# Доска VK WorkSpace

## Установка версии 26.1 на одну машину



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

# Оглавление

# Назначение документа

В документе описана процедура установки Доски VK WorkSpace в минимальной рабочей конфигурации на одну виртуальную машину. Под продуктивной установкой подразумевается установка Доски на сервера клиента и настройка компонентов для последующего использования сотрудниками.

# 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.

# Дополнительная документация

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

Как обновить лицензионный ключ

Настройка интеграции с Active Directory

# Технические требования

Поддерживаемые операционные системы для установки Доски:

- **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 Доска 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.
- 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.

# 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 на СХД.

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

Или перезагрузите операционную систему.

# Требования к ресурсам сервера

По вопросам создания сайзинг-модели обращайтесь к сотрудникам или партнерам компании VK. Продуктивная версия устанавливается на один сервер со следующей конфигурацией:

- 32 vCPU;
- 96 GB RAM;
- 1000 GB SSD;
- HDD для вложений, объем рассчитывается на основании сайзинга.

**Рекомендация**

Используйте процессоры Intel Xeon Gold 6140 и новее.

# Таблица совместимости

| Технология | Версия |
|---|---|
| Мессенджер и ВКС | не старше двух последних версий |
| MS Exchange Server | 2013/2016 |

| Технология | Версия |
| --- | --- |
| 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 для установки

Представители VK предоставили вам следующие данные:

- Ссылку на скачивание дистрибутива Доски 26.1.
- Пароль от архива с дистрибутивом.
- Лицензионный ключ.
- Комплект документации.

Также вам потребуется:

- Набор DNS-записей: A, CNAME, MX, SPF, TXT, NS.
- Поддержка процессорами набора инструкций 3DNow, ADX, AES, AVX, AVX2, BMI, BMI2, CMOV, MMX, MODE64, NOT64BITMODE, NOVLX, PCLMUL, SHA, SSE1, SSE2, SSE41, SSE42, SSSE3 и XOP.
- DKIM-подпись с селекторами для каждого домена (или несколько DKIM с разными селекторами для одного домена).
- Доступ к серверу по SSH с правами администратора (вход по ключу или по паролю).
- Локальная сеть 1 GbE или 10 GbE.
- Отключить swap.
- Сертификаты SSL для каждого CNAME или Wildcard-сертификат для домена.
- Доступ к портам: 25, 80, 143, 443, 465, 993, 1025.
- 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 Доски, на ваших серверах должны быть доступны только необходимые порты. Для доступа к веб-интерфейсу: 80 (http), 443 (https). 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

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 Доски `onprem.ru`, тогда в сертификат необходимо добавить один домен: `*.onprem.ru`

# Какие протоколы использует Доска

- **HTTPS** для доступа к веб-интерфейсу Доски с использованием **TLS**.

- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента.
- **IP in IP** — протокол туннелирования IP.

# Обязательные предварительные действия

## Настройте ротацию логов в journald

Выполните шаги из инструкции Как настроить ротацию логов в journald.

## Создание DNS-записей

Для работы Доски вам нужны:

- Основной домен для Доски
- Набор A- или CNAME-записей.

Для примера в документе будет использоваться **Домен для сервисов Доски** — `onprem.ru`.

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

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

| Назначение домена | Имя домена | Пример |
|---|---|---|
| Домен для проверки доступа | access | access.onprem.ru |
| Веб-интерфейс авторизации | account | account.onprem.ru |
| Доменная авторизация (внутренние запросы браузера) | auth | auth.onprem.ru |
| Интерфейс администрирования | biz | biz.onprem.ru |

| Назначение домена | Имя домена | Пример |
|---|---|---|
| Интеграция с API Почты VK WorkSpace | corsapi | corsapi.onprem.ru |
| Скачивание супераппа VK WorkSpace | dl | dl.mail.onprem.ru |
| Сервис аватарок | filin | filin.onprem.ru |
| Исполняемые статические данные | imgs | imgs.onprem.ru |
| OAUTH2-авторизация | o2 | o2.onprem.ru |
| Общепортальные сервисы авторизации | portal | portal.onprem.ru |
| Домен для облака, реализующего API S3 | hb | hb.onprem.ru |
| Домен для server side взаимодействия с Почтой VK WorkSpace | serverside-api | serverside-api.onprem.ru |
| Сервер авторизации (межсерверные запросы) | swa | swa.onprem.ru |
| Адрес клиентского API Мессенджера и ВКС | u | u.onprem.ru |
| Основной домен Доски | board | board.onprem.ru |

**Внимание**

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

# Дисковое пространство

Минимальный рекомендуемый объем памяти для разделов:

- 5 Гб — `/boot`;
- 40 Гб — `/`;
- 100 Гб — `/home`;
- 40 Гб — `/var/log`;
- 150 Гб — `/var/lib/docker`;
- 200 Гб — `/opt`;

• 40 Гб — `/tmp`.

В зависимости от количества пользователей может быть увеличен объем памяти раздела `/opt/mailOnPremise/dockerVolumes`.

> **Внимание**
>
> Отключите файл подкачки (SWAP).

## Подключение дисков

Если вы планируете монтирование дополнительных дисков, рекомендуется подключить их до начала установки. 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>
```

# 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. Создание пользователя deployer

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. Распаковка дистрибутива

Распакуйте дистрибутив под пользователя deployer (в директорию `/home/deployer`). Вы можете распаковать архив с дистрибутивом и в другую папку или создать подпапку.

Нет принципиальной 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 -P <пароль> <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 -P <пароль> <имя_архива>
```

**MosOS Arbat**

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

export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

unzip -o -P <пароль> <имя_архива>
```

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

# Шаг 3. Разрешить Port Forwarding

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

