



МойОфис Частное Облако

Руководство по установке

ПОЧТА (PSN)



ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Мой Офис «Частное Облако»

Мой Офис «Почта»

РУКОВОДСТВО ПО УСТАНОВКЕ

2021.04

На 46 листах

Москва

2021



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.

© ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ», 2013–2021

Содержание

Перечень сокращений, терминов и определений	7
1 Общие сведения	9
1.1 Назначение	9
1.2 Требования к квалификации персонала	9
1.3 Системные требования	10
1.3.1 Аппаратные требования	10
1.3.2 Программные требования	11
1.3.2.1 Поддерживаемые операционные системы	11
1.3.2.2 Рекомендации по настройке ОС	11
1.3.2.3. Рекомендации по разбиению дисков	11
1.3.2.4 Настройка синхронизации времени	12
1.3.2.5 Настройка инфраструктурной машины	12
1.3.2.6 Настройка DNS	12
1.3.2.7 Доступ из сети интернет	14
1.3.2.8 Ресурсные записи для функционирования	14
1.4 Ограничения	15
2 Описание архитектуры «МойОфис Почта»	16
2.1. Общая архитектурная схема	16
2.2. Детальная архитектурная схема «МойОфис Почта»	16
3 Типовые схемы установки «МойОфис Почта»	18
3.1 Конфигурация без отказоустойчивости	18
3.2 Кластерная отказоустойчивая конфигурация	18
3.3 Типовая схема масштабирования	18
4 Первичная установка	19
4.1 Состав дистрибутива	19
4.2 Подготовка к установке	19
4.2.1 Описание ролей	19
4.2.2 Подготовка инфраструктуры установки	21

4.2.2.1 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива (с доступом в Интернет)	22
4.2.2.3 Подготовка серверов, на которые будет производиться инсталляция дистрибутива (без доступа в Интернет)	22
4.2.3 Настройка основных параметров установки	23
4.2.3.1 VIP Адреса	23
4.2.3.2 Конфигурационные параметры	23
4.2.3.3 Пароли	24
4.2.3.4 Параметры LDAP	25
4.2.3.6 Сертификаты и ключ DKIM	26
4.2.4 Настройка дополнительных параметров установки	27
4.2.4.1 Прочие параметры конфигурации	27
4.2.4.2 Интеграция с облачными редакторами	28
4.2.5 Настройка межсетевого экранирования	31
4.2.6 Разграничение доступа	32
4.2.7 Настройка удаленного доступа	32
4.3 Установка «МойОфис Почта»	32
4.3.1 Конфигурация без отказоустойчивости	32
4.3.1.1 Запуск установки	32
4.3.1.2 Проверка корректности установки	32
4.3.2 Кластерная отказоустойчивая конфигурация	33
4.3.2.1 Запуск установки	33
4.3.2.2 Проверка корректности установки	33
4.4 Установка в составе «МойОфис Частное Облако»	33
5 Обновление с предыдущих версий	34
5.1 Состав дистрибутива	35
5.2 Подготовка к обновлению	35
5.2.1 Описание ролей	35
5.2.2 Проверка и настройка инфраструктуры установки	35
5.2.3 Проверка и настройка основных параметров установки	35
5.2.4 Проверка и настройка дополнительных параметров установки	35
5.2.5 Проверка и настройка межсетевого экранирования	35
5.2.6 Проверка и настройка разграничения доступа	35

5.2.7 Проверка и настройка удаленного доступа	35
5.2.8 Создание резервных копий	35
5.2.8.1 База данных:	35
5.2.8.2 Схема LDAP:	36
5.2.8.2 Почтовые ящики:	36
5.3 Обновление «МойОфис Почта»	37
5.3.1 Конфигурация без отказоустойчивости	37
5.3.1.1 Запуск обновления	37
5.3.1.2 Проверка корректности обновления	37
5.3.1.3 Миграция данных	37
5.3.2 Кластерная отказоустойчивая конфигурация	38
5.3.2.1 Масштабирование конфигурации	38
5.3.2.1 Запуск обновления	38
5.3.2.2 Проверка корректности обновления	38
5.3.2.3 Миграция данных	38
6 Дополнительные возможности и рекомендации по установке	41
6.1 Варианты запуска установки	41
6.2 Использование AD в продукте «МойОфис Почта»	41
6.3 Замена сертификатов	43
6.4 Использование веб-браузера caldav сервера	44
6.5 Синхронизация аватарок между доменами	44
6.6 Синхронизация пользователей с Битрикс24	45
7 Техническая поддержка	46

Перечень сокращений, терминов и определений

Сокращение, термин	Расшифровка и определение
ПО МойОфис	Программное обеспечение. «МойОфис Почта». «МойОфис Частное Облако»
DNS	Domain Name System, система доменных имён
CAB	Common Address Book, общая адресная книга пользователей Системы
CO	CloudOffice, «МойОфис Облачные Редакторы»
FQDN	Fully Qualified Domain Name, полностью определённое имя домена
FS	File Storage, «МойОфис Хранилище»
IMAP	Internet Messagess Access Protocol, протокол доступа к ящику электронной почты
IPVS	IP Virtual Server, модуль маршрутизации трафика L4
LDAP	Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам
PSN	Postal Solution, «МойОфис Почта»
PSNAPI	Postal Solution API, API «МойОфис Почта»
SMTP	Simple Mail Transfer Protocol, протокол передачи сообщений электронной почты
SSH	Secure Shell
URL	Uniform Resource Locator, единый указатель ресурса
VIP	Virtual IP, виртуальный IP адрес, совместно используемый несколькими нодами
XML	eXtensible Markup Language
БД	База Данных
Контур инсталляции	Приватная сеть, в рамках которой происходит обмен техническими данными между серверами инсталляции
Нода, node	Сервер одной из ролей

Сокращение, термин	Расшифровка и определение
Плейбук, playbook	Сборник скриптов
ОС	Операционная система
Докер, docker	Система контейнеризации

Таблица 1. Перечень сокращений, терминов и определений.

1 Общие сведения

1.1 Назначение

Почтовая система (в дальнейшем Система) – это программное обеспечение, предназначенное для получения, отправки и хранения сообщений электронной почты корпоративных пользователей.

«МойОфис Почта» – универсальная коммуникационная система enterprise-уровня, обеспечивающая:

- создание, передачу, получение и сообщений электронной почты;
- работу с общей и личной адресными книгами;
- календарное планирование.

