VK WorkSpace

Настройка интеграции с панелью администратора VK WorkSpace

Инструкция для администраторов

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

Оглавление

Назначение документа

В документе описана настройка интеграции VK Teams версии 24.5 и выше и панели администратора VK WorkSpace версии 1.23. Документ предназначен для использования администраторами организации.

Условно процесс настройки интеграции VK Teams с панелью администратора можно разделить на несколько шагов:

1. Выполните настройки на стороне VK Teams.
2. Разверните панель администратора VK WorkSpace и интегрируйте ее с VK Teams.
3. Настройте интеграцию панели администратора с ActiveDirectory.
4. Выключите синхронизацию пользователей через сервис Keycloak.

После настройки интеграции пользователи VK Teams синхронизируются с ActiveDirectory через панель администратора. Поэтому, если у вас настроена интеграция VK Teams с ActiveDirectory, настройте интеграцию панели администратора с ActiveDirectory и после этого удалите LDAP-подключение VK Teams.

Подробное описание шагов представлено ниже.

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

Дополнительная документация

Инструкция по установке VK Teams на одну виртуальную машину, Инструкция по установке кластера VK Teams

Инструкция по интеграции VK Teams 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.

Предварительные действия

1. Если у вас еще не установлен VK Teams, 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.
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.

Предварительные условия

1. Доступ к виртуальной машине, на которой установлен VK Teams.
2. Данные для разворачивания панели администратора VK WorkSpace (получите у представителя VK):
   - Ссылка на скачивание дистрибутива панели администратора VK WorkSpace.
   - Пароль от архива с дистрибутивом.
   - Лицензионный ключ.
3. Доступ к 25 порту, так как панель администратора VK WorkSpace использует протоколы SMTP, ESMTP.

Технические требования

Поддерживаемые операционные системы для установки панели администратора:

- Astra Linux SE Орел — версии 1.7.3.
- РЕД ОС — версии 7.3.2;

Версия ядра — от 5.15; 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.

Продуктивная версия панели администратора устанавливается на одну виртуальную машину со следующей конфигурацией:

- 32 vCPU.
- 128 GB RAM.
- 300 GB HDD/SSD.

> **Примечание**
>
> По техническим требованиям для распределенной инсталляции и по вопросам создания сайзинг-модели обращайтесь к сотрудникам или партнерам компании VK.

Таблица совместимости

Технология	Версия
VK Teams	не старше двух последних версий
Keycloak/OAuth	не старше версии 2.x
Kerberos	5
MySQL	8.0.22

1. Выполните настройки на стороне VK Teams

Шаг 1. Создайте токен biz-admin

1. На сервере VK Teams 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 VK Teams 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 VK Teams 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 VK Teams 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 VK Teams

1. На сервере VK Teams 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
```

Шаг 5. Настройте сервис Stentor

1. На сервере VK Teams 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 клиентском приложении VK Teams

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

1. На сервере VK Teams перейдите в конфигурационный файл **/usr/local/nginx-im/html/myteam/myteam-config.json**:

```
vim /usr/local/nginx-im/html/myteam/myteam-config.json
```

2. 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"
      },
    }
}
```

3. 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
        ]
    }
}
```

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

На сервере VK Teams выполните команду:

```
kubectl delete pod -n vkteams myteam-admin-<pod ID>
```

Актуальное значение pod ID можно получить с помощью команды:

```
kubectl get pods -A | grep 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

