GS LABS
GS GROUP

Публичный - L0

Система генерации ключей Keys Generation System (KGS)

Руководство по установке

Индекс	KGS-IG
Конфиденциальность	Публичный - L0
Ревизия	1.0
Статус	Согласован

Содержание

1. Аннотация . . . 5
2. Термины и сокращения . . . 6
3. Общие сведения . . . 8
3.1. Назначение . . . 8
3.2. Схема развертывания компонентов . . . 8
3.3. Системные требования . . . 9
3.3.1. FTP server . . . 9
3.3.1.1. Программное обеспечение . . . 9
3.3.1.2. Аппаратное обеспечение . . . 9
3.3.2. Database Server . . . 10
3.3.2.1. Программное обеспечение . . . 10
3.3.2.2. Аппаратное обеспечение . . . 10
3.3.3. Processing Server . . . 10
3.3.3.1. Программное обеспечение . . . 10
3.3.3.2. Аппаратное обеспечение . . . 10
3.3.4. Требования по безопасности . . . 10
3.3.5. Требования к квалификации обслуживающего персонала . . . 10
4. Рекомендации по установке операционных систем . . . 12
4.1. DB Server . . . 12
4.2. Processing Server . . . 12
5. Предварительные действия . . . 13
6. Настройка FTP server . . . 14
6.1. Настройка операционной системы . . . 14
6.1.1. Расширение репозиториев . . . 14
6.1.2. Установка дополнительных утилит . . . 14
6.1.3. Настройка времени/часовых поясов на серверах . . . 15
6.1.4. Настройка NTPDATE . . . 15
6.1.5. Задание имени сервера . . . 15
6.2. Установка и настройка proftp . . . 15
6.3. Создание пользователей и каталогов . . . 16
6.3.1. Общая структура папок, используемая в KGS . . . 16
6.3.2. Структура папок пользователей . . . 16
6.3.3. Исходные пользователи . . . 17
6.3.4. Общий алгоритм создания пользователей и папок на FTP-Server . . . 18
6.3.5. Создание директорий на FTP-Server . . . 18

6.3.6. Создание пользователей на FTP-Server . . . 19
7. Настройка DB Server . . . 20
7.1. Настройка операционной системы . . . 20
7.1.1. Расширение репозиториев . . . 20
7.1.2. Установка дополнительных утилит . . . 20
7.1.3. Проверка наличия локали en_US.utf8 и ru_RU.UTF-8 . . . 21
7.1.4. Настройка времени/часовых поясов на серверах . . . 21
7.1.5. Настройка NTPDATE . . . 21
7.1.6. Настройка фаервола iptables . . . 21
7.1.7. Задание имени сервера . . . 21
7.2. Настройка NFS и монтирование папки бекапов с DB Server на Processing Server . . . 22
7.2.1. Настройка NFS-server на DB Server . . . 22
7.3. Установка и настройка БД . . . 22
7.3.1. Установка PostgreSQL . . . 22
7.3.2. Настройка PostgreSQL . . . 23
7.3.3. Создание директории для Tablespace . . . 23
7.3.4. Редактирование файла по начальному наполнению БД . . . 23
7.3.5. Установка KMI_DB_SCH . . . 23
7.3.6. Установка KMI_DB_API . . . 24
7.4. Установка и настройка компонентов KGS на DB Server . . . 24
7.4.1. Установка и настройка файлов KGS Framework (KMI_FW) . . . 24
7.4.1.1. Установка компонентов на DB Server . . . 24
7.4.1.2. Настройка конфигурационного файла KGS . . . 24
7.4.1.3. Настройка PATH . . . 25
7.5. Проверка автоматического запуска компонентов KGS Framework (KMI_FW) . . . 25
7.5.1. Проверка автоматического запуска KMI_FW_BACKUP . . . 25
7.6. Настройка режима бекапирования СУБД . . . 25
8. Настройка Processing Server . . . 27
8.1. Настройка операционной системы . . . 27
8.1.1. Расширение репозиториев . . . 27
8.1.2. Установка дополнительных утилит . . . 27
8.1.3. Проверка наличия локали en_US.utf8 и ru_RU.UTF-8 . . . 28
8.1.4. Настройка времени/часовых поясов на серверах . . . 28
8.1.5. Настройка NTPDATE . . . 28
8.1.6. Настройка фаервола iptables . . . 28
8.1.7. Задание имени сервера . . . 28
8.2. Создание пользователей и каталогов . . . 28
8.2.1. Общие сведения . . . 28

8.2.2. Создание пользователей . . . 29
8.3. Настройка NFS и монтирование папки бекапов с DB Server на Processing Server . . . 29
8.3.1. Настройка NFS-client на Processing Server . . . 29
8.4. Установка и настройка компонентов KGS на Processing Server . . . 29
8.4.1. Установка HASP . . . 29
8.4.2. Настройка ODBC драйверов на Processing Server . . . 30
8.4.3. Установка ограничений . . . 30
8.4.4. Установка и настройка файлов KGS Framework (KMI_FW) . . . 31
8.4.4.1. Установка компонентов на Processing Server . . . 31
8.4.4.2. Настройка конфигурационного файла KGS . . . 32
8.4.4.3. Настройка PATH . . . 32
8.4.5. Установка KMI_FW_DBMK . . . 32
8.4.6. Установка и настройка KGS Console (KMI_CONSOLE) . . . 32
8.4.6.1. Установка файлов KGS Console . . . 33
8.4.7. Настройка keyring . . . 33
8.5. Проверка автоматического запуска компонентов KGS Framework (KMI_FW) . . . 33
8.5.1. Проверка автоматического запуска KMI_FW_DAL, KMI_FW_TRANSFER . . . 33
8.6. Генерация ключей HWRK и DBMK . . . 33
8.7. Создание пользователей KGS Console . . . 34
9. Окончательная настройка и запуск развернутой системы KGS . . . 35
9.1. Запуск служб KGS Framework (KMI_FW) . . . 35
9.2. Пробный запуск . . . 35
9.3. Рекомендации по начальной настройке в KMI_CONSOLE . . . 36
9.4. Многопользовательский режим KGS . . . 36

1. Аннотация

Данный документ является руководством по установке и первоначальной настройке "Системы генерации ключей Keys Generation System (KGS)" (далее по тексту - KGS или Система). Руководство содержит общие сведения о программе, основные группы задач, решаемых системой, требования к аппаратному и программному обеспечению, процедуры установки, настройки и удаления программы, обязанности и задачи администратора, процедуры настройки программы, управления учетными записями, загрузкой и выгрузкой данных, а также описание основных проблем и способов их устранения.

Документ предназначен для пользователей, осуществляющих обслуживание KGS. Руководство ориентировано на администраторов, имеющих навыки практической работы с СУБД PostgreSQL и ОС семейства Linux (в первую очередь, ОС Debian 11.4), обладающих базовыми знаниями по структуре БД KGS.

