

Система управления базами данных Arenadata™ Prosperity

Описание функциональных характеристик

ООО «Аренадата Софтвр», г. Москва, 2025 г.

Система управления базами данных Arenadata™ Prosperity

Описание функциональных характеристик ООО «Аренадата Софтвер», г. Москва, 2025 г.

Руководство может быть полезно администраторам, программистам, разработчикам и сотрудникам подразделений информационных технологий, осуществляющих внедрение и сопровождение кластеров Arenadata.

Контактная информация службы поддержки:

E-mail: info@arenadata.io

Оглавление

1. Требования к инфраструктуре.....	4
1.1. Требования к аппаратному обеспечению.....	4
1.2. Требования к программному обеспечению.....	4
1.3. Требования к уровню подготовки обслуживающего персонала.....	4
1.4. Конфигурация SELinux.....	4
2. Конфигурационные параметры.....	5
3. Подключение к СУБД ADP.....	6
3.1. Подключение к СУБД ADP.....	6
3.2. Подключение к СУБД ADP Advanced.....	7

1. ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ

1.1. Требования к аппаратному обеспечению

Требования к аппаратному обеспечению для установки Система управления базами данных Arenadata Prosperity (далее - ADP) должны определяться исходя из прикладных задач. Серверы, на которые будет выполняться установка ADP, должны удовлетворять следующим минимальным требованиям к аппаратному обеспечению:

- размер оперативной памяти не менее 4 ГБ;
- свободное место на диске не менее 60 ГБ;
- количество ядер - 2.

1.2. Требования к программному обеспечению

На серверах ADP должна быть установлена одна из следующих операционных систем:

- РЕД ОС версий 7.3.4 и 8;
- Astra Linux версии 1.7.5-16 (релиз Astra Linux 1.7.5 UU1);
- Debian версии 11.

1.3. Требования к уровню подготовки обслуживающего персонала

Администратор ADP должен обладать знаниями в следующих предметных областях и программных продуктах:

- администрирование РЕД ОС версий 7.3.4 и 8;
- администрирование Astra Linux версии 1.7.5-16 (релиз Astra Linux 1.7.5 UU1);
- администрирование Debian версии 11;
- базовые знания предметной области.

1.4. Конфигурация SELinux

При использовании РЕД ОС на всех серверах SELinux должен находиться в состоянии **permissive** («разрешенный»).

Для перевода SELinux в состояние **permissive** на РЕД ОС необходимо:

1. Выполнить команду:

```
[ec2-user@proxima-install ~]$ sudo sed -i  
's/SELINUX=enforcing/SELINUX=permissive/g' /etc/selinux/config
```

2. Перезагрузить VM.
3. Проверить статус SELinux с помощью команды:

```
[ec2-user@proxima-install ~]$ getenforce
Permissive
```

2. КОНФИГУРАЦИОННЫЕ ПАРАМЕТРЫ

В данном разделе приведено описание параметров, которые задаются пользователем в диалоговом режиме в процессе инсталляции СУБД ADP.

Табл. 1. Список параметров

Параметр	Описание	Значение по умолчанию
chosen_distr_0_type_0_name	Тип устанавливаемой конфигурации ADP	трехузловая (3_nodes)
chosen_distr_0_type_0_host_0_name, chosen_distr_0_type_0_host_1_name, chosen_distr_0_type_0_host_2_name	Имена серверов (или сервера), на которые (который) будет выполняться установка	db01, db02, db03 в случае Core-редакции / proxima-mgr и proxima-mon в случае Advanced-редакции
chosen_distr_0_type_0_replica_type_0_name	Тип репликации данных в кластере	смешанный (mix)
chosen_distr_0_type_0_replica_virtual_ip	Кластерный виртуальный адрес (который будет перемещаться между узлами кластера)	10.0.0.10
chosen_distr_0_type_0_replica_network	Разрешенная сеть для репликации узлов кластера	10.0.0.0/24
chosen_distr_0_type_0_replica_interface	Сетевой интерфейс, на котором будет поднят кластерный виртуальный адрес	eth0
chosen_distr_0_type_0_security_postgres_password	Пароль для пользователя postgres	CHANGE ME!
chosen_automation_user	Учетная запись, под которой выполняются все процессы автоматизации и которая включена в группу sudo	ec2-user

Параметр	Описание	Значение по умолчанию
chosen_automation_password	Пароль для учетной записи автоматизации	CHANGE ME!

3. ПОДКЛЮЧЕНИЕ К СУБД ADP

3.1. Подключение к СУБД ADP

После завершения установки для подключения к СУБД ADP можно использовать любой из следующих возможных вариантов подключения:

- Для трехузлового кластера:
 - подключение **без пулера** соединений и **без балансировки** запросов на чтение: **Virtual_IP: 5432**;
 - подключение **без пулера** соединений и **с балансировкой** запросов на чтение: **Virtual_IP: 5433**;
 - подключение **через пулер** соединений Odyssey и **без балансировки** запросов на чтение: **Virtual_IP: 7432**;
 - подключение **через пулер** соединений Odyssey и **с балансировкой** запросов на чтение: **Virtual_IP: 7433**;
- Для двухузлового кластера с арбитром:
 - подключение без пулера соединений: **Virtual_IP: 5432**;
 - подключение через пулер соединений Odyssey: **Virtual_IP: 7432**;
- Для двухузловой мастер-реплики:
 - подключение **без пулера** соединений: **Virtual_IP: 5432**;
 - подключение **через пулер** соединений Odyssey: **Virtual_IP: 7432**;
- Для одноузловой конфигурации:
 - подключение **без пулера** соединений: **5432**.
 - подключение **через пулер** соединений Odyssey: **7432**.

В ADP реализованы следующие настройки безопасности, влияющие на подключение к СУБД:

- режим доступа **trust** отключен, доступ к СУБД возможен только после аутентификации по логину и паролю;
- заблокирован доступ пользователя **postgres** через пулер соединений (если необходим доступ через пулер соединений для пользователя с ролью **superuser**, то необходимо создать пользователя с нужной ролью для требуемой цели).

Пример 1. Пример подключения напрямую к СУБД под пользователем **postgres**

```
psql -U postgres -h 10.0.0.1 -p 5432
```

Пример 2. Пример подключения к СУБД через пулер соединений под пользователем **someuser** (доступ для пользователя **postgres** через пулер соединений ограничен)

```
psql -U someuser -h proxima-db.local -p 7432
```

3.2. Подключение к СУБД ADP Advanced

В случае успешной установки ADP Advanced доступ к веб-интерфейсу осуществляется по адресу: <http://proxima-mng/>.

Наименование *proxima-mng* приведено для примера, вместо него необходимо ввести имя выделенного узла управления, указанное в `/etc/hosts`.

Для подключения используются заданные по умолчанию логин и пароль (пароль при первом подключении должен быть изменен на безопасный): `proxima-admin`, `password`.