THE EXPERT'S VOICE® IN ORACLE

Pro Oracle Identity and Access Management Suite

Streamlining authentication and authorization within the enterprise

Kenneth Ramey

Apress®

IOUG independent oracle users group

Pro Oracle Identity and Access Management Suite

Kenneth Ramey

IOUG independent oracle users group

Apress®

Pro Oracle Identity and Access Management Suite

Kenneth Ramey
Colorado Springs, Colorado
USA

ISBN-13 (pbk): 978-1-4842-1522-7 ISBN-13 (electronic): 978-1-4842-1521-0
DOI 10.1007/978-1-4842-1521-0

Library of Congress Control Number: 2016961691

Managing Director: Welmoed Spahr
Lead Editor: Jonathan Gennick
Development Editor: Douglas Pundick
Technical Reviewer: Arup Nanda
Editorial Board: Steve Anglin, Pramila Balan, Laura Berendson, Aaron Black, Louise Corrigan, Jonathan Gennick, Robert Hutchinson, Celestin Suresh John, Nikhil Karkal, James Markham, Susan McDermott, Matthew Moodie, Natalie Pao, Gwenan Spearing
Coordinating Editor: Jill Balzano
Copy Editor: Teresa F. Horton
Compositor: SPi Global
Indexer: SPi Global
Artist: SPi Global

Distributed to the book trade worldwide by Springer Science+Business Media New York, 233 Spring Street, 6th Floor, New York, NY 10013. Phone 1-800-SPRINGER, fax (201) 348-4505, e-mail orders-ny@springer-sbm.com, or visit www.springer.com. Apress Media, LLC is a California LLC and the sole member (owner) is Springer Science + Business Media Finance Inc (SSBM Finance Inc). SSBM Finance Inc is a Delaware corporation.

For information on translations, please e-mail rights@apress.com, or visit www.apress.com.

Apress and friends of ED books may be purchased in bulk for academic, corporate, or promotional use. eBook versions and licenses are also available for most titles. For more information, reference our Special Bulk Sales–eBook Licensing web page at www.apress.com/bulk-sales.

Any source code or other supplementary material referenced by the author in this text is available to readers at www.apress.com. For detailed information about how to locate your book's source code, go to www.apress.com/source-code/.

Printed on acid-free paper

I would like to dedicate this book to my parents Don and Alice, my bother Nick, and my wife Kathleen. They provided me the foundation, drive, and encouragement to get me to this point in my life. All of them pushed me on and kept me honest during the process of writing this book.

About IOUG Press

IOUG Press *is a joint effort by the* ***Independent Oracle Users Group (the IOUG)*** *and* ***Apress*** *to deliver some of the highest-quality content possible on Oracle Database and related topics. The IOUG is the world's leading, independent organization for professional users of Oracle products. Apress is a leading, independent technical publisher known for developing high-quality, no-fluff content for serious technology professionals. The IOUG and Apress have joined forces in IOUG Press to provide the best content and publishing opportunities to working professionals who use Oracle products.*

Our shared goals include:

- Developing content with excellence
- Helping working professionals to succeed
- Providing authoring and reviewing opportunities
- Networking and raising the profiles of authors and readers

To learn more about Apress, visit our website at **www.apress.com**. Follow the link for IOUG Press to see the great content that is now available on a wide range of topics that matter to those in Oracle's technology sphere.

Visit **www.ioug.org** to learn more about the Independent Oracle Users Group and its mission. Consider joining if you haven't already. Review the many benefits at www.ioug.org/join. Become a member. Get involved with peers. Boost your career.

www.ioug.org/join

Apress®

Contents at a Glance

Contents

About the Author

Kenneth Ramey started his career with Oracle products in 1997 while serving in the U.S. Air Force. After an Honorable Discharge, he began focusing primarily on Oracle Application Server and Oracle Identity Management. He is currently working for Centroid as a consultant specializing in Fusion Middleware Products. During his career, Ken has presented regularly on the topics of Fusion Middleware Products, including WebCenter Content and Identity Management, at various events such as Oracle Applications User Group and Independent Oracle User Group Collaborate and the Rocky Mountain Oracle Users Group. As a consultant, he has worked on many projects from small businesses to large multinational companies. He currently lives in Colorado Springs, Colorado, in view of Pike's Peak with his wife Kathleen.

About the Technical Reviewer

Arup Nanda has been an Oracle database administrator (DBA) since 1993, dealing with everything from modeling to security, and has a lot of gray hairs to prove it. He has coauthored five books, written more than 500 published articles, presented more than 300 sessions, delivered training sessions in 22 countries, and actively blogs at `arup.blogspot.com`. He is an Oracle ACE Director, a member of Oak Table Network, an editor for SELECT Journal (the IOUG publication), and a member of the Board for Exadata SIG. Oracle awarded him the DBA of the Year in 2003 and Architect of the Year in 2012. He lives in Danbury, Connecticut, with his wife Anu and son Anish.

Acknowledgments

Throughout my career, I have had the chance to work with some of the best in the industry. These people helped put me on a path that led me to where I am now. There are people like my friend Jim Osborn, whose knowledge and experience helped me get through a number of projects, and his willingness to teach topics instilled the same willingness in me. The various project managers at Centroid (Ann, Carrie, Frank, Rob) with whom I have worked transformed my lackluster documentation skills into the ability to coherently convey complex project aspects. There are the owners of Centroid, who treat their employees like family. Scott Morrell and Paresh Patel, in particular, have mentored me and provided a work environment that encourages innovation and opportunity for professional growth. Jim Brull and Eric Reed have been there to show that the company is willing to let me mold my skills in ways that are mutually beneficial. I cannot forget to mention Ajay Arora, who has helped build my confidence as a leader and provided valued advice and technical knowledge many times.

