# РУКОВОДСТВО АДМИНИСТРАТОРА

Версия 1.2

Листов 157

2021

# АННОТАЦИЯ

Настоящий документ является руководством администратора прикладного программного обеспечения «Аврора Центр» релиз 2.5.1 (далее — ППО).

Настоящий документ содержит общую информацию о ППО, описание установки, обновления, удаления и резервного копирования ППО, а также описывает управление сервисами и их настройками, кроме того, настоящий документ содержит информацию о конфигурационных файлах ППО.

# СОДЕРЖАНИЕ

# 1. ОБЩАЯ ИНФОРМАЦИЯ

## 1.1. Назначение и состав ППО

ППО предназначено для управления мобильными устройствами (МУ), функционирующими под управлением операционной системы (ОС) Аврора, управления жизненным циклом мобильных приложений (МП) и обновлением ОС.

Под обновлением ОС понимается инициализация в ОС процессов получения пакетов с изменениями ОС (образа ОС) из доверенного хранилища и их установки. Получение пакетов с изменениями ОС и их установка осуществляется штатными средствами ОС. ППО не гарантирует успех получения пакетов с изменениями ОС и их установки

ППО является прикладным программным обеспечением со встроенными механизмами защиты информации от несанкционированного доступа.

ППО состоит из следующих подсистем:

- подсистема безопасности (ПБ);
- подсистема «Маркет» (ПМ);
- подсистема Платформа управления (ПУ);
- подсистема обновления ОС (ПООС).

Взаимодействие между подсистемами и компонентами подсистем осуществляется с использованием протокола HTTP стандарт RFC 2616, при этом обмен данными осуществляется в формате RFC 8259 (JSON).

В качестве сервера базы данных (БД) используется сервер с установленной системой управления базами данных (СУБД) Postgres Pro или PostgreSQL, в которой хранятся данные ППО, для чего при развертывании создается специальная БД. Для хранения информации о сессиях используется СУБД Redis.

### 1.1.1. Назначение и состав ПБ

В ПБ реализованы функции безопасности ППО.

ПБ состоит из следующих компонентов:

– Консоль администратора ПБ;

– Консоль входа пользователей;

– Сервер приложений ПБ.

С помощью Консоли администратора ПБ осуществляется управление учетными записями пользователей и работа с журналом регистрации событий.

С помощью Консоли входа пользователей осуществляется ввод идентификационной и аутентификационной информации пользователями ППО.

Сервер приложений ПБ представляет собой совокупность веб-приложений, реализующих функции безопасности, а также позволяющих хранить в БД и предоставлять субъектам доступа ППО доступ к данным об учетных записях пользователей и журналу регистрации событий.

### 1.1.2. Назначение и состав ПМ

ПМ состоит из следующих компонентов:

– Консоль администратора ПМ;

– Консоль разработчика ПМ;

– МП «Аврора Маркет»;

– Сервер приложений ПМ.

С помощью Консоли администратора ПМ Администратор Аврора Маркет получает приложения и данные о приложениях, а также осуществляет согласование приложений с целью их публикации либо отказывает в публикации.

С помощью Консоли разработчика ПМ осуществляется добавление новых и обновление ранее загруженных приложений в ПМ, а также осуществляется доступ к данным о приложениях.

МП «Аврора Маркет» выполняется на МУ под управлением ОС Аврора, служит для отображения данных о приложениях, а также для загрузки, установки, обновления и удаления приложений на МУ.

Сервер приложений ПМ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа ППО информацию о приложениях. Непосредственно сами приложения, а также иконки и скриншоты приложений хранятся в файловом хранилище.

### 1.1.3. Назначение и состав ПУ

ПУ состоит из следующих компонентов:

- Консоль администратора ПУ;
- МП «Аврора Центр»;
- Сервер приложений ПУ.

С помощью Консоли администратора ПУ осуществляется взаимодействие Администратора Платформы Управления с ПУ.

С помощью МП «Аврора Центр» осуществляется активация МУ в ППО.

МП «Аврора Центр» выполняется на МУ под управлением ОС Аврора, служит для получения управляющих сообщений от Сервера приложений ПУ и передачи их компонентам ОС Аврора, а также передачи на Сервер приложений ПУ сведений о настройках и конфигурации ОС Аврора. В зависимости от управляющего сообщения или офлайн-сценария, полученного от Сервера приложений ПУ, МП «Аврора Центр» посредством вызова интерфейсных функций ОС Аврора имеет возможность:

- включать и выключать доступ к камере на МУ;
- включать и выключать доступ к браузеру на МУ;
- обновлять версию ОС на МУ;
- блокировать и разблокировать МУ;
- очищать данные (восстанавливать заводские настройки) МУ;
- устанавливать и удалять приложения на МУ;
- получать данные о состоянии МУ и событиях безопасности МУ;
- получать логи с МУ;
- устанавливать расписание обмена данными с МУ;

– включать и выключать доступ к управлению WLAN настройками;

– включать и выключать доступ к WLAN на МУ;

– включать и выключать доступ к точке доступа WLAN на МУ;

– ограничивать и предоставлять доступ к МТР;

– ограничивать и предоставлять доступ к Bluetooth (функционал доступен для версии ОС Аврора 4.0.1 и выше);

– изменять пароль учетной записи пользователя в ОС Аврора;

– блокировать МУ при смене SIM-карты (офлайн-сценарий);

– блокировать МУ при отсутствии связи с сервером (офлайн-сценарий);

– блокировать МУ при входе в зону действия WLAN (офлайн-сценарий);

– блокировать и разблокировать МУ при нахождении вне зоны действия WLAN (офлайн-сценарий).

Сервер приложений ПУ представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять субъектам доступа ППО данные о настройках ОС Аврора, а также формировать управляющие сообщения для МП «Аврора Центр».

### 1.1.4. Назначение и состав ПООС

ПООС состоит из следующих компонентов:

– Сервер приложений ПООС.

Сервер приложений ПООС представляет собой совокупность веб-приложений, позволяющих хранить в БД и предоставлять следующие данные о пакетах ОС (загрузочный модуль ОС):

– информацию о версиях;

– адрес хранилища пакетов ОС.

Для хранения и дистрибуции пакетов ОС применяется файловый сервер, развернутый с использованием Nginx.

## 1.2. Функции подсистем

Функции ППО:

– ПБ обеспечивает:

- идентификацию и аутентификацию пользователей и МУ;
- управление идентификаторами пользователей и МУ;
- управление средствами аутентификации;
- управление учетными записями пользователей и МУ;
- ролевое управление доступом субъектов доступа к объектам доступа;
- регистрацию событий безопасности;
- предоставление интерфейса пользователям подсистемы.

– ПМ обеспечивает:

- управление жизненным циклом приложений (загрузка, согласование, удаление и публикация);
- управление дистрибуцией опубликованных приложений (скачивание, установка, обновление, удаление приложений на МУ);
- предоставление интерфейса пользователям подсистемы.

– ПУ обеспечивает:

- управление отдельными МУ (оперативное управление);
- управление группами МУ;
- управление политиками;
- управление офлайн-сценариями;
- управление записями о МУ;
- управление записями о пользователях МУ;
- управление приложениями на МУ;
- контроль состояния МУ;
- контроль применения политик на МУ;
- мониторинг событий и предоставление отчетности;

- предоставление интерфейса пользователям подсистемы.

– ПООС обеспечивает:

- предоставление информации о пакетах ОС;
- управление дистрибуцией пакетов ОС.

Все подсистемы ППО позволяют выполнять логирование информационных сообщений, сообщений об ошибках, предупреждений и отладочной информации в системный журнал ОС сервера приложений (systemd).

## 1.3. Условия выполнения

Для функционирования ППО необходимы следующие программно-технические средства.

В таблице (Таблица 1) приведены аппаратные характеристики серверов приложений ППО.

Таблица 1

| Параметр | Количество МУ | | | | |
|---|---|---|---|---|---|
| | 10 000 | 50 000 | 100 000 | 275 000 | 550 000 |
| Процессор | 2 ядра | 3 ядра | 3 ядра | 6 ядер | 6 ядер |
| Объем оперативной памяти | 4 Гб | 4 Гб | 6 Гб | 8 Гб | 8 Гб |
| Объем жесткого диска | HDD 60 Гб | HDD 80 Гб | HDD 110 Гб | HDD 130 Гб | HDD 160 Гб |
| Количество серверов | 3 | 3 | 3 | 3 | 6 |

В таблице (Таблица 2) приведены программные характеристики серверов приложений ППО.

Таблица 2

| Параметр | Значение |
|---|---|
| Операционная система | Одна из следующих ОС:<br>– CentOS версии 7 или выше;<br>– CentOS версии 8 или выше;<br>– Альт 8 СП |
| Балансировщик микросервисов | Nginx Web Server версии 1.18 или выше |
| Система обнаружения сервисов | Consul версии 1.9 или выше |
| Средство управления конфигурациями микросервисов | Consul Template версии 0.25 или выше |
| Сервис гарантированной доставки сообщений | Nats Streaming Server версии 0.20.0 или выше |
| Прикладное программное обеспечение | ППО «Аврора Центр» |

В таблице (Таблица 3) приведены аппаратные характеристики серверов БД.

Таблица 3

| Параметр | Количество МУ | | | | | | |
|---|---|---|---|---|---|---|---|
| | 10 000 ПБ, ПМ, ПУ | 50 000 ПБ, ПМ, ПУ | 100 000 ПБ, ПМ, ПУ | 275 000 | | 550 000 | |
| | | | | ПБ | ПМ, ПУ | ПБ | ПМ, ПУ |
| Процессор | 2 ядра | 3 ядра | 3 ядра | 3 ядра | 4 ядра | 3 ядра | 6 ядер |
| Объем оперативной памяти | 3 Гб | 6 Гб | 8 Гб | 12 Гб | 12 Гб | 24 Гб | 24 Гб |
| Объем жесткого диска | SSD 275Гб | SSD 1.3ТБ | SSD 3ТБ | SSD 5.5ТБ | SSD 2ТБ | SSD 11ТБ | SSD 3.5ТБ |
| Количество серверов | 1 | 1 | 1 | 1 | 1 | 1 | 1 |

В таблице (Таблица 4) приведены программные характеристики серверов БД.

Таблица 4

| Параметр | Значение |
|---|---|
| Операционная система | Одна из следующих ОС:<br>– CentOS версии 7 или выше;<br>– CentOS версии 8 или выше;<br>– Альт 8 СП |
| СУБД | Одна из следующих СУБД:<br>– Postgres Pro 11;<br>– Postgres Pro 12;<br>– PostgreSQL 11.11 или выше (для ОС CentOS);<br>– PostgreSQL 12.6 или выше (для ОС CentOS) |
| СУБД для хранения сессий | Redis 6.0.10 или выше |
| Расширение СУБД PostgreSQL для партиционирования таблиц БД | `pg_partman` 4 или выше |
| Расширение СУБД PostgreSQL поддерживающее быстрый поиск схожих строк | `pg_trgm` |

В таблице (Таблица 5) приведены программные характеристики МУ.

Таблица 5

| Параметр | Значение |
|---|---|
| Операционная система | ОС Аврора |
| Прикладное программное обеспечение | – МП «Аврора Центр»;<br>– МП «Аврора Маркет» |

Для работы пользователей с веб-интерфейсом ППО должны использоваться веб-браузеры, поддерживающие технологии: TLS, CSS3, HTML5, ECMAScript 5 и Cookie. Рекомендуется использовать веб-браузер Chrome версии 75 или выше

Варианты конфигурации среды функционирования, в которых проводилось тестирование ППО, приведены в таблице (Таблица 6).

Таблица 6

| ОС | СУБД | СЗИ НСД |
|---|---|---|
| Сервер приложений | | |
| CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64 | | СЗИ НСД «Dallas Lock Linux» |
| CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64 | | Специальное программное обеспечение (СПО) СЗИ НСД «Аккорд-Х К» |
| CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64 | | СЗИ «Secret Net LSP» версия 1.10.1 |
| CentOS-8.0, kernel: 4.18.0-80.el8.x86_64 | | СЗИ «Secret Net LSP» версия 1.10.1 |
| Альт 8 СП | | |
| Сервер БД/сервер БД и сервер приложений | | |
| CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64 | PostgreSQL 11.11 | СПО СЗИ НСД «Аккорд-Х К» |
| CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64 | PostgreSQL 11.11 | СЗИ НСД «Dallas Lock Linux» |
| CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64 | PostgreSQL 11.11 | СЗИ «Secret Net LSP» версия 1.10.1 |
| CentOS-8.0, kernel: 4.18.0-80.el8.x86_64 | PostgreSQL 11.11 | СЗИ «Secret Net LSP» версия 1.10.1 |
| CentOS-7.5.1804, kernel: 3.10.0-862.11.6.el7.x86_64 | PostgreSQL 12.6 | СПО СЗИ НСД «Аккорд-Х К» |
| CentOS-7.6.1810, kernel: 3.10.0-957.el7.x86_64 | PostgreSQL 12.6 | СЗИ НСД «Dallas Lock Linux» |
| CentOS-7.7, kernel: 3.10.0-1062.9.1.el7.x86_64 | PostgreSQL 12.6 | СЗИ «Secret Net LSP» версия 1.10.1 |
| CentOS-8.0, kernel: 4.18.0-80.el8.x86_64 | PostgreSQL 12.6 | СЗИ «Secret Net LSP» версия 1.10.1 |
| Альт 8 СП | Postgres Pro | |

# 2. УСТАНОВКА ППО

ВНИМАНИЕ! При копировании команд в формате PDF из настоящего документа будьте внимательны. Администратор/Разработчик должен проверять результаты выполнения команд на экране.

## 2.1. Общая информация

Установка ППО и компонентов среды функционирования ППО осуществляется с помощью сценариев установки ППО, выполняемых на управляющей ПЭВМ и написанных с использованием декларативного языка разметки для описания конфигураций Ansible. Сценарии установки ППО позволяют выполнить установку как локально (все компоненты на одной ПЭВМ), так и с удаленной ПЭВМ (управляющей ПЭВМ) (Рисунок 1).

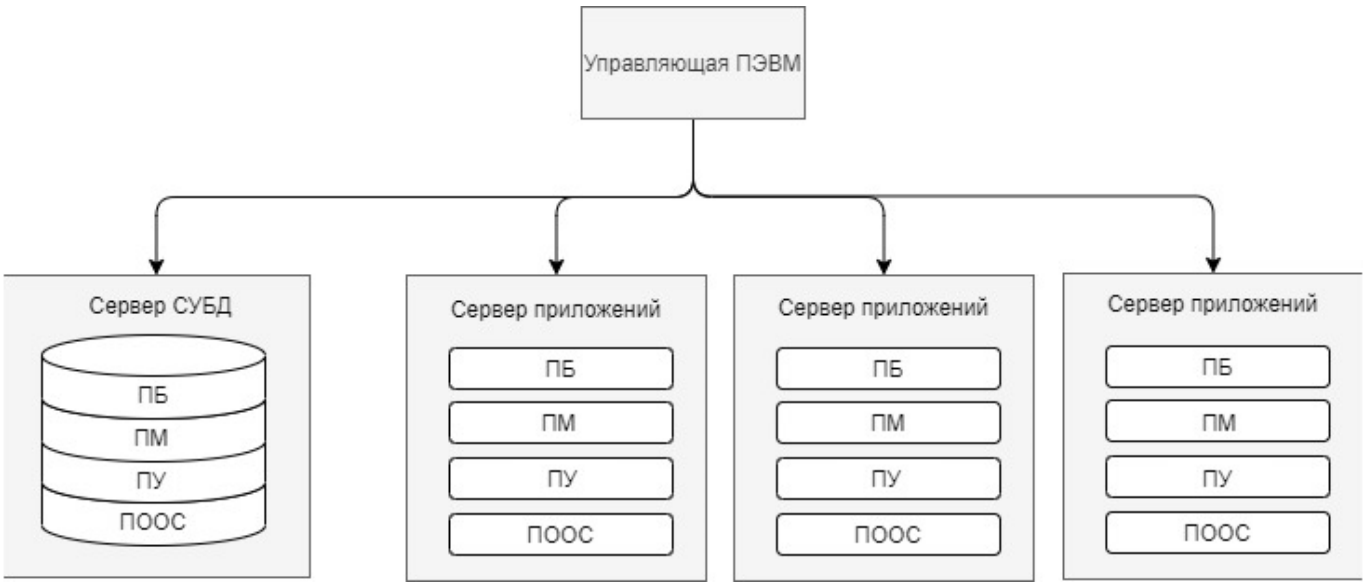



Рисунок 1

Управляющая ПЭВМ необходима только для установки ППО

Установка ППО осуществляется в два этапа:

1) Установка компонентов среды функционирования;
2) Установка ППО.

Предусмотрены следующие типы конфигурационных файлов:

1) Конфигурационные файлы сценариев установки среды функционирования ППО. Описание параметров конфигурационных файлов сценариев установки среды функционирования ППО приведено в разделе 7 настоящего документа;

2) Конфигурационные файлы модулей ППО:

– ПБ;

– ПМ;

– ПУ;

– ПООС.

Описание параметров конфигурационных файлов модулей ППО приведено в разделе 8 настоящего документа.

## 2.2. Порядок установки и настройки ОС на управляющей ПЭВМ, серверах приложений и серверах БД

Для установки и настройки ОС на управляющей ПЭВМ, серверах приложений и серверах БД необходимо выполнить следующие действия:

2.2.1. Установить ОС CentOS версии 7/8 или ОС Альт 8 СП на управляющую ПЭВМ, серверы приложений и серверы БД.

**ВНИМАНИЕ!** Перед установкой, указанной выше ОС необходимо ознакомиться с требованиями, приведенными в документации на СЗИ НСД.

ОС должна быть установлена в минимальной конфигурации без графического интерфейса. Для установки ОС CentOS версии 7/8 необходимо использовать iso-образ, в названии которого содержится «Minimal». Например, CentOS-7-x86_64-Minimal-1810.iso.

Настройки сети ОС должны удовлетворять следующим требованиям:

1) для основного сетевого интерфейса должен присутствовать конфигурационный `ifcfg` файл:

– ОС CentOS: `/etc/sysconfig/network-scripts/ifcfg-<имя интерфейса>`

**ВНИМАНИЕ!** Поддержка пакета `Network scripts` прекращена в ОС CentOS версии 8.x. Необходимо произвести его установку с помощью команды:

```
sudo yum install network-scripts
```

2) сетевой интерфейс должен автоматически запускаться при загрузке ОС.

Для этого значение параметра `ONBOOT` в `/etc/sysconfig/network-scripts/ifcfg-<имя интерфейса>` (для ОС CentOS) должно иметь значение «`yes`»:

```
ONBOOT=yes
```

3) приоритеты в конфигурационном файле `/etc/nsswitch.conf` файле должны выглядеть следующим образом (при использовании `dnsmasq`):

```
hosts: files dns ...
```

где `...` - остальные опции, если они используются.

2.2.2. Перейти в учетную запись пользователя `root` с помощью команды:

```
su -
```

2.2.3. Назначить пользователям ОС права на выполнение команд от имени суперпользователя `root`.

Для этого необходимо добавить пользователя в группу `wheel`, выполнив команду:

```
usermod -aG wheel "имя_пользователя"
```

Разрешить пользователям, входящим в группу `wheel`, выполнять команды без ввода пароля. Для чего в файле `/etc/sudoers` раскомментировать строку:

```
# %wheel    ALL=(ALL)      NOPASSWD: ALL
```

Открыть файл `/etc/sudoers` необходимо от имени суперпользователя `root` с помощью команды:

```
visudo
```

**ВНИМАНИЕ!** Права на выполнение команд от имени суперпользователя `root` должны быть назначены всем пользователям (на управляющей ПЭВМ, серверах приложений и серверах БД), которыми осуществляется установка компонентов среды функционирования, СУБД и ППО. В противном случае, в процессе установки возникнут ошибки.

2.2.4. Установить кодировку UTF-8 с помощью команды:

– ОС CentOS версии 7/8

```
localectl set-locale LANG=en_US.UTF-8
```

– ОС Альт 8 СП

В конфигурационном файле `/etc/sysconfig/i18n` задать следующее значение параметра `LANG`:

```
LANG=en_US.UTF-8
```

2.2.5. Задать имя хоста с помощью команды:

```
hostnamectl set-hostname "имя_хоста.имя_домена"
```

**ВНИМАНИЕ!** При задании имени хоста обязательно должно быть задано имя домена, которое отделяется точкой. Например:

```
hostnamectl set-hostname ocs-app.local
```

2.2.6. В настройках DNS-сервера или файлах `/etc/hosts` указать имена хостов (`hostname`) и полные имена доменов (`FQDN`) всех серверов кластера.

```
"ip-адрес" "имя_хоста.имя_домена"
```

Например (в файле `/etc/hosts`):

```
192.168.0.108 ocs-app.local
```

2.2.7. В файле `/etc/resolv.conf` указать адреса DNS-серверов:

```
nameserver "ip-адрес"
```

Например (в файле `/etc/hosts`):

```
nameserver 192.168.0.1
```

2.2.8. Настроить маршрут по-умолчанию (`default gateway`) через `lan` интерфейс согласно документации ОС.

2.2.9. В ОС CentOS отключить SELinux. Для этого в конфигурационном файле `/etc/selinux/config` необходимо задать следующее значение параметра `SELINUX`:

```
SELINUX=disabled
```

2.2.10. Отключить в ОС межсетевой экран с помощью выполнения следующих команд:

```
systemctl stop firewalld
systemctl disable firewalld
```

2.2.11. Задать текущие дату и время с помощью команды:

```
date -s 'YYYY-MM-DD HH:MI:SS'
```

Например:

```
date -s '2021-03-31 12:34:56'
```

2.2.12. Перезагрузить управляющую ПЭВМ и серверы с помощью команды:

```
reboot
```

## 2.3. Порядок развертывания и настройки управляющей ПЭВМ

**ВНИМАНИЕ!** Перед развертыванием и настройкой управляющей ПЭВМ должны быть установлены и настроены ОС на управляющей ПЭВМ, серверах приложений и серверах БД в соответствии с п. 2.2 настоящего документа.

Для развертывания и настройки управляющей ПЭВМ необходимо выполнить следующие действия:

2.3.1. Установить на управляющей ПЭВМ пакеты с помощью последовательного выполнения команд следующие пакеты:

– ОС CentOS версии 7/8 (управляющая ПЭВМ):

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install python2-pip
sudo python -m pip install --upgrade "pip < 21.0"
sudo python -m pip install wheel
sudo python -m pip install ansible==2.9.18
sudo yum -y install sed
sudo yum -y install coreutils
```

– ОС Альт 8 СП (управляющая ПЭВМ):

```
sudo apt-get install python-module-pip
sudo python -m pip install --upgrade "pip<21.0"
sudo python -m pip install ansible==2.9.18
sudo python -m pip install psycopg2
sudo apt-get -y install jq
sudo apt-get -y install coreutils
```

2.3.2. Настроить SSH доступ управляющей ПЭВМ к серверам приложений и серверам БД (даже в том случае, когда управляющая ПЭВМ и серверы установлены на одной ПЭВМ):

– сформировать ключевую пару на управляющем сервере:

```
ssh-keygen -t rsa
```

– скопировать открытый ключ на сервер приложений и БД:

```
ssh-copy-id <имя пользователя>@<сервер приложений>
ssh-copy-id <имя пользователя>@<сервер БД>
```

– проверить доступ с управляющей машины на серверы приложений и БД по SSH ключу (при выполнении команд ниже ввод пароля не должен требоваться):

```
ssh <имя пользователя>@<сервер приложения>
ssh <имя пользователя>@<сервер БД>
```

Управляющие команды, формируемые сценариями установки ППО, передаются с использованием протокола SSH

2.3.3. Создать на управляющей ПЭВМ отдельный каталог и скопировать в него каталог /server, находящийся на DVD с Изделием.

2.3.4. Перейти в каталог /server с помощью команды:

```
cd <путь к каталогу server>
```

2.3.5. Назначить пользователю право на исполнение файла installer-ac.sh с помощью команды:

```
chmod +x installer-ac.sh
```

2.3.6. Запустить installer-ac.sh с помощью команды:

```
./installer-ac.sh
```

2.3.7. Ознакомиться с «Лицензионным соглашением» и принять его

Для того чтобы принять «Лицензионное соглашение» (Рисунок 2), необходимо после вопроса «Вы принимаете условия лицензии (y/n)?» ввести «y».

В результате в каталоге с файлом installer-ac.sh будет создан каталог install-<версия ППО>. Например, /install-release-v2.5.1.

```
[omp@ocs-app ~]$ ./installer_ac.sh

ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ

ВАЖНО! ПЕРЕД ИСПОЛЬЗОВАНИЕМ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, К КОТОРОМУ ПРИЛАГАЕТСЯ ДАННОЕ ЛИЦЕНЗИОННОЕ СОГЛАШЕ
НИЕ С КОНЕЧНЫМ ПОЛЬЗОВАТЕЛЕМ (ДАЛЕЕ ПО ТЕКСТУ – «ЛИЦЕНЗИОННОЕ СОГЛАШЕНИЕ»), ПОЖАЛУЙСТА, ВНИМАТЕЛЬНО ПРОЧ
ИТАЙТЕ НИЖЕСЛЕДУЮЩИЕ УСЛОВИЯ. ЕСЛИ ВЫ НЕ СОГЛАШАЕТЕСЬ С УСЛОВИЯМИ НАСТОЯЩЕГО ЛИЦЕНЗИОННОГО СОГЛАШЕНИЯ, Т
О ВЫ НЕ ИМЕЕТЕ ПРАВА ИСПОЛЬЗОВАТЬ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ В КАКИХ-ЛИБО ЦЕЛЯХ.

