ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

СИСТЕМА РЕДАКТИРОВАНИЯ И СОВМЕСТНОЙ РАБОТЫ

СИСТЕМА ХРАНЕНИЯ ДАННЫХ

3.3

РУКОВОДСТВО ПО НАСТРОЙКЕ

Версия 1

На 49 листах

Дата публикации: 18.03.2025

Москва
2025

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам.

Товарные знаки «МойОфис», «MyOffice» и «Squadus» 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 (табл. 1).

Таблица 1 — Сокращения и обозначения

Сокращение, термин	Расшифровка и определение
API	Application Programming Interface, интерфейс программирования приложений
Auth SSO	Single Sign-On, процесс аутентификации, позволяющий пользователю один раз войти в систему с одним набором учетных данных для доступа к нескольким приложениям или службам
AMQP	Advanced Message Queuing Protocol, открытый протокол прикладного уровня для передачи сообщений между компонентами систем
CO	Система редактирования и совместной работы
PGS	Система хранения данных
PSN	Приложение почты, календаря и контактов («МойОфис Почта»)
REST API	Архитектурный стиль взаимодействия компонентов распределенного приложения в сети
S3 хранилище	Сервис хранения объектов, предлагаемый поставщиками облачных услуг
SPA	Single Page Application, веб-приложение или веб-сайт, использующий единственный HTML-документ как оболочку для всех веб-страниц и организующий взаимодействие с пользователем через динамически подгружаемые HTML, CSS, JavaScript, обычно посредством AJAX
SIEM	Security information and event management, система (или технология) управления информацией и событиями безопасности
Inventory	Файл, содержащий набор управляемых хостов для автоматизации установки и управления конфигурацией для сервиса Ansible
IOPS	Input/Output Operations Per Second, количество операций ввода/вывода
UI	User interface, интерфейс пользователя
ОС	Операционная система
СУБД	Система управления базами данных, комплекс программно-языковых средств, позволяющих создать базы данных и управлять данными
Тенант	Логический объект, включающий в себя совокупность вычислительных ресурсов, репозиторий и пользователей
ПО	Программное обеспечение

1 ОБЩИЕ СВЕДЕНИЯ

1.1 Назначение

В настоящем документе описан порядок настройки Системы редактирования и совместной работы из состава и Системы хранения данных.

1.2 О компонентах

Система хранения данных — компонент, предназначенный для безопасного хранения корпоративных файлов и обеспечения возможностей авторизации, аутентификации и разграничения прав доступа пользователей.

Система редактирования и совместной работы — компонент, предназначенный для индивидуального и совместного редактирования текстовых и табличных документов, а также просмотра и демонстрации презентаций.

Представленные компоненты входят в состав следующих продуктов:

– «МойОфис Документы Онлайн»;

– «МойОфис Профессиональный 2»;

– «МойОфис Профессиональный 3»;

– «МойОфис Схема»;

– Squadus PRO.

Подробное описание возможностей продукта приведено в документе «Функциональные возможности».

1.3 Перечень технической документации

С помощью технической документации, представленной в таблице 2, осуществляется развертывание серверной части, настройка и администрирование продукта.

Комплект документации распространяется на компоненты продукта:

– Система редактирования и совместной работы (CO);

– Система хранения данных (PGS).

Таблица 2 — Перечень технической документации

Наименование документа	Используемые компоненты	Содержание документа
«Системные требования»	CO, PGS	Системные и программные требования к продукту
«Архитектура»	CO, PGS	Описание архитектуры продукта для выбора типа установки и выделения ресурсов для серверов
«Система редактирования и совместной работы. Руководство по установке»	CO	Порядок установки системы редактирования и совместной работы
«Система хранения данных. Руководство по установке»	PGS	Порядок установки системы хранения данных
«Руководство по настройке»	CO, PGS	Настройка серверов продукта после установки и в ходе эксплуатации системы, а также процессов мониторинга и логирования
«Руководство по администрированию»	CO, PGS	Функции управления тенантом в ходе эксплуатации системы
«Руководство по резервному копированию»	PGS	Порядок резервного копирования баз данных, расположенных в системе хранения данных
«Сервисно-ресурсная модель»	CO, PGS	Логическая модель сервиса, описывающая состав и взаимосвязи компонентов (ресурсов), которые совместно обеспечивают предоставление сервиса
«Руководство по мониторингу»	CO, PGS	Функции отображения текущего состояния системы и отдельных сервисов
«Руководство по работе с API»	CO, PGS	Набор методов для автоматизированного управления пользователями, группами, общими папками, доменами и тенантами

2 УПРАВЛЕНИЕ ТЕНАНТАМИ

В продукте 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 «Руководство по администрированию»).