Outside of work, there are the many friends and family who have been around throughout my life and provided encouragement and a sounding board when I needed it. Special thanks go to Mike Gale and Neland North, who have known me throughout my career and helped guide me from being a new Airman to now, almost 20 years later. They are still trying to help me figure out this thing called life. I will see you guys on the river and on the bike trail. If I did not mention your name here, the omission was not intentional. There are just far too many people to thank and acknowledge in a single book. Thank you all.

Introduction

Many organizations plan for security throughout the product life cycle for each product installed within the environment. Most products provide some sort of user storage mechanism. These individual user stores can be used, and might be a viable solution for smaller environments with few implemented products. However, this can often lead to multiple identity stores, replication of data across business units, and management headaches in larger organizations. In addition, the use of individual user management functions can lead to users maintaining multiple usernames and passwords for all of the products they use. In the end, these users are going to use less secure passwords, or worse, write a list of usernames and passwords and place it under their keyboard.

The solution is to implement a single source for identity data that all applications can leverage for authentication and authorization. The Lightweight Directory Access Protocol (LDAP) was designed to provide a standard way to look up information in an identity store. With LDAP, applications now have a standard way to authenticate and authorize users from external stores, provided it is compliant with the LDAP standard. Business units can now implement software that is LDAP compliant and access the central user store and no longer require users to maintain multiple accounts. Oracle Internet Directory (OID) is Oracle's implementation of a generic LDAP directory. Other Oracle products such as E-Business Suite, WebCenter Content, and OBIEE are designed to work with OID. Being a generic LDAP-compliant directory, OID can be leveraged by other third-party applications as well.

Oracle went a step further and introduced Oracle Access Manager (OAM) to provide single sign-on functionality. Now, instead of each application requiring a separate login request, they can be set up to utilize an existing browser token to authenticate, thus relieving the user from multiple credential entries. OAM supports the Security Assertion Markup Language (SAML), so it can be configured to provide authentication services to third-party cloud-based applications. This also means that Oracle cloud-based solutions such as Human Capital Management can be integrated with an organization's OAM single sign-on environment.

No implementation is complete without some sort of identity life cycle management. In the past, each application was responsible for its own identity store. This led to users having multiple accounts that had to be created and maintained for each application they accessed. When users on-boarded, it could take days to weeks to get access to everything they needed. Conversely, when a user left the organization, there was the possibility that his or her accounts might not be decommissioned in a timely manner, if at all. This posed a large security risk. Oracle Identity Management (OIM) was introduced to bring a new level of governance to enterprise-level identity life cycle management. OIM provides a central interface for the management of user identity data. It can connect to a standard LDAP directory, or by using Oracle Virtual Directory, it can manage data from multiple stores. The automation capabilities provided by OIM can reduce the amount of work required to on-board users and ensure access is removed when a user leaves the organization.

The Oracle Identity and Access Management Suite combines the key elements discussed here to provide an end-to-end solution for user management. Although it should be simple to implement this, there are a variety of steps required to get everything working properly and efficiently. This book is intended to provide a guide to getting the Identity and Access Management Suite up and running in your environment. It demonstrates installation and configuration, along with some architectural discussions to help determine what is required in your environment.

CHAPTER 1

Oracle Identity and Access Management Suite Overview

Oracle Fusion Middleware products are deployed within WebLogic Server architectures. WebLogic Server provides a scalable environment, allowing the enterprise to deploy and manage Oracle products and Java applications with the ability to access database and messaging services. WebLogic Server operates as the application server tier. The capabilities delivered by WebLogic include clustering, high availability, manageability, monitoring, security, and database integration.

The Oracle Identity and Access Management Suite consists of multiple components, each serving a very specific purpose. These components consist of directory services, access management or single sign-on (SSO), identity management, and self-service portals, as well as provisioning, governance, and reporting services.

This chapter provides an introduction to the Oracle Fusion Middleware WebLogic Server environment and the major components involved in configuring the Oracle Identity and Access Management Suite. You will also be presented with a description of the Oracle Identity Management components relevant to the rest of the book.

WebLogic Server

Oracle's WebLogic Server (WLS) is a fully J2EE-compliant application server that will support the Oracle Identity and Access Management Suite components. This environment provides the components necessary for the deployment of custom applications as well as Oracle Fusion Middleware Products like Enterprise Content Management and Oracle Identity and Access Management. As WebLogic Server is an application server, users are able to access these applications via a web browser using the deployed application ports or through an HTTP server serving as a reverse proxy.

To provide enterprise-level service, WebLogic Server supports a number of environmental features.

- *Programming models*: WLS supports a Java EE deployment environment, web services support, Java Messaging, Extensible Markup Language (XML) capabilities, Java Database Connectivity (JDBC) connection resources, and other components.
- *High availability*: This is supported using WebLogic Clusters to distribute work across multiple servers and the ability to detect overload and manage overload conditions. The persistent store and store-and-forward services allow the ability to temporarily store JMS messages and deliver them across services distributed across the cluster.

K. Ramey, *Pro Oracle Identity and Access Management Suite*, DOI 10.1007/978-1-4842-1521-0_1

- *Security*: WLS provides a built-in Lightweight Directory Access Protocol (LDAP) 2.0 identity store that can be used to manage access to services deployed on the server. Beyond this, WLS can be configured to authenticate against a number of different external data stores such as Oracle Internet Directory, Active Directory, and so on. Furthermore the WLS framework allows the integration of identity asserters such as Oracle Access Manager (OAM).
- *Diagnostic framework*: Affords the ability to collect and analyze runtime data about the processes running on the server. This can be used to diagnose issues and tune for better performance.