⚠ **Данный документ опубликован исключительно с целью изучения системных требований для установки продукта, а также ознакомления с последовательностью и деталями процесса установки. Реальная установка продукта производится с использованием внутренних репозиториев ООО "ПЦТ", доступ к которым предоставляется заказчику по запросу.**

2. Термины и сокращения

Термин	Определение
API (Application Programming Interface, Интерфейс программирования приложений)	Набор готовых классов, процедур, функций, структур и констант, предоставляемых приложением (библиотекой, сервисом) для использования во внешних программных продуктах. Используется программистами для написания всевозможных приложений.
DAL (Database Abstraction Layer)	Один из компонентов общей инфраструктуры, обеспечивающий интерфейс для доступа к единой базе данных всех прочих компонентов и приложений.
DMZ (Demilitarized Zone, демилитаризованная зона)	Сегмент сети, содержащий общедоступные сервисы и отделяющий их от частных. В качестве общедоступного сервиса может выступать, например, веб-сервис: обеспечивающий его сервер, который физически размещён в локальной сети (Интранет), должен отвечать на любые запросы из внешней сети (Интернет), при этом другие локальные ресурсы (например, файловые серверы, рабочие станции) необходимо изолировать от внешнего доступа. Цель DMZ – добавить дополнительный уровень безопасности в локальной сети, позволяющий минимизировать ущерб в случае атаки на один из общедоступных сервисов: внешний злоумышленник имеет прямой доступ только к оборудованию в DMZ.
Framework	Структура программной системы; программное обеспечение, облегчающее разработку и объединение разных компонентов большого программного проекта. Framework может включать вспомогательные программы, библиотеки кода, язык сценариев и другое ПО, облегчающее разработку и объединение разных компонентов большого программного проекта. Обычно объединение происходит за счёт использования единого API.
FTP (File Transfer Protocol)	Протокол передачи файлов – стандартный протокол, предназначенный для передачи файлов по TCP-сетям (например, Интернет). Протокол построен на архитектуре "клиент-сервер" и использует разные сетевые соединения для передачи команд и данных между клиентом и сервером.
NFS (Network File System)	Протокол сетевого доступа к файловым системам. Позволяет подключать (монтировать) удалённые файловые системы через сеть.

Репозиторий, хранилище	Место, где хранятся и поддерживаются какие-либо данные. Чаще всего данные в репозитории хранятся в виде файлов, доступных для дальнейшего распространения по сети.

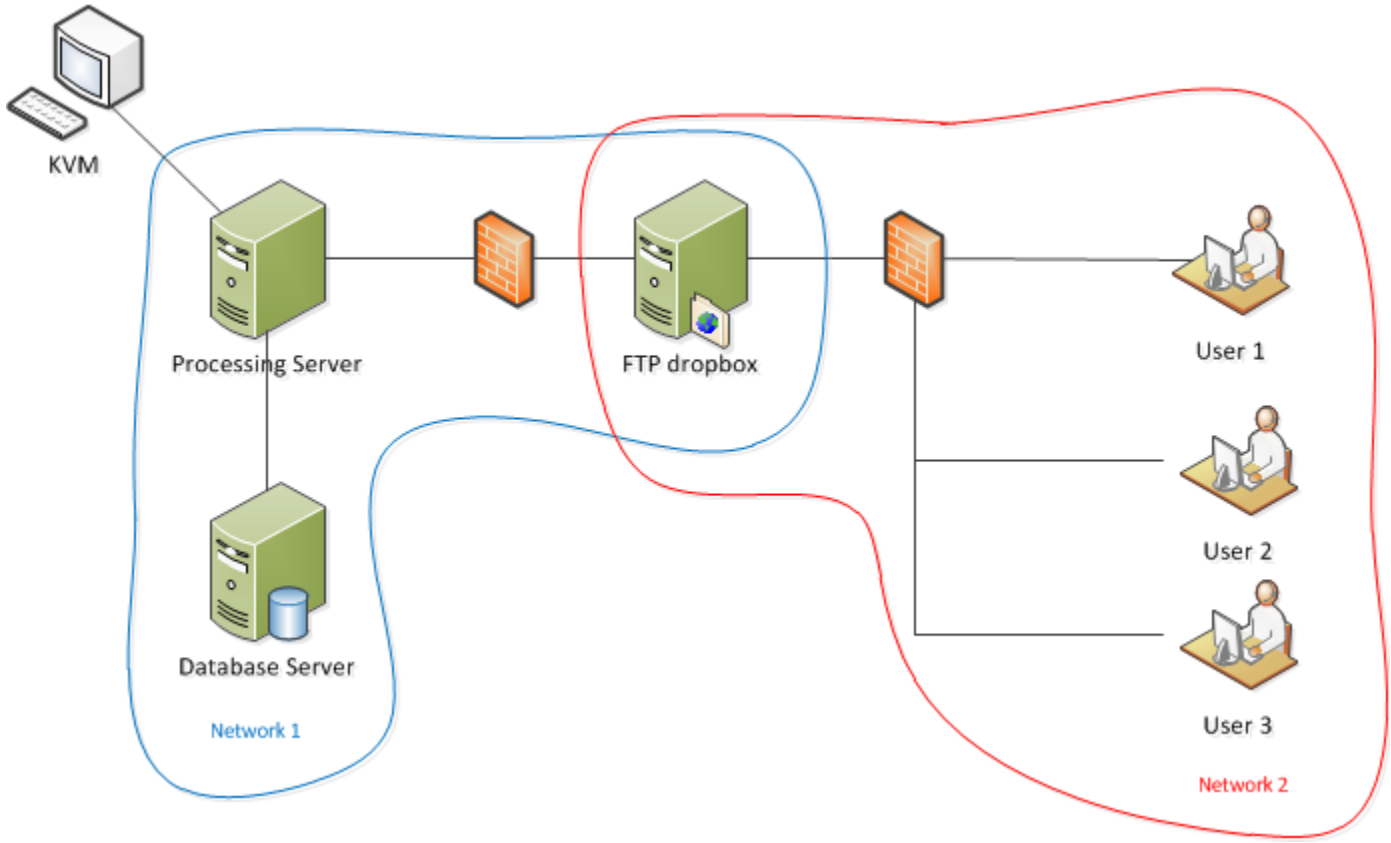
Сокращение	Расшифровка
API	Application Programming Interface
DAL	Database Abstraction Layer
DB	Database
DBMK	Database Master Key
FW	Framework
HWRK	Hardware Root Key
БД	База Данных
СУБД	Система Управления Базами Данных

3. Общие сведения

3.1. Назначение

Система предназначена для работы с ключами, прошиваемыми в однократно программируемую область чипа в процессе его персонализации. Программа предоставляет инфраструктуру, необходимую разработчикам систем, использующих персонализированные ключи. Программа реализует механизмы генерации, безопасного хранения и экспорта ключей для возможности дальнейшего их использования в процессе персонализации чипов на производственной линии.

