

An Oracle White Paper
June 2009

Oracle Virtual Directory 11g

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. 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 for Oracle's products remains at the sole discretion of Oracle.

[

Executive Overview.....	3
Business Challenges.....	5
High Cost of Administration and Compliance Due to Too Many Identity Repositories	5
Difficult To Deploy New Applications due to Lack of a Unified View of Identity	5
Full Consolidation of Identity is Impossible	6
LDAP-enabled Applications Cannot Access Data in Non-LDAP Stores	6
Solution: Oracle Virtual Directory	7
Benefits of Implementing Oracle Virtual Directory.....	7
Reduced Need for Data Synchronization and Identity Stores	7
Accelerate New Application Deployment	8
Ease the Pain of Directory Consolidation.....	8
Quick and High Return on Investment	8
Features of Oracle Virtual Directory	8
Single Interface For Identity	9
LDAP Interface For Non-LDAP Data.....	9
Data Transformation And Application Specific Views	9
Superior Usability	10
Enterprise Scalability, Availability and Manageability	11
Architecture	13
Example Use Cases.....	14
Access Management.....	15

Centralize Database Account and Role Management	15
Conclusion	15

Executive Overview

Directory services is a critical component in enterprise application infrastructure providing applications with identity services such as user profiles, access and authorization data. Well structured and organized directory services is the foundation of efficient and effective identity management solution that enables enterprise applications.

One of the identity management challenges enterprises are facing is the lack of single source for identity data and the proliferation of identity stores including directories and databases. Enterprises have employee information in HR databases and/or Microsoft Active Directories (AD), customer and partner data in CRM databases and additional LDAP directories.

Since AD is the Network Operating System directory for Microsoft Windows, and databases are not readily accessible to many commercial off the shelf (COTS) applications that require LDAP access to identity data, application specific directories proliferate copying and synchronizing identity data and extending schemas. This proliferation of data results in high administration and maintenance cost, inconsistent identity data and compliance issues.

Oracle Directory Services (ODS) addresses these challenges with a unique solution that uses Oracle Virtual Directory (OVD) to provide identity aggregation and transformation without data copying and synchronization while Oracle Internet Directory handles directory storage.

ODS enables enterprises to quickly standardize directory services resulting in reduced cost, accelerated application deployment, enhanced security and improved compliance.

Oracle Virtual Directory is the key component of ODS providing a single standard interface to access identity data no matter where it resides while hiding the complexity of underline data infrastructure. OVD is not LDAP storage, but an identity virtualization service.

It unifies identity data without consolidating, and re-uses identity data without copying.

Furthermore, OVD also transforms underline identity data in real-time to meet application specific needs.

Since Oracle Virtual Directory enables applications to access existing authoritative identity data sources without copying, it reduces the need for application specific user stores and data synchronization, and thus simplifies provisioning project and accelerates application deployment.

With OVD as a component of enterprise identity infrastructure, it also facilitates directory consolidation by decoupling applications from underline identity repositories. Additionally it has pre-integrated “identity publisher” features that enable access to identity information managed in Oracle applications including PeopleSoft, Siebel and Oracle Customer Hubs. Furthermore, OVD is very easy to deploy and manage resulting in quick and high return on investment (ROI).

For customers who also need directory storage (for example to store extended schema attributes that cannot be stored in Active Directory) OVD shares a unified administration and management system with Oracle Internet Directory. This provides customers with the industry’s only truly unified enterprise-class virtual and storage directory services suite.

Business Challenges

Directory services are key building blocks for identity-enabled business applications and the underlying enterprise identity management (IdM) architecture.

Well-structured and organized directory services are the foundation of efficient and effective security services. This is because all IDM applications and most commercial off the shelf (COTS) business applications require a standard mechanism to access identity attributes, and the most common way to access identity attributes is using LDAP. Example identity attributes include user credentials, access privileges and profile information.

Additionally the modern enterprise has different identity attribute needs than they did when LDAP servers first appeared on the market in the 1990s. This is because modern enterprises often have multiple LDAP storage-based servers as well as identity stored in non-LDAP repositories such as HR or CRM databases.

Furthermore, more and more businesses are deploying new external facing applications that often require storage for identity data such as credentials for non-internal people like vendors, partners and even customers.

These requirements led to several challenges in deploying identity related applications within the enterprise.

