Oracle® Enterprise Manager

Cloud Control Getting Started with Oracle Fusion Middleware Management

12*c* Release 2 (12.1.0.2)

E24215-03

September 2012

Oracle Enterprise Manager Cloud Control Getting Started with Oracle Fusion Middleware Management 12*c* Release 2 (12.1.0.2)

E24215-03

Contributor: Venkatesh Audinarayana, Neelima Bawa, Leo Cloutier, Paul Coghlan, Pradeep Gopal, Jacqueline Gosselin, Nicole Haba, Dan Hynes, Maheshwari Hatte, Glen Hawkins, Arivalagan Kaliyaperumal, Shiraz Kanga, James Kao, Dennis Lee, Pushpa Raghavachar, Rishi Saraswat, Karthik Somasundaram

Contents

4 Testing Application Load and Performance

5 Monitoring Business Applications

Part II Monitoring Oracle Exalogic Elastic Cloud

6 Monitoring Oracle Exalogic Elastic Cloud

Part III Monitoring WebLogic Domain

7 Monitoring WebLogic Domains

Part IV Managing Oracle SOA

8 Overview of Oracle SOA Management

9 Discovering and Monitoring Oracle BPEL Process Manager

10 Discovering and Monitoring Oracle Service Bus

11 Discovering and Monitoring the SOA Suite

Part VI Using JVM Diagnostics

13 Introduction to JVM Diagnostics

14 Using JVM Diagnostics

15 Troubleshooting JVM Diagnostics

Part VII Managing Oracle Coherence

16 Getting Started with Management Pack for Oracle Coherence

17 Monitoring a Coherence Cluster

Part VIII Using Identity Management

18 Getting Started with Identity Management

19 Prerequisites for Discovering Identity Management Targets

20 Discovering and Configuring Identity Management Targets

Part IX Using Application Dependency and Performance

21 Introduction to Application Dependency and Performance

22 Exploring Application Dependency and Performance

23 Exporting Data

Preface

Enterprise Manager 12*c* provides a rich and powerful compliance management framework that automatically tracks and reports conformance of managed targets to industry, Oracle, or internal standards. Enterprise Manager 12*c* ships with compliance standards for Oracle hardware and software including Database, Exadata Database Machine, Fusion Middle Ware, VM Manager and more. These compliance standards validate conformance to Oracle configuration recommendations, best practices, and security recommendations.

Audience

This document is intended for database administrators.

This document provides you with an understanding of the provided Oracle Database related compliance standards and how to go about using them. Although the Oracle compliance standards can be customized to match a user's specific requirements, the scope of this document is to explain how to use the compliance standards as provided.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Access to Oracle Support

Oracle customers have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

For more information, see the following document in the Oracle Enterprise Manager Release 12*c* documentation set:

- *Oracle Enterprise Manager Lifecycle Management Guide*

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Part I

Managing Oracle Fusion Middleware

The chapters in this part describe how you can discover and monitor Oracle Fusion Middleware targets, including Oracle WebLogic Server and deployed Java EE applications.

The chapters are:

1

Introduction to Middleware Management

This chapter provides an introduction to how you can use Oracle Enterprise Manager Cloud Control to monitor and manage middleware software, including Oracle Fusion Middleware and Oracle WebLogic Server.

> **Note:** The features documented in this manual pertain to Enterprise Manager for Oracle Fusion Middleware Plug-in version 12.1.0.3.

This chapter covers the following:

- Middleware Management with Enterprise Manager Cloud Control
- Fusion Middleware Control Versus Cloud Control

1.1 Middleware Management with Enterprise Manager Cloud Control

Middleware is the software that enables your enterprise applications to run. Managing the underlying middleware technology can be difficult, and IT organizations often have to rely on a variety of specialized tools. This can lead to inefficiency and may introduce complexities and risks.

Enterprise Manager Cloud Control is the definitive tool for middleware management and allows you to manage both Oracle applications and custom Java EE applications that run on a combination of Oracle Fusion Middleware as well as non-Oracle middleware software.

Oracle Enterprise Manager Cloud Control is a Web browser-based, graphical user interface that you can use to monitor multiple Oracle Fusion Middleware Farms and Oracle WebLogic Domains. In fact, Cloud Control provides deep management solutions for Oracle technologies including Oracle packaged applications, Oracle Database and Oracle VM.

Enterprise Manager Cloud Control supports the discovery, monitoring and central management of the entire family of Oracle Fusion Middleware components, including:

- Oracle WebLogic Server farms, domains, clusters and single server instances
- Clustered and standalone Java EE applications
- Web tier components, including Oracle HTTP Server and Oracle Web Cache
- Service-Oriented Architecture (SOA) components
- Oracle Identity Management
- Metadata Services repositories

- Oracle WebCenter
- Oracle Portal
- Oracle Business Intelligence Discoverer
- Oracle Forms Services
- Oracle Reports
- Directory Server Enterprise Edition
- Oracle Coherence
- Oracle Exalogic Elastic Cloud
- Oracle Application Server
- Java EE

Cloud Control also offers extensive support for non-Oracle technologies through more than two dozen heterogeneous management plug-ins and connectors including Microsoft MOM, IBM WebSphere Application Server, JBoss Application Server, EMC storage, F5 BIG IP, Check Point Firewall, and BMC Remedy.

A key benefit of Enterprise Manager Cloud Control is that unlike other Fusion Middleware management utilities - such as Fusion Middleware Control and the WebLogic Server Administration Console - you can monitor and manage multiple middleware targets, such as all of your WebLogic Server domains, from a single console.

You can also view real time as well as historic performance metrics collected from middleware targets. This enables you to monitor the availability and performance of Oracle Fusion Middleware software both in real time and from a historical perspective for trend analysis and diagnosing availability and performance problems.

Enterprise Manager Cloud Control also enables you to manage the infrastructure upon which the middle tier depends. You can manage underlying operating systems and hosts on which the middleware software is installed. You can also monitor the databases used by deployed applications, enabling you to diagnose application performance problems and identify the true root cause of the problem and the tier (middleware, database) on which it occurs.

The built-in topology viewer allows you to visualize and monitor your entire Oracle Fusion Middleware environment in a graphical display. Topologies can be viewed for a single SOA composite, an Oracle WebLogic Domain, or across multiple Oracle WebLogic Domains.

Management of Service-Oriented Architecture (SOA) components such as BPEL processes and infrastructure components such as Oracle Service Bus, is also supported. The infrastructure provides monitoring, fault management, configuration management, deployment and dependency views of wiring between components.

1.2 Fusion Middleware Control Versus Cloud Control

This section compares the Oracle Fusion Middleware management capabilities of Oracle Enterprise Manager Fusion Middleware Control (Fusion Middleware Control) and Oracle Enterprise Manager Cloud Control.

1.2.1 Managing Fusion Middleware with Fusion Middleware Control

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for the farm, cluster, domain, servers, components, and applications. The Fusion Middleware Control home pages make it easy to locate the most important monitoring data and the most commonly used administrative functions all from your Web browser.

Fusion Middleware Control is a part of the Oracle Fusion Middleware installation. With Fusion Middleware Control, you can:

- Manage a single Oracle Fusion Middleware Farm and a single WebLogic Domain.
- Monitor the availability and performance of Fusion Middleware software in real time mode.
- Perform routine administration tasks such as deploying applications, configuring parameters etc.

For more details, see the *Oracle Fusion Middleware 11g Administrator's Guide*.

1.2.2 Key Oracle Fusion Middleware Management Features

Cloud Control provides full historical monitoring across the middleware tier, from WebLogic Server instance and the Java virtual machine (JVM) it runs within to the Oracle Fusion Middleware components running on the application server. It also provides full configuration and lifecycle management of middleware components, while the product's extensive performance monitoring and diagnostics capabilities enable troubleshooting issues anywhere within the middleware tier.

With Oracle Enterprise Manager Cloud Control, you can:

- Centrally manage multiple Oracle Fusion Middleware Farms and WebLogic Domains.
- Manage third party products such as IBM WebSphere Application Server, JBoss Application Server, Apache Tomcat and the Microsoft .NET Framework.
- Manage non-middleware software such as underlying operating systems and hardware on which the middleware software is installed. This allows administrators to correlate middleware performance with its underlying host performance.
- Manage database software and diagnose application performance problems and identify the true root cause of the problem and the tier (middleware, database) on which it occurs.
- Monitor the availability and performance of Oracle Fusion Middleware software in real time and from a historical perspective for trend analysis.
- Diagnose availability and performance problems.
- Monitor and trace important end-user requests from the client to the service endpoint across all the servers and applications associated with each transaction.
- Use Application Dependency and Performance (ADP) to analyze Java EE and SOA applications.
- Monitor Java applications and diagnose performance problems in production using JVM Diagnostics.
- Define Service Level Objectives (SLOs) in terms of out-of-box system-level metrics as well as end user experience metrics to accurately monitor and report on Service Level Agreement (SLA) compliance.

- Perform several critical tasks like:
  - Setting thresholds on performance metrics. When these thresholds are violated, e-mail and page notifications are sent.
  - Tracking configuration changes and comparing configurations between example test environment and production environment.

2 Discovering Middleware Targets

In order to manage and monitor Oracle Fusion Middleware components such as WebLogic Server instances and clusters, as well as the Java EE applications that depend on them, Enterprise Manager Cloud Control must first "discover" the Fusion Middleware Domain containing these components.

Once discovered, the domain and the components within it can be promoted to "managed target" status. In this process, Management Agents are assigned to each target, enabling Enterprise Manager Cloud Control to collect the data needed to monitor the target.

> **Note:** The Oracle Fusion Middleware versions for which discovery is supported in Oracle Enterprise Manager Cloud Control release 12.1.0.2 is available from the certification matrix located on My Oracle Support (`https://support.oracle.com`).

This chapter contains the following sections:

- Enabling Automatic Discovery of Fusion Middleware Targets
- Discovering Targets Manually
- Discovering New or Modified Domain Members

2.1 Enabling Automatic Discovery of Fusion Middleware Targets

Cloud Control provides the ability to automatically search for potential Oracle Fusion Middleware targets on host machines that are already being managed by Cloud Control. You can configure automatic discovery to run on a regular schedule, such as every 2 days. Discovery is run every 24 hours by default.

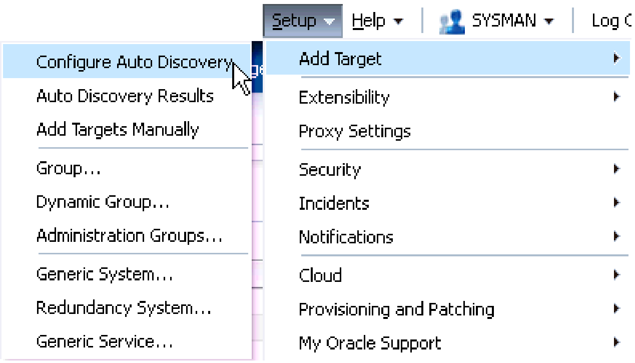
Once automatic discovery has been configured, you can check the Auto Discovery Results page to see what new Oracle Fusion Middleware targets have been discovered. You can then promote targets to managed target status by assigning a Management Agent to monitor and manage the target. To make things a bit easier, the Management Agent should already be pushed on to the target host. This enables you to configure auto-discovery on that host.

The following describes the process for configuring automatic discovery of Oracle Fusion Middleware targets only. However, Cloud Control actually enables you to configure discovery of a variety of Oracle target types.

Note: The automatic discovery feature is not supported for Oracle WebLogic Server version 8.x.

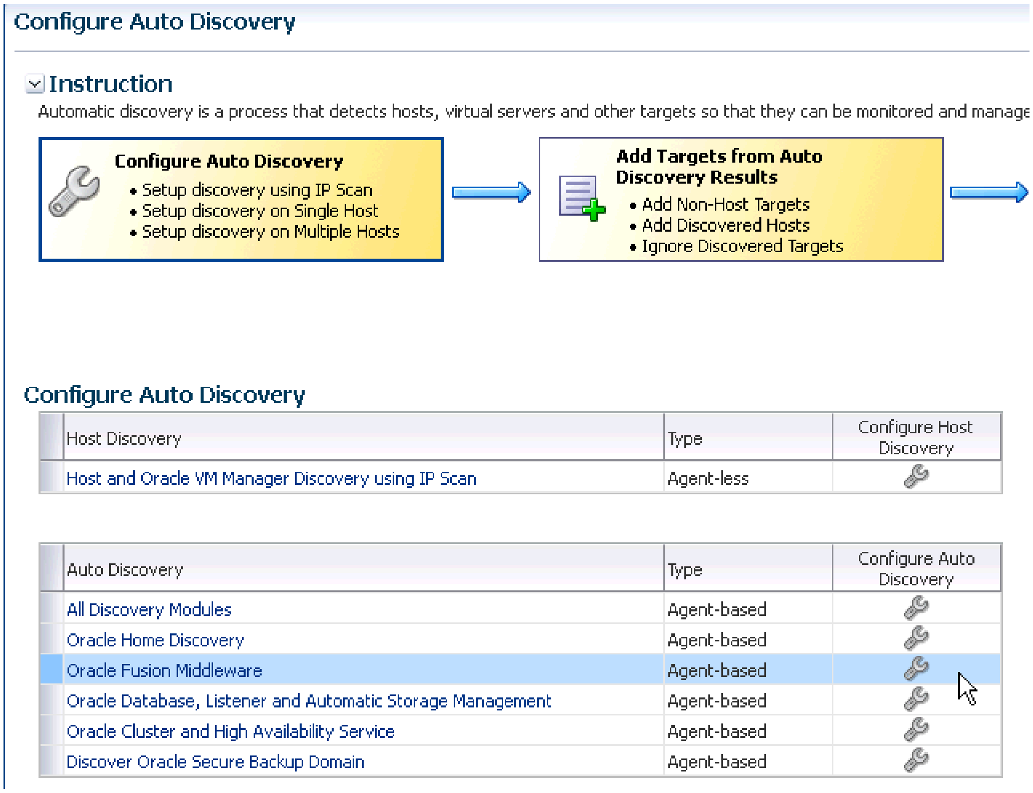
1. From the **Setup** menu, select **Add Target**, then select **Configure Auto Discovery**.

Figure 2–1 Configure Auto Discovery Option



2. On the Configure Auto Discovery page, select the Oracle Fusion Middleware link in the table to configure auto discovery for Oracle Fusion Middleware or click the icon in the **Configure Host Discovery** column to configure that Oracle Fusion Middleware row.

Figure 2–2 Configure Auto Discovery Page



Configure Auto Discovery

Instruction

Automatic discovery is a process that detects hosts, virtual servers and other targets so that they can be monitored and manage

Configure Auto Discovery
- Setup discovery using IP Scan
- Setup discovery on Single Host
- Setup discovery on Multiple Hosts

Add Targets from Auto Discovery Results
- Add Non-Host Targets
- Add Discovered Hosts
- Ignore Discovered Targets

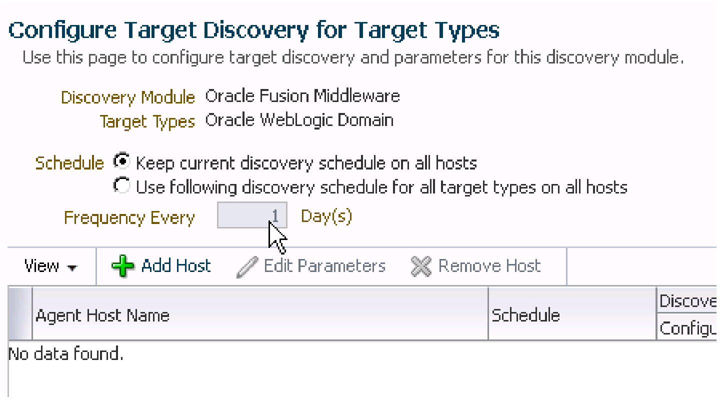
Configure Auto Discovery

Host Discovery	Type	Configure Host Discovery
Host and Oracle VM Manager Discovery using IP Scan	Agent-less	

Auto Discovery	Type	Configure Auto Discovery
All Discovery Modules	Agent-based	
Oracle Home Discovery	Agent-based	
Oracle Fusion Middleware	Agent-based	
Oracle Database, Listener and Automatic Storage Management	Agent-based	
Oracle Cluster and High Availability Service	Agent-based	
Discover Oracle Secure Backup Domain	Agent-based	

3. Set the schedule at which the discovery job will be run, in days. This schedule will be applied to all selected hosts. By default the job will run every 24 hours.

Figure 2–3 Schedule for Configuring Target Discovery



Configure Target Discovery for Target Types

Use this page to configure target discovery and parameters for this discovery module.

Discovery Module Oracle Fusion Middleware

Target Types Oracle WebLogic Domain

Schedule ● Keep current discovery schedule on all hosts

○ Use following discovery schedule for all target types on all hosts

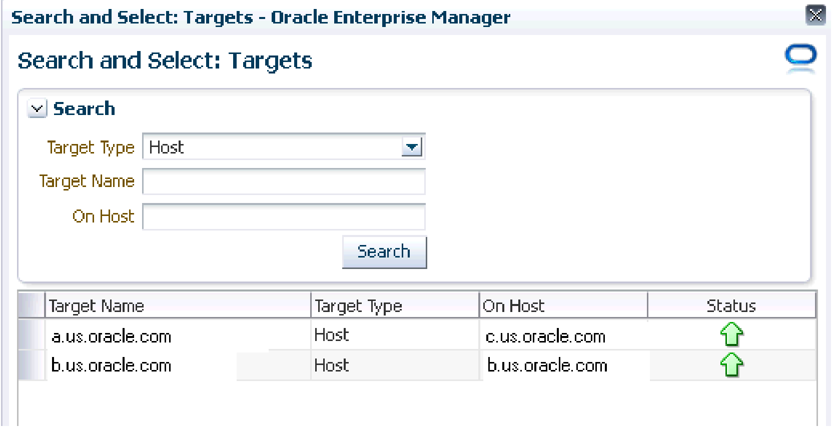
Frequency Every 1 Day(s)

Agent Host Name	Schedule	Discove Configu

No data found.

4. Click **Add Host**. Select the host machines you want to include in the discovery.

Figure 2–4 Host Machines Available for Discovery



Search and Select: Targets - Oracle Enterprise Manager

Search and Select: Targets

Search

Target Type Host

Target Name

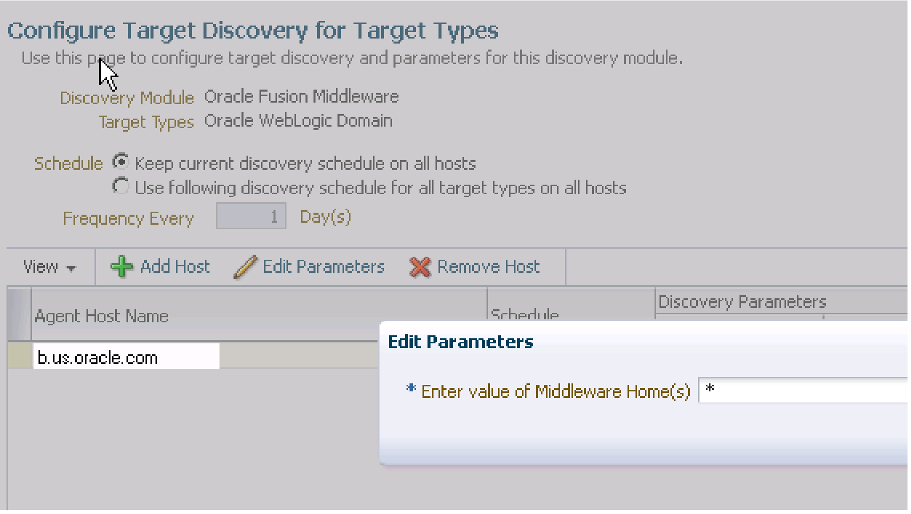
On Host

Target Name	Target Type	On Host	Status
a.us.oracle.com	Host	c.us.oracle.com	⇧
b.us.oracle.com	Host	b.us.oracle.com	⇧

5. Select a host in the table, and then click **Edit Parameters** to specify the Middleware Homes to search for targets. The Middleware Home is the top-level directory for all Oracle Fusion Middleware products, created when Oracle WebLogic Server is installed.

   Enter * to search all Middleware Homes, or specify the path to one or more Middleware Homes on the host, each separated by a comma.

Figure 2–5   Edit Parameters



Configure Target Discovery for Target Types

Use this page to configure target discovery and parameters for this discovery module.

Discovery Module Oracle Fusion Middleware

Target Types Oracle WebLogic Domain

Schedule ● Keep current discovery schedule on all hosts
○ Use following discovery schedule for all target types on all hosts

Frequency Every 1 Day(s)

b.us.oracle.com

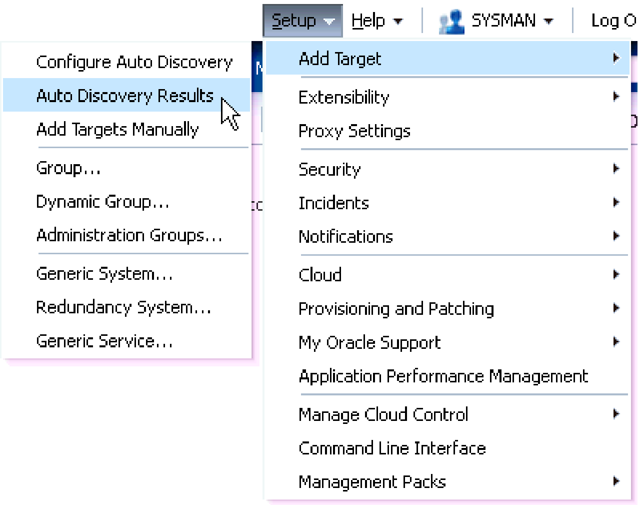
Edit Parameters

* Enter value of Middleware Home(s) *

6. Click the **OK** button located at the right of the screen. At this point, automatic discovery has been enabled, and the discovery job will run at the scheduled frequency.

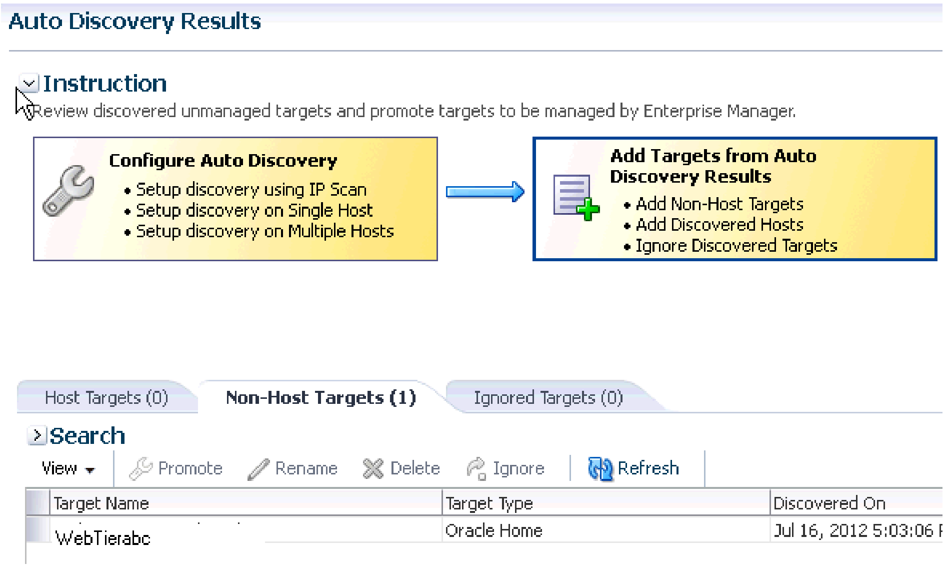
7. Once automatic discovery has been enabled, you should check Cloud Control regularly to view the list of discovered targets. From the **Setup** menu, select **Add Target**, then select **Auto Discovery Results**.

Figure 2–6   Auto Discovery Results Option



8. Click the **Non-Host Targets** tab to view the discovered Oracle Fusion Middleware targets.

Figure 2–7 Auto Discovery Results Page



Auto Discovery Results

Instruction

Review discovered unmanaged targets and promote targets to be managed by Enterprise Manager.

Configure Auto Discovery
- Setup discovery using IP Scan
- Setup discovery on Single Host
- Setup discovery on Multiple Hosts

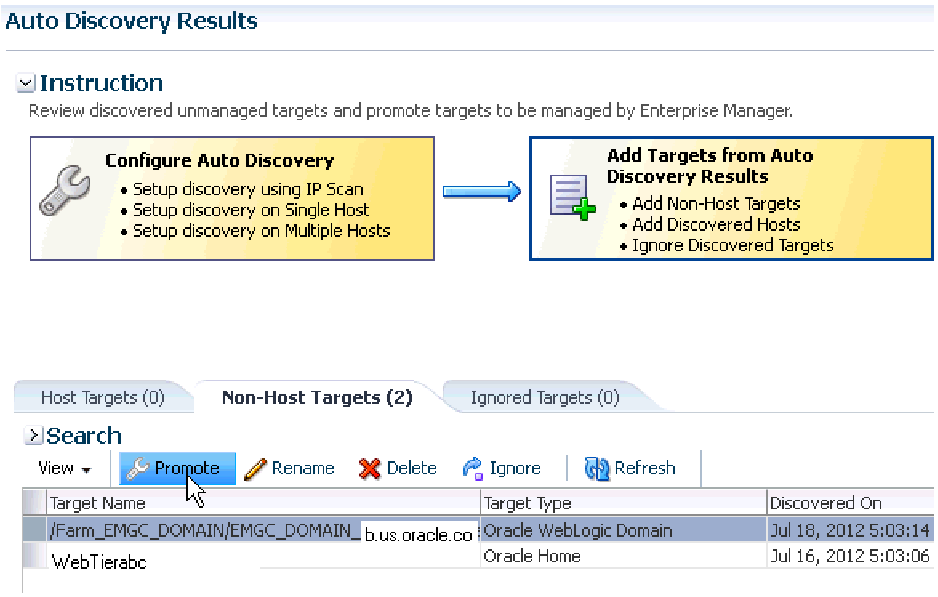
Add Targets from Auto Discovery Results
- Add Non-Host Targets
- Add Discovered Hosts
- Ignore Discovered Targets

Target Name	Target Type	Discovered On
WebTierabc	Oracle Home	Jul 16, 2012 5:03:06 I

9. Select a target, then click **Promote**.

   If multiple targets of various types are listed, you can expand Search, then select the Target Type you are looking for (such as Oracle WebLogic Domain). Click **Search** to display the selected discovered target types.

Figure 2–8 Promote Tab



Auto Discovery Results

Instruction

Review discovered unmanaged targets and promote targets to be managed by Enterprise Manager.

Configure Auto Discovery
- Setup discovery using IP Scan
- Setup discovery on Single Host
- Setup discovery on Multiple Hosts

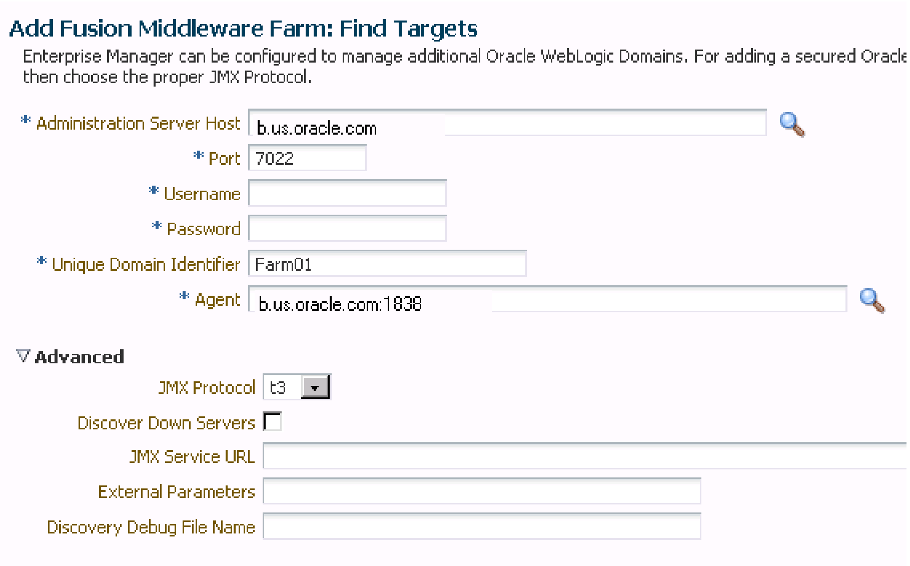
Add Targets from Auto Discovery Results
- Add Non-Host Targets
- Add Discovered Hosts
- Ignore Discovered Targets

Target Name	Target Type	Discovered On
/Farm_EMGC_DOMAIN/EMGC_DOMAIN_ b.us.oracle.co	Oracle WebLogic Domain	Jul 18, 2012 5:03:14
WebTierabc	Oracle Home	Jul 16, 2012 5:03:06

10. Supply or accept values for the following parameters:

    Figure 2–9 shows the parameters that need to be provided.

Figure 2–9 Parameters



Add Fusion Middleware Farm: Find Targets

Enterprise Manager can be configured to manage additional Oracle WebLogic Domains. For adding a secured Oracle then choose the proper JMX Protocol.

* Administration Server Host	b.us.oracle.com
* Port	7022
* Username	
* Password	
* Unique Domain Identifier	Farm01
* Agent	b.us.oracle.com:1838

▽ Advanced

JMX Protocol	t3
Discover Down Servers	□
JMX Service URL	
External Parameters	
Discovery Debug File Name	

- Administration Server Host

  Enter the host name on which the Administration Server is installed and running for the Oracle WebLogic Domain that you want to promote to a managed target, for example: `myhost06.example.com`

- Port

  Enter the WebLogic Administration Server port. The default is 7001.

  If the WebLogic Administration Server is secured using the Secure Sockets Layer (SSL) protocol, specify the location of the trusted keystore file. The keystore is a protected database that holds keys and certificates for an enterprise. See **Advanced Parameters**.

- Enter the WebLogic Administration Server user name and password.

  If you want to discover the target only for monitoring purposes, then it is sufficient to provide a user name that has a monitoring role. If you want to monitor the target and also perform start/stop operations, then ensure that you provide a user name that has either an operator role or an administrator role.

  Note: There is the potential of account locking issues if you enter the default WebLogic user name, and the account password is changed without updating the Enterprise Manager monitoring credentials for the Domain and Farm.

- Unique Domain Identifier.

  Specify a Unique Domain Identifier. This value is used as a prefix to ensure farm names are unique in environments with the same domain name. By default, Enterprise Manager will pre-pend the name with "Farm", followed by a two-digit number, such as "Farm01".

- Agent

  Host name for a Management Agent that will be used to discover the Fusion Middleware targets.

  If a Management Agent exists on the WebLogic Administration Server host, the host name for this Management Agent will be supplied by default.

However, you can specify any Management Agent on any host that is managed by Cloud Control to perform the discovery.

Note: To access all supported features, Oracle recommends that you have a Management Agent local to each managed server in the domain and to use that Management Agent to monitor the WebLogic Servers on that local host machine. Though remote Management Agents can manage WebLogic Server targets, the local Management Agent is recommended.

Some features that are *not* supported when there is no local Management Agent:

- To patch a WebLogic Server, you need a local Management Agent on each WebLogic Server machine.
- If you want to use Oracle Support Workbench for a WebLogic Server target, then the target requires a local Management Agent.
- Cloning requires a local Management Agent at the source administration server machine and a local Management Agent at all destination machines.

Advanced Parameters

If the target domain is secured, expand the Advanced node to specify the protocol to use in the Protocol field. The default value is t3.

For additional details on discovering a domain secured using the Secure Sockets Layer (SSL) protocol, see section "C" in My Oracle Support Note 1093655.1. You can access My Oracle Support at the following URL:

`https://support.oracle.com/CSP/ui/flash.html`

- JMX Protocol

  Used to make a JMX connections to the Administration Server. For Secure domain JMX protocol - use t3s. If WebLogic domain is using a demo certifciate, this certficate is automatically updated to monitoring and discovery agent. If a custom certificate is used, refer to Chapter 7, "Monitoring WebLogic Domains" for information on how to import a certificate.

- Discover Down Servers

  Use this check box to discover servers that are down. While adding Oracle Fusion Middleware WebLogic Domain targets to Enterprise Manager Cloud Control, you can now choose whether to add WebLogic Server targets that are discovered in a down state. This gives you more control in determining what to automatically add to Cloud Control for centralized management and monitoring.

  To monitor down servers, their Listener Address must be set. Otherwise, these servers will have 'temp-host' as host value and the local agent cannot be determined for monitoring. Therefore, the servers will always be shown as down.

  When servers come up, this WebLogic domain needs to be refreshed for populating the correct host name and monitoring.

- JMX Service URL

  Optionally supply the Java Management Extensions (JMX) Service URL that will be used to establish a JMX connection to the WebLogic Administration Server. For example:

```
service:jmx:t3://server.example.com:5555/jndi/weblogic.management.m
beanservers.domainruntime
```

   If you do not specify this URL, Enterprise Manager will provide the Service URL based on the host port and protocol. If this is specified, the Administration server host and port information still must be provided in the input parameters.

- External Parameters

  Optionally enter any system properties to be used by the Java process to connect to the WebLogic Administration Server in the Parameters field.

  Supply space-separated name/value pairs. Preface each parameter with `-D`. For example:

  ```
  -Dparam1=xxx -Dparam2=yyy -Dparam3=zzz
  ```

- Discovery Debug File Name

  If problems occur while adding Middleware-related targets or refreshing domain membership, you can enable additional debugging information to quickly diagnose and resolve the issue. This file will be created in the discovery Agent's log directory.

11. Click **Continue**. Enterprise Manager will discover all Fusion Middleware targets within the domain.
12. Click **Close** in the Finding Targets dialog to automatically assign Management Agents to the discovered targets.

    The Assign Agents page lists each Fusion Middleware target discovered and the Management Agent assigned to each. Agents are automatically assigned as follows:

    - If a local Management Agent is installed on the discovered target host, that Agent will be assigned.
    - If a local Management Agent cannot be found on the host, the Agent specified in the Targets page will be assigned.

    Note that you can also manually assign Management Agents to specific targets, if desired.
13. Click **Add Targets** to assign Management Agents as listed in the Assign Agents page.

    The Saving Target to Agent processing window appears, indicating how many total targets have been added and successfully saved. It will also indicate the number of targets that were unsuccessfully added.
14. Click **Close** in the processing window when finished. The Results page displays the targets and Agent assignments.
15. Click **OK** when finished. There may be a delay before these targets are visible and monitored. All the agents used for monitoring the targets must be up.

2.2 Discovering Targets Manually

This section covers the following:

- Discovering a WebLogic 9.x or 10.x Domain Using Cloud Control
- Discovering Multiple WebLogic Domains Using EM CLI

2.2.1 Discovering a WebLogic 9.x or 10.x Domain Using Cloud Control

Oracle WebLogic Server release 9.x and 10.x domains and their respective components can be discovered using Enterprise Manager Cloud Control. A wizard guides you through the discovery process.

> **Note:** To discover a WebLogic Server domain, the Administration Server must be up because the Management Agent must make a JMX connection to it. If the Administration Server is down, discovery cannot occur.
>
> Thereafter, to monitor the WebLogic Server domain, the Administration Server need not be up.

1. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**.
2. Select the **Add Non-Host Targets Using Guided Process (Also Adds Related Targets)** option.
3. Select **Oracle Fusion Middleware** as the target type.
4. Click **Add Using Guided Discovery**.
5. Supply or accept values for the following parameters:

   - Administration Server Host

     Enter the host name on which the Administration Server is installed and running for the Oracle WebLogic Domain that you want to promote to a managed target, for example: myhost06.example.com

   - Port

     Enter the WebLogic Administration Server port. The default value is 7001.

     If the WebLogic Administration Server is secured using the Secure Sockets Layer (SSL) protocol, specify the location of the trusted keystore file. The keystore is a protected database that holds keys and certificates for an enterprise. See **Advanced Parameters**.

   - Enter the WebLogic Administration Server user name and password.

     If you want to discover the target only for monitoring purposes, then it is sufficient to provide a user name that has a monitoring role. If you want to monitor the target and also perform start/stop operations, then ensure that you provide a user name that has either an operator role or an administrator role.

   - Unique Domain Identifier.

     Specify a Unique Domain Identifier. This value is used as a prefix to ensure farm names are unique in environments with the same domain name. By default, Enterprise Manager will pre-pend the name with "Farm", followed by a two-digit number, such as, "Farm01".

   - Agent

     The host name for a Management Agent that will be used to discover the Fusion Middleware targets.

     If a Management Agent exists on the WebLogic Administration Server host, the host name for this Management Agent will be supplied by default.

However, you can specify any Management Agent on any host that is managed by Cloud Control to perform the discovery.

Note: To access all supported features, Oracle recommends that you have a Management Agent local to each managed server in the domain and to use that Management Agent to monitor the WebLogic Servers on that local host machine. Though remote Management Agents can manage WebLogic Server targets, the local Management Agent is recommended.

Some features that are *not* supported when there is no local Management Agent:

- To patch a WebLogic Server, you need a local Management Agent on each WebLogic Server machine.
- If you want to use Oracle Support Workbench for a WebLogic Server target, then the target requires a local Management Agent.
- Cloning requires a local Management Agent at the source administration server machine and a local Management Agent at all destination machines.

Advanced Parameters

If the target domain is secured, expand the Advanced node to specify the protocol to use in the Protocol field. The default value is t3.

For additional details on discovering a domain secured using the Secure Sockets Layer (SSL) protocol, see section "C" in My Oracle Support Note 1093655.1. You can access My Oracle Support at the following URL:

https://support.oracle.com/CSP/ui/flash.html

- JMX Protocol

  Used to make a JMX connections to the Administration Server.

- Discover Down Servers

  Use this check box to discover servers that are down. While adding Oracle Fusion Middleware WebLogic Domain targets to Enterprise Manager Cloud Control, you can now choose whether to add WebLogic Server targets that are discovered in a down state. This gives you more control in determining what to automatically add to Cloud Control for centralized management and monitoring.

  To monitor down servers, their Listener Address must be set. Otherwise, these servers will have ’temp-host’ as host value and the local agent cannot be determined for monitoring. Therefore, the servers will always be shown as down.

  When servers come up, this WebLogic domain needs to be refreshed for populating the correct host name and monitoring.

- JMX Service URL

  Optionally supply the Java Management Extensions (JMX) Service URL that will be used to establish a JMX connection to the WebLogic Administration Server. For example:

  ```
  service:jmx:t3://server.example.com:5555/jndi/weblogic.management.m
  beanservers.domainruntime
  ```

  If you do not supply a value, Enterprise Manager will provide the Service URL based on the host port and protocol. If this is specified, the

Administration server host and port information still must be provided in the input parameters.

- External Parameters

  Optionally enter any system properties to be used by the Java process to connect to the WebLogic Administration Server in the Parameters field.

  Supply space-separated name/value pairs. Preface each parameter with `-D`. For example:

  ```
  -Dparam1=xxx -Dparam2=yyy -Dparam3=zzz
  ```

- Discovery Debug File Name

  If problems occur while adding Middleware-related targets or refreshing domain membership, you can enable additional debugging information to quickly diagnose and resolve the issue.

6. Click **Continue**. Enterprise Manager will discover all Fusion Middleware targets within the domain.
7. Click **Close** in the Finding Targets dialog to automatically assign Management Agents to the discovered targets.

   The Assign Agents page lists each Fusion Middleware target discovered and the Management Agent assigned to each. Agents are automatically assigned as follows:

   - If a local Management Agent is installed on the discovered target host, that Agent will be assigned.
   - If a local Management Agent cannot be found on the host, the Agent specified in the Targets page will be assigned.

   Note that you can also manually assign Management Agents to specific targets, if desired.
8. Click **Add Targets** to assign Management Agents as listed in the Assign Agents page.

   The Saving Target to Agent processing window appears, indicating how many total targets have been added and successfully saved. It will also indicate the number of targets that were unsuccessfully added.
9. Click **Close** in the processing window when finished. The Results page displays the targets and Agent assignments.
10. Click **OK** when finished. There may be a delay before these targets are visible and monitored. All the agents used for monitoring the targets must be up.

2.2.2 Discovering Multiple WebLogic Domains Using EM CLI

If you have multiple WebLogic domains that you want to manage through Enterprise Manager Cloud Control, you can use the Enterprise Manager Command Line Interface (EM CLI) discover_wls verb to discover them all at once, rather than discovering them one at a time using the discovery wizards.

The discover_wls verb can be used to discover WebLogic Server versions 7.x, 8.x, 9.x, and 10.x domains. The verb reads a file named domain_discovery_file that contains the information required to discover each domain.

See the *Enterprise Manager Command Line Interface* book for instructions on using the discover_wls verb.

2.3 Discovering New or Modified Domain Members

In the typical enterprise, Oracle WebLogic domains do not remain static. Instead, membership in the domain changes regularly: New Java EE applications are deployed, WebLogic Server instances are created or removed, clusters are added, and so on.

By default, Enterprise Manager Cloud Control is not automatically aware of changes made to Oracle WebLogic domains that have been configured as managed targets. However, the application does provide the ability to discover and uptake new or modified domain members.

This section covers the following:

- Enabling Automatic Discovery of New Domain Members
- Manually Checking for New or Modified Domain Members

2.3.1 Enabling Automatic Discovery of New Domain Members

You can enable a pre-defined Cloud Control job named "WebLogic Domain Refresh" to automatically discover new domain members and add them as managed targets.

> **Note:** Whenever you perform the Refresh operation, the Administration Server must be up and the Discovery Agent must be able to connect to it using JMX.

1. From the **Targets** menu, select **Middleware**.
2. Click on the WebLogic Domain you want to enable the job for in the Middleware home page.
3. In the General region of the page, click the timestamp link next to the **WebLogic Domain Refreshed** property. The Refresh WebLogic Domain dialog opens.
4. Check the **Enable Automatic Refresh** box in the Refresh WebLogic Domain dialog, then click **OK**.

Once enabled, the job will check for new domain members once every 24 hours by default. To change the job settings, including the frequency at which it is run:

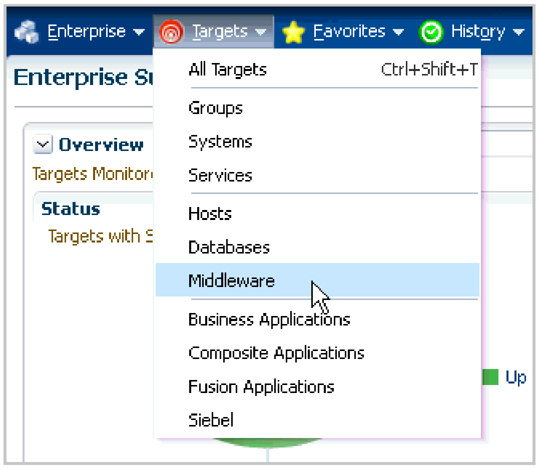
1. Click the **Jobs** tab.
2. Click the job title in the Job Activity page.
3. Click **Edit**.

2.3.2 Manually Checking for New or Modified Domain Members

You can use Cloud Control to check a domain for new or modified members on a periodic basis.

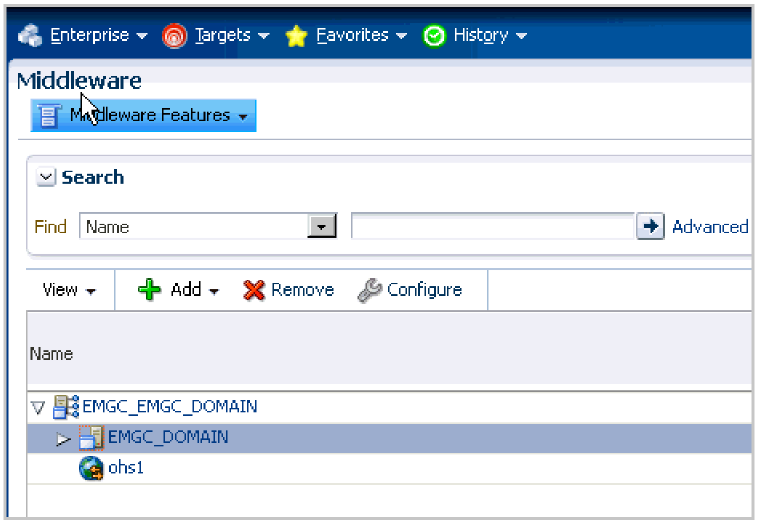
1. From the **Targets** menu, select **Middleware**.

Figure 2–10 Targets Menu



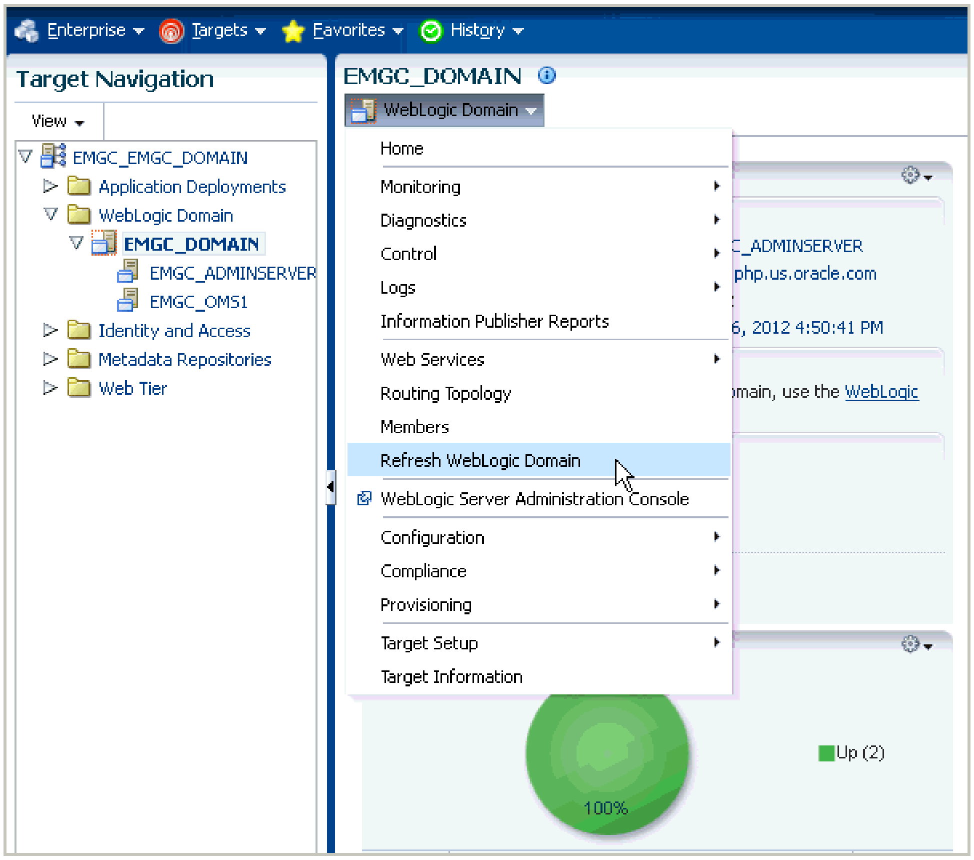
2. Click the WebLogic Domain you want to (enable the job for in the Middleware home page) refresh.

Figure 2–11 WebLogic Domain to Enable



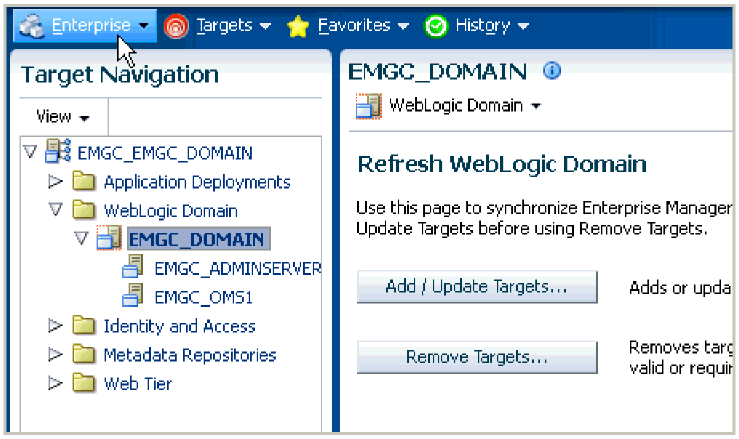
3. From either the **Farm** or **WebLogic Domain** menu, select **Refresh WebLogic Domain**. The Refresh WebLogic Domain dialog opens.

Figure 2–12 Refresh WebLogic Domain Menu Option



4. Click **Add/Update Targets**. The Management Agent refreshes by connecting to the Administration Server. The Administration Server must be up for the refresh to occur. Click **Close** on the Confirmation page. Cloud Control will search the domain for new and modified targets.

Figure 2–13 Add/Update Option on Refresh WebLogic Domain Page



Refresh WebLogic Domain

Use this page to synchronize Enterprise Manager
Update Targets before using Remove Targets.

Adds or upda

Removes targ
valid or requir

5. The Assign Agents page displays the Fusion Middleware targets discovered and the Management Agent assigned to each. Click **Add Targets** to assign Management Agents as listed in the Assign Agents page.

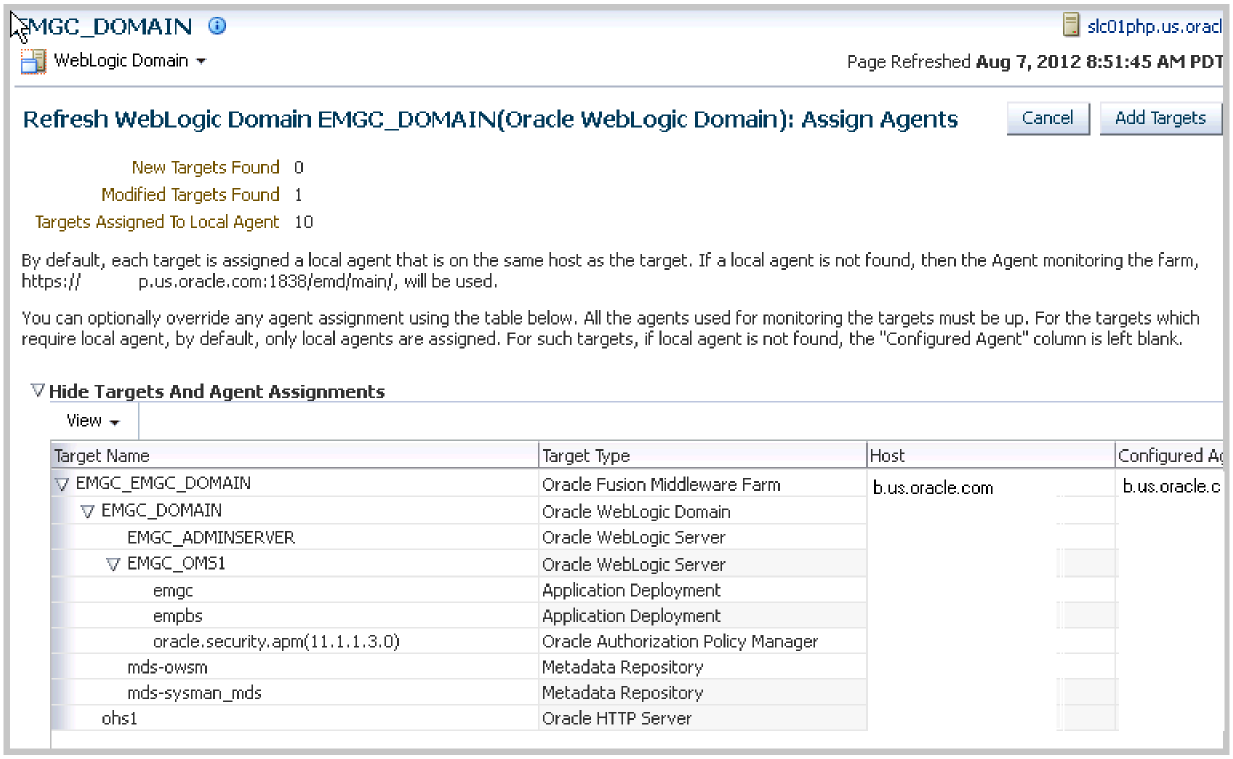
   Agents are automatically assigned as follows:

- If a local Agent can be found on the target host, that Agent will be assigned.
- If a local Agent cannot be found on the host, the Agent specified in the Targets page will be assigned.

Note that you can also manually assign Agents to specific targets, if desired.

You can also modify the Domain Global Properties, for example, Contact, Cost Center, Lifecycle Status, and so on).

Figure 2–14 Assign Agents Page



EMGC_DOMAIN

slc01php.us.oracl

WebLogic Domain

Page Refreshed **Aug 7, 2012 8:51:45 AM PDT**

Refresh WebLogic Domain EMGC_DOMAIN(Oracle WebLogic Domain): Assign Agents

Cancel Add Targets

New Targets Found 0

Modified Targets Found 1

Targets Assigned To Local Agent 10

By default, each target is assigned a local agent that is on the same host as the target. If a local agent is not found, then the Agent monitoring the farm, https:// p.us.oracle.com:1838/emd/main/, will be used.

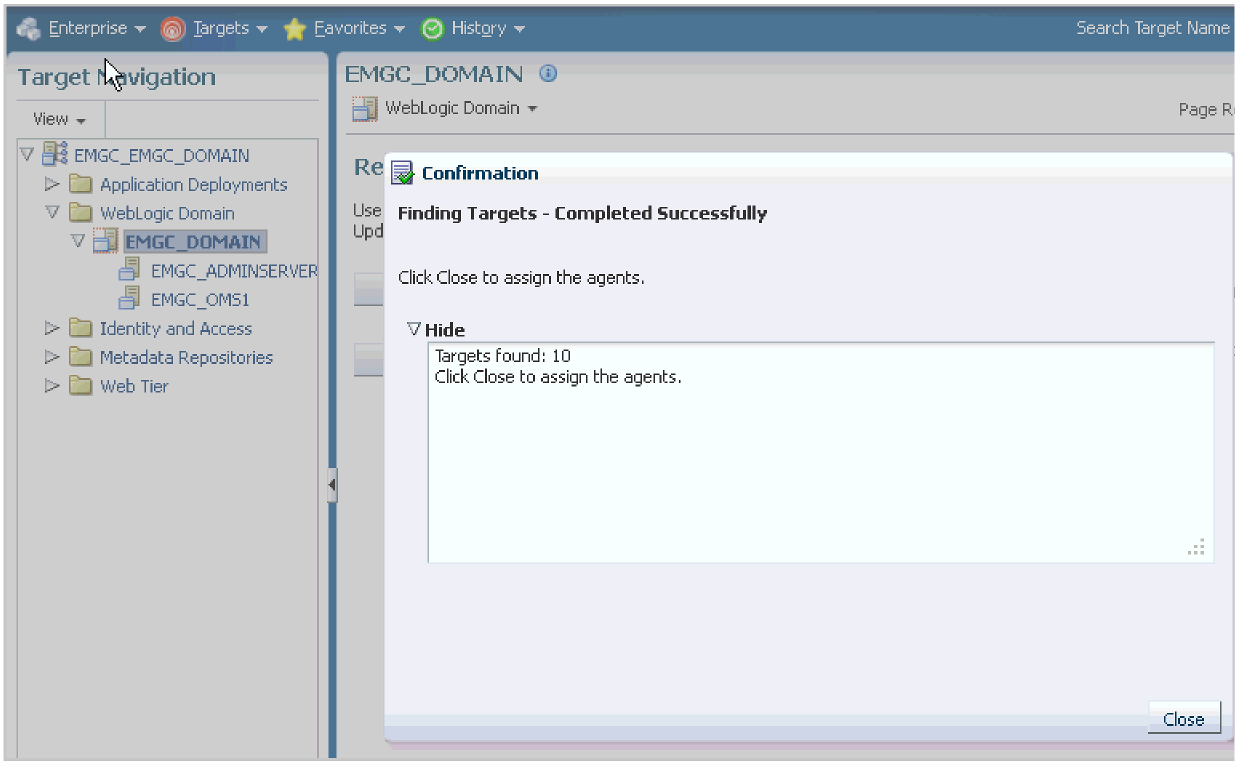
You can optionally override any agent assignment using the table below. All the agents used for monitoring the targets must be up. For the targets which require local agent, by default, only local agents are assigned. For such targets, if local agent is not found, the "Configured Agent" column is left blank.

▽ **Hide Targets And Agent Assignments**

View

Target Name	Target Type	Host	Configured Ag
▽ EMGC_EMGC_DOMAIN	Oracle Fusion Middleware Farm	b.us.oracle.com	b.us.oracle.c
▽ EMGC_DOMAIN	Oracle WebLogic Domain		
EMGC_ADMINSERVER	Oracle WebLogic Server		
▽ EMGC_OMS1	Oracle WebLogic Server		
emgc	Application Deployment		
empbs	Application Deployment		
oracle.security.apm(11.1.1.3.0)	Oracle Authorization Policy Manager		
mds-owsm	Metadata Repository		
mds-sysman_mds	Metadata Repository		
ohs1	Oracle HTTP Server		

Figure 2–15 Confirmation of Finding Targets



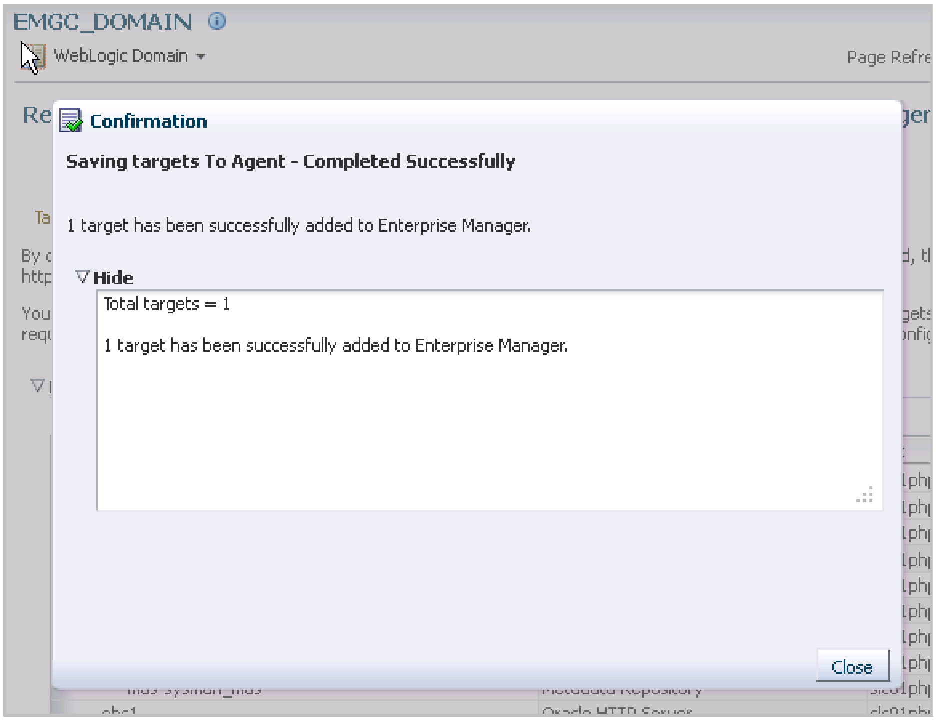
Finding Targets - Completed Successfully

Click Close to assign the agents.

Targets found: 10
Click Close to assign the agents.

6. The Saving Targets to Agent processing window appears, indicating how many total targets have been added and successfully saved. It will also indicate the number of targets that were unsuccessfully added.

Figure 2–16 Confirmation Saving Targets to Agent



Saving targets To Agent - Completed Successfully

1 target has been successfully added to Enterprise Manager.

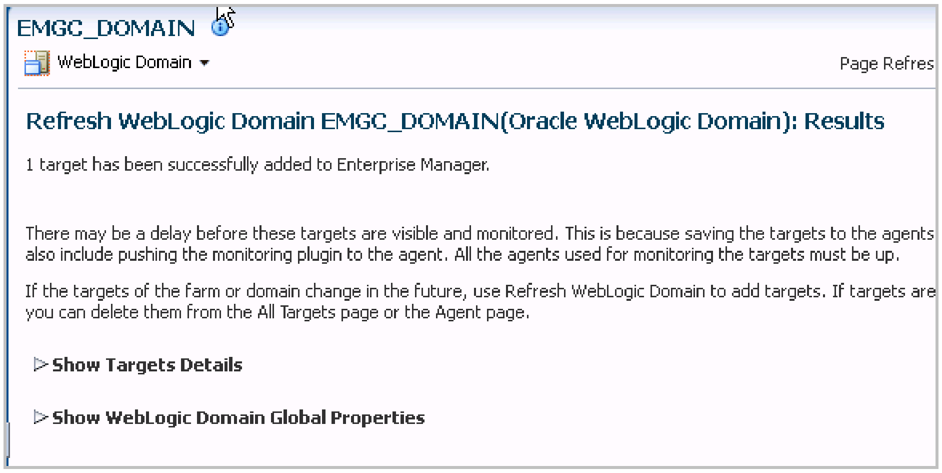
Total targets = 1

1 target has been successfully added to Enterprise Manager.

7. Click **Close** in the processing window when finished. The Results page displays the following options: Show Targets Details and Show Weblogic Domain Global Properties. The Show Targets Details page shows the targets and Agent assignments.

   Note: If there were targets that were removed, you can go back to the Refresh WebLogic Domain page and click **Remove Targets** to remove the targets and any historical information in the Management Repository. See Removing Targets.

Figure 2–17 Refresh WebLogic Domain Results Page



Refresh WebLogic Domain EMGC_DOMAIN(Oracle WebLogic Domain): Results

1 target has been successfully added to Enterprise Manager.

There may be a delay before these targets are visible and monitored. This is because saving the targets to the agents also include pushing the monitoring plugin to the agent. All the agents used for monitoring the targets must be up.

If the targets of the farm or domain change in the future, use Refresh WebLogic Domain to add targets. If targets are you can delete them from the All Targets page or the Agent page.

▷ **Show Targets Details**

▷ **Show WebLogic Domain Global Properties**

8. Click **OK** when finished. There may be a delay before these targets are visible and monitored. All the agents used for monitoring the targets must be up.

2.3.3 Removing Targets

Removing targets from the Management Repository:

- Identifies targets that are deleted from the Weblogic Domain, for example, WebLogic Servers, Clusters, Applications (both generic and custom), and any other System Components.
- Shows the list of targets which *might* have been deleted from the product, but Enterprise Manager cannot determine if they were deleted or not. For these targets, decide whether these targets should be deleted and mark them as such.
- Shows duplicate targets. For example, if for the same application deployment there is a custom and a generic target, the will shows the generic target which can be deleted.
- Shows the older versioned application deployments which can be deleted if a newer version of the same application is present.
- Lists all the down servers. You can decide to either blackout or delete these servers.

3

Managing Middleware Targets

This chapter describes how you can use Enterprise Manager to monitor Middleware software.

> **Note:** Oracle provides a free self-paced course regarding the best practices on managing WebLogic and Service Oriented Architecture (SOA) applications and infrastructure. It consists of interactive lectures, videos, review sessions, and optional demonstrations, and lasts about two hours.
>
> The *Oracle Enterprise Manager Cloud Control 12c: Best Practices for Middleware Management* self-study is available at `http://www.oracle.com/webfolder/technetwork/tutorials/tutorial/em/Oracle%20Enterprise%20Manager%20Cloud%20Control%2012c%20Middleware%20Management%20Best%20Practices%20Self-Study%20Course/player.html`

This chapter covers the following:

3.1 Middleware Targets in Enterprise Manager

After you have added a Middleware target (e.g. Oracle Fusion Middleware, Oracle WebLogic Domain, Oracle Application Server, JBoss Application Server), you can view general information about the targets including their status and availability on the Middleware page. You can drill down into each target to get further details like how the target is performing, where it is deployed, the version, location of its home directory, and so on.

You can also view the number of critical, warning, and error alerts generated for the past 24 hours. These alerts indicate that a particular metric condition has been encountered. For example, an alert is triggered when a metric threshold is reached. Using these details, you can drill down to investigate the target and the problem that triggered the alert.

You can monitor the following components using Oracle Enterprise Manager Cloud Control:

- Oracle Fusion Middleware Components
- Oracle Application Server Components
- Non-Oracle Middleware Components

3.1.1 Oracle Fusion Middleware Components

A farm is a collection of components managed by Fusion Middleware Control. It can contain Oracle WebLogic Domains, one Administration Server, one or more Managed Servers, and the Oracle Fusion Middleware components that are installed, configured, and running in the domain. You can monitor the following Oracle Fusion Middleware components using Enterprise Manager:

- **Oracle WebLogic Domains, Clusters, and Managed Servers**: A WebLogic Server domain is a logically related group of WebLogic Server resources that you manage as a unit. A domain includes one or more WebLogic Servers and may also include WebLogic Server clusters. Clusters are groups of WebLogic Servers instances that work together to provide scalability and high-availability for applications. With Oracle Enterprise Manager, you can monitor and manage the farm, domains, clusters, servers, and deployed applications.
- **Oracle SOA Suite**: The Oracle SOA Suite enables services to be created, managed, and orchestrated into SOA composite applications. Composite applications enable you to easily assemble multiple technology components into one SOA composite application. Oracle SOA Suite plugs into heterogeneous infrastructures and enables enterprises to incrementally adopt SOA. You can:
  - Automatically discover and model SOA components such as BPEL Process Manager, Oracle Service Bus, Service Engines, and so on.
  - Monitor the health and performance of the SOA components.
  - Trace the flow of an instance across all SOA Infrastructure applications.
  - Create systems, services, and aggregate services.
- **Oracle WebCenter**: The Oracle WebCenter is an integrated set of components with which you can create social applications, enterprise portals, collaborative communities, and composite applications, built on a standards-based, service-oriented architecture. It combines dynamic user interface technologies with which to develop rich internet applications, the flexibility and power of an integrated, multichannel portal framework, and a set of horizontal Enterprise 2.0 capabilities delivered as services that provide content, collaboration, presence, and social networking capabilities. Based on these components, Oracle WebCenter also provides an out-of-the-box, enterprise-ready customizable application, WebCenter Spaces, with a configurable work environment that enables individuals and groups to work and collaborate more effectively.
- **Oracle Web Tier**: This consists of:
  - Oracle HTTP Server: Oracle HTTP Server (OHS) is the underlying deployment platform for all programming languages and technologies that Oracle Fusion

Middleware supports. It provides a Web listener and the framework for hosting static and dynamic pages and applications over the Web. Based on the proven technology of the Apache 2.2.10 infrastructure, OHS includes significant enhancements that facilitate load balancing, administration, and configuration. It also includes a number of enhanced modules, or mods, which are extensions to the HTTP server that extend its functionality for other enterprise applications and services. You can:

      - Automatically discover and monitor Oracle HTTP Servers running within the application servers.
      - View a list of metrics to gauge the server performance and virtual host performance.
      - View the top URLs being accessed.
      - Perform the enterprise configuration management tasks like viewing, comparing, and searching configuration information.

  - **Oracle Web Cache**: Oracle Web Cache is a content-aware server accelerator, or reverse proxy, for the Web tier that improves the performance, scalability, and availability of Web sites that run on any Web server or application server, such as Oracle HTTP Server and Oracle WebLogic Server. Oracle Web Cache is the primary caching mechanism provided with Oracle Fusion Middleware. Caching improves the performance, scalability, and availability of Web sites that run on Oracle Fusion Middleware by storing frequently accessed URLs in memory. You can:

    - Automatically discover and monitor OracleAS Web Cache instances running within application servers.
    - View the metrics associated with this target to analyze their performance.
    - Perform enterprise configuration tasks like viewing, comparing, and searching configuration information.

- **Oracle Identity Management**: This is an enterprise identity management system that automatically manages users' access privileges within the resources of an enterprise. The architecture of Oracle Identity Management works with the most demanding business requirements without requiring changes to existing infrastructure, policies, or procedures. It provides a shared infrastructure for all Oracle applications. It also provides services and interfaces that facilitate third-party enterprise application development. These interfaces are useful for application developers who need to incorporate identity management into their applications.

- **Oracle Portal**: This is a Web-based tool for building and deploying e-business portals. It provides a secure, manageable environment for accessing and interacting with enterprise software services and information resources. A portal page makes data from multiple sources accessible from a single location.

- **Oracle Forms Services** is a middle-tier application framework for deploying complex, transactional forms applications to a network such as an Intranet or the Internet. With Oracle Forms Services, business application developers can quickly build comprehensive Java client applications that are optimized for the Internet without writing any Java code, and that meet (and exceed) the requirements of professional user communities. These Java client applications are Web-deployed applications available on demand for rapid processing of large amounts of data and rapid completion of complex calculations, analysis, and transactions.

- **Oracle Coherence** is a component of Oracle Fusion Middleware that enables organizations to predictably scale mission-critical applications by providing fast and reliable access to frequently used data. By automatically and dynamically partitioning data in memory across multiple servers, Oracle Coherence enables continuous data availability and transactional integrity, even in the event of a server failure. As a shared infrastructure, Oracle Coherence combines data locality with local processing power to perform real-time data analysis, in-memory grid computations, and parallel transaction and event processing. Oracle Coherence comes in three editions. You can:
  - Discover and manage a Coherence cluster and its various entities.
  - Monitor and configure various components such as nodes, caches, services, connections, and connection manager instances of a Coherence cluster.
  - Deploy and install a Coherence node based on the Provisioning Advisory framework.
- **Oracle Business Intelligence** is a complete, integrated solution that addresses business intelligence requirements. Oracle Business Intelligence includes Oracle Business Intelligence Reporting and Publishing, Oracle Business Intelligence Discoverer, and Oracle Business Intelligence Publisher. You can:
  - Manually discover Oracle BI Suite EE targets, and monitor their overall health.
  - Diagnose, notify, and correct performance and availability problems in Oracle BI Suite EE targets.
  - Access current and historical performance information using graphs and reports.
  - Perform enterprise configuration management tasks like viewing, comparing, and searching configuration information.
- Oracle Universal Content Management System provides a unified application for several different kinds of content management. It is an enterprise content management platform that enables you to leverage document management, Web content management, digital asset management, and records retention functionality to build and complement your business applications. Building a strategic enterprise content management infrastructure for content and applications helps you to reduce costs, easily share content across the enterprise, minimize risk, automate expensive, time-intensive and manual processes, and consolidate multiple Web sites onto a single platform for centralized management. Through user-friendly interfaces, roles-based authentication and security models, Oracle Universal Content Management empowers users throughout the enterprise to view, collaborate on or retire content, ensuring that all accessible distributed or published information is secure, accurate and up-to-date.

3.1.2 Oracle Application Server Components

You can monitor Oracle Application Server 10g components like Oracle Application Server Farms, Oracle Application Server Clusters, Oracle Application Servers, OC4J, Oracle HTTP Servers, Oracle Web Cache, Oracle Portal, Oracle Wireless, Oracle Forms Services, Oracle Reports Services, Oracle Business Intelligence, and Oracle Identity Management.

3.1.3 Non-Oracle Middleware Components

In addition to monitoring Oracle Middleware components, Enterprise Manager can also be used to monitor non-Oracle Middleware software. The third-party Middleware software that can be monitored includes the following:

- WebSphere Application Server
- WebSphere MQ
- JBoss Application Server
- Apache Tomcat
- Apache HTTP Server
- Microsoft Exchange Server
- Microsoft Internet Information Services
- Microsoft Active Directory
- Microsoft Commerce Server
- Microsoft BizTalk Server
- Microsoft Internet Security and Acceleration
- Microsoft .NET Framework

3.2 Monitoring Middleware Targets

Enterprise Manager organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for the farm, domain, servers, components, and applications.

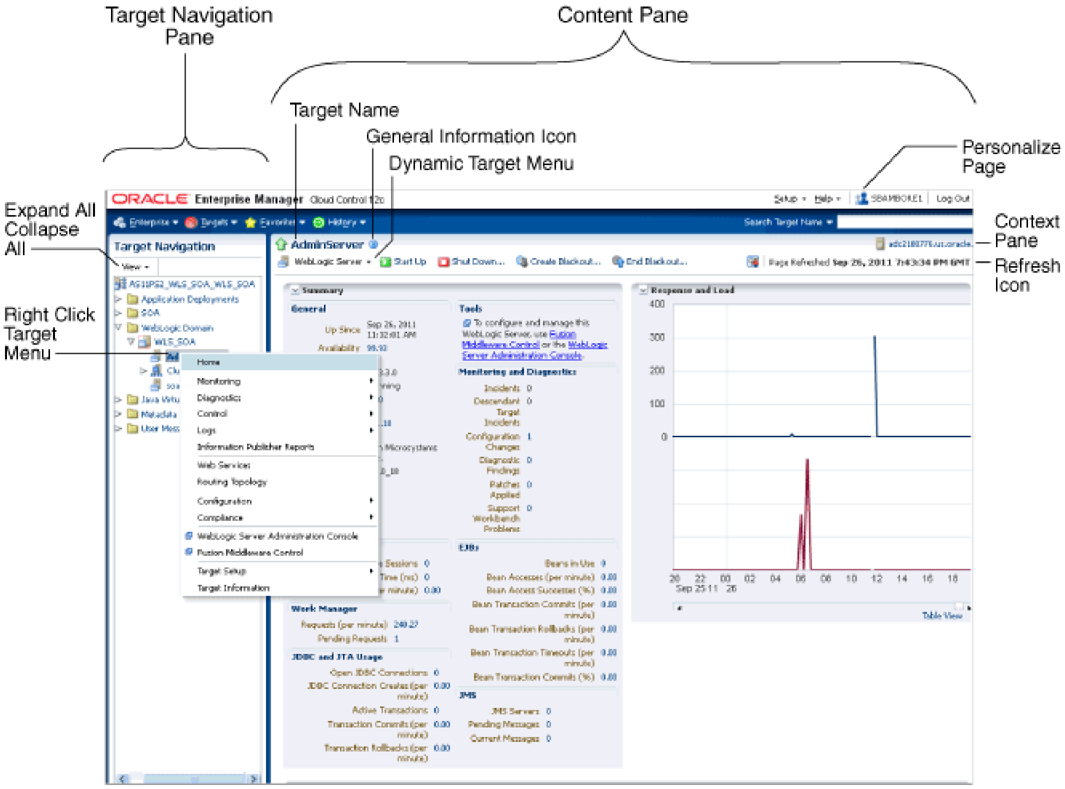
3.2.1 Target Home Page

Enterprise Manager provides centralized monitoring across domains, configuration management, provisioning, real time and historical performance analysis. You need to drill down to Oracle Fusion Middleware Control to perform administrative tasks and manage components in your farm.

The Home pages make it easy to locate the most important monitoring data and the most commonly used administrative functions—all from your Web browser.

When you login into Enterprise Manager and select a Middleware target, the Home page for the target is displayed. For example, when you click on a WebLogic Server target in the Middleware page, the following screen is displayed.

Figure 3–1 WebLogic Server Home Page



This figure shows the target navigation pane on the left and the content page on the right. From the target navigation pane, you can expand the tree and select a component or an application. When you select a target, the target's home page is displayed in the content pane and that target's menu is displayed at the top of the page, in the context pane. You can also view the menu for a target by right-clicking the target in the navigation pane.

In the preceding figure, the following items are called out:

- **Target Navigation Pane** lists all of the targets in a navigation tree
- **Content Pane** shows the current page for the target. When you first select a target, that target's home page is displayed.
- **Dynamic Target Menu** provides a list of operations that you can perform on the currently selected target. The menu that is displayed depends on the target you select. The menu for a specific target contains the same operations as those in the Right-Click Target Menu.
- **Right-Click Target Menu** provides a list of operations that you can perform on the currently selected target. The menu is displayed when you right-click the target name in the target navigation pane. In the figure, even though the WebLogic Server is selected and its home page is displayed, the right-click target menu displays the operations for the selected target.
- **Target Name** is the name of the currently selected target.
- **Context Pane** provides the host name, the time of the last page refresh, the Refresh icon, and the Personalize Page icon.
- **View**: You can select options to Expand All / Collapse All, Scroll First, and Scroll Last in the navigation tree.

- **Refresh** icon indicates when the page is being refreshed. Click it to refresh a page with new data. (Refreshing the browser window refreshes the page but does not retrieve new data.)

From the Home page, you can also access the Fusion Middleware Control and WebLogic Server Administration Console by clicking on the appropriate link or selecting the appropriate menu item on the page.

3.2.2 Out-of-box Metrics

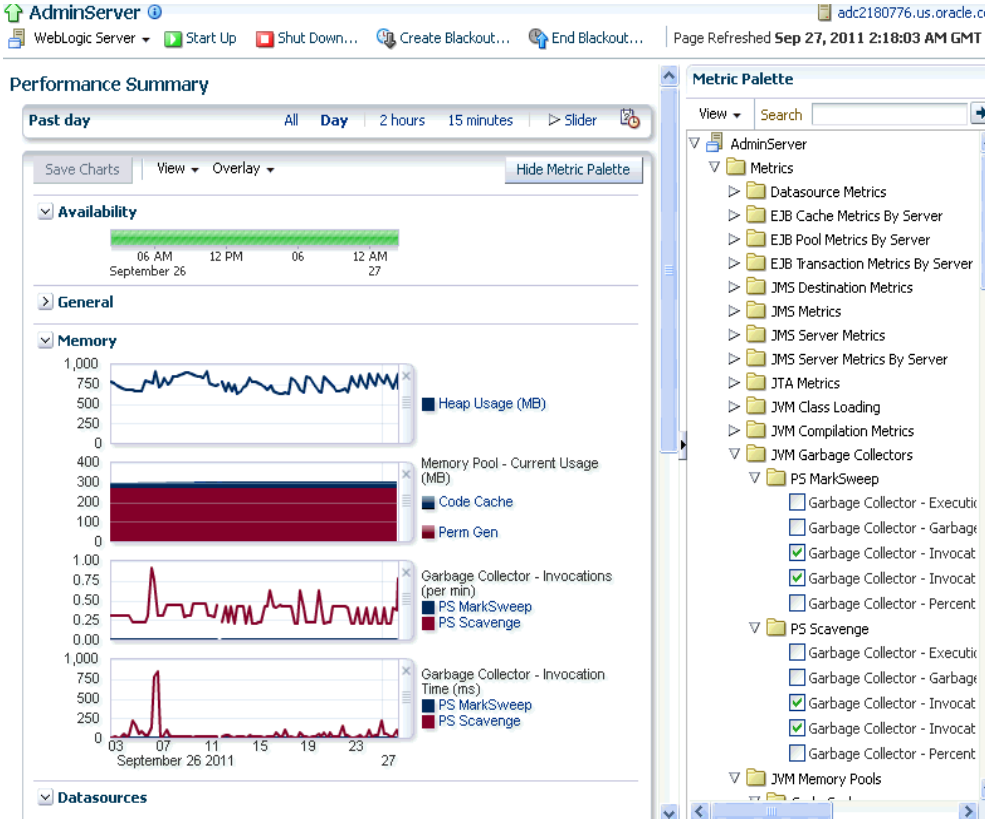
Enterprise Manager provides a set of pre-defined performance metrics for each Middleware target. These metrics are available for domains, cluster, server, applications, web services, resources etc. The metric data is collected and stored in the Management Repository. For more details on the pre-defined metrics, see the *Oracle Fusion Middleware Metric Reference Guide*.

For example, Enterprise Manager can automatically monitor:

- The CPU or memory consumption of the application server, including detailed monitoring of individual Java Virtual Machines (JVMs) being run by Oracle WebLogic servers.
- Java EE application responsiveness from the application down through individual servlets and Enterprise JavaBeans (EJBs)
- Oracle HTTP Server session volumes, connection duration, and error rates
- Oracle Web Cache hit rates and volumes
- Top servlets based on number of requests, maximum processing time, and highest average processing time

The performance metrics provide details about the metric as a current real time value (30 seconds, 1 minute, or 5 minutes) or a previous value (past 24 hours, 7 days, or 31 days). The historical information is displayed as graphs and a table. By using graphs, you can easily watch for trends, and by using tables, you can examine details of past metric severity history. The out-of-metrics can be viewed from the performance summary pages as shown below:

Figure 3–2 Performance Summary Page



You can change which charts are displayed on the performance page and then save the changes on a per-user, per-target-type basis. You can also save multiple customized versions of a performance page, giving each version a name. This will save time by allowing quick access to previously created version of the page. The Performance Summary feature allows you to create named chart views. The generic performance page is always shown in the context of one primary target. However, the performance of that target may be dependent on, or affect the performance of other targets. To explore these relationships you can chart metrics for multiple related targets on one performance page. The Performance Summary feature allows you to chart metrics for multiple related targets.

3.2.3 Analyzing Historical Performance

Enterprise Manager allows you to analyze historic metric data and perform trend analysis. In Fusion Middleware Control, you cannot analyze historical metric data and the real-time analysis is limited to a single domain. But in Enterprise Manager, the metrics are collected and stored in the Management Repository, so you can analyze the data well after the situation has changed. For example, you can use historical data and diagnostic reports to research an application performance problem that occurred days or even weeks ago.

You can even provide a customized time period for which the data should be retrieved from the Management Repository. You can customize the time period for:

- Pre-defined range of the last 24 hours, last 7 days, or last 31 days
- Customized range of any number of days, weeks, months, or years
- Any start date and end date (such that the duration is not greater than 99 years)

Note: You can analyze historical metric data with Enterprise Manager only. You cannot use Fusion Middleware Control to analyze historic performance.

3.2.4 Setting Metric Thresholds for Alert Notifications

Metric snapshots are named snapshots of a target's past performance. You can use metric snapshots to calculate thresholds based on deviations from this past performance. Thresholds are boundary values against which monitored metric values are compared. You can specify a threshold such that, when a monitored metric value crosses that threshold, an alert is generated. You can get critical alerts when a monitored metric has crossed its critical threshold or warning alerts when a monitored metric has crossed its warning threshold.

Enterprise Manager provides a comprehensive set of features that facilitates automated monitoring and generation of alerts. You can gather and evaluate diagnostic information for targets distributed across the enterprise, and an extensive array of Middleware performance metrics are automatically monitored against predefined thresholds. By selecting a metric, you can determine whether the thresholds have been defined for a particular metric. These thresholds are used as a mechanism to generate alerts. These alerts in turn are used to notify you whether a target is up or down, the response time is slow, and so on. Thus, you can monitor their overall performance.

You can set up corrective actions to automatically resolve an alert condition. These corrective actions ensure that routine responses to alerts are automatically executed, thereby saving you time and ensuring that problems are dealt with before they noticeably impact the users.

3.2.5 Monitoring Templates

You can also use monitoring templates to simplify the task of standardizing monitoring settings across your enterprise. You can specify the monitoring settings once and apply them to all Oracle Fusion Middleware targets. A Monitoring template defines all the parameters you would normally set to monitor Middleware target, such as:

- Target type to which the template applies
- Metrics (including user-defined metrics), thresholds, metric collection schedules, and corrective actions

When a change is made to a template, you can reapply the template across the affected targets in order to propagate the new changes. You can reapply monitoring templates as often as needed.

3.2.6 Managing and Creating Blackouts

Enterprise Manager comes with a bundle of performance and health metrics that enable automated monitoring of application targets in your environment. When a metric reaches the predefined warning or critical threshold, an alert is generated and the administrator is notified.

However, there are occasions when you want to perform maintenance work on your Middleware targets, and not want any alerts to be generated while you are bringing them down. In this case, you can schedule a blackout and suspend monitoring of the Middleware targets.

Blackouts allow you to suspend any data collection activity on one or more monitored targets, thus allowing you to perform scheduled maintenance on targets. If you continue monitoring during these periods, the collected data will show trends and other monitoring information that are not the result of normal day-to-day operations. To get a more accurate, long-term picture of a target's performance, you can use blackouts to exclude these special-case situations from data analysis. Enterprise Manager allows you to define new blackouts; view the status of existing blackouts; and edit, stop, and delete blackouts that are not required.

3.2.7 Extend Monitoring for Applications Deployed to WebLogic Server

Many administrators often require custom logic to be written to check for conditions specific to their application environments. Enterprise Manager allows integration of application instrumentation in the Enterprise Manager event monitoring infrastructure. If application developers expose application instrumentation using standards like JMX or Web Services operations, then you can build management plug-ins for the instrumentation using easy-to-use command line tools, and leverage the Enterprise Manager event monitoring system to monitor it. You do not have to edit any XML files or write any integration code to integrate such instrumentation. Follow these procedures to integrate application-defined instrumentation:

- Use Command Line Interfaces that analyze MBean interfaces for JMX and WSDL for Web Services and create management plug-ins
- Import Management Plug-in Archive in Enterprise Manager
- Deploy Management Plug-in to Management Agents
- Create Target-type instances for the target types defined in Management Plug-in Archive
- Leverage the Enterprise Manager event monitoring system including monitoring templates, corrective actions, historical and real time metric views, alerts, customization of notification rules, and methods on events generated from application instrumentation metrics.

Administrators are able to add performance metrics beyond those available out-of-box for JMX-instrumented applications deployed on Oracle WebLogic Server. Administrators can additionally monitor JMX-enabled applications by defining new target type that can be monitored via management plug-ins, and then use a command line tool `emjmxcli` to automate the generation of the target metadata and collection files.All JMX-enabled applications deployed to the WebLogic Server can be consolidated and monitored by a single management tool, Enterprise Manager.

3.2.8 Request Monitoring

Request Monitoring provides end-to-end visibility into requests and helps localize end-user performance problems based on the deployment model. You can monitor, understand, and visualize how servers interact with each other to deliver business end-user services requests. You can trace important end-user requests from the client to the service endpoint across all the servers and applications associated with each transaction. The trace data is used to model the call-path for these requests where call-paths represent the inter-server relationship and performance metrics for these requests. You can only monitor synchronous transactions running on WebLogic servers. With Request Monitoring, you can:

- Trace end-user transactions and capture the complete call-path of important requests.

- Reduce problem localization by diagnosing poorly performing requests and identifying the servers whose behavior (service time) deviates most from the norm.
- Reduce fault discovery time and set performance level objectives on request response times.
- Reduce fault-reason identification time by allowing the user to launch into Oracle Enterprise Manager JVM Diagnostics feature. This allows performance diagnostics to be done within the context of the problem experienced as well as historical statistics of the system when it was behaving normally.

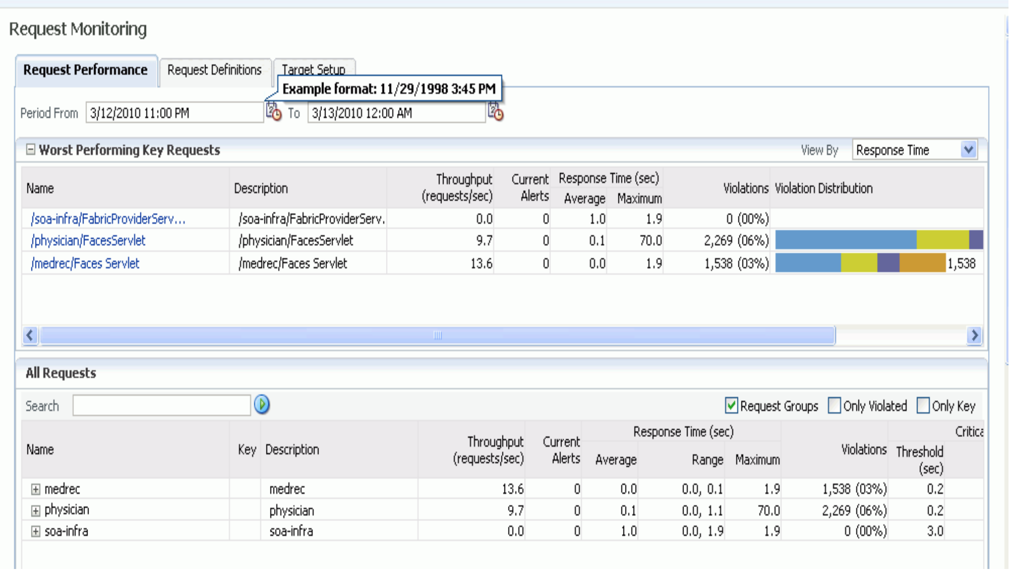
3.2.8.1 Defining and Managing Transactions Being Monitored

A request is a server entry-point that can be invoked by a Web Browser or an application. A group of request instances related to each other by some common attributes is known as a request. A collection of requests is known as a transaction group. A transaction can belong to one or more transaction groups. Violations occur when the critical and warning thresholds are exceeded. The administrator can mark one or more important requests as key requests. Alerts are generated for key requests only.

You can define requests that need to be monitored and tracked and group them for reporting purposes. A set of pre-defined requests and request groups are provided by default. You can create a new request, edit or delete an existing transaction. To define a request:

1. From the **Targets** menu, select **Middleware**.
2. From the **Middleware Features** menu, select **Request Monitoring**.
3. Click **Request Performance** to view the performance of the request during a specific time period.

Figure 3–3 Request Performance Page



Period From 3/12/2010 11:00 PM To 3/13/2010 12:00 AM

Worst Performing Key Requests — View By: Response Time

Name	Description	Throughput (requests/sec)	Current Alerts	Response Time (sec)		Violations	Violation Distribution
				Average	Maximum		
/soa-infra/FabricProviderServ...	/soa-infra/FabricProviderServ.	0.0	0	1.0	1.9	0 (00%)	
/physician/FacesServlet	/physician/FacesServlet	9.7	0	0.1	70.0	2,269 (06%)	
/medrec/Faces Servlet	/medrec/Faces Servlet	13.6	0	0.0	1.9	1,538 (03%)	1,538

All Requests

Search ☑ Request Groups □ Only Violated □ Only Key

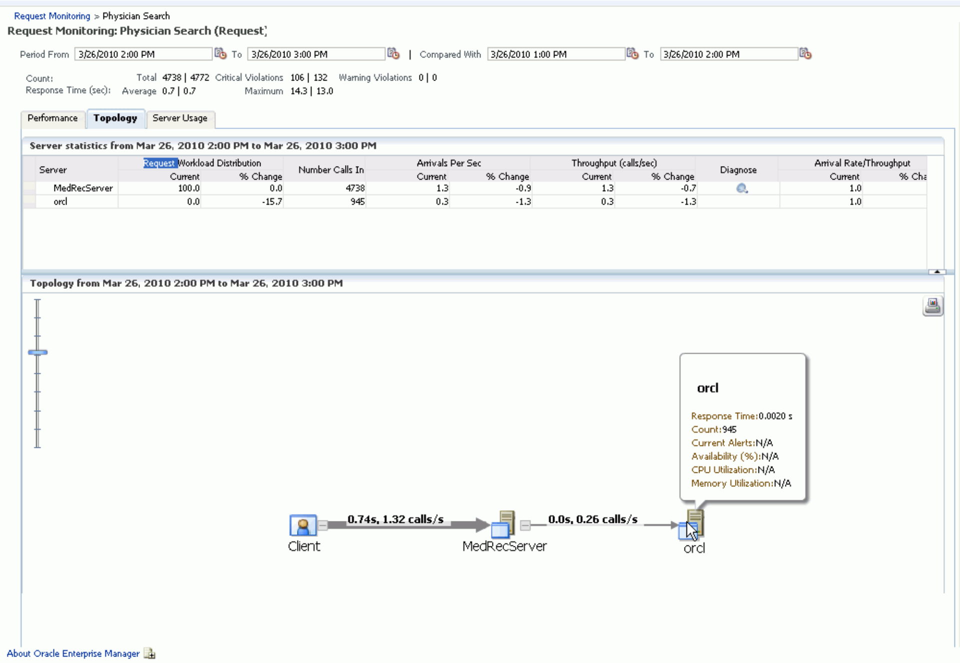
Name	Key	Description	Throughput (requests/sec)	Current Alerts	Response Time (sec)			Violations	Critica
					Average	Range	Maximum		Threshold (sec)
⊞ medrec		medrec	13.6	0	0.0	0.0, 0.1	1.9	1,538 (03%)	0.2
⊞ physician		physician	9.7	0	0.1	0.0, 1.1	70.0	2,269 (06%)	0.2
⊞ soa-infra		soa-infra	0.0	0	1.0	0.0, 1.9	1.9	0 (00%)	3.0

4. Click on a request to drill down to the Performance tab. The performance charts show the volume of requests over a time period and the average response time of all requests during this period. Two performance charts are displayed for the

current and the comparison period. The charts provide a historic response time analysis of the request over the selected period of time.

