МойОфис®

Частное облако

Руководство по установке

ХРАНИЛИЩЕ (PGS)

ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ»

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Мой Офис Хранилище

Мой Офис Частное облако

РУКОВОДСТВО ПО УСТАНОВКЕ

2020.02

На 17 листах

Москва
2020

Все упомянутые в этом документе названия продуктов, логотипы, торговые марки и товарные знаки принадлежат их владельцам. Товарные знаки «МойОфис» и «MyOffice» принадлежат ООО «НОВЫЕ ОБЛАЧНЫЕ ТЕХНОЛОГИИ».

Ни при каких обстоятельствах нельзя истолковывать любое содержимое настоящего документа как прямое или косвенное предоставление лицензии или права на использование товарных знаков, логотипов или знаков обслуживания, приведенных в нем. Любое несанкционированное использование этих товарных знаков, логотипов или знаков обслуживания без письменного разрешения их правообладателя строго запрещено.

Содержание

Перечень сокращений, терминов и определений

Перечень терминов и определений приведен в таблице 1.

Сокращение, термин	Расшифровка и определение
ПО МойОфис	Программное обеспечение. МойОфис Хранилище. МойОфис Частное облако
PGS	Pythagoras
ОС	Операционная система
БД	База данных
DNS	Domain Name System

Таблица 1. Перечень сокращений, терминов и определений.

1 Общие сведения

1.1 Назначение

Файловое хранилище (далее – Хранилище) входит в состав МойОфис Частное облако. МойОфис Частное облако – продукт для организации виртуальной рабочей среды в государственных организациях и крупных коммерческих предприятиях. Включает редакторы текста, таблиц, презентаций и приложения для управления почтой, календарем и контактами. МойОфис Частное облако позволяет работать в частном облаке на мобильных устройствах и в веб-браузерах.

Подробное описание функций ПО МойОфис приведено в документе «Функциональные возможности МойОфис Частное Облако».

1.2 Требования к квалификации персонала

Администратор МойОфис Хранилище должен соответствовать следующим требованиям:

- Основы сетевого администрирования;
- 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 системой контейнеризации Docker:
- Опыт работы с системой виртуализации VMWare vSphere ESXi 6.5 и выше;
- Опыт работы с командной строкой ОС Linux:
- Знания в объеме курсов RedHat RH124, RH134, RH254
- Знания в объеме, достаточном для сдачи сертифицированного экзамена RedHat EX300;
- Опыт работы со службой доменных имен (DNS);
- Знание основных терминов (DNS, IP-адрес и т.д.);
- Понимание принципов работы DNS серверов (корневые серверы, TLD-серверы, разрешающий сервер имен и т.д);
- Знание основных типов записей DNS;

- Знание видов архитектуры, а так же основных компонентов инфраструктуры открытых ключей (PKI), к которым относятся:
- Закрытый и открытый ключ;
- Сертификат открытого ключа;
- Регистрационный центр (RA);
- Сертификационный центра (CA);
- Хранилище сертификатов (CR);
- Практический опыт администрирования:
    - СУБД ArangoDB
    - GlusterFS
    - Keycloak
    - PostgreSQL
    - ElasticSearch
    - Redis
    - RabbitMQ
    - ETCD
- Опыт работы с системой автоматизации развертывания Ansible;
- Опыт работы со стандартными офисными приложениями;

1.3 Системные требования

1.3.1 Операционная система и ПО:

- Поддерживаются следующие дистрибутивы:
- Centos 7.8 (рекомендуемый дистрибутив)
- AstaLinux Орел
- AltLinux 9.0
- Для всех операционных систем требуется наличие установленного Python версии 3 с модулем pip. Для CentOS - отключенный SELinux.
- Для машины, с которой будет выполнять деплой требуется наличие Ansible 2.9

1.3.2 Конфигурация без отказоустойчивости

	CPU	RAM	HDD (Gb)
Минимальная	8	16	50 + Квота пользователей на использование дискового пространства
Рекомендованная	32	64	100 + Квота пользователей на использование дискового пространства + База данных

Таблица 2. Характеристики конфигурации без отказустойчивости

- Скорость сетевой подсистемы — 1Gbit/s или выше;
- Должен быть установлен один из поддерживаемых дистрибутивов операционной системы.

