

# Oracle Unified Directory

ORACLE WHITE PAPER | AUGUST 2017






## 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	
Executive Summary	4
Oracle Unified Directory	6
Overview	6
Java-based directory	7
Maturity and Stability	7
Leveraging Oracle Berkeley Database Java Edition	7
Highly Available Solution	7
Performance for current and future needs	8
Social Networking Ready	9
Scale directory service with business growth	9
Advanced replication model	10
Superior manageability and supportability	11
Highly secure directory service	12
A standards based directory server	13
Extensibility Framework for directory services	13
Oracle Unified Directory flexible deployments	13
Single Data Center HA	14
Multi-Data Center HA	15
DSEE and OUD compatibility	16
Embedded directory service	16
What Makes Oracle Unified Directory Elastic	16



Global Index	16
Replication Service	16
Directory Integration Platform	17
The Fusion Middleware Directory	18
A Directory to centrally manage Oracle database users	18
Elastic Directory Deployment Use Cases	19
Traditional Enterprise Using Infrastructure As A Service	20
Directory service for Telecom and Service Providers	22
Providers of Software and Platform As A Service	23
Beyond LDAP - Making Directory Services More Valuable	24
Conclusion	24

## Executive Summary

Applications, whether for internet or intranet, on-premise or in-the-cloud, must be able to authenticate and authorize user access. The foundation to support application authentication and authorization services is an LDAP-based identity store.


While LDAP (Lightweight Directory Access Protocol) is not new, it is not only still relevant, but is also growing in importance as more businesses adopt customer-facing applications, mobile computing and cloud computing-based solutions. This growth results in extremely large number of objects that are managed in LDAP directories.

In addition, new computing initiatives also push the envelope for performance. For example, mobile computing often uses user location or presence data to personalize the service in real-time, resulting in new requirements for un-usually high write performance in addition to high search performance.

Cloud computing has its own characteristics. Cloud services providers start small but with huge growth potential and they are offering on-demand services to their clients, so they require a directory infrastructure that is elastic and can grow with business without huge up-front investment.

A long-standing goal for many organizations is to have a single enterprise identity repository. However, it is not practical due to regulation, politics and technical issues such as common schema for hundreds or even thousands of applications. Maintaining a number of isolated directories in the enterprise comes with significant challenges. It is costly to maintain and support. It is complex to keep current user identity information up-to-date. It is bad user experience to maintain multiple IDs or passwords while creating more help desk calls. Furthermore, it is difficult to enforce enterprise compliance policies and enable Single Sign-On.

Finally, the market has provided various fragmented tools and components to achieve tasks such as storing objects, accessing, synchronizing, consolidating or virtualizing them, but none of the vendors have a unified solution. Achieving interoperability, validation, and certification of disparate components is challenging. The need to learn and maintain many components from multiple vendors render management difficulties resulting in increased operational cost and decreased productivity.



To address the above challenges, Oracle is introducing Oracle Unified Directory (OUD); the world's first unified directory services solution with storage, synchronization, proxy and virtualization.

OUD, together with Directory Integration Platform (DIP), provides unified directory services and uniquely combines virtual directory, meta-directory, and data storage capabilities. Being a Java solution, OUD simplifies multiple platform support, deployment, and ongoing maintenance. OUD and DIP are part of Oracle Directory Services Plus (ODS Plus) suite that also includes Oracle Internet Directory (OID).

OUD brings significant new capabilities to market addressing current challenges and providing support for future growth on demand.

OUD is a "Carrier Grade" directory service that scales to the largest environment. In managing subscribers, it scales with "Carrier Grade" data management for privacy and security. It can perform authentication on the scale of billions of subscribers and related devices to maximize average revenue per subscriber.

OUD, together DIP, is the first and only unified Java-based directory service that provides storage, synchronization, proxy and virtualization capabilities. The unified solution provides architecture flexibility and optimization, accelerates IDM projects and application deployments, and reduces total cost of ownership.

To further speed up deployment and push the envelope for performance, Oracle Optimized Solution for OUD (OOS4OUD), OUD on Oracle T-series hardware and Solaris 11, delivers 3x performances with 1/3 of the cost.

The remaining paper outlines why OUD is the best directory for modern computing environments and how it will save time and money while optimizing return on investment.

## Oracle Unified Directory

### Overview

ODU is a comprehensive next generation directory service entirely developed in Java. It is fully LDAP v3 compliant, easy to deploy and manage, and has monitoring capabilities that addresses large deployments with high performance. ODU, together with the synchronization server DIP and the ODU Proxy for virtualization capabilities, is the industry's first and only Java-based unified directory solution.

ODU's unique design allows it to be flexibly configured for core LDAP storage, LDAP proxy, synchronization and replication with an existing ODSEE instance.

The unified directory approach enables deployment of fewer fragmented components and provides deployment flexibility. High availability and reduced administration is assured via its proxy and replication technology, for monolithic and distributed deployments. For large scale distributed deployments, the global index capability of ODU addresses the traditional limitations of a distributed configuration.

ODU provides support for Elastic Directory Services, enabling support for any deployment scenario to match current and future requirements. The Elastic Directory Services introduces a revolutionary approach that allows adding directory servers and storage on demand without having to stop and start the directory service.

In the past, sizing a directory service infrastructure traditionally was based on maximum capacity required for the next few years anticipating future growth and leading to significant initial capital expenditure.

ODU changes the scenario by eliminating the need to overbuild a monolithic system by providing the following key features:

- » Distributed global indexing
- » Robust and flexible replication services with partial and fractional replication
- » Directory synchronization for identity and password unification with DIP
- » Identity Virtualization natively through Proxy capabilities or integration with Oracle Virtual Directory (OVD)
- » Web-based UI – Oracle Unified Directory Services Manager (OUDSM)

These features provide the elastic flexibility required for current environments including support for cloud computing.

In addition, ODU is integrated with Oracle Fusion Middleware. ODU can be used as the identity store for Fusion Middleware, Fusion Middleware applications, and Fusion Applications.

While ODU core storage is based on the open source OpenDS project, supported initially by Sun and now Oracle, it includes a wealth of unique additional functionalities and capabilities that goes much beyond LDAP storage.

Finally, ODU was developed by the combined engineering team who built ODSEE – and formerly Sun DSEE -, OID and OVD. This team built the most widely deployed suite of enterprise directory products in the world.

## Java-based directory

Oracle Unified Directory is a J2SE application offering lightweight deployment.

