Мессенджер и ВКС

Настройка интеграции с кластерной инсталляцией Панели администратора VK WorkSpace

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

Оглавление

Назначение документа

В документе описана настройка интеграции Мессенджер и ВКС версии 25.2 и выше и кластерной инсталляцией Панели администратора VK WorkSpace версии 1.24 и выше. Документ предназначен для использования администраторами организации.

> ⚠ **Внимание**
>
> Чтобы настроить интеграцию с Мессенджер и ВКС версии 24.9 и ниже, обратитесь к сотрудникам или партнерам компании VK.

Условно процесс настройки интеграции Мессенджер и ВКС с кластерной инсталляцией Панели администратора можно разделить на несколько шагов:

1. Выполните настройки на стороне Мессенджер и ВКС.
2. Разверните кластерную инсталляцию Панели администратора VK WorkSpace и интегрируйте ее с Мессенджер и ВКС.
3. Настройте интеграцию Панели администратора с ActiveDirectory.
4. Выключите синхронизацию пользователей через сервис Keycloak.

Подробное описание шагов представлено ниже.

После настройки интеграции пользователи Мессенджер и ВКС синхронизируются с ActiveDirectory через Панель администратора. Поэтому, если у вас настроена интеграция Мессенджер и ВКС с ActiveDirectory, настройте интеграцию Панели администратора с ActiveDirectory и после этого удалите LDAP-подключение Мессенджер и ВКС.

> ⚠ **Внимание**
>
> Для production-систем рекомендуется производить настройки во время технологического окна.
> Все команды в консоли выполняются под пользователем root.

Дополнительная документация

Инструкция по установке Мессенджер и ВКС на одну виртуальную машину, Инструкция по установке кластера Мессенджер и ВКС

Инструкция по интеграции Мессенджер и ВКС с контроллером домена по протоколу LDAP — в инструкции описано управление параметрами синхронизации LDAP.

Настройка интеграции с Active Directory — в инструкции описана настройка интеграции Панели администратора VK WorkSpace с Active Directory.

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

Управление структурой организаций — в инструкции описана работа со структурой организаций в Панели администратора VK WorkSpace.

Развертывание и настройка сервисов групповых политик — в инструкции описаны шаги для развертывания и включения сервисов групповых политик.

Групповые политики — в инструкции описана работа с групповыми политиками в Панели администратора VK WorkSpace.

Предварительные условия

1. Если у вас еще не установлен Мессенджер и ВКС, установите его, пропустив настойку синхронизации пользователей с LDAP-сервером.
2. Выпустите SSL-сертификат — в сертификате укажите домен, на котором будет расположена Панель администратора. Можно использовать SSL-сертификат на один домен. Требования к сертификату:
   - CN — домен, на котором будет расположена Панель администратора.
   - Расширение san не нужно.
   - Тип DV (Domain Validation) — проверять только владение доменом.
   - `extendedKeyUsage = serverAuth`.
   - Public Key — нужен.
3. Подготовьте почтовый домен вашей корпоративной электронной почты. Если у вас нет корпоративной почты, создайте ее.
4. Создайте домен Панели администратора.

   Домен Панели администратора должен содержать поддомен biz, пример домена — biz.<ваш_домен>.ru.

   Создайте A- или CNAME-запись для данного домена в DNS. Возможна как A-запись, так и CNAME-запись, в зависимости от того, где будет развернута Панель администратора. Необходима запись, которая будет указывать на сервер VK WorkSpace, остальное зависит от ваших текущих настроек и Nginx (если он есть). Например, вы можете указать biz.example.ru. как CNAME-запись к example.ru, если для вашего Nginx настроена маршрутизация запросов. Если нет, то стоит создать A-запись для Панели администратора.
5. Доступ к виртуальной машине, на которой установлен Мессенджер и ВКС.
6. Получите у представителя VK данные для разворачивания Панели администратора VK WorkSpace:
   - Ссылка на скачивание дистрибутива Панели администратора VK WorkSpace.
   - Пароль от архива с дистрибутивом.
   - Лицензионный ключ.

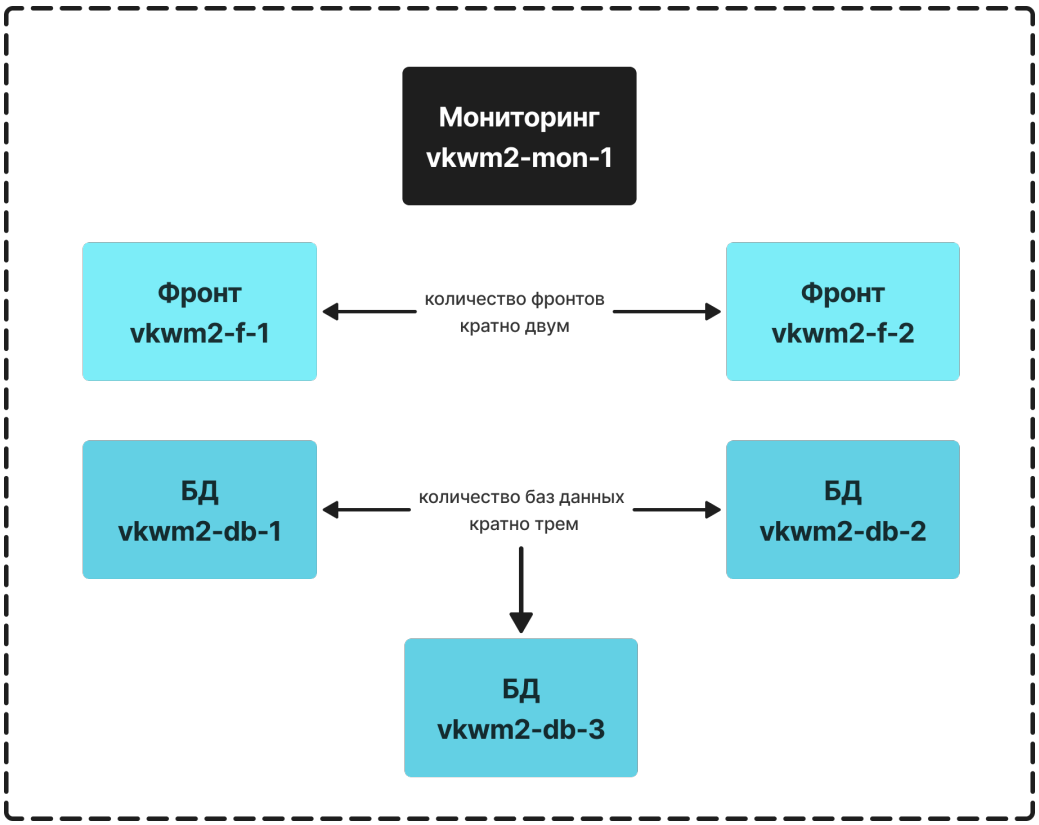
7. Доступ к почтовому серверу по 25 порту, так как Панель администратора VK WorkSpace использует протоколы SMTP, ESMTP.

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.

Схема тестового кластера

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



Минимальная отказоустойчивая конфигурация на 6 машин, которая будет описана в документе, выглядит таким образом:

- 1 ВМ отводится под мониторинг;
- 2 ВМ — под фронты;
- 3 ВМ — под базы данных;

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

Технические требования

Поддерживаемые операционные системы для установки Панели администратора:

- **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.

Пример настройки параметров ОС

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

Настройки 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
```

Настройка 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

До установки Панели администратора:

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

   ```
   DefaultLimitNOFILE=524288:524288
   ```

2. 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

Требования к ресурсам серверов

Минимальные технические параметры для 6 машин, если на инсталляции планируется включить функциональность групповых политик:

- Установщик + мониторинг: 8 vCPU, 16 GB RAM, 150 GB SSD;
- Фронт №1: 8 vCPU, 16 GB RAM, 100 GB SSD;
- Фронт № 2: 8 vCPU, 16 GB RAM, 100 GB SSD;
- База данных №1: 8 vCPU, 16 GB RAM, 50 GB SSD;
- База данных №2: 8 vCPU, 16 GB RAM, 50 GB SSD;
- База данных №3: 8 vCPU, 16 GB RAM, 50 GB SSD;

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

Таблица совместимости

Технология	Версия
Мессенджер и ВКС	не старше двух последних версий
Keycloak/OAuth	не старше версии 2.x
Kerberos	5
MySQL	8.0.22

Примечание

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

Список портов для установки

Внимание

Чтобы обеспечить безопасность Почты на ваших серверах должны быть доступны только необходимые порты.

Для доступа к веб-интерфейсу: 80 (http), 443 (https). Для получения почты: 25 (SMTP). Вы должны сами определить с каких IP-адресов будут доступны порты.

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
TCP	9091	calico-node	Демон динамической маршрутизации	Сбор метрик prometheus	victoria-metrics
TCP	5000	registry	Хранилище docker-образов	Подключение к сервису	Все машины инсталляции
TCP	2379	infraetcd	etcd, которое хранит инфраструктурные		

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
			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 данные, например настройки сети	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP	8080	cadvisor	Инструмент снятия телеметрии с контейнеров	Сбор метрик prometheus	victoria-metrics
TCP	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	8428	victoria-metrics	Инструмент prometheus-подобного хранилища метрик	Подключение к хранилищу	vimana, Grafana
TCP	22	sshd	Демон операционной системы, предоставляющий консоль пользователю	ssh подключения	Onpremise-deployer

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
TCP	8888	onpremise-deployer	Приложения для установки и начальной настройки VK WorkSpace	Подключение администраторов	Администраторы
UDP	2003	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры

1. Выполните настройки на стороне Мессенджер и ВКС

Шаг 1. Создайте токен biz-admin

1. На сервере Мессенджер и ВКС перейдите в конфигурационный файл **/usr/local/etc/import_prismtokens.yaml**:

```
vim /usr/local/etc/import_prismtokens.yaml
```

2. В секции **prismtokens** создайте секцию **biz-admin**, как в примере ниже, и задайте токен в поле **key**:

```
prismtokens:
  biz-admin:
    methods:
      - _any
    ips: // список ip-адресов гипервизоров-фронтов Панели администратора
      - 192.0.2.1
      - 192.0.2.2
    akes: true
    key: <your_token>
```

   Этот токен понадобится вам ниже.

3. Чтобы изменения вступили в силу, выполните команду:

```
/usr/local/bin/import_prismtokens.py -f /usr/local/etc/import_prismtokens.yaml
```

При распределенной инсталляции Мессенджер и ВКС команда выполняется на одном из серверов.

Шаг 2. Откройте доступ в окружение администратора

Пропустите этот шаг, если не планируете создавать мини-аппы и управлять ими.

1. На сервере Мессенджер и ВКС перейдите в файл конфигурации **/usr/local/nginx-im/confv2/conf.d/myteam-admin_allow_hosts.inc**:

   ```
   vim /usr/local/nginx-im/confv2/conf.d/myteam-admin_allow_hosts.inc
   ```

2. В поле **allow** вместо <real.mail.ip> укажите список IP-адресов гипервизоров-фронтов Панели администратора VK WorkSpace:

   ```
   allow 192.0.2.1 192.0.2.2;
   ```

3. Чтобы изменения вступили в силу, выполните команду:

   ```
   nginx.sh reload
   ```

Шаг 3. Добавьте CN-группы администраторов

1. На сервере Мессенджер и ВКС перейдите в конфигурационный файл **/usr/share/tarantool/extra_config/nomail-1/nomail-1_extra_conf.lua**

   ```
   vim /usr/share/tarantool/extra_config/nomail-1/nomail-1_extra_conf.lua
   ```

2. В поле **myteam-admin** укажите CN-группы администраторов:

   ```
   cfg.otp_permission.apps = {
       ['myteam-client'] = '*',
       ['download_ios_application'] = '*',
       ['myteam-admin'] = {
           'myteam-admin'
       },
   }
   ```

3. Чтобы изменения вступили в силу, выполните команду:

   ```
   echo "dofile('/usr/share/tarantool/extra_config/nomail-1/nomail-1_extra_conf.lua')" |
   tarantoolctl enter nomail-1
   ```

4. Проверить актуальные настройки можно командой:

   ```
   echo "cfg.otp_permission.apps" | tarantoolctl enter nomail-1
   ```

Шаг 4. Создайте учетную запись с доступом в окружение администратора Мессенджер и ВКС

1. На сервере Мессенджер и ВКС в любой удобной папке создайте файл **users.yaml** и заполните его данными учетной записи (в примере ниже это admin@admin.qdit):

```
users:
    admin@admin.qdit:
        email: admin@admin.qdit
        firstName: admin
        lastName: admin
        attributes:
            memberOf: ["myteam-admin"] #член группы "myteam-admin" с доступом в окружение
администратора
```

   где memberOf: — название группы пользователей с доступом в окружение администратора.

   Объект users имеет тип Hash. При использовании расширенного формата yaml-файла username должен совпадать с email. В примере выше это admin@admin.qdit.

2. После создания **users.yaml** выполните в консоли команду:

```
users.py --cmd add -c users.yaml
```

3. Получите adminSn и adminRid созданной учетной записи:

```
 echo "show admin@admin.qdit" | nc 127.1 4281
```

   Значения rid и sn будут в выводе команды:

```
[root@superteams] centos# echo "show admin@admin.qdit" | nc 127.1 4281
$ rid: 0:100504
friendly: admin admin
fn: admin
ln: admin
am: -
-
Мобильный: -
sn: admin@admin.qdit
```

4. Перейдите в файл конфигурации **myteam-admin.yml**:

```
cd /usr/local/etc/k8s/helmwave/
vim projects/godmod/values/myteam-admin.yml
```

5. В секции **mpop** укажите адрес Панели администратора, sn (adminSn) и rid (adminRid), полученные на предыдущем шаге:

```
mpop:
    enable: false
    swa_host: http://biz.<domain>
    swa_url: /int/CheckSession
    adminSn: admin@admin.qdit // указать значение adminSn, полученное на предыдущем
шаге
    adminRid: 0:100504  // указать значение adminRid, полученное на предыдущем шаге
```

Шаг 5. Настройте сервис Stentor

1. На сервере Мессенджер и ВКС перейдите в конфигурационный файл **/usr/local/nginx-im/confv2/conf.d/stentor.conf**:

```
vim /usr/local/nginx-im/confv2/conf.d/stentor.conf
```

2. В поле **allow** вместо <real.mail.ip> укажите IP-адреса гипервизоров-фронтов Панели администратора VK WorkSpace:

