

Management Pack Plus for Identity Management

Oracle® Enterprise Manager 11g Grid Control Release 1
(11.1.0.1.0)

Getting Started Guide

ORACLE®

Contents

Management Pack Plus for Identity Management	4
<i>Introduction to the Management Pack Plus for Identity Management</i>	4
Functional Overview.....	4
Monitored Targets.....	6
Additional Sources of Information	10
System Requirements.....	12
Installing Oracle Enterprise Manager Grid Control 11g Release 1	14
Prerequisites for Discovering Oracle Identity Management Targets in Enterprise Manager	14
<i>Discovering & Configuring Oracle Identity Management Targets</i>	20
Discovering Oracle Access Manager Access Server 10.1.4.2, 10.1.4.3.0.....	20
Discovering Oracle Access Manager Identity Server 10.1.4.2, 10.1.4.3.0	23
Discovering Oracle Identity Federation Server 10.1.4.2, 10.1.4.3.0	27
Discovering Oracle Identity Manager Server 9.1.0.1.....	29
Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0	30
Discovering Oracle Identity Management 11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0) and Oracle Identity and Access Management 11g (11.1.1.3.0)	32
Discovering Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g	34
Collecting User Statistics for Oracle Internet Directory	35
Creating Identity and Access System.....	37
Creating Generic Service or Web Application Targets for Identity Management.....	39
Creating a Service Dashboard Report.....	44
Updating Monitoring Configuration for Individual Identity Management Targets	45
Adding or Removing Targets from the System Topology.....	45
Removing Servers or Components from an Existing Identity Management Topology	45
<i>Performance Management and Diagnostics</i>	46
Monitoring Basics	46
Monitoring Templates	53
User-Defined Metrics	53
Real-Time Performance Charts.....	54
<i>Configuration Management</i>	54
Viewing Configurations	55
Comparing Configurations.....	56
Configuration History	56
<i>Service Level Management</i>	57
Service Tests and Beacons.....	57
Performance and Usage	60
Availability	61
Service-Level Rules	61

Topology View	62
Service Performance	62
Reports	63
<i>Oracle Identity Management Performance Metrics.....</i>	<i>64</i>
Access Manager – Access Server 10g	65
Access Manager – Identity Server 10g	67
Identity Manager Server 9.1.x	69
Identity Manager Repository 9.1.x	70
Identity Federation Server 10g.....	71
Oracle Internet Directory 11g.....	75
Directory Integration Platform Server 11g.....	79
Oracle Virtual Directory 11g.....	81
Identify Federation Server 11g.....	83
Oracle Adaptive Access Manager Server 11g.....	86
Oracle Adaptive Access Manager Cluster 11g.....	90
Oracle Access Manager Server 11g	90
Oracle Access Manager Cluster 11g	93
Oracle Identity Manager Server 11g	95
Oracle Identity Manager Cluster 11g	99
Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g	100
<i>Troubleshooting the Management Pack Plus for Identity Management</i>	<i>100</i>
Failure to Discover Oracle Access Manager, Oracle Identity Manager or Oracle Identity Federation	100
What OS User Privileges required for Windows Host Preferred Credentials	101
Certain Metrics Are Not Collected	101
The Status of Certain Components in Enterprise Manager Differs from the Status of the Same Components in the Windows Services Panel	102
Internet Explorer Crashes When Trying to Perform Multiple Recording Transactions for the Same Application.....	102
How to enable Browser Simulation on Windows XP beacon?	103
<i>Title and Copyright Information</i>	<i>104</i>

Management Pack Plus for Identity Management
Oracle Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0)
Getting Started Guide
February 2011

This document provides a brief introduction to the Management Pack Plus for Identity Management. It guides you through the process of discovering and configuring Oracle Identity Management targets and discusses key features in the Management Pack Plus for Identity Management. It covers the following sections:

- [Introduction to the Management Pack Plus for Identity Management](#)
- [Discovering & Configuring Oracle Identity Management Targets](#)
- [Performance Management and Diagnostics](#)
- [Configuration Management](#)
- [Service Level Management](#)
- [Oracle Identity Management Performance Metrics](#)
- [Troubleshooting the Management Pack Plus for Identity Management](#)

Introduction to the Management Pack Plus for Identity Management

This section covers the following topics:

- [Functional Overview](#)
- [Monitored Targets](#)
- [Additional Sources of Information](#)
- [System Requirements](#)
- [Installing Oracle Enterprise Manager Grid Control 10g Release 1](#)
- [Prerequisites for Discovering Oracle Identity Management Targets in Enterprise Manager](#)

Functional Overview

As more and more businesses rely on the Oracle Identity and Access Management Suite to control access to their mission-critical applications (both packaged applications and custom-built web applications) and to provision resources across their organizations, the need to achieve predictable performance and availability for Oracle Identity Management systems has become a top priority for many businesses. An outage or slow performance in access and identity services, for instance, can have negative impacts on the business bottom-line as end-users are unable to log in to mission-critical applications. To help you maximize the value of Oracle Identity Management systems, and to deliver a superior ownership experience while keeping a lid on the systems management costs, Oracle provides Oracle Management Pack Plus for Identity Management (the Identity Management Pack), which leverages Oracle Enterprise Manager Grid Control's advanced management capabilities, to provide an integrated and top-down solution for your Oracle Identity Management environment.

NEW FEATURES

- New enterprise-wide view of Oracle Identity Management
 - A new “Identity and Access” page provides a centralized view of all Oracle Identity Management components – including Identity Management 10g and Identity Management 11g components.
 - From the “Identity and Access” page, users can discover Identity Management components, create systems and services based on the underlying dependencies and monitor the overall health of the Identity Management environment
- Performance Management
 - Performance monitoring for Identity Management 11g components – including Oracle Internet Directory, Oracle Virtual Directory, Directory Integration Platform, Oracle Identity Federation, Oracle Access Manager, Oracle Adaptive Access Manager, and Oracle Identity Manager.
 - A wide range of out-of-box performance metrics to find root causes of problems that could potentially slow performance, extend response times, or create outages
 - Customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts
 - Drill down into usage and performance statistics for:
 - **Oracle Identity Federation Providers** – showing authentication requests and responses, HTTP and SOAP requests and responses, and authentication response processing time
 - **Oracle Internet Directory User Statistics** – showing failed and completed LDAP operations like Add/Bind/Compare/Delete/Modify/Search
 - **Directory Integration Platform Synchronization and Provisioning Profiles** – showing job status, successful/skipped/failed changes, completion time, and errors
 - **Oracle Identity Manager Adapters**—showing completed executions and average/maximum/minimum execution time
 - **Oracle Access Manager Clients and Domains**—showing authentication and authorization frequency, latency and success to fail ratio
- Configuration Management
 - Perform key configuration management tasks like keeping track of configuration changes for diagnostic and regulatory purposes, taking snapshots to store configurations, and comparing component configurations to ensure consistency of configurations within the same environment or across different environments.
- Enhanced Interface for Managing Fusion Middleware
 - ADF-based interface
 - Navigation tree on left controls details displayed on right
 - Customize home page views via drag and drop of regions

- o Context sensitive menus
- o In-context drilldowns to Fusion Middleware Control and WebLogic Server Administration Console

BENEFITS

- A centralized systems management solution to efficiently manage multiple Oracle Identity Management deployments including testing, staging, and production environments from a single console
- Gain the ability to monitor a wide range of performance metrics for all critical Identity Management components to find root causes of problems that could potentially slow performance or create outages
- Automated configuration management to accelerate problem resolution
- Record synthetic Web transactions (or service tests) to monitor Identity Management Service availability and analyze end user response times
- Define Service Level Objectives (SLO's) in terms of out-of-box system-level metrics as well as end user experience metrics to accurately monitor and report on Service Level Agreement (SLA) compliance.

Monitored Targets

The monitored targets in the Management Pack Plus for Identity Management are summarized in [Table 1](#).

Table 1 Licensed Targets in Management Pack Plus for Identity Management

Enterprise Manager Target Type	Purpose
Oracle Identity Management 10g Targets	
Access Manager - Access Server	Representation of Oracle Access Manager – Access Server providing access to metrics, alerts, charts, and configuration management.
Access Manager - Identity Server	Representation of Oracle Access Manager – Identity Server providing access to metrics, alerts, charts, and configuration management.
Access Manager - Access System	System target modeled with Oracle Access Manager – Access Server(s), LDAP Server(s), Database Instance(s) and the underlying hosts as the key components providing an end-to-end system oriented view of the monitored Oracle Access Manager – Access System targets. The Access Manager – Access System target provides access to metrics, alerts, charts, and topology view.
Access Manager - Identity System	System target modeled with Oracle Access Manager – Identity Server(s), LDAP Server(s), Database Instance(s) and the underlying hosts as the key components

Enterprise Manager Target Type	Purpose
	providing an end-to-end system oriented view of the monitored Oracle Access Manager – Identity System targets. The Access Manager – Identity System target provides access to metrics, alerts, charts, and topology view.
Identity Federation Server	Representation of Oracle Identity Federation Server providing access to metrics, alerts, charts, and customized reports.
Identity Federation System	System target modeled with Oracle Identity Federation Server(s), LDAP Server(s), Database Instance(s), Oracle HTTP Server(s), OC4J and the underlying hosts as the key components providing an end-to-end system oriented view of the monitored Oracle Identity Federation System targets. The Identity Federation System target provides access to metrics, alerts, charts, and topology view.
Identity Manager Server	Representation of Oracle Identity Manager Server providing access to metrics, alerts, charts, and customized reports.
Identity Manager Repository	Representation of Oracle Identity Manager Repository providing access to metrics, alerts, charts, and customized reports.
Identity Manager System	System target modeled with Oracle Identity Manager Server(s), Oracle Identity Manager Repository, Database Instance(s), Application Server(s) – (e.g. JBoss Application Server and Oracle Weblogic Server), and the underlying hosts as the key components providing an end-to-end system oriented view of the monitored Oracle Identity Manager System targets. The Identity Manager System target provides access to metrics, alerts, charts, and topology view.
Delegated Administration Server	Representation of Delegated Administration Server providing access to metrics, alerts, charts, and customized reports.
Directory Integration Platform Server	Representation of Directory Integration Platform Server providing access to metrics, alerts, charts, and customized reports.
Oracle Internet Directory	Representation of Oracle Internet Directory providing access to metrics, alerts, charts, and customized reports.
Single Sign-On Server	Representation of Single Sign-On Server providing access to metrics, alerts, charts, and customized

Enterprise Manager Target Type	Purpose
	reports.
Oracle Identity Management 11g Targets	
Oracle Internet Directory	Representation of Oracle Internet Directory providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, customized reports, and drilldown into user statistics showing failed and completed LDAP operations like Add/Bind/Compare/Delete/Modify/Search.
Identity Federation Server	Representation of Identity Federation Server providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, customized reports, and drilldown into Identity Federation Providers – showing authentication requests and responses, HTTP and SOAP requests and responses, and authentication response processing time.
Directory Integration Platform Server	Representation of Directory Integration Platform Server providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, customized reports, and drilldown into Directory Integration Platform Synchronization and Provisioning Profiles – showing job status, successful/skipped/failed changes, completion time, and errors.
Oracle Virtual Directory	Representation of Oracle Virtual Directory providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, and customized reports.

Enterprise Manager Target Type	Purpose
Oracle Access Manager Cluster	Representation of Oracle Access Manager Cluster providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, and customized reports.
Oracle Access Manager	Representation of Oracle Access Manager Server providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, customized reports, and drilldown into Oracle Access Manager Clients and Domains showing authentication and authorization frequency, latency and success to fail ratio.
Oracle Identity Manager Cluster	Representation of Oracle Identity Manager Cluster providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, and customized reports.
Oracle Identity Manager	Representation of Oracle Identity Manager Server providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, customized reports, and drilldown into Oracle Identity Manager Adapters—showing completed executions and average/maximum/minimum execution time.
Oracle Adaptive Access Manager Cluster	Representation of Oracle Adaptive Access Manager Cluster providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, and

Enterprise Manager Target Type	Purpose
	customized reports.
Oracle Adaptive Access Manager	Representation of Oracle Adaptive Access Manager Server providing ADF-based interface with access to a navigation tree, context sensitive menus, drilldowns to Fusion Middleware Control and WebLogic Server Administration Console, customizable performance summaries with a “Metric Palette” that allows users to drag and drop performance charts, metrics, alerts, and customized reports.
Identity and Access System	System target that can be modeled with any discovered Oracle Identity Management target (including both Identity Management 10g and Identity Management 11g targets) and the underlying hosts, databases and LDAP servers as the key components providing an end-to-end system oriented view of the monitored Identity Management environment. The Identity and Access System target provides access to metrics, alerts, charts, and topology view.
<u>Targets associated with both Identity Management 11g and Identity Management 11g targets</u>	
Generic Service	With the Management Pack Plus for Identity Management, users can create targets of type Generic Service associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, Identity Manager System, and Identity and Access System. The Generic Service target provides an end-to-end service oriented view of the monitored Oracle Identity Management targets with access to performance and usage metrics, service tests, service level rules, service availability definition, alerts, charts, and topology view.
Host	Representation of hosts running Oracle Identity Management components providing access to metrics, alerts, performance charts, remote file editor, log file alerts, user-defined metrics, host commands and customized reports.

Additional Sources of Information

Refer to the documentation listed in [Table 2](#) for additional information about the Management Pack Plus for Identity Management. Because the pack leverages many of Enterprise Manager's underlying capabilities, the base documentation is applicable in many cases.

Table 2 Additional Documentation for the Management Pack Plus for Identity Management

Book	Chapter	Information
<i>Enterprise Manager Concepts Guide</i> http://download.oracle.com/docs/cd/E11857_01/em.111/e11982/toc.htm	All	Overall information on the capabilities of Oracle Enterprise Manager Grid Control
	Identity Management	Monitoring Oracle Identity Management targets and creating/configuring associated services.
	Service Management	Defining Service Level Objective, Running Service Level Reports
	Enterprise Configuration Management	Viewing Configurations, Comparing Configurations, Taking Configuration Snapshots, Using Configuration Policy
<i>Enterprise Manager Grid Control Basic Installation Guide</i> http://download.oracle.com/docs/cd/E11857_01/install.111/e15838/toc.htm	All	Installing Enterprise Manager Grid Control Server and Agents
<i>Enterprise Manager Grid Control Advanced Installation and Configuration Guide</i> http://download.oracle.com/docs/cd/E11857_01/install.111/e16847/toc.htm	All	Advanced Configuration Topics
<i>System Monitoring Plug-in for Oracle</i>	All	The System Monitoring Plug-in for Oracle Directory Server Enterprise Edition is available

Book	Chapter	Information
<i>Directory Server Enterprise Edition Installation Guide</i> http://download.oracle.com/otn/java/oem/ODSEE_EMPI_documentation_v1.0.pdf		for Oracle Enterprise Manager Grid Control 10.2.0.x as well as 11.1. This plug-in is part of the Management Pack Plus for Identity Management license allowing you to discover and monitor Oracle Directory Server Enterprise Edition.

You may also get more information about the product on Oracle Technology Network (OTN) forums and tutorials area for Enterprise Manager. Information will be posted on OTN when available. A copy of the Enterprise Manager documentation set is also available on OTN as well. URL to the site is: <http://www.oracle.com/technology>.

System Requirements

Refer to [Table 3](#) for a list of supported Oracle Identity Management products in the Management Pack Plus for Identity Management in Enterprise Manager Grid Control 11g Release 1 (11.1.0.1.0). Please check Enterprise Manager's certification matrix on My Oracle Support for a list of supported platforms.

Table 3 Supported Oracle Identity Management Products and Platforms in the Management Pack Plus for Identity Management in Enterprise Manager Grid Control 11g Release 1 (11.1.0.1.0)

Product	Version	Application Server	Directory Server/ Database
Oracle Access Manager	10.1.4.2, 10.1.4.3.0	N/A	Oracle Internet Directory 10.1.4.x, Microsoft Active Directory
Oracle Identity Federation	10.1.4.2, 10.1.4.3.0	Oracle Application Server 10g	Oracle Internet Directory 10.1.4.x
	11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0)	Oracle WebLogic Server 10.3	Oracle Internet Directory 11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0)

Product		Version	Application Server	Directory Server/ Database
Oracle Identity Manager		9.1.0.1	Oracle WebLogic Server 10.3, JBoss Application Server	Oracle Database
Oracle Identity Management Suite	Oracle Internet Directory	10.1.4.2, 10.1.4.3.0	Oracle Application Server 10g	Oracle Database
	Single Sign-On Server			
	Delegated Administration Services			
	Directory Integration Platform			
Oracle Internet Directory		11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0)	Oracle WebLogic Server 10.3	Oracle Database
Directory Integration Platform		11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0)	Oracle WebLogic Server 10.3	Oracle Database
Oracle Virtual Directory		11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0)	Oracle WebLogic Server 10.3	N/A
Oracle Access Manager		11g (11.1.1.3.0)	Oracle WebLogic Server 10.3	Oracle Database
Oracle Adaptive Access Manager		11g (11.1.1.3.0)	Oracle WebLogic Server 10.3	Oracle Database
Oracle Identity Manager		11g (11.1.1.3.0)	Oracle WebLogic Server 10.3, Oracle SOA Suite 11.1.1.3.0	Oracle Database

Product	Version	Application Server	Directory Server/ Database
Oracle Directory Server Enterprise Edition	6.x, 7.x, 11g (11.1.1.3.0)	N/A	N/A

Installing Oracle Enterprise Manager Grid Control 11g Release 1

Before you begin configuring Grid Control 11g Release 1 (11.1.0.1.0) to manage your Identity Management components, you must install and configure Grid Control 11g Release 1 (11.1.0.1.0) on at least one host computer on your network. Oracle recommends that you install Grid Control on dedicated host(s). For example, if the Identity Management components are installed on host1.us.oracle.com, then install and configure the Oracle Management Service and Oracle Management Repository on host2.us.oracle.com. Install the Grid Control 11g Management Agent on every host that includes the components you want to manage with Grid Control.

See Also:

Oracle Enterprise Manager Grid Control Basic Installation Guide 11g Release 1 (11.1.0.1.0)

All installation files can be accessed on Oracle's OTN website:

<http://www.oracle.com/technology/software/products/oem/index.html>

Prerequisites for Discovering Oracle Identity Management Targets in Enterprise Manager

Before you start monitoring Oracle Identity Management targets in Enterprise Manager, you must perform the following tasks:

- Install the Enterprise Manager Grid Control 11g Release 1 (11.1.0.1.0)

The information required to perform these steps is available in the *Oracle Enterprise Manager Grid Control Basic Installation Guide 11g Release 1 (11.1.0.1.0)*

http://download.oracle.com/docs/cd/E11857_01/install.111/e15838/toc.htm

- Install Grid Control 11g Release 1 (11.1.0.1.0) Agent on each of the hosts that run Oracle Identity Management components.

If you would like to monitor additional targets, such as Oracle Application Server, Oracle Weblogic Server, JBoss Application Server, MS Active Directory, MS IIS and databases supporting Oracle Identity Management, and you have the proper license for monitoring

these targets, then install Grid Control 11g Release 1 (11.1.0.1.0) Agent on these hosts as well.

- After Enterprise Manager Grid Control OMS and Agents are installed, please complete the following steps before initiating the discovery process:

Oracle Access Manager 10.1.4.2, 10.1.4.3.0

1. Install Oracle Access Manager SNMP Agent on each of the hosts where Oracle Access Manager's Access Server and Identity Server are running. The SNMP Agent collects performance metrics and configuration parameters for Oracle Access Manager's Access Server and Identity Server allowing you to monitor the various Oracle Access Manager components through Enterprise Manager Grid Control. Refer to the Oracle Access Manager Installation Guide for instructions on installing the SNMP Agent (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/snmp.htm#CHDFBJJC).
2. Configure the SNMP Agent and specify the Agent's UDP and TCP Ports as well as the SNMP Agent Community Name. Make sure that you record the SNMP Agent UDP Port and Community Name – as these details will be needed in the discovery process. Refer to the Oracle Access Manager Installation Guide for instructions on configuring the SNMP Agent (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/snmp.htm#CEGEIIFI). Also, refer to the Oracle Access Manager Identity and Common Administration Guide for instructions on setting up the SNMP Agent (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25343/snmpmtr.htm#CEGHHDBC).
3. Enable SNMP monitoring for both the Oracle Access Manager Access Server and Oracle Access Manager Identity Server by completing the following tasks:
 - From the Identity (or Access) System Console, select System Configuration, Identity Server (or Access Server).
 - Click a link for a particular server.
 - Select the Modify button to display the page where you can turn SNMP monitoring on or off. Select the SNMP State On button at the bottom of the page to turn on the collection of SNMP statistics.
 - In the SNMP Agent Registration Port field, enter the port number to define or change the port on which the SNMP Agent listens.
 - Restart the Identity Server (or Access Server).

ORACLE Identity Administration

User Manager Group Manager

System Configuration | User Manager Configuration | Group Manager Configuration | Org Manager Configuration | Common Configuration

- Password Policy
- Lost Password Policy
- Directory Profiles
- Identity Servers**
- WebPass
- Server Settings
- Diagnostics
- Administrators
- Styles
- Photos

Group File Name: /oblix/logs/uebugfile.lst

Transport Security* ☒ Open ☐ Simple ☐ Cert

Maximum Session Time (hours)*: 24

Number of Threads*: 20

Audit to Database Flag (auditing on/off) ☒ Off ☐ On

Audit to File Flag (auditing on/off) ☒ Off ☐ On

Audit File Name:

Audit File Maximum Size (bytes): 100000

Audit File Rotation Interval (seconds): 7200

Audit Buffer Maximum Size (bytes): 25000

Audit Buffer Flush Interval (seconds): 7200

Log Threshold: Warning and above

Log Handler Definitions

Name	Log Level	Output To
☐ LogFatal2Sys	Fatal	System Log
☐ LogAll2File	All Log Levels	File

Add Delete

Scope File Name*: /oblix/logs/scopefile.lst

SNMP State* ☐ Off ☒ On

SNMP Agent Registration Port*: 6162

Note: If you change the fields marked with an Asterisk(*), you must restart this Identity Server.