5. Click on the **Topology** tab. The following screen is displayed.

Figure 3–4 Request Monitoring: Topology Page



Request Monitoring > Physician Search

Request Monitoring: Physician Search (Request)

Period From 3/26/2010 2:00 PM To 3/26/2010 3:00 PM | Compared With 3/26/2010 1:00 PM To 3/26/2010 2:00 PM

Count: Total 4738 | 4772 Critical Violations 106 | 132 Warning Violations 0 | 0

Response Time (sec): Average 0.7 | 0.7 Maximum 14.3 | 13.0

Server statistics from Mar 26, 2010 2:00 PM to Mar 26, 2010 3:00 PM

Server	Request Workload Distribution		Number Calls In	Arrivals Per Sec		Throughput (calls/sec)		Diagnose	Arrival Rate/Throughput	
	Current	% Change		Current	% Change	Current	% Change		Current	% Cha
MedRecServer	100.0	0.0	4738	1.3	-0.9	1.3	-0.7	🔍	1.0	
orcl	0.0	-15.7	945	0.3	-1.3	0.3	-1.3		1.0	

Topology from Mar 26, 2010 2:00 PM to Mar 26, 2010 3:00 PM

orcl

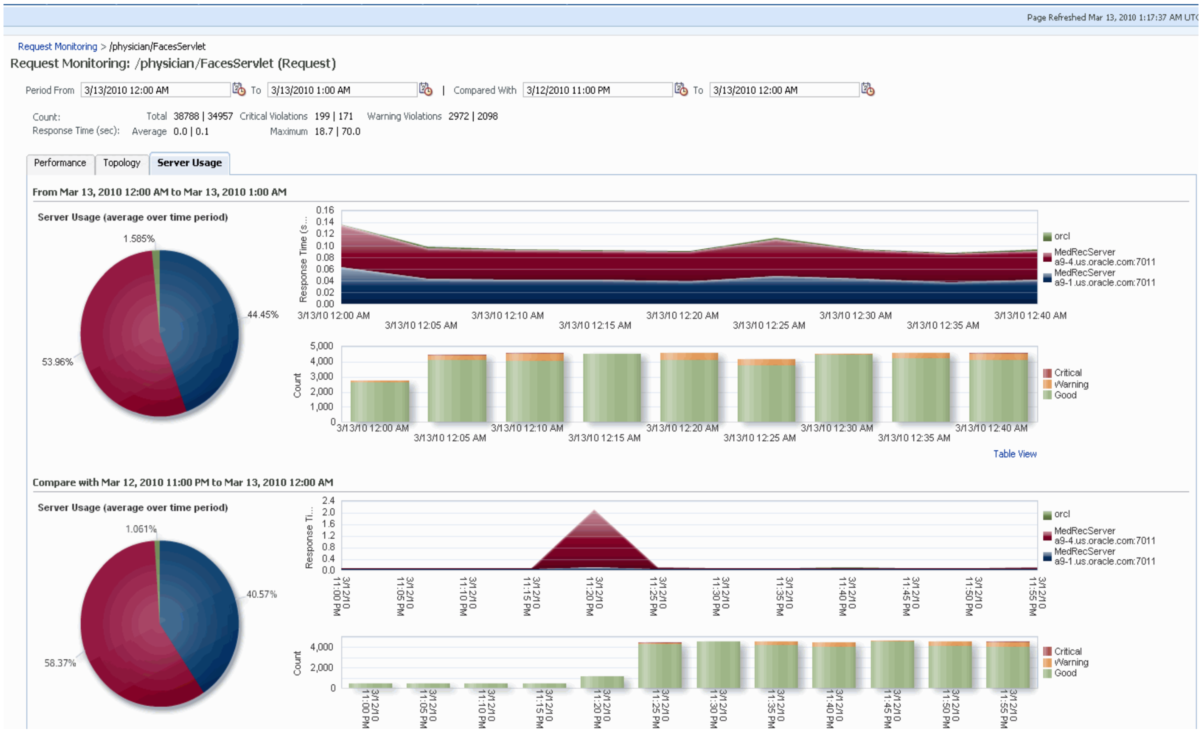
Response Time:0.0020 s
Count:945
Current Alerts:N/A
Availability (%):N/A
CPU Utilization:N/A
Memory Utilization:N/A

The topology chart shows the aggregate server level call paths of the request. The chart shows the calls made between the clients and the clusters or servers. Click on the icon on a cluster to view all the servers that are part of the cluster. Place the cursor on a cluster or server to view the following details:

- **Response Time**: The average response time taken by the server to process all the calls for the selected period.
- **Count**: The total number of calls that have been made to the server.
- **Current Alerts**: These alerts show the status of the server or cluster and indicate whether it is up or down, blacked out, or unreachable.

6. Click on the Server Usage tab. The following screen is displayed.

Figure 3–5 Server Usage Page



Page Refreshed Mar 13, 2010 1:17:37 AM UTC

Request Monitoring > /physician/FacesServlet

Request Monitoring: /physician/FacesServlet (Request)

Period From 3/13/2010 12:00 AM To 3/13/2010 1:00 AM | Compared With 3/12/2010 11:00 PM To 3/13/2010 12:00 AM

Count: Total 38788 | 34957 Critical Violations 199 | 171 Warning Violations 2972 | 2098

Response Time (sec): Average 0.0 | 0.1 Maximum 18.7 | 70.0

These charts show the workload distribution for the selected request in each server. The charts display the average of the percentage contribution of each server or cluster in the selected time period. You can see the workload distribution for good requests, requests that have violated the warning thresholds, and requests that have violated the critical thresholds.

3.3 Diagnosing Performance Problems

This section describes the methods and tools used to diagnose performance problems. You can:

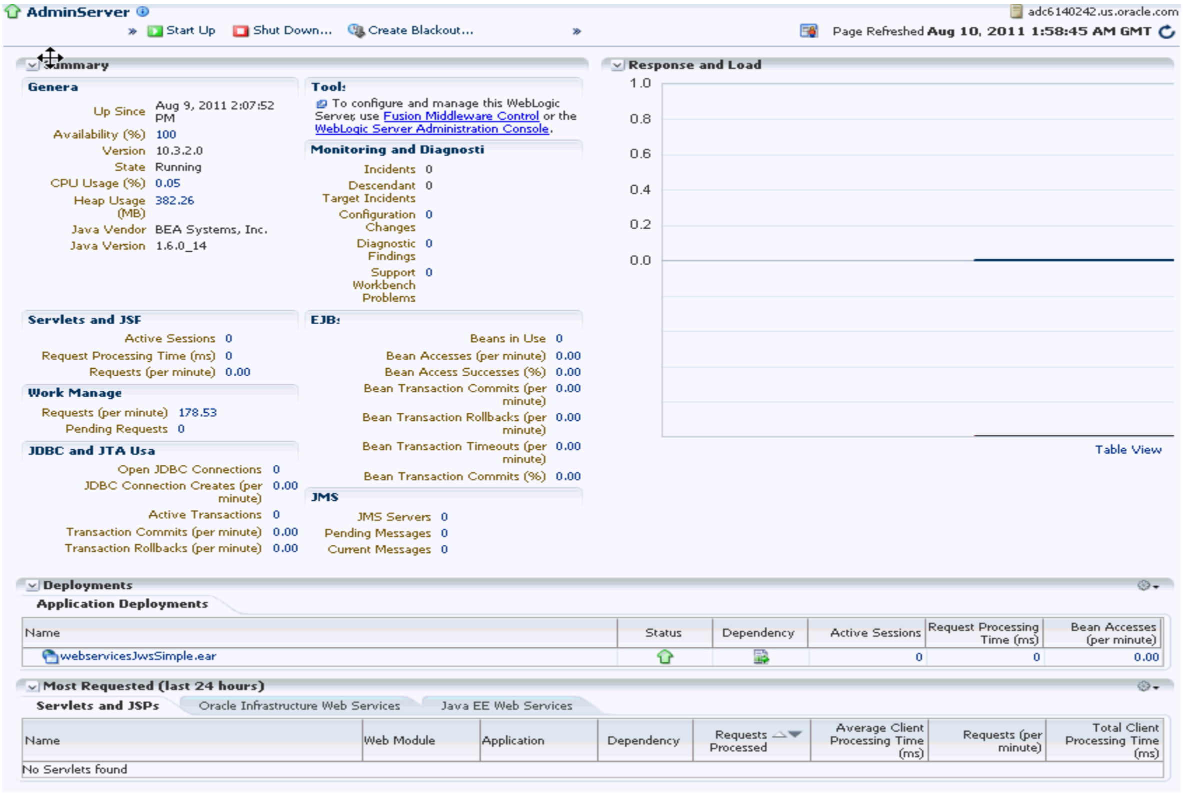
- View the list of most active Servlets and JSPs and identify the ones that are causing the bottleneck.
- Analyze Java EE and SOA applications using Application Dependency and Performance.
- Use Java Diagnostics to diagnose performance problems in production.

3.3.1 Using Home Pages to Diagnose Performance Issues

When you are troubleshooting performance problems, it can be helpful to know which servlets or JSPs are the most active. By viewing the Most Requested section on the WebLogic Server Home page, you can identify the most active Java servlets, JSPs, Web Services, or Java EE Services running on the WebLogic Server instance.

When you receive an alert notification, Enterprise Manager makes it easy for you to investigate the problem and take corrective actions wherever required. For example, notification of excessive CPU consumption by WebLogic Server may lead to investigation of the applications running on that instance. By using the Servlets and JSPs tab in the Most Requested section of the WebLogic Server Home page, you can quickly identify the highest volume or least responsive application. You can then drill down and diagnose application’s servlets, Java Server Pages (JSPs), or EJBs to identify the bottleneck.

Figure 3–6 WebLogic Server Home Page



Page Refreshed **Aug 10, 2011 1:58:45 AM GMT**

Genera

Up Since	Aug 9, 2011 2:07:52 PM
Availability (%)	100
Version	10.3.2.0
State	Running
CPU Usage (%)	0.05
Heap Usage (MB)	382.26
Java Vendor	BEA Systems, Inc.
Java Version	1.6.0_14

Tool:

To configure and manage this WebLogic Server, use Fusion Middleware Control or the WebLogic Server Administration Console.

Monitoring and Diagnosti

Incidents	0
Descendant Target Incidents	0
Configuration Changes	0
Diagnostic Findings	0
Support Workbench Problems	0

Servlets and JSF

Active Sessions	0
Request Processing Time (ms)	0
Requests (per minute)	0.00

Work Manage

Requests (per minute)	178.53
Pending Requests	0

JDBC and JTA Usa

Open JDBC Connections	0
JDBC Connection Creates (per minute)	0.00
Active Transactions	0
Transaction Commits (per minute)	0.00
Transaction Rollbacks (per minute)	0.00

EJB:

Beans in Use	0
Bean Accesses (per minute)	0.00
Bean Access Successes (%)	0.00
Bean Transaction Commits (per minute)	0.00
Bean Transaction Rollbacks (per minute)	0.00
Bean Transaction Timeouts (per minute)	0.00
Bean Transaction Commits (%)	0.00

JMS

JMS Servers	0
Pending Messages	0
Current Messages	0

Name	Status	Dependency	Active Sessions	Request Processing Time (ms)	Bean Accesses (per minute)
webservicesJwsSimple.ear	⇧		0	0	0.00

Name	Web Module	Application	Dependency	Requests Processed	Average Client Processing Time (ms)	Requests (per minute)	Total Client Processing Time (ms)
No Servlets found							

3.3.2 Middleware Diagnostics Advisor

The Middleware Diagnostics Advisor analyzes the entire stack and provides diagnostic findings by identifying the root cause of a problem. It correlates and analyzes the input and offers advice on how to resolve the problem. For example, it can help you identify that slow SQL statements or a JDBC connection pool is causing a performance bottleneck.

You can view the diagnostic findings for one or more servers in a WebLogic Domain if the Middleware Diagnostics Advisor has been enabled.

To view the diagnostic findings, navigate to the Home page of the WebLogic Domain and from the **WebLogic Domain** menu, select **Diagnostics**, then select **Middleware Diagnostics Advisor**. The Performance Findings chart shows a window in time for the last analysis period that contains one or more findings. For details on enabling the Middleware Diagnostics Advisor and viewing the performance findings, see the Enterprise Manager Online Help.

3.3.3 Diagnostics Snapshots

A diagnostic snapshot consists of all the necessary data to diagnose an issue. The actual diagnostic snapshot data depends on what targets are included in generating the diagnostic snapshot. It also provides a collective snapshot of both JVM and WebLogic Server diagnostics and log data that can be exported or imported into other Cloud Control systems for analysis at a later date. This allows administrators to determine the root cause of problems and ensure that they do not occur again. These snapshots supplement the Fusion Middleware Support Workbench feature.

A diagnostic snapshot can be generated in the context of an Enterprise Manager target such as a Fusion Middleware Farm. If the diagnostic snapshot needs to be created in the context of multiple farms, then this can be done by generating the diagnostic snapshot in the context of a group target that includes multiple Fusion Middleware farms, or you can begin from one Fusion Middleware farm and subsequently add targets from other Fusion Middleware Farms.When generating the diagnostic snapshot, you can name the diagnostic snapshot, select the targets that should be used for generating the diagnostic snapshot, select the duration during which the data will be collected for the snapshot and also select an option to either import the generated diagnostic snapshot data into the same Enterprise Manager instance or export the generated diagnostic snapshot data into single or multiple files that can then be imported back into another Enterprise Manager instance (or the same Enterprise Manager instance) later.

3.4 Administering Middleware Targets

Enterprise Manager allows you to monitor multiple domains and provides configuration management, diagnostics, automation, and historical performance analysis. From Enterprise Manager, you can drill down to Oracle Fusion Middleware Control or Oracle WebLogic Administration Console to monitor and administer your Oracle Fusion Middleware environment

- Oracle Fusion Middleware Control: Fusion Middleware Control is a Web browser-based, graphical user interface that you can use to monitor and administer a farm. Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for the farm, domain, servers, components, and applications. With Fusion Middleware Control, you can perform various tasks like managing the SOA environment, deploying ADF applications, managing Fusion Middleware components, etc.
- Oracle WebLogic Server Administration Console: Oracle WebLogic Server Administration Console is a Web browser-based, graphical user interface that you use to manage a WebLogic Server domain. It is accessible from any supported Web browser with network access to the Administration Server. With the WebLogic Server Administration Console, you can perform various tasks like managing the WebLogic Server, managing data sources, JMS resources, etc.

3.4.1 Process Control

Enterprise Manager allows you to perform process control tasks such as starting, stopping, or restarting Middleware targets. You can perform these tasks by selecting the Control option in the menu from the Home page of a target. You can also schedule a job to perform these operations. For example, for a WebLogic Server Domain, you can create a job to automatically start, stop, or restart the servers in the domain. You can also view details about the jobs that are scheduled, running, suspended, or the ones that have a problem.

3.5 Lifecycle Management

Enterprise Manager Cloud Control offers lifecycle management solutions that help you meet all lifecycle management challenges easily by automating time-consuming tasks related to discovery, initial provisioning and cloning, patching, configuration management, ongoing change management, and compliance management.

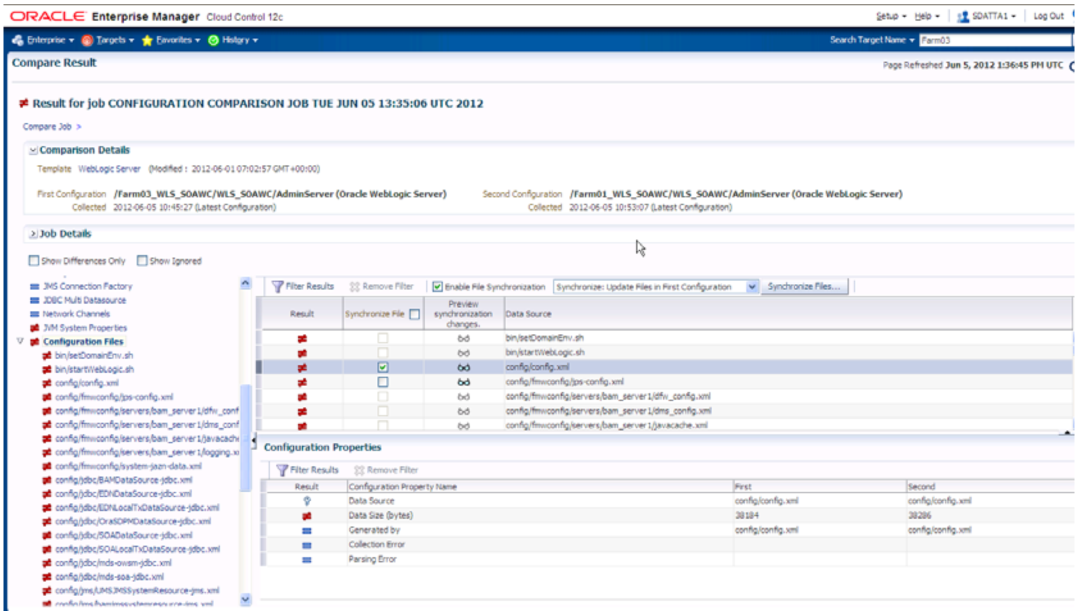
3.5.1 Managing Configurations

Enterprise Manager provides a suite of configuration management functions that can be performed on Middleware targets.

Oracle Management Agent collects configuration information about Oracle Fusion Middleware targets from their respective configuration files, and communicates this information over HTTP/HTTPS to Oracle Management Service, which stores it in the Management Repository. This information is periodically collected and updated while maintaining the audit of changes. Configuration files for Middleware targets are also collected. For example, for WebLogic Server, the `config.xml` configuration file is collected from the WebLogic Administration Server. The Enterprise Manager configuration management capabilities efficiently guide the users to desired configuration data in a particular component.

You can compare these configuration details and view the differences and similarities between the two instances of a Middleware target. You have the flexibility to compare two last collected configurations or two saved configuration files. You can also compare one configuration with multiple configurations or one configuration in the Management Repository with a saved configuration file. When a comparison operation results in differences that you do not require, you can synchronize the configurations so that one of configurations replaces the other one. This synchronization can be performed on demand based on the configuration files being compared.

Figure 3–7 Comparing Configuration Files


ORACLE Enterprise Manager Cloud Control 12c
Setup ▾ Help ▾ SDATTA1 ▾ Log Out
Enterprise ▾ Targets ▾ Favorites ▾ History ▾
Search Target Name ▾
Filter Results
Remove Filter
Synchronize Files...

Search Target Name: Farm03

Compare Result

Page Refreshed **Jun 5, 2012 1:36:45 PM UTC**

Result for job CONFIGURATION COMPARISON JOB TUE JUN 05 13:35:06 UTC 2012

Compare Job >

Comparison Details

Template WebLogic Server (Modified : 2012-06-01 07:02:57 GMT +00:00)

First Configuration **/Farm03_WLS_SOAWC/WLS_SOAWC/AdminServer (Oracle WebLogic Server)**
Collected 2012-06-05 10:45:27 (Latest Configuration)

Second Configuration **/Farm01_WLS_SOAWC/WLS_SOAWC/AdminServer (Oracle WebLogic Server)**
Collected 2012-06-05 10:53:07 (Latest Configuration)

Job Details

□ Show Differences Only □ Show Ignored

- JMS Connection Factory
- JDBC Multi Datasource
- Network Channels
- JVM System Properties
- **Configuration Files**
  - bin/setDomainEnv.sh
  - bin/startWebLogic.sh
  - config/config.xml
  - config/fmwconfig/jps-config.xml
  - config/fmwconfig/servers/bam_server1/dfw_conf
  - config/fmwconfig/servers/bam_server1/dms_conf
  - config/fmwconfig/servers/bam_server1/javacach
  - config/fmwconfig/servers/bam_server1/logging.x
  - config/fmwconfig/system-jazn-data.xml
  - config/jdbc/BAMDataSource-jdbc.xml
  - config/jdbc/EDNDataSource-jdbc.xml
  - config/jdbc/EDNLocalTxDataSource-jdbc.xml
  - config/jdbc/OraSDPMDataSource-jdbc.xml
  - config/jdbc/SOADataSource-jdbc.xml
  - config/jdbc/SOALocalTxDataSource-jdbc.xml
  - config/jdbc/mds-owsm-jdbc.xml
  - config/jdbc/mds-soa-jdbc.xml
  - config/jms/UMSJMSSystemResource-jms.xml

☑ Enable File Synchronization Synchronize: Update Files in First Configuration

Result	Synchronize File □	Preview synchronization changes.	Data Source
≠	□	👓	bin/setDomainEnv.sh
≠	□	👓	bin/startWebLogic.sh
≠	☑	👓	config/config.xml
≠	□	👓	config/fmwconfig/jps-config.xml
≠	□	👓	config/fmwconfig/servers/bam_server1/dfw_config.xml
≠	□	👓	config/fmwconfig/servers/bam_server1/dms_config.xml
≠	□	👓	config/fmwconfig/servers/bam_server1/javacache.xml

Configuration Properties

Result	Configuration Property Name	First	Second
	Data Source	config/config.xml	config/config.xml
≠	Data Size (bytes)	38184	38286
=	Generated by	config/config.xml	config/config.xml
=	Collection Error		
=	Parsing Error		

You can also compare configurations by using the default comparison templates. A comparison template is associated with a specific target type that determines the configuration item type and property that is to be compared. A template can specify rules or expressions that enable you parse comparison data and fine-tune comparisons. For example, you can specify rules that indicate which differences must trigger an alert and which differences must be ignored when the configuration is compared.

Using Enterprise Manager, you can search configurations across Middleware targets and find configuration anomalies - whether they are a mismatch of an install/patch version of Oracle Fusion Middleware software, or they are a mismatch of the software configuration data. You can perform more intelligent searches to identify all the components hosting a particular application or other resources. You can create and save more intelligent searches. For example, you can create a new search to retrieve all 10.3.5 WebLogic Server targets running on the Linux 64 bit platform that are using JDK 1.6.0_31.

In addition, for BPEL Process Manager targets, you can view the BPEL Processes, its different versions, and the suitcase files associated with each version. You can also compare the BPEL Process suitcase files of different versions and track the changes that were made to a version. shows you how the versions can be selected and compared. This allows you to identify the cause for improved or deteriorated performance due to a change in the BPEL Process suitcase file.

3.5.2 Compliance Management

Enterprise Manager Cloud Control offers the following compliance management solutions:

- The compliance results capability enables you to evaluate the compliance of Middleware targets and systems as they relate to your business best practices for configuration, security, and storage. In addition, compliance results provide advice of how to change configuration to bring your Middleware targets and systems into compliance.
- Using the compliance library, you can define, customize, and manage:
  - Compliance frameworks
  - Compliance standards
  - Compliance standard rules

  By using these self-defined entities, you can test your environment against the criteria defined for your company or regulatory bodies.

3.5.3 Patch Management

Patching is one of the critical phases of the software lifecycle that helps you maintain the software over a period of time and keep it updated with bug fixes and latest features offered by the software vendor. However, in today's world, with numerous software deployments across your enterprise, patching becomes very complex and virtually impossible to manage. Considering these challenges, Enterprise Manager Cloud Control provides an integrated My Oracle Support Patches and Updates functionality that not only simplifies the patch operation but also offers timely and easy access to patch and support information during the patch planning phase. This helps you utilize the wealth of information from My Oracle Support to implement the best possible patch rollout for your organization. Enterprise Manager Cloud Control introduces a new concept called Patch Plans that enables you to create a collection of patches you want to apply to one or more targets. Each target can have a separate group of patches. In addition, you can save the deployment options of a patch plan as a patch template, and have new patch plans created out of the patch template.

3.5.4 Provisioning

Rather than spend resources on manually installing and configuring Oracle Fusion Middleware software, administrators would rather spend time and money on more strategic initiatives. To help achieve this, Enterprise Manager has automated common provisioning operations such as cloning Oracle SOA Suite 12c and scaling out an Oracle WebLogic Domain. Making such critical datacenter operations easy, efficient and scalable results in lower operational risk and lower cost of ownership. To access these provisioning operations, navigate to the Patching and Provisioning page in Enterprise Manager and click **Middleware Provisioning** and select either of the following:

- **Fusion Middleware Provisioning**: You can automate the cloning of WebLogic Domains and / or Middleware Homes either from a reference installation or from a profile present in the software library.
- **Fusion Middleware Domain Scale Up**: You can automate the scaling up or scaling out of a domain or cluster by adding a new managed server to an existing cluster or by cloning a managed server.

For more details on using these procedures, see the *Enterprise Manager Lifecycle Management Guide*.

3.5.4.1 Cloning from Test to Production Environments

Typically, creating a new environment to support SOA applications entails several manual, error prone installation and configuration steps. With Oracle Enterprise Manager this can be accomplished with very little effort and time via a predefined, customizable deployment procedure. This deployment procedure clones an existing SOA Suite environment to a new set of hardware per a hierarchical series of steps. These predefined steps can be edited or disabled and new steps or custom scripts can be added to the deployment procedure to satisfy unique business needs.

The deployment procedure also supports secure host authentication using super user do (sudo) or pluggable authentication modules (PAM). While running the deployment procedure, administrators can specify configuration settings such as the domain name, credentials for the administration console, port values, and JDBC data resources. After the procedure completes, the newly created SOA environment is discovered and automatically added to the console for centralized management and monitoring.

3.5.4.2 Scaling Out Domains

To address growing business demands, modern data centers must augment and relocate resources quickly. Using Oracle Enterprise Manager, administrators can rapidly scale out a WebLogic Domain and Cluster with additional managed servers to accommodate an increase in application load.

3.5.4.3 Deploying / Undeploying Java EE Applications

You can deploy, undeploy, and redeploy Java EE applications (.war and .ear files) on a WebLogic Server. You can create a Java EE Application component in the Software Library and deploy multiple versions of an application, or roll-back to a previous version.

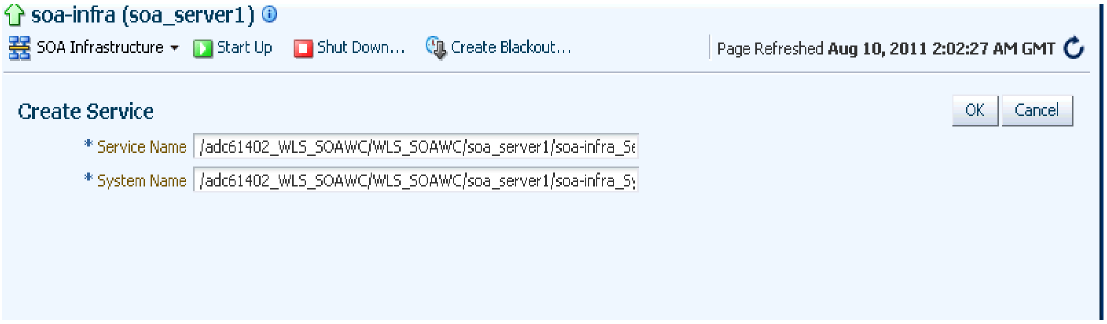
3.6 Managing Service Levels

Enterprise Manager allows you to create infrastructure services for Middleware targets such as Oracle BPEL Process Manager targets, Oracle Service Bus targets and Oracle SOA Composite and SOA Infrastructure instances.

An infrastructure service is a dependency service that is created to identify the infrastructure components on which the Middleware target depends. Here, the infrastructure components refer to hosts, databases, application servers, and so on that work together to host the Middleware target.

You can either create an infrastructure service with a new system or an existing system, or simply refresh an existing infrastructure service, if there is already one existing. By creating infrastructure services and systems, you can better manage your Middleware targets and also the components on which the Middleware targets depend.

Figure 3–8 Create Service for SOA Infrastructure



* Service Name /adc61402_WLS_SOAWC/WLS_SOAWC/soa_server1/soa-infra_Se

* System Name /adc61402_WLS_SOAWC/WLS_SOAWC/soa_server1/soa-infra_Sy

For example, once you create an infrastructure service for an Oracle SOA Infrastructure target, Enterprise Manager allows you to create an aggregate service for every process within that SOA Infrastructure target. An aggregate service is a logical grouping of services, in this case, infrastructure services and availability services. Aggregate Services give you a bird's-eye view of the services that have been created for the SOA Infrastructure target and helps you monitor their availability, performance, and usage. Service availability can be composed of both metrics on the underlying target and service test results from period synthetic transaction execution.

You can define service level (measure of service quality) for a service. A service level is defined as the percentage of time during business hours a service meets specified availability, performance and business criteria.

A Service Level specifies the percentage of time a service meets the performance and availability criteria as defined in the Service Level Rule. By default, a service is expected to meet the specified criteria 85% of the time during defined business hours. You may raise or lower this percentage level according to service expectations. A service level measures service quality using two parameters: Expected and Actual Service Levels.

- Expected Service Level: A Service Level specifies the percentage of time a service meets the performance and availability criteria as defined in the Service Level Rule. By default, a service is expected to meet the specified criteria 85% of the time during defined business hours. You may raise or lower this percentage level according to service expectations.
- Actual Service Level: The Actual Service Level defines the baseline criteria used to define service quality.

3.6.1 Service Dashboard

The Service Dashboard provides a consolidated view of the critical aspects of the service including the status, availability, type of service, performance, and the SLAs that have been enabled for this service. It also shows the performance and usage metrics for the service, status of the key components, and any system incidents.

You can view all the information related to the service on a single page and assess the health of the service. You can customize the dashboard by adding or removing regions according to your requirements and make these changes available to all the users.

You can also personalize the dashboard and make changes that are visible only to you and not to the other users.

3.7 Job System

You can use Enterprise Manager job system to schedule tasks you want to automate. You can schedule a job for a target by selecting the **Control** menu option on the Home page. For example, for an Oracle WebLogic Server Domain, you can create a job to automatically start, stop, or restart the servers in the domain. You can view details about the jobs that are scheduled, running, suspended, or the ones that have a problem. You can also use jobs to automate the execution of the WLST (WebLogic Scripting Tool) scripts. See the *Enterprise Manager Cloud Control Administrator's Guide* for more details on the Job System and its functionality.

3.7.1 Log File Rotation

Oracle Application Server components generate log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information.

However, the information recorded in log files is voluminous, thus making it difficult to track what update was made at what time. Also because of the huge quantity of information updated periodically, the log files grow in size and occupy more space on the system over a period of time. The only way to manage these log files is to manually archive the contents to another file and store them in a different location.

Considering these impediments, Enterprise Manager has been enhanced with a log rotation feature that helps you manage the logs of Oracle Application Server components more effectively. In particular, you can use Enterprise Manager to:

- Schedule a job that automatically rotates a log at the scheduled date and time
- Manage space on your system by storing the rotated log files in a different directory

Enterprise Manager allows you to view the logs of a particular Oracle Application Server component type and select the ones that need to be rotated. Note that a log rotation job can also be part of a multi-task job.

When a log rotation job is executed, Enterprise Manager automatically stops the component whose logs have to be rotated. After it is stopped, the content from its existing log file is moved to another file that is distinguished with the timestamp when it was actually rotated. The original log file is kept empty for new log details to be populated. Once this is done, Enterprise Manager restarts the component.

Note: The log rotation feature cannot be used with the WebLogic Server.

3.7.2 Log File Viewer

You can centrally search logs generated by WebLogic and Oracle Fusion Middleware across all Oracle Fusion Middleware components. You can perform structured log searches based on log properties such as time, severity, or Execution Context ID (ECID). You can also download log files or export messages to a file. This feature provides ready access to log files no matter where they are stored on the file system.

3.8 Topology Viewer

Enterprise Manager provides a Topology Viewer which is a graphical representation of routing relationships across targets, components and elements. You can easily determine how requests are routed across components. For example, you can see how requests are routed from Oracle Web Cache, to Oracle HTTP Server, to a Managed Server, to a data source.

The Topology Viewer provides the basic navigation applications, such as zoom, pan, and fit-to-contents. You can change the source of data being viewed, the layout mode, and the flow direction between objects. Filters allow you to alter global properties of the topology diagram, such as the visibility of link labels or altering the link style. It enables you to easily monitor your environment. You can see which entities are up and which are down. You can also print the topology or save it to a .gif file. For more details, see the Enterprise Manager Online Help.

3.9 Support Workbench

Enterprise Manager Support Workbench enables you to investigate, report, and, in some cases, repair problems (critical errors). You can gather first-failure diagnostic data, obtain a support request number, and upload diagnostic data to Oracle Support. The Support Workbench also recommends and provides easy access to Oracle advisors that help you repair SQL-related problems, data corruption problems, and more. You can use Support Workbench within Fusion Applications to:

- View a Fusion Aggregated Diagnostic Summary: Fusion applications are deployed across multiple systems, and incidents are therefore recorded in multiple Automatic Diagnostic Repository homes. You can get a quick summary of diagnostic data across all targets and Automatic Diagnostic Repository homes aggregated by the instance, product family, or cluster application.
- Execute Tests to Diagnose a Problem: You can link to Oracle Application Diagnostics Testing for a given Fusion Application, where you can execute additional tests to help diagnose the problem.
- Create a Package and Upload it to Oracle Support: You can create a package, add additional diagnostics and files, upload the package to Oracle Support, and then create a Service Request.

> **Note:** You need to discover and promote the Fusion Database targets before you can use Enterprise Manager Support Workbench for the Fusion Repository target.

4 Testing Application Load and Performance

This chapter describes how you can perform load and performance testing of applications with real-world production workloads using the Application Replay feature of Enterprise Manager. With Application Replay you can capture application workloads on production systems, and then replay them against test systems while maintaining the precise timing, concurrency, and transaction order of the workload.

This chapter covers the following:

4.1 Introduction to Application Replay

Application Replay enables realistic testing of planned changes to any part of the application stack from application server down to disk, by re-creating the production workload on a test system. Using Application Replay, you can capture a workload on the production system and replay it on a test system with the exact timing, concurrency, and transaction characteristics of the original workload. This enables you to fully assess the impact of the change, including undesired results, new contention points, or plan regressions. In addition, extensive analysis and reporting is provided to help identify any potential problems, such as new errors encountered and performance divergence. Types of changes that can be tested with Application Replay include application server upgrades, hardware updates, O/S changes, configuration changes, and so on. Capturing real-world production workload eliminates the need to develop simulation workloads or scripts, resulting in significant cost reduction and time savings. By using Application Replay, realistic testing of complex applications that previously took months using load simulation tools can now be completed in days. As a result, you can rapidly test planned changes and adopt new technologies with a higher degree of confidence and at lower risk.

4.2 Testing Against Real-World Application Workloads

Today's enterprise application deployments are highly complex and, therefore, challenging to manage. They comprise multiple tiers, such as Web servers, application servers, and databases, running on multiple hosts. Their software architecture combines multiple independent components, such as client-side user interfaces, business logic and data access mechanisms, in addition to stateful client-server protocols typically built over HTTP.

Due to the complexity of these structures, predicting the behavior of the entire stack in a production environment is extremely difficult. Given the complexity of these deployments, and the absence of system-wide verification techniques, effective testing is critical to ensuring successful deployment after an infrastructure change.

The Application Replay feature provides a testing structure that works by first capturing the entire workload relevant to an application (as generated by the application's Web interface) at the production site.

The captured application workload is then moved to the test environment, where the replay driver infrastructure on one or more hosts, reproduce the captured workload, preserving its original properties, such as concurrency and request timings.

Finally, extensive performance and correctness data from all layers of the stack is collected and reported. This enables you to compare the replay with the original captured workload. In this way, any issues resulting from infrastructure changes that occurred during the replay can be identified, and appropriate troubleshooting action undertaken to prevent them from occurring in production. Moreover, it increases your confidence in a successful deployment.

Benefits

The use of *real* workloads offers a number of significant advantages over testing techniques based on synthetic workloads. In particular:

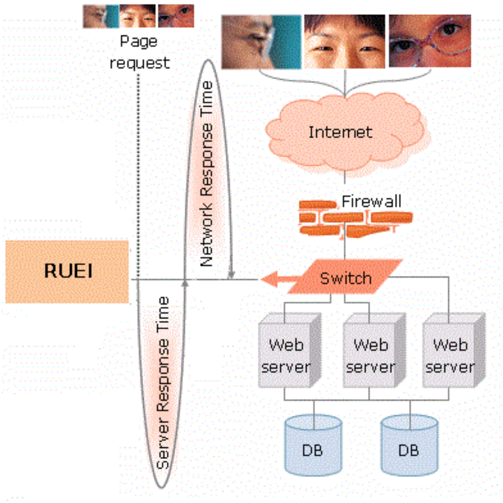
- It provides a system-wide perspective starting from the user's activity. This is in contrast to the traditional piecemeal testing of individual components that provides little information on their combined behavior and performance under a realistic workload.
- Rather than relying on pre-determined scenarios, the use of real workloads provides comprehensive testing, subjecting the system to real users operations. For Web applications, this not only means exploring all possible ways a user interacts with the system, but also all possible load conditions. This is necessary because systems behave quite differently under different workload characteristics (for example, the number of concurrent users).
- Far greater insight is obtained into possible errors. Test results include data for every layer of the stack, and these can be correlated across different layers. Besides performance, it also provides a means to verify correct execution, by checking for errors or unexpected server responses.

4.3 Capturing Application Workload Using RUEI

In order to capture Web application workloads, Application Replay uses Oracle Real User Experience Insight (RUEI). This is a Web-based utility to report on real-user traffic requested by, and generated from, your Web infrastructure. It measures the response times of pages and user flows at the most critical points in your network infrastructure. It provides you with powerful analysis of your network and business infrastructure, while an insightful diagnostics facility allows application managers and IT technical staff to perform root-cause analysis.

Typically, RUEI is installed before the Web servers, behind a firewall in the DMZ. The data collection method is based on Network Protocol Analysis (NPA) technology. This data collection method is shown in Figure 4–1.

Figure 4–1 How RUEI Collects Data



When an object is requested by a visitor, RUEI sees the request and starts measuring the time the Web server requires to present the visitor with the requested object. At this point, RUEI knows who requested the page (IP client), which object was requested, and from which server the object was requested (IP server).

When the Web server responds and sends the object to the visitor, RUEI sees that response, and stops timing the server response time. At this stage, RUEI can see whether there is a response from the server, whether this response is correct, how much time the Web server required to generate the requested object, and the size of the object.

RUEI is also able to see whether the object was completely received by the visitor, or if the visitor aborted the download (proof of delivery). Therefore, RUEI can determine the time it took for the object to traverse the Internet to the visitor, and can calculate the Internet throughput between the visitor and the server (connection speed of the visitor).

Further information about RUEI is available from the following location:

`http://www.oracle.com/us/products/enterprise-manager/index.html`

4.4 Synchronized vs. Non-Synchronized Replay

Application Replay supports the use of synchronization. This ensures that each replayed request sees exactly the same database state it saw during the capture process. In this way, the responses generated during capture and replay can be directly compared. In addition, data divergence between capture and replay is minimized. This is explained at greater length in "Analyzing Replay Results".

While the use of synchronized workload captures is clearly preferable, it is important to understand that:

- The use of the synchronization facility places additional requirements on your production and test environments. These are explained in "Using Synchronization".
- Non-synchronized workload captures require considerably less disk space. This is because information about the current database state does not need to be retained. Therefore, their use is recommended in test scenarios where differences between the responses generated in the capture and replay environments is not an issue. For example, in loading and stress testing.

4.5 Prerequisites and Considerations

This section describes the requirements that must be met, and the issues that should be considered, in order to use the Application Replay facility for workload capture and replay. It is *strongly* recommended that you carefully review this information before proceeding with a workload capture.

> **Important:** It is *strongly* recommended that you review the Oracle Support Web site to obtain up-to-date information about supported RUEI, application server, and database versions, as well as patches, configurations, known issues, and workarounds.

This section covers the following:

- Using RUEI to Capture Application Workloads
- Configuring Required User Privileges in Enterprise Manager
- Using Synchronization
- Setting up the Test System Database
- Restarting the Database and Application Stack
- Setting up the Capture Directory

4.5.1 Using RUEI to Capture Application Workloads

In order to use RUEI to capture your application workloads, you must ensure that:

- RUEI version 12.1 (or higher) has been configured to monitor the required applications. See the Oracle Support Web site (`http://www.oracle.com/support/contact.html`) for information about required releases and hot fixes. Information about deployment options and requirements is available from the *Oracle Real User Experience Insight Installation Guide*.
- You have a valid user name and password combination. If necessary, contact your RUEI Administrator. Note that the user account must have Security Officer permission. For further information about roles and permissions, see the *Oracle Real User Experience Insight User's Guide*.
- You have the URL used to access the RUEI installation. If necessary, contact your RUEI Administrator.
- The configured RUEI logging and masking policies are consistent with the use of Application Replay. This is described in the following section.

RUEI Configuration for Application Replay

As mentioned above, you must ensure that the RUEI logging and masking policies are configured as follows:

1. Select **Configuration**, **Security**, **Replay logging policy**, and click the Default replay action setting. This must be set to "Complete logging".
2. Select **Configuration**, **Security**, **Masking**, **URL prefix masking**, and click the Default masking action setting. This must be set to "Logging".
3. Note that if you expect a high level of traffic during the workload capture, it is recommended that you select **Configuration**, **Security**, **Collector data retention policy**, and ensure that sufficient storage has been assigned for each application that is planned to be captured.

For further information on these configuration procedures, see Chapter 13 "Managing Security-Related Information" of the *Oracle Real User Experience Insight User's Guide*.

4.5.2 Configuring Required User Privileges in Enterprise Manager

The following Enterprise Manager privileges must be assigned to users of the Application Replay facility:

- `ASREPLAY_VIEWER` in order to view captures, replays, and replay tasks.
- `ASREPLAY_OPERATOR` in order to create, modify, or submit captures, replays, and replay tasks.

In addition to the above, users must also be assigned the `PERFORM_OPERATION_ANYWHERE` privilege.

In order for database users to run the Application Replay facility with database capture, the following privileges must be granted to the user:

```
GRANT ADMINISTER ANY SQL TUNING SET TO asreplay;
GRANT EXECUTE ON DBMS_LOCK TO asreplay;
GRANT EXECUTE ON DBMS_WORKLOAD_CAPTURE TO asreplay;
GRANT EXECUTE ON DBMS_WORKLOAD_REPLAY TO asreplay;
GRANT CREATE SESSION TO asreplay;
GRANT CREATE ANY DIRECTORY TO asreplay;
GRANT SELECT_CATALOG_ROLE TO asreplay;
GRANT BECOME USER TO asreplay;
GRANT DROP ANY DIRECTORY to asreplay;
```

Note that in the above example, the database user is assumed to be called `asreplay`.

4.5.3 Using Synchronization

In order to make use of the synchronization functionality within Application Replay, you must ensure that:

- Oracle Fusion Middleware has been installed and configured. See the Oracle Support Web site (`http://www.oracle.com/support/contact.html`) for information about required releases and patch sets. For further information, see the *Oracle Fusion Middleware Installation Planning Guide* available at the following location:

  `http://download.oracle.com/docs/cd/E14571_01/install.1111/b32474/start.htm`

- Oracle Database has been installed and configured. See the Oracle Support Web site (`http://www.oracle.com/support/contact.html`) for information about required releases and patch sets. For further information, see the relevant *Database Installation Guide* available at the following location:

http://www.oracle.com/pls/db112/portal.portal_db?selected=11&frame=

- The database user needs to be assigned the privileges described in the *Oracle Database Security Guide* available at the following location:

  http://download.oracle.com/docs/cd/B19306_01/network.102/b14266/admusers.htm

- The user capturing and replaying application workloads has access to the host directory used to store capture files.
- The database user has `EXECUTE` privilege on `DBMS_WORKLOAD_REPLAY`.
- The files used during replay are on a shared file location that is accessible by all Replay Client systems using the same directory path. If synchronization has been enabled, this is also required for the appropriate database systems.
- It is recommended that the time zone and time settings for all host systems (such as RUEI, Oracle Fusion Middleware, and Oracle database) used during capture and replay should be the same to prevent clock skew.

Note that if you are using the database synchronization facility, be aware that only one database capture can be generated against a production environment at given time.

4.5.4 Setting up the Test System Database

Before a workload can be replayed, the logical state of the application data on the replay system should be similar to that of the capture system when replay begins. Therefore, you should have a strategy in place to restore the application server and database state on the test system. To restore the application server state, you should consult your application administrator. To restore the database state, consider using one of the following methods:

- Recovery Manager (RMAN) `DUPLICATE` command. For further information, see the *Oracle Database Backup and Recovery User's Guide*.
- Snapshot standby. For further information, see the *Oracle Data Guard Concepts and Administration*.
- Data Pump Import and Export. For further information, see the *Oracle Database Utilities*.

4.5.5 Restarting the Database and Application Stack

This step is not required, although restarting the database and application server components before starting capture ensures that ongoing and dependent transactions are allowed to be completed or rolled back before the capture begins. This minimizes divergence during replay, which is always desirable. On the other hand, if the database is not restarted before the capture begins, transactions that are in progress, or have yet to be committed, may not be fully captured in the workload. Therefore, ongoing transactions may not be replayed properly, because only the part of the transaction whose calls were captured will be replayed, resulting in data divergence.

Moreover, any subsequent transactions with dependencies on the incomplete transactions may also generate errors during replay. Before restarting the database and application server components, determine an appropriate time to shut down the production database before the workload capture when it is the least disruptive. For example, you may want to capture a workload that begins at 8:00 a.m. However, to avoid service interruption during normal business hours, you may not want to restart the database during this time. In this case, you should consider starting the workload capture at an earlier time, so that the database can be restarted at a time that is less disruptive. Once the application is restarted, it is important to start the capture before any user sessions reconnect and start issuing any workload. Otherwise, transactions performed by these user sessions will not be replayed properly in subsequent replays, because only the part of the transaction whose calls were executed *after* the workload capture is started will be replayed.

4.5.6 Setting up the Capture Directory

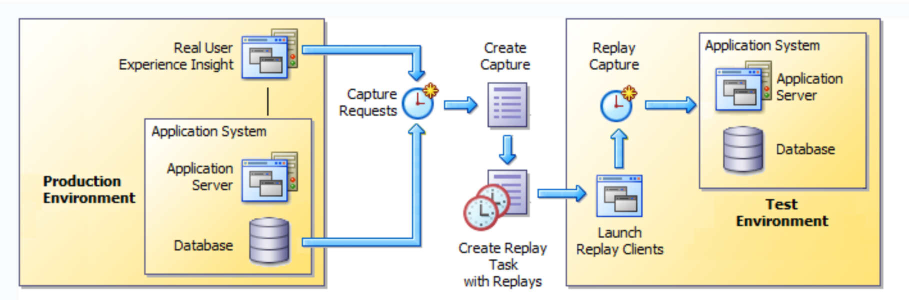
Determine and set up the directory where the captured workload will be stored. Before starting the capture, ensure that the directory is empty and has sufficient disk space to store the workload. If the directory runs out of disk space during a capture, the capture will be terminated.

To estimate the required disk space, it is recommended that you run a test capture on your workload for a short duration (typically, a few minutes), and then use this to extrapolate the space required for a full capture. To avoid potential performance issues, you should also ensure that the target replay directory is mounted on a separate file system.

4.6 Understanding the Capture and Replay Process

Figure 4–2 shows the architecture of the Application Replay facility.

Figure 4–2 Application Capture and Replay Architecture



The capture part of Application Replay operates within the context of a production environment. This deployment comprises Web and application servers, and a database. The Web-tier capture mechanism is provided by RUEI. It writes information about the monitored traffic to capture files. These contain HTTP requests, responses, and timings, along with all other data necessary to accurately reproduce the production workload against a test system. Once the capture is complete, the generated files constitute a complete representation of the entire production workload. In addition, the synchronization facility also captures the corresponding database workload for both capture analysis.

The replay part of Application Replay operates within the context of a test system. This comprises an application stack that runs the system configuration under test. One or more Replay Clients reproduce the captured workload, preserving its original properties, such as concurrency and request timings. Further, the Application Replay facility uses synchronization to ensure that each replayed request sees the exact application state it saw during capture so that the responses are directly comparable. Finally, it collects a wealth of performance and verification data from all layers of the stack, and allows you to compare the replay with the original capture upon which it is based.

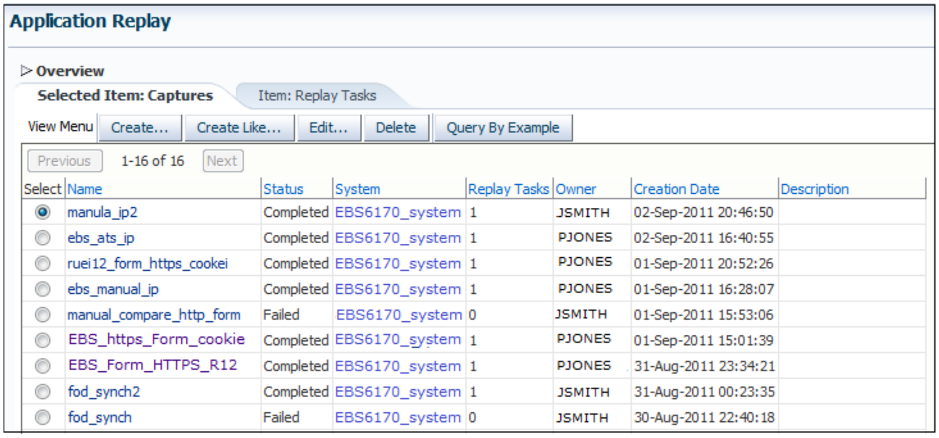
Depending on the volume and concurrency of the workload capture, it may be necessary to deploy multiple Replay Clients, each assigned a portion of the workload. Recommendations about required Replay Clients based on the captured workload are available when scheduling a replay.

4.7 Creating Application Workload Captures

To create an application workload capture:

1. From the **Enterprise** menu, select **Quality Management**, then **Application Replay**.
2. Click **Captures**. The currently defined captures are listed. An example is shown in Figure 4–3.

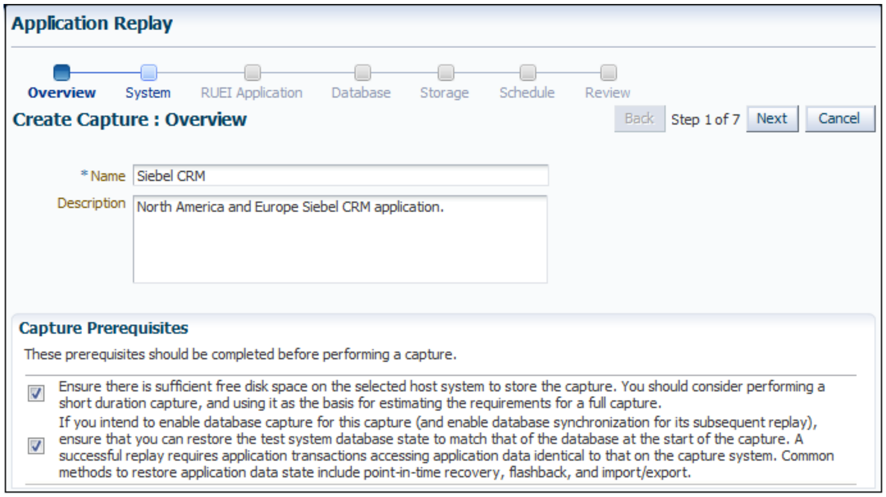
Figure 4–3 Application Replay Page



Select	Name	Status	System	Replay Tasks	Owner	Creation Date	Description
●	manula_ip2	Completed	EBS6170_system	1	JSMITH	02-Sep-2011 20:46:50	
○	ebs_ats_ip	Completed	EBS6170_system	1	PJONES	02-Sep-2011 16:40:55	
○	ruei12_form_https_cookei	Completed	EBS6170_system	1	PJONES	01-Sep-2011 20:52:26	
○	ebs_manual_ip	Completed	EBS6170_system	1	PJONES	01-Sep-2011 16:28:07	
○	manual_compare_http_form	Failed	EBS6170_system	0	JSMITH	01-Sep-2011 15:53:06	
○	EBS_https_Form_cookie	Completed	EBS6170_system	1	PJONES	01-Sep-2011 15:01:39	
○	EBS_Form_HTTPS_R12	Completed	EBS6170_system	1	PJONES	31-Aug-2011 23:34:21	
○	fod_synch2	Completed	EBS6170_system	1	JSMITH	31-Aug-2011 00:23:35	
○	fod_synch	Failed	EBS6170_system	0	JSMITH	30-Aug-2011 22:40:18	

3. Click **Create** or **Create Like**. The page shown in Figure 4–4 appears.

Figure 4–4 Create Capture (Overview) Page



Create Capture : Overview

* Name: Siebel CRM

Description: North America and Europe Siebel CRM application.

Capture Prerequisites

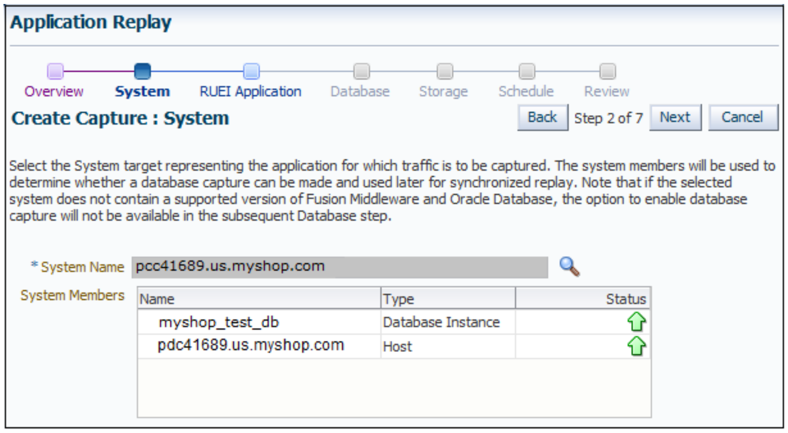
These prerequisites should be completed before performing a capture.

☑ Ensure there is sufficient free disk space on the selected host system to store the capture. You should consider performing a short duration capture, and using it as the basis for estimating the requirements for a full capture.

☑ If you intend to enable database capture for this capture (and enable database synchronization for its subsequent replay), ensure that you can restore the test system database state to match that of the database at the start of the capture. A successful replay requires application transactions accessing application data identical to that on the capture system. Common methods to restore application data state include point-in-time recovery, flashback, and import/export.

4. Specify a unique name for the new capture. Optionally, specify a brief description for the traffic to be captured. It is recommended that you include an indication of the purpose and scope of the capture. Carefully review the prerequisite information, and click the acknowledgement check boxes to indicate that they have been met. When ready, click **Next**. The page shown in Figure 4–5 appears.

Figure 4–5 Create Capture (System) Page



Create Capture : System

Step 2 of 7

Select the System target representing the application for which traffic is to be captured. The system members will be used to determine whether a database capture can be made and used later for synchronized replay. Note that if the selected system does not contain a supported version of Fusion Middleware and Oracle Database, the option to enable database capture will not be available in the subsequent Database step.

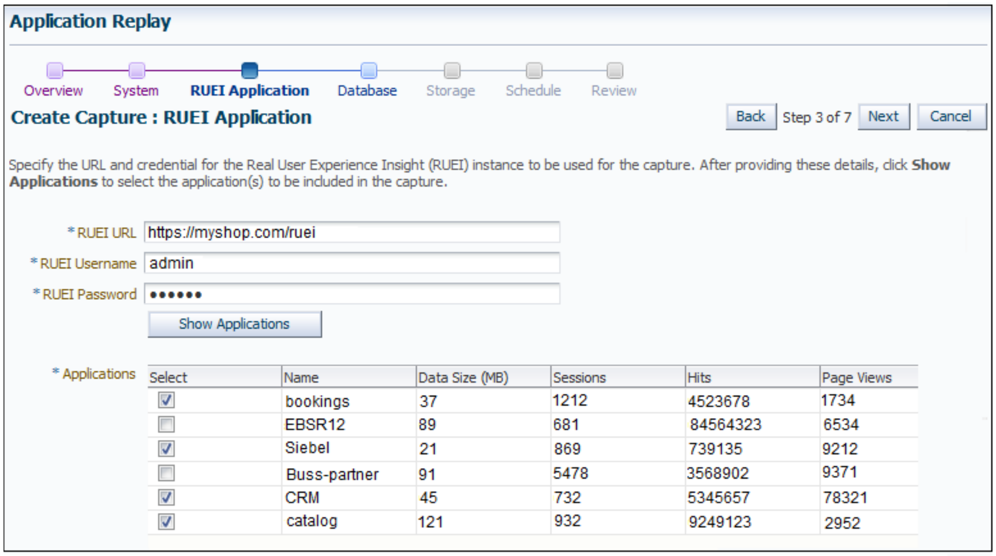
* System Name: pcc41689.us.myshop.com

System Members

Name	Type	Status
myshop_test_db	Database Instance	⇧
pdc41689.us.myshop.com	Host	⇧

5. Click the **Select System** icon, and select the target that represents the applications for which traffic is to be captured. It is recommended that you review the status of the selected component, and ensure that it will be available throughout the planned capture. Note that if the selected target does not include supported versions of Oracle Fusion Middleware and Oracle Database components, the Create Capture (Database) Page (shown in Figure 4–7) is not available, and is skipped. When ready, click **Next**. The page shown in Figure 4–6 appears.

Figure 4–6 Create Capture (RUEI Application) Page



Create Capture : RUEI Application

Step 3 of 7

Specify the URL and credential for the Real User Experience Insight (RUEI) instance to be used for the capture. After providing these details, click **Show Applications** to select the application(s) to be included in the capture.

* RUEI URL: https://myshop.com/ruei

* RUEI Username: admin

* RUEI Password: ••••••

* Applications

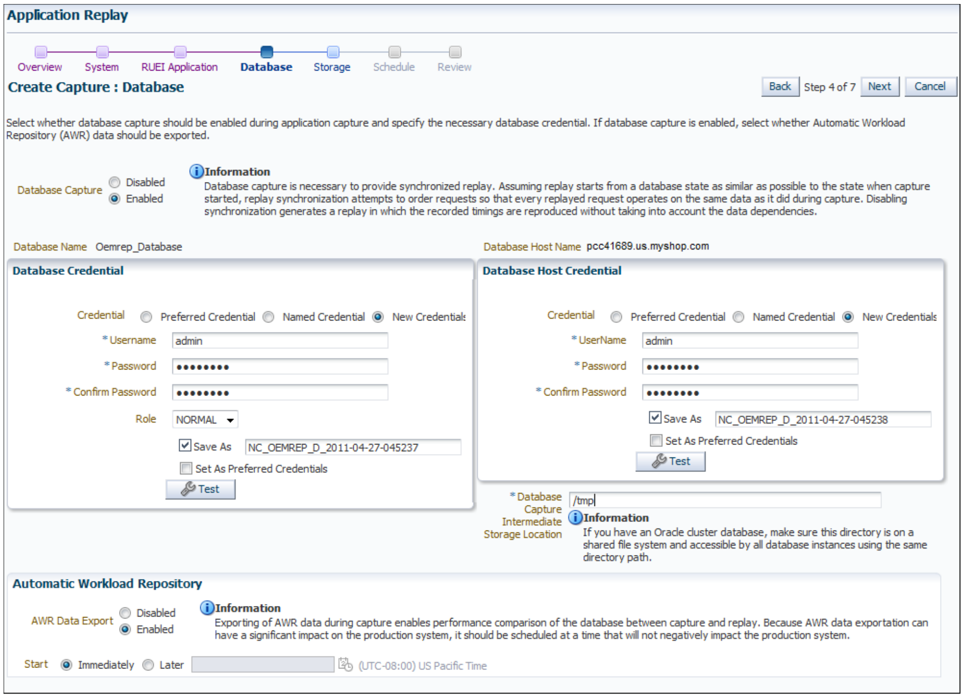
Select	Name	Data Size (MB)	Sessions	Hits	Page Views
☑	bookings	37	1212	4523678	1734
□	EBSR12	89	681	84564323	6534
☑	Siebel	21	869	739135	9212
□	Buss-partner	91	5478	3568902	9371
☑	CRM	45	732	5345657	78321
☑	catalog	121	932	9249123	2952

6. Specify the URL used to access the RUEI installation. This must be based on a secure (HTTPS) connection. Specify a valid user name and password combination.

The specified user must have Security Officer permission. If necessary, contact your RUEI Administrator for this information.

Click **Show Applications** to view the applications currently being monitored by the specified RUEI deployment. Note that you can use the traffic information available for each application to determine its suitability for capture. In particular, when selecting the applications to be included in the capture, you should ensure that the applications are running, and traffic volumes and error levels are within acceptable bounds. When ready, click **Next**. The page shown in Figure 4–7 appears.

Figure 4–7 Create Capture (Database) Page



Application Replay

Create Capture : Database

Select whether database capture should be enabled during application capture and specify the necessary database credential. If database capture is enabled, select whether Automatic Workload Repository (AWR) data should be exported.

Database Capture ○ Disabled ● Enabled

Information
Database capture is necessary to provide synchronized replay. Assuming replay starts from a database state as similar as possible to the state when capture started, replay synchronization attempts to order requests so that every replayed request operates on the same data as it did during capture. Disabling synchronization generates a replay in which the recorded timings are reproduced without taking into account the data dependencies.

Database Name Oemrep_Database

Database Host Name pcc41689.us.myshop.com

Database Credential

Credential ○ Preferred Credential ○ Named Credential ● New Credentials
* Username admin
* Password ••••••••
* Confirm Password ••••••••
Role NORMAL
☑ Save As NC_OEMREP_D_2011-04-27-045237
□ Set As Preferred Credentials

Database Host Credential

Credential ○ Preferred Credential ○ Named Credential ● New Credentials
* UserName admin
* Password ••••••••
* Confirm Password ••••••••
☑ Save As NC_OEMREP_D_2011-04-27-045238
□ Set As Preferred Credentials

* Database Capture Intermediate Storage Location /tmp

Information
If you have an Oracle cluster database, make sure this directory is on a shared file system and accessible by all database instances using the same directory path.

Automatic Workload Repository

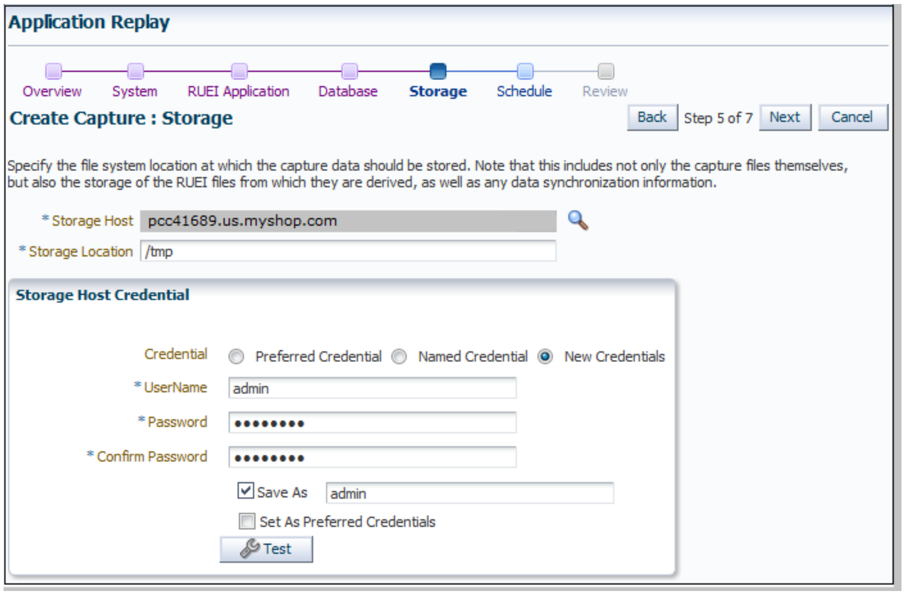
AWR Data Export ○ Disabled ● Enabled

Information
Exporting of AWR data during capture enables performance comparison of the database between capture and replay. Because AWR data exportation can have a significant impact on the production system, it should be scheduled at a time that will not negatively impact the production system.

Start ● Immediately ○ Later (UTC-08:00) US Pacific Time

7. Specify whether database capture should be enabled during application capture. This is required for synchronized replay. If enabled, specify the necessary database and host credentials, the file system location on the database host system used for intermediate capture storage, and whether Automatic Workload Repository (AWR) data should be exported. Note that if AWR export is enabled, you need to specify when exporting should begin. By default, it is performed immediately after capture is completed. When ready, click **Next**. The page shown in Figure 4–8 appears.

Figure 4–8 Create Capture (Storage) Page



Create Capture : Storage

Specify the file system location at which the capture data should be stored. Note that this includes not only the capture files themselves, but also the storage of the RUEI files from which they are derived, as well as any data synchronization information.

* Storage Host: pcc41689.us.myshop.com

* Storage Location: /tmp

Storage Host Credential

Credential: ○ Preferred Credential ○ Named Credential ● New Credentials

* UserName: admin

* Password: ••••••••

* Confirm Password: ••••••••

☑ Save As: admin

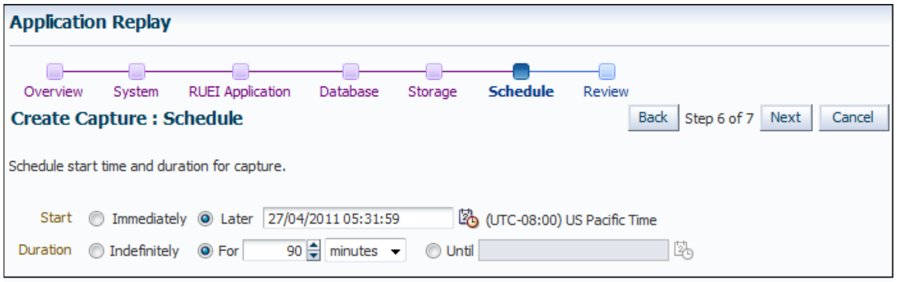
□ Set As Preferred Credentials

8. Specify the host and file system location where the capture data should be stored. Note that this includes not only the capture files themselves, but also the storage of the RUEI files from which they are derived, as well as any data synchronization information.

> **Important:** Capture files can require large amounts of disk space. Therefore, it is recommended that you perform a short capture, and then use that as the basis for calculating the required disk space for the planned capture. In addition, be aware that the generated capture files are in a proprietary format, and should *not* be modified.

Click the **Select Target** icon. A new window opens that allows you to view the available targets. Click a target to select it. Note that only one host target can be selected. You can use the **Target Type** menu to restrict the listing of targets to specific types. Note that it is also recommended that you review the status of the selected targets, and ensure that they will be available throughout the planned capture. Specify the credentials of the selected storage host. When ready, click **Next**. The page shown in Figure 4–9 appears.

Figure 4–9 Create Capture (Schedule) Page



Create Capture : Schedule

Schedule start time and duration for capture.

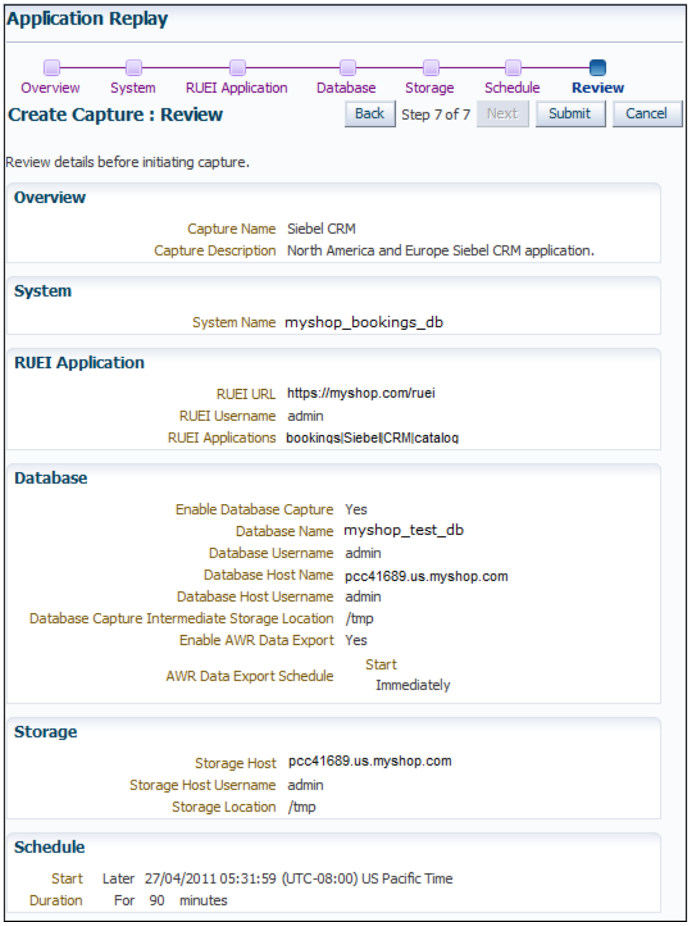
Start: ○ Immediately ● Later 27/04/2011 05:31:59 (UTC-08:00) US Pacific Time

Duration: ○ Indefinitely ● For 90 minutes ○ Until

9. Specify the start and stop times for the planned capture. By default, capture starts immediately. Note that, by default, the capture will run for the next 15 minutes. It is *strongly* recommended that you carefully consider the capture's duration and, if scheduled to run indefinitely, regularly review the capture process to prevent the creation of excessively large capture files. When ready, click **Next**. The page shown in Figure 4–10 appears.

> **Important:** If the capture is configured to run indefinitely, it must be stopped manually from the Capture Page. It is *strongly* recommended you regularly check the size of the created capture to prevent running out of storage space.

Figure 4–10 Create Capture (Review) Page



Create Capture : Review

Review details before initiating capture.

Overview

Capture Name: Siebel CRM
Capture Description: North America and Europe Siebel CRM application.

System

System Name: myshop_bookings_db

RUEI Application

RUEI URL: https://myshop.com/ruei
RUEI Username: admin
RUEI Applications: bookings|Siebel|CRM|catalog

Database

Enable Database Capture: Yes
Database Name: myshop_test_db
Database Username: admin
Database Host Name: pcc41689.us.myshop.com
Database Host Username: admin
Database Capture Intermediate Storage Location: /tmp
Enable AWR Data Export: Yes
AWR Data Export Schedule: Start Immediately

Storage

Storage Host: pcc41689.us.myshop.com
Storage Host Username: admin
Storage Location: /tmp

Schedule

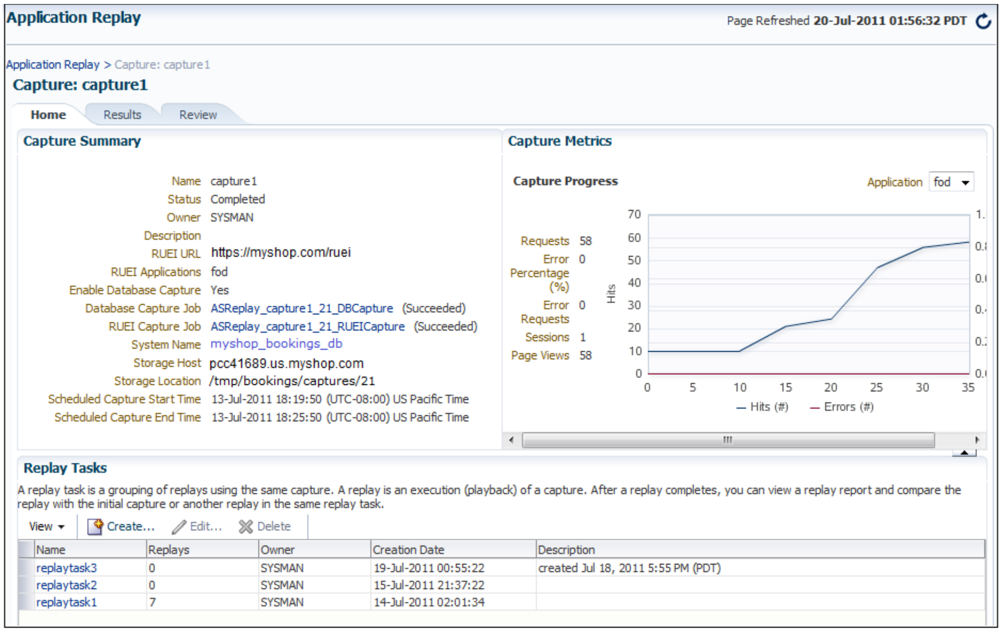
Start: Later 27/04/2011 05:31:59 (UTC-08:00) US Pacific Time
Duration: For 90 minutes

10. Review the planned capture's properties before launching it. If necessary, use the **Back** and **Next** buttons to amend the capture's properties. When ready to launch the new capture, click **Submit**.

4.8 Monitoring the Capture Process

Once a capture has been started, you can monitor the capture process to ensure that the intended traffic is being correctly captured, and that the application system is working under normal conditions. An example of a capture progress report is shown in Figure 4–11.

Figure 4–11 Capture Page



Capture: capture1

Capture Summary

Name capture1
Status Completed
Owner SYSMAN
Description
RUEI URL https://myshop.com/ruei
RUEI Applications fod
Enable Database Capture Yes
Database Capture Job ASReplay_capture1_21_DBCapture (Succeeded)
RUEI Capture Job ASReplay_capture1_21_RUEICapture (Succeeded)
System Name myshop_bookings_db
Storage Host pcc41689.us.myshop.com
Storage Location /tmp/bookings/captures/21
Scheduled Capture Start Time 13-Jul-2011 18:19:50 (UTC-08:00) US Pacific Time
Scheduled Capture End Time 13-Jul-2011 18:25:50 (UTC-08:00) US Pacific Time

Requests 58
Error Percentage (%) 0
Error Requests 0
Sessions 1
Page Views 58

Replay Tasks

A replay task is a grouping of replays using the same capture. A replay is an execution (playback) of a capture. After a replay completes, you can view a replay report and compare the replay with the initial capture or another replay in the same replay task.

Name	Replays	Owner	Creation Date	Description
replaytask3	0	SYSMAN	19-Jul-2011 00:55:22	created Jul 18, 2011 5:55 PM (PDT)
replaytask2	0	SYSMAN	15-Jul-2011 21:37:22	
replaytask1	7	SYSMAN	14-Jul-2011 02:01:34	

Be aware that there is a lead time of appropriately 10 minutes after the start of a capture before progress information about it becomes available. This is available from the Application Replay page (Figure 4–3). In either case, the characteristics of the capture are detailed in terms of its volume, performance, and errors. In this way, you can assess the quality of the capture, and its usefulness for testing purposes.

Note that the number of requests monitored during the capture process is particularly useful for assessing the capture's progress. In the event of an unusually high level of errors, you can use the Job page (available by clicking the RUEI Capture Job setting) to drill-down into specific errors.

4.9 Replaying Application Workload Captures

You can replay a workload capture against a test system. Besides issuing identical HTTP requests, the replay mechanism also mimics the characteristics of the capture in terms of concurrency and timing. This section provides information about the following parts of the replay process:

- Preparing to Replay Workload Captures
- Understanding Replays and Replay Tasks
- Resolving References to External Systems
- Remapping URLs
- Substituting Sensitive Data
- Replaying Workload Captures
- Analyzing Replay Results

4.9.1 Preparing to Replay Workload Captures

Proper planning of the workload replay ensures that the replay will be accurate. Replaying a workload capture requires the following steps:

- Ensure that the application data state on the test system is logically equivalent to that of the capture system at the start time of workload capture. This is described in "Setting up the Test System Database".
- All references to external systems have been resolved. This is explained in "Resolving References to External Systems".

4.9.2 Understanding Replays and Replay Tasks

It is important to understand that a replay is an execution (playback) of a workload capture. A replay task is a group of replays based on the same capture. After a replay is completed, you can view a replay report and compare the replay with the initial capture, or create another replay within the same replay task. Typically, the replays within a replay task perform the same purposes. For example, a database or host system configuration with multiple parameter changes.

It is recommended that replays are grouped into the same replay task in order to facilitate comparison. For example, those that relate to the testing of the same database upgrade patch.

4.9.3 Resolving References to External Systems

A captured workload may contain references to external systems, such as database links or external tables. It is critical that you reconfigure these external interactions to avoid impacting other production systems during replay. Typical external references that need to be resolved before replaying a workload are shown in Table 4–1.

Table 4–1 References to External Systems

Type	Description
Database links	Typically, it is not desirable for the replay system to interact with other databases. Therefore, you should reconfigure all database links to point to an appropriate database that contains the data needed for replay.
External tables	All external files specified using directory objects referenced by external tables need to be available to the database and application server during replay. The content of these files should be the same as during capture, and the filenames and directory objects used to define external tables should also be valid.
Directory objects	You should reconfigure any references to directories on the production system by appropriately redefining the directory objects present in the replay system after restoring the database.
URLs	URLs/URIs that are stored in the database and application server need to be configured so that Web services accessed during the capture will point to the appropriate URLs during replay. If the workload refers to URLs that are stored in the production system, you should isolate the test system network during replay.
E-mails	To avoid resending E-mail notifications during replay, any E-mail server accessible to the replay system should be configured to ignore requests for outgoing E-mails.

Important: To avoid impacting other production systems during replay, it is *strongly* recommended that you run the replay within an isolated private network that does not have access to the production environment hosts.

4.9.4 Remapping URLs

URLs in the workload capture files need to be remapped to different values before replay within the test environment. For example, the Web application URL in every request needs to be remapped to that of the test system.

Note that wildcard characters are not supported within remapped URLs. All required domain and port numbers must be fully specified.

4.9.5 Substituting Sensitive Data

The RUEI installation monitoring your network traffic can be configured to omit the logging of sensitive information. This is called *masking*, and prevents passwords and other sensitive information from being recorded on disk. Further information on the use of this facility is available from the *Oracle Real User Experience Insight User's Guide*.

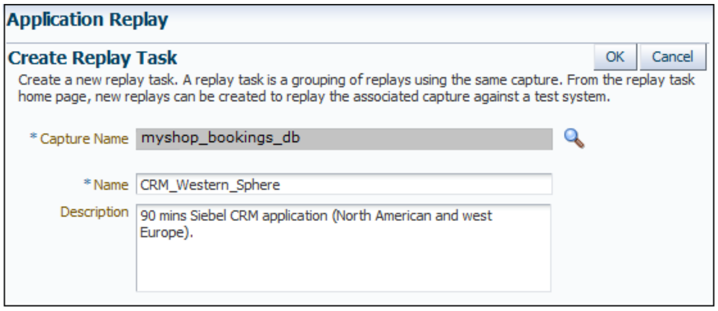
It is important to understand that Application Replay only supports the substitution of one value for each masked field. For example, if an application logon password field is masked, you will need to set up one common alternative logon password for all user accounts in the test system.

4.9.6 Replaying Workload Captures

To replay a workload capture using Enterprise Manager:

1. From the **Enterprise** menu, select **Quality Management**, then **Application Replay**. The page shown in Figure 4–3 appears.
2. From the **Replay Tasks** section, click **Create** or **Create Like**. The page shown in Figure 4–12 appears.

Figure 4–12 Create Replay Task Page



Application Replay

Create Replay Task

Create a new replay task. A replay task is a grouping of replays using the same capture. From the replay task home page, new replays can be created to replay the associated capture against a test system.

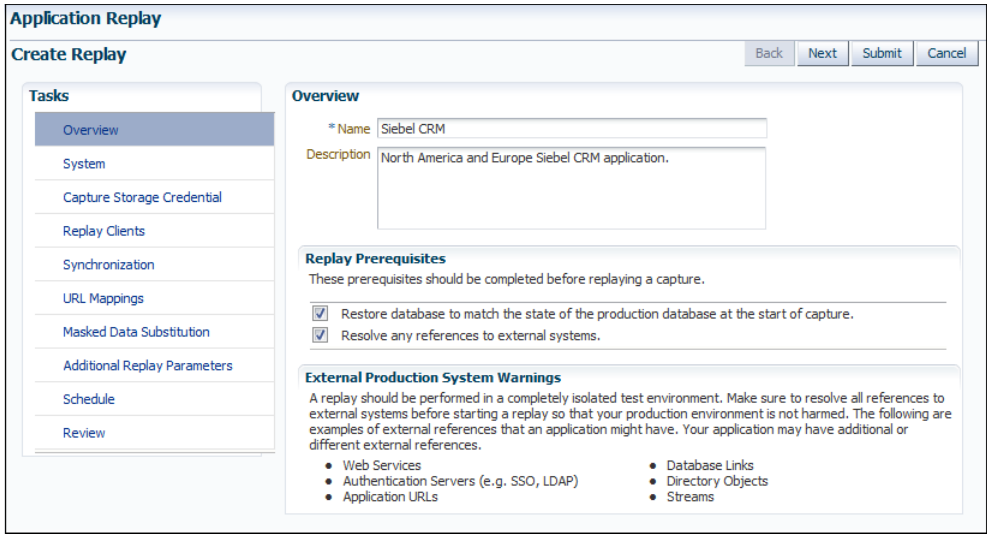
* Capture Name: myshop_bookings_db

* Name: CRM_Western_Sphere

Description: 90 mins Siebel CRM application (North American and west Europe).

3. Click the **Select Capture** icon. A new window opens that allows you to select the capture upon which the replay task should be based. Specify a unique name for the new replay task. Optionally, specify a brief description. It is recommended that you include an indication of the replay task's purpose and scope. When ready, click **OK**. You are returned to the page shown in Figure 4–3.
4. Click the newly created replay task. The page shown in Figure 4–13 appears.

Figure 4–13 Create Replay (Overview) Page



Overview

* Name: Siebel CRM

Description: North America and Europe Siebel CRM application.

Replay Prerequisites

These prerequisites should be completed before replaying a capture.

☑ Restore database to match the state of the production database at the start of capture.

☑ Resolve any references to external systems.

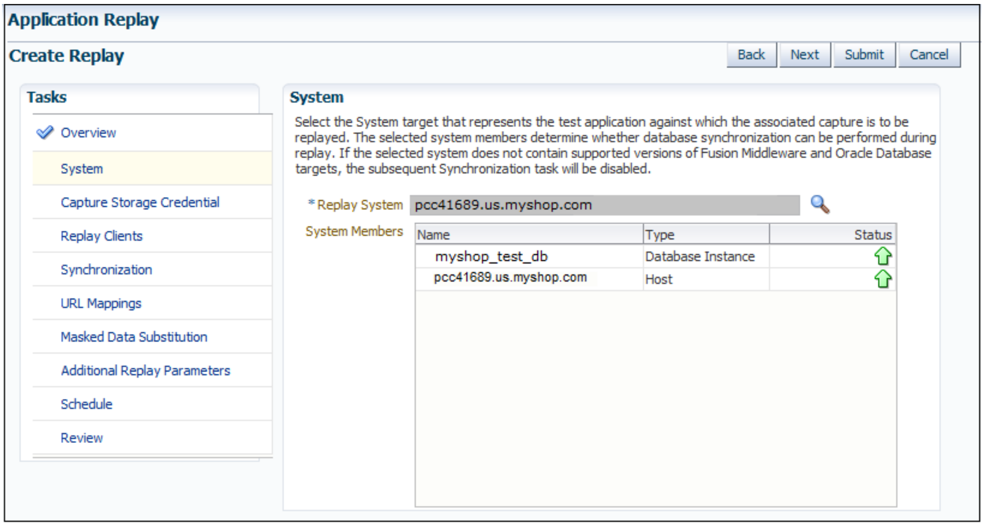
External Production System Warnings

A replay should be performed in a completely isolated test environment. Make sure to resolve all references to external systems before starting a replay so that your production environment is not harmed. The following are examples of external references that an application might have. Your application may have additional or different external references.

- Web Services
- Authentication Servers (e.g. SSO, LDAP)
- Application URLs
- Database Links
- Directory Objects
- Streams

5. Specify a name for the replay. It must be unique among the selected replay task. Optionally, specify a brief description for the traffic to be replayed. It is recommended that you include an indication of the purpose and scope of the replay. Carefully review the perquisite information, and click the acknowledgement check boxes to indicate that they have been met. When ready, click **System**. The page shown in Figure 4–14 appears.

Figure 4–14 Create Replay (System) Page



System

Select the System target that represents the test application against which the associated capture is to be replayed. The selected system members determine whether database synchronization can be performed during replay. If the selected system does not contain supported versions of Fusion Middleware and Oracle Database targets, the subsequent Synchronization task will be disabled.

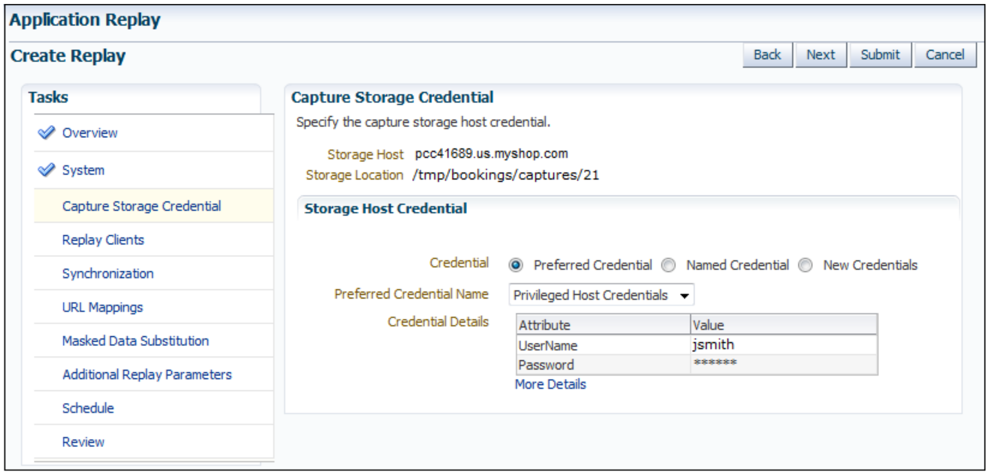
* Replay System: pcc41689.us.myshop.com

System Members

Name	Type	Status
myshop_test_db	Database Instance	⇧
pcc41689.us.myshop.com	Host	⇧

6. Click the **Select System** icon, and select the targets that represent the test environment against which the capture should be replayed. It is recommended that you review the status of the selected components, and ensure that they will be available throughout the planned replay. When ready, click **Capture Storage Credential**. The page shown in Figure 4–15 appears.

Figure 4–15 Create Replay (Capture Storage Credential) Page



Capture Storage Credential

Specify the capture storage host credential.

Storage Host pcc41689.us.myshop.com

Storage Location /tmp/bookings/captures/21

Storage Host Credential

Credential ● Preferred Credential ○ Named Credential ○ New Credentials

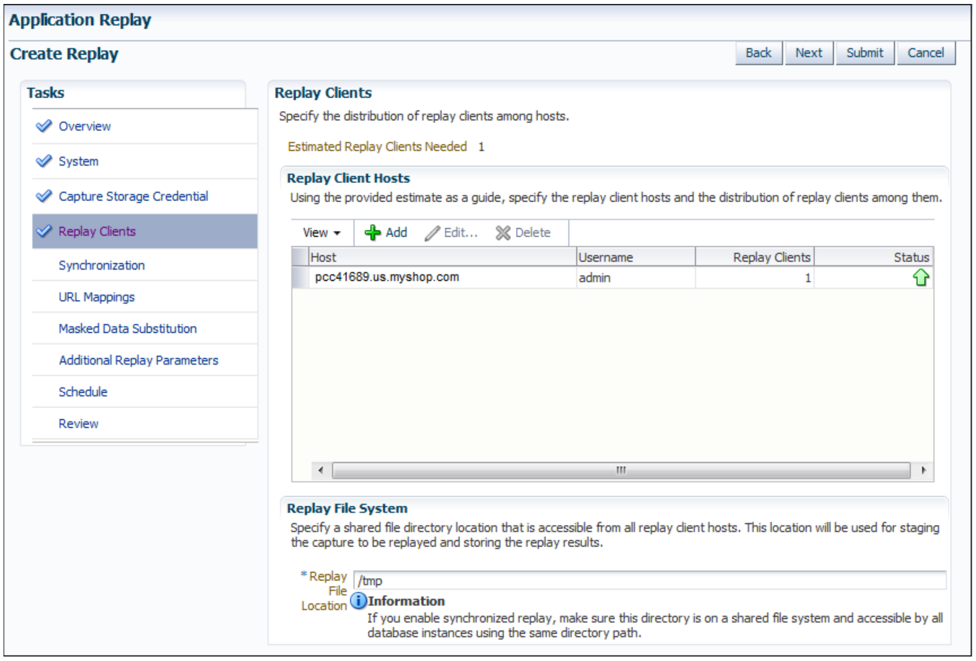
Preferred Credential Name: Privileged Host Credentials

Credential Details

Attribute	Value
UserName	jsmith
Password	******

7. Specify the credentials of the selected storage host. When ready, click **Replay Clients**. The page shown in Figure 4–16 appears.

Figure 4–16 Create Replay (Replay Clients) Page



Replay Clients

Specify the distribution of replay clients among hosts.

Estimated Replay Clients Needed 1

Replay Client Hosts

Using the provided estimate as a guide, specify the replay client hosts and the distribution of replay clients among them.

Host	Username	Replay Clients	Status
pcc41689.us.myshop.com	admin	1	⇧

Replay File System

Specify a shared file directory location that is accessible from all replay client hosts. This location will be used for staging the capture to be replayed and storing the replay results.

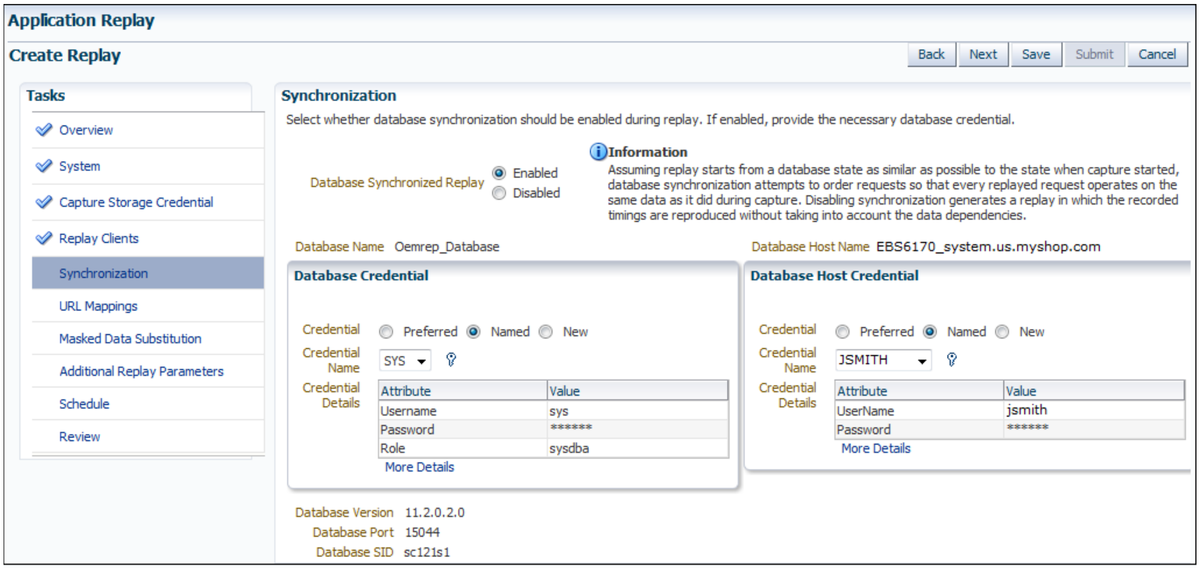
* Replay File Location /tmp

Information

If you enable synchronized replay, make sure this directory is on a shared file system and accessible by all database instances using the same directory path.

8. Specify the Replay Clients that will be used to generate the workload on the test system. Note that the provided estimate should be used as a basis for scaling the planned replay. Specify the file system location to be used for storing the capture files and replay results. This location must be on a shared file system and accessible from the Replay Client hosts and database hosts (if synchronization is enabled) via exactly the same file directory path. When ready, click **Synchronization**. The page shown in Figure 4–17 appears.

Figure 4–17 Create Replay (Synchronization) Page



Synchronization

Select whether database synchronization should be enabled during replay. If enabled, provide the necessary database credential.

Database Synchronized Replay ● Enabled ○ Disabled

Information
Assuming replay starts from a database state as similar as possible to the state when capture started, database synchronization attempts to order requests so that every replayed request operates on the same data as it did during capture. Disabling synchronization generates a replay in which the recorded timings are reproduced without taking into account the data dependencies.

Database Name Oemrep_Database

Database Host Name EBS6170_system.us.myshop.com

Database Credential

Credential ○ Preferred ● Named ○ New

Credential Name SYS

Credential Details

Attribute	Value
Username	sys
Password	******
Role	sysdba

More Details

Database Host Credential

Credential ○ Preferred ● Named ○ New

Credential Name JSMITH

Credential Details

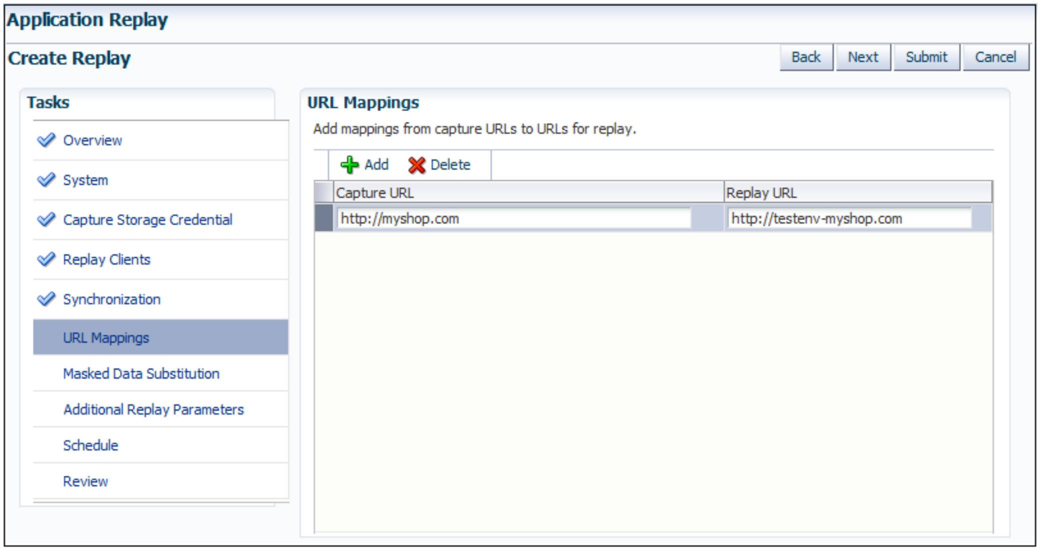
Attribute	Value
UserName	jsmith
Password	******

More Details

Database Version 11.2.0.2.0
Database Port 15044
Database SID sc121s1

9. Specify whether database synchronization should be enabled during the replay. Note that, if enabled, you will need to provide relevant database and host credentials. When ready, click **URL Mappings**. The page shown in Figure 4–18 appears.

Figure 4–18 Create Replay (URL Mappings) Page



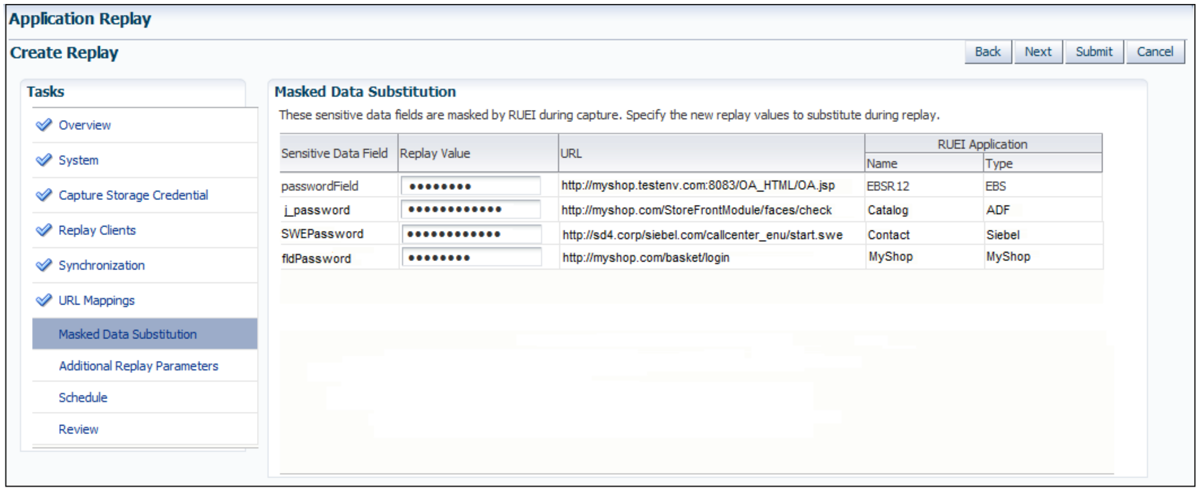
URL Mappings

Add mappings from capture URLs to URLs for replay.