```
location / {
    proxy_pass http://stentor_upsync$uri$is_args$args;
    allow 127.0.0.0/8;
    allow 10.32.0.0/16;
    allow <real.mail.ip>; // вместо <real.mail.ip> укажите IP-адреса гипервизоров-фронтов
Панели администратора VK WorkSpace
        deny all;
}
```

Шаг 6. Настройте отображение оргструктуры в Супераппе VK WorkSpace

Пропустите этот шаг, если не планируете подключать оргструктуру в Панели администратора VK WorkSpace.

1. На сервере Мессенджер и ВКС в конфигурационном файле **/usr/local/nginx-im/html/myteam/myteam-config.json** добавьте в секцию **services – config**:

```
"services": {
    "config": {
      "orgstructure": { // добавьте эту секцию, если пользуетесь функциональностью
структуры организаций
        "external": false,
        "needs_auth": true,
        "new": true,
        "url": "https://webim.<domain-vkt>/webapps/orgstructure",
        "url-dark": "https://webim.<domain-vkt>/webapps/orgstructure"
      },
    }
}
```

2. Добавьте в секцию **disposition**:

```
"disposition": {
    "desktop": {
        "leftbar": [
            "tasks",
            "calls",
            "orgstructure" // добавьте, если пользуетесь функциональностью структуры
организаций
        ]
    },
    "mobile": {
        "services": [
            "discover"
        ],
        "tabs": [
            "calls",
            "tasks",
            "orgstructure" // добавьте, если пользуетесь функциональностью структуры
организаций
        ]
    }
}
```

3. Примение изменения.

   Для инсталляции на одну виртуальную машину выполните команду:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true hwup -t godmod
```

   Для кластерной инсталляции:

```
HELMWAVE_USE_LOCAL_REPO_CACHE=true HELMWAVE_ENV_NAME=cluster hwup -t godmod
```

4. Перейдите в конфигурационный файл **/usr/local/nginx-im/confv2/cond.d/c4.conf** и добавьте после секции **direct upload version** секцию **location**:

```
location /files/ {
        set $original_script_uri $safe_uri;
        error_page 418 = @filesproxy;
        return 418;
    }
    location @filesproxy {
        rewrite ^/files(.*)$ $1;
        break;

        proxy_set_header   Host             files-c.myteaminternal;
        proxy_set_header   X-Real-IP        $remote_addr;
        proxy_set_header   X-Forwarded-For  $remote_addr;
        proxy_set_header   X-LB-Client-IP $remote_addr;
        # We have proxy enabled. In this case If-Mod.. is not passed to apache. This is
fix.
        proxy_set_header If-Modified-Since $http_if_modified_since;
        # MNT-155052 - universal ID for ICQ
        proxy_set_header X-Req-Id $hostname_short:$connection_requests:$connection:$msec;

        proxy_set_header X-Scheme $scheme;
        proxy_set_header X-LB-Client-IP $remote_addr;
```

```
        proxy_set_header HTTP_X_SSL_OFFLOAD $is_ssl;
        proxy_set_header X-Custom-SSL-Offload $is_ssl;
        proxy_set_header X-Original-Host $host;
        proxy_set_header X-Script-URL "$original_script_uri";

        proxy_pass http://files-c.myteaminternal;
}
```

5. Проверьте конфигурацию Ngnix:

```
nginx.sh  test
```

6. При отсутствии ошибок примените изменения:

```
nginx.sh reload
```

Шаг 7. Пересоздайте pod админ-консоли

Перезапустите под в технологическое окно (может приводить к сбою в новых подключениях). На сервере Мессенджер и ВКС выполните команду:

```
kubectl delete pods -n vkteams -l app=myteam-admin
```

2. Разверните Панель администратора VK WorkSpace

Шаг 1. Создайте пользователя deployer

1. В командной строке на сервере Панели администратора VK WorkSpace выполните последовательность команд:

   Astra Linux

   a. Задайте пароль и создайте пользователя deployer:

   ```
   sudo -i
   DEPLOYER_PASSWORD=mURvnxJ9Jr
   useradd -G astra-admin -U -m -s /bin/bash deployer
   echo deployer:"$DEPLOYER_PASSWORD" | chpasswd
   ```

   Проигнорируйте ошибку "НЕУДАЧНЫЙ ПАРОЛЬ: error loading dictionary", если она появилась.

   b. Авторизуйтесь под пользователем deployer:

```
sudo -i -u deployer
ssh-keygen -t rsa -N ""
```

c. Нажмите на клавишу Enter (согласиться с вариантом по умолчанию).

d. Скопируйте ssh-ключ в нужную директорию:

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

e. Опционально: проверьте, что можно подключиться без пароля:

```
ssh deployer@localhost
```

f. `exit`

РЕД ОС

a. Задайте пароль и создайте пользователя deployer:

```
sudo -i
DEPLOYER_PASSWORD=mURvnxJ9Jr
useradd -G wheel -U -m -s /bin/bash deployer
echo deployer:"$DEPLOYER_PASSWORD" | chpasswd
```

b. Авторизуйтесь под пользователем deployer:

```
sudo -i -u deployer
ssh-keygen -t rsa -N ""
```

c. Нажимите на клавишу Enter (согласиться с вариантом по умолчанию).

d. Скопируйте ssh-ключ в нужную директорию:

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

e. Опционально: проверьте, что можно подключиться без пароля:

```
ssh deployer@localhost
```

f. `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
```

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

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

1. Если на машину не установлен unzip, скачайте его:

```
sudo apt-get install unzip
```

2. Распакуйте дистрибутив:

```
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P <пароль> <имя_архива>
```

РЕД ОС

1. Если на машину не установлен unzip, скачайте его:

```
sudo yum install unzip
```

2. Распакуйте дистрибутив:

```
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. 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.

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

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

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

Ответ в случае успешного запуска установщика выглядит следующим образом:

Astra Linux

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

РЕД ОС

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

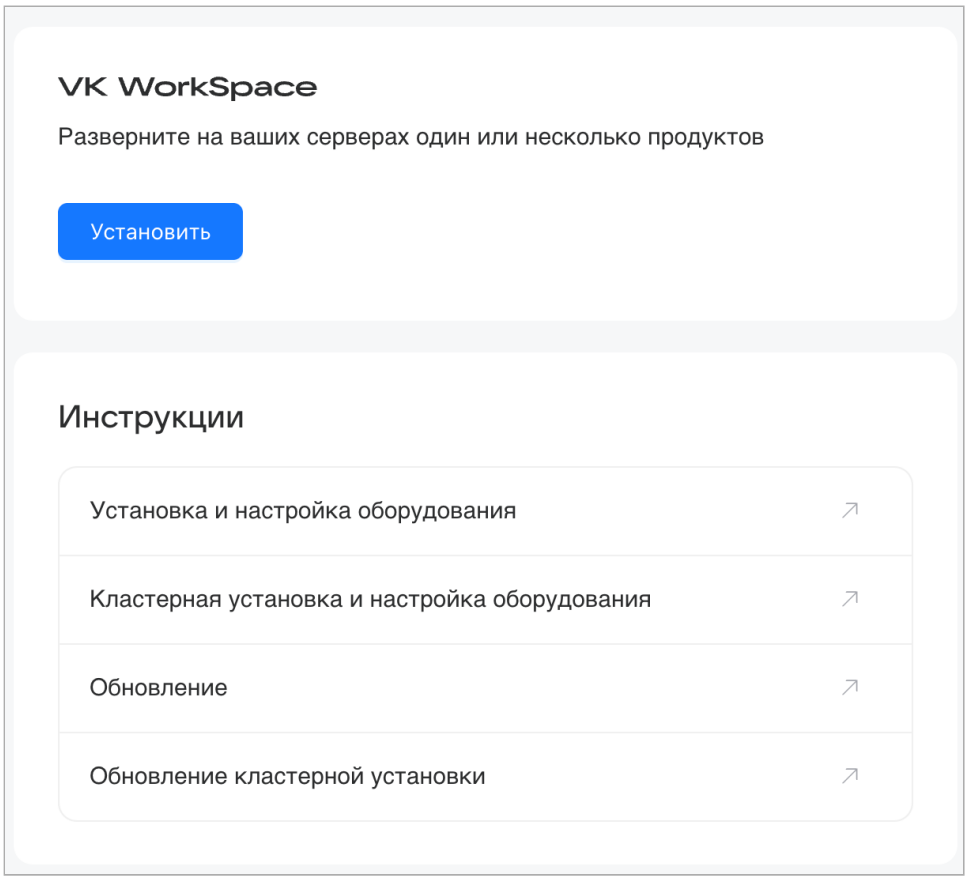
Примечание

Невозможность включения службы rsyslog не повлияет на корректность работы сервиса.

Шаг 4. Выберите вариант установки

Перейдите в веб-интерфейс установщика Панели администратора по адресу http://server-ip-address:8888. Если перейти по этому адресу не удается, убедитесь, что firewall был отключен.

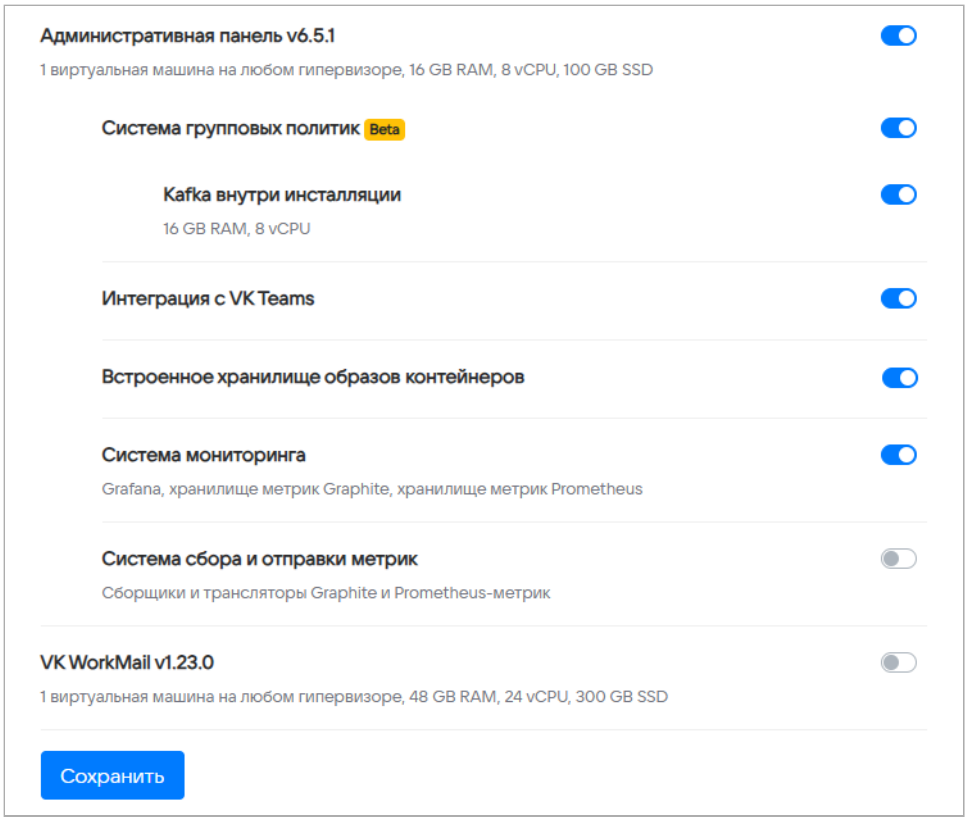
На стартовой странице нажмите на кнопку **Установка**.



Шаг 5. Выбор продуктов и опций

Включите флаг **Административная Панель**.

В открывшемся списке выберите нужные вам компоненты:



Система групповых политик — если в дальнейшем планируется настраивать сервисы групповых политик.

Kafka внутри инсталляции — если при настройке групповых политик НЕ будет использован внешний сервис Kafka.

Интеграция с Мессенджер и ВКС — обязательный компонент.

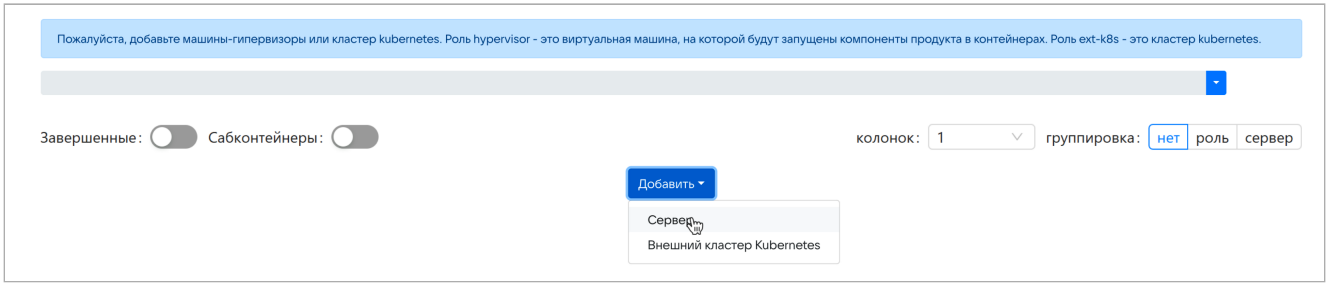
Система мониторинга — опциональный компонент. Не используется совместно с компонентом **Система сбора и отправки метрик**.

Система сборка и отправки метрик — опциональный компонент. Не используется совместно с компонентом **Система мониторинга**.

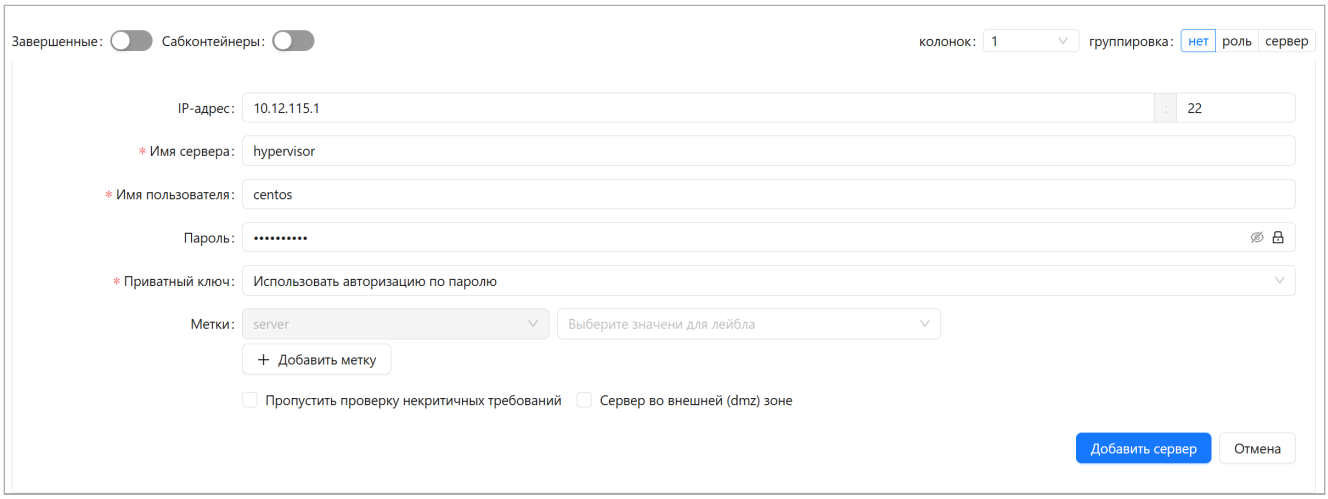
Нажмите на кнопку **Далее** внизу страницы, чтобы перейти к следующему шагу.

