включенными все проверки. Подробнее о работе проверок можно прочитать здесь: Диагностика системы в веб-интерфейсе установщика



В зависимости от этапа установки будет меняться цвет индикатора:

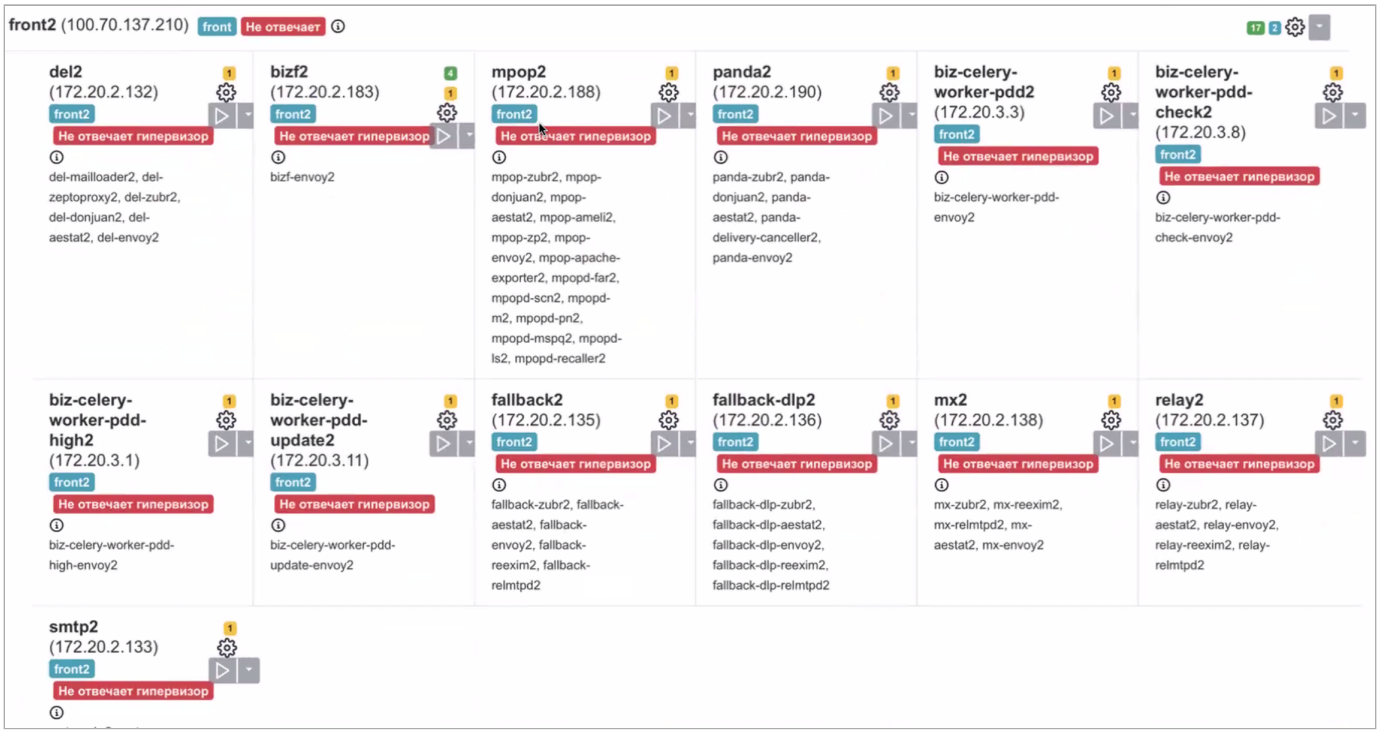
- **Серый** — в ожидании начала генерации;
- **Синий** — в процессе генерации;
- **Желтый** — шаг будет повторен (автоматически);
- **Красный** — ошибка.

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

Если в процессе установки и настройки системы происходят изменения конфигурации, некоторые задачи могут потребовать повторного выполнения.

