**DATABASE SECURTY: ORACLE LABEL SECURITY**

“Oracle Label Security enables companies and government organizations to consolidate data with similar sets of sensitive data – but with different access requirements (including government classified data) – into the same database. Oracle Label Security implements multilevel access controls based on the classification of the data and the access label (security clearance) of the application user. This powerful capability enables sensitive R&D projects, non-public financial information and multi-level security requirements to be enforced inside the Oracle Enterprise Edition database, including Oracle Exadata. ”

- Oracle

**Introduction**

Oracle Label Security controls the display of individual table rows using labels that are assigned to individual table rows and application users.

Oracle Label Security is based on multi-level security (MLS) requirements that are found in government and defence organizations. You can easily restrict sensitive information to only authorized users. Oracle Label Security is based on Oracle Virtual Private Database (VPD). However, unlike VPD, Oracle Label Security provides the access mediation functions, data dictionary tables, and policy-based architecture out of the box, eliminating customized coding and providing a consistent label-based access control model that can be used by multiple applications. Oracle Label Security policies can be applied to one or more application tables. Oracle Label Security works by comparing the row label with a user's label authorizations. Oracle Label Security software is installed by default, but not automatically enabled.

OLS enforces access controls by comparing a data classification label with a user’s security clearance. A security clearance can be thought of as an extension to standard database privileges and roles. For example, a very common database operation is to grant select on an application table to a user or a role. However, how do you restrict access to highly sensitive data? For that to happen two things have to take place: First the database has to know what data is considered highly sensitive and secondly the database has to know the security clearance of the user. Oracle Label Security solves this problem by providing the ability to define data classification labels, assign security clearances to users, assign data classification labels to data, and enforce access control. Historically the design approach used to achieve this type of functionality was based on database views, triggers and lookup tables. However, that approach required extensive application changes and resulted in inconsistent implementations across applications. Oracle Label Security is enforced within the database, below the application layer, providing stronger security and eliminating the need for application views and triggers.

**Virtual Private Databases (VPD)**

Virtual Private Databases (VPD) allow multiple users to access a single schema whilst preventing them from accessing data that is not relevant to them. Although this type of access can be controlled by the application, access via other methods (SQL\*Plus) would leave the data open to abuse. VPD uses Fine-Grained Access Control to limit which data is visible to specific users.

Introduced in Oracle8i, a Virtual Private Database (VPD) is the most popular security feature of Oracle Database Enterprise Edition. It is used when the standard object privileges and associated database roles are insufficient to meet the application security requirements.

Oracle VPD enables you to create security policies or group policies to control database access at the row and column level. It allows multiple users to access a single schema while preventing them from accessing data which is not relevant to them. VPD uses Fine-Grained Access Control to limit visibility of the data to the specific users. This is also referred to as the Row Level Security (RLS) and Fine Grained Access Control (FGAC).

Generally, we leverage data access control in application accessing the data. Oracle VPD security policies provide a mechanism to secure data at the database level itself. The ability to secure data at a granular database object level is a very powerful feature of VPD.

By principle, Oracle Virtual Private Database adds a dynamic WHERE clause to an SQL statement that is issued against the table, view, or is a synonym of an applied Oracle Virtual Private Database security policy.

We attach security policies directly to the database tables, views, or synonyms. Oracle Virtual Private Database enforces security to a fine level of granularity directly on these objects. As a result, the policies are automatically applied whenever a user accesses data from these objects. There is no way to bypass the VPD security policy added for these objects.

When a user accesses the VPD enforced object (table, view, or synonym), based on the VPD predicate function, Oracle engine dynamically modifies the SQL statement of the user.

An additional WHERE clause condition is added as returned by the policy function of the object being accessed. Oracle engine modifies the statement dynamically as returned by the predicate function of the VPD policy. Oracle Virtual Private Database policies can be applied to SELECT, INSERT, UPDATE, INDEX, and DELETE statements.