1.4 Ограничения

- Не допускается в среде виртуализации использовать клонированные виртуальные машины для инсталляции продукта;
- Не допускается копирование установленных операционных систем между физическими серверами или использование образа предустановленной операционной системы для развертывания физических серверов;
- Не допускается оверкоммит ресурсов в среде виртуализации;
- Не допускается использование DHCP-служб в сегменте сети инсталляции

2 Описание архитектуры МойОфис Хранилище

Общая архитектурная схема МойОфис Частное Облако приведена на Рисунке 1.

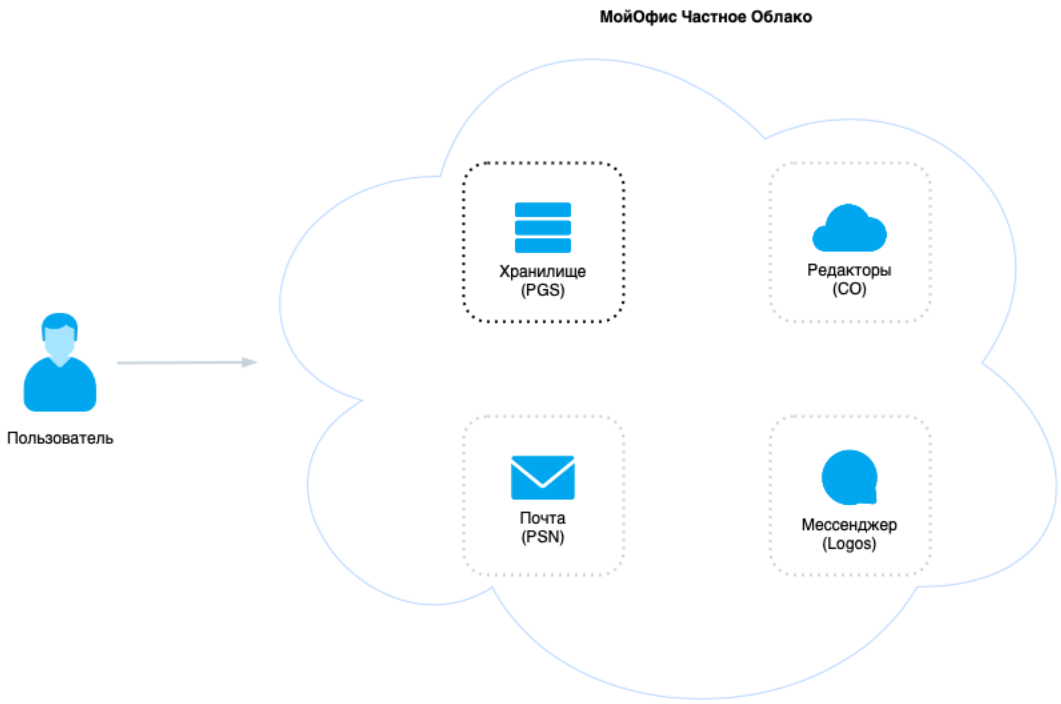

Рисунок 1 – Общая архитектурная схема МойОфис Частное Облако

3 Типовые схемы установки МойОфис Хранилище

3.1 Конфигурация без отказоустойчивости

Базовая или standalone инсталляция – характеризуется тем что все серверные роли развертываются в единственном экземпляре, что не требует установки подсистемы балансировки.

4 Первичная установка

4.1 Состав дистрибутива

Дистрибутив включает в себя:

1. Набор Ansible ролей;

2. Набор контейнеров для запуска хранилища.

4.2 Подготовка к установке

4.2.1 Описание ролей

Инвентарный файл (inventory file) содержит логические группы (роли), на которые будет разделен кластер инсталляции. Файл в формате yaml - https://docs.ansible.com/ansible/latest/reference_appendices/YAMLSyntax.html.

