МойОфис

Частное Облако 2

В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

Руководство по установке

СИСТЕМА ХРАНЕНИЯ ДАННЫХ (PGS)

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«МОЙОФИС ЧАСТНОЕ ОБЛАКО 2» В ВАРИАНТЕ ИСПОЛНЕНИЯ ГОСТ

СИСТЕМА ХРАНЕНИЯ ДАННЫХ (PGS)

РУКОВОДСТВО ПО УСТАНОВКЕ

2.8G

На 45 листах

Москва
2024

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 9
1.3 Структура 10
1.4 Состав дистрибутива 12
1.5 Перечень технической документации 12
1.6 Требования к персоналу 13
1.7 Типовые схемы установки 15
1.7.1 Standalone 15
1.7.2 Кластерная установка 15
1.7.3 Порядок установки серверов 15
1.8 Программные и аппаратные требования 16
2 Подготовка к установке 17
2.1 Конфигурирование ОС Astra 17
2.1.1 Установка на Astra SE 1.7 в защищенных вариантах 17
2.1.2 Установка на усиленном уровне защищенности («Воронеж») 18
2.2 Настройка сетевых соединений 19
2.3 Подготовка сервера с ролью operator 20
2.3.1 Установка дополнительного ПО 20
2.3.2 Установка в сети без выхода в интернет 20
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 Настройка ГОСТ-шифрования и сертификатов 21
2.4.5 Создание самоподписанного сертификата PGS 22
2.5 Настройка параметров установки 22
2.5.1 Конфигурирование файла inventory: hosts 23
2.5.2 Конфигурирование файла inventory: переменные 26

2.5.3 Рекомендации по настройке дисков для ролей 31
2.5.3.1 Настройка межсетевого экранирования 32
2.5.4 Настройка дополнительных параметров установки 33
3 Установка 34
3.1 Порядок запуска установки 34
3.2 Проверка корректности установки 34
3.3 Обновление 35
4 Карта портов PGS 36
4.1 Карта портов для внутренних соединений 36
4.2 Карта внешних портов 38
4.3 Рекомендации по открытым портам и доступам 41
5 Техническая поддержка 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, использующаяся 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
PGS	Pythagoras, Система хранения данных в составе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ»
PSN	Poseidon, приложение почты, календаря и контактов «МойОфис Почта»
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

«МойОфис Частное Облако 2» в варианте исполнения ГОСТ — комплекс безопасных веб-сервисов и приложений для организации хранения, доступа и совместной работы с файлами и документами внутри компании, использующих отечественные средства криптографической защиты информации. Взаимодействие всех клиентских приложений с серверными системами осуществляется по сетевым каналам, защищенным с помощью протокола TLS с использованием отечественной криптографии.

В состав продукта входят:

– Система хранения данных для безопасного хранения корпоративных файлов иобеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей;

– Система редактирования и совместной работы для индивидуального и совместного редактирования презентаций, текстовых и табличных документов;

– Административная панель системы хранения для управления пользователями, группами, общими папками, доменами и тенантами.

В состав продукта входят следующие приложения для работы в веб-браузерах и намобильных устройствах:

– «МойОфис Документы» — веб-приложение для организации структурированного хранения файлов, выполнения операций с файлами и папками, настройки совместного доступа;

– «МойОфис Текст» — веб-редактор для быстрого и удобного создания и форматирования текстовых документов любой сложности;

– «МойОфис Таблица» — веб-редактор для создания электронных таблиц, ведения расчетов, анализа данных и просмотра сводных отчетов;

– «МойОфис Презентация (Beta)» — веб-редактор для создания, оформления и демонстрации презентаций;

– «МойОфис Документы» для мобильных платформ — приложение для просмотра и редактирования текстовых документов, электронных таблиц и презентаций, просмотра PDF-файлов, а также доступа к облачным хранилищам на смартфонах и планшетах с ОС Android, iOS и iPadOS.

Подробное описание возможностей продукта приведено в документе« «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Функциональные возможности».

Функциональные возможности, предоставляемые PGS, 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 2» в варианте исполнения ГОСТ);
– широкие возможности по работе в собственном домене;
– интеграцию с другими компонентами ПО «МойОфис Частное Облако 2» в варианте исполнения ГОСТ: СО (Редакторы) и PSN (Почта).

Данный документ описывает установку Системы хранения данных (PGS).

1.2 Описание архитектуры

Система хранения данных (далее — PGS) является составным компонентом ПО «МойОфис Частное Облако 2» в варианте исполнения ГОСТ, в которое также входит Система редактирования и совместной работы (СО) – программные решения для редактирования текста, таблиц и презентаций.

Общая архитектурная схема «МойОфис Частное Облако 2» в варианте исполнения ГОСТ приведена на рисунке 1.

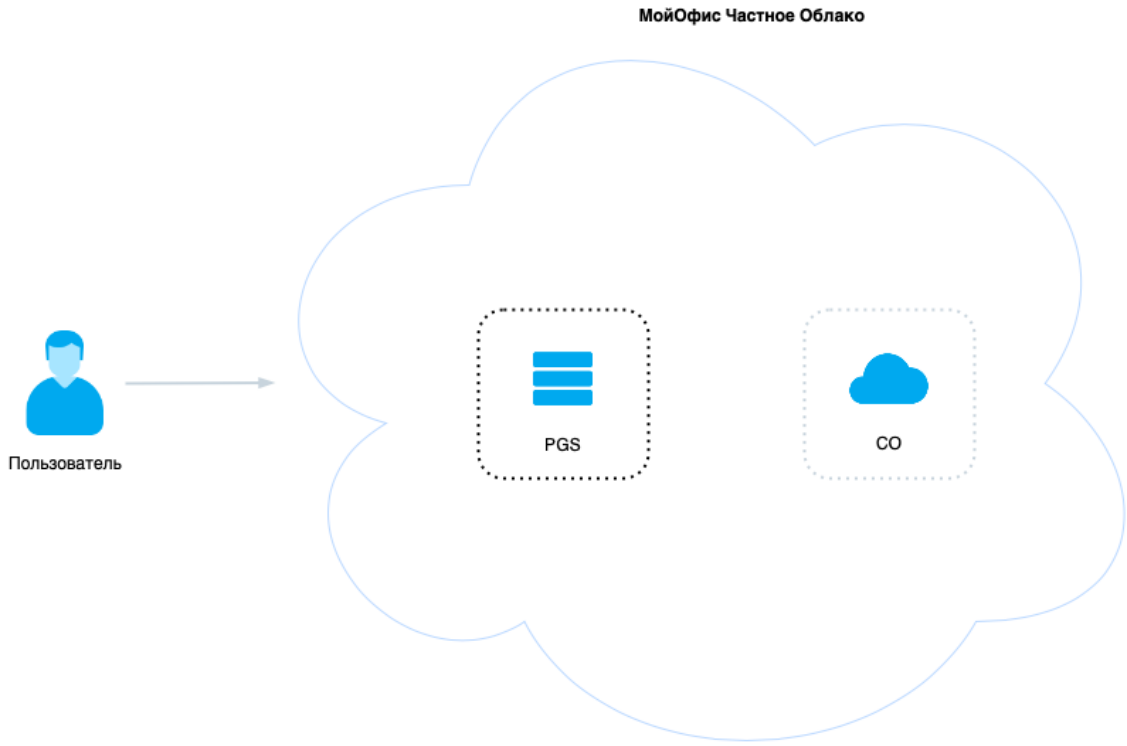

Рисунок 1 — Общая архитектурная схема «МойОфис Частное Облако 2» в варианте исполнения ГОСТ

Все элементы «МойОфис Частное Облако 2» в варианте исполнения ГОСТ 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.

Более подробно об этом указано в соответствующих руководствах по установке компонентов «МойОфис Частное Облако 2» в варианте исполнения ГОСТ.

1.3 Структура

Внутренняя структура PGS представляет собой набор сервисов, обеспечивающих работу ПО и взаимодействие с другими компонентами «МойОфис Частное Облако 2» в варианте исполнения ГОСТ. Более подробно сервисы (представленные в виде установочных ролей) описаны в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Архитектура».

Детальная архитектурная схема PGS приведена на рисунке 2.

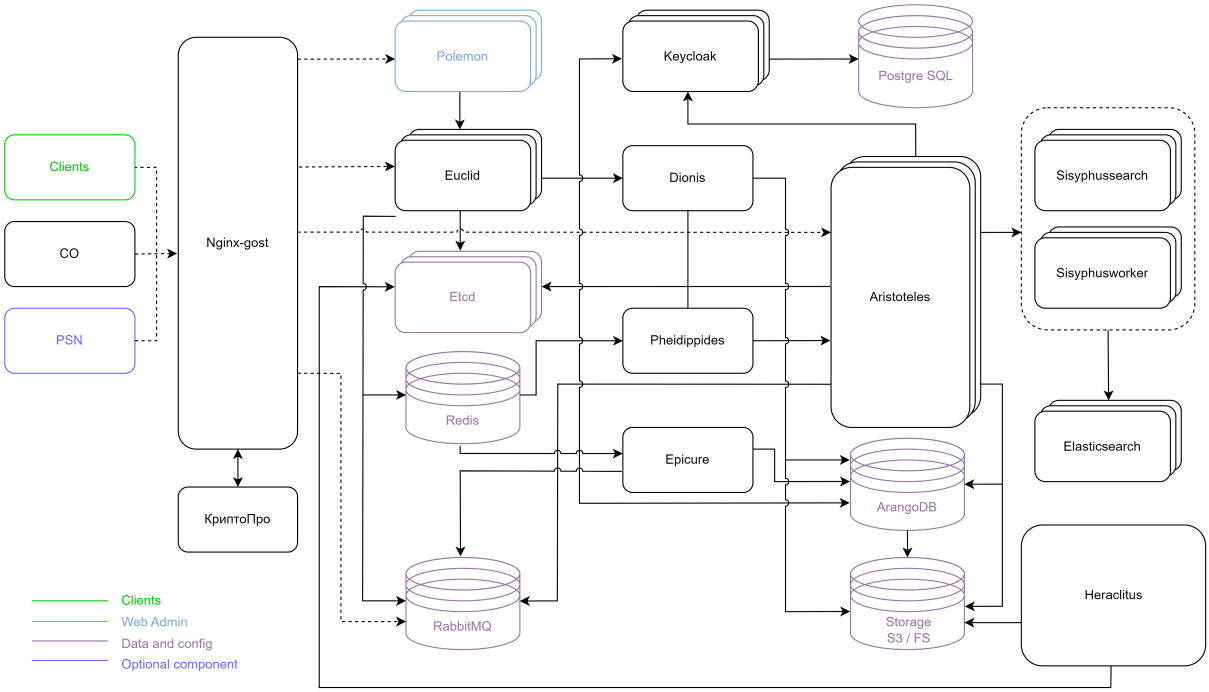

Рисунок 2 — Архитектурная схема PGS

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

Таблица 2 — Перечень сервисов PGS

Наименование сервиса	Описание
КриптоПро	Сервис, обеспечивающий шифрование при работе с документами
Arangodb	База данных, содержащая метаданные файлов (например, информацию о владельце документа, правах доступа и пр.)
Aristoteles	Сервер приложений, выступающий backend-частью для компонентов CO 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 по хранящимся файлам
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-gost	Прокси-сервис, обеспечивающий доступ до: rabbitmq, aristotels, euclid, polemon
Pheidippides	Сервис, осуществляющий обработку событий в Redis каналах (автоматическая блокировка IP-дресов/публичных ссылок)
Polemon	Сервис веб-администрирования Euclid (веб-интерфейс административной панели)
Postrgres	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 PGS>CO 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

Наименование сервиса	Описание
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 PGS представляет собой архив в формате *.tgz и включает в себя:

– набор Ansible плейбуков для развертывания ролей;

– архив образа Docker Registry;

– набор контейнеров для запуска PGS;

– 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 Частное Облако 2» в варианте исполнения ГОСТ.

Комплект документации распространяется на компоненты продукта «МойОфис Частное Облако 2» в варианте исполнения ГОСТ:

– Систему редактирования и совместной работы (CO);

– Систему хранения данных (PGS).

Таблица 3 — Перечень технической документации

Наименование документа	Используемые компоненты	Содержание документа
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Системные требования»	CO, PGS	Системные и программные требования к продукту
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Архитектура»	CO, PGS	Описание архитектуры продукта для выбора типа установки и выделения ресурсов для серверов
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Система редактирования и совместной работы (CO). Руководство по установке»	CO	Порядок установки системы редактирования и совместной работы (CO)
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Система хранения данных (PGS). Руководство по установке»	PGS	Порядок установки системы хранения данных (PGS)

Наименование документа	Используемые компоненты	Содержание документа
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по настройке»	CO, PGS	Настройка серверов продукта после установки и в ходе эксплуатации системы, а также процессы мониторинга и логирования
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по администрированию»	CO, PGS	Функции управления тенантом в ходе эксплуатации системы
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по резервному копированию»	PGS	Порядок резервного копирования баз данных, расположенных в системе хранения данных
«"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Сервисно-ресурсная модель»	CO, PGS	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 сервера или физические сервера).

1.7.1 Standalone

Конфигурация без отказоустойчивости используется для разработки или демонстрации возможностей продукта.

Для установки продукта «МойОфис Частное Облако 2» в варианте исполнения ГОСТ 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.

1.7.3 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 Частное Облако 2" в варианте исполнения ГОСТ. Системные требования».

2. Если комплект поставляемого ПО включает в себя продукт МойОфис Почта 2», то необходимо выполнить установку почтового сервера, с помощью сервера с ролью `operator`.

Порядок установки почтового сервера представлен в документе «МойОфис Почта 2». Руководство по установке почтового сервера.

3. С помощью сервера с ролью `operator` необходимо подготовить инфраструктуру и выполнить установку Системы хранения данных (PGS).

4. С помощью сервера с ролью `operator` необходимо подготовить инфраструктуру и выполнить установку Системы редактирования и совместной работы (СО).

5. Для дальнейшей работы сервер с ролью `operator` не используется, и может потребоваться только для переустановки системы или отдельных сервисов.

6. С помощью документов по настройке, перечисленных в разделе «Перечень технической документации», выполнить необходимые интеграции и установить параметры сервисов.

1.8 Программные и аппаратные требования

Программные и аппаратные требования к текущей версии ПО указаны в документе

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 уровнень 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). Проверить уровень целостности пользователя возможно с помощью команды:

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

2. Установка Ansible и работа невозможна при включенном запрете включения бита выполнения. Перед началом установки на всех серверах необходимо выполнить команду:

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

3. Установка Ansible и работа PGS невозможна при включенном режиме замкнутой программной среды. Необходимо проверить статус режима с помощью команды:

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

INACTIVE

4. При статусе ACTIVE перед началом установки на всех серверах необходимо выполнить команду:

```
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

Наименование команды	Статус
astra-lkrg-control status	INACTIVE
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. Следует проверить доступность репозиториев, для проверки 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

Настройка сетевого соединения должна быть выполнена 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

2.3.2 Установка в сети без выхода в интернет

Для установки продукта «МойОфис Частное Облако 2» в локальной сети, без прямого выхода в интернет, необходимо обеспечить доступность дополнительных пакетов ПО. Перечень необходимого ПО приведен в документе

2.4 Подготовка инфраструктуры установки

2.4.1 Проверка и подготовка дистрибутива ПО

Для выполнения проверки и подготовки 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_2.8.tar.gz.md5
```

– для SHA256 с помощью команды:

```
sha256sum -c MyOffice_PGS_2.8.tar.gz.sha256
```

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

```
mkdir install_MyOffice_PGS
tar xf MyOffice_PGS_2.8.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	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 «Конфигурирование файла inventory: переменные» данного руководства. Nginx host

соответствует адресу, указанному в файле inventory для роли `nginx` (подробнее в разделе «Конфигурирование файла inventory: hosts»).

Адрес вида `admin-<env>.<default_domain>` должен быть доступен для системных администраторов.

2.4.3 Настройка сертификатов

Для работы веб-интерфейса PGS необходима установка SSL-сертификатов. Сертификаты необходимо разместить в каталоге, соответствующему доменному имени PGS (`<default_domain>`). Пример расположения каталога:

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

где `~/install_MyOffice_PGS` – корневой каталог установки.

Подробное описание переменных представлено в разделе «Конфигурирование файла inventory: переменные» данного руководства.

Список необходимых сертификатов размещен в таблице 7.

Таблица 7 — Перечень необходимых сертификатов

Наименование сертификата	Описание
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	При наличии самоподписанных или не публичных доверенных SSL-сертификатов

Рекомендуется использовать сертификаты, полученные от публичных центров сертификации.

2.4.4 Настройка ГОСТ-шифрования и сертификатов

Для установки «МойОфис Хранилище» с поддержкой ГОСТ шифрования необходимо сформировать pfx-контейнер из сертификатов, указанных в разделе «Настройка сертификатов».

Сформированный pfx-контейнер `certkey-rsa.pfx` необходимо разместить в директории `~\MyOffice_PGS_XXXX.XX\certificates\gost\<DEFAULT_DOMAIN>`.

Пример команды создания pfx-контейнера с помощью утилиты OpenSSL:

```
openssl pkcs12 -export -out gost\<DEFAULT_DOMAIN>\certkey-rsa.pfx -inkey
<KEY> -in <CERTIFICATE>
```

При наличии CA сертификата или цепочки в формате *.pem, необходимо создать pfx-контейнер `roots-rsa.pfx` и разместить в директории:

```
~\MyOffice_PGS_XXXX.XX\certificates\gost\<DEFAULT_DOMAIN>
```

Пример команды для создания pfx-контейнера с помощью утилиты OpenSSL:

```
openssl pkcs12 -export -out gost\<DEFAULT_DOMAIN>\roots-rsa.pfx -in <CERTIFICATE> -nokeys
```

Дополнительно к созданным pfx-контейнерам, необходимо получить от провайдера готовый pfx-контейнер с ГОСТ сертификатом и ключом сервера `certkey-gost.pfx` (или с корневым сертификатом `roots-gost.pfx`). Полученные контейнеры необходимо разместить в директории `~\MyOffice_PGS_XXXX.XX\certificates\gost\<DEFAULT_DOMAIN>`.

При использовании сертификатов старше 15 месяцев в системе с сертификацией ГОСТ возникают неполадки в работе сервиса Nginx.
Для устранения неполадок необходимо выполнить операции, описанные в Приложение А.

2.4.5 Создание самоподписанного сертификата PGS

Для создания самоподписанного сертификата в среде установки PGS необходимо запустить исполняемый файл `gen_self_signed_cert.sh` из каталога установки. При запуске файла указывается домен, привязанный к создаваемому сертификату. Пример запуска:

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

После создания файл сертификата будет автоматически размещен в необходимом каталоге (см. раздел «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 находятся в папке с дистрибутивом по следующим адресам:

– для конфигурации без отказоустойчивости:

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

– для кластерной установки:

```
~/install_MyOffice_PGS/inventory/hosts-hl.yaml
```

– для кластерной установки с ArangoDB на одном сервере:

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

Файл inventory использует формат .yaml, синтаксис которого описан в документации Ansible. Операция копирования выполняется следующей командой:

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

Сконфигурированный файл рекомендуется сохранить отдельно на внешнем ресурсе для дальнейшего использования при восстановлении и/или переустановке системы.

2.5.1 Конфигурирование файла inventory: hosts

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 роли `pythagoras` серверу с доменным именем `host.example.com` необходимо указать следующие значения:

```
pythagoras:
 hosts:
  host.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 устанавливаются 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 установки в файле inventory указывается несколько адресов серверов в соответствующей группе.

Текущей версией ПО поддерживается кластеризация для сервисов, перечисленных в таблице 8. В таблице указано минимально необходимое количество серверов для работы кластера. В зависимости от инфраструктуры и типа установки количество серверов может быть изменено.

Таблица 8 — Поддержка кластеризации

Наименование сервиса	Группа	Количество серверов
Pythagoras	Pythagoras	2
Keycloak	Keycloak	2
ArangoDB*	ArangoDB	2(1*)
	Arangodb_agent	3(1*)
Elasticsearch	Search	3
Redis	Redis	2
RabbitMQ	RabbitMQ	3
Etcd	Etcd	3
Nginx	Nginx	2

Наименование сервиса	Группа	Количество серверов
Postgres	Postgres	2
Docker Registry	Infrastructure	1
Syslog-ng		
Monitoring		
Storage	Storage	3

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

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

Одновременно работающие пользователи — единовременное выполнение операций по редактированию документов несколькими тысячами пользователей. Общее количество суммируется из соотношения один пользователь — одна сессия редактирования или совместного редактирования одного документа.

Пример такой конфигурации находится в файле: `hosts-hl-sa.yaml`. Для включения односерверной установки ArangoDB необходимо задать следующие значения переменным:

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

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.

Пример конфигурации для кластерной установки находится в шаблоне `hosts-hl.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 при использовании PGS 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 должен быть отформатирован в файловую систему XFS и не должен быть смонтирован на момент развертывания (кроме ситуации повторного запуска).

В режиме `volume_device_<role>: "False"` никаких 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"`.

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

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 файла inventory: переменные»;

– `<service_name>` – имя сервиса;

– `<element>` – название файла лога.

В случае кластерной установки модуля CO требуется настройка балансировщика нагрузки между PGS и его auth-нодами. Для этого в inventory 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.

Дальнейшая настройка inventory файла представлена в разделе «Конфигурирование файла inventory: переменные».

Дополнительная информация по интеграции с СО описана в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Руководство по настройке».

2.5.2 Конфигурирование файла inventory: переменные

Процесс настройки переменных файла inventory состоит в заполнении секции `vars`. Доступные значения и способы заполнения секции указаны в таблице 9.

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 PGS 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 9 — 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.yaml по умолчанию False, в шаблоне hosts-hl.yaml по умолчанию True
arango_cluster	Включение и отключение кластерного режима установки сервиса Arango. Принимает значения True и False. В шаблоне hosts-sa.yaml и hosts-hl-sa.yaml по умолчанию False, в шаблоне hosts-hl.yaml по умолчанию True
default_domain	Зарегистрированный домен установки PGS. Для корректной работы необходим установленный актуальный SSL-сертификат

Переменная	Значение и способ заполнения
env	Элемент доменного имени установки и предназначен для разграничения доступа к сервисам PGS
swarm_network_encryption	Включает шифрование внутренней оверлейной сети Docker swarm, значение по умолчанию False. Влияет на производительность системы
nginx_gost_enabled	Включение или отключение установки системы с поддержкой ГОСТ шифрования. Принимает значения True и False. По умолчанию False.
admin_interface_ext_port	Порт Nginx для доступа к интерфейсу администратора, значение по умолчанию — 443. При изменении значения по умолчанию для порта в PGS необходимо учесть новое значение в компоненте CO (Подробнее см. в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Система редактирования и совместной работы (CO). Руководство по установке»). При включении интеграции с почтовой системой PSN следует изменить порт для доступа к интерфейсу администратора PGS в компоненте PSN (Подробнее см. в документе «"МойОфис Почта 2". Руководство по установке»)
api_interface_ext_port	Порт Nginx для доступа к API интерфейсу, значение по умолчанию — 443. При изменении значения по умолчанию для порта в PGS необходимо учесть новое значение в компоненте CO (Подробнее см. в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ. Система редактирования и совместной работы (CO). Руководство по установке»). При включении интеграции с почтовой системой PSN следует изменить порт для доступа к `pgs_api` в параметрах компонента PSN (Подробнее см. в документе «"МойОфис Почта 2". Руководство по установке»)
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	Задает максимально возможное число тенантов в текущей установке (максимально допустимое значение 100)
keycloak_password	Пароль для пользователя PGS в Keycloak (он же Администратор Master Realm)
keycloak_realm_password	Внутренний пароль для администраторов тенантов Keycloak (используется только для сервисного обслуживания системы)
keycloak_postgres_password	Пароль БД PostgreSQL (используется как хранилище для Keycloak)
arangodb_password	Пароль пользователя PGS в ArangoDB
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`
elasticsearch_heap_size	Выделение памяти для сервиса 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
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)
heraclitus_cron	Задает время запуска сервиса Heraclitus. Для определения времени запуска используется формат, аналогичный формату Cron. Значение по умолчанию "0 2 * * *".
Блок default_tenant	
Блок default_tenant	Предназначен для создания тенанта по умолчанию, необходимого для дальнейшей работы с пользователями в веб-интерфейсе PGS
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 «/»
retention_file_time	Время хранения файлов после удаления из корзины. Значение в днях, по умолчанию 30

Переменная	Значение и способ заполнения
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. False — если используется стороннее s3-хранилище
use_old_minio	Принимает значения: true/false При значении False из дистрибутива PGS будет установлен MinIO версии RELEASE.2023-12-13T23-28-55Z При значении True будет установлен MinIO максимально совместимой версии RELEASE.2022-06-25T15-50-16Z Переменная со значением false предназначена: 1. Для первичной установки Частного Облака. 2. Если в инфраструктуре не используется собственное s3-хранилище. 3. Если в инфраструктуре не предустановлен MinIO ранних версий датой выпуска до 2022-06-26. Переменная со значением true предназначена: 1. Для последующей установки Частного Облака (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 Частного Облака, где в качестве storage type использовалось значение s3. 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
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. В случае использования MinIO, выглядит следующим образом: `http://pgs-<ENV>.<DEFAULT_DOMAIN>:9000`.

Переменная	Значение и способ заполнения
	Значения `<env>` и `<default_domain>` соответствуют указанным в начале данной таблицы
secret_key	Параметр, соответствующий настройкам хранилища s3. При использовании сервиса MinIO совпадает со значением переменной `minio_secret_key`
access_key	Параметр, соответствующий настройкам хранилища s3. При использовании сервиса MinIO совпадает со значением переменной `minio_access_key`
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 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
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 co	
Блок co	Переменные, которые необходимо заполнить для интеграции с компонентом CO. Более подробно о заполнении блока представлено в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ». Система редактирования и совместной работы (CO). Руководство по установке».
coapiurl	Путь доступа к API компонента CO. Данная переменная представляет собой URL-адрес и порт, указывающие на целевой сервер с ролью `auth` компонента CO. Пример: coapiurl: "https://co-api-url.ru:8443"
co_lb	Включает и выключает настройку балансировки с помощью сервиса Keepalived. 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_keepalived_pass	Пароль для сервиса keepalived (только для кластерной установки)
Блок installation_commons	
Блок installation_commons	Значения переменных данного блока должны соответствовать аналогичным в компоненте CO, за исключением `app_admin_password`. Значение этой переменной генерируется администратором при установке компонента PGS.

Переменная	Значение и способ заполнения
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	Более подробно о заполнении блока представлено в документе «"МойОфис Частное Облако 2" в варианте исполнения ГОСТ». Система редактирования и совместной работы (СО). Руководство по установке».
co_manage_api_username	Имя пользователя для API-авторизации компонента СО. Должно совпадать со значением переменной `co_manage_api_username` в конфигурации СО
co_manage_api_password	Пароль для API-авторизации компонента СО. Должен совпадать со значением переменной `co_manage_api_password` в конфигурации СО
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 СО. Значение зависит от наличия сервиса в СО. Доступные значения: True и False, по умолчанию False
poseidon_integration	Включение и выключение интеграции с «МойОфис Почта», доступные значения: True и False
Блок poseidon	
Блок poseidon	Параметры подключения к «МойОфис Почта», если включена интеграция. Подробные сведения об установке и настройке PSN см. документ «МойОфис Почта»
pbm_url	Ссылка для 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` при установке PSN
ssl_verify	Параметры шифрования для почты. Принимает значения True и False, False — 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. Точки монтирования для роли `storage` в разных режимах указаны в таблице 10.

Таблица 10 — 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

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

4.1 Для хранилища MinIO требования представлены в таблице 11.Таблица 11 — Конфигурация отказоустойчивости для хранилища S3 MinIO

Конфигурация отказоустойчивости	Количество нод/серверов	Количество независимых дисков
минимальная	3	2
рекомендуемая	4	4

4.2 Хранилище GlusterFS устанавливается в режиме `replicated`, в котором количество нод/серверов в роли `STORAGE` не влияет на потенциальное доступное место для PGS. 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.

2.5.3.1 Настройка межсетевого экранирования

Для обеспечения стабильной работы PGS не рекомендуется использовать сетевое экранирование между серверами. Необходимые для работы ПО сетевые порты приведены в таблице 12.

Таблица 12 — Сетевые порты, используемые подсистемой PGS

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

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

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 СО сервера, 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.

2.5.4 Настройка дополнительных параметров установки

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

3 УСТАНОВКА

3.1 Порядок запуска установки

Для запуска установки PGS 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 13);

При успешном выполнении команды сервисы PGS будут запущены автоматически.

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

Таблица 13 — Дополнительные ключи установки

Значение ключа	Описание
-e monitoring_enable=<value>	Устанавливает True или не устанавливает False сервисы мониторинга Prometheus и Grafana. По умолчанию true
-e content_search_enable=<value>	Устанавливает True или не устанавливает False сервисы для поиска по содержимому документов в облачных редакторах СО. По умолчанию – true
-e kernel_ml_enable=<value>	Включает True или отключает False обновление ядра ОС (релизы ветки mainline). По умолчанию – true
-e kernel_ml_deb_enable=<value>	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 файла inventory: переменные».

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 PGS 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 1/1A
pgs-keycloak_keycloak 1/1
pgs-monitoring_cadvisor 1/1
pgs-monitoring_dockerd-exporter 1/1
pgs-monitoring_grafana 1/1
pgs-monitoring_nod-exporter 1/1
pgs-monitoring_prometheus 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
```

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

3.3 Обновление

При обновлении PGS 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 PGS

4.1 Карта портов для внутренних соединений

Карта портов для внутренних соединений представлена в таблице 14.

Таблица 14 — 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
			5672/tcp	rabbitmq
	heraclitus		2379/tcp	etcd
			6379/tcp	redis
			8529/tcp	arangodb
			8852/tcp	euclid
			5672/tcp	rabbitmq
			8080/tcp	keycloak
	epicure		8529/tcp	arangodb
			6379/tcp	redis
	flower	5555/tcp	8529/tcp	arangodb
			6379/tcp	redis
	dionis		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

Группа Ansible	Сервис	Прослушиваемый порт	Порт подключения	Куда обращается(имя swarm service)
				кластера)
			2379/tcp	etcd
			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	postgress	5432/tcp 8008/tcp 5000/tcp 5001/tcp	2379/tcp	etcd
			5432/tcp 8008/tcp 5000/tcp 5001/tcp	postgress
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 15.

Таблица 15 — Карта внешних портов

Группа Ansible	Сервис	Прослуши-ваемый 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
				PSN (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
				PSN (если нужна интеграция)
			514/udp	syslog локально на IP 172.17.0.1
	heraclitus	-	9000/tcp	Серверы с ролью Storage для подключения к S3

Группа Ansible	Сервис	Прослуши-ваемый порт	Порт подключения	Куда обращается (имя swarm service)
				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
	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	postgress	-	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

Группа Ansible	Сервис	Прослуши-ваемый порт	Порт подключения	Куда обращается (имя swarm service)
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 (первый сервер с ролью infrastructure)
	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 docker_gwbridge_ip)
			23529/tcp*	haproxy (обращение идет через docker_gwbridge_ip)
			30692/tcp*	haproxy (обращение идет через docker_gwbridge_ip)
			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 docker_gwbridge_ip)
	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 15):

– для установки 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 PSN исходящие подключения к серверу PSN.

5 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.

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 PGS.

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 `keycloack` 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.r7xptti1p7an@    | etcd
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@    | 2379
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@    | 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.r7xptti1p7an@    | panic: Can't create rabbit
wrapper
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@    |
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@    | goroutine 1 [running]:
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@    | main.main()
pgs-sisyphus_sisyphusworker.1.r7xptti1p7an@
|     /go/src/cmd/worker/main.go:29 +0x80a
pgs-sisyphus_sisyphusworker.1.kry1r9x8vcdg@    | etcd
pgs-sisyphus_sisyphusworker.1.kry1r9x8vcdg@    | 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}}\
t{{.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 Использование сертификатов старше 15 месяцев

Описание проблемы:

На рабочих системах с сертификацией ГОСТ при использовании сертификатов старше 15 месяцев некорректно функционирует сервис Nginx.

Решение:

Обход данного ограничения подразумевает нарушение формуляра CSP и выполняется под собственную ответственность заказчика:

1. Для получения идентификатора контейнера Nginx `<container-id>` необходимо выполнить команду:

```
docker ps | grep pgs-nginx_nginx | awk -F' ' '{print $1}'
```

Пример идентификатора на выходе: `9c9f9aa55280`

2. С полученным идентификатором зайти в контейнер nginx и исполнить необходимую настройку конфигурации при помощи утилиты cpconfig:

```
docker exec <container-id> /bin/bash -c\
 "/opt/cprocsp/sbin/amd64/cpconfig -ini '\config\parameters'\
 -add long ControlKeyTimeValidity 0"
```

3. Для использования новой конфигурации следует перезагрузить сервис Nginx с помощью команды:

```
docker exec <container-id> /bin/bash -c "/opt/nginx/sbin/nginx -s reload"
```

4. При кластерной установке системы необходимо создать образ изменений и внести изменения в каждый контейнер Nginx с помощью команды:

```
docker commit <container-id>\
 pgs-private-registry:5001/pythagoras/pgs-nginx:1.18.0-gost
```