Oracle Identity Manager 11g Sizing Guide

A White Paper

December 2010

Contents

1. Introduction

Oracle Identity Manager, Oracle's industry leading identity administration and user provisioning solution, provides operational and business efficiency through centralized administration and complete automation of identity and user provisioning events across the enterprise, as well as extranet applications. In its latest 11g release, Oracle Identity Manager has been architecturally optimized for cloud, distributed, and in-house environments.

This white paper describes infrastructure sizing for Oracle Identity Manager 11g deployments (i.e. versions 11.1.1.3 or later in the 11g release series) to enable customers to take advantage of the new architecture.

2. Architecture Overview

Oracle Identity Manager 11g is a user provisioning and administration solution that automates account lifecycle management and improves regulatory compliance by providing actionable attestation. Customers can get an end-to-end view of "who has what" and "who had what, when, and how did they get it" by using the rich reporting capabilities of Oracle Identity Manager 11g.

2.1 Functional Architecture

The following figure illustrates Oracle Identity Manager's functional architecture, which consists of three areas:

- Identity Administration
- Resource Administration
- Request Management

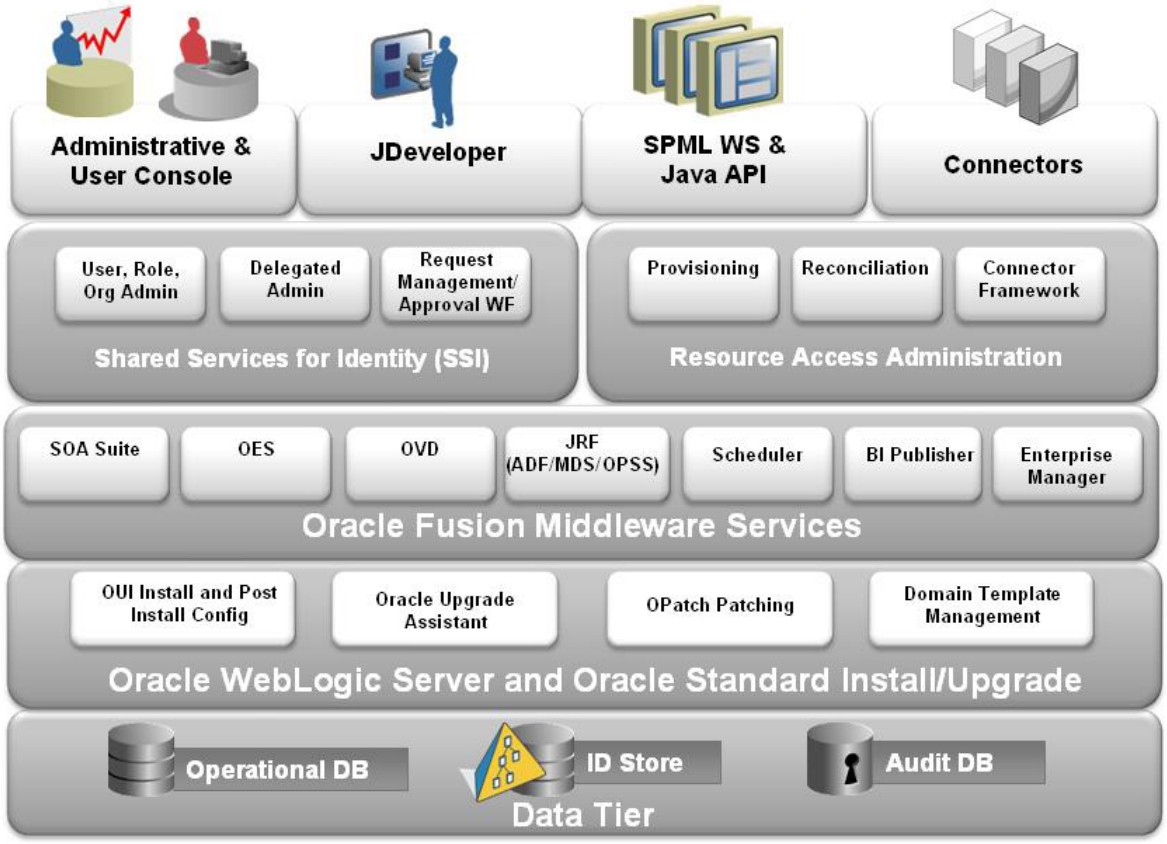

Figure 1: Oracle Identity Manager Functional Architecture

The following sections describe these three areas.

