

- [Инструкция по установке экземпляра ПО, предоставленного для проведения экспертной проверки](#)

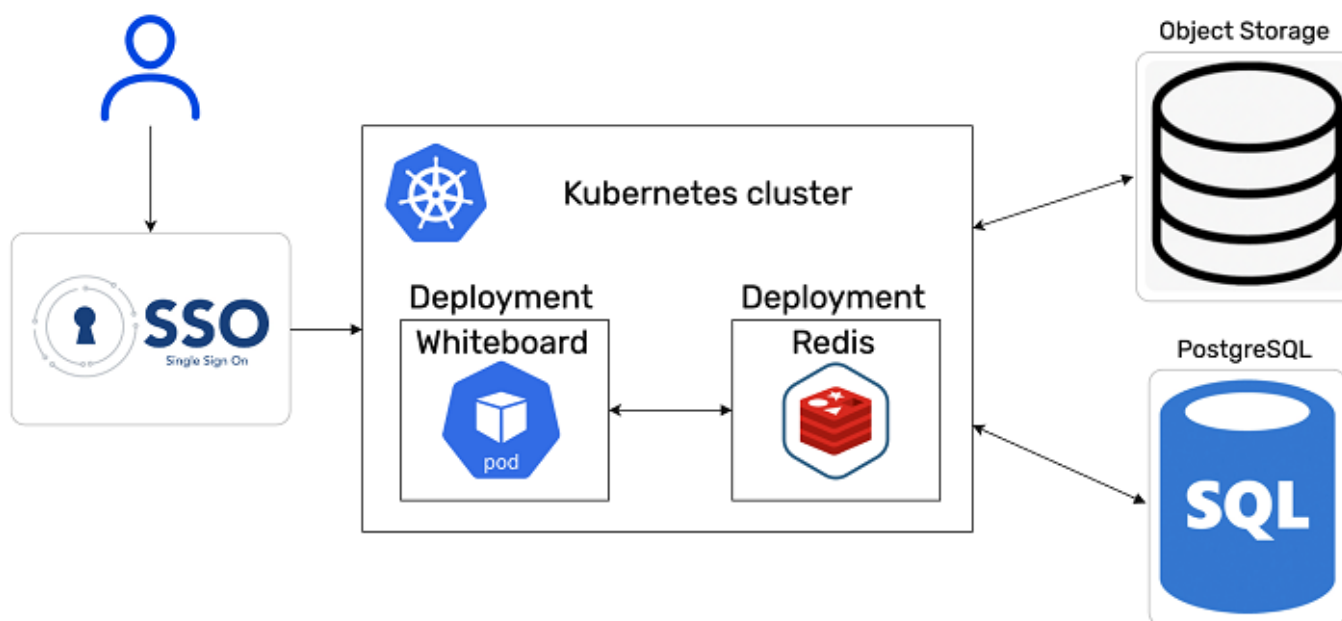
Инструкция по установке экземпляра ПО, предоставленного для проведения экспертной проверки

Установка

Пример развертывания

В статье описано развертывание Яндекс Диска в Kubernetes с помощью менеджера пакетов Helm. В качестве смежных сервисов выбраны СУБД PostgreSQL, система идентификации AD FS, использующая протокол SAML, или Keycloak с поддержкой протокола OpenID для организации единого входа (SSO), а также объектное хранилище Object Storage.

Схема взаимодействия компонентов



Вы можете воспользоваться приведенной ниже конфигурацией с минимальным набором параметров, чтобы протестировать приложение. Если Яндекс Диск подойдет для выполнения ваших задач, приобретите лицензии и разверните аналогичную структуру внутри вашего контура или продолжайте использовать облачный вариант.

Шаг 1. Подготовка к установке

1. Создайте кластер базы данных PostgreSQL.
2. Настройте Object Storage и создайте в нем бакет.
3. Сконфигурируйте сервер вашего провайдера идентификации: SAML (AD FS) или OpenID (Keycloak).
4. Подготовьте данные для задания параметров SSO: SAML (AD FS) или OpenID (Keycloak).
5. Подготовьтесь к работе с Kubernetes:
 - 5.1. Создайте кластер Kubernetes.
 - 5.2. Установите менеджер пакетов Helm.