Шаг 6. Добавьте гипервизоры

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



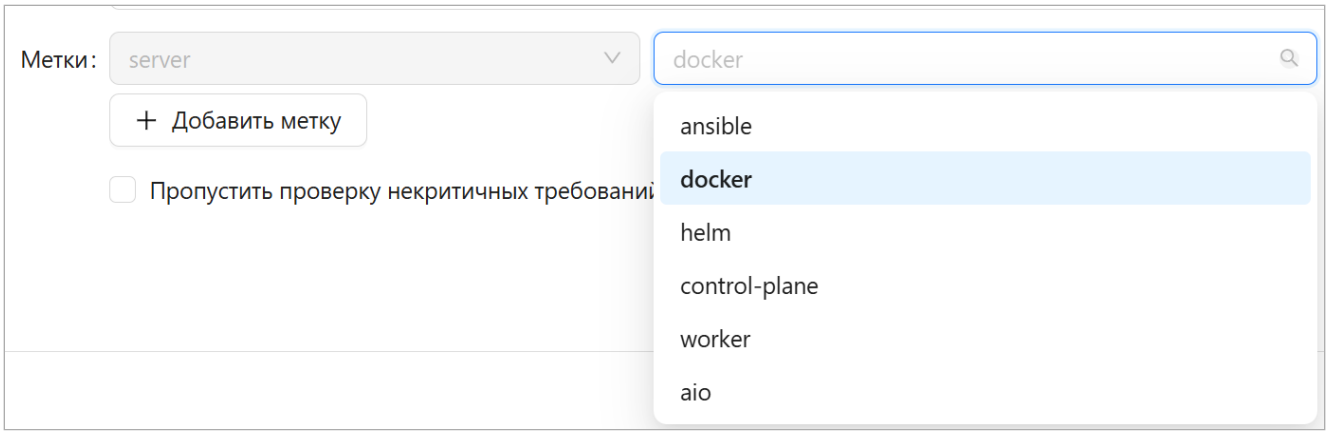
Откроется окно добавления гипервизора:



3. Заполните поля:

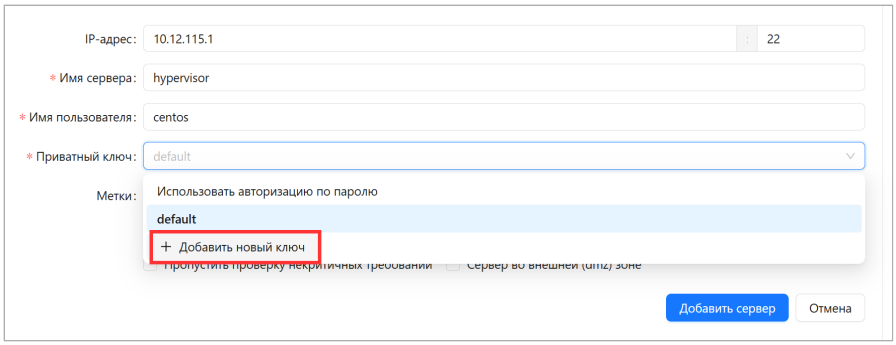
   - **Роль** — hypervisor.
   - **IP** — адрес машины, на которую производится установка.
   - **SSH-порт** — стандартный для SSH, выбран по умолчанию, менять его не нужно.
   - **Имя гипервизора** — укажите имя гипервизора или оставьте поле пустым. В случае если вы оставите поле незаполненным, имя гипервизора будет взято из **hostname -s** и добавится автоматически. 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.

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



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

   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, 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 **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** — 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.

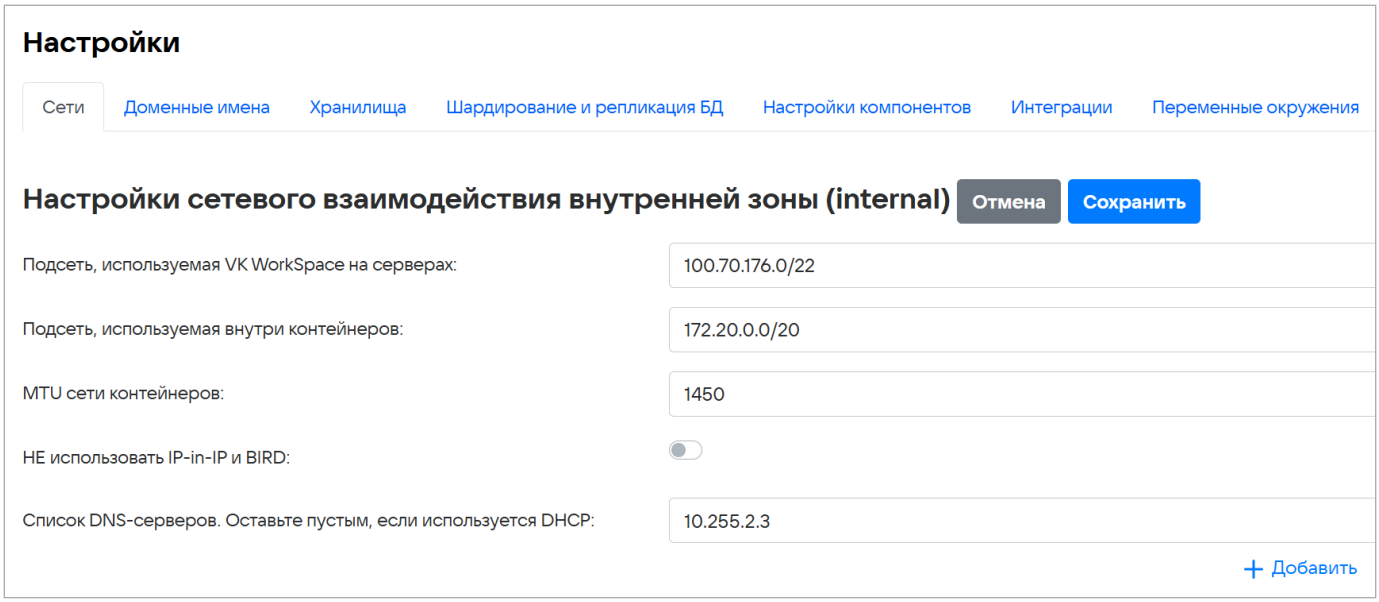
8. Аналогичным образом добавьте еще 5 гипервизоров:

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

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

Шаг 7. Укажите настройки сети

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 виртуальной машине в соответствии с рекомендациями: для RedOS, для Astra Linux.

2. Убедитесь, что:

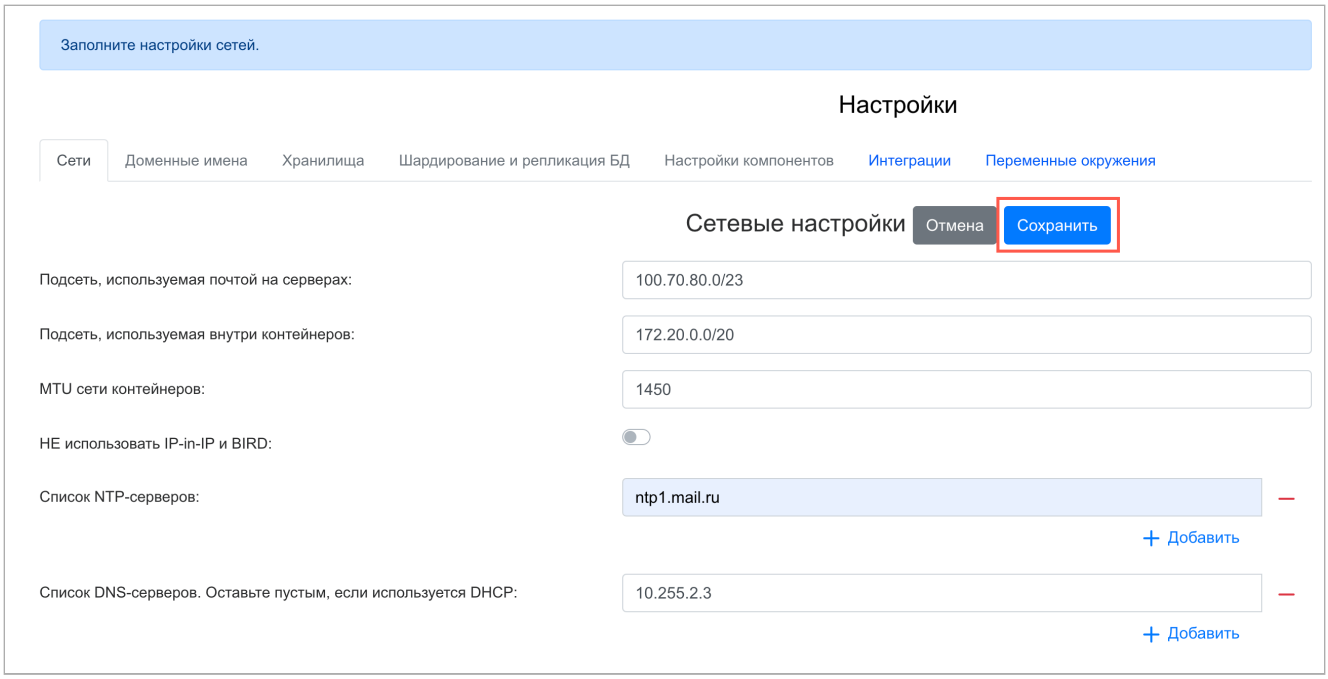
   - **Подсеть, используемая Панелью администратора на серверах** имеет доступ на 80 или 443 порт.
   - **Подсеть, используемая внутри контейнеров** полностью свободна, уникальна и принадлежит только Панели администратора VK WorkSpace.

> **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.

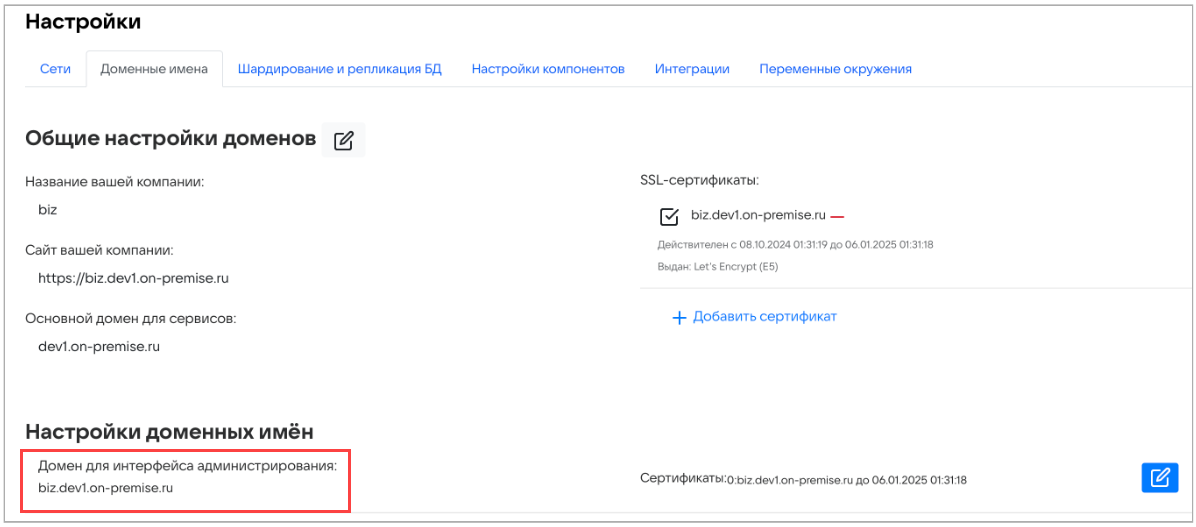
Флаг **НЕ использовать IP-in-IP и BIRD** в большинстве случаев должен оставаться неактивным. Если на машине используется динамическая маршрутизация и необходимо включение опции, обратитесь к представителю VK.

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



Шаг 8. Доменные имена

1. На вкладке **Доменные имена** нажмите на иконку  и укажите:
   - Основной домен для сервисов — домен, созданный для Панели администратора выше.
   - Домен? по которому будет доступен интерфейс администрирования — biz.<основной домен>.

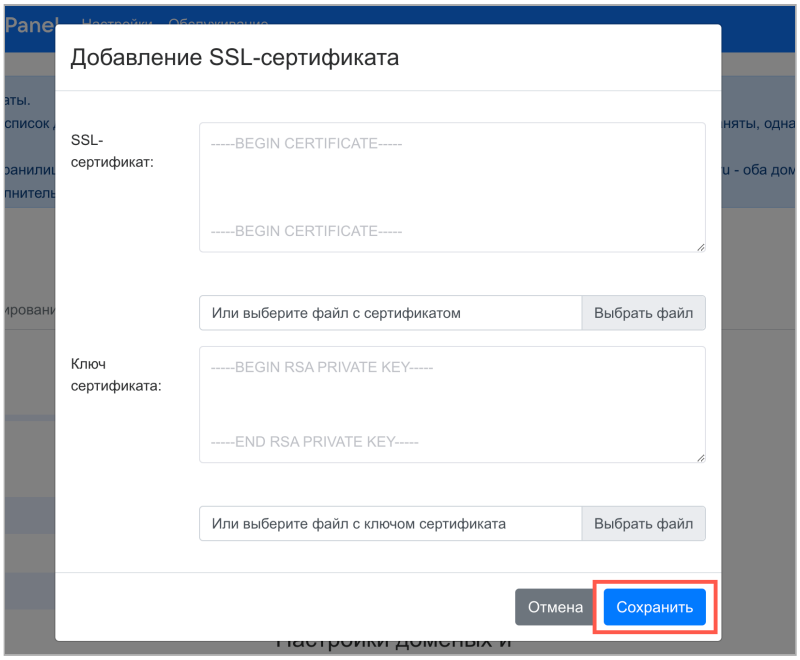


> **Внимание**
>
> Для доменных имен нельзя использовать `etc/hosts`.

2. Нажмите на кнопку **Сохранить**.
3. Нажмите на кнопку **Добавить сертификат** под заголовком **SSL-сертификаты**.
4. 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-----`.

5. Кликните по кнопке **Сохранить**:



Есть второй вариант:

a. Нажмите на кнопку **Выбрать файл**.

b. Укажите путь к файлу с сертификатом .crt.

c. Укажите путь к файлу с ключом .key.

d. 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** в правом верхнем углу.

