An Oracle White Paper
October 2012

Oracle Identity Management 11gR2 Sizing and Capacity Planning
Disclaimer

The following is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. This document is subject to change at Oracle’s sole discretion.
Introduction

This document is designed to provide capacity planning and environment sizing estimates based on the computing power required for deploying Oracle Identity Management 11gR2 components. The purpose of this document is to help Oracle field representatives approximate hardware requirements (number of processors) necessary for a given sales situation.

For the purposes of Oracle software licensing, the term "processor" is the total number of processor cores used by any of the Oracle Identity Management 11gR2 components multiplied by the respective core multiplier. The core multiplier is based on the processor architecture defined in the Processor Core Factor Table, which is available at the following web page: http://www.oracle.com/us/corporate/contracts/processor-core-factor-table-070634.pdf. Currently (2012), most server configurations start with 4 cores and go up from there. For example, Oracle SPARC T4 has 8 cores per processor and T3 has 8 or 16 cores, Intel Xeon processors support up to 10 cores, and AMD Opteron processors support up to 16 cores. Every processor must be licensed. This includes restricted-use licenses that ship with a specific product that run on separate processors.

The various components making up the Oracle Identity Management 11gR2 platform perform various tasks leveraging hardware resources such as applications servers and database servers in different ways. As a result, the parameters used to estimate the computing power requirements needed for a specific solution may vary for each Oracle Identity Management 11gR2 component.

This document first introduces the Oracle Identity Management 11gR2 platform. The second part provides sizing information for Oracle Identity Management 11gR2 components, and the last part gives examples of typical customer deployments.
Introducing Oracle Identity Management 11gR2

Oracle shipped Oracle Identity Management 11gR2 in July 2012. Oracle Identity Management 11gR2 leverages previous Oracle Identity Management releases and emphasizes the following themes and drivers:

- **Simplified user experience.** Access request is as simple as shopping online for the access needed using a user interface that is easily configurable through end-user screen-design tools.

- **New cloud, mobile, and social services:** Full, secure integration of mobile applications with the enterprise’s backend identity management infrastructure. Support for enterprise interaction with social networking sites through standard, lightweight interfaces and access protocols.

- **Enhanced governance:** Role catalogs and enhanced certification review with multiple-level certification. Server-based privileged account management (PAM) providing a password checkout system for heterogeneous, shared operating system, enterprise application, and database accounts leveraging a single workflow, a single resource connector set, and a single attestation model.

- **Extreme scale:** For example, Java-based Oracle Unified Directory (OUD) achieves three times the performance of its predecessor at one sixth of the cost on an Oracle SPARC T4 server. Oracle Access Manager (OAM) can support 250 million users with 3,000 authentications per second.

Oracle Identity Management 11gR2 includes three platforms: Oracle Directory Services, Oracle Identity Governance, and Oracle Access Management. Each of these platforms includes services implemented in a suite of fully interconnected and integrated components.

![Figure 1: Oracle Identity Management 11gR2 Logical View](image)

Each of the platforms shown in Figure 1 is described in the following section.
Oracle Identity Management 11gR2 Components

The following tables summarize Oracle Identity Management 11gR2 main services and components.

**Platform Security Services**

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Platform Security Services (OPSS)</td>
<td>OPSS is a standards-based, enterprise-grade framework exposing security services through pluggable abstraction layers in Oracle WebLogic Server (WLS). OPSS includes security APIs for authentication, authorization, session management, identity context, identity governance, credential store, policy store, and audit. OPSS is used by developers to weave security into Fusion applications. OPSS services are consumed by all Oracle Fusion Middleware (OFM) components at runtime. (OPSS and OES (described below) share the same authorization API code line.) <em>Note:</em> A portability layer (known as Java Required Files or JRF) includes components not included in the Oracle WLS installation. These components provide common functionality for Oracle applications (Oracle Identity Management 11gR2 components consume the portability layer’s functionality at runtime). JRF allows one to accommodate OFM components on third-party application servers.</td>
</tr>
<tr>
<td>Oracle Web Services Manager (OWSM)</td>
<td>OWSM is the policy-centric security lynchpin for OFM web services. OWSM secures standards-compliant web services (Java EE, Microsoft .NET, PL/SQL, etc.), SOA composites, Oracle WebCenter’s remote portlets, and Oracle Fusion Applications.</td>
</tr>
<tr>
<td>Oracle Entitlement Server (OES)</td>
<td>OES is a fine-grained authorization engine that externalizes, unifies, and simplifies the management of complex entitlement policies. OES is used by multiple OFM components to support context-aware access control and delegation. OES includes Oracle Authorization Policy Manager (APM), an administration console for OES and OPSS-based authorization policies.</td>
</tr>
</tbody>
</table>

**Directory Services**

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Internet Directory (OID)</td>
<td>OID is an LDAP directory server and directory integration platform (DiP) implemented on top of Oracle Database technology providing unsurpassed level of scalability, high-availability, and information security.</td>
</tr>
<tr>
<td>Oracle Unified Directory (OUD)</td>
<td>OUD is a Java-based, all-in-one LDAP directory solution including storage, proxy, synchronization, and virtualization capabilities.</td>
</tr>
<tr>
<td>Oracle Directory Server Enterprise Edition (ODSEE)</td>
<td>ODSEE is an enterprise identity service including the LDAP Directory Server, Directory Proxy, Directory Synchronization, a web-based management user interface (Directory Services Control Center – DSCC), and deployment tools. ODSEE is the industry’s leading carrier-grade directory.</td>
</tr>
<tr>
<td>Oracle Virtual Directory (OVD)</td>
<td>OVD is a Java-based application designed to provide real-time identity aggregation and transformation without data copying or data synchronization. OVD provides a single standard interface to access identity data no matter where it resides while hiding the complexity of the underlying data infrastructure. OVD is integrated with multiple OFM components.</td>
</tr>
<tr>
<td>Oracle Directory Services Manager (ODSM)</td>
<td>ODSM is the web-based administration user interface for directory services configuration. ODSM is the centralized administration component for OID, OUD, and OVD (ODSEE has its own console).</td>
</tr>
</tbody>
</table>
## Access Management

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Access Manager (OAM)</td>
<td>OAM provides centralized, policy driven, identity-context-based services for web applications authentication, web single sign-on (SSO), identity assertion, and built-in service provider identity federation. OAM integrates with a broad array of authentication mechanisms, third-party web servers and application servers, and standards-based federated SSO solutions to ensure maximum flexibility and a well-integrated, comprehensive web access control solution.</td>
</tr>
<tr>
<td>Oracle Adaptive Access Manager (OAAM)</td>
<td>OAAM provides context-aware resource protection through real-time fraud prevention, software-based multifactor authentication, and unique authentication strengthening.</td>
</tr>
<tr>
<td>Oracle Identity Federation (OIF)</td>
<td>OIF is a self-contained solution enabling browser-based, cross-domain single sign-on using industry standards (SAML, WS-Federation, OpenID). OIF seamlessly integrates with third-party identity and access management solutions. OIF supports a lightweight federation extension (&quot;Fedlet&quot;) allowing a service provider to immediately federate with an identity provider without requiring a full-blown federation solution in place (OIF and Fedlet are independent from each other).</td>
</tr>
<tr>
<td>Oracle Security Token Service (STS)</td>
<td>OSTS establishes a trust relationship between online partners through web services. OSTS provides both standard and proprietary security token issuance, validation, and exchange. OSTS is part of OAM (described above).</td>
</tr>
<tr>
<td>Oracle Mobile and Social Service</td>
<td>Oracle Mobile and Social Service is designed to secure mobile access to applications leveraging the enterprise’s existing back-end identity management infrastructure. Oracle Mobile and Social Service provides client software development kits used by developers to weave security into native mobile applications for tight integration with backend identity management. Oracle Mobile and Social Service enables enterprises to securely leverage social identities for personalization and federated sign-on to help organizations grow their business through social networks.</td>
</tr>
<tr>
<td>Oracle Enterprise Single Sign-On (eSSO)</td>
<td>OESSO is a Microsoft Windows desktop-based set of components providing unified authentication and SSO to thick- and thin-client applications with no modification required to existing applications.</td>
</tr>
<tr>
<td>Oracle Enterprise Gateway (OEG)</td>
<td>OEG is a security gateway deployed in the DMZ. OEG supports multi-protocol and multi-format web services and web application programming interfaces, data redaction (in conjunction with OES), identity propagation, and access to legacy applications. OEG provides firewall protection for RESTful service calls into the Oracle Mobile and Social Service.</td>
</tr>
</tbody>
</table>

