

# Почта VK WorkSpace

**Установка тестовой версии на одну машину.  
Версия 26.1**

Назначение документа	4
Требования к администраторам	4
Дополнительная документация	4
Технические требования	4
Как использовать системы виртуализации	5
Пример настройки параметров ОС	6
Пример настройки параметров ОС	6
Требования к ресурсам сервера	8
Предварительные условия для установки	8
Как работать с Wildcard-сертификатами	9
Какие протоколы использует Почта	9
Обязательные предварительные действия	10
Настройте ротацию логов в journald	10
Создание DNS-записей	10
Дисковое пространство	14
Этапы установки	14
Действия в командной строке на сервере	14
Шаг 1. Создание пользователя deployer	14
Шаг 2. Распаковка дистрибутива	17
Шаг 3. Разрешить Port Forwarding	18
Шаг 4. Запуск установщика как сервиса	18
Действия в веб-интерфейсе установщика	19
Шаг 1. Добавьте лицензионный ключ	20
Шаг 2. Выберите продукты и компоненты	21
Шаг 3. Добавьте гипервизоры (серверы)	27
Шаг 4. Сетевые настройки	29
Шаг 5. Доменные имена	30
Добавление SSL-сертификатов	31
Шаг 6. Запуск установки гипервизора	32

Шаг 7. Генерация контейнеров	34
Шаг 8. Хранилища	37
Шаг 9. Шардирование и репликация БД	37
Шаг 10. Запуск установки всех машин	38
Шаг 11. Завершение установки, инициализация домена и вход в панель администратора	38
Альтернативный способ проверить MX-запись	41
Логи и полезные команды	43

# Назначение документа

---

В документе описана тестовая установка Почты VK WorkSpace на одну виртуальную машину. Под тестовой установкой подразумевается быстрая установка с базовыми настройками для демонстрации возможностей почтовой системы.

## Требования к администраторам

---

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

## Дополнительная документация

---

[Инструкция по установке обновлений Почты](#) — в документе содержится информация по обновлению Почты.

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

[Выпуск SSL-сертификатов с Let's Encrypt](#)

[Как обновить лицензионный ключ](#)

## Технические требования

---

Поддерживаемые операционные системы для установки Почты:

- **Astra Linux SE Орел** — версия 1.7.5+, версия ядра — **5.15**.
- **Astra Linux SE Орел** — версия 1.8, версия ядра — **6.1**.
- **РЕД ОС** — версия 7.3.5, версия ядра — **6.1**.
- **РЕД ОС** — версия 7.3с (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 Почта VK WorkSpace работала 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.

## Пример настройки параметров ОС

### Важно

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

## Пример настройки параметров ОС

### Важно

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

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

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

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

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

### Дополнительные настройки для сертифицированной РЕД ОС 7.3

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

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

До установки Почты VK WorkSpace:

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

```
DefaultLimitNOFILE=524288:524288
```

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

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

Установить пакеты можно с помощью команды:

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

### Дополнительные настройки для MosOS Arbat

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

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

3. Примените изменения:

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

Или перезагрузите операционную систему.

# Требования к ресурсам сервера

Тестовая версия корпоративной почты устанавливается на один сервер со следующей конфигурацией:

- 24 vCPU;
- 96 GB RAM;
- 400 GB SSD.

Версия ядра — **от 5.15**; архитектура системы — **x86\_64**.

## Рекомендация

Используйте процессоры Intel Xeon Gold 6140 и новее.

## Предварительные условия для установки

Представители VK предоставили вам следующие данные:

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

Также вам потребуется:

- Набор DNS-записей: A, CNAME, MX, TXT, NS.
- Доступ к серверу по SSH с правами администратора.
- Локальная сеть 1 GbE или 10 GbE.
- Отключить swap.
- Сертификаты SSL для каждого CNAME или Wildcard-сертификат для домена (информацию о выпуске SSL-сертификатов вы найдете в разделе [Дополнительная документация](#)).
- 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.

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

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

- Отдельный mTLS прокси-сервер с обязательной проверкой клиентских сертификатов. Управление ключами происходит посредством PKI заказчика.
- Использование (меж)сетевых экранов как на операционной системе сервера установщика 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 почты `mail.onprem.ru`, а домен для хранилища `mail-st.onprem.ru`, тогда в сертификат необходимо добавить шесть доменов:

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

## Какие протоколы использует Почта

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

# Обязательные предварительные действия

## Настройте ротацию логов в journald

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

## Создание DNS-записей

Для работы почты необходима **MX-запись** (рекомендуемый приоритет — 10), которая обязательно ведет на `mxs.<домен для почты>`. Тестовую установку можно завершить без правильной и рабочей MX-записи.

Помимо этого вам нужно создать: - Два основных домена: для почты и для хранилищ. - Набор A- или CNAME-записей.

Для примера в документе будут использоваться следующие DNS-записи:

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

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

### **Внимание**

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

Далее в таблицах представлены списки A- или CNAME-записей, которые нужно создать перед установкой Почты. Домены из таблиц должны являться поддоменами для двух основных.

### Для почты:

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

Назначение домена	Имя домена	Пример
Веб-интерфейс авторизации	<code>account</code>	<code>account.mail.onprem.ru</code>
Домен для проверки доступа	<code>access</code>	<code>access.mail.onprem.ru</code>

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

Назначение домена	Имя домена	Пример
Загрузка файлов в VK WorkDisk	cld-uploader.cloud	cld-uploader.cloud.mail.onprem.ru
Скачивание файлов в веб-интерфейсе VK WorkDisk	cloclo.cloud	cloclo.cloud.mail.onprem.ru
Загрузка файлов в VK WorkDisk	cloclo-upload.cloud	cloclo-upload.cloud.mail.onprem.ru
Интеграция с API VK WorkDisk	openapi.cloud	openapi.cloud.mail.onprem.ru
Загрузка файлов в публичные папки в VK WorkDisk	pu.cloud	pu.cloud.mail.onprem.ru
Портальная авторизация VK WorkDisk	sdc.cloud	sdc.cloud.mail.onprem.ru
Загрузка больших почтовых вложений в VK WorkDisk	uploader.e	uploader.e.mail.onprem.ru
Превью файлов в VK WorkDisk	thumb.cloud	thumb.cloud.mail.onprem.ru
Веб-интерфейс Почты	e	e.mail.onprem.ru
Сервис аватарок	filin	filin.mail.onprem.ru
IMAP Почты	imap	imap.mail.onprem.ru
Неисполняемые статические данные	img	img.mail.onprem.ru
Исполняемые статические данные	imgs	imgs.mail.onprem.ru
MX Почты	mxs	mxs.mail.onprem.ru
OAuth2-авторизация	o2	o2.mail.onprem.ru
	portal	portal.mail.onprem.ru

