An Oracle White Paper
September, 2011

Managing Oracle Identity Management with Enterprise Manager 12c Cloud Control

ORACLE

Executive Summary

Oracle Enterprise Manager is Oracle's integrated enterprise IT management product line and provides the industry's first complete cloud lifecycle management solution. Oracle Enterprise Manager's Business-Driven IT Management capabilities allow you to quickly set up, manage and support enterprise clouds and traditional Oracle IT environments from applications to disk. Enterprise Manager allows customers to achieve:

- *Best service levels for traditional and cloud applications* through management from a business perspective including Oracle Fusion Applications
- *Maximum return on IT management* investment through the best solutions for intelligent management of the Oracle stack and engineered systems
- *Unmatched customer support experience* through real-time integration of Oracle's knowledgebase with each customer environment

Introduction

Oracle Enterprise Manager's Fusion Middleware Management solutions provide full-lifecycle management for Oracle Weblogic Suite, Oracle SOA suite, Oracle Coherence, Oracle Identity Management, Oracle WebCenter, and Oracle Business Intelligence Enterprise Edition. Oracle Enterprise Manager provides a single console to manage these assets from a business and service perspective, including user experience management, change and configuration management, patching, provisioning, testing, performance management, business transaction management and automatic tuning for these diverse environments.

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.

As part of Oracle Fusion Middleware, Oracle Identity Management provides a unified integrated security platform designed to manage user identities, provision resources to users, secure access to corporate resources, enable trusted online business partnerships, and support governance and compliance across the enterprise. Oracle Identity Management ensures the integrity of large application grids by enabling new levels of security and completeness to address the protection of enterprise resources and the management of the processes acting on those resources.

Oracle Identity Management provides a comprehensive set of market-leading services including identity administration and role management; user provisioning and compliance; web applications and web services access control; single sign-on and federated identities; fraud detection; strong, multifactor authentication and risk management; role governance and identity analytics, audit and reports. All Oracle Identity Management components leverage the product suite's best-in-class, highly scalable directory and identity virtualization services to maximize operational efficiency and ensure the highest levels of performance and availability.

As more and more businesses rely on the Oracle Identity Management to control access to their mission-critical 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 the Management Pack Plus for Identity Management, which leverages Oracle Enterprise Manager's advanced management capabilities, to provide an integrated and top-down solution for your Oracle Identity Management environment. In addition to the Management Pack Plus for Identity Management, 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 Management Pack Plus for Identity Management as well as other Oracle tools to manage your Oracle Identity Management environment.

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 Management environment 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 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.

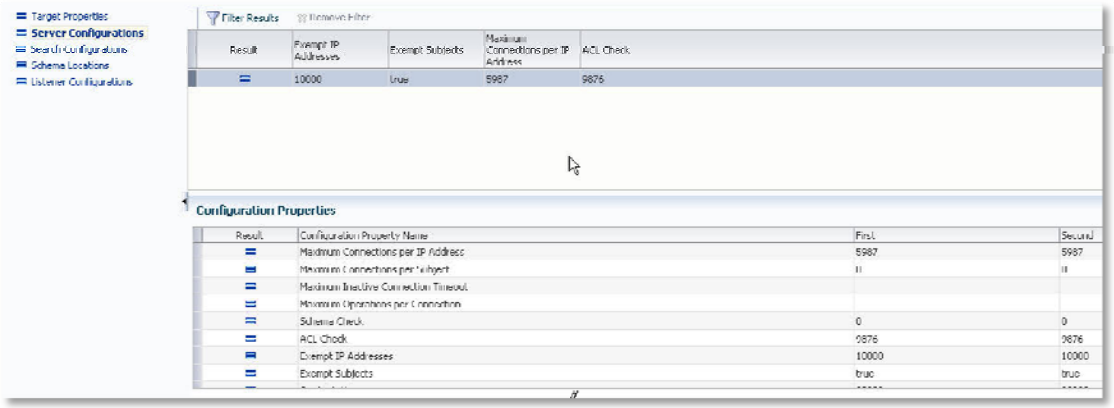

Figure 1 – Configuration Comparison

To ensure that the configurations of Oracle Virtual Directory in your production environment are consistent with your staging or test environments, your administrators may also use Management Pack Plus for Identity Management's Configuration Comparison tool and 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.

