

Сведения об установке экземпляра программы

Универсальный выделенный модуль управления персональными данными “Forward PDM”

Forward PDM (Personal Data Management) – Универсальный выделенный модуль управления персональными данными (Personal Data Management) предназначен для изоляции процессов хранения и обработки персональных данных в выделенном защищенном модуле реализующем как установленное законодательством взаимодействие с субъектом персональных данных и оператором, так и процессы обработки персональных данных, логирование производимых с персональными данными операций, а также операции по их отправке в специализированные информационные системы, например в случаях установленных законодательством и проведение верификации путем сравнения с персональными данными, хранящимися в специализированных информационных системах, в том числе государственных.

Модуль позволяет добавить необходимую функциональность к любой информационной системе и организовать работу с персональными данными без передачи их в информационную систему, не предназначенную для работы с персональными данными пользуясь универсальными идентификаторами, не содержащими персональной информации, при этом необходимый доступ к персональным данным осуществляется через предоставление специального интерфейса субъекту персональных данных и оператору.

Использование системы будет максимально полезно для операторов связи и других услуг, служб, осуществляющих обработку персональных данных и т. д., которые хотят получить быструю, надежную и удовлетворяющую требованиям законодательства систему работы с персональными данными. Система поддерживает кластерное масштабирование и может использоваться в распределенных сетях крупных федеральных и региональных компаний, операторов связи и других информационных систем.

Контактная информация: support@fw-t.ru

1 Дистрибутив

1.1 Распространение дистрибутива

Дистрибутив комплекта программ распространяется на физических носителях (USB-flash накопителе) или по ссылке на облачное хранилище.

Дистрибутив формируется для каждого заказчика с учетом технологической экосистемы и необходимых модулей расширения функционала.

Подробная документация поставляется после адаптации системы в процессе внедрения с учетом особенностей кастомизации.

1.2 Содержание дистрибутива

Перечень устанавливаемых компонентов осуществляется в соответствии со спецификацией поставки.

Дистрибутивы поставляются как Docker-образы для каждого микросервиса системы и обеспечивают корректную установку PDM.

В состав дистрибутива входят:

- PDM Service
- Auditor Service.

При необходимости отдельно передаются дополнительные файлы (файлы конфигурации Docker Compose или Kubernetes манифестов, конфигурационные файлы .yaml, .env, values.yaml для Helm).

Помимо Docker-образов, дистрибутив может поставляться в виде архивов .tar для систем, не имеющих доступа к удалённым репозиториям. В этом случае образы загружаются командой:

```
```bash
docker load < <имя_файла>.tar
```

## 2 Порядок установки программного обеспечения

---

Модуль PDM устанавливается из Docker-образов с использованием системы оркестрации контейнеров Kubernetes.

Специалистами Форвард-Телеком проводится групповое обучение специалистов Заказчика по разворачиванию и настройкам системы в целях обеспечения её дальнейшей корректной эксплуатации.

### 2.1 Подготовка к установке

Перед установкой PDM необходимо подготовить инфраструктуру и выполнить следующие предварительные требования.

#### 2.1.1 Подготовка инфраструктуры

- Развернутый и настроенный кластер Kubernetes;
- Наличие сети с изоляцией компонентов или настройка дополнительных механизмов авторизации (SSL-сертификаты) для защиты межсервисного взаимодействия;
- Подключенное и настроенное объектное хранилище, поддерживающее полный Amazon S3 API;
- Развернутый и настроенный экземпляр Keycloak.

#### 2.1.2 Подготовка баз данных

Перед установкой PDM необходимо создать две схемы в PostgreSQL:

- Основная БД для хранения структурированных данных;
- БД аудита для хранения журнала событий.

#### 2.1.3 Настройка Keycloak

Для корректной работы PDM в Keycloak должны быть выполнены следующие настройки:

- Создан realm для PDM;
- Создан клиент (client) для PDM с поддержкой протоколов OAuth 2.0 и OpenID Connect;
- Настроены роли с атрибутом `pdn_role="true"`, в частности:  
personal-data-user  
administrator;  
auditor;  
operator;  
viewer.
- Настроены маппинги атрибутов для ролей:

ActionType (CREATE, READ, READ\_ANONYMOUS, UPDATE, DELETE);

MasterType (тип сущности).

#### **2.1.4 Настройка объектного хранилища S3**

- Создан bucket для хранения файлов документов;
- Сгенерированы ключи доступа (access key и secret key);
- Настроены политики доступа к bucket.

#### **2.1.5 Подготовка Kubernetes**

- Настроен Ingress Controller;
- Настроены StorageClass для постоянного хранения данных;
- Настроены Secrets для хранения чувствительной информации;
- Настроены ConfigMaps.

### **2.2 Установка**

Порядок инсталляции PDM представляет собой последовательное выполнение действий по:

1. Получению Docker-образов компонентов PDM;
2. Конфигурированию Kubernetes;
3. Настройке переменных окружения;
4. Запуску компонентов PDM.

#### **2.2.1 Получение Docker-образа**

При наличии сетевого доступа к GitLab (Container Registry) получить docker-образ и выполнить команду вида:

```
docker pull registry.gitlab.ru/group/project/release:latest
```

#### **2.2.2 Конфигурирование Kubernetes**

Использовать предоставляемые манифесты Kubernetes или создать их на основе шаблонов.

#### **2.2.3 Настройка параметров**

Конфигурация генерируется автоматически в соответствующих директориях.

При необходимости производится настройка параметров окружения:

- Общие настройки;
- Настройки для Keycloak;
- Настройки кэширования.

## 2.2.4 Настроечные параметры сервисов PDM

- Внешние сервисы

Категория	Название	Для сервиса	Название
БД	PostgreSQL	PDM Service	main-db
	PostgreSQL	Auditor Service	audit-db
Identity Provider	Keycloak	PDM Service	keycloak
S3	Любой, поддерживающий полный Amazon S3 API	PDM Service	s3

- PDM Service

Название переменной окружения	Значение
SERVER_PORT	Порт для приложения (8080)
SPRING_DATASOURCE_URL	jdbc:postgresql://main-db:5432/\${DB_POSTGRES_DB}
SPRING_DATASOURCE_USERNAME	\${DB_POSTGRES_USER}
SPRING_DATASOURCE_PASSWORD	\${DB_POSTGRES_PASSWORD}
AWS_ENDPOINT	s3.endpoint
AWS_BUCKETNAME	s3.bucketname
AWS_ACCESSKEY	s3.accessKey
AWS_SECRETKEY	s3.secretKey
AWS_S3_FORCE_PATH_STYLE	true
AWS_REGION	cod
JAVA_TOOL_OPTIONS	
APP_AUDITOR_CONNECTION_INFO	audit-service.hostname (8080)
AUTHORITY_SYNCHRONIZE_ENABLED	Необходимо ли синхронизировать роли с identity provider – true
KEYCLOAK_REALM	keycloak.realmName
KEYCLOAK_SERVER_URL	keycloak.hostname
SPRING_SECURITY_OAUTH2_CLIENT_REGISTRATION_KEYCLOAK_CLIENT_ID	keycloak.client.id

Название переменной окружения	Значение
OTEL_SDK_DISABLED	true

- **Auditor Service**

Название переменной окружения	Значение
SERVER_PORT	Порт для приложения (8080)
SPRING_DATASOURCE_URL	jdbc:postgresql://audit-db:5432/\${AU_POSTGRES_DB}
SPRING_DATASOURCE_USERNAME	\${AU_POSTGRES_USER}
SPRING_DATASOURCE_PASSWORD	\${AU_POSTGRES_PASSWORD}
JAVA_TOOL_OPTIONS	true
OTEL_SDK_DISABLED	true

## 2.2.5 Запуск PDM

Для запуска системы необходимо выполнить развертывание в следующей последовательности:

1. Внешние сервисы:

- БД модуля,
- БД аудита (может быть одна и та же БД),
- Keycloak

2. Основные компоненты PDM в правильном порядке:

Auditor Service и PDM Service и – в результате запуска этих 2 сервисов создается набор необходимых таблиц/последовательностей/прочее в пустой БД (по умолчанию используется схема public);

3. Проверка работоспособности системы.

**ВАЖНО:** Запуск PDM Service будет блокирован в случае недоступности или незавершенной инициализации сервисов предыдущего уровня, а также при невозможности установления сетевого взаимодействия с указанными компонентами.

Примечание: При запуске читаются роли из Keycloak, копируются в локальную БД ПДн и создаётся минимальный набор модификаторов доступа для доменных объектов.

## 2.3 Дополнительные сведения

### 2.3.1 Миграции базы данных

Liquibase-миграции выполняются автоматически при запуске контейнеров сервисов. В логах контейнеров отображаются применённые изменения.

Операции с базой данных выполняются администратором БД.

Управление Docker-контейнерами осуществляется DevOps-специалистами Форвард.

### 2.3.2 Резервное копирование

Рекомендуется настроить регулярное резервное копирование:

- Баз данных PostgreSQL (основной и аудита);
- Объектного хранилища S3;
- Конфигураций Kubernetes.