

Платформа iSpace. Развёртывание и запуск

1 Общая информация

iSpace – это программная платформа, предназначенная для создания no-code бизнес-приложений для автоматизации процессов, а также решения других задач по управлению контентом и организации коллективной работы. iSpace включает в себя базовые функциональные возможности, необходимые для управления контентом, рабочими процессами, безопасностью и пр.

Платформа iSpace построена с использованием свободно распространяемого программного обеспечения. Все используемые в платформе сторонние компоненты входят в перечень программных средств, рекомендованных Минцифры РФ к применению на объектах КИИ.

1.1 Структура платформы

Наиболее полная архитектура развертывания платформы iSpace представлена на рисунке (Рисунок 1), включает в себя балансировку нагрузки между фермами, каждая из которых состоит из сервера приложений и сервера баз данных. Дополнительно логическая архитектура включает в себя аналитическую СУБД для построения аналитических отчетов, сервер индексации и поиска, сервера совместной работы с офисными приложениями, сервера каталога пользователей, сервера авторизации.

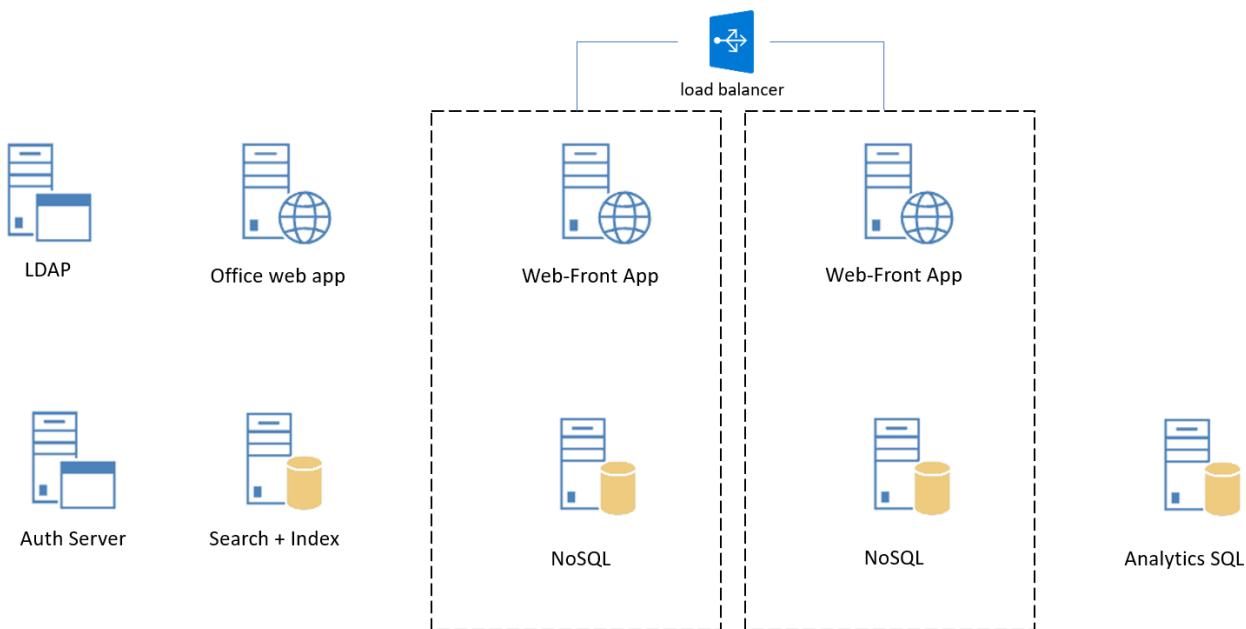


Рисунок 1. Архитектура развертывания высокой доступности

Минимальное развертывание платформы должно производиться на двух-серверной ферме, состоящей из СУБД и сервера приложений.

1.2 Список используемых компонентов

В таблице (Таблица 1) приведены основные модули и компоненты, необходимые для использования платформы iSpace. В зависимости от варианта развертывания некоторые, указанные в таблице (Таблица 1) позиции могут не использоваться.