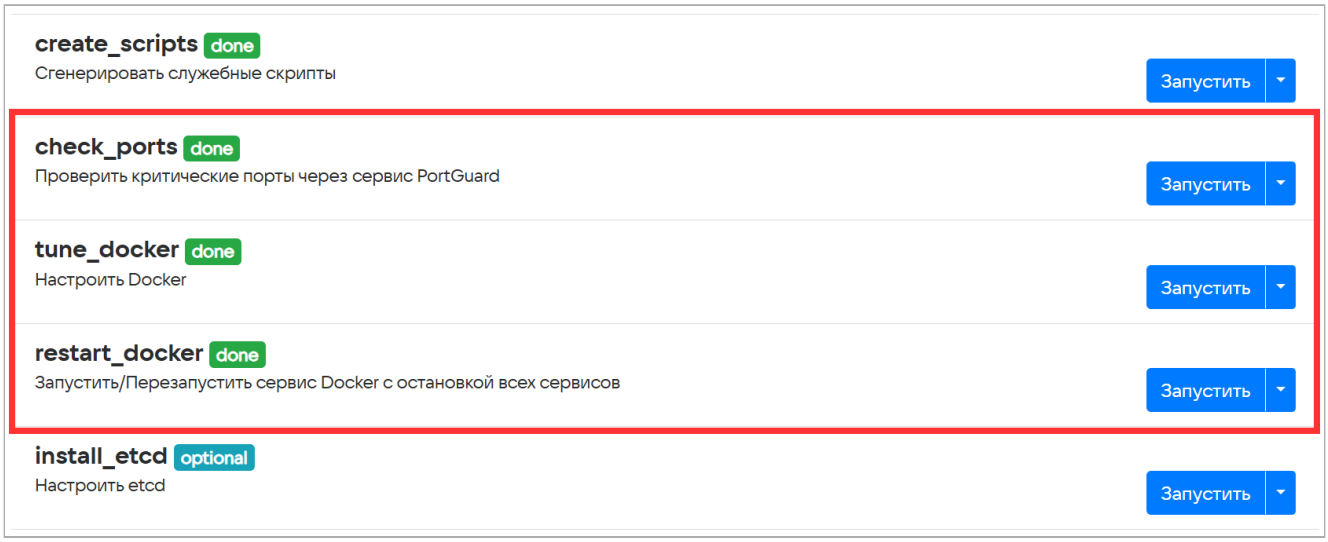
Шаг 9. Запустите установку гипервизоров

Для начала установки необходимо перейти 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 шаги до **upload_docker_repo** включительно.

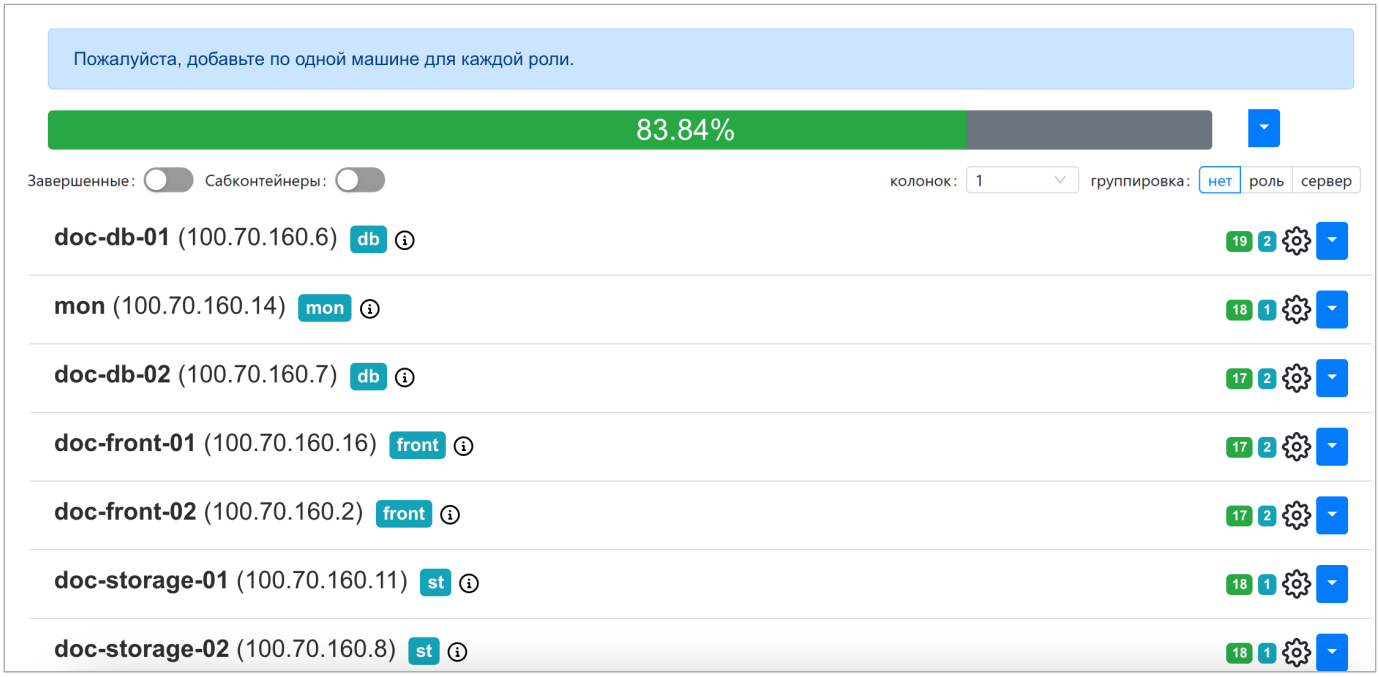


2. Вернитесь обратно к списку машин и перейдите в настройки первого гипервизора-стораджа.
3. Вручную запустите шаги до **install_etcd** включительно. По завершении шага первый узел etcd будет установлен.

4. Таким же способом установите etcd на остальные два гипервизора-стоража.
5. После того, как кластер etcd собран, запустите установку всех гипервизоров по порядку или общую автоматическую установку.

> **Внимание**
>
> Не рекомендуется запускать 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.

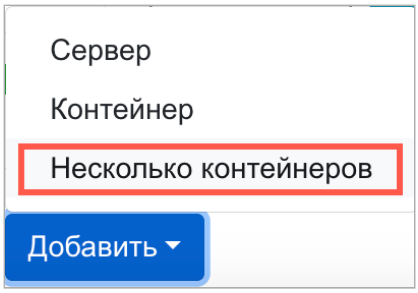


Кликните по значку ⓘ и перейдите в раздел **Описание сервисов**, чтобы посмотреть развернутую информацию о назначении ролей, их дублируемости, зависимостях и т.п. В этом же выпадающем меню вы найдете дополнительную документацию, сможете включить или выключить продукты (внутри раздела **Продукты**) и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

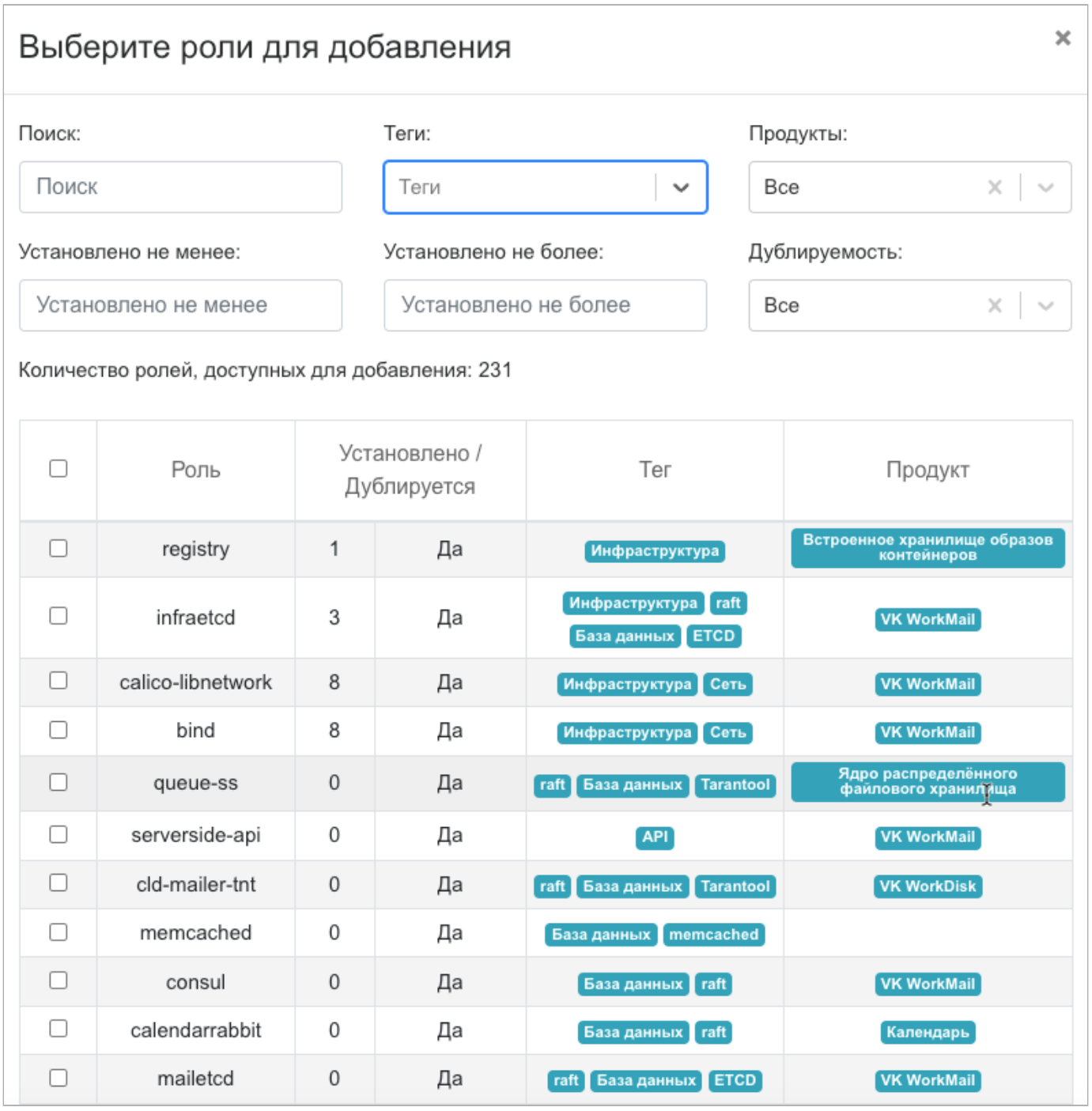
Шаг 10. Распределите контейнеры по гипервизорам

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

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



Откроется окно выбора ролей.



При распределении ролей нужно соблюдать такой порядок:

1. raft
2. Базы данных
3. Мониторинг

4. API
5. Все, что осталось (опционально)

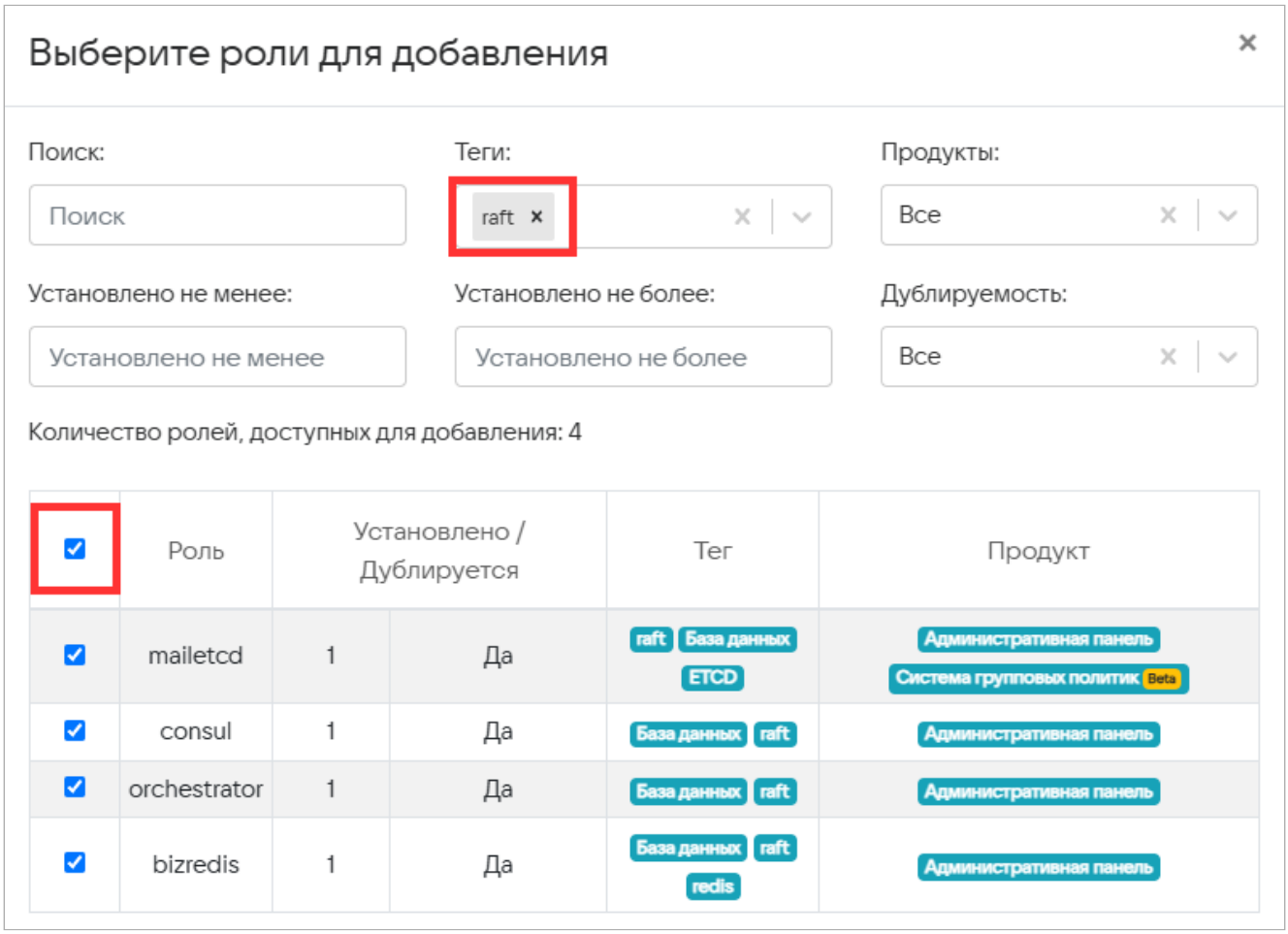
> **Внимание**
>
> Порядок распределения ролей принципиально важен, при его нарушении вы столкнетесь с ошибками.

