Руководство по установке

Система редактирования и совместной работы (СО) МойОфис

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Система редактирования и совместной работы (СО) МойОфис»

РУКОВОДСТВО ПО УСТАНОВКЕ

2.1

На 60 листах

Москва

2022

Содержание

Перечень сокращений, терминов и определений

Перечень терминов и определений приведен в таблице 1.

Таблица 1 – Перечень сокращений, терминов и определений

Сокращение, термин	**Расшифровка и определение**
AD	Active Directory, Активный каталог
API	Application Programming Interface, интерфейс программирования приложений
Auth SSO	Single Sign-On, подсистема единого входа (аутентификации и авторизации)
CA	Certificate Authority, удостоверяющий центр для подтверждения подлинности ключей шифрования
CDN	Content Delivery Network, сеть доставки содержимого (в данном случае одна из ролей Auth SSO сервера)
CO	CloudOffice, Облачный Офис, общее название продукта, нейтральное с точки зрения бренда
CU	Converter Unit, сервис конвертирования разных форматов файлов
DCS	Document Collaboration Service, сервис редактирования и коллаборации документов на базе кода Core
DNS	Domain Name System, система доменных имён
DU	Document Unit, синоним DCS
EFK	Стек ПО для централизованного сбора и визуализации логов, ElasticSearch + Fluentd + Kibana
ESIA	ЕСИА, Единая Система Идентификации и Аутентификации, информационная система в РФ, обеспечивающая санкционированный доступ участников информационного взаимодействия (граждан-заявителей и должностных лиц органов исполнительной власти) к информации, содержащейся в государственных и иных информационных системах
ETCD	Распределенная система хранения конфигурации
FCM	Firebase Cloud Messaging, сервис нотификаций мобильных приложений Google, ранее назывался GCM
FS	Общее название для сервисов FileStorage, Хранилища, а также протоколов доступа к нему. Смотри также PGS
FQDN	Fully Qualified Domain Name, полностью определённое имя домена
GCM	Google Cloud Messaging, сервис нотификаций мобильных приложений Google, заменен сервисом FCM
HMS	Huawei Mobile Services, сервис нотификаций мобильных приложений Huawei
Inventory file	Инвентарный файл Ansible с перечислением ролей и их IP адресов
IPVS	IP Virtual Server

Сокращение, термин	Расшифровка и определение
JKS	Java Key Store, хранилище ключей и сертификатов, доступных виртуальной машине Java
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
Landing	Стартовая страница
LDAP	Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам
LO	LibreOffice, фильтры которого используются для импортирования устаревших бинарных форматов документов
NPS	Native Process Service, сервис управления нативными процессами (например, конвертацией)
PGS	Pythagoras, сервисы файлового хранилища, работающие по протоколам FS (Web API, App API, Card API)
PSN	Poseidon, приложение почты, календаря и контактов
Quick launch	Меню быстрого запуска
SMTP	Simple Mail Transfer Protocol, протокол передачи почтовых сообщений
SSH	Secure Shell, «безопасная оболочка»
UI	User Interface, пользовательский интерфейс
URL	Uniform Resource Locator, единый указатель ресурса
UX	User Experience, «опыт пользователя»
VIP	Виртуальный IP адрес, балансировка которого осуществляется через IPVS
Бандл, bundle	Пакет обновлений CDN
Воркер, worker	Процесс-обработчик
Плейбук, playbook	Сборник скриптов (сценариев) Ansible

1. Общие сведения

1.1. Назначение

1.2. Требования к квалификации персонала

Администратор Системы должен соответствовать следующим требованиям:

- основы сетевого администрирования:
  - о сетевая модель OSI и стек протоколов TCP/IP;
  - IP-адресация и маски подсети;
  - маршрутизация: статическая и динамическая;
  - протокол обеспечения отказоустойчивости шлюза (VRRP);
- опыт работы с подсистемой виртуализации на уровне эксперта:
  - установка Docker;
  - запуск / остановка / перезапуск контейнеров;
  - работа с реестром контейнеров;
  - работа с VMWare vSphere ESXi 6.5 и выше;
  - получение конфигурации контейнеров;
  - сеть в Docker, взаимодействие приложений в контейнерах;
  - решение проблем контейнерной виртуализации;
- опыт работы с командной строкой ОС Linux:
  - знания в объеме курсов Red Hat RH124, RH134, RH254;
  - знания в объеме, достаточном для сдачи сертификационного экзамена Red Hat EX300;
- опыт работы со службой доменных имен (DNS):
  - знание основных терминов (DNS, IP-адрес и так далее);
  - понимание принципов работы DNS (корневые серверы, TLD-серверы, серверы имен доменов, разрешающий сервер имен и так далее);
  - знание типов записи и запросов DNS;
- знание видов архитектуры, а также основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:
  - закрытый и открытый ключи;
  - сертификат открытого ключа;
  - регистрационный центр (RA);
  - сертификационный центр (CA);
  - хранилище сертификатов (CR);
- практический опыт администрирования на уровне эксперта:
  - Redis;
  - ETCD;
  - RabbitMQ.
  - Elasticsearch.

- опыт работы с системой автоматизации развёртывания Ansible;

1.3. Системные требования

Базовый продукт / дистрибутив	Аппаратные требования	Программные требования
минимальные	рекомендуемые	
Система редактирования и совместной работы (СО) МойОфис, серверная часть	Дистрибутив СО	Отдельный сервер или виртуальная машина: * Intel Xeon E3 CPU или выше (4 vCPU в случае виртуальной машины) * Скорость сетевой подсистемы — 1Gbit/s * 16Gb RAM * 250Gb HDD * Число sequential IOPS должно быть не ниже 50 (standalone), не ниже 100 (cluster). Сброс данных на диск через fsync должен укладываться в 10ms. Для нагруженного кластера рекомендуются NVMe диски. * Запуск docker storage на файловой системе **XFS** с флагом `ftype=1`.

Для обеспечения функциональности клиентского доступа экземпляр «Система редактирования и совместной работы (СО) МойОфис» должен быть доступен с пропускной способностью не ниже 1 МБ/с по следующим TCP портам: 143, 993, 80, 443, 25, 587

1.4. Ограничения

1.4.1. Ограничения при выполнении установки на оборудовании без поддержки отказоустойчивости

Режим и последующая настройка параметров на оборудовании без поддержки отказоустойчивости предоставляется в целях демонстрации функциональности «{comm_component}». **Данный режим не поддерживается, не рекомендуется его использовать.**

В данном режиме все роли устанавливаются на один физический или виртуальный сервер.

1.4.2. Ограничение при выполнении кластерной установки

Не желательно (допустимо в целях экономии ресурсов, но за счет ухудшения отказоустойчивости) совмещать серверные роли между собой. Каждый физический или виртуальный сервер должен содержать только одну серверную роль.

1.4.3. Ограничение по работе с подсистемой управления конфигурациями

В подсистеме управления конфигурациями не должно быть конфигурационных файлов самой подсистемы. В том числе конфигурационного файла, который по умолчанию устанавливается с пакетом (например, /etc/ansible/ansible.cfg). Такой файл требуется удалить либо перезаписать образцом из поставляемого ПО. Подробнее смотри в https://docs.ansible.com/ansible/latest/reference_appendices/config.html#theconfiguration-file

1.4.4. Ограничение по работе с системами виртуализации

Следующие системы виртуализации поддерживаются для обеспечения работы «{comm_component}»:

- HyperV.
- VMWare.
- KVM.

1.5. Рекомендации

1.5.1. Рекомендации по использованию файловых систем

В соответствии с рекомендациями производителей операционных систем рекомендуется:

- для CentOS и RedHat – использовать файловую систему xfs с флагом `ftype=1`.
- для AltLinux и AstraLinux – использовать файловую систему ext4.

1.5.2. Рекомендации по версии ядра Linux

- Требуется ядро mainline (обновляется по умолчанию, если не передан флаг `UPGRADE_KERNEL=false`) С более старыми версиями ядер (lts) работоспособность не гарантируется из-за особенностей Docker (требуется полная поддержка cgroup2 в ядре).

1.5.3. Рекомендации по разбивке дисков

Разбивку дисков рекомендуется выполнять следующим образом:

- для серверов всех ролей, кроме `log` — не менее 20 Гб для штатной работы ОС;
- для сервера роли `log` — не менее 100 Гб для штатной работы ОС и хранения всех логов;

1.5.4. Рекомендуемая версия python

```
3.6+
```

1.5.5. Рекомендуемые зависимости python

Зависимости присутствуют в файле `requirements.txt` Для установки данных зависимостей из файла необходимо выполнить команду:

```
pip3 install -r ~/install_co/requirements.txt
```

2. Описание архитектуры Система редактирования и совместной работы (СО) МойОфис

2.1. Общая архитектурная схема

Общая архитектурная схема «Система редактирования и совместной работы (СО) МойОфис» приведена на Рисунке 1.

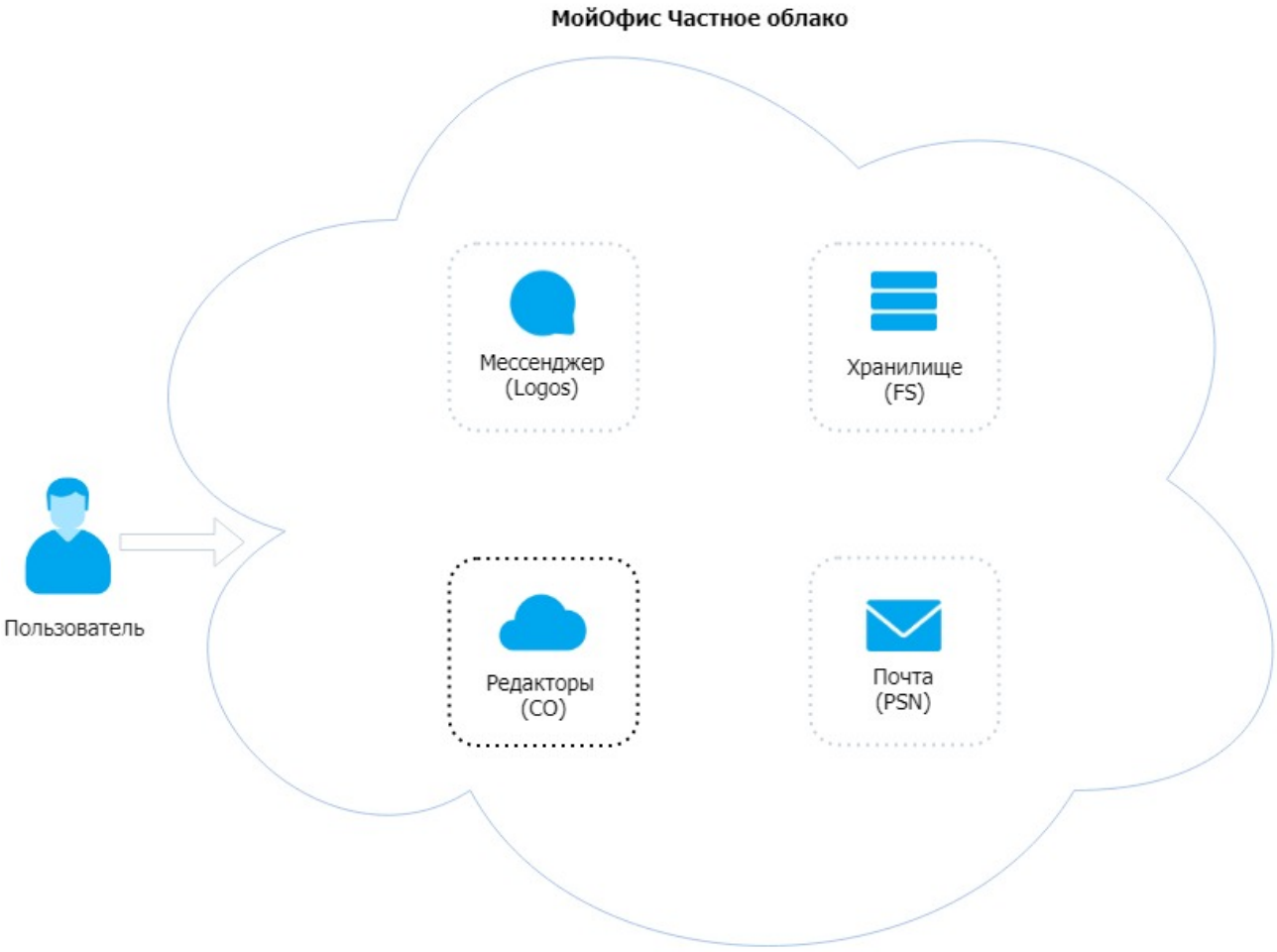

Рисунок 1 – Общая архитектурная схема «Система редактирования и совместной работы (СО) МойОфис»

2.2. Детальная архитектурная схема «{comm_component}»

Данная схема «{comm_component}» приведена на Рисунке 2.