1. ОПРЕДЕЛЕНИЯ
«Правообладатель» – общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открыт
ая мобильная платформа»), 420500, Республика Татарстан, Верхнеуслонский район, г. Иннополис, ул. Универс
итетская, д. 7, офис 59, ОГРН 1161690087020.
«ПО» – прикладное программное обеспечение «Аврора Центр» (ППО «Аврора Центр»), состоящее из следующих по
дсистем: прикладного программного обеспечения «Аврора Центр: Платформа управления» (ППО «Аврора Центр: П
латформа управления»), прикладного программного обеспечения «Аврора Центр: Маркет» (ППО «Аврора Центр: М
аркет») и Сервиса уведомлений Аврора, подробное описание функциональных возможностей которого содержатся
 в Документации. Данное Лицензионное соглашение применяется как к ППО «Аврора Центр», включающему в себя
 все перечисленные выше подсистемы, так и к каждой подсистеме в отдельности вне зависимости от комплектн
ости.
«Документация» – относящиеся к ПО сопроводительные материалы, в том числе Руководство по установке и нас
тройке, Руководство Пользователя, Руководство Администратора, которые принадлежат Правообладателю.
«Устройство» – это аппаратная система (физическая или виртуальная) со встроенным запоминающим устройство
м, на которых может быть запущено ПО.
«Права на интеллектуальную собственность» – все права на интеллектуальную и промышленную собственность,
включая права на изобретения, открытия и патенты на изобретения, включая заявки на выдачу патентов и пер
еизданные патенты, повторные заявки или заявки в продолжение и частичные продолжения; авторские права; о
бразцы и промышленные образцы; товарные знаки, знаки обслуживания, оформление товара и права на аналогич
ные объекты; секреты производства (ноу-хау), коммерческую тайну и конфиденциальную информацию; права на
топологии интегральных микросхем и права на фотошаблоны; и другие исключительные права.
«Лицензионное соглашение» – предоставляемое Вам Правообладателем ограниченное право на использование фун
кциональности ПО на условиях простой (неисключительной) лицензии в соответствии с условиями настоящего Л
ицензионного соглашения.
«Конечный пользователь» – любое юридическое лицо (организация), которое приобрело ПО для собственного ис
пользования и не для продажи.
«Пользователь» – физическое лицо, непосредственно осуществляющее эксплуатацию ПО в целях и порядке, опре
деляемом Конечным пользователем.
Настоящее Лицензионное соглашение является юридическим соглашением между Вами (далее по тексту – Конечны
й пользователь) и Правообладателем.
```

Рисунок 2

## 2.4. Порядок настройки компонентов среды функционирования ППО и ППО

### 2.4.1. Настройка компонентов среды функционирования

Для настройки компонентов среды функционирования необходимо выполнить следующие действия:

2.4.1.1. Перейти в каталог со сценариями установки с помощью команды:

```
cd install-<версия ППО>/install-ac/
```

Например:

```
cd install-release-v2.5.1/install-ac/
```

Дальнейшие действия по установке и настройке компонентов среды функционирования ППО, а также ППО, необходимо выполнять из данного каталога

2.4.1.2. В конфигурационном файле `inventories/hosts.yml` задать адреса серверов (имена хостов), на которые будут установлены компоненты среды функционирования ППО.

Для отображения адреса ПЭВМ необходимо выполнить команду:

```
hostname
```

Задание адресов осуществляется путем их добавления в секцию `hosts`, например:

```
...
        app:
          hosts:
            acenterapp01:
            acenterapp02:
            acenterapp03:
```

Допускается добавление адресов путем добавления хостов в группы, и дальнейшим переиспользованием групп. Например, для Nginx будут заданы адреса из группы `app`, которая заполнена выше:

```
...
    ocs:
      children:
        app:
          hosts:
            ocs-app.local:
        nginx:
          children:
            app:
```

Также допускается смешанное задание адресов путем их добавления в секцию `hosts` и путем добавления хостов в группы, и дальнейшим переиспользованием групп. Например, для Nginx будут заданы адреса из группы `app`, которая заполнена выше и адреса из секции `hosts`:

```
...
    ocs:
      children:
        app:
          hosts:
            acenterapp01:
            acenterapp02:
            acenterapp03:
        nginx:
          children:
```

```
        app:
      hosts:
        acenterapp04:
        acenterapp05:
```

Конфигурационный файл сценария установки среды функционирования ППО на одной ПЭВМ с адресом `ocs-app.local` имеет следующий вид:

```
all:
  children:
    ocs:
      children:
        app:
          hosts:
            ocs-app.local:
        postgresql:
          children:
            postgresql_masters:
              hosts:
                ocs-app.local:
            postgresql_slaves:
              hosts:
        nginx:
          children:
            app:
          hosts:
        consul:
          children:
            consul_servers:
              children:
                app:
              hosts:
            consul_agents:
        consul_template:
          children:
            app:
        nats_streaming_server:
          children:
                app:
          hosts:
        redis:
          children:
            redis_masters:
              children:
                app:
              hosts:
            sentinel:
              children:
                app:
              hosts:
```

Примеры файлов `hosts.yml` для однонодовой и кластерной конфигурации приведены в каталоге `samples/ac/inventories/`.

Описание параметров конфигурационного файла `inventories/hosts.yml` приведено в п. 7.1.1 настоящего документа.

2.4.1.3. В конфигурационном файле `config/vars/_vars.yml` необходимо задать либо поменять предустановленные значения следующих параметров:

– параметры подключения подсистем ППО к БД

```
postgresql:
  dbname: example_db_name     # database name
  port: 5432                  # port
  user: example_user          # user
  password: ocs               # password
```

– пароль суперпользователя СУБД Postgresql, который был задан при установке СУБД:

```
postgres_password: "postgres"
```

– токен доступа к сервису гарантированной доставки сообщений `Nats Streaming Server`:

```
nats: auth_token: "FF12fddgdhFLL"
```

– пароль доступа к СУБД Redis в параметре `redis_password`:

```
redis_password: "@rTT9089087fslk"
```

– токен доступа к системе обнаружения сервисов `Consul`:

```
consul_acl_master_token: "ae9f5abb-6b8f-9252-59c5-53bcb651f182"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 7.1.2 настоящего документа.

2.4.1.4. Настроить параметры взаимодействия клиентов СУБД (при необходимости).

По умолчанию сценарии установки автоматически задают параметры взаимодействия клиентов (например, серверов приложений ППО) СУБД.

Дополнительную настройку взаимодействия клиентов СУБД необходимо осуществлять в соответствии с п. 2.8.2 настоящего документа.

### 2.4.2. Настройка ППО (подсистем ППО)

**ВНИМАНИЕ!** Перед выполнением настроек необходимо ознакомиться с информацией, приведенной в п. 8.2.7 настоящего документа.

Для настройки ППО необходимо выполнить следующие действия:

2.4.2.1. Перейти в созданный каталог (каталог: `/install-<версия ППО>/install-ac/`) и отредактировать конфигурационный файл `config/vars/_vars.yml`

В данном конфигурационном файле необходимо задать, либо поменять предустановленные значения:

– доменное имя для межсервисного взаимодействия в рамках одной ноды (узла сервера) должно иметь значение `local` (`domain: local`);

– внешние (публичные) адреса ППО, например:

```
aps_admin_address: "http://ocs-app.local:8009"
aps_client_address: "http://ocs-app.local:8009"
aps_dev_address: "http://ocs-app.local:8009"
aps_market_address: "http://ocs-app.local:8009"
auth_admin_address: "http://ocs-app.local:8009"
auth_public_address: "http://ocs-app.local:8009"
emm_admin_address: "http://ocs-app.local:8009"
emm_mobile_address: "http://ocs-app.local:8009"
pkgrepo_admin_address: "http://ocs-app.local:8009"
pkgrepo_mobile_address: "http://ocs-app.local:8009"
push_admin_address: "http://ocs-app.local:8009"
push_public_address: http://ocs-app.local:8009
```

При установке ППО в однонодовой конфигурации внешний адрес ППО в указанных выше параметрах можно не задавать. В данном случае будет использовать адрес, заданный в группе app конфигурационного файла `inventories/hosts.yml`.

– уровень детализации сообщений логирования (рекомендуется задать "`info`" при тестовой эксплуатации и "`warning`" при промышленной эксплуатации):

```
logger_level: "info"
```

Описание `config/vars/_vars.yml` параметров конфигурационного файла приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

2.4.2.2. Задать секретные ключи клиентов (сервисов)

Можно задать один общий ключ для всех клиентов, либо задать отдельный ключ для каждого клиента.

Общий ключ задается в параметре `ac_common_client_secret` конфигурационного файла `config/vars/_vars.yml`, например:

```
ac_common_client_secret: "7dd7c204aa4f6192e70fadc5642d3755" # common
OIDC client secret for AC installation
```

Описание `config/vars/_vars.yml` параметров конфигурационного файла приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

Секретные ключи клиентов (сервисов) задаются в параметре `*_client_secret` конфигурационных файлов подсистем ППО (файлы: `config/subsystems/<название подсистемы>/vars/_vars.yml`) например:

```
auth_admin_console_client_secret: "7dd7c204aa4f6192e70fadc5642d3755"
# Secret for OIDC client auth-admin-console
```

Описание параметров конфигурационных файлов `config/subsystems/<название подсистемы>/vars/_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

2.4.2.3. В секциях `system` и `cookie` конфигурационного файла `config/subsystems/auth/config/services/config.yml.j2` задать пароли, используемые для защиты критичной информации (например, `cookie` сессии).

**ВНИМАНИЕ!** Длина пароля должна быть не менее 16 символов.

Для этого необходимо удалить приведенные примеры и задать новые значения паролей, например:

```
    system:
      - kdj%93cxk+57nMa4
    cookie:
      - 9v_wer8*&r=_hY8u
```

**ВНИМАНИЕ!** При обновлении ППО нельзя удалять старые пароли. Новые пароли должны быть добавлены в начало списка.

Описание параметров конфигурационного файла `config/subsystems/auth/config/services/config.yml.j2` приведено в п. 8.3.2 настоящего документа.

2.4.2.4. Выполнить настройки безопасности ППО, другие дополнительные настройки ППО и настройки подсистем ППО (при необходимости).

**ВНИМАНИЕ!** Перед установкой ППО необходимо выполнить настройки безопасности ППО, дополнительные настройки ППО и настройки подсистем ППО (при необходимости).

Перечень и описание дополнительных настроек ППО приведен в подразделе 2.8 настоящего документа.

## 2.5. Порядок установки компонентов среды функционирования ППО и ППО

### 2.5.1. Установка компонентов среды функционирования ППО

Для установки компонентов среды функционирования ППО необходимо выполнить действия, описанные ниже.

2.5.1.1. Обеспечить синхронизацию времени между нодами кластера

При эксплуатации ППО в кластерной конфигурации, необходимо обеспечить синхронизацию времени между нодами кластера (например, с помощью утилиты `chrony`).

Для проверки синхронизации времени необходимо запустить bash-скрипт, предварительно задав адреса хостов в переменной `HOSTS`:

```
#!/bin/bash
HOSTS="
example-db01.ompcloud
example-db02.ompcloud
example-inp1int01.ompcloud
example-inp1int02.ompcloud
example-inp1int03.ompcloud
"
# Prepare ssh sessions to increase speed time checking.
for i in $HOSTS
do
  ssh $i "echo $i session created" > /dev/null
```

```
done
for i in $HOSTS
do
  ssh $i "echo $i `date`" &
done
sleep 10
```

2.5.1.2. Отключить сокрытие ошибок в конвейере (pipeline) с помощью команды:

```
set -o pipefail
```

2.5.1.3. Установить на серверы приложений и серверы БД необходимые пакеты с помощью команд:

– серверы приложений:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u <имя пользователя> --extra-vars
"node_type=app" --limit app
```

– серверы БД:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u <имя пользователя> --extra-vars
"node_type=db" --limit postgresql
```

Например:

– серверы приложений:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u omp --extra-vars "node_type=app" --limit app
```

– серверы БД:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u omp --extra-vars "node_type=db" --limit
postgresql
```

Для того, чтобы установить все пакеты на все серверы (на все серверы приложений и серверы БД независимо от их типа) необходимо выполнить команду:

```
ansible-playbook -i inventories/hosts.yml play-managed-node-
prerequisites.yml -vv -u <имя пользователя>
```

Порядок действий для самостоятельной установки пакетов приведен в п. 2.8.8 настоящего документа.

2.5.1.4. Установить компоненты среды функционирования ППО с помощью команды:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh --database
"<версия СУБД PostgreSQL>" --extra-vars "force_upgrade=true"
```

Например:

```
ANSIBLE_USER="omp" ./deploy-infra.sh --database "11" --extra-vars
"force_upgrade=true"
```

В случае, если требуется репликация БД, команду установки компонентов среды функционирования необходимо запустить с параметром `--extra-vars "pg_slave_recreate=true"`:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh --database
"<версия СУБД PostgreSQL>" --extra-vars "force_upgrade=true
pg_slave_recreate=true"
```

Описание параметров запуска скрипта `deploy-infra.sh` и их возможные значения приведены в подразделе 3.1 настоящего документа.

ВНИМАНИЕ! Скрипт `deploy-infra.sh` позволяет устанавливать только СУБД PostgreSQL 11/12. СУБД Postgres Pro необходимо устанавливать самостоятельно.

При использовании СУБД Postgres Pro либо, если установку СУБД PostgreSQL 11/12 необходимо выполнить самостоятельно (без использования сценариев установки компонентов среды функционирования ППО), то команда установки компонентов среды функционирования имеет следующий вид:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh --skip-database
```

Описание установки и настройки СУБД Postgres Pro, а также требования к самостоятельной установке СУБД приведены подразделе 2.7 настоящего документа.

Также можно выполнить установку компонентов среды функционирования по отдельности с помощью следующих команд:

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c dnsmasq --
extra-vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c nginx --extra-
vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c consul --extra-
vars "force_upgrade=true"
```

```
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c consul-template
--extra-vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c nats-streaming-
server --extra-vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c redis --extra-
vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c ocs-user --
extra-vars "force_upgrade=true"
ANSIBLE_USER="<имя пользователя>" ./deploy-infra.sh -c db --database
<версия СУБД PostgreSQL> --extra-vars "force_upgrade=true"
```

### 2.5.2. Установка ППО

Для установки ППО необходимо выполнить команду:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --database <СУБД>
```

Описание параметров запуска скрипта `deploy-ac.sh` и их возможные значения приведены в подразделе 3.2 настоящего документа.

Например:

```
ANSIBLE_USER=omp ./deploy-ac.sh --database 11
```

Для установки подсистем по отдельности необходимо в параметре --subsystems задать имя подсистемы. Пример установки подсистем ПБ, ПМ, ПУ и ПООС по отдельности:

```
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems auth --database 11
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems appstore --database 11
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems emm --database 11
ANSIBLE_USER=omp ./deploy-ac.sh --subsystems pkgrepo --database 11
```

### 2.5.3. Выполнить ограничения по применению, а также выполнить настройки СЗИ и настройки безопасности компонентов среды функционирования

**ВНИМАНИЕ!** После установки и настройки ППО необходимо выполнить ограничения по применению, выполнить настройки безопасности компонентов среды функционирования и настроить СЗИ. Необходимая информация приведена в п. 2.8.7 настоящего документа.

### 2.5.4. Проверка корректности установки и функционирования ППО

Проверка осуществляется в соответствии с подразделом 2.11 настоящего документа.

## 2.6. Адреса веб-консолей

Первоначальный вход в ППО осуществляется с помощью Консоли администратора ПБ и предустановленной учетной записи с ролью Администратор учетных записей:

– логин: admin@omprussia.ru;

– пароль: admin.

При первом входе в ППО необходимо сменить пароль

В таблице (Таблица 7) приведены адреса веб-консолей.

Таблица 7

| Веб-консоль | URL-адрес веб-консоли |
|---|---|
| **При разделении трафика по портам** | |
| Консоль администратора ПБ | http://<сервер приложения>:8019 |
| Консоль администратора ПМ | http://<сервер приложения>:8015 |
| Консоль разработчика ПМ | http://<сервер приложения>:8014 |
| Консоль администратора ПУ | http://<сервер приложения>:8011 |
| **При разделении трафика по basepath (url-адресам)** | |
| Консоль администратора ПБ | http://<сервер приложения>:8009/auth/admin/ |
| Консоль администратора ПМ | http://<сервер приложения>:8009/appstore/admin/ |
| Консоль разработчика ПМ | http://<сервер приложения>:8009/appstore/dev/ |
| Консоль администратора ПУ | http://<сервер приложения>:8009/emm/admin/ |

## 2.7. Самостоятельная установка и настройка СУБД

### 2.7.1. Порядок установки и настройки СУБД Postgres Pro

Для установки и настройки СУБД Postgres Pro необходимо выполнить следующие действия:

2.7.1.1. Установить на серверы БД с помощью последовательного выполнения команд следующие пакеты:

– ОС CentOS версии 7 (сервер БД):

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install unzip
sudo yum -y install perl-libs
sudo yum -y install libxslt
sudo yum -y install postgresql-libs
sudo yum -y install libicu
sudo yum -y install python-psycopg2
```

– ОС Альт 8 СП (сервер БД):

```
sudo apt-get -y install jq
sudo apt-get -y install unzip
sudo apt-get -y install python-module-pkginfo
```

2.7.1.2. Установить и инициализировать СУБД Postgres Pro

При инициализации СУБД должны быть установлены следующие значения параметров:

```
LC_COLLATE 'en_US.UTF-8'
LC_CTYPE 'en_US.UTF-8'
ENCODING UTF8
```

Установка и инициализация СУБД Postgres Pro осуществляется в соответствии с эксплуатационной документацией на СУБД. После установки СУБД необходимо назначить пароль для пользователя `postgres` и создать на время установки символьную ссылку (`symlink`) для сокета PostgreSQL PRO с помощью следующих команд:

```
psql -U postgres
ALTER USER postgres with PASSWORD 'пароль';
exit
sudo ln -s /tmp /var/run/postgresql
```

2.7.1.3. В конфигурационных файлах СУБД `pg_hba.conf и postgresql.conf` задать следующие параметры:

– тип соединения, диапазон IP-адресов клиентов БД;

– имя БД, имя пользователя;

– способ аутентификации клиентов;

– пароль пользователя СУБД в параметре `pg_superuser_password`.

2.7.1.4. Установить расширение `pg_partman` с помощью команды:

– ОС CentOS версии 7

```
sudo rpm -ivh pg_partman11pro-v4.3.0-1.el7.x86_64.rpm
```

– ОС Альт 8 СП

```
sudo rpm -ivh pg_partman11pro-4.3.0-1.alt.x86_64.rpm
```

Указанные rpm-пакеты находятся на DVD с загрузочными модулями ППО в каталоге `/server/install-infra.tar.gz/install-infra/binary/postgresql/pg_partman/`.

2.7.1.5. Перезапустить сервис СУБД Postgres Pro с помощью команды:

```
sudo systemctl restart postgrespro-std-11
```

### 2.7.2. Порядок установки и настройки СУБД PostgreSQL 11/12

2.7.2.1. Установить на серверы БД, работающие под управлением ОС CentOS с помощью последовательного выполнения команд следующие пакеты:

– ОС CentOS версии 7 (сервер БД):

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install unzip
sudo yum -y install perl-libs
sudo yum -y install libxslt
sudo yum -y install postgresql-libs
sudo yum -y install libicu
sudo yum -y install python-psycopg2
```

– ОС CentOS версии 8 (сервер БД):

```
sudo yum -y install epel-release
sudo yum -y install jq
sudo yum -y install unzip
sudo yum -y install perl-libs
sudo yum -y install libxslt
sudo yum -y install postgresql-libs
sudo yum -y install libicu
sudo yum -y install python-psycopg2
sudo yum -y install python38
sudo yum -y install python38-pip
ln -s /usr/libexec/platform-python /usr/bin/python
```

2.7.2.2. Выполнить установку и настройку СУБД PostgreSQL 11/12 в соответствии с документацией на СУБД.

При инициализации СУБД должны быть установлены следующие значения параметров:

```
LC_COLLATE 'en_US.UTF-8'
LC_CTYPE 'en_US.UTF-8'
ENCODING UTF8
```

2.7.2.3. Установить расширение pg_partman с помощью команды:

– ОС CentOS версии 7 и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.2.0-1.rhel7.x86_64.rpm
```

– ОС CentOS версии 8 и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.4.0-1.rhel8.x86_64.rpm
```

– ОС Альт 8 СП и СУБД PostgreSQL 11

```
sudo rpm -ivh pg_partman11-4.1.0-1-alt.x86_64.rpm
```

– ОС CentOS версии 7 и СУБД PostgreSQL 12

```
sudo rpm -ivh pg_partman12-4.4.1-1.rhel7.x86_64.rpm
```

– ОС CentOS версии 8 и СУБД PostgreSQL 12

```
sudo rpm -ivh pg_partman12-4.4.0-1.rhel8.x86_64.rpm
```

Указанные rpm-пакеты находятся на DVD с загрузочными модулями ППО в каталоге `/server/install-infra.tar.gz/install-infra/binary/postgresql/pg_partman/`.

2.7.2.4. Перезапустить сервис СУБД 12 в соответствии с документацией на СУБД.

## 2.8. Дополнительные настройки ППО и среды функционирования ППО

### 2.8.1. Настройка взаимодействия сервера приложений ПУ с SMTP-сервером

Для настройки взаимодействия ППО с SMTP-сервером необходимо в секции `SMTP` конфигурационного файла сценариев установки ПУ `_vars.yml` (`config/subsystems/emm/vars/_vars.yml`) задать требуемые значения:

– адрес эл. почты, с которого отправляются письма (параметр: `from`);

– адрес сервера эл. почты (параметр: `address`);

– тип аутентификации (параметр: `authType`);

– параметры для заданного типа аутентификации (`usrername, password` и др.).

---

Значения параметров `from` и `username` должны быть идентичны, иначе почтовый сервер будет отклонять сообщения

---

Описание параметров конфигурационного файла сценариев установки ПУ `_vars.yml` (`config/subsystems/emm/vars/_vars.yml`) приведено в п. 8.3.4 настоящего документа.

В ПУ поддерживаются `PLAIN`, `CRAM-MD5`, `LOGIN` типы аутентификации `SMTP`. В зависимости от используемого типа аутентификации необходимо задать следующие параметры (остальные параметры оставить без изменений):

– `PLAIN`

```
smtp:
  from: "user@example.com"
  address: "smtp.example.com:1025"
  tls: true
  authType: "PLAIN"
  host: "example.com"
  username: "test_username"
  password: "test_password"
  identity: "identity"
```

– CRAM-MD5

```
smtp:
  from: "user@example.com"
  address: "smtp.example.com:1025"
  tls: true
  authType: "CRAM-MD5"
  username: "test_username"
  secret: "test_secret"
```

– LOGIN

```
smtp:
  from: "user@example.com"
  address: "smtp.example.com:1025"
  tls: true
  authType: "LOGIN"
  username: "test_username"
  password: "test_password"
```

– без аутентификации

