

An Oracle White Paper
August 2010

Case Study – Optimizing E-Business Suite Management Using Oracle Application Management Suite for Oracle E-Business Suite

Disclaimer

The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described for Oracle's products remains at the sole discretion of Oracle.

Contents

Executive Summary.....	3
Introduction.....	6
About the Application Management Suite	6
About Oracle Corporation’s Global Single Instance	7
Organizational Responsibilities/Matrix	9
Impact of the Management Suite on IT Operations and Management	10
Middleware Component Management	10
Performance Management.....	10
Centralization and Standardization of Tools and Processes.....	10
Reporting Efficiencies.....	11
Consumers of Management Suite Data	11
Considerations on the Installation and Discovery Process.....	13
Autoconfig.....	13
Socket vs. Servlet Mode.....	13
Leveraging Single Sign-On	13
Middleware Changes.....	13
Java Virtual Machine	14
AMP Implementation Process, Tools, and Examples.....	15
Oracle’s process for configuring AMP	15
Standard Metrics	17
User Defined Metrics.....	20
Automated Corrective Actions.....	21
Policies	22
Monitoring Templates.....	24
Leveraging Group Functionality	25
Group Administration.....	25

System Group.....	26
Notification Rules.....	26
Performance Monitoring	29
Java Virtual Machine Administration and Monitoring.....	31
Concurrent Manager Administration	33
Workflow Manager Administration	35
Information Publishing (Reporting) & Dashboards	37
Application Service Level Management	41
Further Information	42
Conclusion.....	43
Appendix A – Permissions Changes for iAS Tech Stack.....	44
Appendix B – JVM Access Setup	48

Executive Summary

The purpose of this section is to summarize the key points of the entire document. The critical points from this whitepaper are:

- The document highlights the process and results of the real-world implementation of the Application Management Suite for E-Business Suite for Oracle Corporation’s Global Single Instance (GSI) of E-Business Suite.
 - It provides an in-depth review of the monitoring and management capabilities of the Management Suite, as well as practical guidance on how native Enterprise Manager Functionality (i.e., Metrics (Standard and Custom), Templates, Groups, System Groups, Alerts, Notifications, Reports and Dashboards, Service Level Monitoring) was applied to the management of E-Business Suite components.
- The implementation of the Management Suite resulted in a 66% reduction in error resolution time for E-Business Suite-related issues.
- The implementation the Management Suite freed up DBA time by approximately 35%, allowing administrators to concentrate on higher value-added tasks, projects, and new features.
- Management Suite functionality enabled system administrators to manage their E-Business Suite instances more proactively, thereby improving system availability, reliability, and predictability.
- Management Suite functionality enabled executive management to make better, timelier decisions on the use of resources – both hardware and personnel.
- The implementation allowed the GSI team to re-engineer their support structure by:
 - Eliminating proprietary tools/solutions
 - Centralizing on a common toolset and reporting structure
 - Standardizing processes
 - Expanding the usage and footprint of Oracle Enterprise Manager
- For the first time, administrators were able to obtain E-Business Suite-specific activity and data, such as:
 - Java Virtual Machine (JVM) – The ability to quickly and easily determine JVM activity, including CPU, memory, active threads, memory pools, metrics, and more.
 - Concurrent Manager – The ability to streamline the monitoring, alerting, and reporting on various aspects of concurrent manager, ensuring maximum

availability.

- Forms and OA Framework Services - The ability to monitor services and metrics associated with Forms (socket-mode) and Self-Service Apps.
- Workflow – The ability to report on activity, up/down status, set metrics, and manage Workflow activity.
- Configuration reporting – The ability to archive point-in-time configurations, for either reference or comparison purposes for patches, personalizations, profile options, workflow services, to name a few.
- The implementation team made extensive use of standard Enterprise Manager functionality to manage and report on E-Business Suite components, including:
 - Metrics – Both Standard and User-Defined (i.e., Custom) metrics were set on E-Business Suite components to enable administrators to set thresholds, alerts, and notifications. The result is that administrators can be more proactive in managing E-Business Suite instances.
 - Templates – Templates were used to standardize which metrics were implemented for certain targets. Not only did this speed the discovery process, but also enabled the comparison of metrics between different targets.
 - Groups and System Groups – Group functionality was used to band together many related targets into a single unit. This enabled mass updates of settings to targets within the same group, as well as comparison between groups. In addition, System Groups are a cornerstone for Dashboards and Application Service Level Management (ASLM).
 - Reporting and Dashboards – One of the core aspects of Enterprise Manager is the reporting capabilities – both standard and custom. The team leveraged this capability for trending analysis, historical analysis, operations reports, and executive reports. Reports that had previously taken several hours to collate and prepare, could now be done in a matter of minutes.
- This document focuses on the monitoring capabilities of Application Management Suite for Oracle E-Business Suite. The project utilized the majority of management suite. Certain aspects of the management suite are currently under review, including “Automated Cloning” and “End-User Monitoring”.
- This document does not address the base installation of the Management Suite. It assumes a successful installation of the product, including any and all patches, as well as a successful discovery of the E-Business Suite instance.
- **Important:** In August of 2010, Oracle created the “Oracle Application Management Suite for Oracle E-Business Suite”, which is comprised of four previously independent Oracle products; Real User Experience Insight (RUEI), Oracle Application Management Pack for E-Business Pack (AMP), Oracle Application

Change Management Pack for Oracle E-Business Suite (ACP), and the Oracle Configuration Management Pack for Applications. For the purposes of this document, “Oracle Application Management Suite for Oracle E-Business Suite” and “Oracle Application Management Pack for Oracle E-Business Suite (AMP)” can be used interchangeably.

Introduction

The purpose of this document is to highlight the process and results of a real-world implementation of the Application Management Suite for E-Business Suite for Oracle Corporation's Global Single Instance (GSI) of E-Business Suite.

This document also provides practical guidance on how native Enterprise Manager Functionality (i.e., Metrics (Standard and Custom), Templates, Groups, System Groups, Alerts, Notifications, Reports and Dashboards, Service Level Monitoring) was applied to the management of E-Business Suite components.

About the Application Management Suite

The Management Suite extends Enterprise Manager Grid Control to help monitor, manage, and clone Oracle E-Business Suite instances more effectively. The pack, in conjunction with Enterprise Manager, provides a consolidated, end-to-end E-Business Suite management solution.

In particular, the Management Suite offers the following key capabilities for E-Business Suite-specific services and components:

- Automated Discovery of critical E-Business Suite services and components
- Monitoring and management of E-Business Suite components (e.g., Concurrent Managers/Programs, Workflow, Forms services, JVM, etc.)
- Ability to set Metrics on select E-Business Suite components
- Ability to generate alerts, notifications, and corrective actions
- Configuration management and reporting
- Historical reporting
- Service Level Management
- Automated Cloning
- ...and additional features

Further information on the functional capabilities of the Management Suite can be found on the Oracle Technology Network (OTN) under [Application Management Suite for Oracle E-Business Suite Data Sheet](#)

About Oracle Corporation's Global Single Instance

Oracle Corporation's GSI (Global Single Instance) refers to the single E-Business Suite instance that Oracle uses for financial transactions and reporting.

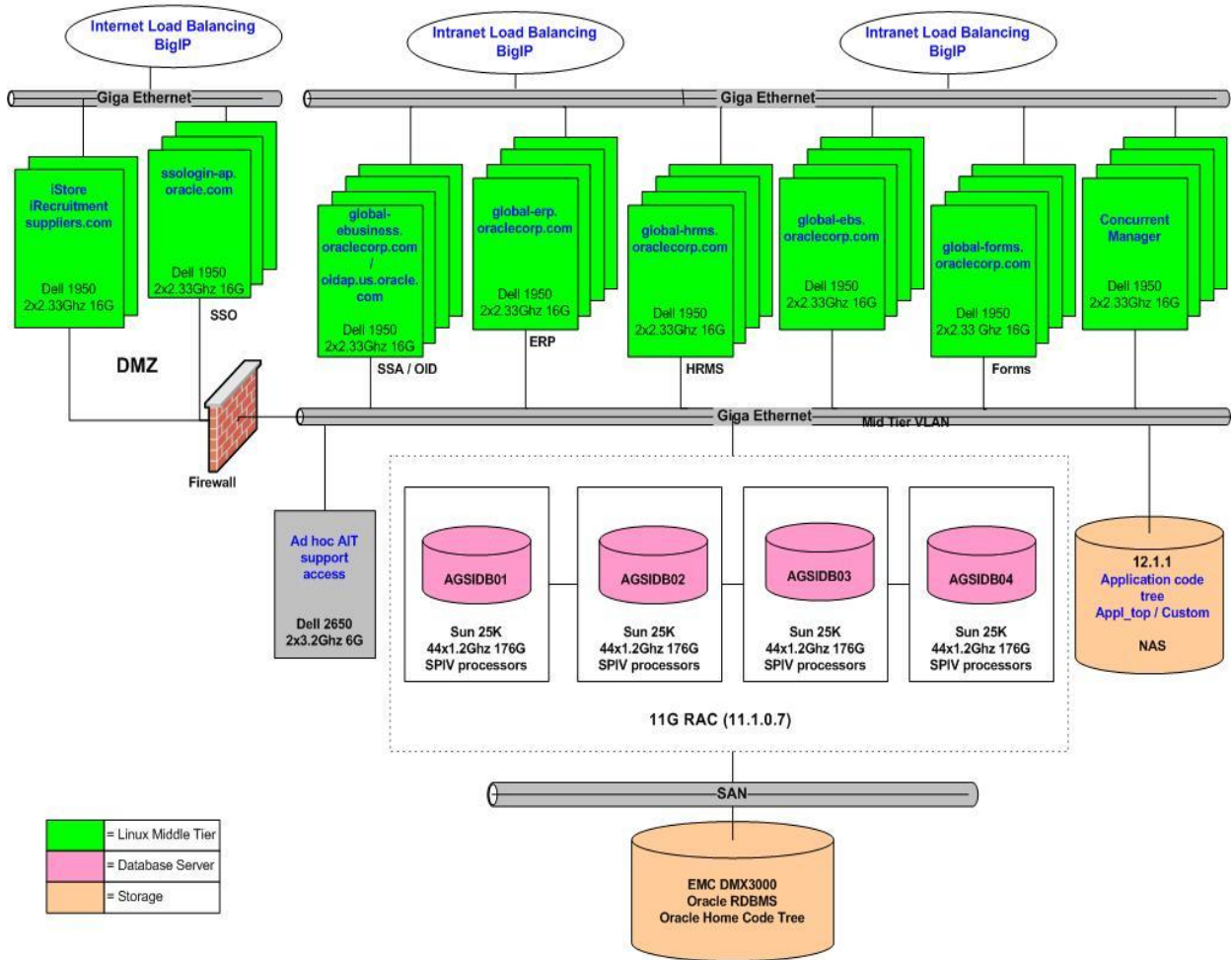
Oracle Corporation has implemented a global single instance (GSI) of E-Business Suite that includes many of the available products/modules (e.g., Financials, Distribution, Manufacturing, etc.) for all of the countries in which Oracle operates. Details on the actual implementation of Enterprise Manager in GSI are captured in the whitepaper "[Managing Many Environments as One](#)".