3.2. Схема развертывания компонентов



На схеме используются следующие обозначения:

- **Database Server** – физический сервер (ОС Debian, x64), на котором развернута база данных (PostgreSQL 17 (последней версии)) и модуль Backup. Входит в выделенную физическую сеть “Network 1”.

- **Processing Server** – физический сервер (ОС Debian, x64), на котором развернуты все компоненты Framework (за исключением Backup) и Workflows. Сервер входит в выделенную физическую сеть “Network 1”.
  Оба сервера (Database Server и Processing Server) расположены в отдельном защищенном помещении, доступ в которое ограничен.

  ⚠ На всех серверах используется ОС Debian или аналоги.

- **KVM** (keyboard, video, mouse) - **Терминал** – физическое оборудование, подсоединенное к Processing Server, используемое пользователем для выполнения определенных работ (workflows) в KGS.

  ⓘ Фактически это ЭВМ/терминал, с которой(которого) пользователь управляет KGS (работает в KMI_CONSOLE).

  Предполагается, что пользователь имеет доступ к KGS только посредством KVM, который подключен к серверу в защищенном помещении.

  ⚠ **Обратите внимание!** Здесь и далее используются внутренние системные обозначения компонентов (например, KMI_CONSOLE). Соответствие между названиями компонентов (подсистем KGS) и внутренними обозначениями приведено в документе "Система генерации ключей Keys Generation System (KGS). Общее описание", в разделе "Архитектура".

- **FTP dropbox** – выделенный сервер для обмена информацией по FTP. Входит в две физические сети “Network 1” и “Network 2”. Сервер осуществляет соединения в рамках сети “Network 1” только с Processing Server и только по протоколу FTP (firewall). Сервер осуществляет соединения в рамках сети “Network 2” только с фиксированным набором рабочих станций и только по протоколу FTP (firewall).
- **User 1/2/3** – рабочие станции в рамках сети “Network 2”, которым разрешен доступ на FTP dropbox.

Передача данных в / из KGS осуществляется только посредством файлов. Все файлы, в свою очередь, пересылаются только через FTP dropbox.

3.3. Системные требования

3.3.1. FTP server

3.3.1.1. Программное обеспечение

- Эталонный образ Debian 11.4, 64bit (см. гл.4 Рекомендации по установке операционных систем).

3.3.1.2. Аппаратное обеспечение

- Требований нет.

3.3.2. Database Server

3.3.2.1. Программное обеспечение

- Эталонный образ Debian 12, 64bit (см. гл.4 Рекомендации по установке операционных систем).
- СУБД PostgreSQL 17 (последней версии).
- Python 3 64bit.

> ⚠ Python3 входит в состав эталонного образа ("устанавливается из коробки").

3.3.2.2. Аппаратное обеспечение

- Требований нет.

3.3.3. Processing Server

3.3.3.1. Программное обеспечение

- Эталонный образ Debian 11.4, 64bit (см. гл.4 Рекомендации по установке операционных систем).
- Python 3 64bit.

> ⚠ Python3 входит в состав эталонного образа ("устанавливается из коробки").

- программно-аппаратная система защиты HASP (HASP-driver и HASP-ключ).

3.3.3.2. Аппаратное обеспечение

- HASP-USB.

3.3.4. Требования по безопасности

Защита системы от несанкционированного доступа обеспечивается с помощью специальной системы развертывания, при которой компоненты KGS и база данных находятся в одной физической сети, а пользователи системы – в другой. Доступ из одной сети в другую осуществляется с помощью сервера FTP dropbox. Сервер осуществляет соединения только с фиксированным набором рабочих станций и только по протоколу FTP (firewall).

Database Server и Processing Server должны находиться в закрытом помещении с системой контроля доступа. Пользователь имеет доступ к KGS только с помощью KVM, который подключен к Processing Server в закрытом помещении.

3.3.5. Требования к квалификации обслуживающего персонала

Администратор KGS должен:

- обладать теоретическими знаниями и практическим опытом работы с ОС Debian;
- обладать теоретическими знаниями и практическим опытом работы с СУБД PostgreSQL (язык plsql);
- знать структуру БД KGS (KMI_DB_SCH);
- иметь общее представление о системе KGS.

Перейти к Содержанию...

4. Рекомендации по установке операционных систем

4.1. DB Server

Для DB Server при инсталляции ОС рекомендуется разбить HDD на 3 раздела: 1-й – для ОС, 2-й – для файлов postrges, 3-й – для файлов с бекапами, wal-файлов и tablespace базы. Размер 1-го раздела следует выбирать достаточным для ОС, исходя из особенностей ОС Debian, размер 2-го раздела (для файлов СУБД PostgreSQL) – не менее 100 ГБ, объем 3-го раздела – все остальное пространство, но не менее 400 ГБ.

4.2. Processing Server

При установке Processing Server количество разделов на HDD – не имеет значения (достаточно использовать один раздел).

Перейти к Содержанию...

5. Предварительные действия

Введение

Процедуры установки и настройки системы KGS приведены ниже.

Здесь и далее предполагается, что система KGS будет развернута на трёх серверах:

- FTP
- DB Server
- Processing Server

В связи с этим установка и настройка компонентов KGS описана аналогичным образом.

Действия рекомендуется выполнять в указанном порядке, тем не менее, некоторые процедуры могут быть выполнены в относительно любой момент времени.

Указанные особенности приведены в соответствующих подразделах.

Предварительные действия

До установки KGS на сервера в общем случае нужно выполнить следующие действия:

1. Получить IP-адреса машин (серверов), на которых будет развернут KGS.
2. Завести пользователей.
3. Настроить firewalls на серверах.

Перейти к Содержанию...

6. Настройка FTP server

6.1. Настройка операционной системы

Самым простым способом установки ОС является её установка из специально подготовленного образа *Debian **X**.iso*, который содержит дистрибутив самой ОС Debian, а также многие системные пакеты. Ссылка на образ и инструкцию по установке предоставляется по запросу.

6.1.1. Расширение репозиториев

Расширение репозиториев необходимо выполнить на ВСЕХ серверах (Database Server, Processing Server, FTP-Server).

Все операции выполнять под *sudo*.

Последовательность действий:

1. На ВСЕ сервера, которые будут использоваться KGS, необходимо предварительно установить ОС Debian 11.4 x64.
2. Подключить репозиторий производителя Системы (ссылка предоставляется по запросу), содержащий необходимые системные пакеты (доступ к репозиторию предоставляется по запросу).
3. Установить необходимые пакеты с помощью команды вида:

```
sudo apt-get install [packet_name]
```

6.1.2. Установка дополнительных утилит

Процедура выполняется на всех серверах.

Данные программные пакеты устанавливаются для удобства установщика. Их перечень может быть изменен.

Утилиты, которые должны быть установлены на FTP server:

- sudo curl iptables ssh
- openssh-client=1:8.4p1-5 zlib1g=1:1.2.11.dfsg-2 libc6=2.31-13+deb11u2
- openssh-server libarchive13 libpython3.9
- nano wget mc ntpdate

Описание последовательности действий предоставляется по запросу.