```
AllowTcpForwarding yes
```

# Шаг 4. Запуск установщика как сервиса

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:

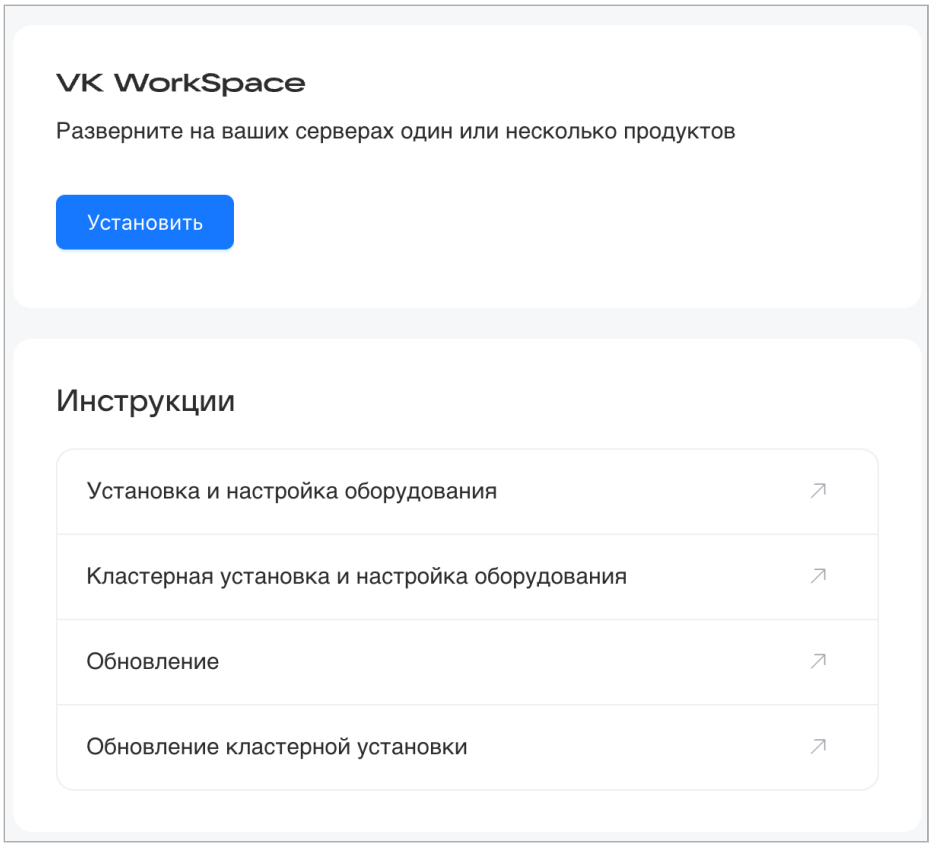
```
journalctl -u deployer
```

И убедитесь, что порт 8888 слушают:

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

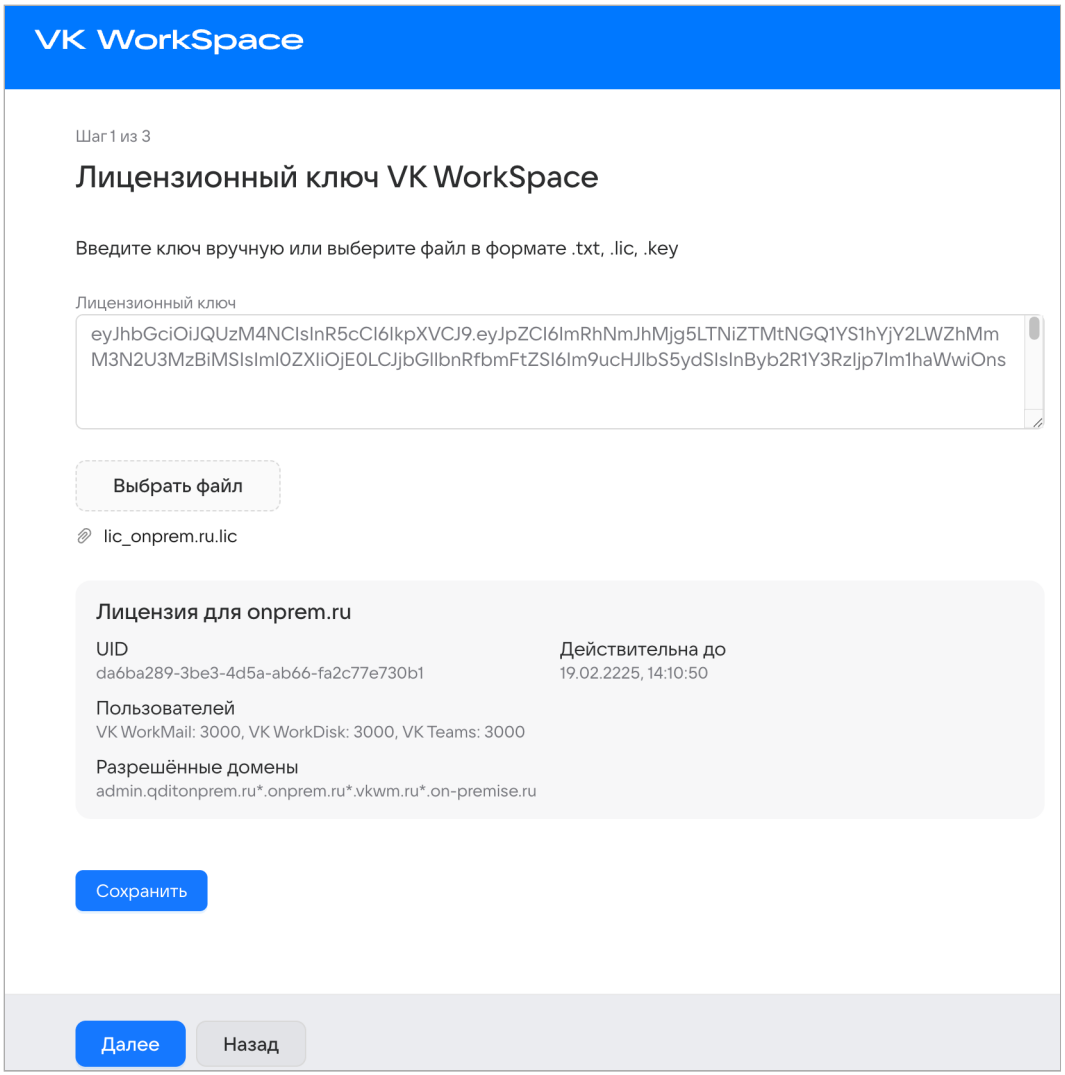
# Действия в веб-интерфейсе установщика

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 флаг **Доска VK WorkSpace**.
2. Нажмите на кнопку **Далее**.
3. Включите нужные вам компоненты в разделе **Администрирование**.

> **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 |
| --- | --- |
| Авторизация | **Обязательный продукт**. Сервисы, расширяющие возможности обычной авторизации |
| **Авторизация**. Single sign-on аутентификация | SSO позволяет пользователю войти в систему один раз и получить доступ к нескольким связанным приложениям или сервисам |
| Система аудита действий пользователя | Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB) |
| Система BI-аналитики | **Beta** |
| **Система BI-аналитики.** Kafka внутри инсталляции | 16 GB RAM, 8 vCPU |
| 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** |
| **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 | |

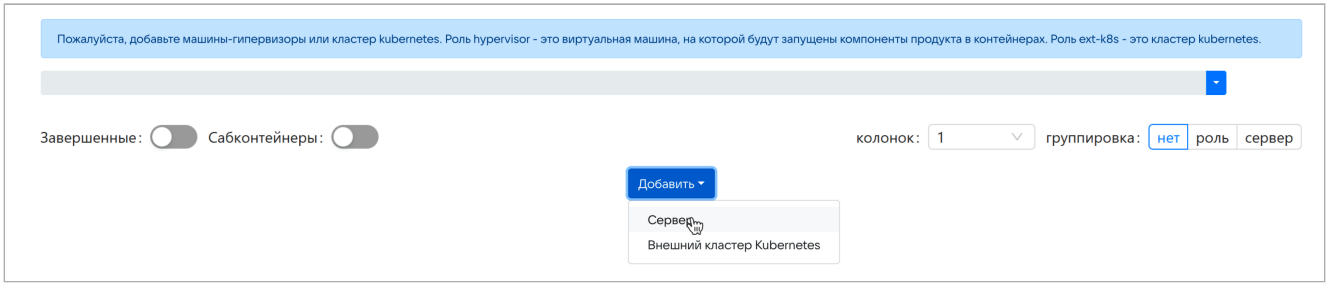
| Продукт | Описание |
| --- | --- |
| | Возможность развертывания в среде контейнеризации Kubernetes |
| Средства резервного копирования (бэкапирования) | Средства резервного копирования данных диска, почты, календарей, профилей пользователей и адресных книг |
| Система мониторинга | Набор сервисов, обеспечивающих хранение метрик сервисов в базе данных Prometheus и визуализацию данных с помощью Grafana |
| Система сбора и отправки 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 | |
| OneDB Tarantool Groups | Переключает тарантулы выбранных групп на фреймворк OneDB |
| 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 | |
| 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 с Kerberos (SSO-авторизация) | Позволяет использовать SSO для авторизации в продуктах VK WorkSpace |

| Продукт | Описание |
| --- | --- |
| **Интеграция с Kerberos.** Внешняя web-авторизация через провайдера blitz | **Beta** |
| **Интеграция с Kerberos.** Keycloak внутри инсталляции | |
| **Интеграция с Kerberos.** Интеграция с внешним Keycloak сервером | |
| Двухфакторная аутентификация | Добавление дополнительной проверки при авторизации для усиления безопасности |
| Интеграция почты с мессенджером VK WorkSpace | |

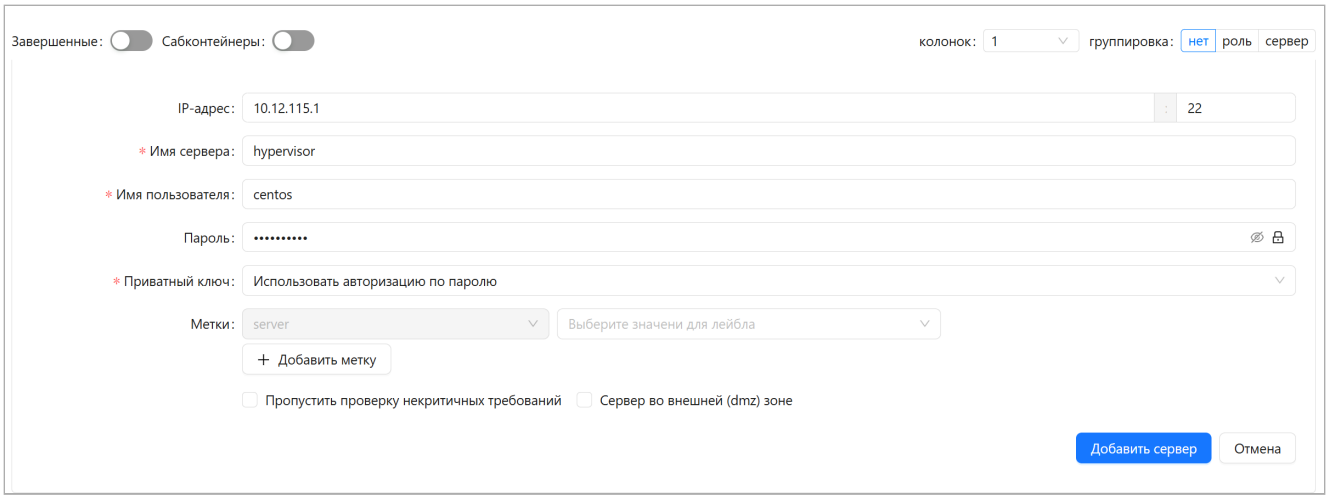
4. Нажмите на кнопку **Далее**.

# Шаг 3. Добавьте гипервизоры (серверы)

1. Нажмите на кнопку **Добавить**.
2. В выпадающем меню выберите **Сервер**.



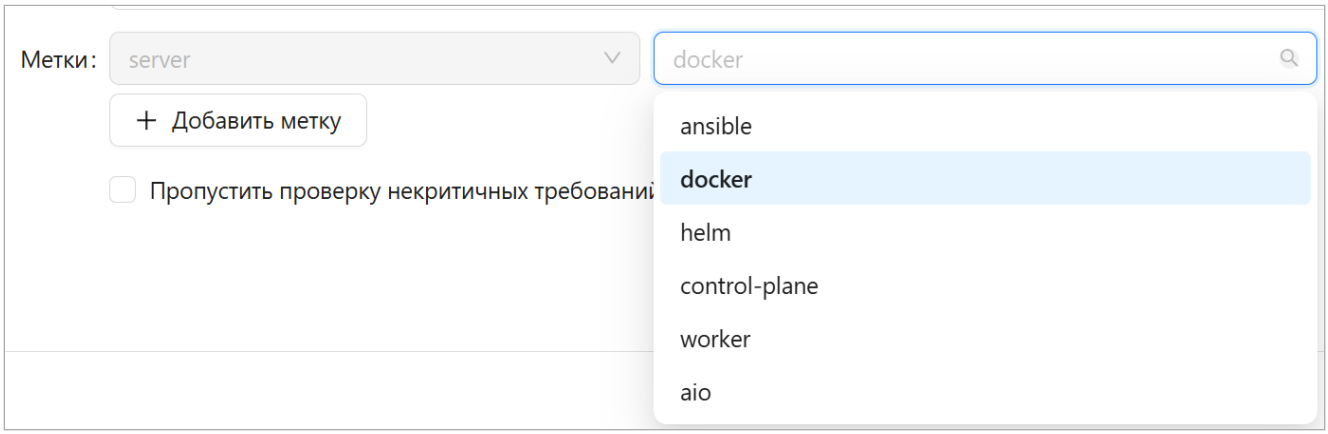

Откроется окно добавления гипервизора:




3. Заполните поля:

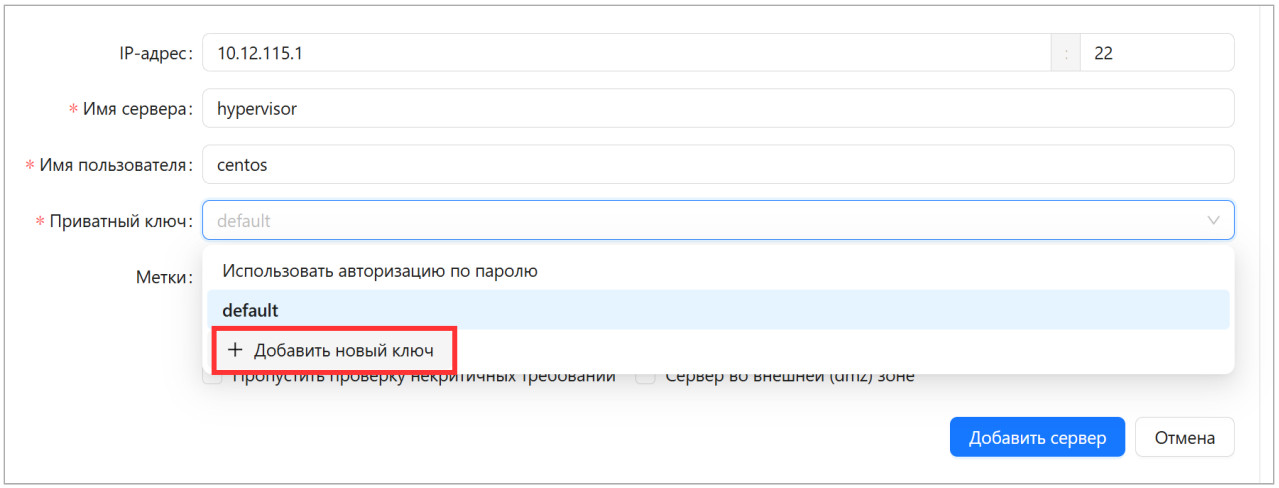
   - **IP-адрес** — адрес машины, на которую производится установка.
   - **Имя сервера** — укажите имя сервера (гипервизора) или оставьте поле пустым. В случае если вы оставите поле незаполненным, имя гипервизора будет взято из `hostname -s` и добавится автоматически. В документации будет использовано имя **hypervisor1**.
   - **Имя пользователя** — укажите имя того пользователя, под которым запущен установщик. В рассматриваемом примере это пользователь deployer.
   - **Пароль** — необходимо ввести пароль пользователя, под которым запущен установщик, если он был задан при создании. Появялется, если в поле **Приватный ключ** выбрана опция **Использовать авторизацию по паролю**.

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