## Identity Governance

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Identity Manager (OIM)</td>
<td>OIM is a role-based server designed to administer both intranet and extranet user access privileges across a company’s resources throughout the entire identity management life cycle, from initial on-boarding to final de-provisioning of an identity. In extranet environments, OIM’s superior scalability allows enterprises to support millions of customers accessing the company’s resources using traditional clients (e.g., browsers) or mobile devices.</td>
</tr>
<tr>
<td>Oracle Identity Analytics (OIA)</td>
<td>OIA helps enterprises address regulatory mandates, automate processes, and quickly make compliance a repeatable and sustainable part of business. OIA integrates with OIM for role administration and role-based provisioning automation as part of Oracle remediation (OIA and OIM share the same data model).</td>
</tr>
</tbody>
</table>
Oracle Identity Management 11gR2 Sizing and Capacity Planning

Oracle Privilege Accounts Manager (OPAM)

OPAM is a server-based password repository designed to generate, provision, and manage passwords for privileged users accessing specific resources such as operating systems root accounts, and enterprise application and database server administration accounts. OPAM relies on ICF-based connectors to access the resources that need to be used by privileged users.

Identity Connector Framework (ICF)

ICF is an abstraction layer between OIM or OPAM and a target system (ICF offers many features that developers would otherwise need to implement). ICF includes Connector Application Programming Interfaces (API) and Connector Service Provider Interfaces (SPI). Typically, a target system calls the Connector API and the Connector SPI is implemented by developers for each target system. ICF may be installed on a different server from OIM or OPAM.

Operational Manageability

<table>
<thead>
<tr>
<th>COMPONENTS</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Identity Navigator (OIN)</td>
<td>OIN is an SSO-enabled launch pad for all Oracle Identity Management services' administrative consoles.</td>
</tr>
</tbody>
</table>

Oracle Identity Management Sizing

This section is divided up into three parts: Oracle Directory Services Plus, Oracle Access Management, and Oracle Identity Governance.

Oracle Directory Services Plus

This section is a high-level summary of the Oracle Directory Services Plus (ODS+) Sizing Guide, available at the following web page:

[http://webcenter.us.oracle.com/webcenter/content/conn/UCM/path/PersonalSpaces/brad.diggs@oracle.com/Public/ODS+_11g_Core_Sizing_Guide-20120110.pdf](http://webcenter.us.oracle.com/webcenter/content/conn/UCM/path/PersonalSpaces/brad.diggs@oracle.com/Public/ODS+_11g_Core_Sizing_Guide-20120110.pdf).

The ODS+ products and tools to be including when sizing a directory service opportunity can include any of the following:

- Oracle Unified Directory (OUD) directory server
- Oracle Unified Directory proxy server
- Oracle Directory Server Enterprise Edition (ODSEE) directory server
- Oracle Directory Server Enterprise Edition (ODSEE) proxy server
- Oracle Internet Directory (OID) directory server
- Oracle Virtual Directory (OVD)
- Directory Integration Platform (DIP)
• Oracle Directory Service Manager (ODSM)
• Enterprise User Security (EUS)
• Oracle Authentication Services for Operating Systems (OAS4OS)
• LDAP based Name Services (LDAP NS)
• Oracle Enterprise Manager Fusion Middleware Control (OEM FMW)
• Oracle Enterprise Manager Grid Control (OEM GC)

OEM GC does not ship with ODS+. It is used to augment monitoring of the ODS+ products. EUS, OAS4OS, and LDAP NS are tools that ODS+ customers can leverage to simplify and streamline database and enterprise authentication and name services.

ODS+ is typically licensed for production environments by processor. Non-production environments may also be licensed by processor but are typically licensed by named user.

This section is intended to address directory service deployments with 10 million or less entries. If the directory service that you are seeking to size exceeds 10 million entries or has special performance or availability requirements, contact the respective product’s product manager.

To simplify sizing for 10 million or less entries, the following table provides a high level summary of the number of cores necessary to minimally satisfy basic availability, serviceability, and performance requirements. Availability ensures that the directory service continues to operate if a directory server instance fails. Serviceability ensures that the directory service continues to be highly available when one instance is taken offline. Performance ensures that there are enough directory server instances to meet performance expectations.

<table>
<thead>
<tr>
<th>DATA CENTERS</th>
<th>SERVERS</th>
<th>AVAILABILITY</th>
<th>SERVICEABILITY</th>
<th># OF CORES</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>No</td>
<td>No</td>
<td>2</td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>Yes</td>
<td>No</td>
<td>4</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>Yes</td>
<td>Yes</td>
<td>6</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>Yes</td>
<td>Yes</td>
<td>8</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>Yes</td>
<td>Yes</td>
<td>12</td>
</tr>
</tbody>
</table>

**ODS+ Architectural Overview**

Figure 2 provides an overview of the architectural components that are typically included in a new ODS+ deployment. Each architectural component has its own unique sizing requirements. However, multiple architectural components can be collocated on a single server, depending on the resource constraints and requirements for the service. When sizing a deployment, estimate as if each architectural component used at least one processor core per instance even if some components are collocated on a single server.
Directory service deployments include a wide variety of topologies. For example, highly available environments include a network load balancer and OVD or OUD proxies in the DMZ and two directory servers in the data tier; highly available and serviceable environments include a network load balancer and OVD or OUD proxies in the DMZ and three directory servers in the data tier; highly available and serviceable environments spanning several data centers include the same deployment type as highly available environments in each data center.

The combination of core count, and clock frequency per processor, and whether multi-threading is enabled together form the computational basis for performance extrapolation. For example, a server with a 2GHz 4-core HT enabled processor that delivers 15,000 search operations per second may yield over 31,000 search operations per second in a server with a 3.4GHz 6-core HT enabled processor.

\[
\frac{(15,000 \times 6 \times 3.4GHz)}{(4 \times 2GHz)} = 31,875 \text{ search operations per second}
\]

Actual performance may vary according to many factors but this data can be a reference for small and simple use cases.

**ODS+ Components Considerations**

Each of the component products within the ODS+ suite may have unique considerations when sizing the number of cores required.

**OID Database Considerations:** OID includes an Oracle database, one or more LDAP servers, and a replication server. For lower-end implementations (under 10M entries), the Oracle database can be co-located on the same physical server as the LDAP and replication services. However, OID also supports running the database on other servers as well, in which case additional cores will be required.
for the Oracle database. Further, the specific database used for OID may require additional servers and consequently more processor cores. For example, implementing an Oracle Real Application Cluster (RAC) database as the backend for OID may require additional servers.