Capture URL	Replay URL
http://myshop.com	http://testenv-myshop.com

10. Specify the URL mappings that should be used during the replay. That is, how the URLs encountered during capture should be substituted when replayed within the test environment. When ready, click **Masked Data Substitution**. The page shown in Figure 4–19 appears.

Figure 4–19 Create Replay (Masked Data Substitution) Page



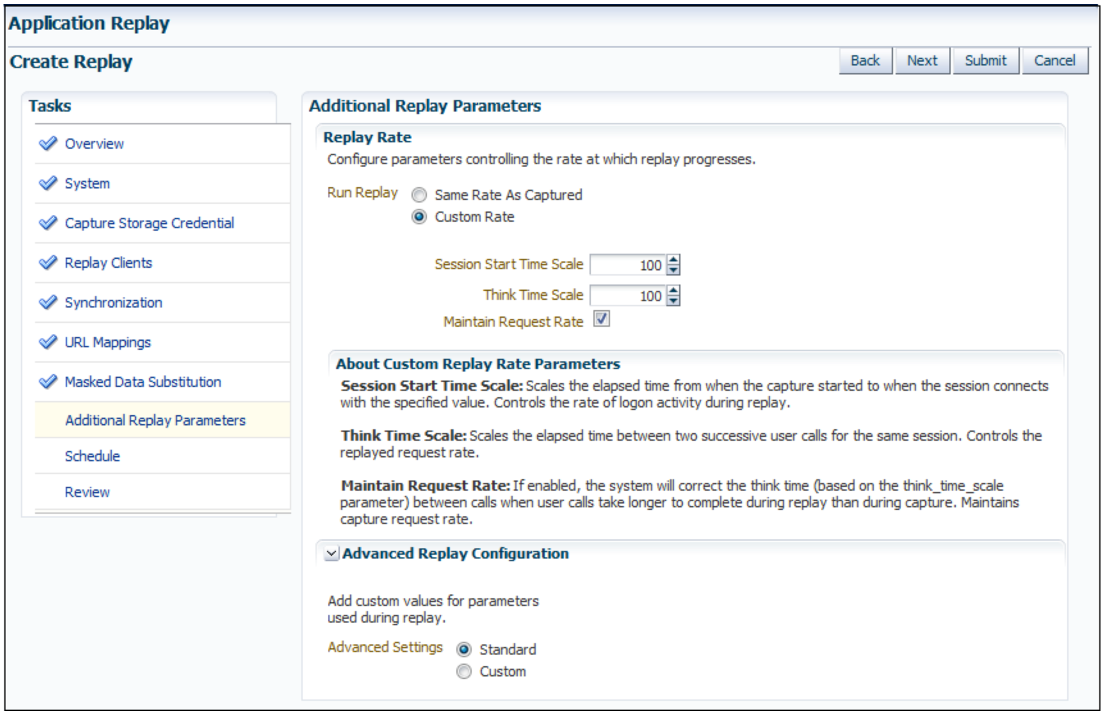
Masked Data Substitution

These sensitive data fields are masked by RUEI during capture. Specify the new replay values to substitute during replay.

Sensitive Data Field	Replay Value	URL	RUEI Application	
			Name	Type
passwordField	••••••••	http://myshop.testenv.com:8083/OA_HTML/OA.jsp	EBSR12	EBS
j_password	••••••••••••	http://myshop.com/StoreFrontModule/faces/check	Catalog	ADF
SWEPassword	••••••••••••	http://sd4.corp/siebel.com/callcenter_enu/start.swe	Contact	Siebel
fldPassword	••••••••	http://myshop.com/basket/login	MyShop	MyShop

11. RUEI can be configured to omit the logging of sensitive information (such as passwords, credit card details, and so on) from being recorded on disk. Because the values of these fields are not recorded, they need to be explicitly specified for replay. When ready, click **Additional Replay Parameters**. The page shown in Figure 4–20 appears.

Figure 4–20 Create Replay (Additional Replay Parameters) Page



Additional Replay Parameters

Replay Rate

Configure parameters controlling the rate at which replay progresses.

Run Replay ○ Same Rate As Captured
● Custom Rate

Session Start Time Scale 100

Think Time Scale 100

Maintain Request Rate ☑

About Custom Replay Rate Parameters

Session Start Time Scale: Scales the elapsed time from when the capture started to when the session connects with the specified value. Controls the rate of logon activity during replay.

Think Time Scale: Scales the elapsed time between two successive user calls for the same session. Controls the replayed request rate.

Maintain Request Rate: If enabled, the system will correct the think time (based on the think_time_scale parameter) between calls when user calls take longer to complete during replay than during capture. Maintains capture request rate.

Advanced Replay Configuration

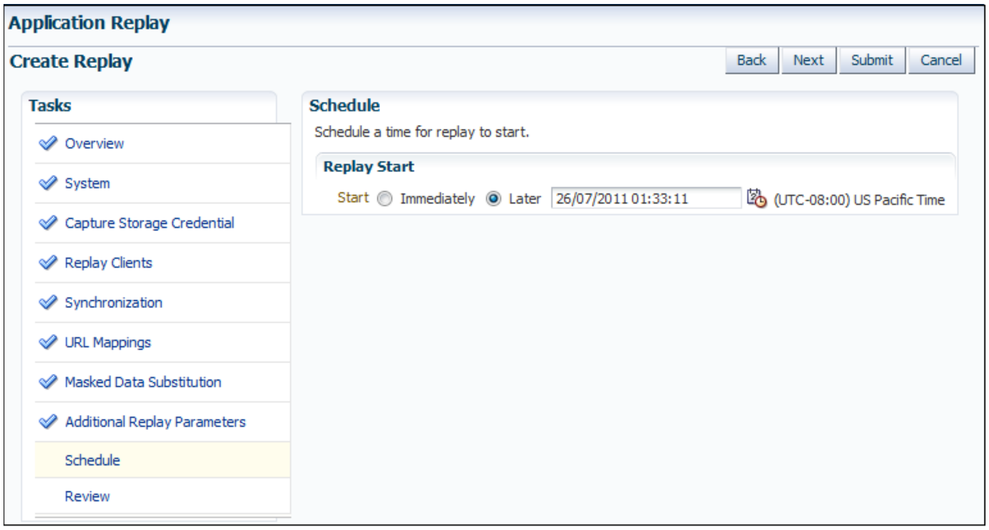
Add custom values for parameters used during replay.

Advanced Settings ● Standard
○ Custom

12. Specify whether the replay should progress at the same rate as in the original capture or at an alternative rate. In the case of the latter, you need to specify the appropriate session start time scale, think time scale, and whether the request rate should be maintained at the original rate. Expand the **Advanced Replay Parameters** section to specify whether the standard advanced settings should have

their standard values or custom values. When ready, click **Schedule**. The page shown in Figure 4–21 appears.

Figure 4–21 Create Replay (Schedule) Page



Schedule

Schedule a time for replay to start.

Replay Start

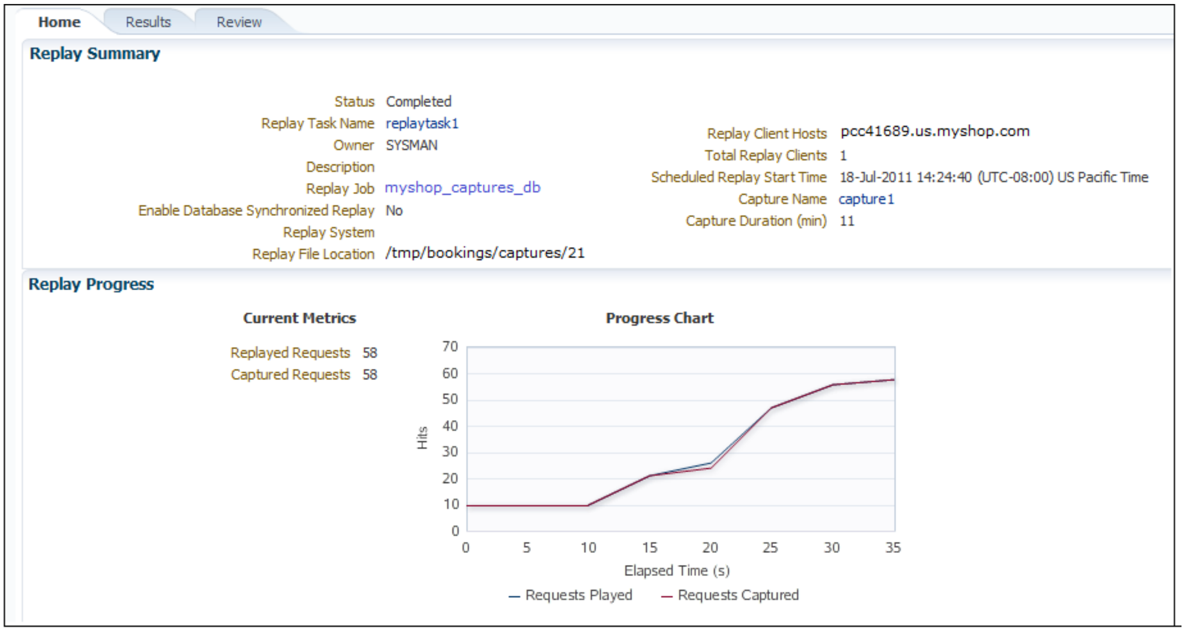
Start ○ Immediately ● Later 26/07/2011 01:33:11 (UTC-08:00) US Pacific Time

13. Specify when the replay should start. When ready, click **Review**.
14. A summary of the planned replay is displayed. If necessary, use the **Back** and **Next** buttons to move between sections. When ready, click **Submit** to launch the replay.

4.9.7 Analyzing Replay Results

Detailed information about a selected replay is available by clicking it within the Application Replay Page. An example of a replay overview is shown in Figure 4–22.

Figure 4–22 Example Replay Summary



Replay Summary

Status Completed
Replay Task Name replaytask1
Owner SYSMAN
Description
Replay Job myshop_captures_db
Enable Database Synchronized Replay No
Replay System
Replay File Location /tmp/bookings/captures/21

Replay Client Hosts pcc41689.us.myshop.com
Total Replay Clients 1
Scheduled Replay Start Time 18-Jul-2011 14:24:40 (UTC-08:00) US Pacific Time
Capture Name capture1
Capture Duration (min) 11

Replay Progress

Current Metrics

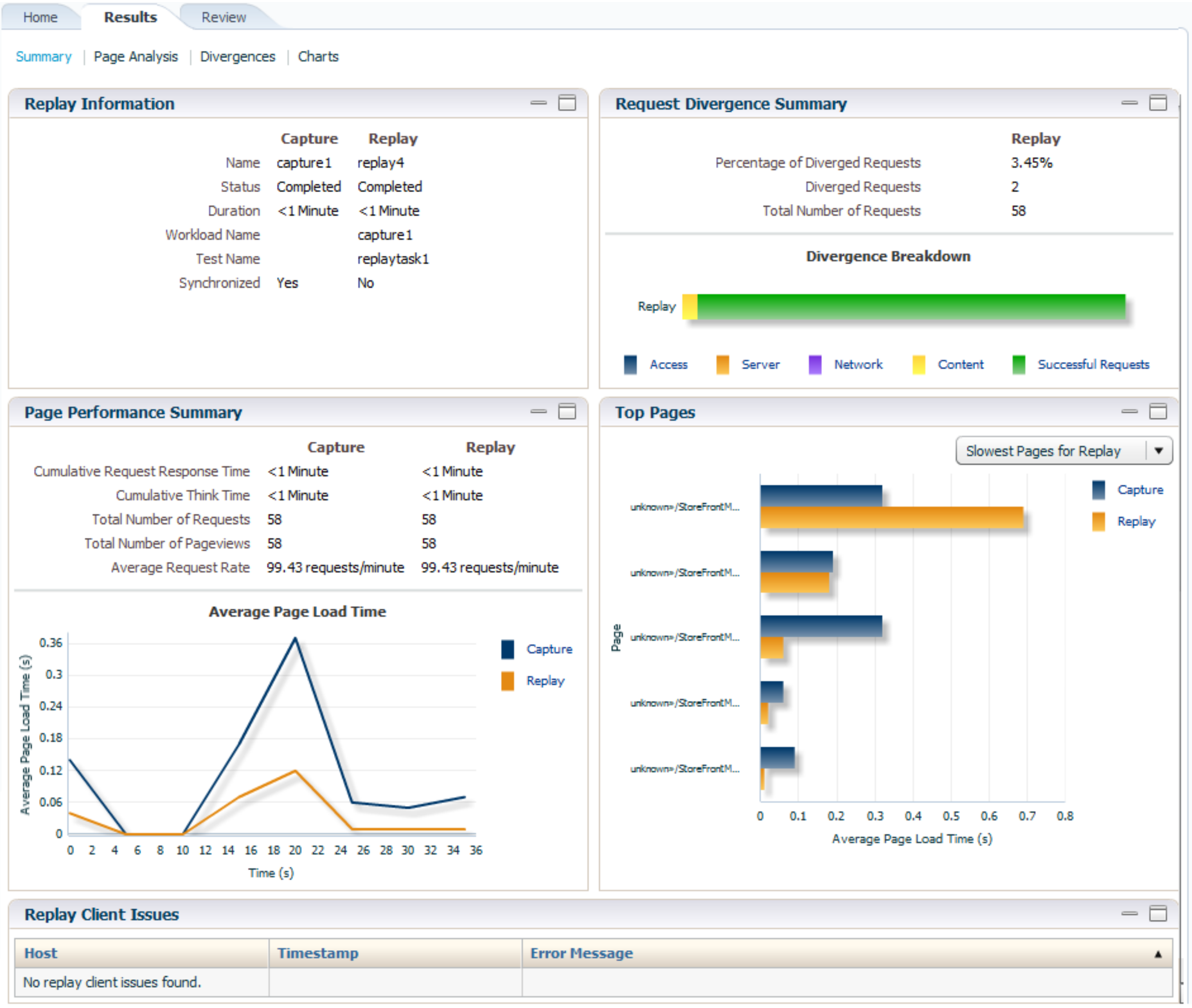
Replayed Requests 58
Captured Requests 58

It consists of three parts:

- **Home**: provides a overview of the replay, its associated replay task, and the capture upon which it based. The progress of the replay, and a comparison with the original capture, is also provided.
- **Results**: provides more detailed information about the request divergence. This includes a comparison of page performance during the original capture and the replay, and the application pages that experienced the highest level of divergence. An example is shown in Figure 4–23.

  Within this section, The **Page Analysis** section allows you to an analysis of each application page across selected metrics. The **Divergences** section allows you to view information restricted to specific divergence types (such as access, content, and so on). The **Charts** section allows you to view detailed replay information across specific metrics (such as average page load time).
- **Review**: provides information about the replay environment (such as the credentials, host, and replay clients), as well as the URL mappings and masked data substitutions used during the replay.

Figure 4–23 Example Replay Results Summary



Replay Information

	Capture	Replay
Name	capture1	replay4
Status	Completed	Completed
Duration	<1 Minute	<1 Minute
Workload Name		capture1
Test Name		replaytask1
Synchronized	Yes	No

Request Divergence Summary

	Replay
Percentage of Diverged Requests	3.45%
Diverged Requests	2
Total Number of Requests	58

Page Performance Summary

	Capture	Replay
Cumulative Request Response Time	<1 Minute	<1 Minute
Cumulative Think Time	<1 Minute	<1 Minute
Total Number of Requests	58	58
Total Number of Pageviews	58	58
Average Request Rate	99.43 requests/minute	99.43 requests/minute

Top Pages

Replay Client Issues

Host	Timestamp	Error Message ▲
No replay client issues found.		

4.10 Troubleshooting

This section provides guidance on dealing with the most common problems encountered when capturing and replaying workloads. In addition, it is recommended that you review the Oracle Support Web site for information about known issues and workarounds. It is available at the following location:

https://support.oracle.com

RUEI Installation

Ensure that the RUEI installation used to monitor the applications in the workload capture meets the following requirements:

- Check the Oracle Support Web site for information about supported versions and required hot fixes.
- RUEI has been configured to monitor the required applications. Information about deployment options and requirements is available from the *Oracle Real User Experience Insight Installation Guide*.

- You have a valid user name and password combination. If necessary, contact your RUEI Administrator. Note that the user account must have Security Officer permission. For further information about roles and permissions, see the *Oracle Real User Experience Insight User's Guide*.
- Full-Session Replay (FSR) has been enabled, and sufficient storage has been assigned, for each application that is planned to be captured. In addition, you should ensure that each application's data replay logging and masking settings are compatible with the use of FSR. For information, see the *Oracle Real User Experience Insight User's Guide*.
- Ensure that your Web server has been configured to use static SSL certificates. This is necessary because RUEI does not support dynamic SSL certificates.
- If your application make use of jumbo frames, increase the RUEI capture length from its default 2kb to 64kb by issuing the following command on the RUEI Reporter system as the `root` user:

  ```
  execsql config_set_profile_value wg System config CaptureLength replace 65536
  ```

Synchronization

If you are using synchronization replay, ensure that your capture and replay environments meet the requirements described in Section 4.5.3, "Using Synchronization".

Capture Checklist

In addition to the requirements indicated above, you should also ensure that:

- RUEI is correctly capturing all required traffic using the appropriate logging and masking policies. For information on verifying its configuration, see the *Oracle Real User Experience Insight User's Guide* available at the following location:

  `http://www.oracle.com/technetwork/documentation/realuserei-091455.html`

- The database host user ID belongs to the same group as the Enterprise Manager Agent user account.

Replay Checklist

In addition to the requirements indicated above, you should also ensure that:

- All required URLs have been correctly remapped, as described in Section 4.9.4, "Remapping URLs". Check whether the test system has been configured as HTTP or HTTPS, the domain name of the Web server, and the relevant port number. In addition, verify that the full domain name is specified in the URL, and not just the host name.
- It is *strongly* recommended that you do not replay a captured workload in a production environment.
- Ensure that you have provided a substitute value for all sensitive data fields that were masked during capture. This is described in Section 4.9.5, "Substituting Sensitive Data".

5 Monitoring Business Applications

This chapter describes how you can use Oracle Enterprise Manager to obtain Application Performance Management (APM) capabilities to maximize the performance and availability of your business-critical applications.

This is achieved through the creation and monitoring of business application targets. These are managed targets that provide an intuitive representation of the relationship between your applications and business transactions and the underlying IT infrastructure. The RUEI and BTM-monitored components that comprise these business applications provide information across the enterprise, and facilitate central monitoring of their structure, status, availability, dependencies, and performance. The registration and monitoring of their associated RUEI and BTM systems is also described.

The chapter covers the following:

5.1 The Oracle Approach to the APM Challenge

Organizations have increasingly come to understand that the elements that deliver value to them need to be managed in a business-driven (rather than application-centric) manner. In particular, this has emerged as a result of the following factors:

- The three biggest problems facing IT administrators are slow response times, users experiencing errors, and application availability. Moreover, most organizations only find out about these problems through end user complaints.
- The above issues are equally important to end users, and equally difficult for IT management to resolve. This applies to both package and custom applications.

- Application architectures have undergone a dramatic change from client-server deployments to n-tier, SOA, and composite architectures. As a result, traditional application monitoring is not suitable for these modern architectures.

The Oracle Enterprise Management Solution

To address the challenges outlined above, Oracle Enterprise Manager encompasses the following key aspects to managing application performance:

- A sub-optimal application can negatively impact not only the immediate business activities that users are trying to perform, but also the organization’s image and, ultimately, profitability. Therefore, IT operations must be managed from the end-user perspective.
- In order to understand why these problems occurred, it is necessary to manage the infrastructure that powers the applications, and analyze the processing of business transactions. Business transactions are often executed by arranging existing applications and infrastructure to implement business processes. Typically, they incorporate a wide variety of technologies, deployed across many platforms and organizational boundaries. However, despite the complexity of such processes, they must behave as single, seamless transactions from the business users’ perspective.
- Once a problem is isolated to a particular component, IT can perform in-depth diagnostics of that component. As numerous technologies are used in typical application environments, and each piece of technology presents its own idiosyncrasies, specialized tools built with in-depth knowledge of the component are needed to troubleshoot them. These tools are available for both Java and non-Java applications running on Oracle Database, as well as major packaged Oracle Applications such as Siebel CRM.
- Leveraging Oracle’s unparalleled expertise in Java technologies, Oracle Enterprise Manager provides deep diagnostics for any JVM within the application infrastructure providing immediate insight into actual thread stack or other common JVM issues.
- For applications running on Oracle Database, Oracle Enterprise Manager provides best-in-class diagnostics unavailability to other tools on the market. Built into Oracle Database is a self-diagnostic engine, called Automatic Database Diagnostic Monitoring (ADDM), that periodically examines the state of the database, automatically identifies potential database performance bottlenecks, and recommends corrective actions. Oracle Enterprise Manager 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.
- Modern distributed application environments are highly complex, with many moving parts, including system components such as application servers, databases, and servers. The ability to model all aspects of application environments, and discover all relevant application components and their relationships, is essential to the management of this complexity. Moreover, Oracle Enterprise Manager also maps performance measurement metrics to application components automatically.

5.2 Introduction to Business Applications

Oracle Enterprise Manager ensures that your applications are performing at their peak, and that end users are satisfied with their performance. It monitors the performance and availability of business-critical applications, transactions, and services, as well as the experience of customers that access your services. It also enables organizations to identify and prioritize problems based on business impact, and helps resolve problems across today's highly complex application environments before they affect users.

This functionality is available through the creation and monitoring of business application target service types. These unify the dedicated application performance monitoring, diagnostics, and reporting capabilities available through Oracle Real User Experience Insight (RUEI), Oracle Business Transaction Management (BTM), and system monitoring through Oracle Enterprise Manager Cloud Control.

A business application is a managed target service type that represents a logical application. It defines a unit of management as perceived by the user, and defines the logical scope for Oracle Enterprise Manager’s Application Performance Management (APM) capabilities. Examples of business applications could include business-critical applications based on Oracle CRM Fusion Application or an in-house developed web application.

Benefits of Business Application Monitoring

The use of business applications offers a number of significant advantages over traditional IT-centric approaches that only focus on system health issues. In particular, they:

- Allow you to manage your applications in their business context, measuring, and alerting on the basis of the end-users’ experience.
- Provide dashboards with complete visibility across multi-tier composite applications. Moreover, these can easily be customized to display any relevant metric information.
- Provide a visualization of all target relationships within a business service.

Application Monitoring Using RUEI, BTM, and System Monitoring

RUEI is a web-based utility that reports on the real-user traffic requested by, and generated from, your web infrastructure. It allows you to analyze your network and business infrastructure, and provides a diagnostics facility that allows application managers and IT technical staff to perform root-cause analysis. For further information, see the *Oracle Real User Experience Insight User's Guide*.

BTM provides automatic monitoring of the services and transactions within your application environment. It allows you to understand their interaction, business context, consumers, and business payload. For further information, see *Oracle Business Transaction Management Online Help*.

System monitoring provides insights into the behavior of the monitored application infrastructure. It collects metrics and reports on the health of all components from the hosts to the application servers and the deployed Java EE applications. It also provides deep-dive diagnostics tools for the application servers and the databases.

Systems, Services, Business Applications, and Key Components

Within Oracle Enterprise Manager, there are two types of targets: systems and services. A service target represents some functionality provided or supported by a system. A business application is a service target. Hence, when you create a business application, you need to associate it with a system that represents the infrastructure underlying the service functionality.

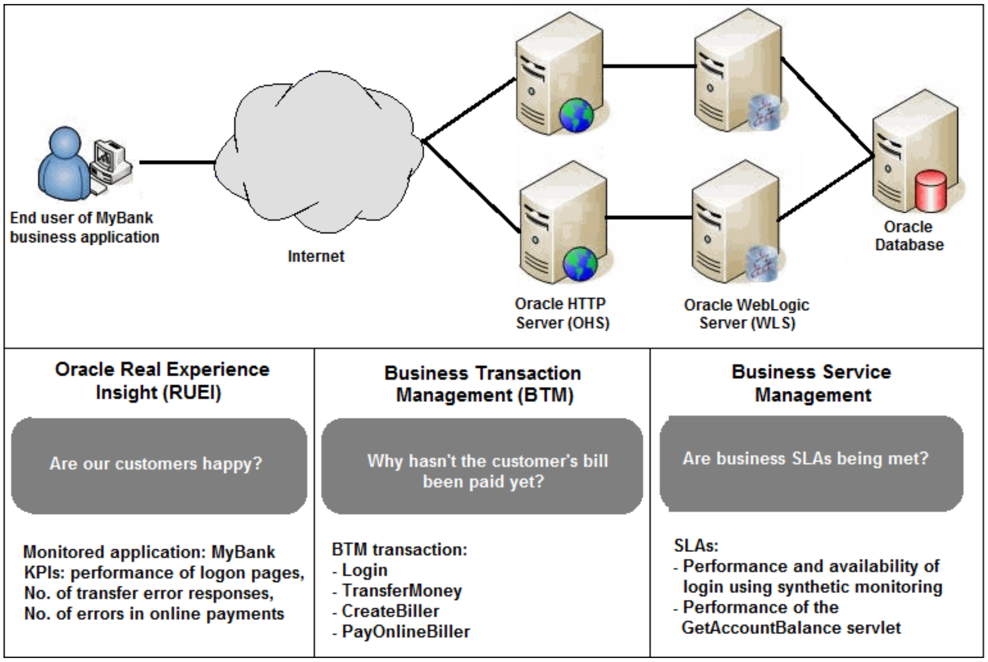
Consider an example business application that contains an order entry application which is implemented by a collection of physical (system) resources. The application is deployed in a Web Logic domain, modeled as a system target whose members are the individual managed servers. The business application could include transactions deployed in containers. Each of these containers is an application server, possibly within a single Web Logic domain. In this case, the Web Logic domain is the system target. In the case that the transaction spans multiple domains, it is recommended that you create a composite application within Oracle Enterprise Manager.

The key components within the system target are then monitored to determine the business application's availability. For instance, for a transaction, the key components will be the servers where the services that comprise the transaction are running.

5.2.1 MyBank: An Example Business Application

This section presents an extended example of a business application. Consider the situation in which end users access a banking application (MyBank) that allows them to perform such tasks as the payment of bills. This business application is delivered through the infrastructure shown in Figure 5–1.

Figure 5–1 The MyBank Business Application


End user of MyBank business application
Internet
Oracle HTTP Server (OHS)
Oracle WebLogic Server (WLS)
Oracle Database

Oracle Real Experience Insight (RUEI)	Business Transaction Management (BTM)	Business Service Management
Are our customers happy?	Why hasn't the customer's bill been paid yet?	Are business SLAs being met?
Monitored application: MyBank KPIs: performance of logon pages, No. of transfer error responses, No. of errors in online payments	BTM transaction: - Login - TransferMoney - CreateBiller - PayOnlineBiller	SLAs: - Performance and availability of login using synthetic monitoring - Performance of the GetAccountBalance servlet

The end-user experience of the MyBank business application is monitored through RUEI, while Key Performance Indicators (KPIs) are used to monitor its key aspects, such as the availability and performance of the logon page, and the number of errors in transfer responses and online payments.

BTM monitors the performance of the services and transactions deployed within the application environment used to deliver the business application. This is done through tracking of each transaction execution as it progresses through the different tiers of the application. This is complemented by the ability to perform root-cause analysis to locate bottlenecks, errors, and incomplete transaction instances.

Proactive application monitoring is achieved through the establishment of business objectives that define acceptable levels of performance and availability. Within Oracle Enterprise Manager, these business objectives are referred to as Service Level

Agreements (SLAs) and are composed of Service Level Objectives (SLOs) that measure specific metrics.

Insight into each of these key aspects of a business application's operation and delivery is available through a number of dedicated regions or the Oracle Enterprise Manager console.

5.3 Prerequisites and Considerations

This section describes the requirements that must be met, and the issues that should be considered, in order to use the Business Applications facility. It is *strongly* recommended that you carefully review this information before proceeding with the creation of business applications.

> **Important:** It is recommended that you review the My Oracle Support website to obtain up-to-date information about the supported RUEI and BTM products, as well as patches, configurations, known issues, and workarounds.

This section covers the following:

- Using RUEI to Monitor Business Applications
- Using BTM to Monitor Business Applications

5.3.1 Using RUEI to Monitor Business Applications

In order to use RUEI to monitor the performance and behavior of your business applications, you must ensure that the following requirements have been met:

- RUEI version 12.1.0.3 (or higher) has been installed and configured to monitor the required applications, suites, and services. Information about deployment options and requirements is available from the *Oracle Real User Experience Insight Installation Guide*.
- The Reporter system must be accessible to Oracle Enterprise Manager via an HTTPS connection on port 443. Other component host systems (such as Collector, Processing Engine, and database servers) do not need to be accessible to Oracle Enterprise Manager unless you intend to make them managed targets (see Section 5.4, "Registering RUEI/BTM Systems").
- The statistics data retention setting (which governs the availability of statistical information such as violation counters) has been configured to be consistent with your business application reporting requirements. The procedure to do this is described in the *Oracle Real User Experience Insight User's Guide*.
- If you intend to export session information from the Session Diagnostics facility, you should ensure that the exported session is not older than the period specified for the Full Session Replay (FSR) data retention setting. In addition, the URL prefix masking setting should be specified as "Complete logging". For more information, see the *Oracle Real User Experience Insight User's Guide*.

Registering RUEI Installations with Self-Signed Certificates

A RUEI installation can use a self-signed certificate. This is explained in the *Oracle Real User Experience Insight Installation Guide*. However, Oracle Enterprise Manager only accepts SSL certificates issued by a trusted Certificate Authority (CA), and that contain a valid Common Name (CN). Therefore, in order to be able to register a RUEI installation with Oracle Enterprise Manager, you need to do the following:

1. Verify that the certificate is valid. One way to do this is to attempt to access the Oracle Enterprise Manager system through a browser via HTTPS and view the certificate details. You should ensure the certificate' s date validity. If the certificate's date range does not include the period your Oracle Enterprise Manager system is running, you will not be able to use it.

2. Download the certificate to your Oracle Enterprise Manager system. Many browsers provide an option when creating a security exception for a self-signed certificate to also save the certificate to a file. This file should reside in your hosted system for the next step to register it in a keystore. The example below assumes that you stored the file containing the certificate in `~/rueicertfile.txt`.

3. Add the certificate to the keystore. Within Oracle Enterprise Manager, two keystores are used to communicate with a RUEI system via SSL: one for discovery, and one for the communication once RUEI is registered. Both keystores need to contain the same certificate. Issue the following commands on the Oracle Enterprise Manager system:

```
keytool -import -keystore AgentTrust.jks -file ~/rueicertfile.txt -alias \
rueicacerts -storepass welcome
keytool -import -keystore DemoTrust.jks -file ~/rueicertfile.txt -alias \
rueicacerts -storepass DemoTrustKeyStorePassPhrase
```

4. In order for Oracle Enterprise Manager to work with the new certificate, perform a total bounce. Issue the following commands:

```
$ORACLE_HOME/bin/emctl stop oms -all -force
$ORACLE_HOME/bin/emctl stop agent
$ORACLE_HOME/bin/emctl start oms
$ORACLE_HOME/bin/emctl start agent
```

5.3.2 Using BTM to Monitor Business Applications

In order to use BTM to monitor the performance and behavior of your business applications, you must ensure that the following requirements have been met:

- BTM version 12.1.0.3 (or higher) has been installed and configured. Installation and configuration instructions are provided in the *Oracle Business Transaction Management Installation Guide*.
- The server where the central BTM server is deployed must be accessible to the Oracle Management Server (OMS) on the port where the BTM system's managed server is listening.
- The business transactions you intend to monitor via the business application facility have been defined within the BTM user interface. The procedure for doing this is described in the *Business Transaction Management Online Help*.

5.4 Registering RUEI/BTM Systems

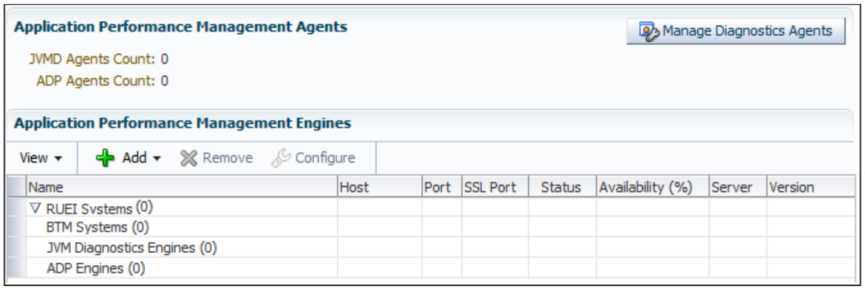
Before you can create business applications based on RUEI-monitored applications and services, or BTM-monitored transactions, you must first register the appropriate RUEI or BTM system with Oracle Enterprise Manager.

Note: You must have Super Administrator privileges in order to access the Application Performance Management page.

Do the following:

1. From the **Setup** menu, select **Application Performance Management**. The Application Performance Management page shown in Figure 5–2 appears. The currently registered systems are listed.

Figure 5–2 Application Performance Management Agents



Application Performance Management Agents

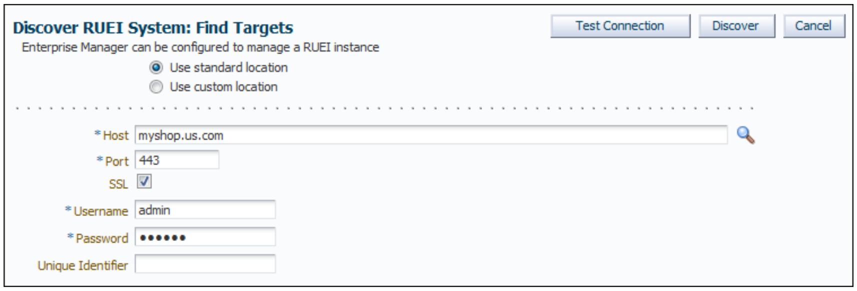
JVMD Agents Count: 0
ADP Agents Count: 0

Application Performance Management Engines

Name	Host	Port	SSL Port	Status	Availability (%)	Server	Version
▽ RUEI Systems (0)							
BTM Systems (0)							
JVM Diagnostics Engines (0)							
ADP Engines (0)							

2. Select **Real User Experience Insight System** or **Business Transaction Management System** from the **Add** drop down. A page similar to the one shown in Figure 5–3 appears.

Figure 5–3 Discover RUEI System Page



Discover RUEI System: Find Targets

Enterprise Manager can be configured to manage a RUEI instance

● Use standard location
○ Use custom location

* Host	myshop.us.com
* Port	443
SSL	☑
* Username	admin
* Password	••••••
Unique Identifier	

3. Specify whether the RUEI or BTM system is running in a standard or custom location.

4. Specify the host system where the Reporter system or BTM Sphere is located. Click **Select Target**. A new window opens that allows you to view the available systems. You can use the **Target Type** menu to search for specific target types.

5. Specify the port number used to communicate with the RUEI Reporter or BTM Sphere.

6. Specify whether a secure connection should be used to the RUEI Reporter or BTM Sphere. If so, the necessary SSL certificates must be registered with Oracle Enterprise Manager. This is described in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* available at the following location:

   `http://docs.oracle.com/cd/E24628_01/install.121/e24089/appdx_troubleshooting.htm#CEGBIGBH`

7. Specify a valid user name and password combination. For a RUEI system, the specified user must have Security Officer permission. Note that if SSO is enabled, you need to specify `em_user` and the appropriate password. For a BTM system,

the specified user must have the assigned role of `btmAdmin`. If necessary, consult your RUEI/BTM Administrator.

8. Optionally, specify a string to be attached to the RUEI/BTM system name. For example, if "SanitySite" is specified, then each of the system's component names will be prefixed with "SanitySite_", creating system names such as "SanitySite_BTM_System".

9. In the case of a custom location, specify the full URL of the WSDL RUEI/BTM discovery service. In the case of a BTM system, this should be in the following form:

   ```
   http://host:port/btmcentral/sphere/discoveryService/?wsdl
   ```

   In the case of a RUEI instance, this should be in the following form:

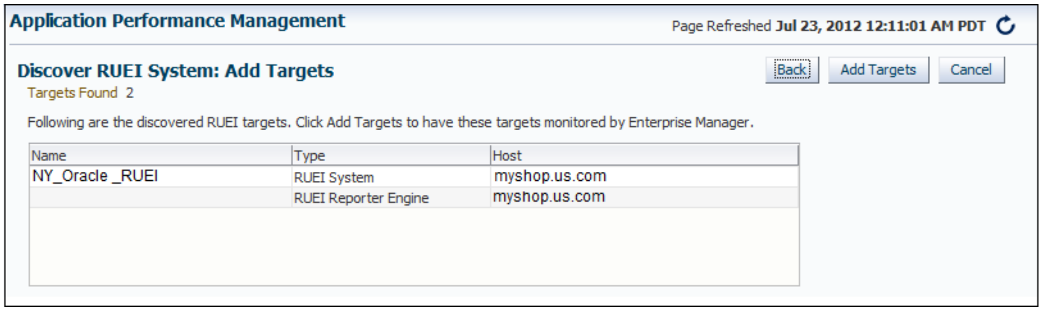
   ```
   http://host:port/ruei/service.php?endPoint=uxDiscoveryService&wsdl
   ```

10. Specify the URL of Management Agent to be used to collect metric information about the system. If it is managed by Oracle Enterprise Manager, you can click **Select** to specify it.

11. Click **Test Connection** to verify whether a working connection to the RUEI/BTM system can be made.

12. Click **Discover**. An overview of the components associated with the selected system is displayed. An example is shown in Figure 5–4.

Figure 5–4 Discover RUEI Instance: View Targets Page



Application Performance Management

Page Refreshed Jul 23, 2012 12:11:01 AM PDT

Discover RUEI System: Add Targets

Targets Found 2

Following are the discovered RUEI targets. Click Add Targets to have these targets monitored by Enterprise Manager.

Name	Type	Host
NY_Oracle _RUEI	RUEI System	myshop.us.com
	RUEI Reporter Engine	myshop.us.com

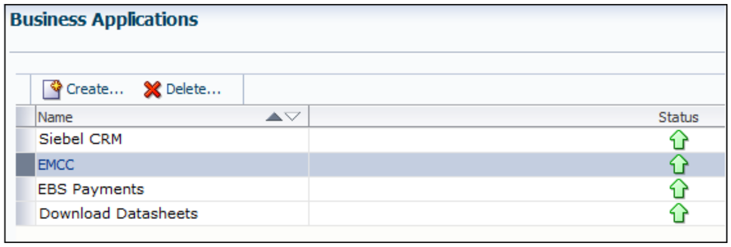
13. Click **Add Targets** to have each of the system's components become a managed target within Oracle Enterprise Manager. Note that if you do so, each system must be accessible to a Management Agent. Further information about managed targets is available from the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

5.5 Creating Business Applications

To create a business application, you need to specify the RUEI-monitored applications, suites, and services, or BTM-monitored transactions upon which it is based. Do the following:

1. From the **Targets** menu, select **Business Applications**. The currently defined business applications are displayed. The page shown in Figure 5–5 appears.

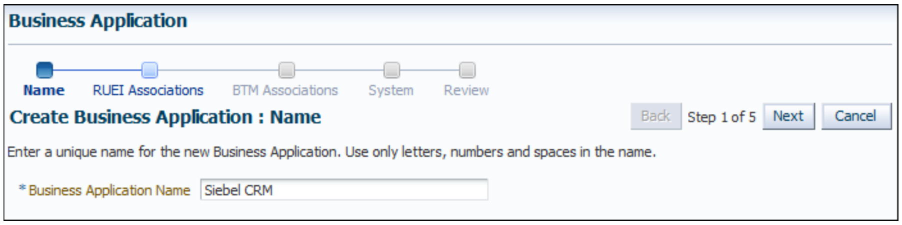
Figure 5–5 Business Application Page



Name	Status
Siebel CRM	⇧
EMCC	⇧
EBS Payments	⇧
Download Datasheets	⇧

2. Click **Create**. The page shown in Figure 5–6 appears.

Figure 5–6 Create Business Application (Name) Page

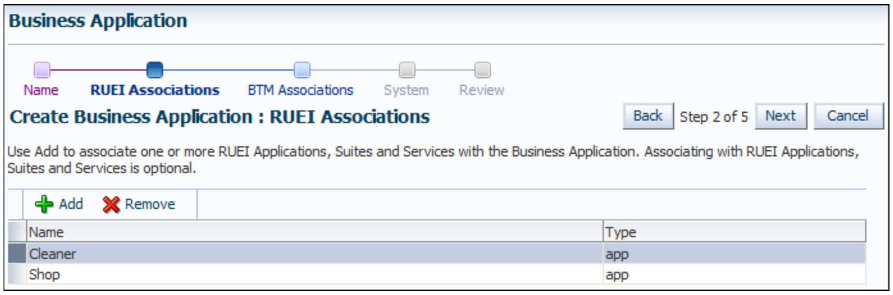


Enter a unique name for the new Business Application. Use only letters, numbers and spaces in the name.

* Business Application Name: Siebel CRM

3. Specify a unique name for the new business application. It is recommended that you include an indication of the purpose and scope of the business application as part of the name. Note that business applications cannot be renamed later. When ready, click **Next**. The page shown in Figure 5–7 appears.

Figure 5–7 Create Business Application (RUEI Associations) Page

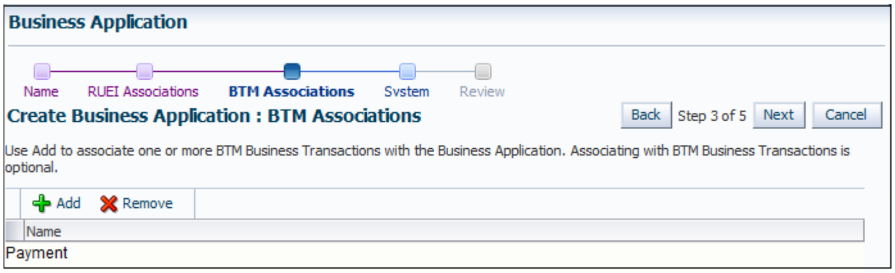


Use Add to associate one or more RUEI Applications, Suites and Services with the Business Application. Associating with RUEI Applications, Suites and Services is optional.

Name	Type
Cleaner	app
Shop	app

4. Click **Add**. A new window opens that allows you to select the RUEI-monitored applications, suites, and services upon which the business application should be based. You can use the **Type** menu to restrict the listing to specific types. When ready, click **Next**. The page shown in Figure 5–8 appears.

Figure 5–8 Create Business Application (BTM Associations) Page



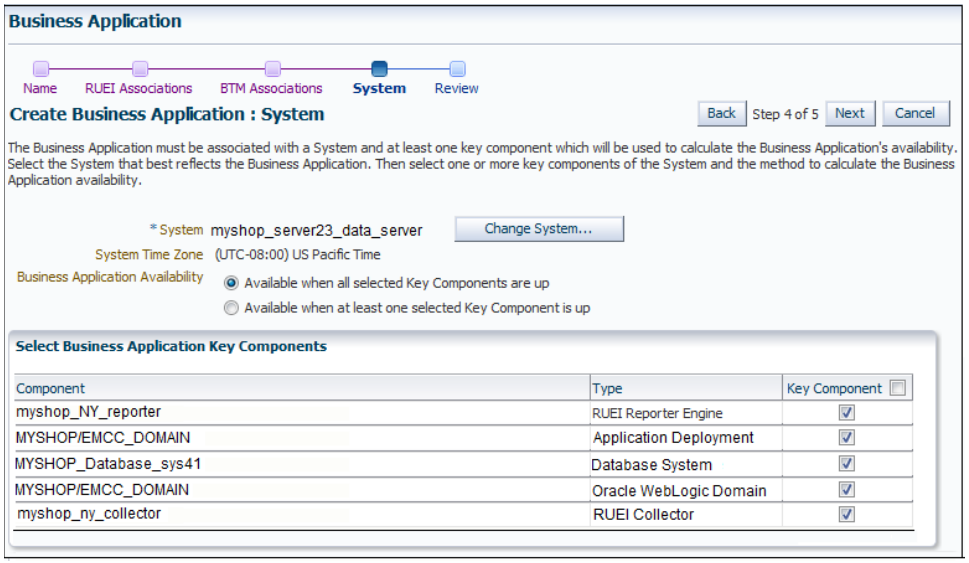
Create Business Application : BTM Associations

Use Add to associate one or more BTM Business Transactions with the Business Application. Associating with BTM Business Transactions is optional.

Name
Payment

5. Click **Add**. A new window opens that allows you to select the BTM-monitored transactions upon which the business application should be based. When ready, click **Next**. The page shown in Figure 5–9 appears.

Figure 5–9 Create Business Application (System) Page



Create Business Application : System

The Business Application must be associated with a System and at least one key component which will be used to calculate the Business Application's availability. Select the System that best reflects the Business Application. Then select one or more key components of the System and the method to calculate the Business Application availability.

* System myshop_server23_data_server

System Time Zone (UTC-08:00) US Pacific Time

Business Application Availability
● Available when all selected Key Components are up
○ Available when at least one selected Key Component is up

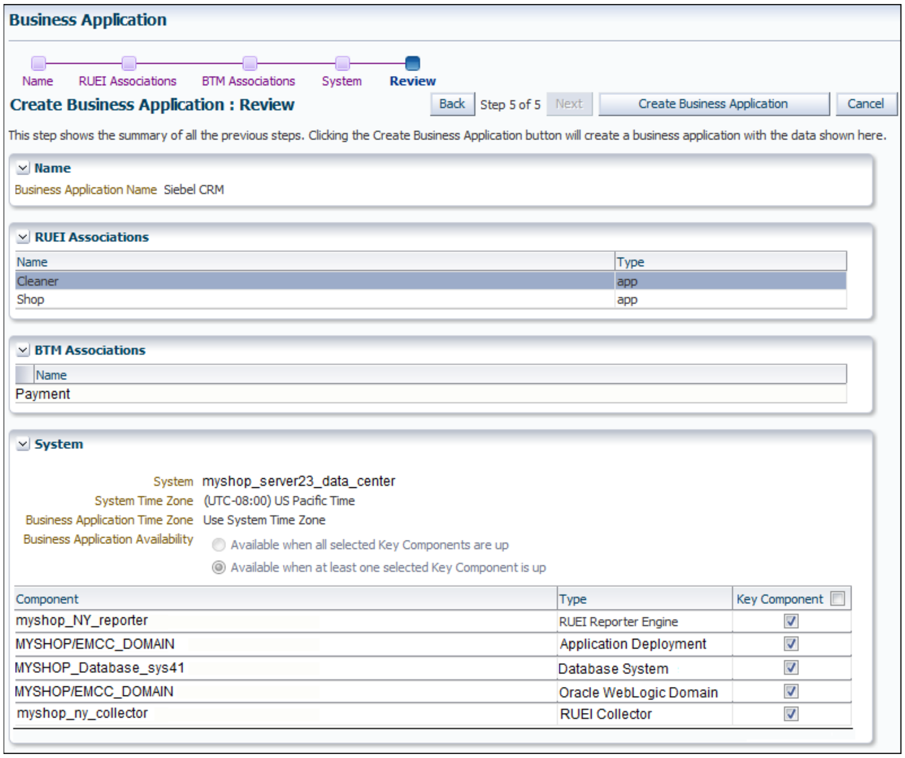
Select Business Application Key Components

Component	Type	Key Component □
myshop_NY_reporter	RUEI Reporter Engine	☑
MYSHOP/EMCC_DOMAIN	Application Deployment	☑
MYSHOP_Database_sys41	Database System	☑
MYSHOP/EMCC_DOMAIN	Oracle WebLogic Domain	☑
myshop_ny_collector	RUEI Collector	☑

6. Click **Select System** and select the system that hosts the business application. This should be a system that encompasses the infrastructure that the business application runs on.

   Use the **Key Component** check boxes to select the system members used in the calculation of the business application's availability. Two rules are available: either *all* specified key components for a business application must be up, or *at least one* of them must be up (the default). When ready, click **Next**. The page shown in Figure 5–10 appears.

Figure 5–10 Create Business Application (Review) Page



Create Business Application : Review

This step shows the summary of all the previous steps. Clicking the Create Business Application button will create a business application with the data shown here.

Name

Business Application Name Siebel CRM

RUEI Associations

Name	Type
Cleaner	app
Shop	app

BTM Associations

Name
Payment

System

System myshop_server23_data_center
System Time Zone (UTC-08:00) US Pacific Time
Business Application Time Zone Use System Time Zone
Business Application Availability
○ Available when all selected Key Components are up
● Available when at least one selected Key Component is up

Component	Type	Key Component □
myshop_NY_reporter	RUEI Reporter Engine	☑
MYSHOP/EMCC_DOMAIN	Application Deployment	☑
MYSHOP_Database_sys41	Database System	☑
MYSHOP/EMCC_DOMAIN	Oracle WebLogic Domain	☑
myshop_ny_collector	RUEI Collector	☑

7. Review the new business application's properties before creating it. If necessary, use the **Back** and **Next** buttons to amend its properties. When ready, click **Create Business Application**. The newly created business application appears on the Business Application page (Figure 5–5).

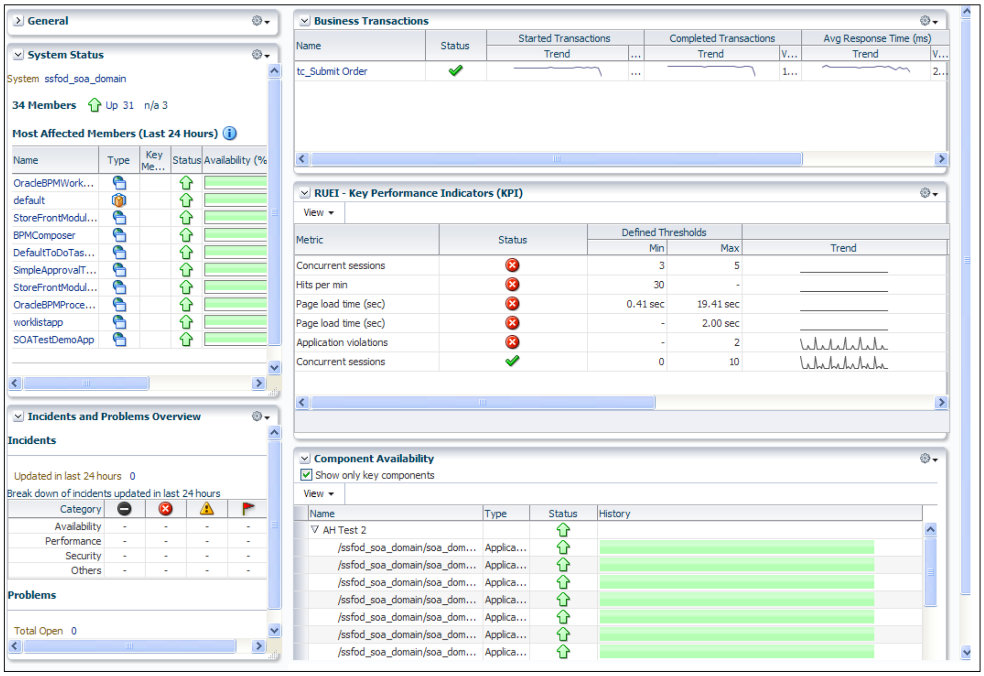
5.6 Monitoring Business Applications

Once a business application has been created, you can monitor its performance and availability, as well as the status of the systems (hosts, databases, and middleware components) that deliver it within the underlying IT infrastructure. In this way, you can obtain end-to-end visibility of your applications and services, and ensure that end-user requirements are being met.

To view the status of your business applications:

1. From the **Targets** menu, select **Business Applications**. The currently defined business applications are listed. An example is shown in Figure 5–5.
2. Click the required business application. The selected business application home page appears. An example is shown in Figure 5–11.

Figure 5–11 Business Application Home Page



General

System Status

System ssfod_soa_domain

34 Members Up 31 n/a 3

Most Affected Members (Last 24 Hours)

Name	Type	Key Me...	Status	Availability (%
OracleBPMWork...			⇧	🟩
default			⇧	🟩
StoreFrontModul...			⇧	🟩
BPMComposer			⇧	🟩
DefaultToDoTas...			⇧	🟩
SimpleApprovalT...			⇧	🟩
StoreFrontModul...			⇧	🟩
OracleBPMProce...			⇧	🟩
worklistapp			⇧	🟩
SOATestDemoApp			⇧	🟩

Incidents and Problems Overview

Incidents

Updated in last 24 hours 0

Break down of incidents updated in last 24 hours

Category	⊖	⊗	⚠	⚑
Availability	-	-	-	-
Performance	-	-	-	-
Security	-	-	-	-
Others	-	-	-	-

Problems

Total Open 0

Business Transactions

Name	Status	Started Transactions		Completed Transactions		Avg Response Time (ms)	
		Trend	...	Trend	V...	Trend	V...
tc_Submit Order	✓		...		1...		2...

RUEI - Key Performance Indicators (KPI)

View ▾

Metric	Status	Defined Thresholds		
		Min	Max	Trend
Concurrent sessions	⊗	3	5	
Hits per min	⊗	30	-	
Page load time (sec)	⊗	0.41 sec	19.41 sec	
Page load time (sec)	⊗	-	2.00 sec	
Application violations	⊗	-	2	
Concurrent sessions	✓	0	10	

Component Availability

☑ Show only key components

View ▾

Name	Type	Status	History
▽ AH Test 2		⇧	
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩
/ssfod_soa_domain/soa_dom...	Applica...	⇧	🟩

3. Each region provides specific information on the various operational aspects of the selected business application. By default, the following regions are available:

   - **General**: indicates the business application's status and availability. Click the **Availability (%)** item to view a history of its status for the selected time period.

   - **Component Availability**: indicates the availability of the components that deliver the business application.

   - **System Status**: indicates the business application's availability over the last 24 hours.

   - **Incidents and Problems Overview**: indicates the number of outstanding critical, warning, and error alerts associated with the selected business application.

   - **RUEI - Key Performance Indicators (KPI)**: indicates the status of the KPIs associated with the business application's targets.

   - **Business Transactions**: the use of this region is explained in Section 5.10, "Monitoring BTM Transactions".

4. From the **Business Application** drop down, select **Real User Experience (RUEI)** and then **Real User Experience (RUEI) Data**. Information about the selected business application is available from a number of regions. Their use is described in Section 5.7, "Monitoring RUEI Components".

5. From the **Business Application** drop down, select **Real User Experience (RUEI)** and then **RUEI Session Diagnostics**. The use of this facility is described in Section 5.8, "Working with the RUEI Session Diagnostics Facility".

5.7 Monitoring RUEI Components

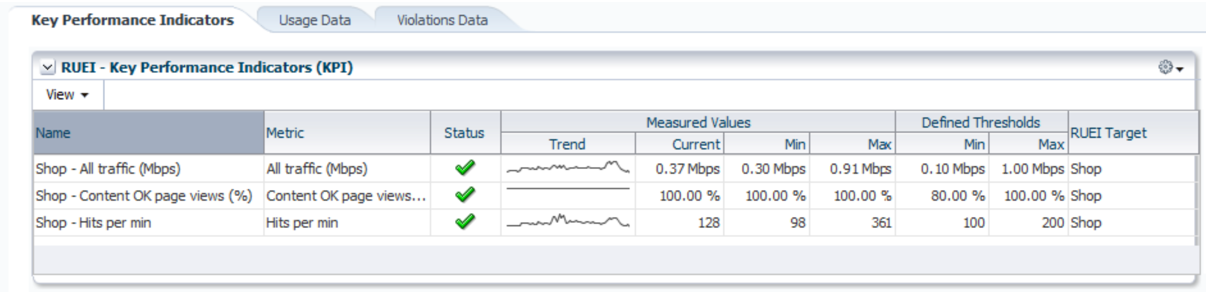
Information about the RUEI-monitored applications, suites, and services within a business application is available from the following regions:

- RUEI - Key Performance Indicators (KPI) Region
- RUEI - Top User and Application Violations Region
- RUEI - Top Executed User Requests Region
- RUEI - Top Users Region
- Real User Session Diagnostics

5.7.1 RUEI - Key Performance Indicators (KPI) Region

This region enables you to review relevant information about key aspects of the RUEI application, suite, or service upon which the business application is based. For example, you could have KPIs defined for such things as availability issues, performance, and visitor traffic. An example is shown in Figure 5–12.

Figure 5–12 RUEI - Key Performance Indicators (KPI) Region


Key Performance Indicators
Usage Data
Violations Data
RUEI - Key Performance Indicators (KPI)
View

Name	Metric	Status	Measured Values				Defined Thresholds		RUEI Target
			Trend	Current	Min	Max	Min	Max	
Shop - All traffic (Mbps)	All traffic (Mbps)	✓		0.37 Mbps	0.30 Mbps	0.91 Mbps	0.10 Mbps	1.00 Mbps	Shop
Shop - Content OK page views (%)	Content OK page views...	✓		100.00 %	100.00 %	100.00 %	80.00 %	100.00 %	Shop
Shop - Hits per min	Hits per min	✓		128	98	361	100	200	Shop

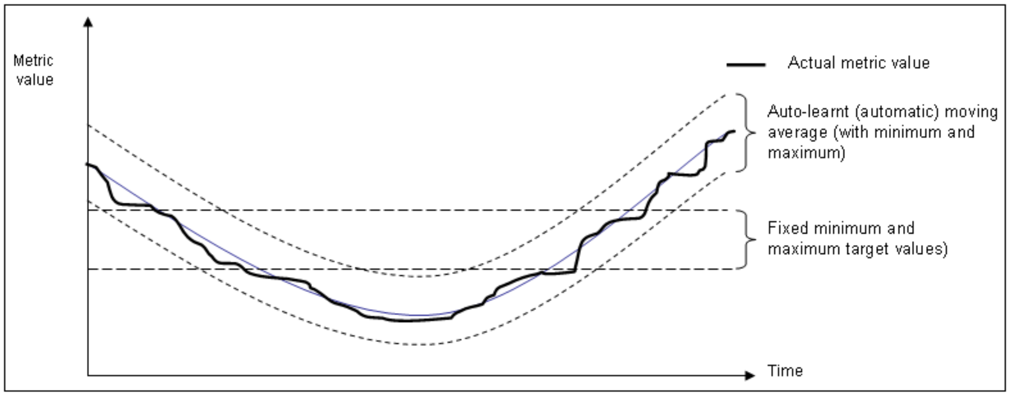
Understanding Report Metric Values

A KPI's metric value is always calculated over a 1-minute interval. That is, the metric's value is derived from its average value over that 1-minute period. Within the RUEI instance's configuration, The KPI calculation range specifies how many of these 1-minute period averages should be used when calculating the metric's reported value. By default, the calculation range is one minute. However, a longer calculation range can be specified if you want extreme values to be averaged out over a longer period. For example, if a calculation range of 10 minutes is specified, the metric's value over each reported 1-minute period is calculated based on the averages for the previous 10 1-minute periods. Similarly, a calculation range of 15 minutes would specify that the reported value should be derived from the averages for the last 15 1-minute periods.

Automatic and Fixed Targets

In addition to fixed targets, KPIs can be based on automatic (or auto-learnt) targets. Because visitor traffic and usage patterns can differ widely during the course of a day, these auto-learnt minimum and maximum targets are calculated as moving averages for the current 1-minute period, based on the measured metric value for that 1-minute period over the last 30 days. For example, when a KPI metric is measured at 10.45 AM, the average against which it is compared is calculated from the last 30 days of measurements at 10.45 AM. The minimum and maximum targets can be defined in terms of small, medium, or large deviations from these moving averages. In contrast, a fixed KPI target essentially represents a straight line, as either a minimum or maximum. This is shown in Figure 5–13.

Figure 5–13 Automatic and Fixed KPI Targets Contrasted



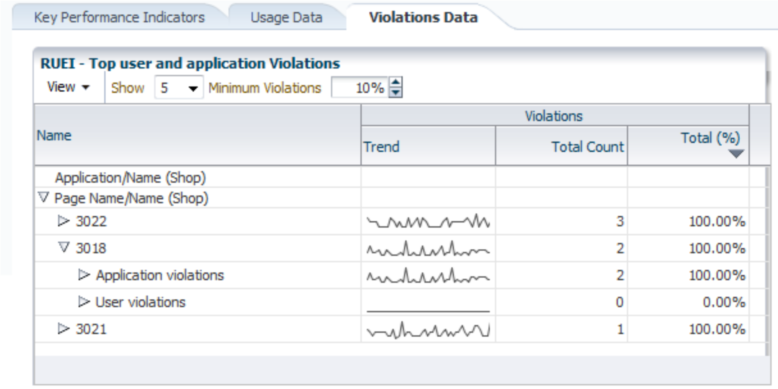
Alert Handling

Optionally, KPIs can be configured within RUEI to generate alerts when they move outside their defined boundaries. If enabled, the configuration defines the duration the KPI must be down before an alert is generated, the severity of the reported incident, and whether an additional notification should be generated when the KPI has returned to its defined boundaries. The reporting of these alerts is described in Section 5.9, "Monitoring KPI and SLA Alert Reporting".

5.7.2 RUEI - Top User and Application Violations Region

This region enables you to examine the suite and application pages, as well as service functions, with the highest number of violations associated with them. An example is shown in Figure 5–14.

Figure 5–14 RUEI - Top User and Application Violations Region



RUEI - Top user and application Violations

View ▾ | Show 5 ▾ Minimum Violations 10%

Name	Violations		
	Trend	Total Count	Total (%)
Application/Name (Shop)			
▽ Page Name/Name (Shop)			
▷ 3022		3	100.00%
▽ 3018		2	100.00%
▷ Application violations		2	100.00%
▷ User violations		0	0.00%
▷ 3021		1	100.00%

The application violation counter reports the number of website, network, server and content errors, while the user violation counter reports the number of content notifications and client aborts. Note that a content notification is the detection of a predefined string within a page (such as "Order processed successfully"), while a client abort refers to a page view that was aborted by the client, possibly because the client closed the browser, or clicked reload, or clicked away, while the page was loading.

For each suite instance, total counters are also reported for each of its associated suite-specific data items (such as Oracle Fusion view ID). See the *Oracle Real User Experience Insight User's Guide* for further information on these items.

Note that the number of items (such as page names or suite-specific data items) listed for a category can be controlled via the **Show** menu. For example, list only the 5 or 10 items with the most violations. The **Minimum Violations** menu allows you to specify the threshold of violation incidents that needs to be met for a page before being reported.

Violation Reporting

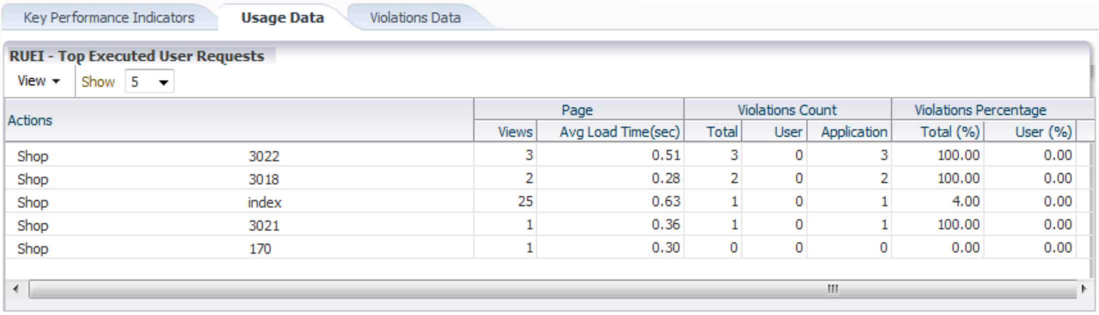
Note if a page or object experienced several types of errors (for example, both a network and a web service error), the page or object error is not recorded multiple times. Instead, it is reported according to the following order: website, server, network, and content. For example, an object that experienced both a website and a network error, it is recorded as a website error rather than a network error.

The application violation counter reports the total number of website, network, server, and content errors. The user violation counter reports the total number of content notifications and client aborts. An example of the possible use of these counters would be the creation of dashboards to track the general health of specific applications. These counters are also available for use as KPI metrics.

5.7.3 RUEI - Top Executed User Requests Region

This region enables you to view the most frequent user requests and actions, and their impact on the business application. These actions can be specific page names, or combinations of suite-specific dimensions (such as Siebel screen, module, and view names). An example is shown in Figure 5–15.

Figure 5–15 RUEI - Top Executed User Requests Region



RUEI - Top Executed User Requests

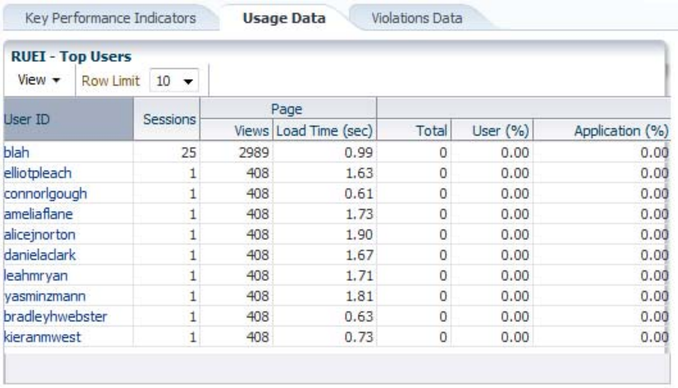
Actions		Page		Violations Count			Violations Percentage	
		Views	Avg Load Time(sec)	Total	User	Application	Total (%)	User (%)
Shop	3022	3	0.51	3	0	3	100.00	0.00
Shop	3018	2	0.28	2	0	2	100.00	0.00
Shop	index	25	0.63	1	0	1	4.00	0.00
Shop	3021	1	0.36	1	0	1	100.00	0.00
Shop	170	1	0.30	0	0	0	0.00	0.00

Using this region, you can verify the performance of the most popular user requests associated with a business application (such as downloads or payment handlings).

5.7.4 RUEI - Top Users Region

This region enables you to monitor the most active users of the targets associated with the business application. This includes session and page view information, as well as user and application violation indicators. An example is shown in Figure 5–16.

Figure 5–16 RUEI - Top Users Region



User ID	Sessions	Page				
		Views	Load Time (sec)	Total	User (%)	Application (%)
blah	25	2989	0.99	0	0.00	0.00
elliotpleach	1	408	1.63	0	0.00	0.00
connorlgough	1	408	0.61	0	0.00	0.00
ameliaflane	1	408	1.73	0	0.00	0.00
alicejnorton	1	408	1.90	0	0.00	0.00
danielaclark	1	408	1.67	0	0.00	0.00
leahmryan	1	408	1.71	0	0.00	0.00
yasminzmann	1	408	1.81	0	0.00	0.00
bradleyhwebster	1	408	0.63	0	0.00	0.00
kieranmwest	1	408	0.73	0	0.00	0.00

You can select users and obtain detailed information about their associated sessions through the Session Diagnostics facility (described in Section 5.8, "Working with the RUEI Session Diagnostics Facility").

5.7.5 Real User Session Diagnostics

The Session Diagnostics facility provides a powerful means for you to perform root-cause analysis of operational problems. It supports session performance breakdown, including the impact of failing pages and hits on sessions, the full content of each failed page, and the relationship between objects, page views, and sessions. Moreover, it offers the opportunity to track exactly what error messages visitors to the monitored website receive, and when. With this ability to recreate application failures, you can accurately and immediately eliminate annoying and problematic parts of your web pages. Further information about the use of this region is available in Section 5.8, "Working with the RUEI Session Diagnostics Facility".

5.8 Working with the RUEI Session Diagnostics Facility

The Session Diagnostics facility provides a powerful means for you to perform root-cause analysis of operational problems. It supports session performance breakdown, including the impact of failing pages and hits on sessions, the full content of each failed page, and the relationship between objects, page views, and sessions. Moreover, it offers the opportunity to track exactly what error messages visitors to the monitored website receive, and when. With this ability to recreate application failures, you can accurately and immediately eliminate annoying and problematic parts of your web pages.

This section covers the following:

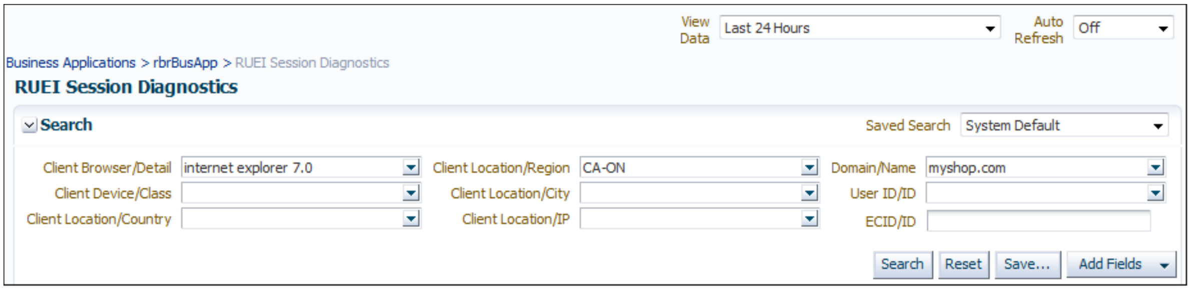
- Getting Started
- Customizing Session Diagnostics Reporting
- Exporting Full Session Information
- Exporting Session Pages to Microsoft Excel

5.8.1 Getting Started

To locate the diagnostics information you require, do the following:

1. From the **Business Application** drop down, select **Real User Experience (RUEI)** and then **RUEI Session Diagnostics**. The RUEI Session Diagnostics page shown in Figure 5–17 appears.

Figure 5–17 RUEI Session Diagnostics Search Page



Business Applications > rbrBusApp > RUEI Session Diagnostics

RUEI Session Diagnostics

View Data: Last 24 Hours

Auto Refresh: Off

Saved Search: System Default

Client Browser/Detail: internet explorer 7.0

Client Device/Class:

Client Location/Country:

Client Location/Region: CA-ON

Client Location/City:

Client Location/IP:

Domain/Name: myshop.com

User ID/ID:

ECID/ID:

2. Use the **View Data** menu to select the required period. Note that the availability of session diagnostics information is determined by the Statistics and Session Diagnostics data retention policy settings specified for the associated RUEI instance. For more information, see the *Oracle Real User Experience Insight User's Guide*.

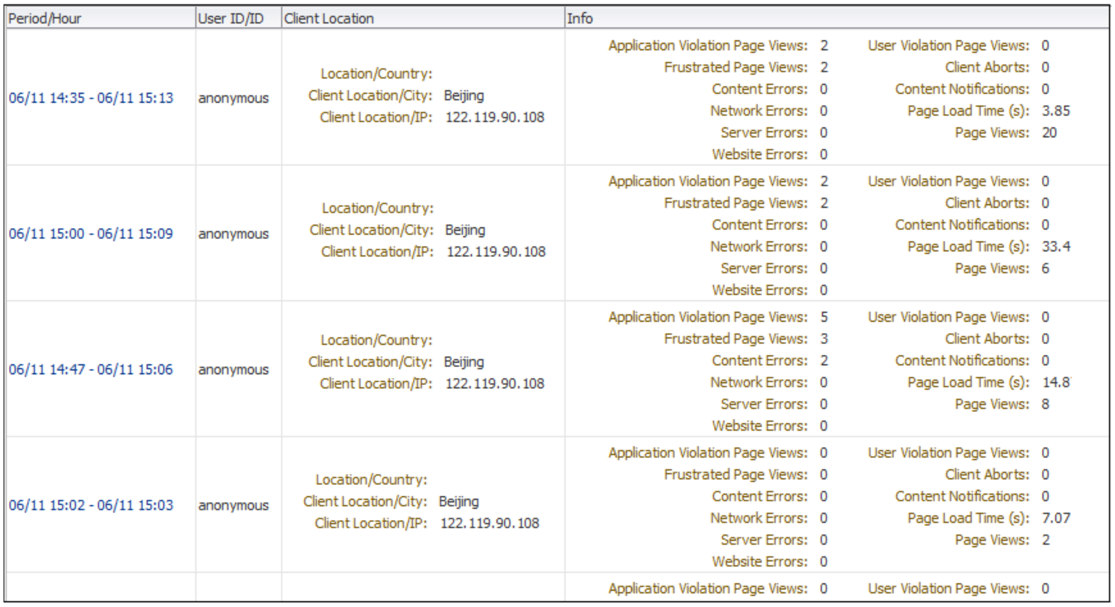
3. Specify the appropriate search criteria to locate the required user record(s). The available default search criteria are controlled by the RUEI instance configuration (described in Section 5.8.2, "Customizing Session Diagnostics Reporting"). You can click **Add Fields** to make additional search criteria available. Be aware that while the use of wildcard characters (*) is supported, all other search characters are treated as literals. Also, *all* criteria specified for the search must be met for matched user records to be reported.

   Note that you can specify multiple values for a single dimension by clicking **Add Fields**, and selecting the required dimension. In this case, only *one* of the specified values needs to be found in order for a match to be made.

   After updating the appropriate search filters, you can save the search combination by clicking **Save**. Note that changes to saved searches can influence the available fields within the **Add Fields** facility. In addition, the predefined list of available dimensions is based on the business application definition. For example, only oracle Fusion-specific dimensions are available if the business application is defined as a Oracle Fusion suite.

   When ready, click **Search**. The results of the search are shown in the lower part of the area. An example is shown in Figure 5–18.

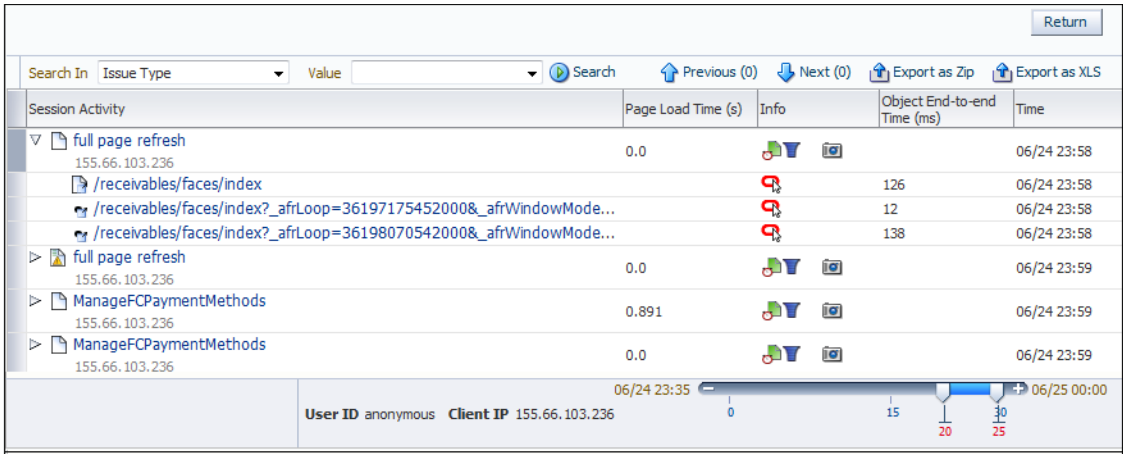
Figure 5–18 Session Diagnostics Search Results



Period/Hour	User ID/ID	Client Location	Info	
06/11 14:35 - 06/11 15:13	anonymous	Location/Country: Client Location/City: Beijing Client Location/IP: 122.119.90.108	Application Violation Page Views: 2 Frustrated Page Views: 2 Content Errors: 0 Network Errors: 0 Server Errors: 0 Website Errors: 0	User Violation Page Views: 0 Client Aborts: 0 Content Notifications: 0 Page Load Time (s): 3.85 Page Views: 20
06/11 15:00 - 06/11 15:09	anonymous	Location/Country: Client Location/City: Beijing Client Location/IP: 122.119.90.108	Application Violation Page Views: 2 Frustrated Page Views: 2 Content Errors: 0 Network Errors: 0 Server Errors: 0 Website Errors: 0	User Violation Page Views: 0 Client Aborts: 0 Content Notifications: 0 Page Load Time (s): 33.4 Page Views: 6
06/11 14:47 - 06/11 15:06	anonymous	Location/Country: Client Location/City: Beijing Client Location/IP: 122.119.90.108	Application Violation Page Views: 5 Frustrated Page Views: 3 Content Errors: 2 Network Errors: 0 Server Errors: 0 Website Errors: 0	User Violation Page Views: 0 Client Aborts: 0 Content Notifications: 0 Page Load Time (s): 14.8 Page Views: 8
06/11 15:02 - 06/11 15:03	anonymous	Location/Country: Client Location/City: Beijing Client Location/IP: 122.119.90.108	Application Violation Page Views: 0 Frustrated Page Views: 0 Content Errors: 0 Network Errors: 0 Server Errors: 0 Website Errors: 0	User Violation Page Views: 0 Client Aborts: 0 Content Notifications: 0 Page Load Time (s): 7.07 Page Views: 2
			Application Violation Page Views: 0	User Violation Page Views: 0

4. Click the required user record from the displayed list. After selecting a user record, information about it is shown. An example is shown in Figure 5–19.

Figure 5–19 Example Session Activity Listing



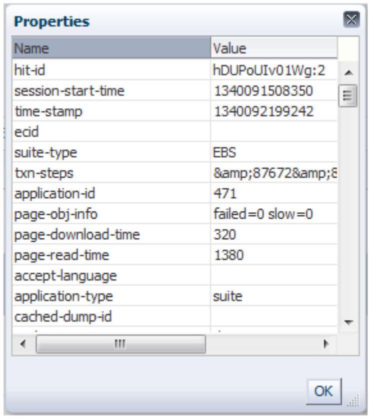
Session Activity	Page Load Time (s)	Info	Object End-to-end Time (ms)	Time
full page refresh 155.66.103.236	0.0			06/24 23:58
/receivables/faces/index			126	06/24 23:58
/receivables/faces/index?_afrLoop=36197175452000&_afrWindowMode...			12	06/24 23:58
/receivables/faces/index?_afrLoop=36198070542000&_afrWindowMode...			138	06/24 23:58
full page refresh 155.66.103.236	0.0			06/24 23:59
ManageFCPaymentMethods 155.66.103.236	0.891			06/24 23:59
ManageFCPaymentMethods 155.66.103.236	0.0			06/24 23:59

User ID anonymous **Client IP** 155.66.103.236

5. The overview shows the pages and actions recorded within the selected user record. Icons indicate slow or failed objects, the page-loading satisfaction, whether replay content is available, and whether clickout is available to JVM Diagnostics to provide activity information.

6. You can click a page or object within the selected user session to open a window with detailed technical information about it. An example is shown in Figure 5–20.

Figure 5–20 Page Properties Window



Properties

Name	Value
hit-id	hDUPoUIv01Wg:2
session-start-time	1340091508350
time-stamp	1340092199242
ecid	
suite-type	EBS
txn-steps	&amp;87672&amp;8
application-id	471
page-obj-info	failed=0 slow=0
page-download-time	320
page-read-time	1380
accept-language	
application-type	suite
cached-dump-id	

7. The list of matched user sessions shown in Figure 5–18 is based upon the period selected in the **View** menu. For example, if the period "Last hour" is selected, the list of matched user sessions is based on sessions that were active during that period. However, they may have started or finished outside this period. For this reason, you can use the slider at the bottom of Figure 5–19 to restrict the displayed page views and actions to a more specific period.

8. Optionally, click **Export as Zip** to export the session's complete contents to external utilities for further analysis (described in Section 5.8.3, "Exporting Full Session Information") or **Export as XLs** to export a summary of the pages within the session (described in Section 5.8.4, "Exporting Session Pages to Microsoft Excel").

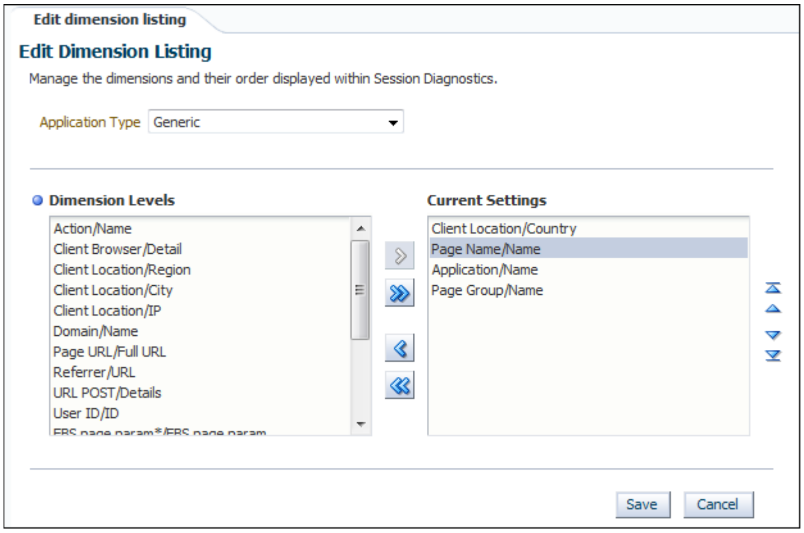
5.8.2 Customizing Session Diagnostics Reporting

You can control the specific dimensions reported in Session Activity part of the Session Diagnostics for applications, suites and services. To do so:

1. From the **Setup** menu, select **Application Performance Management**. The currently registered RUEI instance is shown in the **RUEI Systems** region of the Application Performance Management page shown in Figure 5–2.

2. Select the required RUEI system. Click **Configure**. The Edit Dimension Listing page shown in Figure 5–21 appears.

Figure 5–21 Edit Dimension Listing Page



Edit Dimension Listing

Manage the dimensions and their order displayed within Session Diagnostics.

Application Type: Generic

Dimension Levels

Action/Name
Client Browser/Detail
Client Location/Region
Client Location/City
Client Location/IP
Domain/Name
Page URL/Full URL
Referrer/URL
URL POST/Details
User ID/ID
EBS page param*/EBS page param

Current Settings

Client Location/Country
Page Name/Name
Application/Name
Page Group/Name

3. Use the **Application Type** menu to select whether you want to modify the dimension listings for generic applications (that is, applications that are not suite-based), services, or suites. If the latter, you will need to specify the suite type.

4. Use **Move** and **Remove** to select the dimensions that should be listed. Once selected, you can control the order in which it appears in the list. When ready, click **Save**.

5.8.3 Exporting Full Session Information

In addition to viewing session information, you can also export complete session contents to external utilities for further analysis or integration with other data. For example, this offers the opportunity to use complete real-user sessions as the basis for test script generation. Test platforms, such as Oracle Application Testing Suite (ATS), can easily be configured to generate automated test scripts for an application’s most commonly encountered usage scenarios.

In addition, this facility can also be used to support powerful root-cause analysis. Complete user session information can be provided to application or operations specialists to help identify unusual or difficult to isolate issues. Sensitive information within the exported data is masked according to the actions defined in the HTTP protocol item masking facility. This is described in the *Oracle Real User Experience Insight User’s Guide*.

To export session information:

1. Locate the required session, and click **Export as Zip**.

2. Depending on how your browser is configured, you are either prompted to specify the location to which the zip file should be saved, or it is immediately saved to the defined default location.

Important

In order for the session export files to be created correctly, you should:

- Ensure that the requirements for exporting session information described in Section 5.3, "Prerequisites and Considerations" have been met.

- Verify the exported content files (described in the following section) are present before attempting to import an exported RUEI session into an external utility.

Understanding the Structure of the Exported Data

The exported session zip file contains the following files:

- `data.tab`: contains the direct (raw) hit information for the selected session extracted from the Collector log file.
- `page.tab`: contains the direct (raw) page information for the selected session extracted from the Collector log file.
- `content_`*`hitno`*`.tab`: contains the complete (raw) content information for the indicated hit. There is a file for each hit within the `data.tab` file that has content. For example, if the third and sixth hits had content available for them, two files would be created: `content_3.tab` and `content_6.tab`.

  Viewable versions of the files cited in the hit file are also available under the `content_viewer` directory. This means that data transferred with chunked encoding can be immediately viewed. Note that the same *`hitno`* as in the `data.tab` file is used in their file naming.
- `index.html`: allows developers and other interested parties outside RUEI to view and analyze session details as they would appear within the Session Diagnostics facility, with access to source, page and object details, and element identification.

> **Note:** The log files used as the basis for creating exported session files are also used internally by RUEI. The format and contents of these files is subject to change without notice.

5.8.4 Exporting Session Pages to Microsoft Excel

You can export a summary of the pages within the currently selected session to Microsoft Excel. To do so:

1. Locate the required, and click **Export as XLS**. Depending on how your browser is configured, you are either prompted to specify the tool with which to open the file directly (by default, Microsoft Excel), or it is immediately saved to the defined default location.
2. Within Microsoft Excel, you can view and edit the generated file. The exported page view history and session summary can be used to compile sets of real-user sessions. For example, to be used as the basis for testing or performance analysis.

Controlling Row Creation and Ordering

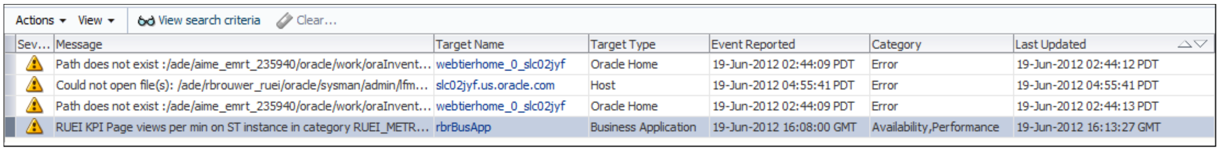
Be aware that the rows that appear in the Microsoft Excel export are based on the currently specified RUEI configuration. This is described in Section 5.8.2, "Customizing Session Diagnostics Reporting".

5.9 Monitoring KPI and SLA Alert Reporting

The alerts generated by KPIs defined for the applications, suites, and services, as well as for the SLAs for the transactions that comprise your business applications are reported as events in Incident Manager. To view these events:

1. From the **Enterprise** menu, select **Monitoring**, and then **Incident Manager**. Open the **Events Without Incidents** predefined view. An example is shown in Figure 5–22.

Figure 5–22 RUEI KPI Alerting Within Incident Manager



Sev...	Message	Target Name	Target Type	Event Reported	Category	Last Updated
⚠	Path does not exist :/ade/aime_emrt_235940/oracle/work/oraInvent...	webtierhome_0_slc02jyf	Oracle Home	19-Jun-2012 02:44:09 PDT	Error	19-Jun-2012 02:44:12 PDT
⚠	Could not open file(s): /ade/rbrouwer_ruei/oracle/sysman/admin/lfm...	slc02jyf.us.oracle.com	Host	19-Jun-2012 04:55:41 PDT	Error	19-Jun-2012 04:55:41 PDT
⚠	Path does not exist :/ade/aime_emrt_235940/oracle/work/oraInvent...	webtierhome_0_slc02jyf	Oracle Home	19-Jun-2012 02:44:09 PDT	Error	19-Jun-2012 02:44:13 PDT
⚠	RUEI KPI Page views per min on ST instance in category RUEI_METR...	rbrBusApp	Business Application	19-Jun-2012 16:08:00 GMT	Availability,Performance	19-Jun-2012 16:13:27 GMT

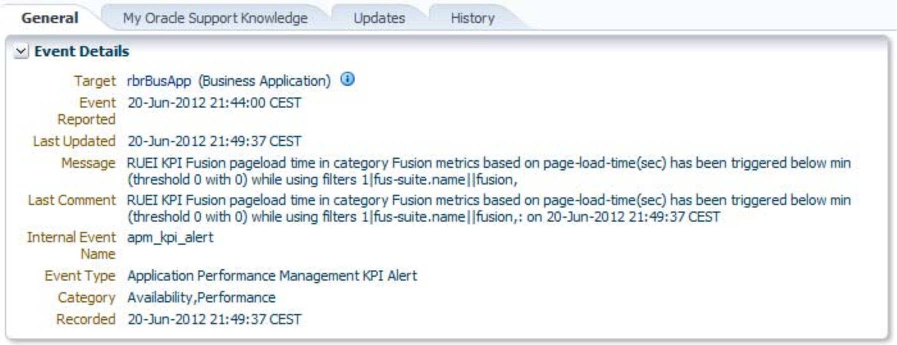
2. Click the event of interest to view more information about it.

3. Event detail information varies depending on whether the event is based on a RUEI KPI or BTM SLA. Each is described in the following sections.

RUEI Event Detail

The status of the KPIs defined for the applications, suites, and services that comprise your business applications are reported in the RUEI - Key Performance Indicators (KPIs) region (explained in Section 5.7.1, "RUEI - Key Performance Indicators (KPI) Region"). The detail event information for alerts generated by RUEI KPIs is shown in Figure 5–23.

Figure 5–23 KPI Alert Event Details



Target rbrBusApp (Business Application)

Event Reported 20-Jun-2012 21:44:00 CEST

Last Updated 20-Jun-2012 21:49:37 CEST

Message RUEI KPI Fusion pageload time in category Fusion metrics based on page-load-time(sec) has been triggered below min (threshold 0 with 0) while using filters 1|fus-suite.name||fusion,

Last Comment RUEI KPI Fusion pageload time in category Fusion metrics based on page-load-time(sec) has been triggered below min (threshold 0 with 0) while using filters 1|fus-suite.name||fusion,: on 20-Jun-2012 21:49:37 CEST

Internal Event Name apm_kpi_alert

Event Type Application Performance Management KPI Alert

Category Availability,Performance

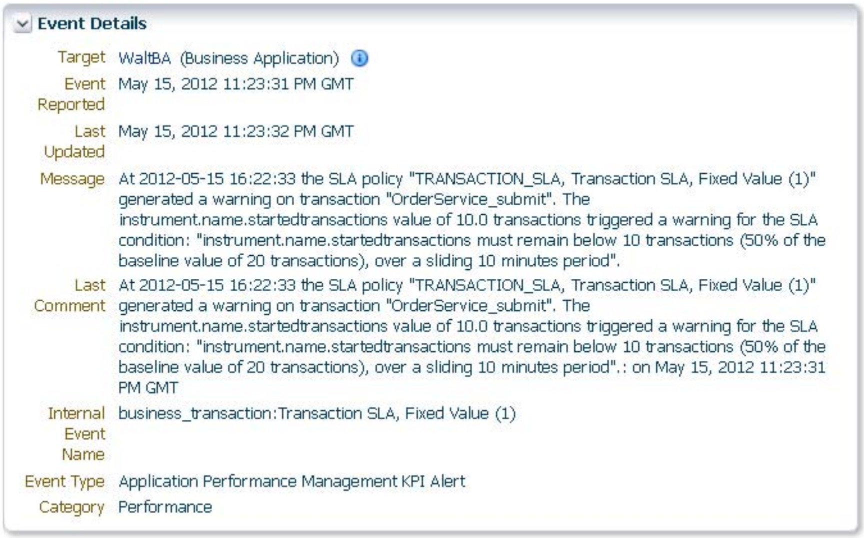
Recorded 20-Jun-2012 21:49:37 CEST

This provides information about the business application associated with the KPI, as well as the metric upon which the KPI is based. Note that for ease of management, KPIs within RUEI are grouped into categories, which can be customized to contain related performance indicators. For example, separate categories could be defined for business and IT-related issues, such as user flow completion, visitor traffic, website availability, and so on.

BTM Event Detail

Information about BTM SLA alerts is shown on the **Alerts** tab and on the **SLA Compliance** tab for BTM. Events corresponding to these alerts are also shown in the **Events Without Incidents** view of the Incident Manager. When you click the event of interest, information similar to that shown in Figure 5–24 is displayed.

Figure 5–24 BTM SLA Alert Event Details



Event Details

Target	WaltBA (Business Application)
Event Reported	May 15, 2012 11:23:31 PM GMT
Last Updated	May 15, 2012 11:23:32 PM GMT
Message	At 2012-05-15 16:22:33 the SLA policy "TRANSACTION_SLA, Transaction SLA, Fixed Value (1)" generated a warning on transaction "OrderService_submit". The instrument.name.startedtransactions value of 10.0 transactions triggered a warning for the SLA condition: "instrument.name.startedtransactions must remain below 10 transactions (50% of the baseline value of 20 transactions), over a sliding 10 minutes period".
Last Comment	At 2012-05-15 16:22:33 the SLA policy "TRANSACTION_SLA, Transaction SLA, Fixed Value (1)" generated a warning on transaction "OrderService_submit". The instrument.name.startedtransactions value of 10.0 transactions triggered a warning for the SLA condition: "instrument.name.startedtransactions must remain below 10 transactions (50% of the baseline value of 20 transactions), over a sliding 10 minutes period".: on May 15, 2012 11:23:31 PM GMT
Internal Event Name	business_transaction:Transaction SLA, Fixed Value (1)
Event Type	Application Performance Management KPI Alert
Category	Performance

Information is provided about the following:

- **Target**: the business application containing the service or transaction for which the event was reported.
- **Event Reported**: the date and time when the event was reported.
- **Last Updated**: if the severity of the event has changed, this indicates the date and time when it has changed.
- **Message**: details about the event and the condition that triggered it.
- **Last Comment**: indicates comments manually added to events via the "Comments..." link in Incident Manager. If none have been added, then the original message is reported.
- **Internal Event Name**: a combination of the managed object type whose threshold was breached (`business_transaction`, `service`, or `service_endpoint`) and the original SLA policy name.
- **Event Type**: this is always "Application Performance Management KPI Alert" for BTM SLA alerts.
- **Category**: this is always "Performance" for BTM SLA alerts.

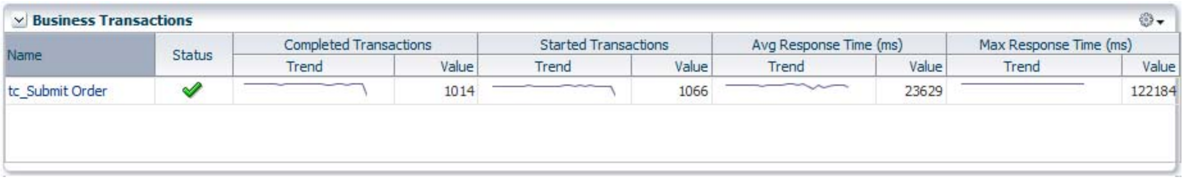
Important

In order for BTM Service Level Agreement alerts to be reported as events in Oracle Enterprise Manager, you must set up a connection between BTM and the EM repository. Please consult the *Business Transaction Management Installation Guide* for instructions on how to configure this connection.

