МойОфис®

Частное облако

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

МойОфис Частное Облако

МойОфис Логос

РУКОВОДСТВО ПО УСТАНОВКЕ

2019.03

На 19 листах

Москва

2019

Содержание

1. Перечень сокращений, терминов и определений

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 форматов документов на базе кода Core

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

FS
: FileStorage, Хранилище

FQDN
: Fully Qualified Domain Name, полностью определённое имя домена

Inventory file
: Инвентарный файл Ansible к 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

Landing
: Стартовая страница

LDAP
: Lightweight Directory Access Protocol, облегчённый протокол доступа к каталогам

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

2. Системные требования

2.1. Односерверный режим

Применяются следующие требования:

- Может использоваться физический сервер или виртуальная машина.
- Минимальные параметры (девелоперская конфигурация): 8Gb RAM, 100Gb HDD, Intel Core i5 CPU (2 vCPU в случае виртуальной машины).
- Рекомендуемые параметры: 16Gb RAM, 250Gb HDD, Intel Xeon E3 CPU или выше (4 vCPU в случае виртуальной машины).
- Скорость сетевой подсистемы — 1Gbit/s или выше.
- Должен быть установлен один из поддерживаемых дистрибутивов.

2.2. Сервер установки

Применяются следующие требования:

- Может использоваться физический сервер или виртуальная машина.
- Может быть переиспользован сервер задействованный при развёртывании системы CO.
- Минимальные параметры: 8Gb RAM, 100Gb HDD, Intel Core i5 CPU (2 vCPU в случае виртуальной машины).
- Должен быть установлен один из поддерживаемых дистрибутивов.
- С сервера установки должен быть возможен доступ на все хосты кластера под пользователем root или другим пользователем с sudo привилегиями `(ALL=(ALL) NOPASSWD: ALL)`
- На сервере установки должен быть инсталлированы:
  - Пакет Ansible версии 2.8.1 или 2.8.2 (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 2.7+ или Python 3.5+ (рекомендован).
  - 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).

Чтобы иметь возможность производить установку через SSH, используя пароль, необходимо настроить конфигурацию ssh клиента (ssh_config) следующим образом:

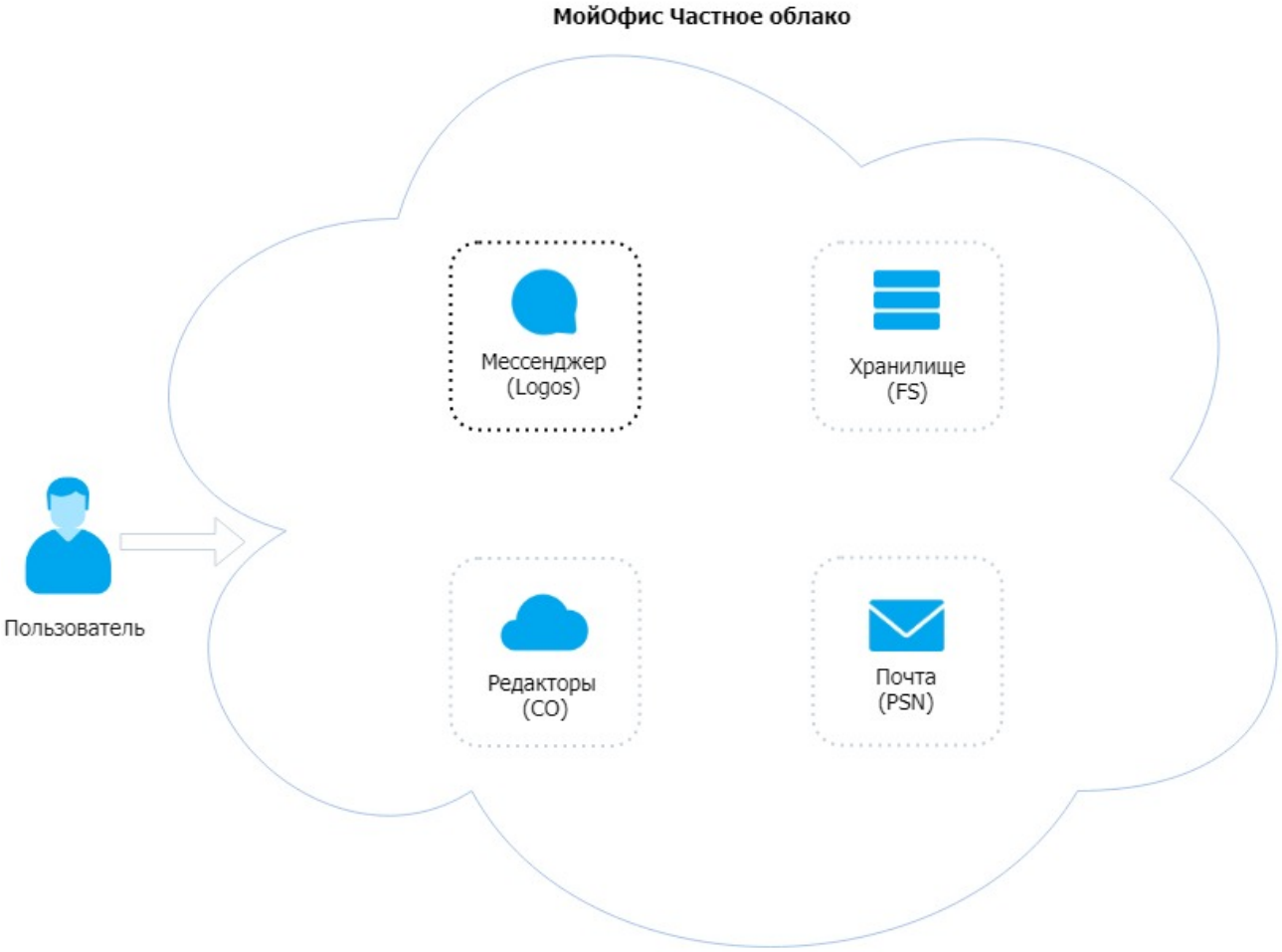
```
StrictHostKeyChecking no
UserKnownHostsFile=/dev/null
```

