

Установка тестовой версии Почты VK WorkSpace на одну машину

Тестовая установка

Назначение документа	4
Требования к администраторам	4
Технические требования	4
Требования к ресурсам сервера	6
Предварительные условия для установки	6
Как работать с Wildcard-сертификатами	7
Какие протоколы использует Почта	7
Обязательные предварительные действия	8
Создание DNS-записей	8
Дисковое пространство	11
Этапы установки	11
Действия в командной строке на сервере	12
Шаг 1. Создание пользователя deployer	12
Шаг 2. Распаковка дистрибутива	13
Шаг 3. Разрешить Port Forwarding	14
Шаг 4. Запуск установщика как сервиса	14
Действия в веб-интерфейсе установщика	15
Шаг 1. Выбор варианта установки	15
Шаг 2. Выбор продуктов	16
Шаг 3. Добавление лицензионного ключа	16
Шаг 4. Добавление гипервизора	17
Шаг 5. Сетевые настройки	19
Шаг 6. Доменные имена	21
Добавление SSL-сертификатов	21
Шаг 7. Запуск установки гипервизора	23
Шаг 8. Генерация контейнеров	24
Шаг 9. Хранилища	28
Шаг 10. Шардирование и репликация БД	28
Шаг 11. Запуск установки всех машин	29

Шаг 12. Завершение установки, инициализация домена и вход в панель администратора	29
Альтернативный способ проверить MX-запись	32
Дополнительная документация	34
Логи и полезные команды	34

Назначение документа

В документе описана тестовая установка Почты 1.24 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.

Технические требования

Поддерживаемые операционные системы для установки Почты:

- **Astra Linux SE Опел** — версия 1.7.3.
- **РЕД ОС** — версия 7.3.2.
- **РЕД ОС** — версия 7.3с (сертифицированная).

Версия ядра — **5.15**; архитектура системы — **x86_64**.

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

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
```

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:

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

```
DefaultLimitNOFILE=524288:524288
```

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

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

Требования к ресурсам 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**.

Предварительные условия для установки

Представители VK предоставили вам следующие данные:

- ссылку на скачивание дистрибутива Почты 1.24,
- 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.

Внимание

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 четыре домена:

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

Какие протоколы использует Почта

- **CalDav** для синхронизации календаря;
- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента;
- **HTTPS** для доступа к веб-интерфейсу почты с использованием **TLS**;
- **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);

Обязательные предварительные действия

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	account	account.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

Назначение домена	Имя домена	Пример
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 VK Teams	calendarmsg	calendarmsg.mail.onprem.ru
Мобильный календарь	calendartouch	calendartouch.mail.onprem.ru
Статические данные календаря	calendarx	calendarx.mail.onprem.ru
VK WorkDisk	cloud	cloud.mail.onprem.ru
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

Назначение домена	Имя домена	Пример
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
Общепортальные сервисы авторизации	portal	portal.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

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

Назначение домена	Имя домена	Пример
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
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

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
```

Внимание

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

2. Выполните команду `sudo visudo`.
3. В файле `/etc/sudoers` уберите `#` в начале следующей строки:

Astra Linux

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

РЕД ОС

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

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

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

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

Шаг 2. 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>
```



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-proxy).

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

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

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

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

Ответ в случае успешного запуска установщика выглядит следующим образом:

Astra Linux

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

РЕД ОС

```
The authenticity of host 'localhost (:::1)' can't be established.
ED25519 key fingerprint is SHA256:g8si032KUsRU9oC/MHro9WaTNKj4R+DkmVnVa7QsYCo.
This key is not known by any other names
# Введите "yes" и нажмите Enter, чтобы подтвердить подключение
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Примечание

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

Действия в веб-интерфейсе установщика

Для перехода в веб-интерфейс в адресной строке браузера необходимо указать 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**.

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

1. Включите флаг **VK WorkMail**.
2. В открывшемся списке отметьте **VK WorkDisk**.
3. 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

