

Установка тестовой версии VK WorkMail на одну машину

Тестовая установка

Назначение документа	4
Технические требования	4
Предварительные условия для установки	4
Обязательные предварительные действия	5
Создание DNS-записей	5
Дисковое пространство	8
Этапы установки	8
Действия в командной строке на сервере	9
1. Создание пользователя deployer	9
2. Распаковка дистрибутива	11
3. Запуск установщика как сервиса	11
1. Выбор варианта установки	13
2. Выбор продуктов	14
3. Добавление лицензионного ключа	15
4. Добавление гипервизора	15
5. Сетевые настройки	17
6. Доменные имена	18
6.1 Добавление SSL-сертификатов	20
7. Запуск установки гипервизора	22
8. Генерация контейнеров	23
9. Хранилища, Шардирование и репликация БД	24
10. Запуск установки всех машин	26
11. Завершение установки, инициализация домена и вход в панель администратора	27
Дополнительная документация	29
Приложение 1. Что делать, если при входе в панель администратора появляется ошибка «Неверный пароль»	29
Приложение 2. Обновление лицензионного ключа	31
Приложение 3. Логи и полезные команды	32
Приложение 4. Выпуск SSL-сертификатов с Let's Encrypt	33

Назначение документа

В документе содержится информация о тестовой установке **VK WorkMail 1.20** на одну виртуальную машину. Под тестовой установкой подразумевается быстрая установка с базовыми настройками для демонстрации возможностей почтовой системы.

Технические требования

Рекомендованные операционные системы для установки VK WorkMail:

- **Astra Linux SE Орел** — версии 1.7.3 и выше;
- **РЕД ОС** — версии от 7.3 и выше;
- **CentOS 7.9**.

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

- **24 GB vCPU**;
- **64 GB RAM**;
- **400 GB SSD**.

Предварительные условия для установки

Представители VK предоставили вам следующие данные:

- ссылку на скачивание дистрибутива **VK WorkMail 1.20**,
- 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 [приложении](#));
- **доступ к портам**: 25, 80, 143, 443, 465, 993, 1025;

- **tar**;
- утилита для распаковки zip-архивов, например **7zip** или **unzip**.

Используемые протоколы почты:

- **CalDav** для синхронизации календаря;
- **Kerberos** или **NTLM** — протокол взаимодействия с **Active Directory** клиента;
- **HTTPS** для доступа к веб-интерфейсу почты с использованием **TLS**;
- **SMTP** — протокол отправки почтовых сообщений (порт 25/465);
- **IMAP** — протокол получения почтовых сообщений (порт 143/993).

Обязательные предварительные действия

Создание DNS-записей

Для работы почты необходима **MX-запись** (рекомендуемый приоритет — 10), которая обязательно ведет на `mxs.<домен для почты>`.

Помимо этого вам нужно создать два основных домена: **для почты** и **для хранилищ**, а также набор **A-** или **CNAME-записей**.

Для примера в документе будут использоваться следующие **DNS-записи**:

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

Важно

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 таблице представлен список **A-** или **CNAME-записей**, которые нужно создать перед установкой **VK WorkMail**. Домены из таблицы должны являться **поддоменами** для двух основных.

Назначение домена	Имя домена	Основной домен
Веб-интерфейс авторизации	account	Для почты
Скачивание вложений VK WorkMail	af	Для почты
Скачивание исполняемых вложений VK WorkMail	af	Для хранилищ
Проксирование активного контента вложений VK WorkMail	ampproxy	Для хранилищ
Просмотр вложений VK WorkMail	apf	Для почты
Просмотр исполняемых вложений VK WorkMail	apf	Для хранилищ
Доменная авторизация (внутренних запросов браузера)	auth	Для почты
Домен для панели расширенного просмотра действий пользователей	becca	Для почты
Интерфейс администрирования	biz	Для почты
Blobcloud-аттачи	blobcloud.e	Для почты
Домен для BMW gRPC запросов	bmw	Для почты
Капча	c	Для почты
Календарь	calendar	Для почты
Домен интерфейса календаря для VK Teams	calendarmsg	Для почты
Мобильный календарь	calendartouch	Для почты
Статические данные календаря	calendarx	Для почты
VK WorkDisk	cloud	Для почты
Загрузка файлов в VK WorkDisk	cld-uploader.cloud	Для почты

Назначение домена	Имя домена	Основной домен
Скачивание файлов в веб-интерфейсе VK WorkDisk	cloclo.cloud	Для почты
Защита от XSS-атак при скачивании файлов из VK WorkDisk	cloclo	Для хранилищ
Загрузка файлов в VK WorkDisk	cloclo-upload.cloud	Для почты
Интеграция с API VK WorkDisk	openapi.cloud	Для почты
Загрузка файлов в публичные папки в VK WorkDisk	pu.cloud	Для почты
Портальная авторизация VK WorkDisk	sdc.cloud	Для почты
Скачивание больших почтовых вложений из VK WorkDisk	cloclo-stock	Для хранилищ
Загрузка больших почтовых вложений в VK WorkDisk	uploader.e	Для почты
Превью файлов в VK WorkDisk	thumb.cloud	Для почты
Распаковка архивов в интерфейсе VK WorkDisk	cld-unzipper	Для хранилищ
Интеграция с API VK WorkMail	corsapi	Для хранилищ
Веб-интерфейс VK WorkMail	e	Для почты
Сервис аватарок	filin	Для почты
IMAP VK WorkMail	imap	Для почты
Неисполняемые статические данные	img	Для почты
Исполняемые статические данные	imgs	Для почты
MX VK WorkMail	mxs	Для почты
OAuth2-авторизация	o2	Для почты

Назначение домена	Имя домена	Основной домен
Общепортальные сервисы авторизации	portal	Для почты
Проксирование внешних вложений VK WorkMail	proxy	Для хранилищ
Домен для текстового редактора R7-office	docs	Для хранилищ
Облако, реализующее S3 API	hb	Для хранилищ
SMTP VK WorkMail	smtp	Для почты
Сервер авторизации (межсерверные запросы)	swa	Для почты
Облако временных вложений VK WorkMail	tmpatt	Для хранилищ
Webdav	webdav.cloud	Для почты

Итоговый пример домена: `af` (субдомен из таблицы) + `vbastra@mail.onprem.ru` (основной домен из примера, который вы замените своим) = `af.vbastra@mail.onprem.ru`.

Важно

Изменять доменные имена из таблицы запрещено!

Установщик VK WorkMail 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

1. Создание пользователя deployer

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 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 ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.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 ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys

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

CentOS

```
# Создаем пользователя
adduser deployer
passwd deployer
usermod -aG wheel deployer

# Авторизовываемся под этим пользователем
su - deployer
# Создаем ключ
ssh-keygen -t rsa
# Прописываем в authorized_key для ssh
cat ~/.ssh/id_rsa.pub >> ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
```

Важно

Вся дальнейшая установка будет производиться под созданным пользователем **deployer**. Пользователь должен иметь права администратора.