6.1.3. Настройка времени/часовых поясов на серверах

⚠ Процедура выполняется на BCEX серверах: Processing Server, DB Server, FTP-Server.

Все операции выполнять под *sudo*.

Описание последовательности действий предоставляется по запросу.

6.1.4. Настройка NTPDATE

⚠ Процедура выполняется на BCEX серверах: Processing Server, DB Server, FTP-Server.

Цель – синхронизация времени по расписанию, каждые 12 часов.

Все операции выполнять под *sudo*.

Описание последовательности действий предоставляется по запросу.

6.1.5. Задание имени сервера

Рекомендуется задать серверу понятное имя hostname, например: kgs-ftp.

⚠ Процедура выполняется на всех серверах.

Все операции выполнять под *sudo*.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

6.2. Установка и настройка proftp

⚠ Процедура выполняется на FTP-server, в любое время, но до запуска системы.

ⓘ Настройку FTP-сервера должна осуществляться системным администратором.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

6.3. Создание пользователей и каталогов

⚠ Процедура выполняется на Processing Server, DB Server и FTP-Server.

6.3.1. Общая структура папок, используемая в KGS

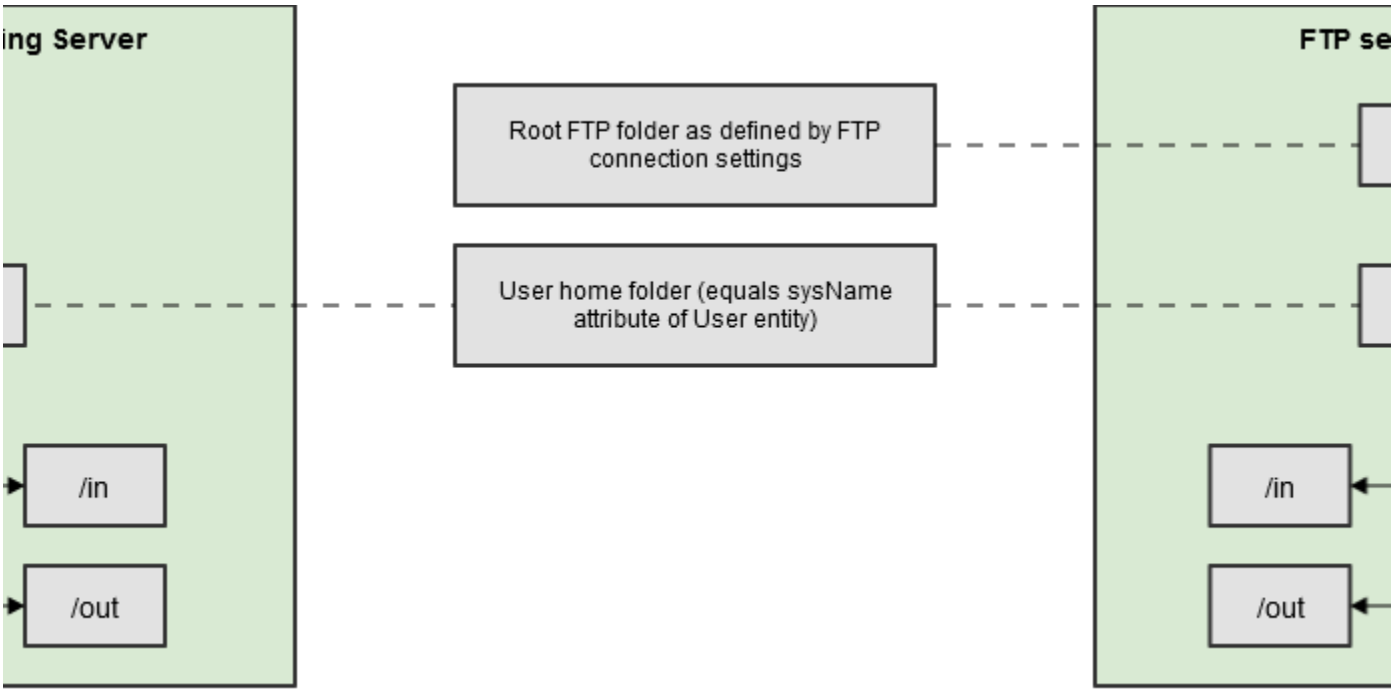
Предполагается следующая структура каталогов при разворачивании системы:

- Все файлы компонентов системы KGS (исполняемые файлы, библиотеки, файлы скриптов и т.д.) будут располагаться в каталоге */opt/kmi*. В данном каталоге будет создана структура папок, соответствующая названиям компонентов системы (kmi_dal, console и т.д.), библиотеки будут находиться непосредственно в каталоге *kmi_files*.
- Домашние каталоги пользователей системы KGS будут находиться на шифрованном разделе в оперативной памяти сервера. В данных директориях будут создаваться временные файлы с ключами в процессе работы Workflow, также через данные каталоги будет происходить обмен файлами с FTP-сервером. Подробности о структуре папок пользователей на Processing Server и на FTP Server – см. в разделе Структура папок пользователей.
- На FTP-сервере корневой каталог FTP будет располагаться по пути */opt/kmi/kmi_ftp*, в нем будут созданы папки пользователей системы (см. структуру папок в разделе Структура папок пользователей).
- Файлы СУБД с данными базы данных KMI_DB – в каталоге */opt/kmi_tablespace*
- Файлы с бекапами базы данных будут создаваться на DB Server в папке */var/backups*. Файлы бекапа будут перемещаться из данной папки на FTP-сервер, при проблемах передачи на FTP файлы будут оставаться в этой папке.
- Временные файлы базы данных, файлы WAL режима архивации БД – в каталоге */tmp* в соответствующих подкаталогах. Подробности описаны в Настройка режима бекапирования СУБД.
- Файлы с логами компонентов – в каталоге */var/log/kmi*.

6.3.2. Структура папок пользователей

Для экспорта / импорта данных на Processing server и FTP-сервере должны быть созданы папки и настроены права пользователей.

Общая схема необходимых директорий приведена на рисунке ниже.



Настройка папок производится администратором KGS и обновляется при каждом создании/удалении пользователя в консоли KGS.

> ⚠ Как правило, используется иерархическая структура папок БЕЗ элемента workflow_folder, т.е. вместо */user_folder/workflow**N**_folder/in(out)* используется */ user_ folder/ in(out)*.
>
> Структура меняется администратором KGS путем изменения настроечных параметров для соответствующих операций (workflows).

6.3.3. Исходные пользователи

На момент установки системы планируется создать следующих пользователей:

- *kmiadmin*: администратор KGS, обладает правами суперпользователя на все директории и операции в KGS, под этим пользователем настраиваются все компоненты KGS (в ОС на Processing Server и DB Server). Пользователь kmiadmin также создается в СУБД, этот пользователь является владельцем базы и администратором базы KMI_DB, под этим пользователям подключается DAL к базе KMI_DB. Пользователь создается автоматически при развертывании KMI_DB.
- *backup*: пользователь с данным именем создается в системе KGS, не имеет доступа в интерфейс, а используется только для создания/передачи бекапов БД на FTP-сервер.