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

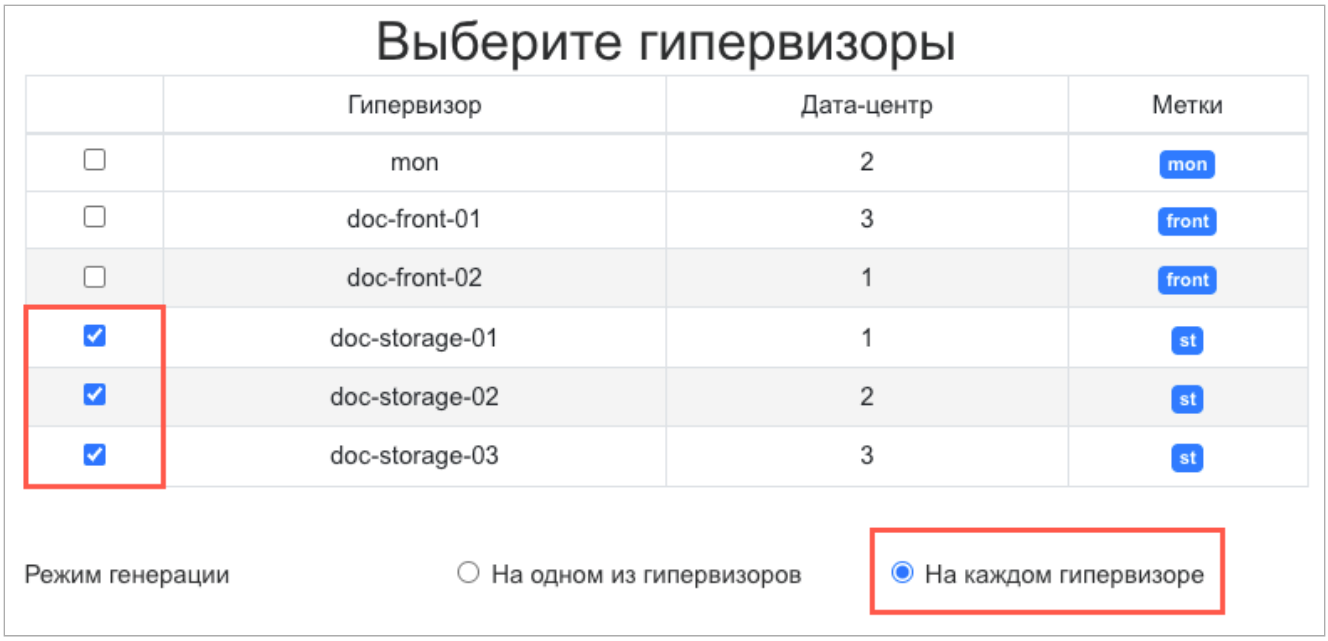
Порядок действий при распределении контейнеров

На гипервизоры, отведенные под базы данных, необходимо добавить кластер **raft**.

1. В выпадающем меню выберите тег **raft**.
2. Для фильтра **Установлено 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 базы данных.
5. Режим генерации — **На каждом гипервизоре**.



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

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

Следующий шаг — распределение ролей для баз данных.

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

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

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

Завершающий этап — распределить роли для API.

1. Выберите тег **API**.

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

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

1. Откройте окно добавления выбора ролей, нажав на **Добавить** → **Несколько контейнеров**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Список ролей, доступных для добавления, должен быть пустым. Если это не так, распределите оставшиеся роли по гипевизорам в соответствии с тегами.

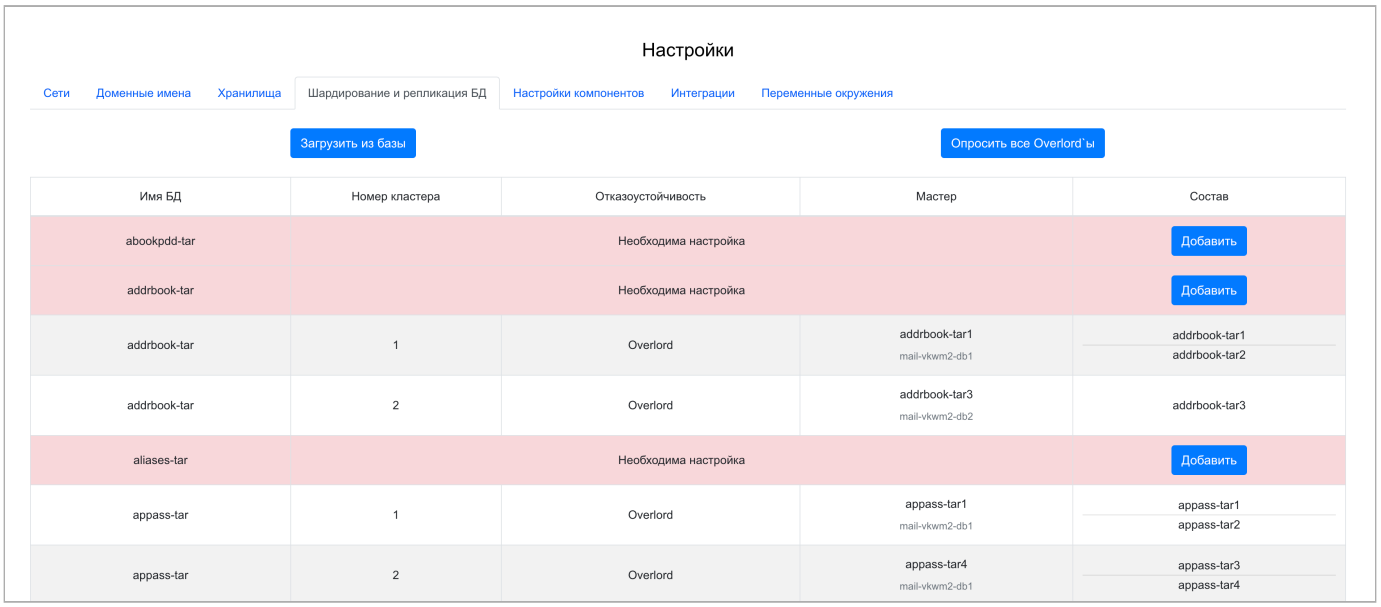
После того как все контейнеры сгенерированы, нажмите на зеленую кнопку **Далее** в правом верхнем углу.

Шаг 11. 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.

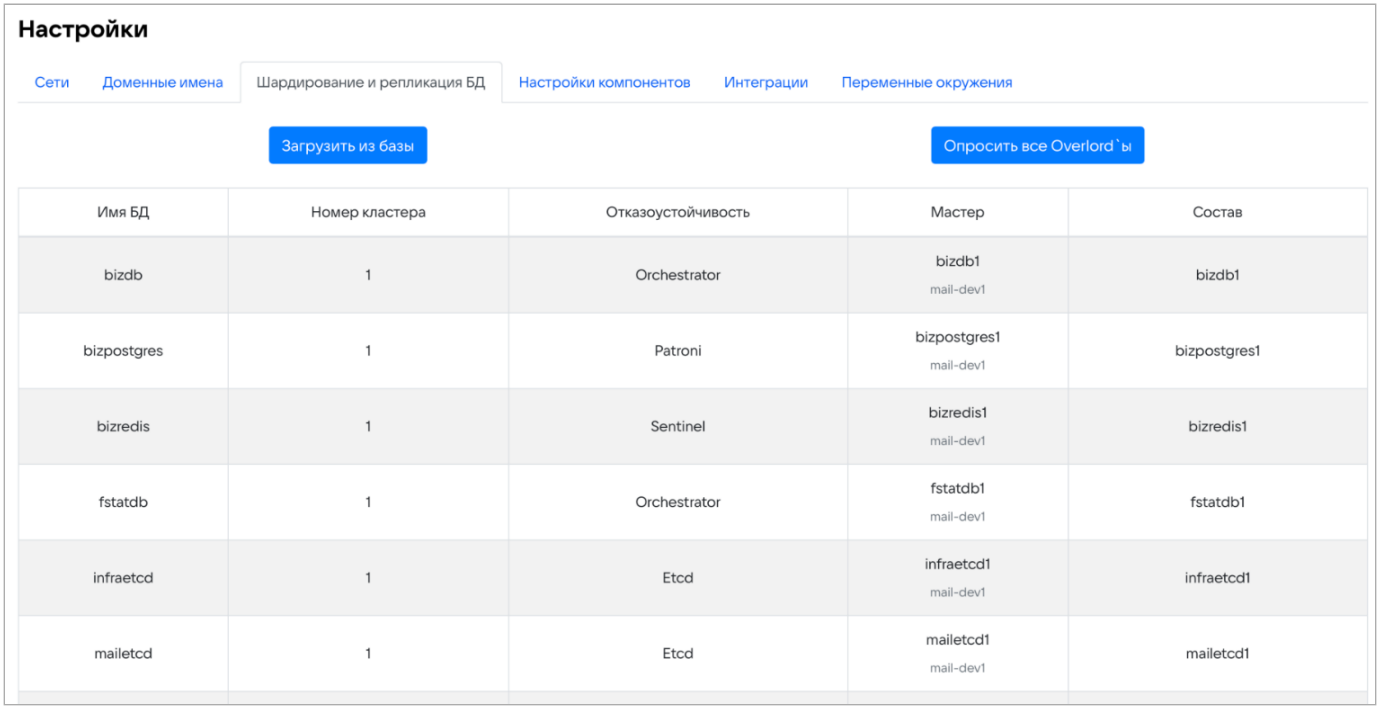


Чтобы добавить кластер:

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.

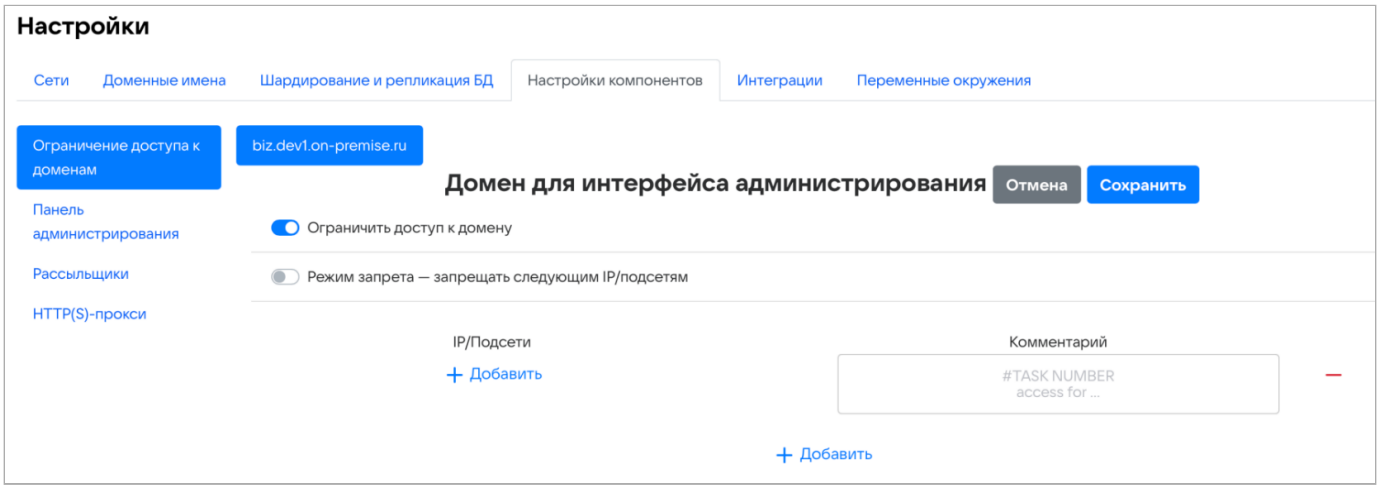
После добавления всех кластеров появится возможность перейти к следующему шагу с помощью кнопки **Далее**.



Шаг 12. Настройте компоненты

Ограничение доступа к доменам

На вкладке **Настройки компонентов** выберите нужный домен и нажмите на иконку  . После включения флага **Ограничить доступ к домену** появится раздел с более детальными настройками:



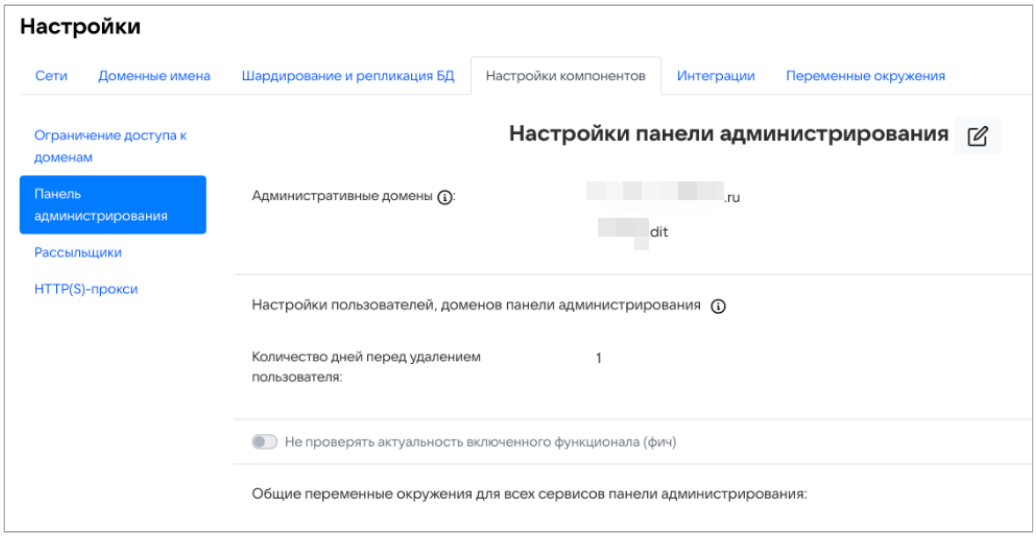
Ограничить доступ к домену — если включен только этот флаг, в поле ниже нужно будет ввести IP/подсети, которым будет **разрешен** доступ к домену. Также вы можете добавить комментарии, если это необходимо.

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 иконку  в общей строке состояния. Для этого перейдите к списку шагов, кликнув по логотипу в левом верхнем углу веб-интерфейса.

