An Oracle White Paper
September 2011

Oracle Internet Directory 11g

ORACLE

Executive Summary

Directory Services are critical components in an enterprise application infrastructure, providing applications with identity services such as user profiles, access and authorization data. Well-structured and organized directory services are the foundation of efficient and effective identity management solutions that enable enterprise applications.

One of the identity management challenges enterprises face is the lack of a single source for identity data and the proliferation of identity stores, including directories and databases. Enterprises have employee information in HR databases and/or Active Directory (AD), customer and partner data in CRM databases and/or LDAP directories. Since AD is the Network Operating System directory for 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.

In addition, new computing initiatives, such as mobile computing, cloud computing and social networking, brings new challenges, As the population with smartphones like iPhone explodes, and as the number of social netwoking users grow exponetially, it results in extremely large number of objects that are managed in LDAP directories.

In addition to extremely large number of managed objects, 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 extremely high write performance in addition to high search performance.

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

Oracle Directory Services Plus (ODSPlus) addresses these challenges with a unique solution that provides complete storage, proxy, synchronization and virtualization capabilities. ODSPlus includes Oracle Unified Directory (OUD), Oracle Virtual Directory (OVD), Oracle Directory Server Enterprise Edition (ODSEE), and Oracle Internet Directory (OID).

- OUD is the newly introduced, next generation directory that provides storage and proxy capabilities in one product, and together with OVD and Directory Integration Platform (DIP), provides all Java unified directory services and uniquely combines virtual directory, meta-directory and data storage capabilities.

- OVD is the market leading virtual directory server that provides identity aggregation and transformation without data copying and synchronization.

- Oracle Internet Directory (OID), built on Oracle Database and fully integrated with Oracle databases, middleware and application products, handles data storage and synchronization services.

- ODSEE, former Sun directory also known as iPlanet, SunOne directory, is lightwieght and most deployed for heterogeaous environment with storage and synchronization capabilities.

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

OID has the ability to store multiple contexts to manage data otherwise spread in multiple sources into a single instance. With built-in high availability features like directory replication and cluster support, together with extreme performance demonstrated in the two-billion-entry benchmark and OID-ExaData 500-million-entry bechmark, OID is built to be a general purpose directory required for identity data storage in an enterprise, while its full integration with Oracle technology stack makes it an ideal fit to Oracle environment..

Business Challenges and Requirements

Directory services are key building blocks for secure 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 that 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, new computing initiatives, such as mobile computing, cloud computing and social networking, require LDAP to manage extremely large number of objects, to deliver high performance to manage dynamic data like location and presence, and to be elastic to grow with the cloud.

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

- While Microsoft Active Directory is pervasive within enterprises, it does not provide the functionality to be a general purpose Enterprise Directory Service because of limitations imposed on it being the Network Operating System directory for Windows.

- To address Active Directory limitations, Microsoft provides Active Directory Lightweight Directory Services (AD LDS)1. However, due to AD LDS's application specific nature, the

[1] AD LDS formerly known as Active Directory Application Mode (ADAM)

proliferation of AD LDS within enterprises is like weeds in a garden resulting in cost and manageability issues.

- In addition to AD and AD LDS, enterprises also have many other directories with identity data spread and duplicated amongst them.

- Furthermore, the source of truth for identity data is usually the HR database and Master-Data-Management solutions that are not accessible by LDAP applications. As a result, LDAP directories are added to synchronize data from these authoritative data sources.

These challenges result in high administration and maintenance cost, inconsistent identity data, insecure systems, and difficulty in compliance.

Thus a modern general purpose directory service solution is needed to address these challenges to help organizations improve ROI from existing resources, simplify the management of identity attribute data and reduce costs by eliminating the need to have directory server proliferation.

To meet these needs the solution must provide:

- Service-oriented access layer including both LDAP and Web Service access points

- Ability to aggregate identity data from multiple, heterogeneous stores including LDAP, databases and Web Services without needing to synchronize the data into a central store

- Ability to provide scalable, secure and flexible storage to facilitate both legacy directory consolidation as well as provide for storage for new computing initiatives

- Unified management console which includes integration with carrier-grade operational monitoring system

Solutions

Only Oracle Directory Services Plus (ODSPlus) provides a directory service solution that meets above requirements. 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 Oracle Unified Directory (OUD), Oracle Internet Directory (OID), and Oracle Directory Server Enterprise

Edition (OSEE) provide data storage and synchronization services. This white paper focuses on OID, and OVD, OUD and ODSEEare covered separately in their own white papers.