1.2 Требования к квалификации персонала

Администратор «МойОфис Почта» 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 с системой контейнеризации Docker:
 - установка Docker;
 - запуск / остановка / перезапуск контейнеров;
 - работа с реестром контейнеров;
 - получение конфигурации контейнеров;
 - сеть в Docker, взаимодействие приложений в контейнерах;
 - решение проблем контейнерной виртуализации;
- Опыт работы с VMWare vSphere ESXi 6.5 и выше;
- Опыт работы с командной строкой ОС Linux;
- Знания в объеме курсов Red Hat RH124, RH134, RH254;

- Знания в объеме, достаточном для сдачи сертификационного экзамена Red Hat EX300;
- Опыт работы со службой доменных имен (DNS):
 - знание основных терминов (DNS, IP-адрес и так далее);
 - понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен и так далее);
 - знание типов записи и запросов DNS;
- знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся: закрытый и открытый ключи;
 - сертификат открытого ключа;
- регистрационный центр (RA);
 - сертификационный центр (CA);
- хранилище сертификатов (CR);

1.3 Системные требования

1.3.1 Аппаратные требования

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

Таблица 2. Аппаратные требования.

- Скорость сетевой подсистемы — 1Gbit/s или выше;
- Данная конфигурация может быть использована только для функционального тестирования;
- Должен быть установлен один из поддерживаемых дистрибутивов операционной системы;
- Для отказоустойчивой конфигурации должны использоваться 7 или более виртуальных машин.

1.3.2 Программные требования

1.3.2.1 Поддерживаемые операционные системы

- Centos 8.1 (рекомендуемый дистрибутив);
с предустановленными пакетами, см. ниже;
- Centos 7.9;
- AstraLinux 2.12;
- AltLinux 9;

1.3.2.2 Рекомендации по настройке ОС

- Для инсталляции ОС рекомендуется использовать **минимальный** вариант установки ОС;
- Перевести **SELinux** в состояние Disabled;
- Предустановленные пакеты для CentOS 8.1: python3, python-setuptools, wget, python3-netaddr;
- Настроить имя хоста и параметры сети. Необходимо учитывать, что интерфейс по умолчанию, используемый в инсталляции для передачи данных, определяется по наличию пути по умолчанию (default route) в конфигурации интерфейса на целевом сервере.

1.3.2.3. Рекомендации по разбиению дисков

Назначение	Точка монтирования	Объем	Группы
ОС	/	50gb	all
БД	/opt/psn/db/data	10% от квоты, выделенной для пользователей	db
Логи	/opt/syslogng-data/logs/	Зависит от объема и сроков хранения информации	log
Аттачи к событиям при кластерной конфигурации	/data/glusterfs/psn-eattach	Зависит от объема аттачей к событиям	web-client
Вложения документов	/data/glusterfs/psn-preview	Зависит от объема вложений	web-client

Назначение	Точка монтирования	Объем	Группы
Аттачи к событиям при бескластерной конфигурации	/opt/psn/web-client/data/eattach	Зависит от объема аттачей к событиям	web-client
Вложения документов при бескластерной конфигурации	/opt/psn/web-client/data/preview/files	Зависит от объема вложений	web-client
Квота почтовых ящиков пользователей	/data/glusterfs/dovecot	суммарный объем квот пользователей + 20%	be
Квота почтовых ящиков пользователей при бескластерной конфигурации	/var/dovecot	суммарный объем квот пользователей + 20%	be

Таблица 3. Разбиение дисков.

1.3.2.4 Настройка синхронизации времени

Для корректной работы «МойОфис Почта» необходимо настроить службу синхронизации времени на серверах.

1.3.2.5 Настройка 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.

1.3.2.6 Настройка DNS

На всех серверах «МойОфис Почта» настроить DNS, который будет корректно разрешать имена системы в приватные IP адреса. Доменные имена приведены в Таблице 4.

Доменное имя	Cluster IP	SA IP	Комментарий
autoconfig[-env].domain.name	inv_vip_web	IP адрес fe	
cab[-env].domain.name	inv_vip_web	IP адрес cab	
imap[-env].domain.name	inv_vip_mail	IP адрес be	
{{inv_url_prefix}}[-env].domain.name	inv_vip_web	IP адрес fe	переменная inv_url_prefix по умолчанию имеет значение mail
psnapi[-env].domain.name	inv_vip_web	IP адрес fe	обязателен только для разрешения внутри контура инсталляции
smtp[-env].domain.name	inv_vip_mail	IP адрес be	
pbm[-env].domain.name	inv_vip_mail	IP адрес be	
admin[-env].domain.name	inv_vip_web	IP адрес fe	В случае установки без интеграции

Таблица 4. Доменные имена.

Где `inv_vip_mail` , `inv_vip_web` - переменные из инвентарного файла.

Для внешних систем доменные имена должны корректно разрешаться в соответствующий публичный IP адрес.

Для инсталляции с Облачными Редакторами на серверах PSN имена внутри контура инсталляции должны разрешаться корректно. Доменные имена приведены в Таблице 5.

Имя	Во что разрешать
pgs[-env].domain.name	inv_fs_url
mtadmin[-env].domain.name	CNAME fsapi
appapi[-env].domain.name	CNAME fsapi

Таблица 5. Доменные имена для инсталляции с Облачными Редакторами.

где `inv_fs_url` - переменная из инвентори файла.

- Для инсталляции «МойОфис Хранилище» необходимо корректно настроить DNS по инструкции, прилагаемой с продуктом, с учетом указанных выше доменных имен;
- Данные изменения можно внести после установки «МойОфис Хранилище». (см. Инструкцию по установке «МойОфис Хранилище»);

1.3.2.7 Доступ из сети интернет

Для доступа к почтовой системе из сети Интернет необходим один публичный IP адрес и доменные имена системы, корректно разрешающиеся в данный IP адрес. Так же необходимо настроить NAT в соответствии с таблицей ниже. Необходимые порты приведены в таблице 6.

Порты	Приватный адрес
993, 465, 587, 25, 4190, 48666	inv_vip_mail
80, 443, 444, 636	inv_vip_web

Таблица 6. Порты.

1.3.2.8 Ресурсные записи для функционирования

Почтовая система требует дополнительные записей в DNS для доставки и отправки писем:

- MX
- SRV
- PTR
- TXT (SPF, DKIM)

Обратитесь к документации по настройке вашего DNS-сервера для получения подробной информации о добавлении ресурсных записей.