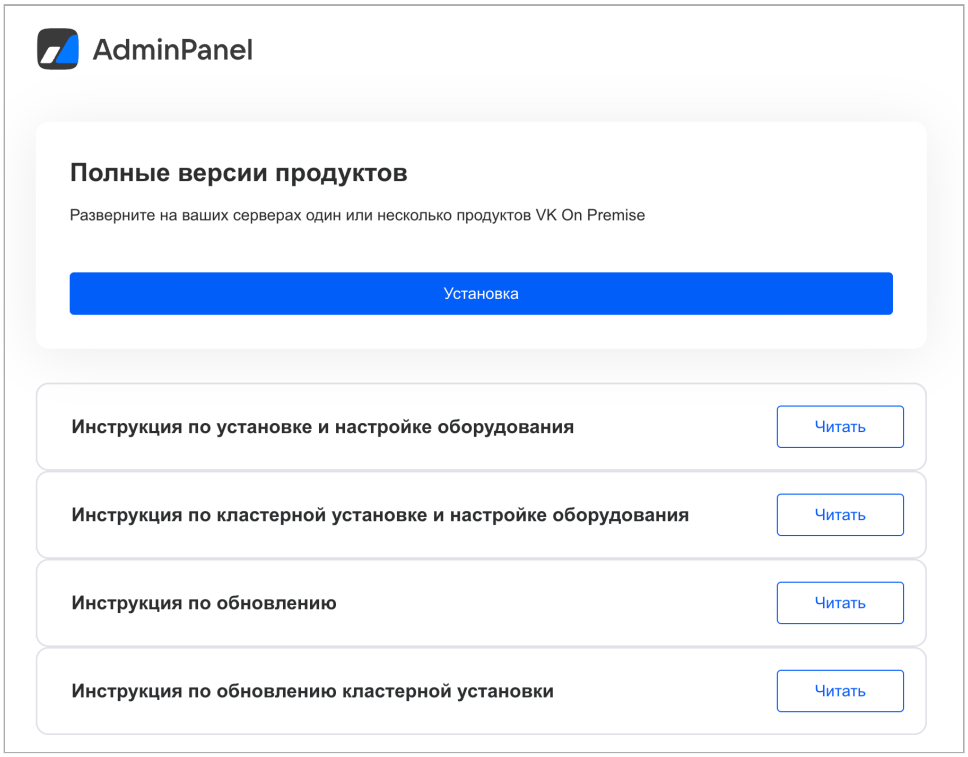
```
The authenticity of host 'localhost (::1)' can't be established.
ED25519 key fingerprint is SHA256:g8siO32KUsRU9oC/MHro9WaTNKj4R+DkmVnVa7QsYCo.
This key is not known by any other names
# Введите "yes" и нажмите Enter, чтобы подтвердить подключение
Are you sure you want to continue connecting (yes/no/[fingerprint])?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

> **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.

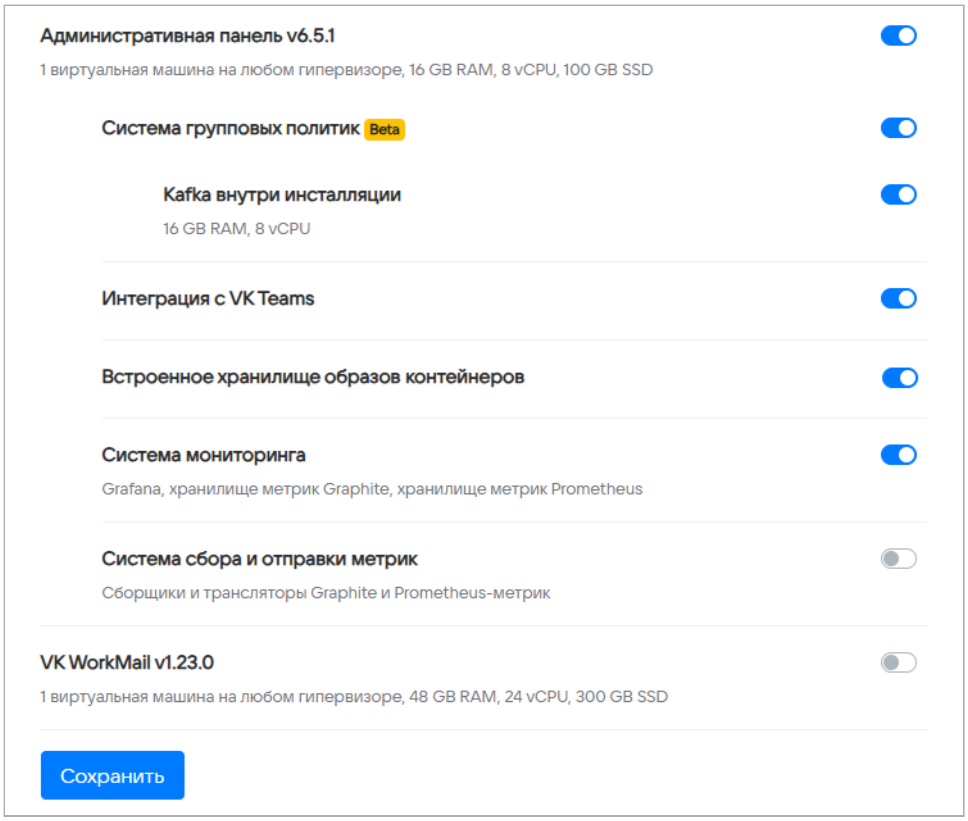
На стартовой странице нажмите на кнопку **Установка**.



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 VK Teams — обязательный компонент.

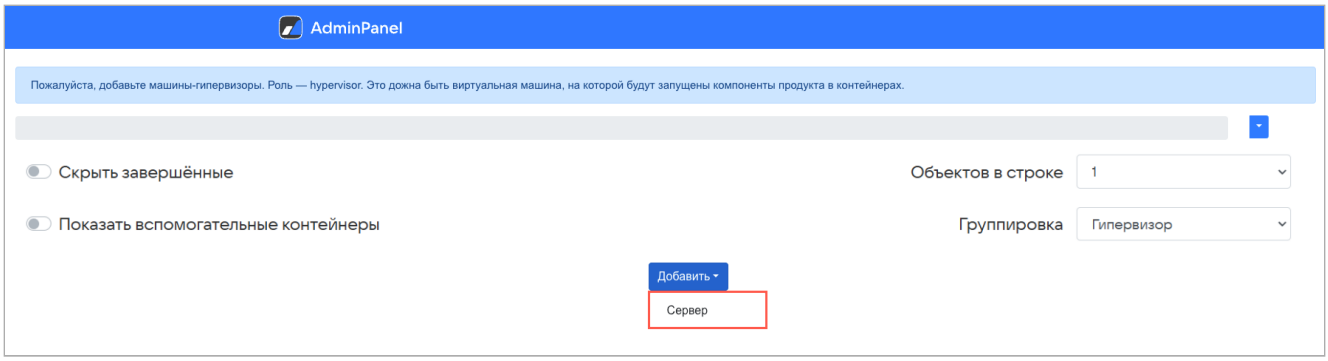
Система мониторинга — опциональный компонент. Не используется совместно с компонентом **Система сбора и отправки метрик**.

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

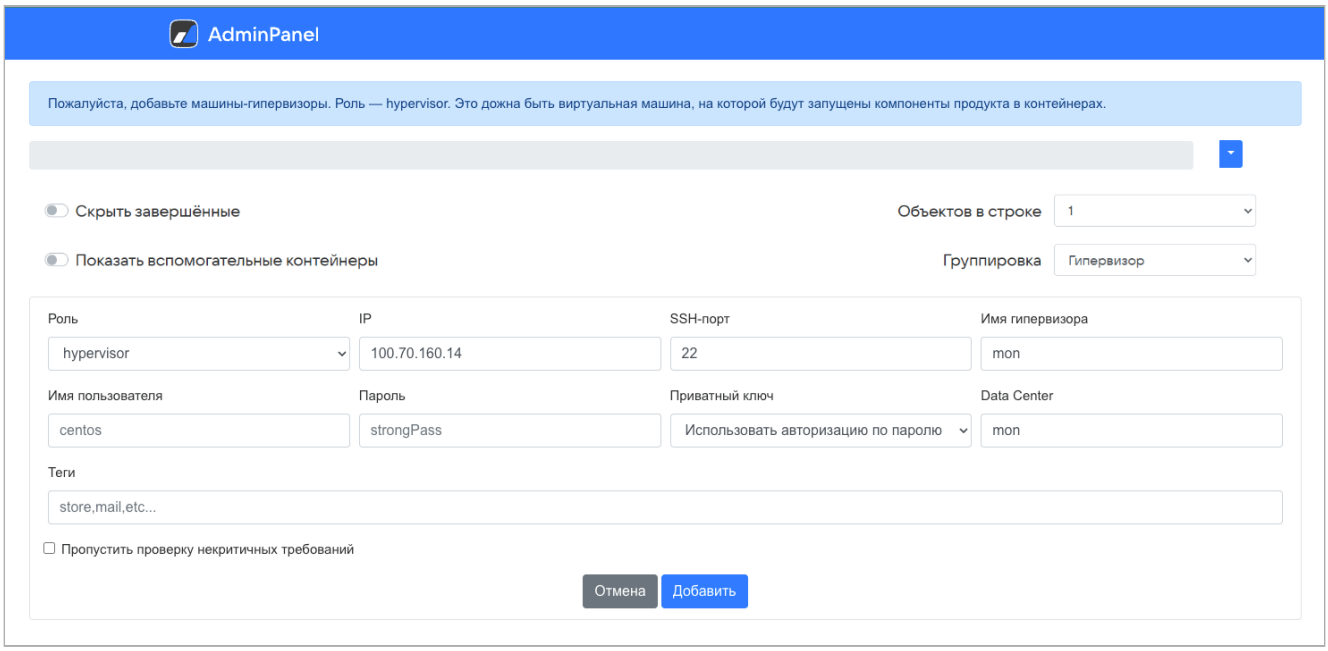
Нажмите на кнопку **Далее** внизу страницы, чтобы перейти к следующему шагу.

Шаг 6. Добавьте гипервизор

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



Откроется окно добавления гипервизора:

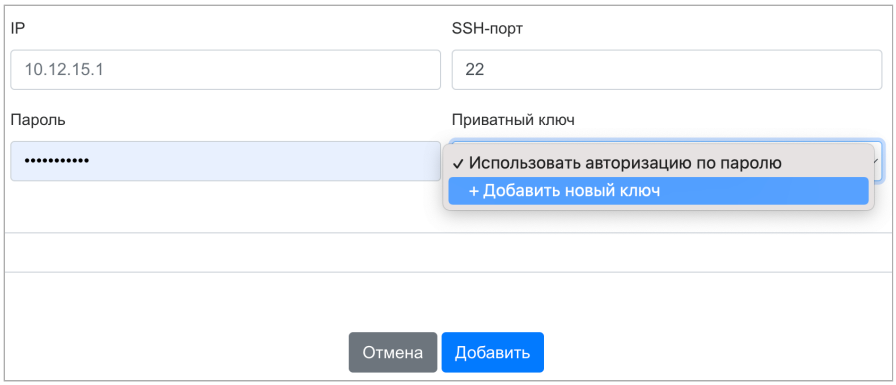


3. Заполните поля:

   - **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. 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**.

5. При необходимости настройте дополнительные поля:

   - **Data Center** — используется в кластерной установке, оставьте это поле пустым.
   - **Теги** — добавление тегов актуально только для кластерной установки, для моно-инсталляции создание тегов не требуется.
   - **Пропустить проверку некритичных требований** — если отметить чекбокс, будет пропущена проверка версии ядра и флагов процессора (sse2, avx). В большинстве случаев выбор чекбокса не требуется.