High Cost of Administration and Compliance Due to Too Many Identity Repositories

Many organizations find themselves spending large amounts of time and money on compliance due to too many identity repositories. Specifically this means they are duplicating existing data into application specific silos. This often happens because existing data repositories are either not flexible enough to meet application requirements or are trapped in proprietary databases instead of being accessible via standard protocols.

Many identity silos result in redundant identity administration efforts, in-consistent security, and difficulty in proving compliance. To address these issues, many enterprises are deploying provisioning solutions to automate the identity management lifecycle and provide reports to facilitate compliance. However, to deploy provisioning for many target systems is costly and time consuming. As a result, only a small subset of identity repositories is being provisioned. On the other hand, data synchronization solution is difficult to set up and costly to maintain.

The real challenge is how to reduce the number of identity stores and re-use identity data from a few authoritative ones without copying.

Difficult To Deploy New Applications due to Lack of a Unified View of Identity

Many applications that leverage LDAP such as portals, business intelligence and access management face longer deployment times because the data they need is not provided in a unified LDAP view. The longer it takes to deploy an application the longer it takes for the organization to see any benefits of the application including ROI.

Unified views of identity are prevented because regulatory, political, or technical reasons prevent from aggregating data into a central LDAP store or because one or more of the attributes (or role information) is stored in non-LDAP sources.

Additionally even if there currently is a single view of identity it's a very brittle view - if the company changes through a merger or acquisition – the unified view breaks.

Or if a new application is deployed that requires a slightly different view of the same data – the view is not usable by this application.

Due to the lack of a flexible, unified view of identity, organizations continue to add application specific identity stores to deploy new applications. As a result, it takes longer to deploy new applications and further complicates the identity infrastructure.

Full Consolidation of Identity is Impossible

One possible solution to the “too many identity stores” and “lack of unified view of identity” is to try to do identity consolidation. However, it is impractical or impossible to have one gigantic identity store.

There are many reasons for this:

- It takes most organizations a year or more to come up with a single unified schema – which is often inflexible for new applications
- Internal data politics make it harder to get copy of all identity data
- Determining how to duplicate existing and conflicting security rules adds more time and cost
- Regulations can prevent certain pieces of data from being centrally stored or cross organizational/national boundaries
- Architecture best practices may require the separation of employee, customer, and partner identity data

While an organization can consolidate and eliminate some repositories, multiple stores will still exist. The consolidation process itself is costly and time consuming.

LDAP-enabled Applications Cannot Access Data in Non-LDAP Stores

One of the reasons why organizations end up with too many identity stores and thus face compliance challenges as well as taking longer times to deploy new applications is that key identity information is trapped in relational databases. This is a problem because most

applications that can leverage external authentication and authorization sources are able to do via a standard protocol – LDAP. And in most cases the enterprise LDAP server will still not have all of the identity data needed to satisfy all of the potential requests and instead that data will be left locked in proprietary databases.

Thus organizations are not able to achieve a strong ROI on their legacy identity investments because the data is not accessible via a standard interface.

Solution: Oracle Virtual Directory

Only Oracle Directory Services provides a directory service solution that addresses above challenges. Oracle has the most comprehensive directory services offering on the market, including virtualization, storage and synchronization. Oracle Virtual Directory (OVD) provides identity aggregation and transformation without synchronization while the Oracle Internet Directory (OID) provides data storage. This white paper focuses on OVD, and OID is covered separately in its own white paper.

OVD is not LDAP storage, but an identity virtualization service. It unifies identity data without consolidating, and re-uses identity data without copying. The key features of the virtual directory include:

- Single interface for identity
- LDAP interface for non-LDAP data including databases and Web services
- Data Transformation and Application Specific Views
- Enterprise Scalability, Availability and Manageability

These features and the virtual directory architecture are covered later in this document.

Benefits of Implementing Oracle Virtual Directory

Reduced Need for Data Synchronization and Identity Stores

OVD is designed to be connected to multiple data-stores and to expose their data on-demand without any additional synchronization. These data stores can be LDAP, databases or Web Services. The data can then be unified in the proper format. For example if different types of user populations are stored in different sources (for example staff in Microsoft Active Directory and customers in an Oracle database) all sources can be searched simultaneously without needing to copy the data into another source.