Для определения принадлежности сервера к роли необходимо добавить его доменное имя или IP адрес в соответствующую секцию в шаблоне инвентарного файла. Например:

```
pythagoras:
  hosts:
    host.example.com
```

На релиз 2020.02 существует восемь ролей:

1. Pythagoras – роль, разворачивающая главные сервисы хранилища:
   a. Aristoteles - сервер приложений, обеспечивающий большую часть работы логики ПО;
   b. Euclid - REST API сервис для администрирования ПО;
   c. Sisyphus - Сервис поиска по содержимому документов;
   d. Polemon – сервис веб-администрирования Euclid.
2. Keycloak – SSO сервис;
3. ArangoDB – База данных метаданных файлов;
4. Redis – База данных ключ-значение для неперсистетных данных;
5. RabbitMQ – очередь сообщений;
6. ElasticSearch – поисковая система;

7. Docker-Registry – docker registry сервис для хранения и распространения docker контейнеров;
8. ETCD сервер конфигурации.

Все роли могут быть совмещены на одном сервере. Пример заполнения:

```
all:
  children:
    docker_registry:
      hosts:
        host.example.com
    pythagoras:
      hosts:
        host.example.com
    keycloak:
      hosts:
        host.example.com:
          volume_device_keycloak: "False"
          volume_device_keycloak_path: "/dev/disk/by-uuid/<UUID>"
    arangodb:
      hosts:
        host.example.com:
          volume_device_arangodb: "False"
          volume_device_arangodb_path: "/dev/disk/by-uuid/<UUID>"
    redis:
      hosts:
        host.example.com
    rabbitmq:
      hosts:
        host.example.com
    elasticsearch:
      hosts:
        host.example.com:
          volume_device_elasticsearch: "False"
          volume_device_elasticsearch_path: "/dev/disk/by-uuid/<UUID>"
    etcd:
      hosts:
        host.example.com
```

Обратите внимание на роли keycloak, arangodb, elasticsearch: у этих ролей есть дополнительные переменные volume_device_<role> и volume_device_<role>_path. Заполнение этих переменных (а именно – перевод volume_device_<role> в состояние True и volume_device_<role>_path путь до файловой системы) необходимо при использовании для хранения данных PGS на блочных устройствах, форматированных в xfs. Этот режим является **рекомендуемым**. Особенности работы в режиме volume_device_<role> True:

1. Не допускается использование одного и того же раздела диска на одном сервере (виртуальной машине) для нескольких ролей;
2. Допускается использование для каких-то ролей режима volume_device_<role> True, а для других volume_device_<role> False;
3. Диск должен быть отформатирован в файловую систему xfs и не должен быть смонтирован на момент разворачивания (кроме ситуации повторного запуска).

4.2.2 Подготовка инфраструктуры установки

4.2.2.1 Подготовка сервера, с которого будет производиться инсталляция дистрибутива (оператор)

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

1. После копирования инсталляционного архива проверить его контрольную сумму md5:

```
md5sum -c MyOffice_PGS_XXXX.XX.md5
```

В имени архива цифры версии коммерческого релиза представлены знаками X.

Распаковать содержимое инсталляционного архива в произвольную директорию, и перейти в неё:

```
mkdir install_MyOffice_PGS

tar xf MyOffice_PGS_XXXX.XX.tgz -C install_MyOffice_PGS
cd install_MyOffice_PGS
```

Не рекомендуется распаковывать новый дистрибутив в директорию предыдущей версии.

1. Установить на инфраструктурную машину ansible 2.9;
2. В целях удобства организовать ssh доступ на все сервера с инфраструктурной машины пользователем root.

4.2.2.2 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива. (с доступом в интернет)

При наличии доступа в интернет на целевых машинах фактически никакой подготовки серверов не требуется, все необходимые зависимости предустановятся в рамках работы инсталлятора.

4.2.2.3 Подготовка целевых серверов, на которые будет производиться инсталляция дистрибутива. (без доступа в интернет)

Если целевые машины не имеют доступа в интернет, то необходимо предустановить следующие yum пакеты (названия приведены для centos 7.7):

1. python3
2. libselinux-python3
3. docker-ce (репозиторий https://download.docker.com/linux/centos/docker-ce.repo)
4. docker-ce-cli (репозиторий https://download.docker.com/linux/centos/docker-ce.repo)
5. containerd.io (репозиторий https://download.docker.com/linux/centos/docker-ce.repo)
6. python2-pip
7. rsync

Python pip пакеты:

1. docker
2. passlib
3. bcrypt
4. jsondiff
5. pyyaml

4.3 Заполнение переменных

Необходимые для установки переменные находятся в шаблоне inventory файла:

1. DEFAULT_DOMAIN – домен инсталляции
2. KEYCLOAK_PASSWORD – пароль для пользователя pgs в keycloak (администратор master realm)
3. KEYCLOAK_POSTGRES_PASSWORD – пароль БД postgres (используется как хранилище для keycloak)

4. ARANGODB_PASSWORD – пароль пользователя pgs в arangodb
5. RABBITMQ_PASSWORD – пароль пользователя rabbitmq
6. REDIS_PASSWORD - пароль доступа в redis
7. storage.type – тип хранения файлов, доступны значения fs и s3
8. filesystem.path – пусть до файловой системы хранения, если используется storage.type = fs
9. блок s3 – доступ к хранилищу s3, если используется storage.type = s3
10. co.coapiurl – URL доступа к COAPI, используется приватный адрес, порт по умолчанию 8888
11. блок installation_commons – заполнить весь блок в соответствии с компонентом CO
12. LOGOS_INTEGRATION_ENABLED – включение и выключение интеграции с МойОфис Логос.
13. блок LOGOSDB – параметры базы данных, используемой МойОфис Логос
14. POSEIDON_INTEGRATION - включение и выключение интеграции с МойОфис Почта
15. блок POSEIDON – параметры подключения к МойОфис Почта
16.

4.4 Настройка дополнительных параметров установки

Дополнительные параметры установки находятся в файле group_vars/all.yml. Менять их без согласования с вендором ПО не рекомендуется.

4.5 Настройка межсетевого экранирования

Для корректной работы рекомендуется не использовать сетевое экранирование между серверами. Для доступа к хранилищу «извне» используются порты

1. 8851 – основное API хранилища;
2. 8852 – REST API доступа к администрированию хранилища;
3. 8854 - WEB администрирование хранилища.

4.6 Установка МойОфис Хранилище

4.6.1 Запуск установки

Для запуска установки необходимо выполнить команду

```
./deploy.sh <hosts.yaml> <additional ansible keys>
```

4.6.2 Проверка корректности установки

1. Для проверки корректности установки можно выполнить команду:

```
curl -X POST https://<DEFAULT_DOMAIN>:8851/?cmd=api_version
| python3 -m json.tool
```

Ожидаемый вывод:

```
{
    "response": {
        "API": "4.45.0",
        "WebAPI": "4.32.3",
        "success": "true"
    },
    "success": "true"
}
```

2. Проверить, что все сервисы запущены:

```
docker service ls |grep pgs| awk -v OFS='\t' '{print $2,
$4}' | column -t
```

Ожидаемый вывод:

```
pgs-arangodb_arangodb            1/1
pgs-elasticsearch_elasticsearch  1/1
pgs-etcd_etcd                    1/1
pgs-keycloak_keycloak            1/1
pgs-keycloak_postgres            1/1
pgs-rabbitmq_rabbitmq            1/1
pgs-redis_redis                  1/1
pgs_aristoteles                  1/1
pgs_euclid                       1/1
pgs_polemon                      1/1
pgs_sisyphussearch               1/1
pgs_sisyphusworker               1/1
```

4.6.3 Создание тенанта и пользователей.

Для создания тенанта по умолчанию необходимо воспользоваться REST API Euclid, примеры вызовов:

1. Аутентификация и получение токена:

   Переменная KEYCLOAK_PASSWORD из инвентарного файла.

```
curl -XPOST "<EUCLID_URL:PORT>/auth -d 'username=pgs' -d
'password=${KEYCLOAK_PASSWORD}'
```

2. Создание тенанта:

```
curl --header "Authorization: ${token}" -XPOST
"<EUCLID_URL:PORT>/tenants" -d "default_domain=<Default
Domain>" -d "name=default" -d "admin_password=<Admin
password>" -d "admin_recovery_email=<Recovery Email>" -d
"max_user_count=1000" -d 'max_user_count=1000'
```

После этого можно администрировать тенант пользователем admin@<Default Domain> и паролем <Admin password>, с помощью административного web интерфейса. По умолчанию доступен по адресу https://admin.<domain>:8854

5 Техническая поддержка

Контактная информация службы технической поддержки ООО «Новые облачные технологии» в случае возникновения вопросов, неописанных в данном руководстве:

Адрес электронной почты: support@service.myoffice.ru

Телефон: 8-800-222-1-888.