Management Pack Plus for Identity Management'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. Management Pack Plus for Identity Management 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 Management Pack Plus for Identity Management, 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 Management Pack Plus for Identity Management allows you to create customized reports that can be used to communicate SLA compliance to the application owners.

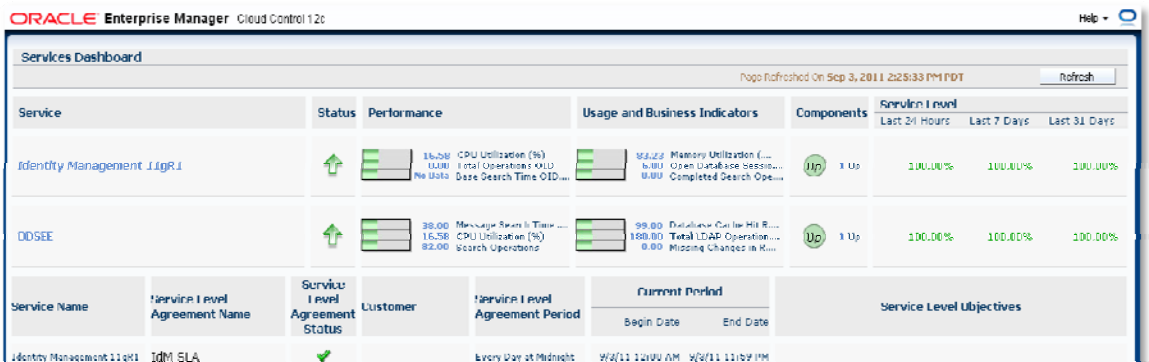

Figure 2 – Oracle Identity Management Services Dashboard

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 Oracle Identity Manager Oracle Internet Directory, Oracle Virtual Directory, Oracle Identity Federation, 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 Management Pack Plus for Identity Management 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 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 Directory Server Enterprise Edition (6.x, 7.x and 11g), Oracle Virtual Directory, Oracle Identity Federation, Oracle Access Manager, Oracle Identity Manager, and Oracle Adaptive Access Manager. 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.

The Management Pack Plus for Identity Management includes a comprehensive set of monitoring and notification features to enable administrators to proactively detect and respond to IT problems across their entire application stack. While Enterprise Manager continues to provide out-of-box monitoring for newly discovered targets, administrators can customize these monitoring settings to fit their

datacenter needs. For database targets, this includes the use of adaptive thresholds which can automatically alert on statistically unusual values of performance metrics based on the database's own performance history. For other target types, easy access to a target's metric history is provided, enabling administrators to determine appropriate threshold values based on the range of typical metric values. If there are conditions specific to the datacenter that need to be monitored, administrators can define new metrics for any monitored target using metric extensions. If an alert has a well-known remediation solution, then administrators can setup corrective action scripts that will automatically execute and resolve the alert when it is detected, thereby minimizing the need for manual intervention. In addition, alert history is also easily accessible to enable administrators to see what actions have been taken in previous occurrences of the alert.

The desired monitoring settings for a target can be defined in a monitoring template, one template per type of target. When a set of monitoring templates for different target types are bundled together into a template collection and associated with an administration group, then the deployment of monitoring settings across targets is fully automated by Enterprise Manager. Specifically, when a target is added to an administration group, the monitoring settings associated with the group are automatically applied to the target, thereby streamlining and simplifying the process of monitoring setup for targets.