VPD Features and Concerns:

* Prevent SQL injection attacks from application layer
* Integrate with other DB security features –Redaction –redact column data –Label Security –protect column data
* Increased VPD complexity over time leads to maintainability concerns
* Use VPD to meet simple requirements

**OLS vs VPD**

OLS is based on top of VPD. VPD is the lower level technology, it allows policies to be defined that act upon tables or views that they are associated with. OLS takes the metaphor further and associates a label (hence label security) with each record. These labels are then used with a cross reference of user’s rights to decide whether a record can be accessed. i.e. they have levels such as in secret service or military definitions, such as SECRET, TOP SECRET etc. Users who are allowed to access a certain level (e.g SECRET) then they can access data at that level or lower.

Oracle VPD is a term used for several powerful security features like, fine grained access control (FGAC), application context and global application context. VPD policies are written using PL/SQL, and can be assigned to an individual table or view. An information request, that accesses a table or view protected by VPD, is modified according to the policy assigned to the table or view.

VPD policies can be as simple as enforcing access during business hours. VPD policies can restrict access by comparing the value of an attribute in an individual row with an application context value. Global application context allows an application context to be accessed across multiple database sessions, reducing or eliminating the need to create a separate application context for each user session.

Oracle Label Security is an out-of-the-box solution for row level security. No coding or software development is required, allowing the administrator to focus completely on the policy. Oracle Label Security provides an interface for creating policies, specifying enforcement options, defining data sensitivity labels, establishing user label authorizations, and protecting individual tables or schemes.

Data sensitivity labels provide a powerful and flexible method of restricting access to data. For example, data belonging to different organizations or companies can be separated using data sensitivity labels and selectively shared between companies by changing the data sensitivity label.

Depending on the complexity of the security policy, Oracle Virtual Private Database may be the preferred method for implementing your security policy. Oracle Label Security is best suited for situations where access control decisions need to be based on the sensitivity of the information