На macOS это можно сделать при помощи команды:

```
brew install helm
```

Порядок установки на другие системы описан в документации к Helm.

5.3. Зарезервируйте IP-адрес вашего балансировщика нагрузки.

Балансировщик нагрузки используется сервисом для распределения трафика.

5.4. Настройте DNS-запись типа A для вашего домена и укажите в ней IP-адрес балансировщика.

Вы можете создать A-запись:

- В личном кабинете на сайте регистратора — если домен не делегирован на Яндекс.
- В кабинете организации Яндекс 360 для бизнеса — если домен делегирован на Яндекс.

Шаг 2. Получение и настройка пакета Helm

1. Скачайте ZIP-файл с примером пакета Helm и распакуйте архив.

Пакет содержит в себе:

- папку `templates` с шаблонами манифестов Kubernetes;
- файл `chart.yaml` — чарт для развертывания сервиса в Kubernetes;
- файл `values.yaml` со списком конфигурационных параметров.

2. Задайте значения для параметров конфигурации — в текстовом редакторе откройте файл `values.yaml` и отредактируйте его, указав значения параметров в соответствии с комментариями.

Содержание файла `values.yaml`

```
image:
  repository: docker-registry.pruffme.com/disk
  pullPolicy: IfNotPresent

# Первый запуск chart выполняется с --set install=true
install: false

resources:
  limits:
    memory: 6Gi
    cpu: "6"
  requests:
    memory: 512Mi
    cpu: "0.8"

# Сертификат TLS и приватный ключ. Имеют маску по домену
tls:
  crt: |-
    -----BEGIN CERTIFICATE-----
```

```

MII***=
-----END CERTIFICATE-----
key: |-
-----BEGIN PRIVATE KEY-----
MII***=
-----END PRIVATE KEY-----

# Доменное имя, по которому обращаются пользователи
domain: boards.domain.ru

# IP-адрес балансировщика нагрузки
loadBalancerIP: xx.xx.xx.xx

# Ключ лицензии
license: "demo"

# Тип СУБД, используемой в качестве основной (mongodb или postgres)
mainDatabaseType: postgres

# Порты контейнера приложения
ports:
  # Внешний порт, по которому обращаются конечные пользователи приложения
  # (ingress)
  https: 443
  # Внутренний порт, на котором приложение ожидает подключения
  inner: 443

livenessProbe:
  enabled: false
  path: /
  initialDelaySeconds: 30
  periodSeconds: 10
  timeoutSeconds: 5
  failureThreshold: 3
  successThreshold: 1
readinessProbe:
  enabled: false
  path: /
  initialDelaySeconds: 30
  periodSeconds: 10
  timeoutSeconds: 5
  failureThreshold: 5
  successThreshold: 1

# Параметры mongodb, СУБД и pod. Применяются, если mainDatabaseType ==
# mongodb
mongodb:
  # Если используется внешняя СУБД mongodb, установите значение path, а также
  # укажите relatedContainers.mongodb.enabled: false в строке 208
  # Формат path: "mongodb://username:password@disk-mongodb-hostname:27017"
  path: ""

```

```

# Имя базы данных
database: "disk"

# Параметры postgres, СУБД. Применяются, если mainDatabaseType == postgres
postgres:
  user: "pruffme"
  database: "editboard"
  password: "password"
  host: "host.net"
  port: 6432
  max: 20
  idleTimeoutMillis: 300000
  connectionTimeoutMillis: 200000
  maxUses: 7500

# Параметры redis
redis:
  enabled: true
  port: 6379
  pass: ""
  name: "disk-redis"

# Параметры clickhouse
clickhouse:
  enabled: false
  # Установите значение url, если используется внешняя СУБД clickhouse
  # Формат url: "http://disk-clickhouse/"
  url: ""
  # Следующие значения для подключения к СУБД (внешней или внутри pod),
  # создания и настройки pod, создания БД
  ports:
    http: 8123
  database: "pruffme"
  username: "pruffme"
  password: "pruffme"
  flushNumber: 1

# Параметры S3 Object Storage
s3:
  # Версия AWS SDK
  version: 2
  # Идентификатор доступа пользователя. Используется вместе с секретным
  # ключом для аутентификации запросов к хранилищу
  accessKey: "****"
  # Секретный ключ пользователя. Выступает в паре с идентификатором доступа
  # для создания подписанных запросов
  secretKey: "****"
  # Название контейнера, который используется для хранения данных
  bucket: "boards"
  # URL сервиса хранилища
  endpoint: "https://storage.yandexcloud.net"

