

ORACLE INTERNET DIRECTORY

10.1.4.2

KEY FEATURES AND BENEFITS

ORACLE INTERNET DIRECTORY

- LDAP v2 and v3 Compliant
- Common Criteria EAL4
- OpenGroup LDAP Certified
- Easy wizard driven deployment
- Most Comprehensive High Availability and Disaster Recovery Configurations; Unique cluster configuration where a single Directory can span multiple hardware nodes
- Scalability with number of CPUs in SMP hardware and number of nodes in Cluster hardware; Scalable to terabytes of directory data and thousands of connections
- N-Way Multi-master, Fan-out, partial and fractional replication support
- Automatic Instance Recovery, Complete, Point-in-time and Flashback Recovery
- Management integration with Oracle Enterprise Manager
- Integration with Microsoft Active Directory, Sun, Novell, OpenLDAP
- Integration with Oracle E-Business Suite, Siebel, Peoplesoft
- Flexible Password Policies and Fine Grained Access Control Policies
- Extensible via Plug-in framework

Oracle Internet Directory is an LDAPv3 directory that leverages the scalability, high availability and security features of the Oracle Database. Oracle Internet Directory serves as the central user repository for Oracle Identity Management, a component of Oracle Fusion Middleware, simplifying user administration in the Oracle environment and providing a standards-based application directory for the heterogeneous enterprise. Additionally, Oracle Directory Synchronization allows seamless integration with other directories and enterprise user repositories, allowing users to leverage identity information wherever it resides.

Scalability and High Availability

Oracle Internet Directory has a multi-threaded, multi-process, multi-instance process model with Oracle Database 10g as directory data store. This unique architecture translates to tremendous flexibility enabling several High Availability configurations and opens up scalability possibilities on all kinds of hardware configurations. In terms of the ability to scale with CPUs on single hardware node deployments, Oracle Internet Directory architecture places no limit on the number of CPUs. Multiple processes and nodes for a single Directory also mean that a very high number [tens of thousands] of concurrent connections can be handled. Like the database underneath it, Oracle Internet Directory scales to support terabytes of real-world directory information on a single server.

The underlying Oracle database running with large data stores and heavy loads can recover from system failures in a matter of seconds. Oracle Internet Directory supports the most comprehensive set of High Availability options including active-passive and active-active Clusters, Replication and Data Guard based Disaster Recovery configurations. Oracle Internet Directory offers a rich set of Replication configurations that easily scales to a high number of replicas if required. The Maximum Availability Architecture that comprises of Oracle Database 10g RAC based OID Cluster configuration and Multi-master Directory Replication is unmatched by solutions from other Directory Servers in the industry. For more information see [High Availability Guide](#)

Security

Oracle Internet Directory supports two unique database security features, [Oracle Database Vault](#) and [Oracle Transparent Data Encryption](#).

Copyright 2006, 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 is it 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, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

ORACLE IDENTITY MANAGEMENT PRODUCTS

Oracle Access Manager delivers critical functionality for access control, single sign-on, and user profile management in the heterogeneous application environment.

Oracle Identity Manager is a powerful and flexible enterprise identity provisioning and compliance monitoring solution that automates the creation, updating, and removal of users from enterprise systems such as directories, email, databases, and ERP.

Oracle Identity Federation enables cross-domain single sign-on with the industry's only identity federation server that is completely self-contained and ready to run out-of-the box.

Oracle Internet Directory is a robust and scalable LDAP V3-compliant directory service that leverages the high availability capabilities of the Oracle 10g Database platform.

Oracle Virtual Directory provides Internet and industry standard LDAP and XML views of existing enterprise identity information, without synchronizing or moving data from its native locations.

Oracle Web Services Manager is a comprehensive solution for adding policy-driven security and management capabilities to existing or new Web services.

Oracle Enterprise Single Sign-On provides users with unified sign-on and authentication across all their enterprise resources, including desktops, client-server, custom and host-based mainframe applications.

Oracle Database Vault addresses common regulatory compliance requirements and reduces the risk of insider threats by:

- Preventing highly privileged users (DBA) from accessing application data
- Enforcing separation of duty
- Providing controls over who, when, where and how applications, data and databases can be accessed.

Oracle Database Transparent Data Encryption supports enterprise PCI compliance efforts by transparently encrypting data when it is written to disk and decrypting it when it is read back to the authorized user. Applications don't have to be modified, and authorized users won't even notice the fact that the data has been encrypted on the storage media.

Complementary to the database security features, Oracle Internet Directory offers comprehensive and flexible support for directory access control. This includes entry level, attribute level, and prescriptive access control to provide varying levels of security to custom fit enterprise and service provider needs. An administrator can grant or restrict access to a specific directory attribute, entry, group or naming context. Oracle Internet Directory implements three levels of user authentication: anonymous, password-based, and certificate-based using Secure Sockets Layer (SSL) v3 for authenticated access and data privacy.

Oracle Internet Directory offers sophisticated password policy management capabilities based on the password's "state" or "value". Password value policies e.g. use mixed case characters (ie. minimum upper and/or lower case characters), special characters (non-alphanumeric) and maximum repeated characters. Password state policies are used e.g. to assist user account life-cycle management such as grace logins constrained by time period (in addition to login instances) and minimum age for password self-modification. Multiple password policies can be created per directory subtree or on entry level. These features allow administrators to define consistent enterprise security policies across applications.