Затем в файле `/etc/sudoers` раскомментируйте строку, следующую после

```
## Same thing without a password:
```

Astra Linux

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

РЕД ОС

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

CentOS

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

Для этого нужно выполнить команду `sudo visudo` и убрать **#** в начале приведенной выше строки, после чего выйти 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
```

2. Распаковка дистрибутива

Распакуйте дистрибутив под пользователя **deployer**. Нет принципиальной разницы, каким архиватором пользоваться.

Ниже приведен пример для **unzip**:

Astra Linux

```
# В случае 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

```
# В случае если на машину не установлен unzip, скачиваем его:
sudo yum install unzip
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P пароль имя_архива
```

CentOS

```
# В случае если на машину не установлен unzip, скачиваем его:
sudo yum install unzip
export UNZIP_DISABLE_ZIPBOMB_DETECTION=true
unzip -o -P пароль имя_архива
```



Важно

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

3. Запуск установщика как сервиса

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

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

```
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])?
```

CentOS

```
deployer.service was added/updates
see status: <systemctl status deployer.service>
deployer service rsyslog config was added/updates
see logs: <less /var/log/deployer.log>
deployer.service was enable and started
see status: <systemctl status deployer.service>
```

Примечание

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

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

2. Выбор продуктов

Включите флаг **VK WorkMail**. В открывшемся списке отметьте **VK WorkDisk** и перейдите к следующему шагу, нажав на кнопку **Далее** внизу страницы.

3. Добавление лицензионного ключа

Введите лицензионный ключ или укажите путь к файлу лицензии **.lic**, затем нажмите на кнопку **Далее**.

 AdminPanel

Лицензионный ключ

Лицензионный ключ VK WorkMail:


Выбрать файл

Лицензия 0187e174-d83f-75c2-806f-8408d935b622 для onprem.ru. Количество пользователей: VK WorkMail - 30, VK WorkDisk - 30. Разрешённые почтовые домены: "doc-mail.dev.onprem.ru", "admin.qdit". Действительна до 27.09.2023, 17:51:43

Далее

4. Добавление гипервизора

Нажмите на кнопку **Добавить**, в выпадающем меню выберите **Сервер**.

 AdminPanel

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

☐ Не показывать завершённые

☐ Показать вспомогательные контейнеры

Объектов в строке

1

Группировать

Не группировать

Добавить ▾

Сервер

Откроется окно добавления гипервизора:

The screenshot shows the 'AdminPanel' interface for adding a hypervisor. At the top, a blue header contains the 'AdminPanel' logo. Below it, a light blue banner provides instructions: 'Пожалуйста, добавьте машины - гипервизоры. Роль - hypervisor. Это должна быть виртуальная машина, на которой будут запущены компоненты продукта в контейнерах.' The form includes several controls: a toggle for 'Не показывать завершённые' (disabled), a dropdown for 'Объектов в строке' set to '1', a toggle for 'Показать вспомогательные контейнеры' (disabled), and a dropdown for 'Группировать' set to 'Не группировать'. The main form fields are: 'Роль' (hypervisor), 'IP' (10.12.15.1), 'SSH-порт' (22), 'Имя гипервизора' (Hypervisor), 'Имя пользователя' (centos), 'Пароль' (strongPass), 'Приватный ключ' (Использовать авторизацию по паролю), 'Data Center' (DC1), and 'Теги' (store, mail, etc...). A checkbox 'Пропустить проверку не критичных требований' is at the bottom left. 'Отмена' and 'Добавить' buttons are at the bottom right.

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.
- Добавьте **ssh-ключ**:
 - В поле **Приватный ключ** выберите **Добавить новый ключ**.

This screenshot shows a dialog box for adding an SSH key. It has two input fields: 'IP' (10.12.15.1) and 'SSH-порт' (22). Below them are 'Пароль' (masked with dots) and 'Приватный ключ'. A dropdown menu is open for 'Приватный ключ', showing two options: '✓ Использовать авторизацию по паролю' (selected) and '+ Добавить новый ключ'. At the bottom are 'Отмена' and 'Добавить' buttons.

* В поле **Имя ключа** укажите любое удобное имя в соответствии с их назначением **deployerRSA**. *
Перейдите в консоль, выполните в ней команду `cat ~/.ssh/id_rsa` и скопируйте ключ. * Затем вставьте его в поле **Приватный ключ**. Его нужно указать полностью, включая:
`-----BEGIN RSA PRIVATE KEY-----` и `-----END RSA PRIVATE KEY-----` * Поле **Пароль ключа** оставьте пустым. * Кликните по кнопке **Сохранить**. * **Пропустить проверку не критичных требований** — при

выборе чекбоска будет пропущена проверка версии ядра и флагов процессора (sse2, avx). В большинстве случаев заполнение чекбоска не требуется.

После этого нажмите на кнопку **Добавить** — гипервизор отобразится в веб-интерфейсе установщика.

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

The screenshot shows the AdminPanel interface with a blue header bar containing the logo and navigation links. A green box highlights the 'Далее' (Next) button in the top right corner. Below the header, there are several settings: a toggle for 'Не показывать завершённые' (Do not show completed), a dropdown for 'Объектов в строке' (Objects per row) set to 1, a toggle for 'Показать вспомогательные контейнеры' (Show auxiliary containers), and a dropdown for 'Группировать' (Group by) set to 'Не группировать' (Do not group). At the bottom, there is a list of items, with 'infra-03 (100.70.81.216)' visible, and a 'Добавить' (Add) button.

5. Сетевые настройки

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

The screenshot shows the 'Сетевые настройки' (Network settings) page in the AdminPanel. The page has a blue header bar with the logo and navigation links. Below the header, there is a light blue banner with the text 'Заполните настройки сетей.' (Fill in the network settings). The main content area is titled 'Настройки' (Settings) and has several tabs: 'Сети' (Networks), 'Доменные имена' (Domain names), 'Хранилища' (Storage), 'Шардирование и репликация БД' (Sharding and database replication), 'Настройки компонентов' (Component settings), 'Интеграции' (Integrations), and 'Переменные окружения' (Environment variables). The 'Сети' tab is selected, and the 'Сетевые настройки' (Network settings) section is active. It contains several input fields: 'Подсеть, используемая почтой на серверах:' (Subnet used for mail on servers) with the value '100.70.80.0/23', 'Подсеть, используемая внутри контейнеров:' (Subnet used inside containers) with the value '172.20.0.0/20', 'MTU сети контейнеров:' (Container network MTU) with the value '1450', and a toggle for 'НЕ использовать IP-in-IP и BIRD:' (Do not use IP-in-IP and BIRD) which is currently turned off. There are also two lists: 'Список NTP-серверов:' (NTP servers list) with a '+ Добавить' (Add) button, and 'Список DNS-серверов. Оставьте пустым, если используется DHCP:' (DNS servers list. Leave empty if DHCP is used) with the value '10.255.2.3' and a '+ Добавить' (Add) button. At the top of the settings section, there are 'Отмена' (Cancel) and 'Сохранить' (Save) buttons.