A Pure Java approach brings much broader platform choice for deployment. Additional benefits include leveraging Java memory management, reducing exposure to memory leak and server instability and leveraging Oracle and Sun expertise in Java virtual machine, Java coding and tuning resulting in efficiency to bring unmatched performance to the market

ODU, together with DIP is the industry's first and only Java based unified directory solution.

## Maturity and Stability

Although OUD is a relatively new product it is built with proven and mature underlying technologies. It is based on the open source project OpenDS for the core server. It also introduces many innovative features and capabilities such as proxy and global indexes that are only available through OUD.

The best directory experts in the world, who created ODSEE (previously known as Netscape, iPlanet, SunOne directory), OID, and OVD, engineered this next generation directory product. The team re-used many concepts available as part of ODSEE to ensure full compatibility. The underlying technology has reached maturity and stability over the past few years, and has benefited from extensive testing and validation, both in open source for the core server and by Oracle for all components.

Finally our DSEE rich tests and real uses cases scenarios built over years of interaction with our largest customers have been used to validate the stability and maturity of OUD.

## Leveraging Oracle Berkeley Database Java Edition

ODU embarks on the Oracle Berkeley Database Java Edition (OBDB JE). This object-oriented database is the Java Edition (JE) of the database used for ODSEE, with proven stability and years of production. Its Object-oriented data model efficiently maps directory entries to objects in the database.

OBDB JE benefits from the same advantages as OUD by being Java-based. In addition, as the Java Edition requires less I/O than the C edition to complete write tasks, overall write performance is significantly improved.

Finally, changes can be committed at file system level without going to disk to increase write performances and backups are hardware architecture independent providing more restore flexibility.

## Highly Available Solution

Service reliability is extremely important, as many applications depend on a directory service. OUD can be deployed to support reach Service Level Agreements with high availability and even address telecommunication grade demanding environments with 99.999% availability.

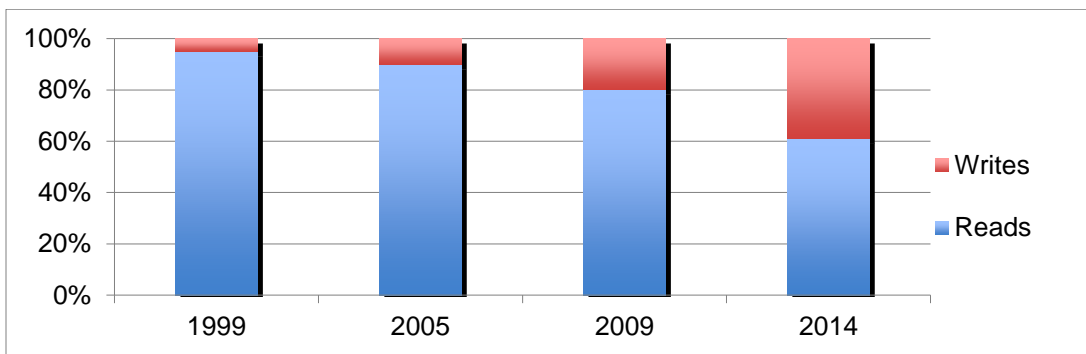
Configurations can be easily architected with OUD proxy to ensure high availability between directory server instances or even between groups of directory server instances.

High availability is not just achieved by two redundant servers in one location. OUD provides flexibility to deploy multiple instances in multiple data-centers located across the globe, so that if there's a major outage in one data center requests can be transparently routed to other data-centers, providing instant geo-recovery. OUD also provides index and backup verification tools to ensure that these are not corrupted or backed up as corrupted.

For configuration that includes data on multiple servers, OUD includes advanced LDAP referrals capabilities such as support for multiple data centers with priority order for referrals, support for private servers in referral links, support for referrals pointing to an IP-load-balancer or a proxy server.

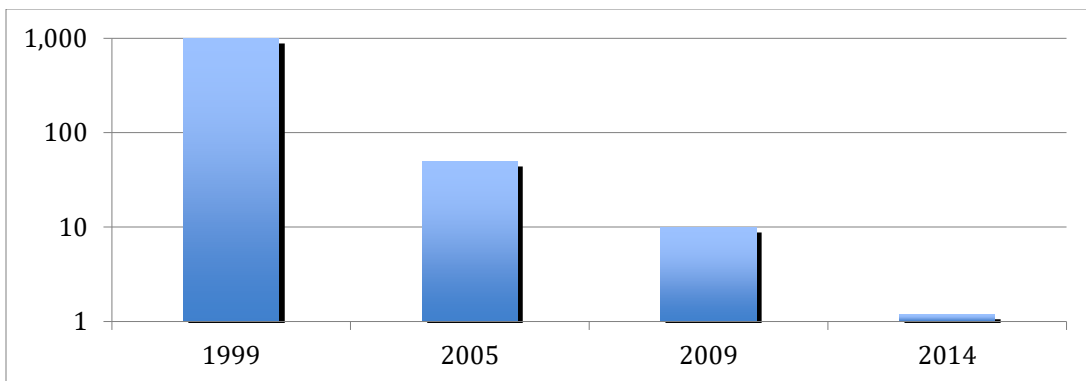
### Performance for current and future needs

Performance is essential for directory services. With traditional directories, created several years ago, the focus was only on maximizing read and search performances. OUD was designed upfront to increase not only read performance but also write performance. This means that it can be leveraged for many new types of applications, for example scenarios where specific attributes might be updated very frequently to reflect status or location.




**Figure 1:** Evolution of read vs. write operations in directory usage patterns as expressed in Requests for Proposals (RFPs)

When it comes to performance, OUD not only provides high throughput for read and write, but it also ensures predictable response time in the micro to milli-second range to maximize application performance.



**Figure 2:** Response time requirements in milli-seconds as expressed in RFPs



Also OUD components can be combined to maximize throughput to reach the highest demands. When hardware limits are reached, it is easy to add additional machines to drive global system throughput even further. Adding more directory server replicas will linearly increase read throughput. If a distributed architecture is selected to reach write performance requirements, the OUD global index will make this much easier as it will be able to keep track of the partition in which a given entry is stored, avoiding performance degrading broadcast operations.

Even if performance is not the primary requirement, leveraging OUD efficiency - with cache usage optimization and auto-tuning - results in less hardware (CPU, Memory, and Disks) to achieve service level agreements. Consequently, total cost of ownership will be much lower than with traditional directory solutions.

