

REVOKE

Версии сервера

Firebird v0.9 Firebird v1.0 Firebird v1.5 Firebird v2.0

Формат

```
REVOKE {
  [GRANT OPTION FOR] <privileges>
  ON [TABLE] {tablename | viewname}
  FROM { <object_list>
    | <user_list>
    | GROUP Unix_group}
  | EXECUTE ON PROCEDURE procname
  FROM { <object_list>
    | <user_list>
    | GROUP Unix_group}
    | [ADMIN OPTION FOR] <role_grantee_list> FROM {PUBLIC |
  <role_grantee_list>}
} [{GRANTED BY | AS} [USER] grantor]
| ALL ON ALL FROM <user_list>;

<privileges> ::= ALL [PRIVILEGES] | <privilege_list>

<privilege_list> ::= {
SELECT
| DELETE
| INSERT
| UPDATE [(col [,col ...])]
| REFERENCES [(col [,col ...])]
} [, <privilege_list> ...]

<object_list> ::= {
PROCEDURE procname
| TRIGGER triname
| VIEW viewname
| PUBLIC
} [, <object_list> ...]

<user_list> ::= {
[USER] username
```

```
| [ROLE] rolename
| Unix_user
} [, <user_list> ...]
```

```
<role_granted> ::= rolename [, rolename ...]
```

```
<role_grantee_list> ::= [USER] username [, [USER] username ...]
```

Аргумент	Описание
tablename	Имя таблицы, у которой должна быть отозвана привилегия.
viewname	Имя представления, у которого должна быть отозвана привилегия.
procname	Имя хранимой процедуры, для которой должна быть отозвана привилегия EXECUTE или у которой должны быть отозваны привилегии.
trigname	Имя триггера.
col	Столбец таблицы, у которого должна быть отозвана привилегия.
username	Имя пользователя, у которого отзываются привилегии или у которого отнимается роль.
rolename	Имя роли.
Unix_group	Имя группы пользователей в операционных системах семейства UNIX.
grantor	Пользователь от имени, которого отзываются привилегии.

Описание

Оператор REVOKE отменяет привилегии для пользователей, ролей, хранимых процедур, триггеров и представлений выданные оператором GRANT.

У таблиц можно отобразить следующие привилегии:

Привилегия	Описание
ALL	Объединяет привилегии SELECT, INSERT, UPDATE, DELETE и REFERENCES. Отменяет сразу все привилегии для таблицы или представления
SELECT	Отменяет привилегию на чтение из таблицы или представления
DELETE	Отменяет привилегии на удаление записи из таблицы или представления
INSERT	Отменяет привилегию на добавление записи в таблицу или представление
UPDATE	Отменяет привилегию на изменение записи в таблице или представлении
REFERENCES	Отменяет возможность ссылаться на указанные столбцы внешним ключом

У хранимых процедур можно отобразить привилегию EXECUTE. Она позволяет выполнять хранимые процедуры и делать выборку данных из процедур выбора (с помощью оператора SELECT).

В предложении FROM указывается список пользователей, ролей и объектов базы данных (процедур, триггеров и представлений) у которых будут отняты перечисленные привилегии. Необязательные предложения USER и ROLE позволяют уточнить, у кого именно выдается привилегия. Если ключевое слово USER или ROLE не указано, то сервер проверяет, существует ли роль с данным именем, если таковой не существует, то привилегии отбираются у пользователя. Если привилегия отбирается у объекта базы данных, то необходимо обязательно указывать тип объекта.

Только пользователь, который назначил привилегию, может удалить ее. Если привилегии были назначены специальному пользователю PUBLIC, то отменять привилегии необходимо для пользователя PUBLIC. Специальный пользователь PUBLIC используется, когда необходимо предоставить привилегии сразу всем пользователям. Однако не следует рассматривать PUBLIC как группу пользователей.

Необязательное предложение GRANT OPTION FOR отменяет для соответствующего пользователя или роли право предоставления другим пользователям или ролям привилегии к таблицам, представлениям, триггерам, хранимым процедурам.

Другое назначение оператора REVOKE в отборе назначенных группе пользователей ролей оператором GRANT. В этом случае после предложения REVOKE следует список ролей, которые будут отозваны у списка пользователей, указанных после предложения FROM.

Необязательное предложение ADMIN OPTION FOR отменяет ранее предоставленную административную опцию (право на передачу предоставленной пользователю роли другим) из грантополучателей, не отменяя прав на роль. В одном операторе могут быть обработаны несколько ролей и/или грантополучателей.

При предоставлении прав в базе данных в качестве лица, предоставившего эти права, обычно записывается текущий пользователь. Используя предложение GRANTED BY можно предоставлять права от имени другого пользователя. При использовании оператора REVOKE после GRANTED BY права будут удалены только в том случае, если они были зарегистрированы от удаляющего пользователя. Для облегчения миграции из некоторых других реляционных СУБД нестандартное предложение AS поддерживается как синоним оператора GRANTED BY.

Предложение GRANTED BY может использовать:

- Владелец базы данных;
- SYSDBA;
- Любой пользователь, имеющий права на роль RDB\$ADMIN и указавший ее при соединении с базой данных;
- При использовании флага AUTO ADMIN MAPPING - любой администратор операционной системы Windows (при условии использования сервером доверенной авторизации - trusted authentication), даже без указания роли.

Даже владелец роли не может использовать GRANTED BY, если он не находится в вышеупомянутом списке.

Если после ключевого слова REVOKE указано предложение ALL ON ALL, то это позволяет отменить все привилегии (включая роли) на всех объектах от одного или более пользователей и/или ролей. Это - быстрый способ «очистить» (отобрать) права, когда пользователю должен быть заблокирован доступ к базе данных. *Примечания:*

- Когда оператор REVOKE ALL ON ALL вызывается привилегированным пользователем (владельцем базы данных, SYSDBA или любым пользователем, у которого CURRENT_ROLE - RDB\$ADMIN), удаляются все права независимо от того, кто их предоставил. В противном случае удаляются только права, предоставленные текущим пользователем;
- Не поддерживается предложение GRANTED BY;
- Этот оператор не удаляет флаг пользователя, давшего права на хранимые процедуры, триггеры или представления (права на такие объекты конечно удаляются).

Пример

Следующая инструкция отнимает привилегию SELECT на таблицу от пользователя:

```
REVOKE SELECT ON COUNTRY FROM MIREILLE;
```

Следующая инструкция забирает привилегию EXECUTE на процедуру от другой процедуры и пользователя:

```
REVOKE EXECUTE ON PROCEDURE GET_EMP_PROJ
```

См. также

[GRANT](#), [CREATE ROLE](#), [DROP ROLE](#)

Источник

langref.pdf

From:

<http://firebirdsql.su/> - Словарик по FireBird

Permanent link:

<http://firebirdsql.su/doku.php?id=revoke>

Last update: **2014/12/27 07:42**

