

MANAGEMENT PACK FOR IDENTITY MANAGEMENT



A CENTRALIZED SYSTEMS
MANAGEMENT SOLUTION
FOR ORACLE IDENTITY
MANAGEMENT

FEATURES

- **Single-Step Discovery:** A simple target discovery wizard for both Oracle Identity Management 10g and Oracle Identity Management 11g components allows you to quickly set up your monitoring environment.
- **Performance Monitoring:** Proactively monitor your Oracle Identity Management environment from both systems & end-user perspectives. A wide range of out-of-box performance metrics are collected for monitored Oracle Identity Management targets 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 Oracle Identity Management targets. Thresholds may be defined against server and component statistics such as CPU utilization, the number of failed and successful authentications /authorizations, average response time, provisioning metrics (e.g. number of newly provisioned /created/deleted/disabled/locked users), Identity Provider and Service Provider metrics, and up/down status of servers and components. In addition to relying on system

Management Pack for Identity Management leverages Oracle Enterprise Manager Grid Control's broad set of capabilities in configuration management, performance monitoring and diagnostics, and service level management to provide a centralized systems management solution for Oracle Identity Management.

Complete Management Solution

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

Single-Step Discovery

A simple target discovery wizard is available for both Identity Management 10g and Identity Management 11g components. The supported Identity Management 10g components include Oracle Access Manager (OAM) 10g, Oracle Identity Manager (OIM) 9.x, Oracle Identity Federation (OIF) 10g, and Oracle Identity Management Suite 10g (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Services, and Single Sign-On). The supported Identity Management 11g components include Oracle Internet Directory, Oracle Directory Integration Platform, Oracle Virtual Directory, Oracle Identity Federation, Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager. Single-step discovery enables you to quickly set up your monitoring environment. Upon completing target discovery, configuration settings that are defined in the monitored Oracle Identity Management targets will be automatically detected and stored in the Management Repository, which is Oracle Enterprise Manager Grid Control's integrated Configuration Management Database (CMDB).

Configuration Management

With the Management Pack for Identity Management, you can perform key

performance metrics, you may use Management Pack for Identity Management's Service Tests to record synthetic web transactions that include 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 be successfully authenticated and authorized against a certain WebGate for the service to be considered available. Enterprise Manager uses these logical tasks or 'transactions' to define the availability of the Identity Management environment. In addition to synthetic web transactions, Enterprise Manager also supports LDAP tests that allow you to record LDAP operations against a specific LDAP server (including Oracle Virtual Directory). With the LDAP tests, you can specify the username/password, Search Filter, Search Base, and Compare Attribute Name/Value. These synthetic web transactions are recorded, and the stored transaction or 'service test' can be launched at a user-defined interval from strategic locations across the user-base.

- **Configuration Management:** Perform key configuration management tasks like keeping track of configuration changes for diagnostic and regulatory purposes, taking snapshots to store configurations, and comparing component configurations to ensure consistency of configurations within the same environment or across different environments.
- **Service Level Management:** Model Oracle Identity Management services down to the key components they rely on, define service levels based on business requirements and report against clearly defined Service Level Objectives

configuration management tasks like keeping track of configuration changes, taking snapshots to store configurations, and comparing component configurations. To ensure that the configurations of all critical Oracle Identity Management components in your production environment are consistent with your staging or test environments, you can use Configuration Snapshots to save working configurations into the Management Repository or into an external XML file and then use the Configuration Comparison tool to compare the configuration in the production environment against the test or staging environments. Configuration Comparison helps you ensure the consistency of configurations in your environment – thus reducing “configuration drift.” To diagnose performance problems that may be related to system configuration changes, you can use Management Pack for Identity Management’s Configuration History tool to keep track of all configuration changes to locate the root cause of performance problems.

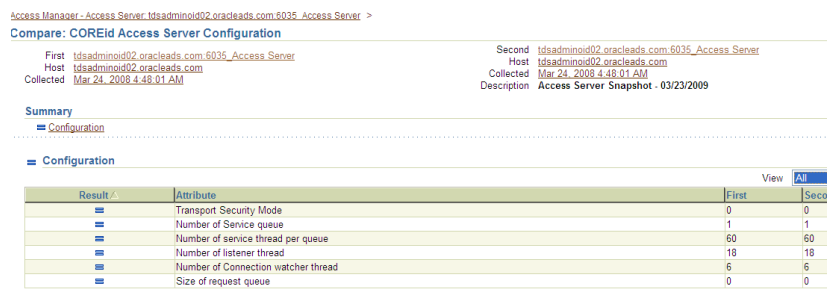


Figure 1. Configuration Comparison

Performance Monitoring

With the Management Pack for Identity Management, you can proactively monitor your Oracle Identity Management environment from both systems & end-user perspectives. A wide range of out-of-box performance metrics are collected for monitored Oracle Identity Management targets 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 Oracle Identity Management targets.

Using the pack, your administrators may monitor the health of all critical Identity Management components – including both Identity Management 10g and Identity Management 11g components. Thresholds may be defined against server and component statistics such as CPU utilization, the number of failed and successful authentications/authorizations, average response time, provisioning metrics (e.g. number of newly provisioned/created/deleted/disabled/locked users), Identity Provider and Service Provider metrics, and up/down status of servers and components.

(SLO's).

BENEFITS

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



Figure 2. Oracle Virtual Directory (OVD) Performance Summary

In addition to relying on system performance metrics, you may use Management Pack for Identity Management’s Service Tests to record synthetic web transactions that include 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 be successfully authenticated and authorized against a certain WebGate for the service to be considered available. Enterprise Manager uses these logical tasks or ‘transactions’ to define the availability of the Identity Management environment. In addition to synthetic web transactions, Enterprise Manager also supports LDAP tests that allow you to record LDAP operations against a specific LDAP server (including Oracle Virtual Directory). With the LDAP tests, you can specify the username/password, Search Filter, Search Base, and Compare Attribute Name/Value. These synthetic web transactions are recorded, and the stored transaction or ‘service test’ can be launched at a user-defined interval from strategic locations across the user-base.

Service Level Management

A common dilemma in organizations is balancing business needs with IT spending. Since Identity Management services address how organizations authenticate people, manage their access to confidential information, and audit the transactions that flow between the various systems, Identity Management administrators constantly need to satisfy application owners while keeping a lid on spending and increasing IT efficiency. Key questions that need to be answered include:

- What is the impact of Identity Management on business applications?
- How do we prioritize Identity Management activities according to business needs?
- When changes are made to the Identity Management environment, what is the potential impact on the business?

Some key performance indicators (KPI) needed to answer these questions may be traditional system-based indicators while others may need to be derived from the business applications that depend on the Identity Management infrastructure for access control and user provisioning. Management Pack for Identity Management’s

RELATED PRODUCTS

The following Oracle Enterprise Manager Grid Control products can be used with the Management Pack for Identity Management to provide management coverage for your entire system environment and support for each phase of the application lifecycle:

- Oracle Real User Experience Insight
- Diagnostic Pack for Oracle Database
- Tuning Pack for Oracle Database
- Configuration Management Pack for Oracle Database
- Management Pack for Oracle WebLogic Server
- Diagnostics Pack for Non-Oracle Middleware
- Provisioning and Patch Automation Pack
- Load Testing for Web Applications
- System Monitoring Plug-in for Hosts
- System Monitoring Plug-in for Non-Oracle Databases
- System Monitoring Plug-in for Non-Oracle Middleware
- System Monitoring Plug-in for Network Devices

service level management capabilities help you define service level objectives (SLO) based on business requirements, model the end-to-end Identity Management service down to the system components it depends on, monitor performance against these goals, and report on service level agreement (SLA) (or operational level agreement (OLA)) to key stakeholders.

With the Management Pack for Identity Management, you can model services for Oracle Identity Management allowing you to view information on the availability of the service based on the underlying Identity Management components that host the service or based on service tests that most closely match the critical functionality of your Identity Management process. Aggregated information on the status of the service and underlying components are summarized on the Identity Management Service home page allowing you to obtain an overall perspective on the environment and monitor service level agreements (SLAs) in real-time. Additionally, the Management Pack for Identity Management allows you to create customized reports that can be used to communicate SLA compliance to the application owners.

Service	Status	Performance	Usage and Business Indicators	Components	Service Level		
					Last 24 Hours	Last 7 Days	Last 31 Days
Oracle Access Manager - Access Service	Up	CPU Utilization (%) 0.00 Perceived Total Time... 0.00 Failed Authentications...	0.00 Total Failed Authent... 0.00 Total Users Sessions No Data LDAP client connect...	1 Up	100.00%	100.00%	100.00%
Oracle Access Manager - Identity Service	Up	CPU Utilization (%) 14.00 Perceived Total Time... 0.00 Average Service Time...	0.00 Number of requests f... 0.00 Total Failed Logins 0.00 Total Users Sessions	1 Up	100.00%	100.00%	100.00%
Oracle Identity Federation Service	Up	CPU Utilization (%) 11.00 Perceived Total Time... 0.00 Request Processing T...	0.00 Active HTTP Connecti... 0.00 Total Users Sessions No Data Total Open Login Ses...	1 Up	100.00%	100.00%	100.00%

Figure 3. Oracle Identity Management Services Dashboard

Contact Us

For more information about [insert product name], please visit oracle.com or call +1.800.ORACLE1 to speak to an Oracle representative.

| Oracle is committed to developing practices and products that help protect the environment

Copyright © 2010, Oracle and/or its affiliates. All rights reserved.

This document is provided for information purposes only and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. UNIX is a registered trademark licensed through X/Open Company, Ltd. 0110