5.10 Monitoring BTM Transactions

The **Business Transactions** region shown on the Business Application page (Figure 5–11) provides a high-level overview of each transaction within the selected business application. An example is shown in Figure 5–25.

Figure 5–25 Business Transactions Region



Business Transactions

Name	Status	Completed Transactions		Started Transactions		Avg Response Time (ms)		Max Response Time (ms)	
		Trend	Value	Trend	Value	Trend	Value	Trend	Value
tc_Submit Order	✓		1014		1066		23629		122184

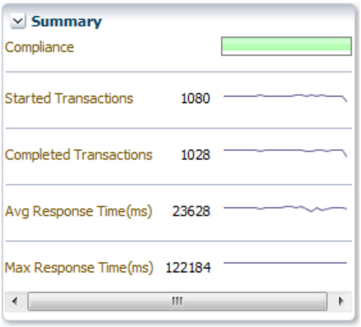
For each transaction, it indicates:

- The transaction's current compliance status.
- The number of transaction instances started during the period. A transaction instance starts when an instance of the primary operation flow is started.
- The number of transaction instances that completed during the period. An instance is considered to have completed when both its start and end messages have been observed, regardless of whether condition alerts occurred.
- The average amount of time a transaction requires to complete. For each transaction instance, this is calculated as the time from when the instance's start message is observed until its end message is observed.
- The maximum amount of time a transaction requires to complete. This is the single highest response time from all transaction instances observed during the period.

You can click a transaction to view more information about it. This opens the Transaction Home page, where you can view the following regions:

- **Summary**: provides a graphic rendering of the transactions' overall compliance and core metrics. An example is shown in Figure 5–26.

Figure 5–26 Summary Region

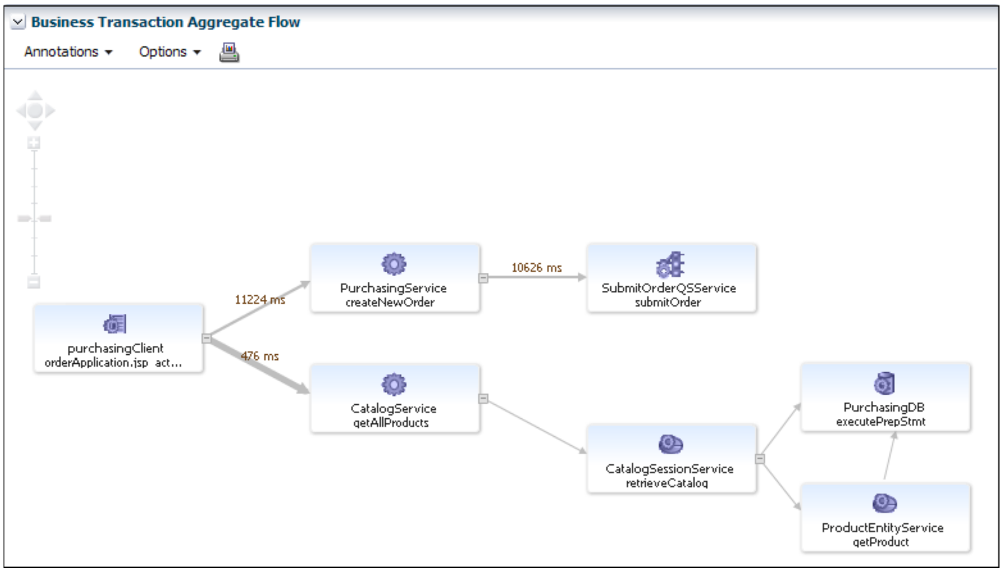


Summary

Compliance	🟩
Started Transactions	1080
Completed Transactions	1028
Avg Response Time(ms)	23628
Max Response Time(ms)	122184

- **Business Transaction Aggregate Flow**: provides a graphical rendering of the operations that make up the selected transaction and their status. An example is shown in Figure 5–27.

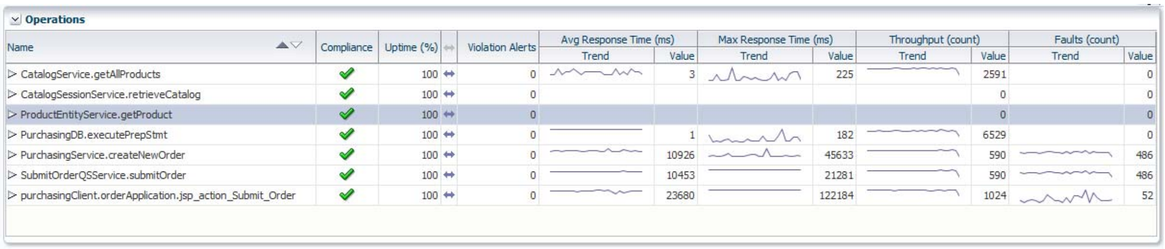
Figure 5–27 Business Transaction Aggregate Flow Region


Business Transaction Aggregate Flow
Annotations
Options
11224 ms
476 ms
10626 ms
purchasingClient orderApplication.jsp act...
PurchasingService createNewOrder
SubmitOrderQSService submitOrder
CatalogService getAllProducts
CatalogSessionService retrieveCatalog
PurchasingDB executePrepStmt
ProductEntityService getProduct

This region provides you with a complete picture of the transaction and helps you understand the flow of work through it. You can use it to identify and resolve issues related to performance, and to isolate the cause of failing components in a business process. Based on the dependencies revealed by discovery, the services that interact within the transaction are also revealed. Additional information is usually available if you move the cursor over the links that connect operations or the operation itself. This should allow you to identify bottlenecks, faulty components, slow components, and unusually light or heavy traffic.

- **Operations**: indicates all the logical operations associated with the transaction. An example is shown in Figure 5–28.

Figure 5–28 Operations Region



Operations

Name	Compliance	Uptime (%)		Violation Alerts	Avg Response Time (ms)		Max Response Time (ms)		Throughput (count)		Faults (count)	
					Trend	Value	Trend	Value	Trend	Value	Trend	Value
▷ CatalogService.getAllProducts	✓	100	↔	0		3		225		2591		0
▷ CatalogSessionService.retrieveCatalog	✓	100	↔	0						0		0
▷ ProductEntityService.getProduct	✓	100	↔	0						0		0
▷ PurchasingDB.executePrepStmt	✓	100	↔	0		1		182		6529		0
▷ PurchasingService.createNewOrder	✓	100	↔	0		10926		45633		590		486
▷ SubmitOrderQSService.submitOrder	✓	100	↔	0		10453		21281		590		486
▷ purchasingClient.orderApplication.jsp_action_Submit_Order	✓	100	↔	0		23680		122184		1024		52

You can expand an operation to view its corresponding endpoints. Note that an operation might have several corresponding endpoints if it has been replicated or if different endpoints are used for secure/unsecure communication. For each endpoint, the host name and port for the container where the endpoint resides are also displayed, together with its status and performance data. If you right click an endpoint in the **Operations** or **Business Transaction Aggregate Flow** region, you can choose to display the tabs associated with the physical operation. The context menu that is displayed when you right-click an operation also provides the option to access the JVMD view or the Request Instance Diagnostics view:

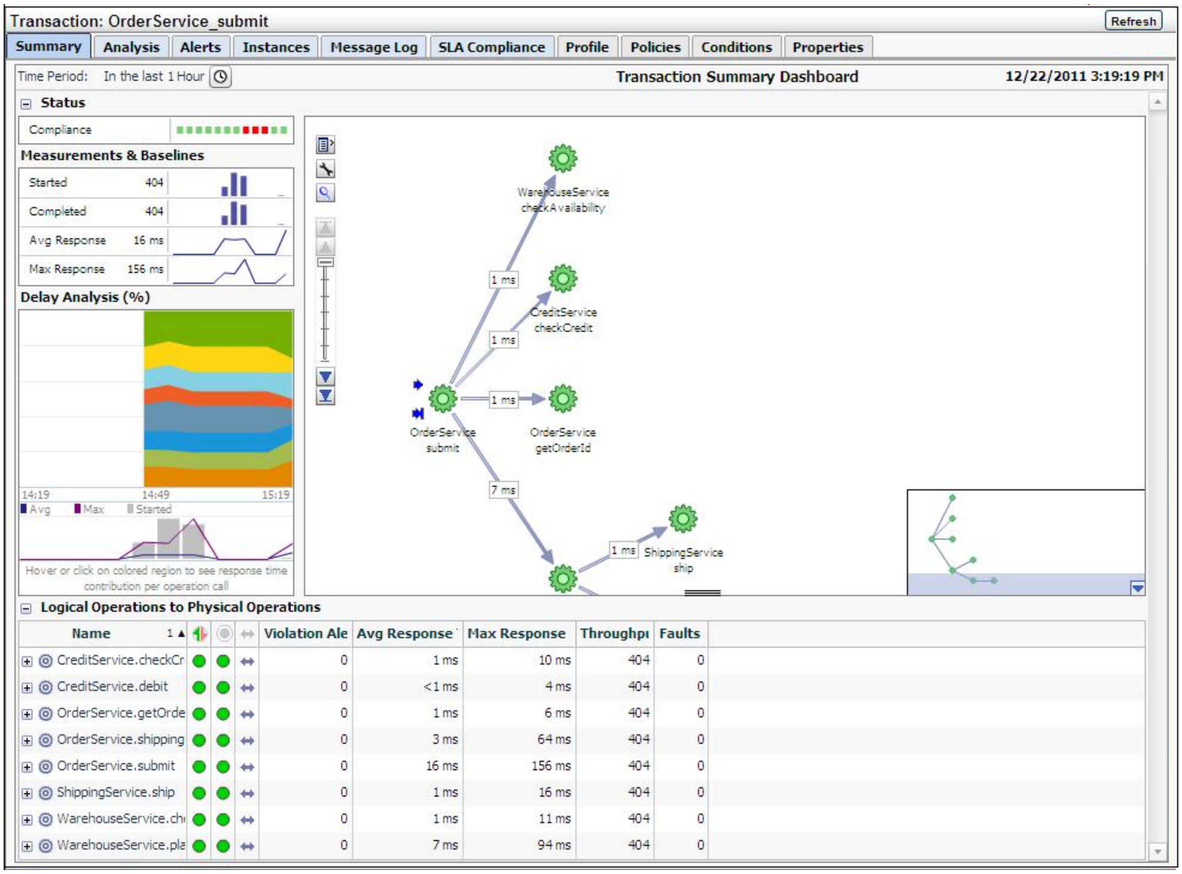
- The **JVM Diagnostics** view allows you to view the details of an executing Java Virtual Machine (JVM) process for the period within which a given operation executes. You can see stack frames for executing threads, thread state information, aggregate information about the frequency and cost of method execution, information regarding the holding of Java and DB locks, and details about the objects in the Java heap. JVMD also stores historical data for each JVM it monitors so that you can view data relating to things that have happened in the past and get a sense for historical trends.
- The **Request Instance Diagnostics** view allows you to trace the path of a request in a WebLogic domain and to generate a report of all the metrics associated with a particular instance of the request.

Please see *Business Transaction Management Online Help* for additional information about these views.

5.11 Working Within Business Transaction Manager

Additional information about a selected transaction is available by clicking **Launch BTM** at the top-right hand of the Transaction Home page. This will open a new window with the Business Transaction Management console providing extended information about the selected transaction. Note that the first time you open this window you will need to provide a valid BTM user name and password. An example is shown in Figure 5–29.

Figure 5–29 Business Transaction Management Console



Transaction: OrderService_submit

Time Period: In the last 1 Hour

Transaction Summary Dashboard

12/22/2011 3:19:19 PM

Status

Compliance	

Measurements & Baselines

Started	404
Completed	404
Avg Response	16 ms
Max Response	156 ms

Delay Analysis (%)

Hover or click on colored region to see response time contribution per operation call

Logical Operations to Physical Operations

Name 1 ▲			↔	Violation Ale	Avg Response	Max Response	Throughpı	Faults
CreditService.checkCr	●	●	↔	0	1 ms	10 ms	404	0
CreditService.debit	●	●	↔	0	<1 ms	4 ms	404	0
OrderService.getOrde	●	●	↔	0	1 ms	6 ms	404	0
OrderService.shipping	●	●	↔	0	3 ms	64 ms	404	0
OrderService.submit	●	●	↔	0	16 ms	156 ms	404	0
ShippingService.ship	●	●	↔	0	1 ms	16 ms	404	0
WarehouseService.ch	●	●	↔	0	1 ms	11 ms	404	0
WarehouseService.pla	●	●	↔	0	7 ms	94 ms	404	0

The following sections describe the Tabs display as they apply to a given transaction; similar information is displayed if you look at tabs for a physical operation. Further information is available from the *Oracle Business Transaction Management Online Help*.

5.11.1 Summary Information

The **Summary** tab uses four panes and a grid view to present performance information in a **Transaction Summary Dashboard**. It contains the following elements:

- A **Status** pane indicating the overall compliance for the transaction.
- A **Measurement and Baselines** pane detailing the number of started and completed transactions, average response times, and maximum response times. If baselines have been defined for the transaction, these are shown as gray lines.
- A map of the transaction detailing average response times for each transaction link. Place the cursor over each service icon to obtain detailed performance information for that service. The thickness of the arrows indicates throughput.
- The **Delay analysis** pane, which you can use in conjunction with the map pane, provides a graphical rendering of the proportion of the overall response time that is spent in each hop (link) of the transaction.

  Each colored area of the grid corresponds to a transaction link. Clicking within a colored region highlights its corresponding link in the map and displays the percentage of the response time taken up by that hop.

  At the bottom of this pane, a graph shows the average and maximum response times, and the number of started transactions. Clicking within the pane displays a vertical red line that shows how the colored proportions correspond to message traffic flows.
- A grid view showing the logical and physical operations that make up the transaction, and the following instruments for each: violation alerts, average response time, maximum response time, throughput, and faults.

5.11.2 Analyzing Transaction Information

The **Analysis** tab displays detailed current performance and usage information for the selected transaction. It contains the panes described in Table 5–1.

Table 5–1 Panes Within Analysis Tab

Pane	Description
Performance	Provides data about started transactions, completed transactions, condition alerts, average response time, and maximum response time. The data is displayed in graphic form as well as using a grid view.
Conditions	Provides information about condition alerts that have been triggered in a given time period: the name of the condition that was met, the endpoint where the condition alert was triggered, and the number of condition alerts triggered. Conditions must have been defined for this information to be collected and displayed.
Consumer Usage	Displays performance information segmented by consumer for the given time period: started transactions, completed transactions, average response time, and maximum response time. Consumers must have been defined and consumer segmentation enabled for this information to be collected and displayed.

Table 5–1 (Cont.) Panes Within Analysis Tab

Pane	Description
Breakdown by Client Address	Displays performance information segmented by client IP address: started transactions, completed transactions, average response time, and maximum response time. The client address is the machine host name from which the request was sent. The table lists all client addresses that sent requests, and displays the aggregated performance measurements associated with each client address. Segmentation by client IP address must be enabled for this data to be collected and displayed.
Violation Alerts	Displays information about service level agreement (SLA) violations. The display distinguishes between warning alerts and failure alerts. The graph shows aggregate measurements for violation alerts. The grid view lists more detailed information: showing alerts for each SLA policy. SLAs must have been created for this information to be collected and displayed.
Custom Charting	Lets you set up a customized chart and table similar to the Performance pane, but with instruments of your choosing. Click **Choose Instruments**, and select the instruments you want displayed in the chart and table. You can select multiple instruments. When you set up a custom chart/table for a transaction, it is available for any selected transaction.
Custom Breakdown	You can set up a custom table of numeric instruments segmented in various ways. Click **Choose Instruments** and select the instruments that you want displayed in the table. Click **Choose Segments** and select how you want to segment the measurements. You can select multiple segments.

5.11.3 Viewing Alerts

The **Alerts** tab shows information about all alerts occurring in the given time period. Business Transaction Management issues the following types of alerts:

- Service level agreement alerts issued when a deviation occurs from the standards of performance you have defined for a transaction.
- Condition alerts issued when a condition is satisfied. Conditions can test for faults, specific property values, or a missing message.
- System alerts issued to provide information about the health of the monitoring infrastructure.

The grid view shows the following information for each alert: time of occurrence, an icon denoting the severity of the alert, the source of the alert, the instrument measured, and for SLA alerts, the enforcement value. To obtain more information about a given alert, click the **Inspector** icon to open an inspector window.

Service level agreement alerts are also reported as events in Incident Manager. For more information on accessing these events, see Section 5.9, "Monitoring KPI and SLA Alert Reporting".

5.11.4 Viewing Transaction Instances

The **Instances** tab allows you to view captured transaction instances.

A transaction usually executes many times in a given period. If you have enabled transaction instance logging or if you have enabled fault monitoring, Business Transaction Management tracks the flow of messages included in the transaction and maps these to particular *transaction instance*s. It assembles the messages for a transaction instance in the following cases:

- When an alert is generated as a result of a fault, or a condition being met.
- When you explicitly ask for assembly.

Once a transaction instance is assembled, you can use the **Instances** tab to access detailed performance information for that instance. You can also use the **Message Log** tab to search for messages containing particular property values.

Viewing Aggregate Information

In the **Instances** tab, The ID column of the table lists both instances that have been assembled (these have an ID value assigned) and instances that have not been assembled (these are blank). Information for each instance shows when it was captured, what the overall response time for the transaction instance was, and values for properties if you have created these.

The **Show instances** filtering control allows you to list instances that have occurred in a set time period or to show only assembled instances.

Which instances you choose to assemble depends on what interests you. For example, you might want to assemble an instance with an unusually slow response time; or you might want to assemble an instance with an unexpected property value.

If you are capturing a very large set of messages, you might want to use the **Message Log** tab to search for a smaller set of messages, based on property values, and then assemble one or more of these.

Inspecting an Assembled Instance

You can assemble an instance by clicking the **Inspector** (magnifying glass icon) for the instance. This opens a **Transaction Instance Inspector**. It consists of three parts:

- The top part of the inspector shows the name of the transaction, the time the assembled instance started executing, its ID, the number of message exchanges, the total messages exchanged, and the response time between the starting and ending messages. Any warnings or faults are also shown.
- The instance map shows the entire transaction instance, with the response time given for each request/response link. Move the cursor over the operation name to view the service type, endpoint name, host name, and port. Right clicking an operation allows you to view JVM diagnostics.
- A grid view shows detailed information for each message included in the transaction instance. The view includes property values if these have been defined. Right clicking a row allows you to view JVM diagnostics.

Clicking the magnifying glass (tear-off control) for any operation, opens a **Message Content** inspector window, and displays the contents of the selected message if you have enabled message content logging for that operation.

5.11.5 Viewing Message Logs

You can use the **Message Log** tab to view the following information:

- If instance logging is enabled, you can view information about each message logged in a specified time period, as well as the value of any property associated with a message. You can also use the **Message Log Search** tool to search for a message or messages that contain property values of interest.
- If message content logging is enabled, you can view information about each message logged in a specified time period, as well as its content. In this case, in addition to searching for messages based on property values, you can also search based on the content of any message element (free text search).

Business Transaction Management logs message content or instance and property values are only available if you have done the following:

- Enabled monitoring for the transaction.
- Enabled the appropriate type of logging for the transaction (instance or message).
- Selected one or more operations for message logging.

Logged information is stored according to storage settings that you define when you create the transaction.

Viewing Message Content

The **Message Log** tab uses a grid view to display a list of messages, showing the arrival time of the request message, the service that includes the selected operation, the location of the endpoint that implements the service, the operation (message), and the type of operation. If there are any properties associated with the operation, their values are shown in additional columns whose title is the property name.

If you have message content logging enabled, double clicking on any message shows you the contents of the message. The set of messages shown in the grid varies depending on the setting of the filters shown at the top of the tab. These allow you to see the following:

- All operations or specific operations chosen from a drop down list.
- Any response, only successful operations, only failures.
- Messages that arrived within a time interval denoted by the last specified time period, since a certain time, or between two given times.

You can use these controls to narrow the selection of messages shown in the grid. After you change filter settings, click **Search** again to repopulate the grid. You can further restrict your search by using the **Message Search tool** accessed from the **Choose Content...** link. This allows you to search for messages based on their property values or, if message content is enabled, based on message content. This tool is described in the next section.

Searching for Messages

You can find messages belonging to the current transaction, by clicking the **Choose Content...** link from the **Message Log** tab. This brings up a dialog that includes three areas to use for specifying search criteria: an area labeled **Message property** search, an area labeled **ECID**, and one labeled **Free text** search. You use controls in these areas to search for a set of messages based on a property value, an ECID value, and/or on text content. As you enter property, ECID, and free-text values, a search expression is constructed in the text box at the top of the dialog. To clear the text box and start over, press **Clear**.

Additional information about using Oracle query language to construct your query is available at the following location:

http://download.oracle.com/docs/cd/B28359_01/text.111/b28304/cqoper.htm#BABBJGFJ

When you are done defining the expression to be used in the search, click **OK**. Then click **Search** to repopulate the grid according to your newly defined search criteria. For more information about the Message Log Search tool for searching for messages with a specific ECID, see the *Business Transaction Management Online Help*.

5.11.6 Viewing Service Level Agreement Compliance

The **SLA Compliance** tab displays the current state of Service Level Agreement (SLA) compliance for the selected transaction. These are specified during transaction creation. You use such agreements to set standards of performance for a business application. You can then monitor deviations from those standards. To view both condition alerts and SLA alerts, use the **Alerts** tab. The SLA Compliance tab has the following subtabs:

- The **Threshold Compliance** subtab provides real-time monitoring of the selected transaction. It uses a grid view. Each row represents one performance objective. The columns provide various types of static information that identify and define the objectives. Also provided are the following dynamic columns with real-time monitoring values:
  - The **Current Status** column can have three possible values: a green circle indicates that the transaction is in SLA compliance, a yellow triangle indicates that the warning threshold for the transaction is currently in violation, and a red diamond indicates that the failure threshold for the objective is currently in violation.
  - The **Value** column displays the current value of the instrument on which the objective is based. Click the magnifying glass next to a value to pop up a chart showing the instrument's recent history.
- The **Baselines** subtab displays historical baseline values for the transaction that you can use as a reference point. Data is shown only if baselines for the selected object have been defined.

5.11.7 Viewing Policies Applied to Transactions

Use the **Policies** tab to view information about policies associated with a transaction. By default, the tab shows information about applied policies. You can use the filter control to view changed policies, disabled policies, pending policies, rejected policies, and unapplied policies. The name of the applied policy is shown in a tree view in the **Name** column. Expanding the policy node shows the following information:

- **Policy Status Details** lists any issues arising from the application of the policy.
- **Monitored Object Type** specifies the targets to which the policy is applied.
- **Location** specifies the address of a target endpoint.
- **Management Intermediary** specifies the Business Transaction Management agent that is applying the policy.

Double clicking the policy name in the **Policy** tab, opens a new window that you can use to view alert, profile, and target information for the selected policy.

5.11.8 Viewing Transaction Profile Information

Use the **Profile** tab to see a map of the transaction and to see its definition. It also provides the following information:

- The date the transaction definition was last modified.
- Any user attributes defined for the transaction.
- The transaction identifier, which is sometimes needed to identify the transaction in CLI commands.

5.11.9 Viewing Transaction Conditions

When you define a transaction, you can associate one or more conditions with the transaction. A *condition* is an expression that Business Transaction Management evaluates against each instance of the transaction. Conditions can test for faults, specific property values, or missing messages. Use the **Condition** tab to display the conditions defined for a transaction. This tab allows you to do the following:

- View the status of fault monitoring: enabled or disabled.
- View condition definitions and status.

Use the **Alerts** tab to see whether any of the conditions have been violated. You cannot change fault monitoring status or condition definitions from the Enterprise Management console.

5.11.10 Viewing Transaction Properties

Properties are variables that hold values associated with the request or response phase of an operation. Properties are commonly used to facilitate searches, to surface message elements without having to log message content, to define conditions, and to enable consumer segmentation. Use the **Properties** tab to display a list of all the properties defined for messages included in a transaction. In addition to listing the properties, the tab shows information about the following:

- The service and operation for which the property is defined.
- The phase (request/response) of the operation.
- The data type of the property value.
- Whether the value is deemed sensitive.
- Whether it is mapped to a consumer (denoted by a human icon on the left) and what consumer-mapped attribute it is associated with.
- A description if you have supplied one when you created the property.

You cannot modify a property value from the Enterprise Management console.

Part II

Monitoring Oracle Exalogic Elastic Cloud

The chapter in this part describes how you can monitor the Oracle Exalogic Elastic Cloud.

The chapter is:

6

Monitoring Oracle Exalogic Elastic Cloud

Oracle Exalogic is an engineered hardware and software system designed to provide the ideal platform for the Oracle Fusion Middleware and business applications. By deploying Exalogic Elastic Cloud, you can increase the performance and efficiency of existing Linux, Solaris and Java applications and improve application and infrastructure reliability, scalability and availability.

The Oracle Exalogic Elastic Cloud is a system consisting of software, firmware and hardware, on which you can deploy Oracle business applications and Oracle Fusion Middleware or software. Exalogic dramatically improves performance of standard Linux, Solaris and Java applications and reduces costs across the application lifecycle.

Oracle Exalogic Elastic Cloud is modeled as a system target rather than a group target within Enterprise Manager Cloud Control. The following targets can comprise the Oracle Exalogic Elastic Cloud:

- Infiniband Network - An Infiniband Network has IB Switches as members. This is a one to many association.
- SOA Infrastructure
- WebLogic Domains
- Coherence Clusters
- OTD
- Hardware Targets (such as PDU, CISCO Switch, ZFS, and ILOMs)

  For more information about adding assets to Exalogic which can then be used for monitoring on Enterprise Manager Cloud Control, refer to the documentation at the link below:

  `http://docs.oracle.com/cd/E27363_01/doc.121/e27511/asset_mgmt.htm#OPCFG4201`
- Hosts

You can use the following sections in this chapter to learn more about how to monitor the Oracle Exalogic Elastic Cloud:

- Prerequisites to Discovering Oracle Exalogic Elastic Cloud
- Using the Exalogic Elastic Cloud Discovery Wizard
- Upgrading Exalogic System Targets to the Version 12.1.0.3 Fusion Middleware Model
- Displaying and Using the Exalogic Elastic Cloud Dashboard
- Refreshing the Exalogic Elastic Cloud

- Monitoring the Hardware Components of Exalogic Elastic Cloud
- Viewing Application Deployments in Exalogic Elastic Cloud Targets
- Viewing WebLogic Domains in Exalogic Elastic Cloud Targets
- Viewing Coherence Clusters in Exalogic Elastic Cloud Targets
- Viewing Hosts in Exalogic Elastic Cloud Targets
- Visualizing Relationships Between Exalogic Software and Hardware Components
- Analyzing the Impact of Component Failures

6.1 Prerequisites to Discovering Oracle Exalogic Elastic Cloud

There are several steps you must perform before you can discover Oracle Exalogic Elastic Cloud in Enterprise Manager Cloud Control. The following sections outline these steps in detail and provide you with the information you need to set up the Exalogic Elastic Cloud targets:

- Importing Ops Center Certificate to the Oracle Management Agent Keystore
- Critical Prerequisites For OVMM Discovery
- ZFS Plug-in and Oracle VM Manager Registration Preconfiguration Steps

6.1.1 Importing Ops Center Certificate to the Oracle Management Agent Keystore

This section provides step-by-step instructions about how to export the certificate from the Enterprise Manager Ops Center keystore and how to import the certificate into the Enterprise Manager agent keystore. These steps are a prerequisite for Exalogic Elastic Cloud discovery in Enterprise Manager Cloud Control.

Use these steps to export the Ops Center Enterprise Controller trust certificate and import it to the Enterprise Manager Cloud Control Management Agent:

1. Change directory to `OPS_AGENT_HOME/oem-ec/security/jsse` where OPS_AGENT_HOME is the path to the Oracle Enterprise Manager Ops Center home. For example, `/etc/opt/sun/cacao2/instances/oem-ec/security/jsse`:

   ```
   [root@localhost~]# cd OPS_AGENT_HOME/oem-ec/security/jsse
   ```

   This directory change is on the VM where the Ops Center Enterprise Controller is running.

2. Export the certificate using keytool that corresponds to the JDK configured to run Ops Center

   ```
   [root@localhost jsse]# $JAVA_HOME/jre/bin/keytool -export
   -alias cacao_agent -file oc.crt -keystore truststore
   -storepass trustpass
   ```

   This command exports the certificate file (oc.crt) in the local directory, for example, `OPS_AGENT_HOME/oem-ec/security/jsse`. In the above command, *trustpass* is the default password for the Ops Center keystore unless changed. The Ops Center Certificate is stored in file *oc.crt*. You can import the Ops Center certificate to the Oracle Management Agent TrustStore using the following steps. The Agent used for communication with Enterprise Manager Ops Center should be running on the same host instance. If it is not, transfer the certificate to the host instance where the agent that you want to configure is running.

3. Change directories to the agent home, where $OMS_AGENT_HOME is the Oracle Management Agent home:

   ```
   cd $OMS_AGENT_
   HOME/core/12.1.0.2.0/stage/sysman/config/montrust
   ```

4. Enter the following command:

   ```
   $OMS_AGENT_HOME/agent_inst/bin/emctl secure add_trust_cert_
   to_jks -trust_certs_loc $CERT_LOC/oc.crt -password welcome
   -alias wlscertgencab
   ```

   Alternatively you can enter this command:

   ```
   [root@localhost montrust]# $JAVA_HOME/jre/bin/keytool -import
   -keystore $OMS_AGENT_
   HOME/core/12.1.0.2.0/stage/sysman/config/montrust/AgentTrust.
   jks -alias wlscertgencab -file $CERT_LOC/oc.crt
   ```

   When prompted, enter the password *welcome* unless changed from the default, and click **Enter**.

   If you follow this step for exporting the certificate, the path to the certificate file will be `OPS_AGENT_HOME/oem-ec/security/jsse/oc.crt`

   Alternatively, you can also do the following:

   a. Export the certificate.

   b. Copy the certificate to `$OMS_AGENT_HOME/core/12.1.0.2.0/stage/sysman/config/montrust`

   c. Change the directory using the following command:

      ```
      cd $OMS_AGENT_
      HOME/core/12.1.0.2.0/stage/sysman/config/montrust
      ```

   d. Run the import command as mentioned. For example:

      ```
      $JAVA_HOME/jre/bin/keytool -import -keystore $OMS_AGENT_
      HOME/core/12.1.0.2.0/stage/sysman/config/montrust/AgentTru
      st.jks -alias wlscertgencab -file oc.crt
      ```

5. To verify that the certificate has been imported correctly, run the following command:

   ```
   [root@localhost montrust]# $JAVA_HOME/jre/bin/keytool -list
   -keystore $OMS_AGENT_
   HOME/core/12.1.0.2.0/stage/sysman/config/montrust/AgentTrust.
   jks
   ```

   You should see the entry for `wlscertgencab alias` you created in the output.

6. After verifying that the certificate has been successfully imported, restart the agent by using the stop and start procedure in the following documentation:

   `http://docs.oracle.com/cd/E25054_01/doc.1111/e24473/emctl.htm#BABEFBDI`

6.1.2 Critical Prerequisites For OVMM Discovery

> **Warning:** Exalogic configurations supporting virtualization must each have Oracle Virtual Machine Manager (OVMM) properly configured for read-only access by Enterprise Manager Cloud Control as a mandatory requirement as described in the following procedure. Failure to configure each Oracle Virtual Machine Manager (OVMM) for read-only access by Enterprise Manager Cloud Control will result in an unsupported configuration. Operations performed in this unsupported configuration may result in software outages and necessitate the re-installation of the Exalogic Control software.

If OVMM was registered with Enterprise Manager Cloud Control prior to performing the OVMM-Enterprise Manager read-only configuration procedure above, then you must choose Synchronize Operation from the OVM Manager Target menu in Enterprise Manager.

You must perform the following steps as a prerequisite to OVMM discovery:

1. Login to OVMM vServer as oracle user, and then perform the commands in the sequence below.
2. `cd /u01/app/oracle/ovm-manager-3/ovm_shell`
3. `sh ovm_shell.sh  --url=tcp://localhost:54321 --username=admin --password=<ovmm admin user password>`
4. `ovm = OvmClient.getOvmManager ()`
5. `f = ovm.getFoundryContext ()`
6. `j = ovm.createJob ( 'Setting EXALOGIC_ID' );`

   The EXALOGIC_ID can be found in the em-context.info on dom0 located in the following file path location:

   `/var/exalogic/info/em-context.info`

   You must log in to dom0 as a root user to obtain this file. For example, if the em-context.info file content is *ExalogicID=Oracle Exalogic X2-2 AK00018758*, then the EXALOGIC_ID will be AK00018758.
7. `j.begin ();`
8. `f.setAsset ( "EXALOGIC_ID", "<Exalogic ID for the Rack>");`
9. `j.commit ();`
10. `Ctrl/d`

You can validate the configuration following these steps by observing that several menus for the *manager/pool/server/guest vm* target are disabled. Specifically, you can validate that OVM Manager is in read-only mode by right-clicking the registered OVM manager under Infrastructure Cloud.

All the active operation menu items in the second and third tier of the list, such as Create Zone, Create Virtual Server Pool, and Manage Network, are disabled (grayed out) and are not available for selection. Conversely, if you choose an item from the pull-down menus that are displayed when you click either the VM Manager or VM Guest menu option, the same menu items may not be grayed out. However, if you select one of the active management options, Enterprise Manager displays an error message stating that the action cannot be performed, thus indicating that the OVM Manager is in read-only mode.

6.1.3 ZFS Plug-in and Oracle VM Manager Registration Preconfiguration Steps

For virtualized Exalogic configurations, there are several preconfiguration steps you must complete. The first configures the Enterprise Manager Cloud Control ZFS plug-in (optional), the second registers the Oracle VM Manager with Enterprise Manager Cloud Control (mandatory), and the third configures the Exalogic Guest Base Template and the Exalogic network.

For non-virtualized Exalogic configurations, the ZFS plug-in can be configured in step one outlined below as part of a recommended but optional configuration:

1. Configure the ZFS Plug-in

   - It is recommended that the agent used for the ZFS configuration reside on the same host as the Exalogic Enterprise Controller. If an Enterprise Manager Cloud Control Agent is not present on the vServer, deploy one using the following documentation:

     http://docs.oracle.com/cd/E24628_01/install.121/e22624/install_agent.htm#CACJEFJI

   - Install and Configure the Enterprise Manager Cloud Control ZFS plug-in using the following documentation:

     http://download.oracle.com/otn/java/oem/Oracle_GC_Plugin_Installguide.html

2. Register the Oracle VM Manager with Enterprise Manager Cloud Control

   - Use the Enterprise Manager Cloud Control Agent deployed on the same vServer as the OVM Manager. If an Enterprise Manager Cloud Control Agent is not present on the vServer please deploy one using the following documentation:

     http://docs.oracle.com/cd/E24628_01/install.121/e24089/part_installing_agent.htm

   - In order to see Exalogic vServers in the Enterprise Manager 12c Exalogic navigation tree you must register the Oracle VM Manager with Enterprise Manager Cloud Control. Please use the following documentation as a guide:

     http://docs.oracle.com/cd/E24628_01/doc.121/e28814/cloud_setup.htm#CEGICIFE

3. As a prerequisite for Enterprise Manager management of a virtual Exalogic configuration the Exalogic Guest Base Template and Exalogic network must be configured according to the following documentation:

   http://docs.oracle.com/cd/E24628_01/doc.121/e35776/emexl.htm

6.2 Using the Exalogic Elastic Cloud Discovery Wizard

You can use the Exalogic Elastic Cloud Discovery wizard to discover and monitor an Exalogic target in Enterprise Manager.

The Exalogic Elastic Cloud Discovery process identifies the targets present in the Exalogic Elastic Cloud and maps them to Enterprise Manager targets, then adds Enterprise Manager targets as Exalogic Elastic Cloud system members.

To use the Exalogic Elastic Cloud Discover wizard, follow these steps:

1. In Enterprise Manager, navigate to the Systems page.
2. From the Add drop-down list, choose **Exalogic Elastic Cloud** and click **Add**.

   Enterprise Manager displays the Discover Exalogic Elastic Cloud page which allows you to enter the parameters and values required to discover an Oracle Exalogic target.
3. Specify a unique **Name** for the Oracle Exalogic target you want to monitor in the Name field.
4. Select an **Agent** on one of the hosts in the Exalogic System to perform the discovery. For virtual Exalogic configurations, select the agent running on the same vServer as the Exalogic enterprise controller. If an Enterprise Manager Cloud Control Agent is not present on the vServer, deploy one using the following documentation:

   `http://docs.oracle.com/cd/E24628_01/install.121/e22624/install_agent.htm#CACJEFJI`

   For non-virtual Exalogic configurations, select an Agent on one of the hosts in the Exalogic System to perform the discovery.

   If you choose an agent that is not part of the Exalogic System, an error message appears stating that no Exalogic Property File can be found and indicating that you must choose an Agent which is on an Exalogic System Host. For a virtual deployment the host may not have the ID.
5. Choose the **Deployment Type** from the drop-down. You can select either **Physical** or **Virtual**.
6. Provide details about the Ops Center Enterprise Controller monitoring the Exalogic Elastic Cloud you want to discover. You must enter information in the **Ops Center Host Name** field, the **Ops Center Port** field, and the credentials in the **Username** and **Password** fields.
7. Click **Next**. Enterprise Manager displays the Discover Oracle Exalogic Targets: Discovered Targets page. The page displays all member targets (such as PDU, Switches, ILOM) that are discovered as part of the system and displays other discovered hardware targets in virtual discovery.
8. Click **Finish** to complete discovery. You can also choose Back to return to the Discover Exalogic Elastic Cloud page or Cancel to terminate the discovery process.

   Enterprise Manager displays a confirmation that the Exalogic Elastic Cloud instance has been added and begins to monitor the Exalogic Elastic Cloud target. The new target is displayed on the Systems page.

6.3 Upgrading Exalogic System Targets to the Version 12.1.0.3 Fusion Middleware Model

You can upgrade the Exalogic System targets discovered in Enterprise Manager version 11 of Grid Control and Enterprise Manager version 12 of Cloud Control to the 12.1.0.3 Fusion Middleware model. Before you upgrade the Exalogic System targets, however, the Management Agent monitoring the Exalogic System target must also be upgraded and the Management Agent should have the version 12.1.0.3 Fusion Middleware Plug-in.

The upgrade job is available as a library job by choosing **Jobs** from the **Enterprise** menu and then selecting **Library**. Select the job name, **Upgrade Exalogic Systems To Fusion Middleware 12.1.0.3.0 Model**. The job can be run more than once. Run this job after upgrading the OMS and the Management Agent monitoring the Exalogic System target. If the job is successful, Enterprise Manager displays a confirmation message indicating that all Exalogic systems have been upgraded and the job is complete. If one or more Management Agents monitoring Exalogic System targets are not upgraded, the job will fail. Under such circumstances, first upgrade those Management Agents and then try submitting this job to upgrade the Exalogic System targets.

6.4 Displaying and Using the Exalogic Elastic Cloud Dashboard

Use the Software tab on the Exalogic Elastic Cloud Dashboard to display status information including alerts and key performance metrics of the following targets in the Exalogic Elastic Cloud:

- Application Deployments
- WebLogic Domains
- Coherence Clusters
- Hosts
- SOA
- OTD

You can also use the Exalogic Elastic Cloud Dashboard page to access the Hardware tab where you can view information about the hardware and infrastructure of the Exalogic Elastic Cloud.

To display and use the Exalogic Elastic Cloud Dashboard, follow these steps:

1. In Enterprise Manager, navigate to the Systems page. Filter the entries in the Search field by choosing **Exalogic Elastic Cloud** from the drop-down list and click **Go**. In the Search Results table, choose the Exalogic Elastic Cloud you want to view.

   Enterprise Manager displays the Exalogic Elastic Cloud Home page where you can monitor the components on the Exalogic Dashboard.

2. You can view detailed information about each software component by choosing the component name from the Exalogic Elastic Cloud drop-down list. Only the software components are visible in the Exalogic drop-down list. Other hardware components can be seen in the Members tab.

   Enterprise Manager displays the component page you selected. For example, select WebLogic Domains Summary page to see the charts showing the status of weblogic servers, Request Processing Time metric information, CPU Usage, Requests per minute, and Heap Usage data.

3. You can return to this page at any time by choosing Home from the Exalogic Elastic Cloud drop-down list.

4. You can display General Information about the Exalogic target by choosing Target Information from the Exalogic Elastic Cloud drop-down list.

6.5 Refreshing the Exalogic Elastic Cloud

You should consider refreshing the system whenever you upgrade the Exalogic Rack, for example, from a quarter to half. You should also consider refreshing when you discover OVMM or ZFS targets after the Exalogic system is discovered. To refresh the Exalogic Elastic Cloud, follow these steps:

1. From the Targets menu, select **Exalogic**.
2. From the list of Exalogic targets, click the Exalogic Elastic Cloud target you want to view.
3. From the Exalogic Elastic Cloud menu, choose **Refresh Exalogic Elastic Cloud**.

   Cloud Control displays a page where you must click **Refresh** to start the refresh action or **Cancel** to cancel. When the refresh action completes, Enterprise Manager displays a Confirmation page that shows the targets found and prompts you to press any button to continue.
4. Click **Close**.

   When you close the Confirmation page, the Discover Exalogic Elastic Cloud: Discovered Targets page appears where you can view all targets associated with the system. You can then click **Add Targets** to save the targets.

6.6 Monitoring the Hardware Components of Exalogic Elastic Cloud

You can monitor the hardware components of an Exalogic Elastic Cloud by following these steps:

1. From the Enterprise Manager Systems page, click the Exalogic Elastic Cloud target from the table. Alternatively, you can choose **Exalogic** from the Targets menu.

   Enterprise Manager displays the Exalogic Elastic Cloud Dashboard page.
2. Click the **Hardware** tab to view a schematic showing the hardware configuration of the Exalogic Elastic Cloud.

   You can use the Hardware tab to view information such as Temperature (by turning on the **Temperature** option at the top of the Exalogic Schematic) and Status, as well as a Hardware Schematic depicting the current state of the hardware.

   The Hardware tab displays the number of hardware units in each category along with their status in the Overview section. It also shows the Incidents associated with the hardware. The Exalogic Schematic depicts the hardware, such as Infiniband Switches, Storage Heads, Storage Disks, and Compute Nodes and employs a Legend that indicates the current state (Up, Down, Unallocated, and so on) of each.

   You can use the Incidents section to monitor hardware issues that arise and then drill down to the Incident Manager page by clicking the **Incident Summary** for more details about the incident.

6.7 Viewing Application Deployments in Exalogic Elastic Cloud Targets

Use the Application Deployments page in the Exalogic Elastic Cloud target area to view details about the applications hosted on the hosts running on the Exalogic Elastic Cloud target.

To view application deployments in Exalogic Elastic Cloud targets, follow these steps:

1. In Enterprise Manager, navigate to the Systems page. Filter the entries in the Search field by choosing **Exalogic Elastic Cloud** from the drop-down list and clicking **Go**. In the Search Results table, choose the Exalogic Elastic Cloud you want to view.

Enterprise Manager displays the Exalogic Elastic Cloud Home page where you can monitor the status of the Exalogic target and its components.

2. Choose **Application Deployments** from the Exalogic Elastic Cloud menu.

   Enterprise Manager displays the Application Deployments page.

3. You can choose to show All Domains or filter by specific domains by choosing the domain from the Show menu.
4. You can drill down to specific applications, targets, domains, or dependencies by clicking on its related value in each row.
5. You can filter the list of applications by choosing a value from the Status drop-down. You can select from Up, Down, Unknown, Blackout, and All.
6. You can change the column appearance of the table by clicking **View** and choosing which Columns to display, expanding or collapsing rows, or scrolling to the first or last row. You can also reorder columns.
7. You can use the Topology tab to display a pictorial view of the Application Deployments in various relational configurations.

6.8 Viewing WebLogic Domains in Exalogic Elastic Cloud Targets

You can use Enterprise Manager to view details about the domains hosted on the virtual machines running on Exalogic Elastic Cloud target. To view WebLogic domains in Exalogic Elastic Cloud targets, follow these steps:

1. In Enterprise Manager, navigate to the Systems page. Filter the entries in the Search field by choosing **Exalogic Elastic Cloud** from the drop-down list and click **Go**. In the Search Results table, choose the Exalogic Elastic Cloud you want to view.

   Enterprise Manager displays the Exalogic Elastic Cloud Home page where you can monitor the status of the Exalogic target and its components.

2. Choose **WebLogics Domain** from the Exalogic Elastic Cloud menu. You can choose to view either a Summary of the WebLogic Domains or specific information about Members.

   Enterprise Manager displays the related WebLogic Domain page.

3. On the Summary page you can view a chart that shows the status of the WebLogic Domains and displays the percentage of domains that are up and down. You can also view server information that shows the Server Status and alert and policy violation information for each. You can monitor charts that display metric information such as Request Processing Time and CPU Usage and you can drill down through these charts for more detailed information. Change the chart view to a table view by clicking **Table View** or **Chart View** beneath each table or chart. The Server table displays information about servers and domains showing host information and related metrics.
4. On the Members page, you can view the Status information along with alerts and policy violation and metric data for each WebLogic Server or Domain. Use the Performance Summary section to view metrics for each, such as Host and Cluster information and metrics such as Heap Usage and Request Processing Time.

6.9 Viewing Coherence Clusters in Exalogic Elastic Cloud Targets

You can use Enterprise Manager Cloud Control to view details about the Coherence targets that comprise the Exalogic Elastic Cloud target. To display Coherence Clusters in Cloud Control, follow these steps:

1. In Enterprise Manager, navigate to the Systems page. Filter the entries in the Search field by choosing **Exalogic Elastic Cloud** from the drop-down list and click **Go**. In the Search Results table, choose the Exalogic Elastic Cloud you want to view.

   Enterprise Manager displays the Exalogic Elastic Cloud Home page where you can monitor the status of the Exalogic target and its components.

2. Choose **Coherence Clusters** from the Exalogic Elastic Cloud menu.

   Enterprise Manager displays the Coherence Clusters page.

3. You can view a chart that shows the status of the Coherence Clusters and displays the percentage of clusters that are up and down.
4. You can drill down to specific values for each cluster such as Alerts and Policy Violations along with Node information.
5. You can filter the list of clusters by choosing a value from the Status drop-down. You can select from Up, Down, Unknown, Blackout, and All.
6. You can change the column appearance of the table by clicking **View** and choosing which Columns to display. You can also reorder columns.
7. The Coherence Clusters page displays two charts showing the Top Nodes With Lowest Available Memory and Caches With Lowest Hit To Get Ratio. You can drill down to specific node information by clicking on the Node name below the Top Nodes With Lowest Available Memory chart.
8. The Nodes table displays information about each Node, including Host and several metric values such as Memory Available, Gets, and Puts.
9. The Applications table displays information about applications such as Local Attribute Cache, Clustered Session Cache, and other metrics. You can drill down to specific information about each application by clicking the Application name.

6.10 Viewing Hosts in Exalogic Elastic Cloud Targets

You can view details about the host targets hosted on the physical and virtual machines running on the Exalogic Elastic Cloud target. To display the hosts information, follow these steps:

1. In Enterprise Manager, navigate to the All Targets page. Filter the entries in the Search field by choosing **Exalogic Elastic Cloud** from the drop-down list and click **Go**. In the Search Results table, choose the Exalogic Elastic Cloud you want to view.

   Enterprise Manager displays the Exalogic Elastic Cloud Home page where you can monitor the status of the Exalogic target and its components.

2. Choose **Hosts** from the Exalogic Elastic Cloud menu.

   Enterprise Manager displays the Hosts page.

3. You can view a chart that shows the status of the hosts and displays the percentage of hosts that are up and down.

4. You can view information about the Middleware Targets that lists the Type, Status, CPU Utilization percentage, Memory Utilization percentage, and Incident statistics along with Configuration Changes.
5. You can view charts showing the CPU Utilization percentage based on time and similarly, Memory Utilization based on time.

6.11 Visualizing Relationships Between Exalogic Software and Hardware Components

Use Enterprise Manager Cloud Control to visualize relationships among Exalogic software and hardware components. To see the routing topology among these components, follow these steps:

1. From the Targets menu, select **Exalogic**.
2. From the list of Exalogic targets, click the Exalogic Elastic Cloud target you want to view.
3. From the Exalogic Elastic Cloud menu, select **Routing Topology**.
4. View the relationships between Exalogic software and hardware components.

6.12 Analyzing the Impact of Component Failures

You can analyze the impact of component failures in an Exalogic environment by following these steps:

1. From the Targets menu, select **Exalogic**.
2. From the list of Exalogic targets, click the Exalogic Elastic Cloud target you want to view.
3. From the navigation panel, click the Oracle Infiniband Network you want to view.
4. From the Infiniband Network menu, select **Topology**.
5. Identify any problems with a component by observing status and incident badges, or by showing metric values by way of the Annotations toolbar menu.
6. Identify components linked to the problem component in the diagram.

6.13 Configuring Exalogic Oracle Engineered System Healthchecks

For more information about configuring Exalogic Oracle-engineered system healthchecks, see the *Oracle Enterprise Manager System Monitoring Plug-In Installation Guide for Oracle Engineered System Healthchecks*.

Part III

Monitoring WebLogic Domain

The chapter in this part describes how you can monitor the Oracle WebLogic Domain.

This chapter is:

- Chapter 7, "Monitoring WebLogic Domains"

7

Monitoring WebLogic Domains

When using Enterprise Manager version 12.1 and a Secure Socket Layer (SSL) protocol to discover and monitor WebLogic servers, the Intelligent Agent must be able to *trust* the server before it can establish a secure communication link. The Agent maintains a Java Keystore (JKS) truststore containing certificates of Certification Authorities (CAs) which it can trust when establishing a secure connection. The Agent comes with nine well-known CA certificates.

It is recommended that customers using WebLogic t3s in a production environment use certificates signed by a well-known Certification Authority (CA), such as VeriSign or Thawte, on their WebLogic servers. A few popular Root CA certificates are available out-of-box in the Agent's JKS-based truststore and does not require any action by the customer. However, if self-signed certificates or the default (out-of-box) demo certificate are being used on the Weblogic servers, then the following step is needed to explicitly import the Root CA certificate for these server certificates to the Agent's truststore.

The JKS Agent truststore is located at the following location:

```
$ORACLE_HOME/sysman/config/montrust/AgentTrust.jks
```

Note: ORACLE_HOME is the Management Agent's instance home.

Updating the Agent truststore is required on ALL Enterprise Manager Agents involved in the discovery and monitoring of the WebLogic domain using any secure protocol.

7.1 Updating the Agent Truststore

To update the Agent truststore (AgentTrust.jks), you use EMCTL. If the default demo certificate, or a self-signed certificate is being used on the WebLogic servers for t3s/iiops, then the Root CA certificate for this must be added to AgentTrust.jks in order for the Agent to be able to discover and monitor these WebLogic servers and J2EE applications using t3s. An EMCTL command is provided for this purpose.

```
emctl secure add_trust_cert_to_jks [-password <password> -trust_certs_loc <loc>
-alias <alias>]
```

Where:

- password = password to the AgentTrust.jks (if not specified, you will be prompted for the password at the command line)
- trust_certs_loc = location of the certificate file to import
- alias = alias for the certificate to import

7.1.1 Importing a Demo WebLogic Server Root CA Certificate.

To import the Root CA certificate for a Demo WebLogic server into the Agent's truststore, the EMCTL *secure* command needs to be executed from the host on which the Agent is located.

```
<ORACLE_HOME>/bin/emctl secure add_trust_cert_to_jks -password "welcome"
```

Note: ORACLE_HOME is the Management Agent's instance home.

The following example demonstrates a typical session using the secure command with the *add_trust_cert_to_jks* option.

Example 7–1 Sample Session

```
./emctl secure add_trust_cert_to_jks -password welcome
Oracle Enterprise Manager 12c Release 1 Cloud Control 12.1.0.2.0
Copyright (c) 1996, 2012 Oracle Corporation.  All rights reserved.

Message   :   Certificate was added to keystore
ExitStatus: SUCCESS
```

The default out-of-box password for the AgentTrust.jks is "welcome" and it is recommended that this be changed using the JDK keytool utility. If no password is specified along with the EMCTL command, the system will prompt you for the password.

7.1.2 Importing a Custom Root CA Certificate

If the WebLogic servers are secured with another certificate, such as a self-signed certificate, then that Root CA certificate must be imported into the Agent's truststore as follows:

```
<ORACLE_HOME>/bin/emctl secure add_trust_cert_to_jks -password "welcome" trust_
certs_loc <location of certificate> -alias <certificate-alias>
```

Note: ORACLE_HOME is the Management Agent's instance home.

7.2 Changing the Default AgentTrust.jks Password Using Keytool

The following JVM keytool utility command will let you change the default out-of-box password to the AgentTrust.jks.

```
<ORACLE_HOME>/jdk/bin/keytool -storepasswd -keystore AgentTrust.jks -storepass
welcome -new myNewPass
```

Note: ORACLE_HOME is the Management Agent's instance home.

7.3 Collecting JVM Performance Metrics for WebLogic Servers

In order to collect JVM performance metrics from platform MBeans, the Mbeans must be made accessible via the runtime MBeanServer. To do this, from the WebLogic console, set **PlatformMBeanServerEnabled=true**. *Domain->Advanced*

> **Note:** This only applies to WebLogic server installations where Java Required Files (JRF) are not installed.

7.3.1 Setting the PlatformMBeanServerUsed Attribute

If you are using WebLogic server versions 9.2.0.40, 10.0.2.0, 10.3.1 and 10.3.2 and certain patch releases of 9.x, you must explicitly set the *PlatformMBeanServerUsed* attribute to *TRUE* in addition to setting the *PlatformMBeanServerEnabled* (shown in the previous section). You set the *PlatformMBeanServerUsed* attribute using the WebLogic Scripting Tool (WLST), as shown in the next section.

> **Note:** From WebLogic server versions 10.3.3 onwards, the default out-of-box behavior enables platform MBeans to be accessible via runtime MBeanServers. Hence, this section can be skipped.

7.3.2 Activating Platform MBeans on WebLogicServer 9.x to 10.3.2 versions

The following WebLogic Scripting Tool session shown in Example 7–2 demonstrates how to use check and set the PlatformMBeanServerUsed attribute.

User actions are shown in bold.

Example 7–2 Setting PlatformMBeanServerUsed

```
cd common/bin/

ade:[ adminsw_easvr ] [adminsw@mymachine bin]$ ./wlst.sh

CLASSPATH=/net/mymachine/scratch/shiphomes/wl/wl10/patch_
wls1002/profiles/default/sys_manifest_classpath/weblogic_
patch.jar:/net/mymachine/scratch/shiphomes/wl/wl10/patch_
cie640/profiles/default/sys_manifest_classpath/weblogic_
patch.jar:/net/mymachine/scratch/shiphomes/wl/wl10/jrockit_150_
15/lib/tools.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/weblogic_sp.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/weblogic.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/feat
ures/weblogic.server.modules_
10.0.2.0.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/features/com.bea.cie
.common-plugin.launch_
2.1.2.0.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/webservices.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/o
rg.apache.ant_
1.6.5/lib/ant-all.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/net.sf.antc
ontrib_1.0b2.0/lib/ant-contrib.jar:

PATH=/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/bin:/net/mymachine/scratch/shiphomes/wl/wl10/modules/org.apache.ant_
1.6.5/bin:/net/mymachine/scratch/shiphomes/wl/wl10/jrockit_150_
15/jre/bin:/net/mymachine/scratch/shiphomes/wl/wl10/jrockit_150_
15/bin:/home/adminsw/products/valgrind/bin:/ade/adminsw_
easvr/oracle/jdk/bin:/ade/adminsw_
easvr/oracle/work/middleware/oms/perl/bin:/bin:/usr/local/bin:/usr/local/remote/pa
ckages/firefox-1.5.0.3:/ade/adminsw_easvr/oratst/bin:/ade/adminsw_
easvr/oracle/buildtools/bin:/ade/adminsw_easvr/oracle/emdev/merge:/ade/adminsw_
easvr/oracle/emdev/utl:/ade/adminsw_easvr/oracle/utl:/pdp/pds/utl:/ade/adminsw_
easvr/oracle/work/middleware/oms/bin:/ade/adminsw_
easvr/oracle/nlsrtl3/bin:/opt/SUNWspro/bin:/usr/ccs/bin:/usr/bin:/usr/sbin:/ade/ad
minsw_
easvr/oracle/opmn/bin:/usr/X11R6/bin:/home/adminsw/products/valgrind/bin:/home/adm
insw/products/valgrind/bin:/usr/kerberos/bin:/home/adminsw/products/valgrind/bin:/
bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin:/usr/local/ade/bin:/bin:/usr/local/bin
```

```
Your environment has been set.

CLASSPATH=/net/mymachine/scratch/shiphomes/wl/wl10/patch_
wls1002/profiles/default/sys_manifest_classpath/weblogic_
patch.jar:/net/mymachine/scratch/shiphomes/wl/wl10/patch_
cie640/profiles/default/sys_manifest_classpath/weblogic_
patch.jar:/net/mymachine/scratch/shiphomes/wl/wl10/jrockit_150_
15/lib/tools.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/weblogic_sp.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/weblogic.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/feat
ures/weblogic.server.modules_
10.0.2.0.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/features/com.bea.cie
.common-plugin.launch_
2.1.2.0.jar:/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/server/lib/webservices.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/o
rg.apache.ant_
1.6.5/lib/ant-all.jar:/net/mymachine/scratch/shiphomes/wl/wl10/modules/net.sf.antc
ontrib_
1.0b2.0/lib/ant-contrib.jar::/net/mymachine/scratch/shiphomes/wl/wl10/wlserver_
10.0/common/eval/pointbase/lib/pbembedded51.jar:/net/mymachine/scratch/shiphomes/w
l/wl10/wlserver_
10.0/common/eval/pointbase/lib/pbtools51.jar:/net/mymachine/scratch/shiphomes/wl/w
l10/wlserver_10.0/common/eval/pointbase/lib/pbclient51.jar

Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline>

wls:/offline> connect('weblogic','welcome1','mymachine:7501')
Connecting to t3://mymachine:7501 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain 'base_
domain'.

Warning: An insecure protocol was used to connect to the server. To ensure
on-the-wire security, the SSL port or Admin port should be used instead.

wls:/base_domain/serverConfig> edit()
Location changed to edit tree. This is a writable tree with DomainMBean as the
root. To make changes you will need to start an edit session via startEdit().

For more help, use help(edit)

wls:/base_domain/edit> startEdit()
Starting an edit session ...
Started edit session, please be sure to save and activate your changes once you
are done.

wls:/base_domain/edit !> cd('JMX')

wls:/base_domain/edit/JMX !> ls()
drw-   base_domain

wls:/base_domain/edit/JMX !> cd ('base_domain')

wls:/base_domain/edit/JMX/base_domain !> ls()
-rw-   CompatibilityMBeanServerEnabled              true
```

```
-rw-   DomainMBeanServerEnabled                     true
-rw-   EditMBeanServerEnabled                       true
-rw-   InvocationTimeoutSeconds                     0
-rw-   ManagementEJBEnabled                         true
-rw-   Name                                         base_domain
-rw-   Notes                                        null
-rw-   PlatformMBeanServerEnabled                   true
-rw-   PlatformMBeanServerUsed                      false **
-rw-   RuntimeMBeanServerEnabled                    true
-r--   Type                                         JMX

-r-x   freezeCurrentValue                           Void : String(attributeName)
-r-x   isSet                                        Boolean : String(propertyName
)
-r-x   restoreDefaultValue                          Void : String(attributeName)
-r-x   unSet                                        Void : String(propertyName)

wls:/base_domain/edit/JMX/base_domain !> set('PlatformMBeanServerUsed','true')
wls:/base_domain/edit/JMX/base_domain !> ls()

-rw-   CompatibilityMBeanServerEnabled              true
-rw-   DomainMBeanServerEnabled                     true
-rw-   EditMBeanServerEnabled                       true
-rw-   InvocationTimeoutSeconds                     0
-rw-   ManagementEJBEnabled                         true
-rw-   Name                                         base_domain
-rw-   Notes                                        null
-rw-   PlatformMBeanServerEnabled                   true
-rw-   PlatformMBeanServerUsed                      true  **
-rw-   RuntimeMBeanServerEnabled                    true
-r--   Type                                         JMX
-r-x   freezeCurrentValue                           Void : String(attributeName)
-r-x   isSet                                        Boolean : String(propertyName
)
-r-x   restoreDefaultValue                          Void : String(attributeName)
-r-x   unSet                                        Void : String(propertyName)

wls:/base_domain/edit/JMX/base_domain !> activate()
Activating all your changes, this may take a while ...
The edit lock associated with this edit session is released once the activation is
completed.

The following non-dynamic attribute(s) have been changed on MBeans
that require server re-start: **
MBean Changed : com.bea:Name=base_domain,Type=JMX
Attributes changed : PlatformMBeanServerUsed

Activation completed
wls:/base_domain/edit/JMX/base_domain> ade:[ adminsw_easvr ] [adminsw@mymachine
bin]$
ade:[ adminsw_easvr ] [adminsw@mymachine bin]$
```

****NOTE**: *PlatformMBeanServerUsed* attribute is present in WebLogic releases 10.3.1.0 and 10.3.2.0 and also for certain patch releases of prior versions. If above *PlatformMBeanServerUsed* attribute is NOT present, or if it is present and already set to true, then running the commands are not necessary.

Part IV

Managing Oracle SOA

The chapters in this part describe how you can discover and monitor Oracle BPEL Process Manager, Oracle Service Bus, and Oracle SOA Suite.

The chapters are:

- Chapter 8, "Overview of Oracle SOA Management"
- Chapter 9, "Discovering and Monitoring Oracle BPEL Process Manager"
- Chapter 10, "Discovering and Monitoring Oracle Service Bus"
- Chapter 11, "Discovering and Monitoring the SOA Suite"

8

Overview of Oracle SOA Management

The Oracle SOA Management Pack Enterprise Edition delivers comprehensive management capabilities for a Service-Oriented Architecture-based (SOA) environment. By combining SOA runtime governance, business-IT alignment, and SOA infrastructure management with Oracle's rich and comprehensive system management solution, Enterprise Manager Cloud Control significantly reduces the cost and complexity of managing SOA-based environments.

Table 8–1 Highlights of Oracle SOA Management Pack Enterprise Edition

Feature	Benefit
Centralized management console	Provides administrators managing SOA environments with a consolidated browser-based view of the entire enterprise, thereby enabling them to monitor and manage all of their components from a central location.
Discovery and service modeling	Provides discovery of the following: ■ Oracle SOA Infrastructure deployed to the WebLogic Server. ■ Oracle SOA Composite applications deployed to the SOA Infrastructure. ■ Oracle BPEL processes deployed to the Oracle BPEL Process Manager (BPEL Process Manager) server and the dependent partner links. ■ Oracle Service Bus-based business and proxy services. ■ Service modeling offers out-of-the-box automated system modeling capabilities for the SOA infrastructure.
Runtime governance	Defines SOAP tests to measure and record availability and performance of partner links (or any Web service) and business/proxy services for historical trending, troubleshooting, and root cause analysis purposes. Also provides an error hospital of process instances with drill-downs into instance details.
Infrastructure management	Monitors the availability and performance of the SOA infrastructure components. Both current and historic availability of targets (such as BPEL Process Manager or Oracle Service Bus) are recorded for troubleshooting and root cause analysis.
Configuration management	Collects configuration information for the BPEL Process Manager server/domains/processes and Oracle Service Bus. The parameters can be refreshed, saved, or compared with another target. Different versions of the same target can also be compared.
Deployment automation	Automates the deployment of the following: ■ SOA Artifacts Provisioning: This includes provisioning of SOA Composites, Oracle WebLogic Server Policies, Assertion Templates, and JPS Policy and Credential Stores. ■ BPEL processes on BPEL Process Managers ■ Oracle Service Bus resources from a source OSB domain to a target OSB domain. For detailed information on the provisioning procedures, see *Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching*.
Adapter metrics	Provides throughput and error metrics for different adapters in graphical format.
Business-IT alignment	Enables you to consolidate their IT and business management tools into a unified system. BAM-EM integration unites business KPIs and system metrics in one system for correlation and trending.

Table 8–1 (Cont.) Highlights of Oracle SOA Management Pack Enterprise Edition

Feature	Benefit
Service level management	Enables you to monitor services from the end-user’s perspective using service tests or synthetic transactions, model relationships between services and underlying IT components, and report on achieved service levels.
Application Dependency and Performance	Enables you to manage your SOA solutions by leveraging a model-driven top-down approach within your development, quality assurance (QA), staging, and production environments. Business application owners and operational staff can automatically discover your BPEL workflows and correlate them with the underlying Web services; Enterprise Service Buses (ESBs); and back-end Java 2 Platform, Enterprise Edition (Java EE) resources through detailed modeling and drill-down directly into the performance metrics at the component level. For more information, see Chapter 21, "Introduction to Application Dependency and Performance"
Historical analysis and reporting	Store the collected metric and configuration data in a central repository, thereby enabling administrators to analyze metrics through various historical views and facilitate strategic trend analysis and reporting.
Instance Tracing	Allows you to trace the message flow across SOA Composites and SOA Infrastructure instances monitored by Enterprise Manager Cloud Control.
Business Transaction Management	Provides monitoring of business transactions as they flow across tiers and continuous discovery of components, transaction flow, service dependencies and relationships.
Dehydration Store	Shows the performance of the database that is used by the SOA Infrastructure. Using this data, the SOA administrator can identify problems that are causing the performance bottleneck.

9 Discovering and Monitoring Oracle BPEL Process Manager

This chapter describes how you can discover and monitor Oracle BPEL Process Manager (BPEL Process Manager) using Enterprise Manager Cloud Control.

In particular, this document covers the following:

- Supported Versions
- Understanding the Discovery Mechanism
- Understanding the Discovery Process
- Setting Up Oracle Software Library
- Discovering BPEL Process Manager
- Configuring BPEL Process Manager
- Troubleshooting BPEL Process Managers

9.1 Supported Versions

The following are the versions of BPEL Process Manager that are supported for monitoring in Enterprise Manager Cloud Control.

Table 9–1 Supported Versions

Supported BPEL Process Manager Version	Application Server Deployed To	Supported in Enterprise Manager
Oracle BPEL Process Manager 10.1.2	Oracle Application Server 10g Release 1 (10.1.2)	Enterprise Manager 10g Release 4 (10.2.0.4) or higher Enterprise Manager 11g Enterprise Manager 12c
Oracle BPEL Process Manager 10.1.3.1 and 10.1.3.3 *(Part of Oracle SOA Suite 10.1.3.1 and 10.1.3.3)*	Oracle Application Server 10g Release 1 (10.1.3.1) and (10.1.3.3)	Enterprise Manager 10g Release 3 (10.2.0.3) or higher Enterprise Manager 11g Enterprise Manager 12c
Oracle BPEL Process Manager 10.1.3.1 and 10.1.3.3 *(Part of Oracle SOA Suite 10.1.3.1 and 10.1.3.3)*	Oracle WebLogic Managed Server 9.2	Enterprise Manager 10g Release 5 (10.2.0.5) or higher Enterprise Manager 10 g Release 4 (10.2.0.4) with one-off patches applied. For details, see Section 9.3, "Understanding the Discovery Process". Enterprise Manager 11g Enterprise Manager 12c

Table 9–1 (Cont.) Supported Versions

Supported BPEL Process Manager Version	Application Server Deployed To	Supported in Enterprise Manager
Oracle BPEL Process Manager 10.1.3.1 and 10.1.3.3 *(Part of Oracle SOA Suite 10.1.3.1 and 10.1.3.3)*	IBM WebSphere Application Server 6.1	Enterprise Manager 10g Release 5 (10.2.0.5) or higher Enterprise Manager 10g Release 4 (10.2.0.4) with one-off patches applied. For details, see Section 9.3, "Understanding the Discovery Process". Enterprise Manager 11g Enterprise Manager 12c
Oracle BPEL Process Manager 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.4)*	Oracle Application Server 10g Release 1 (10.1.3.1) and (10.1.3.3)	Enterprise Manager 10g Release 5 (10.2.0.5) or higher Enterprise Manager 11g Release 1 (11.1.0.1) Enterprise Manager 12c
Oracle BPEL Process Manager 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.4)*	Oracle WebLogic Managed Server 9.2	Enterprise Manager 10g Release 5 (10.2.0.5) or higher Enterprise Manager 11g Enterprise Manager 12c
Oracle BPEL Process Manager 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.4)*	IBM WebSphere Application Server 6.1	Enterprise Manager 10g Release 5 (10.2.0.5) or higher Enterprise Manager 11g Enterprise Manager 12c

9.2 Understanding the Discovery Mechanism

The following describes the mechanism followed for discovering BPEL Process Managers in Enterprise Manager Cloud Control.

Table 9–2 Mechanism for Discovering BPEL Process Managers

BPEL Process Manager Version	Application Server Deployed To	Discovery Mechanism	Process
Oracle BPEL Process Manager 10.1.2	Oracle Application Server 10g Release 1 (10.1.2)	Manual/Automatic Discovery	■ If the Management Agent is installed before Oracle Application Server and BPEL Process Manager are installed, then you must **manually discover** that Oracle Application Server and BPEL Process Manager in Enterprise Manager Cloud Control. ■ If the Management Agent is installed after Oracle Application Server and BPEL Process Manager are installed, then Enterprise Manager Cloud Control **automatically discovers** that Oracle Application Server and BPEL Process Manager The Management Agent can be installed along with Enterprise Manager Cloud Control or separately as a standalone product. For discovery procedures, see Section 9.5.1, "Deployed to Oracle Application Server".
Oracle BPEL Process Manager 10.1.3.1, 10.1.3.3, 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.1, 10.1.3.3, 10.1.3.4)*	Oracle Application Server 10g Release 1 (10.1.3.1) and (10.1.3.3)	Manual/Automatic Discovery	■ If the Management Agent is installed before Oracle Application Server and BPEL Process Manager are installed, then you must **manually discover** that Oracle Application Server and BPEL Process Manager in Enterprise Manager Cloud Control. ■ If the Management Agent is installed after Oracle Application Server and BPEL Process Manager are installed, then Enterprise Manager Cloud Control **automatically discovers** that Oracle Application Server and BPEL Process Manager The Management Agent can be installed along with Enterprise Manager Cloud Control or separately as a standalone product. For discovery procedures, see Section 9.5.1, "Deployed to Oracle Application Server".

Table 9–2 (Cont.) Mechanism for Discovering BPEL Process Managers

BPEL Process Manager Version	Application Server Deployed To	Discovery Mechanism	Process
Oracle BPEL Process Manager 10.1.3.1, 10.1.3.3, 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.1, 10.1.3.3, 10.1.3.4)*	Oracle WebLogic Managed Server 9.2	Manual Discovery	First, manually discover Oracle WebLogic Managed Server. For procedures, see Section 9.5.2.1, "Discovering Oracle WebLogic Managed Server". Then, manually discover BPEL Process Manager. For procedures, see Section 9.5.2.2, "Deployed to Oracle WebLogic Managed Server".
Oracle BPEL Process Manager 10.1.3.1, 10.1.3.3, 10.1.3.4 *(Part of Oracle SOA Suite 10.1.3.1, 10.1.3.3, 10.1.3.4)*	IBM WebSphere Application Server 6.1	Manual Discovery	First, manually discover IBM WebSphere Application Server. For procedures, see Section 9.5.3.1, "Discovering IBM WebSphere Application Server". Then, manually discover BPEL Process Manager. For procedures, see Section 9.5.3.2, "Deployed to IBM WebSphere Application Server".
Oracle BPEL Process Manager 10.1.3.5	Oracle WebLogic Managed Server 10.x	Manual Discovery	First, manually discover Oracle WebLogic Managed Server. For procedures, see Section 9.5.2.1, "Discovering Oracle WebLogic Managed Server". Then, manually discover BPEL Process Manager. For procedures, see Section 9.5.2.2, "Deployed to Oracle WebLogic Managed Server".

9.3 Understanding the Discovery Process

The following describes the overall process involved in discovering and monitoring BPEL Process Manager in Enterprise Manager Cloud Control. Follow the instructions outlined against each step in this process to successfully discover and monitor your BPEL Process Manager.

Table 9–3 Discovery Process

Step	Requirement	Description

1	BPEL Process Manager	Install the BPEL Process Manager software in one of the following ways:
		■ For Oracle middleware, download and install the BPEL Process Manager using Oracle BPEL Process Manager 10.1.2, Oracle SOA Suite 10.1.3.1, 10.1.3.3, or 10.1.3.4 from the following URL:
		`http://www.oracle.com/technology/software/tech/soa/index.html`
		■ For non-Oracle middleware, download and install the BPEL Process Manager from the following URL:
		`http://www.oracle.com/technology/software/products/ias/bpel/index.html`

2	Enterprise Manager Cloud Control	To monitor BPEL Process Manager 10.x, install Enterprise Manager Cloud Control 12c. For information about installing the base release of Enterprise Manager Cloud Control, see the *Enterprise Manager Cloud Control Installation and Basic Configuration Guide* available at: `http://www.oracle.com/technology/documentation/oem.html` Oracle recommends that you install the Enterprise Manager Cloud Control components on a host that is different from the host where the BPEL Process Manager is installed. For example, if the BPEL Process Manager is installed on host1.xyz.com, then install and configure Oracle Management Service (OMS) and the Management Repository on host2.xyz.com.

Table 9–3 (Cont.) Discovery Process

Step	Requirement	Description

3	Oracle Management Agent
	(Management Agent)
		Install Oracle Management Agent 12c or higher on every host where BPEL Process Manager is installed.
		If Oracle Application Server/BPEL Process Manager and Enterprise Manager Cloud Control are all on the same host, then you do not have to install a separate Management Agent. The Management Agent that comes with Enterprise Manager Cloud Control is sufficient. However, if they are different hosts, then you must install a separate Management Agent on every host where BPEL Process Manager is installed.
		You can install the Management Agent in one of the following ways:
		■ Invoke the installer provided with Enterprise Manager 10*g* Cloud Control Release 3 (10.2.0.3) or higher, and select the installation type **Additional Management Agent**.
		■ Use the Agent Deploy application within the Cloud Control console.
		■ Use the full agent kit that is available at:
		`http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`
		For information about installing the Management Agent, see the *Enterprise Manager Cloud Control Installation and Basic Configuration Guide* available at:
		`http://www.oracle.com/technology/documentation/oem.html`

4	Discovery in Enterprise Manager Cloud Control	BPEL Process Managers deployed to Oracle Application Servers are automatically discovered in Enterprise Manager Cloud Control. BPEL Process Managers deployed to Oracle WebLogic Managed Servers and IBM WebSphere Application Servers must be manually discovered in Enterprise Manager Cloud Control. For procedures to discover them, see Section 9.5, "Discovering BPEL Process Manager".

9.4 Setting Up Oracle Software Library

If you are using Enterprise Manager 12c to discover and monitor the BPEL Process Manager deployed to Oracle WebLogic Managed Server 9.2 and IBM WebSphere Application Server 6.1, you must set up Oracle Software Library (Software Library) as described below:

To set up the Software Library:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the **Actions** menu, select **Administration**.
3. In the Software Library: Administration page, select the Storage Type and click **Add** from the Actions menu.
4. In the Add Software Library Location window, specify a valid directory path where you want to store the raw data for the components, and click **OK**.

> **Note:** For more information about setting up the Software Library, see the *Enterprise Manager Advanced Installation and Configuration Guide* available at the following URL:
>
> `http://www.oracle.com/technology/documentation/oem.html`

9.5 Discovering BPEL Process Manager

This section describes the procedures for discovering BPEL Process Managers. In particular, this section covers the following:

- Deployed to Oracle Application Server
- Deployed to Oracle WebLogic Managed Server

- Deployed to IBM WebSphere Application Server

9.5.1 Deployed to Oracle Application Server

A BPEL Process Manager deployed to Oracle Application Server is manually or automatically discovered in Enterprise Manager Cloud Control depending on when the Management Agent is installed.

- If the Management Agent is installed before Oracle Application Server and BPEL Process Manager are installed, then you must manually discover that Oracle Application Server and BPEL Process Manager in Enterprise Manager Cloud Control.
- If the Management Agent is installed after Oracle Application Server and BPEL Process Manager are installed, then Enterprise Manager Cloud Control automatically discovers that Oracle Application Server and BPEL Process Manager.

> **Note:** You must install a Management Agent on every host where BPEL Process Manager is installed. If Oracle Application Server/BPEL Process Manager and Enterprise Manager Cloud Control are all on the same host, then you need not install a separate Management Agent. The Management Agent that comes with Enterprise Manager Cloud Control is sufficient. However, if they are different hosts, then you must install a separate Management Agent on every host where BPEL Process Manager is installed. The Management Agent can be installed along with Enterprise Manager Cloud Control or separately as a standalone product.

Also note that if you have added a new BPEL Process Manager to an Oracle Application Server that is already discovered and monitored in Enterprise Manager Cloud Control, then you must manually *rediscover* that Oracle Application Server.

To manually discover or *rediscover* Oracle Application Server:

1. From the **Targets** menu, select **Middleware**.

   The Middleware page that lists all the middleware targets being monitored is displayed. In Enterprise Manager 10g Cloud Control Release 4 (10.2.0.4) or lower, the Middleware tab is Application Servers.

2. (Only for *Rediscovering*) In the Middleware page, select the Oracle Application Server that you want to rediscover and click **Remove**.

3. In the Middleware page, from the **Add** list, select **Oracle Application Server** and click **Go**. The Add Oracle Application Server Target: Specify Host page is displayed.

4. Enter the name of the host where that Oracle Application Server is running, and click **Continue**.

   Enterprise Manager Cloud Control rediscovers that Oracle Application Server along with its core components and the newly added BPEL Process Manager.

9.5.2 Deployed to Oracle WebLogic Managed Server

To discover the BPEL Process Manager deployed to Oracle WebLogic Managed Server, you have to first discover and add Oracle WebLogic Managed Server to Enterprise Manager Cloud Control.

This section describes the procedures for the following:

- Discovering Oracle WebLogic Managed Server
- Deployed to Oracle WebLogic Managed Server

9.5.2.1 Discovering Oracle WebLogic Managed Server

To discover and add Oracle WebLogic Managed Server to Enterprise Manager Cloud Control:

1. From the **Targets** menu, select **Middleware**.

   Enterprise Manager Cloud Control displays the Middleware page that lists all the middleware targets being monitored. In Enterprise Manager 10g Cloud Control Release 4 (10.2.0.4) or lower, the Middleware tab is Application Servers

2. In the Middleware page, from the **Add** list, select **Oracle Fusion Middleware / WebLogic Server Domain**, and click **Go**.

   Enterprise Manager Cloud Control displays the Add Oracle Fusion Middleware / WebLogic Server Domain wizard that captures the details of the Oracle WebLogic Server Domain to be discovered and monitored.

3. In the wizard, specify the required details and click **Next** on each page to reach the end of the wizard.

   For information about the details to be provided for each page of the wizard, click **Help** on each page.

4. In the last page of the wizard, click **Finish** to complete the discovery process and add the target to Cloud Control for monitoring purposes.

   Enterprise Manager Cloud Control displays the Middleware page with a confirmation message that confirms that the Oracle WebLogic Manager Server has been successfully added to Cloud Control. In the Middleware page that shows all the middleware targets being monitored, you can see the Oracle WebLogic Managed Server you just added.

9.5.2.2 Deployed to Oracle WebLogic Managed Server

To discover and add the BPEL Process Manager deployed to Oracle WebLogic Managed Server:

1. From the **Setup** menu, select **Add Targets**, then select **Add Targets Manually**. Now select the **Add Non-Host Targets by Specifying Target Monitoring Properties** option.

2. Select the target type from the drop-down list and click the torch icon to select a Monitoring Agent. Click **Add Manually.** The Select Application Server page of the Add BPEL Process Manager wizard is displayed.

   a. In the Select Application Server page, provide the following details and click **Next**.

Table 9–4 Select Application Server Page - Element Description

UI Page Element	Description
Application Server Type	Select the type of application server where the BPEL Process Manager to be discovered is running.

Table 9–4 (Cont.) Select Application Server Page - Element Description

UI Page Element	Description
Application Server Name	Specify the name of the application server where the BPEL Process Manager to be discovered is running. If you are not sure about the name, click the each icon (torch icon) to view a list of application servers and select the appropriate one. The application server name must be suffixed with *oracleBPELServer*.

b. In the Target Details page, provide the following details and click **Next**.

Table 9–5 Target Details Page - Element Description

UI Page Element	Description
Oracle Home	Specify the full path to the Oracle Application Server home directory where the BPEL Process Manager is installed. For example, /opt/app/orabpel/product/10.1.3.1/OracleAS.
Application Server Home	Specify the full path to the directory where Oracle WebLogic Managed Server (to which the BPEL target is deployed) is running. For example, /opt/wls9.2/weblogic9.2.

Note:

- Enterprise Manager Cloud Control checks the configuration settings of the associated application server and prefills the values for fields such as BPEL Process Manager Name, Display Name, Context Provider URL, and Oracle BPEL PM Console URL.
- At this point, if you encounter a discovery failure error, then follow the workaround steps given in Table 9–9 to resolve the issue.

c. In the Host Credentials page, specify the operating system credentials of the host where BPEL Process Manager is running. By default, the fields are prefilled with preferred credentials that are stored in the Management Repository for the selected host. You can either use these prefilled values or edit them to override the preferred credentials with your new credentials.

d. In the Review page, review the details and click **Finish** to complete the discovery process and add the target to Enterprise Manager Cloud Control.

Enterprise Manager Cloud Control displays the Agent home page with a confirmation message that confirms that the BPEL Process Manager has been successfully added for monitoring.

3. To verify whether the BPEL Process Manager has been added, click **Targets** and then **Middleware**.

Enterprise Manager Cloud Control displays the Middleware page that shows all the middleware targets being monitored, including the Oracle WebLogic Managed Server and the BPEL Process Manager you just added.

9.5.3 Deployed to IBM WebSphere Application Server

To discover the BPEL Process Manager deployed to IBM WebSphere Application Server, you have to first discover and add IBM WebSphere Application Server to Enterprise Manager Cloud Control.

This section describes the procedures for the following:

- Discovering IBM WebSphere Application Server
- Deployed to IBM WebSphere Application Server

9.5.3.1 Discovering IBM WebSphere Application Server

To discover and add IBM WebSphere Application Server to Enterprise Manager Cloud Control:

1. From the **Targets** menu, select **Middleware**.

   Enterprise Manager Cloud Control displays the Middleware page that lists all the middleware targets being monitored.

2. In the Middleware page, select **IBM WebSphere Application Server** from the **Add** drop-down list and click **Go**.

   Enterprise Manager Cloud Control displays the Add IBM WebSphere Application Server wizard that captures the details of the IBM WebSphere Application Server to be discovered and monitored.

3. In the Add IBM WebSphere Application Server wizard, specify the required details and click **Next** on each page to reach the end of the wizard.

   For information about the details to be provided for each page of the wizard, click **Help** on each page.

4. In the last page of the Add IBM WebSphere Application Server wizard, click **Finish** to complete the discovery process and add the target to Enterprise Manager Cloud Control for monitoring purposes.

   Enterprise Manager Cloud Control displays the Middleware page with a confirmation message that confirms that the IBM WebSphere Application Server has been successfully added for monitoring. In the Middleware page that shows all the application server being monitored, you can see the IBM WebSphere Application Server you just added.

9.5.3.2 Deployed to IBM WebSphere Application Server

To discover and add the BPEL Process Manager deployed to IBM WebSphere Application Server:

1. From the **Setup** menu, select **Add Targets**, then select **Add Targets Manually**. Now select the **Add Non-Host Targets** by Specifying Target Monitoring Properties option.

2. Select the target type from the drop-down list and click the torch icon to select a Monitoring Agent. Click **Add Manually**. The Select Application Server page of the Add BPEL Process Manager wizard is displayed.

   a. In the Select Application Server page, provide the following details and click **Next**.

Table 9–6 Select Application Server Page - Element Description

UI Page Element	Description
Application Server Type	Select **IBM WebSphere Application Server** from the list.
Application Server Name	Specify the name of IBM WebSphere Application Server where the BPEL Process Manager to be discovered is running. If you are not sure about the name, click the search icon (torch icon) to view a list of application servers and select the appropriate one. The application server name must be suffixed with *oracleBPELServer*.

b. In the Target Details page, provide the following details and click **Next**.

Table 9–7 Target Details Page - Element Description

UI Page Element	Description
Oracle Home	Specify the full path to the Oracle Application Server home directory where the BPEL Process Manager is installed. For example, /opt/app/orabpel/product/10.1.3.1/OracleAS.
Application Server Home	Specify the full path to the directory where IBM WebSphere Application Server (to which the BPEL target is deployed) is running.
BPEL Application Installation Location	Specify the full path to the installation directory where the BPEL application is installed.For example, if the BPEL application is installed in <$WEBSPHERE_HOME>/profiles/AppSrv01/installedApps/sta00114Cell01/CollaxaWebApplications-sta00114Node01.ear, then specify the path as <$WEBSPHERE_HOME>/profiles/AppSrv01/installedApps. Here, replace $WEBSPHERE_HOME with the full path of the application home location.

Note: Enterprise Manager Cloud Control checks the configuration settings of the associated application server and prefills the values for fields such as BPEL Process Manager Name, Display Name, Context Provider URL, and Oracle BPEL PM Console URL.

c. In the Host Credentials page, specify the operating system credentials of the host where BPEL Process Manager is running. By default, the fields are prefilled with preferred credentials that are stored in the Management Repository for the selected host. You can either use these prefilled values or edit them to override the preferred credentials with your new credentials.

d. In the Review page, review the details and click **Finish** to complete the discovery process and add the target to Enterprise Manager Cloud Control.

Enterprise Manager Cloud Control displays the Agent home page with a confirmation message that confirms that the BPEL Process Manager has been successfully added for monitoring.

Note: At this point, if you encounter a discovery failure error, then follow the workaround steps given in Table 9–10 and resolve the issue.

3. To verify whether the BPEL Process Manager has been added, select Middleware from the Targets menu. /

   Enterprise Manager Cloud Control displays the Middleware page that shows all the middleware targets being monitored, including the IBM WebSphere Application Server and the BPEL Process Manager you just added.

9.6 Configuring BPEL Process Manager

After discovering BPEL Process Manager, you must perform the following configuration steps:

- Specifying Details for Monitoring BPEL Process Manager
- Registering BPEL Process Manager Credentials and Host Credentials

9.6.1 Specifying Details for Monitoring BPEL Process Manager

Follow these steps to specify the details required for monitoring BPEL Process Managers. If the values are prefilled, then validate them.

1. In the BPEL Process Manager Home page, select **Target Setup**, then select **Monitoring Configuration** from the **BPEL Process Manager** menu.
2. In the Monitoring Configuration page, specify the following details. If these values are prefilled, then validate them.

   - **BPEL Admin Username** - Specify the BPEL administrator user ID.
   - **BPEL Password** - Specify the BPEL admin password.

     When adding the credentials, validate the following two criteria:

     – BPEL Admin User ID and password should have BPEL Admin role

     – The same credentials should succeed for the BPEL console login operation

   - **Initial Context Factory** - Specify the initial context factor. You can copy the following string value:

     ```
     com.evermind.server.rmi.RMIInitialContextFactory
     ```

   - **Context Provider URL** - Specify the context provider URL. You can copy the following string value:

     ```
     opmn:ormi://<host>:<opmn_port>:home/orabpel
     ```

     Note: Replace the <host>,<opmn port> with the correct host address and opmn port number details for the Oracle Application Server where the BPEL Process Manager is deployed.

     To retrieve SOA Applications Server OPMN PORT details, follow these steps:

     1. Open the configuration file `$SOA_ORACLE_HOME/opmn/conf/opmn.xml`. $SOA_ORACLE_HOME corresponds to SOA Application server home location.
     2. Identify the value of the request port attribute in the configuration file.

   - **BPEL Repository Host Name -** Specify the BPEL Dehydration store (database) host name.

- **BPEL Repository Port -** Specify the BPEL Dehydration store (database) port.
- **BPEL Repository SID -** Specify the BPEL Dehydration store (database) SID.
- **BPEL Repository User Name -** Specify the BPEL Dehydration store (database) user name. By default, the user name is `orabpel`.
- **BPEL Repository Password -** Specify the BPEL Dehydration store (database) password. By default, the password is `welcome1`.
- **Recoverable Instances Time Threshold (Days) -** Specify the number of days for which the retryable instances must be shown.
- **Process Aggregate State -** Specify 5, a numeric value that signifies the **constant** state of the BPEL target.

3. Click **OK** to save the settings.

9.6.2 Registering BPEL Process Manager Credentials and Host Credentials

Follow these steps to register the credentials of the BPEL Process Manager, and the credentials of the host where BPEL Process Manager is running.

1. From the **Setup** menu, select **Security**, then select **Preferred Credentials.**
2. Select the Host target type and click **Manage Preferred Credentials**.
3. Select **Normal Host Credentials** in the Credential Set column in the Default Preferred Credentials section and click **Set**.
4. In the Select Named Credential window, enter the user name and password and click **Save** to return to the Preferred Credentials page.
5. Select Oracle BPEL Process Manager target type and click **Manage Preferred Credentials**.
6. Select **Monitoring Administrator Credentials** in the Credential Set column in the Default Preferred Credentials section and click **Set**.
7. In the Select Named Credential window, enter the user name and password and click **Save**.

9.7 Troubleshooting BPEL Process Managers

This section describes the errors you might encounter while discovering BPEL Process Managers, and the workaround steps you can follow to resolve each of them.

This section covers the following:

- Discovery Errors on Target Details Page
- Discovery Errors on Review Page
- Discovery Errors on Review Page

9.7.1 Discovery Errors on Target Details Page

The following error occurs in the Target Details page of the Add BPEL Process Manager wizard where you provide details about the BPEL Process Manager installed on Oracle WebLogic Managed Server.

Table 9–8 Errors on Target Details Page While Adding BPEL Process Manager Deployed to Oracle WebLogic Managed Server

Error Message	Workaround Steps
`Oracle BPEL Process Manager not found in the selected Application Server. Select another Application Server.`	This error may occur if BPEL is not deployed on the selected Application Server or if the configuration data has not been collected. To resolve this issue: 1. Select another Application Server. 2. Navigate to the Application Server Home page and select **Configuration,** then select **Last Collected** from the Application Server target menu.

9.7.2 Discovery Errors on Review Page

The following errors occur in the Review page of the Add BPEL Process Manager wizard when you are about to add a BPEL Process Manager installed on Oracle WebLogic Managed Server, to Enterprise Manager Cloud Control for monitoring purposes.

Table 9–9 Errors on Review Page While Adding BPEL Process Manager Deployed to Oracle WebLogic Managed Server

Error Message	Workaround Steps
`Discovery Failure - Oracle BPEL Process Manager target discovery failed due to incorrect host credentials.`	1. In the last page of the Add BPEL Process Manager wizard where you see this error message, click **Previous** to reach the Host Credentials page. 2. In the Host Credentials page, specify the correct host credentials or set the preferred credentials for the specific host. Ensure that these are Agent user credentials.
`Oracle BPEL Process Manager Discovery Failed - Unable to connect to Oracle BPEL Process Manager. The possible reasons can be incorrect path or insufficient permission to access Oracle BPEL Process Manager home location or inaccessible Oracle BPEL Process Manager home location. Review the specified value.`	1. In the last page of the Add BPEL Process Manager wizard, click **Previous** repeatedly to reach the Target Details page. 2. In the Target Details page, verify the Oracle home location of the BPEL Process Manager. 3. In the Target Details page, verify the installation location of the associated application server.
`Oracle BPEL Process Manager Discovery Failed - Unable to connect to Oracle BPEL Process Manager. The possible reasons can be incorrect path or insufficient permission to access Oracle BPEL Process Manager home location or inaccessible Oracle BPEL Process Manager home location. Review the specified value.`	Ensure that the BPEL directories have read permission for the Agent user.

9.7.3 Discovery Errors on Review Page

The following errors occur in the Review page of the Add BPEL Process Manager wizard when you are about to add a BPEL Process Manager installed on IBM WebSphere Application Server, to Enterprise Manager Cloud Control for monitoring purposes.

Table 9–10 Error on Review Page While Adding BPEL Process Manager Deployed to IBM WebSphere Application Server

Error Message	Workaround Steps
`Discovery Failure - Oracle BPEL Process Manager target discovery failed due to incorrect host credentials.`	1. In the last page of the Add BPEL Process Manager wizard where you see this error message, click **Previous** to reach the Host Credentials page. 2. In the Host Credentials page, specify the correct host credentials or set the preferred credentials for the specific host. Ensure that these are Agent user credentials.

`Oracle BPEL Process Manager Discovery Failed - Unable to connect to Oracle BPEL Process Manager. The possible reasons can be incorrect path or insufficient permission to access Oracle BPEL Process Manager home location or inaccessible Oracle BPEL Process Manager home location. Review the specified value.`	1. In the last page of the Add BPEL Process Manager wizard where you see this error message, click **Previous** repeatedly to reach the Target Details page.
	2. In the Target Details page, verify the BPEL application installation location.
	For example, the BPEL application may be installed at the following location:
	`<$WEBSPHERE_HOME>/profiles/AppSrv01/installedApps/sta00114Cell01/CollaxaWebApplications-sta00114Node01.ear`
	In this case, the path you specify must look like this:
	`<$WEBSPHERE_HOME>/profiles/AppSrv01/installedApps`
	Note: Replace `$WEBSPHERE_HOME` with the absolute application home location.
	3. In the Target Details page, verify the application server home location of the associated application server.
	4. In the Target Details page, verify the Oracle home location of the BPEL Process Manager.

9.7.4 Display Errors on Processes Page

Sometimes, after the discovery of a BPEL Process Manager, the BPEL process may occasionally not be listed in the BPEL Process Manager Processes page in Enterprise Manager Cloud Control.

