

Oracle Directory Services

Buyer's Guide

ORACLE WHITE PAPER | JUNE 2015





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.



Table of Contents

Introduction	1
Business Drivers	2
Oracle Directory Services	3
Key Considerations for Some Popular Scenarios	4
Cloud	4
Mobile	4
Customer-Facing Internet	4
Employee-Facing Intranet	5
Directory Services Checklist	5
Conclusion	7



Introduction

In the late 1990s, directory servers were essentially designed as white-page applications for providing users with secure access to enterprise resources through authentication and authorization processes. Since then, their use has been extended to partners and customers, thus creating the need to support an increasing number of diverse users and communities. Today, directory services need to accommodate hundreds of millions of users and provide additional services to break identity silos. With the ubiquitous use of mobile devices as well as cloud deployments and the integration of social networks identities into the enterprise fabric, billions of objects are transacted everyday through directory services.

Modern directory services now go beyond the initial capability to store objects in an identity repository. Directory solutions have evolved around three foundation services:

- » Storage: Persisting and maintaining entries representing identities.
- » Synchronization: Moving and synchronizing identity information across multiple identity repositories.
- » Virtualization: Leveraging information from multiple, heterogeneous identity repositories without physically moving data while preserving ownership.

Directory services are now an integral part of a highly secure, highly available, auditable, coherent, and simplified Identity Management solution. While modern directory services provide much more than serving a specific operating system, they have to seamlessly integrate with your existing environment and stay compatible with your existing applications.

Selecting the appropriate solution goes beyond meeting immediate, basic requirements. Oracle Directory Services offers the following benefits:

- » An all-in-one solution for storage, synchronization and virtualization that eliminates the need for integration, accelerates time to value, improves security and reduces costs.
- » Compliance with industry standards, scalable to billions of users and objects with required performance to address current and future business growth.
- » Support enterprise, cloud and mobile requirements.

This buyer's guide is designed to help develop a clear understanding of the key features and requirements when evaluating a directory services solution.

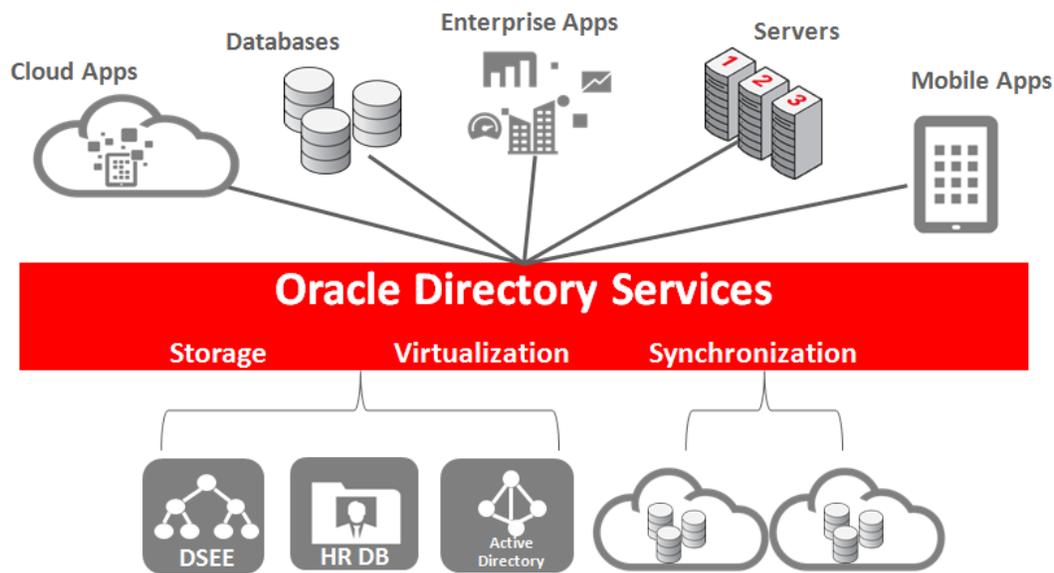
Business Drivers

Although there are many practical reasons to select a directory services solution, it is necessary to understand how such a solution can positively impact the business. In this section, we take a look at key business drivers for adopting modern directory services in today's enterprise.

