Oracle® Identity Management Pack

Getting Started Guide

Amjad Afanah

03/21/2009

ORACLE

Contents

Oracle® Identity Management Pack
Getting Started Guide
10g Release 4 (10.2.0.4.0) / 10g Release 5 (10.2.0.5.0)

Oracle® Identity Management Pack
Getting Started Guide
10g Release 4 (10.2.0.4.0) / 10g Release 5 (10.2.0.5.0)
March 2009

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

Introduction to the Identity Management Pack

This section covers the following topics:

Functional Overview

The Identity Management Pack leverages Oracle Enterprise Manager Grid Control's broad set of capabilities in configuration management, performance management, and service level management to manage the end-to-end Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation environments.

Single-step discovery of Oracle Access Manager (OAM), Oracle Identity Manager (OIM), and Oracle Identity Federation (OIF) allows you to quickly set up your monitoring environment.

With the IdM Pack, you can proactively monitor your Oracle Identity Management environment from both a systems-oriented view and an end-user perspective. Out-of-box collection of key performance metrics for monitored components helps facilitate rapid time to value - allowing you to set up alerts based on warning and critical thresholds, view current and historical performance information using graphs and reports, and

diagnose performance problems by identifying bottlenecks in any of the monitored targets.

You can also monitor your Oracle Identity Management environment from an end-user perspective using synthetic service tests. These tests are designed to simulate key end user activities such as logging into an application via single sign-on. The tests are run via beacons from locations that are representative of your user communities within your network to actively measure the performance and availability of your Identity and Access services.

Additionally you can perform key configuration management tasks like keeping track of configuration changes, taking snapshots to store configurations, and comparing component configurations for Oracle Access Manager.

Finally yet importantly, the IdM Pack provides service level management capabilities that allow you to model your Identity and Access services down to the key components they rely on, define service levels based on business requirements and report against clearly defined Service Level Objectives (SLO's).

When combined with other Enterprise Manager packs and plug-ins for managing Oracle and non-Oracle database, middleware, network devices and hosts, you can achieve complete end-to-end management of your entire Oracle Identity Management environment.

Monitored Targets

The monitored targets in the Identity Management Pack are summarized in Table 1. These targets have been added to Enterprise Manager in order to facilitate the management of Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation.

Table 1 Licensed Targets in Identity Management Pack

Enterprise Manager Target Type	Purpose
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.

Enterprise Manager Target Type	Purpose
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 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. Oracle Application Server, 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.
Web Application or Generic Service	With the Identity Management Pack, 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

Enterprise Manager Target Type	Purpose
	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.

In addition to the targets in Table 1, the Identity Management Pack leverages the targets that are included in the Identity Management Grid Control Plug-in (e.g. Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Delegated Administration Services, Oracle Application Server Single Sign-On, etc.). It is recommended that the Grid Control Plug-in be installed in addition to the Identity Management Pack to set up a comprehensive monitoring environment.

Please refer to the Identity Management Infrastructure Administrator's Guide for more information about the Identity Management Grid Control Plug-in: http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b15994/imcontrol.htm#OIMAG010

Additional Sources of Information

Refer to the documentation listed in Table 2 for additional information about the Identity Management Pack. 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 Identity Management Pack

Book	Chapter	Information
Enterprise Manager Grid Control Quick Start Guide (http://download.oracle.com/docs/cd/B16240_01/doc/user.102/b28678/toc.htm)	All	Introduction to Enterprise Manager Grid Control - It is highly recommended that you go over this piece of documentation first if you are new to using Oracle Enterprise Manager
Enterprise Manager Concepts	All	Overall information on the capabilities of Oracle Enterprise Manager Grid Control

Book	Chapter	Information
Guide (http://download.oracle.com/docs/cd/B16240_01/doc/em.102/b31949/toc.htm)		
	Identity Management	Monitoring Oracle Identity Management targets and creating/configuring associated services.
	System Monitoring	Setting up Thresholds and Alerts
	Service Management	Defining Service Level Objective, Running Service Level Reports
	Managing Deployments Chapter	Viewing Configurations, Comparing Configurations, Taking Configuration Snapshots, Using Configuration Policy
	Host and Third-Party Target Management	Monitoring the Operating System and the Host
	Information Publisher	Creating Custom Reports
Enterprise Manager Grid Control Installation and Basic Configuration (http://download.oracle.com/docs/cd/B16240_01/doc/em.102/e10953/toc.htm)	All	Installing Enterprise Manager Grid Control Server and Agents
Enterprise Manager Advanced Configuration (http://download.oracle.com/docs/cd/B16240_01/doc/em.102/e10954/toc.htm)	All	Advanced Configuration Topics
	Sizing and Maximizing the Performance of Oracle Enterprise Manager	Capacity Planning and Tuning for Oracle Enterprise Manager
Oracle Identity	Identity Management	Monitoring Oracle Identity Management

Book	Chapter	Information
Management Infrastructure Administrator's Guide (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b15994/toc.htm)	Grid Control Plug-in	Infrastructure components: Oracle Internet Directory, Oracle Application Server Single Sign-On, Oracle Delegated Administration Services, and Oracle Directory Integration Platform, using the features of the Oracle Enterprise Manager 10g Grid Control Console
Oracle® Application Server Administrator's Guide (http://download.oracle.com/docs/cd/B28196_01/core.1014/b28185/toc.htm)	Introduction to Administration Tools - About Oracle Enterprise Manager 10g Grid Control	Installing and Using the Identity Management Grid Control Plug-in

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 and platforms in the Identity Management Pack in Enterprise Manager Grid Control 10g Release 4 (10.2.0.4).

Refer to Table 4 for a list of supported Oracle Identity Management products and platforms in the Identity Management Pack in Enterprise Manager Grid Control 10g Release 5 (10.2.0.5).

Table 3 Supported Oracle Identity Management Products and Platforms in the Identity Management Pack in Enterprise Manager Grid Control 10g Release 4 (10.2.0.4)

Product	Version	Platform	Application Server	Directory Server
Oracle Access Manager	10.1.4.0.1	Windows, Linux	N/A	Oracle Internet Directory 10.1.4, Microsoft Active Directory

Product	Version	Platform	Application Server	Directory Server
Oracle Identity Federation	10.1.4.0.1	Windows, Linux	Oracle Application Server 10g	Oracle Internet Directory 10.1.4, Oracle Database (User Data Store)
Oracle Identity Manager	9.0.1	Windows	WebLogic 8.1 SP6 (Sun jdk 1.4.2_09 or later), JBoss 4.0.2 (Sun jdk 1.4.2_09 or later), WebSphere 5.1.1.5 (IBM jdk 1.5.0 or later)	Oracle Database, Microsoft SQL Server 2000
	9.0.1	Linux	JBoss 4.0.2 (Sun jdk 1.4.2_09 or later), WebSphere 5.1.1.5 (IBM jdk 1.5.0 or later)	Oracle Database, Microsoft SQL Server 2000

Table 4 Supported Oracle Identity Management Products and Platforms in the Identity Management Pack in Enterprise Manager Grid Control 10g Release 5 (10.2.0.5)

Product	Version	Platform	Application Server	Directory Server
Oracle Access Manager	10.1.4.0.1, 10.1.4.2	Windows, Linux	N/A	Oracle Internet Directory 10.1.4, Microsoft Active Directory 2000/2003. *Note*: Other Directory Servers can be used, but will not be discovered in Enterprise Manager.

Product	Version	Platform	Application Server	Directory Server
Oracle Identity Federation	10.1.4.0.1, 10.1.4.2	Windows, Linux	Oracle Application Server 10g	Oracle Internet Directory 10.1.4, Microsoft Active Directory 2000/2003, Oracle Database 10.2.0.2, 11.1.0.6 (User Data Store) *Note*: Other Directory Servers can be used, but will not be discovered in Enterprise Manager.
Oracle Identity Manager	9.0.1	Windows	WebLogic 8.1 SP6 (Sun jdk 1.4.2_09 or later), JBoss 4.0.2 (Sun jdk 1.4.2_09 or later), WebSphere 5.1.1.5 (IBM jdk 1.5.0 or later)	Oracle Database, Microsoft SQL Server 2000
	9.0.1	Linux	JBoss 4.0.2 (Sun jdk 1.4.2_09 or later), WebSphere 5.1.1.5 (IBM jdk 1.5.0 or later)	Oracle Database, Microsoft SQL Server 2000

Product	Version	Platform	Application Server	Directory Server
	9.1.0.1	Windows, Linux	JBoss 4.2.3 (Sun JDK 1.6.0_10 or later), WebLogic 10.3 (Sun JDK 1.6.0_10 or later), WebSphere 6.1.0.9 (IBM jdk 1.5.0 or later)	Oracle Database, Microsoft SQL Server 2005

Installing Oracle Enterprise Manager Grid Control 10g Release 4 / 10g Release 5

Before you begin configuring Grid Control 10g Release 4 (10.2.0.4) or 10g Release 5 (10.2.0.5) to manage your Identity Management components, you must install and configure Grid Control 10g Release 4 (10.2.0.4) or 10g Release 5 (10.2.0.5) on at least one host computer on your network. Oracle recommends that you install the Grid Control components on their own host or hosts. For example, if the Identity Management Pack middle tier is 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 10.2 Oracle Management Agent on every host that includes the components you want to manage with Grid Control.

Note:

- Installing Enterprise Manager Grid Control 10g Release 4 / 10g Release 5 requires any previous releases of Grid Control – that is any 10.2.0.x.0 installation, and upgrade to 10.2.0.4.0 release. If you do not have a previous release, but want to have a 10.2.0.4.0 Grid Control environment, then first install 10.2.0.1.0 Grid Control (10.2.0.2.0 for Windows), and then upgrade it to 10.2.0.4.0 – please see the README file for Enterprise Manager 10gR4: (http://www.oracle.com/technology/software/products/oem/htdocs/gridR4_10204_readme.html).

- The installation of the Grid Control 10g Release 4 (10.2.0.4) and 10g Release 5 (10.2.0.5) Agent does not require a previous release of Grid Control 10g agent. The installation file for the Grid Control Agent is found on Oracle's OTN website: (http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html).

See Also:

Oracle Enterprise Manager Basic Installation and Configuration for Oracle Enterprise Manager Grid Control 10.2 (http://www.oracle.com/technology/documentation/oem.html)

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 Manger, you must perform the following tasks:

- Install the Enterprise Manager Grid Control 10g Release 4 (10.2.0.4) / 10g Release 5 (10.2.0.5)

The information required to perform these steps is available in Chapter 3 of the *Oracle Enterprise Manager Grid Control Installation and Basic Configuration Guide* (http://download.oracle.com/docs/cd/B16240_01/doc/em.102/e10953/installing_em.htm#CJGIGIBB).

- Install Grid Control 10g Release 4 (10.2.0.4) / 10g Release 5 (10.2.0.5) Agent on each of the hosts where Oracle Access Manager, Oracle Identity Federation and Oracle Identity Manager run on.

The information required to perform these steps is available in Chapter 3 of the *Oracle Enterprise Manager Grid Control Installation and Basic Configuration Guide* (http://download.oracle.com/docs/cd/B16240_01/doc/em.102/e10953/installing_em.htm#CJGIGIBB)

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 10g Release 4 (10.2.0.4) / 10g Release 5 (10.2.0.5) Agent on these hosts as well.

- Install Identity Management Grid Control Plug-in on each of the hosts where Oracle Identity Management Infrastructure components run on.

In addition to installing Grid Control 10g Release 4 (10.2.0.4) / 10g Release 5 (10.2.0.5) Agent on each of the hosts where Oracle Access Manager, Oracle Identity Federation and Oracle Identity Manager run on, you may also install the Identity Management Grid Control Plug-in to monitor the Oracle Identity Management Infrastructure components. The Oracle Identity Management Infrastructure components include Oracle Internet Directory (OID), Oracle Directory Integration Platform (DIP), Oracle Application Server Single Sign-On (SSO), and Oracle

Delegated Administration Services (DAS). You can download the Identity Management Grid Control Plug-in from OTN: (http://www.oracle.com/technology/software/products/ias/htdocs/101401.html).

For information about installing and using the Identity Management Grid Control Plug-in, please refer to the Oracle Application Server Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/core.1014/b28185/tools.htm#BEIBAHHJ).

For information about monitoring Oracle Identity Management Infrastructure components, please refer to the Oracle Identity Management Infrastructure Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b15994/imcontrol.htm#BHBGFGBI).

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

  Oracle Access Manager

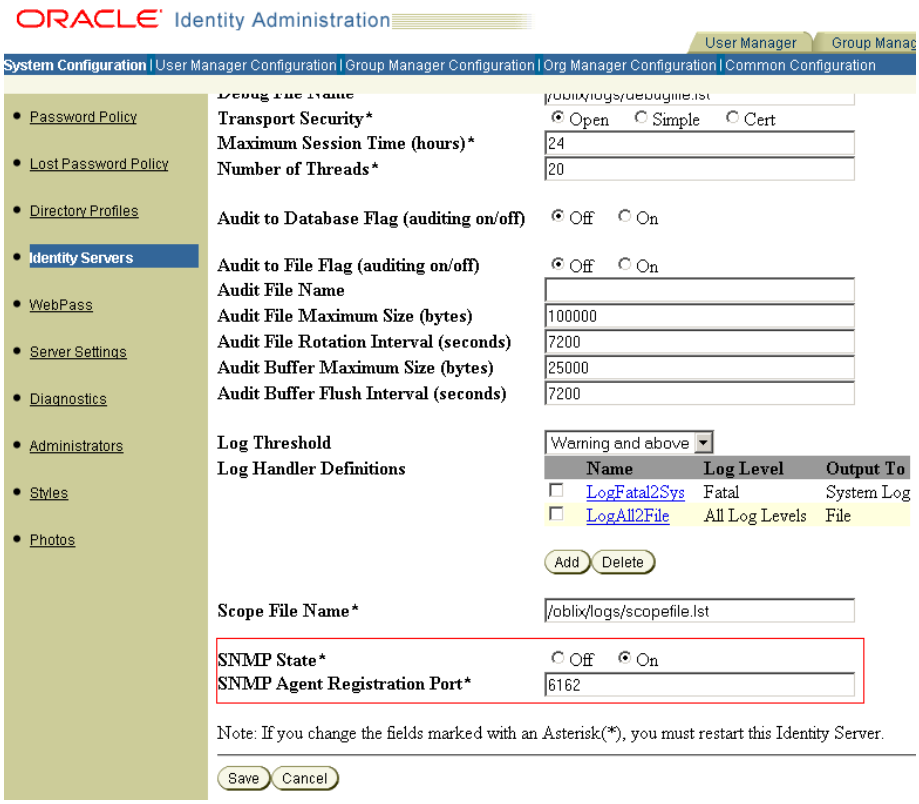
  1. Install Oracle Access Manager SNMP Agent on each of the hosts where Oracle Access Manager's Access Server and Identity Server are running. The SNMP Agent collects performance metrics and configuration parameters for Oracle Access Manager's Access Server and Identity Server allowing you to monitor 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/snmpmntr.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).



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).

4. 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/a_srvr.htm#BGBEFBBD).

5. 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 Manger 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**: Download and install the Identity Management Grid Control Plug-in from OTN: (http://www.oracle.com/technology/software/products/ias/htdocs/101401.html). For information about installing and using the Identity Management Grid Control Plug-in, please refer to the Oracle Application Server Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/core.1014/b28185/tools.htm#BEIBAHHJ). For information about monitoring Oracle Identity Management Infrastructure components, please refer to the Oracle Identity Management Infrastructure Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b15994/imcontrol.htm#BHBGFGBI).
    - **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

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#BCGDGAAJ).

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 Gird Control:
    - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.
    - 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 Manger 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**: Download and install the Identity Management Grid Control Plug-in from OTN: (http://www.oracle.com/technology/software/products/ias/htdocs/101401.html). For information about installing and using the Identity Management Grid Control Plug-in, please refer to the Oracle Application Server Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/core.1014/b28185/tools.htm#BEIBAHHJ). For information about monitoring Oracle Identity Management Infrastructure components, please refer to the Oracle Identity Management Infrastructure Administrator's Guide: (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b15994/imcontrol.htm#BHBGFGBI).
   - **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 Gird 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

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 **All Targets** sub-tab.
     - Select **Agent** from the **Search** dropdown menu and click on the **Go** button. Select the Grid Control Agent on which the JBoss Application Server is running.
     - 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.

   - **WebLogic Application Server Version: 8.1 with SP4**:
     - Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.
     - Select **Agent** from the **Search** dropdown menu and click on the **Go** button. Select the Grid Control Agent on which the WebLogic Application Server is running.
     - Select **BEA WebLogic Managed Server** 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 **All Targets** sub-tab.
     - Select **Agent** from the **Search** dropdown menu and click on the **Go** button. Select the Grid Control Agent on which the WebSphere Application Server is running.
     - 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 Gird 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).

Discovering & Configuring Oracle Identity Management Targets

This section covers the following topics:

Discovering Oracle Access Manager Access Server

Enterprise Manager has a simple discovery wizard for Oracle Identity and Access Management Suite targets. The discovery wizard collects details about Oracle Identity Management 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 integrated configuration management database (CMDB).

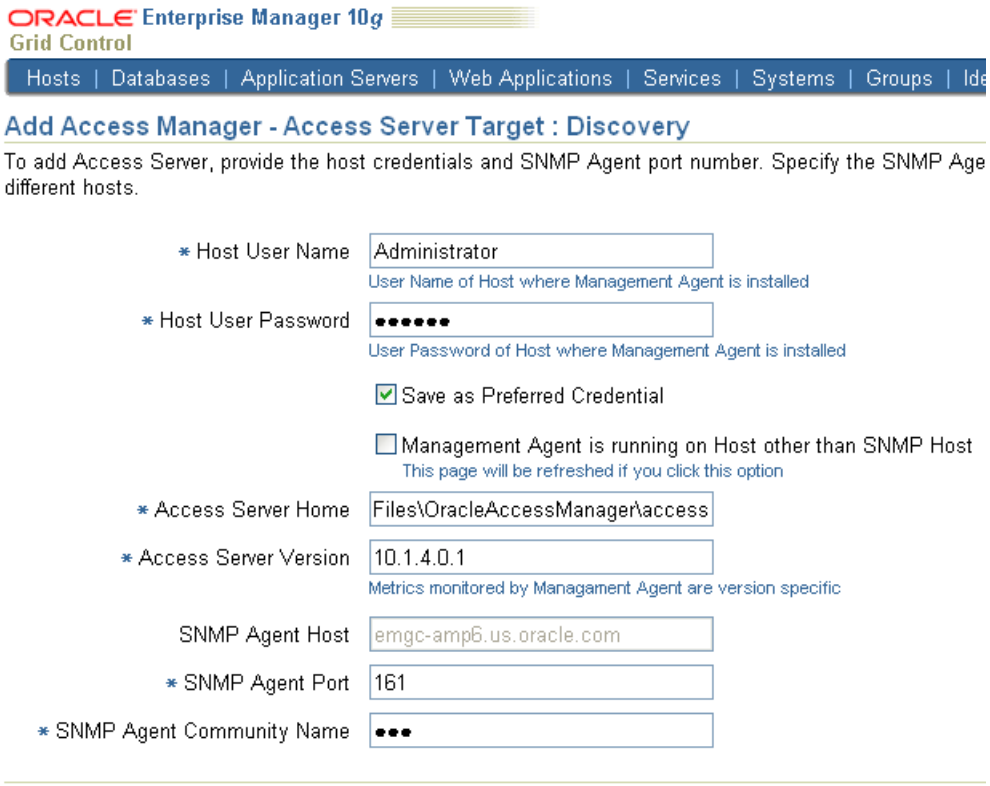
To discover Oracle Access Manager – Access Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.

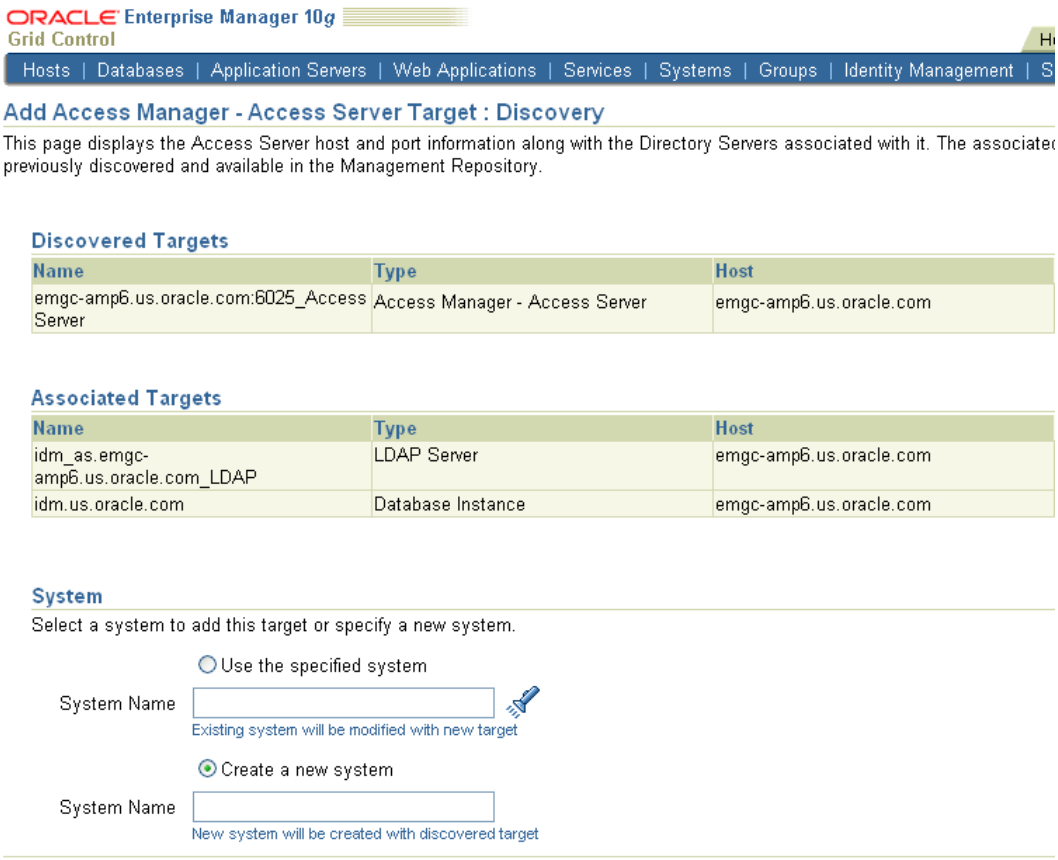
2. Select **Identity and Access Mgmt Suite** from the **Add** dropdown menu and click on the **Go** button.

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.

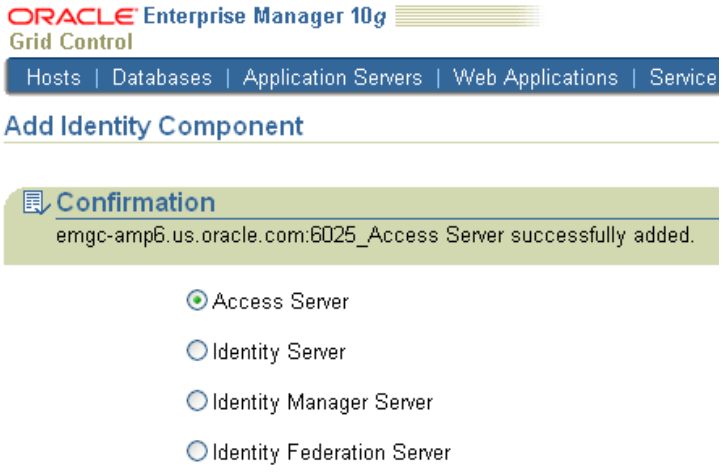
4. Enter the information requested for Oracle Access Manager – Access Server. Click **Next** once all information requested is entered.
   a. **Host User Name**: Username on the operating system with administrator privileges.
   b. **Host User Password**: Password of host administrator account.
   c. **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.



5. 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.



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



Discovering Oracle Access Manager Identity Server

Enterprise Manager has a simple discovery wizard for Oracle Identity and Access Management Suite targets. The discovery wizard collects details about Oracle Identity

Management 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 integrated configuration management database (CMDB).

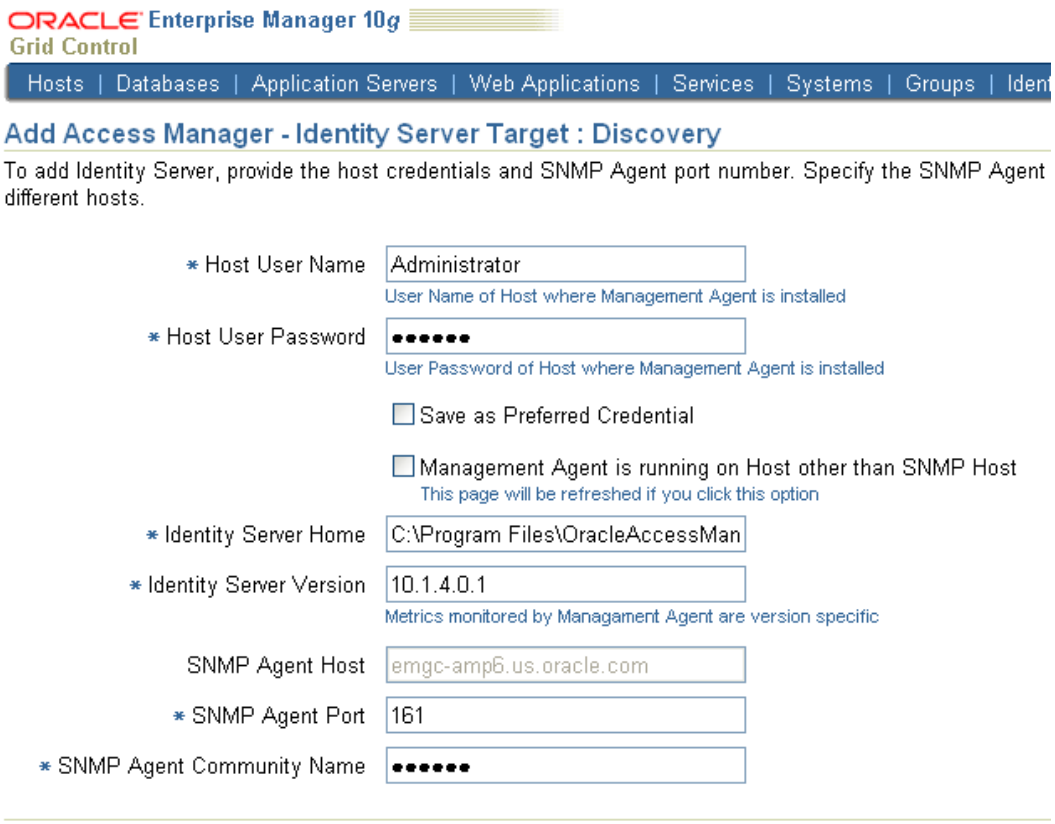
To discover Oracle Access Manager – Identity Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.

2. Select **Identity and Access Mgmt Suite** from the **Add** dropdown menu and click on the **Go** button.

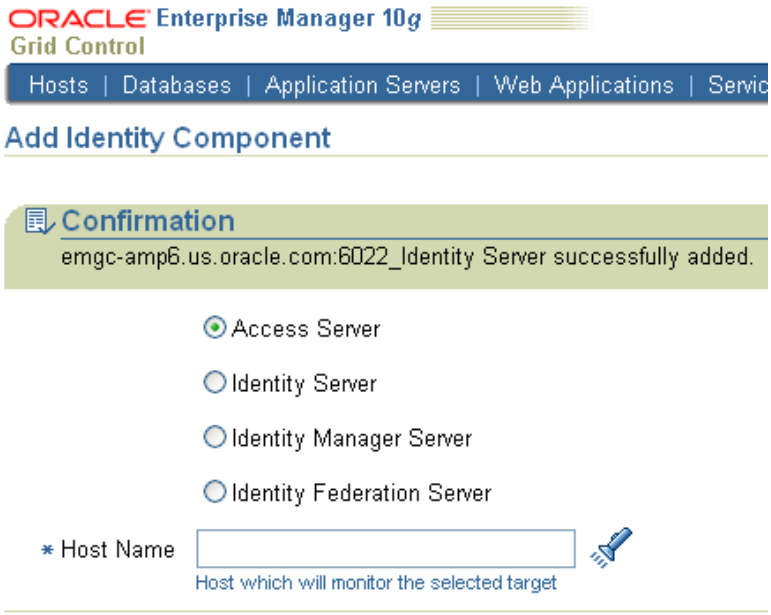
3. Select the radio button for **Identity Server** and enter the host name on which your Oracle Access Manager Identity Server is running. Click **OK** to continue with the discovery of the Identity Server.

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.



5. 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.

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



Discovering Oracle Identity Federation Server

Enterprise Manager has a simple discovery wizard for Oracle Identity and Access Management Suite targets. The discovery wizard collects details about Oracle Identity Management 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 integrated configuration management database (CMDB).

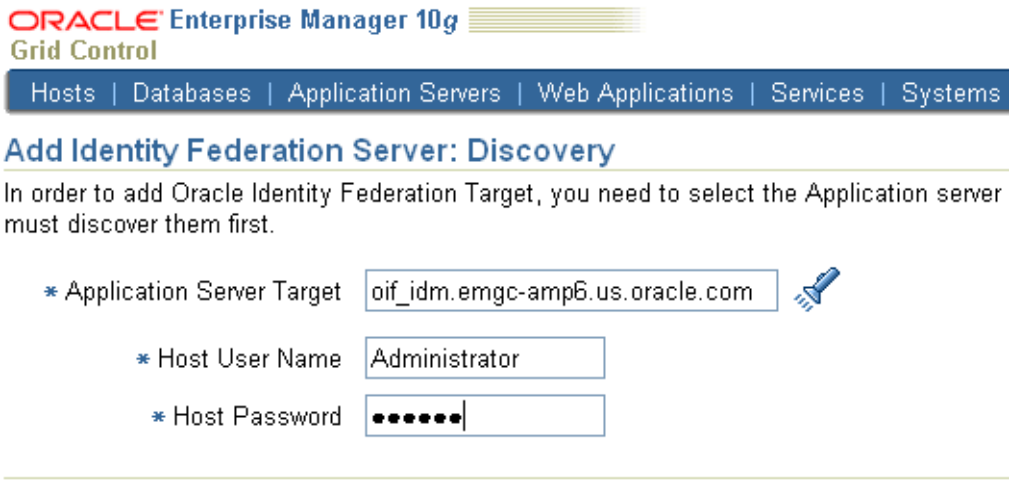
To discover Oracle Identity Federation Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.

2. Select **Identity and Access Mgmt Suite** from the **Add** dropdown menu and click on the **Go** button.

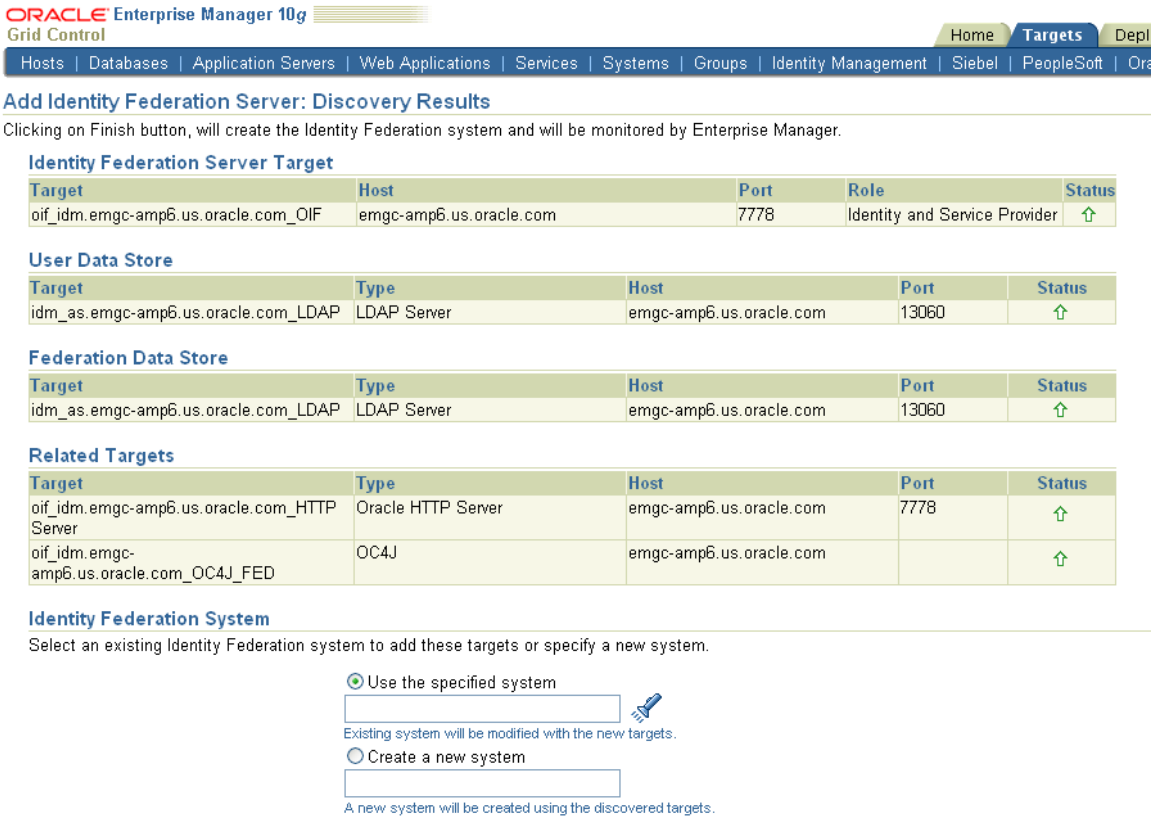
3. Select the radio button for **Identity Federation Server** and enter the host name on which your Oracle Identity Federation Server is running. Click **OK** to continue with the discovery of the Identity Federation Server.

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.

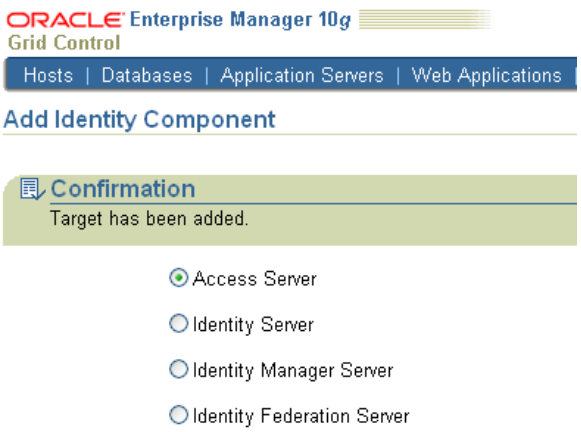


5. Enterprise Manager discovers the topology of your Oracle Identity Federation Server deployment including the associated databases and directory servers. To

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.



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



Discovering Oracle Identity Manager Server

Enterprise Manager has a simple discovery wizard for Oracle Identity and Access Management Suite targets. The discovery wizard collects details about Oracle Identity Management 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 integrated configuration management database (CMDB).

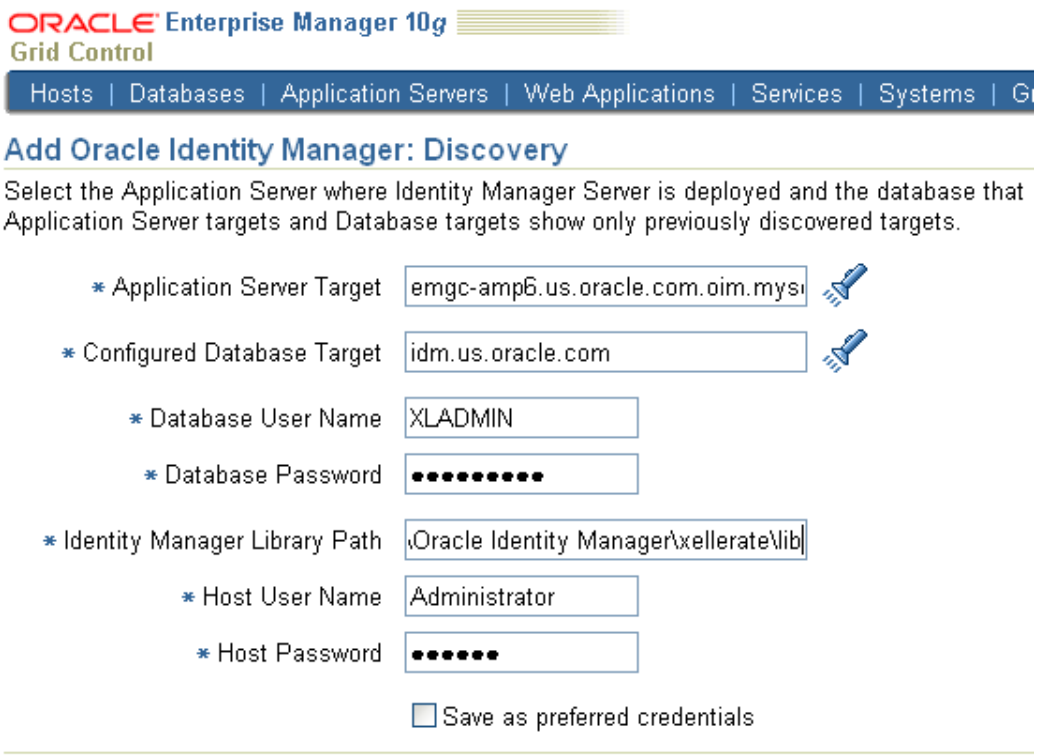
To discover Oracle Identity Manager Server, perform the following steps:

1. Log in to Enterprise Manager. Navigate to the **Targets** tab and select **All Targets** sub-tab.

2. Select **Identity and Access Mgmt Suite** 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.



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.

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

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

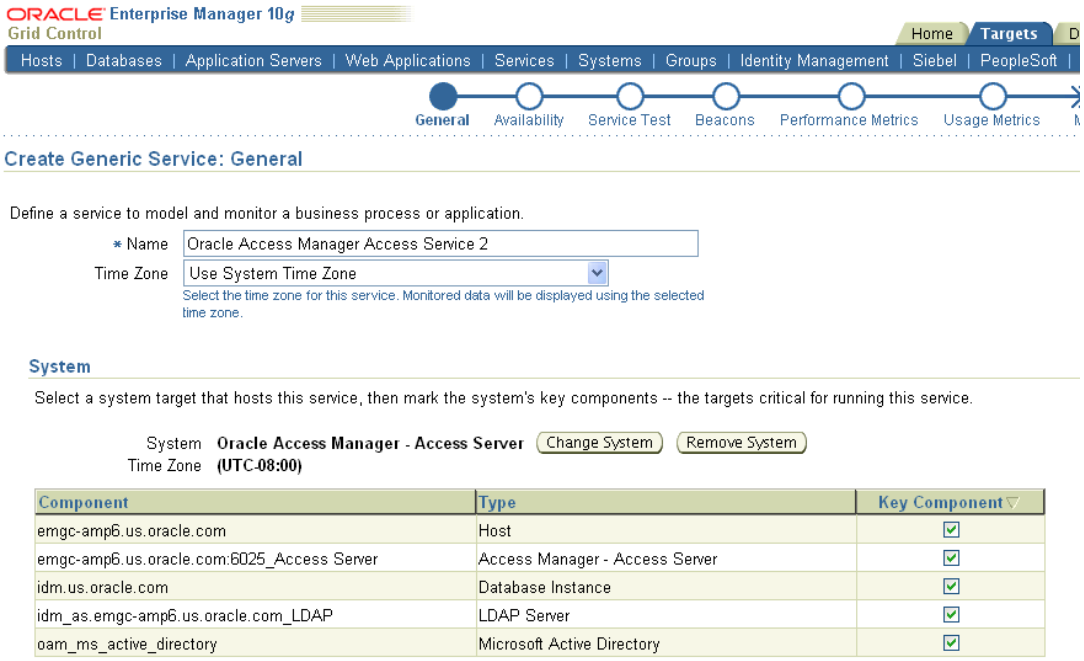
With the Identity Management Pack, users can create targets of type **Generic Service** or **Web Application** associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, and Identity Manager System. The 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 **All Targets** sub-tab.

2. Select **Generic Service** or **Web Application** from the **Add** dropdown menu and click on the **Go** button.

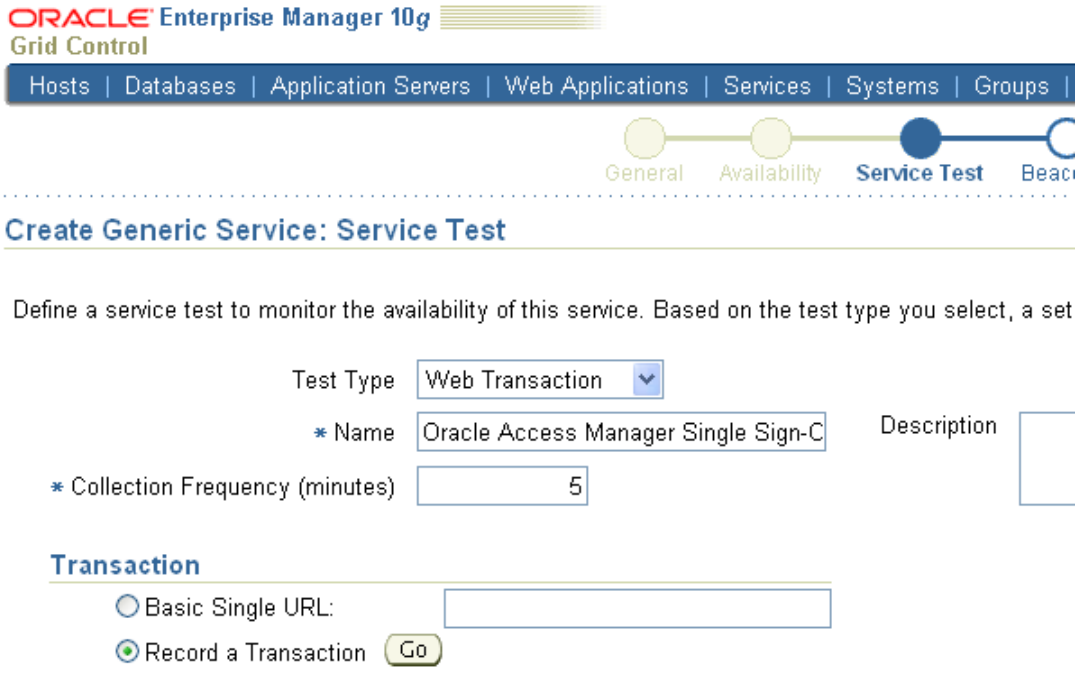
3. Enter the general information requested for the new Generic Service. Click **Continue** once all information requested is entered.
    a. **Name**: Enter a name for your new Generic Service – e.g. Oracle Access Manager Access Service
    b. **Time Zone**: Select a time zone for your service
    c.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



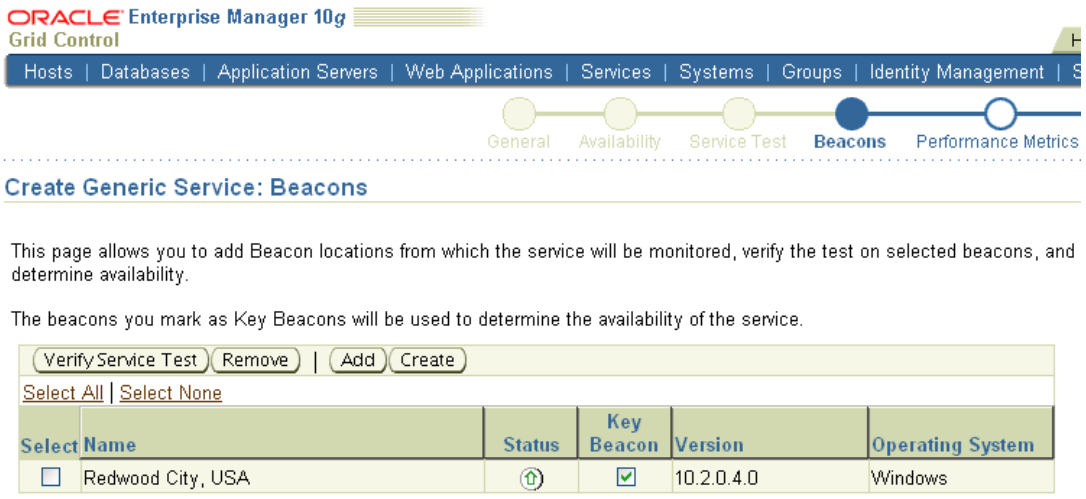
4. Enter the availability information requested for the new Generic Service. Click **Continue** once all information requested is entered.
    a. **Define availability based on**:
        i. **Service Test**: Choose this option if the availability of your service is determined by the availability of 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.

5. 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**.

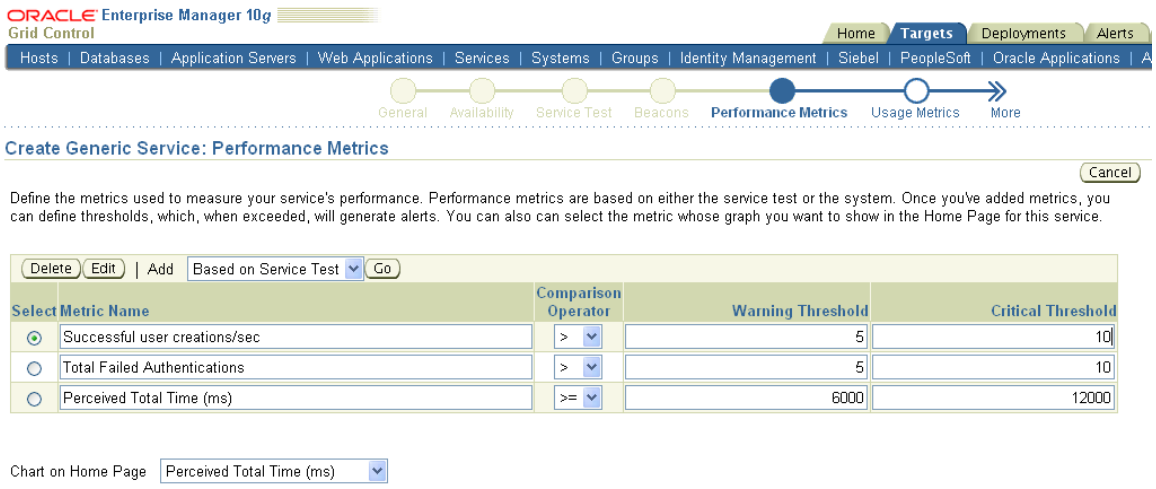
b. **Name**: Enter a name for your new service test – e.g. “Simple Login Test”
c. **Collection Frequency (Minutes)**: Enter the desired collection frequency for your service test.
d. **Transaction**:
    i. **Basic Single URL**: If you would like to test a single page, enter a URL for your service test.
    ii. **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.