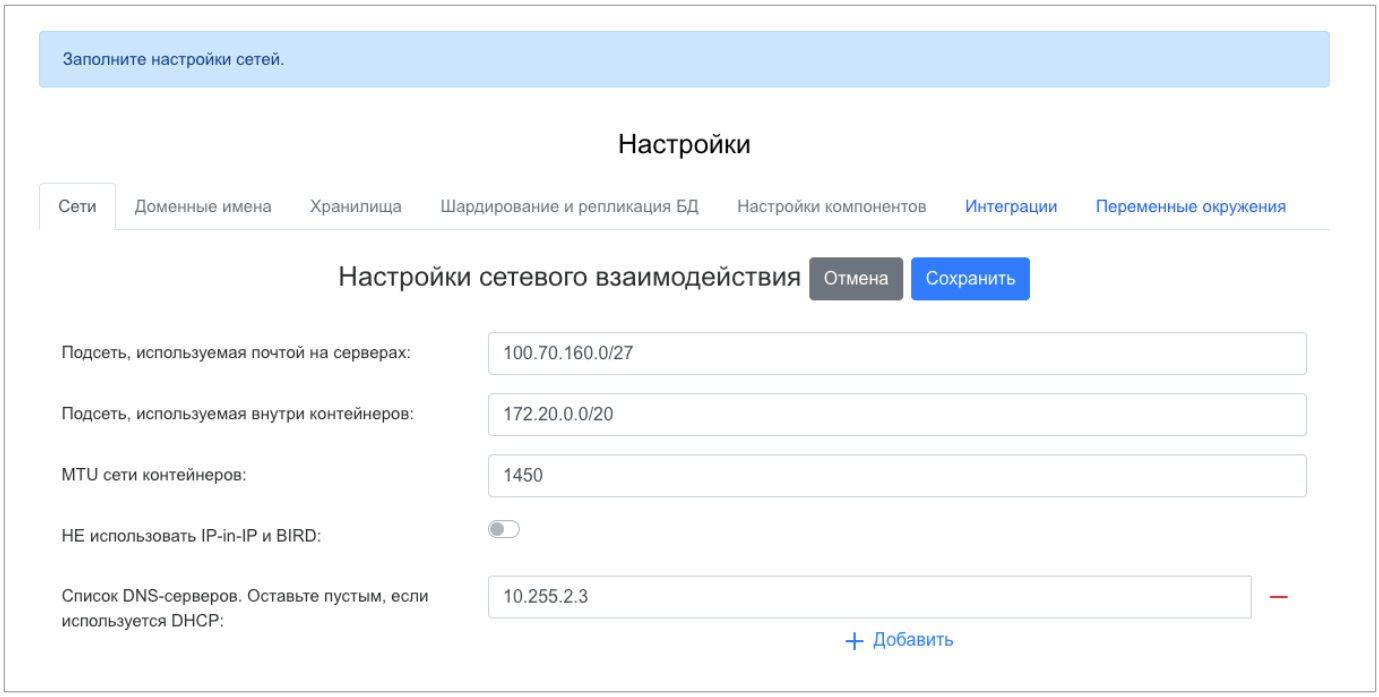
6. После заполнения полей нажмите на кнопку **Добавить** — гипервизор отобразится в веб-интерфейсе установщика.

> **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.

7. 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:

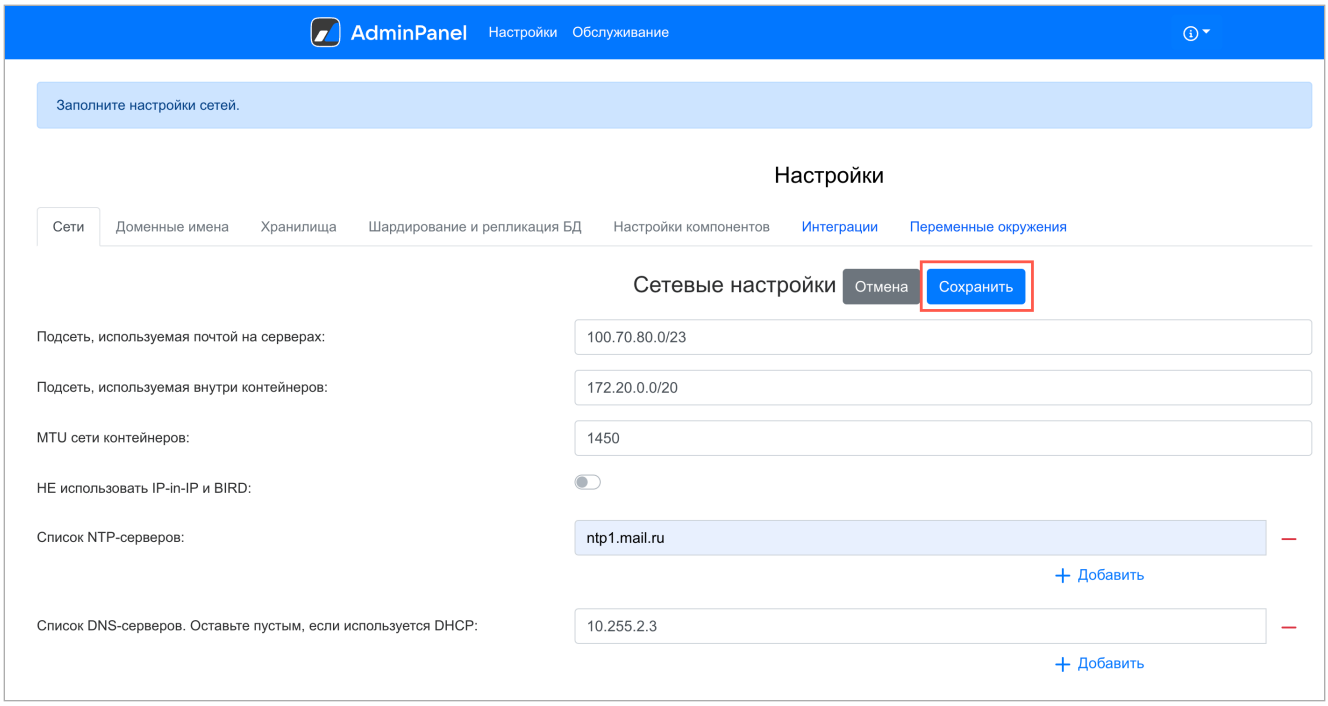
   - **Подсеть, используемая Панелью администратора на серверах** имеет доступ на 80 или 443 порт.
   - **Подсеть, используемая внутри контейнеров** полностью свободна, уникальна и принадлежит только панели администратора VK WorkSpace.

> **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. По умолчанию используется 20 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:

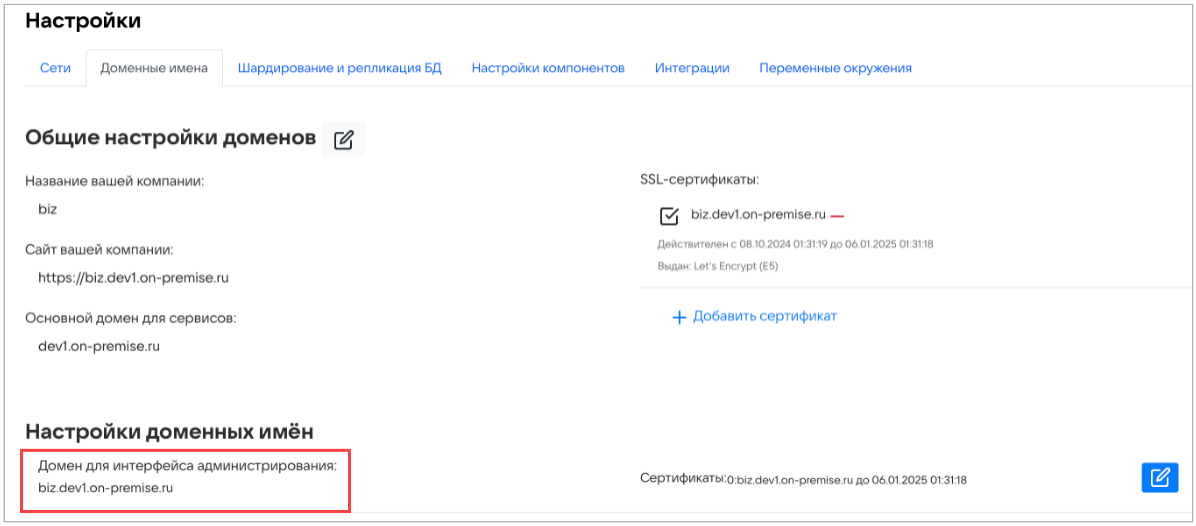


Шаг 8. Доменные имена

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`.

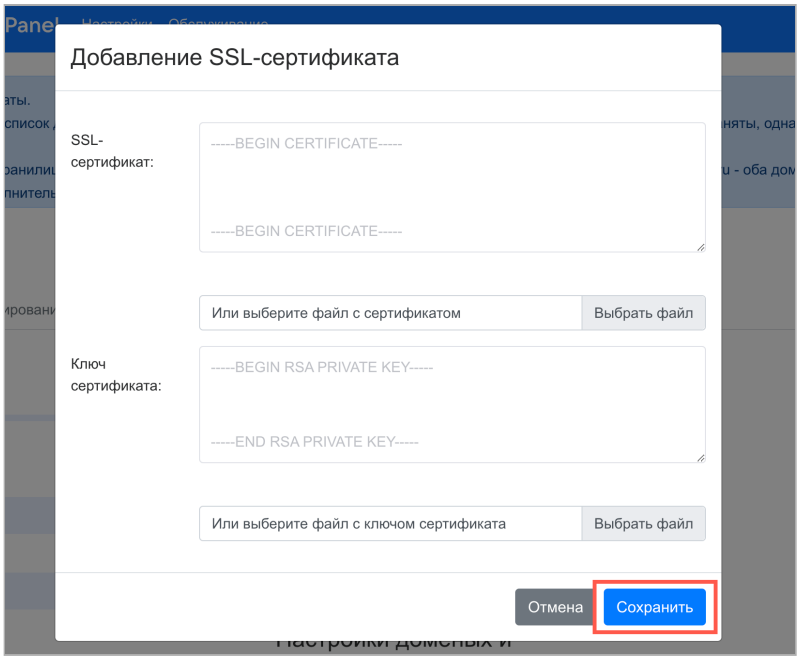
2. Нажмите на кнопку **Сохранить**.
3. Нажмите на кнопку **Добавить сертификат** под заголовком **SSL-сертификаты**.
4. В открывшейся форме введите сертификат и ключ. Их необходимо указать полностью, включая:

`-----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.

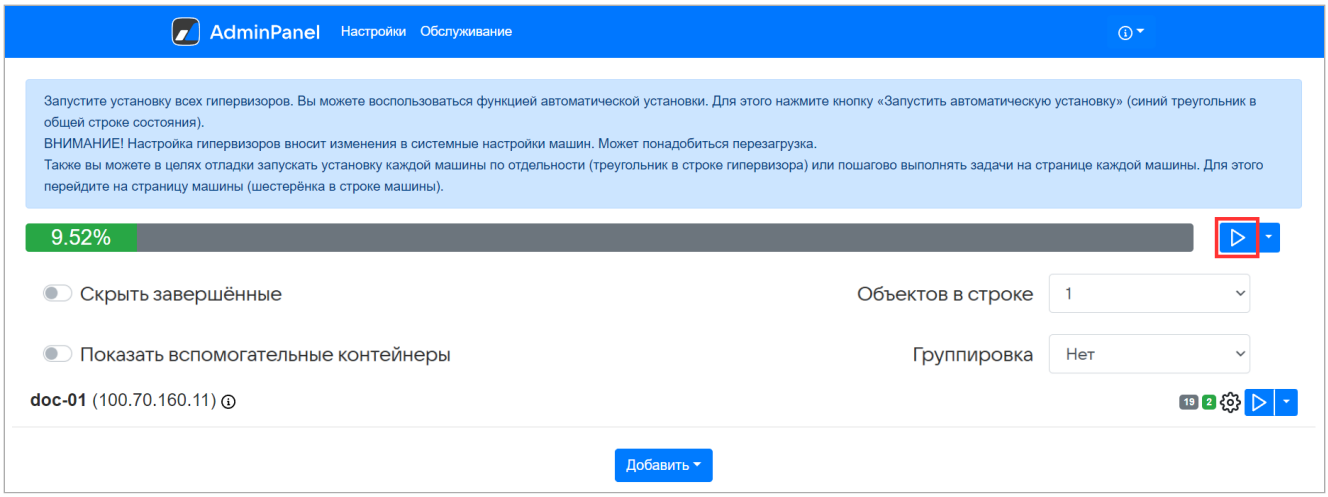
d. Кликните по кнопке **Сохранить**.

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

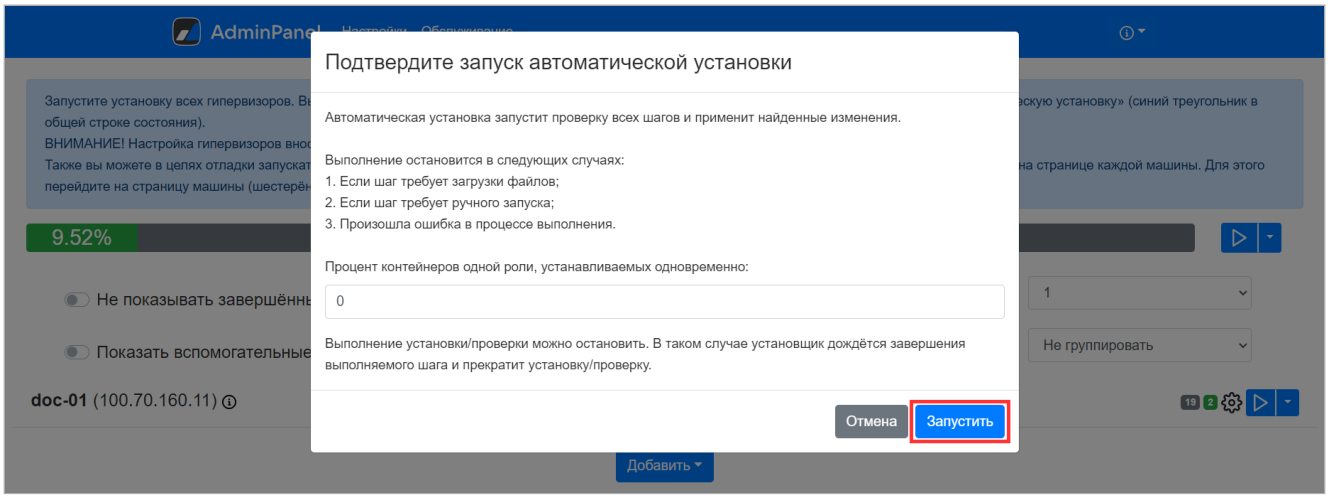
Если всё верно, в интерфейсе не будет отображаться ошибок и красной подсветки. Нажмите на зеленую кнопку **Далее** в правом верхнем углу.

Шаг 9. Запустите установку гипервизора

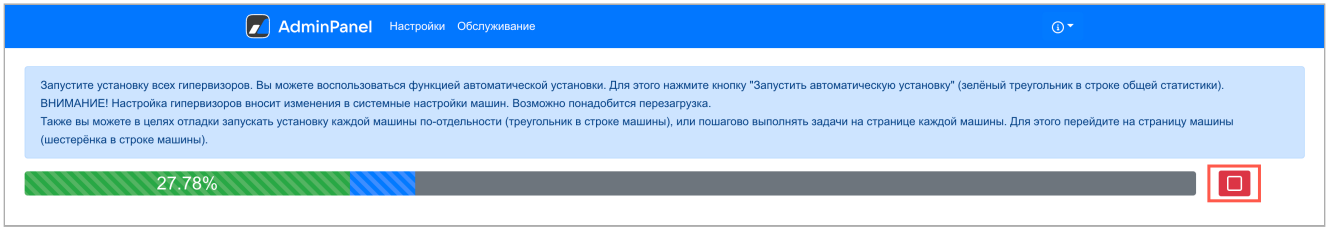
1. Нажмите на логотип **AdminPanel**, чтобы перейти к общей строке состояния.
