An Oracle White Paper
April 2009

Leading Practices for Driving Down the Costs of Managing Your Oracle Identity and Access Management Suite

ORACLE

INTRODUCTION

Identity Management has become more visible as a business requirement across all industries and affects organizations of all sizes. In the current environment a security breach has the potential to impact a business's bottom line - damaging its reputation, customer loyalty and profitability. Furthermore, compliance with governance and privacy regulations has put an unprecedented executive level focus on the need for strong security controls. This becomes a challenging task in a constantly changing environment where granting appropriate and timely access to information is critical. Oracle Identity Management addresses how organizations can effectively authenticate people, manage their access to confidential information, and audit the transactions that flow between the various systems.

The Oracle Identity and Access Management Suite is a comprehensive identity and access management solution that provides best-in-class technologies including: web access control; identity administration; user provisioning; federated identity management; directory services; and enterprise wide user provisioning. The Oracle Identity and Access Management Suite is comprised of Oracle Access Manager, Oracle Identity Federation, Oracle Identity Manager, Oracle Internet Directory and Oracle Virtual Directory.

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. In addition to the Identity Management Pack, Oracle provides a set of tools that complement the pack and that cover the entire Identity Management lifecycle. In the following pages, we'll describe how you may use the Identity Management Pack as well as other Oracle tools to manage your Oracle Identity Management environment.

ACHIEVING A SUPERIOR OWNERSHIP EXPERIENCE FOR ORACLE IDENTITY MANAGEMENT WITH THE MANAGEMENT PACK FOR IDENTITY MANAGEMENT

Businesses today are relying more and more on automated business processes through packaged applications or home grown custom-built applications. As applications become more critical to the business, a top-down approach to managing them becomes paramount. Oracle offers a unique solution for managing applications with a top-down approach across the entire Oracle application stack ranging from packaged and SOA applications, middleware, database, Linux, and virtualization. Specifically, a key requirement for managing Oracle Identity and Access Management Suite is the ability to manage the entire Identity Management stack, which includes IdM-specific components such as Oracle Access Manager – Access Server, Oracle Access Manager – Identity Server, Oracle Identity Manager Server, Oracle Identity Manager Repository, Oracle Identity Federation Server, and Oracle Internet Directory, as well as infrastructure components such as databases, application servers and operating systems. All these components must work optimally together in order to deliver the availability and performance required of your Oracle Identity Management environment. Therefore, it is important that all these components be managed together. Oracle provides Oracle Management Pack for Identity Management (the Identity Management Pack) to provide an integrated and top-down solution for your Oracle Identity Management environment.

The Identity Management Pack leverages Oracle Enterprise Manager Grid Control's broad set of capabilities in performance monitoring and diagnostics, service level management, and configuration management to manage the end-to-end Oracle Identity and Access Management Suite environment. Single-step discovery of Oracle Access Manager, Oracle Identity Manager, and Oracle Identity Federation allows you to quickly set up your monitoring environment. With the Identity Management Pack, you can proactively monitor your Oracle Identity and Access Management Suite 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 and Access Management Suite 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 or completing a certain operation against an LDAP server. The tests are run via beacons from locations within your network to actively measure the performance and availability of your Identity and Access services. Finally, yet importantly, the Identity Management Pack provides service level management capabilities that allow you to model your 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 (SLO's). This approach helps you focus your resources on issues that are truly important – those that actually impact your business.

The Identity Management Pack is complemented by other Oracle products such as Oracle Access Manager Client Tools (including Identity System Console and Access System Console), Oracle Identity Manager Administrative and User Console, Oracle Identity Manager Diagnostic Dashboard, Oracle Identity Federation Administration Console, Oracle Identity Federation Monitoring Console, Oracle BI Publisher (for publishing reports for Oracle Identity Manager and Oracle Access Manager), Oracle Application Testing Suite, Oracle Database Management Packs, Oracle Middleware Management Packs, Oracle Provisioning Pack and System Monitoring Plug-in's for third party technologies to provide management coverage for your entire system environment, and support for each phase of the Identity Management lifecycle.

COMPLETE IDENTITY MANAGEMENT LIFECYCLE COVERAGE

The deployment of Oracle Identity Management systems goes through three distinct phases – Implement, Manage, and Optimize. In the very first implementation cycle, you need to plan your installation and set up the application servers, LDAP servers and databases associated with your Identity Management deployment. In subsequent cycles, you may take an already deployed Oracle Identity Manager, Oracle Access Manager or Oracle Identity Federation and make further configuration changes to the systems. Throughout the implementation process, you need to constantly test the Identity Management systems to make sure that they are meeting your performance targets. You would also be constantly migrating configuration changes from development to test to staging environments. Ultimately, when you are ready to go live with your Identity Management systems, you would deploy your tested configuration from staging to production environment.

As you enter production, the focus shifts to management. You need to monitor the performance and availability of the Identity Management environment from both end user and system component perspectives. If a problem is detected, you need to triage the problem quickly and engage the right expert to locate the problem root cause. In addition, you need to monitor operational changes that are made to the environment on an on-going basis to ensure that these changes do not introduce problems into your environment.

Lastly, you need to "fine tune" your environment in order to achieve further optimization. The starting point of this process is a set of service level and capacity utilization reports that provide insight into the performance, availability and resource utilization of your Identity Management environment. You may use the information provided by these reports to decide whether to apply software patches from Oracle, tune the LDAP server, or make functional adjustments to the deployed Identity Management systems in order to improve the end user experience.

In the following pages, we'll describe how you may use various Oracle technologies to accomplish tasks in each of the three application lifecycle phases.

IMPLEMENT

Challenge 1 – Orchestrating Controlled Installation and Deployment of Oracle Identity Management

After load tests confirm the desired performance characteristics of the deployed Identity Management system, you are ready to have your administrators deploy the Identity Management systems into production.