Получение настроек тенанта на стороне 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 «Система хранения данных (PGS). Руководство по установке»).

	Для версии 3.1 и выше существует запрет использования спецсимволов (в том числе и символа «точка») в имени тенанта.

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 3.

Таблица 3 — 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 «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 Настройка PGS

2.2.1 Общие требования

1. Файл `cert.pem` для доверенного сертификата должен содержать следующую цепочку сертификатов:

– сертификат на домен;
– промежуточные сертификаты (если есть).

2. Файл `cert.pem` для самоподписанного сертификата должен содержать следующую цепочку сертификатов:

– сертификат на домен;
– промежуточные сертификаты (если есть);
– сертификат корневой.

3. Файлы сертификата и ключа не должны содержать пустых строк.

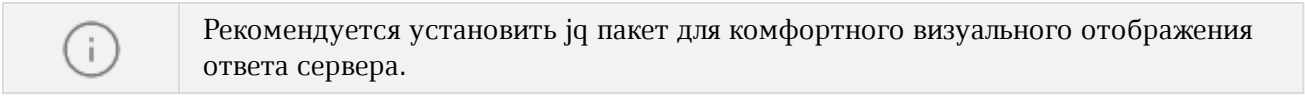
2.2.2 Назначение переменных

Для выполнения команд необходимо объявить локальные переменные и присвоить им свои значения, которые должны совпадать с аналогичными переменными inventory файлов CO и PGS.

Пример заполнения для создания тенанта с именем `second.example.net` и доменом `second.example.net` на домене продукта `example.net`:

```
url=https://admin.example.net/adminapi
name=second.example.net
domain=second.example.net
cert_file=/root/second.example.net/cert.pem
cert_key_file=/root/second.example.net/server.nopass.key
couser_password=переменная openresty_api_password \
из /root/install_co/group_vars/main.yml
fs_app_key=1403386F683139F1975730171DC40967DE67201170AA5B1CBCCF894DD7815942
fs_app_iv=AEB2DB5F3F3F4B4E3289C94C507F89D6
fs_app_salt=BBA9B6CDBD87F78A
passwd=переменная KEYCLOAK_PASSWORD из ~/install_MyOffice_PGS/inventory/hosts.yml
```


2.2.3 Порядок выполнения



Для создания тенанта со стороны PGS следует:

1. Для получения токена необходимо выполнить следующую команду:

```
pgs_token=$(curl -k -XPOST "$url/auth" -d "username=pgs" \
-d "password=$passwd" 2>/dev/null | jq ".token" - | cut -d '"' -f2)
```

2. Для получения tenant_id необходимо выполнить следующую команду:

```
tenant_id=$(curl -k -XGET "$url/tenants/$name" -H \
"Authorization: $pgs_token" | jq ".id" - | cut -d '"' -f2)
```

3. Для подготовки файла сертификата необходимо удалить пробелы и проставить символы конца строки с помощью команды:

```
cert=$(cat $cert_file | sed 's/$/\\n/' | tr -d '\n' | sed 's/\\n$//')
```

4. Шифрование ключа выполняется с помощью xxd. Перед выполнением команды необходимо установить xxd.

```
cert_key=$(cat $cert_key_file | openssl enc -aes-256-cbc \
-e -K $fs_app_key -iv $fs_app_iv -S $fs_app_salt | xxd -ps -u -c 32 | tr -d '\n')
```

5. Для добавления сертификата и ключа на PGS необходимо выполнить следующую команду:

```
curl -s -k -H "Authorization: $pgs_token" "$url/smtp_conf/$name" \
-X PUT -H 'Content-Type: application/json' --data \
"{\"cert\":\"$cert\",\"key\":\"$cert_key\"}"
```

6. Выполнить перезагрузку тенанта с помощью команды:

```
curl -s -k -u 'couser:$couser_password' \
-XPOST http://co:8888/api/manage/config/tenants/$tenant_id/reload
```

2.3 Настройка ETCD

Для проверки и корректировки действий, выполненных в разделе «Настройка CO».