```
smtp:
  from: "user@example.com"
  address: "smtp.example.com:1025"
  tls: true
```

### 2.8.2. Настройка взаимодействия клиентов СУБД

Настройки взаимодействия клиентов с СУБД задаются в секции `pg_hba_settings` конфигурационного файла `config/vars/_vars_infra.yml`.

В данной секции содержатся следующие параметры:

– `type` - тип подключения к СУБД;

– `name` - имена пользователей СУБД, правила доступа для которых определяет данная запись;

– `database` - имена баз данных, доступ к которым описывает данная запись;

– `address` - IP-адрес подключения или IP-адрес подсети;

– `method` - метод аутентификации.

Описание секций конфигурационного файла приведено в п. 7.1.3 настоящего документа.

### 2.8.3. Настройка разделения трафика

ППО позволяет разделять входящий трафик (url-запросы) следующими способами:

– по портам - в данном случае каждая Консоль администратора/разработчика (либо API для взаимодействия с МП) привязана к определенному порту;

– по `basepath` (url-адресам) - в данном случае каждая Консоль администратора/разработчика (либо API для взаимодействия с МП) привязана к определенному url-адресу;

– по доменам (субдоменам) – в данном случае каждая Консоль администратора/разработчика и API для взаимодействия с МП (либо группа консолей и API) привязана к определенному домену. Рекомендуется публичные консоли и API привязывать к домену, который имеет доступ из сети Интернет, а внутренние консоли (Консоли администраторов) привязывать к домену, не имеющему доступ из сети Интернет.

При установке ППО «по умолчанию» разделение трафика осуществляется по `basepath` (url-адресам)

Для того чтобы выполнить настройку разделения трафика, необходимо в конфигурационном файле `config/vars/_vars.yml` задать значения параметров в соответствии с таблицей (Таблица 8).

Приведенные в таблице значения `basepath` (не пустые значения `basepath`) и номера портов носят рекомендательный характер и могут быть изменены. При разделении трафика по портам значения `basepath` в конфигурационном файле должны быть пустыми, кроме **`pkgrepo_repo_basepath`**.

Таблица 8

| Сервис (модуль) | Параметры |
|---|---|
| **При разделении трафика по портам** | |
| `Auth public API gateway` (интерфейс ППО для идентификации и | `auth_public_address: http://<сервер приложения>:8018`<br>`auth_public_basepath: ""` |

| Сервис (модуль) | Параметры |
|---|---|
| аутентификации пользователей) | |
| `Auth admin API gateway` (Консоль администратора ПБ) | `auth_admin_address: "http://<сервер приложения>:8019"`<br>`auth_admin_basepath: ""` |
| `AMM device API gateway` (API для взаимодействия с МП «Аврора Центр») | `emm_mobile_address: "http://<сервер приложения>:8012"`<br>`emm_mobile_basepath: ""` |
| `AMM admin API gateway` (Консоль администратора ПУ) | `emm_admin_address: "http://<сервер приложения>:8011"`<br>`emm_admin_basepath: ""` |
| `Aurora market admin API gateway` (Консоль администратора ПМ) | `aps_admin_address: "http://<сервер приложения>:8015"`<br>`aps_admin_basepath: ""` |
| `Aurora market development API gateway` (Консоль разработчика ПМ) | `aps_dev_address: "http://<сервер приложения>:8014"`<br>`aps_dev_basepath: ""` |
| `Aurora market client API gateway` (API для взаимодействия с МП «Аврора Маркет») | `aps_client_address: "http://<сервер приложения>:8016"`<br>`aps_market_address: "http://<сервер приложения>:8016"`<br>`aps_client_basepath: ""`<br>`aps_market_basepath: ""` |
| `Package repository admin API gateway` (API для взаимодействия с ПООС, только для взаимодействия ПУ с ПООС) | `pkgrepo_admin_address: "http://<сервер приложения>:8022"`<br>`pkgrepo_admin_basepath: ""` |
| `Package repository device API` (API для взаимодействия МУ с ПООС) | `pkgrepo_mobile_address: "http://<сервер приложения>:8023"`<br>`pkgrepo_mobile_basepath: ""` |
| Файловый сервер ПООС | `pkgrepo_repo_address: http://<сервер приложения>:8030` |

| Сервис (модуль) | Параметры |
|---|---|
| | pkgrepo_repo_basepath: "/pkgrepo/mobile" |
| При разделении трафика по basepath (url-адресам) | |
| Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей) | auth_public_address: "http://<сервер приложения>:8009"<br>auth_public_basepath: "/auth/public" |
| Auth admin API gateway (Консоль администратора ПБ) | auth_admin_address: "http://<сервер приложения>:8009"<br>auth_admin_basepath: "/auth/admin" |
| AMM device API gateway (API для взаимодействия с МП «Аврора Центр») | emm_mobile_address: "http://<сервер приложения>:8009"<br>emm_mobile_basepath: "/emm/mobile" |
| AMM admin API gateway (Консоль администратора ПУ) | emm_admin_address: "http://<сервер приложения>:8009"<br>emm_admin_basepath: "/emm/admin" |
| Aurora market admin API gateway (Консоль администратора ПМ) | aps_admin_address: "http://<сервер приложения>:8009"<br>aps_admin_basepath: "/appstore/admin" |
| Aurora market development API gateway (Консоль разработчика ПМ) | aps_dev_address: "http://<сервер приложения>:8009"<br>aps_dev_basepath: "/appstore/dev" |
| Aurora market client API gateway (API для взаимодействия с МП «Аврора Маркет») | aps_client_address: "http://<сервер приложения>:8009"<br>aps_market_address: "http://<сервер приложения>:8009"<br>aps_client_basepath: "/appstore/mobile"<br>aps_market_basepath: "/appstore/mobile" |
| Package repository admin API gateway (API для взаимодействия с ПООС, только для взаимодействия ПУ с | pkgrepo_admin_address: "http://<сервер приложения>:8009"<br>pkgrepo_admin_basepath: "/pkgrepo/admin" |

| Сервис (модуль) | Параметры |
|---|---|
| ПООС) | |
| Package repository device API (API для взаимодействия МУ с ПООС) | pkgrepo_mobile_address: "http://<сервер приложения>:8009"<br>pkgrepo_mobile_basepath: "/pkgrepo/mobile" |
| Файловый сервер ПООС | pkgrepo_repo_basepath: "/pkgrepo/mobile"<br>pkgrepo_repo_address: "http://<сервер приложения>:8009" |
| При разделении трафика по доменам | |
| Auth public API gateway (интерфейс ППО для идентификации и аутентификации пользователей) | auth_public_basepath: ""<br>auth_public_address: "http://<субдомен.домен>" |
| Auth admin API gateway (Консоль администратора ПБ) | auth_admin_address: http://<субдомен.домен><br>auth_admin_basepath: "" |
| AMM device API gateway (API для взаимодействия с МП «Аврора Центр») | emm_mobile_address: "http://<субдомен.домен>"<br>emm_mobile_basepath: "" |
| AMM admin API gateway (Консоль администратора ПУ) | emm_admin_address: "http://<субдомен.домен>"<br>emm_admin_basepath: "" |
| Aurora market admin API gateway (Консоль администратора ПМ) | aps_admin_address: "http://<субдомен.домен>"<br>aps_admin_basepath: "" |
| Aurora market development API gateway (Консоль разработчика ПМ) | aps_dev_address: "http://<субдомен.домен>"<br>aps_dev_basepath: "" |
| Aurora market client API gateway (API для взаимодействия | aps_client_address: "http://<субдомен.домен>"<br>aps_market_address: "http://<субдомен.домен>"<br>aps_client_basepath: ""<br>aps_market_basepath: "" |

| Сервис (модуль) | Параметры |
|---|---|
| с МП «Аврора Маркет») | |
| Package repository admin API gateway (API для взаимодействия с ПООС, только для взаимодействия ПУ с ПООС) | pkgrepo_admin_address: "http://<субдомен.домен>"<br>pkgrepo_admin_basepath: "" |
| Package repository device API (API для взаимодействия МУ с ПООС) | pkgrepo_mobile_address: "http://<субдомен.домен>"<br>pkgrepo_mobile_basepath: "" |
| Файловый сервер ПООС | pkgrepo_repo_address: http://<субдомен.домен><br>pkgrepo_repo_basepath: "/pkgrepo/mobile" |

Также в параметре `listen` конфигурационного файла `config/subsystems/pkgrepo/vars/ocs-pkgrepo-nginx-static.yml` необходимо задать внешний (публичный) порт для взаимодействия МУ с ПООС. Значение порта должно соответствовать значению порта, указанному в параметре `pkgrepo_mobile_address` конфигурационного файла `config/vars/_vars.yml`.

Ниже приведен пример разделение трафика на два домена (внутренний – не доступный из сети Интернет, и внешний – доступный из сети Интернет):

```
aps_admin_address: "https://int-ocs.ompcloud"
aps_dev_address: "https://int-ocs.ompcloud"
aps_market_address: "https://int-ocs.ompcloud.ru"
auth_admin_address: "https://int-ocs.ompcloud"
auth_public_address: "https://int-ocs.ompcloud.ru"
emm_admin_address: "https://int-ocs.ompcloud"
emm_mobile_address: "https://int-ocs.ompcloud.ru"
pkgrepo_admin_address: "https://int-ocs.ompcloud.ru"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

### 2.8.4. Пример настройки единого файлового хранилища

Установить NFS сервер в соответствии с официальной документацией на ОС RedHat, приведенной на следующей странице: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/storage_administration_guide/nfs-serverconfig.

Выполнить монтирование файловой системы NFS к каталогу /ocs с помощью команды:

```
mount example.com:/export/ocsfs /ocs
```

где,

- example.com – имя узла файлового сервера NFS;
- /export/ocsfs – каталог, который экспортирует example.com;
- /ocs – каталог, к которому осуществляется монтирование.

Для проверки корректности монтирования необходимо выполнить команду:

```
ls /ocs
```

и убедиться, что полученный список файлов соответствует списку файлов в каталоге /export/ocsfs на компьютере example.com.

Также выполнить монтирование файловой системы NFS можно путем редактирования файла /etc/fstab. Для этого в данный файл необходимо добавить запись следующего вида:

```
example.com:/export/ocsfs /ocs nfs defaults 0 0
```

Редактирование файла /etc/fstab должно осуществляться пользователем с правами root.

В файловом хранилище создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, rpm-пакеты), загружаемые разработчиками. Для этого нужно создать каталог в соответствии с параметром filestorage_path конфигурационного файла config/subsystems/appstore/vars/_vars.yml и в созданном каталоге создать каталог applications-api:

```
mkdir -p /ocs/appstore/applications-api
```

Параметр `filestorage_path` конфигурационного файла `config/subsystems/appstore/vars/_vars.yml` может иметь следующий вид:

```
filestorage_path: "/ocs/appstore"
```

Описание параметров конфигурационного файла `config/subsystems/appstore/vars/_vars.yml` приведено в п. 8.3.3 настоящего документа.

В файловом хранилище создать каталог, в котором будут храниться пакеты ОС ПООС:

```
mkdir -p /ocs/pkgrepo
```

Создаваемый каталог должен соответствовать параметрам, заданным в конфигурационном файле `pkgrepo.nginx.conf` веб-сервера Nginx Web Server.

### 2.8.5. Настройка кэширования ответов сервисов

Для увеличения производительности ППО применяется кэширование ответов сервисов с помощью Nginx. При этом доступ к закэшированным данным осуществляется через шлюзы доступа ППО.

Настройки кэширования задаются в следующих конфигурационных файлах сценариев установки среды функционирования ППО:

1) в конфигурационном файле `shared_roles/nginx/defaults/main.yml` задаются:

– `cache_enabled` - включение/выключение кэширования;

– `cache_path` - каталог хранения кэша;

– `keys_zone` - имя зоны в разделяемой памяти, где будет храниться кэш;

– `keys_zone_size` - размер зоны в разделяемой памяти;

– `cache_max_size` - максимальный размер выделяемой под кэш памяти (когда место заканчивается, nginx сам удаляет устаревшие данные);

– `cache_inactive` - время, после которого кэш будет автоматически очищаться.

Например:

```
cache_enabled: true
cache_path: "/var/cache/nginx"
keys_zone: "proxy_cache"
keys_zone_size: "50m"
cache_max_size: "10G"
cache_inactive: "30m"
```

Максимальный размер выделяемой под кэш памяти должен быть не менее 10 Гб

2) в конфигурационных файлах `config/subsystems/<название подсистемы>/vars/services.yml` задаются API функции (endpoint-ы) ППО для которых необходимо выполнять кэширование, а также параметры кэширования для каждой API функции:

– `proxy_cache` - включение кэширования для API функции;

– `proxy_cache_valid` - время кэширования ответа (возможно задать время кэширования для определенных статусов ответа);

– `proxy_cache_lock` - параметр определяет возможность прохождения нескольких запросов на бэкенд (к сервисам ППО). При значении «on» запрещается прохождение нескольких запросов к сервису ППО, все повторные запросы будут ожидать появления ответа в кэше, либо таймаут блокировки запроса к странице.

– `proxy_cache_use_stale` - параметр определяет, в каких случаях можно использовать устаревший закэшированный ответ;

– `add_header: "X-Cache-Status $upstream_cache_status"` - директива добавляет HTTP-заголовок, содержащий статус кэширования.

Например:

```
...
      nginx_location_dashboard:
        path: "~ /v1/dashboards/[^/]+$"
        proxy_cache: "proxy_cache"
        proxy_cache_valid: "200 {{ cache_interval_dynamic }}"
        proxy_cache_lock: "on"
        proxy_cache_use_stale: "updating"
        proxy_cache_background_update: "on"
        add_header: "X-Cache-Status $upstream_cache_status"
```

### 2.8.6. Действия по безопасной установке и настройке средства

Установка, настройка и эксплуатация ППО должна осуществляться в соответствии с эксплуатационной документацией на ППО.

При использовании ППО в ГИС, не содержащих информации, составляющей государственной тайны 1 класса защищенности, в ИС персональных данных 1 уровня защищенности и в автоматизированных системах управления 1 класса защищенности должны быть установлены значения параметров, приведенные в таблице (Таблица 9).

Таблица 9

| Параметр | Значение (для ГИС 1-го класса) |
|---|---|
| Конфигурационный файл ПБ (сценария установки ПБ): `/var/ocs/auth/config.yml` (`config/subsystems/auth/config/services/config.yml.j2`) | |
| Период времени неиспользования идентификатора (учетной записи) пользователя, через которое происходит его блокирование: `config.maxAccountInactivityPeriod` | не более 45 дней<br>`maxAccountInactivityPeriod: 1080h` |
| Минимальная длина пароля: `config.passwordSettings.minLength` | не менее 8 символов<br>`config.passwordSettings.minLength: 8` |
| Алфавит пароля:<br>`config.passwordSettings.minDigits`<br>`config.passwordSettings.minUpperLetters`<br>`config.passwordSettings.minLowerLetters`<br>`config.passwordSettings.minSpecialChars` | не менее 70 символов<br>`minDigits: 1`<br>`minUpperLetters: 1`<br>`minLowerLetters: 1`<br>`minSpecialChars: 1` |
| Максимальное время действия пароля: `config.passwordExpirationTime` | не более 60 дней<br>`passwordExpirationTime: "1440h"` |

| Параметр | Значение (для ГИС 1-го класса) |
|---|---|
| Число последних использованных паролей, которые запрещено использовать пользователями при создании новых паролей:<br>`config.passwordHistoryDepth` | `passwordHistoryDepth: 3` |
| Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки:<br>`config.failedLoginTries` | не более 3<br>`failedLoginTries: 3` |
| Время блокировки учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации:<br>`config.failedLoginBlockTime` | не менее 15 минут<br>`failedLoginBlockTime: "15m"` |
| Количество одновременных сессий для привилегированных учетных записей:<br>`config.privilegedSessionsLimit` | не более 2-х<br>`privilegedSessionsLimit: 2` |
| Время бездействия (неактивности) пользователя, через которое осуществляется завершение сеанса пользователя:<br>`config.session.rememberFor` | не более 5 минут<br>`rememberFor: 5m` |
| Конфигурационные файлы ПМ и ПУ (сценариев установки ПМ и ПУ):<br>`/var/ocs/appstore/config.yml`<br>`(config/subsystems/appstore/config/services/config.yml.j2)`<br>`/var/ocs/emm/config.yml`<br>`(config/subsystems/emm/config/services/config.yml.j2)` | |
| Время бездействия (неактивности) пользователя, через которое осуществляется завершение сеанса пользователя:<br>`config.session.rememberFor` | не более 5 минут<br>`rememberFor: 5m` |

Более подробное описание параметров конфигурационных файлов `config.yml` и `config.yml.j2` приведено в пунктах 8.3.2, 8.3.3 и 8.3.4 настоящего документа.

### 2.8.7. Действия по реализации функций безопасности среды функционирования ППО

#### 2.8.7.1. Установка, настройка и эксплуатация СЗИ НСД

Эксплуатация ППО и СУБД должна осуществляться в одной из следующих ОС:

– CentOS версии 7 с установленными СЗИ НСД «Dallas Lock Linux», или СЗИ «Secret Net LSP», или СЗИ НСД «Аккорд-Х К»;

– CentOS версии 8 или выше;

– Альт 8 СП.

Установка СЗИ НСД должна осуществляться после установки ППО. После установки СЗИ НСД необходимо повторно назначить пользователям ОС права на выполнение команд от имени суперпользователя root в соответствии с подразделом 2.2 настоящего документа.

Установка, настройка и эксплуатация СЗИ НСД и ОС Альт 8 СП должна осуществляться в соответствии с эксплуатационной документацией на СЗИ (ОС).

#### 2.8.7.2. Меры по межсетевому экранированию

В ИС должна осуществляться защита периметра (физических и (или) логических границ) ИС с использованием межсетевого экрана требуемого класса защиты.

Межсетевой экран должен пропускать трафик только на внешние порты ППО, остальной трафик должен быть запрещен. Перечень внешних портов ППО в зависимости от варианта настройки приведен в таблице (Таблица 10).

Таблица 10

| Номер порта (протокол) | Описание | Конфигурационный файл, в котором задается порт | Тип порта[1] |
|---|---|---|---|
| Сервисы ППО «Аврора Центр» | | | |
| 10000 - 10500 (tcp) | Порты сервисов ППО | `shared_roles/systemd-deploy/templates/systemd-supplicant.sh.j2 /usr/bin/systemd-supplicant.sh` | внутренний |
| Nginx | | | |
| 80 (tcp) | Служит для взаимодействия сервисов ППО друг с другом и используется в том случае, когда осуществляется разделение трафика по basepath (url-адресам) | `shared_roles/consul-template/defaults/main.yml` | внутренний |
| 8009 (tcp) | Балансировщик микросервисов (Nginx Web Server). Используется в том случае, когда осуществляется разделение трафика по basepath (url-адресам) | `shared_roles/consul-template/templates/ocs.conf.ctmpl.j2 /etc/consul-template/templates/ocs.conf.ctmpl` | внешний |
| 8011 (tcp) | `AMM admin API gateway` (Консоль администратора ПУ) | `config/subsystems/emm/vars/services.yml` | внешний или внутренний |

[1] Типы портов:

1. Внешние - доступ к данному типу портов осуществляется из-за пределов контролируемой зоны. Например, запросы от пользователей с ролью Пользователь Аврора Маркет. Доступ к данным портам имеет нарушитель;
2. Внутренние - доступ к данному типу портов может осуществляться только из контролируемой зоны. Данные порты используются для взаимодействия: между сервисами ППО, сервисов ППО с компонентами среды функционирования ППО, компонентами среды функционирования ППО, привилегированных пользователей с ППО.

| Номер порта (протокол) | Описание | Конфигурационный файл, в котором задается порт | Тип порта[1] |
|---|---|---|---|
| 8012 (tcp) | `AMM device API gateway` (API для взаимодействия с МП «Аврора Центр») | `config/subsystems/emm/vars/services.yml` | внешний |
| 8014 (tcp) | `Aurora market development API gateway` (Консоль разработчика ПМ) | `config/subsystems/appstore/vars/services.yml` | внешний |
| 8015 (tcp) | `Aurora market admin API gateway` (Консоль администратора ПМ) | `config/subsystems/appstore/vars/services.yml` | внешний или внутренний |
| 8016 (tcp) | `Aurora market client API gateway` (API для взаимодействия с МП «Аврора Маркет») | `config/subsystems/appstore/vars/services.yml` | внешний |
| 8018 (tcp) | `Auth public API gateway` (интерфейс ППО для идентификации и аутентификации пользователей) | `config/subsystems/auth/vars/services.yml` | внешний |
| 8019 (tcp) | `Auth admin API gateway` (Консоль администратора ПБ) | `config/subsystems/auth/vars/services.yml` | внутренний |
| 8022 (tcp) | `Package repository admin API gateway` (API для взаимодействия с ПООС, только для взаимодействия ПУ с ПООС) | `config/subsystems/pkgrepo/vars/services.yml` | внутренний |
| 8023 (tcp) | `Package repository device API` (API для взаимодействия МП «Аврора Центр» с ПООС) | `config/subsystems/pkgrepo/vars/services.yml` | внутренний |

| Номер порта (протокол) | Описание | Конфигурационный файл, в котором задается порт | Тип порта[1] |
|---|---|---|---|
| 8030 (tcp) | Файловый сервер ПООС | config/subsystems/pkgrepo/vars/ocs-pkgrepo-nginx-static.yml | внешний |
| СУБД PostgreSQL | | | |
| 5432 (tcp) | СУБД PostgreSQL | shared_roles/postgresql/defaults/main.yml | внутренний |
| СУБД Redis | | | |
| 6379 (tcp) | redis-server | shared_roles/redis/defaults/main.yml | внутренний |
| 26379 (tcp) | redis-sentinel | shared_roles/redis/defaults/main.yml | внутренний |
| Consul | | | |
| 8300 (tcp) | https://www.consul.io/docs/install/ports | | внутреннее |
| 8301 (tcp/udp) | https://www.consul.io/docs/install/ports | | внутренний |
| 8302 (tcp/udp) | https://www.consul.io/docs/install/ports | | внутренний |
| 8600 (tcp/udp) | https://www.consul.io/docs/install/ports | shared_roles/consul/defaults/main.yml | внутренний |
| 8500 (tcp) | https://www.consul.io/docs/install/ports | shared_roles/consul/defaults/main.yml | внутренний |
| Nats Streaming Server | | | |
| 4222 (tcp) | nats_port | shared_roles/nats-streaming-server/defaults/main.yml | внутренний |
| 6222 (tcp) | nats_cluster_port | shared_roles/nats-streaming-server/defaults/main.yml | внутренний |
| 8222 (tcp) | nats_monitoring_port | shared_roles/nats-streaming-server/defaults/main.yml | внутренний |
| Dnsmasq | | | |
| 53 | dnsmasq | | внутренний |
| Операционная система | | | |
| 22 | Порт SSH. Используется для развертывания и | | внутренний |

| Номер порта (протокол) | Описание | Конфигурационный файл, в котором задается порт | Тип порта[1] |
|---|---|---|---|
| | администрирования ППО.<br>**Внимание!** Возможность использования данного порта определяется документацией СЗИ от НСД | | |

Рекомендуется запретить доступ к ППО привилегированных пользователей из-за пределов контролируемой зоны, запретив доступ к Консоли администратора ПБ. Также при необходимости можно запретить доступ к остальным веб-консолям. Для этого, в зависимости от варианта настройки ППО, необходимо разрешить трафик только на требуемых портах, либо только по требуемым url-адресам в соответствии с таблицей (Таблица 8)

#### 2.8.7.3. Настройка ОС

В целях затруднения возможностей сбора информации о системе, необходимо исключить метки времени из заголовков TCP пакетов. Для этого необходимо выполнить следующие действия:

2.9.7.3.1. В конфигурационный файл `/etc/sysctl.conf` добавить строку:

```
net.ipv4.tcp_timestamps = 0
```

2.9.7.3.2. Применить конфигурацию, выполнив команду:

```
sysctl -p /etc/sysctl.conf
```

2.9.7.3.3. Проверить корректность конфигурации, выполнив команду:

```
sysctl -a | grep net.ipv4.tcp_timestamps
```

Если настройки сделаны правильно, то должно быть выведено значение:

```
net.ipv4.tcp_timestamps = 0
```

### 2.8.8. Самостоятельная установка необходимых пакетов на серверы приложений и серверы БД

Для установки необходимых пакетов на серверы приложений и серверы БД необходимо выполнить действия, описанные далее.

2.8.8.1. Получить список необходимых пакетов

Перечень необходимых пакетов, которые должны быть установлены на серверы приложений и серверы БД задан в файле `play-managed-node-prerequisites.yml`, находящемся в каталоге со сценариями установки ППО. Данный файл имеет следующую структуру:

```
...
    - name: install requirements to <операционная система>
...
        - name: install os packages on db node
          loop:
            <перечень пакетов сервера БД>
        - name: install os packages on app node
          loop:
            <перечень пакетов сервера приложений>
```

В секции `name: install requirements to <операционная система>` задается перечень пакетов для указанной ОС. Данная секция содержит две подсекции, в которых задается перечень пакетов для сервера приложений и сервера БД.

В подсекции `name: install os packages on db node` задается перечень пакетов для сервера БД.

В подсекции `name: install os packages on app node` задается перечень пакетов для сервера приложений.

Пример перечня пакетов для сервера приложений и сервера БД, функционирующих под управлением ОС CentOS 7:

```
...
  tasks:
    - name: install requirements to CentOS7
      block:
        - debug:
            msg: install requirements to CentOS7

        - name: install os packages on db node
          package:
            name: "{{ item }}"
            state: present
          loop:
            - epel-release
            - jq
```

```
            - unzip
            - perl-libs
            - libxslt
            - postgresql-libs
            - libicu
            - python-psycopg2
          when: node_type == "db" or node_type == "all"

        - name: install os packages on app node
          package:
            name: "{{ item }}"
            state: present
          loop:
            - net-tools
            - epel-release
            - jq
            - unzip
            - perl-libs
            - libxslt
            - postgresql-libs
            - libicu
            - dnsmasq
            - bind-utils
          when: node_type == "app" or node_type == "all"
      when: ansible_distribution == "CentOS" and
ansible_distribution_major_version == "7"
```

2.8.8.2. Установить пакеты

Установка пакетов осуществляется в соответствии с документацией на ОС.

### 2.8.9. Требования к установке и настройке внешнего балансировщика Nginx

Установки и настройка внешнего балансировщика Nginx осуществляется пользователями (системными администраторами) ППО самостоятельно. При этом внешний балансировщик должен поддерживать проксирование tcp-соединений. Для этого необходимо:

– в конфигурационном файле Nginx (файл: `/etc/nginx/nginx.conf`) добавить строку:

```
load_module '/usr/lib64/nginx/modules/ngx_stream_module.so';
```

– перезапустить Nginx с помощью команды:

```
sudo systemctl reload nginx
```

### 2.8.10. Активация (разблокировка) учетной записи пользователя с помощью sql-запроса к БД

Разблокировка учетных записей пользователей ППО осуществляется Администратором учетных записей с помощью Консоли администратора ПБ. Однако учетная запись Администратора учетных записей тоже может быть заблокирована (например, если Администратора учетных длительное время был не активен).

В этом случае, для разблокировки учетной записи, необходимо выполнить следующие действия:

2.8.10.1. Подключится к БД ПБ (auth) с помощью следующих команд:

```
psql -U auth -h <ip-адрес сервера БД> -d auth
\c auth
```

Например,

```
psql -U auth -h 192.168.0.107 -d auth
\c auth
```

2.8.10.2. Разблокировать учетную запись пользователя с помощью с sql-запроса:

```
update accounts_users.accounts set is_active=true where login='<email
пользователя>';
```

Например,

```
update accounts_users.accounts set is_active=true where
login='admin@omprussia.ru';
```

### 2.8.11. Действия после сброса МУ к заводским настройкам

Сброс МУ очищает его до заводских настроек. После сброса МУ, в зависимости от того, каким образом были первоначально установлены МП ППО (МП «Аврора Центр» и МП «Аврора Маркет»), могут либо отсутствовать, либо сброшены до первоначальной версии.

После сброса МУ необходимо выполнить следующие действия:

1) установить МП ППО, если после сброса МУ они отсутствуют;

2) активировать МУ в ПУ в соответствии с документом «Руководство пользователя. Часть 3. Подсистема Платформа управления»;

3) обновить МП ППО в соответствии с подразделом 5.2 настоящего документа.

## 2.9. Описание настройки подсистем ППО

### 2.9.1. Описание настройки ПМ

Настройка ПМ заключается в настройке файлового хранилища ПМ.