Before you install Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation in production, you need to go through the pre-installation instructions and configure all the components associated with these deployments – including application servers, LDAP servers and databases. Oracle Identity Manager provides a Diagnostic Dashboard that allows you to check the pre-installation and post-installation environments for components required by Oracle Identity Manager. The Diagnostic Dashboard is a Web application that runs on the application server and is highly recommended before installing Oracle Identity Manager.

Once your Oracle Identity Management systems are installed and appropriately configured, you can now set up your environment by completing the administrative tasks associated with configuring users, groups, policies and defining approval and provisioning processes. For Oracle Access Manager, you would need to configure both the Identity System and the Access System. To configure the Identity System applications, you need to know what attributes in the directory you want to display, and what attributes you want to be able to modify. After configuring the Identity System to work with data in your directory, you can configure structural object classes for the User Manager, Group Manager, and Organization Manager, and define rules for how to display attribute values on an Identity System application profile page. You can also define Identity workflows, which include series of steps for creating, deleting, and modifying attributes in the Identity System, configure password policies and delegate administration. The Access System enables you to control who is allowed to access data. You can create access policies that extend beyond the Identity System applications. To configure the Access System, you need to create a policy domain and define resources to protect. You can also define authentication and authorization schemes, create a master audit rule, and set up single sign-on to allow users to authenticate to multiple applications with one login.

For Oracle Identity Manager, you would need to create or import users, organizations, and user groups, and define access policies and provisioning/approval processes. An Oracle Identity Manager User can be created through reconciliation from one or more trusted identity sources, such as HRMS or LDAP, manually through the Administrative and User Console, or through the Java APIs and/or the SPML Web Service. You can then create organizations and user groups,

and define access policies, which govern the list of users and resources that can be provisioned or revoked. Finally, you can set up your approval process, which determines whether a resource is to be approved for provisioning to one or more users or organizations.

When deploying Oracle Identity Federation in a network of trusted sources and destinations, you will need to exchange information with other site administrators, and configure identity providers and service providers accordingly. You will need to establish cross-domain trust by setting up authentication and exchanging keys or certificates among the network of trusted sources and destinations. Besides exchanging identities and securing communications involving those identities, parties that plan to engage in a federated network must agree on a range of additional topics, such as: federation protocols, services, and profiles. You will need to work with others in your network to ensure that the various Identity Providers and Service Providers understand their business partners' setups in order for federation to work properly.

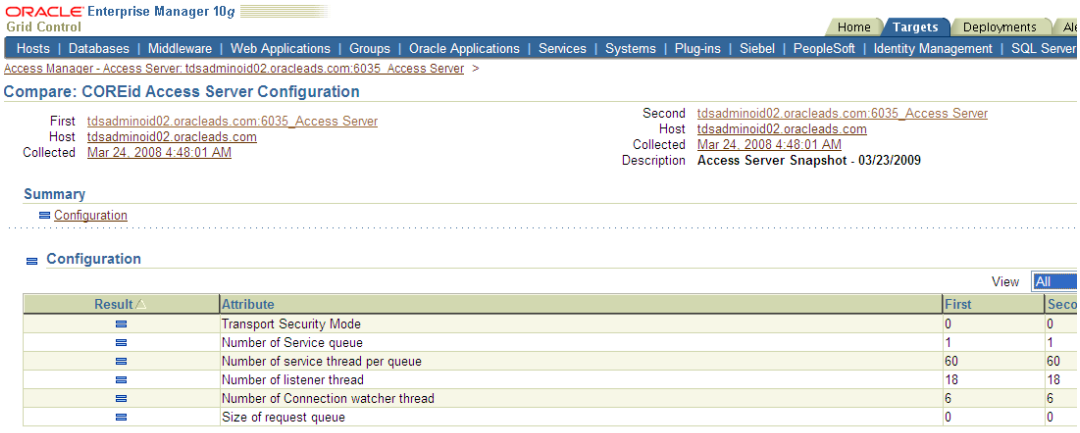

Figure 1 – Configuration Comparison

To ensure that the configurations of Oracle Access Manager – Access Server and Oracle Access Manager – Identity Server in your production environment are consistent with your staging or test environments, your administrators may also use Identity Management Pack's Configuration Comparison tool to compare the configuration in the production environment against the test or stage environments.

MANAGE

Challenge 2 – Aligning Identity Management Priorities with Business Demands

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 IT 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.

Identity Management Pack's 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.

Service Level Objectives can be specified not only in terms of the system-level metrics for the components supporting the service, but also in terms of end user experience metrics. Identity Management Pack is unique in allowing all these classes of metrics to be used in measuring service levels. The basis for the service level management capability is a modeling facility that allows you to define an Identity Management service to be composed of component services and supporting infrastructure.

With the Identity Management Pack, you can model services for Oracle Access Manager, Oracle Identity Manager and Oracle Identity Federation – 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 Identity Management Pack allows you to create customized reports that can be used to communicate SLA compliance to the application owners.

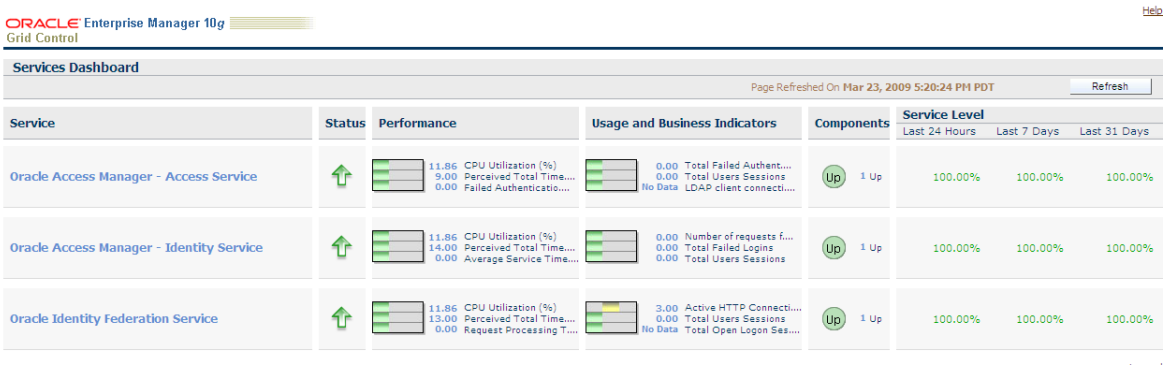

Figure 2 – Oracle Identity Management Services Dashboard

Challenge 3 – Proactive Monitoring of the Complete Oracle Identity Management Environment

