Руководство по установке

ПОЧТА (PSN)

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

МойОфис Почта

РУКОВОДСТВО ПО УСТАНОВКЕ

2.1

На 48 листах

Москва

2022

Содержание

Перечень сокращений, терминов и определений **6**

1 Общие сведения **8**

1.1 Назначение . . . 8

1.2 Требования к квалификации персонала . . . 8

1.3 Системные требования . . . 9

1.4 Ограничения . . . 10

2 Описание архитектуры «МойОфис Почта» **11**

3 Типовые схемы установки «МойОфис Почта» **12**

3.1 Конфигурация без отказоустойчивости . . . 12

3.2 Кластерная отказоустойчивая конфигурация . . . 12

3.3 Типовая схема масштабирования . . . 12

4 Первичная установка **13**

4.1 Состав дистрибутива . . . 13

4.2 Подготовка к установке . . . 13

4.2.1 Описание ролей . . . 13

4.2.2 Подготовка инфраструктуры установки . . . 14

4.2.2.1 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива (с доступом в Интернет) . . . 15

4.2.2.2 Подготовка серверов, на которые будет производиться инсталляция дистрибутива (без доступа в Интернет) . . . 15

4.2.2.3 Проверка и подготовка инсталляционного архива . . . 16

4.2.3 Настройка основных параметров установки . . . 17

4.2.3.1 Конфигурирование инвентарного файла: hosts . . . 17

4.2.3.2 Конфигурирование инвентарного файла: переменные . . . 20

4.2.4 Настройка дополнительных параметров установки . . . 30

4.2.5 Настройка DNS . . . 30

4.2.6 Настройка межсетевого экранирования . . . 31

4.3 Установка «МойОфис Почта» . . . 32

4.3.1 Запуск установки . . . 32

4.3.2 Проверка корректности установки . . . 32
4.3.3 Интеграция с «МойОфис Хранилище» (PGS) . . . 33
4.3.4 Интеграция с сервисом TrueConf . . . 34
4.3.4.1 Настройки сервера «МойОфис Почта» . . . 34
4.3.4.2 Настройки административной панели TrueConf . . . 35
4.3.5 Интеграция с Active Directory . . . 37
4.4 Настройка интеграции с Infowatch Traffic Monitor . . . 37
4.4.1 Установка InfoWatch Traffic Monitor в разрыв трафика . . . 37
4.4.1.1 Перехват SMTP-трафика методом отправки скрытой копии . . . 38
4.4.1.2 Перехват HTTP/S-трафика методом отправки почты на корпоративный прокси-сервер 39
4.4.2 Установка агента InfoWatch Device Monitor . . . 40

5 Обновление с PSN 1.0 **42**
5.1 Конфигурация без отказоустойчивости . . . 42
5.2 Конфигурация с отказоустойчивостью . . . 43

6 Создание резервных копий **46**
6.1 Создание резервных копий службы каталогов LDAP . . . 46
6.2 Переустановка службы каталогов LDAP . . . 47

7 Техническая поддержка **48**

Перечень сокращений, терминов и определений

Сокращение, термин	Расшифровка и определение
389-ds, 389 Directory Server	Служба каталогов, предназначенная для централизованного управления доступом к ресурсам на множестве сетевых серверов.
Ansible	Система управления конфигурациями, использующаяся для автоматизации настройки и развертывания программного обеспечения.
API	Application Programming Interface, интерфейс программирования приложений
CO	CloudOffice, Облачный Офис, общее название продукта (группы редакторов)
DNS	Domain Name System, система доменных имён
Docker	Программное обеспечение для автоматизации развёртывания и управления приложениями в средах с поддержкой контейнеризации
IMAP	Internet Messagess Access Protocol, протокол доступа к ящику электронной почты
LDAP	Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам
Node (нода)	Сервер одной из ролей
PGS	File Storage, Pythagoras, программный продукт «МойОфис Хранилище»
PSN, PSN 2.0	Poseidon, приложение почты, календаря и контактов (оно же «МойОфис Почта»)
PSNAPI	API «МойОфис Почта»
SMTP	Simple Mail Transfer Protocol, протокол передачи сообщений электронной почты
SSH	Secure Shell, «безопасная оболочка»
URL	Uniform Resource Locator, единый указатель ресурса
БД	База данных
Вендор (vendor)	Поставщик брендированного продукта

Сокращение, термин	Расшифровка и определение
Кластер (cluster)	Объединенная группа серверов
Контур инсталляции	Приватная сеть, в рамках которой происходит обмен техническими данными между серверами инсталляции
Плейбук (playbook)	Набор последовательных инструкций для выполнения команд Ansible
ПО	Программное обеспечение
ОС	Операционная система
Тенант (tenant)	Элемент мультиарендной системы
Хост (host)	Устройство, предоставляющее сервисы формата “клиент-сервер”

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 со службой доменных имен (DNS):
  - Знание основных терминов (DNS, IP-адрес и т.д.);
  - Понимание принципов работы DNS серверов (корневые серверы, TLD-серверы, разрешающий сервер имен и т.д.);
  - Знание основных типов записей DNS:
    - A (address)
    - MX
    - SRV
    - PTR
    - TXT (SPF, DKIM)
  - Опыт обращения к RFC по следующим ресурсным записям:
    - Simple Mail Transfer Protocol;
    - Anti-Spam Recommendations for SMTP MTAs;
    - DomainKeys Identified Mail (DKIM) and Mailing Lists;
    - Sender Policy Framework (SPF) for Authorizing Use of Domains in Email;

    - Use of SRV Records for Locating Email Submission/Access Services;
    - Locating Services for Calendaring Extensions to WebDAV (CalDAV) and vCard Extensions toWebDAV (CardDAV).
- Опыт работы с командной строкой ОС Linux.
- Опыт работы с ПО для контейнеризации Docker/Docker Swarm.
- Знание видов архитектуры, а так же основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:
    - Закрытый и открытый ключ;
    - Сертификат открытого ключа;
    - Регистрационный центр (RA);
    - Сертификационный центра (CA);
    - Хранилище сертификатов (CR).
- Практический опыт работы и администрирования сервисов: Redis, RabbitMQ, PostgreSQL, 389 Directory Server, Dovecot, Postfix, GlusterFS, etcd.
- Опыт работы с системой автоматизации развертывания Ansible.

1.3 Системные требования

- Поддерживаемая операционная система: **Centos 7.9**;
- Скорость сетевой подсистемы – 1Gbit/s или выше;
- В Таблице 2 приведены характеристики аппаратного обеспечения конфигурации для функционального тестирования (без отказоустойчивости).

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

Таблица 2. Характеристики аппаратной конфигурации без отказоустойчивости

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

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

Таблица 3. Разбиение дисков

> Подробнее о кластерной инсталляции написано в разделе 3 данного руководства.

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;
- В соответствии с рекомендациями производителей операционных систем, для CentOS рекомендуется использовать файловую систему xfs.

2 Описание архитектуры «МойОфис Почта»

Внутренняя структура «МойОфис Почта» представляет собой набор сервисов, обеспечивающих работу ПО и взаимодействие с компонентами «МойОфис Частное Облако». Более подробно сервисы (представленные в виде инсталляционных ролей) описаны в параграфе 4.2.1 данного руководства. Детальная архитектурная схема «МойОфис Почта» приведена на Рисунке 1.

