

Кластерная установка сервиса Почта

Установка Почты 1.22 на кластер из 8 машин

Оглавление

Назначение документа	4
Схема тестового кластера	4
Технические требования	5
Таблица совместимости	5
Предварительные условия	6
Как работать с Wildcard-сертификатами	6
Какие протоколы использует Почта	7
Обязательные предварительные действия	7
Создание DNS-записей	7
Подключение дисков	11
Список портов для установки	11
Этапы установки	13
Действия в командной строке на сервере	13
Шаг 1. Создание пользователя deployer	13
Шаг 2. Распаковка дистрибутива	15
Шаг 3. Запуск установщика как сервиса	16
Действия в веб-интерфейсе установщика	17
Шаг 1. Выбор варианта установки	17
Шаг 2. Выбор продуктов и опций	18
Шаг 3. Добавление лицензионного ключа	21
Шаг 4. Добавление гипервизора	21
Шаг 5. Сетевые настройки	23
Шаг 6. Доменные имена	25
Добавление SSL-сертификатов	26
Шаг 7. Установка гипервизоров	28
Шаг 8. Распределение контейнеров по гипервизорам	31
Порядок действий при распределении контейнеров	33
Шаг 9. Хранилища	36
Раздел Mescalito	39

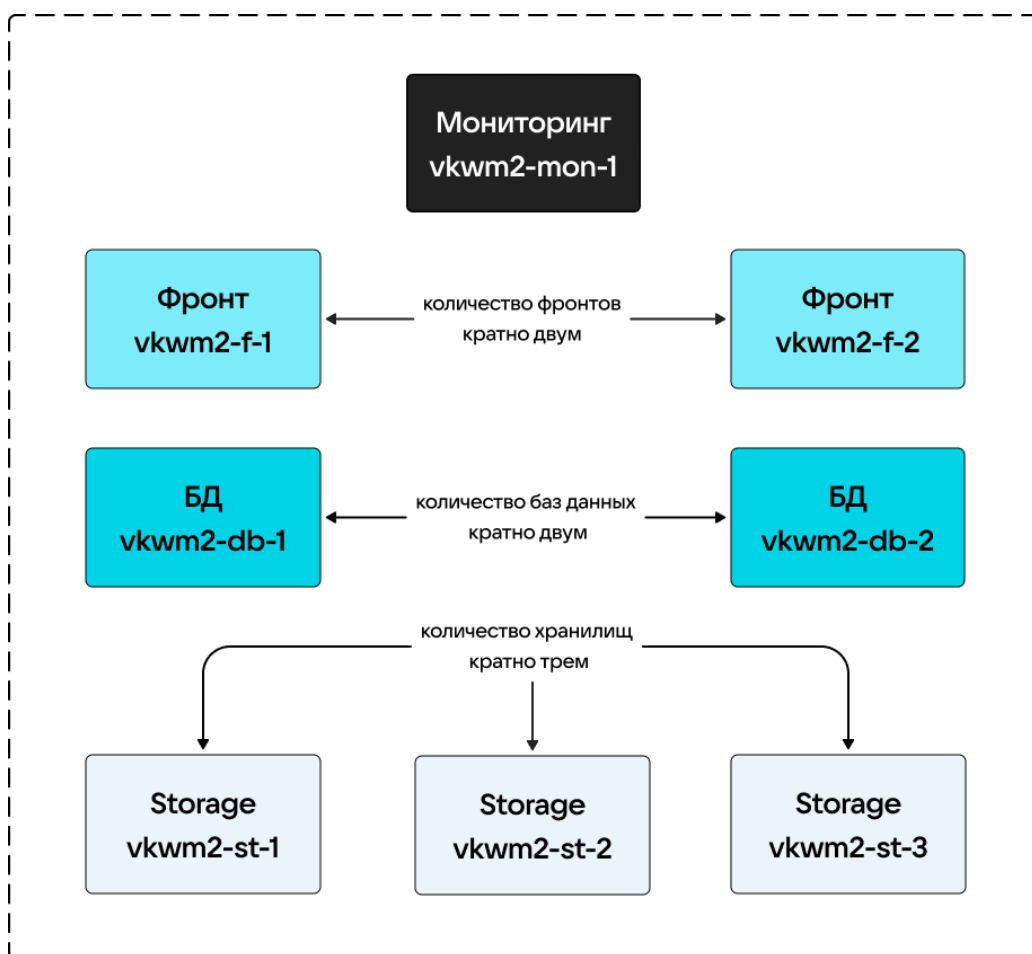
fstab	40
Шаг 10. Шардирование и репликация БД	41
Шаг 11. Настройка компонентов	42
Авторизация	43
Адресная книга	45
Настройки почты	46
Ограничение доступа к доменам	47
Панель администрирования	49
Политика изменения паролей пользователей	50
Почтовый транспорт	51
Рассылщики	54
Система расширенных транспортных правил	55
Система учета действий пользователей	56
Мониторинг	57
Настройки HTTP(S)-прокси	59
Шаг 12. Интеграции	60
Сборщик почты	60
Интеграция с другими инсталляциями Почты	61
Настройки системы BI-аналитики	62
Шаг 13. Переменные окружения	63
Шаг 14. Запуск установки всех машин	64
Шаг 15. Завершение установки, инициализация домена и вход в панель администратора	68
Шаг 16. Добавление дополнительных доменов	70
Настройка интеграции с Active Directory	71
Дополнительная документация	73
Логи и полезные команды	73

Назначение документа

В документе описана процедура кластерной установки Почты. Минимальной отказоустойчивой конфигурацией для установки почтовой системы считается кластер на 8 машин.

Схема тестового кластера

Вне зависимости от размера кластера нужно соблюдать следующее соотношение виртуальных машин:



Минимальная отказоустойчивая конфигурация на 8 машин, которая будет описана в документе, выглядит таким образом:

- 1 VM отводится под мониторинг;
- 2 VM — под фронты;
- 2 VM — под базы данных;
- 3 VM — под хранилища.

Дистрибутив Почты и файл `onpremise-deployer_linux` должны находиться на гипервизоре, отведенном под мониторинг.

Технические требования

Поддерживаемые операционные системы для установки Почты:

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

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

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

Минимальные технические параметры для 8 машин:

- Установщик + мониторинг: 8 vCPU, 16 GB RAM, 200 GB SSD;
- Фронт №1: 16 vCPU, 32 GB RAM, 150 GB SSD;
- Фронт № 2: 16 vCPU, 32 GB RAM, 150 GB SSD;
- База данных №1: 16 vCPU, 16 GB RAM, 150 GB SSD;
- База данных №2: 16 vCPU, 16 GB RAM, 150 GB SSD;
- Хранилище №1: 8 vCPU, 8 GB RAM, 250 GB SSD;
- Хранилище №2: 8 vCPU, 8 GB RAM, 250 GB SSD;
- Хранилище №3: 8 vCPU, 8 GB RAM, 250 GB SSD.

Внимание

По вопросам создания сайзинг-модели специально для вашей компании обратитесь к представителям VK.

Таблица совместимости

Технология	Версия
VK Teams	не старше двух последних версий
MS Server	2013/2016
Keycloak/OAuth	не старше версии 2.x
Kerberos	5
MySQL	8.0.22

Технология	Версия
P7-Офис	ee-2024.1.1.375.rev1

Предварительные условия

Представители VK предоставили вам следующие данные:

- ссылку на скачивание дистрибутива Почты 1.22;
- пароль от архива с дистрибутивом;
- лицензионный ключ;
- комплект документации.

Также вам потребуются:

- Набор DNS-записей: A, CNAME, MX, SPF, TXT, NS.
- Поддержка процессорами набора инструкций 3DNow, ADX, AES, AVX, AVX2, BMI, BMI2, CMOV, MMX, MODE64, NOT64BITMODE, NOVLX, PCLMUL, SHA, SSE1, SSE2, SSE41, SSE42, SSSE3 и XOP для каждого гипервизора.
- DKIM-подпись с селекторами для каждого домена (или несколько DKIM с разными селекторами для одного домена).
- Доступ к серверам по SSH с правами администратора (вход по ключу или по паролю).
- Локальная сеть 1 GbE или 10 GbE.
- Отключить swar.
- Сертификаты SSL для каждого CNAME или Wildcard-сертификат для домена.
- Доступ к портам: 25, 80, 143, 443, 465, 993, 1025.
- tar.
- Утилита для распаковки zip-архивов, например 7zip или unzip.
- Active Directory или другая служба каталогов, работающая по протоколу LDAP.

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 25/465);
- **IMAP** — протокол получения почтовых сообщений (порт 143/993);
- **IP in IP** — протокол туннелирования IP.

Обязательные предварительные действия

Создание DNS-записей

Для работы Почты вам нужны:

- МХ-запись (рекомендуемый приоритет — 10), которая обязательно ведет на mxs.<домен для почты>
- Два основных домена: для почты и для хранилищ.
- Набор А- или СNAME-записей.

Примечание

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

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 представлен список A- или CNAME-записей, которые нужно создать перед установкой сервиса Почта. 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
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

Назначение домена	Имя домена	Пример
Статические данные календаря	calendarx	calendarx.mail.onprem.ru
VK WorkDisk	cloud	cloud.mail.onprem.ru
Загрузка файлов в VK WorkDisk	clid- uploader.cloud	clid- 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		
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
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

Назначение домена	Имя домена	Пример
Облако временных вложений Почты	tmpatt	tmpatt.mail-st.onprem.ru

Внимание

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

Подключение дисков

К машинам, отведенным под хранилища, рекомендуется заранее подключить диски. Подключенные диски необходимо разбить на разделы, для этого можно использовать любые привычные утилиты, например fdisk.

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

Пример команды для создания файловой системы ext4:

```
mkfs.ext4 <путь к устройству>
```

Внимание

Минимальный размер раздела диска, используемого под хранилище, составляет 25 GB.

Список портов для установки

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: 25 (smtp), 143 (imap), 465(smtps), 993 (imaps). Вы должны сами определить с каких IP-адресов будут доступны порты.

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
TCP	9091	calico- node	Демон динамической маршрутизации	Сбор метрик prometheus	victoria-metrics
TCP	5000	registry	Хранилище docker-образов	Подключение к сервису	Все машины инсталляции
TCP	2379	infraetcd	etcd, которое хранит инфраструктурные данные, например настройки сети	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP	2380	infraetcd	etcd, которое хранит инфраструктурные данные, например настройки сети	Общение между инстансами etcd	Другие infraetcd
TCP	4001	infraetcd	etcd, которое хранит инфраструктурные данные, например настройки сети	Подключение клиентов (потребителей)	Все машины и контейнеры инсталляции
TCP	8080	cadvisor	Инструмент снятия телеметрии с контейнеров	Сбор метрик prometheus	victoria-metrics
TCP	2003	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры
TCP	2004	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры

Протокол	Порт	Служба/ Контейнер	Описание службы/ контейнера	Назначение порта	Кто обращается
TCP	22	sshd	Демон операционной системы, предоставляющий консоль пользователю	ssh подключения	Onpremise-deployer
TCP	179	Bird	Calico. Работа BGP сессий	—	Между всеми серверами системы
TCP	8888	onpremise-deployer	Приложения для установки и начальной настройки VK WorkSpace	Подключение администраторов	Администраторы
UDP	2003	carbclick	Сервис, который принимает метрики и передает их в clickhouse	Прием метрик	Любые контейнеры

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

При кластерной установке вам нужно создать пользователя deployer и скопировать ssh-ключи на всех виртуальных машинах в кластере. Необязательно добавлять один и тот же ssh-ключ, главное, чтобы VM с установщиком имела доступ по ssh к другим VM в кластере. Ниже алгоритм, который надо выполнить на

ВМ с установщиком. На остальных машинах нужно создать пользователя deployer и скопировать ssh-ключи.

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>
```

```
# 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. 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.

