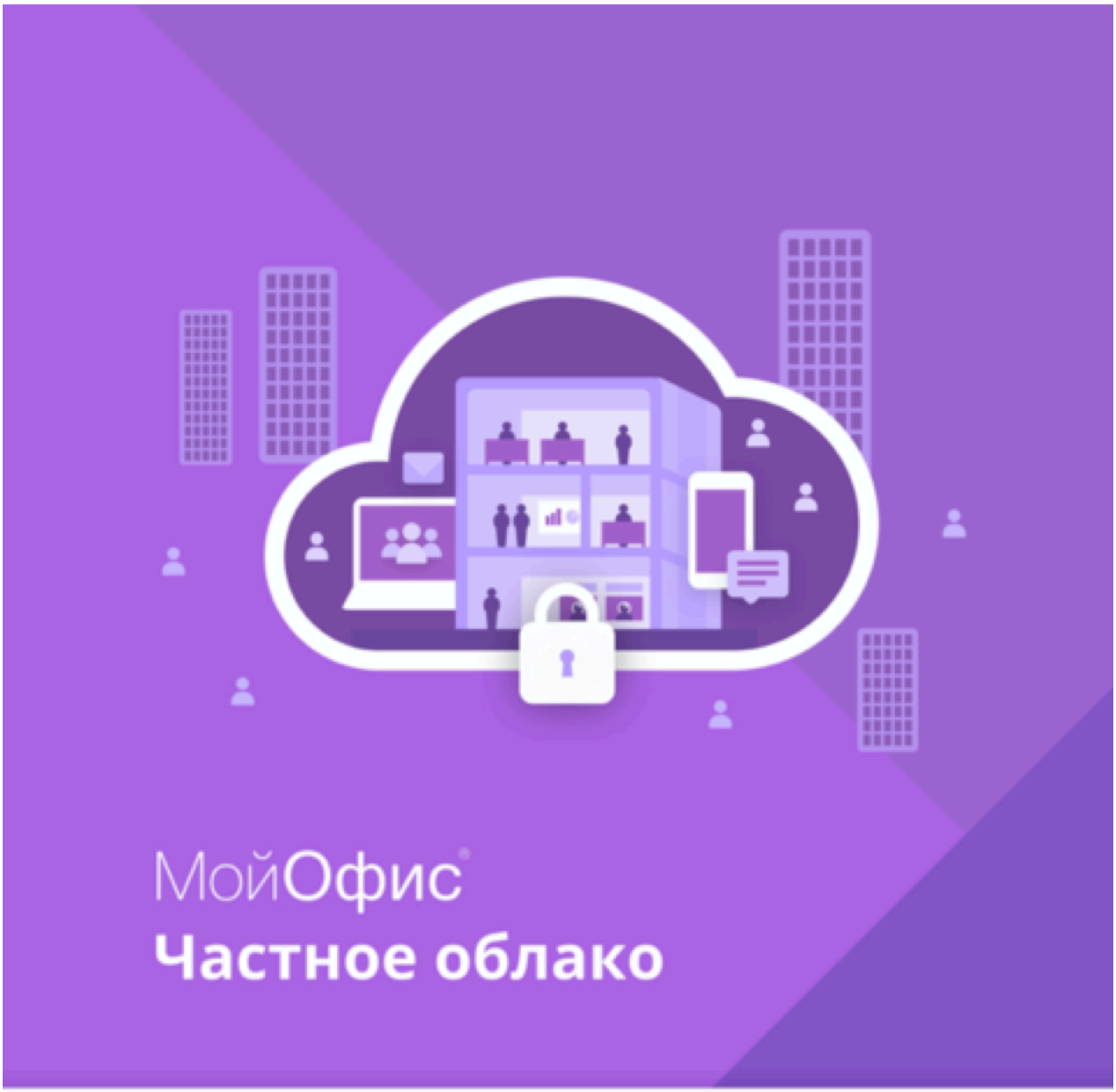

МойОфис®

Частное облако

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

МойОфис Частное Облако

МойОфис Почта

РУКОВОДСТВО ПО УСТАНОВКЕ

2019.03

Москва

2019

Оглавление

Термины и сокращения

-	**Пояснение**
API	Application programming interface, интерфейс программирования приложений
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

Системные требования

1. Требования к инфраструктуре

1.1. 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.