6.3.4. Общий алгоритм создания пользователей и папок на FTP-Server

В общем случае последовательность действий следующая:

1. Создать пользователя с именем *username*:

```
sudo useradd <username>
```

2. Задать пароль пользователя с именем *username*:

```
sudo passwd <username>
```

3. Повторно ввести пароль для подтверждения.
4. Создать иерархию папок пользователя:

```
sudo mkdir -p /opt/kmi_ftp/<username>/{in,out}
```

5. Выдать пользователю права доступа на созданные папки:

```
sudo chmod 776 /opt/kmi_ftp/<username> -R
sudo chown <username>:<username> /opt/kmi_ftp/<username> -R
```

После создания пользователя и выдачи ему прав доступа рекомендуется загрузить public PGP-ключ пользователя в KMI_DB. Ключи пользователя *username* загружаются из папки */in* текущего пользователя (т.е. пользователя, под которым выполняется операция в KMI_CONSOLE), а не USERNAME. Каждый пользователь, который будет экспортировать данные на FTP-сервер, должен иметь один или несколько PGP-ключей.

6.3.5. Создание директорий на FTP-Server

Директории создавать от sudo:

```
sudo mkdir /opt/kmi_ftp
sudo mkdir /opt/kmi_ftp/backup
sudo mkdir /opt/kmi_ftp/user1
sudo mkdir /opt/kmi_ftp/user2
```

У каждого пользователя должна быть своя папка: user1 – */opt/kmi_ftp/user1*, user2 – */opt/kmi_ftp/user2* и т.д.

Пользователь kmiadmin должен иметь home-директорию "--home */opt/kmi_ftp*", т.е. корневой каталог (для остальных пользователей).

6.3.6. Создание пользователей на FTP-Server

Необходимо установить proftp (см. Установка и настройка proftp).

Действия, описанные ниже, необходимо выполнить для КАЖДОГО пользователя. В приведенном примере используется имя пользователя (*user 2*), его необходимо заменить на выбранное значение.

1. Выполнить команды:

```
sudo touch /etc/proftpd/ftpd.passwd
sudo ftpasswd -passwd --file=/etc/proftpd/ftpd.passwd --name=user2 --shell=/bin/false --home /opt/kmi_ftp
/user2/ --uid=119 --gid=65500
```

2. Система запросит пароль для *user2*, ввести пароль и подтвердить его.

Перейти к Содержанию...

7. Настройка DB Server

7.1. Настройка операционной системы

Аналогично описанному выше.

7.1.1. Расширение репозиториев

Аналогично описанному выше.

7.1.2. Установка дополнительных утилит

⚠ Процедура выполняется на всех серверах.

Данные программные пакеты устанавливаются для удобства установщика. Их перечень может быть изменен.

Утилиты, которые должны быть установлены на DB Server:

- Аналогично FTP server:
  - sudo curl iptables ssh
  - openssh-client=1:8.4p1-5 zlib1g=1:1.2.11.dfsg-2 libc6=2.31-13+deb11u2
  - openssh-server libarchive13 libpython3.9
  - nano wget mc ntpdate
- Дополнительно:
  - lshw libjsoncpp24
  - libtool unixodbc
  - libpgm-5.3-0 libsodium23 libzmq5
  - libboost1.74-all-dev
  - pigz

ⓘ Утилита lshw необходима для генерации Binding key, используемого в лестнице ключей, – без неё KGS работать не будет.

Пакеты libtool и unixodbc необходимы для работы KMI_FW_DAL; пакеты libpgm-5.3-0, libsodium23, libzmq5 устанавливаются на оба сервера; пакет libjsoncpp24 - для работы KMI_FW_DAL (см. Установка и настройка файлов KGS Framework (KMI_FW)).

pigz предназначен для ускорения процесса архивации на многоядерных системах.

Описание последовательности действий предоставляется по запросу.

7.1.3. Проверка наличия локали en_US.utf8 и ru_RU.UTF-8

> На серверах с ОС Debian кодировка UTF-8 должна быть установлена ПО УМОЛЧАНИЮ. Тем не менее, необходимо УДОСТОВЕРИТЬСЯ в том, что нужная локаль (en_US.utf8 и ru_RU.UTF-8) установлена на серверах.
>
> Использование русской кодировки на серверах KGS НЕ ПРИВЕТСТВУЕТСЯ, тем не менее, команда создания БД требует установленной русской локали.

> Процедура выполняется на Processing Server и DB Server.

Подробное описание приведено здесь:

http://webhamster.ru/mytetrashare/index/mtb0/1355746267lougdkzfg3

7.1.4. Настройка времени/часовых поясов на серверах

Аналогично описанному выше.

7.1.5. Настройка NTPDATE

Аналогично описанному выше.

7.1.6. Настройка фаервола iptables

> Процедура выполняется как на Processing Server, так и на DB Server.

На Database Server необходимо разрешить подключения к СУБД PostgreSQL и NFS. Так как DB Server будет доступен только для подключения со стороны Processing Server, можно разрешить доступ только с ip-адреса Processing Server без указания портов используемых сервисов, при необходимости можно ограничить список портов.

Настройки следует выполнять под правами суперпользователя (под *sudo*).

Описание последовательности действий предоставляется по запросу.

7.1.7. Задание имени сервера

Рекомендуется задать серверу понятное имя hostname, например: kgs-db.

Аналогично описанному выше.

Перейти к Содержанию...

7.2. Настройка NFS и монтирование папки бекапов с DB Server на Processing Server

Требования:

- наличие NFS-server на DB Server;
- наличие NFS-client на Processing Server;
- Папка *'some_path_to_files_with_backups'* смонтирована на Processing Server в папку */var/backups/out* (фиксированный путь).

> ⚠ В приведенном ниже подразделе использован следующий IP-адрес для Processing Server – 192.168.14.160.

Подробное описание приведено здесь:

http://www.tecmint.com/how-to-setup-nfs-server-in-linux/

7.2.1. Настройка NFS-server на DB Server

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

7.3. Установка и настройка БД

> ⚠ БД устанавливается на DB Server. Процедура должна быть выполнена ДО запуска DAL.

7.3.1. Установка PostgreSQL

Все операции выполнять под *sudo*.

Перед началом установки KMI_DB на Database Server необходимо установить СУБД PostgreSQL 17. Описание процедуры установки и настройки PostgreSQL выходит за рамки данного документа. Процедуру установки можно посмотреть, например, здесь: https://computingforgeeks.com/how-to-install-postgresql-14-on-debian/

В общем случае, последовательность действий следующая:

1. Подключить репозиторий производителя Системы, содержащий необходимые системные пакеты (было выполнено ранее, см. Расширение репозиториев).
2. Обновить список пакетов системы:

```
sudo apt-get update
```

3. Установить пакеты postgresql:

```
sudo apt-get install postgresql-17 postgresql-client-17 postgresql-contrib postgresql postgresql-common
postgresql-client-common
```

7.3.2. Настройка PostgreSQL

Описание последовательности действий предоставляется по запросу.