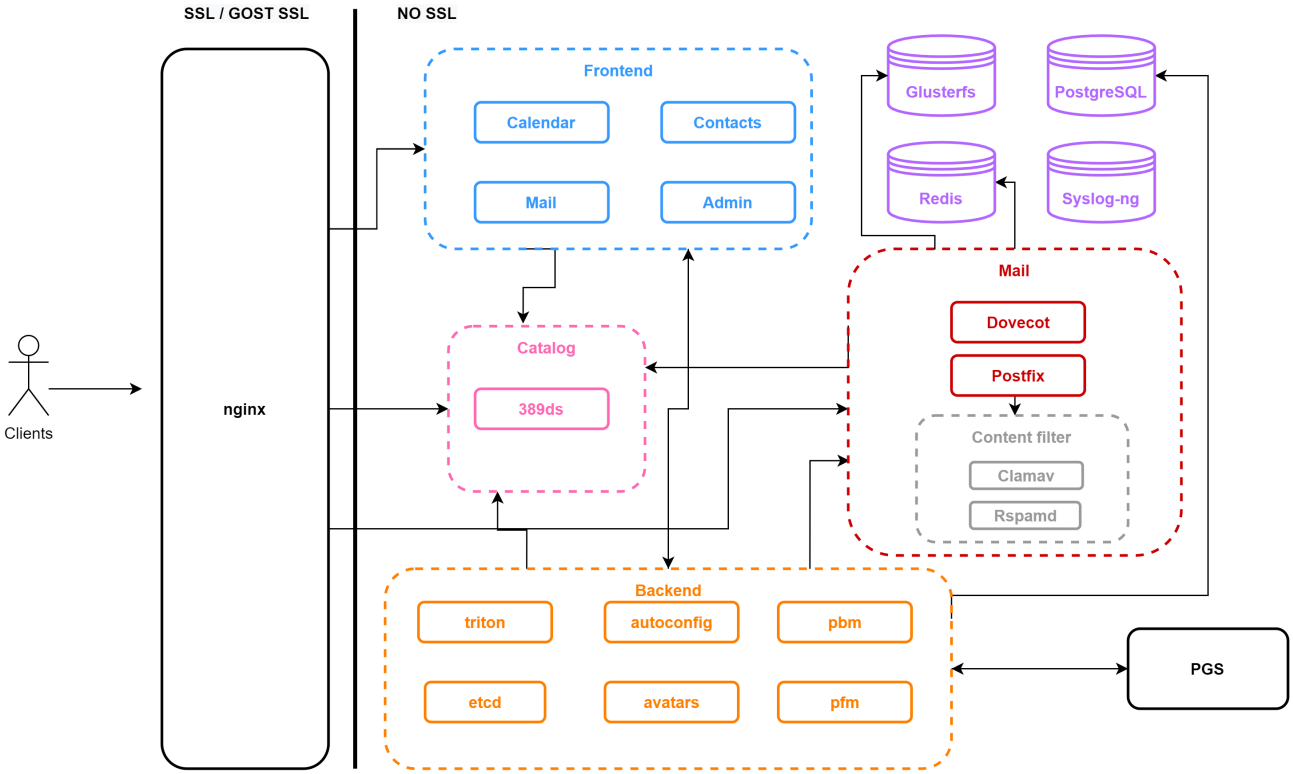

Рисунок 1. Архитектурная схема «МойОфис Почта»

3 Типовые схемы установки «МойОфис Почта»

3.1 Конфигурация без отказоустойчивости

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

3.2 Кластерная отказоустойчивая конфигурация

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

Более подробно о конфигурировании кластерной инсталляции «МойОфис Почта» рассказано в разделе 4.3 данного руководства.

3.3 Типовая схема масштабирования

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

4 Первичная установка

4.1 Состав дистрибутива

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

- Набор Ansible плейбуков для развертывания ролей;
- Архив образа Docker Registry.

4.2 Подготовка к установке

4.2.1 Описание ролей

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

Роль	Значение
Backend	Занимается установкой сервисов, отвечающих за функционирование внутренней, программно-аппаратной части продукта.
LDAP	Устанавливает сервис 389-ds (выполняющий роль LDAP-сервера).
Certificates	Роль, отвечающая за установку сертификатов.
Chrony	Сервис синхронизации времени.
Common	Базовые настройки для машин, установка необходимых пакетов и зависимостей.
Docker Registry	Сервис для хранения и распространения контейнеров Docker.
Etcd	Распределенная система хранения ключей и конфигураций для сервисов.
Frontend	Отвечает за разворачивание веб-интерфейса «МойОфис Почта».
Glusterfs	Распределённая масштабируемая файловая система для объединения хранилищ данных, находящихся на разных серверах в одну сетевую файловую систему.

Роль	Значение
Mail	Роль, разворачивающая сервисы, необходимые для работы PSN 2.0: `rspamd` – система фильтрации спама, `dovecot` – IMAP и POP3-сервер, `clamav` – почтовый антивирус, `postfix` – агент передачи почты.
Proxy	Прокси-сервер nginx.
Postgres (PostgreSQL)	Основная база данных.
Redis	База данных “ключ-значение” для не персистентных данных.
Syslog-ng	Сервис сбора логов работы компонентов программного комплекса.
Sysctl	Применение настроек ядра почтовой программы.
Timezone	Часовой пояс по умолчанию в формате tz database.

Таблица 4. Логические роли системы «МойОфис Почта»

4.2.2 Подготовка инфраструктуры установки

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

1. Скачать и инсталлировать минимальный серверный вариант CentOS поддерживаемой версии (7.9 в данном релизе, см. параграф 1.3 данного руководства).
    - Отключить систему SELinux.
    - CentOS имеет механизм разграничения на основании доступа к файлам и каталогам. Каждому администратору системы строго рекомендуется иметь отдельную учетную запись в системе.
2. Предустановить на ОС следующие пакеты: python3 (версии не ниже 3.6), python3-pip, rsync.
3. С инфраструктурной машины должен быть возможен ssh-доступ на все хосты целевого сервера инсталляции. В целях удобства, рекомендуется сделать это при помощи ssh-ключа пользователем root или другим пользователем с sudo привилегиями.

> Рекомендуется отключить удаленное подключение от пользователя root. Для этого в файле `/etc/ssh/sshd_config` следует 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. На инфраструктурную машину должен быть инсталлирован пакет Ansible 4.4.*. Работа более поздних версий возможна, но не гарантирована. > Подробная документация по установке Ansible
5. Во избежание проблем, не рекомендуется использовать системы, на которых ранее были проведены инсталляции программного обеспечения, не относящегося к дистрибутиву «МойОфис Почта».
6. Используемая файловая система под docker-контейнеры должна официально поддерживаться текущей версией Docker. Если используется XFS, то файловая система должна быть создана с опцией `-n ftype=1` (вариант по умолчанию в рекомендованных ОС).
7. 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.
8. Для корректной работы «МойОфис Почта» необходимо настроить службу синхронизации времени на всех серверах контура установки.

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 1-2 и 5-8 из раздела 4.2.2.1 данного руководства.

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

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

В данном релизе возможность установки продукта без доступа в Интернет не предусмотрена. Если инфраструктурная машина и целевые серверы расположены в локальной сети и не имеют прямого доступа в Интернет, инсталляцию можно произвести в экспериментальном порядке, заранее предустановив на них пакеты Yum и python3 pip, указанные в Таблице 5:

Пакет	Рекомендуемый репозиторий
python3	https://www.python.org/downloads/source/
python3-pip	https://pypi.org/project/pip/
docker-ce	https://download.docker.com/linux/centos/docker-ce.repo
docker-ce-cli	https://download.docker.com/linux/centos/dockerce.repo
rsync	https://rsync.samba.org/
Пакеты Python3 pip	
docker	https://pypi.org/project/docker/
passlib	https://pypi.org/project/passlib/
bcrypt	https://pypi.org/project/bcrypt/3.1.7/
jsondiff	https://pypi.org/project/jsondiff/
pyyaml	https://pypi.org/project/PyYAML/
selinux	https://pypi.org/project/selinux/

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

4.2.2.3 Проверка и подготовка инсталляционного архива

Для выполнения проверки и подготовки дистрибутива, необходимо:

1. После копирования инсталляционного архива проверить его контрольную сумму MD5, в дальнейшем сверив её с переданной вендором ПО:

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

> В имени архива цифры версии коммерческого релиза представлены знаками X.