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

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

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

Ответ в случае успешного запуска установщика выглядит следующим образом:


```
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 укажите адрес: `http://server-ip-address:8888`. Если перейти по этому адресу не удастся, убедитесь, что `firewall` был отключен.

Шаг 1. Выбор варианта установки

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

Полные версии продуктов

Разверните на ваших серверах один или несколько продуктов VK On Premise

[Установка](#)

Инструкция по установке и настройке оборудования

[Читать](#)

Инструкция по кластерной установке и настройке оборудования

[Читать](#)

Инструкция по обновлению

[Читать](#)

Инструкция по обновлению кластерной установки

[Читать](#)

Шаг 2. Выбор продуктов и опций

1. Включите флаг **VK WorkMail**.
2. В открывшемся списке отметьте **VK WorkDisk** и нужные вам компоненты.
3. Выберите интеграции, которые планируете настраивать.

Выбор продуктов

VK WorkMail v1.21.1

1 виртуальная машина на любом гипервизоре, 48 GB RAM, 24 vCPU, 300 GB SSD

Административная панель

Ядро объектного хранилища S3

Ядро распределённого файлового хранилища

API больших вложений VK WorkMail

Календарь

Миграция календарей по протоколу EWS

Бот календаря для VK Teams

VK WorkDisk

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

Интеграция с антивирусом по протоколу ICAP

Система миграции WorkDisk из внешних сервисов **Beta**

Продукт	Примечание
Инструменты разработки	
Встроенное хранилище образов контейнеров	
Интеграция с VK Teams	
Интеграция с другими инсталляциями VK WorkMail	Deprecated
Интеграция с Kerberos (SSO-авторизация)	
Средства резервного копирования почтовых ящиков	

Продукт	Примечание
Двухфакторная аутентификация	
Интеграция с редактором «МойОфис»	
Редактор «Р7-Офис» внутри инсталляции	2 GB RAM, 2 vCPU
Интеграция с редактором «Р7-Офис»	
Система расширенных транспортных правил	
Бот новых почтовых сообщений для VK Teams	
Сервис анализа логов доставки почты	16 GB RAM, 16 vCPU, Beta
Система групповых политик	Beta
Система BI-аналитики	Beta
Система отправки push-уведомлений на мобильные устройства	
Система мониторинга	Grafana, хранилище метрик Graphite, хранилище метрик Prometheus
Система сбора и отправки метрик	Сборщики и трансляторы Graphite и Prometheus-метрик
Система аудита действий пользователя	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)
Система аудита действий пользователя (облегчённая версия)	Сервисы записи и чтения действий пользователей, хранилище действий пользователей (PostgreSQL)

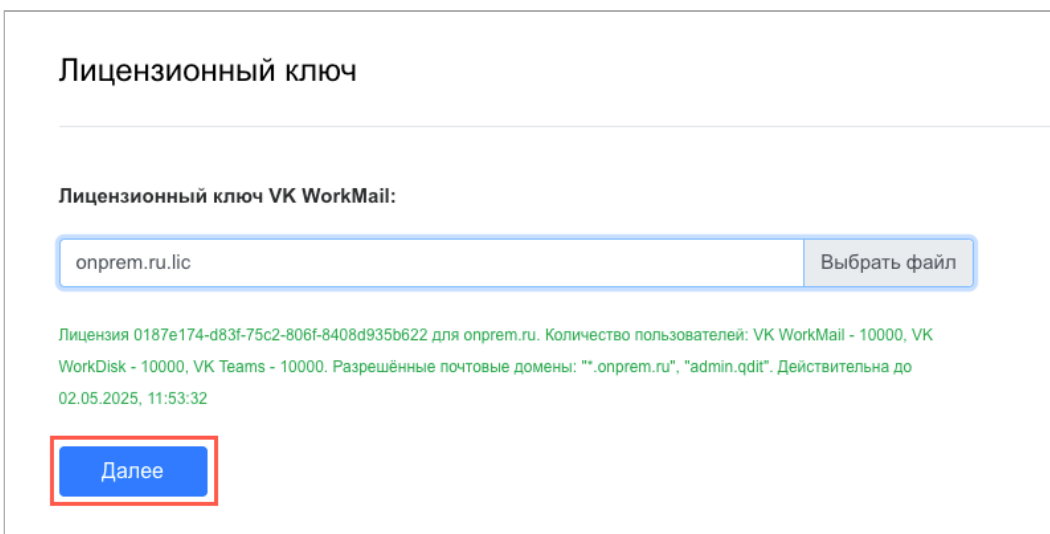
Примечание

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

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

Шаг 3. Добавление лицензионного ключа

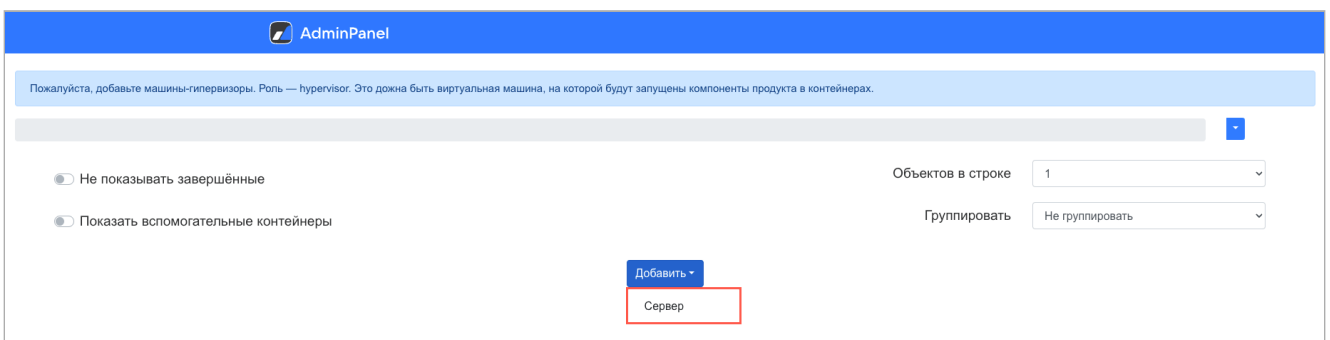
1. Введите лицензионный ключ или укажите путь к файлу лицензии **.lic**.
2. Нажмите на кнопку **Далее**.



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

Показать вспомогательные контейнеры
 Группировать

Роль	IP	SSH-порт	Имя гипервизора
<input type="text" value="hypervisor"/>	<input type="text" value="100.70.160.14"/>	<input type="text" value="22"/>	<input type="text" value="mon"/>
Имя пользователя	Пароль	Приватный ключ	Data Center
<input type="text" value="centos"/>	<input type="text" value="strongPass"/>	<input type="text" value="Использовать авторизацию по паролю"/>	<input type="text" value="mon"/>

Теги

Пропустить проверку некритичных требований

3. Заполните поля:

- **Роль** — hypervisor.
- **IP** — адрес машины, на которую производится установка.
- **SSH-порт** — стандартный для SSH, выбран по умолчанию, менять его не нужно.
- **Имя гипервизора** — укажите имя гипервизора или оставьте поле пустым. В случае если вы оставите поле незаполненным, имя гипервизора будет взято из `hostname -s` и добавится автоматически. В документации будет использовано имя **hypervisor1**.
- **Имя пользователя** — укажите имя того пользователя, под которым запущен установщик. В рассматриваемом примере это пользователь `deployer`.
- **Пароль** — необходимо ввести пароль пользователя, под которым запущен установщик, если он был задан при создании.

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

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

IP	SSH-порт
<input type="text" value="10.12.15.1"/>	<input type="text" value="22"/>
Пароль	Приватный ключ
<input type="text" value="....."/>	<input checked="" type="checkbox"/> Использовать авторизацию по паролю <input type="button" value="+ Добавить новый ключ"/>

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

с. Перейдите в консоль.

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

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

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

f. Поле **Пароль ключа** оставьте пустым.

g. Кликните по кнопке **Сохранить**.

5. При необходимости настройте дополнительные поля:

- **Data Center** — в поле нужно указать дата-центр, на котором размещен гипервизор. Поле актуально и для инсталляций, размещенных в одном дата-центре. Все гипервизоры необходимо распределить по трем фактическим/условным дата-центрам.
- **Теги** — для большей наглядности и простоты поиска вы можете присвоить гипервизорам теги в зависимости от их роли. Например: st1, st2, st3.
- **Пропустить проверку некритичных требований** — если отметить чекбокс, будет пропущена проверка версии ядра и флагов процессора (sse2, avx). В большинстве случаев выбор чекбокса не требуется.

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

Примечание

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

7. Аналогичным образом добавьте еще 7 гипервизоров:

- 2 — под фронты,
- 2 — под базы данных,
- 3 — под хранилища.

8. 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:	<input type="text" value="100.70.160.0/27"/>
Подсеть, используемая внутри контейнеров:	<input type="text" value="172.20.0.0/20"/>
MTU сети контейнеров:	<input type="text" value="1450"/>
НЕ использовать IP-in-IP и BIRD:	<input type="checkbox"/>
Список DNS-серверов. Оставьте пустым, если используется DHCP:	<input type="text" value="10.255.2.3"/> -
	+ Добавить

1. Укажите **DNS-сервер**.

Внимание

Обязательно настройте NTP на VM в соответствии с рекомендациями: для [RedOS](#), для [Astra Linux](#).

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**.

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

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

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

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

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

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

- **Название вашей компании** — введите название компании, которое будет отображаться в интерфейсе 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

Для доменных имен нельзя использовать `etc/hosts`.

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

Укажите основные домены и добавьте SSL-сертификаты.

Под спойлером дополнительных настроек находится список доменов, которые вы должны занести в DNS. Вы можете помять 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

SSL-сертификаты:

Сохраните настройки доменов для добавления сертификатов

Сайт вашей компании:

https://

Основной домен для сервисов:

mail.mycompany.ru

Заполните поле

Домен для облачных хранилищ:

st.mycompany.ru

Заполните поле

Настройки доменных имён 40

Домен для веб-интерфейса авторизации:

Ошибка:

hostname_is_not_suitable

После сохранения доменных имен появятся ошибки. Они пропадут после добавления SSL-сертификатов на следующем шаге, но **SMTP**, **MX** и **IMAP** могут остаться красными — это нормально.

Добавление SSL-сертификатов

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

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

и

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

3. Кликните по кнопке **Сохранить**.

Добавление SSL-сертификата

SSL-сертификат:

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

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

Или выберите файл с сертификатом

Ключ сертификата:

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

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

Или выберите файл с ключом сертификата

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 (у **SMTP**, **MX** и **IMAP** красная подсветка может остаться). Нажмите на зеленую кнопку **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

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 

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 

Шаг 7. Установка гипервизоров

Для начала установки необходимо перейти к списку гипервизоров — для этого нажмите на логотип **AdminPanel**.

Порядок установки принципиален, так как из них формируется **кластер etcd**. Для кворума кластеру необходимо **N/2+1** экземпляров etcd. В минимальной конфигурации узлы etcd должны быть установлены

на **три машины**, две из которых должны быть постоянно доступны. В документе будет описан вариант установки etcd в минимальной конфигурации.

1. Перейдите в настройки гипервизора, отведенного под мониторинг. Вручную запустите шаги до **upload_docker_repo** включительно.

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
hypervisor_repo done	Загрузить архив пакетов для гипервизора	Будет использован hypervisorRepo.tar из хранилища. Загрузить другой? Запустить
install_hypervisor_packs new	Установить пакеты для запуска контейнеров	Запустить
upload_docker_repo new	Загрузить образ и создать Docker Registry	Будет использован dockerRegistry.tar из хранилища. Загрузить другой? Запустить
configure_etc_hosts new	Настроить resolve инфраструктурных контейнеров	Запустить ▾
create_scripts new	Сгенерировать служебные скрипты	Запустить ▾

2. Вернитесь обратно к списку машин и перейдите в настройки первого гипервизора-стораджа.

3. Вручную запустите шаги до **install_etcd** включительно. По завершении шага первый узел etcd будет установлен.

check_needed_packs done	Проверить наличие Docker и Docker Compose	Запустить
hypervisor_repo done	Загрузить архив пакетов для гипервизора	Будет использован <code>hypervisorRepo.tar</code> из хранилища. Загрузить другой? Запустить
install_hypervisor_packs done	Установить пакеты для запуска контейнеров	Запустить
upload_docker_repo optional	Загрузить образ и создать Docker Registry	Будет использован <code>dockerRegistry.tar</code> из хранилища. Загрузить другой? Запустить
configure_etc_hosts done	Настроить <code>resolve</code> инфраструктурных контейнеров	Запустить ▾
create_scripts done	Сгенерировать служебные скрипты	Запустить ▾
tune_docker done	Настроить Docker	Запустить ▾
restart_docker done	Запустить/Перезапустить сервис Docker с остановкой всех сервисов	Запустить
install_etcd inProgress	Настроить etcd	Запустить

4. Таким же способом установите etcd на остальные два гипервизора-стораджа.

5. После того, как кластер etcd собран, запустите установку всех гипервизоров по порядку или общую автоматическую установку.

⚠ Внимание

Не рекомендуется запускать установку нескольких гипервизоров одновременно — это может привести к ошибкам.

На изображении ниже приведен пример того, как выглядит веб-интерфейс установщика после завершения установки всех гипервизоров.

Пожалуйста, добавьте по одной машине для каждой роли.

83.84%

Не показывать завершённые
 Объектов в строке

Показать вспомогательные контейнеры
 Группировать

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

Кликните по значку ⓘ 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.

Шаг 8. Распределение контейнеров по гипервизорам

По завершении установки всех гипервизоров можно приступить к распределению и генерации контейнеров.

В нижней части экрана выберите **Добавить** → **Несколько контейнеров**.

Сервер

Контейнер

Несколько контейнеров

Добавить ▾

Откроется окно выбора ролей.

Выберите роли для добавления



Поиск:

Теги:

Продукты:

Установлено не менее:

Установлено не более:

Дублируемость:

Количество ролей, доступных для добавления: 231

<input type="checkbox"/>	Роль	Установлено / Дублируется		Тег	Продукт
<input type="checkbox"/>	registry	1	Да	Инфраструктура	Встроенное хранилище образов контейнеров
<input type="checkbox"/>	infraetcd	3	Да	Инфраструктура raft База данных ETCD	VK WorkMail
<input type="checkbox"/>	calico-libnetwork	8	Да	Инфраструктура Сеть	VK WorkMail
<input type="checkbox"/>	bind	8	Да	Инфраструктура Сеть	VK WorkMail