Finally, with regard to performance distribution in the long run, OUD was designed to provide consistent performance over time and not only during peak demands.

### Social Networking Ready

Beside high performance in writes to leverage frequent updates to location data stored in user entries, OUD provides proximity search control that can be used to specify proximity conditions using search operation filters.

OUD also includes join search control that retrieves related entry tree chains, such as friends, managers, and so on in a single search operation. For example, one query can return all people in the directory who are within 1 mile of certain location.

### Scale directory service with business growth

Scalability for directory is defined as the ability to grow with business. The OUD architecture supports growth as needed. A monolithic approach to sizing equipment based on current and future requirements is straight forward. However, this might be a costly solution from a CAPEX standpoint. The partitioned approach supplements the directory service with additional servers to support growth when needed to lower TCO.

When configured in proxy mode, OUD provides capabilities to scale by distributing entries across multiple directory server storage instances (distribution partitions).

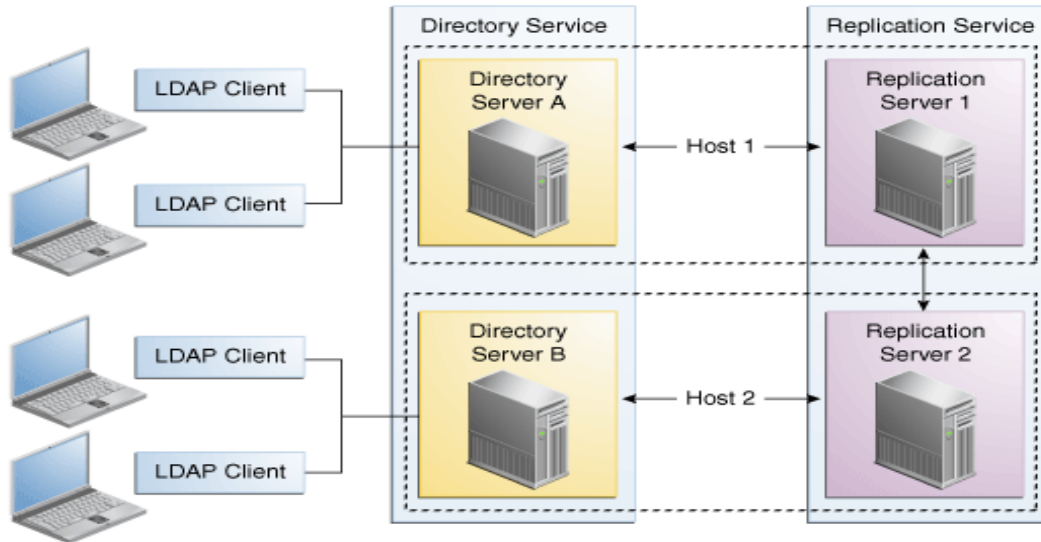
Typical use cases for this partitioned approach include:

- » Deployment of billions of users on commodity servers.
- » Throughput of 50K updates/sec and above.

OUD includes a Global Index capability that maps the directory entries to the distribution partition in which the data is stored. When OUD proxy receives a request from the client, the distribution looks up the attribute entry in the global index, and forwards the client request to the correct partition. This eliminates the need for broadcasts.

### Advanced replication model

Replication is architected to support large-scale deployments with many masters. OUD introduces the concept of Replication Servers that are dedicated to handling replication across the topology. This means that directory server instances remain focused on their primary goal, which is serving client applications, and replication servers remain focused on propagating changes between servers in a timely manner, with low latency.



**Figure 3:** Directory Server instances and Replication Server instances.

Replication provides an *assured* mode, where changes are confirmed to the client application only when information is safely secured in multiple directories. So, it is guaranteed that the change is effectively made in at least two different locations.

To help comply with various regulations and security mandates, OUD provides fractional replication, so that some attributes (such as social security numbers or PIN codes) can be defined so that they would not be replicated to a less secured environment.

Finally, OUD includes a unique, highly available, *changelog* so that external applications can consume directory updates without impacting directory service performance.

## Superior manageability and supportability

ODU provides superior manageability and supportability over other solutions including installation of instances, day-to-day operation, exceptional operations, critical situations and interface into support.

Installing ODU is simple and smooth, leveraging the common Oracle Universal Installer and setup panel so that ODU is up and running in just a few clicks.

For other management tasks, ODU provides a powerful command-line interface, covering 100% of the features and designed to support scripting so that customer can manage their environment with their own administrative scripts. Most of the command-line interfaces also include an interactive mode.

In addition, ODU has a web-based administration console, OUDSM, and is integrated with Oracle Enterprise Manager Cloud Control (EMCC) for management and monitoring:

- » OUDSM is provided as part of ODU distribution and allows administration of LDAP data and all server parameters. OUDSM is the unified administration console for ODU.

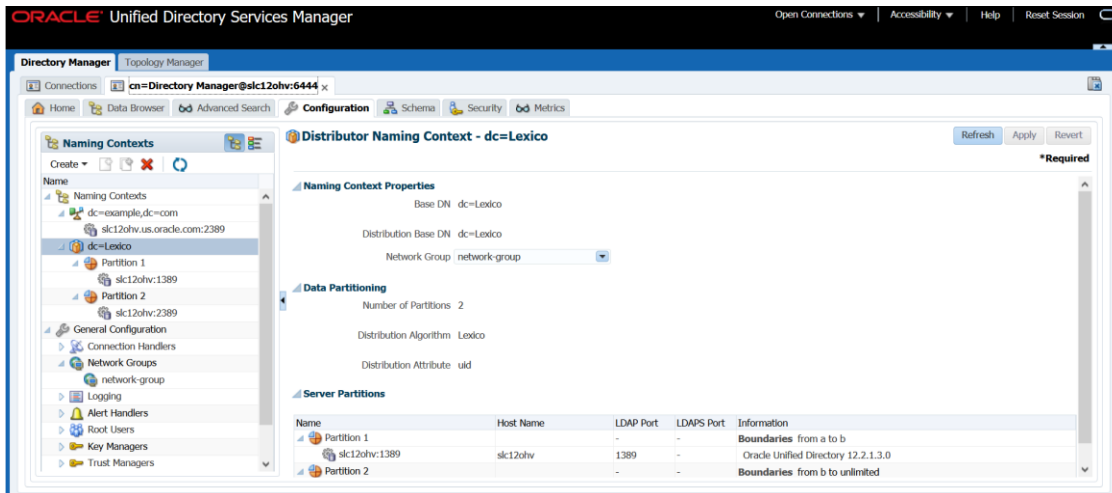


Figure 4: Oracle Unified Directory Services Manager console

- » The EMCC console provides access to many ODU monitoring parameters and provides the necessary archiving to ensure historical analysis.