Для подробной информации о ресурсных записях обратитесь к следующим RFC:

- 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 to WebDAV (CardDAV);

1.4 Ограничения

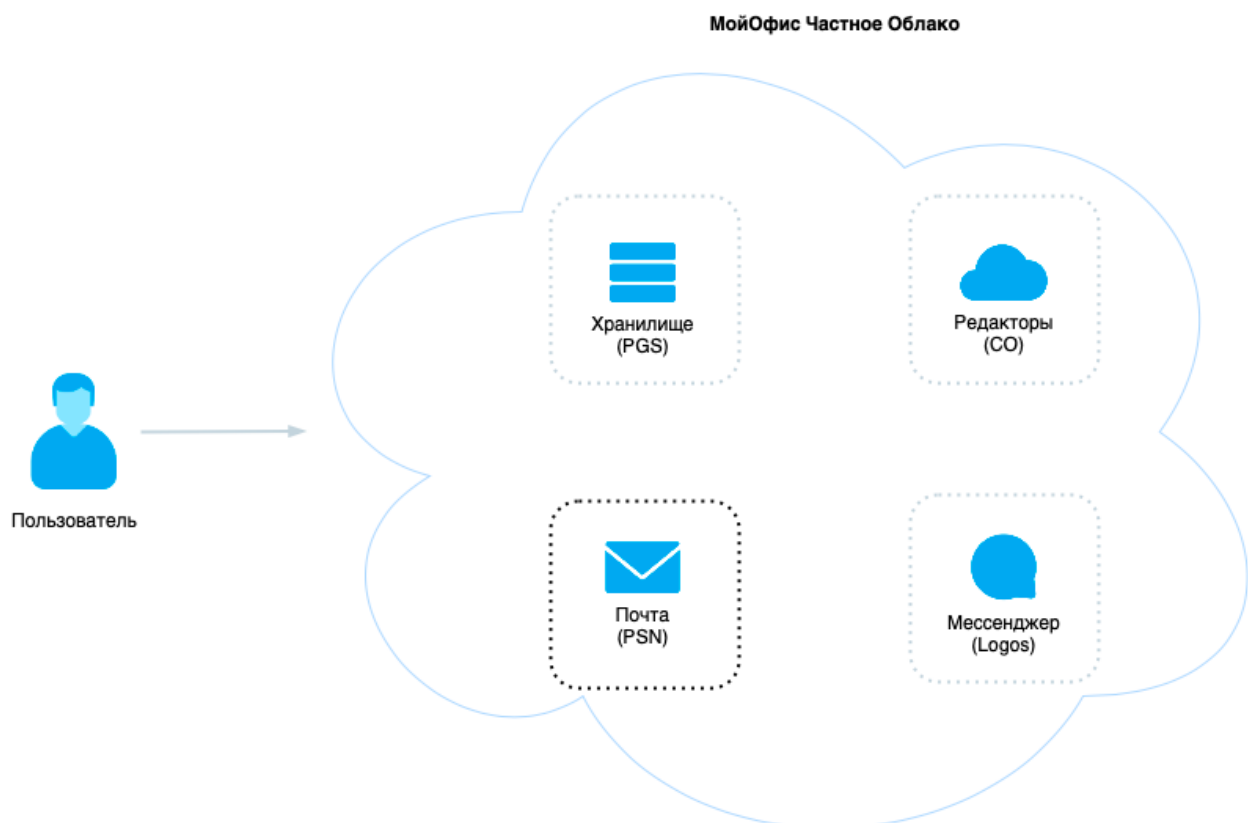
- Не допускается в среде виртуализации использовать клонированные виртуальные машины для инсталляции продукта;
- Не допускается копирование установленных операционных систем между физическими серверами или использование образа предустановленной операционной системы для развертывания физических серверов;
- Не допускается оверкоммит ресурсов в среде виртуализации;
- Не допускается использование DHCP-служб в сегменте сети инсталляции;

2 Описание архитектуры «МойОфис Почта»

2.1. Общая архитектурная схема

Общая архитектурная схема «МойОфис Частное Облако» приведена на Рисунке 1.

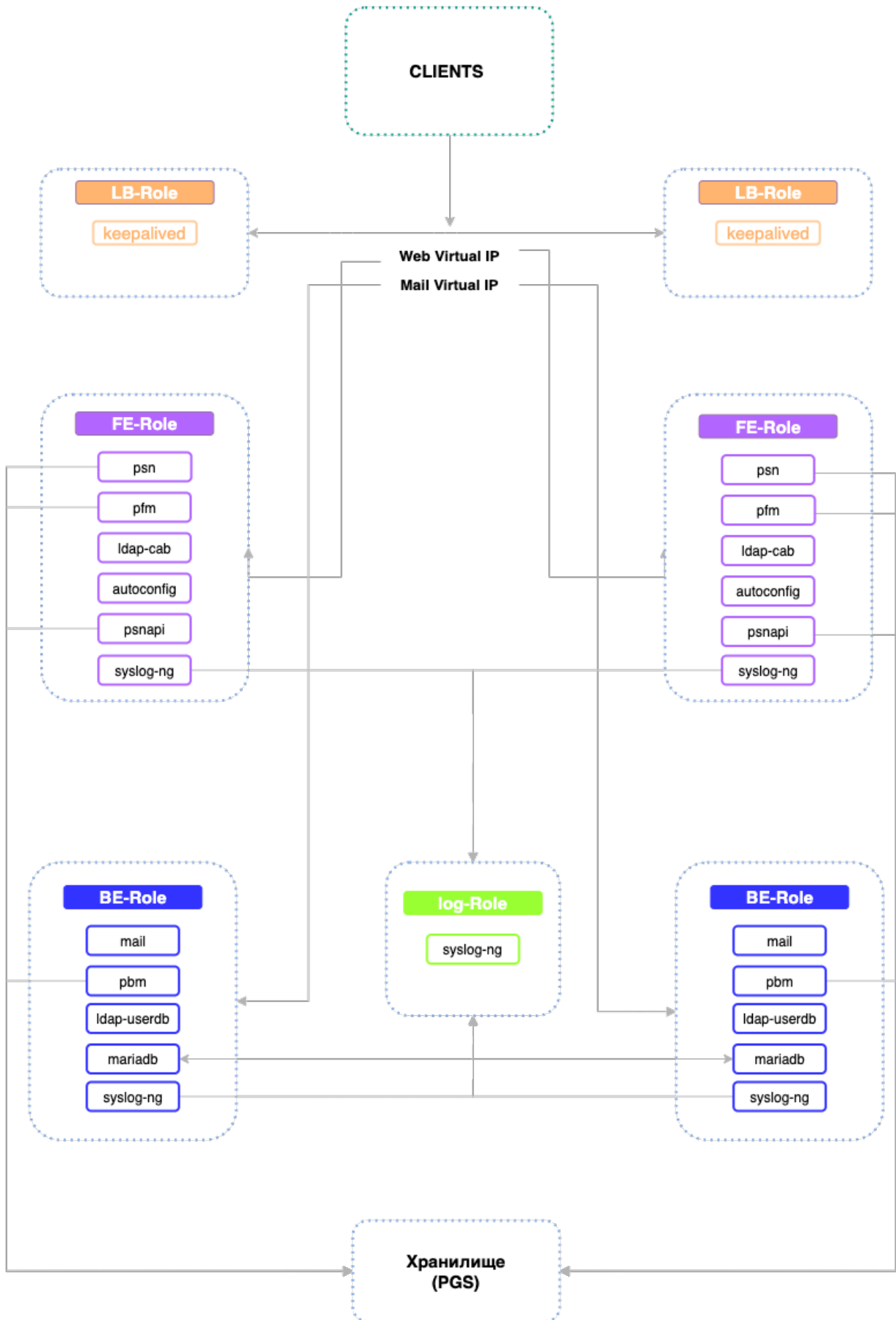
Рисунок 1. Общая архитектурная схема «МойОфис Частное Облако»:



2.2. Детальная архитектурная схема «МойОфис Почта»

Данная схема «МойОфис Почта» приведена на Рисунке 2.