OVD also supports split-profile via its join adapter. A split-profile is where one part of a user's profile exists in one source (for example username and password in LDAP) but another portion exists in another source (such as their management chain in HR database). The join adapter then allows applications to see the data as a single virtual entry.

With these capabilities OVD allows organizations to reduce the need to do data synchronization, which then reduces the number of identity stores. This results in simpler compliance efforts and increased ROI on existing identity stores.

Accelerate New Application Deployment

As stated earlier, one of the reasons why new applications can be delayed in deployment is because of the lack of a unified identity source. OVD's real-time application specific views of data allow it to speed up new application deployments by providing a single point of truth leveraging existing identity data. Thus applications no longer need to worry about where to go for their identity, which eliminates any deployment delays due to identity information.

Ease the Pain of Directory Consolidation

While it is not possible to completely consolidate all identity data into a single consolidated store – organizations can often still consolidate into fewer directory services. When this is done, this often results in schema and Directory Information Trees (DIT) changes, which can be significant. Thus applications often need to be changed or modified. Because OVD is placed between applications and the source systems, it abstracts changes in the source environment from the applications. This reduces the problems that can result from a directory consolidation project.

Quick and High Return on Investment

With OVD, organizations are able to leverage existing identity stores and do not require any additional storage. In addition, OVD is very simple to install and configure. In many cases OVD customers are able to bring an OVD instance live and into production within a matter of weeks. Thus customers can see a very quick and high return on investment. And because OVD is re-using their existing identity stores as well as accelerating deployment of new applications, it increases ROI in these areas as well.

Features of Oracle Virtual Directory

The key features of OVD are:

- Single interface for identity
- LDAP interface for non-LDAP data including databases and Web services

- Data Transformation and Application Specific Views
- Superior Usability
- Enterprise Scalability, Availability and Manageability

Single Interface For Identity

OVD provides a single virtually consolidated access to a user's identity information regardless of where the data is stored. This could include, for example, credential information in an LDAP store, employee data stored in a HR database and role information stored in a Web Service.

OVD provides a Join adapter, which allows OVD to support split-profile. A split profile is one where the user identity data is split between two or more sources. For example, a user's identity information is stored in a database, an LDAP server and a Web service but applications want to treat it as a single entry

The Join adapter uses a join rule (similar to a SQL join condition) to virtually link the data together into a "super-entry".

LDAP Interface For Non-LDAP Data

Many applications including Oracle Access Management Suite and Oracle Enterprise Database use LDAP to access identity information. Thus to leverage data in a database or a Web Service, the data must be made accessible via an LDAP interface.

OVD contains adapters that allow LDAP-enabled applications to leverage database or Web-service data directly without needing to copy the data into another server.

For example, OVD can expose PeopleSoft HR data or Siebel Universal Customer Master (UCM) data as LDAP for applications to access.

Data Transformation And Application Specific Views

OVD not only provides the ability to virtually unify data it can also transform data and provide application specific views.

Data Transformation

OVD supports the following types of data transformations:

- Namespace mapping such as making an LDAP server of "o=Oracle.com" become "dc=oracle,dc=com"
- Field name mapping such as renaming "cn" to "FullName"
- Value translation such as changing "ORCL" into "ORACLE"

- Hide Data such as hide phone number if attribute “donotpublish=yes”

Many of these transformations are possible with configuration. However, customers can do their own business-logic driven transformations using OVD Java plug-in API.

Application Specific Views

Because OVD is stateless and supports data transformations it is able to create application specific views of data. This means that different applications – all accessing the same OVD can appear to be accessing completely different data schema, structure, attribute name and values. This simplifies the deployment of new applications because administrators no longer have to worry about if a new application requires its own schema that is re-using existing data. OVD turns this into a simple configuration exercise and the new application can be rolled out much more quickly.

Superior Usability

OVD is managed via a centralized browser-based management console named Oracle Directory Services Manager (ODSM).

ORACLE Directory Services Manager

Version Information
 ODSM 11.1.1.1.0 OVD 11.1.1.1.0 Adapter Package 1

Name	Type	Visibility	Root
AD	LDAP Adapter	Yes	dc=mydomain,dc=com
OE	Database Adapter	Yes	ou=oe,dc=mydomain,dc=com

Navigation Tabs

- [Data Browser](#)
Navigate the virtual LDAP directory using the browse tree.
- [Schema](#)
Manage attributes and object classes.
- [Security](#)
Manage access control points.
- [Advanced](#)
Manage mapping templates, deployed mappings, global plug-ins, libraries, server views and configure wizards.
- [Adapter](#)
Manage adapters for LDAP, local store, custom, join, and database.