5. При необходимости добавьте **SSH-ключ**, чтобы указать установщику, какой именно ключ использовать для входа на эту машину кластера:

   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 **Сохранить**.

6. При необходимости настройте дополнительные поля:

   - **Пропустить проверку некритичных требований** — если отметить чекбокс, будет пропущена проверка версии ядра и флагов процессора (sse2, avx). В большинстве случаев выбор чекбокса не требуется.
   - **Сервер во внешней (dmz) зоне** — Оставьте чекбокс пустым.

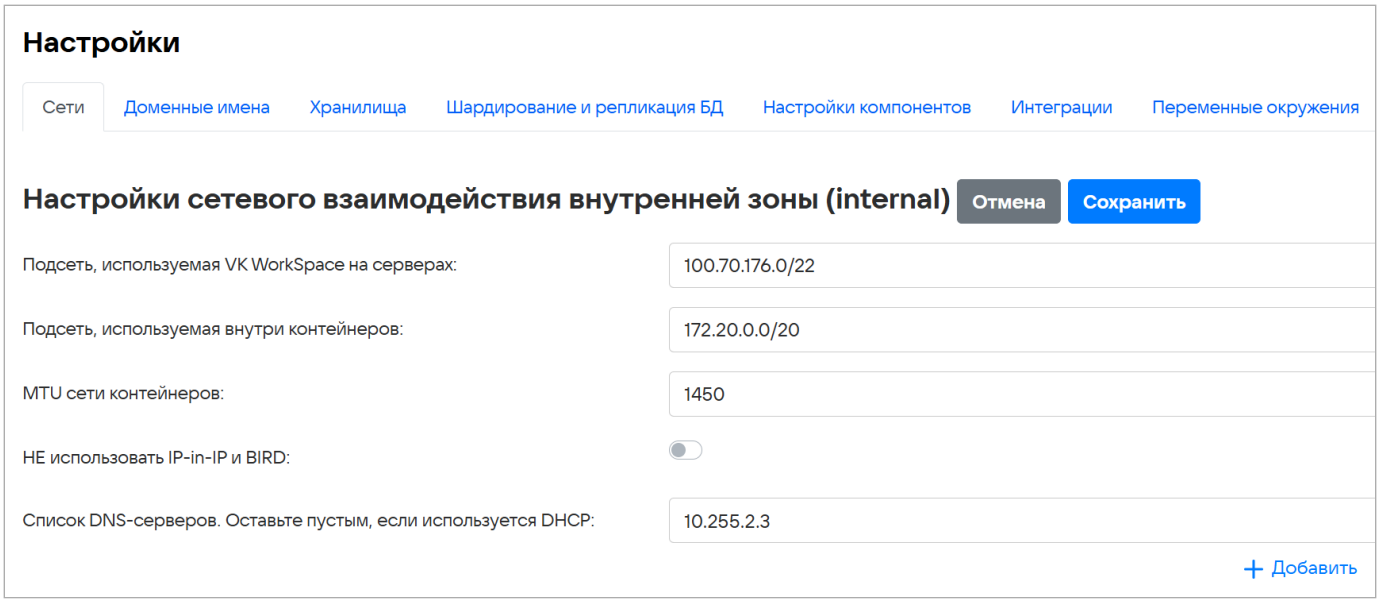
7. После заполнения полей нажмите на кнопку **Добавить сервер** — гипервизор отобразится в веб-интерфейсе установщика.

> **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. Нажмите на зеленую кнопку **Далее** в правом верхнем углу для перехода к следующему шагу.

# Шаг 4. 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 ВМ в соответствии с рекомендациями к используемой ОС: RedOS, Astra Linux или MosOS Arbat.

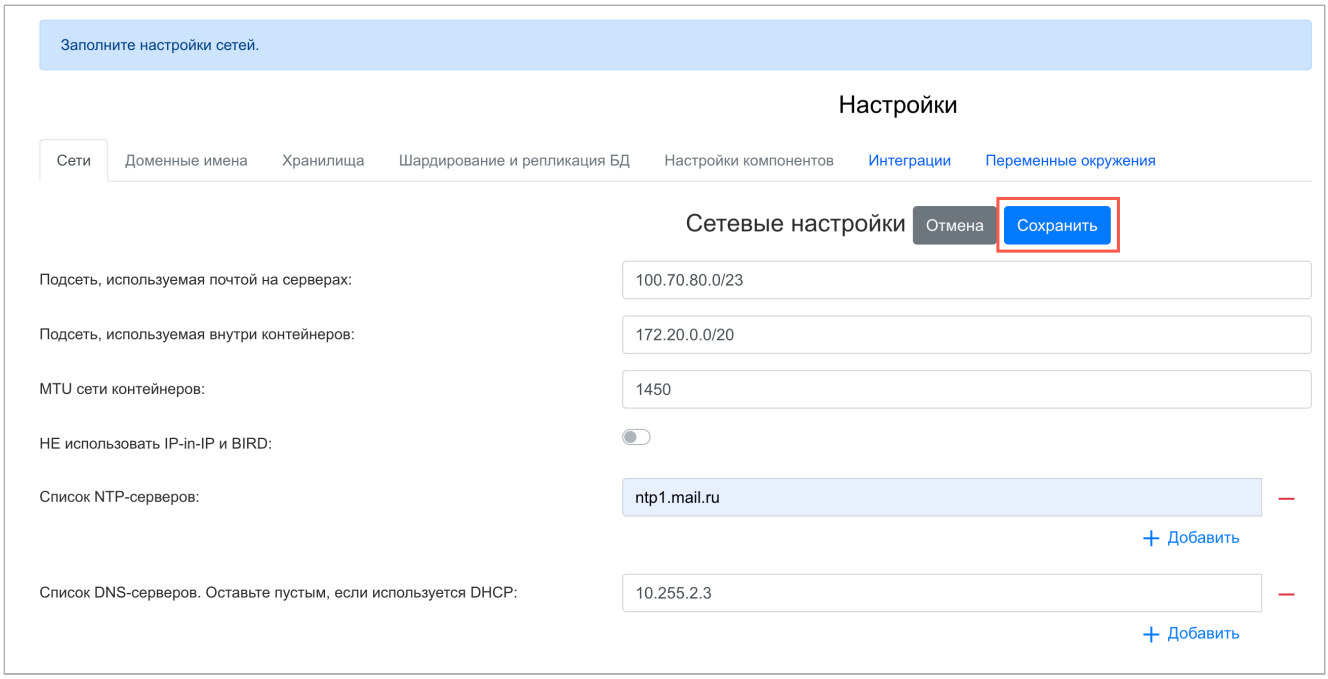
2. Убедитесь, что:
   - **Подсеть, используемая VK WorkSpace на серверах** имеет доступ на **80-й** или **443-й** порт.
   - **Подсеть, используемая внутри контейнеров** полностью свободна, уникальна и принадлежит только Доске.

> **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 установке на 1 ВМ в среднем создается более 650 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 5. Доменные имена

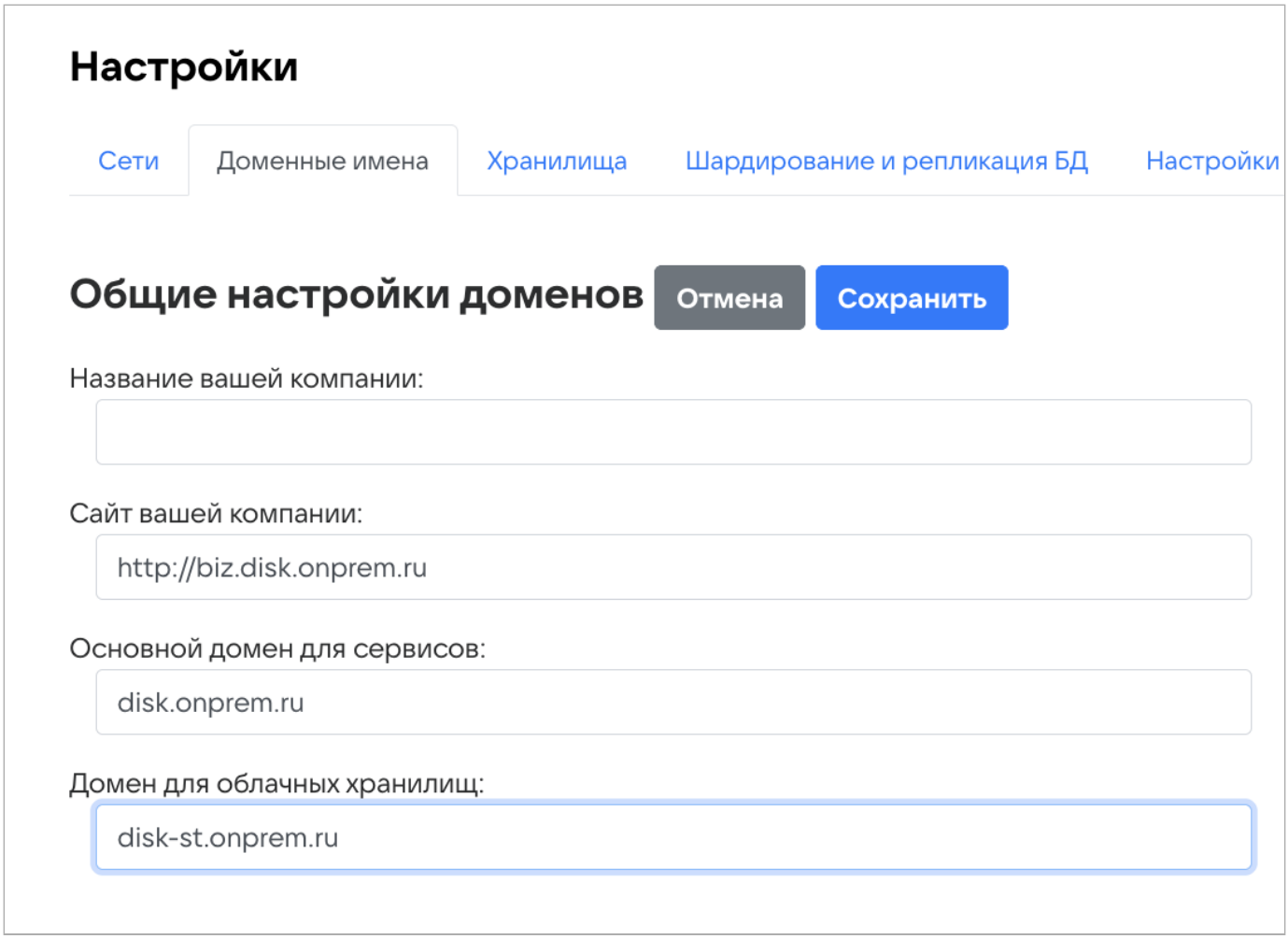
Подробную информацию о создании доменных имен вы найдете в разделе Создание DNS-записей.

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

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

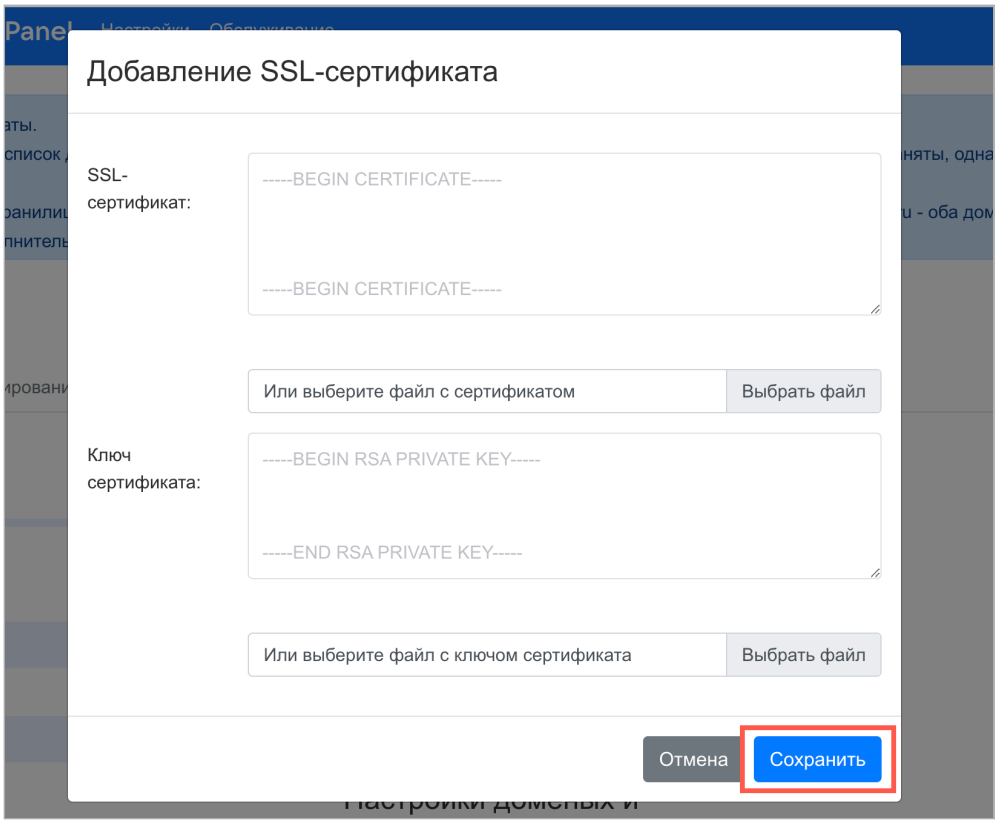
## Добавление SSL-сертификатов

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:

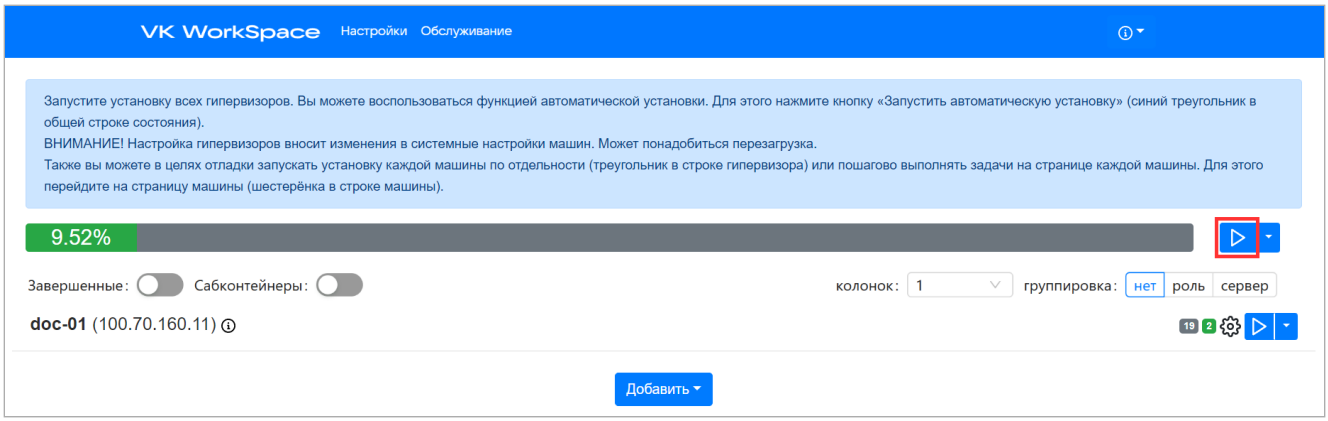
1. Нажмите на кнопку **Выбрать файл**.
2. Укажите путь к файлу с сертификатом **.crt**.
3. Укажите путь к файлу с ключом **.key**.
4. Кликните по кнопке **Сохранить**.

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

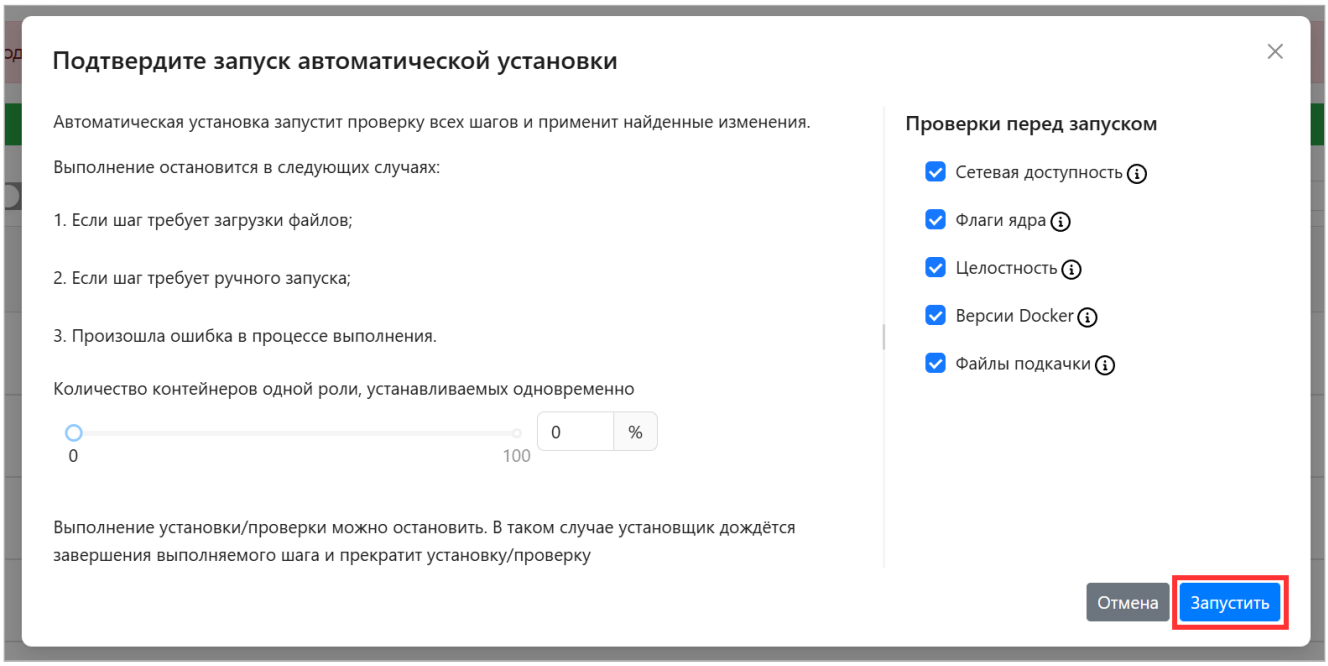
Если всё верно, в интерфейсе не будет отображаться ошибок и красной подсветки. Нажмите на зеленую кнопку **Далее**.

# Шаг 6. Запуск установки гипервизора

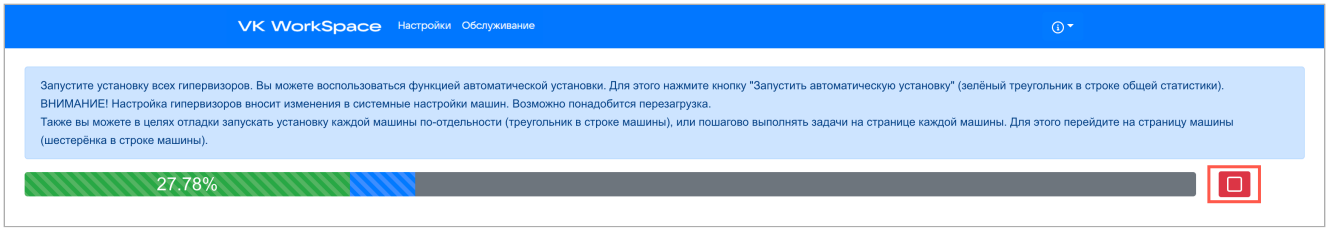
1. Нажмите на логотип в левом верхнем углу веб-интерфейса, чтобы перейти к общей строке состояния.
2. Кликните по кнопке **Play** (треугольник) рядом с общей строкой состояния в верхней части экрана.




3. Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**. Перед запуском автоматической установки оставьте включенными все проверки. Подробнее о работе проверок можно прочитать здесь: Диагностика системы в веб-интерфейсе установщика




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

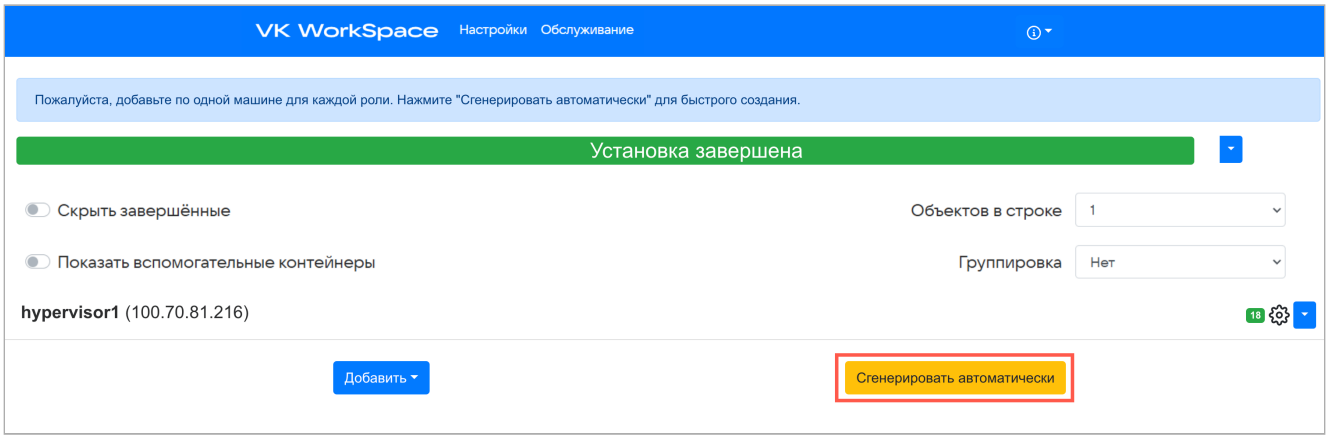



В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуется повторный запуск автоматической установки.

Для повторного запуска нажмите на кнопку **Play** в верхней общей строке состояния или рядом с названием гипервизора.

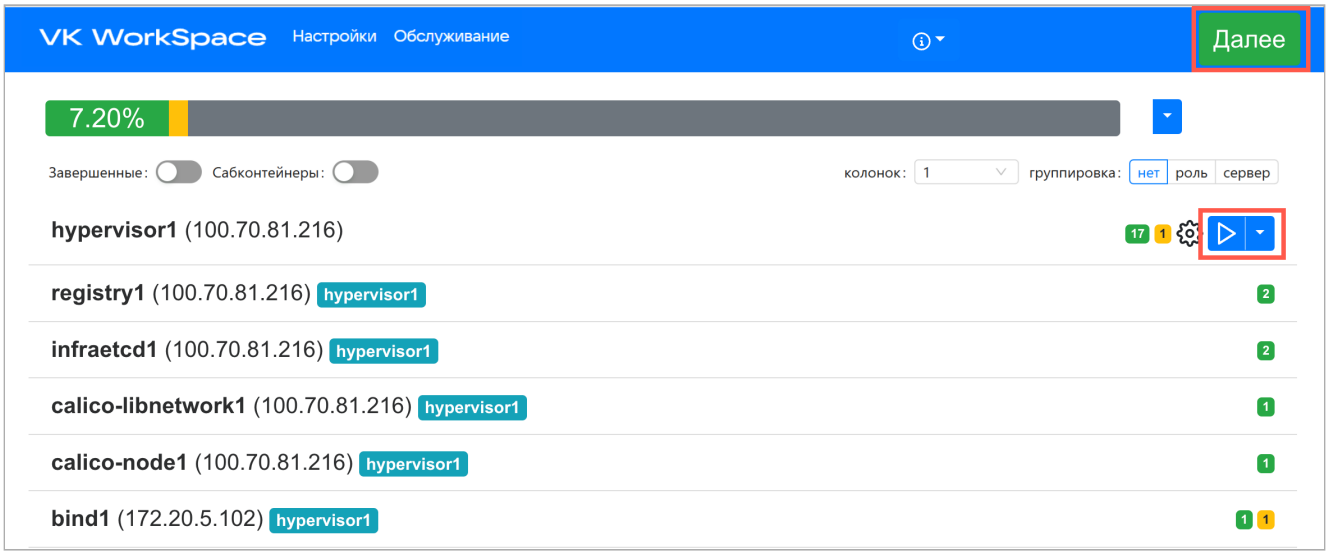
# Шаг 7. Генерация контейнеров

1. Нажмите на кнопку **Сгенерировать автоматически**, чтобы добавить по одному контейнеру для каждой роли.

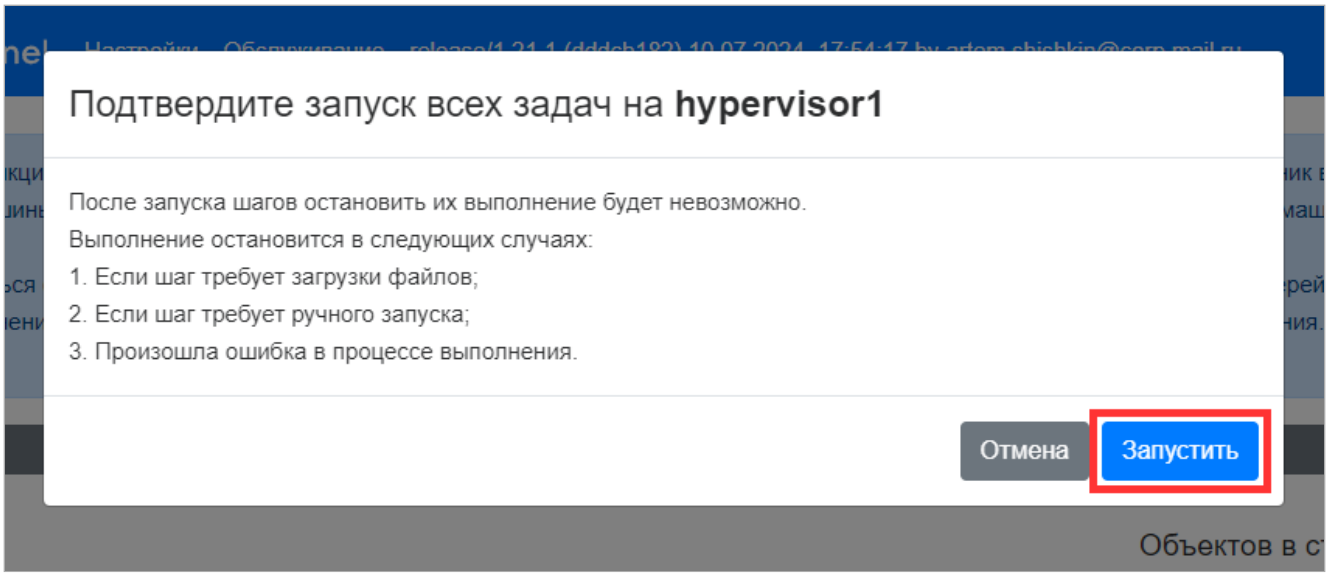



   На экране начнут появляться сгенерированные контейнеры. В случае появления ошибок используйте раздел Логи и полезные команды.

   Через некоторое время в правом верхнем углу появится кнопка **Далее**, напротив гипервизора появится кнопка **Play**.



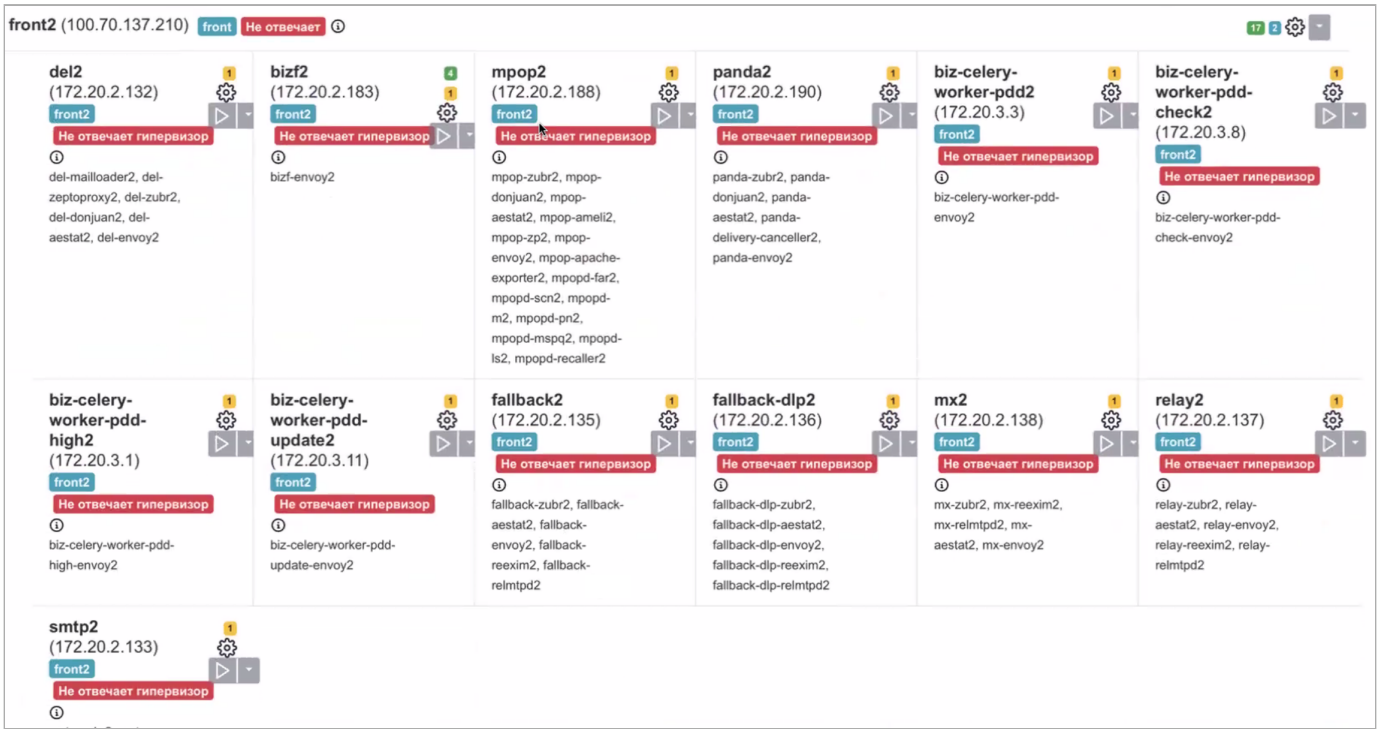

