Руководство по установке

МОЙОФИС ХРАНИЛИЩЕ 2.3

МойОфис

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

МойОфис Частное Облако

РУКОВОДСТВО ПО УСТАНОВКЕ

МойОфис Хранилище 2.3

На 38 листах

Москва

2023

МойОфис

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 средах с поддержкой контейнеризации
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
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
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

Сокращение, термин	Расшифровка и определение
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
Сервер-оператор	Сервер, с которого будет производиться установка системы
Тенант (tenant)	Элемент мультиарендной системы
Хост (host)	Устройство, предоставляющее сервисы формата “клиент-сервер”
Целевой сервер	Сервер, на который будет производиться установка системы

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.

Функциональные возможности, предоставляемые «МойОфис Хранилище» включают 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 (в составе «МойОфис Частное Облако»);
- Широкие возможности по работе в собственном домене;
- Интеграцию с другими компонентами ПО «МойОфис Частное облако»: CO (Редакторы) и PSN (Почта).

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 и запросов 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 подсистемами виртуализации на уровне эксперта:
    - Работа с подсистемой контейнерной виртуализации (Docker);
    - Работа с одной из подсистем серверной виртуализации на базе гипервизоров Hyper-V, VMWare vSphere ESXi, KVM.
- 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 на уровне эксперта:
    - СУБД ArangoDB;
    - Файловой системы GlusterFS;
    - SSO-сервиса Keycloak;
    - СУБД PostgreSQL;
    - Поисковой системы ElasticSearch;
    - Redis;
    - Обработчика сообщений RabbitMQ;
    - Сервера конфигурации ETCD.
- Опыт работы с подсистемой централизованного управления Ansible.

1.3 Системные требования

1.3.1 Аппаратные требования

- Скорость сетевой подсистемы - 1 Gbit/s или выше.
- Рекомендуемая система виртуализации - VMWare ESXi, KVM.
- В таблице 2 приведены минимальные требования к аппаратному обеспечению для установки конфигурации без отказоустойчивости:

CPU	RAM (Gb)	HDD (Gb)
8	16	50 + Квота пользователей на использование дискового пространства

Таблица 2. Характеристики конфигурации без отказоустойчивости

> Конфигурация без отказоустойчивости (standalone) используется в целях демонстрации функциональных возможностей «МойОфис Хранилище». В производственных средах настоятельно рекомендуется использовать кластерную (отказоустойчивую) конфигурацию, более подробно о которой написано в разделе 3.2 данного руководства.

1.3.2 Программные требования

Требования к программному обеспечению для установки «МойОфис Хранилище» приведены в таблице 3:

Требование	Описание
Операционная система	Centos 7.9
	Альт Сервер 10
	Ubuntu 20.04
	РЕД ОС 7.3.1 «Муром»
	Astra Linux Common Edition 2.12.43
	Astra Linux Special Edition 1.7 (дополнительные требования для данной ОС указаны в разделе 1.3.2.1)
Python	Версия не ниже 3.6 с модулем pip (для сервера-оператора)
Ansible	На сервер-оператор должен быть инсталлирован Ansible версии 4.4.* (соответствует пакету ansible-core 2.11). Проверка версии осуществляется командой `ansible --version`
Доступ	Для каждого сервера, на котором выполняется установка должен быть обеспечен ssh-доступ. В целях удобства рекомендуется сделать это при помощи ssh-ключа пользователем root или другим пользователем с sudo привилегиями: `(ALL=(ALL) NOPASSWD: ALL)`

Требование	Описание
Стандартные репозитории ОС	Подключение всех стандартных репозиториев ОС либо их зеркал (во внутренней сети для установок в закрытом контуре)
Репозиторий epel (Для ОС CentOS 7)	Подключение репозитория epel (либо его локальной копии для установок в закрытом контуре)
Репозитории elrepo, docker-ce, PyPi и ppa:canonical-kernel-team/ppa (PPA for Canonical Kernel Team)	Подключение локальных копий репозиториев для установки соответствующих пакетов ядра Linux и Docker, а также модулей Python, не входящих в состав поставки (для установок в закрытом контуре)

Таблица 3. Требования к программному обеспечению для установки «МойОфис Хранилище»

> Во избежание проблем, рекомендуется не использовать системы, на которых ранее были проведены инсталляции программного обеспечения, не относящегося к дистрибутиву «МойОфис Хранилище», а также проверить, что на выбранную ОС установки не загружены никакие дополнительные программные пакеты помимо тех, что будут скачаны в процессе инсталляции.