Рисунок 2. Детальная архитектурная схема «МойОфис Почта»:



3 Типовые схемы установки «МойОфис Почта»

3.1 Конфигурация без отказоустойчивости

В данной конфигурации все роли устанавливаются на один виртуальный или физический сервер. Такая конфигурация может использоваться в целях разработки или демонстрации возможностей продукта (virtual appliance).

3.2 Кластерная отказоустойчивая конфигурация

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

3.3 Типовая схема масштабирования

Для односерверной (не кластерной) конфигурации возможно только вертикальное масштабирование. Переход от такой конфигурации к кластерной возможен только путем полной переустановки «МойОфис Почта». Для кластерной отказоустойчивой конфигурации поддерживается вертикальное (рекомендуемое) и горизонтальное масштабирование (кроме сервиса ldap и сервиса базы данных).

4 Первичная установка

4.1 Состав дистрибутива

Дистрибутив содержит:

- Набор Ansible ролей для установки и обновления «МойОфис Почта»;
- Репозиторий Docker контейнеров;
- Инструкцию по установке.

4.2 Подготовка к установке

4.2.1 Описание ролей

Инвентарный файл (inventory file) содержит логические группы (роли), на которые будет разделен кластер инсталляции. Данные роли описаны в Таблице 7.

Роль	Группа хостов	Описание	Комментарии	Максимальное кол-во серверов
ac	fe	Автоконфигуратор для десктопного клиента		2
backup	all	Роль для выполнения бэкапа бд и схемы лдап		
bootstrap	all	Роль для первичной настройки ОС и установки необходимых сервисов		
certificates	fe, be	Роль установки сертификатов		
docker_service	all	Роль установки и настройки Docker		

Роль	Группа хостов	Описание	Комментарии	Максимальное кол-во серверов
be	be	Роль установки и настройки почтовой системы		2
db	db	Роль установки и настройки сервера бд		2
glusterfs	fe, be	Роль настройки glusterfs		2
keepalived	lb	Роль настройки системы балансировки		2
ldap	cab, userdb	Роль установки и настройки службы каталогов	не поддерживается смена количества нод после первичной инсталляции	2
log	all	Роль настройки логирования		
psnapl	fe	Роль установки и настройки psnapl сервиса		
registry	registry	Роль настройки локального докер репозитория		
webclient	fe	Роль установки веб-клиента		2

Роль	Группа хостов	Описание	Комментарии	Максимальное кол-во серверов
fe	fe	Вспомогательная роль для установки веб-клиента		

Таблица 7. Роли.

Для определения принадлежности сервера к роли необходимо добавить его IP адрес в соответствующую секцию в инвентарном файле. Например:

```
[log]
plog.myoffice.ru
```

4.2.2 Подготовка инфраструктуры установки

При выполнении проверки и подготовки инсталляционных архивов необходимо выполнить следующие действия:

1. После копирования инсталляционного архива проверить его контрольную сумму md5:

В имени архива цифры версии коммерческого релиза представлены знаками X.

```
md5sum -c MyOffice_Mail_PSN_XXXX.XX.md
```

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

Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

```
tar xvzf "MyOffice_Mail_PSN_*.tar.gz"
cd install_myoffice_psn_*
```

3. Установить на инфраструктурную машину пакеты:

- Ansible 2.10.5 (работа на более новой версии возможна, но не гарантирована)
- Jinja2 версии 2.10 или выше.

4. Заполнить инвентарный файл на основании входящих в состав дистрибутивов примеры, находящимся по пути: **inventory/standalone.example** (в случае установки без отказоустойчивости) или **inventory/cluster.example** (в случае установки с отказоустойчивостью)

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

Для подготовки **целевых серверов** к установке для них необходимо выполнить пункты из параграфа 1.3.2 данного руководства.

При наличии доступа в Интернет на целевых машинах никакой иной подготовки серверов не требуется, все необходимые зависимости установятся в рамках работы инсталлятора.

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

Если сервер-оператор и целевые серверы расположены в локальной сети и не имеют прямого доступа в Интернет, то необходимо предустановить на них пакеты: (названия приведены для CentOS 8, без зависимостей):

Для всех серверов:

- python3
- python3-setuptools
- docker-ce
- docker-ce-cli
- containerd.io
- rsync

Для серверов с ролью **lb**:

- keepalived
- lvsadm

Для серверов с ролью **fe, be** (в случае кластерной установки):

- glusterfs-server

Пакеты `pip` для всех серверов:

- docker

4.2.3 Настройка основных параметров установки

4.2.3.1 VIP Адреса

VIP адрес - совместно используемый адрес для распределения нагрузки между нодами и обеспечения отказоустойчивости. Параметры приведены в таблице 8.

Переменная	Назначение	Значение по умолчанию	Комментарии
<code>inv_vip_mail</code>	Виртуальный адрес для балансировки серверов с ролью be	Отсутствует	новый IP адрес, не задействованный в сегменте сети
<code>inv_vip_web</code>	Виртуальный адрес для балансировки серверов с ролью fe	Отсутствует	новый IP адрес, не задействованный в сегменте сети

Таблица 8. VIP.

4.2.3.2 Конфигурационные параметры

Переменная	Назначение	Значение по умолчанию	Комментарии
<code>standalone</code>	Выбор типа инсталляции: кластер или однонодовая	<code>false</code>	Если производится инсталляция на один сервер изменить значение на <code>true</code>
<code>inv_domain_fqdn</code>	доменное имя инсталляции в формате FQDN	<code>example.com</code>	
<code>inv_env</code>	используемое окружение для инсталляции	не задается	добавляет постфикс именам, <code>mail</code> становится <code>mail-env</code> , а почтовый домен <code>env.inv_domain_fqdn</code>

Переменная	Назначение	Значение по умолчанию	Комментарии
<code>inv_url_prefix</code>	префикс доменного имени, используемый для веб-клиента	<code>mail</code>	определяет адрес используемый для вебклиента, отступает на уровень выше от <code>inv_domain_fqdn</code> , например <code>mail.example.com</code>
<code>inv_quota_size</code>	размер квоты почтового ящика по умолчанию	2G (используйте 0 для отключения)	дефолтное значение квоты почтового ящика, параметр задается в Кб, для упрощения записи можно использовать значения G(Гб), M(Мб), K(Кб)

Таблица 9. Конфигурационные параметры.