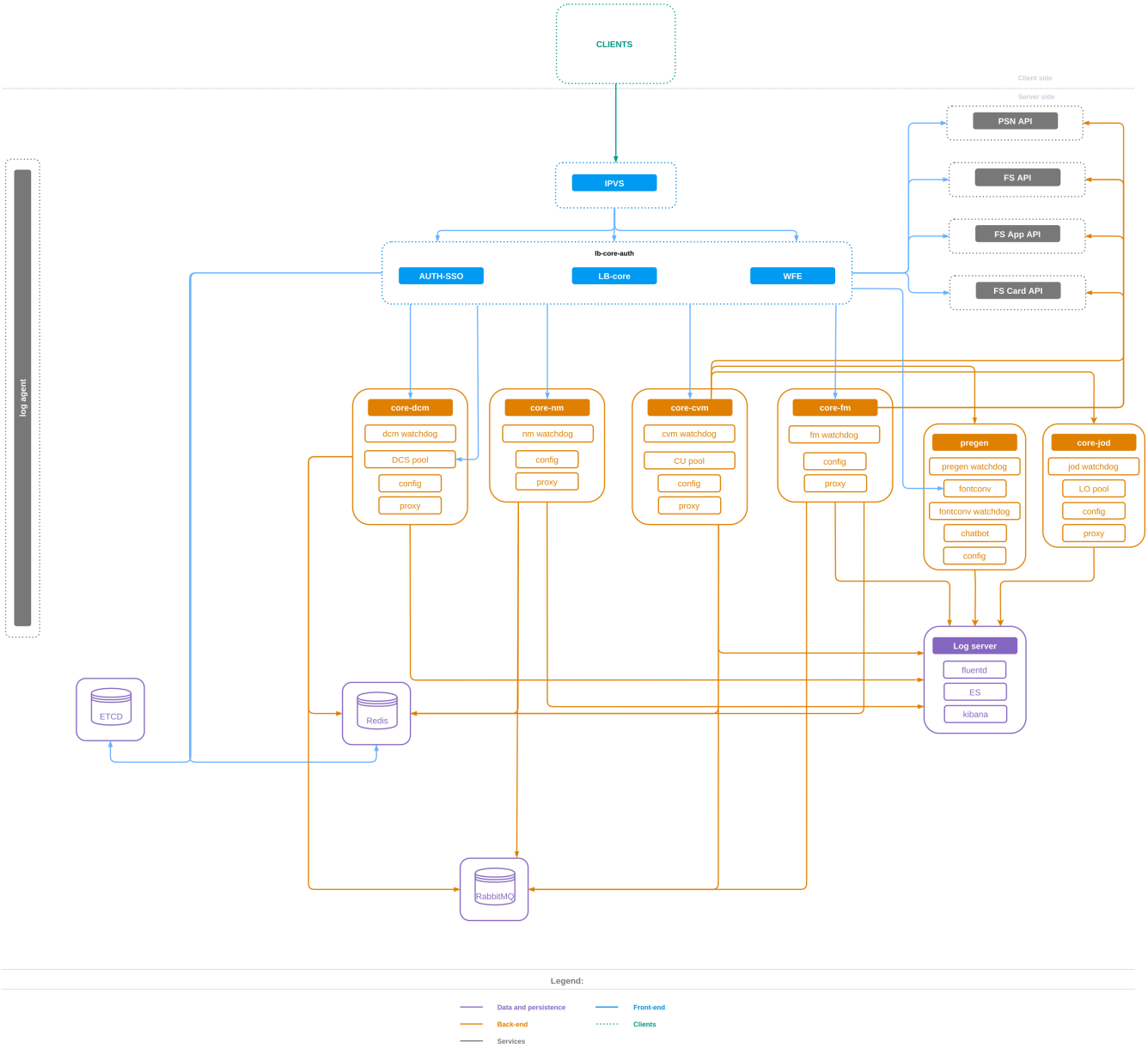

Рисунок 2 – Детальная архитектурная схема «{comm_component}»

3. Типовые схемы установки «Система редактирования и совместной работы (СО) МойОфис»

3.1. Конфигурация без отказоустойчивости

В данной конфигурации все роли устанавливаются на один виртуальный сервер, на несколько виртуальных серверов в рамках одного физического сервера, или на несколько виртуальных серверов при количестве хостов в каждой роли, не превышающим 1 (кроме роли log). Такая конфигурация может использоваться в целях разработки или демонстрации возможностей продукта (virtual appliance).

3.2. Кластерная отказоустойчивая конфигурация

В данной конфигурации все роли (при количестве хостов более 1 в каждой роли, кроме `log`), устанавливаются на разные виртуальные сервера, а также, по возможности, разносятся на разные физические сервера или гипервизоры.

3.3. Типовая схема масштабирования

Для односерверной (не кластерной) конфигурации возможно только вертикальное масштабирование. При этом следует учитывать ограничения Docker и других системных сервисов. Переход от такой конфигурации к кластерной возможен только путем полной переустановки «Система редактирования и совместной работы (СО) МойОфис».

Полноценное масштабирование возможно только для кластерной отказоустойчивой конфигурации. Масштабированию в первую очередь следует подвергать узлы кластера с ролями `dcm` (влияет на количество одновременно открытых документов), `cvm` и `pregen` (влияет на количество конвертаций, скорости загрузки, скачивания, печати документов). После добавления необходимых ресурсов следует:

- Подготовить сервер(а) в соответствии с разделом 5.2.
- Запустить деплой в соответствии с разделом 9.2.2
- Произвести проверку инсталляции в соответствии с разделом 9.2.3

4. Первичная установка

4.1. Состав дистрибутива

В состав дистрибутива входит программное обеспечение «{comm_component}». Дистрибутив предствляет собой tgz архив, содержащий:

- Ansible плейбуки для развёртывания ролей.
- Архив образа docker registry.
- Архивы docker образов для каждого из сервисов, входящих в состав продукта.
- Руководство по установке «{comm_component}».

5. Подготовка к установке

5.1. Описание ролей

Таблица 2 – Описание ролей ansible, входящих в состав пакета установки.

Наименование роли	**Расшифровка и определение**	**Примечание**
auth	Развёртывание сервиса SSO и внешней балансировки (openresty-lb-core-auth) в Docker.	
boostrap	Подготовка хоста. Установка необходимых системных пакетов. Установка и настройка ядра Linux. Общая часть функционала очистки системы (при `-e CLEANUP=true`).	Общая роль.
bundles-upload	Загрузка пакетов обновления CDN (бандлов).	Выполняется только во время деплоя.
chatbot	Развёртывание сервиса Chatbot (интеграции с мессенджерами).	
common	Создание необходимых директорий, генерация сертификатов.	Общая роль.
config	Заполнение общих настроек в Etcd, развёртывание сервиса confd.	Общая роль.
core-cvm	Развёртывание сервисов CVM/JOD/NPS в Docker. Запуск пула CU.	
core-dcm	Развёртывание сервиса DCM в Docker. Запуск пула DU.	
core-fm	Развёртывание сервиса FM в Docker.	
core-jod	Развёртывание сервиса JOD в Docker. Запуск пула LO.	
core-nm	Развёртывание сервиса NM в Docker.	
docker	Установка сервиса Docker.	Общая роль.
etcd	Развёртывание сервиса etcd в Docker.	Общая роль.

Наименование роли	Расшифровка и определение	Примечание
fluentd-agent	Развёртывание сервиса Fluentd в Docker.	Общая роль.
haproxy	Развёртывание сервиса внутренней балансировки (haproxy) в Docker.	Общая роль.
imc	Развёртывание узла или кластера Redis в Docker.	
imc-sen	Развёртывание узла или кластера Redis Sentinel в Docker.	
log	Развёртывание стека EFK (ElasticSearch, Fluentd, Kibana).	Опционально. Возможно логирование с использованием journald и локальных лог файлов.
lsyncd	Установка сервиса синхронизации CDN между узлами кластера (lsyncd).	Общая роль.
mq	Развёртывание узла или кластера RabbitMQ в Docker.	
nginx-gost	Развёртывание сервиса проксирования и приёма TLS соединений с поддержкой ГОСТ шифрования.	Опционально. Совмещается с ролью `lb_core_auth`.
pregen	Развёртывание сервиса pregen в Docker.	
registry	Развёртывание сервиса docker registry в Docker и импорт образов docker из архива.	Выполняется только на месте оператора.
service	Развёртывание etcd-browser в Docker.	

5.2. Подготовка инфраструктуры установки

Во избежание проблем не рекомендуется использовать системы, на которых ранее были проведены инсталляции программного обеспечения, не относящегося к дистрибутиву «{comm_component}».

В случае возникновения проблем во время деплоя рекомендуется установка на "чистую" систему или использование параметра деплоя `-e CLEANUP=true` (`-e CLEANUP_ES=true` в случае проблем с Elastic Search).

Используемая файловая система под docker контейнеры, должна официально поддерживаться текущей версией docker. Если используется XFS, то файловая система должна быть создана с опцией `-n ftype=1` (вариант по умолчанию в рекоменованных ОС).

На все хосты, выделенные под инсталляцию «Система редактирования и совместной работы (СО) МойОфис», включая место оператора, необходимо инсталлировать минимальный серверный вариант операционной системы одной из рекомендованных версий:

- CentOS
  - Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, https://mirror.yandex.ru/centos/7.9.2009/isos/x86_64/CentOS-7-x86_64-Minimal-2009.iso
  - Произвести установку в минимальном варианте.
- Astra Linux

- Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, https://mirror.yandex.ru/astra/current/orel/iso/orel-2.12.40-25.12.2020_14.45.iso
- Произвести установку в минимальном варианте.

- Alt Linux
  - Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, https://mirror.yandex.ru/altlinux/p9/images/server/x86_64/alt-server-9.1-x86_64.iso
  - Произвести установку в минимальном варианте.

С места оператора установки должен быть возможен доступ на все хосты кластера под пользователем root или другим пользователем с sudo привилегиями `(ALL=(ALL) NOPASSWD: ALL)`.

На месте оператора установки должен быть также инсталлированы:

- Пакет Ansible версии не ниже 4.3.0. (по инструкции https://docs.ansible.com/ansible/latest/installation_guide/intro_installation.html). Работа с более новыми версиями Ansible возможна, но не гарантирована.
- Пакет Python 3.6 или выше.
- Пакет jinja2 версии 2.10+ для соответствующей версии Python (для CentOS пакет python-jinja2 можно обновить с любого репозитория OpenStack, например http://mirror.centos.org/centos/7/cloud/x86_64/openstack-queens).

5.2.1. Проверка и подготовка инсталляционных архивов

При выполнении проверки и подготовки инсталляционных архивов необходимо выполнить следующие действия:

В имени архива цифры версии коммерческого релиза представлены знаками X.

1. После копирования инсталляционного архива необходимо проверить его контрольную сумму Sha256. Для этого необходимо скопировать в файл (например, `checksum.sha256`) контрольную сумму, переданную вместе с дистрибутивом, и запустить следующую команду:

```
sha256sum -c <<< \
"$(cat checksum.sha256) MyOffice_CO_XXXX.XX.XX.tgz"
```

2. Распаковать содержимое инсталляционного архива в произвольную директорию, например `~/install_co/`, и перейти в эту директорию:

```
mkdir -p ~/install_co/
tar xzf "MyOffice_CO_XXXX.XX.XX.tgz" -C ~/install_co/
cd ~/install_co/
```

5.3. Общие настройки системы

1. Настроить имя хоста, параметры сети.
2. Настроить имя хоста, параметры сети, включая специальные требования для входного IPVS балансировщика:
   - На lo интерфейсе всех серверов (узлов кластера) с ролью `[lb_core_auth]` создать альяс с `ip = REAL_IP/32`. В общем случае это внешний IP-адрес балансировщика IPVS, и перед инсталяцией его

следует уточнить у администраторов PGS. Этот пункт разрешит нодам принимать пакеты, которые приходят с `dst.address = REAL_IP`.

- Процесс развертывания автоматически добавит на эти же узлы следующие параметры в `sysctl.conf` и выполнит их применение через `sysctl -p`, что запретит нодам отвечать на ARP запросы про адреса, настроенные для loopback интерфейса:

```
net.ipv4.conf.all.arp_ignore = 1
net.ipv4.conf.all.arp_announce = 2
```

2. На узлах с ролью `[lb_core_auth]` сконфигурировать внешний DNS. Убедиться, что ресолвятся и доступны:
   - **SMTP** сервер (`smtp[-<DOMAIN_ENV>].<DOMAIN_NAME>` в PSN, или другой, используемый в настройках формы обратной связи в свойствах тенанта).
   - **FS API** (`fsapi[-<DOMAIN_ENV>].<DOMAIN_NAME>`, или другой, указанный в параметре `FS_API_URL`).
   - **FS App API** (`appapi[-<DOMAIN_ENV>].<DOMAIN_NAME>`, или другой, указанный в параметре `FS_APP_URL`).
   - **FS Card API** (`cardapi[-<DOMAIN_ENV>].<DOMAIN_NAME>`, или другой, указанный в параметре `FS_CARD_URL`).
   - **PSN API** (`mail[-<DOMAIN_ENV>].<DOMAIN_NAME>`, или другой, указанный в параметре `MAIL_BASE_URL`).
3. Создать записи в DNS:
   - `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `A`, содержит внешний `REAL_IP` адрес входного **IPVS** балансировщика.
   - `cdn[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `CNAME`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`
   - `coapi[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `CNAME`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`
   - `docs[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `CNAME`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`
   - `files[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `CNAME`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`
   - `links[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `CNAME`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>`
   - `_https._tcp[.<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `SRV`, значение `auth[-<DOMAIN_ENV>].<DOMAIN_NAME>` - опционально, для мобильных клиентов

Изменение префиксов и параметры инсталляции `DOMAIN_ENV`, `DOMAIN_NAME` описаны далее.

5.4. Настройки системы в "закрытом периметре"

В случае установки «Система редактирования и совместной работы (СО) МойОфис» в "закрытом периметре", то есть в локальной сети, не имеющей прямого выхода в Интернет, на всех хостах, включая место оператора, необходимо обеспечить доступность зеркал следующих yum репозиториев:

- http://mirror.centos.org/centos/7/os/x86_64/
- http://mirror.centos.org/centos/7/extras/x86_64/

- http://mirror.centos.org/centos/7/updates/x86_64/
- http://download.fedoraproject.org/pub/epel/7/x86_64/
- https://download.docker.com/linux/centos/7/x86_64/stable/

Поддержка "закрытого периметра" находится в экспериментальном состоянии!

5.5. Настройка основных параметров установки

5.5.1. Расположение примеров конфигурационных файлов

Тип деплоя	Путь к инвентарному файлу	Путь к файлу параметров
Односерверный режим	`~/install_co/inventory/standalone`	`~/install_co/properties/standalone.yml`
Кластерный высокодоступный режим	`~/install_co/inventory/cluster`	`~/install_co/properties/cluster.yml`

5.5.2. Конфигурирование инвентарного файла

Инвентарный файл (inventory file) содержит логические группы (роли), на которые должен быть поделен кластер. Роли могут совмещаться, то есть на одном и том же сервере (виртуальной машине) может быть развернуто несколько ролей, работающих одновременно.

Для конфигурирования инвентарного файла необходимо открыть пример инвентарного файла в текстовом редакторе и заменить все IP-адреса на внутренние адреса кластера. При необходимости возможно добавить или удалить сервера в группах.

5.5.3. Конфигурирование параметров инсталляции

Для конфигурирования обязательных и опциональных параметров инсталляции необходимо открыть файл-пример параметров в текстовом редакторе и произвести настройки:

На текущий момент поддерживается задание в URL имени хоста или IP-адреса PGS, который должен быть разрешим DNS и доступен со всех узлов CO. Прописывание хоста PGS в `/etc/hosts` **не достаточно**, так как Nginx не имеет возможности прочесть адрес оттуда.

- `DOMAIN_NAME` — необходимо раскомментировать строку и изменить значение параметра на требуемый, например `DOMAIN_NAME: "example.com"`.
- `FS_API_URL` — HTTP URL доступа к FS WebAPI. Необходимо раскомментировать строку и изменить значение параметра на требуемое при инсталляции PGS.
- `FS_APP_URL` — HTTP URL доступа к FS AppAPI. Необходимо раскомментировать строку и изменить значение параметра на требуемое при инсталляции PGS.
- `FS_CARD_URL` — HTTP URL доступа к FS CardAPI (бывший MailAPI). Необходимо раскомментировать строку и изменить значение параметра на требуемое при инсталляции PGS.