Oracle Internet Directory is the only directory service that provides the capabilities to meet modern enterprise directory storage requirements as a general-purpose directory and better fits with oracle environment.

- OID provides the ability to store multiple contexts, thus disparate data can be managed in a single service. For example this means it is possible to eliminate the need to have different Active Directory LDS instances that were created to handle different directory schema for different applications.

- OID is able to scale to extremely large deployments on less hardware with high performance as demonstrated by its published Two-Billion-Entry Benchmark test. This reduces the footprint required to deploy enterprise directory services in the data-center resulting in cost savings and a greener enterprise.

- OID is the most secure directory service providing security at every level from data in transit to storage and backups. In addition to LDAP security, it leverages Oracle database security features like Database Vault and Transparent Data Encryption. Database Vault enables separation of duty (SOD) while Transparent Data Encryption secures data in storage and backup.

- OID provides several layers of high availability (HA) to ensure maximum availability. In addition to multi-master LDAP replication, OID also supports Oracle database Real Application Cluster (RAC) and Oracle Application Server Clusters (OracleAS Cluster).

- OID provides un-paralled ease of use for a general purpose directory storage via Oracle Directory Services Manager (ODSM). Gone are the days when managing common person & group data meant scrolling through lists of hard to decipher attributes. OID data management is intuitive and leverages the latest Web 2.0 technology. ODSM is the common unified management console for all Oracle Directory Services products including OID and OVD.

- OID provides advanced tools to help enterprise standardize on it and consolidate multiple Active Directories, AD LDS, Sun, eDirectory, OpenLDAP, etc into a single directory storage. Specifically, OID provides directory migration utilities and directory synchronization solutions to facilitate the standardization process.

Benefits

Increased ROI and reduced cost

- Standardize on OID as the general purpose directory reduces the number of directories.
- Data integration with AD leverages AD enterprise investments, preventing the need to add an AD LDS for each new application.
- Better leverage on existing OID infrastructure and expertise that comes with Oracle applications.

Enhanced Security

- Data security in transit, storage, and backup.
- Separation of duty (SOD) with Oracle Database Vault.

Out of the box Application Integration

Oracle's directory strategy is to directory enable all of Oracle's products. As a result OID is the optimized directory solution for Oracle applications and Oracle Identity and Access Management solutions, E.g., Oracle Access manager, Oracle E-Business Suite, PeopleSoft, Siebel CRM, etc.

In addition, OID is the only directory supported by Oracle Database Enterprise User Security (EUS) to centralize user and role management, and is the only directory that provides fully automated integration with Unix and Linux operating systems to centralize account management (Oracle Authentication Services for Operating Systems).

Oracle Internet Directory Technical Details

Architecture overview

Oracle Internet Directory is designed to provide a highly available and scalable directory infrastructure with high performance. It is a general purpose directory as part of Oracle Identity Management Suite.

Oracle Internet Directory (Figure 1) provides a unique, robust, and secure platform for enterprise directory services. By implementing LDAP services on top of Oracle database

technology, Oracle Internet Directory can provide LDAP directory services with an unprecedented level of scalability, high-availability and information security.

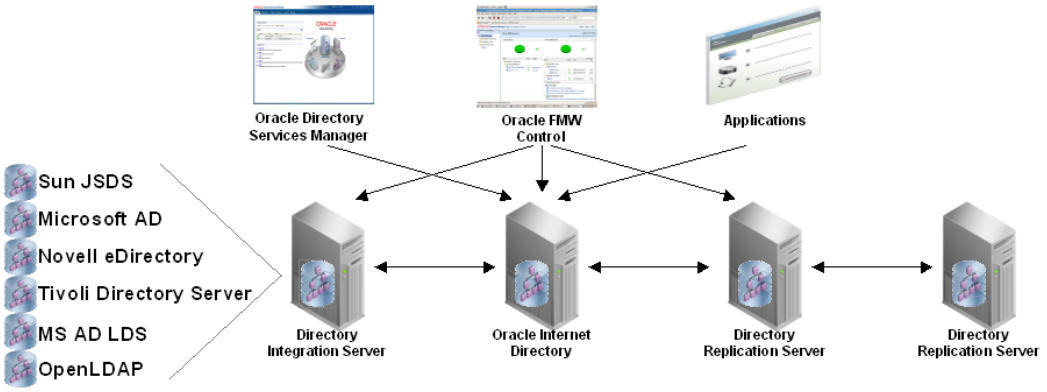

Figure 1: **Oracle Internet Directory Components**

Key Functions

Scalability

Scalability of a directory service can be evaluated in a number of different ways. For example, scalability can be related to the total number of objects supported in a directory tree, or total number of concurrent clients and queries supported. Another aspect is the ability of the directory to scale with the hardware is run on. Oracle Internet Directory addresses all aspects of scalability:

- The number of entries, or directory objects that can be supported on a single server instance.
- The number of simultaneous client accesses supported by the server.
- Scale with the number of CPU's per server or nodes in a HW cluster

Experience has shown that these aspects of scalability are of particular interest to service providers, such as telcos and extranet environments, because they require to a large degree the number of directory server nodes required to support a given directory information tree.

Oracle Internet Directory has demonstrated industry-leading performance in large scale deployments. Most recently a two billion (2,000,000,000) users benchmark was performed which demonstrated 101,000 searches/sec with 800 clients, and 99,500 searches/sec with 16,000 clients on a single Linux server with 32 CPU's and showed almost linear scalability by enabling more CPU's.

The architecture of Oracle Internet Directory supports throughput and scalability in a couple of ways.

- The LDAP servers running on an Oracle Internet Directory server node are multithreaded to use database connection pooling to prevent running into resource limitations as the number of simultaneous LDAP client connections increases.
- The ability to run multiple LDAP server processes on a single Oracle Internet Directory server node. This architecture scales very well vertically by increasing the number of server process per HW node as well horizontally by distributing server processes over clustered HW nodes.

Oracle Internet Directory's 'multi-threaded, multi-process, multi-instance' architecture is unique in the industry.

High Availability

High availability is a concern for all enterprise environments. Business applications depend on user identity information stored in directories, failure often means unavailability of the applications to users, for example, if users fail to login. Oracle Internet Directory is designed to enable continuous service availability at different layers, on the OID server process level and the data storage level. For data distribution, two types of replication are supported:

- Advanced Symmetric Replication Services (ASR)-based – Multi-master replication between Oracle Internet Directory servers ensures that if any of the servers in the replicated environment goes down, any other server can act as the "master". Based on robust and field-proven Oracle Database replication technology, this ensures full availability even in the event of hardware failure.
- LDAP based multi master replication with any number of nodes is another option with release 11gR1. LDAP replication compared to ASR based replication provides more flexible deployment topologies with very little overhead and very granular filtering and partitioning options.

The flexibility to combine these replication options in a single architecture offers the best possible solution for the deployment of highly available and distributed directory services. Administrators can add, delete, and populate directory server nodes in a replicated community of servers without loss of availability.

Replication handles geographic data distribution for HA purposes. For local HA, Oracle Internet Directory leverages a number of high availability features from Oracle's Application Server and Database servers. This includes technology such as Real Application Clusters (RAC) and Oracle Application Server Cluster (OracleAS cluster). Figure 2 below shows an example of a deployment using both technologies.

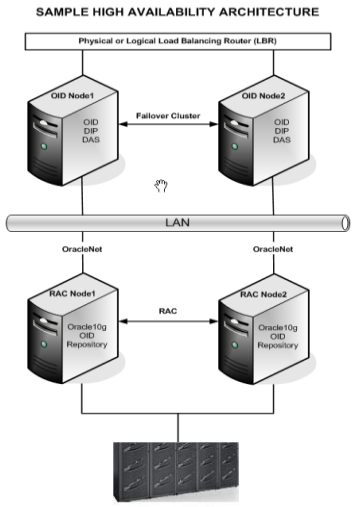

Figure 2: **Standard high available Oracle Internet Directory deployment**

The two local HA features, OracleAS cluster and Oracle RAC can be combined with OID's flexible, one way, two way, or multi master replication topologies to achieve a Maximum Availability Architecture (MAA) which is required for geographically distributed data centers. More details can be found the MAA admin guide.

Information Security

Oracle Internet Directory administrators can define their directory service environment so as to provide different levels of access to the directory information based on how a given user was authenticated. Both password and certificate-based authentication are natively supported.

Integrated access controls (ACL) support very fine-grained control over how access to data is granted or denied. For example, user entries in a directory might have several attributes associated with them. These could be things like phone numbers, e-mail addresses etc. An administrator may want to give anyone the ability to look up an e-mail address in the directory. He/She may want to require a password before displaying more sensitive information such as department and telephone numbers. Finally, she may require strong authentication by authorized personnel before exposing Social Security Number. All of these access privileges can be defined with Oracle Internet Directory.

Since Oracle Internet Directory can be used for user authentication, it also provides sophisticated password policy support.

Password polices govern how passwords are used and the criteria for creation. They can specify, for example, the maximum length of time a given password is valid or the minimum number of characters a password must contain.

Oracle Internet Directory supports external authentication for users when user passwords are stored in third party directories and not synchronized with Oracle Internet Directory. This provides for easy and accelerated deployment along-side existing directory infrastructure to address some of the concerns associated with copying passwords.

With 11g R1, Oracle Internet Directory offers attribute level encryption. Administrators can specify a list of sensitive attributes that have to be stored encrypted in the directory for higher protection.

Another layer of protection is build around preventing denial of service (DOS) attacks, which is important when 24x7 availability is required for OID as a central component for user authentication.

In addition, OID supports two unique database security features, Oracle Database Vault and Oracle Transparent Data Encryption.

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

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

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

The LDAP security functions, together with Oracle database security functions, clearly distinguish Oracle Internet Directory from others.

Superior Usability

OID 11gR1 delivers superior usability with Oracle Directory Services Manager (ODSM). Based on Oracle's Application Development Framework (ADF), ODSM provides administrators with an easy-to-use administration tool leveraging Web 2.0 technologies.

ODSM is the unified management tool for both OID and Oracle Virtual Directory (OVD). Instead of having to go through a learning curve to get used to two distinct administration tools

for two components (OID and OVD), ODSM guides the administrator through the various tasks to manage both servers.

Extensive use of deployement accelerators relief the administrator of requiring to know every detail when creating e.g. new schema objects or users. Predefined templates for users and groups display the most relevant information at a glance. Visual hints like icons distinguish users and groups from standard directory data. User and group data can be presented in a more user-friendly way than other directory objects.