1. Инициировать считывание параметров тенанта в PGS и получить ID целевого тенанта:

```
tenant_id=$(curl -s -H "Authorization: ${pgs_token}" \
   https://${pgsapi}/adminapi/tenants | jq -r ".[] | select(.default_domain == \"${domain}\") | .id")
```

Где:

`${pgsapi}` — основной рабочий домен PGS;

`${domain}` — домен целевого тенанта.

2. Для того, чтобы проверить параметры сертификата и ключа сертификата следует выполнить на ноде CO с ролью etcd команду следующего вида:

```
# Узнать текущую версию ${etcd_version}
docker exec -it $(docker ps -qf name=etcd3) etcdctl ls /nct/co
/nct/co/28.0.9
docker exec -it $(docker ps -qf name=etcd3) etcdctl get /nct/co/${etcd_version}/tenants/${tenant_id}
```

Где:

`${etcd_version}` — текущая версия ветки ETCD;

`${tenant_id}` — ID тенанта, полученный в п.1.

3. В случае, если параметры сертификата и ключа не появились в выводе программы, необходимо выполнить запрос в CO следующего вида:

```
curl -s -u 'CO_MANAGE_API_USERNAME:CO_MANAGE_API_PASSWORD' \
  -XPOST http://<auth_domain>:8888/api/manage/config/tenants/${tenant_id}/reload
```

Где:

`<auth_domain>` — домен авторизации в CO;

`CO_MANAGE_API_USERNAME:CO_MANAGE_API_PASSWORD` — атрибуты доступа к CO API.

2.4 Настройка PSN

1. Первым шагом настройки на стороне PSN («МойОфис Почта 3») является подготовка сертификата и ключа сертификата в PEM-формате. Сертификат должен быть выписан на домен тенанта в wildcard-виде `*.${domain}` или для следующих имен:

```
mail.${domain}
smtp.${domain}
imap.${domain}
psnapi.${domain}
pbm.${domain}
cab.${domain}
autoconfig.${domain}
```

Где `${domain}` — домен целевого тенанта.

Файлы сертификата и ключа не должны содержать пустых строк. Также сертификат должен содержать полную цепочку промежуточных центров сертификации (CA), если такие имеются.

Более подробно настройка сертификатов для PSN описана в документации по «МойОфис Почта 3».

2. Следующим шагом для формирования PUT-запроса в API PSN необходимо получить токен авторизации в PBM (backend manager), пример:

```
creator='<creator_email>'
pass='<password>'
pbm_domain='<pbm_domain>'

psn_token=$(curl -s "https://${pbm_domain}/v2/auth" \
  -d login=${creator} \
  -d password=${pass} | jq -r .result.access_token)
```

Где:

`<creator_email>` — логин в PBM общего вида `creator@<install_domain>` ;

`<password>` — значение переменной ds389_manager_user из инвентарного файла установки PSN;

`<pbm_domain>` — URL сервера PSN с ролью PBM общего вида `pbm[-env].<install_domain>` .

3. Сформированный PUT-запрос выполняется следующей командой:

```
webmail="mail.${domain}"

curl -H "Authorization: Bearer ${psn_token}" -XPUT \
  https://${pbm_domain}/v2/domains/${tenant_id}/${domain} \
  -F "webmail_domain=${webmail}" \
  -F "crt=@${cert_file}" \
  -F "key=@${cert_key_file}"
 #если не получилось передать сертификаты через флаг -F, можно передать json через -d
psn_cert=$(cat $cert_file | sed 's/$/\\n/' | tr -d '\n' | sed 's/\\n$//')
psn_key=$(cat $cert_key_file | sed 's/$/\\n/' | tr -d '\n' | sed 's/\\n$//')
curl -X PUT -H 'Accept: application/json' \
  -H 'Accept-Encoding: gzip, deflate' -H "Authorization: Bearer ${psn_token}" \
  -H 'Content-Type: application/json' \
   -d  "{\"webmail_domain\":  \"${webmail}\",  \"key\":  \"${psn_key}\",  \"crt\": \"${psn_cert}\"}" https://${pbm_domain}/v2/domains/${tenant_id}/${domain}
```

Где:

`<pbm_domain>` — URL сервера PSN с ролью PBM;

`${tenant_id}` — ID тенанта (получается методом, аналогичном описанному п.1);

`${domain}` — целевой домен;

`${webmail}` — имя `mail.${domain}` (имя домена PSN с ролью mail).

