МойОфис

Частное Облако

Руководство по установке

ХРАНИЛИЩЕ (PGS)

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Мой Офис «Частное Облако»

Мой Офис «Хранилище»

РУКОВОДСТВО ПО УСТАНОВКЕ

2021.04

На 38 листах

Москва

2021

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам. Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

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

Содержание

Перечень сокращений, терминов и определений

Сокращение, термин	Расшифровка и определение
AD	MS Active Directory
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)
Docker	ПО для автоматизации развёртывания и управления приложениями в среде виртуализации
Docker Registry	Масштабируемое серверное приложение для хранения и распространения контейнеров Docker
DNS	Domain Name System, система доменных имён
Inventory file	Инвентарный файл Ansible с перечислением ролей и их IP адресов
Logos	Сервис быстрого обмена сообщениями, документами и файлами внутри организации или предприятия; корпоративный мессенджер, входящий в «МойОфис Частное Облако»
MD5-хеш (hash)	Контрольная сумма, предназначенная для проверки целостности файла
PGS	Pythagoras, альтернативное название программного продукта «МойОфис Хранилище»
PSN	Poseidon, приложение почты, календаря и контактов (оно же «МойОфис Почта»)
REST API	Архитектурный стиль взаимодействия компонентов распределённого приложения в сети

Сокращение, термин	Расшифровка и определение
S3 хранилище	Сервис хранения объектов, предлагаемый поставщиками облачных услуг
SSH	Secure Shell, «безопасная оболочка»
SSO	Single Sign-On, технология единого ввода
URL	Uniform Resource Locator, единый указатель ресурса
XFS	64-битная журналируемая файловая система
Yum	Менеджер программных пакетов для дистрибутивов Linux
БД	База данных
Вендор (vendor)	Поставщик брендированного продукта
Кластер (cluster)	Объединенная группа серверов
ЕСИА	Единая система идентификации и аутентификации
Оверкоммит (overcommit)	Опция гипервизора по избыточной аллокации памяти для виртуальных машин
ОС	Операционная система
Персистентность	Свойство структур данных, сохраняющих свои состояния и доступ к этим состояниям
Плейбук (playbook)	Набор последовательных инструкций для выполнения команд Ansible
ПО	Программное обеспечение
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

«МойОфис Хранилище» - продукт для создания централизованного хранилища данных в крупных организациях и предприятиях, обеспечивающий быстрый доступ к документам с компьютеров, мобильных устройств и из веб-браузеров. «МойОфис Хранилище» входит в состав программного пакета для организации виртуальной рабочей среды «МойОфис Частное Облако» и представляет собой пользовательский интерфейс к системе хранения МойОфис.

> Подробнее о «МойОфис Частное Облако» можно прочитать на официальной странице продукта.

Функционал, предоставляемый «МойОфис Хранилище» включает в себя:

- Поддержку систем виртуализации KVM и VMware vSphere ESXi;
- Поддержку работы с S3-совместимыми хранилищами;
- Совместимость с Active Directory;
- Возможность подключения учетных записей и последующей авторизации через ЕСИА;
- Широкие возможности по работе в собственном домене;
- Интеграцию с другими компонентами ПО «МойОфис Частное облако»: CO (Редакторы), PSN (Почта) и Logos (Корпоративный мессенджер).

1.2 Требования к квалификации персонала

Администратор «МойОфис Хранилище» 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.
- Опыт работы с командной строкой ОС Linux:

    - Знания в объеме курсов RedHat RH124, RH134, RH254;
    - Знания в объеме, достаточном для сдачи сертифицированного экзамена RedHat EX300.
- Опыт работы с системой контейнеризации Docker:
    - Установка Docker;
    - Запуск / остановка / перезапуск контейнеров;
    - Работа с реестром контейнеров;
    - Работа с VMWare vSphere ESXi 6.5 и выше;
    - Получение конфигурации контейнеров;
    - Сеть в Docker, взаимодействие приложений в контейнерах;
    - Решение проблем контейнерной виртуализации.
- 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 администрирования:
    - СУБД ArangoDB;
    - Файловой системы GlusterFS;
    - SSO-сервиса Keycloak;
    - СУБД PostgreSQL;
    - Поисковой системы ElasticSearch;
    - СУБД Redis;
    - Обработчика сообщений RabbitMQ;
    - Сервера конфигурации ETCD.
- Опыт работы с системой автоматизации развертывания Ansible.

1.3 Системные требования

- Должен быть установлен один из следующих поддерживаемых дистрибутивов операционной системы:
    - Centos 7.9

> Рекомендуемый дистрибутив, поддержка более поздних версий не гарантируется.

  - Astra Linux Орел 2.12
  - ALT Linux 9.0

- Скорость сетевой подсистемы - 1 Gbit/s или выше.
- Рекомендуемая система виртуализации - VMWare ESXi.
- В Таблице 2 приведены характеристики аппаратного обеспечения для установки конфигурации без отказоустойчивости.