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

```
mkdir install_MyOffice_PSN
tar xvzf MyOffice_PSN_XXXX.XX.tgz -C install_MyOffice_PSN
cd install_MyOffice_PSN
```


> Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

4.2.3 Настройка основных параметров установки

Для конфигурирования установки необходимо создать **инвентарный файл** (inventory file), шаблон которого находится в директории инсталлятора по адресу:

```
~\MyOffice_PSN_XXXX.XX\inventory\hosts.yml
```

Файл шаблона можно открыть в текстовом редакторе и, заполнив секции `hosts` и `vars` в соответствии с дальнейшими инструкциями, сохранить под любым именем.

> Инвентарный файл использует формат .yaml, более подробно о синтаксисе можно прочитать в документации Ansible. Сконфигурированный файл рекомендуется сохранить на внешнем ресурсе для дальнейшего использования на случай восстановления и/или переустановки системы.

4.2.3.1 Конфигурирование инвентарного файла: hosts

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

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

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

> Более подробно о значении ролей рассказано в параграфе 4.2.1 данного руководства.

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

```
all:
  children:
### SECTION 1: grouping by Roles
```



```
infra:
  children:
    docker_registry:
      hosts:
        host.example.com:
db:
  children:
    etcd:
      hosts:
        host.example.com:
          volume_device_etcd: "False"
          volume_device_etcd_path: "/dev/disk/by-uuid/<UUID>"
    redis:
      hosts:
        host.example.com:
    postgres:
      hosts:
        host.example.com:
          volume_device_postgres: "False"
          volume_device_postgres_path: "/dev/disk/by-uuid/<UUID>"
    ldap:
      hosts:
        host.example.com:
frontend:
  children:
    proxy:
      hosts:
        host.example.com:
backend:
  hosts:
    host.example.com:
mail:
  hosts:
```



```
        host.example.com:
```

Следует обратить дополнительное внимание на роли `etcd` и `postgres` : у них есть дополнительные переменные `volume_device_<role>` и `volume_device_<role>_path` . Заполнение этих переменных **необходимо** при использовании данного ПО для хранения данных на блочных устройствах, форматированных в файловую систему XFS. В таком случае, значения меняются на:

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

Где `<role>` – логическая роль, `<filesystem_path>` – путь до файловой системы устройства.

Особенности работы в режиме `volume_device_<role>: "True"` :

1. Не допускается использование одного и того же раздела диска на одном сервере (или виртуальной машине) для нескольких ролей.
2. Диск должен быть отформатирован в файловую систему XFS и не должен быть смонтирован на момент разворачивания (кроме ситуации повторного запуска).

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

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

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

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

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

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

```
    db:
      children:
        etcd:
          hosts:
```



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

- В текущем релизе для группы `ldap`, отвечающей за сервисы каталогов, максимальное число указываемых хостов при кластерной инсталляции равно двум. Хосты в группе должны быть сконфигурированы с **разными** именами (hostname), менять которые в процессе эксплуатации не следует во избежание некорректной работы системы. >Для изменения hostname в уже установленной системе, необходимо произвести процедуру резервирования данных службы и переустановить её. Подробный процесс описан в разделах 6.1 и 6.2 данного руководства.
- Сервису `syslog` в инвентарном файле присваивается хост, на котором будут храниться логи, собираемые со всех серверов установки. Путь к логам будут выглядеть следующим образом:

```
/opt/poseidon/logs/
```

> В standalone-установке имплементация сервиса нецелесообразна (логи в этом случае уже собираются на одной машине). Для того, чтобы пропустить установку `syslog`, необходимо удалить соответствующую ему группу хостов из инвентарного файла перед установкой программы.

4.2.3.2 Конфигурирование инвентарного файла: переменные

Дальнейший процесс настройки будет состоять из заполнения секции `vars` – переменных инвентарного файла. Доступные значения и способы заполнения данной секции указаны в Таблице 6 данного руководства.

> Все параметры переменных необходимо указывать в двойных кавычках.

Переменная	Значение и способ заполнения
`dev_mode:`	*Developer mode*, режим разработчика. Принимает значения `True` и `False`, в случае значения `True` открывает порты сервисов наружу для организации доступа разработчиков к стенду установки (не используется в работающей с пользователями системе).
`swarm_network_encryption:`	Включает шифрование внутренней оверлейной сети Docker swarm, значение по умолчанию `False`. Влияет на производительность системы, подробнее о данном виде шифрования.
Блок **setup**:	Устанавливает зависимости для формирования доменных имен внутри среды инсталляции, а также настраивает параметры для сертификации.
`default_instance_language:`	Задаёт язык интерфейса по умолчанию для пользователей в тенантах. Возможные значения: `Russian`, `English`, `Bashkir`, `French`, `Spanish`, `Italian`, `Portuguese`.
`external_domain:`	Зарегистрированный домен инсталляции. Для корректной работы необходим установленный актуальный SSL-сертификат.
`domain_module:`	Шаблон формирования внешних доменных имён инсталляции, позволяет гибко настроить принцип их генерации. Примеры работы шаблона при использовании домена test.example.com и префикса auth: `{service}-{domain}` – auth-test.example.com `{service}.{domain}` – auth.test.example.com `{service}-mail.{domain}` – auth-mail.test.example.com

Таким образом можно гибко настраивать принцип формирования доменных имен инсталляции. Это может пригодиться, например, если у вас есть wild-card сертификат SSL на доменное имя example.com и *.example.com, но нет на* .test.example.com. Вы можете установить `DOMAIN_MODULE:` в значение `{service}-{domain}` и получить

домены третьего уровня, которые подходят под текущий wild-card сертификат SSL.

Переменная	Значение и способ заполнения
Блок **tls:**	Указываются параметры для TLS-сертификата.
`cert_filename:`	Имя файла TLS-сертификата для внешнего домена. Файл содержит SSL-сертификат на `*.<EXTERNAL_DOMAIN>` , промежуточные сертификаты и корневой в формате PEM. Значение по умолчанию: `server.pem` .
`key_filename:`	Имя файла ключа TLS-сертификата для внешнего домена. Сам файл содержит приватный ключ сертификата в формате PEM, не требующий кодовой фразы.Значение по умолчанию: `server.key` .
Блок **dkim:**	Указываются параметры для цифровой подписи DKIM.
`key_filename:`	Имя файла приватного ключа цифровой подписи DKIM. Значение по умолчанию: `dkim.key` .

Заполнение данных переменных позволяет задать имена файлов сертификатов и ключей в индивидуальном порядке. TLS-сертификаты и файл ключа DKIM необходимо разместить в директории установки по следующему пути:

```
~\MyOffice_PSN_XXXX.XX\certificates
```

> Инсталляция PSN 2.0 без установки сертификатов невозможна.

Переменная	Значение и способ заполнения
Блок **passwords:**	Для основных сервисов инсталляции рекомендуется использовать надёжные пароли, в этом может помочь утилита `pwgen 10 1` . Рекомендуемые значения: большие и маленькие латинские буквы, цифры, специальные символы: &!% (символ $ использовать нельзя).
`system_user:`	Пароль пользователя для отправки системных сообщений.

Переменная	Значение и способ заполнения
`postgres_superuser:`	Пароль суперпользователя PostgreSQL.
`postgres_replica_user:`	Пароль пользователя для репликации PostgreSQL в случае кластерной установки.
`postgres_db_user:`	Пароль пользователя баз данных PSN 2.0.
`redis_user:`	Пароль доступа к БД Redis.
`ds389_manager_user:`	Пароль доступа к службе каталогов 389 Directory Server.
`ds389_replicator_user:`	Пароль пользователя для репликации 389 Directory Server в случае кластерной установки.
`dovecot_adm_user:`	Пароль доступа к сервису хранения писем.
`psnapi_adm_user:`	Пароль доступа к API компонента PSN 2.0.
`etcd_browser_user:`	Пароль для веб-интерфейса сервиса Etcd. Авторизация производится юзером `psnuser` по административному адресу (сформированному по шаблону) с указанным портом 8081. Значение по умолчанию: `psnpass` .
`default_tenant_admin_user:`	Пароль тенанта по умолчанию (default) при установке без интеграции с «МойОфис Хранилище» (PGS).
`mon_user:`	Используется при заполнении группы хостов `monitoring` (опционально) для доступа к интерфейсу Grafana. Значение по умолчанию: `admin` .
`mon_user_hash:`	Хэш пароля для мониторинга. Пример генерации: `openssl passwd -apr1 $mon_user`
`master_user:`	Пароль для сервисной учётной записи (мастер-пользователя). Данная запись предоставляет административный доступ к письмам и почтовым ящикам пользователей при условии обращения через веб-клиент. Авторизация при помощи данной записи недоступна извне.