Назначение домена	Имя домена	Пример
Общепортальные сервисы авторизации		
POP3 Почты	pop	pop.mail.onprem.ru
SMTP Почты	smtp	smtp.mail.onprem.ru
Сервер авторизации (межсерверные запросы)	swa	swa.mail.onprem.ru
Webdav	webdav.cloud	webdav.cloud.mail.onprem.ru
Доска VK Workspace	board	board.mail.onprem.ru

#### Для хранилищ:

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

Назначение домена	Имя домена	Пример
Скачивание исполняемых вложений Почты	af	af.mail-st.onprem.ru
Проксирование активного контента вложений Почты	ampproxy	ampproxy.mail-st.onprem.ru
Просмотр исполняемых вложений Почты	apf	apf.mail-st.onprem.ru
Защита от XSS-атак при скачивании файлов из VK WorkDisk	cloclo	cloclo.mail-st.onprem.ru
Скачивание больших почтовых вложений из VK WorkDisk	cloclo-stock	cloclo-stock.mail-st.onprem.ru
Распаковка архивов в интерфейсе VK WorkDisk	cld-unzipper	cld-unzipper.mail-st.onprem.ru
Интеграция с API Почты	corsapi	corsapi.mail-st.onprem.ru
Проксирование внешних вложений Почты	proxy	proxy.mail-st.onprem.ru

Назначение домена	Имя домена	Пример
Домен для текстового редактора R7-office	docs	docs.mail-st.onprem.ru
Облако, реализующее S3 API	hb	hb.mail-st.onprem.ru
Облако временных вложений Почты	tmpatt	tmpatt.mail-st.onprem.ru
Домен для Grafana	grafana	grafana.mail-st.onprem.ru

### **Внимание**

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

## Дисковое пространство

100% дискового пространства необходимо смонтировать в корневой раздел файловой системы. Также нужно выключить файл подкачки (SWAP).

## Этапы установки

Весь процесс установки можно разделить на два этапа:

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

## Действия в командной строке на сервере

### Шаг 1. Создание пользователя deployer

1. В командной строке выполните последовательность команд:

Astra Linux

```
sudo -i
```

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

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

echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

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

# Перелогиниваемся под пользователем deployer
sudo -i -u deployer

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

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

chmod 600 /home/deployer/.ssh/authorized_keys

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

exit
```

## РЕД ОС

```
sudo -i

# Задаем пароль и создаем пользователя deployer
DEPLOYER_PASSWORD=mURvnxJ9Jr

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

echo deployer:"$DEPLOYER_PASSWORD" | chpasswd

# Перелогиниваемся под пользователя deployer
sudo -i -u deployer

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

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

chmod 600 /home/deployer/.ssh/authorized_keys

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

exit
```

## MosOS Arbat

```
sudo -i

# Задаем пароль и создаем пользователя deployer
```

```

DEPLOYER_PASSWORD=xJ9JrmURvn

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

# MosOS автоматически не создает группу для нового пользователя

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

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

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

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

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

exit

```

### **Внимание**

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

2. Выполните команду `sudo visudo`.

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

#### Astra Linux

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

#### РЕД ОС

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

#### MosOS Arbat

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

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

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

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

## Шаг 2. Распаковка дистрибутива

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

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

### Astra Linux

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

export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

unzip -o -P <пароль> <имя_архива>
```

### РЕД ОС

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

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

export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

unzip -o -P <пароль> <имя_архива>
```

### MosOS Arbat

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

export UNZIP_DISABLE_ZIPBOMB_DETECTION=true

unzip -o -P <пароль> <имя_архива>
```

### **Внимание**

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

## Шаг 3. Разрешить Port Forwarding

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

```
AllowTcpForwarding yes
```

## Шаг 4. Запуск установщика как сервиса

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

### **Важно**

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

```
journalctl -u deployer
```

И убедитесь, что порт 8888 слушают:

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

## Действия в веб-интерфейсе установщика

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

## VK WorkSpace

Разверните на ваших серверах один или несколько продуктов

Установить

### Инструкции

Установка и настройка оборудования



Кластерная установка и настройка оборудования



Обновление



Обновление кластерной установки



## Шаг 1. Добавьте лицензионный ключ

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



Продукт	Описание
Авторизация	<b>Обязательный продукт.</b> Сервисы, расширяющие возможности обычной авторизации
<b>Авторизация.</b> Single sign-on аутентификация	SSO позволяет пользователю войти в систему один раз и получить доступ к нескольким связанным приложениям или сервисам
Система аудита действий пользователя	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)
Система BI-аналитики	<b>Beta</b>
<b>Система BI-аналитики.</b> Kafka внутри инсталляции	16 GB RAM, 8 vCPU
Базы Данных	Включение обратной совместимости с версиями VK WorkSpace для определенных сервисов, ранее поддерживающих только работу с MySQL.
<b>Базы Данных.</b> Использовать MySQL	
Инструменты разработки	Включает дополнительные сервисы для тестирования системы, например, генерирование аккаунтов
Поддержка Российских криптографических стандартов (ГОСТ TLS)	<b>Beta.</b> Позволяет VK WorkSpace работать с российскими криптографическими стандартами: ГОСТ Р 34.12-2015 (шифрование) и ГОСТ Р 34.10-2012 (электронные подписи). Это необходимо для обеспечения безопасного соединения
Система групповых политик	<b>Beta</b>
<b>Система групповых политик.</b> Kafka внутри инсталляции	16 GB RAM, 8 vCPU
Встроенное хранилище образов контейнеров	Хранения образов контейнеров почтовой системы внутри вашей инфраструктуры
VK Kubernetes	

Продукт	Описание
	Возможность развертывания в среде контейнеризации Kubernetes
Средства резервного копирования (бэкапирования)	Средства резервного копирования данных диска, почты, календарей, профилей пользователей и адресных книг
Система мониторинга	Набор сервисов, обеспечивающих хранение метрик сервисов в базе данных Prometheus и визуализацию данных с помощью Grafana
Система сбора и отправки метрик	Сборщики и трансляторы Graphite и Prometheus-метрик
Прогноз и контроль объёма почтового хранилища	<b>Beta.</b> Мониторинг заполнения хранилища почты
Интеграция с редактором «МойОфис» по протоколу WOPF	
OneDB Tarantool Groups	Переключает тарантулы выбранных групп на фреймворк OneDB
Редактор «P7-Офис» внутри инсталляции	Позволяет использовать встроенный в VK WorkSpace редактор «P7-Офис». Требует дополнительных ресурсов системы
Интеграция с редактором «P7-Офис» по протоколу WOPF	
Ядро объектного хранилища S3	<b>Обязательный продукт.</b> Сервисы обеспечивающие хранение любых неструктурированных данных по протоколу S3
<b>Ядро объектного хранилища S3.</b> Ядро распределённого файлового хранилища	<b>Обязательный продукт.</b> Отвечает за логику распределения данных по узлам, целостность и отказоустойчивость хранилища
Интеграция с Kerberos (SSO-авторизация)	Позволяет использовать SSO для авторизации в продуктах VK WorkSpace

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

4. Нажмите на кнопку **Далее**.

