Secure Data Mining in Oracle Database 10*g*

Know More, Do More, Spend Less

An Oracle White Paper
May 2005

Secure Data Mining in Oracle Database 10*g*

Know More, Do More, Spend Less

Secure Data Mining in Oracle Database 10*g*

Know More, Do More, Spend Less

In this paper, we present the advantages of Oracle Data Mining (ODM) over traditional methods in enabling secure, embedded, predictive capabilities for enterprise applications. We first present the business motivation for using ODM for advanced analytics, followed by a short technical presentation of the product, and finally, its compliance with the overall Oracle10*g* security framework.

MOTIVATION

The most innovative, successful, global companies consider their corporate data, their applications, and business processes built around this data to be their strategic and competitive assets. For such organizations, given globalization and round-the-clock Internet-based business activity, 24x7 availability of reliable information and intelligence is a core requirement. Severe corporate governance and structural failures over the last decade have dramatically increased U.S. and international regulatory requirements. Further, data privacy issues and the constant specter of random domestic and foreign threats have made information security mission-critical for a company's IT infrastructure. In sum, companies must guard their corporate assets even more closely, but at the same time, extract new insights and opportunities from the information/data flow, in real-time, to stay competitive.

Technology Imperatives

These developments have introduced new technology imperatives for data management over and beyond the traditional requirements of scalable transaction processing, content management, high availability and so on.

- **Data Integration and Quality** – the need for integrating data from disparate silos into a cohesive whole that reflects the most current state of the enterprise. Also, as part of this integration process, the need to validate and clean the data so that each source adds definitive value, rather than noise, to the corporate knowledge base.
- **Business Process Management and Controls** – the need for passive and active audits, controls and oversight at key stages of information flow and processing, with elevated levels of individual (as opposed to just corporate) accountability.

- **Embedded Business Intelligence** – the need for rapid, interactive, accurate reporting on key performance indicators for various business activities, the need for gathering summarized intelligence from warehoused operational data, and the need to embed this intelligence back into the operational stream.
- **Embedded, Predictive Intelligence and Advanced Analytics** – the need to sift through structured and unstructured (predominantly, Text) data to find new, non-obvious, hidden information to help the organization discover patterns and make predictions about *future* events. Also, the need to embed this intelligence back into the operational stream, and to repeat this process in a virtuous cycle as new data arrives into the flow.
- **Security** – the need for secure internal and external access to the data and information across the enterprise, with much finer grain access control to sensitive information than traditional mechanisms.

Oracle addresses all facets of such complex, large data management problems through a broad array of technologies spanning the Oracle Database 10*g*, Oracle Application Server 10*g*, and Oracle E-Business Suite 11*i*. This paper focuses on Oracle Data Mining and its ability to address the needs of secure advanced analytics for mission-critical data management.

Example Applications

First, we will briefly highlight how ODM can help in a few hotbeds of IT activity in recent times, where the need for secure and integrated analytics is most urgent.

Finance

The *Sarbanes-Oxley Act* (2002) holds the CEO and CFO of every large, publicly traded company (including its domestic and foreign subsidiaries) personally accountable for providing investors with accurate, transparent, and complete financial statements by virtue of ensuring compliance of enterprise-wide financial controls and business processes with the Act. Of the many directives in the Act, Sections 302 (Corporate Responsibility for Financial Reports), 404 (Management Assessment of Internal Controls) and 801 (Corporate and Criminal Fraud Accountability) impact the company's (disparate) financial and operational systems the most. These directives mandate that reports should be based on a single version of the truth about the company's fiscal health – at greater frequency, and shorter reporting time windows – starting from the year 2005.