4.2.3.3 Пароли

Переменная	Назначение	Политика безопасности
<code>inv_lb_keepalived_pass</code>	пароль для взаимодействия LB-нод, используется не более 8 символов	
<code>inv_db_aurora_pass</code>	пароль для доступа к БД веб-клиента	+
<code>inv_db_mysql_root_pass</code>	пароль суперпользователя для доступа к БД	+
<code>inv_be_dovecot_admin_pass</code>	пароль для синхронизации данных между MDA	

Переменная	Назначение	Политика безопасности
<code>inv_users_pass</code>	после инсталляции создается два почтовых ящика: <code>test@[env.]inv_domain_fqdn</code> и <code>postmaster@[env.]inv_domain_fqdn</code> с указанным паролем	
<code>inv_db_aurora_password_key</code>	ключ шифрования пароля в БД	+

Таблица 10. Пароли.

4.2.3.4 Параметры LDAP

Переменная	Назначение	Значение по умолчанию
<code>inv_ldap_msad</code>	переключение на использование Microsoft Active Directory	<code>false</code> (Внутренняя служба каталогов)
<code>inv_ldap_server</code>	адрес для доступа к серверу службы каталогов	<code>{{ inv_vip_userdb }}</code>
<code>inv_ldap_dn</code>	distinguished name	<code>dc=test,dc=ru</code>
<code>inv_ldap_binddn</code>	учетная запись для подключения по протоколу LDAP к службе каталогов. требует изменений только в случае использования внешней службы каталогов	<code>cn=Manager, {{inv_ldap_dn}}</code>
<code>inv_ldap_pass</code>	пароль в открытом виде для учетной записи <code>inv_ldap_binddn</code>	

Переменная	Назначение	Значение по умолчанию
<code>inv_ldap_search_user</code>	organizational unit для хранения данных по учетным записям пользователей. обычно не требует изменений	<code>OU=People, {{inv_ldap_dn}}</code>
<code>inv_ldap_search_group</code>	organizational unit для хранения данных по группам рассылок. обычно не требует изменений	<code>OU=Groups, {{inv_ldap_dn}}</code>
<code>inv_ldap_search_cab</code>	organizational unit для хранения данных адресной книги	<code>OU=CAB, {{inv_ldap_dn}}</code> в случае интеграции с FS-PGS или <code>OU=CAB,ou=default, {{inv_ldap_dn}}</code> без интеграции

Таблица 11. Параметры LDAP.

4.2.3.6 Сертификаты и ключ DKIM

Для добавления сертификатов в директории

```
~/install-psn_xxxx.xx/certificates
```

необходимо создать директорию, соответствующую сконфигурированному имени домена в переменной `inv_domain_fqdn`, содержащую файлы:

server.pem — содержит SSL-сертификат на *.DOMAIN_NAME, промежуточные сертификаты и корневой, в указанном порядке, в формате PEM; **server.key** — приватный ключ сертификата в формате PEM, не требующий кодовой фразы; **ca.pem** - корневой сертификат в формате PEM. Можно не использовать в случае использования сертификата от доверенного поставщика или если на сервере уже установлен необходимый корневой сертификат. В случае инсталляции с сертификатом выписанным собственным удостоверяющим центром или использования самоподписанного сертификата, ca.pem заполнять обязательно.

Для использования цифровой подписи DKIM, необходимо создать в директории

```
~/install-xxxx.xx/certificates
```

вложенную директорию `dkim` содержащую файл ключа:

`dkim.key` - приватный ключ для создания подписи DKIM.

В этой же директории после инсталляции будет создан файл `dkim.pub` с открытым ключом для использования в DNS. Конфигурация для цифровой подписи будет настроена только в случае существования указанного файла.

`dhparams.pem` — параметры алгоритма DH обмена ключами. Данный файл возможно сгенерировать командой `openssl dhparam -out dhparams.pem 2048` .

Структура хранения сертификатов и ключей для инсталляции:

```
certificates
├── example.com
│   ├── dkim
│   │   ├── dkim.key
│   │   └── dkim.pub
│   ├── ca.pem
│   ├── server.key
│   └── server.pem
└── dhparams.pem
```

4.2.4 Настройка дополнительных параметров установки

4.2.4.1 Прочие параметры конфигурации

Переменная	Назначение	Значение по умолчанию	Комментарии
<code>inv_virtual_domains</code>	дополнительные почтовые домены, используемые для получения писем	по умолчанию не определена, необходимо раскомментировать для использования	значения указываются через запятую

Переменная	Назначение	Значение по умолчанию	Комментарии
<code>inv_be_rsmapped_dkim</code>	селектор для использования DKIM подписи	<code>mail</code>	
<code>inv_postfix_trusted</code>	Доверенные сети для получения почтовых сообщений.		IP адреса разделенные запятой. Текущую сеть в параметре не размещается
<code>docker_network</code>	Задаёт сеть работы Docker.	<code>172.17.0.0/16</code>	
<code>docker_bip</code>	Задаёт IP адрес бридж-интерфейса докера.	<code>172.17.0.1/16</code>	
<code>triton_integration</code>		Нет	Выставить в False

Таблица 12. Прочие параметры.