ORACLE Virtual Directory

Diagram illustrating the Oracle Virtual Directory architecture components:

- Data Browser
- Identity Storage
- Advanced
- Adapter
- Security
- Schema

Rich User Experience

ODSM provides a task-oriented, desktop-like access to OVD administration tasks. Additionally it leverages the Oracle ADF framework to provide a consistent experience across all Fusion applications.

High Performance Technologies

ODSM is able to leverage functionality such as partial-page rendering (also called AJAX) and real-time scrolling to provide a low-latency, consistent user experience

Unified Administration

For customers who are using OID 11g – ODSM provides a consistent administration console for both OID and OVD. Thus it reduces the time & training needed to learn how to manage Oracle Directory Services products.

Enterprise Scalability, Availability and Manageability

The OVD is designed to be scalable, highly available and easy to manage. Additionally its architecture makes it easier to scale and manage the master-data sources.

Scaling OVD For Performance

Since OVD is stateless, it is easy to scale by adding nodes. Additionally it can help scale the back-end sources by using its own load-balancing capability (assuming the sources have redundancy) and routing. For example OVD can route requests to different sources based on name or uid ranges. OVD can also leverage additional Oracle technology such as Oracle TimesTen or Oracle Coherence to help reduce latency and improve scalability.

OVD can be deployed either centrally or geographically dispersed depending upon application requirements.

OVD Availability

OVD is stateless, so it is easier to deploy with high availability than other alternatives. The simplest way to make OVD highly available is to add multiple nodes and then use round-robin DNS or load-balancer to route requests properly.

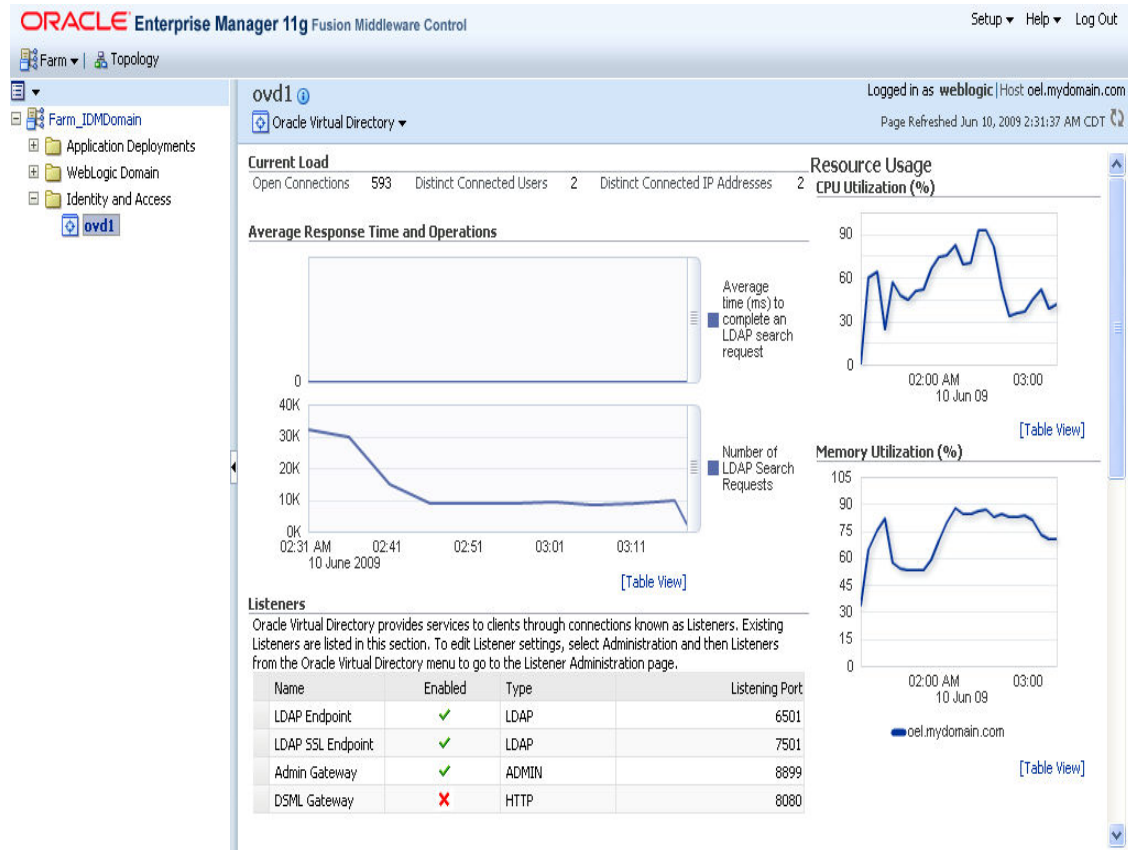
OVD supports the ability to keep all server configurations synchronized without needing to manually copy & paste configuration between machines.