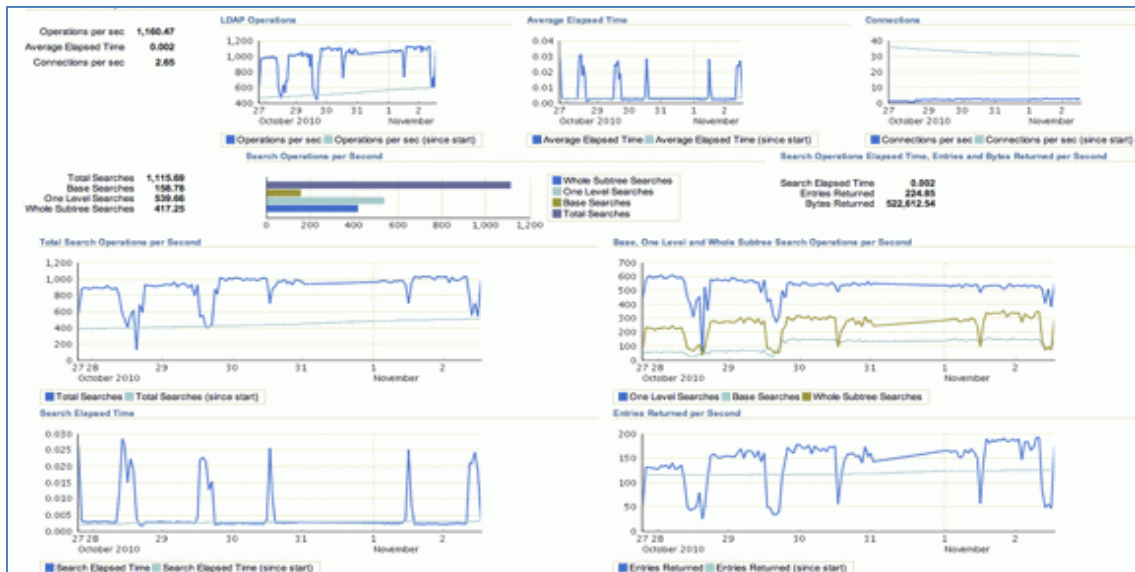


Figure 5: Oracle Enterprise Manager Cloud Control console

All server configuration parameters can be updated dynamically without requiring stop and start cycles to ensure high availability and flexibility. Configuration parameters can be versioned and backed up so that any incorrect configuration can be easily reversed.

ODU provides information that helps to identify abnormal behaviors resulting from users' inappropriate or non-standard requests. This information can be used to optimize indexes, restrict access to certain types of requests, or plan for enhancements.

ODU provides the capability to schedule recurring tasks to more efficiently manage operations and data. This means that certain tasks, for example backups, can be performed everyday at a specific time.

Backups also provide a compression option as well as support for incremental backups.

Importing data from LDIF files can be cumbersome sometimes. ODU provides options, such as selecting only part of the entry to be imported from the LDIF file, erasing the server database before importing data or appending new data to the server database.

### Highly secure directory service

As directory service manages highly sensitive data, security is paramount. ODU provides policy based fine-grained access control including policies based on the type of secured connection through which the directory is accessed. ACL mechanism defines access rules down to the attribute sub-types level.

ODU also includes advanced password policies with:

- » Customizable attributes for storing passwords
- » Password change through extended operations as per RFC 3602
- » Large choice of password storage schemes

- » Password aging with expiration warnings and grace logins
- » Recording of last login time in user entries
- » Temporary account soft locking on invalid passwords
- » User passwords hashed (even during replication) and masked in audit-logs

To protect against dictionary attacks, OUD includes new password validation functionality.

When creating new users, OUD keeps those accounts protected by a preset password that is randomly generated.

Replication is always protected by strong SSL/TLS authentication. As part of the product setup, OUD includes a wizard to directly activate SSL/TLS and to avoid painful SSL/TLS configuration.

In addition, OUD proxy provides an additional point of control for traffic routed to directory servers and it is well suited to secure further access made to the directory to prevent Denial Of Service (DOS) attacks.

Finally, OUD is designed to be secure from its inception. As with all Oracle products, OUD is written according to secure coding practice to avoid introducing risky coding practices that could be exploited by malicious programs.

#### A standards based directory server

LDAP directories have enjoyed great success in adoption, largely because standards that have made directory integration easier and reliable. OUD supports the latest LDAP standards, such as RFC 2696 (Paged results), RFC 3671 (Collective attributes), RFC 4512 (Name forms & DIT (Directory Information Tree) rules), RFC 4514 (Attribute syntax checks), RFC 4525 (LDAP increment), RFC 4527 (Pre and Post operation read controls), RFC 4528 (Assertions), RFC 4529 (Request attributes by objectclass), and draft RFC (Subtree Delete Control).

In addition, to these latest LDAP standards OUD provides the following advanced features:

- » OUD unifies static and dynamic groups via new virtual static groups. This capability enables the definition of the list of participants in a dynamic group, in the same manner as a traditional static group.
- » Ability to search in all suffixes via a single search operation.

#### Extensibility Framework for directory services

OUD includes a public Plug-in API that can be used as an Extensibility Framework to add custom logics into LDAP operation processing to enrich directory services. New services added via plug-ins can be for example: new data-transformation or data-filtering, new algorithms to load balance or to distribute data.

#### Oracle Unified Directory flexible deployments

OUD proxy provides flexible deployment scenarios. In addition, to high availability and additional security, by isolating client applications from directly accessing the directory server instance, the OUD proxy can intelligently route requests to the right server or group of servers based on current server load or on the type of request.

In the case of large-scale deployments, the proxy can increase scalability by distributing the entries across multiple data partitions to avoid managing a single, large underlying database. This makes it easier to manage,

back up, and administer. In this model, data is distributed in smaller standardized data segments. The distribution model is also a means to get more write performance out of the entire solution as each directory server's individual performance adds up to provide the global service write throughput.

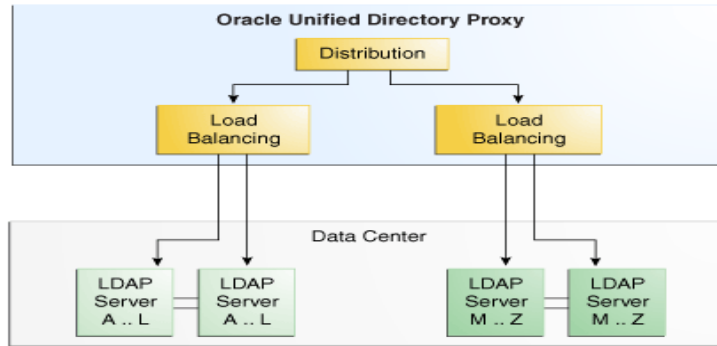


Figure 6: A typical OUD deployment with load-balancing and data-distribution

### Single Data Center HA

Here is a typical OUD deployment with a single data center:

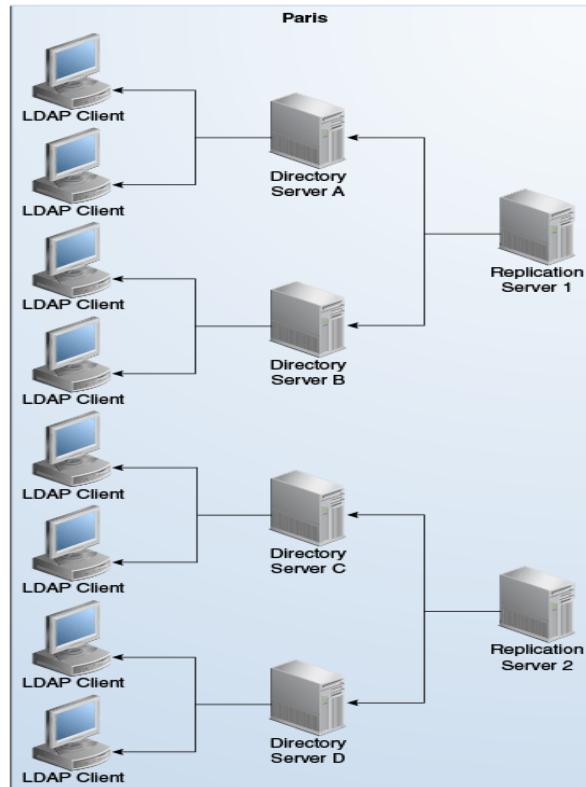


Figure 7: OUD deployed in a single Data-center

## Multi-Data Center HA

Here is what OUD in multiple data center topology ensuring geographical redundancy typically looks like:

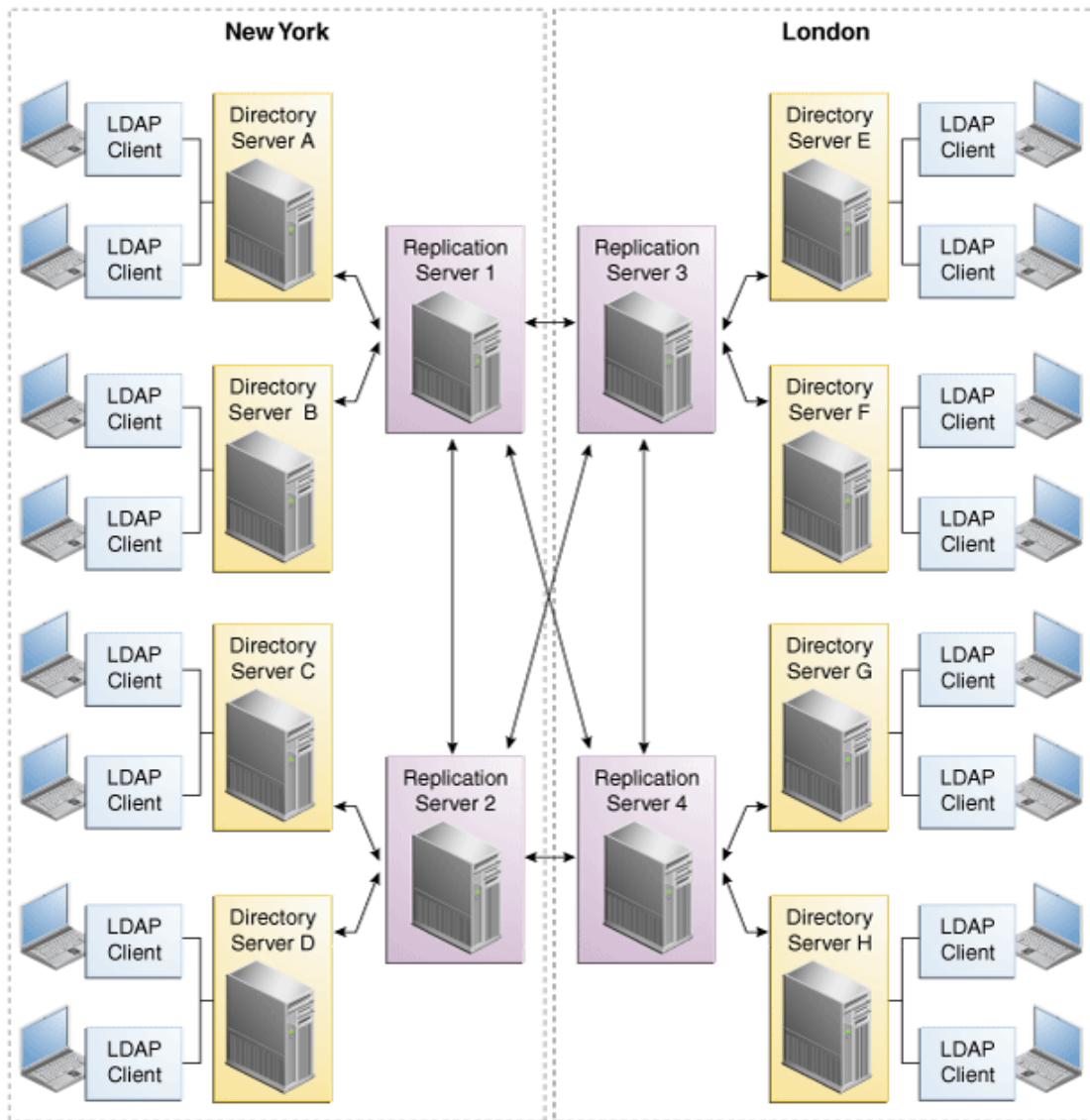


Figure 8: A typical OUD deployment with Highly-Available deployment between two Data-centers

## DSEE and OUD compatibility

DSEE customers may decide to upgrade to OUD. To ease the upgrade, OUD provides out-of-the-box bi-directional synchronization and replication capabilities with DSEE. This enables OUD and DSEE to run in parallel in a mixed environment so that the environment can transition to OUD over time. This also helps validate upgrade strategy application by application, and most importantly, without downtime. The replication gateway service of OUD is designed to handle change synchronization in both directions and to make the required adaptations.