2.3. Операционная система

Для сервера установки и машин Logos поддерживаются следующие дистрибутивы:

- CentOS 7.5.1804 (рекомендован).
- Astra Linux "Orel" 2.12.
- Alt Linux 8.2.

3. Общая схема МойОфис Частное Облако



4. Подготовка целевой операционной системы

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

В случае возникновения проблем во время деплоя рекомендуется установка на "чистую" систему или использование параметра деплоя `-e CLEANUP=true`.

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).

Необходимо инсталлировать минимальный серверный вариант операционной системы одной из рекомендованных версий.

4.1. CentOS

- Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, https://mirror.yandex.ru/centos/7.5.1804/isos/x86_64/CentOS-7-x86_64-Minimal-1804.iso
- Произвести установку в минимальном варианте.

4.2. Astra Linux

- Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, https://mirrors.edge.kernel.org/astra/stable/orel/iso/orel-current.iso
- Произвести установку в минимальном варианте.

4.3. Alt Linux

- Скачать образ дистрибутива рекомендованной версии с одного из официальных зеркал, например, http://ftp.basealt.ru/pub/distributions/ALTLinux/p8/images/server/alt-8-server-x86_64.iso
- Произвести установку в минимальном варианте.

4.4. Общие настройки системы

1. Настроить имя хоста, параметры сети.
    - Процесс развертывания автоматически добавит на целевой машине следующие параметры в `sysctl.conf` и выполнит их применение через `sysctl -p`:

```
net.ipv4.tcp_keepalive_time = 600
net.ipv4.tcp_keepalive_intvl = 60
net.ipv4.tcp_keepalive_probes = 3
```

2. Убедиться, что ресолвятся и доступны:
    - **Card API** сервер (`cardapi[-<DOMAIN_ENV>].<DOMAIN_NAME>` или другой, указанный в параметре FS_CARD_URL).
    - **FS App API** (`appapi[-<DOMAIN_ENV>].<DOMAIN_NAME>`, или другой, указанный в параметре `FS_APP_URL`).
    - **DB** сервер указанный в параметре `FS_IMPORT_DB_HOST`

Желательно убедиться, что возможно подключение к базе данных на **DB** сервере с использованием утилиты `psql` и данных, указанных в следующих параметрах:

- **FS_IMPORT_DB_USER**
- **FS_IMPORT_DB_PASS**
- **FS_IMPORT_DB_PORT**
- **FS_IMPORT_DB_DB_NAME**

Установить утилиту `psql` можно по инструкции https://www.postgresql.org/download/linux/redhat/

3. Создать запись в DNS:
    - `logos[-<DOMAIN_ENV>].<DOMAIN_NAME>`, тип `A`, содержит внешний `REAL_IP` адрес

Параметры инсталляции `DOMAIN_ENV`, `DOMAIN_NAME` описаны далее в разделе 5.3.

