19c ORACLE Database

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 Database Enterprise Edition, including Oracle Exadata.

DATA CLASSIFICATION

Oracle Label Security assigns a data label or data classification to application data, enabling sensitive data to reside in the same table with less sensitive data. Oracle Label Security enforces control by comparing the data label with the label or security clearance of the user requesting access. Data Labels can be attached as hidden columns to existing tables, providing transparency to existing applications by mediating access based on the data label but not returning the actual data label in the SQL statement. Alternatively, the data label can be explicitly requested, but only for those rows the label authorization of the requesting user permits.

2014 Jabberwocky Rd	Southlake	PUBLIC
2011 Interiors Blvd	South San Francisco	HIGHLY_SENSITIVE::UNITED_STATES
2007 Zagora St	South Brunswick	PUBLIC
2004 Charade Rd	Seattle	HIGHLY_SENSITIVE::UNITED_STATES
147 Spadina Ave	Toronto	PUBLIC
6092 Boxwood St	Whitehorse	PUBLIC
40-5-12 Laogianggen	Beijing	SENSITIVE::ASIA
1298 Vileparle (E)	Bombay	PUBLIC
12-98 Victoria Street	Sydney	PUBLIC
198 Clementi North	Singapore	SENSITIVE::ASIA
8204 Arthur St	London	PUBLIC

Figure 1: Oracle Label Security Data Labels

Data labels can be comprised of three components. The first component is a mandatory level. Examples of levels include public, confidential, and sensitive. The second component is optional and

Key Business Benefits

- Reduce operational and storage costs by enabling different sets of data, with different levels of sensitivity, to co-mingle in the same system environment.
- Reduce costs of developing or re-coding applications to meet row level access control requirements based on clearance levels.
- Easy, cost-efficient route for compliance requirements for multilevel security, mandatory access control, and manage access to data on a "need to know" basis.
- Comply with government and commercial requirements for highly secure products. Prior releases have been evaluated at International Common Criteria EAL4+.
- Optimized to support environments with mandatory access control/ compartmentalization requirements with multiple data and user classification labels.
- Leverage existing Oracle Enterprise Manager skills to build Policies and manage labels.

ORACLE

is known as a compartment. Multiple compartments can be assigned to a data label and are used to enforce additional special access requirements. For example, a data label protecting special customer accounts might contain the compartment VIP. The third and final component of a label is optional and is known as a group. Examples of groups include organizations or territories such as office of the CEO, AMERICAS, and Europe. Labels will always include a level, and may contain zero or more groups and/or compartments.

USER LABELS AND ACCESS MEDIATION

A user label consists of a maximum and minimum levels, compartments and groups. 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, write operations, 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. For example, a data label of Sensitive:VIP:Executive,CEO would require a user to have access to Sensitive data, the VIP compartment and either the Executive or CEO groups.

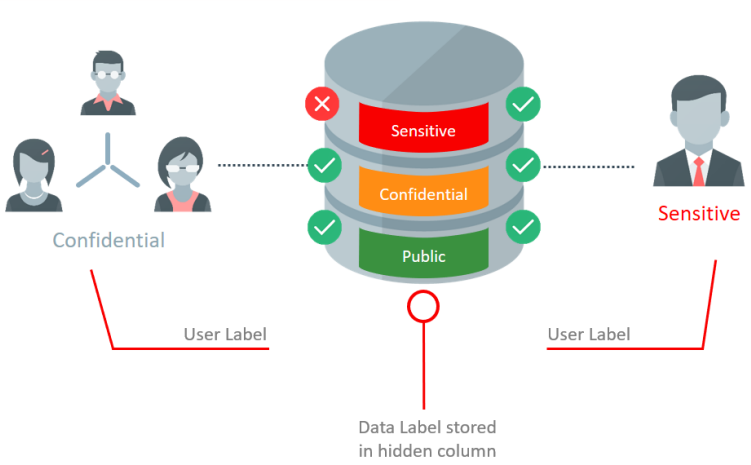

Figure 2: User labels and access mediation

ASSIGNING DATA LABELS

Data labels are comprised of a sensitivity level, zero or more compartments, and zero or more groups. Prior to creating a data label, the valid label components are defined and stored inside the Oracle data dictionary using Oracle Enterprise Manager. Data labels can be automatically assigned to table rows using a labeling function or the user's current session label. Labeling functions enable the data labels to be computed based on different application attributes. Labels can also be assigned by specifying the actual label in the insert statement using either the numeric label tag or the char_to_label function. For low storage overhead, Oracle Label Security uses a numeric tag to represent the data label on each row. The function label_to_char can be used to convert a numeric label tag to its external or text version.

LABEL SECURITY AND EU GDPR

Under the European Union Data Protection Regulation (EU GDPR), data subjects have the right to request an organization to stop processing their data – *Restriction of Processing*. In such cases, the

Key Features

- Data access enforcement is implemented in the database to ensure access control policies are enforced regardless of how and where data is accessed.
- Proxy authorization and built-in access control logic eliminates the requirement to code complex rules into applications
- Dozens of out of the box label functions, including the least upper bound (LUB) and merge label functions
- Hidden columns for data labels
- Flexible and granular enforcement controls, enabling enforcement on READ, UPDATE, INSERT and DELETE operations
- Enable Trusted Stored Procedures by assigning privileges such as FULL or READ
- Supports assignment of label authorizations to non-database users such as application users, IP addresses and other factors
- Integrated with Oracle Database Vault to use security labels as factors for trusted paths
- Integrated with Real Application Security to allow labels to be assigned to Real Application Security users

Related Products

Oracle Database 19c Defense-In-Depth Security Solutions:

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Data Masking and Subsetting Pack
- Oracle Audit Vault and Database Firewall
- Oracle Database Security Assessment Tool

organization will need to design a control to block individual records from continued processing. Depending on the application and schema design, the use of application customization, or use of Oracle Label Security may be appropriate. Label Security can be used to attach security related metadata to individual data rows. Labels can then be used to control if a row can be further processed (access control).

Another use case under EU GDPR scope is using Oracle Label Security for *Consent* management. In this case, data labels can be used to store users' consent definitions.

The EU GDPR's *right for erasure* can also benefit from Oracle Label Security and its data-labeling feature. A process could label rows "to be forgotten" that could be later processed by a data erasure procedure.

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 Internet Directory enables Oracle Label Security policies, data labels and user labels to be centrally managed for an entire enterprise.

19c ORACLE Database

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

Oracle is committed to developing practices and products that help protect the environment

ORACLE