OUD is designed and tested to ensure maximized compatibility with DSEE so that applications supported with ODSEE should work with OUD.

## Embedded directory service

Due to its unique characteristics, OUD can be easily embedded in applications or in hardware. Its small footprint both from memory and disk can accommodate memory requirements, while its light and modular deployment makes it extremely flexible. Finally, as the Oracle Berkeley Database is included in OUD, the directory is a self-contained solution that can be deployed across a large scope of potential hardware.

## What Makes Oracle Unified Directory Elastic

There are three technologies that enable the Oracle Unified Directory to provide elastic directory services.

These are described as follows:

### Global Index

Amazon made the word “elastic” synonymous with cloud computing by providing an infrastructure as a service that allows its customers to add computing or storage capacity on-demand.

The Global Index does the same for directory services by making it very simple for administrators to add storage transparently to client applications.

For example, with traditional directories if a system was designed to support 1 million entries and suddenly needed to support 3 million entries, it would require building an entirely new instance and then migrating the old data to the new instance.

With the Global Index, OUD administrators can add new servers and the Global Index will take care of routing requests to the new servers.

### Replication Service

If an organization decides to deploy new applications on an infrastructure as a service that requires local access to the directory data, it is important to make sure that the data can be replicated securely and easily.

OUD makes it simple to add a new instance to an existing replication topology. This is because the replication service is a separate service from the directories, so it has minimum overhead to the servers themselves.

## Directory Integration Platform

Another key element to elasticity is the ability to synchronize with existing data. This data could exist in other third party LDAP servers or databases.

OID works with Oracle Directory Integration Platform (DIP). DIP is a component of Oracle Directory Services that has been in production for over 10 years. It was originally created to synchronize between third party identity stores and OID. DIP has been enhanced to bi-directionally synchronize with OID without any dependency on OID. When it comes to users and passwords synchronization between OID and Active Directory, DIP performs the task in a unique way that does not require modification or additional software installation on Windows servers running Active Directory Domain Controllers.

The benefits of using DIP are:

- » Keeps data synchronized between the third party identity stores and OID without needing to program or write scripts.
- » Enables administrators to selectively synchronize objects.
- » Allows Administrators to perform data translation during synchronization, for example translate *samaccountname* to *uid*.
- » Handles entry change detection, based on how the data source works, for example *changelog* for certain directories and *timestamp* for sources that do not have *changelog*.

The reason why DIP is important for elastic directory is that if an organization deploys an application in the cloud it needs identity profile information to function. This profile information can be used for authentication, authorization, and personalization.

While there are many ways to eliminate the need to synchronize passwords to the cloud application using technologies such as Oracle Virtual Directory or Oracle Identity Federation, for authorization and personalization, it is better to have some identity info local to the cloud application.

This is because authorization and personalization data is more frequently accessed and thus network latencies can have a significant impact on application performance.

By using DIP it becomes easy to keep the authorization data synchronized to directories in the cloud by synchronizing the data that is needed using DIP.

Another use of DIP with OID is when OID is deployed as an application-specific directory. An application-specific directory is a directory instance that is deployed to meet the requirements of a specific application. Usually this is done to avoid the need to extend schema or change the DIT in the enterprise directory.

While a virtual directory capability can often be used to eliminate the need for an application directory, in some cases it cannot be avoided. DIP makes it easy to keep core identity data (such as name and user id) synchronized in the application directory without affecting the enterprise directory.

## The Fusion Middleware Directory

LDAP directory is at the core of production Oracle Fusion Middleware deployments. Any Fusion Middleware deployment leverages a directory service for authentication, authorization, personalization, and security policy store. For example, an existing third-party directory service may be used for user identity while Oracle Directory Services, including OUD, store extended attributes that applications built on Fusion Middleware may want to use.

The entire Fusion Middleware stack including WebLogic server and Fusion Middleware applications, such as Web Center, SOA Suite, Fusion Applications, and so support OUD as an identity store.

The advantage of using OUD with Oracle Fusion Middleware deployment is that everything is based on Java. If the directory service in the organization is managed by a team that is used to managing embedded-database style directory services (such as with Oracle DSEE) then managing OUD will be a familiar environment.

Additionally, OUD is not limited to just being used by Oracle Fusion Middleware based applications. More broadly, any application that requires LDAP-based authentication, authorization, or personalization can make use of OUD. Thus, a single OUD deployment can be used for supporting Oracle Fusion Middleware applications, traditional enterprise applications and finally new cloud computing deployments that require an elastic directory service. Furthermore, it maintains full compatibility with ODSEE, so the applications run with ODSEE today will work with OUD.

## A Directory to centrally manage Oracle database users

OUD can centrally manage Oracle Database user accounts to simplify database user management. OUD is also able to proxy requests to other directories. OUD for Oracle Enterprise User Security supports:

- » Management of schema or role mapping at an enterprise level via the Enterprise Security Manager.
- » Unique passwords to the database schema instead of shared passwords.

Oracle Enterprise User Security allows:

- » End users to authenticate user name and passwords to the database, which are stored in OUD.
- » Enterprises to map users and groups to a shared schema instead of having multiple people share a schema password.
- » Management of roles (enterprise roles) in the directory to database roles.

