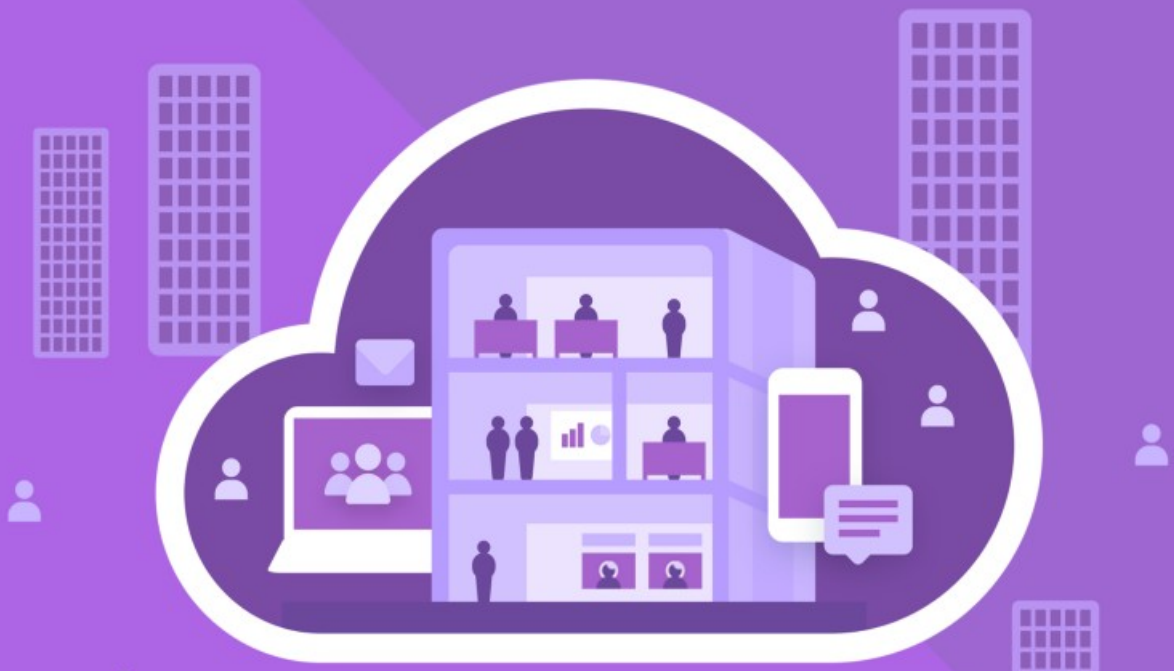

МойОфис
Частное Облако 2

Руководство по настройке

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ «МОЙОФИС ЧАСТНОЕ ОБЛАКО 2»

РУКОВОДСТВО ПО НАСТРОЙКЕ

2.8

На 51 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

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ, ТЕРМИНОВ И ОПРЕДЕЛЕНИЙ

В настоящем документе используются 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 программного обеспечения
API	Application Programming Interface, интерфейс программирования приложений
CDN	Content Delivery Network, сервис обеспечивающий кастомизацию
CO	CloudOffice, Облачный Офис, общее название продукта (группы редакторов)
Docker	ПО для автоматизации развертывания и управления приложениями в средах с поддержкой контейнеризации
Docker Registry	Масштабируемое серверное приложение для хранения и распространения контейнеров Docker
DNS	Domain Name System, система доменных 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»
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, позволяющий производить удаленное управление
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
Бандл	Группа объектов для кастомизации сервиса, представленных в виде упакованного файла
БД	База данных
Вендор (vendor)	Поставщик брендированного продукта
ESIA	Единая система идентификации и аутентификации
Кластер (cluster)	Объединенная группа серверов
Метабандл	Группа обьектов для кастомизации сервисов, представленных в виде упакованного файла
Оверкоммит (overcommit)	Опция гипервизора по избыточной аллокации памяти для виртуальных машин
ОС	Операционная система
Тенант	Логический объект, включающий в себя совокупность вычислительных ресурсов, пользователей и репозиторий

1 НАЗНАЧЕНИЕ

«МойОфис Частное Облако 2» – комплекс безопасных веб-сервисов и приложений для организации хранения, доступа и работы с файлами и документами внутри компании.

В состав продукта входят:

- Система хранения данных для безопасного хранения корпоративных файлов и обеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей;
- Система редактирования и совместной работы для индивидуального и совместного редактирования текстовых и табличных документов, а также просмотра и демонстрации презентаций;
- 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 на мобильных 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 операционными системами Android, iOS и iPadOS.

Текущий документ описывает настройки «МойОфис Частное Облако 2» после установки.

Конфигурация системы осуществляется с помощью сервисов:

– etcd-браузер для CO;

– etcdctl для PGS.

Адрес etcd-браузера зависит от типа установки и указывается в процессе развертывания системы.

Если описание настройки включает в себя изменение inventory файла, конфигурация должна быть выполнена перед установкой системы.

После внесения изменений может потребоваться перезапуск контейнеров изменяемого сервиса (например: Euclid). Для обеспечения бесперебойной работы сервисов для пользователей рекомендуется проводить изменения в период минимальной нагрузки на систему.

2 УПРАВЛЕНИЕ ТЕНАНТАМИ

В «МойОфис Частное Облако 2» работа с объектами реализована в тенантах. Тенанты между собой полностью изолированы. Управление настройками конкретного тенанта осуществляется администратором тенанта в веб-приложении «Администрирование» (подробнее см. в документе «МойОфис Частное Облако 2». Руководство по администрированию»).

Получение настроек тенанта на стороне компонента CO проверяется с помощью etcd (CO) по адресу `tenants/<id тенанта>`, для тенанта с доменом установки значение указано в параметре `tenants/default`.

2.1 Создание тенанта

Для создания тенанта по умолчанию во время установки системы необходимо заполнить значениями блок переменных файла inventory `default_tenant` (подробнее см. в документе ««МойОфис Частное облако 2». Система хранения данных (PGS). Руководство по установке»).

Для создания тенанта по умолчанию после установки или создания дополнительных тенантов необходимо воспользоваться REST API сервиса Euclid.

Примеры shell-команд:

1. Аутентификация и получение токена авторизации для пользователя PGS:

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

2. Создание тенанта:

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

В приведенных примерах используются переменные, описанные в таблице 2.

Таблица 2 — Переменные для создания тенанта

Наименование переменной	Описание	Примечание
<token>	Токен авторизации	-
<default_domain>	Домен установки PGS	Переменная PGS*
<domain>	Домен, соответствующий создаваемому тенанту	При создании дополнительного тенанта (не по умолчанию) должен отличаться от значения переменной <default_domain>
<name>	Имя создаваемого тенанта	По умолчанию имеет значение default
<admin password>	Пароль администратора веб-интерфейса	-
<recovery email>	Адрес электронной почты для восстановления пароля администратора	-
<default_domain>	Домен установки PGS	Переменная PGS*
<env>	Элемент доменного имени установки	Переменная PGS*
<Nginx_https_ext_port>	Порт Nginx для доступа к сервисам	Переменная PGS*
<keycloak_password>	Пароль для пользователя PGS в Keycloak	Переменная PGS*

* — переменные, заполненные в соответствии с документом «МойОфис Частное облако 2». Система хранения данных (PGS). Руководство по установке».

Администрирование данного тенанта выполняется с помощью веб-интерфейса, по умолчанию доступного по адресу:

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

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

2.2 Изменение количества тенантов

Настройка позволяет ограничить количество тенантов. Значение изменяется с помощью переменной, указанной в таблице 3.

Таблица 3 — Переменная для изменения количества тенатов

Наименование сервиса	Наименование переменной	Тип переменной	Значение
Euclid (PGS)	/pgs/euclid/max_tenants	integer	от 1 до 100 (100 максимально доступное значение, установлено по умолчанию)

2.3 Настройка логина со своим тенантом

По умолчанию пользователь с доменом @test.demo.example.com может авторизоваться по адресу: https://authdemo.example.com/auth.

