睿创神脑
RUICHUANGSHENNAO

PolarDB
PostgreSQL

PostgreSQL 对象权限管理

睿创神脑
RUICHUANGSHENNAO

PolarDB PostgreSQL

Objectives

- PostgreSQL对象权限概述
- PostgreSQL对象权限授权与回收

睿创神脑
RUICHUANGSHENNAO

对象权限概述

PolarDB PostgreSQL

- 每个数据库对象都有一个所有者，默认情况下，所有者拥有该对象的所有权限
- 在数据库中所有的权限都和角色挂钩
- 对超级用户postgres不做权限检查，其它用户走ACL(Access ControL List)
- 对于数据库对象，开始只有所有者和超级用户可以做任何操作，其它走ACL

睿创神脑
RUICHUANGSHENNAO

对象权限概述

PolarDB PostgreSQL

- 对象级别的权限
  - 表级对象权限控制
  - 列级别权限控制
  - 序列权限控制
  - 类型域的权限控制(域简单来说就是自定义的带约束的数据类型)
  - FDW权限控制
  - FS权限控制
  - 函数权限控制
  - \h GRANT显示所有可设置的访问权限

睿创神脑
RUICHUANGSHENNAO

对象权限概述

PolarDB PostgreSQL

- 对象权限列表

```
rolename=xxxx -- privileges granted to a role
        =xxxx -- privileges granted to PUBLIC
            r -- SELECT ("read")
            w -- UPDATE ("write")
            a -- INSERT ("append")
            d -- DELETE
            D -- TRUNCATE
            x -- REFERENCES
            t -- TRIGGER
            X -- EXECUTE
            U -- USAGE
            C -- CREATE
            c -- CONNECT
            T -- TEMPORARY
       arwdDxt -- ALL PRIVILEGES (for tables, varies for other objects)
            * -- grant option for preceding privilege
      /yyyy -- role that granted this privilege
```

睿创神脑
RUICHUANGSHENNAO

对象权限概述

PolarDB PostgreSQL

- 对象权限含义
  - SELECT：允许从指定表，视图或序列的任何列或列出的特定列进行SELECT。也允许使用COPY TO。在UPDATE或DELETE中引用现有列值也需要此权限。对于序列，此权限还允许使用currval函数。对于大对象，此权限允许读取对象。
  - INSERT：允许将新行INSERT到指定的表中。如果列出了特定列，则只能在INSERT命令中为这些列分配（因此其他列将接收默认值）。也允许COPY FROM。
  - UPDATE：允许更新指定表的任何列或列出的特定列，需要SELECT权限。
  - DELETE：允许删除指定表中的行，需要SELECT权限。
  - TRUNCATE：允许在指定的表上截断数据。
  - REFERENCES：允许创建引用指定表或表的指定列的外键约束。
  - TRIGGER：允许在指定的表上创建触发器。
  - CREATE：对于数据库，允许在数据库中创建新的schema、table、index。
  - CONNECT：允许用户连接到指定的数据库。在连接启动时检查此权限。
  - TEMPORARY、TEMP：允许在使用指定数据库时创建临时表。
  - EXECUTE：允许使用指定的函数或过程以及在函数。
  - USAGE：对于schema，允许访问指定模式中包含的对象；对于sequence，允许使用currval和nextval函数。对于类型和域，允许在创建表，函数和其他模式对象时使用类型或域。
  - ALL PRIVILEGES：一次授予所有可用权限。

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 对象权限授权
  - 每种类型的对象权限都不一样，详细可参考：

    https://www.postgresql.org/docs/9.6/static/sql-grant.html

  - 基本语法参考（表对象）：

```
GRANT { { SELECT | INSERT | UPDATE | DELETE | TRUNCATE | REFERENCES | TRIGGER }
[, ...] | ALL [ PRIVILEGES ] }
ON { [ TABLE ] table_name [, ...]
     | ALL TABLES IN SCHEMA schema_name [, ...] }
TO role_specification [, ...] [ WITH GRANT OPTION ]
```

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 授权示例

--授权单个权限给用户

```
GRANT SELECT  ON tab_name TO role_name;
```

--授权多个/所有权限给用户

```
GRANT SELECT, UPDATE, INSERT ON tab_name TO role_name;
GRANT ALL ON tab_name TO role_name;
```

--授权某模式下所有表的查询权限给用户

```
GRANT SELECT ON ALL TABLES IN SCHEMA schema_name TO role_name;
```

--授权列权限给用户

```
GRANT SELECT (col1), UPDATE (col1) ON  tab_name TO role_name;
```

--授权所有权限给所有用户

```
GRANT ALL ON tab_name TO public;
```

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 查看对象权限
  - 查看对象权限数据字典表

    information_schema.table_privileges
  - 显示对象的访问权限列表

    \z或\dp [tablename]