Укажите **NTP-сервер** и **DNS-сервер**.

Важно

Обязательно настройте NTP в соответствии с рекомендациями: для [RedOS](#), для [Astra Linux](#). Не следует указывать белый NTP-сервер.

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 **VK WorkMail**.

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**.

После проверки всех настроек 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

6. Доменные имена

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

- Название вашей компании,
- Сайт вашей компании,
- Основной домен для сервисов,
- Домен для облачных хранилищ.

Важно

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 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

Отмена

Сохранить

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:

Сохраните настройки доменов для добавления сертификатов

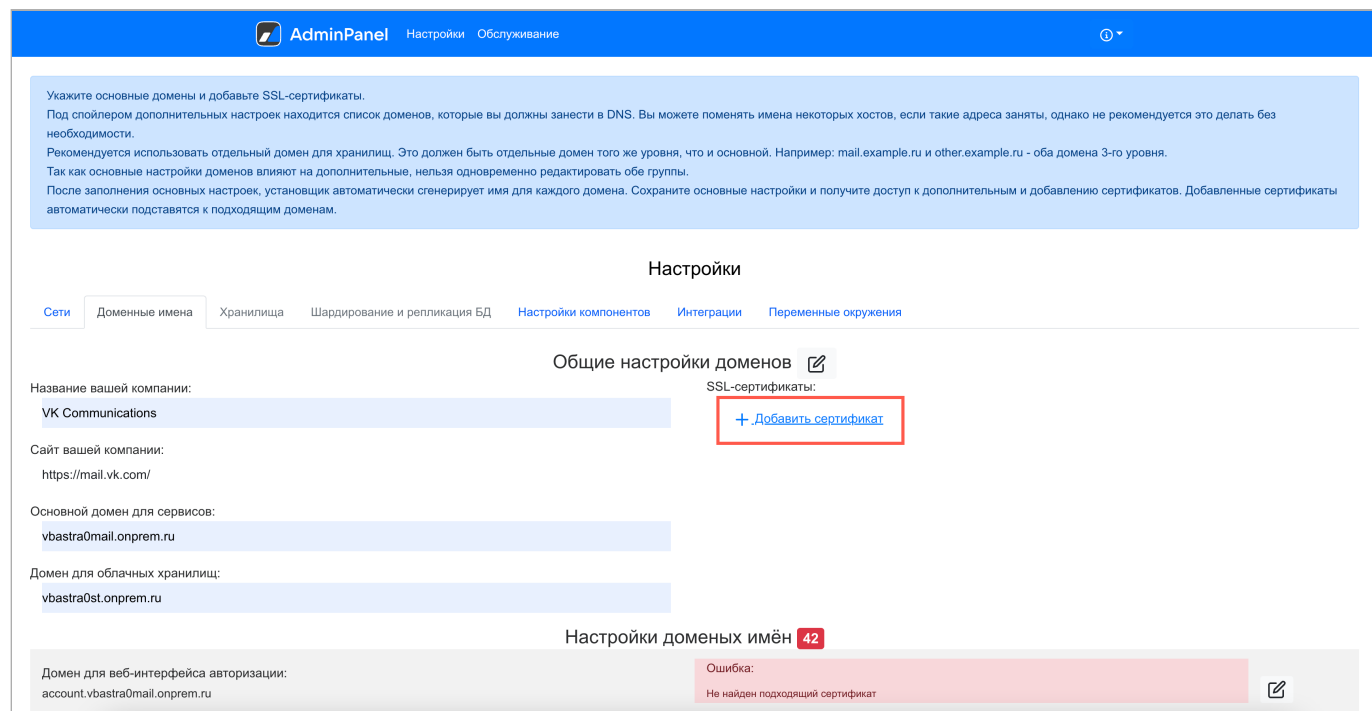


Примечание

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

6.1 Добавление SSL-сертификатов

Нажмите на кнопку **Добавить сертификат** под заголовком **SSL-сертификаты**.



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.

AdminPanel Настройки Обслуживание

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

В открывшейся форме введите сертификат и ключ. Их необходимо указать полностью, включая:

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

и

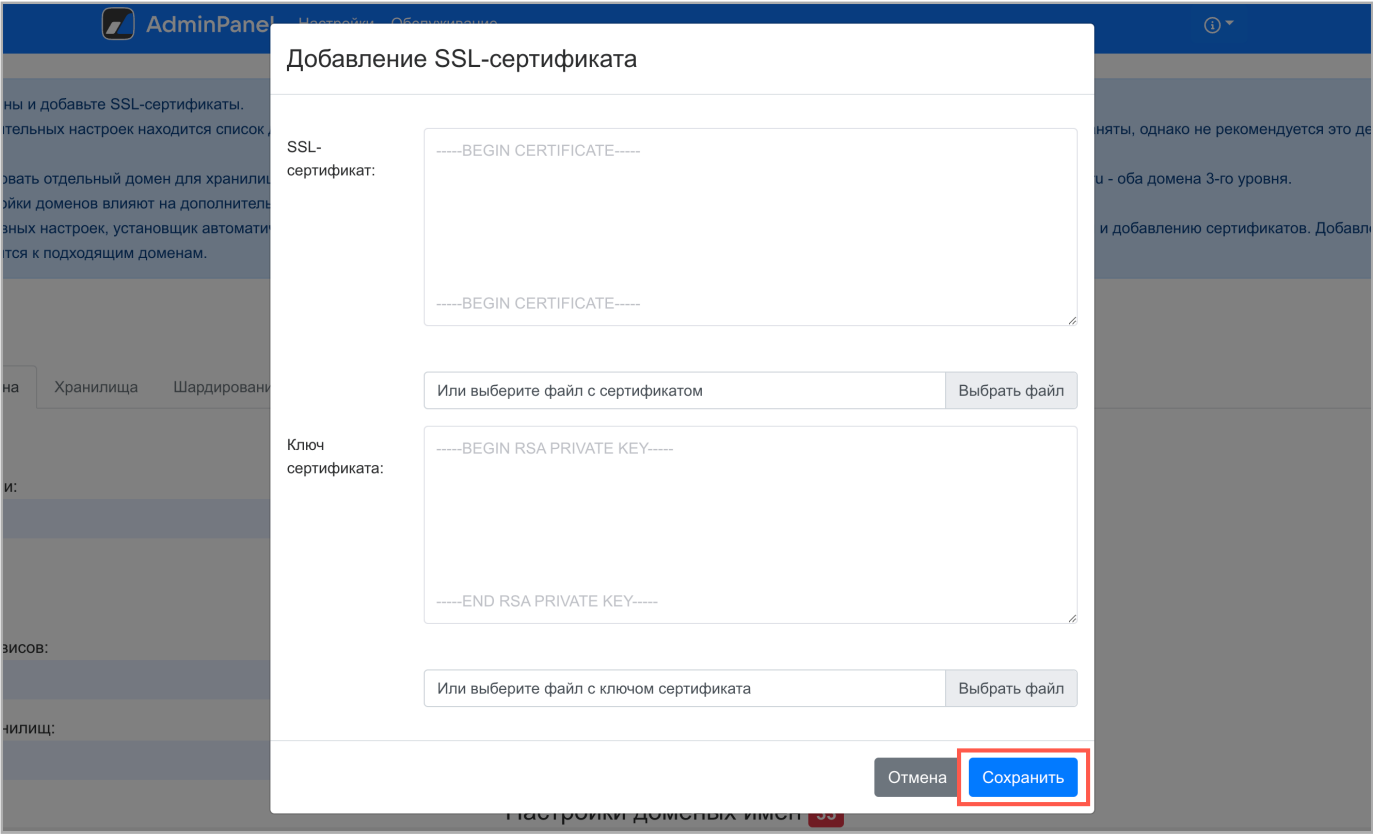
-----BEGIN PRIVATE KEY----- и -----END PRIVATE KEY----- .