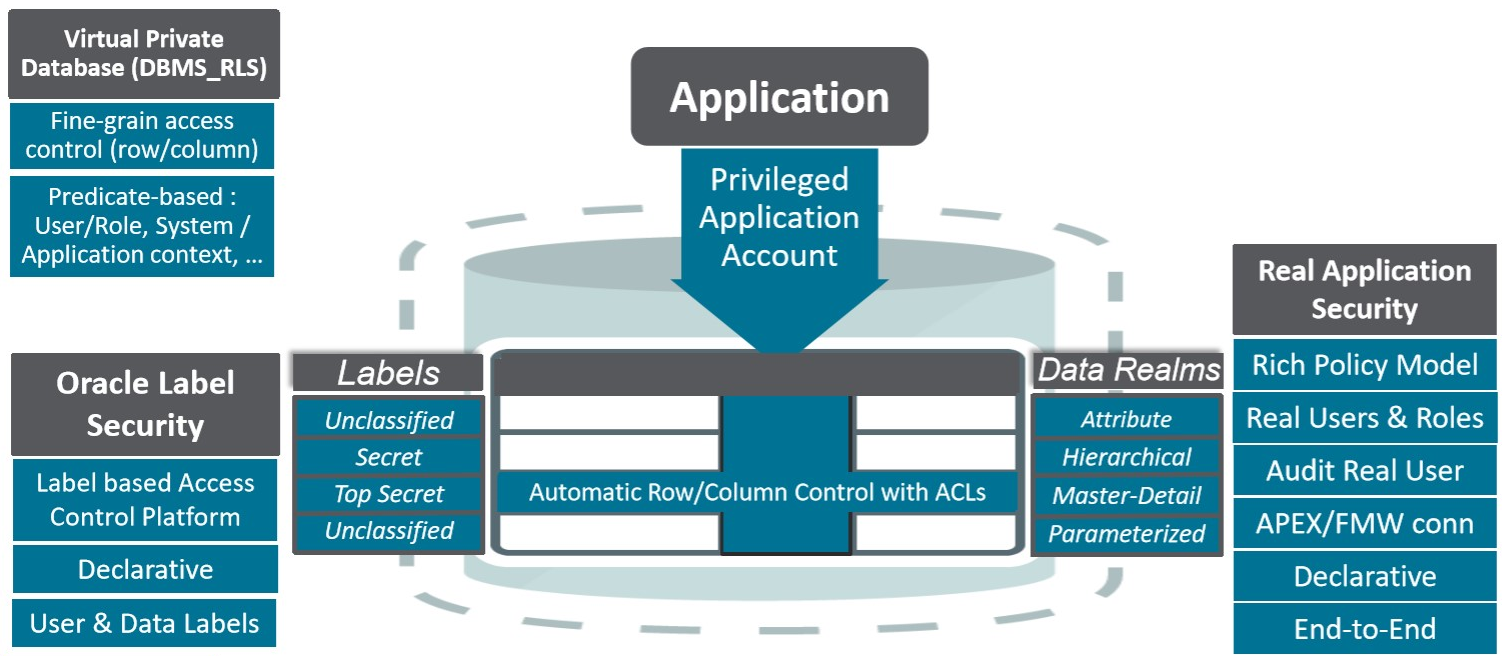


Figure 1 Oracle Data Driven Securtiy

**Components of Oracle Label Security**

Oracle Label Security has two high-level components

**Labels**

* Consists of User and Data labels
* Governs access to specific protected objects

**Policies**

* Labels, rules, authorizations, and protected tables

Oracle label controls the access to data by using:

* The label of the data row to which access is requested
* The label of the user session requesting access
* The policy privileges for that user session

**Policy**

OLS policies are named containers for a collection of data labels, user security clearances, and protected objects. Multiple policies can be defined within a single database. Each OLS policy can have a default set of protective enforcement options, such as READ CONTROL and WRITE CONTROL. The default enforcement options are used when a policy is applied to an application table. Enforcement options can also be customized on a per table basis. When defining an OLS policy, a column name must be provided to store the data classification label. When a policy is applied to an existing application table, the additional column can be appended as a hidden column, thus enabling existing SQL statements to continue working without any changes.

**Label Components**

Every label contains three components: a single level (sensitivity) ranking, zero or more horizontal compartments or categories and zero or more hierarchical groups. Label components consist of levels, compartments and groups. These label components are used to create data labels as well as to assign security clearances to database or application type users. **Levels** are hierarchical in nature and are used to assign the degree of sensitivity. **Compartments** are used to segregate data within a given Level and Groups are used to segregate data organizationally within a given Level. A given data label can have one level, zero or more compartments and zero or more groups associated with it.

***Level:***

* The level is a hierarchical component that denotes the sensitivity of the data. Each and every data label must have a level. A typical organization might define levels such as Confidential, Sensitive and Highly Sensitive.

***Compartments:***

* The compartment component is optional and is sometimes referred to as a category and is nonhierarchical. Typically, one or more compartments are defined to compartmentalize data.
* Compartments might be defined for a specific type of data, knowledge area or project that requires special approval.
* Compartments identify areas that describe the sensitivity of the labeled data, providing a finer level of granularity within a level
* The compartment component is not hierarchical
* If compartments are specified, then a user whose level would normally permit access to a row's data will nevertheless be prevented from such access unless the user s' label also contains all the compartments appearing in that row's label.

***Groups:***

* The group component is optional and is very similar to a compartment with a few exceptions. Each group can have a parent child relationship. Groups are most often used to segregate data by organization.
* The group component is hierarchical and is used to reflect ownership
* Example: suppose one has two groups of users, IT and Software Engineering. Users with the label IT cannot access to data labeled SE (and vice versa), because they are “at the same level”
* Suppose that one has a group University Admins(UA). Users in this group must be allowed to access the data of both IT and SE group.
* To this end, one can establish a group hierarchy, where UA is the group “parent” of IT and SE groups.