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

	CPU	RAM (Gb)	HDD (Gb)
Минимальная	8	16	50 + Квота пользователей на использование дискового пространства
Рекомендованная	32	64	100 + Квота пользователей на использование дискового пространства + База данных

Таблица 2. Характеристики конфигурации без отказоустойчивости

1.4 Ограничения

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

2 Описание архитектуры «МойОфис Хранилище»

2.1 Общая архитектурная схема

«МойОфис Хранилище» является составным компонентом программного продукта «МойОфис Частное Облако», в который также входят:

- CO (Редакторы) - программные решения для редактирования текста, таблиц и презентаций.
- PSN («МойОфис Почта») - почтовый сервер.
- Logos («МойОфис Логос») - коммуникационный сервис (мессенджер)

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

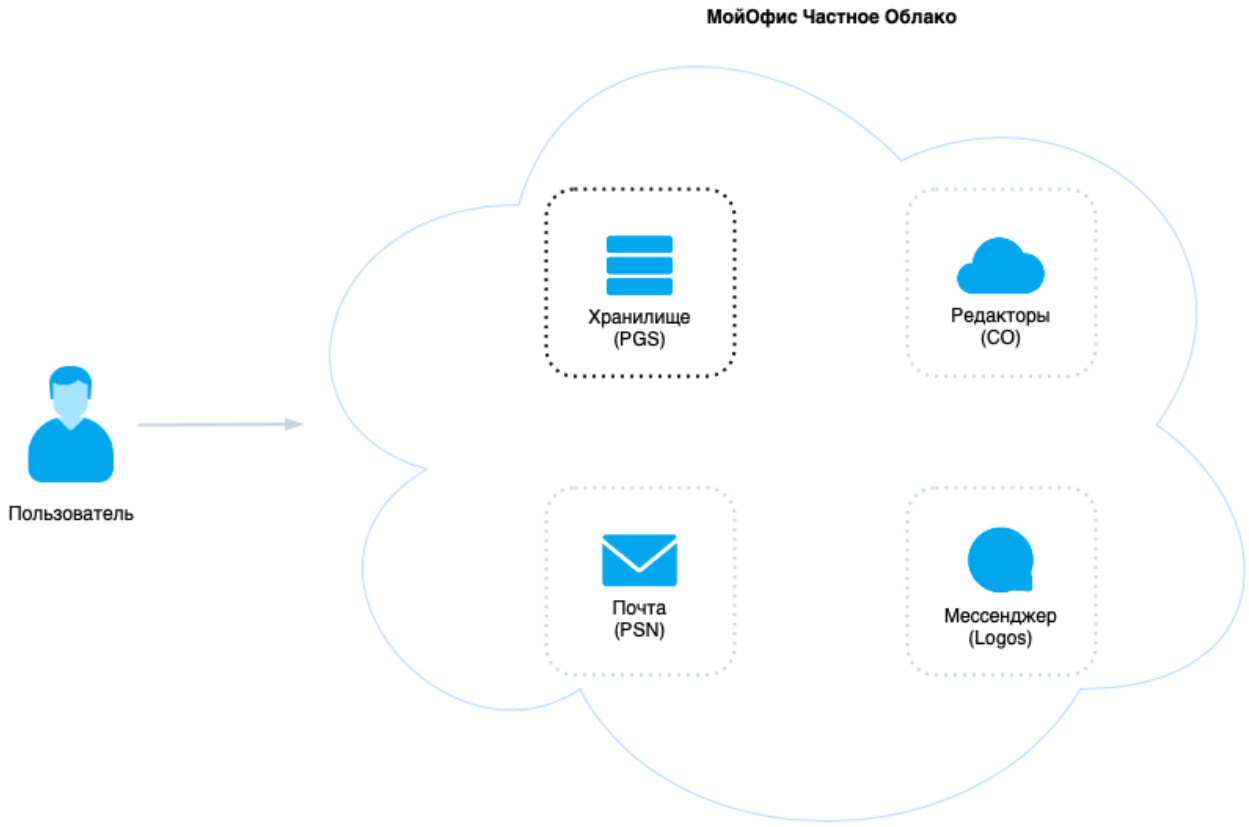

Рисунок 1. Общая архитектурная схема «МойОфис Частное Облако».

> Все элементы «МойОфис Частное Облако» возможно сконфигурировать для внутреннего взаимодействия, в таком случае порядок установки компонентов не важен. В задачу администратора входит корректное указание переменных и доменных имен в конфигурационных файлах, необходимые связи и зависимости инсталляционные пакеты образуют сами. Более подробно об этом указано в соответствующих руководствах по установке компонентов «МойОфис Частное Облако».

2.2 Детальная архитектурная схема

Внутренняя структура «МойОфис Хранилище» представляет собой набор сервисов, обеспечивающих работу ПО и взаимодействие с другими компонентами «МойОфис Частное Облако». Более подробно сервисы (представленные в виде инсталляционных ролей) описаны в параграфе 4.2.1 данного руководства. Детальная архитектурная схема «МойОфис Хранилище» приведена на Рисунке 2.

