

# Диск VK WorkSpace

Установка Диска 25.4 на одну машину

# Оглавление

---

Назначение документа	4
Требования к администраторам	4
Дополнительная документация	4
Технические требования	4
Как использовать системы виртуализации	5
Пример настройки параметров ОС	6
Требования к ресурсам сервера	7
Таблица совместимости	8
Предварительные условия для установки	8
Как работать с Wildcard-сертификатами	9
Какие протоколы использует Диск	10
Обязательные предварительные действия	10
Настройте ротацию логов в journald	10
Создание DNS-записей	10
Дисковое пространство	13
Подключение дисков	13
Этапы установки	14
Действия в командной строке на сервере	14
Шаг 1. Создание пользователя deployer	14
Шаг 2. Распаковка дистрибутива	16
Шаг 3. Разрешить Port Forwarding	17
Шаг 4. Запуск установщика как сервиса	17
Действия в веб-интерфейсе установщика	19
Шаг 1. Выбор варианта установки	19
Шаг 2. Выбор продуктов и опций	20
Шаг 3. Добавление лицензионного ключа	22
Шаг 4. Добавление гипервизора	23
Шаг 5. Сетевые настройки	25

Шаг 6. Доменные имена	26
Добавление SSL-сертификатов	27
Шаг 7. Запуск установки гипервизора	29
Шаг 8. Генерация контейнеров	30
Шаг 9. Хранилища	33
Шаг 10. Шардирование и репликация БД	34
Шаг 11. Настройка компонентов	34
Ограничение доступа к доменам	34
Панель администрирования	35
Рассыльщики	36
Система учета действий пользователей	37
Мониторинг	38
Настройки HTTP(S)-прокси	40
Шаг 12. Интеграции	41
Настройка интеграции с внешней почтой	41
Настройки системы BI-аналитики	41
Шаг 13. Укажите переменные окружения	42
Шаг 14. Запустите установку всех машин	43
Шаг 15. Инициализируйте домен и войдите в Панель администратора	44
Добавление дополнительных доменов	46
Логи и полезные команды	46

# Назначение документа

---

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

## Требования к администраторам

---

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

## Дополнительная документация

---

[Что делать, если при входе в панель администратора появляется ошибка «Неверный пароль»](#)

[Как обновить лицензионный ключ](#)

[Настройка интеграции с Active Directory](#)

## Технические требования

---

Поддерживаемые операционные системы для установки Диска:

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

Архитектура системы — **x86\_64**.

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

#### **Внимание**

Чтобы Диск VK WorkSpace работал корректно, нужно установить оперативное обновление ядра ОС указанной выше версии. Версия должна быть актуальной на момент установки.

## Как использовать системы виртуализации

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

### **vCPU**

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

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

### **RAM**

Не назначайте суммарную vRAM выше физической RAM хоста.

### **Механизмы экономии памяти**

Не включайте механизмы ballooning и сжатия памяти.

### **swap**

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

### **Резервирования ресурсов виртуальных машин**

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

### **Хранилище**

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

# Пример настройки параметров ОС

## Важно

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

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

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

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

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

## РЕД ОС

### Дополнительные настройки для сертифицированной РЕД ОС 7.3

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

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

До установки Диска VK WorkSpace:

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`

Установить пакеты можно с помощью команды:

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

## MosOS

### Дополнительные настройки для MosOS Arbat

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

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

## Требования к ресурсам сервера

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

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



### Рекомендация

Используйте процессоры Intel Xeon Gold 6140 и новее.

## Таблица совместимости

Технология	Версия
Мессенджер и ВКС	не старше двух последних версий
MS Exchange Server	2013/2016
Keycloak	17, с использованием OAuth 2.0
Kerberos	5
P7-Офис	ee-2024.1.1.375.rev1

### Примечание

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

## Предварительные условия для установки

Представители VK предоставили вам следующие данные:

- Ссылку на скачивание дистрибутива Диска 25.4.
- Пароль от архива с дистрибутивом.
- Лицензионный ключ.
- Комплект документации.

Также вам потребуется:

- Набор DNS-записей: A, CNAME, MX, SPF, TXT, NS.
- Поддержка процессорами набора инструкций 3DNow, ADX, AES, AVX, AVX2, BMI, BMI2, CMOV, MMX, MODE64, NOT64BITMODE, NOVLX, PCLMUL, SHA, SSE1, SSE2, SSE41, SSE42, SSSE3 и XOP.
- DKIM-подпись с селекторами для каждого домена (или несколько DKIM с разными селекторами для одного домена).
- Доступ к серверу по SSH с правами администратора (вход по ключу или по паролю).
- Локальная сеть 1 GbE или 10 GbE.
- Отключить swap.
- Сертификаты SSL для каждого CNAME или Wildcard-сертификат для домена.

- Доступ к портам: 25, 80, 143, 443, 465, 993, 1025.
- Доступ к административным портам: 22, 8888\*.
- tar.
- Утилита для распаковки zip-архивов, например 7zip или unzip.
- Active Directory или другая служба каталогов, работающая по протоколу LDAP.

#### **Внимание**

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

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

#### **Информация**

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

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

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

## Как работать с Wildcard-сертификатами

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

- `*.disk.onprem.ru`
- `*.cloud.disk.onprem.ru`
- `*.disk-st.onprem.ru`

# Какие протоколы использует Диск

- **HTTPS** для доступа к веб-интерфейсу Диска с использованием **TLS**.
- **CalDAV** для синхронизации календаря.
- **CardDAV** для синхронизации и управления контактами.
- **WebDAV** для работы с Диском.
- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента.
- **IP in IP** — протокол туннелирования IP.

## Обязательные предварительные действия

### Настройте ротацию логов в journald

Выполните шаги из инструкции [Как настроить ротацию логов в journald](#).

### Создание DNS-записей

Для работы Диска вам нужны:

- Два основных домена: для Диска и для хранилищ.
- Набор A- или CNAME-записей.

#### Примечание

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

Для примера в документе будут использоваться следующие DNS-записи:

- **Домен для сервисов Диска** — `disk.onprem.ru`. При создании домена рекомендуется соблюдение структуры: `***disk.***.***` или `***disk.***`.
- **Домен для облачных хранилищ** — `disk-st.onprem.ru`. Пример структуры: `***st.***.***` или `***cloud.***`.

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

## **Внимание**

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

Далее в таблицах представлен список A- или CNAME-записей, которые нужно создать перед установкой сервиса Диск. Домены из таблиц должны являться поддоменами для двух основных.

### **Для Диска:**

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

Назначение домена	Имя домена	Пример
Веб-интерфейс авторизации	account	account.disk.onprem.ru
Доменная авторизация (внутренних запросов браузера)	auth	auth.disk.onprem.ru
Интерфейс администрирования	biz	biz.disk.onprem.ru
Капча	c	c.disk.onprem.ru
VK WorkDisk	cloud	cloud.disk.onprem.ru
Загрузка файлов в VK WorkDisk	cld-uploader.cloud	cld-uploader.cloud.disk.onprem.ru
Скачивание файлов в веб-интерфейсе VK WorkDisk	cloclo.cloud	cloclo.cloud.disk.onprem.ru
Загрузка файлов в VK WorkDisk	cloclo-upload.cloud	cloclo-upload.cloud.disk.onprem.ru
Интеграция с API VK WorkDisk	openapi.cloud	openapi.cloud.disk.onprem.ru
Загрузка файлов в публичные папки в VK WorkDisk	pu.cloud	pu.cloud.disk.onprem.ru
Портальная авторизация VK WorkDisk	sdc.cloud	sdc.cloud.disk.onprem.ru
	uploader.e	uploader.e.disk.onprem.ru