Для настройки авторизации пользователя с доменом @test.demo.example.com только через https://auth-test.demo.example.com необходимо выполнить следующие действия:

1. Преобразовать сертификат (цепочка сертификатов, с сохранением последовательности передачи в сервисе Nginx) в строку путем замены переносов строк на символы \n с помощью команды:

```
sed -i -z 's/\n/\\n/g' cert.pem
```

2. Зашифровать ключ (в PEM формате, без изменений, многострочный) с помощью команды:

```
openssl enc -aes-256-cbc -K $FS_APP_ENCRYPTION_KEY -iv\
$FS_APP_ENCRYPTION_IV -in key.pem | xxd -ps -c 4096
```

3. Разместить ключ и сертификат в PGS с помощью Euclid API:

```
export token=$(curl -fs -XPOST\
 https://pgsdemo.example.com/adminapi/auth\
 -d 'username=pgs' -d 'password=...' | jq-r .token)\
curl -XPUT https://pgs-demo.example.com/adminapi/smtp_conf/srv --data\
-raw '{"cert":"...","key":"..."}' -H "Authorization: $token" -H\
"Content-Type: application/json"
```

4. Проверить настройку уведомлений и связи между PGS и CO с помощью интеграционных тестов (подробнее см. раздел «Установка» документа «МойОфис Частное Облако 2» «Система редактирования и совместной работы МойОфис (CO)». Руководство по установке»). В случае неправильной настройки уведомлений или связи необходимо выполнить перезагрузку тенанта с помощью команды:

```
curl -XPOST https://coapidemo.example.com:8443/api/manage/config/\
tenants/pgs19825/reload --usercouser:...
```


3 ДОПОЛНИТЕЛЬНЫЕ НАСТРОЙКИ ФАЙЛОВЫХ ОПЕРАЦИЙ

3.1 Срок хранения удаленных файлов

После удаления пользователем файлов или папок из своей корзины удаленные объекты заданное время хранятся в системе. Функция предназначена для случаев необходимости восстановления удаленных объектов. Срок хранения таких удаленных объектов может быть настроен.

Установка времени выполняется с помощью переменной, указанной в таблице 4.

Таблица 4 — Изменение времени хранения удаленных файлов

Наименование сервиса	Наименование переменной	Тип переменной	Единицы измерения	Значение по умолчанию
etcd (PGS)	/pgs/fs/ remove_threshold	integer	секунда	2592000000

3.2 Настройки функции загрузки файлов

3.2.1 Настройка максимального размера фрагмента загружаемого файла

Для настройки максимального размера загружаемого фрагмента файла необходимо изменить значение переменной, указанной в таблице 5.

Рекомендуется не изменять данный параметр.

Таблица 5 — Максимальный размер фрагмента загружаемого файла

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Диапазон значений
etcd (CO)	config/wfe/ max.upload.chunk.size	integer	байт	52428800 (значение по умолчанию)

3.2.2 Настройка максимального размера загружаемого файла

По умолчанию в системе установлено ограничение на допустимый размер загружаемого пользователем файла – 5 Гбайт.

Для изменения ограничения необходимо установить новое значение переменной, указанной в таблице 6.

Таблица 6 — Максимальный размер загружаемого файла

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Диапазон значений
etcd (CO)	config/wfe/ max.upload.file.size	integer	байт	52428800 (5 Гбайт) (значение по умолчанию)

3.2.3 Настройка автоматической конвертации документов внешнего формата при загрузке

В «МойОфис Частное облако 2» реализована функция автоматической конвертации документов внешнего формата при загрузке их в систему. После установки CO функция будет включена по умолчанию в режим `ask` (отображение диалогового окна с запросом действия).

При конвертации документов во внутренний формат возможно изменение структуры и форматирования документа внутреннего формата.

После загрузки документа с конвертацией в «МойОфис Частное облако 2» небходимо убедиться, что в документ не внесено существенных изменений, мешающих дальнейшей работе. Удаление исходного файла внешнего формата рекомендуется выполнять после проверки.

Поддерживаемые форматы документов для конвертации, типы внутреннего формата документов и шаблонов представлены в таблице 7.

Таблица 7 — Формат документов и шаблонов после конвертации

Формат документа до конвертации	Формат документа после конвертации
*.docx, *.doc, *.odt, *.txt, *.rtf, *.docm	*.xodt
*.dotx, *.ott, *.dot	*.xott
*.xlt, *.ots, *.xltx	*.xots
*.xlsx, *.xls, *.ods, *.xlsm	*.xods
*.odp, *.pps, *.pptx, *.ppt, *.pptm, *.ppsx	*.xodp
*.potx, *.otp, *.pot	*.xotp

В дальнейшем Пользователь может самостоятельно переопределить параметры загрузки файлов с автоматической конвертацией с помощью настроек профиля (подробнее см. в документе «"МойОфис Документы". Веб-приложение. Руководство пользователя»).

С помощью ETCD администратор может изменить настройку функции. Управление распространяется на:

– новых пользователей;

– пользователей, не изменивших значение по умолчанию в профиле.

Для пользователей, сменивших в профиле значение по умолчанию, режим автоматической конвертации не изменяется.

Для управления функцией необходимо использовать переменные, указанные в таблице 8.

Таблица 8 — Управление загрузкой файлов с конвертацией

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	config/wfe/upload.conversion.enabled	boolean	true (по умолчанию) / false	Включение /отключение конвертации
	config/wfe/upload.conversion.option	string	always	Всегда конвертировать
			never	Никогда не конвертировать
			ask (по умолчанию)	Диалоговое окно с запросом действия

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Для работы с `ansible-playbook` переменные принимают следующий вид:

```
openresty_upload_conversion_enabled
openresty_upload_conversion_option
```

Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml]\
 -e openresty_upload_conversion_option=always
```

3.3 Отключение возможности скачивания документов

В «МойОфис Частное облако 2» предусмотрена возможность отключения скачивания документов с помощью пользовательского интерфейса.

Для управления функцией необходимо изменить значение переменной, указанной в таблице 9.

Таблица 9 — Отключение возможности скачивания

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	config/wfe/download.disabled	boolean	true / false (по умолчанию)

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml] -e DOWNLOAD_DISABLED=true
```

3.4 Управление запросом уведомлений об изменениях

В «МойОфис Частное облако 2» реализована функция уведомления пользователей об изменениях в файлах.

Для включения уведомлений необходимо использовать административную панель (см. в документе «"МойОфис Частное облако 2". Руководство по администрированию»).

Запросы отправляются на сервер автоматически с заданным интервалом. Увеличение значения интервала между запросами может снизить нагрузку на сервер.

Для изменения значения необходимо использовать переменную, указанную в таблице 10.

Таблица 10 — Установка интервала уведомления по изменениям

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	config/wfe/ check.notice.interval.sec	integer	секунда	180 (по умолчанию)

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Для работы с `ansible-playbook` переменная принимает следующий вид:

```
openresty_check_notice_interval_sec
```

Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml]\
 -e openresty_check_notice_interval_sec=120
```

3.5 Отключение возможности копирования контента документов

В «МойОфис Частное Облако 2» предусмотрена возможность отключения копирования во внешний буфер обмена (clipboard) содержимого документов (как в режиме просмотра, так и в режиме редактирования). При этом копирование/вставка внутри редактора документов продолжит работать.

Для управления настройкой необходимо изменить значение переменной, указанной в таблице 11.

Таблица 11 — Отключение возможности копирования

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	config/wfe/ external.clipboard.disabled	boolean	true / false (по умолчанию)

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml] -e EXTERNAL_CLIPBOARD_DISABLED=true
```

3.6 Настройка режима открытия документа в редакторе

Настройка служит для выбора режима открытия документа внутреннего формата в редакторе. При включении настройки документы всегда открываются в редакторе в режиме просмотра. При отключении настройки документы открываются в редакторе в соответствии с правами доступа пользователя.