<input type="checkbox"/>	queue-ss	0	Да	raft База данных Tarantool	Ядро распределённого файлового хранилища
<input type="checkbox"/>	serverside-api	0	Да	API	VK WorkMail
<input type="checkbox"/>	cld-mailer-tnt	0	Да	raft База данных Tarantool	VK WorkDisk
<input type="checkbox"/>	memcached	0	Да	База данных memcached	
<input type="checkbox"/>	consul	0	Да	База данных raft	VK WorkMail
<input type="checkbox"/>	calendarrabbit	0	Да	База данных raft	Календарь
<input type="checkbox"/>	mailetcd	0	Да	raft База данных ETCD	VK WorkMail

При распределении ролей нужно соблюдать такой порядок:

1. Хранилища + raft
2. xtaz
3. Базы данных
4. Мониторинг
5. Почтовый транспорт
6. API
7. Все, что осталось (опционально)

⚠ Внимание

Порядок распределения ролей принципиально важен, при его нарушении вы столкнетесь с ошибками.

Для выбора ролей используйте поле **Теги** в качестве фильтра.

Порядок действий при распределении контейнеров

Первыми должны быть выбраны роли для хранилищ:

1. В выпадающем меню выберите тег **Хранилище**.
2. Для фильтра **Установлено не более:** установите значение **0**.
3. Отметьте все доступные для установки роли с помощью чекбокса в таблице.

Поиск:

Теги:

Продукты:

Установлено не менее:

Установлено не более:

Дублируемость:

Количество ролей, доступных для добавления: 22

<input checked="" type="checkbox"/>	Роль	Установлено / Дублируется		Тег	Продукт
<input checked="" type="checkbox"/>	stz-opt-bm	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	stz-metad-bm	0	Да	Хранилище	VK WorkDisk API больших вложений VK WorkMail
<input checked="" type="checkbox"/>	stz-skel-bm	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	s3storage	0	Да	Хранилище	Ядро распределённого файлового хранилища
<input checked="" type="checkbox"/>	stz-main-bm	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	stz-del-bm	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	stz-search-bm	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	crow-index	0	Да	База данных Хранилище Почтовый поиск	VK WorkMail
<input checked="" type="checkbox"/>	extract-http	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	stz	0	Да	Хранилище	VK WorkMail
<input checked="" type="checkbox"/>	metad-xtaz	0	Да	raft База данных Tarantool Хранилище	VK WorkDisk API больших вложений VK WorkMail

4. Ниже в списке гипервизоров отметьте те, которые были отведены под стораджи.

5. Режим генерации — **На каждом гипервизоре**.

Выберите гипервизоры

	Гипервизор	Дата-центр	Метки
<input type="checkbox"/>	doc-db-01	1	db
<input type="checkbox"/>	mon	2	mon
<input type="checkbox"/>	doc-db-02	2	db
<input type="checkbox"/>	doc-front-01	3	front
<input type="checkbox"/>	doc-front-02	1	front
<input checked="" type="checkbox"/>	doc-storage-01	1	st
<input checked="" type="checkbox"/>	doc-storage-02	2	st
<input checked="" type="checkbox"/>	doc-storage-03	3	st

Режим генерации На одном из гипервизоров На каждом гипервизоре

6. Нажмите на кнопку **Добавить**. Всплывающее окно, в котором выполнялись предыдущие действия, закроется.

На каждом из гипервизоров-хранилищ нужно дополнительно сгенерировать еще по одному контейнеру **xtaz** и **metad_xtaz**:

1. В поиске введите **xtaz**.
2. Выберите контейнеры **xtaz** и **metad_xtaz** с помощью чекбоксов.
3. В списке гипервизоров отметьте те, которые были отведены под стораджи.
4. Режим генерации — **На каждом гипервизоре**.
5. Нажмите на кнопку **Добавить**. Всплывающее окно, в котором выполнялись предыдущие действия, закроется.

Внимание

Для всех последующих ролей должно быть установлено значение 0 в фильтре **Установлено не более**. Если пропустить этот фильтр, кластер не соберется.

Помимо этого на гипервизоры-стораджи необходимо добавить кластер **raft**.

1. В выпадающем меню выберите тег **raft**.
2. Для фильтра **Установлено не более**: установите значение **0**.
3. Отметьте все доступные для установки роли с помощью чекбокса в таблице.
4. Ниже в списке гипервизоров отметьте те, которые были отведены под стораджи.

5. Режим генерации — **На каждом гипервизоре**.

6. Нажмите на кнопку **Добавить**. Всплывающее окно, в котором выполнялись предыдущие действия, закрывается.

Следующий шаг — распределение ролей для баз данных.

1. Выберите тег **База данных**.

2. Для фильтра **Установлено не более**: установите значение **0**.

3. Отметьте **Все** доступные для установки роли.

4. Ниже выберите гипервизоры, отведенные под базы данных.

5. Режим генерации — **На каждом гипервизоре**.

6. Нажмите на кнопку **Добавить**.

Чтобы добавить роли для мониторинга, повторно откройте окно выбора ролей.

1. Выберите тег **Мониторинг**.

2. Для фильтра **Установлено не более**: установите значение **0**.

3. Отметьте **Все** доступные для установки роли.

4. Выберите гипервизор-мониторинг.

5. Режим генерации — **На каждом гипервизоре**.

6. Нажмите на кнопку **Добавить**.

Далее нужно распределить роли для почтового транспорта. Перейдите в окно выбора ролей, нажав **Добавить** → **Несколько контейнеров**.

1. Выберите тег **Почтовый транспорт**.

2. Для фильтра **Установлено не более**: установите значение **0**.

3. Отметьте **Все** доступные для установки роли.

4. Выберите гипервизоры, отведенные под фронты.

5. Режим генерации — **На каждом гипервизоре**.

6. Нажмите на кнопку **Добавить**.

Завершающий этап — распределить роли для API.

1. Выберите тег **API**.

2. Для фильтра **Установлено не более**: установите значение **0**.

3. Отметьте **Все** доступные для установки роли.

4. Выберите гипервизоры, отведенные под фронты.

5. Режим генерации — **На каждом гипервизоре**.

6. Нажмите на кнопку **Добавить**.

Финальная проверка для того чтобы убедиться, что все роли распределены:

1. Откройте окно добавления выбора ролей, нажав на **Добавить** → **Несколько контейнеров**.

2. Для фильтра **Установлено не более**: установите значение **0**.
3. Список ролей, доступных для добавления, должен быть пустым. Если это не так, распределите оставшиеся роли по гипервизорам в соответствии с тегами.

После того как все контейнеры сгенерированы, нажмите на зеленую кнопку **Далее** в правом верхнем углу.

Шаг 9. Хранилища

Внимание

Минимальный размер раздела диска, используемого под хранилище, составляет 25 GB.

В разделе формируются дисковые пары для гипервизоров-хранилищ. Разделение на дисковые пары происходит автоматически, если вы не подключали дополнительные диски. В таком случае можно переходить в настройке **mescalito**, описанной в следующем шаге.

Ручная настройка дисковых пар требуется в случаях, когда дополнительные диски подключены.

Информация

Под дисковой парой подразумеваются связанные разделы дисков, которые размещены на двух разных гипервизорах. Для повышения отказоустойчивости на дисковую пару записываются одни и те же данные.

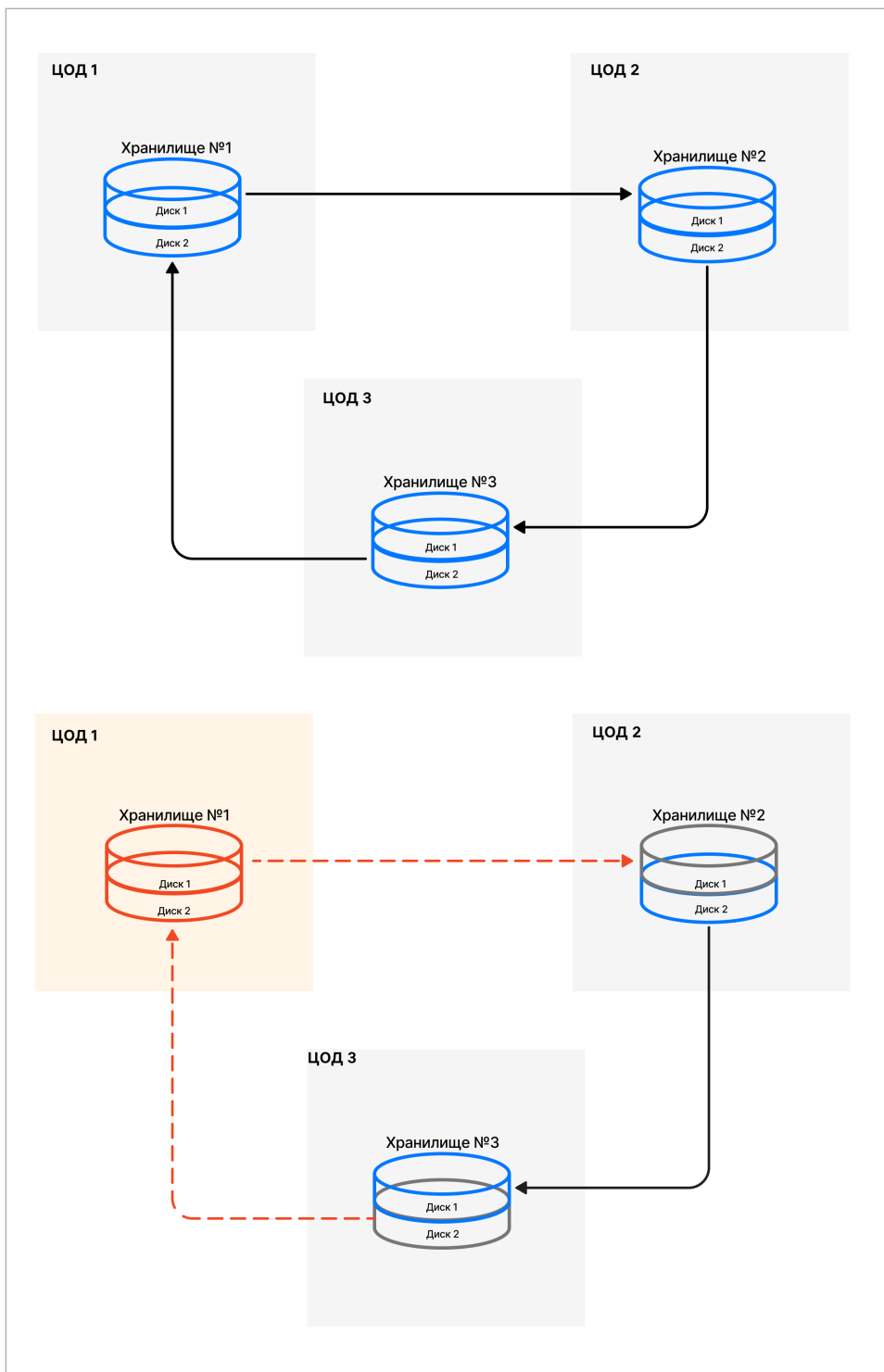
В документе описана процедура ручного распределения дисковых пар. При автоматическом формировании дисковых пар настройка не требуется.

Минимальная отказоустойчивая конфигурация: 3 машины, на каждой из которых по 2 дисковых раздела — всего 6 разделов.

При такой конфигурации:

- Всегда есть пара на запись.
- Остальные пары доступны для чтения.

При сборке хранилищ дисковые пары объединяются в «логические треугольники». Объединение происходит по принципу: 1-2, 2-3, 3-1.



Примечание

Стрелки на изображении показывают, какие диски объединены в пару. На нижней части изображения демонстрируется ситуация, когда одно из хранилищ вышло из строя.

В списке слева будут отображаться доступные хранилища, отмеченные восклицательными знаками.

Нужно перейти на вкладку каждого хранилища и сформировать дисковые пары.

Настройки

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

cidst 1

Хранилище файлов WorkDisk и S3

☰

Не делить хранилище по назначению

Диск 1			Диск 2			#
#	Контроллер	Устройство	Размер	Контроллер	Устройство	Размер
Добавить или сгенерировать дисковые пары Данные о дисках от 14.03.2024, 12:01:31. Обновить						

В минимальной конфигурации, где к каждому из трех гипервизоров-хранилищ подключено по диску, которые, в свою очередь, разделены на 2 части мы имеем:

- Диск хранилища 1 разделен на 2 части.
- Диск хранилища 2 разделен на 2 части.
- Диск хранилища 3 разделен на 2 части.

Всего 6 разделов дисков (2 на одном гипервизоре, 2 — на втором, еще 2 — на третьем).

Внимание

В интерфейсе под Диск 1 и Диск 2 подразумеваются разделы хранилищ. Между собой также нужно будет объединить часть диска, размещенного на одном хранилище, с частью диска, размещенного на другом хранилище. При увеличении количества разделов дисков и/или подключенных дисков принцип объединения сохраняется.

1. Нажмите на кнопку **Добавить**.
2. В выпадающем меню выберите контроллер и устройство для Диска 1 первой пары.
3. Выберите контроллер и устройство для Диска 2 первой пары.
4. Повторите шаги 2-3 еще для двух пар.







На изображении ниже приведен пример для хранилища **zepto_skel**:

Настройки

Хранилище тел писем
возможно размещение на накопителях типа HDD

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

blobcloud
cldst
crow_index
mailcloud
mescalito
mescalito_metad
zepto_del
zepto_main
zepto_metad
zepto_opt
zepto_search
zepto_skel
fstab

Диск 1					Диск 2				
#	Контроллер	Номер	Устройство	Размер	Контроллер	Номер	Устройство	Размер	#
1	stz-skel-bm1.qdit mail-vkwm2-st1 (astra)	1	/dev/vdb1 (ext4) d08f96a7-0ad2-43b5-a256-5fd3d345dd7d	50.00Gb	stz-skel-bm2.qdit mail-vkwm2-st2 (redos)	1	/dev/vdb1 (ext4) 0c020513-ccb2-41e1-b18d-79b5a9fe87e9	50.00Gb	 
2	stz-skel-bm2.qdit mail-vkwm2-st2 (redos)	2	/dev/vdb2 (xfs) 1a353141-89fe-43d1-a8d3-4572623f42bd	50.00Gb	stz-skel-bm3.qdit mail-vkwm2-st3 (alma)	1	/dev/vdb1 (ext4) 2277dcea-2765-4b24-a0cf-bd8a4d6da894	50.00Gb	 
3	stz-skel-bm1.qdit mail-vkwm2-st1 (astra)	2	/dev/vdb2 (xfs) a683bb83-6541-4b72-a1fb-1a435effa72f	50.00Gb	stz-skel-bm3.qdit mail-vkwm2-st3 (alma)	2	/dev/vdb2 (xfs) 18b40182-0e47-4692-84e3-f88af269cb48	50.00Gb	 









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

Данные о дисках от 04.07.2024, 17:10:18. [Обновить](#)

Раздел Mescalito

Для обеспечения отказоустойчивости в разделе уже заданы автоматические настройки кластеров хранилищ писем.

Кластеры хранилищ индексов писем VK WorkMail

№ кластера	Полон 	Тип ящиков	Обработчики 	Хранилища индексов	
1	<input checked="" type="checkbox"/>	сервисный	stm1	xtaz1	 
			mail-vkwm2-st1, astra	mail-vkwm2-st1, astra	
			stm2	xtaz2	
			mail-vkwm2-st2, redos	mail-vkwm2-st2, redos	
2	<input type="checkbox"/>	корпоративный	stm3	xtaz3	 
			mail-vkwm2-st3, alma	mail-vkwm2-st3, alma	
			stm2	xtaz4	
			mail-vkwm2-st2, redos	mail-vkwm2-st1, astra	
			stm1	xtaz5	 
			mail-vkwm2-st1, astra	mail-vkwm2-st2, redos	
			stm3	xtaz6	
			mail-vkwm2-st3, alma	mail-vkwm2-st3, alma	

Обработчики писем (mescalito) запускаются в контейнерах **stm**. Их задача — собирать письма из частей, находящихся в разных хранилищах.

В хранилищах индексов (tarantool xtaz) хранится информация о последних действиях пользователей в их почтовых ящиках (горячий кэш). Из хранилищ индексов формируются кластеры, которые обрабатываются в stm.

Информация

Появление ошибки `failed to allocate X bytes` (или ошибок с подобной формулировкой) при проверке системных логов контейнеров `xtaz` свидетельствует о недостатке памяти.

Существует 2 типа ящиков:

- Сервисный — `admin@admin.qdit` (администраторы почты).
- Корпоративный — все остальные ящики системы, которые администрируются в `biz.<почтовый домен>`.

Внимание

Обработчики работают в однопоточном режиме. Перенаправление информации на другой обработчик будет производиться только в случае недоступности хранилища, на котором установлен соответствующий `stm`.

Для обеспечения отказоустойчивости для каждого кластера необходимо назначать по 2-3 обработчика, находящихся на разных машинах или в разных дата-центрах.

Информация

Контейнеры `stm` устанавливаются на каждый гипервизор-сторадж, поэтому количество обработчиков равно количеству машин, отведенных под хранилища. При необходимости могут быть сгенерированы дополнительные контейнеры `stm` вручную.

fstab

Раздел актуален для ситуаций, когда были подключены дополнительные диски.

Необходимый набор томов для контейнеров хранилища выдается в виде набора записей для `/etc/fstab`.

Внимание

Установщик ничего не монтирует и не изменяет в `/etc/fstab`.

Отредактировать `fstab` и смонтировать разделы нужно самостоятельно в консоли. Монтировать рекомендуется по UUID.

Ниже для примера приведен скриншот с одного из наших тестовых стендов.

FSTab

mail-vkwm2-db-2 mail-vkwm2-f-2 mail-vkwm2-st-2 mail-vkwm2-f-1 mail-vkwm2-mon-1 mail-vkwm2-db-1 mail-vkwm2-st-3 mail-vkwm2-st-1

UUID defaults 0 0