Save Cancel

Refer the Oracle Access Manager Identity and Common Administration Guide for instructions on setting up the SNMP Agent

(http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25343/snmpmntr.htm#BABFFDDA).

- Complete **all** the configuration steps for the Oracle Access Manager Identity Server and Oracle Access Manager Access Server. Make sure that the communication details and the directory server details are defined so that Enterprise Manager can discover the topology of your Oracle Access Manager environment. Refer to the Oracle Access Manager Installation Guide for instructions on configuring the Identity Server (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/id_setup.htm#CHDHIBIB) and the Access Server (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/assvr.htm#BGBEFBBD).
- If you plan to monitor the Directory Server through Oracle Enterprise Manager Grid Control, then make sure that the directory server is appropriately discovered in Enterprise Manager before moving on to the discovery of Oracle Access Manager Identity Server and Oracle Access Manager Access Server. Complete the following tasks to discover the supported directory servers:
 - Oracle Internet Directory 10.1.4:** Discovery of Oracle Identity Management Suite 10g (including Oracle Internet Directory, Directory

Integration Platform, Delegated Administration Server, and Single Sign-On Server) can be done using the discovery wizard on the Identity and Access page. From the *Identity and Access* page, select “*Identity Management 10g (OID, DAS, DIP, SSO)*” from the *Add* drop-down menu. For more information, please refer to the [Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0](#) section.

- **Microsoft Active Directory:** Download and install Oracle System Monitoring Plug-in for Microsoft Active Directory from OTN: (<http://www.oracle.com/technology/software/products/oem/htdocs/system-monitoring-connectors.html>). For information about installing and using the System Monitoring Plug-in for Microsoft Active Directory, please refer to Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Microsoft Active Directory (http://download.oracle.com/docs/cd/B16240_01/doc/install.102/b28044/toc.htm).

Oracle Identity Federation 10.1.4.2, 10.1.4.3.0

1. Complete all the configuration steps for the Oracle Identity Federation. Make sure that the Federation Data Store details and User Data Store details are defined so that Enterprise Manager can discover the topology of your Oracle Identity Federation environment. Refer to the Oracle Identity Federation Administrator's Guide for instructions on configuring the Identity Federation (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25355/configuring.htm#BCGDGAJ).
2. Discover the Oracle Application Server on which Oracle Identity Federation is deployed in Enterprise Manager Grid Control. Complete the following steps to discover Oracle Application Server in Grid Control:
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Middleware** sub-tab. Note: If the Middleware sub-tab is not shown, please add it by clicking on **Preferences > Target Subtabs**.
 - Select **Oracle Application Server** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for Oracle Application Server. Click **Next** once all information requested is entered.
3. If you plan to monitor the Directory Server through Oracle Enterprise Manager Grid Control, then make sure that the directory server is appropriately discovered in Enterprise Manager before moving on to the discovery of Oracle Identity Federation Server. Complete the following tasks to discover the supported directory servers:
 - **Oracle Internet Directory 10.1.4:** Discovery of Oracle Identity Management Suite 10g (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server) can be done using the discovery wizard on the Identity and Access page. From the *Identity and Access* page, select “*Identity Management 10g (OID, DAS, DIP, SSO)*” from the *Add* drop-down menu.

For more information, please refer to the [Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0](#) section.

- **Microsoft Active Directory:** Download and install Oracle System Monitoring Plug-in for Microsoft Active Directory from OTN: (<http://www.oracle.com/technology/software/products/oem/htdocs/system-monitoring-connectors.html>). For information about installing and using the System Monitoring Plug-in for Microsoft Active Directory, please refer to Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Microsoft Active Directory (http://download.oracle.com/docs/cd/B16240_01/doc/install.102/b28044/toc.htm).
4. If Oracle Database is used for the User Data Store, make sure that the database instance is discovered in Enterprise Manager Grid Control before moving on to the discovery Oracle Identity Federation Server. Complete the following steps to discover Oracle Database Instance in Grid Control:
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.
 - Select **Database Instance** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for the Database Instance. Click **Next** once all information requested is entered.

Oracle Identity Manager 9.1.0.1

1. Complete all the configuration steps for Oracle Identity Manager. Make sure that the application server and database are appropriately set up and configured for Oracle Identity Manager. Refer to the Oracle Identity Manager Installation and Upgrade Guide for instructions on configuring Oracle Identity Manager (http://download.oracle.com/docs/cd/B31081_01/index.htm).
2. Discover the application server on which Oracle Identity Manager is deployed in Enterprise Manager Grid Control. Complete the following steps to discover the supported application servers:
 - **JBoss Application Server Version 4.0.2:**
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Middleware** sub-tab. *Note:* If the Middleware sub-tab is not shown, please add it by clicking on *Preferences > Target Subtabs*.
 - Select **JBoss Application Server** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for the JBoss Application Server. Click **Next** once all information requested is entered.
 - **Oracle WebLogic Application Server Version 7.x and 8.x**
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Middleware** sub-tab. *Note:* If the Middleware sub-tab is

not shown, please add it by clicking on *Preferences > Target Subtabs*.

- Select **Oracle WebLogic Domain 7.x and 8.x** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for the WebLogic Application Server. Click **Next** once all information requested is entered.
- **WebSphere Application Server Version: 5.1.1.5:**
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Middleware** sub-tab. *Note:* If the Middleware sub-tab is not shown, please add it by clicking on *Preferences > Target Subtabs*.
 - Select **IBM WebSphere Application Server** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for the WebSphere Application Server. Click **Next** once all information requested is entered.
3. If Oracle Database is used for Oracle Identity Manager, make sure that the database instance is discovered in Enterprise Manager Grid Control before moving on to the discovery Oracle Identity Manager Server. Complete the following steps to discover Oracle Database Instance in Grid Control:
 - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.
 - Select **Database Instance** from the **Add** dropdown menu and click on the **Go** button.
 - Enter the information requested for the Database Instance. Click **Next** once all information requested is entered.
 4. If Microsoft SQL Server is used for Oracle Identity Manager, make sure that SQL Server is discovered in Enterprise Manager Grid Control before moving on to the discovery Oracle Identity Manager Server. Download and install Oracle System Monitoring Plug-in for Microsoft SQL Server from OTN: (<http://www.oracle.com/technology/software/products/oem/htdocs/system-monitoring-connectors.html>). For information about installing and using the System Monitoring Plug-in for Microsoft SQL Server, please refer to Oracle Enterprise Manager System Monitoring Plug-in Installation Guide for Microsoft SQL Server (http://download.oracle.com/docs/cd/B16240_01/doc/apirefs.102/e12776/toc.htm).

Oracle Access Manager 11g (11.1.1.3.0)

1. Download and install a critical patch required for discovering Oracle Access Manager Server target. The patch number is **10094106** and can be downloaded from My Oracle Support (<https://support.oracle.com/CSP/ui/flash.html#tab=PatchHomePage%28page=PatchHomePage&id=%28%29%29,%28page=PatchSearchResultsHome&id=%28from=bookmark&viewItem=0&search=%3CSearch%3E%0A%20%20%3CFilter%20>

[name=%22patch_number%22%20op=%22IS%22%20value=%2210094106%22%20type=%22patch_number%22/%3E%0A%20%20%3CFilter%20name=%22platform%22%20op=%22IS%22%20value=%22%22%20type=%22platform%22/%3E%0A%3C/Search%3E&flag=search%29%29\).](#)

Oracle Directory Server Enterprise Edition (formerly Sun Java Directory Server Enterprise Edition) 6.x, 7.x, and 11g (11.1.1.3.0)

1. Download and install **Oracle System Monitoring Plug-in for Oracle Directory Server Enterprise Edition**. The plug-in can be downloaded from OTN (<http://www.oracle.com/technetwork/oem/grid-control/downloads/plugin-directory-server-198363.html>). The plug-in will need to be downloaded on the host running the Enterprise Manager Grid Control – Oracle Management Service (OMS).
2. Follow the instructions in the Installation Guide to install and configure the plug-in (http://download.oracle.com/otn/java/oem/ODSEE_EMPI_documentation_v1.0.pdf).

Discovering & Configuring Oracle Identity Management Targets

This section covers the following topics:

- [Discovering Oracle Access Manager Access Server 10.1.4.2, 10.1.4.3.0](#)
- [Discovering Oracle Access Manager Identity Server 10.1.4.2, 10.1.4.3.0](#)
- [Discovering Oracle Identity Federation Server 10.1.4.2, 10.1.4.3.0](#)
- [Discovering Oracle Identity Manager Server 9.1.0.1](#)
- [Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0](#)
- [Discovering Oracle Identity Management 11g PS1 \(11.1.1.2.0\), 11g PS2 \(11.1.1.3.0\)](#)
- [Collecting User Statistics for Oracle Internet Directory](#)
- [Creating Identity and Access System](#)
- [Creating Generic Service or Web Application Targets for Identity Management](#)
- [Creating a Service Dashboard Report](#)
- [Updating Monitoring Configuration for Individual Identity Management Targets](#)
- [Adding or Removing Targets from the System Topology](#)
- [Removing Servers or Components from an Existing Identity Management Topology](#)

Discovering Oracle Access Manager Access Server 10.1.4.2, 10.1.4.3.0

Enterprise Manager has a simple discovery wizard for Oracle Access Manager 10g targets. The discovery wizard collects details about Oracle Access Manager Targets including information about the hostname, host login credentials, SNMP agent credentials, and other details.

After the discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Enterprise Manager's Repository.

To discover Oracle Access Manager – Access Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 10g (OAM, OIF, OIM)** from the **Add** dropdown menu and click on the **Go** button.
3. Select the radio button for **Access Server** and enter the host name on which your Oracle Access Manager Access Server is running. Click **OK** to continue with the discovery of the Access Server.
4. Enter the information requested for Oracle Access Manager – Access Server. Click **Next** once all information requested is entered.
 - a. **Host User Name:** Username on the operating system with administrator privileges.
 - b. **Host User Password:** Password of host administrator account.
 - c. **Save as Preferred Credentials:** Select this checkbox if you would like to save the username/password for the administrator account.
 - d. **Management Agent running on Host other than SNMP Host:** Select this checkbox if your Grid Control Agent is running on a host other than the SNMP Agent host.
 - e. **Access Server Home:** Enter the home directory of your Access Server (<OAM_HOME>\access) – e.g. C:\Program Files\OracleAccessManager\access
 - f. **Access Server Version:** Enter the version of your Oracle Access Manager – Access Server – e.g. 10.1.4.0.1
 - g. **SNMP Agent Host:** If your SNMP Agent is running on a host other than the Grid Control Agent host, then enter the SNMP Agent hostname. Otherwise, please skip this section.
 - h. **SNMP Agent Port:** Enter the UDP Port of the SNMP Agent – e.g. 161
 - i. **SNMP Agent Community Name:** Enter the community name of the SNMP Agent.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Ides

Add Access Manager - Access Server Target : Discovery

To add Access Server, provide the host credentials and SNMP Agent port number. Specify the SNMP Agent port number for different hosts.

* Host User Name

Administrator

User Name of Host where Management Agent is installed

* Host User Password

••••••

User Password of Host where Management Agent is installed

☒ Save as Preferred Credential

☐ Management Agent is running on Host other than SNMP Host
This page will be refreshed if you click this option

* Access Server Home

Files\OracleAccessManager\access

* Access Server Version

10.1.4.0.1

Metrics monitored by Management Agent are version specific

SNMP Agent Host

emgc-amp6.us.oracle.com

* SNMP Agent Port

161

* SNMP Agent Community Name

•••

- Enterprise Manager discovers the topology of your Oracle Access Manager – Access Server deployment including the associated databases and directory servers. To add this topology into an existing Access Manager – Access System target, select the radio button for **“Use the specified system”** and select an existing target of type **Access Manager – Access System**. If you would like to create a new Access Manager – Access System target, select the radio button for **“Create a new system”** and enter the name of new system target. Click **Finish** to complete the discovery.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | S

Add Access Manager - Access Server Target : Discovery

This page displays the Access Server host and port information along with the Directory Servers associated with it. The associated previously discovered and available in the Management Repository.

Discovered Targets

Name	Type	Host
emgc-amp6.us.oracle.com:6025_Access Server	Access Manager - Access Server	emgc-amp6.us.oracle.com

Associated Targets

Name	Type	Host
idm_as.emgc-amp6.us.oracle.com_LDAP	LDAP Server	emgc-amp6.us.oracle.com
idm.us.oracle.com	Database Instance	emgc-amp6.us.oracle.com

System

Select a system to add this target or specify a new system.

☐ Use the specified system

System Name


Existing system will be modified with new target

☒ Create a new system

System Name

New system will be created with discovered target

6. The next page shows a message confirming the discovery of Oracle Access Manager – Access Server.

Hosts | Databases | Application Servers | Web Applications | Service

Add Identity Component

Confirmation

emgc-amp6.us.oracle.com:6025_Access Server successfully added.

- ☒ Access Server
- ☐ Identity Server
- ☐ Identity Manager Server
- ☐ Identity Federation Server

Discovering Oracle Access Manager Identity Server 10.1.4.2, 10.1.4.3.0

Enterprise Manager has a simple discovery wizard for Oracle Access Manager 10g targets. The discovery wizard collects details about Oracle Access Manager Targets including information about the hostname, host login credentials, SNMP agent credentials, and other details.

After the discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Enterprise Manager's Repository.

To discover Oracle Access Manager – Identity Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. Note: If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 10g (OAM, OIF, OIM)** from the **Add** dropdown menu and click on the **Go** button.
3. Select the radio button for **Identity Server** and enter the host name on which your Oracle Access Manager Identity Server is running. Click **OK** to continue with the discovery of the Identity Server.
4. Enter the information requested for Oracle Access Manager – Identity Server. Click **Next** once all information requested is entered.
 - a. **Host User Name**: Username on the operating system with administrator privileges.
 - b. **Host User Password**: Password of host administrator account.
 - c. **Save as Preferred Credentials**: Select this checkbox if you would like to save the username/password for the administrator account.
 - d. **Management Agent running on Host other than SNMP Host**: Select this checkbox if your Grid Control Agent is running on a host other than the SNMP Agent host.
 - e. **Identity Server Home**: Enter the home directory of your Identity Server (<OAM_HOME>\identity) – e.g. C:\Program Files\OracleAccessManager\identity
 - f. **Identity Server Version**: Enter the version of your Oracle Access Manager – Identity Server – e.g. 10.1.4.0.1
 - g. **SNMP Agent Host**: If your SNMP Agent is running on a host other than the Grid Control Agent host, then enter the SNMP Agent hostname. Otherwise, please skip this section.
 - h. **SNMP Agent Port**: Enter the UDP Port of the SNMP Agent – e.g. 161
 - i. **SNMP Agent Community Name**: Enter the community name of the SNMP Agent.

[Hosts](#) | [Databases](#) | [Application Servers](#) | [Web Applications](#) | [Services](#) | [Systems](#) | [Groups](#) | [Identity](#)

Add Access Manager - Identity Server Target : Discovery

To add Identity Server, provide the host credentials and SNMP Agent port number. Specify the SNMP Agent different hosts.

* Host User Name

Administrator

User Name of Host where Management Agent is installed

* Host User Password

••••••

User Password of Host where Management Agent is installed

☐ Save as Preferred Credential

☐ Management Agent is running on Host other than SNMP Host
This page will be refreshed if you click this option

* Identity Server Home

C:\Program Files\OracleAccessMan

* Identity Server Version

10.1.4.0.1

Metrics monitored by Management Agent are version specific

SNMP Agent Host

emgc-amp6.us.oracle.com

* SNMP Agent Port

161

* SNMP Agent Community Name

••••••

- Enterprise Manager discovers the topology of your Oracle Access Manager – Identity Server deployment including the associated databases and directory servers. To add this topology into an existing Access Manager – Identity System target, select the radio button for **“Use the specified system”** and select an existing target of type **Access Manager – Identity System**. If you would like to create a new Access Manager – Identity System target, select the radio button for **“Create a new system”** and enter the name of new system target. Click **Finish** to complete the discovery.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | Si

Add Access Manager - Identity Server Target : Discovery

This page displays the Identity Server host and port information along with the Directory Servers associated with it. The associated previously discovered and available in the Management Repository.

Discovered Targets

Name	Type	Host
emgc-amp6.us.oracle.com:6022_Identity Server	Access Manager - Identity Server	emgc-amp6.us.oracle.com

Associated Targets

Name	Type	Host
oam_ms_active_directory	Microsoft Active Directory	emgc-amp6.us.oracle.com
idm.us.oracle.com	Database Instance	emgc-amp6.us.oracle.com

System

Select a system to add this target or specify a new system.

☐ Use the specified system

System Name

Existing system will be modified with new target

☒ Create a new system

System Name

New system will be created with discovered target

6. The next page shows a message confirming the discovery of Oracle Access Manager – Identity Server.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | Si

Add Identity Component

Confirmation

emgc-amp6.us.oracle.com:6022_Identity Server successfully added.

☒ Access Server

☐ Identity Server

☐ Identity Manager Server

☐ Identity Federation Server

* Host Name

Host which will monitor the selected target

Discovering Oracle Identity Federation Server 10.1.4.2, 10.1.4.3.0

Enterprise Manager has a simple discovery wizard for Oracle Identity Federation targets. The discovery wizard collects details about Oracle Identity Federation targets including information about the hostname, host login credentials, and other details.

After the discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Enterprise Manager's Repository.

To discover Oracle Identity Federation Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. Note: If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 10g (OAM, OIF, OIM)** from the **Add** dropdown menu and click on the Go button.
3. Select the radio button for **Identity Federation Server** and enter the host name on which your Oracle Identity Federation Server is running. Click **OK** to continue with the discovery of the Identity Federation Server.
4. Enter the information requested for Oracle Identity Federation Server. Click **Next** once all information requested is entered.
 - a. **Application Server Target**: Select the Application Server target on which Oracle Identity Federation is running.
 - b. **Host User Name**: Username on the operating system with administrator privileges.
 - c. **Host User Password**: Password of host administrator account.

Hosts | Databases | Application Servers | Web Applications | Services | Systems

Add Identity Federation Server: Discovery

In order to add Oracle Identity Federation Target, you need to select the Application server must discover them first.

* Application Server Target 

* Host User Name

* Host Password

- Enterprise Manager discovers the topology of your Oracle Identity Federation Server deployment including the associated databases and directory servers. To add this topology into an existing Identity Federation System target, select the radio button for **“Use the specified system”** and select an existing target of type **Identity Federation System**. If you would like to create a new Identity Federation System target, select the radio button for **“Create a new system”** and enter the name of new system target. Click **Finish** to complete the discovery.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | Siebel | PeopleSoft | Ora

Add Identity Federation Server: Discovery Results

Clicking on Finish button, will create the Identity Federation system and will be monitored by Enterprise Manager.

Identity Federation Server Target

Target	Host	Port	Role	Status
oif_idm.emgc-amp6.us.oracle.com_OIF	emgc-amp6.us.oracle.com	7778	Identity and Service Provider	↑

User Data Store

Target	Type	Host	Port	Status
idm_as.emgc-amp6.us.oracle.com_LDAP	LDAP Server	emgc-amp6.us.oracle.com	13060	↑

Federation Data Store

Target	Type	Host	Port	Status
idm_as.emgc-amp6.us.oracle.com_LDAP	LDAP Server	emgc-amp6.us.oracle.com	13060	↑

Related Targets

Target	Type	Host	Port	Status
oif_idm.emgc-amp6.us.oracle.com_HTTP Server	Oracle HTTP Server	emgc-amp6.us.oracle.com	7778	↑
oif_idm.emgc-amp6.us.oracle.com_OC4J_FED	OC4J	emgc-amp6.us.oracle.com		↑

Identity Federation System

Select an existing Identity Federation system to add these targets or specify a new system.

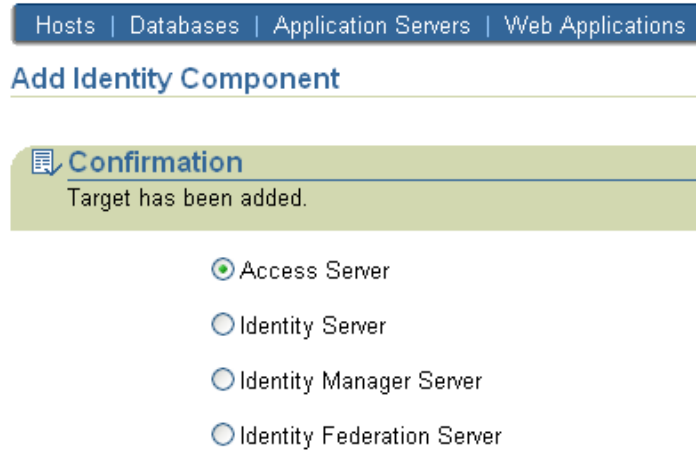
☒ Use the specified system 

Existing system will be modified with the new targets.

☐ Create a new system

A new system will be created using the discovered targets.

- The next page shows a message confirming the discovery of Oracle Identity Federation Server.



Discovering Oracle Identity Manager Server 9.1.0.1

Enterprise Manager has a simple discovery wizard for Oracle Identity Manager targets. The discovery wizard collects details about Oracle Identity Manager targets including information about the hostname, host login credentials, and other details.

After the discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Enterprise Manager's Repository.