For the purposes of the Oracle Identity and Access Management environment, this book discusses how to use the following components.

- The administration server provides a graphical user interface (GUI) for managing all components of the deployment. Each WLS domain has one administration server that can be run on any of the WebLogic hosts. The administration server manages the configuration data for the domain, clusters, managed servers, data sources, security settings, and application deployments.
- A domain is a logical unit of management for server resources within the WLS. All aspects of the environment are contained within a domain, including the managed servers, database sources, messaging services, application deployments, machines, and clusters.
- Machines represent a physical host that houses managed servers. A single administration server can manage multiple machines. The administration server communicates with each machine's node manager for start and stop operations of each managed server. A single physical host can have multiple machines configured listening on different ports if necessary.
- WebLogic Clusters consist of one or more WLS instances that work together, providing high availability and the ability to scale the environments laterally.
- A managed server is a logical WLS construct where applications can be deployed.
- Data sources are JDBC connections configured within the WLS to be used by applications deployed within the various managed servers. Targeting a data source at specific managed servers makes it available to only those specified.
- Security realms define authentication providers and asserters that protect the application resources. Security groups, users, and policies can all be defined within the WebLogic security realms.

Oracle Directory Services

Oracle Directory Services makes up the core of Oracle Identity and Access Management. Consisting of multiple options, Directory Services provides identity and policy storage, directory synchronization, and virtualization functionality that can be leveraged by various applications in use by the enterprise. These options include the following:

- *Oracle Internet Directory (OID)*: Database-based fully LDAP-V3 compatible identity directory.
- *Oracle Unified Directory (OUD)*: Java-based LDAP-V3 compliant identity directory.
- *Oracle Virtual Directory (OVD)*: Directory integration that enables management of multiple sources without the need for data replication.

Oracle Internet Directory

OID is a fully LDAP-V3 compliant directory using the Oracle Database for storage. This allows OID to leverage database features such as Real Application Clusters and Multimaster Replication in conjunction with OID clusters and the Fusion Middleware architecture to provide a highly available and scalable environment. The Oracle Directory Services Manager provides a standard front end for the maintenance of users, security groups, object classes, attributes, and policies within the OID. Figure 1-1 presents a basic high-availability environment of OID or OVD using a Real Application Clusters Database environment.

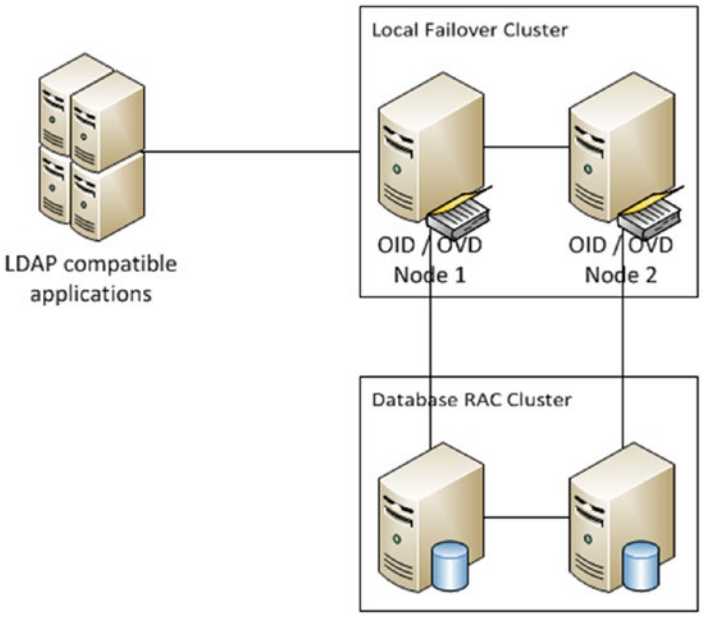

Figure 1-1. *Basic local high availability configuration*

OID allows the storage of disparate identity data through the ability to store multiple contexts. This allows data that might be stored in multiple sources to be managed in a single instance. For example, if the enterprise has implemented multiple Active Directory Lightweight Directory Service instances to manage users in various LDAP enabled applications, OID can be leveraged to provide a single LDAP source for all applications.

Using an Oracle database for the data repository, OID is able to leverage features such as Transparent Data Encryption and Database Vault to provide security at every level of operation. The ability to leverage these database features separates security duties by allowing the database to handle the data store and backup security.

OID provides the ability to synchronize other directories in use within the enterprise. The Directory Integration Platform, shown in Figure 1-2, allows administrators to create and maintain synchronization profiles for Active Directory, Sun eDirectory, OpenLDAP, and others. This enables the enterprise to consolidate user repositories and provide application security with a standardized general-purpose LDAP directory.