```
# <device-spec> <mount-point> <fs-type> <options> <dump> <pass>
```

```
UUID=2b0dcada-4f9c-41e1-b7e4-221713585ed2 /opt/mailOnPremise/dockerVolumes/s3storage1/storage/1 ext4 defaults 0 0
UUID=c3521227-dd6f-435f-9eeb-cd063cdf5237 /opt/mailOnPremise/dockerVolumes/s3storage1/storage/3 ext4 defaults 0 0
UUID=d769e833-021e-4075-a3b3-8bd352267c5c /opt/mailOnPremise/dockerVolumes/stz-skel-bm1/zepto/disk1 xfs defaults 0 0
UUID=ab4d08f0-0fe2-4e4e-83c5-cc47b2d039af /opt/mailOnPremise/dockerVolumes/stz-skel-bm1/zepto/disk2 xfs defaults 0 0
```

Пример команд для монтирования разделов:

```
vi /etc/fstab

# Вставляем строки, скопированные из веб-интерфейса установщика.
# Сохраняем изменения.

mount -a

# Получаем набор предупреждений <путь> mount point does not exist

mkdir -p <путь>

# Повторяем для всех путей

mount -a
```

Шаг 10. Шардирование и репликация БД

Настройка в этом разделе актуальна только для очень крупных инсталляций. В большинстве случаев достаточно настроек по умолчанию, и можно перейти к следующему шагу с помощью кнопки **Далее**.

Внимание

Добавлять кластеры БД можно только на этапе первоначальной установки.

Чтобы добавить более одного кластера, потребуется сгенерировать дополнительные контейнеры.

AdminPanel Настройки Обслуживание Далее				
Настройки				
Сети Доменные имена Хранилища Шардирование и репликация БД Настройки компонентов Интеграции Переменные окружения				
Загрузить из базы		Опросить все Overlord'ы		
Имя БД	Номер кластера	Отказоустойчивость	Мастер	Состав
abookpdd-tar		Необходима настройка		Добавить
addrbook-tar		Необходима настройка		Добавить
addrbook-tar	1	Overlord	addrbook-tar1 mail-vkwm2-db1	addrbook-tar1 addrbook-tar2
addrbook-tar	2	Overlord	addrbook-tar3 mail-vkwm2-db2	addrbook-tar3
aliases-tar		Необходима настройка		Добавить
appass-tar	1	Overlord	appass-tar1 mail-vkwm2-db1	appass-tar1 appass-tar2
appass-tar	2	Overlord	appass-tar4 mail-vkwm2-db1	appass-tar3 appass-tar4

Последовательность действий для добавления кластеров:

1. Нажмите кнопку **Добавить** в первой строке, отмеченной красным.
2. Добавьте контейнеры БД (кнопка **Добавить контейнер БД**). В зависимости от типа базы данных может быть добавлен как один контейнер, так и два.
3. Сохраните изменения.
4. Повторите шаги 1-4 для каждой строки, отмеченной красным.

После добавления всех кластеров появится возможность перейти к следующему шагу с помощью кнопки **Далее**.

AdminPanel Настройки Обслуживание Далее				
Настройки				
Сети Доменные имена Хранилища Шардирование и репликация БД Настройки компонентов Интеграции Переменные 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

Шаг 11. Настройка компонентов

В разделе выполняются настройки различных компонентов почтовой системы.

Настройки

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

Авторизация

[Адресная книга](#)

[Настройки панели администрирования](#)

[Настройки почты](#)

[Ограничение доступа к доменам](#)

[Политика изменения паролей пользователей](#)

[Почтовый транспорт](#)

[Система учёта действий пользователей](#)

[HTTP\(S\)-прокси](#)

Настройки авторизации

Настройки авторизации по паролю через внешние протоколы ?

IMAP
 SMTP
 WebDav
 CalDav

Включить систему противодействия подбору паролей

Ограничение попыток авторизации по IP

Попыток в минуту :	20
Попыток в час :	250
Попыток в день :	1000

Список IP с **неограниченным** количеством попыток

Авторизация

В разделе есть возможность настроить защиту от подбора паролей. Для этого нажмите на кнопку редактирования.

Настройки

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

Авторизация

[Адресная книга](#)

[Настройки панели администрирования](#)

[Настройки почты](#)

[Ограничение доступа к доменам](#)

[Политика изменения паролей пользователей](#)

[Почтовый транспорт](#)

[Система учёта действий пользователей](#)

[HTTP\(S\)-прокси](#)

Настройки авторизации Отмена Сохранить

Настройки авторизации по паролю через внешние протоколы ?

IMAP
 SMTP
 WebDav
 CalDav

Включить систему противодействия подбору паролей

Ограничение попыток авторизации по IP

Попыток в минуту :	<input type="text" value="20"/>
Попыток в час :	<input type="text" value="250"/>
Попыток в день :	<input type="text" value="1000"/>

Список IP с **неограниченным** количеством попыток + Добавить

Настройки авторизации по паролю через внешние протоколы — позволяет запретить пользователям авторизовываться во внешних приложениях (MS Outlook, Почта/Календарь на iOS и т.п.) с помощью основного пароля почты.

Если флаг одного или нескольких протоколов включен, для авторизации по этим протоколам пользователю потребуется не пароль от почты, а одноразовый пароль, сформированный в разделе **Настройки** → **Безопасность** аккаунта Почты.

По кнопке **Добавить** пользователю нужно будет ввести название внешнего приложения, для которого нужно сгенерировать пароль, ввести пароль основной пароль аккаунта.

[← Вернуться](#)

Пароли для внешних приложений

Пароль для внешнего приложения — это пароль, который нужно использовать для входа в аккаунт через почтовые приложения: Microsoft Outlook, Почта на iOS и так далее.

Вы вводите его только один раз вместо основного пароля.

Календарь Mac

×

Календарь iPhone

×

Добавить

После чего нужно будет скопировать сгенерированный код и ввести его во внешнее приложение при первом входе под учетной записью Почты.

Если флаг протокола выключен, для входа во внешнее приложение достаточно будет ввести пароль аккаунта Почты.

Примечание

Для получения информации о принципе работы системы ограничения SSO-авторизации по IP/группе в ActiveDirectory обратитесь к представителю VK.

Также в разделе вы можете ограничить количество попыток входа в Почту по IP и по адресу электронной почты и добавить IP и/или адреса в белый список.

Адресная книга

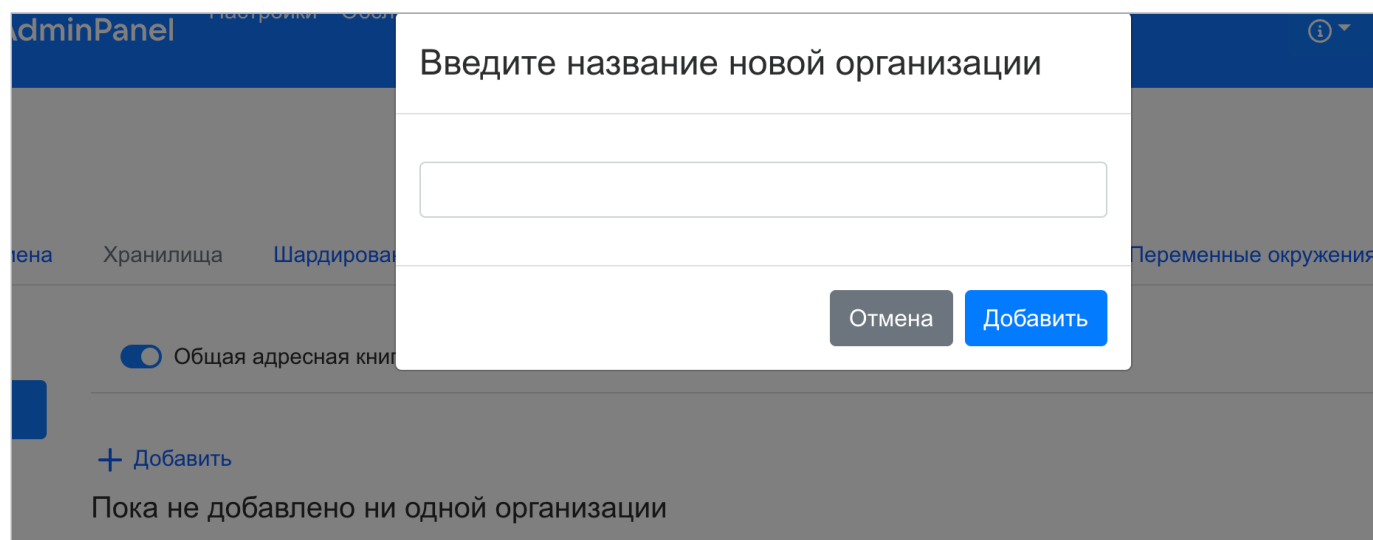
Для случаев, когда необходимо создать общие почтовые ящики для адресов из разных доменов, включите флаг **Общая адресная книга для всех доменов**.

Информация

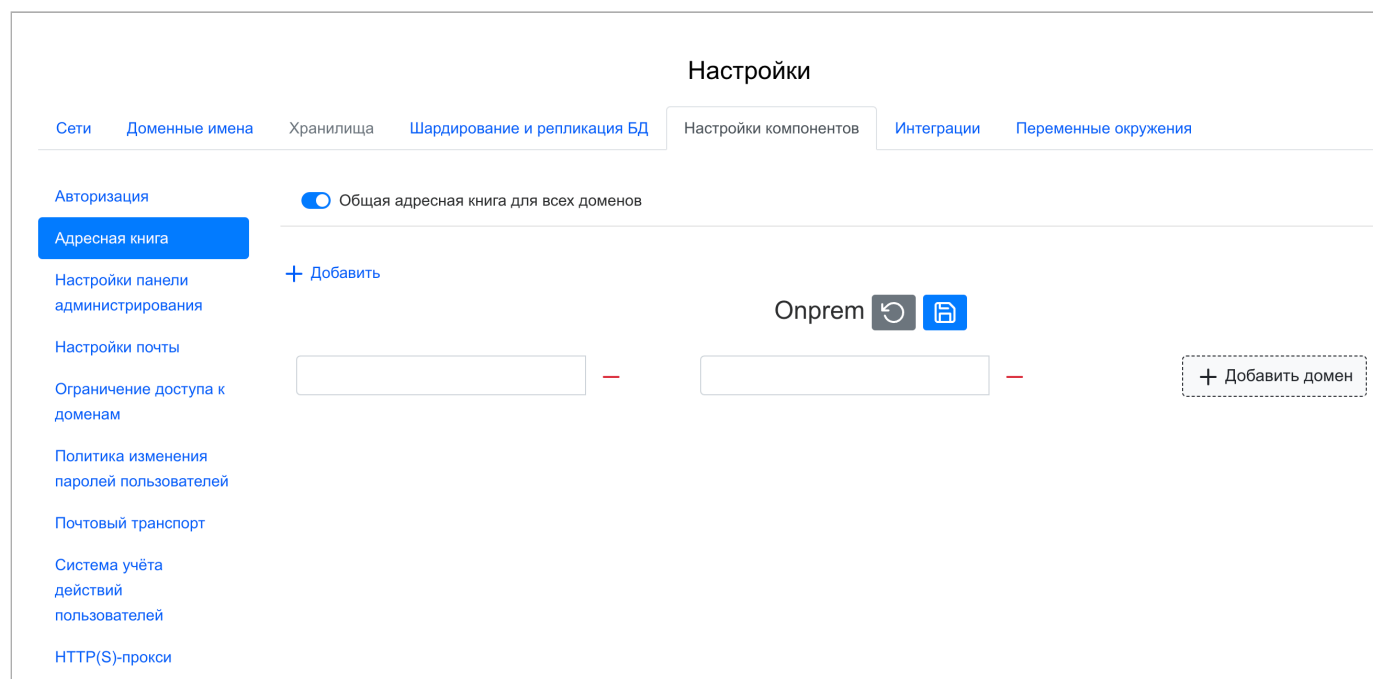
Дальнейшая настройка общих почтовых ящиков производится в административной панели (biz.<почтовый домен>).

Чтобы создать организацию, под которой будут объединены домены, кликните по кнопке **Добавить**.

Появится всплывающее окно, куда нужно ввести название организации.



С помощью кнопки **Добавить домен** введите адреса доменов, относящихся к одной организации.



Также есть возможность изменить названия организаций, добавить дополнительные домены и удалить домены/организации. После создания организаций перейдите к списку машин, чтобы повторить нужные шаги.

Настройки почты

Для изменения настроек в разделе нажмите на кнопку редактирования .

Настройки

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

Авторизация

Адресная книга

Настройки панели администрирования

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

Система учёта действий пользователей

HTTP(S)-прокси

Настройки почты

[Отмена](#) [Сохранить](#)

Максимальная глубина вложенности папок:

Максимальное количество получателей в письме:

Запретить смену имени в подписи к письму

Поменять местами Имя и Фамилию в подписи к письму

Максимальная глубина вложенности папок — вы можете изменить разрешенную глубину вложенности папок, создаваемых пользователями в своих почтовых ящиках. Значение этого поля также используется при миграции. Если глубина вложенности в исходной системе больше установленного значения, папки будут переноситься в папку с крайней допустимой глубиной.

Максимальное количество получателей в письме — можно ограничить количество пользователей, которым письмо будет отправлено одновременно. Значение по умолчанию — 30 получателей, но, если вы хотите изменить их количество, минимальное значение — 100.

Если необходимо запретить в подписи смену имени или поменять местами имя и фамилию, включите соответствующие флаги.

Ограничение доступа к доменам

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

Настройки

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

Авторизация account.dev12.on-premise.ru af.dev12.on-premise.ru af.dev12st.on-premise.ru ampproxy.dev12st.on-premise.ru apf.dev12.on-premise.ru

