Руководство по установке

Сервер совместного редактирования (ССР) МойОфис

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

«Сервер совместного редактирования (ССР) МойОфис»

РУКОВОДСТВО ПО УСТАНОВКЕ

2.3

На 47 листах

Москва

2022

Содержание

1. Общие сведения . . . 9
   1.1. Назначение . . . 9
   1.2. Требования к квалификации персонала . . . 9
   1.3. Системные требования . . . 10
   1.4. Ограничения . . . 10
      1.4.1. Ограничения при выполнении установки на оборудовании без поддержки отказоустойчивости . . . 10
      1.4.2. Ограничение при выполнении кластерной установки . . . 10
      1.4.3. Ограничение по работе с подсистемой управления конфигурациями . . . 10
      1.4.4. Ограничение по работе с системами виртуализации . . . 11
   1.5. Рекомендации . . . 11
      1.5.1. Рекомендации по использованию файловых систем . . . 11
      1.5.2. Рекомендации по версии ядра Linux . . . 11
      1.5.3. Рекомендации по разбивке дисков . . . 11
      1.5.4. Рекомендуемая версия python . . . 11
      1.5.5. Рекомендуемые зависимости python . . . 11
2. Типовые схемы установки «Сервер совместного редактирования (ССР) МойОфис» . . . 12
   2.1. Конфигурация без отказоустойчивости . . . 12
   2.2. Кластерная отказоустойчивая конфигурация . . . 12
   2.3. Типовая схема масштабирования . . . 12
3. Первичная установка . . . 13
   3.1. Состав дистрибутива . . . 13
4. Подготовка к установке . . . 13
   4.1. Описание ролей . . . 13
   4.2. Подготовка инфраструктуры установки . . . 14
      4.2.1. Проверка и подготовка инсталляционных архивов . . . 15
   4.3. Общие настройки системы . . . 15
   4.4. Настройки системы в "закрытом периметре" . . . 16
   4.5. Настройка основных параметров установки . . . 16
      4.5.1. Расположение примеров конфигурационных файлов . . . 16
      4.5.2. Конфигурирование инвентарного файла . . . 16
      4.5.3. Конфигурирование параметров инсталляции . . . 17
      4.5.4. Конфигурирование приватных параметров . . . 17
      4.5.5. Конфигурирование авторизации для системных сервисов . . . 17
      4.5.6. Конфигурирование сертификатов . . . 18
      4.5.7. Конфигурирование ГОСТ сертификатов . . . 19
   4.6. Настройка дополнительных параметров установки . . . 19
      4.6.1. Добавление доверенных сертификатов . . . 19
      4.6.2. Конфигурирование NTP серверов . . . 20
      4.6.3. Конфигурирование дополнительных серверов для логирования . . . 20
      4.6.4. Дополнительная настройка политики ротации логов . . . 20
      4.6.5. Система синхронизации файлов CDN между хостами . . . 20
      4.6.6. Включение поддержки SELinux . . . 21
      4.6.7. Настройка префиксов виртуальных хостов . . . 21
      4.6.8. Конфигурирование DNS серверов . . . 21