5. Включите нужные вам компоненты в разделе **Почта VK WorkSpace**.

Продукт	Описание
Система Antispam	Комплекс сервисов анализирующих письма и помечающих их как спам. Подробнее: <a href="#">Как включить Антиспам систему</a>
Календарь	<b>Обязательный продукт.</b> Продукт VK WorkSpace для управления календарями и событиями
<b>Календарь.</b> Миграция календарей по протоколу EWS	Миграция календарей пользователей из внешних систем для работы в VK WorkSpace. Миграция производится по протоколу EWS
<b>Календарь.</b> Интеграция календаря с TrueConf (сервер)	
<b>Календарь.</b> Интеграция календаря с TrueConf (плагин)	Для создания ссылок на звонки TrueConf при планировании встреч

Продукт	Описание
<b>Календарь.</b> Бот календаря для мессенджера VK WorkSpace	Настройки для автоматической отправки уведомлений о событиях Календаря в бот мессенджера VK WorkSpace
Поддержка протокола CardDAV	Синхронизации контактов между почтовой системой и клиентскими приложениями
API больших вложений VK WorkMail	<b>Обязательный продукт.</b> Набор сервисов для хранения больших вложений почты
Система расширенных транспортных правил	Настройки для управления потоками входящих и исходящих писем в целях усиления безопасности
Внешняя зона (DMZ)	Опция включает возможность создавать сервера для размещения их в DMZ-зоне. DMZ (Demilitarized Zone) — это изолированный сегмент сети, который находится между внешней (интернет) и внутренней (доверенной) сетью организации. Служит для размещения общедоступных сервисов, таких как веб-серверы, почтовые серверы и DNS-серверы, что позволяет минимизировать риски для внутренних ресурсов и сервисов
Управление размерами ящиков и политиками хранения писем в почтовых ящиках	<b>Beta.</b> Назначение групповых политик хранения на отдельные группы пользователей
Импорт данных из Microsoft Exchange	<b>Beta.</b> Сервис получения из MS Exchange in-place архивов, пользовательских правил обработки почты
Распределённая инсталляция	Возможность настройки связей между отдельно развёрнутыми инсталляциями для управления маршрутизацией почты, просмотра занятости пользователей в календарях и объединения контактов в общую адресную книгу. Неприменимо для инсталляции, развёрнутой в минимально рабочей конфигурации на одной виртуальной машине. Подробнее: <a href="#">Геораспределенная Почта VK WorkSpace</a>
	<b>Beta.</b> Дает возможность установить VK WorkSpace в катастрофоустойчивой конфигурации на двух ЦОД и

Продукт	Описание
Поддержка режима катастрофоустойчивости 2 ЦОД + witness	дополнительном сервере, не находящемся в этих двух ЦОД
Экспорт событий во внешний брокер (Kafka)	Позволяет настроить экспорт событий во внешнюю Kafka для дальнейшей аналитики
Редактирование данных во внешнем Active Directory	<b>Beta.</b> Сервис редактирования данных в Active Directory
Управление автоматическим удалением писем	<b>Beta.</b> Настройки управления автоматическим удалением писем
Бот новых почтовых сообщений для для мессенджера VK WorkSpace	Уведомления о новых полученных письмах будут отправляться в бот мессенджера VK WorkSpace
Автоматическое удаление старых писем	<b>Deprecated.</b> Дает возможность настраивать автоматическое удаление старых писем. Устаревшая функциональность
Компактная версия некоторых сервисов	Компактная версия сервисов обрабатывающих почтовые очереди
Интеграция с другими инсталляциями VK WorkSpace	<b>Deprecated.</b> Устаревшая версия геораспределенной Почты VK WorkSpace. Не поддерживается и не рекомендуется к включению
Система поиска писем во всех ящиках, доступна в интерфейсе Административной панели	Функциональность позволяет искать и удалять письма из интерфейса
Поддержка протокола POP3	Опция включает поддержку протокола POP3
Система отправки push-уведомлений на мобильные устройства	
Сервис анализа логов доставки почты	<b>Beta.</b> Включение набора сервисов обеспечивающих логирование почты. Хранит в базе данных сведения о получателе, отправителе, теме письма и времени

Продукт	Описание
	прохождения сообщения через сервера внутри установки

#### Примечание

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

6. Нажмите на кнопку **Далее**.

7. Включите нужные вам компоненты в разделе **Диск VK WorkSpace**.

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

8. Нажмите на кнопку **Далее**.

## Шаг 3. Добавьте гипервизоры (серверы)

1. Нажмите на кнопку **Добавить**.

2. В выпадающем меню выберите **Сервер**.

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.

---

Завершенные:     Сабконтейнеры:

колонок:     группировка:  роль

**Добавить** ▾

Сервер

Внешний кластер Kubernetes

Откроется окно добавления гипервизора:

Завершенные:  Сабконтейнеры:  колонок: 1 группировка: нет роль сервер

IP-адрес: 10.12.115.1 22

\* Имя сервера: hypervisor

\* Имя пользователя: centos

Пароль: .....

\* Приватный ключ: Использовать авторизацию по паролю

Метки: server Выберите значения для лейбла

+ Добавить метку

Пропустить проверку некритичных требований  Сервер во внешней (dmz) зоне

Добавить сервер Отмена

### 3. Заполните поля:

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

### 4. При необходимости добавьте **SSH-ключ**:

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

IP-адрес: 10.12.115.1 22

\* Имя сервера: hypervisor

\* Имя пользователя: centos

\* Приватный ключ: default

Метки: Использовать авторизацию по паролю

default

+ Добавить новый ключ

Пропустить проверку некритичных требований  Сервер во внешней (dmz) зоне

Добавить сервер Отмена

- 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.
- **Сервер во внешней (dmz) зоне** — Оставьте чекбокс пустым.

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

#### **Примечание**

При добавлении сервера реализована проверка на наличие команд **tar**, **scp** и необходимых инструкций виртуализации на процессорах. Если при проверке они не будут найдены, то сервер не будет добавлен, а администратор получит сообщение об ошибке.