Адресная книга apf.dev12st.on-premise.ru as.dev12.on-premise.ru auth.dev12.on-premise.ru biz.dev12.on-premise.ru blobcloud.e.dev12.on-premise.ru

Настройки панели администрирования bmw.dev12.on-premise.ru c.dev12.on-premise.ru calendar.dev12.on-premise.ru calendartouch.dev12.on-premise.ru calendarx.dev12.on-premise.ru

Настройки почты cloud.dev12.on-premise.ru cld-uploader.cloud.dev12.on-premise.ru cloclo.cloud.dev12.on-premise.ru cloclo.dev12st.on-premise.ru

Ограничение доступа к доменам cloclo-upload.cloud.dev12.on-premise.ru openapi.cloud.dev12.on-premise.ru pu.cloud.dev12.on-premise.ru sdc.cloud.dev12.on-premise.ru

Политика изменения паролей пользователей cloclo-stock.dev12st.on-premise.ru uploader.e.dev12.on-premise.ru thumb.cloud.dev12.on-premise.ru cld-unzipper.dev12st.on-premise.ru

Почтовый транспорт corsapi.dev12st.on-premise.ru e.dev12.on-premise.ru filin.dev12.on-premise.ru img.dev12.on-premise.ru imgs.dev12.on-premise.ru o2.dev12.on-premise.ru

Система учёта действий пользователей portal.dev12.on-premise.ru proxy.dev12st.on-premise.ru docs.dev12st.on-premise.ru hb.dev12st.on-premise.ru swa.dev12.on-premise.ru

HTTP(S)-прокси tmpatt.dev12st.on-premise.ru webdav.cloud.dev12.on-premise.ru

Домен для веб-интерфейса авторизации

Отмена Сохранить

Ограничить доступ к домену

Режим запрета — запрещать следующим IP/подсетям

IP/Подсети Комментарий

+ Добавить #TASK NUMBER access for ...

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

Настройки

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

Авторизация account.dev12.on-premise.ru af.dev12.on-premise.ru af.dev12st.on-premise.ru ampproxy.dev12st.on-premise.ru apf.dev12.on-premise.ru

Адресная книга apf.dev12st.on-premise.ru as.dev12.on-premise.ru auth.dev12.on-premise.ru biz.dev12.on-premise.ru blobcloud.e.dev12.on-premise.ru bmw.dev12.on-premise.ru

Настройки панели администрирования c.dev12.on-premise.ru calendar.dev12.on-premise.ru calendartouch.dev12.on-premise.ru calendarx.dev12.on-premise.ru cloud.dev12.on-premise.ru

Настройки почты cld-uploader.cloud.dev12.on-premise.ru cloclo.cloud.dev12.on-premise.ru cloclo.dev12st.on-premise.ru cloclo-upload.cloud.dev12.on-premise.ru

Ограничение доступа к доменам openapi.cloud.dev12.on-premise.ru pu.cloud.dev12.on-premise.ru sdc.cloud.dev12.on-premise.ru cloclo-stock.dev12st.on-premise.ru uploader.e.dev12.on-premise.ru

Политика изменения паролей пользователей thumb.cloud.dev12.on-premise.ru cld-unzipper.dev12st.on-premise.ru corsapi.dev12st.on-premise.ru e.dev12.on-premise.ru filin.dev12.on-premise.ru

Почтовый транспорт img.dev12.on-premise.ru imgs.dev12.on-premise.ru o2.dev12.on-premise.ru portal.dev12.on-premise.ru proxy.dev12st.on-premise.ru docs.dev12st.on-premise.ru

Система учёта действий пользователей hb.dev12st.on-premise.ru swa.dev12.on-premise.ru tmpatt.dev12st.on-premise.ru webdav.cloud.dev12.on-premise.ru

Домен для веб-интерфейса авторизации

Отмена Сохранить

Ограничить доступ к домену

Режим запрета — запрещать следующим IP/подсетям

IP/Подсети Комментарий

+ Добавить #TASK NUMBER access for ...

+ Добавить


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

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

⚠ Внимание

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

Панель администрирования

Внутри раздела нужно ввести SPF-запись и DKIM-селектор почтового домена. Так же есть возможность произвести некоторые настройки для административной панели (`biz.<почтовый домен>`). Чтобы начать настройку, нажмите кнопку редактирования .

Настройки

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

Авторизация

Адресная книга

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Панель администрирования

Политика изменения паролей пользователей

Почтовый транспорт

Рассылки



Система расширенных транспортных правил

Система учёта действий пользователей

HTTP(S)-прокси


Настройки панели администрирования


Отмена Сохранить


Административные домены : 

[+ Добавить](#)

Настройки DKIM и SPF для сервера

Серверная SPF-запись :

DKIM-селектор :

Настройки пользователей, доменов панели администрирования 

Количество дней перед удалением пользователя:

Размер облака пользователя по умолчанию (Мб):

Разрешить предварительную настройку сборщиков для всего домена

Не проверять актуальность включенного функционала (фич)

Общие переменные окружения для всех сервисов панели администрирования:

[+ Добавить](#)

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

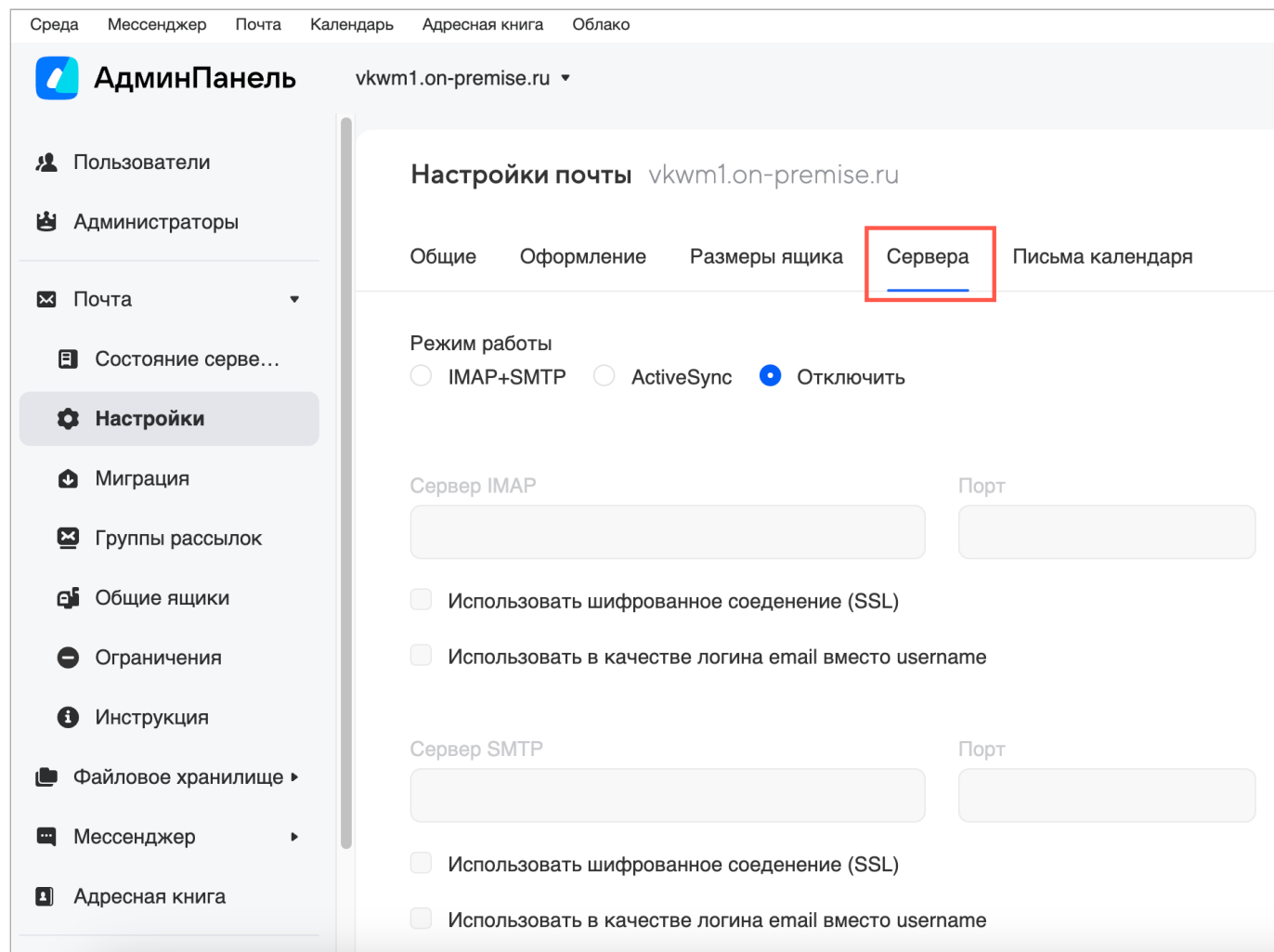
Серверная SPF-запись — введите в поле имя SPF-записи в DNS вашего домена, например: `my_spf_record.onprem.ru`. По умолчанию в SPF-запись ищется по следующему имени: `_spf.<почтовый домен>`. Подробнее про SPF-запись можно прочитать в статье [Настройка SPF](#).

DKIM-селектор — в поле нужно добавить селектор DKIM-подписи почтового домена.

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

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

Разрешить предварительную настройку сборщиков для всего домена — включите флаг, если необходимо отобразить окно настроек сборщиков писем в административной панели `biz.<почтовый домен>/domains/`.



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

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

Политика изменения паролей пользователей

Внимание

При интеграции с Active Directory эта вкладка неактуальна. С включенной интеграцией пользователи, заведенные внутри Почты, не смогут совершать никаких действий.

Для изменения настроек во вкладке кликните по кнопке редактирования .

Настройки

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

Авторизация

Адресная книга

Настройки панели администрирования

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

Мониторинг

HTTP(S)-прокси

Политика изменения паролей пользователей

Отмена
Сохранить

Разрешить пользователям менять пароли

Установить максимальный срок действия пароля

Максимальный срок действия пароля (в секундах) :

3.00 месяцев

Разрешить пользователям менять пароли — включенный флаг разрешает пользователям менять пароли для своих почтовых ящиков.

Установить максимальный срок действия пароля — при установленном флаге можно установить срок действия пароля. Срок задается в секундах (под полем есть подсказка о том, сколько это будет в более крупных единицах измерения).

Почтовый транспорт

В этой вкладке вы можете изменить нужные вам настройки, нажав на кнопку редактирования .

Настройки

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

Авторизация

Адресная книга

Настройки панели администрирования

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

Мониторинг

HTTP(S)-прокси

Настройки почтового транспорта

Отмена
Сохранить

Перемещать письма в спам по заголовку от **Kaspersky Linux Mail Server** ⓘ

Устанавливать заголовок **Received** в соответствии требованиям **Kaspersky Linux Mail Server**

Не сбрасывать письма на **MX-сервере** при проблемах доставки в **медленную очередь** ⓘ

Запретить на **MX-сервере** приём писем **для** неприпаркованных доменов ⓘ

Запретить на **MX-сервере** приём писем **от** припаркованных доменов ⓘ

Исключения ⓘ + Добавить

Перед почтовой системой есть почтовый шлюз ⓘ

Промежуточный MX-сервер ⓘ:

Отправлять письма **внутри** системы через почтовый шлюз ⓘ

Список почтовых шлюзов для писем внутри почтового решения ⓘ оставьте пустым, если достаточно отправки по MX-записи + Добавить

Перемещать письма в спам по заголовку от Kaspersky Linux Mail Server — включите флаг, если необходима проверка на заголовок X-KLMS-Message-Action. Если у письма присутствует этот заголовок и его значение отличается от **clean**, оно будет автоматически отправляться в папку Спам.

Устанавливать заголовок Received в соответствии требованиям Kaspersky Linux Mail Server — в некоторых случаях Kaspersky Linux Mail Server не может определить последний хоп (расстояние между ближайшими узлами в сетевом протоколе) передаваемого сообщения, из-за этого могут появиться ошибки с валидацией отправителя и проверкой SPF. Чтобы избежать подобных ситуаций, установите этот флаг.

Не сбрасывать письма на MX-сервере в медленную очередь при проблемах доставки — включите флаг, если ваша антиспам/антивирус система не умеет определять сервер отправки почты. Так как медленная почтовая очередь в Почте реализована отдельным шлюзом, с выключенным флагом могут происходить сбои при проверке подлинности отправителя.