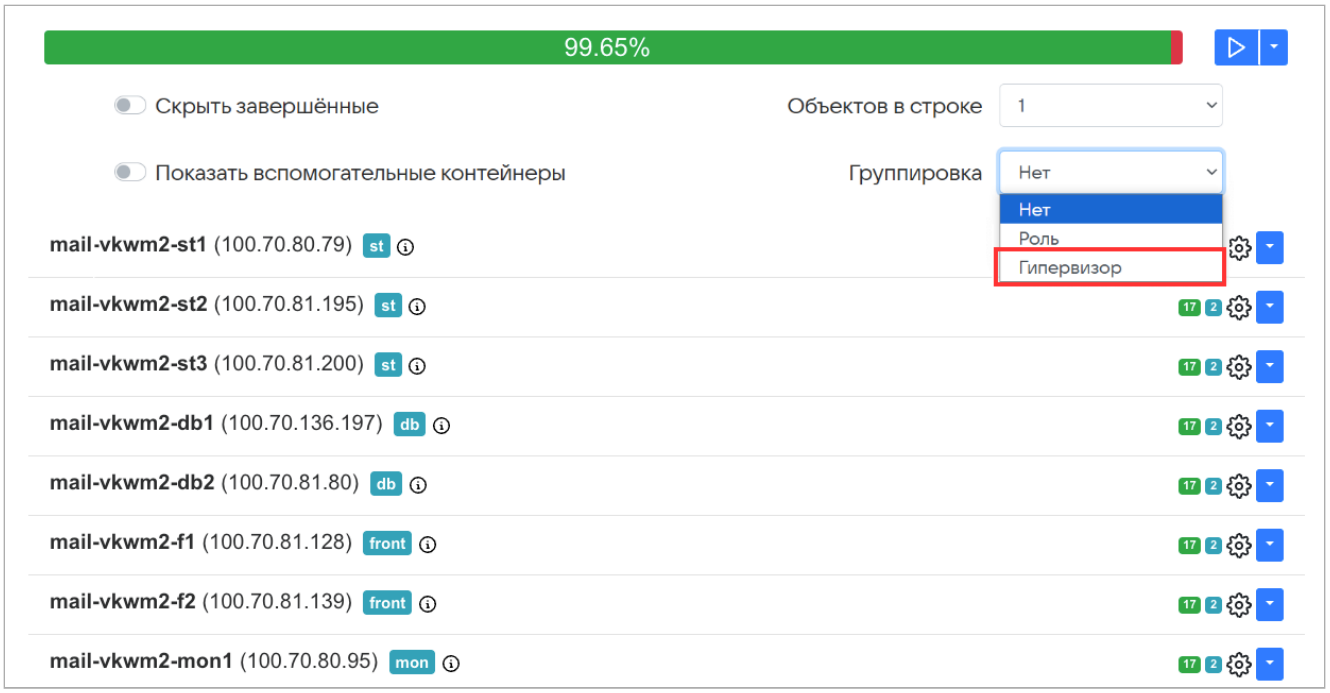
Для повторного запуска необходимо нажать на кнопку **Play** в общей строке состояния в верхней части экрана или рядом с названием конкретного контейнера.

При появлении ошибок на гипервизоре на нем появится тег **Не отвечает**, а на контейнерах, относящихся к этому гипервизору — **Не отвечает гипервизор**.