Переменная	Значение и способ заполнения
Блок **secure:**	Ключи для внутреннего шифрования. Блок заполняется перед установкой, изменять его в дальнейшем **не следует** во избежание потери доступа к системе.
`db_secret_key:`	
`internal_secret_key:`	
`auth_jwt_key:`	Должен состоять из минимум 16 символов.
Блок **notifications:**	Бóльшая часть значений переменных данного блока находится в аккаунте консоли Firebase (или консоли Huawei для устройств Huawei). В случае отсутствия у администратора системы учетной записи в данной консоли, он может обратиться за доступом непосредственно к вендору ПО «МойОфис Почта». Значения переменных указываются в кавычках.
Блок **mobile:**	Данный блок переменных отвечает за настройку мобильных уведомлений.
`enabled`	Включает и выключает мобильные уведомления, доступные значения `true` и `false`, по умолчанию `false`.
`ios_bundle_name`	Значение по умолчанию `iosmailemb`. Изменять не требуется.
`android_bundle_name`	Значение по умолчанию `amail`. Изменять не требуется.
`google_conf_file_name`	Имя файла конфигурации json. Значение по умолчанию - `google_push.json`. Пример заполнения указан ниже.

Пример заполнения конфигурационного json-файла:

```
{
  "type": "service_account", // Значение по умолчанию. Изменять не требуется.
  "project_id": "<PROJECT_ID>", // Соответствует значению из графы Project ID вкладки General раздела Your project.
```

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

Готовый файл необходимо разместить в директории установки по следующему пути:

```
~\MyOffice_PSN_XXXX.XX\certificates
```

Переменная	Значение и способ заполнения
Блок **ios:**	Данный блок отвечает за мобильные уведомления в устройствах на операционной системе iOS. Значения переменных находятся в соответствующих графах Firebase console, доступ к которой администратору системы предоставляется вендором ПО «МойОфис Почта». Для настройки уведомлений iOS необходимо авторизоваться в консоли Firebase, зайти на вкладку General в раздел Your Apps и выбрать там нужный проект (iOS).
`api_key`	Соответствует значению из графы Web API Key вкладки General раздела Your Apps.

Переменная	Значение и способ заполнения
`app_id`	Соответствует значению из графы App ID вкладки General раздела Your Apps.
`messaging_sender_id`	Соответствует значению из графы Sender ID вкладки Cloud Messaging.
`project_id`	Соответствует значению из графы Project ID вкладки General раздела Your project.
Блок **android:**	Данный блок отвечает за мобильные уведомления в устройствах на операционной системе Android. Значения переменных находятся в соответствующих графах Firebase console, доступ к которой администратору системы предоставляется вендором ПО «МойОфис Почта». Для настройки уведомлений Android необходимо авторизоваться в консоли Firebase, зайти на вкладку General в раздел Your Apps и выбрать там нужный проект (Android).
`api_key`	Соответствует значению из графы Web API Key вкладки General раздела Your Apps.
`app_id`	Соответствует значению из графы App ID вкладки General раздела Your Apps.
`messaging_sender_id`	Соответствует значению из графы Sender ID вкладки Cloud Messaging.
`project_id`	Соответствует значению из графы Project ID вкладки General раздела Your project.

Переменная	Значение и способ заполнения
Блок **huawei:**	Данный блок отвечает за мобильные уведомления в устройствах на операционной системе Huawei. Значения переменных находятся в соответствующих графах консоли Huawei, доступ к которой администратору системы предоставляется вендором ПО «МойОфис Почта». Для настройки уведомлений Huawei необходимо авторизоваться в консоли Huawei, зайти в настройки проекта в раздел Основная информация и найти там необходимые значения.
`enabled`	Включает и выключает мобильные уведомления для Huawei, доступные значения `true` и `false`, по умолчанию `false`.
`client_id`	Соответствует значению из графы ID приложения.
`client_secret`	Соответствует значению из графы секрет клиента.
`huawei_bundle_name`	Значение по умолчанию `huawei`. Изменять не требуется.
Блок **web:**	Данный блок переменных отвечает за настройку web-пушей. Значения переменных находятся в соответствующих графах Firebase console, доступ к которой администратору системы предоставляется вендором ПО «МойОфис Почта». Для настройки web-пушей необходимо авторизоваться в консоли Firebase, зайти на вкладку General в раздел Your Apps и выбрать там нужный проект (Web App).
`enabled`	Включает и выключает web-пуши, доступные значения `true` и `false`, по умолчанию `false`.
`webpush_bundle_name`	Значение по умолчанию `webpush`. Изменять не требуется.
`api_key`	Соответствует значению из графы Web API Key вкладки General раздела Your Apps.

Переменная	Значение и способ заполнения
`vapid_key`	Соответствует значению из графы Key pair вкладки Cloud messaging раздела Web configuration.
`auth_domain`	Домен авторизации Firebase. Значение представляет собой адрес вида `<PROJECT_ID>.firebaseapp.com`, где `<PROJECT_ID>` соответствует значению из графы Project ID вкладки General раздела Your project.
`database_url`	Путь к базе данных Firebase. Значение представляет собой адрес вида `<PROJECT_ID>.firebaseio.com`, где `<PROJECT_ID>` соответствует значению из графы Project ID вкладки General раздела Your project.
`project_id`	Соответствует значению из графы Project ID вкладки General раздела Your project.
`storage_bucket`	Путь к хранилищу объектов. Значение представляет собой адрес вида `<PROJECT_ID>.appspot.com`, где `<PROJECT_ID>` соответствует значению из графы Project ID вкладки General раздела Your project.
Блок **integrations:**	В данном блоке указываются параметры для интеграции с другими компонентами «МойОфис Частное Облако».
Блок **trueconf:**	В данном блоке указываются параметры для интеграции с TrueConf.
`enabled:`	Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
`url:`	Соответствует ссылке на API TrueConf.
`delete_after:`	Время в секундах, по прошествии которого завершенная конференция будет удалена.
Блок **pgs:**	В данном блоке указываются параметры для интеграции с «МойОфис Хранилище» (PGS).

Переменная	Значение и способ заполнения
`enabled:`	Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
`appapi_user_password:`	Значение переменной `KEYCLOAK_PASSWORD` из инвентарного файла «МойОфис Хранилище» (PGS).
`co_oauth2_client_secret:`	Переменная ключа, должна совпадать с `MAIL_OAUTH2_CLIENT_SECRET` в конфигурации CO.
Блок **ad:**	В данном блоке указываются параметры для интеграции с Active Directory. Актуально для инсталляции **без** интеграции с PGS.
`enabled:`	Включение интеграции. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.
`host:`	Адрес контроллера домена.
`base_dn:`	База пользователей Active Directory.
`login:`	Логин учетной записи, от имени которой будет осуществляться вход и поиск по базе AD.
`password:`	Пароль учетной записи, от имени которой будет осуществляться вход и поиск по базе AD.
`port:`	Порт для подключения к AD по протоколу LDAP. Обычно принимает значения `389` (для подключения без шифрования) или `636` (с шифрованием).
`ssl:`	Использование протокола с шифрованием. Переменная принимает значения `True` (интеграция включена) и `False` (интеграция отключена). Не может быть оставлена пустой.

Таблица 6. Значения и способы заполнения переменных инвентарного файла инсталляции PSN 2.0

4.2.4 Настройка дополнительных параметров установки

Дополнительные параметры установки находятся в файле `~/group_vars/all/main.yml` . Менять их без согласования с вендором ПО не рекомендуется.