2. Кликните по кнопке **Play** напротив гипервизора.
3. Подтвердите автоматический запуск задач на гипервизоре, нажав на кнопку **Запустить**.



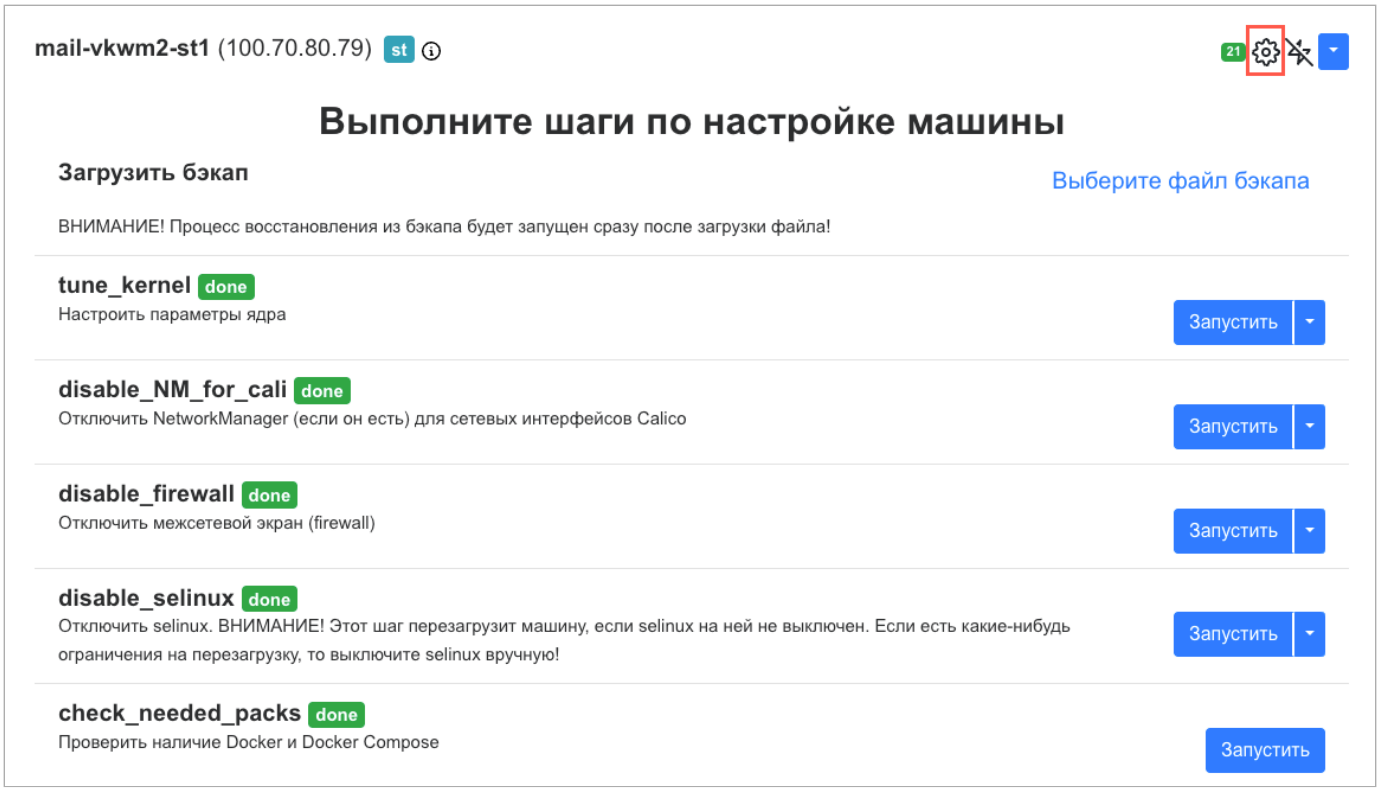

4. На генерацию требуется время. Подождите, пока исчезнет кнопка **Play** напротив гипервизора.
5. Нажмите на кнопку **Далее** для перехода к следующему шагу.

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.

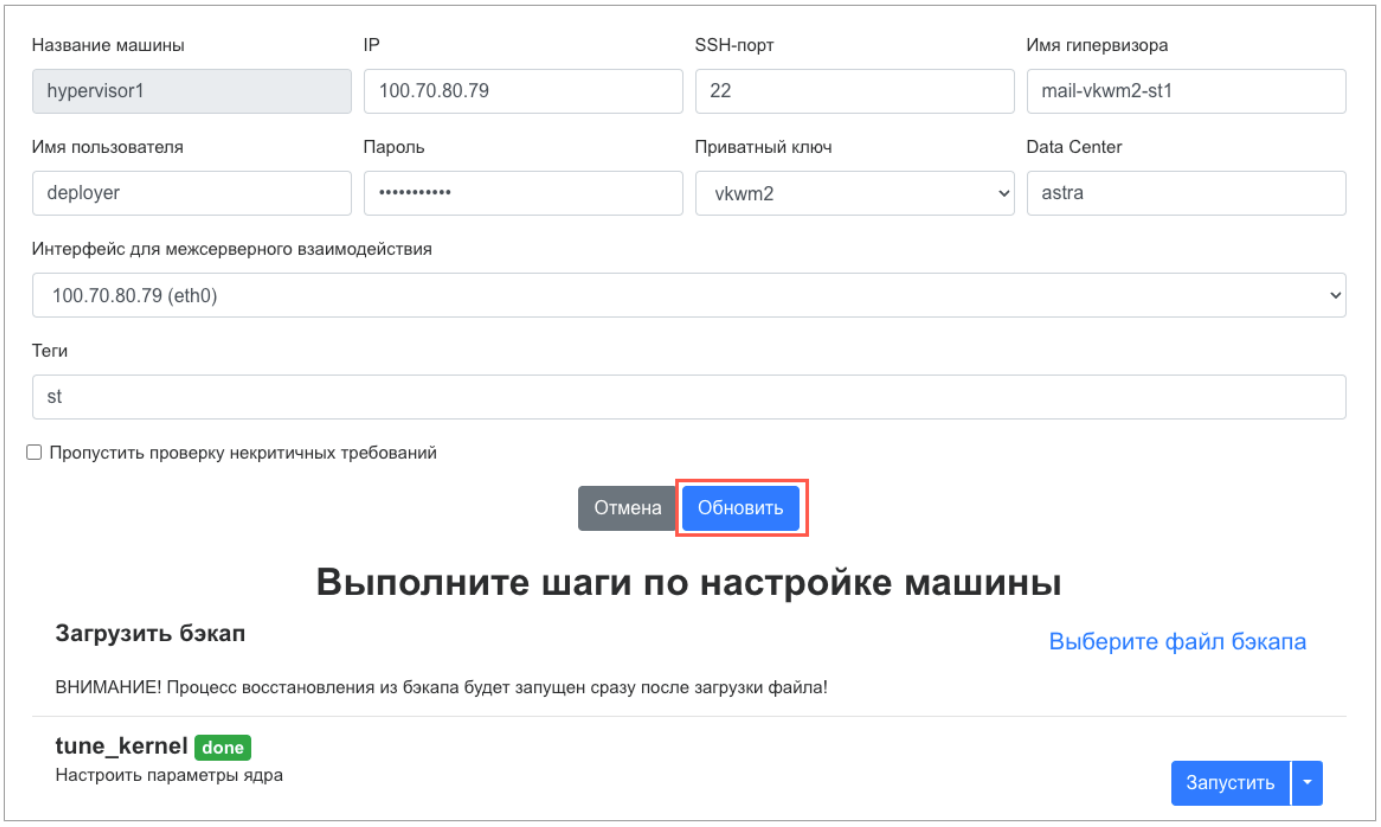
При появлении ошибок на гипервизоре на нем появится тег **Не отвечает**, а на контейнерах, относящихся к этому гипервизору — **Не отвечает гипервизор**.




Затем перейдите в командную строку и устраните ошибку. По завершении необходимо нажать на шестеренку в строке гипервизора и еще раз на странице списка шагов на гипервизоре.



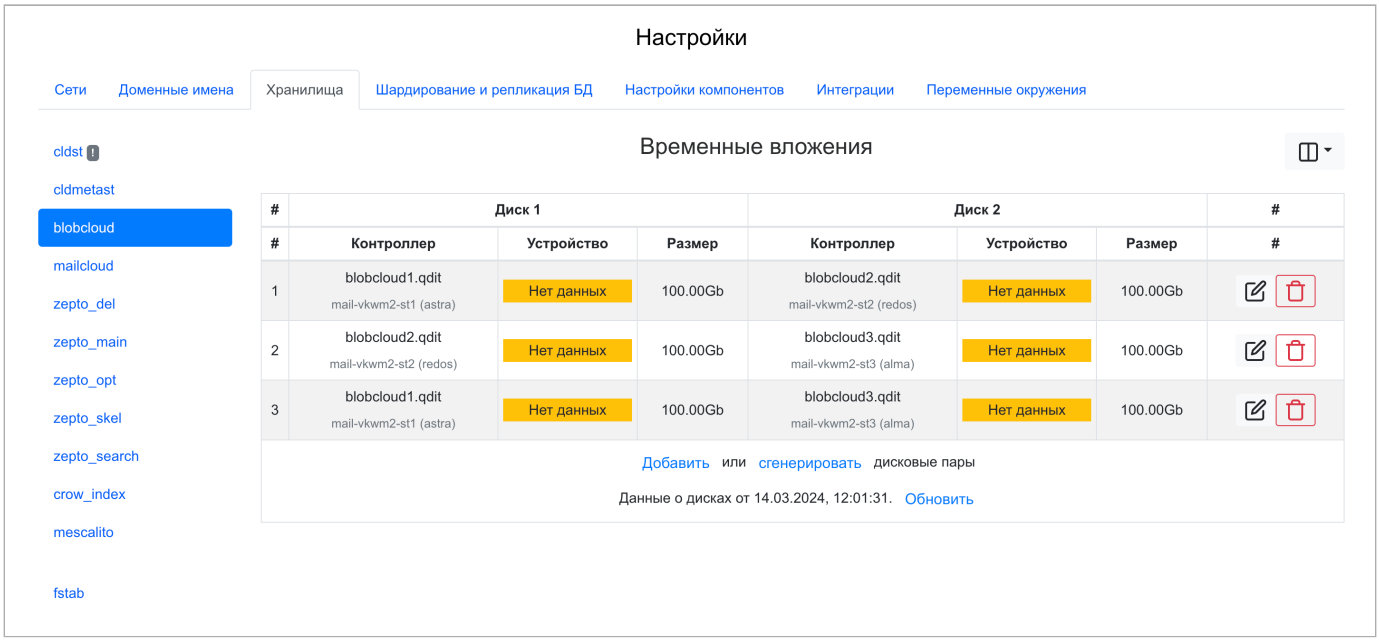

В окне настроек гипервизора нажмите на кнопку **Обновить**.




Повторно запустите автоматическую установку.

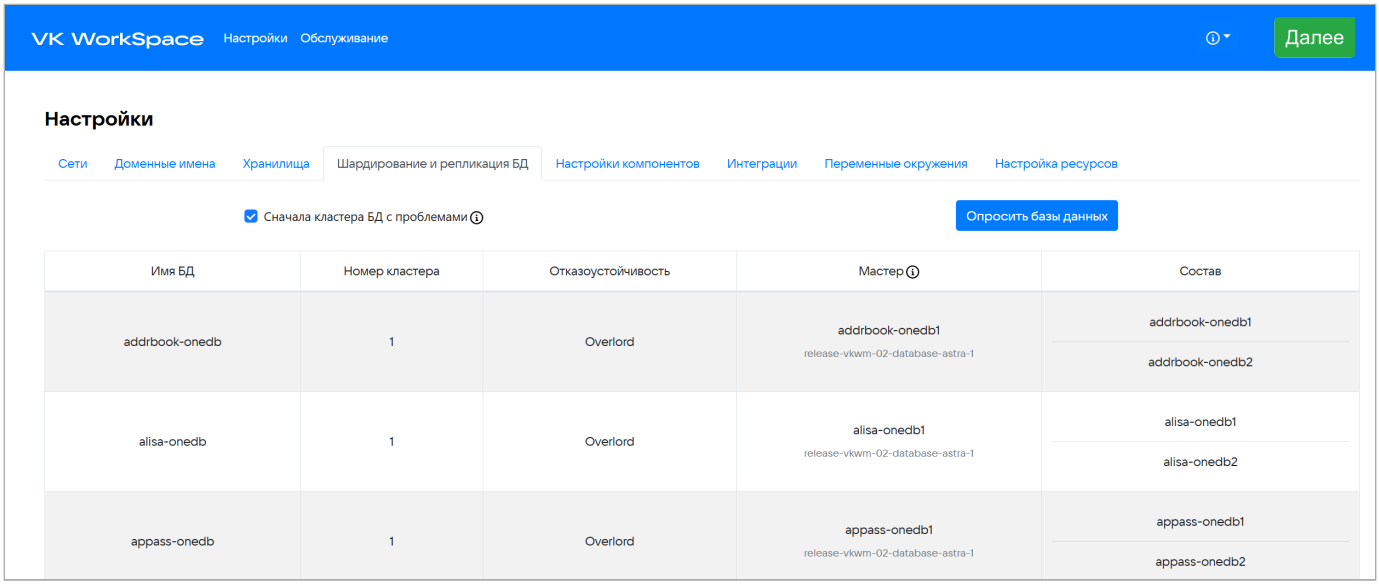
# Шаг 8. Хранилища

Для установки на одну машину достаточно автоматического распределения по дисковым парам, поэтому дополнительная настройка не требуется, нажмите на кнопку **Далее**.




# Шаг 9. Шардирование и репликация БД

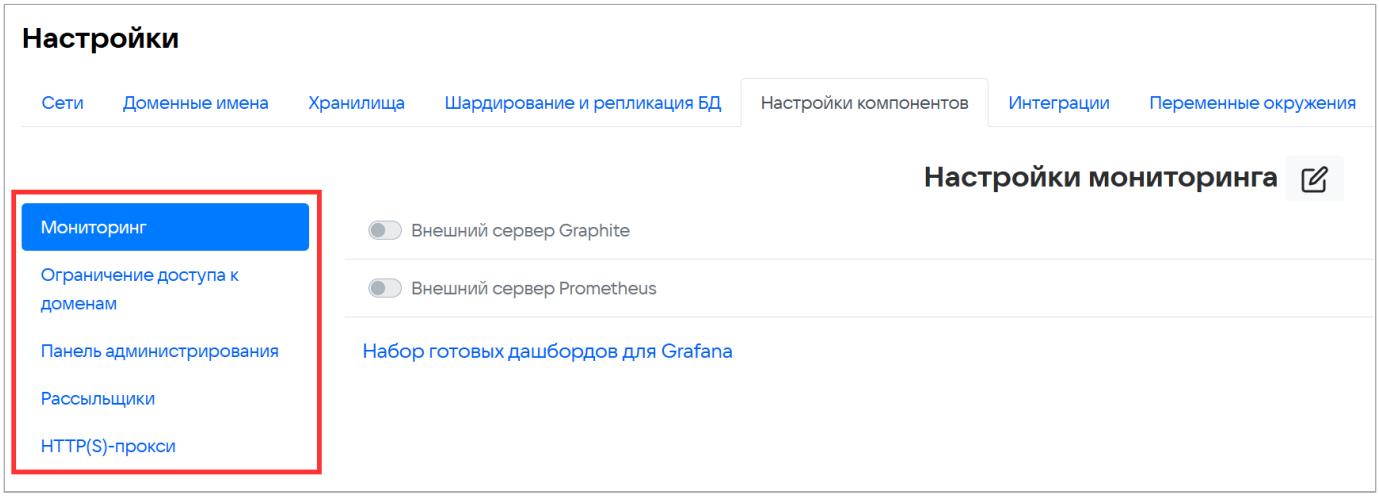
На вкладке **Шардирование и репликация БД** нажмите на кнопку **Далее**.




Шардирование (сегментирование) БД используется в кластерной установке для обеспечения отказоустойчивости и масштабируемости, в моноинсталляции не используется.

# Шаг 10. Настройка компонентов

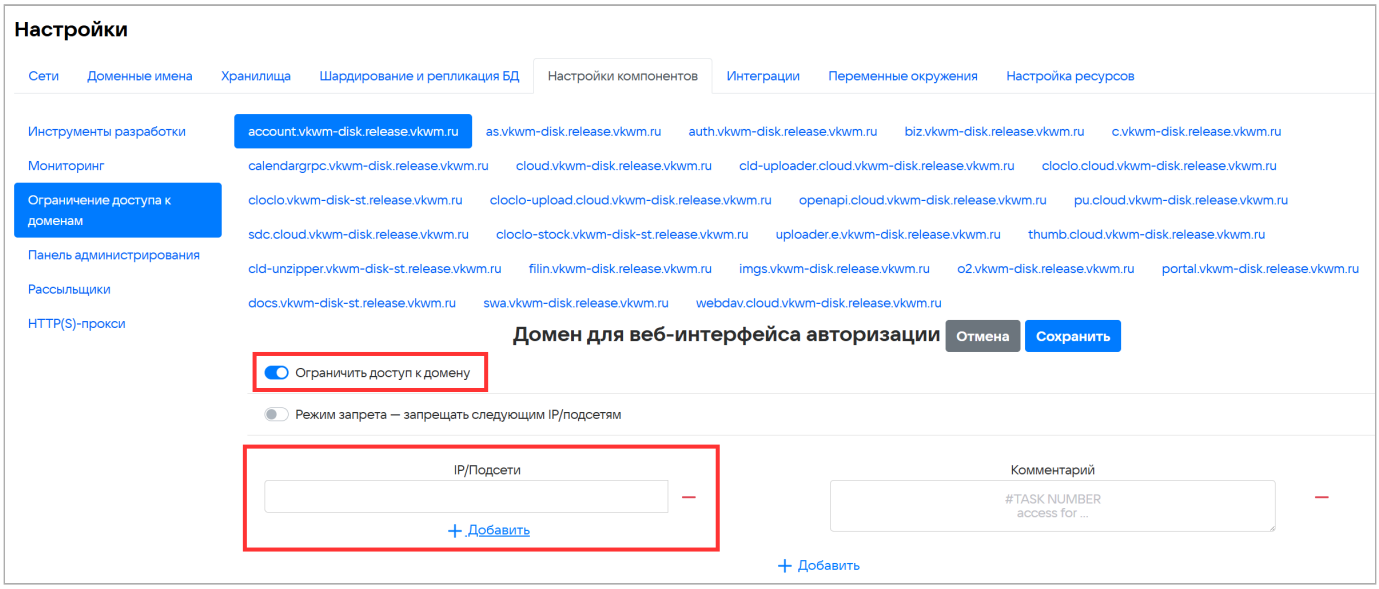
В разделе выполняются настройки различных компонентов системы.




## 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.

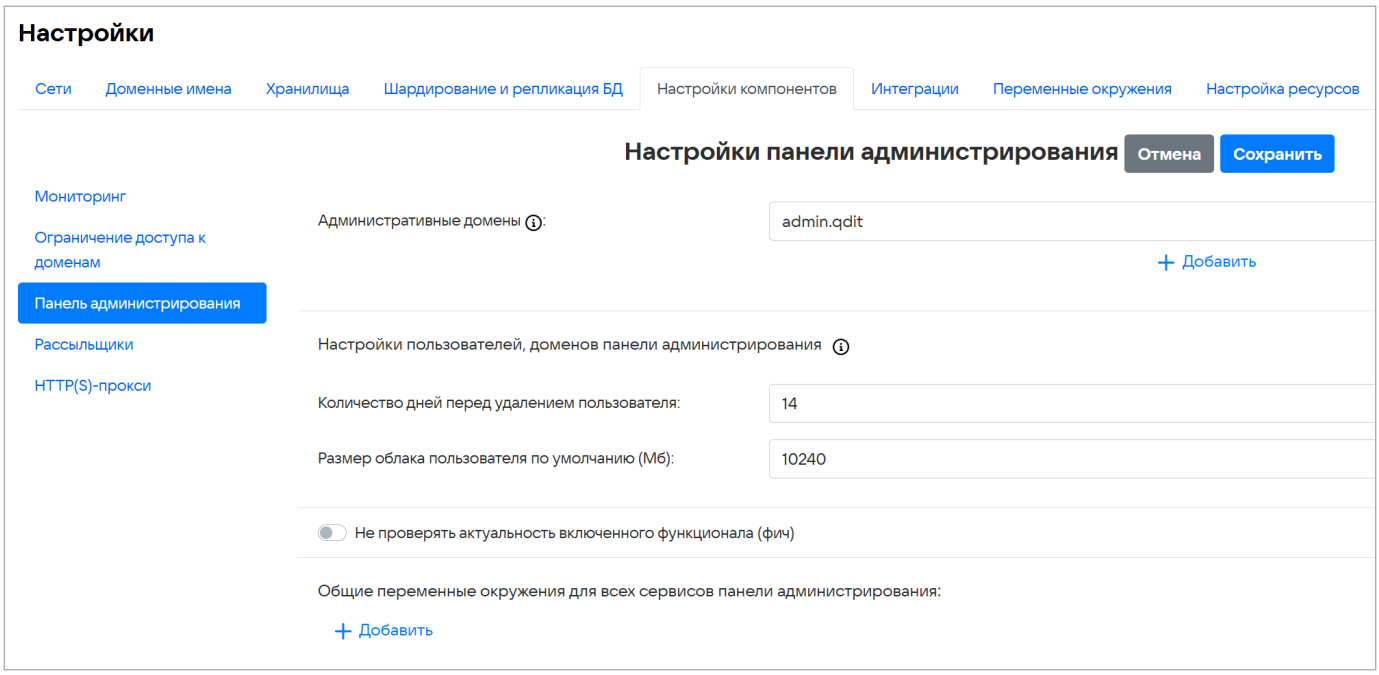