Настройка будет применяться при следующих способах открытия документа в системе:

– при нажатии на документ внутреннего формата в файловом менеджере;

– при переходе по внутренней ссылке к документу внутреннего формата.

После установки CO настройка будет включена по умолчанию, что позволит системе снизить нагрузку на серверы.

Пользователь может самостоятельно изменить режим открытия документа с помощью настроек профиля (подробнее см. в документе «МойОфис Документы». Веб-приложение. Руководство пользователя).

Управление режимом выполняется с помощью переменной, указанной в таблице 12.

Таблица 12 — Переменная для настройки режима открытия документа

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	config/wfe/ preview.internal.first.enabled	boolean	true (по умолчанию)/ false

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Для работы с `ansible-playbook` переменная принимает следующий вид:

```
openresty_preview_internal_first_enabled
```


Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml]\
 -e openresty_preview_internal_first_enabled=false
```

3.7 Отключение корпоративной адресной книги

В «МойОфис Частное Облако 2» настройка позволяет скрыть перечень корпоративных контактов в следующих случаях:

– при поиске адресатов для предоставления общего доступа к объекту;

– при поиске адресатов для отправки писем.

Управление настройкой выполняется с помощью переменной, указанной в таблице 13.

Таблица 13 — Переменная для настройки отображения адресной книги

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	config/wfe/ corporate.contacts.enabled	boolean	true (по умолчанию) / false

3.8 Настройка автоматического отключения неактивного пользователя

В «МойОфис Частное Облако 2» предусмотрено автоматическое отключение пользователей от редактируемого документа, в случае их бездействия.

Изменение времени задается с помощью переменной, указанной в таблице 14.

Таблица 14 — Переменная для настройки прерывания сессии

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	config/wfe/du_max_time_for_ inactive_collaborator_mins	integer	минута	180 (значение по умолчанию)

3.9 Ограничение количества пользователей при совместном редактировании

В «МойОфис Частное Облако 2» предусмотрено ограничение на количество пользователей, одновременно редактирующих один документ. По умолчанию 15 пользователей может одновременно редактировать один документ (находиться в одной сессии редактирования), остальные могут открыть документ только для просмотра.

Увеличение общего количества пользователей в данной функции может приводить к затруднениям в работе с документом: увеличении времени открытия документа и ошибкам

при загрузке. Для сохранения стабильной работы системы рекомендуется использовать значение по умолчанию.

Для изменения ограничения необходимо установить новое значение переменной, указанной в таблице 15.

Таблица 15 — Управление количеством пользователей при совместном редактировании

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	config/nps-du/ Du.Env.MaxCollaboratorsSlots	integer	15

Управление функцией поддерживается на этапе развертывания CO. Изменение значения переменной выполняется при запуске скрипта установки.

Для работы с `ansible-playbook` переменная принимает следующий вид:

```
du_max_collaborators
```

Пример команды настройки функции:

```
[ansible-playbook playbooks/main.yml] -e du_max_collaborators=20
```

4 НАСТРОЙКА ИНТЕРФЕЙСНЫХ СИСТЕМНЫХ УВЕДОМЛЕНИЙ

4.1 Баннер «О планируемых работах на сервере»

Настройка баннера «О планируемых работах на сервере» выполняется внесением изменений в конфигурационный файл, указанный в таблице 16.

Таблица 16 — Переменная для настройки баннера

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	config/wfe/banner.notification.json	строка в формате JSON	отсутствует

Пример настройки:

```
{"id":31219,"start":1575331200000,"stop":1575504000000,"close":true,\
"content":{"ru-RU":"<div class='mo-banner__content-inner \
mo-banner__contentinner_warning'><h3 class='mo-banner__title'>\
Внимание</h3><div>4 декабря с 09:00 до 11:00 по московскому \
времени будет обновление сервера редактирования до последней \
версии приложения.</div></div>","en-US":"<div \
class='mo-banner__content-innermo-banner__content-inner_warning'>\
<h3 class='mobanner__title'>Warning</h3><div>On December 4th \
from 09:00 am untill1:00 am (GMT+3) stand will be updated with latest \
application version.Stand could be unreachable.</div></div>"}}
```

При обновлении баннера необходимо изменить `id` на число вида `'1ddmmyy'`. Пример записи: для 05.12.23 - `1051223`

4.2 Баннер «Об истечении срока действия пароля пользователя»

Переменная в таблице 17 регулирует период уведомления пользователя об истечении срока действия пароля (не работает при включенной интеграции с Microsoft Active Directory).

Таблица 17 — Настройка уведомления о сроке действия пароля

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	config/wfe/password.expiry.notice.days.int	integer	5

4.3 Уведомление пользователя о приближении окончания его квоты

Функция предназначена для уведомления пользователя о приближении к ограничению выделенного ему размера хранения личных файлов (квоте).

Если текущий остаток личной квоты пользователя меньше или равен установленному значению, то пользователь получает предупреждение о приближении окончания квоты.

Настройка остатка квоты изменяется с помощью переменной, указанной в таблице 18.

Таблица 18 — Настройка остатка квоты для уведомления

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	config/wfe /low.space.threshold	integer	проценты	1-100 (10 по умолчанию)

5 КАСТОМИЗАЦИЯ

5.1 Настройка главной страницы и меню быстрого запуска

Настройка доступных для запуска значков приложений (appswitcher) на целевой странице Auth/SSO и в меню быстрого запуска (quicklaunch) выполняется с помощью изменения параметров `config/wfe/appswitcher.landing.json` и `config/wfe/appswitcher.quicklaunch.json` в etcd.

Это список всех доступных по умолчанию приложений в установке.

Массив `order` управляет порядком отображения значка приложения в списке. Ключ `main` указывает на главный значок на целевой странице.

Пример: appswitcher.landing.json

```
{
"order":[
"wfm",
"mail",
"contacts",
"calendar",
"profile",
"admin"
],
"main":"wfm"
}
```

Пример: appswitcher.quicklaunch.json

```
{
"order":[
"landing",
"wfm",
"mail",
"contacts",
"calendar"
]
}
```

5.2 Настройка доступных языков

Настройка доступных языков (локализаций) веб-приложений (language switcher) выполняется с помощью параметра `config/wfe/branding/excluded.locales.json` в etcd.

Часть языков, находящихся в дистрибутиве локализации, пользователю не доступны. По умолчанию возможность выбора в UI локализации `["hi-IN"]` не предусмотрена.

Список всех локализаций, включенных в дистрибутив, перечислен в параметре `config/wfe/branding/available.languages.json` в etcd.

5.3 Персонализация с помощью cdn_bundle

Пакеты CDN предоставляют возможность замены или актуализации брендинга устанавливаемого продукта, а также добавления перечисленных ниже функций без остановки работы сервиса:

– добавление или изменение справочного веб-контента;

– добавление поддерживаемых языков;

– добавление локализации или других ресурсов, используемых подсистемой СО.

Каждый пакет содержит документ, который описывает содержимое и версию пакета, а также содержит информацию о совместимости с версиями СО. Во время развертывания подсистемы СО в CDN устанавливаются минимально необходимые пакеты ресурсов для работы данной конфигурации.

Каждый пакет выполняет одну из двух функций:

– добавляет новые ресурсы;

– обновляет своим содержимым существующие CDN ресурсы.

Загрузка нового пакета не ограничивает доступ по прямым ссылкам к предыдущим ревизиям ресурсов (например, ссылки на изображения в отправленных письмах-уведомлениях).

Несколько бандлов могут быть объединены в общий архив, метабандл, устанавливаемый как единое целое.

5.3.1 Описание состава бандла

`Cdn_bundle` представляет из себя директорию с файлами, которые будут добавлены на CDN.

Файл `cdn_bundle.json` — манифест в формате JSON, описывающий структуру бандла и перечень параметров для настройки.

5.3.2 Структура cdn_bundle.json

Файл `cdn_bundle.json` состоит из следующих переменных:

- `bundleVersion` — версия бандла;
- `formatVersion` — версия формата описания бандла (на данный момент есть только версия «1»);
- `description` — произвольная строка с описанием;
- `merge` — объединять или заменять структуры данных с одинаковыми именами в etcd (по умолчанию false);
- `properties` — массив полей etcd, которые необходимо переопределить.

5.3.3 Ключи cdn_bundle.json

За образец принимается файл `cdn_bundle.json`. При работе с файлом допускается внесение изменений только для значений (узлы value). Состав ключей указан в таблице 19.

Таблица 19 — Перечень ключей cdn_bundle.json

Наименование ключа	Описание
wfe/appswitcher.quicklaunch.json	Определяет состав и последовательность приложений в выпадающем меню
wfe/appswitcher.landing.json	Определяет состав и последовательность приложений на странице приложений
wfe/appswitcher.apps.json	Содержит ссылки на приложения
appswitcher.quicklaunch.actions.json	Определяет состав быстрых действий

5.3.4 Описание полей в ключе wfe/appswitcher.apps.json

Параметры в таблице 20 соответствуют ключам в `"wfe/appswitcher.quicklaunch.json"` и `"wfe/appswitcher.landing.json"`.

Таблица 20 — Параметры ключа wfe/appswitcher.apps.json

Поле	Требования	Описание
url	Обязательное поле	Адрес приложения
title	Обязательное поле	Название приложения
iconUrl	Обязательное поле	Путь к иконке приложения внутри бандла, например: "% cdn_base_url%/apps/some.svg"
style	Необязательное поле	Произвольные стили в формате jss

Поле	Требования	Описание
isQuick	Необязательное поле	Флаг, отвечающий за то, чтобы приложение попало в «быстрые действия» (quick actions). Для включения функции необходимо задать значение `true`

Все ключи и значения (кроме key и value) должны быть в двойных кавычках `""`, которые экранированы обратным слэшем `"\"`, например:

```
\"wfm\":{\"url\":\"//files-domain3.domain2.domain1\"}
```

В поле value определены ссылки на приложения, предусмотрен функционал установки значков приложений.

5.3.5 Последовательность создания бандла

1. Создать директорию с произвольным названием, которая будет содержать манифест (`cdn_bundle.json`) и директорию с ресурсами.

2. Создать `cdn_bundle.json`. Пример файла `cdn_bundle.json` с кастомным приложением «1С»:

```
      {
      "bundleVersion": "custom-12.0.5.5",
      "formatVersion": 1,
      "description": "Customizations description","merge": false,"properties": [
      {
      "key": "wfe/appswitcher.quicklaunch.json",
      "value":
      "{\"order\":\[\"1c\",\"calendar\",\"landing\",\"mail\",\"wfm\",
\"contacts\", \"admin\"]}"
      },
      {
      "key": "wfe/appswitcher.landing.json","value":
      "{\"order\":[\"wfm\",\"mail\",\"contacts\",\"calendar\",\"profile\",
\"admin\",\"1c\"], \"main\":\"wfm\"}"
      },
      {
      "key": "wfe/appswitcher.apps.json","value": "{
      \"1c\":{\"url\":\"https://example.com\",\"title\":{\"ru-RU\":
\"1СБухгалтерия\"},\"iconUrl\":\"%cdn_base_url%/apps/1c.png\"},
      \"landing\":{\"url\":\"//auth-{base_url}/landing\"},\"wfm\":{\"url\":
\"//files-{base_url}\"},
      \"mail\":{\"url\":\"//mail-{base_url}    \"},\"contacts\":{\"url\":\"//mail-
{base_url}/#contacts\"},
      \"calendar\":{\"url\":\"//mail-{base_url}/#calendar\"},\"profile\":
{\"url\":\"//auth-{base_url}/profile\",\"userTypes\":[\"default\"]},
      \"admin\":{\"url\":\"//admin-{base_url}\",\"userTypes\":[\"admin\"]}
      }"
      }
      ]
      }
```

В примере манифеста указаны: кастомное приложение и все базовые приложения «МойОфис Документы», а именно `landing`, `wfm`, `mail`, `contacts`, `calendar`, `profile`, `admin`.

2.1 Для создания бандла необходимо выполнить следующие действия:

– во всех базовых приложениях значение переменной `base_url` должно быть представлено в виде ссылки на сервер с развернутой средой «МойОфис Документы». Для удобства допускается использовать поиск (Ctrl + F) с заменой всех вхождений. Например: у адреса https://example.com/ переменная `base_url` будет представлена в ввиде значения `example.com`;

– заменить «1С» на название кастомного приложения (в примере есть три вхождения). Аналогично заменить `url`, `title`, `iconUrl`, относящиеся к кастомному приложению.

При создании записей кавычки внутри поля `"value"` должны быть экранированы обратным слешем: `\"ru-RU\"`.

3. Создание директории с ресурсами.

В директории с ресурсами располагают файлы, которые будут добавлены на CDN. В качестве примера будет использован значок кастомного приложения.

Например директория с ресурсами называется `resources`. В ней расположена директория `icons`, в которой будет размещена иконка кастомного приложения `custom_icon.svg`. В результате в файле `cdn_bundle.json` путь до иконки будет выглядеть следующим образом: `%cdn_base_url%/resources/icons/custom_icon.svg`.

Иконка требуется только для кастомных приложений, для базовых приложений «МойОфис Частное Облако 2» иконка не требуется.

При использовании иконок применяются следующие правила:

– иконки, необходимые для интеграции с внешними продуктами, запрашиваются у соответствующего вендора;

– для продуктов «МойОфис» иконки можно скачать по ссылке: https://myoffice.ru/files/identity/logo_icons_MyOffice.zip;

– если при подготовке кастомизированного бандла иконки не будут приложены для подключаемых внешних приложений, то для данных приложений в «МойОфис Документы» будет отображаться универсальная иконка;

– допускается использование разных форматов изображений (png, svg). Предпочтительно svg.

4. Загрузка бандла на сервер.

Для загрузки необходима директория с бандлом, которая содержит `cdn_bundle.json` и директорию с ресурсами. Перед загрузкой на сервер директорию с бандлом нужно упаковать в формат tar.gz или tgz архив. Полученный архив загрузить на сервер.

5.3.6 Загрузка с помощью Manage API

Подготовленный бандл (или метабандл) загружается с помощью `Manage_API`, адрес `<SSO_IP>` сервера Auth/SSO выбирается из указанных в группах `co_lb_core_auth` или `co_lb_core_wopi` файла inventory.

После загрузки появится сообщение с кодом `HTTP 200` и `JSON`, описывающим текущую ревизию.

При возможных ошибках сообщение будет содержать код `400` и `JSON`, с описанием ошибки:


```
curl -s 'http://<SSO_IP>:8888/api/manage/cdn/upload' -F
'file=@cdn_bundle.tar.gz'
или
curl -sk 'https://<SSO_IP>:8443/api/manage/cdn/upload' -F
'file=@cdn_bundle.tar.gz'
```

Пример успешного ответа:

```
{"message":"CDN bundle uploaded and installed as revision 1","success"
:"true"}
Пример ошибки при загрузке бандла:
{"message":"CDN bundle installation error: can't open manifest
(cdn_bundle.json is missing?)","success":"false"}
```

Во время загрузки один из рабочих процессов (worker) Nginx может быть на некоторое время заблокирован. После загрузки произойдет перезагрузка рабочих процессов Nginx, и будет применена новая конфигурация CDN (процесс может занять длительное время, если будут перезагружаться сервисы Core).

Контролировать загрузку бандла возможно по ответам объекта CDN с помощью анализа JSON.

Адрес `https://auth.<domain_name>/config`

(или `https://auth-<domain_env>.<domain_name>/config`).

Объект CDN содержит специальный объект `_versions`, включающий данные в виде `<версия бандла> : <номер ревизии>`.

5.3.7 Загрузка обновлений CDN

Загрузка пакетов обновлений CDN (бандлов) выполняется системным администратором при установке продукта после завершения скрипта развертывания CO.

В текущей версии ПО не реализованы следующие функции:

- возврат на предыдущую версию (возможно ручное изменение в etcd в ветке config/cdn и на файловой структуре в /srv/docker/lsyncd/data);
- проверка целостности и безопасности архива;
- использование цифровой подписи;
- использование тенантно-зависимых ресурсов;
- использование UI управления ресурсами;
- блокирование механизма обновления на время работ по обновлению (устанавливать сразу несколько обновлений параллельно с одного или с нескольких узлов роли `co_lb_core_auth` категорически запрещено).

5.3.8 Система синхронизации файлов CDN между хостами

Синхронизация файлов производится с помощью lsyncd по протоколу `rsync over ssh`. В режиме службы lsync работает на серверах с ролью `co_lb_core_auth`. Синхронизация данных запускается с помощью механизма ядра `inotify`, отслеживается обновление или появление новых файлов и директорий. Параметры синхронизации настраиваются в файле `/srv/docker/lsyncd/conf/lsyncd/lsyncd.conf`.

6 НАСТРОЙКА ФУНКЦИИ ПОИСКА

6.1 Поиск файлов по содержимому

В файловом менеджере реализован поиск файлов по их содержимому. По умолчанию данная функция включена при установке.

Включение или отключение функции выполняется с помощью переменной, указанной в таблице 21.

Таблица 21 — Управление режимом поиска

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (PGS)	/pgs/installation_commons/ search_content	boolean	true (по умолчанию) / false

6.2 Поиск в режиме просмотра документов

Опция предоставляет доступ к функции поиска в режиме просмотра документов в веб-редакторе и в режиме предварительного просмотра в файловом менеджере. По умолчанию данная функция выключена при установке.

При включении функции возникают следующие ограничения в функциональности:

– поиск будет работать только с новыми документами и файлами, которые изменили после включения флага;

– на всех старых документах вместо поиска будет пустое поле, что может ввести пользователей в заблуждение.

При использовании функции возможно снижение производительности системы.

Во время работы системы включение или отключение функции выполняется с помощью переменной, указанной в таблице 22.

Таблица 22 — Управление режимом просмотра после установки

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	config/wte/read.mode.search.enabled	boolean	true (по умолчанию) / false

Включение или отключение функции при установке системы выполняется с помощью переменной, указанной в таблице 23.

Таблица 23 — Управление режимом просмотра при установке

Наименование сервиса	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/main.yml	pregen_search_enabled*	boolean	true (по умолчанию) / false

* — переменная не вписана в файл, необходимо вручную записать наименование переменной и ее значение.

7 ИНТЕГРАЦИОННЫЕ РЕШЕНИЯ

7.1 Интеграция с почтовыми системами

По умолчанию «МойОфис Частное Облако 2» устанавливается без подключения к почтовым системам. Режим «по умолчанию» задается с помощью значений переменных в inventory файле компонента CO, указанных в таблице 24.

Таблица 24 — Настройка интеграции с почтовыми системами

Расположение переменной	Наименование переменной	Тип переменной	Значение по умолчанию
group_vars/co_setup/main.yml	mail_integration_mode	string	none
group_vars/co_setup/main.yml	common_mail_notification_enabled	boolean	false

При изменении режима интеграции (подключения к почтовым системам) необходимо выполнить переустановку системы с указанием соотвествующего значения для параметра `mail_integration_mode`.

Изменение этого параметра с помощью etcd (CO) может привести к некорректной работе интеграции.

Без интеграции с почтовой системой эксплуатировать «МойОфис Частное Облако 2» не рекомендуется, так как будут недоступны следующие функции:

– запрос доступа;

– восстановление пароля пользователя;

– обратная связь;

– почтовые оповещения.

7.1.1 Интеграция с Mailion

Настройка и назначение интеграции представлены в документе ««Malion». Руководство по администрированию».

7.1.2 Интеграция с PSN

Установка «МойОфис Почта 2» должна быть завершена до создания первого тенанта в системе PGS. В обратном случае тенант (и пользователи, входящие в него) не будут синхронизированы с почтой.

Для обеспечения интеграции «МойОфис Почта» с компонентом «"МойОфис Частное облако 2". Система хранения данных (PGS)» необходимо выполнить настройки, представленные в документе «"МойОфис Почта". Руководство по установке почтового сервера».

Дополнительно в inventory файле необходимо задать значения для переменных, указанных в таблице 25.

Таблица 25 — Настройка интеграции с PSN

Расположение переменной	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/main.yml	mail_integration_mode	string	psn2
group_vars/co_setup/main.yml	common_mail_notification_enabled	boolean	true
group_vars/co_setup/main.yml	csp_allowed_frame_ancestors	list	demo1.example.net demo2.example.net

7.1.3 Настройка работы с внешними почтовыми системами по SMTP

В случае интеграции с внешней почтовой системой в «МойОфис Частное Облако 2» будут доступны следующие функции:

– отправка пользователю почтовых оповещений о смене пароля администратором системы;

– отправка пользователю приветственного письма при регистрации его в системе;

– возможность быстрого перехода в почтовый клиент с главного экрана системы или из меню выбора программ (при условии развертывания специального бандла с настройками);

– отправка файла по почте;

– отправка внутренней ссылки на объект по почте;

– уведомление пользователя по почте о предоставлении ему или изменении его прав доступа к объекту;

– запрос доступа к объекту;

– восстановление пароля;

– возможность отправки обратной связи по работе с системой.

Для отправки системных писем-уведомлений (приветственного письма, письма о смене или восстановлении пароля и т.п.) необходимо использовать внешний сервис SMTP.

Для отправки почтовых уведомлений в «МойОфис Частное Облако 2» необходимо задать значение для переменной, указанной в таблице 26.

Таблица 26 — Настройка интеграции с внешними почтовыми системами

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	/nct/co/config/ common/mail.notification.enabled	boolean	true / false (по умолчанию)

Для включения почтовых уведомлений при установке в inventory файле необходимо задать значение для переменной, указанной в таблице 27.

Таблица 27 — Настройка почтовых уведомлений

Расположение переменной	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/main.yml	common_mail_ notification_enabled	boolean	true / false (по умолчанию)

Настройка параметров сервиса SMTP осуществляется в пользовательском интерфейсе администратора тенанта установки (подробнее см. в документе «"МойОфис Частное Облако 2".Руководстве по администрированию»).

При использовании собственного сервиса SMTP внутри тенанта системные письма-уведомления могут быть отправлены от несколько тенантов (от кастомного тенанта или тенанта установки).

7.2 Интеграция со Squadus

Предусмотрена интеграция ПО «МойОфис Частное Облако 2» с корпоративным мессенджером Squadus. Назначение и описание интеграции приведено в документе «Описание интеграции ПО «МойОфис Частное Облако 2» и ПО «Squadus».

Процесс настройки интеграции описан в документе «Настройка интеграции ПО «МойОфис Частное Облако 2» и ПО «Squadus».

7.3 Интеграция с MS Active Directory

Для настройки интеграции в PGS необходимо произвести следующие действия:

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

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

2. Перезапустить сервисы `pgs_aristoteles` и `pgs_euclid`.

3. Открыть веб-интерфейс Keycloak

(адрес по умолчанию `http://<ENV>.<DEFAULT_DOMAIN>:8091/auth`).

4. Выбрать тенант (или realm), для которого нужна интеграция.

5. Нажать `User Federation`.

6. Из выпадающего меню выбрать провайдера LDAP (Add provider) с именем `pgsldapnew`.

7. Заполнить параметры в соответствии с таблицей 28.

Таблица 28 — Значение параметров для интеграции PGS с AD

Параметр	Значение	Комментарий
usernameLDAPAttribute	sAMAccountName (или другое текущее значение атрибута в AD)	Атрибут, назначаемый как имя пользователя в Keycloak
uuidLDAPAttribute	sAMAccountName (или другое текущее значение атрибута в AD)	Атрибут уникального идентификатора объекта
editMode	UNSYNCED	Внутренний атрибут Keycloak, позволяющий обновлять пользовательские данные на LDAP-сервере в режиме «только чтение»
connectionUrl	Хост в формате ldap://111.1.1.1	Хост для подключения к каталогу AD
usersDn	Данные для подключения к AD соответственно настройкам сервера	Путь до OU (организационной единицы), в которой хранятся учетные записи пользователей
bindDn	Логин пользователя AD	Полное имя (DN, distinguished name) учетной записи пользователя в каталоге, от имени которого будет производиться работа с каталогом
bindCredential	Пароль пользователя AD	Пароль учетной записи пользователя в каталоге, от имени которого будет производиться работа с каталогом

8. Остальные параметры оставить по умолчанию.

9. Нажать `Save` и `Synchronize all users`.

10. На вкладке `Users` в левом меню можно просмотреть список всех импортированных пользователей.

11. В случае наличия ошибок возможно вернуться на вкладку `User Federation` к провайдеру `pgsldapnew` и нажать `Remove imported` для очистки списка пользователей.

12. При длине DN больше чем 255 символов, возникают проблемы, связанные с ограничением на количество символов в таблице postgres, в этом случае необходимо выполнить следующую команду:

```
docker exec $(docker ps -q -f name=pgs-postgres) psql -U\
 keycloak -c "ALTER TABLE user_attribute ALTER COLUMN\
 value TYPE TEXT;"
```

7.4 Настройка работы «МойОфис Частное Облако 2» с настольными редакторами «МойОфис»

При эксплуатации у Заказчика настольных редакторов МойОфис (из состава Продуктов – Стандартный и Профессиональный) при установке «МойОфис Частное Облако 2» может быть включена возможность открытия из Частного Облака документов в настольных редакторах.

Управление настройкой осуществляется с помощью переменной, указанной в таблице 29.

Таблица 29 — Переменная для настройки работы с настольными редакторами

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	config/wfe/open.in.desktop.editors.enabled	boolean	false

7.5 Интеграция с системами сбора и хранения событий безопасности

Совместная работа «МойОфис Частное Облако 2» версии 2.6 (и выше) с внешними SIEM-системами позволяет передавать во внешние SIEM-системы события безопасности, фиксируемые в «МойОфис Частное Облако 2», в формате CEF по протоколу syslog для их дальнейшего хранения и анализа средствами внешней системы. Регистрация событий безопасности обеспечена в соответствии с требованиями приказов ФСТЭК России № 17, 21, 31, 239.

Подробное описание представлено в документе «Руководство по настройке интеграции с внешними SIEM-системами».

7.6 Интеграция с антивирусными системами

В ПО «МойОфис Частное Облако 2» предусмотрена интеграция с ПО Kaspersky Endpoint Security (KES).

Обеспечены следующие сценарии интеграции:

– сканирование файлов в режиме On-access;

– сканирование файлов в режиме On-deman;

– восстановление зараженных файлов;

– проверка целостности файлов на сервере PGS;

– проверка целостности компонентов PGS в реальном времени и по требованию.

Подробная информация предоставляется по запросу.

7.7 Интеграция с ESIA

Для настройки авторизации в «МойОфис Частное Облако 2» с помощью ESIA (привязка учетных записей «МойОфис Частное Облако 2» к учетным записям ESIA) может использоваться программный продукт ESIA-Bridge от ООО «РЕАК СОФТ». При использовании ESIA-Bridge настройки интеграции с ESIA общие для всех тенантов инсталляции.

7.7.1 Установка ESIA-Bridge

ESIA-Bridge устанавливается на выделенный виртуальный сервер с минимальной конфигурацией, представленной в таблице 29.

Таблица 30 — Параметры минимальной конфигурации для ESIA-Brige

Параметр конфигурации	Значение
Количество ядер процессора	2 vCpu (тип процессора Intel)
Обьем оперативной памяти	4 Гбайт
Обьем жесткого диска	20 Гбайт (тип HDD)

Работа ESIA-Bridge на сервере поддерживается для ОС Debian / CentOS / RHEL или Windows. В качестве примера в инструкции рассматривается установка и настройка ESIABridge для ОС Linux.

Установка ESIA-Bridge должна быть произведена в соответствии с действующей инструкцией на программу. Дистрибутив ESIA-Bridge поставляется в виде самораспаковывающегося bin-файла. Для установки необходимо выполнить команду:


```
./esia-bridge-1.XX.0.bin
```

После установки ESIA-Bridge создаются следующие директории:

```
/bin
/conf
/lib
```

Файл с настройками для ESIA-Bridge по умолчанию располагается в файле `/usr/share/esiabridge/conf/esia-bridge.conf`.

Формат записи FQDN с установленным ПО ESIA-Bridge: `esia-bridge.<domain_name>`. Запись должна быть создана в публично доступном DNS-сервере. Для аутентификации пользователя и использовании файла cookie, домен ESIA-Bridge должен совпадать с доменом СО.

7.7.2 Конвертирование ГОСТ сертификата ESIA-Bridge

Конвертирование ГОСТ-сертификата системы, подключаемой к ESIA, из формата PFX контейнера «КриптоПро» в формат BKS, поддерживаемый ESIA-Bridge, осуществляется сторонними утилитами (подробнее см. раздел «Настройка работы с ключами ГОСТ Р 34.10-2012» инструкции ESIA-Bridge):