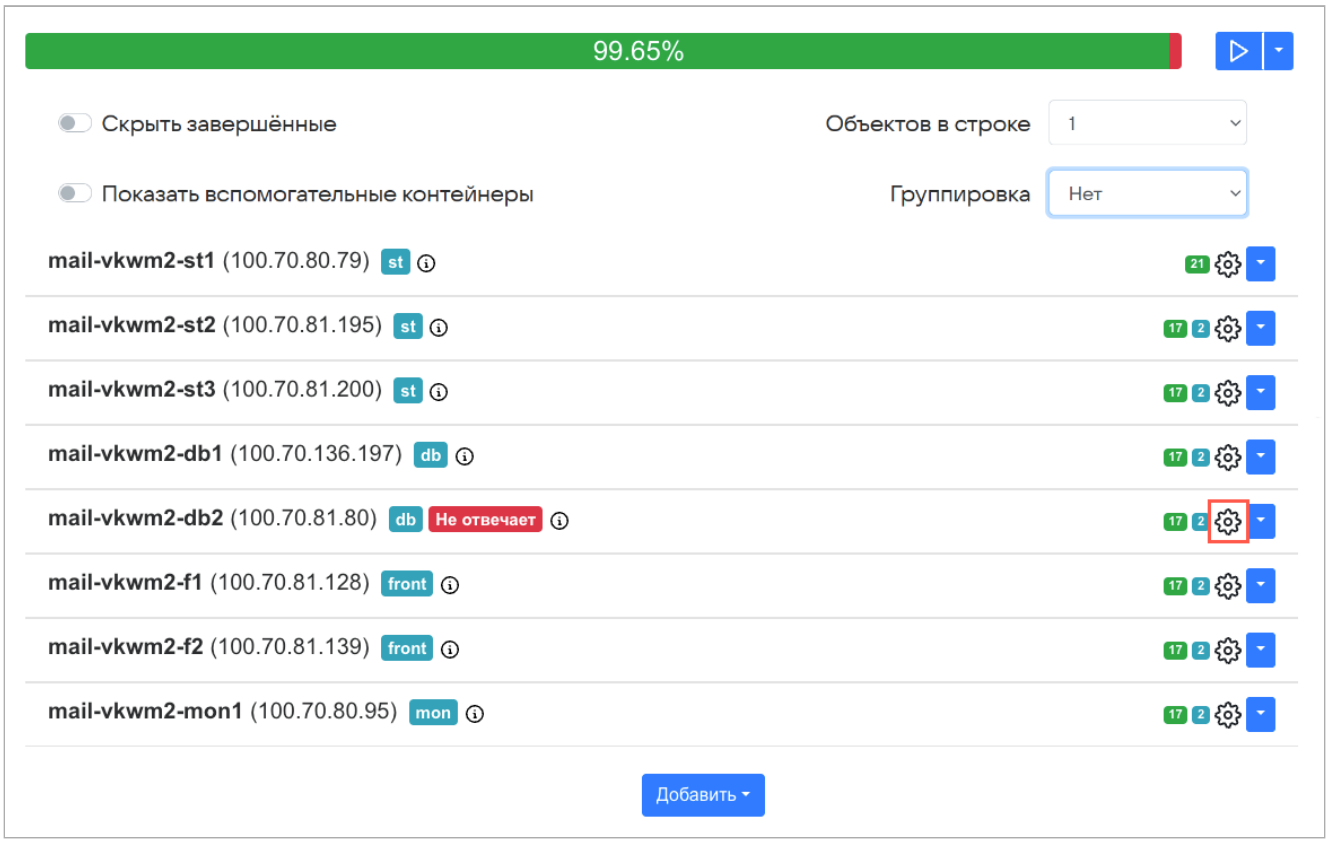


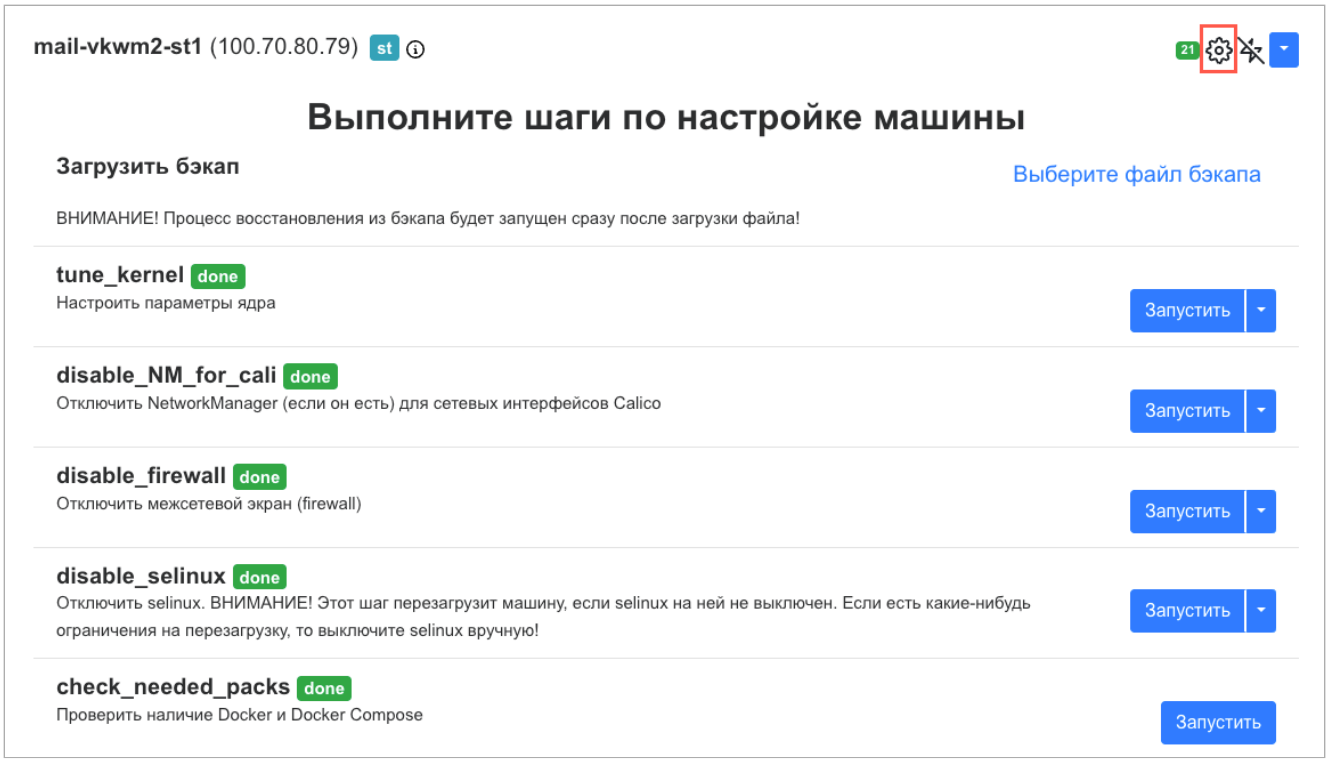
Чтобы продолжить установку:

1. Сгруппируйте объекты по гипервизору — так вам будет наглядно видно, на каком гипервизоре ошибка.