2.1.1 Identity Administration

Customers can administer their users based on a fine-grained authorization model. Oracle Identity Manager provides a flexible, delegated administration model that can be based on attribute-level delegated administration policies. Administrators can perform actions only on users they are authorized to administer and can perform these operations on a single user or in bulk.

Oracle Identity Manager provides a rich role model, which allows customers to define roles, grant entitlements to those roles, and define membership rules. They can define sophisticated provisioning policies (or Access Policies) to use in automated account provisioning and entitlements. By using this role-based model, customers can automate account lifecycle management to a large extent.

End-Users can leverage the Web 2.0-based, rich user interface to access self service functionality, including lost password management, account and entitlement requests, approval management, etc. Authorized users can carry out these operations for themselves or on behalf of other users in bulk.

Additionally, Oracle Identity Manager allows customers to restrict functionality based on organizations, enabling them to define delegation policies for extranet identity administration.

2.1.2 Resource Administration

Customers can manage accounts and entitlement grants for their users in various target systems by using Oracle Identity Manager. The feature-rich Connector Framework enables customers to create and manage the account lifecycle in a wide variety of target systems and to manage the entitlement grants in these applications. In addition, customers can combine the rich delegated administration model, roles and provisioning policies, and the strong integration with a large number of target applications, to automate the end-to-end lifecycle of an account and to alleviate the burden on the IT staff.

Oracle Identity Manager provides a new, high performance reconciliation engine that detects changes to existing accounts and rogue accounts. Customers can get up to 10x performance gains, which helps in dealing with extranet deployments.

2.1.3 Request Management

Oracle Identity Manager provides significant innovations in its request management feature. Using the concept of a request template and a context-sensitive request creation wizard, users can create requests in the context of their current views.

Customers can combine the rich delegated administration model with request templates to allow end users and administrators to pick from a catalog of request templates that are tailored for the context of the user. Additionally, end users can submit requests for themselves or in bulk for a set of users.

Oracle Identity Manager leverages the rich workflow capabilities of BPEL and Human Workflow components of the Oracle SOA Suite, referred to as SOA hereafter, to carry out approvals and workflow routing. Customers can define complex approval rules, escalation policies, and actionable notification for agile approval management.

2.2 Technical Architecture

Oracle Identity Manager is a J2EE application with a three-tier architecture. These tiers include

- A Presentation tier that is built using Oracle's Application Development Framework (ADF)
- A Business Services tier that contains the following core services,
    - Platform Services
    - Request Engine
    - Provisioning Engine
    - Web Services
    - Identity Administration Services
- A Data tier that is based on an ANSI SQL database, like the Oracle RDBMS. This tier includes
    - Reconciliation Services
    - Reporting Services
    - Audit Services

Oracle Identity Manager leverages the Fusion Middleware (FMW) platform for

- Infrastructure services such as monitoring, clustering, load balancing, Java Message Service (JMS), and Web Services security
- Administrative functions such as installation, patching, and upgrades
- Lifecycle management functions such as test-to-production (T2P) of configuration metadata and user customizations, application server configurations, scale out, etc.

Describing the many innovative architectural enhancements to Oracle Identity Manager 11g is not within the scope of this white paper. To better understand the innovative manner in which Oracle Identity Manager can scale for a multi-million user population, please see the resources listed in the Additional Resources section.

From a sizing perspective, there are three areas to consider (as shown in Figure 2):