1.3.2.1 Требования для ОС Astra Linux SE при усиленном или максимальном уровне целостности

При установке Astra Linux SE с усиленным или максимальным уровнем целостности в устанавливаемой ОС включается мандатное управление доступом по умолчанию, в результате чего каждому пользователю системы при входе требуется задать уровень целостности. Для корректной работы установки PGS в дальнейшем, пользователю, от имени которого будет работать Ansible, необходимо установить максимальный уровень целостности (`63` , соответствует администратору ОС). Проверить уровень целостности пользователя возможно командой:

```
pdp-id -i
```

Работа с Ansible в ОС Astra Linux SE (в усиленном или максимальном уровне) невозможна, если включен режим запрета установки бита исполнения. В этом режиме любому пользователю, даже входящему в группу администраторов (кроме root), запрещается создавать исполняемые сценарии для командной оболочки (`+x`). Проверить статус режима возможно командой:

```
cat /parsecfs/nochmodx
```

Результат выполнения команды: `1` — режим включен; `0` — режим выключен.

Отключить режим запрета установки бита исполнения возможно командой:

```
astra-nochmodx-lock disable
```

1.3.3 Рекомендации по использованию файловых систем

В соответствии с рекомендациями производителей операционных систем для CentOS рекомендуется использовать файловую систему XFS.

Разбивку дисков рекомендуется выполнять следующим образом:

- в режиме с отказоустойчивостью (cluster) для серверов всех ролей, кроме syslog, рекомендуется выделить не менее 40 Gb для штатной работы ОС;
- в режиме без отказоустойчивости (standalone) рекомендуется выделить не менее 50 Gb на корневой раздел;
- в режиме с отказоустойчивостью (cluster) для сервера роли syslog рекомендуется выделить не менее 100 Gb для штатной работы ОС и хранения всех логов;
- более подробная информация по разбиению дисков для конкретных ролей подсистемы «МойОфис Хранилище» указана в разделе 4.3.3 данного руководства.

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).

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 входит СО (Редакторы) - программные решения для редактирования текста, таблиц и презентаций.

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

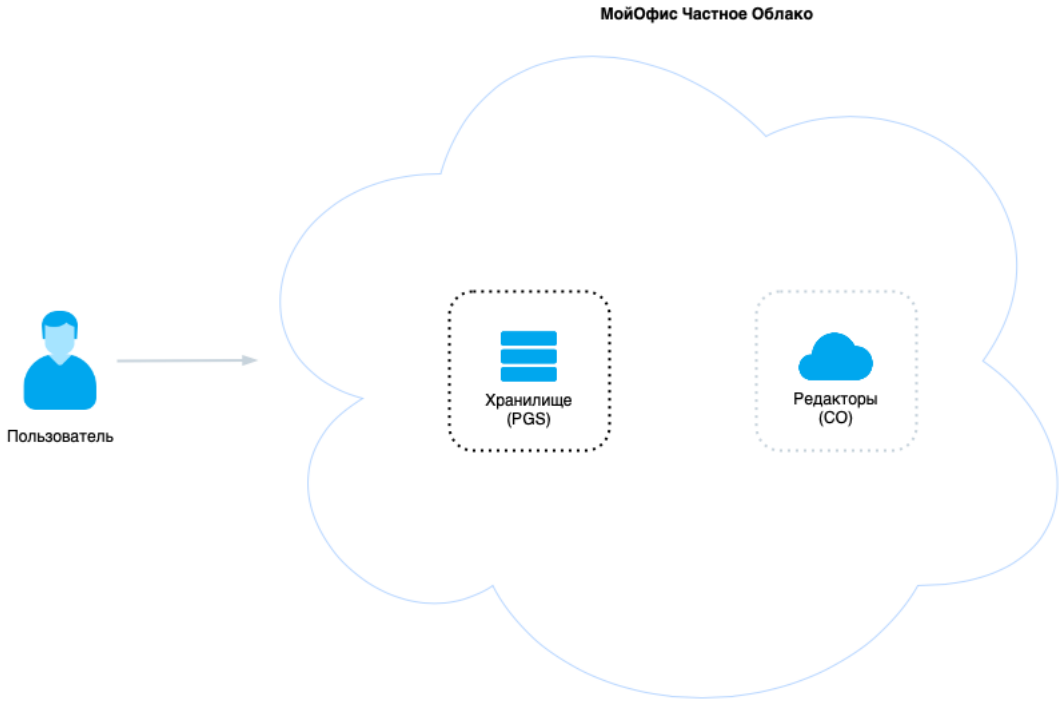

Рисунок 1. Общая архитектурная схема «МойОфис Частное Облако».

> 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 (представ-

ленные в виде инсталляционных ролей) описаны в разделе 4.2.1 данного руководства. Детальная архитектурная схема «МойОфис Хранилище» приведена на Рисунке 2.

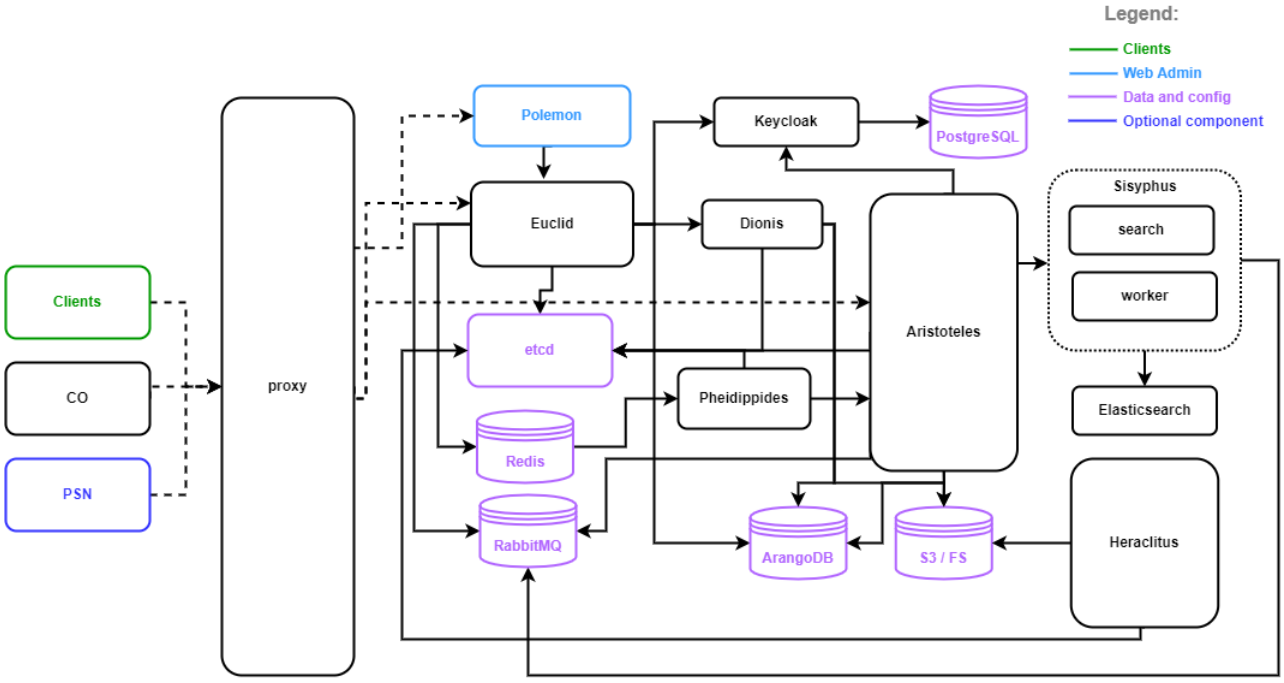

Рисунок 2. Архитектурная схема «МойОфис Хранилище».

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 серверы, а также, по возможности, разносятся на разные физические серверы или гипервизоры. Аппаратные требования для такого типа установки рассчитываются индивидуально для каждого технического проекта, единственным определенным ограничением будет минимальное количество виртуальных машин в контуре установки – 3.

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).
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 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.
15. Monitoring – Сервисы Prometheus и Grafana для мониторинга состояния системы.

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

4.2.2 Подготовка инфраструктуры установки

4.2.2.1 Настройка DNS

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.

4.2.2.2 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.

4.2.2.3 Настройка сертификатов

Для корректной работы веб-интерфейса «МойОфис Хранилище» необходима установка соответствующих SSL-сертификатов. Данные сертификаты (в PEM и KEY формате) следует поместить в директорию, соответствующую сконфигурированному имени домена по следующему пути:

```
~\MyOffice_PGS_XXXX.XX\certificates\<DOMAIN>
```

Где `~\MyOffice_PGS_XXXX.XX` - корневой каталог установки, `<DOMAIN>` - директория, соответствующая сконфигурированному имени домена.

Список необходимых для работы сертификатов:

- `server.crt` – содержит SSL-сертификат для `*.<DEFAULT_DOMAIN>` и все промежуточные сертификаты, кроме корневого доверенного. Расположение промежуточных сертификатов соответствует описанию в документации nginx.
- `server.nopass.key` – приватный ключ сертификата, не требующий кодовой фразы.
- `ca.crt` – все доверенные SSL-сертификаты (самоподписанные или не публичные).

4.2.2.4 Создание самоподписанного сертификата для «МойОфис Хранилище» (опционально)

Для создания самоподписанного сертификата в среде установки «МойОфис Хранилище» необходимо использовать исполняемый файл `gen_self_signed_cert.sh` из директории установки, запустив его в консоли и указав привязанный к создаваемому сертификату домен. Пример:

```
gen_self_signed_cert.sh <DOMAIN>
```

Создаваемый файл сертификата будет автоматически помещен в необходимую установке директорию (см. раздел 4.2.2.3 данного руководства).

4.3 Настройка параметров установки

Перед запуском установки необходимо скопировать шаблон инвентарного файла (inventory file) в корневой каталог дистрибутива и заполнить в нём секции `hosts` и `vars` в соответствии с дальнейшими инструкциями.

Шаблоны для заполнения находятся в папке с дистрибутивом по следующим адресам:

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

(для конфигурации без отказоустойчивости) или

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

(для кластерной инсталляции).

> Инвентарный файл использует формат .yaml, синтаксис которого описан в документации Ansible.

Операция копирования исполняется командой следующего вида:

```
cp inventory/hosts-sa.yaml hosts.yml
```

Сконфигурированный файл рекомендуется сохранить на внешнем ресурсе для дальнейшего использования на случай восстановления и/или переустановки системы.

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 серверы в группах. В данном примере (фрагмент шаблона `hosts-sa.yaml`) все роли будут устанавливаться на один сервер по адресу `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>"
```

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: 3 хоста;
- RabbitMQ: 3 хоста;
- Elasticsearch: 3 хоста;
- Etcd: 3 хоста;
- Nginx: 2 хоста;
- Storage: 3 хоста (обязательно).

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

```
  storage: #3 minimum
    hosts:
      host.example.com:
      host.example.com:
      host.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: # cluster installation requires a minimum of 3 agents; otherwise, leave
group empty
      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>"
    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:
```

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:
```


Также следует обратить дополнительное внимание на роли `arangodb`, `arangodb_agent`, `elasticsearch`, `postgres` и `storage`: 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"`.

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 `syslog` 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 нагрузки 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 данного руководства.

Установка служб мониторинга опциональна, для ее пропуска необходимо удалить группу хостов `monitoring` из инвентарного файла перед установкой программы.

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` .
>
> Спецсимволы `<>{}|&;*?@`$!` в значениях переменных необходимо экранировать символом `\` .