Для этих параметров поддерживаются схемы http и https. Для повышения безопасности рекомендуется использовать защищенный вариант (https), либо гарантировать сетевое соединение между CO и PGS в доверенной внутренней подсети при выборе схемы http.

- `FS_APP_LOGIN` — необходимо раскомментировать строку и задать логин пользователя FS AppAPI (заранее созданный при деплое PGS в переменной инвентори `APP_ADMIN_LOGIN`).

- DOMAIN_ENV — опционально раскомментировать строку и изменить значение параметра на требуемый, например, "99-9"; при этом все записи в DNS для CO необходимо будет скорректировать по форме <префикс>-<DOMAIN_ENV>.<DOMAIN_NAME>, например auth-99-9.example.com; почта по умолчанию будет использовать домен @<DOMAIN_ENV>.<DOMAIN_NAME>, например @99-9.example.com.
- HMS_ENABLED — опционально добавить в файл с примерами параметров или передать как дополнительный параметр в командной строке. Значение true означает включение работы с нотификациями через HMS (Huawei Mobile Services), при этом должны быть заполнены остальные параметры HMS. Значение false или пустое значение — выключает эту возможность.

Описание возможных дополнительных параметров приведено в Таблице 1 в Приложении 1.

5.5.4. Конфигурирование приватных параметров

Для конфигурирования приватных параметров необходимо скопировать шаблонный файл параметров плейбуков:

```
cp ~/install_co/group_vars/all/.private.yml
~/install_co/group_vars/all/private.yml
```

Далее необходимо открыть файл ~/install_co/group_vars/all/private.yml в текстовом редакторе, и заполнить обязательные и опциональные настройки.

Обязательными настройками являются:

- Группа Auth encryption settings
- Группа Chatbot properties (при интеграции редакторов с мессенджером Dialog).
- Группа Common encryption settings
- Группа FS App settings
- Группа FS App encryption settings
- Группа Mobile notifications (в случае использования сервисов нотификации Google или Huawei).
- Параметр FS_TOKEN_SALT_EXT
- Параметр ERLANG_COOKIE
- Параметр CRYPTO_PRO_LICENSE (в случае использования дистрибутива с поддержкой ГОСТ шифрования, и наличии лицензии "КриптоПро CSP")

Для поддержки функциональности системных писем-нотификаций от PGS и CO необходимо после завершения их инсталляции настроить параметры SMTP, убедившись, что FS AppAPI работает корректно. По умолчанию параметры SMTP **не заданы**.

Описание возможных дополнительных параметров приведено в Таблице 1 в Приложении 1.

5.5.5. Конфигурирование авторизации для системных сервисов

Настройки авторизации находятся файле ~/install_co/group_vars/all/private.yml:

Имя	Значение
CO_MANAGE_API_USERNAME	Имя пользователя для доступа к CO Manage API

Имя	Значение
CO_MANAGE_API_PASSWORD	Пароль пользователя для доступа к CO Manage API
ERLANG_COOKIE	уникальная строка (секрет) для кластеризации RabbitMQ
ETCD_BROWSER_USERNAME	имя пользователя для Etcd Browser
ETCD_BROWSER_PASSWORD	пароль для Etcd Browser
HAPROXY_USERNAME	имя пользователя для страниц статистики HAProxy
HAPROXY_PASSWORD	пароль для страниц статистики HAProxy
KIBANA_USERNAME	имя пользователя для Kibana
KIBANA_PASSWORD	пароль пользователя для Kibana в открытом виде
PRIVATE_REGISTRY_USERNAME	имя пользователя для Docker Registry
PRIVATE_REGISTRY_PASSWORD	пароль для Docker Registry в открытом виде, необходим для использования в скриптах
RABBITMQ_USERNAME	имя пользователя для RabbitMQ
RABBITMQ_PASSWORD	пароль для RabbitMQ
REDIS_PASSWORD	пароль для Redis команды AUTH

Следующие пароли будут созданы автоматически, если не указаны в конфигурации в `~/install_co/group_vars/all/private.yml`:

- `ETCD_BROWSER_PASSWORD`
- `HAPROXY_PASSWORD`
- `RABBITMQ_PASSWORD`
- `REDIS_PASSWORD`

Их значения будут выведены в лог деплоя, а также попадут в файл `/opt/co/systemd/systemd-env`. В этом файле можно посмотреть текущие пароли для сервисов в открытом виде.

5.5.6. Конфигурирование сертификатов

Раздел обязателен для релизов без поддержки ГОСТ шифрования или с флагом `GOST_ENABLED=false`!

Для конфигурирования сертификатов в директории `~/install_co/certificates` необходимо создать директорию, соответствующую сконфигурированному имени домена `<DOMAIN_NAME>`, содержащую файлы в формате **PEM**:

- `server.crt` — содержит SSL-сертификат на `*.<DOMAIN_NAME>` и все промежуточные сертификаты, кроме корневого доверенного, расположенные в указанном порядке (как описано в http://nginx.org/en/docs/http/ngx_http_ssl_module.html#ssl_certificate).
- `server.nopass.key` — приватный ключ сертификата, не требующий кодовой фразы.
- `ca.crt` — все доверенные SSL сертификаты.

По умолчанию этот файл представляет собой ссылку на файл корневых сертификатов, установленных в системе. При необходимости изменений файла `ca.crt`, использовать символические ссылки на внешние файлы не допустимо, так как они не будут доступны внутри Docker контейнера!

- `dhparams.pem` — параметры алгоритма DH обмена ключами. Данный файл возможно сгенерировать командой `openssl dhparam -out dhparams.pem 2048`.

Использование самоподписанных сертификатов крайне нежелательно с точки зрения безопасности. Данный способ может использоваться только при инсталляции в ознакомительных целях.

5.5.7. Конфигурирование ГОСТ сертификатов

Только для релизов с поддержкой ГОСТ шифрования и включенным флагом `GOST_ENABLED=true`! При этом предыдущий раздел выполнять не нужно!

Поддержка ГОСТ шифрования осуществляется при помощи программного обеспечения "КриптоПро CSP". Для полноценной работы необходимо приобретение серверной лицензии "КриптоПро CSP". По умолчанию, при отсутствии лицензии, время работы ограничено.

После успешной настройки сертификатов появляется поддержка шифрования каналов связи с клиентскими приложениями в соответствии со стандартом ГОСТ 34.10-2018 (описан в https://ru.wikipedia.org/wiki/%D0%93%D0%9E%D0%A1%D0%A2_34.10-2018). При этом сохраняется режим совместимости с клиентами, не поддерживающими ГОСТ шифрование.

Для конфигурирования ГОСТ сертификатов в директории `~/install_co/certificates/gost` необходимо создать директорию, соответствующую сконфигурированному имени домена `<DOMAIN_NAME>`, содержащую файлы в формате **PFX**:

- `certkey-gost.pfx` — содержит ГОСТ 34.10-2018 сертификат и приватный ключ (без кодовой фразы) на `*.<DOMAIN_NAME>`, обязательный файл.
- `certkey-rsa.pfx` — содержит RSA сертификат и приватный ключ (без кодовой фразы) на `*.<DOMAIN_NAME>`, обязательный файл.
- `roots-gost.pfx` — содержит все дополнительные доверенные и промежуточные ГОСТ 34.10-2018 сертификаты, опционально.
- `roots-rsa.pfx` — содержит все дополнительные доверенные и промежуточные RSA сертификаты, опционально.

Использование самоподписанных сертификатов или сертификатов тестового УЦ нежелательно с точки зрения безопасности. Данный способ может использоваться только при инсталляции в ознакомительных целях.

5.5.8. Настройка ключей шифрования

В целях безопасности в дистрибутиве отсутствуют какие-либо ключи шифрования по умолчанию.

FS_APP_PASSWORD

Пароль PGS пользователя FS AppAPI. Это же значение указывается в конфигурации инсталляции PGS в переменной инвентори `APP_ADMIN_PASSWORD`.

FS_APP_ENCRYPTION_KEY

FS_APP_ENCRYPTION_IV

FS_APP_ENCRYPTION_SALT

Секретный ключ, вектор инициализации и соль для данных алгоритма **AES-256-CBC**, используемого для шифрования секретных данных тенантов, переданных через FS App API и сохраненных в Etcd (ключ сертификата, пароль SMTP). После деплоя они не хранятся в Etcd, а помещаются в файл `/opt/co/wfe/properties/auth_config.props` на узлах с ролью `[lb_core_auth]`. **Эти значения должны быть заданы одинаковыми вместе с PGS.** Для их генерации можно использовать следующий вызов:

```
openssl enc -aes-256-cbc -k "<password phrase>" -P -md sha256
```

AUTH_ENCRYPTION_KEY

AUTH_ENCRYPTION_IV

AUTH_ENCRYPTION_SALT

Секретный ключ, вектор инициализации и соль для данных алгоритма **AES-256-CBC**, используемого для шифрования mail_session токена. **Эти значения должны быть заданы одинаковыми вместе с PGS.** Для их генерации можно использовать следующий вызов:

```
openssl enc -aes-256-cbc -k "<password phrase>" -P -md sha256
```

FS_TOKEN_SALT_EXT

Соль дайджеста токена из инвентори PGS, значение переменной `FS_TOKEN_SALT_EXT`. В SSO используется для авторизации пользователей из LDAP или ESIA. Задается произвольной строкой символов из набора Latin1, чувствительна к регистру. **Это значение должны быть задано одинаковым вместе с PGS.**

5.6. Настройка дополнительных параметров установки

5.6.1. Добавление доверенных сертификатов

В случае использования в окружении самоподписанных сертификатов или собственного центра сертификации (CA), необходимо добавить такие сертификаты в список доверенных для ролей `[core_*]` и `[lb_core_auth]`.

Перед началом деплоя необходимо положить CA (и другие доверенные) сертификаты в формате **PEM** в директорию `certificates/custom-ca/` в плейбуках. Во время деплоя эти сертификаты будут автоматически добавлены в `ca.crt` файл для `[lb_core_auth]` роли.

Для Java сервисов требуется добавить CA сертификаты в Java KeyStore (далее JKS). Процесс добавления происходит автоматически внутри контейнера. При старте контейнера, все сертификаты, обнаруженные в `/opt/co/ssl/custom-ca/`, будут добавлены в JKS с помощью утилиты `keytool`. Чтобы JKS сохранялся при перезапуске Docker контейнера, он подключается (маппится) из внешней файловой системы и находится в `/opt/co/ssl/custom-ca/java/cacerts`.

Существует возможность использовать свой **JKS**. Его следует поместить в директорию `certificates/custom-ca/java/` под именем `cacerts`. Однако, лучше использовать сертификаты в формате PEM.

JKS с измененным паролем (то есть не "changeit", как по умолчанию в JRE) на данный момент не поддерживаются.

Для активации механизма добавления доверенных сертификатов необходимо запустить плейбуки с параметром `-e CUSTOM_CA=true`.

Статус импорта сертификатов можно посмотреть командой:

```
journalctl -u <имя_юнита>
```

5.6.2. Конфигурирование интеграции с ESIA с помощью ESIA-Bridge

Данный подраздел опционален.

Применяется только при необходимости интеграции Auth/SSO с авторизацией через ЕСИА (привязкой аккаунтов PGS к учетным записям ЕСИА).

В этом варианте интеграции используется программный продукт ESIA-Bridge от ООО «РЕАК СОФТ». При использовании ESIA-Bridge настройки интеграции с ЕСИА общие для всех тенантов CO!

ESIA-Bridge устанавливается на выделенный виртуальный сервер с минимальной конфигурацией — 2 vCpu (Intel), 4 GB RAM, 20 Gb HDD. Работа ESIA-Bridge на сервере поддерживается для операционных систем Debian / CentOS / RHEL или Windows. В данной инструкции рассматривается установка и настройка ESIA-Bridge в Linux.

Установка ESIA-Bridge должна быть произведена в соответствии с инструкцией https://identityblitz.ru/products/esia-bridge/documentation/ Дистрибутив ESIA-Bridge поставляется в виде самораспаковывающегося bin-файла. Для установки необходимо выполнить команду:

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

По результатам успешной установки ESIA-Bridge создаются следующие директории:

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

Конфигурация ESIA-Bridge по умолчанию располагается в файле `/usr/share/esia-bridge/conf/esia-bridge.conf`.

Пример FQDN, на котором будет располагаться ESIA-Bridge: `esia-bridge.<DOMAIN_NAME>`, эта запись должна быть создана в публично доступном DNS. Домен ESIA-Bridge должен совпадать с доменом CO, в противном случае установить сессионную cookie не получится.

Конвертирование ГОСТ сертификата

Конвертирование ГОСТ сертификата системы, подключаемой к ЕСИА, из формата PFX контейнера КриптоПро в формат BKS, поддерживаемый ESIA-Bridge, осуществляется сторонними утилитами (смотри также 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 имеющегося там файла.

В конфигурацию ESIA-Bridge должны быть внесены следующие изменения:

- `domain="esia-bridge.<DOMAIN_NAME>:9000"`, при этом порт 9000 должен быть открыт в настройках сетевого экрана сервера ESIA-Bridge.
- `esia.host` – домен среды ЕСИА, 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 ЕСИА.
- `name` — имя вызывающей системы в ЕСИА.
- `cookieDomain` — домен СО, на который будет устанавливаться сессионная cookie, то есть `<DOMAIN_NAME>`

После изменения настроек ESIA-Bridge, сервис должен быть перезапущен командой `systemctl restart esia-bridge`.

Для конфигурирования интеграции с ЕСИА со стороны СО необходимо открыть файл `~/install_co/group_vars/all/private.yml` (смотри также 5.4) в текстовом редакторе и произвести следующие настройки:

- `ESIA_BRIDGE_ENTRANCE_URI` — точка входа в ESIA-Bridge со стороны СО, например `http://esia-bridge.example.com:9000/blitz/bridge/entrance`
- `ESIA_BRIDGE_USER_URI` — адрес, по которому СО запрашивает данные об авторизованном в ЕСИА пользователе, например `http://esia-bridge.example.com:9000/blitz/bridge/user`

Для конфигурирования интеграции с ЕСИА со стороны PGS необходимо произвести дополнительные настройки тенанта в разделе ЕСИА таким образом, чтобы в настройках тенанта в Etcd появились следующие параметры:

```
"properties": {
  "esia": {
    "can_esia_auth":1,
    "support_esia_auth":1
  },
  ...
}
```

Запрос к PGS API, который необходимо для этого выполнить, приведен в инструкции по деплою PGS.