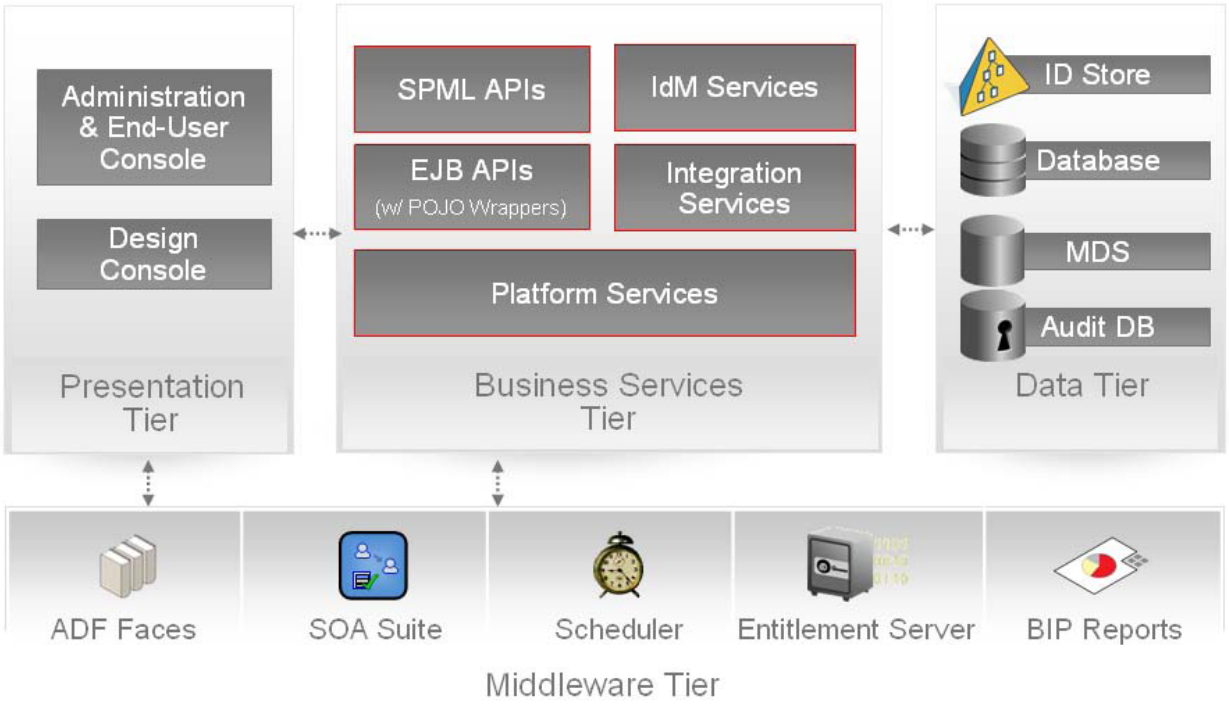

Figure 2: Oracle Identity Manager Technical Architecture

- **The Presentation tier**

  Oracle Identity Manager uses ADF Faces, an AJAX-enabled library of user interface (UI) components. This UI framework provides reusable UI templates, partial page rendering, reusable page regions, and many other features. This tier also provides separation between the UI and the back-end business tier.

- **The Business Services tier**

  This tier provides the following services and capabilities:

  - Core services that include Identity Administration services, Policy Management services, and Provisioning and Reconciliation service.
  - An API that enables custom clients to integrate with Oracle Identity Manager.
  - Integration services that include the Connector Framework, Web Services, and Adapter Factory.
  - Platform services that include Request Services, Entity Manager, and Scheduler.

  In a typical deployment, Oracle Identity Manager receives requests from different channels. End users can use the Oracle Identity Manager Web UI to submit requests or to invoke operations, custom clients, and Web Services that can make API or SPML requests. All operations, regardless of the channel, delegate execution to the Business Services tier. It is important to understand how these operations are executed and what impact they have on sizing.

An operation; such as user creation, role modification, or resource provisioning consists of business logic units, also known as Event Handlers, that are executed in sequence. Event handlers can be synchronous or asynchronous. Each operation includes the following key stages:

- **Pre-processing stage:** Oracle Identity Manager validates data and, if required, generates missing data. For example, a user creation operation may require a user ID and a password to be generated.

- **Action stage:** Oracle Identity Manager performs the actual operation. Typically, customers are discouraged (but not prevented) from overriding the action.

- **Post-processing stage:** Oracle Identity Manager performs other operations that must be executed as a result of the action. For example, when a user's profile is updated, Oracle Identity Manager recalculates the user's role membership and subsequently evaluates the impact of access policies on the user.