Запретить на MX-сервере прием писем для неприпаркованных доменов — чтобы запретить прием писем для доменов с непроверенной MX-записью, включите этот флаг. При включенной отправке писем внутри системы через почтовый шлюз эта опция также будет включена автоматически.

Информация

Чтобы домен считался **припаркованным**, он должен быть добавлен в панель администратора (`biz.<почтовый домен>`); **MX-запись** припаркованного домена должна быть проверена. **Перепиской внутри системы** будет считаться обмен сообщениями между **двумя припаркованными доменами**. Чтобы домен считался **известным**, достаточно добавить его в панель администратора.

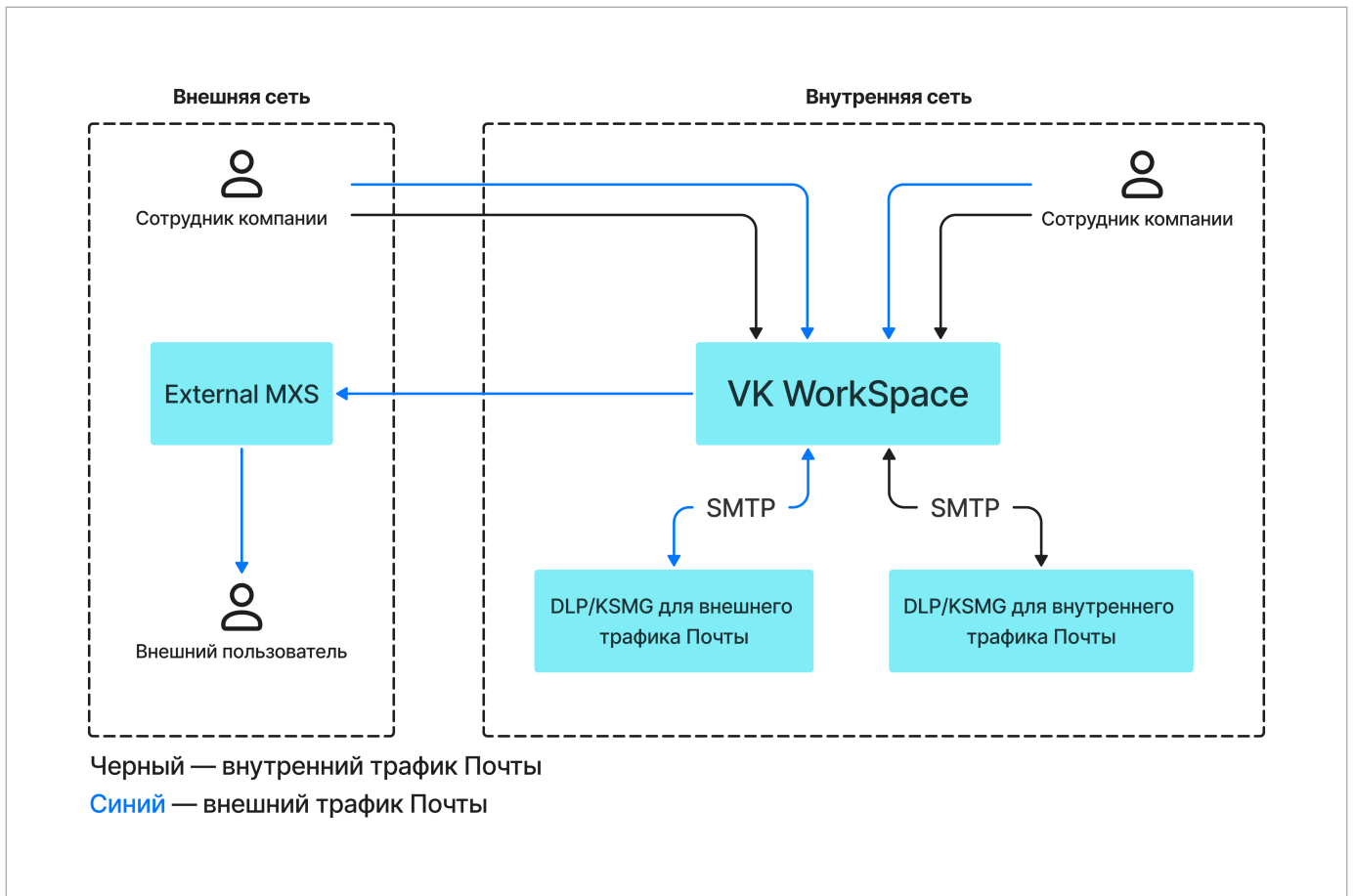
Запретить на MX-сервере прием писем от припаркованных доменов — используется для защиты от подделки злоумышленниками писем локальных пользователей. Это неполноценная защита от подделки отправителя, поэтому рекомендуется установка полноценной антиспам-системы.

Перед почтовой системой есть почтовый шлюз — если перед почтовой системой VK WorkSpace будет установлен какой-либо почтовый шлюз, включите этот флаг. В поле нужно будет ввести адрес промежуточного MX.

Отправлять письма внутри системы через почтовый шлюз — если в вашей инфраструктуре есть система DLP или система антивирусной проверки и вы хотите отправлять всю исходящую переписку через них, включите эту опцию. Письмо от внутреннего отправителя будет перенаправляться в DLP/антивирус для проверки, а затем возвращаться в Почту для доставки отправителю. DLP/антивирус при этом должны работать в режиме SMTP relay. Если опция выключена, письма внутри системы доставляются сразу в почтовый ящик получателя.

Отправлять письма за пределы системы через почтовый шлюз — если в вашей инфраструктуре есть система DLP или система антивирусной проверки и вы хотите отправлять всю исходящую переписку ко внешним отправителям через них, включите эту опцию. Письмо от внутреннего отправителя будет перенаправляться в DLP/антивирус для проверки, а затем отправляться во внешний контур для доставки отправителю. DLP/антивирус при этом должны работать в режиме SMTP relay. Если опция выключена, письма внутри системы доставляются сразу в почтовый ящик получателя.

Ниже представлена схема движения трафика Почты при интеграции с системой DLP:



Отправлять письма за пределы системы через почтовый шлюз ⓘ

Список почтовых шлюзов для отправки писем за пределы почтового решения ⓘ добавьте хотя бы один сервер [+ Добавить](#)

Кастомные маршруты для доменов ⓘ	Почтовые домены	+ Добавить
----------------------------------	-----------------	----------------------------

Список серверов, имеющих право отправлять почту без авторизации ⓘ [+ Добавить](#)

Список серверов, имеющих право отправлять почту без авторизации для определённых почтовых доменов ⓘ [+ Добавить](#)

Отправлять копии сообщений внутри системы на email ⓘ:

Канонические (PTR) имена гипервизоров ⓘ

mail-dev12:

Кастомные маршруты для доменов — вы можете перенаправить домены на заданные шлюзы вместо стандартных. Вы можете внести в раздел «Почтовые домены» несколько доменов и задать для них

несколько адресов шлюзов. Если нужно добавить по одному шлюзу для каждого домена, используйте кнопку **Добавить**.

Список серверов, имеющих право отправлять почту без авторизации — добавьте список IP-адресов серверов, почта с которых будет приниматься без авторизации. В список нужно обязательно добавить адреса шлюзов, с которых почта должна возвращаться в сервис Почта. В этот же список можно внести серверы рассылки почты или в соответствии с их назначением МФУ, отсканированные документы с которых будут отправляться без авторизации. Почта, отправленная в Почту VK WorkSpace без авторизации, будет приниматься на порту **1025**.

Список серверов, имеющих право отправлять почту без авторизации для определенных почтовых доменов — если вы планируете использовать несколько почтовых доменов, есть возможность добавить для каждого домена свои доверенные IP. Письма с указанных доменов должны отправляться на порт **1025**.

Отправлять копии сообщений внутри системы на email — в почтовой системе VK WorkSpace реализована возможность отправки копий внутренней переписки на специальный ящик. В таком случае проверка внутренних писем не будет блокировать потоки почты.

Канонические (PTR) имена гипервизоров — укажите название хоста в PTR-записи. PTR-запись позволяет определить по IP имя хоста, с которого приходит почта. Если при проверке имя хоста будет отличаться, письмо не будет доставлено или попадет в папку Спам.

Рассылщики

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

Настройки

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

[Авторизация](#) [VK WorkDisk](#) [Отзыв письма VK WorkMail](#) **Панель администрирования**

[Адресная книга](#) **Панель администрирования** [Отмена](#) [Сохранить](#)

[Настройки почты](#) Email отправителя:

[Ограничение доступа к доменам](#) Имя отправителя:

[Панель администрирования](#) Адрес сервера пересылки:

[Политика изменения паролей пользователей](#) Порт сервера пересылки:

[Почтовый транспорт](#)

Рассылки

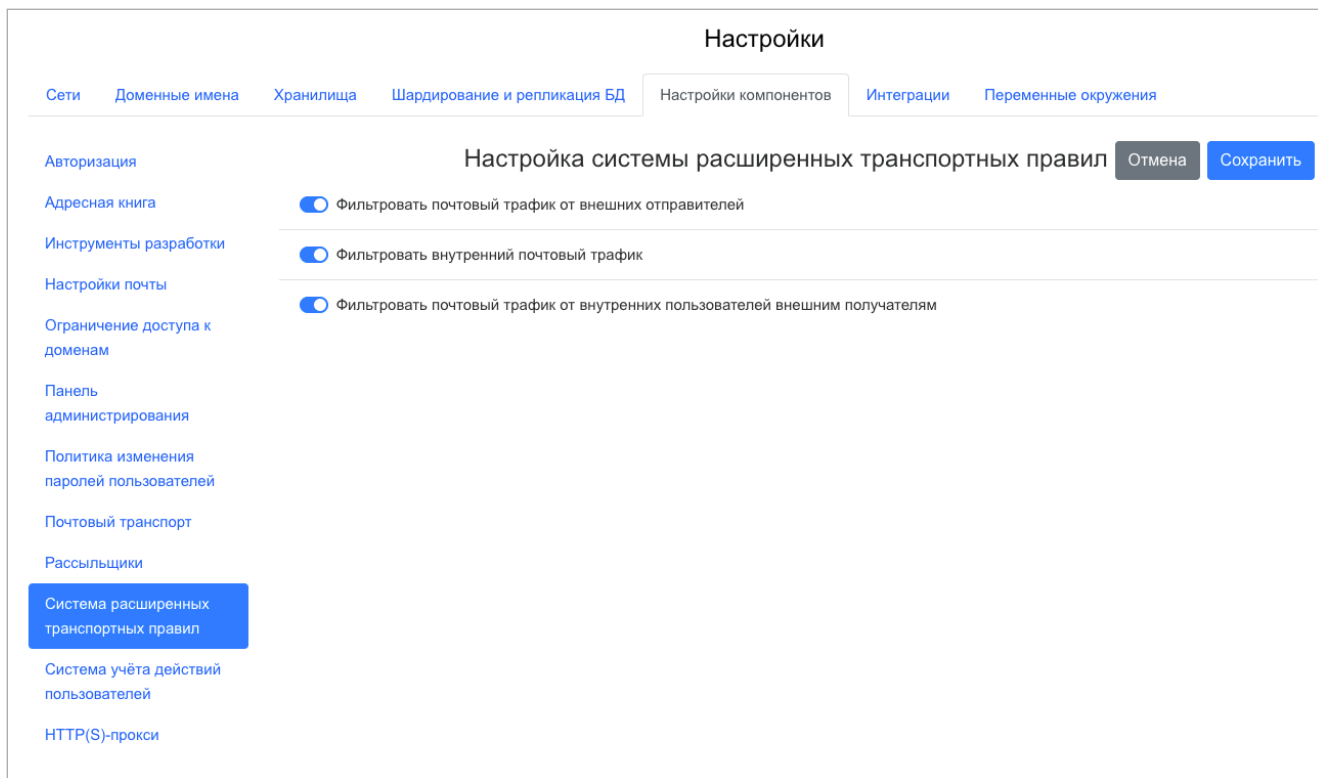
[Система учёта действий пользователей](#)

[HTTP\(S\)-прокси](#)

1. Введите email и имя отправителя.
2. Введите адрес и порт сервера рассылки.
3. Сохраните изменения.
4. Перейдите к списку ролей и запустите автоматическую установку, чтобы применить настройки.

Система расширенных транспортных правил

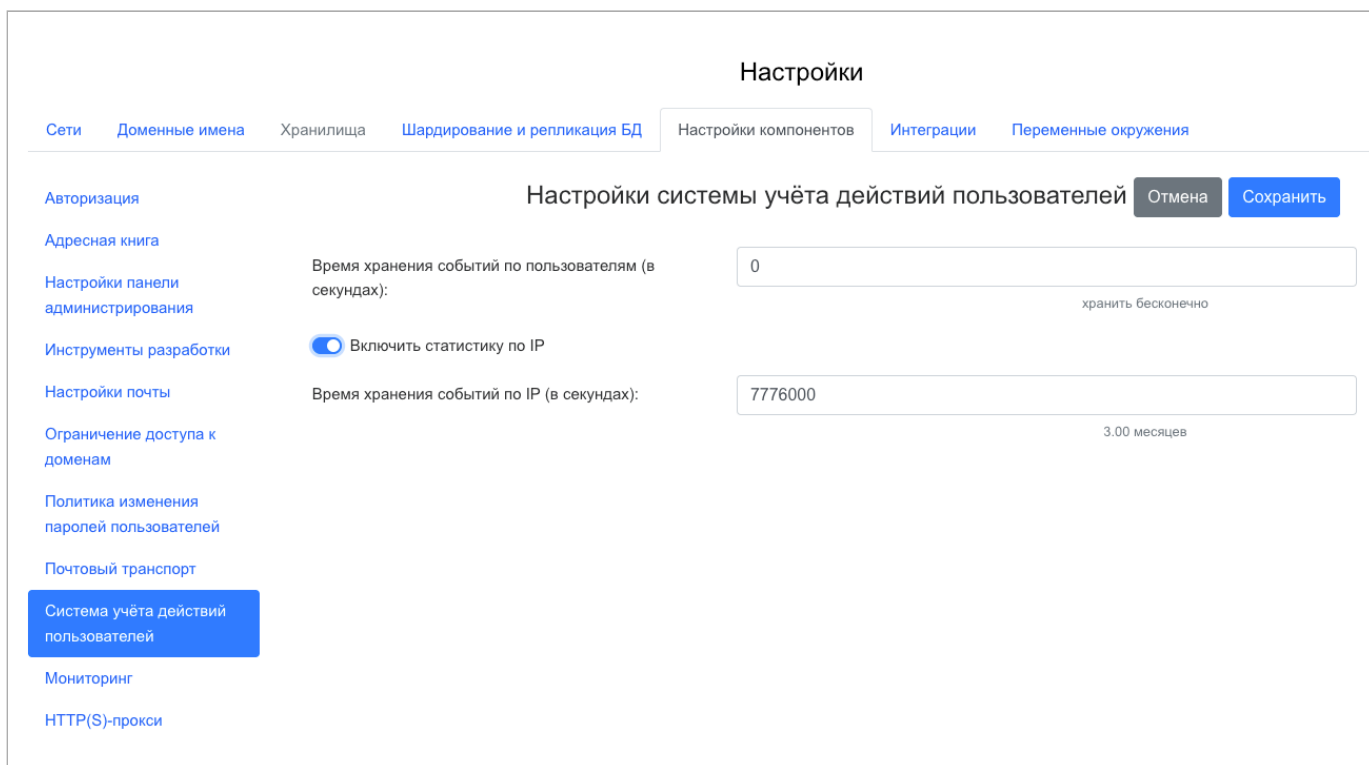
1. Нажмите на **i** и перейдите в раздел **Продукты**.
2. Включите флаг **Система расширенных транспортных правил**.
3. Перейдите к списку ролей и запустите автоматическую установку.
4. Когда нужные роли сгенерируются, перейдите в раздел **Компоненты** → **Система расширенных транспортных правил** и включите нужные флаги.



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

Система учета действий пользователей

Чтобы изменить время хранения логов, кликните по кнопке редактирования.



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

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

Мониторинг

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

Чтобы включить внешнюю систему мониторинга:

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

Система отправки push-уведомлений на мобильные устройства

Система мониторинга
Grafana, хранилище метрик Graphite, хранилище метрик Prometheus

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

Система аудита действий пользователя
Сервисы записи и чтения действий пользователей, хранилище действий пользователей (ScyllaDB)

Дублирование действий пользователей во внешние хранилища

Система аудита действий пользователя (облегчённая версия)
Сервисы записи и чтения действий пользователей, хранилище действий пользователей (PostgreSQL)

Сохранить

Примечание



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

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

Внимание

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

- Чтобы предотвратить возможные проблемы, перейдите в консоль и перезапустите установщик с помощью команды: `sudo systemctl restart deployer`.
- После перезапуска в списке ролей отобразятся роли, которые нужно удалить. Если в интерфейсе не подсветились роли для удаления, перезагрузите страницу.

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

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

Настройки

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

Авторизация

Адресная книга

Настройки панели администрирования

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

Система учёта действий пользователей

Мониторинг

HTTP(S)-прокси

Настройки мониторинга

Отмена
Сохранить

Внешний сервер Graphite

IP-адрес или домен Graphite-сервера:

Порт Graphite-сервера:

Протокол подключения:

Внешний сервер Prometheus

IP-адрес или домен Prometheus-сервера:

Порт Prometheus-сервера:

[Набор готовых дашбордов для Grafana](#)

9. Сохраните изменения.

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

Настройки HTTP(S)-прокси

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