Using Oracle Data Mining and other built-in statistical capabilities in the Oracle database, you can embed intelligence into your mission-critical applications to:

♦ detect noncompliant and fraudulent transactions/activities
♦ develop user/customer/account profiles
♦ find association relationship of co-occurring items and/or events for audit
♦ mine unstructured (Text) documents for nuggets of information

- clean your data for subsequent analysis or processing
- identify key data elements that affect or influence target performance metrics

Banking

The *BASEL II New Accord* (2003) is a regulatory framework agreed upon by the central banks in the G-10 nations to leverage recent advances in financial theory and IT and incorporate risk measurement into their daily business practices – by the year 2007. The Accord seeks to strengthen existing capital adequacy standards by introducing more sensitive metrics for credit and market risks, and new capital requirements for operational risk. The three "pillars" of the Accord – viz. Minimum Capital Requirement, Supervisory Review Process, and Market Discipline and Reporting – detail requirements for the supervisory review process, outline external disclosure standards, and place greater oversight responsibility and market-based discipline on the bank's management. This is the stick, now the carrot. Adequate compliance with the accord will allow the bank to maintain lesser reserves to cover for credit risks. This reduction in reserves can translate to billions of dollars/euros/yen of unfettered capital for the bank.

Besides the applications discussed under the area of finance, ODM can be used in conjunction with other analytical features in the RDBMS for:

- computing the probability of default (PD) for credit risk
- various scoring and predictive applications such as application scoring, behavioral scoring, profit scoring, collection scoring, bankruptcy prediction
- exploratory data analysis and preprocessing
- computing various performance metrics and statistics on borrowers

Health Care

Today, HMOs and various health care agencies spend (or plan to spend) millions of dollars on data integration and privacy protection of sensitive patient, employee, and research data. Ironically, many then resort to analysis techniques or tools that require extraction or download of this sensitive data into less secure file systems or removable media. Then they spend more time and resources integrating the results of analysis back into their operational data stream. This is inherently inefficient and insecure. For many customers, and particularly many of the Fortune 500 health-care organizations that use the Oracle platform, the more logical and cost-effective path is to use the secure, powerful, built-in analytical features in Oracle.

There is incentive for this approach on the regulatory front also. The Health Information Portability and Accountability Act (HIPAA, 2002) is a privacy law enacted by the U.S. Congress to protect consumers from having their personal health information exploited by insurance companies, employers, and other enterprises – legitimate or otherwise. HIPAA regulations affect any health information that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse. HIPAA mandates administrative, physical and technical safeguards for secure internal and external access to healthcare information. Large providers must comply with HIPAA by 2005, and all providers, big and small, by 2008.

Oracle Data Mining can help health-care organizations:

- detect noncompliant and fraudulent activities, particularly in insurance.
- identify likely targets and promising leads in clinical diagnostics or drug research
- discover new clusters or segments in a population under study
- develop user/patient profiles
- mine unstructured data and the reams of documents typical in health care

Government

The U.S. Government currently ranks in the top-tier of worldwide organizations in new IT infrastructure and R&D investments. The U.S. Dept of Homeland Security (DHS) has the unenviable charter of bringing together 30+ disparate agencies, and unifying their IT infrastructure under a single cohesive, intelligent information framework. The Transportation Security Administration (TSA), Bureau of Citizenship and Immigration (BCIS), Federal Bureau of Investigation (FBI), Dept of State and various civilian and military Intelligence agencies have mission-critical requirements for information integration and analysis under the most stringent security constraints. The demanding needs of these organizations elevate the phrase "actionable intelligence" to an entirely different level of significance.

ODM finds several applications in this domain, chief among them being:

- electronic intrusion detection on networks and IT infrastructure
- identifying/profiling suspects at border crossings and ports of entry and exit
- analyzing/detecting fraudulent, suspicious activities
- finding association relationship of co-occurring items and/or events
- as part of a toolkit for cyber forensics – the discipline that is used in post-crime analysis of data obtained from occurrences of cyber fraud, libelous/malicious email, intellectual property theft, misuse of computing resources, among others.

Other federal agencies such as the Internal Revenue Service (IRS) and the National Institutes of Health (NIH) also need one or more of the advanced analytical requirements discussed above.

Note that, besides these specific applications, ODM can find use in traditional CRM applications in all of the above scenarios, besides Telecommunications, Retail and other areas. Some popular use cases include:

- Anticipate and prevent customer attrition
- Acquire new customers and identify the most profitable customers
- Identify promising cross-sell and up-sell opportunities

Given this motivation, the rest of the paper is organized as follows. The next section introduces the technical features and key differentiators of ODM. The subsequent section walks through a comprehensive list of security features offered by the Oracle10*g* platform, and discusses how ODM fits/complies with these features. The paper concludes with a benefits summary, and references.