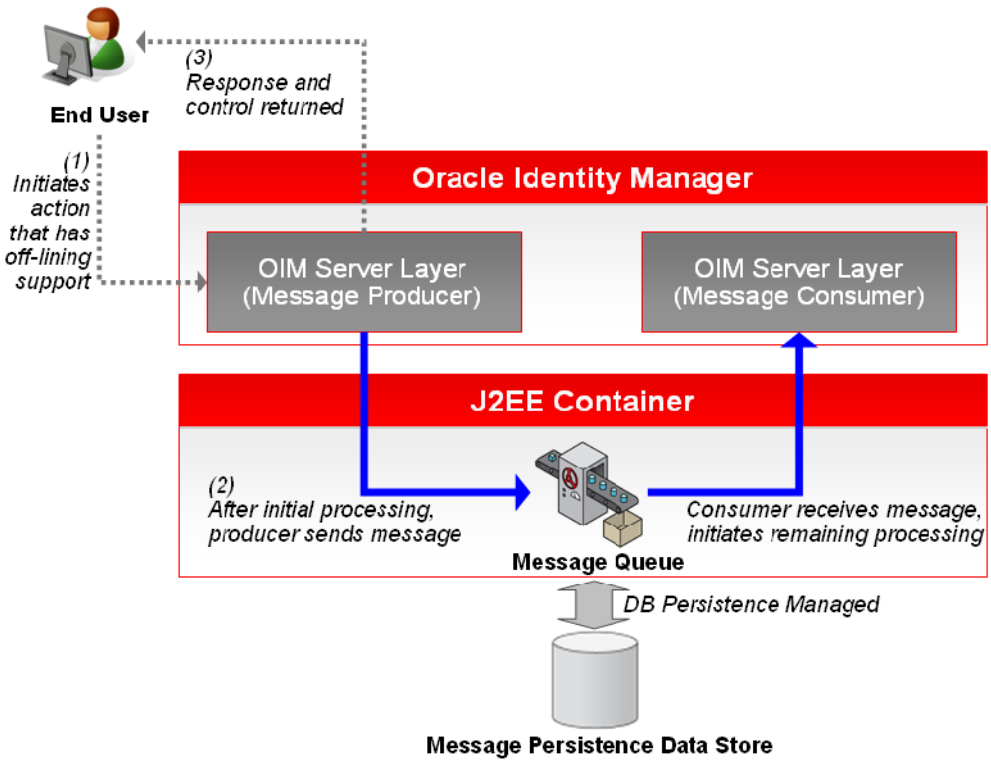

Figure 3: JMS-Based Processing of Oracle Identity Manager Operations

Customers can extend an operation by adding their extensions in either the pre- or post-processing steps. (In some cases, customers might also want to override the action step.) The time it takes to execute an operation is directly proportional to the number of synchronous event handlers that must be executed and the time taken to execute the slowest synchronous event handler.

With few exceptions, Oracle Identity Manager defers post-processing operations by leveraging Java Message Service (JMS) queues. After the action has been completed, Oracle Identity Manager submits JMS messages for the post-processing steps. Message-driven beans (MDB) consume and process these messages. This approach decouples the end user request and the action from the complex, resource-intensive post-processing operations. As a result, Oracle Identity Manager can respond faster to end user requests and can scale linearly from an end user request perspective. From a sizing perspective, the deferred processing approach makes JMS message processing a key sizing factor.

- **Data Tier**

  The Data tier includes

  - Audit Services
  - Reconciliation Services
  - Reporting Services

  Oracle Identity Manager provides a powerful audit engine that collects extensive data for audit and compliance purposes. You can use the audit functionality together to capture, archive, and view entity and transactional data for compliance monitoring and IT-centric processes and forensic auditing. Therefore, with the audit and compliance modules, Oracle Identity Manager provides profile auditing, reporting, and attestation features. You can capture, transport, store, retrieve, and remove historical data over its life cycle. Security is maintained at every stage of the data life cycle.

  Any action that a user performs in Oracle Identity Manager translates into an Application Programming Interface (API) call or a Message Driven Bean (MDB) picking up a message to process an action. Because an action can cause multiple changes, all changes are combined into an audit transaction. The audit engine generates a transaction ID to identify the changes made in the transaction.

  Customers can control auditing granularity by setting the relevant auditing level parameters. At its finest level, the auditing engine will audit the following:

  - User profile changes
  - User configuration changes
  - Role profile changes
  - Account definition changes
  - Account data changes

  From a sizing perspective, customers must consider the impact to performance and data growth when setting audit levels.

