INDEX

[INDEX 1](#_Toc261857202)

[REVISION HISTORY 1](#_Toc261857203)

[SCOPE 1](#_Toc261857204)

[IMPLEMENTATION 1](#_Toc261857205)

[OBJECTS INVOLVED 3](#_Toc261857206)

REVISION HISTORY

|  |  |  |  |
| --- | --- | --- | --- |
| Document Version | Date | Description | Contributors |
| V.1. | 14/05/2009 | Initial Draft | M.Fariello |

SCOPE

The scope of this document is limited to describe the database objects involved in the row level security (RLS) functionality within Registration and the topics of your implementation.

Also, this document describes briefly some requirements of the application but these requirements are explained exhaustively in the document “RequirementsDesign\_RLS.docx”

(<http://sharepoint1:6035/rnd/informatics/suite/cboe1101/Project%20Documents/Requirements%20and%20Design%20Specifications/Registration/RequirementsDesign_RLS.docx>)

IMPLEMENTATION

In the Registration Application uses the activation of Oracle Row Level Security to restrict to the users logged to see only the data authorized.

This restriction is applied to database level; in this way a user connected directly to database is not able to see data not authorized with the exception of the owner of the schema of registration (usually RegDB) and the System users that is able to see all dada.

The implementation of RLS is for associate a “function” to each “table” through “policies”. The function associated is executed every time that the data of the tables are consulted. The associate function gets the condition that must meet the data recovered.

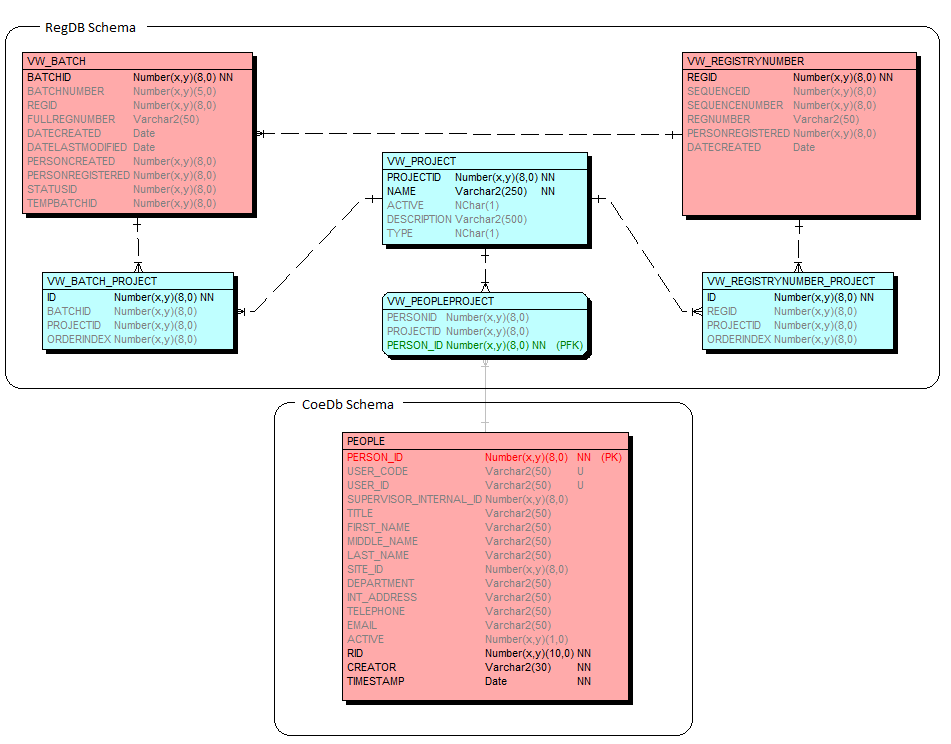
There are two ways to activate or deactivate the row level security in registration. One of these is through the question “Do you want to activate Row-Level security?” when the scripts of registration are executed. Also once created the registration schema is able activate or deactivate RLS via the next PL/SQL sentences executed as the system user : *RegDB.RegistrationRLS.ActivateRLS('True');* It is not possible from application web.

The state of RLS (active or no active) can be consulted through ActivateRLS.GetStateRLS function. This function returns the value of the next tag into the xml field CoeConfiguration.ConfigurationXML: “Registration/applicationSettings/groups/add[@name="REGADMIN"]/settings/add[@name="ActiveRLS"]/@value”

To support the requirement of security, the RLS uses five tables (Compound\_Molecule, Reg\_Numbers, Structures, Batches and Projects). The use of joins between these tables and the rest of registration tables extends the restrictions to all tables.

You can see in the following diagram the views used to support the requirement of security. Each people can be related with one or more project. Also, there are others two relations with project, one to Registry Level and other one to Batch Level.

If there are relations to level Batch, this is taken into count for only show the batches associated to the user’s projects. If there aren’t relations to level Batch, then the relation in Registry Level is taken into consideration for only to show the batches associated to the user’s projects.



OBJECTS INVOLVED

|  |  |  |
| --- | --- | --- |
| Objects Type | Name | Description |
| Package | RegistrationRLS | Contains the functions and procedures needed to manage the functionality RLS. |
| Procedures and functions | PROCEDURE ActivateRLS(AState Varchar2); | Turns on or off the RLS functionality. |
|  | FUNCTION GetStateRLS RETURN Boolean; | If RLS is Active then return True. |
|  | PROCEDURE SetEnableRLS(AState in BOOLEAN); | Turns on or off temporally the RLS functionality. |
|  | FUNCTION PeopleProject\_RLL\_Function(p\_schema in VARCHAR2, p\_object in VARCHAR2) RETURN VARCHAR2; | The value returned is used as condition for each consult done on the tables. |
| Variable | RegistrationRLS.gEnableRLS | Used to turns on or off temporally the RLS functionality in a session. |
| Package | ConfigurationManager | Used to get the parameter that identifies the RLS state. The state could be active or no active. |
| Policies | Compound\_MoleculePolicy | These polices associates a table with the role RegistrationRLS.PeopleProject\_RLL\_Function. This function returns the condition used to filter the rows restricted according to the user connected |
|  | Reg\_NumbersPolicy |
|  | StructuresPolicy |
|  | BatchesPolicy |
|  | ProjectsPolicy |
| Tables | Compound\_Molecule | The data of these tables are filtered according to the accesses allowed when a consult on the tables is requested |
|  | Reg\_Numbers |
|  | Structures |
|  | Batches |
|  | Projects |
|  | CoeConfiguration | The column ConfigurationXML hold the tag “Registration/applicationSettings/groups/add[@name="REGADMIN"]/settings/add[@name="ActiveRLS"]/@value”. This tag identifies if the RLS functionality is actived. |