4.6.9. Отключение возможности копирования контента документов во внешний буфер обмена . . . 21
4.6.10. Интеграция по протоколу WOPI . . . 22
4.6.11. Настройка пула DU . . . 22
4.7. Настройка межсетевого экранирования . . . 22
4.8. Настройка удаленного доступа . . . 23
5. Установка «МойОфис Документы» . . . 23
5.1. Конфигурация без отказоустойчивости . . . 23
5.1.1. Запуск установки . . . 23
5.2. Кластерная отказоустойчивая конфигурация . . . 24
5.2.1. Запуск установки . . . 24
5.2.2. Проверка корректности установки . . . 24
6. Обновление с предыдущих версий . . . 25
6.1. Состав дистрибутива . . . 25
7. Подготовка к обновлению . . . 25
7.1. Описание ролей . . . 25
7.2. Проверка и настройка инфраструктуры установки . . . 25
7.2.1. Проверка и настройка основных параметров установки . . . 25
7.2.2. Проверка и настройка дополнительных параметров установки . . . 25
7.2.3. Проверка и настройка межсетевого экранирования . . . 25
7.2.4. Проверка и настройка разграничения доступа . . . 25
7.2.5. Проверка и настройка удаленного доступа . . . 25
7.2.6. Создание резервных копий . . . 25
8. Обновление «МойОфис Документы» . . . 25
8.1. Конфигурация без отказоустойчивости . . . 25
8.1.1. Запуск обновления . . . 25
8.1.2. Проверка корректности обновления . . . 26
8.2. Кластерная отказоустойчивая конфигурация . . . 26
8.2.1. Масштабирование конфигурации . . . 26
8.2.2. Запуск обновления . . . 26
8.2.3. Загрузка обновлений CDN . . . 26
8.2.4. Создание бандла . . . 26
8.2.5. Загрузка CDN бандла через Manage API . . . 26
9. Дополнительные возможности и рекомендации по установке . . . 28
9.1. Настройка мониторинга состояния . . . 28
9.2. Диагностика состояния подсистем СО . . . 28
9.2.1. Сбор сведений оборудования . . . 28
9.2.2. Диагностика состояния nginx . . . 28
9.2.3. Диагностика состояния lsyncd . . . 29
9.2.4. Диагностика состояния rabbitmq . . . 29
9.2.5. Диагностика состояния haproxy . . . 29
10. Техническая поддержка . . . 30
10.1. Системные сообщения . . . 30
10.2. Известные проблемы и способы решения . . . 30
10.2.1. Проблемы, вызванные ошибками аллокатора памяти ядра Linux . . . 30
Описание проблемы . . . 30
Решение . . . 30
10.2.2. Проблема при установке на ноды с ограниченными ресурсами . . . 30

Описание проблемы . . . 30
Решение . . . 31
11. Приложение 1. Дополнительные опции и параметры развёртывания . . . 33
11.1. Формирование CDN бандла . . . 45
11.2. Описание полей в ключе `wfe/appswitcher.apps.json` . . . 45
12. Приложение 3. Настройка подсистем СО . . . 47
12.1. Настройка доступных языков . . . 47
12.2. Настройка ротации логов в ElasticSearch . . . 47

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**
API	Application Programming Interface, интерфейс программирования приложений
CA	Certificate Authority, удостоверяющий центр для подтверждения подлинности ключей шифрования
CDN	Content Delivery Network, сеть доставки содержимого
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
ETCD	Распределенная система хранения конфигурации
FQDN	Fully Qualified Domain Name, полностью определённое имя домена
Inventory file	Инвентарный файл Ansible с перечислением ролей и их IP адресов
IPVS	IP Virtual Server
JKS	Java Key Store, хранилище ключей и сертификатов, доступных виртуальной машине Java
JSON	JavaScript Object Notation
JVM	Java Virtual Machine
LO	LibreOffice, фильтры которого используются для импортирования устаревших бинарных форматов документов
NPS	Native Process Service, сервис управления нативными процессами (например, конвертацией)
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

Сокращение, термин	Расшифровка и определение
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

- Должен быть установлен один из следующих поддерживаемых дистрибутивов операционной системы:
  - Centos 7.9
  - Astra Linux Орел 2.12.43
  - ALT Linux 9.0

	CPU	**RAM (GB)**	**Disk (GB)**	**Network**
минимальные	Intel Xeon E5	16	50 HDD	1Gbit/s
рекомендуемые	Intel Xeon E5 или выше	24	250 SSD * 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.	10Gbit/s

Для обеспечения функциональности клиентского доступа экземпляр «Сервер совместного редактирования (ССР) 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 «МойОфис Документы». **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 «МойОфис Документы»:

- 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. Типовые схемы установки «Сервер совместного редактирования (ССР) МойОфис»

2.1. 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).

2.2. 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.

2.3. 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 «Сервер совместного редактирования (ССР) 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

3. Первичная установка

3.1. Состав дистрибутива

В состав дистрибутива входит программное обеспечение «МойОфис Документы». 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 «МойОфис Документы».