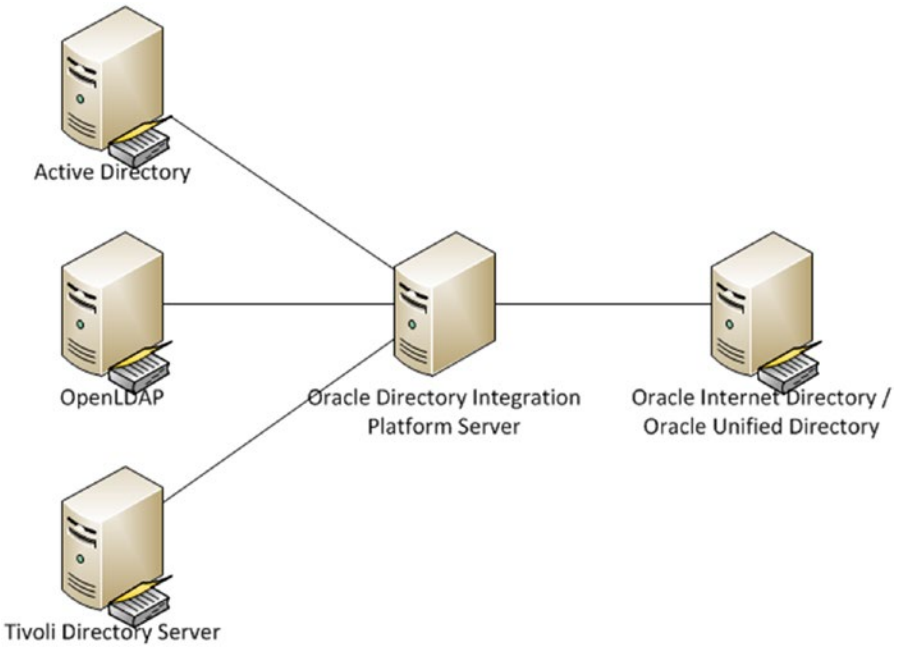

Figure 1-2. *Directory Integration Platform*

In addition to integrating multiple disparate identity stores by copying data and transforming it to match the needs within the OID store, OID is also able to perform replication of data between OID nodes to provide high availability and scalability for performance.

With OID, the organization is presented with multiple replication concepts. Full replication involves propagating the entire directory to other IOD nodes instead of sending only a specified portion of the structure to other nodes. For the transport layer of replication, OID supports both LDAP replication and Database Advanced Replication. The former relies on the LDAP protocol to convey data from one OID instance to another, whereas Oracle Database Advanced Replication requires the database to replicate the data between database instances. The last concept to be presented is the replication direction. OID supports single master, multimaster, and fan-out replication. As the names suggest, single master can be thought of as replication from a master node to all other nodes in one direction. Multimaster allows changes from any node to be replicated to the others. Fan-out is a sort of combination of the two previous directions, where a master node replicates out to other nodes and those child nodes can then replicate either full or partial data to other nodes.

Although OID has a long-standing history and is currently compatible with other Oracle Identity Management components such as OIM and OAM, along with Fusion Middleware products and applications, Oracle has indicated that the future direction of Directory Services is OUD.

Oracle Unified Directory

OUD represents Oracle's release of the industry's first Java-based, LDAP-V3 and Directory Services Markup Language (DSML) v2 compliant directory service that combines storage, proxy, synchronization, and virtualization in a single platform. OUD provides a high level of performance and elastic scalability and high availability using commodity-level hardware and flexible deployment architectures. While providing this level of service, OUD is able to maintain high levels of security and monitoring.

OUD's architecture allows for global indexing, increasing its elastic scalability. This feature allows administrators to add servers; OUD will handle routing of new requests to the new servers and storage as needed. This eliminates the need for building new environments and migrating large amounts of data. Another benefit of this indexing is that sizing needs can be addressed on an as-needed basis. No longer do administrators need to determine the current size requirements and estimate growth over the next few years. Entries can also be distributed across multiple directory storage instances. Figure 1-3 shows an environment that has been distributed across mulitple nodes as well as clustered to provide failover protection.

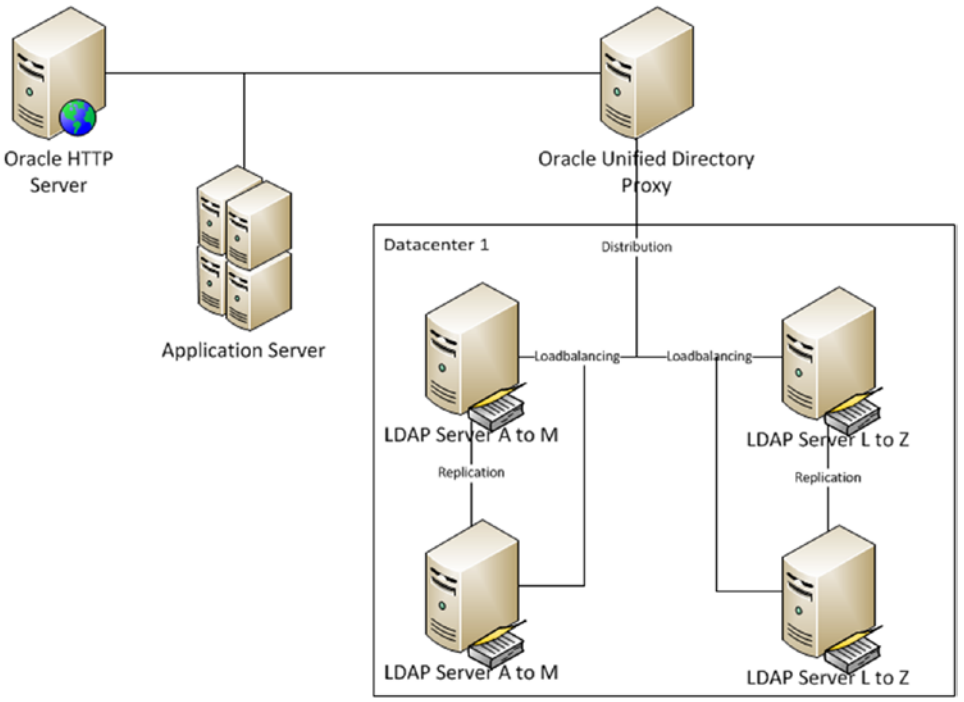

Figure 1-3. *Distributed architecture*

To support high availability while also promoting high performance, OUD separates the tasks of directory services and replication services. As discussed previously, OUD allows the distribution of servers across multiple data centers. To support this, OUD introduces replication servers shown in Figure 1-4. These are servers dedicated to replicating data across the entire environment, leaving client request handling to the directory servers.