To discover Oracle Identity Manager Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 10g (OAM, OIF, OIM)** from the **Add** dropdown menu and click on the Go button.
3. Select the radio button for **Identity Manager Server** and enter the host name on which your Oracle Identity Manager is running. Click **OK** to continue with the discovery of the Oracle Identity Manager Server.
4. Enter the information requested for Oracle Identity Manager Server. Click **Next** once all information requested is entered.
 - a. **Application Server Target:** Select the Application Server target on which Oracle Identity Manager is running.
 - b. **Configured Database Target:** Select the configured Database target used by Oracle Identity Manager.

- c. **Database User Name:** Enter the database username used to access the tablespace reserved for Oracle Identity Manager.
- d. **Database Password:** Enter the password for the database account reserved for Oracle Identity Manager.
- e. **Identity Manager Library Path:** Enter the directory path for the Oracle Identity Manager library (<OIM_HOME>\xellerate\lib).
- f. **Host User Name:** Username on the operating system with administrator privileges.
- g. **Host User Password:** Password of host administrator account.

Hosts | Databases | Application Servers | Web Applications | Services | Systems | G

Add Oracle Identity Manager: Discovery

Select the Application Server where Identity Manager Server is deployed and the database that Application Server targets and Database targets show only previously discovered targets.

* Application Server Target 

* Configured Database Target 

* Database User Name

* Database Password

* Identity Manager Library Path

* Host User Name

* Host Password

☐ Save as preferred credentials

5. Enterprise Manager discovers the topology of your Oracle Identity Manager Server deployment including the associated databases and directory servers. To add this topology into an existing Identity Manager System target, select the radio button for “**Use the specified system**” and select an existing target of type **Identity Manager System**. If you would like to create a new Identity Manager System target, select the radio button for “**Create a new system**” and enter the name of new system target. Click **Finish** to complete the discovery.
6. The next page shows a message confirming the discovery of Oracle Identity Manager Server.

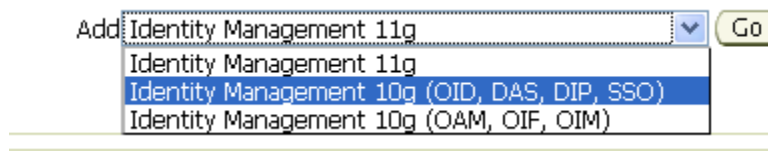
Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0

Enterprise Manager has a simple discovery wizard for Oracle Identity Management Suite 10g (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server) targets. The discovery wizard collects details about Oracle

Identity Management Suite 10g targets including information about the hostname, host login credentials, and other details.

To discover Oracle Identity Management Suite 10g (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server), perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 10g (OID, DAS, DIP, SSO)** from the **Add** dropdown menu and click on the Go button.



3. Select the host on which Oracle Identity Management Suite 10g targets are running.



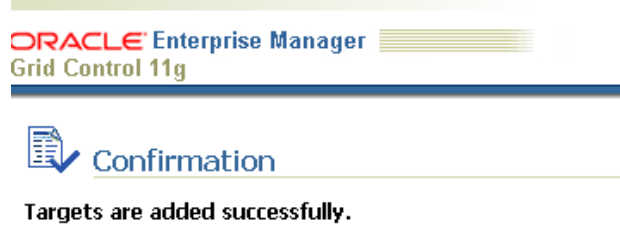
4. A confirmation page lists Oracle Application Servers found on the host selected. Click **OK** to continue. *Important:* Please make sure that the Application Server is up before discovering the Identity Management Suite targets.

Discover Application Servers: Results

The following targets were successfully discovered by the Agent. By clicking the OK button, all the Oracle Application Server targets and their

Name	Type
im1014.stbda07.us.oracle.com	Oracle Application Server

5. A final confirmation page appears. Click **OK** to finish the discovery process.

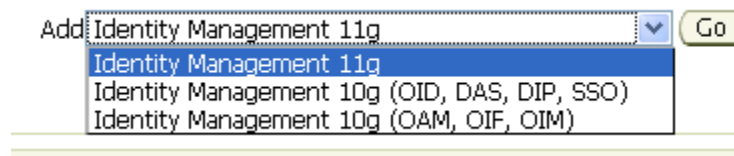


Discovering Oracle Identity Management 11g PS1 (11.1.1.2.0), 11g PS2 (11.1.1.3.0) and Oracle Identity and Access Management 11g (11.1.1.3.0)

Enterprise Manager has a simple discovery wizard for Oracle Identity Management 11g (including Oracle Internet Directory, Directory Integration Platform, Oracle Virtual Directory, and Oracle Identity Federation) targets as well as Oracle Identity and Access Management 11g (including Oracle Access Manager, Oracle Adaptive Access and Oracle Identity Manager) targets. The discovery wizard collects details about Oracle Identity Management 11g targets including information about the host, WebLogic Username/Password, and other details.

Before discovering the targets associated with Oracle Access Manager 11g please download and install the patch **10094106** as per the steps in the [pre-requisites](#) section. To discover Oracle Identity Management 11g (including Oracle Internet Directory, Directory Integration Platform, Oracle Virtual Directory, Oracle Identity Federation, Oracle Access Manager, Oracle Adaptive Access Manager and Oracle Identity Manager), perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select **Identity Management 11g** from the **Add** dropdown menu and click on the **Go** button.



3. Enter the information requested to discover Oracle Identity Management 11g targets.
 - a. **Administration Server Host:** The host on which the WebLogic domain for Identity Management is running

- b. **Port:** The port used for the WebLogic domain.
- c. **Username/Password:** The WebLogic domain username/password.
- d. **Unique Domain Identifier:** A unique identifier for the Identity Management domain.
- e. **Agent:** The agent that is running on the Identity Management host.

ORACLE Enterprise Manager 11g
Grid Control

Home Targets Deployments All Targets Identity and Access

Hosts Databases Middleware Web Applications Services Systems Groups Virtual Servers

Add Fusion Middleware Farm: Find Targets

Enterprise Manager can be configured to manage additional Oracle WebLogic Domains.

* Administration Server Host:

* Port:

* Username:

* Password:

* Unique Domain Identifier:

* Agent:

Unique Domain Identifier is used to create unique target name. Characters '/', '\', and spaces are not allowed.

☐ Advanced

4. A list of all the Identity Management targets is listed. Click **Add** to complete the discovery. **Note:** If the **Configured Agent** text-box is blank for one or more of the targets, please copy and paste the agent URL before you proceed.

ORACLE Enterprise Manager 11g
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports My Oracle Support

Hosts Databases Middleware Web Applications Services Systems Groups Virtual Servers All Targets Identity and Access

Page Refreshed Jan 19, 2010 10:01:01 AM

Add Fusion Middleware Farm: Assign Agents

Targets Found: 12
Targets Assigned To Local Agent: 10

You can optionally override any agent assignment using the table below.

☐ Hide Targets And Agent Assignments

Target Name	Target Type	Host	Configured Agent
IdM11Farm_IDMDomain	Oracle Fusion Middleware Farm		https://stbpo32.oracle.com:3872/emd/main/
oid1	Oracle Internet Directory	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
ovd1	Oracle Virtual Directory	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
IDMDomain	Oracle WebLogic Domain		https://stbpo32.oracle.com:3872/emd/main/
AdminServer	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
ASConfigManagement	Application Deployment	stbpo32.oracle.com	[Inherited From Parent]
wls_ods1	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
odsm(11.1.1.2.0)	Application Deployment	stbpo32.oracle.com	[Inherited From Parent]
DIP(11.1.1.2.0)	Directory Integration Platform Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
wls_of1	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
OIF(11.1.1.2.0)	Identity Federation Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/
ohs1	Oracle HTTP Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/

Save All Targets To This Agent:

5. The status of target discovery is summarized in this screen. Make sure that all targets have been successfully added to Enterprise Manager. Press the **OK** button to finish the discovery process.

ORACLE Enterprise Manager 11g
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports My Oracle Support

Hosts | Databases | **Middleware** | Web Applications | Services | Systems | Groups | Virtual Servers | All Targets | Identity and Access

Page Refreshed Jan 19, 2010 10:03:30 AM PST

Add Fusion Middleware Farm: Results

12 targets have been successfully added to Enterprise Manager.

There may be a delay before these targets are visible and monitored.

If the targets of the farm or domain change in the future, use Refresh Farm or Refresh WebLogic Domain to add targets. If targets are later removed from the farm or domain, you can delete them from the All Targets page or the Agent page.

☐ Hide Targets Details

Target Name	Target Type	Host	Configured Agent	Status
IdM11Farm_IDMDomain	Oracle Fusion Middleware Farm		https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
oid1	Oracle Internet Directory	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
owd1	Oracle Virtual Directory	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
IDMDomain	Oracle WebLogic Domain		https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
AdminServer	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
ASConfigManagement	Application Deployment	stbpo32.oracle.com	[Inherited From Parent]	Successfully saved target to ag
wls_ods1	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
odsm(11.1.1.2.0)	Application Deployment	stbpo32.oracle.com	[Inherited From Parent]	Successfully saved target to ag
DIP(11.1.1.2.0)	Directory Integration Platform Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
wls_oif1	Oracle WebLogic Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
OIF(11.1.1.2.0)	Identity Federation Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag
ohs1	Oracle HTTP Server	stbpo32.oracle.com	https://stbpo32.oracle.com:3872/emd/main/	Successfully saved target to ag

OK

6. The discovered targets will now be listed on the **Identity and Access** page.

ORACLE Enterprise Manager
Grid Control 11g

Home Targets Deployments All Targets

All Targets | Hosts | Databases | **Middleware** | Web Applications | Services | Systems | Groups | Virtual Servers | Siebel | Identity and Access

Identity and Access

View Components

Expand All Collapse All

Name	Status	Version	Host	Alerts
Identity and Access				
Internet Directory Server	1 (1)			
/IdM11gR1_IDMDomain/asinst_1/oid1		11.1.1.2.0	ec2as11g	0 0
Virtual Directory Server	1 (1)			
/IdM11gR1_IDMDomain/asinst_1/owd1		11.1.1.2.0	ec2as11g	0 0
Directory Integration Platform Server	1 (1)			
/IdM11gR1_IDMDomain/IDMDomain/wls_ods1/DIP(11.1.1.2.0)		11.1.1.2.0	ec2as11g	0 0
Identity Federation Server	1 (1)			
/IdM11gR1_IDMDomain/IDMDomain/wls_oif1/OIF(11.1.1.2.0)		11.1.1.2.0	ec2as11g	0 0

Discovering Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g

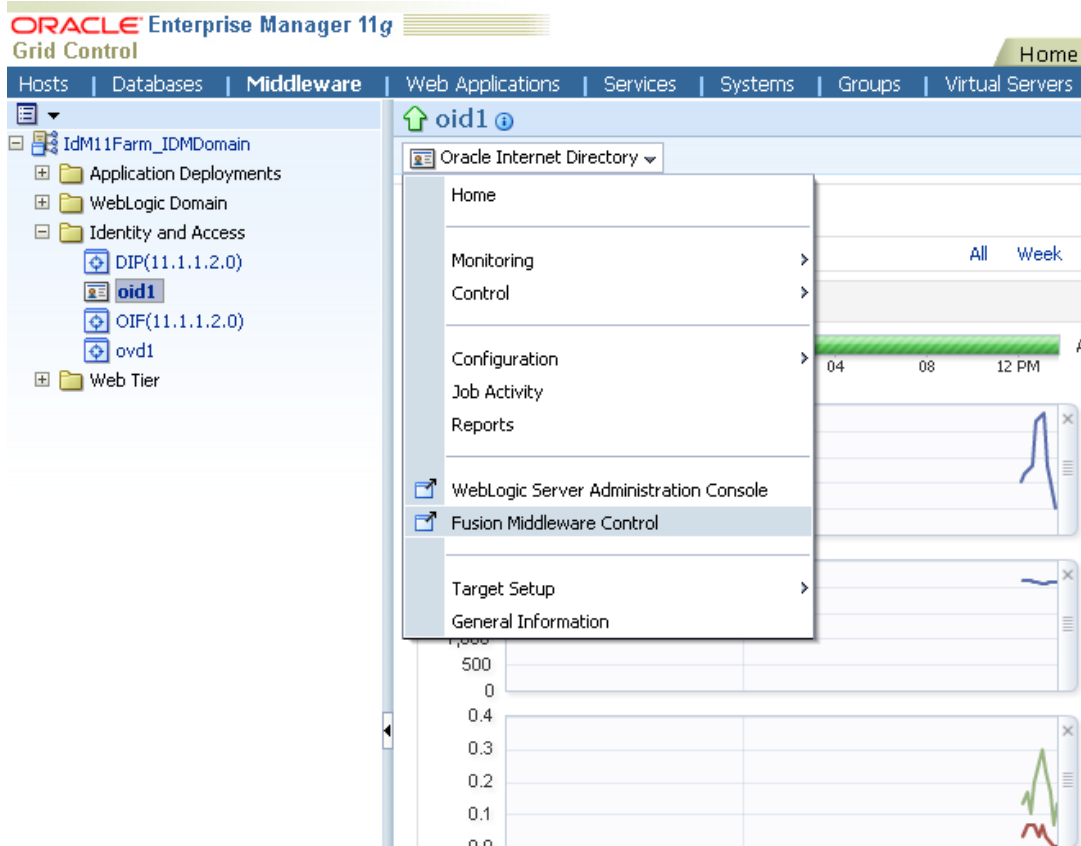
Download and install the **System Monitoring Plug-in for Oracle Directory Server Enterprise Edition** as per the instructions in the [pre-requisites](#) section. Please refer to the Installation Guide for the System Monitoring Plug-in for Oracle Directory Server Enterprise Edition (http://download.oracle.com/otn/java/oem/ODSEE_EMPI_documentation_v1.0.pdf).

Collecting User Statistics for Oracle Internet Directory

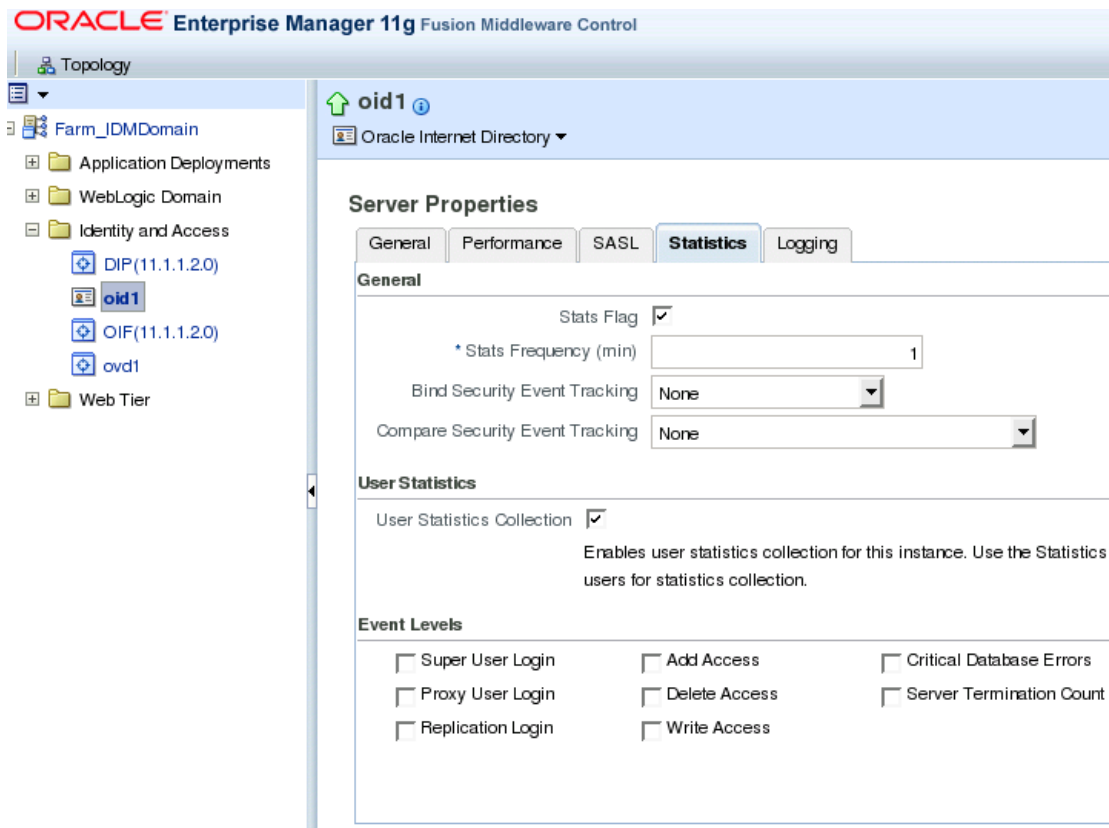
With Enterprise Manager, you can collect user statistics for Oracle Internet Directory allowing you to view charts for failed and completed LDAP operations like Add/Bind/Compare/Delete/Modify/Search.

To enable the collection of user statistics, perform the following steps:

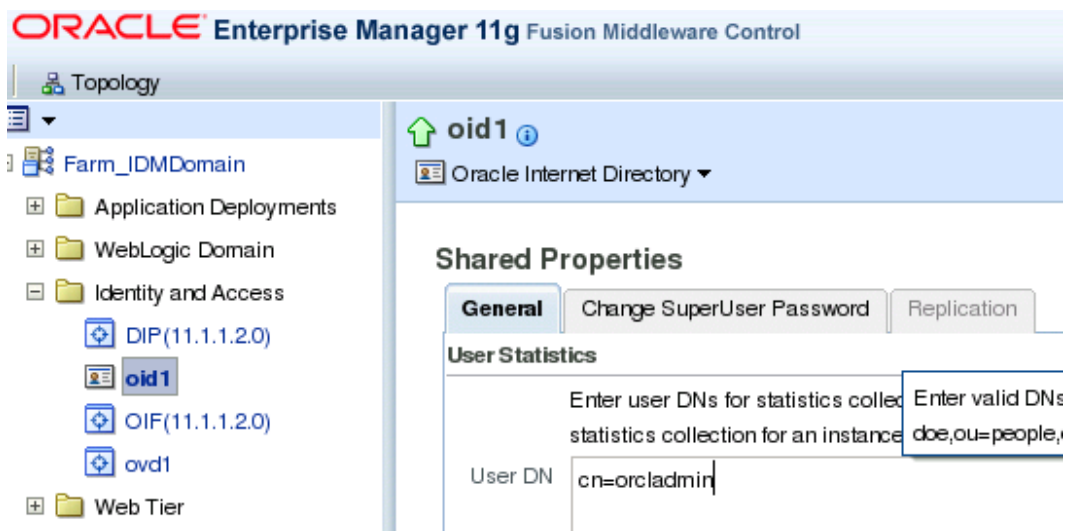
1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. Note: If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. Select the discovered **Oracle Internet Directory** target.
3. From the target menu, select **Fusion Middleware Control**.



4. From the target menu in Fusion Middleware Control, select **Administration > Server Properties**. Check the box next to **User Statistics Collection** to enable this feature. Click **Apply** to save your changes.



- From the target menu in Fusion Middleware Control, select **Administration > Shared Properties**. Enter a valid DN (e.g. cn=orcladmin) to enable user statistics collection for that user.



Creating Identity and Access System

With Enterprise Manager, you can create an **Identity and Access System** target that can be modeled with any discovered Oracle Identity Management target (including both Identity Management 10g and Identity Management 11g targets) and the underlying hosts, databases and LDAP servers as the key components providing an end-to-end system oriented view of the monitored Identity Management environment. The Identity and Access System target provides access to metrics, alerts, charts, and topology view. In addition to monitoring your Oracle Identity Management environment from a system perspective, you may also monitor your environment from a service-oriented perspective using Grid Control's Service Level Management framework – please view the [Service Level Management](#) section for more information about Service Level Management.

To create a target of type **Identity and Access System** associated with any of the monitored Identity Management targets, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - a. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - b. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - c. Click **Apply** to save your changes.
2. From the **View** drop-down menu, select **Systems and Services**.

ORACLE Enterprise Manager
Grid Control 11g

All Targets | Hosts | Databases | Middleware | Web Applications | Services | Systems

Identity and Access

View: Systems and Services

Components

Systems and Services

Systems

Add Identity and Access System Go

Select Name	Type
No System Found	

Services

Add

Select Name	Status
No Service Found	

3. Select **Identity and Access System** from the drop-down menu and click on **Go**.
4. Select the Identity Management domain that you would like to include in your system topology and click **Next** to continue.

Create Identity and Access System

Select IDM Install Select Targets Summary

Select IDM Install

Select the Identity Management installation from the table and proceed to next step to select the targets related to the installation

View ▾

Application Server	Install Version	IDM Targets
/im11ps2_IM11PS2Domain/IM11PS2Domain	11.1.1.0	DIP(11.1.1.2.0) , OIF(11.1.1.2.0) , ovd1 , oid1
ias.adc2110365.us.oracle.com	10.1.4	Single Sign-On:orasso , ias.adc2110365.us.oracle.c
im1014.stbda07.us.oracle.com	10.1.4	im1014.stbda07.us.oracle.com_LDAP , Single Sign-C

5. Select the targets within the domain that you would like to include in your system topology. You can also add additional targets that are not in the Identity Management domain – e.g. MS Active Directory, databases, etc. Click **Next** to continue.