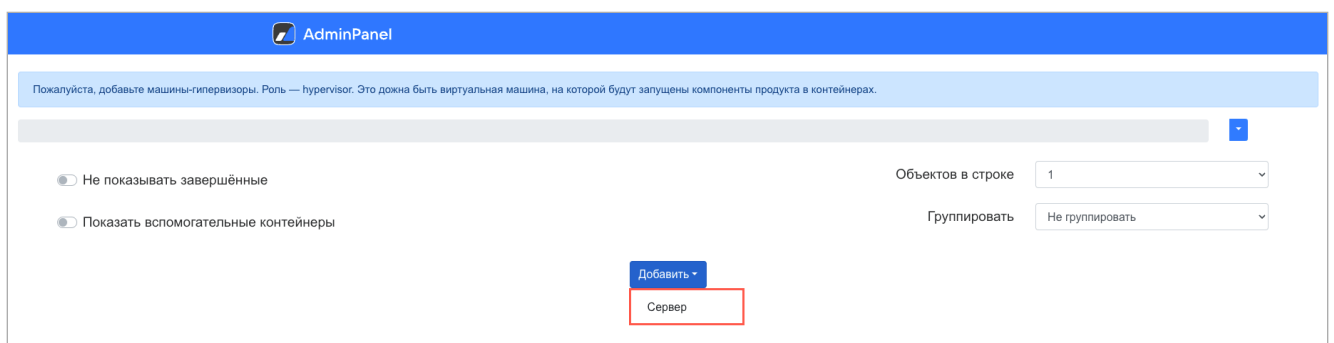
Лицензия 0187e174-d83f-75c2-806f-8408d935b622 для onprem.ru. Количество пользователей: VK WorkMail - 10000, VK WorkDisk - 10000, VK Teams - 10000. Разрешённые почтовые домены: "*.onprem.ru", "admin.qdit". Действительна до 02.05.2025, 11:53:32

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**.



Откроется окно добавления гипервизора:

AdminPanel

Пожалуйста, добавьте машины-гипервизоры. Роль — hypervisor. Это должна быть виртуальная машина, на которой будут запущены компоненты продукта в контейнерах.

☐ Не показывать завершённые

Объектов в строке 1

☐ Показать вспомогательные контейнеры

Группировать Не группировать

Роль

hypervisor

IP

100.70.160.14

SSH-порт

22

Имя гипервизора

mon

Имя пользователя

centos

Пароль

strongPass

Приватный ключ

Использовать авторизацию по паролю

Data Center

mon

Теги

store,mail,etc...

☐ Пропустить проверку некритичных требований

Отмена

Добавить

3. Заполните поля:

- **Роль** — hypervisor.
- **IP** — адрес машины, на которую производится установка.
- **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.
- **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.

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

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

IP

10.12.15.1

SSH-порт

22

Пароль

.....

Приватный ключ

✓ Использовать авторизацию по паролю

+ Добавить новый ключ

Отмена

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.

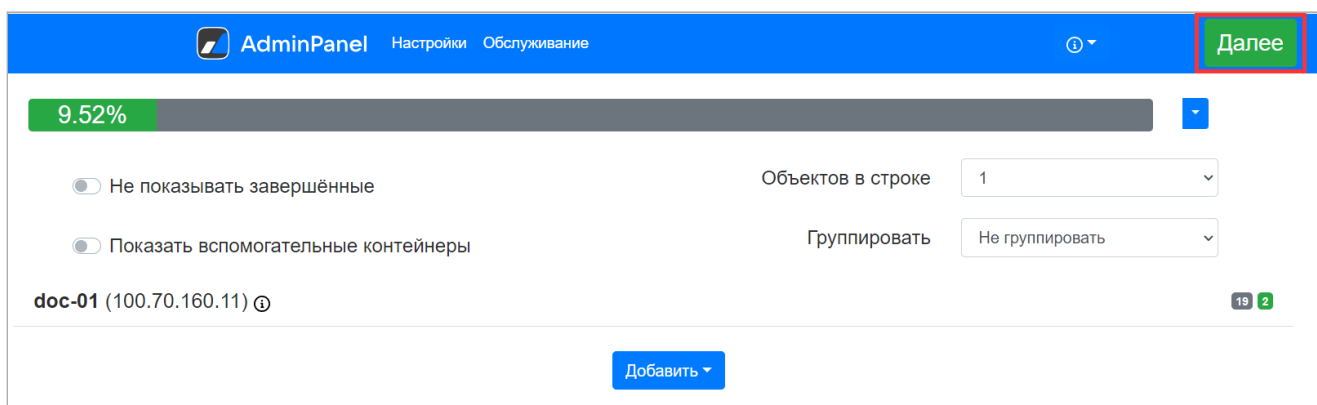
г. Кликните по кнопке **Сохранить**.

5. При необходимости настройте дополнительные поля:

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

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

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.

Заполните настройки сетей.

Настройки

Сети

Доменные имена

Хранилища

Шардирование и репликация БД

Настройки компонентов

Интеграции

Переменные окружения

Настройки сетевого взаимодействия

Отмена

Сохранить

Подсеть, используемая почтой на серверах:

100.70.160.0/27

Подсеть, используемая внутри контейнеров:

172.20.0.0/20

MTU сети контейнеров:

1450

НЕ использовать IP-in-IP и BIRD:



Список DNS-серверов. Оставьте пустым, если используется DHCP:

10.255.2.3

+ Добавить

1. Укажите **DNS-сервер**.

