Our take at « row level » security

Sébastien Clément, Biologist & DBA, Canadian Forest Service

forest_data

tree_name	height	diameter	data_source_id
poplar_13111	12.7	25	1
poplar_13112	14.3	35	1
poplar_13113	11.5	22	1
poplar_13114	15.4	33	1
birch_00216	6.1	12	2
birch_00217	7.3	12	2
birch_00218	5.3	11	2
maple_45110	23.4	25	3
maple_45111	13.1	17	3

Project #1

Project #2

...

data_source_references

data_source_id	reference
1	raw_data_2012.xls
1	article_Peter2012.pdf
1	Johns_email.msg
2	project_14.xls
2	protocol.doc
3	Hubert_et_al_2014.pdf
3	Greene_et_al_2014.pdf
3	details.txt

roles_allowed_data_sources

rolename	data_source_id
john	1
john	3
emilia	2
emilia	3

View with a join

v_forest_data

```
SELECT * FROM forest_data
NATURAL JOIN roles_allowed_data_sources;
```

tree_name	height	diameter	data_source_id	rolename
poplar_13111	12.7	25	1	john
poplar_13112	14.3	35	1	john
poplar_13113	11.5	22	1	john
poplar_13114	15.4	33	1	john
birch_00216	6.1	12	2	emilia
birch_00217	7.3	12	2	emilia
birch_00218	5.3	11	2	emilia
maple_45110	23.4	25	3	john
maple_45111	13.1	17	3	john
maple_45110	23.4	25	3	emilia
maple_45111	13.1	17	3	emilia

...+ current_user()

v_forest_data_filtered

```
SELECT * FROM forest_data
NATURAL JOIN roles_allowed_data_sources
WHERE rolename="current_user"();
```

John's view

tree_name	height	diameter	data_source_id	rolename
poplar_13111	12.7	25	1	john
poplar_13112	14.3	35	1	john
poplar_13113	11.5	22	1	john
poplar_13114	15.4	33	1	john
maple_45110	23.4	25	3	john
maple_45111	13.1	17	3	john

Emilia's view

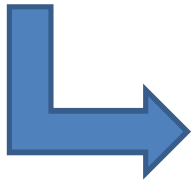
tree_name	height	diameter	data_source_id	rolename
birch_00216	6.1	12	2	emilia
birch_00217	7.3	12	2	emilia
birch_00218	5.3	11	2	emilia
maple_45110	23.4	25	3	emilia
maple_45111	13.1	17	3	emilia

What about groups?

```
CREATE ROLE all_teams;
CREATE ROLE team1;
GRANT all_teams TO team1;
GRANT team1 TO emilia, john;
```

roles_allowed_data_sources

rolename	data_source_id
team1	2
team1	3
emilia	1



WANTED!

included_user	data_source_id
emilia	1
emilia	2
john	2
emilia	3
john	3

Then use views to...

1 . Get relationship between users & groups:

```
CREATE VIEW v_users_in_groups AS
          SELECT
                    (SELECT rolname FROM pg_roles WHERE oid=member) AS user_or_group,
                    (SELECT rolname FROM pg_roles WHERE oid=roleid) AS group
          FROM pg_auth_members;
```

System catalog table

v_users_in_groups

user_or_group	group
team1	all_teams
emilia	team1
john	team1

2 .break down each group into constituent users OR groups:

```
CREATE VIEW v_groups_flattened AS
        WITH RECURSIVE levels(higher_level,lower_level) AS (
                SELECT
                        group AS higher_level,
                        uaer_or_group AS lower_level
                FROM v_users_in_groups
        UNION
        SELECT levels.higher_level,v_users_in_groups.user AS lower_level FROM levels,v_users_in_groups
                WHERE levels.lower_level=v_users_in_groups.group
        )
        SELECT higher_level,lower_level FROM levels ORDER BY 1,2;
```

v_groups_flattened

higher_level	lower_level
all_teams	team1
all_teams	emilia
all_teams	john
team1	emilia
team1	john

3 .keep groups on the left, users only on the right:

```
CREATE VIEW v_groups_and_users_flattened AS
        SELECT higher_level AS group_or_user,lower_level AS included_user
        FROM v_groups_flattened
        JOIN v_users ON lower_level=rolname
        UNION (SELECT rolname,rolname FROM v_users)
        ORDER BY 1,2;
```

View listing users only (pg_roles)

v_groups_and_users_flattened

group_or_user	included_user
all_teams	emilia
all_teams	john
team1	emilia
team1	john
emilia	emilia
john	john

User 2 user correspondence

4. Transform groups into individual users (or keep users):

roles_allowed_data_sources

rolename	data_source_id
team1	2
team1	3
emilia	1

+

v_groups_and_users_flattened

group_or_user	included_user
all_teams	emilia
all_teams	john
team1	emilia
team1	john
emilia	emilia
john	john

```
CREATE VIEW v_roles_allowed_data_sources_flattened AS
        SELECT DISTINCT data_source_id,included_user
        FROM roles_allowed_data_sources rads,v_groups_and_users_flattened vguf
        WHERE rads.rolename=vguf.group_or_user
        ORDER BY 1,2;
```

v_roles_allowed_data_sources_flattened

data_source_id	included_user
1	emilia
2	emilia
2	john
3	emilia
3	john

Final filtered view:

roles_allowed_data_sources

rolename	data_source_id
team1	2
team1	3
emilia	1

v_forest_data_filtered

```
SELECT * FROM forest_data
NATURAL JOIN v_roles_allowed_data_sources_flattened
WHERE included_user="current_user"();
```

John's view

tree_name	height	diameter	data_source_	rolename
birch_00216	6.1	12	2	john
birch_00217	7.3	12	2	john
birch_00218	5.3	11	2	john
maple_45110	23.4	25	3	john
maple_45111	13.1	17	3	john

Emilia's view

tree_name	height	diameter	data_source_	rolename
poplar_13111	12.7	25	1	emilia
poplar_13112	14.3	35	1	emilia
poplar_13113	11.5	22	1	emilia
poplar_13114	15.4	33	1	emilia
birch_00216	6.1	12	2	emilia
birch_00217	7.3	12	2	emilia
birch_00218	5.3	11	2	emilia
maple_45110	23.4	25	3	emilia
maple_45111	13.1	17	3	emilia

Contact:

Sébastien Clément
Biologist & DBA
Canadian Forest Service

https://apps-scf-cfs.rncan.gc.ca/treesource/en/login