ORACLE LABEL SECURITY

KEY FEATURES AND BENEFITS

FEATURES AND BENEFITS

- Secure consolidation of sensitive data using data labels
- Transparent data classification using hidden columns for data labels
- Flexible enforcement controls
- Integration with Oracle Enterprise Manager and Oracle Identity Management for centralized enterprise management
- Complete PL/SQL API with functions for managing policies, comparing and interpreting data labels

Data consolidation requires the ability to enforce strong access controls on sensitive data. Oracle Label Security data labels enable the Oracle database to know the sensitivity of data consolidated from multiple databases. Data labels such as confidential and sensitive can be assigned to data, enabling sensitive data to reside in the same table as less sensitive data. Oracle Label Security compliments existing application security by enforcing access control at the row level based on data classification.

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 as less sensitive data. Oracle Label Security enforces access 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. Oracle Label Security benefits include:

- Secure consolidation of sensitive data
- Transparent data classification using hidden columns
- Flexible enforcement controls

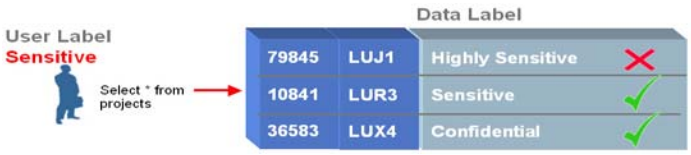

Figure 1. Oracle Label Security Access Control

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*.

RELATED PRODUCTS

- Oracle Database Vault
- Oracle Advanced Security
- Oracle Audit Vault
- Oracle Secure Backup
- Oracle Data Masking

User Labels and Access Mediation

A user label consists of a maximum and minimum level, 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 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 a 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.

Assigning Data Labels

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. Default labels can also be assigned based on the users current label or by specifying the label in the insert statement. For low storage overhead, Oracle Label Security uses a numeric data type to store data labels with data rows. Oracle Label Security functions such as label_to_char can be used to convert a numeric label 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 Meta Link note 234599.1 for details on how to install Oracle Label Security in an Oracle E-Business Suite environment.

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

ORACLE