

Oracle Label Security

18^c ORACLE[®]
Database

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.

KEY FEATURES AND BENEFITS

- Secure consolidation of data with different data classifications without the need for multiple system environments
- Data access enforcement is implemented in the database to ensure access control policies are enforced regardless of how and where data is accessed.
- Optimized to support environments with mandatory access control/compartmentalization requirements with multiple data and user classification labels.
- Policy based architecture, with easy management of labels and policies through Oracle Enterprise Manager.
- 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

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 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.

- 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
- Prior releases have been evaluated at International Common Criteria EAL4+

RELATED PRODUCTS

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

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

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 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: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 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.

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.

ORACLE®

CONNECT WITH US

 blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle oracle.com

CONTACT US

For more information about [insert product name], visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

Integrated Cloud Applications & Platform Services

Copyright © 2018, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0218