Панель администрирования

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

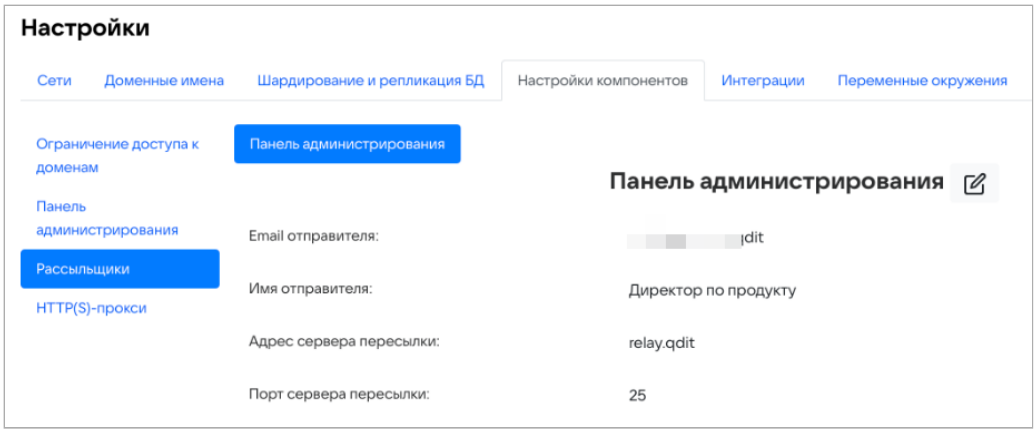


Количество дней перед удалением пользователя — количество дней, по прошествии которых пользователь будет удален из Панели администратора VK WorkSpace. Изменение настройки по умолчанию актуально при одновременном использовании Панели администратора VK WorkSpace с Active Directory. По умолчанию выставлен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

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

Рассыльщики

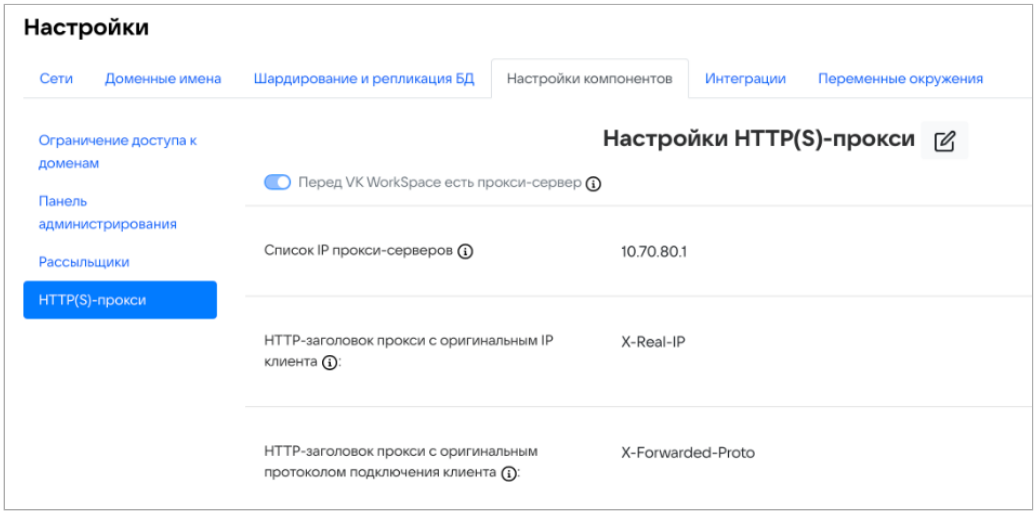
В разделе настраиваются служебные почтовые рассылки для внутренних пользователей. Чтобы перейти к настройкам, нажмите на иконку  .



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.

Настройки HTTP(S)-прокси

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



Список IP прокси-серверов — введите в поле список IP-адресов, с которых VK WorkSpace 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 VK WorkSpace введите заголовок оригинального протокола подключения.

Шаг 13. Настройте интеграцию с Мессенджер и ВКС

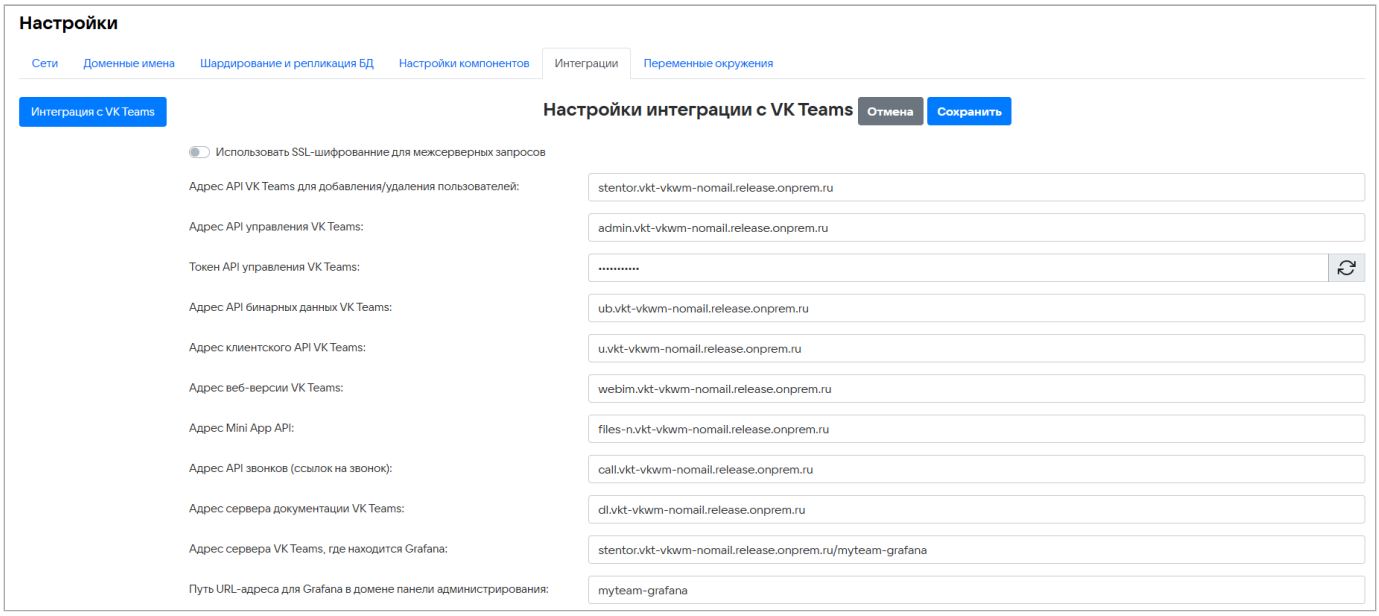
1. Перейдите на вкладку **Интеграции** → **Интеграция с Мессенджер и ВКС**.
2. Включите флаг **Использовать SSL шифрование для межсерверных запросов**.
3. Заполните все поля:

Название поля	**Значение**
Адрес API Мессенджер и ВКС для добавления/удаления пользователей	stentor.<домен Мессенджер и ВКС>.ru
Адрес API управления Мессенджер и ВКС	admin.<домен Мессенджер и ВКС>
Токен API управления Мессенджер и ВКС	Нажмите на серую кнопку в поле, чтобы сгенерировать токен. Этот токен понадобится вам ниже.
Адрес API бинарных данных Мессенджер и ВКС	ub.<домен Мессенджер и ВКС>
Адрес клиентского API Мессенджер и ВКС	u.<домен Мессенджер и ВКС>
Адрес веб-версии Мессенджер и ВКС	webim.<домен Мессенджер и ВКС>
Адрес Mini App API	files-n.<домен Мессенджер и ВКС>
Адрес API звонков (ссылок на звонок)	call.<домен Мессенджер и ВКС>
Адрес сервера документации Мессенджер и ВКС	Укажите адрес портала организации, по которому доступен Суперапп VK WorkSpace и инструкции Мессенджер и ВКС, например: dl.<домен Мессенджер и ВКС>
Адрес сервера Мессенджер и ВКС, где находится Grafana	Для версии Мессенджер и ВКС 24.2 и ниже: stentor.<домен Мессенджер и ВКС>/myteam-grafana Начиная с версии Мессенджер и ВКС 24.3: stentor.<домен Мессенджер и ВКС>/grafana
	myteam-grafana

Название поля	Значение
Путь URL-адреса для Grafana в домене Панели администрирования	
Токен Мессенджер и ВКС для получения структуры организаций в Панели администрирования	Значение key из шага Создайте токен biz-admin
Пользователь ClickHouse Мессенджер и ВКС	biz
Пароль пользователя ClickHouse Мессенджер и ВКС	Чтобы получить пароль, выполните команду: `cat /usr/local/etc/k8s/helmwave/projects/godmod/secrets/clickhouse-metric-cluster.yml | grep password: | cut -d':' -f2 | sed 's/ //'`
Список IP адресов/подсетей Мессенджер и ВКС (для ACL в SWA)	<IP-адреса серверов Мессенджер и ВКС>

Примечание

На скриншоте ниже в качестве домена Мессенджер и ВКС используется vkt-02.on-premise.ru. Используйте ваш домен Мессенджер и ВКС.



Шаг 14. Укажите токен на сервере Мессенджер и ВКС

Скорректируйте конфигурацию etcd:

1. Пропишите в etcd Мессенджер и ВКС токен API управления Мессенджер и ВКС, сгенерированный на шаге выше:

   ```
   etcdctl --endpoints etcd.im-etcd.svc.cluster.local:2379 put '/vars/services/godmod/
   production/private/service/auth/secret/secret' <token>
   ```

   где <token> — это токен API управления Мессенджер и ВКС.

2. Укажите подсети для сетевого соединения Панели администратора и Мессенджер и ВКС:

   ```
   etcdctl --endpoints etcd.im-etcd.svc.cluster.local:2379 put '/vars/services/godmod/
   production/private/service/auth/secret/ip_subnets' '["192.0.2.0/24","203.0.113.0/24"]'
   ```

   где 192.0.2.0/24 и 203.0.113.0/24 — примеры подсетей.

3. Далее выполните команды:

   ```
   etcdctl --endpoints etcd.im-etcd.svc.cluster.local:2379 put '/vars/services/godmod/
   production/private/service/auth/secret/enable' 'true'
   ```

   ```
   etcdctl --endpoints etcd.im-etcd.svc.cluster.local:2379 put '/vars/services/godmod/
   production/private/service/auth/mpop/enable' 'false'
   ```

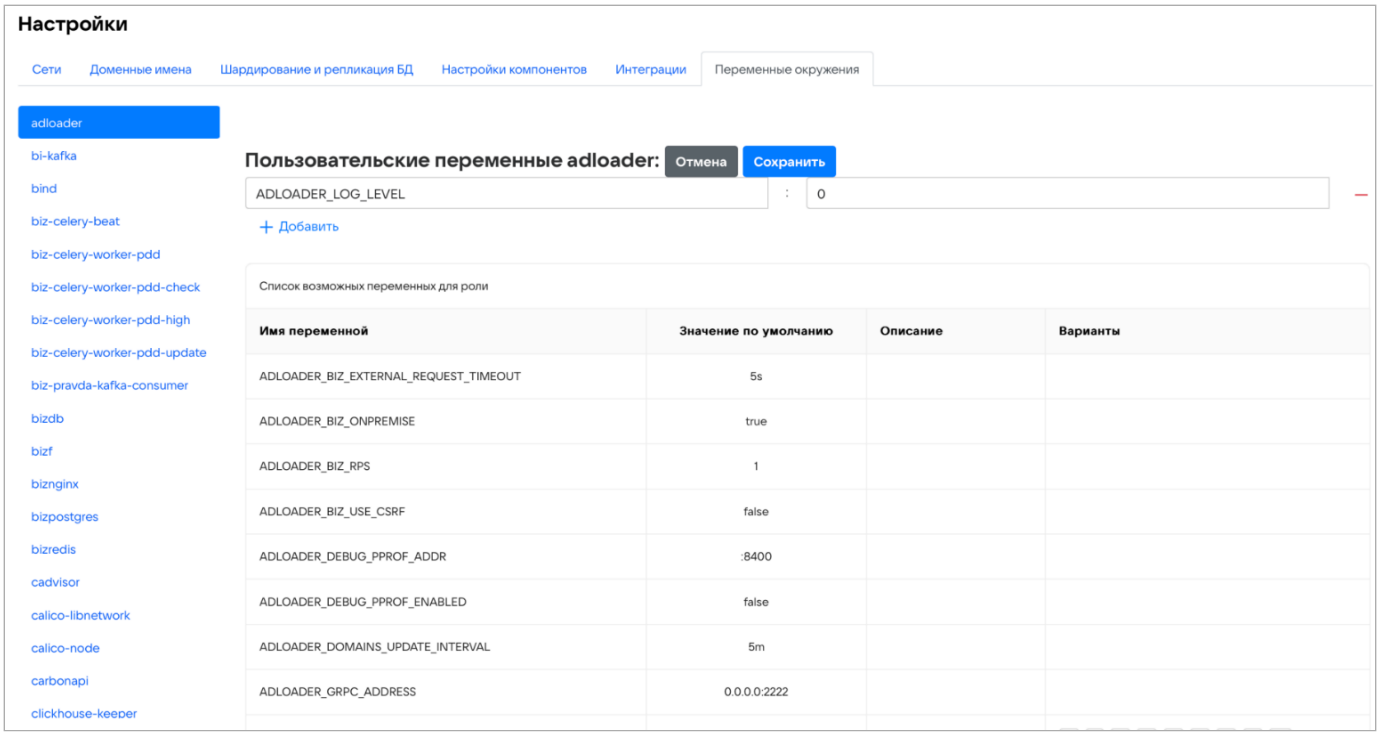
4. Выполните рестарт виртуальной машины:

   ```
   reboot
   ```

> **Внимание**
>
> Если на данном шаге появились какие-либо ошибки, обратитесь в службу технической поддержки.

Шаг 15. Укажите переменные окружения

В разделе производится настройка кастомных переменных Панели администратора.