***Data Labels***

* A label can be any one of the following four combinations of components:
* a single level component, with no groups or compartments, such as U::
* a level and a set of compartments with no groups, such as U:Alpha, Beta:
* a level and a set of groups with no compartments, such as U::FIN, ASIA
* a level with both compartments and groups, such as U:Beta,Psi:ASIA,FIN

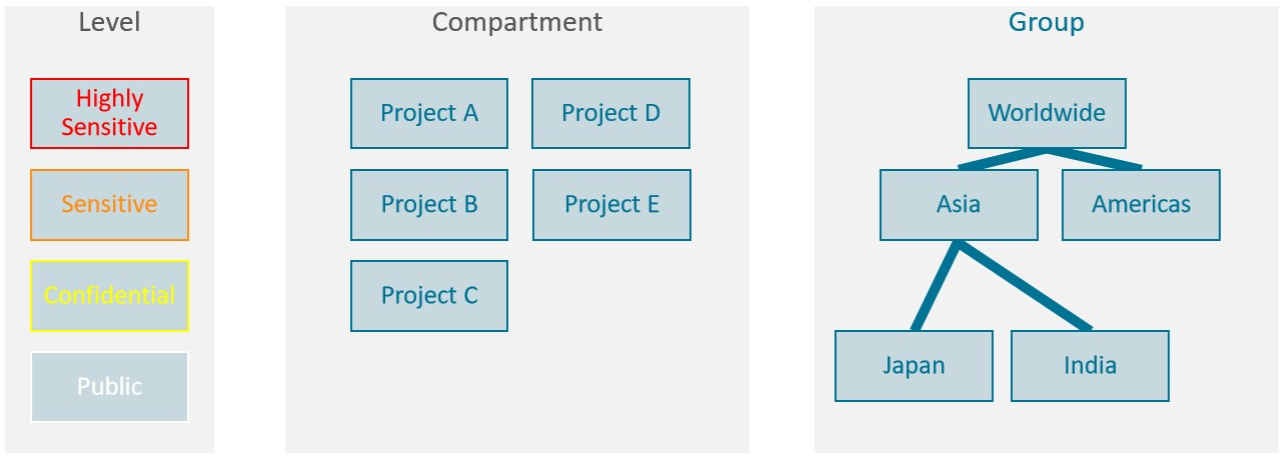


Figure 2 Understanding a Label

OLS provides the ability to define data classification labels to match specific business and organizational requirements. For example, a government organization might have levels such as *Secret* and *Confidential* while a commercial organization might have levels such as *Confidential* and *Public.*

When a user authenticates to the Oracle Database, Oracle Label Security initializes the user label. For applications that do not use physical database users, Oracle Label Security provides a built-in proxy capability that can be used by the application to tell Label Security who the user really is. Oracle Label Security provides flexible enforcement controls, enabling access control to be enforced on read operations only, write operations only, or both. When mediating access, Oracle Label Security first compares the user level with the level assigned to the data label. Second, it checks to see that the user has at least one of the groups assigned to the data label. Third, it checks to see that the user has all of the compartments assigned to the data label.