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 查看对象权限示例
  - 查看对象权限数据字典表

```
select grantor,grantee,privilege_type,is_grantable
from information_schema.table_privileges
where table_name='t1';
```

testdb

table_name	grantor	grantee	privilege_type	is_grantable
t1	postgres	PUBLIC	INSERT	NO
t1	postgres	PUBLIC	SELECT	NO
t1	postgres	PUBLIC	UPDATE	NO
t1	postgres	PUBLIC	DELETE	NO
t1	postgres	PUBLIC	TRUNCATE	NO
t1	postgres	PUBLIC	REFERENCES	NO
t1	postgres	PUBLIC	TRIGGER	NO

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 查看对象权限示例
  - 显示对象的访问权限列表

\z或\dp [tablename]

```
                                 Access privileges
 Schema | Name | Type  |     Access privileges     | Column privileges | Policies
--------+------+-------+---------------------------+-------------------+----------
 public | t1   | table | postgres=arwdDxt/postgres+|                   |
        |      |       | =arwdDxt/postgres         |                   |
(1 row)
```

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 回收示例

--回收单个权限

```
REVOKE SELECT  ON tab_name FROM role_name;
```

--回收多个/所有权限

```
REVOKE SELECT, UPDATE, INSERT ON tab_name FROM role_name;
REVOKE  ALL ON tab_name FROM role_name;
```

--回收某模式下所有表的查询权限

```
REVOKE  SELECT ON ALL TABLES IN SCHEMA schema_name FROM role_name;
```

--回收列权限

```
REVOKE  SELECT (col1), UPDATE (col1) ON  tab_name FROM role_name;
```

--回收所有权限

```
REVOKE  ALL ON tab_name FROM public;
```

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 回收示例（特例）

  - 任何用户对public模式都有all的权限，为了安全可以禁止用户在指定数据库下对public 模式的create权限。

```
REVOKE CREATE ON  SCHEMA public FROM public;
```

  - 属主可以取消自己在指定表上的某些权限

```
REVOKE UPDAE ON tab_name FROM role_name;

REVOKE ALL ON tab_name FROM role_name;
```

  - 属主可以授权自己在指定表上的某些权限

```
GRANT ALL ON tab_name TO role_name;
```

睿创神脑
RUICHUANGSHENNAO

对象权限管理

PolarDB PostgreSQL

- 赋予角色默认权限

```
Command:     ALTER DEFAULT PRIVILEGES
Description: define default access privileges
Syntax:
ALTER DEFAULT PRIVILEGES
    [ FOR { ROLE | USER } target_role [, ...] ]
    [ IN SCHEMA schema_name [, ...] ]
    abbreviated_grant_or_revoke
```

```
where abbreviated_grant_or_revoke is one of:

GRANT { { SELECT | INSERT | UPDATE | DELETE | TRUNCATE | REFERENCES | TRIGGER }
    [, ...] | ALL [ PRIVILEGES ] }
    ON TABLES
    TO { [ GROUP ] role_name | PUBLIC } [, ...] [ WITH GRANT OPTION ]

GRANT { { USAGE | SELECT | UPDATE }
    [, ...] | ALL [ PRIVILEGES ] }
    ON SEQUENCES
    TO { [ GROUP ] role_name | PUBLIC } [, ...] [ WITH GRANT OPTION ]
```

- 批量权限赋予

```
postgres=# \h grant
Command:     GRANT
Description: define access privileges
Syntax:
GRANT { { SELECT | INSERT | UPDATE | DELETE | TRUNCATE | REFERENCES | TRIGGER }
    [, ...] | ALL [ PRIVILEGES ] }
    ON { [ TABLE ] table_name [, ...]
         | ALL TABLES IN SCHEMA schema_name [, ...] }
    TO role_specification [, ...] [ WITH GRANT OPTION ]
    [ GRANTED BY role_specification ]
```

睿创神脑
RUICHUANGSHENNAO

对象易主管理

PolarDB PostgreSQL

两种方法来转移对象的拥有者：

1、转移单个表的属主（1、超级用户；2、属主，原属主必须是被授权用户的成员）

```
Alter table tabl_name owner to new_owner;
```

2、转移当前数据库表的属主（超级用户操作，如果属主是postgres，则不允许，因为其中包含数据字典表，只能用第一种方式单表修改。）

```
Reassign owned by  old_role to new_role;
```

睿创神脑
RUICHUANGSHENNAO

PolarDB
PostgreSQL

总结

- PostgreSQL对象权限概述
- PostgreSQL对象权限授权与回收

睿创神脑
RUICHUANGSHENNAO

PolarDB PostgreSQL

练习

- 1、新建2个普通用户a、b, 新建1个数据库db并将owner设置为a, 使用a在db中创建1个schema s, 在s中创建一张表tbl, 请赋予最小权限使得b可以访问db.s.tbl的数据.
- 2、请将未来a在db.s中创建的表的查询权限都默认赋予给b.

睿创神脑
RUICHUANGSHENNAO

PolarDB PostgreSQL