Настройки

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

Авторизация

Адресная книга

Настройки панели администрирования

Инструменты разработки

Настройки почты

Ограничение доступа к доменам

Политика изменения паролей пользователей

Почтовый транспорт

Система учёта действий пользователей

Мониторинг

HTTP(S)-прокси

Настройки HTTP(S)-прокси

Отмена
Сохранить

Перед VK WorkSpace есть прокси-сервер ⓘ

Список IP прокси-серверов ⓘ -

[+ Добавить](#)

HTTP-заголовок прокси с оригинальным IP клиента ⓘ:

HTTP-заголовок прокси с оригинальным протоколом подключения клиента ⓘ:

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

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

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

Шаг 12. Интеграции

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

[Настройка интеграции VK Teams и Почты](#) — с помощью документа вы сможете настроить интеграцию между VK Teams и Почтой.

[Миграция календарей по протоколу EWS](#) — документ по настройке миграции событий из MS Exchange в сервис Почта.

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

[Аудит действий пользователей](#) — в документе описаны предусмотренные в Почте системы аудита действий пользователя и их отличия. Описано, как включить сбор статистики по IP и настроить отправку событий во внешние хранилища.

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

Сборщик почты

В разделе есть возможность добавить почтовые серверы для синхронизации/миграции, а также список папок, которые не будут участвовать в синхронизации.

Белый список удалённых серверов — по умолчанию в полях указаны внутренние IP-адреса. Если вы планируете миграцию почты с других почтовых серверов, добавьте их IP-адреса или имена в белый список — Почта будет определять эти IP/хосты как публичные. При миграции из систем с белым IP/

доменом поле можно оставить пустым. При настройке миграции в административной панели вам нужно будет ввести IP/хост, с которого будет производиться миграция.

Список папок, исключенных из синхронизации — если у вас есть папки, которые не должны участвовать в синхронизации в соответствии с их назначением «Черновики» и «Удаленные», введите их названия через запятую **в строгом соответствии** с оригинальным названиям из вашей системы (названия папок регистрозависимы).

Интеграция с другими инсталляциями Почты

Информация

Функциональность устарела и будет в скором времени удалена.

В разделе вы можете настроить интеграции с несколькими инсталляциями Почты и/или миграции с Exchange и других почтовых серверов.

Чтобы перейти к настройкам, нажмите на кнопку редактирования. Появится возможность изменить значения полей.

Настройки

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

Интеграция с WOPI-редактором **Настройки интеграции с другими инсталляциями VK WorkMail** Отмена Сохранить

Лицензия редактора Р7-Офис Список адресов машин с БД namespace sharing: —
+ Добавить

Сборщик почты Перенаправлять письма неизвестных получателей на сервер:

Интеграция с другими инсталляциями VK WorkMail **Deprecated**

Дублирование действий пользователей во внешние хранилища

Список адресов машин с БД namespace sharing — с помощью кнопки **Добавить** внесите IP-адреса машин с инсталляциями Почты. При нескольких инсталляциях введите все адреса машин, объединенных в БД namespace sharing.

Каждая из инсталляций получит реплики каталогов пользователей с IP, указанных в поле. При отправке письма система будет знать, на какой почтовый сервер его направить.

По умолчанию в поле указан локальный IP. Если вы пока что не планируете работу с несколькими инсталляциями, оставьте значение по умолчанию.

Внимание

Если в интеграции участвуют кластерные инсталляции Почты, в поле нужно ввести IP-адреса контейнеров **tnt-fedman1**.

Также потребуется настройка переменных окружения, описанная в следующем шаге.

Перенаправлять письма неизвестных получателей на сервер — если вы будете проводить миграцию с других почтовых серверов, введите его IP-адрес в поле. В случаях, когда письмо отправляется в адрес пользователей, которые еще не мигрировали в Почту, система будет автоматически перенаправлять их на указанный IP-адрес. Перенаправление будет работать только для припаркованных доменов.

Примечание

Дальнейшая настройка миграции с Exchange или других почтовых серверов производится в административной панели Почты VK WorkSpace по завершении установки.

Продублируйте значение по умолчанию из поля выше, если перенаправление писем в данный момент не требуется.

Сохраните изменения и перейдите к следующему шагу, нажав на кнопку **Далее**.

Настройки системы BI-аналитики

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

Примечание

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

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

Настройки

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

Интеграция с WOPI-редактором **Настройки подключения к внешнему серверу Kafka** Отмена Сохранить

Лицензия редактора P7-Офис Адрес сервера Kafka + Добавить

Настройки для Системы BI-Аналитики **1** Имя топика аналитики Kafka: example: analytics-events

Сборщик почты Имя топика почтовой аналитики Kafka: example: mail-events

Интеграция с другими инсталляциями VK WorkMail **Deprecated** Имя топика событий авторизации Kafka: example: security-events

Дублирование действий пользователей во внешние хранилища

Сохраните изменения.

Перейдите к списку ролей, кликнув по логотипу **AdminPanel**. Внизу страницы необходимо создать дополнительные роли.

1. Нажмите на кнопку **Добавить** → **Несколько контейнеров**.
2. В поле **Установлено не более:** введите значение **0**. Появятся контейнеры для распределения.
3. Добавьте контейнеры для Clickhouse на гипервизоры для хранилищ.
4. Если вы используете Kafka внутри инсталляции, распределите контейнеры с Kafka на гипервизоры для баз данных тем же способом (с помощью кнопки **Добавить**).
5. По окончании генерации контейнеров запустите **автоматическую установку** в общей строке состояния.

Когда установка будет завершена, у вас появится возможность просматривать статистику Диска в панели администратора.

Шаг 13. Переменные окружения


В разделе производится настройка кастомных переменных почтовой системы.

Внимание

Настройка переменных окружения возможна только после консультации с представителем VK.

Настройки

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

Установленные пользователем переменные **abookpdd-tar*** ещё не заданы 

Список возможных переменных для роли

Имя переменной	Значение по умолчанию	Описание	Варианты
OVERLORD_CHECKOUT_INTERVAL	60s	Период опроса участников кластера	
OVERLORD_ETCD_PREFIX	/mailonpremise/overlord/	Путь хранения ключей в ETCD	
OVERLORD_ETCD_TIMEOUT	5s	Таймаут подключения к ETCD	
OVERLORD_GCTUNE_DISABLE	true	Выключение gctune для Go	<input type="checkbox"/> true <input type="checkbox"/> false
OVERLORD_GCTUNE_MEM_LIMIT		Ограничение памяти для gc	
OVERLORD_LOG_LEVEL	warn		<input type="checkbox"/> debug <input type="checkbox"/> warn <input type="checkbox"/> info <input type="checkbox"/> error

Чтобы добавить кастомную переменную:

1. Нажмите на кнопку редактирования.
2. Нажмите кнопку **Добавить**.

3. В выпадающем меню выберите название переменной.
4. Введите значение переменной. Значение переменной должно быть введено корректно, иначе установщик не позволит создать переменную.

Настройки

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

Установленные пользователем переменные **abookpdd-tar*** ещё не заданы Отмена Сохранить

abookpdd-tar
addrbook-tar
adloader
aliases-tar
ameli-common
appass-tar
arbuzapi
attfiledb
attfront
attpairdb
attprevfront

OVERLORD_CHECKOUT_INTERVAL : Значение переменной ⓘ

Поле должно соответствовать правилу *id+([m]hs)\$

[+ Добавить](#)

Список возможных переменных для роли

Имя переменной	Значение по-умолчанию	Описание	Варианты
OVERLORD_CHECKOUT_INTERVAL	60s	Период опроса участников кластера	
OVERLORD_ETCD_PREFIX	/mailonpremise/overlord/	Пусть хранения ключей в ETCD	
OVERLORD_ETCD_TIMEOUT	5s	Таймаут подключения к ETCD	
OVERLORD_GCTUNE_DISABLE	true	Выключение gctune для Go	<input type="checkbox"/> true <input type="checkbox"/> false