ORACLE DATA MINING

Oracle Data Mining is scalable, powerful, data mining software built into the Oracle Database.

Traditional approaches for data mining include:

- client-server tools that operate on data extracted from the corporate database into local client file systems, or
- web-integrated tools that mine data accessed across loosely coupled systems, or
- mining engines that are packaged with, but not fully integrated into the database.

These products involve data transfer from the database (either the mission-critical OLTP system or a data warehouse) to the analytics engine, possibly with several data transformation engines/steps intervening between the two entities. They also involve subsequent transfer of results (models, summarizations) to the production system for deployment (i.e. for scoring new data and/or analysis). Besides the obvious cost of managing such multiple, dedicated islands of data, the lack of consolidation and data movement between these islands renders the overall system inefficient at providing a holistic view of enterprise data, and a system that is inherently insecure.

A fundamental strength of Oracle Data Mining is that its mining server is a *cohesive, integral component of the RDBMS platform*, designed to leverage and extend all the powerful capabilities of the database engine for scalability, security, performance, and availability over incremental releases of the product. All analytical functions and powerful mining algorithms like Support Vector Machines, Association Rules, and Decision Trees operate directly on the data stored in the database and are implemented based on the database kernel primitives. The resulting mining models are stored and managed in the database, and they can be used to score new data and/or retrieve summarizations and analysis through industry-standard SQL and widely used Oracle interfaces and tools.

The same Oracle10*g* platform offers complementary technologies for BI such as relational and multi-dimensional OLAP, analytic/aggregate/window/forecasting functions, data partitioning, parallelism, materialized views, ETL (extract-translate-load), bit-mapped indexes, and star schemas. The Oracle Application Server 10*g* supports BI Reporting, development tools and Portals. Along with Oracle's traditional OLTP strengths, all these parts combined to enable consolidation of mission-critical data into one common, secure, scalable Oracle10*g* BI platform.

ODM is available as an option to the Oracle Database 10*g* Enterprise Edition. It consists of Data Miner – a GUI wizard for business analysts; Native Oracle SQL Prediction functions; PL/SQL packages for building and deploying models; and a standards-based Java API for J2SE/J2EE-based application development. ODM is integrated into Oracle BI tools such as Discoverer and third-party BI tools from SPSS™, SAP™, Inforsense™ and others.

ORACLE10*G* – A SECURE PLATFORM FOR DATA MINING

Oracle10*g* offers the most comprehensive, standards-based, N-tiered security architecture and capabilities. The Oracle Security Platform consists of Oracle Database 10*g* and Identity Management (a component of Oracle Application Server 10*g*). The database protects the raw data with its support for object privileges, roles, fine-grained access control, label-based security, and data encryption. The Database, E-Business Suite 11*i*, Collaboration Suite, Portal (a component of Oracle Application Server 10*g*), and third-party applications can leverage Identity Management to centrally manage authorizations for the entire enterprise, and as a single point of integration.

By virtue of its integration into the platform, Oracle Data Mining complies with many of Oracle10*g* security capabilities.

Security in Oracle Data Mining

Oracle Data Mining supports multi user access to models, with certain caveats.

Mining Models

Mining models can be created in individual database user schemas (such as HR, AP, AR, and so on), but their privilege-based security is more stringent than on other database objects. Unlike tables and views, access privileges (`CREATE`, `DROP`, `READ` etc.) cannot be granted on mining model objects. Instead, models can be exported from a (source) schema into another (target) schema.

To illustrate this, consider two user schemas, A and B – where A owns (by virtue of creating) the model `modA`, and B owns the table `tabB` that is to be scored using the model. The simplest way to make this happen is for user A to export the model `modA`, and for user B to import the model into his/her schema and score `tabB` using the model. Note that the imported model is as good as one owned by B in that, B can rename or drop this imported model.

Java API

In Release 1[1] of Oracle Database 10*g*, the DBA must enable a DMUSER_ROLE for every user of the Java API – as an added security mechanism for metadata related to the API. In Release 2, the Java API follows the same invoker's rights semantics as the PL/SQL packages by virtue of being layered on the same server foundation.