4. Подготовка к установке

4.1. 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.
common	Создание необходимых директорий, генерация сертификатов.	Общая роль.
config	Заполнение общих настроек в Etcd, развёртывание сервиса confd.	Общая роль.
core-cu-pool	Развёртывание сервиса SDD-CU, запуск пула CU в Docker.	
core-cvm	Развёртывание сервисов CVM/JOD/NPS в Docker. Запуск пула CU.	
core-dcm	Развёртывание сервиса DCM в Docker. Запуск пула DU.	
core-du-pool	Развёртывание сервиса SDD-DU, запуск пула DU в Docker.	
core-jod	Развёртывание сервиса JOD в Docker.	
core-nm	Развёртывание сервиса NM в Docker.	
docker	Установка сервиса Docker.	Общая роль.
etcd	Развёртывание сервиса etcd в Docker.	Общая роль.
fluentd-agent	Развёртывание сервиса Fluentd в Docker.	Общая роль.

Наименование роли	Расшифровка и определение	Примечание
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.	

4.2. Подготовка инфраструктуры установки

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

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 рекомендованных ОС).

На все хосты, выделенные под инсталляцию «Сервер совместного редактирования (ССР) 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).

4.2.1. 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/
```

4.3. Общие настройки системы

1. Настроить имя хоста, параметры сети.
2. Настроить имя хоста, параметры сети, включая специальные требования для входного IPVS балансировщика:
    - 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 ресолвится и доступен:

- **SMTP** сервер (`smtp[-<DOMAIN_ENV>].<DOMAIN_NAME>` используемый в настройках формы обратной связи в свойствах тенанта).

3. Создать записи в DNS:
   - `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>`

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

4.4. Настройки системы в "закрытом периметре"

В случае установки «Сервер совместного редактирования (ССР) 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!

4.5. Настройка основных параметров установки

4.5.1. 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`

4.5.2. 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 развер-

нуто 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.

Нельзя разносить на разные виртуальные сервера `core-dcm` и `core-du-pool`. Должны устанавливаться на одни и те же хосты. Аналогичное требование предъявляется к ролям `core-cvm` и `core-cu-pool`.

4.5.3. Конфигурирование параметров инсталляции

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

- `DOMAIN_NAME` — необходимо раскомментировать строку и изменить значение параметра на требуемый, например `DOMAIN_NAME: "example.com"`.
- `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`.

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

4.5.4. 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:

- Параметр `ERLANG_COOKIE`
- Параметр `CRYPTO_PRO_LICENSE` (в случае использования дистрибутива с поддержкой ГОСТ шифрования, и наличии лицензии "КриптоПро CSP")

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

4.5.5. 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
`CO_MANAGE_API_PASSWORD`	Пароль пользователя для доступа к CO Manage API

Имя	Значение
ERLANG_COOKIE	уникальная строка (секрет) для кластеризации RabbitMQ, длиной от 1 до 255 символов (латинских букв или цифр)
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.

4.5.6. 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.

4.5.7. 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.

4.6. Настройка дополнительных параметров установки

4.6.1. Добавление доверенных сертификатов

Данный подраздел опционален.

В случае использования в окружении самоподписанных сертификатов или собственного центра сертификации (CA), необходимо перед началом деплоя поместить собственные корневые и доверенные сертификаты в формате **PEM** в директорию `certificates/custom-ca/` в плейбуках. Во время деплоя эти сертификаты

(файлы с расширением **pem** или **crt**) будут скопированы на узлы кластера.

Для включения этой функциональности необходимо добавить опцию `-e CUSTOM_CA=true` при запуске инсталляционного скрипта (смотри также Приложение 1).

4.6.2. 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"
```

4.6.3. 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`

4.6.4. 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`.

4.6.5. 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`.

4.6.6. 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!

4.6.7. Настройка префиксов виртуальных хостов

Данный подраздел опционален.

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

- `CDN_PREFIX` префикс адреса CDN
- `COAPI_PREFIX` префикс адреса COAPI
- `DOCS_PREFIX` префикс адреса приложения редакторов

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

Записи в DNS должны соответствовать новым префиксам.