2. Убедитесь, что:

- **Подсеть, используемая почтой 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. По умолчанию используется 20-я подсеть.

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



AdminPanel

Настройки

Обслуживание



Заполните настройки сетей.

Настройки

Сети

Доменные имена

Хранилища

Шардирование и репликация БД

Настройки компонентов

Интеграции

Переменные окружения

Сетевые настройки

Отмена

Сохранить

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

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 поменять 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 поменять 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

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

SSL-сертификаты: [+ Добавить сертификат](#)

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**.

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

Домен для веб-интерфейса авторизации:

account.doc-mail.docvk.tech

Домен для скачивания вложений VK WorkMail:

af.doc-mail.docvk.tech

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

✎

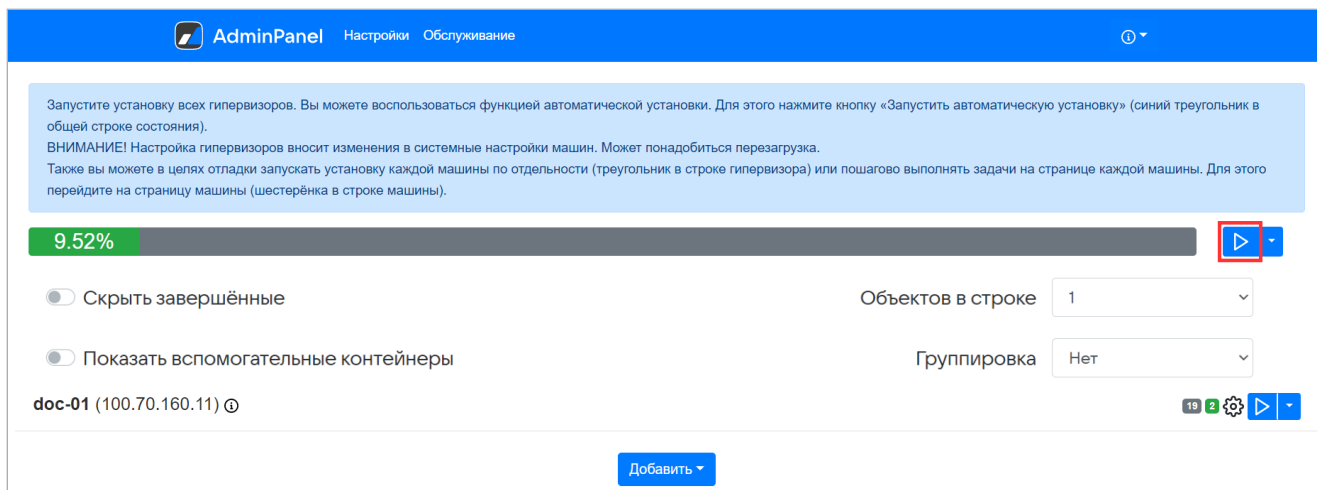
Сертификаты:

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

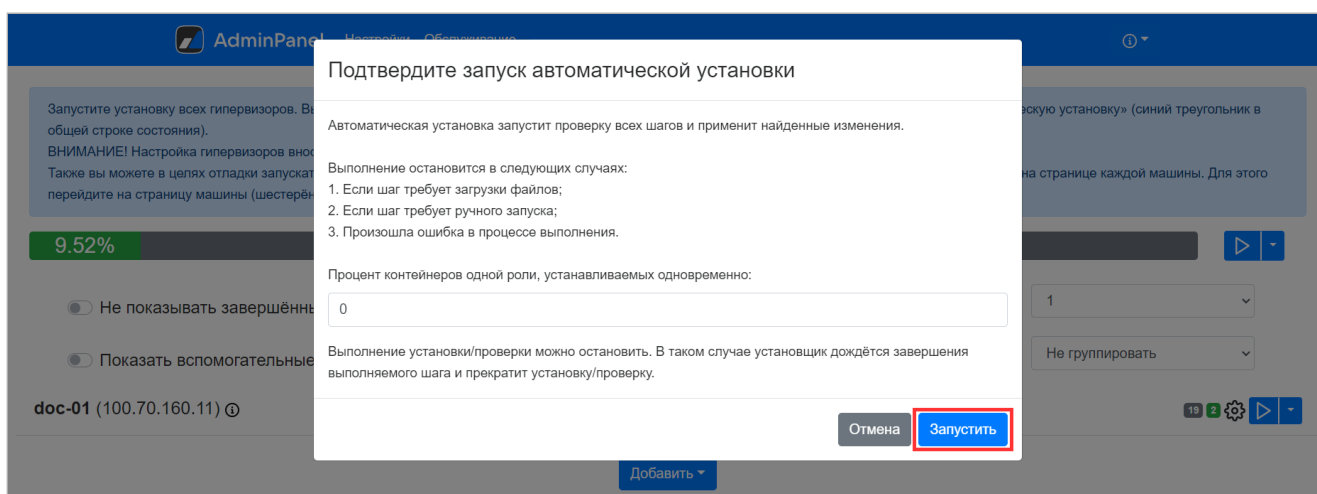
✎

Шаг 7. Запуск установки гипервизора

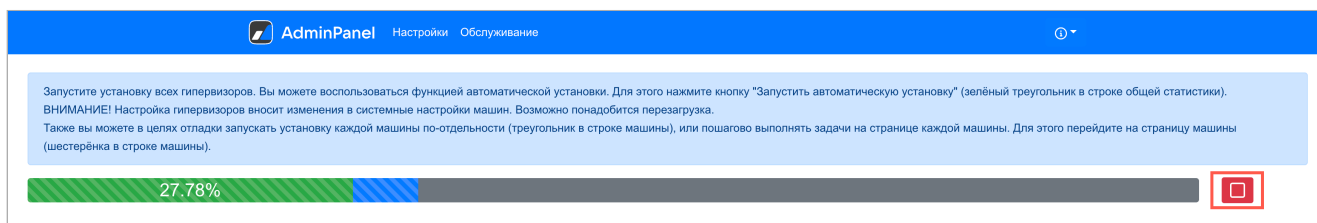
1. Нажмите на логотип **AdminPanel**, чтобы перейти к общей строке состояния.
2. Кликните по кнопке **Play** (треугольник) рядом с общей строкой состояния в верхней части экрана.



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



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

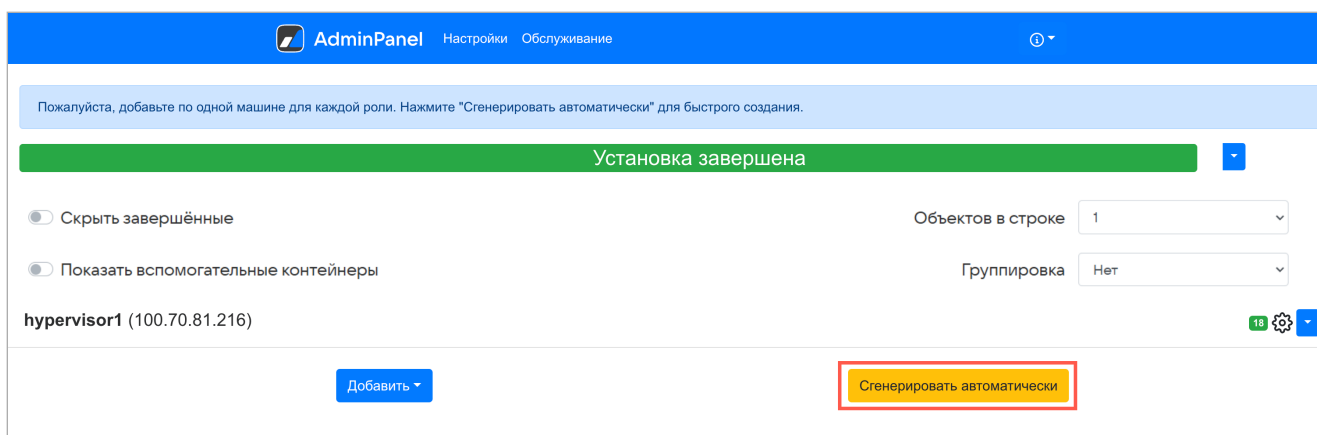


В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуются повторный запуск автоматической установки.

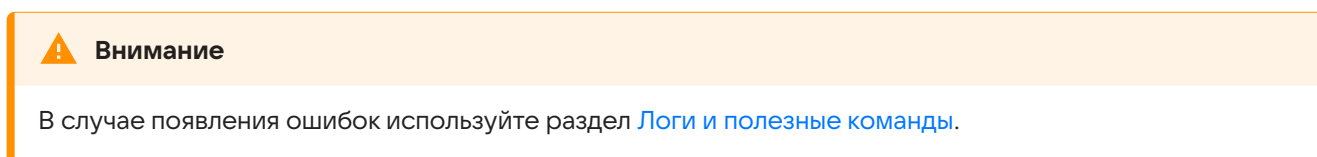
Для повторного запуска нажмите на кнопку **Play** в верхней общей строке состояния или рядом с названием гипервизора.