Create Identity and Access System

Select IDM Install **Select Targets** Summary

Select Targets

Select the Identity Management and their related targets that should be part of the sytem

* System Name

* Select System Timezone

Selected Install Version 11.1.1.0

Selected Application Server /im11ps2_IM11PS2Domain/IM11PS2Domain

+ Add - Delete

Target Display Name	Target Name	Target Type	Time Zone
DIP(11.1.1.2.0)	/im11ps2_IM11PS2Domain/IM11PS2Domain/wls_ods1	Directory Integration Platform S	PST8PDT
stbda07.us.oracle.com	stbda07.us.oracle.com	Host	PST8PDT
OIF(11.1.1.2.0)	/im11ps2_IM11PS2Domain/IM11PS2Domain/wls_oif1	Identity Federation Server	PST8PDT
ovd1	/im11ps2_IM11PS2Domain/asinst_ps2/ovd1	Oracle Virtual Directory	PST8PDT
oid1	/im11ps2_IM11PS2Domain/asinst_ps2/oid1	Oracle Internet Directory	PST8PDT
im11	im11	Database Instance	PST8PDT

6. Click **Finish** to complete the creation of Identity and Access System.

Create Identity and Access System

Select IDM Install Select Targets **Summary**

Summary

Review the data and click OK to create the System

System Name idm system1
 System TimeZone PST8PDT
 Selected Install Version 11.1.1.0
 Selected Application Server /im11ps2_IM11PS2Domain/IM11PS2Domain

Target Display Name	Target Name	Target Type	Time Zone
DIP(11.1.1.2.0)	/im11ps2_IM11PS2Domain/IM11PS2Domain/wls_ods1	Directory Integration Platform S	PST8PDT
stbda07.us.oracle.com	stbda07.us.oracle.com	Host	PST8PDT
OIF(11.1.1.2.0)	/im11ps2_IM11PS2Domain/IM11PS2Domain/wls_oif1	Identity Federation Server	PST8PDT
ovd1	/im11ps2_IM11PS2Domain/asinst_ps2/ovd1	Oracle Virtual Directory	PST8PDT
oid1	/im11ps2_IM11PS2Domain/asinst_ps2/oid1	Oracle Internet Directory	PST8PDT
im11	im11	Database Instance	PST8PDT

Creating Generic Service or Web Application Targets for Identity Management

The discovery wizard for Oracle Identity and Access Management Suite allows you to create a System target to store the end-to-end topology of monitored Oracle Identity Management components. The Management Pack Plus for Identity Management allows you to create the following System targets:

- Access Manager – Access System
- Access Manager – Identity System
- Identity Federation System
- Identity Manager System
- Identity and Access System

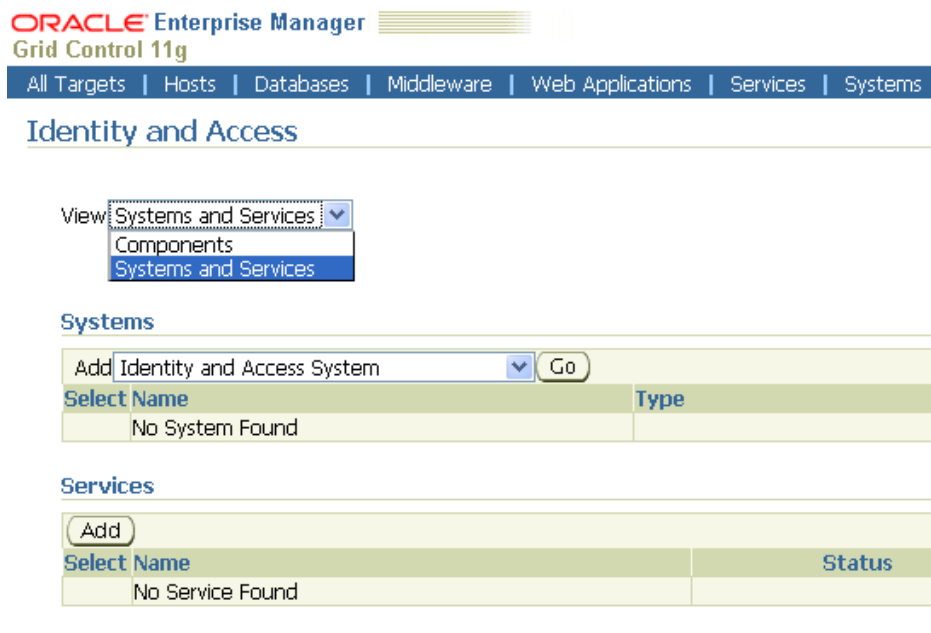
A System target is modeled with all monitored Oracle Identity Management components and the underlying hosts as the key components providing an end-to-end system oriented view of the monitored Oracle Identity Management environment. A System target provides access to metrics, alerts, charts, and topology view of all the infrastructure components. In addition to monitoring your Oracle Identity Management environment from a system perspective, you may also monitor your environment from a service-oriented perspective using Grid Control's Service Level Management framework – please view the [Service Level Management](#) section for more information about Service Level Management.

With the Management Pack Plus for Identity Management, users can create targets of type **Generic Service** or **Web Application** associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, and Identity Manager System. The Web Application or Generic Service target provides an end-to-end service oriented view of the monitored Oracle Identity

Management targets with access to performance and usage metrics, service tests, service level rules, service availability definition, alerts, charts, and topology view.

To create a target of type **Generic Service** associated with any of the monitored Identity Management Systems, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **Identity and Access** sub-tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by performing the following steps:
 - d. Click on **Preferences** (on the top right-hand corner of the screen) and then select **Target Subtabs**.
 - e. Move **Identity and Access** to the **Selected Target Subtabs** section.
 - f. Click **Apply** to save your changes.
2. From the **View** drop-down menu, select **Systems and Services**.



3. Click **Add** from the **Services** section.
4. Enter the general information requested for the new Generic Service. Click **Continue** once all information requested is entered.
 - a. **Name:** Enter a name for your new Generic Service – e.g. Oracle Access Manager Access Service
 - b. **Time Zone:** Select a time zone for your service
 - c. **Select System:** Select a system to be associated with your new service – e.g. **Access Manager – Access System**

ORACLE Enterprise Manager 10g
Grid Control

Home Targets

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | Siebel | PeopleSoft

General Availability Service Test Beacons Performance Metrics Usage Metrics

Create Generic Service: General

Define a service to model and monitor a business process or application.

* Name:

Time Zone:
Select the time zone for this service. Monitored data will be displayed using the selected time zone.

System

Select a system target that hosts this service, then mark the system's key components -- the targets critical for running this service.

System: **Oracle Access Manager - Access Server**

Time Zone: **(UTC-08:00)**

Component	Type	Key Component
emgc-amp6.us.oracle.com	Host	☒
emgc-amp6.us.oracle.com:6025_Access Server	Access Manager - Access Server	☒
idm.us.oracle.com	Database Instance	☒
idm_as.emgc-amp6.us.oracle.com_LDAP	LDAP Server	☒
oam_ms_active_directory	Microsoft Active Directory	☒

5. Enter the availability information requested for the new Generic Service. Click **Continue** once all information requested is entered.

- a. **Define availability based on:**

- i. **Service Test:** Choose this option if the availability of your service is determined by the availability of a critical functionality to your end users. For more information, please see the [Service Level Management](#) section.
 - ii. **System:** Your service's availability can alternatively be based on the underlying system that hosts the service. For more information, please see the [Service Level Management](#) section.

ORACLE Enterprise Manager 10g
Grid Control

Hosts | Databases | Application Servers | Web Applications

Create Generic Service: Availability

You can define the service's availability based on either system.

Define availability based on:

6. Enter the service test information requested for the new Generic Service. Click **Continue** once all information requested is entered.

- a. **Test Type:** Select the type of test that you would like to record or configure. For regular web transactions, select **Web Transaction**. For LDAP Service Tests, select **LDAP**.
- b. **Name:** Enter a name for your new service test – e.g. “Simple Login Test”
- c. **Collection Frequency (Minutes):** Enter the desired collection frequency for your service test.
- d. **Transaction:**
 - iii. **Basic Single URL:** If you would like to test a single page, enter a URL for your service test.
 - iv. **Record a Transaction:** Click on the **Go** button to record a web transaction that navigates through multiple pages in your application. For more information, please see the [Service Level Management](#) section.

ORACLE® Enterprise Manager 10g 
Grid Control

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups |

General Availability **Service Test** Beacons

Create Generic Service: Service Test

Define a service test to monitor the availability of this service. Based on the test type you select, a set

Test Type

* Name Description

* Collection Frequency (minutes)

Transaction

☐ Basic Single URL:

☒ Record a Transaction

6. Enter the beacon information requested for the new Generic Service. Click **Continue** once all information requested is entered.
 - a. **Add:** Select an available beacon where a Grid Control Agent is running. For more information, please see the [Service Level Management](#) section.
 - b. **Create:** Create a new beacon by selecting a discovered Grid Control Agent. For more information, please see the [Service Level Management](#) section.



Create Generic Service: Beacons

This page allows you to add Beacon locations from which the service will be monitored, verify the test on selected beacons, and determine availability.

The beacons you mark as Key Beacons will be used to determine the availability of the service.

Select	Name	Status	Key Beacon	Version	Operating System
☐	Redwood City, USA		☒	10.2.0.4.0	Windows

7. Enter the performance metrics information requested for the new Generic Service. Click **Continue** once all information requested is entered.
 - a. **Add Based on Service Test:** Click on the **Go** button to add performance metrics based on the recorded service test. Define the Warning Threshold and Critical Threshold for your alerts. For more information, please see the [Service Level Management](#) section.
 - b. **Add Based on System:** Click on the **Go** button to add performance metrics based on the monitored Oracle Identity Management components. Define the Warning Threshold and Critical Threshold for your alerts. For more information, please see the [Service Level Management](#) section.



Create Generic Service: Performance Metrics

Define the metrics used to measure your service's performance. Performance metrics are based on either the service test or the system. Once you've added metrics, you can define thresholds, which, when exceeded, will generate alerts. You can also select the metric whose graph you want to show in the Home Page for this service.

Select	Metric Name	Comparison Operator	Warning Threshold	Critical Threshold
☒	Successful user creations/sec	>	5	10
☐	Total Failed Authentications	>	5	10
☐	Perceived Total Time (ms)	>=	6000	12000

Chart on Home Page:

8. Enter the usage metrics information requested for the new Generic Service. Click **Next** once all information requested is entered.
 - a. **Add Based on System:** Click on the **Add** button to add usage metrics based on the monitored Oracle Identity Management components. Define the Warning

Threshold and Critical Threshold for your alerts. For more information, please see the [Service Level Management](#) section.

ORACLE Enterprise Manager 10g
Grid Control

Home Targets Deployments Alerts

Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | Identity Management | Siebel | PeopleSoft | Oracle Applications | A

Previous Performance Metrics **Usage Metrics** Review

Create Generic Service: Usage Metrics Cancel

Usage metrics measure user demand for your service. You can define usage metrics based on the metrics of one or more system components. Once you've added metrics, you can define thresholds, which, when exceeded, will generate alerts. You can also select the metric whose graph you want to show in the Home Page for this service.

Select Metric Name	Comparison Operator	Warning Threshold	Critical Threshold
☐ CPU Utilization (%)	>	70	90

Chart on Home Page

- Review the information and click on **Finish** to complete the creation of your new **Generic Service**. **Note:** You can update the information you entered after creating a Generic Service target. For more information, please see the [Service Level Management](#) section.

Creating a Service Dashboard Report

Once you've created Generic Service or Web Application targets associated with your monitored Oracle Identity Management Systems, you can create a Services Monitoring Dashboard that summarizes Service Level Agreement Compliance, Actual Service Level Achieved, Key Performance and Usage Metrics, and Status of Key Components.

Perform the following steps to create a Services Monitoring Dashboard:

- From the Enterprise Manager Console, click the **Reports** tab.
- Click the **Create** button.
- Enter the general information requested for the new Report. Click on the **Elements** tab once all information requested is entered.
 - Title:** Enter a title for your new dashboard
 - Category/Sub-Category:** Select a category and sub-category for your dashboard – e.g. Category: Monitoring, Sub-Category: Dashboards
 - Use the specified target:** Leave blank if this report has no report-wide target.
 - Options – Visual Style:** Select **Dashboard** for a dashboard-view of your services.
- Enter the elements information requested for the new Report. Click on the **Schedule** tab once all information requested is entered.
 - Add:** Select **Services Monitoring Dashboard** and click on the **Continue** button.
 - Set Parameters:** Click on the **Set Parameters** button. Select the available services and click on the **Move** button to add them to the Selected Services.
- Enter the schedule information requested for the new Report. Click on the **Access** tab once all information requested is entered.
 - Schedule:** Enter your scheduling preferences for the report
 - E-Mail Report:** Enter the email address and preferences for the report recipient.

6. Enter information about your access and security preferences for the new report. Click **OK** to create the new Services Monitoring Dashboard.

Updating Monitoring Configuration for Individual Identity Management Targets

You may update the monitoring configuration details for individual Oracle Identity Management targets. Updating monitoring configuration details for individual Oracle Identity Management targets can be used to enter new details about monitored targets including information about the hostname, Installation Home, host login credentials, database credentials, and SNMP Agent designated port and community name. For instance, if the database credentials for accessing the Oracle Identity Manager tables changed, then you can update the monitoring configuration details for **Identity Manager Server** using the Monitoring Configuration page.

Perform the following steps to update monitoring configuration for individual BI-EE targets:

1. From the Enterprise Manager Console, click the **Targets** tab.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management target that you would like to update. For instance, if you would like to update Identity Manager Server, click on the target of type **Identity Manager Server**.
4. Click on the **Monitoring Configuration** link in the **Related Links** section.
5. Update the information and click **OK** to save the new changes.

Adding or Removing Targets from the System Topology

The Management Pack Plus for Identity Management allows you to create the following System targets:

- Access Manager – Access System
- Access Manager – Identity System
- Identity Federation System
- Identity Manager System

Perform the following steps to add or remove a target from the “System” topology:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management System targets – e.g. **Access Manager – Access System**.
4. Click on the **Edit System** link from the **Related Links** section.
5. Click on the **Add** or **Remove** button and select the target you would like to add or remove from the System topology.

Removing Servers or Components from an Existing Identity Management Topology

After discovering Oracle Identity Management targets, you may manually remove individual targets. However, this will delete the respective target information from the Enterprise Manager repository.

After that entry is deleted, Enterprise Manager does not monitor that target anymore.

Perform the following steps for manually removing components from an existing enterprise are:

- Go to the **All Targets** tab, search for the server or component you want to delete, select the radio button next to the server or component name, and click the **Remove** button.

Performance Management and Diagnostics

Because of the size, complexity, and criticality of today's enterprise IT operations, the challenge for IT professionals is to be able to maintain high levels of component availability and performance for both applications and all components that make up the application's technology stack. Monitoring the performance of these components and quickly correcting problems before they can impact business operations is crucial.

For more information about Application Performance Management, please refer to the System Monitoring section of the *Enterprise Manager Concepts Guide*:

http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b31949/toc.htm

The Management Pack Plus for Identity Management in Enterprise Manager provides comprehensive, flexible, easy-to-use monitoring functionality that supports the timely detection and notification of impending IT problems across your Oracle Identity Management environment.

This chapter covers the following topics:

- [Monitoring Basics](#)
- [Monitoring Templates](#)
- [User-Defined Metrics](#)
- [Real-Time Performance Charts](#)

Monitoring Basics

System monitoring functionality permits unattended monitoring of your IT environment. The Management Pack Plus for Identity Management in Enterprise Manager comes with a comprehensive set of performance and health metrics that allows monitoring of key components in your Oracle Identity Management environment, such as Access Manager – Access Server, Access Manager – Identity Server, Identity Manager Server, Identity Federation Server, as well as the underlying hosts on which they run.

The collected performance metrics for the monitored Oracle Identity Management targets are described in the [Oracle Identity Management Performance Metrics](#) section.

For information about collected performance metrics for the underlying hosts please refer to the Host section of the *Enterprise Manager Framework, Host, and Services Metric Reference Manual*:

(http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b16230/toc.htm).

The Management Agent on each monitored host monitors the status, health, and performance of all managed components (also referred to as targets) on that host. If a target goes down, or if a performance metric crosses a warning or critical threshold, an alert is generated and sent to Enterprise Manager and to Enterprise Manager administrators who have registered interest in receiving such notifications.

Systems monitoring functionality and the mechanisms that support this functionality are discussed in the following sections:

- [Out-of-Box Monitoring](#)
- [Metric Baselines](#)
- [Alerts](#)
- [Notifications](#)
- [Corrective Actions](#)
- [Blackouts](#)

Out-of-Box Monitoring

Enterprise Manager's Management Agents automatically start monitoring their host's systems (including hardware and software configuration data on these hosts) as soon as they are deployed and started. Metrics from all monitored components are stored and aggregated in the Management Repository, providing administrators with a rich source of diagnostic information and trend analysis data. When critical alerts are detected, notifications are sent to administrators for rapid resolution.

Out-of-box, Enterprise Manager monitoring functionality provides:

- In-depth monitoring with Oracle-recommended metrics and thresholds.
- Access to real-time performance charts.
- Collection, storage, and aggregation of metric data in the Management Repository. This allows you to perform strategic tasks such as trend analysis and reporting.
- E-mail notification for detected critical alerts.

The Management Pack Plus for Identity Management in Enterprise Manager monitors all critical components in your Oracle Identity Management environment.

Some examples of monitored metrics are:

- Successful/Failed Authentications and Authorizations (Oracle Access Manager – Access Server)
- Successful/Failed Requests (Oracle Access Manager – Identity Server)
- Application Response Time (Oracle Identity Manager Server)
- Number of Provisioned Users, Number of Users Deleted/Disabled/Locked (Oracle Identity Manager Repository)
- Identity Provider & Service Provider Metrics (Oracle Identity Federation Server)
- LDAP Server Load, Total Users Sessions (Oracle Internet Directory)
- Network Interface Total I/O Rate (Host)

Perform the following steps to view all metrics collected for a monitored Oracle Identity Management target:

1. Click the **Targets** tab on the Enterprise Manager Console.

2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Identity Management targets. For instance, if you would like to view the collected metrics for Access Manager – Access Server, click on the target of type **Access Manager – Access Server**.
4. Click on the **All Metrics** link in the **Related Links** section.

Some metrics have associated predefined limiting parameters called thresholds that cause alerts to be triggered when collected metric values exceed these limits. Enterprise Manager allows you to set metric threshold values for two levels of alert severity:

- **Warning** - Attention is required in a particular area, but the area is still functional.
- **Critical** - Immediate action is required in a particular area. The area is either not functional or indicative of imminent problems.

Perform the following steps to change the warning and critical thresholds of performance metrics for a monitored Oracle Identity Management target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Identity Management targets. For instance, if you would like to change performance metrics thresholds for Access Manager - Access Server, click on the target of type **Access Manager - Access Server**.
4. Click on the **Metric and Policy Settings** link in the **Related Links** section.

In addition to monitoring your Oracle Identity Management environment from a system perspective, you may also monitor your environment from a service-oriented perspective using Grid Control's Service Level Management framework – please view the [Service Level Management](#) section for more information about Service Level Management.

You can define metrics to measure the performance of the service. You can add performance metrics from any of the key components that are critical for running the service. Once you've added metrics, you can define thresholds, which, when exceeded, will generate alerts.

Perform the following steps to add performance metrics based on any of the key components and change the warning and critical thresholds for the selected metrics:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. From the **View** drop-down menu, select **Systems and Services**.
4. Click on one of the Oracle Identity Management Service targets of type **Generic Service**. For more information, please see the [Creating Generic Service or Web Application Targets for Identity Management](#) section.
5. Click on the **Monitoring Configuration** tab.
6. Click on the **Performance Metrics** link.
7. Select **Based on System** from the **Add** dropdown list and click on the **Go** button.
8. Select the Oracle Identity Management target that you would like to monitor from the **Target Type** dropdown list, and then select the desired performance metric from the **Metric** dropdown list. Click **Continue** to proceed.

9. Define the **Warning Threshold** and **Critical Threshold** for the selected performance metric and click **OK** to save your changes.

Metric Baselines

Metric baselines are statistical characterizations of system performance over well-defined time periods. Metric baselines can be used to implement adaptive alert thresholds for certain performance metrics as well as provide normalized views of system performance. Adaptive alert thresholds are used to detect unusual performance events. Baseline normalized views of metric behavior help administrators explain and understand such events. Metric baselines are well defined time intervals (baseline periods) over which Enterprise Manager has captured system performance metrics. The underlying assumption of metric baselines is that systems with relatively stable performance should exhibit similar metric observations (that is, values) over times of comparable workload.

Two types of baseline periods are supported: moving window baseline periods and static baseline periods. Moving window baseline periods are defined as some number of days prior to the current date (example: Last 7 days). This allows comparison of current metric values with recently observed history. Moving window baselines are useful for operational systems with predictable workload cycles (example: OLTP days and batch nights). Static baselines are periods of time that you define that are of particular interest to you (example: end of the fiscal year). These baselines can be used to characterize workload periods for comparison against future occurrences of that workload (example: compare end of the fiscal year from one calendar year to the next).

Once metric baselines are defined, they can be used to establish alert thresholds that are statistically significant and adapt to expected variations across time. For example, you can define alert thresholds to be generated based on significance level, such as the HIGH significance level thresholds are values that occur 5 in 100 times. Alternatively, you can generate thresholds based on a percentage of the maximum value observed within the baseline period. These can be used to generate alerts when performance metric values are observed to exceed normal peaks within that period.

Note:

Metric baselines are supported for the Oracle Identity Management Service of type **Generic Service** only – other Oracle Identity Management targets do not support metric baselines.

Perform the following steps to customize metric baselines for the Oracle Identity Management Service of type **Generic Service**:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. From the **View** drop-down menu, select **Systems and Services**.
4. Click on the Oracle Identity Management Service target of type **Generic Service**.
5. Click on the **Monitoring Configuration** tab.
6. Click on the **Metric Baselines** link in the **Related Links** section.

Alerts

When a metric threshold value is reached, an alert is generated. An alert indicates a potential problem; either a warning or critical threshold for a monitored metric has been crossed. An alert can also be generated for various target availability states, such as:

- Target is down.
- Oracle Management Agent monitoring the target is unreachable.

For information about defining warning and critical thresholds, please refer to the [Out-of-Box Monitoring](#) section.

