МойОфис
Почта 3

В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

Руководство по установке

СЕРВЕРНАЯ ЧАСТЬ

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«МОЙОФИС ПОЧТА 3»
В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

СЕРВЕРНАЯ ЧАСТЬ

3.1G

РУКОВОДСТВО ПО УСТАНОВКЕ

Версия 1

На 71 листах

Дата публикации: 12.09.2024

Москва

2024

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

СОДЕРЖАНИЕ

В настоящем документе используются следующие сокращения (см. таблицу 1).

Таблица 1 – Сокращения и расшифровки

Сокращение	Расшифровка и определение
389-ds, 389 Directory Server	Служба каталогов
Ansible	Система управления конфигурациями, использующаяся для автоматизации настройки и развертывания программного обеспечения
API	Application Programming Interface, интерфейс программирования приложений
CO	CloudOffice, Облачный Офис, общее название продукта (группы редакторов)
DNS	Domain Name System, система доменных имён
Docker	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации
IMAP	Internet Messagess Access Protocol, протокол доступа к ящику электронной почты
LDAP	Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам
Node (нода)	Сервер одной из ролей
PGS	File Storage, Pythagoras, программный продукт «Система хранения данных МойОфис»

Сокращение	Расшифровка и определение
PSN	Poseidon, приложение почты, календаря и контактов (оно же «МойОфис Почта»)
PSNAPI, PBMAPI	API «МойОфис Почта»
Resource overcommit	Ситуация, при которой виртуальных ресурсов выделяется больше, чем физических
SMTP	Simple Mail Transfer Protocol, протокол передачи сообщений электронной почты
SSH	Secure Shell, «безопасная оболочка»
URL	Uniform Resource Locator, единый указатель ресурса
БД	База данных
Вендор (vendor)	Поставщик брендированного продукта
Кластер (cluster)	Объединенная группа серверов
Контур инсталляции	Приватная сеть, в рамках которой происходит обмен техническими данными между серверами инсталляции
Плейбук (playbook)	Набор последовательных инструкций для выполнения команд Ansible
ПО	Программное обеспечение
ОС	Операционная система
Соль	Строка данных, предназначенная для вычисления хэша
Тенант (tenant)	Элемент мультиарендной системы
Хост (host)	Устройство, предоставляющее сервисы формата “клиент-сервер”

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

«МойОфис Почта 3» в варианте исполнения ГОСТ - корпоративная почтовая система для ведения деловой переписки, планирования рабочего времени и управлениями контактами в государственных организациях и на коммерческих предприятиях, использующих отечественные средства криптографической защиты информации.

Продукт позволяет шифровать и расшифровывать сообщения, подписывать сообщения электронной подписью сообщений и проверять электронную подпись отправителей. Взаимодействие всех клиентских приложений с серверными системами осуществляется по сетевым каналам, защищенным с помощью протокола TLS с использованием отечественной криптографии.

Включает почтовую систему, административную панель почтовой системы и приложения для управления почтой, календарем, контактами и задачами на компьютерах, в веб-браузерах и на мобильных устройствах.

1.2 Требования к квалификации персонала

Администратор должен соответствовать следующим требованиям:

- Основы сетевого администрирования:
  - Сетевая модель OSI и стек протоколов TCP/IP;
  - IP-адресация и маски подсети;
  - Маршрутизация: статическая и динамическая;
  - Протокол обеспечения отказоустойчивости шлюза (VRRP).
- Опыт работы со службой доменных имен (DNS):
  - Знание основных терминов (DNS, IP-адрес и т.д.);
  - Понимание принципов работы DNS серверов;
  - Знание основных типов записей DNS:
    - A (address)
    - MX
    - SRV
    - PTR
    - TXT (SPF, DKIM)

  - Опыт обращения к RFC по следующим ресурсным записям:
    - Simple Mail Transfer Protocol;
    - Anti-Spam Recommendations for SMTP MTAs;
    - DomainKeys Identified Mail (DKIM) and Mailing Lists;
    - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email;
    - Use of SRV Records for Locating Email Submission/Access Services;
    - Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions toWebDAV (CardDAV).
- Опыт работы с командной строкой ОС Linux.
- Опыт работы с ПО для контейнеризации Docker/Docker Swarm.
- Знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:
  - Закрытый и открытый ключ;
  - Сертификат открытого ключа;
  - Регистрационный центр (RA);
  - Сертификационный центра (CA);
  - Хранилище сертификатов (CR).
- Практический опыт работы и администрирования сервисов: Redis, PostgreSQL, 389 Directory Server, Dovecot, Postfix, GlusterFS, etcd.
- Опыт работы с системой автоматизации развертывания Ansible.

1.3 Системные требования

– Поддерживаемые операционные системы: **Centos 7.9**, **Astra Linux 1.7 SE**, **Альт Сервер 9, 10.1**, **RedOS 7.3.2, РОСА «ХРОМ» 12 Сервер**;
– Скорость сетевой подсистемы для взаимодействия между серверами в случае кластерной инсталляции – 1Gbit/s или выше;
– В таблице 2 приведены характеристики аппаратного обеспечения конфигурации для функционального тестирования (без отказоустойчивости).

Таблица 2. Характеристики аппаратной конфигурации без отказоустойчивости

Конфигурация	CPU	RAM (Gb)	HDD (Gb)
минимальная	4	8	50 + Квота пользователей на использование дискового пространства
рекомендованная	8	16	100 + Квота пользователей на использование дискового пространства + База данных

– Рекомендации по разбиению дисков целевого сервера для ОС и пользовательских квот приведены в таблице 3.

Таблица 3. Разбиение дисков

Назначение	Точка монтирования	Объем
ОС	/	50GB
Квота почтовых ящиков пользователей при standalone-конфигурации	/var/dovecot	суммарный объем квот пользователей + 20%

Подробнее о кластерной инсталляции написано в разделе Типовые схемы установки данного руководства.

1.3.1 Рекомендации по использованию файловых систем

В соответствии с рекомендациями производителей операционных систем для **CentOS** рекомендуется использовать файловую систему XFS, для **Альт Сервер**, **Astra Linux**, **RedOS** и **РОСА «ХРОМ»** - ext4.

Разбивку дисков рекомендуется выполнять следующим образом:

– в режиме с отказоустойчивостью (cluster) для серверов всех ролей, кроме syslog, рекомендуется выделить не менее 40 Gb для штатной работы ОС;
– в режиме без отказоустойчивости (standalone) рекомендуется выделить не менее 50 Gb на корневой раздел;
– в режиме с отказоустойчивостью (cluster) для сервера роли `syslog` рекомендуется выделить не менее 100 Gb для штатной работы ОС и хранения всех логов;

– более подробная информация по разбивке дисков для конкретных ролей подсистемы «МойОфис Почта» указана в разделе Рекомендации по разбиению дисков данного руководства.

Окончательные системные требования и требования к дисковой подсистеме расчитываются по запросу исходя из сайзинга.

1.4 Ограничения

– Не допускается в среде виртуализации использовать клонированные виртуальные машины для инсталляции продукта;
– Не допускается копирование установленных операционных систем между физическими серверами или использование образа предустановленной операционной системы для развертывания физических серверов;
– Не допускается resource overcommit в среде виртуализации (см. таблицу 1);
– Не допускается использование DHCP-служб в сегменте сети инсталляции.

2 ОПИСАНИЕ АРХИТЕКТУРЫ «МОЙОФИС ПОЧТА»

Внутренняя структура «МойОфис Почта» представляет собой набор сервисов, обеспечивающих работу ПО и взаимодействие с компонентами «МойОфис Частное Облако». Более подробно сервисы (представленные в виде инсталляционных ролей) описаны в разделе Описание ролей данного руководства. Детальная архитектурная схема «МойОфис Почта» приведена на Рисунке 1.

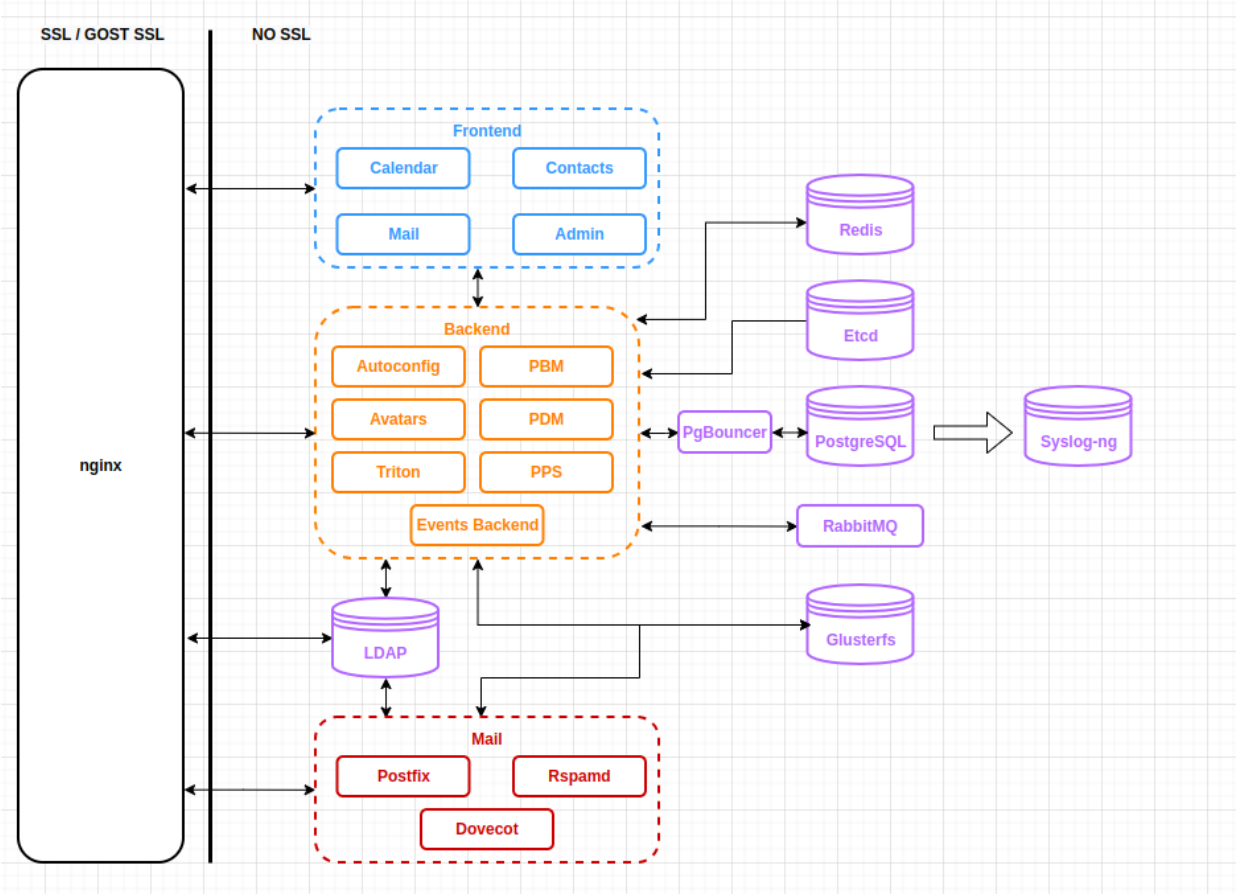

Рисунок 1. Архитектурная схема «МойОфис Почта»

3 ТИПОВЫЕ СХЕМЫ УСТАНОВКИ «МОЙОФИС ПОЧТА»

3.1 Конфигурация без отказоустойчивости

Данная конфигурация характеризуется тем, что все серверные роли развертываются в единственном экземпляре. Инсталляция такого типа не требует установки подсистемы балансировки – все роли устанавливаются на один физический (или виртуальный) сервер, или на несколько виртуальных серверов в рамках одного физического сервера, при количестве хостов в каждой роли, не превышающем один. Такая конфигурация может использоваться в целях разработки или демонстрации возможностей продукта (virtual appliance).