4.5. Настройки системы в "закрытом периметре"

В случае установки Logos в "закрытом периметре", то есть в локальной сети, не имеющей прямого выхода в Интернет, на всех машинах Logos (кроме сервера установки) 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. 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-Logos-XXXX.XX.XX.tgz"
```

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

```
mkdir -p ~/install_logos/
tar xzf "MyOffice-Logos-XXXX.XX.XX.tgz" -C ~/install_logos/
cd ~/install_logos/
```

6. Настройка сборника скриптов (плейбуков) Ansible

6.1. Расположение примеров конфигурационных файлов

Тип деплоя	Путь к инвентарному файлу
Односерверный режим	`~/install_logos/inventory/standalone`
Односерверный высокодоступный режим	`~/install_logos/inventory/standalone`

6.2. Конфигурирование инвентарного файла

Инвентарный файл (inventory file) содержит логические группы (роли), на которые должен быть поделен сервер.

Для конфигурирования инвентарного файла используется python скрипт `generator.py`. Для корректной работы скрипта необходимо задать имя целевой машины в переменной окружения ANSIBLE_DEPLOY_HOST.

```
export ANSIBLE_DEPLOY_HOST=<target-hostname>
```

6.3. Конфигурирование приватных параметров

Для конфигурирования приватных параметров необходимо скопировать шаблонный файл параметров плейбуков:

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

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

- `FS_CARD_URL` — HTTP URL доступа к адресной книге FS. Необходимо раскомментировать строку и изменить значение параметра на требуемое при инсталляции FS. Параметр должен совпадать с аналогично названным параметром в файлах директории properties CO.
- `FS_APP_URL` — HTTP URL доступа к FS AppAPI. Необходимо раскомментировать строку и изменить значение параметра на требуемое при инсталляции FS. Параметр должен совпадать с аналогично названным параметром в файлах директории properties CO.

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

- `FS_APP_LOGIN` — необходимо раскомментировать строку и задать логин пользователя FS AppAPI (заранее созданного в базе FS).
- `FS_APP_PASS` — необходимо раскомментировать строку и задать пароль (в открытом виде) пользователя FS AppAPI.
- `FS_IMPORT_DB_DB_NAME` — имя базы данных в Postgres DB, указываемое при развёртывании FS.
- `FS_IMPORT_DB_USER` — пользователь для авторизации в указанной базе Postgres DB.
- `FS_IMPORT_DB_PASS` — пароль для авторизации в указанной базе Postgres DB.
- `FS_IMPORT_DB_HOST` — FQDN или VIP сервиса Postgres для импорта данных из FS.
- `FS_IMPORT_DB_PORT` — порт сервиса Postgres для импорта данных из FS.
- `PORTAINER_PASSWORD` — пароль для доступа к сервису portainer.
- `RABBITMQ_USERNAME` — имя пользователя для RabbitMQ.
- `RABBITMQ_PASSWORD` — пароль пользователя RabbitMQ.
- `POSTGRES_USERNAME` — имя пользователя базы данных Postgres в Logos.
- `POSTGRES_PASSWORD` — пароль пользователя базы данных Postgres в Logos.
- `POSTGRES_DATABASE` — имя базы данных Postgres в Logos.
- `DB_HOST` — FQDN или VIP сервиса Postgres собственной базы Logos. При развёртывании в односерверном режиме указать значение `postgres`
- `DB_PORT` — порт сервиса Postgres собственной базы Logos.
- `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`.
- `apns_cert_url` — оставить пустым. Используется для отладки.
- `apns_bundle_id` — ID бандла сертификатов для работы с **APNS**, https://help.swiftic.com/hc/en-us/articles/202916391-Find-Your-App-s-Bundle-ID
- `apns_dev_mode` — оставить `false`. Используется для отладки.
- `apns_cert_pass` — указать пароль к сертификату APNS, если он задан.
- `fcm_sender_id` — ID отправителя в Firebase, https://firebase.google.com/docs/cloud-messaging/concept-options
- `fcm_server_key` — серверный ключ в Firebase
- `fcm_endpoint` — HTTP API адрес сервиса FCM
- `registry_images_dir` — указать "registry"

- `registry_private_hostname` — указать "logos-private-registry"
- `registry_private_port` — указать "5000"
- `registry_image` — указать "registry"
- `registry_tag` — указать "2.6.2"
- `PRIVATE_REGISTRY_USERNAME` — логин для доступа к локальному Docker registry. Задаётся произвольно.
- `PRIVATE_REGISTRY_PASSWORD` — пароль для доступа к локальному Docker registry. Задаётся произвольно.
- `DOCKER_REGISTRY` — оставить неизменным. Содержит адрес и порт, по которому будет доступен локальный репозиторий Docker.
- `REPO_HOSTNAME` — оставить пустым. Используется для отладки.

6.4. Конфигурирование сертификатов

Для конфигурирования сертификатов в директории `~/install_logos/certificates` необходимо создать директорию, соответствующую сконфигурированному имени домена `<DOMAIN_NAME>`, содержащую следующие 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` — (опционально) 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.

- `logosx.p12` — **APNS** сертификат для push-уведомлений iOS, поместить в директорию `~/install_logos/certificates/apns/`.

6.5. Дополнительные параметры для односерверного высокодоступного режима

- `redis_cluster_name` — имя внешнего кластера Redis, например "imc" в CO, https://redis.io/topics/sentinel
- `redis_cluster_master_client_port` — порт мастера внешнего кластера Redis.
- `redis_cluster_master_password` — пароль мастера внешнего кластера Redis.

- `redis_sentinel_cluster_ip_master` — ip адрес текущего мастера внешнего кластера Redis.
- `MQ_HA_HOSTS` — список ip адресов или hostname узлов внешнего кластера RabbitMQ.

7. Инсталляция подсистемы Logos

Порядок инсталляции и тестирования Logos (как части Облачного Офиса) указан в документации по развёртыванию СО.

Для запуска инсталляции подсистемы Logos необходимо запустить скрипты установки Ansible из директории `~/install_logos/`.

7.1. Односерверный режим