When an alert is generated, you can access details about the alert from the Enterprise Manager console. In the **All Targets Alerts** section of the Enterprise Manager home page, you can view **Critical Alerts**, **Warning Alerts** and **Errors** for all monitored targets. You can also view a summary of alerts for monitored Oracle Identity Management targets on the **Identity and Access** page.

The home page of any of the monitored Oracle Identity Management targets lists the alerts specific to that target. You may also view a history of alerts for diagnostics purposes.

Perform the following steps to view alert history for a monitored Oracle Identity Management target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Identity Management targets. For instance, if you would like to view alert history for Access Manager - Access Server, click on the target of type **Access Manager - Access Server**.
4. Click on **Alert History** link in the Related Links section.

Enterprise Manager provides various options to respond to alerts. Administrators can be automatically notified when an alert triggers and/or corrective actions can be set up to automatically resolve an alert condition.

For information about setting up notifications, please refer to the [Notifications](#) section.

For information about setting up corrective actions, please refer to the [Corrective Actions](#) section.

Notifications

When a target becomes unavailable or if thresholds for performance are crossed, alerts are generated in the Enterprise Manager console and notifications are sent to the appropriate

administrators. Enterprise Manager supports notifications via e-mail (including e-mail-to-page systems), SNMP traps, and/or by running custom scripts.

Enterprise Manager supports these various notification mechanisms via notification methods. A notification method is used to specify the particulars associated with a specific notification mechanism, for example, which SMTP gateway(s) to use for e-mail, which OS script to run to log trouble-tickets, and so on. Super Administrators perform a one-time setup of the various types of notification methods available for use. Once defined, other administrators can create notification rules that specify the set of criteria that determines when a notification should be sent and how it should be sent. The criteria defined in notification rules include the targets, metrics and severity states (clear, warning or critical) and the notification method that should be used when an alert occurs that matches the criteria. For example, you can define a notification rule that specifies e-mail should be sent to you when CPU Utilization on any host target is at critical severity, or another notification rule that creates a trouble-ticket when any database is down. Once a notification rule is defined, it can be made public for sharing across administrators. For example, administrators can subscribe to the same rule if they are interested in receiving alerts for the same criteria defined in the rule. Alternatively, an Enterprise Manager Super Administrator can assign notification rules to other administrators such that they receive notifications for alerts as defined in the rule.

Notifications are not limited to alerting administrators. Notification methods can be extended to execute any custom OS script or PL/SQL procedure, and thus can be used to automate any type of alert handling. For example, administrators can define notification methods that call into a trouble ticketing system, invoke third-party APIs to share alert information with other monitoring systems, or log a bug against a product.

Perform the following steps to customize notifications:

1. Click the **Setup** link on the Enterprise Manager Console (located in the upper right section).
2. Click on the **Notification Methods** tab.
3. Enter information required for the Mail Server and add the desired notification methods

Corrective Actions

Corrective actions allow you to specify automated responses to alerts. Corrective actions ensure that routine responses to alerts are automatically executed; thereby saving administrator time and ensuring problems are dealt with before they noticeably impact users. For example, if Enterprise Manager detects that a component, such as the Identity Manager Server is down, a corrective action can be specified to automatically run an OS command to start it back up. A corrective action is thus any task you specify that will be executed when a metric triggers a warning or critical alert severity. By default, the corrective action runs on the target on which the alert has triggered. Administrators can also receive notifications for the success or failure of corrective actions.

Corrective actions for a target can be defined by all Enterprise Manager administrators who have been granted OPERATOR or greater privilege on the target. For any metric, you can define different corrective actions when the metric triggers at warning severity or at critical severity.

Corrective actions must run using the credentials of a specific Enterprise Manager administrator. For this reason, whenever a corrective action is created or modified, the credentials that the modified action will run with must be specified.

Perform the following steps to set up corrective actions based on performance metrics for a monitored Oracle Identity Management target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Identity Management targets. For instance, if you would like to set up corrective actions based on performance metrics thresholds for Access Manager - Access Server, click on the target of type **Access Manager - Access Server**.
4. Click on the **Metric and Policy Settings** link in the **Related Links** section.
5. Click on the **Edit** link for the performance metric for which you would like to set up corrective action.
6. Click on the **Add** button in the **Corrective Actions** section to add corrective actions for either critical or warning thresholds.

Blackouts

Blackouts allow you to support planned outage periods to perform emergency or scheduled maintenance. When a target is put under blackout, monitoring is suspended, thus preventing unnecessary alerts from being sent when you bring down a target for scheduled maintenance operations such as database backup or hardware upgrade. Blackout periods are automatically excluded when calculating a target's overall availability.

A blackout period can be defined for individual targets, a group of targets or for all targets on a host. The blackout can be scheduled to run immediately or in the future, and to run indefinitely or stop after a specific duration. Blackouts can be created on an as-needed basis, or scheduled to run at regular intervals. If, during the maintenance period, you discover that you need more (or less) time to complete maintenance tasks, you can easily extend (or stop) the blackout that is currently in effect. Blackout functionality is available from both the Enterprise Manager console as well as via the Enterprise Manager command-line interface (EMCLI). The EMCLI is often useful for administrators who would like to incorporate the blacking out of a target within their maintenance scripts. When a blackout ends, the Management Agent automatically re-evaluates all metrics for the target to provide current status of the target post-blackout.

If an administrator inadvertently performs scheduled maintenance on a target without first putting the target under blackout, these periods would be reflected as target downtime instead of planned blackout periods. This has an adverse impact on the target's availability records. In such cases, Enterprise Manager allows Super Administrators to go back and define the blackout period that should have happened at that time. The ability to create these retroactive blackouts provides Super Administrators with the flexibility to define a more accurate picture of target availability.

Perform the following steps to set up blackouts for a monitored Oracle Identity Management target:

1. Click the **Setup** link on the Enterprise Manager Console (located in the upper right section).
2. Click on the **Blackouts** tab.
3. Click on the **Create** button to launch a blackout wizard.
4. Select the desired target types and enter all the requested information

Monitoring Templates

Monitoring templates simplify the task of standardizing monitoring settings across your enterprise by allowing you to specify the monitoring settings once and apply them to your monitored targets. This makes it easy for you to apply specific monitoring settings to specific classes of targets throughout your enterprise. For example, you can define one monitoring template for test databases and another monitoring template for production databases.

A monitoring template defines all Enterprise Manager parameters you would normally set to monitor a target, such as:

- Target type to which the template applies.
- Metrics (including user-defined metrics), thresholds, metric collection schedules, and corrective actions.

When a change is made to a template, you can reapply the template across affected targets in order to propagate the new changes. You can reapply the monitoring templates as often as needed. For any target, you can preserve custom monitoring settings by specifying metric settings that can never be overwritten by a template.

Perform the following steps to set up blackouts for a monitored Oracle Identity Management target:

1. Click the **Setup** link on the Enterprise Manager Console (located in the upper right section).
2. Click on the **Monitoring Templates** tab.
3. Click on the **Create** button to launch a monitoring template wizard.
4. Select the desired target and click **Continue**.
5. Enter the information requested (including Warning and Critical Thresholds) and click **OK** to save your settings.

User-Defined Metrics

User-defined metrics allow you to extend the reach of Enterprise Manager's monitoring to conditions specific to particular environments via custom scripts. Once a user-defined metric is defined, it will be monitored, aggregated in the repository, and can trigger alerts like any other metric in Enterprise Manager. The supported user-defined metrics in the Management Pack Plus for Identity Management are the one created at the host-level (Operating System). Operating System (OS) User-Defined Metrics can be accessed from Host target home pages and allow you to implement custom monitoring functions via OS scripts.

Perform the following steps to set up user-defined metrics for the underlying hosts supporting the Oracle Identity Management environment:

1. Click the **Targets** tab on the Enterprise Manager Console.

2. Click the **All Targets** tab.
3. Click on the target of type **Host** on which Oracle Identity Management components are running.
4. Click on the **User-Define Metrics** link in the **Related Links** section.
5. Click on the **Create** button to create a new user-define metric
6. Enter all the requested information and click **OK** to save your changes.

If you already have your own library of custom monitoring scripts, you can leverage Enterprise Manager's monitoring features by integrating these scripts with Enterprise Manager as OS user-defined metrics.

Real-Time Performance Charts

Real-time performance charts are available for all monitored Oracle Identity Management targets. The performance charts displayed are based on performance metrics collected by Enterprise Manager.

In Oracle Enterprise Manager Grid Control 11gR1, customizable performance summaries are available for Oracle Identity Management 11gR1 targets with a “Metric Palette” that allows users to drag and drop performance charts. Additionally, drill-downs into usage and performance statistics are available for:

- Oracle Identity Federation Providers – showing authentication requests and responses, HTTP and SOAP requests and responses, and authentication response processing time
- Oracle Internet Directory User Statistics – showing failed and completed LDAP operations like Add/Bind/Compare/Delete/Modify/Search
- Directory Integration Platform Synchronization and Provisioning Profiles – showing job status, successful/skipped/failed changes, completion time, and errors

The collected performance metrics for the monitored Oracle Identity Management targets are described in the [Oracle Identity Management Performance Metrics](#) section.

Configuration Management

This chapter explains how Enterprise Manager Grid Control simplifies the monitoring and management of Oracle Access Manager targets in your enterprise through Configuration Management.

For more information about Configuration Management, please refer to the Enterprise Configuration Management section of the *Enterprise Manager Concepts Guide*:
http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b31949/toc.htm

Configuration Management allows you to view, save, track, compare, and search the configuration information stored in the Management Repository for the monitored Oracle Identity Management targets. The ability to compare configuration settings is useful in diagnostic situations when administrators need to find out what parameter has changed, or how two servers or server components differ from each other. Configuration Management is also useful in achieving regulatory compliance cost effectively, as it could be extremely tedious and error prone to try to keep track of changes manually.

Note:

The Management Pack Plus for Identity Management supports configuration management for the monitored Oracle Access Manager 10g targets: *Access Manager – Access Server* and *Access Manager – Identity Server*, as well as Oracle Identity Management 11gR1 targets: *Oracle Internet Directory*, *Oracle Virtual Directory*, *Identity Federation Server*, and *Directory Integration Platform Server*.

This section covers the following topics:

- [Viewing Configurations](#)
- [Comparing Configurations](#)
- [Configuration History](#)

Viewing Configurations

Using the Management Pack Plus for Identity Management, you can perform the following actions for monitored Oracle Access Manager targets: *Access Manager – Access Server* and *Access Manager – Identity Server*.

- View the last collected and saved configuration
- Save configurations to a configuration file (XML file) or to the Management Repository
- Search collected configuration data
- View the history of configuration changes
- Compare configurations (refer to "[Comparing Configurations](#)" in this chapter for more detailed information)

Perform the following steps to view configuration of a monitored Oracle Identity Management target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Access Manager targets. For instance, if you would like to view configuration for Access Manager – Access Server, click on the target of type **Access Manager – Access Server**.
4. Click on the **View Configuration** link in the **Configuration** section.
5. To save a “snapshot” of the current configuration, click on the **Save** button.
6. You may select “Save to Enterprise Manager Repository” or “Export to File”. Click **OK** to continue.

Comparing Configurations

Grid Control gives you the tools to perform comparisons between configurations of the same target type. These comparisons are useful for quickly finding similarities and differences between two or more configurations.

You can compare:

- Two configurations in the Management Repository
- Two saved configuration files
- One configuration to multiple configurations
- A configuration in the Management Repository to a saved configuration file

When two target configurations are compared, all categories of collected configuration information are included. Grid Control presents the summary results of the comparison in a tabular format. More information that is detailed is available by drilling down from those summary results.

Perform the following steps to compare configurations of a monitored Oracle Access Manager target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Access Manager targets. For instance, if you would like to compare configurations for Access Manager – Access Server, click on the target of type **Access Manager – Access Server**.
4. Click on the **Compare Configuration** link in the **Configuration** section.
5. You may select another target (in this case, another Access Manager – Access Server) for comparison or click on **Saved Configurations** to launch a comparison between the current configuration and an already saved configuration snapshot.
6. To compare the current configuration to multiple snapshots, click on **Compare Multiple Configurations** link in the **Configuration** section of the Access Manager – Access Server target home page.

Configuration History

Grid Control gives you the tools to view the history of configuration changes for all monitored Oracle Access Manager targets.

Perform the following steps to view configuration history of a monitored Oracle Access Manager target:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **Identity and Access** tab. *Note:* If the Identity and Access sub-tab is not shown, please add it by clicking on Preferences > Target Subtabs.
3. Click on one of the Oracle Access Manager targets. For instance, if you would like to view configuration history for Access Manager – Access Server, click on the target of type **Access Manager – Access Server**.
4. Click on the **Configuration History** link in the **Configuration** section.

5. From the **View History Records** dropdown menu, select **Show All** to view all the configuration changes that occurred in Access Manager – Access Server
6. Click on the **Details** link to view more information about a specific change
7. The configuration changes can also be saved to a CSV file by clicking on the **Save to File** button.

The change history audit trail is useful not only for diagnostic purposes, but also for compliance, as laws such as SOX and HIPAA require traceability of changes at all levels of the application stack. Because changes are tracked automatically, it makes compliance a lot easier, quicker and less expensive to implement.

Service Level Management

In addition to monitoring performance metrics for each individual Oracle Identity Management target, you may also monitor your environment from a service-oriented perspective using Grid Control's Service Level Management.

With the Management Pack Plus for Identity Management, users can create targets of type **Generic Service** or **Web Application** associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, and Identity Manager System. The Web Application or Generic Service target provides an end-to-end service oriented view of the monitored Oracle Identity Management targets with access to performance and usage metrics, service tests, service level rules, service availability definition, alerts, charts, and topology view.

For more information about Service Level Management, please refer to the Service Management section of the *Enterprise Manager Concepts Guide*:

http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b31949/toc.htm

Enterprise Manager Grid Control provides a comprehensive monitoring solution that helps you to effectively manage services from the overview level to the individual component level. When a service fails or performs poorly, Grid Control provides diagnostics tools that help to resolve problems quickly and efficiently, significantly reducing administrative costs spent on problem identification and resolution. Finally, customized reports offer a valuable mechanism to analyze the behavior of the applications over time.

Service Level Management is discussed in the following sections:

- [Service Tests and Beacons](#)
- [Performance and Usage](#)
- [Availability](#)
- [Service-Level Rules](#)
- [Topology View](#)
- [Service Performance](#)
- [Reports](#)

Service Tests and Beacons

Service tests are functional tests that are defined by Enterprise Manager administrators to represent end user tasks, and are used to determine the availability and performance of a

service. The availability of a service is defined in terms of the successful execution of either all or at least one of the 'key' service tests defined for the service.

For the Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation, an administrator can define a combination of one or more navigation paths within the application to be used as the criteria for determining the service's availability. For example, Oracle Access Manager requires that a user successfully log on (i.e. a user is successfully authenticated and authorized) for the service to be considered available. Enterprise Manager uses these logical tasks or 'transactions' to define the availability of a Web application. These critical paths of business processes for Web applications are recorded, and the stored transaction or 'service test' can be launched at a user-defined interval from strategic locations across the user-base.

Availability using service tests are monitored from various global user communities within the network. A service may be unavailable for all users or it may be a problem that is impacting users contained only within a specific network or location. To determine application availability from different end-points, 'beacons' are used to play back service tests at specified intervals from various locations that are representative of your user communities. Beacons are client robots that collect availability and performance data at specified intervals at strategic locations in the network.

Perform the following steps to add a beacon:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the target of type **Agent** on which you would like to create a beacon
4. From the **Add** dropdown list, select **Beacon** and click on the **Go** button.

Perform the following steps to record a web transaction with critical paths as a service test:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service** or **Web Application**. For more information, please see the [Creating Generic Service or Web Application Targets for Identity Management](#) section.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Service Tests and Beacons** link.
6. From the **Service Tests** section, select **Web Transaction** from the **Test Type** dropdown list and click on the **Add** button. *Note:* You can also select **LDAP Service Tests** allowing you to execute Search/Compare operations against an LDAP Server – e.g. OID and OVD.
7. Click on the **Go** button to Record a Transaction
8. Click on the **Record** button and navigate through the critical paths in your web-browser. Close the web-browser when you are done and click on the **Continue** button.
9. Verify the recorded steps and click on the **Continue** button.
10. Select either **Browser Simulation** or **Request Simulation** as the **Playback Mode**. Refer to [Request Simulation vs. Browser Simulation](#) section for more information about the differences between the two playback modes.
11. Verify all the information and click **OK** to save your service test.
12. From the **Beacons** section, click on the **Add** button.
13. Select the desired beacon and click on the **Select** button.

14. To enable your newly created service test, select your service test from the **Service Tests** section and click on the **Enable** button.

Perform the following steps to configure an LDAP service test:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service**. For more information, please see the [Creating Generic Service or Web Application Targets for Identity Management](#) section.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Service Tests and Beacons** link.
6. From the **Service Tests** section, select **LDAP** from the **Test Type** dropdown list and click on the **Add** button.
7. Fill in the information requested on the page – including username/password, Search Base, and Compare Attribute Name/Value.
8. Verify all the information and click **OK** to save your service test.

Request Simulation vs. Browser Simulation

The **Request Simulation** mode in Grid Control 10.2.0.4 is equivalent to the web transaction monitoring capability in Grid Control 10.2.0.3.

In Grid Control 10.2.0.3, when a web transaction is recorded, the web transaction monitoring capability records all the HTTP requests that the browser made. The Beacon plays back a web transaction by sending an equivalent set of HTTP requests. Due to the dynamic nature of HTTP requests (especially session specific parameters), the request simulation approach may not be suitable for certain web transactions because requests that contain parameters only relevant to the recording session may not be recorded.

In Grid Control 10.2.0.4, a new mode of playback: **Browser Simulation** was introduced. When a web transaction is recorded, all the HTTP requests, as well as the mouse and keyboard actions are recorded. A Beacon plays back a web transaction by either sending HTTP requests (Request Simulation) or by opening a browser and performing these mouse and keyboard actions (Browser Simulation). For example, data entry in a text field, mouse click on a button, etc.

At the end of the web transaction recording, a user needs to pick a playback mode – (Request Simulation or Browser Simulation) based on a simple heuristic.

Steps to verify the Request Simulation mode is suitable after recording:

1. Select the radio button **Request Simulation**.
2. Click **Play** next to the selection.
3. Observe the playback flow. Pay attention to any abnormal pages.
4. Click **Verify Service Test**, this may take a while depends on the complexity of the test.
5. Make sure the beacon reports the status as Up.
6. Click **Continue** to go back to the web transaction creation screen.

Steps to verify the Browser Simulation mode is suitable after recording:

1. Make sure you have Grid Control 10.2.0.4 Agent running on Windows XP Platform for the selected beacon. The Browser Simulation playback mode is supported on Windows XP beacons only – Browser Simulation is not supported on Windows 2000/2003 beacons. For information about setting up Windows XP beacons to support Browser Simulation, please refer to the [Troubleshooting the Management Pack Plus for Identity Management](#) section.
2. Select the radio button **Browser Simulation**.
3. Click **Play** next to the selection.
4. Observe the playback flow. Again, pay attention to any abnormal pages.
5. If the play seems to work successfully, save the web transaction.

Performance and Usage

You can define metrics to measure the performance and usage of the service. Performance indicates the response time of the service as experienced by the end user. Usage metrics are based on the user demand or load on the system. Once you've added metrics, you can define thresholds, which, when exceeded, will generate alerts.

Additionally, the charts for the performance and usage metrics that you define will be displayed in the **Charts** page (sub-tab).

Finally, the performance metrics that you add will be available for defining the Availability of the service as discussed in the following section.

Perform the following steps to add performance metrics:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service** or **Web Application**.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Performance Metrics** link.
6. You may select **Based on System** or **Based on Service Test** from the **Add** dropdown list. Click on the **Go** button.
7. Define the **Warning Threshold** and **Critical Threshold** for the selected performance metric and click **OK** to save your changes.

Perform the following steps to add usage metrics:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service** or **Web Application**.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Usage Metrics** link.
6. Click on the **Add** button and select the desired usage metrics.

7. Define the **Warning Threshold** and **Critical Threshold** for the selected performance metric and click **OK** to save your changes.

Availability

"Availability" of a service is a measure of the end users' ability to access the service at a given point in time. However, the rules of what constitutes availability may differ from one application to another. For example, for a Customer Relationship Management (CRM) application, availability may mean that a user can successfully log on to the application and access a sales report. For an online store, availability may be monitored based on whether the user can successfully log in, browse the store, and make an online purchase.

Grid Control allows you to define the availability of your service based on service tests or systems.

- **Service Test-Based Availability:** Choose this option if the availability of your service is determined by the availability of a critical functionality to your end users. While defining a service test, choose the protocol that most closely matches the critical functionality of your business process, and beacon locations that match the locations of your user communities. You can define one or more service tests using standard protocols and designate one or more service tests as "Key Tests." These key tests can be executed by one or more "Key Beacons" in different user communities. A service is considered available if one or all key tests can be executed successfully by at least one beacon, depending on your availability definition.
- **System-Based Availability:** Your service's availability can alternatively be based on the underlying system that hosts the service. Select the components that are critical to running your service and designate one or more components as "Key Components," which are used to determine the availability of the service. The service is considered available as long as at least one or all key components are up and running, depending on your availability definition.

Perform the following steps to define the availability of a service:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service** or **Web Application**.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Availability Definition** link.
6. You may select **Service Test** or **System** from the **Define Availability Based On** dropdown list.
7. Enter the request information and click **OK** to save your changes.

Service-Level Rules

Service-level parameters are used to measure the quality of the service. These parameters are usually based on actual service-level agreements or on operational objectives.