Также существует **второй вариант** добавления: нажмите на кнопку **Выбрать файл** и укажите путь к файлу с сертификатом **.crt** и к файлу с ключом **.key**.

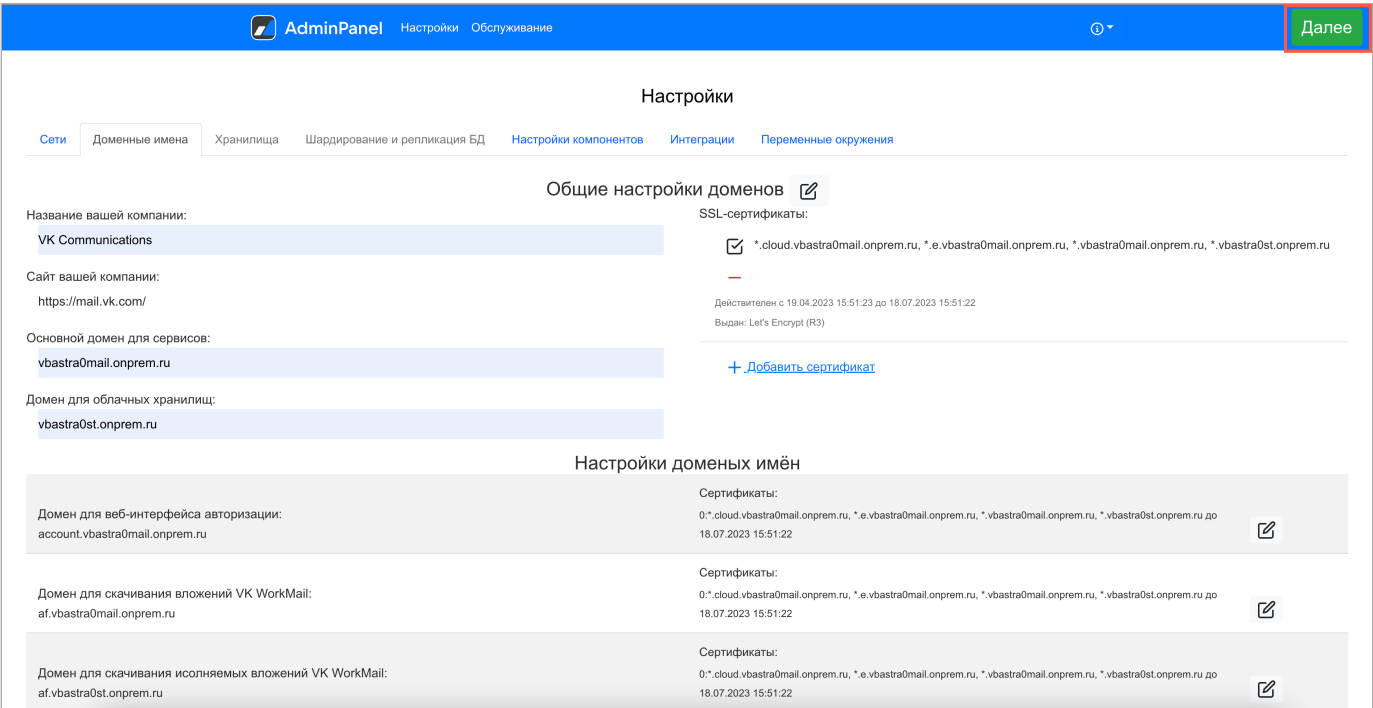
Примечание

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

Кликните по кнопке **Сохранить**.



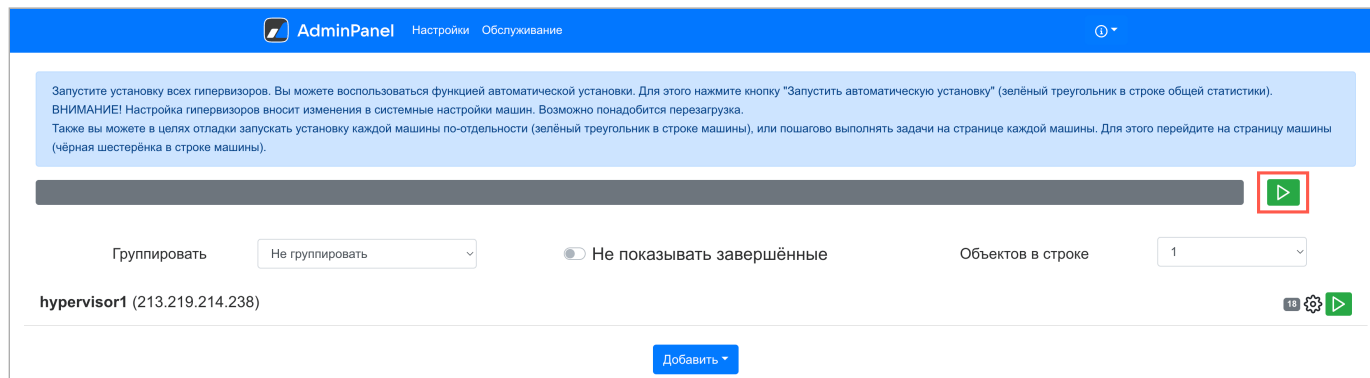
Если всё верно, в интерфейсе не будет отображаться ошибок и красной подсветки. Нажмите на зеленую кнопку **Далее**.