```

```

# Регион, в котором расположено хранилище
region: "ru-central1"
# Часть URL в начале ссылки на файл. Обычно это путь к bucket
publicPrefix: "https://storage.yandexcloud.net/boards/"
# Параметр, который указывает, нужно ли использовать старый стиль при
формировании пути к объектам в S3
s3ForcePathStyle: false
# Версия API, которую следует использовать при работе с S3
apiVersion: "latest"
# Список расширений файлов, которые поддерживаются для хранения. Позволяет
ограничить типы файлов, которые могут быть загружены пользователями
extensions:
  - "png"
  - "jpeg"
  - "jpg"
  - "pdf"
  - "docx"
  - "doc"
  - "xlsx"
  - "xls"
  - "pptx"
  - "ppt"
  - "mp4"
  - "mp3"
acl: "public-read"

jwtkey: "testtest"

# Список модулей и их параметры
modules:
  test:
    enabled: true
    apiPartner: "test"
    apiKey: "1234567890abcdefgh1234567890abcd"
  sso:
    enabled: true
    moduleType: "sso"
    type: "saml"
    entryPoint: "https://adfs.domain.ru/adfs/ls"
    issuer: "https://boards.domain.ru/sso/"
    cert: "adfs/cert.crt"
    callbackUrl: "https://boards.domain.ru/sso/callback"
    fieldId: "nameID"
    fieldName: "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name"
    exitUrl: "https://boards.domain.ru"
    apiPartner: "sso"
    apiKey: "sso"
  x509:
    createSecret: true
    certificate: |
      -----BEGIN CERTIFICATE-----
      MII***==

```

```
-----END CERTIFICATE-----

admins:
  - "admin@domain.ru"

# Параметры резервных копий диска
dump:
  enabled: false
  # Время ожидания (в часах) после последнего изменения диска, по истечении
  # которого будет сделан снэпшот (моментальный снимок)
  dumpDashboardsWait: 1
  # Время (в часах) после создания последнего снэпшота, по истечении которого
  # будет автоматически создаваться резервная копия
  dumpDashboardsInterval: 6

# Параметры логирования действий во внешние системы
logs:
  enabled: false
  # Путь к файлу, в который будет записываться события из раздела "Журнал
  # событий" в формате CEF
  cefLog: "/home/user/log.cef"
  # Вывод логов в syslog
  syslog:
    ip: "127.0.0.1"
    port: 514
  # Список ID событий, которые не будут фиксироваться в логах
  skiplogs:
    - 11

# Параметры импорта объектов из Miro
miro:
  enabled: false
  # Клиентский номер приложения Miro (https://developers.miro.com/docs/try-
  # out-the-web-sdk)
  clientId: "*****"
  # Секретный ключ приложения
  secret: "*****"
  # Параметр, который задает, нужно ли сохранять в таблицу
  # dashboards_import_tasks_items исходные объекты из Miro
  debug: true

# Данные для создания подов (pods) дополнительных сервисов в Kubernetes
# Указываются, если вы используете эти сервисы при работе с основным
# приложением и если такие поды еще не существуют в вашем контуре
relatedContainers:
  mongodb:
    enabled: false
    # Параметры mongodb для создания pod и подключения к нему
    image: mongodb/mongodb-community-server:6.0-ubi8
    name: disk-mongodb
    port: 27017
```

```

rootPassword: "disk"
username: "disk"
password: "disk"
persistence:
  enabled: true
  storageClass: "standard"
  accessModes:
    - ReadWriteOnce
  size: 10Gi
  pv:
    # persistent volume – создаётся только для локального тестирования
    (например, minikube), размещается на хосте
    create: false
    name: pv-001
    path: "/data/pv-001/"
minio:
  # Параметры minio для создания pod и подключения к нему
  enabled: false
  image: bitnami/minio:latest
  name: "disk-minio"
  storageHostname: storage.disk.test
  rootUser: minio-root-user-disk
  rootPassword: minio-root-insecured-password
  ports:
    api: 9000
    dashboard: 9001
  persistence:
    enabled: true
    storageClass: "standard"
    accessModes:
      - ReadWriteOnce
    size: 10Gi
    pv:
      # persistent volume – создаётся только для локального тестирования
      (например, minikube), размещается на хосте
      create: false
      name: pv-002
      path: "/data/pv-002/"
clickhouse:
  # Параметры clickhouse для создания pod и подключения к нему
  enabled: false
  image: clickhouse/clickhouse-server
  name: "disk-clickhouse"
  persistence:
    enabled: true
    storageClass: "standard"
    accessModes:
      - ReadWriteOnce
    size: 10Gi
    pv:
      # persistent volume – создаётся только для локального тестирования
      (например, minikube), размещается на хосте