  Reconciliation is the process by which operations; such as user creation, modification, or deletion that are started on the target system are communicated to Oracle Identity Manager. The reconciliation process compares the entries in Oracle Identity Manager and the target

system repository, determines the difference between the two repositories, and applies the latest changes to Oracle Identity Manager.

In Oracle Identity Manager 11g, the reconciliation engine delegates the processing of changes, matching rule evaluation and applying the changes to the database. This process allows Oracle Identity Manager to take advantage of batching and bulk operations in the database, scale to a multi-million user population, and provide as much as 10x performance improvement. Because reconciliation primarily takes place in the database, database sizing becomes a key part of the overall Oracle Identity Manager sizing exercise.

The impact of reconciliation on sizing depends upon these factors:

- The number of authoritative sources
- The number of resources
- The number of accounts per resource
- The frequency of reconciliation
- The degree of change in all resources (authoritative and target)
- The amount of pre- or post-processing of data involved

3 Deployment Architectures

The Oracle Identity Manager platform leverages the flexibility of the J2EE framework, along with its scalability features, to provide a number of different deployment options to the customer, depending on their requirements. This section reviews some common deployment options. Oracle WebLogic Server, referred to as WebLogic hereafter, as the J2EE application server is used as the J2EE application server for these options

3.1 Baseline Deployment

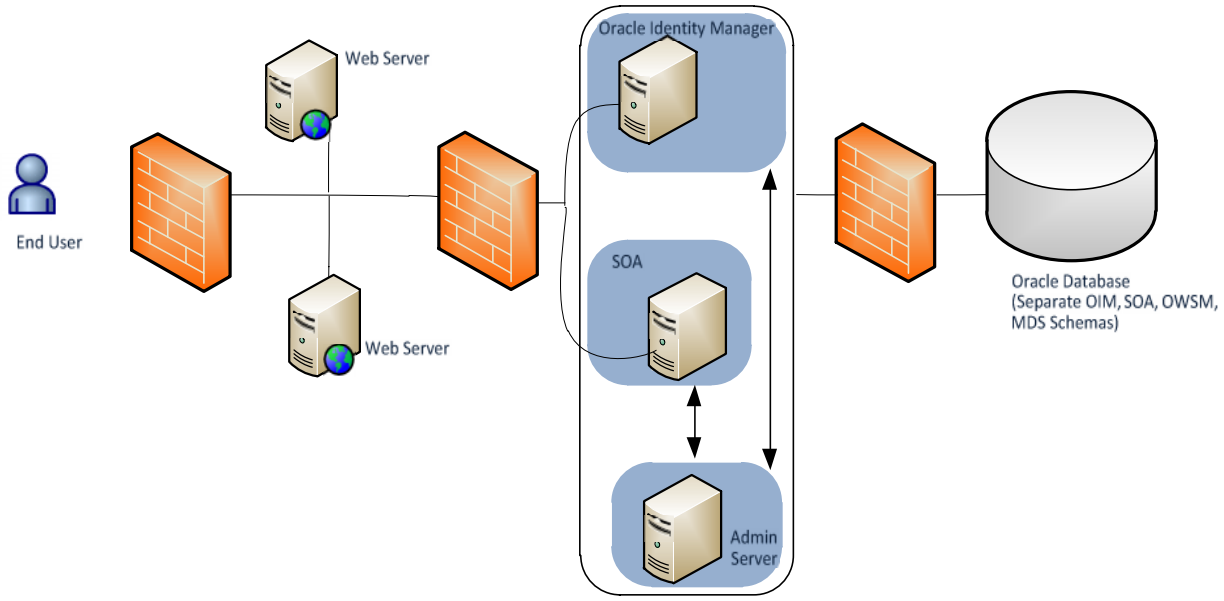

Figure 4 : Baseline Oracle Identity Manager Architecture

The baseline deployment of Oracle Identity Manager 11g consists of the following components.

- A WebLogic Admin Server (shared)
- A WebLogic Managed Server instance for Oracle Identity Manager 11g
- A WebLogic Managed Server instance for SOA, OWSM (Oracle Web Services Manager) for web services security
- An Oracle database instance which stores the product schemas for the various Fusion Middleware components along with Oracle Identity Manager and SOA.
- A Web Server to act as a proxy for the OIM and SOA Managed Servers.