In order to deliver the service level required by your application owners, your administrators need to monitor your entire Identity Management environment proactively. This requires them to monitor all the components that make up your Identity Management environment, including Oracle Access Manager – Access Server, Oracle Access Manager – Identity Server, Oracle Identity Manager Server, Oracle Identity Manager Repository, Oracle Identity Federation Server, Oracle Internet Directory, application servers, databases, server machines, network and storage devices. The key metrics that your administrators need to monitor include component up/down status, load, resource utilization, performance, exceptions such as errors/warnings, etc. Many administrators prefer to monitor the Identity Management environment in a "lights out" manner – alerting the administrators only when a problem occurs and allowing them to concentrate on their other duties when the Identity Management systems are functioning normally.

The Identity Management Pack provides an integrated solution for proactively monitoring one or multiple Identity Management environments from a single console. Using the pack, your administrators may monitor the health of all critical Identity Management components, including but not limited to the Oracle Access Manager – Access Server, Oracle Access Manager – Identity Server, Oracle Identity Manager Server, Oracle Identity Manager Repository, and Oracle Identity Federation Server. 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. A complete list of collected metrics is available in the **Getting Started Guide with the Identity Management Pack** (http://download.oracle.com/docs/cd/B16240_01/doc/doc.102/IdentityManagementPack_GS.pdf).

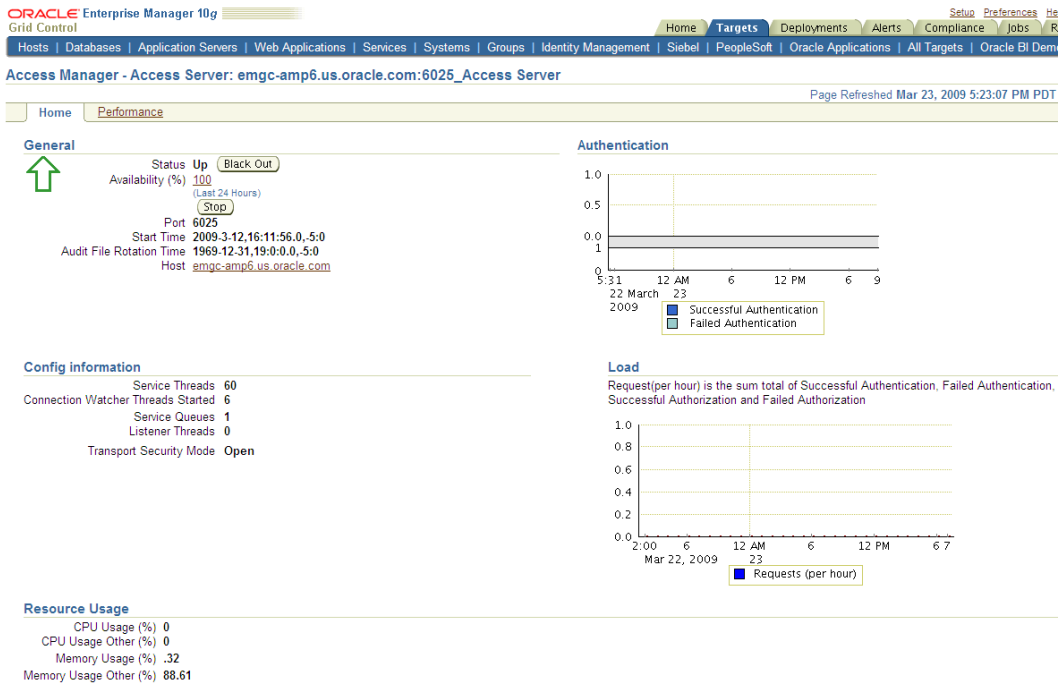

Figure 3 – Oracle Access Manager – Access Server Home Page

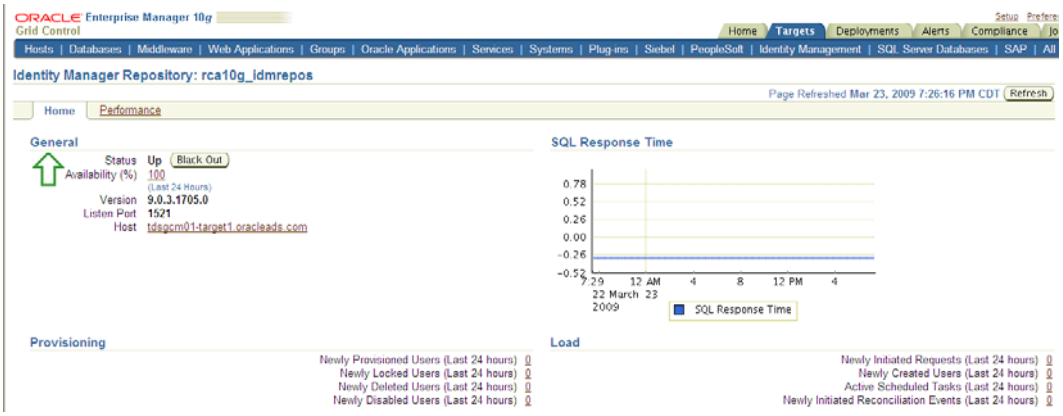

Figure 4 – Oracle Identity Manager Repository Home Page

Log files that are associated with the various Identity Management components (e.g. Oracle Access Manager – Identity Server logs) can be monitored by specifying error codes, or by defining regular expressions that match the log messages. In addition to relying on system performance metrics and error logs, you may use Identity Management Pack'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.

While monitoring the various statistics, you may rely on Identity Management Pack's built-in event management capabilities. Notification methods could be defined to send email, trigger SNMP traps to forward alerts to third party management tools, or to kick off custom scripts. Notification may be defined according to a schedule, so that different administrators who are on duty at different times would get the alerts during their shifts.