**OVD Virtualization Considerations:** The amount of processing power is proportional to the amount of virtualization applied as well as the amount of customization employed for special needs.

**Encryption Considerations:** Each of the ODS+ components supports encryption for network transport, storage, or both. Encryption can add over 10 times the amount of non-encrypted processing load. If encryption is required, determine if the encryption can be offloaded to crypto accelerators.

**ODS+ Usage Scenarios**

The following table summarizes five usage scenarios used for estimating ODS+ sizing, based on the number of users, subscribers (110K, 500K, 1M, 5M, 10M). The correlations expressed in the table below are arbitrary.

<table>
<thead>
<tr>
<th>ENTRIES, USERS, OR SUBSCRIBERS</th>
<th>110K</th>
<th>500K</th>
<th>1M</th>
<th>5M</th>
<th>10M</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Small</td>
<td>Medium</td>
<td>Medium</td>
<td>Large</td>
<td>Large</td>
</tr>
<tr>
<td>Service Provider</td>
<td>Small</td>
<td>Small</td>
<td>Medium</td>
<td>Medium</td>
<td>Large</td>
</tr>
<tr>
<td>Peak Concurrency</td>
<td>15%</td>
<td>5%</td>
<td>5%</td>
<td>10%</td>
<td>10%</td>
</tr>
<tr>
<td>Data Size</td>
<td>800MB</td>
<td>4GB</td>
<td>8GB</td>
<td>40GB</td>
<td>80GB</td>
</tr>
<tr>
<td>Data+CL+Logs</td>
<td>20.8GB</td>
<td>24GB</td>
<td>28GB</td>
<td>60GB</td>
<td>100GB</td>
</tr>
<tr>
<td>Peak/s</td>
<td>Sustained/s</td>
<td>Auth Response (ms)</td>
<td>200</td>
<td>100</td>
<td>100</td>
</tr>
<tr>
<td>Peak/s</td>
<td>Sustained/s</td>
<td>Auth Response (ms)</td>
<td>300</td>
<td>250</td>
<td>50</td>
</tr>
<tr>
<td>Peak/s</td>
<td>Sustained/s</td>
<td>Auth Response (ms)</td>
<td>10</td>
<td>5</td>
<td>800</td>
</tr>
<tr>
<td>Peak/s</td>
<td>Sustained/s</td>
<td>Auth Response (ms)</td>
<td>5</td>
<td>2</td>
<td>800</td>
</tr>
<tr>
<td>Peak/s</td>
<td>Sustained/s</td>
<td>Auth Response (ms)</td>
<td>10</td>
<td>5</td>
<td>600</td>
</tr>
</tbody>
</table>

**Sizing Considerations**

There are four main considerations when sizing an ODS+ directory service architecture. The following sections outline each requirement and how each requirement translates to the processor core
count estimation. ODS+ core sizing typically starts off with 8 or 12 cores in order to meet minimal high availability and performance requirements.

**High Availability Requirement:** Directory service high availability is typically achieved by implementing two or more directory server nodes in a replicated topology. OID has the additional option of being able to be configured in a high availability cluster either through DataGuard or by upgrading to the RAC database. The replicated directory service topology and RAC methods result in 2 or more active-active nodes that can service directory service load.

Two servers are sufficient for minimal high availability. However, if a server needs to be taken offline for maintenance, the directory service will no longer be highly available. Thus, a minimum of 3 servers is required to achieve a highly available directory service that is also serviceable.

OVD, DIP, OUD proxy, and ODSEE proxy all similarly employ two or more nodes for availability. If there are sufficient resources available per server, these components can be collocated on the same servers as the directory server instances. Whether implementing 2 or 3 directory server nodes, most customers are able to satisfy the performance requirements with a single directory service node. This is because most modern servers come at a minimum with 2GHz 4-core processors. Any of the three directory server products in the ODS+ portfolio can deliver thousands of LDAP search operations per second with a server of this size.

Having 2-3 directory server nodes for high availability would translate into between 8-12 cores depending on whether the customer wants to have a serviceable or just highly available directory service. The actual number of servers and cores per server is determined by the full set of requirements and not just the minimal high availability requirements.

**Multiple-Datacenter Requirement:** A directory service is often deployed in multiple datacenters in order to avoid a single point of failure. OVD, DIP, OUD proxy, and ODSEE proxy may also be implemented in each of the datacenters for high availability. If there are sufficient resources available per server, these components can be collocated on the same servers as the directory server instances.

For performance purposes, customers often place directory server instances in each of the primary datacenters. This approach reduces latency to the LDAP applications, provides horizontal scalability of the directory service, and minimizes WAN bandwidth costs by keeping LDAP client traffic from going over the WAN.

The best way to estimate the number servers required for multi-datacenter directory architectures is to multiply the number of data centers by the minimal number of directory servers per datacenter. In most cases, the minimum number of servers per datacenter is 2. For example, a minimal highly available directory service architecture that spans 3 datacenters would require 6 servers. With the minimum of 4 cores per server, the resulting minimal core count would be 24 processor cores.

**Data Caching Requirement:** As the size of the customer’s directory data grows, the caching requirement grows as well. For optimal performance, the server’s random access memory (RAM) should be sufficiently large to fit all of the directory data with extra room for the operating system and other system processes. A directory server data set size that exceeds the memory capacity of a server may
require adding more processors or upgrading to the next larger server model in order to accommodate more RAM to properly cache all of the directory data.

The amount of RAM that fits in a server is often correlated to the number of processors installed. For example, a server that supports up to 96GB of RAM may only be able to fit 48GB of RAM with a single processor installed. The second processor is required in order to upgrade to the full 96GB of RAM.

Performance Requirement: Directory service performance can be defined by several criteria. Consider the following examples:

- Operational – The directory must be able to handle a minimum of 1,000 search operations per second.
- Latency: The average response time must be less than 1 second per operation.
- Concurrency: The directory service must be able to handle 1,000 concurrent connections.
- Synchronicity: The directory service must take no longer than 1 second to replicate an update throughout the replication topology.
- Administrative: A backup or restore of the server cannot exceed 72 hours.

Caching applies almost exclusively to the directory server storage products such as OUD, ODSEE, and OID. However, if OVD is configured to cache data or use external caching, the server containing OVD and its cache will also need to be sized to fit the desired amount of data to be cached. This may be a subset of the directory data or it may be intended to fit the entire directory data set.

Deploying ODS+ on Virtual Platforms

Oracle only supports the following virtual platforms: Oracle VM Server for x86, Oracle VM Server for SPARC, and Oracle Solaris Containers.

Based on Oracle’s licensing policy for virtualization platforms, if the virtualization platform doesn’t support hard partitioning, the customer will have to pay for all cores in the physical server, otherwise the customer pays for the number of hard partitioned cores that are dedicated to the software to be licensed. Hard partitioning means that a whole core and all of that core’s threads are dedicated to a specific virtual machine such that the core and its threads cannot be used by any other process or virtual machine on the server. Any virtualization technology that does not support true hard partitioning requires that all cores of the server be licensed for use by the ODS+ products running on that server.

Threads per core are not part of the core accounting equation. For example, if a server has 8 processor cores with 8 threads per core, the only number that should be used for core accounting is the actual number of cores. In this example, a customer would be licensed for 8 cores rather than 64 threads.

