19c ORACLE Database

Oracle Label Security

The need for more sophisticated controls on access to sensitive data is becoming increasingly important as organizations address emerging security requirements around data consolidation, privacy and compliance. Maintaining separate databases for highly sensitive customer data is costly and creates unnecessary administrative overhead. However, consolidating databases sometimes means combining sensitive financial, HR, medical or project data from multiple locations into a single database for reduced costs, easier management and better scalability. Oracle Label Security provides the ability to tag data with a data label or a data classification to allow the database to inherently know what data a user or role is authorized for and allows data from different sources to be combined in the same table as a larger data set without compromising security.

Access to sensitive data is controlled by comparing the data label with the requesting user's label or access clearance. A user label or access clearance can be thought of as an extension to standard database privileges and roles. Oracle Label Security is centrally enforced within the database, below the application layer, providing strong security and eliminating the need for complicated application views.

PRODUCT OVERVIEW

What is Oracle Label Security?

Oracle Label Security (OLS) is a security option for the Oracle Enterprise Edition database and mediates access to data rows by comparing labels attached to data rows in application tables (sensitivity labels) and a set of user labels (clearance labels).

ORACLE

Who should consider Oracle Label Security?

Sensitivity labels are used in some form in virtually every industry. These industries include health care, law enforcement, energy, retail, national security and defense industries. Examples of label use include:

- Separating individual branch store, franchisee, or region data
- Financial companies with customers that span multiple countries with strong government privacy controls
- Consolidating and securing sensitive R&D projects
- Minimizing access to individual health care records
- Protecting HR data from different divisions
- Securing classified data for Government and Defense use
- Complying with U.S. State Department's International Traffic in Arms (ITAR) regulations
- Supporting multiple customers in a multi-tenant SaaS application
- Restrict data processing, tracking consent and handling right to erasure requests under EU GDPR

What can Oracle Label Security do for my security needs?

Oracle Label Security can be used to label data and restrict access with a high degree of granularity. This is particularly useful when multiple organizations, companies or users share a single application. Sensitivity labels can be used to restrict application users to a subset of data within an organization, without having to change the application. Data privacy is important to consumers and stringent regulatory measures continue to be enacted. Oracle Label Security can be used to implement privacy policies on data, restricting access to only those who have a need-to-know.

COMPONENTS AND FEATURES

What are the main components of Oracle Label Security?

Label Security provides row level data access controls for application users. This is called Label Security because each user and each data record have an associated security label.

The User label consist of three components – a level, zero or more compartments and zero or more groups. This label is assigned as part of the user authorization and is not modifiable by the user.

Session labels also consists of the same three components and are different from the user label based on the session that was established by the user. For example if the user has a Top Secret level component, but the user logged in from a Secret workstation, the session label level would be Secret.

Data security labels have the same three components as the User and Session labels.

Label components – the three label components are level, compartment and group.

- Levels indicate the sensitivity level of the data and the authorization for a user to access sensitive data. The user (and session) level must be equal or greater than the data level to access that record.

- Data can be part of zero or more compartments. The user/session label must have every compartment that the record data has for the user to successfully retrieve the record. For example, if the data label compartments are A, B and C – the session label must at least contain A, B and C to access that data record.
- Data can have zero or more groups in the group component. The user/session label needs to have at least one group that matches a data record's group(s) to access the data record. For example, if the data record had Boston, Chicago and New York for groups, then the session label needs only Boston (or one of the other 2 groups) to access the data.
- Protected objects are tables with labeled records.
- Label Security policies are a combination of User labels, Data labels and protected objects.

Does Oracle Label Security provide column-level access control?

No, Oracle Label Security is not column-aware.

A column-sensitive Virtual Private Database (VPD) policy can determine access to a specific column by evaluating OLS user labels. An example of this type of OLS and VPD integration is available as a white paper on the OLS OTN webpage.

A VPD policy can be written so that it only becomes active when a certain column (the 'sensitive' column) is part of a SQL statement against a protected table. With 'column sensitivity' switch on, VPD either returns only those rows that include information in the sensitive column the user is allowed to see, or it returns all rows, with all cells in the sensitive column being empty, except those values the user is allowed to see.