4.6.8. 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"
```

4.6.9. 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}`

4.6.10. Интеграция по протоколу WOPI

При интеграции внешнего хранилища с редакторами по протоколу WOPI (https://en.wikipedia.org/wiki/Web_Application_Open_Platform_Interface) сервис NM не задействован, поэтому группа ролей `core_nm`, в инвентори должны быть пустые.

Некоторые другие компоненты «Сервер совместного редактирования (ССР) 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_*
- 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/officeonline.

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.

Также при возникновении ситуации, в которой в режиме просмотра документа копирование выделенного текста не работает, нужно предоставить iframe доступ к Clipboard API следующим образом: `<iframe src="editor_url" allow="clipboard-read; clipboard-write"></iframe>`

4.6.11. 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` 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.

4.7. 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)

4.8. 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: []
```

5. Установка «МойОфис Документы»

5.1. Конфигурация без отказоустойчивости

5.1.1. 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 CO будут запущены автоматически.

5.2. Кластерная отказоустойчивая конфигурация

5.2.1. 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.

5.2.2. Проверка корректности установки

Аналогична проверке конфигурации без отказоустойчивости.

6. Обновление с предыдущих версий

Процесс обновления «Сервер совместного редактирования (ССР) МойОфис» полностью аналогичен процессу первичной установки.

6.1. Состав дистрибутива

Состав дистрибутива приведен в п. 4.1.

7. Подготовка к обновлению

7.1. Описание ролей

Описание ролей приведено в п. 5.1.

7.2. Проверка и настройка инфраструктуры установки

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

7.2.1. Проверка и настройка основных параметров установки

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

7.2.2. Проверка и настройка дополнительных параметров установки

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

7.2.3. Проверка и настройка межсетевого экранирования

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

7.2.4. Проверка и настройка разграничения доступа

Поддерживается SELinux. Дополнительной настройки не требуется.

7.2.5. Проверка и настройка удаленного доступа

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

7.2.6. Создание резервных копий

В процессе работы на хостах «МойОфис Документы» не хранятся персистентно данные пользователя, поэтому создания резервных копий не требуется.

8. Обновление «МойОфис Документы»

8.1. Конфигурация без отказоустойчивости

8.1.1. Запуск обновления

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

8.1.2. Проверка корректности обновления

Проверка обновления аналогична проверке установки, описанной в п. 6.1.2

8.2. Кластерная отказоустойчивая конфигурация

8.2.1. Масштабирование конфигурации

Процесс масштабирования аналогичен приведенному в п. 3.3.

8.2.2. Запуск обновления

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

8.2.3. 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.

8.2.4. Создание бандла

Описание правил формирования и создания бандла содержится в Приложении 1.

8.2.5. 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>`.

9. Дополнительные возможности и рекомендации по установке

9.1. Настройка мониторинга состояния

Не поддерживается в данном релизе.

9.2. Диагностика состояния подсистем CO

9.2.1. 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**).

9.2.2. 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.

9.2.3. 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`.

9.2.4. 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.

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.

9.2.5. 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.

10. 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.

10.1. Системные сообщения

10.2. 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).

10.2.1. 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.

10.2.2. 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.

11. 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
ANALYTICS_ENABLED	нет	true	Флаг включения посылки сообщений аналитики в Fluentd агент (локально)
AUDIT_ENABLED	нет	false	Флаг включения/отключения аудита
AUDIT_SYSLOG_HOST	нет	нет	Имя хоста системы сбора событий информационной безопасности. События передаются в формате syslog
AUDIT_SYSLOG_PORT	нет	нет	Порт для приема данных системой сбора событий информационной безопасности
AUDIT_SYSLOG_SOCKET_TYPE	нет	нет	Протокол передачи данных в систему сбора событий информационной безопасности (tcp, udp)
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`)
CDN_RELEASE_HASH	да	нет	Определяет часть URL в CDN для идентификации данного релиза
CHANNEL_MAX	нет	2047	Максимально допустимое количество каналов в кластере RabbitMQ для согласования с клиентами. Значение 0 означает «неограниченный». Использование большего количества каналов увеличивает объем памяти брокера
COAPI_HTTP_SOCKET_TIMEOUT_MILLIS	нет	-1	Таймаут соединения с сервисом COAPI через HAPROXY, если определен и меньше значения HAPROXY_HTTP_TIMEOUT_MILLIS

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
`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
`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_DU_USE_NATIVE`	нет	`false`	Флаг включения режима пула DU
`CU_EXECUTION_TIMEOUT_DEFAULT`	нет	`30s`	Таймаут операции конвертации, запускаемому через NPS.
`CU_EXECUTION_TIMEOUT_HEAVY`	нет	`30s`	Таймаут операции конвертации, запускаемому через продвинутый NPS.
`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)

