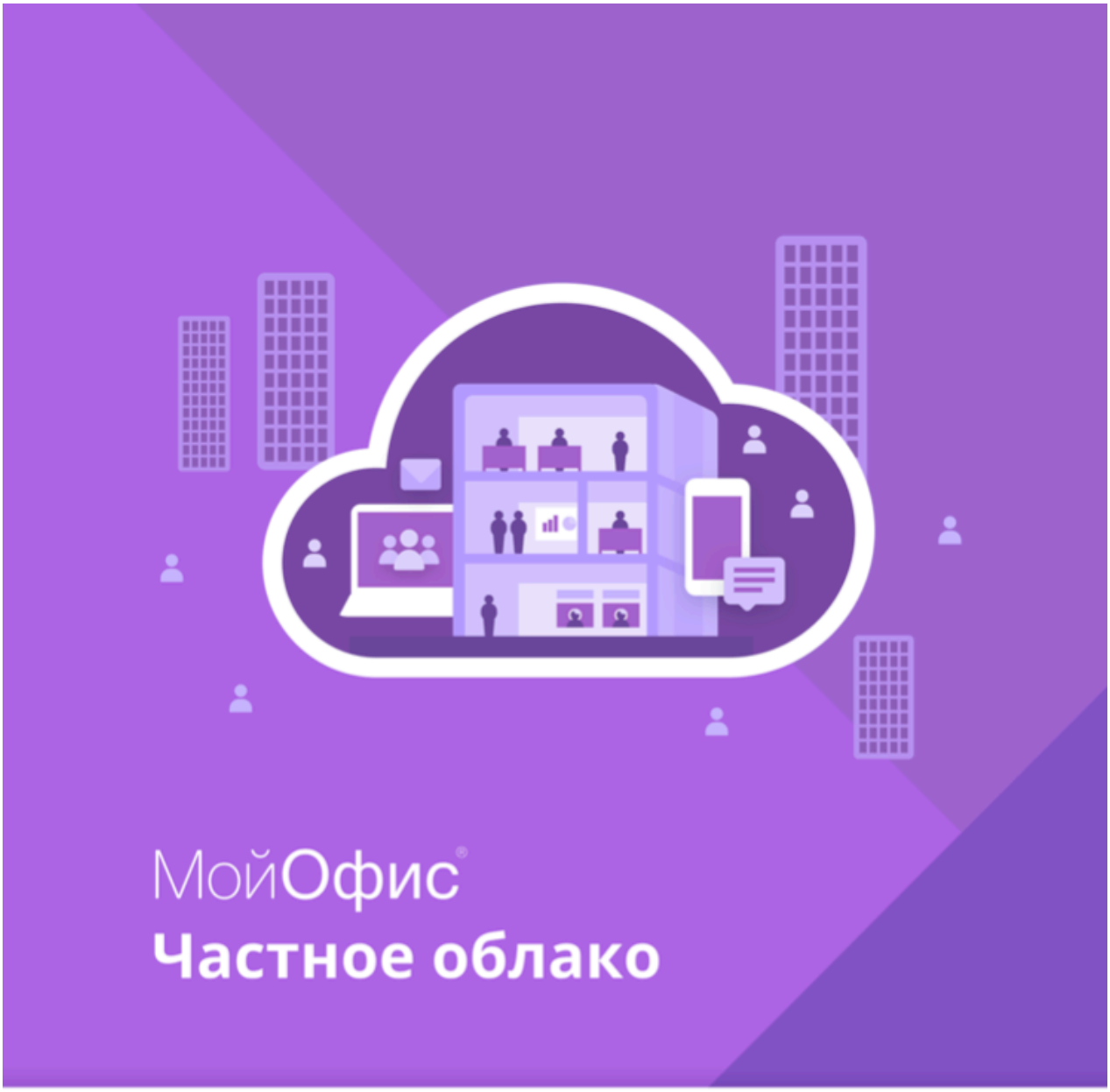

Руководство по установке

МойОфис Почта

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

МойОфис Частное Облако

МойОфис Почта

РУКОВОДСТВО ПО УСТАНОВКЕ

2020.02

На 43 листах

Москва

2020

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.

Перечень сокращений, терминов и оределений

Перечень терминов и определений приведен в таблице 1.

Таблица 1 – 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	Сервер одной из ролей
Плейбук	Сборник скриптов
ОС	операционная система
Докер	Система контейнеризации

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 Аппартные требования

Аппаратные требования приведены в Таблице 2.

Таблица 2. Аппаратные требования

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

- 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 предустанеоывленными пакетами, см.ниже;
- Centos 7.8;
- AstaLinux 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

Рекомендации по разбиению дисков приведенеы в таблице 3.

Таблица 3. Рабиение дисков

Назначение	Точка монтирования	Объем	Группы
ОС	/	50gb	all
БД	/opt/psn/db/data	10% отквоты, выделенной для пользователей	db
Логи	/opt/syslogng-data/logs/	Зависитот 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
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

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.

Таблица 4. Доменные имена

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

где `inv_vip_mail`, `inv_vip_web` - переменные из инвентори файла.

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

Для инсталляции с Облачными Редакторами насерверах PSN внутри контура инсталляции должны корректно разрешаться имена. Доменные имена приведены в таблице 5.

Таблица 5. Доменные имена для инсталляции с Облачными Редакторами

Имя	**Во что разрешать**
fsapi[-env].domain.name	inv_fsapi_vip
mtadmin[-env].domain.name	CNAME fsapi
appapi[-env].domain.name	CNAME fsapi

где `inv_fsapi_vip` - переменная из инвентори файла.

- Для инсталляции МойОфис Хранилище необходимо корректо настроить DNS по инструкции прилагаемой с продуктом, с учетом указаных 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.

Таблица 6. Порты

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

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 обратитесьследующим 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 toWebDAV (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 МойОфисДокументы

Данная схема МойОфис Почта приведена на Рисунке 2.

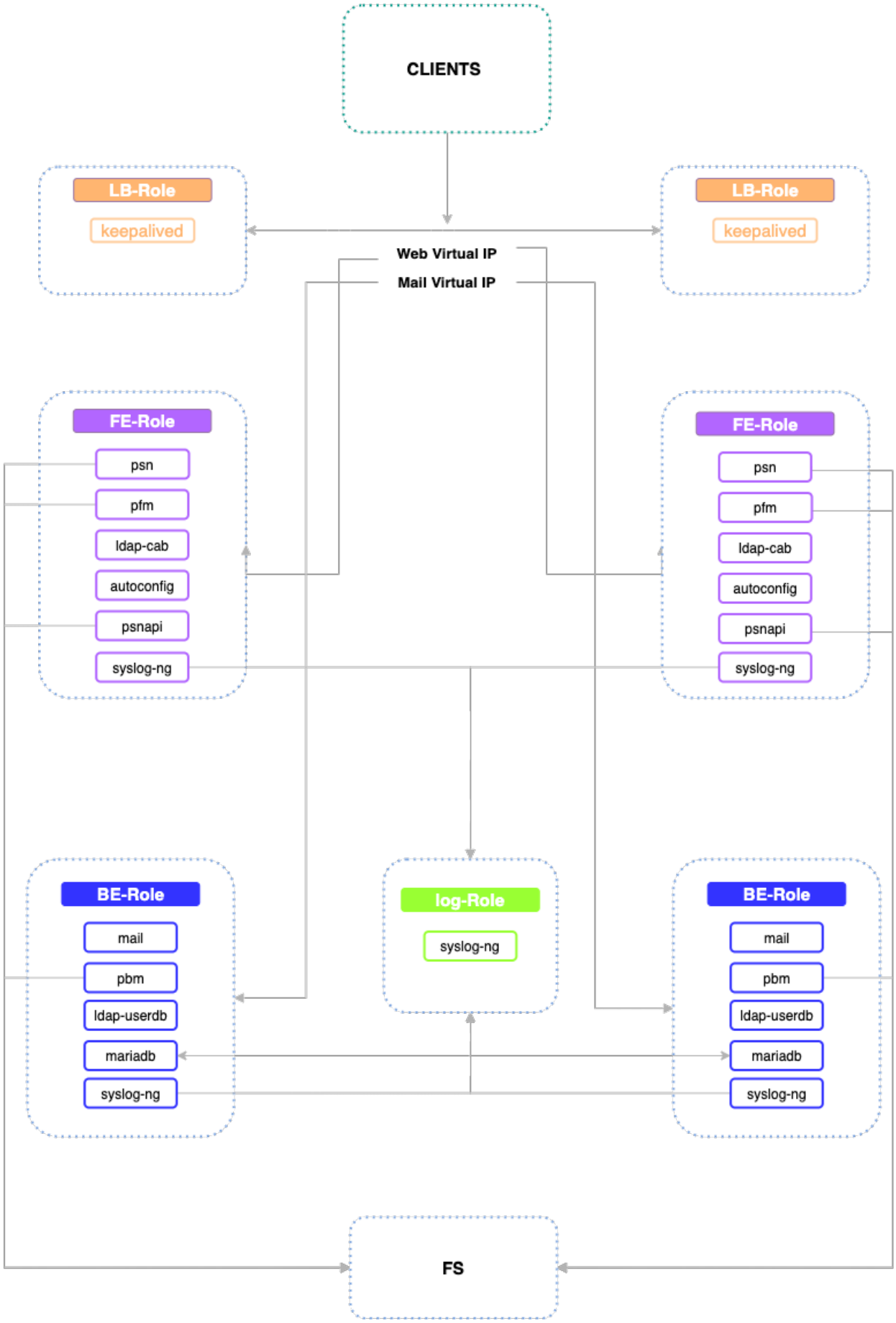

Рисунок 2 – Детальная архитектурная схема МойОфис Почта

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 (рекомендуеммое) 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;
- Набор необходимых пакетов для установки в закрытом контуре;
- 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.

Таблица 7. Роли

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		
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		
psnapi	fe	Роль установки и настройки psnapi сервиса		
registry	registry	Роль настройки локального докер репозитория		
webclient	fe	Роль установки веб-клиента		2
fe	fe	Вспомогательная роль для установки веб-клиента		

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 ≥ 2.9
    - Jinja2 ≥ 2.10
4. Заполнить инвентори файл на основании входящих в состав дистрибутивов примеры, находящимся по пути: **inventory/standalone.example** (в случе установки без отказоустойчивости) или **inventory/cluster.example** (в случае установки с отказоустойчиаостью)

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.

Таблица 8. VIP.

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

4.2.3.2 Конфигурационные параметры

Параметры приведены в таблице 9

Таблица 9. Конфигурационные параметры

Переменная	Назначение	Значение по умолчанию	Комментарии
standalone	Выбор типа инсталяции: кластер или однонодовая	false	Если производится инсталяция на один сервер изменить, значение на true
inv_domain_fqdn	доменное имя инсталляции в формате FQDN	example.com	---
inv_env	используемое окружение для инсталляции	не задается	добавляет постфикск именам, напр. mail становится mail-env, а почтовый домен env.inv_domain_fqdn
inv_url_prefix	префикс доменного имени, используемый для веб-клиента	mail	определяет адрес используемый для webклиента, отступает на уровень выше от inv_domain_fqdn, напр. mail.example.com
inv_quota_size	рзамер квоты почтового ящико 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)

4.2.3.3 Пароли

Параметры приведены в таблице 10.

Таблица 10. Пароли

Переменная	Назначение	Политика безопасности
inv_lb_keepalived_pass	пароль для взаимодействия LB-нод, используется не более 8 символов	
inv_db_aurora_pass	пароль для доступа к БД веб-клиента	+
inv_db_mysql_root_pass	пароль суперпользователя для доступа к БД	+
inv_be_dovecot_admin_pass	пароль для синхронизации данных между MDA	
inv_users_pass	после инсталляции создается два почтовых ящика test@[env.]inv_domain_fqdn и postmaster@[env.]inv_domain_fqdn, с указанным паролем	
inv_db_aurora_password_key	ключ шифрования пароля в БД	+

4.2.3.4 Параметры LDAP

Параметры приведены в таблице 11.

Таблица 11. Параметры LDAP

Переменная	Назначение	Пример	Комментарии
inv_ldap_msad	переключение на использование Microsoft Active Directory	false	по умолчанию используется false (Внутренняя служба каталогов)
inv_ldap_server	адрес для доступа к серверу службы каталогов	{{ inv_vip_userdb }}	по умолчанию используется inv_vip_userdb
inv_ldap_dn	distinguished name	dc=test,dc=ru	
inv_ldap_binddn	учетная запись для подключения по протоколу LDAP к службе каталогов	cn=Manager, {{inv_ldap_dn}}	требует изменений только в случае использования внешней службы каталогов
inv_ldap_pass	пароль в открытом виде для учетной записи inv_ldap_binddn		
inv_ldap_search_user	organizational unit для хранения данных по учетным записям пользователей	OU=People, {{inv_ldap_dn}}	обычно не требует изменений
inv_ldap_search_group	organizational unit для хранения данных по группам рассылок	OU=Groups, {{inv_ldap_dn}}	обычно не требует изменений
inv_ldap_search_cab	organizational unit для хранения данных адресной книги	OU=CAB, {{inv_ldap_dn}} или OU=CAB,ou=default, {{inv_ldap_dn}}	В случае инсталляции с переменной `inv_fs_integration=false` , переменная `inv_ldap_search_cab` должна иметь знчение `OU=CAB,ou=default,{{inv_ldap_dn}}` , если `inv_fs_integration=true` , следует выставить `inv_ldap_search_cab: OU=CAB,{{inv_ldap_dn}}`

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 (~/installpsn/certificates/inv_domain_fqdn/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

Параметры приведены в таблице 12.

Таблица 12. Прочие параметры

Переменная	Назначение	Значение по умолчанию	Комментарии
inv_virtual_domains	дополнительные почтовые домены, используемые для получения писем	по умолчанию не определена, необходимо раскомментировать для использования	значения указываются через запятую 'domain.ru, domain2.ru'
inv_be_rsmapd_dkim_selector	селектор для использования DKIMподписи	mail	
inv_postfix_trusted_networks	Доверенные сети для получения почтовых сообщений.		IP адреса разделенные запятой. Текущую сеть в параметре не размещается
docker_network	Задает докерную сеть.	172.17.0.0/16	
docker_bip	Задает ip адрес бридж-интерфейса докера.	172.17.0.1/16	

4.2.4.2 Интеграции с облачными редакторами

Параметры приведены в таблице 13.

Таблица 13. Интеграции с облачными редакторами

Переменная	Назначение	Значение по умолчанию	Комментарии
inv_fs_integration	подключение к МойОфис Хранилище (true/false)	false (интеграция отключена)	используется для определения интеграции с облачными редакторами
inv_fs_tenant_replication	копирование тенантной структуры в PSN (true/false)	false (копирование отключено)	используется для копирования сертификатов и почтовых доменов тенантов заведенных в FS
fs_legacy	Для итеграции с FS релиза Mint	false	Если FS новее версии Mint значение не менять
inv_fsapi_vip	адрес виртуального IP FS-API	any_ip_addr	указывается в случае с инсталляции с облачными редакторами, задается во

			время инсталляции FS
inv_fsdb_vip	адрес виртуального IP FS-DB	any_ip_addr	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
inv_fsdb_port	порт виртуального IP FS-DB	25432	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
vmail_db_name	имя базы данных vmail в FS	fs	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
vmail_db_user	имя пользователя имеющего доступ на чтение из базы vmail в FS	{{ vmail_db_name }}	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
vmail_db_pass	пароль пользователя имеющего доступ на чтение из базы vmail в FS	false	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
inv_fs_mtadmin_login	логин для подключения MTADMIN-API	mtadminapi_user	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
inv_fs_mtadmin_pass	Дпароль для подключения MTADMINAPI	mtadminapi_pass	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
FS_APP_USER	Пользователь для доступа к Fs APP API	app-co	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
FS_APP_ENC_PASSWORD	параметры шифрования		указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции CO
COMMON_ENCRYPTION_KEY	параметры шифрования		указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции CO
COMMON_ENCRYPTION_IV	параметры шифрования		указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции CO
FS_APP_ENCRYPTION_KEY	параметры		указывается в случае с инсталляции с облачными

	шифрования		редакторами, задается во время инсталляции FS
FS_APP_ENCRYPTION_IV	параметры шифрования		указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS

4.2.5 Настройка межсетевого экранирования

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

Таблица 14 – Описание портов, доступ к которым необходимо обеспечить

Номер порта	Связанный IP	Назначение
80	0.0.0.0	http
443	0.0.0.0	https
444	0.0.0.0	autoconfig-https
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

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 строчку `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 7.8** выставить значение `interpreter_python = /usr/bin/python` в файле **ansible.cfg**

Для запуска инсталляции подсистемы PSN необходимо запустить shell-скрипт.

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

При этом лог-файл процесса развертывания будет сохранен `deploy_psn_$DATE.log`.

При успешном выполнении скрипта сервисы подсистемы PSN будут запущены автоматически.

После установки, применить миграции 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 тестовове 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 создалось;
- Зайти в настройки, изменить любые параметры и убедиться, что настройки сохранены;
- В случае установки с интеграцией с FS проверить работу синхронизации:

  - Команда `curl -X POST https://pbm-DOMAIN_ENV.DOMAIN_NAME:48666/actions?cmd=domainsync` должна возвращать `true`;

  - Команда `curl -X POST https://pbm-DOMAIN_ENV.DOMAIN_NAME:48666/actions?cmd=tennantsync` должна возвращать `true`;

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 Мой Офис 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.

Для миграции данных необходимо сделать резервные копии трех сущностей:

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

> Важно! Не производить обновление без наличия свежих бэкапов

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 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:

Для этого необходимо выполнить несколько шагов:

1) Выполнить команду для получения всех пользователе в лдап и сохранить вывод в файл

```
ldapsearch -o ldif-wrap=no -x -D "{{ inv_ldap_binddn }}" -w '{{ inv_ldap_pass }}' -b "dc=green.myoffice-app,dc=ru" -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 серврее 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:

Для этого необходимо выполнить несколько шагов:

1) Выполнить команду для получения всех пользователе в лдап 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 сторонней службы каталогов в продукте МойОфис Почта

В этом случае параметры в разделе инвентарного файла будут использованы в качестве конфигурации для подключения к службе каталогов. Так же необходимо учитывать, что с этими параметрами дополнительно будет создана новая конфигурация службы LDAP встроенной в МойОфис Почта. Т.к. адресная книга (CAB) использует службу каталогов для хранения контактов. Для корректной интеграции с внешними службами каталогов потребуется внести изменения для учетных записей пользователей и добавить атрибуты maildrop и alias (атрибут должен поддерживать множественные значения). Данный атрибут используется для определения финального адреса доставки в группах рассылки. (см. подробнее http://www.postfix.org/LDAP_README.html#example_group)

Для настройки конфигурации с существующими службами каталогов может потребоваться точная настройка запросов для получения корректных данных. Это можно сделать уже после завершения инсталляции на нодах роли BE. Запросы настраиваются в файлах:

/etc/postfix/login_maps.cf - карта логинов;
/etc/postfix/virtual_alias_users.cf -

карта для проверки дополнительных адресов почтовых ящиков;
/etc/postfix/virtual_mailbox_maps.cf - карта для проверки существования почтовых ящиков; /etc/postfix/virtual_mailgroups.cf - карта для получения конечных почтовых ящиков из групп рассылок; /etc/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.

Например, для фала /etc/dovecot/dovecot-ldap-pass.conf.ext запрос к службе каталогов происходит с использованием поля mail. mail=%u где mail - атрибут в службе каталогов, а %u - полное имя пользователя user@domain В запросе можно переопределить как атрибут, так и передаваемое значение. Возможные варианты:

Переменная	Назначение	Комментарии
%u	полное имя пользователя user@domain	user@domain
%n	часть имени пользователя до @	user

Настройки для подключения к MS AD или другим сторонним службам каталогов.

Настройка интеграции с MS AD производится уже после завершения инсталляции стенда. В приведенных ниже файлах необходимо поменять поля, отмеченные комментарием.

На серверах PBE необходимо изменить следующие файлы:

`/etc/dovecot/dovecot-ldap-user.conf.ext`