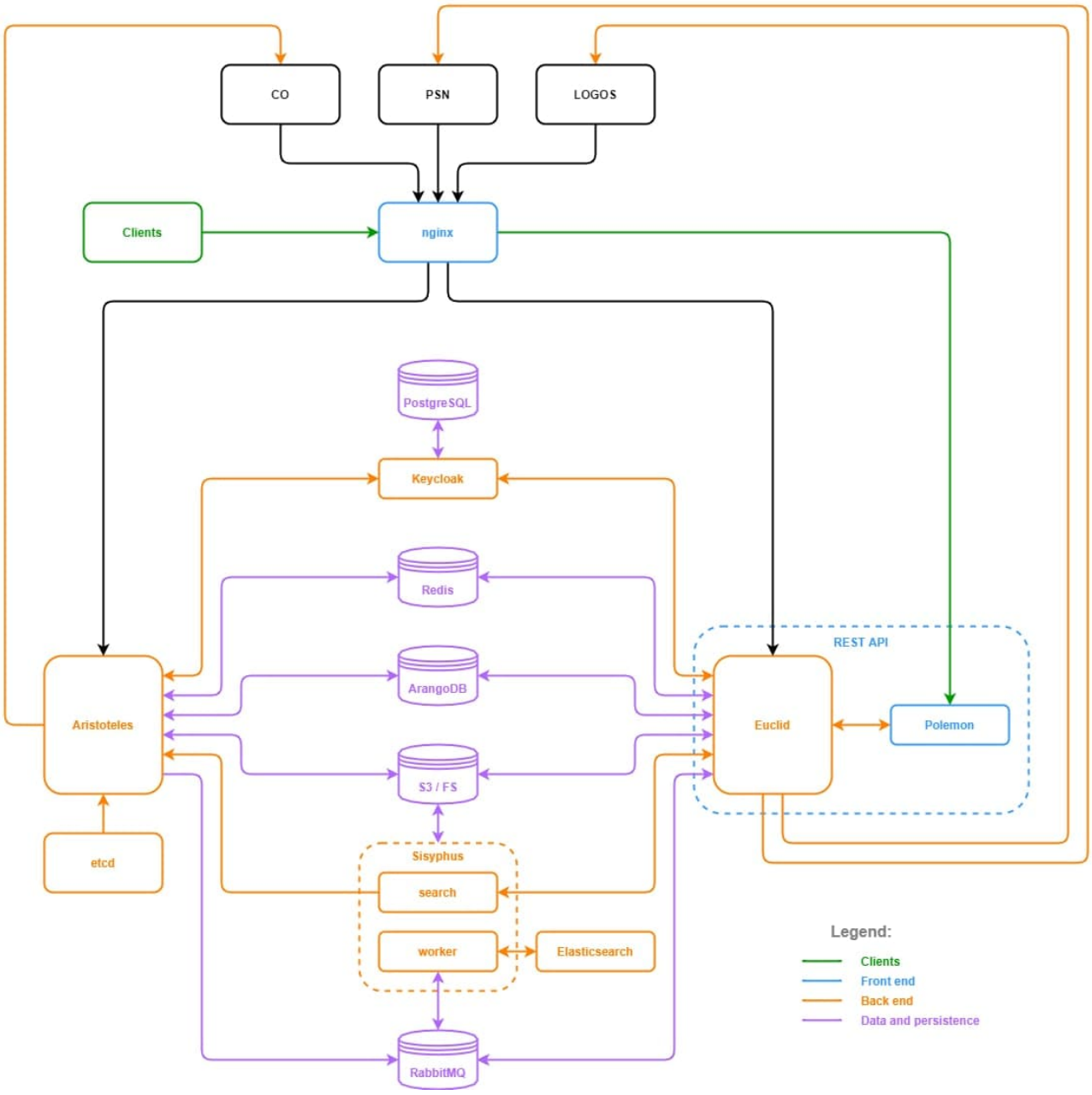

Рисунок 2. Архитектурная схема «МойОфис Хранилище».

3 Типовые схемы установки «МойОфис Хранилище»

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.

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 Хранилище» 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 резервному копированию «МойОфис Хранилище».

4 Первичная установка

4.1 Состав дистрибутива

Дистрибутив «МойОфис Хранилище» представляет собой инсталляционный архив в формате *.tgz и включает в себя:

1. Набор Ansible плейбуков для развертывания ролей;
2. Архив образа Docker Registry;
3. Набор контейнеров для запуска «МойОфис Хранилище»;
4. Файл MD5-хеша.

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. Ниже следует список данных ролей для PGS:

1. Pythagoras – роль, разворачивающая главные сервисы PGS:
   - Aristoteles – сервер приложений, обеспечивающий большую часть работы логики ПО.
   - Euclid – REST API сервис для администрирования ПО.
   - Sisyphus – сервис поиска по содержимому документов.
   - Polemon – сервис веб-администрирования Euclid (веб-интерфейс).
   - Logos-sync – сервис для синхронизации с БД мессенджера Logos.
2. Keycloak – SSO сервис.
3. Postgres (PostgreSQL) – база данных для сервиса авторизации Keycloak.
4. ArangoDB – база данных метаданных файлов.
5. Redis – база данных “ключ-значение” для не персистентных данных.
6. RabbitMQ – очередь сообщений.
7. ElasticSearch – поисковая система.
8. Docker Registry – сервис для хранения и распространения контейнеров Docker.
9. ETCD – сервер конфигурации. Также используется базой данных Postgres при её запуске в кластерном режиме для обмена информацией о состоянии и конфигурации кластера.
10. nginx – прокси-сервер.

11. Minio – сервис облачного объектного хранилища (решение от «МойОфис» с S3-совместимым API).
12. Common – базовые настройки для машин, установка необходимых пакетов и зависимостей.
13. Glusterfs – распределённая масштабируемая файловая система для объединения хранилищ данных, находящихся на разных серверах в одну сетевую файловую систему.
14. syslog-ng – сервис сбора логов работы компонентов программного комплекса.