Не забудьте повторить шаги на гипервизоре (нужные шаги уже отмечены желтым). Также можно нажать на кнопку **Play** в общей строке состояния. Для этого перейдите к списку шагов, кликнув по логотипу в левом верхнем углу веб-интерфейса.

**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

Чтобы начать настройку, нажмите кнопку редактирования .




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

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

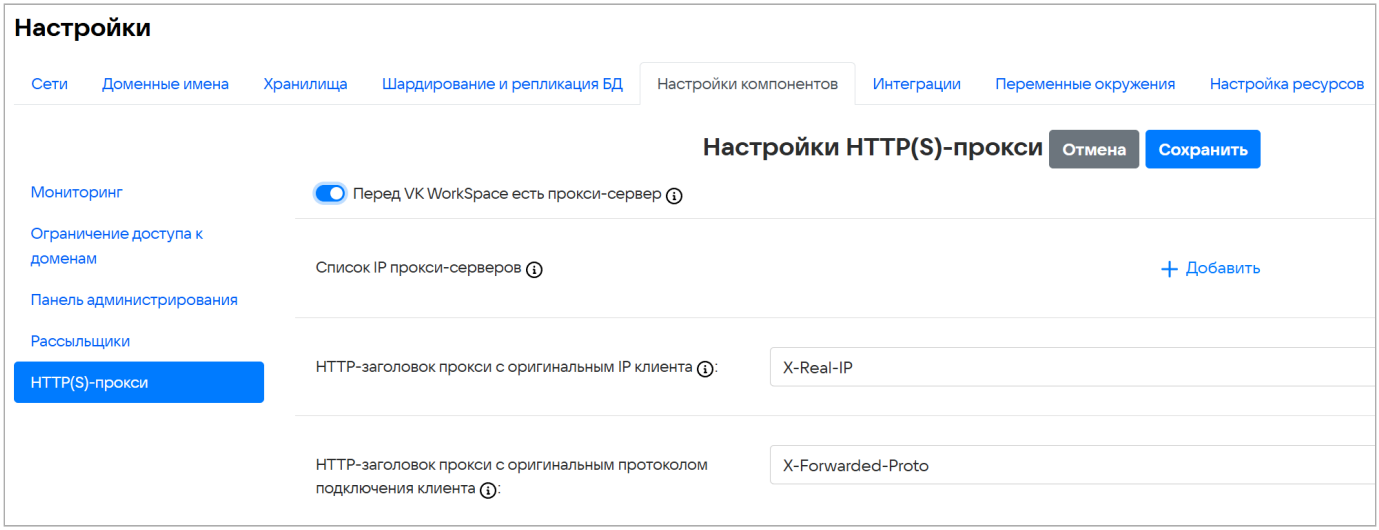
**Размер облака пользователя по умолчанию (Мб)** — при необходимости ограничьте максимальный размер облака для каждого пользователя.

**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.

## 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 Доска 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 сервисов введите заголовок оригинального протокола подключения.

# Шаг 11. Интеграции

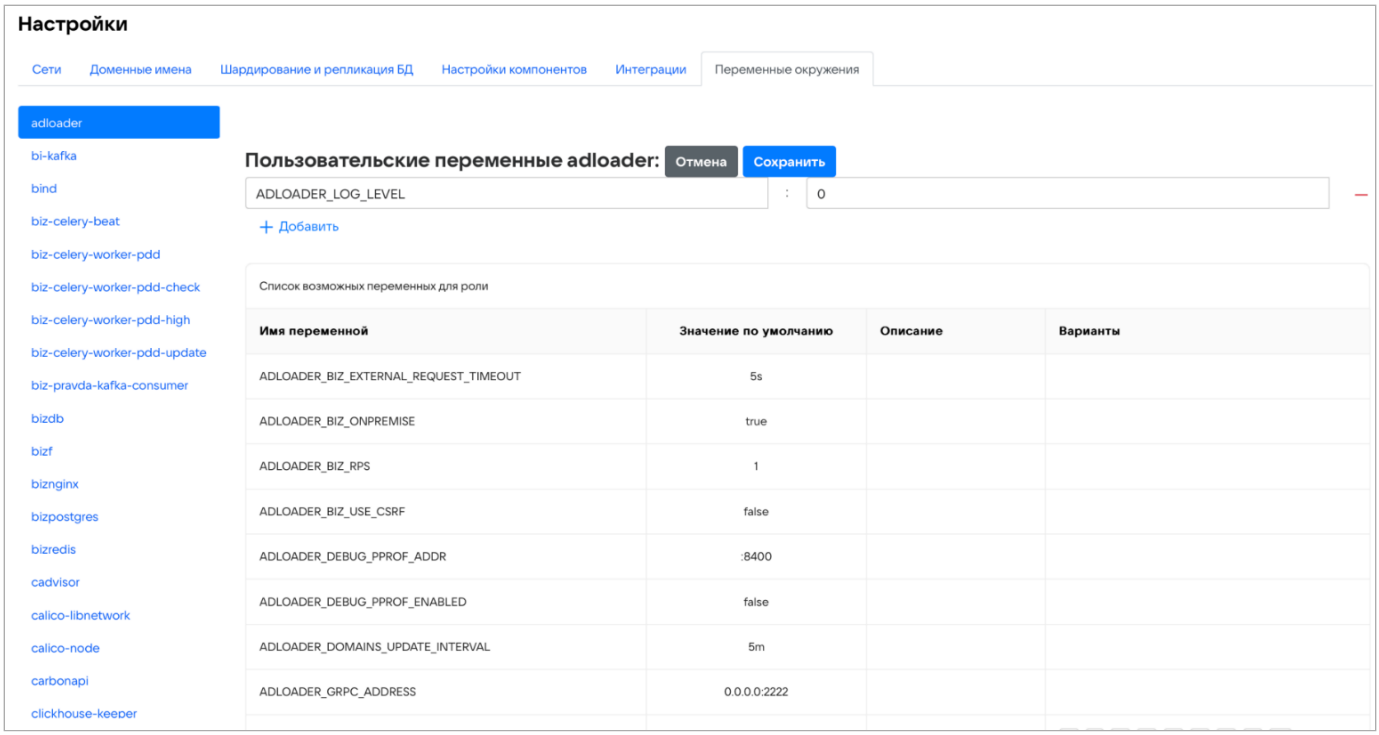
В блоке будут отображаться интеграции, которые вы включили на этапе выбора продуктов и опций (настройки интеграций могут также находиться в верхнем меню).

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

Настроить дублирование действий пользователей во внешние хранилища

# Шаг 12. Укажите переменные окружения

В разделе производится настройка кастомных переменных Панели администратора.




**Внимание**

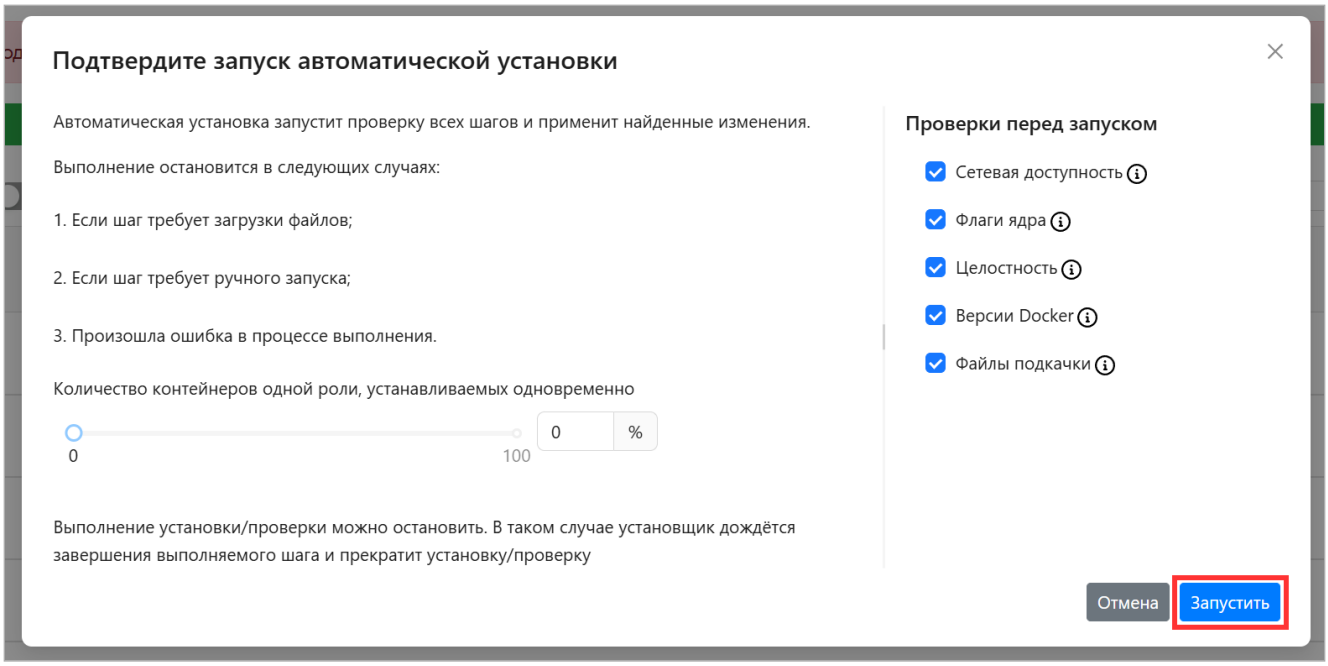
Настройка переменных окружения возможна только после консультации с представителем VK.

Чтобы добавить кастомную переменную:

1. Нажмите на иконку  и кнопку **Добавить**.
2. В выпадающем меню выберите название переменной.
3. Введите значение переменной. Значение переменной должно быть введено корректно, иначе установщик не позволит создать переменную.
4. Нажмите на кнопку **Сохранить**.
5. Нажмите на кнопку **Далее** для перехода к следующему шагу.