Таблица 1. Программные модули и компоненты в составе iSpace

№	Тип	Наименование и рекомендуемая версия
1	СУБД NoSQL	Mongo DB, версия 8 или выше
2	Аналитическая СУБД	PostgreSQL, версия 13 или выше
3	Фреймворк	ReactJS, ASP.NET Core
4	Фронт веб-сервер и сервер приложений	Nginx, версия 1.18 или выше
5	Операционная система	Ubuntu (v.20 или выше) или Astra Linux (v.1.7 или выше) или Debian (v.11 или выше) или аналог или Windows (2019 или выше)
6	Поиск и индексация	ElasticSearch (v.8.16 или выше) или OpenSearch
7	LDAP	Microsoft Active Directory или аналог
8	Office Web-app	Мой Офис / P7 Офис / OnlyOffice / LibreOffice / MS Office Online Server или аналог
9	Сервер аутентификации и авторизации	Keycloak, версия 24 или выше
10	Хранилище файлов	S3 MinIO (2024 год или выше) / VK Tech Object Storage или аналог
11	Мониторинг	Prometheus, Logstash, Grafana или аналоги
12	Сервис кэширования	Redis
13	Брокер сообщений	RabbitMQ (v.3.13 или выше)

1.3 Системные требования

Выполнение этих требований обеспечивает производительность системы и создает комфортные условия для работы 100 пользователям при среднем размере файла вложения 1 Мб и общим количеством документов и файлов в хранилище до 100 000. В случае изменения или превышения числа пользователей требования должны быть пересмотрены.

Таблица 2. Требования к серверам

Роль	Процессор	Память	Диски	Сетевые интерфейсы	Кол-во
Фронт веб-сервер (Front-end server) и сервер приложений (Application server)	64-bit, four-core, 2.5 GHz minimum per core Архитектура x64	24..32 GB	100 GB 300 GB	Eth 1Gb	1
Сервер СУБД (возможно использование существующих в организации экземпляров СУБД, удовлетворяющих требованиям)	64-bit, four-core, 2.5 GHz minimum per core Архитектура x64	24..32 GB	100 GB 600 GB	Eth 1Gb	1
Клиентские компьютеры	1 GHz or faster x86/x64 processor with SSE2 instruction set	2..8 Gb	от 20Gb	Eth 100Mbit	N

Интерфейсный веб-сервер и сервер приложений могут быть реализованы в виде виртуальных машин. Сервер СУБД должен быть размещён на физическом сервере с быстрой дисковой подсистемой.

Замечание: Для целей тестирования и разработки допустимо развертывание всех компонент системы на одном сервере.

1.4 Требования к рабочим местам пользователей

На рабочих местах пользователей должны быть установлен Internet-браузер: Google Chrome, Яндекс браузер, MS Edge, Apple Safari, или другие браузеры на Chromium.

У сотрудников, выполняющих работу с документами, должен быть установлен соответствующий офисный пакет.

1.5 Сведения об авторских правах

iSpace лицензируется в соответствии с лицензионным соглашением на программное обеспечение, распространяемым вместе с продуктом. Программное обеспечение можно использовать или копировать только в соответствии с условиями его лицензии.

© 2025 iSpace. Все права защищены.

1.6 Лицензионная политика

Чтобы прочитать лицензионное соглашение, пожалуйста, перейдите по ссылке: <https://ispace-platform/eula>

Политика лицензирования: [iSpace Политика лицензирования](#)

2 Развёртывание

2.1 Предварительная подготовка

Платформа iSpace может быть развернута на одном или нескольких физических или виртуальных серверах в зависимости от планируемой нагрузки, требований к отказоустойчивости и других параметров целевой системы.

Вне зависимости от схемы развертывания необходимо подготовить:

1. Виртуальные машины в необходимом количестве
Параметры виртуальных машин определяются индивидуально для каждого случая.
2. Доступ к серверам
Предоставить доступ ко всем серверам по протоколам SSH. С серверов обеспечить доступ в Интернет на время установки компонент системы.
Минимально должен быть доступен по протоколу HTTPS Docker Hub (<https://hub.docker.com/>) и репозиторий iSpace (<https://repo.ispace-platform.ru>).
3. Учетные записи для развертывания
Учетная запись для развертывания платформы iSpace должна иметь права подключения к серверам по протоколу SSH, быть членом группы docker и иметь права на запись в каталоги для развертывания /var/iSpace (см. раздел 2.2.2 шаги 1-4).
Предоставьте учетной записи права sudo chown и chmod на файлы и каталоги в /var/iSpace

4. Доменные имена

Необходимо определить доменное имя для доступа к iSpace и сделать соответствующую запись в DNS <FQDN>.

Желательно для всех виртуальных машин определить доменные имена в соответствии с внутренними нормативами именования.

5. SSL сертификаты

Для использования протокола HTTPS для доступа к iSpace нужен SSL сертификат (закрытая(*.key) и открытая(*.crt)) часть в формате x509 для выбранного доменного имени <FQDN>.

6. Доступ к LDAP серверу

Для настройки входа пользователей через доменные УЗ нужен ip-адрес контроллера домена, протокол (ldap или ldaps) и порт сервера LDAP. А также логин\пароль учетки, у которой есть доступ к чтению в LDAP и полный путь до OU (группы пользователей), из которой нужно брать пользователей.