> Таким образом, роли соответствуют архитектурным элементам «МойОфис Хранилище». Для более наглядного понимания структуры программного пакета можно обратиться к параграфу 2.2 данного руководства.

4.2.2 Подготовка инфраструктуры установки

Перед началом установки необходимо настроить DNS для разрешений следующих имен в адрес, куда будет установлен сервер nginx:

Доменное имя	Хост	Описание
`admin-<ENV>.<DEFAULT_DOMAIN>`	`nginx host`	Адрес веб-панели администрирования PGS
`pgs-<ENV>.<DEFAULT_DOMAIN>`	`nginx host`	Адрес точки входа для API

Переменные `<ENV>` и `<DEFAULT_DOMAIN>` заполняются в соответствии с разделом 4.3.2 данного руководства, `nginx host` соответствует адресу, указанному в инвентарном файле для роли `nginx` (подробнее в разделе 4.3.1).

Адрес вида `admin-<ENV>.<DEFAULT_DOMAIN>` должен быть доступен извне.

4.2.2.1 Подготовка сервера, с которого будет производиться инсталляция дистрибутива

Для подготовки к инсталляции сервера, с которого будет производиться инсталляция (в дальнейшем - **сервер-оператор**), нужно выполнить следующие действия:

1. Необходимо скачать и инсталлировать минимальный серверный вариант ОС одной из рекомендованных версий (см. параграф 1.3 данного руководства).
2. Для всех операционных систем требуется наличие установленного Python версии 3 с модулем pip.
3. Для CentOS требуется отключить систему SELinux.

4. С сервера-оператора 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.

5. На сервер-оператор должен быть инсталлирован пакет Ansible версии 2.10.

   > Подробная документация по установке Ansible

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

7. 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).

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

Для подготовки **целевых серверов** к установке для них необходимо выполнить пункты 1-3 и 6-7 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.

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

Если сервер-оператор и целевые серверы расположены в локальной сети и не имеют прямого доступа в Интернет, то, помимо вышеупомянутых действий, необходимо предустановить на них пакеты Yum, указанные в Таблице 3 (названия приведены для CentOS 7.7):

Пакет	Рекомендуемый репозиторий
python3	https://www.python.org/downloads/source/
libselinux-python3	https://pkgs.org/download/libselinux-python3
docker-ce	https://download.docker.com/linux/centos/docker-ce.repo
docker-ce-cli	https://download.docker.com/linux/centos/dockerce.repo
containerd.io	https://download.docker.com/linux/centos/dockerce.repo
python2-pip	https://pypi.org/project/pip/
rsync	https://rsync.samba.org/

Пакет	Рекомендуемый репозиторий
Пакеты Python 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/

Таблица 3. Пакеты Yum для предустановки на серверы без доступа в Интернет.

4.2.2.4 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_PGS_XXXX.XX.md5
```

> 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_PGS
tar xf MyOffice_PGS_XXXX.XX.tgz -C install_MyOffice_PGS
cd install_MyOffice_PGS
```

> Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

3. Для корректной работы веб-интерфейса «МойОфис Хранилище» необходима установка соответствующих SSL-сертификатов. Данные сертификаты (в *.pem и* .key формате) следует поместить в папку `certificates` , созданную в корневом каталоге установки. Пример:

```
~\MyOffice_PGS_XXXX.XX\certificates\server.key
```

4.3 Настройка параметров установки

Для конфигурации установки необходимо открыть **инвентарный файл** (inventory file), находящийся по адресу:

```
~\MyOffice_PGS_XXXX.XX\inventory\hosts-sa.yaml
```

(для конфигурации без отказоустойчивости) или

```
~\MyOffice_PGS_XXXX.XX\inventory\hosts-hl.yaml
```

(для кластерной инсталляции) в текстовом редакторе и заполнить секции `hosts` и `vars` в соответствии с дальнейшими инструкциями.

> Инвентарный файл использует формат .yaml, более подробно о синтаксисе можно прочитать в документации Ansible.

4.3.1 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:

```
pythagoras:
   hosts:
      host.example.com
```

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

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:
    docker_registry:
      hosts:
        host.example.com:
    pythagoras:
      hosts:
        host.example.com:
    keycloak:
      hosts:
        host.example.com:
    arangodb:
      hosts:
        host.example.com:
          volume_device_arangodb: "False"
          volume_device_arangodb_path: "/dev/disk/by-uuid/<UUID>"
    redis:
      hosts:
        host.example.com:
    rabbitmq:
      hosts:
        host.example.com:
    elasticsearch:
      hosts:
        host.example.com:
          volume_device_elasticsearch: "False"
          volume_device_elasticsearch_path: "/dev/disk/by-uuid/<UUID>"
    postgres:
      hosts:
        host.example.com:
          volume_device_postgres: "False"
          volume_device_postgres_path: "/dev/disk/by-uuid/<UUID>"
    etcd:
```