There are two causes for this and two ways to ensure they display on the Processes page. The sections below discuss these causes and workaround steps to fix them.

9.7.4.1 No Credentials Specified for Monitoring BPEL Process Manager

You may not have specified the credentials required for monitoring BPEL Process Managers. To address this, do the following:

1. In the BPEL Process Manager Home page, select **Target Setup**, then select **Monitoring Configuration** from the **BPEL Process Manager** menu.
2. In the Monitoring Configuration page, check the following fields:
   - **BPEL Admin Username** - Provide the BPEL administrator user ID.
   - **BPEL Password** - Provide the BPEL admin password.

     When adding the credentials validate the following two criteria:

     – BPEL Admin User ID and password should have BPEL Admin role

     – The same credentials should succeed for the BPEL console login operation
   - **Initial Context Factory** - In case this field is empty, copy the following string value:

```
com.evermind.server.rmi.RMIInitialContextFactory
```

- **Context Provider URL** - In case this field is empty, copy the following highlighted string value:

  ```
  opmn:ormi://<host>:<opmn_port>:home/orabpel
  ```

  > **Note:** Replace the <host>,<opmn port> with the correct host address and opmn port number details for the Oracle Application Server where the BPEL Process Manager is deployed.

3. Click **OK** to save the settings.

9.7.5 Retrieving the OPMN Port

To retrieve SOA Applications Server OPMN PORT details, follow these steps.

1. Open the configuration file `$SOA_ORACLE_HOME/opmn/conf/opmn.xml`. `$SOA_ORACLE_HOME` corresponds to SOA Application server home location.
2. Identify the value of the request port attribute in the configuration file.

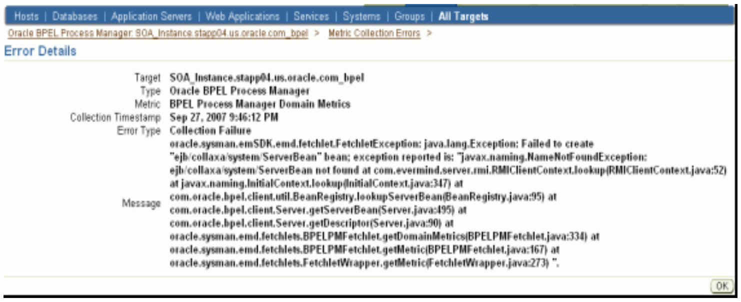
9.7.6 javax.naming.NameNotFoundException Error

The following error occurs in the error details page when incorrect provider URL is specified.

Table 9–11 javax.naming.NameNotFoundException Error - Workaround Steps

Error Message	Workaround Steps
`oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create "ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NameNotFoundException:...` (See Figure 9–1)	1. Validate the format of the string. 2. Verify if the OPMN port is correct. 3. Verify if the <oc4j_instance> name is properly substituted with the correct value, that is, the OC4J name value. The format must be like this: `opmn:ormi://<host>:<opmn_port>:home/orabpel`

Figure 9–1 javax.naming.NameNotFoundException Error



Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | All Targets
Oracle BPEL Process Manager: SOA_Instance.stapp04.us.oracle.com_bpel > Metric Collection Errors >
OK

Error Details

Target SOA_Instance.stapp04.us.oracle.com_bpel

Type Oracle BPEL Process Manager

Metric BPEL Process Manager Domain Metrics

Collection Timestamp Sep 27, 2007 9:46:12 PM

Error Type Collection Failure

Message

```
oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create
"ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NameNotFoundException:
ejb/collaxa/system/ServerBean not found at com.evermind.server.rmi.RMIClientContext.lookup(RMIClientContext.java:52)
at javax.naming.InitialContext.lookup(InitialContext.java:347) at
com.oracle.bpel.client.util.BeanRegistry.lookupServerBean(BeanRegistry.java:95) at
com.oracle.bpel.client.Server.getServerBean(Server.java:495) at
com.oracle.bpel.client.Server.getDescriptor(Server.java:90) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getDomainMetrics(BPELPMFetchlet.java:334) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getMetric(BPELPMFetchlet.java:167) at
oracle.sysman.emd.fetchlets.FetchletWrapper.getMetric(FetchletWrapper.java:273) ".
```

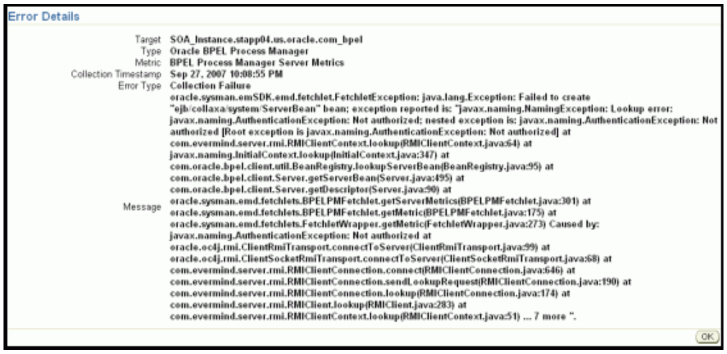
9.7.7 javax.naming.NamingException Error

The following error occurs in the error details page when incorrect password is specified.

Table 9–12 javax.naming.NamingExceptionError - Workaround Steps

Error Message	Workaround Steps
`oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create "ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NamingException: Lookup error:...` (See Figure 9–2)	1. Validate the values specified for **BPEL Admin username** and **BPEL Password** fields in the Monitoring Configuration page. (Confirm the validity of credentials by using the same credentials to log in to the BPELConsole).

Figure 9–2 javax.naming.NamingException Error



Error Details

Target SOA_Instance.stapp04.us.oracle.com_bpel
Type Oracle BPEL Process Manager
Metric BPEL Process Manager Server Metrics
Collection Timestamp Sep 27, 2007 10:08:55 PM
Error Type Collection Failure
Message

```
oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create
"ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NamingException: Lookup error:
javax.naming.AuthenticationException: Not authorized; nested exception is: javax.naming.AuthenticationException: Not
authorized [Root exception is javax.naming.AuthenticationException: Not authorized] at
com.evermind.server.rmi.RMIClientContext.lookup(RMIClientContext.java:64) at
javax.naming.InitialContext.lookup(InitialContext.java:347) at
com.oracle.bpel.client.util.BeanRegistry.lookupServerBean(BeanRegistry.java:95) at
com.oracle.bpel.client.Server.getServerBean(Server.java:495) at
com.oracle.bpel.client.Server.getDescriptor(Server.java:90) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getServerMetrics(BPELPMFetchlet.java:301) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getMetric(BPELPMFetchlet.java:175) at
oracle.sysman.emd.fetchlets.FetchletWrapper.getMetric(FetchletWrapper.java:273) Caused by:
javax.naming.AuthenticationException: Not authorized at
oracle.oc4j.rmi.ClientRmiTransport.connectToServer(ClientRmiTransport.java:99) at
oracle.oc4j.rmi.ClientSocketRmiTransport.connectToServer(ClientSocketRmiTransport.java:68) at
com.evermind.server.rmi.RMIClientConnection.connect(RMIClientConnection.java:646) at
com.evermind.server.rmi.RMIClientConnection.sendLookupRequest(RMIClientConnection.java:190) at
com.evermind.server.rmi.RMIClientConnection.lookup(RMIClientConnection.java:174) at
com.evermind.server.rmi.RMIClient.lookup(RMIClient.java:283) at
com.evermind.server.rmi.RMIClientContext.lookup(RMIClientContext.java:51) ... 7 more ".
```

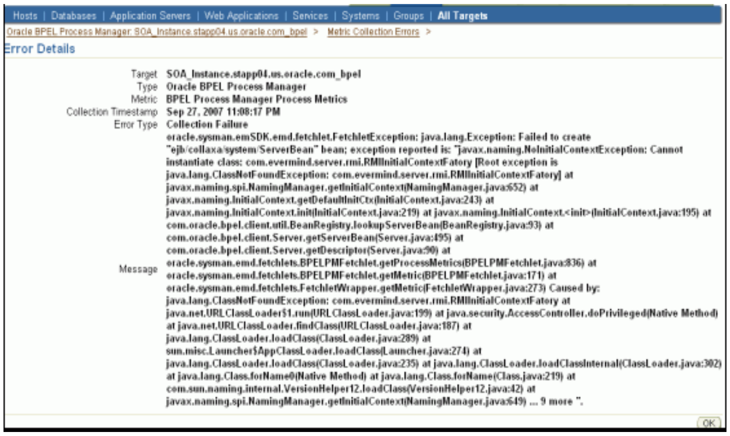
9.7.8 javax.naming.NoInitialContextException Error

The following error occurs in the error details page when incorrect *Initial Context Factory* value is specified.

Table 9–13 javax.naming.NoInitialContextException Error - Workaround Steps

Error Message	Workaround Steps
`oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create "ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NoInitialContextException: Cannot instantiate class:...` (See Figure 9–3)	1. Provide the following value for the **Initial Context Factory** field in the Monitoring Configuration page: `com.evermind.server.rmi.RMIInitialContextFactory`

Figure 9–3 javax.naming.NoInitialContextException Error


Hosts | Databases | Application Servers | Web Applications | Services | Systems | Groups | All Targets
Oracle BPEL Process Manager: SOA_Instance.stapp04.us.oracle.com_bpel > Metric Collection Errors >
OK

Error Details

Target SOA_Instance.stapp04.us.oracle.com_bpel

Type Oracle BPEL Process Manager

Metric BPEL Process Manager Process Metrics

Collection Timestamp Sep 27, 2007 11:08:17 PM

Error Type Collection Failure

Message

```
oracle.sysman.emSDK.emd.fetchlet.FetchletException: java.lang.Exception: Failed to create
"ejb/collaxa/system/ServerBean" bean; exception reported is: "javax.naming.NoInitialContextException: Cannot
instantiate class: com.evermind.server.rmi.RMIInitialContextFatory [Root exception is
java.lang.ClassNotFoundException: com.evermind.server.rmi.RMIInitialContextFatory] at
javax.naming.spi.NamingManager.getInitialContext(NamingManager.java:652) at
javax.naming.InitialContext.getDefaultInitCtx(InitialContext.java:243) at
javax.naming.InitialContext.init(InitialContext.java:219) at javax.naming.InitialContext.<init>(InitialContext.java:195) at
com.oracle.bpel.client.util.BeanRegistry.lookupServerBean(BeanRegistry.java:93) at
com.oracle.bpel.client.Server.getServerBean(Server.java:495) at
com.oracle.bpel.client.Server.getDescriptor(Server.java:90) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getProcessMetrics(BPELPMFetchlet.java:836) at
oracle.sysman.emd.fetchlets.BPELPMFetchlet.getMetric(BPELPMFetchlet.java:171) at
oracle.sysman.emd.fetchlets.FetchletWrapper.getMetric(FetchletWrapper.java:273) Caused by:
java.lang.ClassNotFoundException: com.evermind.server.rmi.RMIInitialContextFatory at
java.net.URLClassLoader$1.run(URLClassLoader.java:199) at java.security.AccessController.doPrivileged(Native Method)
at java.net.URLClassLoader.findClass(URLClassLoader.java:187) at
java.lang.ClassLoader.loadClass(ClassLoader.java:289) at
sun.misc.Launcher$AppClassLoader.loadClass(Launcher.java:274) at
java.lang.ClassLoader.loadClass(ClassLoader.java:235) at java.lang.ClassLoader.loadClassInternal(ClassLoader.java:302)
at java.lang.Class.forName0(Native Method) at java.lang.Class.forName(Class.java:219) at
com.sun.naming.internal.VersionHelper12.loadClass(VersionHelper12.java:42) at
javax.naming.spi.NamingManager.getInitialContext(NamingManager.java:649) ... 9 more ".
```

9.7.9 Error While Creating BPEL Infrastructure Services

The following error occurs when you are creating a new BPEL infrastructure service.

Table 9–14 javax.naming.NoInitialContextException Error - Workaround Steps

Error Message	Workaround Steps
`An error encountered while discovering the dependencies. Please try again.`	1. Apply patch 10849036 on the OMS and try creating the BPEL infrastructure service again: `com.evermind.server.rmi.RMIInitialContextFactory`

9.7.10 Metric Collection Errors for BPEL Process Manager Partner Link Metrics

The following metric collection error appears on the home page when you monitor BPEL 10.1.3.3 or 10.1.3.4 using Oracle Management Agent 12c:

Table 9–15 Metric Collection Errors for BPEL Process Manager Partner Link Metrics - Workaround Steps

Error Message	Workaround Steps
`java.rmi.UnmarshalException: Error deserializing return-value: java.io.InvalidClassException: javax.xml.namespace.QName; local class incompatible: stream classdesc serialVersionUID = -9168763693265281 64, local class serialVersionUID = -9120448754896609940 at com.oracle.bpel.client.util.ExceptionUtils.handleServerException(ExceptionUtils.java:82) at com.oracle.bpel.client.BPELProcessHandle.getDescriptor(BPELProcessHandle.java:207) at oracle.sysman.emd.fetchlets.BPELPMFetchlet.getPartnerLinkMetrics(BPELPMFetchlet.java:873) at oracle.sysman.emd.fetchlets.BPELPMFetchlet.getMetric(BELPMFetchlet.java:235) at oracle.sysman.emd.fetchlets.FetchletWrapper.getMetric(FetchletWrapper.java:382)`	Follow the workaround described in the My Oracle Support Note 735128.1. You can access My Oracle Support at the following URL: `https://support.oracle.com/CSP/ui/flash.html`

9.7.11 Agent Monitoring Metric Errors

This error occurs if the same Agent is used to monitor the BPEL 10g and OSB, and BPEL 10g and SOA 11g targets.

Table 9–16 Metric Errors During Agent Monitoring

Error Message	Workaround
The following exception has occurred: `Exception at getPartnerLinkMetrics: java.lang.NoClassDefFoundError: Could not initialize class javax.rmi.PortableRemoteObject`	The same Management must not be used to monitor BPEL 10g and OSB, and BPEL 10g and SOA 11g targets.

10

Discovering and Monitoring Oracle Service Bus

This chapter describes how you can discover and monitor Oracle Service Bus (OSB) using Enterprise Manager Cloud Control.

In particular, this document covers the following:

- Supported Versions
- Understanding the Discovery Mechanism
- Understanding the Discovery Process
- Downloading One-Off Patches
- Discovering Oracle Service Bus
- Enabling Management Packs
- Monitoring Oracle Service Bus in Cloud Control
- Generating Oracle Service Bus Reports Using BI Publisher
- Troubleshooting Oracle Service Bus

10.1 Supported Versions

The following are the versions of OSB that are supported for monitoring in Enterprise Manager Cloud Control Release 12*c*.

- Aqualogic Service Bus 2.6
- Aqualogic Service Bus 3.0
- Oracle Service Bus 10gR3
- Oracle Service Bus 11.1.1.2.0
- Oracle Service Bus 11.1.1.3.0
- Oracle Service Bus 11.1.1.4.0
- Oracle Service Bus PS4
- Oracle Service Bus PS5

10.2 Understanding the Discovery Mechanism

The OSB deployed to Oracle WebLogic Managed Server is automatically discovered in Enterprise Manager Cloud Control when that Oracle WebLogic Managed Server is discovered and added to Enterprise Manager Cloud Control.

The discovery of OSB depends on the whether the Oracle WebLogic Managed Server is already being monitored in Enterprise Manager Cloud Control.

- If Oracle WebLogic Managed Server is not being monitored in Cloud Control, then first discover and add it to Cloud Control; this will automatically discover the OSB that is deployed to it.
- If Oracle WebLogic Managed Server is already being monitored in Cloud Control, then refresh the membership of the Oracle WebLogic Server Domain to which the Oracle WebLogic Managed Server belongs. This will automatically discover the OSB that is deployed to it.

For instructions to discover OSB, see Section 10.5, "Discovering Oracle Service Bus".

10.3 Understanding the Discovery Process

The following table describes the overall process involved in discovering and monitoring OSB in Enterprise Manager Cloud Control. Follow the instructions outlined against each step in this process to successfully discover and monitor your OSB.

Table 10–1 Discovery Process

Step	Requirement	Description
1	Oracle Service Bus	Install the OSB software. **Note:** Before you launch the OSB Deployment Procedure, ensure that Sun JDK has been installed.
2	Enterprise Manager Cloud Control	Install Enterprise Manager 12c. For information about installing the base release of Enterprise Manager Cloud Control, see the *Enterprise Manager Cloud Control Basic Installation and Configuration Guide* available at: `http://www.oracle.com/technology/documentation/oem.html` Oracle recommends that you install the Enterprise Manager Cloud Control components on a host that is different from the host where OSB is installed. For example, if OSB is installed on host1.xyz.com, then install and configure Oracle Management Service (OMS) and the Management Repository on host2.xyz.com.

Table 10–1 (Cont.) Discovery Process

Step	Requirement	Description

3	Oracle Management Agent
	(Management Agent)
		Install Oracle Management Agent 12c on the host where OSB is installed.
		If OSB and Enterprise Manager Cloud Control are on the same host, then you do not have to install a separate Management Agent. The Management Agent that comes with Enterprise Manager Cloud Control is sufficient. However, if they are different hosts, then you must install a separate Management Agent on the host where OSB is installed. Alternatively, the Management Agent can also be installed on a different host and made to remotely monitor the OSB target on another host.
		You can install the Management Agent in one of the following ways:
		■ Invoke the installer provided with Enterprise Manager 12c, and select the installation type **Additional Management Agent**. Then apply the 10.2.0.5 Agent patch on it.
		■ Use the Agent Deploy application within the Enterprise Manager 12c.
		■ Use the full agent kit that is available at:
		`http://www.oracle.com/technology/software/products/oem/htdocs/agentsoft.html`
		For information about installing the Management Agent, see the *Enterprise Manager Cloud Control Basic Installation and Configuration Guide* available at:
		`http://www.oracle.com/technology/documentation/oem.html`

4	One-Off Patches	The support for discovering and monitoring of OSB is enabled only when the one-off patches as described in Section 10.4, "Downloading One-Off Patches" are applied to the WebLogic Server Home where OSB is running.
5	Discovery in Enterprise Manager Cloud Control	OSB is automatically discovered when the Oracle WebLogic Server Domain to which it is deployed is discovered and added to Enterprise Manager Cloud Control.

10.4 Downloading One-Off Patches

To view OSB services in Enterprise Manager Cloud Control, you must apply the following patches to your OSB servers.

Table 10–2 One-Off Patches

Oracle Service Bus Version	ID	Password
Oracle Service Bus 2.6	EMMU	83XNT2D4
Oracle Service Bus 2.6.1	9NAF	TLZE4IPI
Oracle Service Bus 3.0	RPCD	JJEC2EY2
Oracle Service Bus 10.3.0	9HPA	FFLQHDHP
Oracle Service Bus 10.3.1	No Patch Required	
Oracle Service Bus 11.1.1.3.0 and 11.1.1.4.0, and Oracle Service Bus PS4 and PS 5	No Patch Required	

You can apply the patches in one of the following ways:

- **Online mode** - Using the SmartUpdate tool available with Oracle WebLogic Managed Server
- **Offline mode** - Manually copying the JAR files and classes to the OSB directories

For information about downloading these patches and applying them in either offline or online mode, see My Oracle Support Note 804148.1. You can access My Oracle Support at:

`https://support.oracle.com/CSP/ui/flash.html`

Note: After applying the patches, restart the WebLogic domain and all of the management agents monitoring the domain.

10.5 Discovering Oracle Service Bus

The OSB deployed to Oracle WebLogic Managed Server is automatically discovered in Enterprise Manager Cloud Control when that Oracle WebLogic Managed Server is discovered and added to Enterprise Manager.

Before discovering OSB, identify whether the Oracle WebLogic Managed Server is already being monitored in Enterprise Manager.

- If Oracle WebLogic Managed Server is not being monitored in Enterprise Manager, then first discover and add it to Enterprise Manager Cloud Control; this will automatically discover the OSB that is deployed to it.
- If Oracle WebLogic Managed Server is already being monitored in Enterprise Manager, then refresh the membership of the Oracle WebLogic Server Domain to which the Oracle WebLogic Managed Server belongs. This will automatically discover the OSB that is deployed to it.

This section outlines the instructions for discovering OSB for the cases described above. In particular, this section covers the following:

- Discovering OSB Deployed to WLS Not Monitored by Enterprise Manager
- Discovering OSB Deployed to WLS Monitored by Enterprise Manager

10.5.1 Discovering OSB Deployed to WLS Not Monitored by Enterprise Manager

To discover OSB deployed to Oracle WebLogic Manager Server that is not monitored in Cloud Control, first discover that Oracle WebLogic Manager Server in Enterprise Manager Cloud Control; this will automatically discover the OSB that is deployed to it. To discover Oracle WebLogic Manager Server, follow these steps:

1. From the **Targets** menu, select **Middleware**.

   Enterprise Manager Cloud Control displays the Middleware page that lists all the middleware targets being monitored.

2. In the Middleware page, select **Oracle Fusion Middleware/WebLogic Server Domain** from the **Add** drop-down list and click **Go**.

   Enterprise Manager Cloud Control displays the Add Oracle Fusion Middleware / WebLogic Server Domain wizard that captures the details of the Oracle WebLogic Server Domain to be discovered and monitored.

3. In the Add Oracle Fusion Middleware / WebLogic Server Domain wizard, specify the required details and click **Next** on each page to reach the end of the wizard.

   For information about the details to be provided for each page of the wizard, click **Help** on each page.

4. In the last page of the Add Oracle Fusion Middleware / WebLogic Server Domain wizard, click **Finish** to complete the discovery process and add the target to Cloud Control for monitoring purposes.

   Enterprise Manager displays the Middleware page with a confirmation message that confirms that the Oracle WebLogic Manager Server has been successfully added to Cloud Control.

In the Middleware page that shows all the middleware targets being monitored, you can see the Oracle WebLogic Managed Server and the OSB you just added. Note that, at this point, OSB will be the last target listed in the table. To see it nested under its Oracle WebLogic Managed Server, click **Refresh** on this page. Alternatively, navigate to another tab or page, and then return to the Middleware page.

Note:

- After discovering and adding OSB to Enterprise Manager Cloud Control, you can monitor its status from the OSB Home page. You can use the Services page to view a list of services.

  For the first collection that happens, you will see the value "0" for all the metrics that are enabled in Oracle Enterprise Manager Release 12*c*. This is an expected behavior. From the second collection onwards, you should see the actual metric values. However, if you still see the value "0", then perhaps the service monitoring is turned off. To resolve this issue, on the Services page, click Launch Console to access the OSB Console, and turn on the service monitoring and set the level to "pipeline" or "action"
- In the case of clustered OSB domain, the Management Agent installed on Admin Server host should be used to discover the entire domain. This constraint is not applicable for version 12.1.0.2 of Cloud Control. This is only valid up to version 12.1.0.1 of Cloud Control.

10.5.2 Discovering OSB Deployed to WLS Monitored by Enterprise Manager

To discover OSB deployed to Oracle WebLogic Managed Server that is already being monitored in Cloud Control, refresh the membership of the Oracle WebLogic Server Domain to which the Oracle WebLogic Managed Server belongs. This will automatically discover the OSB that is deployed to it.

To refresh the membership of the Oracle WebLogic Server Domain to which the Oracle WebLogic Managed Server belongs, follow these steps:

1. From the **Targets** menu, select **Middleware**.
2. On the **Middleware** page, select the **Oracle WebLogic Server Domain** target from the list of Middleware targets being monitored.
3. On the Oracle WebLogic Server Domain Home page, in the General section, click **Refresh Domain**. Enterprise Manager Cloud Control displays the membership page that lists the OSB that is currently not being monitored. Click **OK**.

   Enterprise Manager Cloud Control refreshes the membership and returns to the Oracle WebLogic Server Domain Home page.

   Note: On the Oracle WebLogic Server Domain Home page, in the Status section, the legend of the status pie chart may not show an increased count to indicate the newly added OSB target. This is an expected behavior because Enterprise Manager Cloud Control takes a few seconds to reflect the membership details in this section.

4. Click the **Members** tab and verify whether the OSB has been added.

10.6 Enabling Management Packs

Besides monitoring the status of OSB, if you want to gain access to additional value-added features, then you must enable the Management Pack for SOA.

To enable the Management Pack for SOA:

1. From the **Setup** menu, select **Management Packs**, then select **Management Pack Access**.

   Enterprise Manager Cloud Control displays the Management Pack Access page.

2. In the Management Pack Access page, from the Search list, select **Oracle Service Bus**.

   Enterprise Manager Cloud Control lists all the Oracle Service Bus targets being monitored.

3. From the table, for the Oracle Service Bus target you are interested in, enable the SOA Management Pack Enterprise Edition and click **Apply**.

10.7 Monitoring Oracle Service Bus in Cloud Control

Enterprise Manager Cloud Control helps you monitor the health of Oracle Service Bus targets deployed to Oracle WebLogic Managed Servers. When you discover Oracle WebLogic Manager Servers, Cloud Control automatically discovers the Oracle Service Bus targets deployed to them and adds them for central monitoring and management.

For each Oracle Service Bus target being monitored, Cloud Control provides information about its status, availability, performance, services, alerts, business services, and proxy services. It also allows you to view the latest configuration details, save them at a particular time, and compare them with another Oracle Service Bus instances. Oracle Service Bus also provides a graphical view representation for the dependencies between proxy services and business services.

In addition to monitoring capabilities, Cloud Control also allows you to black out an Oracle Service Bus target and create infrastructure services. While blackout helps you suspend the monitoring of the target for a temporary period (for example, during maintenance), infrastructure services are dependency services that are created to identify the infrastructure components on which the Oracle Service Bus target depends.

10.7.1 Enabling Monitoring for OSB Services

If you are not able to view OSB data on Enterprise Manager pages, it may be because monitoring is disabled for OSB Services. Before you can view OSB data in Enterprise Manager, check to see if monitoring is enabled for OSB Services. You can do that by following these steps:

1. Click the **OSB Console** link in the OSB Home Summary region.
2. Log into the OSB target.
3. Click **Create** (to create the new session).
4. On the left navigation panel, click **Operations** and then choose **Global Settings**.
5. Determine whether monitoring is enabled. To enable monitoring, select the check box to update it.
6. Activate the session.

10.8 Generating Oracle Service Bus Reports Using BI Publisher

You can use Enterprise Manager to print Oracle Service Bus reports using BI Publisher Enterprise Reports. Oracle Business Intelligence (BI) Publisher is an enterprise reporting solution for authoring, managing, and delivering highly formatted documents. Oracle BI Publisher also allows you to build custom reporting applications that leverage existing infrastructure. Reports can be designed using familiar desktop products and viewed online or scheduled for delivery to a wide range of destinations.

For example, you can generate an OSB Services Report that describes the way OSB services have been performing over a period of time. The report provides charts to list the top 5 OSB Services and a table with critical metric details for all the services.

The following table describes the OSB-related reports you can choose.

Table 10–3 OSB Reports

OSB Report	Description
OSB Service Summary Report	The OSB Service Summary Report provides information about the Average Response Time, Open Instances Count, Fault Instances Count, and Web Service Security Violation Count for the selected service. The OSB Service Summary Report displays a chart with the top 5 OSB services based on Average Response Time or Throughput across the selected OSB services for the specified time period. The report can be sorted based on a performance metric (for example, Average Response Time) or a usage metric (for example, Instance Count). As part of the report parameters setting, you can use options that allow you to select the OSB Service by Projects or by selecting individual services.
OSB Service Operations Summary Report	The OSB Service Operations Summary Report provides internal operation level details for the selected service. The details in the report cover the Average Response Time, Open Instances Count, Fault Instances Count, and Web Service Security Violation Count. The report can be sorted based on a performance metric or a usage metric. As part of the report parameters setting, you can use options that allow you to select the OSB Service by Projects or by selecting individual services.
OSB Proxy Service Flow Component Performance Summary Report	A message flow is composed of components that define the logic for routing and manipulating messages as they flow through a proxy service. The OSB Proxy Service Flow Component Performance Summary Report provides internal flow component details for the selected proxy service. The details in the report display the Average Response Time, Open Instances Count, Fault Instances Count, and Web Service Security Violation Count. The report can be sorted based on a performance metric or a usage metric. As part of the report parameters setting, you can use options that allow you to select the OSB Service by Projects or by selecting individual services.

To print OSB reports using BI Publisher Enterprise reports, follow these steps:

1. From the Enterprise menu, click **Reports**, and then click **BI Publisher Enterprise Reports**.

   Enterprise Manager Cloud Control displays the login page for BI Publisher Enterprise Reports.

2. Enter your credentials to log into BI Publisher.

   The BI Publisher Enterprise page displays, showing you Recent reports, Others, and Favorites. You can use this page to create a new report, submit a report job, and perform other tasks.

3. Click the Report you want to display.
4. On the Report page, use the parameter filters to tailor the report structure that displays, then click **Refresh**.

   You can view the OSB Services Report using the filters based on the various search parameters available at the top of the page, such as Target Name, Date Range, and so on. Similarly, you can view the report based on the Sort By option as well, allowing you to sort the report by Service Name or Average Response Time, for example.

   You can refresh the report anytime by clicking the Refresh icon on the upper right side of the OSB Service Report tab. You can hide or display the search parameters by clicking the Parameters icon. You can choose to view the report in various formats such as HTML, PDF, RTF, Excel, and PowerPoint by clicking the View Report icon. Likewise you can display more available actions by clicking the Actions icon. For more help about using BI Publisher, click the help icon.

10.9 Troubleshooting Oracle Service Bus

This section describes the errors you might encounter while discovering OSB, and the workaround steps you can follow to resolve each of them.

10.9.1 Required Patches Missing

The following error occurs when you try to discover OSB from an Oracle WebLogic Admin Server that has not been patched with the required one-off patches.

Table 10–4 oracle.sysman.emSDK.emd.fetchlet.FetchletException Error - Workaround Steps

Error Message	Workaround Steps
`oracle.sysman.emSDK.emd.fetchlet.FetchletException: The MBean is not available on the OSB instance. The required EM plug in patch should be missing on OSB instance.`	Apply the one-off patches as described in Section 10.4, "Downloading One-Off Patches".

10.9.2 System and Service

The following error occurs if configuration information has not been collected for the selected Application Server.

Table 10–5 Create System and Service Error - Workaround Steps

Error Message	Workaround Steps
`An error encountered while discovering the dependencies. This may occur if some configuration information is missing. Check whether the configuration information was collected for the dependent targets and then try again.`	Collect the latest configuration data by navigating to the Application Server Home page and clicking **Configuration** and then select **Last Collected** from the Application Server menu.

10.9.3 SOAP Test

The following error occurs when the Management Agent is upgraded to Enterprise Manager 12c with OMS 10.2.0.5.

Table 10–6 SOAP Test Error - Workaround Steps

Error Message	Workaround Steps
`Add SOAP Test failed. The selected service has an invalid or incorrect WSDL URL. Check whether the Oracle Service Bus Target URL value is valid in the Monitoring Configuration page of the selected target. To access the Monitoring Configuration page, go to the Oracle Service Bus Homepage and from the Related Links section, select Monitoring Configuration.`	If the Management Agent has been upgraded to 12c with OMS 10.2.0.5, the following workaround must be applied to support the SOAP test. In the Monitoring Configuration page for the OSB target, set the **Server URL to Access Proxy Services** property to the URL for the specific WebLogic Server target. The URL must be in the format: `http://<host>:<port>/`. For example, `http://stade61.us.oracle.com:7001/`

11

Discovering and Monitoring the SOA Suite

This chapter describes how you can discover and configure the components of the SOA Suite 11g using Enterprise Manager Cloud Control.

In particular, this document covers the following:

- New Features in This Release
- Supported Versions
- Understanding the Discovery Process
- Discovering the SOA Suite
- Post Discovery Steps
- Generating SOA Reports Using Information Publisher
- Dehydration Store Monitoring
- Service Topology
- UDDI Publishing
- Generating SOA Reports Using BI Publisher
- Provisioning SOA Artifacts and Composites
- Support Workbench
- Troubleshooting

11.1 New Features in This Release

The new features that have been introduced in the 12c version of the SOA Suite are:

- Dehydration Store: You can view the performance of the database relevant to the SOA engine. You can review the general health of the database engine and identify problems that are causing a performance bottleneck.
- Service Topology: You can see a graphical end to end view of the composite applications. It depicts the various application components and their interactions happening at runtime.
- SOA Partition: You can deploy SOA composite applications into separate sections of the SOA Infrastructure known as partitions.
- Instance Tracing Enhancements: Instance tracing can now be performed at the component level and you can view the audit trail for individual component instances.
- UDDI Publishing: Publishing a service to UDDI is now supported.

11.2 Supported Versions

The following are the versions of the SOA Suite 11g that are supported in Enterprise Manager Cloud Control 12c:

- 11.1.1.2.0 (PS1)
- 11.1.1.3.0 (PS2)
- 11.1.1.4.0 (PS3)
- 11.1.1.5.0 (PS4)
- 11.1.1.6.0 (PS5)

11.3 Understanding the Discovery Process

The following describes the overall process involved in discovering and monitoring SOA Suite 11g in Enterprise Manager Cloud Control. Follow the instructions outlined against each step in this process to successfully discover and monitor the SOA Suite.

Table 11–1 Understanding the Discovery Process

Oracle SOA Suite Version	Application Server Deployed To	Discovery Mechanism	Process
Oracle SOA Suite 11.1 PS2	Oracle WebLogic Managed Server	Manual Discovery	1. First, manually discover Oracle WebLogic Managed Server. For procedures, see Section 9.5.2.1, "Discovering Oracle WebLogic Managed Server". 2. To monitor the SOA Suite, you can use an agent running locally on the Administration Server of the WebLogic domain or a remote management agent running on another host that is not part of the WebLogic domain. **Note:** If you use a remote agent to monitor the SOA Suite, the Instance Tracing and View Recoverable Instances features are not supported. 3. To ensure the all the metric data is collected, add the `soa-infra-mgmt.jar` and the `oracle-soa-client-api.jar` files to the `$AGENT_HOME/plugins/oracle.sysman.emas.agent.plugin_12.1.0.0.0/archives/jlib/` (the Agent Home directory). If the `extjlib` directory does not exist, it can be created under `$FMW_PLUGIN_HOME/archives/jlib`. This step is required only if you are using a remote agent to monitor the SOA Suite. **Note:** For SOA PS3 and higher, the `jrf-api.jar` file must also be present in the Agent Home directory.

11.4 Discovering the SOA Suite

This section describes the procedure for discovering the SOA Suite 11g. You can use a local or a remote Management Agent to perform the discovery process. In the case of discovery using a local agent, you need to use a Management Agent that is running on the same host as the Administration Server.

1. From the **Targets** menu, select **Middleware**.

   Oracle Enterprise Manager Cloud Control displays the Middleware page that lists all the middleware targets being monitored.

2. In the Middleware page, from the **Add** list, select Oracle Fusion Middleware / WebLogic Domain and click **Go**. Specify the Administration Server Host, Port, User Name, Password, Agent (local or remote) and the JMX Protocol and click **Continue**.

3. You will return to the Middleware page. You will see the SOA instances under the WebLogic Domain.

> **Note:** SOA Composites that are created after the discovery of SOA Suite Domain are not displayed automatically. To view all the SOA Composites, navigate to the Home page of the WebLogic Server target and select the **Refresh Domain** option from the menu.

11.4.1 Discovering the SOA Suite Using a Remote Agent

You can discover the SOA Suite 11g using a remote agent which may be running on a host that is different from the host on which the Administration Server is running. In this case, you may not be able to perform certain operations like instance tracing and viewing recoverable instances.

To ensure the all the metric data is collected, add the `soa-infra-mgmt.jar` and the `oracle-soa-client-api.jar` files to the `$AGENT_HOME/plugins/oracle.sysman.emas.agent.plugin_12.1.0.0.0/archives/jlib/` (the Agent Home directory). If the `extjlib` directory does not exist, it can be created. This step is required only if you are using a remote agent to monitor the SOA Suite.

> **Note:** For SOA PS3 and higher, the `jrf-api.jar` file must also be present in the Agent Home directory.

11.5 Post Discovery Steps

After discovering the SOA Suite 11g, you must perform the following additional configuration steps:

1. Set the instance state in the Common Properties page:
   a. Click **Fusion Middleware Control** on the SOA Infrastructure Home Page.
   b. Navigate to the Home page of the SOA Infrastructure target.
   c. Select **Common Properties** from the SOA-Infra drop-down menu.
   d. On the Common Properties page, select the **Capture Composite Instance State** check box.
2. Set the SOA database details like the host name, port, and credentials.
   a. Navigate to the Middleware page in Enterprise Manager Cloud Control.
   b. Select a SOA Infrastructure home from the list and click **Configure**.
   c. The SOA Infrastructure Home page is displayed. Click **Monitoring Configuration** from the SOA-Infra drop-down menu.
   d. Set the SOA database details in the Monitoring Configuration page.
3. Set preferred credentials for the WebLogic Domain.
   a. From the **Setup** menu, select **Security**, then select **Preferred Credentials**.
   b. Select the Oracle WebLogic Domain target and click **Managed Preferred Credentials**.
   c. Select WebLogic Administrator Credentials in the Target Preferred Credentials and click **Set**.

d. Enter the user name and password in the Select Named Credentials window and click **Save**.

11.5.1 Configuring Instance Tracing

To enable Instance Tracing for any SOA Infrastructure instances involved in executing composite instances:

1. Follow the sequence listed under Step 3 of the Section 11.5, "Post Discovery Steps" section.
2. To view the state of the listed instances, enable the Capture Composite State flag by following the sequence listed Step 1 of the Section 11.5, "Post Discovery Steps" section.

11.5.2 Viewing Application Dependency and Performance (ADP) Metrics

If the SOA instance is being monitored by the ADP Manager, additional metrics such as Arrival Rate, Minimum, Maximum, and Average Response Time will be collected.

> **Tip:** The ADP Manager must be registered before it can collect the metric data. For details on registering the ADP Manager, see *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

11.6 Setting Up and Using SOA Instance Tracing

To configure and trace a SOA Composite instance, follow these steps:

1. Login to Enterprise Manager and navigate to the SOA Composite Home page of the instance to be traced.
2. From the **SOA Composite** menu, select **Trace Instance**.
3. Find the instance you want to trace by specifying search criteria such as Instance ID, Instance Creation Time Window, Instance Count, Sensor Values and so on. Click **Search**.

> **Note:** You must set the Preferred Credentials must be set for the WebLogic Domain and the Monitoring Agent Host to retrieve search data.
>
> - WebLogic Domain: To set the Administrator Credentials for the WebLogic Domain (SOA Domain Target), select **Security**, then select **Preferred Credentials** from the **Setup** menu. Select Oracle WebLogic Domain as the Target Type and click **Manage Preferred Credentials**. Specify the WebLogic Administrator credentials and click OK.
> - Monitoring Agent Host: To set the Preferred Credentials for the host on which the Management Agent has been installed, select **Security**, then select **Preferred Credentials** from the **Setup** menu. Select Host as the Target Type and click **Manage Preferred Credentials**. Specify the Normal Host Credentials for the host and click **OK**.

4. The list of instances that match the search criteria is displayed. Select the instance you want to trace and click **Trace**.

5. In the Select SOA Infrastructure window, select one or more SOA Infrastructure targets for which the trace information is to be gathered. Specify the WebLogic Administration and Host Credentials for these targets and click **OK**.
6. A trace job is submitted to collect the instance trace data from the selected targets and the flow trace for the instance is generated.
7. When the job has been completed, click **Job Status** to view the flow trace data. Click the **Log Viewer** link to access the log messages related to the instance.
8. Click the **Component Instance** to drill down to the component instance audit trail which shows the activity level execution details.

11.7 Generating SOA Reports Using Information Publisher

This section describes the procedure to create SOA Reports.

1. From the Targets menu, select **Middleware**, and click on a SOA Infrastructure target. The SOA Infrastructure Home page appears.
2. From the SOA Infrastructure menu, select the **Information Publisher Reports**.

   The out-of-box SOA reports are displayed under the SOA Performance Reports section.
3. Select a report from the section (for example, you can select **Pending Instance Statistics**) and click **Create Like**. The Create Report Definition page is displayed.
4. In the General page, enter the following details:
   a. Enter the BPEL Process Name as the title.
   b. Click the Set Time Period to set the time interval for the report.
   c. Click the **Run report using target privileges of the Report Owner (SYSMAN)** check box in the Privileges section.
5. Click the **Elements** tab and click the **Set Parameters** icon for the Pending Instance Statistics Element in the table.
6. In the Set Parameters page, click the torch icon to select a Composite Name. The Result Set Size with default values for the Pending Instance Statistics report is displayed.
7. Select a Component Name from the list, enter the Result Set Size and click **Continue** to return to the Elements page.
8. The selected target name is displayed in the Elements table.
9. To schedule periodic report generation, click the **Schedule** tab.
10. Specify the schedule type and other details and click **OK**.
11. You will return to the Report Home page where the newly scheduled report is displayed in the table. Click the report name to view the details.

11.8 Dehydration Store Monitoring

The Dehydration Store Diagnostics feature provides a dedicated view that allows you to analyze the behavior of the SOA Dehydration database. You can monitor SQL performance metrics and table growth specifically in the context of the SOA Suite's use of the database. The view displays both throughput and wait bottleneck data which allows you to monitor the general health of the target database instance. Using Active

Session History, you can track usage data and display it as a table space chart, a growth rate chart, or an execution chart.

11.8.1 Enabling Monitoring of the SOA Dehydration Store

To configure and enable monitoring of the SOA Dehydration Store, follow these steps:

1. From the **Targets** menu, select **Databases** to check if the database target representing the SOA Dehydration Store has been discovered in Enterprise Manager.
2. Check if at least one configuration for the SOA Infrastructure and WebLogic Server targets is available.
3. On the monitoring configuration for the SOA Infrastructure target, the following fields related to SOA Repository must be configured:
   - SOA Repository Connection Descriptor: The connection URL string specified for the JDBC data source on the WebLogic server. This configuration is collected as part of the configuration collection mechanism for the SOA Server instance. For example: `jdbc.oracle.thin@host:port/sid` (or service_name).
   - SOA Repository Host Name: The database listener host for the SOA database instance. This is optional if the connection string has already been configured.
   - SOA Repository Port: - The database listener port for the SOA database instance. This is optional if the connection string has already been configured.
   - SOA Repository Schema Name: The schema name configured for SOA Dehydration Store.
   - SOA Repository User Name: The schema name configured for SOA Dehydration Store.
   - SOA Repository Password: The password for the SOA schema user.SOA Repository SID: The SID for the SOA database instance.

If you do not see data after these configuration details have been specified, you must wait for the next collection interval.

11.8.2 Viewing the SOA Dehydration Store Data

To view the dehydration diagnostics data, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a SOA Infrastructure target.
2. In the SOA Infrastructure Home page, click the **Dehydration Store** tab.
3. The following details area displayed:
   - Throughput indicators that provide details of the general health of the database instance.
   - Wait bottleneck issues related to the CPU, I/O, and Wait events.
   - Tablespace utilization for the SOA schema.
   - Performance data recorded by the ASH.
   - Key SOA tables and tablespace details related to the SOA schema.

11.9 Service Topology

The Service Topology provides a graphical end to end view of the composite applications. It depicts the various application components and their interactions happening at runtime. It allows you to view the service level dependencies among the components and provides key performance statistics and incidents information for them. Composite applications are distributed in nature and this view helps you quickly visualize the structure, status, availability, dependencies, configuration changes, and performance of business-critical distributed applications from one place and easily identify any availability or performance issues.

The Service Topology Viewer shows the following:

- Service to Service Calls: It allows you to view the Service to Service calls between any two SOA entities (Composites/J2EE Applications/OSB/BPEL 10g instances) by clicking the link between the entities.
- Dependency Highlighting: It allows you to view the dependencies for any service. If you click on a service, all the services that it is dependent on and vice versa are highlighted.
- Database Associations: Shows all the databases used by the SOA Composites, BPEL 10g instance and J2EE applications.
- External Services: Shows the services that are used by a SOA Composite application but are external to it or not managed by Enterprise Manager Cloud Control.

For more details, refer to the Enterprise Manager Online Help.

11.10 UDDI Publishing

To publish a service to UDDI, navigate to the Services and References Home page, select a service from the table and click **Publish to UDDI** from the menu. The Publish Service to UDDI window is displayed with the following fields:

- Service Name: The name of Web Service to be published to the UDDI Registry. This is a Read Only field.
- Service Description: The description of the selected Web Service.
- Service Definition Location: The URL location of the Service Definition. This is a Read Only field.
- UDDI Source: A logical name for an external UDDI registry source. Select the UDDI Source from the drop-down list.
- Business Name: The name of the data structure in the UDDI registry. Select a Business Name that has been registered with the UDDI from the list.

Click **OK** to start the process that publishes the web service to UDDI or click **Cancel** to cancel publishing the service.

11.11 Generating SOA Reports Using BI Publisher

You can use Enterprise Manager to print SOA reports using BI Publisher Enterprise Reports. Oracle Business Intelligence (BI) Publisher is an enterprise reporting solution for authoring, managing, and delivering highly formatted documents. Oracle BI Publisher also allows you to build custom reporting applications that leverage existing infrastructure. Reports can be designed using familiar desktop products and viewed online or scheduled for delivery to a wide range of destinations.

The following table describes the SOA reports that can be generated using BI Publisher:

Table 11–2 SOA Reports

SOA Report	Description
SOA Infrastructure Performance Report	The SOA Infrastructure Performance Summary Report provides information about the average response time, error rate, throughput, system faults, business faults, web service policy violation faults for selected SOA Composite. It displays a chart with the top 5 SOA Composites based on average response time or throughout across the selected SOA composites for specified time period. The report can be sorted based on performance metric (avg. response time) or the usage metric (instance count). As part of the report parameters setting, you can use options that allow you to select the SOA Composite by Partitions or by selecting individual composites.
SOA Composite Detailed Performance Report	The SOA Composite Detailed Performance Summary Report provides information about the average response time, error rate, throughput, system faults, business faults, web service policy violation faults for each selected composite assembly part such as service, reference, and service component. This is an in-depth report that provides complete details about the each assembly part in the SOA Composite. It displays a chart with the top 5 SOA Composites based on average response time or throughout across the selected SOA Composites for a specified time period. The report can be sorted based on performance metric (avg. response time) or the usage metric (instance count). As part of the report parameters setting, you can use options that allow you to select the SOA Composite by Partitions or by selecting individual composites.
Top 5 SOA Composites (From Dehydration Store)	This report shows how the SOA Composites have been performing over a period of time. Charts listing the top 5 SOA composites are displayed and critical metric data for all the SOA composites are displayed in a table.

To print SOA reports using BI Publisher, follow these steps:

1. From the **Enterprise** menu, select **Reports**, then select **BI Publisher Enterprise Reports**.

   Enterprise Manager Cloud Control displays the login page for BI Publisher Enterprise Reports.

2. Enter your credentials to log into BI Publisher.

3. The BI Publisher Enterprise page displays, showing you Recent reports, Others, and Favorites. You can use this page to create a new report, submit a report job, and perform other tasks.

4. Click the Report you want to view.

5. You can select different filters such as SOA Composite Name, Partition Name, Date Range, and so on to view the report. You can also select a Sort By option to sort the report on Composite Name, Sorted Instances, and so on.

6. You can refresh the report anytime by clicking the **Refresh** icon on the upper right side of the SOA Report tab. You can hide or display the search parameters by clicking the Parameters icon. You can choose to view the report in various formats

such as HTML, PDF, RTF, Excel, and PowerPoint by clicking the **View Report** icon. Likewise you can display more available actions by clicking the **Actions** icon. For more help about using BI Publisher, click the help icon.

11.12 Provisioning SOA Artifacts and Composites

The SOA Artifacts Deployment Procedure allows you to:

- Provision SOA Artifacts from a reference installation or from a gold image
- Create a gold image of the SOA Artifacts
- Provision SOA Composites either from the Software Library or from another accessible location.

For more details on the SOA Artifacts Deployment Procedure, see the *Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching*.

11.13 Support Workbench

The Support Workbench page provides access to diagnostic data for problems and incidents. To view this page, navigate to the SOA Infrastructure Home page, and from the SOA Infrastructure menu, select Diagnostics, then select Support Workbench.

Enter the credentials for the host on which the WebLogic server is running and the WebLogic credentials for the WebLogic server. Click **Continue** to log into the Support Workbench page. On this page, you can do the following:

- View problem or incident details.
- View, create, or modify incident packages.
- View health checker findings
- Close resolved problems.

For more details on using this feature, see the Enterprise Manager Online Help.

11.14 Troubleshooting

This section describes the errors you might encounter while discovering the SOA Suite 11g and the workaround steps you can follow to resolve each of them.

This section covers the following:

- Discovery
- Monitoring
- Instance Tracing
- Faults
- Application Dependency and Performance Integration
- Information Publisher Reports
- BI Publisher Reports
- Systems and Services
- BPEL Recovery
- SOA License Issue

- Dehydration Store Issue

11.14.1 Discovery

The following error occurs when the SOA instances are being discovered.

Table 11–3 Error Message:

Error Message	Workaround Steps
`New SOA Composite deployed on the SOA Server from JDeveloper are not displayed automatically in Enterprise Manager Cloud Control.`	To discover the newly deployed SOA Composites in Enterprise Manager Cloud Control, you must run the **Refresh Farm** menu option for the associated WebLogic Domain.

11.14.2 Monitoring

The following error occurs when the collection frequency causes a delay in the collection of configuration data.

Table 11–4 Error Description

Error Description	Workaround Steps
`All metrics are not displayed.`	Enterprise Manager Cloud Control uses the Management Agent to collect metric data. For the first collection, the agent may need 15 minutes to upload the metric data.

11.14.3 Instance Tracing

The following error occurs when the instance is traced.

Instance Search Fails - Same reason as BPEL first column. If Management Agent is down or unreachable.

Table 11–5 Error Message:

Error Message	Workaround Steps
`Instance Tracing Job Fails`	1. Navigate to the Jobs page and locate the Instance Tracing job (Composite Name + Instance ID + Timestamp in ms) and view the output to identify the step that has failed. 2. Resolve the issue and run the job again by clicking **Retry** on the Jobs page. 3. Navigate to the Instance Tracing page to view the trace results. You can also submit a new job by running the Trace Instance option on the Instance Tracing page.

11.14.4 Faults

The following errors occur when:

- All instances with faults are not displayed as only the last 10 values are collected.
- The most recently collected fault instances do not appear in the Faults and Messages page.

Table 11–6 Error Message:

Error Description	Workaround Steps
`All instances with faults are not populated in Enterprise Manager Cloud Control.`	By default, you can only view the latest 10 faults collected during the last 15 minutes. To view additional faults, navigate to Fusion Middleware by clicking the link in the General section on the target Home page.

11.14.5 Application Dependency and Performance Integration

When you click on the Application Dependency and Performance link in the SOA Instance Home page, you may see a blank page. This error may occur if:

- Application Dependency and Performance is not being used to monitor the SOA instance.
- Application Dependency and Performance has not been registered in Enterprise Manager Cloud Control.

Table 11–7 Error Message:

Error Message	Workaround Steps
`Missing ADP Data - Add the metrics - and add one for blank page.`	To monitor data collected using ADP, the ADP Manager must be registered and configured.

11.14.6 Information Publisher Reports

This section lists report related errors.

Table 11–8 Error Message:

Error Description	Workaround Steps
`Report generation fails due to invalid database details.`	1. Navigate to the All Targets page. 2. Select the SOA Infrastructure target on which the specific SOA Composite has been deployed and click **Configure**. 3. In the Monitoring Configuration page, specify the database connection details and the credentials and click **OK**.
`No targets found message for Oracle SOA Composite Reports.`	You cannot use the out-of-box reports directly. You must use the Create Like option to generate custom reports based on the SOA Composite Target type.
`Report generation fails due to invalid host details.`	Set valid credentials for the host target on which the SOA Infrastructure instance is running.

11.14.7 BI Publisher Reports

This section lists BI Publisher report related errors.

Table 11–9 Error Message:

Error Description	Workaround Steps
`Exception Encountered For One of SOA BIP Report If SOA Dehydration Is Not Configured`	If the SOA Dehydration store details are not configured in BI Publisher, the SOA Composite Report (from Dehydration Store) is not generated, and the following exception message is displayed: `The report cannot be rendered because of an error, please contact the administrator. Parameter name: P_PARTITION_NAME Can not establish database connection(EMSOA)` To work around this issue, you must manually create the SOA database connection by choosing JDBC Connection from the Administration menu after the BI Publisher setup has been configured. The name of the data source name should be EMSOA. Use the following steps to create the EMSOA data source: 1. From the **Enterprise** menu, select **Reports**, and then select **BI Publisher Reports**. The BI Publisher Enterprise login page appears. 2. Enter your credentials to log in to BI Publisher. 3. Click the Administration link available at the top right corner. 4. Navigate to the Data Sources page by clicking the **JDBC Connection** link in the Data Sources section. Click **Add Data Source**. 5. Enter EMSOA in the Data Source field, specify the driver type, driver class, connection string, user name, and password. Click **Test Connection** to ensure that the connection can be established successfully. 6. Click **Apply**. The newly created EMSOA jdbc data source appears on the Data Sources page. Once you have created the EMSOA data source, the issue should be resolved.

11.14.8 Systems and Services

The following error occurs when you try to refresh a service that has not been created.

Table 11–10 Error Message:

Error Message	Workaround Steps
`Create Service option does not work.`	System and service creation depends on the configuration collection of the SOA Infrastructure and related targets. Check the log file for details.
`Refresh Service option does not work.`	The Refresh Service function works for an existing Infrastructure service. In case the service does not exist, it should be created using the Create Service menu option.

11.14.9 BPEL Recovery

The following error occurs when invalid credentials are provided.

Table 11–11 Error Message:

Error Message	Workaround Steps
`Invalid Host and WebLogic Domain Credentials`	For the BPEL Recovery functionality to work, the host credentials and WebLogic Domain credentials must to be available in the preferred credential store. Set the valid credentials and try again.

11.14.10 SOA License Issue

The following error occurs if the SOA Management Pack EE has not been enabled.

Table 11–12 Error Message

Error Message	Workaround Steps
`The page requested is part of the SOA Management Pack EE.`	The SOA Management Pack EE must be enabled for the specific SOA Infrastructure target. To enable the license, follow these steps: 1. From the **Setup** menu, select **Management Packs**, then select **Management Pack Access**. 2. Select SOA Infrastructure in the Target Type drop-down box. 3. Uncheck and check the SOA Management Pack EE. 4. Click **Apply** and navigate to the SOA Composite page.

11.14.11 Dehydration Store Issue

Data is not displayed on the Dehydration Store page.

Table 11–13 Error Message

Error Message	Workaround Steps
`Data is not displayed in the Dehydration Store page.`	This error may occur if there is a data mismatch between the values specified for the database target and the WebLogic Server Datasource. To resolve this issue, follow these steps: 1. Compare the Database Host and SID value of the database target with the value collected for the WebLogic Server JDBC Datasource configuration. 2. If the values are different, select **Services** from the **Targets** menu. Select **DataSources**, then select **SOALocalTxtSource**, then click **Connection Pool** to update the Datasource Connection URL

Part V

Managing Oracle Business Intelligence

The chapter in this part describes how you can discover, monitor, and administer Oracle Business Intelligence instance and Oracle Essbase targets in Enterprise Manager Cloud Control 12*c*.

This part contains the following chapter:

12 Discovering and Monitoring Oracle Business Intelligence Instance and Oracle Essbase

Oracle Business Intelligence (Oracle BI), a part of Oracle Business Analytics, is a combination of technology and applications that provide a range of business intelligence capabilities, such as enterprise performance management, financial performance management, data integration, data warehousing, as well as a number of query, reporting, analysis, and alerting tools.

You can use Enterprise Manager Cloud Control 12c to monitor certain Oracle Business Intelligence targets. Monitoring the status, performance, and health of Oracle Business Intelligence targets enables you to set up a more efficient business intelligence system.

By monitoring a target using Enterprise Manager, you obtain a complete and up to date overview of the status, availability, performance, and health of the target. Enterprise Manager displays complex target performance data in a simple form, using graphs and pie charts. It also keeps you informed about target metrics crossing their threshold levels, target alerts, and target incidents that require user action.

This chapter explains how to monitor Oracle BI Instance and Oracle Essbase targets in Enterprise Manager Cloud Control 12c. It consists of the following sections:

- Overview of Oracle Business Intelligence Targets You Can Monitor
- Understanding the Monitoring Process
- Discovering Oracle Business Intelligence Instance and Oracle Essbase Targets
- Monitoring Oracle Business Intelligence Instance and Essbase Targets
- Administering Oracle Business Intelligence Instance and Essbase Targets

12.1 Overview of Oracle Business Intelligence Targets You Can Monitor

This section gives an overview of the Oracle Business Intelligence targets you can monitor using Enterprise Manager Cloud Control 12c Release 2. It contains the following:

- Oracle Business Intelligence Instance
- Oracle Essbase

12.1.1 Oracle Business Intelligence Instance

Oracle Business Intelligence Instance (BI Instance) is a logical grouping of Business Intelligence components that can be configured as a unit to deliver a single integrated business intelligence capability. Every BI Instance target is part of a WebLogic domain.

For information on WebLogic domains, refer to *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard.*

A BI Instance target consists of a number of components, which can be monitored individually using Enterprise Manager. Table 12–1 describes these components.

Table 12–1 Oracle Business Intelligence Instance Components

Component	Description
BI Server	This component provides query and data access capabilities for Oracle Business Intelligence, and provides services for accessing and managing the enterprise semantic model.
BI Presentation Server	This component provides the framework and interface for the presentation of Oracle Business Intelligence data to web clients. It maintains an Oracle BI Presentation Catalog service on the file system for customizing this presentation framework.
BI Cluster Controller	This component manages Oracle Business Intelligence Server (BI Server) clusters. It also manages the active-passive clustering of the Oracle Business Intelligence Scheduler (BI Scheduler) components.
BI Scheduler	This component provides extensible scheduling for analyses to be delivered to users at specified times.
BI Java Host	This component provides component services that enable Oracle BI Presentation Services to support various components such as Java tasks for Oracle BI Scheduler, Oracle BI Publisher, and graph generation. It also enables Oracle BI Server query access to Hyperion Financial Management and Oracle Online Analytical Processing (OLAP) data sources.

12.1.2 Oracle Essbase

Oracle Essbase is a multidimensional database management system that provides business performance management solutions for meeting the complex calculation requirements of analysts across an enterprise.

Oracle Essbase consists of an Online Analytical Processing (OLAP) server that provides an environment for deploying pre-packaged applications and developing custom analytic and performance management applications. Every Essbase target is part of a WebLogic domain. For information on WebLogic domains, refer to *Oracle Fusion Middleware Creating Domains Using the Configuration Wizard.*

Using Enterprise Manager, you can monitor the Essbase server and every deployed Essbase application individually.

12.2 Understanding the Monitoring Process

To monitor Oracle Business Intelligence Instance (BI Instance) and Oracle Essbase targets, follow these steps:

1. Install Oracle Business Intelligence.

   For information on how to install Oracle Business Intelligence, refer to *Oracle Fusion Middleware Installation Guide for Oracle Business Intelligence.*

2. Install the Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2.0) system. If you are using an earlier version of Enterprise Manager Cloud Control, upgrade it to 12c Release 2 (12.1.0.2.0).

For information on how to install the Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2.0) system, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

For information on how to upgrade to Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2.0), refer to *Oracle Enterprise Manager Cloud Control Upgrade Guide.*

> **Note:** Oracle recommends that you install the Enterprise Manager Cloud Control system on a different host, other than the one on which you have installed Oracle Business Intelligence.

3. If the host on which you installed Oracle Business Intelligence does not have Oracle Management Agent (Management Agent) installed, install a 12.1.0.2.0 Management Agent. If the host has a Management Agent of version earlier than 12.1.0.2.0 installed, upgrade the Management Agent to 12.1.0.2.0.

   For information on how to install a Management Agent, refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide.*

   For information on how to upgrade a Management Agent to 12.1.0.2.0, refer to *Oracle Enterprise Manager Cloud Control Upgrade Guide.*

4. If the host on which you installed Oracle Business Intelligence does not have the Oracle Fusion Middleware plug-in installed, deploy the 12.1.0.3.0 Oracle Fusion Middleware plug-in on the host. If an earlier version of the plug-in exists on the host, upgrade it to 12.1.0.3.0.

   The Oracle Fusion Middleware plug-in (12.1.0.3.0) is a default plug-in that is downloaded to the OMS host when you install a 12.1.0.2.0 OMS.

   For information on how to deploy a plug-in and upgrade an existing plug-in, refer to the Using Plug-Ins chapter of the *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

5. Discover the required BI Instance and Essbase targets.

   BI Instance and Essbase targets are automatically discovered when you discover the WebLogic domain that they are part of.

   The BI Instance and Essbase targets you want to monitor may be part of an undiscovered WebLogic domain, or a previously discovered WebLogic domain.

   For information on how to discover BI Instance and Essbase targets part of an undiscovered WebLogic domain, see Section 12.3.1.

   For information on how to discover BI Instance and Essbase targets part of a previously discovered WebLogic domain, see Section 12.3.2.

6. Monitor the BI Instance and Essbase targets.

   For information on how to monitor BI Instance and Essbase targets, see Section 12.4.

12.3 Discovering Oracle Business Intelligence Instance and Oracle Essbase Targets

Oracle Business Intelligence Instance (BI Instance) and Oracle Essbase targets you want to discover may be part of an undiscovered WebLogic domain, or a discovered WebLogic domain.

This section contains the following:

- Discovering Targets of an Undiscovered WebLogic Domain
- Discovering New or Modified Targets of a Discovered WebLogic Domain

---

Note: This section is applicable only for Oracle Business Intelligence Enterprise Edition 11g targets.

12.3.1 Discovering Targets of an Undiscovered WebLogic Domain

To discover BI Instance and Essbase targets part of an undiscovered WebLogic domain, first discover the WebLogic domain that the targets are part of. To do so, either enable the automatic discovery of WebLogic domains, or discover the required WebLogic domains manually. After discovering the WebLogic domains, you must promote the targets and assign Management Agents to monitor them.

The following sections explain how to perform these actions.

Enabling Automatic Discovery of Targets

In this method, you enable the automatic discovery of Fusion Middleware targets to automatically discover the various WebLogic domains in the enterprise. Also, you promote the BI Instance and Essbase targets part of the WebLogic domains, and assign Management Agents to monitor these targets. For information on how to use this method, see Section 2.1.

Discovering Targets Manually

In this method, you manually discover WebLogic domains. Also, you promote the BI Instance and Essbase targets part of the WebLogic domains, and assign Management Agents to monitor these targets. For information on how to use this method, see Section 2.2.

12.3.2 Discovering New or Modified Targets of a Discovered WebLogic Domain

In a typical enterprise, WebLogic domains are not static. New or modified domain members, such as BI Instance and Essbase targets, may be added to a discovered WebLogic domain at any point of time. Either enable the automatic discovery of these added targets, or discover them manually. After discovering these targets, you must promote the targets and assign Management Agents to monitor them.

The following sections explain how to perform these actions.

Enabling Automatic Discovery of Targets

In this method, you enable the automatic discovery of new or modified WebLogic domain member targets, such as BI Instance and Essbase targets. Also, you promote the new or modified domain member targets, and assign Management Agents to monitor them. For information on how to use this method, see Section 2.3.1.

Discovering Targets Manually

In this method, you manually check a WebLogic domain for new members, such as BI Instance and Essbase targets, and discover them. Also, you promote the new or modified domain member targets, and assign Management Agents to monitor them. For information on how to use this method, see Section 2.3.2.

12.4 Monitoring Oracle Business Intelligence Instance and Essbase Targets

To monitor Oracle Business Intelligence Instance (BI Instance) and Essbase targets, navigate to the home page of the required target.

To navigate to the home page of a BI Instance or Essbase target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.

Using the target home page, you can perform a number of monitoring tasks. These tasks are described in this section, which contains the following:

- Performing General Monitoring Tasks
- Performing Target-Specific Monitoring Tasks

> **Note:** This section is applicable only for Oracle Business Intelligence Enterprise Edition 11g targets.

12.4.1 Performing General Monitoring Tasks

This section explains how to perform general BI Instance and Essbase target monitoring tasks, such as viewing target status and availability, performance, health, alerts, incidents, and so on.

This section contains the following elements:

General

- Viewing Target General and Availability Summary
- Viewing Target Status and Availability History

Performance

- Viewing Target Performance or Resource Usage
- Viewing Target Metrics
- Viewing or Editing Target Metric and Collection Settings
- Viewing Target Metric Collection Errors

Health

- Viewing Target Health
- Viewing Target Alert History
- Viewing Target Incidents
- Viewing Target Logs

Configuration, Jobs, and Compliance

- Viewing Target Configuration and Configuration File
- Viewing Target Job Activity

- Viewing Target Compliance

12.4.1.1 Viewing Target General and Availability Summary

To view a general summary of the target details, navigate to the **Summary** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.

The **Summary** section provides background information about the target, which helps you locate the target binaries, log files, metadata and configuration files, for viewing or editing purposes.

Table 12–2 describes the elements of the **Summary** section.

Table 12–2 Target General and Availability Summary

Element	Description
Up Since	*(Displayed only when the target is up)* Time the target was last started successfully.
Down Since	*(Displayed only when the target is down)* Time the target was last stopped.
Availability	Percentage availability of the target.
Version	Version of the target software.
Oracle Home	Location of the target binaries.
Oracle Instance	Location of the target content files, metadata, configuration files and log files.
Port	Port used by the target for communication.
Running Applications (Only for Essbase Server targets)	Number of Essbase applications currently up and running.
Unexposed Applications (Only for Essbase Server targets)	Number of Essbase applications currently not being accessed by any user.
Connected Users (Only for Essbase Server targets)	Number of users currently connected through one or more of the applications.
Storage Type (Only for Essbase application targets)	Type of data storage used by the application.
Cubes (Only for Essbase application targets)	Number of cubes contained in the application.
Query Tracking (Only for Essbase application targets)	Whether or not query tracking, that is, tracking data combinations having a large number of data values that require aggregation, is enabled.

Table 12–2 (Cont.) Target General and Availability Summary

Element	Description
Memory Usage (MB) (Only for Essbase application targets)	Memory used by the application in MB.
Threads (Only for Essbase application targets)	Number of application threads.

12.4.1.2 Viewing Target Status and Availability History

To view the status and availability history of a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **Status History.**

Sometimes, due to network problems and system errors, the target might be down, or the Oracle Management Service (OMS) might not be able to reach the Management Agent that monitors the target. The Availability (Status History) page provides information about when, and for how long these situations occurred for a particular target. This information is essential for troubleshooting target related incidents.

The Availability (Status History) page consists of the **Overall Availability, Downtime History,** and **General** sections. The **Overall Availability** section consists of a pie chart depicting the availability of the target, from the time it was discovered. The **Downtime History** section provides detailed information about the periods when the target was down.

Table 12–3 describes the elements of the **General** section.

Table 12–3 Target Status and Availability History

Element	Description
Current Status	Current status of the target, whether it is up and running, or down.
Up Since	*(Displayed only when the target is up)* Time the target was last started successfully.
Down Since	*(Displayed only when the target is down)* Time the target was last stopped.
Availability (%)	Percentage availability of the target.
Down Time (minutes)	Duration for which the target was down.
Blackout Time (minutes)	Total duration of blackouts set on the target.
Agent Down Time (minutes)	Duration for which the Oracle Management Agent monitoring the target was down.
System Error Time (minutes)	Duration for which the target could not be monitored, due to a system error.

Table 12–3 (Cont.) Target Status and Availability History

Element	Description
Status Pending Time (minutes)	Duration for which the status of the target could not be determined.

12.4.1.3 Viewing Target Performance or Resource Usage

To view the performance or resource usage of a target, navigate to the **Response** or **CPU and Memory Usage** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target. Graphs depicting the target performance or target resource usage are displayed.
4. (Optional) To view the performance or resource usage data in a tabular format, click **Table View.**

> **Note:** For the BI Instance, BI Server, and BI Presentation Server targets, you can view only performance data, and not resource usage data, on the target home page. For other BI Instance component targets, and Essbase targets, you can view only resource usage data and not performance data on the target home page.

Target Performance

The **Response and Load** section displays the performance of the BI Instance, BI Server, or BI Presentation Server target. For these targets, the **Response and Load** section can consist of the following graphs:

- The variation of Average Query Time with time

  Average Query Time is the average time the BI Server or BI Presentation Server takes to execute a query. The Average Query Time is collected and uploaded to the Oracle Management Repository every fifteen minutes, by default.

- The variation of Server Queries (per second) with time

  Server Queries (per second) is the number of queries processed by the BI Server or BI Presentation Server in one second. Server Queries (per second) is collected and uploaded to the Oracle Management Repository every fifteen minutes, by default.

- The variation of Completed Requests (per second) with time

  Completed Requests (per second) is the number of requests completed by the BI Presentation Server in one second. Completed Requests (per second) is collected and uploaded to the Oracle Management Repository every fifteen minutes, by default.

Carefully observing these graphs can sometimes provide early warnings about server overloading, reduced server access, and so on. Analyzing graphical data collected over a long period of time can help you set up a more efficient BI Server or BI Presentation Server.

For detailed information on target performance, access the Performance Summary page. To access this page, from the **Business Intelligence Instance, BI Server** or **BI Presentation Services** menu, select **Monitoring,** then select **Performance Summary.**

Target Resource Usage

The **CPU and Memory Usage** section displays the resource usage of the target. It consists of two graphs:

- The variation of CPU Usage (%) with time

  CPU Usage specifies the percentage of CPU time used by the target. A large value of CPU Usage can cause the Business Intelligence components and applications to slow down, reducing their performance. The CPU Usage is collected and uploaded to the Oracle Management Repository every fifteen minutes, by default.

- The variation of Memory Usage (MB) with time

  Memory Usage specifies the amount of memory used by the target. A large value of Memory Usage can cause the Business Intelligence components and applications to slow down. The Memory Usage is collected and uploaded to the Oracle Management Repository every fifteen minutes, by default.

Carefully observing these graphs can sometimes provide early warnings about application overloading, component downtime, and so on.

12.4.1.4 Viewing Target Metrics

To view all the metrics collected for a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **All Metrics.**

The All Metrics page displays details about all the metrics collected for a particular target. The average value, threshold values, collection schedule, and metric value history is displayed for each collected metric.

12.4.1.5 Viewing or Editing Target Metric and Collection Settings

To view and edit the metric and collection settings for a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **Metric and Collection Settings.**
5. To edit the collection schedule or thresholds of a metric, or any other collected item, click the corresponding icon present in the **Edit** column.

The Metric and Collection Settings page provides details about target metric collection thresholds and target metric collection schedules. Using this page, administrators can edit the warning threshold and critical threshold values of target metrics and other collected items, as well as the time intervals at which these are collected.

12.4.1.6 Viewing Target Metric Collection Errors

To view the metric collection errors for a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **Metric Collection Errors.**

The Metric Collection Errors page provides details about the errors encountered while obtaining target metrics. These details give you an idea of the metrics that may not represent the performance of the target accurately, as errors were encountered while collecting them.

12.4.1.7 Viewing Target Health

To view a summary of the health of the target, navigate to the **Monitoring and Diagnostics** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.

The **Monitoring and Diagnostics** section specifies the number of abnormal occurrences related to the target that require user action, and the number of changes made to the target configuration, within a particular time interval. This information is useful to administrators who want to quickly get an idea of the overall health of the target, and know the number of issues that need to be resolved. For more details on target configuration, access **Configuration** from the BI Instance component menu or Essbase target menu.

Table 12–4 describes the elements of the **Monitoring and Diagnostics** section.

Table 12–4 Target Health

Element	Description
Incidents	The number of unresolved situations or issues that impact the target negatively, and hence require user action. The displayed integer is also a link to the Incident Manager page.
Descendant Target Incidents (Only for Essbase Server Targets)	The number of incidents related to Essbase applications. The displayed integer is also a link to the Incident Manager page.
Configuration Changes	The number of changes made to the target configuration in the last seven days. The displayed integer is also a link to the Configuration History page.

12.4.1.8 Viewing Target Alert History

To view the alert history of a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **Alert History.**

The Alert History page provides details about target metrics, such as the periods when a particular metric was beyond its critical threshold value, the periods when the metric could not be calculated, and so on. These details help you plan corrective measures for metric-related problems, before any severe damage or prolonged downtime can occur.

Table 12–5 describes the elements of the Alert History page.

Table 12–5 Target Alert History

Element	Description
Metric	Parameter related to the performance of the target.
History	Condition of the metric at various times. The condition can have the values Critical, Warning, Clear, and No Data.

12.4.1.9 Viewing Target Incidents

To view the incidents related to the target, navigate to the **Incidents** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.

The **Incidents** section provides details about the various events, related to the target, that negatively impact the business intelligence system. These events require user action. The details provided by this section, such as the incident summary, severity, target, target type, and so on, are essential for troubleshooting.

For detailed reports on target incidents, access the Incident Manager page. To access this page, from the BI Instance component menu or Essbase target menu, select **Monitoring,** then select **Incident Manager.**

For details on the elements of the **Incidents** section, refer to *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

12.4.1.10 Viewing Target Logs

To view the log messages related to a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.

3. From the BI Instance component or Essbase target menu displayed on the target home page, select **Logs,** then select **View Log Messages.**
4. (Optional) To view or download the target log files, click **Target Log Files,** select the required log file, then click **View Log File** or **Download,** respectively.
5. (Optional) To export log messages to a file, from the Log Messages page, select the required messages. From the **Export Messages to File** menu, click the file format you want to export the selected messages to. Choose a location, and download the file.

The target logs are a repository of target error messages, warnings, and notifications. They can be used for tracing the intermediate steps of an operation, and are essential for troubleshooting incidents and problems.

You can use the Log Messages page to view all log messages, search for a particular message, view messages related to a message, export messages to a file, view the target log files, and download the log files. For more information about log files, refer to *Oracle Enterprise Manager Cloud Control Administrator's Guide.*

For the BI Instance target, this page displays log messages related to all system components and Java EE components. For the BI Instance component targets and Essbase targets, this page displays only those log messages that are related to the target.

Table 12–6 describes the elements of the Log Messages page.

Table 12–6 Target Log Messages

Element	Description
Time	Date and time when the log message was created.
Message Type	Type of the log message. Message Type can be Incident Error, Error, Warning, Notification, Trace, or Unknown. These types represent the decreasing severity of messages, with Trace representing the least severe message and Incident Error representing the most severe message. Unknown indicates that Message Type is not known.
Message ID	9-digit string that uniquely identifies the message within the framework.
Message	Text of the log message.
Execution Context ID (ECID)	Global unique identifier of the execution of a particular request, in which a target component participates. You can use the ECID to correlate error messages from different target components.
Relationship ID	Identifier which distinguishes the work done by a particular thread on a particular process, from the work done by any other thread on the same, or any other process, on behalf of the same request.
Component	Target component that generated the message.
Module	Identifier of the module that generated the message.
Incident ID	Identifier of the incident to which the message corresponds.
Instance	Oracle Instance containing the target component that generated the message.
Message Group	Group containing the message.
Message Level	An integer value representing the severity of the message. Ranges from 1 (most severe) to 32 (least severe).

Table 12–6 (Cont.) Target Log Messages

Element	Description
Hosting Client	Identifier of the client or security group related to the message.
Organization	Organization ID for the target component that generated the message. This ID is `oracle` for all Oracle components.
Host	Name of the host where the message was generated.
Host IP Address	Network address of the host where the message was generated.
User	User whose execution context generated the message.
Process ID	Identifier of the process or execution unit that generated the message.
Thread ID	Identifier of the thread that generated the message.
Upstream Component	Component that the message generating component works with, on the client side.
Downstream Component	Component that the message generating component works with, on the server side.
Detail Location	URL linking to additional information about the message.
Supplemental Detail	Detailed information about the message, more detailed than the message text.
Target Log Files	Link to the target log files.
Log File	Log file containing the message.

12.4.1.11 Viewing Target Configuration and Configuration File

To view the configuration data of a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Configuration,** then select **Last Collected** to access the Target Configuration browser.
5. (Optional) To export target configuration data to a configuration file, click **Export.** The exported target configuration data is stored in a `.xls` file.

Use the Target Configuration browser to view the latest configuration data of the target. Using the browser, you can also search for configuration data, view saved target configurations, compare target configurations, and view the target configuration history.

12.4.1.12 Viewing Target Job Activity

To view the past, currently running, and scheduled jobs related to a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.

3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Job Activity.**

The Job Activity page displays target jobs related to target administrative tasks, such as starting the target, stopping the target, target blackouts, and so on.

Use the Job Activity page to search for a particular job and retrieve job details such as the owner, status, scheduled start time, and so on. You can also use the Job Activity page to perform target job administration tasks, such as creating, editing, suspending, and resuming a job.

12.4.1.13 Viewing Target Compliance

To view the compliance of a target to compliance standards or compliance frameworks, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Compliance,** then select **Results.**
5. To view the compliance results of a target with respect to a particular compliance standard, select **Compliance Standards.** To view the compliance results of a target with respect to a particular compliance framework, select **Compliance Frameworks.**

Use the Compliance Results page to view the compliance of a target to compliance standards and compliance frameworks. This page also lists the number of violations made to compliance standards and compliance frameworks, hence giving you an idea of whether the targets in your enterprise adhere to established standards or not.

For more information on target compliance, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*

12.4.2 Performing Target-Specific Monitoring Tasks

This section explains how you can perform target-specific BI Instance and Essbase target monitoring tasks, such as viewing BI Instance dashboard reports, BI Instance scheduler reports, Essbase application data storage details, and so on.

This section contains the following:

BI Instance

- Viewing Oracle Business Intelligence Dashboard Reports
- Viewing Oracle Business Intelligence Scheduler Reports
- Viewing Oracle Business Intelligence Instance Key Metrics

Essbase

- Viewing Oracle Business Intelligence Essbase Applications Summary
- Viewing Oracle Business Intelligence Essbase Application Data Storage Details

12.4.2.1 Viewing Oracle Business Intelligence Dashboard Reports

To view Oracle Business Intelligence dashboard reports, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance. Click the BI Instance name.
3. From the **Business Intelligence Instance** menu, select **Dashboard Reports.**
4. From the **View** list, select the set of dashboard reports you want to view.

> **Note:** To view Oracle Business Intelligence dashboard reports in Enterprise Manager Cloud Control, you must enable usage tracking. For information on how to enable usage tracking, refer to the Managing Usage Tracking chapter of the *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition.*

Using this page, you can view the dashboard usage in the past 7 days, the dashboards that failed in the past 24 hours, the top dashboards by resource usage in the past 7 days, and the top users by resource usage in the past 7 days. These details tell you which dashboards are the most popular, which dashboards failed recently, which dashboards use the maximum resources, and which user is the most active. An in-depth analysis of these details can provide important insights into the functioning of an enterprise.

> **Note:** Without specifying the correct credentials on the Monitoring Credentials page, you cannot access certain dashboard reports. Hence, ensure that you specify the appropriate credentials on the Monitoring Credentials page, before accessing the Dashboard Reports page.
>
> To access the Monitoring Credentials page, from the **Business Intelligence Instance** menu, select **Target Setup,** then select **Monitoring Credentials.**

Table 12–7 describes the elements of the Dashboard Reports page.

Table 12–7 Oracle Business Intelligence Dashboard Reports

Element	Description
User	User who accessed the dashboard.
Total Sessions	Total number of user sessions which accessed the dashboard.
Last Accessed On	Time when the dashboard was last accessed.
Dashboard	Dashboard name.
Error Code	Dashboard error code.
Error Message	Dashboard error message.
Repository	Name of the repository accessed by the dashboard.
Subject Area	Information about business areas, or the groups of users in an organization.
Start Time	Time when the server received the logical request for the dashboard.

Table 12–7 (Cont.) Oracle Business Intelligence Dashboard Reports

Element	Description
End Time	Time when the server completed servicing the logical request for the dashboard.
View Log Messages	View log messages related to the dashboard.
Total Time	Total time taken to service all logical requests made for a particular dashboard. **Note:** In the Top Users by Resource Usage in Last 7 Days reports, this element represents the total time taken to service all logical requests made by a particular user.
Database Time	Time taken by the database to complete all physical requests made for a particular dashboard. **Note:** In the Top Users by Resource Usage in Last 7 Days reports, this element represents the time taken by the database to complete all physical requests made by a particular user.
Compile Time	Time taken to convert all logical requests made for a particular dashboard. **Note:** In the Top Users by Resource Usage in Last 7 Days reports, this element represents the time taken to convert all logical requests made by a particular user, to physical requests.
Failed Logical Requests	Number of logical requests made for the dashboard that failed. **Note:** In the Top Users by Resource Usage in Last 7 Days reports, this element represents the number of logical requests made by a particular user that failed.
Total Logical Requests	Total number of logical requests made for the dashboard. **Note:** In the Top Users by Resource Usage in Last 7 Days reports, this element represents the total number of logical requests made by a particular user.

12.4.2.2 Viewing Oracle Business Intelligence Scheduler Reports

To view Oracle Business Intelligence scheduler reports, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance. Click the BI Instance name.
3. From the **Business Intelligence Instance** menu, select **Scheduler Reports.**
4. From the **View** list, select the set of scheduler reports you want to view.

Using this page, you can view the BI Instance target jobs that failed in the past 24 hours, and the BI Instance target jobs that have been scheduled to begin later. These details inform you about the jobs that failed recently and the jobs scheduled to take place in the future, giving you a summary of the BI Instance past and future job activity.

Table 12–8 describes the elements of the Scheduler Reports page.

Table 12–8 Oracle Business Intelligence Instance Scheduler Reports

Element	Description
Job Name	Name of the job, as specified by the user who created it.
Instance ID	ID of the job instance.

Table 12–8 (Cont.) Oracle Business Intelligence Instance Scheduler Reports

Element	Description
Job ID	ID of the job.
Start Time	Time the job started.
End Time	Time the job ended or failed.
Error Message	Error message of the failed job.
User	User who created the job.
Scheduled Time	Time the job is scheduled to begin.
Script Type	Type of script to be executed.

12.4.2.3 Viewing Oracle Business Intelligence Instance Key Metrics

To view the key metrics related to the BI Instance target, navigate to the **Metrics** section by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance. Click the BI Instance name.

The **Metrics** section displays the key metrics used to monitor the performance of the BI Instance. Analyzing these metrics provides early warnings of errors and incidents, and helps you identify problem areas quickly.

To view all BI Instance metrics, access the All Metrics page. To access this page, from the **Business Intelligence Instance** menu, select **Monitoring,** then select **All Metrics.** For more information on this page, see Section 12.4.1.4.

Table 12–9 describes the elements of the **Metrics** section.

Table 12–9 Oracle Business Intelligence Instance Key Metrics

Metric	Description
Request Processing Time (ms)	Average time, in milliseconds, taken by the BI Servers to process a request. This metric is collected from the time the BI Analytics application was last started.
SOA Request Processing Time (ms)	Average time, in milliseconds, taken by the Oracle WebLogic Server cluster to process a web services request. This metric is collected from the time the BI SOA application was last started.
Average Query Time (seconds)	Average time, in seconds, taken by the BI Servers to process a query. This metric is collected from the time the BI Server was last started.
Active Sessions	Total number of active sessions for the BI Instance. This metric is collected from the time the BI Analytics application was last started.
Requests (per minute)	Average number of requests, per minute, received by the BI Servers. This metric is collected from the time the BI Analytics application was last started.
SOA Requests (per minute)	Average number of servlet and/or JavaServer Pages (JSP) invocations, per minute, for web services requests across the Oracle WebLogic Server cluster. This metric is collected from the time the BI SOA application was last started.
Presentation Services Requests (per second)	Average number of requests, per second, received by the BI Presentation Servers. This metric is collected from the time the BI Presentation Server was last started.

Table 12–9 (Cont.) Oracle Business Intelligence Instance Key Metrics

Metric	Description
Server Queries (per second)	Average number of queries, per second, completed by the BI Servers. This metric is collected from the time the BI Server was last started.
Failed Queries	Number of failed BI Server queries. This metric is collected from the time the BI Presentation Server was last started.

12.4.2.4 Viewing Oracle Business Intelligence Essbase Applications Summary

To view a summary of Oracle Business Intelligence Essbase applications, navigate to the **Applications** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having an Essbase Server target. Click the Essbase Server name.

The **Applications** section provides details about the status, resource usage, and data storage type of the various Essbase applications under the Essbase server. This section is useful to administrators who want to quickly obtain an overview of the availability and storage details of the Essbase applications being monitored.

> **Note:** If the applications displayed in the **Applications** section are different from the ones displayed in the **Target Navigation** window, refresh the Oracle Fusion Middleware farm. To do this, from the **Target Navigation** window, click the Oracle Fusion Middleware farm name. From the **Farm** menu, click **Refresh WebLogic Domain.** Click **Add/Update Targets.**

Table 12–10 describes the elements of this section.

Table 12–10 Oracle Business Intelligence Essbase Applications Summary

Element	Description
Name	Name of the application.
Status	Application status, whether the application is up or down.
Storage Type	Type of application data storage.
Memory Usage (MB)	Memory, in MB, used by the application.
Cubes	Number of cubes contained in the application.

12.4.2.5 Viewing Oracle Business Intelligence Essbase Application Data Storage Details

To view details about how data for an Oracle Business Intelligence Essbase application is stored, navigate to the **Cubes** section, by following these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having an Essbase Server target. Click the Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required Essbase application.

The **Cubes** section provides structural and usage information about the cubes contained in the Essbase application. These details tell you about how data storage is designed for the application, and how accessible the application data is at the moment.

Table 12–11 describes the elements of this section.

Table 12–11 Oracle Business Intelligence Essbase Application Data Storage Details

Element	Description
Name	Name of the cube.
Dimensions	Number of dimensions the cube has.
Connected Users	Number of users currently connected to the cube data.
Locks	Number of data block locks currently held on the cube.
Data Cache Size (KB)	Size, in KB, of the buffer in memory that holds uncompressed data blocks.

12.5 Administering Oracle Business Intelligence Instance and Essbase Targets

To administer Oracle Business Intelligence Instance (BI Instance) and Essbase targets using Enterprise Manager Cloud Control, navigate to the home page of the required target. For information on how to do this, see Section 12.4.

Using Enterprise Manager Cloud Control, you can perform general, as well as target specific administration tasks.

This section contains the following:

- Performing General Administration Tasks
- Performing Target-Specific Administration Tasks

Note: This section is applicable only for Oracle Business Intelligence Enterprise Edition 11g targets.

12.5.1 Performing General Administration Tasks

This section explains how to perform general BI Instance and Essbase target administration tasks, such as starting, stopping, or restarting the target, administering target access privileges, administering target blackouts, and so on.

This section contains the following:

- Starting, Stopping, or Restarting the Target
- Administering Target Access Privileges
- Administering Target Blackouts
- Viewing Target Monitoring Configuration

12.5.1.1 Starting, Stopping, or Restarting the Target

To start, stop, or restart a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.

3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. Click **Start Up, Shut Down,** or **Restart** to start, stop, or restart the target, respectively. Alternatively, from the BI Instance component menu or Essbase target menu, select **Control,** then select **Start Up, Shut Down,** or **Restart.**

To run certain patching and maintenance tasks, you may need to stop the target, perform the task, and restart it once the operation is complete.

12.5.1.2 Administering Target Access Privileges

To manage the access privileges for a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Target Setup,** then select **Administrator Access.**
5. Click **Add** to grant target access privileges to a role or an administrator.

Use the Access page to set target privileges for roles and administrators. The available privileges are View, Operator, and Full.

View only allows you to view the target in the console, whereas Operator allows you to view targets, and perform all administrative actions except deleting targets. Full allows you to view targets, and perform all administrative actions.

12.5.1.3 Administering Target Blackouts

To administer the blackouts for a target, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Monitoring,** then select **Blackouts.**

Blackouts suspend data collection on a monitored target. Blackouts are useful when you want to perform scheduled maintenance tasks on monitored targets.

Use the Blackouts page to search for existing target blackouts, edit existing blackouts, define new blackouts, and stop blackouts. You can also create and stop blackouts using the BI Instance component menu, or the Essbase target menu. To create or stop a blackout, from the BI Instance component menu, or the Essbase target menu, select **Control,** then select **Create Blackout** or **End Blackout,** respectively.

12.5.1.4 Viewing Target Monitoring Configuration

To view the monitoring configuration details for a particular target, follow these steps:

1. From the **Targets** menu, select **Middleware.**

2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance or Essbase Server target. Click the BI Instance or Essbase Server name.
3. From the navigation tree in the **Target Navigation** window, click the name of the required target.
4. From the BI Instance component menu or Essbase target menu displayed on the target home page, select **Target Setup,** then select **Monitoring Configuration.**

The Monitoring Configuration page provides information about instance properties of the target, which provide internal details about target monitoring.

Table 12–12 describes the elements of the Monitoring Configuration page.

Table 12–12 Target Monitoring Configuration

Element	Description
Canonical Path	Component path of the form `instance_name/component_name`.
Oracle Instance Home	Location of the target content files, metadata, configuration files and log files.
DB Class String	String needed to form a JDBC connection with a target repository.
DB Connection String	String that specifies information about the target repository, and the means to connect to it.
DB Password	Repository database password.
DB User Name	Repository database user name.
Domain Home	Domain home directory of the WebLogic domain that the target is a part of.
Is JRF Enabled	Whether Oracle Java Required Files (JRF) is applied to the target instance or not.
Monitoring Mode	Indicates whether the Enterprise Manager instance uses a repository while monitoring the target or not. Repo indicates that a repository is used, whereas Repo-less indicates that a repository is not used.
Version	Version of the target software.

12.5.2 Performing Target-Specific Administration Tasks

This section explains how to perform target-specific BI Instance and Essbase target administration tasks, such as viewing BI Instance component failovers, and editing BI Instance monitoring credentials.

This section contains the following:

- Viewing Oracle Business Intelligence Component Failovers
- Editing Oracle Business Intelligence Monitoring Credentials

12.5.2.1 Viewing Oracle Business Intelligence Component Failovers

To view the BI Instance component failovers, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having a BI Instance target. Click the BI Instance name.
3. Select the **Availability** tab, then select **Failover.**

This page displays the risk levels of BI Instance component failure, the recommended backup actions to prevent component failures, and the backup or secondary hosts for components that have failovers configured. Administrators can use this information to plan failovers for BI Instance components that have a high risk of failure.

For more information on the recommended backup actions to avoid BI Instance component failures, refer to *Oracle Fusion Middleware System Administrator's Guide for Oracle Business Intelligence Enterprise Edition.*

12.5.2.2 Editing Oracle Business Intelligence Monitoring Credentials

To edit the BI Instance monitoring credentials, follow these steps:

1. From the **Targets** menu, select **Middleware.**
2. From the navigation tree, select the Oracle Fusion Middleware farm having an BI Instance. Click the BI Instance name.
3. From the **Business Intelligence Instance** menu, select **Target Setup,** then select **Monitoring Credentials.**
4. Edit the required fields, then click **Save.**

This page enables you to specify and edit the credentials required to connect to the database which stores scheduling and usage tracking information. Without specifying the correct credentials on this page, you cannot access certain dashboard reports. Hence, ensure that you specify the appropriate credentials on this page, before accessing the Dashboard Reports page.

Table 12–13 describes the elements of the Monitoring Credentials page.

Table 12–13 Oracle Business Intelligence Instance Monitoring Credentials

Element	Description
Database Type	Type of the database.
Hostname	Name of the host on which the database is installed.
Port	Port used for communicating with the database.
Service Name	Name of the database service.
Username	User name used for database login.
Password	Password used for database login.

Part VI

Using JVM Diagnostics

The chapters in this part provide information regarding JVM Diagnostics. The chapters are:

- Chapter 13, "Introduction to JVM Diagnostics"
- Chapter 14, "Using JVM Diagnostics"
- Chapter 15, "Troubleshooting JVM Diagnostics"

13 Introduction to JVM Diagnostics

This chapter provides an overview of JVM Diagnostics. It contains the following sections:

- Overview
- New Features in this Release
- Supported Platforms and JVMs
- User Roles

13.1 Overview

Mission critical Java applications often suffer from availability and performance problems. Developers and IT administrators spend a lot of time diagnosing the root cause of these problems. Many times, the problems occurring in production environments either cannot be reproduced or may take too long to reproduce in other environments. This can cause severe impact on the business.

Oracle Enterprise Manager Cloud Control 12c's JVM Diagnostics enables administrators to diagnose performance problems in Java application in the production environment. By eliminating the need to reproduce problems, it reduces the time required to resolve these problems. This improves application availability and performance. Using JVM Diagnostics, administrators will be able identify the root cause of performance problems in the production environment without having to reproduce them in the test or development environment. It does not require complex instrumentation or restarting of the application to get in-depth application details. Application administrators will be able to identify Java problems or Database issues that are causing application downtime without any detailed application knowledge. The key features of JVM Diagnostics are:

- Java Activity Monitoring and Diagnostics with Low Overhead
- In-depth Visibility of JVM Activity
- Real Time Transaction Tracing
- Cross-Tier Correlation with Oracle Databases
- Memory Leak Detection and Analysis
- JVM Pooling
- Real-time and Historical Diagnostics

13.1.1 Java Activity Monitoring and Diagnostics with Low Overhead

JVM Diagnostics provides in-depth monitoring of Java applications without slowing them down. It helps you to identify the slowest requests, slowest methods, requests waiting on I/O, requests using a lot of CPU cycles, and requests waiting on database calls. It also identifies the end-user requests that have been impacted by resource bottlenecks. Application resources that are causing the performance bottleneck are also visible.

13.1.2 In-depth Visibility of JVM Activity

JVM Diagnostics provides immediate visibility into the Java stack. You can monitor thread states and Java method/line numbers in real time and you can proactively identify issues rather than diagnosing issues like application crashes, memory leaks, and application hangs after they occur.

13.1.3 Real Time Transaction Tracing

If a particular request is hanging or if the entire application is slow, administrators can perform a real-time transaction trace to view current Java application activity. You can see the offending threads and their execution call stacks. You can also analyze various bottleneck resources such as how much time a thread spent in waiting for a database lock. Complex problems such as activity in one thread (or request) affecting the activity in the other thread or rest of the JVM can be found very quickly.