To reduce the possibility of false alarms, Identity Management Pack uses several tactics to throttle the rising number of alerts. First, you may define an alert to go off only if a certain condition persists for a certain number of sampling intervals. This approach prevents a singular rogue event such as a spike from triggering un-necessary alert. Second, you may define a "Notification Rule" to stop sending alerts after a certain number of attempts so that you are not alerted repeatedly if a condition persists and you already know about it. Furthermore, you may define threshold alerts against metric snapshots so that the alerts are based on deviation from observed behavior of the components.

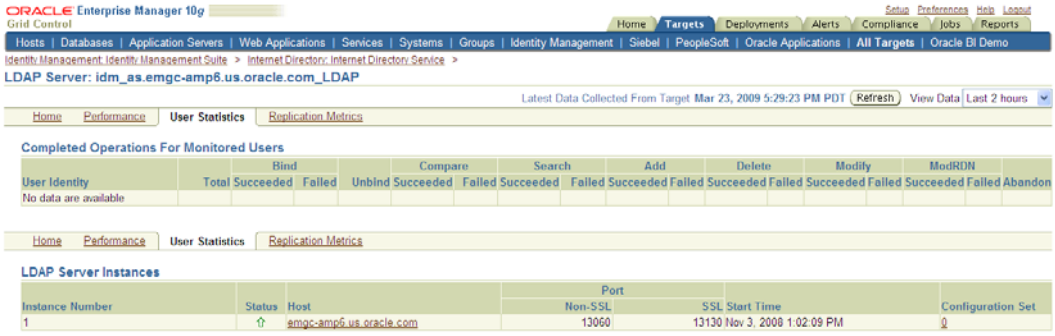

Figure 5 – Oracle Internet Directory User Statistics

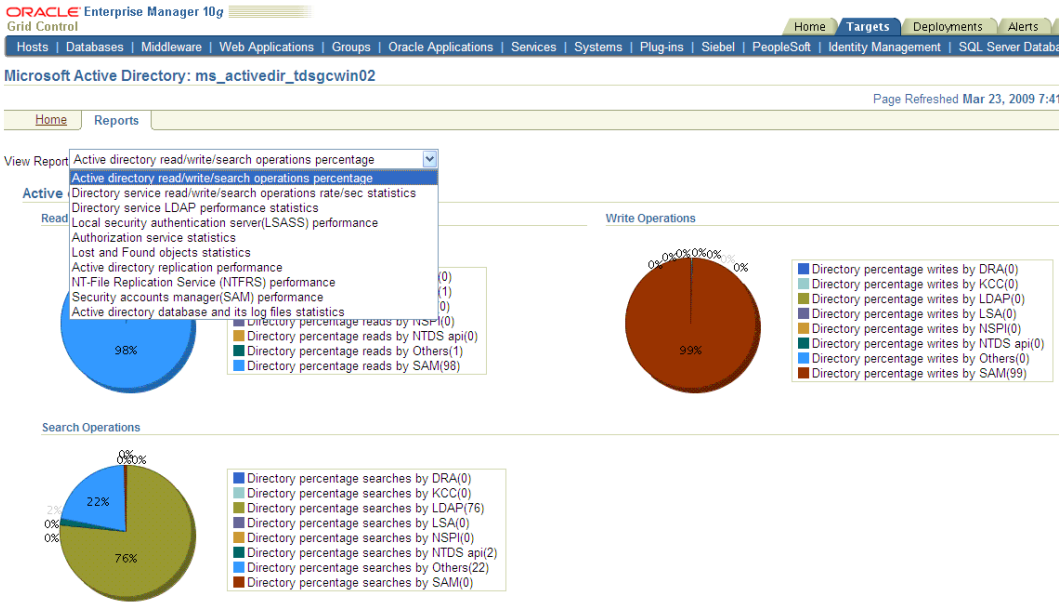

Figure 6 – Microsoft Active Directory Performance Charts

Besides managing the Identity Management components, Oracle Enterprise Manager provides a range of management packs and system monitoring plug-in's to cover the infrastructure components that support the Identity Management deployment. For example, the System Monitoring Plug-in for Microsoft Active Directory leverages Grid Control's management capabilities to provide a complete monitoring solution for the Active Directory. You may mix and match these additional packs and plug-in's to complement the core application monitoring provided by the Identity Management Pack.

If you use Oracle Database in your Oracle Identity Manager or Oracle Identity Federation deployment, you may use Oracle Database Diagnostic Pack for deep monitoring of the database's functions such as tablespace, buffer pool, memory, CPU and I/O. If you use Microsoft SQL Server or IBM DB2, you may use the System Monitoring Plug-in for Non-Oracle Database to perform similar type of monitoring.

Lastly, to monitor infrastructure technologies such as F5 Big-IP Load Balancer, EMC Storage Arrays and NetApp Filers, Oracle offers System Monitoring Plug-in for Network Devices and System Monitoring Plug-in for Storage Devices. Management data collected through these plug-in's as well as from database and middleware packs can be combined with system and end user experience data collected from the Identity Management Pack on the same Oracle Enterprise Manager instance to give Identity Management administrators a holistic, top-down and end-to-end view of the entire Identity Management environment and the extended infrastructure.

All Metrics

Expand All | Collapse All

Metrics	Thresholds	Collection Schedule
idm_as.emgc-amp6.us.oracle.com_LDAP		
(Critical Event)Super User Failed Logins	All	Every 10 Minutes
(Critical Event)Super User Successful Logins	All	Every 10 Minutes
(Critical Events)General System Resource Events	Some	Every 10 Minutes
(Critical Events)System Resource Events(3113 Errors)	None	Every 10 Minutes
(Critical Events)System Resource Events(3114 Errors)	None	Every 10 Minutes
(Critical Events)System Resource Events(Ora Errors)	All	Every 10 Minutes
(Resource Statistics)LDAP Server Memory Growth	None	Every 10 Minutes
(Resource Statistics)LDAP Server's Active Database Connections	None	Every 10 Minutes
(Resource Statistics)LDAP Server's Open Database Connections	None	Every 10 Minutes
Closed LDAP Logon Session Statistics	None	Every 10 Minutes
Configuration sets of LDAP Server	None	Real-time Only
LDAP Entry Cache Hit Ratio	None	Every 10 Minutes
LDAP Load	None	Every 10 Minutes
LDAP Operation Latency	None	Every 10 Minutes
LDAP Operations Profile	None	Every 10 Minutes
LDAP Response	None	Every 10 Minutes
LDAP Server Resource Usage	None	Every 15 Minutes
LDAP Server Total User Sessions	None	Every 10 Minutes
New LDAP Logon Session Statistics	None	Every 10 Minutes
Open LDAP Logon Session Statistics	None	Every 10 Minutes
Replication Server Configuration Set Information	None	Real-time Only
Response	All	Every 5 Minutes
Running instances of LDAP Replication Server	None	Real-time Only
Running instances of LDAP Server	None	Real-time Only
Size of Audit Log Purge Queue	All	Every 10 Minutes
Size of General Statistics Purge Queue	All	Every 10 Minutes
Size of Health Statistics Purge Queue	All	Every 10 Minutes
Size of Security Refresh events Purge Queue	All	Every 10 Minutes
Size of System Resource events Purge Queue	All	Every 10 Minutes
Size of Tombstone Purge Queue	All	Every 10 Minutes
Stopped instances of LDAP Server	None	Real-time Only
Total Number ChangeLogs in Purge Queue	All	Every 10 Minutes
Total Number Remote ChangeLogs in Purge Queue	All	Every 10 Minutes
Total Number of HIQ ChangeLogs	None	Every 10 Minutes
Total Number of Local ChangeLogs	None	Every 10 Minutes
Total Number of New ChangeLogs	None	Every 10 Minutes
Total Number of Retry ChangeLogs	None	Every 10 Minutes
Total number ChangeLogs to be processed	All	Every 10 Minutes
User LDAP Operations Stats	None	Every 10 Minutes

Figure 7 – Oracle Internet Directory All Metrics

Challenge 4 – Monitoring Performance and Availability

No matter how well tuned the Identity Management environment is during testing, production performance problems may still occur because of unforeseen usage or interdependencies with other components of the IT infrastructure. Studies indicate that most performance issues are still reported first by end users before IT administrators find out about them. Unfortunately, this delay means that business operations have been impacted.

Your administrators need to proactively identify the user issues before the end user community is impacted by a performance problem. Some of the questions that your IT staff needs to answer related to the end-to-end monitoring are:

- Can end-users access and quickly load Identity Management services – including single sign-on and access to resources?
- Can end users be authenticated and authorized successfully?
- Are performance problems impacting all end-users or are they limited to a geographical region?

In addition to monitoring the wide range performance metrics collected by Grid Control for all critical Identity Management components (refer to Challenge 3), you can use Identity Management Pack's synthetic service test to monitor availability and performance. These tests are designed to simulate key end user activities such as authenticating against a certain Access Server through a WebGate or logging into an Identity Server through a WebPass. The tests are run via "beacons" from locations within your network to actively measure the performance and availability of your Identity Management environment from an end user perspective. In addition to synthetic web transactions, Oracle 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. Because these tests are played back automatically via beacons and do not rely on actual end users being present, they can be used for accurate performance trending analysis and for proactive monitoring.

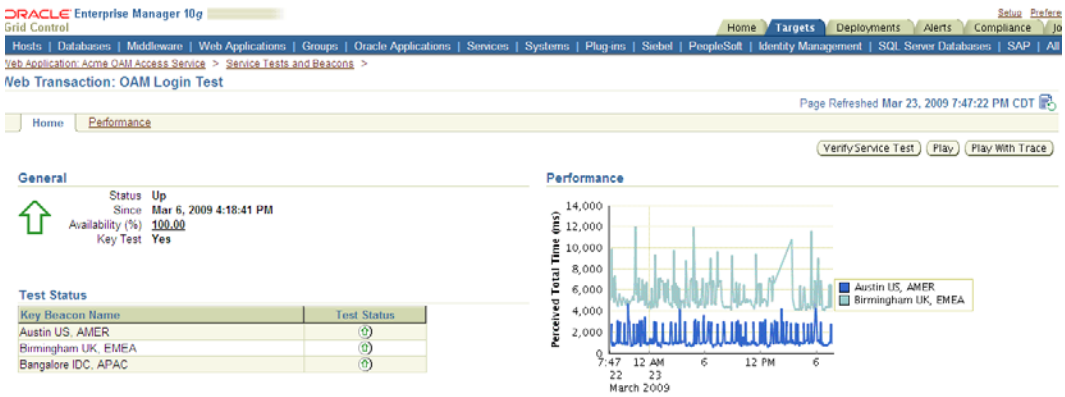

Figure 8 – Synthetic Service Test Performance Chart

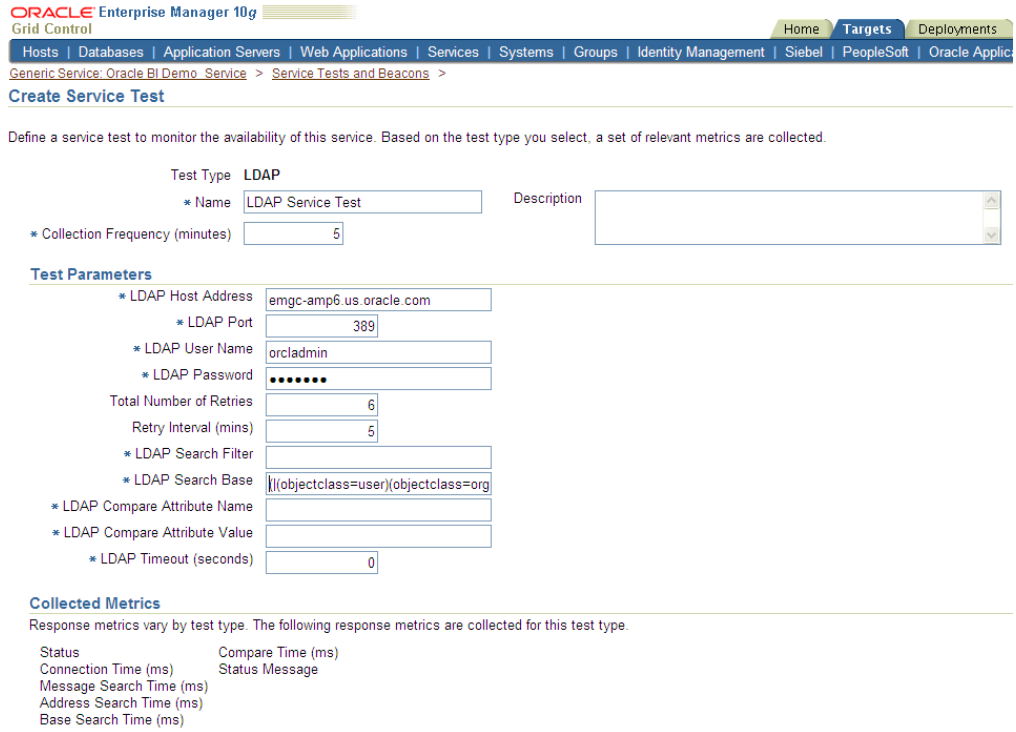

Figure 9 – LDAP Service Test

Challenge 5 – Diagnosing Production Problems Quickly

When problems are detected, you need to fix them quickly in order to minimize impacts to your end users. Diagnosing problems can be a very tedious task often involving guesswork because of difficulties in accessing pertinent diagnostic information and because of the large number of components in an Identity Management environment. Performing diagnostics can be a resource intensive task, often requiring several people involved in managing the Identity Management environment – including Identity Management administrators, database administrators, OS administrators and network administrators. If every problem needs the attention of all the administrators, then the task of diagnosing problems will be very expensive and time consuming to perform.

The Identity Management Pack simplifies diagnostics by presenting relevant diagnostic information and providing tools to analyze information from the different parts of the Identity Management environment. The pack simplifies initial problem triage so that the task can be done quickly and with fewer people. It also provides deep diagnostic capabilities to identify problems that are caused by a specific Identity Management component.

The starting point of a diagnostic effort is examining the Identity Management Service. With the Identity Management Pack, users can create targets of type Generic Service associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, and Identity Manager System. The Generic Service target provides an end-to-end service oriented view of the monitored Oracle Identity Management targets with access to performance and usage metrics, service tests, service level rules, service availability definition, alerts, charts, and topology view. The Identity Management Service home page shows the availability of the service based on the underlying Oracle 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 components and service tests and critical alerts are summarized on this page allowing you to obtain an overall perspective on the environment before you proceed to deeper investigation.

From the service home page, you may view the availability history of the service and the current service levels. Then, begin the triage process by examining service test statistics to see whether the problem is network location specific. If it is network specific, you may then engage the network administrator to resolve the problem. If not, you may use the Topology Viewer to look at 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. You can also bring up metric history information of the various servers and components to see if the problem is due to over utilization or lack of resource. Identity Management Pack automatically saves all the metrics that are collected from your Identity Management environment, so you can go back to a point in time to examine the state of the system when the problem occurred.

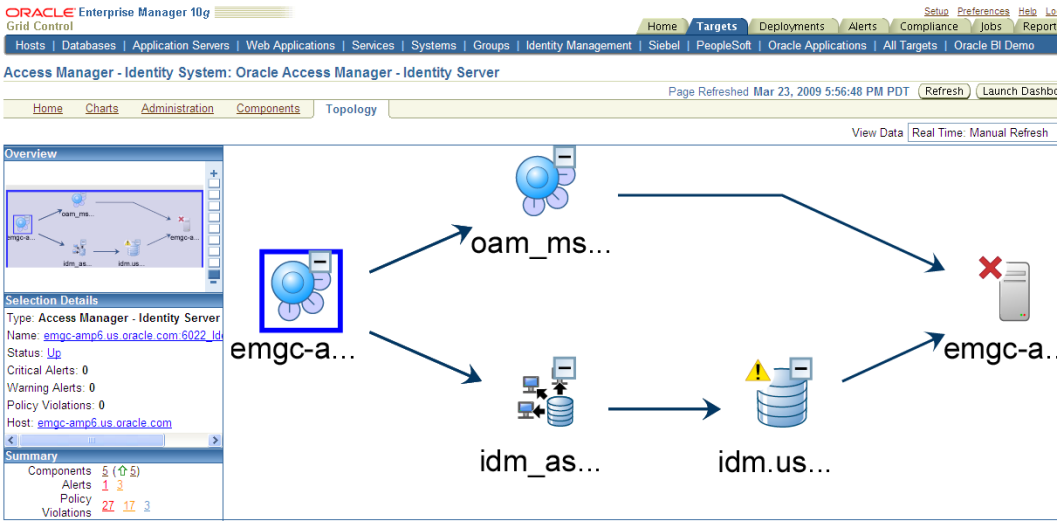

Figure 10 – Oracle Access Manager – Identity Service Topology View

For problems that are more intermittent or are tied to specific requests or users, you can drill down into Identity Management logs to identify the root cause of the problem. With the Identity Management Pack, you can monitor Identity Management log files for the occurrence of user-specific errors or abnormal conditions. Log files are periodically scanned for the occurrence of desired patterns or error codes and an alert is raised when the pattern occurs during a given scan. The logging feature in Oracle Access Manager enables you to collect a wide range of program execution data so that you can troubleshoot system performance issues and diagnose component health problems. You can send the log data generated by a specific component to either of the following destinations, or neither, or both:

- A log file stored in the directory tree under the root installation directory of the component generating the data.
- The system file of the machine hosting the component logging data. (When more than one component resides on the same host, all components can send data to the system log file on that machine.)