```
      hosts:
        host.example.com:
    nginx:
      hosts:
        host.example.com:
    minio:
      hosts:
        host.example.com:
          volume_device_minio: False
          volume_device_minio_path:
["/dev/disk/by-uuid/<UUID>","/dev/disk/by-uuid/<UUID>", "...", "..."]
```

> Сервис `minio` не рекомендуется использовать при инсталляции без отказоустойчивости ввиду нецелесообразности данного действия. Но если возникает необходимость, то необходимое минимальное количество дисков на хосте должно составлять 4.

В режиме **кластерной инсталляции** в инвентарном файле указывается несколько хостов (адресов серверов) в соответствующей группе. На данный момент поддерживается кластеризация для следующих сервисов (рядом указано необходимое количество хостов для работы кластера):

- Pythagoras: 2 хоста.
- Postgres: 2 хоста.
- Keycloak: 2 хоста.
- ArangoDB: 2 хоста для серверов баз данных (группа `arangodb`) и 3 хоста для агентов, обеспечивающих функционирование кластера (группа `arangodb_agent`). При заполнении данной группы хостов кластерная установка ArangoDB запускается автоматически.
- redis: 2 хоста.
- RabbitMQ: 2 хоста.
- Elasticsearch: 3 хоста.
- etcd: 3 хоста.
- nginx: 2 хоста.
- Minio: 3 хоста (рекомендуется).

Пример конфигурации (фрагмент инвентарного файла `hosts-hl.yaml`):

```
    keycloak:
      hosts:
        host.example.com:
        host-2.example.com:
    arangodb:
      hosts:
        host.example.com:
          volume_device_arangodb: "False"
          volume_device_arangodb_path: "/dev/disk/by-uuid/<UUID>"
        host-2.example.com:
          volume_device_arangodb: "False"
          volume_device_arangodb_path: "/dev/disk/by-uuid/<UUID>"
    arangodb_agent:
      hosts:
        host.example.com:
          volume_device_agent: False
          volume_device_agent_path: "/dev/disk/by-uuid/<UUID>"
        host-2.example.com:
          volume_device_agent: False
          volume_device_agent_path: "/dev/disk/by-uuid/<UUID>"
        host-3.example.com:
          volume_device_agent: False
          volume_device_agent_path: "/dev/disk/by-uuid/<UUID>"
    minio:
      hosts:
        host.example.com:
          volume_device_minio: False
          volume_device_minio_path:
["/dev/disk/by-uuid/<UUID>","/dev/disk/by-uuid/<UUID>"]
        host-2.example.com:
          volume_device_minio: False
          volume_device_minio_path:
["/dev/disk/by-uuid/<UUID>","/dev/disk/by-uuid/<UUID>"]
```

```
    syslog: # remove this group in order to disable syslog service
      hosts:
        host.example.com:
    co_lb:
      hosts:
        co-lb-1.example.com:
        co-lb-2.example.com:
    co_auth:
      hosts:
        co-auth-1.example.com:
        co-auth-2.example.com:
```

- Группа хостов `arangodb_agent` используется для кластерной инсталляции с использованием агентов и имеет следующую особенность: для нее необходимо выделить как минимум **3** отдельных хоста (или больше, но нечётное число). В ином случае, группу следует оставить не заполненной:

```
    arangodb_agent:
      hosts:
```

При указании `storage.type = "fs"` (см. раздел 4.3.2 данного руководства), группа хостов `minio` не заполняется и имеет следующий вид:

```
    minio:
      hosts:
```

- Также следует обратить дополнительное внимание на роли `arangodb` , `arangodb_agent` , `elasticsearch` , `postgres` и `minio` : 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).
3. В случае установки `postgres` в кластерном режиме использование блочных устройств также является необходимостью. Таким образом, переменные `volume_device_postgres` должны принимать значения `"True"` для каждой хост-машины в группе `postgres` (что показано в примере заполнения инвентарного файла выше).

   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 случае с ролью `minio` на каждом хосте необходимо указать как минимум 2 дисковых ресурса в квадратных скобках, двойных кавычках и через запятую:

```
volume_device_minio_path: ["/dev/disk/by-uuid/<UUID>","/dev/disk/by-uuid/<UUID>"]
```

- Сервису `syslog` в инвентарном файле присваивается хост, на котором будут храниться логи, собираемые со всех серверов установки. Пути к логам будут выглядеть следующим образом:

```
/var/log/pgs/<service_name>/<element>.log
```

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.

- В случае кластерной установки модуля CO требуется настройка балансировщика нагрузки между PGS и его auth-нодами. Для этого в инвентарном файле PGS предусмотрены две группы:
  - `co_lb` - группа хостов, на которых будет установлен и настроен сервис балансировки нагруз-

ки keepalived.

- `co_auth` - группа, в которой нужно указать сетевые адреса auth-нод модуля CO.

Кроме групп, в инвентарном необходимо указать 3 дополнительных переменных в блоке **co**, о чем подробнее в следующем разделе руководства.

Дополнительная информация по интеграции с CO указана в разделе 4.6.4.

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

4.3.2 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 4 данного руководства.

> Все параметры переменных необходимо указывать в двойных кавычках.
> Рекомендуется использовать надёжные пароли, в этом может помочь утилита `pwgen 10 1` .

Переменная	Значение и способ заполнения
`DEV_MODE`	*Developers 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).
`DEFAULT_DOMAIN`	Зарегистрированный домен инсталляции «МойОфис Хранилище». Для корректной работы необходим установленный актуальный SSL-сертификат (см. параграф 4.2.2.1 данного руководства).
`ENV`	Окружение инсталляции. Данный параметр определяет элемент доменного имени инсталляции и предназначен для разграничения доступа к сервисам PGS.

Переменная	Значение и способ заполнения
`NGINX_HTTPS_EXT_PORT`	Порт nginx, по которому будет осуществляться доступ к сервисам. Значение по умолчанию - `443` . Его следует поменять в ситуации, когда роль `nginx` инсталляции PGS и роль `openresty-lb-core-auth` CO (Редакторов «МойОфис») совмещены на одной виртуальной машине, и данный порт уже используется инсталляцией CO.

> Таким образом, после заполнения вышеупомянутых переменных будет сформированы адреса вида `https://admin-<ENV>.<DEFAULT_DOMAIN>: <NGINX_HTTPS_EXT_PORT>` , по которым в дальнейшем будет осуществляться доступ к сервисам PGS

Переменная	Значение и способ заполнения
`CUSTOM_CA`	Заполняется при использовании самоподписанных сертификатов, допустимые значения: `True` или `False` . При установлении значения `True` файл ключа (например, формате .pem) кладется в папку `Certificates` в корневой директории установки (см. пункт 4.2.2.4 данного руководства).
`KEYCLOAK_PASSWORD`	Пароль для пользователя PGS в Keycloak (Администратор Master Realm).
`KEYCLOAK_REALM_PASSWORD`	Внутренний пароль для администраторов тенантов Keycloak (используется только для сервисного обслуживания системы).
`KEYCLOAK_POSTGRES_PASSWORD`	Пароль БД PostgreSQL (используется как хранилище для Keycloak).
`ARANGODB_PASSWORD`	Пароль пользователя PGS в ArangoDB.

Переменная	Значение и способ заполнения
`ARANGODB_JWT_SECRET`	Переменная, используемая в режиме кластерной установки ArangoDB для коммуникации между элементами системы (агентами, координаторами и серверами баз данных). Генерируется пользователем аналогично другим сервисным паролям (например, утилитой `pwgen`).
`RABBITMQ_PASSWORD`	Пароль пользователя RabbitMQ.
`REDIS_PASSWORD`	Пароль доступа в Redis.
`SEARCH_CONTENT`	Параметр, позволяющий активировать и деактивировать поиск по содержимому документов. Принимает значения `True` (по умолчанию) и `False`.
`PATRONI_REPLICATION_PASSWORD`	Пароль для репликации БД PostgreSQL.
Блок **default_tenant:**	Предназначен для создания тенанта по умолчанию, необходимого для дальнейшей работы с пользователями в веб-интерфейсе PGS.
`ADMIN_PASSWORD:`	Пароль администрирования тенанта.*Обязательный параметр, без его указания тенант создан не будет.*
`ADMIN_RECOVERY_EMAIL:`	Почта для восстановления доступа к тенанту. *Обязательный параметр, без его указания тенант создан не будет.*
`MAX_USERS:`	Количество пользователей в тенанте, значение по умолчанию `1000`.
`ADMIN_USERNAME:`	Пользовательское имя администратора. значение по умолчанию `admin`
`QUOTA_PER_USER:`	Выделенное пользователю место на хранилище, указывается в байтах, значение по умолчанию `1000000000` (~1 GB)

Переменная	Значение и способ заполнения
`storage: type:`	Выбор типа системы хранения файлов, доступны значения `fs` и `s3` (файловая система и файловый хостинг, соответственно).
`filesystem: path:`	Путь до файловой системы хранения, если используется `storage.type = "fs"` .
Блок **s3**	Параметры доступа к хранилищу s3, если используется `storage.type = "s3"` . Информацию по заполнению переменных следует запросить у хостинг-провайдера, ниже приведены указания для заполнения при использовании сервиса Minio от «МойОфис».
`minio_used:`	`True` - если используется сервис Minio от «МойОфис», `False` - если используется стороннее s3-хранилище.
`endpoint:`	Url доступа к сетевому хранилищу. В случае использования Minio, выглядит следующим образом: `http://pgs-<ENV>.<DEFAULT_DOMAIN>:9000` .Значения `<ENV>` и `<DEFAULT_DOMAIN>` соответствуют указанным в начале таблицы.
`secret_key:`	При использовании Minio, задается администратором при установке, минимальная длина - 8 символов.
`access_key:`	При использовании Minio, задается администратором при установке, минимальная длина - 8 символов.
`bucket:`	Сущность, представляющая собой отдельную директорию для хранения пользовательских данных. При использовании Minio, к заполнению обязательна - указывается произвольное имя, директория создается в корневой папке сама.

Переменная	Значение и способ заполнения
`service_name:`	При использовании Minio указывается значение `s3` .
`region_name:`	При использовании Minio указывается значение `myoffice` .
`acl:`	Сущность для разграничения прав доступа, в случае с Minio необязательна к заполнению.
`system: TIMEZONE:`	Временная зона (часовой пояс) установки. Значение по умолчанию `"Europe/Moscow"` Список допустимых значений находится по ссылке.
Блок **co**	Переменные, которые необходимо заполнить для интеграции с компонентом CO (Редакторы) программного пакета «МойОфис Частное Облако». Детальная информация по компоненту находится в официальном руководстве по установке «МойОфис Частное Облако».
`coapiurl:`	Путь доступа к API компонента CO. Данная переменная представляет собой URL-адрес (порт по умолчанию: 8888), указывающий на целевой сервер с ролью `Auth` компонента CO. Пример: `coapiurl: "http://co-api-ip.ru:8888"`
`co_lb:`	Включает и выключает настройку балансировки при помощи сервиса `keepalived` , принимает значения `True` и `False` , соответственно.
`vip_auth:`	Виртуальный IP-адрес, доступное значение — произвольный свободный IP-адрес в сети инсталляции.
`lb_keepalived_pass:`	Пароль для сервиса `keepalived` .

Переменная	Значение и способ заполнения

Блок **installation_commons**
`FS_TOKEN_SALT_EXT:`
`FS_APP_ENCRYPTION_KEY:`
`FS_APP_ENCRYPTION_IV:`
`FS_APP_ENCRYPTION_SALT:`
`AUTH_ENCRYPTION_KEY:`
`AUTH_ENCRYPTION_IV:`
`AUTH_ENCRYPTION_SALT:`
`APP_ADMIN_LOGIN:` `APP_ADMIN_PASSWORD:`
	Значения переменных данного блока должны соответствовать аналогичным переменным в компоненте CO (файл приватных параметров плейбуков `private.yml`). Более подробно о заполнении блока можно узнать в разделе 5.5.4 руководства по установке «МойОфис Частное Облако».

`LOGOS_INTEGRATION_ENABLED`	Включение и выключение интеграции с «МойОфис Логос», доступные значения: `True` и `False` . Дополнительная информация также находится в разделе 4.6.5 данного руководства.
блок **LOGOSDB:** `HOST:` `USERNAME:` `PASSWORD:` `DB:` `PORT:`	Параметры базы данных, используемой «МойОфис Логос». Сведения об установке и настройке данного компонента находятся в официальном руководстве по установке «МойОфис Логос».
`POSEIDON_INTEGRATION`	Включение и выключение интеграции с «МойОфис Почта», доступные значения: `True` и `False` .
блок **POSEIDON**	Параметры подключения к «МойОфис Почта». Более подробные сведения об установке и настройке данного компонента находятся в официальном руководстве по установке «МойОфис Почта».
`PBM_URL:`	Url доступа к почтовому серверу «МойОфис Почта» формата `https://pbm.myoffice-app.ru:48666` .
`SSL_VERIFY:`	Параметры шифрования для почты. Принимает значения `True` и `False` , `False` - в случае использования самоподписанных сертификатов.

Таблица 4. Значения и способы заполнения переменных инвентарного файла инсталляции PGS.

4.4 Настройка дополнительных параметров установки

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

4.5 Настройка межсетевого экранирования

Для корректной работы «МойОфис Хранилище» рекомендуется не использовать сетевое экранирование между серверами. Необходимые для работы ПО сетевые порты приведены ниже в Таблице 5:

Порт	Назначение
8851	Доступ к основному API «МойОфис Хранилище».
8852	REST API доступа к администрированию «МойОфис Хранилище».
8854	WEB администрирование «МойОфис Хранилище» (административная панель управления).

Таблица 5. Сетевые порты, используемые подсистемой PGS.

Порт 443 (или другой установленный для использования с nginx порт) необходимо добавить в исключения фаерволла в соответствии с настройками выбранной ОС установки.

4.6 Установка «МойОфис Хранилище»

4.6.1 Запуск установки

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

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

Где `<hosts.yaml>` - инвентарный файл, сконфигурированный в соответствии с параграфом 4.3.1 данного руководства, `<additional ansible keys>` - дополнительные ключи установки.

> Подробнее о дополнительных ключах в документации Ansible.

В случае возникновения проблем во время установки, рекомендуется установка на “чистую” систему или использование ключа `-e CLEANUP=true` .

При успешном выполнении скрипта сервисы подсистемы PGS будут запущены автоматически.

4.6.2 Проверка корректности установки

1. Для проверки корректности установки необходимо на машине с ролью `pythagoras` выполнить в терминале команду:

```
curl -X POST
https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi/?cmd=api_version
| python3 -m json.tool
```

Где `<ENV>` , `<DEFAULT_DOMAIN>` и `<NGINX_HTTPS_EXT_PORT>` - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства.

Пример ожидаемого вывода (значения `API` и `WebAPI` могут быть другими):

```
{"response": {"Aristoteles": "3.2.4-861", "API": "4.45.0", "WebAPI": "4.32.3",
"success": "true"}, "success": "true"}
```

2. Для проверки запуска сервисов PGS выполняется следующая команда:

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

Ожидаемый вывод:

```
pgs-arangodb_arangodb            1/1
pgs-elasticsearch_elasticsearch  1/1
pgs-etcd_etcd                    1/1
pgs-keycloak_keycloak            1/1
pgs-nginx_nginx                  1/1
pgs-postgres_postgres            1/1
pgs-rabbitmq_rabbitmq            1/1
pgs-redis_redis                  1/1
```

```
pgs_aristoteles                 1/1
pgs_euclid                      1/1
pgs_logos-sync                  1/1
pgs_polemon                     1/1
pgs_sisyphussearch              1/1
pgs_sisyphusworker              1/1
```

Если какой-либо из сервисов не запустился, значение напротив имени сервиса будет выглядеть как `0/1` .

> Проверку работы веб-интерфейса административной панели можно будет выполнить на следующем этапе установки.

4.6.3 Создание тенанта

Создание тенанта по умолчанию происходит в процессе установки в случае, если был заполнен блок переменных инвентарного файла **default_tenant**. Если необходимо создать еще один тенант (или тенант по умолчанию не был создан), следует воспользоваться REST API сервиса Euclid.

Примеры shell-команд:

1. Аутентификация и получение токена авторизации для пользователя PGS:

```
curl -X POST
"https://admin-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/adminapi/auth" -d
"username=pgs" -d "password=<KEYCLOAK_PASSWORD>"
```

Где `<ENV>` , `<DEFAULT_DOMAIN>` , `<NGINX_HTTPS_EXT_PORT>` и `<KEYCLOAK_PASSWORD>` - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства.

2. Создание тенанта:

```
curl --header "Authorization: ${token}" -X POST
"https://admin-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/adminapi/tenants" -d
"default_domain=<DOMAIN>" -d "name=<NAME>" -d "admin_password=<Admin password>" -d
"admin_recovery_email=<Recovery Email>" -d "max_user_count=1000"
```

Где:

- `token` - полученный в предыдущем шаге токен авторизации.
- `<DEFAULT_DOMAIN>` - домен инсталляции PGS, соответствующая переменная из инвентарного файла.
- `<DOMAIN>` - Домен, соответствующий создаваемому тенанту. При создании *дополнительного* тенанта (не по умолчанию) не может быть тождественен `<DEFAULT_DOMAIN>` .
- `<ENV>` , `<NGINX_HTTPS_EXT_PORT>` - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства.
- `<NAME>` - имя создаваемого тенанта. По умолчанию имеет значение `default` .
- `<Admin password>` - пароль администратора веб-интерфейса.
- `<Recovery Email>` - адрес электронной почты для восстановления пароля администратора.

Данный тенант можно администрировать при помощи веб-интерфейса, по умолчанию доступного по адресу:

```
https://admin-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>
```

Где `<ENV>` , `<DEFAULT_DOMAIN>` и `<NGINX_HTTPS_EXT_PORT>` - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства.

> Логин для авторизации администратора в тенанте будет выглядеть как `admin@<DOMAIN>` .

4.6.4 Интеграция с редакторами CO

Для конфигурации внутреннего взаимодействия «МойОфис Хранилище» с редакторами «МойОфис», необходимо обратиться к инвентарному файлу соответствующей инсталляции CO и установить там следующие параметры:

Переменная	Значение
`FS_API_URL:`	`"https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi"`
`FS_APP_URL:`	`"https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi"`
`FS_APP_LOGIN:`	`"app-co"`

Переменная	Значение
FS_CARD_URL:	"https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi"

Где <ENV> , <DEFAULT_DOMAIN> и <NGINX_HTTPS_EXT_PORT> - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства. Более подробная информация по конфигурации редакторов «МойОфис» находится в официальной инструкции по установке продукта.

4.6.5 Интеграция с мессенджером Logos

Параметры инвентарного файла «МойОфис Хранилище» для работы с базой данных мессенджера Logos описаны в разделе 4.3.2 данного руководства. В остальном, настройка интеграции проводится аналогично подобной для редакторов. Необходимо обратиться к инвентарному файлу соответствующей инсталляции «МойОфис Логос» и установить там следующие параметры:

Переменная	Значение
FS_CARD_URL:	"https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi"
FS_APP_URL:	"https://pgs-<ENV>.<DEFAULT_DOMAIN>:<NGINX_HTTPS_EXT_PORT>/pgsapi"
FS_APP_LOGIN:	"app-co"

Где <ENV> , <DEFAULT_DOMAIN> и <NGINX_HTTPS_EXT_PORT> - переменные, заполненные в соответствии с разделом 4.3.2 данного руководства. Более подробная информация по настройке и установке «МойОфис Логос» находится в официальной инструкции по установке продукта.

4.6.6 Интеграция с Active Directory

Для конфигурирования интеграции «МойОфис Хранилище» с AD необходимо произвести следующие действия:

1. Открыть доступ к компоненту Keycloak из внешней сети, выполнив следующую команду:

```
docker service update --publish-add published=8091,target=8080
pgs-keycloak_keycloak
```

2. Перезапустить сервисы `pgs_aristoteles` и `pgs_euclid` .
3. Открыть веб-интерфейс Keycloak (адрес по умолчанию `http://<DEFAULT_DOMAIN>:8091/auth`).
4. Выбрать тенант (или `realm`), для которого нужна интеграция.
5. Нажать `User Federation` .
6. Из выпадающего меню выбрать провайдера LDAP (`Add provider`) с именем `pgsldap` .
7. Заполнить параметры следующим образом:

Параметр	Значение
`Edit mode`	`Unsynced`
`Vendor`	`Active Directory`
`Username LDAP Attribute`	`sAMAccountName`
`Connection URL`	Путь доступа в формате `ldap://111.1.1.1`
`Users DN`	Данные для подключения к AD соответственно настройкам сервера
`Bind DN`	Логин пользователя AD
`Bind credential`	Пароль
`Search scope`	`One level` или `Subtree` в зависимости от настроек сервера AD

8. Остальные параметры оставить по умолчанию.
9. Нажать `Save` и `Synchronize all users` .
10. На вкладке `Users` в левом меню можно просмотреть список всех импортированных пользователей.
11. В случае наличия ошибок возможно вернуться обратно на вкладку `User Federation` к провайдеру `pgsldap` и нажать `Remove imported` для очистки списка пользователей.

5 Обновление с предыдущих версий

Процесс обновления «МойОфис Хранилище» полностью аналогичен процессу первичной установки.

6 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.