18c ORACLE Database

Oracle Label Security

Technical White Paper

ORACLE WHITE PAPER | MARCH 2018

Table of Contents

Introduction

Over the past 30 years Oracle has been the industry leader in building advanced data security solutions that make it possible to protect sensitive information. Oracle Label Security (OLS) is part of Oracle's defense-in-depth approach to security and is the industry's most advanced solution for controlling access to data based on data classification. This ability is critical for enforcing the principle of "need-to-know" for data access as well as enabling data consolidation. Data consolidation not only reduces cost, but also improves efficiencies in data analysis and decision making.

While Oracle Label Security fits well with military and intelligence agency applications, it also works well in commercial applications with multi-national privacy concerns and data consolidation requirements. For example, countries and companies are demanding stronger privacy controls where only privileged users (administrators) from certain countries are allowed access to their data. Other companies are consolidating similar databases from subsidiaries and retail outlets and require limits on what is visible to each group. Oracle Label Security has out of the box features to enable these and similar use cases.

Oracle Label Security mediates access based on data sensitivity labels (referred to in this document as data labels) and user label authorizations (referred to in this document as user labels.) Oracle Label Security benefits commercial organizations attempting to address numerous access control challenges including those associated with database and application consolidation, privacy laws and regulatory compliance requirements. Oracle Label Security also provides multi-level security capabilities for government and defense applications. Oracle Label Security has been evaluated to the Common Criteria for Information Technology Security Evaluation (ISO15408). Most recently Oracle Label Security 11.1.0.7 completed an independent evaluation to the Common Criteria at EAL4+. Oracle Label Security manageability is completely integrated with Oracle Enterprise Manager which replaces the legacy Oracle Policy Manager that was available with previous releases of the product. Oracle Label Security is available with Oracle Database Enterprise Edition, as well as with the High Performance Package and Extreme Performance Editions of Oracle Database Cloud Service.

Oracle Label Security Concepts

The need for more sophisticated controls on application 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 data (projects, HR, finance) is costly and creates unnecessary administrative overhead. However, consolidating databases sometimes means combining data from different sensitive 'need to know' databases in one system. Oracle Label Security provides the ability to tag data with a data label or a data classification. This capability allows the database to inherently know what data is appropriate for each user and enforce security controls. Data can also be labeled with degree of sensitivity (or level). For example, in government and defense applications, data might be labeled unclassified, secret, or top secret.

Oracle Label Security enforces access controls by comparing a data classification label with a user's access clearance. Access clearance can be thought of as an extension to standard database privileges and roles. For example, a very common database operation is to grant select on an application table to a user or a role. However, how do you restrict access to highly sensitive data? For that to happen two things have to take place: First, the database has to know what data is considered highly sensitive and secondly, the database has to know the access clearance of the user. Oracle Label Security solves this problem by providing the ability to define data classification labels, assign access clearances to users, assign data classification labels to data, and enforce access control. Historically the design approach used to achieve this type of functionality was based on database views, triggers and lookup tables. However, that approach required extensive application changes and resulted in inconsistent implementations across applications. Oracle Label Security is enforced within the database, below the application layer, providing stronger security and eliminating the need for application views and triggers. This enforces the access rights across all applications that connect to the data including reporting and business intelligence tools that normally require their own security model.

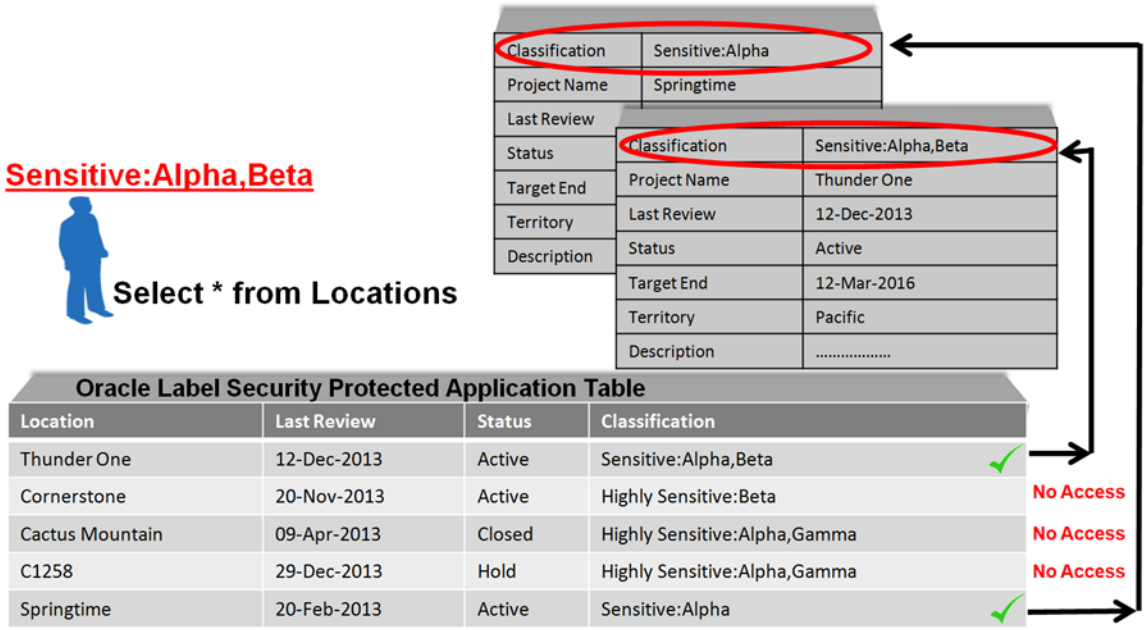

Figure 1. Oracle Label Security leverages user labels and data labels to control data access.

Much like any sophisticated security product, planning your deployment of Oracle Label Security is very important and will help avoid potential problems. The steps below provide a basic guideline for deploying Oracle Label Security. The implementation can be performed using Oracle Enterprise Manager or the Oracle Label Security API / command line interface. It may be useful to work with a sample demonstration table first to get a firm understanding of how data labels mediate access control as well as the various enforcement options available in Oracle Label Security.

TABLE 1. ORACLE LABEL SECURITY IMPLEMENTATION STEPS

» *Perform the data analysis steps recommended in this paper.*
» *Create the Oracle Label Security policy.*
» *Define necessary data label components including levels, compartments and groups.*
» *Provision user labels (Max, Min, Default)*
» *Create the data labels for the policy using the components (levels, compartments and groups) already defined.*
» *Apply the policy to the application tables. Note that once applied, no data will be accessible unless special privileges have been granted to the user.*
» *Update legacy data with appropriate data labels using the techniques described in this paper.*

We will work from the inside out in this white paper, beginning with the core components (data labels, user labels) before we discuss policies and data analysis steps.

Data Labels and Protected Objects

Data label components include levels, compartments and groups. Levels are most commonly used in government and defense projects. These label components are used to create data labels as well as to assign access clearances to database or application type users. Levels are hierarchical in nature and are used to assign the degree of sensitivity. Compartments are used to segregate data within a given level. Groups are used to segregate data organizationally within a given level. A given data label must have one Level, zero or more Compartments and zero or more Groups associated with it. For commercial deployments using only Groups, a default Level will need to be created in addition to the Groups.

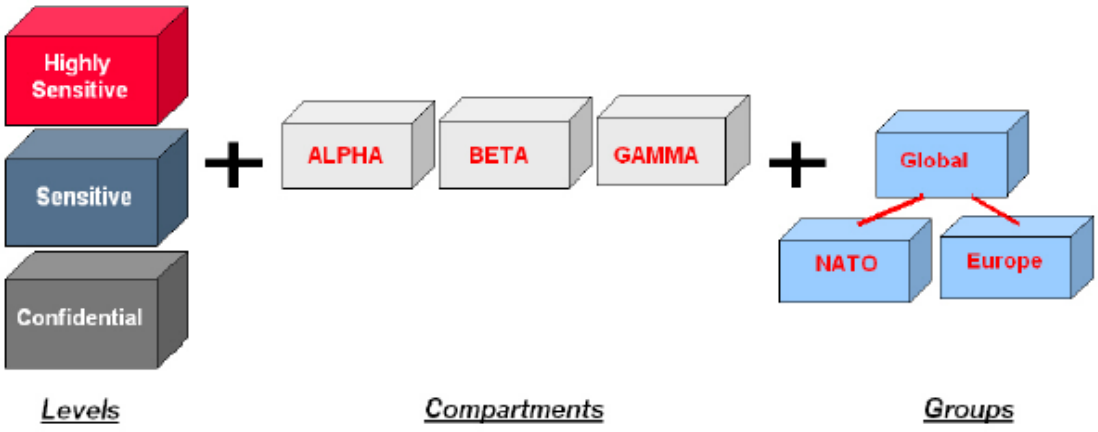

Figure 2. Oracle Label Security data levels can include levels, compartments and groups

TABLE 2. ORACLE LABEL SECURITY - DATA LABEL COMPONENTS

Components	Description
Compartment	The compartment component is optional and is sometimes referred to as a category and is non hierarchical. Typically one or more compartments are defined to compartmentalize data. Compartments might be defined for a specific type of data, knowledge area, geography, or project that requires special approval.
Group	The group component is optional and is very similar to a compartment with a few exceptions. Each group can have a parent child relationship. Groups are most often used to segregate data by organization.
Level	The level is a hierarchical component that denotes the sensitivity of the data frequently used with government and defense data. Each and every data label must have a level. An organization might define levels such as Confidential, Sensitive and Highly Sensitive. If an organization doesn't need multiple levels, a single default level needs to be defined.

Oracle Label Security provides the ability to define data classification labels to match specific business and organizational requirements. For example, a government organization might have levels such as Secret and Confidential while a commercial organization might have levels such as Confidential and Public.

TABLE 3. INDUSTRY SPECIFIC POLICIES AND DATA LABELS

Industry	Level	Compartment	Group
Government and Defense	Confidential Secret Top Secret	Desert Storm Border Protection	NATO Homeland Security
Law Enforcement	Level 1 Level 2 Level 3	Internal Affairs Drug Enforcement	Local Jurisdiction FBI Justice Department
Human Resources	Confidential Sensitive Highly Sensitive	PII Data Investigation	Global US EMEA
Health Care	Confidential Public	Patient Doctor	Lab_Technician Medical_Assistant

Industry	Level	Compartment	Group
Retail Financials	Default*	None	Each Store, Country, Regions, Financial Groups
R&D	Default*	Project	Project Members, Project Lead, Corporate Finance, Corporate Legal

* While levels are not used to determine access for this use case, a level is required to be set.

Using Data Labels

The first and most important step in planning your Oracle Label Security deployment is determining your organization's data label requirements. This means determining what Data Labels or Sensitivity you require to protect your information. Determining your data label requirements generally means analyzing your application and identifying the tables that you plan to protect with Oracle Label Security. This is best accomplished with the assistance of an application administrator or developer who has knowledge of the application schema. In most cases, only a small percentage of the application tables will require an Oracle Label Security policy. Once the candidate tables have been identified, the data contained in the tables needs to be evaluated. The assistance of a data analyst or someone with an understanding of the data may be required. It is recommended that future application data needs be considered as well. This will create a robust set of initial label components.

Note that a single Oracle Label Security policy can have up 9999 levels and up to 9999 compartments and groups. However, most commercial organizations use only a single default level whereas a government or defense implementation might use between 2 and 5 levels.

The external or text representation of a data label uses colons and commas to separate the various components. For example, the data label [Sensitive:Alpha,Beta:UK] contains the level (Sensitive), two compartments (Alpha and Beta), and one group (UK). The data label [Default::US_Country] has the single required level called Default and the group US_Country.

Internally, Oracle Label Security uses a numeric identifier called a label tag for each sensitivity label. Label tags are established when creating the data label. Label tags are stored with each row in a protected column defined by the administrator when a policy is created. The administrator can choose to have the column appended to an application table as an invisible column. Appending the column as an invisible column will eliminate any possibility of existing update or insert statements failing due to the fact the statement didn't qualify the columns names in the statement. It is important to note that the Oracle Label Security policy column can pre-exist in an application table prior to applying an Oracle Label Security policy. To take advantage of this, the application table column type must be number (10). This allows applications to be designed with an Oracle Label Security policy column built-in.

Note that while sensitivity labels and label tags can be created dynamically at run time, Oracle highly recommends defining and documenting all sensitivity labels and associated label tags prior to their being used to label data.

When deciding whether to use compartments, groups, or both, it is important to understand their differences with respect to required user authorization.

TABLE 4. REQUIRED USER AUTHORIZATIONS FOR LABEL COMPONENTS

Label Components	Required User Authorization
Compartment	User must be authorized to all compartments listed in the data label. For example, in order for a user to access data labeled “Sensitive: Alpha, Beta”, the user must have been authorized to at least the “Sensitive” level and to both the “Alpha” and “Beta” compartments. Unlike levels, the number assigned to a compartment has no meaning other than determining the display order of multiple compartments when using internal functions.
Group	User must be authorized to at least one of the groups listed in the data label or be authorized to a parent group. For example, in order for a user to access data labeled “Default::Canada”, the user must have been authorized to the Default level and the Canada group. But the parent of the Canada group is North America Region group so that group can also access the data. Note the colon separating the level, compartment and group sections in the label. Unlike levels, the number assigned to a group has no meaning other than determining the display order of multiple groups when using the label_to_char function or similar functions.
Level	User must be authorized to the level or higher. For example, in order for a user to access data labeled “Sensitive”, the user must have been authorized to at least the “Sensitive” level. The number assigned to the level determines its ranking.

If the application has an entity relationship (ER) diagram, it may be useful to annotate on the diagram the range of data labels for each entity.

User Labels

User labels are an important part of Oracle Label Security and determine whether a user can access information protected with a data label. User labels are comprised of a minimum and maximum level, a default level and a row level. In addition, user labels can have compartments and groups. For example, a user can be assigned a maximum level of Sensitive and a minimum level of Public. Database users also have a default label that is initialized when the user connects to the database. This is sometimes referred to as the active session label. The session label is simply the user’s current level combined with compartments and groups. The session label may differ from the user label based on rules that change it due to the connection. For example, even if a user has a Highly Sensitive level as part of their user label, if the connection is a remote session through VPN the session label may be restricted to the Sensitive level.

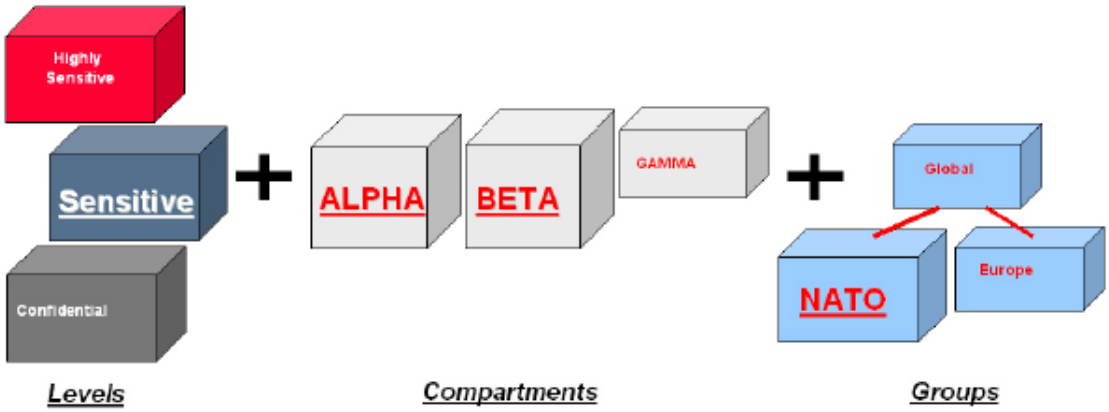

Figure 3. User Label Components include Levels, Compartments and Groups.

TABLE 5. ORACLE LABEL SECURITY – USER LABEL COMPONENTS

Clearance Components	Description
Maximum Level	The maximum sensitivity level a user is authorized to access. For example this might be Sensitive or Highly Sensitive.
Minimum Level	The minimum sensitivity level a user is authorized to write data. For example, an administrator can prevent users from labeling data as Confidential by assigning a minimum level of Sensitive.
Default Level	The level used by default when a user connects to the database. For example, a user can set his or her default level to Sensitive. When he or she connects to the system, the default level will be initialized to Sensitive.
Row Level	The default level used to label data inserted into the database by the user through the application or directly through a tool such as SQL*Plus.
Read Compartments	The set of compartments assigned to the user and used during READ access mediation. For example, if a user has compartments A, B and C, he could view data which has compartments A and B but not data which has compartments A, B, C and D.
Write Compartments	The set of compartments assigned to the user and used during WRITE access mediation. For example, a user could be given READ and WRITE access to compartments A and B but READ-ONLY access to compartment C. If an application record was labeled with compartments A, B and C, the user would not be allowed to update the record because he or she does not have WRITE access on compartment C.
Read Groups	The set of groups assigned to the user and used during READ access mediation. For example, if a user had the group Manager, he could view data that has the Manager group but not data that had only the Senior VP group.
Write Groups	The set of groups assigned to the user and used during WRITE access mediation. For example, a user could be given READ and WRITE access to group Senior VP but READ-ONLY access to group Manager. If an application record was labeled with a single group, Manager, the user would not be allowed to update the record because he or she does not have WRITE access on the Manager group.

Oracle Label Security user labels must be established by the security administrator before an application user can access an application table protected by Oracle Label Security. Note that when multiple policies are present in the database, separate user authorizations must be established for each policy.

For example, below are two tables, Data Sources and Customers. Both tables have unique Label Security policies applied. In order for a user to be able to view data from both tables, the user would have to be assigned user labels for both policies. In this case a user would have to have a user label level equal to at least Highly Sensitive for policy1, and equal to at least Sensitive for policy 2, in order to see all the data.

TABLE 6. DATA SOURCES TABLE

Source	Renewal Date	POL1_SECLAB
SW-R1	201001	Highly Sensitive
SW-R1	201002	Sensitive

TABLE 7. CUSTOMERS TABLE

Name	Location	POL2_SECLAB
ACME	New York	Sensitive
WIDGET	London	Confidential

In the unusual case where multiple policies are assigned to the same table, the policies are 'anded' together. In this example, two policies, policy1 and policy2 are assigned to the same table. Each policy adds an invisible column to the base table. If a user has a user label with a level of Sensitive and the group Mergers for policy1 and has a user label with a level of Sensitive for policy2, then the user would only see the project Galaxy because the first row also requires Highly Sensitive for policy 2.

TABLE 8. PROJECTS TABLE (2 POLICIES APPLIED)

Project Name	Location	POL1_SECLAB	POL2_SECLAB
Condor	New York	Sensitive: : Mergers	Highly Sensitive
Galaxy	HQ	Confidential	Sensitive

While it is possible to specify specific READ or WRITE permissions on individual compartments and groups, in most use cases users will have both READ and WRITE permissions on all compartments and groups they are authorized to access.

Please note that care should be taken to make sure that the total number of compartments and groups authorized to a specific user does not exceed a character string greater than 4000. When assigning the level, compartments and groups, each component is stored internally using 5 characters. For example, if a user is given access to the level "Sensitive" and the compartments "Alpha" and "Beta", internally Label Security will use 10 characters to represent

the compartments. Since each user always has a single level, it is important to monitor the total number of compartments and groups the user is authorized to access.

Policies

Oracle Label Security policies are named containers for a collection of data labels, user labels, and protected objects. Multiple policies can be defined within a single database. Each Oracle Label Security policy can have a default set of protective enforcement options such as READ CONTROL and WRITE CONTROL. The default enforcement options are used when a policy is applied to an application table. Enforcement options can also be customized on a per table basis. When defining an Oracle Label Security policy, a column is used to store the data classification label. When a policy is applied to an existing application table, the column can be appended as an invisible column, thus enabling existing SQL statements and applications to continue working without any changes.

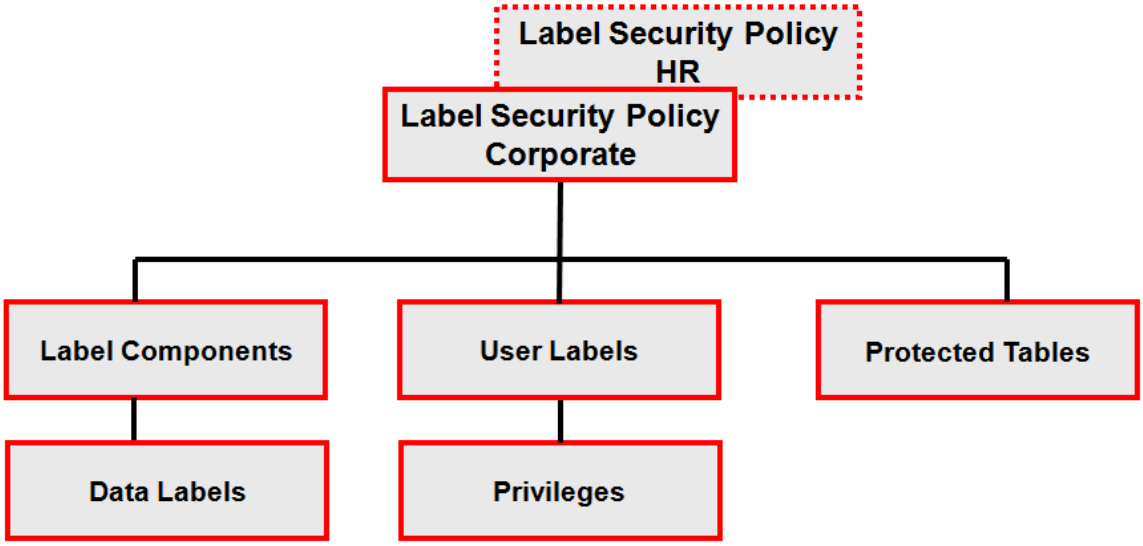

Figure 4. Oracle Label Security Policy Model

Multiple Label Security policies can exist in the same database with different enforcement options. Policy enforcement options can be customized for each policy and for each protected table. When a Label Security policy is created, a default set of enforcement options can be established. When the policy is then applied to an individual table, the enforcement options can again be customized. For example, in some cases the READ CONTROL option may be sufficient because the database user is restricted from update and delete operations by the underlying database table privileges. While multiple policies can be created, each additional policy requires additional processing during database operations so the number of Oracle Label Security policies should be minimized as much as possible.

TABLE 9. ORACLE LABEL SECURITY POLICY ENFORCEMENT OPTIONS

Policy Enforcement Option	Policy Enforcement Description
READ_CONTROL	Applies policy enforcement to SELECT operations using the Oracle Label Security algorithm for read access.
INSERT_CONTROL	Applies policy enforcement to INSERT operations using the Oracle Label Security algorithm for write access.
UPDATE_CONTROL	Applies policy enforcement to UPDATE operations using the Oracle Label Security algorithm for write access.
DELETE_CONTROL	Applies policy enforcement to DELETE operations using the Oracle Label Security algorithm for write access.
WRITE_CONTROL	Applies policy enforcement on INSERT, UPDATE, and DELETE operations. If this option is set, it enforces INSERT_CONTROL, UPDATE_CONTROL, and DELETE_CONTROL.
LABEL_DEFAULT	If the user does not explicitly specify a label on INSERT, the user's default row label value is used. By default, the row label value is computed internally by Oracle Label Security using the user's label. The default value would be comprised of the default ROW LEVEL combined with the WRITE COMPARTMENTS and WRITE GROUPS. A user can set the row label independently, but only to: A level which is less than or equal to the level of the session label, and greater than or equal to the user's minimum level. Include a subset of the compartments and groups from the session label, for which the user is authorized to have write access.
LABEL_UPDATE	Applies policy enforcement to UPDATE operations that set or change the value of a label attached to a row. The WRITEUP, WRITEDOWN, and WRITEACROSS privileges are only enforced if the LABEL_UPDATE option is set.
CHECK_CONTROL	Applies READ_CONTROL policy enforcement to INSERT and UPDATE statements to assure that the new row label is read-accessible by the user after INSERT or UPDATE statement.
ALL_CONTROL	Applies all enforcement options.
NO_CONTROL	Applies no enforcement options. A labeling function or a SQL predicate can nonetheless be applied.

Oracle Label Security policies by definition have a default set of enforcement options. The enforcement options are READ, INSERT, UPDATE, DELETE, LABEL UPDATE, ALL CONTROL and CHECK CONTROL. Once a policy is applied to an application table, the enforcement options can be customized.

Label Strategy

Defining a label strategy requires understanding the various roles and responsibilities of the user population. For example, a user might be designated as an analyst, highly privileged user, or administrative user. Understanding the various roles and responsibilities may require the assistance of managers and security administrators. After the user population has been separated into one or more roles or functional areas, a comparison needs to be performed between the data labels and the user label requirements. These need to correspond correctly for each of the tables identified earlier. This step is important as to prevent data from being assigned a sensitivity label that no user has access to. In other words, the information required to perform a specific job responsibility might be out of reach to the application user due to his or her user label. In the worst case, data might be assigned a data label that no user can access, effectively hiding the data.

TABLE 10. SAMPLE ORACLE LABEL SECURITY AUTHORIZATION ANALYSIS

Table	Data	User			
		C	**S**	**S:A:US**	**S:A,B:US,UK**
Assets	C::UK	No Access	No Access	No Access	Access
	C::US	No Access	No Access	Access	Access
Projects	C	Access	Access	Access	Access
	S	No Access	Access	Access	Access
	S:A:US	No Access	No Access	Access	Access
	S:B:UK	No Access	No Access	No Access	Access
	S:A,B:US	No Access	No Access	No Access	Access

Review and Document

It is important that implementers review and document the information gathered. Include such information as a list of application tables that need to be protected, the reason why, as well as a list of label components and their meanings. This information will also be useful for applying other security controls as well such as Oracle Database Vault Realms, Data Masking and Tablespace Encryption. This document should become part of the enterprise security policy and should be considered sensitive and kept in a safe location.

Oracle Label Security Administration

Installation Guidance

With Oracle Database 12c, Oracle Label Security is installed by default, but not enabled. You can enable Oracle Label Security using the Oracle Database Configuration Assistant (DBCA) or through the SQL*Plus command line.

Earlier versions of the Oracle Database, Oracle Label Security does not install by default. When running the Oracle installer you must choose the custom installation option and manually check the box beside Oracle Label Security. Please note that you must run the Oracle Installer, as it is not sufficient to simply run the associated Oracle Label Security object creation catalog scripts. The installer will re-link the Oracle binary executable during the installation of Oracle Label Security. After running the Oracle Installer you should also run the Oracle Database Configuration

Assistant (DBCA). DBCA will execute the necessary catalog scripts to create the Oracle Label Security administration account, tables, views, functions and procedures.

Please note that if you have already successfully installed Oracle Database Vault (11g) then Oracle Label Security is already installed. However, the administration account for Oracle Label Security will be locked by default. Oracle Database Vault customers have a restricted use license of Oracle Label Security allowing it to be installed. Creating Oracle Label Security specific policies through Oracle Enterprise Manager or the Oracle Label Security API requires a separate Oracle Label Security license not included with Oracle Database Vault.

Administering Users and Roles

With Oracle Database Enterprise Edition 12c, a security related account called LBACSYS is configured. Prior versions will have it configured by the Oracle Database Configuration Assistant (DBCA). The LBACSYS account contains the data dictionary that store Oracle Label Security policies, data labels, protected objects, enforcement settings and user security clearances. LBACSYS stands for Label Based Access Control SYS. This user is separate from the Oracle Database SYS and SYSTEM accounts and should be used to provision named user accounts for administering Oracle Label Security. After enabling Oracle Label Security the LBACSYS account will be locked. The designated Oracle database security administrator will need to unlock the LBACSYS account before it can be used to grant roles and privileges to the named accounts. Oracle recommends customers not use LBACSYS to manage Oracle Label Security since this is a shared account and will not be able to audit end-users correctly.

Access to information stored in LBACSYS is controlled through policy specific roles and database views. Management of specific policies can be delegated to authorized individuals using Oracle Label Security specific database roles and by granting privileges on specific administrative packages.

In addition to holding the metadata associated with Oracle Label Security, the LBACSYS account will also hold several dozen procedures and functions. Examples of Oracle Label Security specific functions installed include char_to_label and label_to_char. These two functions provide translation between an external human readable label and the internal numeric label tag representation stored within the database. Another important function is the Oracle Label Security_DOMINATES function. This function enables a program module to compare two labels and determine whether one label dominates another label. For example, a program module might want to determine whether a user can perform a specific action by comparing a user's active session label with a fixed label. This function can also be used within Oracle Database Vault command rules to determine whether a user should be able to perform a specific operational task within the database. Using labels with Database Vault is an alternative use case for security clearances outside of pure data classification and provides for a finer grained separation of duty capability. In addition, labels can also be used with the Data Redaction product and with the Oracle Database Real Application Security feature.

Oracle Label Security administration is performed using the Oracle Enterprise Manager Database Console and navigating to the target Server. On the Server page you will find a section called Security. Here you will find a link for Oracle Label Security administration. Note that all administrative tasks related to Oracle Label Security can be performed using the available PL/SQL API. The PL/SQL API is fully documented in the Oracle Label Security Administrator's Guide.

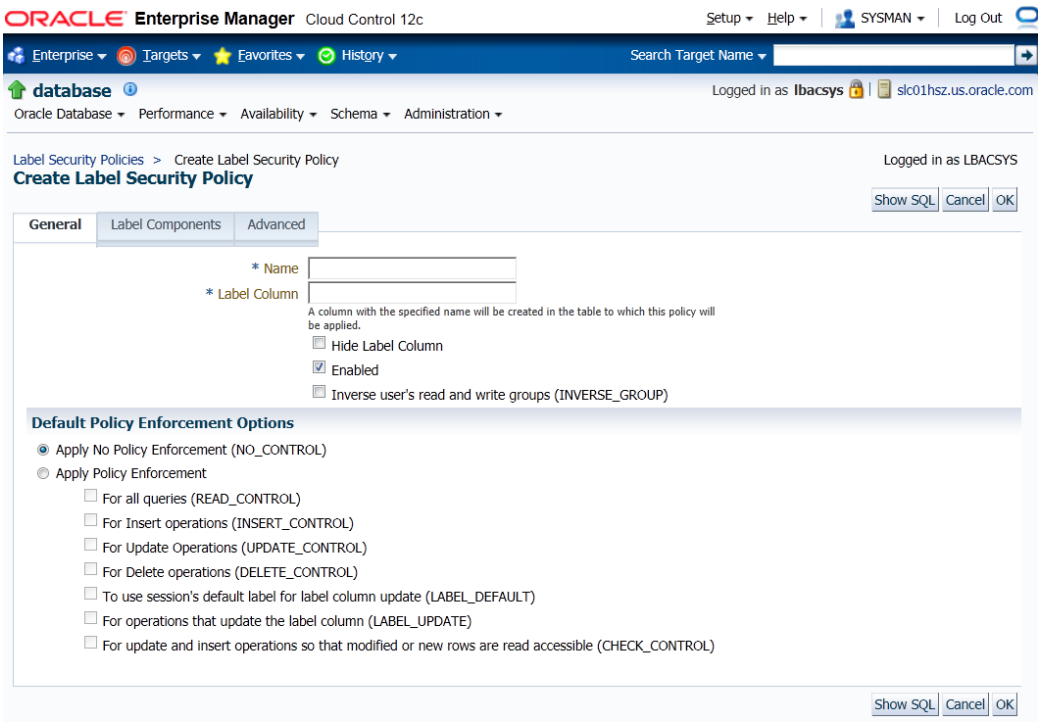

Figure 5. Oracle Label Security Enterprise Manager Interface

Delegated administration is possible using Oracle Label Security. When an Oracle Label Security policy "policyname", is created a new database role policyname_DBA is also created. In the following code, the Oracle Label Security Administrator creates a policy called HRSEC and gives the user the HRSEC_DBA role and authorizations to manage policy label components and label authorizations.

```
CONNECT OLS_ANDREW

EXECUTE SA_SYSDBA.CREATE_POLICY('HRSEC', 'HR_LABEL');

GRANT HRSEC_DBA TO OLS_HR_HOLLY;

GRANT EXECUTE ON SA_COMPONENTS TO OLS_HR_HOLLY;

GRANT EXECUTE ON SA_USER_ADMIN TO OLS_HR_HOLLY;

GRANT EXECUTE ON SA_LABEL_ADMIN TO OLS_HR_HOLLY;

GRANT EXECUTE ON SA_POLICY_ADMIN TO OLS_HR_HOLLY;

GRANT EXECUTE ON SA_AUDIT_ADMIN TO OLS_HR_HOLLY;
```

Once granted, ols_hr_holly can execute the package and create label components, user labels, data labels and administer policies. Note that when any of the above packages are called, the package will check to see if the administrator has been granted the policyname_DBA role corresponding to the one specified on the input line. Since multiple Label Security policies can exist in a single database, each package requires the policy name to be supplied as an input argument. Optionally, individual administrators could be granted execute on different packages, enabling separation-of-duty to be customized.

Oracle Label Security/Virtual Private Database Enforcement Exemptions

The following exceptions are important to understand when using either Oracle Label Security and/or Virtual Private Database (VPD) policies.

TABLE 11. ORACLE LABEL SECURITY/VIRTUAL PRIVATE DATABASE ENFORCEMENT EXEMPTIONS

Exception	Description
SYS objects	VPD and Label Security policies cannot be applied to objects in SYS schema.
SYSDBA role	Any user that connects with the AS SYSDBA role is exempt from VPD and Label Security policies.
DIRECT path export	Oracle VPD policies and Label Security policies are not enforced during DIRECT path export.
EXEMPT ACCESS POLICY database privilege	Any user granted the Oracle Database EXEMPT ACCESS POLICY privilege, directly or through a database role is exempt from both VPD and Label Security policies.

Trusted Stored Procedures

The Oracle Label Security privileges READ and FULL can be granted to stored procedures, enabling access to all data within the execution context of a stored procedure but not directly by the user calling the stored procedure or function.

User Privileges

Oracle Label Security has several privileges that can be assigned to users and stored procedures. Examine privileged users and determine what if any privileges should be assigned.

TABLE 12. ORACLE LABEL SECURITY PRIVILEGES

Privilege	Description
READ	The READ authorization enforces no additional read access control. Access mediation is still enforced on UPDATE, INSERT and DELETE operations. Oracle Label Security makes no mediation check on SELECT operations.
FULL	The FULL authorization turns off all Oracle Label Security access mediation. A user with the FULL authorization can perform SELECT, UPATE, INSERT and DELETE operations with no label authorizations. Note that Oracle SYSTEM and OBJECT authorizations are still enforced. For example, a user must still have SELECT on the application table. The FULL authorization turns off the access mediation check at the individual row level.
COMPACCESS	The COMPACCESS privilege allows a user to access data based on the row label's compartments, independent of the row label's groups
WRITEDOWN	The WRITEDOWN authorization allows a user to modify the level component of a label and lower the sensitivity of the label. For example, application data which is labeled Highly Sensitive: Alpha, Beta could be changed to Sensitive: Alpha, Beta. This authorization is only applicable to policies that use the label update enforcement option.

Privilege	Description
WRITEUP	The WRITEUP authorization allows a user to modify the level component of a label and raise the sensitivity of the label. For example, application data which is labeled Sensitive: Alpha, Beta could be changed to Highly Sensitive: Alpha, Beta. Note that the Maximum Level label authorization assigned to the user would limit modification. This authorization is only applicable to policies that use the label update enforcement option.
WRITEACROSS	The WRITEACROSS authorization allows a user to modify the compartments and groups in a label to any valid compartment and group defined in Oracle Label Security for the policy. For example, data labeled Sensitive: Alpha could be modified to Sensitive: Alpha, Beta even though the user was not authorized for the Beta compartment. This authorization is only applicable to policies that use the label update enforcement option.
PROFILEACCESS	The PROFILE ACCESS authorization allows a user to assume the Oracle Label Security authorizations of another user. For example, user Scott who has access to compartments A, B, and C could assume the profile of user Joe who has access to compartments A, B, C and D. This functionality might be useful in an environment where an application uses a single application account for all application users. Note that the PROFILEACCESS privilege cannot be granted to a stored procedure.

Oracle Label Security and Virtual Private Database Capability

Oracle Label Security also provides the ability to add an ad hoc restrictive 'where' clause or 'condition' when a policy is applied to an application table. This 'where' clause is used in conjunction with data labels to determine access and provides an easy to use, simple capability similar to creating an Oracle Virtual Private Database (VPD) policy. The 'where' clause is attached to the Oracle Label Security policy, thus there is no need to create a separate PL/SQL package as is the case with pure VPD type implementations.

Oracle Identity Management Integration

Oracle Label Security provides integration with Oracle Identity Management. This feature enables centralized management of policy definitions, data labels and user label authorizations. Oracle Identity Management must be licensed separately for this capability.

Best Practices

Mapping Application Users to Database Users

Oracle Label Security supports common application architectures including situations where the middle-tier connects to the database using a single database account. To accomplish this, Oracle Label Security provides the ability for an authorized user to assume the label authorization profile of another user. The PROFILE_ACCESS authorization is required to execute the SET_ACCESS_PROFILE procedure. Oracle Label Security does not enforce a mapping between a physical database account and the user name specified when establishing user labels. For example, user labels and Oracle Label Security privileges can be assigned to a database user named SCOTT who happens to have a database account or an application user such as JSMITH who is only known to the application layer and doesn't have a real account in the database. The only difference is that when the user SCOTT logs into the database Oracle Label Security will automatically establish an active session label based on levels, compartments and groups assigned to SCOTT. In order for the active session label to be established for application user JSMITH, a call to the Oracle Label Security function set_access_profile is required. This function acts as a proxy for Oracle Label Security and accepts an Oracle Label Security policy name along with an application user name.

Applications can use one of the many Oracle SYS_CONTEXT variables in combination with the SET_ACCESS_PROFILE command. Applications using Oracle Enterprise User Security can pass the EXTERNAL_NAME SYS_CONTEXT value to the SET_ACCESS_PROFILE command.

```
SQL> EXECUTE SA_SESSION.SET_ACCESS_PROFILE
('PRIVACY',SYS_CONTEXT('USERENV','EXTERNAL_NAME');
```

Applications can also pass the PROXY_USER or CLIENT_IDENTIFIER as follows:

```
SQL> EXECUTE SA_SESSION.SET_ACCESS_PROFILE
('PRIVACY',SYS_CONTEXT('USERENV','PROXY_USER');
SQL> EXECUTE SA_SESSION.SET_ACCESS_PROFILE
('PRIVACY',SYS_CONTEXT('USERENV','CLIENT_IDENTIFIER');
```

Note that Oracle Label Security security clearances can be assigned to Database Vault factors such as IP addresses. This capability provides powerful and interesting security deployments for organizations with complex security requirements.

Legacy Data Labeling

Once an Oracle Label Security policy is applied to an application table with READ CONTROL, no rows will be visible until valid data labels have been assigned to each data row. This is because the label tag field will be NULL. You can optionally grant the administrator responsible for labeling the initial data the Label Security authorization FULL. This will allow the administrator to see all rows regardless of the data label and ensure that all legacy data rows are property labeled.

Several methods exist for labeling legacy data. The first method for labeling legacy data simply uses an update statement against the base table.

```
UPDATE SALES SET SECLAB = CHAR_TO_LABEL:('HRSEC','S')
WHERE REGION_ID = 104;
```

This statement updates the SALES table and sets the policy label column SECLAB equal to the internal label tag defined for SENSITIVE in the HRSEC policy where SALES column REGION_ID is equal to 104.

A government (defense) related example would be:

```
SQL> UPDATE LOCATIONS SET SECLAB = CHAR_TO_LABEL('DEFENSE','S')
WHERE REGION_ID = 104;
```

This statement updates the LOCATIONS table and sets the policy label column SECLAB equal to the internal label tag defined for SECRET in the Defense policy where LOCATIONS column REGION_ID is equal to 104.

The second method for labeling legacy data is to switch database connections during the data load. If the policy applied to the SALES table includes the LABEL_DEFAULT option, the users default ROWLABEL value will be used to set initialize the label tag column.

```
CONNECT US_SALES_MGR
INSERT INTO SALES (COL1, COL2, COL3) VALUES ('ACME',.....);
CONNECT EU_SALES_MGR
INSERT INTO SALES (COL1, COL2, COL3) VALUES ('WIDGET',.....);
```

Oracle Data Pump could also be used in a similar method using data exports from the distributed databases. The user specified on the Oracle Data Pump command line would have a default active session label equal to the desired data classification value.

The third method is to write a labeling function using PL/SQL. Oracle Label Security label functions are written in PL/SQL. An example of a labeling function can be found in the Oracle Label Security administrator's guide.

Performance Considerations

Performance is important to all applications. Adding new functionality to existing applications requires due diligence up front to minimize the performance impact. Oracle Label Security provides row level security, basically turning on a security check at each row prior to allowing access. Oracle Label Security will add a delay during login authentication to initialize additional security contexts in Oracle memory. For common application type models, the same delay will be encountered when calling the set_access_profile function. The amount of delay will vary depending on the number of Oracle policies and the number of label components defined. The performance overhead will depend on a variety of factors including:

» Number and size of tables protected by Oracle Label Security

» Oracle Label Security enforcement options used

» Complexity of existing application PL/SQL logic

» Number of Oracle Label Security policies in place

Identifying the tables that require a Label Security policy is an important part of the upfront analysis. If all rows in a table are always accessed, applying a Label Security policy that assigns a data label to each row is not recommended and is probably redundant. Careful consideration of where to apply Label Security policies will result in an efficient use of the technology. In some cases, other Oracle Database security features may be more appropriate for addressing a given requirement than assigning a data label to each row.

Carefully consider the enforcement options you apply to an application table and use only those that are necessary to meet your security requirements. Each additional security check performed by Oracle Label Security will add additional performance overhead.

Oracle also recommends defining the associated label tags so that they fall within the range associated with the level of the data label. For example, suppose the levels Confidential and Sensitive have been defined along with two compartments, Alpha and Beta. The number associated with Confidential is 5000 and the number associated with Sensitive is 10000. When the valid data labels are defined the associated label tags associated with the level of Confidential and compartments Alpha and Beta should be between 5000 and 10000. For example, the data label Confidential:Alpha might have a label tag of 5050 and the data label Sensitive:Alpha,Beta might have a label tag of 10055.

Oracle partitioning can be used with Oracle Label Security to physically partition data based on data classification. For example, data with a classification of Highly Sensitive can be located in a separate partition from data with a classification of Sensitive. Partitioning can also provide performance benefits through partition elimination, enabling Oracle Label Security to quickly skip data that resides outside of the users' security clearance. This is especially applicable to data warehouse environments where it will provide query optimization through partition elimination. This is particularly useful for large tables. Oracle Label Security will quickly skip data that resides in partitions outside of the user's label.

The example below would place all data with label tags less than 2000 in partition sx1, all data with label tags less than 3000 in partition sx2, and all data with label tags less than 4000 in partition sx3. Partitioning based on the data label also physically separates data at the storage level based on its sensitivity.

```
CREATE TABLE EMPLOYEE (
EMPNO NUMBER(10) CONSTRAINT PK_EMPLOYEE PRIMARY KEY,
ENAME VARCHAR2(10),
JOB VARCHAR2(9),
SEC_LABEL NUMBER(10))
TABLESPACE PERF_DATA
PARTITION BY RANGE (SEC_LABEL))
(PARTITION SX1 VALUES LESS THAN (2000) NOLOGGING,
PARTITION SX2 VALUES LESS THAN (3000),
PARTITION SX3 VALUES LESS THAN (4000) );
```

Existing composite indexes can be modified to include the policy column added by Oracle Label Security. This can substantially improve performance for complex queries.

Should any user or stored procedure need access to all data it is recommended that the user or stored procedure be given the Oracle Label Security specific privilege READ or FULL. This will help reduce overhead and increase performance.

When labeling new data, Oracle Label Security label functions will have the most performance overhead as they will invoke an internal database trigger. Using the LABEL DEFAULT enforcement policy option will have the least performance overhead.

Depending on the application usage, consideration should be given to creating bitmap indexes on the column added by Oracle Label Security to the application table. The percentage of unique labels compared to the number of data rows is usually low. Bitmap indexes will slow down data loads but increase performance on select statements.

Conclusion

Data classification plays a vital role not only in enforcing the principle of need-to-know but also in securely consolidating sensitive data. Historically, sensitive data has been stored in physically separate systems. However, this approach has limited the ability to perform advanced analysis and business intelligence.

Oracle Label Security provides the industry's most advanced and flexible data classification solution. Using a policy based architecture, Oracle Label Security provides the ability to define data labels, assign security labels and protect application tables within the Oracle Database, reducing operational and storage costs by enabling different sets of data with different levels of sensitivity to reside in the same database. Oracle Label Security policies provide the ability to define custom data labels for virtually any industry ranging from healthcare to law enforcement to defense, reducing the cost of developing or re-coding applications to meet row level access control requirements based on clearance levels. Flexible enforcement options allow access control to be finely tuned to meet a variety of compliance and regulatory requirements.

Management of Oracle Label Security policies can be performed using Oracle Enterprise Manager and integration with Oracle Identity Management provides centralized enterprise management. Oracle Label Security has been

independently evaluated under the international common criteria at EAL4+ and complies with government and commercial requirements for highly secure products.

ORACLE

Oracle Corporation, World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065, USA

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

White Paper Title
March 2018
Author: [OPTIONAL]
Contributing Authors: [OPTIONAL]