Шаг 8. Генерация контейнеров

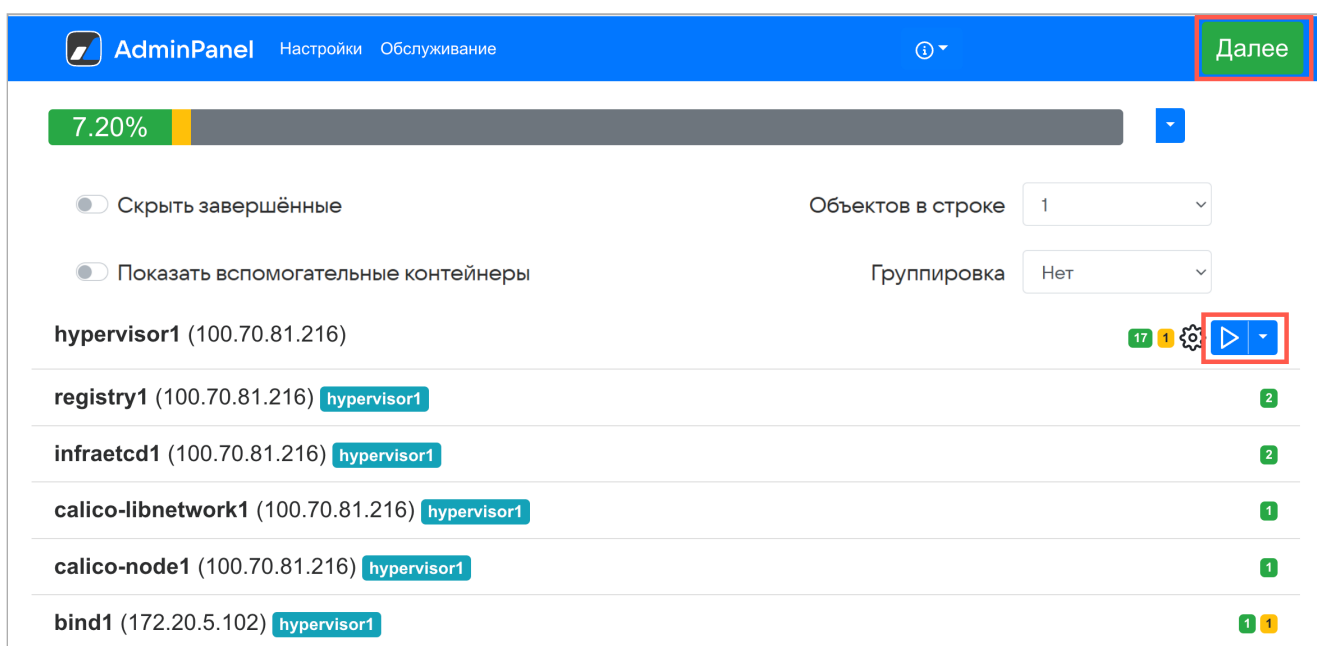
1. Нажмите на кнопку **Сгенерировать автоматически**, чтобы добавить по одному контейнеру для каждой роли.



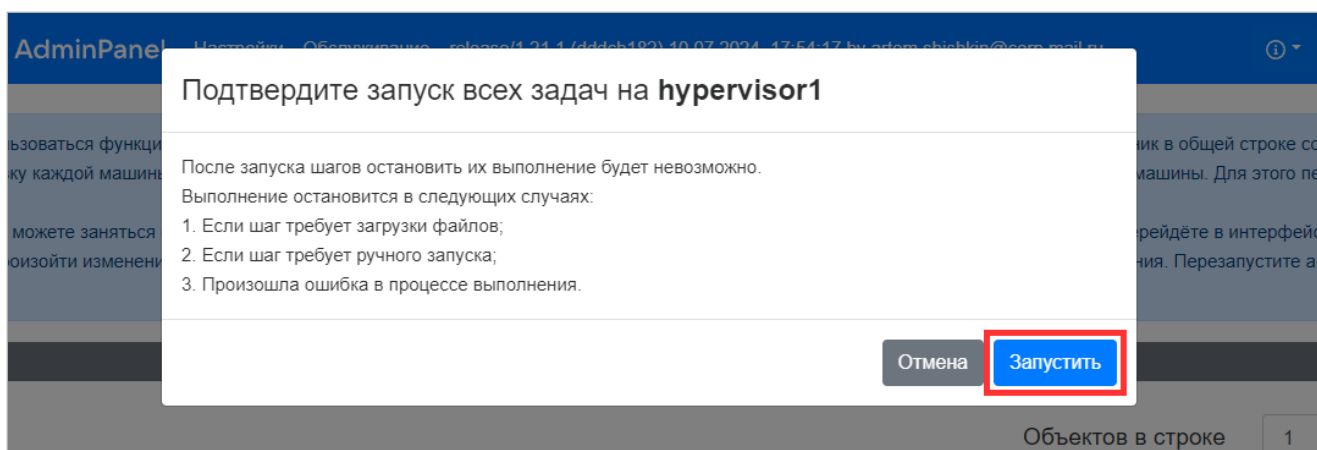
На экране начнут появляться сгенерированные контейнеры.