Oracle Access Management

This section provides sizing information for the following components: Oracle Access Manager (OAM), Oracle Identity Federation (OIF), Oracle Security Token Service (OSTS), Oracle Mobile and
Social Service (OMS), Oracle Adaptive Access Manager (OAAM), Oracle Enterprise Single Sign-on (OESSO), and Oracle Enterprise Gateway (OEG). Sizing guidelines for combined solutions (OAM, OIF, OSTS, OMS) and as well as Oracle Access Management platform considerations are also provided.

For sizing guidelines, the transaction load may be steady (basic assumption) or peak.

• **Steady Load Scenario:** In the case of Oracle Access Management, authentications, authorizations, token evaluation and exchange, and risk evaluation operations are a reflection of regular business activity and it is assumed that they happen at a steady pace throughout the day. At a steady state, changes to dynamic policies may not have a significant impact on throughput. A steady state load is defined to be 30% of CPU usage with an average latency of less than 1s, 100ms, 100ms for authentication, token validation, and authorization operations respectively. It is assumed that a policy change throughput is 10 policies per second.

• **Peak Load Scenario:** When load increases on the Oracle Access Management server, it is assumed to be the result of authentication/login and token issuance activity. For example, for internal deployments, the spike may occur on Mondays for the first two hours of the business day when most employees are logging in. Authorization is generally a reflection of business activity, which is sustained at a steady rate. If deviating from these operation assumptions, it is recommended to tune the Oracle Access Management environment to achieve optimal performance and reflect usage characteristics for a given deployment. Please refer to the tuning considerations outlined in the Fusion Middleware Performance Guide 11gR2.

The following peak load characteristics apply to a given standard recommended topology: Peak authentication throughput: 2x steady state throughput; Peak CPU usage: 90%; Peak authorization throughput: 1.2x steady state throughput.

**Enterprise Deployment**

An enterprise deployment is an Oracle best practices blueprint based on proven Oracle high-availability technologies and recommendations for Oracle Fusion Middleware. Detailed instructions and recommendations to create enterprise level topologies are covered as part of the Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (http://docs.oracle.com/cd/E21764_01/core.1111/e12035/toc.htm).

**Deployment Environments**

Multiple environments are used during the lifecycle of a project:

• **Development** (sometimes referred to as “Integration”): This environment is used to deploy Oracle Access Management products, and configure and implement specific use cases for a specific customer deployment.

• **Pre-Production** (sometimes referred to as “Test” or “Staging”): This environment typically contains a replica of the production environment data. This environment is used to test new releases of the project, and simulate production environment behavior.
• Production: This environment supports full-blown production applications and services.

Customers may choose the options of having a demonstration, training or stress / performance environment. From a sizing perspective, these environments can be mapped to either a development or pre-production environment.

**Oracle Access Management Sizing Guidelines**

This section provides sizing guidelines for Oracle Access Management components including Oracle Access Manager (OAM), Oracle Identity Federation (OIF), Oracle Security Token Service (OSTS), and Oracle Mobile and Social Service (OMS).

Oracle Access Management components are installed together and share a common services platform and a common administrative platform from which they can be enabled or disabled to meet specific customer requirements.

The following guidelines are designed as a steady-state load reference for determining hardware requirements for specific customer deployments, based on the following assumptions:

• A deployment handles up to 1 million end users and/or 100 applications (larger deployments are described in the following section).

• Sizing applies to a single data center. Multiple data centers need to be sized independently.

It is recommended that the production configuration be setup for disaster recovery, i.e., the configuration is duplicated in a different location. Disaster recovery environments need to be sized separately.

<table>
<thead>
<tr>
<th>COMPONENT / SETTINGS</th>
<th>DEVELOPMENT</th>
<th>PRE-PRODUCTION</th>
<th>PRODUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run-Time Server</td>
<td>All three components deployed on the same machine.</td>
<td>2 Servers - 4 Quad-Core CPUs</td>
<td>4 Servers - 4 Quad-Core CPUs</td>
</tr>
<tr>
<td></td>
<td>1 Server - 2 Dual-Core CPUs</td>
<td>16 GB RAM each</td>
<td>with 16 GB RAM each</td>
</tr>
<tr>
<td></td>
<td>16 GB RAM</td>
<td>Heap Size: 1 GB</td>
<td>Heap Size: 8 GB</td>
</tr>
<tr>
<td>Administration Server</td>
<td>1 Server - 2 Dual-Core CPUs</td>
<td>1 Server - 2 Dual-Core CPUs</td>
<td>1 Server - 2 Dual-Core CPUs</td>
</tr>
<tr>
<td></td>
<td>with 16 GB RAM</td>
<td>with 16 GB RAM</td>
<td>with 16 GB RAM</td>
</tr>
<tr>
<td></td>
<td>Heap Size: 4 GB</td>
<td>Heap Size: 4 GB</td>
<td>Heap Size: 4 GB</td>
</tr>
<tr>
<td>Policy (Database) Server</td>
<td>2 (RAC) Servers - 1 Dual-Core CPU with 16 GB RAM each</td>
<td>2 (RAC) Servers - 1 Dual-Core CPU with 16 GB RAM each</td>
<td>2 (RAC) Servers - 1 Dual-Core CPU with 16 GB RAM each</td>
</tr>
<tr>
<td></td>
<td>Storage: 4KB per login session and 10 KB per policy object</td>
<td>Storage: 4KB per login session and 10 KB per policy object</td>
<td></td>
</tr>
</tbody>
</table>

The following table shows smaller deployments as a percentage of the 1 million-user deployment described in the table above.

<table>
<thead>
<tr>
<th>DEPLOYMENT SIZE</th>
<th># OF USERS</th>
<th>AUTH TPS</th>
<th>AUTHZ TPS</th>
<th>% OF STANDARD H/W</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Small</td>
<td>&lt; 250K</td>
<td>50</td>
<td>600</td>
<td>35%</td>
</tr>
<tr>
<td>Small</td>
<td>&lt; 500K</td>
<td>100</td>
<td>1300</td>
<td>60%</td>
</tr>
<tr>
<td>Medium</td>
<td>&lt; 750K</td>
<td>200</td>
<td>2700</td>
<td>80%</td>
</tr>
<tr>
<td>Standard</td>
<td>&lt; 1 Million</td>
<td>300</td>
<td>4000</td>
<td>100%</td>
</tr>
</tbody>
</table>
Very large deployment sizing guidelines make the same assumption as above. The following formula is used for very large deployments:

\[ Ssf = \left( 0.4 \times \left( \frac{\text{Required}_\text{AuthN}_\text{TPS}}{300} + \frac{\text{Required}_\text{Fed}_\text{AuthN}_\text{TPS}}{50} \right) + \frac{\text{Required}_\text{Token}_\text{Operations}_\text{TPS}}{125} \right) + \left( 0.4 \times \frac{\text{Required}_\text{AuthZ}_\text{TPS}}{3000} \right) + \left( 0.2 \times \frac{\text{Number}_\text{of}_\text{Resources} + \text{Number}_\text{of}_\text{Policies}}{1000} \right) \times (1 + \frac{u}{100})^n \]

Where:
- \( Ssf \) = System scaling factor, where a value of 1 is the recommended standard production deployment.
- \( \text{Required}_\text{AuthN}_\text{TPS} \) = The authentication throughput that the system is expected to handle (authentication transactions per second).
- \( \text{Required}_\text{Fed}_\text{AuthN}_\text{TPS} \) = The federated authentication throughput that the system is expected to handle (federated authentication transactions per second).
- \( \text{Required}_\text{Token}_\text{Operations}_\text{TPS} \) = The Security Token Service (STS) throughput that the system is expected to handle (STS transactions per second).
- \( \text{Required}_\text{AuthZ}_\text{TPS} \) = The authorization throughput that the system is expected to handle (authorization transactions per second).
- \( \text{Number}_\text{of}_\text{Resources} \) = The total number of OAM-protected resources.
- \( \text{Number}_\text{of}_\text{Policies} \) = The total number of OAM policies.
- \( u \) = % rate of increase in usage.
- \( n \) = time period of usage growth in years.