4.2.4.2 Интеграция с облачными редакторами

Переменная	Назначение	Значение по умолчанию
<code>inv_fs_integration</code>	подключение к «МойОфис Хранилище» (true/false). используется для определения интеграции с облачными редакторами	<code>false</code> (интеграция отключена)
<code>inv_fs_url</code>	подключение к «МойОфис Хранилище» (PGS) (URL для подключения к pgsapi (FSAPI))	Нет
<code>inv_fsapp_url</code>	подключение к «МойОфис Хранилище» (PGS) (URL для подключения к adminapi (FSAPP))	Нет

Переменная	Назначение	Значение по умолчанию
<code>inv_fsapp_root_password</code>	подключение к «МойОфис Хранилище» (PGS). пароль администратора от FSAPP. параметр необходимо взять из инвентарного файла PGS.	Нет
<code>inv_fs_tenant_replication</code>	копирование тенантной структуры в PSN (true/false). используется для копирования сертификатов и почтовых доменов тенантов заведенных в FS. при установке с хранилищем PGS выставить <code>false</code>	<code>false</code> (копирование отключено)
<code>fs_legacy</code>	интеграция с FS релиза Mint (если FS новее - значение не менять)	<code>false</code>
<code>inv_fsapi_vip</code>	адрес виртуального IP FS-API. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>any_ip_addr</code>
<code>inv_fsdb_vip</code>	адрес виртуального IP FS-DB. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>any_ip_addr</code>
<code>inv_fsdb_port</code>	порт виртуального IP FS-DB. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	25432
<code>vmail_db_name</code>	имя базы данных vmail в FS. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>fs</code>

Переменная	Назначение	Значение по умолчанию
<code>vmail_db_user</code>	имя пользователя имеющего доступ на чтение из базы vmail в FS. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>{{ vmail_db_name }}</code>
<code>vmail_db_pass</code>	пароль пользователя имеющего доступ на чтение из базы vmail в FS. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>false</code>
<code>inv_fs_mtadmin_login</code>	логин для подключения MTADMIN-API. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>mtadminapi_user</code>
<code>inv_fs_mtadmin_pass</code>	пароль для подключения MTADMINAPI. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>mtadminapi_pass</code>
<code>FS_APP_USER</code>	Пользователь для доступа к Fs APP API. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	<code>app-co</code>
<code>FS_APP_ENC_PASSWORD</code>	параметры шифрования. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции CO	
<code>COMMON_ENCRYPTION_KEY</code>	параметры шифрования. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции CO	

Переменная	Назначение	Значение по умолчанию
COMMON_ENCRYPTION_IV	параметры шифрования. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции CO	
FS_APP_ENCRYPTION_KEY	параметры шифрования. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	
FS_APP_ENCRYPTION_IV	параметры шифрования. указывается в случае с инсталляцией с облачными редакторами, задается во время инсталляции FS	

Таблица 13. Интеграция с облачными редакторами.

4.2.5 Настройка межсетевого экранирования

Сетевые порты, доступ к которым необходим с внешних IP адресов, приведены в таблице ниже.

Номер порта	Связанный IP	Назначение
80	0.0.0.0	http
443	0.0.0.0	https
444	0.0.0.0	autoconfig-https
48666	0.0.0.0	pbm
636	0.0.0.0	ldap-https
25	0.0.0.0	smtp
587	0.0.0.0	smtp
465	0.0.0.0	smtp over ssl
993	0.0.0.0	imap
4190	0.0.0.0	sieve

Таблица 14. Описание портов, доступ к которым необходимо обеспечить.

4.2.6 Разграничение доступа

Все поддерживаемые системы имеют механизм разграничения на основании доступа к файлам и каталогам. Каждому администратору системы строго рекомендуется иметь отдельную учетную запись в системе.

4.2.7 Настройка удаленного доступа

Рекомендуется отключить удаленное подключение от пользователя `root`. Для этого в файле `/etc/ssh/sshd_config` закомментировать строку `PermitRootLogin` и выполнить перезапуск сервиса `sshd` командой `systemctl restart sshd`.

Каждый администратор системы для доступа по ssh-ключу должен поместить его публичную часть в своем домашнем каталоге в файл `~/.ssh/authorized_keys`.

4.3 Установка «МойОфис Почта»

4.3.1 Конфигурация без отказоустойчивости

4.3.1.1 Запуск установки

При установке на **centos 7.9** выставить значение `interpreter_python = /usr/bin/python` в файле `ansible.cfg`

Для запуска инсталляции подсистемы PSN необходимо запустить команду:

```
./deploy_psn.sh <inventory_name> [дополнительные параметры...]
```

При этом лог-файл процесса развертывания будет сохранен `deploy_psn_$(date +%Y%m%d).log`.

При успешном выполнении скрипта сервисы подсистемы PSN будут запущены автоматически.

После установки, применить миграции для базы данных командой:

```
./migrate_db.sh <inventory_name>
```

4.3.1.2 Проверка корректности установки

В браузере открыть страницу `https://mail-<DOMAIN_ENV>.<DOMAIN_NAME>`.

- Убедиться, что загрузилась страница авторизации;

- Убедиться, что при удачной авторизации происходит переход на страницу веб интерфейса почты;
- Отправить тестовое письмо и убедиться, что оно дошло;
- Зайти в контакты, убедиться, что в группах рассылки имеется тестовая группа (в случае чистой установки);
- Зайти в календарь, создать тестовое событие и убедиться, что оно создано;
- Зайти в настройки, изменить любые параметры и убедиться, что настройки сохранены;

4.3.2 Кластерная отказоустойчивая конфигурация

4.3.2.1 Запуск установки

Запуск установки аналогичен запуску, описанного в п. 4.3.1.1

4.3.2.2 Проверка корректности установки

Проверка аналогична, описанной в п 4.3.1.2

4.4 Установка в составе «МойОфис Частное Облако»

Для установки продукта с облачными редакторами необходимо:

- Заполнить параметры, описанные в п. 4.2.4.2;
- Произвести действия описанные в разделе 4.3;

5 Обновление с предыдущих версий

Данный дистрибутив предназначен для чистой установки, либо для миграции с версий 2020.01 Quassia и более поздних. Информация по чистой установке приведена в разделе 4. Информация по миграции описана в настоящем разделе.

Важно! Не производить обновление без наличия свежих бэкапов

Для миграции данных необходимо сделать резервные копии трех сущностей:

- Схема LDAP;
- База данных;
- Почтовые ящики;

5.1 Состав дистрибутива

Состав дистрибутива описан в разделе 4.1.

5.2 Подготовка к обновлению

5.2.1 Описание ролей

Описание роле описано в разделе 4.2.1.

5.2.2 Проверка и настройка инфраструктуры установки

Настройка описана в разделе 4.2.2.

5.2.3 Проверка и настройка основных параметров установки

Настройка описана в разделе 4.2.3.

5.2.4 Проверка и настройка дополнительных параметров установки

Настройка описана в разделе 4.2.4.

5.2.5 Проверка и настройка межсетевого экранирования

Настройка описана в разделе 4.2.5.

5.2.6 Проверка и настройка разграничения доступа

Настройка описана в разделе 4.2.6.

5.2.7 Проверка и настройка удаленного доступа

Настройка описана в разделе 4.2.7.

5.2.8 Создание резервных копий

5.2.8.1 База данных:

```
docker exec db-container sh -c 'exec mysqldump aurora -uaurora -p"{{  
inv_db_aurora_pass }}" > /some/path/on/your/host/aurora_dump.sql'
```

`db-container` - имя контейнера предыдущего релиза. Можно получить, выполнив команду:

```
docker ps --format '{{ .Names }}' | grep mariadb
```

`inv_db_aurora_pass` - переменная в инвентори файла.