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**.

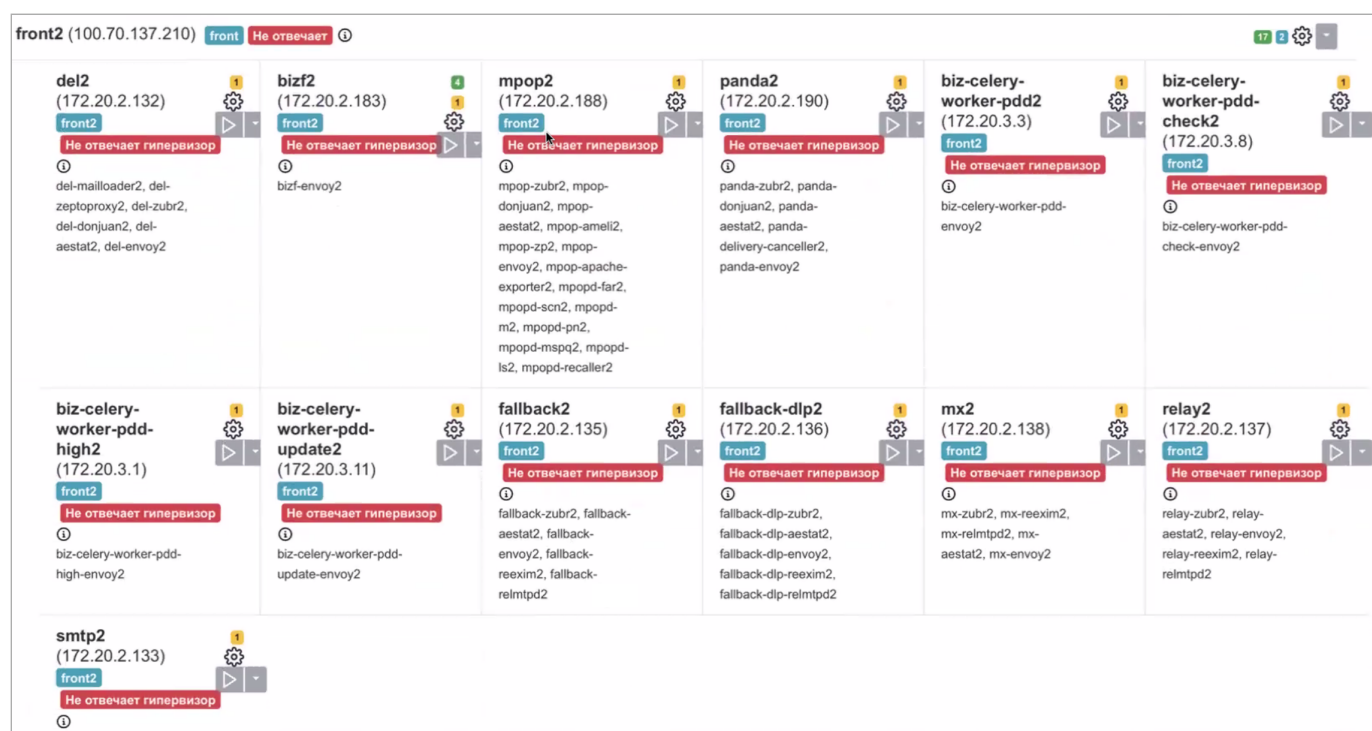


4. На генерацию требуется время. Подождите, пока исчезнет кнопка **Play** напротив гипервизора.

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**.



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
hypervisor1	100.70.80.79	22	mail-vkwm2-st1
Имя пользователя	Пароль	Приватный ключ	Data Center
deployer		vkwm2 	astra
Интерфейс для межсерверного взаимодействия			
100.70.80.79 (eth0) 			
Теги			
st			
☐ Пропустить проверку некритичных требований			
		Отмена	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 9. Хранилища

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

Настройки

СетиДоменные именаХранилищаШардирование и репликация БДНастройки компонентовИнтеграцииПеременные окружения

cldst

cldmetast

blobcloud

mailcloud

zepto_del

zepto_main

zepto_opt

zepto_skel

zepto_search

crow_index

mescalito

fstab

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 10. Шардирование и репликация БД

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

AdminPanel

НастройкиОбслуживание

Далее

Настройки

СетиДоменные именаХранилищаШардирование и репликация БДНастройки компонентовИнтеграцииПеременные окружения

Загрузить из базы

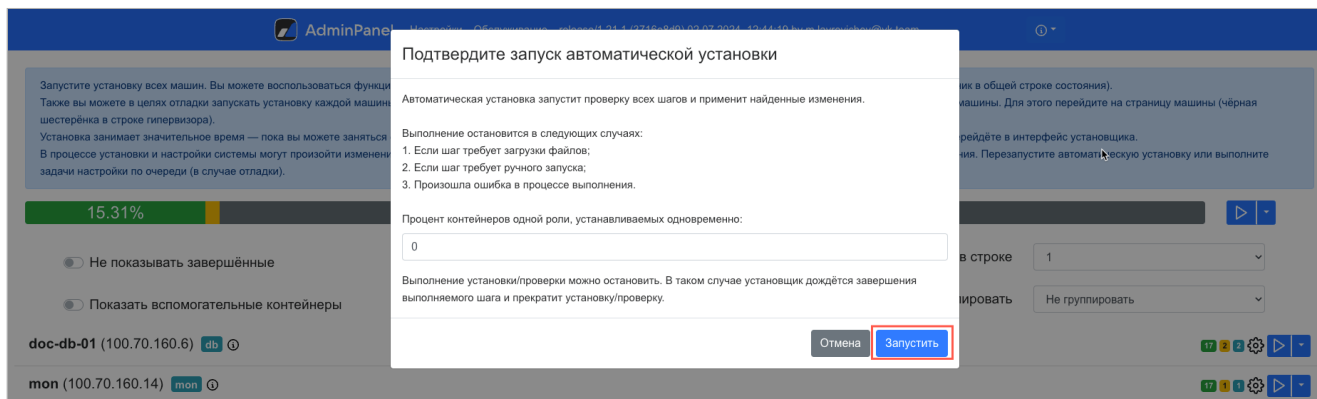
Опросить все Overlord'ы

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. 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**.

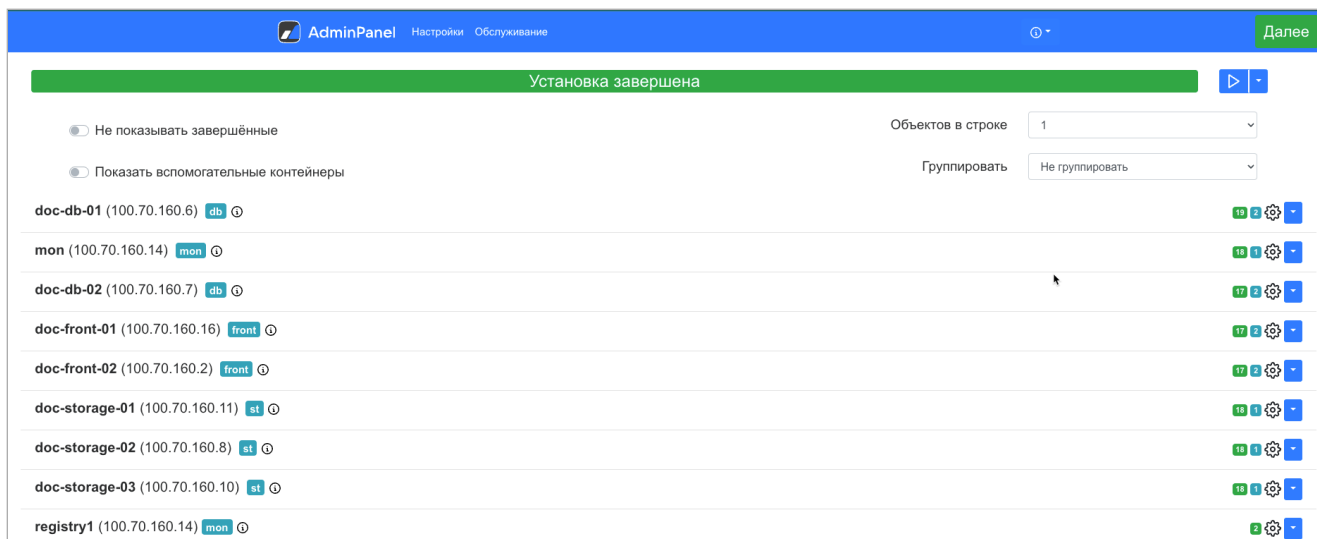
Если в процессе установки и настройки системы происходят изменения конфигурации, некоторые задачи могут потребовать повторного выполнения.