The sizing formula accommodates sizing for individual products as well as sizing for Oracle Access Management (Access Manager, Security Token Service, Identity Federation, Mobile and Social). 0 should be specified for the operational parameters that are not relevant for a deployment that only has a subset of the Oracle Access Management services. For example, if OIF is not planned to be deployed, specify 0 for the \( \text{Required}_\text{Fed}_\text{Authn}_\text{TPS} \) parameter. (Parameters for Oracle Mobile and Social will be provided at a later date.)

The Oracle Access Management platform uses an LDAP Directory to persist identity information. In addition, it relies on LDAP schema extensions to store password control and state information. However, this has minimal impact on LDAP sizing.

The Oracle Access Management platform uses a relational database system to persist policy information, e.g., access, authentication, token assurance policies, application policies, entitlements, security artifacts (credentials, keys), web access management sessions, and a transient state. The number of web access management user sessions impacts database sizing and scales linearly with the authentication and authorization throughput.

Oracle Access Management uses a relational database to persist audit information. Audit information sizing is dependent on the configured Audit Filter setting (NONE, LOW, MEDIUM or HIGH).
centralized audit database is required to store audit information generated by the integrated Oracle Access Management components. Assuming 30 days of audit data retention, a filter setting of MEDIUM requires 750MB of database storage. A filter setting of LOW requires 250 MB of database storage (Oracle Audit Vault cannot be used with Oracle Access Management products at this time).

To account for the differences in the performance of processor chipsets, the sizing calculator output must be adjusted by multiplying it with a processor chipset specific number.

\[
\text{Processor\_Specific\_Ssf} = \text{Ssf} \times \text{Chipset\_Core\_Factor}
\]

where Chipset\_Core\_Factor is defined by the Core Factor Table (described at the beginning of this document).

**Oracle Identity Federation Sizing Guidelines**

Oracle Access Manager 11gR2 supports the Service Provider (SP) side of federation. Identity Provider (IdP) functionality is available as part of the Oracle Fusion Middleware 11.1.1.6 release, it is not available as part of the Oracle Access Management 11gR2 release.

The following table summarizes sizing to support up to 3 million federation users for a single data-center. The production configuration should be duplicated for disaster recovery.

<table>
<thead>
<tr>
<th>COMPONENT / SETTINGS</th>
<th>DEVELOPMENT</th>
<th>PRE-PRODUCTION</th>
<th>PRODUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run-Time Server</td>
<td>1 Server - 2 Dual-Core CPUs 6 GB RAM</td>
<td>2 Servers – 4 Dual-Core CPUs 16 GB RAM each</td>
<td>3 Servers - 4 Dual-Core CPUs with 16 GB RAM each</td>
</tr>
</tbody>
</table>

Because Oracle Identity Federation is stateless, it only requires disk space for installation, configuration, and log files. Typically, the default disk drive that comes with a server is sufficient to meet OIF’s production requirements.

**Oracle Fedlet**

The Oracle Fedlet is a standalone, compact, easy to deploy SAML 2.0 service provider implementation. It includes a small software package and a simple file-based configuration, embeddable into an SP's Java or .NET application. The Fedlet establishes SSO between an IdP instance and the SP application without requiring a fully featured federation product on the SP side. The Fedlet can accept SAML 2.0 assertions from any SAML 2.0 IdP and retrieve user attributes to accomplish SSO and content personalization. The Fedlet can be downloaded as a separate ZIP file including all the components required to deploy the Fedlet with a Java or .NET SP application. To use the Fedlet, you are not required to install any other federation components on the SP side.

When sizing the Fedlet, base your calculations on the characteristics of the hardware running the Fedlet-enabled applications. The shared resources are used for processing both authentications performed by the Fedlet and operational actions performed by the application itself. For example, if a customer has 2 application instances in production deployment, with each application instance running on a 4 dual-core CPU server, the overall number of CPUs used by Fedlet will be 16 (4 x 2 x 2).
For OIF deployments with more than 3 million users, please consult Oracle Identity Management product management.

**Oracle Adaptive Access Manager Sizing Guidelines**

Oracle Adaptive Access Manager (OAAM) is designed to provide strong authentication and fraud detection. OAAM supports multiple layers of security including device fingerprinting, location intelligence, behavioral profiling, real-time risk analysis, and risk-based identity verification, interdiction and alerting.

Sizing Assumptions:

- The deployment handles up to 1 million end users with standard complexity (out of the box policies), strong authentication and knowledge-based authentication (KBA).
- The sizing guidelines are applicable for steady state load scenarios.
- The recommendations apply for a single data center. Multiple data centers need to be sized independently.
- It is recommended that the production configuration be set up for disaster recovery. This typically means that the production configuration is duplicated in a different location. Disaster recovery environments need to be sized separately.

The following table summarizes OAAM sizing.

<table>
<thead>
<tr>
<th>COMPONENT / SETTINGS</th>
<th>DEVELOPMENT</th>
<th>PRE-PRODUCTION</th>
<th>PRODUCTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Run-Time Server</td>
<td>All three components deployed on the same machine. 1 Server - 1 Quad-Core CPU 16 GB RAM Heap Size: 6 GB Storage: 5 GB</td>
<td>2 Servers - 4 Quad-Core CPUs 16 GB RAM each Heap Size: 8 GB</td>
<td>8 Servers - 4 Quad-Core CPUs with 16 GB RAM each Heap Size: 8 GB</td>
</tr>
<tr>
<td>Administration Server</td>
<td>1 Server - 2 Dual-Core CPUs with 16 GB RAM Heap Size: 4 GB</td>
<td>1 Server - 2 Dual-Core CPUs with 16 GB RAM Heap Size: 4 GB</td>
<td></td>
</tr>
<tr>
<td>Database Server</td>
<td>2 (RAC) Servers - 1 Dual-Core CPU with 16 GB RAM each Storage: 4KB per login session and 10 KB per policy object</td>
<td>2 (RAC) Servers – 1 Dual-Core CPU with 32 GB RAM each Storage: 3.3 TB</td>
<td></td>
</tr>
</tbody>
</table>

The following sizing formula is used for deployments greater than 1 million end users.

\[
Ssf = \left[ \frac{\text{Required Transaction}}{100} \right] \times \left( 1 + \frac{u}{100} \right)^n
\]

Where:

- \( Ssf = \) System scaling factor, with a value of 1 is recommended for standard production deployments.
• Required_Transaction = The transaction (login and application) throughput that the system is expected to handle per second.

• u = % rate of increase in usage.

• n = Time period of usage growth in years.

Database Sizing: OAAM uses a relational database to persist user and transactional information. Assuming 5 devices per user, 10 rules per login, 15 days or rule log retention, 20 customer calls per day, 100,000 alerts per data, 1,000,000 transactions per login per day, and 730 days of data archival, every 1 million users require 3.3 TB of database storage. Shared pool and SGA memory allocation should be at least 16 GB.