Назначение домена	Имя домена	Пример
Загрузка больших почтовых вложений в VK WorkDisk		
Превью файлов в VK WorkDisk	thumb.cloud	thumb.cloud.disk.onprem.ru
Сервис аватарок	filin	filin.disk.onprem.ru
Исполняемые статические данные	imgs	imgs.disk.onprem.ru
OAuth2-авторизация	o2	o2.disk.onprem.ru
Общепортальные сервисы авторизации	portal	portal.disk.onprem.ru
Сервер авторизации (межсерверные запросы)	swa	swa.disk.onprem.ru
Webdav	webdav.cloud	webdav.cloud.disk.onprem.ru

#### Для хранилищ:

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

Назначение домена	Имя домена	Пример
Защита от XSS-атак при скачивании файлов из VK WorkDisk	cloclo	cloclo.disk-st.onprem.ru
Скачивание больших почтовых вложений из VK WorkDisk	cloclo-stock	cloclo-stock.disk-st.onprem.ru
Распаковка архивов в интерфейсе VK WorkDisk	cld-unzipper	cld-unzipper.disk-st.onprem.ru
Домен для текстового редактора R7-office	docs	docs.disk-st.onprem.ru

### **Внимание**

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

## Дисковое пространство

Минимальный рекомендуемый объем памяти для разделов:

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

В зависимости от количества пользователей может быть увеличен объем памяти раздела `/opt/mail0nPremise/dockerVolumes` .

### **Внимание**

Рекомендуется отключить файл подкачки (SWAP).

## Подключение дисков

Если вы планируете монтирование дополнительных дисков, рекомендуется подключить их до начала установки. Подключенные диски необходимо разбить на разделы, для этого можно использовать любые привычные утилиты, например `fdisk`.

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

Пример команды для создания файловой системы ext4:

```
mkfs.ext4 <путь к устройству>
```

# Этапы установки

---

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

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

## Действия в командной строке на сервере

---

### Шаг 1. Создание пользователя deployer

1. В командной строке выполните последовательность команд:

#### Astra Linux

```
sudo -i

# Задаем пароль и создаем пользователя deployer
DEPLOYER_PASSWORD=mURvnxJ9Jr

useradd -G astra-admin -U -m -s /bin/bash deployer

echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

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

# Перелогиниваемся под пользователем deployer
sudo -i -u deployer

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

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

chmod 600 /home/deployer/.ssh/authorized_keys

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

exit
```

#### РЕД ОС

```
sudo -i

# Задаем пароль и создаем пользователя deployer
DEPLOYER_PASSWORD=mURvnxJ9Jr
```

```
useradd -G wheel -U -m -s /bin/bash deployer

echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

# Перелогиниваемся под пользователя deployer
sudo -i -u deployer

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

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

chmod 600 /home/deployer/.ssh/authorized_keys

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

exit
```

## MosOS Arbat

```
sudo -i

# Задаем пароль и создаем пользователя deployer

DEPLOYER_PASSWORD=xJ9JrmURvn

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

# MosOS автоматически не создает группу для нового пользователя

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

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

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

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

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

exit
```

### **Внимание**

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

2. Выполните команду `sudo visudo`.

3. В файле `/etc/sudoers` уберите `#` в начале следующей строки:

#### Astra Linux

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

#### РЕД ОС

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

#### MosOS Arbat

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

4. Выйдите из **Vim** с сохранением файла.

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

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

## Шаг 2. Распаковка дистрибутива

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

Нет принципиальной разницы, каким архиватором пользоваться. Ниже приведен пример для **unzip**:

#### Astra Linux

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

export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

unzip -o -P <пароль> <имя_архива>
```

## РЕД ОС

```
# Если на машину не установлен unzip, скачиваем его:  
sudo yum install unzip  
  
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true  
  
unzip -o -P <пароль> <имя_архива>
```

## MosOS Arbat

```
# Если на машину не установлен unzip, скачиваем его:  
sudo zypper install unzip  
  
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true  
  
unzip -o -P <пароль> <имя_архива>
```

### Внимание

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

## Шаг 3. Разрешить Port Forwarding

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

```
AllowTcpForwarding yes
```

## Шаг 4. Запуск установщика как сервиса

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

## Важно

Для подключения администратора к веб-интерфейсу установщика используется порт 8888. Рекомендуется настроить защиту порта через firewall либо наложенными средствами (TLS-проxy).

Не рекомендуется оставлять установщик включенным, если вы не проводите работы по установке и настройке системы. Запустили установщик → Провели установку → Выключили установщик. Если нужна донастройка системы, то снова включите установщик.

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

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

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

Ответ в случае успешного запуска установщика выглядит следующим образом:

### Astra Linux

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

### РЕД ОС

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

### MosOS Arbat

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

## Примечание

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

Если не получилось запустить `deployer` как сервис, то проверьте состояние SELinux:

```
getenforce
ausearch -m avc -ts recent
```

SELinux может ограничивать доступы запускаемого файла, чтобы временно отключить SELinux, выполните команду:

```
setenforce 0
```

## Действия в веб-интерфейсе установщика

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

### Шаг 1. Выбор варианта установки

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

 AdminPanel

#### Полные версии продуктов

Разверните на ваших серверах один или несколько продуктов VK On Premise

[Установка](#)

Инструкция по установке и настройке оборудования [Читать](#)

Инструкция по кластерной установке и настройке оборудования [Читать](#)

Инструкция по обновлению [Читать](#)

Инструкция по обновлению кластерной установки [Читать](#)

## Шаг 2. Выбор продуктов и опций

1. Включите флаги **Административная панель** и **VK WorkDisk**.
2. Включите нужные вам компоненты в каждом из продуктов.
3. Выберите интеграции, которые планируете настраивать.

### Административная панель

Продукт	Описание
Система групповых политик	<b>Beta</b>
<b>Система групповых политик.</b> Kafka внутри инсталляции	16 GB RAM, 8 vCPU
Интеграция с VK Teams	
Встроенное хранилище образов контейнеров	
Поддержка Российских криптографических стандартов (ГОСТ TLS)	<b>Beta</b>
Прогноз и контроль объёма почтового хранилища	
Базы данных	
Система мониторинга	Grafana, хранилище метрик Graphite, хранилище метрик Prometheus
Система сбора и отправки метрик	Сборщики и трансляторы Graphite и Prometheus-метрик

### VK WorkDisk

#### **Внимание**

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

Продукт	Описание
Административная панель v6.7.2	<b>Обязательный продукт.</b> Требования: 1 виртуальная машина на любом гипервизоре, 16 GB RAM, 8 vCPU, 100 GB SSD
Ядро объектного хранилища S3 + Ядро распределённого файлового хранилища	<b>Обязательный продукт</b>
API больших вложений VK WorkMail	<b>Обязательный продукт</b>
Интеграция с антивирусом по протоколу ICAP	
Система миграции WorkDisk из внешних сервисов	
Инструменты разработки	
Интеграция с Kerberos (SSO-авторизация)	
<b>Интеграция с Kerberos.</b> Keycloak внутри инсталляции v17.0.1	1 GB RAM, 1 vCPU
<b>Интеграция с Kerberos.</b> Интеграция с внешним Keycloak сервером	
Средства резервного копирования	
Интеграция с редактором «МойОфис»	
Редактор «P7-Офис» внутри инсталляции	2 GB RAM, 2 vCPU
Интеграция с редактором «P7-Офис»	
Система BI-аналитики	<b>Beta</b>
<b>Система BI-аналитики.</b> Kafka внутри инсталляции	16 GB RAM, 8 vCPU

Продукт	Описание
<b>Система BI-аналитики.</b> Дублирование действий пользователей во внешние хранилища	
Поддержка Российских криптографических стандартов (ГОСТ TLS)	<b>Beta</b>
Система проверки файлов Диска через DLP	<b>Beta</b>
Система аудита действий пользователя	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)
Система аудита действий пользователя (облегчённая версия)	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (PostgreSQL)

#### Примечание

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

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

## Шаг 3. Добавление лицензионного ключа

1. Введите лицензионный ключ или укажите путь к файлу лицензии **.lic**.
2. Нажмите на кнопку **Далее**.

## Лицензионный ключ

Лицензионный ключ VK WorkMail:

onprem.ru.lic

Выбрать файл

Лицензия 0187e174-d83f-75c2-806f-8408d935b622 для onprem.ru. Количество пользователей: VK WorkMail - 10000, VK WorkDisk - 10000, VK Teams - 10000. Разрешённые почтовые домены: ".onprem.ru", "admin.qdit". Действительна до 02.05.2025, 11:53:32

Далее

Информацию о том, как обновить лицензионный ключ или проверить сроки действия лицензий по продуктам VK WorkSpace, вы сможете найти в [разделе с дополнительной документацией](#).

## Шаг 4. Добавление гипервизора

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

The screenshot shows the AdminPanel interface. At the top, there is a blue header with the AdminPanel logo. Below the header, there is a blue banner with the text: "Пожалуйста, добавьте машины-гипервизоры или кластер kubernetes. Роль hypervisor - это виртуальная машина, на которой будут запущены компоненты продукта в контейнерах. Роль ext-k8s - это кластер kubernetes." Below the banner, there is a search bar and a dropdown arrow. On the left, there are two radio buttons: "Скрыть завершённые" (selected) and "Показать вспомогательные контейнеры". On the right, there are two dropdown menus: "Объектов в строке" (set to 1) and "Группировка" (set to Нет). In the center, there is a blue "Добавить" button with a dropdown arrow. The dropdown menu is open, showing two options: "Сервер" (selected) and "Внешний кластер Kubernetes".

Откроется окно добавления гипервизора:

The screenshot shows the AdminPanel interface with the "Add Hypervisor" form open. The form has the same header and banner as the previous screenshot. Below the banner, there are the same search bar and dropdown arrow. On the left, there are the same two radio buttons. On the right, there are the same two dropdown menus. The form fields are as follows:

Роль	IP	SSH-порт	Имя гипервизора
hypervisor	10.12.15.1	22	Hypervisor
Имя пользователя	Пароль	Приватный ключ	Data Center
centos	strongPass	Использовать авторизацию по паролю	DC1

Below the form fields, there is a text input field for "Теги" with the value "store,mail,etc...". At the bottom, there is a checkbox "Пропустить проверку некритичных требований" which is unchecked. At the bottom right, there are two buttons: "Отмена" and "Добавить".

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):

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

The screenshot shows a form with the following fields and options:

- IP:** 10.12.15.1
- SSH-порт:** 22
- Пароль:** [masked]
- Приватный ключ:** A dropdown menu is open, showing:
  - Использовать авторизацию по паролю
  - + Добавить новый ключ

At the bottom of the form are two buttons: **Отмена** and **Добавить**.