Thin or thick (i.e. OCI-based) JDBC can be used to connect to the database, but the API is compatible with thin JDBC features. The user/session associated with the database connection object should have the necessary privileges to read tables and views and to create new objects in their current schema.

[1] Implies 10.1.0.4, as of this writing. Please upgrade to the latest 10.1.0.4 patch release.

Data Miner

Oracle Data Miner is a client-based GUI tool, available for downloads from the Oracle Technology Network. This tool is layered on the Java API in Release 1, and hence governed by the same security requirements as the Java API. In Release 2, this tool can generate both Java and PL/SQL code.

PL/SQL Packages

The PL/SQL packages in ODM support *invoker's rights* privileges similar to other built-in packages shipped with the RDBMS. This enables their reuse across all user sessions.

Each procedure or function in the package(s) that requires a table or view as user input also accepts the schema name as an optional input (the default is the current user schema). If the user (schema/session) that invokes a procedure or function has read access to the tables in a given schema name, and if the tables exist in those schemas, the operation(s) will succeed without privilege related errors.

Some of the procedures create output objects (tables and views) containing results of the operation. For these to succeed, the invoking user session must have privileges to create tables and/or views (unlike earlier releases, Database 10*g* requires the administrator to explicitly provide these privileges). Note that creation of objects happens only in the current user's schema. In other words, there is no optional schema name parameter for output objects. These procedures create entire objects with predetermined schemas. They do not populate pre-existing tables or views. The name of the object to be created is required as input.

The PL/SQL packages do not require any special roles or access privileges beyond the regular schema privileges assigned for any user to run the sample programs.

SQL Prediction Operators

Oracle Data Mining supports powerful SQL operators to score new data using mining models, such as `PREDICTION`, `PREDICTION_PROBABILITY`, and more (See the Database 10*g* Release 2 SQL Reference for syntax). These operators enable real-time scoring and natural pipelining of the scoring results into other wrapping SQL statements or applications, without the need for creation of output objects as seen in operations such as `APPLY`, `COMPUTE_*`.

These operators support schema extended model names, which may appear counter-intuitive, given that ODM does not yet support privilege assignments for model objects. But there are a few instances where this feature can be used to provide a semblance of sharing of models, especially if model export/ import is not a preferred solution.

Consider the example discussed above, where user A owns the model and user B owns `tabB` – the table that is to be scored using the model `modA`. If B can grant SELECT privileges on `tabB` to A, then A could create a view representing the query that scores `tabB` based on `modA`, and grant SELECT privileges on the view to B. This will enable B to obtain scored results on `tabB` without needing to import `modA` into its schema. An example view provided by A can be created as follows:

```
CREATE VIEW ScoreView AS
SELECT PREDICTION (A.modA USING *) FROM B.tabB;
```

Note that user A can enable other user schemas to score `tabB` by granting SELECT privileges on the view `ScoreView`.

Metadata Security and Administration Tasks

Oracle Data Mining has a dedicated schema, called DMSYS, to maintain its metadata and other secure entities. This *pseudo*-SYS schema should be activated only by the DBA after a product installation. Similar to the SYS schema, objects under this schema should *never* be directly accessed or modified.

Mining models are stored in a collection of database objects such as tables, indexes, synonyms and views that have obfuscated names with proprietary prefixes. By virtue of their presence in the user's schema and table-space, these may show up as user-owned objects in catalog views. But the contents of these objects are meaningless and intended to be opaque to the user. It is the responsibility of the user/DBA to ensure that these objects are *never* directly accessed or modified by any user application.

The DBA has to perform a few administrative tasks to make the Java API and Data Miner available for general use. In Release 1, a separate role called DMUSER_ROLE has to be created (using the script `dm/admin/odmcrt.sql`), and every user of the ODM Java API or Data Miner must be granted privileges on this role. This is no longer a requirement in Release 2. Additionally, some schema level privileges have to be granted to enable users to run the data mining samples (which involve creation of output objects). These are listed in the script `dm/admin/odmusr.sql` in Release 1, and documented for Release 2.

ORACLE DATA MINING AND THE ORACLE10*G* SECURITY PLATFORM

Given an idea of the database user level security for mining models, the following technical sections discuss ODM compliance (and any limitations thereof) with other key features in the Oracle Security Platform – starting first with Database features, and then looking at N-tier security capabilities.