7. Доступ к почтовому серверу

Для настройки возможности отправки уведомлений пользователям, необходимо предоставить ip-адрес\порт почтового сервера, учетную запись и пароль, если на почтовом сервере отключена анонимная отправка e-mail

2.2 Установка

Платформа поставляется в виде образов Docker, содержащих в себе все компоненты с уже настроенным окружением и всеми внутренними зависимостями.

Docker — программное обеспечение для автоматизации развёртывания и управления приложениями в среде виртуализации на уровне операционной системы. Суть и одно из предназначений Docker такое же, как и у виртуальных машин — это изоляция работы различных конфликтующих программ внутри одного сервера. Наглядно увидеть отличия между виртуальной машиной и контейнером можно, пройдя по ссылке: [What is a Container?](#)

Таким образом, установка платформы сводится к четырем шагам:

1. Установка Docker Engine и Docker Compose внутри Ubuntu Linux.
2. Загрузка образов в среду Docker.
3. Подготовка скриптов.
4. Запуск готовых Docker сервисов с компонентами платформы с помощью скрипта. В любом варианте развертывания используется режим Docker Swarm и Docker сервисы (а не просто контейнеры). Для подробной информации см. <https://docs.docker.com/engine/swarm/key-concepts>.

2.2.1 Установка Docker и Docker Compose

Установить Docker в соответствии с инструкцией: [Install Docker Engine on Ubuntu](#). Версия должна быть не ниже 20.10.13.

Выполнить настройку Docker по инструкции: [Post-installation steps for Linux](#).

Установить [Docker Compose](#). Warning Версия должна быть не ниже 2.10.2.

Проверьте версию Docker. Проверить версию Docker можно следующими командами:

```
docker --version
```

```
docker compose version
```

Для обновления Docker необходимо выполнить секцию **Upgrade Docker Engine** на странице [Install Docker Engine on Ubuntu](#).

Если в системе присутствует два и более активных сетевых интерфейса (например, один для корпоративной внутренней сети, а второй для выхода в Интернет), то может потребоваться дополнительно инициализировать Docker Swarm и указать желаемый IP (с которого должна работать платформа). Команда для ручной инициализации Docker Swarm:

```
docker swarm init --advertise-addr <ip address>
```

2.2.2 Подготовка к установке

Данные операции необходимо выполнить до развертывания платформы под пользователем root или пользователем, который может выполнять операции sudo.

Шаг 1. Установка производится от имени пользователя, у которого должны быть права на запуск контейнеров docker, для этого включите пользователя в группу docker (если такой группы нет, то создайте ее).

```
/usr/sbin/groupadd docker  
/usr/sbin/usermod -aG docker $USER
```

Шаг 2. Рекомендуется создать группу ispace и включить в нее пользователя, назначить группой по умолчанию

```
/usr/sbin/groupadd ispace  
/usr/sbin/usermod -aG ispace $USER  
/usr/sbin/usermod -g ispace $USER
```

Шаг 3. Настроить автозапуск docker engine

```
systemctl enable docker.service  
systemctl enable containerd.service
```

Шаг 4. Создать папку, в которой будут находиться данный и лог файлы iSpace.

```
mkdir /var/iSpace  
chown $USER:ispace /var/iSpace  
chmod 775 /var/iSpace
```

Шаг 5. Рекомендуется конфигурационные файлы для запуска docker разместить в папке /var/iSpace/docker (далее - \$ISPACE_CONF_DIR). Создадим этот каталог.

Установим переменную только для текущей сессии:

```
export ISPACE_CONF_DIR=/var/iSpace/docker  
mkdir $ISPACE_CONF_DIR  
sudo chown $USER:ispace $ISPACE_CONF_DIR  
chmod 775 $ISPACE_CONF_DIR
```

Шаг 6. Доступ к платформе осуществляется через браузер по доменному имени. Выберите доменное имя для доступа к платформе и сделайте соответствующую запись в DNS.

Шаг 7. По умолчанию доступ к платформе, так же, как и взаимодействие между ее компонентами, осуществляется по протоколу https. Несмотря на то, что можно перенастроить работу по протоколу http это крайне не рекомендуется по соображениям безопасности. Для обеспечения работы по протоколу https необходимо выпустить и предоставить для использования платформой сертификаты SSL.