Grid Control's Service Level Management feature allows you to proactively monitor your enterprise against your service-level agreements to verify that you are meeting the availability, performance, and business needs within the service's business hours. For service-level agreements, you may want to specify the levels according to operational or contractual objectives.

By monitoring against service levels, you can ensure the quality and compliance of your business processes and applications.

Perform the following steps to edit service-level rule for a service:

1. Click the **Targets** tab on the Enterprise Manager Console.
2. Click the **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service** or **Web Application**.
4. Click on the **Monitoring Configuration** tab.
5. Click on the **Edit Service Level Rule** link from the **Related Links** section.
6. Enter the request information and click **OK** to save your changes.

Topology View

Use the **Topology** page (sub-tab), to view the dependencies between the service, its system components, and other services that define its availability. Upon service failure, the potential causes of failure, as identified by Root Cause Analysis, are highlighted in the topology view. In the topology, you can view dependent relationships between services and systems.

Service Performance

Grid Control provides a graphical representation of the historic and current performance and usage trends in the **Charts** page (sub-tab). You can view metric data for the current day (24 hours), 7 days, or 31 days. The thresholds for any performance or usage alerts generated during the selected period are also displayed in the charts. This helps you to easily track the performance and usage of the service test or system over time and investigate causes of service failure.

Use the **Test Performance** page (sub-tab) to view the historical and current performance of the service tests from each of the beacons. If a service test has been defined for this service, then the response time measurements as a result of executing that service test can be used as a basis for the service's performance metrics. It is possible to have multiple response time measurements if the service access involves multiple steps or the service provides multiple business functions. Alternatively, performance metrics from the underlying system components can also be used to measure performance of a service.

If performance of a service seems slow, it may be due to high usage of the service. Monitoring the service usage helps diagnose poor performance by indicating whether the service is affected by high usage of a system component.

Reports

Enterprise Manager provides out-of-box reports that are useful for monitoring services and Web applications. You can also set the publishing options for reports so that they are sent out via email at a specified period of time.

For information about creating Services Monitoring Dashboards, please see the [Creating a Service Dashboard Report](#) section.

Additionally, Enterprise Manager provides an out-of-box report for Oracle Internet Directory. Perform the following steps to view the usage statistics report for Oracle Internet Directory:

1. Click on the **Reports** tab.
2. Select **Oracle Internet Directory** from the **Target Type** drop-down menu.

ORACLE Enterprise Manager
Grid Control 11g

Report Definitions

Search

Title:
 Owner:
 Target Type:
 Target Name:

[Expand All](#) | [Collapse All](#)

Select Title

☐	▼ Reports
-----------------------	-----------

3. Select the **User Operation Statistics** report.

☐	▼ LDAP Directory Server
☐	<u>User Operation Statistics</u>
☐	▼ Policy Groups

4. Enter the hostname for the Oracle Internet Directory and click **Continue**

Specify Target for Report

Report **User Operation Statistics**

Specify a Oracle Internet Directory to include in this report.

Oracle Internet Directory 

5. View the report

ORACLE Enterprise Manager
Grid Control 11g

Home Target

User Operation Statistics

Oracle Internet Directory **/im11ps2_IM11PS2Domain/asinst_ps2/oid1**
Time Period **Last 24 Hours PDT** [Set Time Period](#)

Summary Operation Counts of Monitored Users

USER_DN	TOTAL	TOTAL_BIND	TOTAL_COMPARE	TOTAL_SEARCH	TOTAL_ADD	TOTAL_MODIFY	TOTAL_MODRDN	TOTAL_DELETE	TOTAL_ABANDON	TOTAL_UNBIND
	0	0	0	0	0	0	0	0	0	0

Detailed Bind Operation Counts of Monitored Users

USER_DN	TOTAL_BIND	BIND_SUCC	BIND_FAIL	PROXYBIND_SUCC	PROXYBIND_FAIL	UNBIND
	0	0	0	0	0	0

Detailed Compare and Search Operation Counts of Monitored Users

USER_DN	COMPARE_SUCC	COMPARE_FAIL	BASE_SRCH_SUCC	BASE_SRCH_FAIL	ONE_LVL_SRCH_SUCC	ONE_LVL_SRCH_FAIL	SUB_SRCH_SUCC	SUB_SRCH_FAIL
	0	0	0	0	0	0	0	0

Detailed Other LDAP Operation Counts of Monitored Users

USER_DN	ADD_SUCC	ADD_FAIL	DELETE_SUCC	DELETE_FAIL	MODIFY_SUCC	MODIFY_FAIL	MODRDN_SUCC	MODRDN_FAIL	ABANDON
	0	0	0	0	0	0	0	0	0

For more information about Service Level Management, please refer to the Information Publisher section of the *Enterprise Manager Concepts Guide*:

http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b31949/toc.htm

Oracle Identity Management Performance Metrics

Performance metrics are collected for all the monitored Oracle Identity Management targets. This section describes all the performance metrics collected and provides some guidelines for using performance metrics.

- [Access Manager – Access Server 10g](#)
- [Access Manager – Identity Server 10g](#)
- [Identity Manager Server 9.1.x](#)
- [Identity Manager Repository 9.1.x](#)
- [Identity Federation Server 10g](#)
- [Oracle Internet Directory 11g](#)
- [Directory Integration Platform Server 11g](#)
- [Oracle Virtual Directory 11g](#)
- [Identity Federation Server 11g](#)

- [Oracle Adaptive Access Manager Server 11g](#)
- [Oracle Adaptive Access Manager Cluster 11g](#)
- [Oracle Access Manager Server 11g](#)
- [Oracle Access Manager Cluster 11g](#)
- [Oracle Identity Manager Server 11g](#)
- [Oracle Identity Manager Cluster 11g](#)
- [Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g](#)

Access Manager – Access Server 10g

The metrics collected for the Access Manager – Access Server are shown in [Table 4](#). The performance metrics for the Access Manager – Access Server are exposed via the SNMP Agent.

Table 4 Access Manager – Access Server 10g Metrics

Metric	Managed Object	Description	Metric Collection
Audit Log Rotation Time			
Audit Log Rotation Time	aaaTimeAuditLogWasRotatedOID	Time when the audit log file was rotated. This setting is determined in the configuration for this Access Server specified in the Access System Console.	SNMP Agent
Audit Request			
Number of Audit Requests	aaaAuditRequestsOID	The number of audit requests made by this Access Server instance.	SNMP Agent
Directory Server Live Connection			
Directory Server Live Connection	aaaDirectoryServerNoOfLiveConnectionsOID	The number of connections against the directory.	SNMP Agent
Failed Authentications			
Failed Authentications (Since Last Collection)	aaaAuthenticationsDeniedOID	The number of unsuccessful authentications by the Access Server instance - since last collection.	SNMP Agent
Total Failed Authentications	aaaAuthenticationsDeniedOID	The total number of unsuccessful authentications by the Access Server instance.	SNMP Agent + Computed
Failed Authentications (%)			
Failed Authentications (%) (Since Last Collection)	aaaAuthenticationsDeniedOID	The percentage of unsuccessful authentications by the Access Server instance - since last collection.	SNMP Agent + Computed
Total Failed Authentications (%)	aaaAuthenticationsDeniedOID	The total percentage of unsuccessful authentications by the Access Server instance.	SNMP Agent + Computed
Failed Authorizations			
Failed Authorizations (Since Last Collection)	aaaAuthorizationsDeniedOID	The number of unsuccessful authorizations by the Access Server instance - since last collection.	SNMP Agent
Total Failed Authorizations	aaaAuthorizationsDeniedOID	The total number of unsuccessful authorizations by the Access Server instance.	SNMP Agent + Computed

Failed Authorizations (%)			
Failed Authorizations (%) (Since Last Collection)	aaaAuthorizationsDeniedOID	The percentage of unsuccessful authorizations by the Access Server instance - since last collection.	SNMP Agent + Computed
Total Failed Authorizations (%)	aaaAuthorizationsDeniedOID	The total percentage of unsuccessful authorizations by the Access Server instance.	SNMP Agent + Computed
Request Processed by Access Server			
Requests Processed (Since Last Collection)	coreidRequestsProcessedOID	The number of requests processed by the Access Server instance - since last collection	SNMP Agent
Total Requests Processed	coreidRequestsProcessedOID	The total number of requests processed by the Access Server instance	SNMP Agent + Computed
Resource Usage			
CPU Idle (%)	N/A	Percentage of Idle CPU Usage by the Access Server instance	Computed
CPU Other (%)	N/A	Percentage of "Other" CPU Usage by the Access Server instance	Computed
CPU Usage (%)	N/A	Percentage of Active CPU Usage by the Access Server instance	Computed
Free Memory (%)	N/A	Percentage of Free Memory available to the Access Server instance	Computed
Memory Usage (%)	N/A	Percentage of Memory Usage by the Access Server instance	Computed
Memory Usage (MB)	N/A	Memory Usage (MB) by the Access Server instance	Computed
Other Memory Usage (%)	N/A	Percentage of "Other" Memory Usage by the Access Server instance	Computed
Other Memory Usage (MB)	N/A	Other Memory Usage (MB) by the Access Server instance	Computed
Total Memory (MB)	N/A	Total Memory Usage (MB) by the Access Server instance	Computed
Response			
Status	N/A	Status of the Access Server instance	Computed
Successful Authentications			
Successful Authentications (Since Last Collection)	aaaAuthenticationsSuccessOID	The number of successful authentications by the Access Server instance - since last collection.	SNMP Agent
Total Successful Authentications	aaaAuthenticationsSuccessOID	The total number of successful authentications by the Access Server instance.	SNMP Agent + Computed
Successful Authentications (%)			
Successful Authentications (%) (Since Last Collection)	aaaAuthenticationsSuccessOID	The percentage of successful authentications by the Access Server instance - since last collection.	SNMP Agent + Computed
Total Successful Authentications (%)	aaaAuthenticationsSuccessOID	The total percentage of successful authentications by the Access Server instance.	SNMP Agent + Computed
Successful Authorizations			

Successful Authorizations (Since Last Collection)	aaaAuthorizationsSuccessfulOID	The number of successful authorizations by the Access Server instance - since last collection.	SNMP Agent
Total Successful Authorizations	aaaAuthorizationsSuccessfulOID	The total number of successful authorizations by the Access Server instance.	SNMP Agent + Computed
Successful Authorizations (%)			
Successful Authorizations (%) (Since Last Collection)	aaaAuthorizationsSuccessfulOID	The percentage of successful authorizations by the Access Server instance - since last collection.	SNMP Agent + Computed
Total Successful Authorizations (%)	aaaAuthorizationsSuccessfulOID	The total percentage of successful authorizations by the Access Server instance.	SNMP Agent + Computed
Up Since			
Up Since	aaaStartTimeOID	The date and time when this Access Server instance was last started.	SNMP Agent

Access Manager – Identity Server 10g

The metrics collected for the Access Manager – Identity Server are shown in [Table 5](#). The performance metrics for the Access Manager – Identity Server are exposed via the SNMP Agent.

Table 5 Access Manager – Identity Server 10g Metrics

Metric	Managed Object	Description	Metric Collection
Failed Cache Flush Requests			
Failed Cache Flush Requests (Since Last Collection)	coreidTotalNumOfCacheFlushRequestFailOID	The number of unsuccessful cache flush requests issued by the Identity Server - since last collection	SNMP Agent
Total Failed Cache Flush Requests	coreidTotalNumOfCacheFlushRequestFailOID	Total number of unsuccessful cache flush requests issued by the Identity Server	SNMP Agent + Computed
Directory Server Live Connection			
Directory Server Live Connection	aaaDirectoryServerNoOfLiveConnectionsOID	The number of connections against the directory.	SNMP Agent
Failed Logins			
Failed Logins (Since Last Collection)	coreidNumOfLoginsFailureOID	The number of failed login attempts to the Identity Server instance - since last collection.	SNMP Agent
Total Failed Logins	coreidNumOfLoginsFailureOID	Total number of failed login attempts to the Identity Server instance	SNMP Agent + Computed
Failed Requests			
Failed Requests (Since Last Collection)	coreidNumOfRequestsFailOID	The number of requests for this Identity Server that produced an error - since last collection	SNMP Agent + Computed
Total Failed Requests	coreidNumOfRequestsFailOID	Total number of requests for this Identity Server that produced an error	SNMP Agent + Computed
Failed Sent Emails			

Failed Sent Emails (Since Last Collection)	coreidNumOfEmailSentFailOID	The number of failed attempts to send email from this Identity Server instance - since last collection	SNMP Agent
Total Failed Sent Emails	coreidNumOfEmailSentFailOID	Total number of failed attempts to send email from this Identity Server instance	SNMP Agent + Computed
Request Processed by Identity Server			
Requests Processed (Since Last Collection)	coreidRequestsProcessedOID	The number of requests processed by the Identity Server instance - since last collection	SNMP Agent
Total Requests Processed	coreidRequestsProcessedOID	Total number of requests processed by the Identity Server instance	SNMP Agent + Computed
Resource Usage			
CPU Idle (%)	N/A	Percentage of Idle CPU Usage by the Identity Server instance	Computed
CPU Other (%)	N/A	Percentage of "Other" CPU Usage by the Identity Server instance	Computed
CPU Usage (%)	N/A	Percentage of Active CPU Usage by the Identity Server instance	Computed
Free Memory (%)	N/A	Percentage of Free Memory available to the Identity Server instance	Computed
Memory Usage (%)	N/A	Percentage of Memory Usage by the Identity Server instance	Computed
Memory Usage (MB)	N/A	Memory Usage (MB) by the Identity Server instance	Computed
Other Memory Usage (%)	N/A	Percentage of "Other" Memory Usage by the Identity Server instance	Computed
Other Memory Usage (MB)	N/A	Other Memory Usage (MB) by the Identity Server instance	Computed
Total Memory (MB)	N/A	Total Memory Usage (MB) by the Identity Server instance	Computed
Response			
Status	N/A	Status of the Identity Server instance	Computed
Successful Cache Flush Requests			
Successful Cache Flush Requests (Since Last Collection)	coreidTotalNumOfCacheFlushRequestSuccessOID	The number of successful cache flush requests issued by the Identity Server - since last collection	SNMP Agent
Total Successful Cache Flush Requests	coreidTotalNumOfCacheFlushRequestSuccessOID	Total number of successful cache flush requests issued by the Identity Server	SNMP Agent + Computed
Successful Logins			
Successful Logins (Since Last Collection)	coreidNumOfLoginsOID	The number of successful login attempts to the Identity Server instance - since last collection.	SNMP Agent
Total Successful Logins	coreidNumOfLoginsOID	Total number of successful login attempts to the Identity Server instance	SNMP Agent + Computed
Successful Requests			
Successful Requests (Since Last Collection)	coreidNumOfRequestsSuccessOID	The number of requests successfully handled by this Identity Server instance - since last collection	SNMP Agent

Total Successful Requests	coreidNumOfRequestsSuccessOID	Total number of requests successfully handled by this Identity Server instance	SNMP Agent + Computed
Up Since			
Up Since	aaaStartTimeOID	The date and time when this Identity Server instance was last started.	SNMP Agent
Average Service Time			
Average Service Time Per Request (Seconds)	coreidTotalServiceTimeOID, coreidRequestsProcessedOID	Computed Metric: Total time, in seconds, the Identity Server has taken to serve requests since the last restart (divided by) total number of requests processed by the Identity Server instance	SNMP Agent + Computed

Identity Manager Server 9.1.x

The metrics collected for the Identity Manager Server are shown in [Table 6](#).

Table 6 Identity Manager Server 9.1.x Metrics

Metric	Description
JDBC Metrics	
JDBC Connection Pool Name	JDBC Connection Pool Name
JTA Metrics	
Active JTA Transactions Count	Active JTA Transactions Count
Committed JTA Transactions Count	Committed JTA Transactions Count
Total JTA Transactions Count	Total JTA Transactions Count
JVM Metrics	
JVM Heap Usage	JVM Heap Usage
Java Vendor	Java Vendor
Java Version	Java Version
Load Metrics	
Active Invocations	Active Invocations
Active Sessions Count	Active Sessions Count
Performance	
Application Response Time	Application Response Time
Average Application Response Time	Average Application Response Time
Invocations Per Second	Invocations Per Second
Runtime Metrics	
Active Threads Count	Active Threads Count

CPU Load	CPU Load
Heap Usage	Heap Usage
Used Physical Memory	Used Physical Memory
Response	
Status	The status of the Identity Manager Server

Identity Manager Repository 9.1.x

The metrics collected for the Identity Manager Repository are shown in [Table 7](#).

Table 7 Identity Manager Repository 9.1.x Metrics

Metric	Description
Load Metrics	
Number of Users Created	Number of Users Created
Number of Reconciliation Events Initiated	Number of Reconciliation Events Initiated
Number of Requests Initiated	Number of Requests Initiated
Number of Scheduled Tasks Initiated	Number of Scheduled Tasks Initiated
Provisioning Metrics	
Number of Users Deleted	Number of Users Deleted
Number of Users Disabled	Number of Users Disabled
Number of Locked Users	Number of Locked Users
Number of Provisioned Users	Number of Provisioned Users
Remote Manager Metrics	
Host	Host
Message	Message
Service Name	Service Name
Status	The status of the Identity Manager Repository
Response	
Logon Time	Logon Time
Status Msg	Status Message

Scheduled Tasks Metrics	
Scheduled Task Execution Time	Scheduled Task Execution Time

Identity Federation Server 10g

The metrics collected for the Identity Federation Server are shown in [Table 8](#).

Table 8 Identity Federation Server 10g Metrics

Metric	Description
Response	
Status	Current Oracle Identity Federation Server availability (Up/Down)
Authentication Requests Sent by the Service Provider	
Authentication Requests Sent	Total number of authentication requests sent
Authentication Requests Sent Per Second	The rate at which authentications requests are sent: Total number of authentication requests sent per second
Signed Authentication Requests Sent	Total number of signed authentication requests sent
Authentication Requests Containing Allow Federation Creation Sent	Total number of authentication requests containing Allow Federation Creation sent
Authentication Response Sent by the Service Provider	
Authentication Response Failed	Total failed authentication requests
Authentication Response Sent	Total authentication requests sent
Authentication Response Sent Successfully	Total authentication requests sent successfully
Signed Authentication Response Sent	Total signed authentication requests sent
Successful Authentication Requests Sent By Service Provider (%)	The percentage of total authentication requests sent successfully
Authentication Requests Received by the Identity Provider	
Authentication Requests Received	Total number of authentication requests received
Authentication Requests Received Per Second	The rate at which authentications requests are received: Total number of authentication requests received per second
Signed Authentication Requests Received	Total number of signed authentication requests received

Authentication Requests Containing Allow Federation Creation Received	Total number of authentication requests containing Allow Federation Creation received
Authentication Response Received by the Identity Provider	
Authentication Response Failed	Total failed authentication requests
Authentication Response Received	Total authentication requests received
Authentication Response Received Successfully	Total authentication requests received successfully
Signed Authentication Response Received	Total signed authentication requests received
Successful Authentication Requests Received By Identity Provider (%)	The percentage of total authentication requests received successfully
Federation Termination Requests Sent by the Service Provider	
Federation Termination Requests Sent	Total number of Federation Termination Requests sent
Signed Federation Termination Requests Sent	Total number of signed Federation Termination Requests sent
Federation Termination Requests Received by the Service Provider	
Federation Termination Requests Received	Total number of Federation Termination Requests received
Signed Federation Termination Requests Received	Total number of signed Federation Termination Requests received
Federation Termination Requests Sent by the Identity Provider	
Federation Termination Requests Sent	Total number of Federation Termination Requests sent
Signed Federation Termination Requests Sent	Total number of signed Federation Termination Requests sent
Federation Termination Requests Received by the Identity Provider	
Federation Termination Requests Received	Total number of Federation Termination Requests received
Signed Federation Termination Requests Received	Total number of signed Federation Termination Requests received
Federation Termination Response Sent by the Service Provider	
Federation Termination Response Failed	Total failed Federation Termination Requests
Federation Termination Response Sent	Total Federation Termination Requests sent

Federation Termination Response Sent Successfully	Total Federation Termination Requests sent successfully
Signed Federation Termination Response Sent	Total signed Federation Termination Requests sent
Successful Federation Termination Requests Sent By Service Provider (%)	The percentage of total Federation Termination Requests sent successfully
Federation Termination Response Received by the Service Provider	
Federation Termination Response Failed	Total failed Federation Termination Requests
Federation Termination Response Received	Total Federation Termination Requests received
Federation Termination Response Received Successfully	Total Federation Termination Requests received successfully
Signed Federation Termination Response Received	Total signed Federation Termination Requests received
Successful Federation Termination Requests Received By Service Provider (%)	The percentage of total Federation Termination Requests received successfully
Federation Termination Response Sent by the Identity Provider	
Federation Termination Response Failed	Total failed Federation Termination Requests
Federation Termination Response Sent	Total Federation Termination Requests sent
Federation Termination Response Sent Successfully	Total Federation Termination Requests sent successfully
Signed Federation Termination Response Sent	Total signed Federation Termination Requests sent
Successful Federation Termination Requests Sent By Identity Provider (%)	The percentage of total Federation Termination Requests sent successfully
Federation Termination Response Received by the Identity Provider	
Federation Termination Response Failed	Total failed Federation Termination Requests
Federation Termination Response Received	Total Federation Termination Requests received
Federation Termination Response Received Successfully	Total Federation Termination Requests received successfully
Signed Federation Termination Response Received	Total signed Federation Termination Requests received

Successful Federation Termination Requests Received By Identity Provider (%)	The percentage of total Federation Termination Requests received successfully
Name Registration Requests Sent by the Service Provider	
Name Registration Requests Sent	Total number of Name Registration Requests sent
Signed Name Registration Requests Sent	Total number of signed Name Registration Requests sent
Name Registration Requests Received by the Service Provider	
Name Registration Requests Received	Total number of Name Registration Requests received
Signed Name Registration Requests Received	Total number of signed Name Registration Requests received
Name Registration Requests Sent by the Identity Provider	
Name Registration Requests Sent	Total number of Name Registration Requests sent
Signed Name Registration Requests Sent	Total number of signed Name Registration Requests sent
Name Registration Requests Received by the Identity Provider	
Name Registration Requests Received	Total number of Name Registration Requests received
Signed Name Registration Requests Received	Total number of signed Name Registration Requests received
Name Registration Response Sent by the Service Provider	
Name Registration Response Failed	Total failed Name Registration Requests
Name Registration Response Sent	Total Name Registration Requests sent
Name Registration Response Sent Successfully	Total Name Registration Requests sent successfully
Signed Name Registration Response Sent	Total signed Name Registration Requests sent
Successful Name Registration Requests Sent By Service Provider (%)	The percentage of total Name Registration Requests sent successfully
Name Registration Response Received by the Service Provider	
Name Registration Response Failed	Total failed Name Registration Requests
Name Registration Response Received	Total Name Registration Requests received

Name Registration Response Received Successfully	Total Name Registration Requests received successfully
Signed Name Registration Response Received	Total signed Name Registration Requests received
Successful Name Registration Requests Received By Service Provider (%)	The percentage of total Name Registration Requests received successfully
Name Registration Response Sent by the Identity Provider	
Name Registration Response Failed	Total failed Name Registration Requests
Name Registration Response Sent	Total Name Registration Requests sent
Name Registration Response Sent Successfully	Total Name Registration Requests sent successfully
Signed Name Registration Response Sent	Total signed Name Registration Requests sent
Successful Name Registration Requests Sent By Identity Provider (%)	The percentage of total Name Registration Requests sent successfully
Name Registration Response Received by the Identity Provider	
Name Registration Response Failed	Total failed Name Registration Requests
Name Registration Response Received	Total Name Registration Requests received
Name Registration Response Received Successfully	Total Name Registration Requests received successfully
Signed Name Registration Response Received	Total signed Name Registration Requests received
Successful Name Registration Requests Received By Identity Provider (%)	The percentage of total Name Registration Requests received successfully

Oracle Internet Directory 11g

The metrics collected for Oracle Internet Directory are shown in [Table 9](#).