4.2.5 Настройка DNS

Перед началом установки необходимо настроить DNS для разрешений некоторых доменных имен в адрес, куда будет установлен сервер **nginx** (раздел **proxy** инвентарного файла). Необходимая для настройки информация указана в Таблице 7. Поскольку внешнее доменное имя в PSN 2.0 формируется посредством шаблона (переменная `domain_module` , см. раздел 4.2.3.2), в таблице указан только требуемый префикс.

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

Префикс	Комментарий
`admin`	Адрес веб-панели администрирования PSN 2.0 в случае установки без интеграции с «МойОфис Хранилище» (PGS). В случае интеграции с PGS, данное имя должно разрешаться в адрес хоста, присвоенного роли **nginx** инвентарного файла «МойОфис Хранилище».
`autoconfig`	
`cab`	
`imap`	
`mail`	
`psnapi`	Адрес точки входа для API. Обязателен только для разрешения внутри контура инсталляции.
`smtp`	
`pbm`	

Таблица 7. Настройка DNS

Для внешних систем доменные имена должны корректно разрешаться в соответствующий публичный IP-адрес. Необходимая для настройки внешних записей типа SRV информация указана в Таблице 8:

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

Таблица 8. Сведения про необходимые для инсталляции внешние DNS-записи

4.2.6 Настройка межсетевого экранирования

Для корректной работы «МойОфис Почта» рекомендуется не использовать сетевое экранирование между серверами. Необходимые для работы ПО сетевые порты приведены ниже в Таблице 8:

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

Таблица 8. Сетевые порты, доступ к которым необходим с внешних IP-адресов

4.3 Установка «МойОфис Почта»

4.3.1 Запуск установки

Для запуска установки подсистемы PSN 2.0 необходимо перейти в директорию установки и выполнить в терминале следующую команду:

```
./deploy_psn.sh <hosts.yaml> <additional ansible keys>
```

Где `<hosts.yaml>` – инвентарный файл, сконфигурированный в соответствии с параграфом 4.2.3.1 данного руководства, `<additional ansible keys>` – дополнительные ключи установки.

> Подробнее о дополнительных ключах в документации Ansible.

Файл логов процесса развертывания будет сохранен под именем `deploy_psn_$<DATE>.log` .

При успешном выполнении команды сервисы подсистемы будут запущены автоматически.

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

4.3.2 Проверка корректности установки

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

```
docker service ls | grep psn | awk -v OFS='\t' '{print $2, $4}' | column -t
```

Ожидаемый вывод:

```
psn-backend_autoconfig     1/1
psn-backend_avatars        1/1
psn-backend_pbm            1/1
psn-backend_pfm            1/1
psn-backend_triton         1/1
psn-etcd_browser           1/1
psn-etcd_etcd              1/1
psn-frontend_web_admin     1/1
```



```
psn-frontend_web_calendar  1/1
psn-frontend_web_contacts  1/1
psn-frontend_web_mail      1/1
psn-ldap_ldap              1/1
psn-mail_clamav            1/1
psn-mail_dovecot           1/1
psn-mail_freshclam         1/1
psn-mail_postfix           1/1
psn-mail_rspamd            1/1
psn-nginx-proxy_nginx      1/1
psn-postgres_postgres      1/1
psn-redis_redis            1/1
```

2. В браузере открыть страницу `mail.<EXTERNAL_DOMAIN>` (по формированию доменных имен и среды инсталляции см. раздел 4.2.3.2 данного руководства):
    - Убедиться, что загрузилась страница авторизации;
    - При установке без интеграции с «МойОфис Хранилище» проверить авторизацию тенанта по умолчанию (`admin@<domain>` , где `<domain>` – основной домен контура установки).
    - Проверить, что при удачной авторизации происходит переход на страницу веб-интерфейса почты;
    - Отправить тестовое письмо и убедиться, что оно дошло;
    - Зайти в календарь, создать тестовое событие;
    - Зайти в настройки, изменить любые параметры и убедиться, что настройки сохранены.

4.3.3 Интеграция с «МойОфис Хранилище» (PGS)

Для полноценной интеграции «МойОфис Почта» с компонентом «МойОфис Хранилище» (PGS), необходимо:

1. Заполнить блок интеграции (**integrations: pgs:**) в инвентарном файле PSN 2.0 (подробнее в разделе 4.2.3.2 данного руководства).
2. Настроить DNS контура инсталляции в соответствии с рекомендациями из пункта 4.2.5 данного руководства.

Установка «МойОфис Почта» должна быть завершена **до** создания первого тенанта в системе PGS («МойОфис

Хранилище»). В обратном случае тенант (и пользователи, входящие в него) не будут синхронизированы с почтой.

4.3.4 Интеграция с сервисом TrueConf

4.3.4.1 Настройки сервера «МойОфис Почта»

Для интеграции «МойОфис Почта» с сервисом коммуникаций TrueConf необходимо выполнить следующие действия на стороне сервера инсталляции:

1. Через браузер авторизоваться в сервисе ETCD инсталляции «МойОфис Почта» используя адрес вида:

   ```
   <domain>:8081
   ```

   Где `<domain>` – основной домен установки «МойОфис Почта», `8081` – порт авторизации.

2. Данные для авторизации:

- Логин `psnuser`
- Пароль: значение переменной `etcd_browser_user` из инвентарного файла установки (см. раздел 4.2.3.2 данного руководства)

3. В ETCD Browser установить следующие значения по пути `services/trueconf/` :

   ```
   delete_after: 60
   enabled: True
   url: <trueconf_url>
   ```

   Где `<trueconf_url>` – адрес по которому сервис TrueConf будет доступен всем пользователям (см. раздел 4.3.4.2).

4. На сервере инсталляции «МойОфис Почта» найти конфигурационный файл:

   ```
   <DOMAIN>/opt/poseidon/web_calendar/config.json
   ```

   Где `<DOMAIN>` – основной домен установки «МойОфис Почта».

5. Установить следующие значения в переменных конфигурационного файла:

   ```
   "useConference": true,
   "useTrueconfConference": true,
   ```

6. Перезапустить сервис Docker следующей командой:


```
docker service update psn-frontend_web_calendar --force
```

> Вышеупомянутые действия выполнять не требуется, если настройка была произведена в инвентарном файле до инсталляции.

4.3.4.2 Настройки административной панели TrueConf

- В административной панели TrueConf на вкладке `Веб / Настройки` в разделе `Внешний адрес веб страницы TrueConf Server` необходимо указать адрес, соответствующий значению `<TRUECONF_URL>` из пункта 3 раздела 4.3.4.1 настоящей инструкции.
- Следующим шагом будет заполнение настроек LDAP на вкладке `LDAP / Active Directory` , раздел `LDAP` , кнопка `Настройки LDAP` в административной панели TrueConf. Пример заполнения указан в Таблице 9:

Параметр	Значение
Тип сервера	389 Directory Server
Безопасное соединение	Да
Ручная настройка	Да
Сервер	Сервер инсталляции LDAP-сервиса «МойОфис Почта» (адрес хоста с установленным сервисом 389 Directory Server)
Порт	636
Базовый DN	`ou=People,dc=<domain>,dc=ru` , где `<domain>` – основной домен установки «МойОфис Почта».
Аутентификация	Простая
Имя	`cn=Manager,dc=<domain>,dc=ru` , где `<domain>` – основной домен установки «МойОфис Почта».
Пароль	Значение переменной `ds389_manager_user` из инвентарного файла установки (см. раздел 4.2.3.2 данного руководства)
Включить NTLM-аутентификацию для автоматического входа пользователей домена Active Directory	Да

Таблица 9. Настройки LDAP административной панели TrueConf

Заполнение настроек также необходимо и в разделе `Дополнительно` (см. Таблицу 10):

