Arenadata™ Database

Версия - archive_5.24.0-arenadata6

Интеграция кластера ADB и LDAP

2021 Arenadata™

Оглавление

1 Общий принцип авторизации пользователей в СУБД ADB с использованием LDAP-сервера 3

2 Настройка интеграции ADB и LDAP 4

В документе приведен общий принцип авторизации пользователей в СУБД Arenadata DB с использованием LDAP-сервера и настройка интеграции ADB и LDAP. Документ может быть полезен администраторам, программистам, разработчикам и сотрудникам подразделений информационных технологий и информационной безопасности, осуществляющих внедрение кластера.

Important: Контактная информация службы поддержки – e-mail: info@arenadata.io

Глава 1

Общий принцип авторизации пользователей в СУБД ADB с использованием LDAP-сервера

Общий принцип авторизации пользователей в СУБД **Arenadata DB** (**ADB**) с использованием LDAP-сервера реализуется в три этапа:

1. Выбирается необходимое множество пользователей LDAP, которым следует обеспечить доступ в СУБД;
2. Выбранные пользователи создаются в СУБД вручную или с помощью скрипта, при необходимости их также добавляют в отдельную группу;
3. Вносится информация о связи пользователей в СУБД с пользователями LDAP в файле настройки доступа *pg_hba.conf*.

В дальнейшем при обращении к СУБД с использованием имени пользователя, требующего синхронизации, кластер **ADB** проверяет валидность пользователя с помощью LDAP-сервера.

Глава 2

Настройка интеграции ADB и LDAP

Для настройки авторизации пользователей **ADB** через LDAP необходимо выполнить следующие действия:

1. Убедиться, что известны необходимые данные для настройки:

- хост и порт LDAP-сервера (в примере используется хост *ldap_host*, порт *389*);
- формат DN LDAP-сервера (в примере используется *OU=Regions,DC=org_name,DC=local*);
- имя пользователя и пароль для входа в LDAP-сервер (в примере используется имя пользователя *ldap_sys_user*, пароль *ldap_sys_passwd*);
- список пользователей для синхронизации;
- поле записи в LDAP, отвечающее за связь пользователя в LDAP и в СУБД (обычно *sAMAccountName*).

2. Установить на сервер-мастер пакет openldap-clients:

```
yum install openldap-clients -y
```

3. Выполнить пробный поиск на сервере LDAP с сервера-мастера ADB. Пример:

```
ldapsearch -D "CN= ldap_sys_user,OU=System Accounts,DC=org_name,DC=local" -b "OU=Regions,DC= org_
↪name,DC=local" -h ldap_host -w ldap_sys_passwd "sAMAccountName=H.Simpson"
```

Убедиться, что поиск для выбранных пользователей завершается успешно.

4. Создать пользователей в СУБД и при необходимости добавить их в группу. Пример:

- создание группы:

```
adb=# create role ldap_users;
```

- создание пользователя:

```
adb=# create role "H.Simpson" login;
```

- включение пользователя в группу:

```
adb=# grant ldap_users to "H.Simpson";
```

5. Связать группу пользователей в ADB с LDAP-сервером, внеся изменение в файл pg_hba.conf на мастер-сервере ADB. Пример:

```
host   all  +ldap_users   0.0.0.0/0   ldap ldapserver=ldap_host ldapbasedn="OU=Regions,DC= org_
↪name,DC=local" ldapbinddn="CN=ldap_sys_user,OU=System Accounts,DC=org_name,DC=local"␣
↪ldapbindpasswd="ldap_sys_passwd" ldapsearchattribute="sAMAccountName"
```

6. Зафиксировать изменения в СУБД:

```
gpstop -u
```

7. Проверить подключение к СУБД.

Для проверки можно воспользоваться утилитой **psql**, однако подключение должно выполняться с хоста, отличного от мастера СУБД (любой из сегментов или других серверов):

```
[root@sdw1 ~]# psql -h mdw -U "H.Simpson"
Password for user H.Simpson:
< enter H.Simpson domain password >
```