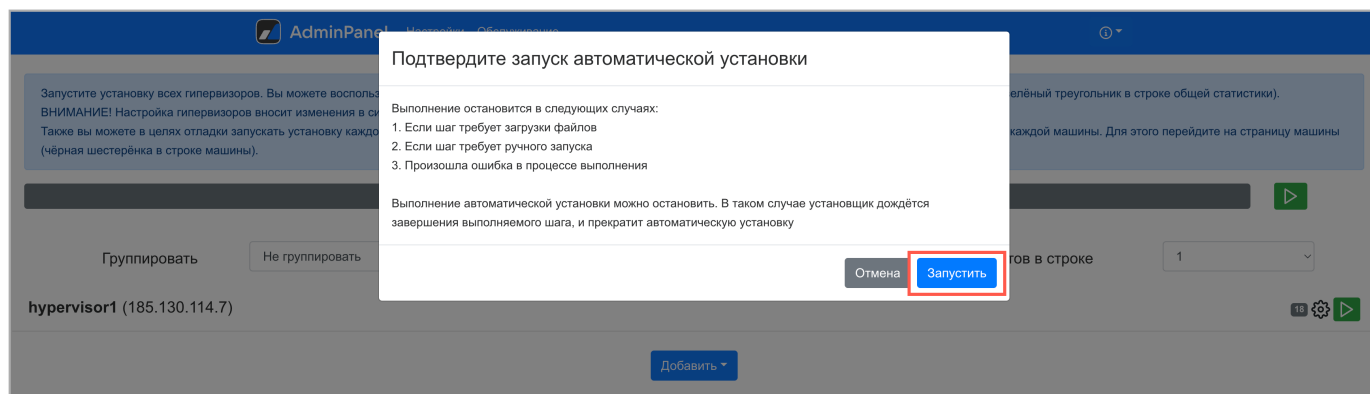
7. Запуск установки гипервизора

Начала установки перейдите к общей строке состояния — для этого нажмите на логотип **AdminPanel**.

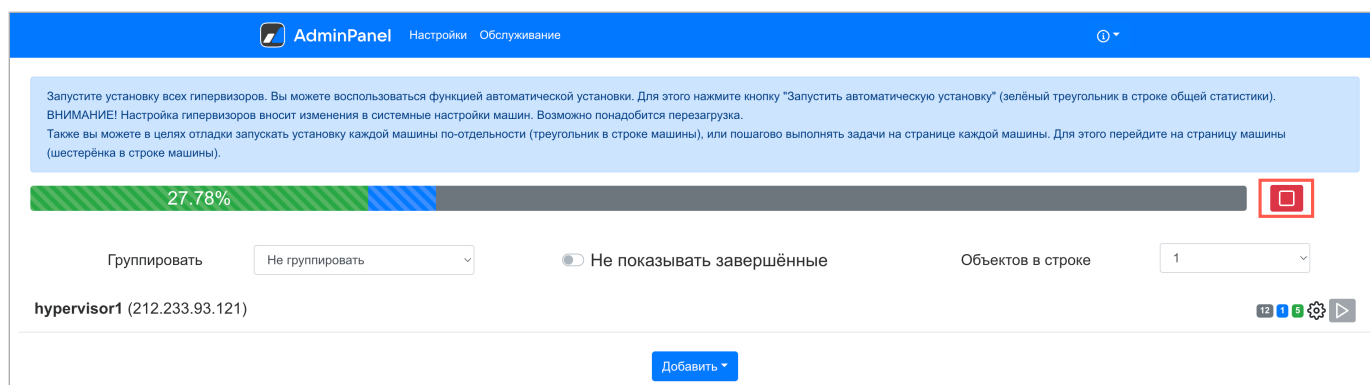
Кликните по кнопке **Play** (треугольник) рядом с общей строкой состояния в верхней части экрана.



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



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

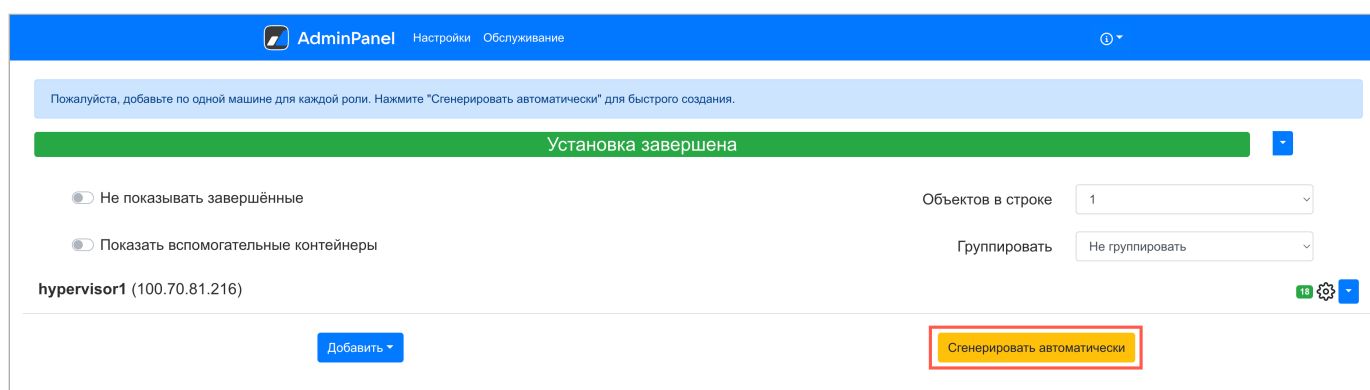


Примечание

В процессе установки и настройки системы происходят изменения конфигурации. Виртуальная машина может перезагрузиться, и потребуется повторный запуск автоматической установки. Для повторного запуска нажмите на зеленую кнопку **Play** либо в верхней общей строке состояния, либо рядом с названием гипервизора.

