ORACLE LABEL SECURITY

KEY FEATURES AND BENEFITS

- Secure consolidation of data with different data classifications
- Policy based architecture, enabling multiple policies to co-exist in the same database.
- Built-in access control logic eliminates programming requirements
- Dozens of out of the box label functions, including the least upper bound (LUB) and merge label functions
- Hidden columns for data labels
- Supports one big user application models with proxy authorization
- 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 up to 9999 levels, 9999 compartments and 9999 groups.
- Supports assignment of label authorizations to non-database users such as application users, IP addresses and other factors
- Integrated with Oracle Database Vault
- Prior releases have been evaluated at International Common Critieria EAL4+

Oracle Label Security enables government and defense organizations to consolidate data with different data classifications into the same database. Access to data is restricted based on the classification of the data and the security clearance of the application user. This powerful capability enables multi-level security requirements to be enforced inside the Oracle Enterprise Edition database, including Oracle Exadata.

Data Classification

Based on U.S. Department of Defense Multi-Level Security (MLS) concepts, 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 hierarchical level. Examples of Levels include *public*, *confidential*, and *sensitive*. The second component is optional and 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.*

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

RELATED PRODUCTS

Oracle Database 12c Defense-in-Depth Security Solutions:

- Oracle Database Vault
- Oracle Advanced Security
- Oracle Data Masking
- Oracle Audit Vault and Database Firewall

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. For example, a data label of *Sensitive:VIP:Eexecutive,CEO* would require a user to have access to *Sensitive* data, the *VIP* compartment and either the *Executive* or *CEO* groups.

Assigning Data Labels

Data labels are comprised of a hierarchical 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.

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.

Application Certification

Please refer to Oracle Support note 234599.1 for details on how to install Oracle Label Security in an Oracle E-Business Suite environment.

Contact Us

For more information about Oracle Label Security, visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

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

Hardware and Software, Engineered to Work Together

ORACLE