3.2 Highly Available

In this deployment, Oracle Identity Manager and SOA are deployed in a J2EE cluster. The cluster is front-ended by a pair of web servers, which proxy requests generated in the UI and SPML layers to the cluster with the help of the web server's proxy plug-ins. A load balancer load balances the requests to the HTTP servers.

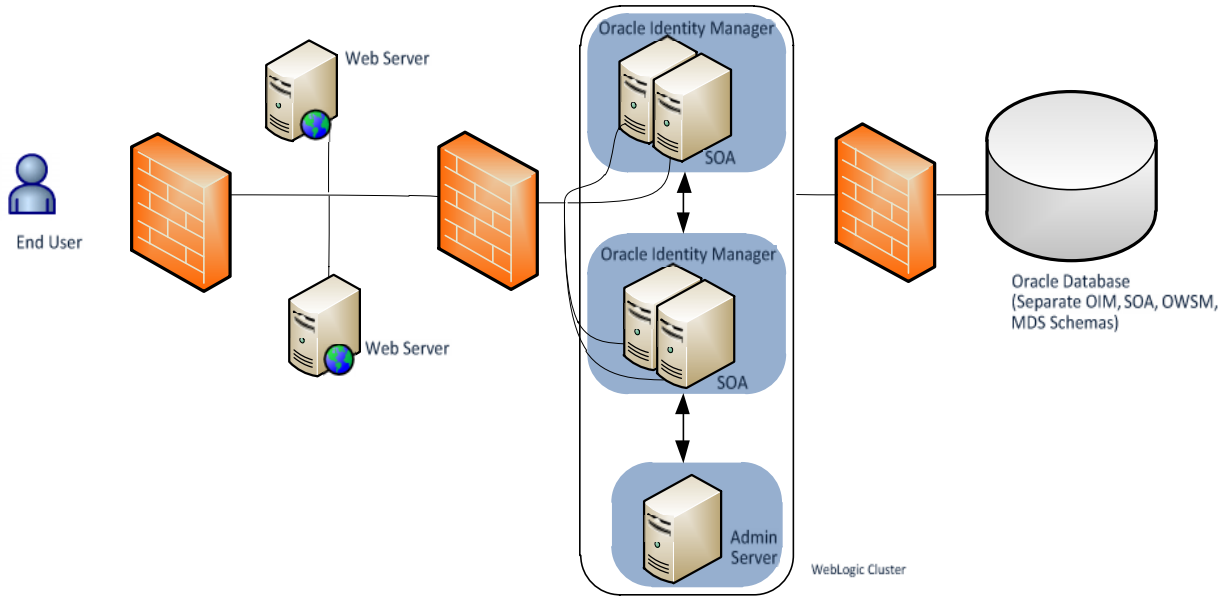

Figure 5: Highly available Oracle Identity Manager Deployment

This deployment consists of the following components

- A pair of load balanced web servers
- A WebLogic cluster consisting of pair of co-located Oracle Identity Manager and SOA managed server deployments. In this deployment, each machine hosts a WebLogic managed server for Oracle Identity Manager and SOA each.
- A WebLogic Admin Server located on an independent machine.
- An Oracle database instance which stores the product schemas for the various Fusion Middleware components. The database instance can be RAC or non-RAC. Generally, it is recommended that customers follow the Oracle Maximum Availability architecture (MAA) recommendations for database high availability. Please see the Additional Resources section for more information on MAA.

4. Sizing a Deployment

There is no single guideline in infrastructure sizing. Many factors influence the ultimate outcome including

- Network performance,
- Deployment complexity,
- Number and type of resources, and
- Database performance.

Customers should also note that additional tuning may be required, depending upon the selected hardware, to get optimal performance.

4.1 Baseline

A baseline deployment of Oracle Identity Manager, as shown in Figure 4, consists of the following components

- WebLogic Managed Server for Oracle Identity Manager 11g
- WebLogic Managed Server for SOA
- WebLogic Admin Server (shared by the managed servers)
- Database instance containing the product schemas

The following hardware configuration is required to support this baseline.