2. Кликните по иконке  рядом с общей строкой состояния в верхней части экрана:



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



4. Дождитесь завершения установки гипервизора:

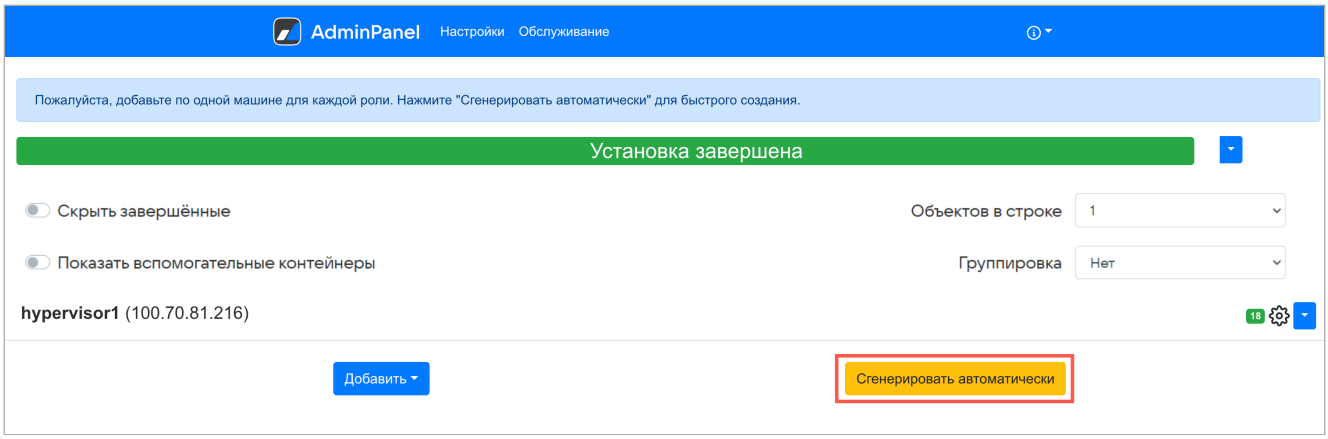


В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуется повторный запуск автоматической установки.

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

Шаг 10. Сгенерируйте контейнеры

1. В случае моноустановки нажмите на кнопку **Сгенерировать автоматически**, чтобы добавить по одному контейнеру для каждой роли:



В случае распределенной установки:

a. Нажмите на кнопку **Добавить** → **Несколько контейнеров**.

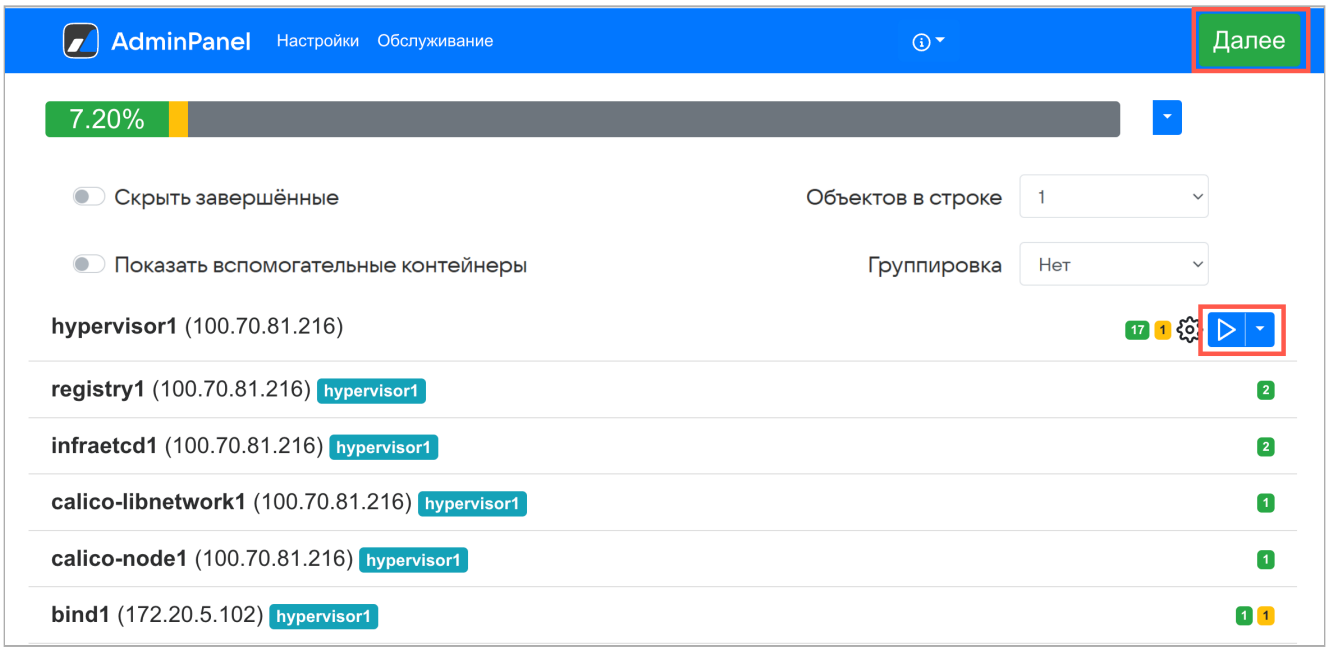
b. Установите фильтр **Установлено не более 0**.

c. Распределите недостающие контейнеры по гипервизорам с учетом дублируемости.

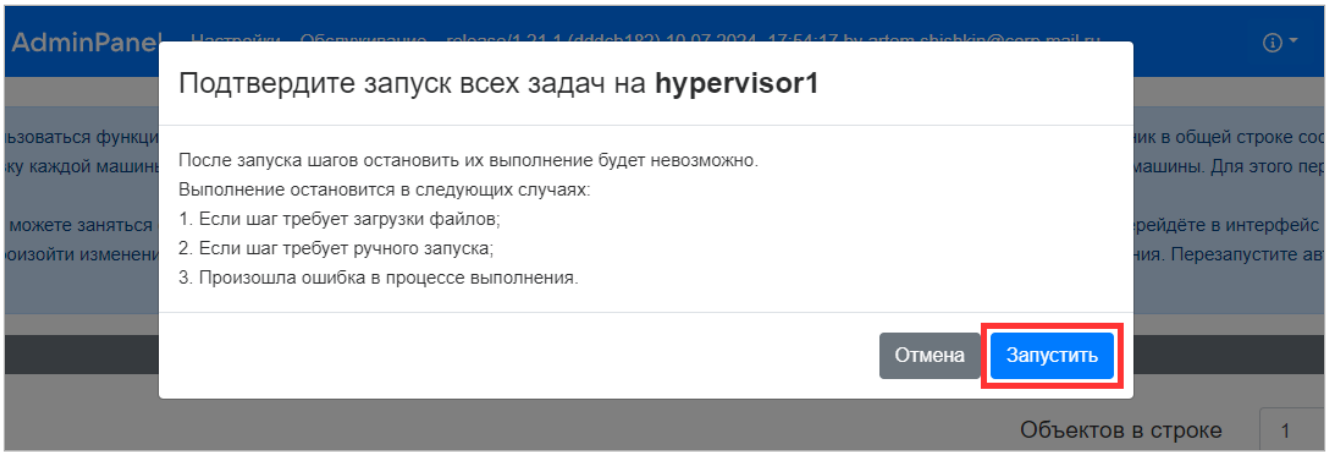
d. Нажмите на кнопку **Добавить**.

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 иконка  :



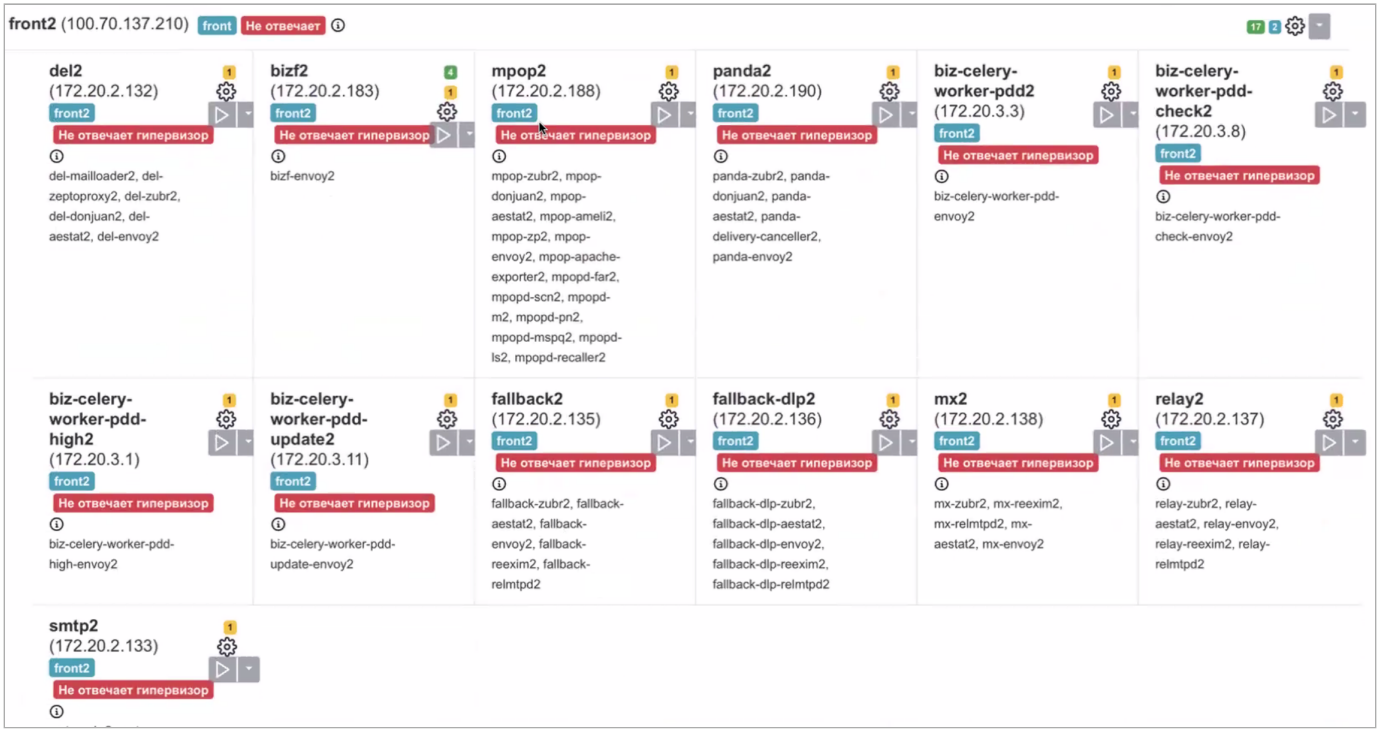
2. Кликните по иконке  напротив гипервизора.
3. Подтвердите автоматический запуск задач на гипервизоре, нажав на кнопку **Запустить**:



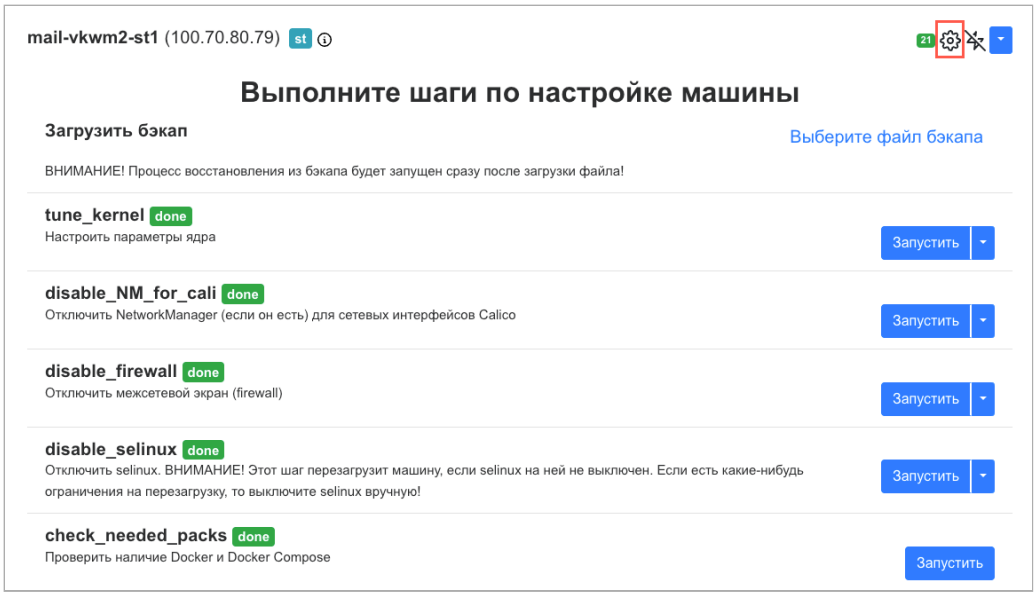
4. На генерацию требуется время. Подождите, пока исчезнет иконка  напротив гипервизора.
5. Нажмите на кнопку **Далее** для перехода к следующему шагу.

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

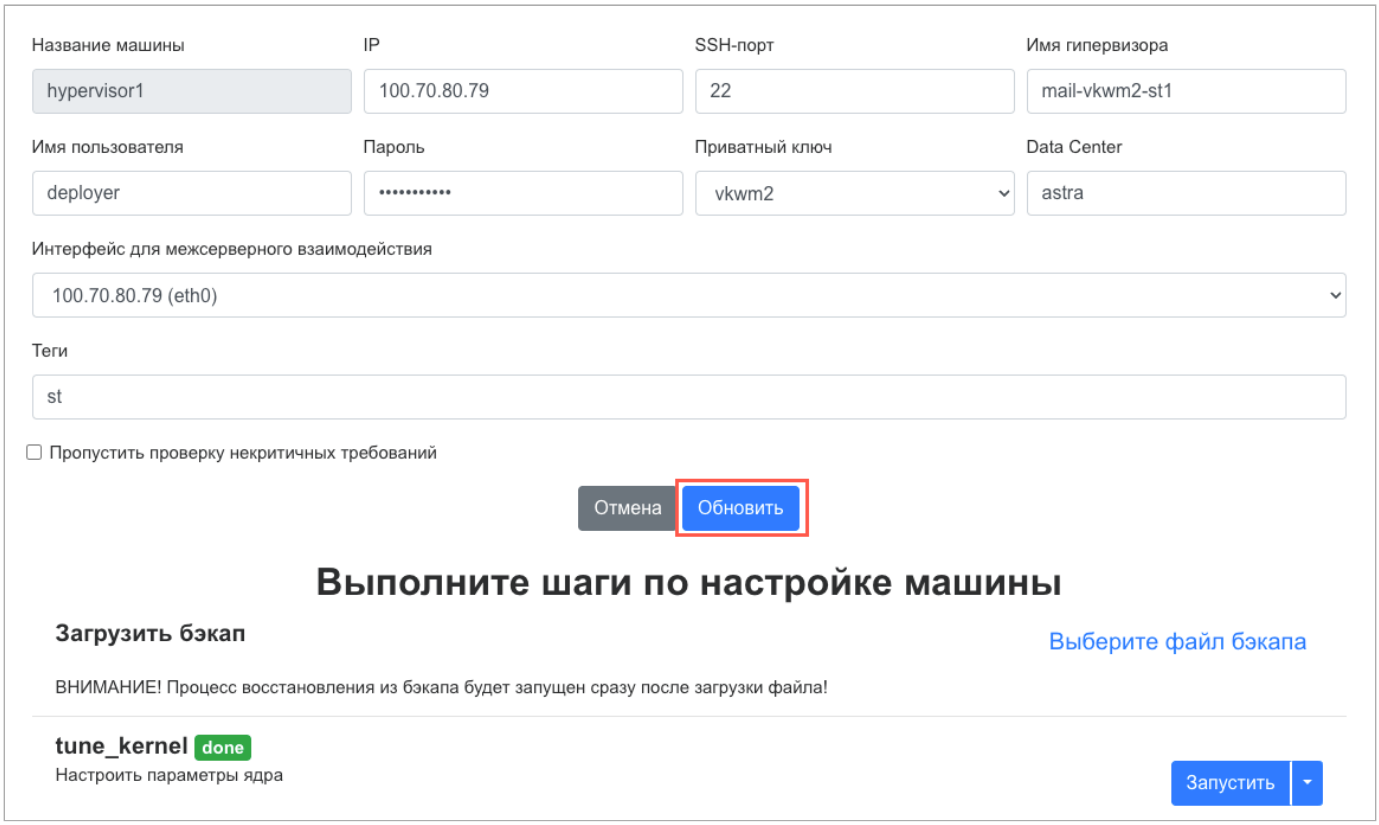
При появлении ошибок на гипервизоре на нем появится тег **Не отвечает**, а на контейнерах, относящихся к этому гипервизору — **Не отвечает гипервизор**.



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.



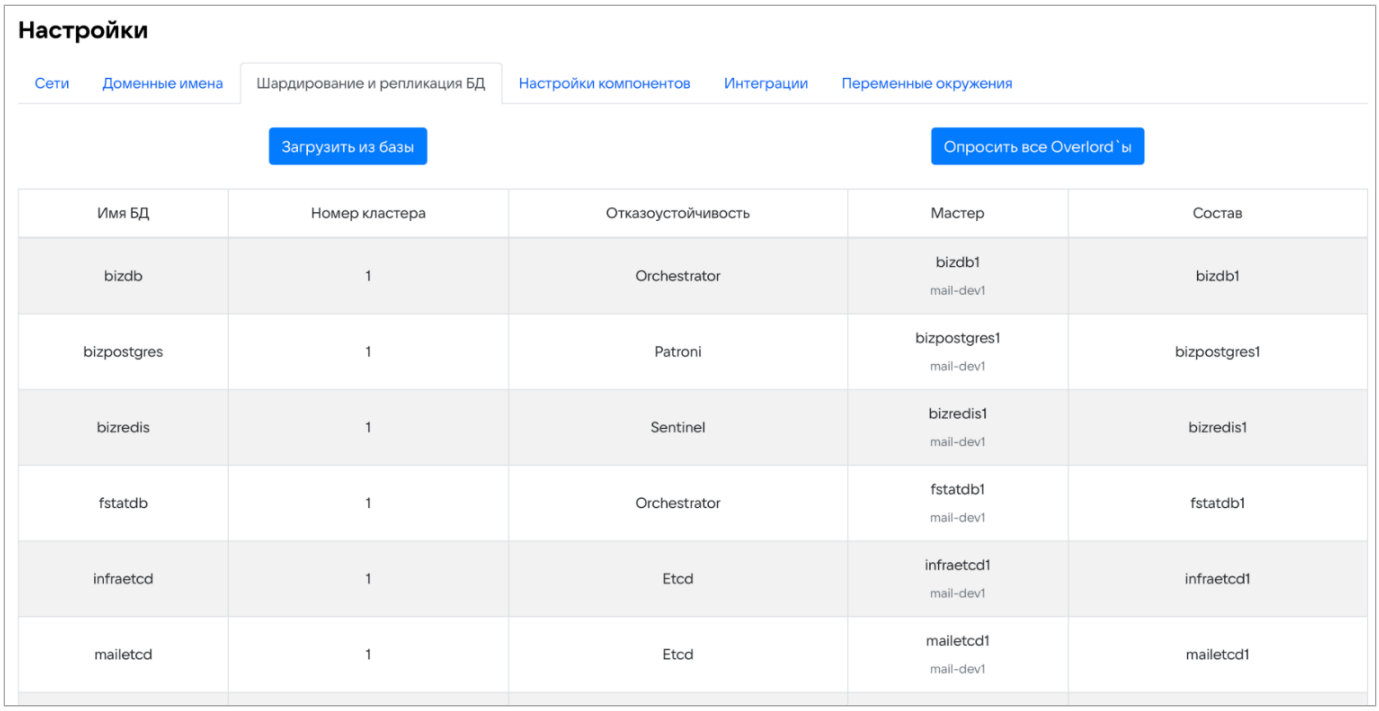