The key aspects of the GSI are:

- Database size: 16.1 Terabyte
- Number of end-users: 70,406
- Average number of end-users per month: 12,312
- Average number of workflow transactions per month: 433,822
- Platforms: Dell 1950 (midtier); Sun E25K; Netapp Filer; EMC DMX Tower
- Version of E-Business Suite: 12.1.1
- Version of Enterprise Manager: 10.2.0.5.3
- Version of AMP: 3.1
- Number of System Administrators and DB/Apps Administrators: 3/6
- Other Enterprise Manager Packs and plug-ins being used: Performance Pack, Configuration Mgmt , DB Change Pack, DB Masking Pack, DB Tuning Pack, Service Level Mgmt Pack, BigIP Plug-in, EMC Plug-in NetApp Plug-in

The following is the current architecture:

GSI Production Architecture - Austin Data Center



Organizational Responsibilities/Matrix

With such a massive implementation of E-Business Suite, it was imperative that a clear segregation of duties would be a key success factor. GSI was able to leverage the Role-Based Access Control (RBAC) capabilities in Enterprise Manager and the Management Suite to successfully allow the appropriate level of access between different groups.

The following different groups had different responsibilities:

Activity	Responsible Group
Disk Infrastructure/Host (DB & Middleware)	Global IT
Database/Listener/ASM/DR/Concurrent Manager	Product DEV IT Business Apps Database Services
Middleware/Context Files/BigIP	Product DEV IT Business App Services
Backups	Global IT
Patching	Product DEV IT Patching Services

Impact of the Management Suite on IT Operations and Management

The implementation and use of the Management Suite has had a huge impact on the day-to-day operations of GSI. From the Application Services group to Performance Services, the Management Suite functionality has allowed them to centralize and standardize their proactive monitoring and triage process, reducing issue resolution time by 66%.

Middleware Component Management

Prior to the implementation of the Management Suite, there were different tools and processes for monitoring different middleware components. Achieving a unified support model for these different components, such as forms servers, HTTP processes, and JVMs was a daunting task.

With the Management Suite, the GSI team was able to reduce the use of crontab entries, take advantage of automated corrective actions, and dramatically reduce the need for human intervention to correct problems.

This enabled the management team to focus on the more strategic aspects of the business, instead of being mired down in the day-to-day tactical issues.

Performance Management

Prior to the implementation of the Management Suite, the GSI team had a number of different custom tools to proactively monitor and identify issues.

With the Management Suite, the GSI team was able to centralize the triage tools, remove custom monitoring tools and with a central solution in place, reduce the resolution time on performance issues by 60%.

From an analysis perspective, moving to a centralized, integrated toolset enabled us to:

1. Collate and review data from a holistic perspective
2. Locate and highlight possible “hot spots” in the application
3. Proactively identify possible performance issues that would have had a negative impact on application availability.

Centralization and Standardization of Tools and Processes

Moving to a centralized framework allowed the GSI team to standardize our monitoring and triage process. This ensured that all team members were using the same process for all environments in the enterprise.

In turn, this also enabled the GSI team to standardize their support and response documentation. Prior to the implementation of the Management Suite, they had process documents that were written by a number of team members.

With the Management Suite, the GSI team was able to ensure that all team members adhered to a single support model, reducing errors in correction as well as ensuring continual enhancement of their knowledge base.

Reporting Efficiencies

With the Management Suite, the GSI team was able to streamline historic as well as real-time reporting on specific E-Business Suite data points.

This infrastructure enabled the GSI team to perform trend analysis on a whole new set of E-Business Suite data points, such as forms and web users, concurrent manager, workflow manager, and JVM usage – something they were never able to do prior to the Management Suite’s implementation.

The result is that Management (i.e., Operations and Executive) now has 24/7 visibility into System performance and availability. In addition, the reporting functionality assisted in hardware capacity planning for specific time periods - such as corporate quarter close.

Consumers of Management Suite Data

There are many different roles within Oracle GSI that use data generated from the Management Suite – from database administrators to the applications management team to Senior Executives.

Administrators

Prior to the deployment of the Management Suite, the GSI team struggled with providing a simple way for our application administrators to proactively review, triage and diagnose problems at the middleware level.

With the Management Suite, they were able to create “System Groups” that provide a top down view of throughput and performance for all modules implemented in the E-Business Suite. This included JVM CPU usage, Heap Usage (MB) as well as active threads. This data can be viewed real-time or historically. In addition, reports can be auto-generated via the Information Publishing module within Enterprise Manager.

Executives

Prior to the implementation of the Management Suite, it took the GSI team days to gather, parse, and collate data with wider host and database metrics, and present an integrated report to management.

Today, this can be accomplished in a matter of minutes via standard views in the Management Suite.

For example, the GSI team was able to provide clear cut justification in a matter of minutes for capacity requirements from data tracked in the Management Suite.

Considerations on the Installation and Discovery Process

Autoconfig

Autoconfig is a mandatory prerequisite for AMP, so it is necessary to run autoconfig to ensure that all setup, configuration, and context files are clean, accurate, and up-to-date.

This will ensure that when the discovery process is run, there will be no errors. In addition, it is important to ensure that after autoconfig is run during scheduled outages on the E-Business Suite, you review the status of the E-Business Suite environment in Enterprise Manager to ensure it is reflecting an accurate status.

Socket vs. Servlet Mode

Post discovery, review the Forms setup and validate the use of socket mode or servlet mode forms. Remove all targets from the E-Business Suite that are not active.

Leveraging Single Sign-On

Single Sign-On (SSO) provides a central secure tool that simplifies logon for various applications in our enterprise including the E-Business Suite. With SSO, the GSI team was able to reduce the administration overhead for end user access by 75%.

In addition, SSO streamlined the GSI user auditing process, ensuring that they maintained compliance with the Sarbanes–Oxley Act of 2002.

Finally, the GSI team was able to integrate the Enterprise Manager console itself, into the SSO infrastructure. A full review and implementation details can be found under the [Oracle Enterprise Single Sign-On Suite Plus](#) section on OTN.

Middleware Changes

When the implementation of the AMP began, there was a requirement to update a number of permissions and setup changes for the middleware as well as the JVMs supporting the E-Business Suite infrastructure.

If one has previously implemented the Enterprise Manager agent with an operating system (OS) user that is NOT the same owner as the IAS or JVM tech stack, changes to the configuration files are required to ensure a successful discovery. Appendix A lists all required permissions changes for each IAS mid-tier in an E-Business Suite infrastructure.

With the changes made on the middleware tech stacks (IAS), administrators will also need to ensure that, when autoconfig is run, the permission changes are maintained to ensure that the target status is accurate.

Java Virtual Machine

Prior to running the discovery process, changes are required for the JVMs so that the agent owner at the OS level is not the same as the tech stack owner. If the changes are not complete, the data in the E-Business Suite plug-in will be inaccurate or, in some cases, missing.

Finally, there will be metrics collection errors for the JVM targets. In Appendix B, there is a list of process and settings that need to be execute before the discovery process.

AMP Implementation Process, Tools, and Examples

This section details the process that Oracle underwent to determine configuration settings for AMP, and subsequently implement them.

Oracle's process for configuring AMP

Once the E-Business Suite instance has been discovered, it is now time to review the metrics and policies that are relevant to the various target types in each particular instance.

Since each instance is different, it is critical to set the metrics and then review the trend over a period of time to ensure that you have the proper settings. The GSI team completed this at each target level, setting the thresholds on required metrics. Once the thresholds were set, administrators then adjusted the templates for an enterprise wide change or at the specific target level, based on alerts seen.

A trend can be observed for any given metric by monitoring that specific metric over a certain time period (e.g., weekly, monthly, custom period, etc.).

To illustrate this process, the GSI team was interested in establishing metrics and thresholds for middleware "CPU Usage %". The team was able to accomplish this in the following manner:

1. Go to a middleware (IAS) target home page and scroll down to the bottom. Locate the link for "All Metrics", which displays a list of all metrics available for this target type.

General

Status: **Up** (Black Out)
 Availability (%): **100** (Last 24 Hours)
 Application URL: <http://amts516.us.oracle.com:7777>
 Version: **10.1.2.3.0**
 Installation Type: **Identity Management**
 Oracle Home: /u01/app/oracle/product/ias10g12_infra_aitat
 Host: amts516.us.oracle.com

Application URL Response (seconds)

Components

Select	Name	Type	Current Status
<input type="checkbox"/>	HTTP_Server	HTTP Server	↑
<input type="checkbox"/>	OC4J_SECURITY	OC4J	↑
<input type="checkbox"/>	OID	OID LDAP Server	↑
<input type="checkbox"/>	Single Sign-On:orasso	Single Sign-On Server	↑

Alerts

No Alerts found.

Host Alerts

Metric	Severity	Message	Alert Triggered	Last Value	Last Checked
Memory Utilization (%)	×	Memory Utilization is 95.91%	Jun 25, 2010 8:07:23 AM	96.05	Jun 25, 2010 9:07:23 AM

Related Links

- Apply Patch
- Monitoring Configuration
- Alert History
- Access
- Check Application URL
- All Metrics**
- Blackouts
- Target Properties
- Administer Metric and Policy Settings
- Reports

- The “CPU Usage (%)” metric is located under the “Resources Usage” link. Click on this and it will provide an overview of this specific metric.
- Locate the “View Data” dropdown, and change this to “31 Days”. This displays the average, maximums, and minimums for a 31 day period.

Statistics

- Last Known Value: 1.71
- Average Value: 1.76
- High Value: 2.82
- Low Value: .04
- Warming Threshold: 70
- Critical Threshold: 75
- Occurrences Before Alert: 2
- Corrective Action: None

Metric Value

View Data: Last 31 days

Alert History

Severity	Timestamp	Message	Last Comment	Details
✓	Oct 26, 2009 1:45:59 PM	CPU Utilization is 1.53%		

In this particular example, the “High Value” data point over the last 31 days hasn’t been above 3%. Therefore, an initial setting on this metric for this target of 10% (as a warning threshold) and 15% (as a critical threshold) would be probably be appropriate. Obviously, these thresholds can continue to be fine-tuned as more data is available.

Standard Metrics

“Standard” metrics refer to those pre-seeded metrics that are shipped with AMP.

When reviewing metrics, it is important to get a baseline on the targets in question. For every environment, the metrics will be different.

The key aspects from the GSI implementation are:

1. Complete a review of the metrics that are “out of the box” and then add or remove metrics based on requirements.
2. After the metrics baseline was established, set up metrics thresholds on the environment and then observe the alerts trend for 31 days. This can be done by reviewing the alerts shown on the home page for Enterprise Manager.
3. Once the initial 31 day trend results were obtained and analyzed, the GSI team adjusted the metrics on a single target – and used those settings to create the metrics template.

The screenshots below provide examples of the thresholds that were set for the GSI environment (the listing includes just middleware and E-Business Suite targets, since this document assumes setup the database, host and disk subsystem for an existing environment).





Middleware (IAS):

Metric and Policy Settings

Cancel OK

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Component Memory Usage (%)	>	80	90	None	Every 5 Minutes	
CPU Usage (%)	>	70	75	None	Every 5 Minutes	
Memory Usage (%)	>	80	90	None	Every 5 Minutes	
Up/Down Status			Down	None	Every 5 Minutes	

TID: Fmmtu Thresholds will display alerts for that metric

Middleware (HTTP):

Metric and Policy Settings Cancel OK

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Active HTTP Connections	>	135	140	None	Every 5 Minutes	
Active HTTP Requests	>	135	140	None	Every 5 Minutes	
Active Requests for a Virtual Host	>	135	140	None	Every 5 Minutes	
CPU Usage (%)	>	90	95	None	Every 5 Minutes	
Error Rate (%)	>	1	1.5	None	Every 5 Minutes	
HTTP 400s percentage	>	5	15	None	Every 5 Minutes	
HTTP 500s percentage	>	5	15	None	Every 5 Minutes	
Memory Usage (%)	>	90	95	None	Every 5 Minutes	
Percentage of Busy Processes	>	85	90	None	Every 5 Minutes	
Percentage of Requests Resulted in Internal Errors	>	1	1.5	None	Every 5 Minutes	
Percentage of Requests that Were Failures	>	1	1.5	None	Every 30 Minutes	
Percentage of Requests that Were Failures	>	1	1.5	None	Every 5 Minutes	
Percentage of Requests that Were Failures	>	1	1.5	None	Every 30 Minutes	
Up/Down Status			Down	None	Every 1 Minute	

☞ TIP Empty Thresholds will disable alerts for that metric.

Middleware (OACORE):

Metric and Policy Settings Cancel OK

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Memory Usage (%)	>	80	90	None	Every 5 Minutes	
Up/Down Status			Down	None	Every 1 Minute	

☞ TIP Empty Thresholds will disable alerts for that metric.

E-Business Suite (Home):

Metric and Policy Settings Cancel OK

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Concurrent Requests Error Rate (%)	>	5	10	None	Every 15 Minutes	
Concurrent Requests Pending (Standby)	>		2000	None	Every 15 Minutes	
Concurrent Requests Running	>		450	None	Every 15 Minutes	
Concurrent Requests Scheduled	>		5000	None	Every 15 Minutes	
Context Files Edited	>	0		None	Every 1 Hour	
Errored Business Event System Messages	>	5000	10000	None	Every 15 Minutes	
Errored Workflow Notifications	>	5000	10000	None	Every 60 Minutes	
Expired Business Event System Messages	>	1000	5000	None	Every 15 Minutes	
Forms Sessions	>	3900	4000	None	Every 15 Minutes	
Number of Forms Database Sessions per Application	>	1000	1100	None	Every 15 Minutes	
Number of Web Users (Hourly)	>	4800	4900	None	Every 60 Minutes	
Patches Applied	>	5	10	None	Every 1 Hour	
Ready Business Event System Messages	>	5000	10000	None	Every 15 Minutes	
Service Status	=		DOWN	None	Every 15 Minutes	
Status			Down	None		
Undeliverable Business Event System Messages	>	5000	10000	None	Every 15 Minutes	
Unsent Workflow Notifications	>	10000	50000	None	Every 60 Minutes	
Waiting Business Event System Messages	>	10000	50000	None	Every 15 Minutes	

☞ TIP Empty Thresholds will disable alerts for that metric.

Workflow Notification (Listener):

Metric and Policy Settings

Cancel OK

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Errored Java Events	>=	0		None	Every 15 Minutes	
Errored PLSQL Events	>=	0		None	Every 15 Minutes	
Pending Java Events	>=	0		None	Every 15 Minutes	
Pending PLSQL Events	>=	0		None	Every 15 Minutes	
Status			Down	None	Every 15 Minutes	

TIP Empty Thresholds will disable alerts for that metric.

Workflow Notification (Engine):

Cancel OK

Metric and Policy Settings

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Deferred Items	>=	0		None	Every 15 Minutes	
Status			Down	None	Every 15 Minutes	

TIP Empty Thresholds will disable alerts for that metric.

Metric Thresholds Links

[Metric Snapshots](#)

Metric Thresholds Policies

Concurrent Manager:

Cancel OK

Metric and Policy Settings

Metric Thresholds Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Status			Down	None	Every 5 Minutes	

TIP Empty Thresholds will disable alerts for that metric.

Metric Thresholds Links

[Metric Snapshots](#)

Metric Thresholds Policies





Java Virtual Machine (JVM):


Metric and Policy Settings

Cancel OK

Metric Thresholds
Policies

View Metrics with thresholds ▾

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
Deadlocked Thread Count	>=	<input type="text" value=""/>	<input type="text" value="1"/>	None	Every 5 Minutes	
OC4J JVM - CPU Usage (%)	>	<input type="text" value="90"/>	<input type="text" value="95"/>	None	Every 5 Minutes	
OC4J JVM Instance - Heap Usage (MB)	>	<input type="text" value="1900"/>	<input type="text" value="1960"/>	None	Every 5 Minutes	
Status			Down	None	Every 1 Minute	

 TIP Empty Thresholds will disable alerts for that metric.

[Metric Thresholds Links](#)

User Defined Metrics

“User Defined Metrics (UDMs)” refer to those metrics that customers can create to address their own, unique requirements. Where possible, GSI made every attempt to use standard, out of the box metrics when monitoring our targets. However, there are certain cases where a “custom” solution is required.

The User Defined Metric enables the administrator to create scripts that can be scheduled at the target level with thresholds that will notify when a specific issue is seen. This can be at the host level, the database level or the application server level.

The key aspects and capabilities from the GSI implementation are:

1. With AMP, the GSI team was able to migrate from custom UDMs to standard metrics around status of the workflow and concurrent manager status.
2. UDMs can only be created at the host, database and middleware level. On these targets, the GSI team was able to shore up any special requirements that standard metrics wouldn't satisfy.
3. It is important to assign logical, intuitive names to the UDMs for quick administration and understanding.
4. A UDM created on the master target will also be included in the template. Therefore, all UDMs that are part of the baseline should be created on the first target. Once completed, create the template and then apply it to all remaining targets of that type.

Additional information on how to configure and when to use can be found in the [Oracle® Enterprise Manager Advanced Configuration 10g Release 5 \(10.2.0.5\)](#) under section 14, User-Defined Metrics.

Automated Corrective Actions

“Automated Corrective Actions” refer to the ability to automate the restart or recovery of a certain service that is down in Enterprise Manager, such as Workflow or Concurrent Managers.

Once the standard and user defined metrics were established, the GSI team created a corrective action for a specific metric - so when the alert is fired, a script can be run to correct the problem and therefore, minimize the manual intervention.