Настройку файлового хранилища необходимо выполнять после установки ППО

Для настройки файлового хранилища ПМ необходимо выполнить следующие действия:

– на Сервере приложений ПМ создать каталог, в котором будут храниться файлы МП (иконки, скриншоты, rpm-пакеты), загружаемые разработчиками, либо каталог, к которому будет монтироваться единое файловое хранилище;

– в случае если файлы МП будут храниться в каталоге на Сервере приложений ПМ, необходимо создать каталог в соответствии с параметром `filestorage_path` конфигурационного файла `config/vars/_vars.yml`, в созданном каталоге создать каталог `applications-api` и сделать владельцем данного каталога пользователя ocs, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs/appstore/applications-api
sudo chown ocs:ocs /ocs/appstore/applications-api
```

Параметр `filestorage_path` конфигурационного файла `config/vars/_vars.yml` может иметь следующий вид:

```
filestorage_path: "/ocs/appstore"
```

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

– при использовании единого файлового хранилища для хранения файлов МП на Сервере приложений ПМ необходимо создать каталог `/ocs` и сделать владельцем данного каталога пользователя ocs, под которым работают сервисы ПМ:

```
sudo mkdir -p /ocs
sudo chown ocs:ocs /ocs
```

**ВНИМАНИЕ!** При эксплуатации ППО в кластерной конфигурации все ноды Сервера приложений ПМ должны иметь доступ к единому файловому хранилищу. Соответственно все ноды Сервера приложений ПМ должны быть настроены на работу с данным файловым хранилищем.

Пример настройки единого файлового хранилища и работы Сервера приложений ПМ (ноды Сервера приложений ПМ) приведены в п. 2.8.4 настоящего документа.

### 2.9.2. Описание настройки ПУ

#### 2.9.2.1. Настройка подключения ПУ к серверу LDAP

Для настройки взаимодействия ППО с сервером LDAP необходимо в секции `ldap_server` конфигурационного файла `config/vars/_vars.yml` задать требуемые значения:

– `address` — адрес расположения сервера LDAP;

– `parent_group` — группа, с которой будет производиться экспорт данных из сервера LDAP;

– `user_cn` — логин технической учетной записи сервера LDAP;

– `password` — пароль от технической учетной записи сервера LDAP;

– `page_size` — количество элементов, которое будет импортировано за одну итерацию.

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

Пример настройки подключения к серверу LDAP в `_vars.yml`:

```
ldap_server:
  address:  "ldap://dc01.omptest.test"
  parent_group: "ou=Test,DC=omptest,DC=local"
  user_cn: "OMPTEST\\\\Admin"
  password: "&UJM,ki8"
  page_size: 1000
```

Описание требований к данным, содержащимся в Active Directory, приведено в таблице (Таблица 11).

**ВНИМАНИЕ!** Параметры E-mail, First_name, Last_name являются обязательными.

Таблица 11

| Параметр | Описание | Примечание |
|---|---|---|
| Group | Название группы пользователей. Формат: от 3 до 64 символов | Если группа пользователей МУ уже существует, то выполняется привязка группы к пользователям МУ |
| E-mail (обязательный) | Рабочая почта пользователя МУ. Формат: <логин>@<доменное_имя>, от 2 до 256 символов | Рабочая почта пользователя МУ должна быть уникальной |
| First_name (обязательный) | Имя пользователя МУ. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел | |
| Last_name (обязательный) | Фамилия. Формат: от 2 до 64 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел | |
| Job_title | Должность. Формат: от 2 до 256 символов. Символы: а-я; a-z; А-Я; A-Z; -; пробел | |
| Phone_number | Номер телефона. Формат: от 2 до 64 символов. Только цифры | |

#### 2.9.2.2. Настройка взаимодействия Сервера приложений ПУ с Сервисом уведомлений Аврора версии 1.0.0

2.9.2.2.1. Синхронизировать время между Сервером приложений ПУ и Сервисом уведомлений Аврора (СУА)

2.9.2.2.2. Зарегистрировать в СУА проект и получить следующие настройки:

– `ID проекта` - идентификатор проекта, используемый при формировании URL;

– `адрес Push-сервера`;

– clientId. Аккаунт учетной записи в подсистеме безопасности Push-сервиса (в большинстве случаев совпадает с ID проекта);

– scope и audience. Параметры, определяющие список запрашиваемых разрешений к ресурсам;

– privateKey и privateKeyId. Связка ключей для использования в запросе по получению токена.

– ID приложения.

2.9.2.2.3. В конфигурационном файле config/vars/_vars.yml задать значения следующих параметров:

– push_public_address - публичный адрес СУА (значение параметра должно соответствовать значению параметра push_public_address в конфигурационном файле push-server.yml);

– push_mobile_hostname - имя хоста СУА, к которому будет подключаться Push-демон;

– push_mobile_port - номер порта СУА, к которому будет подключаться Push-демон.

Например:

```
push_public_address: "http://ocs-app.local:8009"
push_mobile_hostname: 192.168.0.115
push_mobile_port: 999
```

Описание параметров конфигурационного файла config/vars/_vars.yml приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

2.9.2.2.4. Включить в ПУ возможность отпарвлять Push-уведомления

Для этого в секции push_notification_system конфигурационного файла config/subsystems/emm/vars/_vars.yml необходимо задать для параметра enabled значение true:

```
push_notification_system:
  enabled: true
```

Описание параметров конфигурационного файла `config/subsystems/emm/vars/_vars.yml` приведено в п. 8.3.4 настоящего документа.

2.9.2.2.5. Задать настройки взаимодействия с Push-сервером

Для этого в секции `push_notification_system` конфигурационного файла `config/subsystems/emm/vars/_vars.yml` необходимо задать значения для следующих параметров:

- `project_id` - ID проекта;
- `client_id` - clientId;
- `application_id` - ID приложения;
- `scopes` (значения должны быть указаны через пробел);
- `audience` (значения должны быть указаны через пробел);
- `key_id` - privateKeyId;
- `private_key` - privateKey;
- `token_url` - url-адрес функции (endpoint-а) для получения токена авторизации.

**ВНИМАНИЕ!** Значения параметров должны быть заданы в двойных кавычках.

Для того, чтобы задать `privat_key` необходимо:

- через пробел после параметра `private_key` поставить символ «|»;
- на новой строке задать значение закрытого ключа, соблюдая указанные в примере отступы:

```
private_key: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCjorNYuLCQK5X/
    . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
    pVDY99MLH8DJiElTOMwzkuhivn2tmm45A93+FZO9GlFHW9P0k4GbUQk1h2Mn4YfB
    RcuVd606gAQh+bbIrqDzeeZ51yY+FA==
    -----END RSA PRIVATE KEY-----
```

Для получения значения `token_url` необходимо в адресной строке веб-браузера выполнить запрос `<url-адрес push-сервера>/api/v1/.well-known`, в полученном ответе найти строку содержащую «`/oauth2/token`» и задать данную

строку в параметре token_url, например:

```
token_url: "http://push.omp.ru/auth/public/oauth2/token"
```

Пример секции push_notification_system конфигурационного файла config/subsystems/emm/vars/_vars.yml:

```
  push_notification_system:
  project_id: "emm_bug1mrej27oa0eryt5s0"
  push_public_address: "https://push.omp.ru"
  api_url: "https://push.omp.ru/push/public/api/v1/"
  client_id: "emm_bug1mrej27oa0eryt5s0"
  scopes: "openid offline message:update"
  audience: "ocs-auth-public-api-gw ocs-push-public-api-gw"
  token_url: "https://push.omp.ru/auth/public/oauth2/token"
  key_id: "public:7N2vJSOV5q"
  private_key: |
    -----BEGIN RSA PRIVATE KEY-----
    MIIJQgIBADANBgkqhkiG9w0BAQEFAASCCSwwggkoAgEAAoICAQCjorNYuLCQK5X/
    . . . . . .
    pVDY99MLH8DJiElTOMwzkuhivn2tmm45A93+FZO9GlFHW9P0k4GbUQk1h2Mn4YfB
    RcuVd606gAQh+bbIrqDzeeZ51yY+FA==
    -----END RSA PRIVATE KEY-----
```

Описание параметров конфигурационного файла config/subsystems/emm/vars/_vars.yml приведено в п. 8.3.4 настоящего документа.

2.9.2.2.6. Переустановить ПУ в соответствии с пунктом 2.5.2 астоящего документа.

### 2.9.2.3. Настройка взаимодействия Сервера приложений ПУ с Сервисом уведомлений Аврора версии 1.1.0

При необходимости взаимодействия Сервера приложений ПУ с СУА необходимо выполнить следующие настройки:

2.9.2.3.1. Синхронизировать время между Сервером приложений ПУ и СУА

2.9.2.3.2. Зарегистрировать в СУА проект и получить конфигурационные файлы с настройками: push-mobile-app.yml и push-server.yml

2.9.2.3.3. Скопировать полученные конфигурационные файлы в каталог config/subsystems/emm/vars/ сценариев установки ППО

2.9.2.3.4. В конфигурационном файле config/vars/_vars.yml задать значения следующих параметров:

– push_public_address - публичный адрес СУА (значение параметра должно соответствовать значению параметра push_public_address в конфигурационном файле push-server.yml);

– push_mobile_hostname - имя хоста СУА, к которому будет подключаться Push-демон;

– push_mobile_port - номер порта СУА, к которому будет подключаться Push-демон.

Например:

```
push_public_address: "http://ocs-app.local:8009"
push_mobile_hostname: 192.168.0.115
push_mobile_port: 999
```

Описание параметров конфигурационного файла config/vars/_vars.yml приведено п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

2.9.2.3.5. Включить в ПУ возможность отпарвлять Push-уведомления

Для этого в секции push_notification_system конфигурационного файла config/subsystems/emm/vars/_vars.yml необходимо задать для параметра enabled значение true:

```
push_notification_system:
  enabled: true
```

Описание параметров конфигурационного файла config/subsystems/emm/vars/_vars.yml приведено в п. 8.3.4 настоящего документа.

2.9.2.3.6. Переустановить ПУ в соответствии с пунктом 2.5.2 настоящего документа.

### 2.9.3. Описание настройки ПООС

Для загрузки пакетов ОС в файловое хранилище ПООС необходимо выполнить следующие действия:

1) скопировать в произвольный каталог файлового хранилища ПООС архив с пакетами ОС и распаковать его в каталог, заданный в параметре `root` секции `location /pkgrepo/mobile` конфигурационного файла `/etc/nginx/conf.d/locations-external/ocs-pkgrepo-nginx-static.location` (по умолчанию каталог: `/ocs/pkgrepo/repos`), либо в параметре `repos_root` конфигурационного файла `install-<версия ППО>/install-ac/config/subsystems/pkgrepo/vars/ocs-pkgrepo-nginx-static.yml` сценариев установки ППО:

```
tar -xf <имя файла с архивом> -C /ocs/pkgrepo/repos
rm <имя файла с архивом>
```

2) зарегистрировать переданный релиз (версию), добавив в файл `/ocs/pkgrepo/meta/main.json` описание из переданного вместе с архивом meta-файла. Путь к файлу `main.json` задается в параметре `alias` секции `location /pkgrepo/mobile/meta` конфигурационного файла `/etc/nginx/conf.d/locations-external/ocs-pkgrepo-nginx-static.location` (по умолчанию каталог: `/ocs/pkgrepo/meta`), либо в параметре `meta_root` конфигурационного файла `install-<версия ППО>/install-ac/config/subsystems/pkgrepo/vars/ocs-pkgrepo-nginx-static.yml` сценариев установки ППО. Пример файла `main.json`:

```
{
  "brand": "OMPCert",
  "releases": [
    {
      "deviceModel": "p4903",
      "latest": "3.0.2.23",
      "versions": [
        {
          "version": "3.0.2.22",
      "from": []
        },
        {
          "version": "3.0.2.23",
          "from": [
              "3.0.2.22"
      ]
    }
      ]
    },
    {
      "deviceModel": "l801em",
      "latest": "3.0.2.23",
```

```
      "versions": [
        {
          "version": "3.0.2.22",
      "from": []
        },
        {
          "version": "3.0.2.23",
          "from": [
              "3.0.2.22"
      ]
    }
      ]
    }
  ]
}
```

3) перезапустить сервис `ocs-pkgrepo-pkg-repo-api` с помощью команды:

```
sudo systemctl restart ocs-pkgrepo-pkg-repo-api*
```

4) для проверки корректности настройки необходимо войти в Консоль администратора ПУ, далее перейти в «Администрирование - Настройки - Интеграция - Обновление ОС» и убедиться, что отображаются имя сервера, модели устройств и доступные версии ОС (Рисунок 3).

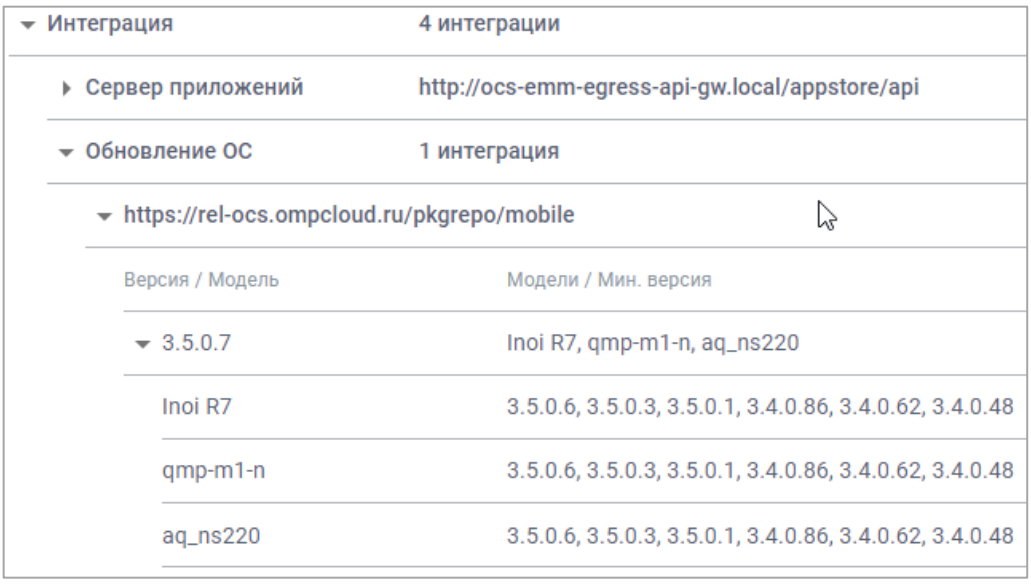



Рисунок 3

## 2.10. Установка МП

**ВНИМАНИЕ!** Для не сертифицированной (корпоративной) версии ОС Аврора, МП «Аврора Маркет» и МП «Аврора Центр» поставляются вместе ОС (входят в состав ОС).

### 2.10.1. Установка МП на МУ с помощью приложения «Терминал»

Для установки МП на МУ с помощью приложения «Терминал» необходимо выполнить следующие действия:

1) подключить МУ к ПЭВМ с помощью USB-кабеля;

2) на МУ переключиться в режим «Протокол передачи мультимедиа (MTP)», в результате в ОС отобразится внешний носитель «INOI R7» (Рисунок 4);

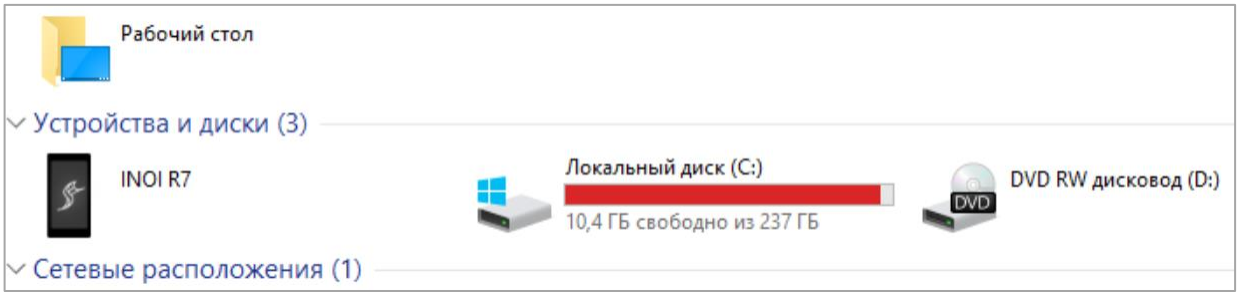



Рисунок 4

3) перейти в каталог Downloads и скопировать в него загрузочный модуль МП (RPM-пакеты);

Загрузочный модуль в зависимости от версии ОС, находится на DVD с загрузочным модулем в каталоге:

- МП «Аврора Центр»:
  - `/mobile_apps/aurora_center/3.2.2/` (для ОС Аврора версии 3.2.2);
  - `/mobile_apps/aurora_center/3.4.0/` (для ОС Аврора версии 3.4.0);
- МП «Аврора Маркет»:
  - `/mobile_apps/aurora_market/3.2.2/` (для ОС Аврора версии 3.2.2);
  - `/mobile_apps/aurora_market/3.4.0/` (для ОС Аврора версии 3.4.0);

4) используя МП МУ «Терминал», перейти в каталог с RPM-пакетами, с помощью команды:

```
cd /home/nemo/Downloads/
```

Предварительно необходимо задать пароль для приложения «Терминал». Для этого необходимо выполнить следующие действия:

– провести по экрану снизу вверх на экране приложений и коснуться значка  . Отобразится меню настроек;

– в меню настроек перейти к разделу «Настройка защиты»;

– выбрать пункт «Доступ к терминалу» и сгенерировать пароль (либо задать пароль вручную);

5) установить пакеты, с помощью команды:

```
devel-su pkcon install-local *.rpm
```

### 2.10.2. Установка МП на МУ с помощью ПУ

Установка МП «Аврора Маркет» также может осуществляться с помощью ПУ, подробное описание приведено в документе «Руководство пользователя. Часть 3. Подсистема Платформа управления».

## 2.11. Проверка корректности установки и функционирования ППО

### 2.11.1. Общие сведения

Для проверки корректности установки и функционирования ППО, а также среды функционирования ППО в состав сценариев установки включена утилита для формирования диагностического отчета.

Для формирования диагностического отчета необходимо перейти в каталог со сценариями установки (каталог: `install-<версия ППО>/install-ac/`) и выполнить команду:

```
ansible-playbook play-diagnostic-report.yml -i inventories/hosts.yml -
vv --user <имя пользователя>
```

В результате выполнения команды в каталоге report будет сформирован файл в report.html.

Диагностический отчет формируется в виде файла в формате HTML и содержит следующие разделы:

– общая информация о статусе сервисов ППО;

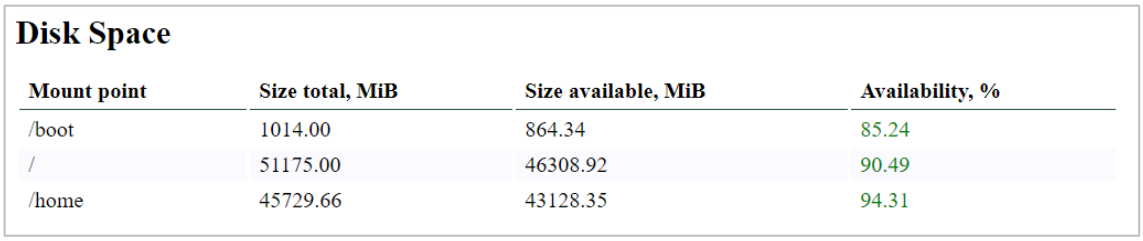
– общая информация о статусе компонентов среды функционирования;

– разделы, содержащие детальную информацию об отдельных сервисах ППО и компонентах среды функционирования.

### 2.11.2. Описание параметров диагностического отчета

#### 2.11.2.1. Раздел «Disk Space»

Информация о полном и доступном объеме дискового пространства для ППО приведена на рисунке (Рисунок 5).



**Disk Space**

| Mount point | Size total, MiB | Size available, MiB | Availability, % |
|---|---|---|---|
| /boot | 1014.00 | 864.34 | 85.24 |
| / | 51175.00 | 46308.92 | 90.49 |
| /home | 45729.66 | 43128.35 | 94.31 |

Рисунок 5

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 12).

Таблица 12

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Mount points | Каталог, к которому монтируется файловое хранилище (точка монтирования) | Путь к каталогу, например: `/home`. |
| Size total, MiB | Размер файлового хранилища, примонтированного к заданному каталогу | Объем физической памяти в Мб, например: 45729,66 |
| Size available, MiB | Объем свободного места в файловом хранилище, примонтированного к заданному каталогу | Объем физической памяти в Мб, например: 43128,35 |
| Availability, % | Объем свободного места в файловом хранилище в процентном соотношении (к полному объему) | От 0 до 100, например: 94.31 |

В случае если объем свободного места в менее 15%, то поле закрашивается красным цветом

#### 2.11.2.2. Раздел «Systemd Unit Status»

В данном разделе приведена общая информация о статусе сервисов ППО и компонентов среды функционирования и состоит из следующих подразделов:

##### 2.11.2.2.1 OCS Targets

Информация об автозапуске сервисов ППО (наличии конфигурационных файлов запуска групп сервисов `*.target` в автозапуске) приведена на рисунке (Рисунок 6).

**Systemd Unit Status**

| Service name | Status |
|---|---|
| **OCS Targets** | |
| ocs-appstore-admin-api-gw.target | enabled |
| ocs-appstore-adminconsole-ui.target | enabled |
| ocs-appstore-applications-api.target | enabled |
| ocs-appstore-client-api-gw.target | enabled |
| ocs-appstore-dev-api-gw.target | enabled |
| ocs-appstore-devconsole-ui.target | enabled |
| ocs-appstore-egress-api-gw.target | enabled |
| ocs-appstore-settings-api.target | enabled |
| ocs-appstore.target | enabled |

Рисунок 6

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 13).

Таблица 13

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Service name | Имя конфигурационного файла запуска группы сервисов | Возможные значения определяются перечнем сервисов ППО и имеют следующий формат `<имя группы сервисов>.target`, например: `ocs-appstore-admin-api-gw.target`. |
| Status | Информация о присутствии конфигурационного файла запуска группы сервисов в автозапуске | `enabled` - присутствует в автозапуске<br>`disabled` - отсутствует в автозапуске |

#### 2.11.2.2.2 OCS Services

Информация о статусе сервисов ППО приведена на рисунке (Рисунок 7).

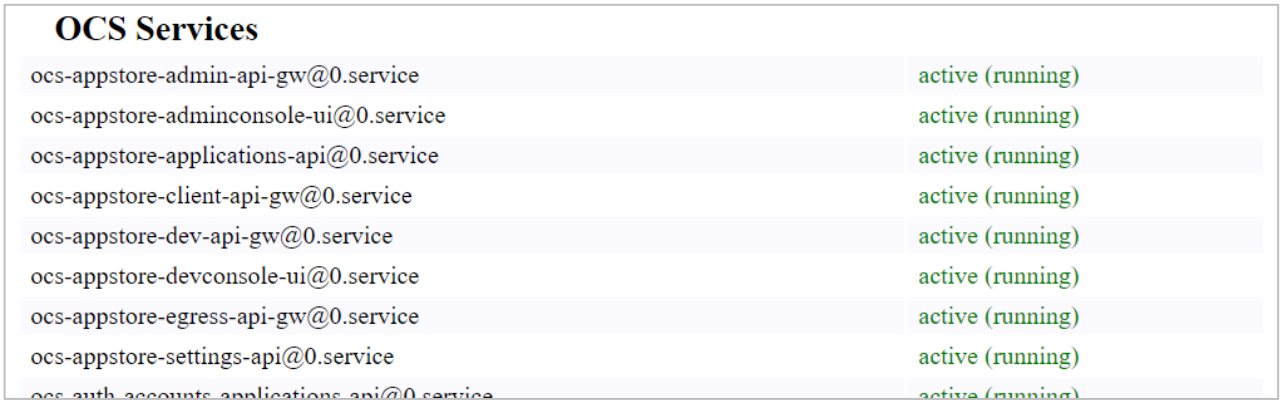



Рисунок 7

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 14).

Таблица 14

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Service name | Название сервиса ППО | Возможные значения определяются перечнем сервисов ППО и имеют следующий формат `<имя группы сервисов>@<номер экземпляра сервиса в группе>.service`, например: `ocs-appstore-admin-api-gw@0.service`. |
| Status | Информация о статусе сервиса | `active (running)` - сервис запущен и выполняется;<br>`activating` - сервис запускается;<br>`deactivating` - сервис выключается;<br>`inactive` – сервис выключен;<br>`failed` - при запуске сервиса произошла ошибка |

#### 2.11.2.2.3 Mandatory services

Информация о статусе сервисов – компонентов среды функционирования приведена на рисунке (Рисунок 8).

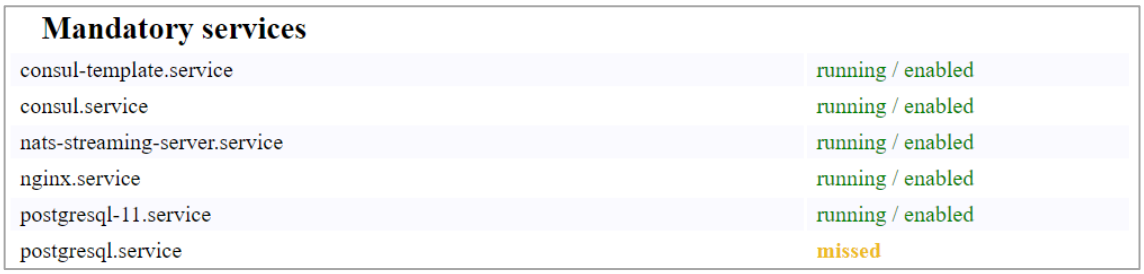



Рисунок 8

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 15).

Таблица 15

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Service name | Название сервиса компонента среды функционирования | Возможные значения имеют следующий формат `<имя сервиса>.service` и определяются Разарботчиком. Перечень возможных значений:<br>`consul-template.service`<br>`consul.service`<br>`nats-streaming-serever.service`<br>`nginx.service`<br>`postgresql-11.service`<br>`postgresql.service` |
| Status | Информация о статусе сервиса | `active (running)` - сервис запущен и выполняется;<br>`activating` - сервис запускается;<br>`deactivating` - сервис выключается;<br>`inactive` - сервис выключен;<br>`failed` – при запуске сервиса произошла ошибка;<br>`enabled` - сервис присутствует в автозапуске;<br>`disabled` - сервис отсутствует в автозапуске;<br>`missed` - компонент отсутствует |

### 2.11.2.3. Раздел «OIDC Clients»

Информация об OIDC-клиентах приведена на рисунке (Рисунок 9).

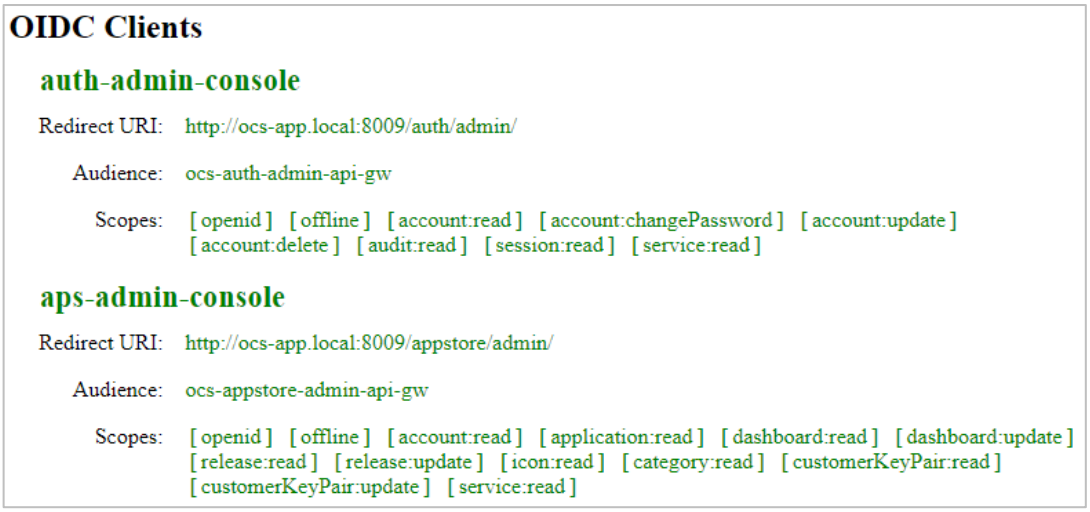



Рисунок 9

По каждому OIDC-клиенту приведена следующая информация:

– идентификатор OIDC-клиента (например, `emm-admin-console`);

– в поле «Scope» приведен перечень действий (прав) доступных OIDC-клиенту;

– в поле «Return/redirect URI» находится список URI для автоматического перехода для авторизованного и неавторизованного пользователя;

– в поле «Audience» указано название шлюза доступа, который и является OIDC-клиентом.

#### 2.11.2.4. Раздел «Consul Services Registration»

На рисунке (Рисунок 10) отображается пример статуса регистрации сервисов в системе обнаружения сервисов (Consul).

**Consul Services Registration**

| Service name | Code | Status |
|---|---|---|
| ocs-appstore-admin-api-gw | 200 | passing |
| ocs-appstore-client-api-gw | 200 | passing |
| ocs-appstore-dev-api-gw | 200 | passing |
| ocs-auth-admin-api-gw | 200 | passing |
| ocs-auth-public-api-gw | 200 | passing |
| ocs-emm-admin-api-gw | 200 | passing |
| ocs-emm-device-api-gw | 200 | passing |
| ocs-pkgrepo-admin-api-gw | 200 | passing |
| ocs-pkgrepo-device-api-gw | 200 | passing |

Рисунок 10

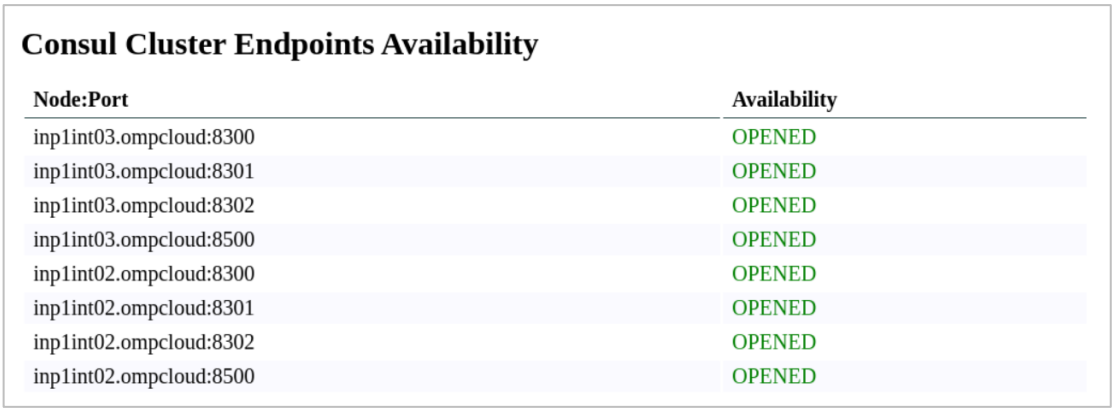
Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 16).

Таблица 16

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Service name | Название сервиса ППО | Возможные значения определяются перечнем сервисов ППО |
| Code | Код http-ответа | Возможные значения определяются протоколом HTTP |
| Status | Информация о статусе регистрации сервиса в системе обнаружения сервисов (Consul) | Возможные значения определяются Consul. Статус «passing» означает, что проверка пройдена успешно |

#### 2.11.2.5. Раздел «Consul Cluster Endpoints Availability»

Проверка доступности интерфейсных функций системы обнаружения сервисов (Consul) представлена на рисунке (Рисунок 11).



**Consul Cluster Endpoints Availability**

| Node:Port | Availability |
|---|---|
| inp1int03.ompcloud:8300 | OPENED |
| inp1int03.ompcloud:8301 | OPENED |
| inp1int03.ompcloud:8302 | OPENED |
| inp1int03.ompcloud:8500 | OPENED |
| inp1int02.ompcloud:8300 | OPENED |
| inp1int02.ompcloud:8301 | OPENED |
| inp1int02.ompcloud:8302 | OPENED |
| inp1int02.ompcloud:8500 | OPENED |

Рисунок 11

Перечень интерфейсных функций Consul приведен в документации на Consul (`https://www.consul.io/docs/install/ports`). Информация по доступности интерфейсных функций Consul предоставляется только в случае кластерной (многонодовой) конфигурации.

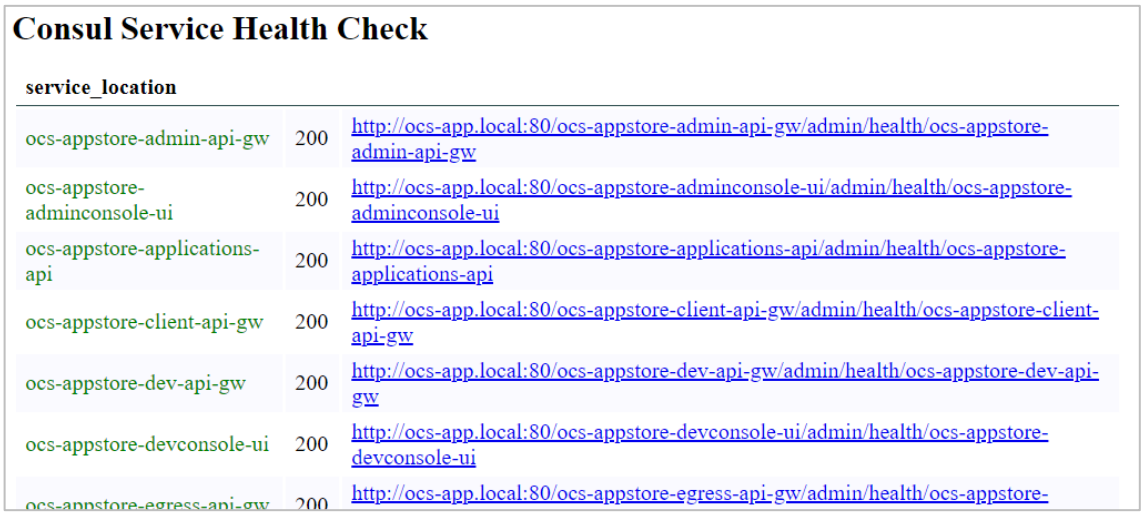
Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 17).

Таблица 17

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Node:Port | Адрес функции | Адрес функции представлен в следующем формате: `<имя хоста>:<порт>`.<br>Проверка выполняется только для функций доступных на следующих портах: 8300, 8301, 8302, 8500.<br>Например: `inp1int03.ompcloud:8300` |
| Availability | Статус доступности функции | В случае доступности функции принимает значение «OPENED».<br>В ином случае выводится код ошибки и сообщение, определяемое Consul |

### 2.11.2.6. Раздел «Consul Service Health Check»

Статус регистрации сервисов ППО в системе обнаружения сервисов Consul представлен на рисунке (Рисунок 12).



**Consul Service Health Check**

| service_location | | |
|---|---|---|
| ocs-appstore-admin-api-gw | 200 | http://ocs-app.local:80/ocs-appstore-admin-api-gw/admin/health/ocs-appstore-admin-api-gw |
| ocs-appstore-adminconsole-ui | 200 | http://ocs-app.local:80/ocs-appstore-adminconsole-ui/admin/health/ocs-appstore-adminconsole-ui |
| ocs-appstore-applications-api | 200 | http://ocs-app.local:80/ocs-appstore-applications-api/admin/health/ocs-appstore-applications-api |
| ocs-appstore-client-api-gw | 200 | http://ocs-app.local:80/ocs-appstore-client-api-gw/admin/health/ocs-appstore-client-api-gw |
| ocs-appstore-dev-api-gw | 200 | http://ocs-app.local:80/ocs-appstore-dev-api-gw/admin/health/ocs-appstore-dev-api-gw |
| ocs-appstore-devconsole-ui | 200 | http://ocs-app.local:80/ocs-appstore-devconsole-ui/admin/health/ocs-appstore-devconsole-ui |
| ocs-appstore-egress-api-gw | 200 | http://ocs-app.local:80/ocs-appstore-egress-api-gw/admin/health/ocs-appstore- |

Рисунок 12

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 18).

Таблица 18

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Первый столбец | Название сервиса ППО | Возможные значения определяются перечнем сервисов ППО. Зеленый цвет названия сервиса говорит о том, что сервис функционирует в штатном режиме |
| Второй столбец | Код http-ответа | Возможные значения определяются протоколом HTTP |
| Третий столбец | url-адрес функции (endpoint) сервиса «healthcheck» | Содержит url-адрес функции «healthcheck», которая возвращает информацию о статусе сервиса |

Перечисленные заголовки `"service_location"`, `"expose_location"`, `"service_vhost"`, `"expose_port"` – это режимы работы `consul-template`.

### 2.11.2.7. Раздел «Cluster Nodes Reachability»

Результат проверки доступности серверов (нод) кластера представлен на рисунке (Рисунок 13).

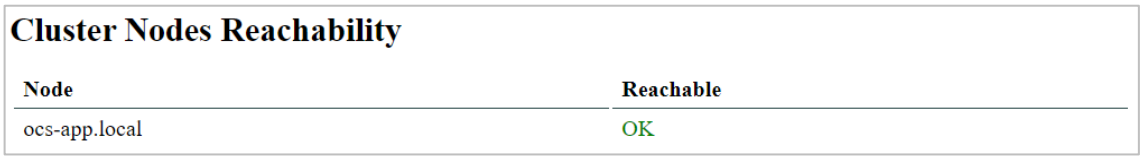



Рисунок 13

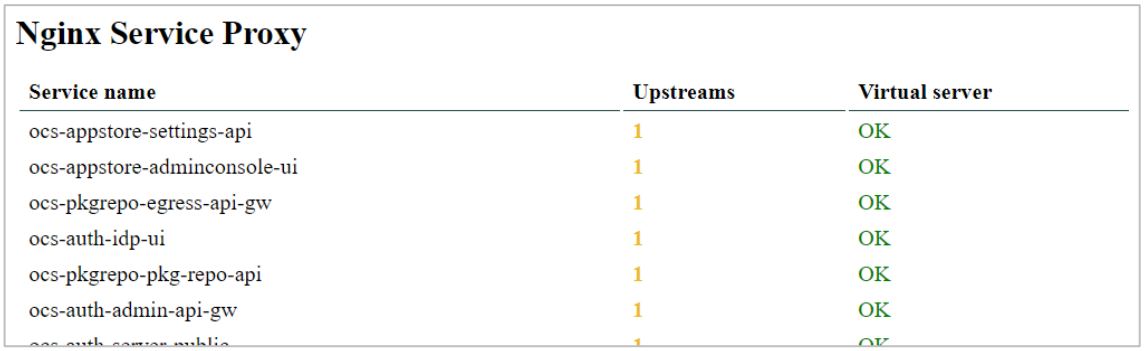
Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 19).

Таблица 19

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Node | Адрес сервера (хоста) | Определяется доменными именами хостов |
| Reachable | Информация о доступности сервера | Может принимать значения: «OK» (в случае доступности) или содержать сообщение об ошибке, которое вернет утилита ping |

### 2.11.2.8. Раздел «Nginx Service Proxy»

Информация о проверке конфигурации балансировщика микросервисов Nginx Web Server для каждого сервиса ППО приведена на рисунке (Рисунок 14).



**Nginx Service Proxy**

| Service name | Upstreams | Virtual server |
|---|---|---|
| ocs-appstore-settings-api | 1 | OK |
| ocs-appstore-adminconsole-ui | 1 | OK |
| ocs-pkgrepo-egress-api-gw | 1 | OK |
| ocs-auth-idp-ui | 1 | OK |
| ocs-pkgrepo-pkg-repo-api | 1 | OK |
| ocs-auth-admin-api-gw | 1 | OK |
| ocs-auth-server-public | 1 | OK |

Рисунок 14

Описание назначения столбцов таблицы, а также информация о возможных значениях приведены в таблице (Таблица 20).

Таблица 20

| Название столбца | Описание | Возможные значения (примеры значений) |
|---|---|---|
| Service name | Название сервиса ППО | Возможные значения определяются перечнем сервисов ППО |
| Upstreams | Количество экземпляров сервиса, заданных в конфигурационном файле Nginx | Целочисленные значения от 1 до n |
| Virtual server | Информация о наличие секции «server» для указанного сервиса ППО в конфигурационном файле Nginx.<br>В данной секции заданы настройки «виртуального» сервиса ППО, который осуществляет перенаправление (проксирование) http-запросов на «реальные» экземпляры сервиса | «ОК» - секция `server` присутствует<br>«`No server block found!`» - секция отсутствует |

### 2.11.2.9. Раздел «Filestorage Configuration»

Информация о конфигурации файловых хранилищ ПМ и ПООС представлена на рисунке (Рисунок 15).


Рисунок 15

Настройка «Filestorage location» содержит путь к каталогу и его статус.

В настройке «Configuration file» указан конфигурационный файл, в котором задан путь к файловому хранилищу.

# 3. УПРАВЛЕНИЕ КОМПОНЕНТАМИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ, СЕРВИСАМИ, НАСТРОЙКАМИ СЕРВИСОВ И ПОДСИСТЕМ

## 3.1. Управление компонентами среды функционирования ППО

Управление сервисами ППО заключается в их установке, обновлении и удалении, и осуществляется с помощью скрипта `deploy-infra.sh` из каталога `install-<версия ППО>`, созданного на этапе развертывания управляющей ПЭВМ (см. подраздел 2.3).

Формат команды управления сервисами имеет следующий вид:

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh <параметры> --extra-vars "force_upgrade=true"
```

Описание параметров команды управления:

1) `<имя пользователя>`

В параметре указывается имя привилегированного sudo-пользователя, под которым настроен SSH-доступ к серверам приложений и БД.

Доступ по SSH к среде функционирования ППО может быть недоступен в соответствии с политиками компании. В данном случае необходимо во всех командах `ansible-playbook` в конце добавлять параметр `--ask-pass`.

2) `-a, --action`

Данный параметр задает действие, которое необходимо выполнить.

Параметр может принимать следующие значения:

– параметр отсутствует - будет выполнена установка или обновление компонента (компонентов);

– `flush_all` - будет выполнено удаление компонента (компонентов).

3) `-c, --components`

Данный параметр задает компонент среды функционирования, для которого будет выполнена команда управления. Параметр может принимать следующие значения:

- `dnsmasq;`
- `nginx;`
- `consul;`
- `consul-template;`
- `nats-streaming-server;`
- `redis;`
- `ocs-user;`
- `db.`

В данном параметре может задаваться список подсистем, например:

```
--components dnsmasq, nginx
```

По умолчанию (если параметр на задан) команда управления будет применена ко всем компонентам.

4) `-d, --database`

Данный параметр задает версию СУБД PostgreSQL.

Параметр может принимать следующие значения:

- «11» - при использовании СУБД PostgreSQL 11;
- «12» - при использовании СУБД PostgreSQL 12.

При отсутствии параметра будет установлена СУБД PostgreSQL 11.

В случае, если в перечне компонентов (параметр --components) отсутствует СУБД, то значение данного параметра будет игнорироваться.

5) `--skip-database`

При наличии данного параметра СУБД не устанавливается.

6) `-l, --limit`

Данный параметр задает перечень хостов, для которых будет выполнена команда управления, например:

```
--limit  example01.omp, example02.omp
```

По умолчанию (если параметр на задан) команда управления будет применена ко всем хостам согласно инвентарному файлу `inventories/hosts.yml`.

7) `-e, --extra-vars`

В данном параметре передаются внешние переменные для скриптов развертывания. В ППО используются следующие внешние переменные:

– `force_upgrade=true` - служит для принудительного обновления компонентов среды функционирования ППО;

– `pg_slave_recreate=true` - служит для инициализации реплики БД.

8) `--help`

Вывод справочной информации.

Примеры команд управления:

1) установка или обновление всех компонентов:

```
ANSIBLE_USER="omp" ./deploy-infra.sh --database "11" --extra-vars
"force_upgrade=true"
```

2) установка или обновление Nginx на хосте `ocs-app.local`:

```
ANSIBLE_USER="omp" ./deploy-infra.sh --components nginx --limit ocs-
app.local --extra-vars "force_upgrade=true"
```

3) удаление Nginx:

```
ANSIBLE_USER="omp" ./deploy-infra.sh --components nginx --action
flush_all
```

4) получение справочной информации:

```
./deploy-infra.sh --help
```

## 3.2. Управление сервисами ППО

Управление сервисами ППО заключается в их установке, запуске, остановке, перезапуске, изменении настроек и осуществляется с помощью скрипта `deploy-ac.sh из каталога install-<версия ППО>`, созданного на этапе развертывания управляющей ПЭВМ (см. п. 2.3.7).

Формат команды управления сервисами имеет следующий вид:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh <параметры>
```

Описание параметров команды управления:

1) `<имя пользователя>`

В параметре указывается имя привилегированного sudo-пользователя, под которым настроен SSH-доступ к серверам приложений и БД.

Доступ по SSH к среде функционирования ППО может быть недоступен в соответствии с политиками компании. В данном случае необходимо во всех командах `ansible-playbook` в конце добавлять параметр `--ask-pass`.

2) `-s, --subsystems`

Данный параметр задает подсистему, для которой будет выполнена команда управления. Параметр может принимать следующие значения:

- `auth` (для ПБ);
- `appstore` (для ПМ);
- `emm` (для ПУ);
- `pkgrepo` (для ПООС).

В данном параметре может задаваться список подсистем, например:

```
--subsystems auth,appstore,emm,pkgrepo
```

По умолчанию (если параметр на задан) параметр имеет значение:

```
--subsystems auth,appstore,emm,pkgrepo
```

3) `-a, --apps`

Данный параметр задает перечень сервисов, для которых будет выполнена команда управления. Например:

```
--apps ocs-auth-adminconsole-ui,ocs-appstore-adminconsole-ui
```

Если необходимо выполнить команду сразу для всех сервисов подсистемы, то необходимо перечислить через запятую все сервисы подсистемы, либо задать значение параметра:

```
--apps all
```

По умолчанию (если параметр не задан), то параметр имеет значение «all».

В случае если заданные в параметре «`--apps`» сервисы не соответствуют заданным в параметре «`--subsystems`» подсистемам, то управляющая команда к таким сервисам применена не будет. При этом управление шлюзами доступа (сервисами шлюзов доступа) осуществляется в рамках той подсистемы, для которой они предназначены. Состав подсистем приведен в таблице (Таблица 21)

Таблица 21

| Значение параметра «--subsystems» | Сервисы (значение параметра «--apps») |
|---|---|
| ПБ | |
| auth | ocs-auth-admin-api-gw |
| | ocs-auth-public-api-gw |
| | ocs-auth-server-public-proxy |
| | ocs-auth-idp-api |
| | ocs-auth-accounts-devices-api |
| | ocs-auth-accounts-users-api |
| | ocs-auth-server-admin |
| | ocs-auth-server-public |
| | ocs-auth-audit-api |
| | ocs-auth-adminconsole-ui |
| | ocs-auth-idp-ui |
| ПМ | |
| appstore | ocs-appstore-applications-api |
| | ocs-appstore-settings-api |
| | ocs-appstore-adminconsole |
| | ocs-appstore-devconsole-ui |
| | ocs-appstore-admin-api-gw |
| | ocs-appstore-client-api-gw |
| | ocs-appstore-dev-api-gw |
| | ocs-appstore-egress-api-gw |

| Значение параметра «--subsystems» | Сервисы (значение параметра «--apps») |
|---|---|
| ПУ | |
| emm | ocs-emm-applications-api |
| | ocs-emm-dispatcher-api |
| | ocs-emm-devices-api |
| | ocs-emm-state-manager-api |
| | ocs-emm-enrollments-api |
| | ocs-emm-policies-api |
| | ocs-emm-reports-api |
| | ocs-emm-users-api |
| | ocs-emm-journal-api |
| | ocs-emm-jobs-api |
| | ocs-emm-adminconsole-ui |
| | ocs-emm-admin-api-gw |
| | ocs-emm-device-api-gw |
| | ocs-emm-egress-api-gw |
| ПООС | |
| pkgrepo | ocs-pkgrepo-pkg-repo-api |
| | ocs-pkgrepo-device-api-gw |
| | ocs-pkgrepo-admin-api-gw |
| | ocs-pkgrepo-egress-api-gw |

4) `-A, --action`

Данный параметр задает действие, которое необходимо выполнить. Перечень допустимых действий и соответствующие им значения параметра приведены в таблице (Таблица 22).

Таблица 22

| Значение параметра «action» | Действие |
|---|---|
| deploy | Установка |
| start | Запуск |
| stop | Остановка |
| restart | Перезапуск |
| config | Изменение настроек (переустановка конфигурационного файла) |
| flush_all | Удаление |

По умолчанию (если параметр не задан) параметр имеет значение `deploy`.

5) `-c, --clients`

Данный параметр задает OIDC клиентов, для которых будет выполнена команда управления. Например:

```
--clients auth-admin-console, aps-admin-console
```

Если необходимо выполнить команду сразу для всех OIDC клиентов, то необходимо перечислить через запятую все OIDC клиенты, либо задать значение параметра:

```
--clients all
```

По умолчанию (если параметр не задан) параметр имеет значение `all`.

6) `-d, --database`

Данный параметр задает СУБД, которая установлена на сервере БД. Параметр может принимать следующие значения:

- 11 (для СУБД PostgreSQL 11);
- 12 (для СУБД PostgreSQL 12);
- 11-pro (для СУБД Postgres Pro 11);
- 12-pro (для СУБД Postgres Pro 12).

Например:

```
--database 11
```

По умолчанию (если параметр не задан) параметр имеет значение «11».

7) `--help`

Вывод справочной информации.

Примеры команд управления:

1) остановка всех сервисов ПМ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --action stop
```

2) запуск сервисов `ocs-appstore-applications-api` и `ocs-appstore-adminconsole` ПМ:

```
ANSIBLE_USER=omp ./deploy-ac.sh --apps ocs-appstore-applications-
api,ocs-appstore-adminconsole --action start
```

3) получение справочной информации:

```
./deploy-ac.sh --help
```

## 3.3. Управление настройками сервисов и подсистем ППО

Управление настройками сервисов и подсистем ППО может осуществляться двумя способами.

### 3.3.1. Способ 1 (рекомендуемый)

Для изменения настроек сервисов и подсистем ППО данным способом необходимо выполнить следующие действия:

3.3.1.1. Задать требуемые значения параметров в конфигурационных файлах сценариев установки подсистем ППО. Описание параметров конфигурационных файлов сценариев установки подсистем ППО приведено в подразделе 8.3 настоящего документа.

3.3.1.2. Переустановить конфигурационные файлы с помощью следующей команды:

– ПБ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems auth --
action config
```

– ПМ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems appstore -
-action config
```

– ПУ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems emm --
action config
```

– ПООС:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems pkgrepo --
action config
```

### 3.3.2. Способ 2

Для изменения настроек сервисов и подсистем ППО данным способом необходимо выполнить следующие действия:

3.3.2.1. Задать требуемые значения параметров в конфигурационных файлах сервисов и подсистем ППО. Описание параметров конфигурационных файлов сценариев установки подсистем ППО приведено в разделе 8 настоящего документа.

3.3.2.2. Перезапустить требуемые сервисы с помощью следующей команды:

– ПБ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems auth --
apps <перечень сервисов ПБ> --action restart
```

– ПМ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems appstore -
-apps <перечень сервисов ПМ> --action restart
```

– ПУ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems emm --apps
<перечень сервисов ПУ> --action restart
```

– ПООС:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems pkgrepo --
apps <перечень сервисов ПООС> --action restart
```

# 4. РЕЗЕРВНОЕ КОПИРОВАНИЕ

ВНИМАНИЕ! Приведенные ниже имена файлов и каталогов характерны для типового варианта установки ППО и среды функционирования ППО.

## 4.1. Резервное копирование после установки (обновления) ППО

После успешной установки (обновления) ППО необходимо создать резервную копию каталога `install-<версия ППО>/install-ac/`.

## 4.2. Периодическое резервное копирование и резервное копирование перед установкой обновлений

Периодичность резервного копирования определяется регламентами эксплуатирующей организации.

Периодическое резервное копирование и резервное копирование перед установкой обновлений выполняется в приведенной ниже последовательности.

### 4.2.1. Резервное копирование данных

4.2.1.1. Создать резервные копии баз данных ПБ (auth), ПМ (appstore), ПУ (emm) и ПООС (pkgrepo).

Резервная копия БД выполняется в соответствии с эксплуатационной документацией на используемую СУБД либо в соответствии с регламентами эксплуатирующей организации.

4.2.1.2. Создать резервную копию каталога с файлами МП «Аврора Маркет».

Для этого необходимо создать резервную копию каталога `/ocs/appstore/applications-api` на Сервере приложений ПМ, либо в едином файловом хранилище, в зависимости от того какой вариант хранения файлов используется.

4.2.1.3. Создать резервную копию каталога с файлами пакетов ОС ПООС.

Для этого необходимо создать резервную копию каталога `/ocs/pkgrepo` на Сервере приложений ПООС либо в едином файловом хранилище, в зависимости от того, какой вариант хранения файлов используется.

### 4.2.2. Резервное копирование ППО

4.2.2.1. Создать резервную копию каталога с конфигурационными файлами подсистем и сервисов ППО (каталог: `/var/ocs/`).

