



МойОфис Профессиональный 3

Руководство по установке

СИСТЕМА ХРАНЕНИЯ ДАННЫХ

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

**ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ
«МОЙОФИС ПРОФЕССИОНАЛЬНЫЙ 3»
СИСТЕМА ХРАНЕНИЯ ДАННЫХ
3.0**

РУКОВОДСТВО ПО УСТАНОВКЕ

Версия 1

На 45 листах

Дата публикации: 18.06.2024

**Москва
2024**

МойОфис

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

1	Общие сведения	8
1.1	Назначение	8
1.2	Описание архитектуры	8
1.3	Структура	9
1.4	Состав дистрибутива	11
1.5	Перечень технической документации	11
1.6	Требования к персоналу	12
1.7	Типовые схемы установки	14
1.7.1	Standalone	14
1.7.2	Кластерная установка	14
1.8	Порядок установки серверов	14
1.9	Программные и аппаратные требования	15
2	Подготовка к установке	16
2.1	Конфигурирование ОС Astra	16
2.1.1	Установка на Astra SE 1.7 в защищенных вариантах	16
2.1.2	Установка на усиленном уровне защищенности («Воронеж»)	17
2.2	Настройка сетевых соединений	18
2.3	Подготовка сервера с ролью operator	19
2.3.1	Установка дополнительного ПО	19
2.3.2	Установка в сети без выхода в интернет	19
2.4	Подготовка инфраструктуры установки	20
2.4.1	Проверка и подготовка дистрибутива ПО	20
2.4.2	Настройка DNS	20
2.4.3	Настройка сертификатов	21
2.4.4	Создание самоподписанного сертификата	21
2.5	Настройка параметров установки	22
2.5.1	Конфигурирование ролей файла hosts.yml	22
2.5.1.1	Конфигурация для кластерной установки	24
2.5.1.2	Конфигурация для кластерной установки с ArangoDB	25

2.5.1.3 Сбор событий и метрик, хранение образов	25
2.5.2 Конфигурирование переменных файла hosts.yml	26
2.5.3 Рекомендации по настройке дисков для ролей	31
2.5.4 Настройка межсетевого экранирования	33
2.5.5 Настройка дополнительных параметров установки	34
3 Установка	35
3.1 Порядок запуска установки	35
3.2 Проверка корректности установки	35
3.3 Обновление	36
4 Карта портов	37
4.1 Карта портов для внутренних соединений	37
4.2 Карта внешних портов	39
4.3 Рекомендации по открытым портам и доступам	42
Приложение А - Известные проблемы и способы их решения	43

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В настоящем документе применяют следующие сокращения с соответствующими расшифровками (см. таблицу 1).

Таблица 1 — Сокращения и расшифровки

Сокращение, термин	Расшифровка и определение
AD	Microsoft Active Directory
Ansible	Система управления конфигурациями, используемая для автоматизации настройки и развертывания ПО
API	Application Programming Interface, интерфейс программирования приложений
CO	CloudOffice, Облачный Офис, общее название продукта (группы редакторов)
Docker	Приложение для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации
Docker Registry	Масштабируемое серверное приложение для хранения и использования контейнеров Docker
DNS	Domain Name System, система доменных имен
Inventory	Файл ПО Ansible с перечислением ролей и их IP-адресов
MD5-хеш (hash)	Контрольная сумма, предназначенная для проверки целостности файла
IOPS	Количество операций ввода/вывода — параметр для измерения производительности систем хранения
REST API	Архитектурный стиль взаимодействия компонентов распределенного приложения в сети
S3 хранилище	Сервис хранения объектов, предлагаемый поставщиками облачных услуг
SSH	Secure Shell, «безопасная оболочка» сетевой протокол прикладного уровня, для удаленного управления
SSO	Single Sign-On, технология единого входа
URL	Uniform Resource Locator, единый указатель ресурса
XFS	64-битная файловая система с журналом событий
Yum	Менеджер программных пакетов для дистрибутивов Linux
БД	База данных
Вендор (vendor)	Поставщик брендированного продукта
ЕСИА	Единая система идентификации и аутентификации
Кластер (cluster)	Объединенная группа серверов
Оверкоммит (overcommit)	Опция гипервизора по избыточной аллокации памяти для виртуальных машин
ОС	Операционная система

Сокращение, термин	Расшифровка и определение
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

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

Функциональные возможности, предоставляемые Системой хранения данных, 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 Профессиональный 3»;
- широкие возможности по работе в собственном домене;
- интеграцию с другими компонентами ПО «МойОфис Профессиональный 3».

В данном руководстве описана установка Системы хранения данных.

1.2 Описание архитектуры

Система хранения данных является составным компонентом ПО «МойОфис Профессиональный 3», в которое также входит Система редактирования и совместной работы — программные решения для редактирования текста, таблиц и презентаций.

Общая архитектурная схема «МойОфис Профессиональный 3» приведена на рисунке 1.

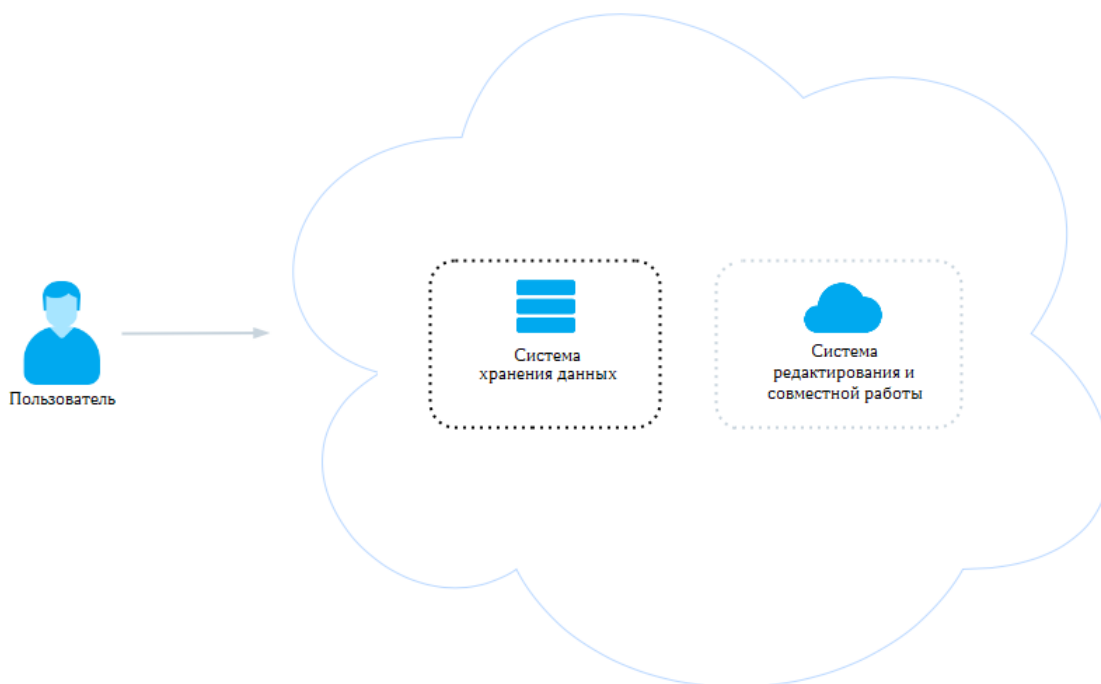


Рисунок 1 — Общая архитектурная схема «МойОфис Профессиональный 3»

Все элементы «МойОфис Профессиональный 3» возможно настроить для обеспечения внутреннего взаимодействия, в таком случае порядок установки компонентов не важен.

В задачу администратора входит заполнение обязательных переменных и настройка соотношения доменных имен серверов, необходимые связи и зависимости пакеты установки образуют автоматически.

Подробнее см. в соответствующих руководствах по установке компонентов «МойОфис Профессиональный 3».

1.3 Структура

Внутренняя структура Системы хранения данных представляет собой набор сервисов, обеспечивающих работу ПО и взаимодействие с другими компонентами «МойОфис Профессиональный 3». Сервисы (представленные в виде установочных ролей) подробно описаны в документе «"МойОфис Профессиональный 3". Архитектура».

Детальная архитектурная схема Системы хранения данных приведена на рисунке 2.