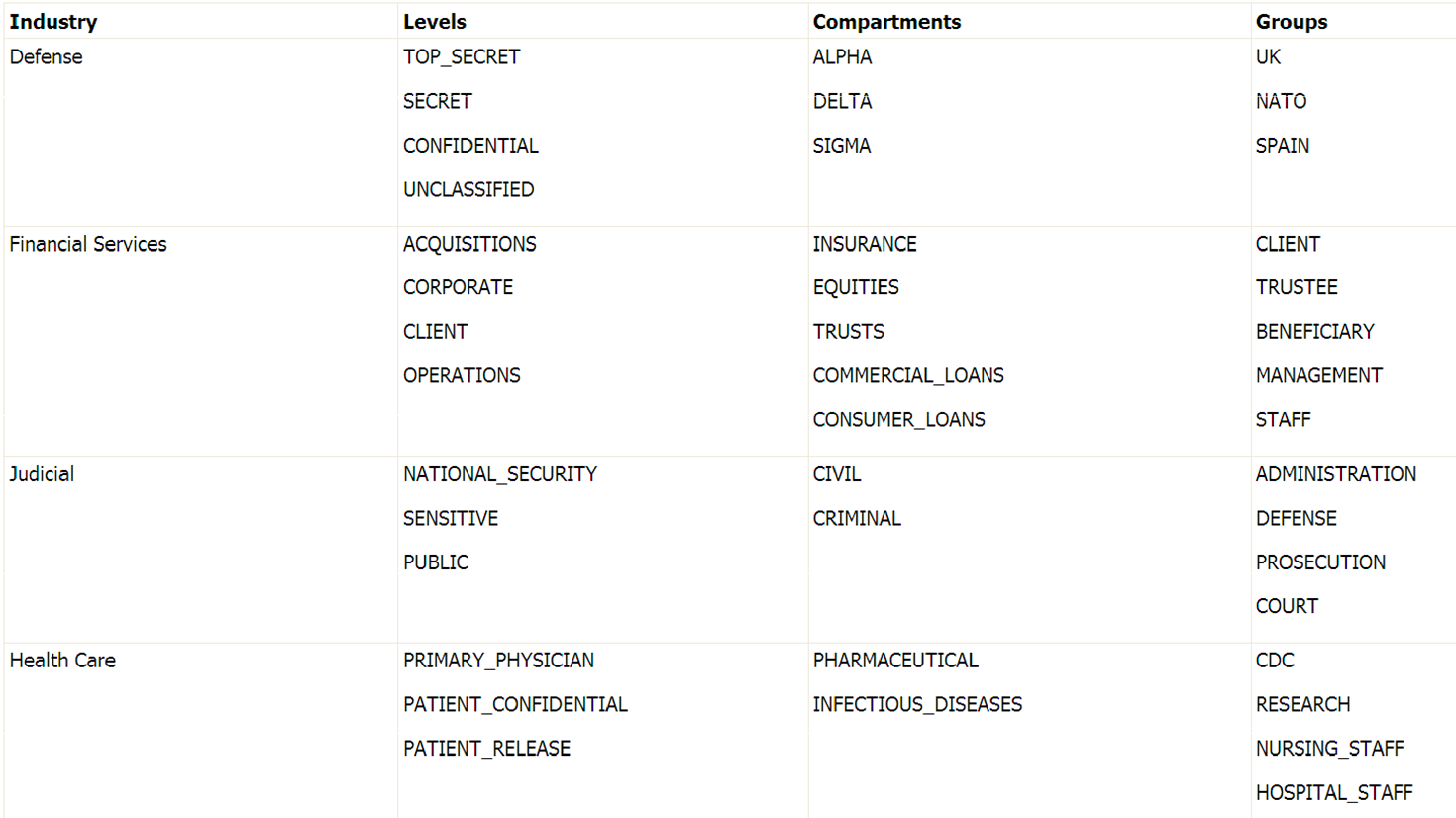


Figure 3 Data Labels

***User Labels:***

* A user label specifies that user's sensitivity level plus any compartments and groups that constrain the user's access to labeled data.
* Each user is assigned a range of levels, compartments, and groups, and each session can operate within that authorized range to access labeled data within that range.

Table A User Labels and level authorizations

|  |  |  |  |
| --- | --- | --- | --- |
| Type | Short | Long | Description |
| Maximum | HS | HIGHLY\_SENSETIVE | User’s highest level |
| Minimum | P | PUBLIC | User’s lowest level |
| Default | C | CONFIDENTIAL | User’s default level |
| Row | C | CONFIDENTIAL | Row level on INSERT |

The administrator specifies the list of compartments and groups that a user can place in her session label. Write access must be explicitly given for each compartment. The Row designation indicates whether the compartment should be used as part of the default row label for newly inserted data.