В окне настроек гипервизора нажмите на кнопку **Обновить**.



Повторно запустите автоматическую установку.

Шаг 11. Шардирование и репликация БД

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

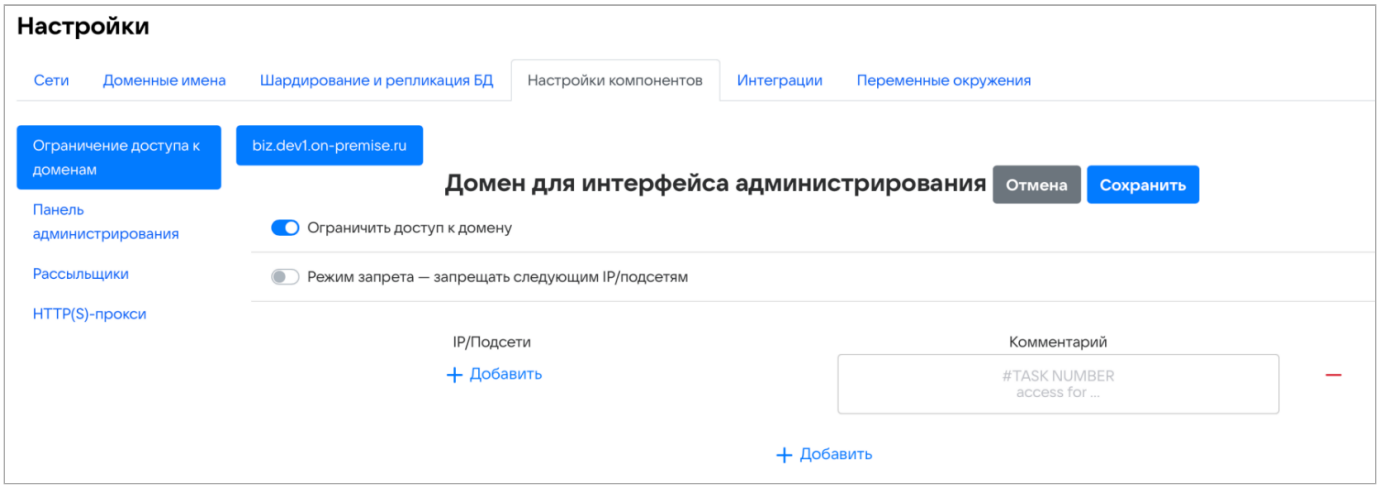


Шардирование (сегментирование) БД используется в кластерной установке для обеспечения отказоустойчивости и масштабируемости, в моноинсталляции не используется.

Шаг 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:



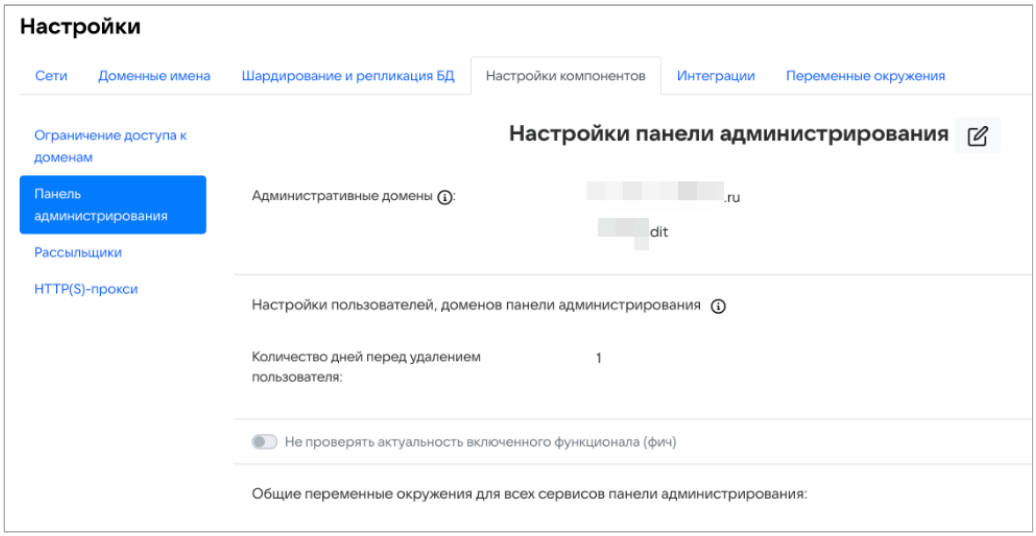
Ограничить доступ к домену — если включен только этот флаг, в поле ниже нужно будет ввести IP/подсети, которым будет **разрешен** доступ к домену. Также вы можете добавить комментарии, если это необходимо.

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 **AdminPanel**.

Панель администрирования

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

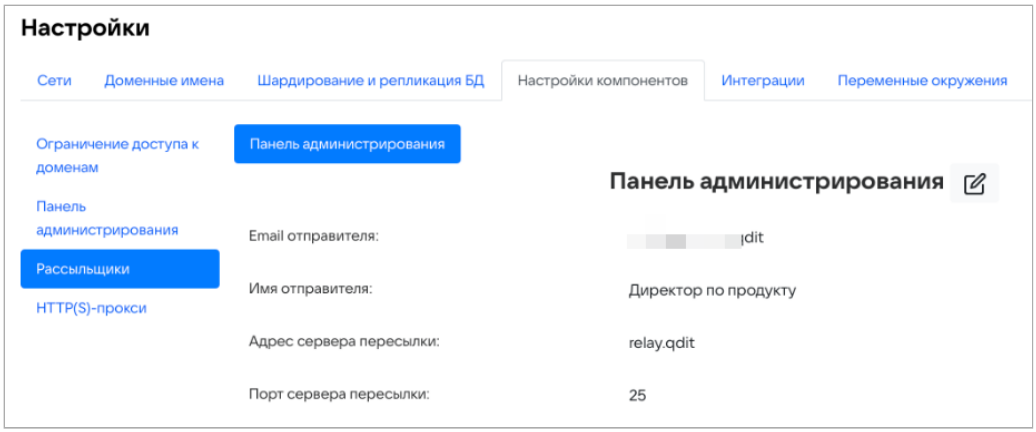


Количество дней перед удалением пользователя — количество дней, по прошествии которых пользователь будет удален из панели администратора VK WorkSpace. Изменение настройки по умолчанию актуально при одновременном использовании панели администратора VK WorkSpace с Active Directory. По умолчанию выставлен 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

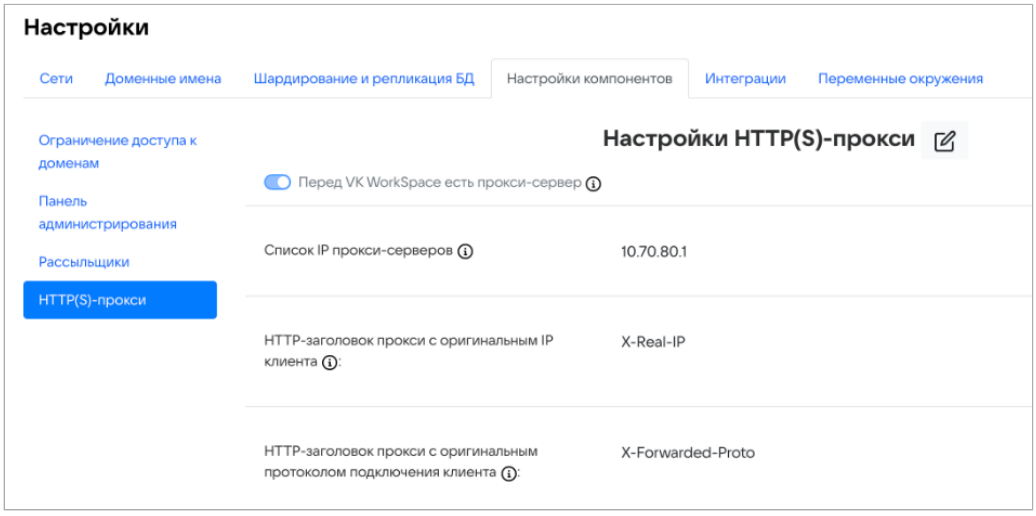
В разделе настраиваются служебные почтовые рассылки для внутренних пользователей. Чтобы перейти к настройкам, нажмите на иконку  .



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 VK Teams

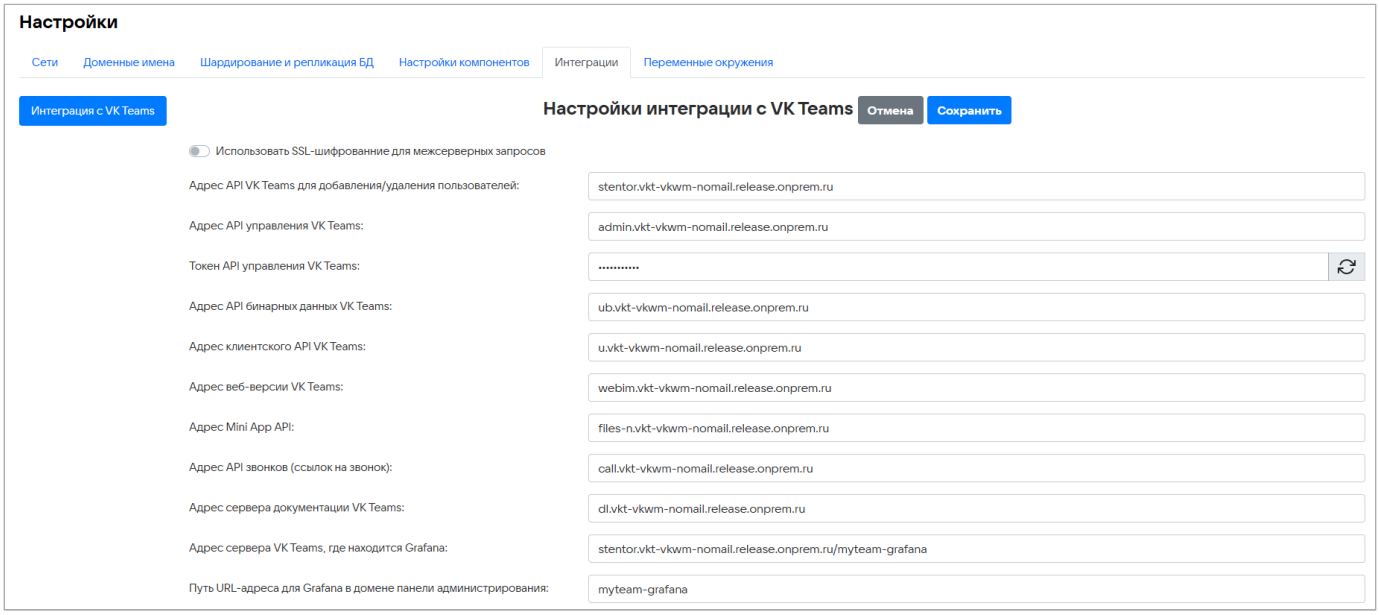
1. Перейдите на вкладку **Интеграции** → **Интеграция с VK Teams**.
2. Включите флаг **Использовать SSL шифрование для межсерверных запросов**.
3. Заполните все поля:

Название поля	**Значение**