Middle Tier

	Node 1	Node 2
CPU	1 x86 CPU Dual Core	1 x86 CPU Dual Core
Minimum RAM	6 GB	6 GB
Minimum Heap	-ms2048m –mx2048m per Managed Server	-ms2048m –mx2048m per Managed Server
Number of Managed Servers	OIM and SOA Managed Server and Admin Server	OIM and SOA Managed Server

Database Tier (for Oracle Identity Manager and SOA)

CPU	1 x86 CPU Dual Core
Minimum RAM	6 GB
Disk Space	500 GB

Notes:

- The database hardware assumes that SOA, Oracle Identity Manager and related components share the same database.
- The middle tier hardware is for the SOA and Oracle Identity Manager managed servers only.
- Both managed servers may be deployed on a single machine or each Oracle Identity Manager/ SOA managed server may be on separate machines.

The baseline configuration supports the deployment characteristics shown below.

Deployment Characteristics

Metric	Volume metrics
Number of Users	25,000
Number of logged in users	2500
Number of concurrent operations	25
Number of Roles	1,000 with average 10 members per role
Number of Organizations	1000
Total number of resources	5
Number of Resources per user	5
Proportion of provisioning done via Requests	50%
Number of Access Policies	1000 with 2 resources per Access Policy
Audit level	Form
Reconciliation	5% change in a target system with weekly reconciliation with a SLA of 3 hours
Average UI response time	5 seconds
Average CPU utilization	60%

4.2 Scaling the deployment

With the baseline configuration as a starting point, customers can scale out their deployment based on a variety of factors, including

- Total user population,
- Projected number of concurrent operations,
- Projected bulk operations,
- Projected number of requests
- Number of roles and role members per role
- Number of roles and resources associated with a access policy
- Projected number of user attribute changes
- Projected volume of trusted and target resource reconciliation

The factors mentioned above individually and collectively affect infrastructure sizing. Customers should use the metrics given below to calculate the hardware required.

Note:

1. It is recommended that customers keep a 10-20% spare capacity to allow the deployment to handle out-of-bound situations, rather than operating the deployment at capacity.
2. Deployments should factor in Disaster Recovery scenarios where the cluster node(s) may be required to handle the load of the failed nodes.

4.2.1 Scaling the Oracle Identity Manager deployment

Using the baseline deployment as a starting point, customers should

- Add an additional Oracle Identity Manager Managed Server for every 50 concurrent operation
- Add an additional SOA Managed Server for every 200 outstanding requests
- Augment database server capacity by 1 dual core CPU and 6 GB RAM) for any of the following conditions
    - every 25 concurrent operations,
    - 100% increase in reconciliation volume,
    - 25% increase in role operations such as role grants and role revokes
    - 50% increase in number of resources

4.2.2 Scaling the Oracle Database for Oracle Identity Manager and SOA

- Storage capacity planning

Using the baseline as the starting point, customers should plan for any of the following conditions.

- 25% growth in disk space when the number of resources provisioned are doubled
- 50% growth in disk space when the number of users are doubled
- 20% growth in disk space when the number of requests submitted is doubled
- 30% growth in disk space when the number of roles or role memberships is doubled.

- Sizing the database machine for performance

Using the baseline as the starting point, it is suggested that customers consider adding an additional CPU to the database server for any of the following conditions

- For every 100 concurrent operations,
- For every increment of 500,000 users upto 2 million users.
- For every increment of 50 Access Policies with 1 resource per Policy
- For every 50 connected resources that are provisioned and reconciled.

For accurate forecasting, customers should leverage the Oracle Enterprise Manager Database Console and set baselines and alerts. This will help them plan database capacity augmentation more accurately.

5 Conclusion

Identity administration and provisioning deployments may be complex in nature. Many factors such as end user operations, usage spikes, role-based access, etc. play a part in determining the load. Oracle Identity Manager 11g offers significant architectural and functional innovations that enable scaling to extranet user populations and handle hundreds of concurrent operations. The combination of Oracle Identity Manager's innovative use of Fusion Middleware and the Oracle Database ensure that customers following the sizing guidelines can arrive at a fairly accurate deployment.

Additional Resources

- What's new in Oracle Identity Management 11g
  http://www.oracle.com/us/products/middleware/identity-management/new-in-oim11g-163958.pdf
- Oracle Identity Manager Technical White Paper
  http://www.oracle.com/technetwork/middleware/id-mgmt/overview/identity-manager-wp-11gr1-156947.pdf
- Oracle Maximum Availability Architecture
  http://www.oracle.com/technetwork/database/features/availability/maa-090890.html

Oracle Identity Manager 11g Sizing Guide
December 2010

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