# Шаг 13. Запустите установку всех машин

1. В веб-интерфейсе установщика Панели администратора кликните по иконке  рядом с общей строкой состояния в верхней части экрана.
2. Подтвердите запуск автоматической установки, нажав на кнопку **Запустить**.




В зависимости от этапа установки будет меняться цвет индикатора:

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

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

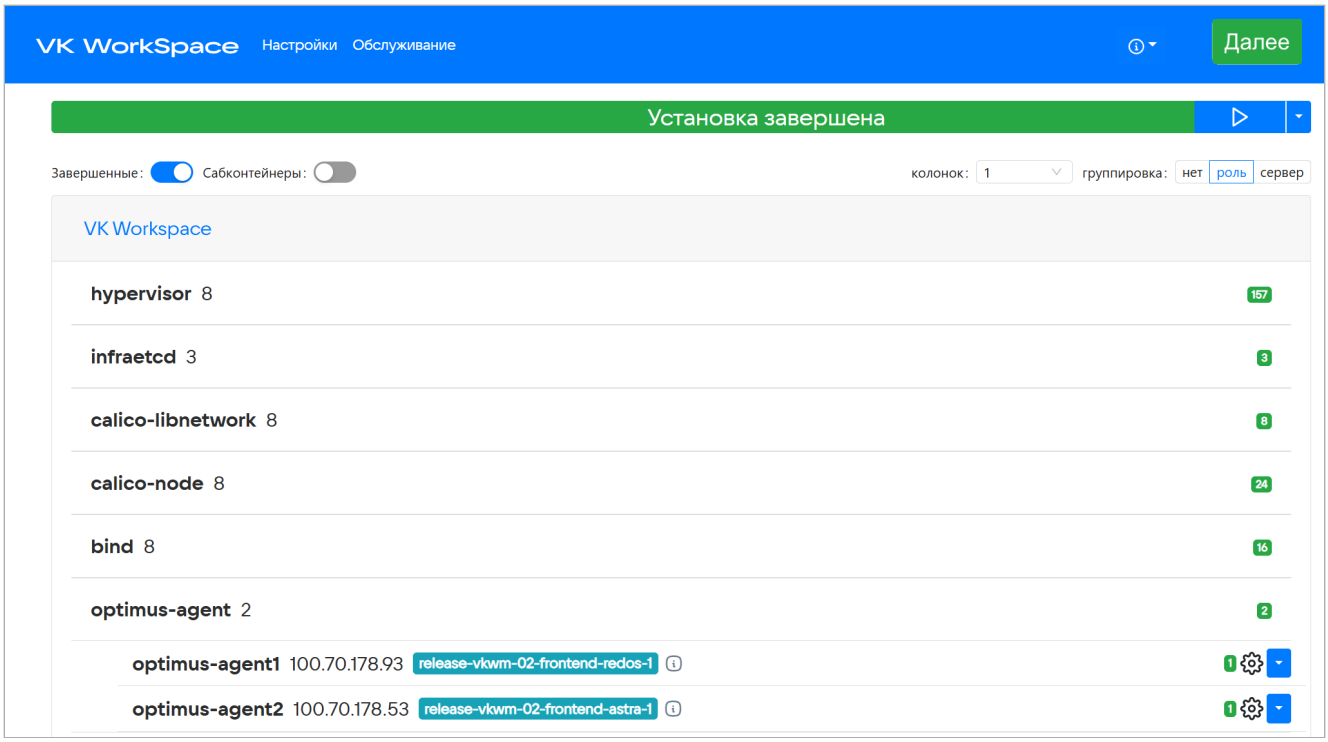
Если в процессе установки и настройки системы происходят изменения конфигурации, некоторые задачи могут потребовать повторного выполнения.

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

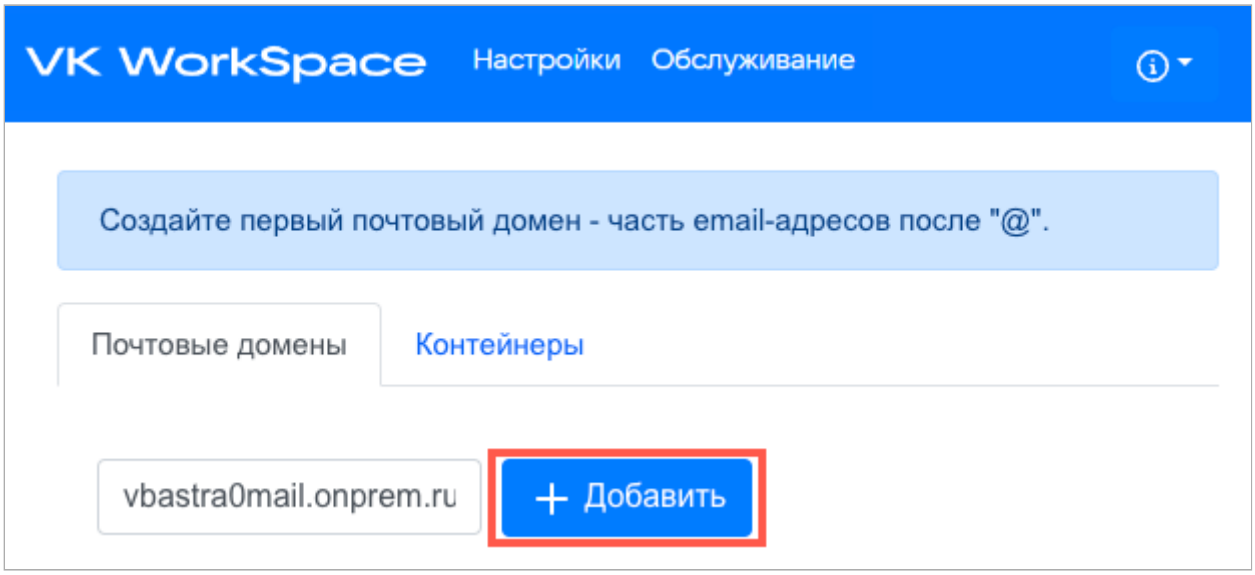
# Шаг 14. Инициализируйте домен и войдите в Панель администратора

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

1. Нажмите на кнопку **Далее** в правом верхнем углу.




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




Домен считается подтвержденным после добавления в Панель администратора.

В адресную строку скопируйте адрес Панели администратора и введите данные:

- 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`.

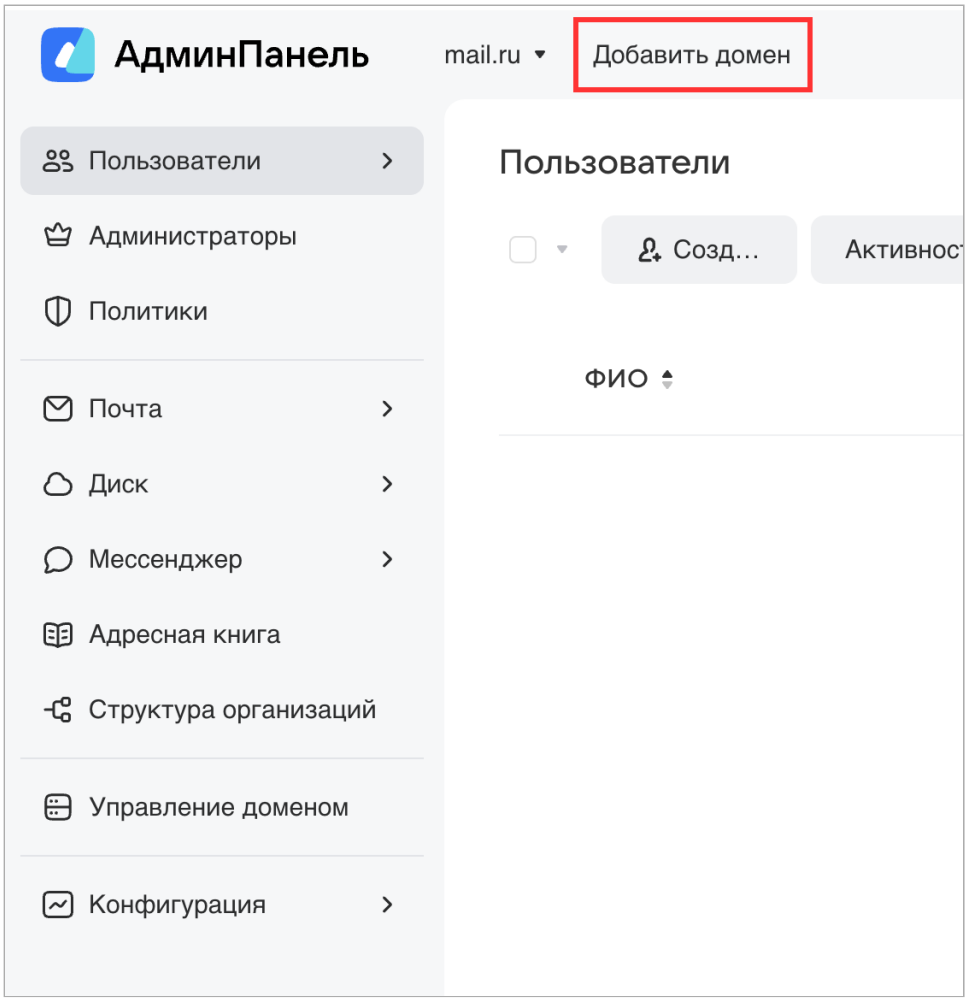
Если логин и пароль были введены правильно, вы попадете в Панель администратора.

**Внимание**

Когда установка закнчится можно удалить архив, 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 Панели администратора.

# Добавление дополнительных доменов

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




# Логи и полезные команды

Все команды, перечисленные ниже, следует выполнять в консоли.

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 незапустившихся контейнеров:

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

8. Удалить контейнер:

```
sudo docker rm имя_контейнера
```

Автор: Груздев Никита

27 апреля 2026 г.