For convenience, the many thousands of program events and states reportable through logging in Oracle Access Manager are classified within an eight-level, pyramidal hierarchy. At the highest level, the Fatal category includes about 60 catastrophic events that usually force a component to exit. At the bottom of the pyramid, the Trace level reports about 900 Oracle Access Manager API and 150 third-party API calls and their outcomes.

Oracle Identity Federation also provides a number of log files that are maintained in the $ORACLE_HOME/fed/log directory and that provide useful information for monitoring server instances. The log files include:

- federation.log: This log file contains the runtime log records for the Oracle Identity Federation server.
- federation-error.log: This log file contains error messages generated by the Oracle Identity Federation server.
- federation-msg.log: This log file contains the SAML2.0/Liberty 1.x messages exchanged between Oracle Identity Federation and peer providers.

For problems that may be system configuration related, use Identity Management Pack's configuration analysis tool to locate the cause of a problem in Oracle Access Manager. You may query against Oracle Enterprise Manager's configuration management database (CMDB) to find out whether parameters in Oracle Access Manager – Identity Server or Oracle Access Manager – Access Server have changed. You may also compare configuration settings across different Oracle Access Manager components and between servers to find out why there are discrepancies in behavior amongst different environments.

In addition to logs, audit reports can be used for diagnostic purposes as well. The auditing feature in Oracle Access Manager collects and presents data pertaining to policy and profile settings, system events, and usage patterns. Oracle Access Manager can generate two types of audit reports:

- Static: These reports are derived from policy and profile information that is stored on the Oracle Access Manager directory server.
- Dynamic: These reports are derived from Access System and Identity System events that are collected from the servers in your system.

Preconfigured Oracle BI Publisher audit report templates for Oracle Access Manager are available to download from OTN: http://www.oracle.com/technology/products/id_mgmt/coreid_acc/index.html. Some of the reports that are available for Oracle Access Manager include:

- Access Failures by User: The number of authorization requests from a given user that failed during a given interval.
- Access Failures by Resource: The number of authorization requests for a given resource that failed during a given interval.
- Access Privileges: All the users allowed to access a list containing one or more resources as well as all the resources accessible by a list containing one or more users.
- User Profile History: Changes to password, policy, profile, and so on for all users.
- Group History: A list of groups that a user has been added to or removed from in a given interval.
- Revoked Users: A list of users who have been locked out of the system.

- Deactivated Users: A list of users whose access accounts have been deactivated. Lists of reactivated users can also be generated.
- Password Changes: The number of passwords that have been changed throughout the system during a given interval.
- User Status Changes: The groups to which a given user or users has been added within a given interval.
- Identity History: Changes to password, policy, profile, and so on for one or more individual users.
- Workflow Execution Time: The average and maximum length of time it has taken to complete a workflow during a given period.

Oracle Identity Manager also provides a number of reports that can be used for diagnostic purposes. You can generate operational and historical data reports that provide information about the resources available to Oracle Identity Manager users. While these reports are primarily used by administrators and auditors for compliance and auditing purposes, they can also be helpful in troubleshooting performance problems. Preconfigured Oracle BI Publisher report templates for Oracle Identity Manager are available to download from OTN: http://www.oracle.com/technology/products/id_mgmt/oxp/index.html. Some of the historical reports that can be useful in diagnostics include:

- Resource Activity: Returns the history of all provisioning and approval activities for a resource.
- Password Reset Success Failure: Returns the password change metrics for Oracle Identity Manager users.
- Users Created: Lists all users created in a specified time interval.
- Users Deleted: Lists all users deleted in a specified time interval.
- Users Disabled: Lists all users disabled in a specified time interval.
- Users Unlocked: Lists all users (accounts) unlocked in a specified time interval.

If you use Oracle Database in your Oracle Identity Manager or Oracle Identity Federation deployments, you may use Oracle Database Diagnostic Pack to carry out deep database level diagnostics. The pack includes a self-diagnostic engine built right into Oracle Database kernel, called Automatic Database Diagnostic Monitoring (ADDM). ADDM periodically examines the state of the database, automatically identifies potential database performance bottlenecks, and recommends corrective actions. Oracle Database Diagnostic Pack presents ADDM's findings and recommendations in a convenient and intuitive fashion, and guides administrators step-by-step to quickly resolve performance problems by implementing ADDM's recommendations. ADDM starts its analysis by focusing on the activities that the database is spending most time on and then drills down through a sophisticated problem classification tree to determine the root

cause of problems. The problem classification tree used by ADDM encapsulates decades of performance tuning experience of Oracle's own performance experts and it has been specifically designed to accurately diagnose the most frequently seen problems, such as CPU and I/O bottlenecks, poor connection management, undersized memory, resource intensive SQL statements, lock contention, etc. Each ADDM finding has an associated impact and benefit measure to enable prioritized handling of the most critical issues. To better understand the impact of the findings over time, each finding has a descriptive name that facilitates search, a link to number of previous occurrences of the finding in the last 24 hours, and affected instances.