A full list of corrective action created can be found in the Corrective Action Library, a sample of which is in the below screenshot:

The screenshot displays the Oracle Enterprise Manager 10g interface for the Corrective Action Library. The left-hand navigation pane includes various configuration options, with 'Corrective Action Library' highlighted by a red circle. The main content area shows a table of corrective actions. The table has columns for 'Name', 'Corrective Action Type', and 'Owner'. The actions listed include:

Select	Name	Corrective Action Type	Owner
<input checked="" type="radio"/>	AITAPRCAMTS523	Multi-Task	
<input type="radio"/>	AITAU RESOURCE CALENDAR	Multi-Task	
<input type="radio"/>	ALLOWED FAILED LOGIN ATTEMPTS (CLUSTER DATABASE)	SQL Script	
<input type="radio"/>	ALLOWED FAILED LOGIN ATTEMPTS (DATABASE INSTANCE)	SQL Script	
<input type="radio"/>	BACKUP NQUERY LOG	OS Command	
<input type="radio"/>	CORRECTIVEACTIONFOR RS	Multi-Task	
<input type="radio"/>	EM_JANITOR_SID	OS Command	
<input type="radio"/>	RESOURCECALENDAR	OS Command	
<input type="radio"/>	SEGMENTS APPROACHING MAX EXTENTS CA	OS Command	
<input type="radio"/>	SEGMENTS APPROACHING MAXIMUM EXTENTS COUNT - FIX	OS Command	
<input type="radio"/>	TEST_PSP	OS Command	
<input type="radio"/>	TESTPSP	OS Command	

A blue box with the text "Intentionally Blocked Out" is overlaid on the right side of the table. The interface also includes navigation tabs at the top (Home, Targets, Deployments, Alerts, Compliance, Jobs, Reports) and a footer with copyright information.

One example from the Oracle GSI implementation is automating the restart of agents.

For example, when the GSI team receives an alert for agent down, we set the number of occurrences to 3. This means that the alerts won't fire until the threshold status is broken 3 consecutive times. Once the alert fires 3 consecutive times, the support group will receive an alert. This is effective as sometimes there is network “noise” and using a corrective action, the support group will only receive alerts for actual issues.

Another example is using corrective actions for log file clean up for the database and the middleware. When GSI Support receives an alert that a log file system is filling up, a shell script that cleans up the log areas is automatically executed. The benefit is a more timely response to the issue, as well as no manual intervention.

From an Oracle Applications E-Business Suite perspective, the GSI team had setup corrective actions to restart processes when their status goes down. If the restart isn't successful, a support ticket is sent to the appropriate team.

Policies

Policies represent the “best practices” for IT management, as defined by Oracle.

System configurations will change over time, due to normal administrative actions, such as patch application, adding files and directories, and changing of ports. Policies enable administrators to know when changes have happened, and then permit or deny those changes to ensure compliance with corporate directives.

Finally, policies ensure that any new environments introduced to the environment comply with accepted standards.

The key aspects of the Oracle GSI implementation are:

1. When reviewing the various targets, it is a good idea to review the “out of the box” policies when provisioning targets. Under the “Compliance” tab, there is a list of policies under the “Library” link.
2. The GSI team focused on the security policies, although there are also policies for “Configuration” and “Storage”, to name a few. The process to deploy the required security policies is very simple - we distributed the list of security policies to the Security teams, requesting review and input as to the policies that they would like to deploy.
3. Once the feedback was received, the GSI team created a “Security Policy Monitoring Template” and applied the policies to the designated targets.
4. Then, a notification rule was created to address the policy violations. Alerts are then routed to the Security team for review. After the Security team completed a review of the alerts and ensured that action was required, they would then forward the alert to the proper group for action/correction.
5. Once the issue was corrected on the target with the violation, the alert would clear in Enterprise Manager and the issue would auto close. Therefore, when the policy was reviewed in the future, no new alert would be fired.
6. In addition, once all security policies are applied and violations are addressed, administrators can review the status around security for any target type via the link on the target home page under the security section. Click on the “Security at a Glance” and it will summarize violations and overall percentage of compliance.

The following screenshots highlight the security policies implemented for the following target types:

- HTTP Server

- Web Cache
- OC4J

HTTP Server:

Policy	Severity	Category	Type	Description	Owner	Used in Monitoring Templates	Used by Targets
HTTP Server Access Logging	Critical	Security	Oracle HTTP Server	Verifies whether Access Logging is enabled	<SYSTEM>	1	113
HTTP Server Directory Indexing	Critical	Security	Oracle HTTP Server	Verifies that Directory Indexing is disabled	<SYSTEM>	1	113
HTTP Server Dummy Wallet	Critical	Security	Oracle HTTP Server	Checks whether a Dummy Wallet is being used on HTTP Server	<SYSTEM>	1	113
HTTP Server Owner And Setuid Bit	Critical	Security	Oracle HTTP Server	Verifies that the HTTPd binary is not owned by a super user	<SYSTEM>	1	113
HTTP Server SSL	Critical	Security	Oracle HTTP Server	Checks whether Secure Socket Layer (SSL) is enabled for Single Sign-On (SSO) on HTTP Server	<SYSTEM>	1	113
HTTP Server Writable Files	Warning	Security	Oracle HTTP Server	Checks whether users other than the owner have write permission in the Document Root folder	<SYSTEM>	1	113

TIP Policies provided by Oracle are owned by <SYSTEM>.

Web Cache:

The following table lists all the policies and where they are currently in-use.

Page Refreshed J

Advanced Search

Category: Policy:
 Severity: Owner:
 Target Type:
 [Simple Search](#)

Policy	Severity	Category	Type	Description	Owner	Used in
Web Cache Access Logging	Critical	Security	Web Cache	Checks whether access logging is enabled on Web Cache	<SYSTEM>	
Web Cache Dummy Wallet	Critical	Security	Web Cache	Checks whether a Dummy Wallet is being used on Web Cache	<SYSTEM>	
Web Cache Owner And Setuid Bit	Critical	Security	Web Cache	Verifies that the webcached binary is not owned by a super user	<SYSTEM>	
Web Cache Writable Files	Warning	Security	Web Cache	Checks whether users other than the owner have write permission in the Document Root folder	<SYSTEM>	

TIP Policies provided by Oracle are owned by <SYSTEM>.

OC4J:

The following table lists all the policies and where they are currently in-use.

Page Refreshed Jun 18, 2010 7:14:09 AM PDT

Advanced Search

Category: Policy:
 Severity: Owner:
 Target Type:
 [Simple Search](#)

Policy	Severity	Category	Type	Description	Owner	Used in Monitoring Templates	Used by Targets
OC4J Password Indirection	Critical	Security	OC4J	Verifies that password indirection is used in OC4J XML configuration and deployment files	<SYSTEM>	1	32

TIP Policies provided by Oracle are owned by <SYSTEM>.

Additional information on Policies can be found in the [Oracle® Enterprise Manager Policy Reference Manual 10g Release 5 \(10.2.0.5\)](#)

Monitoring Templates

When deploying any target type, it is important that the metrics on like target types have a basic standard setup. The GSI team used templates to ensure that the same Standard (i.e., out-of-the-box) and User Defined Metrics (UDM) (i.e., custom metrics) are applied across all like targets.

The key aspects of the GSI implementation are:

1. Prior to discovering the middleware targets, review and set all Standard metrics
2. Investigate and set any requirements for UDMs. Before adding these to the template, simply discover the first middleware target, add the UDMs and then create the standard template. Once this is complete, administrators will have all standard metrics as well as UDMs in the same “baseline” template.
3. This process should be used for any target type to ensure a standard baseline is created. Templates can be created by any user so it is also important to designate the single user that will administer baseline templates. This also ensures that templates aren’t changed outside of the standard process.
4. It is also important to establish and maintain logical/intuitive naming conventions for the templates. In GSI’s case, user administrators were established for the database, mid-tier and applications templates. Therefore, when working with the application templates, the applications template/notification rule owner is used to administer.

The naming convention we used for templates was as follow:

- Admin User: APPS_CR_TS_NOTIFY
(APPS_<Critical>_<Test/Stage>_NOTIFY)
 - Template Name: APPS_EBIZ_GSI (APPS_<Type>_<Environment>)
 - Target Type: Oracle Applications
5. Once the template is created, it can be applied to multiple targets.

In addition, templates can be used against to compare metrics between different targets. This assists in configuration management, ensuring that like targets have the same baseline standard and User Defined Metrics.

Leveraging Group Functionality

The ability to “group” many targets into a single unit facilitates notifications as well as the management of individual targets. With Groups and System Groups, administrators can update settings and compare the standard templates created to the targets in a given group to ensure that standards are applied.

In addition, creating System Groups is critical to the setup of the Application Service Level Management (ASLM) module. System groups are associated with web transactions that proactively monitor and reflect infrastructure outages for a given application transaction.

Group Administration

After all required targets were discovered, the next step was to create groups to facilitate ease of administration of multiple, related targets. It was critical that the grouping of targets is completed in a very organized fashion.

In the GSI implementation, a number of best practices were followed:

1. Separate the groups by midtier hosts, database hosts and application targets.
2. For the application groups, the naming convention includes the application supported with the suffix “_apps” (e.g. gsiap_apps). This group includes all Oracle Applications E-Business Suite target types for a given environment.
3. For the mid-tier groups, use the same naming convention specific to the environment with the suffix “_mts”. This group includes the host, agent, Application Service Level Management (ASLM) transactions, and the IAS targets.

This configuration enabled the following capabilities:

1. The use of Group Level Dashboards (located on the right side of the group home page).
2. The ability to compare targets in the group against user defined templates. Under the group administration tab, one can search the configuration for the targets in that group.
3. The ability to obtain a deployment summary around hardware, OS levels and Oracle Homes.

Additional information can be found in the [Oracle® Enterprise Manager Grid Control Quick Start Guide 10g Release 2 \(10.2\)](#) under section 4, Managing Groups.