Table 9 Oracle Internet Directory 11g Metrics

(Critical Event) Super User Failed Logins
Failed LDAP Super User Login
(Critical Event) Super User Successful Logins
Successful LDAP Super User Login

<i>(Critical Events) General System Resource Events</i>
Critical General Sys Resource Event Occurrences
Critical General Sys Resource Event Type
<i>(Critical Events) System Resource Events (3113 Errors)</i>
Number of 3113 Error Occurrences
<i>(Critical Events)System Resource Events (3114 Errors)</i>
Number of 3114 Error Occurrences
<i>(Critical Events) System Resource Events (Ora Errors)</i>
Critical Ora Error Occurrences
<i>(Resource Statistics) LDAP Server Memory Growth</i>
Average memory growth (%)
<i>(Resource Statistics) LDAP Server's Active Database Connections</i>
Active Database Sessions
<i>(Resource Statistics) LDAP Server's Open Database Connections</i>
Open Database Sessions
<i>Closed LDAP Logon Session Statistics</i>
Total Closed Logon Sessions
<i>LDAP Entry Cache Hit Ratio</i>
Server Entry Cache Hit Ratio
<i>LDAP Failed Bind Operations Profile</i>
Failed Bind Operations
<i>LDAP Load</i>
Server Load
<i>LDAP Operation Response Time</i>
Bind Operation Response Time
Compare Operation Response Time
Messaging Search Operation Response Time
<i>LDAP Operations Profile</i>
Completed Abandon Operations
Completed Add Operations
Completed Bind Operations
Completed Compare Operations
Completed Delete Operations
Completed Modify Operations
Completed Modrdn Operations
Completed Search Operations
Completed Unbind Operations
Total Operations
<i>LDAP Response</i>
Server Response (ms)
<i>LDAP Server Resource Usage</i>

CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (MB)
New LDAP Logon Session Statistics
Total New Logon Sessions
OID Replication Server Percentage CPU
Replication Server Percentage CPU
OID Replication Server Virtual Memory Size
Replication Server Memory Size
OID Server Percentage CPU Utilization
OID Server Percentage CPU
OID Server Virtual Memory Size
OID Server Memory Size
Open LDAP Logon Session Statistics
Total Open Logon Sessions
Replication Server Configuration Set Information
Number of Threads per Supplier for Change Processing
Number of Threads per Supplier for Transporting Changes
Replication Supplier Details
HIQ Changelog Count
Name of the Supplier Replica
New Changelog Count
Replication Agreement Type
Retry Changelog Count
Resource Usage
CPU Idle Time (%)
CPU Utilization (%)
Free Memory (%)
Free Memory (MB)
Heap Usage (MB)
Memory Utilization (%)
Memory Utilization (MB)
Other CPU Utilization (%)
Other Memory Utilization (MB)
Other Memory Utilization (%)
Start Time (ms since Epoch)
Total Memory (MB)
Up Time (ms since Epoch)
Response
Status
Running instances of LDAP Replication Server

Config Set
Downtime Count
Oracle Directory Server
Start Time
Size of Audit Log Purge Queue
Total Number of Audit Log Objects in Purge Queue
Size of General Statistics Purge Queue
Total Number of General Statistics Objects in Purge Queue
Size of Health Statistics Purge Queue
Total Number of Health Statistics Objects in Purge Queue
Size of Security Refresh events Purge Queue
Total Number of Security Refresh events Objects in Purge Queue
Size of System Resource events Purge Queue
Total Number of System Resource events Objects in Purge Queue
Size of Tombstone Purge Queue
Total Number of Tombstone Objects in Purge Queue
Stopped instances of LDAP Server
Config Set Number
Host Name
Total Number ChangeLogs in Purge Queue
Total Number of Local Changelogs in Purge Queue
Total Number Remote ChangeLogs in Purge Queue
Total Number of Remote Changelogs in Purge Queue
Total Number of HIQ ChangeLogs
HIQ Changelog Count
Total Number of Local ChangeLogs
Total Number of Local Changelogs
Total Number of New ChangeLogs
New Changelog Count
Total Number of Retry ChangeLogs
Retry Changelog Count
Total number ChangeLogs to be processed
Total Changelogs to be processed
User LDAP Operations Stats
Abandon Operations
Failed Add Operations
Failed Base Search Operations
Failed Bind Operations
Failed Compare Operations
Failed Delete Operations
Failed ModRdn Operations

Failed Modify Operations
Failed OneLevel Search Operations
Failed Proxy Bind Operations
Failed Subtree Search Operations
Successful Add Operations
Successful Base Search Operations
Successful Bind Operations
Successful Compare Operations
Successful Delete Operations
Successful ModRdn Operations
Successful Modify Operations
Successful OneLevel Search Operations
Successful Proxy Bind Operations
Successful Subtree Search Operations
Unbind Operations

Directory Integration Platform Server 11g

The metrics collected for Directory Integration Platform Server are shown in [Table 10](#).

Table 10 Directory Integration Platform Server 11g Metrics

<i>Directory Integration Platform</i>
Host
Parent
Process
<i>Directory Integration Platform All Profiles (Aggregated Metrics)</i>
Average LDAP Search Time
Average LDAP Write Time
Average Profile Execution Time(ms)
Total Changes Attempted
Total Successful Changes
<i>Directory Integration Platform All Profiles (Consolidated)</i>
Avg Processing Time
Process
Host
Last Change Number
Last Execution Error Value
Last Execution Time
Last Successful Execution Time
Max Processing Time
Min Processing Time
Profile Job Status

Status of last sync operation
Directory Integration Platform Health Metric
Host
MBean Status
Name
Quartz Scheduler Status
Directory Integration Platform Operations Summary
Total Count of all Failed Provisioning Operations
Total Count of all Failed Synchronization Operations
Total Count of all Successful Provisioning Operations
Total Count of all Successful Synchronization Operations
Total Count of all Failed Operations
Total Count of all Successful Operations
Directory Integration Platform Provisioning Profile Runtime Operational Metrics
Failed Add Group Operations
Failed Add Identity Operations
Failed Add Subscription Operations
Failed Add User Operations
Failed Delete Group Operations
Failed Delete Identity Operations
Failed Delete Subscription Operations
Failed Delete User Operations
Failed Modify Group Operations
Failed Modify Identity Operations
Failed Modify User Operations
Successful Add Group Operations
Successful Add Identity Operations
Successful Add Subscription Operations
Successful Add User Operations
Successful Delete Group Operations
Successful Delete Identity Operations
Successful Delete Subscription Operations
Successful Delete User Operations
Successful Modify Group Operations
Successful Modify Identity Operations
Successful Modify User Operations
Total Failed Provisioning Operations for Profile
Total Successful Provisioning Operations for Profile
Directory Integration Platform Synchronization Profile Runtime Operational Metrics
Failed Add Operations
Failed Delete Operations
Failed Modify Operations

Skipped Operations
Successful Add Operations
Successful Delete Operations
Successful Modify Operations
Total Failed Synchronization Operations for Profile
Total Successful Synchronization Operations for Profile
Directory Integration Platform Synchronization Profiles
Host
Profile Type
Directory Integration Platform Provisioning Profiles
Host
Profile Type
Directory Integration Profile Cumulative Statistics
Total Changes Failed
Total Changes Synchronized
Resource Usage
CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (KB)
Response
Status

Oracle Virtual Directory 11g

The metrics collected for Oracle Virtual Directory are shown in [Table 11](#).

Table 11 Oracle Virtual Directory 11g Metrics

Adapter Metrics
Number of Add Operations
Average Time (ms) to Complete an LDAP Search Request
Number of Delete Operations
Enabled
Maximum Time(ms) to Complete a Search Request
Minimum Time(ms) to Complete a Search Request
Number of Modify Operations
Open Connections
Operational Version
Number of all Operations
Provisioned Version
Number of Search Operations
Number of Bind Operations
Number of Connections Processed

Number of Connections Reused
Number of Rename Operations
Type
Connected IPs
Current Connections
Total Connections
Connected Users
Current Connections
Total Connections
Resource Usage
CPU Idle Time (%)
CPU Utilization (%)
Free Memory (%)
Free Memory (MB)
Heap Usage (MB)
Memory Utilization (%)
Memory Utilization (MB)
Other CPU Utilization (%)
Other Memory Utilization (%)
Other Memory Utilization (MB)
Start Time (ms since Epoch)
Total Memory (MB)
Up Time (ms since Epoch)
Response
Up/Down Status
Server Latency Metrics
Average time (ms) to Complete an LDAP Search Request
Maximum Time(ms) to Complete a Search Request
Minimum Time(ms) to Complete a Search Request
Number of LDAP Add Requests
Number of LDAP Binds Requests
Number of LDAP Delete Requests
Number of LDAP Modify Requests
Number of LDAP Rename Requests
Number of LDAP Search Requests
Total Operations
Server wide Connection Metrics
Total No of IPs connected currently
Total No of Open Connections
Total No of Operations
Total No of Users connected currently

Identify Federation Server 11g

The metrics collected for Identity Federation Server are shown in [Table 12](#).

Table 12 Identity Federation Server 11g Metrics

<i>Data Model</i>
Active IdP Federation Creation Time (ms)
Active IdP Federation Deletion Time (ms)
Active IdP Federation Retrieval Time (ms)
Active SP Federation Creation Time (ms)
Active SP Federation Deletion Time (ms)
Active SP Federation Retrieval Time (ms)
Affiliation Federation Creation Time (ms)
Affiliation Federation Retrieval Time (ms)
Database BLOB Creation Time (ms)
Database BLOB Retrieval Time (ms)
IdP Federation Creation Time (ms)
ProfileState Data Deletion Time (ms)
ProfileState Object Creation Time (ms)
ProfileState Object Retrieval Time (ms)
Provider Federation Deletion Time (ms)
Provider Federation Retrieval Time (ms)
Provider Metadata Retrieval Time (ms)
SAML Artifact Creation Time (ms)
SAML Artifact Deletion Time (ms)
SAML Artifact Retrieval Time (ms)
SP Federation Creation Time (ms)
Server Configuration Retrieval Time (ms)
Session Deletion Time (ms)
Session Object Retrieval Time (ms)
Temporary Provider Federation Retrieval Time (ms)
Time to Persist Session Data (ms)
Time to Persist a Provider Federation (ms)
User Object Retrieval Time (ms)
User Session Retrieval or Creation Time (ms)
<i>Data Tier Connectivity</i>
Open Server Connections
<i>Protocol Profiles</i>
ApplicationController Requests
ArtifactResolve Error Responses
ArtifactResolve Requests
ArtifactResolve Responses

AttributeQuery Error Responses
AttributeQuery Requests
AttributeQuery Responses
AuthnRequest Error Responses
AuthnRequest Processing time at the IdP (ms)
AuthnRequest Requests
AuthnRequest Responses
AuthnResponse Processing Time at the SP (ms)
Error Responses
Event Processing Time (ms)
Global Logout Time (ms)
HTTP Requests using POST Binding
HTTP Requests using POST Simple Sign Binding
HTTP Requests using Redirect Binding
HTTP Responses using POST Binding
HTTP Responses using POST Simple Sign Binding
HTTP Responses using Redirect Binding
HTTP and SOAP Requests
HTTP and SOAP Responses
Incoming Request Processing Time (ms)
Local User Authentication Time (ms)
Logout Error Responses
Logout Requests
Logout Responses
ManageNameID Error Responses
ManageNameID Requests
ManageNameID Responses
NameIDs of EmailAddress Format processed
NameIDs of Kerberos Format processed
NameIDs of Persistent Format processed
NameIDs of Transient Format processed
NameIDs of Unspecified Format processed
NameIDs of WindowsDomainQualifiedName Format processed
NameIDs of X509SubjectName Format processed
Received XML Requests successfully Parsed
Received XML Requests with Parsing Failures
RequestSecurityToken Responses
Requests Encrypted
Requests Signed
Requests both Signed and Encrypted
Responses Encrypted
Responses Signed

Responses both Signed and Encrypted
SAML Artifact Processing Time (ms)
SOAP Requests
SOAP Responses
Protocol Profiles Summary
ApplicationController Requests
ArtifactResolve Error Responses
ArtifactResolve Requests
ArtifactResolve Responses
AttributeQuery Error Responses
AttributeQuery Requests
AttributeQuery Responses
AuthnRequest Error Responses
AuthnRequest Processing time at the IdP (ms)
AuthnRequest Requests
AuthnRequest Responses
AuthnResponse Processing Time at the SP (ms)
Error Responses
Event Processing Time (ms)
Global Logout Time (ms)
HTTP Requests using POST Binding
HTTP Requests using POST Simple Sign Binding
HTTP Requests using Redirect Binding
HTTP Responses using POST Binding
HTTP Responses using POST Simple Sign Binding
HTTP Responses using Redirect Binding
HTTP and SOAP Requests
HTTP and SOAP Responses
Incoming Request Processing Time (ms)
Local User Authentication Time (ms)
Logout Error Responses
Logout Requests
Logout Responses
ManageNameID Error Responses
ManageNameID Requests
ManageNameID Responses
NameIDs of EmailAddress Format processed
NameIDs of Kerberos Format processed
NameIDs of Persistent Format processed
NameIDs of Transient Format processed
NameIDs of Unspecified Format processed
NameIDs of WindowsDomainQualifiedName Format processed

NameIDs of X509SubjectName Format processed
Received XML Requests successfully Parsed
Received XML Requests with Parsing Failures
RequestSecurityToken Responses
Requests Encrypted
Requests Signed
Requests both Signed and Encrypted
Responses Encrypted
Responses Signed
Responses both Signed and Encrypted
SAML Artifact Processing Time (ms)
SOAP Requests
SOAP Responses
Resource Usage
CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (KB)
Response
Status
Security Protocol Messages
URL Query String Signature Verification Time (ms)
URL Query String Signing Time (ms)
XML Decryptions Failures
XML Decryptions Successes
XML Encryptions Generated
XML Message Decryption Time (ms)
XML Message Encryption Time (ms)
XML Message Marshalling Time (ms)
XML Message Signature Verification Time (ms)
XML Message Signing Time (ms)
XML Message Unmarshalling Time (ms)
XML Signatures Generated
XML Signatures Verification Failures
XML Signatures Verification Successes

Oracle Adaptive Access Manager Server 11g

The metrics collected for Oracle Adaptive Access Manager Server are shown in [Table 13](#).

Table 13 Oracle Adaptive Access Manager Server 11g Metrics

CheckPoint Execution Summary
Average CheckPoint Processing Time (ms) for all Request since Server Startup

Maximum Number of Threads Active since Server Startup (RunTimes_Execution)
Maximum Time (ms) taken by any CheckPoint since Server Startup
Minimum Time (ms) taken by any CheckPoint since Server Startup
Time(ms) taken for servicing all CheckPoint since Server Startup
Total Number of CheckPoint's Completed
Total Numbers of Threads Active (RunTimes_Execution)
Datasource Metrics
Datasource - Available Connections
Datasource - Cached Statements Used (%)
Datasource - Cached Statements Used (per minute)
Datasource - Cached Statements not Used (per minute)
Datasource - Connection Leaks (per minute)
Datasource - Connection Pool Size
Datasource - Connection Refresh Failures (per minute)
Datasource - Connection Request Failures (per minute)
Datasource - Connection Requests (per minute)
Datasource - Connection Requests Waiting
Datasource - Connection Requests that Waited (per minute)
Datasource - Connection Wait Successes (%)
Datasource - Connection Wait Successes (per minute)
Datasource - Connections Created (per minute)
Datasource - Connections in Use
Datasource - Failed Waiting Connection Requests (per minute)
Datasource - State
Datasource - Statement Cache Size
Datasource - Statements Added to Cache (per minute)
Datasource - Statements Discarded from Cache (per minute)
Datasource - Successful Connections (%)
Datasource - Unavailable Connections
EJB Module Metrics
EJB Module - Bean Access Failures (per minute)
EJB Module - Bean Access Successes (%)
EJB Module - Bean Accesses (per minute)
EJB Module - Bean Activations (per minute)
EJB Module - Bean Destroys (per minute)
EJB Module - Bean Transaction Commits (per minute)
EJB Module - Bean Transaction Rollbacks (per minute)
EJB Module - Bean Transaction Timeouts (per minute)
EJB Module - Beans in Use
EJB Module - Cache Hits (%)
EJB Module - Cache Misses (per minute)
EJB Module - Cached Beans

EJB Module - Free Bean Instances
EJB Transaction Metrics
EJB Transaction - Bean Transaction Commits (%)
EJB Transaction - Bean Transaction Commits (per minute)
EJB Transaction - Bean Transaction Rollbacks (per minute)
EJB Transaction - Bean Transaction Timeouts (per minute)
Login Metrics Summary
Failed Logins (%) (since last collection)
Logins Blocked (%) (since last collection)
Logins Challenged (%) (since last collection)
Number of Failed Logins per sec since the server startup
Number of Logins Challenged during the last collection Interval
Number of Logins Failed during the last collection Interval
Number of Logins Blocked during the last collection Interval
Number of Successful Logins during the last collection Interval
Number of Successful Logins per sec since the server startup
Number of Total Logins attempted during the last collection Interval
Successful Logins (%) (since last collection)
Overview Metrics
Active Sessions
Bean Access Failures (per minute)
Bean Accesses (per minute)
Bean Activations (per minute)
Bean Destroys (per minute)
Bean Successes (%)
Bean Transaction Commits (%)
Bean Transaction Commits (per minute)
Bean Transaction Rollbacks (per minute)
Bean Transaction Timeouts (per minute)
Beans in Use
Cache Accesses (per minute)
Cache Hits (%)
Cache Misses (per minute)
Cached Beans
Free Bean Instances
MDB Messages (per minute)
Request Processing Time (ms)
Requests (per minute)
Work Manager Pending Requests
Work Manager Requests (per minute)
Policy Execution Summary
Average Execution Time (ms) for all Policies since Server startup

Maximum Number of Threads Active since Server Startup (Models_Execution)
Maximum Time taken by any Policy since Server Startup(ms)
Minimum Time taken by any Policy since Server Startup(ms)
Time taken for servicing all Policies since Server Startup(ms)
Total Number of Policies Processed
Total Numbers of Threads Active (Models_Execution)
Resource Usage
CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (KB)
Response
UpDown Status
Rule Execution Summary
Average Execution Time (ms) for all Request since Server startup (Rules_Execution)
Maximum Number of Threads Active since Server Startup (Rules_Execution)
Maximum Time(ms) taken by any Request since Server Startup (Rules_Execution)
Minimum Time(ms) taken by any Request since Server Startup (Rules_Execution)
Time(ms) taken for servicing all Request's since Server Startup (Rules_Execution)
Total Number of Requests Completed (Rules_Execution)
Total Numbers of Threads Active (Rules_Execution)
Rule Processing Summary
Average Execution Time (ms) for all Request since Server startup (ProcessRules)
Maximum Number of Threads Active since Server Startup (ProcessRules)
Maximum Time taken by any Request since Server Startup(ms) (ProcessRules)
Minimum Time taken by any Request since Server Startup(ms) (ProcessRules)
Time taken for servicing all Request's since Server Startup(ms) (ProcessRules)
Total Number of Requests Completed (ProcessRules)
Total Numbers of Threads Active (ProcessRules)
Servlet/JSP Metrics
Servlet/JSP - Reloads (per minute)
Servlet/JSP - Request Processing Time (ms)
Servlet/JSP - Requests (per minute)
Update Authorization Status Summary
Average Execution Time (ms) for all Request since Server startup (UpdateAuthStatus)
Maximum Number of Threads Active since Server Startup (UpdateAuthStatus)
Maximum Time(ms) taken by any Request since Server Startup(ms) (UpdateAuthStatus)
Minimum Time(ms) taken by any Request since Server Startup (UpdateAuthStatus)
Time(ms) taken for servicing all Request's since Server Startup (UpdateAuthStatus)
Total Number of Requests Completed (UpdateAuthStatus)
Total Numbers of Threads Active (UpdateAuthStatus)
Update Log Summary
Average Execution Time (ms) for all Request since Server startup (UpdateLog)

Maximum Number of Threads Active since Server Startup (UpdateLog)
Total Numbers of Threads Active (UpdateLog)
Web Module Metrics
Web Module - Active Sessions
Web Module - Request Processing Time (ms)
Web Module - Requests (per minute)

Oracle Adaptive Access Manager Cluster 11g

The metrics collected for Oracle Adaptive Access Manager Cluster are shown in [Table 14](#).