8. Генерация контейнеров

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



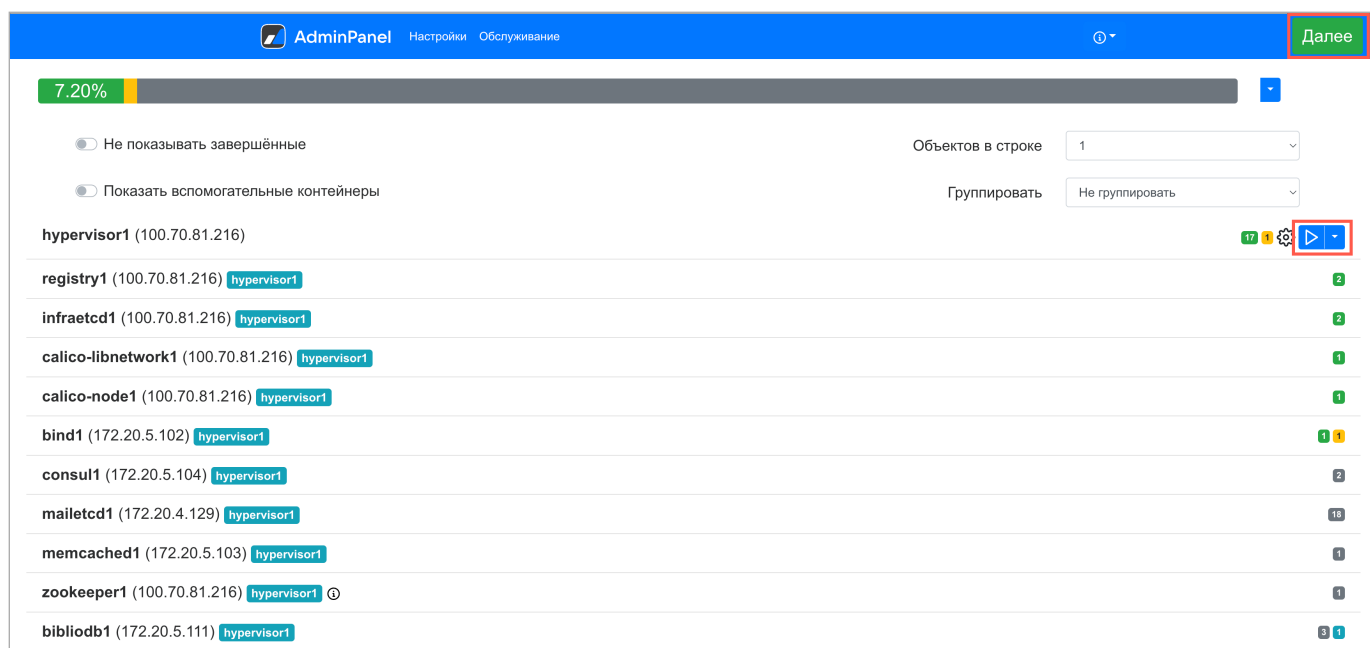
The screenshot shows the AdminPanel interface with a blue header bar containing the logo and navigation links. A light blue message box at the top states: "Пожалуйста, добавьте по одной машине для каждой роли. Нажмите 'Сгенерировать автоматически' для быстрого создания." Below this is a green bar indicating "Установка завершена". There are two toggle switches: "Не показывать завершённые" (disabled) and "Показать вспомогательные контейнеры" (disabled). To the right are dropdown menus for "Объектов в строке" (set to 1) and "Группировать" (set to "Не группировать"). A table lists the hypervisor "hypervisor1 (100.70.81.216)" with a status icon and a settings gear. At the bottom, there is a "Добавить" button and a highlighted "Сгенерировать автоматически" button.

На экране начнут появляться сгенерированные контейнеры.

Важно

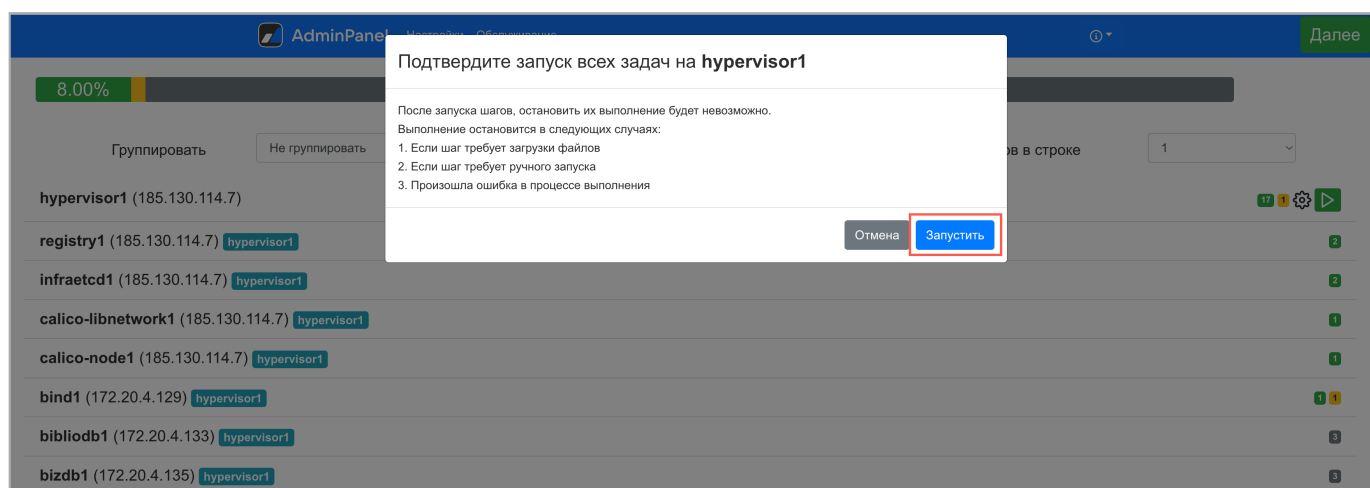
В случае появления ошибок используйте раздел [Логи и полезные команды](#).

Через некоторое время изменится статус в строке состояния, в правом верхнем углу появится кнопка **Далее**, напротив гипервизора **hypervisor1** появится кнопка **Play**.



Кликните по кнопке **Play** напротив гипервизора **hypervisor1**.

Подтвердите автоматический запуск задач на гипервизоре, нажав на кнопку **Запустить**.



На генерацию требуется время. Подождите, пока исчезнет зеленая кнопка **Play** напротив гипервизора **hypervisor1**, и нажмите на кнопку **Далее** для перехода к следующему шагу.

Информация

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

9. Хранилища, Шардирование и репликация БД

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

Настройки

СетиДоменные именаХранилищаШардирование и репликация БДНастройки компонентовИнтеграцииПеременные окружения

cldst1

cldmetastblobcloudmailcloudzepto_delzepto_mainzepto_optzepto_skelzepto_searchcrow_indexmescalitofslab

Хранилище файлов WorkDisk и S3

Не делить хранилище по назначению

#	Диск 1			Диск 2			#
#	Контроллер	Устройство	Размер	Контроллер	Устройство	Размер	#
<div>Добавитьилисгенерироватьдисковые пары</div> <div>Данные о дисках от 14.03.2024, 12:01:31.Обновить</div>							

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

AdminPanelНастройкиОбслуживание

Далее

Настройки

СетиДоменные именаХранилищаШардирование и репликация БДНастройки компонентовИнтеграцииПеременные окружения