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.

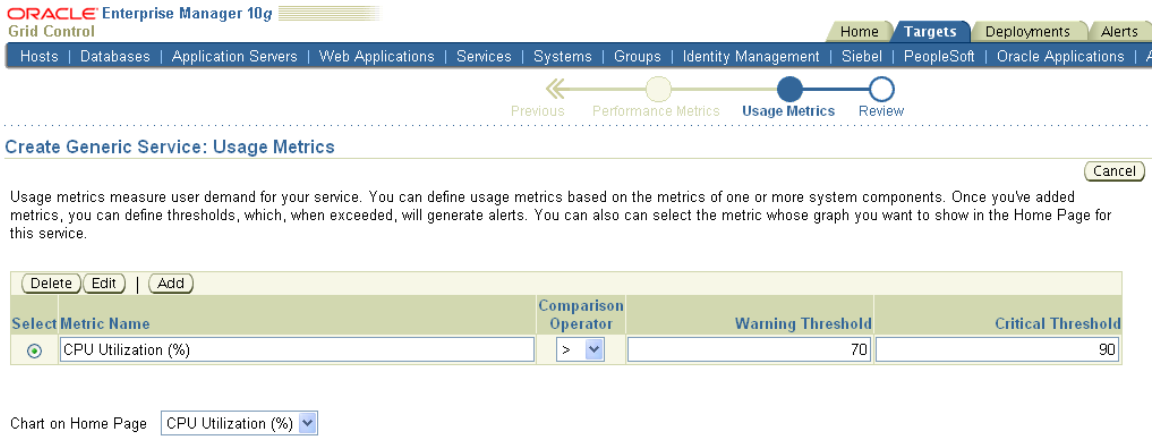


7. Enter the performance metrics information requested for the new Generic Service. Click **Continue** once all information requested is entered.
    a. **Add Based on Service Test**: Click on the **Go** button to add performance metrics based on the recorded service test. Define the Warning Threshold 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.



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.



9. 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:

1. From the Enterprise Manager Console, click the **Reports** tab.
2. Click the **Create** button.
3. Enter the general information requested for the new Report. Click on the **Elements** tab once all information requested is entered.
   a. **Title**: Enter a title for your new dashboard
   b. **Category/Sub-Category**: Select a category and sub-category for your dashboard – e.g. Category: Monitoring, Sub-Category: Dashboards
   c. **Use the specified target**: Leave blank if this report has no report-wide target.
   d. **Options – Visual Style**: Select **Dashboard** for a dashboard-view of your services.
4. Enter the elements information requested for the new Report. Click on the Schedule tab once all information requested is entered.
   a. **Add**: Select **Services Monitoring Dashboard** and click on the **Continue** button.
   b. **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.
5. Enter the schedule information requested for the new Report. Click on the Access tab once all information requested is entered.

a. **Schedule**: Enter your scheduling preferences for the report
b. **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 Identity Management Pack 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 Identity Management Pack 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 Identity Management Pack 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 Identity Management Pack 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 **All Targets** tab.
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 **All Targets** tab.
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.

With the Identity Management Pack, 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.

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 **All Targets** tab.

3. Click on one of the Oracle Identity Management Service targets 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 **Performance Metrics** link.
6. Select **Based on System** from the **Add** dropdown list and click on the **Go** button.
7. 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.
8. 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 **All Targets** tab.
3. Click on the Oracle Identity Management Service target of type **Generic Service**.
4. Click on the **Monitoring Configuration** tab.
5. 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.

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 **All Targets** tab.
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 **All Targets** tab.
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 Identity Management Pack 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-define 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.

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 Access Manager targets: Access Manager – Access Server and Access Manager – Identity Server. 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 Identity Management Pack supports configuration management for the monitored Oracle Access Manager targets only: Access Manager – Access Server and Access Manager – Identity Server. The Configuration Management Pack for Non-

Oracle Systems is needed to take advantage of configuration management features for the underlying hosts running other Oracle Identity Management components.

This section covers the following topics:

Viewing Configurations

Using the Identity Management Pack, 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 **All Targets** tab.
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 **All Targets** tab.
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 **All Targets** tab.
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 Identity Management Pack, 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.
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 Identity Management Pack 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.

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
- Access Manager – Identity Server
- Identity Manager Server
- Identity Manager Repository
- Identity Federation Server

Access Manager – Access Server

The metrics collected for the Access Manager – Access Server are shown in Table 5. The performance metrics for the Access Manager – Access Server are exposed via the SNMP Agent.

Table 5 Access Manager – Access Server 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)	aaaAuthorizationsSuccessOID	The number of successful authorizations by the Access Server instance - since last collection.	SNMP Agent
Total Successful Authorizations	aaaAuthorizationsSuccessOID	The total number of successful authorizations by the Access Server instance.	SNMP Agent + Computed

Successful Authorizations (%)			
Successful Authorizations (%) (Since Last Collection)	aaaAuthorizationsSuccessOID	The percentage of successful authorizations by the Access Server instance - since last collection.	SNMP Agent + Computed
Total Successful Authorizations (%)	aaaAuthorizationsSuccessOID	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

The metrics collected for the Access Manager – Identity Server are shown in Table 6. The performance metrics for the Access Manager – Identity Server are exposed via the SNMP Agent.

Table 6 Access Manager – Identity Server 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

The metrics collected for the Identity Manager Server are shown in Table 7.

Table 7 Identity Manager Server 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

The metrics collected for the Identity Manager Repository are shown in Table 8.

Table 8 Identity Manager Repository 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

The metrics collected for the Identity Federation Server are shown in Table 9. The performance metrics for the Identity Federation Server are exposed via the SNMP Agent.

Table 9 Identity Federation Server 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

Troubleshooting the Identity Management Pack

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 Identity Management Pack.
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 Identity Management Pack. 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.