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

с. Перейдите в консоль.

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

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

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

ф. Поле **Пароль ключа** оставьте пустым.

г. Кликните по кнопке **Сохранить**.

5. 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.

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 5. Сетевые настройки

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

### Настройки

Сети | Доменные имена | Хранилища | Шардирование и репликация БД | Настройки компонентов | Интеграции | Переменные окружения

#### Настройки сетевого взаимодействия внутренней зоны (internal) Отмена Сохранить

Подсеть, используемая VK WorkSpace на серверах:	<input type="text" value="100.70.176.0/22"/>
Подсеть, используемая внутри контейнеров:	<input type="text" value="172.20.0.0/20"/>
MTU сети контейнеров:	<input type="text" value="1450"/>
НЕ использовать IP-in-IP и BIRD:	<input type="checkbox"/>
Список DNS-серверов. Оставьте пустым, если используется DHCP:	<input type="text" value="10.255.2.3"/>

[+ Добавить](#)

1. Укажите **DNS-сервер**.

### Внимание

Обязательно настройте NTP на VM в соответствии с рекомендациями к используемой ОС: [RedOS](#), [Astra Linux](#) или [MosOS Arbat](#).

2. Убедитесь, что:

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

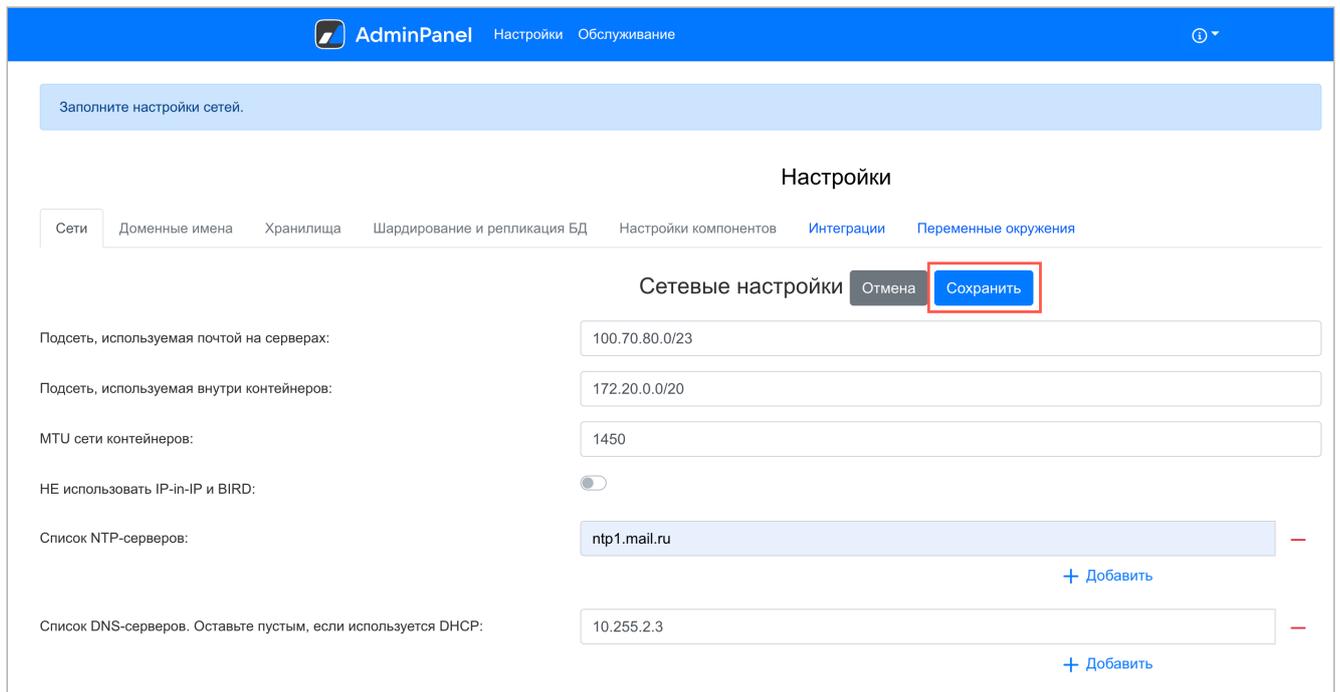
## Примечание

Эта подсеть используется только для трафика между контейнерами внутри системы. Если автоматически вычисленная подсеть уникальна и не пересекается с другими подсетями заказчика, значения менять не нужно. При установке на 1 VM в среднем создается более 650 контейнеров, поэтому по умолчанию используется 20-я подсеть.

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

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

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



The screenshot shows the 'AdminPanel' interface for network settings. The page title is 'Настройки' (Settings) and the sub-section is 'Сетевые настройки' (Network Settings). The 'Save' button is highlighted with a red box. The settings include:

- Подсеть, используемая почтой на серверах: 100.70.80.0/23
- Подсеть, используемая внутри контейнеров: 172.20.0.0/20
- MTU сети контейнеров: 1450
- НЕ использовать IP-in-IP и BIRD:
- Список NTP-серверов: ntp1.mail.ru (+ Добавить)
- Список DNS-серверов. Оставьте пустым, если используется DHCP: 10.255.2.3 (+ Добавить)

## Шаг 6. Доменные имена

Подробную информацию о создании доменных имен вы найдете в разделе [Создание DNS-записей](#).

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

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

## ⚠ Внимание

Для доменных имен нельзя использовать `etc/hosts`.

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

Укажите основные домены и добавьте SSL-сертификаты.  
Под спойлером дополнительных настроек находится список доменов, которые вы должны занести в DNS. Вы можете менять имена некоторых хостов, если такие адреса заняты, однако не рекомендуется это делать без необходимости.  
Рекомендуется использовать отдельный домен для хранилищ. Это должен быть отдельный домен того же уровня, что и основной. Например: `mail.example.ru` и `other.example.ru` — оба домена 3-го уровня.  
Так как основные настройки доменов влияют на дополнительные, нельзя одновременно редактировать обе группы.  
После заполнения основных настроек, установщик автоматически сгенерирует имя для каждого домена. Сохраните основные настройки и получите доступ к дополнительным, а также к добавлению сертификатов. Добавленные сертификаты автоматически подставятся к подходящим доменам.

### Настройки

Сети | Доменные имена | Хранилища | Шардирование и репликация БД | **Настройки компонентов** | Интеграции | Переменные окружения

#### Общие настройки доменов

Отмена Сохранить

SSL-сертификаты:  
Сохраните настройки доменов для добавления сертификатов

Название вашей компании:  
 ⓘ  
Заполните поле

Сайт вашей компании:

Основной домен для сервисов:  
 ⓘ  
Заполните поле

Домен для облачных хранилищ:  
 ⓘ  
Заполните поле

#### Настройки доменных имён 40

Домен для веб-интерфейса авторизации:

Ошибка:  
`hostname_is_not_suitable`

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

## Добавление SSL-сертификатов

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

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

и

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

3. Кликните по кнопке **Сохранить**.

Добавление SSL-сертификата

SSL-сертификат:

-----BEGIN CERTIFICATE-----

-----BEGIN CERTIFICATE-----

Или выберите файл с сертификатом

Выбрать файл

Ключ сертификата:

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----

Или выберите файл с ключом сертификата

Выбрать файл

Отмена

Сохранить

Есть второй вариант:

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

#### **Примечание**

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

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

Далее

## Настройки

Сети
Доменные имена
Хранилища
Шардирование и репликация БД
Настройки компонентов
Интеграции
Переменные окружения

### Общие настройки доменов ✎

Название вашей компании:  
VK Tech

Сайт вашей компании:  
https://tech.vk.com/

Основной домен для сервисов:  
doc-mail.docvk.tech

Домен для облачных хранилищ:  
doc-st.docvk.tech

SSL-сертификаты:

\*.cloud.doc-mail.docvk.tech, \*.doc-mail.docvk.tech, \*.doc-st.docvk.tech, \*.e.doc-mail.docvk.tech, doc-mail.docvk.tech —

Действителен с 03/07/2024 16:05:39 до 01/10/2024 16:05:38  
Выдан: Let's Encrypt (R11)

+ Добавить сертификат