5.6.3. Конфигурирование встроенной интеграции с ESIA

Встроенная интеграция с ЕСИА на данный момент не поддерживается, следует использовать ESIA-Bridge.

Данный подраздел опционален.

Применяется только при необходимости интеграции Auth/SSO с авторизацией через ЕСИА (привязкой аккаунтов PGS к учетным записям ЕСИА).

Для конфигурирования интеграции с ЕСИА необходимо открыть файл `~/install_co/group_vars/all/private.yml` (смотри также 5.4) в текстовом редакторе и произвести следующие настройки:

- `ESIA_TEST_AC_URL` — адрес получения access code в тестовой среде ЕСИА, например `https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac`.
- `ESIA_TEST_TE_URL` — адрес token exchange в тестовой среде ЕСИА, например `https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te`.
- `ESIA_TEST_RS_URL` — адрес resource server в тестовой среде ЕСИА, например `https://esia-portal1.test.gosuslugi.ru/rs`.
- `ESIA_PROD_AC_URL` — адрес получения access code в продуктивной среде ЕСИА, например `https://esia.gosuslugi.ru/aas/oauth2/ac`.
- `ESIA_PROD_TE_URL` — адрес token exchange в продуктивной среде ЕСИА, например `https://esia.gosuslugi.ru/aas/oauth2/te`.
- `ESIA_PROD_RS_URL` — адрес resource server в продуктивной среде ЕСИА, например `https://esia.gosuslugi.ru/rs`.

Для правильной работы SSO с ЕСИА необходимо произвести дополнительные настройки в админке тенанта в разделе ЕСИА, и настроить ключ, сертификат и мнемонику системы, зарегистрированной в ЕСИА. Также интеграция с ЕСИА должна быть разрешена на уровне всей инсталляции PGS.

Интеграция с ЕСИА не совместима с LDAP/AD интеграцией!

5.6.4. Конфигурирование интеграции с AD через PGS

Данный подраздел опционален.

Применяется только при необходимости интеграции Auth/SSO с PGS, в котором настроена связь с внешним

сервером MS ActiveDirectory.

Для конфигурирования интеграции с AD необходимо изменить следующее значения в файле параметров инсталляции:

- `AUTH_AD` — изменить значение параметра на `true`.

5.6.5. Конфигурирование интеграции с почтой Poseidon

Для конфигурирования интеграции с Poseidon (далее PSN) необходимо изменить следующее значения в файле параметров инсталляции:

- `MAIL_INTEGRATION_MODE` — изменить значение параметра на `psn`.

Будет применена бесшовная интеграция Auth/SSO с инсталляцией почты, календаря и контактов PSN. Если базовый URL PSN не соответствует значению по умолчанию `mail.<DOMAIN_NAME>` (или `mail-<DOMAIN_ENV>.<DOMAIN_NAME>` в случае не пустого `DOMAIN_ENV`), необходимо задать базовый URL PSN в файле параметров инсталляции (смотри также 5.1, 5.3):

- `MAIL_BASE_URL` — базовый URL PSN (без схемы).

Базовый URL календаря PSN в этом случае будет настроен на `<MAIL_BASE_URL>/#calendar`, контактов — на `<MAIL_BASE_URL>/#contacts`, а доступ к Mail и Card API через роутинг `<MAIL_BASE_URL>/api`.

В случае медленной работы PSN Ajax API возможно потребуется настройка таймаута логина SSO после инсталляции, путем изменения значения (в миллисекундах) в Etcd (например, через Etcd Browser) в ветке `wfe/login.request.timeout.millis`.

В случае отказа от интеграции с PSN необходимо установить следующее значение в файле параметров инсталляции:

- `MAIL_INTEGRATION_MODE` — изменить значение параметра на `none` (Значение по умолчанию).

5.6.6. Конфигурирование интеграции с почтой Poseidon 2.0

Для конфигурирования интеграции с Poseidon 2.0 (далее PSN 2.0) необходимо изменить следующее значение в файле параметров инсталляции:

- `MAIL_INTEGRATION_MODE` — изменить значение параметра на `psn2`.

Необходимо заполнить следующие параметры в private.yml

- `MAIL_OAUTH2_CLIENT_ID` — значение данного параметра по умолчанию "psn", должно меняться совместно с настройками деплоя PSN 2.0
- `MAIL_OAUTH2_CLIENT_SECRET`
- `MAIL_OAUTH2_REDIRECT_URI`

Пример параметров в private.yml :

```
MAIL_OAUTH2_CLIENT_ID: "psn"
MAIL_OAUTH2_CLIENT_SECRET: "Fegre53mrth5eu6h"
MAIL_OAUTH2_REDIRECT_URI: "https://mail-domain.example.com/system/sso"
```

PSN 2.0 находится в экспериментальном состоянии!

5.6.7. Конфигурирование NTP серверов

Данный подраздел опционален.

Для конфигурирования NTP серверов необходимо открыть файл `~/install_co/group_vars/all/private.yml` в текстовом редакторе и добавить следующий блок в файл, изменив IP-адреса на требуемые:

```
# NTP settings
NTP_SERVERS:
  - "127.0.0.1"
  - "1.2.3.4"
```

5.6.8. Конфигурирование дополнительных серверов для логирования

Данный подраздел опционален.

Для конфигурирования дополнительных Fluentd серверов для сбора логов необходимо открыть файл `~/install_co/group_vars/all/private.yml` в текстовом редакторе и добавить следующий блок в файл, изменив IP-адреса и порты на требуемые:

```
# LOG servers for the environment
LOG_SERVERS:
  - ip: "server_1_ip_address"
    port: "24225"
  - ip: "server_2_ip_address"
    port: "24225"
```

Эта возможность существует только при использовании в инсталляции роли `[log]` и параметра `FLUENT_LOGGING_ENABLED=true`

5.6.9. Отключение функциональности мессенджера

Данный подраздел опционален.

Для отключения ссылки на приложение мессенджера Логос со стартовой страницы SSO и отключения интеграции с чатами Логос из текстовых редакторов необходимо добавить опцию `-e MESSENGER=NONE` при запуске инсталляционного скрипта (смотри также Приложение 1).

5.6.10. Включение функциональности редактора презентаций

Данный подраздел опционален.

Редактор презентаций находится в экспериментальном состоянии!

Для включения функциональности редактора презентаций необходимо добавить опцию `-e`

`PRESENTATION_EDITOR_DISABLED=false` при запуске инсталляционного скрипта (смотри также Приложение 1). После инсталляции, этой опцией можно управлять через Etcd флагом `config/wfe/presentation.editor.disabled`.

5.6.11. Дополнительная настройка политики ротации логов

Данный подраздел опционален.

Настройка ротации логов (logrotate) в данный момент автоматизирована и выполняется при инсталляции. Политику ротации логов можно перенастроить в конфигурационном файле `~/install_co/roles/bootstrap/templates/logrotate/co`.

5.6.12. Система синхронизации файлов CDN между хостами

Синхронизация файлов производится с помощью демона lsyncd по протоколу **rsync over ssh**. В режиме демона lsync работает на хостах с ролью `[lb_core_auth]`. Синхронизация данных запускается с помощью механизма ядра *inotify*, то есть отслеживается обновление или появление новых файлов и директорий. Задачи для синхронизации настраиваются в файле `/etc/lsyncd.conf`.

5.6.13. Включение поддержки SELinux

Данный подраздел опционален.

По умолчанию, в процессе деплоя происходит перевод подсистемы SELinux в состояние **disabled**.

Для включения поддержки SELinux необходимо добавить опцию `-e SELINUX_ENABLED=true` при запуске инсталляционного скрипта (смотри также Приложение 1).

Поддержка SELinux находится в экспериментальном состоянии!

5.6.14. Настройка префиксов виртуальных хостов

Данный подраздел опционален.

Префиксы виртуальных хостов Nginx (по умолчанию `auth`, `cdn`, `coapi`, `docs`, `files`, `links`) можно изменить с помощью параметров:

- `AUTH_PREFIX` префикс адреса приложения авторизации и лендинга Auth/SSO
- `CDN_PREFIX` префикс адреса CDN
- `COAPI_PREFIX` префикс адреса COAPI
- `DOCS_PREFIX` префикс адреса приложения редакторов
- `FILES_PREFIX` префикс адреса приложения файлового менеджера
- `LINKS_PREFIX` префикс адреса ссылок на документы

В имени префикса нельзя использовать символы `.` или `_`, остальные допустимые символы описаны в RFC1123.

Записи в DNS должны соответствовать новым префиксам. Настройка префиксов должна производиться совместно с настройками **PGS** и **PSN**.

5.6.15. Конфигурирование DNS серверов

Данный подраздел опционален.

Для конфигурирования DNS серверов необходимо открыть файл `~/install_co/group_vars/all/private.yml` в текстовом редакторе и добавить следующий блок в файл, изменив IP-адреса на требуемые:

```
# DNS settings in /etc/resolv.conf
DNS_SERVERS:
  - "127.0.0.1"
  - "8.8.8.8"
```

5.6.16. Отключение возможности скачивания документов

Данный подраздел опционален.

Предусмотрена опция отключения возможности скачивания документов в пользовательском интерфейсе. Для этого во время деплоя следует передать дополнительную опцию: `-e DOWNLOAD_DISABLED=true` при запуске инсталляционного скрипта (смотри также Приложение 1). В случае необходимости, эту опцию можно впоследствии настроить в Etcd во время эксплуатации стенда администратором инсталляции: `config/wfe/download.disabled={true,false}`

5.6.17. Отключение возможности копирования контента документов во внешний буфер обмена

Предусмотрена опция отключения возможности копирования во внешний буфер обмена (clipboard) содержимого документов (как в режиме просмотра, так и в режиме редактирования). При этом копирование/вставка внутри редактора документов продолжает работать. Для этого во время деплоя следует передать дополнительную опцию: `-e EXTERNAL_CLIPBOARD_DISABLED=true` при запуске инсталляционного скрипта (смотри также Приложение 1). В случае необходимости, эту опцию можно впоследствии настроить в Etcd во время эксплуатации стенда администратором инсталляции: `config/wfe/external.clipboard.disabled={true,false}`

5.6.18. Интеграция с мессенджерами

По умолчанию интеграция с мессенджером отключена.

Настройка интеграции с Dialog

Интеграция с Dialog будет доступна для всех пользователей инсталляции.

Для включения и настройки интеграции необходимо открыть файл `~/install_co/group_vars/all/private.yml` в текстовом редакторе и изменить значения следующих настроек:

- DIALOGBOT_TOKEN: токен для работы с Dialog API.
- DIALOGBOT_SERVER: HTTP URL сервера Dialog API.
- DIALOGBOT_WEB: HTTP URL веб-сервиса Dialog.

Там же, или через опцию запуска скрипта деплоя:

- MESSENGER: "DIALOG" — добавить настройку для интеграции с Dialog.

5.6.19. Интеграция по протоколу WOPI

Данный подраздел опционален.

При интеграции внешнего хранилища с редакторами по протоколу WOPI (https://en.wikipedia.org/wiki/Web_Application_Open_Platform_Interface) сервисы Chatbot, FM и NM не задействованы, поэтому группы ролей `core_fm`, `core_nm`, `chatbot` в инвентори должны быть пустые.

Другие компоненты «Система редактирования и совместной работы (СО) МойОфис» также не используются в этом режиме, поэтому следующие переменные в файле `~/install_co/group_vars/all/private.yml` заполнять не нужно (оставить пустые значения):

- AUTH_ENCRYPTION_*
- DIALOGBOT_*
- FS_*
- GCM_*
- HMS_*
- SQUADUSBOT_*

В этом же файле необходимо указать домен сервиса Nextcloud в переменной `CSP_ALLOWED_FRAME_ANCESTORS`, например: `CSP_ALLOWED_FRAME_ANCESTORS: '[ "nextcloud.example.com" ]'`

Для включения режима WOPI во время деплоя следует передать дополнительные опции: `-e WOPI_ENABLED=true -e MESSENGER=NONE` при запуске инсталляционного скрипта (смотри также Приложение 1).

Интеграция с мессенджерами в режиме WOPI недоступна.

Интеграция с WOPI тестировалась только для хранилища Nextcloud с плагином https://apps.nextcloud.com/apps/wopi.

В конфигурационном файле Nextcloud config/config.php необходимо добавить параметр `'allow_local_remote_servers'⇒ true`

На сервере Nextcloud в режиме администратора следует указать интеграцию с Office Online, указав адрес `https://docs[-<DOMAIN_ENV>.]<DOMAIN_NAME>` После этого можно будет открывать имеющиеся в хранилище документы на редактирование обычным пользователем.

5.6.20. Получение нотификаций от PGS

Данный подраздел опционален.

Предусмотрена опция получения нотификаций о действиях с профилем пользователя на стороне PGS. Для этого необходимо активировать федерацию:

Со стороны СО необходимо открыть файл `~/install_co/group_vars/all/private.yml` (смотри также 5.4) в текстовом редакторе и произвести следующие настройки:

- `PGS_RABBITMQ_USERNAME` — пользователь rabbitmq PGS.

- PGS_RABBITMQ_PASSWORD — пароль пользователя rabbitmq PGS. Необходимо раскомментировать строку и изменить значение параметра эквивалентное параметру RABBITMQ_PASSWORD из инсталляции PGS.

Там же, или через опцию запуска скрипта деплоя:

- RABBITMQ_FEDERATION_ENABLED: true — включение федерации rabbitmq.

Проверка статуса федерации приведена в п. 10.2.4

5.6.21. Настройка пула DU

Для поддержки большего числа открытых документов на ноду кластера (до **1000**), требования к системе возрастают. Рекомендуется использовать ноды с 8 vCPU / 24 GB памяти / SSD для роли [core_dcm]. При этом следует явно указать размер пула DU с помощью проперти DU_POOL_SIZE_MIN (значение DU_POOL_SIZE_MAX при этом не задается!) Также необходимо убедиться в том, что включен своп в системе на этих узлах кластера с помощью проперти SWAP_ENABLED. В случае отсутствия свопа, он будет автоматически создан в файле размером **4 GB** в корне файловой системы.

5.7. Настройка межсетевого экранирования

Сетевые порты, доступ к которым необходим с внешних IP адресов, приведены в таблице ниже.

Таблица 3 – Описание портов, доступ к которым необходимо обеспечить снаружи

Номер порта	Связанный IP	Назначение
80	0.0.0.0	http
443	0.0.0.0	https

Сетевые порты, доступ к которым необходим с внутренних IP адресов, приведены в таблице ниже.