OVERLORD_GCTUNE_MEM_LIMIT		Ограничение памяти для gc	

5. Нажмите на кнопку **Сохранить**.
6. Нажмите на кнопку **Далее** для перехода к следующему шагу.

Шаг 14. 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**.

AdminPanel

Подтвердите запуск автоматической установки

Автоматическая установка запустит проверку всех шагов и применит найденные изменения.

Выполнение остановится в следующих случаях:

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

Процент контейнеров одной роли, устанавливаемых одновременно:

0

Выполнение установки/проверки можно остановить. В таком случае установщик дождётся завершения выполняемого шага и прекратит установку/проверку.

Отмена Запустить

В зависимости от этапа установки будет меняться цвет индикатора:

- **Серый** — в ожидании начала генерации;
- **Синий** — в процессе генерации;

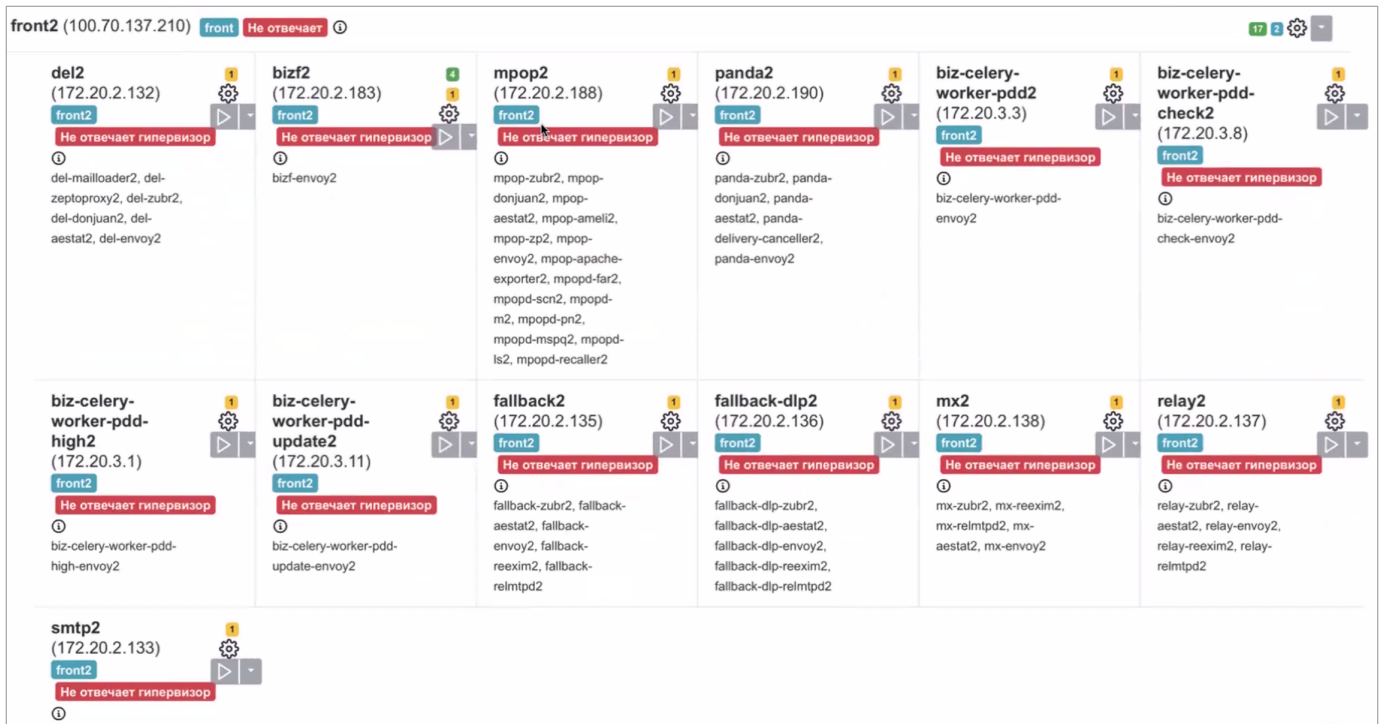
- **Желтый** — шаг необходимо повторить (установщик делает это самостоятельно);
- **Красный** — ошибка.

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.

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



Чтобы продолжить установку:

1. Сгруппируйте объекты по гипервизору — так вам будет наглядно видно, на каком гипервизоре ошибка.

99.65%

Не показывать завершённые
 Объектов в строке: 1

Показать вспомогательные контейнеры
 Группировать:
 ✓ Не группировать
 По роли
По гипервизору

mail-vkwm2-st1 (100.70.80.79)	st		
mail-vkwm2-st2 (100.70.81.195)	st	17 2	⚙️
mail-vkwm2-st3 (100.70.81.200)	st	17 2	⚙️
mail-vkwm2-db1 (100.70.136.197)	db	17 2	⚙️
mail-vkwm2-db2 (100.70.81.80)	db	17 2	⚙️
mail-vkwm2-f1 (100.70.81.128)	front	17 2	⚙️
mail-vkwm2-f2 (100.70.81.139)	front	17 2	⚙️
mail-vkwm2-mon1 (100.70.80.95)	mon	17 2	⚙️

2. После этого перейдите в командную строку и устраните ошибку. По завершении необходимо нажать на шестеренку в строке гипервизора, на котором была ошибка, затем на странице в списке шагов на гипервизоре.




99.65%

Не показывать завершённые
 Объектов в строке: 1

Показать вспомогательные контейнеры
 Группировать: По гипервизору

mail-vkwm2-st1 (100.70.80.79)	st		21 ⚙️
mail-vkwm2-st2 (100.70.81.195)	st		17 2 ⚙️
mail-vkwm2-st3 (100.70.81.200)	st		17 2 ⚙️
mail-vkwm2-db1 (100.70.136.197)	db		17 2 ⚙️
mail-vkwm2-db2 (100.70.81.80)	db	Не отвечает	17 2 ⚙️
mail-vkwm2-f1 (100.70.81.128)	front		17 2 ⚙️
mail-vkwm2-f2 (100.70.81.139)	front		17 2 ⚙️
mail-vkwm2-mon1 (100.70.80.95)	mon		17 2 ⚙️

Добавить

mail-vkwm2-st1 (100.70.80.79) st 21   

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

3. 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			
<input type="checkbox"/> 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!

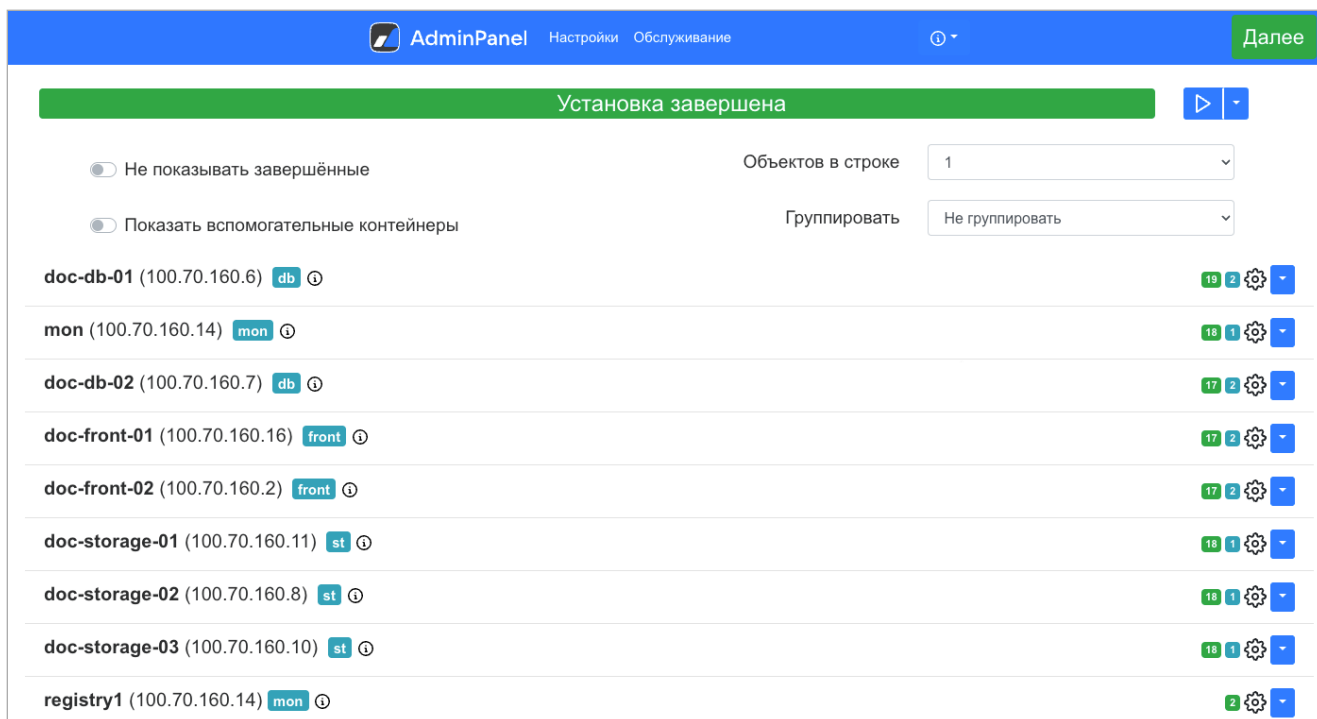
tune_kernel done
Настроить параметры ядра Запустить ▾

4. Повторно запустите автоматическую установку.

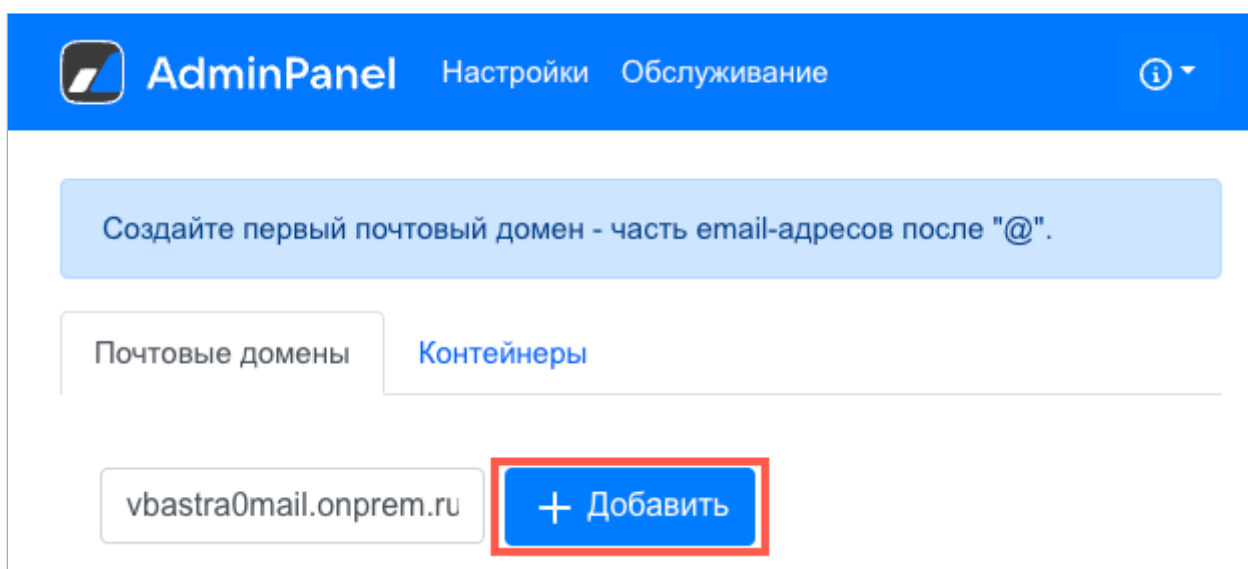
Шаг 15. Завершение установки, инициализация домена и вход в панель администратора

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**.



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>/biz0wner.pass.`

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	Нет записи. Создайте запись с указанными параметрами.
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.

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 RtwvMI5Mfh2EUEXVagkpm2aYqTNL71NXknUciGPEzHXKh svW9vVTm0p2t9qLFoaaztpkzZkpBwIDAQAB

[Инструкция по настройке](#)

После проверки МХ-записи установку можно считать оконченной. Также потребуется настройка **SPF-записи** и **DKIM-подписи**. Инструкции по их настройке вы найдете по [ссылке](#).

⚠ 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.

Шаг 16. Добавление дополнительных доменов

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

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

vbastra0mail.onprem.ru

Подключить новый проект

✓ **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 адресами в этом домене.

Инструкция по настройке

На обновление записей может потребоваться до 72 часов.

⚠ **Необходима настройка DNS записей для работы DKIM**

Если хотите сделать домен **припаркованным**, необходимо пройти проверку MX-записи способом, описанным выше. Чтобы сделать домен известным для Почты, достаточно просто добавить домен в СПИСОК.

Настройка интеграции с Active Directory

Почта переносит из Active Directory список пользователей, группы рассылок и контакты. При этом Почта не хранит пароли пользователей, то есть вся цепочка аутентификации происходит на стороне AD (LDAP-провайдера). Для каждого домена интеграция с AD настраивается отдельно. Чтобы настроить интеграцию:

1. Перейдите в панель администратора по адресу `biz.<почтовый домен>`.
2. Перейдите в раздел **Конфигурация** → **Настройки**.
3. Уберите чекбокс **Не использовать AD**.

AdminPanel
vbastra0mail.onprem.ru ▾

- 👤 Пользователи
- 👤 Администраторы
- ✉ Почта ▸
- 📁 Файловое хранилище ▸
- 📖 Адресная книга
- 🏢 Структура компании
- ⚙ Управление доменом
- ⚙ Конфигурация ▾
- ⚙ **Настройки**
- 📊 Мониторинг

Настройки

Active Directory

Адрес AD

Каталоги пользователей

Логин администратора

Пароль администратора

Поле свойства «Отчество»

Использовать шифрованное соединение (LDAPS)

+ Добавить сертификат

Игнорировать ошибки сертификата

Дополнительные настройки

Сбрасывать сессии пользователей при изменении пароля

Использовать в качестве логина email вместо username

Не использовать AD

Сохранить

4. Заполните поля:

Адрес AD — адрес вашего каталога Active Directory.

Каталоги пользователей — введите значение поля **distinguishedName** из списка атрибутов каталога. Например, `OU=demoapp.DC=presale.DC=local`.

✎ Примечание

Если вам нужно указать больше одного каталога пользователей, обратитесь к представителю VK.

Логин администратора — логин пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

Пароль администратора — пароль пользователя Active Directory с правами на чтение каталога и авторизацию пользователей.

Поле свойства «Отчество» — если вы используете свойство **Отчество**, введите его значение в это поле.

Использовать шифрованное соединение (LDAPS) — есть возможность добавления сертификата LDAPS с помощью кнопки **Добавить сертификат**.

Игнорировать ошибки сертификата — отметьте этот чекбокс, если у вас самоподписанный SSL-сертификат.

Сбрасывать сессии пользователей при изменении пароля — если чекбокс отмечен, при изменении пароля пользователя в Active Directory будет сбрасываться сессия в Почте.

Использовать в качестве логина email вместо username — в текущей версии поле не используется.

5. Нажмите на кнопку **Сохранить**.

Синхронизация с AD выполняется один раз в час. Если AD содержит много данных, то одного часа может быть недостаточно для синхронизации всего объема. В этом случае через час после настройки подключения в разделе Пользователи отобразятся не все пользователи из AD, а только часть. Просто подождите еще час.

Внимание

Если объем данных в AD очень большой, при синхронизации может временно отображаться ошибка 502 (или 504). Не переживайте, дождитесь окончания синхронизации.

Если пользователи не появились в Почте, нужно проверить корректность настроек синхронизации с Active Directory с помощью консольной команды:

```
sudo journalctl -fu onpremise-container-adloader1.service
```

Дополнительная документация

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

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

[Как обновить лицензионный ключ](#)

[Установщик не может получить доступ до гипервизора](#)

Логи и полезные команды

Все команды, перечисленные ниже, следует выполнять в консоли машины-мониторинга.

1. Перезапуск установщика:

```
sudo systemctl restart deployer
```

2. Логи установщика:

```
sudo journalctl -fu deployer
```

3. Список запущенных контейнеров:

```
docker ps
```

4. Логи конкретного контейнера:

```
sudo journalctl -eu имя_контейнера
```

5. Статус контейнера:

```
systemctl status имя_контейнера
```

6. Посмотреть список «сломанных» контейнеров:

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

7. Посмотреть список всех не запустившихся контейнеров:

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

8. Удалить контейнер:

```
sudo docker rm имя_контейнера
```

Дата обновления документа: 16.09.2024