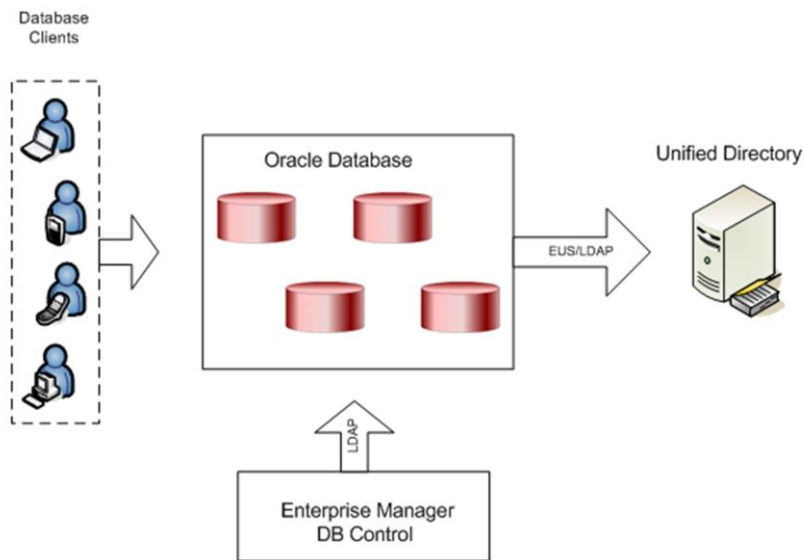


Figure 9: Typical Deployment of EUS with OUD

## Elastic Directory Deployment Use Cases

An elastic directory is different from a traditional directory model by being designed to explicitly support the variety of use cases that modern directory services require. For example, historically most organizations were focused on building a single enterprise directory service.

While OUD can be used for traditional directory use cases, it also supports elastic deployments as a true elastic directory service.

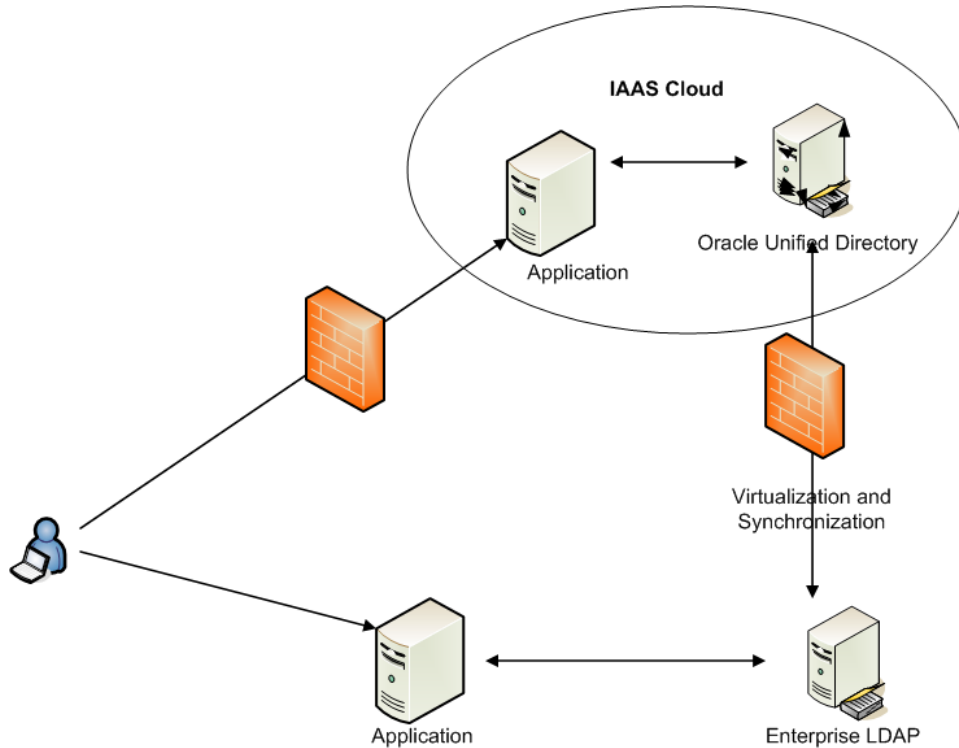
This section defines what that means and why organizations need an elastic directory service to take advantage of next generation hardware and applications.

There are three general areas where elastic directory can have the most productive use.

They are:

- » Traditional Enterprise Using Infrastructure As A Service
- » Telecom, Cable, and Internet Service Providers
- » Software and Platform As A Service Providers

## Traditional Enterprise Using Infrastructure As A Service



**Figure 10:** Example Infrastructure As A Service Deployment

One of the fastest growing areas of IT is the use of external computing infrastructure, such as those provided by Oracle Cloud, Amazon Elastic Cloud Computing (Amazon EC2) or Rackspace. Oracle already supports running Oracle products in these environments including Oracle applications such as PeopleSoft, Enterprise Business Suite, and Siebel.


Additionally, customers can run their own internal applications, such as those written in PHP, Java, or SOA-suite.

The benefit to customers is that they can now take advantage of the cloud-based infrastructure for testing, disaster recovery, or easier procurement, assuming they are allowed to use these resources as external to the IT infrastructure, in particular for identity and access management.

These hosted applications may also have a need for their own identity stores for authorization, personalization, and policy. To reduce latency it is better to keep this data stored in the same cloud infrastructure as the applications.

Oracle Unified Directory elastic directory functionality offers an easy solution.

First, OUD can be easily deployed either as a full install, which implies installing both the management and server components or customers can choose to install only the server components. The hosted server can then either be managed entirely via the command-line or via a centralized administration console located within the internal IT hosted infrastructure.



Second, OUD provides two ways to easily keep identities and roles synchronized with the internal enterprise directory. One way is to use OUD replication, if the enterprise directory is also an OUD. This replication could be a complete replica or just a subset of the data (for security and confidentiality reasons) called fractional replication. Another way to keep data synchronized is to use DIP to synchronize data between an enterprise identity store, such as Microsoft Active Directory and OUD. Customers can also use an existing provisioning system to keep identities synchronized if they choose.

Third, for applications that rely upon LDAP for authentication, OUD provides the following options to ensure that users that login to cloud application have the same user name and password as their other applications:

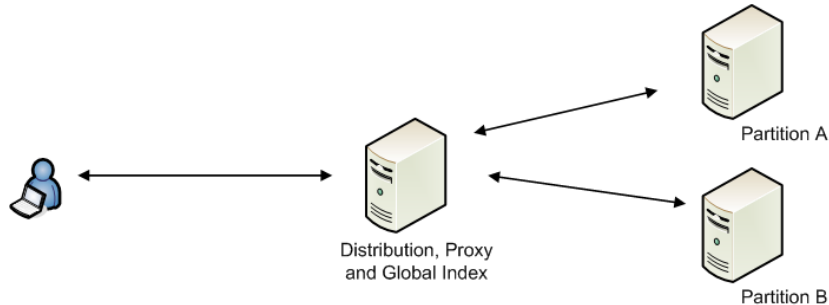
- » OUD replication service can replicate the password.
- » DIP can synchronize password changes.
- » Customers can leverage OUD Proxy or deploy OVD with OUD. With OUD Proxy or OVD configured as a directory firewall in the enterprise DMZ, it is easy to configure the environment to directly authenticate securely against the enterprise LDAP store, while keeping the rest of the data local in OUD.