Адрес API VK Teams для добавления/удаления пользователей	stentor.<домен VK Teams>.ru
Адрес API управления VK Teams	admin.<домен VK Teams>
Токен API управления VK Teams	Нажмите на серую кнопку в поле, чтобы сгенерировать токен. Этот токен понадобится вам ниже.
Адрес API бинарных данных VK Teams	ub.<домен VK Teams>
Адрес клиентского API VK Teams	u.<домен VK Teams>
Адрес веб-версии VK Teams	webim.<домен VK Teams>
Адрес Mini App API	files-n.<домен VK Teams>
Адрес API звонков (ссылок на звонок)	call.<домен VK Teams>
Адрес сервера документации VK Teams	Укажите адрес портала организации, по которому доступно клиентское приложение и инструкции VK Teams, например: dl.<домен VK Teams>
Адрес сервера VK Teams, где находится Grafana	Для версии VK Teams 24.2 и ниже: stentor.<домен VK Teams>/myteam-grafana Начиная с версии VK Teams 24.3: stentor.<домен VK Teams>/grafana
Путь URL-адреса для Grafana в домене панели администрирования	myteam-grafana
	Значение key из шага Создайте токен biz-admin

Название поля	Значение
Токен VK Teams для получения структуры организаций в панели администрирования	
Пользователь ClickHouse VK Teams	biz
Пароль пользователя ClickHouse VK Teams	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 VK Teams (для ACL в SWA)	<IP-адрес сервера VK Teams>

Примечание

На скриншоте ниже в качестве домена VK Teams используется vkt-02.on-premise.ru. Используйте ваш домен VK Teams.



Шаг 14. Укажите токен на сервере VK Teams

Скорректируйте конфигурацию etcd:

1. Пропишите в etcd VK Teams токен API управления VK Teams, 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 VK Teams.

2. Укажите подсети для сетевого соединения панели администратора и VK Teams:

```
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:

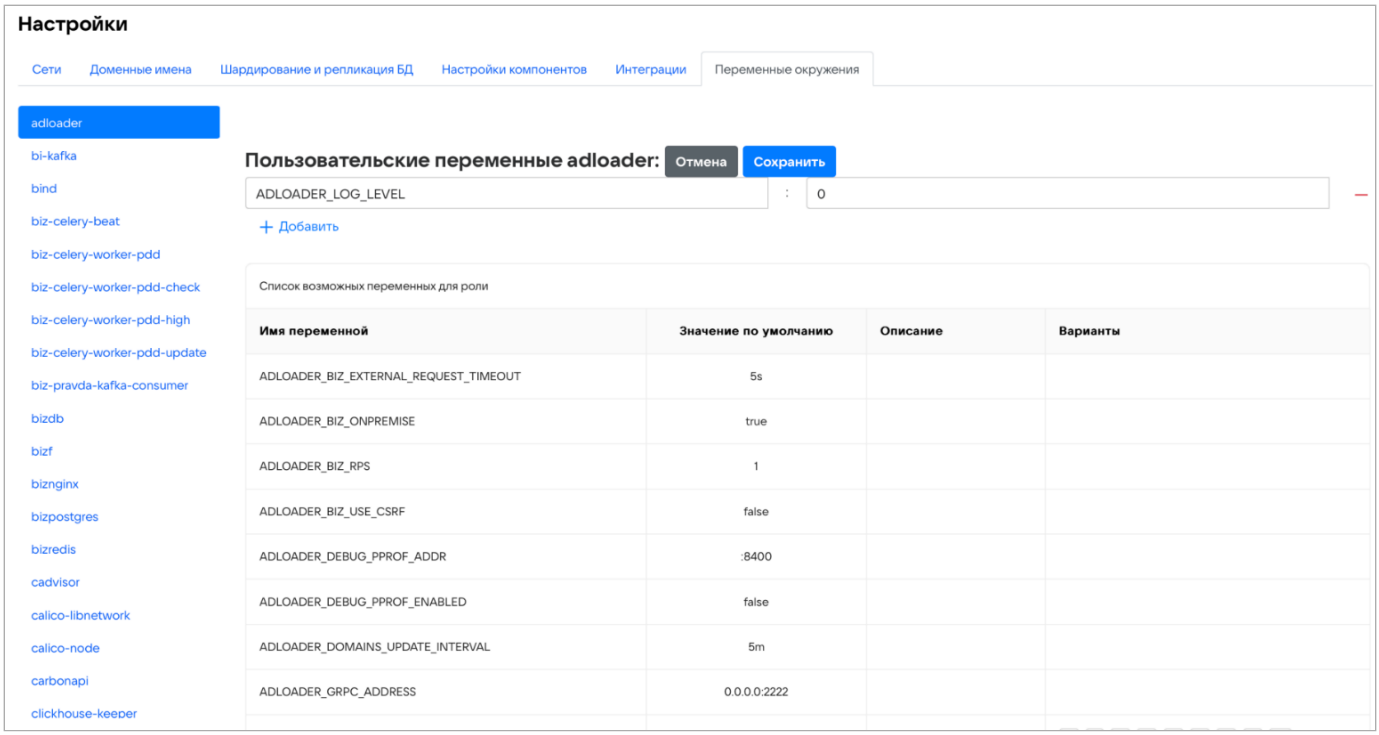
```
reboot
```

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

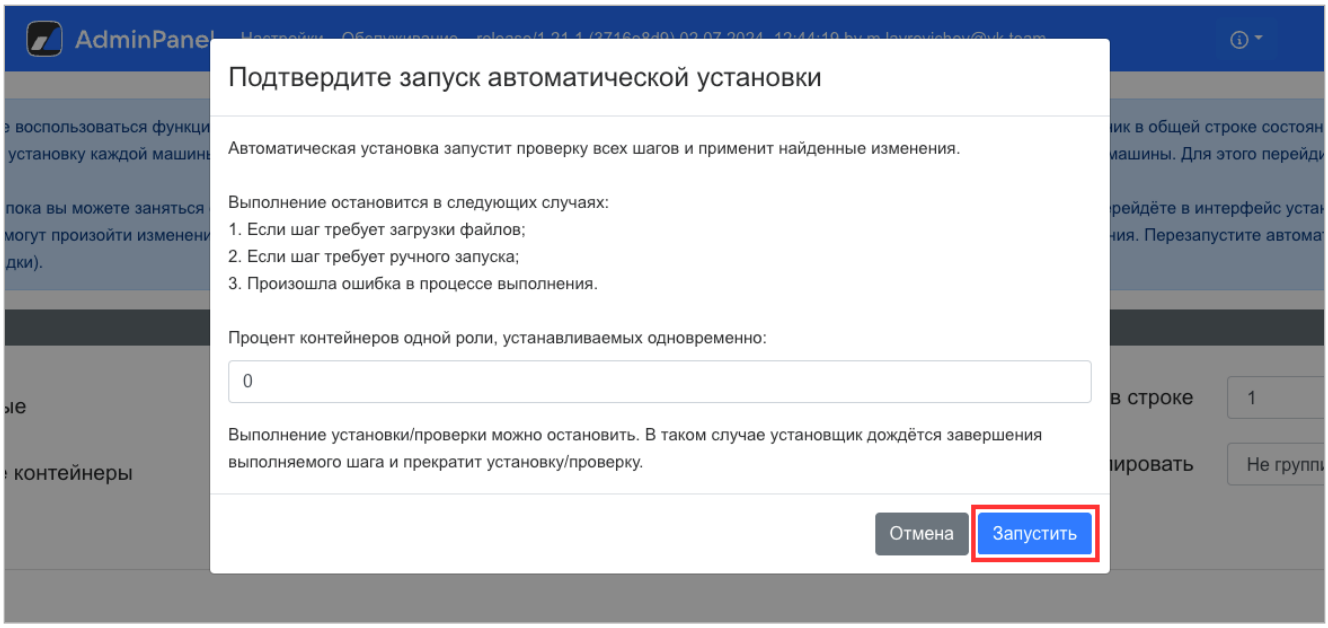
Настройка переменных окружения возможна только после консультации с представителем VK.