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

Шаг 12. Завершение установки, инициализация домена и вход в панель администратора

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

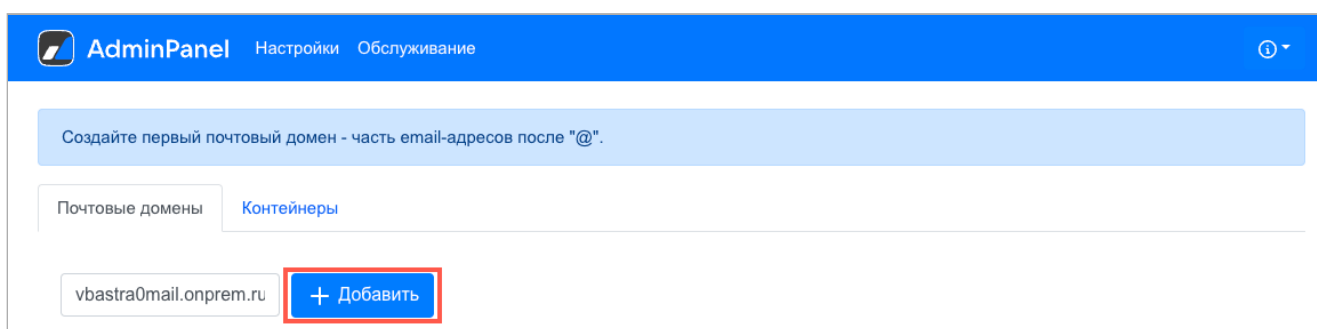
1. Нажмите на кнопку **Далее**.



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.



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?](#).

VK WorkSpace

Войти в аккаунт

admin@admin.qdit

Ввести пароль →

☒ запомнить

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

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

VK Tech

Почта

Календарь

Адресная книга

Облако

АдминПанель

doc-mail.docvk.tech

Пользователи

Администраторы

Почта

Состояние сервера

Настройки

Миграция

Группы рассылок

Общие ящики

Ограничения

Инструкция

Файловое хранилище

Адресная книга

Управление доменом

Конфигурация

Состояние сервера doc-mail.docvk.tech

Последний шаг — настройте MX-запись

Без MX-записи нельзя отправлять и получать письма.

	Должно быть	Сейчас
Имя поддомена:	@	
Тип записи:	MX	
Данные:	mxs.doc-mail.docvk.tech.	
Приоритет:	10	

Проверить сейчас

Настроена автоматическая проверка записей.
О результате мы сообщим вам по электронной почте.

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

Страница 31 из 35

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

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=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDic2
3h3A6tEFx/oSdVhWBtSoArt15wVqMgdhtWsK3WnYj95g8hUV
hqKIErA13MUX1WGfVc/mfISnTlcBMVDOpWYTE2C3WbD4d
RtwvMI5Mfh2EUEXVagkpme2aYqTNL71NXknUclGPEzHXKh
svW9vVTm0p2t9qLFoaztpkzZkpBwIDAQAB

Инструкция по настройке

После проверки **MX-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 MX-запись

При тестовой установке необязательно иметь правильную MX-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										
🔍 Найти										
Действие: ----- ▾ Выполнить Выбрано 0 объектов из 1										
☐	NAME	TYPE	DOMAIN VERSION	ПОДТВЕРЖДЕН?	ФИЧИ	IS ALIAS	USER COUNT	BLOCKED ADMIN AND ALL EMAILS	CREATED AT	UTM SOURCE
☐	doc-mail.docvk.tech	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: doc-mail.docvk.techType: СайтType: HTML-файл

Mx status: Есть необходимая MX-записьSpf status: Нет необходимой SPF записи

Ns status: Проверка NS записей не проводилась

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

Mx bad at:Дата:Сегодня📅Время:Сейчас🕒

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

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

4. Сохраните изменения.

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

VK TechПочтаКалендарьАдресная книгаОблако

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

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=MIGfMA0GCSSqGSIlb3DQEBAQUAA4GNADCBiQKBgQDlc23h3A6tEFx/oSdVhWBtSoArt15wVqMgdhtWsK3WnYj95g8hUVhqKlErA13MUX1WGfVC/mfISnTlCtBMVDOpWYTE2C3WbD4dRtwwMl5Mfh2EUExVagkpme2aYqTNL71NXknUclGPExHXXhsVW9vVTm0p2l9qLFoazltpkzZkpBwIDAQAB

Инструкция по настройке

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](#)

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

 12 марта 2025 г.