Oracle Enterprise Single Sign-On

Oracle Enterprise Single Sign-on Suite Plus (OESSO) allows users to login to enterprise applications using a single password to access any credential-protected application on the desktop, network, or Internet. In addition to SSO, OESSO offers a highly scalable enterprise infrastructure, including client-side Windows password reset, centralized user provisioning, support for kiosk environments, strong authentication, and comprehensive auditing. OESSO includes desktop components and requires LDAP directory storage for user, template, policy, and security related artifacts, and a relational database for reporting data.

Desktop Sizing: a Microsoft Windows system with 2 GB of RAM minimum.

Directory Sizing: An LDAP server is required for vGOConfig, vGOSecret, vGouserData, User Objects, Templates, Password Policies, Admin Overrides, Saved Credentials for an end user, and PM Instructions for a user. The recommended storage sizing is as follows:

Storage_in_MB = \#_of_Users * 1000 * (\#_of_Saved_Creds + \#_of_PM_Instructions_per_User)

Database Sizing: A database server is used to store data for reporting purposes. The recommended storage database sizing is as follows:

Storage_in_GB = \#_of_Users * \#_of_Transactions_per_User * 0.25 * 1000

Oracle Enterprise Gateway

Oracle Enterprise Gateway (OEG) is a security gateway typically deployed in the DMZ. Unlike other Oracle Access Management components, OEG is a Java application that doesn’t run in an application server but runs on the operating system directly.

A calculator (provided in a Microsoft Excel spreadsheet) available at https://stheehive.oracle.com/content/dav/st/IdM%20Evangelist%27s%20Workspace/Public%20Documents/OEG/OEG_Capacity_Planner.xls allows you to determine the following sizing and capacity planning requirements:

• Throughput per OEG instance (expressed in transactions per second) based on the size of the workload (e.g., body of a SOAP message), and processing parameters such as message encryption,
signature, XSD request validation, and XSLT transformation. If the resulting throughput is under
the customer’s requirement, another OEG instance will be necessary.

- Failover requirements based on the throughput per OEG instance both in production and non-
  production environments.

**Oracle Entitlement Server**

(Information for OES will be provided at a later time.)

**Oracle Access Management Components Co-Deployment**

To optimize the hardware resources used, some co-deployment may be possible based on the
following guidelines:

- Oracle Access Manager and Oracle Virtual Directory can be deployed on the same physical server in
cases where Oracle Virtual Directory is used primarily for Oracle Access Manager deployments.

- Oracle Access Manager and Oracle Adaptive Access Manager can be deployed on the same managed
server. When both products are co-deployed, it is expected that the steady state CPU load does not
exceed 50%. When deployed together, OAM and OAAM can share the same database provided
session overflow is minimal (this can be accomplished by increasing the Coherence cache).

- Oracle Access Management and Oracle Unified Directory can be deployed on the same physical
server, depending on the number of users and RAM to allow OUD to be able to cache user data.

- The entire Oracle Identity Management Suite can technically be deployed on the same physical
hardware with the following configuration / design considerations: Authentication throughput can
be reduced by increasing the idle or inactivity timeouts, authorization throughput can be reduced by
defining public and anonymous resources as excluded resources.

**Oracle Identity Governance**

Oracle Identity Governance includes Oracle Identity Manager (OIM), Oracle Identity Analytics (OIA),
and Oracle Privileged Accounts Manager (OPAM).

**Oracle Identity Manager**

Oracle Identity Manager (OIM) is a powerful and flexible enterprise identity management system that
automatically manages users' access privileges within enterprise IT resources. OIM is designed to
manage user access privileges across all of a company’s resources, throughout the entire identity
management lifecycle, from initial creation of access privileges to dynamically adapting to changes in
business requirements.

Sizing guidelines for OIM are based on the simplified deployment architecture provided in Figure 3.
The OIM sizing guidelines provided in this section assume that system configuration and
administration tasks are infrequent on the production servers. End-user traffic is expected to be high
(sizing is based on end-user operations).
From a sizing perspective the OIM server and the database are the most important components. OIM and SOA (required for OIM operation) should be installed in clustered deployments. Sizing consists in determining how much computational capacity is required for a specific installation to meet its usage. Capacity may be materialized using multiple physical servers, virtual servers, and clusters.

Other administrative processes part of an OIM deployment such as the Oracle WebLogic Server (WLS) administration console, Oracle Entitlement Server (OES), Oracle Enterprise Manager (EM), and Oracle Business Intelligence (BI) Publisher need to be sized separately based on their specific requirements and added to the overall OIM sizing.

Disaster recovery, high-availability, and peak load variation requirements are not considered in the baseline sizing guidelines described in this section. Disaster recovery typically means that the production configuration is duplicated in a different location. High availability can be configured with various levels of service assurance. Depending on acceptable response time and throughput requirements, the customer should decide how many additional nodes are required in the topology to support high availability.

Specific sizing guidelines are provided by a sizing calculator (Microsoft Excel spreadsheet) available at the following location:

https://stbeehive.oracle.com/content/dav/st/IdM%20Evangelist%27s%20Workspace/Public%20Documents/OIM/OIM11gR2_Sizing_Calculator.xlsx

Sizing Parameters

- **Number of active users**: This is the total number of users who are actively using OIM.

- **Number of screen transitions while using OIM**: End users of a business application normally interact with the OIM user interface (out-of-the-box or customized by the end-user). Depending on the business application usage, a logged-in end-user will navigate through a defined screen flow. Each time a screen is transitioned and rendered some operations are performed on the server side. This parameter defines the average number of OIM screens an active user interacts with. For example, if
a business application is designed only for user profile management and only password and self-registration screens are exposed, the average number of screens may be between 3 and 5. Conversely, if the application is designed for identity and account management, the user may use between 8 and 10 screens on average.

- **Think time per transition**: This is the average amount of time a user spends on understanding and filling in a form on the screen. This depends on the complexity of the screens and the familiarity of users with these screens. For an application designed only for identity management, the user may spend between 20 and 60 seconds on a screen and for an application designed for identity and account management, the user may spend between 30 and 90 seconds on a screen.

- **Response time for a screen transition**: This is the average response time of the frequently used screens in a business application, below 5 seconds on average. This parameter heavily depends on the level of customizations performed by the user on the OIM’s user interface, and on the server side. The lower the response time, the higher the number of active users that can be supported. A higher response time means that the resources are retained and consumed for a longer period of time for a single operation, and concurrent access to such operations adds up quickly.

- **Average number of major post-processing events**: This is the average number of post-processing event handlers executed as a result of user interface activities, e.g., accounts changes, access policy evaluations, and role membership evaluations.

- **Number of records to reconcile**: The total number of reconciliation records expected in each available reconciliation window. If an installation is expected to perform reconciliation on a continuous basis combined with hours of actual end-user transactions, the characteristics need to be determined through actual observations in a staging or QA environment.

- **Reconciliation time window**: The amount of time available to process reconciliation records.

- **Number of major post-processing steps per reconciliation record**: Most often trusted reconciliation is the determining factor as it can trigger access-policy-based provisioning. This factor can be determined by how many users are changed / created per day.

- **CPU load factor**: The load factor is the percentage of CPU usage acceptable under a steady load of transactions. The CPU load factor may be acceptable at higher level for off-normal-hour batch jobs, and reconciliation. During normal hours of operation, a lower CPU load factor is recommended for load surges in end-user transactions.