Внимание

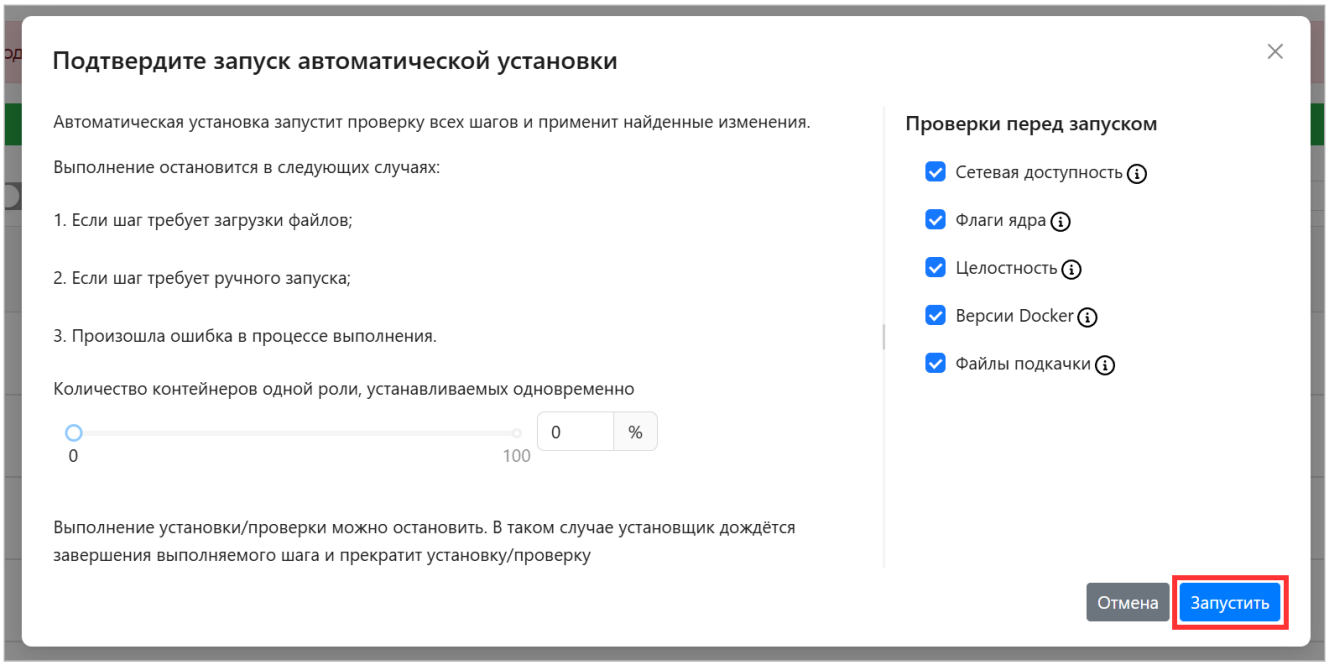
Настройка переменных окружения возможна только после консультации с представителем VK.

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 16. 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:

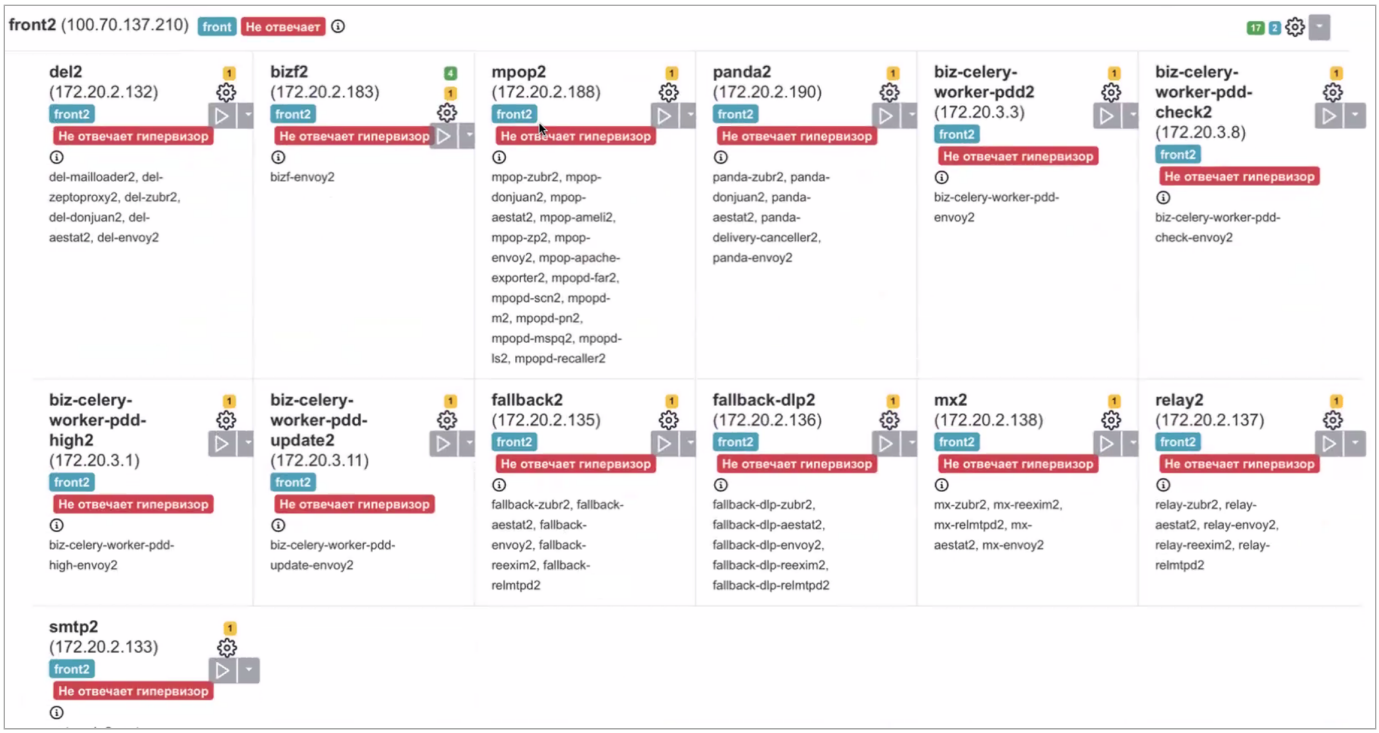
- **Серый** — в ожидании начала генерации.
- **Синий** — в процессе генерации.
- **Желтый** — шаг будет повторен (автоматически).
- **Красный** — ошибка.

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.

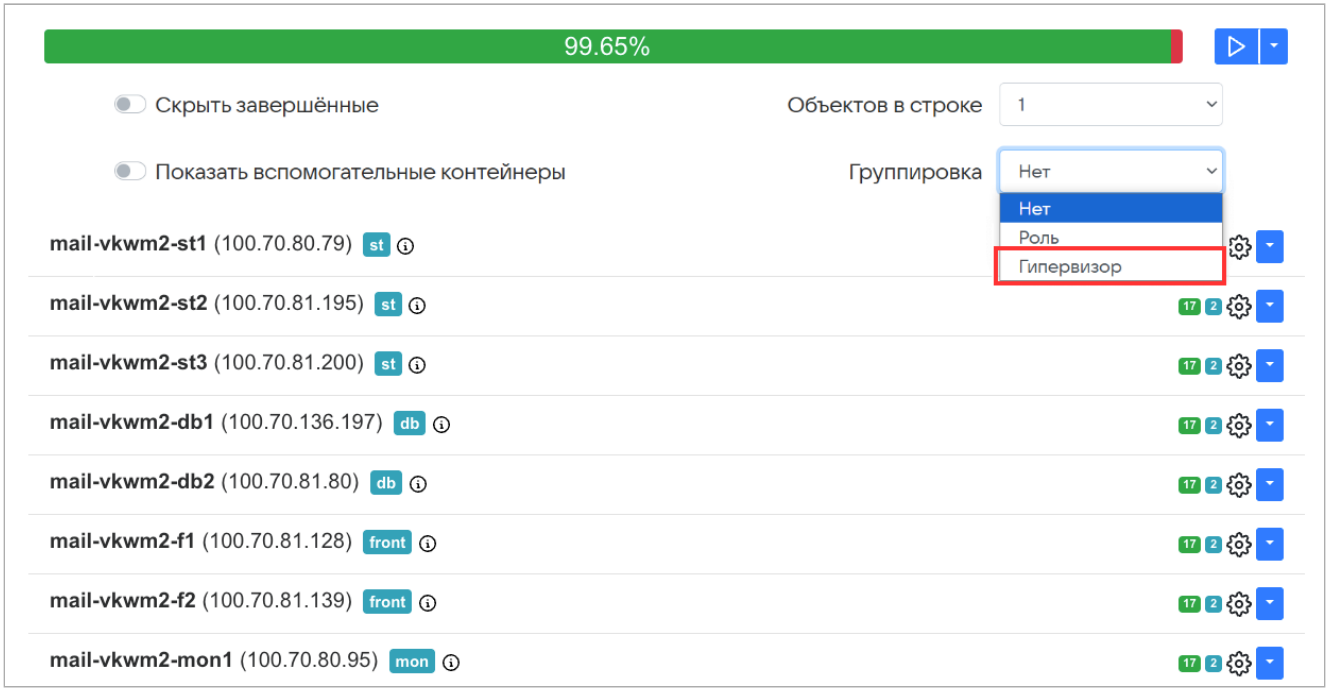
Для повторного запуска необходимо нажать на иконку  в общей строке состояния в верхней части экрана или рядом с названием конкретного контейнера.

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

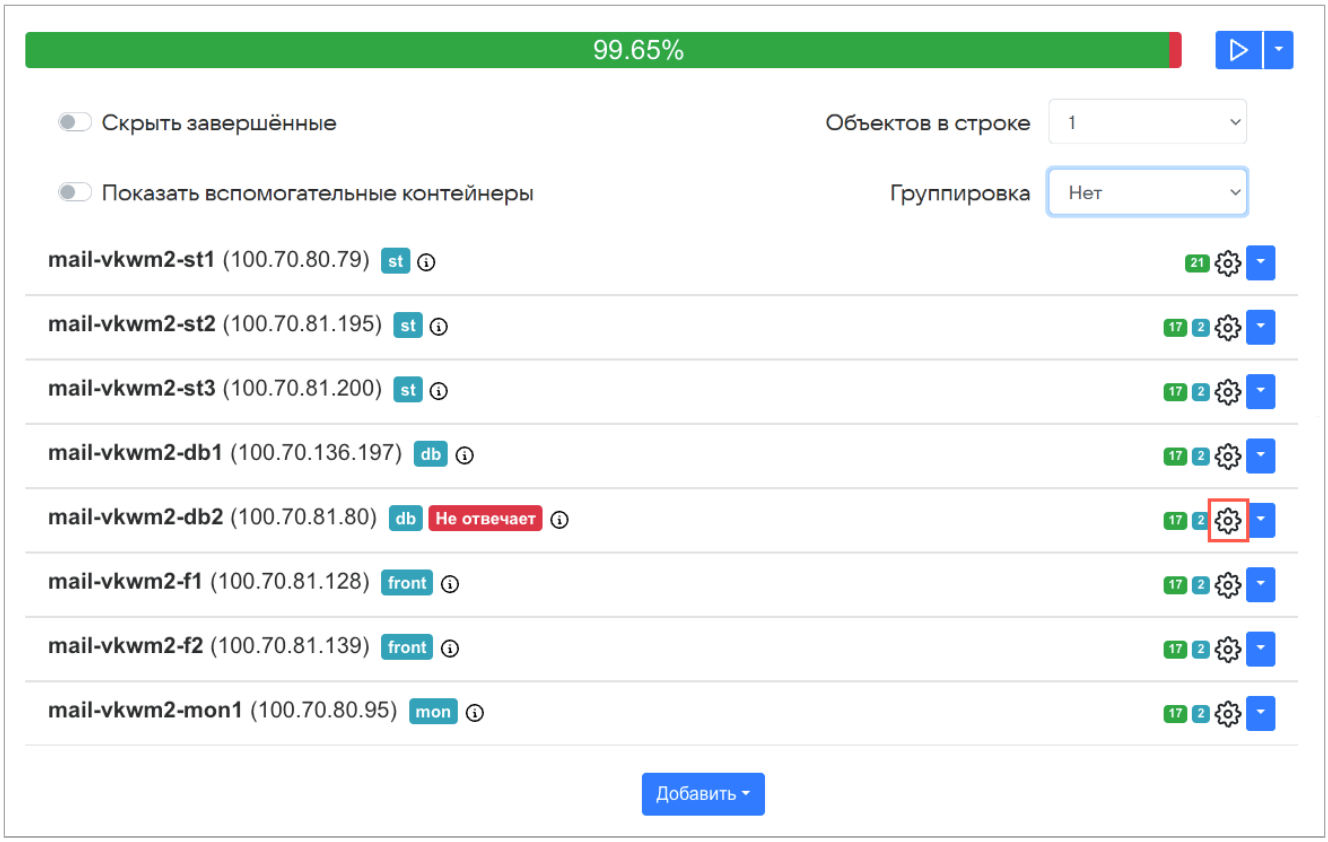


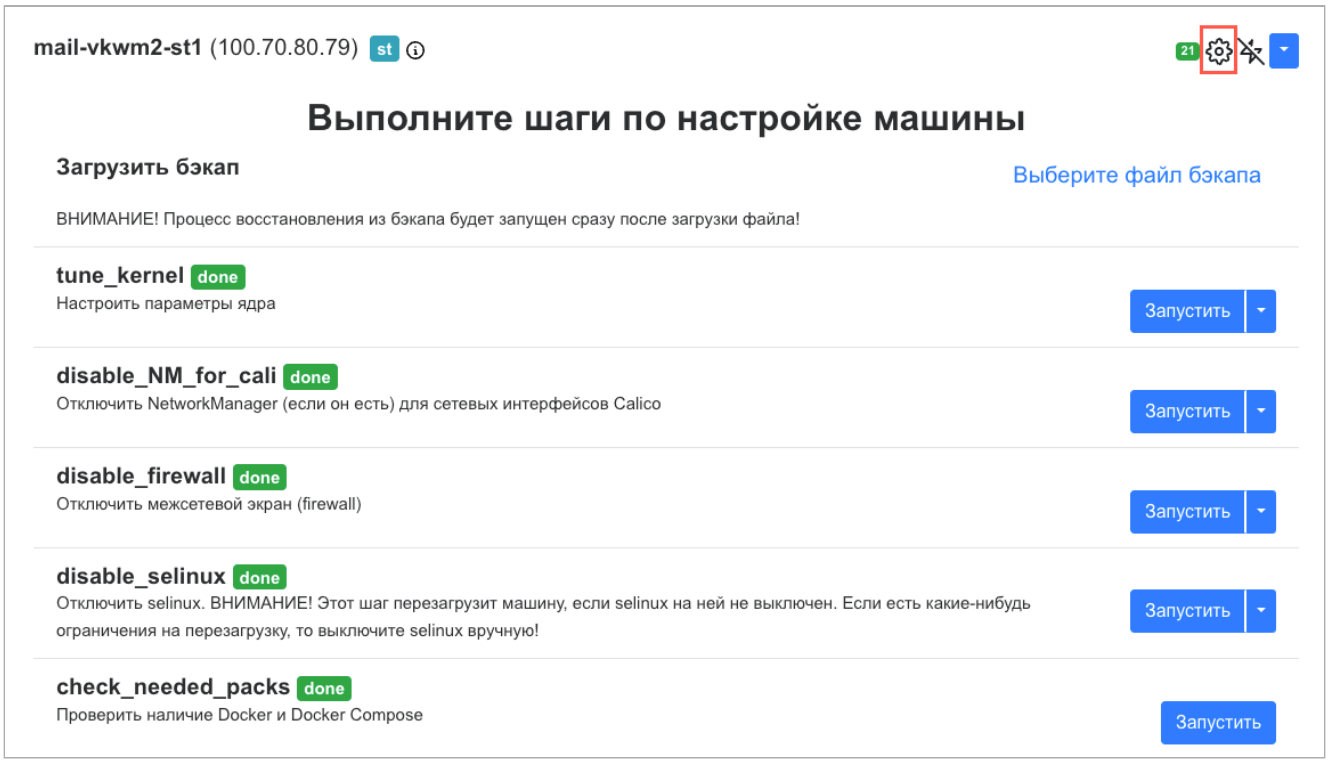
Чтобы продолжить установку:

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

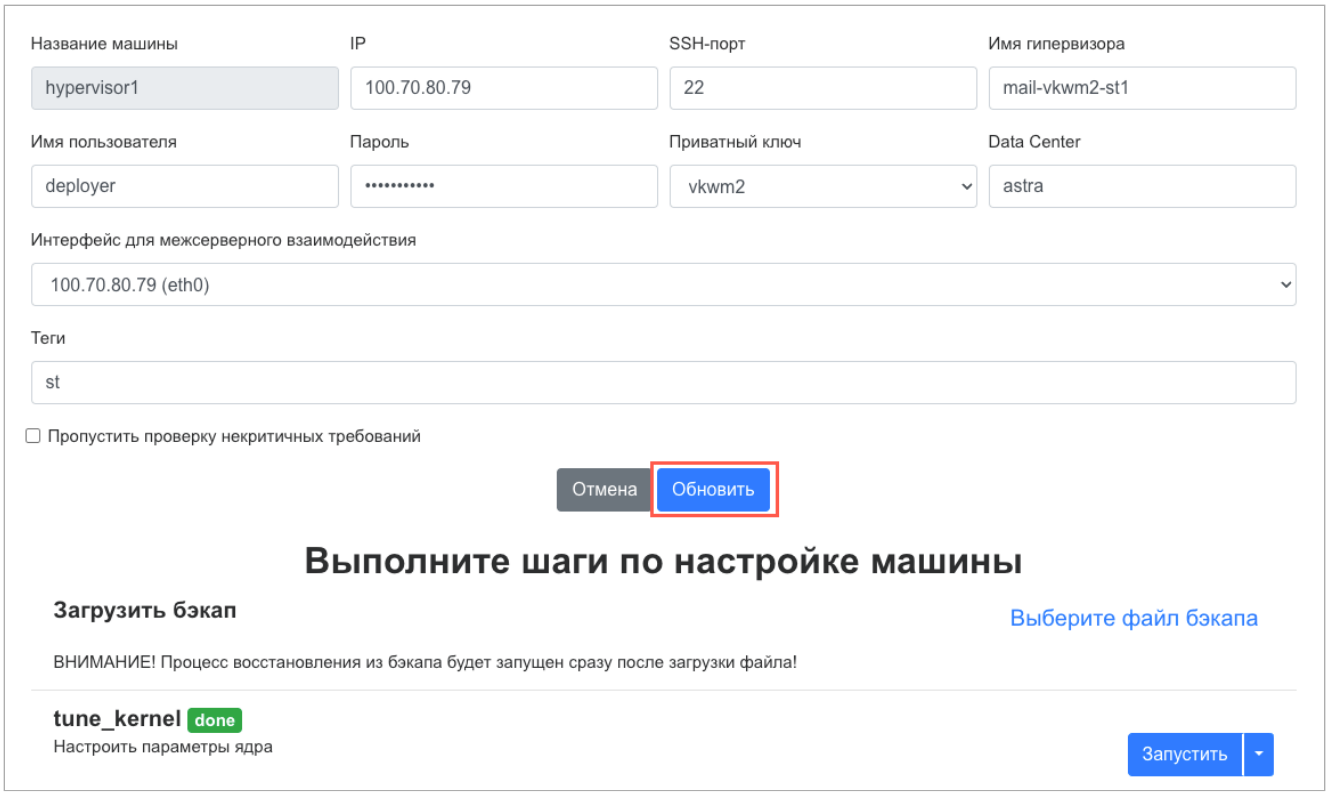


2. После этого перейдите в командную строку и устраните ошибку. По завершении необходимо нажать на шестеренку в строке гипервизора, на котором была ошибка, затем на странице в списке шагов на гипервизоре.





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

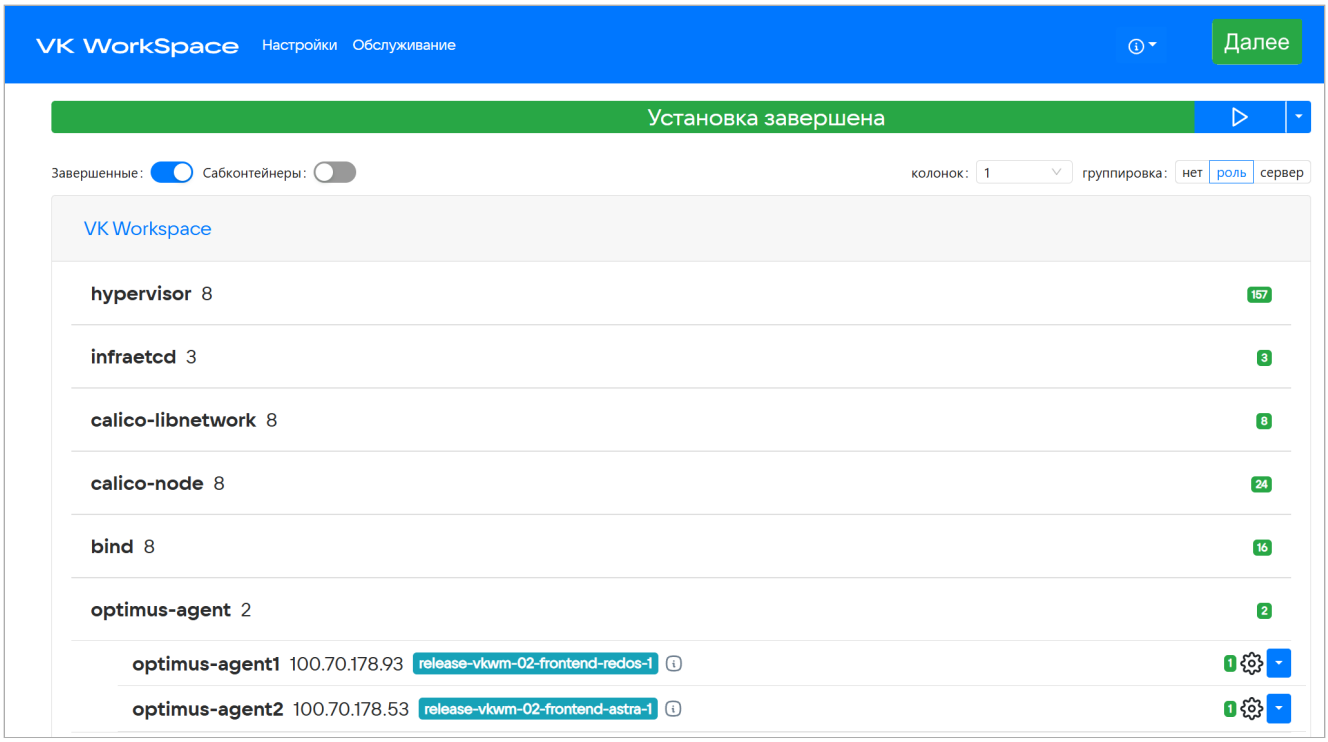


4. Повторно запустите автоматическую установку.

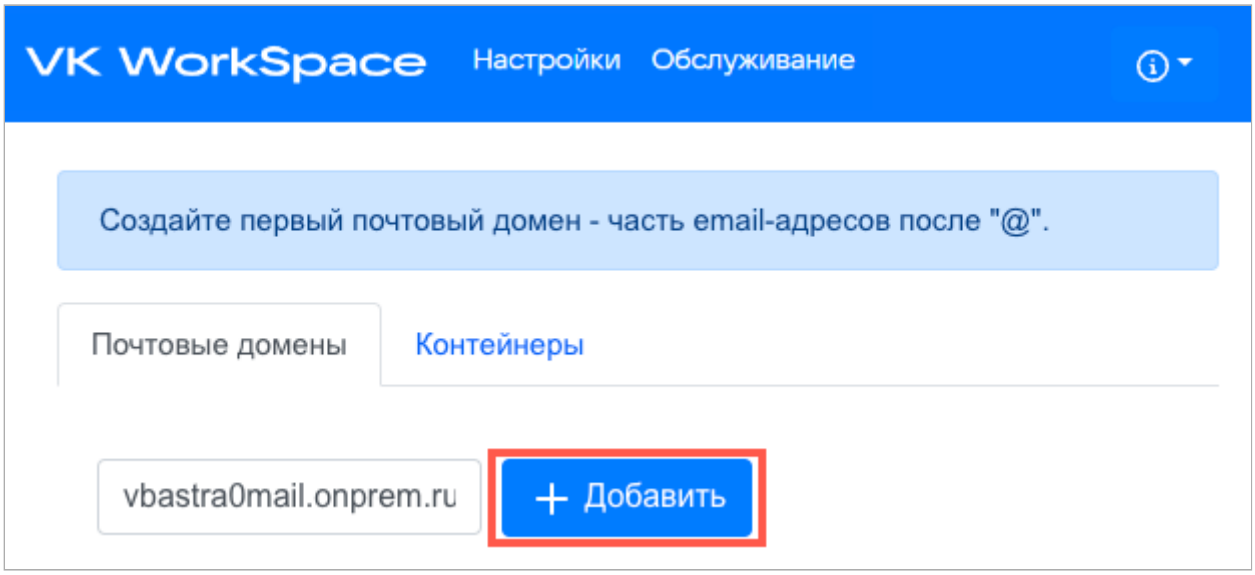
Шаг 17. Инициализируйте домен и войдите в Панель администратора

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

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



2. Введите имя почтового домена вашей корпоративной почты 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

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 Панели администратора.

3. Добавьте пользователей в Панель администратора

При наличии ActiveDirectory настройте интеграцию в Панели администратора (см. инструкцию).

Если у вас нет ActiveDirectory:

1. Обратитесь в службу технической поддержки для подключения функциональности создания и управления пользователями в Панели администратора.
2. После подключения функциональности импортируйте пользователей при помощи CSV-файла (см. инструкцию).

Важно

Списки пользователей в Мессенджер и ВКС и Панели администратора должны совпадать. Синхронизация пользователей с ActiveDirectory и массовое добавление пользователей при помощи CSV-файла занимает некоторое время. Дождитесь полной синхронизации с ActiveDirectory и загрузки всех пользователей.

Если у вас нет ActiveDirectory, интеграция с Панелью администратора считается завершенной. Если настроена интеграция Мессенджер и ВКС с ActiveDirectory, удалите LDAP-подключение (см. ниже).

4. Удалите LDAP-подключение Мессенджер и ВКС

Примечание

Пропустите этот шаг, если у вас нет ActiveDirectory или интеграция с ActiveDirectory не настраивалась.

1. Чтобы удалить LDAP-подключение, на сервере Мессенджер и ВКС выполните команды:

```
>kccli ldap delete --name <имя вашего LDAP сервера> //удаление по имени
>kccli ldap delete --id <id вашего LDAP сервера> //удаление по ID
```

Используйте удаление по ID в случае, если ранее было заведено несколько LDAP-серверов с неуникальными именами. Получить ID подключений можно, выполнив команду:

```
kccli ldap get
```

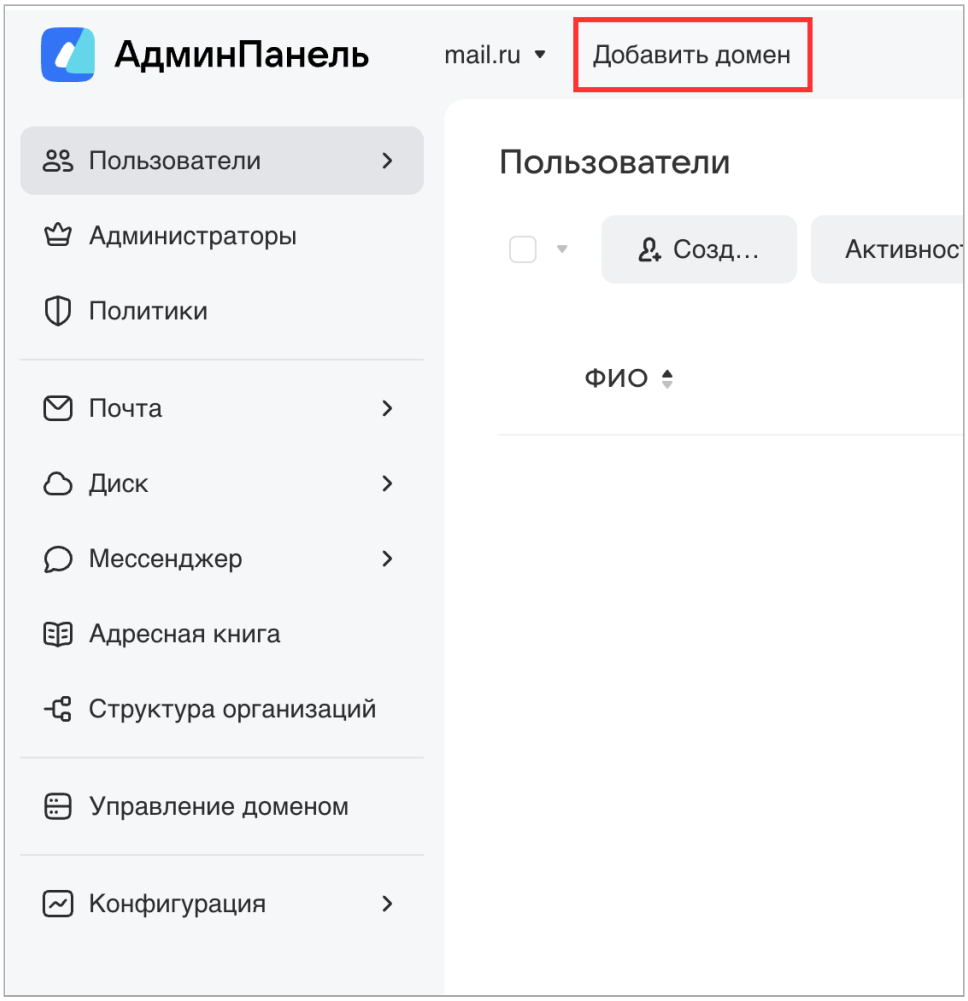
2. Выполните рестарт виртуальной машины:

```
reboot
```

Интеграция с Панелью администратора считается завершенной.

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
```

Технический писатель: Белова Ирина

23 марта 2026 г.