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
CU_MAX_MEM_DEFAULT	нет	512mb	Количество памяти, доступной отдельному контейнеру конвертации, запускаемому через NPS, указанных единиц памяти.
CU_MAX_MEM_HEAVY	нет	1gb	Количество памяти, доступной отдельному продвинутому контейнеру конвертации, запускаемому через NPS, указанных единиц памяти.
CU_POOL_SIZE	нет	4/10	Размер пула CU на серверах в секции [core_cu_pool]
CVM_CONVERSION_QUEUE_CONSUMERS_MAX	нет	-1	Количество консьюмеров CVM (влияет на количество процессов CU, по умолчанию равно RABBITMQ_CONSUMERS_COUNT_MULTIPLICATOR*vCPU)
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	700000	Таймаут соединения с сервисом CVM через HAPROXY, если определен
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_NOTIFICATIONS_QUEUE_CONSUMERS_MAX	нет	-1	Количество консьюмеров DCM (влияет на количество обрабатываемых сообщений от DU, по умолчанию равно RABBITMQ_CONSUMERS_COUNT_MULTIPLICATOR*vCPU)
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
DEV_NGINX	нет	false	Флаг включения режима разработки серверных компонент Nginx

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
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_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
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_MEM_DEFAULT	нет	750mb	Количество памяти, доступной отдельному контейнеру DU, запускаемому через NPS, указанных единиц памяти.
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_MIN	нет	40/100	Размер пула DU в случае CU_DU_USE_NATIVE=false на серверах в секции [core_du_pool] или начальный размер пула DU в противном случае Для изменения этого значения после деплоя с CU_DU_USE_NATIVE=false следует использовать Etcd ключ /nct/co/<release-version>/config/nps-du/du.PoolSize, или ключ /nct/co/<release-version>/config/dcm/dcm.du.native.duPoolSize в противном случае.
ERLANG_COOKIE	да	нет	Разделяемый секрет для взаимодействия Erlang процессов в кластере RabbitMQ (алфавитно-цифровая строка в кодировке Latin1 от 1 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
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_FLUSH_THREADS	нет	2/8	Число тредов fluentd плагина, пишуших в ElasticSearch. Увеличение может быть необходимо при использовании более производительного внешнего кластера ES
ES_FLUSH_WORKERS	нет	2/8	Число тредов fluentd плагина, пишуших в ElasticSearch. Увеличение может быть необходимо при использовании более производительного внешнего кластера ES
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]
ETCD_BROWSER_USERNAME	да	couser	Пользователь для авторизации в веб приложении Etcd Browser на сервере с ролью [service]

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
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]
FLUENTD_AGENT_PORT_MONITOR	нет	24220	Порт мониторинга состояния Fluentd-агента (только внутри Docker контейнера)

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
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
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_SYSLOG_SEVERITY	нет	info	Уровень логирования от HAProxy. При большом внутреннем трафике рекомендуется использовать error или выше
HAPROXY_HTTP_TIMEOUT_MILLIS	нет	90000	Общий таймаут соединения с сервисом COAPI 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_TCP_SYSLOG_SEVERITY	нет	warning	Уровень логирования от HAProxy. При большом внутреннем трафике рекомендуется использовать error или выше

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
HAPROXY_USERNAME	да	couser	Пользователь для авторизации в веб-интерфейсе HAProxy
INFLUX_ADMIN_ENABLED	нет	true	Флаг включения администрирования базы событий Influx внутренней системы мониторинга (не установлена по умолчанию), только для разработки!
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	4	Количество процессов LibreOffice, запускаемых каждым сервисом JOD. Их увеличение необходимо только для обработки большого числа документов устаревших бинарных офисных форматов (doc, xls, ppt)
JOD_MAX_CONNECTIONS	нет	200	Максимальное количество одновременных исходящих REST запросов с одного узла CVM к JOD-сервису
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