Загрузить из базы

Опросить все Overlord'ы

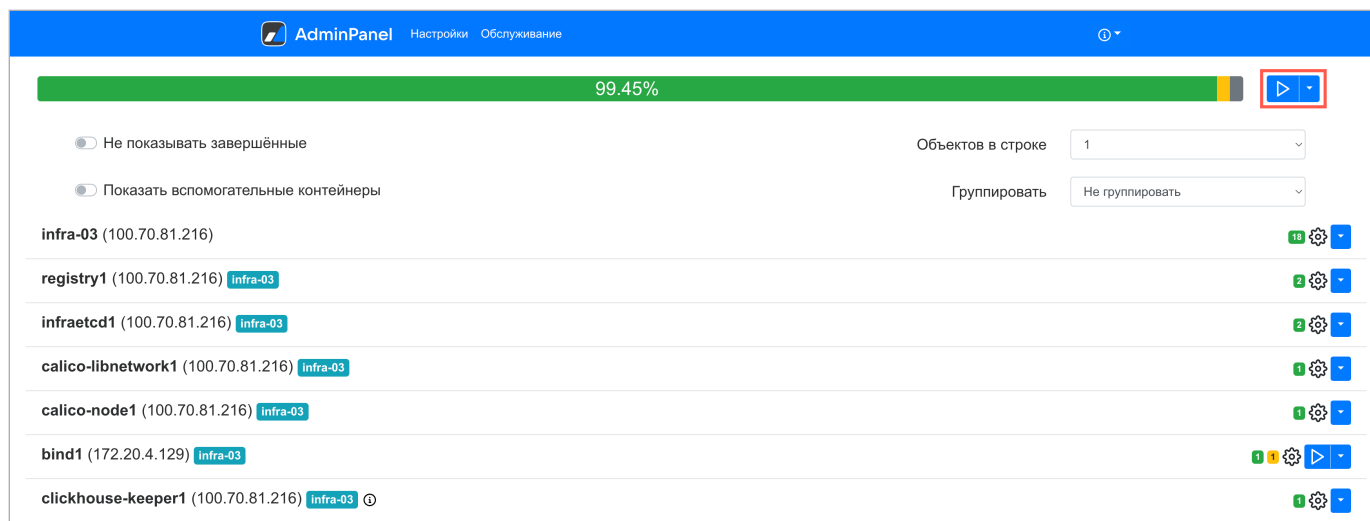
Имя БД	Номер кластера	Отказоустойчивость	Мастер	Состав
abookpdd-tar	1	Overlord	abookpdd-tar2 mail-vkwm2-db2	abookpdd-tar2 abookpdd-tar1
addrbook-tar	1	Overlord	addrbook-tar1 mail-vkwm2-db1	addrbook-tar1 addrbook-tar2
addrbook-tar	2	Overlord	addrbook-tar3 mail-vkwm2-db2	addrbook-tar3
addrbook-tar	3	Overlord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

Примечание

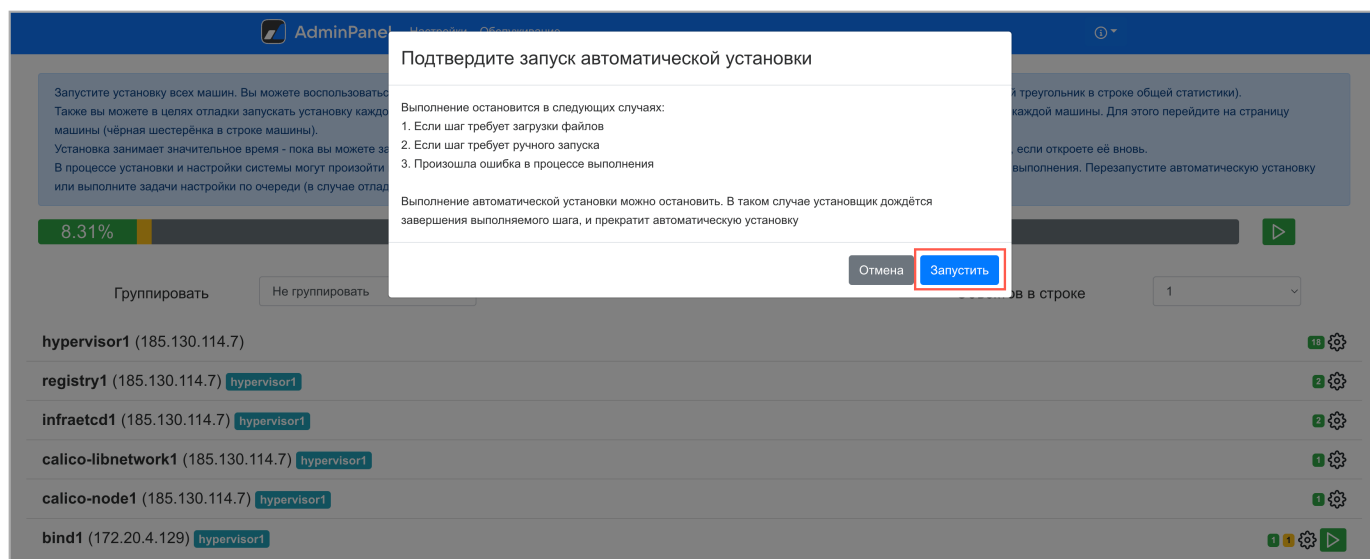
Несколько кластеров БД (PostgreSQL, Tarantool, MySQL и т.п.) нужны на больших инсталяциях, в тестовой установке не применяются.

10. Запуск установки всех машин

Кликните по кнопке **Play** рядом с общей строкой состояния в верхней части экрана.



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.

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

Примечание

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.

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

Когда установка будет завершена, соответствующий статус отобразится в строке состояния. Для перехода к следующему шагу нажмите на кнопку **Далее**.

Установка завершена

Не показывать завершённые

Показать вспомогательные контейнеры

Объектов в строке

1

Группировать

Не группировать

infra-03 (100.70.81.216)	13	⚙️	+
registry1 (100.70.81.216) infra-03	2	⚙️	+
infraetcd1 (100.70.81.216) infra-03	2	⚙️	+
calico-libnetwork1 (100.70.81.216) infra-03	1	⚙️	+
calico-node1 (100.70.81.216) infra-03	1	⚙️	+
bind1 (172.20.4.129) infra-03	2	⚙️	+
clickhouse-keeper1 (100.70.81.216) infra-03 ⓘ	1	⚙️	+
consul1 (172.20.4.131) infra-03	2	⚙️	+
mailetd1 (172.20.4.130) infra-03	13	⚙️	+
memcached1 (172.20.4.132) infra-03	1	⚙️	+

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

AdminPanel

Настройки

Обслуживание

ⓘ

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 /home/deployer/bizOwner.pass`.

VK WorkSpace

Войти в аккаунт

admin@admin.qdit

Ввести пароль →

☒ запомнить

Если логин и пароль были введены правильно, вы попадете в панель администратора. Для проверки **MX-записи** нажмите на кнопку **Проверить сейчас**.

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

Последний шаг — настройте MX-запись

Без MX-записи нельзя отправлять и получать письма.

	Должно быть	Сейчас
Имя поддомена:	@	
Тип записи:	MX	Нет записи. Создайте запись с указанными параметрами.
Данные:	mxs.vbastra0mail.onprem.ru.	
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.