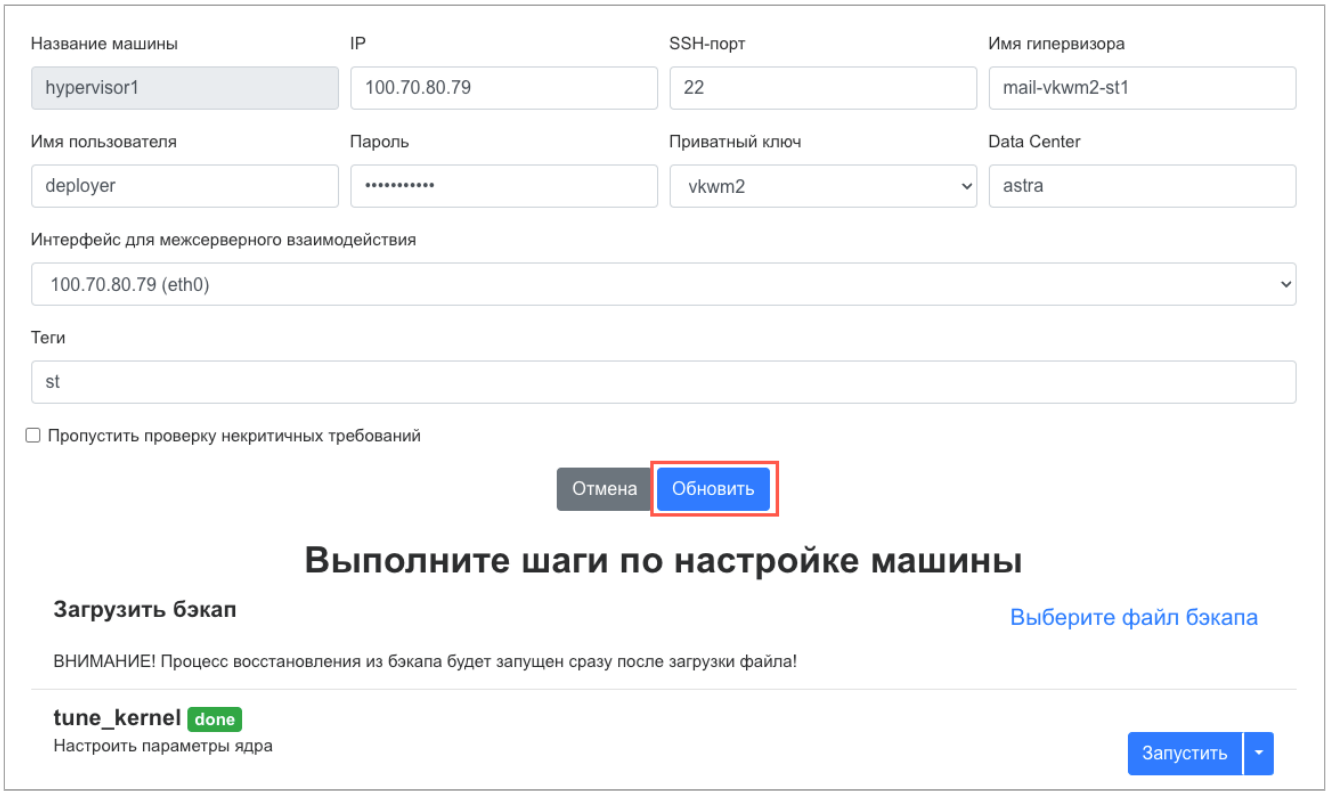


2. После этого перейдите в командную строку и устраните ошибку. По завершении необходимо нажать на шестеренку в строке гипервизора, на котором была ошибка, затем на странице в списке шагов на гипервизоре.





3. В окне настроек гипервизора нажмите на кнопку **Обновить**.