```

```
create: false
name: pv-003
path: "/data/pv-003/"

testJob:
  enabled: false
```

Шаг 2. Запуск в режиме установки и конфигурирование

1. Запустите терминал и перейдите в папку с распакованным архивом.
2. Запустите приложение в режиме установки.

На режим установки указывает значение `true` параметра `install`. Запуск можно произвести с помощью команды:

```
helm install disk . --set install=true
```

3. Сконфигурируйте настройки сервера с помощью веб-инсталлятора. Большинство параметров будут предзаполнены на основании данных из файла `values.yaml`.

3.1. Запустите веб-инсталлятор.

Для этого перейдите по ссылке `https://<АДРЕС_СЕРВЕРА_ДИСКА>`, где вместо `<АДРЕС_СЕРВЕРА_ДИСКА>` — укажите адрес сервера Яндекс Диска, который доступен:

- по IP-адресу балансировщика, зарезервированного в п.5.3 на шаге подготовки;
- по домену, к которому вы привязали IP-адрес балансировщика п.5.4 на шаге подготовки.

Подставьте в адрес одно из этих значений.

- 3.2. В окне приветствия нажмите **Далее**.

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

☐ Соединение с БД

☐ Структура БД

☐ Хранилище

☐ Шаблоны

☐ Завершено

Дополнительно

☐ Настройка SSO

☐ Администратор

☐ Завершено

Добро пожаловать в веб-инсталлятор

Программа установки поможет вам настроить подключение к базе данных, s3 хранилищу, SSO и доступ к панели администрирования приложения

В конце базовой, либо после полной настройки приложения, вам будет предоставлена возможность загрузки конфигурационного файла

Более подробно процесс установки и настройки описан в документации

 [Документация](#)

Для продолжения нажмите кнопку "Далее"

ПРЕДУПРЕЖДЕНИЕ: Данная программа защищена законами об авторских правах и международными соглашениями.

Далее

3.3. Выберите базу данных Postgres и нажмите **Далее**.

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

☐ Соединение с БД

☐ Структура БД

☐ Хранилище

☐ Шаблоны

☐ Завершено

Дополнительно

☐ Настройка SSO

☐ Администратор

☐ Завершено

Выбор Основной базы данных

Выберите тип базы данных с которой будет работать приложение. База уже должна быть подготовлена к работе

Postgres

Назад

Далее

3.4. Проверьте параметры подключения к БД и проверьте соединение.

Начало

☒ Приветствие

☐ Основные настройки

☒ Выбор БД

☐ Соединение с БД

☐ Структура БД

☐ Хранилище

☐ Шаблоны

☐ Завершено

Дополнительно

☐ Настройка SSO

☐ Администратор

☐ Завершено

Соединение с базой данных

user

user1

password

database

db1

host

port

6432

☐ Состояние неизвестно

Проверить соединение

Назад

Далее

3.5. Обновите структуру базы данных.

Начало

☒ Приветствие

Основные настройки

☒ Выбор БД

☒ Соединение с БД

☒ Структура БД

☐ Хранилище

☐ Шаблоны

☐ Завершено

Дополнительно

☐ Настройка SSO

☐ Администратор

☐ Завершено

Структура базы данных

☒ Структура БД в порядке

Обновить структуру

Назад

Далее

3.6. Проверьте настройки объектного хранилища.

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

○ Хранилище

○ Шаблоны

○ Завершено

Дополнительно

○ Настройка SSO

○ Администратор

○ Завершено

Настройка файлового хранилища

Выбор Файлового хранилища

S3 хранилище

Префикс ссылки домена

access_key

secret_key

bucket

endpoint

region

ru-central1

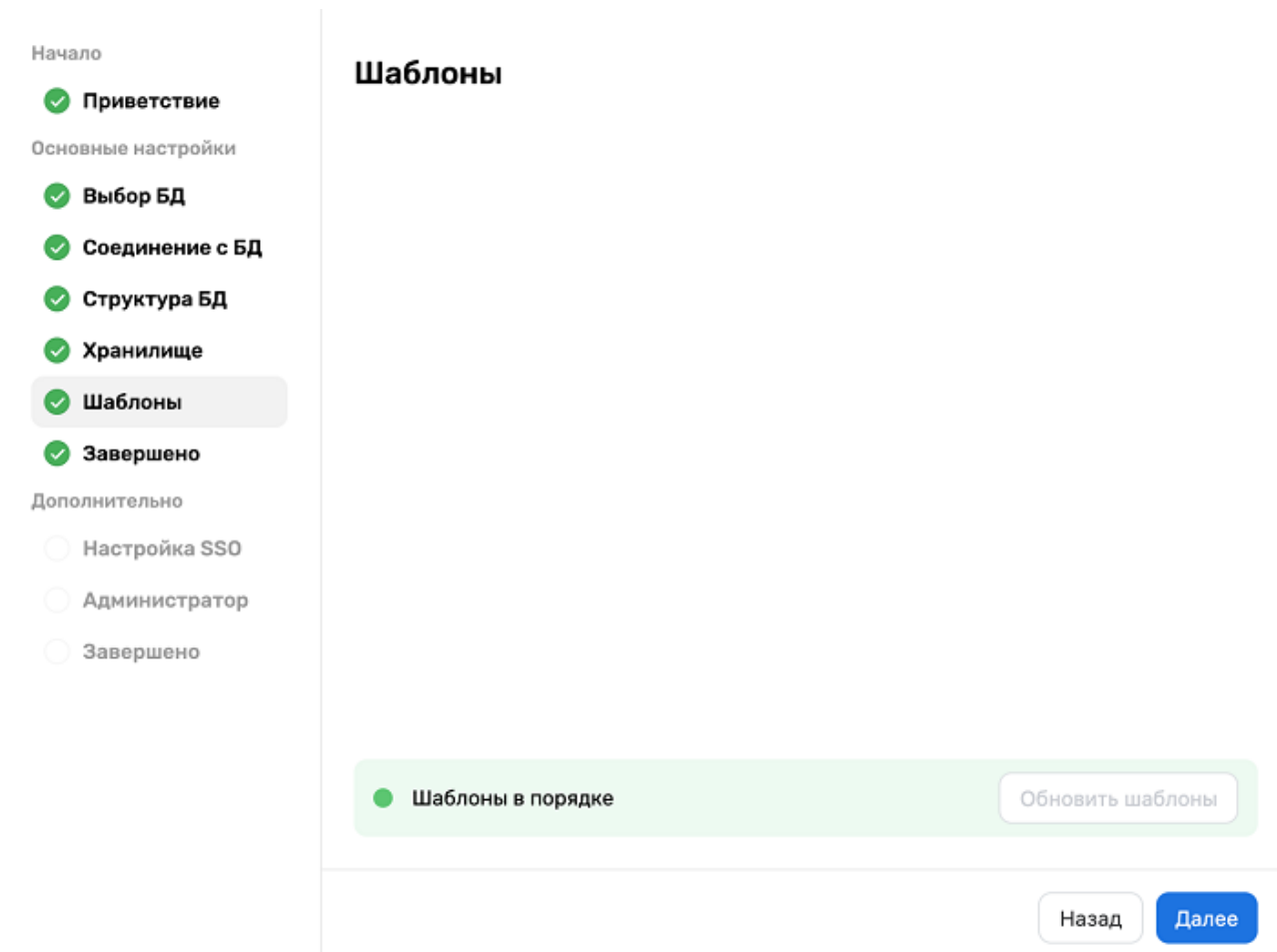
☐ S3(Version 2)

Назад

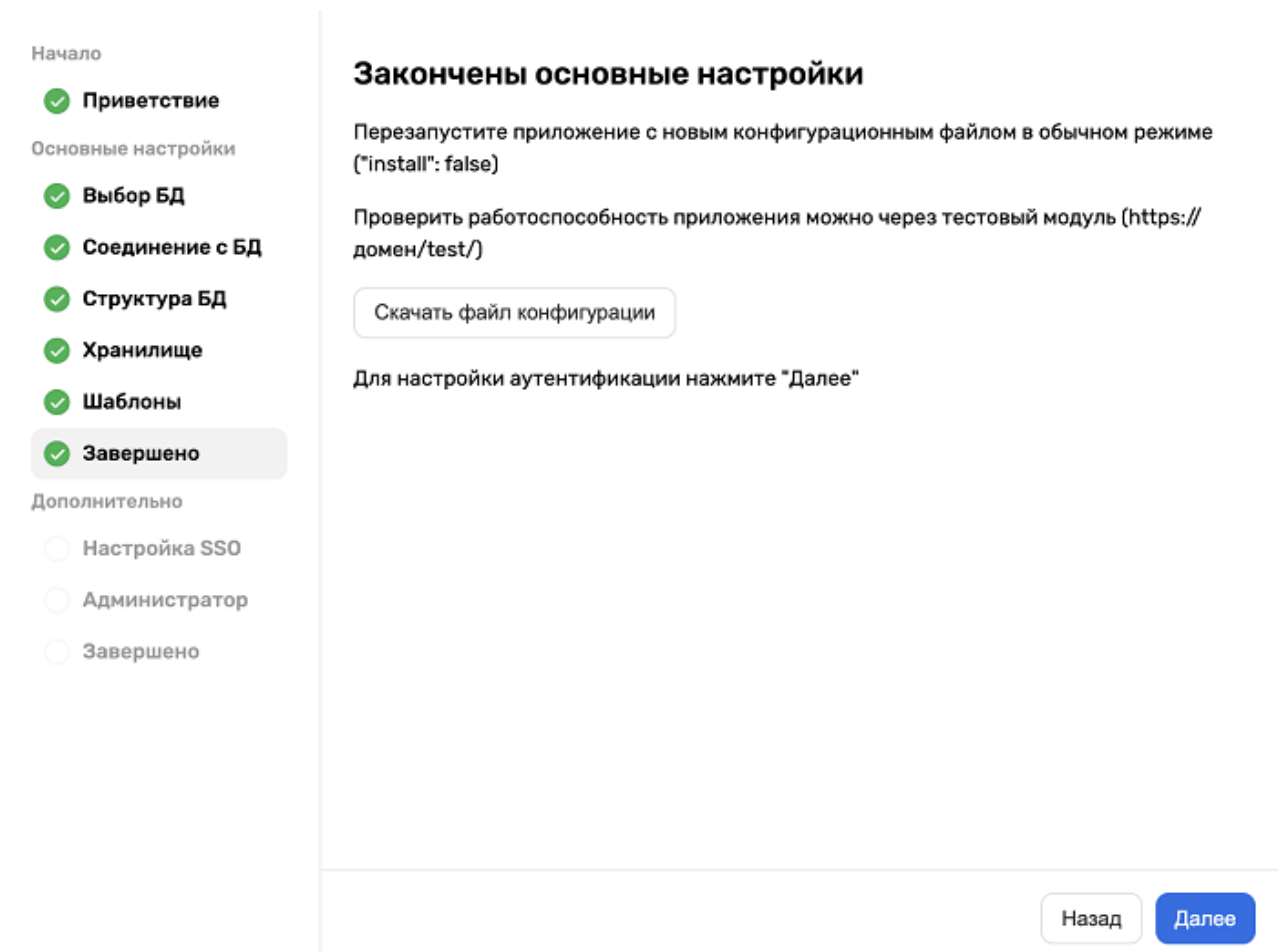
Далее

3.7. Обновите шаблоны.

13



3.8. Подтвердите завершение основной настройки.



3.9. Проверьте параметры SSO.