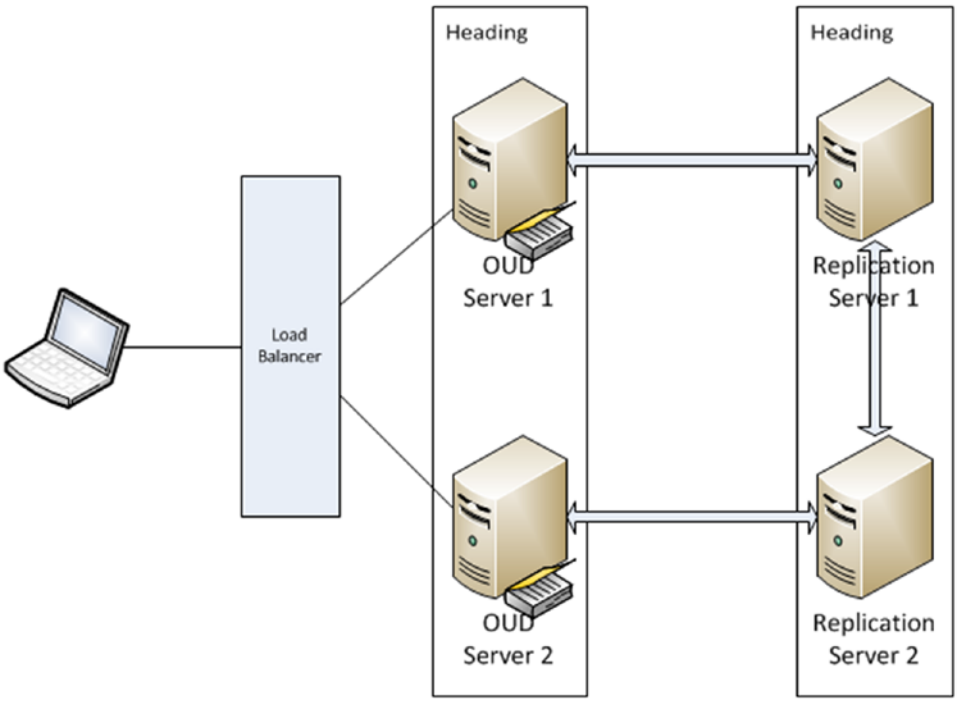

Figure 1-4. *Oracle Unified Directory replication*

During the OUD replication described in Figure 1-4, each OUD server connects to one replication server. It then sends and receives all changes to that server. The replication servers communicate changes received to all the other replication servers in the environment. The OUD replication servers communicate these changes to the OUD servers connected to them. A change number assigned by the OUD server that initiates the change identifies the change and is used by the replication servers to ensure that changes are populated to the other OUD servers. This change number is also stored in a persistent store that is used to populate changes to OUD servers that might have been disconnected from the replication servers. If changes occur on both OUD servers at the same time and cause conflicts, each OUD server will replay the changes until all conflicts are resolved.

The replication server manages connections to the OUD servers and listens for changes from other replication servers. These changes are populated to the directory servers connected to it. These replication servers are created automatically when an OUD server is configured for replication. As such, these can run on the same Java virtual machine (JVM) or host. To save resources, an OUD server can be configured to perform both directory and replication server functions. However, for larger environments, Oracle recommends these functions be separated to different servers.

Much like OID, the Directory Integration Platform can be used to copy identity data from third-party LDAP repositories to provide a central data store for application authentication. It should be noted that this is the same functionality presented earlier for OID. As such, it is producing a copy of identity data that must be maintained. Some organizations might not wish to manage multiple copies of LDAP data. This is addressed with OVD.

Oracle Virtual Directory

OVD provides a method of presenting multiple identity stores as a single source without the need for synchronization and replicating data. Presenting a single source enables enterprise applications to access identity data from multiple sources such as the database, EBS, Active Directory, and OID.

Aggregation of multiple data sources allows the enterprise to leverage existing identity data across multiple sources without the need for replicating data or setting up complicated synchronization tasks. Because OVD presents multiple data sources without copying the underlying data, significant savings can be realized as storage costs are reduced.

A key capability of OVD is its ability to transform identity data into application-specific views. Thus it can present non-LDAP data such as database or web services in the proper format required for the various applications in place in the enterprise. For example, OVD can be leveraged to present Siebel Customer Master data as an LDAP source for authentication of other applications. The translation capability not only allows multiple applications to view the data as needed, but it also allows the organizations to retain control over how they manage and share identity data within their own repositories.

Not only can OVD present multiple data stores as a single source, it can support the concept of split profiles. For example, an enterprise might store all identity data in Active Directory. However, applications such as EBS might require additional metadata for authorization stored in OID or the human resources database. The OVD adapters will allow applications to view this data as a single entry. Figure 1-5 shows a representation of multiple directory sources being consolidated with OVD. As this environment is virtual, it is all done without replication.

