COMP3311 Week 09 Lecture

Catalogs

Catalogs

An RDBMS maintains a collection of relation instances.

To do this, it also needs information *about* relations:

- name, owner, primary key of each relation
- name, data type, constraints for each attribute
- authorisation for operations on each relation

Similarly for other DBMS objects (e.g. views, functions, triggers, ...)

This information is stored in the *system catalog*.

(The "system catalog" is also called "data dictionary" or "system view")

... Catalogs

DBMSs use a hierarchy of namespaces to manage names:

Database (or **Catalog**)

- top-level namespace; contains schemas
- users connect to/work in a "current" database

Schema

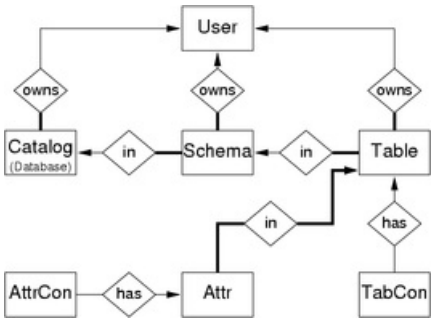
- second-level namespace; contains tables, views, etc.
- users typically work within a "current" schema

Table

- lowest-level namespace; contains attributes
- SELECT queries set a context for attribute names

... Catalogs

DBMSs store the catalog data in a collection of special tables:



(A small fragment of the meta-data tables in a typical RDBMS)

... Catalogs

SQL:2003 standard metadata: `INFORMATION_SCHEMA`.

`INFORMATION_SCHEMA` is available globally and includes:

Schemata(catalog_name, schema_name, schema_owner, ...)

Tables(table_catalog, table_schema, table_name, table_type, ...)

Columns(table_catalog, table_schema, table_name, column_name,
ordinal_position, column_default, data_type, ...)

Views(table_catalog, table_schema, table_name, view_definition, ...)

Table_Constraints(..., constraint_name, ..., constraint_type, ...)

etc. etc. etc.

PostgreSQL and Schemas

When you run `psql`

- you specify database (e.g. `ass2`)
- it specifies a default schema: `public`

All object references are relative to the current schema.

Can access objects in other schemas via: *Schema*`.`*Object*

(e.g. `public.students`, `information_schema.tables`, ...)

To change schemas: **`set schema`** '*Schema*'

PostgreSQL provides SQL standard `INFORMATION_SCHEMA`

Exercise: Exploring the Catalog (1)

7/25

Using the `INFORMATION_SCHEMA`, write a view to list the names of all tables in the `public` schema

The view should be defined/invoked as follows:

```
select * from myTables;
  name
--------
 table1
 table2
 table3
 ...
```

[Solutions]

Exercise: Exploring the Catalog (2)

8/25

Using the `INFORMATION_SCHEMA`, write a view to list the tables+attributes in the `public` schema

The view should be defined/invoked as follows:

```
select * from mySchema;
 table  |            attributes
--------+--------------------------------
 table1 | attr1a, attr1b, attr1c, attr1d
 table2 | attr2a, attr2b
 table3 | attr3a, attr3b, attr3c
 ...
```

[Solutions]

Exercise: Exploring the Catalog (3)

9/25

Using the `INFORMATION_SCHEMA`, write a PLpgSQL function

```
create or replace function
    myTableDef(_table text) returns text
as ...
```

- whose argument is a table name (from the `public` schema)
- whose result is a `CREATE TABLE` statement to build the table
- only handle constraints mentioned in the `columns` table

Extension: add all constraints (not just the ones in `columns`)

[Solutions]

Exercise: Size of each Table

10/25

Write a PLpgSQL function to produce a list of user tables, along with a count of the number of tuples in each table.

The function should be defined/invoked as follows:

```
create type PopulationRecord as
    ("table" text, ntuples integer);

create or replace function
    dbpop() returns setof PopulationRecord
...
select * from dbpop();
```

```
 table | ntuples
-------+--------
     R |     25
     S |     12
```

[Solutions]

PostgreSQL Catalog

Most DBMSs had defined their own catalog tables before `INFORMATION_SCHEMA` was standardised.

The PostgreSQL catalog contains around 80 tables and views

- most describe schema data (tables, attributes, constraints, ...)
- others deal with DB configuration and statistics
- others deal with users, roles, privileges
- all are called `pg_`*XXX* (e.g. `pg_tables`)
- many have primary key via implicit `oid` attribute

Course Notes contain details of important catalog tables.

For full details, see Chapter 45 in PostgreSQL documentation.

Security, Privilege, Authorisation

Database Access Control

Access to DBMSs involves two aspects:

- having execute permission for a DBMS client (e.g. `psql`)
- having a username/password registered in the DBMS

Establishing a *connection* to the database:

- user supplies database/username/password to client
- client passes these to server, which validates them
- if valid, user is "logged in" to the specified database

... Database Access Control

Note: we don't need to supply username/password to `psql`

- `psql` works out which user by who ran the client process
- we're all PostgreSQL super-users on our own servers
- servers are configured to allow super-user direct access

Note: access to databases via the Web involves:

- running a script on a Web server
- using the Web server's access rights on the DBMS

Access specified in `/srvr/`*YOU*`/pgsql903/pg_hba.conf`

... Database Access Control

SQL standard doesn't specify details of users/groups/roles.