LDAP Имя	Значение
Login	trueconflogin
Display Name	cn
First Name	givenName
Last Name	sn
Email	mail
Max Results	50000
Filter Disabled	(!(nsrole=cn=nsdisablerole.*))
Group Member	uniqueMember
Filter Login	(trueconflogin=%s)
Filter CallID	(trueconflogin=%S)
Filter Group	(objectClass=GroupOfUniqueNames)
Work Phone	telephoneNumber
Home Phone	homePhone
TrustPartner Attr	trustPartner
FlatName Attr	flatName
TrustedDomain Filter	(objectClass=trustedDomain)
ForeignSecurityPrincipal Filter	(objectClass=foreignSecurityPrincipal)
Trust Enabled	1
Use Avatars	1
Allow Avatar Propagating	1
AddressBook Refresh	900
TimeOut	30
thumbnailPhoto Attr	thumbnailPhoto
jpegPhoto Attr	jpegPhoto
thumbnailPhoto Attr	thumbnailPhoto

Таблица 10. Дополнительные настройки в административной панели TrueConf

Остальные значение следует оставить пустыми. После заполнения всех настроек необходимо нажать кнопку **Применить**. При корректном заполнении всех параметров в разделе `Пользователи / Учетные записи пользователей` загрузится список учетных записей следующего вида (Рисунок 2):

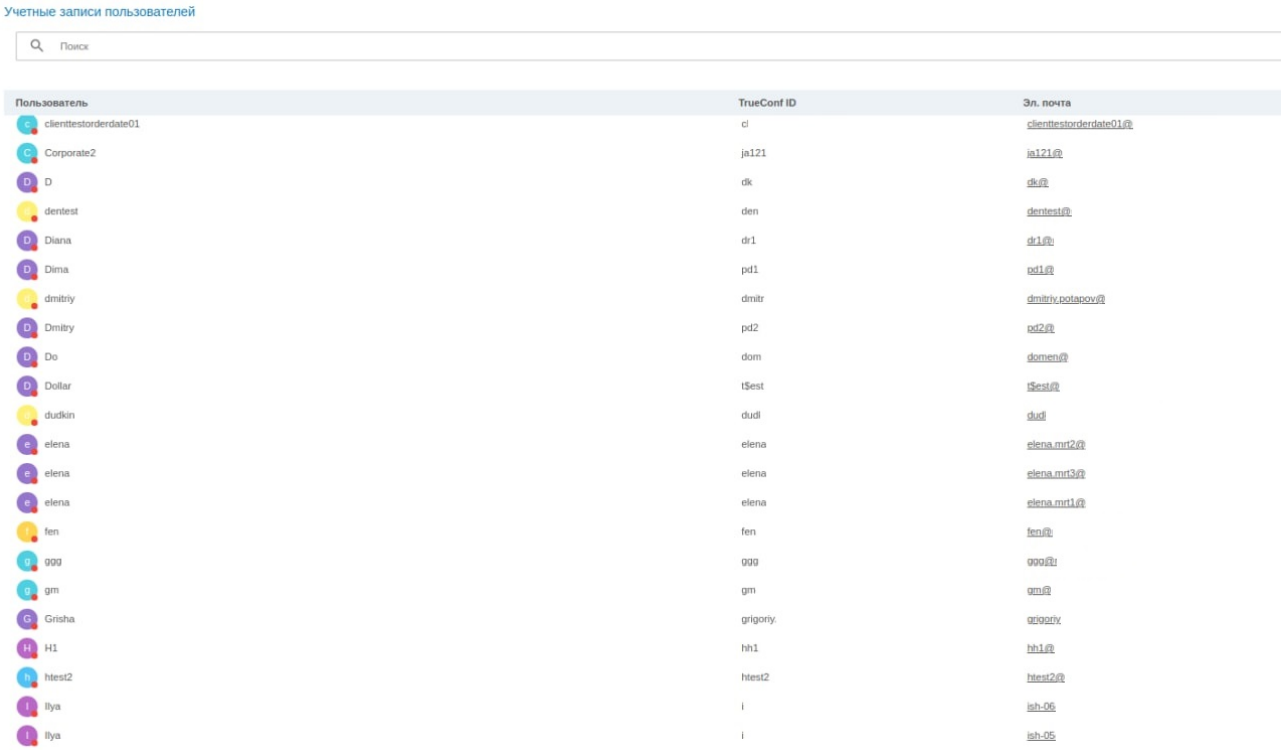

Рисунок 2. Учетные записи «МойОфис Почта» в административной панели TrueConf

4.3.5 Интеграция с Active Directory

При установке «МойОфис Почта» без интеграции с «МойОфис Хранилище» (PGS), Active Directory возможно использовать как базу данных пользователей. Для этого следует заполнить блок интеграции (**integrations: ad:**) в инвентарном файле PSN 2.0 (подробнее в разделе 4.2.3.2 данного руководства).

4.4 Настройка интеграции с Infowatch Traffic Monitor

InfoWatch Traffic Monitor – DLP-система, которая предотвращает утечки конфиденциальной информации на основе полноценного контентного анализа информационных потоков.

Раздел описывает порядок и особенности настройки «МойОфис Почта» и InfoWatch Traffic Monitor для совместной работы. Методы развёртывания DLP-системы различаются в зависимости от рабочей среды (веб-браузер, настольный и мобильный клиент).

4.4.1 Установка InfoWatch Traffic Monitor в разрыв трафика

Метод установки InfoWatch Traffic Monitor в разрыв трафика работает при использовании «МойОфис Почта» в веб-браузере, настольном или мобильном клиентах. Существует два способа перехвата информационных потоков:

- По протоколу SMTP

- По протоколу HTTP/S

4.4.1.1 Перехват SMTP-трафика методом отправки скрытой копии

В результате работы данного метода сервис Postfix, встроенный в систему InfoWatch Traffic Monitor, получает копии писем, отправленных по SMTP-протоколу. Предполагается, что письма, содержащие конфиденциальную информацию (в т.ч. файлы вложений), созданы в клиенте «МойОфис Почта». В DLP-системе создается событие для каждого из писем, информация о которых затем помещается в базу данных.

Визуальная схема работы изображена на Рисунке 3:

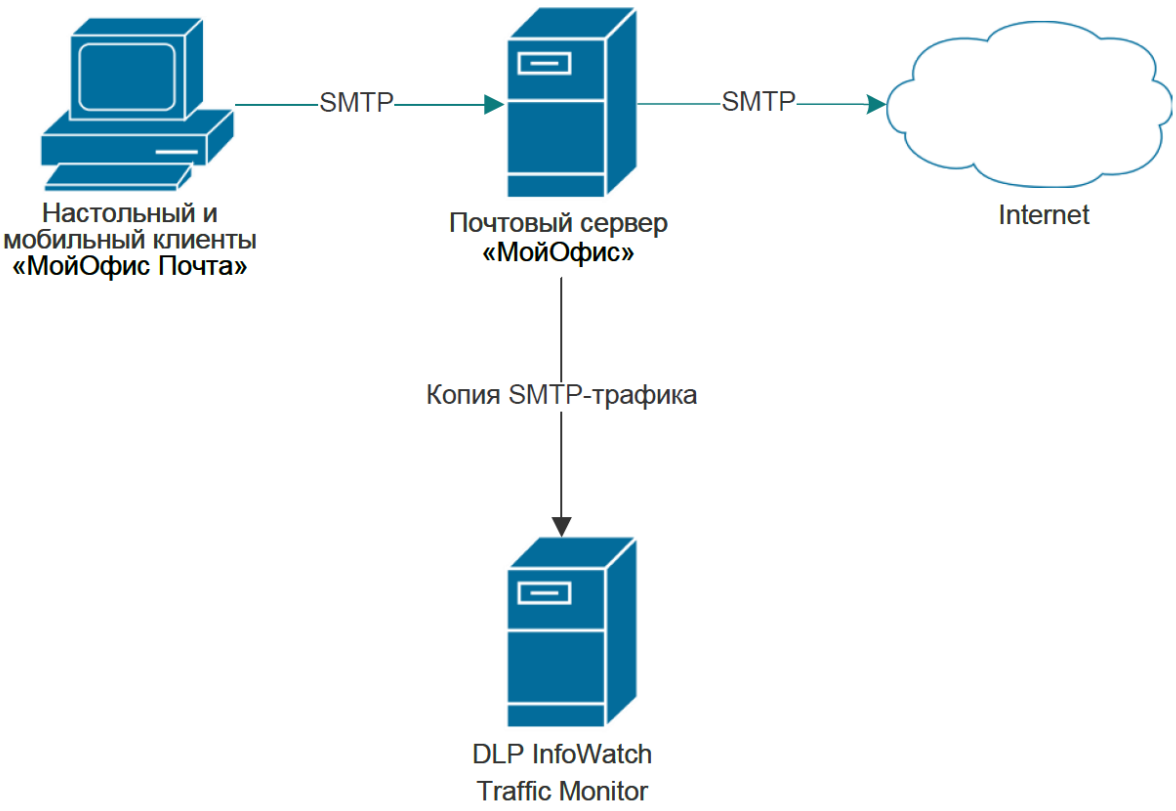

Рисунок 3. Установка DLP Infowatch Traffic Monitor в разрыв (режим “скрытая копия”)