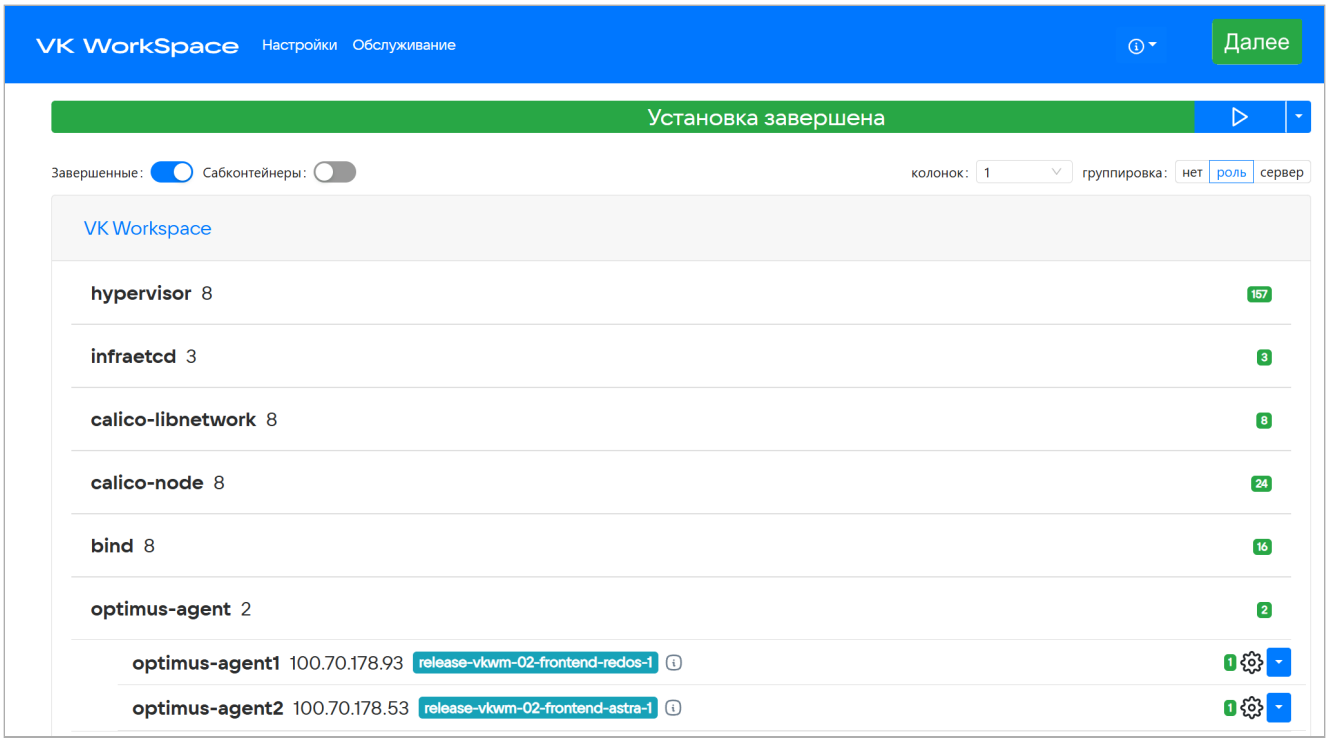


4. Повторно запустите автоматическую установку.

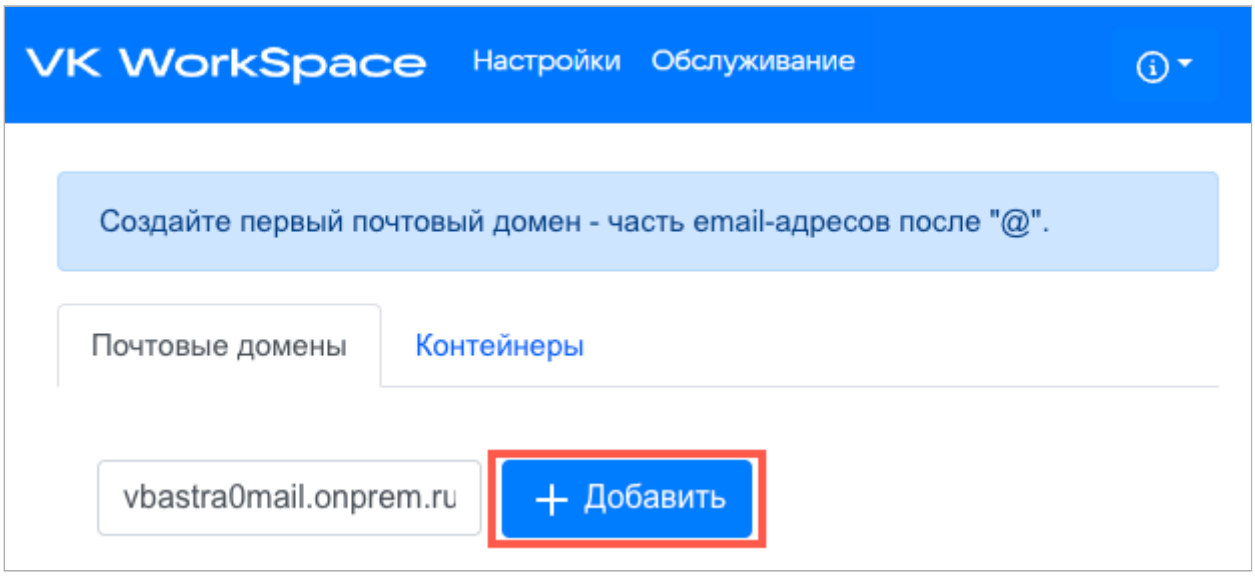
Шаг 15. Завершение установки, инициализация домена и вход в панель администратора

Когда установка будет завершена, соответствующий статус отобразится в строке состояния.

1. Нажмите на кнопку **Далее**.