Once monitoring is in place and events are detected and raised on monitored targets, notifications for these events can be sent to the appropriate administrators. Notifications include email / page notifications, the execution of custom scripts and PL/SQL procedures, and the sending of SNMP traps. In addition, management connectors can also be used to open helpdesk tickets for incidents (based on important events) and/or send event information to other third party management systems.

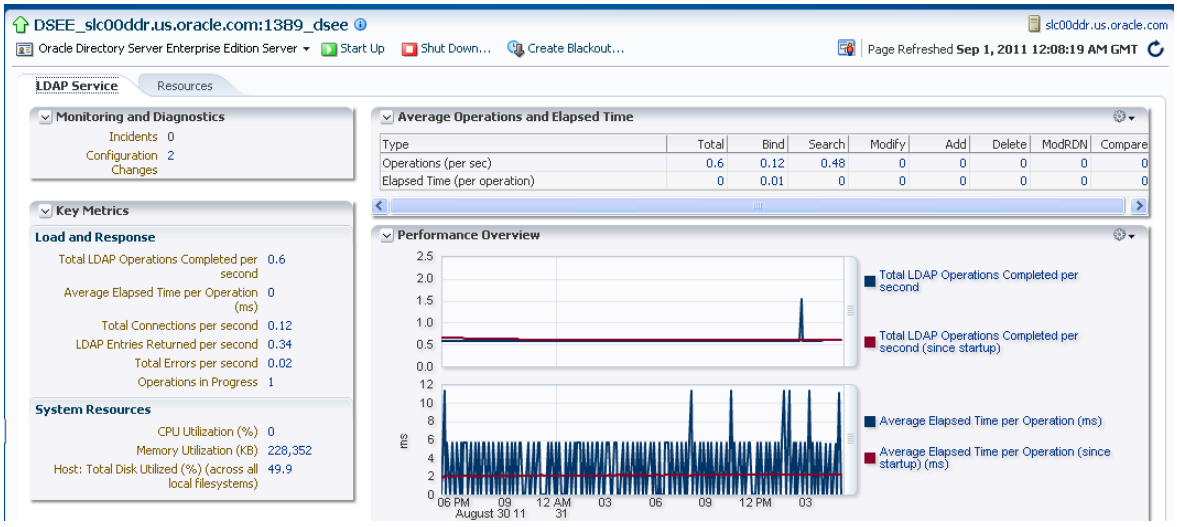

Figure 3 – Oracle Directory Server Enterprise Edition Home Page

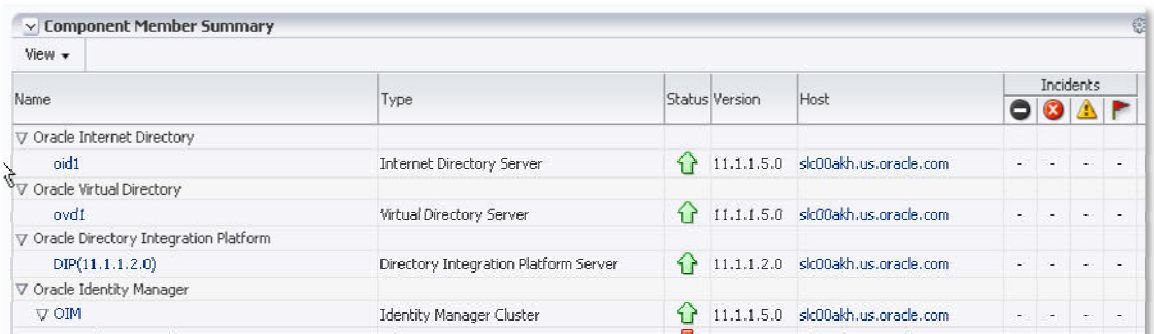

Figure 4 – Identity and Access Dashboard – Component Member Summary

Log files that are associated with the various Identity Management components (e.g. Oracle Access Manager 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 Management Pack Plus 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 Internet Directory, Oracle Directory Server Enterprise Edition, Oracle Unified Directory, and 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.