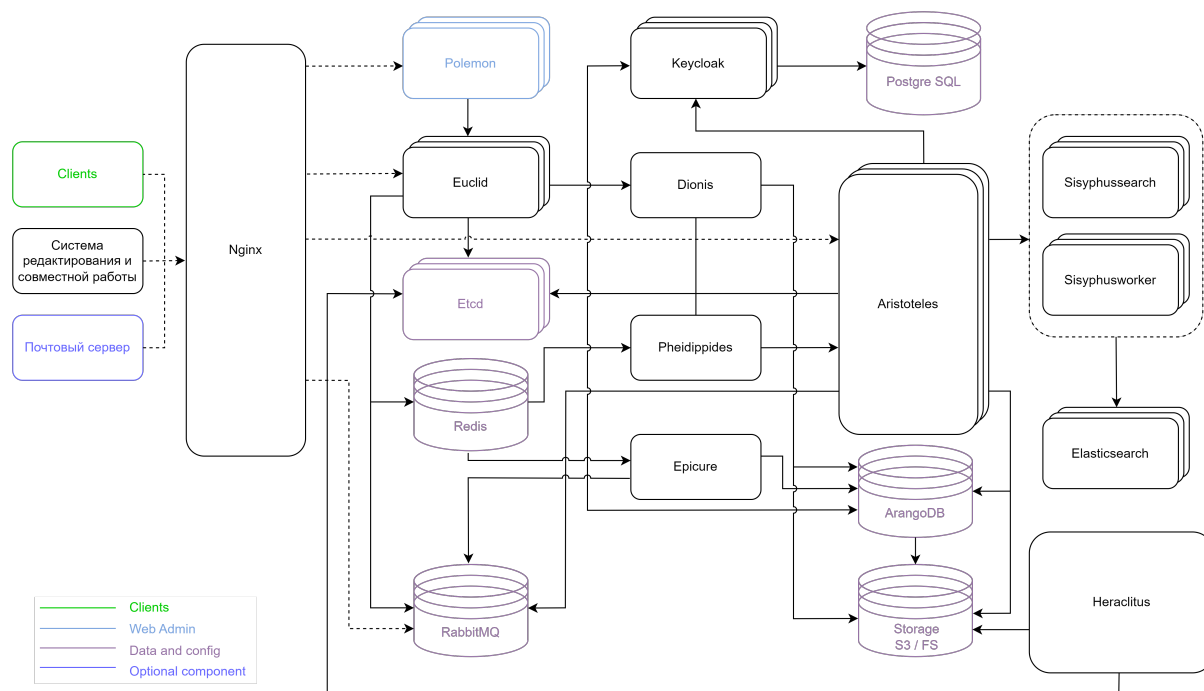


Рисунок 2 — Архитектурная схема Системы хранения данных

Описание сервисов, представленных на рисунке 2, находится в таблице 2.

Таблица 2 — Перечень сервисов Системы хранения данных

Наименование сервиса	Описание
Arangodb	База данных, содержащая метаданные файлов (например, информацию о владельце документа, правах доступа и пр.)
Aristoteles	Сервер приложений, выступающий backend-частью для компонентов СО в части выполнения файловых операций, разграничения прав доступа, версионирования, фиксации истории событий по объектам
Dionis	Сервис, отвечающий за удаление и переназначение прав доступа для объектов пользователей
Elasticsearch	Сервис, отвечающий за поиск по содержимому в хранящихся файлах
Epicure	Сервис формирования и отправки сообщений безопасности с последующей отправкой в аудит системы (SIEM)
Etcd	Сервис, содержащий конфигурацию приложений, при кластерном развертывании также используется сервисом Postgres для создания кластера
Euclid	Rest API сервис, отвечающий за администрирование пользователей в системе, выступающий backend-частью для компонента Polemon (веб-администрирование)
Heraclitus	Сервис очистки архивных данных, удаленных пользователями из корзины. Имеет возможность настройки сроков хранения архивных данных и автоудаления их с диска по заданному расписанию
Keycloak	Сервис SSO, хранящий в себе настройки инсталляции, данные по тенантам и пользователям
Nginx	Прокси-сервис, обеспечивающий доступ до: Rabbitmq, Aristotels, Euclid, Polemon
Pheidippides	Сервис, осуществляющий обработку событий в Redis каналах (автоматическая блокировка IP-адресов/публичных ссылок)
Polemon	Сервис веб-администрирования Euclid (веб-интерфейс административной панели)
Postgres	PostgreSQL, база данных для сервиса авторизации Keycloak
RabbitMQ	Очередь сообщений. Используется для передачи документов в elasticsearch для поиска по содержимому документов и для передачи межкомпонентных уведомлений от Системы хранения данных в Систему редактирования и совместной работы об изменении настроек хранилища
Redis	База данных «ключ-значение» для не персистентных данных (в основном используется для хранения токенов и других авторизационных данных)
Sisyphus_sisyphussearch	Сервис, осуществляющий поиск по содержимому документов в Elasticsearch
Sisyphus_sisyphusworker	Сервис, осуществляющий передачу файлов из RabbitMQ в Elasticsearch
Storage S3/FS	Блок storage — осуществляет хранение файлов системы. В качестве хранилища FS в проекте используется GlusterFS. В качестве хранилища S3 в проекте используется MinIO

1.4 Состав дистрибутива

Дистрибутив Системы хранения данных представляет собой архив в формате *.tgz и включает в себя:

- набор Ansible плейбуков для развертывания ролей;
- архив образа Docker Registry;
- набор контейнеров для запуска Системы хранения данных;
- файлы хеша в форматах MD5 и SHA256.

1.5 Перечень технической документации

Перечень технической документации, представленный в таблице 3, предназначен для развертывания серверной части, настройки и дальнейшего администрирования продукта «МойОфис Профессиональный 3».

Комплект документации распространяется на компоненты продукта «МойОфис Профессиональный 3»:

- Систему редактирования и совместной работы;
- Систему хранения данных.

Таблица 3 — Перечень технической документации

Наименование документа	Используемые компоненты	Содержание документа
«"МойОфис Профессиональный 3". Системные требования»	Система редактирования и совместной работы, Система хранения данных	Системные и программные требования к продукту
«"МойОфис Профессиональный 3". Архитектура»	Система редактирования и совместной работы, Система хранения данных	Описание архитектуры продукта для выбора типа установки и выделения ресурсов для серверов
«"МойОфис Профессиональный 3". Система редактирования и совместной работы. Руководство по установке»	Система редактирования и совместной работы	Порядок установки системы редактирования и совместной работы
«"МойОфис Профессиональный 3". Система хранения данных. Руководство по установке»	Система хранения данных	Порядок установки системы хранения данных
«"МойОфис Профессиональный 3". Руководство по настройке»	Система редактирования и совместной	Настройка серверов продукта после установки и в ходе эксплуатации системы, а также процессов мониторинга и логирования

Наименование документа	Используемые компоненты	Содержание документа
	работы, Система хранения данных	
«"МойОфис Профессиональный 3". Руководство по администрированию»	Система редактирования и совместной работы, Система хранения данных	Функции управления тенантом в ходе эксплуатации системы
«"МойОфис Профессиональный 3". Руководство по резервному копированию»	Система хранения данных	Порядок резервного копирования баз данных, расположенных в системе хранения данных
«"МойОфис Профессиональный 3". Сервисно-ресурсная модель»	Система редактирования и совместной работы, Система хранения данных	Логическая модель сервиса, описывающая состав и взаимосвязи компонентов (ресурсов), которые совместно обеспечивают предоставление сервиса

1.6 Требования к персоналу

Для работы с ПО Администратору необходимо обладать релевантным опытом по следующим направлениям:

1. 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).

2. Работа с подсистемой виртуализации на уровне эксперта:

- установка Docker;
- запуск/остановка/перезапуск контейнеров;
- работа с реестром контейнеров;
- работа с VMware vSphere ESXi 6.5 и выше;
- получение параметров контейнеров;
- сеть в Docker, взаимодействие приложений в контейнерах;
- решение проблем контейнерной виртуализации.

3. Работа с командной строкой ОС Linux:

- знания в объеме курсов Red Hat RH124, RH134, RH254;
- знания в объеме, достаточном для сдачи сертификационного экзамена Red Hat EX300.

4. Работа со службой доменных имен DNS:
 - знание основных терминов (DNS, IP-адрес);
 - понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен);
 - знание типов записи и запросов DNS.
5. Знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI);
 - закрытый и открытый ключи;
 - сертификат открытого ключа;
 - регистрационный центр (RA);
 - сертификационный центр (CA);
 - хранилище сертификатов (CR).
6. Работа с системой автоматизации развертывания Ansible.
7. 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.

1.7 Типовые схемы установки

Структура сервиса может быть представлена двумя типами установки:

- standalone (на один виртуальный сервер или на несколько виртуальных серверов в рамках одного физического сервера);
- кластерная (все роли устанавливаются на разные виртуальные или физические серверы).

1.7.1 Standalone

Конфигурация без отказоустойчивости используется для разработки или демонстрации возможностей продукта.

Для установки продукта «МойОфис Профессиональный 3» в минимальной конфигурации необходимо использовать три сервера:

- сервер с ролью `operator` для управления процессом установки;
- сервер с ролью `cosa` для установки редакторов и дополнительного ПО;
- сервер с ролью `pgs` для размещения и хранения базовых библиотек и файлов.

1.7.2 Кластерная установка

Отказоустойчивая конфигурация, используемая для типовой установки продукта.

Для сохранения уровня отказоустойчивости не рекомендуется совмещать серверные роли между собой. Совмещение допускается в отдельных случаях для экономии ресурсов.

1.8 Порядок установки серверов

1. Необходимо подготовить сервер с ролью `operator` в соответствии с разделом «Подготовка сервера с ролью `operator`».

В качестве сервера с ролью `operator` может использоваться рабочий компьютер пользователя, отвечающий требованиям, указанным в документе «"МойОфис Профессиональный 3". Системные требования».

2. С помощью сервера с ролью `operator` следует подготовить инфраструктуру и выполнить установку Почтового сервера. Порядок установки почтового сервера представлен в документе «"МойОфис Профессиональный 3". Почтовая система. Руководство по установке почтового сервера».

3. С помощью сервера с ролью `operator` необходимо подготовить инфраструктуру и выполнить установку Системы хранения данных в соответствии с настоящим руководством.

4. С помощью сервера с ролью `operator` следует подготовить инфраструктуру и выполнить установку Системы редактирования и совместной работы в соответствии с документом . Система редактирования и совместной работы (СО). Руководство по установке».

1.9 Программные и аппаратные требования

Программные и аппаратные требования к текущей версии ПО указаны в документе «"МойОфис Профессиональный 3". Системные требования».

2 ПОДГОТОВКА К УСТАНОВКЕ

2.1 Конфигурирование ОС Astra

2.1.1 Установка на Astra SE 1.7 в защищенных вариантах

Основные отличия между вариантами защищенности Astra SE 1.7 приведены в таблице 4.

Таблица 4 — Уровни защищенности ОС Astra

Функция безопасности	Уровень защиты «Базовый»	Уровень защиты «Усиленный»	Уровень защиты «Максимальный»
Замкнутая программная среда	Не доступна	Доступна (по умолчанию выключена)	Доступна (по умолчанию выключена)
Очистка освобождаемой внешней памяти	Не доступна	Доступна (по умолчанию выключена)	Доступна (по умолчанию выключена)
Мандатный контроль целостности	Не доступна	Доступна (по умолчанию включена)	Доступна (по умолчанию включена)
Мандатное управление доступом	Не доступна	Не доступна	Доступна (по умолчанию включена)

Наименование ОС Астра в соответствии с уровнем защиты:

- Базовый уровень — Астра 1.7 «Орел»;
- Усиленный уровень — Астра 1.7 «Воронеж»;
- Максимальный уровень — Астра 1.7 «Смоленск».

Текущий уровень защищенности проверяется с помощью команды:

```
root@voronezh:~# astra-modeswitch list
0 base(orel)
1 advanced(voronezh)
2 maximum(smolensk)
root@voronezh:~# astra-modeswitch get
1
```

Текущий статус замкнутой программной среды проверяется с помощью команды:

```
root@voronezh:~# astra-digsig-control status
ACTIVE
```

Текущий статус очистки освобождаемой внешней памяти (очистка разделов подкачки и гарантированное удаление файлов) проверяется с помощью команды:

```
root@voronezh:~# astra-swapwiper-control status
ACTIVE
root@voronezh:~# astra-secdel-control status
ACTIVE
on /
```


Текущий статус мандатного контроля целостности проверяется с помощью команды:

```
root@voronezh:~# astra-mic-control status  
ACTIVE
```

Текущий статус мандатного управления доступом проверяется с помощью команды:

```
root@voronezh:~# astra-mac-control status  
INACTIVE
```

Текущий статус запрета включения бита выполнения проверяется с помощью команды:

```
root@voronezh:~# astra-nochmodx-lock status  
ACTIVE
```

2.1.2 Установка на усиленном уровне защищенности («Воронеж»)

Установка осуществляется Ansible от имени пользователя astra, для которого должна быть настроена возможность выполнять sudo без пароля.

1. Пользователю astra необходимо установить максимальный уровень целостности 63 (соответствует администратору ОС). Для проверки уровня целостности пользователя необходимо выполнить следующую команду:

```
root@voronezh:~# pdp-id -i  
63
```

2. Установка Ansible и работа невозможна при включенном запрете бита исполнения.

Перед началом установки на всех серверах следует выполнить команды:

```
astra@voronezh:~$ sudo astra-nochmodx-lock disable  
astra@voronezh:~$ sudo astra-nochmodx-lock status  
INACTIVE
```

3. Установка Ansible и работа Системы хранения данных невозможна при включенном режиме замкнутой программной среды. Для проверки статуса режима необходимо выполнить следующую команду:

```
astra@voronezh:~$ sudo astra-digsig-control status  
INACTIVE
```

4. При статусе ACTIVE перед началом установки на всех серверах следует выполнить команды:

```
astra@voronezh:~$ sudo astra-digsig-control disable  
astra@voronezh:~$ sudo reboot  
astra@voronezh:~$ sudo astra-digsig-control status  
INACTIVE
```

5. Необходимо проверить статусы параметров безопасности, значения которых должны соответствовать таблице 5.

Таблица 5 — Параметры безопасности по умолчанию

Наименование команды	Статус
astra-bash-lock status	INACTIVE
astra-commands-lock status	INACTIVE
astra-docker-isolation status	INACTIVE
astra-hardened-control status	INACTIVE
astra-interpreters-lock status	ACTIVE
astra-lkrig-control status	INACTIVE

Наименование команды	Статус
astra-macros-lock status	INACTIVE
astra-modban-lock status	INACTIVE
astra-overlay status	INACTIVE
astra-ptrace-lock status	ACTIVE
astra-sumac-lock status	INACTIVE
astra-shutdown-lock status	INACTIVE
astra-ufw-control status	INACTIVE
astra-ulimits-control status	INACTIVE

6. Для проверки доступности репозитория необходимо выполнить команду:

```
apt-get update
```

Команда должна завершаться без ошибки.

При наличии сбойного зеркала репозитория (например, <http://mirror.yandex.ru/astra/stable/orel/repository> orel InRelease), его необходимо удалить из директории `/etc/apt/sources.list`.

2.2 Настройка сетевых соединений

Настройку сетевого соединения необходимо выполнить на всех серверах, предназначенных для установки системы, в том числе на сервере с ролью `operator`.

Для работы серверов в локальной сети необходимо задать следующие параметры:

- IP-адрес;
- Маска подсети;
- Основной шлюз;
- DNS-сервер.

2.3 Подготовка сервера с ролью operator

2.3.1 Установка дополнительного ПО

В соответствии с документом «"МойОфис Профессиональный 3". Системные требования» на сервере с ролью `operator` необходимо установить пакеты дополнительного ПО.

Рекомендуется использовать «чистую» ОС для предотвращения появления ошибок, связанных с использованием конфигурационных файлов.

Конфигурационные файлы, установленные по умолчанию (например: `/etc/ansible/ansible.cfg`), необходимо удалить или заменить файлами из комплекта поставляемого ПО.

Для установки пакетов необходимо обеспечить серверу с ролью `operator` выход в интернет.



Запрещается установка последних версий дополнительного ПО, доступных в репозитории. Перед установкой следует ознакомиться с требованиями к версиям `ansible-core` и модулям Python.

2.3.2 Установка в сети без выхода в интернет

Для установки продукта «МойОфис Профессиональный 3» в локальной сети, без прямого выхода в интернет, необходимо обеспечить доступность дополнительных пакетов ПО. Перечень необходимого ПО приведен в документе «"МойОфис Профессиональный 3". Системные требования».

Для обеспечения доступности необходимо выполнить следующие действия:

- скачать файлы со стандартного репозитория с помощью прямого выхода в интернет;
- разместить файлы на локальном сервере;
- обеспечить доступ к серверу по локальной сети;
- установить ПО и настроить локальный репозиторий;
- выполнить замену стандартного репозитория на локальный;

Замена стандартного репозитория на локальный выполняется на сервере с ролью `operator`.

2.4 Подготовка инфраструктуры установки

2.4.1 Проверка и подготовка дистрибутива ПО

Для подготовки и проверки дистрибутива необходимо:

1. После копирования архива проверить его контрольную сумму и сравнить значение с данными полученными от вендора ПО:

– для MD5 с помощью команды:

```
md5sum -c MyOffice_PGS_3.0.tar.gz.md5
```

– для SHA256 с помощью команды:

```
sha256sum -c MyOffice_PGS_3.0.tar.gz.sha256
```

2. Распаковать содержимое архива в произвольный каталог и перейти в него:

```
mkdir install_MyOffice_PGS  
tar xf MyOffice_PGS_3.0.tgz -C install_MyOffice_PGS  
cd install_MyOffice_PGS
```



Не рекомендуется распаковывать новый дистрибутив в каталог предыдущей версии.

2.4.2 Настройка DNS

Перед началом установки необходимо настроить DNS-сервер, указав адрес установки сервера Nginx (см. таблицу 6).

Таблица 6 — Настройка DNS

Доменное имя с использованием <code><env></code>	Доменное имя без использования <code><env></code>	Хост	Описание
<code>admin-<env>.<default_domain></code>	<code>admin.<default_domain></code>	Nginx host	Адрес веб-панели администрирования Системы хранения данных
<code>pgs-<env>.<default_domain></code>	<code>pgs.<default_domain></code>	Nginx host	Адрес точки входа для API

Переменные `<env>` и `<default_domain>` заполняются в соответствии с разделом «Конфигурирование переменных файла `hosts.yml`» данного руководства. `Nginx host` соответствует адресу, указанному в файле `inventory` для роли `nginx` (подробнее см. в разделе «Конфигурирование ролей файла `hosts.yml`»).

Следует обеспечить доступ к адресу вида `admin-<env>.<default_domain>` для системных администраторов.

2.4.3 Настройка сертификатов

Для работы веб-интерфейса Системы хранения данных необходима установка SSL-сертификатов. Сертификаты необходимо разместить в каталоге, соответствующему доменному имени Системы хранения данных (`<default_domain>`).

Пример расположения каталога:

```
~/install_MyOffice_PGS/certificates/<default_domain>
```

где `~/install_MyOffice_PGS` — корневой каталог установки.

Подробное описание переменных см. в разделе «Конфигурирование переменных файла `hosts.yml`» данного руководства.

Список необходимых сертификатов размещен в таблице 7.

Таблица 7 — Перечень необходимых сертификатов

Наименование сертификата	Описание
server.crt	Содержит SSL-сертификат для <code>*.<default_domain></code> 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	При наличии самоподписанных или не публичных доверенных SSL-сертификатов

Рекомендуется использовать сертификаты, полученные от публичных центров сертификации.

2.4.4 Создание самоподписанного сертификата

Для создания самоподписанного сертификата в Системе хранения данных необходимо запустить исполняемый файл `gen_self_signed_cert.sh` из каталога установки. При запуске файла указывается домен, привязанный к создаваемому сертификату.

Пример команды создания сертификата:

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

После создания файл сертификата будет автоматически размещен в необходимом каталоге (см. в разделе «Настройка сертификатов»).

2.5 Настройка параметров установки

Директория установки содержит предзаполненные файлы конфигураций, подготовленные для упрощения настройки системы. Необходимо скопировать шаблон файла `inventory` в корневой каталог дистрибутива и заполнить секции `hosts` и `vars`. Шаблоны для заполнения в зависимости от типа конфигурации представлены в таблице 8.

Таблица 8 — Шаблоны файлов конфигурации

Тип конфигурации	Расположение шаблона
Конфигурация без отказоустойчивости	<code>~/install_MyOffice_PGS/inventory/hosts-sa.yaml</code>
Кластерная установка	<code>~/install_MyOffice_PGS/inventory/hosts-hl.yaml</code>
Кластерная установка с ArangoDB на одном сервере	<code>~/install_MyOffice_PGS/inventory/hosts-hl-sa.yaml</code>

Файл `inventory` использует формат `.yaml`, синтаксис которого описан в документации Ansible.

Операция копирования выполняется с помощью команды:

```
cp ~/install_MyOffice_PGS/inventory/hosts-sa.yaml hosts.yaml
```

После заполнения файл конфигурации рекомендуется хранить отдельно на внешнем ресурсе. Файл может потребоваться при восстановлении и/или переустановке системы.

2.5.1 Конфигурирование ролей файла `hosts.yaml`

Для определения роли сервера необходимо добавить его доменное имя или IP-адрес в соответствующую секцию в шаблоне файла `inventory`. После назначения роли серверу при установке будут выполнены команды Ansible.

Пример. Для назначения группы ролей `pythagoras` серверу с доменным именем `host.example.com` необходимо указать следующие значения:

```
pythagoras:
  hosts:
    host1.example.com:
```

При совмещении всех ролей на одном сервере в шаблоне файла `inventory` дублируется секция `hosts`. При изменении конфигурации установки возможно добавление или удаление серверов в группах.

Пример (фрагмент шаблона `hosts-sa.yaml`). Все роли и группы ролей устанавливаются на один сервер по адресу `host.example.com`:

```
all:
  children:
    pgs:
      children:
        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 установки в файле inventory указывается несколько IP-адресов или доменных имен серверов в соответствующей группе.

Текущей версией ПО поддерживается кластеризация для сервисов, перечисленных в таблице 9. В таблице указано минимально необходимое количество серверов для работы кластера. В зависимости от инфраструктуры и типа установки количество серверов может быть изменено.

Таблица 9 — Поддержка кластеризации

Наименование сервиса	Группа	Количество серверов
Aristoteles Dionis Epicure Euclid Heraclitus Pheidippides Polemon Sisyphusworker	Pythagoras	2
Keycloak	Keycloak	2
ArangoDB*	ArangoDB	2(1*)
	Arangodb_agent	3(1*)
Elasticsearch Sisyphussearch	Search	3
Redis	Redis	3
RabbitMQ	RabbitMQ	3
EtcD	EtcD	3
Nginx	Nginx	2
Postgres	Postgres	2
Docker Registry Syslog-ng Monitoring	Infrastructure	1
Storage	Storage	3

* — допускается установка сервиса ArangoDB на один сервер при кластерной установке

2.5.1.1 Конфигурация для кластерной установки

Пример конфигурации для кластерной установки находится в шаблоне `hosts-h1.yaml`. Группа хостов `arangodb_agent` используется для кластерной установки с использованием `agent`.

Для работы группы необходимо выделить не менее 3-х отдельных хостов (количество хостов должно быть нечетным числом). В ином случае группу следует оставить незаполненной:

```
arangodb_agent:
  hosts:
```

Роли `arangodb`, `arangodb_agent`, `search`, `postgres`, `storage` содержат дополнительные переменные `volume_device_<role>` и `volume_device_<role>_path`, необходимые для хранения данных на блочных устройствах, форматированных в файловую систему XFS.

Пример значений для переменных:

```
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 следует отформатировать в файловую систему XFS. На момент развертывания системы диск должен быть размонтирован (кроме ситуации повторного запуска).

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

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

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

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

При кластерной установке Системы редактирования и совместной работы потребуется настройка балансировщика нагрузки между Системой хранения данных и его auth-нодами. Для этого в `inventory` файле Системы хранения данных 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 Системы редактирования и совместной работы.

Дополнительная информация по интеграции с Системой редактирования и совместной работы описана в документе «"МойОфис Профессиональный 3". Руководство по настройке».

2.5.1.2 Конфигурация для кластерной установки с ArangoDB

Если при эксплуатации (использовании) продукта предусматривается более 3000 одновременно работающих пользователей, то рекомендуется установка сервиса ArangoDB на один сервер.



Одновременно работающие пользователи — пользователи единовременно выполняющие операции по редактированию документов. Общее количество таких пользователей суммируется из соотношения один пользователь = одна сессия редактирования или совместного редактирования одного документа.

Пример такой конфигурации находится в файле `hosts-h1-sa.yaml`. Для включения односерверной установки ArangoDB файл `inventory (hosts-h1-sa.yaml)` должен содержать переменные со следующими значениями:

```
PGS_CLUSTER = true
ARANGO_CLUSTER = false
```



При установке сервиса ArangoDB на один сервер отказоустойчивость сервисом не обеспечивается. Отказоустойчивость следует обеспечить с помощью настройки гипервизора и аппаратной части установки. Для сохранения данных рекомендуется настроить регулярное резервное копирование.

2.5.1.3 Сбор событий и метрик, хранение образов

Группа ролей `infrastructure` служит для хранения образов установки, а также сбора событий и метрик мониторинга системы. Их работа не блокирует работу Системы хранения данных.

События, собираемые со всех серверов установки сервисом Syslog-ng, будут храниться на сервере, назначенном группе ролей `infrastructure` в файле `inventory`. Путь к журналу событий будет выглядеть следующим образом:

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

Где:

- `<env>`, `<default_domain>` — переменные, заполненные в соответствии с разделом «Конфигурирование переменных файла `hosts.yml`»;
- `<service_name>` — имя сервиса;
- `<element>` — название файла лога.

2.5.2 Конфигурирование переменных файла hosts.yml

Процесс настройки переменных файла inventory состоит в заполнении секции `vars`. Доступные значения и способы заполнения секции указаны в таблице 10.

Параметры переменных необходимо указывать в двойных кавычках. Спецсимволы «<>{|&,*?@`\$!» в значениях переменных необходимо экранировать символом «\». Для обеспечения безопасности при работе ПО рекомендовано использовать надежные пароли, содержащие спецсимволы и произвольные символы разных регистров.

Доступ к сервисам Системы хранения данных обеспечивается с помощью переменных:

```

- DEV_MODE;
- PGS_CLUSTER;
- DEFAULT_DOMAIN;
- ENV;
- SWARM_NETWORK_ENCRYPTION;
- ADMIN_INTERFACE_EXT_PORT.
```

После заполнения перечисленных переменных будет сформирован адрес: `https://admin-<env>.<default_domain>:<admin_interface_ext_port>`, который служит для обеспечения доступа к сервису.