3.2 Кластерная отказоустойчивая конфигурация

В данной конфигурации роли (все или некоторые) устанавливаются на разные виртуальные сервера, а также, по возможности, разносятся на разные физические сервера или гипервизоры.

Более подробно о конфигурировании кластерной инсталляции «МойОфис Почта» рассказано в разделе Подготовка инфраструктуры установки данного руководства.

3.3 Типовая схема масштабирования

Для односерверной (не кластерной) конфигурации возможно только вертикальное масштабирование. При этом следует учитывать ограничения Docker и других системных сервисов. Переход от такой конфигурации к кластерной возможен только путем резервирования баз данных и переустановки программного продукта в соответствии с руководством по установке «МойОфис Почта».

4 УСТАНОВКА

4.1 Состав дистрибутива

Дистрибутив «МойОфис Почта» представляет собой инсталляционный архив в формате .tgz и файлы SHA256 и MD5-хеша с контрольной суммой. Архив включает в себя:

– набор Ansible плейбуков для развертывания ролей;
– архив образа Docker Registry.

4.2 Подготовка к установке

4.2.1 Описание ролей

В процессе развёртывания Ansible работает с логическими группами (или ролями), на которые будет разделён целевой сервер (или группа серверов) инсталляции. Они указаны в таблице 4.

Таблица 4. Логические роли системы «МойОфис Почта»

Роль	Значение
check-certificates	Проверка наличия ssl-сертификатов, необходимых для работы Продукта
chrony	Настройка сервиса синхронизации времени
timezone	Установка системного часового пояса
sysctl	Конфигурирование необходимых параметров ядра с помощью sysctl
common	Установка необходимых пакетов и зависимостей
docker	Роль, отвечающая за установку и настройку Docker
swarm	Роль для включения системы оркестрации Docker Swarm
docker registry	Запуск сервиса для хранения и распространения контейнеров Docker
load balancer	Роль для настройки внешего балансировщика трафика
etcd	Запуск распределенной системы хранения конфигураций для сервисов
postgres	Запуск основной базы данных
redis	Запуск сервиса баз данных "ключ-значение"
ldap	Запуск сервиса службы каталогов
frontend	Запуск веб-интерфейса «МойОфис Почта»
backend	Запуск сервисов, отвечающих за функционирование внутренней программной части Продукта
proxy	Запуск проксирующейго сервиса (nginx)

Роль	Значение
mail	Запуск сервисов почтовой подсистемы
syslog	Запуск сервиса сбора логов работы компонентов программного комплекса
users	Создание первого тенанта с системе (выполняется в случае установки без интеграции с Частным Облаком)

4.2.2 Подготовка инфраструктуры установки

4.2.2.1 Подготовка инфраструктурной машины

Инфраструктурная машина – выделенный сервер для проведения инсталляции. С инфраструктурной машины должен быть обеспечен доступ ко всем серверам, на которые производится инсталляция. Для инсталляции конфигурации без отказоустойчивости допустимо использовать один сервер в качестве инфраструктурного и целевого. Основные действия, которые необходимо выполнить на инфраструктурной машине:

1. Скачать и инсталлировать минимальный серверный вариант выбранной операционной системы (см. раздел Системные требования данного руководства).
2. Предустановить на целевую ОС python3 (версии не ниже 3.6), rsync.
3. С инфраструктурной машины должен быть возможен ssh доступ на все хосты целевого сервера инсталляции, рекомендуется сделать это при помощи ssh ключа пользователем root или другим пользователем с sudo привилегиями.
4. На инфраструктурную машину должен быть инсталлирован пакет ansible-core версий 2.11 или 2.12. Работа других версий возможна, но не гарантирована.
5. В некоторых дистрибутивах RedHat механизм SELinux включен в режим **Enforcing**, что может потенциально привести к проблемам с установкой. Предлагается перевести его в режим **Permissive**, при котором действия не блокируются, а в лог аудита попадает отчет о действиях.

Подробная документация по установке Ansible

4.2.2.2 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива (общие рекомендации)

Во избежание проблем не рекомендуется использовать системы, на которых ранее были проведены инсталляции программного обеспечения, не относящегося к дистрибутиву «МойОфис Почта»

Для подготовки целевых серверов к установке для них необходимо выполнить следующую последовательность действий:

1. Настроить имя хоста и параметры сети. В случае кластерной установки имя каждого хоста должно быть уникальным. Необходимо учитывать, что интерфейс, используемый в инсталляции для передачи данных, определяется по наличию пути по умолчанию (default route) в конфигурации интерфейса на целевом сервере.
2. Для корректной работы «МойОфис Почта» необходима служба синхронизации времени на всех серверах контура установки. Настройка синхронизации времени производится в процессе деплоя. Для указания адресов ntp-серверов, необходимо изменить переменную `ntp_servers` в `group_vars/all/main.yml`. Значение по умолчанию:

```
ntp_servers:
  - "0.centos.pool.ntp.org"
  - "1.centos.pool.ntp.org"
  - "2.centos.pool.ntp.org"
  - "3.centos.pool.ntp.org"
```

3. Предустановить на целевые ОС python3 (версии не ниже 3.6).

4.2.2.3 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива (с доступом в Интернет)

Для подготовки целевых серверов к установке для них необходимо выполнить последовательность действий из раздела Подготовка инфраструктуры установки данного руководства.

При наличии доступа в Интернет на целевых машинах никаких дальнейших действий не требуется.

4.2.2.4 Подготовка серверов, на которые будет производиться инсталляция дистрибутива (без доступа в Интернет)

В случае, если инфраструктурная машина и целевые серверы расположены в локальной сети и не имеют прямого доступа в Интернет, инсталляцию можно произвести, заранее предустановив на них необходимые пакеты, указанные в таблице 5.

Таблица 5. Пакеты для предустановки на серверы без доступа в Интернет

ОС	Пакет	Примечания
Альт Линукс	ansible-core, ansible, jinja2	Версия ansible-core 2.11 или 2.12
	docker-engine / docker-ce	В новых версиях docker-engine, в старых версиях пакет называется docker-ce. Пользователь, от имени которого происходит развертывание пакетов, должен иметь права на установку и запуск контейнеров.
	python3-module-bcrypt	
	python3-module-docker	
	python3-module-jsondiff	
	python3-module-passlib	
	python3-module-policycoreutils	
	python3-module-pyaml	
	rsync	
	glusterfs9-server	В случае кластерной установки.

Astra Linux	ansible	В AstraLinux 1.7 Ansible необходимо устанавливать через pip:
		`python3 -m pip install ansible-core==2.11.6`
		`python3 -m pip install ansible==4.7.0`
		`python3 -m pip install jinja2`

	docker.io	Пользователь, от имени которого происходит развертывание пакетов, должен иметь права на установку и запуск контейнеров.
	python3-bcrypt	
	python3-docker	
	python3-jsondiff	
	python3-passlib	
	python3-requests	

ОС	Пакет	Примечания
	python3-yaml	
	rsync	
	glusterfs-server	В случае кластерной установки. Установку GlusterFS рекомендуется производить из официального репозитория glusterfs, в стандартных репозиториях Astra Linux устаревшая версия)
CentOS	ansible-core, ansible, jinja2	Версия ansible-core 2.11 или 2.12
	docker-ce	Пользователь, от имени которого происходит развертывание пакетов, должен иметь права на установку и запуск контейнеров.
	rsync	
	Пакеты pip3:	
	bcrypt	Версия 3.1.7
	docker	
	jsondiff	
	passlib	
	pyyaml	
	requests	Версия < 2.29
	selinux	
	glusterfs-server	В случае кластерной установки.
РОСА	ansible-core, ansible, jinja2	Версия ansible-core 2.11 или 2.12
	docker-ce	Пользователь, от имени которого происходит развертывание пакетов, должен иметь права на установку и запуск контейнеров.
	rsync	
	Пакеты pip3:	
	bcrypt	Версия 3.1.7
	docker	
	jsondiff	
	passlib	
	pyyaml	

ОС	Пакет	Примечания
	requests	Версия < 2.29
	selinux	
	glusterfs-server	В случае кластерной установки.
RedOS	ansible-core, ansible, jinja2	Версия ansible-core 2.11 или 2.12
	docker-ce	Пользователь, от имени которого происходит развертывание пакетов, должен иметь права на установку и запуск контейнеров.
	rsync	
	Пакеты pip3:	
	bcrypt	Версия 3.1.7
	docker	
	jsondiff	
	passlib	
	pyyaml	
	requests	Версия < 2.29
	selinux	
	glusterfs-server	В случае кластерной установки.

В случае оффлайн установки плейбук необходимо запускать с параметром `--skip-tags common,docker` (см. подробности о запуске установки в разделе Запуск установки)

4.2.2.5 Проверка и подготовка инсталляционного архива

Для выполнения проверки и подготовки дистрибутива, необходимо:

1. После копирования инсталляционного архива проверить его контрольную сумму MD5 и/или SHA256, в дальнейшем сверив ее с переданной вендором ПО:

```
md5sum -c MyOffice_PSN_SRV-XXX.tgz.md5sum
sha256sum -c MyOffice_PSN_SRV-XXX.tgz.sha256sum
```

В имени архива цифры версии коммерческого релиза представлены знаками X.

2. Распаковать содержимое инсталляционного архива в произвольную директорию и перейти в нее:

```
mkdir install-psn
tar xvzf MyOffice_PSN_SRV-XXX.tgz -C install-psn
cd install-psn
```

Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

3. Перед началом инсталляции ознакомьтесь с главой Известные проблемы и способы их решения.

4.2.3 Настройка основных параметров установки

Для конфигурирования установки необходимо изменить **инвентарный файл** (inventory file), который находится по адресу:

```
inventory/hosts.yml
```

Файл можно открыть в текстовом редакторе и обновить секции `hosts` и `vars` в соответствии с дальнейшими инструкциями.

Инвентарный файл использует формат .yml, более подробно о синтаксисе можно прочитать в документации Ansible. После окончательного заполнения инвентарного файла необходимо сделать его резервную копию, в дальнейшем она может понадобиться для последующих обновлений и некоторых операций по обслуживанию текущей установки.

4.2.3.1 Конфигурирование инвентарного файла: hosts

В секциях `hosts` следует указать доменное имя или IP-адрес целевого сервера, на который будет производиться инсталляция той или иной роли. Для определения принадлежности целевого сервера к роли необходимо добавить его доменное имя или IP-адрес в соответствующую секцию в шаблоне инвентарного файла. Пример:

```
      redis:
         hosts:
            host.example.com
```

Таким образом, роль `redis` была присвоена серверу с доменным именем `host.example.com`, и на данном хосте в дальнейшем будут исполнены установочные команды Ansible.

Более подробно о значении ролей рассказано в разделе Описание ролей данного руководства.

Все роли могут быть совмещены на одном сервере, в таком случае в шаблоне инвентарного файла дублируется секция `hosts`. При необходимости возможно добавить или удалить сервера в группах. В данном примере все роли будут устанавливаться на один сервер по адресу `host.example.com`:

```
      all:
        children:
### SECTION 1: grouping by Roles
          infra:
            children:
              docker_registry:
                hosts:
                  host.example.com:
          db:
            children:
              etcd:
                hosts:
                  host.example.com:
                    volume_device_etcd: "False"
                    volume_device_etcd_path: "/dev/disk/by-uuid/<UUID>"
              redis:
                hosts:
                  host.example.com:
              postgres:
                hosts:
                  host.example.com:
                    volume_device_postgres: "False"
                    volume_device_postgres_path: "/dev/disk/by-uuid/<UUID>"
```

```
            ldap:
              hosts:
                host.example.com:
        frontend:
          children:
            proxy:
              hosts:
                host.example.com:
         backend:
           hosts:
             host.example.com:
         mail:
           hosts:
             host.example.com:
         loadb:
           hosts:
             loadb.example.com:
```

Следует обратить дополнительное внимание на роли `etcd` и `postgres`: у них есть дополнительные переменные `volume_device_<role>` и `volume_device_<role>_path`. Заполнение этих переменных **необходимо** при использовании разделов на выделенных блочных устройствах для хранения данных указанными сервисами. В таком случае, значения меняются на:

```
volume_device_<role>: "True"
volume_device_<role>_path: "<filesystem_path>"
```

Где `<role>` – логическая роль, `<filesystem_path>` – путь до файловой системы устройства. Особенности работы в режиме `volume_device_<role>: "True"`:

1. Не допускается использование одного и того же раздела диска на одном сервере (или виртуальной машине) для нескольких ролей. Необходимо указывать пути, которые не изменятся после перезагрузки сервера или добавлении новых устройств. В случае **кластерной** установки необходимо указывать идентичные пути до устройств для всех нод соответствующей роли. Таким образом, лучше всего использовать тома `lvm` и указывать путь до них в формате `/dev/mapper/<группа томов>/<логический том>`

2. На разделе должна быть создана файловая система, раздел не должен быть смонтирован на момент инсталляции (кроме ситуации повторного запуска или обновления с предыдущих версий).

В режиме `volume_device_<role>: "False"` никаких дополнительных действий от пользователя не требуется, данные хранятся в соответствующих каталогах по умолчанию:

```
/var/lib/docker/volumes/<volume_name>
```

Где `<volume_name>` – том (каталог Docker), привязанный к контейнеру устанавливаемой роли.

Допускается использование для некоторых ролей режима `volume_device_<role>: "True"`, а для других `volume_device_<role>: "False"`.

Режим `volume_device_<role>: "True"` рекомендуется использовать только если выделенное устройство более производительное, например, `ssd`.

В режиме **кластерной инсталляции** на всех нодах соответствующей роли используется путь до устройства, указанный для первой ноды роли (см. пункт 1).

В режиме **кластерной инсталляции** в инвентарном файле указывается несколько хостов (адресов серверов) в соответствующей группе. На данный момент поддерживается кластеризация для всех перечисленных в шаблоне инвентарного файла сервисов кроме `docker_registry`, `syslog` и `monitoring`.

Пример конфигурации (фрагмент инвентарного файла `hosts.yml`):

```
db:
  children:
    etcd:
      hosts:
        host.example.com:
          volume_device_etcd: "False"
          volume_device_etcd_path: "/dev/disk/by-uuid/<UUID>"
        host-2.example.com:
```

```
            volume_device_etcd: "False"
            volume_device_etcd_path: "/dev/disk/by-uuid/<UUID>"
      redis:
        hosts:
          host.example.com:
          host-2.example.com:
```

Хосты в группах `ldap`, `etcd` и `redis` должны быть сконфигурированы с разными именами (hostname), менять которые в процессе эксплуатации не следует во избежание некорректной работы системы. В случае, если на уже установленном PSN требуется изменить hostname на хостах группы `ldap`, обратитесь к разделу Изменение hostname на хостах группы ldap данного руководства.

Для изменения hostname на хостах группы etcd обратитесь к разделу Изменение hostname на хостах группы etcd.

Для изменения hostname на хостах группы redis обратитесь к разделу Изменение hostname на хостах группы redis.

4.2.3.2 Конфигурирование инвентарного файла: переменные

Дальнейший процесс настройки будет состоять из заполнения секции `vars` – переменных инвентарного файла.

В инвентарном файле структура данной секции выглядит следующим образом:

```
vars:
  setup:
  .....
     passwords:
     .....
     secure:
     .....
     notifications:
        mobile:
        .....
        ios:
        .....
        android:
```

```
            .....
           web:
            .....
      integrations:
           pgs:
           .....
           klms:
           .....
           siem:
           .....
              collector:
              .....
           catalog:
              .....
              mail:
              .....
              cab:
              .....
      conference:
           squadus:
           .....
           trueconf:
           .....
           videomost:
           .....
           webinar:
           .....
```

Доступные значения и способы заполнения данной секции указаны в таблице 6 данного руководства.

Все параметры переменных необходимо указывать в двойных кавычках за исключением `True/False`.

Таблица 6. Значения и способы заполнения переменных инвентарного файла

Переменная	Значение и способ заполнения
Блок **setup**	Общие настройки стенда и настройки формирования доменных имен внутри среды инсталляции
auth_proxy	Для внутреннего использования, значение `False`

Переменная	Значение и способ заполнения
dev_mode	*Developer mode*, режим разработчика. Принимает значения `True` и `False`, в случае значения `True` добавляет журнал `access_log` для сервисов `triton`, `pbm`, `autoconfig`
swarm_network_encryption	Включает шифрование внутренней оверлейной сети `Docker swarm`, значение по умолчанию `False`. Влияет на производительность системы, подробнее о данном виде шифрования
default_instance_language	Задаёт язык интерфейса по умолчанию для пользователей в тенантах. Возможные значения: `Russian`, `English`, `Bashkir`, `French`, `Spanish`, `Italian`, `Portuguese`
autoconfig_auth_salt	Соль для подключения к глобальной адресной книге. Рекомендуемые значения: большие и маленькие латинские буквы, цифры
external_domain	Зарегистрированный домен инсталляции. Для корректной работы необходим установленный актуальный SSL-сертификат

domain_module	Шаблон формирования внешних доменных имён инсталляции, позволяет гибко настроить принцип их генерации. Примеры работы шаблона при использовании префикса `mail` и домена `test.example.com`:
	`{service}-{domain} | mail-test.example.com`
	`{service}.{domain} | mail.test.example.com`
	Таким образом можно гибко настраивать принцип формирования доменных имен инсталляции. Это может пригодиться, например, если у вас есть Wildcard SSL-сертификат на доменное имя *example.com* и *.example.com*, но нет на *.test.example.com*. Вы можете установить `DOMAIN_MODULE:` в значение `{service}-{domain}` и получить домены третьего уровня, которые подходят под текущий Wildcard SSL-сертификат

Переменная	Значение и способ заполнения
gost	Используется для установки версии GOST из специального дистрибутива, в обычном дистрибутиве значение поля должно быть `False`
cryptopro_license	Используется для установки версии GOST из специального дистрибутива, в обычном дистрибутиве игнорируется
dynamic_webdomains	Возможность динамического добавления WEB-доменов. Принимает значения `False` и `True`. В случае `False` нет возможности динамического добавления нового WEB-домена. Переменная используется только для WEB-доменов
ldap_debug	Принимает значения `True` и `False` , в случае значения `True` пароли, заданные для новых локальных пользователей будут храниться в base64 без шифрования
custom_ca	Принимает значения `True` и `False` , включает поддержку сертификатов, выпущенных непубличными центрами сертификации. Подробности см. в разделе Настройка сертификатов
utf8_support	Принимает значения `True` и `False`. В случае `True` добавляется поддержка многобайтовых кодировок в адресе электронной почты
log_socket	Принимает значения `True` и `False`. В случае `True` журнальные файлы сервисов перенаправляются в коллектор логов на выделенную ноду, указаную в группе `syslog`
cert_path	Путь относительно директории с дистрибутивом, по которому будут размещены ssl-сертификаты, используемые при установке Продукта (см. разделы Настройка SSL-сертификатов, Настройка подписи DKIM)
balancing	Принимает значения `True` и `False`, включает режим установки с балансировкой входящего трафика
virtual_ipaddress	В случае, если указано 2 хоста в группе loadb, то значение переменной используется для создания виртуального IP адреса сервиса keepalived на хостах группы loadb

Переменная	Значение и способ заполнения
mdbox_format	Принимает значения `True` и `False`. В случае `True` dovecot будет хранить письма в формате mdbox, иначе - в maildir. Для новых установок рекомендуется использовать формат mdbox. Для перевода стендов на формат mdbox требуется миграция (см. раздел Миграция на формат хранения писем mdbox)
mdbox_altstorage	Принимает значения `True` и `False`. В случае `True` включается функционал дополнительного хранилища писем dovecot. Используется для хранения писем, полученных позже определенной даты на дополнительно выделенном объемном, но менее проиводительном хранилище
skip_mail_glusterfs_tasks	Принимает значение `True` и `False`. В случае `True` во время установки пропускаются задачи по настройке и подключению томов glusterfs для роли mail. Может использоваться при ручной настройке glusterfs или при использовании другой распределенной файловой системы. Актуально только для кластерной установки
skip_backend_glusterfs_tasks	Принимает значение `True` и `False`. В случае `True` во время установки пропускаются задачи по настройке и подключению томов glusterfs для роли backend. Может использоваться при ручной настройке glusterfs или при использовании другой распределенной файловой системы. Актуальна только для кластерной установки
cluster_drbd	Принимает значение `True` и `False`. В случае `True` IMAP-сервис dovecot запускается только на ноде, указанной в `cluster_drbd_mail_node`, а не на всех нодах группы mail. Необходима для работы продукта при хранении писем на томе drbd либо в режиме синхронизации при помощи rsync. Подробности см. в разделе Установка для большого количества пользователей
cluster_drbd_mail_node	Метка ноды, где будут храниться актуальные письма в случае `cluster_drbd = true`. Принимает значение вида dovecot, если используется drbd или mailN, где N порядковый номер ноды если используется rsync

Переменная	Значение и способ заполнения
cluster_drbd_mail_path	Задает путь до каталога с письмами в режиме cluster_drbd_mail_node
policy_server	Принимает значение `True` и `False`. В случае `True` добавляется сервис фильтрации почты, позволяющий настраивать ограничения на доставку сообщений для почтового ящика. Более подробную информацию см. в документе «МойОфис Почта 3. Руководство по администрированию»
dynamic_maillists	Принимает значение `True` и `False`. В случае `True` добавляется сервис, позволяющий создавать динамические группы рассылки. Более подробную информацию в документе «МойОфис Почта 3. Руководство по администрированию»
Блок **passwords**	Для основных сервисов инсталляции рекомендуется использовать надёжные пароли, в этом может помочь утилита `pwgen 10 1`. Рекомендуемые значения: большие и маленькие латинские буквы, цифры, специальные символы: &!% (символ $ использовать нельзя)
postgres_superuser	Пароль суперпользователя PostgreSQL
postgres_replica_user	Пароль пользователя для репликации PostgreSQL в случае кластерной установки
postgres_db_user	Пароль пользователя баз данных PSN
redis_user	Пароль доступа к БД Redis
ds389_manager_user	Пароль доступа к службе каталогов 389 Directory Server
ds389_replicator_user	Пароль пользователя для репликации 389 Directory Server в случае кластерной установки
dovecot_adm_user	Пароль доступа к сервису хранения писем
psnapi_adm_user	Пароль доступа к API компонента PSN

Переменная	Значение и способ заполнения
etcd_browser_user	Пароль для веб-интерфейса сервиса etcd
default_tenant_admin_user	Пароль тенанта по умолчанию (`default`) при установке без интеграции с PGS
master_user	Пароль для сервисной учётной записи (мастер-пользователя). Данная запись предоставляет административный доступ к письмам и почтовым ящикам пользователей приусловии обращения через веб-клиент. Авторизация при помощи данной записинедоступна извне
rabbitmq_user	Пароль доступа к сервису RabbitMQ
Блок **secure**	Ключи для внутреннего шифрования. Блок заполняется перед установкой, изменять его вдальнейшем **не следует** во избежание потери доступа к системе
db_secret_key	
internal_secret_key	Ограничения: # A-Za-z, num 0-9, spec char &!$&%
auth_jwt_key	Должен состоять из минимум 16 символов
Блок **notifications**	Бóльшая часть значений переменных данного блока находится в аккаунте консоли Firebase (или консоли Huawei для устройств Huawei)
Блок **mobile**	Данный блок переменных отвечает за настройку мобильных уведомлений
enabled	Включает и выключает мобильные уведомления, доступные значения `True` и `False`, по умолчанию `False`
ios_bundle_name	Значение по умолчанию `iosmailemb`. Изменять не требуется
android_bundle_name	Значение по умолчанию `amail`. Изменять не требуется
google_conf_file_name	Имя файла конфигурации json. Значение поумолчанию - `google_push.json`. Пример заполнения указан ниже

<table>
<tr><th>Переменная</th><th>Значение и способ заполнения</th></tr>
<tr><td colspan="2">

```
{
    "type": "service_account", // Значение по умолчанию. Изменять не требуется.
    "project_id": "<PROJECT_ID>", // Соответствует значению из графы Project ID вкладки General раздела Your project.
    "private_key_id": "<PRIVATE_KEY_ID>", // Генерируется кнопкой Generate new private key на вкладке Service accounts раздела Your project.
    "private_key": "<PRIVATE_KEY>", // Генерируется кнопкой Generate new private key на вкладке Service accounts раздела Your project.
    "client_email": "<CLIENT_EMAIL>", // Соответствует значению из графы Firebase service account вкладки Service accounts раздела Your project.
    "client_id": "100609742970758476105", // Значение по умолчанию. Изменять не требуется.
    "auth_uri": "https://accounts.google.com/o/oauth2/auth", // Значение по умолчанию. Изменять не требуется.
    "token_uri": "https://oauth2.googleapis.com/token", // Значение по умолчанию. Изменять не требуется.
    "auth_provider_x509_cert_url": "https://www.googleapis.com/oauth2/v1/certs", // Значение по умолчанию. Изменять не требуется.
    "client_x509_cert_url": "https://www.googleapis.com/robot/v1/metadata/x509/firebaseadminsdk-wrdsa%40amail-push.iam.gserviceaccount.com" // Значение по умолчанию. Изменять не требуется.
}
```

Готовый файл необходимо разместить в директории установки по следующему пути:

```
~/MyOffice_PSN_SRV-XXX/certificates
```

</td></tr>
<tr><td>Блок ios</td><td>Данный блок отвечает за мобильные уведомления в устройствах на операционной системе iOS. Для настройки уведомлений iOS необходимо получить доступ и авторизоваться в консоли Firebase, зайти на вкладку General в раздел Your Apps и выбрать там нужный проект (iOS).</td></tr>
<tr><td>api_key</td><td>Соответствует значению из графы Web API Key вкладки General раздела Your Apps.</td></tr>
<tr><td>app_id</td><td>Соответствует значению из графы App ID вкладки General раздела Your Apps.</td></tr>
</table>

Переменная	Значение и способ заполнения
messaging_sender_id	Соответствует значению из графы **Sender ID** вкладки **Cloud Messaging**.
project_id	Соответствует значению из графы **Project ID** вкладки **General** раздела **Your project**.
Блок **android**	Данный блок отвечает за мобильные уведомленияв устройствах на операционной системе Android. Для настройки уведомлений Android необходимополучить доступ и авторизоваться в консоли Firebase, зайти на вкладку **General** в раздел **Your Apps** и выбрать там нужный проект (Android).
api_key	Соответствует значению из графы **Web API Key** вкладки **General** раздела **Your Apps**.
app_id	Соответствует значению из графы **App ID** вкладки **General** раздела **Your Apps**.
messaging_sender_id	Соответствует значению из графы **Sender ID** вкладки **Cloud Messaging**.
project_id	Соответствует значению из графы **Project ID** вкладки **General** раздела **Your project**.
Блок **huawei**	Данный блок отвечает за мобильные уведомленияв устройствах на операционной системе Huawei. Для настройки уведомлений Huawei необходимо получить доступ и авторизоваться в консоли Huawei, зайти в настройки проекта в раздел **Основная информация** и найти там необходимые значения.
enabled	Включает и выключает мобильные уведомления для Huawei, доступные значения `True` и `False`, по умолчанию `False`.
client_id	Соответствует значению из графы **ID** приложения.
client_secret	Соответствует значению из графы секрет клиента.
huawei_bundle_name	Значение по умолчанию `huawei`. Изменять не требуется.

Переменная	Значение и способ заполнения
Блок **web**	Данный блок переменных отвечает за настройкуweb-пушей. Для настройки web-пушей необходимо получить доступ и авторизоваться в консоли Firebase, зайти на вкладку **General** в раздел **Your Apps** и выбрать там нужный проект (Web App).
app_id	Соответствует значению из графы **App Id** вкладки **General** раздела **Your Apps**.
enabled	Включает и выключает web-пуши, доступныезначения `True` и `False` , по умолчанию `False` .
webpush_bundle_name	Значение по умолчанию `webpush`. Изменять не требуется.
messaging_sender_id	Соответствует значению из графы **Project number** вкладки **General** раздела **Your Apps**.
api_key	Соответствует значению из графы **Web API Key** вкладки **General** раздела **Your Apps**.
vapid_key	Соответствует значению из графы **Key pair** вкладки **Cloud messaging** раздела **Web configuration**.
auth_domain	Домен авторизации Firebase. Значение представляет собой адрес вида <PROJECT_ID>.firebaseapp.com, где <PROJECT_ID> соответствует значению из графы **Project ID** вкладки **General** раздела **Your project**.
database_url	Путь к базе данных Firebase. Значение представляет собой адрес вида <PROJECT_ID>.firebaseio.com, где <PROJECT_ID> соответствует значению из графы
project_id	Соответствует значению из графы **Project ID** вкладки **General** раздела **Your project**.
storage_bucket	Путь к хранилищу объектов. Значениепредставляет собой адрес вида <PROJECT_ID>.appspot.com, где <PROJECT_ID> соответствует значению из графы **Project ID** вкладки **General** раздела **Your project**.
Блок **integrations**	В данном блоке указываются параметры для интеграции с внешними сервисами.

Переменная	Значение и способ заполнения
Блок **pgs**	В данном блоке указываются параметры дляинтеграции с PGS.
enabled	Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
appapi_user_password	Значение переменной KEYCLOAK_PASSWORD из инвентарного файла PGS.
co_oauth2_client_secret	Переменная ключа, должна совпадать с MAIL_OAUTH2_CLIENT_SECRET в конфигурации CO.
Блок **klms**	Kaspersky Security for Linux Mail Server. Более подробная информация указана в разделе **Настройка интеграции с Kaspersky Security for Linux Mail Server** в документе «МойОфис Почта 3. Руководство по администрированию».
enabled	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
host	Способ заполнения данной настройки см. в разделе **Настройка интеграции с Kaspersky Security for Linux Mail Server** в документе «МойОфис Почта 3. Руководство по администрированию».
Блок **siem**	Блок настройки SIEM-системы.
enabled	Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
Блок **collector**	Блок для настройки отправки событий в подсистему событийной аналитики. Настраивается на этапе деплоя. Для изменения настроек в работающей системе, изменить значения в инвентарном файле и запустить деплой спараметром `-t syslog`.
host	IP-адрес или имя хоста.

Переменная	Значение и способ заполнения
protocol	Протокол TCP/UDP.
port	Порт.
Блок **catalog**	В данном блоке указываются параметры для интеграции со службой каталогов.
enabled	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
host	Адрес контроллера домена.
port	Порт для подключения к службе каталогов по протоколу LDAP. Обычно принимает значения 389 (для подключения без шифрования) или 636 (с шифрованием).
ssl	Использование протокола с шифрованием. Переменная принимает значения True (шифрование включено) и False (шифрование отключено)
login_dn	Логин учетной записи, от имени которой будет осуществляться вход и поиск по БД службы каталогов.
password	Пароль учетной записи, от имени которой будет осуществляться вход и поиск по БД службы каталогов.
Блок **mail**	Используется для настройки подключения к базе пользователей почтового ядра (учетные записи и группы рассылки).
mail_base_dn	Путь до контейнера с учетными записями пользователей, используется почтовым ядром.
groups_base_dn	Путь до контейнера с группами рассылок, используется почтовым ядром. Оставить пустым,если группы рассылок не используются.
sync_attr	Атрибут синхронизации. Рекомендованное значение для AD: mail или sAMAccountName. Рекомендованное значение для FreeIPA/ALDPro/OpenLDAP/389ds: `mail` или `uid`.

Переменная	Значение и способ заполнения
groups_filter	Фильтр групп. Значение по умолчанию `(&(objectClass=group)(mail=%s))`. Стоит обратить внимание на то, что в фильтре необходимо использовать переменные `%s, %u (%s – email-адрес), %u` - часть до @, таким образом формируется конечный фильтр для поиска конкретной группы.
domain	Переменная используется только при значении `sync_attr` равным `sAMAccountName` или `uid`. Принимает значение домена, который могут использовать пользователи в логине для входа на стенд. Можно указать только один домен. В случае, если переменная не заполнена и `sync_attr` указан как `sAMAccountName` или `uid`, используется домен инсталляции. Если на стенде, интегрированным со сторонним каталогом, будет использоваться несколько доменов, необходимо настроить синхронизацию по атрибуту, который содержит адрес электронной почты - mail.
Блок **cab**	Используется для настройки подключения к базе адресной книги (пользователи и группы рассылки).
enabled	Синхронизация адресной книги со сторонней службой каталогов. Принимает значения True (синхронизация включена) и False (синхронизация отключена)
host	Адрес сторонней службы каталогов
port	Порт для подключения к службе каталогов по протоколу LDAP. Обычно принимает значения 389 (для подключения без шифрования) или 636 (с шифрованием)
login_dn	Логин учетной записи, от имени которой будет осуществляться вход и поиск по БД службы каталогов
password	Пароль учетной записи, от имени которой будет осуществляться вход и поиск по БД службы каталогов
ssl	Использование протокола с шифрованием. Переменная принимает значения True (шифрование включено) и False

Переменная	Значение и способ заполнения
	(шифрование отключено)
users_base_dn	Путь до контейнера с учетными записями пользователей для формирования адресной книги.
users_filter	Фильтр пользователей. Значение по умолчанию `(&(objectClass=person)(mail=*))`. Изменять не требуется.
groups_base_dn	Путь до контейнера с группами рассылок, используется для синхронизации адресной книги. Оставить пустым, если группы рассылок не используются.
groups_filter	Фильтр групп рассылок. Рекомендованноезначение для AD: `(&(objectClass=group)(mail=*))`.Рекомендованное значение для FreeIPA/ALDPro/OpenLDAP/389ds: `(&(objectClass=groupOfNames)(mail=*))`.
Блок **conference**	Параметры для интеграции с ВКС системами. Основной блок настроек для данной интеграции выполняется после инсталляции «МойОфис Почта». Более подробная информация по настройке работы ВКС и PSN находится в документе «МойОфис Почта. Руководство по администрированию».
enabled	Принимает значение `True` (когда интеграция с одинм из сервисов ВКС включена) и `False` (интеграция отключена).
Блок **squadus**	Параметры для интеграции с мессенджером Squadus. Основной блок настроек для данной интеграции выполняется *после* инсталляции «МойОфис Почта». Более подробная информацияпо настройке работы Squadus и PSN находится в документе «МойОфис Почта. Руководство по администрированию»
enabled	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.

Переменная	Значение и способ заполнения
url	Ссылка на веб интерфейс Squadus для быстрого перехода из меню выбора приложений в PSN.
Блок **trueconf**	В данном блоке указываются параметры для интеграции с TrueConf.
enabled	Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
url	Соответствует ссылке на API TrueConf.
delete_after	Время в секундах по прошествии которого завершенная конференция будет удалена.
client_id	`client_id` для oauth2 токена. Информация о `client_id` доступна в административной панели сервиса `trueconf`.
client_secret	`client_secret` для oauth2 токена. Информация о `client_secret` доступна в административной панели сервиса `trueconf`.
Блок **videomost**	В данном блоке указываются параметры для интеграции с videomost.
enabled	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Основной блок настроек для данной интеграции выполняется после инсталляции «МойОфис Почта». Более подробная информация по настройке работы ВКС и PSN находится в документе «МойОфис Почта. Руководство по администрированию».
Блок **webinar**	В данном блоке указываются параметры для интеграции с webinar.
enabled	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Основной блок настроек для данной интеграции выполняется после инсталляции «МойОфис Почта». Более

Переменная	Значение и способ заполнения
	подробная информация по настройке работы ВКС и PSN находится в документе «МойОфис Почта. Руководство по администрированию».

4.2.3.3 Настройка дополнительных параметров установки

Дополнительные параметры установки находятся в файле `~/group_vars/all/main.yml` (см. таблицу 7).

Таблица 7. Дополнительные параметры установки

Параметр	Комментарий
`allow_mail_force_revoke`	Разрешить отзыв отправленных писем даже если они уже прочитаны получателем. Принимает значения `True / False`.
`allow_mail_revoke`	Разрешить отзыв отправленных писем. Принимает значения `True / False`.
`attachment_max_size`	Задает максимальный размер письма и вложений, которые можно прикрепить в веб интерфейсе (в Мб): – `mail`: 15 - максимальный размер письма, который может быть отправлен или получен системой; – `web_mail`: 10 - максимальный размер вложения, который можно прикрепить к письму в веб интерфейсе почты; – `web_calendar`: 10 - максимальный размер вложения, который можно прикрепить к событию в веб интерфейсе календаря.
`nginx_monitoring`	Принимает значения `True/False`. `True` включает возможность мониторинга сервиса nginx на порту 8081. URL для обращения - IP-адрес или доменное имя fe-ноды вида http://pfe1:8081/ В случае кластерной инсталляции необходимо мониторить все fe-ноды отдельно.
`nginx_monitoring_allowed_host`	Подсеть, с которой разрешено обращаться для мониторинга сервиса. В случае `nginx_monitoring = false` данный параметр игнорируется.
`ntp_servers`	Список ntp-серверов, с которых будет синхронизироваться время на нодах системы (см. раздел Подготовка инфраструктуры установки).

Параметр	Комментарий
triton.monitoring	Принимает значения True/False. True включает возможность мониторинга сервиса triton (nginx-unit) на порту 8081. URL для обращения - IP-адрес или доменное имя любой fe-ноды вида http://pfe1:8081/triton-N/status/applications/triton, где в triton-N вместо N подставялется порядковый номер реплики службы. В случае кластерной инсталляции необходимо мониторить все реплики сервиса triton отдельно. Например, если развернуто три реплики triton, необходимо мониторить triton-1, triton-2 и triton-3.
triton.monitoring_allowed_host	Подсеть, с которой разрешено обращаться для мониторинга сервиса.
web_mail_allow_short_login	Принимает значения True/False. True разрешает вводить логин в форме авторизации в web-интерфейсе НЕ в формате электронной почты.
web_mail_disableChangeAvatar	Управляет возможностью изменять аватар пользователям. True - запрещено, False - разрешено.
web_mail_max_count_for_sharing_folders	Целое число. Максимальное допустимое количество папок, доступных для одновременного выбора при шаринге почтовых папок.

4.2.3.4 Рекомендации по разбиению дисков для ролей

– для серверов с ролью mail рекомендуется выделить независимые диски или блочные устройства соответствующих размеров, которые будут использоваться для хранения почты;
– точка монтирования для ролей backend и mail в режиме с отказоустойчивостью:

```
/data
```

– точка монтирования для роли mail в standalone режиме:

```
/var/dovecot
```

4.2.3.5 Рекомендации по количеству хостов для ролей

Рекомендуемое количество хостов для ролей указано в таблице 8.

Таблица 8 - Рекомендуемое количество хостов для ролей

Роль	Количество хостов в случае кластеризации ролей
etcd, redis	три, либо пять
postgres, ldap	два (ограничение текущего релиза: более двух недопустимо)
haproxy(load balancer)	не более двух

4.2.4 Настройка сертификатов

4.2.4.1 Настройка SSL-сертификатов

Для корректной работы веб-интерфейса «МойОфис Почта» необходимы соответствующие SSL-сертификаты. Они должны быть размещены в директории, которая указана в переменной `setup.cert_path` в разделе Конфигурирование инвентарного файла: переменные.

Список необходимых для работы сертификатов:

- `server.crt` – содержит SSL-сертификат для `*.<DEFAULT_DOMAIN>` и все промежуточные сертификаты, кроме корневого доверенного. Расположение промежуточных сертификатов соответствует описанию в документации nginx;
- `server.nopass.key` – приватный ключ сертификата, не требующий кодовой фразы;
- `ca.crt` – доверенный SSL-сертификат (собственного непубличнного УЦ). Используется только при значении переменной setup.custom_ca = True (см. раздел Конфигурирование инвентарного файла: переменные). В файле может быть размещен только один сертификат. При необходимости добавления дополнительных сертификатов необходимо разместить их в отдельных файлах, имена файлов должны соответствовать шаблону `ca_*.crt`, например: `ca_ad.crt`, `ca_web.crt`. Каждый дополнительный сертификат должен располагаться в отдельном файле.

4.2.4.2 Настройка подписи DKIM

Для работы механизма подписи сообщений DKIM необходим приватный ключ `dkim.key`, который следует поместить в директорию, которая указана в переменной `setup.cert_path` в разделе Конфигурирование инвентарного файла: переменные.

Инсталляция PSN без SSL-сертификатов и ключа подписи DKIM невозможна

4.2.4.3 Сертификаты для ГОСТ

Для установки «МойОфис Почта» с поддержкой ГОСТ шифрования из вышеупомянутых сертификатов необходимо сформировать pfx-контейнер, который должен быть доступен по пути:

```
~/MyOffice_PSN_SRV-XXX/certificates/gost/<DEFAULT_DOMAIN>/certkey-rsa.pfx
```

Пример создания pfx-контейнера через команду openssl:

```
openssl pkcs12 -export -out gost/<DEFAULT_DOMAIN>/certkey-rsa.pfx -inkey
<KEY> -in <CERTIFICATE>
```

При наличии рутового сертификата или цепочки в формате *.pem, необходимо создать pfx-контейнер, который должен быть доступен по пути:

```
~/MyOffice_PSN_SRV-XXX/certificates/gost/<DEFAULT_DOMAIN>/roots-rsa.pfx
```

Пример команды для создания подобного контейнера:

```
openssl pkcs12 -export -out gost/<DEFAULT_DOMAIN>/roots-rsa.pfx -in
<CERTIFICATE> -nokeys
```

Дополнительно к созданным контейнерам, необходимо иметь предоставленный провайдером готовый контейнер с ГОСТ сертификатом и ключом сервера certkey-gost.pfx (опционально - с корневым сертификатом roots-gost.pfx). К ним необходимо организовать доступ по следующим путям:

```
~/MyOffice_PSN_SRV-XXX/certificates/gost/<DEFAULT_DOMAIN>/certkey-gost.pfx
~/MyOffice_PSN_SRV-XXX/certificates/gost/<DEFAULT_DOMAIN>/roots-gost.pfx
```

4.2.4.4 Создание самоподписанного SSL-сертификата

Для создания самоподписанного сертификата в среде установки «МойОфис Почта» необходимо использовать исполняемый файл `gen_self_signed_cert.sh` из директории установки, запустив его в консоли и указав привязанный к создаваемому сертификату домен.

Пример:

```
gen_self_signed_cert.sh <DOMAIN>
```

Сгенерированные сертификаты будут помещены в директорию `certificates/`

4.2.4.5 Генерация DKIM ключей

Для генерации новой пары DKIM ключей на работающем стенде на любом сервере группы mail необходимо выполнить команду

```
docker exec $(docker ps -qf name=rspamd) rspamadm dkim_keygen
-s mail -b 2048
```

При выполнении команды будет выведен приватный ключ, который необходимо сохранить в файле с именем `dkim.key` и значение TXT - записи `mail._domainkey`, которую необходимо прописать в соответствующую зону DNS-сервера.

Для генерации ключа в случае первоначального деплоя или на любом другом сервере выполнить команду

```
openssl genrsa -out dkim.key 2048
```

При выполении команды будет создан приватный ключ и сохранен в файл `dkim.key`.

Сгенерированный ключ `dkim.key` необходимо разместить в каталоге `certificates/<DOMAIN>/dkim.key`.

Для получения публичного ключа из закрытого необходимо выполнить команду:

```
openssl rsa -in dkim.key -pubout -outform der 2>/dev/null | openssl
base64 -A
```

При выполении команды будет создан публичный ключ, который необходимо прописать в TXT - запись `mail._domainkey` соответствующей зоны DNS-сервера со значением `v=DKIM1;k=rsa;p=<публичная часть ключа>`.

4.2.4.6 Результат настройки сертификатов

Пример структуры папок для домена `myoffice.ru` с двумя CA сертификатами:

```
install-psn/certificates/
├─ default
|   ├─ dkim
|   |   └─ dkim.key
|   ├─ server.crt
|   └─ server.nopass.key
└─ myoffice.ru
   ├─ ca_ad.crt
   ├─ ca.crt
   ├─ dkim.key
   ├─ server.crt
   └─ server.nopass.key
```

Значения переменных

```
setup.cert_path: "myoffice.ru";
setup.custom_ca: true
```

4.2.5 Настройка DNS

Перед началом установки необходимо настроить DNS для разрешений некоторых доменных имен в следующий адрес:

– адрес, куда будет установлен сервер `nginx` (раздел proxy инвентарного файла);
– адрес, указывающий на адрес внешнего балансировщика, в случае кластерной инсталляции.

Список необходимых имен указан в таблице 9. Поскольку внешнее доменное имя в PSN формируется посредством шаблона (переменная `domain_module`, см. раздел Конфигурирование инвентарного файла: переменные), в таблице указан только требуемый префикс.

Пример:
В случае с доменом `test.example.com`, при значении переменной `domain_module`: `"{service}-{domain}"`, и хосте `1.1.1.1`, присвоенном роли `proxy`, домен `admin-test.example.com` будет разрешаться в `1.1.1.1`

Таблица 9. Имена для настройки DNS

Префикс	Комментарий
mailadmin	Адрес веб-панели администрирования PSN
autoconfig	Адрес сервиса автоконфигурирования для подключения клиентов MyOffice (мобильный или десктопный клиент)
mail	Адрес главной страницы веб-интерфейса почты
cab	Адрес для подключения к глобальной адресной книги
imap	Адрес для подключения с сервису imap
smtp	Адрес для подключения с сервису smtp
pbm	Адрес для подключения с API сервису PBM (см. Руководство по Администрированию)

Для внешних систем доменные имена должны корректно разрешаться в соответствующий публичный IP-адрес. Информация, необходимая для настройки внешних записей типа SRV, приведена в таблице 10. Настройка записей SRV необязательна.

Таблица 10. Настройка внешних DNS-записей

Имя записи	Тип	Порт	Адрес
_caldavs._tcp	SRV	443	mail.<setup.**external_domain**>
_caldavs._tcp	SRV	443	<setup.**external_domain**>
_imap._tcp	SRV	143	imap.<setup.**external_domain**>
_imaps._tcp	SRV	993	imap.<setup.**external_domain**>
_smtps._tcp	SRV	465	smtp.<setup.**external_domain**>
_submission._tcp	SRV	587	smtp.<setup.**external_domain**>
_submissions._tcp	SRV	465	smtp.<setup.**external_domain**>

4.2.6 Настройка межсетевого экранирования

Для корректной работы «МойОфис Почта» рекомендуется не использовать сетевое экранирование между серверами. Необходимые для работы ПО сетевые порты приведены ниже в таблице 11.

Таблица 11. Сетевые порты, доступ к которым необходим с внешних IP-адресов

Номер порта	Назначение (протокол)
80	Используется для незашифрованного HTTP-траффика.
143	Используется протоколом IMAP для получения почты клиентом с использованием шифрования (STARTTLS).
443	Используется для HTTP-траффика с поддержкой шифрования (HTTPS).
636	Используется службой каталогов (LDAP) для передачи данных по LDAPS.
25	Используется для передачи почты между серверами по SMTP.
587	Используется для передачи почты по SMTP от почтового клиента на сервер.
465	Используется для передачи почты по SMTP от почтового клиента на сервер с использованием шифрования (SSL).
993	Используется протоколом IMAP для получения почты клиентом с использованием шифрования (SSL).

4.2.7 Подготовка к установке на ОС РОСА

Для подготовки к установке «МойОфис Почта» на ОС РОСА «ХРОМ» необходимо:

1. Установить пакеты (приведенные ниже команды необходимо выполнить на каждом сервере системы):

```
dnf install cronie python3-pip docker -y
dnf remove sendmail -y
systemctl enable --now docker
```

Все последующие команды необходимо выполнять на инфраструктурной машине, из директории, выбранной при распаковке дистрибутива продукта, см. раздел Проверка и подготовка инсталляционного архива.

2. Исключить из файла `CentOS.yml` пакет `epel-release` с помощью команды:

```
sed -i '/epel-release/s/^/#/' roles/common/vars/CentOS.yml
```

3. Исключить из файла `main.yml` блок «Put SELinux in permissive mode» с помощью команды:

```
sed -i '39,45 s/^/#/' roles/common/tasks/main.yml
```

4. В файл `packages.yml`, расположенный в директории `collections/ansible_collections/nct/system/roles/package_tools/tasks` добавить следующий блок кода:

```
sed -i '39 i\
\
\   - name: "Install packages [urpmi]" \
\     community.general.urpmi: \
\       name: "{{ pkgs_local | default(pkgs, true) }}" \
\       state: "present" \
\     when: \
\       - ansible_pkg_mgr == "urpmi" \
\       - (not ansible_check_mode or (ansible_check_mode and not pkgs_local))' \
collections/ansible_collections/nct/
system/roles/package_tools/tasks/packages.yml
```

5. Добавить в коррекцию использование `urpmi` с помощью команды:

```
sed -i '/.*ansible_pkg_mgr not in*/c\
- ansible_pkg_mgr not in ["yum", "apt", "apt_rpm", "dnf", "urpmi"]' \
collections/ansible_collections/nct/system/roles/package_tools/tasks/packages.yml
```

6. Исключить из файла `main.yml` статус, так как в пункте 4 он указан явно:

```
sed -i 's/package_state/#package_state/'
collections/ansible_collections/nct/system/roles/package_tools/defaults/main.yml
```

Для установки «МойОфис Почта» на ОС РОСА «ХРОМ» следует использовать раздел Запуск установки на ОС РОСА.

4.3 Установка «МойОфис Почта»

4.3.1 Запуск установки

Для обновлении с предыдущей версии следует использовать раздел Обновление с предыдущих версий

Для запуска установки подсистемы PSN необходимо воспользоваться командой `deploy_psn.sh`.

Для установки необходимо перейти в папку установки и выполнить в терминале следующую команду:

```
./deploy_psn.sh hosts.yml <params>
```

Где:

- `hosts.yml` – инвентарный файл, сконфигурированный в соответствии с разделом Конфигурирование инвентарного файла: hosts данного руководства.

- `<params>` - параметры данной команды:

-b, --become - поднять привилегии без запроса пароля;

-u USERNAME, **--user**=USERNAME - учётная запись для логина;

-v, --verbose - включить более подробный режим. Чем больше **v** подряд, тем подробнее будут логи. Оптимальное значение **-vvv**. Данная опция может применяться для отладки сценариев.

Подробнее о дополнительных ключах в документации Ansible

Пользователь, от имени которого производится развертывание (параметр **-u** USERNAME), должен находиться в группе **docker** и иметь права на создание и запуск контейнеров.

Файл логов процесса развертывания будет сохранен под именем `deploy_psn.log`.

При успешном выполнении команды сервисы подсистемы будут запущены автоматически.

В процессе инсталляции не происходит обновление компонентов операционной системы.
Обновление компонентов операционной системы выполняет администратор установочного стенда

4.3.2 Запуск установки на ОС РОСА

Для подготовки установки следует использовать раздел Подготовка к установке на ОС РОСА.

Для запуска установки на ОС РОСА «ХРОМ» необходимо перейти в папку установки и выполнить команду `deploy_psn.sh` с тегами :

```
./deploy_psn.sh hosts.yml \
-e ansible_os_family="RedHat" \
-e ansible_distribution="CentOS" \
--skip-tags docker
```

4.3.3 Проверка корректности установки

Для проверки запуска сервисов «МойОфис Почта» в терминале на целевом сервере выполняется следующая команда:

```
     docker service ls --filter name=psn --format "table {{.Name}}
\t{{.Replicas}}"
```

Ожидаемый вывод:

```
     psn-backend_autoconfig 3/3 (max 1 per node)
     psn-backend_avatars 3/3 (max 1 per node)
     psn-backend_converter 3/3 (max 1 per node)
     psn-backend_events_backend 3/3 (max 1 per node)
     psn-backend_pbm 3/3 (max 1 per node)
     psn-backend_pps 3/3 (max 1 per node) (переменная setup.policy_server)
     psn-backend_pdm 3/3 (max 1 per node) (переменная setup.dynamic_maillists)
     psn-backend_rabbitmq 3/3 (max 1 per node)
     psn-backend_triton 3/3 (max 1 per node)
     psn-etcd_browser 1/1
     psn-etcd_etcd 3/3 (max 1 per node)
     psn-frontend_web_admin 3/3 (max 1 per node)
     psn-frontend_web_calendar 3/3 (max 1 per node)
     psn-frontend_web_contacts 3/3 (max 1 per node)
     psn-frontend_web_mail 3/3 (max 1 per node)
     psn-ldap_ldap 2/2 (max 1 per node)
     psn-mail_director 3/3 (max 1 per node) (в случае кластерной установки)
     psn-mail_dovecot 3/3 (max 1 per node)
     psn-mail_dovemon 1/1 (max 1 per node)
     psn-mail_postfix 3/3 (max 1 per node)
     psn-mail_rspamd 3/3 (max 1 per node)
     psn-nginx-proxy_nginx 3/3 (max 1 per node)
```



```
      psn-postgres_haproxy 2/2 (max 1 per node) (в случае кластерной установки)
      psn-postgres_pgbouncer 2/2 (max 1 per node)
      psn-postgres_postgres1 1/1
      psn-postgres_postgres2 1/1 (в случае кластерной установки)
      psn-redis_redis-master 1/1
      psn-redis_redis-sentinel 3/3 (max 1 per node) (в случае кластерной
установки)
      psn-redis_redis-slave 2/2 (max 1 per node) (в случае кластерной установки)
      psn-syslog_ng_syslog-collector 1/1 (max 1 per node) (в случае кластерной
установки)
      psn-syslog_ng_syslog-relay 3/3 (max 1 per node) (в случае кластерной
установки)
```

Количество реплик зависит от конкретной инсталляции. В `standalone` инсталляции количество реплик всегда равно одной.

В браузере открыть страницу `mail.<EXTERNAL_DOMAIN>` (по формированию доменных имен и среды инсталляции см. раздел Конфигурирование инвентарного файла: переменные данного руководства), далее выполнить следующие действия:

– убедиться, что загрузилась страница авторизации;
– при установке без интеграции с «МойОфис Хранилище» проверить авторизацию тенанта по умолчанию (`admin@<domain>` , где `<domain>` – основной домен контура установки).
– проверить, что при удачной авторизации происходит переход на страницу веб-интерфейса почты;
– отправить тестовое письмо и убедиться, что оно дошло;
– зайти в календарь, создать тестовое событие;
– зайти в настройки, изменить любые параметры и убедиться, что настройки сохранены.

4.3.4 Интеграция с PGS

Для полноценной интеграции «МойОфис Почта» с компонентом PGS необходимо:

1. Заполнить блок интеграции (`integrations: pgs:`) в инвентарном файле PSN (подробнее в разделе Конфигурирование инвентарного файла: переменные данного руководства).
2. Настроить DNS контура инсталляции в соответствии с рекомендациями из пункта Настройка DNS данного руководства и «Руководства по установке системы хранения данных МойОфис (PGS)».

Установка «МойОфис Почта» должна быть завершена до создания первого тенанта в PGS. В обратном случае тенант (и пользователи, входящие в него) не будут синхронизированы с почтой.

4.3.4.1 Подключение сервиса загрузки в облако

Начиная с версии 2.3, в PSN появляется возможность использовать виджет «Загрузить в облако» при прикреплении файла к письму и к событию в календаре. Виджет позволяет загружать прикрепленные к письму файлы пользователя в хранилище пользователя (PGS) автоматически. Для работы сервиса необходимо в настройках СО («МойОфис Частное облако») внести в список доверенных url-адрес, присвоенный роли `mail` при установке PSN.

Более подробно о формировании доменных имен для ролей можно прочитать в описании переменной `domain_module:` раздела Конфигурирование инвентарного файла: переменные данного руководства.

Настройку возможно выполнить в редакторе `etcd` компонента СО или внеся правки в конфигурационный файл по следующему адресу:

```
config/wfe/csp.allowed_frame_ancestors.json
```

Пример оформления записи:

```
["https://mail.myoffice.ru"]
```

4.3.5 Обновление с предыдущих версий

Процедура обновления описана в документе «Руководство по установке МойОфис Почта».

Обновление выполняется тем же способом, что и установка. Перед выполнением обновления необходимо сохранить резервные копии (см. раздел Создание резервных копий).

После обновления с некоторых версий необходимо выполнить миграцию данных. Миграция запускается вручную, после завершения работ по обновлению стенда. В зависимости от количества данных, миграция может занять продолжительное время.

Для обновления с версии PSN 1.0 (2021.04) следует обратиться к руководству версии 2.3.

Для обновления с версии 2.5 и ниже следует обратиться к руководству версии 2.6G.

Для 2.8G предыдущей версией с поддержкой ГОСТ является версия 2.6G. Тем не менее, для обновления с 2.6G на 2.8G будет необходима промежуточная версия 2.7. То есть при обновлении стенда с версией сервера 2.6G, пользователю предварительно нужен дистрибутив 2.7 для миграции данных. При этом полноценная установка версии 2.7 не нужна, можно выполнить установку только определенных компонентов, достаточных для миграции, а именно запустить деплой с параметрами `-t registry,etcd,backend`.

После чего запустить миграции 2.7:

```
docker exec $(docker ps -qf name=psn-backend_triton) \
php db/custom_migrations/2.7/start.php
```

После того, как миграции 2.7 выполнены, следует полноценная установка 2.8G, после чего необходимы миграции 2.8G:

```
docker exec $(docker ps -qf name=psn-backend_triton) \
php db/custom_migrations/2.8/start.php
```

Аналогичным образом, обновление с версии 2.8G на 3.1G следует выполнять через промежуточную версию 3.0. При обновлении с версии 2.8 до 3.0 необходимо выполнить миграцию данных. При обновления с версии 3.0 до 3.1 миграция данных не требуется.

5 СОЗДАНИЕ РЕЗЕРВНЫХ КОПИЙ

5.1 Резервная копия инвентарного файла

После окончательного заполнения инвентарного файла необходимо сделать его резервную копию, в дальнейшем она может понадобиться для последующих обновлений и некоторых операций по обслуживанию текущей установки.

5.2 Резервное копирование etcd

В `etcd` хранятся настройки компонентов стенда. Ценность представляют некоторые настройки компонентов, отличающиеся от стандартных, а также состояние кластера `postgresql` (в случае кластерной инсталляции). Для сохранения значений всех настроек `etcd` в текстовый файл необходимо на любой ноде группы `etcd` выполнить команду

```
docker exec $(docker ps -qf name=etcd_etcd[0-9]) etcdctl get --prefix '' > <path_to_backup>/etcd_keys.txt
```

Все стандартные настройки могут быть восстановлены в случае утери данных `etcd` путем запуска деплоя с параметром `-t etcd`, а остальные через `etcd browser`.

Дополнительно рекомендуется делать снимок данных etcd

```
docker exec $(docker ps -qf name=etcd_etcd[0-9]) etcdctl snapshot save /etcd-data/snapshot.db
```

После выполнения команды он будет доступен по следующему пути:

```
/var/lib/docker/volumes/psn_etcd_data/_data/snapshot.db
```

5.3 Создание резервных копий postgresql

В базе данных хранятся сведения о календарях и событиях пользователей. В текущем релизе можно восстановить состояние базы данных на момент создания резервной копии, которое затронет данные всех пользователей. Для восстановления из резервной копии календарей для конкретных пользователей следует обратиться к вендору ПО.

Процедура резервирования базы данных выполняется следующей командой:

в случае **standalone** инсталляции:

```
docker exec $(docker ps -qf name=postgres_postgre) pg_dump -Fc --clean --create  > <path_to_backup>/postgresql.dump
```

в случае **cluster** инсталляции (на любой из нод `postgres`):

```
docker exec $(docker ps -qf name=postgres_postgre) pg_dump postgresql://psn:<postgres_db_user>@haproxy:5000 -U psn -Fc --clean --create  > <path_to_backup>/postgresql.dump
```

где:

- `<postgres_db_user>` – значение переменной `postgres_db_user` из инвентарного файла инсталляции.

- `<path_to_backup>` – путь к создаваемой резервной копии

Процедура восстановления базы данных из резервной копии выполняется следующим образом:

в случае **standalone** инсталляции:

```
docker exec -i $(docker ps -qf name=postgres_postgre) pg_restore -U psn -Fc -d psn < <path_to_backup>/postgresql.dump
```

в случае **cluster** инсталляции (на любой из нод postgres):

```
docker exec -i $(docker ps -qf name=postgres_postgre) pg_restore -d 'postgresql://psn:<postgres_db_user>/psn' -Fc < <path_to_backup>/postgresql.dump
```

Вышеупомянутый способ не позволяют восстановить уже существующую базу данных. В случае, если это требуется, возможно полностью зачистить данные в `postgresql` перед восстановлением следующими командами:

Для **standalone** инсталляции:

```
docker exec $(docker ps -qf name=postgres_postgre) dropdb psn -U psn
```

```
docker exec $(docker ps -qf name=postgres_postgre) createdb psn -U psn
```

Для **cluster** инсталляции:

```
docker exec $(docker ps -qf name=postgres_postgre) psql postgresql://psn:<postgres_db_user>@haproxy:5000/template1 -c 'drop database psn'
```

```
docker exec $(docker ps -qf name=postgres_postgre) psql
postgresql://psn:<postgres_db_user>@haproxy:5000/template1 -c
'create database psn'
```

Для кластерной инсталляции процедура резервирования и восстановления выполняется **единожды** на любом из хостов группы `postgres` (см. инвентарный файл установки).

5.4 Создание резервных копий службы каталогов LDAP

Процедура **резервирования** службы каталогов выполняется следующей командой:

```
docker exec $(docker ps -qf 'name=ldap') ldapsearch -xD cn=Manager,
dc=<external_domain> -w <ds389_manager_user> '*' >
<path_to_backup>/ldap.ldif
```

Где:

- `<external_domain>` – зарегистрированный домен инсталляции.

Запись домена второго уровня в нотации LDAP выглядит следующим образом для `example.com`: `dc=example,dc=com`

- `<ds389_manager_user>` – значение переменной ds389_manager_user из инвентарного файла инсталляции.
- `<path_to_backup>` – путь к создаваемой резервной копии.

Процедура **восстановления** данных LDAP из резервной копии выполняется следующим образом:

```
cp <path_to_backup>/ldap.ldif
/var/lib/docker/volumes/psn-ldap_ldap_data/_data/ldap.ldif
```

```
docker exec $(docker ps -qf 'name=ldap') ldapadd -xD cn=Manager,
dc=<external_domain> -w <ds389_manager_user> -f /data/ldap.ldif -c
```

Первая команда скопирует файл резервной копии в примонтированную к Docker-контейнеру директорию, вторая – произведет восстановление данных.

Вышеупомянутые способы не позволяют изменить уже существующие записи LDAP. В случае, если это требуется, возможно полностью **зачистить** данные в LDAP перед восстановлением следующей командой:

```
docker exec $(docker ps -qf 'name=ldap') ldapdelete -xD cn=Manager,
dc=<external_domain> -w <ds389_manager_user> -r <external_domain>
```

Если данные перед восстановлением не будут зачищены, то при восстановлении добавятся только отсутствующие записи. Существующие записи не будут изменены даже если данные различаются.

Для кластерной инсталляции процедура резервирования и восстановления выполняется **единожды** на любом из хостов группы `ldap` (см. инвентарный файл установки).

5.5 Резервное копирование вложений к событиям в календаре

Резервное копирование вложений к календарным событиям в текущем релизе рекомендуется выполнять утилитой `rsync`. Для этого необходимо создать резервную копию данных из `/opt/poseidon/triton/eattach/` командой:

```
rsync -a /opt/poseidon/triton/eattach <path_to_backup>
```

5.6 Резервное копирование аватаров

Резервное копирование аватаров пользователей в текущем релизе рекомендуется выполнять утилитой `rsync`. Для этого необходимо создать резервную копию данных из `/opt/poseidon/triton/photos/` командой:

```
rsync -a /opt/poseidon/triton/photos <path_to_backup>
```

6 ИЗМЕНЕНИЕ HOSTNAME

6.1 Изменение hostname на хостах группы ldap

В случае, если на работающей системе потребовалось изменить `hostname` нод, на которых работают сервисы `ldap`, необходимо снять резервную копию данных службы каталогов LDAP и удалить соответствующие службе LDAP элементы `Docker -stack` и `volume` командами, описанными в данном разделе.

Изменение `hostname` на соответствующих нодах и в группе хостов `ldap` инвентарного файла установки производится следующим образом:

1. После проведения процедуры резервирования, описанной в разделе Создание резервных копий службы каталогов LDAP, необходимо удалить соответствующие службе `ldap` элементы `Docker - stack` и `volume` следующими командами:

```
docker stack rm psn-ldap
```

Следующую команду необходимо выполнить на всех хостах группы `ldap` :

```
docker volume rm psn-ldap_ldap_data
```

2. Изменить `hostname` на нодах.

3. Следующим шагом будет изменение `hostname` в группе хостов `ldap` инвентарного файла установки согласно разделу Конфигурирование инвентарного файла: hosts данного руководства и запуск установки с параметром `-t ldap` :

```
./deploy_psn.sh <hosts.yml> -t ldap
```

Команда переустановит только службу каталогов

4. После переустановки службы необходимо восстановить данные из резервной копии согласно инструкциям из раздела Создание резервных копий данного руководства.

6.2 Изменение hostname на хостах группы etcd

В случае, если на работающей системе требуется изменить `hostname` нод, на которых работают сервисы `etcd`, необходимо выполнить следующие действия:

1. Снять резервную копию службы `etcd` и `postgresql` (работа `postgresql` зависит от службы `etcd`). См. разделы Резервное копирование etcd, Создание резервных копий postgresql.

2. Изменить `hostname` на нодах.

3. Изменить `hostname` в группе хостов `etcd` инвентарного файла установки в соответствии с разделом Конфигурирование инвентарного файла: hosts.

4. Выполнить запуск установки с параметром `-t etcd`:

```
./deploy_psn.sh <hosts.yml> -t etcd
```

Либо в качестве альтернативного способа можно вручную внести изменения в параметры службы. Для этого следует на любой из нод группы `etcd` выполнить команду:

```
docker service inspect psn-etcd_etcd --format='{{json .Spec.Labels}}'
```

По выводу команды определить метку службы, связанной со старым значением hostname. Команда вернет записи вида:

```
<old-hostname>-etcd":"etcdN"
```

Далее выполнить команду по изменению метки для службы:

```
docker service update --label-rm <old_hostname>-etcd --label-add
<new_hostname>-etcd=etcdN --force psn-etcd_etcd
```

Где N - номер службы, полученной на предыдущем шаге.

На первой ноде группы `proxy` внести изменения в содержимое файла стека `/opt/poseidon/psn-etcd.yml`. Необходимо заменить соответствующую метку:

```
<old_hostname>-etcd: "etcdN"
```

на

```
<new_hostname>-etcd: "etcdN"
```

6.3 Изменение hostname на хостах группы redis

В случае, если на работающей системе требуется изменить `hostname` нод, на которых работают сервисы `redis`, необходимо выполнить следующие действия:

1. Изменить `hostname` на нодах.
2. Изменить hostname в группе хостов redis инвентарного файла установки в соответствии с разделом Конфигурирование инвентарного файла: hosts.

3. Выполнить запуск установки с параметром `-t redis`:

```
./deploy_psn.sh <hosts.yml> -t redis
```

Либо в качестве альтернативного способа можно вручную внести изменения в параметры службы. Для этого следует на любой из нод группы `redis` выполнить команды:

```
docker service inspect psn-redis_redis --format='{{json .Spec.Labels}}'
docker service inspect psn-redis_sentinel --format='{{json .Spec.Labels}}'
```

По выводу команд определить метки служб, связанных со старым значением `hostname`. Команды вернут записи вида:

```
<old-hostname>-redis":"redis-N"
<old-hostname>-sentinel":"sentinel-N"
```

Далее выполнить команды по изменению меток для служб:

```
docker service update --label-rm <old_hostname>-redis --label-add
<new_hostname>-redis=redis-N --force psn-redis_redis
docker service update --label-rm <old_hostname>-sentinel --label-add
<new_hostname>-sentinel=sentinel-N --force psn-redis_sentinel
```

Где N - номер службы, полученной на предыдущем шаге.

Далее на первой ноде группы proxy внести изменения в содержимое файла стека `/opt/poseidon/psn-redis-stack.yml`. Необходимо заменить соответствующую метку:

```
<old_hostname>-redis: "redis-N"
<old_hostname>-sentinel: "sentinel-N"
```

на

```
<new_hostname>-redis: "redis-N"
<new_hostname>-sentinel: "sentinel-N"
```

Все команды для `sentinel` выполняются только при кластерной установке

7 ИЗВЕСТНЫЕ ПРОБЛЕМЫ И СПОСОБЫ РЕШЕНИЯ

В данном разделе приведены изменения, которые не вошли в дистрибутив текущего релиза и должны быть внесены дополнительно после или во время установки.

7.1 Установка для большого количества пользователей

В текущем релизе выявлена проблема с кластерной установкой, рассчитанной на одновременную работу 500 и более пользователей – производительности, используемой в поставке распределенной файловой системы, для хранения базы данных писем недостаточно. В этом случае рекомендуется развернуть распределённое реплицируемое блочное устройство (drbd) и настроить хранение писем на нем. Так как в репозиториях рекомендуемых дистрибутивов версия drbd устаревшая, до процесса перехода необходимо произвести сборку и установку drbd вручную, см. раздел Установка и первоначальная настройка распределённого блочного устройства.

7.1.1 Установка и первоначальная настройка распределённого блочного устройства

Перед установкой распределённого реплицируемого блочного устройства (drbd) необходимо выполнить подготовку нод. Рекомендуется использовать конфигурацию с тремя нодами: две с данными, третья – без данных, в роли арбитра. Ноды с данными должны быть такими же, как и ноды группы mail, нода в роли арбитра выбирается произвольно. На ноды с данными необходимо подключить отдельные диски требуемого размера, создать на них тома lvm.

Для подготовки нод следует:

1. Обновить пакеты на всех нодах, где будет использоваться drbd (возможно предварительно необходимо подготовить репозитории):

для deb:

```
apt update && apt full-upgrade -y
```

для rpm:

```
yum update -y
```

2. Перезагрузить ноды.
3. Убедиться, что:

– на всех нодах версия ядра совпадает (минимально допустимая версия ядра 3.10):

```
uname -r
```

– на всех нодах установлены уникальные hostname:

```
uname -n
```

– на всех нодах версии docker совпадают:

```
docker version
```

(либо, если docker swarm инициализирован, на любом из manager:

`docker node ls`).

4. Подготовить диски для хранения данных на выделенных для этого двух нодах.

Рекомендуется использовать lvm.

После подготовки нод, следует выбрать ноду, на которой будет происходить сборка пакетов. Действия по сборке выполнять только на выбранной ноде.

Выполнить сборку:

1. Создать структуру директорий относительно домашней:

```
mkdir -p ~/drbd/{bin,kernel,reactor,tools}
```

2. Установить необходимые зависимости:

для deb:

```
apt-get install -yq \
  curl \
  build-essential \
  flex \
  libkeyutils-dev \
  wget
```

для rpm:

```
yum install -y \
  gcc \
  kernel-headers \
  kernel-devel \
  keyutils-libs-devel \
  make \
```



```
  patch
  flex
```

3. Собрать модули ядра drbd. Подготовить сценарий `~/drbd/drbd_kernel.sh` и выполнить его:

```
#!/bin/bash

kernel_modules_ver="9.2.10"
kernel_modules_uri="https://linbit.gateway.scarf.sh/downloads/drbd/9/drbd-$kernel
_modules_ver.tar.gz"

cd ~/drbd/kernel/

wget -qO- "$kernel_modules_uri" | tar xz --strip-components=1

make -j$(nproc --all)
make install DESTDIR=$(pwd)/../bin/kernel/

cd ~
```

4. Собрать утилиты администрирования drbd. Подготовить сценарий `~/drbd/drbd_tools.sh` и выполнить его:

```
#!/bin/bash

tools_ver="9.28.0"
tools_url="https://linbit.gateway.scarf.sh/downloads/drbd/utils/drbd-
utils-$tools_ver.tar.gz"

cd ~/drbd/tools/

wget -qO- "$tools_url" | tar xz --strip-components=1

./configure --prefix=/usr --localstatedir=/var --sysconfdir=/etc --without-manual
--without-84support --with-initscripttype=none --with-pacemaker=no
make tools -j$(nproc --all)
make install DESTDIR=$(pwd)/../bin/tools/

cd ~
```

5. Собрать drbd-reactor. Подготовить сценарий `~/drbd/drbd_reactor.sh` и выполнить его:

```
cd ~/drbd/reactor/

cat > Dockerfile <<"EOF"
FROM rust:1.78

ARG reactor_ver="1.4.2"
ARG reactor_uri="https://linbit.gateway.scarf.sh/downloads/drbd/utils/drbd-reactor-$reactor_ver.tar.gz"

RUN wget -qO- "$reactor_uri" | tar xz -C /tmp --strip-components=1 && \
    cd /tmp; \
        rustup target add x86_64-unknown-linux-musl; \
    cargo build --release --target x86_64-unknown-linux-musl

EOF

docker build . -t reactor

cd ~
docker create --name extract reactor
docker cp extract:/tmp/target/x86_64-unknown-linux-musl/release/drbd-reactor ~/drbd/bin/reactor/
docker cp extract:/tmp/target/x86_64-unknown-linux-musl/release/drbd-reactorctl ~/drbd/bin/reactor/
docker rm extract
```

После выполнения сборки следует переместить каталог `~/drbd/bin/` с собранными пакетами на остальные ноды, на которых будет работать drbd.

Дальнейшие действия выполнять всех выбранных нодах drbd:

1. Установить модуль ядра:

```
cp -r ~/drbd/bin/kernel/lib/modules/$(uname -r)/updates/ /lib/modules/$(uname -r)/; depmod; modprobe drbd; modprobe drbd_transport_tcp
```

2. Установить утилиты администрирования:

```
cp ~/drbd/bin/tools/usr/sbin/drbd* /usr/sbin/
```


3. Установить drbd-reactor:

```
cp ~/drbd/bin/reactor/{drbd-reactor,drbd-reactorctl} /usr/sbin/
```

Далее необходимо подготовить конфигурационные файлы drbd. Для этого необходимо перейти в каталог с дистрибутивом на инфраструктурной машине. В инвентарном файле, в группе хостов drbd, необходимо перечислить ноды, на которых будут запущены службы drbd. Первыми необходимо перечислить ноды с данными, последней – ноду, исполняющую роль арбитра. Службы drbd будут запущены в режиме primary – secondary. Нода, указанная первой, всегда будет стремиться стать primary, поэтому первой необходимо указать ноду, где в данный момент размещается актуальная база данных писем пользователей.

После подготовки инвентарного файла необходимо отредактировать плейбук подготовки конфигурационных файлов drbd `drbd_configs.yml`.

В секции `vars`, в переменной `disk` необходимо указать путь до блочного устройства lvm. Значение по умолчанию подразумевает, что на нодах с данными, в группе томов data, создан том lvm с именем drbd, то есть путь до устройтва `/dev/data/drbd`.

Запустить плейбук подготовки конфигурационных файлов:

```
ansible-playbook –i inventory/<inventory> drbd_configs.yml
```

где `<inventory>` – актуальный инвентарный файл.

После выполнения плейбука, необходимо:

1. Инициализировать ресурс:

На всех нодах, выбранных для работы drbd, выполнить команды:

```
drbdadm create-md dovecot
drbdadm up dovecot
drbdadm status dovecot
```

Далее на одной из нод (выбранной произвольно) выполнить команды:

```
drbdsetup new-current-uuid --clear-bitmap 0
drbdadm primary dovecot
mkfs.ext4 /dev/drbd0
drbdadm secondary dovecot
```

2. Запустить соответствующие службы (команды выполнить на всех нодах, выбранных для работы drbd):

```
systemctl enable --now drbd
systemctl enable --now drbd-reactor
```

3. Определить primary ноду:

```
drbd status dovecot
drbd-reactorctl status dovecot
```

и выполнить на ней команду:

```
chown -R 1001:1001 /drbd/dovecot/
```

После выполнения всех действий на нодах группы mail станет доступно реплицируемое блочное устройство. На primary ноде станет доступна точка монтирования `/drbd/dovecot/`, ее необходимо указать в переменной `cluster_drbd_mail_path` инвентарного файла.

После завершения настроек drbd можно приступать к подготовке стенда для работы с устройством drbd и миграции на него базы данных писем, если это необходимо (см. раздел Миграция на формат хранения писем mdbox).

7.2 Изменение файловой системы

В текущем релизе при установке из дистрибутива на выделенном устройстве требуется файловая система `xfs`. Это поведение можно изменить, отредактировав шаблон конфигурации соответствующей роли до начала деплоя.

- для роли `etcd` в файлах `roles/etcd/templates/etcd.yml.j2` (в случае **standalone** инсталляции) `roles/etcd/templates/etcd-cluster.yml.j2` (в случае **кластерной** инсталляции);
- для роли `postgres` в файлах `roles/postgres/templates/postgres-stack.yml.j2` (в случае **standalone** инсталляции) `roles/postgres/templates/patroni-stack.yml.j2` (в случае **кластерной** инсталляции);

– в конфигурации `volume`, в свойстве `type` указать необходимую файловую систему (`xfs/ext4`).

8 МИГРАЦИЯ НА ФОРМАТ ХРАНЕНИЯ ПИСЕМ MDBOX

Сценарий миграции позволяет перейти на формат хранения базы писем mdbox и, при необходимости, перенести базу на другое блочное устройство. Миграция не затрагивает работу стенда и происходит незаметно для пользователей.

8.1 Подготовка к миграции

Перед запуском процедуры миграции необходимо подготовить конфигурационные файлы. Для этого следует перейти в каталог с дистрибутивом на инфраструктурной машине и открыть плейбук `migrator_prep.yml`.

В зависимости от требований, следует настроить следующие параметры:

- `backup_rsync`: выполнять резервную копию исходной базы писем при помощи rsync. Значение `false` – не выполнять, `true` – выполнять. Копия будет сохранена по пути, указанному в переменной `host_backup_dir`.
- `backup_archive`: выполнять резервную копию исходной базы писем архивированием. Значение `false` – не выполнять, `true` – выполнять. Архив будет сохранен по пути, указанном в переменной `host_backup_dir`. В случае, если `backup_rsync` и `backup_archive` заданы значения `true`, резервная копия будет выполняться как посредством rsync, так и архивированием;
- `del_migrated_mailbox`: удалять исходную базу писем после миграции. Значение `false` – не выполнять, `true` – выполнять. После выполнения миграции база писем в исходном расположении не требуется и не влияет на работу ящика. Исходная база писем может удаляться, если это позволяет свободное дисковое пространство и если может потребоваться оперативный откат к исходной базе.
- `host_backup_dir`: путь до каталога, в который будут сохраняться резервные копии. Для каждого ящика архив будет помещен в собственный каталог. Необходимо рассчитывать доступное место в точке монтирования каталога, исходя из объемов писем на стенде.
- `current_host_maildir`: путь в хостовой операционной системе до каталога исходной базы писем.
- `new_host_maildir`: путь в хостовой операционной системе до каталога нового расположения базы писем. Если `new_host_maildir` совпадет с `current_host_maildir`, при работе мигратора база писем будет только сконвертирована в формат mdbox, без переноса в новое хранилище.

Значения параметров `current_container_maildir` и `new_container_maildir` изменять не нужно.

Далее необходимо запустить плейбук для подготовки модуля миграции:

```
ansible-playbook -i inventory/<inventory> migrator_prep.yml
```

где `<inventory>` – актуальный инвентарный файл.

После выполнения плейбука стенд будет подготовлен для проведения миграции. На нодах mail, в домашнем каталоге, появится модуль миграции – файл `mdbox_migration.sh`.

Необходимо проверить, что стенд функционирует штатно. В случае неисправности можно вернуть стенд к стандартному состоянию, используя команду запуска стенда с тегом `mail`:

```
deploy_psh.sh <inventory> -t mail
```

Миграция запускается на ноде mail, на которой находится актуальная база писем. На этой ноде должна быть установлена утилита `ldapsearch`.

Рекомендуется сначала проверить работу мигратора на нескольких учетных записях. Для указания списка тестовых пользователей в сценарии миграции `mdbox_migration.sh` необходимо использовать переменную USER_LIST. Если данная переменная определена, миграция будет выполнена только для указанных пользователей, иначе – для всех пользователей стенда. Адреса электронной почты следует указывать в скобках, используя пробел в качестве разделителя.

8.2 Запуск миграции

Миграция запускается командой:

```
bash ./mdbox_migration.sh
```

Модуль миграции проверит базовые параметры, после чего начнется процесс миграции. Процесс можно останавливать и запускать без дополнительных действий. Во время миграции можно пользоваться стендом.

После миграции ящиков всех пользователей необходимо в инвентарном файле изменить значение переменной `setup.mdbox_format` на `true` и, если стенд был переведен на работу с drbd, изменить значения переменных: `setup.cluster_drbd` – на `true`,

`setup.cluster_drbd_mail_node` — на `"dovecot"`, а в переменной `setup.cluster_drbd_mail_path` указать путь до актуальной базы данных писем.

После этого следует выполнить команду запуска стенда с тегом `mail` для перевода стенда на работу исключительно с форматом mdbox:

```
deploy_psh.sh <inventory> -t mail
```

9 ТЕХНИЧЕСКАЯ ПОДДЕРЖКА

Контактная информация службы технической поддержки ООО ««Новые облачные технологии» в случае возникновения вопросов, не описанных в данном руководстве:

Адрес электронной почты: support@service.myoffice.ru Телефон: 8-800-222-1-888.