- » **Directory Consolidation:** As there are many siloed sources of information within the enterprise and in the cloud, consolidation is an important driver. Providing directory services that can act as a single authoritative source of truth will reduce complexity and lower cost. Applications can be setup to leverage a single central corporate directory service, eliminating the overhead of managing individual identities in each application. User authentication to multiple databases can also be considered into this single directory service, reducing the burden for DBAs to manage user credentials for each individual database instance and provide a single password for users across all databases. In the same way, all Unix/Linux desktops or servers can leverage a central directory service, instead of each system having its own user/password file to maintain, thus off-loading system administrators' tasks to a central point of control.
- » **Directory Virtualization:** Consolidating siloed sources of information is not always technically feasible or desirable because of multiple data formats, different organizational data ownership, and specific challenges due to data location and access policies. Virtual directory capabilities provide a unified view of data from multiple identity sources at run-time without a need for data consolidation, duplication, or ownership changes. Virtualization helps reducing costs, redundancies, and complexities associated with data compliance and administration. Any application is aware of only one directory, the virtual directory, which unifies data from multiple backend data sources. Finally, a virtual directory brings unification across heterogeneous identity stores (including non-LDAP formats) and applications on premise or in cloud, delivers fast time to value for application deployment.
- » **Enable Cloud:** Support flexible deployments with multi-tenancy leveraging the same directory services to lower operational costs while making it possible to scale and perform as the number of customers and users increases. Enable use cases where data is shared between cloud and on-premise applications. In a dynamic cloud environment, provisioning additional resources on demand are required. Finally, delivering SLAs is a critical success factor for a cloud service in terms of performance, monitoring and management.
- » **Support Mobile and The Internet of Things:** Mobile is transforming the way we live and the way we do business. Provision must be made to address the specific characteristics required by mobile environments such as very large volume of managed identities or change in usage behavior with more write requests as well as location tracked in the directory itself. The Internet of Things is pushing directory services into supporting amounts of identity-related information never seen before.

Oracle Directory Services

Oracle Directory Services provides a unique approach in consolidating all required capabilities for modern directory services into a single solution. By leveraging common technologies it provides a consistent user experience integrated into the Oracle product portfolio.



- 1- Cloud Applications leveraging Directory Services
- 2- Databases users/passwords consolidated in Directory Services
- 3- Enterprise applications leveraging Directory Services
- 4- Unix/Linux/Solaris servers having users/passwords consolidated in Directory Services
- 5- Mobile Applications leveraging Directory Services
- 6- Oracle Directory Services stores information related to users
- 7- Oracle Directory Services creates LDAP views from information that comes from other directories or databases
- 8- Oracle Directory Services can synchronize directory entries with other repositories including in the cloud

Oracle Directory Services provides the following capabilities:

- » **LDAP Storage:** Manage, store, and retrieve entries.
- » **Virtual Directory:** Create virtual directory views from information coming from directories, Database or web services data sources.
- » **Synchronization:** Provide synchronization capabilities for data in the LDAP storage and other 3rd party directories and database systems.

Key Considerations for Some Popular Scenarios

This section describes four scenarios emphasizing best practices: Cloud, Mobile, Customer-Facing Intranet, and Employee-Facing Intranet.

Cloud

As cloud deployments become more mainstream, some considerations for directories include the following.

- » It is important for cloud applications to easily interface with your own on-premise identity store or on-premise applications to interact with directories in the cloud. LDAP is not the preferred access protocol to cross the firewalls, as a result, alternate protocols such as REST have to be supported.
- » To efficiently manage resources and deliver on SLAs, the cloud needs to be dynamic to accommodate load. It should be easy to create new instances on the cloud infrastructure and load data when needed.
- » Ability to unify information through virtualization from multiple sources in the cloud and on premise should be provided.
- » As data might have to be moved between cloud and on premises, secure synchronization is required.