Some typical operations on users:

```
CREATE USER Name IDENTIFIED BY 'Password'
ALTER USER Name IDENTIFIED BY 'NewPassword'
ALTER USER Name WITH Capabilities
ALTER USER Name SET ConfigParameter = ...
```

Capabilities: super user, create databases, create users, etc.

Config parameters: resource usage, session settings, etc.

... Database Access Control

A user may be associated with a *group* (aka *role*)

Some typical operations on groups:

```
CREATE GROUP Name
ALTER GROUP Name ADD USER User1, User2, ...
ALTER GROUP Name DROP USER User1, User2, ...
```

Examples of groups/roles:

- AcademicStaff ... has privileges to read/modify marks
- OfficeStaff ... has privilege to read all marks
- Student ... has privilege to read own marks only

Database Access Control in PostgreSQL

In older versions of PostgreSQL ...

- USERs and GROUPs were distinct kinds of objects
- USERs were added via `CREATE USER` *UserName*
- GROUPs were added via `CREATE GROUP` *GroupName*
- GROUPs were built via `ALTER GROUP ... ADD USER ...`

In recent versions, USERs and GROUPs are unified by ROLEs

Older syntax is retained for backward compatibility.

... Database Access Control in PostgreSQL

PostgreSQL has two ways to create users ...

From the Unix command line, via the command

`createuser` *Name*

From SQL, via the statement:

```
CREATE ROLE UserName Options
-- where Options include ...
PASSWORD 'Password'
CREATEDB | NOCREATEDB
CREATEUSER | NOCREATEUSER
IN GROUP GroupName
VALID UNTIL 'TimeStamp'
```

... Database Access Control in PostgreSQL

Groups are created as ROLEs via

```
CREATE ROLE GroupName
--or--
CREATE ROLE GroupName WITH USER User1, User2, ...
```

and may be subsequently modified by

```
GRANT GroupName TO User1, User2, ...
REVOKE GroupName FROM User1, User2, ...
GRANT Privileges ... TO GroupName
REVOKE Privileges ... FROM GroupName
```

SQL Access Control

SQL access control deals with

- privileges on database objects (e.g. tables, view, functions, ...)
- allocating such privileges to roles (i.e. users and groups)

The user who creates an object is automatically assigned:

- ownership of that object
- a privilege to modify (ALTER) the object
- a privilege to remove (DROP) the object
- along with all other privileges specified below

... SQL Access Control

The owner of an object can assign privileges on that object to other users.

Accomplished via the command:

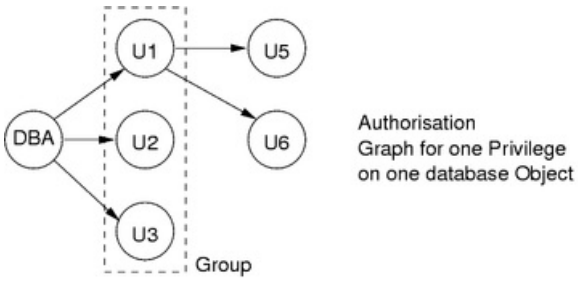
```
GRANT Privileges ON Object
TO ( ListOfRoles | PUBLIC )
[ WITH GRANT OPTION ]
```

Privileges can be ALL (giving everything but ALTER and DROP)

`WITH GRANT OPTION` allows a user who has been granted a privilege to pass the privilege on to any other user.

Effects of privilege granting

- are sometimes subtle (possible conflicts?)
- can be represented by an *authorisation graph*



Privileges can be withdrawn via the command:

```
REVOKE Privileges ON Object
FROM ListOf (Users|Roles) | PUBLIC
CASCADE | RESTRICT
```

Normally withdraws Privileges from just specified users/roles.

`CASCADE` ... also withdraws from users they had granted to.

E.g. revoking from U1 also revokes U5 and U6

`RESTRICT` ... fails if users had granted privileges to others.

E.g. revoking from U1 fails, revoking U5 or U2 succeeds

Privileges available for users on database objects:

`SELECT`:

- user can read all rows and columns of table/view
- this includes columns added later via `ALTER TABLE`

`INSERT` or `INSERT(`*ColName*`)`:

- user can insert rows into table
- if *ColName* specified, can only set value of that column

More privileges available for users on database objects:

- `UPDATE`: user can modify values stored in the table
- `UPDATE(`*ColName*`)`: user can update specified column
- `DELETE`: user can delete rows from the table
- `REFERENCES(`*ColName*`)`: user can use column as foreign key
- `EXECUTE`: user can execute the specified function
- `TRIGGER`: user is allowed to create triggers on table