```
hosts auth_bind dn dnpass base scope deref ldap_version

pass_attrs user_attrs

= dc-01.local dc-02.local = yes # Auth bind = user@local # DN =
password # DN password = OU=Users,DC=dc-01,dc=local = subtree #
Scope = never = 3

= uid=user,userPassword=password = \

# Domain Controller name

# Search Base =quota_rule=*:storage=%{ldap:mailQuota:500M}, \
=uid=vmail, \ =gid=vmail, \ =home=/var/dovecot/%d/%n iterate_attrs
= \ =user=%{ldap:mail}

# Quota

user_filter = (&(memberOf=CN=MyOffice,OU=MyOffice,DC=dc-
01,DC=local) (mail=%u)) # User search filter pass_filter = (&
(memberOf=CN=MyOffice,OU=MyOffice,DC=dc-01,DC=local) (mail=%u)) #
Password search filter iterate_filter = (mail=*) # Iterate
attribute
```

```
default_pass_scheme = PLAIN
```

`/etc/dovecot/dovecot-ldap-pass.conf.ext :`

```
hosts Controller name auth_bind dn dnpass base scope deref
ldap_version

= dc-01.local dc-02.local

= yes = user@local = password = OU=Users,DC=dc-01,dc=local =
subtree = never = 3

# Domain

# Auth bind # DN # DN password # Search Base # Scope

pass_attrs = uid=user,userPassword=password iterate_attrs = \
=user=%{ldap:mail}

user_filter = (&(memberOf=CN=MyOffice,OU=MyOffice,DC=dc-
01,DC=local) (mail=%u)) # User search filter pass_filter = (&
(memberOf=CN=MyOffice,OU=MyOffice,DC=dc-01,DC=local) (mail=%u)) #
Password search filter iterate_filter = (mail=*) # Iterate
attribute

default_pass_scheme = PLAIN

/etc/postfix/virtual_mailbox_maps.cf : server_host = dc-01.local #
Domain Controller name bind = yes # Auth bind bind_dn = user@local
# DN bind_pw = password # DN password version = 3 search_base =
OU=Users,DC=dc-01,dc=local # Search Base scope = sub query_filter =
(mail=%s) result_attribute = mail debuglevel = 0
```

На серверах PFE необходимо изменить следующие файлы:

Для работы глобальной адресной книги из AD

`/opt/psn/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/data/settings/settings.xml`

Строку:

`<GlobalAddressBookVisibility>TenantWide</GlobalAddressBookVisibili ty>`

Заменить на:

`<GlobalAddressBookVisibility>DomainWide</GlobalAddressBookVisibili ty>`

Адресная книга MS AD

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.

6.3 Замена сертификатов

На всех нодах с роялми 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 сертификта 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 бразуер caldav сервера.

Для его отключения необходимо на нодах с ролью **fe**, в файле `/opt/psn/data/settings/config.php` параметр `labs.dav.use-browser-plugin' => true` сменить на `labs.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.myoffce-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, неописанных в данном руководстве:

Адрес электронной почты: support@service.myoffice.ru

Телефон: 8-800-222-1-888.