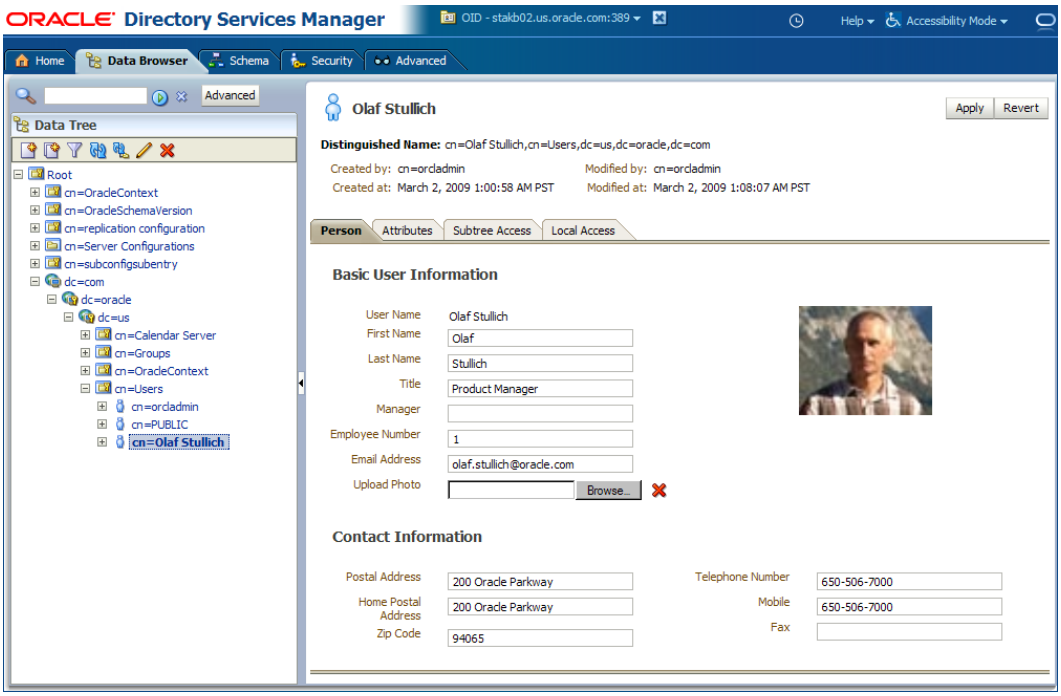

Figure 3: Oracle Directory Services Manager

Other deployment accelerators include wizards for sizing and tuning Oracle Internet Directory and setting up and configure LDAP replication.

The sizing and tuning wizard is built upon the knowledge base of best practices collected during the last ten years together with feedback from production deployments. The wizard can be used standalone without having OID installed. The sizing part provides a best estimate for database tablespace layout and generates the required SQL statements, based on the number of entries, objectclasses used, size of attributes and many other factors. The tuning wizard collects the very details of the planned Oracle Internet Directory usage and based on these factors generates a list of OID and DB tuneable parameters.

To simplify replication setup, the LDAP replication wizard guides the administrator through the process of setting up one way, two way or multimaster replication. The wizard is reentrant, e.g. once a multi master replication is setup, adding or deleting nodes to the existing multi master ring or add / delete fan out nodes in a topology will be performed using the same wizard. The wizard easily handles the very granular tasks to create complex naming contexts including or excluding specific attributes into replication agreements.

Deployment accelerators are accessible through Oracle Enterprise Manager 11g Fusion Middleware Control.

Another aspect of usability (or diagnosability), built into all FMW components, including OID and DIP, is the introduction of execution context identifiers (ECID) attached to directory operations. This is particular useful when an administrator needs to trace an operation, say failed user login, through the complete software stack starting with the web server all the way down to OID and finally the DB. This significantly improves error resolution.

Integrated Management and Monitoring

With the 11g release, administration, managing, and monitoring of Oracle Internet Directory has been streamlined around two complementary components, Oracle Enterprise Manager 11g Fusion Middleware Control (OEM) and Oracle Directory Services Manager (ODSM). OEM is Oracle's system management solution that provides management and monitoring of OID distributed processes and their performance including host characteristics. ODSM is the administration UI that supports administrative tasks like LDAP data browsing, schema creation and modification, manage directory data security and advanced operations such as directory 'changelog' management.

Oracle's flagship system management product, Oracle Enterprise Manager provides an integrated framework for system management and monitoring of distributed deployments from one central place. This provides "administrative transparency" for Oracle shops looking to deploy Oracle Internet Directory in a way that leverages existing Oracle product expertise.

Features include:

- Process Monitoring & Control
- Performance Monitoring – Identity Management and related infrastructure components e.g. database, host, Application Server
- Alerts (Identity Management and related Infrastructure components)
- System Topology Viewer – Identity Management, host and related infrastructure components
- Log management and system troubleshooting
- Audit management and Reporting Framework