### Настройки доменных имён

<p>Домен для веб-интерфейса авторизации: account.doc-mail.docvk.tech</p>	<p>Сертификаты: 0:*.cloud.doc-mail.docvk.tech, *.doc-mail.docvk.tech, *.doc-st.docvk.tech, *.e.doc-mail.docvk.tech, doc-mail.docvk.tech до 01/10/2024 16:05:38 <span style="float: right;">✎</span></p>
<p>Домен для скачивания вложений VK WorkMail: af.doc-mail.docvk.tech</p>	<p>Сертификаты: 0:*.cloud.doc-mail.docvk.tech, *.doc-mail.docvk.tech, *.doc-st.docvk.tech, *.e.doc-mail.docvk.tech, doc-mail.docvk.tech до 01/10/2024 16:05:38 <span style="float: right;">✎</span></p>

## Шаг 7. Запуск установки гипервизора

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

AdminPanel
Настройки
Обслуживание
ⓘ

Запустите установку всех гипервизоров. Вы можете воспользоваться функцией автоматической установки. Для этого нажмите кнопку «Запустить автоматическую установку» (синий треугольник в общей строке состояния).

**ВНИМАНИЕ!** Настройка гипервизоров вносит изменения в системные настройки машин. Может потребоваться перезагрузка.

Также вы можете в целях отладки запускать установку каждой машины по отдельности (треугольник в строке гипервизора) или пошагово выполнять задачи на странице каждой машины. Для этого перейдите на страницу машины (шестерёнка в строке машины).

9.52%

▶

Скрыть завершённые

Показать вспомогательные контейнеры

Объектов в строке

Группировка

doc-01 (100.70.160.11) Ⓢ

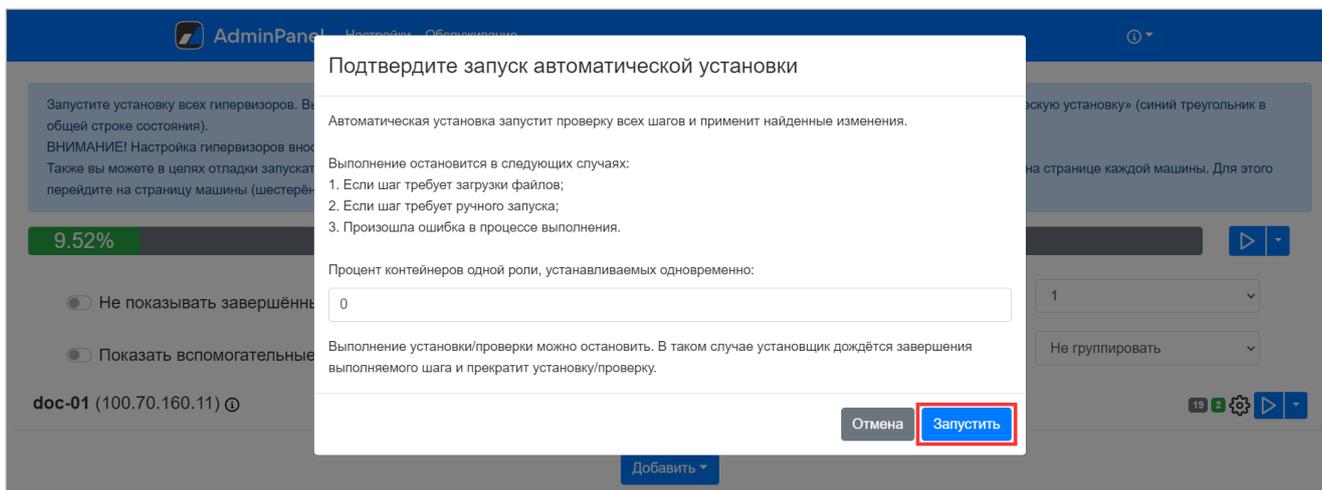
19
⚙️
▶

Добавить

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

### 🔥 Рекомендация

Перед запуском автоматической установки оставьте включенными все проверки. Подробнее о работе проверок можно прочитать здесь: [Диагностика системы в веб-интерфейсе установщика](#)



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

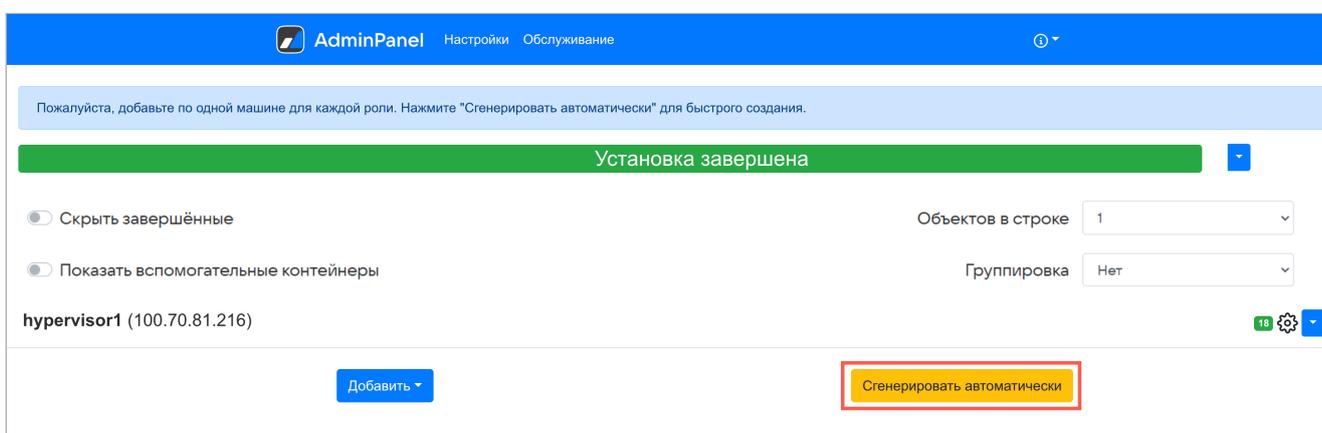


В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуется повторный запуск автоматической установки.

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

## Шаг 8. Генерация контейнеров

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

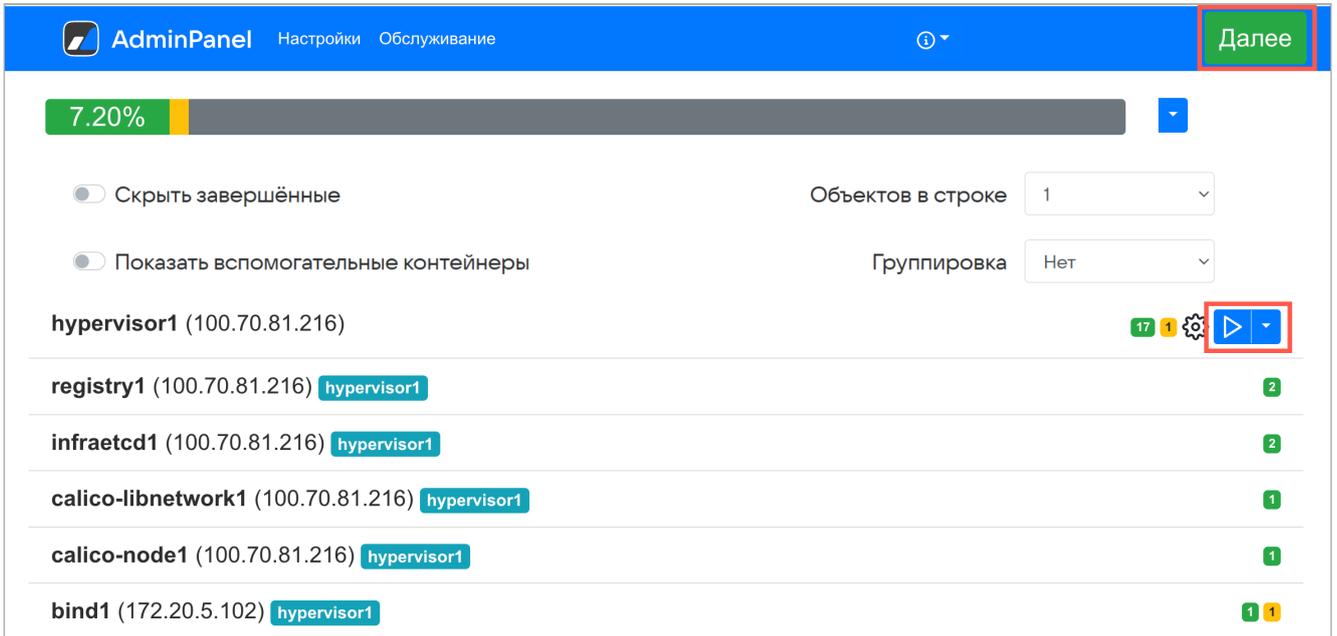


На экране начнут появляться сгенерированные контейнеры.

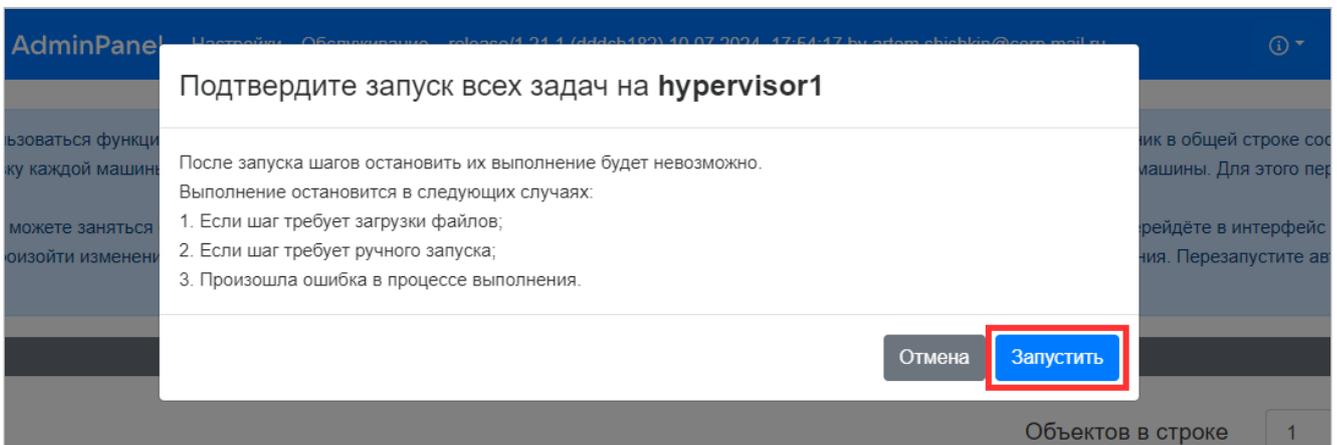
## ⚠ Внимание

В случае появления ошибок используйте раздел [Логи и полезные команды](#).

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



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



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

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

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

front2 (100.70.137.210) front Не отвечает гипервизор

<b>del2</b> (172.20.2.132) front2 Не отвечает гипервизор del-mailloder2, del-zeproxy2, del-zubr2, del-donjuan2, del-aestat2, del-envoy2	<b>bizf2</b> (172.20.2.183) front2 Не отвечает гипервизор bizf-envoy2	<b>mpop2</b> (172.20.2.188) front2 Не отвечает гипервизор mpop-zubr2, mpop-donjuan2, mpop-aestat2, mpop-ameliz, mpop-zp2, mpop-envoy2, mpop-apache-exporter2, mpopd-far2, mpopd-scn2, mpopd-m2, mpopd-pn2, mpopd-mspq2, mpopd-ls2, mpopd-recaller2	<b>panda2</b> (172.20.2.190) front2 Не отвечает гипервизор panda-zubr2, panda-donjuan2, panda-aestat2, panda-delivery-canceller2, panda-envoy2	<b>biz-celery-worker-pdd2</b> (172.20.3.3) front2 Не отвечает гипервизор biz-celery-worker-pdd-envoy2	<b>biz-celery-worker-pdd-check2</b> (172.20.3.8) front2 Не отвечает гипервизор biz-celery-worker-pdd-check-envoy2
<b>biz-celery-worker-pdd-high2</b> (172.20.3.1) front2 Не отвечает гипервизор biz-celery-worker-pdd-high-envoy2	<b>biz-celery-worker-pdd-update2</b> (172.20.3.11) front2 Не отвечает гипервизор biz-celery-worker-pdd-update-envoy2	<b>fallback2</b> (172.20.2.135) front2 Не отвечает гипервизор fallback-zubr2, fallback-aestat2, fallback-envoy2, fallback-reexim2, fallback-relmtpd2	<b>fallback-dlp2</b> (172.20.2.136) front2 Не отвечает гипервизор fallback-dlp-zubr2, fallback-dlp-aestat2, fallback-dlp-envoy2, fallback-dlp-reexim2, fallback-dlp-relmtpd2	<b>mx2</b> (172.20.2.138) front2 Не отвечает гипервизор mx-zubr2, mx-reexim2, mx-relmtpd2, mx-aestat2, mx-envoy2	<b>relay2</b> (172.20.2.137) front2 Не отвечает гипервизор relay-zubr2, relay-aestat2, relay-envoy2, relay-reexim2, relay-relmtpd2
<b>smtp2</b> (172.20.2.133) front2 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.

mail-vkwm2-st1 (100.70.80.79) st

## Выполните шаги по настройке машины

**Загрузить бэкап** Выберите файл бэкапа

ВНИМАНИЕ! Процесс восстановления из бэкапа будет запущен сразу после загрузки файла!

<b>tune_kernel</b> done Настроить параметры ядра	Запустить
<b>disable_NM_for_cali</b> done Отключить NetworkManager (если он есть) для сетевых интерфейсов Calico	Запустить
<b>disable_firewall</b> done Отключить межсетевой экран (firewall)	Запустить
<b>disable_selinux</b> done Отключить selinux. ВНИМАНИЕ! Этот шаг перезагрузит машину, если selinux на ней не выключен. Если есть какие-нибудь ограничения на перезагрузку, то выключите selinux вручную!	Запустить
<b>check_needed_packs</b> done Проверить наличие Docker и Docker Compose	Запустить

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

Название машины: 
 IP: 
 SSH-порт: 
 Имя гипервизора:

Имя пользователя: 
 Пароль: 
 Приватный ключ: 
 Data Center:

Интерфейс для межсерверного взаимодействия:

Теги:

Пропустить проверку некритичных требований

## Выполните шаги по настройке машины

**Загрузить бэкап** [Выберите файл бэкапа](#)

ВНИМАНИЕ! Процесс восстановления из бэкапа будет запущен сразу после загрузки файла!

---

**tune\_kernel** done  
 Настроить параметры ядра

Повторно запустите автоматическую установку.

## Шаг 9. Хранилища

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

### Настройки

[Сети](#)
[Доменные имена](#)
[Хранилища](#)
[Шардирование и репликация БД](#)
[Настройки компонентов](#)