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

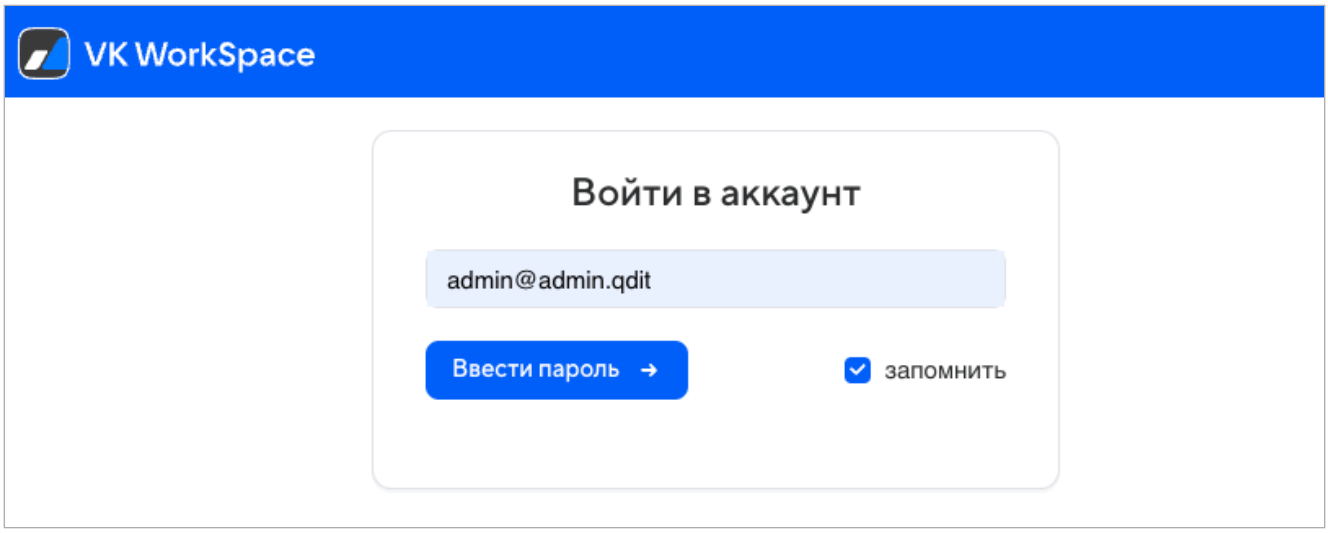


> **Внимание**
>
> С версии 1.24 в Почте VK WorkSpace все домены проверяются на соответствие лицензии. Если домен не входит в лицензию — пользователи этого домена не смогут обмениваться сообщениями. Это условие также распространяется на синонимы доменов.

Откроется новая вкладка, на которой необходимо авторизоваться:

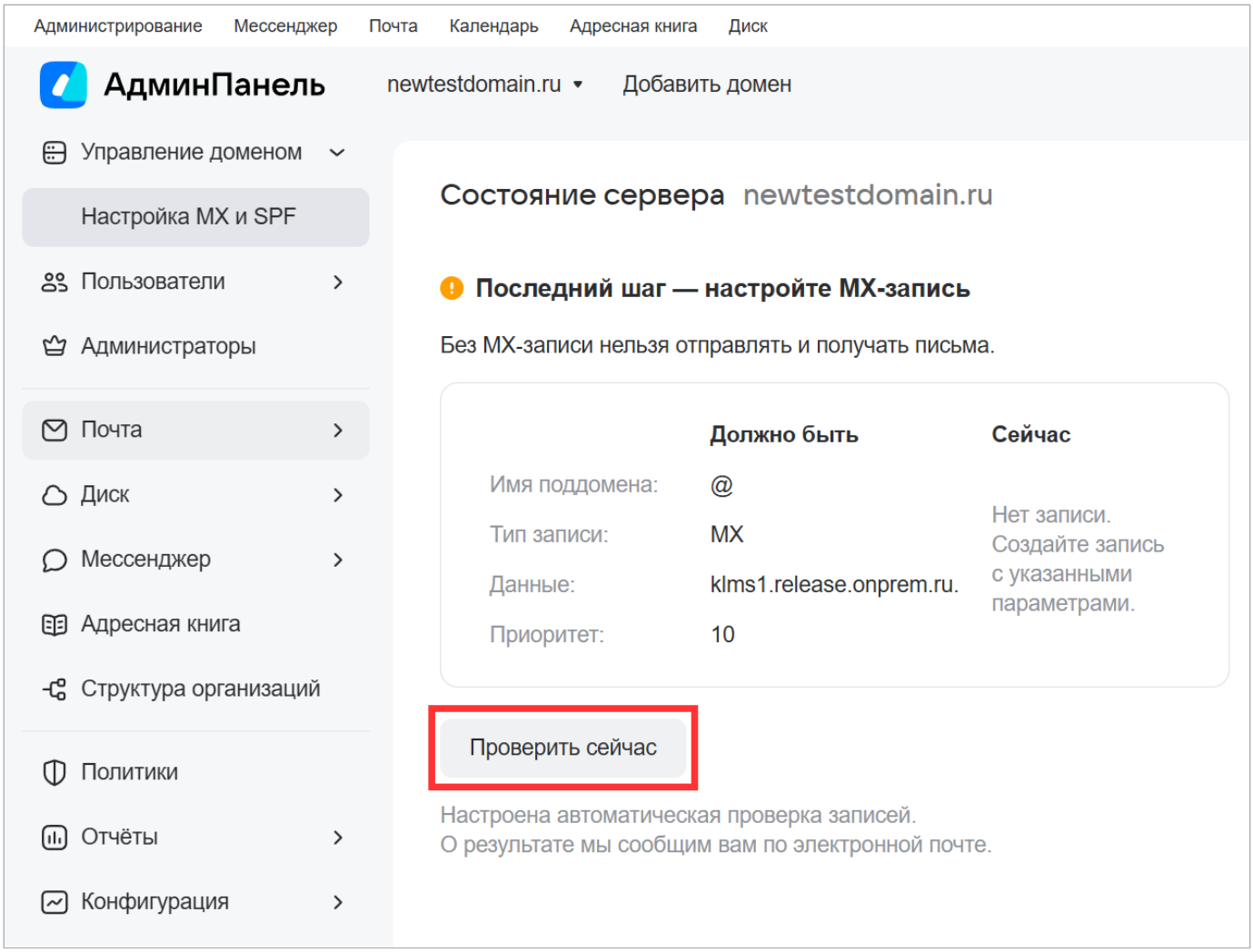
- Имя пользователя — **admin@admin.qdit**.
- Пароль находится в файле — **bizOwner.pass**, для его просмотра введите в консоли команду: `cat <путь до директории с установщиком>/bizOwner.pass`.