To reduce the possibility of false alarms, Management Pack Plus for Identity Management 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.

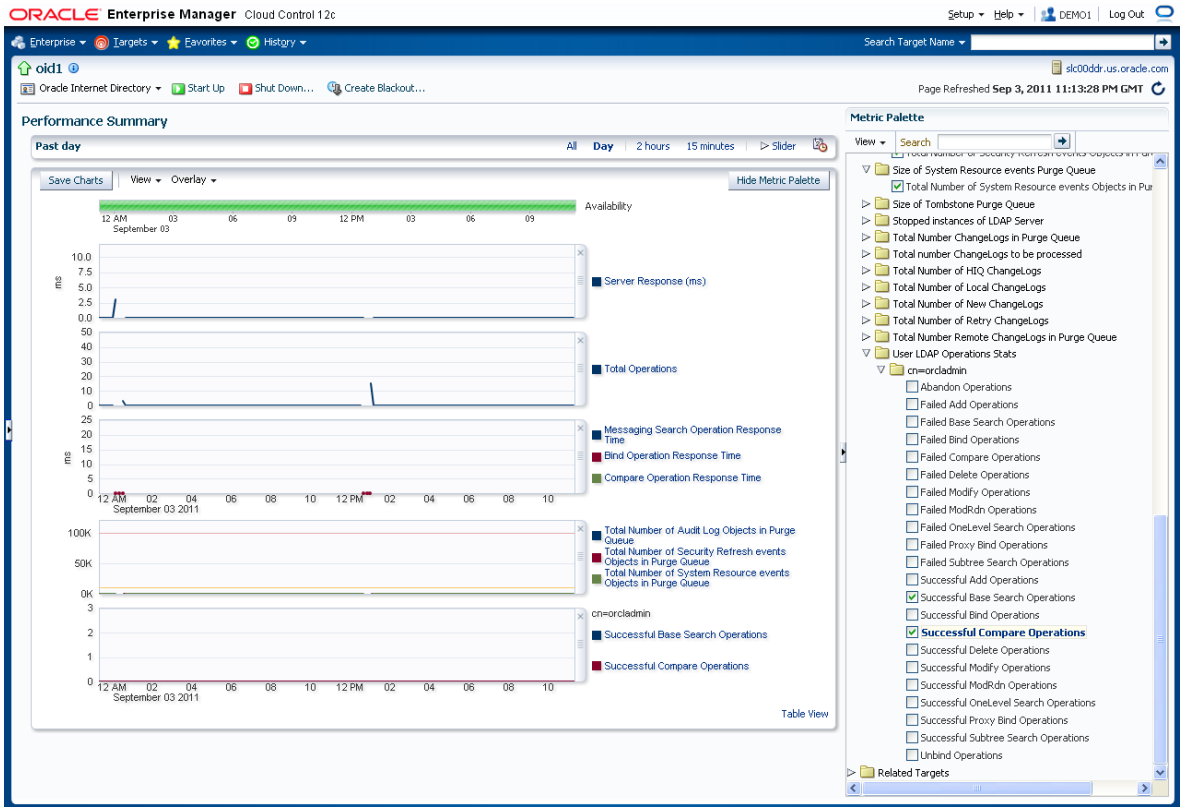

Figure 5 – Oracle Internet Directory Performance Summary

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 Enterprise Manager'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 Management Pack Plus for Identity Management.

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 Management Pack Plus for Identity Management 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.

Challenge 4 – Monitoring End User Experience

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 Identity Management 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 end user issues before the end user community is impacted by a performance problem. The first step in guaranteeing end-user satisfaction is to learn about the end-user performance experience. Some of the questions that your IT staff needs to answer related to the end-user performance experience are:

- Are end-users satisfied with the performance of Identity Management services – including single sign-on and access to resources?
- Are end users authenticated and authorized successfully?
- Are performance problems impacting all end-users or are they limited to a geographical region?