4. В случае настроенной интеграции PSN и PGS для корректной работы SSO (single sign on) необходимо выполнить дополнительную настройку параметров в ETCD (и для CO, и для PSN). Первым шагом будет определение единого секрета для oauth2 следующей командой:

5. Далее на ноде CO с ролью etcd следует выполнить:

```
# Узнать текущую версию ${etcd_version}
docker exec -it $(docker ps -qf name=etcd3) etcdctl ls /nct/co
/nct/co/28.0.9
docker exec -it $(docker ps -qf name=etcd3) etcdctl set \
  /nct/co/${etcd_version}/config/wfe/oauth2_clients/${domain//\.} \
                                "{\"client_secret\":\"${secret}\",\"redirect_uri\": \"https://${webmail}/system/sso\"}"
```

В `clients_id` не допускаются сиволы "." и "_". См. переменную `${domain//\.}` — убираем точки.

Где

`${etcd_version}` — текущая версия ветки ETCD (см. п.2);

`${webmail}`— имя `mail.${domain}` (имя домена PSN с ролью mail);

`${secret}` — секрет для oauth2.

6. При интеграции PSN для работы frame позволяющего добавлять ссылки на файлы из Облака необходимо добавить. Например:

```
# В примере добавлено два домена
docker exec -it $(docker ps -qf name=etcd3) etcdctl set \
               /nct/co/${etcd_version}/config/wfe/csp.allowed_frame_ancestors.json
"[\"https://mail.doc.myoffice-app.ru\",\"https://${webmail}\"]"
```

Где

`${etcd_version}` — текущая версия ветки ETCD;

`${webmail}` — имя `mail.${domain}` (имя домена PSN с ролью mail).

7. На ноде PSN с ролью etcd следует задать параметр командой:

```
docker exec –i $(docker ps -qf name=etcd.1) etcdctl put \
services/co/psn_mail.${domain}                  "{\"client_secret\":\"${secret}\",
\"redirect_uri\":\"https:\/\/mail.${domain}\/system\/sso\",\"client_id\":
\"${domain//\.}\",\"sso_url\":\"https:\/\/auth.${domain}\"}"
```

Где

`${domain}` — целевой домен;

`${secret}` — секрет для oauth2.

8. Финальным шагом будет перезапуск сервис `psn-nginx-proxy_nginx` с любой мастер ноды PSN:

```
docker service update --force psn-nginx-proxy_nginx
```

После успешного выполнения всех приведенных выше операций CO и PSN начнут обрабатывать запросы на новый домен (в том числе с использованием SSO).

2.5 Изменение количества тенантов

Настройка позволяет ограничить количество тенантов. Значение изменяется с помощью переменной, указанной в таблице 4.

Таблица 4 — 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)

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 5.

Таблица 5 — 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 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)

3.2.2 Настройка автоматической конвертации документов внешнего формата при загрузке

В продукте реализована функция автоматической конвертации документов внешнего формата при загрузке их в систему. После установки СО 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 продукт необходимо 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 «Веб-приложение "МойОфис Текст". 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 Управление запросом уведомлений об изменениях

В продукте реализована функция уведомления пользователей об изменениях в файлах.

Для включения уведомлений необходимо использовать административную панель (см. в документе «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 9.

Таблица 9 — 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
```

3.4 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 СО 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 «Веб-приложение "МойОфис Текст". Руководство пользователя»).

Управление режимом выполняется с помощью переменной, указанной в таблице 10.

Таблица 10 — Переменная для настройки режима открытия документа

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

Управление функцией поддерживается на этапе развертывания СО. 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
```

3.5 Отключение корпоративной адресной книги

В продукте 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 11.

Таблица 11 — 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

3.6 Настройка автоматического отключения неактивного пользователя

В продукте предусмотрено автоматическое отключение пользователей от редактируемого документа, в случае их бездействия.

Изменение времени задается с помощью переменной, указанной в таблице 12.

Таблица 12 — Переменная для настройки прерывания сессии

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	nct/co/config/nps-du/ Du.Env.TimeInactivityMins	integer	минута	30 (значение 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:

```
du_max_time_for_inactive_collaborator_mins
```

Пример команды настройки функции:

```
ansible-playbook playbooks/main.yml \
 -e du_max_time_for_inactive_collaborator_mins=60
```


3.7 Настройка длительности сессии

По умолчанию настройка длительности сессии определяется автоматически во время установки системы и составляет 3 дня. Значение по умолчанию можно переопределить с помощью переменной, указанной в таблице 13.