Additionally OVD supports high availability of the data-sources using internal load-balancing capability for LDAP and support for native high-availability capability for database such as Oracle Real Application Clusters (RAC).

Also OVD can leverage other Oracle technologies such as Oracle TimesTen to help provide high-availability for database data that otherwise does not have that capability.

OVD Manageability

OVD 11g provides enterprise manageability through Oracle Enterprise Manager (OEM). OVD is the only virtual directory on the market that comes with enterprise-grade operational management by default.



OEM provides the following features:

- Operational monitoring of server status, adapter status, system status including CPU & Memory utilization
- Single dashboard view of entire deployment topology and server status including all Oracle Fusion Middleware components, databases, and applications.
- Trigger enterprise alerts via SNMP or email

- Integration with Fusion audit and logging viewers enables single place to view OID and OVD logs and end to end tracing of a transaction across application stack from HTTP server to backend LDAP and databases.
- Ability to generate standard reports with default integration with Oracle BI Publisher

Un-surpassed OVD manageability ensures infrastructure health and facilitates enterprise wide large-scale deployments.

Architecture

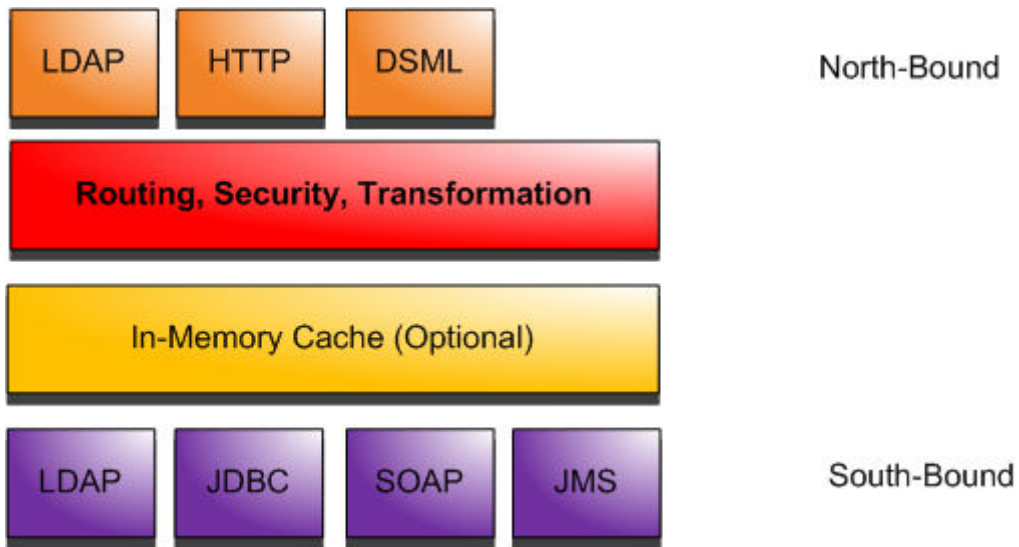
There are two primary components – the OVD server and that is what client applications connect to and the OVD Manager, which is a desktop based management console for server configuration.

Clients connect to the OVD server (e.g. the north-bound interface) via one of the supported listener protocols. Currently supported listeners are LDAP, HTTP and DSML. The HTTP interface provides a Web-gateway application that can be customized to build white-pages application(s) that will work even on mobile devices.