Row-level security and Virtual Private Database

Row-level security and virtual private database are synonymous with *fine grained access control* (FGAC) discussed in other Oracle literature. The fine-grain access alludes to row-level security enforcement – where users can be enabled to access only a select range of rows in a table, and VPD refers the prevalence of this technique in building hosted/ASP, or virtual private, databases.

The traditional means of securing access to whole or parts of objects such as tables by a set of users involves defining multiple user views with different privilege assignments, with database triggers and/or application logic enforcing a security policy. FGAC avoids this inherently complex, brittle infrastructure by requiring just two entities – the table/view/synonym that is to be accessed by multiple users, and a PL/SQL routine implementing the security policy (VPD policy) to be associated with this object. In Oracle10*g*, the VPD policy specification has been enhanced to support column level security – when this policy is enforced, users can be enabled to see all rows of a given table that they have access to, but with values of protected columns masked out as NULLs. See Oracle documentation on FGAC and `DBMS_RLS` package for details.

ODM can build models from, and score data present in, tables enabled for FGAC. The foundation APIs accept table and schema name as inputs for model build, test and scoring operations. All routines that read the FGAC-enabled table will follow the security policy imposed on the invoking user session. However, security policies cannot be specified on output objects because they get created only in the invoking user's schema, and the outputs are not populated into pre-existing tables or views – they are created in whole. You can define security policies on the output objects for use by other applications after the relevant operation completes.

Label Security

Trusted environments such as Defense, Intelligence, R&D and other institutions involved with highly sensitive data require selective access control based on a user's level of security clearance to ensure confidentiality without overbroad limitations. Oracle10*g*'s label security infrastructure addresses this requirement by associating a label (column) with the object to be secured, and an adjoining label-based security policy to be implemented by the user. Labels are strings of the format: <sensitivity ranking :: compartment :: group> that enable definition of sophisticated hierarchical access control rules beyond those of object-level discretionary access control by using data in the row. When a policy is applied, a new column is added to each data row. This column will store the label reflecting each row's sensitivity within that policy. Level access is then determined by comparing the user's identity and label with that of the row.

Each policy that is applied to a table creates a column in the database. By default, the data type of the policy label column is NUMBER. The act of creating a policy does not in itself have any effects on tables or schemas. Applying the policy to a table or schema is what does it. The administrator can decide not to display the column representing a policy by applying the HIDE option to the table. After a policy using HIDE is applied to a table, a user executing a `SELECT *` or a `DESCRIBE` of the object in SQL*Plus will not see the policy label column.

ODM handles objects enabled for label security in the same manner as discussed in the section on FGAC. If the label column is hidden in the input tables, then the ODM APIs will not treat such a column as an attribute to be mined. In the event that the label columns have to be exposed, the user can define a secure view that does not project this column, and use that as input to ODM. Output objects resulting from mining operations can have the label-based security enforced on them after their creation.

Transparent Data Encryption

Database 10*g* Release 2 supports transparent data encryption – a powerful and convenient feature that automatically encrypts database column data before it is written to disk. The DBA can simply alter a table, specifying the columns to be encrypted based on a wallet and an authenticator. All the data in the columns will be encrypted, and subsequent encryption and decryption of data is performed in SQL, completely obviating the need for triggers and other calls to encryption APIs. ODM can mine encrypted columns, with the caveat that the stored model contents may not be fully encrypted. For the present time, these models will need to be protected using the mechanisms discussed earlier.

Auditing

Oracle audit facility allows businesses to audit database activity by statement, by use of system privilege, by object, or by user. The granularity and scope of audit options allows users to record and monitor activity without incurring the performance overhead associated with a general, external, auditing mechanism that may intercept and log all statements, and then filter out the ones of interest. Oracle10*g* provides support for fine-grained auditing of SQL Query and DML statements by the ability to define and associate auditing policies with operations.

Mining models generated by ODM are not yet auditable using the common (SQL DDL-based) mechanisms for database objects like tables and views. However, event notification routines can be written in PL/SQL or Java, layered on mining APIs to notify occurrence of operations such as model creation, apply and so on.