Sometimes the monitoring interval (default 2 seconds) that is in use is too coarse grained. The Java thread of interest may be too short lived or the amount of monitoring data collected may be insufficient. In such cases, you can run a JVM Trace to get fine-grained details of the JVM activity. This feature allows you to monitor your Java application at a very high frequency (default of once every 50ms) for a short period of time. This allows you to identify interdependency of threads, bottleneck resources (DB, I/O, CPU, Locks, Network) & top methods.

13.1.4 Cross-Tier Correlation with Oracle Databases

JVM Diagnostics facilitates tracing of Java requests to the associated database sessions and vice-versa enabling rapid resolution of problems that span different tiers. Administrators can drill down from a JVM Thread in a DB Wait State to the associated Oracle database session. Additionally, they can now drill up from the SQL query to the associated JVM and related WebLogic Server targets (this is applicable only if the database and JVM are being monitored by Enterprise Manager.

This feature highlights the slowest SQL queries and helps administrators to tune SQL and the database to improve the performance application. This facilitates smooth communication between the database administrators and application administrators by isolating the problems to the database or the application tier.

13.1.5 Memory Leak Detection and Analysis

Memory leaks lead to application slowdowns and eventually cause applications to crash. JVM Diagnostics alerts administrators on abnormalities in Java memory consumption. Administrators can use JVM Diagnostics and take heap dumps in production applications without disturbing the application. They can take multiple heap dumps over a period of time, analyze the differences between the heap dumps and identify the object causing the memory leak. Heap analysis can be performed even across different application versions. Differential Heap Analysis with multiple heap dumps makes it easy to identify memory leaks.

13.1.6 JVM Pooling

JVM Diagnostics allows administrators to group sets of JVMs together into JVM pools. This provides the console user with a single view across all related JVMs. Hence all JVM's that make up a single application or a single cluster may be grouped together in an application. This allows administrators to visualize problems naturally and intuitively.

13.1.7 Real-time and Historical Diagnostics

With JVM Diagnostics, you can perform real-time and historical diagnostics on your Java applications. This provides you with detailed insight on the root causes of production problems without having to reproduce the same problem in a Test or QA environment. You can play back transactions interactively from the browser and view the time spent in the network and the server.

Apart from the real-time data, you can also analyze historical data to diagnose problems that occurred in the past. You can view historical data that shows the time taken by end-user requests and the breakdown by Servlet, JSP, EJB, JDBC, and SQL layers.

13.2 New Features in this Release

This section lists some of the new JVM Diagnostics features in Oracle Enterprise Manager Cloud Control 12c:

- Automated JVM Diagnostics Manager and Agent Deployment Procedure.
- Customer provisioning scripts for deploying JVMD agent in production environment.
- New home pages available for JVM Pool and JVM targets.
- Top databases chart added to the JVM and JVM Pool target pages.
- Metric Palette for JVMs and JVM Pools is now available and associated with WebLogic Server targets.
- JVM Diagnostics integrated with the Middleware Diagnostics Advisor.
- Automatic correlation between JVM and WebLogic Server targets.
- JVM Diagnostics region is now included in Composite and Fusion Applications.
- JVM threshold violations are now integrated with the Event subsystem.
- Heap snapshots can be taken in HPROF format for external analysis. Heap snapshots can now be imported.
- Performance Diagnostics and Live Thread Analysis pages can be directly accessed from the JVM target page.
- Bi-directional integration between JVM threads and database sessions through Live Thread Analysis.
- Thread State Transition charts and class histograms are now available.
- RMI Thread State is now supported.
- Wait Time on SQL (DB Wait), Thread Stack Local Objects Browser, Depth and number of locks are now displayed in the Live Thread Analysis page.
- Sample analyzer can be accessed from the Thread State Transition Chart.

- Windows 64, WLS Virtual Edition, Solaris x86-64 and AIX 64 platforms are now supported.
- JVMD Manager is now supported for all OMS platforms.
- The DB Agent is not required for cross tier correlation if you are using Oracle Database 11gR2 or later versions.
- You can drill down to JVM Diagnostics from RUEI and ESS.
- Integration between JVM Diagnostics and Coherence, JVMD and ECM is now available.
- The performance of the JVMTI engine has improved.
- Integration with Enterprise Manager Offline Diagnostics feature. You can now take snapshots of diagnostic data, export this data, or import diagnostic data for a particular collection.

13.3 Supported Platforms and JVMs

The JVM Diagnostics Manager is supported on all platforms on which the Oracle Management Service has been certified.

For the latest certification information, refer to My Oracle Support Note 1415144.1. You can access My Oracle Support at the following URL:

`https://support.oracle.com/CSP/ui/flash.html`

13.4 User Roles

To use JVM Diagnostics, you must have either of the following Enterprise Manager system privileges:

- JVM Diagnostics User: Allows you to view JVM Diagnostics data.
- JVM Diagnostics Administrator: Allows you to manage JVM Diagnostics operations such as creating and analyzing heap and thread snapshots, tracing threads, and so on.

You can define these privileges in the Setup pages. For more details on defining these privileges, see the *Enterprise Manager Security* chapter in the *Administration Guide*.

14 Using JVM Diagnostics

This chapter describes the various tasks you can perform using JVM Diagnostics. In particular, it contains the following:

14.1 Installing JVM Diagnostics

The JVMD Manager runs as an Enterprise JavaBeans (EJB) Technology on a WebLogic Server. The JVMD Agent is deployed on the targeted JVM (the one running a production WebLogic Server). It collects real-time data and transmits it to the JVM Diagnostics Manager. This data is stored in the Management Repository, and the collected information is displayed on Enterprise Manager Cloud Control console for monitoring purposes. The communication between the JVMD Manager and the JVMD Agent can be a secure (SSL) or non-secure connection.

The Application Performance Management Page is a GUI based screen that enables you to deploy JVMD Manager, and monitor the health of the JVMD Manager application in a reliable and an efficient manner. Using the Application Performance Management Page, you can achieve the following:

- Deploy JVM Diagnostics Manager
- Monitor the availability of all the JVMD Managers

- Access information about the JVMD Managers like hosts to which managers are deployed, the current status, the port on which they are running, version, and so on.

For more details on installing JVM Diagnostics, see *Enterprise Manager Cloud Control Basic Installation Guide*.

14.1.1 Monitoring a Standalone JVM

If you need to monitor a standalone JVM, you can manually deploy the JVM Diagnostics Agent by following these steps:

1. From the **Setup** menu, select **Application Performance Management**. Check if the JVM Diagnostics Manager has been enabled. The JVMD Manager is independent and will run in a WLS target in the same domain as the Cloud Control OMS server that is already running. This is essentially another WLS container in the same domain and is very lightweight, so it can run well on the same server as the Cloud Control OMS instances.
2. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**. In the JVM Diagnostics Setup page, click the **JVMs and Pools** tab and then click **Downloads** to download the `jamagent.war` file.
3. Add the `jamagent.war` to the `CLASSPATH` as follows:

   ```
   CLASSPATH=$CLASSPATH:/scratch/ssmith/jvmd/jamagent.war
   ```

   ```
   export CLASSPATH
   ```

4. Start JVM Diagnostics with the JVM Diagnostics Agent as follows:

   ```
   $JAVA_HOME/bin/java -cp $CLASSPATH $JVM_OPT $SYS_OPT jamagent.jamrun
   [$JAMAGENT_PARAMS_LIST] $TARGET_CLASS $TARGET_CLASS_PARAMS
   ```

   where [`$JAMAGENT_PARAMS_LIST`] refers to the JVM Diagnostics Agent parameters. The mandatory parameters are:

   - `jamconshost` = JVM Diagnostics Manager Host
   - `jamconsport` = Listening port of JVM Diagnostics Manager
   - `oracle.ad4j.groupidprop` = [UniqueJVMPoolName]/[UniqueJVMName]

   An example is given below:

   ```
   CLASSPATH="$CLASSPATH:/scratch/ssmith/jamagent.war"
   $JAVA_HOME/bin/java -cp $CLASSPATH $JVM_OPT $SYS_OPT jamagent.jamrun
   jamconshost=10.229.187.109 jamconsport=3800
   oracle.ad4j.groupidprop= MyJVMPool1/JVM50
   ```

14.2 Setting Up JVM Diagnostics

Follow these steps to set up and configure JVM Diagnostics:

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.
2. Click the JVMD Configuration tab and enter the following details:

   - JVMD Manager Log Level: The log level for console diagnostics messages. Log levels 1 to 5 are supported where:

  - 1 = Error
  - 2 = Warning
  - 3 = Info
  - 4 = Debug
  - 5 = Trace

  The default log level is 3.

- Cross Tier Log Level: The log level for cross-tier diagnostic messages. Log levels 1 to 5 are supported where:
  - 1 = Error
  - 2 = Warning
  - 3 = Info
  - 4 = Debug
  - 5 = Trace

  The default log level is 3.

- Agent Request Timeout: The number of seconds that the JVMD Manager waits for the JVMD Agent to respond. You can increase this value if the monitored JVMs are extremely busy and the console times out and disconnects while waiting for a response.
- Agent Loop Request Timeout: The number of seconds that the JVMD Agent waits before it makes the next attempt to communicate to the JVMD Manager.
- Monitoring Aggregation Interval: The frequency at which the detailed monitoring samples should be aggregated into summary data.
- System Sample Interval: The frequency at which system details (cumulative CPU counters, heap size, and number of GCs) should be collected in monitoring.
- Purge Data Older Than: The period for which the detailed monitoring samples should be retained.
- Enable Monitoring: Select this check box to start or stop monitoring.
- Retry Changing Threads: If a thread stack changes during a sample (this can happen when a thread is using CPU), JVM Diagnostics will skip that thread for that sample. If you find missing samples, use this feature to retrace the changed stacks. This will retry (up to 5 times) threads with changing stacks. It will also make system calls to get the stack if possible.

Note: This field is not applicable to the JVMTI (level 0) optimization.

3. Click **Save** to save the parameters.

14.2.1 Viewing Registered JVMs and Managers

Follow these steps to view a list of registered JVMs and JVM Managers:

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.

2. The following tables are displayed:

   - Registered Managers: The following details are displayed:
     - Manager ID: The unique ID assigned to the JVM Manager. This ID identifies the JVM Manager in all the processes.
     - Host: The machine on which the JVM Manager has been deployed.
     - Port: The port of the machine on which the JVM Manager has been deployed.
     - SSL Port: The SSL Port of the machine on which the JVM Manager has been deployed.
     - Build Version: The build version of this JVM Manager.Status: The status of the JVM Manager (Active/Inactive)
   - Registered JVMs: The following details are displayed:
     - Manager ID: The ID of the Manager to which this JVM is connected.
     - JVM ID: This is a unique ID given to the Agent and is used to identify the Agent in all the processes.
     - Pool: The JVM Pool with which the JVM is associated.
     - Host: The Host on which the JVM is running.
     - JVM Name: The name given to the JVM for identification. The basic format of the JVM Name is `<HOST>_<PORT>_jvm` or `<EMFarm>/<Domain>/<Server>_jvm`.
     - CPUs: The number of CPUs.
     - ID: The port on which the JVM is running. (Default: 5555)
     - Heap Size (Kb): The total Heap Size used.
     - Heap Dump Dir: The location of the directory in which the heap snapshots are temporarily stored.
     - Log Level: The log level of the JVM.
     - Status: The status of the JVM (active or inactive).

     Check the **Select** check box and click the **Edit** icon to edit the JVM. In the Edit JVM Information page, you can select a different JVM Pool, modify the JVM Name, Heap Dump Dir, and Log Level. Click **Save** to save the changes or **Reset** to restore the previous values.
   - Registered DB Agents: The following details are displayed:
     - Manager ID: The ID of the Manager to which this DB Agent is connected.
     - DB ID: This is a unique ID given to the DB Agent and is used to identify the DB Agent in all the processes.
     - Host: The host on which the DB Agent is running.
     - CPUs: The number of CPUs.
     - OS User: The user who started the DB Agent.
     - ID: The port on which the DB Agent is running (Default is 5555).
     - Log Level: The log level of the DB Agent.
     - Status: The status of the DB Agent (active or inactive)

Check the **Select** check box and click the **Edit** icon to edit the DB Agent.

14.2.2 Configuring JVM Pools

You can group sets of JVMs into JVM pools that provide monitoring information across all related JVMs in a single view. You can view all the JVM pools in the WebLogic Domain, create a new JVM pool, and edit existing JVM pools.

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.
2. Click the **JVMs and Pools** tab. The list of all available JVM pools is displayed. For each pool, you can view the polling interval, whether polling is enabled, and the e-mail notification recipient. If the **Polling Enabled** flag is set to **Y**, JVMs belonging to this pool will be polled for active requests periodically based on the Poll Interval.
3. Click **Create Pool** to create a new pool.
   a. In the Add JVM Pool Information page, enter the name and description of the JVM pool.
   b. In the **Poll Interval** field, specify the sample interval for JVMs belonging to this pool when monitoring (polling) is enabled.
   c. Check the **Poll Enabled** check box to poll the JVMs belonging to this pool.
   d. Click **Save** to save the JVM Pool information.
4. To delete a pool, check the select check box and click the **Delete** icon. You cannot delete the **Default** and **Other** pools.
5. Click the **Edit** icon to edit an existing JVM pool.
   a. Modify the JVM pool details and click **Save** to save the changes.
   b. To modify the pool thresholds, click **Set Thresholds**. See Section 14.2.2.1, "Updating Pool Thresholds" for details.

14.2.2.1 Updating Pool Thresholds

Follow these steps to edit the pool thresholds:

1. From the **Setup** menu, select **Application Performance Management** and click **Setup JVM Diagnostics** in the Application Performance Management page.
2. Click the **Pools** tab to view the Show JVM Pools page.
3. Click the **Edit** icon of the JVM pool you want to edit.
4. In the Edit JVM Pool Information page, click **Set Thresholds**.
5. In the Edit Thresholds for JVM Pool page, the following details are displayed:
   - Level: Thresholds violations can have a level of R (red) or Y (yellow).
   - Metric: The attribute or metric that is being monitored.
   - Threshold: The value against which the metric is being compared. A violation occurs when the threshold is exceeded after a minimum number of samples have been monitored.
   - Action URL: The URL to be invoked when a threshold violation occurs. This includes internal URLs into the JVMD Console and external URLs. The Action URL can be used to trace a particular thread, all active threads, or dump a

heap in response to a threshold violation. The Action URL can be any valid URL on a remote system. It can also accept URLs on the local JVMD Console. The Action URL should be a valid URL as called from a browser. If not specified, default parameters for the `traceThread` and `heapdump` will be added to the URL.

6. Click **Save** to save the threshold values.

14.2.3 Setting the Monitoring Status

After the JVM pools have set up and configured correctly, you must enable monitoring so that the JVMs in the pool can be monitored. Follow these steps to enable monitoring for a JVM pool:

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.
2. Click the **Monitoring** tab to view the monitoring status of the JVM pools.
3. Click the **Edit** icon to enable or disable monitoring of pools or change their polling intervals by updating the pool properties.
4. You can mark a thread as idle by adding it to an Idle Thread Rule. All threads that have been marked as idle will not be monitored. Click **New Rule** to create a new Idle Thread Rule.
   - **Rule Type**: The Rule Type can be:
     - **Monitor (Waiting on Lock)**: Select this type if you want to ignore threads that are locked with a lock of the specified nameCurrent Call: Select this type if you want to ignore all threads that are making a call to the selected function.
   - **Rule Value**: The Rule Value should contain the class name, method, followed by class+method. An example of a Current Call is `weblogic.socket.PosixSocketMuxer->processSockets`. An example of a Monitor (Waiting on Lock) is `weblogic.socket.PosiSocketMuxer$1`.

   All threads that meet the criteria specified in the Idle Thread Rule will not appear in the View Active Threads screen.

14.2.4 Downloading the JVM Diagnostics Components

You can manually download the various binaries such as JVM Diagnostics Agent, JVM Diagnostics Manager, Database Agent, Load Heap, and deploy them.

Follow these steps to download the binaries:

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.
2. Click the **Downloads** tab. The list of JVM Diagnostics components that can be downloaded is displayed.
3. Click on the download icon for the component to be downloaded. You can download:
   - **JVM Diagnostics Agent WAR File**: The JVM Diagnostics Agent Parameters web.xml Parameters window is displayed. From the Available Managers drop-down, you can select entries that are in the format `<host>:<port>` - for

normal communication, `<host>:<port>(secure communication)` for communication over the SSL Port or you can select `Other`. If you select `Other`, you need to specify the Manager IP Address and the Manager Port to which the JVM Diagnostics Agent is connecting to. While downloading the Agent, you can modify the following parameters:

  - Tuning Timeouts Parameters: You can modify the Connection Retry Time, GC Wait Timeout, Long Request Timeout, and Idle Agent Timeout.
  - Target Association Parameters: If you select **WebLogic Server**, you can specify the Target Name, and Pool Name. If you select **Other Server**, you can specify the Group ID Property and Pool Name.
  - Logging Parameters: You can modify the Agent Log Level.
  - Optimization Level: You can modify the Optimization Level.

- **JVM Diagnostics Manager EAR File**: You can open the `jammanager.ear` file or save it to a specified location.
- **Load Heap**: The `loadheap.zip` is saved to a specified location.

14.2.5 Registering the Database Target

Follow these steps to register the database:

1. From the **Setup** menu, select **Application Performance Management**. Select the JVM Diagnostics Engine row in the Application Performance Management Engines table and click **Configure**.
2. Click the **Register Databases** tab.
3. The list of registered databases is displayed. The database name, host, Oracle SID for the monitored database, and listener port number is displayed. You will also see a flag indicating whether the database agent is required.
4. You can do the following:
   - **Add a Database Instance**: From the Add menu, select **Database Instance** to register an Enterprise Manager database target.
   - **Add a Custom Database**: From the Add menu, select **Custom Database** to register an external database target. Specify the Name, Host, Port, SID, Instance ID, Username, and Password and click **Test Connection** to validate the database details. After the validation, click **OK** to register the database.
   - **Remove**: Select a database from list and click **Remove** to remove a registered database.
   - **Edit**: You cannot edit a Database Instance. Only custom databases can be edited. Select a custom database from the list and click **Edit**.

Note:

- The OS User you specify here must be the same OS User running the database agent. This user must have full database privileges and appropriate environment settings using the SID and path binaries.
- The DB User must the same as the user running the application is being monitored.
- Multiple registrations may be necessary for a single database agent if different database users are running multiple applications.
- For Oracle RAC databases, each node must be registered.

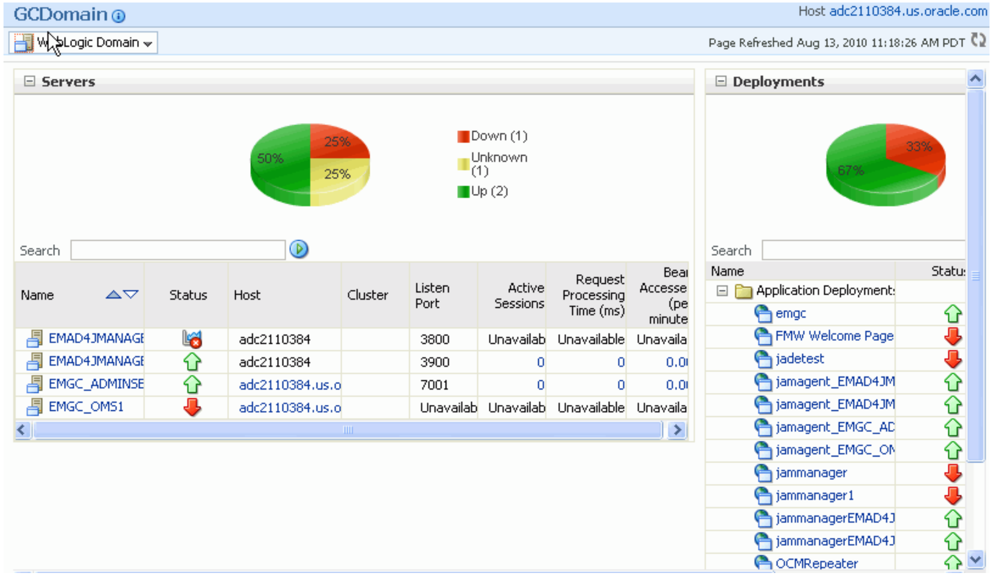
---

5. After the database has been registered, the JVM Diagnostics Manager will start monitoring the cross-tier JVM calls between applications being monitored for a particular JVM and the underlying database.

14.3 Accessing the JVM Diagnostics Pages

After you have deployed the JVM Diagnostics Manager and configured JVM Diagnostics, you can start using the features. Navigate to the **Middleware** tab in Enterprise Manager and click on a JVM Pool, Java Virtual Machine, WebLogic Server, WebLogic Domain or Cluster target. The Home page for the target is displayed.

Figure 14–1 JVM Pool Home Page



Name	Status	Host	Cluster	Listen Port	Active Sessions	Request Processing Time (ms)	Bea Accesse (pe minute
EMAD4JMANAGE	✕	adc2110384		3800	Unavailab	Unavailable	Unavaila
EMAD4JMANAGE	↑	adc2110384		3900	0	0	0.0
EMGC_ADMINSE	↑	adc2110384.us.o		7001	0	0	0.0
EMGC_OMS1	↓	adc2110384.us.o		Unavailab	Unavailab	Unavailable	Unavaila

Name	Statu
Application Deployment:	
emgc	↑
FMW Welcome Page	↓
jadetest	↓
jamagent_EMAD4JM	↑
jamagent_EMAD4JM	↑
jamagent_EMGC_AD	↑
jamagent_EMGC_OM	↑
jammanager	↓
jammanager1	↓
jammanagerEMAD4J	↑
jammanagerEMAD4J	↑
OCMRepeater	↑

To start using JVM Diagnostics, select the JVM Diagnostics option from the JVM Pool drop-down menu and choose the appropriate option.

14.4 Managing JVM Pools

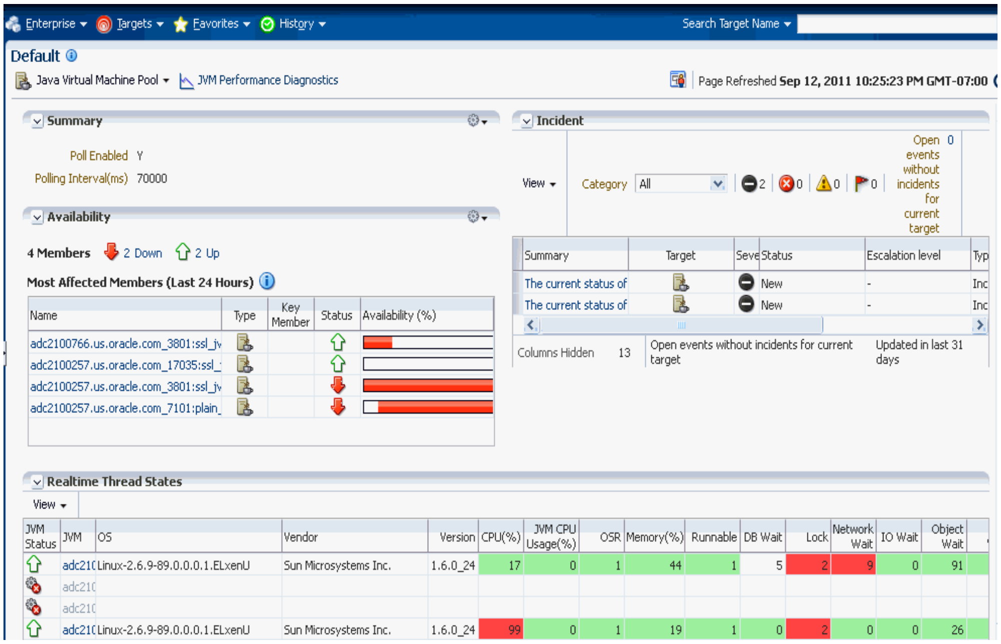
You can group sets of JVMs into JVM pools that provide monitoring information across all related JVMs in a single view. You can monitor all the JVMs in a pool, view historical and real time data for the JVM pool, manage threads and heap snapshots, create a new pool, and edit an existing JVM pool. JVMs and JVM Pools are now targets in Enterprise Manager. You can do the following:

- View the JVM Pool Home Page
- View JVM Pool Performance Diagnostics
- View the JVM Pool Live Thread Analysis
- Manage Thread Snapshots
- Manage Heap Snapshots
- Setup JVM Diagnostics

14.4.1 Viewing the JVM Pool Home Page

The JVM Pool Home page shows the details of all JVMs in the pool.

Figure 14–2 JVM Pool Home Page



Page Refreshed **Sep 12, 2011 10:25:23 PM GMT-07:00**

Poll Enabled Y

Polling Interval(ms) 70000

4 Members 2 Down 2 Up

Most Affected Members (Last 24 Hours)

Name	Type	Key Member	Status	Availability (%)
adc2100766.us.oracle.com_3801:ssl_jv			⇧	
adc2100257.us.oracle.com_17035:ssl_			⇧	
adc2100257.us.oracle.com_3801:ssl_jv			⬇	
adc2100257.us.oracle.com_7101:plain_			⬇	

Category All ⊖2 ⊗0 ⚠0 ⚑0 Open events without incidents for current target 0

Summary	Target	Seve	Status	Escalation level	Typ
The current status of		⊖	New	-	Inc
The current status of		⊖	New	-	Inc

Columns Hidden 13 Open events without incidents for current target Updated in last 31 days

JVM Status	JVM	OS	Vendor	Version	CPU(%)	JVM CPU Usage(%)	OSR	Memory(%)	Runnable	DB Wait	Lock	Network Wait	IO Wait	Object Wait
⇧	adc21(	Linux-2.6.9-89.0.0.0.1.ELxenU	Sun Microsystems Inc.	1.6.0_24	17	0	1	44	1	5	2	9	0	91
	adc21(													
	adc21(													
⇧	adc21(	Linux-2.6.9-89.0.0.0.1.ELxenU	Sun Microsystems Inc.	1.6.0_24	99	0	1	19	1	0	2	0	0	26

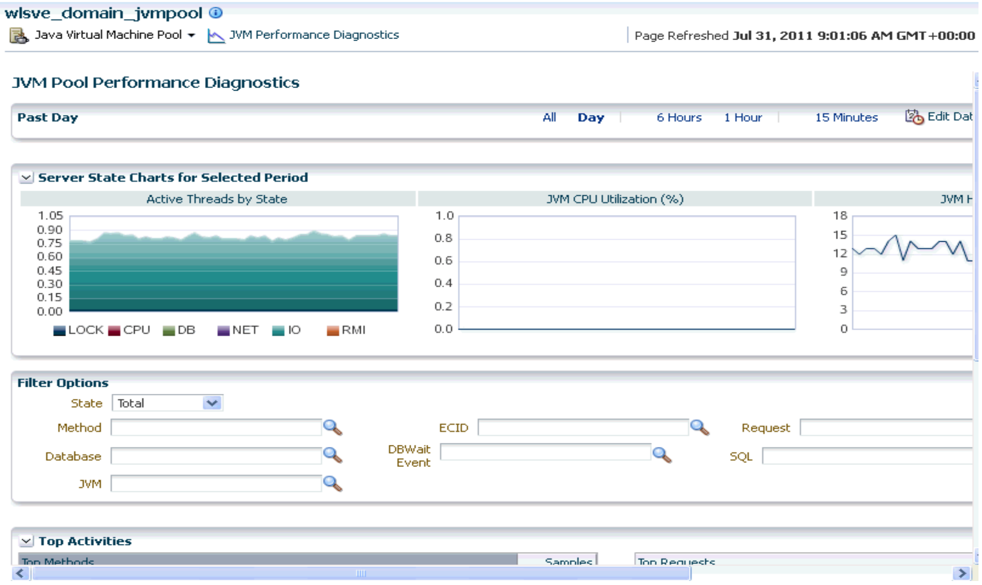
It shows the following details:

- Summary: Shows whether poll is enabled and the Polling Interval.
- Availability: This region shows the availability status of the members in the JVM Pool. Click on a Member link to drill down JVM Home Page.
- Incident: This region shows any open incidents that have occurred, the type, and category of the incident. Click the Summary link to drill down to the Incident Details page.
- Realtime Thread States: This region shows the realtime thread status for each JVM in the pool. The current activity of the JVM including CPU usage, memory, number of threads waiting for a database response, number of threads waiting for synchronization lock, and other details are displayed. Click on the JVM link to drill down to the JVM Performance Diagnostics page.

14.4.2 Viewing the JVM Pool Performance Diagnostics Page

You can view the summary and detailed information of the selected JVM Pool on this page. You can also compare the JVM pool data across two specific time periods. To view this page, select **Middleware** from the **Targets** menu and click on a JVM Pool target. Select the **JVM Performance Diagnostics** option from the **Java Virtual Machine Pool** menu.

Figure 14–3 JVM Pool Performance Diagnostics Page

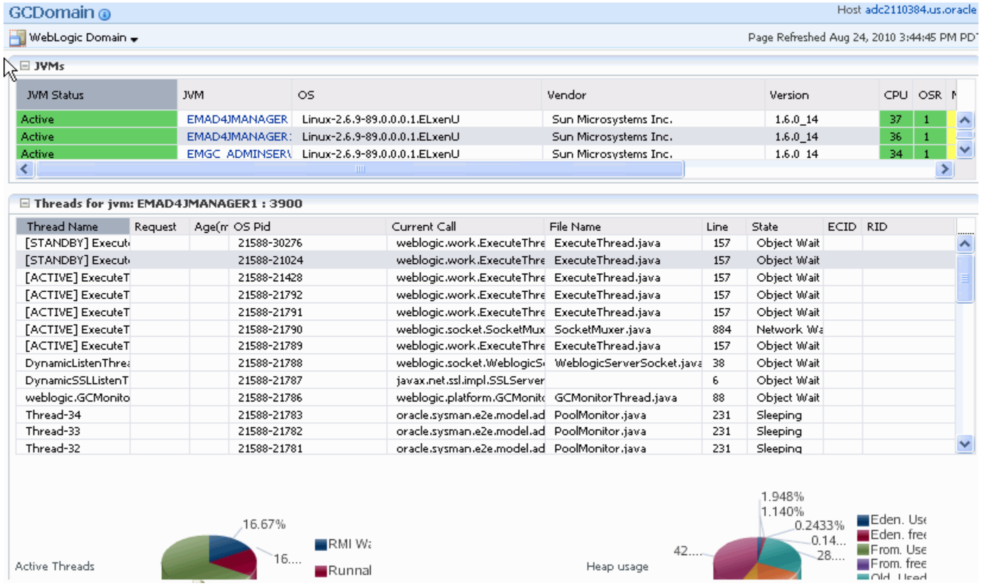


This page shows the summary details of the JVM pools which include the Server State Charts, and a list of Top Methods and Top Requests. You can view the Server State Charts, list of Top Methods, Top Requests, Top DBStates, and Top SQLs. You can filter the data that is displayed by specifying various criteria such as Method Name, JVM Name, Thread State, DBState, and so on. The list of all JVMs in the pool and the server state charts for each JVM is displayed. Click the link to drill down to the Java Virtual Machine Home page.

14.4.3 Viewing the JVM Pool Live Thread Analysis Page

This page shows the real-time data for all the JVMs in the selected pool. This data is useful in analyzing the various active and idle threads on the JVM. During analysis you can drill down from the thread level to methods used in the thread to local variables that are part of the method. From the **Targets** menu, select **Middleware**, and then click on a Java Virtual Machine Pool target. Select the **Live Thread Analysis** option from the **Java Virtual Machine Pool** menu. The JVM Pool Live Thread Analysis Page appears.

Figure 14–4 JVM Pool Live Thread Analysis Page



GCDomain

Host adc2110384.us.oracle

WebLogic Domain

Page Refreshed Aug 24, 2010 3:44:45 PM PD

JVMs

JVM Status	JVM	OS	Vendor	Version	CPU	OSR
Active	EMAD4JMANAGER	Linux-2.6.9-89.0.0.0.1.ELxenU	Sun Microsystems Inc.	1.6.0_14	37	1
Active	EMAD4JMANAGER:	Linux-2.6.9-89.0.0.0.1.ELxenU	Sun Microsystems Inc.	1.6.0_14	36	1
Active	EMGC_ADMINSER\	Linux-2.6.9-89.0.0.0.1.ELxenU	Sun Microsystems Inc.	1.6.0_14	34	1

Threads for jvm: EMAD4JMANAGER1 : 3900

Thread Name	Request	Age(r	OS Pid	Current Call	File Name	Line	State	ECID	RID
[STANDBY] Execut			21588-30276	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
[STANDBY] Execut			21588-21024	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
[ACTIVE] ExecuteT			21588-21428	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
[ACTIVE] ExecuteT			21588-21792	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
[ACTIVE] ExecuteT			21588-21791	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
[ACTIVE] ExecuteT			21588-21790	weblogic.socket.SocketMux	SocketMuxer.java	884	Network Wa		
[ACTIVE] ExecuteT			21588-21789	weblogic.work.ExecuteThre	ExecuteThread.java	157	Object Wait		
DynamicListenThre			21588-21788	weblogic.socket.WeblogicS	WeblogicServerSocket.java	38	Object Wait		
DynamicSSLListenT			21588-21787	javax.net.ssl.impl.SSLServer		6	Object Wait		
weblogic.GCMonito			21588-21786	weblogic.platform.GCMonit	GCMonitorThread.java	88	Object Wait		
Thread-34			21588-21783	oracle.sysman.e2e.model.ad	PoolMonitor.java	231	Sleeping		
Thread-33			21588-21782	oracle.sysman.e2e.model.ad	PoolMonitor.java	231	Sleeping		
Thread-32			21588-21781	oracle.sysman.e2e.model.ad	PoolMonitor.java	231	Sleeping		

This page shows the following:

- JVMs: This table shows the list of JVMs and the current status of each JVM. The current activity of the JVM including CPU usage, memory, number of threads waiting for a database response, number of threads waiting for synchronization lock, and other details are displayed
- **Threads for JVM:** This table shows a list of all the threads running in the JVM. For each thread, the Thread Name, Request, Age, OS PID, Current Call, File Name, Line, State, Waiting On, Wait Time, Lock Held, ECID. If the thread is in the DB Wait State, click on the link to drill down to the Database Home page. See Section 14.5.4.1, "Cross Tier Analysis" for more details.

  If the ADP Agent is running, the Request Name and Request Age are displayed. If a thread is in the **DB Wait State**, the Waiting On column displays the name of the database the thread is waiting on, and the time the thread has to wait is displayed in the Wait Time column.

You can also see two charts, the first one displays the active threads in the JVM, the second one displays the heap status for the JVM.

14.5 Managing JVMs

You can monitor a specific JVM in a pool, view historical and real time data, and so on. You can do the following:

- View the JVM Home Page
- View JVM Performance Diagnostics
- View JVM Performance Summary
- View the Live Thread Analysis Page
- View the Live Heap Analysis Page
- Manage Thread Snapshots
- Manage Heap Snapshots

- Setup JVM Properties

14.5.1 Viewing the JVM Home Page

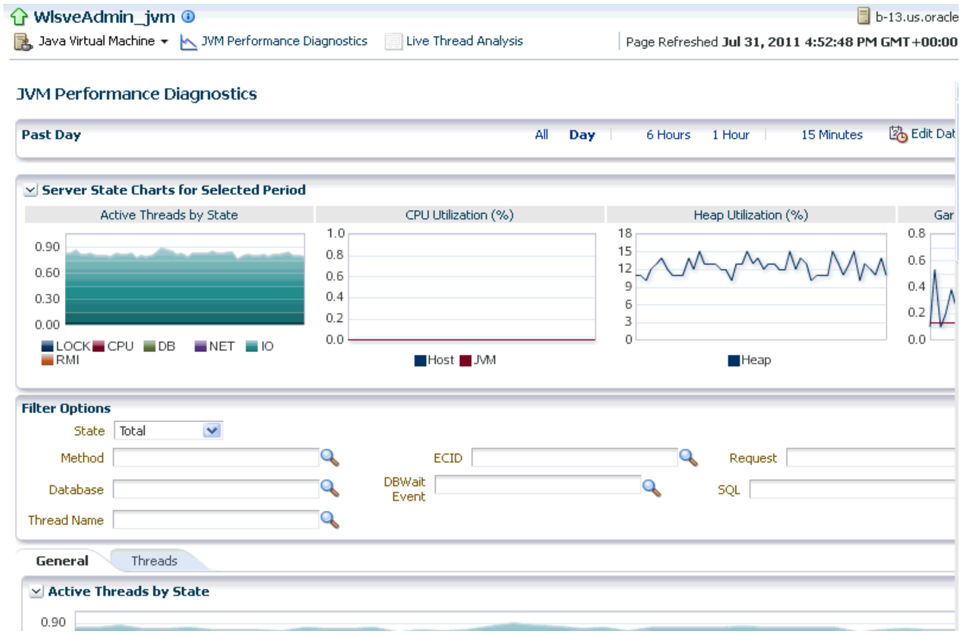
The JVM Home page shows the summary and configuration information of all the JVMs in the JVM pool. Follow these steps to view the JVM Home page:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine target.
2. The JVM Home page with the following details is displayed.
   - Summary: Shows details of the JVM such as the JVM Pool it belongs to, the host, Agent Optimization Level, Agent Log Level, JVM Version, and vendor details.
   - Incident: Shows the thresholds and alerts if any for this JVM.
   - Availability: The availability status of the JVM.
   - Active Threads: The number of active threads in the JVM in the last 24 hours.
   - Realtime Thread States: Shows the state of the various threads in the JVM in the color coded columns. Click on a JVM to view the list of threads in the JVM and the details of each thread.

14.5.2 Viewing the JVM Performance Diagnostics Page

This page shows the summary and detailed information for a specific JVM. To view this page, select **Middleware** from the **Targets** menu and click on a Java Virtual Machine target. Select the **JVM Performance Diagnostics** option from the **Java Virtual Machine** menu.

Figure 14–5 JVM Performance Diagnostics Page



WlsveAdmin_jvm

b-13.us.oracle

Page Refreshed Jul 31, 2011 4:52:48 PM GMT+00:00

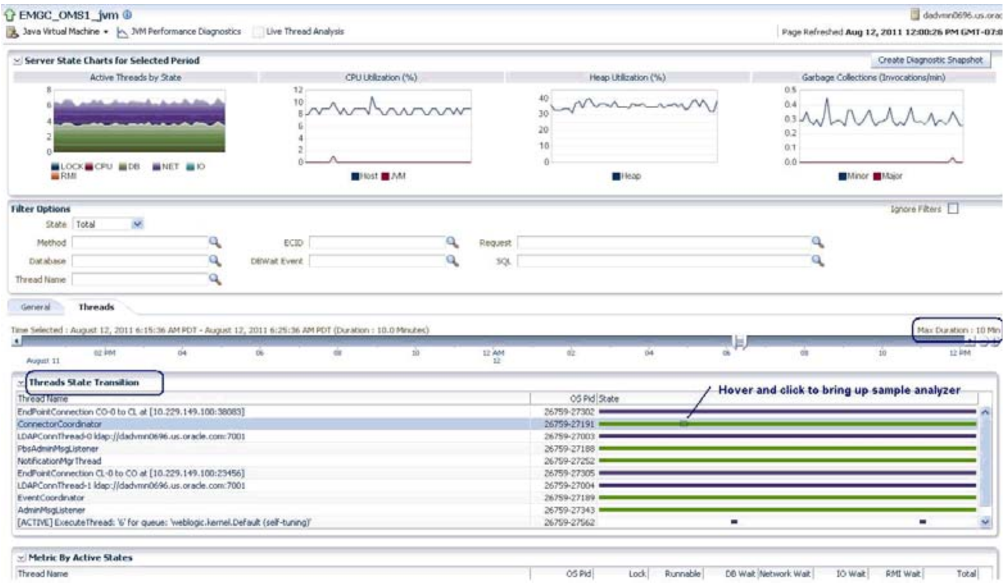
State: Total

This page shows the summary details of the JVM which include the Server State Charts, Active Threads by State, Top Methods, Top Requests, Top DBWait Events, Top

SQLs, and Top Databases. You can filter the data that is displayed by specifying various criteria such as Method Name, JVM Name, Thread State, DBState, and so on.

Click on the **Threads** tab to view the Thread State Transition chart. This chart shows how the threads have transitioned from one state to the other in the selected period.You can change the time interval and move it to a different time period by using the quick time selection control at the top of the page. You can hover over the colored bars to see the transition changes from one state to the other, for example from **Runnable** to **Not Active** or to **Runnable**.

Figure 14–6 Thread State Transition



Ignore Filters □

State: Total

Time Selected : August 12, 2011 6:15:36 AM PDT - August 12, 2011 6:25:36 AM PDT (Duration : 10.0 Minutes)

Thread Name	OS Pid	State
EndPointConnection CO-0 to CL at [10.229.149.100:38083]	26759-27302	
ConnectorCoordinator	26759-27191	
LDAPConnThread-0 ldap://dadvmn0696.us.oracle.com:7001	26759-27003	
PbsAdminMsgListener	26759-27188	
NotificationMgr Thread	26759-27252	
EndPointConnection CL-0 to CO at [10.229.149.100:23456]	26759-27305	
LDAPConnThread-1 ldap://dadvmn0696.us.oracle.com:7001	26759-27004	
EventCoordinator	26759-27189	
AdminMsgListener	26759-27343	
[ACTIVE] ExecuteThread: '6' for queue: 'weblogic.kernel.Default (self-tuning)'	26759-27562	

Thread Name	OS Pid	Lock	Runnable	DB Wait	Network Wait	IO Wait	RMI Wait	Total

Click on a bar graph in the **State** column to view a detailed analysis on the state of the thread. This feature allows you to analyze each sample (JVM snapshot at a specific time) in the monitored data.

Click the Create Diagnostics Snapshot link to collect diagnostic data for the JVM target for a specific period and analyze this data in an offline mode. For more details, see Section 14.12, "JVM Offline Diagnostics"

14.5.3 Viewing the JVM Diagnostics Performance Summary

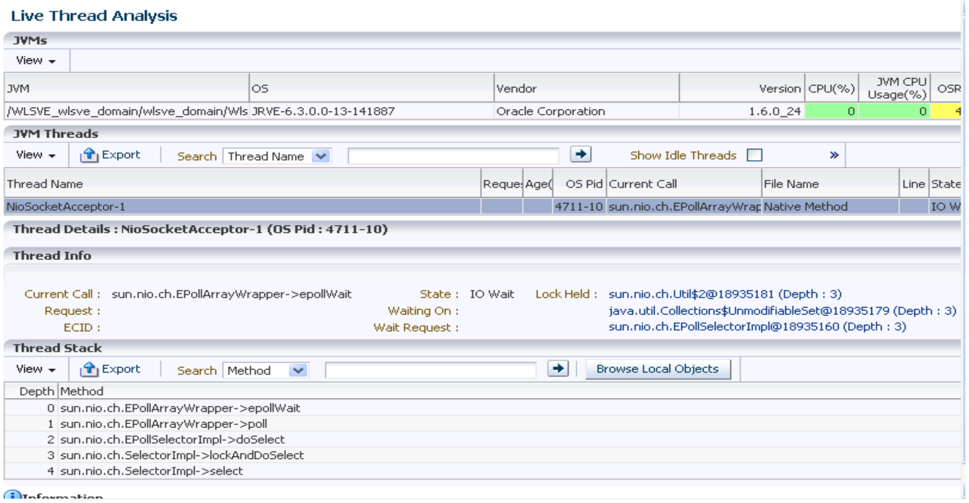
You can view the performance metrics (system and active threads) for a JVM target on the Performance Summary page. A set of charts are displayed on this page for the JVM target. To view the JVM performance metrics, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine target.
2. Select the **Performance Summary** option from the **Java Virtual Machine** menu.
3. A set of default charts that show the values of the JVM performance metrics over a period of time are displayed. Click the **Show Metric Palette** button.
4. The metric palette has a folder for the current target (JVM) and the related targets. You can add or remove metric charts. Leaf nodes act as check boxes. Clicking a leaf node on causes a chart to be added. Clicking it off removes the metric. Dragging a leaf node from the palette to a chart or legend adds the metric to that chart.

14.5.4 Viewing the JVM Live Time Thread Analysis Page

This page shows the real-time data for a selected JVM. This data is useful in analyzing the various active and idle threads on the JVM. During analysis you can drill down from the thread level to methods used in the thread to local variables that are part of the method. To view this page, select **Middleware** from the **Targets** menu and click on a Java Virtual Machine target. Select the **Live Thread Analysis** option from the **Java Virtual Machine** menu.

Figure 14–7 JVM Live Thread Analysis Page



JVM	OS	Vendor	Version	CPU(%)	JVM CPU Usage(%)	OSR
/WLSVE_wlsve_domain/wlsve_domain/Wls	JRVE-6.3.0.0-13-141887	Oracle Corporation	1.6.0_24	0	0	4

Thread Name	Reque:	Age(	OS Pid	Current Call	File Name	Line	State
NioSocketAcceptor-1			4711-10	sun.nio.ch.EPollArrayWrap	Native Method		IO W

Current Call : sun.nio.ch.EPollArrayWrapper->epollWait
Request :
ECID :

State : IO Wait
Waiting On :
Wait Request :

Lock Held : sun.nio.ch.Util$2@18935181 (Depth : 3)
java.util.Collections$UnmodifiableSet@18935179 (Depth : 3)
sun.nio.ch.EPollSelectorImpl@18935160 (Depth : 3)

Depth	Method
0	sun.nio.ch.EPollArrayWrapper->epollWait
1	sun.nio.ch.EPollArrayWrapper->poll
2	sun.nio.ch.EPollSelectorImpl->doSelect
3	sun.nio.ch.SelectorImpl->lockAndDoSelect
4	sun.nio.ch.SelectorImpl->select

This page shows the following:

- **JVM Threads**: This table shows a list of all the threads running in the JVM. Click on a thread to view the thread details in the Thread Info table. For each thread, the Thread Name, Request, Age, OS PID, Current Call, File Name, Line, State, Waiting On, Wait Time, Lock Held, ECID.

  If the ADP Agent is running, the Request Name and Request Age is displayed. If a thread is in the **DB Wait State**, the Waiting On column displays the name of the database the thread is waiting on, and the time the thread has to wait is displayed in the Wait Time column.

  You can perform the following actions:

  – **Take Snapshot of a Selected Thread or Active Threads**: Select a thread from the list and choose the **Take Snapshot of a Selected Thread** option from the Actions menu. The Thread Snapshot page is displayed where you take a snapshot. If you select the **Take Snapshot of Active Threads** option, you can take a snapshot of all active threads running on this JVM. You can specify the following parameters for each snapshot:

  * Poll Interval: Interval after which snapshot should be repeated.

  * Poll Duration: Duration for which the snapshot should be taken.

  * Thread Details: You can specify if the thread details need be included in the snapshot.

  * Try Changing Threads: Sometimes the stack associated with the thread may change rapidly which makes taking the snapshot difficult. If you select this parameter, you can suspend the thread and take the snapshot.

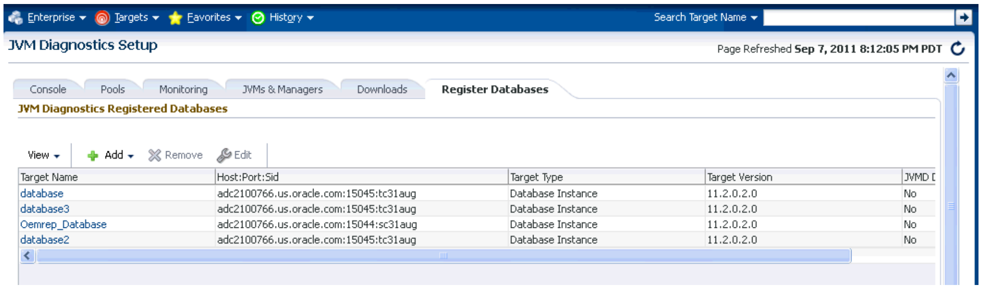
        - Include Network Waits: Specify if network wait threads need to be included in the snapshot.
        - All Threads: Specify if all threads (active and idle) must be included in the snapshot.
        - Allow Trace Interrupt: Indicate whether the trace process can be interrupted.
    - **Mark Idle**: Select a thread from the list and click **Actions > Mark Idle** to mark a thread as idle.
    - **Mark Active**: If you selected the Show Idle Threads check box, a list of idle threads is displayed. Select a thread and click **Actions > Mark Active** to mark it as an active thread.
    - **Show Idle Threads**: Select this check box to list only the idle threads in the JVM Threads table.
    - **Export**: Click **Export** to export the thread details to an Excel file.
- **Thread Info**: This section shows the detailed information for a selected thread. Details of thread including Current Call, Request, ECID, State, Waiting On, and Wait Request are displayed. If the thread is in the DB Wait State, click on the link to drill down to the Database Home page. See Section 14.5.4.1, "Cross Tier Analysis" for more details.
- **Thread Stack**: The Thread Stack table shows the details of the selected thread such as the depth of the thread, methods used in the thread, file where the method is used, and the line number. You can drill down from the method level to a lower level. Select a method from the table and click Browse Local Objects. A popup window is displayed which shows the local variables, objects, their classes, and values. You can export these details to a file by clicking Export. You are prompted to specify the directory in which the file is to be stored. Enter the path and click Save to save file in .csv format.

14.5.4.1 Cross Tier Analysis

You can trace any JVM activity from the JVM thread to the database. You can view cross tier correlation for live threads and historical monitored data.

Before you establish cross tier correlation, ensure that the database is an Enterprise Manager target and has been registered with JVM Diagnostics. To register the database, select the **Application Performance Management** option from the **Setup** menu, then click **Setup JVM Diagnostics** in the Application Performance Management page. Click on the **Register Databases** tab. The list of registered database targets is displayed.

Figure 14–8 JVM Diagnostics Setup



JVM Diagnostics Setup

Page Refreshed **Sep 7, 2011 8:12:05 PM PDT**

JVM Diagnostics Registered Databases

Target Name	Host:Port:Sid	Target Type	Target Version	JVMD
database	adc2100766.us.oracle.com:15045:tc31aug	Database Instance	11.2.0.2.0	No
database3	adc2100766.us.oracle.com:15045:tc31aug	Database Instance	11.2.0.2.0	No
Oemrep_Database	adc2100766.us.oracle.com:15044:sc31aug	Database Instance	11.2.0.2.0	No
database2	adc2100766.us.oracle.com:15045:tc31aug	Database Instance	11.2.0.2.0	No

If the JVMD Agent Required field has a **No** value, you can proceed with the cross tier analysis. If the field has a **Yes** value, you must ensure that the root user or the same OS user who started the database must be running the JVM Diagnostics Database Agent on the target database machine. If the JVMD Agent Required field has a **Status Unavailable** value, you cannot perform cross tier analysis as the JDBC connection to the database cannot be established.

To view the cross tier correlation for live threads, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine target. Select the **Live Thread Analysis** option from the **Java Virtual Machine** menu. See Figure 14–4.
2. In the JVM Threads column, select a thread with a DB Wait State.
3. The thread details are displayed in the Thread Info section. If cross tier correlation has been established, you can see `SID=<value>"SERIALNUM=<value>` when you hover over the State field. Click the **DB Wait** link.
4. The Database Details popup is displayed which shows the host, port, SID, user, and JDBC URL for the target database. Click the **Register All DB Targets** link to register all database targets with JVM Diagnostics and refresh the Live Thread Analysis page.

   Oracle Database 11*g* Release 2 supports special cross tier requirements for JVM Diagnostics and cross tier correlation is automatically established when you click the **Register All DB Targets** link. If you are using an earlier Oracle Database version, the registration process prompts you to run the JVM Diagnostics Agent on the host machine.
5. Click **View Register Databases** to navigate to the Registered Databases page where you can manually register the database target with JVM Diagnostics and check the value in the DB Agent Required column. Click **Add**, to add a database instance or a custom database. If you register a database as a custom database, the DB Name is displayed in the Waiting field in the Threads Info section but the cross tier correlation cannot be established.

To view the cross tier correlation for historical monitored data, follow these steps:

1. From the Targets menu, select **Middleware**, then click on a Java Virtual Machine target. Select the **JVM Performance Diagnostics** option from the **Java Virtual Machine** menu.
2. The three tables Top Databases, Top SQLS, and Top DBWait Events related to the cross tier are displayed. The Top Databases table shows the top databases in which JVM or JVMs in the pool have activities. The Top DBWait Events table shows the top DB Wait events caused by the JVM threads in the database. The Top SQLs table shows the top SQLs executed by the JVM threads in the database. Click the top field of a table to launch a popup which shows the names of the database on which activity was performed.
3. Click the Database Name link to drill down to the Database Diagnostics page which shows the corresponding database activity.
4. Click the Top SQLs and Top DBWait Events links to navigate to the SQL Details page and the ASH Viewer page of database diagnostics.

If cross tier correlation has been established, you can view JVM Diagnostics activities for a database (drilling up from Database Diagnostics to JVM Diagnostics). Click the JVM Diagnostics link in the Performance page to drill up to the JVM Performance Diagnostics page. Data relevant to the time interval, database and other filters is displayed.

14.5.4.2 JVM Diagnostics - Oracle Real Application Cluster Drill-Down

Oracle Real Application Cluster (Oracle RAC) databases have a complex configuration of database instances and listeners. User applications use Oracle RAC services to connect to the database instead of SIDs that are used for single instance databases. User applications connect to Oracle RAC listeners that are listening on different machines than the actual database instances. In JVM Diagnostics, cross tier correlation is established automatically for Oracle RAC databases.

Cross tier correlation cannot be established if the listener is not registered in Enterprise Manager. In this scenario, you can establish cross tier correlation by using either of the following options:

- If you know the database instance that which your application is being connected, add the details of the listener as a property for any database instance in that Oracle RAC. Before you add the listener, you must ensure that it is registered in JVM Diagnostics. For example, to add the `jvmd_db_listeners_additional_info` property to the database instance, follow these steps:

  -
    ```
    Insert into mgmt_target_properties (TARGET_GUID, PROPERTY_NAME,
    PROPERTY_VALUE) values ((select target_guid from mgmt_targets where
    target_name='<DB Instance Name>'), jvmd_db_listeners_additional_
    info','LISTENER_
    adc2110865.us.oracle.com:adc2110865-v.us.oracle.com:10.232.132.249:
    1521')
    ```
  - Remove the database instance target (`DB_INSTANCE_NAME`) that was specified in the query.
  - Ensure that there are no custom databases registered for any of the database target instances which are in Oracle RAC.
- Register a custom database with the same name and SID as the Database Instance. The host, port and service must be the same as the one used in the connect string.

14.5.5 Viewing the JVM Live Heap Analysis Page

This page shows the real time organization of all objects in the JVM Heap. To view this page, select **Middleware** from the **Targets** menu and click on a JVM Pool target. Select the **Live Heap Analysis** option from the **Java Virtual Machine** menu.

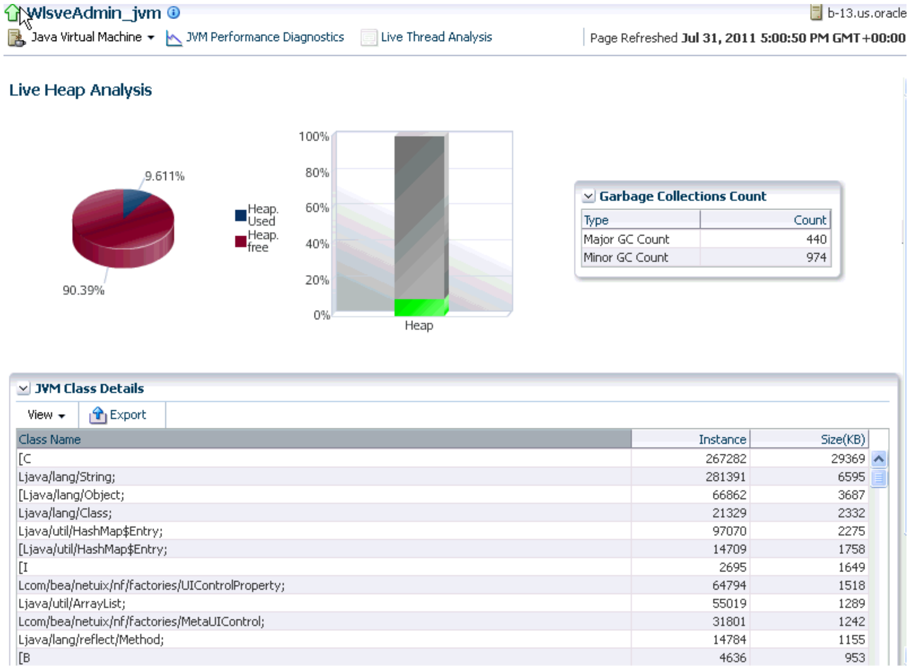
If the JVM is running at Optimization Level 0, the following details are displayed:

- Pie Charts and Bar Charts that show the percentage utilization of the entire heap (free versus used)
- Major and Minor Garbage Collections Count
- Options to take snapshots of active threads or a specific thread.
- JVM Class Details table that displays all the classes in the JVM Heap in decreasing order of their size (in KB). You can export this data to an .xls file using the **Export** option.

Note: For JVMs running at optimization level, the following details are displayed:

- JVM Heap Memory Usage table where the usage (in KB) in various heap spaces.
- JVM Heap Number of Objects table which displays the number of objects in various heap spaces.

Figure 14–9 JVM Live Heap Analysis Page



Garbage Collections Count

Type	Count
Major GC Count	440
Minor GC Count	974

JVM Class Details

Class Name	Instance	Size(KB)
[C	267282	29369
Ljava/lang/String;	281391	6595
[Ljava/lang/Object;	66862	3687
Ljava/lang/Class;	21329	2332
Ljava/util/HashMap$Entry;	97070	2275
[Ljava/util/HashMap$Entry;	14709	1758
[I	2695	1649
Lcom/bea/netuix/nf/factories/UIControlProperty;	64794	1518
Ljava/util/ArrayList;	55019	1289
Lcom/bea/netuix/nf/factories/MetaUIControl;	31801	1242
Ljava/lang/reflect/Method;	14784	1155
[B	4636	953

The following details are displayed:

- Garbage Collections: The number of objects that have been added to the garbage collection. The type of garbage collection i.e. minor or major, and the number of garbage collections of a particular type is displayed.
- JVM Class Details: This table provides a summary of the heap usage by different types of objects in the heap.
  - Space name: The name of the space within the JVM heap.
  - Class: The memory usage by classes in a heap space (in KB).
  - Instance: The number of heap objects for number of instances of classes in a heap space.
  - Size: The size of the JVM heap.

Click **Create Heap Snapshot** to take a heap snapshot. See Section 14.7.2, "Taking a Heap Snapshot" for details. Click **Export** to Excel to export the live heap data an Excel file.

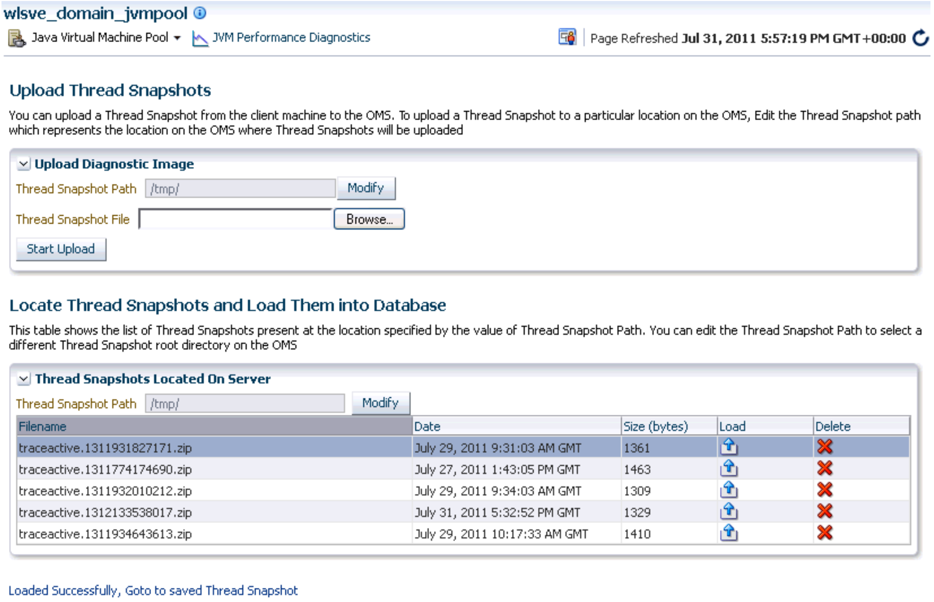
14.6 Viewing the Thread Snapshots

This page lists all the traces that have been loaded into the repository using the **Trace Active Threads** option. The Thread column indicates if all active threads or a specific thread has been traced. The number of samples taken during the trace are displayed. Select a thread and click the **Details** link to drill down to the Diagnostic Image Analysis page. Click the **Upload** link to take a thread snapshot of active threads.

14.6.1 Uploading Thread Snapshots

You can upload thread snapshots to a file and view the data at a later date. You can upload a thread snapshot from the client machine to the OMS. Click the **Thread Snapshots** link from the JVM Pool menu. Click the **Upload** link in the Thread Snapshots page. The Uploading Thread Snapshots page is displayed.

Figure 14–10 Uploading Thread Snapshots



Page Refreshed **Jul 31, 2011 5:57:19 PM GMT+00:00**

Upload Thread Snapshots

You can upload a Thread Snapshot from the client machine to the OMS. To upload a Thread Snapshot to a particular location on the OMS, Edit the Thread Snapshot path which represents the location on the OMS where Thread Snapshots will be uploaded

Upload Diagnostic Image

Thread Snapshot Path: /tmp/ Modify

Thread Snapshot File: Browse...

Start Upload

Locate Thread Snapshots and Load Them into Database

This table shows the list of Thread Snapshots present at the location specified by the value of Thread Snapshot Path. You can edit the Thread Snapshot Path to select a different Thread Snapshot root directory on the OMS

Thread Snapshots Located On Server

Thread Snapshot Path: /tmp/ Modify

Filename	Date	Size (bytes)	Load	Delete
traceactive.1311931827171.zip	July 29, 2011 9:31:03 AM GMT	1361	⇧	✗
traceactive.1311774174690.zip	July 27, 2011 1:43:05 PM GMT	1463	⇧	✗
traceactive.1311932010212.zip	July 29, 2011 9:34:03 AM GMT	1309	⇧	✗
traceactive.1312133538017.zip	July 31, 2011 5:32:52 PM GMT	1329	⇧	✗
traceactive.1311934643613.zip	July 29, 2011 10:17:33 AM GMT	1410	⇧	✗

Loaded Successfully, Goto to saved Thread Snapshot

When you run the Trace Threads option, you can save the trace file in your local machine or on the OMS. To upload the trace file from the:

- **Thread Snapshot Path**: Click **Modify** and specify the location of the diagnostic snapshots on the OMS.
- **Thread Snapshot File**: Click **Browse** to select the Trace Diagnostic Image File and click **Start Upload**.

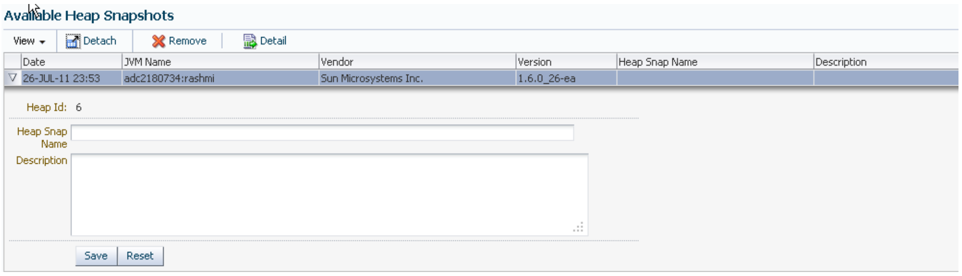
The list of thread snapshots is displayed. Select a file and click the Load icon to load the thread snapshot to the database. A message indicating that the trace file has been loaded successfully is displayed. Click the **Loaded Successfully, Goto Saved Trace** link to view the Diagnostic Image Analysis page.

14.7 Analyzing Heap Snapshots

The JVM Diagnostics memory analysis feature allows you to not only find the objects responsible for the growth but also track their reachability from the root-set. With this feature, you can find the dangling reference responsible for memory leaks. To find a memory leak, you take snapshots of the JVM heap at different points in time. Between the snapshots, your JVM and Java applications continue running at full speed with zero overhead.

A heap snapshot is a snapshot of JVM memory. Each snapshot stores information about the objects in the heap, their relationships and root-set reachability. You can load the snapshots into the repository, and compare them to see where the memory growth has occurred. Click **Heap Snapshots** from the menu in the JVM Pool or JVM Home page.

Figure 14–11 Available Heap Snapshots



	Date	JVM Name	Vendor	Version	Heap Snap Name	Description
▽	26-JUL-11 23:53	adc2180734:rashmi	Sun Microsystems Inc.	1.6.0_26-ea		

Heap Id: 6

Heap Snap Name

Description

The list of available heaps is displayed with the following details:

- Date: The date on which the heap snapshot was taken.
- JVM Name: The server on which the JVM is running.
- Vendor: The name of the JVM Vendor.
- Size: The total size of the Java heap. An adequate heap size helps improve the performance of the application.
- Used: The amount of heap that has already been used.
- %: The percentage of heap used.

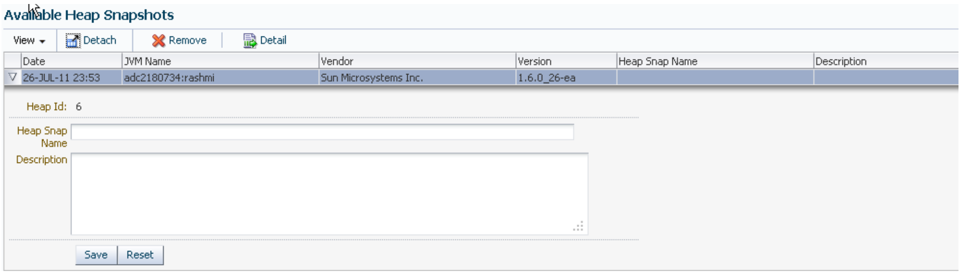
Select a heap from the list and click **Details**. The Heap Root and Usage page is displayed.

14.7.1 Viewing the Available Heap Snapshots

The JVM Diagnostics memory analysis feature allows you to not only find the objects responsible for the growth but also track their reachability from the root-set. With this feature, you can find the dangling reference responsible for memory leaks.To find a memory leak, you take snapshots of the JVM heap at different points in time. Between the snapshots, your JVM and Java applications continue running at full speed with zero overhead.A heap snapshot is a snapshot of JVM memory. Each snapshot stores information about the objects in the heap, their relationships and root-set reachability. You can load the snapshots into the repository, and compare them to see where the memory growth has occurred.

To view and analyze the heap usage, click the Heap Snapshots option from the JVM Pool menu. The list of available heaps with the JVM Name, vendor, size and other details is displayed.

Figure 14–12 Available Heap Snapshots



	Date	JVM Name	Vendor	Version	Heap Snap Name	Description
▽	26-JUL-11 23:53	adc2180734:rashmi	Sun Microsystems Inc.	1.6.0_26-ea		

Heap Id: 6

Heap Snap Name

Description

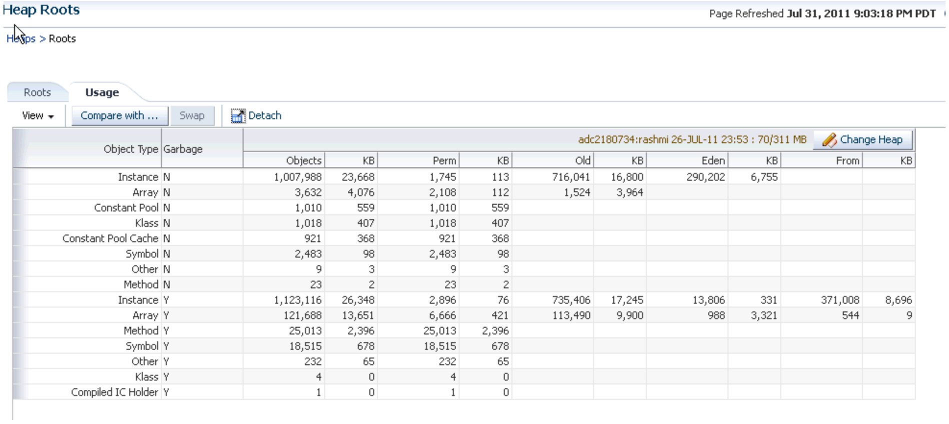
Select a heap snapshot and click the **Detail** link to drill down to the Roots page.

14.7.1.1 Viewing Heap Usage by Roots

To view the heap usage by each class of root, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine or a Java Virtual Machine Pool target.
2. Select **Heap Snapshots** option from the Java Virtual Machine or Java Virtual Machine Pool target.
3. The list of available heaps is displayed.

Figure 14–13 Heap Usage



Page Refreshed **Jul 31, 2011 9:03:18 PM PDT**

adc2180734:rashmi 26-JUL-11 23:53 : 70/311 MB

Object Type	Garbage	Objects	KB	Perm	KB	Old	KB	Eden	KB	From	KB
Instance	N	1,007,988	23,668	1,745	113	716,041	16,800	290,202	6,755		
Array	N	3,632	4,076	2,108	112	1,524	3,964				
Constant Pool	N	1,010	559	1,010	559						
Klass	N	1,018	407	1,018	407						
Constant Pool Cache	N	921	368	921	368						
Symbol	N	2,483	98	2,483	98						
Other	N	9	3	9	3						
Method	N	23	2	23	2						
Instance	Y	1,123,116	26,348	2,896	76	735,406	17,245	13,806	331	371,008	8,696
Array	Y	121,688	13,651	6,666	421	113,490	9,900	988	3,321	544	9
Method	Y	25,013	2,396	25,013	2,396						
Symbol	Y	18,515	678	18,515	678						
Other	Y	232	65	232	65						
Klass	Y	4	0	4	0						
Compiled IC Holder	Y	1	0	1	0						

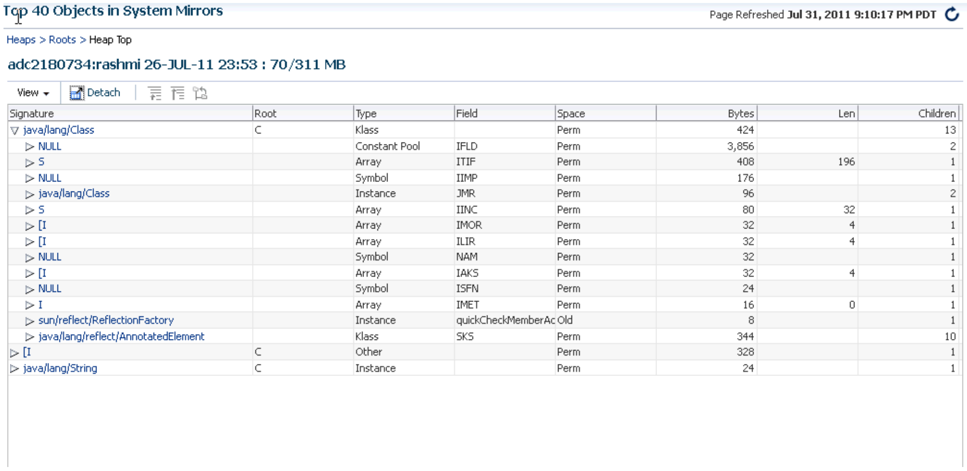
Click on the **Heap Details** tab to view the number of objects and memory reachable from each root. Click on the **Root** link to view the objects directly reachable from the root. The following details are displayed:

- Root: The name of the root is displayed here. Click on the name to drill down to the Top 40 Objects page.
- Object: The total number of objects reachable from this root.
- KB: The total amount of memory reachable from this root.
- Adj: The adjusted memory reachable from this root. This parameter is useful in tracking the memory leak hot-spots.

14.7.1.2 Top 40 Objects

This page shows the top 40 objects reachable from a root. The objects are sorted in descending order by the ascending memory reachable from the object (or the difference of the adjusted memory reachable when comparing two heaps). This view provides a lot of rich detailed information like the amount of memory used by an object, amount of memory reachable by an object (total memory used by all the children), and number of objects reachable from a given object.

Figure 14–14 Top 40 Objects



Top 40 Objects in System Mirrors

Page Refreshed **Jul 31, 2011 9:10:17 PM PDT**

Heaps > Roots > Heap Top

adc2180734:rashmi 26-JUL-11 23:53 : 70/311 MB

Signature	Root	Type	Field	Space	Bytes	Len	Children
▽ java/lang/Class	C	Klass		Perm	424		13
▷ NULL		Constant Pool	IFLD	Perm	3,856		2
▷ S		Array	ITIF	Perm	408	196	1
▷ NULL		Symbol	IIMP	Perm	176		1
▷ java/lang/Class		Instance	JMR	Perm	96		2
▷ S		Array	IINC	Perm	80	32	1
▷ [I		Array	IMOR	Perm	32	4	1
▷ [I		Array	ILIR	Perm	32	4	1
▷ NULL		Symbol	NAM	Perm	32		1
▷ [I		Array	IAKS	Perm	32	4	1
▷ NULL		Symbol	ISFN	Perm	24		1
▷ I		Array	IMET	Perm	16	0	1
▷ sun/reflect/ReflectionFactory		Instance	quickCheckMemberAc	Old	8		1
▷ java/lang/reflect/AnnotatedElement		Klass	SKS	Perm	344		10
▷ [I	C	Other		Perm	328		1
▷ java/lang/String	C	Instance		Perm	24		1

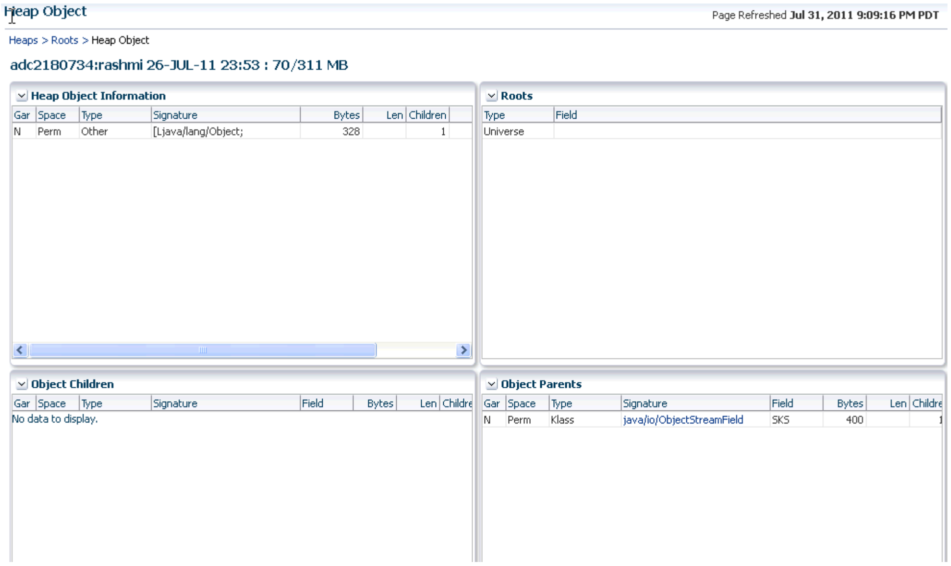
The following details are displayed:

- Signature: The signature of the object. Click on the link to drill down to the Details page.
- Root: This is the internal root identifier.
- Type: The type of the object which can be Klass, Instance, Method, and so on.
- Space: The heap space in which the object is present.
- Bytes: The amount of space used by the object.
- Len: If the object is an array, the length of the array is displayed here.
- Children: The number of descendants reachable from the object.
- Adj: Adjusted memory reachable from this object.
- Depth: Indicates how far this object is from the root.

14.7.1.3 Heap Object Information

This page shows information about a specific object in the heap snapshot. The following details are displayed:

Figure 14–15 Heap Object Information



Heap Object

Page Refreshed **Jul 31, 2011 9:09:16 PM PDT**

Heaps > Roots > Heap Object

adc2180734:rashmi 26-JUL-11 23:53 : 70/311 MB

Heap Object Information

Gar	Space	Type	Signature	Bytes	Len	Children
N	Perm	Other	[Ljava/lang/Object;	328		1

Roots

Type	Field
Universe	

Object Children

Gar	Space	Type	Signature	Field	Bytes	Len	Childre

No data to display.

Object Parents

Gar	Space	Type	Signature	Field	Bytes	Len	Childre
N	Perm	Klass	java/io/ObjectStreamField	SKS	400		1

- Heap Object Information
  - Gar: Indicates whether this object is garbage or reachable from the root.
  - Space: The heap space in which the object is present.
  - Type: The type of the object which can be Klass, Instance, Method, and so on.
  - Signature: The signature of the object.
  - Bytes: The amount of space used by the object.
  - Len: If the object is an array, the length of the array is displayed here.
  - Children: The number of descendants reachable from the object.
  - Adj: Adjusted memory reachable from this object.
  - Depth: Indicates how far this object is from the root.
- Roots
  - Type: The type of root which can be Klass, Instance, Method, and so on.
  - Field: If the root is a local thread, this field contains information about the thread and method.
- Object Children
  - Gar: Indicates whether this child is garbage or reachable from the root.
  - Space: The heap space in which the child is present.
  - Type: The type of the child which can be Klass, Instance, Method, and so on.
  - Signature: The signature of the child. Click on the link to drill down to the Details page.
  - Bytes: The amount of space used by the child.
  - Len: If the child is an array, the length of the array is displayed here.
  - Children: The number of descendants reachable from the child.
  - Adj: Adjusted memory reachable from this child.

  - Depth: Indicates how far this child is from the root.

- Object Parents
  - Gar: Indicates whether this parent is garbage or reachable from the root.
  - Space: The heap space in which the parent is present.
  - Type: The type of the parent which can be Klass, Instance, Method, and so on.
  - Signature: The signature of the parent. Click on the link to drill down to the Details page.
  - Bytes: The amount of space used by the parent.
  - Len: If the parent is an array, the length of the array is displayed here.
  - Children: The number of descendants reachable from the parent.
  - Adj: Adjusted memory reachable from this parent.
  - Depth: Indicates how far this parent is from the root.

14.7.1.4 Comparing Heap Snapshots

To find a memory leak, you can take snapshots of the JVM Heap at different points in time. Each snapshot stores information about the objects in the heap, their relationships and root-set reachability. You can compare two heap snapshots to see where the memory growth has occurred.

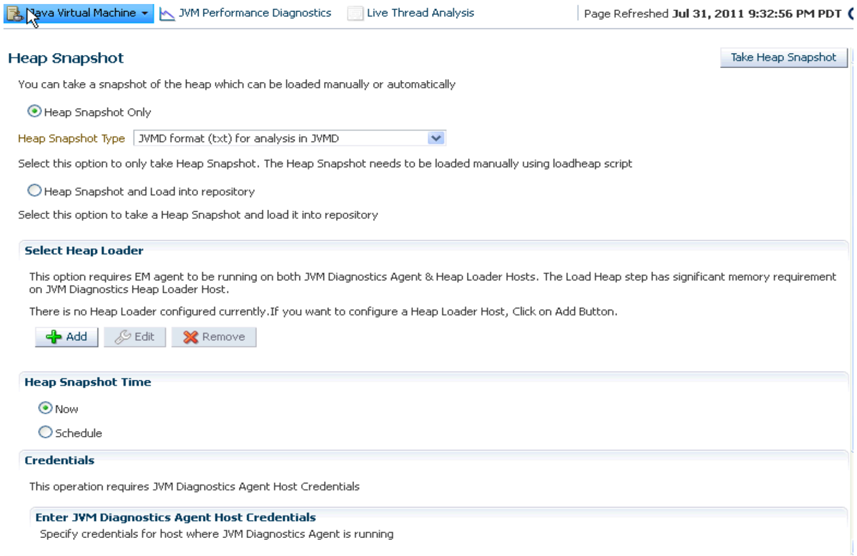
1. From the **Targets** menu, select **Middleware**, then click on a JVM or JVM Pool target.
2. Select **Heap Snapshots** option from the **Java Virtual Machine** or **Java Virtual Machine Pool** menu.
3. The list of available heaps is displayed. Click the **Compare Heaps** tab. The first heap in the list is selected for comparison and you are prompted to select the second heap.
4. The two heaps are compared and a comparison table is displayed in the Diff Heaps page. The details of each heap with the following details are displayed:
   - Objects: The total number of objects reachable from the root.
   - KB: The total amount of memory reachable from the root.
   - Adj: The adjusted memory reachable from this root. This parameter is useful in tracking the memory leak hot-spots. It provides a better representation of the memory used by an object by ignoring backwards pointing references from child objects to their respective parent object.
   - Delta: The difference in the total memory and adjusted reachable memory of the two heaps that are being compared.
5. Click on the root-set with the most growth to diagnose the memory leak.
6. Click the **View Summary** button to see a bottom up view of memory reachable by class of objects.

14.7.2 Taking a Heap Snapshot

A heap snapshot is a snapshot of JVM memory. It shows a view of all objects in the JVM along with the references between those objects. It can be used to study memory usage patterns and detect possible memory leaks. To take a heap snapshot, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a JVM target. The JVM Home page is displayed.
2. Select the **Heap Snapshots** option from the **Java Virtual Machine** menu.
3. The list of available heaps is displayed. Click **Create** in the Available Heaps page.
4. The Heap Snapshot page is displayed.

Figure 14–16 Heap Snapshot Page



Page Refreshed **Jul 31, 2011 9:32:56 PM PDT**

Heap Snapshot

You can take a snapshot of the heap which can be loaded manually or automatically

● Heap Snapshot Only

Heap Snapshot Type: JVMD format (txt) for analysis in JVMD

Select this option to only take Heap Snapshot. The Heap Snapshot needs to be loaded manually using loadheap script

○ Heap Snapshot and Load into repository

Select this option to take a Heap Snapshot and load it into repository

Select Heap Loader

This option requires EM agent to be running on both JVM Diagnostics Agent & Heap Loader Hosts. The Load Heap step has significant memory requirement on JVM Diagnostics Heap Loader Host.

There is no Heap Loader configured currently.If you want to configure a Heap Loader Host, Click on Add Button.

Heap Snapshot Time

● Now

○ Schedule

Credentials

This operation requires JVM Diagnostics Agent Host Credentials

Enter JVM Diagnostics Agent Host Credentials

Specify credentials for host where JVM Diagnostics Agent is running

You can use the following options to take a heap snapshot:

- Taking A Heap Snapshot Only: Choose this option to take a heap snapshot and load it manually to repository using the `loadheap` script.
- Taking a Heap Snapshot And Loading Into Repository: Choose this option to take a snapshot and automatically load it to the repository.

14.7.2.1 Taking A Heap Snapshot Only

To take a heap snapshot and load it manually into the repository using the `loadheap` script, follow these steps:

1. Select the **Heap Snapshot Only** option.
2. Select the **Heap Snapshot Type** which can either of the following:
   - JVMD Format (txt) for analysis in JVMD
   - HPROF Forma (binary) for analysis with external tools
3. Click **Take Snapshot**. The heap snapshot is generated and the file name in which it is stored is displayed. You can upload the heap snapshot and analyze it using appropriate options from the Heap Snapshots menu.

14.7.2.2 Taking a Heap Snapshot And Loading Into Repository

Select this option to take a heap snapshot and automatically load it into the repository.

Prerequisites

- The Management Agent must be deployed on the host machine on which the JVM target is running.

- The Heap Loader Host is a standalone machine (with high CPU and Memory) on which the Management Agent has been deployed.
- DB Client Home which is the location of `ORACLE_HOME` where `sqlldr` & `sqllplus` are present.
- There should be sufficient disk space in the system temp directory.
- A JVM Diagnostics DB User must have been created using the `create_jvm_diagnostic_db_user script`.

To take a heap snapshot and load it into the repository, follow these steps:

1. Select the **Heap Snapshot and Load Into Repository** option. You can select this option if the Management Agent is running on the JVM Diagnostics Agent and the Heap Loader Host.
2. If the Heap Loader Host has not been configured, click **Add**. Specify the Heap Loader Name, DB Client Home (the `ORACLE_HOME` (full absolute path) on the Heap Loader Host where sqlldr and sqlplus are present), and the Heap Loader Host and click **Save**.
3. If the Heap Loader Host has already been configured, the Available Heap Loaders are displayed. Select a heap loader from the list and enter the Host, DB User, and JVM Diagnostics Agent credentials.

Note:

- If preferred credentials for JVM Target & Heap Loader host are set, then the **Enter Credentials** region will not be displayed.
- If the Named Credentials for the JVM Diagnostics DB User is set, the **Enter Credentials** region will not be displayed.

4. Enter the schedule for the heap snapshot and click **Take Snapshot**. The heap snapshot is generated and loaded into the repository.

14.8 Tracing Active Threads

If a particular request is slow or hanging or if the entire application is slow, you can run the real-time transaction trace to view current Java application activity. You can look at the offending threads and their execution stack and analyze how much time a thread spent in waiting for DB wait or wait on a lock. Complex problems such as activity in one thread (or request) affecting the activity in the other thread or rest of the JVM can be found very quickly.

You can trace all active threads and generate a trace file which contains details such as resource usage, thread states, call stack information etc. During tracing, the state and stack of the target thread is sampled at set intervals for the desired duration. Follow these steps to trace active threads:

1. From the **Targets** menu, select **Middleware**, then select a Java Virtual Machine target.
2. Select the **Thread Snapshots** option from the Java Virtual Machine menu, then click **Create**.
3. In the Trace Active Threads page, specify the time interval between successive samples and the duration of the trace. Optionally, you can select the following parameters:

- Trace Thread Details: If this box is unchecked, only the last user call for the active thread will be stored. If the box is checked, all calls for the active thread will be stored, so you can view the call stack. Checking the box increases the overhead and space requirements
- Try Changing Threads: If a thread stack changes during a sample (this can happen when a thread is using CPU), JVM Diagnostics will skip that thread for that sample. If you find missing samples, use this feature to retrace the changed stacks. This will retry (up to 5 times) threads with changing stacks. It will also make system calls to get the stack if possible.
- Include Network Waits: Most JVMs have large number of idle threads waiting for network events. If you leave this check box unchecked, idle threads will not be included in the trace. Checking this box increases the overhead and space requirements.
- Trace All Threads: Check this box if both idle and active threads will be included in the trace.
- Allow Trace Interrupt: Allows you to interrupt the trace process.

4. Click **Start Trace** to generate the trace file. When the trace has been completed successfully, click **Goto Saved Trace** link to view the trace data. The Diagnostic Image Analysis page has the following details:

   - JVM Trace Results: This table provides information about when and where the trace was run. It also shows any filters which have been applied to the results of tracing. Most of the filters are applied by clicking the appropriate link from the tables below. The only exception is the JVM State filter which is applied from here by selecting from the drop-down.
   - Resource Usage: This section shows the system activities such as CPU utilization, heap usage, and garbage collection during tracing.
   - Top States: This chart shows the JVM Trace Analysis for the duration of the trace. Click **DB Wait** to view the DB activity.
   - Top Methods: This section shows a pie-chart of the top methods for the duration of the trace. It shows the name of the method and the number of samples.
   - Threads by State: This table shows the state time line for each thread colored by the state activity. It shows the number of samples in each state for each thread. Click on a thread to drill down to the Thread Details page.
   - Requests by State: This table shows the number of samples in each state for each request. Click on a request to view activity only for that request
   - Methods by State: This table shows number of samples in each state for each method. Click on a method to view activity only for that method.

14.9 Uploading Trace Diagnostics Images

You can upload trace data and heap data to a file and view it at a later date.

Uploading Trace Data

This file can be uploaded and stored on the OMS or on the database. To upload trace data (trace diagnostic image), follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine Pool or a Java Virtual Machine target.

2. Select the **Thread Snapshots** option from the Java Virtual Machine Pool or Java Virtual Machine menu. The list of available thread snapshots is displayed.
3. Click **Upload**. The Upload Trace Diagnostic Images page is displayed.
4. When you run the Trace Threads option, the trace file is saved on your local machine or on the OMS. To upload the trace file:
   - **Thread Snapshot Path**: Click **Modify** and specify the location of the diagnostic snapshots on the OMS.
   - **Thread Snapshot File**: Click **Browse** to select the Trace Diagnostic Image File and click **Start Upload**.
5. The list of trace files present on the specified location on the OMS is displayed. Select a file and click the **Load** icon to load the trace file to the database.
6. A message indicating that the trace file has been loaded successfully is displayed. Click the **Loaded Successfully, Goto Saved Trace** link to view the Diagnostic Image Analysis page or click **Ignore** to remain on the same page.

Uploading Heap Data

A heap snapshot is a snapshot of JVM memory. It shows a view of all objects in the JVM along with the references between those objects. You can upload these heap snapshots into the repository and analyze them to detect memory leaks. To upload a heap snapshot, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine target.
2. Select the **Heap Snapshots** option from the Java Virtual Machine menu. The list of available heap snapshots is displayed.
3. Click **Upload**. The Upload Trace Diagnostic Image page is displayed.
4. When you run the **Take Heap Snapshot** option, the heap snapshot is saved on your local machine or on the OMS. To upload the heap snapshot:
   - **Thread Snapshot Path**: Click **Modify** and specify the location of the diagnostic snapshots on the OMS.
   - **Thread Snapshot File**: Click **Browse** to select the Trace Diagnostic Image File and click **Start Upload**.
5. The list of heap snapshots present on the specified location on the OMS is displayed. Select a file and click the **Load** icon to load the heap snapshot to the database.
6. A message indicating that the heap snapshot has been loaded successfully is displayed. Click the **Loaded Successfully, Goto Saved Snapshot** link or click **Ignore** to remain on the same page.
7. The Diagnostic Image Analysis page is displayed. Click **Description** to view details of the heap snapshot being analyzed. The following Server State charts are displayed:

   The following details are displayed:

   - Garbage Collections: The number of objects that have been added to the garbage collection.
   - JVM Heap Memory Usage: This table provides a summary of the heap usage by different types of objects in the heap.

  - JVM Heap No of Objects: This table provides details of all the objects in the heap.

8. Click **Change / Manage Heap Snapshots**. A list of available heap snapshots for the JVM is displayed.
9. Select a heap snapshot file and click **Analyze** to view the Diagnostic Image Analysis page.

14.10 Viewing the Available Traces

This page lists all the traces that have been loaded into the repository. To view a list of all the available traces, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine Pool or Java Virtual Machine target. The Home page for the target is displayed.
2. Select the **Thread Snapshots** option from the Java Virtual Machine Pool or Java Virtual Machine menu.
3. The list of traces that have been loaded is displayed. The Trace ID, the date, the JVM Name is displayed. The Thread column indicates if all threads or only active threads have been traced.
4. Select a thread from the list and click **Details**. The Diagnostic Image Analysis page with the detailed analysis of the trace file is displayed.

14.11 Analyzing Trace Diagnostic Images

A trace diagnostic image contains details such as resource usage, thread states, call stack information etc. The trace diagnostic image captures thread data at short intervals. If an application is hanging or is slow, you can analyze these threads and find out the application tier that causing the delay.

On the Diagnostic Image Analysis page, you can:

- Click **Description** to view details of the thread snapshot being analyzed. The following Server State charts are displayed:
  - Active Threads by State: This chart shows the status of all threads in the JVM. The threads can be in different states like RMI, IO, NET, DB, CPU, and LOCK.
  - CPU Utilization by JVM: This chart shows the CPU utilization in the JVM.
  - Heap Utilization by JVM: This chart shows the heap utilization in the JVM.
- You can filter the data that is displayed by specifying various criteria such as Method Name, JVM Name, Thread State, DBState, and so on. Check the Ignore Filters check box if you want to ignore the specified filters. The Active Threads by State, Top Requests, Top Methods, Top SQLs, Top DBWait Events, and Top Databases charts are displayed.
- Click on the **Threads** tab to view the Thread State Transition, Metric By Active States, and Method data.
- Click **Change / Manage Traces**. A list of available trace files for the JVM Pool is displayed in the List of Traces Loaded page. The following details are displayed:
  - Trace ID: The port number for the JVM.
  - Date: The date and time the trace was run.
  - JVM Name: The name of the host on which the JVM is running.

- Thread: Indicates whether the trace was run for a specific thread or all active threads.
- Seconds: The trace duration in seconds.
- Samples: The number of samples in the trace.

- Select a trace file and click **Analyze**. The trace details are displayed in the Diagnostic Image Analysis page.
- Click **Offline Diagnostics** to create a diagnostic snapshot.

14.12 JVM Offline Diagnostics

Diagnostic data for one or JVM targets can be collected for a specific period and analyzed in an offline mode. This section describes the various options that are available to collect live JVM data and analyze it in offline mode. It contains the following sections:

- Creating a Diagnostic Snapshot
- Using the Diagnostics Snapshot Page
- Analyzing a Diagnostics Snapshot
- Viewing a Diagnostics Snapshot

14.12.1 Creating a Diagnostic Snapshot

You can create diagnostic snapshots for one or more JVM targets for a specified period. To create a diagnostic snapshot, specify the following:

1. From the **Targets** menu, select **Middleware**.
2. Select the **Manage Diagnostic Snapshots** option from the **Middleware Features** menu.

   The Create Diagnostic Snapshot option is also available in the JVM Performance Diagnostics page. Navigate the Performance Diagnostics page for a JVM, specify the time range for which you want to create the collection and click **Create Diagnostic Snapshot**.
3. Click **Create** in the Diagnostic Snapshots page. You can navigate to this page by clicking **Offline Diagnostics** on the Diagnostic Image Analysis page.
4. Enter a name and description for the diagnostic snapshot.
5. Specify the duration for the diagnostic snapshot.
6. Click **Add**. Select one or more JVM targets for which the diagnostic data is to be collected.

   Note: The JVM targets that you select must belong to the same JVM Pool.
7. Select the diagnostic types for the selected target and click **OK**. You will see a pop-up window that indicates that the diagnostic snapshot is being created. Click **Close** after the diagnostic snapshot has been created. You will return to the Diagnostic Snapshots page.

14.12.2 Using the Diagnostic Snapshots Page

You can collect diagnostic data for one or more JVM targets and analyze them in an offline mode. This page shows the list of diagnostic snapshots that have been created. You can specify search criteria to retrieve a specific snapshot. You can do the following:

- **Create**: Click **Create** to create diagnostic snapshots for one or more JVMs. The Create Diagnostic Snapshot page is displayed.
- **Export**: Select a file and click **Export** to export the diagnostic data to a file. Enter the location in which the file is to be stored. You can review and analyze the saved file in an offline mode on the same or a different host machine.
- **Import**: Click **Import** to import an exported file with diagnostic data for a particular collection object. Specify the name of the file and upload the file from your system. You can analyze the exported file and view a summary of the diagnostic snapshot.
- **Analyze**: Select a file and click **Analyze**. The Analyze Diagnostic Snapshot page is displayed.
- **Delete**: Select a diagnostic snapshot from the list and click **Delete**. A confirmation message is displayed. Click **OK** to delete the diagnostic snapshot.
- **View**: Select a file and click **View**. The View Diagnostic Snapshot page is displayed.

14.12.3 Analyzing a Diagnostic Snapshot

This page displays the summary details of the diagnostic snapshot and a summary of all the diagnostic types of the diagnostic snapshot. You can view the thread stack, thread states, CPU Utilization, Heap Utilization, Active Threads Graphs, and Garbage Collections.

To analyze a diagnostic snapshot, follow these steps:

1. From the **Targets** menu, select **Middleware**.
2. Select the **Manage Diagnostic Snapshots** option from the **Middleware Features** menu.
3. In the Diagnostic Snapshots page, select a snapshot from the list and click **Analyze**.
4. You can analyze details for each JVM for the specified time interval. Click **More Details** to view detailed diagnostics information for the JVM. The Diagnostic Image Analysis page is displayed.

14.12.4 Viewing a Diagnostic Snapshot

This page displays the summary of the targets, target types and the diagnostic information collected.

1. From the **Targets** menu, select **Middleware**.
2. Select the **Manage Diagnostic Snapshots** option from the **Middleware Features** menu.
3. In the Diagnostic Snapshots page, select a snapshot from the list and click **View**.
4. The summary details for the selected JVM target, target types, and the diagnostic information collected for the JVM is displayed.

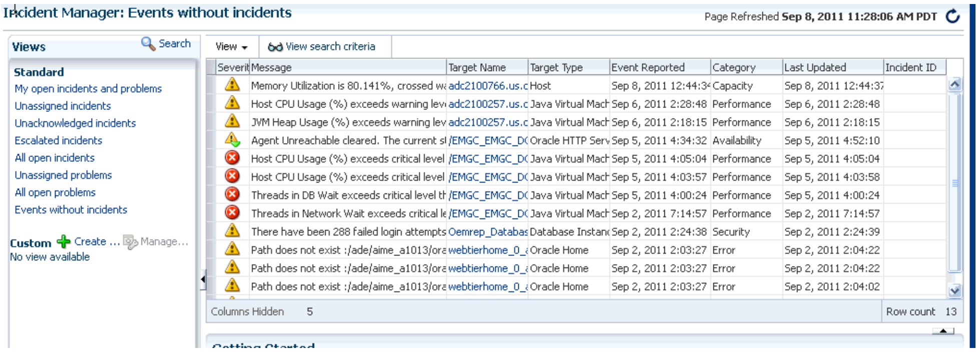
14.13 Viewing JVM Diagnostics Threshold Violations

An event is a discrete occurrence detected by Enterprise Manager related to one or more managed entities at a particular point in time which may indicate normal or problematic behavior. Examples of events include: a database target going down, performance threshold violation, change in application configuration files, successful completion of job execution, or job failure.

JVM Diagnostics threshold violations are now integrated with the Enterprise Manager Event subsystem. When a threshold violation occurs, an Enterprise Manager event is generated. To view the event, follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, then select **Incident Manager**.
2. In the View panel, click **Events without Incidents**. The JVM Diagnostics events are displayed if there are any outstanding JVMD threshold violations.

Figure 14–17 Incident Manager: Events without Incidents



Incident Manager: Events without incidents

Page Refreshed **Sep 8, 2011 11:28:06 AM PDT**

Severit	Message	Target Name	Target Type	Event Reported	Category	Last Updated	Incident ID
⚠	Memory Utilization is 80.141%, crossed wa	adc2100766.us.c	Host	Sep 8, 2011 12:44:3	Capacity	Sep 8, 2011 12:44:37	
⚠	Host CPU Usage (%) exceeds warning lev	adc2100257.us.c	Java Virtual Mach	Sep 6, 2011 2:28:48	Performance	Sep 6, 2011 2:28:48	
⚠	JVM Heap Usage (%) exceeds warning lev	adc2100257.us.c	Java Virtual Mach	Sep 6, 2011 2:18:15	Performance	Sep 6, 2011 2:18:15	
⚠	Agent Unreachable cleared. The current st	/EMGC_EMGC_D(	Oracle HTTP Serv	Sep 5, 2011 4:34:32	Availability	Sep 5, 2011 4:52:10	
⊗	Host CPU Usage (%) exceeds critical level	/EMGC_EMGC_D(	Java Virtual Mach	Sep 5, 2011 4:05:04	Performance	Sep 5, 2011 4:05:04	
⊗	Host CPU Usage (%) exceeds critical level	/EMGC_EMGC_D(	Java Virtual Mach	Sep 5, 2011 4:03:57	Performance	Sep 5, 2011 4:03:58	
⊗	Threads in DB Wait exceeds critical level th	/EMGC_EMGC_D(	Java Virtual Mach	Sep 5, 2011 4:00:24	Performance	Sep 5, 2011 4:00:24	
⊗	Threads in Network Wait exceeds critical le	/EMGC_EMGC_D(	Java Virtual Mach	Sep 2, 2011 7:14:57	Performance	Sep 2, 2011 7:14:57	
⚠	There have been 288 failed login attempts	Oemrep_Databas	Database Instanc	Sep 2, 2011 2:24:38	Security	Sep 2, 2011 2:24:39	
⚠	Path does not exist :/ade/aime_a1013/ora	webtierhome_0_a	Oracle Home	Sep 2, 2011 2:03:27	Error	Sep 2, 2011 2:04:22	
⚠	Path does not exist :/ade/aime_a1013/ora	webtierhome_0_a	Oracle Home	Sep 2, 2011 2:03:27	Error	Sep 2, 2011 2:04:22	
⚠	Path does not exist :/ade/aime_a1013/ora	webtierhome_0_a	Oracle Home	Sep 2, 2011 2:03:27	Error	Sep 2, 2011 2:04:02	

Columns Hidden 5

Row count 13

Getting Started

3. Click on the link in the Target Name column of a JVM Diagnostics Event.

   The JVMD threshold violations will show up in the Incidents table of the JVM or JVM Pool Home page only if the events have been promoted to incidents. For more information on promoting events to incidents, see the *Enterprise Manager Administration Guide*.

15 Troubleshooting JVM Diagnostics

This chapter describes the errors you may encounter while deploying and using JVM Diagnostics and the workaround steps you can follow to resolve each of them. It contains the following sections:

- Cross Tier Functionality Errors
- Trace Errors
- Deployment Script Execution Errors
- LoadHeap Errors
- Errors on JVM Diagnostics UI Pages
- Frequently Asked Questions

15.1 Cross Tier Functionality Errors

This section lists the errors that show the status of the JVM Diagnostics Manager.

Table 15–1 Cross Tier Functionality Errors

Error Message	Workaround Steps

`DBWait link not displayed on JVM Threads Real Time Analysis page.`
`No data displayed in Top DBStates / SQLs tables.`
	Cross tier functionality errors may occur due the following:
	▪ Incorrect database credentials
	▪ Database Agent errors
	If the database credentials are incorrect:
	▪ From the **Setup** menu, select **Middleware Diagnostics**, then click **Setup JVM Diagnostics** in the Middleware Diagnostics page. Click on the **Register Databases** tab and verify the credentials for the registered database to be monitored.
	▪ Enter the id of user who has installed the database in the OS User field.
	▪ Specify the database application user credentials in the DB User field.
	▪ Specify the database system user credentials in the DB User (Explain Plan) field.
	If database agent errors occur, ensure that the database agent is running on a machine on which the database is installed with the correct IP address and port number.
	▪ Select the **Live Thread Analysis** option from the Java Virtual Machine menu. If you see a thread that is in the DB Wait state, it should be a hyperlink. Click on the hyperlink to drill down to the database details and view the database session information including the SQL statements executed.
	▪ If the DB Wait state is not a hyperlink, from the **Setup** menu, select **Middleware Diagnostics**, then click **Setup JVM Diagnostics** in the Middleware Diagnostics page. Set the **Cross Tier Log Level** to 6 and send JVMD Manager logs report issue.

15.2 Trace Errors

This section lists errors that occur during tracing.

Table 15–2 Trace Errors

Error Message	Workaround Steps
`weblogic.transaction.internal.TimedOutException: Transaction timed out after 30 seconds`	This error occurs if the Poll Duration has a large value and results in a timeout. This error does not affect the Trace functionality and can be ignored.

15.3 Deployment Script Execution Errors

This section lists the errors that occur when you run the deployment script.

Table 15–3 Script Execution Errors

Error Message	Workaround Steps
`ScriptException: Error occured while performing deploy: The action you performed timed out after 600,000 milliseconds`	This error occurs when you are deploying the JVM Diagnostics Agent. To resolve this issue, check if the lock for the target WebLogic domain Administration Console has already been acquired. If it has been acquired, release it and run the script again. - Login to the WebLogic Administration Console: *http://<machine address>:<webogic port>/console*. - If you see the **Activate Changes** and **Undo All Changes** buttons in the left pane, click on these buttons to clear them. If the buttons are not cleared, click **Undo All Changes** and run the script again.

15.4 LoadHeap Errors

This section lists loadheap errors.

Table 15–4 LoadHeap Errors

Error Message	Workaround Steps

`glibc detected * free(): invalid next size (fast): 0x0965d090" ./loadheap.sh: line 237: 32357 Aborted ./bin/${bindir}/processlog in=$infile hdr=${sumdata} obj=${objdata} rel=${reldata} root=${rootdata} osum=${objsumdata} rrel=${rootrel} heap=${heap _id} skip=$skipgarbage db=$dbtype $*`
`Error processing file /tmp/heapdump6.txt`
	Check if the heapdump operation has been successfully completed. Open the `heapdump6.txt` file and check if there is a `heapdump finished` string at the end of the file. If you see this string, load the finished dump file.

`Heapdump already in progress, cannot take another heapdump`	Check if the `heapdump` operation has been successfully completed. Open the `heapdump6.txt` file and check if there is a `heapdump finished` string at the end of the file.
`loadheap.sh created unusable unique indexes.`	Run the `loadheap/sql/cleanup.sql` shipped with `loadheap.zip` to fix the unique indexes.

15.5 Errors on JVM Diagnostics UI Pages

This section lists the user interface errors.

Table 15–5 JVM Diagnostics UI Page Errors

Error Message	Workaround Steps
`JAM Console: Socket timed out after recv -- client adc2100083.us.oracle.com:7001 is not Active [0] secs JAM Console jamlooptimeout = [3]JAM CONSOLE: JVM 1 is not active JAM Cons Err Processing Request: 128 JVM 1 is not active jamDAL: jamreq returned 128 return status < 0 from jamDalInst.processRequest`	To resolve this error, increase the Agent Request Timeout (secs) and Agent Loop Request Timeout (secs)

Table 15–5 (Cont.) JVM Diagnostics UI Page Errors

Error Message	Workaround Steps
`Agent is up and running but is not displayed in the real time pages.`	If the log file shows `JAMMANAGER: OLD AGENT or NULL POOl or wrong jamoptimization level`, this indicates that the old jamagent/Dbagent is being used. To resolve this issue, download the latest `jamagent` from **Setup** > **Download** page.
`You do not have the necessary privileges to view this page`	Ensure that you have the required JVM Diagnostics Administrator or User privileges to view the JVM Diagnostics data.

15.6 Frequently Asked Questions

This section lists some of the questions you may have while using JVM Diagnostics. It includes the following:

- Location of the JVM Diagnostics Logs
- JVM Diagnostics Manager Status
- JVM Diagnostics Agent Status
- Monitoring Status
- Creating Less Privileged Users
- Usage of Try Changing Threads Parameter
- Significance of Optimization Levels
- Manually Deploying the JVM Diagnostics Agent
- Log Manager Level
- Repository Space Requirements

15.6.1 Location of the JVM Diagnostics Logs

You can find the JVM Diagnostics logs in the following locations:

- The JVM Diagnostics Manager Log file is located at `$EMGC_JVMDMANAGER1/logs/EMGC_JVMDMANAGER1.out`
- UI related errors are logged in:
  - `$T_WORK/gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/logs/EMGC_OMS1.out`
  - `$T_WORK/gc_inst/user_projects/domains/GCDomain/servers/EMGC_OMS1/logs/EMGC_OMS1.log`
- Communication errors between the JVM Diagnostics Manager and the Console are logged in `$T_WORK/gc_inst/em/EMGC_OMS1/sysman/log/emoms.log`

15.6.2 JVM Diagnostics Manager Status

To check the status of the JVM Diagnostics Manager:

- From the **Setup** menu, select **Middleware Diagnostics**, then click **Setup JVM Diagnostics**.

- Check the JVM Diagnostics Agent log file to verify the connection between Agent and the Manager. If you see an error - `JAM Agent ERROR: Cannot connect to Console:Connection refused`, this indicates that the JVM Diagnostics Manager is not running.
- Check if the message `JAM Console: Agent connection from:[Hostname]` is present in the JVM Diagnostics Manager log file. If this message appears, it indicates that the JVM Diagnostics Manager is running and is connected to the Agent.

15.6.3 JVM Diagnostics Agent Status

To check the status of the JVM Diagnostics Agent:

- From the **Targets** menu, select **Middleware**, then click on a Java Virtual Machine target. Select the **Live Thread Analysis** option from the Java Virtual Machine menu. Check the JVM Status in the Connected JVMs table.
  - If the status is **Not Active**, this indicates that the Agent is not connected to the Manager. Check the agent logs to verify if it is running and the IP address and port number of the Manager is correct.
  - If the status is **No AD4J Agent Deployed**, the JVM Diagnostics Agent must be deployed on that JVM.
- If the JVM Diagnostics Agent is running, the active threads data must be visible. If the JVM Diagnostics Agent is not running, you will see a message - `JVM is inactive, Please try again after some time`.

15.6.4 Monitoring Status

To verify if the JVM Diagnostics Manager is monitoring the data:

1. From the **Setup** menu, select **Middleware Diagnostics**, then click **Setup JVM Diagnostics** in the Middleware Diagnostics page. In the JVMD Configuration page, verify that the **Enable Monitoring** check box is checked.
2. Navigate to the Monitoring page under Setup and check if monitoring status is **On** for the Pool to which the JVM being monitored belongs.
3. Navigate to the JVM Pools page under Setup and verify if the **Poll Enabled** check box has been checked for the Pool to which the JVM being monitored belongs. Monitoring should now be enabled.

15.6.5 Running the create_jvm_diagnostic_db_user.sh Script

You can run the `create_jvm_diagnostic_db_user.sh` script if you want to create less privileged users who can only load heaps using the `loadHeap` script.

15.6.6 Usage of the Try Changing Threads Parameter

This parameter should be used only when the JVM is highly active.

15.6.7 Significance of Optimization Levels

The JVM Diagnostics Agent supports three optimization levels:

- Level 0 indicates that the JVM Diagnostics Agent is using a JVMTI based engine. This level is supported for JDK 6 series on almost all supported platforms.

- Level 1 is a hybrid between level 0 and level 2. It is supported only for very few JDKs on selected platforms.
- Level 2 uses Runtime Object Analysis technique for monitoring as it is efficient at run time.

15.6.8 Custom Provisioning Agent Deployment

You can customize the JVMD Agent deployment in the production environment by running custom provisioning scripts.

After the OMS has been installed, the `jvmd.zip` file can be found in the `plugins/oracle.sysman.emas.oms.plugin_12.1.0.0.0` directory in the Middleware installation directory. The zip file contains a set of scripts in the `customprov` directory. Details on using these scripts are described in the `README.TXT` present in the same directory. To use the custom provisioning scripts, follow these steps:

1. From the **Setup** menu, select **Middleware Diagnostics**, then click the **Setup JVM Diagnostics** in the Middleware Diagnostics page. Click the **Register Databases** tab and download the `jamagent.war` file
2. Make a copy of the deployment profile that includes the location of the downloaded `jamagent.war`, domains, and server details.
3. Run the `Perl script` on the deployment profile which will deploy the JVMD Agent to all the specified servers.

15.6.9 Log Manager Level

The default log manager level is 3. You can temporarily increase this to a higher level if you encounter some issues. Log levels 1 to 5 are supported where:

- 1 - Error
- 2 - Warning
- 3 - Info
- 4 - Debug
- 5 - Trace

15.6.10 Repository Space Requirements

For monitoring data, Oracle recommends 50 MB per JVM per day with the default setting of a 24 hour purge interval. This amount can vary based upon runtime factors (e.g depth of call stacks, etc.) within your environment. Hence, you must check the tablespace growth periodically and if required, you may need to change the space requirements. This will ensure that database growth due to standard monitoring will occur smoothly without sudden spikes. Tablespace sizing can be affected by the following:

- Heap Dumps: Analyzing heaps requires a large amount of tablespace. As a standard practice, we recommend that you must have 5 times the size of heap dump file being loaded in your tablespace. Since you know the size of your dump file, make sure that there is adequate space to accommodate the dump file before it is loaded into the database.
- Thread Traces: While these are smaller than heaps. they are loaded into the database automatically when a user initiates a trace at the console. The size of these threads can vary dramatically depending on the number of active threads

during the trace, the duration of the trace, and the sample interval of the trace. This should usually be under 100MB but if several thread traces have been initiated, it could fill up the database quickly. Before initiating the traces, you must ensure that there is adequate space in the database.

Part VII

Managing Oracle Coherence

The chapters in this part contain information on discovering and monitoring a Coherence cluster. It contains the following chapters:

- Chapter 16, "Getting Started with Management Pack for Oracle Coherence"
- Chapter 17, "Monitoring a Coherence Cluster"

16

Getting Started with Management Pack for Oracle Coherence

This chapter describes the procedure to discover and monitor a Coherence cluster using Oracle Enterprise Manager Cloud Control 12*c*. The following sections are covered in this chapter:

- About Coherence Management
- New Features
- Understanding the Discovery Mechanism
- Enabling the Management Pack

16.1 About Coherence Management

Oracle Coherence is an in-memory data-grid and distributed caching solution. It is composed of many individual nodes or JVMs which work together to provide highly reliable and high speed virtual caching.

Enterprise Manager provides deep visibility into performance of all the artifacts such as caches, nodes, and services. The Cluster Home page displays an overview of the performance hotspots such as nodes with minimum available memory, publisher and receiver success rate, and nodes with maximum send queue size. The Cluster Home page provides immediate visibility into the worst caches in the system based on hits to gets ratio which is an overall health indicator for the cluster.

Nodes and caches can be proactively monitored by the Incident Management feature. You can create a monitoring template by pre-populating the monitoring template with metrics for a Coherence target. You can export and import monitoring templates to share monitoring settings between different Enterprise Manager deployments.

Metric Extensions are the next generation of User-Defined Metrics, which enable you to extend Enterprise Manager to monitor conditions specific to the enterprise's environment by creating new metrics for any target type. The inclusion of Metric Extensions as part of the exported or imported monitoring template provides an easy way to share many Metric Extensions at a time between Enterprise Manager deployments.

You can correlate cluster nodes with the underlying hosts to determine CPU and memory utilization on those hosts in order to make better decisions for scaling your clusters. You can see the association of the caches, nodes, hosts and also Oracle WebLogic targets using Coherence*Web applications.

Highly customizable performance views for monitoring performance charts and trends are available. You can overlay metrics for multiple nodes or caches in the same or different cluster for detail analysis to provide detailed visibility at the desired level. The drill down views allows you to determine the root cause of performance problems or simply identify performance trends in the Coherence Cluster.

To ensure that node departure is detected and resolved in a timely manner, you can setup a monitoring policy to detect departing nodes and replenish those many nodes.

Enterprise Manager provides a centralized cache data management feature that allows you to perform various cache operations such as add/remove index, view cache data, view query explain plan, and so on.

Enterprise Manager monitors the changing configuration of the nodes over a period of time. You can compare configurations of multiple nodes which helps identify performance bottlenecks caused by configuration changes. The Topology Viewer provides a high level topology of the entire cluster and shows the relation between caches, nodes and hosts. You can customize topology view to show some key performance metrics as well.

All of the Coherence Management features are integrated with JVM Diagnostics and provide real-time visibility into the node JVMs. You can drill down to a Coherence node's JVM from within the context of a cache and a cluster to identify the method or thread that is causing a delay. The JVM Diagnostics feature is part of the WLS Management Pack EE and Management Pack for NonOracle Middleware.

Enterprise Manager provides a complete provisioning solution. You can maintain an Oracle Coherence setup image or gold image in the Software Library and deploy it throughout the infrastructure to create completely new clusters or add nodes an existing cluster. You can use the same deployment procedure to updates nodes as well.

16.2 New Features

This section lists the new features in Oracle Enterprise Manager Cloud Control 12*c*. The new features are:

- **Cache Data Management**: You can view, export, import, insert, update, purge, add, and remove indexes, view query explain plan and view trace. See Section 17.5, "Cache Data Management" for details.
- **Topology Viewer**: You can view the top-down hierarchy of the Coherence nodes, caches, clusters, and their related targets in the Topology Viewer. See Section 17.11, "Viewing Configuration Topology" for details.
- **Configuration Metrics Support**: You can store Coherence configuration metrics and perform operations like compare configurations, view last collected configurations, search for configuration data, view saved configurations, and view configuration history. See the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for details on configuration metrics.
- **Performance Summary and Metric Palette Integration**: You can plot charts for critical Coherence cluster component metrics such as node metrics, cache metrics, service metrics, and host metrics. See Section 17.10, "Viewing Performance Summary" for details.
- **JVM Diagnostics Integration**: You can drill down to a Coherence node's JVM from within the context of a cache and a cluster to identify the method or thread that is causing a delay. The JVM Diagnostics feature is part of the WLS Management Pack EE. See Section 17.9, "Integration with JVM Diagnostics" for details.

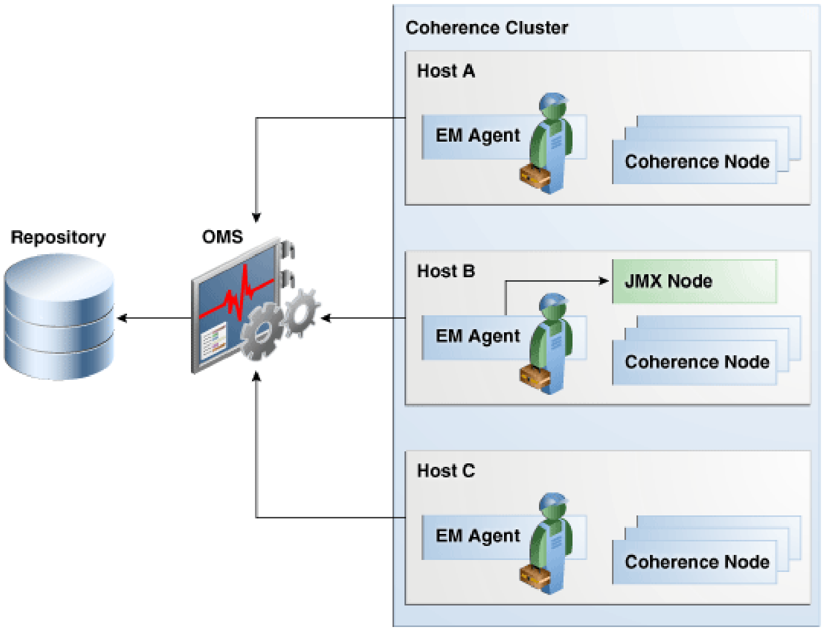
- **Log File Alerts**: You can set up alerts based on a pattern in a log file. Log files are periodically scanned for the occurrence of desired patterns and an alert is raised when the pattern occurs during a given scan. See Section 17.4, "Log File Monitoring" for details.
- **Push Replication**: If a push replication enabled cache is present in your cluster, you can now view the Publisher and Subscriber tables. See Section 17.7, "Push Replication Pattern" for details.
- **Transaction Cache Support**: You can now view specialized distributed caches or transactional caches in a service. See Section 17.8, "Transactional Cache Support" for details.
- **Reap Session Support**: You can now view then reap session metrics in the Application Home page. See Section 17.6, "Reap Session Support" for details.
- **Coherence Provisioning Enhancements**: In this release, the Well Known Address and the Update Nodes features are now available. For more details, see the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide.*
- **Elastic Data Support**: Elastic data is used to seamlessly store data across memory and disk-based devices. To support this feature, new performance and configuration metrics have been added to the Coherence node target in Enterprise Manager 12*c*.
- **Replenish Storage Enabled Nodes**: You can configure corrective actions to start stopped/crashed storage enabled nodes. This enables cluster operation with minimal disruption.

16.3 Understanding the Discovery Mechanism

Enterprise Manager monitors the entire Coherence cluster and its artifacts. The key targets that can be monitored are Oracle Coherence Cluster, Oracle Coherence Node, and Oracle Coherence Cache. The Oracle Coherence Cluster target provides a high level view of the health of the entire cluster. The Oracle Coherence Node and Oracle Coherence Cache are child targets of the Oracle Coherence Cluster. In addition to monitoring the above target types, additional Coherence components such as Services, Connections, and Applications can also monitored.

Figure 16–1 shows the Coherence Monitoring Setup.

Figure 16–1 Coherence Monitoring Setup



As shown in Figure 16–1, a typical Coherence deployment has nodes running on one or more hosts. In order to monitor the Coherence cluster in Enterprise Manager, a central Coherence JMX management node must be configured. This JMX management node must expose all Coherence MBeans and attributes. In addition to configuring the JMX management node, the Management Agent must also be installed and configured on the same host as JMX management node. This is required to discover and monitor the Coherence cluster in Enterprise Manager. To provision new Coherence nodes, start, and stop nodes, the Management Agent must be installed on all hosts on which the nodes are running.

16.3.1 Starting a JMX Management Node

The Management Agent uses the JMX management node (centralized MBean server) to discover and monitor the entire Coherence cluster, including the nodes and caches. As a best practice, it is recommended that the Management Agent is present on the same host as the JMX management node that is used to discover and monitor the Coherence cluster. The Management Agent must be setup on all the machines on which the Coherence nodes are running to monitor and provision the cluster. See the *Using JMX to Manage Coherence* chapter in the *Oracle Coherence Management Guide* for more details on using JMX to manage Oracle Coherence.

The following .jar files must be present in the classpath along with other application specific .jar files.