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).
`PGS_CLUSTER`	Включение и отключение кластерного режима установки системы. Принимает значения `True` и `False` , в шаблоне `hosts-sa.yaml` по умолчанию `False` , в шаблоне `hosts-hl.yaml` по умолчанию `True` .
`SWARM_NETWORK_ENCRYPTION:`	Включает шифрование внутренней оверлейной сети Docker swarm, значение по умолчанию `False` . Влияет на производительность системы, подробнее о данном виде шифрования.

Переменная	Значение и способ заполнения
`DEFAULT_DOMAIN`	Зарегистрированный домен инсталляции «МойОфис Хранилище». Для корректной работы необходим установленный актуальный SSL-сертификат (см. раздел 4.2.2.6 данного руководства).
`ENV`	Окружение инсталляции. Данный параметр определяет элемент доменного имени инсталляции и предназначен для разграничения доступа к сервисам PGS.
`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. раздел 4.2.2.6 данного руководства).
`MAX_TENANTS`	Задает максимально возможное число тенантов в текущей инсталляции.Значение по умолчанию `100` .
`KEYCLOAK_PASSWORD`	Пароль для пользователя PGS в Keycloak (Администратор Master Realm).

Переменная	Значение и способ заполнения
`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.
`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` .
`MONITORING_ADMIN_PASSWORD:`	Используется при заполнении группы хостов `monitoring` (опционально) для доступа к интерфейсу Grafana. Значение по умолчанию: `admin` .
`MONITORING_ADMIN_PASSWORD_HASH:`	Хэш пароля для мониторинга. Пример генерации: `openssl passwd -apr1 $MONITORING_ADMIN_PASSWORD`
`PATRONI_REPLICATION_PASSWORD`	Пароль для репликации БД PostgreSQL.
`ELASTICSEARCH_HEAP_SIZE`	Выделение памяти для Elasticsearch, изменять не требуется.
`SELINUX_ENABLED`	Проверяет режим работы SELinux и переключает его в режим **enforcing**. Используется только для RedHat-based ОС (например, CentOS). Доступные значения: `True` и `False` , по умолчанию `False` .

Переменная	Значение и способ заполнения
`IPTABLES_ENABLED`	Устанавливает и настраивает службы межсетевого экрана (опционально). Доступные значения: `True` и `False`, по умолчанию `False`.
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`.
`QUOTA_PER_USER:`	Выделенное пользователю место на хранилище, указывается в байтах, значение по умолчанию `1000000000` (~1 GB)
Блок **storage:**	
`type:`	Выбор типа системы хранения файлов, доступны значения `fs` и `s3` (файловая система и объектное хранилище, соответственно).
Блок **fs**	
`path:`	Путь до файловой системы хранения, если используется `storage: type: "fs"`.
`retention_file_time:`	Время хранения файлов после удаления из корзины. Значение в днях, по умолчанию `7`.
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».

Переменная	Значение и способ заполнения
`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.
`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.
Блок **system:**	
`TIMEZONE:`	Временная зона (часовой пояс) установки. Значение по умолчанию `"Europe/Moscow"` Список допустимых значений находится по ссылке.

Переменная	Значение и способ заполнения
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` .
Блок **installation_commons**	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».
`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:`	