The external authentication plug-in provides authentication to 3rd party directories like Microsoft Active Directory, SUN Java System Directory Server, Novell eDirectory and OpenLDAP.

Manageability

Oracle Internet Directory includes Oracle Directory Manager, a Java based graphical directory administration tool. It is used for administration of operational aspects of the directory such as directory metadata information, password policies, schema and access control information etc.

Standalone directory deployments of Oracle Internet Directory and Directory Integration Platform can be monitored using the Application Server Control. This will be installed as of an Identity Management Infrastructure installation.

To monitor and administer Oracle Internet Directory and directory replication

Copyright 2006, 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 is it 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, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Key Directory Features

- Implements relevant IETF Version 2 and 3 LDAP RFCs, X.500 information model
- Extensible directory schema
- Supports online changes to directory schema with no downtime
- Multi-byte National Language and Unicode support
- An Open Group LDAP 2000 Branded Server
- Common Criteria Evaluations at EAL4
- Server extensibility via Java and PL/SQL Plug-in's
- Server chaining to access data in non Oracle directories transparently

Performance

- Scales to the capabilities of the Oracle Database 10g to support multi-terabyte data stores
- Unique multi-threaded, multi-process LDAP processes and database connection pooling to support thousands of simultaneous clients
- Delivers millisecond response time independent of data size
- Supports server-side entry caching to improve search performance

Replication and High Availability

- Multi-master replication using Oracle 10g Replication
- Updatable Fan-Out replication (i.e. Multi-master replication) based on LDAP v3 Protocol
- OracleAS cluster

together with Directory Integration Platform in a distributed environment the usage of Enterprise Manager Grid Control is suggested. Grid Control besides many other features provides a topology viewer (important in distributed environments), performance monitoring, reporting framework and process monitoring & control.

Enterprise Manager Grid Control is the single interface of choice for Identity Management components like Oracle Internet Directory, Directory Replication, Directory Integration platform and others.

Oracle Internet Directory has a comprehensive and efficient Server Manageability infrastructure that gathers the necessary information to aid the Monitoring and Management of Oracle Internet Directory. The information gathered by the Server Manageability Infrastructure in Oracle Internet Directory can be exposed to various industry standard monitoring agents and presented to Directory Administrators through suitable GUI interfaces

Oracle Directory Integration Platform

Oracle Internet Directory includes the Directory Integration Platform, which enables customers to synchronize data between various directories and Oracle Internet Directory. The Directory Integration Platform is a set of services and interfaces which allows to develop synchronization solutions with other enterprise repositories. It can also be used to provide Oracle Internet Directory interoperability with third party meta-directory solutions.

Directory Integration Platform includes agents for out-of-the-box synchronization with Oracle Human Resources, Oracle Database, as well as agents for synchronizing information with select third-party LDAP servers, such as SunOne/iPlanet Directory Server, Microsoft Active Directory, Novell eDirectory and OpenLDAP.

Using Directory Integration Platform, customers can build a single enterprise directory with global directory entries containing data from such diverse sources as Human Resources applications, LDAP directories, and other data repositories.

Oracle Directory Integration Platform uses Oracle Internet Directory as the central enterprise directory for both user and configuration data.

Standards Supported and Certifications

Oracle Internet Directory supports a comprehensive range of security standards and protocols.

- LDAP v2 and v3
- SSL v3, TLS 1.0, SASL
- OpenGroup VSLDAP certified
- EAL4 compliant

Copyright 2006, 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 is it 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, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Security

- Support for Oracle Database Vault and Transparent Data Encryption
- Configurable multi Password Policies
- Fine-grained ACL control:
 - Per Entry
 - Per Attribute
 - By Group Membership
 - Prescriptive (Naming Context)
 - By Mode of Authentication
- Configurable SSL v3 data privacy
- Supports anonymous, password-based and certificate-based user authentication
- Strong authentication via X.509 v3 digital certificates for PKI implementations
- Proxy capabilities enable middle-tier applications to access the directory "on behalf of" end user communities
- External authentication plug-in to authenticate against Microsoft Active Directory, SUN Java System Directory, Novell eDirectory and OpenLDAP

Administration

- Oracle Identity Management Grid Control embedded in Enterprise Manager Grid Control for Monitoring and Administration of distributed deployments.
- Oracle Directory Manager, a Java-based GUI directory administration based on Oracle Enterprise Manager framework
- Command-line tools for standard LDAP operations and replication administration
- Specialized tools for bulk loading and exporting of LDIF data
- Delegated Administration Service which enables end users and

Improved integration with Oracle products

Oracle Internet Directory is the Directory of choice for all Oracle product suites and provides the Directory backbone for Oracle Application Server 10g, Oracle Collaboration Suite 10g, Oracle E-Business Suite and Oracle Database Enterprise User and Advanced Security Options. It is also the preferred product for storing Oracle database service names and is replacing Oracle Names for this purpose.

A Component of Oracle Fusion Middleware

Oracle Fusion Middleware is a family of proven middleware products that help organizations achieve greater agility, make better informed business decisions and more easily integrate data and processes across disparate IT systems - including technologies from Oracle and other vendors. Oracle Fusion Middleware features Oracle Application Server 10g, related Application Server products and options, Data Hubs and Oracle Collaboration Suite. These products are available today and are being used by thousands of customers and partners throughout the world.

Additional information can be found at www.oracle.com/middleware.

Further Information

For more information, visit www.oracle.com/identity