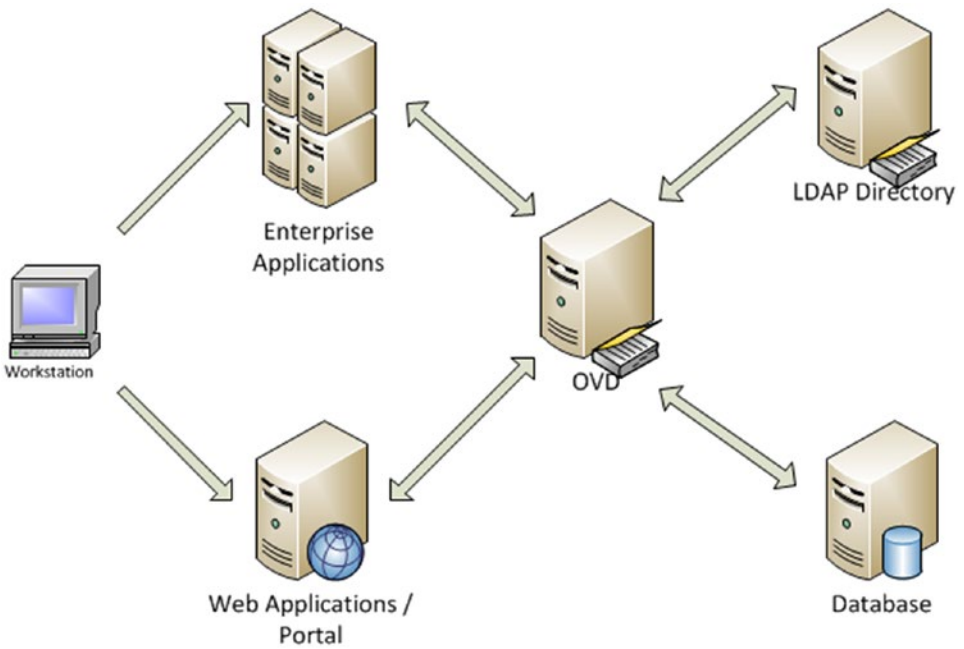

Figure 1-5. *Data flow between application and identity sources through OVD*

Built to be scalable and highly available, OVD can support the enterprise, no matter how large. Scaling for performance can be as simple as adding additional nodes to the cluster. This can be done in a central location or geographically. High availability is supported not only within the OVD environment, but it also supports load balancing and high availability of its data sources. Although this configuration allows a more streamlined environment with no data duplication, it can suffer from issues such as lost data if a user is removed from one source or orphaned accounts and groups.

Oracle Identity and Access Management

Most organizations require Identity Services such as an LDAP repository. Sometimes this is accomplished with a simple network directory such as Microsoft Active Directory. When considering application security, a more general-purpose directory is necessary. OID, OVD, and OUD, presented previously, can be used to provide this service. As more and more applications are introduced to the business, users can become inundated with authentication dialogs as they switch from one application to another.

OAM, a component of the Identity and Access Management Suite, can be leveraged to provide SSO capabilities. This function can greatly reduce the number of times a user must authenticate during the day, thereby increasing productivity. This reduction can also be built on by incorporating external and third-party applications through federation.

With SSO through OAM providing fewer authentication requests, it is important that application users keep secure passwords and accounts. Account management becomes a necessity as single accounts could have access to a multitude of systems and data. Oracle Identity Management is a key component of the Identity Management stack that provides user self-service, user management, and a high level of auditability.

Oracle Access Manager

Oracle Fusion Middleware applications and products have been designed to support Oracle Identity Manager (OIM) components such as OID and OUD for identity information. Furthermore, these resources can be protected using OAM. Oracle Access Manager leverages functionality such as session management, identity context, and risk analysis to provide authentication and authorization, policy administration and enforcement, and SSO capabilities to the application environment. OAM also provides additional functionality, most notably an SSO environment for organizations that employ multiple Oracle products and Identity Federation support to integrate third-party products compatible with Security Assertion Markup Language (SAML).

The core of OAM is providing authentication and authorization services to an enterprise application. It also allows SSO capabilities within Oracle Fusion Middleware-based environments. Figure 1-6 provides a high-level depiction of the OAM architecture. Access requests to protected resources are intercepted by a filter called a WebGate or a mod_osso instance, and sent to OAM for processing. OAM references configurable authentication and authorization policies to determine if the client access will be granted. After successful authentication, a cookie is set to ensure continued access to the requested resource as well as other resources within the OAM environment.