4.2.2.2. Создать резервную копию сервисов ППО.

4.2.2.3. Для этого необходимо создать резервную копию файлов `*.target` и `*.service` по маске `ocs-*`, находящихся в каталоге `/etc/systemd/system/`, а также бинарных файлов сервисов по маске `ocs-*`, находящихся в каталоге `/usr/bin/`.

### 4.2.3. Резервное копирование компонентов среды функционирования

4.2.3.1. Создать резервную копию Nginx Web Server (каталог: `/etc/nginx/`).

4.2.3.2. Создать резервную копию Consul (каталог: `/opt/consul/`).

4.2.3.3. Создать резервную копию Consul Template (каталог: `/etc/consul-template/`).

4.2.3.4. Создать резервную копию Nats Streaming Server (каталог: `/data/nats/`).

4.2.3.5. Создать резервную копию конфигурационных файлов Redis (файлы: `/etc/redis.conf /etc/redis-sentinel.conf`).

4.2.3.6. Создать резервную копию конфигурационных файлов PostgreSQL (файлы: `/var/lib/pgsql/11/data/postgresql.conf`, `/var/lib/pgsql/11/data/pg_hba.conf` для ОС CentOS и `/var/lib/pgsql/data/postgresql.conf`, `/var/lib/pgsql/data/pg_hba.conf` для ОС Альт 8 СП).

4.2.3.7. Создать резервную копию конфигурационных файлов PostgresPro (файлы: `/opt/pgpro/std-11/data/postgresql.conf`, `/opt/pgpro/std-11/data/pg_hba.conf`).

4.2.3.8. Создать резервную копию сетевых настроек.

Для этого необходимо создать резервные копии следующих файлов:

- `/etc/hosts`;
- `/etc/hostname`;
- конфигурационные файлы DNS-сервера.

# 5. ОБНОВЛЕНИЕ ППО И ОС АВРОРА

## 5.1. Обновление сервера приложений ППО

ВНИМАНИЕ! Для установки обновления ППО количество свободного места на жестком диске сервера БД ПБ должно быть не меньше, чем размер самой БД ПБ. При недостаточном количестве свободного места на жестком диске его необходимо увеличить. Время обновления ППО зависит от размера БД и может занять длительное время.

Обновление севера приложений ППО выполняется в следующей последовательности:

5.1.1. Создать резервную копию данных, ППО и компонентов среды функционирования в соответствии с разделом 3 настоящего документа.

5.1.2. Скопировать на управляющую ПЭВМ архив с новой версией ППО и распаковать его в соответствии с пп. 2.3.3 - 2.3.7 настоящего документа.

5.1.3. При обновлении ППО на версию 2.5.1 необходимо перейти в каталог со сценариями установки новой версии ППО (каталог: `install-<новая версия ППО>/install-ac/`) и выполнить команду:

```
ansible-playbook -i inventories/hosts.yml -u <имя пользователя>
release_upgrade/play-upgrade_to_release_2.5.1.yml -vv --diff
```

5.1.4. При обновлении СУБД PostgreSQL 11/12 до новой старшей версии[2] (`major version`), необходимо удалить СУБД (без удаления данных), выполнив команду:

```
ansible-playbook play-postgresql.yml -i "inventories/hosts.yml" -vv --
diff -u <имя пользователя> --extra-var "flush_all=true
skip_subsystems=true"
```

5.1.5. Настроить компоненты среды функционирования ППО и ППО в соответствии с подразделом 2.4 настоящего документа.

[2] Согласно спецификации SemVer 2.0.0.

5.1.6. Установить компоненты среды функционирования в соответствии с п. 2.5.1 настоящего документа.

Устанавливать необходимо только те компоненты среды функционирования, у которых изменилась версия. Для этого необходимо выполнить сравнение версий компонентов среды функционирования в новом и предыдущем загрузочном модуле. Информация о версиях компонентов среды функционирования приведена в третьем столбце файла verions. Файл versions находится в корневом каталоге загрузочного модуля с компонентами среды функционирования.

Пример файла versions:

```
consul                    master          4698dcd2fa0ad1a29a846c2a475046d5e572f66a
consul-template           master          1dd681d509a1c5e3aa1882aeb53ebeb504faeecf
nginx                     master          420ad871296855752ed3bb31e9958ecf0d68ad52
postgresql                master          e7d2e67da97955d2440723a58dfb4510db3907b4
nats-streaming-server     master          fb4a9b55308f29c8bcda3fc1804da92db84e90d6
server-provision-scripts  master          cdcb455e074dd6bc2bcc519ebd842d36c3a29726
redis                     master          f4c6c300e7f9533652bb02008575ff009f8ef985
openssl                   master          7ac23c1d67a6671e20785a9e1cc84d7d8b46103d
cert-distr-infra          branch          1ac040b2fff85ce3c9fbca42a914b34679303acc
```

5.1.7. Установить ППО в соответствии с п. 2.4.2 настоящего документа.

5.1.8. После обновления ППО до версии 2.5.1 необходимо перейти в каталог со сценариями установки новой версии ППО (каталог: `install-<новая версия ППО>/install-ac/`) и выполнить команду:

```
ansible-playbook -i inventories/hosts.yml -u <имя пользователя>
release_upgrade/play-post_upgrade_to_release_2.5.1.yml -vv --diff --
limit <хост с ПМ>
```

В параметре limit необходимо указать имя одного из хостов с установленной ПМ (например, ocs-app.local).

5.1.9. Перезапустить сервис `ocs-pkgrepo-pkg-repo-api` с помощью команды:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems pkgrepo --
apps ocs-pkgrepo-pkg-repo-api --action restart
```

5.1.10. Оповестить пользователей ППО о необходимости очистить кэш и cookies веб-браузера. Иначе при открытии веб-интерфейса ППО будет ошибка HTTP ERROR 400.

## 5.2. Обновление мобильных приложений ППО

**ВНИМАНИЕ!** Перед обновлением МП ППО необходимо обновить сервер приложений ППО в соответствии с подразделом 5.1 настоящего документа, а также ОС Аврора до требуемой версии. Допускается обновление МП до более новой версии (downgrade МП не допускается).

Обновление МП ППО выполняется в следующей последовательности:

5.2.1. Запросить в технической поддержке предприятия-изготовителя пакет `omp-ocs-updater`

Пакет `omp-ocs-updater` представляет собой rpm-пакет, включающий пакеты МП из состава загрузочного модуля ППО, а также bash-скрипт для их правильной установки.

5.2.2. Загрузить в ПМ пакет `omp-ocs-updater` для тех версий ОС Аврора, под которыми происходит эксплуатация МП. Порядок действий по загрузке МП в ПМ приведен в документе «Руководство пользователя. Часть 2. Подсистема «Маркет».

5.2.3. С помощью политики «Приложения / Установка приложений на устройство» (функционал ПУ) установить новую версию МП на тестовую группу устройств с целью проверки корректности обновления. Порядок работы с политиками и группами МУ приведен в документе «Руководство пользователя. Часть 3. Подсистема Платформа управления».

**ВНИМАНИЕ!** В данной группе МУ должны быть устройства под управлением одной и той же трехзначной версии ОС Аврора (например, версии 3.2.3).

5.2.4. Загрузить в ПМ пакет `omp-ocs-updater` для тех версий ОС Аврора, под которыми происходит эксплуатация МП. Порядок действий по загрузке МП в ПМ приведен в документе «Руководство пользователя. Часть 2. Подсистема «Маркет».

5.2.5. Убедиться, что в карточке МУ (в Консоли администратора ПУ) отображается требуемая версия МП.

5.2.6. После успешного обновления МП на тестовой группе МУ, выполнить обновление аналогичным образом для остальных устройств.

## 5.3. Обновление ОС Аврора с помощью ПУ

Обновление ОС Аврора выполняется в следующей последовательности:

5.3.1. Обновить сервер приложений ППО в соответствии с подразделом 5.1 настоящего документа.

5.3.2. Обновить ОС Аврора до требуемой версии на тестовой группе устройств с целью проверки корректности обновления с помощью политики «Приложения/Установить версию ОС». Порядок работы с политиками и группами МУ приведен в документе «Руководство пользователя. Часть 3. Подсистема Платформа управления».

5.3.3. Убедиться, что после окончания, заданного в правиле временного интервала обновления, в карточке каждого устройства из тестовой группы отображается требуемая версия ОС Аврора.

5.3.4. Обновить МП ППО на тестовой группе устройств в соответствии с подразделом 5.2 настоящего документа.

5.3.5. выполнить обновление аналогичным образом для остальных устройств после успешного обновления ОС Аврора и МП на тестовой группе МУ.

# 6. УДАЛЕНИЕ ППО

Для удаления сервисов ППО необходимо выполнить следующие действия:

6.1. Перейти в каталог со сценариями установки ППО.

6.2. Удалить сервисы ППО с помощью следующих команд:

– ПБ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems auth --
action flush_all
```

– ПМ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems appstore -
-action flush_all
```

– ПУ:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems emm --
action flush_all
```

– ПООС:

```
ANSIBLE_USER=<имя пользователя> ./deploy-ac.sh --subsystems pkgrepo --
action flush_all
```

6.3. Удалить компоненты среды функционирования ППО с помощью следующих команд:

– dnsmasq:

```
-ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components
dnsmasq --action flush_all
```

– nginx:

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components nginx -
-action flush_all
```

– consul:

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components consul
--action flush_all
```

– consul template:

```
-ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components
consul-template --action flush_all
```

– nats streaming server:

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components nats-
streaming-server --action flush_all
```

– redis:

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh --components redis --action flush_all
```

– `postgresql` (без удаления данных):

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh  --components db --action flush_all
```

– `postgresql` (с удалением данных):

```
ANSIBLE_USER=<имя пользователя> ./deploy-infra.sh  --components db --action flush_all --extra-vars "pg_uninstall_delete_data=true"
```

# 7. КОНФИГУРАЦИОННЫЕ ФАЙЛЫ СЦЕНАРИЕВ УСТАНОВКИ СРЕДЫ ФУНКЦИОНИРОВАНИЯ

## 7.1. Конфигурационные файлы сценариев установки среды функционирования

### 7.1.1. Инвентарный файл inventories/hosts.yml

В инвентарном файле `inventories/hosts.yml` задаются адреса серверов приложений и серверов БД, на которые будут установлены компоненты среды функционирования. Описание секций инвентарного файла `inventories/hosts.yml` приведено в таблице (Таблица 23).

Таблица 23

| Секция конфигурационного файла | Описание |
|---|---|
| `all.children.ocs.children.app` | Сервера приложений ППО |
| `all.children.ocs.children.postgresql.children.postgresql_masters` | СУБД Postgres |
| `all.children.ocs.children.nginx` | Балансировщик микросервисов «Nginx Web Server» |
| `all.children.ocs.children.consul` | Система обнаружения сервисов «Consul» |
| `all.children.ocs.children.consul-template` | Средство управления конфигурациями микросервисов «Consul Template» |
| `all.children.ocs.children.nats_streaming_server` | Сервис гарантированной доставки сообщений «Nats Streaming Server» |
| `all.children.ocs.children.redis.children.redis_masters` | СУБД Redis для хранения сессий |
| `all.children.ocs.children.redis.children.sentinel` | Redis Sentinel обеспечивает высокую доступность СУБД Redis |

Файл сценария установки для установки среды функционирования ППО на одном сервере с адресом `ocs-app.local` имеет следующий вид:

```
all:
  children:
    ocs:
      children:
        app:
          hosts:
            ocs-app.local:
        postgresql:
          children:
            postgresql_masters:
              hosts:
                ocs-app.local:
            postgresql_slaves:
              hosts:
        nginx:
          children:
            app:
          hosts:
        consul:
          children:
            consul_servers:
              children:
                app:
              hosts:
            consul_agents:
        consul_template:
          children:
            app:
        nats_streaming_server:
          children:
                app:
          hosts:
        redis:
          children:
            redis_masters:
              children:
                app:
              hosts:
            sentinel:
              children:
                app:
              hosts:
```

### 7.1.2. Настройки сценариев установки среды функционирования в конфигурационном файле config/vars/_vars.yml

В данном конфигурационном файле задаются настройки следующих компонентов среды функционирования ППО: Nats Streaming Server, Consul, СУБД Redis и СУБД PostgreSQL.

Описание секций конфигурационного файла, относящихся к сценариям установки среды функционирования, приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

### 7.1.3. Настройки сценариев установки среды функционирования в конфигурационном файле config/vars/_vars_infra.yml

В данном конфигурационном файле задаются настройки СУБД PostgreSQL.

Описание секций конфигурационного файла приведено в таблице (Таблица 24).

Таблица 24

| Секция конфигурационного файла | Описание |
|---|---|
| `pg_settings.listen_addresses` | IP-адреса сетевых интерфейсов, по которым сервер будет принимать подключения |
| `pg_settings.timezone` | Часовой пояс для вывода и ввода значений времени |
| `pg_settings.log_timezone` | Часовой пояс для штампов времени при записи в журнал сервера |
| `pg_hba_settings.type` | Тип подключения |
| `pg_hba_settings.name` | Имя пользователя |
| `pg_hba_settings.database` | Имя БД |
| `pg_hba_settings.address` | IP-адрес хоста или IP-адрес подсети |
| `pg_hba_settings.method` | Метод аутентификации |
| `pg_replication_user.type` | Тип подключения пользователя с ролью «replication» |
| `pg_replication_user.name` | Имя пользователя с ролью «replication» |
| `pg_replication_user.database` | Имя БД |

| Секция конфигурационного файла | Описание |
|---|---|
| pg_replication_user.address | IP-адрес хоста или IP-адрес подсети |
| pg_replication_user.method | Метод аутентификации пользователя с ролью «replication» |
| pg_replication_user.password | Пароль пользователя с ролью «replication» |

С подробным описанием параметров и возможными значениями параметров можно ознакомиться в документации на СУБД PostgreSQL или СУБД Postgres Pro

Конфигурационный файл `config/vars/_vars_infra.yml` может иметь следующий вид:

```
pg_settings: # postgresql.conf parameters
  listen_addresses: "0.0.0.0"
  timezone: "UTC"
  log_timezone: "UTC"

pg_hba_settings: # pg_hba.conf settings
  - type: local ## Unix-socket access
    name: all
    database: all
    method: trust
  - type: host ## Localhost IPv4 access
    name: all
    database: all
    address: 127.0.0.1/32
    method: trust
  - type: host ## DB hosts
    name: all
    database: all
    address: "{{ groups['postgresql'] }}"
    method: md5
  - type: host ## Application hosts
    name: all
    database: all
    address: "{{ groups['app'] }}"
    method: md5
  - type: host  # Gitlab CI vbox-testing
    name: all
    database: all
    address: 172.17.0.0/16
    method: md5
  - type: host  # TODO: What's it local zone for?
    name: all
    database: all
    address: 172.28.0.0/16
    method: md5
```

```
pg_replication_user: # Replication access configuration
  type: host
  name: replication
  database: replication
  address: "{{ ansible_default_ipv4.network }}/24"
  method: md5
  password: 123Qwe!@#
```

# 8. КОНФИГУРАЦИОННЫЕ ФАЙЛЫ ППО (СЦЕНАРИЕВ УСТАНОВКИ ППО)

## 8.1. Общая информация о конфигурационных файлах ППО

ППО содержит следующие типы конфигурационных файлов:

– конфигурационные файлы подсистем ППО (`config.yml`);

– конфигурационные файлы сервисов (модулей) ППО (`<название сервиса>.yml`).

В конфигурационных файлах подсистем содержатся настройки подсистем ППО. Также в конфигурационные файлы подсистем вынесены (могут быть вынесены) отдельные настройки сервисов ППО, которые может изменять администратор ППО. В данном случае в конфигурационном файле содержится секция с именем сервиса. Например, секция для сервиса `ocs-auth-accounts-users-api` выглядит следующим образом:

```
#-----------------------------------------------------------------------
---------
# Parameters for user accounts
#-----------------------------------------------------------------------
---------
ocs-auth-accounts-users-api:

  ##
  # The number of recently used passwords,
  # which system will store for forbidding use it for new password
creating.
  ##
  passwordHistoryDepth: 3

  ##
  # Maximum inactivity period 45 days.
  # If account not use system during this time, account will be
blocked.
  # Must be greater or equal to OIDC refresh token lifetime.
  ##
  maxAccountInactivityPeriod: "1080h"
```

Описание параметров конфигурационных файлов подсистем ППО приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

Конфигурационные файлы подсистем ППО располагаются по следующему пути:

`/var/ocs/<название подсистемы>/config.yml`

Например, конфигурационный файл ПБ:

`/var/ocs/auth/config.yml`

Конфигурационные файлы сервисов содержат настройки сервисов ППО и располагаются по следующему пути:

`/var/ocs/<название подсистемы>/<название сервиса>/<название сервиса>.yml`

Например, конфигурационный файл сервиса `ocs-auth-idp-api` ПБ:

`/var/ocs/auth/ocs-auth-idp-api/ocs-auth-idp-api.yml`

Описание параметров конфигурационных файлов сервисов приведено в самих конфигурационных файлах в виде комментариев.

ВНИМАНИЕ! Редактировать конфигурационные файлы сервисов ППО не рекомендуется.

## 8.2. Общая информация о конфигурационных файлах сценариев установки ППО

Сценарии установки ППО содержат следующие типы конфигурационных файлов:

– конфигурационный файл `inventories/hosts.yml`;

– конфигурационные файлы `config/vars/_vars.yml`;

– конфигурационные файлы подсистем `config/subsystems/<название подсистемы>/vars/_vars.yml`;

– шаблоны конфигурационных файлов подсистем ППО (`config.yml.j2`);

– шаблоны конфигурационные файлы сервисов (модулей) ППО (`<название сервиса>.yml.j2`).

### 8.2.1. Конфигурационный файл inventories/hosts.yml

Конфигурационный файл `inventories/hosts.yml` содержит адреса серверов (имена хостов), на которые установлены (будут установлены) компоненты среды функционирования ППО и подсистемы ППО.

Описание параметров конфигурационных файлов `inventories/hosts.yml` приведено в п. 7.1.1 настоящего документа.

### 8.2.2. Общий конфигурационный файл сценариев установки config/vars/_vars.yml

Конфигурационный файл `config/vars/_vars.yml` является общим для всех подсистем и модулей ППО. В нем содержится полный перечень общих параметров, относящихся к подсистемам и модулям ППО.

Описание параметров конфигурационного файла `config/vars/_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

### 8.2.3. Конфигурационные файлы сценариев установки для подсистем ППО (файлы: config/subsystems/<название подсистемы>/vars/_vars.yml)

Конфигурационные файлы `vars.yml` подсистем содержат параметры, относящиеся к конкретной подсистеме. Также данные файлы могут быть дополнены параметрами из общего конфигурационного файла, значения которых надо переопределить для заданной подсистемы.

Конфигурационные файлы `_vars.yml` в большей части содержат настройки взаимодействия подсистем с компонентами среды функционирования. Располагаются данные конфигурационные файлы в каталоге со сценариями установки по следующему пути:

`config/subsystems/<название подсистемы>/vars/_vars.yml`

Например, конфигурационный файл vars.yml для ПБ:

`config/subsystems/auth/vars/_vars.yml`

Описание параметров конфигурационных файлов `_vars.yml` приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

### 8.2.4. Шаблоны конфигурационных файлов подсистем ППО

На основе данных файлов в процессе установки ППО формируются конфигурационные файлы подсистем ППО. Значения параметров в шаблонах конфигурационных файлах подсистем ППО задаются администратором, а также сценариями установки на основе значений, заданных администратором в конфигурационных файлах `_vars.yml`.

Располагаются данные конфигурационные файлы в каталоге со сценариями установки по следующему пути:

`config/subsystems/<название подсистемы>/config/services/config.yml.j2`

Например, шаблон конфигурационного файла ПБ:

`config/subsystems/auth/config/services/config.yml.j2`

Описание параметров шаблонов конфигурационных файлов подсистем ППО приведено в п. 8.3.2, 8.3.3, 8.3.4, 8.3.5 настоящего документа.

### 8.2.5. Шаблоны конфигурационных файлов сервисов ППО

На основе данных файлов в процессе установки ППО формируются конфигурационные файлы сервисов ППО.

Шаблоны конфигурационных файлов сервисов располагаются в каталоге со сценариями установки по следующему пути:

`config/subsystems/<название подсистемы>/config/services/<название сервиса>/<название сервиса>.yml.j2`

Например, шаблон конфигурационного файла сервиса `ocs-auth-adminconsole-ui` ПБ:

`config/subsystems/auth/config/services/ocs-auth-adminconsole-ui/ocs-auth-adminconsole-ui.yml.j2`

Описание параметров шаблонов конфигурационных файлов сервисов приведено в самих конфигурационных файлах в виде комментариев.

ВНИМАНИЕ! Редактировать шаблоны конфигурационных файлов сервисов ППО не рекомендуется.

### 8.2.6. Конфигурационные файлы окружений

Данные конфигурационные файлы включают:

– общий конфигурационный файл сценариев установки ППО для заданного окружения (файл: `config/environments/<название окружения>/vars/_vars.yml`);

– конфигурационные файлы сценариев установки подсистем ППО для заданного окружения (файлы в каталоге: `config/environments/<название окружения>/<название подсистемы>/vars/`).

В данных конфигурационных файлах переопределяются параметры общего конфигурационного файла сценариев установки ППО и конфигурационных файлов сценариев установки подсистем ППО.

Для того чтобы переопределить параметр, необходимо:

– скопировать параметр (включая секцию, в которую входит параметр) из общего конфигурационного файла сценариев установки ППО или конфигурационного файла сценариев установки подсистем ППО;

– вставить скопированное значение в аналогичный конфигурационный файл для заданного окружения;

– задать требуемое значение параметра.

### 8.2.7. Порядок работы с конфигурационными файлами сценариев установки ППО

В целях оптимизации настройки ППО, а также отдельных подсистем ППО и модулей ППО была реализована следующая структура конфигурационных файлов сценариев установки ППО, приведенная в таблице (Таблица 25).

Таблица 25

| Каталог (имя файла) | Описание | Порядок применения параметров (приоритет параметров) |
|---|---|---|
| config/vars/_vars.yml | Общий (для всех подсистем и модулей ППО) конфигурационный файл сценариев установки ППО. В нем содержится полный перечень общих параметров, относящихся к подсистемам и модулям ППО | 1 (самый низкий приоритет) |
| config/subsystems/<название подсистемы>/vars/<br><br>Например, config/subsystems/auth/vars/ | Конфигурационные файлы сценариев установки подсистем ППО. В них содержатся параметры, относящиеся к конкретной подсистеме. Также данные файлы могут быть дополнены параметрами из общего конфигурационного файла, значения которых надо переопределить для заданной подсистемы | 2 |
| config/environments/<название окружения>/vars/_vars.yml<br><br>Например, config/environments/release/vars/_vars.yml | Общий конфигурационный файл сценариев установки ППО для заданного окружения. В нем могут содержаться параметрами из общего конфигурационного файла, значения которых надо переопределить для заданного окружения | 3 |
| config/environments/<окружение>/<название подсистемы>/vars/<br><br>Например, config/environments/release/auth/vars/ | Конфигурационные файлы сценариев установки подсистем ППО для заданного окружения. В них могут содержаться параметры из общего конфигурационного файла или из конфигурационных файлов подсистем ППО, значения которых надо переопределить для заданного окружения | 4 (самый высокий приоритет) |

При установке ППО параметры конфигурационных файлов применяются согласно порядку, приведенному в таблице (Таблица 25). Т.е. сценарий установки обрабатывает сначала конфигурационные файлы в каталоге `config/vars/`, затем в каталоге `config/subsystems/<название подсистемы>/vars/` и т.д. Если, например, какой-либо параметр одновременно задан и в `config/vars/` и `config/subsystems/<название подсистемы>/vars/`, то ППО будет установлено со значением параметра, заданным в `config/subsystems/<название подсистемы>/vars/`.

Правила обработки сценариями установки ППО параметров, массивов и списков, если они одновременно заданы в нескольких конфигурационных файлах

Правило обработки параметров: Значение параметра в конфигурационном файле с более высоким приоритетом переопределяет значение параметра в конфигурационном файле с более низким приоритетом.

Пример параметра:

```
redis_password: "example_redis_password"
```

Правило обработки массивов: массив в конфигурационном файле с более высоким приоритетом переопределяет массив в конфигурационном файле с более низким приоритетом.

Пример массива:

```
pg_hba_settings:
  - type: local  # Unix-socket access
    name: all
    database: all
    method: trust
  - type: host  # Localhost IPv4 access
    name: all
    database: all
    address: 127.0.0.1/32
    method: trust
  - type: host  # Localhost IPv6 access
    name: all
    database: all
    address: ::1/128
    method: trust
  - type: host  # Gitlab CI vbox-testing
    name: all
    database: all
    address: 172.17.0.0/16
    method: md5
```

Правило обработки списков: если список в конфигурационном файле с более низким приоритетом содержит новые элементы (которых не было в конфигурационном файле с более высоким приоритетом), то они добавляются к исходному списку. Значение параметра в списке, содержащемся в конфигурационном файле с более высоким приоритетом, переопределяет значение параметра из списка содержащемся в конфигурационном файле с более низким приоритетом.

Пример списка:

```
postgresql:
  dbname: example_db_name # database name
  port: 5432              # port
  user: example_user      # user
  password: ocs           # password
  extensions: ["pg_partman_bgw", "pg_trgm", "pg_stat_statements",
"pgcrypto"] # necessary extensions
```

## 8.3. Описание конфигурационных файлов ППО (сценариев установки ППО)

### 8.3.1. Описание конфигурационного файла сценариев установки ППО hosts.yml (файл: inventories/hosts.yml)

8.3.1.1. Описание конфигурационного файла сценариев установки ППО hosts.yml (файл: `inventories/hosts.yml`) приведено в таблице (Таблица 26).

Таблица 26

| Параметр | Описание | Добавлен / Удален |
|---|---|---|
| all.children.ocs.children.app.hosts | Хосты, куда будут установлены серверные приложения ППО | 2.2.0 / - |
| all.children.ocs.children.app.vars.ext_loadbalancer | | 2.2.0 / - |
| all.children.ocs.children.app.vars.int_loadbalancer | | 2.2.0 / - |
| all.children.ocs.children.postgresql.children.postgresql_masters.hosts | Хосты, куда будет установлена СУБД PostgreSQL или Postgres Pro (master) | 2.2.0 / - |

| Параметр | Описание | Добавлен / Удален |
|---|---|---|
| all.children.ocs.children.postgresql.children.postgresql_slaves.hosts | Хосты, куда будет установлена СУБД PostgreSQL или Postgres Pro (slave) | 2.2.0 / - |
| all.children.ocs.children.nginx.children.app | Хосты, куда будет установлен балансировщик микросервисов Nginx Web Server | 2.2.0 / - |
| all.children.ocs.children.consul.children.consul_masters.children.app | Хосты, куда будет установлена система мониторинга сервисов Consul. (master) | 2.2.0 / - |
| all.children.ocs.children.consul.children.consul_agents | Хосты, куда будет установлена система мониторинга сервисов Consul. (agent) | 2.2.0 / - |
| all.children.ocs.children.consul_template.children.children.app | Хосты, куда будет установлен Consul Template | 2.2.0 / - |
| all.children.ocs.children.nats_streaming_server.hosts | Хосты, куда будет установлен сервис гарантированной доставки сообщений Nats streaming server | 2.2.0 / - |
| all.children.ocs.children.redis.children.redis_masters.hosts | Хосты, куда будет установлена СУБД Redis для хранения сессий (master) | 2.2.0 / - |
| all.children.ocs.children.redis.children.redis_slaves.hosts | Хосты, куда будет установлена СУБД Redis для хранения сессий (slave) | 2.2.0 / - |
| all.children.ocs.children.redis.children.sentinel.hosts | Хосты, куда будет установлен Redis Sentinel, обеспечивающий высокую доступность СУБД Redis | 2.2.0 / - |

### 8.3.2. Описание конфигурационных файлов ПБ (сценариев установки ПБ)

8.3.2.1. Описание параметров конфигурационного файла ПБ (`/var/ocs/auth/config.yml`), шаблона конфигурационного файла ПБ (`config/subsystems/auth/config/services/config.yml.j2`) и конфигурационного файла сценариев установки ПБ `_vars.yml`

(config/subsystems/auth/vars/_vars.yml) приведено в таблице (Таблица 27).

Таблица 27

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| config.publicUris.auth. | publicUri | auth_public_uri | Полный адрес публичного API сервера авторизации | 2.2.1 / - |
| config.publicUris.auth. | publicBasepath | auth_public_basepath | Префикс url публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.publicUris.auth. | adminBasepath | auth_admin_basepath | Префикс url к API Консоли ПБ, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.publicUris.emm. | adminUri | emm_admin_uri | Полный адрес API/UI Консоли администратора ПУ | 2.2.1 / - |
| config.publicUris.aps. | adminUri | aps_admin_uri | Полный адрес API/UI Консоли администратора ПМ | 3.0.0 / - |
| config.session. | rememberFor | session_remember_for | Время жизни сессии пользователя консоли | 2.2.0 / - |
| config.session. | renewTimeout | session_renew_timeout | Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | один раз за данный интервал) | |
| config.database. | host | Задается выражением `{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster \| bool %}localhost{% else %}{{ groups['postgresql_masters'] \| first }}{% endif %}` | Адрес (хост) базы данных | 2.2.0 / - |
| config.database. | port | postgresql.port | Порт БД | 2.2.0 / - |
| config.database. | dbname | postgresql.dbname | Имя БД | 2.2.0 / - |
| config.database. | user | postgresql.user | Имя пользователя БД | 2.2.0 / - |
| config.database. | password | postgresql.password | Пароль БД | 2.2.0 / - |
| config.consul. | token | consul_token | Секрет для аутентификации в `consul` | 2.5.0 / - |
| config.redis. | sentinelAddresses | Задается выражением `{{ groups['sentinel'] \| map('regex_replace', '^(.*)$', '\\1:26379') \| join(',') }}` с использованием параметров из hosts.yml | Адрес модуля `sentinel` СУБД Redis | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| config.redis. | sentinelPassword | redis_password | Пароль к модулю sentinel СУБД Redis | 2.2.0 / - |
| config.redis. | masterName | redis_master_name | Идентификатор (имя) БД Redis | 2.2.0 / - |
| config.redis. | password | redis_password | Пароль к СУБД Redis | 2.2.0 / - |
| config.transport. | shutdownTime | transport_shutdown_time | Время на завершение открытых соединений, перед перед тем, как сервис завершит работу | 2.3.0 / - |
| config.transport.nats. | url | Задается выражением {% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}}@{{ host }}:4222{% if not loop.last %},{% endif %}{% endfor %} с использованием параметров из hosts.yml и vars.yml | Адрес сервера NATS | 2.3.0 / - |
| config.transport.nats. | clusterID | nats.cluster_id | Идентификатор кластера NATS (https://docs.nats.io/) | 2.3.0 / - |
| config.transport.nats. | redeliveryCount | - | Количество повторных отправок сообщений шиной при неудачной обработке сообщения | 2.5.0 / - |
| config.transport.http.tls. | enabled | - | Флаг включения TLS протокола | 2.2.0 / - |
| config.transport.http.tls. | private_key | - | Путь к файлу с приватным ключом. | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | При незаполненном значении формируется по принципу `config_folder/app_name/app_name.key` | |
| `config.transport.http.tls.` | `certificate` | - | Путь к файлу с сертификатом (публичный ключ). При незаполненном значении формируется по принципу `config_folder/app_name/app_name.crt` | 2.2.0 / - |
| `config.transport.http.tls.` | `ca_certificate` | - | Путь к файлу с доверенным сертификатом. При незаполненном значении формируется по принципу `config_folder/ca.crt` | 2.2.0 / - |
| `config.transport.http.httpDebug.` | `address` | - | [не используется] Адрес сервера (для служебных debug-эндпоинтов приложения) | 2.4.0 / - |
| `config.transport.http.httpDebug.tls.` | `enabled` | - | [не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| `config.transport.http.httpDebug.tls.` | `private_key` | - | [не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| config.transport.http.httpDebug.tls. | certificate | - | [не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| config.transport.http.httpDebug.tls. | ca_certificate | - | [не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| config.ttl. | login_consent_request | ttl_login_consent_request | Время жизни запроса на авторизацию | 2.2.0 / - |
| config.ttl. | access_token | ttl_access_token | Время жизни access_token | 2.2.0 / - |
| config.ttl. | refresh_token | ttl_refresh_token | Время жизни refresh_token. При значении "-1" считается бесконечным | 2.2.0 / - |
| config.ttl. | id_token | ttl_id_token | Время жизни id_token | 2.2.0 / - |
| config.ttl. | auth_code | ttl_auth_code | Время жизни auth_code | 2.2.0 / - |
| config. | passwordExpirationTime | - | Максимальное время действия пароля. | 2.2.0 / - |
| config.passwordSettings. | minLength | - | Минимальная длина пароля. Значение: 8. Если указать значение меньше, чем 8, то система должна считать, что minPasswordLength = 8. | 2.2.0 / - |
| config.passwordSettings. | maxLength | - | Максимальная длина пароля. Значение: 255. | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | Если указать значение меньше, чем `minPasswordLength` (минимальная длина пароля), то система должна считать, что `maxPasswordLength = minPasswordLength` | |
| `config.passwordSettings.` | `minDigits` | - | Минимальное число цифр в пароле (3) | 2.2.0 / - |
| `config.passwordSettings.` | `minUpperLetters` | - | Минимальное число букв верхнего регистра в пароле (2) | 2.2.0 / - |
| `config.passwordSettings.` | `minlowerLetters` | - | Минимальное число букв нижнего регистра в пароле (2) | 2.2.0 / - |
| `config.passwordSettings.` | `minSpecialchars` | - | Минимальное число спецсимволов в пароле (2) | 2.2.0 / - |
| `config.passwordSettings.` | `upperLetters` | - | Допустимые для пароля символы верхнего регистра `ABCDEFGHIJKLMNOPQRSTUVWXYZ` | 2.2.0 / - |
| `config.passwordSettings.` | `lowerLetters` | - | Допустимые для пароля символы нижнего регистра `abcdefghijklmnopqrstuvwxyz` | 2.2.0 / - |
| `config.passwordSettings.` | `specialChars` | - | Допустимые для пароля специальные символы `!@#$%^&*()_+` | 2.2.0 / - |
| `config.` | `failedLoginTries` | - | Максимальное количество неуспешных попыток | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | аутентификации (ввода неправильного пароля) до блокировки учетной записи.<br>Значение: "3" | |
| config. | failedLoginBlockTime | - | Время блокировки учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации.<br>Значение: "15m" | 2.2.0 / - |
| config. | loginGraceTime | - | Время, в течение которого считаются неуспешные попытки аутентификации перед блокировкой | 2.2.0 / - |
| config. | privilegedSessionsLimit | privileged_sessions_limit | Допустимое количество одновременно запущенных сессий у привилегированной учетной записи | 2.2.0 / - |
| config. | unprivilegedSessionsLimit | unprivileged_sessions_limit | Допустимое количество одновременно запущенных сессий у непривилегированной учетной записи | 2.2.0 / - |
| config. | insecureUri | insecure_uri | Флаг использования незащищенного соединения. Этот параметр надо задавать | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | в true если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов. | |
| config. | expose_internal_errors | expose_internal_errors | Флаг отображения расширенной информации в ошибках. По умолчанию выключен, так как информация может содержать данные, нежелательные к раскрытию. Используется для отладки | 2.5.0 / - |
| config. | insecureRedirectUris | Задается выражением<br>[{% if insecure_uri is defined and insecure_uri %}<br>"{{ emm_admin_uri }}/",<br>"{{ aps_admin_uri }}/",<br>"{{ aps_dev_uri }}/",<br>"{{ auth_admin_uri }}/",<br>"{{ push_admin_uri }}/",<br>{% endif %}] | Список url на которые сервер авторизации разрешает делать редирект по протоколу http в процессе аутентификации. Конфиг можно заполнять только при включенной опции config.insecureUri | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | с использованием параметров из `vars.yml` | | |
| `config.secrets.` | `system` | - | Ключи для шифрования системной информации | 2.2.0 / - |
| `config.secrets.` | `cookie` | - | Ключи для шифрования `cookie`, передаваемые в браузер | 2.2.0 / - |
| `config.` | `allowTerminationFrom` | Задается выражением `[ {% if allow_termination_from is defined %} {% for host in allow_termination_from %} "{{ host }}", {% endfor %} {% endif %} {% for host in groups['app'] %} "{{ hostvars[host]['ansible_default_ipv4']['address'] }}/32", {% endfor %} ]` с использованием параметров из `vars.yml` и `hosts.yml` | Список ip адресов, с которых можно делать запросы на сервер авторизации по протоколу http | 2.2.0 / - |
| `config.ocs-auth-accounts-users-api.` | `passwordHistoryDepth` | - | Число последних использованных паролей, которые запрещено использовать при создании новых паролей. Новый пароль | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | не должен совпадать с паролями из истории в рамках заданного значения. Используется для учетных записей пользователей | |
| config.ocs-auth-accounts-users-api. | maxAccountInactivityPeriod | - | Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована. Используется для учетных записей пользователей. | 2.2.0 / - |
| config.ocs-auth-accounts-devices-api. | passwordHistoryDepth | - | Число последних использованных паролей, которые запрещено использовать при создании новых паролей. Новый пароль не должен совпадать с паролями из истории в рамках заданного значения. Используется для учетных записей с ролью МП «Аврора Центр» | 2.2.0 / - |
| config.ocs-auth-accounts-devices-api. | maxAccountInactivityPeriod | - | Максимальный срок неактивности учетной записи, после которого она должна быть заблокирована. Используется для | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | учетных записей с ролью МП «Аврора Центр» | |
| config. | gatewayTimeout | gateway_timeout | Таймаут запросов на шлюзы | 2.2.0 / - |
| config. | hashWorkers | – | Количество воркеров, вычисляющих хэши паролей. По умолчанию 16. | 2.4.0 / - |
| config.oidcClients.authAdminConsole. | scope | Задается выражением {{ oidc_clients['auth-admin-console'].scope }} с использованием параметров из oidc.yml | Скопы для oidc клиента, который используется для аутентификации в Консоли ПБ | 2.2.0 / - |
| config.oidcClients.authAdminConsole. | returnUri | Задается выражением {{ oidc_clients['auth-admin-console'].redirect_uris \| first }} с использованием параметров из oidc.yml | Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли ПБ | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| `config.logger.` | `level` | `logger_level` | Уровень детализации сообщений логирования.<br>Возможные значения:<br>– `debug` - Логирование отладочной информации. Включает сообщения уровней `debug, info, warn, error;`<br>– `info` - Логирование информации о событиях, не приводящих к ошибкам. Включает сообщения уровней `info, warn, error;`<br>– `warn` - Логирование информации о событиях, которые могут привести к ошибкам. Включает сообщения уровней `warn`, error;<br>– `error` - Логирование информации об ошибках. Включает сообщения уровня `error` | 2.2.0 / - |
| `config.logger.` | `caller` | `logger_caller` | Флаг включения в сообщение лога названия функции и номера строки, в | 2.2.0 / - |

| Параметр в файлах: config.yml, config.yml.j2 | | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|---|
| | | | которой происходит логирование события | |
| config.logger. | humanReadable | logger_human_readable | Флаг включения форматирования сообщений лога в обычный текст (не json) | 2.4.0 / - |
| config.tracing. | enabled | tracing_enabled | Флаг включения трассировки | 2.2.0 / - |
| config.tracing. | sample_rate | tracing_sample_rate | Частота дискретизации трассировки | 2.2.0 / - |
| config.tracing. | reporting_period | tracing_reporting_period | Отчетный период трассировки | 2.2.0 / - |
| config.tracing. | jaeger_agent_endpoint | - | Адрес подключения к Jaeger | 2.2.0 / - |
| config.jaeger. | address | - | Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/) | 2.2.0 / - |
| config. | enablePprof | enable_pprof | Флаг включения отладочного профилировщика | 2.2.0 / - |

### 8.3.3. Описание конфигурационных файлов ПМ (сценариев установки ПМ)

8.3.3.1. Описание параметров конфигурационного файла ПМ (/var/ocs/appstore/config.yml), шаблона конфигурационного файла ПМ (config/subsystems/appstore/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПМ _vars.yml (config/subsystems/appstore/vars/_vars.yml) приведено в таблице (Таблица 28).

Таблица 28

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| config.publicUris.auth. | publicUri | auth_public_uri | Полный адрес публичного API сервера авторизации * | 2.2.1 / - |
| – | – | auth_public_address | Адрес публичного API сервера авторизации | 2.4.0 / - |
| – | – | auth_public_basepath | Basepath публичного API сервера авторизации | 2.4.0 / - |
| config.publicUris.auth. | adminUri | auth_admin_uri | Полный адрес API/UI Консоли ПБ * | 2.2.1 / - |
| – | – | auth_admin_address | Адрес API/UI Консоли ПБ | 2.4.0 / - |
| – | – | auth_admin_basepath | Basepath API/UI Консоли ПБ | 2.4.0 / - |
| config.publicUris.aps. | adminUri | aps_admin_uri | Полный адрес API/UI Консоли администратора ПМ | 2.5.0 / - |
| – | – | aps_admin_address | Адрес API/UI Консоли администратора ПМ | 2.5.0 / - |
| – | – | aps_admin_basepath | Basepath API/UI Консоли администратора ПМ | 2.5.0 / - |
| config.publicUris.aps. | devUri | aps_dev_uri | Полный адрес API/UI Консоли разработчика ПМ * | 2.2.1 / - |
| – | – | aps_dev_address | Адрес API/UI Консоли разработчика ПМ | 2.4.0 / - |
| – | – | aps_dev_basepath | Basepath API/UI Консоли разработчика ПМ | 2.4.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| config.publicUris.aps. | devBasepath | aps_dev_basepath | Префикс API/UI Консоли разработчика ПМ | 2.2.1 / - |
| config.publicUris.aps. | adminBasepath | aps_admin_basepath | Префикс в url для Консоли администратора ПМ | 2.2.1 / - |
| config.publicUris.aps. | marketUri | aps_market_uri | Полный адрес API клиентского шлюза | 2.5.0 / - |
| - | - | aps_market_address | Адрес API клиентского шлюза | 2.5.0 / - |
| - | - | aps_market_basepath | Basepath API клиентского шлюза | 2.5.0 / - |
| config.publicUris.emm. | adminUri | emm_admin_uri | Полный адрес API/UI Консоли администратора ПУ | 2.2.1 / - |
| - | - | emm_admin_address | Адрес API/UI Консоли администратора ПУ | 2.4.0 / - |
| - | - | emm_admin_basepath | Basepath API/UI Консоли администратора ПУ | 2.4.0 / - |
| config.systemUris.auth. | publicAddress | "http://ocs-auth-public-api-gw." + domain | Адрес публичного API авторизации - для межсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.auth. | publicBasepath | - | Префикс публичного API авторизации - для межсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.auth. | adminAddress | "http://ocs-auth-admin-api-gw." + domain | Адрес административного API авторизации - для | 2.2.1 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | | межсистемного взаимодействия | |
| config.systemUris.auth. | adminBasepath | - | Префикс административного API авторизации - для межсистемного взаимодействия | 2.2.1 / - |
| config.session. | rememberFor | session_remember_for | Время жизни сессии пользователя консоли | 2.2.0 / - |
| config.session. | renewTimeout | session_renew_timeout | Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал) | 2.2.0 / - |
| config.oidcClients.apsDevConsole. | scope | oidc_clients['aps-dev-console'].scope из hosts.yml | Скопы для oidc клиента, который используется для аутентификации в Консоли разработчика ПМ | 2.2.0 / - |
| config.oidcClients.apsDevConsole. | returnUri | oidc_clients['aps-dev-console'].redirect_uris из hosts.yml | Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли разработчика ПМ | 2.2.0 / - |
| config.oidcClients.apsAdminConsole. | scope | oidc_clients['aps-admin- | Скопы для oidc клиента, который используется для | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | console'].scope из hosts.yml | аутентификации в Консоли администратора | |
| config.oidcClients.apsAdminConsole. | returnUri | oidc_clients['aps-admin-console'].redirect_uris из hosts.yml | Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли администратора | 2.2.0 / - |
| config.database. | host | формируется из<br>- postgresql_patroni_cluster<br>- groups['postgresql_masters'] из hosts.yml<br>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster \| bool %}localhost{% else %}{{ groups['postgresql_masters'] \| first }}{% endif %} | Адрес (хост) БД | 2.2.0 / - |
| config.database. | port | postgresql.port | Порт БД | 2.2.0 / - |
| config.database. | dbname | postgresql.dbname | Имя БД | 2.2.0 / - |
| config.database. | user | postgresql.user | Имя пользователя БД | 2.2.0 / - |
| config.database. | password | postgresql.password | Пароль БД | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| config.consul. | token | consul_token | Токен для доступа к Consul | 2.5.0 / - |
| config.redis. | sentinelAddress | формируется из - groups['sentinel'] из hosts.yml groups['sentinel'] \| map('regex_replace', '^(.*)$', '\\1:26379') \| join(',') | Адрес модуля sentinel СУБД Redis | 2.2.0 / - |
| config.redis. | sentinelPassword | redis_password | Пароль к модулю sentinel СУБД Redis | 2.2.0 / - |
| config.redis. | masterName | redis_master_name | Идентификатор (имя) БД Redis | 2.2.0 / - |
| config.redis. | password | redis_password | Пароль к СУБД Redis | 2.2.0 / - |
| config.transport. | shutdownTime | transport_shutdown_time | Время на завершение открытых соединений перед тем, как сервис завершит работу | 2.3.0 / - |
| config.transport.nats. | url | формируется из - groups['nats_streaming_server'] из hosts.yml {% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}}@{{ host }}:4222{% if not loop.last | Адрес сервера NATS | 2.3.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | `%},{% endif %}{% endfor %}` | | |
| `config.transport.nats.` | `clusterID` | `nats.cluster_id` | Идентификатор кластера NATS (`https://docs.nats.io/`) | 2.3.0 / - |
| `config.transport.nats.` | `redeliveryCount` | - | Максимальное количество попыток обработать событие. По умолчанию количество попыток - 3. | 2.5.0 / - |
| `config.transport.http.tls.` | `enabled` | - | Флаг включения TLS протокола | 2.3.0 / - |
| `config.transport.http.tls.` | `private_key` | - | Путь к файлу с приватным ключом. При незаполненном значении формируется по принципу `config_folder/app_name/app_name.key` | 2.2.0 / - |
| `config.transport.http.tls.` | `certificate` | - | Путь к файлу с сертификатом (публичный ключ). При незаполненном значении формируется по принципу `config_folder/app_name/app_name.crt` | 2.2.0 / - |
| `config.transport.http.tls.` | `ca_certificate` | - | Путь к файлу с доверенным сертификатом. | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | | При незаполненном значении формируется по принципу `config_folder/ca.crt` | |
| `config.transport.httpDebug.tls.` | `enabled` | - | [не используется] Флаг включения TLS протокола (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| `config.transport.httpDebug.tls.` | `private_key` | - | [не используется] Путь к файлу с приватным ключом (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| `config.transport.httpDebug.tls.` | `certificate` | - | [не используется] Путь к файлу с сертификатом (публичный ключ) (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| `config.transport.httpDebug.tls.` | `ca_certificate` | - | [не используется] Путь к файлу с доверенным сертификатом (для служебных debug-эндпоинтов приложения) | 2.2.0 / - |
| `config.` | `insecureUri` | `insecure_uri` | Флаг использования незащищенного соединения. Этот | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | | параметр надо задавать в `true` если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов. | |
| `config.` | `gatewayTimeout` | `gateway_timeout` | Таймаут запросов при взаимодействии со шлюзами | 2.3.0 / - |
| `config.` | `clientTimeout` | `client_timeout` | Таймаут запросов при межсервисном взаимодействии | 2.3.0 / - |
| `config.logger.` | `level` | `logger_level` | Уровень детализации сообщений логирования. Возможные значения: – `debug` - Логирование отладочной информации. Включает сообщения уровней debug, info, warn, error; – `info` - Логирование информации о событиях, не приводящих к ошибкам. Включает сообщения уровней info, warn, error; | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| | | | – warn - Логирование информации о событиях, которые могут привести к ошибкам. Включает сообщения уровней warn, error;<br>– error - Логирование информации об ошибках. Включает сообщения уровня error | |
| config.logger. | caller | logger_caller | Флаг включения в сообщение лога названия функции и номера строки, в которой происходит логирование события | 2.2.0 / - |
| config.logger. | humanReadable | logger_human_readable | Флаг включения форматирования сообщений лога в обычный текст (не json) | 2.4.0 / - |
| config.tracing. | enabled | tracing_enabled | Флаг включения трассировки | 2.2.0 / - |
| config.tracing. | sample_rate | tracing_sample_rate | Частота дискретизации трассировки | 2.2.0 / - |
| config.tracing. | reporting_period | tracing_reporting_period | Отчетный период трассировки | 2.2.0 / - |
| config.tracing. | jaeger_agent_endpoint | - | Адрес подключения к Jaeger | 2.2.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| config.jaeger. | address | - | Адрес трейсера Jaeger (см. https://www.jaegertracing.io/docs/1.17/) | 2.2.0 / - |
| config. | enablePprof | enable_pprof | Флаг включения отладочного профилировщика | 2.2.0 / - |
| config.publishedReleaseRequiredFields. | changelog | - | Требуется ли заполнение поля «Что нового» для публикации второго и последующих релизов | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | description | - | Требуется ли заполнение поля «Описание приложения» для публикации релиза | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | icon | - | Требуется ли заполнение поля «Иконка» для публикации релиза | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | keywords | - | Требуется ли заполнение поля «Ключевые слова» для публикации релиза | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | minScreenshotCount | - | Количество скриншотов, требуемое для публикации релиза. 0 - не требуются. | 2.4.0 / - |
| config.publishedReleaseR | policyUrl | - | Требуется ли заполнение поля «URL | 2.4.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| equiredFields. | | | политики конфиденциальности» для публикации релиза | |
| config.publishedReleaseRequiredFields. | secondCategory | - | Требуется ли заполнение поля «Категория 2» для публикации релиза | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | supportEmail | - | Требуется ли заполнение поля «email поддержки» для публикации релиза | 2.4.0 / - |
| config.publishedReleaseRequiredFields. | webSiteUrl | - | Требуется ли заполнение поля «Сайт приложения» для публикации релиза | 2.4.0 / - |
| config. | secrets | - | Список секретов для механизма шифрования приватных ключей. Первый в списке - актуальный секрет. Остальные нужны для расшифровки зашифрованных данных (с последующим шифрованием с актуальным секретом) | 2.3.0 / - |