1.2. Конфигурация без отказоустойчивости

-	CPU	RAM(Gb)	HDD(Gb)
минимальная[1]	4	8	50 + Квота пользователей на использование дискового пространства[2]
рекомендованная	8	16	100 + Квота пользователей на использование дискового пространства[2] + База данных[2]

1. Данная конфигурация может быть использована только для функционального тестирования.

2. Рекомендуестя использовать отдельные разделы или диски (подробнее см. р.1.5.).

- Скорость сетевой подсистемы — 1Gbit/s или выше;
- Должен быть установлен один из поддерживаемых дистрибутивов операционной системы.

1.3. Отказоустойчивая конфигурация

-	CPU	RAM(Gb)	HDD(Gb)
минимальная[1]	4	8	50 + Квота пользователей на использование дискового пространства[2]
рекомендованная	8	16	100 + Квота пользователей на использование дискового пространства[2] + База данных[2]

1. Данная конфигурация может быть использована только для функционального тестирования.

2. Рекомендуестя использовать отдельные разделы или диски.

- Скорость сетевой подсистемы — 1Gbit/s или выше;
- Должен быть установлен один из поддерживаемых дистрибутивов операционной системы;
- Должны использоваться 6 или более виртуальных машин. Дополнительная информация о возможных конфигурациях инсталляции в разделе 4.1.1 Роли.

1.4. Операционная система

Поддерживаются следующие дистрибутивы:

- **CentOS 7.5 minimal install** (рекомендуемый дистрибутив);
- Scientific Linux 7.5 minimal install;
- RHEL 7.5 minimal install. Операционная система устанавливается отдельно на каждый физический сервер или виртуальную машину.

1.5. Разбиение дисков

Для серверов рекомендуется использовать отдельные блочные устройства и точки монтирования:

Назначение	Точка монтирования (по умолчанию)	Объем	Группы
диск для ОС	/	50Gb	all
Квота почтовых ящиков пользователей	/var/dovecot	суммарный объем квот пользователей + 20%	mda
БД	/var/lib/mysql-cluster/data	10% от квоты, выделенной для пользователей	db-ad db-mgm
Логи	/var/log	Зависит от объема и сроков хранения информации	all
Аттачи к событиям при кластерной конфигурации	/data/glusterfs/eattach/	Зависит от объема аттачей к событиям	web-client
Аттачи к событиям при бескластерной конфигурации	/opt/psn/eattach/	Зависит от объема аттачей к событиям	web-client

1.6. Настройка NTP

Для корректной работы МойОфис почта необходимо настроить службу синхронизации времени на серверах.

1.7. Инсталляция PSN в составе продуктов МойОфис Частное облако или МойОфис Почта

1.7.1. В случае установки PSN в составе продукта МойОфис Частное облако:

Требуется провести необходимые настройки в конфигурационном файле. За данную конфигурацию отвечает переменная **inv_fs_integration**, которая должна быть выставленна в значение **"true"**. (Подробнее об этом в разделах **4. Настройка инсталляции** и **5. Дополнительные настройки FS для работы с PSN**) Продукты *МойОфис Хранилище* и *МойОфис Облачные Редакторы* должны быть проинсталлированы до начала инсталляции *МойОфис Почта*. Для совместной работы продуктов необходимо чтобы на серверах PSN корректно разрешались доменные имена:

- **fsapi**[-env].domain.name
- **mtadmin**[-env].domain.name
- **appapi**[-env].domain.name
- **cardapi**[-env].domain.name

Внутри контура инсталляции доменные имена должны разрешаться во внутренние IP адреса.

1.7.2. В случае установки PSN в составе продукта МойОфис Почта:

Требуется провести необходимые настройки в конфигурационном файле. За данную конфигурацию отвечает переменная **inv_fs_integration** - достаточно выставить её значение в **false** и **пропустить** раздел 5 "Дополнительные настройки FS для работы с PSN".

1.8. Инфраструктурная машина

Для удобства инсталляции и контроля конфигурации рекомендуется использование выделенного сервера для проведения инсталляции - инфраструктурной машины. 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.

2. Установка и настройка ОС

1. Для инсталляции ОС рекомендуется использовать **минимальный** вариант установки ОС рекомендуемой версии (см. п.1.4);
2. Отключить автоматическое обновление пакетов системы (например, удалением **yum-cron**);
3. Перевести **SELinux** в состояние Disabled;
4. 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.

2.1. Рекомендуемый план имен и IP адресов для отказоустойчивой инсталляции:

Нода	ip address[1]
plog1	10.10.10.200
plb1	10.10.10.201
plb2	10.10.10.202
pbe1	10.10.10.203
pbe2	10.10.10.204
pfe1	10.10.10.205
pfe2	10.10.10.206

1. Первые три октета произвольны и могут использоваться любые.

Возможна инсталляция с выделением отдельных групп для некоторых ролей, подробнее см. р. 4.1.1 Роли. При инсталляции с выделением ролей на отдельные сервера рекомендуется продолжать нумерацию в возрастающем порядке. Приоритет для ролей следующий: db-ad, userdb, cab.

2.2. Рекомендуемый план имен и IP адресов для инсталляции без отказоустойчивости

Нода	**ip address**
для инсталляции	**на один сервер**
psnsa	10.10.10.201
для инсталляции	**на два сервера**
psnsabe	10.10.10.201
psnsafe	10.10.10.202

2.3. 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.

2.4. Таблица NAT для портов

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

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

2.5. Настройка DNS

На всех серверах *МойОфис Почта* настроить DNS, который будет корректно разрешать имена системы в приватные IP адреса:

2.6. Доменные имена

Доменное имя	ip address cluster	ip address SA	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 mda	
{{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
push[-env].*domain.name*	inv_vip_web	IP адрес fe	используется только при использовании push-уведомлений
smtp[-env].*domain.name*	inv_vip_mail	IP адрес be	
pbm[-env].*domain.name*	inv_vip_mail	IP адрес be	

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

2.7. Ресурсные записи для функционирования почты

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)

Для инсталляции с *Облачными Редакторами* на серверах PSN внутри контура инсталляции должны корректно разрешаться имена:

Доменное имя	**Во что разрешать**
fsapi[-env].*domain.name*	IP адрес FS части задаваемый переменной vip_web в Puppet
mtadmin[-env].*domain.name*	cname для fsapi
appapi[-env].*domain.name*	cname для fsapi

- 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)

3. Подготовка инсталляции PSN

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.md5
```

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

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

Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

3. Установить на сервер необходимые пакеты:

- ansible ≥ 2.6.2.0
- rsync

Все необходимые пакеты, зависимости и дополнительные модули можно установить командой:

```
yum localinstall files/repo/7.5/ansible/* files/repo/7.5/rsync*
```

4. Настройка инсталляции

4.1. Настройка параметров

Настройка параметров производится в файле install_cluster или install_sa в директории `inventory`. Для определения инсталляции с отказоустойчивостью или без, используйте соответствующие инвентори файлы-шаблоны.

4.1.1. Роли

Инвентарный файл (inventory file) содержит логические группы (роли), на которые будет разделен кластер инсталляции. Роли могут совмещаться, то есть на одном и том же сервере (виртуальной машине) может быть развернуто несколько ролей, работающих одновременно. При этом необходимо учитывать ограничения на совмещения ролей. В отказоустойчивой конфигурации не рекомендуется совмещать на одном сервере роли:

- DB (ACCESS) + DB(MGMT);
- DB (DATA) + DB(MGMT);м* CAB + USERDB;
- LOG + any other.

Роль	Группа хостов	Привязка ролей	Описание	Комментарий	Максимальное количество серверов
lb	lb	-	Подсистема балансировки нагрузки	-	2
mta	be	-	Почтовая подсистема, контент фильтр	-	3
mda	mda	по умолчанию с be	MDA	-	2
fe	fe	-	Веб-клиент	-	2
web-client	fe	только с fe	Веб-клиент	-	2
ldap	userdb	по умолчанию с be	Служба каталогов	не поддерживается смена количества нод после первичной инсталляции	3
ldap	cab	по умолчанию с fe	Служба каталогов	не поддерживается смена количества нод после первичной инсталляции	3
log	log	-	Агрегатор логов	Всегда устанавливается отдельно от других ролей	1
ac	ac	только с fe	Автоконфигуратор для десктопного клиента	-	2
db-mgm	db-mgm	по умолчанию с fe	Роль управления кластером БД	-	2
db-ad	db-ad	по умолчанию с be	Совмещенная роль доступа и хранения к данным ДБ	-	3
push	push	только с fe,be	Push-уведомления для IOS приложения	Не устанавливается, если используется icshandler	2
icshandler	icshandler	только с fe,be	Сервис обработки ICS	Не устанавливается, если используется push	2

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

```
[log]
10.10.10.200
```

4.1.1.1. Конфигурация без отказоустойчивости

! Для инсталляции с отказоустойчивостью обратитесь к р. 4.1.1.2 Инсталляция производится с использованием одного или нескольких серверов. Для этого в инвентарном файле install_sa необходимо указать правильные IP адреса серверов. В случае инсталляции на один сервер IP адреса должны быть одинаковые для каждой роли.

```
[be]
10.10.10.201

[fe]
10.10.10.202
```

Конфигурация без отказоустойчивости не поддерживает использование выделенного сервера для агрегации логов. Далее можно переходить к р. 4.1.2. Основные параметры инсталляции.

4.1.1.2. Отказоустойчивая конфигурация

Рекомендуется использовать не менее 6 серверов для инсталляции отказоустойчивой конфигурации. Для этого в инвентарном файле необходимо указать правильные IP адреса серверов:

```
[log]
10.10.10.200

[lb]
10.10.10.201
10.10.10.202

[be]
10.10.10.203
10.10.10.204

[fe]
10.10.10.205
10.10.10.206
```

Инсталляция проводится на определенное количество серверов в каждой группе, дополнительная информация в р. 4.1.1. Роли.

Роль LOG является опциональной, если ее необходимо исключить - оставьте секцию [log] пустой. Для использования роли LOG, укажите корректный IP адрес сервера (в инсталляции поддерживается только один сервер для роли log).

По умолчанию ноды роли db-mgm, db-ad, userdb, cab, mda наследуют IP адреса ролей be или fe:

```
#db Access and Data roles combined
[db-ad:children]
be

#db management role
[db-mgm:children]
fe

[mda:children]
be

[cab:children]
fe
```

```
[userdb:children]
be
```

При необходимости можно переопределить IP адреса для данных ролей и установить их на отдельные сервера, например:

```
[db-ad]
10.10.10.207
10.10.10.208
```

В качестве виртуальных адресов необходимо указать IP адреса, не задействованные в текущей сети. Или использовать ранее назначенные VIP(в случае обновления инсталляции). Виртуальные IP адреса будут автоматически настроены на интерфейсе master-ноды балансировщика:

```
inv_vip_mail=10.10.10.220
inv_vip_web=10.10.10.221
```

ВАЖНО Во время первичной инсталляции VIP адрес не должен использоваться в контуре инсталляции.

4.1.2. Основные параметры инсталляции

4.1.2.1. VIP адреса

VIP адрес - совместно используемый адрес для распределения нагрузки между нодами и обеспечения отказоустойчивости. Дополнительная информация по настройке VIP адреса описана в разделах 4.1.1.1 и 4.1.1.2

переменная	назначение	комментарий
inv_vip_*	Виртуальный адрес для доступа к серверам	новый IP адрес не задействованный в сегменте сети

4.1.2.2. Конфигурационные параметры

Переменная	Назначение	Значение по умолчанию	Комментарий
inv_bootstrap	подготовка системы к установке	true	желательно использовать значение true для обеспечения корректных параметров среды инсталляции
inv_domain_fqdn	доменное имя инсталляции в формате FQDN	example.com	напр. example.com
inv_env	используемое окружение для инсталляции	не задается	добавляет постфикс к именам, напр. mail становится mail-env, а почтовый домен env.inv_domain_fqdn
inv_url_prefix	префикс доменного имени, используемый	mail	определяет адрес используемый для web-клиента, отступает на уровень выше от

	для веб-клиента		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)
repo_ip	адрес указывающий на репозиторий инсталляции	не используется	по умолчанию не используется, необходим для указания произвольного репозитория установки пакетов продукта
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
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	5432	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
vmail_db_name	имя базы данных vmail в FS	vmail_box	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	-	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	пароль для подключения MTADMIN-API	mtadminapi_pass	указывается в случае с инсталляции с облачными редакторами, задается во время инсталляции FS
FS_APP_ENC_PASSWORD	параметры шифрования	-	переменные параметров шифрования используются только для инсталляции с Облачными Редакторами.
FS_APP_ENCRYPTION_KEY	параметры шифрования	-	параметры задаются и настраиваются во время установки СО.
FS_APP_ENCRYPTION_IV	параметры шифрования	-	(Для получения подробной информации обратитесь к "5.16. Настройка ключей шифрования" в инструкции по установке Облачных Редакторов).
COMMON_ENCRYPTION_KEY	параметры шифрования	-	для установки только МойОфис Почта не заполняйте значения переменных или удалите их из инвентарного файла
COMMON_ENCRYPTION_IV	параметры шифрования	-	-

4.1.2.3. Пароли

Для паролей, отмеченных в графе "политика безопасности", действует политика - длина не менее 8 символов, наличие цифр, букв в верхнем и нижнем регистре, не менее одного спецсимвола (допустимые спецсимволы !@#$%?()_). В целях безопасности рекомендуется использовать подобную политику для всех задаваемых паролей.

Переменная	Назначение	Политика безопасности
inv_lb_keepalived_pass	пароль для взаимодействия LB-нод, используется не более 8 символов	
inv_db_amavis_pass	пароль для доступа к БД системы проверки контент а почтовых сообщений	+
inv_db_aurora_pass	пароль для доступа к БД веб-клиента	+
inv_db_mysql_root_pass	пароль суперпользователя для доступа к БД	+
inv_admin_pass	пароль для доступа к дополнительным сервисам инсталляции	
inv_dovecot_admin_pass	пароль для синхронизации данных между MDA	
inv_hapass	пароль для доступа к веб интерфейсу подсистемы балансировки нагрузки	
inv_users_pass	после инсталляции создается два почтовых ящика test@[env.]inv_domain_fqdn и postmaster@[env.]inv_domain_fqdn, с указанным паролем.[1]	

1. Автоматически не создается в инсталляции без отказоустойчивости.

4.1.3. LDAP

Для настройки взаимодействия со службой каталогов потребуется внести изменения в раздел инвентарного файла LDAP config section. Этому разделу требуется уделить особое внимание. Возможны два варианта установки: с уже используемой службой каталогов или с использованием встроенной в продукт МойОфис Почта.

4.1.3.1. Использование встроенной службы каталогов в продукте МойОфис Почта.

В этом случае параметры, в разделе инвентарного файла, будут использованы в качестве конфигурации для настройки службы каталогов. С этими параметрами будет создана новая конфигурация.

переменная	назначение	пример	комментарий
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_dc	domain component	test	
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}}`

4.1.3.2. 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	комментарий
%u	полное имя пользователя user@domain	user@domain
%n	часть имени пользователя до @	user

4.1.3.3. 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           = dc-01.local dc-02.local         # Domain Controller name
auth_bind       = yes             # Auth bind
dn              = user@local            # DN
dnpass          = password            # DN password
base            = OU=Users,DC=dc-01,dc=local          # Search Base
scope           = subtree           # Scope
deref           = never
ldap_version    = 3

pass_attrs      = uid=user,userPassword=password
user_attrs      = \
```

```
=quota_rule=*:storage=%{ldap:mailQuota:500M}, \       # Quota
=uid=vmail, \
=gid=vmail, \
=home=/var/dovecot/%d/%n
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/dovecot/dovecot-ldap-pass.conf.ext`:

```
hosts           = dc-01.local dc-02.local                           # Domain
Controller name
auth_bind       = yes                                               # Auth bind
dn              = user@local                                        # DN
dnpass          = password                                          # DN password
base            = OU=Users,DC=dc-01,dc=local                        # Search Base
scope           = subtree                                           # Scope
deref           = never
ldap_version    = 3

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
  'gcontacts.ldap.port' => 636,         # Domain Controller port
  'gcontacts.ldap.uid-field-name' => 'uSNCreated',    # Unique user attribute
  'gcontacts.ldap.bind-dn' => 'user@local',     # DN
  'gcontacts.ldap.bind-password' => 'password',     # DN password
  'gcontacts.ldap.search-dn' => 'DC=dc-01,DC=local',  # Search Base
  'gcontacts.ldap.main-dn' => 'OU=Users',     # Mail DN
  'gcontacts.ldap.email-field-name' => 'mail',      # Email field Name
  '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</GlobalAddressBookVisibility>
```

Заменить на:

```
<GlobalAddressBookVisibility>DomainWide</GlobalAddressBookVisibility>
```

4.1.3.4 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.

4.1.4. 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-psn/certificates` вложенную директорию dkim (`~/install-psn/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.

По умолчанию DKIM создается только для основного домена инсталляции, при необходимости можно добавить конфигурацию по дополнительным доменам. Конфигурация производится в конфигурационном файле

- amavisd-new `/etc/amavisd/amavisd.conf`

Для замены или обновления сертификатов и ключей цифровой подписи DKIM, предусмотрен тег позволяющий запустить только задачи связанные с сертификатами. Подробнее в 4.2.1 Замена сертификатов

4.1.5. Настройка PUSH-уведомлений для ios

По умолчанию переменные для настройки push-уведомлений не указаны в инвентарном файле. Добавьте в файл переменные и укажите их значения:

переменная	назначение	комментарий
inv_push_key	имя файла в ~/install-psn/certificates/inv_domain_fqdn/	имя файла приватного ключа для подключения к сервисам Apple
inv_push_key_id	key_id	идентификатор key_id для подключения к сервисам Apple
inv_push_team_id	team_id	идентификатор team_id для подключения к сервисам Apple

Указанные переменные необходимо добавить в секцию `[all:vars]`

Файл соответствующий имени указанному в `inv_push_key` добавьте в `certificates/inv_domain_fqdn`

4.1.6. Структура хранения сертификатов и ключей для инсталляции

```
certificates
└── example.com
    ├── dkim
    │   ├── dkim.key
    │   └── dkim.pub
    ├── ca.pem
    ├── push_key.p8
    ├── server.key
    └── server.pem
```

4.1.7. Прочие параметры конфигурации

переменная	назначение	значение по умолчанию	комментарий
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_elastic_log_server	использование лог-сервера из СО для агрегации логов	по умолчанию не определена, необходимо раскомментировать для использования	для отключения переменная должна быть закомментирована или удалена из инвентарного файла
inv_be_amavis_dkim_selector	селектор для использования DKIM-подписи	mail	подробнее о настройке цифровой подписи в р. 4.1.4
inv_postfix_trusted_networks	Доверенные сети для получения почтовых сообщений.	-	IP адреса разделенные запятой. Текущую сеть не надо размещать в параметрах

4.2. Запуск инсталляции

Внимание. Если вы производите обновление с предыдущей версии, ознакомьтесь с разделом **6. Обновление с предыдущей версии**.

После завершения конфигурирования, можно приступать к запуску инсталляции. Сервер, с которого производится инсталляция, должен иметь возможность подключаться по сети к каждому серверу на который устанавливается МойОфис Почта. Рекомендуется использовать ssh-ключи. Для безопасности приватные ключи должны храниться на рабочих станциях пользователей и "пробрасываться" вместе с ssh-сессией. (см. подробнее https://www.ssh.com/ssh/agent#sec-SSH-Agent-Forwarding)

Для запуска инсталляции в кластерной (отказоустойчивой) конфигурации необходимо выполнить команду:

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

Для запуска инсталляции в бескластерной конфигурации необходимо выполнить команду:

```
ansible-playbook -i inventory/<install_file> playbook_sa.yml
```

Дополнительно может пригодиться использование опции `-v` - расширенная информация по процессу инсталляции. Добавление символов **v** увеличивает уровень детализации.

В случае запуска инсталляции не от суперпользователя(root) могут возникнуть ошибки установки пакетов и создания конфигурационных файлов. Для решения данной задачи используйте запуск инсталляции с параметрами `-sK`, после чего потребуется ввести пароль пользователя root, например:

```
ansible-playbook -sKi inventory/<install_file> <playbook.yml|playbook_sa.yml>
```

Процесс инсталляции должен завершиться без ошибок.

```
PLAY RECAP *********************************************************
10.10.10.200             : ok=27   changed=14   unreachable=0    failed=0
10.10.10.201             : ok=48   changed=23   unreachable=0    failed=0
10.10.10.202             : ok=48   changed=14   unreachable=0    failed=0
10.10.10.203             : ok=172  changed=107  unreachable=0    failed=0
10.10.10.204             : ok=164  changed=99   unreachable=0    failed=0
10.10.10.205             : ok=131  changed=86   unreachable=0    failed=0
10.10.10.206             : ok=126  changed=81   unreachable=0    failed=0
localhost                : ok=0    changed=0    unreachable=0    failed=0
```

Если возникли ошибки и процесс инсталляции не завершился, проверьте корректность заполнения инвентарного файла.

4.2.1. Замена сертификатов

В процессе эксплуатации системы возникает необходимость замены SSL сертификатов на стенде. Для этого необходимо:

- 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 dirsrv:

```
openssl pkcs12 -export -inkey server.key -in server.crt -out /tmp/crt.p12 -
nodes -name 'server-cert' -passout pass:
certutil -D -d /etc/dirsrv/slapd-ldap -n "server-cert"
pk12util -d /etc/dirsrv/slapd-ldap/ -i /tmp/crt.p12 -W '
```

- Перезапустить сервисы ролей fe, web-client:

```
systemctl restart httpd dirsrv@ldap
```

- Перезапустить сервисы роли be:

```
systemctl restart postfix dovecot dirsrv@ldap
```

5. Дополнительные настройки FS для работы с PSN

Во время установки FS необходимо обратить внимание на параметры подключения к PSN. Для этого обратитесь к соотвествующим инструкциям по установке МойОфис Хранилище.

6. Обновление с предыдущей версии

6.1. 2017.04 (Kawakawa) на 2018.01 (lemon)

Перед обновлением рекомендуется сделать бэкап данных: БД, почтовые ящики, конфигурация подключения к сторонним LDAP-серверам для Postfix и Dovecot.

Обновление на версию 2018.02 (Lemon) необходимо начать с обновления ОС до версии 7.4. Необходимо включить репозитории sl и sl-security после чего запустить команду обновления.

```
yum -y update --exclude=openldap* --exclude=dovecot* --disablerepo=* --
enablerepo=psn --enablerepo=sl --enablerepo=sl-security
```

Для других ОС необходимо выбрать соответствующие базовые репозитории. **Внимание** не используйте репозитории updates и подобные, это может привести к нарушению зависимостей пакетов.

6.2. 2018.01 (Lemon) на 2019.03 (Paprika)

Перед обновлением рекомендуется сделать бэкап данных: БД, почтовые ящики, конфигурация подключения к сторонним LDAP-серверам для Postfix и Dovecot.

Обновление на версию 2019.03 (Paprika) необходимо начать с обновления ОС до версии 7.5. Необходимо включить репозитории sl после чего запустить команду обновления.

```
yum -y update --exclude=openldap* --exclude=dovecot* --disablerepo=* --
enablerepo=sl
```

Для других ОС необходимо выбрать соответствующие базовые репозитории. **Внимание** не используйте репозитории updates, security и подобные - это может привести к нарушению зависимостей пакетов.

После успешного обновления ОС можно приступить к обновлению продукта МойОфис Почта. Обновление происходит аналогично установке, воспользуйтесь данной инструкцией начиная с раздела 3.

6.3. 2018.02 (Mint) или 2018.02.21 (Mint_R) или 2019.01 (Nutmeg), 2019.02 (Oregano) на 2019.03 (Paprika)

Перед обновлением рекомендуется сделать бэкап данных: БД, почтовые ящики, конфигурация подключения к сторонним LDAP-серверам для Postfix и Dovecot. После выполнения бекапа можно приступить к обновлению продукта МойОфис Почта. Обновление происходит аналогично установке, воспользуйтесь данной инструкцией начиная с раздела 3.

7. Бэкап БД

Перед обновлением стенда рекомендуется сделать бэкап БД aurora.

7.1. Создание бэкапа

Для создания бэкапа используется команда:

```
mysqldump -u aurora -p aurora > dump_mysql.sql
```

7.2. Восстановление из созданного дампа

```
mysql -u aurora -p aurora < dump_mysql.sql
```

8. Техническая поддержка

При возникновении вопросов не описанных в данной инструкции вы можете обратиться в службу технической поддержки ООО "Новые облачные технологии".

Адрес электронной почты: support@service.myoffice.ru

Телефон: 8-800-222-1-888