Переменная	Значение и способ заполнения
`APP_ADMIN_LOGIN:`	
`APP_ADMIN_PASSWORD:`	
`AUDIT_LOG_ENABLED`	Переменная предоставляет возможность включения в административном интерфейсе расширенного лога событий. Доступные значения: `True` и `False`, по умолчанию `False`.
`CHATBOT_ENABLED`	Включение и отключение интеграции с сервисом ChatBot компонента CO. Значение зависит от наличия сервиса в установочном пакете CO. Доступные значения: `True` и `False`, по умолчанию `False`. Детальная информация по переменной находится в официальном руководстве по установке «МойОфис Частное Облако».
`CO_MANAGE_API_USERNAME:`	Логин для API-авторизации компонента CO. Должен совпадать со значением переменной `CO_MANAGE_API_USERNAME` в конфигурации CO.
`CO_MANAGE_API_PASSWORD:`	Пароль для API-авторизации компонента CO. Должен совпадать со значением переменной `CO_MANAGE_API_PASSWORD` в конфигурации CO.
блок **POSEIDON**	Параметры подключения к «МойОфис Почта». Более подробные сведения об установке и настройке данного компонента находятся в официальном руководстве по установке «МойОфис Почта».
`POSEIDON_INTEGRATION`	Включение и выключение интеграции с «МойОфис Почта», доступные значения: `True` и `False`.
`PBM_URL:`	Url доступа к почтовому серверу «МойОфис Почта» формата `https://pbm.myoffice-app.ru`.
`PBM_USER_PASSWORD:`	Переменная для авторизации через API PSN. Соответствует значению переменной `ds389_manager_user` в инсталляции PSN.

Переменная	Значение и способ заполнения
`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.

4.3.3 Рекомендации по разбиению дисков для ролей

1. Для серверов с ролями `storage`, `postgres`, `arangodb` и `elasticsearch` рекомендуется выделить независимые диски или блочные устройства.
2. Точка монтирования для роли `storage` в режиме **без отказоустойчивости** при выборе типа хранилища `fs`:

```
/media/storage # Возможно использовать логический раздел.
```

3. Точка монтирования для роли `storage` в режиме **без отказоустойчивости** при выборе типа хранилища `s3`:

```
/opt/Pythagoras/minio/data/sa0/
```

4. Точка монтирования для роли `storage` в режиме **с отказоустойчивостью** при выборе типа хранилища `fs`:

```
/gluster_bricks/pgs-files
```

5. Точка монтирования для роли `storage` в режиме **с отказоустойчивостью** при выборе типа хранилища `s3`:

```
/opt/Pythagoras/minio/data[0-9] # Где 0-9 - это номер используемого диска.
```

6. При выборе типа хранилища `s3` обязательно использование как минимум двух независимых дисковых устройств.
7. Для ролей `postgres`, `arangodb` и `elastcisearch` производить монтирование заранее не нужно. Во время установки устройство будет автоматически смонтировано по следующему пути:


```
/var/lib/docker/volumes/{ service_name }
```

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 (или путь к нему), сконфигурированный в соответствии с разделами 4.3.1 и 4.3.2 данного руководства;

- `<additional ansible keys>` - дополнительные ключи установки. Подробнее о дополнительных ключах см. в документации по Ansible.

При успешном выполнении команды сервисы подсистемы PGS будут запущены автоматически. В процессе инсталляции не происходит обновление компонентов системы. Обновление компонентов системы выполняет администратор установочного стенда.

4.6.2 Проверка корректности установки

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"}
```

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_aristoteles                  1/1
pgs_dionis                       1/1
pgs_euclid                       1/1
```



```
pgs_pheidippides                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_users=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>` .

3. Изменение настроек тенанта (у передаваемых параметров указаны текущие значения по умолчанию):

```
curl --header "Authorization: ${token}" -X PUT "https://admin-<ENV>.<DEFAULT_-
DOMAIN>:<NGINX_HTTPS_EXT_PORT>/adminapi/tenants/<TENANT_NAME>" -d
history_settings='{"history_enabled": False, "history_events_max_count": 100,
"history_expiration_period": 31536000}'
```

Где:

- `history_enabled` – включение/отключение возможности регистрировать и показывать события по объектам; возможные значения `True` или `False` , по умолчанию `False` ;
- `history_events_max_count` – максимальное количество регистрируемых и показываемых событий по одному объекту; значение параметра – целое число (int), по умолчанию `100` ;
- `history_expiration_period` – максимальный период в секундах, за который показываются события по объекту; значение параметра – целое число (int), по умолчанию `31536000` .

4.6.4 Интеграция с редакторами СО

Для конфигурации внутреннего взаимодействия «МойОфис Хранилище» с редакторами «МойОфис», необходимо обратиться к инвентарному файлу соответствующей инсталляции СО 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"`
`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 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

Параметр	Значение
`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.