- Software deployment and patch management

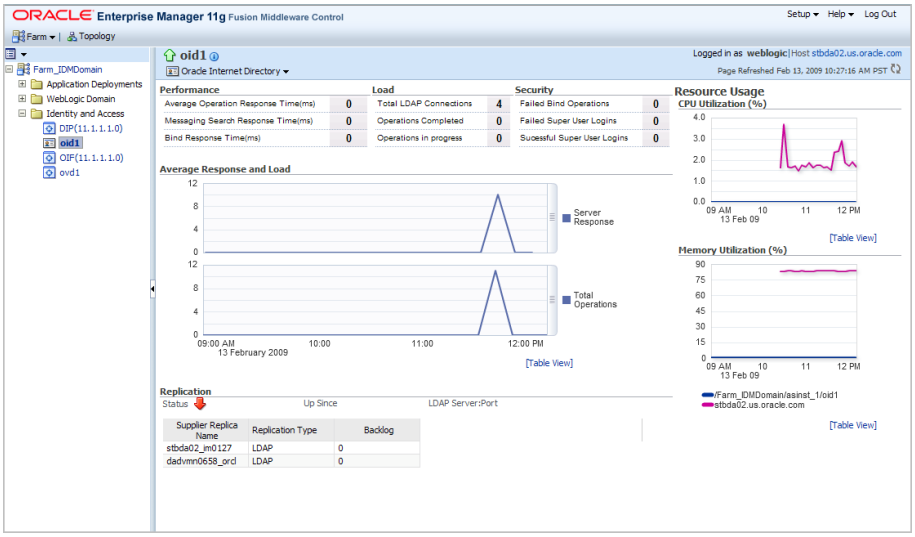

Figure 4: **Oracle Enterprise Manager 11*g* Fusion Middleware Control**

The EM homepage prominently displays the most critical directory operational information like load characteristics or security alerts together with performance and replication related data at a glance.

Every possible aspect of performance monitoring is available in the detailed monitoring dashboard where the administrator can create a customized view of every aspect related to response times and resource usage.

Accessible via OEM are Fusion Middleware services that are leveraged by Oracle Internet Directory. These services are end-to-end network layer security (SSL) configuration and Audit management.

Every administrator who has configured SSL knows how tedious this process can be. Generating certificate requests with the correct information, importing the server certificate and trustpoints and storing them into the correct wallet location, errors can happen at any point of the process. OEM provides a convenient user interface to enter the information and test the configuration.

The audit management framework provides built in compliance to create audit policies for:

- User sessions
- Authorization
- Data Access

- Account Management
- LDAP entry access

Oracle BI publisher is used for audit report generation, with a wide variety of out of the box and customizable reports.

In addition, Oracle Internet Directory integration with he FMW logging framework with standardized error message and enhanced search capabilities relieves the administrator from digging through large log files.

Oracle Directory Integration Platform

Oracle Internet Directory includes the Directory Integration Platform (see Figure 1), enabling customers to synchronize data between various third party data sources and Oracle Internet Directory. Synchronization ensures that changes to directory information are kept consistent between source and target. Synchronization is distinct from replication where source and target are OID.

The Directory Integration Platform is a set of services and interfaces to enable synchronization with other enterprise repositories, and can be used to provide Oracle Internet Directory interoperability with third party meta-directory solutions.

Directory Integration Platform includes connectors for out-of-the-box synchronization with Oracle e-Business Human Resources, Oracle Databases, as well as connectors for synchronizing information with third party LDAP servers, such as Sun Java System Directory Server, Microsoft Active Directory, Active Directory LDS, Novell eDirectory, OpenLDAP, and new with 11gR1 IBM Tivoli.

With Directory Integration Platform, customers can build a single enterprise directory using OID with global directory entries containing data from diverse sources for both user authentication and authorization data, and application configuration data.

The Directory Integration Platform is managed and monitored in EM. Following the same usability guidelines as with OID, deployment accelerators guide through the process of profile creation and graphically mapping attributes between the target directories and OID. Like replication the synchronized data can be specified very granularly and the synchronization engine takes care about the transformation process that needs to happen when data is moved between heterogeneous data sources.

Migration and Consolidation Tools

As part of a migration and consolidation process to reduce the number of enterprise directories and application repositories, Oracle provides various tools to help migrating dispersed data into a consolidated Oracle Internet Directory. Migration will replace the existing directories with a

centralized directory. If it is not possible to replace an existing directory the directory integration platform handles the data consistency via bi-directorial synchronizing.

The first phase of migrating a third-party directory is to create directory schema metadata like attributes and object classes in OID and compared for consistency, and doing this manually is an error prone and time consuming process. The "schemasync" tool automates this task and supports the administrator in the migration process.

The second phase is to export data from the repository and transform it into a LDAP data interchange format (LDIF). The "ldifmigrator" tool generates a LDIF file based on customizable templates and the exported data. Optionally, for a third party directory, the Directory Integration Platform bootstrap feature can be used to load the data into OID, omitting the otherwise required "bulkloader" phase.

Finally the "bulkloader" checks for data consistency, generates intermediate data files and loads them, bypassing the standard LDAP protocol overhead, and directly changing OID database tables content. At the same time new users can be added or modified using LDAP protocol. The feature is useful to transfer large data amounts from development to stage to production or vice versa. Bulkloader can load more then a million entries per hour.