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

## Шаг 4. Сетевые настройки

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

### 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**.

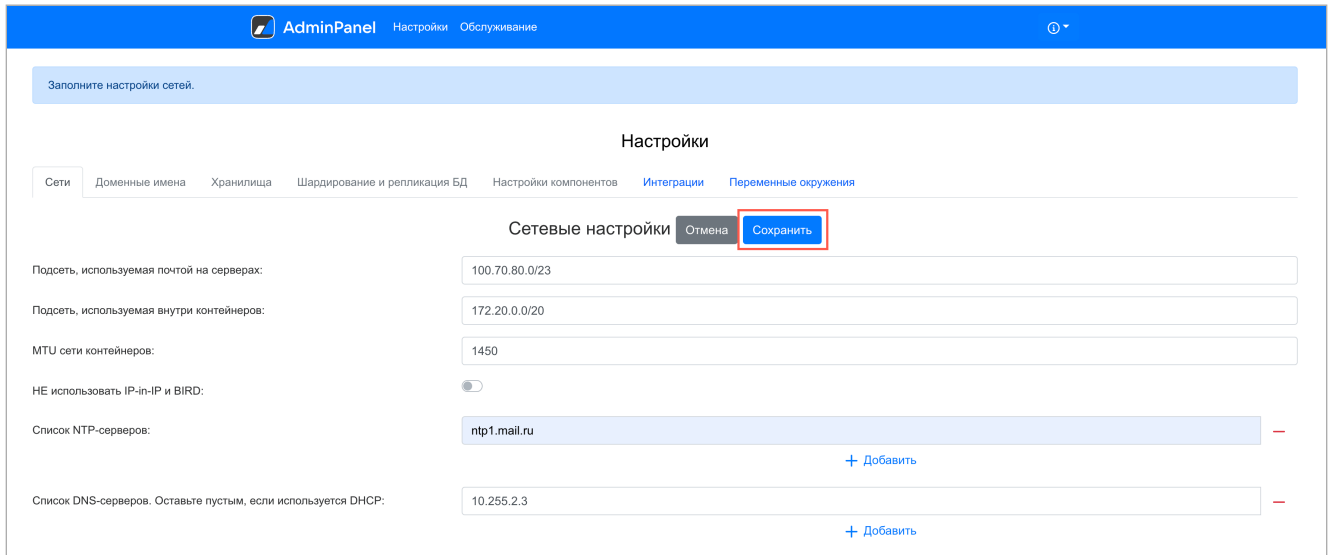
2. Убедитесь, что:

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

## Примечание

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

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). The main section is 'Сетевые настройки' (Network Settings). The 'Сохранить' (Save) button is highlighted with a red box. The form contains the following fields:

- 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 (with a '+ Добавить' button)
- Список DNS-серверов. Оставьте пустым, если используется DHCP: 10.255.2.3 (with a '+ Добавить' button)

## Шаг 5. Доменные имена

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

- Название вашей компании — введите название компании, которое будет отображаться в интерфейсе почты.
- Сайт вашей компании — укажите сайт вашей компании.
- Основной домен для сервисов — в поле необходимо указать ранее созданный основной домен для почты.
- Домен для облачных хранилищ — в поле введите ранее созданный домен для облачных хранилищ.

## Внимание

Основной домен для сервисов и домен для облачных хранилищ должны быть разными.

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 подставляются к подходящим доменам.

## Настройки

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

### Общие настройки доменов

Отмена Сохранить

Название вашей компании:

Моя компания

Заполните поле

Сайт вашей компании:

https://

Основной домен для сервисов:

mail.mycompany.ru

Заполните поле

Домен для облачных хранилищ:

st.mycompany.ru

Заполните поле

SSL-сертификаты:

Сохраните настройки доменов для добавления сертификатов

### 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**.

AdminPanel Настройки Обслуживание

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 и добавлению сертификатов. Добавленные сертификаты автоматически подставляются к подходящим доменам.

## Настройки

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

### Общие настройки доменов

SSL-сертификаты: **+ Добавить сертификат**

Название вашей компании: VK Communications

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

Основной домен для сервисов: vbastra0mail.onprem.ru

Домен для облачных хранилищ: vbastra0st.onprem.ru

### Настройки доменных имён 42

Домен для веб-интерфейса авторизации: account.vbastra0mail.onprem.ru

Ошибка: Не найден подходящий сертификат

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**

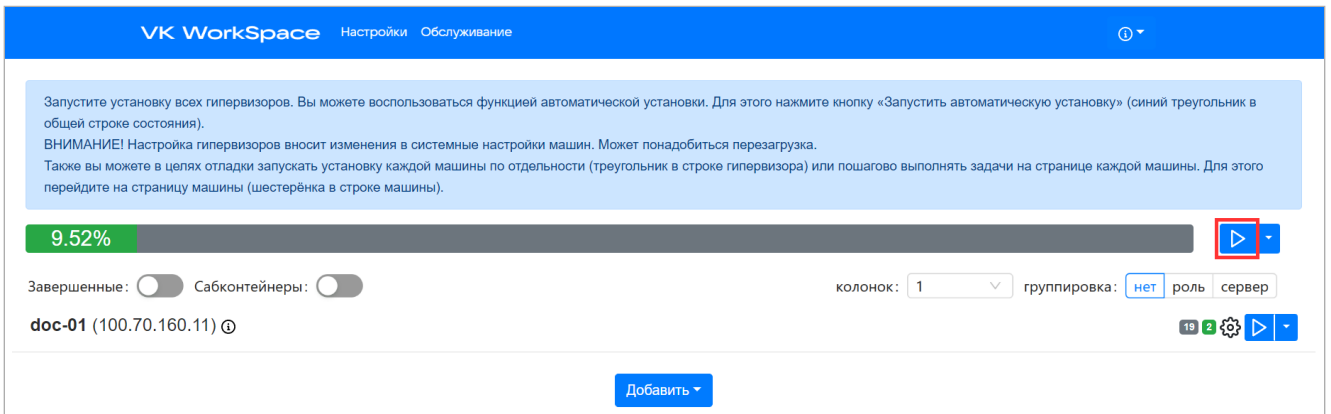
Приватный ключ должен быть добавлен в открытом виде, без секретной фразы. Закодированный ключ отличается от открытого наличием слова ENCRYPTED: BEGIN ENCRYPTED PRIVATE KEY .