Other factors such as CPU used for each screen transition, CPU used for post-processing operations, database CPU used per operation, or the response time per screen transition or per backend operation can also have an effect on sizing. The current sizing guidelines are based on assumptions about these characteristics. These assumptions are based on lab observations (they are also stated in the associated spreadsheet calculator). These factors are heavily influenced by customizations. In addition, some installations may have to support use cases with a very high volume of self-service operations, or full user reconciliations that run very often.
Data Volume

Data volume is a key factor in sizing OIM deployments. As the number of users, roles, accounts and entitlements in the system grow, it influences response time and resource requirements. The effect on middle-tier processes (e.g., the OIM server) is not significant, the impact on the database is substantial. Sizing guidelines are based on following data volumes: 1 million users, 10K roles, 1 million entitlements, and 1,000 application instances.

Other relevant factors of data size growth are audit-level and reconciliation frequency (it is important to follow archival and/or purge recommendations for both). Please contact Oracle product management if the data volume expected is much larger than this baseline reference.

Processor Chipset Factor

The current sizing guidelines are based on an Intel Xeon CPU 51xx, 2.33 GHz, 2 * 2 CPU. To account for the differences in the performance of processor chipsets with different architectures, the sizing calculator output must be adjusted by factoring in the Processor Core Factor table (see beginning of this document).

Sample OIM Deployment Configurations

This section provides sample OIM deployment configurations and recommended values for certain sizing parameters to be used in the sizing calculator. For every pair of OIM and SOA managed servers displayed as OIMHOST (see Figure 3 above), the suggested configuration is 4 cores and 8 GB RAM available. The memory configuration assumed is: a) OIM with 2GB JVM max memory and 1GB perm allocation, b) SOA with 2GB JVM max memory and 1GB perm allocation, and c) 2GB spared for the operating system. The total amount of hardware required for a deployment may be materialized with multiple VMs, or multiple physical servers.

It is assumed that reconciliation is scheduled when business end-user traffic is low. If reconciliation runs in normal business hours (not recommended), you may want to add CPU power for end-user operations and reconciliation.

The calculator spreadsheet updates the number of records based on your input. It gives a perspective on how many changes you could expect over a period of time with such a consistent load. It also provides a level of verification for your assumptions.

Identity Management Only Installations

When a deployment is only addressing identity management use cases, there is less back-office processing for integrating with other applications. In this case, the number of screens used by a logged-in user will be limited to only user, role, and organization management, and there may be less reconciliation post-processing requirements. For such a deployment, follow the assumptions in the sizing calculator.

Sample sizing parameter values for initial assessment:

• Number of screen transitions = 5
• Think time = 30 seconds
• Response time = 5 seconds
• Number of post-processing operations = 2
• Amount of time available to process reconciliation records = 8 hours
• Number of major post-processing steps per record = 2
• CPU load factor = 60%

Lab observations used in assumptions (you can alternatively replace these assumptions with your test environment observations):
• Backend operation response time = 3 seconds
• % CPU used per screen rendering = 7
• % CPU used per post-processing calculation = 7
• % database CPU per operation = 5

Identity Management and Provisioning Installations

A deployment addressing both identity management and provisioning use cases must support more back-office processing to integrate with other applications, and the number of screens used by a logged-in depends on the target system types involved. For such a deployment, follow the assumptions in the sizing calculator.

Sample sizing parameter values for initial assessment:
• Number of screen transitions = 5
• Think time = 45 seconds
• Response time = 5 seconds
• Number of post processing ops = 3
• Amount of time available to process reconciliation records = 8 hours
• Number of major post-processing steps per record = 2
• CPU load factor = 60%

Lab observations used in assumptions (you can alternatively replace these assumptions with your test environment observations):
• Backend operation response time = 10 seconds
• % CPU used per screen rendering = 7
• % CPU used per post-processing calculation = 7
• % database CPU per operation = 5

Very Large Deployments

The current sizing guidelines use a linear model based on lab test results to calculate the hardware requirements. However, when you have a very large deployment, this linear model may not work. As the size and complexity of a deployment grows, the software and operation system may not scale as linearly. Installations with multi-million users or a very high number of active users should be considered as a large deployment.

CPU usage is mostly a factor of the number of operations performed in the system. An installation may need special considerations if it expects very high concurrency, very complex pre-/post-processing logic, or very high frequency / volume of reconciliation events.

This type of deployment can be sized by running performance tests and derive recommendations from them.

Oracle Identity Analytics

Oracle Identity Analytics (OIA) is a component that provides a comprehensive role lifecycle management and identity compliance solution enabling companies to proactively enforce internal security control policies and automate critical identity management processes. Three deployment scenarios are considered, small, medium, and large, and recommendations for each type are provided.

The current sizing guidelines assume a highly available environment, database best practices for high availability, backup and recovery. Load balancing is not factored into the sizing guidelines.

Architecture Overview

OIA is a multi-tiered Java Enterprise Edition (EE) web application. The division of tiers allows OIA to scale according to customers’ performance demands. The main OIA tiers are:

• Presentation tier: A web server layer rendering JSPs, JavaScript, XML to present a user interface accessible through various supported web browsers.

• Logic tier: A Java EE application server forms the middle tier where all business logic of OIA is implemented.

• Data tier: The data tier usually consists of a standalone or clustered relational database environment using Java Database Connectivity (JDBC) to integrate with the logic tier.

Typical OIA deployments include the following components:

• Load-balanced clustered web servers deployed in the DMZ. End users and administrators interact with OIA through these web servers.

• Clustered application servers running OIA in the application tier.
• OIA uses a relational database as its data repository. Depending on the dataset size, the database server can be standalone or clustered. For optimized performance, the application servers and relational database servers can be co-located, for example within the same subnet.

• OIA integrates with identity management systems such as Oracle Identity Manager and Oracle Access Manager.

• OIA uses flat files from target systems such as RACF, Microsoft Active Directory, and ACF2 to build its Identity Warehouse. Typically, the target systems drop flat files on a shared location using SFTP, which is subsequently imported using OIA’s import process. Such target systems are classified as “unmanaged resources.”

Deployment Considerations

OIA performance depends on the response characteristics of each tier discussed in the previous section.

OIA Web Client: The number of concurrent users accessing the system directly affects the web client performance. Performance is also affected by the activities being performed within each user session, i.e., role provisioning, attestation, SoD monitoring, reporting, and dashboarding. Concurrent users and their system activities largely affect CPU and memory requirements of the application server.

OIA Server: Following are some areas of server operation that need to be considered during OIA sizing.

• OIA Import Process: Import jobs are created to populate the OIA’s Identity Warehouse. Data can be imported from a text file or by using direct connections to provisioning systems, in particular Oracle Identity Manager. OIA inserts or updates data in the warehouse and archives all of the data feeds. Importing a large data set can impose resource constraints on the application server, e.g., CPU and memory usage, and the database, e.g., an increase of the table-space size containing OIA’s repository.

• OIA Identity Certification: Identity certification is the process of reviewing user entitlements to ensure that users have not acquired entitlements that they are not authorized to have. Certifications can be scheduled to run on a regular basis to meet compliance requirements. Managers use the Identity Certification module to review their employees’ entitlements to access applications and data. Based on changes reported by OIA, managers can authorize or revoke employee access, as needed. Attestation of a data set of large user entitlements can affect OIA performance caused by resource constraints on the application server and database.