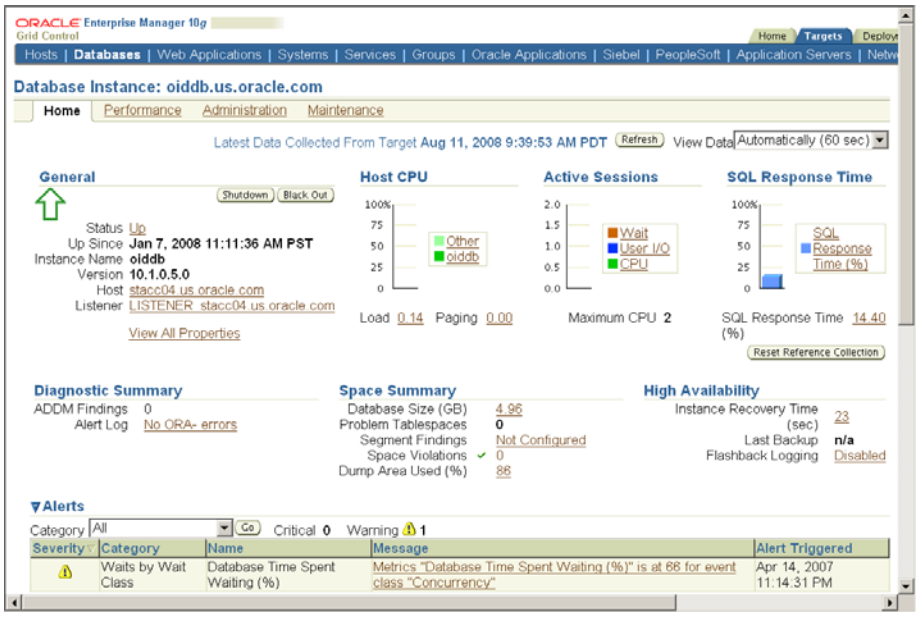

Figure 11 – Oracle Database Diagnostics

OPTIMIZE

Challenge 6 – Making Fact-Based Optimization Decisions

Optimizing an Identity Management environment is a time consuming task often surrounded by myths and legends, few of them based on facts. Like diagnostics, Identity Management optimization is very hard to do unless you have access to the right information. The Identity Management Pack provides the information that you need to make fact-based optimization decisions.

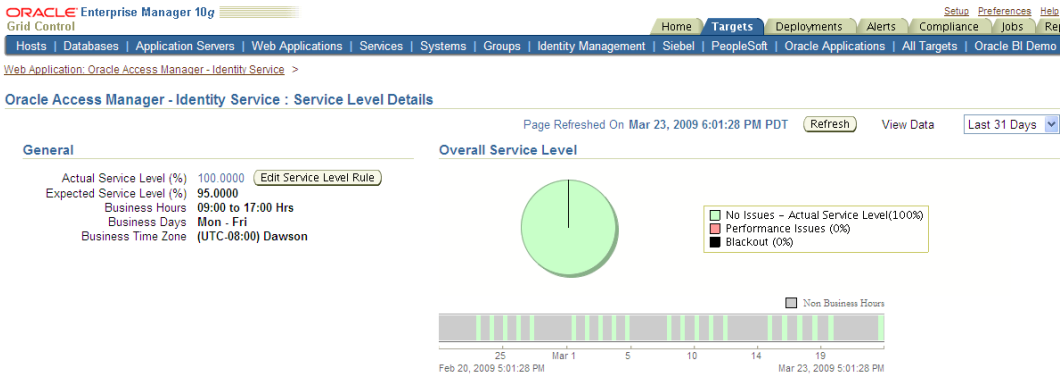

Figure 12 – Service Level Report

The starting point of the optimization process is Identity Management Pack's service level management reports. Based on service level indicators collected from the Identity Management environment over a period, these reports indicate whether the Identity Management services provided the performance and availability needed to support critical business operations. These reports are further complemented by capacity utilization reports of the underlying components, and by audit reports that show the usage patterns of the application.

With this information, you may then decide whether you need to invest in further optimization, which may include tasks such as adjusting the functional configuration of your Identity Management deployment, applying patches from Oracle, tuning the LDAP Server and other Identity Management components, or tuning the database.

To optimize Identity Management components, you need to consider several statistics collected during run-time. These statistics are gathered by the Identity Management Pack and are stored in Oracle Enterprise Manager's repository. You may retrieve them in reports that show the graph of these metrics over time to understand how the Identity Management service environment or compare the metrics across different servers to see if your servers are load balanced properly. Using this information, you may work with your administrators to modify your Identity Management's functional configurations if they prove to be too resource intensive. You may obtain detailed information about Oracle Access Manager – Access Server and Oracle Access Manager – Identity Server through performance charts that can help you identify problems and optimization opportunities. Using this information, you may decide to tune the LDAP Server or tweak the functional configuration to best fit the load profile for your Access Server and Identity Server. You can also monitor the performance of the Oracle Identity Manager Repository and keep track of the number of newly provisioned/created/deleted/disabled/locked users, as well as the number of newly initiated requests. Based on the performance information retrieved for the Oracle Identity Manager Repository, you may decide to log into the Administrative and User Console to verify the requests in queue and make sure the Identity Manager Server is load-balanced.

SUMMARY

Through the Identity Management Pack, you can start centralizing the management of your Oracle Identity Management environment on Oracle Enterprise Manager Grid Control. The Identity Management Pack is designed to complement and extend the bundled tools that are available in the Oracle Identity and Access Management Suite including: Oracle Access Manager Client Tools (like Identity System Console and Access System Console), Oracle Identity Manager Administrative and User Console, Oracle Identity Manager Diagnostic Dashboard, Oracle Identity Federation Administration Console, and Oracle Identity Federation Monitoring Console. While the bundled tools provide tactical administrative functions, the Identity Management Pack leverages Oracle Enterprise Manager's top-down systems management capabilities in performance monitoring and diagnostics, service level management, and configuration management to facilitate proactive monitoring of the end-to-end Oracle Identity Management environment. You can use Oracle Enterprise Manager as the unified console to manage your entire Identity Management infrastructure, including Oracle Access Manager – Access Server, Oracle Access Manager – Identity Server, Oracle Identity Manager Server, Oracle Identity Manager Repository, Oracle Identity Federation Server, Oracle Internet Directory, both Oracle and non-Oracle databases and middleware, as well as your servers, storage and network devices – all of which impact your Identity Management environment's performance and availability. Through the Identity Management Pack, you can achieve a Superior Ownership Experience in manageability and quality for your Oracle Identity Management environment, and deliver the service level required to meet your needs.

Leading Practices for Driving Down the Costs of Managing Your Oracle Identity and Access Management Suite
April 2009
Author: Amjad Afanah
Contributing Authors: Chung Wu

Oracle Corporation
World Headquarters
500 Oracle Parkway
Redwood Shores, CA 94065
U.S.A.

Worldwide Inquiries:
Phone: +1.650.506.7000
Fax: +1.650.506.7200
oracle.com

0109