7.3.3. Создание директории для Tablespace

⚠ Tablespace должно быть создано до установки KMI_DB_SCH и KMI_DB_API.

Создать, если это не было сделано ранее (см. Общая структура папок, используемая в KGS, п.4), на DB-Server хранилище – папку /opt/kmi_tablespace.

7.3.4. Редактирование файла по начальному наполнению БД

Перед установкой KMI_DB следует проверить конфигурацию файла, отвечающего за начальное наполнение БД.

Описание последовательности действий предоставляется по запросу.

7.3.5. Установка KMI_DB_SCH

Особенности:

- В рамках дальнейших алгоритмов подразумевается, что на сервер уже установлен и настроен Postgres, созданы роли и табличное пространство.
- Скрипты запускаются от sudo (не от postgres).
- Необходимо выдать права на папку с файлами, например сделать папку открытой для всех пользователей (наиболее простой вариант):

```
sudo chmod -R 755 /home/kmi_db_sch
sudo chmod -R 755 /home/kmi_db_api
```

- Для установки sch и api вне зависимости от того, устанавливаются они на уже существующие компоненты (обновляются) или при установке на чистый сервер, необходимо запускать один и тот же

единственный скрипт (внутри скрипта происходит запуск нужных скриптов (либо для обновления, либо для изначальной установки)).

- Пароли пользователей KMI_DB (kmiadmin) и postgres могут быть как переданы напрямую (указаны в открытом виде в bash строке), так и переданы в файлах (в которых уже внутри будут пароли для соответствующего пользователя).

Описание последовательности действий предоставляется по запросу.

7.3.6. Установка KMI_DB_API

> Процедуру следует выполнять только после установки KMI_DB_SCH.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

7.4. Установка и настройка компонентов KGS на DB Server

7.4.1. Установка и настройка файлов KGS Framework (KMI_FW)

> Установка компонентов KGS Framework, за исключением KMI_FW_BACKUP, осуществляется на Processing Server. Модуль KMI_FW_BACKUP устанавливается на DB Server.

Установка компонентов KGS Framework осуществляется с помощью DEB-пакетов ОС (Debian). Файлы на обоих серверах будут установлены в папку */opt/kmi/*.

> DEB-пакеты KMI_FW и KMI_CONSOLE используют библиотеки python, поэтому Python3 должен быть установлен до установки этих компонентов.
>
> Поскольку Python3 входит в эталонный образ Debian11 ("устанавливается из коробки"), то дополнительные действия не требуются.

7.4.1.1. Установка компонентов на DB Server

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

7.4.1.2. Настройка конфигурационного файла KGS

⚠ Процедура выполняется после установки компонентов KGS Framework, но до запуска служб KGS Framework, на серверах, на которых установлены эти компоненты (т.е. на Processing Server и DB Server).

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

7.4.1.3. Настройка PATH

⚠ Процедура выполняется на Processing Server и DB Server.

ⓘ Все исполняемые файлы KGS хранятся в папке */opt/kmi/bin*. Для того чтобы не вводить этот каталог в процессе установки, настройки и использования KGS, необходимо настроить систему таким образом, чтобы она по умолчанию искала исполняемые файлы в этом каталоге при каждой сессии.

С этой целью в переменную PATH добавляется каталог */opt/kmi/bin*.

Выполнение этой операции необязательно, применяется исключительно для удобства дальнейшей установки системы.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

7.5. Проверка автоматического запуска компонентов KGS Framework (KMI_FW)

7.5.1. Проверка автоматического запуска KMI_FW_BACKUP

⚠ Автоматический запуск KMI_FW_BACKUP настраивается автоматически при установке компонента с помощью DEB-пакетов (см. "Установка и настройка файлов KGS Framework (KMI_FW)").

Чтобы проверить автоматический запуск сервиса kmi_fw_backup, выполните команду:

```
systemctl is-enabled kmi_fw_backup
```

В случае успеха ответ должен быть следующим:

```
enabled
```

7.6. Настройка режима бекапирования СУБД

⚠ Процедура выполняется до запуска служб KGS, но ПОСЛЕ установки DEB-пакетов.

Необходимо настроить режим архивации БД для резервного копирования (ВСЕ операции выполняются под пользователем postgres). Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

8. Настройка Processing Server

8.1. Настройка операционной системы

Аналогично описанному выше.

8.1.1. Расширение репозиториев

Аналогично описанному выше.

8.1.2. Установка дополнительных утилит

⚠ Процедура выполняется на всех серверах.

Данные программные пакеты устанавливаются для удобства установщика. Их перечень может быть изменен.

Утилиты, которые должны быть установлены на Processing Server:

- Аналогично FTP server:
  - sudo curl iptables ssh
  - openssh-client=1:8.4p1-5 zlib1g=1:1.2.11.dfsg-2 libc6=2.31-13+deb11u2
  - openssh-server libarchive13 libpython3.9
  - nano wget mc ntpdate
- Аналогично DB Server:
  - lshw libjsoncpp24
  - libtool unixodbc
  - libpgm-5.3-0 libsodium23 libzmq5
  - libboost1.74-all-dev
- Дополнительно:
  - logrotate, компилятор C (-y gcc autoconf automake)
  - haveged (libhavege1_1.9.1-7_amd64.deb)
  - libcurl4 libqt5opengl5
  - libgpgme11
  - libarchive for zip64 (libarchive-dev-3.3.2-amd64.deb)

Утилита lshw необходима для генерации Binding key, используемого в лестнице ключей, – без неё KGS работать не будет.

Демон haveged необходим для генерации PGP-ключей заданного размера - при его отсутствии KMI_CONSOLE зависнет на этапе генерации PGP-ключа.

Пакеты libtool и unixodbc необходимы для работы KMI_FW_DAL; пакеты libpgm-5.3-0, libsodium23, libzmq5 устанавливаются на оба сервера; пакеты libcurl4 и libqt5opengl5 - для работы KMI_FW_TRANSFER; пакет libjsoncpp24 - для работы KMI_FW_DAL (см. Установка и настройка файлов KGS Framework (KMI_FW)).

Описание последовательности действий предоставляется по запросу.

8.1.3. Проверка наличия локали en_US.utf8 и ru_RU.UTF-8

Аналогично описанному выше.

8.1.4. Настройка времени/часовых поясов на серверах

Аналогично описанному выше.

8.1.5. Настройка NTPDATE

Аналогично описанному выше.

8.1.6. Настройка фаервола iptables

Аналогично описанному выше.

8.1.7. Задание имени сервера

Рекомендуется задать серверу понятное имя hostname, например: kgs-processing.

Аналогично описанному выше.

Перейти к Содержанию...

8.2. Создание пользователей и каталогов

8.2.1. Общие сведения

Аналогично описанному выше:

- Структура папок пользователей - см. здесь.
- Исходные пользователи - см. здесь.

8.2.2. Создание пользователей

⚠ Пользователи и папки на Processing Server создаются с помощью скрипта (см. Создание пользователей KGS Console), доступного после установки файлов KGS Framework.

Перейти к Содержанию...

8.3. Настройка NFS и монтирование папки бекапов с DB Server на Processing Server

Требования:

- наличие NFS-server на DB Server;
- наличие NFS-client на Processing Server;
- Папка *'some_path_to_files_with_backups'* смонтирована на Processing Server в папку */var/backups/out* (фиксированный путь).

  ⚠ В приведенном ниже подразделе использован следующий IP-адрес для DB Server – 192.168.14.162.

Подробное описание приведено здесь:

http://www.tecmint.com/how-to-setup-nfs-server-in-linux/

8.3.1. Настройка NFS-client на Processing Server

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

8.4. Установка и настройка компонентов KGS на Processing Server

8.4.1. Установка HASP

⚠ Процедура выполняется только на Processing Server.

USB-HASP устанавливается в Processing Server, используется в лестнице ключей.

HASP-ключ используется при шифровании лестницей ключей, экспортированной на сервер из системы KGS. Тем не менее, при описании процедуры установки библиотек KGS (см. Установка библиотек KGS) можно задать параметр **no_hasp**, позволяющий не пользоваться HASP.

Во всех остальных случаях наличие HASP-USB и установленных HASP drivers обязательно для установки и корректной работы библиотек KGS и, как следствие, всей системы.

Описание последовательности действий предоставляется по запросу.

8.4.2. Настройка ODBC драйверов на Processing Server

Для корректной работы БД на ЭВМ (**Processing Server**), с которой будет осуществляться подключение к БД, должны быть установлены и настроены драйверы ODBC.

Процедура выполняется только на Processing Server.

Для корректной работы БД на Processing Server необходимо установить следующее ПО:

- unixodbc-driver;
- PostgreSQL – odbc-driver;

Драйверы и библиотека могут быть установлены в любой момент времени, но до начала эксплуатации KMI_FW_DAL.

Все операции выполнять под *sudo*.

Описание последовательности действий предоставляется по запросу.

8.4.3. Установка ограничений

Необходима проверка ограничений на память (hard/soft), в том числе на размер памяти.

На Processing Server необходимо установить ограничения на область памяти, защищенную от кэширования. По умолчанию, этот объем памяти слишком мал и требует прав *sudo* для разграничения программой доступной памяти: лимит = 1024000 (1 Гб памяти).

Ограничения задаются в файле */etc/security/limits.conf* внесением следующих данных:

```
* hard memlock 1024000
* soft memlock 1024000
```

Ограничения нужно задавать заново при каждом перезапуске сервера.

8.4.4. Установка и настройка файлов KGS Framework (KMI_FW)

Установка компонентов KGS Framework, за исключением KMI_FW_BACKUP, осуществляется на Processing Server. Модуль KMI_FW_BACKUP устанавливается на DB Server.

Установка компонентов KGS Framework осуществляется с помощью DEB-пакетов ОС (Debian). Файлы на обоих серверах будут установлены в папку */opt/kmi/*.

DEB-пакеты KMI_FW и KMI_CONSOLE используют библиотеки python, поэтому Python3 должен быть установлен до установки этих компонентов.

Поскольку Python3 входит в эталонный образ Debian11 ("устанавливается из коробки"), то дополнительные действия не требуются.

DEB-пакеты нужно устанавливать только в определенной последовательности (для сохранения зависимостей между пакетами). Следующий DEB-пакет можно устанавливать, только если успешно установлен предыдущий. Если в процессе установки возникла ошибка, то пакет нужно удалить (команда sudo dpkg -r <название_DEB_пакета>), устранить причину ошибки и установить пакет заново.

Если по каким-либо причинам DEB-пакеты были установлены с ошибкой, то нужно удалить их в обратной последовательности (т.е. снизу вверх).

8.4.4.1. Установка компонентов на Processing Server

Версия библиотеки HASP указывается как значение переменной KMI_HASP_VERSION. Система KGS использует переменную KMI_HASP_VERSION для обработки того, какой вариант HASP должен быть установлен. Описание возможных значений KMI_HASP_VERSION приведено в отдельном документе (доступ **строго ограничен**).

Перед установкой библиотеки kmi_fw_tde необходимо знать версию внешней библиотеки HASP, которая будет использоваться. Если используется значение, отличное от значения по умолчанию, то сначала требуется установить новое значение KMI_HASP_VERSION и лишь затем устанавливать kmi_fw_tde.

Если реальная версия библиотеки HASP и значение переменной KMI_HASP_VERSION не совпадают, то после установки компонентов KGS любой продукт, который использует TDE (т.е. лестницу ключей, генерируемую KGS), не может быть запущен из-за ошибки инициализации.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

8.4.4.2. Настройка конфигурационного файла KGS

Аналогично описанному выше.

8.4.4.3. Настройка PATH

Аналогично описанному выше.

8.4.5. Установка KMI_FW_DBMK

У компонента kmi_fw_dbmk нет зависимостей от других компонентов KGS Framework, поэтому kmi_fw_dbmk по факту может быть установлен и использоваться на любом сервере, если выполнены Системные требования (описаны в документе "DBMKGenerator. Руководство пользователя" (доступ предоставляется по запросу)) и на вход был подан HWRK-ключ, сгенерированный на Processing Server.

Предполагается, что установка kmi_fw_dbmk осуществляется на отдельный сервер. Тем не менее, все необходимые требования для работы kmi_fw_dbmk уже выполнены на Processing Server.

Установка KMI_FW_DBMK выполняется аналогично другим компонентам KMI_FW.

Описание последовательности действий предоставляется по запросу.

8.4.6. Установка и настройка KGS Console (KMI_CONSOLE)

KMI_CONSOLE устанавливается на Processing Server.

Требования:

- Установленный Python3.
- Наличие пользователя с *systemName*, идентичным тому, что занесено в БД, в таблицу **kmi_user**.
- У данного пользователя есть права доступа хотя бы на Management workflow.

8.4.6.1. Установка файлов KGS Console

Описание последовательности действий предоставляется по запросу.

8.4.7. Настройка keyring

⚠ Процедура выполняется на одном сервере с компонентом KMI_FW_DAL, т.е. на Processing Server.

Для дополнительной очистки keyring при перезагрузке ото ВСЕХ ключей (использованных в прошлом или не удалившихся из-за каких-то возможных ошибок) можно монтировать keyring с PGP-ключами в RAM, добавив в */etc/fstab* строку:

```
tmpfs /root/.gnupg tmpfs defaults 0 0
```

Перейти к Содержанию...

8.5. Проверка автоматического запуска компонентов KGS Framework (KMI_FW)

8.5.1. Проверка автоматического запуска KMI_FW_DAL, KMI_FW_TRANSFER

⚠ Автоматический запуск настраивается автоматически при установке компонентов с помощью DEB-пакетов (см. "Установка и настройка файлов KGS Framework (KMI_FW)").