It is fairly easy to have application-specific OUD servers in the cloud, if necessary, because OUD can be installed in a server-only mode. While in a traditional enterprise it is better to have consolidated directory services, for cloud applications (specifically those that might be temporary), as demonstrated in next paragraph it might make more sense to have application-specific directories that store only specific information for those applications.

While it is ideal to have a central directory for user name and passwords, for application-specific attributes, it makes more sense to have application-specific directories because it decentralizes upgrade and patch windows. For example, there are 20 applications that use LDAP. Four of these applications have their own specific schema extensions. For those four it's better that they each have their own application-specific directory, because that way they can upgrade their own application without affecting the rest of the enterprise directory. Also, they can use identity virtualization to eliminate the need for password synchronization. The other 16 applications can use a central enterprise LDAP.

Oracle Directory Services capabilities (such as directory synchronization, replication, and virtualization) can then be leveraged to keep the core data (such as user names, passwords, and roles) in synch with the enterprise directory.

## Directory service for Telecom and Service Providers



**Figure 11:** Example Infrastructure for Telecom and Service Providers

Telecom and service providers continue to see growing numbers of subscribers, customers, and service offerings. To provide optimal customer support and efficient operations they need to deploy a centralized subscriber store.

However, these types of operations need to be fast with ability to scale quickly without requiring a fully sized and provisioned solution on the first day of service. This is where the global index functionality of OUD provides the required elasticity. This feature allows-, OUD customers to add directory storage as required by customer and application demands.

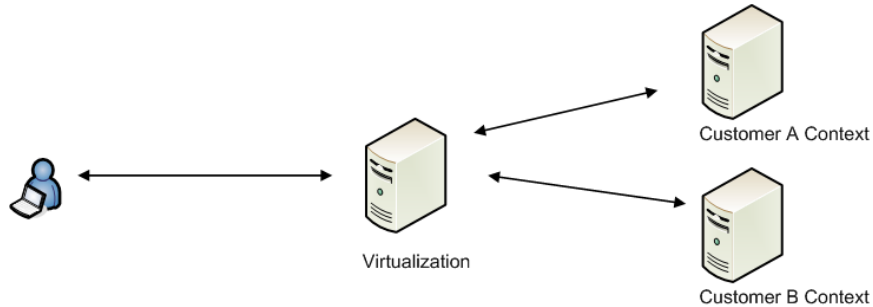
For example, imagine an organization deploys a new Web application that initially only has a few thousand customers. The application goes viral and now they have hundreds of thousands or even millions of new customers. The organization would need to quickly add storage capacity while minimizing capital expenditure.

With the global index feature, new directory storage instances can be added without requiring migration. OUD automatically takes care of adding the users to the new storage as the environment requires.

This means that customers can deploy a single service and only spend the time and capital on the hardware as their customer base grows.

For example, in a telecommunications company a subscriber profile is often split between static information hosted in multiple databases and LDAP servers. The benefit of elastic directory is that a single interface can be provided the links of this data into a single standard interface. OUD Proxy or OVD is used to provide the single point of contact and can query the master database(s) directly for infrequently used data. OUD would be used both to store LDAP-specific attributes (such as passwords) while DIP can be used to synchronize frequently used data from the master database(s) to OUD to reduce latency and query times.

## Providers of Software and Platform As A Service



**Figure 12:** Example Infrastructure for Providers of Software and Platform As A Service

Providers for Software and Platform As A Service have similar requirements as the Telecom /Service Provider use case (meaning they can also benefit from global index) but in most cases they also need to meet multi-tenant requirements.

In a multi-tenant environment, data for different customers are stored in a single directory service. This means that the directory service will host a directory for multiple companies.

ODU also provides features that can make it easier to support multi-tenant directory storage.

First, tenants should be stored in their own directory branch (called a context) and this context can be stored in its own underlying database.

Second, OUD access control lists can be configured so that tenants in one context are not able to access data in another context. For example, the data administrators (as opposed to the personnel who run the actual OUD service) can be restricted to accessing only the Directory Information Tree (DIT) to which they are allowed access.

Third, OUD is integrated with Oracle Fusion Middleware Auditing, providing a comprehensive auditing record of all activities on the system. Oracle Fusion Middleware Auditing also provides a reporting engine (using an included restricted Oracle BI Publisher license), which can be used to generate tenant-specific audit reports.

## Beyond LDAP - Making Directory Services More Valuable

While LDAP is the most widely used standard protocol for authentication and authorization, developers prefer to use Web services to access enterprise developers.

Oracle Directory Services (of which Oracle Unified Directory is a part) enables developers to rapidly build directory-enabled applications without having to know anything about LDAP or LDAP-specific APIs.

There are two ways to do this:

- » DSML v2– Directory Services Markup Language is a standard that provides a SOAP-based Web service access to directory information.
- » Identity Governance Framework (IGF) ArisID Java Interfaces -- The ArisID Java bindings are designed for Java developers who use Oracle Fusion Middleware to write their applications. It is similar to the REST interfaces (in fact, the REST interfaces are built by Oracle using the Java ArisID Interfaces) except using Java. Oracle provides an extension to Oracle JDeveloper to enable rapid application development.

## Conclusion

ODU, together with DIP, is the industry's first and only Java-based unified directory solution to provide storage, synchronization, proxy, and virtualization. It addresses the fragmented solution challenges that enterprises are facing today and significantly reduces total cost of ownership.

Its elastic scalability, high availability, superior performance, and enterprise manageability delivers carrier grade services that scale on demand with business growth.

It is full compatibility with DSEE and enables existing customers to run both DSEE and OUD together in mixed environments with zero downtime upgrade.




Finally, because OUD adheres to the LDAP standards and integrates with Oracle Fusion Middleware platform, it runs easily with existing applications and maximizes the value of data in directory.



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](http://blogs.oracle.com/oracle)
-  [facebook.com/oracle](http://facebook.com/oracle)
-  [twitter.com/oracle](http://twitter.com/oracle)
-  [oracle.com](http://oracle.com)

**Hardware and Software, Engineered to Work Together**

Copyright © 2014, 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. 0817

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