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

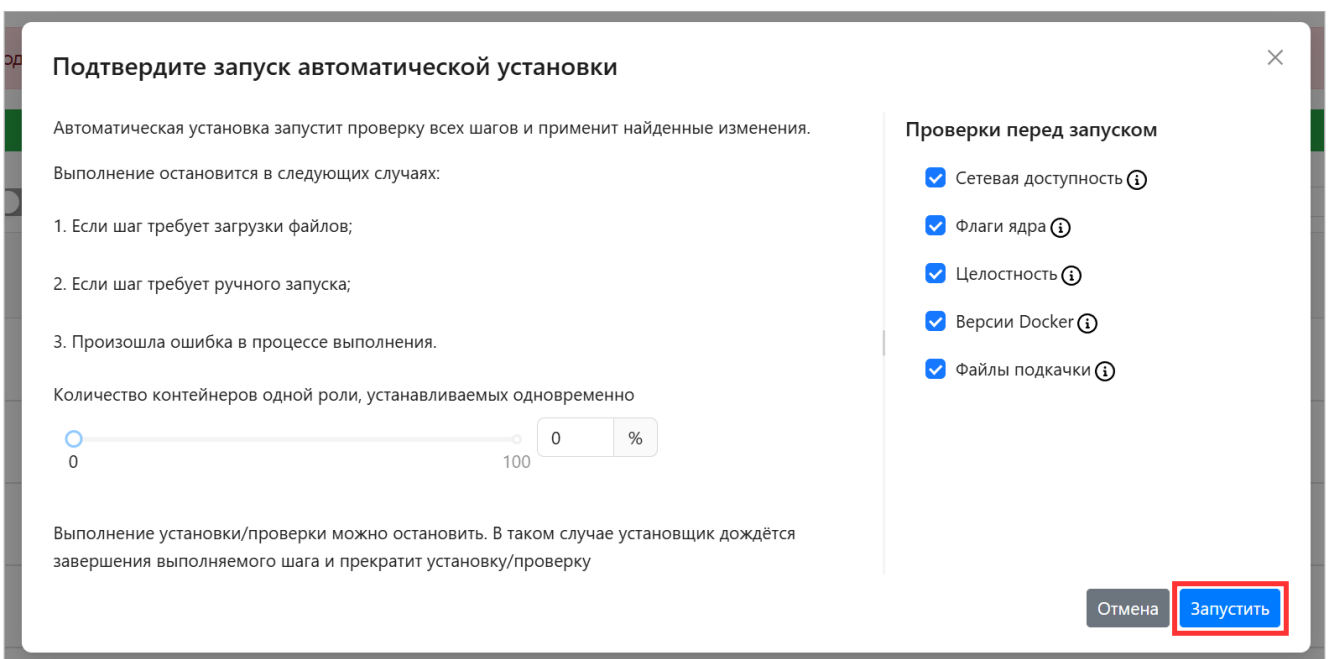
## Шаг 6. Запуск установки гипервизора

1. Нажмите на логотип в левом верхнем углу веб-интерфейса, чтобы перейти к общей строке состояния.

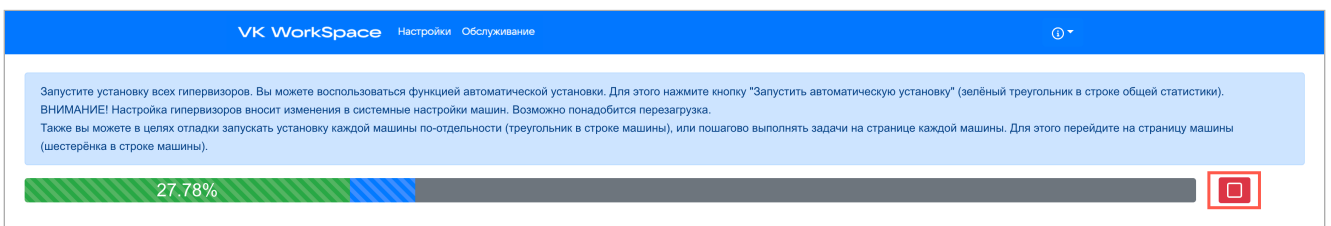
2. Кликните по кнопке **Play** (треугольник) рядом с общей строкой состояния в верхней части экрана.



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



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

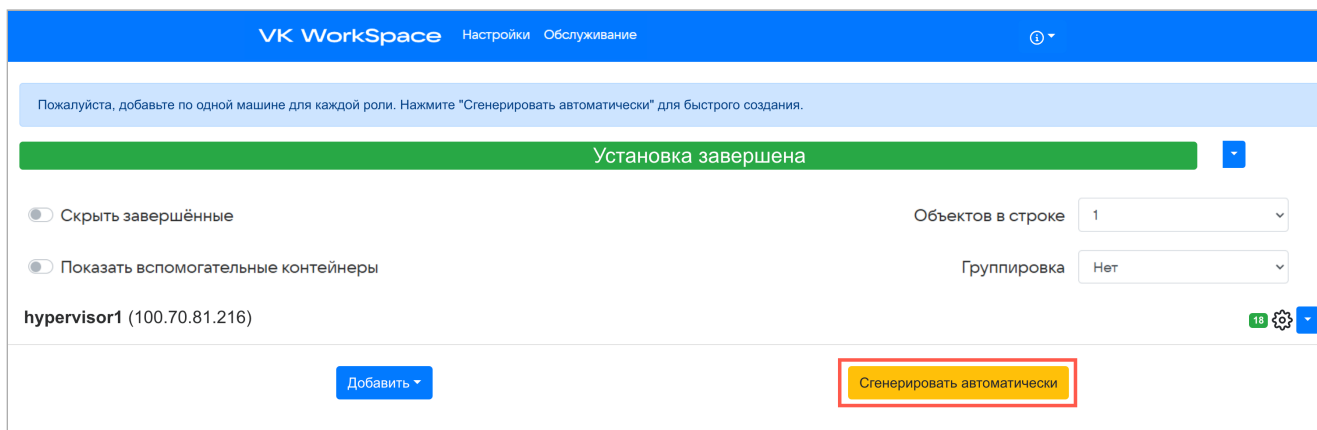


В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуется повторный запуск автоматической установки.

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

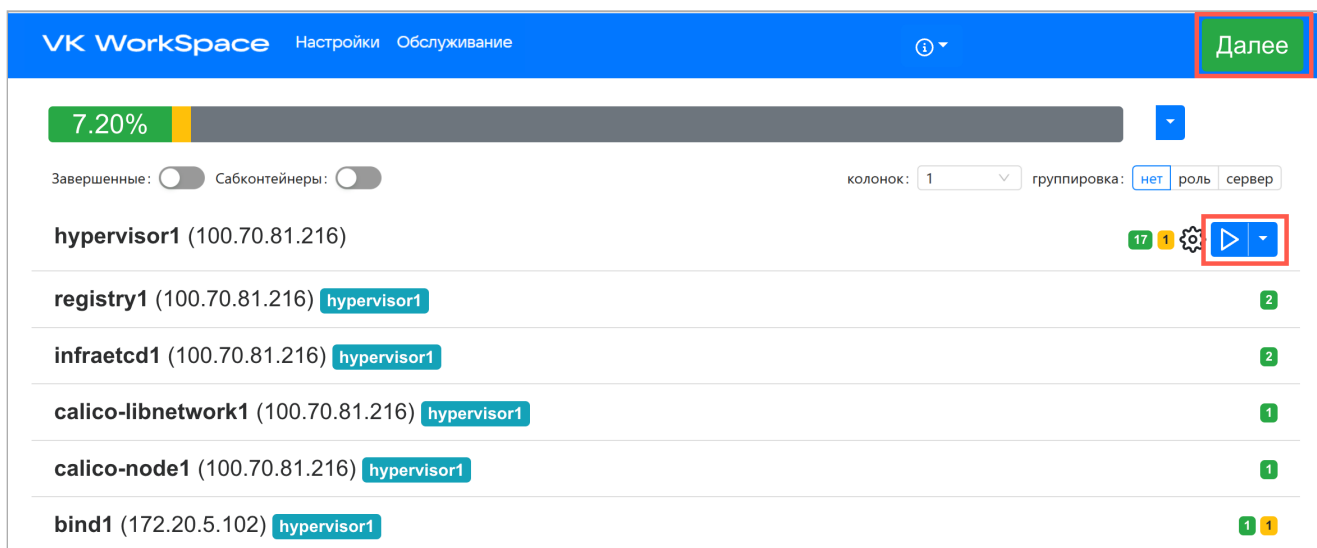
# Шаг 7. Генерация контейнеров

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



На экране начнут появляться сгенерированные контейнеры. В случае появления ошибок используйте раздел [Логи и полезные команды](#).