Чтобы проверить автоматический запуск сервиса kmi_fw_dal, выполните команду:

```
systemctl is-enabled kmi_fw_dal
```

Чтобы проверить автоматический запуск сервиса kmi_fw_transfer, выполните команду:

```
systemctl is-enabled kmi_fw_transfer
```

В обоих случаях ответ должен быть следующим:

```
enabled
```

Перейти к Содержанию...

8.6. Генерация ключей HWRK и DBMK

⚠ Процедура выполняется на Processing Server, перед запуском системы.

Для использования KMI_FW_DAL необходимо последовательно сгенерировать ключи HWRK и DBMK. Ключи являются первыми в цепочке ключей, которыми шифруется секретная часть БД KGS. При отсутствии ключей система работать не будет.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

8.7. Создание пользователей KGS Console

⚠ Процедура выполняется на Processing Server.

Описание последовательности действий предоставляется по запросу.

Перейти к Содержанию...

9. Окончательная настройка и запуск развернутой системы KGS

9.1. Запуск служб KGS Framework (KMI_FW)

⚠ Процедура выполняется на Processing Server и DB Server.

ПРОЦЕДУРА ДОЛЖНА БЫТЬ ВЫПОЛНЕНА ПЕРЕД СДАЧЕЙ СИСТЕМЫ В ЭКСПЛУАТАЦИЮ, КОГДА УСТАНОВЛЕНЫ И НАСТРОЕНЫ ВСЕ КОМПОНЕНТЫ.

Запуск служб KGS осуществляется перед пробным запуском системы, с помощью команды вида:

```
sudo service <_> start
```

Вместо <*название_службы*> подставляются:

- *kmi_fw_dal* - на Processing Server.
- *kmi_fw_transfer* - на Processing Server.
- *kmi_fw_backup* - на DB Server.

Примечание. Вообще название службы совпадает с названием устанавливаемого deb-пакета (до версии компонентов).

В случае успеха в конце выполнения команды должно появиться **OK**.

Перейти к Содержанию...

9.2. Пробный запуск

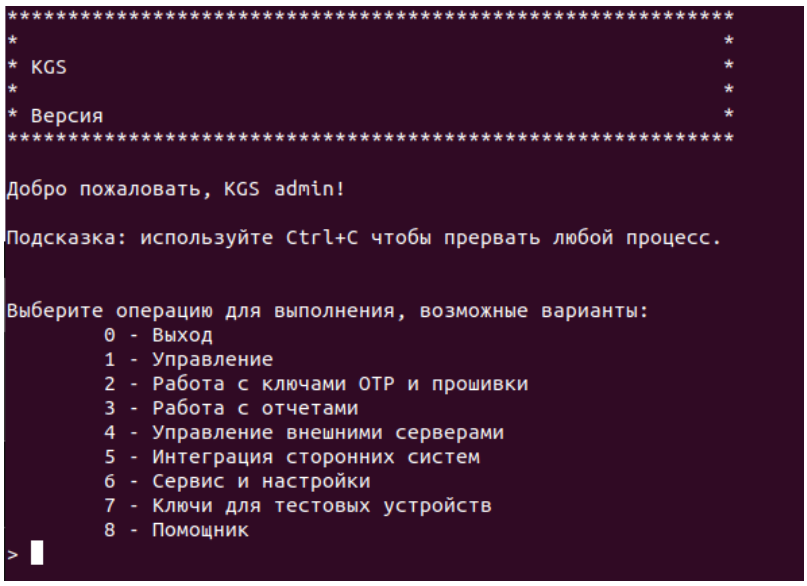
⚠ Пробный запуск осуществляется после установки и настройки всех компонентов KGS.

Управление системой KGS осуществляется с консоли (KVM), расположенной в закрытой комнате с ограниченным доступом.

Последовательность действий:

1. Открыть консоль (KVM).
2. Пройти авторизацию, введя имя пользователя и пароль, выданные администратором системы. После запуска KMI_CONSOLE откроется главное меню программы (см. ниже).

В случае если главное окно программы не появилось, необходимо проверить права доступа для пользователя.



3. Выполнить несколько операций, на которые у пользователя есть права доступа и не связанных с экспортом данных (например, добавить данные с помощью Management, Generate status report). Следует учесть, что многие операции требуют наличия public PGP-ключа в папке пользователя и (или) набор взаимосвязанных данных – при отсутствии этих данных выполнение некоторых операций приведет к ошибке. Подробное описание приведено в документе "Руководство пользователя".
4. Повторить шаги 2 и 3 для других пользователей, созданных в процессе установки KGS.

Перейти к Содержанию...

9.3. Рекомендации по начальной настройке в KMI_CONSOLE

Для эксплуатации системы, установленной "с нуля", рекомендуется выполнить следующие минимальные действия в KMI_CONSOLE:

1. Создать пользователей KMI_CONSOLE, выдать им права доступа на workflows (**Сервис и настройки** -> **Пользователи и разрешения**).
2. Сгенерировать либо импортировать PGP ключи для этих пользователей (**Сервис и настройки** -> **PGP Ключи Пользователя**).
3. Задать основные сущности, с которыми будут оперировать пользователи (см. "Руководство пользователя").

Для получения более подробной информации по работе с KMI_CONSOLE рекомендуется обратиться к документам "Руководство пользователя" и "Руководство администратора" (доступ предоставляется по запросу).

9.4. Многопользовательский режим KGS

В KMI_CONSOLE используется многопользовательский режим: в консоли могут работать одновременно несколько пользователей (пользователи подключаются к консоли удаленно, например, по SSH). Если один пользователь работает в workflow, то указанное workflow будет заблокировано для других пользователей. По окончании работы пользователя с workflow блокировка снимается. Подробности, касающиеся блокировки workflows и действий пользователей, описаны в документе "Руководство пользователя".

В многопользовательском режиме служба KMI_FW_DAL работает с несколькими потоками. При установке системы KGS **количество потоков по умолчанию = 3 шт**. Это означает, что в KMI_CONSOLE могут **одновременно** выполняться три команды (пользователь вызывает команды, например, при отображении списка либо генерации данных, при этом ввод значений при выполнении workflow команду DAL не вызывает). При этом количество пользователей, которые **одновременно** подключены к KMI_CONSOLE, может быть любым (намного больше).

Таким образом, может возникнуть ситуация, когда одновременно будут заняты три потока (т.е. одновременно будут выполняться три команды DAL), при этом есть другие пользователи, подключенные к KMI_CONSOLE и желающие выполнить какую-либо команду DAL. В результате у пользователей, которые не успели "занять" потоки для работы с DAL, KMI_CONSOLE будет "висеть" до освобождения потока.

Если потребуется изменить количество потоков для одновременной работы с DAL, то необходимо выполнить действия, описанные в документе "Руководство администратора" (доступ предоставляется по запросу), в разделе "Запуск KMI_FW_DAL с альтернативными параметрами".