Table 14 Oracle Adaptive Access Manager Cluster 11g Metrics

Login Metrics Rate Summary
Number of Failed Logins per sec
Number of Successful Logins per sec
Login Metrics Summary
Failed Logins (%) (since last collection)
Logins Blocked (%) (since last collection)
Logins Challenged (%) (since last collection)
Number of Logins Blocked during the last collection Interval
Number of Logins Challenged during the last collection Interval
Number of Logins Failed during the last collection Interval
Number of Successful Logins during the last collection Interval
Number of Total Logins attempted during the last collection Interval
Successful Logins (%) (since last collection)
Oracle Adaptive Access Manager Datastore Information
JDBC URL
Response
Status

Oracle Access Manager Server 11g

The metrics collected for Oracle Access Manager Server are shown in [Table 15](#).

Table 15 Oracle Access Manager Server 11g Metrics

Audit Operation
Audit Operations/sec
Average Audit Latency
Process
Server Name
Authentication

Authentication Requests/sec
Authentication Success Failure Ratio
Average Authentication Latency
Hostname
Server Name
Authorizations
Authorization Requests/sec
Authorization Success Failure Ratio
Average Authorization Latency
Hostname
Server Name
JEE Web Service Endpoint Metrics
JEE WS Endpoint - Avg Dispatch Time per interval(ms)
JEE WS Endpoint - Avg Execution Time per interval(ms)
JEE WS Endpoint - Avg Invocation Time per interval(ms)
JEE WS Endpoint - Avg Response Time per interval(ms)
JEE WS Endpoint - Invocation Count
JEE WS Endpoint - Invocation Count Delta
JEE WS Endpoint - Invocation Throughput(per min)
JEE WS Endpoint - Response Error Count
JEE WS Endpoint - Response Error Count Delta
JEE WS Endpoint - Response Error Throughput(per min)
JEE WS Endpoint - Total Dispatch Time Delta(ms)
JEE WS Endpoint - Total Dispatch Time(ms)
JEE WS Endpoint - Total Execution Time Delta(ms)
JEE WS Endpoint - Total Execution Time(ms)
JEE WS Endpoint - Total Response Time Delta(ms)
JEE WS Endpoint - Total Response Time(ms)
Transport Protocol Type
JEE Web Service Operation Metrics
JEE WS Operation - Avg Dispatch Time per interval(ms)
JEE WS Operation - Avg Execution Time per interval(ms)
JEE WS Operation - Avg Invocation Time per interval(ms)
JEE WS Operation - Avg Response Time per interval(ms)
JEE WS Operation - Invocation Count
JEE WS Operation - Invocation Count Delta
JEE WS Operation - Response Error Count
JEE WS Operation - Response Error Count Delta
JEE WS Operation - Total Dispatch Time Delta(ms)
JEE WS Operation - Total Dispatch Time(ms)
JEE WS Operation - Total Execution Time Delta(ms)
JEE WS Operation - Total Execution Time(ms)

JEE WS Operation - Total Response Time Delta(ms)
JEE WS Operation - Total Response Time(ms)
LDAP Operations
Average LDAP Operation Latency
Hostname
LDAP Success Failure Ratio
LDAP Operations/sec
Process
Server Name
Log Operation
Average Log Latency
Log Operations/sec
Process
Server Name
OAM 10g Client
OAM Client Authentication Success Failure Ratio
Hostname
OAM Client NAP Handshake Latency
OAM Client NAP Handshake Success Failure Rate
OAM Client NAP Number of Open Connections
OAM Client Authentication Requests/sec
OAM Client Authorization Requests/sec
OAM Client Authorization Success Failure Ratio
OAM Client Average Authentication Latency
OAM Client Average Authorization Latency
Process
OAM Application Domains
Application Authentication Requests/sec
Application Authentication Success Failure Ratio
Application Authorization Requests/sec
Application Authorization Success Failure Ratio
Average Application Authorization Latency
Average Application Authentication Latency
Hostname
Process
OWSM Policy Violation Detail Metrics
OWSM Policy Category
OWSM Policy Violation - Authentication Fault Delta
OWSM Policy Violation - Authentication Faults
OWSM Policy Violation - Authorization Fault Delta
OWSM Policy Violation - Authorization Faults
OWSM Policy Violation - Confidentiality Fault Delta

OWSM Policy Violation - Confidentiality Faults
OWSM Policy Violation - Integrity Fault Delta
OWSM Policy Violation - Integrity Faults
OWSM Policy Violation - Total Policy Fault Delta
OWSM Policy Violation - Total Policy Faults
Oracle SSO 10g Client
Hostname
OSSO Client Authentication Success Failure Ratio
OSSO Client Authentication Requests/sec
OSSO Client Average Authentication Latency
Process
Oracle Web Service Endpoint Metrics
Oracle WS Endpoint - Avg Invocation Time per interval(sec)
Oracle WS Endpoint - Fault Count
Oracle WS Endpoint - Fault Count Delta
Oracle WS Endpoint - Fault Throughput(per min)
Oracle WS Endpoint - Invocation Count
Oracle WS Endpoint - Invocation Count Delta
Oracle WS Endpoint - Invocation Throughput(per min)
Oracle WS Endpoint - Start Time(ms since Epoch)
Oracle WS Endpoint - Total Invocation Time Delta(sec)
Oracle WS Endpoint - Total Invocation Time(sec)
Oracle Web Service Operation Metrics
Oracle WS Operation - Avg Invocation Time per interval(ms)
Oracle WS Operation - Avg Invocation Time(msec)
Oracle WS Operation - Fault Count
Oracle WS Operation - Fault Count Delta
Oracle WS Operation - Invocation Count
Oracle WS Operation - Invocation Count Delta
Oracle WS Operation - Response Count
Oracle WS Operation - Response Count Delta
Oracle WS Operation - Total Invocation Time Delta(msec)
Oracle WS Operation - Total Invocation Time(msec)
Resource Utilization
CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (KB)
Response
UpDown Status

Oracle Access Manager Cluster 11g

The metrics collected for Oracle Access Manager Cluster are shown in [Table 16](#).

Table 16 Oracle Access Manager Cluster 11g Metrics

<i>Audit Operations (Aggregated)</i>
Audit Operations/sec
Average Audit Latency
Server Name
<i>Authentications (Aggregated)</i>
Authentication Requests/sec
Authentication Success Failure Ratio
Average Authentication Latency
<i>Authorizations (Aggregated)</i>
Authorization Requests/sec
Authorization Success Failure Rate
Average Authorization Latency
<i>LDAP Operations (Aggregated)</i>
Average LDAP Operation Latency
Hostname
LDAP Operations Success Failure Ratio
LDAP Operations/sec
Name
Process
<i>Log Operations (Aggregated)</i>
Average Log Operation Latency
Log Operations/sec
Server Name
<i>OAM 10g Client (Aggregated)</i>
Hostname
OAM Client NAP Handshake Latency
OAM Client NAP Handshake Success Failure Rate
OAM Client NAP Number of Open Connections
OAM Client Authorization Requests/sec
OAM Client Authentication Success Failure Ratio
OAM Client Authorization Requests/sec
OAM Client Authentication Success Failure Ratio
OAM Client Average Authentication Latency
OAM Client Average Authorization Latency
Process
<i>OAM Application Domains (Aggregated)</i>
Application Authentication Requests/sec
Application Authentication Success Failure Ratio
Application Authorization Requests/sec

Application Authorization Success Failure Ratio
Application Authorization Latency
Application Authentication Latency
Hostname
Process
OSSO 10g Client (Aggregated)
OSSO Client Authentication Success Failure Ratio
Hostname
OSSO Client Authentication Requests/sec
OSSO Client Average Authentication Latency
Process
Response
Status

Oracle Identity Manager Server 11g

The metrics collected for Oracle Identity Manager Server are shown in [Table 17](#).

Table 17 Oracle Identity Manager Server 11g Metrics

Adapters
Average Adapter Execution Time (ms)
Completed Adapter Executions
Maximum Adapter Execution Time (ms)
Minimum Adapter Execution Time (ms)
Datasource Metrics
Datasource - Available Connections
Datasource - Cached Statements Used (%)
Datasource - Cached Statements Used (per minute)
Datasource - Cached Statements not Used (per minute)
Datasource - Connection Leaks (per minute)
Datasource - Connection Pool Size
Datasource - Connection Refresh Failures (per minute)
Datasource - Connection Request Failures (per minute)
Datasource - Connection Requests (per minute)
Datasource - Connection Requests Waiting
Datasource - Connection Requests that Waited (per minute)
Datasource - Connection Wait Successes (%)
Datasource - Connection Wait Successes (per minute)
Datasource - Connections Created (per minute)
Datasource - Connections in Use
Datasource - Failed Waiting Connection Requests (per minute)
Datasource - State

Datasource - Statement Cache Size
Datasource - Statements Added to Cache (per minute)
Datasource - Statements Discarded from Cache (per minute)
Datasource - Successful Connections (%)
Datasource - Unavailable Connections
<i>EJB Module Metrics</i>
EJB Module - Bean Access Failures (per minute)
EJB Module - Bean Access Successes (%)
EJB Module - Bean Accesses (per minute)
EJB Module - Bean Activations (per minute)
EJB Module - Bean Destroys (per minute)
EJB Module - Bean Transaction Commits (per minute)
EJB Module - Bean Transaction Rollbacks (per minute)
EJB Module - Bean Transaction Timeouts (per minute)
EJB Module - Beans in Use
EJB Module - Cache Hits (%)
EJB Module - Cache Misses (per minute)
EJB Module - Cached Beans
EJB Module - Free Bean Instances
<i>EJB Transaction Metrics</i>
EJB Transaction - Bean Transaction Commits (%)
EJB Transaction - Bean Transaction Commits (per minute)
EJB Transaction - Bean Transaction Rollbacks (per minute)
EJB Transaction - Bean Transaction Timeouts (per minute)
<i>Events Handler</i>
Average Events Execution Time (ms)
Completed Events Executions
Maximum Events Execution Time (ms)
Minimum Events Execution Time (ms)
Executions and Messages
Total Adapter Executions
Total Events Handler Executions
Total JMS Messages
<i>JEE Web Service Endpoint Metrics</i>
JEE Web Service Endpoint - Average Dispatch Time
JEE Web Service Endpoint - Average Execution Time
JEE Web Service Endpoint - Average Invocation Time
JEE Web Service Endpoint - Average Response Time
JEE Web Service Endpoint - Aggregate Invocation Count
JEE Web Service Endpoint - Invocation Count
JEE Web Service Endpoint - Invocation Throughput (invocations per minute)
JEE Web Service Endpoint - Aggregate Response Error Count

JEE Web Service Endpoint - Response Error Count
JEE Web Service Endpoint - Response Error Throughput (response errors per minute)
JEE Web Service Endpoint - Total Dispatch Time Delta
JEE Web Service Endpoint - Total Dispatch Time
JEE Web Service Endpoint - Total Execution Time Delta
JEE Web Service Endpoint - Total Execution Time
JEE Web Service Endpoint - Total Response Time Delta
JEE Web Service Endpoint - Total Response Time
TransportProtocolType
JEE Web Service Operation Metrics
JEE Web Service Operation - Average Dispatch Time
JEE Web Service Operation - Average Execution Time
JEE Web Service Operation - Average Invocation Time
JEE Web Service Operation - Average Response Time
JEE Web Service Operation - Aggregate Invocation Count
JEE Web Service Operation - Invocation Count
JEE Web Service Operation - Aggregate Response Error Count
JEE Web Service Operation - Response Error Count
JEE Web Service Operation - Total Dispatch Time Delta
JEE Web Service Operation - Total Dispatch Time
JEE Web Service Operation - Total Execution Time Delta
JEE Web Service Operation - Total Execution Time
JEE Web Service Operation - Total Response Time Delta
JEE Web Service Operation - Total Response Time
JMS Queue
Average Processing Time (ms)
Maximum Processing Time (ms)
Minimum processing Time (ms)
Processed Messages
MDS Metrics
IOs Per Document Get
IOs Per MO Content Get
IOs Per Metadata Object Get
Metadata Object Get Processing Time (seconds)
Metadata Object Gets Per Second
Metadata Update Processing Time (seconds)
Metadata Updates Per Second
OWSM Policy Violation Detail Metrics
OWSM Policy Category
OWSM Policy Violation - Authentication Fault Delta
OWSM Policy Violation - Authentication Faults
OWSM Policy Violation - Authorization Fault Delta

OWSM Policy Violation - Authorization Faults
OWSM Policy Violation - Confidentiality Fault Delta
OWSM Policy Violation - Confidentiality Faults
OWSM Policy Violation - Integrity Fault Delta
OWSM Policy Violation - Integrity Faults
OWSM Policy Violation - Total Policy Fault Delta
OWSM Policy Violation - Total Policy Faults
Oracle Web Service Endpoint Metrics
Oracle WS Endpoint - Avg Invocation Time per interval(sec)
Oracle Web Service Endpoint - Fault Count
Oracle WS Endpoint - Fault Count Delta
Oracle Web Service Endpoint - Fault Throughput (faults per minutue)
Oracle Web Service Endpoint - Invocation Count
Oracle WS Endpoint - Invocation Count Delta
Oracle Web Service Endpoint - Invocation Throughput (invocations per minute)
Oracle Web Service Endpoint - Start Time
Oracle WS Endpoint - Total Invocation Time Delta(sec)
Oracle Web Service Endpoint - Total Request Time (sec)
Oracle Web Service Operation Metrics
Oracle WS Operation - Avg Invocation Time per interval(ms)
Oracle WS Operation - Avg Invocation Time(msec)
Oracle Web Service Operation - Faults
Oracle WS Operation - Fault Count Delta
Oracle WS Operation - Invocation Count
Oracle WS Operation - Invocation Count Delta
Oracle WS Operation - Response Count
Oracle WS Operation - Response Count Delta
Oracle WS Operation - Total Invocation Time Delta(msec)
Oracle WS Operation - Total Invocation Time(msec)
Overview Metrics
Active Sessions
Bean Access Failures (per minute)
Bean Accesses (per minute)
Bean Activations (per minute)
Bean Destroys (per minute)
Bean Successes (%)
Bean Transaction Commits (%)
Bean Transaction Commits (per minute)
Bean Transaction Rollbacks (per minute)
Bean Transaction Timeouts (per minute)
Beans in Use
Cache Accesses (per minute)

Cache Hits (%)
Cache Misses (per minute)
Cached Beans
Free Bean Instances
MDB Messages (per minute)
Request Processing Time (ms)
Requests (per minute)
Work Manager Pending Requests
Work Manager Requests (per minute)
Resource Usage
CPU Utilization (%)
Memory Utilization (%)
Memory Utilization (KB)
Response
UpDown Status
SPML Web Services
Average Response Time (ms)
Incoming Calls
Servlet/JSP Metrics
Servlet/JSP - Reloads (per minute)
Servlet/JSP - Request Processing Time (ms)
Servlet/JSP - Requests (per minute)
Web Module Metrics
Web Module - Active Sessions
Web Module - Request Processing Time (ms)
Web Module - Requests (per minute)

Oracle Identity Manager Cluster 11g

The metrics collected for Oracle Identity Manager Cluster are shown in [Table 18](#).

Table 18 Oracle Identity Manager Cluster 11g Metrics

Provisioning Requests
Completed Provisioning Requests
Completed Provisioning Requests Processing Time (per sec)
Failed Provisioning Requests
Pending Provisioning Requests
Reconciliations (last 24 hrs)
Jobs Completed
Jobs Started
Response

Status
Role Grant Requests
Completed Role Grant Requests
Completed Role Grant Requests Processing Time (per sec)
Failed Role Grant Requests
Pending Role Grant Requests
SPML Web Services
Average Response Time (ms)
Incoming Calls
Self Service Requests
Completed Self Service Requests
Completed Self Service Requests Processing Time (per sec)
Failed Self Service Requests
Pending Self Service Requests

Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g

Please refer to the Installation Guide for the System Monitoring Plug-in for Oracle Directory Server Enterprise Edition (http://download.oracle.com/otn/java/oem/ODSEE_EMPI_documentation_v1.0.pdf).

Troubleshooting the Management Pack Plus for Identity Management

This section describes common problems that you may encounter when monitoring and managing Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation with the Management Pack Plus for Identity Management.

It contains the following topics:

- [Failure to Discover Oracle Access Manager, Oracle Identity Manager or Oracle Identity Federation](#)
- [What OS User Privileges required for Windows Host Preferred Credentials](#)
- [Certain Metrics Are Not Collected](#)
- [The Status of Certain Components in Enterprise Manager Differs from the Status of the Same Components in the Windows Services Panel](#)
- [Internet Explorer Crashes When Trying to Perform Multiple Recording Transactions for the Same Application](#)
- [How to enable Browser Simulation on Windows XP beacon?](#)

Failure to Discover Oracle Access Manager, Oracle Identity Manager or Oracle Identity Federation

Problem

The discovery of Oracle Access Manager, Oracle Identity Manager or Oracle Identity Federation fails and, consequently, Enterprise Manager does not create the corresponding Oracle Identity Management targets.

Possible Cause

- The configuration of Oracle Identity Management components is not complete. Make sure that all pre-requisites have been completed before the discovery process. Refer to the [Discovering & Configuring Oracle Identity Management Targets](#) section.
- The credentials requested for discovering the Oracle Identity Management components may be inaccurate – e.g. SNMP Agent UDP Port or Community Name may be incorrect, and as a result, the discover of Oracle Access Manager fails.

Solution

- **Review Supported Products and Platforms:** Make sure that the version and the platform associated with the Oracle Identity Management component that you would like to discover are supported in the Management Pack Plus for Identity Management. For more information, please see the [System Requirements](#) section.
- **Complete ALL Installation Pre-Requisites:** Make sure that all pre-requisites have been completed before the discovery process. Refer to the [Discovering & Configuring Oracle Identity Management Targets](#) section.
- **Provide Accurate Credentials:** The credentials requested for discovering the Oracle Identity Management components may be inaccurate – e.g. SNMP Agent UDP Port or Community Name may be incorrect, and as a result, the discover of Oracle Access Manager fails. Make sure that you provide accurate details.

What OS User Privileges required for Windows Host Preferred Credentials

Problem

When I enter the username and password for the Windows host administrator account, I'm getting the error "Error: invalid agent credentials." What OS privileges are required for the Windows user whose credentials are being passed as preferred credentials when Enterprise Manager 10g requires Host Login credentials?

Solution

The OS user should have the following System Privileges:

- **Log on as a batch job**
- **Log on as a service**

These can be granted to the user via the **Control Panel > Administrative Tools > Local Security Policy**

These privileges are specific to Windows operating systems. There are no similar requirements for Unix/Linux systems.

Certain Metrics Are Not Collected

Problem

Although the discovery completed successfully, some metrics are collected, but other metrics are not.

Possible Cause

The credentials requested for discovering the Oracle Identity Management components may be inaccurate – e.g. SNMP Agent UDP Port or Community Name may be incorrect, and as a result, the metric collection fails.

Solution

- **Complete ALL Installation Pre-Requisites:** Make sure that all pre-requisites have been completed before the discovery process. Refer to the [Discovering & Configuring Oracle Identity Management Targets](#) section.
- **Provide Accurate Credentials:** The credentials requested for discovering the Oracle Identity Management components may be inaccurate – e.g. SNMP Agent UDP Port or Community Name may be incorrect, and as a result, the discover of Oracle Access Manager fails. Make sure that you provide accurate details.

The Status of Certain Components in Enterprise Manager Differs from the Status of the Same Components in the Windows Services Panel

Possible Cause

Enterprise Manager collects Oracle Identity Management metrics only at certain intervals (regular metrics every 15 minutes, availability information every 5 minutes). Therefore, information visible in the Enterprise Manager user interface may be out of sync with the Windows Services panel.

Workaround

If you are interested in monitoring a certain metric in real-time mode for a certain period, go to the **All Metrics** page for a given Oracle Identity Management target, navigate to the desired metric, and change it to Real-time mode. In this mode, collection occurs more frequently and you can follow statistics more closely.

Solution

You can change the collection frequency for individual metrics. If you want the availability metrics to be collected more often, you may change the collection frequency for your key Oracle Identity Management components.

Internet Explorer Crashes When Trying to Perform Multiple Recording Transactions for the Same Application

Possible Cause

A limitation in the application.

Solution

Close and start a new Internet Explorer browser window.

How to enable Browser Simulation on Windows XP beacon?

Possible Cause

To run a Web Transaction (Browser) service test, you need beacons that are running on 10.2.0.4 or later Management Agent on Windows XP.

Solution

Please refer to [Advanced Configuration Guide, Section 7.4.5.2.](#)

Title and Copyright Information

Management Pack Plus for Identity Management
Oracle® Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0)
Getting Started Guide

Copyright © 2011, Oracle and/or its affiliates. All rights reserved.

Author: Amjad Afanah

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

This software is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications which may create a risk of personal injury. If you use this software in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

This software and documentation may provide access to or information on content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.