External Authentication

Another integration and security aspect is OID's external authentication feature which enables seamless authentication against external directories, such as Microsoft Active Directory, Active Directory LDS, SUN Java System Directory Server, Novell eDirectory, and OpenLDAP. In many cases, this can completely remove the requirement to synchronize sensitive password information into OID.

Extensibility and Client Side Development

Oracle Internet Directory 10*g*R1 (9.0.4) was the first to support server extensibility based on a PL/SQL plug-in framework. These PL/SQL program units or plug-ins allow developers to extend or replace LDAP operations with functionality based on their requirements which can include:

- Validating data before the server performs an LDAP operation with the data.
- Auditing of actions after the server successfully completes an LDAP operation.

With version 10*g* R3 (10.1.4) the plug-in framework also supports Java, to open extensibility to a wide developer community.

Client integration for Oracle Internet Directory can be provided through any LDAP-compliant software development kit. These are widely available for a variety of languages including C, Java, PERL, PHP and others. In addition, Oracle offers the Oracle Internet Directory SDK, which is

intended for application developers using Java, C, C++, and PL/SQL and provides some enhancements tailored for usage with Oracle Internet Directory.

Example Use Case: OID for Database Enterprise User Security

This solution allows customers to easily manage multiple databases access for hundreds or thousands of enterprise users. The combination of DB Enterprise User Security (as part of Database Advanced Security) and Oracle Internet Directory or Oracle Virtual Directory form the centerpiece of Oracle's DB enterprise user security strategy.

DB Enterprise users are stores in the directory together with authentication and authorization information (like DB roles and privileges). When a user accesses an Oracle database, the database connects over SSL to the Oracle Internet Directory as an LDAP client to retrieve user authentication and authorization information, which are used to set the security context of the user's session on that database server. Centralized administration reduces administrative overhead for example, to disable access to all databases when an employee is on vacation. All that is required is a single change to the enterprise directory. It also helped customers to reduce password related helpdesk calls in some cases by up to 80%.

Leveraging Enterprise User Security with third party directories like Microsoft Active Directory can be accomplished either be using Directory Integration Platform or Oracle Virtual Directory.

For more details how to integrate EUS with OID see Oracle Directory Services and DB Enterprise User Security Deployment Options on the Oracle Technology website.

Example Use Case: Oracle Authentication Services for OS

For authentication and user management, Unix and Linux systems provide native local account management capability that is very costly to administer and lack consistency across systems. While NIS provides a centralized approach for user management and authentication, it has its own significant security issues.

To address these challenges Oracle Authentication Services for Operating Systems (OAS4OS) enables enterprises to centralize the management of Unix and Linux authentication, user accounts, password policies, and sudo authorization policies using Oracle Internet Directory.

Centerpiece of the solution is OID's integration with major Unix and Linux operating systems using open standards like PAM_LDAP, NSS_LDAP, SUDO LDAP together with configuration, automation and user migration tools.

Further information can be found on the OTN website Oracle Authentication Services for Operating Systems.

Conclusion

Oracle provides the most comprehensive directory services solution on the market including virtualization, storage and synchronization services. Oracle Internet Directory as directory storage and synchronization solution is the most compelling general purpose directory.Key differentiators include:

- Highest reliability, scalability, secure and availability through the underlying use of Oracle Database
- Superior usability based on web 2.0 technologies and enterprise manageability through Oracle Enterprise Manager
- Integration with nearly all Oracle Applications and Services for user identity and application meta-data storage, as well as support for standard LDAP access from third party applications.

Together with OVD and OID migration tools, OID, as a general purpose directory, enables enterprises to standardize identity data storage and directory services to increase ROI and reduce cost while enhance data security.

References

- Oracle Internet Directory 11g And Oracle Exadata In The Facebook Age
- Oracle Virtual Directory
- Directories, Directory Synchronization and Virtual Directories
- 2 Billion User Benchmark (Oracle Internet Directory 10.1.4.0.1)
- Oracle Authentication Services for Operating Systems
- Oracle Directory Services and DB Enterprise User Security Deployment Options

Oracle Internet Directory 11g R1
September 2011
Author: Olaf.Stullich@oracle.com
Contributing Authors: Mark Wilcox, 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

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

0109