2.2.3 Системная настройка и запуск

Шаг 8. Распакуйте содержимое файла ispace-deploy-XXXXXX.tar.gz в папке docker

```
cd $ISPACE_CONF_DIR
tar -xzvf /path/to/file/ispace-deploy-XXXXXX.tar.gz
sudo chown -R $USER:ispace $ISPACE_CONF_DIR/*
```

Необходимо разместить в папку `$ISPACE_CONF_DIR/certs` следующие сертификаты (название сертификатов используется для конфигурации платформы, но может быть изменено. Если необходимо изменить имена сертификатов обратитесь в поддержку):

- `tls.crt` – сертификат открытого ключа
- `tls.key` – сертификат закрытого ключа
- `ca-certificates.crt` - CA bundle

Шаг 9. Создайте pfx контейнер для обеспечения безопасного взаимодействия компонент платформы между собой, сохраните пароль (см. раздел Развёртывание и запуск).

```
cd $ISPACE_CONF_DIR/certs
openssl pkcs12 -export -out ispace-platform.pfx -inkey tls.key -in tls.crt
sudo chown -R $USER:ispace $ISPACE_CONF_DIR/*
```

Шаг 10. Для старта платформы необходимо отредактировать несколько конфигурационных файлов:

1. `$ISPACE_CONF_DIR/.env`
 - Указать доменное имя платформы
 - Указать имя администратора, который будет создан при развертывании
 - Указать новые пароли или оставить по-умолчанию
 - Вписать пароль от pfx сертификата созданный на предыдущем шаге в `Kestrel_Endpoints_MyHttpsEndpoint_Certificate_Password`
 - **НЕ СТОИТ ИЗМЕНЯТЬ ДРУГИЕ ПАРАМЕТРЫ**
2. (Если необходимо) Внесите изменения в `$ISPACE_CONF_DIR/keycloak/keycloak_config.env`. Если платформа разворачивается с подключением к существующему серверу Keycloak, то обратитесь в техническую поддержку за рекомендациями по развертыванию.

После выполненных настроек можно приступать к запуску

```
cd $ISPACE_CONF_DIR
./scripts/firstRun.sh
```

По ходу выполнения скрипта будут разворачиваться и запускаться контейнеры, надо будет следить за появлением возможных ошибок и подтверждать продолжение.

Шаг 11. Заполните паспорт подготовленных серверов по шаблону.

Параметр	Значение	Значение
Роль сервера		
Имя сервера/ IP адрес внутренний и внешний		
Кол-во ядер, шт.		
RAM, Gb		
Диски, Gb		
ОС (версия, редакция)		

Системные учетные записи УЗ: назначение		
СУБД (версия, редакция)		
Подключение к Интернет (да/нет)		

2.3 Процедуры после запуска платформы

После запуска платформы необходимо выполнить следующие действия:

1. Проверить, что платформа доступна из браузера по адресу, указанному в конфигурации `.env` и пользователь может в неё зайти
2. Настроить синхронизацию с LDAP сервером организации (см. документацию KeyCloak https://www.keycloak.org/docs/latest/server_admin/index.html#_ldap).

2.3.1 Создание timer-jobs

Данная операция выполняется только один раз. После ее выполнения создаются повторяющаяся задача `UserSynchronizationJob` и `DataUpdateJob`. Все повторяющиеся задачи можно администрировать по адресу https://ispace_host_name:5001/home/timer/dashboard/recurring.

```
cd $ISPACE_CONF_DIR
./scripts/timerjobs_setup.sh
```

2.3.2 Инициализация демо-данными

В состав поставки входят демо-данные для системы. Для их развертывания необходимо выполнить развертывание бэкапа БД Mongo, который расположен в папке `$ISPACE_CONF_DIR/mongodb/Demo_Content.tar.gz`

```
cd $ISPACE_CONF_DIR
sudo rm -rf /var/iSpace/data/mongo/backup/*
sudo tar -xzf mongodb/Demo_Content.tar.gz -C /var/iSpace/data/mongo/backup/
./scripts/mongo_restore.sh
```

Выбрать дату бэкапа (последнюю из доступных), выбрать базу для восстановления – `iSpaceContent`.

2.4 Обновление

Обновление платформы до новой версии заключается в получении и запуске новых версий образов компонент (`docker` контейнеров). Для этого необходимо отредактировать `docker-compose.yml` файл или обновить его новой версией из соответствующего релиза, выполнить необходимые дополнительные операции.

Рекомендуется сначала полностью остановить систему

```
docker-compose down
```

Отредактировать `/var/iSpace/docker/docker-compose.yml` указав новые версии образов.

Следовать инструкции по обновлению (возможно потребуется выполнение дополнительных скриптов для приведения структур данных в соответствие).

Запустить систему.

```
docker-compose up -d
```

2.5 Удаление

В комплект поставки входит скрипт для корректного удаления всех данных платформы. Удаление образов контейнеров производится в соответствии с инструкцией docker.

Для корректного удаления данных платформы необходимо выполнить скрипт

`$ISPACE_CONF_DIR/scripts/cleanup.sh`