[Интеграции](#)
[Переменные окружения](#)

#### Временные вложения

- cldst
- cldmetast
- blobcloud
- mailcloud
- zepto\_del
- zepto\_main
- zepto\_opt
- zepto\_skel
- zepto\_search
- crow\_index
- mescalito
- fstab

#	Диск 1			Диск 2			#
	Контроллер	Устройство	Размер	Контроллер	Устройство	Размер	
1	blobcloud1.qdit <small>mail-vkwm2-st1 (astra)</small>	Нет данных	100.00Gb	blobcloud2.qdit <small>mail-vkwm2-st2 (redos)</small>	Нет данных	100.00Gb	
2	blobcloud2.qdit <small>mail-vkwm2-st2 (redos)</small>	Нет данных	100.00Gb	blobcloud3.qdit <small>mail-vkwm2-st3 (alma)</small>	Нет данных	100.00Gb	
3	blobcloud1.qdit <small>mail-vkwm2-st1 (astra)</small>	Нет данных	100.00Gb	blobcloud3.qdit <small>mail-vkwm2-st3 (alma)</small>	Нет данных	100.00Gb	

[Добавить](#) или [сгенерировать](#) дисковые пары  
 Данные о дисках от 14.03.2024, 12:01:31. [Обновить](#)

## Шаг 10. Шардирование и репликация БД

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

Имя БД	Номер кластера	Отказоустойчивость	Мастер	Состав
abookpdd-tar	1	Overlord	abookpdd-tar2 mail-vkwm2-db2	abookpdd-tar2 abookpdd-tar1
addrbook-tar	1	Overlord	addrbook-tar1 mail-vkwm2-db1	addrbook-tar1 addrbook-tar2
addrbook-tar	2	Overlord	addrbook-tar3 mail-vkwm2-db2	addrbook-tar3
addrbook-tar	3	Overlord	addrbook-tar4 mail-vkwm2-db1	addrbook-tar4
aliases-tar	1	Overlord	aliases-tar1 mail-vkwm2-db1	aliases-tar1 aliases-tar2
appass-tar	1	Overlord	appass-tar1 mail-vkwm2-db1	appass-tar1 appass-tar2

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

## Шаг 11. Настройка компонентов

В разделе выполняются настройки различных компонентов системы.

**Настройки**

Сети | Доменные имена | Хранилища | Шардирование и репликация БД | **Настройки компонентов** | Интеграции | Переменные окружения

**Настройки мониторинга**

- Мониторинг
- Ограничение доступа к доменам
- Панель администрирования
- Рассылки
- HTTP(S)-прокси

Внешний сервер Graphite

Внешний сервер Prometheus

[Набор готовых дашбордов для Grafana](#)

### Ограничение доступа к доменам

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

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

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

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

### **Внимание**

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

## Панель администрирования

Чтобы начать настройку, нажмите кнопку редактирования .

## Настройки

Сети   Доменные имена   Хранилища   Шардирование и репликация БД   **Настройки компонентов**   Интеграции   Переменные окружения   Настройка ресурсов

### Настройки панели администрирования

Отмена   Сохранить

Мониторинг

Ограничение доступа к доменам

**Панель администрирования**

Рассылки

HTTP(S)-прокси

Административные домены ⓘ:  [+ Добавить](#)

Настройки пользователей, доменов панели администрирования ⓘ

Количество дней перед удалением пользователя:

Размер облака пользователя по умолчанию (МБ):

Не проверять актуальность включенного функционала (фич)

Общие переменные окружения для всех сервисов панели администрирования:

[+ Добавить](#)

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

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

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

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

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

## Рассылки

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

## Настройки

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения Настройка ресурсов

VK WorkDisk **Панель администрирования**

Мониторинг

Ограничение доступа к доменам

Панель администрирования

**Рассылки**

HTTP(S)-прокси

**Панель администрирования** **Отмена** **Сохранить**

Email отправителя:

admin@admin.qdit

Имя отправителя:

Будет использовано значение по умолчанию: Администрирование

Адрес сервера пересылки:

Будет использоваться внутренний сервер пересылки

Порт сервера пересылки:

25

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.

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

## Система учета действий пользователей

Чтобы изменить время хранения логов, кликните по кнопке редактирования.

### Настройки

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения

Авторизация **Настройки системы учёта действий пользователей** **Отмена** **Сохранить**

Адресная книга

Настройки панели администрирования

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

**Система учёта действий пользователей**

Мониторинг

HTTP(S)-прокси

Время хранения событий по пользователям (в секундах):  хранить бесконечно

Включить статистику по IP

Время хранения событий по IP (в секундах):  3.00 месяцев

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

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

## Мониторинг

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

Чтобы включить внешнюю систему мониторинга:

1. Нажмите на **i** и перейдите в раздел **Продукты**.
2. Включите флаг **Система сбора и отправки метрик**. При этом флаг **Система мониторинга** будет автоматически отключен.

**Административная панель v6.5.1**

1 виртуальная машина на любом гипервизоре, 16 GB RAM, 8 vCPU, 100 GB SSD

---

**Система групповых политик** **Beta**

---

**Интеграция с VK Teams**

---

**Встроенное хранилище образов контейнеров**

---

**Система мониторинга**   
Grafana, хранилище метрик Graphite, хранилище метрик Prometheus

---

**Система сбора и отправки метрик**   
Сборщики и трансляторы Graphite и Prometheus-метрики

### Примечание

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

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

### **Внимание**

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

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