```
./ansible-playbook logos.yml -i inventory/standalone -i
inventory/generator.py -t all -u root [дополнительные опции...]
```

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

По умолчанию опция развёртывания `LOG_DRIVER_FLUENTD` содержит значение `true`, что приводит к установке стека **EFK**. При передаче переменной значения `false` логирование будет происходить посредством `journald` (системный журнал).

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 Logos будут запущены автоматически.

7.2. Односерверный высокодоступный режим

Полностью кластерный режим для сервисов Logos еще не поддерживается. В режиме высокой доступности Logos использует внешние кластера сервисов Postgres, RabbitMQ, Redis. Этот режим включается опцией **CLUSTER_MODE=True**

```
./ansible-playbook logos.yml -i inventory/standalone -i
inventory/generator.py -t all -e CLUSTER_MODE=True -u root
[дополнительные опции...]
```

Дополнительные опции аналогичны односерверному режиму.

7.2.1. Подготовка базы для Logos на внешнем кластере Postgres

При первой инсталляции Logos в высокодоступном режиме следует создать новую базу в сервисе Postgres. Для этого необходимо:

1. Создать пользователя, например `logos`, с правами суперпользователя. Его учетные данные должны быть указаны в `POSTGRES_USERNAME`, `POSTGRES_PASSWORD`.
2. Создать новую базу, например `logos`, которой владеет вышеуказанный пользователь. Имя этой базы передается в `POSTGRES_DATABASE`.

7.2.2. Создание виртуального хоста для Logos на внешнем кластере RabbitMQ

При первой инсталляции Logos в высокодоступном режиме следует создать новый виртуальный хост (с именем, указанным в `MQ_VHOST`) в сервисе RabbitMQ. Для этого необходимо выполнить команды:

```
rabbitmqctl add_vhost $MQ_VHOST
rabbitmqctl set_permissions -p $MQ_VHOST $RABBITMQ_USERNAME
```

7.3. Процедура миграции базы данных из Logos версии до релиза Oregano

Резервные копии создаются на машинах с работающей СУБД PostgreSQL (роль DB) следующей командой:

```
PGPASSWORD="lgs_password" pg_dump -U db_lgs_user lgs | ssh
me@backupserver "cat > /backup/fs_oldrelease/lgs.sql"
```

На новой инсталляции производится восстановление резервной копии в СУБД PostgreSQL (роль BE):

```
docker exec -i stolon_fs0_keeper bash -c "PGPASSWORD='lgs_password' psql
-U db_lgs_user -h 172.17.0.1 lgs" < lgs.sql
```

Предварительно необходимо создать такого пользователя в новом сервисе Postgres.