To monitor your end users' experience, you can use Management Pack Plus for Identity Management's synthetic service test. These tests are designed to simulate key end user activities such as authenticating against a certain Access Server through a WebGate. 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.

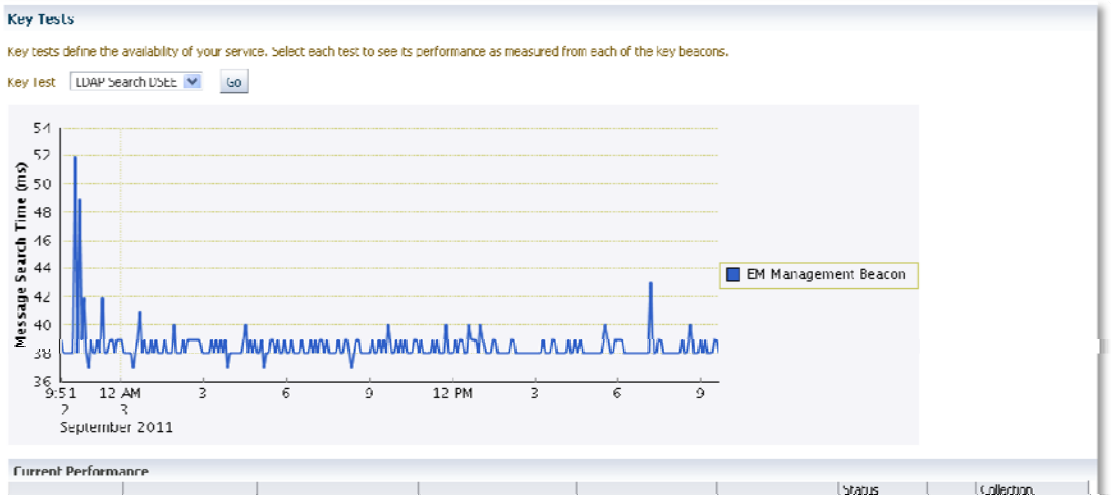

Figure 6 – Synthetic Service Test Performance Chart

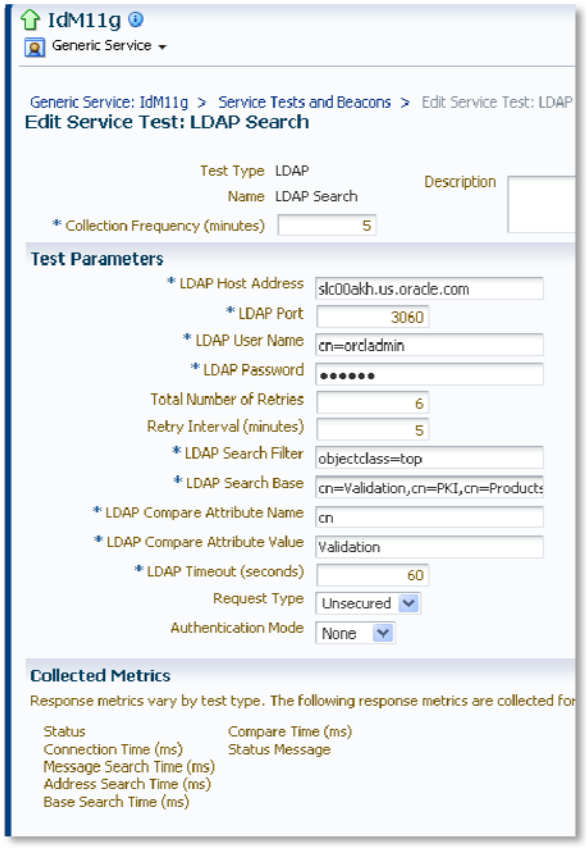

Figure 7 – LDAP Service Test

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 Management Pack Plus for Identity Management 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 Management Pack Plus for Identity Management, users can create targets of type Generic Service associated with any of the monitored Identity Management Systems: Access Manager – Access System, Access Manager – Identity System, Identity Federation System, 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. Management Pack Plus for Identity Management 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 8– Configuration Topology of Identity Management 11g Service

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 Management Pack Plus for Identity Management, 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.