```
sudo systemctl restart deployer
```

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

<b>calendarpg1</b> (172.20.4.166) <b>hypervisor1</b> ⓘ	2
<b>fstatdb1</b> (172.20.4.142) <b>hypervisor1</b> ⓘ	4 1
<b>graphite1</b> (100.70.81.216) <b>hypervisor1</b>	1 
<b>gravedb1</b> (172.20.4.143) <b>hypervisor1</b> ⓘ	3 1
<b>mcrouter1</b> (172.20.4.174) <b>hypervisor1</b> ⓘ	1
<b>mirage1</b> (172.20.4.134) <b>hypervisor1</b> ⓘ	5 1
<b>rpopdb1</b> (172.20.4.144) <b>hypervisor1</b> ⓘ	3 1
<b>seconddb1</b> (172.20.4.140) <b>hypervisor1</b> ⓘ	5 1
<b>swadb1</b> (172.20.4.136) <b>hypervisor1</b> ⓘ	6 1
<b>umi1</b> (172.20.4.138) <b>hypervisor1</b> ⓘ	3 1
<b>victoria-metrics1</b> (100.70.81.216) <b>hypervisor1</b>	1 
<b>graphite-cloud1</b> (172.20.4.160) <b>hypervisor1</b> ⓘ	1
<b>graphite-mail1</b> (172.20.4.149) <b>hypervisor1</b> ⓘ	1

- Удаление может занять некоторое время. Когда все неактуальные роли будут удалены, запустите автоматическую установку.
- Далее перейдите в раздел **Настройки компонентов** → **Мониторинг**. Введите необходимые данные для системы мониторинга, которую вы используете.

**Настройки**

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения Настройка ресурсов

**Настройки мониторинга** Отмена Сохранить

**Мониторинг**

Ограничение доступа к доменам

Панель администрирования

Рассылки

HTTP(S)-прокси

Внешний сервер Graphite

IP-адрес или домен Graphite-сервера:

Порт Graphite-сервера:

Протокол подключения:

Внешний сервер Prometheus

IP-адрес или домен Prometheus-сервера:

Порт Prometheus-сервера:

[Набор готовых дашбордов для Grafana](#)

9. Сохраните изменения.

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

## Настройки HTTP(S)-прокси

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

**Настройки**

Сети Доменные имена Хранилища Шардирование и репликация БД **Настройки компонентов** Интеграции Переменные окружения Настройка ресурсов

**Настройки HTTP(S)-прокси** Отмена Сохранить

**Мониторинг**

Ограничение доступа к доменам

Панель администрирования

Рассылки

**HTTP(S)-прокси**

Перед VK WorkSpace есть прокси-сервер ⓘ

Список IP прокси-серверов ⓘ [+ Добавить](#)

HTTP-заголовок прокси с оригинальным IP клиента ⓘ:

HTTP-заголовок прокси с оригинальным протоколом подключения клиента ⓘ:

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

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

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

## Шаг 12. Интеграции

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

[Интеграция с Keycloak для SSO-авторизации](#) — в документе содержится инструкция по настройке интеграции с сервисом SSO-авторизации.

[Настроить дублирование действий пользователей во внешние хранилища](#)

## Настройка интеграции с внешней почтой

Настройка интеграции с внешней почтой нужна, чтобы получать служебные письма:

- Приглашение пользователя в папку.
- Информационное сообщение о попытке загрузить запрещенный формат.
- Одноразовый пароль для Мессенджера.

Чтобы настроить интеграцию:

1. Перейдите в раздел **Интеграции** → **Интеграция с внешней почтой**.
2. Введите адрес почтового сервера и порт.
3. Нажмите кнопку **Сохранить**.

The screenshot shows the 'Настройки' (Settings) page with the 'Интеграции' (Integrations) tab selected. The main heading is 'Настройки интеграции с внешней почтой' (External Email Integration Settings). There are two buttons: 'Отмена' (Cancel) and 'Сохранить' (Save). The form contains the following fields:

Интеграция с VK Teams		
Дублирование действий пользователей во внешние хранилища	Адрес сервера:	<input type="text" value="smtp.vkwm-02.release.vkwm.ru"/>
Интеграция с WOPI-редактором	Порт сервера:	<input type="text" value="25"/>
Лицензия редактора P7-Офис		
<input type="button" value="Интеграция с внешней почтой"/>		

4. Запустите автоматическую установку.

## Настройки системы BI-аналитики

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

## Примечание

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

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

### Настройки

Сети   Доменные имена   Хранилища   Шардирование и репликация БД   **Настройки компонентов**   Интеграции   Переменные окружения

#### Интеграция с WOPI-редактором

Лицензия редактора P7-Офис

Настройки для Системы BI-Аналитики **1**

Сборщик почты

Интеграция с другими инсталляциями VK WorkMail **Deprecated**

Дублирование действий пользователей во внешние хранилища

#### Настройки подключения к внешнему серверу Kafka

Отмена   Сохранить

+ Добавить

Адрес сервера Kafka

Имя топика аналитики Kafka:

Имя топика почтовой аналитики Kafka:

Имя топика событий авторизации Kafka:

Сохраните изменения, затем запустите **автоматическую установку** в общей строке состояния.

## Шаг 13. Укажите переменные окружения

В разделе производится настройка кастомных переменных Панели администратора.

**Настройки**

Сети   Доменные имена   Шардирование и репликация БД   Настройки компонентов   Интеграции   Переменные окружения

adloader

bi-kafka

bind

biz-celery-beat

biz-celery-worker-pdd

biz-celery-worker-pdd-check

biz-celery-worker-pdd-high

biz-celery-worker-pdd-update

biz-pravda-kafka-consumer

bizdb

bizf

bizginx

bizpostgres

bizredis

cadvisor

calico-libnetwork

calico-node

carbonapi

clickhouse-keeper

**Пользовательские переменные adloader:** Отмена Сохранить

ADLOADER\_LOG\_LEVEL : 0

[+ Добавить](#)

Список возможных переменных для роли

Имя переменной	Значение по умолчанию	Описание	Варианты
ADLOADER_BIZ_EXTERNAL_REQUEST_TIMEOUT	5s		
ADLOADER_BIZ_ONPREMISE	true		
ADLOADER_BIZ_RPS	1		
ADLOADER_BIZ_USE_CSRF	false		
ADLOADER_DEBUG_PPROF_ADDR	:8400		
ADLOADER_DEBUG_PPROF_ENABLED	false		
ADLOADER_DOMAINS_UPDATE_INTERVAL	5m		
ADLOADER_GRPC_ADDRESS	0.0.0.0:2222		

**⚠ Внимание**

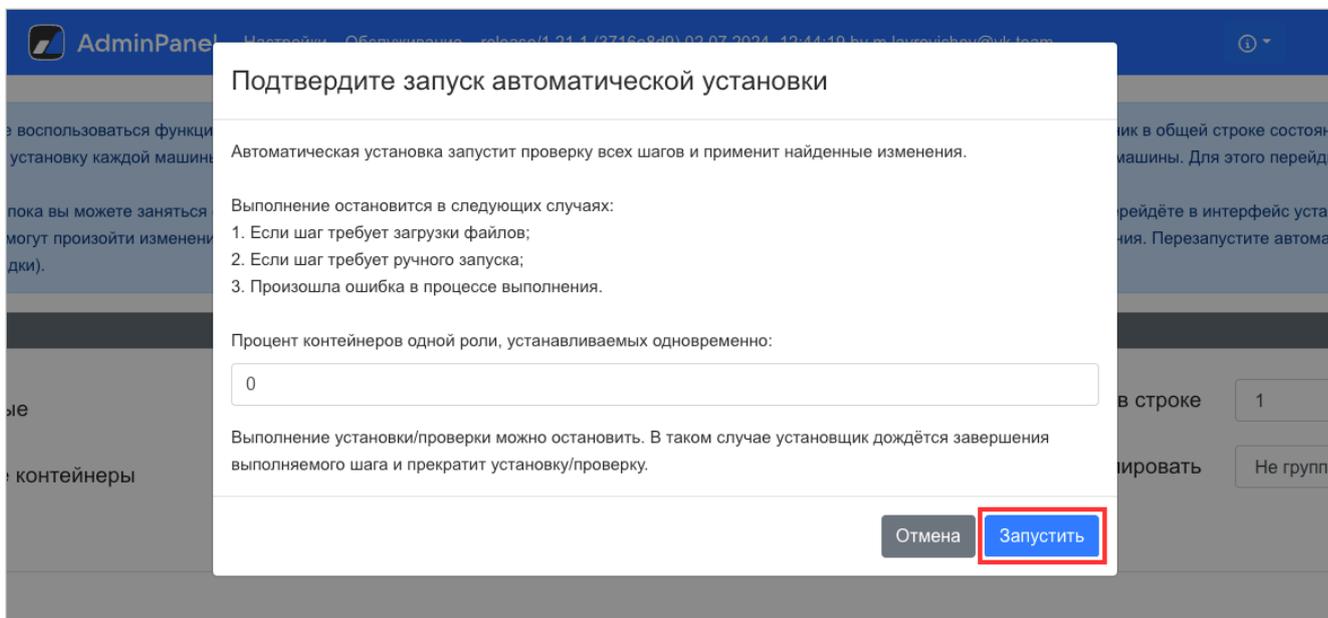
Настройка переменных окружения возможна только после консультации с представителем VK.

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 14. 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 15. 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.

AdminPanel Настройки Обслуживание Далее

Установка завершена

Скрыть завершённые
 Объектов в строке: 1

Показать вспомогательные контейнеры
 Группировка: Нет

doc-db-01 (100.70.160.6)	db	19 2	⚙️	⌵
mon (100.70.160.14)	mon	18 1	⚙️	⌵
doc-db-02 (100.70.160.7)	db	17 2	⚙️	⌵
doc-front-01 (100.70.160.16)	front	17 2	⚙️	⌵
doc-front-02 (100.70.160.2)	front	17 2	⚙️	⌵
doc-storage-01 (100.70.160.11)	st	18 1	⚙️	⌵
doc-storage-02 (100.70.160.8)	st	18 1	⚙️	⌵
doc-storage-03 (100.70.160.10)	st	18 1	⚙️	⌵
registry1 (100.70.160.14)	mon	2	⚙️	⌵

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

AdminPanel Настройки Обслуживание ⓘ

Создайте первый почтовый домен - часть email-адресов после "@".

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>/biz0wner.pass`.

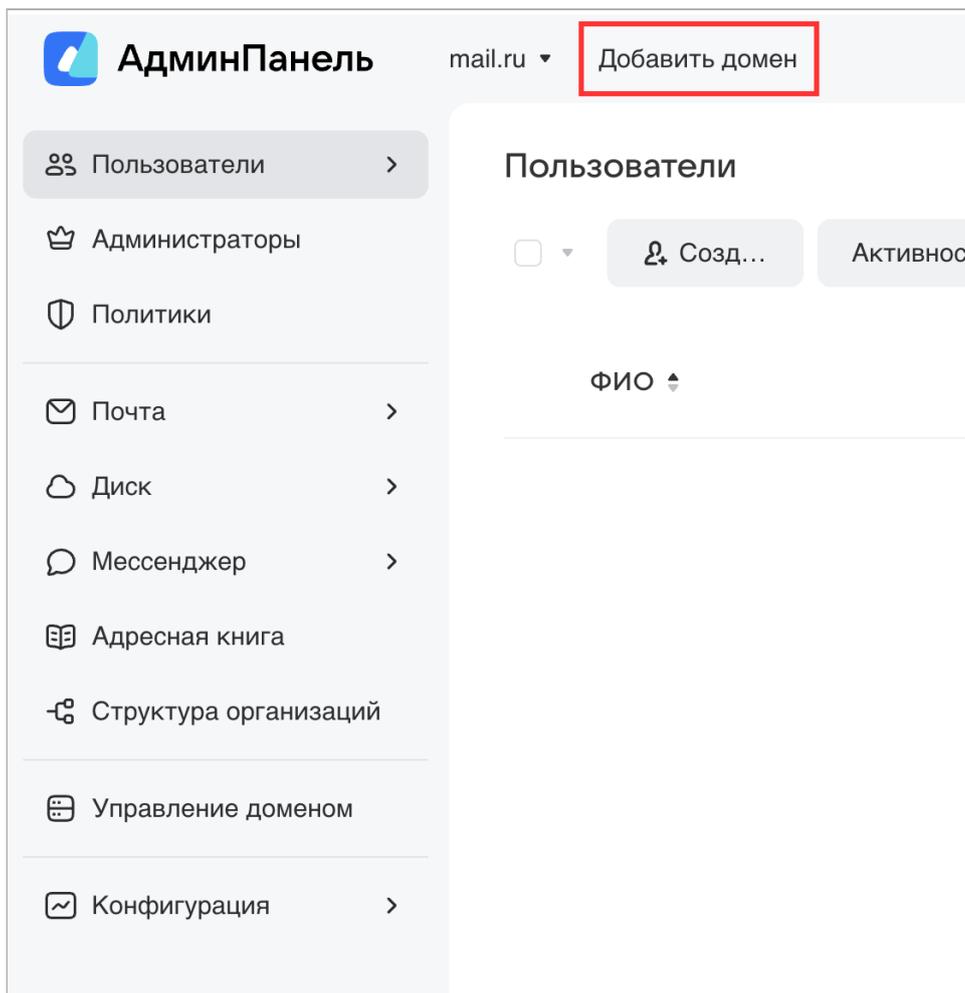
Если логин и пароль были введены правильно, вы попадете в Панель администратора.

#### ⚠️ 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.

# Добавление дополнительных доменов

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



## Логи и полезные команды

Все команды, перечисленные ниже, следует выполнять в консоли.

1. Перезапуск установщика:

```
sudo systemctl restart deployer
```

2. Логи установщика:

```
sudo journalctl -fu deployer
```

3. Список запущенных контейнеров:

```
docker ps
```

4. Логи конкретного контейнера:

```
sudo journalctl -eu имя_контейнера
```

5. Статус контейнера:

```
systemctl status имя_контейнера
```

6. Посмотреть список «сломанных» контейнеров:

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

7. Посмотреть список всех незапустившихся контейнеров:

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

8. Удалить контейнер:

```
sudo docker rm имя_контейнера
```

 Автор: Груздев Никита

 28 ноября 2025 г.