A user cannot directly insert, update, or delete a row that contains a compartment that she does not have authorization to write.

***Session Labels:***

* The session label is the particular combination of level, compartments, and groups at which a user works at any given time.
* The user can change the session label to any combination of components for which he is authorized.
* When a user writes data without specifying its label, a row label is assigned automatically, using the user's session label.





Figure 4 OLS Displays Authorized data records only

**User Privileges**

The policy privileges enable a user or a stored program unit to bypass some aspects of the label based access control policy. The administrator can also authorize the user or program unit to perform specific actions, such as the ability of one user to assume the authorizations of a different user. Privileges can be granted to program units, authorizing the procedure, rather than the user, to perform privileged operations. Examples of OLS specific privileges include READ and FULL. The READ privilege simply allows a user to view all data regardless of its data classification.

**Security Policies** (**Special User Privileges**)

***READ:***

* A user with READ privilege can read all data protected by the policy, regardless of his authorizations or session label. The user does not even need to have label authorizations.
* A user with READ privilege can write to any data rows for which he or she has write access, based on any label authorizations.
* The READ privilege enables optimal performance on SELECTs, since the system behaves as though the Oracle Label Security policy were not even present.

Examples:

* System administrators who need to export data, but who should not be allowed to change data.
* People who must run reports and compile information, but not change data.

***FULL:***

* The FULL privilege has the same effect and benefits as the READ privilege, with one difference: a user with FULL privilege can also write to all the data.

***COMPACCESS:***

* The COMPACCESS privilege allows a user to access data based on the row label's compartments, independent of the row label's groups.
* If a row label has no compartments, then access is determined by the group authorizations. However, when compartments do exist, and access to them is authorized, then the group authorization is bypassed.
* This allows a privileged user whose label matches all the compartments of the data to access any data in any particular compartment, independent of what groups may own or otherwise be allowed access to the data.

***PROFILE\_ACCESS:***

* The PROFILE\_ACCESS privilege allows a session to change its session labels and session privileges to those of a different user.
* This is a very powerful privilege, since the user can potentially become a user with FULL privileges.
* This privilege cannot be granted to a trusted stored program unit.
* Once the label on a row has been set, Oracle Label Security privileges are required to modify the label.
* These privileges include WRITEUP, WRITEDOWN, and WRITEACROSS.

***WRITEUP:***

* The WRITEUP privilege enables the user to raise the level of data within a row, without compromising the compartments or groups.
* The user can raise the level up to his or her maximum authorized level.
* He can raise the level above his current session level, but cannot change the compartments.

***WRITEDOWN:***

* The WRITEDOWN privilege enables the user to lower the level of data within a row, without changing the compartments or groups. The user can lower the level to any level equal to or greater than his or her minimum authorized level.

***WRITEACROSS:***

* The WRITEACROSS privilege allows the user to change the compartments and groups of data, without altering its sensitivity level.

**Manageability**

Policy based administration enables data labels, user labels, enforcement options and protected tables to be easily managed. Multiple Label Security policies can exist in the same database. Oracle Label Security policies, data labels, user labels and protected tables can be managed using Oracle Enterprise Manager. Integration with Oracle Identity Management enables Oracle Label Security policies, data labels and user labels to be centrally managed for an entire enterprise. Oracle Label Security performance has been significantly improved over the past several releases of the Oracle Database.

Online References:

<https://www.postgresql.org/docs/9.1/sql-security-label.html>

<https://docs.oracle.com/database/121/OLSAG/config.htm#OLSAG3798>

<https://docs.oracle.com/cd/B28359_01/network.111/b28529/intro.htm>

<https://blog.yannickjaquier.com/oracle/oracle-label-security-ols-12c-setup.html#preamble>

<https://blog.rackspace.com/intro-virtual-private-databases-vpds>

<https://oracle-base.com/articles/8i/virtual-private-databases>

<https://www.oracle.com/technetwork/database/security/index-088277.html>