Таблица 13 — Переменная для настройки длительности сессии

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	config/wfe/auth.token.ttl	integer	секунды	259000 (значение по умолчанию)

При включении настройки **Безопасность** > **Ограничение длительности сеансов** > **Завершать сеансы пользователей при бездействии** в панели администратора значение переменной `auth.token.ttl` в etcd учитываться не будет (подробнее о настройке см. в документе «Руководство по администрированию»).

3.8 Настройка длительности запроса при разрыве соединения

При восстановлении интернет соединения все пользователи тената одновременно запрашивают текущую папку, что создает большую одномоментную нагрузку. Для уменьшения нагрузки в продукте введена случайная задержка запроса на обновление папки в диапазоне от 1 до n секунд. Значение n устаналивается с помощью переменной, указанной в таблице 14.

Таблица 14 — Переменная для настройки прерывания сессии

Наименование сервиса	Наименование переменной	Тип переменной	Размерность	Значение
etcd (CO)	nct/co/config/wfm/max.request.delay	integer	секунда	60 (значение по умолчанию)

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

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

```
openresty_wfe_max_request_delay
```

Пример команды настройки функции:

```
ansible-playbook playbooks/main.yml \
 -e openresty_wfe_max_request_delay=100
```

3.9 Ограничение количества пользователей при совместном редактировании

В продукте предусмотрено ограничение на количество пользователей, одновременно редактирующих один документ. По умолчанию 20 пользователей может одновременно редактировать один документ (находиться в одной сессии редактирования), остальные могут открыть документ только для просмотра.

Увеличение общего количества пользователей может приводить к затруднениям в работе с документом: увеличении времени открытия документа и ошибкам при загрузке. Для сохранения стабильной работы системы рекомендуется использовать для работы с таблицами не более 50, для работы с текстовыми документами не более 20.

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	20

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 СИСТЕМЫ ДЛЯ РАБОТЫ СО СЛОЖНЫМИ ФАЙЛАМИ

В продукте появились настройки для ограничения использования оперативной памяти при работе со сложными файлами.

Для системы с минимально возможными аппаратными ресурсами работа со сложными файлами ограничена одной операцией над сложным файлом в один момент времени. При увеличении количества операций в один момент времени могут возникать задержки в текущих операциях и ошибки в работе других операций (в том числе над другими файлами), с сохранением общей работы системы.

При возникновении ошибки, связанной с отсутствием возможности редактировать документ необходимо установить значение `false` переменной, представленной в таблице 16.

Таблица 16 — Проверка сложных файлов

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	dcm/dcm.enable.recheck.heavyfile	bolean	true

4.1 Настройка сервиса DU

Выделение дополнительных ресурсов сервису `DU` для открытия файлов на редактирование выполняется с помощью переменной `du_max_memory_heavy`.

Для увеличения количества открытых на редактирование файлов следует изменить в большую сторону значения переменным `du_pool_size` и `du_heavy_unit_count`.

Рекомендуется контролировать используемую сервисом `DU` память средствами мониторинга для сохранения стабильной работы системы.

Для изменения ограничения необходимо установить новые значения переменным, указанным в таблице 17.

Таблица 17 — Переменные для настройки сервиса DU

Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
du_max_memory_heavy	string	гигабайты	"5GB"	Максимальное количество RAM для сложных файлов
du_pool_size	integer	количество сервисов	100	Количество сервисов `DU` для редактирования файлов

Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
du_heavy_unit_count	integer	количество сервисов	2	Количество сервисов `DU` для редактирования сложных файлов