Таблица 4 – Описание портов, доступ к которым необходимо обеспечить изнутри

Номер порта	Связанный IP	Назначение
22	0.0.0.0	ssh
80	0.0.0.0	http
443	0.0.0.0	https
5000	0.0.0.0	docker-registry
8001	0.0.0.0	etcd-browser
8443	0.0.0.0	Manage API (https)
8888	0.0.0.0	Manage API (http)

5.8. Настройка удаленного доступа

Настройка удаленного доступа выполняется при помощи роли sshd. Пример настройки роли приведен ниже:

```
ansible_port: 22
sshd:
 protocol: 2
 accept_env: "LC_*"
 permit_root_login: "no"
 password_authentication: "yes"
 use_dns: "no"
 x11_forwarding: "no"
 allow_groups: []
 allow_users: []
```

6. Установка «{comm_component}»

6.1. Конфигурация без отказоустойчивости

6.1.1. Запуск установки

Для запуска инсталляции подсистемы СО необходимо запустить shell-скрипт из директории `~/install_co/`.

```
./deploy_co.sh standalone -u root [дополнительные опции...]
```

При этом лог-файл процесса развертывания будет сохранен в `~/install_co/deploy_co_$DATE.log`.

Поддерживается опция `--become` для режима sudo в случае пользователя, отличного от root.

По умолчанию опция развёртывания `CLEANUP` содержит значение `false`. При "чистой" установке необходимо передать этой переменной значение `true`.

Дополнительные опции передаются после ключа `-e`.

Для запроса пароля SSH необходимо передать опцию `-k`.
При необходимости использовать приватный ключ вместо опции `-k` следует использовать опцию `–private-key=<путь к файлу приватного ключа>`.

При успешном выполнении скрипта сервисы подсистемы СО будут запущены автоматически.

6.1.2. Проверка корректности установки

Автоматическая проверка интеграционными тестами описана в Приложении 2. Рекомендуется провести ее до ручной проверки.

Ручная проверка состоит в следующем:

- В браузере открыть страницу `https://auth[-<DOMAIN_ENV>.]<DOMAIN_NAME>`
- Убедиться, что загрузилась страница авторизации.

- Убедиться, что при удачной авторизации происходит переход на страницу лендинга.
- Убедиться, что работают все приложения на лендинге.
- Зайти в файловый менеджер, и убедиться, что работает загрузка документа.
- В файловом менеджере создать разные типы документов, и убедиться, что их можно редактировать.

6.2. Кластерная отказоустойчивая конфигурация

6.2.1. Запуск установки

Для запуска инсталляции подсистемы CO необходимо запустить shell-скрипт из директории `~/install_co/`.

```
./deploy_co.sh cluster -u root [дополнительные опции...]
```

Дополнительные опции аналогичны конфигурации без отказоустойчивости.

6.2.2. Проверка корректности установки

Аналогична проверке конфигурации без отказоустойчивости.

7. Обновление с предыдущих версий

Процесс обновления «Система редактирования и совместной работы (СО) МойОфис» полностью аналогичен процессу первичной установки.

7.1. Состав дистрибутива

Состав дистрибутива приведен в п. 4.1.

8. Подготовка к обновлению

8.1. Описание ролей

Описание ролей приведено в п. 5.1.

8.2. Проверка и настройка инфраструктуры установки

Описание проверки и настройки инфраструктуры установки приведено в п. 5.2.

8.2.1. Проверка и настройка основных параметров установки

Описание проверки и настройки данных параметров приведено в п. 5.5.

8.2.2. Проверка и настройка дополнительных параметров установки

Описание проверки и настройки дополнительных параметров установки приведено в п. 5.6.

8.2.3. Проверка и настройка межсетевого экранирования

Описание проверки и настроек межсетевого экранирования приведено в п. 5.7.

8.2.4. Проверка и настройка разграничения доступа

Поддерживается SELinux. Дополнительной настройки не требуется.

8.2.5. Проверка и настройка удаленного доступа

Описание проверки и настройки удаленного доступа приведено в п. 5.9.

8.2.6. Создание резервных копий

В процессе работы на хостах «{comm_component}» не хранятся персистентно данные пользователя, поэтому создания резервных копий не требуется.

9. Обновление «{comm_component}»

9.1. Конфигурация без отказоустойчивости

9.1.1. Запуск обновления

Запуск обновления аналогичен процессу запуска установки, приведенному в п. 6.1.1.

9.1.2. Проверка корректности обновления

Проверка обновления аналогична проверке установки, описанной в п. 6.1.2

9.1.3. Миграция данных

В процессе работы на хостах «{comm_component}» не хранятся персистентно данные пользователя, поэтому миграции данных не требуется.

9.2. Кластерная отказоустойчивая конфигурация

9.2.1. Масштабирование конфигурации

Процесс масштабирования аналогичен приведенному в п. 3.3.

9.2.2. Запуск обновления

Запуск обновления аналогичен процессу запуска установки, приведенному в п. 6.2.1.

9.2.3. Проверка корректности обновления

Проверка обновления аналогична проверке установки, описанной в п. 6.2.2

9.2.4. Миграция данных

В процессе работы на хостах «{comm_component}» не хранятся персистентно данные пользователя, поэтому миграции данных не требуется.

9.2.5. Загрузка обновлений CDN

Обновления CDN предоставляют возможность замены или актуализации брендинга устанавливаемого продукта, а также добавления или изменения справочного web-контента, поддерживаемых языков, локализации или других ресурсов, используемых подсистемой CO, без остановки работы сервиса.

Загрузка пакетов обновлений CDN (бандлов) производится системным администратором, производящим установку продукта, после успешного завершения скрипта развертывания CO. Каждый пакет содержит документ, описывающий содержимое и версию пакета (его *манифест*), а также содержащий информацию о совместимости с версиями CO. Во время развертывания подсистемы CO в CDN устанавливаются минимально необходимые пакеты ресурсов для работы данной конфигурации.

Один пакет может либо добавлять новые и обновлять имеющиеся ресурсы, либо полностью заменять своим содержимым имеющиеся в CDN ресурсы. При этом загрузка нового пакета не исключает доступности по прямым ссылкам предыдущих ревизий ресурсов (например, ссылок на изображения в отправленных письмах-нотификациях). Несколько бандлов могут быть объединены в общий архив, *метабандл*, устанавливаемый как единое целое.

Текущие ограничения:

- Не реализован откат на предыдущую версию (но возможно ручное изменение в Etcd в ветке `config/cdn` и на файловой структуре в `/opt/co/shared`).
- Не проверяется целостность и безопасность архива, не реализована цифровая подпись.
- Нет тенантно-зависимых ресурсов.
- Отсутствует UI управления ресурсами.

Не реализовано блокирование механизма обновления на время работ по обновлению. Поэтому устанавливать сразу несколько обновлений параллельно с одного или с нескольких узлов роли `[lb_core_auth]` категорически запрещено.

9.2.6. Загрузка CDN бандла через Manage API

Подготовленный бандл (или метабандл) можно загрузить через Manage API (смотри раздел 8), адрес <SSO VIP> сервера Auth/SSO берется любой из указанных в группе `[lb_core_auth]` инвентарного файла. В ответ должен прийти код HTTP 200 и JSON, описывающий текущую ревизию, либо код ошибки 400 и JSON, содержащий сообщение с описанием ошибки:

```
curl -s 'http://<SSO VIP>:8888/api/manage/cdn/upload' -F
'file=@cdn_bundle.tar.gz'
```

или

```
curl -sk 'https://<SSO VIP>: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 рестарт рабочих процессов Nginx, и новая конфигурация CDN будет применена (это может занять большое время на кластере, если будут перезагружаться сервисы Core). Проконтролировать загрузку бандла можно по адресу `https://auth.<DOMAIN_NAME>/config` (или `https://auth-<DOMAIN_ENV>.<DOMAIN_NAME>/config`), путем анализа JSON объекта CDN в ответе. Объект CDN содержит специальный объект `_versions`, включающий данные в виде `<версия бандла> : <номер ревизии>`.

10. Дополнительные возможности и рекомендации по установке

10.1. Настройка мониторинга состояния

Не поддерживается в данном релизе.

10.2. Диагностика состояния подсистем CO

10.2.1. Сбор сведений оборудования

Плейбук для централизованного сбора данных о хостах инсталляции.

```
ansible-playbook -i inventory/<inventory_path> hardware-report.yml [-b]
```

После выполнения создается файл hardware-report-<timestamp>.json в текущей директории. Этот файл в формате JSON содержит информацию о хосте оператора (откуда производится деплой) и всех хостах инсталляции. Эта информация включает в себя данные о процессоре, памяти, диске, сетевом интерфейсе, а также о версии докера. Запускать этот сценарий можно как до, так и после деплоя CO. Полученный файл можно передать службе технической поддержки (смотри **Приложение 11**).

10.2.2. Диагностика состояния nginx

Проверка статуса работы подсистем Auth/SSO и Core осуществляется по адресам:

- `http://<локальный-адрес-сервера>:8888/api/manage/core/status`, параметр `"all"` в ответе должен быть равен строке `"OK"`.
- `http://<локальный-адрес-сервера>:8888/api/manage/docs/status`

Проверка текущей конфигурации осуществляется по адресу:

- http://<локальный-адрес-сервера>:8888/api/manage/config

Просмотр логов доступа и ошибок системы Auth/SSO (в случае отсутствия сервера с ролью `[log]`) осуществляется по адресам:

- http://<локальный-адрес-сервера>:8888/api/manage/logs/error
- http://<локальный-адрес-сервера>:8888/api/manage/logs/access
- http://<локальный-адрес-сервера>:8888/api/manage/logs/access_full

Просмотр списка активных сессий и залогиненных пользователей подсистемы Auth/SSO осуществляется по адресам:

- `http://<локальный-адрес-сервера>:8888/api/manage/sessions`
- `http://<локальный-адрес-сервера>:8888/api/manage/users`

Адрес сервера берется любой из указанных в группе `[lb_core_auth]` инвентарного файла.

По соображениям безопасности доступ к данному порту ограничен на стороне Nginx локальным хостом и внутренними (приватными) сетями с адресами по стандарту RFC1918. Категорически запрещается открывать доступ к нему из публичных сетей.

10.2.3. Диагностика состояния lsyncd

Данный раздел применим только для кластерного режима инсталляции (в односерверной конфигурации lsyncd **не используется**).

Проверить успешность синхронизации можно в лог файле. Его местонахождение указано в файле конфигурации `/etc/lsyncd.conf` (по умолчанию `/opt/co/lsyncd/logs/lsyncd.log`). Демон lsyncd должен быть запущен на всех узлах с ролью `[lb_core_auth]`, проверить его статус можно при помощи `systemctl status lsyncd`.

10.2.4. Диагностика состояния rabbitmq

Проверка статуса очередей сообщений осуществляется через Web интерфейс RabbitMQ по адресу `http://<локальный-адрес-сервера>:15672` с использованием логина и пароля, настроенных в разделе 5.5. Адрес сервера берется любой из указанных в группе `[mq]` инвентарного файла. При необходимости имеется возможность проверить состояние кластера RabbitMQ, создать или удалить очередь обмена или отдельные сообщения.

Проверить успешно настроенную федерацию rabbitmq можно, обратившись в веб интерфейс rabbitmq CO по адресу `http://<локальный-адрес-сервера>:15672/#/federation`

После каждого деплоя, редеплоя, рестарта части PGS, или CO необходимо проверить, что RabbitMQ в PGS имеет виртуальный хост с именем "co". Если такого vhost нет, то его нужно создать в админке Rabbit UI. Для доступа в админку используйте доменное имя указывающее на сервер PGS, доменное имя формируется на базе зарегистрированного домена инсталляции «МойОфис Хранилище». (см. Документацию PGS) и порт 15673: `http://pgs-<ENV>.<DEFAULT_DOMAIN>:15673`. В качестве логина и пароля используются значения переменных `PGS_RABBITMQ_USERNAME` и `PGS_RABBITMQ_PASSWORD`, описанные ранее в файле `private.yml`.

По соображениям безопасности доступ к данному порту должен быть ограничен локальным хостом и внутренними (приватными) сетями с адресами по стандарту RFC1918. Категорически запрещается открывать доступ к нему из публичных сетей.

10.2.5. Диагностика состояния haproxy

Проверка статуса сервиса haproxy (доступность бекендов, статистика подключений) осуществляется через Web интерфейс HAProxy по адресам:

- `http://<локальный-адрес-сервера>:8889/api/manage/stats`, http соединения
- `http://<локальный-адрес-сервера>:8890/api/manage/stats`, tcp соединения

Доступ осуществляется с использованием логина и пароля, настроенных в разделе 5.5.

Адрес сервера берется любой из указанных в группах `[lb_core_auth], [core_*]` инвентарного файла.

По соображениям безопасности доступ к данному порту должен быть ограничен локальным хостом и внутренними (приватными) сетями с адресами по стандарту RFC1918. Категорически запрещается открывать доступ к нему из публичных сетей.

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.

11.1. Системные сообщения

11.2. Известные проблемы и способы решения

Для применения патча рекомендуется использовать команду `patch -p1 < patchfile` из корневой директории плейбуков, либо внести изменения вручную в нужный файл (файлы).

11.2.1. Проблемы, вызванные ошибками аллокатора памяти ядра Linux

Описание проблемы

Проблема характерна только для ядер Linux версий 3.x, для ядер >= 4.4 проблема не воспроизводится. Для обновления ядра можно использовать параметр `-e UPGRADE_KERNEL=true` при деплое.

В некоторых случаях в процессе работы инсталляции могут наблюдаться спонтанные сбои запуска Docker контейнеров. Для пользователя это чаще всего проявляется в невозможности сконвертировать или открыть документ. Мониторинг доступной (available) памяти показывает большие значения, от 2 Гб и более, при этом величина закешированной (buff/cache) памяти сравнима, или превышает значение доступной. В системном журнале появляются разные ошибки аллокатора памяти, например `page allocation failure`, `running exec setns process for init caused \"exit status 34\"`, `Unable to create nf_conn slab cache` и другие.

Решение

Полноценное решение проблемы на данный момент не известно. Существуют отдельные тикеты на Docker, описывающие похожие проблемы, например https://github.com/moby/moby/issues/31037 Описание диагностики приведено в http://www.lijiaocn.com/%E9%97%AE%E9%A2%98/2017/11/13/problem-unable-create-nf-conn.html Возможный баг ядра описан в https://bugzilla.redhat.com/show_bug.cgi?id=1401012

В случае диагностирования подобной проблемы рекомендуется сперва применить следующую команду:

```
sync && echo 2 > /proc/sys/vm/drop_caches
```

В случае дальнейшего проявления аналогичных ошибок рекомендуется перезагрузка виртуальной машины.

11.2.2. Проблема при установке на ноды с ограниченными ресурсами

Описание проблемы