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**.

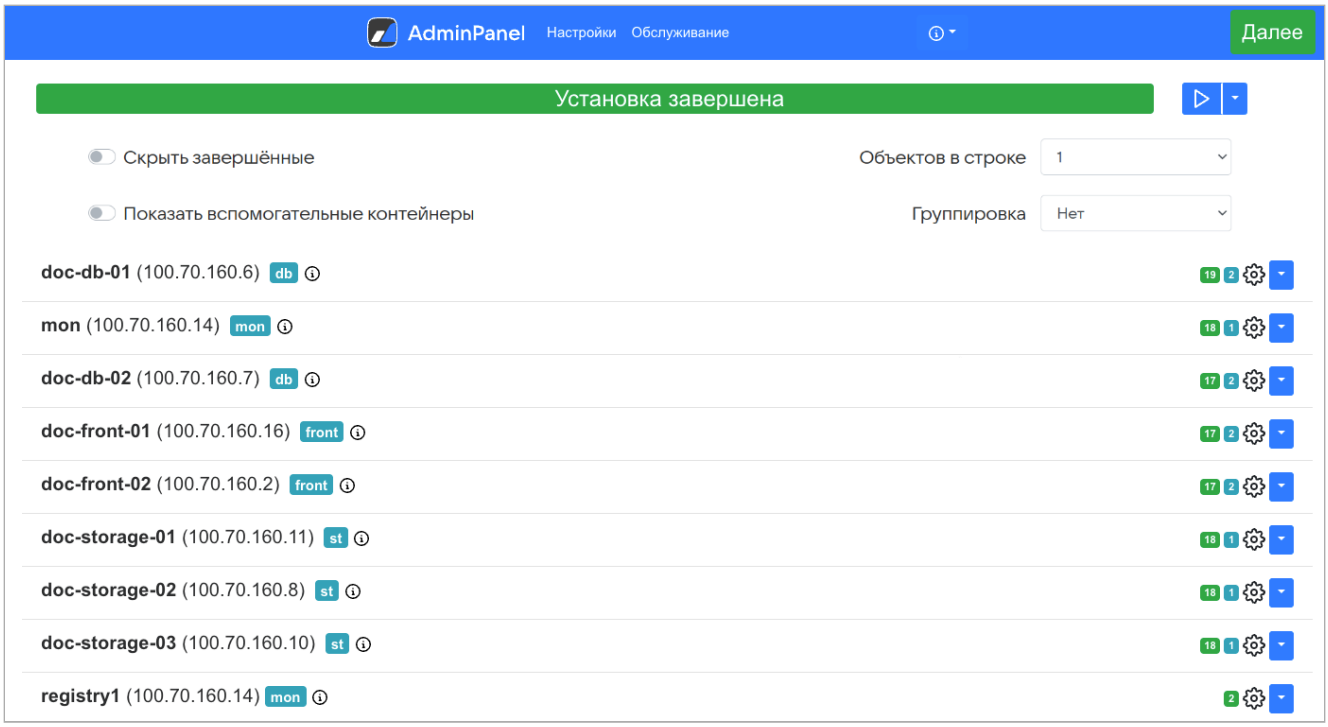
Если в процессе установки и настройки системы происходят изменения конфигурации, некоторые задачи могут потребовать повторного выполнения.

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

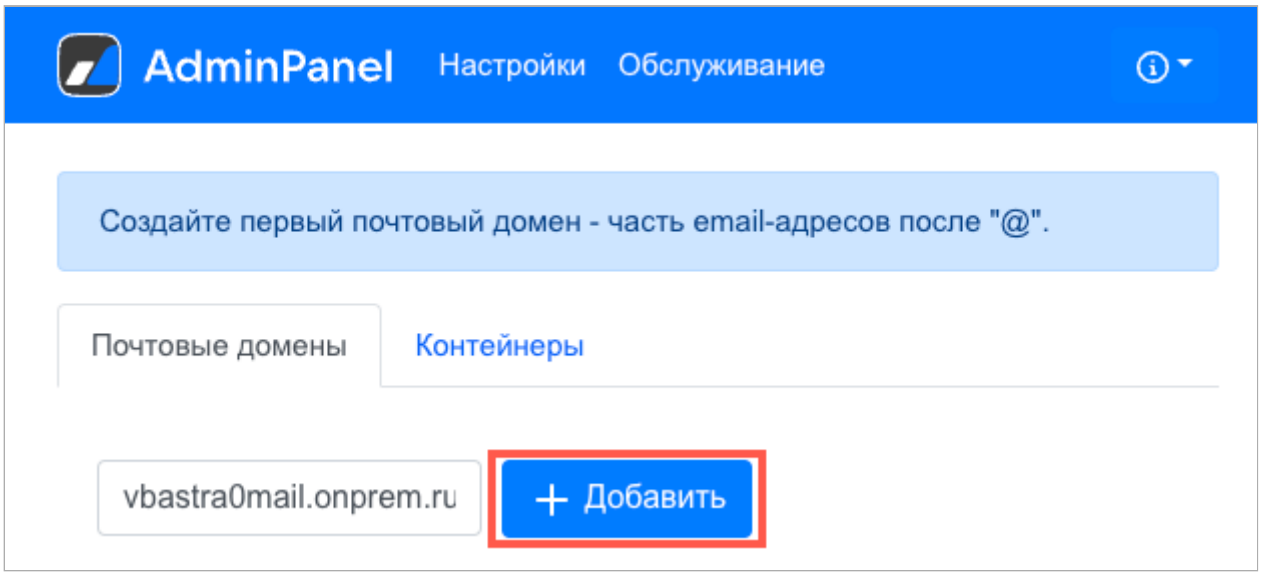
Шаг 17. Инициализируйте домен и войдите в панель администратора

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.

Откроется новая вкладка, на которой необходимо авторизоваться:

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

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 массового добавления пользователей в панели администратора.
2. После подключения функциональности импортируйте пользователей при помощи CSV-файла (см. инструкцию).

> **Важно**
>
> Списки пользователей в VK Teams 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 VK Teams с ActiveDirectory, удалите LDAP-подключение (см. ниже).

4. Удалите LDAP-подключение VK Teams

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

1. Чтобы удалить LDAP-подключение, на сервере VK Teams 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
   ```

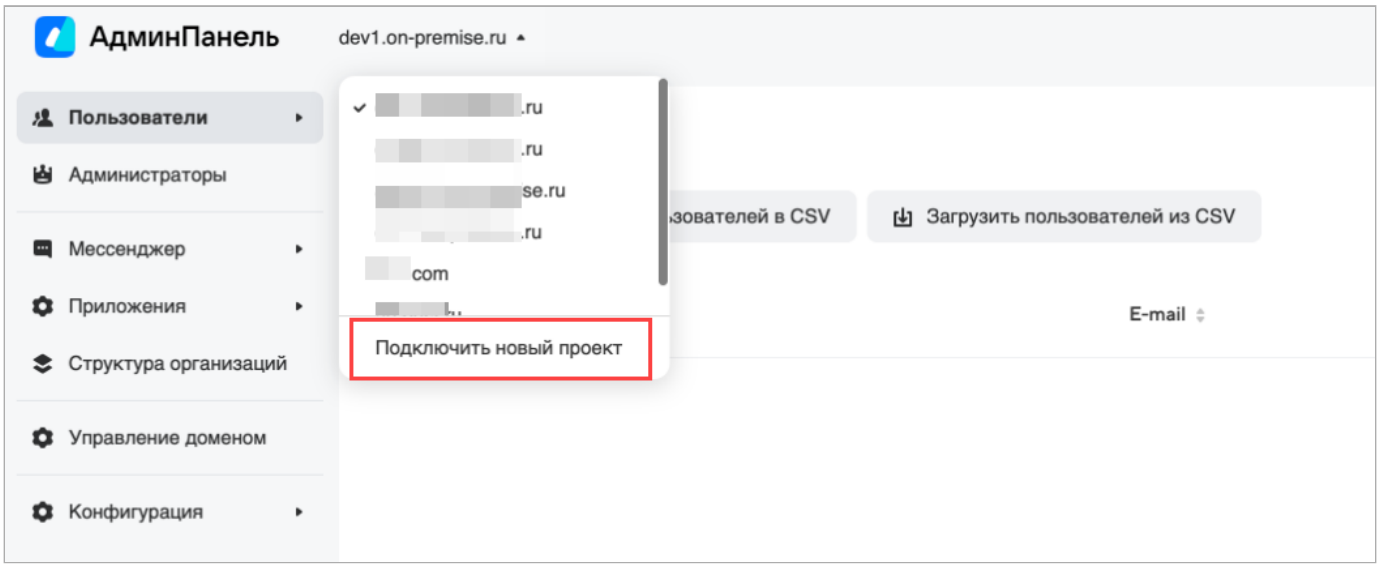
2. Выполните рестарт виртуальной машины:

   ```
   reboot
   ```

Интеграция с панелью администратора считается завершенной.

Добавление дополнительных доменов

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



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: Белова Ирина

19 декабря 2024 г.