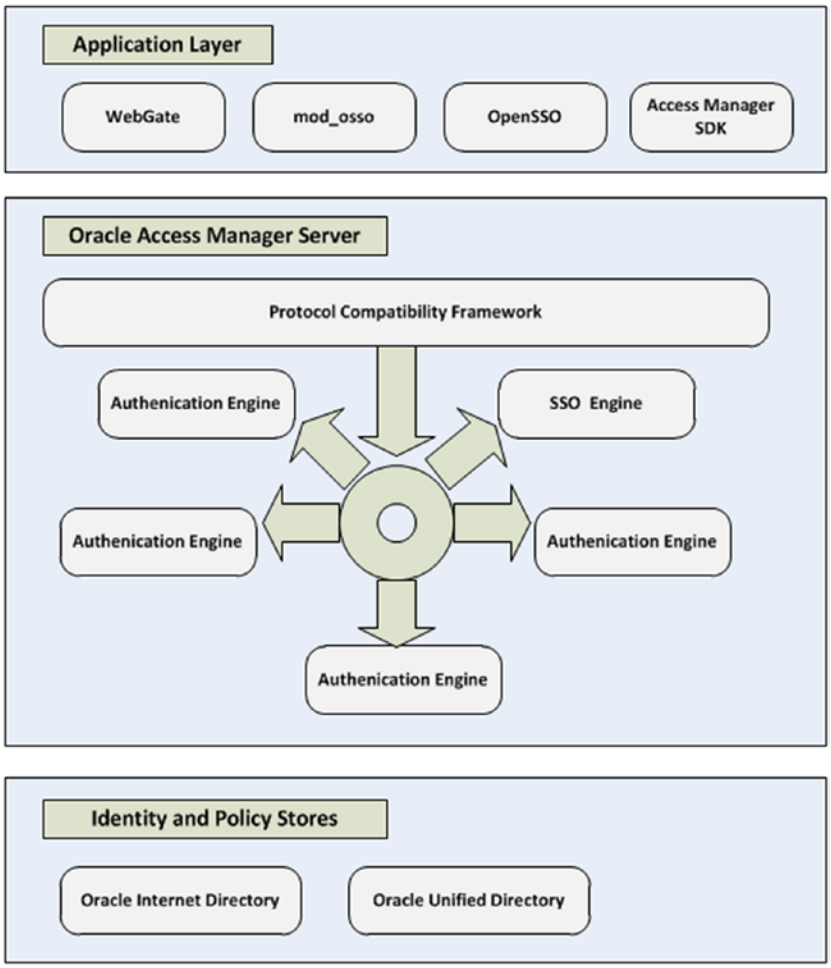

Figure 1-6. *Breakout of Oracle Access Manager components*

Oracle Adaptive Access Management

OAM does not only provide authentication and authorization services; it also enables the organization to increase security awareness and fraud detection across multiple levels of the organization's application architecture such as the web, data, and application tiers. Oracle Adaptive Access Manager (OAAM) strengthens the security of OAM's authentication mechanisms by adding the ability to learn behaviors and detect possible fraudulent activities. The real-time and batch risk analysis component of OAAM serves to verify user identities and the validity of activities using patterns, rule engine, actions, and transaction analysis.

The following are some of the risk analysis components of OAAM:

- *Device fingerprinting*: This functionality collects attributes of devices used to connect during a user's transaction. These attributes are used to identify possible fraudulent access requests.
- *Behavioral profiling*: OAAM can learn users' normal behavior, device information, locations, and other data to provide proactive detection of possible misuse or security breaks.
- *Risk engine analytics*: This feature allows the real-time analysis of events, user profiles, device fingerprints, geolocation, and other data to determine the level of risk during user interactions. The trail of analytics can be audited to ensure proper actions were taken.
- *Predictive analysis*: This facilitates the integration with Oracle Data Mining to provide anomaly detection based on historical data. This can also be used to base change decisions on analysis data as different models are tested.
- *Investigative forensics*: This can be used to provide sets of data for auditing and fraud investigation efforts. The data can be customized using Business Intelligence Publisher or out-of-the-box templates can be used. These reports can assist security investigators in identifying instances and possible related fraudulent access.
- *Universal risk snapshots*: These are used to back up, restore, and migrate existing security policies and configurations.

User-facing components preventing malware and phishing attacks augment OAAM analysis functionality to provide an end-to-end solution. End users can be presented with virtual authentication devices, knowledge-based authentication questions, and one-time password mechanisms to prevent unauthorized account access.

The user-facing components of Oracle Adaptive Access Management include the following:

- *Device fingerprinting*: This provides the ability of OAAM to collect metadata regarding users' devices. This data may include cookies, hardware configurations, geolocation, and network configurations. This data is used to detect changes in user behavior.
- *Knowledge-based authentication*: This provides a secondary form of authentication by requiring the user to answer security questions.
- *Answer logic*: This component enables OAAM to detect fundamentally correct answers to knowledge-based authentication questions even if they have minor typographical errors.
- *One-time password*: This functionality makes it possible for users to receive a one-time use password via short message service (SMS) or e-mail to be used for authentication to systems.
- *Self-service password management*: Users are empowered to create and reset their credentials using self-service.

Identity Federation

As companies move toward cloud-based services or employ external web applications, and other cross-domain services, the need to be able to authenticate to these services using the same credentials grows. Identity Federation enables the organization to simplify management of user access by eliminating the multiple sets of credentials traditionally required for a disparate environment where applications might exist in multiple domains. OAM supports federation with SAML, OpenID, form-fill, and OAuth.

The two functional components of Oracle Access Manager Identity Federation are the Service Provider and the Identity Provider. The Identity Provider component is responsible for establishing the users' identity, filtering attributes, asserting the identity information, and maintaining sessions. The Service Provider takes care of mapping the attributes, linking the identities, and passing identity information to the applications.

During login, as an Identity Provider, OAM first authenticates the user. If the user session has timed out, the Identity Provider will determine if the user needs to reauthenticate. Finally, the Identity Provider component determines if the partner application requires a challenge compatible with the level or scheme specified during the request. To support this, OAM allows the configuration of flexible authentication mechanisms. Identity Federation uses a federation authentication method and OAM Authentication Scheme mappings to control how the user should be challenged for authentication.

During logout, the Access Manager Identity Federation service provider supports two different flows depending on where the logout was initiated: from OAM or from the federated partner application.

During an OAM-initiated logout:

1. The user requests the logout via OAM.
2. OAM ends the Access Manager session.
3. OAM instructs the various WebGate instances to remove the user's session cookies.
4. The OAM federation services performs a logout operation causing logout of partner applications by either redirecting the user with an HTTP redirect or by sending a logout request via Simple Object Access Protocol (SOAP) message.
5. The OAM federation service terminates the federated session.

If the logout is initiated via the partner application:

1. The partner application redirects the user to the OAM federation service.
2. The federation service marks the session for logout.
3. The user is redirected to OAM for logout.
4. OAM instructs the various WebGate instances to remove the user's session cookies.
5. The OAM federation service performs a logout operation causing logout of partner applications by either redirecting the user with an HTTP redirect or by sending a logout request via SOAP message.
6. The OAM federation service terminates the federated session.