```
TASK [bundles-upload : Show failed uploads]
*********************************************************************
*********************************
task path: /root/install_co_2021.01/roles/bundles-
upload/tasks/main.yml:119
fatal: FAILED! =>
 msg:
 - |-
 -1 --- Could not find or access '/root/.ansible/tmp/ansible-tmp-
1615902121.7462332-9800-36130470129979/myoffice.20.0.6.393.tgz' on the
Ansible Controller.
 If you are using a module and expect the file to exist on the remote,
see the remote_src option
 - |-
 -1 --- Could not find or access '/root/.ansible/tmp/ansible-tmp-
1615902169.396169-10219-252985504775064/sso-app-20.0.6.19-branding-
myoffice.tar.gz' on the Ansible Controller.
 If you are using a module and expect the file to exist on the remote,
see the remote_src option
```

Она является следствием загруженности нод, совмещающих свою роль с ролью кластера Etcd, так как по умолчанию активная часть кластера Etcd разворачивается на нодах с ролью `[mq]`.

Решение

Рекомендуемое решение — выделить под Etcd отдельные 3 ноды следующей минимальной конфигурации:

- 2 vCPU.
- 2Gb RAM.

Далее сконфигурировать инвентори-файл:

```
all:
  children:
    etcd:
      hosts:
        x.x.x.1:
        x.x.x.2:
        x.x.x.3:
```

Повторить деплой (с `-e CLEANUP=true`).

Проверить диски на совместимость с etcd. Воспользуйтесь утилитой от RedHat:

```
docker run --volume /var/lib/etcd:/var/lib/etcd:Z quay.io/openshift-
scale/etcd-perf
```

После завершения работы она выдает статистику и подходит ли хост для работы с etcd:

```
99th percentile of fsync is 6389760 ns
99th percentile of the fsync is within the recommended threshold - 10
ms, the disk can be used to host etcd
```

Дополнительным решением может стать поднятие таймаута etcd в плейбуках до деплоя увеличив значение `etcd.connection.timeout` в файле `roles/auth/templates/apps/wfe.properties.j2` на большее.

12. Приложение 1. Дополнительные опции и параметры развёртывания

Дополнительные опции и параметры развёртывания можно поместить в файл параметров в формате yml (смотри разделы 5.1, 5.3). Также возможно указать дополнительные аргументы при запуске скрипта развёртывания в командной строке (смотри разделы 6.1, 6.2):