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

Страница 28 из 34

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=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDlc2
3h3A6tEFx/oSdVhWBiSoArt15wVqMgdhtWsK3WnYj95g8hUV
hqKIErA13MUX1WGiVC/mfISnTlcBMVDOpWYTE2C3WbD4d
RtwvMI5Mfh2EUEXVagkpme2aYqTNL71NXknUclGPEzHXKh
svW9vVTm0p2t9qLFoaztpkzZkpBwIDAQAB

Инструкция по настройке

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

Важно

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.

Дополнительная документация

Инструкция по установке обновлений VK WorkMail — в документе содержится информация по обновлению **VK WorkMail**.


Приложение 1. Что делать, если при входе в панель администратора появляется ошибка «Неверный пароль»

Перепроверьте, что пароль скопирован верно. Чтобы просмотреть пароль, введите в консоли команду:
`cat /home/deployer/VKWorkMail/biz0wner.pass`. Если пароль был правильным, а ошибка всё равно появилась, также необходимо сгенерировать новый пароль.

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

Страница 29 из 34

В веб-интерфейсе деплоера перейдите к списку контейнеров, кликнув по логотипу **Admin Panel**

 AdminPanel

Настройки Обслуживание

ⓘ

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

Почтовые домены

Контейнеры

testpismail.onprem.ru

+ Добавить

Найдите в списке контейнеров **fmail1** и нажмите на значок шестеренки справа от названия контейнера.

cld-beaver1 (172.20.4.254)	hypervisor1	1 ⚙
nylon-proxy1 (172.20.4.253)	hypervisor1	1 ⚙
adloader1 (172.20.5.3)	hypervisor1	1 ⚙
mailapi1 (172.20.4.255)	hypervisor1	1 ⚙
mpop1 (172.20.5.1)	hypervisor1	1 ⚙
oper1 (172.20.5.2)	hypervisor1	1 ⚙
panda1 (172.20.5.0)	hypervisor1	1 ⚙
fmail1 (172.20.5.7)	hypervisor1	2 ⚙
img1 (172.20.5.5)	hypervisor1	1 ⚙
lightning1 (172.20.5.4)	hypervisor1	1 ⚙
lightning-intapi1 (172.20.5.9)	hypervisor1	1 ⚙
matter1 (172.20.5.8)	hypervisor1	1 ⚙
streamer-hotbox1 (172.20.5.10)	hypervisor1	1 ⚙
streamer-int1 (172.20.5.11)	hypervisor1	1 ⚙

Запустите выполнение шага **get_biz_owner**.

AdminPanel

НастройкиОбслуживание

1

fmail1 (172.20.5.7)

hypervisor1

2

⚙

Выполните шаги по настройке машины

up_container

done

Подготовить файлы конфигурации, статические данные, запустить контейнер

Запустить

get_biz_owner

done

Создать суперпользователя. Суперпользователь - администратор всех почтовых доменов, обслуживаемых почтовым сервером

Запустить

Дождитесь окончания выполнения шага, затем скопируйте новый пароль.

Приложение 2. Обновление лицензионного ключа

Если вам нужно обновить лицензионный ключ, нажмите на значок ⓘ и в выпадающем меню выберите **Обновить лицензионный ключ**.

AdminPanel

НастройкиОбслуживание

1

Пожалуйста, добавьте по одной машине для каждой роли. Нажмите "Сгенерировать автоматически" для быстрого создания.

Установка завершена

Группировать

Не группировать

Не показывать завершённые

Объектов в строке

hypervisor1 (212.233.93.121)

18

⚙

registry1 (212.233.93.121)

hypervisor1

2

infraetcd1 (212.233.93.121)

hypervisor1

2

calico-libnetwork1 (212.233.93.121)

hypervisor1

1

calico-node1 (212.233.93.121)

hypervisor1

1

bind1 (172.20.4.129)

hypervisor1

2

bibliodb1 (172.20.4.130)

hypervisor1

3

Продукты

Обновить лицензионный ключ

Инструкция по установке

Инструкция по установке демо-версии

Описание системы VK WorkMail

В открывшемся окне вы сможете просмотреть информацию о текущих лицензиях, а также обновить лицензионный ключ.

Текущая лицензия:

UUID:

Клиент: on-premise.ru

Почтовые домены: "*.on-premise.ru"

Продукты:

VK WorkMail: с 26.01.2022, 14:09:30 по 08.01.2033, 14:09:30 на 100000 пользователей

VK WorkDisk: с 26.01.2022, 14:09:30 по 08.01.2033, 14:09:30 на 100000 пользователей

VK Teams: с 26.01.2022, 14:09:30 по 08.01.2033, 14:09:30 на 100000 пользователей

Лицензионный ключ VK WorkMail:

Или выберите файл с лицензионным ключом

Выбрать файл

Сохранить

Если вы вносили какие-либо изменения, кликните по кнопке **Сохранить**.

Приложение 3. 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
```

Приложение 4. Выпуск SSL-сертификатов с Let's Encrypt

Официальная инструкция **EFF** (Electronic Frontier Foundation) для **CentOS** доступна по [ссылке](#).

Примечание

На машине должен быть установлен [snapd](#).

Последовательность действий в консоли:

1. Проверьте, что установлена последняя версия snapd.

```
sudo snap install core
sudo snap refresh core
```

2. Удалите пакеты Certbot, установленные через менеджер пакетов ОС, если такие есть.

```
sudo yum remove certbot
```

3. Установите Certbot через snapd.

```
sudo snap install --classic certbot
```

4. Подготовьте команду Certbot к запуску.

```
sudo ln -s /snap/bin/certbot /usr/bin/certbot
```

5. Сгенерируйте сертификаты. В примере ниже используются тестовые домены:

- testpismail.onprem.ru
- testpisst.onprem.ru
- e.testpismail.onprem.ru

- cloud.testpismail.onprem.ru

```
certbot certonly --manual --preferred-challenges dns \  
-d *.testpismail.onprem.ru -d *.testpisst.onprem.ru \  
-d *.e.testpismail.onprem.ru -d *.cloud.testpismail.onprem.ru
```

6. В процессе выпуска сертификата нужно будет завести в DNS четыре TXT-записи. Certbot напишет, какие именно.

После появления информации о первой записи нажмите Enter для отображения следующей. После того как все четыре записи будут добавлены, Certbot сгенерирует сертификаты.

Пример ответа Certbot:

```
Please deploy a DNS TXT record under the name:  
_acme-challenge.cloud.mail-training1.on-premise.ru.  
with the following value:  
8bFwSSolYouA-B1tit2MmpjXYZJZ06Y0DA1djDMIHe
```

7. После того как сертификаты будут сгенерированы, в консоли отобразятся пути к ним.

```
Successfully received certificate.  
Certificate is saved at:  
/etc/letsencrypt/live/mail-training1.on-premise.ru/fullchain.pem  
Key is saved at:  
/etc/letsencrypt/live/mail-training1.on-premise.ru/privkey.pem  
This certificate expires on 2023-01-08.  
These files will be updated when the certificate renews.
```

Дата обновления документа: 18.03.2024