Для настройки перехвата трафика по SMTP-протоколу необходимо настроить правило, отправляющее скрытую копию (BCC) для каждого отправленного письма. Правило настраивается в сервисе Postfix на стороне почтовой системы (сервер «МойОфис Почта» с ролью `mail`). На вышеупомянутом сервере следует найти конфигурационный файл по следующему адресу:

```
/opt/poseidon/postfix/main.cf
```

И прописать в нём следующий параметр:


```
always_bcc = <dlp_mail_address>
```

Где `<dlp_mail_address>` – почтовый адрес домена, MX-запись которого указывает на сервер InfoWatch Traffic Monitor.

После выполнения настройки следует перезапустить контейнеризатор следующей командой:

```
docker service update psn-mail_postfix --force --with-registry-auth
```

4.4.1.2 Перехват HTTP/S-трафика методом отправки почты на корпоративный прокси-сервер

Данный метод актуален только при работе в почтовой системе «МойОфис Почта» через веб-браузер.

Подмену сертификата и разбор HTTPS-трафика осуществляет корпоративный прокси-сервер. После разбора HTTPS-трафика, прокси-сервер отправляет разобранный трафик в виде HTTP по ICAP-протоколу на сервер InfoWatch Traffic Monitor (Рисунок 4).

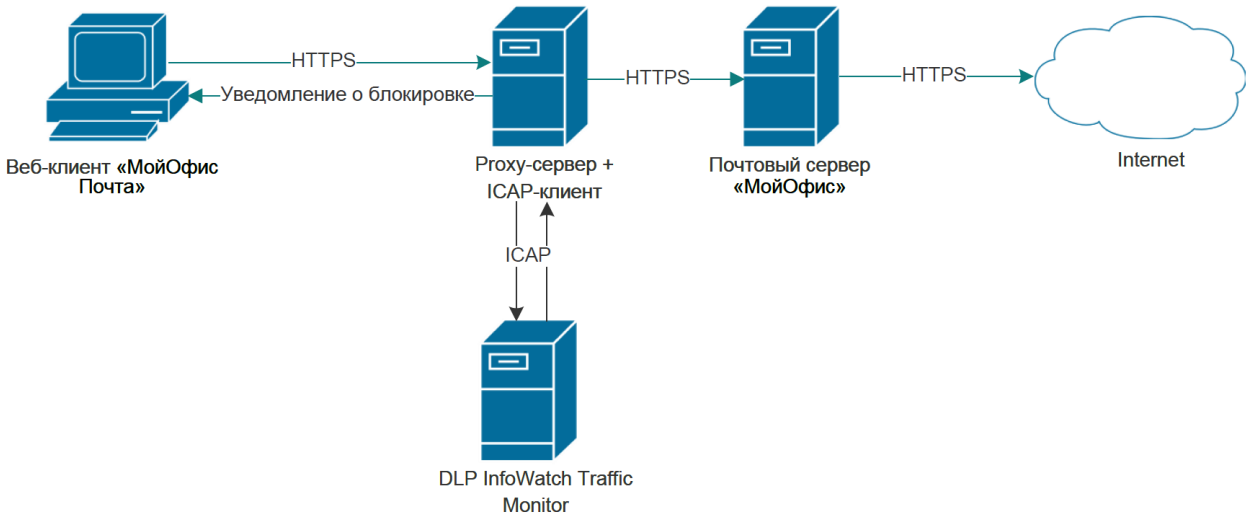

Рисунок 4. Установка DLP Infowatch traffic monitor “в разрыв” (режим блокировки)

Существует два способа работы метода:

- Копия – письма, содержащие конфиденциальную информацию (в т.ч. вложения и изображения) не фильтруются, и их копии отправляются на сервер InfoWatch Traffic Monitor.
- Блокировка – обнаружение конфиденциальной информации происходит на уровне DLP-сервера InfoWatch Traffic Monitor. Далее производится разрешение или запрет на передачу HTTPS-трафика. При блокировке трафика конфиденциальная информация не доходит до сервера «МойОфис Почта».

Более подробно ознакомиться с совместимыми системами и настройкой прокси-сервера возможно в документе «Руководство администратора InfoWatch Traffic Monitor 7.1» (раздел 4.4.2 Перехват трафика, передаваемого по протоколу ICAP).

При использовании данного метода настройки со стороны сервера «МойОфис Почта» не требуется. Для клиента необходимо добавить сертификат прокси-сервера в список доверенных корневых сертификатов браузера каждого рабочего места, контроль исходящего HTTPS-трафика которого планируется.

4.4.2 Установка агента InfoWatch Device Monitor

Агент InfoWatch Device Monitor работает при использовании с системой «МойОфис Почта» в веб-браузере и настольном клиенте. Весь перехваченный по протоколам HTTPS и SMTPS трафик будет отправлен для анализа на сервер Traffic Monitor.

Одним из преимуществ метода установки агента на устройства пользователей является возможность постепенного внедрения анализа трафика в организации. Из недостатков – повышенное внимание к потребностям каждого пользователя. Схема взаимодействия данного метода приведена на Рисунке 5:

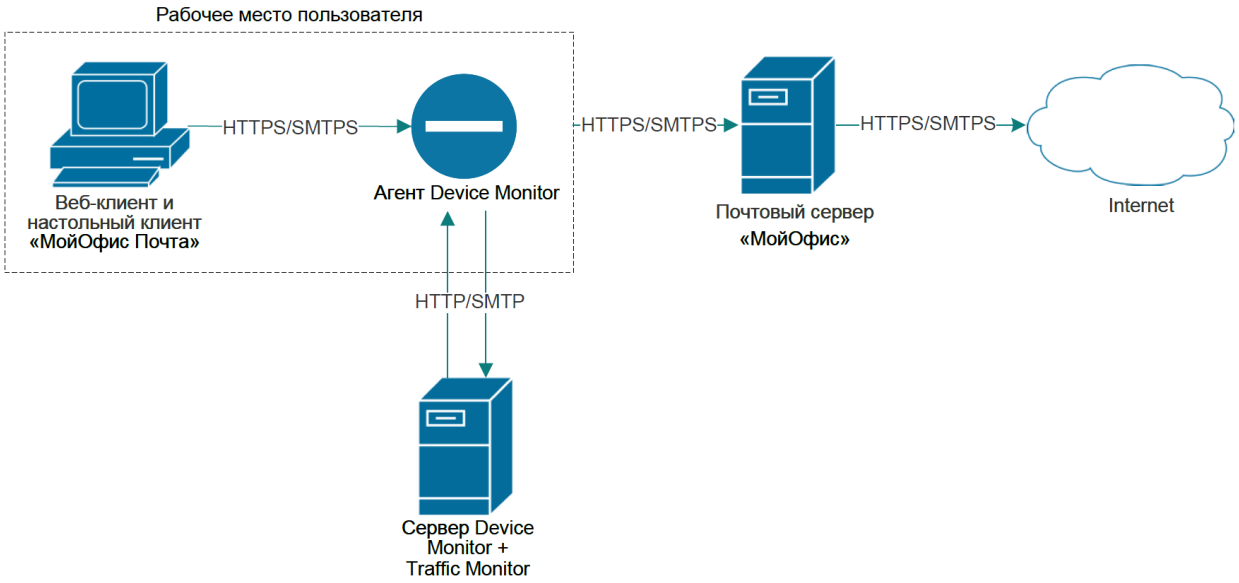

Рисунок 5. Установка агента Infowatch Device Monitor

Обнаружение конфиденциальной информации происходит на уровне агента InfoWatch Device Monitor. При блокировке трафика конфиденциальная информация не доходит до сервера «МойОфис Почта».

Установка агента осуществляется соответственно документу «InfoWatch Traffic Monitor. Руководство пользователя».

После установки агента InfoWatch Device Monitor для почтового клиента «МойОфис Почта», установленного

в ОС Windows необходимо произвести следующие действия:

- На машине пользователя необходимо зайти в оснастку `certlm.msc` (из меню Пуск).
- В дереве сертификатов найти InfoWatch Transparency Proxy Root:

```
Сертификаты – локальный компьютер\Доверенные корневые центры
сертификации\Сертификаты\InfoWatch Transparency Proxy Root
```

- В контекстном меню выбранного сертификата выбрать **Все задачи** - **Экспорт…** и экспортировать выбранный сертификат (в формате .CER, кодировка DER) на доступный локальный или сетевой ресурс.
- В почтовом клиенте «МойОфис Почта» зайти в настройки сертификатов (кнопка - пункт меню **Настройки** - **Приватность и защита** - кнопка **Управление сертификатами**) и нажать кнопку **Импортировать…**
- Выбрать экспортированный ранее сертификат InfoWatch Transparency Proxy Root, в появившемся диалоговом окне проставить галки напротив опций:
  - **Доверять при идентификации веб-сайтов**
  - **Доверять при идентификации пользователей электронной почты**
- Нажать кнопку **ОК** два раза для сохранения настроек.

5 Обновление с PSN 1.0

Процесс обновления «МойОфис Почта» производится в несколько этапов. Исходная инсталляция должна соответствовать следующим параметрам:

- Произведена интеграция с PGS («МойОфис Хранилище»).
- Обеспечен доступ к контейнерам и работающим на их сервисам (LDAP с ролью `FE`, LDAP с ролью `BE`, база данных `MariaDB`).

5.1 Конфигурация без отказоустойчивости

Для начала миграции необходимо создать конфигурационный файл миграции (в формате php), пример которого указан ниже:

```
<?php
define('MYSQL_HOST', '<HOSTNAME>'); // Хост MySQL
define('MYSQL_DB_NAME', '<MYSQL_DB_NAM>');
define('MYSQL_DB_PASSWORD', '<MYSQL_PASSWORD>');
define('MYSQL_LOGIN', '<MYSQL_LOGIN>');
define('MYSQL_PORT', '<MYSQL_PORT>');
define('PGS_URL', '<PGS_URL>'); // PGS Euclid endpoint
define('PGS_LOGIN', '<LOGIN>');
define('PGS_PASSWORD', '<PASSWORD>');
define('TRITON', '<TRITON>'); // Main URL
define('USERS_FILE', '<USERS_FILE>');
define('PSN_PASSWORD_KEY', '<PSN_PASSWORD_KEY>'); //inv_db_aurora_password_key
define('PBM_HOST', '<PBM_HOST>');
define('HOST', '<HOST>');
define('DEFAULT_TENANT', '<DEFAULT_TENANT>'); // Tenant for migrating resources
define('OLD_CAB_HOST', '<OLD_CAB_HOST>'); // Cab ldap
define('OLD_CAB_PASSWORD', '<OLD_CAB_PASSWORD>');
define('OLD_CAB_BIND_DN', '<OLD_CAB_BIND_DN>');
define('OLD_CAB_PORT', '<OLD_CAB_PORT>');
define('OLD_CAB_SEARCH_BASE', '<OLD_CAB_SEARCH_BASE>');
define('OLD_USERDB_HOST', '<OLD_USERDB_HOST>'); // Userdb ldap
define('OLD_USERDB_PASSWORD', '<OLD_USERDB_PASSWORD>');
```

```
define('OLD_USERDB_BIND_DN', '<OLD_USERDB_BIND_DN>');
define('OLD_USERDB_PORT', '<OLD_USERDB_PORT>');
define('OLD_USERDB_SEARCH_BASE', '<OLD_USERDB_SEARCH_BASE>');
define('RECID_PERIOD', <RECID_PERIOD>);
define('EVENT_PERIOD', <EVENT_PERIOD>);
?>
```

Следующим шагом необходимо смонтировать конфигурационный файл в сервис triton:

```
docker service update --mount-add
type=bind,source=<SOURCE>/config.php,target=/opt/triton/db/config.php psn-backend_triton
```

Где `<SOURCE>/config.php` – путь до конфигурационного файла на хосте.

Команда запуска миграции:

```
docker exec -i $(docker ps -qf name=triton) bash -c 'php /opt/triton/db/main.php'
```

Лог выполняемого процесса переноса будет доступен по адресу:

```
/opt/poseidon/logs/triton/migrations.log
```

При успешном выполнении миграции процесс завершится без ошибок.

5.2 Конфигурация с отказоустойчивостью

Для процедуры миграции с кластерной конфигурации PSN 1.0 необходимо выбрать сервер роли `backend`, с которого будет происходит миграция. После этого командой удалить swarm-метку соседней ноды сервиса triton и уменьшить количество реплик до 1:

```
docker node update --label-rm backend <SERVER>
docker service scale psn-backend_triton=1
```

Где `<SERVER>` – имя сервера, на котором swarm-метка будет удалена. В результате сервис triton должен остаться в одном экземпляре, пример:

```
whejdaqz79de psn-backend_triton replicated 1/1
psn-private-registry:5001/poseidon/triton:1.0.39-858
```


Дальнейшие действия по настройке и запуску миграции аналогичны алгоритму миграции из конфигурации без отказоустойчивости.

После работы миграции, необходимо произвести обратные действия по возвращению swarm-метки и количества экземпляров сервиса triton следующей командой:

```
docker node update --label-add backend:true <SERVER>
docker service scale psn-backend_triton=2
```

Финальным шагом необходимо убедиться, что все сервисы запущены и работают, пример работающей конфигурации:

```
psn-backend_autoconfig 2/2
psn-backend_avatars 2/2
psn-backend_pbm 2/2
psn-backend_pfm 2/2
psn-backend_triton 2/2
psn-etcd_browser 1/1
psn-etcd_etcd 3/3
psn-etcd_etcd1 1/1
psn-etcd_etcd2 1/1
psn-etcd_etcd3 1/1
psn-frontend_web_calendar 2/2
psn-frontend_web_contacts 2/2
psn-frontend_web_mail 2/2
psn-ldap_ldap 2/2
psn-mail_clamav 2/2
psn-mail_dovecot 2/2
psn-mail_freshclam 2/2
psn-mail_postfix 2/2
psn-mail_rspamd 2/2
psn-nginx-proxy_nginx 2/2
psn-postgres_haproxy 2/2
psn-postgres_postgres1 1/1
psn-postgres_postgres2 1/1
```



```
psn-redis_redis-master 1/1
psn-redis_redis-sentinel 2/2
psn-redis_redis-slave 1/1
psn-syslog_ng_syslog-ng 5/5
```


6 Создание резервных копий

6.1 Создание резервных копий службы каталогов LDAP

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

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

Где:

- `<external_domain>` – зарегистрированный домен инсталляции.

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

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

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

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

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

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

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

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

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

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

6.2 Переустановка службы каталогов LDAP

После проведения процедуры резервирования, описанной в разделе 6.1, необходимо удалить соответствующие службе `ldap` элементы Docker – stack и volume следующими командами:

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

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

Следующим шагом будет изменение hostname в группе хостов `ldap` инвентарного файла установки согласно разделу 4.2.3.1 данного руководства и запуск установки с параметром `-t ldap` :

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

> Команда переустановит **только** службу каталогов.

После переустановки службы необходимо восстановить данные из резервной копии, согласно инструкциям из раздела 6.1 данного руководства.

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.