System Group

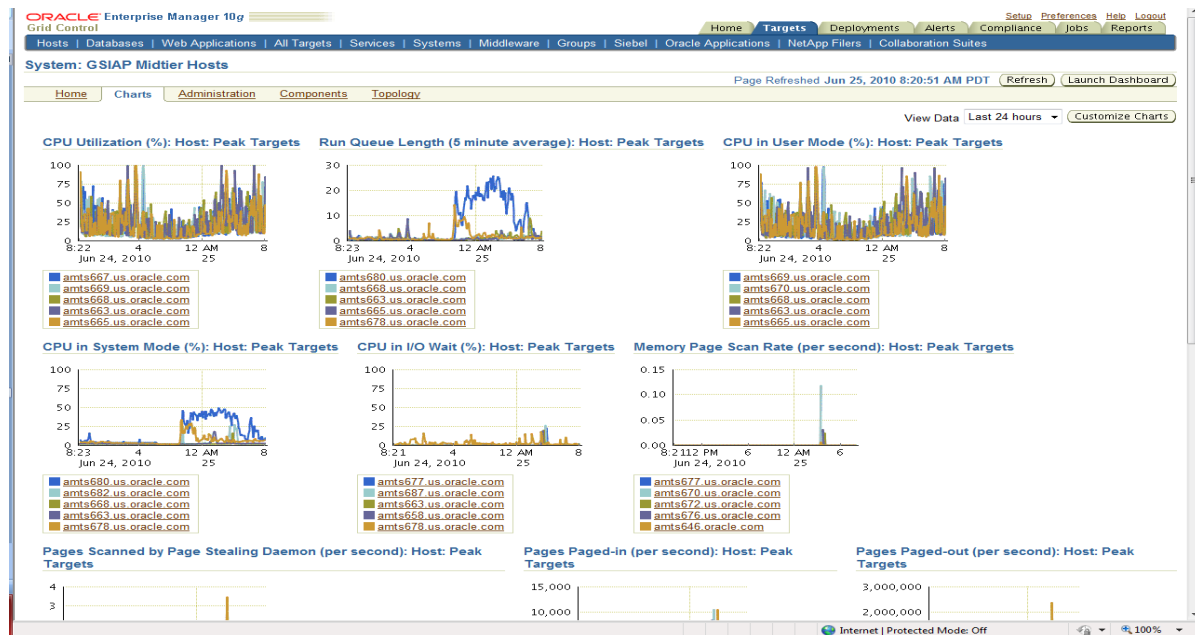
Another type of group is the “System Group”, which is a group with all of the targets that make up the infrastructure supporting a given application.

This type of group allowed GSI to:

- Create a “chart” view of specific metrics across the targets added to the System Group.
- Enable the Application Service Level Management (ASLM) Web Transaction, thereby expanding the use of root cause analysis for a given application downtime.

The GSI team created a System Group of middleware hosts and middleware applications. Once created, the chart tab was configured to display midtier hosts CPU & Memory on the middleware hosts, middleware OC4J statistics.

This provided an overview of the environment’s infrastructure that allowed our administrators to quickly and easily identify problem areas, such as performance issues or general application instability. The screenshot below highlights this capability.



Notification Rules

Notification rules are the drivers for all alerts received when a metric threshold is breached. It is critical that the rules are properly configured and implemented, otherwise, in the event there are issues with rules, notifications aren’t sent and proactive information to parties concerned is lost.

Notification rules are based on target type, metric and level of notification (i.e., P1 or P2). Under this configuration, one can assign a group with multiple target types and specify the target type that you want to notify against.

In the GSI implementation, a number of best practices were followed:

1. Since notification rules are created and administered at the Enterprise Manager User level, the GSI team created a single Enterprise Manager user that is used to administer all notification rules. This user had super administrator privileges and is only accessed by the Enterprise Manager administrative team.
2. Logical and intuitive naming conventions and notification definitions are critical. As the implementation progresses, it becomes apparent that multiple notification rules are required to satisfy different requirements from database, midtier and application owners. In addition, the use of multiple notification methods is available in this setup.
3. The naming convention the GSI team used consists of the notification level rule number for that section. That is, the GSI team configured different rules for database, midtier and applications environments. For example, the naming convention for an application rule that notifies as a P1 would be:
 - Name: P1rule1_APP
 - Owner: Rule_Admin
 - Description: Stage and Critical E-Business Suite Application: p1's for alert, p2 for warning and error
4. As additional rules are created, the GSI team would increment the rule number (i.e., P1rule2, P1rule3...). For the applications rules, the GSI team used the same naming convention for the rule name with the suffix "_APP" and provided the proper description to ensure clarity.
5. When creating the rule, administrators can also specify the target type, metrics, and the notification method desired. In most cases, one would use the e-mail notification method. In addition, administrators can also create custom notification methods in the Enterprise Manager repository and interface with external notification systems. Enterprise Manager also provides interfaces to other standard call tracking systems such as Remedy.
6. Once the rules are created, administrators can then associate a group that was previously created with the rule. This simplifies the administration of notification rules. When groups are created with various targets, the group can be associated with a notification rule and as notification rules are driven by target type, only the target types that are addressed in the rule will be notified against. This facilitates the addition and removal of targets.

7. When a new target is discovered, simply add the new target to the required group and after the metrics template is applied, the rule will then notify on the required metrics. In addition, when it is required to stop metrics or remove a target, administrators can simply remove the target in question from the group and the notifications will stop.

Finally, additional information around notifications can be found in the [Oracle® Enterprise Manager Advanced Configuration 10g Release 5 \(10.2.0.5\)](#) under section 14, Configuring Notifications.

Performance Monitoring

Performance monitoring of an E-Business Suite instance can be a large and complex task, with many moving parts. This section will cover some common areas to review using AMP, and how it can assist in triaging various performance issues.

The key aspects of the GSI implementation are:

1. From the instance homepage in AMP, administrators can immediately see session activity. Since the GSI team was familiar with the trends in their environment, they could quickly see if the user counts on that environment are “out of bounds”.

For example, if there were an influx in users, administrators might want to take note to further review JVM status as well as host level statistics to see if the end user is experiencing any application issues. Conversely, if there is a sharp reduction in user counts, this can also indicate that there are infrastructure problems as users are not able to access the application.

2. Also on the home page, administrators can get a quick overview on component health for that E-Business Suite instance. The status of all components is listed on the left side of the home page. Finally, scrolling down the page, administrators can see the health of each middleware environment and a list of any outstanding alerts for that environment, based on metrics thresholds set.
3. Clicking on the “Performance” link provides further get details on the Concurrent Manager, User Sessions, and workflow throughput.
4. AMP provides trend analysis at the application level as well as the infrastructure level. This functionality helps to reduce the resolution time for any issues seen, based on data in the user interface, as well as the setting of proper metrics thresholds.
5. Finally, out of the box, there is an Infrastructure Dashboard Link in the top right hand side of the Performance page for any E-Business Suite. This provides an overview of the health of the Concurrent Manager, Self Service Applications and Workflow process. The following is an example.

Services Dashboard									
Page Refreshed On Jun 25, 2010 9:06:35 AM PDT Refresh									
Service	Status	Performance	Usage and Business Indicators	Components	Service Level				
					Last 24 Hours	Last 7 Days	Last 31 Days		
gsiap-Concurrent Processing Service		 0.48 Concurrent Requests ... 91.45 Concurrent Requests ...	 632.00 OC4J Requests per Se... 303.00 Running Requests per....	 3 Up	100.00%	100.00%	99.75%		
gsiap-Self Service Applications Service		 3.27 OC4J Requests per Se....	 1.36 HTTP Server CPU Usag... 5.62 OC4J CPU Usage (%)	 2 Up	100.00%	99.89%	99.96%		
gsiap-Workflow Service		 0.00 Errored Java Events 0.00 Pending Java Events	 31414.00 Background Engine De....	 5 Up	100.00%	99.69%	98.66%		

Java Virtual Machine Administration and Monitoring

When reviewing performance and status of an E-Business Suite instance, it is critical to ensure that the JVMs that support those applications are healthy. AMP allows administrators to proactively monitor, and gather real-time data for, each JVM.

Prior to implementing the Management Suite, this was a difficult process and was accomplished primarily with custom tools that were authored by different groups and monitored individually. With the implementation of the Management Suite, GSI was able to standardize and centralize this effort, and improve our ability to detect possible issues with the application before it affects our end users.

Details on the JVMs are found in the “Performance” tab for each E-Business Suite. Within this view, administrators can see all JVMs supporting that given E-Business Suite instance and get a “bird’s eye” view of the activity in that instance.

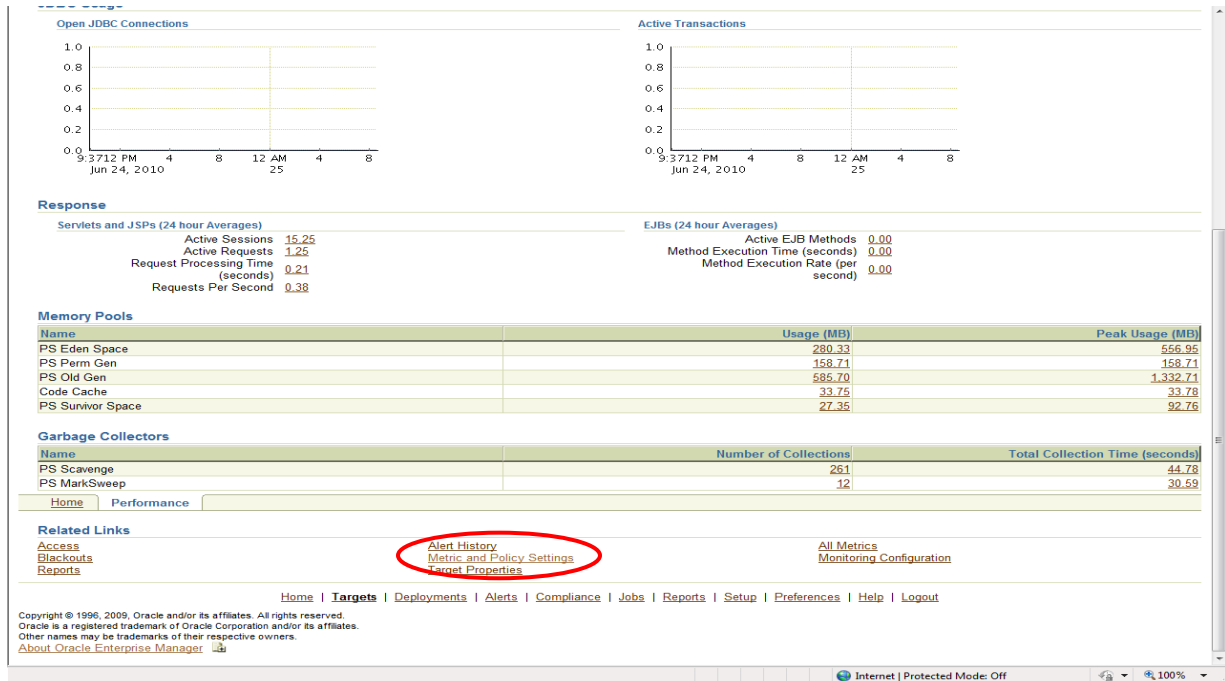
Drilling down into a specific JVM, one can get version info as well as a list of outstanding alerts