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) При высокой нагрузке рекомендуется повысить до warning
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_CONNECTIONS	нет	200	Максимальное количество одновременных исходящих REST запросов с одного узла DCM, CVM к NPS-сервисам
NM_NOTIFICATIONS_QUEUE_CONSUMERS_MAX	нет	-1	Количество консьюмеров NM (влияет на количество обрабатываемых сообщений, которые далее передаются пользователям, по умолчанию равно RABBITMQ_CONSUMERS_COUNT_MULTIPLICATOR*vCPU)
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). В случае деплоя кластерной роли lb_core_auth на машину с большим числом ядер, необходимо ограничить это значение до 4-8 максимум
PREGEN_HTTP_SOCKET_TIMEOUT_MILLIS	нет	720000	Таймаут соединения с сервисом PREGEN через HAPROXY, если определен
PREGEN_MAX_CONNECTIONS	нет	200	Максимальное количество одновременных исходящих REST запросов с одного узла DCM, CVM к PREGEN-сервису
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	10	Длина очереди высокоприоритетных задач сервиса PREGEN. Увеличение длины очереди не рекомендуется, возможно только для низкопроизводительного кластера

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
PREGEN_QUEUE_LOW	нет	10	Длина очереди низкоприоритетных задач сервиса PREGEN. Увеличение длины очереди не рекомендуется, возможно только для низкопроизводительного кластера
PREGEN_WORKERS_HIGH	нет	10	Количество воркеров (параллельных обработчиков) высокоприоритетных задач сервиса PREGEN. Увеличение числа воркеров возможно при наличии большого количества ресурсов на серверах с ролью [pregen]
PREGEN_WORKERS_LOW	нет	10	Количество воркеров (параллельных обработчиков) низкоприоритетных (тяжелых, медленных) задач сервиса PREGEN. Увеличение числа воркеров возможно при наличии большого количества ресурсов на серверах с ролью [pregen]
PREGEN_WORKER_MAX_MEM	нет	1024/2048	Максимальное количество памяти, доступной каждому воркеру в сервисе PREGEN, мегабайт. Значение необходимо увеличивать, если размер обрабатываемых документов (например, таблиц) выше среднего
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_CHANNEL_MAX	нет	2047	Максимальное количество каналов в RabbitMQ. Должно быть не менее значения CHANNEL_MAX
RABBITMQ_CONSUMERS_COUNT_MULTIPLICATOR	нет	1	Мультипликатор для расчета количества консьюмеров очередей RabbitMQ у компонентов CVM, DCM, FM, NM. В случае нагруженного кластера с малым числом ядер, следует увеличить до 10
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]

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
RABBITMQ_LOG_LEVEL	нет	info	Уровень логирования сервисов RabbitMQ. Используемые значения: debug (максимум), info, warning, error (минимум) или none (отключение логирования)
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_CLIENT_OUTPUT_BUFFER_LIMIT_NORMAL_HARD_LIMIT	нет	0	Значение hard лимита памяти на Redis для обработки запросов normal клиентов. При высокой нагрузке рекомендуется 2g
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_NORMAL_SOFT_LIMIT	нет	0	Значение soft лимита памяти на Redis для обработки запросов normal клиентов. При высокой нагрузке рекомендуется 1g
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_NORMAL_SOFT_SECONDS	нет	0	Время, в течении которого может быть превышен soft лимит памяти на Redis для обработки запросов normal клиентов. При высокой нагрузке рекомендуется 1200
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_SLAVE_HARD_LIMIT	нет	1g/2g	Значение hard лимита памяти на Redis для обработки запросов slave клиентов
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_SLAVE_SOFT_LIMIT	нет	500m/1g	Значение soft лимита памяти на Redis для обработки запросов slave клиентов
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_SLAVE_SOFT_SECONDS	нет	600	Время, в течении которого может быть превышен soft лимит памяти на Redis для обработки запросов slave клиентов
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_PUBSUB_HARD_LIMIT	нет	1g/2g	Значение hard лимита памяти на Redis для обработки запросов pubsub клиентов
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_PUBSUB_SOFT_LIMIT	нет	500m/1g	Значение soft лимита памяти на Redis для обработки запросов pubsub клиентов