Таблица 10 — Переменные секции vars

Переменная	Значение и способ заполнения
DEV_MODE	Developers mode, режим разработчика. Принимает значения True и False. При значении True — открывает порты сервисов для внешнего подключения, в целях 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.yml по умолчанию — False, в шаблоне hosts-hl.yml по умолчанию — True, в шаблоне hosts-hl-sa.yml по умолчанию — True
ARANGO_CLUSTER	Включение и отключение кластерного режима установки сервиса Arango. Принимает значения True и False. В шаблоне hosts-sa.yml и hosts-hl-sa.yml по умолчанию — False, в шаблоне hosts-hl.yml по умолчанию — True
DEFAULT_DOMAIN	Зарегистрированный домен установки Системы хранения данных. Для корректной работы необходим установленный актуальный SSL-сертификат
ENV	Элемент доменного имени установки, предназначенный для разграничения доступа к сервисам Системы хранения данных

Переменная	Значение и способ заполнения
ADMIN_INTERFACE_EXT_PORT	<p>Порт Nginx для доступа к интерфейсу администратора, значение по умолчанию — 443.</p> <p>При изменении значения по умолчанию для порта в Системе хранения данных необходимо учесть новое значение в Системе редактирования и совместной работы (Подробнее см. в документе «"МойОфис Профессиональный 3". Система редактирования и совместной работы. Руководство по установке»).</p> <p>При включении интеграции с почтовой системой следует изменить порт для доступа к интерфейсу администратора Системы хранения данных в Почтовом сервере (Подробнее см. в документе «"МойОфис Профессиональный 3". Почтовая система. Руководство по установке почтового сервера»)</p>
API_INTERFACE_EXT_PORT	<p>Порт Nginx для доступа к API интерфейсу, значение по умолчанию — 443.</p> <p>При изменении значения по умолчанию для порта в Системе хранения данных необходимо учесть новое значение в компоненте Системе редактирования и совместной работы (Подробнее см. в документе «"МойОфис Профессиональный 3". Система редактирования и совместной работы. Руководство по установке»).</p> <p>При включении интеграции с почтовой системой следует изменить порт для доступа к pgs_api в параметрах Почтового сервера (Подробнее см. в документе «"МойОфис Профессиональный 3". Почтовая система. Руководство по установке почтового сервера»)</p>
SWARM_NETWORK_ENCRYPTION	Включает шифрование внутренней оверлейной сети Docker swarm, значение по умолчанию — False. Влияет на производительность системы
CUSTOM_CA	Заполняется при использовании самоподписанных сертификатов, допустимые значения: True или False. При значении True — файл ключа (например, в формате .crt) размещается в директории Certificates в корневом каталоге установки
MAX_TENANTS	Задаёт максимально возможное число tenants в текущей установке (максимально допустимое значение 100)
HERACLITUS_CRON	Задаёт время запуска сервиса Heraclitus. Для определения времени запуска используется формат, аналогичный формату Cron. Значение по умолчанию — "0 2 * * *".
KEYCLOAK_PASSWORD	Пароль для пользователя Системы хранения данных в Keycloak (он же Администратор Master Realm). Длина значения не менее 10 символов
KEYCLOAK_REALM_PASSWORD	Внутренний пароль для администраторов tenants Keycloak (используется только для сервисного обслуживания системы). Длина значения не менее 10 символов
KEYCLOAK_POSTGRES_PASSWORD	Пароль БД PostgreSQL (используется как хранилище для Keycloak). Длина значения не менее 10 символов
ARANGODB_PASSWORD	Пароль пользователя Системы хранения данных в ArangoDB
RABBITMQ_PASSWORD	Пароль пользователя RabbitMQ

Переменная	Значение и способ заполнения
REDIS_PASSWORD	Пароль доступа в Redis
PATRONI_REPLICATION_PASSWORD	Пароль для репликации БД PostgreSQL (только для кластерной установки)
GRAFANA_ADMIN_PASSWORD	Пароль доступа к интерфейсу Grafana в случае установки с ключом: -e monitoring_enable=true
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
IPTABLES_ENABLED	Устанавливает и настраивает службы межсетевого экрана (опционально). Доступные значения: True и False, по умолчанию — False
QUOTA_PER_GROUP	Выделенное место для хранения общих папок. указывается в байтах, значение по умолчанию — 10737418240 (10 Гбайт)
Блок default_tenant	
Блок default_tenant	Предназначен для создания тенанта по умолчанию, необходимого для дальнейшей работы с пользователями в веб-интерфейсе Системы хранения данных
ADMIN_PASSWORD	Пароль для администрирования тенанта (обязательный параметр, при отсутствии значения тенант создан не будет)
ADMIN_RECOVERY_EMAIL	Почта для восстановления доступа к тенанту (обязательный параметр, при отсутствии значения тенант создан не будет)
MAX_USERS	Количество пользователей в тенанте, значение по умолчанию — 1000
QUOTA_PER_USER	Выделенное пользователю место в хранилище, указывается в байтах, значение по умолчанию — 1000000000 (~1 Гбайт)
Блок storage	
Блок storage	Блок настроек системы хранения файлов
type	Выбор типа системы хранения файлов, доступны значения fs (файловая система) и s3 (объектное хранилище). В качестве хранилища fs в проекте используется GlusterFS. В качестве хранилища s3 в проекте используется MinIO
Блок fs	
path	Путь до файловой системы хранения fs. Значение должно заканчиваться символом «/». Значение по умолчанию — /media/storage
retention_file_time	Время хранения файлов после удаления из корзины, указывается в днях, значение по умолчанию — 30
Блок s3	
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
minio_used	True — если используется сервис MinIO.

Переменная	Значение и способ заполнения
	False — если используется стороннее s3-хранилище
use_old_minio	<p>Принимает значения: True/False</p> <p>При значении False из дистрибутива будет установлен MinIO версии RELEASE.2023-12-13T23-28-55Z</p> <p>При значении True будет установлен MinIO максимально совместимой версии RELEASE.2022-06-25T15-50-16Z</p> <p>Переменная со значением False предназначена:</p> <ol style="list-style-type: none"> 1. Для первичной установки продукта. 2. Если в инфраструктуре не используется собственное s3-хранилище. 3. Если в инфраструктуре не предустановлен MinIO ранних версий датой выпуска до 2022-06-26. <p>Переменная со значением true предназначена:</p> <ol style="list-style-type: none"> 1. Для последующей установки продукта (не первичной). 2. Для использования ранних версий MinIO, при условии что MinIO ранее был установлен (текущая используемая версия выпущена до 2022-06-26). 3. Для обновления с версий ≥ 2.7 до актуальной версии продукта, где в качестве storage type использовалось значение s3. <p>Для обновления MinIO с версии RELEASE.2022-06-25T15-50-16Z до RELEASE.2023-12-13T23-28-55Z необходимо использовать официальное руководство https://min.io/docs/minio/linux/operations/install-deploy-manage/migrate-fs-gateway.html</p>
minio_access_key	Переменная задается при использовании сервиса MinIO. Значение в произвольном виде, минимальная длина — 8 символов
minio_secret_key	Переменная задается при использовании сервиса MinIO. Значение в произвольном виде, минимальная длина — 8 символов
url	Ссылка для доступа к сетевому хранилищу. При использовании MinIO имеет следующий вид: <pre>http://pgs-<ENV>.<DEFAULT_DOMAIN>:9000.</pre> Значения <code><env></code> и <code><default_domain></code> соответствуют переменным, указанным в начале данной таблицы
secret_key	Параметр, соответствующий настройкам хранилища s3. При использовании сервиса MinIO совпадает со значением переменной <code>minio_secret_key</code>
access_key	Параметр, соответствующий настройкам хранилища s3. При использовании сервиса MinIO совпадает со значением переменной <code>minio_access_key</code>
bucket	Контейнер для хранения объектов в хранилище s3. При использовании хранилища s3 необходимо указать значение. При отсутствии контейнера — он будет создан при первой записи файлов
service_name	При использовании сервиса MinIO указывается значение s3

Переменная	Значение и способ заполнения
region_name	При использовании сервиса MinIO указывается значение myoffice
acl	Сущность для разграничения прав доступа, в случае с MinIO необязательна к заполнению
s3_max_capacity	Параметр, определяющий максимальное пространство, доступное в s3, указывается в байтах
Блок system	
TIMEZONE	Временная зона (часовой пояс) установки в формате базы tz. Значение по умолчанию — "Europe/Moscow"
Блок со	
Блок со	Переменные, которые необходимо заполнить для интеграции с Системой редактирования и совместной работы. Более подробно о заполнении блока см. в документе «"МойОфис Профессиональный 3". Система редактирования и совместной работы. Руководство по установке»
coapiurl	Путь доступа к API Системы редактирования и совместной работы. Данная переменная представляет собой URL-адрес и порт, указывающие на целевой сервер с ролью auth Системы редактирования и совместной работы. Пример: coapiurl: "https://co-api-url.ru:8443"
co_lb	Включает и выключает настройку балансировки с помощью сервиса Keeralived. Принимает значения True и False (только для кластерной установки)
vip_auth	Виртуальный IP-адрес, доступное значение — произвольный свободный IP-адрес в сети установки (только для кластерной установки)
lb_keeplived_pass	Пароль для сервиса keeplived (только для кластерной установки)
Блок installation_commons	
Блок installation_commons	Значения переменных данного блока должны соответствовать аналогичным в Системе редактирования и совместной работы, за исключением app_admin_password. Значение этой переменной генерируется администратором при установке Системы хранения данных. Более подробно о заполнении блока см. в документе «"МойОфис Профессиональный 3". Система редактирования и совместной работы. Руководство по установке»
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_PASSWORD	
CO_MANAGE_API_USERNAME	

Переменная	Значение и способ заполнения
	<code>co_manage_api_username</code> в конфигурации Системы редактирования и совместной работы
<code>CO_MANAGE_API_PASSWORD</code>	Пароль для API-авторизации в Системе редактирования и совместной работы. Должен совпадать со значением переменной <code>co_manage_api_password</code> в конфигурации Системы редактирования и совместной работы
<code>TWO_FA_ENCRYPTION_KEY</code>	Ключ для шифрования 2FA секретов, длиной 64 символа
<code>AUDIT_LOG_ENABLED</code>	Переменная предоставляет возможность включения в административном интерфейсе расширенного лога событий. Доступные значения: <code>True</code> и <code>False</code> , по умолчанию — <code>False</code>
<code>CHATBOT_ENABLED</code>	Включение и отключение интеграции Системы редактирования и совместной работы с сервисом ChatBot. Значение зависит от наличия сервиса в Системе редактирования и совместной работы. Доступные значения: <code>True</code> и <code>False</code> , по умолчанию — <code>False</code>
<code>POSEIDON_INTEGRATION</code>	Включение и выключение интеграции с «МойОфис Профессиональный 3». Почтовый сервер», доступные значения: <code>True</code> и <code>False</code>
Блок POSEIDON	
Блок POSEIDON	Параметры подключения к «МойОфис Профессиональный 3». Почтовый сервер», если включена интеграция. Подробные сведения об установке и настройке Почтового сервера см. в документе «МойОфис Профессиональный 3». Почтовая система. Руководство по установке почтового сервера»
<code>PBM_URL</code>	Ссылка для доступа к почтовому серверу «МойОфис Профессиональный 3». Почтовый сервер» в формате <code>https://pbm.example.com</code>
<code>PBM_USER_PASSWORD</code>	Переменная для авторизации через API «МойОфис Профессиональный 3». Почтовый сервер». Соответствует значению переменной <code>ds389_manager_user</code> при установке Почтового сервера
<code>SSL_VERIFY</code>	Параметры шифрования для почты. Принимает значения <code>True</code> и <code>False</code> , <code>False</code> — в случае использования самоподписанных сертификатов

2.5.3 Рекомендации по настройке дисков для ролей

1. Для серверов с ролями `storage`, `postgres`, `arangodb` и `search` рекомендуется выделить независимые диски или блочные устройства.

2. Для ролей `postgres`, `arangodb` и `search` монтирование выполняется автоматически во время установки. Путь к смонтированным ролям:

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

Где `<service_name>` — имя роли.

3. Для серверов с ролью `storage` монтирование независимых дисков или блочных дисков автоматически не производится. При необходимости перед установкой Системы хранения данных блочные устройства (разделы или диски) следует монтировать по директориям, указанным в таблице 11. Рекомендуется использовать форматирование XFS поверх форматирования LVM.

Таблица 11 — Точки монтирования для роли `storage`

Тип хранилища	Режим установки с поддержкой отказоустойчивости	Точка монтирования	Комментарий
fs*	-	/media/storage	Возможно использовать логический раздел
fs*	+	/gluster_bricks/pgs-files	-
s3	-	/opt/Pythagoras/minio/data/sa0/	-
s3	+	/opt/Pythagoras/minio/data[0-9]	0-9 — номер используемого диска

* — при использовании хранилища типа `fs` точка монтирования на серверах с ролью `pythagoras` задается с помощью переменной `path` в файле `inventory`.

4. При выборе типа хранилища `s3` следует ознакомиться с требованиями к конфигурации отказоустойчивости.

4.1 Хранилище GlusterFS устанавливается в режиме `replicated`, в котором количество нод/серверов в роли `storage` не влияет на потенциально доступное место для Системы хранения данных. При увеличении количества нод/серверов повышается отказоустойчивость.

Место хранения ограничено размером раздела тома хранения `brick`. При создании раздела `brick` рекомендуется использовать менеджер логических дисков LVM для обеспечения возможности расширения объема дискового пространства.

4.2 Требования к хранилищу MinIO представлены в таблице 12.

Таблица 12 — Конфигурация отказоустойчивости для хранилища S3 MinIO

Конфигурация отказоустойчивости	Количество нод/серверов	Количество независимых дисков*
минимальная	2	2
рекомендуемая	4	4

* — количество независимых дисков на сервер задается с помощью переменной `minio_drives_per_node`. Если значение для переменной не указано, при установке значение будет задано автоматически и равно «2».

4.3 При проектировании количества серверов/дисков для s3 следует учитывать требования ПО:

4.3.1 В `/opt/Pythagoras/minio/data` должны монтироваться диски с использованием файловой системы XFS.

4.3.2 Общее количество дисков включает в себя диски для хранения избыточных данных (MinIO будет использовать половину емкости для избыточного хранения данных) (см. таблицу 13).

Таблица 13 — Распределение дисков для избыточного хранения

Диапазон используемых дисков	Количество дисков для избыточного хранения данных
5 или меньше	2
6 - 7	3
8 или больше	4

4.3.3 При использовании более 16 дисков количество будет поделено на меньшие наборы, для которых будут справедливы требования п. 4.3.2.

4.4 Требования к распределению дисков п. 4.3 описаны для настроек MinIO по умолчанию.

Для изменения параметров необходимо воспользоваться инструкцией с сайта производителя:

<https://min.io/docs/minio/linux/reference/minio-server/settings/storage-class.html#minio-server-envvar-storage-class>



Из-за современной архитектуры серверных CPU существует вероятность деградации производительности при использовании более 8 NVMe на один сервер. При использовании HDD-дисков изменений в работе системы при возрастании количества нод/дисков не замечено.

2.5.4 Настройка межсетевого экранирования

Для обеспечения стабильной работы Системы хранения данных не рекомендуется использовать сетевое экранирование между серверами. Необходимые для работы ПО сетевые порты приведены в таблице 14.

Таблица 14 — Сетевые порты, используемые Системой хранения данных

Порт	Назначение
8851	Доступ к основному API Системы хранения данных
8852	REST API доступа к администрированию Системы хранения данных
8854	Веб-администрирование Системы хранения данных (административная панель управления)

Для доступа к интерфейсу администратора Nginx по умолчанию настроен 443 порт. Для корректной работы необходимо добавить порт в исключения брандмауэра в соответствии с настройками выбранной ОС установки.

Для доступа к API интерфейсу по умолчанию в Nginx настроен 443 порт. Для корректной работы следует открыть доступ только со стороны сервера Системы редактирования и совместной работы, для всех остальных подключений порт должен быть закрыт.

В целях ограничения доступа к API интерфейсу рекомендуется использовать различные порты для интерфейса администратора и API интерфейса.

2.5.5 Настройка дополнительных параметров установки

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

3 УСТАНОВКА

3.1 Порядок запуска установки

Для запуска установки Системы хранения данных необходимо перейти в каталог установки и выполнить следующую команду:

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

Где:

- `<hosts.yml>` — файл inventory (или путь к нему), сконфигурированный в соответствии с разделом «Настройка параметров установки»;
- `<additional ansible keys>` — дополнительные ключи установки (см. таблицу 15);

При успешном выполнении команды сервисы Системы хранения данных будут запущены автоматически.

Автоматическое обновление компонентов системы не включено в процесс установки ПО, обновление выполняется вручную администратором.

Таблица 15 — Дополнительные ключи установки

Значение ключа	Описание
<code>-e monitoring_enable=<value></code>	Устанавливает при значении True или не устанавливает при значении False сервисы мониторинга Prometheus и Grafana. По умолчанию — True
<code>-e content_search_enable=<value></code>	Устанавливает при значении True или не устанавливает при значении False сервисы для поиска по содержимому документов в облачных редакторах СО. По умолчанию — True
<code>-e kernel_ml_enable=<value></code>	Включает True или отключает False обновление ядра ОС (релизы ветки mainline). По умолчанию — True
<code>-e kernel_ml_deb_enable=<value></code>	Включает True или отключает False обновление ядра Debian-based ОС (релизы ветки mainline). По умолчанию — True

3.2 Проверка корректности установки

Для проверки корректности установки необходимо на сервере с ролью `pythagoras` выполнить следующую команду:

```
curl -X POST\  
https://pgs-<env>.<default_domain>:<api_interface_ext_port>/pgsapi/?\  
cmd=api_version | python3 -m json.tool
```

Где `<env>`, `<default_domain>` и `<api_interface_ext_port>` — переменные, заполненные в соответствии с разделом «Конфигурирование переменных файла hosts.yml».

Пример ожидаемого вывода:

```
{
  "response": {
    "API": "4.45.0",
    "Aristoteles": "13.2.32-5826",
    "WebAPI": "4.32.3",
    "success": "true"
  },
  "success": "true"
}
```

Для проверки запуска сервисов Системы хранения данных необходимо выполнить следующую команду:

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

Пример вывода:

```
pgs-arangodb_arangodb 1/1
pgs-elasticsearch_elasticsearch 1/1
pgs-etcd_etcd 1/1
pgs-haproxy_haproxy_monitoring 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-sisyphus_sisyphussearch 1/1
pgs-sisyphus_sisyphusworker 1/1
pgs_aristoteles 1/1
pgs_dionis 1/1
pgs_epicure 1/1
pgs_euclid 1/1
pgs_flower 1/1
pgs_heraclitus 1/1
pgs_pheidippides 1/1
pgs_polemon 1/1
```

При ошибке запуска значение напротив имени сервиса будет выглядеть «0/1».

3.3 Обновление

При обновлении Системы хранения данных с пропуском версии (например с 2.5 до 2.8) необходимо выполнить следующую команду:

```
docker exec $(docker ps -q -f name=pgs_aristoteles)\
bash -c "./run_all_migrations.sh"
```

4 КАРТА ПОРТОВ

4.1 Карта портов для внутренних соединений

Карта портов для внутренних соединений представлена в таблице 16.

Таблица 16 — Карта портов для внутренних соединений

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается(имя swarm service)	
nginx	nginx	443/tcp 5673/tcp 15673/tcp 9002/tcp	5672/tcp	rabbitmq	
			15672/tcp	rabbitmq	
			8851/tcp	aristoteles	
			8852/tcp	euclid	
			8854/tcp	polemon	
			9000/tcp	minio	
pythagoras	polemon	8854/tcp			
	euclid	8852/tcp	2379/tcp	etcd	
			6379/tcp	redis	
			8080/tcp	keycloak	
			8529/tcp	arangodb	
			7002/tcp	dionis	
			5672/tcp	rabbitmq	
	aristoteles	8851/tcp	2379/tcp	etcd	
			6379/tcp	redis	
			8080/tcp	keycloak	
			8529/tcp	arangodb	
			7000/tcp	sisyphus	
			2379/tcp	euclid	
	heraclitus	-	-	5672/tcp	rabbitmq
				2379/tcp	etcd
				6379/tcp	redis
				8529/tcp	arangodb
				8852/tcp	euclid
				5672/tcp	rabbitmq
	epicure	-	-	8080/tcp	keycloak
				8529/tcp	arangodb
				6379/tcp	redis
				8529/tcp	arangodb
				6379/tcp	redis
				8529/tcp	arangodb
	flower	5555/tcp	-	6379/tcp	redis
				6379/tcp	redis
	dionis	7002/tcp	-	6379/tcp	redis
				2379/tcp	etcd
	pheidippides	-	-	6379/tcp	redis
2379/tcp				etcd	
8851/tcp				aristoteles	
keycloak	keycloak	8080/tcp	8080/tcp	keycloak(в рамках кластера)	
			2379/tcp	etcd	

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается(имя swarm service)
			5432/tcp	postgres в SA
			5000/tcp	postgres в кластере
arangodb	arangodb	8529/tcp 8530/tcp	8529/tcp 8530/tcp	arangodb_agent(в режиме кластера)
arangodb_agent	arangodb_agent	8529/tcp 8530/tcp	8529/tcp 8530/tcp	arangodb(в режиме кластера)
search	sisyphus	7000/tcp	2379/tcp	etcd
			9200/tcp	elasticsearch
			5672/tcp	rabbitmq
	elasticsearch	9200/tcp		
rabbitmq	rabbitmq	5672/tcp 15672/tcp		
redis	redis	6379/tcp		
etcd	etcd	2379/tcp		
postgres	postgres	5432/tcp 8008/tcp 5000/tcp 5001/tcp	2379/tcp	etcd
			5432/tcp 8008/tcp 5000/tcp 5001/tcp	postgres
infrastructure	haproxy_postgres	20432/tcp*	5432/tcp	для всех postgres сервисов
	haproxy	20432/tcp*	5432/tcp	для всех postgres сервисов
		23529/tcp*	8529/tcp	для всех arangodb сервисов
		23080/tcp*	8080/tcp	для всех keycloak сервисов
		30692/tcp*	15692/tcp	для всех RabbitMQ сервисов
		20555/tcp	5555/tcp	для сервиса flower

* — увеличение количества портов в зависимости от количества серверов в сервисе.

Пример:

Для 3-х сервисов arangodb порты будут: 23529/tcp, 23530/tcp, 23531/tcp.

Для 4-х сервисов arangodb порты будут: 23529/tcp, 23530/tcp, 23531/tcp, 23532/tcp.

** — для работы docker swarm необходимо открыть порты: 2376/tcp, 2377/tcp, 7946/tcp, 7946/udp, 4789/udp.

*** — на момент установки необходимо, чтобы был доступен 5001/tcp с сервера с ролью `infrastructure`.

4.2 Карта внешних портов

Карта портов представлена в таблице 17.

Таблица 17 — Карта внешних портов

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается (имя swarm service)
Внешние подключения относительно swarm кластера				
nginx	nginx	443/tcp 5673/tcp 15673/tcp 9002/tcp	9000/tcp	Серверы с ролью storage для подключения к S3 MinIO и к другим серверам с s3 сервисом
			514/udp	syslog локально на IP 172.17.0.1
pythagoras	polemon		514/udp	syslog локально на IP 172.17.0.1
	euclid	8852/tcp	6379/tcp	Серверы с ролью redis
			9000/tcp	Серверы с ролью storage для подключения к S3 MinIO и к другим серверам с s3 сервисом
				Почтовый сервер (если нужна интеграция)
			514/udp	syslog локально на IP 172.17.0.1
	aristoteles	-	6379/tcp	Серверы с ролью redis
			9000/tcp	Серверы с ролью storage для подключения к S3 MinIO и к другим серверам с s3 сервисом
				Почтовый сервер (если нужна интеграция)
			514/udp	syslog локально на IP 172.17.0.1
	heraclitus	-	9000/tcp	Серверы с ролью storage для подключения к S3 MinIO и к другим серверам с s3 сервисом
			6379/tcp	Серверы с ролью redis
			514/udp	syslog локально на IP 172.17.0.1
epicure	-		514/udp	syslog локально на IP 172.17.0.1

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается (имя swarm service)
	flower	-	514/udp	syslog локально на IP 172.17.0.1
	pheidippides	-	514/udp	syslog локально на IP 172.17.0.1
keycloak	keycloak	-	514/udp	172.17.0.1
arangodb	arangodb	-	514/udp	syslog локально на IP 172.17.0.1
arangodb_agent	arangodb_agent	-	514/udp	syslog локально на IP 172.17.0.1
search	sisyphus	-	9000/tcp	Серверы с ролью storage для подключения к S3 MinIO и к другим серверам с s3 сервисом
			514/udp	syslog локально на IP 172.17.0.1
	elasticsearch	-	514/udp	syslog локально на IP 172.17.0.1
rabbitmq	rabbitmq	-	514/udp	syslog локально на IP 172.17.0.1
redis	redis	6379/tcp	514/udp	syslog локально на IP 172.17.0.1
etcd	etcd	-	514/udp	syslog локально на IP 172.17.0.1
postgres	postgres	-	514/udp	syslog локально на IP 172.17.0.1
infrastructure	haproxy_postgres	20432/tcp*	514/udp	syslog локально на IP 172.17.0.1
	haproxy	20432/tcp*	514/udp	syslog локально на IP 172.17.0.1
		23529/tcp*	514/udp	syslog локально на IP 172.17.0.1
		23080/tcp*	514/udp	syslog локально на IP 172.17.0.1
		30692/tcp*	514/udp	syslog локально на IP 172.17.0.1
		20555/tcp	514/udp	syslog локально на IP 172.17.0.1
За пределами swarm сервиса				
storage	minio	9002/tcp	-	-
infrastructure	nct_syslog_ng	514/udp	-	-
	grafana	3000/tcp	514/udp	syslog локально на IP 172.17.0.1
			9090/tcp	prometheus

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается (имя swarm service)
				(первый сервер с ролью <code>infrastructure</code>)
	prometheus	9090/tcp	514/udp	syslog локально на IP 172.17.0.1
			9100/tcp	pgs_node_exporter (все сервера в файле inventory)
			9101/tcp	cadvisor (все сервера в группе pgs)
			9187/tcp	pgs_postgres_exporter (все сервера в группе postgres)
			23080/tcp*	haproxy (обращение идет через <code>docker_gwbridge_ip</code>)
			23529/tcp*	haproxy (обращение идет через <code>docker_gwbridge_ip</code>)
			30692/tcp*	haproxy (обращение идет через <code>docker_gwbridge_ip</code>)
			9121/tcp	redis_exporter (все сервера в группе redis)
	redis_exporter	9121/tcp	6379/tcp	redis(все сервера в группе redis)
	postgresql_exporter	9187/tcp	20432/tcp*	haproxy (обращение идет через <code>docker_gwbridge_ip</code>)
	cadvisor	9101/tcp	-	-
	node-exporter	9100/tcp	-	-
	Docker-registry***	5001/tcp	-	-

* — увеличение количества портов в зависимости от количества серверов в сервисе.

Пример:

Для 3-х сервисов arangodb порты будут: 23529/tcp, 23530/tcp, 23531/tcp.

Для 4-х сервисов arangodb порты будут: 23529/tcp, 23530/tcp, 23531/tcp, 23532/tcp.

** — для работы docker swarm необходимо открыть порты: 2376/tcp, 2377/tcp, 7946/tcp, 7946/udp, 4789/udp.

*** — на момент установки необходимо, чтобы был доступен 5001/tcp с сервера с ролью `infrastructure`.

4.3 Рекомендации по открытым портам и доступам

Необходимо обеспечить внешние входящие соединения для серверов с ролью `nginx` (порты перечислены в таблице 17):

- на всех серверах для использования `ssh` необходимо открыть порт `22/tcp`;
- все порты, необходимые для работы ПО `Docker Swarm` и `Docker`;
- доступ до сервера с ролью `infrastructure` для просмотра `Grafana dashboard`;

Доступ для дополнительного ПО и интеграции:

- при установке `GlusterFS` необходимо открыть порты: `24007/tcp`, `24008/tcp`, `49152-49156/tcp` для серверов с ролью `storage` и `pythagoras`;
- при интеграции с `s3` доступ до `s3` хранилища;
- при интеграции с «МойОфис Профессиональный 3». Почтовый север» исходящие подключения к серверу почты.

Приложение А

Известные проблемы и способы их решения

А.1 Бесконечная загрузка во вкладке «Группы» панели администратора

Описание проблемы:

Возникновение бесконечной загрузки во вкладке «Группы» панели администратора Системы хранения данных.

Для просмотра журнала событий необходимо подключиться к серверу с ролью `infrastructure` и выполнить следующую команду:

```
tail -n 100 /var/log/pgs/<env>.<default_domain>/euclid/critical.log
```

где `<env>`, `<default_domain>` — переменные из файла `inventory`.

Пример отображения ошибки в журнале событий:

```
RITICAL - 2023-10-31 12:53:04,037 - pgs.euclid - GET /tenants/Default/groups,
Internal server error 500 | - ms
Headers: {'X-FORWARDED-FOR':
...
...
Error: None
Traceback (most recent call last):
  File "/usr/local/lib/python3.11/site-packages/falcon/api.py", line 269, in
  __call__
    responder(req, resp, **params)
  File "/usr/local/lib/python3.11/site-
packages/falconswaggerautodoc/schema_decorators.py", line 42, in wrapped
    f(self, *f_args, **f_kwargs)
  File "/opt/Pythagoras/Euclid/endpoints/groups.py", line 91, in on_get
    tenant=req.tenant).data}
    ^^^^^
  File "/opt/Pythagoras/Euclid/serializers/group_serializers.py", line 64, in
  data
    return [self._serialize_group(group) for group in self.groups]
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/opt/Pythagoras/Euclid/serializers/group_serializers.py", line 64, in
<listcomp>
    return [self._serialize_group(group) for group in self.groups]
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/opt/Pythagoras/Euclid/serializers/group_serializers.py", line 47, in
_serialize_group
    res["users"] = self.serialize_groupmembers(users)
    ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
  File "/opt/Pythagoras/Euclid/serializers/group_serializers.py", line 78, in
serialize_groupmembers
    if "middle_name" in user["attributes"] else ""
    ~~~~~^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
KeyError: 'attributes'
```

Решение:

1. Запустить на сервере с ролью keycloak следующую команду:

```
docker exec $(docker ps -qf name=keycloak)\
/opt/jboss/keycloak/bin/kcadm.sh create clear-user-cache\
-r <realm> -s realm=<realm> --server\
http://localhost:8080/auth --realm master\
--user pgs --password <KEYCLOAK_PASSWORD>
```

2. Запустить на сервере с ролью pythagoras следующую команду:

```
docker exec $(docker ps -q -f name=pgs_aristoteles)\
bash -c "python initializers/RedisInit.py"
```

A.2 Не запускается сервис SisyphusWorker

Описание проблемы:

Не запускается сервис SisyphusWorker и журнал событий содержит следующие ошибки:

```
pgs-sisyphus_sisyphusworker.1.hvjracizck85@ | etcd
pgs-sisyphus_sisyphusworker.1.hvjracizck85@ | 2379
pgs-sisyphus_sisyphusworker.1.hvjracizck85@ | 2023/11/13 16:58:24 can't
get arango config with error: client: etcd cluster is unavailable or
misconfigured; error #0: client: endpoint http://etcd:2379 exceeded
header timeout
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | etcd
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | 2379
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | level=error ts=2023-11-
13T16:58:31Z type=rabbit_wrapper err="dial tcp 10.0.1.14:5672: connect:
connection refused"
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | panic: Can't create rabbit
wrapper
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ |
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | goroutine 1 [running]:
pgs-sisyphus_sisyphusworker.1.r7xpttilp7an@ | main.main()
| /go/src/cmd/worker/main.go:29 +0x80a
pgs-sisyphus_sisyphusworker.1.krylr9x8vcdg@ | etcd
pgs-sisyphus_sisyphusworker.1.krylr9x8vcdg@ | 2379
```

Необходимо проверить статус работы сервиса RabbitMQ с помощью команды:

```
docker service ps --format 'table {{.Name}}\t{{.DesiredState}}'\
pgsrabbitmq_rabbitmq
```

Пример ответа:

NAME	DESIRED STATE
pgs-rabbitmq_rabbitmq.1	Running

Проверить, что журнал событий RabbitMQ содержит следующие сообщения:

```
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
Try to reach pgs-rabbitmq_rabbitmq.3.yq5fexvo3q5g9afw5c8hkotkt
```

Решение:

1. Уменьшить количество репликаций для сервиса с помощью команды:

```
docker service scale pgs-rabbitmq_rabbitmq=1
```

2. Выполнить перезапуск последнего docker контейнера сервиса RabbitMQ

(необходимо выполнить данную команду на ноде, где запущен данный контейнер)

```
docker restart $(docker ps -q -f name=pgs-rabbitmq)
```

3. Проверить статус работы сервиса SisyphusWorker с помощью команды:

```
docker service ps pgs-sisyphus_sisyphusworker --format 'table {{.Name}}\nt{{.DesiredState}}'
```

Пример ответа:

NAME	DESIRED STATE
pgs-sisyphus_sisyphusworker.1	Running
pgs-sisyphus_sisyphusworker.2	Running
pgs-sisyphus_sisyphusworker.3	Running

4. Восстановить кластер для сервиса RabbitMQ с помощью команды:

```
docker service scale pgs-rabbitmq_rabbitmq=3
```

A.3 Ошибка синхронизации пользователя при настроенной синхронизации с Active Directory

Описание проблемы:

Отсутствие у пользователя в БД (PostgreSQL) значения поля `federation_link`, вызывает ошибку обновления данных пользователя при синхронизации и другие ошибки.

Пример ошибки:

```
Apr 25 14:33:04 pgs-lime.myoffice-app.ru keycloak[23752]: 2024-04-25 14:33:04,967 ERROR [org.keycloak.services.error.KeycloakErrorHandler] (executor-thread-29) Uncaught server error: java.lang.NumberFormatException: Cannot parse null string
```

Решение:

На сервере с ролью `postgres` выполнить запрос на обновление поля:

```
update public.user_entity
set federation_link='<federation-link-uuid>'
where username=...;
```

Значение поля `federation-link-uuid` можно получить из логов сервиса Keycloak.

Внутри одной федерации `federation-link-uuid` будет одинаковым. Допускается скопировать значение поля другого пользователя такой же федерации.