```
... -e OPTION1=value1 -e OPTION2=value2
```

Опции, указанные в командной строке, имеют наивысший приоритет и перекрывают значения одноименных опций (свойств) в yml файлах.

Везде в таблице "флаг" означает `false`= выключение, `true`= включение указанной опции. Значения по умолчанию, разделенные /, показывают разные значения для односерверного режима и для кластера.

Таблица 1. Основные параметры развертывания и дополнительные опции.

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
`ADMIN_BASE_URL`	нет	нет	Переопределяет полный URL приложения администратора тенанта Admin в `/config`
`ANALYTICS_ENABLED`	нет	`true`	Флаг включения посылки сообщений аналитики в Fluentd агент (локально)
`AUTH_AD`	нет	`false`	Флаг включения режима интеграции PGS с AD (изменяет UI/UX в SSO)
`AUTH_ENCRYPTION_IV`	да	нет	Вектор инициализации алгоритма AES-256-CBC, используемого для шифрования mail_session токена
`AUTH_ENCRYPTION_KEY`	да	нет	Секретный ключ алгоритма AES-256-CBC, используемого для шифрования mail_session токена
`AUTH_ENCRYPTION_SALT`	да	нет	Соль для данных, передаваемых в алгоритм AES-256-CBC, используемый для шифрования mail_session токена
`AUTH_LDAP`	нет	`false`	Флаг включения режима интеграции SSO с LDAP (изменяет UI/UX в SSO, авторизует через LDAP и создает пользователей в PGS)
`AUTH_PREFIX`	нет	`auth`	Имя виртуального хоста в конфигурации Nginx в виде `~^${AUTH_PREFIX}.*$` (также учитывается в URL Auth/SSO в `/config`)
`BRANDING`	да	`myoffice`	Выбор имени брендинга из включенного в данный дистрибутив. Параметр приведён для справки, его значение изменять запрещено!
`CDN_PREFIX`	нет	`cdn`	Имя виртуального хоста в конфигурации Nginx в виде `~^${CDN_PREFIX}.*$` (также учитывается в URL CDN в `/config`)

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
`CDN_RELEASE_HASH`	`да`	`нет`	Определяет часть URL в CDN для идентификации данного релиза
`CHATBOT_LOG_LEVEL`	`нет`	`info`	Уровень логирования сервиса Chatbot. Используемые значения: `debug` (максимум), `info`, `warning`, `error` (минимум)
`CHATBOT_MAX_MEM`	`нет`	`512mb`	Количество памяти, доступной сервису Chatbot, указанных единиц памяти.
`CHATBOT_NODEJS_OPTS`	`нет`	`""`	Дополнительные опции Node.js сервиса Chatbot, рекомендуется значение `--optimize_for_size` для инсталляций, ограниченных по памяти на серверах из секции `[chatbot]`
`COAPI_HTTP_SOCKET_TIMEOUT_MILLIS`	`нет`	`-1`	Таймаут соединения с сервисом COAPI через HAPROXY, если определен и меньше значения HAPROXY_HTTP_TIMEOUT_MILLIS
`CHECK_ENVIRONMENT`	`нет`	`true`	Флаг включения проверки валидности окружения (нужного количества серверов определенных ролей, версии Ansible, virtualenv)
`COAPI_PREFIX`	`нет`	`coapi`	Имя виртуального хоста в конфигурации Nginx в виде `~^${COAPI_PREFIX}.*$` (также учитывается в URL COAPI в `/config`)
`CORS_ALLOWED_HEADERS`	`нет`	`[]`	Список дополнительных HTTP заголовков, которые можно передавать на сервер при XHR запросе веб приложений при помощи CORS, добавляется к списку заголовка Access-Control-Allow-Headers
`CORS_ALLOWED_ORIGINS`	`нет`	`[]`	Список дополнительных origin, к которым разрешены XHR запросы веб приложений при помощи CORS, при валидном запросе origin вернется в заголовке Access-Control-Allow-Origin
`CO_DIR`	`нет`	`/opt/co`	Абсолютный путь к директории инсталляции (экспериментально)
`CO_ES_DIR`	`нет`	`/opt/es`	Абсолютный путь к директории ElasticSearch, где хранятся индексируемые логи (директория не очищается при `-e CLEANUP=true`)
`CPUS_ALLOWED_DU`	`нет`	`0.8/0.5`	Ограничения ресурсов процессора для процессов DU в Docker контейнере
`CPU_ALLOWED_COEF`	`нет`	`0.8/1.0`	Ограничения ресурсов процессора для сервисов CO в Docker контейнерах
`CPU_SHARES`	`нет`	`900/800`	Ограничения ресурсов процессора для сервисов CO в Docker контейнерах
`CPU_SHARES_DU`	`нет`	`512/800`	Ограничения ресурсов процессора для процессов DU в Docker контейнере

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
CRYPTO_PRO_LICENSE	нет	""	Лицензия "КриптоПро CSP" в случае использования дистрибутива с поддержкой ГОСТ шифрования
CSP_ALLOWED_FRAME_ANCESTORS	нет	[]	Список дополнительных хостов, с которых допустимо открывать приложение вьюера в iframe при помощи CSP, добавляется к списку frame-ancestors заголовка Content-Security-Policy
CU_LOG_LEVEL	нет	info	Уровень логирования процесса CU (конвертора документов). Допустимые значения: trace (максимум), debug, info, warn, error, fatal (минимум) или none (отключение логирования)
CU_POOL_SIZE	нет	10	Размер пула CU на серверах в секции [core_cvm]
CVM_DBG_PORT	нет	9003	Порт JVM для отладки CVM при включенном DEV_CORE, только для разработки!
CVM_HEAP	нет	512m	Размер памяти (хипа JVM) сервиса CVM
CVM_HTTP_SOCKET_TIMEOUT_MILLIS	нет	-1	Таймаут соединения с сервисом CVM через HAPROXY, если определен и меньше значения HAPROXY_HTTP_TIMEOUT_MILLIS
CVM_MAX_CONSUMER_NUM	нет	-1	Количество консьюмеров CVM (влияет на количество процессов CU, по умолчанию равно числу доступных vCPU)
DCM_DBG_PORT	нет	9004	Порт JVM для отладки DCM при включенном DEV_CORE, только для разработки!
DCM_HEAP	нет	512m	Размер памяти (хипа JVM) сервиса DCM
DCM_MAX_LA_MULTIPLICATOR	нет	2/4	Коэффициент вычисления веса DCM для балансировки по load average
DCM_MAX_RAM_MULTIPLICATOR	нет	0.1/0.01	Коэффициент вычисления веса DCM для балансировки по объёму доступной памяти
DCM_STATE_UPDATE_INTERVAL_MILLIS	нет	5000	Интервал обновления состояния DCM/DU в Redis в миллисекундах, используется в Nginx для получения информации о балансировке сервисов
DEPLOY_CHECK_TIMEOUT	нет	300	Время таймаута ожиданий операций при деплое в секундах, также таймаут рестарта сервисов в вотчдогах
DEPLOY_TYPE	нет	нет	Тип развертывания (cluster или standalone); если значение не задано, тип определяется по количеству узлов с ролью mq (1: standalone, 2 и более: cluster)
DEV_CORE	нет	false	Флаг включения режима разработки серверных компонент CVM/DCM/JOD/FM/NM
DEV_MODE	нет	false	Флаг включения глобального режима разработки

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
DEV_NGINX	нет	false	Флаг включения режима разработки серверных компонент Nginx
DEV_NGINX_REVISION	нет	false	Бранч, тег или ревизия кода Nginx в режиме разработки DEV_NGINX
DEV_PREGEN	нет	false	Флаг включения режима разработки серверных компонент Pregen
DEV_WFE	нет	false	Флаг включения режима разработки серверных компонент WFE
DEV_WTE	нет	false	Флаг включения режима разработки серверных компонент WTE
DNS_SERVERS	нет	[]	Список из ip адресов (до 3-х) для модификации файла /etc/resolv.conf (используется директива nameserver)
DOCKER_MTU_SIZE	нет	1500	Размер MTU сетевого моста для Docker
DOCKER_REGISTRY	да	нет	Имя приватной Docker Registry, используемой для инсталляции. По умолчанию контейнеры используют "dockreg.ncloudtech.ru"
DOCKER_STORAGE_DRIVER	нет	overlay	Устройство хранения для Docker, по умолчанию overlay при ядрах < 4.x, overlay2 в противном случае.
DOCS_PREFIX	нет	docs	Имя виртуального хоста в конфигурации Nginx в виде ~^${DOCS_PREFIX}.*$ (также учитывается в URL редакторов в /config)
DOMAIN_NAME	да	нет	Выбор имени базового домена инсталляции, 2-го уровня или ниже, без точки в начале или в конце
DOMAIN_ENV	нет	нет	Выбор "окружения" домена инсталляции. Если параметр определен, то добавляется как суффикс после имени виртуального хоста через дефис
DOWNLOAD_DISABLED	нет	false	Флаг включения опции отключения возможности скачивания документов в пользовательском интерфейсе
DU_LOG_LEVEL	нет	info	Уровень логирования процесса DU (редактора-коллаборатора документов). Допустимые значения: trace (максимум), debug, info, warn, error, fatal (минимум) или none (отключение логирования)
DU_MAX_TIME_FOR_INACTIVE_COLLABORATOR_MINS	нет	180	Время, по истечении которого пользователи, открывшие файл на редактирование, будут отключены от редактируемого документа в случае их бездействия.

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
DU_POOL_SIZE_MAX	нет	400	Не используется в случае SDD_DU_ENABLED=true. Иначе, максимальный допустимый размер пула DU на серверах в секции [core_dcm]. Для изменения этого значения после деплоя следует использовать Etcd ключ /nct/co/<release-version>/config/dcm/docker.duPoolSizeMax. Значение этого параметра должно превышать значение DU_POOL_SIZE_MIN (Etcd ключ /nct/co/<release-version>/config/dcm/docker.duPoolSize) не менее, чем на 10 (или фактического значения Etcd ключа /nct/co/<release-version>/config/dcm/docker.countOfDuToBeStartedAdditionally).
DU_POOL_SIZE_MIN	нет	100	Размер пула DU в случае SDD_DU_ENABLED=true на серверах в секции [core_dcm] или начальный размер пула DU в противном случае (при этом максимальное количество DU ограничивается автоматически доступной памятью /proc/meminfo:MemAvailable, метрикой LA и значением DU_POOL_SIZE_MAX). Изменять это значение в большую сторону рекомендуется после завершения установки, так как запуск DU вызывает большую нагрузку. Для изменения этого значения после деплоя с SDD_DU_ENABLED=true следует использовать Etcd ключ /nct/co/<release-version>/config/nps-du/du.PoolSize, или ключ /nct/co/<release-version>/config/dcm/docker.duPoolSize в противном случае.
ERLANG_COOKIE	да	нет	Разделяемый секрет для взаимодействия Erlang процессов в кластере RabbitMQ (алфавитно-цифровая строка в кодировке Latin1 до 255 символов). Инструменты управления конфигурацией и оркестрации контейнеров должны убедиться, что каждый контейнер узла RabbitMQ в кластере использует одно и то же значение. Например: "DSIFUHDISFLEWWELKBLJB98273489237941". Подробное описание соответствующего параметра RABBITMQ_ERLANG_COOKIE можно найти в официальной документации по кластеризации RabbitMQ https://www.rabbitmq.com/clustering.html
ESIA_PROD_AC_URL	нет	https://esia.gosuslugi.ru/aas/oauth2/ac	Адрес получения access code в продуктивной среде ЕСИА

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
ESIA_PROD_TE_URL	нет	https://esia.gosuslugi.ru/aas/oauth2/te	Адрес token exchange в продуктивной среде ЕСИА
ESIA_PROD_RS_URL	нет	https://esia.gosuslugi.ru/rs	Адрес resource server в продуктивной среде ЕСИА
ESIA_TEST_AC_URL	нет	https://esia-portal1.test.gosuslugi.ru/aas/oauth2/ac	Адрес получения access code в тестовой среде ЕСИА
ESIA_TEST_TE_URL	нет	https://esia-portal1.test.gosuslugi.ru/aas/oauth2/te	Адрес token exchange в тестовой среде ЕСИА
ESIA_TEST_RS_URL	нет	https://esia-portal1.test.gosuslugi.ru/rs	Адрес resource server в тестовой среде ЕСИА
ES_HEAP_SIZE	нет	1g/8g	Объём хипа JVM для ElasticSearch на сервере с ролью [log]
ES_HOST	нет	127.0.0.1	IP-адрес ElasticSearch на сервере с ролью [log]
ES_INDEX_RETENTION_PERIOD_DAYS	нет	120	Время хранения логов в ElasticSearch, дней. Более старые индексы удаляются автоматически
ES_PORT	нет	9200	IP-порт ElasticSearch на сервере с ролью [log]
ETCD_API_PREFIX	нет	v2/keys	Префикс формирования URL доступа к ключам Etcd
ETCD_BROWSER_PASSWORD	да	нет	Пароль для авторизации в веб приложении Etcd Browser на сервере с ролью [service]
ETCD_BROWSER_PORT	нет	8001	Порт веб приложения Etcd Browser на сервере с ролью [service]

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
ETCD_BROWSER_USERNAME	да	couser	Пользователь для авторизации в веб приложении Etcd Browser на сервере с ролью [service]
ETCD_CLIENT_PORT	нет	2379	IP-порт клиентского протокола (http/https) сервиса Etcd
ETCD_CO_PREFIX	нет	nct/co	Префикс дерева ключей конфигурации CO в Etcd
ETCD_ELECTION_TIMEOUT	да	6000	Таймаут выборов ведущего в кластере Etcd, в миллисекундах
ETCD_HEARTBEAT_INTERVAL	да	600	Интервал посылки запроса о доступности узла (heartbeat) в кластере Etcd, в миллисекундах
ETCD_INITIAL_CLUSTER_TOKEN	нет	etcd-cluster-1	Токен автообнаружения сервисов Etcd для их кластеризации
ETCD_SERVER_PORT	нет	2380	Порт протокола межсервисного взаимодействия (tcp) в кластере Etcd
EXT_FLUENT_FORWARD_HOST	нет	127.0.0.1	FQDN или IP-адрес Fluentd-сервера вместо значения из [log] инвентарного файла
EXT_FLUENT_FORWARD_PORT	нет	24225	IP-порт Fluentd-сервера вместо значения из [log] инвентарного файла
EXTERNAL_CLIPBOARD_DISABLED	нет	false	Флаг включения опции отключения возможности копирования во внешний буфер обмена
FILES_PREFIX	нет	files	Имя виртуального хоста в конфигурации Nginx в виде ~^${FILES_PREFIX}.*$ (также учитывается в URL FM в /config)
FLUENTD_AGENT_PORT_FORWARD	нет	24224	Порт приема и форвардинга логируемых сообщений в формате JSON/MsgPack по протоколу http Fluentd-агента
FLUENTD_AGENT_PORT_INPUT_COMMON_HTTP	нет	5180	Порт приема логируемых сообщений в формате JSON по протоколу http Fluentd-агента
FLUENTD_AGENT_PORT_INPUT_COMMON_SYSLOG	нет	5140	Порт приема логируемых сообщений в формате Syslog по протоколу udp Fluentd-агента
FLUENTD_AGENT_PORT_INPUT_NGINX_ANALYTICS	нет	5160	Порт приема сообщений серверной аналитики Nginx в формате JSON по протоколу udp Fluentd-агента на серверах с ролью [lb_core_auth]
FLUENTD_AGENT_PORT_INPUT_NGINX_SYSLOG	нет	5185	Порт приема логируемых сообщений Nginx в формате Syslog по протоколу udp Fluentd-агента на серверах с ролью [lb_core_auth]
FLUENTD_AGENT_PORT_INPUT_NGINX_WEB_ANALYTICS	нет	5165	Порт приема сообщений веб аналитики Nginx в формате JSON по протоколу udp Fluentd-агента на серверах с ролью [lb_core_auth]

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
FLUENTD_AGENT_PORT_MONITOR	нет	24220	Порт мониторинга состояния Fluentd-агента (только внутри Docker контейнера)
FLUENTD_AGENT_SYSLOG_FACILITY	нет	local0	Установка (facility) приема логируемых сообщений в формате Syslog по протоколу udp Fluentd-агента
FLUENTD_SERVER_PORT_FORWARD	нет	24225	Порт приема и форвардинга логируемых сообщений в формате JSON/MsgPack по протоколу http Fluentd-сервера с ролью [log]
FLUENTD_SERVER_PORT_MONITOR	нет	24221	Порт мониторинга состояния Fluentd-сервера (только внутри Docker контейнера) с ролью [log]
FLUENT_LOGGING_ENABLED	нет	false/true	Флаг включения посылки сообщений логирования в локальный Fluentd-агент вместо лог-файлов
FM_DBG_PORT	нет	9001	Порт JVM для отладки FM при включенном DEV_CORE, только для разработки!
FM_HEAP	нет	512m	Размер памяти (хипа JVM) сервиса FM
FS_API_URL	да	нет	URL доступа к FS API от серверов CO, может включать в себя порт, без / в конце, поддерживаются HTTP/HTTPS схемы
FS_APP_ENCRYPTION_IV	да	нет	Вектор инициализации алгоритма AES-256-CBC, используемого для шифрования секретных данных тенантов, переданных через FS App API и сохраненных в Etcd (ключ сертификата, пароль SMTP)
FS_APP_ENCRYPTION_KEY	да	нет	Секретный ключ алгоритма AES-256-CBC, используемого для шифрования секретных данных тенантов, переданных через FS App API и сохраненных в Etcd (ключ сертификата, пароль SMTP)
FS_APP_ENCRYPTION_SALT	да	нет	Соль для данных, передаваемых в алгоритм AES-256-CBC, используемый для шифрования секретных данных тенантов, переданных через FS App API и сохраненных в Etcd (ключ сертификата, пароль SMTP)
FS_APP_LOGIN	да	нет	Полный логин (с доменом) созданного в PGS пользователя FS AppAPI
FS_APP_PASSWORD	нет	нет	Пароль пользователя FS AppAPI, указанного в FS_APP_LOGIN. После запуска SSO пароль не может быть изменён!
FS_APP_URL	да	нет	URL доступа к FS App API от серверов CO, может включать в себя порт, без / в конце, поддерживаются HTTP/HTTPS схемы
FS_TOKEN_SALT_EXT	да	нет	Соль дайджеста токена из PGS конфига, значение FS_TOKEN_SALT_EXT
GCM_AUTHORIZATION_KEY	нет	""	Ключ аккаунта Google Cloud Messaging, указанного в GCM_PROJECT_ID

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
GCM_PROJECT_ID	нет	""	Идентификатор аккаунта Google Cloud Messaging, используемого для отправки нотификаций мобильным клиентам Android/iOS
GOST_ENABLED	нет	false	Флаг включения поддержки ГОСТ шифрования в случае использования такого дистрибутива
GRAFANA_DASH_PORT	нет	3001	Порт дашборда внутренней системы мониторинга Grafana (не установлена по умолчанию), только для разработки!
HAPROXY_HTTP_TIMEOUT_MILLIS	нет	90000	Общий таймаут соединения с сервисами CVM, COAPI, PREGEN через HAPROXY. Если он -1, то используются значения для каждого сервиса отдельно.
HAPROXY_PASSWORD	да	нет	Пароль для авторизации в веб-интерфейсе HAProxy
HAPROXY_PORT_AMQP	нет	20002	Порт проксирования RabbitMQ на серверах с ролью [core_*]
HAPROXY_PORT_COAPI	нет	20005	Порт проксирования COAPI на серверах с ролью [core_*]
HAPROXY_PORT_CVM	нет	20004	Порт проксирования CVM на серверах с ролью [core_*]
HAPROXY_PORT_NEXTCLOUD_FSAPI	нет	20003	Порт проксирования NEXTCLOUD (не установлен по умолчанию) на серверах с ролью [core_*]
HAPROXY_PORT_PREGEN	нет	20001	Порт проксирования PREGEN на серверах с ролью [core_*]
HAPROXY_PORT_STATS_HTTP	нет	8889	Порт веб интерфейса статистики HAProxy HTTP бекендов на серверах с ролью [core_*]
HAPROXY_PORT_STATS_TCP	нет	8890	Порт веб интерфейса статистики HAProxy TCP бекендов на серверах с ролью [core_*]
HAPROXY_USERNAME	да	couser	Пользователь для авторизации в веб-интерфейсе HAProxy
HMS_AUTHORIZATION_KEY	нет	""	Ключ аккаунта Huawei Mobile Services, указанного в HMS_PROJECT_ID
HMS_ENABLED	нет	false	Флаг включения режима интеграции с Huawei Mobile Services в сервисе NM
HMS_PROJECT_ID	нет	""	Идентификатор аккаунта Huawei Mobile Services, используемого для отправки нотификаций мобильным клиентам Android
INFLUX_ADMIN_ENABLED	нет	true	Флаг включения администрирования базы событий Influx внутренней системы мониторинга (не установлена по умолчанию), только для разработки!

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
INFLUX_ADMIN_PORT	нет	8083	Порт дашборда администрирования http протокола базы событий Influx внутренней системы мониторинга (не установлена по умолчанию), только для разработки!
INFLUX_HTTP_PORT	нет	8086	Порт клиентского API http протокола базы событий Influx внутренней системы мониторинга (не установлена по умолчанию), только для разработки!
JIRA_EMAIL_FIELD_NAME	нет	""	Название поля с email в тикете JIRA
JIRA_ISSUE_TYPE	нет	""	Тип заводимого тикета в JIRA
JIRA_PASSWORD	нет	""	Пароль пользователя в JIRA для автоматического заведения тикетов
JIRA_PROJECT_ID	нет	""	Идентификатор проекта в JIRA для автоматического заведения тикетов
JIRA_URL	нет	""	URL доступа к JIRA API
JIRA_USERNAME	нет	""	Логин пользователя в JIRA для автоматического заведения тикетов
JOD_DBG_PORT	нет	9005	Порт JVM для отладки JOD при включенном DEV_CORE, только для разработки!
JOD_HEAP	нет	512m	Размер памяти (хипа JVM) сервиса JOD
JOD_LO_INSTANCES	нет	2	Количество процессов LibreOffice, запускаемых каждым сервисом JOD
JOD_MAX_TASKS_BEFORE_RESTART	нет	200	Максимальное количество преобразований до принудительного перезапуска процесса LibreOffice в JOD. Установка значения 0 или отрицательного числа убирает лимит
KIBANA_PASSWORD	да	нет	Пароль для авторизации в Kibana в открытом виде
KIBANA_USERNAME	да	couser	Пользователь для авторизации в Kibana
LDAP_BASE_DN	нет	нет	Начальный узел дерева LDAP для поиска пользователей при авторизации через SSO
LDAP_BIND_DN	нет	нет	Логин пользователя с правом поиска для авторизации SSO в LDAP сервере
LDAP_BIND_PASS	нет	нет	Пароль пользователя с правом поиска для авторизации SSO в LDAP сервере
LDAP_PORT	нет	нет	Порт LDAP сервера для SSO (обычно 389)
LDAP_SERVER	нет	нет	FQDN или IP адрес LDAP сервера для SSO
LINKS_PREFIX	нет	links	Имя виртуального хоста в конфигурации Nginx в виде `~^${LINKS_PREFIX}.*$` (также учитывается в URL Links в `/config`)

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
LOGBACK_CO_LEVEL	нет	info	Уровень логирования сервисов CVM, DCM, FM и NM. Используются значения: all (максимум), trace, debug, info, warn, error (минимум) или off (отключение логирования)
MAIL_BASE_URL	нет	нет	Переопределяет полный URL приложения Mail в /config
MAIL_INTEGRATION_MODE	нет	none	Параметр режима интеграции SSO с почтой Poseidon (PSN) (изменяет базовые URL Почты, Календаря и Контактов в SSO, дополнительно авторизует пользователя через PSN Ajax API после успешного логина в PGS, манипулирует кукой p7auth), или полностью отключает интеграцию в режиме none
MESSENGER	нет	NONE	Тип мессенджера для интеграции чата в редакторы при помощи сервиса Chatbot. Возможные значения: DIALOG и none (отключение интеграции)
NM_DBG_PORT	нет	9002	Порт JVM для отладки NM при включенном DEV_CORE, только для разработки!
NM_HEAP	нет	512m	Размер памяти (хипа JVM) сервиса NM
NPS_LOG_LEVEL	нет	info	Уровень логирования сервиса NPS. Используемые значения: debug (максимум), info, warning, error (минимум) или off (отключение логирования)
NPS_MAX_MEM_DEFAULT	нет	512mb	Количество памяти, доступной отдельному контейнеру конвертации, запускаемому через NPS, указанных единиц памяти.
OPENRESTY_LB_CORE_AUTH_MNG_PORT	да	8888	Порт http протокола для Manage API сервиса SSO
OPENRESTY_LB_CORE_AUTH_MNG_PORT_TLS	да	8443	Порт https протокола для Manage API сервиса SSO
OPENRESTY_WORKERS	нет	2/auto	Количество воркеров Nginx (auto означает vCPU * 2)
PGS_RABBITMQ_USERNAME	нет	"rabbitmq"	Пользователь доступа к rabbitmq на стороне PGS
PGS_RABBITMQ_PASSWORD	нет	нет	Пароль доступа к rabbitmq на стороне PGS на стороне PGS
PGS_RABBITMQ_PORT_AMQP	нет	5673	Порт веб интерфейса rabbitmq на стороне PGS
PGS_RABBITMQ_PORT_MNG	нет	15673	Порт управления rabbitmq на стороне PGS
PGS_RABBITMQ_VHOST	нет	"co"	Имя виртуального хоста rabbitmq на стороне PGS

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
PREGEN_HTTP_SOCKET_TIMEOUT_MILLIS	нет	-1	Таймаут соединения с сервисом PREGEN через HAPROXY, если определен и меньше значения HAPROXY_HTTP_TIMEOUT_MILLIS
PREGEN_NODEJS_OPTS	нет	""	Дополнительные опции Node.js сервиса PREGEN, рекомендуется значение `--optimize_for_size` для инсталляций, ограниченных по памяти на серверах из секции `[pregen]`
PREGEN_QUEUE_HIGH	нет	100	Длина очереди высокоприоритетных задач сервиса PREGEN
PREGEN_QUEUE_LOW	нет	100	Длина очереди низкоприоритетных задач сервиса PREGEN
PREGEN_WORKERS_HIGH	нет	10	Количество воркеров (параллельных обработчиков) высокоприоритетных задач сервиса PREGEN
PREGEN_WORKERS_LOW	нет	10	Количество воркеров (параллельных обработчиков) низкоприоритетных задач сервиса PREGEN
PREGEN_WORKER_MAX_MEM	нет	2048	Количество памяти, доступной каждому воркеру в сервисе PREGEN, мегабайт.
PRESENTATION_EDITOR_DISABLED	нет	true	Флаг запрещения работы редактора презентаций.
PRIVATE_DOMAINS	нет	[]	Список доменов, сертификаты для которых выкачиваются из Artifactory, только для разработки!
PRIVATE_REGISTRY_HOST	да	co-private-registry	Имя хоста приватной Docker Registry, используемой для инсталляции
PRIVATE_REGISTRY_IMAGE	да	registry	Тег образа приватной Docker Registry, используемой для инсталляции
PRIVATE_REGISTRY_PASSWORD	да	нет	Пароль для Registry в открытом виде.
PRIVATE_REGISTRY_PORT	да	5000	Порт приватной Docker Registry, используемой для инсталляции
PRIVATE_REGISTRY_USERNAME	да	couser	Логин приватной Docker Registry, используемой для инсталляции
RABBITMQ_DIST_PORT	нет	25672	Порт межсервисного взаимодействия tcp протокола сервиса RabbitMQ на серверах с ролью `[mq]`
RABBITMQ_EPMD_PORT	нет	4369	Порт Erlang кластеризации EPMD tcp протокола сервиса RabbitMQ на серверах с ролью `[mq]`
RABBITMQ_LOG_LEVEL	нет	info	Уровень логирования сервисов RabbitMQ. Используемые значения: `debug` (максимум), `info`, `warning`, `error` (минимум) или `none` (отключение логирования)

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
RABBITMQ_FEDERATION_ENABLED	нет	false	Флаг включения федерации rabbitmq
RABBITMQ_LOG_MESSAGES_LIMIT	нет	200	Максимальное количество лог сообщений в секунду на одном узле RabbitMQ (при превышении лимита сообщения отбрасываются)
RABBITMQ_MNG_PORT	нет	15672	Порт веб интерфейса http протокола сервиса RabbitMQ на серверах с ролью [mq]
RABBITMQ_NODE_PORT	нет	5672	Порт клиентского взаимодействия tcp протокола AMQP сервиса RabbitMQ на серверах с ролью [mq]
RABBITMQ_PASSWORD	да	нет	Пароль для сервиса (API, веб интерфейс) RabbitMQ
RABBITMQ_USERNAME	да	couser	Логин для сервиса (API, веб интерфейс) RabbitMQ
RABBITMQ_VHOST	нет	co	Виртуальный хост RabbitMQ
REDIS_LOG_LEVEL	нет	info	Уровень логирования сервисов Redis. Используемые значения: debug (максимум), verbose, notice, warning (минимум)
REDIS_MS_PORT	нет	6379	Порт клиентского взаимодействия tcp протокола RESP сервиса Redis на серверах с ролью [mq]
REDIS_PASSWORD	да	нет	Пароль для Redis AUTH на серверах с ролью [mq]
REDIS_SENTINEL_NAME_IMC	нет	imc	Имя базы Redis для мониторинга через Redis Sentinel на серверах с ролью [mq]
REDIS_SENTINEL_QUORUM	нет	2	Минимальное количество Redis Sentinel сервисов для принятия решения об изменении статуса мастера Redis на серверах с ролью [mq]
REDIS_SEN_PORT	нет	26379	Порт клиентского взаимодействия tcp протокола RESP сервиса Redis Sentinel на серверах с ролями [mq], [core_*]
REGISTRATION_ENABLED	нет	true	Флаг включения возможности регистрации новых пользователей через веб интерфейс Auth/SSO
SDD_DU_ENABLED	нет	true	Флаг отключения режима пула DU
SELINUX_ENABLED	нет	false	Флаг включения поддержки SELinux (экспериментально)
SWAP_ENABLED	нет	false	Флаг использования swap файла для поддержки работы с пулом DU повышенного размера (экспериментально)
SYSTEM_TIMEZONE	да	Etc/GMT-3	Устанавливает часовой пояс системы на каждом сервере инсталляции
UPGRADE_KERNEL	нет	false	Флаг включения режима обновления ядра до версии 4.4 LTS (используется ядро из elrepo.org)

13. Приложение 2. Запуск интегрированных тестов

После завершения предварительной проверки подсистемы CO, при наличии работающих инсталляций PGS и (опционально) PSN, необходимо запустить интеграционные тесты.

Тесты должны быть запущены с сервера установки.

13.1. Настройка параметров скрипта запуска интеграционных тестов

Параметры скрипта запуска интеграционных тестов `~/install_co/run_integration.sh` передаются через переменные окружения. Их значения должны соответствовать параметрам данной инсталляции. Некоторые примеры значений параметров указаны в скрипте.

Обязательные параметры:

- `ETCD_BROWSER_URL` — полный адрес (URL) сервиса Etcd Browser на узле с ролью `[service]`.
- `ETCD_BROWSER_USERNAME` — имя пользователя etcd-browser.
- `ETCD_BROWSER_PASSWORD` — пароль для etcd-browser.
- `SUPER_ADMIN` — логин суперадмина PGS (для создания тестовых тенантов и их админов).
- `SUPER_PASSWORD` — пароль суперадмина PGS.
- `MAIL_DOMAIN` — почтовый домен инсталляции, без `@`.
- `PGS_POINT` — полный адрес (URL) PGS сервиса Euclid API.

Опциональные параметры:

- `TAG_INTEGRATION` — тег образа Docker контейнера с интеграционными тестами.
- `DOCKER_REGISTRY` — адрес (FQDN и опционально порт) Docker Registry, где располагается указанный в `TAG_INTEGRATION` образ.
- `REGISTRY_USERNAME` — логин в указанный Docker Registry.
- `REGISTRY_PASSWORD` — пароль в указанный Docker Registry.
- `ACCOUNT_NAME` — префикс имени домена создаваемого тенанта, не должен содержать `.` или `_`.
- `PASSWORD` — пароль создаваемого администратора тенанта и всех создаваемых пользователей.
- `TESTSET` — набор тестов, используются следующие наборы:
  - `fast` — очистка простых аккаунтов, запуск интеграционных тестов (используется по умолчанию);
  - `all` — пересоздание простых и корпоративных аккаунтов, запуск интеграционных тестов;
- `SSL_IGNORE` — игнорировать невалидные или самоподписанные SSL сертификаты.
- `MAX_WAIT` — максимальное время ожидания асинхронных операций в секундах.
- `LOG_OUT` — путь к лог файлу ошибок тестов.
- `INFO_LOG_OUT` — логировать в файл вместо stdout.
- `LOG_LEVEL` — уровень логирования (debug info warn error).
- `DNS` — адрес непубличного DNS сервера для закрытой инсталляции.
- `TENANT_ADMIN` — полный логин админа тенанта в виде `<логин>@<домен-тенанта>[.<окружение>].<домен-инсталляции>`. Например, `admin@test-deploy.mrt.myoffice.ru`. Поддомен не должен содержать символы `.` и `_`. Тенант и пользователи в нём будут созданы перед тестовым прого-

ном.

Если передан параметр `TENANT_ADMIN`, переменные `MAIL_DOMAIN` и `ACCOUNT_NAME` игнорируются.

13.2. Пример запуска интеграционных тестов