Mobile

Modern directory services need to provide the required infrastructure to support mobile access to applications.

- » The use of mobile devices increases the proliferation of identities, not just traditional users, but also associated data such as mobile SIM cards, subscriber contract numbers, device identities, etc. This means that directories have to scale up and manage billions of objects.
- » New types of mobile “users” are emerging, for example, connected objects such as cars, game consoles, etc. More generally, the Internet of Things is also pushing beyond the scalability of traditional enterprise directories required because they have to support connected devices in addition to employees, partners, and customers.
- » Mobile access enables new user experiences with location-aware applications. Location data is dynamic as the user moves around, generating increased update traffic on directory services. A modern directory not only has to provide high search performance but also extremely high write performance.
- » Directories enabling direct mobile access to provide mobile white pages or address book services require REST interfaces.

Customer-Facing Internet

The Internet delivers global 24x7 access to your business assets. In addition to supporting traditional authentication and SSO, below are some key considerations that your directory services need to address.

- » The solution needs to be scalable to support your business growth. It also needs to provide consistent response time even during peak business hours. Performance and scalability issues will result in lost transactions or even lost customers. For consumer-facing Internet applications, you may need to support hundreds of millions of users.
- » High Availability (HA) with multiple data center real-time replication is a must as downtime results in lost business opportunities and bad user experience.
- » As business conditions can be very dynamic, flexibility in routing LDAP traffic to the most efficient server available to meet application needs is a legitimate expectation.
- » Directory Services can contain highly sensitive information, therefore built-in security such as fine-grained access controls and data / communication encryption is critical to mitigate or prevent security breaches or stolen user identity data. Providing an extra layer of security through an LDAP proxy layer will further isolate your internal infrastructure from external traffic.

Employee-Facing Intranet

Directory services are the foundation of your corporate intranet and its security. To maximize productivity and ensure security and compliance, below are some key considerations for use of directory services in employee-facing intranets.

- » High availability is critical to the enterprise. Directory services must ensure zero-downtime across all corporate operation sites wherever they are located. Flexibility and scalability is required to support many intranet applications, sometimes thousands of them.
- » Directory services should be able to consolidate information from many sources, such as other LDAP directories, Microsoft Active Directory, files, or databases.
- » Even after directory consolidation, multiple identity repositories could exist. Directory services should provide a means to synchronize between those repositories such as Active Directory, HR Databases, etc., and ways to virtualize multiple data sources.
- » As mergers and acquisitions are a norm in today's business, providing quick and easy integration between existing applications and existing directories using virtualization technology is important as it helps the enterprise to remain efficient and adapt quickly to changes.

Directory Services Checklist

This section is broken down into functional sub-sections describing the key functionality required.

UNIFIED SOLUTION

Key Functionality	Feature / Benefit
One directory product to provide storage, synchronization and virtualization	Address need for modern directory services in a single product offering combining storage, proxy, virtualization and synchronization. Provide a consistent, secure experience while installing, managing and monitoring the service. This effectively eliminates the need for point-product integration and simplifies deployments.
Storage	An LDAP V3 compliant directory to store identity information with high performance search and write operations.
Synchronization	Ability to sync data bi-directionally with other directories such as Active Directory and databases such as Oracle.
Virtualization	Ability to provide a unified view of data at run-time from multiple backend data sources such as Active Directory, LDAP servers and, databases without moving data around. Ability to transform data and schema on the fly to fit applications requirements without impacting backend data.

EASY TO DEPLOY AND MANAGE

Key Functionality	Feature / Benefit
Intuitive single administration console	Eliminate the need for specific training on multiple interfaces to multiple services. All information is accessed in a single, coherent administrative approach.
Real-time monitoring and management	Provide a global monitoring solution that can monitor system health, manage the system environment, and handle data analysis.
Test to Production	Provide tools to automate the promotion of the environment from development, to test, to production.