| config.smtp. | from | - | Почта и имя отправителя | 3.0.0 / - |

| Параметр в файлах: config.yml, config.jml.j2 | | Параметр в файле _vars.yml | Описание (* помечены поля, которые запрещено редактировать) | Добавлено /Удалено |
|---|---|---|---|---|
| config.smtp. | address | - | Адрес почтового сервера | 3.0.0 / - |
| config.smtp. | authType | - | Тип аутентификации | 3.0.0 / - |
| config.smtp. | host | - | Имя хоста для аутентификации | 3.0.0 / - |
| config.smtp. | username | - | Имя пользователя для аутентификации | 3.0.0 / - |
| config.smtp. | password | - | Пароль для аутентификации | 3.0.0 / - |
| config.smtp. | identity | - | identity для аутентификации обычно совпадает с username или пустая строка | 3.0.0 / - |
| config.smtp. | secret | - | Ключ для подписи сообщений с помощью md5 hmac | 3.0.0 / - |

### 8.3.4. Описание конфигурационных файлов ПУ (сценариев установки ПУ)

8.3.4.1. Описание параметров конфигурационного файла ПУ (/var/ocs/emm/config.yml), шаблона конфигурационного файла ПУ (config/subsystems/emm/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПУ _vars.yml (config/subsystems/emm/vars/_vars.yml) приведено в таблице (Таблица 29).

Таблица 29

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.insecureUri | insecure_uri | Использование незащищенного | 2.2.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| | | соединения. Этот параметр необходимо задавать в `true` если используется незащищенное соединение (http протокол). Он влияет на формирование Cookie заголовков, проверку редиректов. | |
| `config.publicUris.emm.mobileUri` | `emm_mobile_uri` | Полный адрес API для МП «Аврора Центр» | 2.2.0 / - |
| `config.publicUris.emm.adminBasepath` | `emm_admin_basepath` | Префикс административного API/UI ПУ | 2.2.0 / - |
| `config.publicUris.auth.publicUri` | `auth_public_uri` | Полный адрес публичного API сервера авторизации | 2.2.0 / - |
| `config.publicUris.auth.adminUri` | `auth_admin_uri` | Полный адрес административного API/UI сервера авторизации | 2.2.0 / - |
| `config.publicUris.aps.adminUri` | `aps_admin_uri` | Полный адрес административного API/UI ПМ | 2.2.0 / - |
| `config.systemUris.auth.publicAddress` | - | Хост публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия | 2.2.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.systemUris.auth.publicBasepath | - | Префикс публичного API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия | 2.2.0 / - |
| config.systemUris.auth.adminAddress | - | Хост админского API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.auth.adminBasepath | - | Префикс к админскому API сервера авторизации, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.aps.marketAddress | - | Хост API подсистемы «Маркет», используемый для внутреннего межподсистемного взаимодействия | 2.2.0 / - |
| config.systemUris.aps.marketBasepath | - | Префикс к API подсистемы «Маркет», используемый для внутреннего межподсистемного взаимодействия | 2.2.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.systemUris.pkgRepo.adminAddress | - | Хост административного API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.pkgRepo.adminBasepath | - | Префикс к административному API подсистемы обновлений, используемый для внутреннего межподсистемного взаимодействия | 2.2.1 / - |
| config.systemUris.push.adminAddress | - | Хост административного API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия | 2.3.0 / - |
| config.systemUris.push.adminBasepath | - | Префикс к административному API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия | 2.3.0 / - |
| config.systemUris.push.publicAddress | - | Хост публичного API подсистемы Push-уведомлений, используемый для внутреннего | 2.4.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| | | межподсистемного взаимодействия | |
| config.systemUris.push.publicBasepath | - | Префикс к публичному API подсистемы Push-уведомлений, используемый для внутреннего межподсистемного взаимодействия | 2.4.0 / - |
| config.redis.sentinelAddress | формируется из groups['sentinel'] из hosts.yml | Адрес модуля sentinel СУБД Redis | 2.2.0 / - |
| config.redis.sentinelPassword | redis_password | Пароль к модулю sentinel СУБД Redis | 2.2.0 / - |
| config.redis.masterName | - | Идентификатор (имя) БД Redis | 2.2.0 / - |
| config.redis.password | redis_password | Пароль к СУБД Redis | 2.2.0 / - |
| config.session.rememberFor | session_remember_for | Время жизни сессии | 2.2.0 / - |
| config.session.renewTimeout | session_renew_timeout | Интервал обновления сессий (при активности пользователя запросы на обновление сессии будут посылаться не на каждую активность, а один раз за данный интервал) | 2.2.0 / - |
| config.oidcClients.emmAdminConsole.scope | формируется из oidc_clients['emm-admin-console'].scope из hosts.yml | Скопы для oidc клиента, который используется для аутентификации в Консоли администратора ПУ | 2.2.1 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.oidcClients.emmAdminConsole.returnUri | oidc_clients['emm-admin-console'].returnUri из hosts.yml | Адрес, на который сервер авторизации сделает редирект после аутентификации в Консоли администратора ПУ | 2.2.1 / - |
| config.database.host | формируется из<br>- postgresql_patroni_cluster<br>- groups['postgresql_masters'] из hosts.yml<br>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster \| bool %}localhost{% else %}{{ groups['postgresql_masters'] \| first }}{% endif %} | Адрес (хост) БД ПУ | 2.2.0 / - |
| config.database.port | postgresql.port | Порт БД ПУ | 2.2.0 / - |
| config.database.user | postgresql.user | Имя пользователя БД ПУ | 2.2.0 / - |
| config.database.dbname | postgresql.dbname | Имя БД ПУ | 2.2.0 / - |
| config.database.password | postgresql.password | Пароль БД ПУ | 2.2.0 / - |
| config.consul.token | consul_token | Токен для доступа к Consul | 2.5.0 / - |
| config.transport.address | - | Порт, на котором запускается сервис (модуль) ПУ.<br>Пример: ":8080" | 2.2.0 / - |
| config.transport.tls.enabled | - | Доступность TLS протокола | 2.2.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.transport.shutDownTime | transport_shutdown_time | Время на завершение открытых соединений, перед перед тем, как сервис завершит работу | 2.2.0 / - |
| config.transport.nats.url | формируется из groups['nats_streaming_server'] из hosts.yml auth_token {% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}}@{{ host }}:4222{% if not loop.last %},{% endif %}{% endfor %} | Адрес сервера NATS | 2.2.0 / - |
| config.transport.nats.clusterID | - | Идентификатор кластера NATS | 2.2.0 / - |
| config.zipkin.address | | Адрес подключения к Zipkin | 2.1.1 / 2.2.1 |
| config.tracing.enabled | - | Доступность трейсера | 2.2.1 / - |
| config.tracing.sample_rate | - | Частота дискретизации трассировки | 2.2.1 / - |
| config.tracing.reporting_period | - | Отчетный период трассировки | 2.2.1 / - |
| config.tracing.jaeger_agent_endpoint | - | Адрес подключения к Jaeger | 2.2.1 / - |
| config.jaeger.address | - | Адрес подключения к Jaeger, см. https://www.jaegertracing.io/docs/1.17/ | 2.4.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| `config.enablePprof` | `enable_pprof` | Флаг включения pprof, используется для отладки кода | 2.4.0 / - |
| `config.logger.level` | `logger_level` | Уровень детализации сообщений логирования. Возможные значения:<br>– `debug` - Логирование отладочной информации. Включает сообщения уровней debug, info, warn, error;<br>– `info` - Логирование информации о событиях, не приводящих к ошибкам. Включает сообщения уровней info, warn, error;<br>– `warning` - Логирование информации о событиях, которые могут привести к ошибкам. Включает сообщения уровней warn, error;<br>– `error` – Логирование информации об ошибках. Включает сообщения уровня error | 2.2.0 / - |
| `config.logger.caller` | `logger_caller` | Признак включения в лог дополнительных полей (имя файла, название функции):<br>– `false`;<br>– `true` | 2.2.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.logger.gateway_gin_log_enabled | gateway_gin_log_enabled | Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа) | 2.2.1 / 2.4.0 |
| config.logger.humanReadable | logger_human_readable | Флаг управления редактированием логгера | 2.4.0 / - |
| config.smtp.from | - | Адрес эл. почты, с которой отправляются письма | 2.2.0 / - |
| config.smtp.address | - | Адрес сервера эл. почты | 2.2.0 / - |
| config.smtp.AuthType | - | Тип авторизации. Может принимать значения CRAM-MD5, PLAIN, LOGIN, либо не заполняться | 2.4.0 / - |
| config.smtp.Identity | - | Идентификатор учетной записи пользователя, обычно совпадает с Username<br>Заполняется для типа авторизации PLAIN | 2.4.0 / - |
| config.smtp.Username | - | Логин пользователя<br>Заполняется для типа авторизации PLAIN, CRAM-MD5, LOGIN | 2.4.0 / - |
| config.smtp.Password | - | Пароль пользователя<br>Заполняется для типа авторизации PLAIN, LOGIN | 2.4.0 / - |
| config.smtp.Host | - | Адрес (хост) почтового сервера.<br>Заполняется для типа авторизации PLAIN | 2.4.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.smtp.Secret | - | Ключ, с помощью которого подписываются hmac.md5 данные между сервером и клиентом.<br>Заполняется для типа авторизации CRAM-MD5 | 2.4.0 / - |
| config.smtp.tls | - | Доступность неявного TLS для SMTP при необходимости:<br>– true;<br>– false.<br>Значение зависит от конфигурации сервера | 2.4.0 / - |
| config.qrCodeTtl | - | Время жизни QR-кода | 2.2.0 / - |
| config.jobService.url | - | Внутренний адрес сервиса Jobs | 2.3.0 / - |
| config.ldapServer.address | ldap_server.address | Адрес LDAP сервера<br>пример: "ldap://msk1pdc.omp.ru" | 2.3.0 / - |
| config.ldapServer.userCN | ldap_server.user_cn | Логин от технической учетной записи от LDAP сервера | 2.3.0 / - |
| config.ldapServer.password | ldap_server.password | Пароль от технической учетной записи от LDAP сервера | 2.3.0 / - |
| config.ldapServer.parentGroup | ldap_server.parent_group | Название группы, с которой будет происходить импорт данных орг. структуры из LDAP сервера | 2.3.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| config.ldapServer.pageSize | ldap_server.page_size | Количество элементов, которое будет импортировано за одну итерацию. Максимальное значение: 1000 | 2.3.0 / - |
| - | project_name | Имя проекта | 2.2.1 / - |
| - | download_mode | Модуль для скачивания исходников | 2.2.1 / - |
| - | repository_dir | Директория для скачивания исходников | 2.2.1 / - |
| - | postgresql.extensions | Необходимые расширения для Postgres | 2.2.1 / - |
| - | postgres_password | Пароль для подключения к БД Postgres | 2.2.1 / - |
| - | nats.auth_token | Используется для формирования config.transport.nats.url | 2.2.1 / - |
| - | redis_password | Используется для формирования config.redis.sentinelPassword, config.redis.password | 2.2.1 / - |
| - | auth_public_address | Используется для:<br>– для генерации oidc клиентов;<br>– формирования переменных *_uri | 2.2.1 / - |
| | auth_admin_address | | 2.2.1 / - |
| | aps_admin_address | | 2.2.1 / - |
| | aps_market_address | | 2.2.1 / - |
| | emm_admin_address | | 2.2.1 / - |
| | emm_mobile_address | | 2.2.1 / - |
| | pkgrepo_admin_address | | 2.2.1 / - |
| | push_admin_address | | 2.3.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| | auth_public_basepath | | 2.2.1 / - |
| | auth_admin_basepath | | 2.2.1 / - |
| | emm_admin_basepath | | 2.2.1 / - |
| | emm_mobile_basepath | | 2.2.1 / - |
| | aps_admin_basepath | | 2.2.1 / - |
| | aps_market_basepath | | 2.2.1 / - |
| | pkgrepo_admin_basepath | | 2.2.1 / - |
| - | emm_admin_console_client_secret | Используется для генерации OIDC клиентов | 2.2.1 / - |
| - | same_site_mode | Определяет параметр sameSite для csrf-куки (допустимые значения: "strict","lax","none","") | 2.3.0 / 2.5.0 |
| - | krakendcsrf_enabled | Использование CSRF на гейтвеях, принимает значения:<br>– true;<br>– false | 2.3.0 / - |
| - | expose_internal_errors | Используется для управления внутренней ошибкой в ответах запросов к сервисам, принимает значения:<br>– true;<br>– false | 2.5.0 / - |
| aurora_mobility_management_client_secret | - | | 2.2.1 / - |
| emm_integration_account_client_secret | - | | 2.2.1 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| domain | http://ocs-appstore-admin-api-gw.{{ domain }}/api/categories | | 2.2.1 / - |
| pushNotificationSystem.enabled | Push_notification_system.enabled | Используется для удобного включения и отключения функции отправки настроек Push-уведомлений (на бэкэнде) | 2.4.0 / - |
| pushNotificationSystem.hostname | | IP-адрес или имя хоста сервиса Push-уведомлений | 2.4.0 / - |
| pushNotificationSystem.port | | Порт сервиса Push-уведомлений | 2.4.0 / - |
| pushNotificationSystem.applicationID | | Идентификатор приложения, с которым регистрируется МП в сервисе Push-уведомлений | 2.4.0 / - |
| pushNotificationSystem.mobileHostname | push_mobile_hostname | IP-адрес или имя хоста сервиса Push-уведомлений для МП | 2.4.0 / - |
| pushNotificationSystem.mobilePort | push_mobile_port | Порт сервиса Push-уведомлений для МП | 2.4.0 / - |
| pushNotificationSystem.messageTTL | Push_notification_system.messageTTL | Время жизни Push-уведомления | 2.4.0 / - |
| pushNotificationSystem.projectId | Push_notification_system.project_id | Идентификатор проекта для отправки Push-уведомлений | 2.4.0 / - |
| pushNotificationSystem.clientId | Push_notification_system.client_id | Идентификатор клиента технической учетной записи | 2.4.0 / - |

| Параметр файлах: config.yml, config.yml.j2 | Параметр в файле _vars.yml | Описание | Добавлено /Удалено |
|---|---|---|---|
| pushNotificationSystem.privateKey | Push_notification_system.private_key | Приватный ключ технической учетной записи | 2.4.0 / - |
| pushNotificationSystem.keyId | Push_notification_system.key_id | Приватный ключ технической учетной записи, указывает, какой ключ используется на сервисе авторизации | 2.4.0 / - |
| pushNotificationSystem.audience | Push_notification_system.audience | Audience в понятии OAuth2 https://tools.ietf.org/id/draft-tschofenig-oauth-audience-00.html | 2.4.0 / - |
| pushNotificationSystem.scopes | Push_notification_system.scopes | Скопы для oidc клиента, которые используются для аутентификации в ПУ | 2.4.0 / - |
| pushNotificationSystem.tokenURL | Push_notification_system.token_url | URL для получения токена авторизации | 2.4.0 / - |

### 8.3.5. Описание конфигурационных файлов ПООС (сценариев установки ПООС)

#### 8.3.5.1. Описание параметров конфигурационного файла ПООС (/var/ocs/pkgrepo/config.yml), шаблона конфигурационного файла ПООС (config/subsystems/pkgrepo/config/services/config.yml.j2) и конфигурационного файла сценариев установки ПООС _vars.yml (config/subsystems/pkgrepo/vars/_vars.yml) приведено в таблице (Таблица 30).

Таблица 30

| Параметр в общем конфигурационном файле config.yml.j2 | Параметр в конфигурационном файле vars.yml | Описание | Добавлено/ Удалено |
|---|---|---|---|
| config.publicUris.auth.publicUri | auth_public_uri | Полный адрес публичного API сервера авторизации | 2.2.0 / - |
| | | | 2.4.0 / - |
| | | | 2.4.0 / - |
| config.database.host | формируется из:<br>– postgresql_patroni_cluster;<br>– groups['postgresql_masters']<br><br>{% if postgresql_patroni_cluster is defined and postgresql_patroni_cluster \| bool %}localhost{% else %}{{ groups['postgresql_masters'] \| first }}{% endif %} | Адрес (хост) БД ПООС | 2.2.0 / - |
| config.database.port | postgresql.port | Порт БД ПООС | 2.2.0 / - |
| config.database.user | postgresql.user | Имя пользователя БД ПООС | 2.2.0 / - |
| config.database.dbname | postgresql.dbname | Имя БД ПООС | 2.2.0 / - |
| config.database.password | postgresql.password | Пароль БД ПООС | 2.2.0 / - |
| config.redis.sentinelAddress | формируется из groups['sentinel'] | Адрес модуля sentinel СУБД Redis | 2.2.0 / - |
| config.redis.sentinelPassword | redis_password | Пароль к модулю sentinel СУБД Redis | 2.2.0 / - |

| Параметр в общем конфигурационном файле config.yml.j2 | Параметр в конфигурационном файле vars.yml | Описание | Добавлено/ Удалено |
|---|---|---|---|
| config.redis.masterName | - | Идентификатор (имя) БД Redis | 2.2.0 / - |
| config.redis.password | redis_password | Пароль к СУБД Redis | 2.2.0 / - |
| config.transport.tls.enabled | - | Доступность TLS протокола | 2.2.0 / - |
| config.transport.shutDownTime | transport_shutdown_time | Время на завершение открытых соединений перед тем, как сервис завершит работу | 2.2.0 / - |
| config.transport.nats.url | формируется из:<br>– groups['nats_streaming_server']<br>– auth_token<br><br>{% for host in groups['nats_streaming_server'] %}nats://{{nats.auth_token}}@{{ host }}:4222 {% if not loop.last %}, {% endif %}{% endfor %} | Адрес сервера NATS | 2.2.0 / - |
| config.transport.nats.clusterID | - | Идентификатор кластера NATS | 2.2.0 / - |
| config.zipkin.address | - | Адрес подключения к Zipkin | 2.2.0 / 2.2.1 |
| config.tracing.enabled | - | Доступность трейсера | 2.2.1 / - |
| config.tracing.sample_rate | - | Частота дискретизации трассировки | 2.2.1 / - |
| config.tracing.reporting_period | - | Отчетный период трассировки | 2.2.1 / - |
| config.tracing.jaeger_agent_endpoint | - | Адрес подключения к Jaeger | 2.2.1 / - |

| Параметр в общем конфигурационном файле config.yml.j2 | Параметр в конфигурационном файле vars.yml | Описание | Добавлено/ Удалено |
|---|---|---|---|
| `config.jaeger.address` | - | Адрес подключения к Jaeger, см. `https://www.jaegertracing.io/docs/1.17/` | 2.4.0 / - |
| `config.enablePprof` | `enable_pprof` | Флаг включения pprof, используется для отладки кода | |
| `config.logger.level` | `logger_level` | Уровень детализации сообщений логирования. Возможные значения:<br>– `debug`;<br>– `info`;<br>– `warning`;<br>– `error` | 2.2.0 / - |
| `config.logger.caller` | - | Признак включения в лог дополнительных полей (имя файла, название функции)<br>– `false`;<br>– `true` | 2.2.0 / - |
| `config.logger.gateway_gin_log_enabled` | `gateway_gin_log_enabled` | Флаг включения логирования входящего запроса на шлюзе (url запроса и http-статус ответа) | 2.2.1 / - |
| `config.logger.humanReadable` | `logger_human_readable` | Флаг управления редактированием логгера | 2.4.0 / - |
| - | `project_name` | Имя проекта | 2.2.0 / - |
| - | `download_mode` | Режим загрузки. Доступные типы:<br>– `` `http` ``: загружать артефакты из внешнего HTTP-хранилища | 2.2.0 / - |

| Параметр в общем конфигурационном файле config.yml.j2 | Параметр в конфигурационном файле vars.yml | Описание | Добавлено/ Удалено |
|---|---|---|---|
| | | напрямую на управляемый узел;<br>– `httplocal`: загрузить артефакты из внешнего http-хранилища на управляющий узел, затем скопировать на управляемый узел;<br>– `local`: не загружать артефакты из внешнего http-хранилища, они должны каким-то образом существовать на контрольном узле, копировать локальные артефакты с контрольного узла на управляемый узел | |
| – | repository_dir | Путь к локальному хранилищу артефактов кэша | 2.2.0 / - |
| – | postgresql.extensions | Необходимые расширения | 2.2.0 / - |
| – | postgres_password | Пароль от postgres | 2.2.0 / - |
| – | nats.auth_token | Используется для формирования config.transport.nats.url | 2.2.0 / - |
| – | redis_password | Используется для формирования: config.redis.sentinelPassword, config.redis.password | 2.2.0 / - |
| – | auth_public_address | Используется для: | 2.2.0 / - |

| Параметр в общем конфигурационном файле config.yml.j2 | Параметр в конфигурационном файле vars.yml | Описание | Добавлено/ Удалено |
|---|---|---|---|
| | auth_admin_address | – для генерации oidc клиентов;<br>– формирования переменных *_uri | 2.2.0 / - |
| | auth_public_basepath | | 2.2.0 / - |
| | auth_admin_basepath | | 2.2.0 / - |
| | pkgrepo_mobile_address | | 2.2.0 / - |
| | pkgrepo_mobile_basepath | | 2.2.0 / - |
| - | updateServers.address | Адрес обращения МУ к репозиторию с обновлением ОС | 2.5.0 / - |
| | retrieveReleasesPeriod | Период времени для перечитывания метафайла релизов | 2.2.0 / - |
| - | pkgrepo_integration_account_client_secret | Используется для генерации OIDC клиентов | 2.2.0 / - |
| - | pkgrepo_mobile_uri | Полный адрес репозитория с обновлениями ОС для МУ | 2.2.0 / - |
| | | | 2.4.0 / - |
| | | | 2.4.0 / - |
| - | auth_admin_uri | Полный адрес адинского API/UI сервера авторизации | 2.2.0 / - |
| | | | 2.4.0 / - |
| | | | 2.4.0 / - |

# ПЕРЕЧЕНЬ ТЕРМИНОВ И СОКРАЩЕНИЙ

Используемые в настоящем документе термины и сокращения приведены в таблице (Таблица 31).

Таблица 31

| Термин/ Сокращение | Расшифровка |
|---|---|
| БД | База данных |
| Воркер | Потоки, принадлежащие браузеру, которые можно использовать для выполнения JS-кода без блокировки цикла события |
| ГИС | Государственная информационная система |
| ИС | Информационные системы |
| Механизм CORS | Механизм CORS (Cross-origin resource sharing) – технология современных браузеров, которая позволяет предоставить веб-странице доступ к ресурсам другого домена |
| МП | Мобильное приложение |
| МУ | Мобильное устройство |
| ОС | Операционная система |
| ОТК | Отдел технического контроля |
| ПБ | Подсистема безопасности |
| ПМ | Подсистема «Маркет» |
| ПООС | Подсистема обновления ОС |
| ППО | Прикладное программное обеспечение «Аврора Центр» |
| Предприятие-изготовитель | Общество с ограниченной ответственностью «Открытая мобильная платформа» (ООО «Открытая мобильная платформа») |
| ПУ | Подсистема Платформа управления |
| ПЭВМ | Персональная электронно-вычислительная машина |
| СЗИ | Средство защиты информации |
| СЗИ НСД | Средство защиты информации от несанкционированного доступа |
| СПО | Специальное программное обеспечение |
| СУА | Сервис уведомлений Аврора |
| СУБД | Система управления базами данных |

| Термин/ Сокращение | Расшифровка |
|---|---|
| Субъект доступа | Лицо или процесс, действия которого регламентируются правилами разграничения доступа.<br>Субъектами доступа являются пользователи и МП «Аврора Центр» (процесс МП «Аврора Центр») ППО. Субъекту доступа может быть назначена одна или несколько из следующих перечисленных ролей:<br>– МП «Аврора Центр» – роль назначается учетным записям МП «Аврора Центр» (сервис/процесс без участия пользователей, который управляет МУ);<br>– Администратор учетных записей – роль позволяет осуществлять управление учетными записями;<br>– Оператор аудита – роль позволяет осуществлять действия по работе с журналом регистрации событий ППО;<br>– Администратор Аврора Маркет – роль позволяет осуществлять все действия по управлению ПМ через интерфейс системы;<br>– Разработчик – роль позволяет осуществлять добавление новых и обновление ранее загруженных приложений в ПМ, а также получать информацию о приложениях;<br>- Редактор приложений - роль позволяет осуществлять обновление любых ранее загруженных приложений в ПМ, а также получать о них информацию;<br>– Пользователь Аврора Маркет – роль позволяет осуществлять загрузку приложений из ПМ, а также получать информацию о приложениях;<br>– Администратор Платформы Управления – роль позволяет осуществлять все действия по управлению ПУ через интерфейс ППО |
| Токен (маркер) | Токен - аутентификационные данные, которые выдаются пользователю после успешной авторизации и являются ключом для доступа к службам |

| Термин/ Сокращение | Расшифровка |
|---|---|
| API | Application Programming Interface – описание способов (набор классов, процедур, функций, структур или констант), которыми одна компьютерная программа может взаимодействовать с другой программой |
| Cookie | Небольшой фрагмент данных, отправленный веб-сервером и хранимый на ПЭВМ пользователя. Веб-клиент (обычно веб-браузер) всякий раз при попытке открыть страницу соответствующего сайта пересылает этот фрагмент данных веб-серверу в составе HTTP-запроса |
| CSS3 | Cascading Style Sheets 3 – спецификация CSS. Представляет собой формальный язык, реализованный с помощью языка разметки |
| ECMAScript 5 | Встраиваемый расширяемый не имеющий средств ввода-вывода язык программирования, используемый в качестве основы для построения других скриптовых языков |
| HEALTH-запрос | Запрос проверки доступности API |
| HTML5 | HyperText Markup Language, version 5 – язык для структурирования и представления содержимого веб-страницы |
| HTTP | HyperText Transfer Protocol – протокол прикладного уровня передачи данных. Основой HTTP является технология «клиент-сервер», то есть предполагается существование потребителей (клиентов), которые инициируют соединение и посылают запрос, и поставщиков (серверов), ожидают соединения для получения запроса, производят необходимые действия и возвращают обратно сообщение с результатом |
| HTTPS | Hypertext Transfer Protocol Secure - расширение протокола HTTP для поддержки шифрования в целях повышения безопасности. Данные в протоколе HTTPS передаются поверх криптографических протоколов SSL или TLS |
| IMEI | International Mobile Equipment Identity – уникальный номер мобильного устройства, состоящий из 15 цифр |
| JSON | JavaScript Object Notation – текстовый формат обмена данными, основанный на JavaScript |

| Термин/ Сокращение | Расшифровка |
|---|---|
| MAC | Media Access Control – уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей |
| OIDC | OpenID Connect – уровень аутентификации OAuth 2.0, инфраструктуры авторизации. Контролируется OpenID Foundation |
| QR-код | Quick Response Code – код быстрого реагирования, предоставляющий информацию для быстрого ее распознавания с помощью камеры на мобильном устройстве |
| SSH | Secure SHell – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов) |
| TLS | Transport Layer Security – криптографический протокол, обеспечивающий защищенную передачу данных между узлами в сети Интернет |
| URL | Uniform Resource Locator – единообразный локатор (определитель местонахождения) ресурса |

# ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

| № версии документа | Содержание изменения | ФИО инициатора | Дата |
|---|---|---|---|
| 1.0 | Начальная версия | Иванова Н. | 07.07.2021 г. |
| 1.1 | Внесено уточнение | Иванова Н. | 03.08.2021 г. |
| 1.2 | Внесено уточнения | Адронова К. | 26.08.2021 |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |