Oracle Label Security

Label Security enforces row-level access controls by classifying data based on sensitivity, ensuring users can only access authorized information. This allows organizations to reduce operational and storage costs by securely storing data of varying sensitivity levels within a single database.

[1.0]

PURPOSE STATEMENT

This document provides an overview of features and enhancements included in the latest releases of Oracle Label Security. It is intended solely to help you assess the business benefits of using Oracle Label Security preventive controls and to plan your Data Security and IT projects.

DISCLAIMER

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

Table of contents

INTRODUCTION

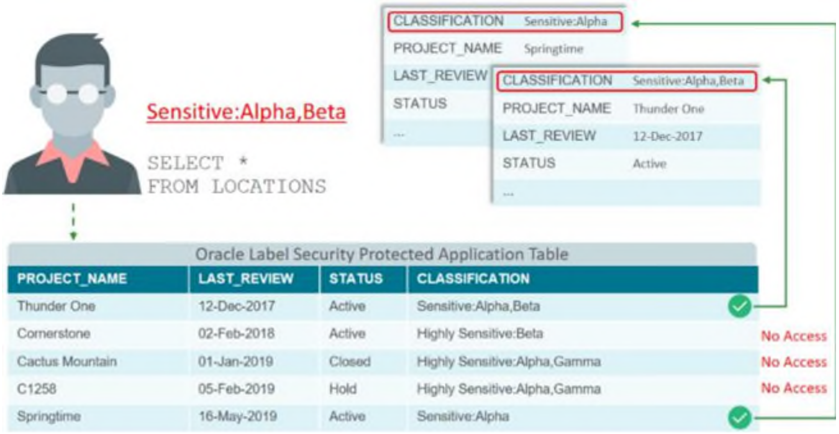
Over the past 40 years, Oracle has been the industry leader in building innovative data security solutions that make it possible to protect sensitive information. Oracle Label Security is part of Oracle's defense-in-depth approach to security and is the industry's most advanced solution for controlling access to data based on data classification. While this technology was designed to meet US government, military, and intelligence agency standards, Label Security also applies to commercial organizations with user data separation requirements. Both government and commercial organizations use Label Security to consolidate multiple databases to reduce operational costs and simplify data analysis and decision-making. Government agencies align their data classification standards and then use Label Security to share data across agencies. Commercial companies use Label Security to separate data from different nationalities, allowing users from various countries to access data and meet local privacy and compliance requirements. Other companies are consolidating similar databases from subsidiaries and retail outlets that require limits on what is visible to each group. Label Security can be used with vector data to limit searches to only authorized data rows. Label Security has out-of-the-box features to enable these and similar use cases.

Label Security mediates access based on data sensitivity labels (referred to in this document as data labels) and user label authorizations (referred to as user labels). Label Security has consistently been evaluated as part of the Oracle Database to the Common Criteria for Information Technology Security Evaluation (ISO15408). Oracle Label Security is easily managed using API calls or Oracle Enterprise Manager.

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 sensitive data from different databases in one system. Label Security provides the ability to tag data with a data label or a data classification. This capability allows the database to know what data is appropriate for each user and enforce security controls. Data can also be labeled with a degree of sensitivity (known as a level). For example, in government and defense applications, data might be labeled unclassified, secret, or top secret. In contrast, a healthcare application may label data as public, confidential, restricted, or highly restricted.

Label Security enforces access controls by comparing a data classification label with a user's access clearance. Access clearance can be considered an extension to standard database privileges and roles. For example, a pervasive database operation is to GRANT the SELECT privilege on an application table to a user or a role. With this privilege, the user or role can select all the rows in the table. To restrict access to highly sensitive data rows, two things must occur: First, the database must know what data is considered highly sensitive. Second, the database must know the user's access clearance. 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 to achieve this functionality was based on database views, triggers, and lookup tables. However, that approach required extensive application changes and resulted in inconsistent implementations. Label Security is built-in and enforced within the database, below the application layer, providing stronger security and eliminating the need for application views and triggers. This enforces access rights across all applications that connect to the data, including reporting and business intelligence tools that generally require their own security model.



Oracle Label Security Protected Application Table

PROJECT_NAME	LAST_REVIEW	STATUS	CLASSIFICATION	
Thunder One	12-Dec-2017	Active	Sensitive:Alpha,Beta	✓
Cornerstone	02-Feb-2018	Active	Highly Sensitive:Beta	No Access
Cactus Mountain	01-Jan-2019	Closed	Highly Sensitive:Alpha,Gamma	No Access
C1258	05-Feb-2019	Hold	Highly Sensitive:Alpha,Gamma	No Access
Springtime	16-May-2019	Active	Sensitive:Alpha	✓

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

Label Security is an established Oracle product that can address simple to complex requirements. Proper analysis and planning are key to a successful Label Security deployment, as with any other sophisticated security product. The steps below provide a basic guideline for deploying Label Security. The implementation can be performed using Oracle Enterprise Manager or the Label Security API. First, it may be helpful to begin with a sample demonstration table to understand how data labels mediate access control and the various enforcement options available in Label Security.

Oracle Label Security Implementation Steps

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

This paper focuses on 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. These components are used to create data labels and assign user labels to database or application-type users. Levels are ordered from more sensitive to less sensitive. Compartments are independent and used to segregate data within a given level. Groups are used to segregate data organizationally within a given level. Groups can have an inherited or parent-child hierarchical relationship, where having access to the parent Group provides access to the child Group. A given data label must have at least one Level, zero or more Compartments, and zero or more Groups. A single default Level must be created for user or data labels for deployments using only Compartments or Groups.

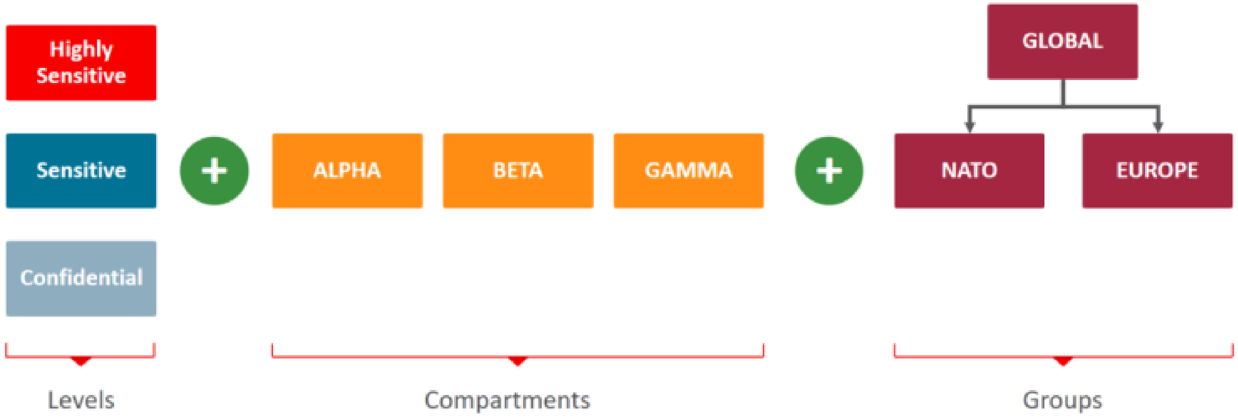


Figure 2. Oracle Label Security data levels can include levels, compartments, and groups.

Oracle Label Security - Data Label Components

LABEL COMPONENTS	DESCRIPTION
Level	The level is a component that denotes the sensitivity of the data. Every data and user label must have a level. An organization might define levels such as Confidential, Sensitive, and Highly Sensitive. Even if an organization does not need to use levels, a single default level must be defined.
Compartment	The compartment component is optional and is independent of each other. 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, such as HR, Finance, or Accounting.
Group	The group component is optional and is very similar to a compartment, except each group can have a parent-child relationship (hierarchy). Groups are most often used to segregate data by organizational structure or region, such as Europe with child groups of France and Portugal or North America with child groups of the US and Canada.

Examples of industry-specific policies and data labels

INDUSTRY	LEVEL	COMPARTMENT	GROUP
Government and Defense	Confidential Secret Top Secret	Operation Unified Assistance 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 NA, Canada, USA EMEA, France, Portugal, Germany LATAM, Mexico, Brazil, Argentina
Health Care	Public Confidential	Patient Doctor	Lab Technician Medical Assistant
Retail Financials	Default*	None	Each Store, Country, Region, Financial Group

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 default level must be set.

Using Data Labels

Determining your organization's data label requirements is the first and most crucial step in planning your Label Security deployment. This means deciding what Levels, Compartments, and/or Groups you require to protect your information. Determining your data label requirements generally means analyzing your application and identifying the tables you plan to protect with Label Security. This is best accomplished with an application administrator or developer who knows the application schema. In most cases, only a small percentage of the application tables require a Label Security policy. Once the candidate tables have been identified, the data contained in the tables will need to be evaluated. A data analyst or someone who understands the data may be required. It is recommended that future application data be considered as well. This will create a robust set of initial label components.

A Label Security policy can have up to 9999 levels, compartments, and groups. However, many commercial organizations use only a single default level, whereas a government or defense implementation might use between two and five levels.

The text-based representation of a data label uses colons and commas to separate the 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] has the single required level called Default and the group US.

Internally, Label Security uses a numeric identifier called a label tag for each data 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 have the column appended to an application table as a visible or invisible column. Appending the column as an invisible column will eliminate any possibility of existing select, insert, or update statements failing because the SQL statement didn’t qualify the names of the columns in the statement. It is important to note that the Label Security policy column can pre-exist in an application table before applying a Label Security policy. The application table column data type must be number (10) to take advantage of this. This allows applications to be designed with a built-in Label Security policy column.

Required User Authorizations for Label Components

LABEL COMPONENTS	DESCRIPTION
Level	The user must be authorized to the level or higher. For example, 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.
Compartment	The user must be authorized to access all compartments listed on the data label. For example, to access data labeled “Sensitive:Alpha,Beta,” the user must have been authorized to at least the “Sensitive” level and 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	The 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, 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 group so the North America group can also access the data. The colon separates the label's level, compartment, and group sections. 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.

If the application has an entity-relationship (ER) diagram, annotating the range of data labels for each entity on the diagram may be helpful.

User Labels

User labels determine whether a user can access information protected with a data label. User labels comprise 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 a VPN, the session label may be restricted to the Sensitive level.

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

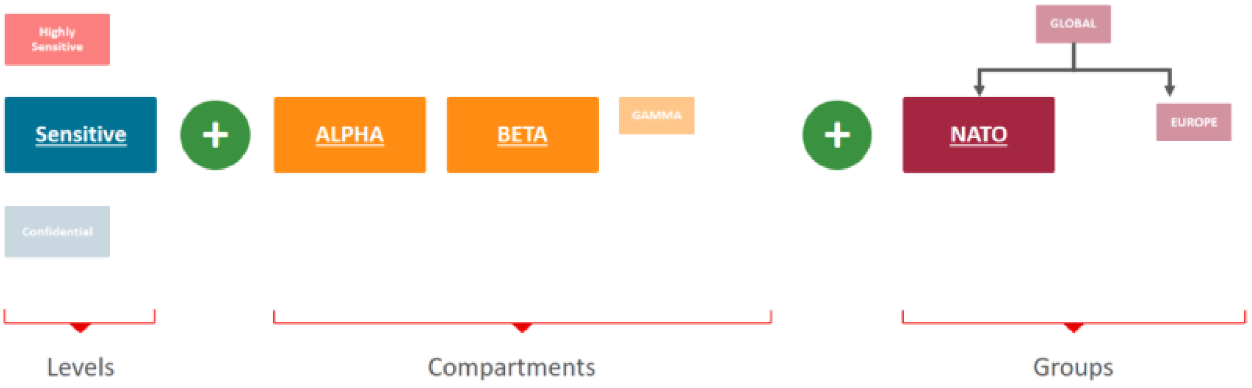


Figure 3: User Label Components include Levels, Compartments and Groups

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 essential to prevent data from being assigned a sensitivity label that no user can access. In other words, the information required to perform a specific job responsibility might be out of reach to the application user due to their user label. In the worst case, data might be assigned a data label that no user can access, effectively hiding the data.

Sample 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**
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

Implementers must review and document the information gathered. This should include a list of application tables that need to be protected, the reason why, and a list of label components and their meanings. This information will also help inform the application of other security controls, such as Oracle Database Vault Realms or Command Rules, Oracle Data Redaction Policies, Oracle Data Masking Definitions, and Tablespace Encryption. This document should become part of the enterprise security policy, be considered sensitive, and be kept safe.

LABEL SECURITY ADMINISTRATION

Installation Guidance

Label Security is installed with the Oracle Database by default but not configured or enabled. You can configure and enable it using the Oracle Database Configuration Assistant (DBCA) or the command line. Follow the steps in the documentation to create Label Security policies, levels, compartments, and/or groups.

Enable Label Security in the pluggable databases (PDBs) where you plan to create Label Security policies. You cannot create policies in the root compartment because Label Security is not designed to protect data dictionary objects.

Administering Users and Roles

The LBACSYS account contains the data dictionary that stores Label Security policies, data labels, protected objects, enforcement settings, and user security clearances. LBACSYS stands for Label Based Access Control SYS. Beginning with Oracle 19c, LBACSYS, like other Oracle-provided accounts, is configured as a schema-only account. When you use Label Security, the database security officer will need to run the ALTER USER command to provide a password to LBACSYS so the Label Security administrator can access the account to grant LBAC roles to named users. Once the Label Security administrator has completed granting roles, the database security officer can rerun ALTER USER to turn LBACSYS into a schema-only account. Oracle recommends that customers not use LBACSYS to manage Label Security since this is a shared account and will not be able to audit end-users correctly. As a good practice, grant the LBAC_DBA database role to trusted users who will administer Label Security for day-to-day use.

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 Label Security specific database roles and by granting privileges on specific administrative packages. In addition to holding the metadata associated with Label Security, the LBACSYS account will have several dozen procedures and functions.

Label Security allows for delegated administration. When a Label Security policy, “POLICYNAME,” is created, a new database role, POLICYNAME_DBA, is also created. That role can then be used to manage policy label components and label authorizations and should be granted to a named user responsible for managing the policy.

Label Security Enforcement Exemptions

The following exceptions are essential to understand when using Label Security policies.

Label Security enforcement exemptions

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

Trusted Stored Procedures

A trusted stored program unit is created the same way that a standard procedure, function, or package is created. The program unit becomes trusted when you grant it Label Security privileges. The Label Security privileges granted to a user can also be granted to a trusted stored procedure. Doing so enables access to data within the execution context of a stored procedure but not directly by the user calling the stored procedure or function.

Label Security and Database Vault Capability

Many Label Security functions can be used within Oracle Database Vault rule sets 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 a finer-grained separation of duty capability.

Label Security and Virtual Private Database Capability

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

Label Security and Data Redaction Policies

Label Security can also be used with Data Redaction to help decide if a redaction policy will be applied. For example, a Data Redaction policy can be applied where the Label Security user session label allows access to redacted or unredacted data.

BEST PRACTICES

Mapping Application Users to Database Users

Label Security supports common application architectures, including “n-tier” applications that connect to the database using a single database account. To accomplish this, Label Security allows a session label to be set based on an application user instead of the database schema user. The application user’s session label may equal the database user’s session label or a subset. For example, the application user may have access to one Compartment and one Group instead of multiple compartments and groups.

Labeling Existing Data

If data labels are not populated in the label tag for existing data, no rows will be visible once a Label Security policy is applied to an application table. 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 existing data rows are correctly labeled.

The following are methods to apply data labels to existing data:

1. SQL UPDATE statements that populate the controlled table's label tag based on the current user's session label.
2. Use a database user with the required session label and populate the table with the data. If the Label Security-controlled table has an active policy, the session label will be applied to the data as it is loaded. Oracle Data Pump could also be used with this method to import data from other databases.
3. Write a PL/SQL function to label the rows based on the data's characteristics and the session's context.

Performance Considerations

Performance is essential to all applications. Adding new functionality to existing applications requires careful planning and due diligence to minimize the impact on performance. Label Security enforces a security check on each row before allowing access and during login authentication to initialize additional security contexts. The delay will vary depending on the number of Oracle policies and the number of label components defined. Performance will depend on a variety of factors, including:

- Number of Label Security policies in place
- Number and size of tables protected by Label Security
- Label Security enforcement options used
- Complexity of existing or new application PL/SQL logic

Identifying the tables that require a Label Security policy is an integral part of the pre-implementation 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. For example, if all rows are always accessed, using Oracle Database Vault to control when, where, why, and how a table is accessed may be more efficient than labeling every row. Each additional security check will add performance overhead regardless of the feature or functionality.

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 related to Sensitive is 10000. When the valid data labels are defined, the 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 Label Security to physically partition data based on data classification. For example, data with a Highly Sensitive classification can be located in a separate partition from data with a Sensitive classification.

Partitioning can also provide performance benefits through partition pruning, enabling Label Security to quickly skip data that resides outside the users' security clearance. Partitioning is widely used in data warehouse environments or applied to large tables where it provides query optimization through partition elimination, and Label Security can also leverage it. Label Security will quickly skip data in partitions outside the user's label.

Existing composite indexes can be modified to include the policy column added by 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 they be given the Label Security specific privilege READ or FULL. This will help reduce overhead and increase performance.

The LABEL DEFAULT enforcement policy option will have the least performance overhead when labeling new data.

Depending on the application usage, consideration should be given to creating bitmap indexes on the column added by 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 is vital in enforcing the need-to-know principle and 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.

Label Security provides the industry's most advanced and flexible data classification solution. Using a policy-based architecture, 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 varying sensitivity levels to reside in the same database. 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.

Oracle Enterprise Manager can manage Label Security policies. Label Security has been independently evaluated under international common criteria and complies with government and commercial requirements for highly secure products.

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 facebook.com/oracle twitter.com/oracle