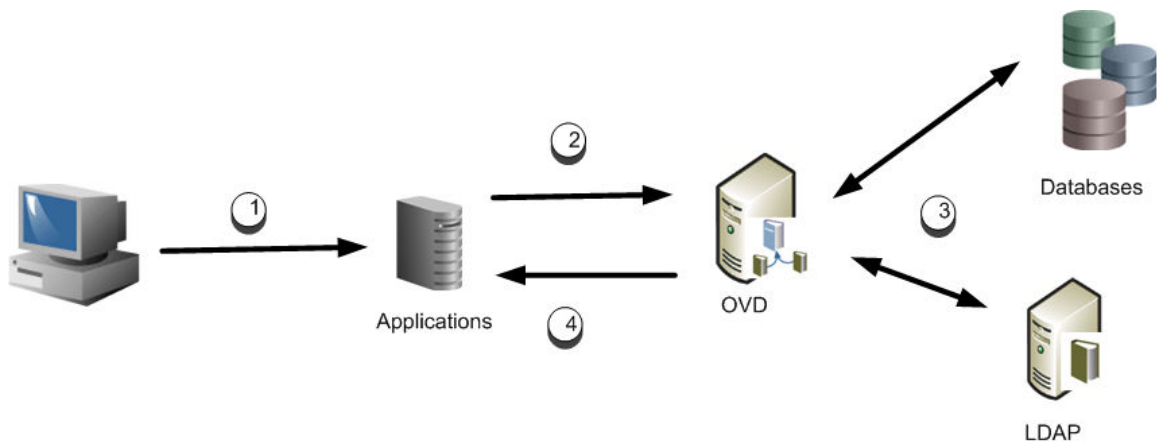
OVD listeners only provide enough logic to convert the incoming request into the internal Java API call. This is called the Global Service Interface or GSI. The GSI is used by any listener and allows OVD logic to be applied regardless of the actual north-bound protocol.

The GSI passes the data to the OVD routing engine. The routing engine is where the data transformation, linking of split profiles, security and routing to proper sources occur.

OVD connects to the specific sources using south-bound adapters. The default adapters include LDAP, and Database (JDBC). OVD also provides a Java API that can support creating custom adapters for example to connect to a Web Service or a JMS system.



The following diagram shows an example of how the data flows between applications and OVD.



- ① Client connects to an application (e.g. Portal)
- ② Application accesses OVD to locate, authenticate, and authorize the user as if the OVD was a standard LDAP Server
- ③ OVD transforms the request into one or more native requests to the authoritative identity sources (e.g. via LDAP, SQL, or Web Services)
- ④ OVD normalizes responses from the native identity sources and transmits the results in a way that the application can use to grant or deny access to the client or create a personalized response

Example Use Cases

The following are example use cases for Oracle Virtual Directory.

Access Management

Most access management products including all of the components of the Oracle Access Management suite leverage LDAP for authentication and to get the data they need to make authorization decisions.

OVD simplifies the ability to connect these applications to multiple directories, data stored in non-directory sources or split-profile data (OVD also protects the applications from changes in the identity infrastructure (for example DIT changes because of company re-org or a merger).

Thus by allowing organizations to leave identity data where it is – whether it is in multiple directories or in legacy databases they are able to maximize their ROI by re-using their existing identity stores. It will also reduce the time needed to deploy a new access management product (or a portal, which has its own LDAP-based account or profile management) because data will not need to be consolidated into a single repository.

Centralize Database Account and Role Management

Oracle Enterprise Database supports centralizing accounts and roles into an enterprise directory. The database can use OVD to allow this data to be stored into Microsoft Active Directory or Sun LDAP. This reduces the number of passwords that a person needs to be remembered and can eliminate the need to have a provisioning product to update individual databases.

This maximizes the benefits of database and account security while eliminating the hassle and problems caused by trying to copy existing identity data into multiple repositories.

Conclusion

Oracle Virtual Directory is a critical component of a secured identity infrastructure to simplify the environment and help deliver the IT promise of compliance, cost reduction, and accelerated application deployment.

Because OVD allows organizations to re-use existing identity sources and provides application specific views it provides the following benefits:

- Reduced need for data synchronization
- Accelerate the time needed to deploy new applications
- Ease the pain of directory consolidation
- Quick and high Return on Investment

For further information on OVD please see:

<http://www.oracle.com/identity>



Oracle Virtual Directory 11g
June 2009
Author: Mark Wilcox
Contributing Authors: Forest Yin

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
oracle.com
fs



| Oracle is committed to developing practices and products that help protect the environment

Copyright © 2009, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

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