The screenshot displays the Oracle Enterprise Manager 10g Performance page for a specific JVM. The page is titled "OC4J JVM: amts671_hrms.amts671.us.oracle.com_oacore_JVM_1". The "General" section shows the JVM is "Up" (Black Out) since "Jun 23, 2010 11:37:14 AM" with 100% availability. The "Response and Load" section contains a line graph showing "Request Processing Time (seconds)" and "Requests Per Second" over a 24-hour period. The "Alerts" section shows "No Alerts found". The "Related Links" section includes "Monitoring Configuration", "Alert History", "Access", "All Metrics", "Blackouts", "Target Properties", and "Metric and Policy Settings Reports".

From the screenshot above, it is very easy to determine JVM activity, as well as quickly ascertain if there are any outstanding issues around CPU, Memory and Active Threads.

Finally, scrolling down the page, administrators can see statistics for the Memory Pools and Garbage Collection. From our experience, it is critical that the Garbage Collection process isn’t running too often for a JVM. Frequent execution of the Garbage Collection process can shed light on a potential problem.

Lastly, it is possible to establish metrics for JVMs - by clicking on the “Metrics and Policy Settings” link at the bottom of the page.



Concurrent Manager Administration

With the discovery of the E-Business Suite environment in Enterprise Manager, the proactive monitoring of the Concurrent Manager becomes much simpler. Out-of-the-box, the GSI team was able to streamline the monitoring, alerting and reporting on various aspects of the concurrent managers, ensuring maximum availability.

The GSI team was able to create dashboards and reporting tools that assisted the administrator in ensuring that the processes are healthy. The following is an example of the dashboard.



The above screenshot provides a quick overview on the health of a certain concurrent process. All of the data points in this dashboard can be setup with metrics and generate alerts/notifications.

In this particular example, there are 651 active processes. Clicking on this number shows the average, max and current status for the last 24 hrs.

The GSI implementation used this data to establish trends and then set metrics to generate notifications when thresholds were breached. A high number indicates that there may be a problem with the overall process and the execution of requests. Within this same view, administrators can review Current Activity and Usage data by concurrent manager process.

In addition, at the bottom of the UI, there is a link that takes you to a view of active concurrent requests by application as well as status on those requests. The following is an example of this view.

Oracle E-Business Suite: ospiap-Oracle E-Business Suite > All Metrics >

Active Concurrent Requests by Application

Page Refreshed Jun 22, 2010 12:36:37 PM PDT

Previous Show All 30 Next

Application Short Name	Application Name	Non-Repeating Pending requests (Normal and Standby)	Repeating Pending requests (Normal and Standby)	Non-Repeating Running requests	Repeating Running requests
FND	Application Object Library	2	2	5	2
PASA	PA Analyzer	1	0	2	0
MIS_AR	Oracle Receivables Custom	0	27	3	0
XLA	Subledger Accounting	0	0	1	0
MISASO	Custom ASO	10	0	0	0
PO	Purchasing	4	0	1	0
MISONT	Custom Order Management	15	0	0	0
WSH	Shipping Execution	0	0	1	0
MISFII	Custom Oracle Financials Intelligence	0	0	1	1
OKS	Service Contracts	26	0	1	1
AR	Receivables	15	0	22	0
MIS_CN	Oracle Custom Sales Compensation	0	0	1	0
CSI	Install Base	0	0	6	0
IEX	Collections	0	0	0	1
MISIPM	Custom Imaging Process Management	0	0	0	1
MISPER	MIS Personnel	14	7	4	3
MISAP	MIS Payables	0	0	1	0
MISBEN	Custom Oracle Advanced Benefits	0	0	10	0
OFS	Custom Order Fulfillment System	12	0	0	0
PA	Projects	0	0	4	1
MISOKC	MIS Oracle Contracts Extensions	0	0	5	1
SQLAP	Payables	0	0	3	0
ALR	Alert	0	0	1	2
MISJTF	Custom CRM Foundation	0	0	1	2

Another view that is very helpful is the Hourly Completed Requests review. This link is also at the bottom of the main page and can assist in troubleshooting the concurrent manager. The following is an example of that view.

Hourly Completed Requests

Page Refreshed Jun 22, 2010 12:40:33 PM PDT

Name	Value
Concurrent Requests Completed Successfully	2703
Concurrent Requests Completed With Warning	243
Concurrent Requests Completed With Error	3
Concurrent Requests Successful Requests Rate (%)	91.658189
Concurrent Requests Warning Rate (%)	8.240081
Concurrent Requests Error Rate (%)	0.101729

Home | **Targets** | Deployments | Alerts | Compliance | Jobs | Reports | Setup | Preferences | Help | Logout

Copyright © 1996, 2009, Oracle and/or its affiliates. All rights reserved.
 Oracle is a registered trademark of Oracle Corporation and/or its affiliates.
 Other names may be trademarks of their respective owners.
[About Oracle Enterprise Manager](#)

Workflow Manager Administration

AMP also includes functionality to manage and monitor Workflow Manager.

Within the administration tab under the specific E-Business Suite environment, administrators can review the workflow configuration and archive a specific day's configuration – either for later review, or to compare it to another previously saved configuration - in order to highlight changes over a period of time.

Oracle Enterprise Manager 10g
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Oracle E-Business Suite Workflow_esiap-Workflow Infrastructure >

Generic Service Components Custom Workflows

View Configuration: Oracle E-Business Suite Workflow

Collected From Target Jun 24, 2010 3:07:27 PM
Description Latest Configuration

Workflow Version 2.6

Generic Service Components

Related Details

Select	Component Id	Component Name	Component Type	Component Type Display Name	Concurrent Queue Name	Concurrent Queue Display Name	Container Type	Container Type Display Name	Inbound Agent Name	Inbound Agent Display Name	Outbound Agent Name	Outbound Agent Display Name	Max Idle Time	Startup Mode	Startup Mode Display Name
<input checked="" type="radio"/>	28.023	wf_deferred_14_temp_wf	WF_AGENT_LISTENER	Workflow Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_DEFERRED	WF_DEFERRED				AUTOMATIC	Automatic
<input type="radio"/>	24.025	wf_java_deferred_c4_f	WF_JAVA_AGENT_LISTENER	Workflow Java Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_JAVA_DEFERRED	Workflow Java Deferred In Queue				AUTOMATIC	Automatic
<input type="radio"/>	24.024	wf_java_deferred_c3	WF_JAVA_AGENT_LISTENER	Workflow Java Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_JAVA_DEFERRED	Workflow Java Deferred In Queue				AUTOMATIC	Automatic
<input type="radio"/>	24.023	wf_java_deferred_c2	WF_JAVA_AGENT_LISTENER	Workflow Java Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_JAVA_DEFERRED	Workflow Java Deferred In Queue				AUTOMATIC	Automatic
<input type="radio"/>	24.022	wf_java_deferred_c1	WF_JAVA_AGENT_LISTENER	Workflow Java Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_JAVA_DEFERRED	Workflow Java Deferred In Queue				AUTOMATIC	Automatic
<input type="radio"/>	26.022	wf_deferred_13_temp_i	WF_AGENT_LISTENER	Workflow Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_DEFERRED	WF_DEFERRED				AUTOMATIC	Automatic
<input type="radio"/>	22.022	wf_deferred_12_temp_xmlpos	WF_AGENT_LISTENER	Workflow Agent Listener	WFALSNRSVC	Workflow Agent Listener Service	GSM	Oracle Applications GSM	WF_DEFERRED	WF_DEFERRED				AUTOMATIC	Automatic

The ability to archive point-in-time configurations, for either reference or comparison reporting purposes, also exists for:

- System Overview for E-Business Suite
- E-Business Suite Patching information (custom and standard) as well as an overall
- Concurrent Manager
- Workflow

All of these options can be found in the Administration Tab for each instance.