```
java -cp gost-keytool.jar:bcprov-jdk15on-1.62.jar \
ru.reaxoft.gost.Keytool import_pkcs12 \
--srckeystore certkey-esia-gost.pfx \
--srcstorepass "" \
--srckeypass "" \
--srcalias csp_exported \
--destkeystore esia-bridge.bks \
--deststoretype BKS \
--deststorepass "" \
--destkeypass "" \
--destalias gost2012
```

Отличием данной команды от приведенной в официальной инструкции является использование более новой версии библиотеки `bcprov`, позволяющей работать с хранилищами, созданными новыми версиями «OpenSSL» и «КриптоПро». При успешной конвертации, созданный этой командой файл `esia-bridge.bks` должен быть размещен в директории `/usr/share/esia-bridge/conf/` вместо находящегося там файла.

В конфигурацию ESIA-Bridge необходимо внести изменения в соответствии с таблицей 31.

Таблица 31 — Изменение конфигурации ESIA-Bridge

Наименование переменной	Описание
domain="esia-bridge.<domain_name>:9000"	Порт 9000 должен быть открыт в настройках сетевого экрана сервера ESIA-Bridge
esia.host	Домен среды ESIA, продуктивной или тестовой
clients	Лицензия на используемый домен <domain_name>, приобретается отдельно у компании РЕАК СОФТ, при этом параметр host должен указывать FQDN SSO, то есть auth[-<domain_env>].<domain_name>;
id	Мнемоника вызывающей системы в ESIA
name	Имя вызывающей системы в ESIA
cookieDomain	Домен CO, на который будет устанавливаться сессионная cookie, то есть <domain_name>

После изменения настроек ESIA-Bridge необходимо перезапустить сервис командой: `systemctl restart esia-bridge`.

7.7.3 Настройка «МойОфис Частное Облако 2» для интеграции с ESIA

Для подключения интеграции с ESIA со стороны «МойОфис Частное Облако 2» необходимо задать значения для переменных, указанных в таблице 32.

Таблица 32 — Настройка ESIA для «МойОфис Частное Облако 2»

Наименование сервиса	Наименование переменной	Тип переменной	Значение
etcd (CO)	/nct/co/config/wfe/authentication.esia.bridge.enabled	boolean	true / false (по умолчанию)
etcd (CO)	/nct/co/config/wfe/authentication.esia.bridge.entrance_uri	string	http://esiabridge.example.com:9000/blitz/bridge/entrance
etcd (CO)	nct/co/config/wfe/authentication.esia.bridge.user_uri	string	http://esia-bridge.example.com:9000/blitz/bridge/user

Для подключения интеграции с ESIA во время установки в inventory файле необходимо задать значения для переменных, указанных в таблице 33.

Таблица 32 — Настройка ESIA для «МойОфис Частное Облако 2» при установке

Расположение переменной	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/main.yml	esia_bridge_enabled	string	true / false (по умолчанию)
group_vars/co_setup/main.yml	esia_bridge_entrance_uri	boolean	http://esiabridge.example.com:9000/blitz/bridge/entrance
group_vars/co_setup/main.yml	esia_bridge_user_uri	string	http://esia-bridge.example.com:9000/blitz/bridge/user

8 МОНИТОРИНГ И ЛОГИРОВАНИЕ

8.1 Логирование Java-сервисов

8.1.1 Сохранение логов

Предусмотрена функция сохранения журнала событий на диске, после запуска java-сервисов DCM, CVM, NM, FM, JOD, AUDIT, в течении фиксированного времени. Функция предназначена для упрощения поиска неисправностей при запуске.

Путь размещения для примера: `/srv/docker/dcm/logs/dcm.log`.

Для управления функцией необходимо изменить значение переменным, указанным в таблице 33.

Таблица 33 — Управление функцией сохранения логов после запуска

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	config/common/logger.logback.startup.debug.enabled	boolean	true (по умолчанию) / false	Включение/ отключение функции
	config/common/logger.logback.startup.debug.duration	string	PT5m (по умолчанию)	Установка времени в формате ISO 8601

8.1.2 Размещение временной папки

Временная папка для java-сервисов: DCM, CVM, NM, FM, JOD, AUDIT размещается из контейнера на хосте.

Например: `/tmp` (внутри контейнера DCM) размещается на сервере хоста по следующему пути: `/srv/docker/dcm/tmp`.

Функция предназначена упрощения удаления временных файлов при переполнении диска без переустановки docker-контейнеров.

Рекомендуется перезапустить docker-контейнер после удаления временных файлов, для исключения ошибок при его работе.

8.2 Функция отправки ошибок

8.2.1 Установка и настройка Sentry

В «МойОфис Частное облако 2» реализована функция отправки ошибок в сервис аналитики Kibana или сервис Sentry. По умолчанию ошибки отправляются в сервис аналитики Kibana.

Сервис Sentry не входит в комплект поставки ПО, его установка и настройка выполняется администратором самостоятельно. При настройке Sentry следует учитывать рекомендации, изложенные в разделе «Рекомендации по конфигурированию Sentry».

Для настройки функции отправки ошибок необходимо использовать переменные, указанные в таблице 34.

Если в настройках оба сервиса отключены, то отчеты об ошибках отправляться не будут.

Таблица 34 — Отправка ошибок

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	common/logger. analytics.enabled	boolean	true (по умолчанию) / false	Включение/отключение отправки данных в сервис аналитики Kibana
	config/wte/error.log. analytics.enabled	boolean	true (по умолчанию) / false	Отправка ошибок в сервис аналитики Kibana Ошибки отправляются только при включении переменной common/logger.analytics. enabled
	config/wte/error.log. sentry.dsn	string	""	Отправка ошибок в сервис Sentry
	config/wfe/routing/error . log.sentry.url	string	""	Hostname сервера Sentry, если сервер развернут в другом домене
	config/wte/error.log. feedback.enabled	boolean	true (по умолчанию) / false	Включение/отключение поля обратной связи. Функция доступна после включения отправки ошибок в один из сервисов с помощью переменных: wte/error.log.sentry.dsn wte/error.log.analytics. enabled

При включении поля обратной связи с помощью переменной `wte/error.log.feedback.enabled` пользователь может оставить собственный комментарий к ошибке. Этот комментарий будет отправлен в зависимости от конфигурации:

– в Sentry и дополнит соответствующее событие ошибки;

– в сервис аналитики Kibana отдельным событием, с сохранением идентификатора `eventId` из оригинального события ошибки.

События ошибок сервиса аналитики дополняются идентификатором пользователя и идентификатором события.

8.2.2 Рекомендации по конфигурированию Sentry

1. Для сохранения безопасности следует ограничить доступ к серверу Sentry для группы пользователей, которым определены соответствующие процессы допуска к пользовательской информации.

	Ограничения доступа к логам не позволят использовать сервис для отладки развития атаки, а также для получения ID объектов/пользователей.

2. При настройке SSL и в DSN указать `url` с использованием `https`.

3. В настройках проекта следует включить **Verify TLS/SSL** для создания защищенного соединения с сервером Sentry.

4. В настройках проекта необходимо указать домен/или несколько доменов продукта, в меню **Allowed Domains**, для ограничения обращений к серверу от сторонних доменов.

8.2.3 Сбор пользовательской аналитики

В «МойОфис Частное облако 2» реализован сбор пользовательской аналитики, по умолчанию функция выключена. После включения сохраняет действия пользователя при работе с сервисами «МойОфис Частное облако 2». Пользовательская аналитика собирается автоматически и направляется POST-запросами на `url:/api/v1/analytics/user_analytics`.

Для получения, обработки и хранения данных силами администратора системы следует развернуть дополнительный прокси-сервер, собирающий и обрабатывающий данные из POST-запросов.

Для управления функцией сбора пользовательской аналитики необходимо использовать переменную, указанную в таблице 35.

Таблица 35 — Управление пользовательской аналитикой

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
etcd (CO)	config/wte/ user.analytics.enabled	Boolean	true / false (по умолчанию)	включение/ отключение функции

8.3 Системы мониторинга PGS

В качестве системы мониторинга PGS используется Prometheus с отображением информации с помощью Grafana. Prometheus собирает метрики от нескольких источников, перечисленных в таблице 36.

Таблица 36 — Источники метрик

Источник метрики	Сервис	Порт	Примечание
Целевой хост	node-exporter	9100	
Мониторинг docker контейнеров	cadvisor	9101	
Мониторинг сервиса Redis	redis_exporter	9121	
Мониторинг Postgres сервиса	postgres-exporter	9187	
Мониторинг сервиса ArangoDB	напрямую с сервиса ArangoDB с помощью happroxy	-	Доступ до HAProxy возможен только с сервера docker
Мониторинг сервиса Keycloak	напрямую с сервиса Keycloak	-	Доступ до HAProxy возможен только с хоста с docker

С помощью Grafana созданы виртуальные программные панели, каждая из которых предназначена для своего источника данных Prometheus.

Доступ к Grafana осуществляется по порту «3000», логин «admin», пароль задается в файле inventory. Все сервисы запускаются в docker контейнерах.

8.3.1 Node Exporter Extended

Отображает информацию по метрикам, собранным с целевого хоста, таким как использование CPU, RAM, Network, Disk и п.р. Пример графического представления информации приведен на рисунке 1.

Рисунок 1 — Пример представления информации на панели Node Exporter Extended

8.3.2 Docker Monitoring

Отображает использование ресурсов целевого хоста в docker контейнерах. Пример графического представления информации приведен на рисунке 2.

Рисунок 2 — Пример представления информации на панели Docker Monitoring

8.3.3 Redis

Отображает использование ресурсов в сервисе Redis (количество клиентов, использование памяти). Пример графического представления информации приведен на рисунке 3.

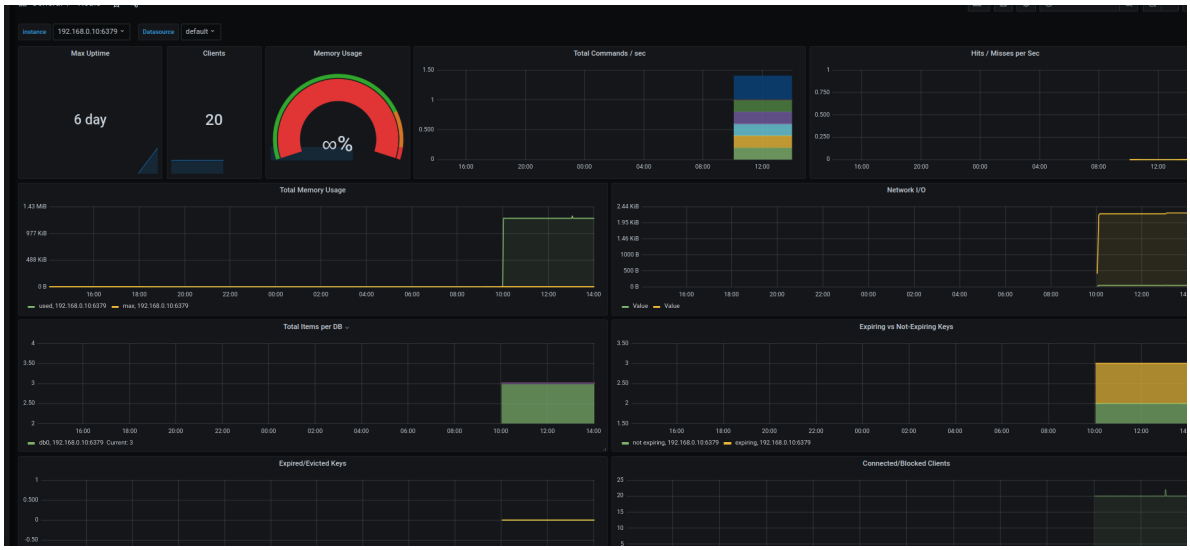

Рисунок 3 — Пример представления информации на панели Redis

8.3.4 ArangoDB_PGS

Отображает все метрики сервиса ArangoDB. Пример графического представления информации приведен на рисунке 4.

Рисунок 4 — Пример представления информации на панели ArangoDB PGS

8.3.5 PostgreSQL Database

Отображает все метрики сервиса PostgreSQL. Пример графического представления информации приведен на рисунке 5.

Рисунок 5 — Пример представления информации на панели PostgreSQL

8.3.6 Keycloak Metrics Dashboard

Отображает все метрики сервиса Keycloak. Пример графического представления информации приведен на рисунке 6.

Рисунок 6 — Пример представления информации на панели Keycloak Metrics Dashboard

8.3.7 Epicure

Отображает все метрики сервиса Epicure. Пример графического представления информации приведен на рисунке 7.

Рисунок 7 — Пример представления информации на панели Epicure-Monitoring

8.3.8 RabbitMQ

Отображает все метрики сервиса RabbitMQ. Пример графического представления информации приведен на рисунке 8.

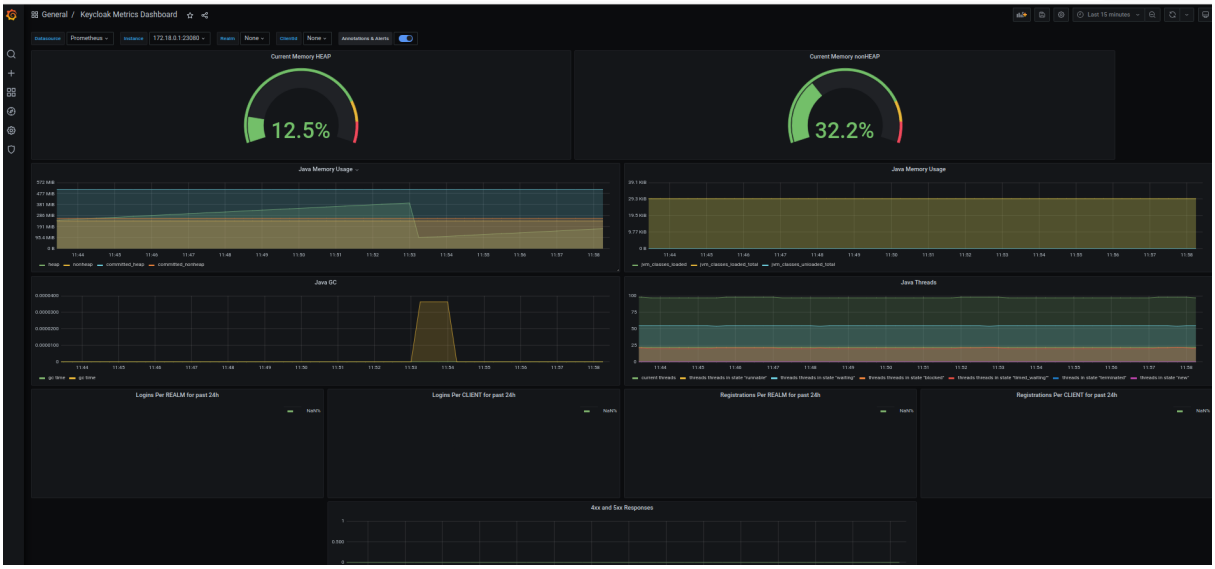

Рисунок 8 — Пример представления информации на панели RabbitMQ-Overview

8.4 Системы мониторинга СО

В качестве системы мониторинга в СО используется Grafana, для логирования используется Kibana. Для доступа к системам мониторинга и логирования СО необходимо использовать параметры, указанные в таблице 37.

Таблица 37 — Доступ к мониторингу СО

Адрес обращения при кластерной установке	Адрес обращения при установке standalone	Имя пользователя	Пароль из переменной
http://kibana.domain.name	http://kibana.domain.name:81	admin	elasticsearch_admin_password
http://grafana.domain.name	http://grafana.domain.name:81	admin	grafana_admin_password

9 ЗАМЕНА SSL-СЕРТИФИКАТА

9.1 Замена сертификата в компоненте CO

Замена сертификата в «МойОфис Частное Облако 2» (компонент CO) выполняется в 2 этапа:

1. В каталоге `/install_co/certificates` необходимо заменить следующие файлы:

– `server.crt` – сертификат внешнего домена;

– `server.nopass.key` – ключ внешнего домена;

– `ca.pem` – все доверенные SSL-сертификаты.

2. После этого выполнить следующую команду:

```
ansible-playbook playbooks/co.yml \
-e tls_certs_generate_cert_force_update=true -t openresty
```

Допускается добавлять в команду другие параметры при необходимости.

9.2 Замена сертификата в компоненте PGS

Замена сертификата в «МойОфис Частное Облако 2» (компонент PGS) выполняется на сервере с ролью Pythagoras:

В директории `/opt/Pythagoras/certificates` необходимо заменить следующие файлы:

– `server.crt` – содержит SSL-сертификат на домен установки и все промежуточные сертификаты, кроме корневого доверенного, расположенные в порядке, описанном в документации Nginx;

– `server.nopass.key` – приватный ключ сертификата, не требующий кодовой фразы;

– `ca.crt` – все доверенные SSL сертификаты.

После этого следует перезагрузить сервер с помощью команды:

```
docker service update pgs-Nginx_Nginx --force
```

При кластерной архитектуре достаточно запустить команду на одном из серверов.

10 ПРОСМОТР ПРОФИЛЯ ЭКСПЛУАТАЦИИ СИСТЕМЫ

Администратор установки может выполнить анализ профиля эксплуатации системы конечными пользователями. Эта информация используется для дальнейшей оптимизации текущих серверных ресурсов.

Для возможности сбора информации о профиле установки необходимо соблюдение следующих требований:

1. В системе развернуты следующие сервисы:

– Elastic;

– Fluentd;

– Kibana (на стороне СО).

2. Установленная система работает на протяжении необходимого для сбора статистики времени (минимальный срок — 1 неделя).

Для создания отчета необходимо:

1. Открыть в **Kibana Dashboard** -> **Profile Dashboard**.

2. Выбрать период времени 1-3 месяца (можно выбрать больший период, но в зависимости от конфигурации и выбранной детализации нагрузка на сервис Kibana может привести к ошибкам).

3. Если данные с дашборда не противоречат политикам безопасности, сделать скриншоты всех графиков и таблиц и передать в «МойОфис» для получения рекомендаций по изменению архитектуры установки с целью опимизации серверных ресурсов.

11 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