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



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

## Подтвердите запуск всех задач на **hypervisor1**

После запуска шагов остановить их выполнение будет невозможно.

Выполнение остановится в следующих случаях:

1. Если шаг требует загрузки файлов;
2. Если шаг требует ручного запуска;
3. Произошла ошибка в процессе выполнения.

Отмена

Запустить

Объектов в с

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**.

Service Name	IP Address	Status
del2	172.20.2.132	Не отвечает гипервизор
del2	172.20.2.132	front2
del2	172.20.2.132	del-mailloader2, del-zeptoproxy2, del-zubr2, del-donjuan2, del-aestat2, del-envoy2
bizf2	172.20.2.183	Не отвечает гипервизор
bizf2	172.20.2.183	front2
bizf2	172.20.2.183	biz-envoy2
mpop2	172.20.2.188	Не отвечает гипервизор
mpop2	172.20.2.188	front2
mpop2	172.20.2.188	mpop-zubr2, mpop-donjuan2, mpop-aestat2, mpop-ameli2, mpop-zp2, mpop-envoy2, mpop-apache-exporter2, mpopd-far2, mpopd-scn2, mpopd-m2, mpopd-pn2, mpopd-mspq2, mpopd-ls2, mpopd-recaller2
panda2	172.20.2.190	Не отвечает гипервизор
panda2	172.20.2.190	front2
panda2	172.20.2.190	panda-zubr2, panda-donjuan2, panda-aestat2, panda-delivery-canceller2, panda-envoy2
biz-celery-worker-pdd2	172.20.3.3	Не отвечает гипервизор
biz-celery-worker-pdd2	172.20.3.3	front2
biz-celery-worker-pdd2	172.20.3.3	biz-celery-worker-pdd-envoy2
biz-celery-worker-pdd-check2	172.20.3.8	Не отвечает гипервизор
biz-celery-worker-pdd-check2	172.20.3.8	front2
biz-celery-worker-pdd-check2	172.20.3.8	biz-celery-worker-pdd-check-envoy2
biz-celery-worker-pdd-high2	172.20.3.1	Не отвечает гипервизор
biz-celery-worker-pdd-high2	172.20.3.1	front2
biz-celery-worker-pdd-high2	172.20.3.1	biz-celery-worker-pdd-high-envoy2
biz-celery-worker-pdd-update2	172.20.3.11	Не отвечает гипервизор
biz-celery-worker-pdd-update2	172.20.3.11	front2
biz-celery-worker-pdd-update2	172.20.3.11	biz-celery-worker-pdd-update-envoy2
fallback2	172.20.2.135	Не отвечает гипервизор
fallback2	172.20.2.135	front2
fallback2	172.20.2.135	fallback-zubr2, fallback-aestat2, fallback-envoy2, fallback-reexim2, fallback-relmtpd2
fallback-dlp2	172.20.2.136	Не отвечает гипервизор
fallback-dlp2	172.20.2.136	front2
fallback-dlp2	172.20.2.136	fallback-dlp-zubr2, fallback-dlp-aestat2, fallback-dlp-envoy2, fallback-dlp-reexim2, fallback-dlp-relmtpd2
mx2	172.20.2.138	Не отвечает гипервизор
mx2	172.20.2.138	front2
mx2	172.20.2.138	mx-zubr2, mx-reexim2, mx-relmtpd2, mx-aestat2, mx-envoy2
relay2	172.20.2.137	Не отвечает гипервизор
relay2	172.20.2.137	front2
relay2	172.20.2.137	relay-zubr2, relay-aestat2, relay-envoy2, relay-reexim2, relay-relmtpd2
smtp2	172.20.2.133	Не отвечает гипервизор
smtp2	172.20.2.133	front2

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.

## 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

[Запустить](#) ⌵

#### disable\_NM\_for\_cali done

Отключить NetworkManager (если он есть) для сетевых интерфейсов Calico

[Запустить](#) ⌵

#### disable\_firewall done

Отключить межсетевой экран (firewall)

[Запустить](#) ⌵

#### disable\_selinux 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](#) ⌵

#### check\_needed\_packs done

Проверить наличие Docker и Docker Compose

[Запустить](#)

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

Название машины	IP	SSH-порт	Имя гипервизора
<input type="text" value="hypervisor1"/>	<input type="text" value="100.70.80.79"/>	<input type="text" value="22"/>	<input type="text" value="mail-vkwm2-st1"/>
Имя пользователя	Пароль	Приватный ключ	Data Center
<input type="text" value="deployer"/>	<input type="password" value="....."/>	<input type="text" value="vkwm2"/> ⌵	<input type="text" value="astra"/>
Интерфейс для межсерверного взаимодействия			
<input type="text" value="100.70.80.79 (eth0)"/> ⌵			
Теги			
<input type="text" value="st"/>			
<input type="checkbox"/> Пропустить проверку некритичных требований			
		<input type="button" value="Отмена"/>	<input type="button" value="Обновить"/>

## 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

[Запустить](#) ⌵

Повторно запустите автоматическую установку.