For problems that may be system configuration related, use Management Pack Plus for Identity Management's configuration management features to locate the cause of a problem in the Identity Management deployment. You may query against Oracle Enterprise Manager's configuration management database (CMDB) to find out whether parameters in the monitored Identity Management components have changed. You may also compare configuration settings across different Oracle

Identity Management 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. 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. 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.

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 Management Pack Plus for Identity Management provides the information that you need to make fact-based optimization decisions.

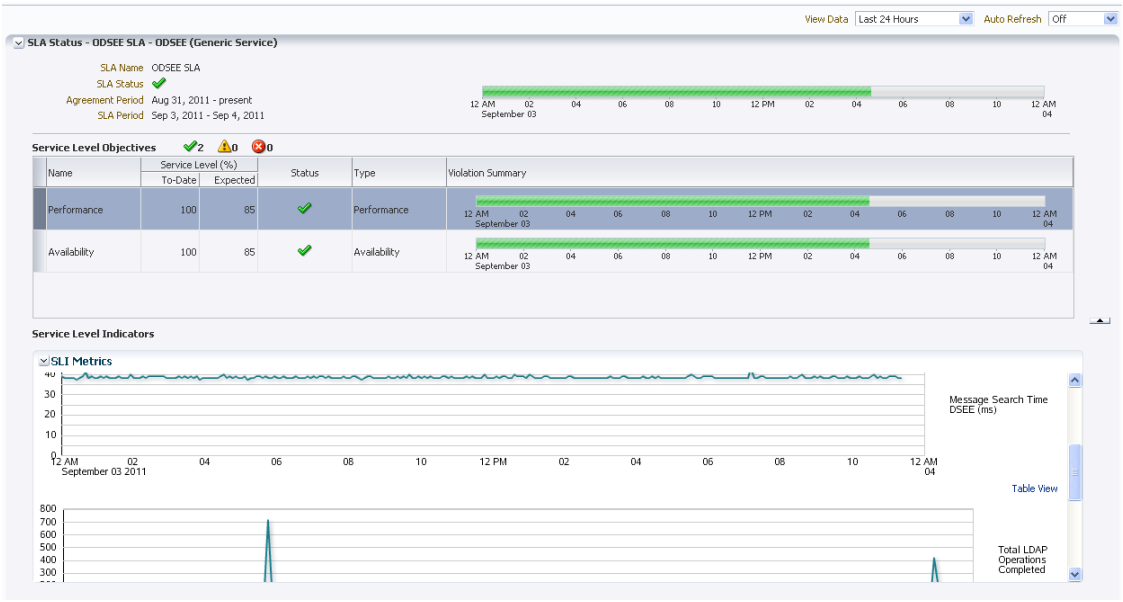

Figure 9 – Service Level Agreement Dashboard

The starting point of the optimization process is Management Pack Plus for Identity Management'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 Management Pack Plus for Identity Management 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.

Conclusion

Through the Management Pack Plus for Identity Management, you can start centralizing the management of your Oracle Identity Management environment on Oracle Enterprise Manager. The Management Pack Plus for Identity Management is designed to complement and extend the bundled tools that are available in the Oracle Identity Management. While the bundled tools provide tactical administrative functions, the Management Pack Plus for Identity Management 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.

Managing Oracle Identity Management with Enterprise Manager 12c Cloud Control
September, 2011
Author: Amjad Afanah
Contributing Authors: Rajiv Taori, James Kao

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

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

Hardware and Software, Engineered to Work Together