ORACLE Enterprise Manager 10g
Grid Control

Home Targets Deployments Alerts Compliance Jobs Reports

Hosts Databases Web Applications All Targets Services Systems Middleware Groups Siebel Oracle Applications NetApp Filers Collaboration Suites

















Oracle Applications: gsiap-Oracle E-Business Suite

Service Level Reports Infrastructure Services Go

Home Performance Administration Maintenance Diagnostics User Monitoring Topology

Page Refreshed Jun 25, 2010 7:57:24 AM

Expand All | Collapse All

Focus Name	Report Administer	Description
▼ All Tasks		
▼ System		
System Overview		Last collected applications system overview configuration
Administration		Administration Dashboard
Patch Information		Last collected patch information configuration
Custom Objects		Last collected custom objects configuration
▶ Application Nodes		View, compare, search, and edit context variables for all nodes
▶ Hosts		View status, edit configuration setting for all hosts
▶ Database Instances		Database Instances
JVM Usage		Monitor Application Modules and Connection Pool for JVMs
Site Level Profiles		Search site level profiles
Database init.ora Parameters		Database Init.ora setting and the recommendation for oracle applications
Patches Applied		Search Patches Applied
Patchset Info		Search Patchset Info
▼ Services		
▶ Concurrent Processing		Last collected concurrent processing configuration
▶ Workflow		Last collected workflow configuration.
▼ Applications Usage		
License Manager		License Manager provides a set of reports that allows you to determine the products, country-specific functionalities and languages that are registered on your Oracle Applications system
Applications Usage Reports		Application Usage Reports such as products installed, application users per module, suppliers and other reports.
▼ Others		
Critical Activity		Schedule, monitor and setup critical activities such as purge transaction data.
Knowledge Base		Setup Knowledge Base, refresh knowledge base catalog contents
SQL Extension		SQL Extension allows administrators to run seeded and custom SQL scripts

Internet | Protected Mode: Off

Information Publishing (Reporting) & Dashboards

One of the core aspects of Enterprise Manager and the Management Suite is its reporting capabilities.

There are a number of “standard” reports in Enterprise Manager. These can be used as is, or can be customized to suit a customer’s unique needs.

Standard “canned” reports can be found specific to Deployment and Configuration, Enterprise Manager Setup, Monitoring, Security, Storage, Patch Set and Software Summary.

The GSI implementation created various custom reports to provide additional insight into status, capacity and configuration. Draft reports are created by the individual users and then migrated to the “production support” user for the reporting module. The “AITSYS_REPORT” user is used to administer and configure the production reports. As well, various reports we run are set to “public access”. This enables administrators to provide report access to management groups without having to log into the Enterprise Manager console.

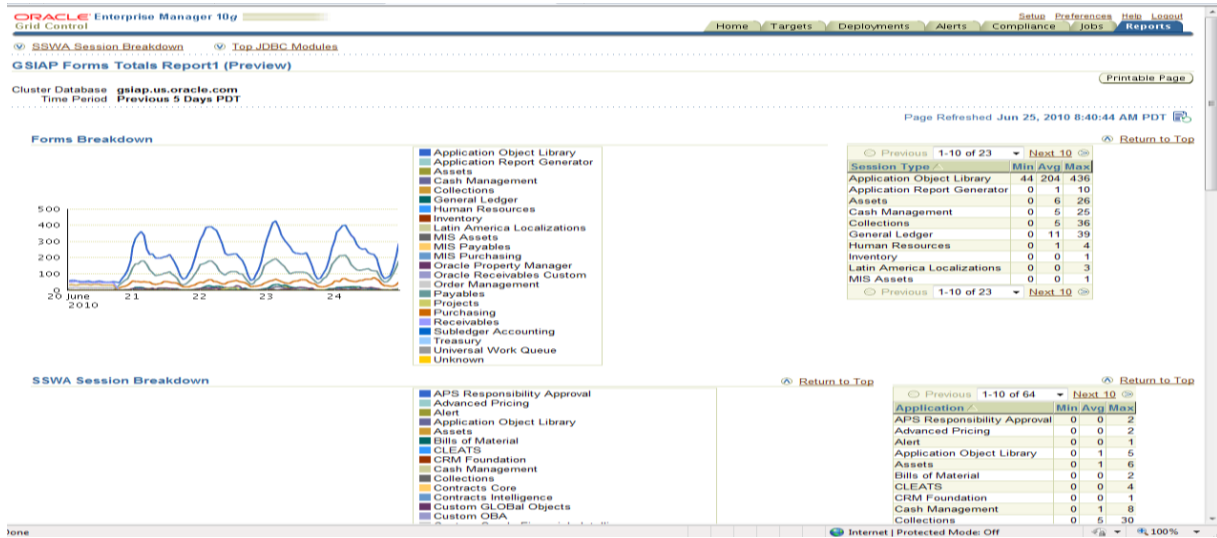
The publishing of a public report can be configured by simply setting the proper privileges for the report to run and then setting the report public under the “Access” section for any report created.

Once this is completed, it is possible to link the report in other web pages for centralized access.

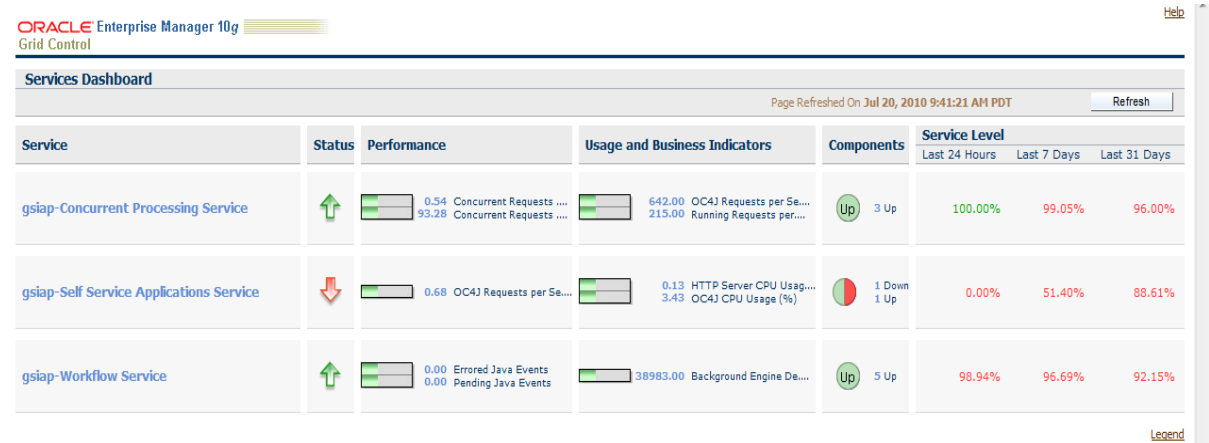
The following are some of the custom reports that GSI has created:

- Database Capacity Trend Analysis
- Application Availability Dashboards
- Systems Dashboards
- Monitoring Template Usage Overview
- Notification Rule Target Breakdown
- Database Target User Defined Metric (UDM) Listing Report

From an E-Business Suite perspective, the GSI team created custom reports such as the following E-Business Suite Session Breakdown Dashboard.



E-Business Suite Services Dashboard



GSIAP E-Business Suite Applications Dashboard



E-Business Suite Systems Dashboard

ORACLE Enterprise Manager 10g Grid Control

System: **gsiap.oracle.com** Page Refreshed Jul 20, 2010 9:47:37 AM PDT Refresh

Previous 1-10 of 20 Next 10

Target Type	Status	Alerts
Automatic Storage Management	↑	8 4
Network Appliance Filer	↑	6 6
Agent	↑	4 1
Host	↑	4 0
Cluster Database	↑	1 6
Oracle Workflow Agent Listener	↑	0 4
Cluster	↑	0 2
Database Instance	↑	0 1
Oracle Workflow Background Engine	↑	0 1
Listener	↑	0 0

Alerts 2 22 25 Previous 1-10 of 51 Next 10

Severity	Target	Date	Message	Acknowledged By	Current Value	Latest Comment
●	gsiap.us.oracle.com	Jul 20, 2010 9:39:52 AM	Tablespace UNDO_004 is 98 percent full			Autoticketing : No SR generated because of exclusion list: rule_name=pInfile3, rule_owner=DBA_PROD_NOTIFY, target_name=gsi%, metric_name=%1%esp%, metric_column=%Used%
●	agsis002.us.oracle.com:1832	Jul 20, 2010 9:32:33 AM	Agent Virtual Memory Growth is 1922.69%		1922.69	
●	erpntap71	Jul 19, 2010 7:05:17 PM	Alert for u01_app_system_prod_2 for 90.5 is cleared		90.5	
●	agsis002.us.oracle.com:1832	Jul 19, 2010 2:40:04 PM	Agent resident memory utilization in KB is 631048		28189840	
●	erpntap71	Jul 19, 2010 11:50:17 AM	Alert for amts555_home for 89 is cleared		87.37	
●	erpntap71	Jul 19, 2010 3:20:17 AM	Alert for amts202_u01_app_oracle for 80.03 is cleared		80.57	
●	agsis004.us.oracle.com	Jul 19, 2010 1:27:00 AM	Process 706 matched by the program name '% and owner 'oracle' is utilizing 26836.09 (MB) of resident memory. It has crossed warning () or critical (26812) threshold.		26911.98	
●	erpntap71	Jul 18, 2010 2:05:17 PM	Alert for amts696_u01_app_oracle for 90.03 is cleared		91.23	
●	agsis001.us.oracle.com:1832	Jul 18, 2010 1:35:45 AM	Agent resident memory utilization in KB is 604344		1281216	
●	amts558_ssa.amts558.us.oracle.com_oacore	Jul 17, 2010 12:29:40 AM	The OC4J instance is down		1	Autoticketing : Created.SR.17878979

Previous 1-10 of 51 Next 10 Legend

GSIAP Database Capacity Summary

ORACLE Enterprise Manager 10g Grid Control

Database Capacity Summary (GSIAP)

Cluster Database **gsiap.us.oracle.com**
Time Period **This Year PDT**

Report Generated Jul 20, 2010 9:49:18 AM PDT

This report displays the monthly cumulative allocated space usage for all tablespaces in the database. In addition, the detailed monthly allocated space usage of each tablespace is displayed for the selected time frame. Historic trend is based on available data for selected time frame. Space usage data is only available for databases managed by agent of version 10.2 and above.