5.2.8.2 Схема LDAP:

Для без отказоустойчивой установки:

```
docker exec ldap-container sh -c 'exec ldapsearch -xD '{{ inv_ldap_binddn }}' -w  
'{{ inv_ldap_pass }}' -b '{{ inv_ldap_dn }}' -LLL' >  
/some/path/on/your/host/ldap_backup.ldif
```

Для отказоустойчивой установки необходим дамп схем с одного из серверов роли be и fe:

```
docker exec ldap-fe-container sh -c 'exec ldapsearch -xD '{{ inv_ldap_binddn }}'  
-w '{{ inv_ldap_pass }}' -b '{{ inv_ldap_dn }}' -LLL' >  
/some/path/on/your/host/ldap_backup_fe.ldif
```

```
docker exec ldap-be-container sh -c 'exec ldapsearch -xD '{{ inv_ldap_binddn }}'  
-w '{{ inv_ldap_pass }}' -b '{{ inv_ldap_dn }}' -LLL' >  
/some/path/on/your/host/ldap_backup_be.ldif
```

`ldap-container` , `ldap-fe-container` , `ldap-be-container` - имя контейнера предыдущего релиза. Можно получить, выполнив команду:

```
docker ps --format '{{ .Names }}' | grep ldap
```

`{{ inv_ldap_binddn }}` , `{{ inv_ldap_pass }}` , `{{ inv_ldap_dn }}` - переменные в инвентори файла.

5.2.8.2 Почтовые ящики:

```
tar czf dovecot.tgz /var/dovecot
```

5.3 Обновление «МойОфис Почта»

5.3.1 Конфигурация без отказоустойчивости

5.3.1.1 Запуск обновления

Для запуска обновления подсистемы PSN с релиза **Quassia** необходимо запустить shell-скрипт.

```
./update_fromQuassia.sh <inventory_name> [дополнительные параметры...]
```

Для запуска обновления подсистемы PSN начиная с релиза **2020-01-R2** необходимо запустить shell-скрипт.

```
./update_psn.sh <inventory_name> [дополнительные параметры...]
```

При этом лог-файл процесса развертывания будет сохранен `update_psn_<DATE>.log`.

При успешном выполнении скрипта сервисы подсистемы PSN будут запущены автоматически.

5.3.1.2 Проверка корректности обновления

Проверка аналогична проверке, описанной в п. 4.3.1.2.

5.3.1.3 Миграция данных

База данных

```
docker exec -i mariadb sh -c 'exec mysql -u aurora -p"{{ inv_db_aurora_pass }}" aurora' < /some/path/on/your/host/aurora_dump.sql
```

После восстановления дампа, применить миграции командой:

```
./migrate_db.sh <inventory_name>
```

LDAP

```
docker exec -i ldap sh -c 'exec ldapadd -c -xD '{{ inv_ldap_binddn }}' -w '{{ inv_ldap_pass }}' -f ldap_backup.ldif -v'
```

После восстановления из дампа необходимо единоразово произвести модификацию схемы.

Если модификация была ранее произведена при обновлении на один из предыдущих релизов, начиная с версии 2020.02, то повторный запуск процедуры не требуется.

Для этого необходимо выполнить несколько шагов:

- 1) Выполнить команду для получения всех пользователей в ldap и сохранить вывод в файл

```
ldapsearch -o ldif-wrap=no -x -D "{{ inv_ldap_binddn }}" -w '{{ inv_ldap_pass }}'  
-b "{{ inv_ldap_binddn }}" -s sub -a always -z 1000000 "(mail=*)" "objectClass" |  
grep dn | awk -F ':' '{ print $2 }' | awk '{$1=$1};1' > ldap_user
```

- 2) Произвести добавление поля для каждого пользователя:

```
while read line; do ldapmodify -a -c -x -D "{{ inv_ldap_binddn }}" -w '{{  
inv_ldap_pass }}' -o ldif-wrap=no <<!  
dn: $line  
changetype: modify  
add: objectClass  
objectClass: NCT  
-  
!  
done<ldap_user
```

Почтовые ящики (при необходимости)

```
tar xvf /path/to/dovecot/archive/ -C /
```

5.3.2 Кластерная отказоустойчивая конфигурация

5.3.2.1 Масштабирование конфигурации

5.3.2.1 Запуск обновления

Запуск обновления аналогичен запуску, описанного в п 5.3.1.1.

5.3.2.2 Проверка корректности обновления

Проверка аналогична проверке, описанной в п. 4.3.1.2.

5.3.2.3 Миграция данных

База данных

На любом сервере с ролью db:

```
docker exec -i mariadb sh -c 'exec mysql -u aurora -p"{{ inv_db_aurora_pass }}"  
aurora' < /some/path/on/your/host/aurora_dump.sql
```

После восстановления дампа, применить миграции командой:

```
./migrate_db.sh <inventory_name>
```

LDAP

На одном из серверов с ролью be и fe восстановить соответствующие бэкапы:

```
docker exec ldap- sh -c 'exec ldapadd -c -xD '{{ inv_ldap_binddn }}' -w '{{  
inv_ldap_pass }}' -f ldap_backup.ldif -v'
```

После восстановления из дампа необходимо единоразово произвести модификацию схемы:

Если модификация была ранее произведена при обновлении на один из предыдущих релизов, начиная с версии 2020.02, то повторный запуск процедуры не требуется.

Для этого необходимо выполнить несколько шагов:

- 1) Выполнить команду для получения всех пользователей в ldap и сохранить вывод в файл

```
ldapsearch -o ldif-wrap=no -x -D '{{ inv_ldap_binddn }}' -w '{{ inv_ldap_pass }}'  
-b '{{ inv_ldap_dn }}' -s sub -a always -z 1000000 "(mail=*)" "objectClass" | grep  
dn | awk -F ':' '{ print $2 }' | awk '{$1=$1};1' > ldap_user
```

- 2) Произвести добавление поля для каждого пользователя:

```
while read line; do ldapmodify -a -c -x -D '{{ inv_ldap_binddn }}' -w '{{  
inv_ldap_pass }}' -o ldif-wrap=no <<!  
dn: $line  
changetype: modify  
add: objectClass  
objectClass: NCT  
-  
!  
done<ldap_user
```

Почтовые ящики (при необходимости)

На одном из сервере с ролью be выполнить:

```
tar xvf /path/to/dovecot/archive/ -C /
```


6 Дополнительные возможности и рекомендации по установке

6.1 Варианты запуска установки

Запуск отказоустойчивой и не отказоустойчивой установки на стендах без доступа к интернету производится командой:

```
./deploy_psn.sh <inventory_name> -e hasInternet=false
```

Пропуск этапа настройки системы:

```
./deploy_psn.sh <inventory_name> -e bootstrap=false
```

6.2 Использование AD в продукте «МойОфис Почта»

Настройки для подключения к MS AD.

Для настройки подключения по `imap` и `smtp` необходимо заполнить соответствующие параметры в инвентарном файле. Эти параметры будут использоваться для генерации конфигурации в следующих файлах (путь указан для хостовой системы):

- `/opt/psn/postfix/login_maps.cf` - карта логинов;
- `/opt/psn/postfix/virtual_alias_users.cf`
- `/opt/psn/postfix/virtual_mailbox_maps.cf` - карта для проверки существования почтовых ящиков;
- `/opt/psn/postfix/virtual_mailgroups.cf` - карта для получения конечных почтовых ящиков из групп рассылок;
- `/opt/psn/postfix/virtual_maildomains.cf`
- `/opt/psn/dovecot/dovecot-ldap-pass.conf.ext` - проверка пароля пользователей при логине в IMAP/SMTP
- `/etc/dovecot/dovecot-ldap-user.conf.ext` - получение конфигурации почтового ящика для доставки писем

Настройки адресной книги.

На серверах FE необходимо изменить следующие файлы:

Для работы глобальной адресной книги из AD `/opt/psn/web-client/data/settings/config.php`

:

```
'gcontacts.ldap' => true,  
  
'gcontacts.ldap.host' => 'ldap://dc-01.local',  
  
# Domain Controller name # Domain Controller port # Unique user attribute # DN #  
DN password 'gcontacts.ldap.search-dn' => 'DC=dc-01,DC=local', # Search Base #  
Mail DN # Email field Name  
  
'gcontacts.ldap.port' => 636,  
  
'gcontacts.ldap.uid-field-name' => 'usnCreated',  
  
'gcontacts.ldap.bind-dn' => 'user@local',  
  
'gcontacts.ldap.bind-password' => 'password',  
  
'gcontacts.ldap.main-dn' => 'OU=Users',  
  
'gcontacts.ldap.email-field-name' => 'mail',  
  
'gcontacts.ldap.name-field-name' => 'name',  
  
'gcontacts.ldap.skip-empty-email' => true,  
  
'gcontacts.ldap.contact-object-class' => '*',
```

В файле `/opt/psn/web-client/data/settings/settings.xml`

Строки `<GlobalAddressBookVisibility>Tenantwide</GlobalAddressBookVisibility>`

Заменить на: `<GlobalAddressBookVisibility>Domainwide</GlobalAddressBookVisibility>`

Для корректного получения списка контактов адресной книги из службы каталогов AD, необходимо поменять дефолтные политики LDAP. MS AD должен отдавать целиком весь список контактов, не ограничивая по количеству записей в одном ответе. Значение по умолчанию - 1000. Значение параметра

`MaxPageSize` должно быть больше количества контактов. Для получения подробной информации обратитесь к соответствующему разделу по настройке параметров Active Directory или используемой службы каталогов.

Настройки групп рассылок.

На серверах FE необходимо изменить файл по пути `/opt/psn/web-client/data/config.php` :

```
define("LDAP_HOST", "{{ inv_ldap_server }}");
define("LDAP_DC", "{{ inv_ldap_dn }}");
define("LDAP_LOGIN", "{{ inv_ldap_binddn }}");
define("LDAP_PASSWORD", "{{ inv_ldap_pass }}");
define("LDAP_SEARCH_BASE", "{{ inv_ldap_search_user }}");
define("LDAP_MAILING_GROUP_BASE", "{{ inv_ldap_search_group }}");
define("LDAP_MAILING_GROUP_NAME_FIELD", "cn");
define("LDAP_MAILING_GROUP_EMAIL_FIELD", "mail");
define("LDAP_MAILING_GROUP_EMAILS_FIELD", "alias");
define("LDAP_MAILING_GROUP_TENANT_FIELD", "tenant-id");
```

6.3 Замена сертификатов

На всех нодах с ролями fe, be заменить сертификат и ключ (незащищенный паролем) по соответствующим путям:

```
/etc/pki/tls/<domain>/server.pem
/etc/pki/tls/<domain>/server.key
```

Выполнить подготовку и импорт сертификат для LDAP:

```
#Backup old cert
docker exec ldap sh -c 'pk12util -d /etc/dirsrv/slapd-ldap/ -o olddscert.p12 -n
"server-cert"'
#Prepare cert
docker exec ldap sh -c 'openssl pkcs12 -export -inkey
/etc/pki/tls/<domain>/server.key -in /etc/pki/tls/<domain>/server.pem -out
/tmp/crt.p12 -nodes -name "server-cert" -passout pass:'
#Delete old cert
```

```
docker exec ldap sh -c 'certutil -D -d /etc/dirsrv/slapd-ldap -n "server-cert"  
#Import new cert  
docker exec ldap sh -c 'pk12util -d /etc/dirsrv/slapd-ldap/ -i /tmp/crt.p12 -w ""'
```

Перезапустить сервисы:

```
docker restart ldap  
docker kill -s HUP autoconfig  
docker kill -s HUP psn  
docker kill -s HUP mail
```

6.4 Использование веб-браузера caldav сервера

В целях безопасности рекомендуется не использовать веб-браузер caldav сервера.

Для его отключения необходимо на нодах с ролью **fe**, в файле `/opt/psn/data/settings/config.php` параметр

```
tabs.dav.use-browser-plugin' => true
```

сменить на

```
tabs.dav.use-browser-plugin' => false
```

6.5 Синхронизация аватарок между доменами

Функция позволяет настроить синхронизацию аватарок между разными доменами, при условии одинакового логина.

Например: у вас есть два ящика, один в домене `myoffice.team`, другой в домене `green.myoffice-app.ru`. Установив в одном из них аватар, он автоматически будет отображаться и с другого домена.

Для включения данного функционала необходимо в файле `/opt/psn/web-client/config.php` заменить строчку

```
define("SPECIAL_ACCOUNTS", false);
```

на

```
define("SPECIAL_ACCOUNTS", array("domain1", "domain2"));
```

6.6 Синхронизация пользователей с Битрикс24

Функция позволяет использовать Битрикс24 апи. Для включения функционала необходимо в файле `/opt/psn/pbm/data/config/configs.py` изменить `BITRIX24 = False` на блок:

```
BITRIX24 = True  
BITRIX_URL = ""  
BX_WEBHOOK = ""  
BX_USERID = ""  
BITRIX24_CUSTOM_ATTR_TO_SURNAME = "PERSONAL_ICQ"
```

Необходимые параметры запросить у администратора Битрикс.

7 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.