PERFORMANCE AND SCALABILITY

Key Functionality	Feature / Benefit
High read and write throughput	Deliver more read and write operations than conventional solutions to enable software and hardware consolidation with a smaller footprint thus reducing the total cost of ownership.
Low latency and predictable response time	Low latency provides better user experience and consistent response time while meeting the requirements of specific SLAs.
Optimized memory usage	Memory usage optimization and data compression techniques allow for better management of valuable data in cache in order to maximize the directory services throughput.
Vertical scalability	Ability to leverage multi-core infrastructure, providing effective vertical scalability so that increased performance and capacity can be achieved by adding more CPUs and memory to an existing configuration.
Horizontal scalability	Ability to distribute data across multiple back-ends with a global catalogue provided for extremely large deployments.

CLOUD READY

Key Functionality	Feature / Benefit
Support for virtualized platform environments	Ability to run on virtual environments, providing flexibility and cost saving while deploying in the cloud.
Virtual directory capability	Essential capability to consolidate information from multiple sources deployed in the cloud and/or on premise.
Synchronization	Ability to move data from and to the directory service to keep data synchronized.
REST interface	Provide REST interface for applications to connect to the directory in order to meet specific customer requirements.

HIGH AVAILABILITY

Key Functionality	Feature / Benefit
Multi-master, active-active and/or active-standby support	High availability is provided via multiple instances keeping each other up to date without the need for additional technology. All instances effectively collaborate to the service and eliminate the need for unused hardware remaining in standby mode.
Multi-master replication across data centers	Replication model ensuring consistency between multiple instances in same data center or across multiple data centers located in different geographical areas.
Assured" replication	Ability to setup replication to guarantee that any change is effectively made in at least two different locations to secure an update before update operation returns.
Highly Available "changelog" service	"Changelog" is implemented as a high-availability service so that changes can be consumed by external applications at all time.

HIGHLY SECURE

Key Functionality	Feature / Benefit
Fine-grained access control	Ability to setup access control lists at the sub-attribute level, providing effective fine-grained access control.
Fractional replication	Sensitive attributes can be excluded from replication to insure they remain under the most secured zones or to comply with regulatory mandates specific to data location.
Support for broad scope of encryption schemes	Support for modern encryption schemes to maximize security, while still supporting old ones for compatibility.
Support for encrypted communication	Data is encrypted while in transit either between client applications and servers or between servers when replicated.
Support for attribute encryption	Sensitive attributes can be encrypted to maximize security when data is at rest.

EASY TO EXTEND

Key Functionality	Feature / Benefit
Plug-in API	Components include APIs to enrich capabilities or to enable customization for specific needs.
Extensible schema	Schema easily extensible without service interruption to support new applications.

Conclusion

Oracle Directory Services is the most comprehensive solution on the market providing storage, synchronization and virtualization capabilities. The suite includes Oracle Directory Server Enterprise Edition (ODSEE, the former Sun directory), Oracle Internet Directory (OID), Oracle Unified Directory (OUD) and Oracle Virtual Directory (OVD). Customers buying Oracle Directory Services have the option to deploy any product(s) in the suite based on use case requirements and/or architecture preferences. While unifying the user experience, Oracle Directory Services ensures high performance, scalability and availability required by the most demanding enterprise and carrier-grade environments. Oracle Directory Services is ideally suited for elastic deployments on premise, in the cloud, or a combination of both. Support for the extensive use of mobile devices allows unrestricted yet secure access to your company assets for improved productivity or business growth. Combined with Oracle Identity and Access Management Suite or your own IAM environment, Oracle Directory Services helps you meet your specific requirements at your own pace while supporting your enterprise growth without disruption.



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

Worldwide Inquiries
Phone: +1.650.506.7000
Fax: +1.650.506.7200

CONNECT WITH US

-  blogs.oracle.com/oracle
-  facebook.com/oracle
-  twitter.com/oracle
-  oracle.com

Hardware and Software, Engineered to Work Together

Copyright © 2015, 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group. 0715