Earliest Collection Time **Jan 1, 2010 12:00:00 AM**
Latest Collection Time **Jul 19, 2010 12:00:00 AM**

Monthly Cumulative Tablespace Allocated Space Usage

Calendar Month	Average Allocated				Maximum Allocated				Minimum Allocated			
	Size (GB)	Used (GB)	Free (GB)	Used (%)	Size (GB)	Used (GB)	Free (GB)	Used (%)	Size (GB)	Used (GB)	Free (GB)	Used (%)
Jul 1, 2010 12:00:00 AM	16,226.78	10,902.52	5,324.25	67.21	16,795.85	10,990.55	5,935.33	68.09	16,081.47	10,777.6	5,132.34	64.66
Jun 1, 2010 12:00:00 AM	16,742.77	10,550.97	6,191.8	63.02	16,778.91	10,879.14	6,442.94	64.85	16,721.95	10,287.01	5,892.06	61.49
May 1, 2010 12:00:00 AM	16,540.84	9,900.14	6,640.7	59.85	16,675.12	10,040.85	6,752.28	60.21	16,458.61	9,736.65	6,554.66	59.07
Apr 1, 2010 12:00:00 AM	16,403.51	10,161.61	6,241.89	61.95	16,445.66	10,506.34	6,772.85	64.1	16,361.88	9,655.87	5,885.43	58.77
Mar 1, 2010 12:00:00 AM	16,125.52	10,295.88	5,829.65	63.85	16,361.88	10,405.29	6,062.79	64.92	15,999.23	10,132.52	5,621.94	62.92
Feb 1, 2010 12:00:00 AM	15,931.36	9,887.11	6,044.25	62.06	15,986.28	10,168.15	6,174.92	63.61	15,918.51	9,743.58	5,818.13	61.21
Jan 1, 2010 12:00:00 AM	15,886	9,819.78	6,066.22	61.81	15,918.51	9,976.58	6,401.29	62.79	15,850.73	9,449.44	5,912.04	59.62

GSIAP Applications Services Dashboard

ORACLE Enterprise Manager 10g Grid Control Help

PDIT Business Application Services Dashboard Page Refreshed On Jul 20, 2010 9:50:04 AM PDT

Service	Status	Performance	Usage and Business Indicators	Components	Service Level		
					Last 24 Hours	Last 7 Days	Last 31 Days
GSI - iProcurement		 6.33 CPU Utilization (%) 0.04 Swap Utilization (%) 1075.00 Connect Time (ms)	 3944.00 iProcurement Users	 1 Up	100.00%	99.69%	99.93%
GSI - Emp Self Srv		 126.00 Connect Time (ms) 4.70 CPU Utilization (%) 0.00 Swap Utilization (%)	 17719.00 Emp Self Srv Users	 1 Up	100.00%	99.78%	99.95%
GSI - Mgr Self Serv		 59.00 Connect Time (ms) 3.57 CPU Utilization (%) 0.00 Swap Utilization (%)	 3315.00 Mgmt Self Srv Users	 1 Up	100.00%	99.91%	99.98%
GSI - Expenses		 116.00 Connect Time (ms) 5.84 CPU Utilization (%) 0.02 Swap Utilization (%)	 8458.00 Expense Apps Users 5653.00 Expenses Submitted	 1 Up	100.00%	99.85%	99.96%
GSI - Notifications		 110.00 Connect Time (ms) 14.70 CPU Utilization (%) 0.01 Swap Utilization (%)	 0.63 Concurrent Requests 30.00 Concurrent Requests 215.00 Concurrent Requests	 1 Up	100.00%	100.00%	100.00%
GSI - iRecruitment		 118.00 Connect Time (ms) 14.82 CPU Utilization (%) 0.00 Swap Utilization (%)	 2880.00 iRecruitment Users	 1 Up	100.00%	100.00%	99.91%

Additional information can be found in the [Oracle® Enterprise Manager Grid Control Quick Start Guide 10g Release 2 \(10.2\)](#) under section 9, Information Publisher.

Application Service Level Management

The Application Service Level Management (ASLM) module enables administrators to proactively monitor the application from the end user perspective. Utilizing the beacon functionality, administrators can simulate the end user experience from a given global location.

The GSI environment has beacons located in India, United Kingdom, Singapore, Texas and Colorado. This gives a good overview of performance for our general employee population.

The transactions that were recorded were simple login/logout transactions that ensure that (simulated) users can access the application via the standard URL. As a best practice, administrators review the “success strings” for each step in the transaction.

Success strings are critical as this will ensure that the transaction is working properly. If the success strings are not properly configured, the transaction will assume that any return of data from the step in the transaction is valid - in some cases, this could give you a false positive.

From a naming convention perspective, as always, thought should be put in to the way things are named. We used the following format:

- <Application>-Application Login-<Sub Application>

The sub application would be the specific application for a given environment (i.e., some applications have separate sections need to be accessed in order to ensure a successful login.

Additional information around Services and ASLM can be found in the [Oracle® Enterprise Manager Grid Control Installation Guide 10g Release 5 \(10.2.0.5.0\)](#) under section 7, Configuring Services.

Further Information

Readers are also encouraged to search Oracle Technology Network (OTN) for the following keywords:

- Application Management Pack for Oracle E-Business Suite
- Application Management Suite for Oracle E-Business Suite
- AMP

Conclusion

When implementing Enterprise Manager, it is critical to plan ahead and understand what is required in the initial deployment. It is also important to plan for expansion and setup the environment so that major changes to your enterprise don't require major changes to the configuration of Enterprise Manager. As well, major changes wouldn't be required when adding targets.

From an application perspective, it is also important to create a test environment so that validation of patches and the roll out of new features can be executed before moving to production. As more and more targets are monitored, it is important to enforce standards via monitoring templates.

Finally, with the proper planning and implementation, Enterprise Manager will enable the administrator to manage the E-Business Suite via the standard Enterprise Manager console. As well, as you expand the enterprise you manage, Enterprise Manager will enable you to roll in new targets as well as new target types while maintaining standards, providing proactive reporting, notifications and management for your critical applications.

Appendix A – Permissions Changes for iAS Tech Stack

```
chmod 750
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/config/ias.properties
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/config
chmod 750
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/opmn/conf/opmn.xml
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/opmn/conf
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/opmn
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/Apache/Apache/conf/ht
tpd.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/j2ee/oacore/config/serv
er.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<HOST_NAME>_cm/ora/10.1.3/j2ee/forms/config/serve
r.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/oc4j-connectors.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/jms.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/j2ee-logging.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/system-application.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/jazn.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/system-jazn-data.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/mapViewerConfig.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
config/oc4j.properties
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacor
e/config/oc4j-connectors.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacor
e/config/jms.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacor
```

```
e/config/j2ee-logging.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacore/config/system-application.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacore/config/jazn.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacore/config/system-jazn-data.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacore/config/ohwconfig.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oacore/config/oc4j.properties
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/jazn.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/j2ee-logging.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/system-application.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/oc4j-connectors.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/system-jazn-data.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/jms.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/forms/config/oc4j.properties
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/config/j2ee_instance_jazn.properties
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/config/jazn.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/config/jazn-data.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/config/iasschema.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Apache/conf/mod_oc4j.conf
chmod 640
```

```

/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/ssl.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/mod_osso.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/oracle_apache.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/security.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/custom.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/ssl_terminator.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/trusted.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/apps.conf
chmod 640 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee/oacore/config/data-
sources.xml
chmod 640 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee/forms/config/data-
sources.xml
chmod 750 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee/oafm
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee/oafm/config
chmod 640 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.3/j2ee/oafm/config/data-
sources.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/Apache/Ap
ache/conf/apps.conf
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
application-deployments/mapviewer/orion-application.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
application-deployments/mapviewer/web/orion-web.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
application-deployments/ascontrol/orion-application.xml
chmod 640
/u01/app/ebiz/<ENV_NAME>/inst/apps/<ENV_NAME>_<HOST_NAME>/ora/10.1.3/j2ee/oafm/
application-deployments/ascontrol/ascontrol/orion-web.xml

```

Files for workflow engine:

```

chmod 750 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/oracore

```

```
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/oracore/zoneinfo  
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/oracore/mesg  
chmod 750 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/sqlplus  
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/sqlplus/mesg  
chmod 640 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/sqlplus/mesg/*  
chmod 750 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/nls  
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/nls/data  
/u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/nls/data/9idata  
chmod 750 /u01/app/ebiz/<ENV_NAME>/apps/tech_st/10.1.2/nls/data/9idata/*
```

Appendix B – JVM Access Setup

OC4J_JVM Errors:

Target `srvas_amts634.amts634.us.oracle.com_oacore_JVM_1`

Type OC4J JVM

Metric Compilation Time

Collection Timestamp Nov 13, 2008 10:47:17 PM

Error Type Collection Failure

Message Error communicating with server.

Note 757927.1: The agent cannot contact the oc4jvms targets in order to collect the metrics as monitoring credentials are not known.

Edit `$IAS_HOME/opmn/conf/opmn.xml` and add `-Dcom.sun.management.jmxremote` for the start-parameters of the OC4J instance associated with the OC4JJVM target.

Snippet example:

```
<ias-component id="default_group">
<process-type id="home" module-id="OC4J" status="enabled">
<module-data>
<category id="start-parameters">
<data id="java-options" value="-server
-Dcom.sun.management.jmxremote
-Djava.security.policy=$ORACLE_HOME/j2ee/home/config/java2.policy
-Djava.awt.headless=true -Dhttp.webdir.enable=false -XX:MaxPermSize=128M
-Xms512M -Xmx1024M -XX:AppendRatio=3"/>
</category>
```

Bounce opmn with `opmnctl stopall / opmnctl startall`.

Set the `authPasswd` property for the OC4J target associated to the monitored OC4JJVM target via the OMS console UI:

Targets -> iAS instance -> OC4J instance -> Monitoring Configuration

Edit the two properties:

Username for Basic authorization (typically `oc4jadmin`)

Password for Basic authorization (typically `oc4jadmin's password`).



Case Study
August 2010
Author: Patrick Combs
Contributing Author: Kenneth Baxter
Implementation Team: Patrick Combs,
Walter Kerszulis, Richard Brinegar, Lynn
Hay, Kiran Mangu

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

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