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
REDIS_CLIENT_OUTPUT_BUFFER_LIMIT_PUBSUB_SOFT_SECONDS	нет	600	Время, в течении которого может быть превышен soft лимит памяти на Redis для обработки запросов pubsub клиентов. При высокой нагрузке рекомендуется 300
REDIS_CLUSTER_NODES	нет		Перечень кластерных нод Redis (например host1:6379,host2:6379)
REDIS_CONNECT_TIMEOUT_MILLIS	нет	2000	Максимальное время ожидания подключения к Redis для запросов от CVM DCM NM FM
REDIS_LOG_LEVEL	нет	info	Уровень логирования сервисов Redis. Используемые значения: debug (максимум), verbose, notice, warning (минимум)
REDIS_MAX_CLIENTS	нет	10000	Максимальное количество одновременно подключенных клиентов к Redis
REDIS_MAX_IDLE	нет	50	Максимальное количество idle соединений от CVM DCM NM FM контейнера к Redis
REDIS_MAX_TOTAL	нет	100	Максимальное количество соединений от CVM DCM NM FM контейнера к Redis
REDIS_MIN_IDLE	нет	50	Минимальное количество idle соединений от CVM DCM NM FM контейнера к Redis
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_READ_TIMEOUT_MILLIS	нет	2000	Максимальное время ожидания ответа от Redis для запросов от CVM DCM NM FM
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_*]
REDIS_TIMEOUT	нет	0	Указание закрыть соединение к Redis если оно не используется в течении этого таймаута. 0 для выключения
REDIS_MAX_TOTAL_NGINX	нет	2500	Максимальное количество одновременных соединений от Nginx контейнера до Redis
REDIS_WAIT_CONNECTION_FROM_POOL_TIMEOUT_MILLIS	нет	2000	Максимальное время ожидания получения возможности соединения от CVM DCM FM NM до Redis

Имя параметра	Обязателен	Значение по умолчанию	Описание параметра, возможные значения и ограничения
SELINUX_ENABLED	нет	false	Флаг включения поддержки SELinux (экспериментально)
SERVER_TOMCAT_THREADS_MAX	нет	200/1000	Максимальное количество входящих потоков обработки REST запросов (сервисов CVM DCM NM FM). Увеличение возможно в зависимости от нагрузки на них
SPRING_REDIS_JEDIS_POOL_MAX_ACTIVE	нет	400	Максимальное количество активных соединений с Redis в пуле (сервисов CVM DCM NM FM)
SPRING_REDIS_JEDIS_POOL_MAX_IDLE	нет	200	Максимальное количество неактивных соединений с Redis в пуле (сервисов CVM DCM NM FM)
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)
WOPI_MAX_CONNECTIONS	нет	200	Максимальное количество одновременных исходящих REST запросов с одного узла DCM к WOPI-серверу

11.1. Формирование CDN бандла

За образец принимается файл cdn_bundle.json.

Менять надо только значения (узлы "value"). Ключ `"wfe/appswitcher.quicklaunch.json"` определяет состав и последовательность приложений в выпадающем меню. Меню можно вызвать кликом по логотипу приложения в левом верхнем углу

Ключ `"wfe/appswitcher.landing.json"` определяет состав и последовательность приложений на странице приложений (появляется сразу после входа в систему)

В ключе `"wfe/appswitcher.apps.json"` прописаны урлы к приложениям и можно указать изображение для любого приложения. Ключ appswitcher.quicklaunch.actions.json отвечает за состав быстрых действий.

11.2. Описание полей в ключе `wfe/appswitcher.apps.json`

В поле `value` определены урлы приложений, можно задать иконки приложений. Ключи в списке соответствуют ключам в `"wfe/appswitcher.quicklaunch.json"` и `"wfe/appswitcher.landing.json"`

url

адрес приложения.

title

название приложения (можно указать переводы для нескольких языков).

Обязательное поле для кастомного приложения

iconUrl

путь к иконке приложения внутри бандла, например `"%cdn_base_url%/apps/some.svg"`.

Обязательное поле для кастомного приложения

style

произвольные стили, если необходимы, в формате `jss`.

Необязательное поле

isQuick

флаг отвечающий за то, чтобы приложение попало в «быстрые действия» (quick actions). Укажите его значение, как "true"

Необязательное поле

Все ключи и значения (кроме `key` и `value`) должны быть в двойных кавычках `""`, которые экранированы обратным слешем "\", например: `\"wfm\":{\"url\":\"//files-domain3.domain2.domain1\"}`

12. 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.

12.1. 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.

12.2. 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
```