SAML (AD FS)

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

✓ Хранилище

✓ Шаблоны

✓ Завершено

Дополнительно

☒ Настройка SSO

☐ Администратор

☐ Завершено

Выбор SSO

SAML

entry_point

https://adfs. .ru/adfs/ls

issuer

https:// .ru/sso

callback_url

https:// .ru/sso/callback

Путь к сертификату

adfs/cert.crt

Поле маппинга для логина пользователя

nameID

Поле маппинга для отображаемого имени в приложении

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

Проверить соединение

НазадДалее

OpenID (Keycloak)

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

✓ Хранилище

✓ Шаблоны

✓ Завершено

Дополнительно

✓ Настройка SSO

✓ Администратор

☐ Завершено

Выбор SSO

Open ID

authorization_url

https://[redacted]/realms/[redacted]/protocol/openid-connect/au

token_url

https://[redacted]/realms/[redacted]/protocol/openid-connect/to

client_id

[redacted]

client_secret

[redacted]

callback_url

https://[redacted]/sso/callback

scope

openid profile email

info_url

https://[redacted]/realms/[redacted]/protocol/openid-connect/us

authorization_type

Назад

Далее

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

✓ Хранилище

✓ Шаблоны

✓ Завершено

Дополнительно

✓ Настройка SSO

✓ Администратор

☐ Завершено

client_id

client_secret

callback_url

https:// /sso/callback

scope

openid profile email

info_url

https:// /realms/ /protocol/openid-connect/us

authorization_type

Bearer

Поле маппинга для логина пользователя

email

Поле маппинга для отображаемого имени в приложении

name

SSO настроено успешно

Проверить соединение

Назад

Далее

3.10. Если список администраторов вы задали в файле `values.yaml`, то в окне выбора администратора никаких дополнительных действий совершать не нужно, даже если поле **Логин** пустое.

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

✓ Хранилище

✓ Шаблоны

✓ Завершено

Дополнительно

✓ Настройка SSO

✓ Администратор

☐ Завершено

Выбор администратора

Введите логин администратора, который будет приходить через SSO. Данный пользователь будет иметь доступ к панели администратора

Логин

admin@domain.com

Панель администратора доступна по ссылке <https://домен/cabinet/admin/>

Назад

Далее

3.11. Подтвердите завершение конфигурирования приложения.

Начало

✓ Приветствие

Основные настройки

✓ Выбор БД

✓ Соединение с БД

✓ Структура БД

✓ Хранилище

✓ Шаблоны

✓ Завершено

Дополнительно

✓ Настройка SSO

✓ Администратор

✓ Завершено

Завершено

Настройка завершена.

Дополненный конфигурационный файл приложения доступен для скачивания

Перезапустите приложение с новым конфигурационным файлом в обычном режиме ("install": false)

Скачать файл конфигурации

Шаг 3. Обновление чарта и запуск в основном режиме

1. Обновите существующий чарт в кластере Kubernetes и установите для параметра `install` значение `false` :

```
helm upgrade disk . --set install=false
```

2. Перезапустите приложение.

- 2.1. Получите список всех развертываний (Deployment):

```
kubectl get deploy
```

- 2.2. Перезапустите Deployment приложения Яндекс Диска:

```
kubectl rollout restart deployment/<DEPLOYMENT-NAME>
```

где `<DEPLOYMENT-NAME>` — имя нужного развертывания, например `deployment-disk` .

3. Проверьте работоспособность сконфигурированного приложения.

- Основная версия личного кабинета доступна по ссылке `https://<ВАШ_ДОМЕН>/cabinet/` , где `<ВАШ_ДОМЕН>` — адрес домена, который вы указали в поле `domain` файла `values.yaml`.
- Если по какой-то причине вы не смогли настроить SSO, но при этом хотите проверить работу сервера, то вы можете это сделать при помощи тестового модуля по ссылке `https://<ВАШ_ДОМЕН>/test/` .

Аккаунт

Сервис доступен для внутренних пользователей организации клиента.

Авторизация

Необходимость авторизации

Чтобы пользоваться сервисом, необходимо авторизоваться.

Порядок авторизации

1. Укажите логин в формате `имя_пользователя@домен_организации` .
2. Нажмите **Войти**.
3. После перенаправления в Active Directory Federation Services организации (далее – ADFS) авторизуйтесь в нем с помощью одного из способов, настроенных в ADFS организации. Например, через логин и пароль.

Демонстрация

Целиком архитектуру и код программы готовы продемонстрировать на нашей инфраструктуре в ходе встречи или видеоконференции.

Контактное лицо: gumennikova@yandex-team.ru — Анастасия Гуменникова, Product Owner Яндекс Диска.