```
export ETCD_BROWSER_URL=http://10.0.0.1:8001
export ETCD_BROWSER_USERNAME=user
export ETCD_BROWSER_PASSWORD=pass
export SUPER_ADMIN=pgs
export SUPER_PASSWORD=pgs_pass
export MAIL_DOMAIN=example.com
export PGS_POINT=https://pgs.example.com/adminapi
./run_integration.sh
```

14. Приложение 3. Настройка подсистем CO

Настройка параметров конфигурации подсистем CO производится через Web-интерфейс Etcd Browser по адресу `http://<локальный-адрес-сервера>:8001` с использованием логина и пароля, настроенных в разделе 5.5. Адрес сервера берется из указанного в группе `[service]` инвентарного файла.

Изменение параметров производится в ветке `/nct/co/<внутренняя версия релиза CO>/config`. После модификации одного или нескольких параметров, изменения можно применить, нажав кнопку Send в правом верхнем углу страницы.

Добавление или удаление параметров применяется сразу, без нажатия кнопки Send. После изменения параметров конфигурации может происходить перезапуск зависимых сервисов, что в свою очередь может вызвать недоступность системы на некоторое время.

По соображениям безопасности доступ к данному порту должен быть ограничен локальным хостом и внутренними (приватными) сетями с адресами по стандарту RFC1918. Категорически запрещается открывать доступ к нему из публичных сетей.

14.1. Настройка доступных языков

Настройка доступных языков (локализаций) в UI веб приложений (language switcher) осуществляется путем изменения параметра `config/wfe/branding/excluded.locales.json` в Etcd. Часть языков (из имеющихся в дистрибутиве локализаций) не доступна пользователю, следующие локализации нет возможности выбрать в UI по умолчанию:

```
["zh-CN", "ar-AR", "hi-IN", "ja-JP"]
```

Список всех локазизаций, включенных в дистрибутив, можно узнать в параметре `config/wfe/branding/available.languages.json` в Etcd.

14.2. Настройка лендинга и меню быстрого запуска

Настройка доступных для запуска иконок приложений (appswitcher) на странице лендинга Auth/SSO и в меню быстрого запуска (quicklaunch) осуществляется путем изменения параметров `config/wfe/appswitcher.landing.json` и `config/wfe/appswitcher.quicklaunch.json` в Etcd. По умолчанию это список всех доступных приложений в инсталляции, смотри также параметры в разделах 5.14, 5.15, которые ограничивают данный список.

Массив `order` управляет порядком появления иконки приложения в списке. Ключ `main` указывает на главную (большую) иконку на лендинге.

appswitcher.landing.json

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

appswitcher.quicklaunch.json

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

14.3. Настройка отправки системных писем-нотификаций

Для отправки системных писем-нотификаций (приветственного письма, письма о смене или восстановлении пароля, и т.п.), требуется внешний по отношению к CO сервис SMTP. Это может быть SMTP сервис внутри PSN, или внешний сервис заказчика инсталляции или администратора тенанта. Этот же сервис будет использоваться (при соответствующих настройках) для отправки отзывов пользователей для службы поддержки (support feedback). Настройка параметров сервиса SMTP (а также сертификатов ЕСИА и адресов саппорта) осуществляется в пользовательском интерфейсе администратора тенанта инсталляции (тенанта, владеющего доменом инсталляции по умолчанию) после завершения инсталляций CO и PGS. Эти настройки могут быть при необходимости в дальнейшем изменены. В случае настройки собственного сервиса SMTP администратором любого другого тенанта, пользователи этого тенанта будут получать системные письма-нотификации от указанного в настройках их тенанта адреса (если тенант пользователя можно определить из контекста обращения), или от адреса из настроек тенанта инсталляции (если тенант пользователя заранее не известен, например запрос на сброс пароля при обращении на домен инсталляции, а не кастомный домен тенанта).

Для корректной отсылки писем-нотификаций следует убедиться, что все необходимые параметры FS AppAPI сконфигурированы, а со стороны PGS настроен механизм обращения по виртуальному ip SSO при изменении настроек тенанта и при необходимости отправки системного письма. Получение настроек тенанта на стороне SSO можно проверить в Etcd по адресу `tenants/<id тенанта>`, для тенанта с доменом инсталляции это будет `tenants/default`.

14.4. Настройка авторизации через ЕСИА

Прежде, чем получить возможность авторизации в ЕСИА через production-сервера госуслуг, необходимо проверить и подтвердить работоспособность системы в песочнице. Подробные руководства о действиях, которые

необходимо выполнить на стороне ЕСИА:

- https://sc.minsvyaz.ru/media/docs/esiametodicheskierekomendatsii2-8.pdf
- http://docplayer.ru/70981722-Esia-instrukciya-po-rabote-s-testovoy-sredoy-1-4.html

В результате этих действий администратору инсталляции (и, возможно, администраторам отдельных тенантов) передаются сгенерированные и зарегистрированные сертификат, ключ и идентификатор системы в тестовой среде (контуре) ЕСИА.

Предварительные настройки параметров ЕСИА (до начала деплоя) описаны в разделе 5.7. По умолчанию используются только параметры, имеющие отношение к тестовой среде. Если в пользовательском интерфейсе администратора тенанта инсталляции (и любого другого тенанта, в котором нужна поддержка авторизации через ЕСИА) все сконфигурировано правильно (разрешена ЕСИА на уровне инсталляции, введены сертификат, ключ и идентификатор), должен заработать функционал авторизации через тестовую среду ЕСИА. После необходимых проверок инсталляции (привязки и отвязки тестовых аккаунтов ЕСИА к пользователям тенантов, выполнения входа в систему через ЕСИА и т.п.), администраторам инсталляции и тенантов необходимо получить сертификат, ключ и идентификатор для продуктивной среды, и заменить их в пользовательском интерфейсе администратора тенанта инсталляции (и других тенантов).

До изменения настроек необходимо отвязать ранее привязанные аккаунты пользователей от ЕСИА, если в дальнейшем планируется их использование в production.

После этого, в Etcd необходимо изменить следующие url на production:

- `config/wfe/authentication.esia.test.ac_url=https://esia.gosuslugi.ru/aas/oauth2/ac`
- `config/wfe/authentication.esia.test.rs_url=https://esia.gosuslugi.ru/rs`
- `config/wfe/authentication.esia.test.te_url=https://esia.gosuslugi.ru/aas/oauth2/te`

Это изменение приведет к переключению всей инсталляции на продуктивный контур ЕСИА. На данный момент нет возможности переключать отдельные тенанты и иметь тестовые/продуктивные тенанты в инсталляции одновременно.

14.5. Настройка ротации логов в ElasticSearch

Начиная с релиза Mint (2018.02), по умолчанию индексы логов, сохраняемых через ElasticSearch, не удаляются при деплое с очисткой рабочей директории (`-e CLEANUP=true`). Полностью удалить старые логи можно при деплое, использовав опцию `-e CLEANUP_ES=true` вместо `-e CLEANUP=true`.

Для предотвращения переполнения диска во время эксплуатации, по умолчанию логи старше 120 дней автоматически удаляются (по cron, с использованием плагина Curator для ES). Это значение (в днях) можно задать опцией `ES_INDEX_RETENTION_PERIOD_DAYS` при деплое, или изменить в дальнейшем на машине с ролью `log` в `/opt/co/systemd/systemd-env` переменную `ES_INDEX_RETENTION_PERIOD_DAYS` и рестартовать сервис:

```
systemctl restart fluentd-server
```