• OIA Identity Audit Process: The Identity Audit module is designed to detect SoD violations. An SoD violation happens when a user account, a user attribute, or a role has been assigned two entitlements that should not be held in combination. While the identity certification module enables managers to certify or revoke access of users, the Identity Audit module has a detection mechanism that monitors users' actual access to resources and captures any violations on a continuous basis.

Deployment Types

OIA deployments can be small, medium, and large as described in the table below.
### Sizing Per Deployment Type

For a medium sized deployment, the application server is clustered. The clustered nodes can exist on the same physical machine as separate node deployments when a high-end machine is used for the application server. A load balancing router can be used to load balance between the nodes for optimal performance.

A large deployment involves a high system load due to large datasets, heavy processing, and a large number of users. It is recommended to add a dedicated clustered web server and a clustered database server, such as Oracle RAC Database. Due to intense computations such as identity certifications, a large JVM heap is highly recommended. Horizontally scaling out by adding more nodes can address increased performance requirements. It is not necessary to have application servers on different machines, multiple nodes with OIA can be deployed on the same physical machine, assuming that the machine is a high-end one and has adequate physical memory and CPU.

The following tables define hardware configurations based on the sizing metrics outlined in the previous section and on actual customer deployments, for the application server and database server tiers.

#### Application Server Configuration

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>SMALL DEPLOYMENT</th>
<th>MEDIUM DEPLOYMENT</th>
<th>LARGE DEPLOYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 Quad-Core, 2.6 GHz</td>
<td>1 Quad-Core, 2.6 GHz</td>
<td>2 Quad-Core, 2.6 GHz</td>
</tr>
<tr>
<td>JCM heap size</td>
<td>2 GB per node</td>
<td>4 GB per node</td>
<td>8 GB per node</td>
</tr>
</tbody>
</table>

#### Database Server Configuration

<table>
<thead>
<tr>
<th>PARAMETER</th>
<th>SMALL DEPLOYMENT</th>
<th>MEDIUM DEPLOYMENT</th>
<th>LARGE DEPLOYMENT</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU</td>
<td>1 Quad-Core, 2.6 GHz</td>
<td>1 Quad-Core, 2.6 GHz</td>
<td>2 Quad-Core, 2.6 GHz</td>
</tr>
<tr>
<td>RAM</td>
<td>2 GB per node</td>
<td>4 GB per node</td>
<td>8 GB per node</td>
</tr>
<tr>
<td>Total SGA size (for Oracle Database)</td>
<td>1 GB</td>
<td>2 GB+</td>
<td>4 GB+</td>
</tr>
<tr>
<td>Open Cursors (for Oracle Database)</td>
<td>300</td>
<td>500</td>
<td>1,500+</td>
</tr>
</tbody>
</table>
OIA Database Size Calculation

The following steps are used to estimate OIA database size requirements for an Oracle Database Server.

**Account Objects:** To calculate the number of account objects, substitute the corresponding values into the following formula:

\[ \text{Total Account Objects} = \text{Number of Resource Types} \times \text{Number of Resources} \times \text{Accounts per Resources} \]

**Policy Objects:** To calculate the number of policy objects, substitute the corresponding values into the following formula (each policy version is an object, add the number of policy versions for the calculation of policy objects):

\[ \text{Total Policy Objects} = \text{Number of Resource Types} \times \text{Number of Resources} \times \text{Policies per Resources} \]

**Total Number of Objects:** To calculate the total number of objects, apply the following formula (each role version is an object, add the number of role versions for the calculation of role objects):

\[ \text{Total Number of Objects} = \text{Global User Objects} + \text{Total Account Objects} + \text{Total Policy Objects} + \text{Total Role Objects} + \text{Total Request Objects} \]

**Database Disk Space:** Objects are typically 120 KB in size, each report and certification is about 4 MB of data, and each identity audit (SoD) violation is about 500 KB in size. To calculate the approximate object disk space, substitute the corresponding values into the following formula:

\[ \text{Approximate Object Disk Space} = \text{Total Number of Objects} \times \text{Size Per Object} \]

\[ \text{Total Database Size} = \text{Approximate Object Disk Space} + (\text{Number of Certifications Annually} \times \text{Size per Report}) + (\text{Number of Reports Annually} \times \text{Size per Report}) + (\text{Average Number of SoD Violations} \times \text{Size per Violation}) \]

As the number of accounts per user grows, the disk space increases exponentially. The space required depends on the number of global users, number of accounts per user, number of resource types and resources.

If the Oracle Database server is used as OIA’s data repository, the automated snapshots using journaling and checkpoint systems add extra hard disk space requirements. Such data recovery constraints must also be factored into the database hard disk free-space requirements when sizing an OIA implementation.
Oracle Privileged Account Manager

Oracle Privileged Account Manager (OPAM) is a server-based password repository designed to generate, provision, and manage passwords for privileged users accessing specific resources. OPAM’s users are database administrators, operating systems root users, and application administrators. OPAM performs mission critical services in the IT deployment it manages; as such it needs to be able to service all requests in a reliable and timely manner.

Figure 4: OPAM High-Availability Topology

The current OPAM sizing guidelines assume the following deployment parameters:

- 100 concurrent sessions (peak load). The expected concurrent load is constrained by the number of administrators in the organization. This parameter drives the memory and processing power requirements on the machines running OPAM.

- 1,000 privileged accounts (10 grants per account) under management. This assumes a sufficiently large environment where deploying OPAM would have tangible benefits to the organization. This parameter drives the disk space requirements on the machines running the relational database server.

- High availability by default. Since OPAM is primarily used by administrators and empowers critical administration tasks (i.e., being able to login to mission critical target systems), OPAM should always be deployed in a high availability configuration. This parameter drives the deployment topology recommendation.

Recommended Topology

Based on the above assumptions we recommend the following highly available deployment topology. OPAM is deployed in an active-active configuration as part of an Oracle Weblogic Server cluster in a single domain (See Figure 4 above).
Hardware Requirements

<table>
<thead>
<tr>
<th>OPAM</th>
<th>RELATIONAL DATABASE SERVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Two OPAMHOSTs with one Dual-Core CPU each and 8GB RAM each.</td>
<td>One relational database server (minimal) with one Dual-Core CPU, 6 GB RAM, 2 GB disk space (RAC is recommended).</td>
</tr>
</tbody>
</table>

Data Sizing

OPAM stores its data in the OPSS Policy Store. The OPSS Policy Store uses the relational database to store its data and the disk footprint for OPAM-specific data has the following characteristics: 1,000 Privileged Accounts = 30 Megabytes of data; 1,000 Grants = 85 Megabytes of data.

An individual deployment can be sized for disk space based on multiples of the above. Sufficient disk space for the OPAM-specific data must be accounted for in addition to the basic footprint of the OPSS Policy Store when sizing the disk space for the relational database node.

Typical Customer Deployments

(To be provided at a later time.)

Conclusion

This self-contained, single format white paper provides capacity planning and sizing guidelines for Oracle Identity Management 11gR2 components and services.

In addition to this document, Enterprise Solutions Group (ESG) is putting together an online identity management sizing tool to be hosted at http://sizingtool.us.oracle.oracle.com/, originally designed to support the following Oracle Identity Management 11gR2 components: Oracle Directory Services, OAM, OAAM, OIF, and OIM. Other components will be supported at a later date.

For specific sizing requirements outside the scope of this document, please contact Oracle Identity Management product management or the author of this document directly at marc.chanliau@oracle.com.