The Service Provider component of Identity Federation within OAM works in conjunction with the Identity Provider to deliver fraud and risk awareness in federated environments. When the Identity Provider authenticates the user, the Service Provider can be triggered to create a session with the appropriate authentication level as mapped with the federation authentication method. These attribute methods are supported as request attributes from the Identity Provider or mapping to an incoming assertion attribute name in the OAM session.

Oracle Access Management Identity Federation supports multiple federation technologies, including SAML, OpenID, OAuth, Social Identity, and form-fill.

- *SAML-based federation*: SAML is an industry standard open framework that allows the sharing of security information. It provides a standard method of transferring information across applications spanning multiple domains. It can also be used to link accounts belonging to a single user in multiple sites. The SAML protocol provides standard security tokens that can be used within multiple security frameworks. SAML also provides a standard method of representing a security token that can be passed among business processes or transactions. This is facilitated using XML documents.
- *OpenID-based federation*: OpenID allows any web site to leverage an authentication standard without the need to develop its own system. It employs the use of a single token that can be used by multiple systems. OAM supports the exchange of an OpenID identifier to exchange identity data. This can be done using a token containing the NameID and other optional attributes or by using the NameID format, a hashed user attribute along with a generated value stored within the data store.
- *OAuth-based federation*: This technology supports delegated authorization. It is an industry standard designed to transparently share private data on one site to another site. OAM supports OAuth within its Identity Federation component, Mobile and Social Security, and the API Gateways (APGs). Through these components, OAM provides token issuance, token validation, and token revocation services that are compliant with OAuth 2.0.

Mobile and Social Access

As today's organizations become more and more reliant on cloud and other web-based applications, their customers and internal users require access from multiple devices and locations including mobile devices. In addition to accessing enterprise resources from mobile devices, many organizations are deploying mobile versions of applications routinely used by their user base. Oracle has addressed this growing need with the Mobile and Social Access component of OAM.

Oracle's Mobile and Social Access leverages the core capabilities of OAM to secure applications. These include the credential collector, authentication and authorization services, and SSO. Designed with security as a platform in mind, Mobile and Social Access integrates with the Adaptive Access Management portion of the OAM stack to provide auditing, device fingerprinting, and risk analysis and authentication compatibility.

Mobile and Social Access allows the enterprise to provide the following capabilities:

- OAuth 2.0-compliant authorization delegation.
- Browser-based and native mobile applications access to identity stores.
- Interaction with cloud-based identity services such as Google and Facebook.
- A REST interface for LDAP operations that can used for user profile services.

API and Web Service Security

OAM delivers the ability to secure web services to support the industry's growing use of service-oriented architecture. Today more and more organizations are exposing web services that can be integrated into other applications in use elsewhere. For instance, a company might wish to include a stock market application

in its own company intranet portal. These web services must be secured to ensure only authorized access to the functionality, lest they be misused. OAM offers standards-compliant functionality to protect web services and application programming interfaces (APIs) using the Web Services Manager (WSM), Secure Token Service, and APG components.

WSM protects Fusion Middleware Product and Application services using protocols such as WS-Security, SAML, and OAuth. WSM allows the enterprise to adjust to the ever-changing security landscape by defining policies, enforcing security, and monitoring events. These capabilities are further augmented by OAAM to help the organization identify possible security breaches and analyze risk to develop new security policies in real time. OAM WSM handles all aspects of web service security including authentication, authorization, confidentiality, and integrity using public key infrastructure to encrypt and decrypt data being passed.

The APG is used to secure access to services and APIs deployed in the cloud or within the enterprise. To do this, the APG is able to evaluate traffic for possible threats, selectively restrict requests that possibly contain threats, and actively scan content for malformed requests and viruses. The gateway also allows an enterprise to integrate LDAP identity and policy stores such as OUD or Active Directory to enforce authentication and authorization rules.

The Secure Token Service manages the relationship between a service provider and the service consumer by providing the token life cycle services; acquisition, validation, and cancellation. This service supports a trust between the web service and the API gateway, an SSO environment, or identity propagation enabled by the Secure Token Service between the client, token-issuing authority, and the token consumer.

Cloud Access Portal

The OAM access portal is designed to simplify access to partner applications and applications integrated with OAM. The access portal provides a cross-platform interface that allows users to access OAM protected resources from any device. The portal affords administrators the ability to automatically provision applications to users' accounts and gives them the ability to provide a catalog for users to select the applications to include on their personalized interfaces. In addition, the access portal will allow users to update their credentials online without the need to contact an administrator or help desk.

All of the OAM supported authentication types can be employed on the portal, thus maximizing the organization's investment and increasing user productivity. It is also able to provide access to federated partner applications and use form-fill authentication injection, which allows users to store credentials that will be used in software-as-a-service (SaaS) or web application login forms. The access portal provides the framework for organizations to deploy an SSO environment within the enterprise, increasing the productivity of their user base by giving them a central location to access their applications.

Oracle Identity Manager

As organizations grow and their user base has access to more and more resources online, the need for stricter controls and intuitive management tools grows. User productivity cannot come at the cost of enterprise security and governance. Businesses must be continually aware of who has access to what and how they received that access to stay on top of possible misuse or fraud. OIM makes up the identity governance component of the Identity and Access Management Suite of products.

The user identity life cycle must be tightly controlled to ensure users have the correct access on their first day and have that access revoked as needed when they change roles or leave the company. In addition, some users might require access that could be out of the ordinary for their job titles. Many of these roles can be granted based on a defined set of rules or selected by the user and approved by managers and administrators. However, tools are required and strict controls must be implemented to ensure correct access.