## Шаг 8. Хранилища

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

### Настройки

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

#### Временные вложения

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


[Добавить](#) или [сгенерировать](#) дисковые пары

Данные о дисках от 14.03.2024, 12:01:31. [Обновить](#)

## Шаг 9. Шардирование и репликация БД


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


### VK WorkSpace

Настройки Обслуживание Настройки  **Далее**

#### Настройки

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

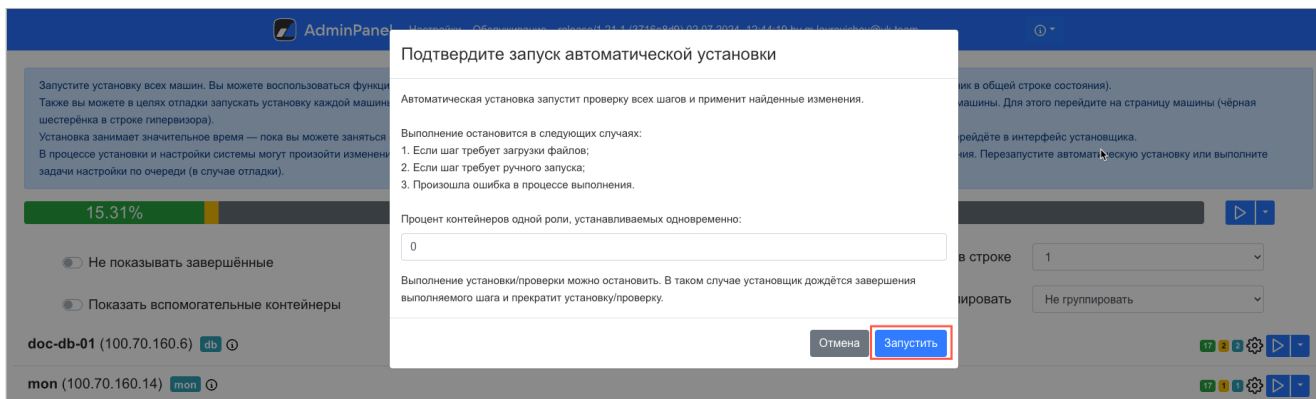
Сначала кластера БД с проблемами  [Опросить базы данных](#)

Имя БД	Номер кластера	Отказоустойчивость	Мастер 	Состав
addrbook-onedb	1	Overlord	addrbook-onedb1 release-vkwm-02-database-astra-1	addrbook-onedb1 addrbook-onedb2
alisa-onedb	1	Overlord	alisa-onedb1 release-vkwm-02-database-astra-1	alisa-onedb1 alisa-onedb2
appass-onedb	1	Overlord	appass-onedb1 release-vkwm-02-database-astra-1	appass-onedb1 appass-onedb2

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

## Шаг 10. Запуск установки всех машин

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



В зависимости от этапа генерации будет меняться цвет индикатора:

- **Серый** — в ожидании начала генерации;
- **Синий** — в процессе генерации;
- **Желтый** — шаг необходимо повторить (установщик делает это самостоятельно);
- **Красный** — ошибка.

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

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

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

## Шаг 11. Завершение установки, инициализация домена и вход в панель администратора

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

1. Нажмите на кнопку **Далее**.

AdminPanel Настройки Обслуживание Далее

Установка завершена

Не показывать завершённые
 Объектов в строке: 1

Показать вспомогательные контейнеры
 Группировать: Не группировать

doc-db-01 (100.70.160.6)	db	15 2
mon (100.70.160.14)	mon	16 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 почтового домена и нажмите на кнопку **Добавить**.

**Внимание**

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

AdminPanel Настройки Обслуживание i

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

Почтовые домены Контейнеры

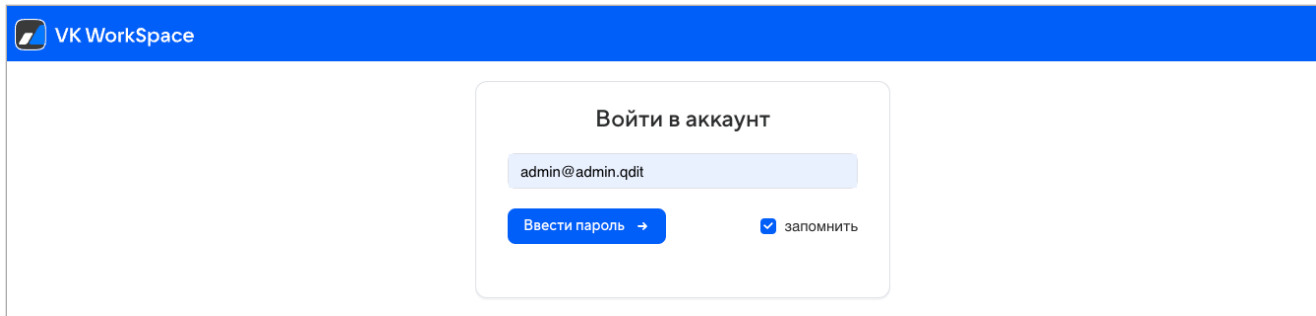
vbastra0mail.onprem.ru + Добавить

Откроется новая вкладка, на которой необходимо авторизоваться:

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

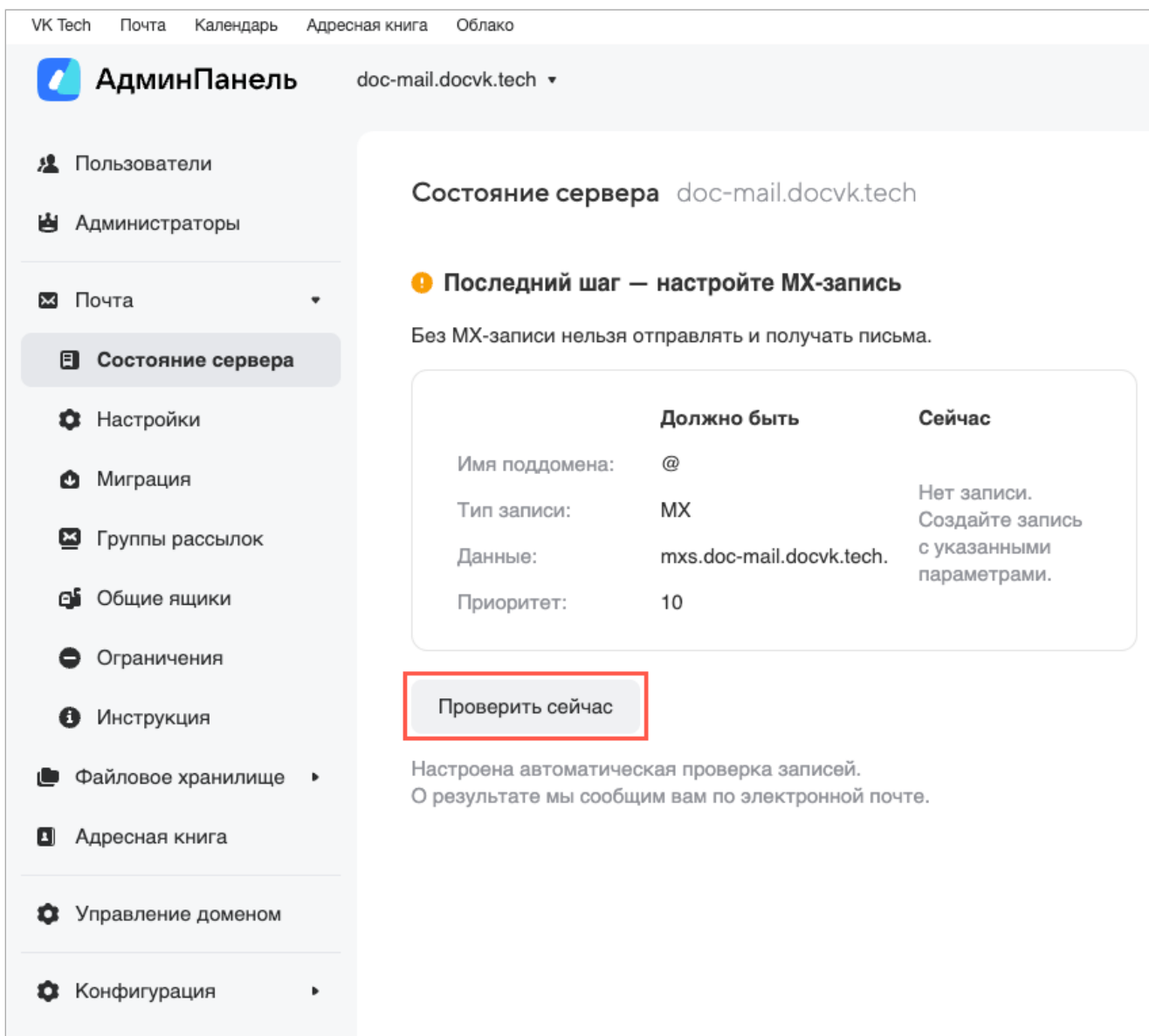
**Примечание**

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



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

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



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

VK Tech Почта Календарь Адресная книга Облако

AdminPanel vbastra0mail.onprem.ru

Пользователи  
Администраторы  
Почта  
Состояние сервера  
Настройки  
Миграция  
Группы рассылок  
Общие ящики  
Инструкция  
Файловое хранилище  
Адресная книга  
Структура компании  
Управление доменом  
Конфигурация

### Состояние сервера vbastra0mail.onprem.ru

**✓ МХ-записи настроены верно**  
Вы можете отправлять и получать письма.

**⚠ SPF-запись не настроена**  
SPF позволяет владельцу домена указать в TXT-записи домена строку, указывающую список серверов, имеющих право отправлять email-сообщения с обратными адресами в этом домене.  
[Инструкция по настройке](#)  
На обновление записей может потребоваться до 72 часов.

**⚠ Необходима настройка DNS записей для работы DKIM**  
Письма, отправленные с вашего домена, не подписываются специальной подписью и могут попадать в спам.

Имя поддомена:	mailru._domainkey
Тип записи:	TXT
Данные:	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlc2 3h3A6tEFx/oSdVhWBtSoArt15wVqMgdhtWsK3WnYj95g8hUV hqKIErA13MUX1WGIvC/mfSnTlcBMVDOPWYTE2C3WbD4d RtwvMI5MfhD2EUExVagkpmE2aYqTNL71NXknUciGPEzHXKh svW9vVTm0p2t9qLFoazitpkzZkpBwIDAQAB

[Инструкция по настройке](#)

После проверки **МХ-записи** установку можно считать оконченной.

#### **⚠ Внимание**

По завершении установки допускается только удаление архива, из которого был распакован дистрибутив в начале установки. Все остальные файлы должны оставаться в папке с файлом **onpremise-deployer\_linux**.

Не удаляйте пользователя `deployer` — эта учетная запись потребуется для обновления и дальнейшей эксплуатации сервиса почты.

## Альтернативный способ проверить МХ-запись

При тестовой установке необязательно иметь правильную МХ-запись, вы можете проверить ее другим способом, чтобы работать с локальным трафиком:

1. Перейдите по адресу `https://biz.server-address/admin/misc/pdd/domain/`.
2. Кликните по домену в списке.

ПАНЕЛЬ УПРАВЛЕНИЯ ЗАКЛАДКИ ПРИЛОЖЕНИЯ АДМИНИСТРИРОВАНИЕ USERS SPECIALS

Главная > Pdd > Domains

Выберите domain для изменения

🔍

Действие: -----  Выбрано 0 объектов из 1

<input type="checkbox"/>	NAME	TYPE	DOMAIN VERSION	ПОДТВЕРЖДЕН?	ФИЧИ	IS ALIAS	USER COUNT	BLOCKED ADMIN AND ALL EMAILS	CREATED AT	UTM SOURCE
<input type="checkbox"/>	<b>doc-mail.docvk.tech</b>	Сайт	2	HTML-файл	deleted-mails-folder, paid-mail	+	0	+	25 июля 2024 г. 12:09	

3. В поле **Mx status** выберите пункт **Есть необходимая MX-запись**.

Главная > Pdd > Domains > doc-mail.docvk.tech (1)

Изменить domain ИСТОРИЯ

Основные

Name:  Тип:  Ступе:

**Mx status:**  Spf status:

Ns status:

Mx ok at: Дата: 31.07.2024 Сегодня  Время: 13:33:20 Сейчас

Mx bad at: Дата:  Сегодня  Время:  Сейчас

Внимание: Ваше локальное время опережает время сервера на 3 часа.

4. Сохраните изменения.

В панели администратора появится уведомление о том, что **MX-запись** настроена верно:

VK Tech Почта Календарь Адресная книга Облако

AdminPanel vbastra0mail.onprem.ru

Пользователи Администраторы Почта **Состояние сервера** Настройки Миграция Группы рассылки Общие ящики Инструкция Файловое хранилище Адресная книга Структура компании Управление доменом Конфигурация

**Состояние сервера vbastra0mail.onprem.ru**

✅ **MX-записи настроены верно**  
Вы можете отправлять и получать письма.

⚠️ **SPF-запись не настроена**  
SPF позволяет владельцу домена указать в TXT-записи домена строку, указывающую список серверов, имеющих право отправлять email-сообщения с обратными адресами в этом домене.  
[Инструкция по настройке](#)  
На обновление записей может потребоваться до 72 часов.

⚠️ **Необходима настройка DNS записей для работы DKIM**  
Письма, отправленные с вашего домена, не подписываются специальной подписью и могут попадать в спам.

Имя поддомена: mailru.\_domainkey

Тип записи: TXT

Данные: v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKgQDic23h3A6tEFx/0sDvhWBtSoArt15wVqMgdhtWsK3WnYj95g8hUVhqKIErA13MUX1WGiVC/mfSnTlcBMVD0pWYTE2C3WbD4dRtwvMl5MfhD2EUExVagkpm2aYqTNL71NXknUclGPEzHXKhsvW9vVTm0p2i9qLFoaztpkzZkpBwIDAQAB

[Инструкция по настройке](#)

# 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 какого-то конкретного контейнера:

```
sudo journalctl -eu имя_контейнера
```

5. Статус контейнера:

```
systemctl status имя_контейнера
```

6. Посмотреть список «сломанных» контейнеров:

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

7. Посмотреть список всех не запустившихся контейнеров:

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

 Автор: Груздев Никита

 11 марта 2026 г.