> **Примечание**
>
> Пароль пользователя admin@admin.qdit хранится зашифрованным в базе данных. Он записывается в файле bizOwner.pass в открытом виде только для администратора при первичной установке. Скопируйте пароль в надёжное место, и удалите bizOwner.pass, чтобы злоумышленники не могли получить пароль. Если пароль администратора утерян, то создайте новый с помощью инструкции: Как изменить пароль пользователя admin@admin.qdit?.

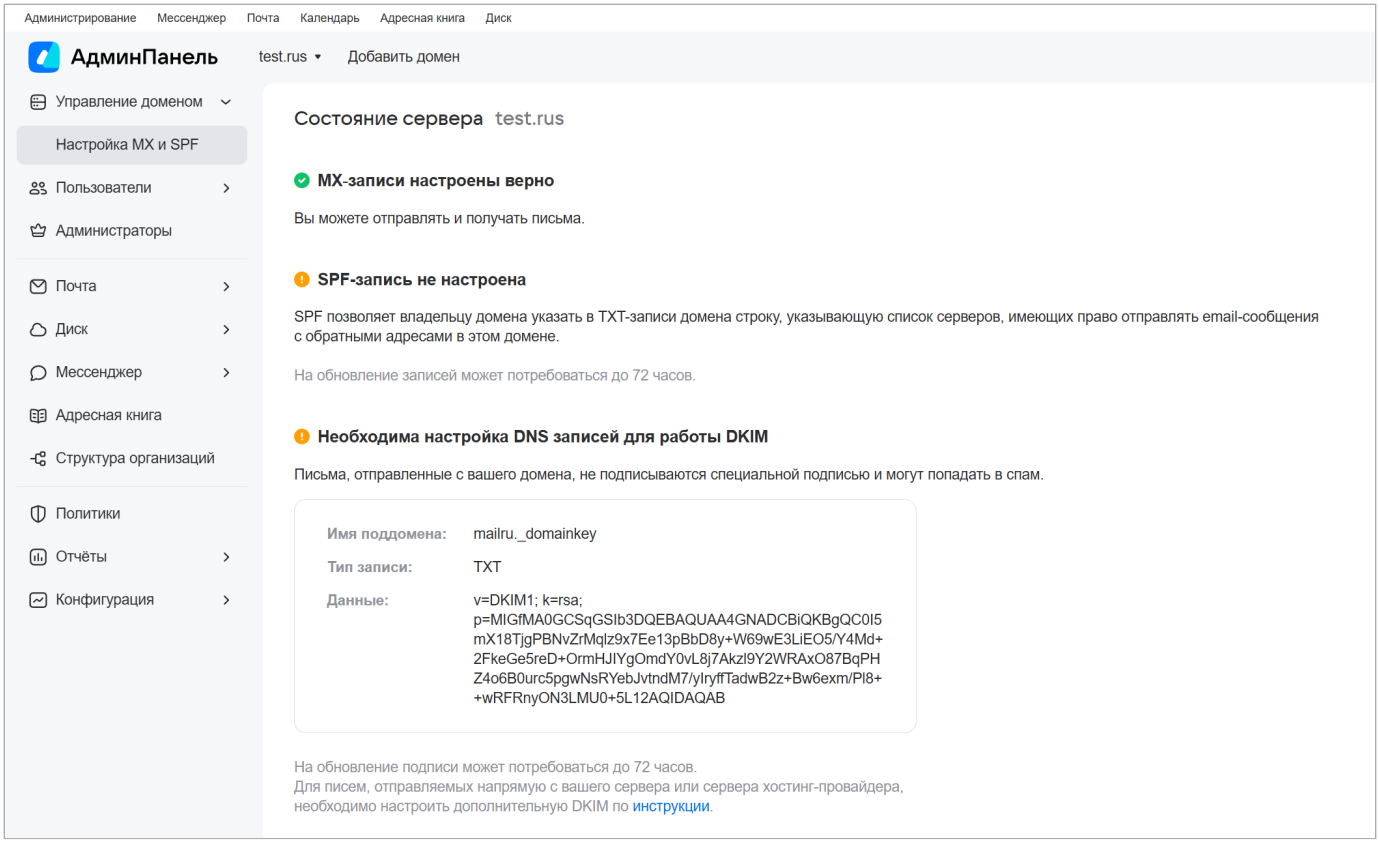


Если логин и пароль были введены правильно, вы попадете в панель администратора.

3. Нажмите на кнопку **Проверить сейчас**, чтобы проверить **MX-запись**.



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

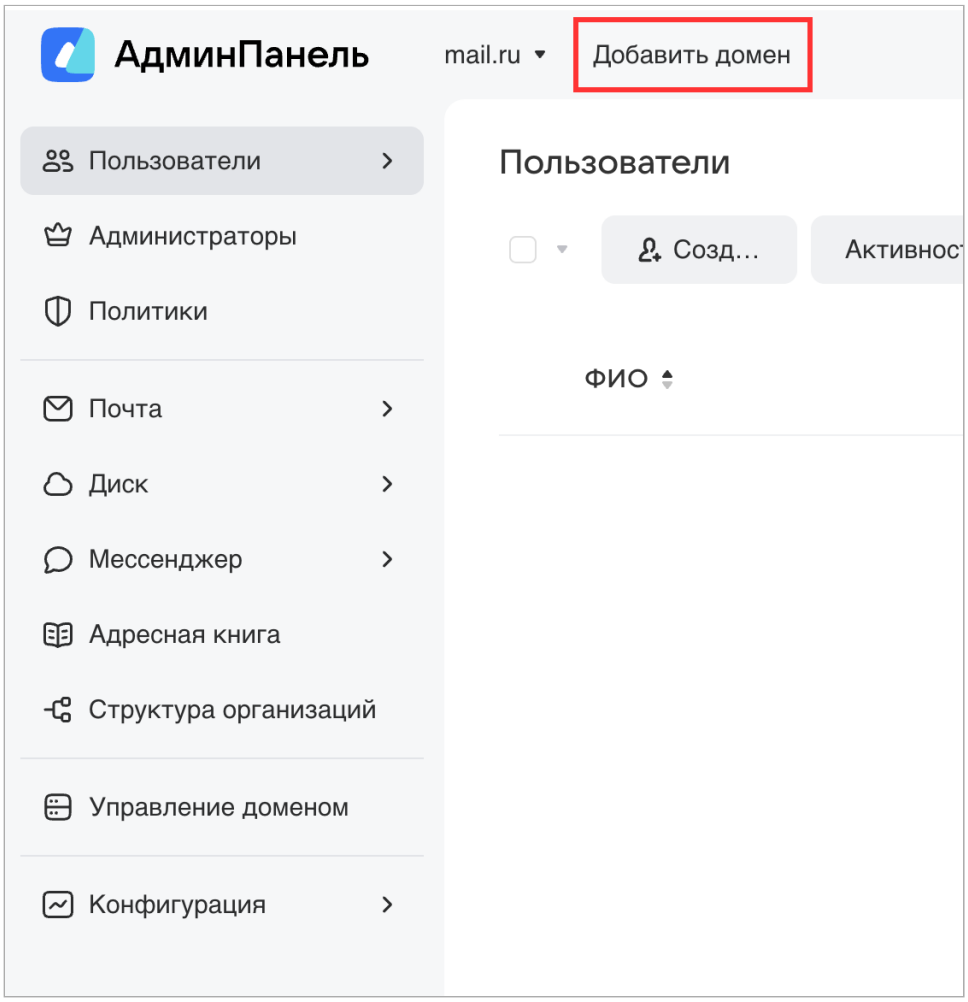


После проверки MX-записи установку можно считать оконченной. Также потребуется настройка **SPF-записи** и **DKIM-подписи**. Инструкции по их настройке вы найдете по ссылке.

> **Внимание**
>
> 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.

Шаг 16. Добавление дополнительных доменов

Если вы планируете использовать несколько доменов, добавьте их с помощью кнопки **Добавить домен**.



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

Внимание

С версии 1.24 в Почте VK WorkSpace все домены проверяются на соответствие лицензии. Если домен не входит в лицензию — пользователи этого домена не смогут обмениваться сообщениями. Это условие также распространяется на синонимы доменов.

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
```

Автор: Груздев Никита

11 июня 2026 г.