Can I base Secure Application Roles on Oracle Label Security?

Yes, the procedure, which determines if the 'set role' command is executed, can evaluate OLS user labels. In this case, the OLS policy does not need to be applied to a table, since row labels are not part of this solution. An example of this can be found as a white paper on the OLS OTN webpage.

What are Trusted Stored Program Units?

Stored procedures, functions and packages execute with the system and object privileges (DAC) of the definer. If the invoker is a user with OLS user clearances (labels), the procedure executes with a combination of the definer's DAC privileges and the invoker's security clearances.

Trusted stored procedures are procedures that are either granted the OLS privilege 'FULL' or 'READ'. When a trusted stored program unit is carried out, the policy privileges in force are a union of the invoking user's privileges and the program unit's privileges.

Are there any administrative tools available for Oracle Label Security?

Beginning with Oracle Database 11gR1, the functionality of Oracle Policy Manager (and most other security related administration tools) has been made available in Oracle Enterprise Manager Cloud Control, enabling administrators to create and manage OLS policies in a modern, convenient and integrated environment.

DEPLOYMENT AND ADMINISTRATION

Where can I find Oracle Label Security?

Oracle Label Security is an option that is part of Oracle Database Enterprise Edition. Oracle Label Security is installed as part of the database and just needs to be enabled.

Should I use Oracle Label Security to protect all my tables?

The traditional Oracle discretionary access control (DAC) objects privileges SELECT, INSERT, UPDATE, and DELETE combined with database roles and stored procedures are sufficient for most tables. Furthermore, before applying OLS to your sensitive tables, some considerations need to be taken into account; they are described in a white paper titled Oracle Label Security – Multi-Level Security Implementation found on the OLS OTN webpage.

Are there any guidelines for using Oracle Label Security and defining sensitivity labels?

Yes, a comprehensive Label Security Administrator's Guide is available online. In addition, examples are available in a white paper and under technical resources on the Oracle Technology Network, which walk you through a list of recommended implementation guidelines. In most cases, the security mechanisms provided at no-cost with the Oracle Enterprise Edition (system and object privileges, Database roles, Secure Application Roles) will be sufficient to address security requirements. Oracle Label Security should be considered when security is required at the individual row level.

Can Oracle Label Security policies and user labels (clearances) be stored centrally in Oracle Identity Management?

Not only can your database users be stored and managed centrally in Oracle Identity Management using Enterprise User Security, but Oracle Label Security policies and user clearances can be stored and managed in Oracle Identity Management as well. This greatly simplifies policy management in distributed environments and enables security administrators to automatically attach user clearances to all centrally managed users.

How can I maintain the performance of my applications after applying Label Security access control policies?

As a best practice:

- Only apply sensitivity labels to those tables that really need protection. When multiple tables are joined to retrieve sensitive, look for the driving table
- Do not apply OLS policies to schemas.
- Usually, there is only a small set of different data classification labels; if the table is mostly used for READ operations, try building an Bitmap Index over the (hidden) OLS column, and add this index to existing indexes in that table.
- Review the Oracle Label Security whitepaper available in the product OTN webpage as it contains a thorough discussion of performance considerations with Oracle Label Security.

Can I use Oracle Label Security with Oracle Database Vault, Real Application Security and Data Redaction?

Yes. Oracle Label Security can provide user labels to be used as factors within Oracle Database Vault and security labels can be assigned to Real Application Security users. It also integrates with

Oracle Advanced Security Data Redaction, enabling security clearances to be used in Data Redaction policies.

MORE INFORMATION

Where can I find more information on Oracle Label Security?

For more information, please see the Oracle Label Security page on Oracle Technology Network (OTN). A variety of helpful information is available online including data sheet, white paper, customer references, end-user documentation, and a discussion forum.

https://www.oracle.com/database/technologies/security/label-security.html

CONNECT WITH US

Call +1.800.ORACLE1 or visit oracle.com.
Outside North America, find your local office at oracle.com/contact.

blogs.oracle.com/cloudsecurity/db-sec facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services