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 du_heavy_unit_count=5
```

4.2 Настройка пользователя

Для конфигурации работы со сложными файлами на стороне пользователя необходимо использовать переменные, указаные в таблице 18.

Таблица 18 — Настройка пользователя для работы со сложными файлами

Наименование переменной	Тип переменной	Размерность	Значение по умолчанию	Описание
co/config/wte/ worker.init.timeout	integer	милли-секунды	200000	Время ожидания инициализации Worker
co/config/wte/ service.init.timeout	integer	милли-секунды	600000	Время ожидания инициализации WTE сервисов
co/config/wte/ document.processing.timeout	integer	милли-секунды	600000	Время ожидания обработки документа сервисом Core
co/config/wte/ document.load.timeout	integer	милли-секунды	180000	Время ожидания обработки и загрузки документа от сервиса DU

5 НАСТРОЙКА ИНТЕРФЕЙСНЫХ СИСТЕМНЫХ УВЕДОМЛЕНИЙ

5.1 Баннер «О планируемых работах на сервере»

Настройка баннера «О планируемых работах на сервере» выполняется внесением изменений в конфигурационный файл, указанный в таблице 19.

Таблица 19 — 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 until11:00 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`

5.2 Баннер «Об истечении срока действия пароля пользователя»

Переменная в таблице 20 регулирует период уведомления пользователя об истечении срока действия пароля (не работает при включенной интеграции с Microsoft Active Directory).

Таблица 20 — 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

5.3 Баннер «О мобильном приложении»

Переменная в таблице 21 устанавливает адрес страницы для скачивания мобильного приложения. Если переменная принимает значение "" кнопка **О мобильном приложении** в веб-интерфейсе не отображается.

Таблица 21 — Настройка скачивания мобильного приложения

Наименование сервиса	Наименование переменной	Тип переменной	Значение по умолчанию
etcd (CO)	config/wfe/mobile.apps.site.url	string	"https://myoffice.ru..."*
* — *https://myoffice.ru/apps/mobile-documents/?utm_source=prod&utm_medium=int&utm_campaign=mob_promo_july24&utm_term=priv_cloud*			

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_wfe_mobile_apps_site_url
```

Пример команды настройки функции:

```
ansible-playbook playbooks/main.yml \
-e openresty_wfe_mobile_apps_site_url=""
```

5.4 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 22.

Таблица 22 — 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)

6 КАСТОМИЗАЦИЯ

6.1 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"
]
}
```

6.2 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.

6.3 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 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.

6.3.1 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.

6.3.2 Структура cdn_bundle.json

Файл `cdn_bundle.json` состоит из переменных, представленных в таблице 23.

Таблица 23 — Переменные cdn_bundle.json

Переменные	Описание
bundleVersion	Версия бандла
formatVersion	Версия формата описания бандла (на данный момент есть только версия «1»)
description	Произвольная строка с описанием
merge	Функция объединения или замены структуры данных с одинаковыми именами в etcd (по умолчанию false)
properties	Массив полей etcd, которые необходимо переопределить

6.3.3 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 24.

Таблица 24 — 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

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

Параметры в таблице 25 соответствуют ключам в `"wfe/appswitcher.quicklaunch.json"` и `"wfe/appswitcher.landing.json"`.

Таблица 25 — 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.

6.3.5 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 `apps`. В ней расположен каталог `icons`, в котором 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 продукта 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.

6.3.6 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>`.

6.3.7 Загрузка обновлений CDN

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

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).

6.3.8 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`.

7 НАСТРОЙКА ФУНКЦИИ ПОИСКА

7.1 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 26.

Таблица 26 — Управление режимом поиска

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

8 ИНТЕГРАЦИОННЫЕ РЕШЕНИЯ

8.1 Интеграция с почтовыми системами

По умолчанию продукт устанавливается без подключения к почтовым системам. Режим «по умолчанию» задается с помощью значений переменных в inventory файле CO, указанных в таблице 27.

Таблица 27 — 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 продукт не рекомендуется, так как будут недоступны следующие функции:

– запрос доступа;

– восстановление пароля пользователя;

– обратная связь;

– почтовые оповещения.

8.1.1 Интеграция с Mailion

Для настройки интеграции продукта с ПО Mailion в inventory файле перед установкой необходимо задать значения для переменных, указанных в таблице 28.

Настройка ПО Mailion представлена в документе ««Malion». Руководство по администрированию».

Таблица 28 — Настройка интеграции с Mailion

Расположение переменной	Наименование переменной	Тип переменной	Значение
group_vars/co_setup/ main.yml	mail_integration_mode	string	none
group_vars/co_setup/ main.yml	common_mail_notification _enabled	boolean	true
group_vars/co_setup/ main.yml	csp_allowed_frame_ancest ors	list	demo1.example.net demo2.example.net

После установки продукта для синхронизации с ПО Mailion необходимо:

1. Для отправки почтовых уведомлений пользователям следует настроить исходящие системные сообщения SMTP-сервера (подробнее см. в документе «Руководство по администрированию»).
2. Для добавления ярлыка ПО Mailion на главную навигационную страницу следует ознакомиться с разделом «Персонализация с помощью cdn_bundle».
3. Для синхронизации каталогов пользователей, сквозной авторизации и аутентификации пользователей в обеих системах необходимо в ETCD настроить параметры OAuth2-клиента в ветке `nct/co/config/wfe/oauth2_clients`:

```
mailion: { "client_secret": "mailionpass", "redirect_uri": "https://<domain_env>/callback" }
```

где `<domain_env>` — доменное имя, используемое при развертывании ПО Mailion.

Значение `redirect_uri` в продукте и ПО Mailion должно содержать идентичное значение.

В системе присутствует ограничение: не реализован автоматический локальный выход (logout) в одной из систем при выходе пользователя из другой системы.

8.1.2 Интеграция с PSN

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

Для обеспечения интеграции «МойОфис Почта 3» с «Системой хранения данных (PGS)» необходимо выполнить настройки, представленные в документе «МойОфис Почта 3. Руководство по установке почтового сервера».

Дополнительно в inventory файле необходимо задать значения для переменных, указанных в таблице 29.

Таблица 29 — 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_ancest ors	list	demo1.example.net demo2.example.net

8.1.3 Настройка работы с внешними почтовыми системами по SMTP

В случае интеграции с внешней почтовой системой в продукте 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 продукте необходимо задать значение для переменной, указанной в таблице 30.

Таблица 30 — 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 31.

Таблица 31 — 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 «Руководство по администрированию»).

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

8.2 Интеграция со Squadus

Предусмотрена интеграция продукта с корпоративным мессенджером Squadus. Назначение и описание интеграции приведено в документе «Система редактирования и совместной работы. Система хранения данных. Интеграция со Squadus».

Процесс настройки интеграции описан в документе «Руководство по настройке интеграции облачного хранилища со Squadus».

8.3 Настройка работы продукта с настольными редакторами «МойОфис»

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

Управление настройкой осуществляется с помощью переменной, указанной в таблице 32.

Таблица 32 — 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

8.4 Интеграция с системами сбора и хранения событий безопасности

Совместная работа продукта версии 2.6 (и выше) с внешними SIEM-системами позволяет передавать во внешние SIEM-системы события безопасности, фиксируемые в продукте, 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».

8.5 Интеграция с антивирусными системами

В продукте 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.

8.6 Интеграция с ESIA

Для настройки авторизации в продукте с помощью ESIA (привязка учетных записей 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.

Для использования функциональности необходимо обратиться в техническую поддержку

8.6.1 Установка ESIA-Bridge

ESIA-Bridge устанавливается на выделенный виртуальный сервер с минимальной конфигурацией, представленной в таблице 33.

Таблица 33 — 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.

8.6.2 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 34.

Таблица 34 — 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 СО, на который будет устанавливаться сессионная cookie, то есть <domain_name>

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

8.6.3 Настройка продукта для интеграции с ESIA

Для подключения интеграции с ESIA со стороны продукта необходимо задать значения для переменных, указанных в таблице 35.

Таблица 35 — Настройка ESIA

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 36.

Таблица 36 — Настройка ESIA 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

9 ЗАМЕНА SSL-СЕРТИФИКАТА

9.1 Замена сертификата в компоненте CO

Замена сертификата в 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 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 ЛОГИРОВАНИЕ JAVA-СЕРВИСОВ

11.1 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 37.

Таблица 37 — 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

11.2 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 для 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.

12 ФУНКЦИЯ ОТПРАВКИ ОШИБОК

12.1 Установка и настройка Sentry

В продукте 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 38.

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

Таблица 38 — 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/wte/sentry.wfe.log.dsn	string	""	Отправка ошибок сервиса WFE в сервис Sentry
	config/wte/sentry.sso.log.dsn	string	""	Отправка ошибок сервиса SSO в сервис Sentry
	config/wte/chatbot.sentry.dsn	string	""	Отправка ошибок сервиса Chatbot в сервис Sentry
	config/wfe/routing/error.log.sentry.url	string	""	Hostname сервера Sentry, если сервер развернут в другом домене

Наименование сервиса	Наименование переменной	Тип переменной	Значение	Описание
	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.

12.2 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.

Ограничение доступа к журналу событий не позволит 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.

12.3 Сбор пользовательской аналитики

В продукте реализован сбор пользовательской аналитики, по умолчанию функция выключена. После включения сохраняет действия пользователя при работе с сервисами продукта. 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 39.

Таблица 39 — 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