Secure Application Role

A secure application role is a role implemented by a package. This package can perform validations to ensure that certain conditions are met before the user can exercise privileges granted to the role in the database; and the database ensures that only this package can determine the correct access conditions. The key benefit of this feature is that it provides a mechanism to secure access to the data from even among *known* users to the database, by policy/program driven authentication of their veracity as a database user. This is particularly useful in N-tier environments, where the package can validate if the user session originated from the mid-tier, or if this was a malicious user bypassing the mid-tier and/or application logic to access the data.

ODM can be used in conjunction with secure application roles. ODM will be operational as long it has read access to input tables for model builds, and create privileges in the current/invoking user session for creation of output objects.

N-tier Security Features

Several other aspects of the Oracle Security Platform, particularly those applicable in N-tier environments can be considered layered, orthogonal technology from the perspective of Oracle Data Mining. These include:

- **Enterprise User Security** - These pertain to technologies that enable scaling of the security platform to (hundreds of) thousands of users in a multi-tier, web environment. Techniques include Internet directory based Enterprise Privilege Administration, Shared Schemas, and Password-Authentication of enterprise users.
- **Identity Management** – The Identity Management infrastructure includes: Oracle Internet Directory – a robust LDAP v3 compliant directory service; Directory Integration and Provisioning – for synchronization between directories and provisioning for Oracle and third-party components; Delegated Administration– for trusted proxy-based administration of directory information by users and administrators; Single Sign-On; and Certificate Authority – that manages X.509 V3 certificates for PKI-based technologies.
- **Proxy Authentication** – N-tier systems can benefit from proxy authenticated user identity from a middle tier to the database. Oracle10*g* supports this capability for communications to the database via OCI, thick and thin JDBC.
- **Advanced Security** – protects the data over the network by thwarting data sniffing, data loss, replay and person-in-the-middle attacks. Native or SSL based encryption of data is supported. Businesses can leverage infrastructures such as Kerberos, PKI, RADIUS and X509v3 certification technology.
- **Java Security** – Oracle10*g* supports an enhanced, JDK1.2 compliant security model that includes fine-grained, policy-based access control model. Thick JDBC uses the full Oracle Net Services communications stack on both client and server, leveraging the encryption and authentication mechanisms from Advanced Security. Oracle10*g* also includes a 100% Java implementation of these mechanisms for thin JDBC-based access to the database, for transfer of secure applets to thin clients.

CONCLUSION

Oracle Data Mining is an option to the Oracle Database 10*g* Enterprise Edition that provides powerful in-database mining capability. It offers several interfaces – ranging from a GUI-tool for the business analyst to SQL Prediction functions and PLSQL/ Java APIs for embedding applications with predictive intelligence. By virtue of its tight integration with the database server, it offers many of the benefits extended to the users by the database. Foremost among them is the ability to mine data in a seamless, scalable, and secure manner under the aegis of an extremely powerful data management platform.

Oracle Data Mining addresses several important requirements for organizations in finance, banking, health care, telecommunication, retail and the Government – that are faced with complex near-term and strategic needs for analytics. Compared to point solutions for advanced analytics, Oracle Data Mining helps customers achieve substantial economies of scale and efficiency. This is particularly true for customers who already use the Oracle platform as the backbone of their enterprise data management infrastructure.

REFERENCES

- ODM literature and white papers (including this one) can be found at http://www.oracle.com/technology/products/bi/odm/index.html (or simply Google™ search on "Oracle Data Mining")
- Oracle10*g* Security features are covered at http://www.oracle.com/technology/deploy/security/db_security/index.html
- Oracle Database 10*g* is covered at http://www.oracle.com/database/index.html
- Oracle Application Server 10*g* is covered at http://www.oracle.com/technology/products/ias/index.html
- Oracle E-Business Suite 11*i* is presented at http://www.oracle.com/technology/products/applications/index.html
  Use this site as a starting point and navigate to literature on specific E-Business Suite components for Sarbanes-Oxley, Basel II, HIPAA and others.
- Oracle-PeopleSoft applications are presented at http://www.peoplesoft.com/corp/en/public_index.jsp

White Paper - Secure Data Mining in Oracle Database 10*g*
May 2005
Author: Ramkumar Krishnan

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
www.oracle.com

Copyright © 2005, Oracle. 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 is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.