```
<OEM_Agent_Home>/plugins/oracle.sysman.emas.agent.plugin_
12.1.0.3.0/archives/coherence/coherenceEMIntg.jar
```

```
<OEM_Agent_Home>/plugins/oracle.sysman.emas.agent.plugin_
12.1.0.3.0/archives/coherence/bulkoperationsmbean.jar
```

Note: The location of the .jar files may change based on the plugin version.

The following Java options must be specified:

- `-Dtangosol.coherence.management.remote=true`
- `-Dtangosol.coherence.management=all`
- `-Dcom.sun.management.jmxremote.port=<open TCP port>`
- `-Dtangosol.coherence.cluster=<cluster name>`
- `-Dtangosol.coherence.member=<unique name in the cluster>`
- `-Dtangosol.coherence.machine=<fully qualified hostname>`
- `-Doracle.coherence.machine=< fully qualified hostname >`
- `-Dtangosol.coherence.distributed.localstorage=false`
- `-server`
- `-Xms256m -Xmx256m` (you must ensure that there are adequate resources for the management node)

Unless JMX authentication is required, add the following Java options:

- `-Dcom.sun.management.jmxremote.authenticate=false`
- `-Dcom.sun.management.jmxremote.ssl=false`

For more details on JMX authentication, refer to the *Java* documentation.

16.3.1.1 Starting a JMX Management Node Using Shell

If you are using a shell script to start the JMX Management Node, you must use the following startup class for Java.

```
oracle.sysman.integration.coherence.EMIntegrationServer
```

16.3.1.2 Starting a JMX Management Node Using WebLogic Console

This option is supported only for Coherence 3.7 and later versions.

If you are starting the JMX Management Node using the WebLogic Console, you cannot customize the JMX management node start up class. To address this, you must add the `custom-mbeans.xml` to the Coherence server that will act as the JMX management node. Add the following snippet to the `custom-mbeans.xml` file.

```
<mbeans>
  <mbean id="100">
    <mbean-class>oracle.sysman.integration.coherence.CacheDataManager
    </mbean-class>
    <mbean-name>type=Custom,name=CacheDataManager
    </mbean-name>
    <enabled>true</enabled>
  </mbean>
  <mbean id="110">
    <mbean-class>oracle.as.jmx.framework.bulkoperations.BulkOperationsMBeanImpl
    </mbean-class>
    <mbean-name>type=BulkOperations</mbean-name>
    <enabled>true</enabled>
  </mbean>
</mbeans>
```

16.3.2 Starting Other Nodes

To start other nodes in the cluster, you must add the following Java options:

- `-Dtangosol.coherence.management.remote=true`
- `-Dtangosol.coherence.member= <unique member name in the cluster>`
- `-Dtangosol.coherence.cluster= <cluster name>`
- `-Dtangosol.coherence.machine=<fully qualified hostname>`
- `-Doracle.coherence.machine=<fully qualified hostname>`

> **Note:** If you are planning to start or stop Coherence nodes from Enterprise Manager, you must specify the following additional start Java options:
>
> `-Doracle.coherence.startscript=<node start script>`
>
> `-Doracle.coherence.home=<coherence home>`

If you are using the WebLogic Console to start a Coherence node (or Coherence Server as referred to within the WebLogic Console), you can use the WebLogic Console to customize the start arguments of the server.

If you are starting the Coherence node in a WebLogic Managed Server, you can specify the above parameters in the `startWebLogic.sh` or in the script you use to start the WebLogic server.

16.3.2.1 Verifying the JMX Management Node Configuration

After the JMX management node has been configured, you can use tools such as JConsole to verify if all the Coherence MBeans and attributes are available at the management node. Ensure that you are using the Machine Name:Port (and JMX credentials if any) to connect to the JMX management node.

16.3.3 Using JVM Diagnostics with Coherence

JVM Diagnostics provides deep visibility into the runtime of the JVM. JVM Diagnostics allows administrators to identify the root cause of performance problems in the production environment without having to reproduce them in the test or development environment. You can view the JVM Diagnostics data if the JVM Diagnostics Manager and JVM Diagnostics Agent have been deployed on the host machine on which the OMS running. To setup JVM Diagnostics on each Coherence node, you must download the JVM Diagnostics Agent.

To download the JVM Diagnostics Agent, follow the steps listed in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*. When the JVM Diagnostics is downloaded, the `jamagent.war` file is downloaded. You must to copy the `.war` file to all machines on which the Coherence nodes are to be integrated with JVM Diagnostics, and add it to the classpath. See Section 17.13, "Best Practices" for more information on how to start a Coherence node with JVM Diagnostics.

16.3.4 Discovering Coherence Targets

Prerequisites

To monitor a Coherence cluster in Enterprise Manager, the following prerequisites must be met:

- Install the 12.1.0.2.0 Management Agent on all hosts where Coherence nodes are running.

- Deploy the 12.1.0.3.0 Fusion Middleware Plug-in on all the Management Agents.
- Verify that all Coherence MBeans are available in the Coherence JMX management node as described in Section 16.3.2.1, "Verifying the JMX Management Node Configuration".

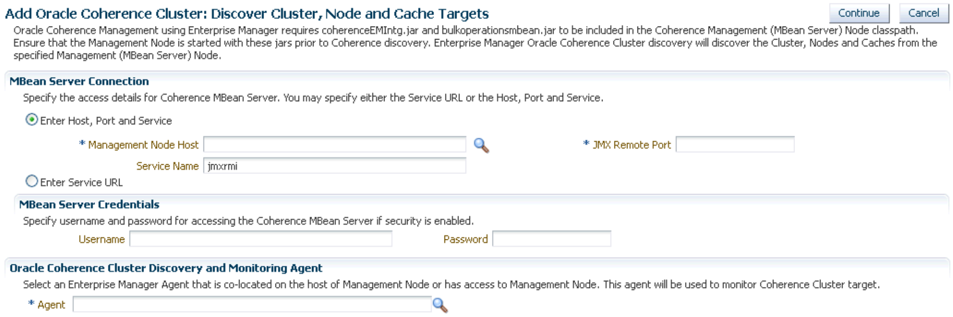
To discover a Coherence target, follow these steps:

1. Login to Enterprise Manager as an administrator with the **Add Target** privilege.
2. From the **Targets** menu, select **Middleware**. You will see a list of Middleware targets.

   > **Note:** Alternatively, you can add a Coherence target from the Setup menu. From the **Setup** menu, select **Add Target**, then select **Add Targets Manually**. In the Add Targets Manually page, select the **Add Non-Host Targets Using Guided Process** option. Follow the steps in the wizard to add the Coherence target.

3. Select Oracle Coherence in the **Add** drop-down box and click **Go**. The Oracle Coherence Cluster: Discover Cluster, Node, and Cache Targets page is displayed.

Figure 16–2 Add Coherence Target



Add Oracle Coherence Cluster: Discover Cluster, Node and Cache Targets

Oracle Coherence Management using Enterprise Manager requires coherenceEMIntg.jar and bulkoperationsmbean.jar to be included in the Coherence Management (MBean Server) Node classpath. Ensure that the Management Node is started with these jars prior to Coherence discovery. Enterprise Manager Oracle Coherence Cluster discovery will discover the Cluster, Nodes and Caches from the specified Management (MBean Server) Node.

MBean Server Connection

Specify the access details for Coherence MBean Server. You may specify either the Service URL or the Host, Port and Service.

● Enter Host, Port and Service

* Management Node Host

* JMX Remote Port

Service Name: jmxrmi

○ Enter Service URL

MBean Server Credentials

Specify username and password for accessing the Coherence MBean Server if security is enabled.

Username

Password

Oracle Coherence Cluster Discovery and Monitoring Agent

Select an Enterprise Manager Agent that is co-located on the host of Management Node or has access to Management Node. This agent will be used to monitor Coherence Cluster target.

* Agent

4. On this page, specify the connection details of the Coherence JMX management node. This is required to discover the Coherence cluster, node and cache targets. You can select either of the following options to provide MBean Server details:
   - Host, Port, and Service: Enter the following details:
     – Select the host on which the Management Node is running.
     – The port used for the JMX RMI connection. If you are using the MBean connector for Coherence MBeans, specify the `tangosol.coherence.management.remote.connectionport` property.

     > **Note:** It is recommended that you use the `com.sun.management.jmxremote.port` property.

     – The service name used for the connection. The default is `jmxrmi`.
   - Service URL that will be used for the connection. You may need to specify the Service URL only in complex cases like when the RMI registry and the MBean

Server ports are different. It is recommended that you use the Machine Name and Port option for the MBean server connection.

5. Select the Management Agent that will be used to monitor the Coherence target and click **Continue**.

6. The details of the discovered targets are displayed. Click **Add Targets** to add these targets to Enterprise Manager.

> **Note:** To automatically discover a new node or target in Enterprise Manager, you must configure the following corrective actions in the Metric and Collection Settings page:
>
> - **Cluster Size Change (To Add Node Entities)** on the Node Replenish and Entity Discovery Alert metric.
> - **Change in Number of Caches (To Add Cache Entities)** on the Cache Entities Discovery Alert metric. This metric is not available out-of-the-box.

16.3.5 Corrective Actions

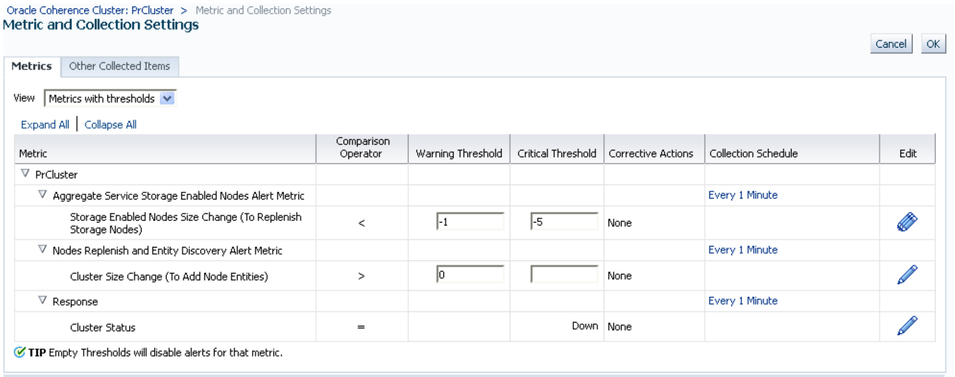
Corrective Actions allow administrators to specify automated responses to alerts or policy violations. Corrective Actions ensure that routine responses to alerts or policy violations are automatically executed, thereby minimizing administrator intervention and ensuring that problems are dealt with before they noticeably impact end users.

If you add a node or a cache after the cluster has been discovered, you must setup the **Discover New Oracle Coherence Nodes** and **Discover New Oracle Coherence Caches** corrective actions to add the node and cache as Enterprise Manager Targets. To setup the corrective actions, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Coherence Cluster target.

2. The Cluster Home page is displayed. From the Oracle Coherence Cluster menu, select **Monitoring**, then select **Metric and Collection Settings**. The Metric and Collection Settings page is displayed.

Figure 16–3 Metric and Collection Settings



Oracle Coherence Cluster: PrCluster > Metric and Collection Settings

Metric and Collection Settings

View: Metrics with thresholds

Metric	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Actions	Collection Schedule	Edit
▽ PrCluster						
▽ Aggregate Service Storage Enabled Nodes Alert Metric					Every 1 Minute	
Storage Enabled Nodes Size Change (To Replenish Storage Nodes)	<	-1	-5	None		✎
▽ Nodes Replenish and Entity Discovery Alert Metric					Every 1 Minute	
Cluster Size Change (To Add Node Entities)	>	0		None		✎
▽ Response					Every 1 Minute	
Cluster Status	=		Down	None		✎

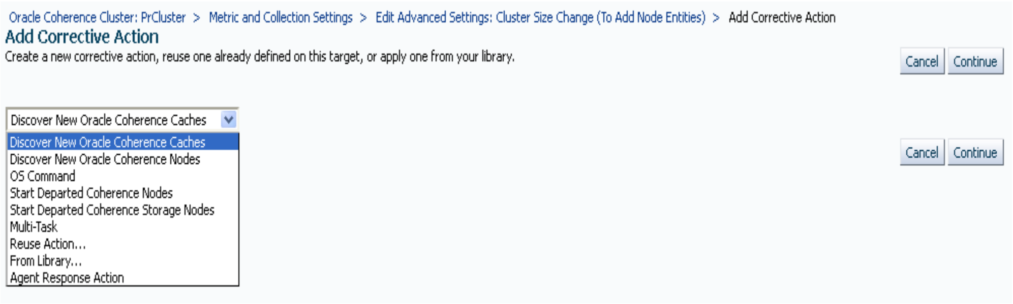
✓ **TIP** Empty Thresholds will disable alerts for that metric.

3. Click the **Edit** icon for the Change Number of Nodes metric. The Edit Advanced Settings page appears.

4. Under the Corrective Actions section, click **Add** for the metric severity (Warning or Critical) for which a corrective action is to be associated.

5. Click **Continue**. The Add Corrective Action page is displayed.

Figure 16–4 Add Corrective Action



Oracle Coherence Cluster: PrCluster > Metric and Collection Settings > Edit Advanced Settings: Cluster Size Change (To Add Node Entities) > Add Corrective Action

Add Corrective Action

Create a new corrective action, reuse one already defined on this target, or apply one from your library.

Cancel
Continue
Discover New Oracle Coherence Caches
Discover New Oracle Coherence Caches
Discover New Oracle Coherence Nodes
OS Command
Start Departed Coherence Nodes
Start Departed Coherence Storage Nodes
Multi-Task
Reuse Action...
From Library...
Agent Response Action
Cancel
Continue

6. Select the **Discover New Coherence Nodes** corrective action from the list and click **Continue**.

7. In the Create Corrective Action page, enter the name and description of the corrective action and click **Continue**. You are returned to the Edit Advanced Settings page with the corrective action set for the metric Warning and/or Critical metric thresholds.

8. Follow this process to set the corrective action for the Change Number of Caches metric.

16.3.6 Refreshing a Cluster

You can manually synchronize the cluster targets with the running Coherence cluster. Click **Refresh** Cluster from the Oracle Coherence Cluster menu. A message indicating that new Coherence nodes and caches that have been discovered will be added as Enterprise Manager targets is displayed. Nodes are updated if there are any changes to their attributes. Click **Continue** to refresh the cluster. This ensures that the latest changes are applied.

> **Note:** Decommissioned nodes and caches will not be removed during the **Refresh** process. You must remove them manually.

16.4 Enabling the Management Pack

You must enable the Management Pack for Oracle Coherence if you want to access additional features beyond Coherence cluster monitoring. To enable the Management Pack, do the following:

1. From the **Setup** menu, select **Management Packs**, then select Management Pack Access.

2. Select **Oracle Coherence** in the Search drop-down list and click **Go**.

3. All the Coherence targets being monitored are displayed. Check the **Pack Access Agreed** check box for the Coherence target and click **Apply** to enable the Management Pack.

17 Monitoring a Coherence Cluster

After you have discovered the Coherence target and enabled the Management Pack Access, you can start monitoring the health and performance of the cluster. You can monitor the entire cluster or drill down to the various entities of the cluster like nodes, caches, services, connection managers, and connections.

This chapter contains the following sections:

- Cluster Level Pages
- Detailed Pages
- Performance Pages
- Log File Monitoring
- Cache Data Management
- Reap Session Support
- Push Replication Pattern
- Transactional Cache Support
- Integration with JVM Diagnostics
- Viewing Performance Summary
- Viewing Configuration Topology
- Troubleshooting Coherence
- Best Practices

17.1 Cluster Level Pages

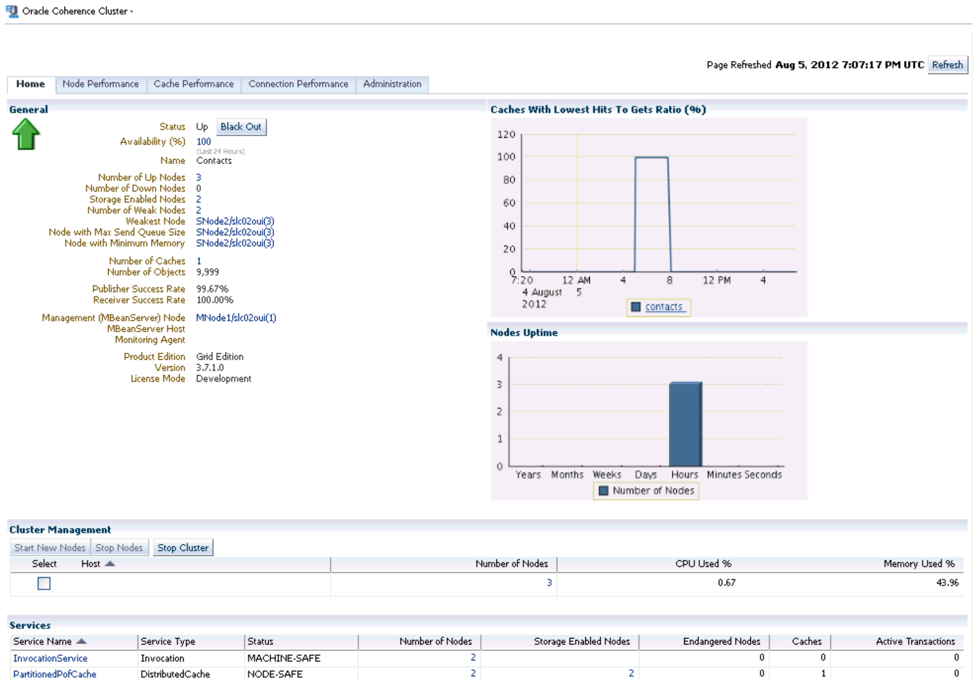
At the cluster level, you can view the Home page for the cluster, view the performance of all nodes, caches, and connections in the cluster, and change configuration for the different entities in the cluster.

17.1.1 Cluster Level Home Page

You can get a global view of the cluster from the Home page by following these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Coherence Cluster target. The Coherence Cluster Home page is displayed.

Figure 17–1 Cluster Home Page



Page Refreshed **Aug 5, 2012 7:07:17 PM UTC**

General

Status	Up
Availability (%)	100 (Last 24 Hours)
Name	Contacts
Number of Up Nodes	3
Number of Down Nodes	0
Storage Enabled Nodes	2
Number of Weak Nodes	2
Weakest Node	SNode2/slc02oui(3)
Node with Max Send Queue Size	SNode2/slc02oui(3)
Node with Minimum Memory	SNode2/slc02oui(3)
Number of Caches	1
Number of Objects	9,999
Publisher Success Rate	99.67%
Receiver Success Rate	100.00%
Management (MBeanServer) Node	MNode1/slc02oui(1)
MBeanServer Host	
Monitoring Agent	
Product Edition	Grid Edition
Version	3.7.1.0
License Mode	Development

Cluster Management

Select	Host ▲	Number of Nodes	CPU Used %	Memory Used %
□		3	0.67	43.96

Services

Service Name ▲	Service Type	Status	Number of Nodes	Storage Enabled Nodes	Endangered Nodes	Caches	Active Transactions
InvocationService	Invocation	MACHINE-SAFE	2		0	0	0
PartitionedPofCache	DistributedCache	NODE-SAFE	2	2	0	1	0

2. This page contains the following sections:

   - General
   - Graphs
   - Cluster Management
   - Service
   - Applications
   - Metric and Host Alerts

17.1.1.1 General

This section contains the following details:

- Name and status of the cluster.
- Availability%: This is really the availability of the cluster management node over the last 24 hours.
- Number of Up Nodes: The number of nodes that are Up. Click on the link to drill down to the Selected Nodes Performance page.
- Number of Down Nodes: The number of nodes that are Down. Click on the link to drill down to the Down Nodes page.
- Storage Enabled Nodes: Indicates the number of nodes that are storage enabled.
- Number of Weak Nodes: The number of nodes that are weak and have communication and performance issues. Click on the link to drill down to the Node Performance page.
- Weakest Node: The weakest node in the cluster. Click on the link to drill down to the Node Home page.

- Node with Max Queue Size: Indicates the node with the maximum queue size value in the cluster.
- Node with Minimum Memory: Indicates the node with the minimum available memory in the cluster.
- Number of Caches and Objects: The number of caches in the cluster and the number of objects stored in all caches in the cluster. Click on the Number of Caches link to drill down to the Cache Performance page.
- Publisher and Receiver Success Rates: The Publisher and Receiver success rate for this cluster node since the node statistics were last reset.
- Management Bean Server Node: This is the management node that contains the Coherence MBeanServer. Click on the link to drill down to the Node Home page.
- Monitoring Agent: The Oracle Management Agent monitoring the cluster.
- MBean Server Host: The host on which the management node is running. If the node on the MBean Server Host is not accessible, the monitoring capability of the entire cluster will be affected. To avoid this, we recommend that at least two management nodes are running on the cluster. If a management node departs from the cluster, you must update the host and port target properties to point to the host with the running management node.
- License Mode: The license mode that this cluster is using. Possible values are Evaluation, Development or Production.
- Product Edition: The product edition that this cluster is running on. Possible values are: Standard Edition (SE), Enterprise Edition (EE), Grid Edition (GE).
- Version: The Coherence version.

17.1.1.2 Graphs

Graphs indicating the health of the cluster are displayed here. The following graphs are displayed:

- Nodes Uptime: This graph displays groups of nodes according to their uptime. The Node Uptime is calculated as the difference between the Current Time and the Node Timestamp. Nodes that have an uptime of less than a minute are displayed in the seconds bar, nodes with an uptime of less than a hour are displayed in the minutes bar and so on.
- Caches with Lowest Hits to Gets Ratio: This graph shows caches (up to a maximum of 5) that have lowest Hits to Gets ratio. Click on the cache name in the legend section to drill down in to the Cache Details page to further investigate the reasons for the low hits to gets ratio.

> **Note:** The data in the General and Graphs section will be refreshed after one collection interval.

17.1.1.3 Cluster Management

In this section, you can start and stop one or more nodes, or stop a cluster.

Prerequisites

To perform Cluster Management operations, you must ensure that:

- The hosts on which the nodes are going to be started or stopped must be monitored targets in Enterprise Manager.

- The Coherence nodes are started with `-Dtangosol.coherence.machine` and `-Doracle.coherence.machine` Java options and the names match the host names monitored by Enterprise Manager.
- The Coherence nodes are started with `-Doracle.coherence.startscript` and `-Doracle.coherence.home` Java options.

  The `oracle.coherence.startscript` option specifies the absolute path to the start script needed to bring up a Coherence node. All customizations needed for starting this node should be in this script. The `oracle.coherence.home` option specifies the absolute path to the location in which the coherence folder is present which is `$INSTALL_DIR/coherence`. This folder contains Coherence binaries and libraries.
- Preferred Credentials have been setup for all hosts on which Cluster Management operations are to be performed.

You can do the following:

- Start New Nodes: You can start one or more nodes based on an existing node. The new node will have the same configuration as the existing node.
- Stop Nodes: You can stop all the nodes on a specific host.
- Stop Cluster: You can stop an entire cluster if all the hosts are managed by Enterprise Manager Cloud Control.

> **Note:** You can set up a corrective action to start departed Coherence Nodes automatically. When a node departs, this corrective action is launched, and the new node is automatically started on the same host on which the node was previously running.
>
> - `oracle.coherence.startscript`: The absolute path to the start script needed to bring up a Coherence node. All customizations needed for starting this node should be in this script.
> - `oracle.coherence.home`: The absolute path to the location in which the coherence folder is present which is `$INSTALL_DIR/coherence`. This folder contains Coherence binaries and libraries.

17.1.1.4 Services

This section shows all the services in the cluster. You can view the type of service, status of the service (Machine-Safe, Node-Safe, and Endangered), the number of nodes supporting the service, storage enabled nodes, endangered nodes, and active transactions.

17.1.1.5 Applications

This section shows the applications that use this Coherence cluster to cache their HTTPSession Objects. You can view details of the Local Cache, Overflow Cache, and Servlet Context Cache.

17.1.1.6 Metric and Host Alerts

This section lists the alerts from various entities in the cluster such as services, connections and connection managers, along with their severity and the date on which the alert was triggered. The alerts are generated based on the thresholds defined in the Metrics Collection file. To configure these threshold values, select the **Monitoring** menu option from the Oracle Coherence Cluster and select the Metric and Collection Settings submenu. Refer to the *Enterprise Manager Online Help* for detailed information on the parameters displayed in the screen.

17.1.1.7 Cluster Level Operations

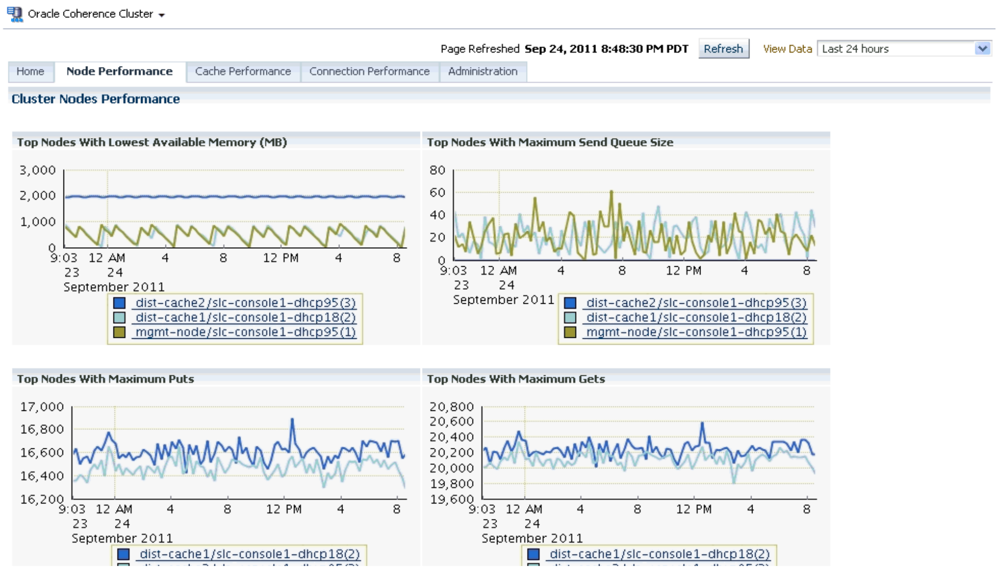
From the Cluster Home page, you can several other operations such as:

- **Viewing The Performance Summary**: From the **Oracle Coherence Cluster** menu, select **Monitoring**, then select **Performance Summary**. You can view the performance of the cluster on this page.
- **Metric and Collection Settings**: From the **Oracle Coherence Cluster** menu, select **Monitoring**, then select **Metric and Collection Settings**. You can set up corrective actions to add nodes and caches as Enterprise Manager targets.
- **Refreshing Cluster**: From the **Oracle Coherence Cluster** menu, select **Refresh Cluster**. You can refresh a cluster to synchronize Coherence targets in Enterprise Manager with a running cluster.
- **Coherence Node Provisioning**: From the **Oracle Coherence Cluster** menu, select Coherence Node Provisioning. You can deploy a Coherence node across multiple targets in a farm. See *Oracle Enterprise Manager Lifecycle Management Administrator's Guide* for more details on Coherence Node Provisioning.
- **Last Collected Configuration**: From the **Oracle Coherence Cluster** menu, select **Configuration,** then select **Last Collected**. You can view the latest or saved configuration data for the Coherence cluster.
- **Topology**: From the **Oracle Coherence Cluster** menu, select **Configuration**, then select **Topology**. The Configuration Topology Viewer provides a visual layout of the Coherence deployment.
- **JVM Diagnostics**: From the **Oracle Coherence Cluster** menu, select **JVM Diagnostics** to view the JVM Pool Performance Diagnostics page.

17.1.2 Cluster Level Node Performance Page

This page displays the node related performance over a specified period of time. Click the **Node Performance** tab to view this page.

Figure 17–2 Coherence Node Performance Page



Oracle Coherence Cluster
Refresh
Home
Node Performance
Cache Performance
Connection Performance
Administration
Cluster Nodes Performance
Top Nodes With Lowest Available Memory (MB)
3,000
2,000
1,000
0
9:03 12 AM 4 8 12 PM 4 8
23 24
September 2011
dist-cache2/slc-console1-dhcp95(3)
dist-cache1/slc-console1-dhcp18(2)
mgmt-node/slc-console1-dhcp95(1)
Top Nodes With Maximum Send Queue Size
80
60
40
20
0
9:03 12 AM 4 8 12 PM 4 8
23 24
September 2011
dist-cache2/slc-console1-dhcp95(3)
dist-cache1/slc-console1-dhcp18(2)
mgmt-node/slc-console1-dhcp95(1)
Top Nodes With Maximum Puts
17,000
16,800
16,600
16,400
16,200
9:03 12 AM 4 8 12 PM 4 8
23 24
September 2011
dist-cache1/slc-console1-dhcp18(2)
Top Nodes With Maximum Gets
20,800
20,600
20,400
20,200
20,000
19,800
19,600
9:03 12 AM 4 8 12 PM 4 8
23 24
September 2011
dist-cache1/slc-console1-dhcp18(2)

Page Refreshed **Sep 24, 2011 8:48:30 PM PDT**

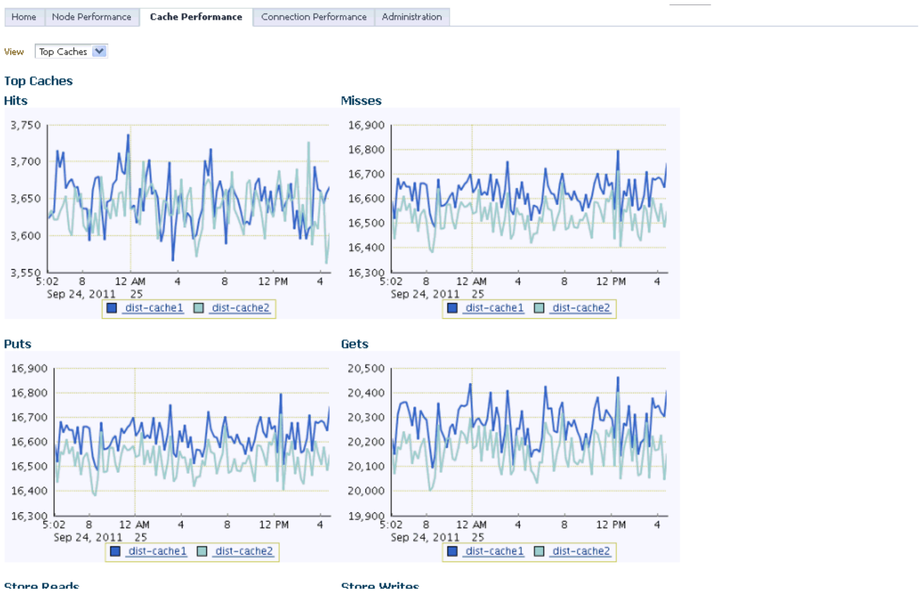
View Data Last 24 hours

This page displays the performance of all the nodes in the cluster over a specified period of time. You can see charts showing upto 5 top nodes with lowest available memory, maximum send queue size, maximum puts, and maximum gets. By default, you can see the average performance metrics for the last 24 hours in all the Performance pages. To view the real time charts, select one of the Real Time options in the View Data drop-down list in any of Performance pages. Using the View Data options, you can also view the average performance metrics for the last 7 or 31 days.The Node Performance page tab shows the performance of all nodes in this cluster. If you click on a link that shows multiple nodes like weak nodes, storage nodes, etc., the performance of the selected nodes will be displayed on this page. You can toggle between the two modes to see the performance of the selected nodes or all the nodes.

17.1.3 Cluster Level Cache Performance Page

This page displays the cache related performance over a specified period of time. You can view the performance of the top caches or all the caches.

Figure 17–3 Cluster Level Cache Performance



Select the **All Caches** option from the drop-down list to view the performance of all the caches in the cluster. If you select the All Caches option, you can see the total and average metric values over the selected period of time.

17.1.4 Cluster Level Connection Performance Page

This page shows the performance of all connection managers and connections in the cluster. The following Connection Manager graphs are displayed:

- Top Connection Managers with Most Bytes Sent since the connection manager was last started.
- Top Connection Managers with Most Bytes Received since the connection manager was last started.

A table with the list of Connection Managers is displayed with the following details:

- Connection Manager: This is the name of the connection manager. It indicates the Service Name and the Node ID where the Service Name is the name of the service used by this Connection Manager. Click on the link to drill down to the Connection Manager Home page.
- Service: The name of the service. Click on the link to drill down to the Service Home page.
- Node ID: An ID is automatically assigned to any node that is part of the cluster.
- Bytes Sent: The number of bytes sent per minute.
- Bytes Received: The number of bytes received per minute.
- Outgoing Buffer Pool Capacity: The maximum size of the outgoing buffer pool.
- Outgoing Byte Backlog: The number of outgoing bytes in the backlog.

The following Connection related graphs are displayed:

- Top Connections with Most Bytes Sent since the connection was last started.

- Top Connections with Most Bytes Received since the connection was last started.

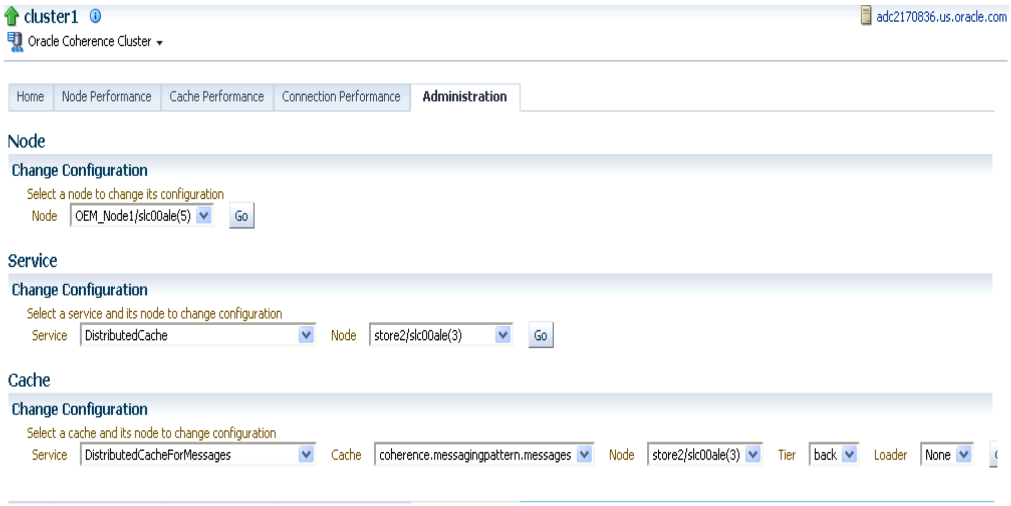
A table with the list of connections is displayed. Click on the link to drill down to the Details page.

- Remote Client: The host on which this connection exists.
- Up Since: The date and time from which this connection is running.
- Connection Manager: This is the name of the connection manager. Click on the link to drill down to the Connection Manager Home page.
- Service: The name of the service. Click on the link to drill down to the Service Home page.
- Node ID: An ID is automatically assigned to any node that is part of the cluster.
- Bytes Sent: The number of bytes sent per minute.
- Bytes Received: The number of bytes received per minute.
- Connection Time: The connection time in minutes.
- Outgoing Message Backlog: The number of outgoing messages in the backlog.
- Outgoing Byte Backlog: The number of outgoing bytes in the backlog.

17.1.5 Cluster Level Administration Page

This page allows you to change the configuration of nodes, caches, and services.

Figure 17–4 Cluster Level Administration Page



Node

Change Configuration

Select a node to change its configuration

Node: OEM_Node1/slc00ale(5) Go

Service

Change Configuration

Select a service and its node to change configuration

Service: DistributedCache Node: store2/slc00ale(3) Go

Cache

Change Configuration

Select a cache and its node to change configuration

Service: DistributedCacheForMessages Cache: coherence.messagingpattern.messages Node: store2/slc00ale(3) Tier: back Loader: None

On this page, you can select an entity (node, cache, or service) for which the configuration needs to be modified and click **Go**. The Change Configuration page is displayed. Enter the new values and click **Update** to save the values and return to the Coherence Cluster Administration page.

17.2 Detailed Pages

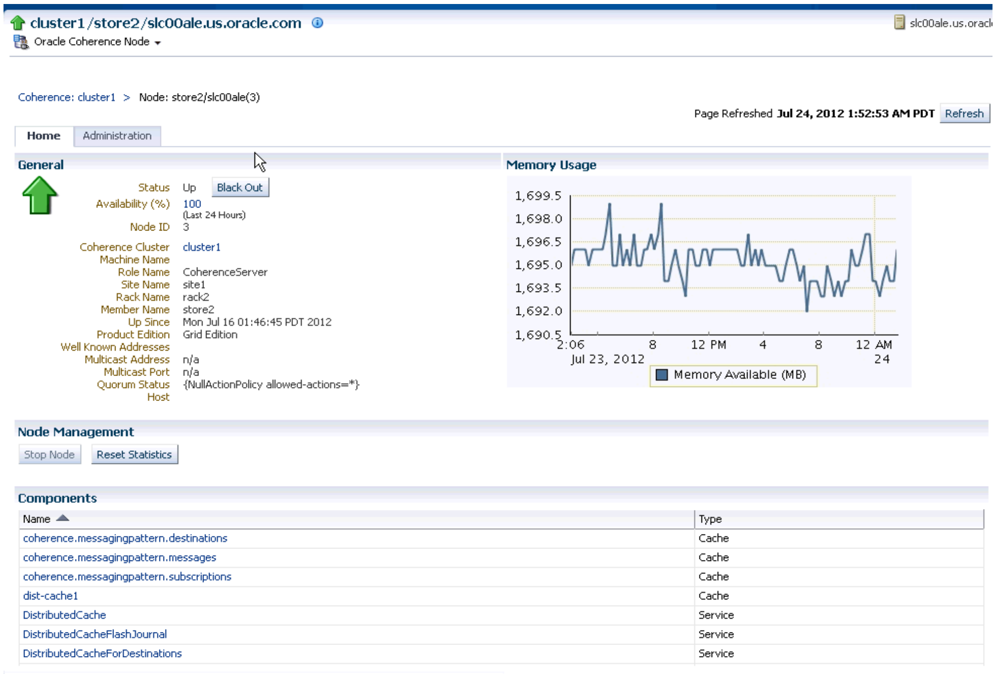
From the cluster level pages, you can click on any hyperlink and drill down to the detailed home pages of each entity in the cluster. Hyperlinks from one entity allow you to go to another entity. For example, you can view all the nodes of a cache in the Cache Detailed page, identify the node that is not contributing well for this cache, click on the node hyperlink and drill down to the Node Detailed page for further investigation.

- **Viewing The Performance Summary**: From the **Oracle Coherence Node** or Oracle Coherence Cache menu, select **Monitoring**, then select **Performance Summary**. You can view the performance of the node or cache on this page.
- **Metric and Collection Settings**: From the **Oracle Coherence Node** or **Oracle Coherence Cache** menu, select **Monitoring**, then select **Metric and Collection Settings**.
- **Last Collected Configuration**: From the **Oracle Coherence Node** or **Oracle Coherence Cache** menu, select **Configuration**, then select **Last Collected**. You can view the latest or saved configuration data for the Coherence cluster.
- **Topology**: From the **Oracle Coherence Node** or **Oracle Coherence Cache** menu, select **Configuration**, then select **Topology**. The Configuration Topology Viewer provides a visual layout of the relationship of the Coherence cluster with other targets.

17.2.1 Node Home Page

This page shows the details and controls of a specific selected node in the Coherence cluster.

Figure 17–5 Node Home Page



Page Refreshed **Jul 24, 2012 1:52:53 AM PDT**

Status	Up
Availability (%)	100 (Last 24 Hours)
Node ID	3
Coherence Cluster	cluster1
Machine Name	
Role Name	CoherenceServer
Site Name	site1
Rack Name	rack2
Member Name	store2
Up Since	Mon Jul 16 01:46:45 PDT 2012
Product Edition	Grid Edition
Well Known Addresses	
Multicast Address	n/a
Multicast Port	n/a
Quorum Status	{NullActionPolicy allowed-actions=*}
Host	

Name ▲	Type
coherence.messagingpattern.destinations	Cache
coherence.messagingpattern.messages	Cache
coherence.messagingpattern.subscriptions	Cache
dist-cache1	Cache
DistributedCache	Service
DistributedCacheFlashJournal	Service
DistributedCacheForDestinations	Service

This page contains the following sections:

- **General**
  - Node ID: When a node becomes part of a cluster, an ID is automatically assigned to the node. This ID can be a new number or the number that was assigned to a Departed Node.

  - Machine Name: The name of the machine on which the node is running.

    Note: You must set the machine name property when a node is started. To set the machine name, set the `-Dtangosol.coherence.machine=HOST_NAME` flag in the start coherence script. The `HOST_NAME` is the complete name of the machine on which the node is running. This allows you to associate the machine name with the Host Details page. See the Coherence documentation for more details on setting this flag.

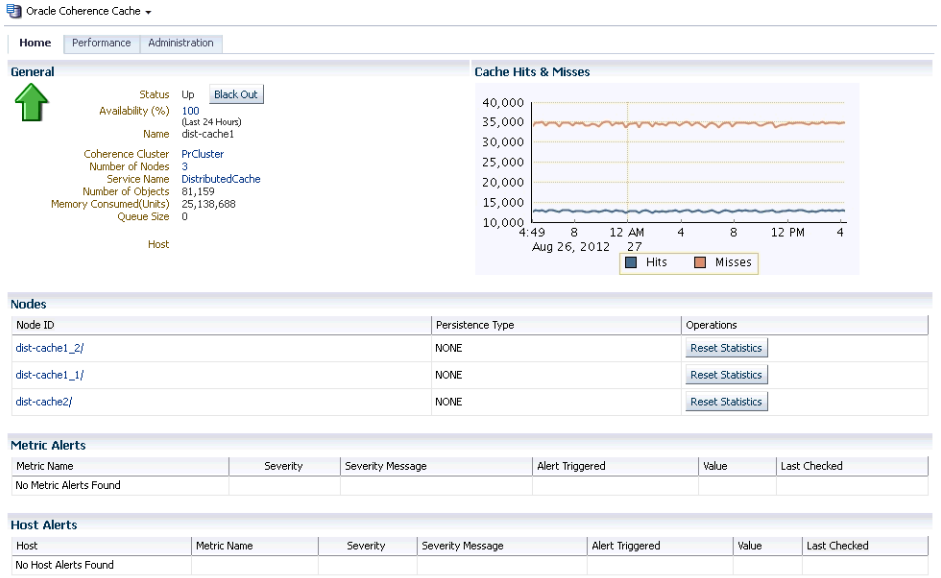
  - Role Name: The role could be storage/data, application/process, proxy or management node.
  - Site Name: This indicates the location of the coherence node.
  - Rack Name: Name of the rack where the machine is located.
  - Member Name: The unique name assigned to the Member.
  - Process Name: Indicates the name of the process on which the node is hosted.
  - Up Since: The date and time from this node has been up and running.
  - Product Edition: The product edition this Member is running. Possible values are: Standard Edition (SE), Enterprise Edition (EE), Grid Edition (GE).
  - Well Known Addresses: If cluster communication has been set to WKA (well known address), the host name and port number are displayed.
  - Multicast Port / Address: The IP address and port number of the Multicast Socket used for group communication.
  - Quorum Status: The current Quorum state.
  - Host: Click on the host name to drill down to the Host Home page.

- **Memory Usage**: The maximum memory and the available memory on this node are displayed as line graphs.
- **Node Management**: In this section, you can click **Stop Node** to stop this node and click **Reset Statistics** to reset all the statistics for this node. See **Prerequisites** in Section 17.1.1.3, "Cluster Management".
- **Components**: The list of components and the type of each component in the cluster are displayed here. Click on the link to drill down to the Component Home page.
- **Metric Alerts**: This table shows a list of all the metric alerts specific to this node.
- **Host Alerts**: This table shows a list of alerts from the host on which this node is running.

17.2.2 Cache Home Page

This page shows the details of the specific selected cache in the Coherence cluster.

Figure 17–6 Cache Home Page



General

Status	Up
Availability (%)	100 (Last 24 Hours)
Name	dist-cache1
Coherence Cluster	PrCluster
Number of Nodes	3
Service Name	DistributedCache
Number of Objects	81,159
Memory Consumed(Units)	25,138,688
Queue Size	0
Host	

Cache Hits & Misses

Nodes

Node ID	Persistence Type	Operations
dist-cache1_2/	NONE	Reset Statistics
dist-cache1_1/	NONE	Reset Statistics
dist-cache2/	NONE	Reset Statistics

Metric Alerts

Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
No Metric Alerts Found					

Host Alerts

Host	Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
No Host Alerts Found						

This page contains the following sections:

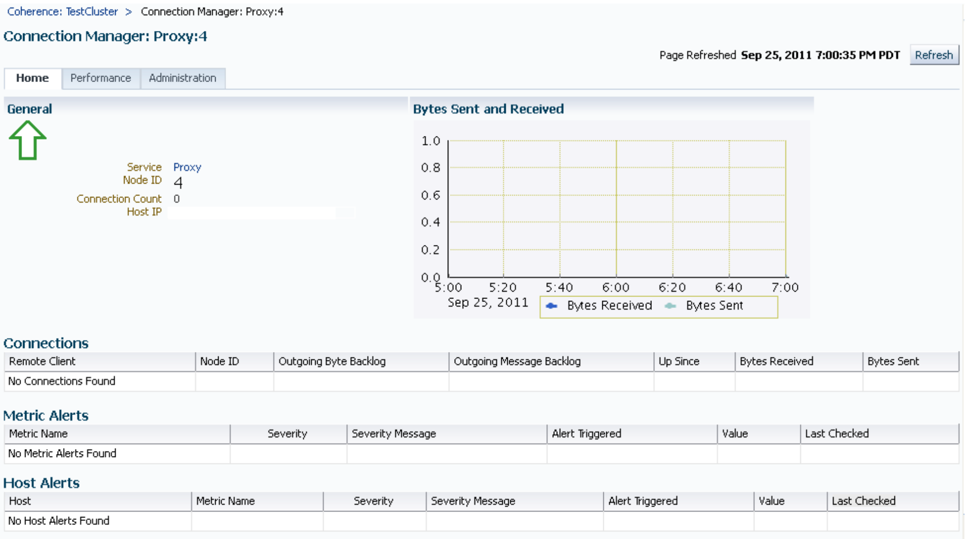
- **General**
  - Status: Indicates the status of the cache.
  - Availability: The percentage of time that the management agent was able to communicate with the cache. Click the percentage link to view the availability details for the past 24 hours.
  - Name: The unique name assigned to the cache.
  - Coherence Cluster: The name of the cluster. Click on the link to drill down to the Cluster Home page.
  - Number of Nodes: The number of nodes on which the cache is running. Click on the link to drill down to the Node Home page.
  - Service Name: The name of the service used by this cache.
  - Number of Objects: Shows the number of objects in the cache.
  - Memory Consumed: The amount of memory used by the cache in units.
  - Queue Size: The size of the write-behind queue size. Applicable only for `WRITE-BEHIND` persistence type.
- **Cache Hits and Misses**: This graph displays the total cache hits and misses per minute.
- **Nodes**: This section lists all the nodes supporting this cache.
  - Node ID: The ID number assigned to the node. Click on the link to drill down to the Node Home page.
  - Persistence Type: The persistence type for this cache. Possible values include: `NONE`, `READ-ONLY`, `WRITE-THROUGH`, `WRITE-BEHIND`.
- **Metric Alerts**: This table shows a list of all the metric alerts specific to this cache.

- **Host Alerts**: This table shows a list of alerts from the host on which this cache is running.
- **Push Replication Tables**: If a push replication enabled cache is present in your cluster, you can see the Publisher and Subscriber tables.

17.2.3 Connection Manager Home Page

Use this page to view the details and controls of a Connection Manager instance in the Coherence cluster.

Figure 17–7 Connection Manager Home Page



Coherence: TestCluster > Connection Manager: Proxy:4

Connection Manager: Proxy:4

Page Refreshed **Sep 25, 2011 7:00:35 PM PDT**

General

Service Proxy
Node ID 4
Connection Count 0
Host IP

Bytes Sent and Received

Connections

Remote Client	Node ID	Outgoing Byte Backlog	Outgoing Message Backlog	Up Since	Bytes Received	Bytes Sent
No Connections Found						

Metric Alerts

Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
No Metric Alerts Found					

Host Alerts

Host	Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
No Host Alerts Found						

This page contains the following sections:

- **General**
  - Service Name: The unique name assigned to the service.
  - Node ID: An ID is automatically assigned to any node that is part of the cluster. This can be a new number or a number that belongs to a Departed node.
  - Connection Count: The number of connections associated with the connection manager instance.
  - Host IP: The IP address of the host machine.
  - Refresh Time: The date and time on which the connection manager instance was last refreshed.
- **Bytes Sent and Received**: This graph displays the number of bytes that were sent and received per minute. Click on the graph to drill down to the Bytes Sent Metric page.
- **Connections**
  - Remote Client: A unique hexadecimal number assigned to each connection.
  - Service Name: The unique name assigned to the service.

- – Node ID: An ID is automatically assigned to any node that is part of the cluster. This can be a new number or a number that belongs to a Departed node.
- – Outgoing Byte Backlog: The number of outgoing bytes in the backlog.
- – Outgoing Message Backlog: The number of outgoing messages in the backlog.
- – Up Since: The date and time from which the connection manager instance is up.
- – Bytes Received: The number of bytes received per minute.
- – Bytes Sent: The number of bytes sent per minute.

- **Metric Alerts**: This table shows a list of all the metric alerts specific to this connection manager.
- **Host Alerts**: This table shows a list of alerts from the host on which this connection manager instance is running.

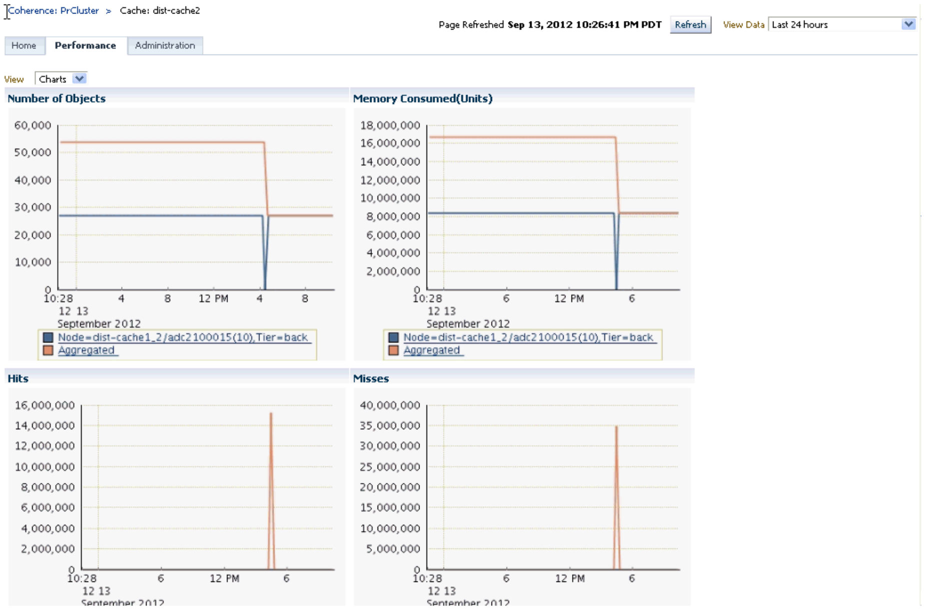
17.3 Performance Pages

Entity level performance pages give detailed views of the performance of this particular entity. For caches performance pages, there are two views - Charts and Metrics. You can select the option from the View drop-down list.

17.3.1 Cache Performance Details Page

This page displays the performance of a specific cache over a specific period of time. You can view charts showing the number of cache hits, misses, store reads, and store writes. You can also see the aggregated totals and average metric values over the selected period of time.

Figure 17–8 Cache Performance Details Page



Coherence: PrCluster > Cache: dist-cache2

Page Refreshed **Sep 13, 2012 10:26:41 PM PDT** Refresh View Data Last 24 hours

View Charts

The following graphs are displayed:

- Number of Objects: This graph shows the number of objects in the cache.
- Memory Consumed (Units): This graph shows the amount of memory consumed by the cache per minute.
- Hits: This graph shows the number of cache hits per minute.
- Misses: This graph shows the number of cache misses per minute.
- Puts: This graph shows the total number of put() operations per minute.
- Gets: This graph shows the total number of get() operations per minute.
- Store Reads: This graph shows the total number of load operations per minute.
- Store Writes: This graph shows the total number of store and erase operations per minute.
- Published Batches (per min)
- Replicated Entries
- Publishing Failures (per min)

Metrics: Select the **Metrics** option in the View By drop-down list to view the totals and averages for the cache.

- Totals / Averages: The aggregated total and average values across all nodes and per node total / average values for the cache during the selected period are displayed.
  - Hits: The number of successful fetches of the cached objects per minute.
  - Misses: The number of failed fetches of the cached objects per minute.
  - Puts: The number of addition of objects to a cache per minute.
  - Gets: The number of retrieval of objects from a cache per minute.
  - Prunes: The number of prune operations on the cache per minute. A prune operation occurs every time the cache reaches its high watermark.
  - Store Reads: The number of reads from a data store per minute.
  - Store Writes: The number of writes to a data store per minute.
  - Number of Objects: The number of objects in the cache.
  - Memory Consumed (Units): The amount of memory used by the cache in units.
  - Average Time (ms): The average execution time for each operation (hits, misses, puts, gets, store reads, and store writes) are displayed. The values since the last collection divided by the time taken by the operations are displayed. For example, if there are 100 Hits and these 100 Hits took 20 milliseconds since last collection, this value is calculated as 100/20 = 5.
- Storage Manager
  - Events Dispatched: The total number of events dispatched by the Storage Manager per minute.
  - Eviction Count: The number of evictions from the backing map managed by this Storage Manager caused by entries expiry or insert operations that would make the underlying backing map to reach its configured size limit.
  - Insert Count: The number of inserts into the backing map managed by this Storage Manager. In addition to standard inserts caused by put and invoke

operations or synthetic inserts caused by get operations with read-through backing map topology, this counter is incremented when distribution transfers move resources into the underlying backing map and is decremented when distribution transfers move data out.

– Remove Count: The number of removes from the backing map managed by this Storage Manager caused by operations such as clear, remove or invoke.

– Listener Filter Count: The number of listener filters.

– Listener Key Count: The number of listener keys.

– Listener Registrations: The number of listener registrations.

– Locks Granted: The number of locks granted.

– Locks Pending: The number of locks pending.

17.3.2 Connection Manager Performance Page

This page displays the performance of the selected connection manager over a specified period of time. The following graphs are displayed:

- Bytes Sent: This graph shows the number of bytes sent since the connection manager was last started.
- Bytes Received: This graph shows the number of bytes received since the connection manager was last started.

Performance:

The average performance over the selected period is displayed.

- Outgoing Byte Backlog: The number of outgoing bytes in the backlog.
- Outgoing Message Backlog: The number of outgoing messages in the backlog.
- Incoming Buffer Pool Capacity: The maximum size of incoming buffer pool.
- Incoming Buffer Pool Size: The currently used value of the incoming buffer pool.
- Outgoing Buffer Pool Capacity: The maximum size of the outgoing buffer pool.
- Outgoing Buffer Pool Size: The currently used value of the outgoing buffer pool.
- Bytes Received: The number of bytes received per minute.
- Bytes Sent: The number of bytes sent per minute.

17.3.3 Connection Performance Page

This page displays the performance of the specific connection over a specified period of time. The following graphs are displayed:

- Bytes Sent: This graph shows the number of bytes sent within the specified period.
- Bytes Received: This graph shows the number of bytes received within the specified period.

Performance

- Remote Address: The IP address of the remote machine from which the bytes are being received.
- Remote Port: The port number of the remote machine from which the bytes are being received.

- Up Since: The date and time from which the connection has been up and running.
- Bytes Received: The number of bytes received per minute.
- Bytes Sent: The number of bytes sent per minute.
- Total Messages Received: The total number of messages received per minute.
- Total Messages Sent: The total number of messages sent per minute.

17.3.4 Service Performance Page

This page displays the performance of the selected service over a specific period of time. The Request Average Duration and the Request Max Duration charts are displayed. You can also see the average metric values over the selected period of time.

17.3.5 Administration Pages

You can drill down to the Administration page for a specific node, cache, connection, or connection manager. You can change configuration for a node, cache, connection, or connection manager. See the Online Help for configuration parameters that can be changed.

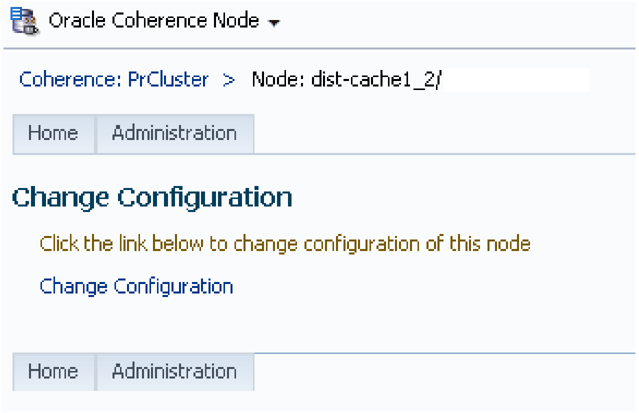
17.4 Log File Monitoring

Enterprise Manager can monitor log files for the occurrence of user specified patterns to check for abnormal conditions. Matching patterns are specified as regular expressions. Log files are periodically scanned for occurrence of one or more patterns and an alert is raised when the pattern occurs during a given scan.

You can set up each Coherence node to log all messages into a log file on the host on which the node is running. You must use a specific naming pattern in the log file name to ensure that it is monitored. To configure the log file monitoring criteria, follow these steps:

1. From the **Targets** menu, select **Middleware**, then click on a Coherence node target.
2. Navigate to the Administration page of the node for which the Log file alerts need to be configured.

Figure 17–9 Node Administration Page



Change Configuration

Click the link below to change configuration of this node

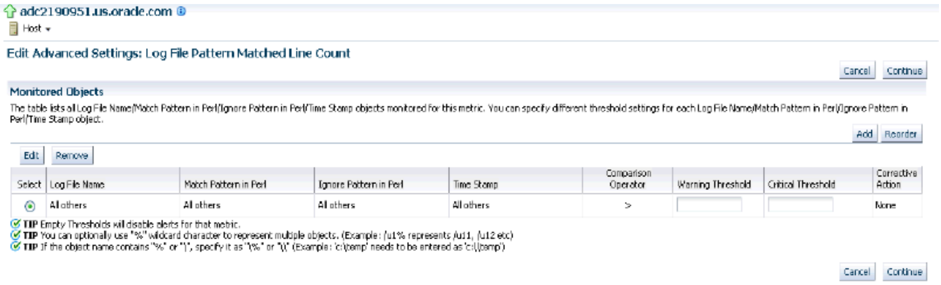
Change Configuration

3. Click the **Log Alert Setup** link. The Metric and Policy Settings page of the host on which the Coherence node is running is displayed.

4. Select **Metric with Thresholds** in the **View** drop-down box and search for the **Log File Pattern Matched Line Count** metric.

5. Click the pencil icon in this row to navigate to the Edit Advanced Settings: Log File Pattern Matched Line Count page.

Figure 17–10 Log File Pattern Matched Line Count Page



Edit Advanced Settings: Log File Pattern Matched Line Count

Monitored Objects

The table lists all Log File Name/Match Pattern in Perl/Ignore Pattern in Perl/Time Stamp objects monitored for this metric. You can specify different threshold settings for each Log File Name/Match Pattern in Perl/Ignore Pattern in Perl/Time Stamp object.

Select	Log File Name	Match Pattern in Perl	Ignore Pattern in Perl	Time Stamp	Comparison Operator	Warning Threshold	Critical Threshold	Corrective Action
●	All others	All others	All others	All others	>			None

✓ TIP Empty Thresholds will disable alerts for that metric.
✓ TIP You can optionally use "%" wildcard character to represent multiple objects. (Example: /u1% represents /u11, /u12 etc)
✓ TIP If the object name contains "%" or "\", specify it as "\%" or "\\" (Example: 'c:\temp' needs to be entered as 'c:\\temp')

6. Click **Add** to add a row to the Monitored Objects table.

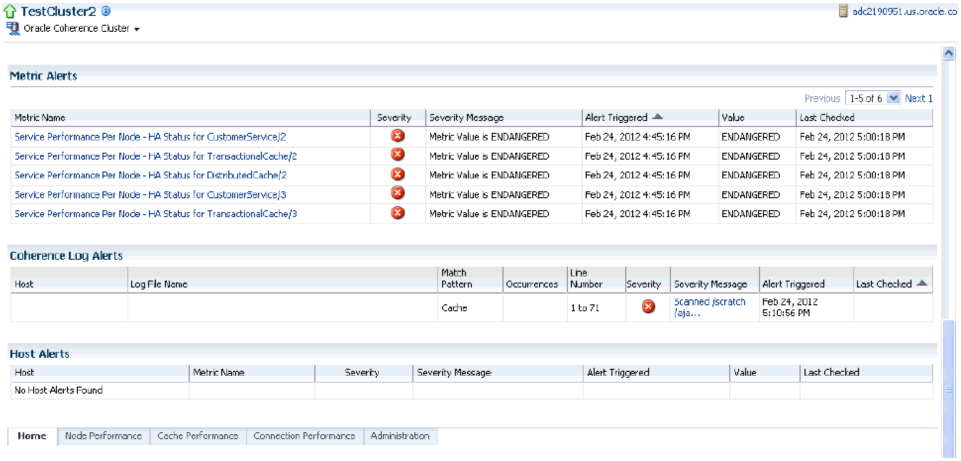
7. In the **Log File Name** field, specify the name in the format `<coherence_cluster_target_name>_<Node_name>_<....any other optional names>.log`. All node log file names must follow this format.

8. Specify the pattern to be matched for or ignored in the **Match Pattern in Perl** and **Ignore Pattern in Perl** fields. Lines matching the *ignore pattern* will be ignored first, then lines matching specified *match patterns* will result in one record being uploaded to the repository for each pattern.

9. Enter the Critical and Warning thresholds for this metric and click Continue. You will return to the Metrics and Collection Settings page. Click **OK** to update the metric.

10. Any alerts generated will be displayed in the Coherence Log Alerts section in the Cluster Home page.

Figure 17–11 Cluster Home Page - Coherence Log Alerts



Metric Alerts

Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
Service Performance Per Node - HA Status for CustomerService/2	☒	Metric Value is ENDANGERED	Feb 24, 2012 4:45:16 PM	ENDANGERED	Feb 24, 2012 5:00:18 PM
Service Performance Per Node - HA Status for TransactionalCache/2	☒	Metric Value is ENDANGERED	Feb 24, 2012 4:45:16 PM	ENDANGERED	Feb 24, 2012 5:00:18 PM
Service Performance Per Node - HA Status for DistributedCache/2	☒	Metric Value is ENDANGERED	Feb 24, 2012 4:45:16 PM	ENDANGERED	Feb 24, 2012 5:00:18 PM
Service Performance Per Node - HA Status for CustomerService/3	☒	Metric Value is ENDANGERED	Feb 24, 2012 4:45:16 PM	ENDANGERED	Feb 24, 2012 5:00:18 PM
Service Performance Per Node - HA Status for TransactionalCache/3	☒	Metric Value is ENDANGERED	Feb 24, 2012 4:45:16 PM	ENDANGERED	Feb 24, 2012 5:00:18 PM

Coherence Log Alerts

Host	Log File Name	Match Pattern	Occurrences	Line Number	Severity	Severity Message	Alert Triggered	Last Checked
		Cache		1 to 71	☒	Scanned /scratch /aja...	Feb 24, 2012 5:10:56 PM	

Host Alerts

Host	Metric Name	Severity	Severity Message	Alert Triggered	Value	Last Checked
No Host Alerts Found						

17.5 Cache Data Management

The Cache Data Management feature allows you to define indexes and perform queries against currently cached data that meets a specified set of criteria.

Note: This feature is available to users with Administration privileges only if the Cache Data Management MBean has been registered in the Coherence JMX management node.

To perform cache data management operations, navigate to the Cache target Administration page and click **Go** in the Cache Data Management section. In the Cache Data Management page, you can select an operation and a query to perform a data management operation on the cache. You can perform the following operations:

- **Add Indexes**: To create an index, select the **Add Index** option in the Operation field. In the Value Extractor List field, specify a comma separated list of expressions that identify the index, and enter the Host Credentials. The Value Extractor is used to extract an attribute from a given object for indexing.
- **Remove Indexes**: To remove an index, select the **Remove Index** option in the Operation field and specify the Value Extractor List that identifies the index. Specify the Host Credentials and click Execute to remove the index from the cache.
- **Export**: You can export the queried data onto a file. Select a query from the Query section or click **Create** to create a new query. Select the **Export** option in the Operation field and enter the absolute path to the file. This file can be saved on the host machine on which the management node is running.
- **Import**: You can import queried data from a file. This file should be present on the host machine on which the management node is running. Select the **Import** option in the operation field and enter the absolute path to the file.
- **Insert**: Select the Insert option in the Operation field and specify an unique (key value) pair. This key value pair will be inserted into the cache and can be provided from:
  - UI Table on this Page: Select the Type of Keys and Type of Values and the Host Credentials.
  - Text File on Management Host: If the queries are stored in a text file, select this option and specify the location of the file.
  - Database Table: If the queries are stored in a database table, specify the Database URL, Credentials, the SQL Query Statement and Properties.
- **Purge**: Select **Purge** from the Operation drop-down list. Data matching the selected query will be deleted from the cache
- **View**: Select **View** from the Operation drop-down list and specify the number of key-value pairs to be displayed on each page. Data matching the criteria will be displayed.
- **Update**: Select **Update** from the Operation drop-down list. Specify the credentials for the host. Select a query from the Query table or create a new query to update the data in the cache.
- **View Explain Plan**: Select **View Explain Plan** from the Operation drop down list. Select a query that is to be evaluated from the Query table. See View Explain page for details.

- **View Trace**: Select **View Trace** from the Operation drop down list. Select a query that is to be evaluated from the Query table. See View Trace page for details.

17.5.1 View Explain Plan

A query explain record provides the estimated cost of evaluating a filter as part of a query operation. The cost takes into account whether or not an index can be used by a filter. The cost evaluation is used to determine the order in which filters are applied when a query is performed. Filters that use an index have the lowest cost and get applied first.

The View Explain Plan option allows you to estimate the cost of evaluating a filter as part of a query operation. When you select this option, a query record containing details of each step in the query is displayed. After viewing the details, click **Execute** to perform the selected operation or **Return** to return to the previous page.

17.5.2 View Trace

The View Trace option allows you to view the actual cost of evaluating a filter as part of a query operation. When you select this option, a query is executed in the cluster and a query record containing details of each step in the query is displayed. After viewing the details, click **Execute** to perform the selected operation or click **Return** to return to the previous page.

17.6 Reap Session Support

HTTPSession Objects for one or more Java EE applications deployed on Application Servers can be cached in the Coherence cluster. These HTTP sessions are cleaned by the Session Reaper and the associated memory is freed up. The Session Reaper is responsible for destroying any sessions that are no longer used, which is determined when the session has timed out. It is configured to scan the entire set of sessions over a certain period of time, called the reaping cycle. The Session Reaper scans for sessions that have expired, and when it finds expired sessions it cleans them up.

To view the reap session metrics, click the **Application** link in the Applications table in the Cluster Home page. The following reap session metrics and graphs are displayed in the Application Home page.

- Reap Duration: This graph shows the average reap duration in minutes.
- Reaped Sessions: This graph shows the average number of reaped sessions in a reap cycle.
- Reaped Sessions (24 Hour Averages): This table shows the average reap session data over the last 24 hours. The following details are displayed:
  - Module Name: The name of the Coherence cluster on which the HTTP sessions have been cached.
  - Node ID: When a node becomes part of a cluster, an ID is automatically assigned to the node. Click on the link to drill down to the Node Home page.
  - Average Reap Duration: The average reap duration since the statistics were last reset.
  - Average Reaped Sessions: The average number of reap sessions since the statistics were last reset.
  - Total Reaped Sessions: The total number of expired sessions that have been reaped since the statistics were last reset.

17.7 Push Replication Pattern

The Push Replication Pattern provides extensible, flexible, high-performance, highly available, and scalable infrastructure to support the replication of EntryOperations occurring in one Coherence Cluster to one or more globally distributed Coherence clusters. The Push Replication Pattern advocates that:

- Operations (such as insert, update and delete) occurring on data in one Site should be pushed using one or more Publishers to an associated device.
- A Publisher is responsible for optimistically replicating operations (in the order in which the said Operations originally occurred) on or with the associated device.
- If a device is unavailable for some reason, the operations to be replicated using the associated Publisher will be queued and executed (in the original order) at a later point in time.

Implementation of the Push Replication Pattern additionally advocates that:

- The data on which operations occur are standard Coherence cache entries.
- Operations replicated include inserts, updates, and deletes of cache entries. This includes NamedCache put and remove, as well as updates that are artifacts of invoking AbstractProcessor.
- The operations that are enqueued for replication are called EntryOperations. They contain key and value pairs of updated cache entries in Binary form.
- A Site is a Coherence Cluster.
- A Site may act as both a sender of Operations and receiver of Operations. That is, multi-way multi-site push replication is permitted.
- A Device may be any of the following; a local cluster, a remote cluster, a file system, a database, an i/o stream, a logging system etc.

After the EntryOperations are captured, they are sent to the messaging layer, for distribution to the Subscribers. The Publishers then publish the currently queued EntryOperations.

The Publisher and Subscriber tables lists all the publishers and subscribers and displays the data used by them. You can Suspend, Drain, or Resume publishing operations on a specific Publisher.

17.8 Transactional Cache Support

Transactional caches are specialized distributed caches that provide transactional guarantees. Transactional caches are required whenever performing a transaction using the Transaction Framework API. Transactional caches cannot interoperate with non-transactional caches.

The CacheMBean managed resource provides attributes and operations for all caches, including transactional caches. Many of the MBeans attributes are not applicable to transactional cache; invoking such attributes simply returns a -1 value. A cluster node may have zero or more instances of cache managed beans for transactional caches. The object name uses the form:

```
type=Cache, service=service name, name=cache name, nodeId=cluster node's
id
```

The following list describes the CacheMBean attributes that are supported for transactional caches.

- AverageGetMillis: The average number of milliseconds per get() invocation.
- AveragePutMillis: The average number of milliseconds per put() invocation since the cache statistics were last reset.
- HighUnits: The limit of the cache size measured in units. The cache will prune itself automatically once it reaches its maximum unit level. This is often referred to as the high water mark of the cache.
- Size: The number of entries in the current data set.
- TotalGets: The total number of get() operations since the cache statistics were last reset.
- TotalGetsMillis: The total number of milliseconds spent on get() operations since the cache statistics were last reset.
- TotalPuts: The total number of put() operations since the cache statistics were last reset.
- TotalPutsMillis: The total number of milliseconds spent on put() operations since the cache statistics were last reset.

17.9 Integration with JVM Diagnostics

JVM Diagnostics allows administrators to identify the root cause of performance problems in the production environment without having to reproduce them in the test or development environment. JVM Diagnostics is a part of WLS Management Pack EE.

You can drill down to a Coherence node's JVM to identify the method or thread that is causing a delay. This feature allows you to trace live threads, identify resource contention related to locks, and trace the Java session to the database.

You can view the JVM Diagnostics data if the JVM Diagnostics Manager and JVM Diagnostics Agent have been deployed on the host machine on which the OMS running. You can deploy the JVM Diagnostics Manager and JVM Diagnostics Agent on:

- Standalone Coherence
- CoherenceWeb

To setup JVM Diagnostics on each Coherence node you need to download the JVM Diagnostics Agent. For more details, see *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide.*

17.10 Viewing Performance Summary

You can use the Performance Summary page to monitor the performance of the cluster, a node, or a cache. From the **Oracle Coherence Cluster** (Node or Cache) menu, select **Monitoring**, then select **Performance Summary**.

A set of default performance charts that shows the values of specific performance metrics over time are displayed. You can customize these charts to help you isolate potential performance issues. You can also view a series of regions specific to the cluster, node, or cache target. For more details, see the Performance Summary Online Help.

17.11 Viewing Configuration Topology

The Configuration Topology Viewer provides a visual layout of the relationship of the Coherence target with other targets. From the **Oracle Coherence Cluster** (Node or Cache) menu, select **Configuration**, then select **Topology**. A topology graph for the Coherence target is displayed. You can determine the source of its health problem and its impact on other targets. You can also view the members of the cluster and its relationships. For more details, see the Configuration Topology Viewer Online Help.

17.12 Troubleshooting Coherence

If you cannot collect metric data for any of the Coherence targets, check the following to ensure that the steps involved in discovering the target have been followed correctly.

- Make sure that the management node has been successfully started and the host on which the management node is running is accessible from the Agent host.
- Specify the appropriate User Name and Password if password authentication is enabled.
- If you are not using SSL to start the management node, make sure that you have started the JVM using the `com.sun.management.jmxremote.ssl=false` option.
- If you did not use the bulk operation MBean JAR to start the management node, you must leave the Bulk Operations Mbean field blank during discovery.

17.13 Best Practices

In this section, you can see some sample code snippets that show you how to use the JVM Diagnostics to start a management node or a storage enabled node.

You must ensure that:

- The Management Agent has been deployed on every machine on which the Coherence node is running.
- Garbage Collection has been enabled on the nodes.
- Heap utilization on the node does not exceed 70%.
- The Discover Corrective Action must be set up on the new nodes and caches.
- The caches must be preconfigured on the node to ensure that Enterprise Manager can easily establish associations during discovery.
- Reusable monitoring templates that can be applied on multiple targets must have been created.
- The node has been refreshed after it has been restarted. To refresh the node, from the **Coherence Cluster** menu, select **Configuration**, then select **Last Collected**. In the Latest Configuration page, from the **Actions** menu, select **Refresh** to refresh the node.

Example 17–1 Starting a Management Node

```
JVMD_HOST=<Host_Where_JVMD_Manager_Is_Running>
JVMD_PORT=<Port_of_the_JVMD_Manager>
JVMD_POOL=Contacts
JAM_PARAMS=" jamagent.jamrun jamconshost=$JVMD_HOST jamconsport=$JVMD_PORT
jampool=$JVMD_POOL"
CP=$CP:<path_where_JAMAgent_is_copied>/jamagent.war:
```

```
<OEM_Agent_Home>/plugins/oracle.sysman.emas.agent.plugin_
12.1.0.3.0/archives/coherence/coherenceEMIntg.jar:
<OEM_Agent_Home>/plugins/oracle.sysman.emas.agent.plugin_
12.1.0.3.0/archives/coherence/bulkoperationsmbean.jar
CACHE_CONFIG=$CONFIG_DIR/$CACHE_CONFIG_FILE_NAME
POF_CONFIG=$CONFIG_DIR/$POF_CONFIG_FILE_NAME
COH_OPTS="$COH_OPTS -cp $CP"
COH_OPTS="$COH_OPTS -Dtangosol.coherence.cacheconfig=$CACHE_CONFIG"
COH_OPTS="$COH_OPTS -Dtangosol.pof.config=$POF_CONFIG"
# using non-default port to prevent accidentally joining other clusters
COH_OPTS="$COH_OPTS -Dtangosol.coherence.clusterport=<open_port>"
$JAVA_HOME/bin/java $COH_OPTS
-Dtangosol.coherence.management.remote=true
-Dcom.sun.management.jmxremote.authenticate=false
-Dtangosol.coherence.management=all
-Dcom.sun.management.jmxremote.ssl=false
-Dtangosol.coherence.cluster=Contacts
-Dtangosol.coherence.member=MNode1
-Dtangosol.coherence.site=MSite
-Dtangosol.coherence.rack=MRack
-Dtangosol.coherence.machine=<FullyQualifiedHostName_of_localhost>
-Doracle.coherence.machine=<FullyQualifiedHostName_of_localhost>
-Dcom.sun.management.jmxremote.port=<OpenTCP_Port>
-Dtangosol.coherence.distributed.localstorage=false
-Doracle.coherence.jamjvmid=Contacts/MNode1
-server
-Xms2048m -Xmx2048m
$JAM_PARAMS
jamjvmid=Contacts/MNode1
oracle.sysman.integration.coherence.EMIntegrationServer $*
```

where:

- The string specified in the `JVMD_POOL` and `-Dtangosol.coherence.cluster` should match. This is used to correlate the Coherence Cluster target and the JVM Pool.
- The `Dtangosol.coherence.member` name must be unique. This name is required for JVM Diagnostics integration.
- The JVM Diagnostics integration parameters are:
  - `-Doracle.coherence.jamjvmid` - <JVM_pool_name>/<member_name>
  - `Jamjvmid` - <JVM_pool_name>/<member_name>

Example 17–2 Starting a Storage Node

```
JVMD_HOST=<Host_Where_JVMD_Manager_Is_Running>
JVMD_PORT=<Port_of_the_JVMD_Manager>
JVMD_POOL=Contacts
JAM_PARAMS=" jamagent.jamrun jamconshost=$JVMD_HOST jamconsport=$JVMD_PORT
jampool=$JVMD_POOL"
CP=$CP:<path_where_JAMAgent_is_copied>/jamagent.war
CACHE_CONFIG=$CONFIG_DIR/$CACHE_CONFIG_FILE_NAME
POF_CONFIG=$CONFIG_DIR/$POF_CONFIG_FILE_NAME
COH_OPTS="$COH_OPTS -cp $CP"
COH_OPTS="$COH_OPTS -Dtangosol.coherence.cacheconfig=$CACHE_CONFIG"
COH_OPTS="$COH_OPTS -Dtangosol.pof.config=$POF_CONFIG"

# using non-default port to prevent accidentally joining other clusters
COH_OPTS="$COH_OPTS -Dtangosol.coherence.clusterport=<cluster_port>"
$JAVA_HOME/bin/java $COH_OPTS
```

```
-Dtangosol.coherence.cluster=Contacts
-Dtangosol.coherence.member=SNode1
-Dtangosol.coherence.management.remote=true
-Dcom.sun.management.jmxremote.authenticate=false
-Dcom.sun.management.jmxremote.ssl=false
-Dtangosol.coherence.machine=<FullyQualifiedHostName_of_localhost>
-Doracle.coherence.machine=<FullyQualifiedHostName_of_localhost>
-Dtangosol.coherence.log.level=5
-Dtangosol.coherence.log=<path_log_file>
-Doracle.coherence.jamjvmid=Contacts/SNode1
-server -Xms2048m -Xmx2048m
$JAM_PARAMS
jamjvmid=Contacts/SNode1
com.tangosol.net.DefaultCacheServer $*
```

Part VIII

Using Identity Management

The chapters in this part provide a brief introduction to the Management Pack Plus for Identity Management. It guides you through the process of discovering and configuring Oracle Identity Management targets and discusses key features in the Management Pack Plus for Identity Management.

The chapters are:

18

Getting Started with Identity Management

As more and more businesses rely on the Oracle Identity and Access Management Suite to control access to their mission-critical applications (both packaged applications and custom-built web applications) and to provision resources across their organizations, the need to achieve predictable performance and availability for Oracle Identity Management systems has become a top priority for many businesses. An outage or slow performance in access and identity services, for instance, can have negative impacts on the business bottom-line as end-users are unable to log in to mission-critical applications.

To help you maximize the value of Oracle Identity Management systems, and to deliver a superior ownership experience while restraining the systems management costs, Oracle provides Oracle Management Pack Plus for Identity Management (the Identity Management Pack), which leverages the Oracle Enterprise Manager Cloud Control advanced management capabilities, to provide an integrated and top-down solution for your Oracle Identity Management environment.

18.1 Benefits of the Using Identity Management Pack

The benefits of using Identity Management Pack include:

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

18.2 Features of the Identity Management Pack

The features in the Identity Management Pack include:

- Enterprise-Wide View of Oracle Identity Management

  - The "Identity and Access" dashboard provides a centralized view of all Oracle Identity Management components - including Identity Management 10*g* and Identity Management 11*g* components.
  - From the "Identity and Access" dashboard, users can view the performance summary of the associated systems and services based on the underlying dependencies and monitor the overall health of the Identity Management environment.

- Performance Management
  - A wide range of out-of-box performance metrics to find root causes of problems that could potentially slow performance, extend response times, or create outages
  - Customizable performance summaries with a "Metric Palette" that allows users to drag and drop performance charts
- Configuration Management
  - Perform key configuration management tasks like keeping track of configuration changes for diagnostic and regulatory purposes, taking snapshots to store configurations, and comparing component configurations to ensure consistency of configurations within the same environment or across different environments.

18.2.1 New Features for this Release

New features for Identify Management Pack include:

- Performance Management
  - Out-of-box reports for Oracle Internet Directory, Oracle Access Manager, and Oracle Identity Manager
  - Oracle Identity Manager database performance page to analyze the performance of the underlying Oracle Identity Manager database in the context of the OIM-specific tables and user. **Note:** The database target will need to be discovered to take advantage of all the features on the database performance page.
- Configuration Management

  Automated compliance monitoring and change detection for Oracle Identity Manager is now available to help customers meet compliance and reporting requirements.

  To enable the compliance standard association with the Oracle Identity Manager Cluster target. Perform the following steps:

  1. Click the Oracle Identity Manager Cluster target. From the **Target** menu, select **Compliance**, then select **Standard Associations**.
  2. Click **Edit Association Settings**. Click **Add** and then select **Oracle Identity Manager Cluster Configuration Compliance**.
  3. Click **OK** and then **OK** again to enable the new association setting.

18.3 Monitoring Oracle Identity Management Components in Enterprise Manager

You can use Enterprise Manager to monitor the following Identity Management 11*g* components (Table 18–1).

Table 18–1 Licensed Targets for Identity Management 11g Targets

Enterprise Manager Target Type	Purpose
Oracle Adaptive Access Manager Oracle Access Manager Oracle Directory Integration Platform Oracle Identity Federation Oracle Identity Manager Oracle Internet Directory Oracle Virtual Directory	Each component will be presented as a target in Enterprise Manager which provides an interface with access to target overview, customizable performance summary, process control, configuration management, compliance analysis, and Information Publisher reports. For all the Oracle Adaptive Access Managers, Oracle Access Managers, and Oracle Identity Managers that are deployed within the same WebLogic domain, a cluster target will be created for each component: ▪ Oracle Adaptive Access Manager Cluster ▪ Oracle Access Manager Cluster ▪ Oracle Identity Manager Cluster Each cluster target is a logically related group of components that are managed as a unit. Every target is part of a WebLogic domain.
Oracle Directory Server Enterprise Edition	The following types of targets will be created for each Oracle Directory Server Enterprise Edition deployment: ▪ Oracle Directory Server Enterprise Edition Server A target represents the LDAP service and all internal resources ▪ Directory Server Group User logical grouping of Oracle Directory Server Enterprise Edition Servers ▪ Directory Server Enterprise A set of Oracle Directory Server Enterprise Edition Servers connected through a network that participates in the service, including Directory Server Groups. Each target provides an interface in Enterprise Manager with access to target overview, customizable performance summary, process control, and configuration management.

The following Identity Management 10*g* components can be monitored by Enterprise Manager (Table 18–2).

Table 18–2 Licensed Targets for Identity Management 10g Targets

Enterprise Manager Target Type	Purpose
Oracle Delegated Administration Server Oracle Directory Integration Platform Oracle Internet Directory Oracle Single Sign-On	Each component will be presented as a target in Enterprise Manager which provides an interface with access to target overview and performance summary

Table 18–2 (Cont.) Licensed Targets for Identity Management 10g Targets

Enterprise Manager Target Type	Purpose
Oracle Access Manager - Access Server Oracle Access Manager - Identity Server Oracle Identity Federation	Each component will be presented as a target in Enterprise Manager which provides an interface with access to target overview and performance summary. A system target will be created for each component to provide end-to-end system oriented view of the component: ■ Access Manager - Access System ■ Access Manager - Identity System ■ Identity Federation System The underlying LDAP servers, database instances and hosts will be monitored within the system.
Oracle Identity Manager	The following types of targets will be created for each Oracle Identity Manager: ■ Identity Manager Server A target represents the server tier of Oracle Identity Manager ■ Identity Manager Repository A target represents the data and enterprise integration tier of Oracle Identity Manager A system target will be created for Oracle Identity Manager to provide an end-to-end system oriented view of the component. ■ Identity Manager System The underlying LDAP servers, database instances, and hosts will be monitored within the system.

The monitored targets in the Identity Management pack associated with both release 10*g* and release 11*g* are summarized in Table 18–3.

Table 18–3 Targets Associated with Both Identity Management 10g and Identity Management 11g Targets

Enterprise Manager Target Type	Purpose
Generic 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, Identity Manager System, and Identity and Access 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.
Host	Representation of hosts running Oracle Identity Management components providing access to metrics, alerts, performance charts, remote file editor, log file alerts, user-defined metrics, host commands and customized reports.

Table 18–3 (Cont.) Targets Associated with Both Identity Management 10g and Identity Management 11g

Enterprise Manager Target Type	Purpose
Oracle Database	Representation of Oracle Database that is used by Oracle Identity Management components providing access to metrics, alerts, performance charts, compliance summary, and configuration management.
Oracle Identity and Access System	System target that can be modeled with any discovered Oracle Identity Management target (including both Identity Management 10*g* and Identity Management 11*g* targets) and the underlying hosts and databases as the key components providing an end-to-end system oriented view of the monitored Identity Management environment. The Identity and Access System target provides access to member status, metrics, charts, incidents, and topology view.
Oracle SOA Suite	Representation of Oracle SOA Suite that is used by Oracle Identity Manager 11*g* providing access to metrics, alerts, performance charts, and configuration management of the SOA infrastructure instance and its service engines.

19 Prerequisites for Discovering Identity Management Targets

This chapter lists the system requirements and prerequisites needed to discover identity management targets.

19.1 System Requirements

Table 19–1 lists the supported Oracle Identity Management products in the Management Pack Plus for Identity Management in Enterprise Manager Cloud Control 12*c* Release 2 (12.1.0.2). Please check the Enterprise Manager certification matrix on My Oracle Support (`http://support.oracle.com`) for the most up-to-date list of supported platforms.

Table 19–1 Supported Identity Management Products and Platforms in Enterprise Manager Cloud Control Release 2 (11.1.0.2)

Product	Version	Application Server	Directory Server/Database
Oracle Access Manager	10.1.4.2; 10.1.4.3.0	Not Applicable	Oracle Internet Directory 10.1.4.x; Microsoft Active Directory
Oracle Access Manager	11.1.1.3.0; 11.1.1.5.0	Oracle WebLogic Server 10.3	Oracle Database
Oracle Adaptive Access Manager	11.1.1.3.0; 11.1.1.5.0	Oracle WebLogic Server 10.3	Oracle Database
Oracle Directory Integration Platform	11.1.1.2.0; 11.1.1.5.0	Oracle WebLogic Server 10.3	Oracle Database

Oracle Directory Server Enterprise Edition	6.x; 7.x;
	11.1.1.3.0;
	11.1.1.5.0
		Not Applicable	Not Applicable

Oracle Identity Federation	10.1.4.2; 10.1.4.3.0	Oracle Application Server	Oracle Internet Directory 10.1.4.x
Oracle Identity Federation	11.1.1.2.0; 11.1.1.5.0	Oracle WebLogic Server 10.3	Oracle Internet Directory 11.1.1.2.0; 11.1.1.3.0; 11.1.1.6
Oracle Identity Management Suite - Delegated Administration Services	10.1.4.2; 10.1.4.3.0	Oracle Application Server 10*g*	Oracle Database
Oracle Identity Management Suite - Directory Integration Platform	10.1.4.2; 10.1.4.3.0	Oracle Application Server 10*g*	Oracle Database

Table 19–1 (Cont.) Supported Identity Management Products and Platforms in Enterprise Manager Cloud Control Release 2 (11.1.0.2)

Product	Version	Application Server	Directory Server/Database
Oracle Identity Management Suite - Oracle Internet Directory	10.1.4.2; 10.1.4.3.0	Oracle Application Server 10*g*	Oracle Database
Oracle Identity Management Suite - Single Sign-On Server	10.1.4.2; 10.1.4.3.0	Oracle Application Server 10*g*	Oracle Database
Oracle Identity Manager	9.1.0.1	Oracle WebLogic Server 10.3; JBoss Application Server	Oracle Database
Oracle Identity Manager	11.1.1.3.0; 11.1.1.5.0	Oracle WebLogic Server 10.3; Oracle SOA Suite 11.1.1.3.0	Oracle Database

Oracle Internet Directory	11.1.1.2.0;
	11.1.1.3.0;
	11.1.1.4.0;
	11.1.1.5.0;
	11.1.1.6.0
		Oracle WebLogic Server 10.3	Oracle Database

Oracle Virtual Directory	11.1.1.2.0;
	11.1.1.3.0;
	11.1.1.4.0;
	11.1.1.5.0;
	11.1.1.6.0
		Oracle WebLogic Server 10.3	Not Applicable

19.2 Installing Oracle Enterprise Manager Cloud Control 12*c* Release 2

Before you begin configuring Cloud Control 12*c* Release 2 to manage your Identity Management components, you must install and configure Cloud Control 12*c* Release 2 on at least one host computer on your network. Oracle recommends that you install Cloud Control on dedicated host(s).

For example, if the Identity Management components are installed on host1.us.oracle.com, then install and configure the Oracle Management Service and Oracle Management Repository on host2.us.oracle.com. Install the Cloud Control 12*c* Management Agent on every host that includes the components you want to manage with Cloud Control.

See Also:

Oracle Enterprise Manager Cloud Control Basic Installation Guide

All documentation files can be accessed on the Oracle OTN website: `http://docs.oracle.com/cd/E24628_01/nav/portal_booklist.htm`

19.3 Prerequisites for Discovering Identity Management Targets in Enterprise Manager

Before you start monitoring Oracle Identity Management targets in Enterprise Manager, you must perform the following tasks:

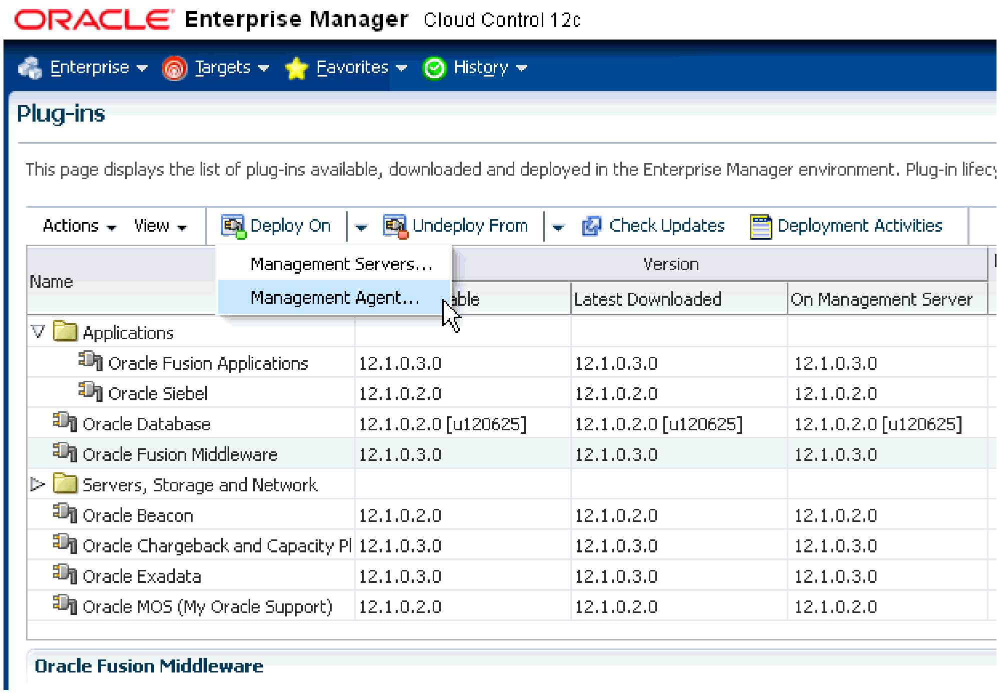
- Install Cloud Control 12*c* Agent on each of the hosts that run Oracle Identity Management components.

  If you would like to monitor additional targets, such as Oracle Application Server, Oracle WebLogic Server, JBoss Application Server, MS Active Directory, MS IIS and databases supporting Oracle Identity Management, and you have the proper license for monitoring these targets, then install Cloud Control 12*c* Management Agent on these hosts as well.

- Deploy the "Oracle Fusion Middleware" plug-in on the agents running on the hosts for Oracle Identity Management.

  1. Log in to Enterprise Manager. Navigate to **Setup**, select **Extensibility**, then select **Plugins**.
  2. Select Oracle Fusion Middleware plug-in and ensure that it has been deployed on the agents running on the hosts for Oracle Identity Management. See Figure 19–1.

Figure 19–1 Plug-Ins Deploy On Options



This page displays the list of plug-ins available, downloaded and deployed in the Enterprise Manager environment. Plug-in lifecy

Name	Version able	 Latest Downloaded	 On Management Server
▽ Applications			
Oracle Fusion Applications	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0
Oracle Siebel	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0
Oracle Database	12.1.0.2.0 [u120625]	12.1.0.2.0 [u120625]	12.1.0.2.0 [u120625]
Oracle Fusion Middleware	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0
▷ Servers, Storage and Network			
Oracle Beacon	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0
Oracle Chargeback and Capacity Pl	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0
Oracle Exadata	12.1.0.3.0	12.1.0.3.0	12.1.0.3.0
Oracle MOS (My Oracle Support)	12.1.0.2.0	12.1.0.2.0	12.1.0.2.0

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

  Oracle Access Manager 10.1.4.2, 10.1.4.3.0

  1. Install Oracle Access Manager SNMP Agent on each of the hosts where the Oracle Access Manager Access Server and Identity Server are running. The SNMP Agent collects performance metrics and configuration parameters for the Oracle Access Manager Access Server and Identity Server allowing you to monitor the various Oracle Access Manager components through Enterprise Manager Cloud Control. Refer to the *Oracle Access Manager Installation Guide* for instructions on installing the SNMP Agent (`http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/snmp.htm#CHDFBJJC`).
  2. Configure the SNMP Agent and specify the Management Agent's UDP and TCP Ports as well as the SNMP Agent Community Name. Make sure that you record the SNMP Agent UDP Port and Community Name; because these details will be needed in the discovery process. Refer to the *Oracle Access Manager Installation Guide* for instructions on configuring the SNMP Agent

(http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/snmp.htm#CEGEIIFI).

Also, refer to the *Oracle Access Manager Identity and Common Administration Guide* for instructions on setting up the SNMP Agent (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25343/snmpmntr.htm#CEGHHDBC).

3. Enable SNMP monitoring for both the Oracle Access Manager Access Server and Oracle Access Manager Identity Server by completing the following tasks:

   – From the Identity (or Access) System Console, select System Configuration, Identity Server (or Access Server).

   – Click a link for a particular server.

   – Click **Modify** to display the page where you can turn SNMP monitoring on or off. Click the **SNMP State On** button at the bottom of the page to turn on the collection of SNMP statistics.

   – In the SNMP Agent Registration Port field, enter the **port number** to define or change the port on which the SNMP Agent listens.

   – Restart the Identity Server (or Access Server).

   Refer the *Oracle Access Manager Identity and Common Administration Guide* for instructions on setting up the SNMP Agent (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25343/snmpmntr.htm#BABFFDDA).

4. Complete all the configuration steps for the Oracle Access Manager Identity Server and Oracle Access Manager Access Server. Ensure that the communication details and the directory server details are defined so that Enterprise Manager can discover the topology of your Oracle Access Manager environment.

   Refer to the *Oracle Access Manager Installation Guide* for instructions on configuring the Identity Server (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/id_setup.htm#CHDHIBIB) and the *Access Server* (http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25353/a_srvr.htm#BGBEFBBD).

5. If you plan to monitor the directory server through Oracle Enterprise Manager Cloud Control, then ensure that the directory server is appropriately discovered in Enterprise Manger before moving on to the discovery of Oracle Access Manager Identity Server and Oracle Access Manager Access Server. Complete the following tasks to discover the supported directory servers:

   – Oracle Internet Directory 10.1.4

     Discovery of Oracle Identity Management Suite 10*g* (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server) can be done using the discovery wizard on the Middleware page. From the Middleware page, select **Oracle Application Server** from the **Add** menu. For more information, refer to the Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0 section.

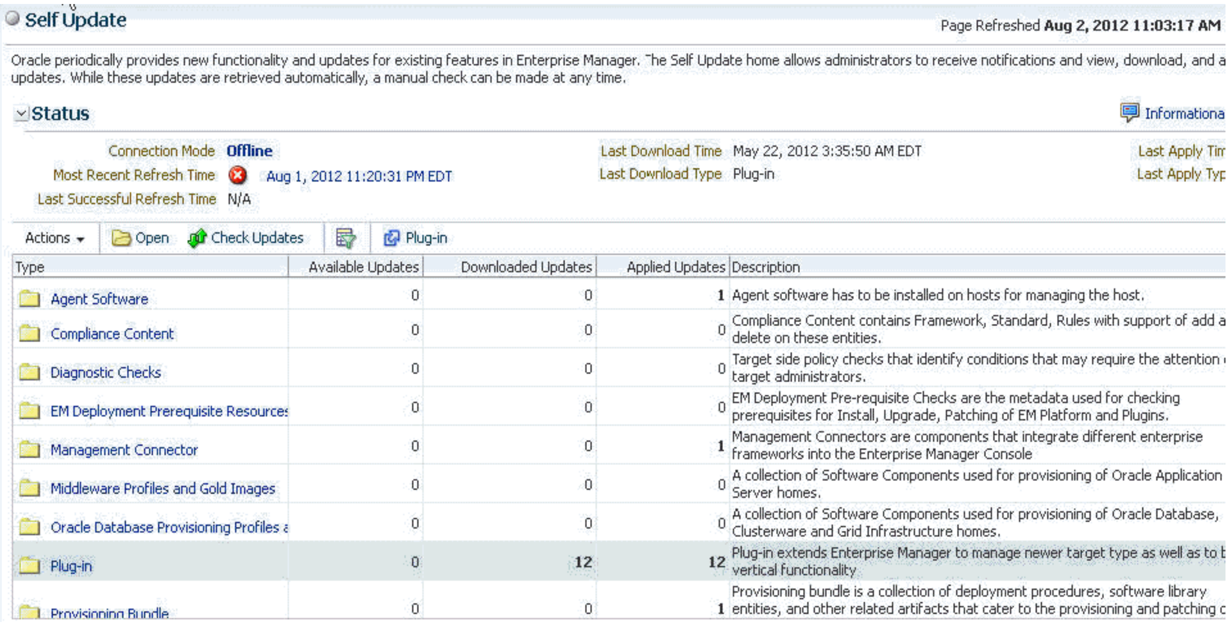
   – Self Update

     Use the Self Update option in Enterprise Manager to get the plug-in.

1) From the **Setup** menu, select **Extensibility**, then select **Self Update**.

2) Click **Plug-in** and select the available plug-in for Microsoft Active Directory or other non-Oracle products that need to be monitored. See Figure 19–2.

Figure 19–2 Self Update Screen



Self Update

Page Refreshed **Aug 2, 2012 11:03:17 AM**

Oracle periodically provides new functionality and updates for existing features in Enterprise Manager. "he Self Update home allows administrators to receive notifications and view, download, and a updates. While these updates are retrieved automatically, a manual check can be made at any time.

Status

Connection Mode **Offline**
Most Recent Refresh Time ☒ Aug 1, 2012 11:20:31 PM EDT
Last Successful Refresh Time N/A

Last Download Time May 22, 2012 3:35:50 AM EDT
Last Download Type Plug-in

Type	Available Updates	Downloaded Updates	Applied Updates	Description
Agent Software	0	0	1	Agent software has to be installed on hosts for managing the host.
Compliance Content	0	0	0	Compliance Content contains Framework, Standard, Rules with support of add a delete on these entities.
Diagnostic Checks	0	0	0	Target side policy checks that identify conditions that may require the attention target administrators.
EM Deployment Prerequisite Resources	0	0	0	EM Deployment Pre-requisite Checks are the metadata used for checking prerequisites for Install, Upgrade, Patching of EM Platform and Plugins.
Management Connector	0	0	1	Management Connectors are components that integrate different enterprise frameworks into the Enterprise Manager Console
Middleware Profiles and Gold Images	0	0	0	A collection of Software Components used for provisioning of Oracle Application Server homes.
Oracle Database Provisioning Profiles a	0	0	0	A collection of Software Components used for provisioning of Oracle Database, Clusterware and Grid Infrastructure homes.
Plug-in	0	12	12	Plug-in extends Enterprise Manager to manage newer target type as well as to b vertical functionality
Provisioning Bundle	0	0	1	Provisioning bundle is a collection of deployment procedures, software library entities, and other related artifacts that cater to the provisioning and patching c

Oracle Identity Federation 10.1.4.2, 10.1.4.3.0

1. Complete all the configuration steps for the Oracle Identity Federation. Ensure that the Federation Data Store details and User Data Store details are defined so that Enterprise Manager can discover the topology of your Oracle Identity Federation environment.

   Refer to the *Oracle Identity Federation Administrator's Guide* for instructions on configuring the Identity Federation (`http://download.oracle.com/docs/cd/B28196_01/idmanage.1014/b25355/configuring.htm#BCGDGAAJ`).

2. Discover the Oracle Application Server on which Oracle Identity Federation is deployed in Enterprise Manager Cloud Control. Complete the following steps to discover Oracle Application Server in Cloud Control:

   – Log in to Enterprise Manager. Select **Target**, then select **Middleware**.

   – From the **Add** menu, select Oracle Application Server.

   – Enter the information requested for Oracle Application Server. Click **Next** once all the information requested is entered.

3. If you plan to monitor the directory server through Oracle Enterprise Manager Cloud Control, then ensure that the directory server is appropriately discovered in Enterprise Manger before moving on to the discovery of Oracle Identity Federation Server. Complete the following tasks to discover the supported directory servers:

   – Oracle Internet Directory 10.1.4

Discovery of Oracle Identity Management Suite 10*g* (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server) can be done using the discovery wizard on the Middleware page.

From the Middleware page, select **Oracle Application Server** from the **Add** menu. For more information, refer to the Discovering Oracle Identity Management Suite 10.1.4.2, 10.1.4.3.0 section.

4. If Oracle Database is used for the User Data Store, ensure that the database instance is discovered in Enterprise Manager Cloud Control before moving on to the discovery Oracle Identity Federation Server. Complete the following steps to discover Oracle Database Instance in Cloud Control:

   - Log in to Enterprise Manager. Select **Targets**, then select **Databases**.
   - Select **Add** from the Search List view.
   - Enter the information requested for the Database Instance. Click **Next** once all the information requested is entered.

Oracle Identity Manager 9.1.0.1

1. Complete all the configuration steps for Oracle Identity Manager. Ensure that the application server and database are appropriately set up and configured for Oracle Identity Manager.

   Refer to the *Oracle Identity Manager Installation and Upgrade Guide* for instructions on configuring Oracle Identity Manager (`http://download.oracle.com/docs/cd/B31081_01/index.htm`).

2. Discover the application server on which Oracle Identity Manager is deployed in Enterprise Manager Cloud Control.

   > **Note:** To verify whether the version of your third-party software for Oracle Identity Manager is supported in Oracle Enterprise Manager Cloud Control release 12.1.0.2, refer to the certification matrix located on My Oracle Support (`https://support.oracle.com`).

   Complete the following steps to discover the supported application servers:

   - JBoss Application Server Version 4.0.2:

     Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

     From the **Add** menu, select **JBoss Application Server**.

     Enter the information requested for the JBoss Application Server. Click **Next** once all the information requested is entered.

   - Oracle WebLogic Application Server Version 7.x and 8.x:

     Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

     From the **Add** menu, select **Oracle WebLogic Domain 7.x and 8.x**.

     Enter the information requested for the WebLogic Application Server. Click **Next** once all information requested is entered.

   - Oracle WebLogic Application Server Version 10.x and later:

     Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

From the **Add** menu, select **Oracle Fusion Middleware/WebLogic Domain**.

Enter the information requested for WebLogic Domain. Click **Continue** once all information requested is entered

– WebSphere Application Server:

  Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

  From the **Add** menu, select **IBM WebSphere Application Server**.

  Enter the information requested for the WebSphere Application Server. Click Next once all information requested is entered.

3. If Oracle Database is used for Oracle Identity Manager, ensure that the database instance is discovered in Enterprise Manager Cloud Control before moving on to the discovery Oracle Identity Manager Server.

   Complete the following steps to discover Oracle Database Instance in Cloud Control:

   Log in to Enterprise Manager. Select **Targets**, then select **Database**.

   Select **Add** from the Search List view.

   Enter the information requested for the Database Instance. Click **Next** once all information requested is entered.

20

Discovering and Configuring Identity Management Targets

This chapter provides the information needed to discover and configure Identity Management targets.

20.1 Discovering Identity Management Targets

This section describes how to discover Identity Management targets.

20.1.1 Discovering Oracle Access Manager Access Server 10.1.4.2 and 10.1.4.3.0

Enterprise Manager has a simple Discovery wizard for Oracle Access Manager 10*g* targets. The Discovery wizard collects details about Oracle Access Manager Targets including information about the host name, host login credentials, SNMP Agent credentials, and other details.

After the Discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into the Management Repository.

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

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.
2. From the **Add** menu, select **Oracle Identity Management 10g (OAM, OIF, OIM).**
3. Select **Access Manager - Access Server** and enter the host name on which your Access Server is running. Click **OK** to continue with the discovery of the Access Server.
4. Enter the information requested for Access Server. (The following table provides descriptions of the fields.) Click **Next** once all information requested is entered.

Field	Description
Host User Name	User name on the operating system with administrator privileges.
Host User Password	Password of host administrator account. ■ Save as Preferred Credentials. Select this check box if you would like to save the user name/password for the administrator account. ■ Management Agent is running on Host other than SNMP Host Select this check box if your Cloud Control Management Agent is running on a host other than the SNMP Agent host.

Field	Description
Access Server Home	Enter the home directory of your Access Server (<OAM_ HOME>\access) - for example, C:\Program Files\OracleAccessManager\access
Access Server Version	Enter the version of your Oracle Access Manager - Access Server - for example, 10.1.4.0.1
SNMP Agent Host	If your Simple Network Management Protocol (SNMP) Agent is running on a host other than the Cloud Control Management Agent host, then enter the SNMP Agent host name. Otherwise, skip this section.
SNMP Agent Port	Enter the UDP Port of the SNMP Agent - for example, 161
SNMP Agent Community Name	Enter the community name of the SNMP Agent.
LDAP Server Host	Name of the Lightweight Directory Access Protocol (LDAP) host. The host name is available in the LDAPSERVERNAME parameter located in the <AccessServerInstallDir>/config/ldap/ConfigDB.xml file.
LDAP Server Port	Name of the LDAP port. The port name is available in the LDAPSERVERPORT parameter located in the <AccessServerInstallDir>/config/ldap/ConfigDB.xml file.
LDAP User Name	Name of the LDAP user. The user name is available in the LDAPROOTDN parameter located in the <AccessServerInstallDir>/config/ldap/ConfigDB.xml file.
LDAP Password	Password for the LDAP user.
LDAP Base	Name of the LDAP base. The base name is available in the LDAPOBLIXBASE parameter located in the <AccessServerInstallDir>/config/configInfo.xml file.

5. Enterprise Manager discovers the topology of your Oracle Access Manager - Access Server deployment including the associated databases and directory servers.

   To add this topology into an existing Access Manager - Access System target, select **Use the specified system**, and select an existing target of type Access Manager - Access System.

   If you want to create a new Access Manager - Access System target, select the **Create a new system** and enter the name of the new system target. Click **Finish** to complete the discovery.

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

20.1.2 Discovering Oracle Access Manager Identity Server 10.1.4.2 and 10.1.4.3.0

Enterprise Manager has a simple Discovery wizard for Oracle Access Manager 10*g* targets. The Discovery wizard collects details about Oracle Access Manager Targets including information about the host name, host login credentials, SNMP Agent credentials, and other details.

After the Discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Management Repository.

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

2. From the **Add** menu, select **Oracle Identity Management 10g (OAM, OIF, OIM).**
3. Select **Access Manager - Identity Server** and enter the host name on which your Identity Server is running. Click **OK** to continue with the discovery of the Identity Server.
4. Enter the information requested for Oracle Access Manager - Identity Server. (The following table describes the fields.) Click **Next** once all information requested is entered.

Field	Description
Host User Name	User name on the operating system with administrator privileges.
Host User Password	Password of host administrator account. ■ Save as Preferred Credentials. Select this check box if you would like to save the user name/password for the administrator account. ■ Management Agent is running on Host other than SNMP Host Select this check box if your Cloud Control Management Agent is running on a host other than the SNMP Agent host.
Identity Server Home	Enter the home directory of your Identity Server (<OAM_HOME>\identity) - for example, C:\Program Files\OracleAccessManager\identity
Identity Server Version	Enter the version of your Oracle Access Manager - Identity Server - for example, 10.1.4.0.1
SNMP Agent Host	If your Simple Network Management Protocol (SNMP) Agent is running on a host other than the Cloud Control Management Agent host, then enter the SNMP Agent host name. Otherwise, skip this section.
SNMP Agent Port	Enter the UDP Port of the SNMP Agent - for example, 161
SNMP Agent Community Name	Enter the community name of the SNMP Agent.

5. Enterprise Manager discovers the topology of your Oracle Access Manager - Identity Server deployment including the associated databases and directory servers. To add this topology into an existing Access Manager - Identity System target, select **Use the specified system** and select an existing target of type Access Manager - Identity System. If you want to create a new Access Manager - Identity System target, select **Create a new system** and enter the name of new system target. Click **Finish** to complete the discovery.
6. The next page shows a message confirming the discovery of Oracle Access Manager - Identity Server.

20.1.3 Discovering Oracle Identity Federation Server 10.1.4.2 and 10.1.4.3.0

Enterprise Manager has a simple Discovery wizard for Oracle Identity Federation targets. The Discovery wizard collects details about Oracle Identity Federation targets including information about the host name, host login credentials, and other details.

After the Discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into the Management Repository.

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

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.
2. From the Add menu, select **Oracle Identity Management 10g (OAM, OIF, OIM)**.
3. Select **Identity Federation Server** and enter the host name on which your Oracle Identity Federation Server is running. Click **OK** to continue with the discovery of the Identity Federation Server.
4. Enter the information requested for Oracle Identity Federation Server. Click **Continue** once all required information is entered.

Field	Description
Application Server Target	Select the Application Server target on which Oracle Identity Federation is running.
Host User Name	User name on the operating system with administrator privileges.
Host User Password	Password of host administrator account.

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

   To add this topology into an existing Identity Federation System target, select **Use the specified system** and select an existing target of type Identity Federation System.

   If you want to create a new Identity Federation System target, select **Create a new system** and enter the name of new system target. Click **Finish** to complete the discovery.
6. The next page shows a message confirming the discovery of Oracle Identity Federation Server.

20.1.4 Discovering Oracle Identity Manager Server 9.1.0.1

Enterprise Manager has a simple Discovery wizard for Oracle Identity Manager targets. The Discovery wizard collects details about Oracle Identity Manager targets including information about the host name, host login credentials, and other details.

After the Discovery wizard is complete, you can add the discovered targets into an existing System topology or you can create a new System target that stores your topology into Enterprise Manager's Repository.

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

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.
2. From the **Add** menu, select **Oracle Identity Management 10g (OAM, OIF, OIM)**.
3. Select **Identity Manager Server** and enter the host name on which your Oracle Identity Manager is running. Click **OK** to continue with the discovery of the Oracle Identity Manager Server.
4. Enter the information requested for Oracle Identity Manager Server. Click **Continue** once all the required information is entered.

Field	Description
Application Server Target	Select the Application Server target on which Oracle Identity Manager is running.

Field	Description
Configured Database Target	Select the configured Database target used by Oracle Identity Manager
Database User Name	Enter the database user name used to access the tablespace reserved for Oracle Identity Manager.
Database Password	Enter the password for the database account reserved for Oracle Identity Manager.
Identity Manager Library Path	Enter the directory path for the Oracle Identity Manager library (<OIM_HOME>\xellerate\lib).
Host User Name	User name on the operating system with administrator privileges
Host Password	Password of host administrator account.

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

   To add this topology into an existing Identity Manager System target, select **Use the specified system** and select an existing target of type Identity Manager System.

   If you would like to create a new Identity Manager System target, select **Create a new system** and enter the name of new system target. Click **Finish** to complete the discovery.

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

20.1.5 Discovering Oracle Identity Management Suite 10.1.4.2 and 10.1.4.3.0

Enterprise Manager has a simple Discovery wizard for Oracle Identity Management Suite 10*g* (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server) targets. The Discovery wizard collects details about Oracle Identity Management Suite 10*g* targets including information about the host name, host login credentials, and other details.

To discover Oracle Identity Management Suite 10*g* (including Oracle Internet Directory, Directory Integration Platform, Delegated Administration Server, and Single Sign-On Server), perform the following steps:

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.
2. From the **Add** menu, select **Oracle Application Server**.
3. Select the host on which Oracle Identity Management Suite 10*g* targets are running.
4. A confirmation page lists Oracle Application Servers found on the host selected. Click **OK** to continue. **Important:** Ensure that the Application Server is up before discovering the Identity Management Suite targets.
5. A final confirmation page appears. Click **OK** to finish the discovery process.

20.1.6 Discovering Identity Management 11g

Enterprise Manager has a simple Discovery wizard for Oracle Identity Management 11*g* (including Oracle Internet Directory, Directory Integration Platform, Oracle Virtual Directory, Oracle Identity Federation, Oracle Access Manager, Oracle Adaptive Access and Oracle Identity Manager) targets. The Discovery wizard collects details about

Oracle Identity Management 11*g* targets including information about the host, WebLogic User Name/Password, and other details.

Note: Before discovering the targets associated with Oracle Access Manager 11*g*, download and install patch 10094106.

To discover Oracle Identity Management 11*g* (including Oracle Internet Directory, Directory Integration Platform, Oracle Virtual Directory, Oracle Identity Federation, Oracle Access Manager, Oracle Adaptive Access Manager and Oracle Identity Manager), perform the following steps:

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.
2. From the **Add** menu, select **Oracle Fusion Middleware/WebLogic Domain.**
3. Enter the information requested to discover Oracle Identity Management 11*g* targets.

Field	Description
Administration Server Host	Host on which the WebLogic domain for Identity Management is running. Import the certificates for this WLS domain on the agent if this is a secured domain.
Port	Port used for the WebLogic domain. Enter a number between 1 and 65535.
User Name	WebLogic domain user name.
Password	WebLogic domain password.
Unique Domain Identifier	A unique identifier for the Identity Management domain and is used to create a unique target name. The Unique Domain Identifier can contain only alphanumeric characters and the special character '_' and cannot contain any other special characters.
Agent	Agent that is running on the Identity Management host. Only an agent 12.1 or later can be used for finding targets.
Advanced Fields	**Description**
JMX Protocol	JMX protocol is used to make a JMX connection to the Administration Server.
Discover Down Servers	This is a signal to discover the servers that are down.
JMX Service URl	JMX Service URL is used to make a JMX connection to the Administration Server. If the URL is not specified, it will be created based on the input parameters. If the URL is specified, the Administration server host and port information must still be provided in the input parameters.
External Parameters	These parameters will be passed to the java process which makes a connection to the Administration Server. All the parameters must begin with -D.
Discovery Debug File Name	The agent side discovery messages for this session will be logged into this file. This file will be generated in the discovery agent's log directory <agent home>/sysman/log. If this file already exists, it will be updated.

4. A list of all the Identity Management targets is listed. Click **Add** to complete the discovery. **Note:** If the Configured Agent text-box is blank for one or more of the targets, copy and paste the Management Agent URL before you proceed.

5. The status of target discovery is summarized in this screen. Ensure that all targets have been successfully added to Enterprise Manager. Press **OK** to finish the discovery process.

6. The discovered targets will now be listed on the Identity and Access dashboard. From the **Targets** menu, select **Middleware**, then select **Middleware Features**.

20.1.7 Discovering Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g

To discover Oracle Directory Server Enterprise Edition 6.x, 7.x, 11g targets, perform the following steps:

1. Log in to Enterprise Manager. Select **Targets**, then select **Middleware**.

2. From the **Add** menu, select **Oracle Directory Server Enterprise Edition.**

3. Enter the information requested.

   a. Oracle Directory Server Enterprise Edition Registry Host: Host of the Directory Server Control Center Registry

   b. Oracle Directory Server Enterprise Edition Registry Port: Port of the Directory Server Control Center Registry

   c. Directory Server User Name - for example CN=Directory Manager

   d. Directory Server User Password

   e. Oracle Directory Server Enterprise Edition Install Home: Path under which Directory Server Enterprise Edition is installed.

   f. Unique Deployment Identifier: A unique identifier for ODSEE deployment.

20.2 Collecting User Statistics for Oracle Internet Directory

With Enterprise Manager, you can collect user statistics for Oracle Internet Directory allowing you to view charts for failed and completed LDAP operations like Add, Bind, Compare, Delete, Modify, and Search.

To enable the collection of user statistics, perform the following steps:

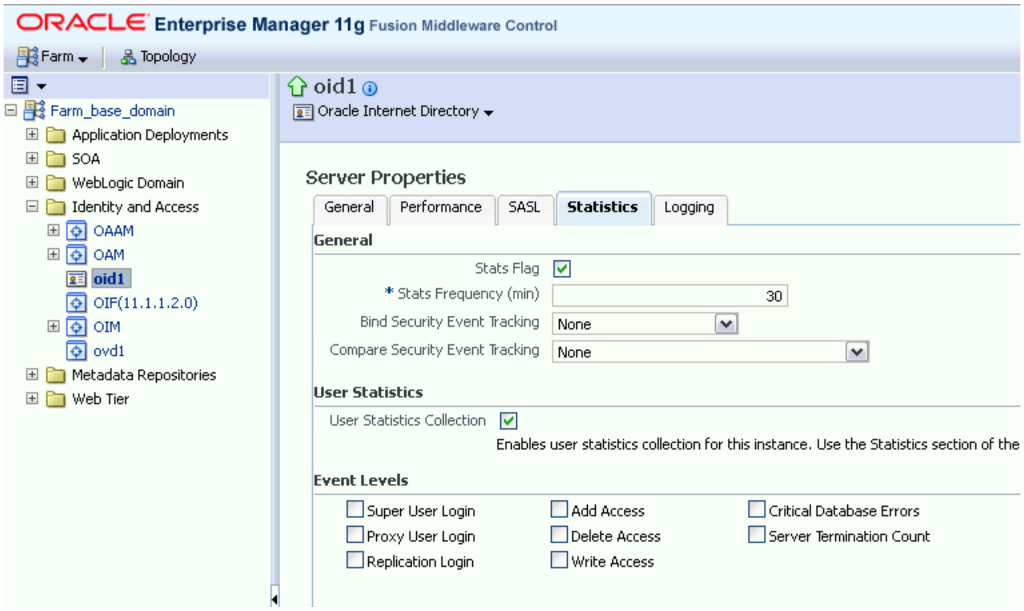
1. From the **Targets** menu, select **Middleware**. From the **Middleware Features** menu, select **Identity and Access.**

2. Select the discovered Oracle Internet Directory target.

3. From the **Oracle Internet Directory** menu, select **Fusion Middleware Control**.

4. From the **Targets** menu in Fusion Middleware Control, select **Administration**, then select **Server Properties**. Check the box next to **User Statistics Collection** to enable this feature. Click **Apply** to save your changes. See Figure 20–1.

Figure 20–1 Server Properties - Statistics Tab



General

Stats Flag ☑

* Stats Frequency (min) 30

Bind Security Event Tracking None

Compare Security Event Tracking None

User Statistics

User Statistics Collection ☑

Enables user statistics collection for this instance. Use the Statistics section of the

Event Levels

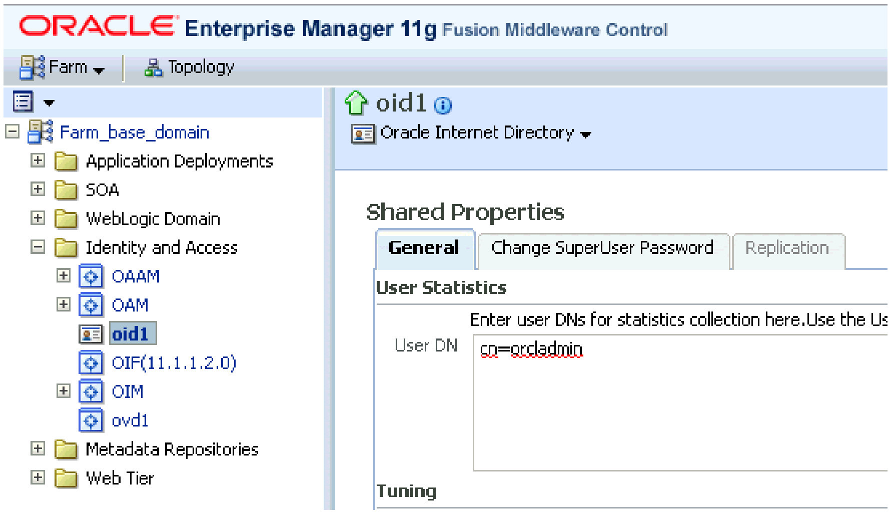
☐ Super User Login ☐ Add Access ☐ Critical Database Errors

☐ Proxy User Login ☐ Delete Access ☐ Server Termination Count

☐ Replication Login ☐ Write Access

5. From the **Target** menu in Fusion Middleware Control, select **Administration**, then select **Shared Properties**. Enter a valid User DN (for example, cn=orcladmin) to enable user statistics collection for that user. See Figure 20–2.

Figure 20–2 Shared Properties - General Tab



User Statistics

Enter user DNs for statistics collection here.Use the Us

User DN cn=orcladmin

20.3 Creating Identity Management Elements

This section describe how to create Identity Management elements.

20.3.1 Creating Identity and Access System

With Enterprise Manager, you can create an Identity and Access System target that can be modeled with any discovered Oracle Identity Management target (including both Identity Management 10g and Identity Management 11g targets) and the underlying hosts, databases and LDAP servers as the key components providing an end-to-end system oriented view of the monitored Identity Management environment.

The Identity and Access System target provides access to metrics, alerts, charts, and topology view. In addition to monitoring your Oracle Identity Management environment from a system perspective, you can also monitor your environment from a service-oriented perspective using the Cloud Control Service Level Management framework.

To create a target of type Identity and Access System associated with any of the monitored Identity Management targets, perform the following steps:

1. Log in to Enterprise Manager. Select **Targets**, then select **Systems**.
2. From the **Add** menu, select **Identity and Access System**.
3. Select the Identity Management root target that you would like to include in your system topology. This can be the WebLogic Domain or the ODSEE Registry server.

   Click **Next** to continue.
4. Select the targets within the domain that you would like to include in your system topology. You can also add additional targets that are not in the Identity Management domain, for example, databases, non-Oracle middleware, and so on. Click **Next** to continue.
5. Click **Finish** to complete the creation of Identity and Access System.

20.3.2 Creating Generic Service or Web Application Targets for Identity Management

The Discovery wizard for Oracle Identity and Access Management Suite allows you to create a System target to store the end-to-end topology of monitored Oracle Identity Management components. The Management Pack Plus for Identity Management allows you to create the following System targets:

- Access Manager - Access System
- Access Manager - Identity System
- Identity Federation System
- Identity Manager System
- Identity and Access System

A System target is modeled with all monitored Oracle Identity Management components and the underlying hosts as the key components providing an end-to-end system oriented view of the monitored Oracle Identity Management environment.

A System target provides access to metrics, alerts, charts, and topology view of all the infrastructure components. In addition to monitoring your Oracle Identity Management environment from a system perspective, you can also monitor your environment from a service-oriented perspective using the Cloud Control Service Level Management framework.

With the Management Pack Plus for Identity Management, users can create targets of type Generic Service or Web Application associated with any of the monitored Identity Management Systems: Access Manager - Access System, Access Manager - Identity System, Identity Federation System, and Identity Manager System.

The Web Application or Generic Service target provides an end-to-end service oriented view of the monitored Oracle Identity Management targets with access to performance and usage metrics, service tests, service level rules, service availability definition, alerts, charts, and topology view.

To create a target of type Generic Service associated with any of the monitored Identity Management Systems, perform the following steps:

1. Log in to Enterprise Manager. Select **Targets,** then select **Services**.
2. From the **Add** menu, select **Generic Service**.
3. Enter the general information requested for the new Generic Service.

20.3.3 Creating a Service Dashboard Report

Once you have created Generic Service or Web Application targets associated with your monitored Oracle Identity Management Systems, you can create a Services Monitoring Dashboard that summarizes Service Level Agreement Compliance, Actual Service Level Achieved, Key Performance and Usage Metrics, and Status of Key Components.

Perform the following steps to create a Services Monitoring Dashboard:

1. From the **Enterprise** menu, select **Reports**, then select **Information Publisher Reports**.
2. Click the **Create** button.
3. Enter the general information requested for the new Report. Click the **Elements** tab once all information requested is entered.
    a. Title

       Enter a title for your new dashboard

    b. Category/Sub-Category

       Select a category and sub-category for your dashboard, for example, Category: Monitoring, Sub-Category: Dashboards

    c. Use the specified target

       Leave blank if this report has no report-wide target.

    d. Options - Visual Style

       Select Dashboard for a dashboard-view of your services.
4. Enter the elements information requested for the new Report. Click the **Schedule** tab once all information requested is entered.
    a. Add

       Select **Services Monitoring Dashboard** and click **Continue**.

    b. Set Parameters

       Click **Set Parameters**. Select the available services and click the **Move** button to add them to the Selected Services.
5. Enter the schedule information requested for the new Report. Click the **Access** tab once all information requested is entered.
    a. Schedule

       Enter your scheduling preferences for the report

    b. E-Mail Report

       Enter the email address and preferences for the report recipient.

6. Enter information about your access and security preferences for the new report. Click **OK** to create the new Services Monitoring Dashboard.

Part IX

Using Application Dependency and Performance

The chapters and appendixes in this part provide information regarding the usage of Application Dependency and Performance (ADP).

The chapters and appendixes are:

- Chapter 21, "Introduction to Application Dependency and Performance"
- Chapter 22, "Exploring Application Dependency and Performance"
- Chapter 23, "Exporting Data"
- Chapter 24, "ADP Methodology"
- Chapter 25, "Troubleshooting Application Dependency and Performance"
- Appendix A, "ADP Configuration Directories and Files"
- Appendix B, "Support Matrix for Application Dependency and Performance"

21 Introduction to Application Dependency and Performance

The Application Dependency and Performance (ADP) pages within Enterprise Manager Cloud Control analyze Java EE, SOA, and Portal applications to capture the complex relationships among various application building blocks in its Application Schema model - the core of the Oracle intelligent platform.

Using ADP you can:

- Monitor performance of applications deployed in the following type of Servers:
  - Oracle SOA Suite 11*g*
  - Oracle Service Bus
  - Java EE
  - Oracle WebLogic Portal
- Have visibility into components defined by way of metadata within a framework (for example, components within a composite) with deep dive visibility, where available
- View static relationships defined between components and services, such as OSB business and proxy services, and SOA services and references

This chapter includes the following:

- Overview
- Architecture

21.1 Overview

Using the insights stored in Application Schema, ADP is able to deliver an Application Service Management (ASM) environment that self-customizes out-of-the-box, evolves with change, minimizes expert involvement, and delivers a holistic, service-oriented view across heterogeneous environments. ADP enables an enterprise to more efficiently manage distributed applications, attain management agility, and lower total cost of ownership.

See the following sections:

- Managing Complex Java EE, SOA, OSB, and Portal Applications
- Delivering a Service-Oriented View Across Environments
- Avoiding Involvement from Java EE, SOA, OSB, Portal, and Application Experts

- Eliminating Repetitive Do-It-Yourself (DIY) Manual Processes
- ADP Solution

21.1.1 Managing Complex Java EE, SOA, OSB, and Portal Applications

Today's Java EE, SOA, OSB, and Portal applications enable enterprises to deliver mission-critical business functions to key constituencies - most often their customers, partners, and employees. These composite applications are assembled from many different Java EE components and exposed services distributed across a heterogeneous environment.

To be effective at managing today's complex, distributed Java EE, SOA, OSB, and Portal applications across a heterogeneous environment, enterprises must adopt an intelligent ASM platform with the following characteristics:

- Provides holistic, service-oriented views across heterogeneous environments

  An intelligent ASM platform must provide high-level service-oriented metrics that map to low-level technology-centric metrics. These measurements must be organized in a service-oriented fashion to deliver a unified, holistic view of the numerous interconnected application components deployed across heterogeneous environments.

- Requires minimal Java EE, SOA, OSB, Portal, and application expertise

  An intelligent ASM platform must have the ability to capture complex relationships among various interconnected components of today's Java EE, SOA, OSB, and Portal applications. This ability can help minimize reliance on Java EE, SOA, OSB, Portal, and application experts for setting up and maintaining effective APM environments.

- Eliminates repetitive DIY manual processes

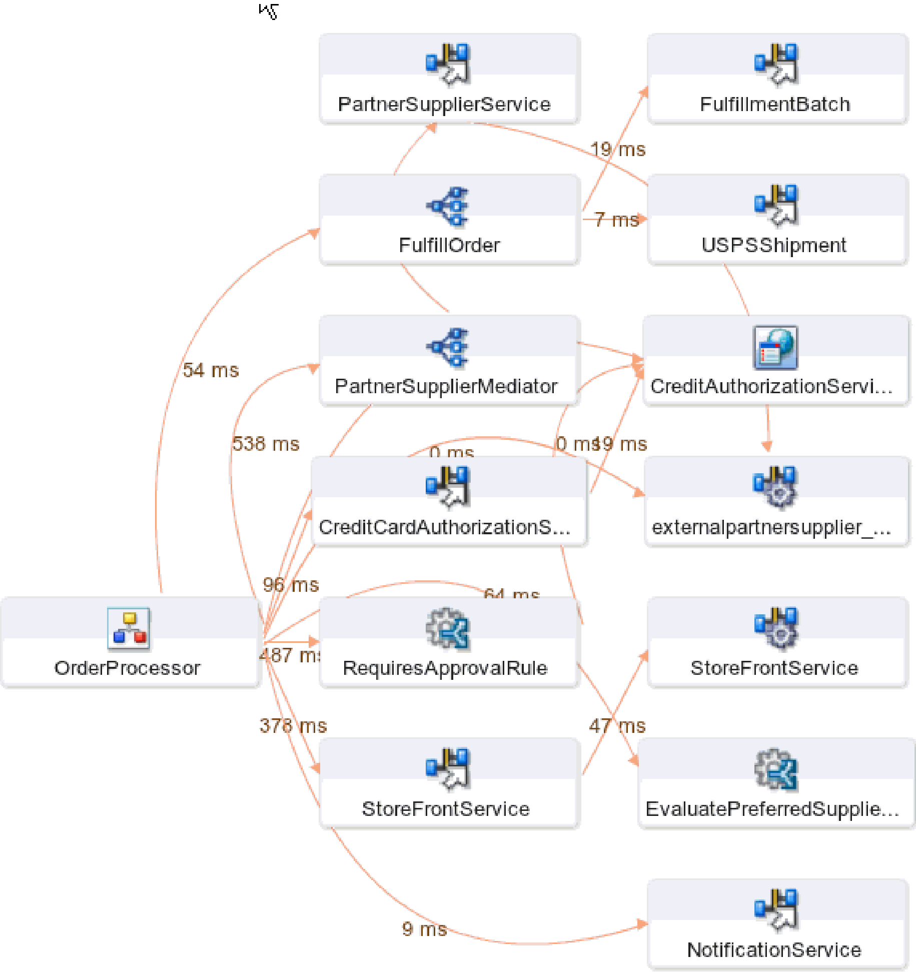
  An intelligent ASM platform must eliminate repetitive DIY manual processes by delivering the ability to self-customize out-of-the-box and evolve with change. Elimination of these repetitive DIY manual processes is the only way to deal with rising complexity and rapid rate of change with ease.

21.1.2 Delivering a Service-Oriented View Across Environments

Today's mission-critical business functions are powered by Java EE, SOA, OSB, and Portal applications that comprise numerous interconnected components deployed across highly distributed environments. To manage these applications effectively, enterprises must first gain an understanding of the complex relationships among the business functions, associated interconnected components, and the underlying runtime environments. To enable clear and accurate understanding, IT organizations need holistic, service-oriented views that span across heterogeneous environments.

Furthermore, appropriate rendering of these views enables users at different levels of the organization to collaborate with each other and do their respective jobs more efficiently.

Figure 21–1 Application Dependency and Performance Topology View in Enterprise Manager Cloud Control



Application Schema Navigation provides efficient ways for you to access relevant information using techniques like hierarchical traversal, architecture model navigation, string queries, drill down, drill out and more.

21.1.3 Avoiding Involvement from Java EE, SOA, OSB, Portal, and Application Experts

To manage Java EE, SOA, OSB, and Portal performance effectively, IT organizations must adopt an intelligent platform like ADP that requires minimal expertise to set up and maintain. Unlike conventional APM toolkits, ADP does not rely on human expertise to set up and maintain customized APM environments. Instead, ADP uses a unique model-driven approach that leverages the information stored in its Application Schema model to keep the involvement of experts to the minimum. ADP's unique ability to self-customize out-of-the-box and evolve with change makes it the perfect solution for managing not only custom enterprise applications, but also applications developed by external parties.

21.1.4 Eliminating Repetitive Do-It-Yourself (DIY) Manual Processes

Based on a unique model-driven approach, ADP eliminates repetitive DIY manual processes. To achieve this level of self-customization and continuous change adoption, ADP uses its AppsSchema modeling technology to perform the critical task of analyzing application structure and infrastructure configuration. After capturing these insights in the Application Schema model, ADP leverages this information to establish a fully customized ASM environment. To keep this environment up-to-date, ADP continuously updates the Application Schema model as new applications are deployed and changes are applied. ADP's unique ability to self-customize out-of-the-box and evolve with change enables fast time-to-value, low total-cost-of-ownership (TCO), and maximal return-on-investment (ROI).

21.1.5 ADP Solution

Oracle provides the industry's first intelligent ASM platform for Java EE, SOA, OSB, and Portal. Unlike conventional APM toolkits, ADP analyzes these applications and captures complex relationships among various application building blocks in its Application Schema model - the brain of this intelligent ASM platform.

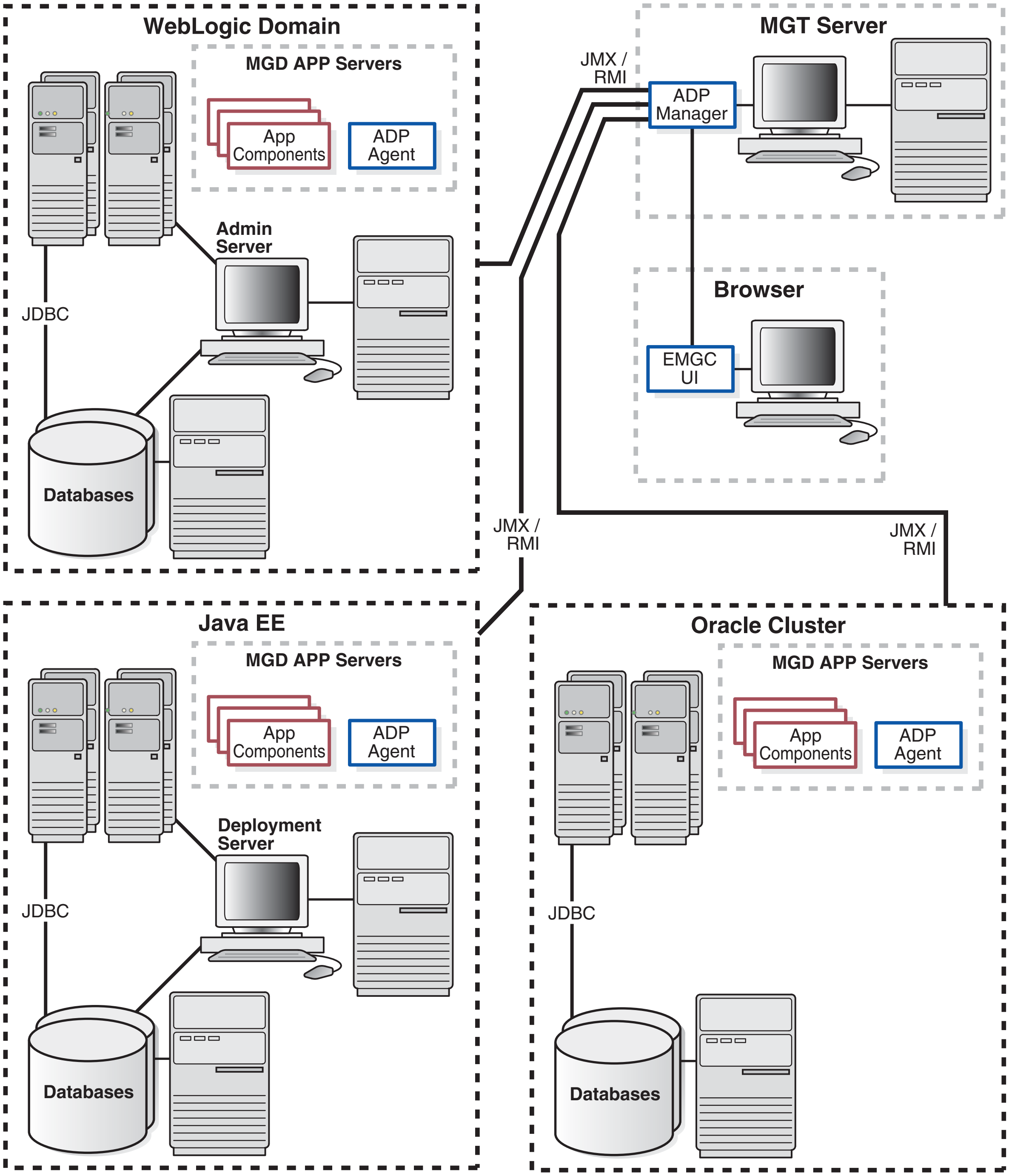
Using the insights stored in the Application Schema model, ADP is able to deliver an ASM solution that self-customizes out-of-the-box, evolves with change, minimizes expert involvement, and delivers a holistic, service-oriented view across heterogeneous environments. Adopting an intelligent platform such as Oracle will enable the enterprise to more efficiently manage distributed applications, attain management agility, and lower total cost of ownership.

21.2 Architecture

ADP employs a multi-tier, fully distributed, configurable architecture to provide the scalability and flexibility to meet the changing needs of enterprise deployments.

ADP operates as a service on the machine and automatically begins running when the machine first boots, and remains on perpetually. ADP is typically installed on its own machine and dedicated to monitor a group of managed application servers.

Figure 21–2 ADP Topology



The following core components are deployed to form the ADP ASM system.

21.2.1 ADP Java Agents

ADP Java Agents are the data collectors of the ADP ASM system. ADP Java Agents are deployed to all managed application servers to perform a series of tasks including collecting performance managements, tracking contextual relationships, and summarizing data in real-time while introducing as little overhead as possible. At the expiration of the predefined aggregation interval, these agents forward the summarized data to ADP for additional analysis. For various Java EE platforms such as Oracle SOA Suite and Oracle WebLogic, ADP leverages their deployment infrastructures to quickly deploy the ADP Java Agents to all application servers.

21.2.2 ADP Manager

ADP Manager is the core analytical engine of the ADP ASM system. In real-time, ADP Manager performs complex mathematical modeling and statistical calculations with summarized data from all ADP Java Agents. ADP Manager can be configured with a backup to provide higher level of availability.

21.2.2.1 ADP Manager and High Availability

Although the ADP Manager does not have high availability (HA) built into it, administrators can have a backup ADP Manager installed on a separate machine; this backup ADP Manager points to the same database but is disabled. If the production ADP Manager fails, the backup ADP Manager can then be enabled against the same database. The backup ADP Manager then rediscovers the application after the agent is redeployed from the backup ADP Manager, to the managed resources in order to synchronize them. All metrics are preserved, assuming the model does not change in the short time frame it takes to bring the backup ADP Manager online.

The key with this backup procedure is to backup the database that ADP uses as its repository in order to preserve the historical data. On the modeling side, the backup ADP Manager has to rediscover the application which should happen automatically, as long as the resources are configured and the new agent has been deployed.

If historical data preservation is not a necessity, users can simply have another ADP Manager and database and swap agents reducing the backup effort considerably.

21.2.3 ADP User Interface

The ADP User Interface (ADP UI) is the primary user interface for ADP users. Users can use ADP UI to set Service Level Objectives (SLOs), analyze monitoring data, and more. The ADP UI is fully configurable. To access ADP:

1. From the **Targets** menu, select **Middleware**.
2. From the **Middleware Features** menu on the Middleware page, select **Application Dependency and Performance**.

22

Exploring Application Dependency and Performance

This chapter examines the following:

- Exploring the User Interface
- Exploring the Monitoring Tab
- Exploring the Configuration Tab
- Exploring the Registration Tab

22.1 Exploring the User Interface

This section explores the ADP User Interface. Topics include:

- Accessing ADP
- General ADP UI Elements
- Drill Down in Operational Dashboard
- Time Frame
- Display Interval
- Graphs and Data Items
- Custom Metrics
- Functional View
- Topology View
- Architecture View
- Metric Types

22.1.1 Accessing ADP

To access the Enterprise Manager Application Dependency and Performance (ADP) feature, do the following:

1. From the **Targets** menu, select **Middleware**.
2. From the **Middleware Features** menu on the Middleware page, select **Application Dependency and Performance**.

22.1.2 General ADP UI Elements

ADP UI consists of the following core components:

- Navigation Pane (left)

  There are three types of workspaces in the ADP navigation pane: *Monitoring, Configuration,* and *Registration*. In the Monitoring workspace, you can navigate the managed environment and monitored applications in a tree.

  – Use the Monitoring workspace to traverse the ADP tree model and identify abnormal activities.

  – Use the Configuration workspace to create, modify, and review various configuration settings for ADP.

  – Use the Registration workspace to enable and disable request monitoring.

- Main Display Window (right)

  As you navigate through the ADP tree model and configuration categories, detailed performance information and configuration settings are displayed in the Main Display Window. You can refresh the Main Display Window at anytime by clicking the Refresh icon.

22.1.3 Drill Down in Operational Dashboard

The Operational Dashboard displays the health indicators for various key entities in the managed environment. ADP uses traditional traffic light colors to represent the health of these various key entities.

For each component, ADP uses the following health indicators to provide a comprehensive view. These health indicators are:

- Performance

  The performance health indicator depicts the relative responsiveness of the monitored entity to the configured threshold.

- Availability

  The availability health indicator informs you to what extent a particular entity is available to service requests. The Availability arrow explains the availability of the particular entity: Red down arrow means the entity is not available whereas the Green up arrow means the entity is available.

- Errors

  The errors health indicator informs you if the number of errors and exceptions encountered by this entity are approaching or violating the configured threshold. If there is any errors in the server, the check mark is in red.

- Load

  The load health indicator depicts how many operations have been performed and requests have been served by a particular entity.

ADP is aware of clusters. As such, these indicators display overall health of a particular entity across the entire cluster.

22.1.4 Time Frame

In ADP, you can specify the length of the time the window information is to be displayed. To specify the length of this time window, select the appropriate length in the Time Frame list. The following Time Frame values are available:

- 1 hour
- 2 hours
- 4 hours
- 8 hours
- 12 hours
- 24 hours

> **Note:** The ADP default data collection interval is 60 seconds. As you adjust the data collection interval, ADP automatically adjusts the display time frames.

ADP automatically adjusts information displayed to fit the specified time window. You can drill down to see detailed performance information for a specific range of time.

For example, visualize the drill down process with two screen shots of the same graph with different Time Frames of the average response time for Portal campaign. The first graph has a Time Frame of 24 hours. The second graph has a Time Frame of 1 hour. By increasing the granularity of the Time Frame, you are performing a drill down operation.

For example, an IT Operations staff noticed abnormally high response time with Portal campaign subsystem. The person decided to investigate further to evaluate the extent of the problem. By changing the Time Frame from 24 hours to 1 hour, this user is able to see that between 14:17 and 14:18, the Portal campaign response time jumped from an average of 1000 milliseconds to 5000 milliseconds. While the problem did not persist, it may warrant additional investigation.

22.1.5 Display Interval

Display Interval, located above the Main Display window, indicates the start and end time for the data displayed in the Main Display Window. Display Intervals change as you change the following settings:

- Time Frame
- Interval Context
- Turning Off Time Frame Limitation

22.1.5.1 Time Frame

When you select a new Time Frame, the Display Interval automatically changes to fit the selected Time Frame. For example, if you were to change the Time Frame from 1 hour to 2 hours, the Start value of the Display Interval changes.

22.1.5.2 Interval Context

Display Interval can also be changed by setting the Interval Context. The settings for the Interval Context are:

- End Time Is Current System Time

  The default Interval Context for ADP is to use the current system time as End value for the Display Interval. In this default setting, you have a sliding Display Interval and can see the latest performance information in the Main Display Window.

- End Time Is Fixed

  You can also change the Interval Context setting to use a fixed time as the End value for the Display Interval. By selecting the fixed Interval Context, you can create a fixed time window to display performance data. The fixed time window is particularly useful for performing analytical tasks.

- Date/Time Selector

  When you select to fix the End time for the Interval Context, the ADP UI enables a pair of Date/Time Selectors to allow you to set Start or End values for the Display Interval. Click the icon next to the Start and End times to open up the Date/Time Selector.

  The Date/Time Selector allows you to set a specific Display Interval to fit your needs. Additionally, the Date/Time Selector enables ADP to compare current performance trends with historical data.

  > **Note:** Changing the start and end time do conceptually different things. Users are advised to always change their time frame by modifying the end time first, and then the start time. Changing the end time moves the window in time, whereas changing the start time increases/decreases the size of the window.

22.1.5.3 Turning Off Time Frame Limitation

To support the display of data for more than twenty four hours, ADP allows you to specify your own time frame for data display. To enable this feature, set **Interval Context** to **End time is fixed** and make sure the **Use time frame:** check box is unchecked. Turning off time frame limitation allows ADP to display eight days worth of data.

For example, when you specify the time frame to be eight days by adjusting the start and end times through the Date/Time Selector, ADP then adjusts its view to display eight days worth of data in a single graph. This feature allows you to perform trending analysis over time.

22.1.6 Graphs and Data Items

ADP displays performance information in various formats. Most commonly used display formats in ADP are tables and graphs.

- On graphs, you can gain more information about a data item by pointing the mouse over the interested item.
- Minimum and maximum response time measurements are stored in their database in addition to average response time measurements. The min and max metrics, if present, are displayed visually in the UI.
- For tables, you can perform a table sort by clicking the blue up/down arrow located in the column headings.

22.1.7 Custom Metrics

While ADP intelligently selects relevant performance metrics based on its Application Schema model, you can further customize the monitoring environment by configuring additional custom metrics. In addition, you can use custom metrics in problem diagnostic situations where additional visibility is needed to pinpoint problem root cause.

To configure a new custom metric:

1. Click **Custom Metric Configuration** on the Configuration tab
2. Click the **Create Custom Metric** button.
3. On the Custom Metric File page, either choose an existing custom metric file or provide the name of a new custom metric file. Click **Continue**. ADP walks you through the configuration process.

Custom Metric Configuration page includes the following fields, see Table 22–1.

Table 22–1 Custom Metric Configuration Page

Field	Description
Name	This text field is for defining the display name for the custom metric.
Resource Name	This list is for defining the resource where the custom metric will be collected.
Class Name	This text field is for defining the fully qualified class name (package + class) associated with the custom metric.
Method Name	This optional text field is for defining the method name associated with the custom metric. **Usage:** 1. Type in * - ADP will instrument all methods. 2. Provide comma separated list of methods with no wildcards - ADP will create method entities and only instruments these methods in the agent. 3. Provide comma separated list of methods with wildcard prefixes or suffixes - ADP will instruct the agent to instrument the methods specified along with the wildcards. 4. Provide 1) or 2) preceded by "!" to create an excluded list - ADP will instruct the agent to instrument all methods in the class not defined in the exclude list. Method field examples: 1. methodA,methodB,methodC 2. ejb*,*context,methodA 3. !ejb*,*context,methodA

After you define the custom metrics, restart the application server instances associated with these customizations. The new custom metrics will be listed under the Custom Metrics node in the ADP navigation tree.

The newly configured custom metric provides class level performance data, for example invocation count and response time.

22.1.8 Functional View

Functional View is a type of Application Schema Visualization - a visual way for ADP to represent the information stored in its Application Schema model. This view is designed to help you understand how business functions are assembled with various functional building blocks. Table 22–2 provides a list of functional views currently available in ADP.

Table 22–2 Functional View

Entity Type	Function View	Description
Process	Process Workflow View	This functional view depicts the workflow associated with the Oracle BPEL business process. It shows all the process nodes and the relationships among them.
Pageflow	Pageflow Functional View	This functional view depicts the logical flow associated with a JPS or Struts pageflow. It shows all the pages in a pageflow and the relationships among them.
OSB Proxy Service	Proxy Service Functional View	This functional view depicts the pipeline and stage flow associated with an OSB Proxy Service.

Depending on the type of entity selected, ADP displays different functional views. Right-click and select Display Functional View to bring up the relevant Functional View associated with the selected entity.

22.1.9 Topology View

Topology View is another type of Application Schema Visualization - a visual way for ADP to represent the information stored in its Application Schema model. This view is designed to help you understand how application environments are assembled with various applications, application server instances, and shared resources. This information helps you map composite applications and their building blocks to application server instances and share resources.

The highest level topology view graphically depicts domains, external resources, and shared database resources. The applications used in the following examples are CSS and MedRec demos.

For example, you can have a topology with two ADP managed resources, CSS Domain and MedRec Domain, two external resources, and a shared database resource. The lines connecting various entities in the Topology Views depict calls made from one entity to another. You can get more information about a specific call by pointing the mouse over a specific line.

It is possible to hide different types of lines in the Topology View. To the line types, right-click the **Topology View** and highlight the **Edge types** option to reveal a list of different edge (arrow) types associated with the current Topology View.

22.1.10 Architecture View

Architecture View is another type of Application Schema Visualization; a visual way for ADP to represent the information stored in its Application Schema model. This view is designed to help you understand the structure and behaviors of Java EE, SOA, and Portal applications at the module and component level. Some Architecture Views also include built-in delay analysis to help identify potential bottlenecks in a given call path.

The Architecture View in ADP is capable of showing application structure and component relationships at two levels: module and component levels. At each level, ADP can show both active and potential call paths. Table 22–3 describes various types of Architecture Views.

Drill down on a specific application to launch into the Architecture View. This action demonstrates the logical progression of drilling from high level resource-centric topology view, down through application-centric topology view, to module-centric architecture view. Using this logical drill down, you can understand the structure of your application runtime environments and diagnose problems.

Table 22–3 Various Types of Architecture View

Tab Name	Description
Module Level Execution	This is the default Architecture View at the module level. The Module Level Execution view shows the active calling relationships among various Java EE modules (EAR, WAR, JAR, and so on). Shared resources are also included.
Module Level	The Module Level view shows the potential calling relationships among various Java EE modules. Shared resources are also included. It should also be noted that any object that is not connected within the static view will not be included at this level and if there are no static connections at all between objects, every potential object relationship will be displayed. By default, the Module Level view is not enabled.
Component Level Execution	This is the default Architecture View at the component level. The Component Level Execution view shows the active calling relationships among different Java EE components (EJB, servlet, JSP, and so on). Shared resources are also included.
Component Level	The Component Level view shows the potential calling relationships among various Java EE components. Shared resources are also included. Similar to the module level, any object that is not connected within the static view will not be included at this level and if there are no static connections at all between objects, every potential object relationship will be displayed. By default, the Component Level view is not enabled.

These various types of architecture views are color coded in order to provide additional information. Table 22–4 lists color codes and their meanings.

Table 22–4 Architecture View Color Codes

Background Color	Description
Orange	The orange background color represents entry points into the application or module. The orange color also represents that these entities belong to the same application or module currently selected (in context).
Green	The green background color represents entry points into the application or module. The green color also represents that these entities belong to other applications or modules (out of context). The green color is also used to represent share resources.
White	The white background color represents that these entities belong to the same application and module currently selected (in context).
Blue	The blue background color represents that these entities belong to other applications and modules (out of context). The blue color also represents shared resources.

ADP graphically depicts active calling relationships among various Java EE modules and shared resources.

22.1.10.1 Accessing the Architecture View

There are several ways to access the Architecture View. One way is through the Deployments node associated with a specific application under the Application Node. Application specific Architecture View can be accessed using the Deployments node on the Oracle Tree.

The last way to access the Architecture View is by right-clicking a managed entity and selecting the Architecture View. Right-click and select Architecture View to start the drill down process.

22.1.10.1.1 Arrows in Architecture Views The arrows connecting various entities in the Architecture Views depict calls made from one entity to another. You can get more information about a specific call by pointing the mouse over a specific arrow. Mousing over arrows shows the details of a specific call in Architecture View

It is possible to hide different types of arrows in the Architecture View. To do this, right-click on the Architecture View and highlight the Edge types option to reveal a list of different edge (arrow) types associated with current Architecture View. Unchecking a specific edge type hides all lines of that type in the Architecture View. Checking a specific edge type makes these lines appear.

To hide all lines not connected with a specific entity, select a monitored entity in the Architecture View, right-click and select **Hide other edges**. Highlight an entity and select **Hide other edges** to hide all arrows not connected to the managed entity.

22.1.10.1.2 Architecture View Summary The Architecture View Summary provides the delay analysis associated with the active call path displayed. The table and pie chart displayed in the right pane guides you to leading delay contributors in the displayed call path. Selecting a specific component in the call path brings up component specific information. You will see the following tabs:

- Summary tab first which includes high-level delay data for both inbound and outbound calls.
- The Instrumentation tab shows detailed method level performance data associated with the selected component. Click the Instrumentation tab to see detailed performance measurements and information at the method level.
- The Errors/Exceptions tab shows the errors metrics associated with the selected portal or BPEL process.
- The SQL Statement tab shows SQL statements and their performance data associated with the selected component.
- The Transactions tab shows the transaction events associated with the selected portal and children below. By default, the Transactions tab is not enabled.

22.1.11 Metric Types

Table 22–5 describes various types of metrics provided by ADP.

Note: All the ADP metric tables have a View drop-down list to change the order of the columns in the tables.

Table 22–5 Metric Types

Examples	Metric Type	Metric Description
Active Sessions Completions Pending Requests Running Instances Max Capacity Messages High	Snapshot Count	A count of the monitored entity at a point in time. ADP plots these snapshot counts in trend graphs.

Table 22–5 (Cont.) Metric Types

Examples	Metric Type	Metric Description
Requests Serviced Total Sessions [Processes] Aborted [Processes] Terminated [Method] Invocation Count Bytes Received	Aggregated Count	A count of the monitored entity incrementally aggregated from the beginning of display time window. ADP shows these aggregated counts in summary tables.
Response Time Elapse Time Connection Delay	Average Timing	Calculated every sampling period (default 60 seconds), the average timing is calculated by dividing the total amount of time needed to complete the monitored business unit of work by the number of completed business units of work. ADP uses this data in the following two ways: 1. Plot the average timings in trend graphs. 2. Calculate average timing of this business unit of work for the display time window and display in a summary table.
Min/Max	Minimum and Maximum Response Time Measurement	Minimum and maximum response time measurements found per collection sampling intervals. These are stored in their embedded database in addition to average response time measurements. The default is 60 seconds.

22.2 Exploring the Monitoring Tab

When ADP is pointed to an Oracle WebLogic domain or an Oracle SOA Suite cluster, it automatically discovers information about this particular domain including all deployed applications, configuration, resources, and others. ADP displays this information in the Monitoring tab under Oracle Enterprise Manager.

Each node represents a construct in the platforms monitored by ADP. Each construct is described in this section.

Note: Promote to dashboard can be configured in ADP to incorporate ADP metrics tables in the ADP dashboard page. The dashboard configuration can be selected for the entity type which is discovered by ADP and to display the entity metrics table on the dashboard.

This section includes the following topics:

- Monitoring ADP Entities
- WebLogic
- Oracle WebLogic Portals
- Oracle BPEL Processes
- Oracle ESB
- Oracle WebCenter
- Processes
- Web Services
- Pageflows
- Services

- WSRP Producers
- Integration
- Applications
- Oracle WebLogic Resources
- Oracle Resources
- Custom Metrics
- Status
- Service Component Architecture (SCA)

22.2.1 Monitoring ADP Entities

Performance can be monitored for the ADP entities:

- SOA Suite 11*g*
- OSB Applications
- Java EE Applications
- ADF Applications

22.2.1.1 Monitoring SOA Suite 11*g* Performance

To monitor the performance of service-oriented architecture applications (SOA), perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the SOA Infrastructure target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Monitoring** tab.

3. ADP discovers all the deployed Composites on the configured Oracle WebLogic Domain.

4. A Composite node appears under the configured ADP Manager (for example, select Oracle Enterprise Manager, select SOAServer, then select Composites).

   Under the Composites node, the following nodes appear:

   - SCA Partition
   - Composite
     - Services
     - Components
     - References
     - Wires

The performance metrics are displayed on the right-hand side panel when the respective node is selected.

22.2.1.2 Monitoring OSB Performance

To monitor the performance of Oracle Service Bus (OSB) applications, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the OSB target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Monitoring** tab, then select OSB in the tree.
3. ADP discovers all the deployed OSB proxy and business services on the configured Oracle WebLogic Domain.
4. An OSB node appears under the configured ADP Manager (for example, select Oracle Enterprise Manager, select servicbusServer, then select OSB).

   Under the OSB node, the following nodes appear:

   - Business Services
   - Proxy Services
     - Pipeline
     - References

The performance metrics are displayed on the right-hand side panel when the respective node is selected.

22.2.1.3 Monitoring Java EE Application Performance

To monitor the performance of Java EE applications, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the Java EE Application target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Monitoring** tab, then select the application in the tree.
3. ADP discovers Java EE artifacts like Servlet/JSPs, EJBs, and Web services.
4. You can find Java EE Application related data under following nodes:

   - Applications
   - Web Services
   - Services

The performance metrics for related components are displayed on the right-hand side panel when the respective component is selected.

22.2.1.4 Monitoring ADF Application Performance

To monitor the performance of Application Development Framework (ADF) applications, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the ADF target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Monitoring** tab, then select the application in the tree.
3. ADP discovers all the deployed ADF artifacts on the configured Oracle WebLogic Domain release 11*g*R1.

4. An ADF node appears under the configured ADP Manager (for example, Oracle Enterprise Manager, select Server, then select ADF). The ADF node contains the following:

   - ADF taskflows
   - JSF Pages
   - Managed Beans
   - Business Components

The performance metrics for related components are displayed on the right-hand side panel when the respective component is selected.

22.2.2 WebLogic

You can perform the following on WebLogic using Application Dependency and Performance.

- Monitor a WebLogic portal
- Add a WebLogic domain to be monitored by an existing ADP manager
- Remove a WebLogic Domain from monitoring

22.2.2.1 Monitoring WebLogic Portal Performance

Perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. In the Related Links section, click **Application Dependency and Performance** link.

2. Click the **Monitoring** tab, then select the application in the tree.
3. ADP discovers portal on the configured Oracle WebLogic Domain.
4. A Portals node appears under the configured ADP Manager (for example, Oracle Enterprise Manager, select PortalServer, then select Portals). The Portals node contains the following:

   - Portal Desktop, which is made up of Books, which are in turn made up of Pages, which in turn are made up of Portlets

The performance metrics for related components are displayed on the right-hand side panel when the respective component is selected.

22.2.2.2 Adding WebLogic Domain To Be Monitored By Existing ADP Manager

To add a WebLogic domain to be monitored by an existing ADP manager, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the WebLogic target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Configuration** tab and expand the Configuration (Manager Name). Click **Resource Configuration** and provide the details.

22.2.2.3 Removing a WebLogic Domain From Monitoring

To remove a WebLogic domain from being monitored, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. In the **Related Links** section, click **Application Dependency and Performance**.

2. Click the **Configuration** tab and expand the Configuration (Manager Name). Click **Resource Configuration,** choose the resource, and click **Delete Resource**.

22.2.3 Oracle WebLogic Portals

The Portals node under Oracle Enterprise Manager contains information about all deployed WebLogic Portal applications in the managed domains. The Portals node is organized hierarchically using the same framework developers use to build these Portal applications. The minimum and maximum response time measurements are stored in the database in addition to the average response time measurements. These metrics, if present, display visually in the Main Display Window on the right.

For WebLogic Portal, this hierarchy contains the following (Table 22–6):

Table 22–6 WebLogic Portal Hierarchy

Component	Description
Portals	The Portal is the logical containment unit for a Portal application. A typical Portal can contain a few desktops, several books, tens of pages, and hundreds of portlets.
Desktops	The desktop is the top-level container for the portal components included in that specific view of the portal. Portal administrators can create new desktops beyond what portal developers create in WebLogic Workshop.
Books	The top-level book contains all sub-books, pages, and portlets. The top-level book defines the initial menu navigation style used for the desktop. For each sub-book you add to a desktop you can select a different navigation style.
Pages	Pages and sub-books are the navigable containers used for organizing portlets.
Portlets	Portlets are the containers that surface Web content and applications in your desktops.

When you click the Portals node under Oracle Enterprise Manager, ADP displays summary information on active portal applications. This summary includes the following (Table 22–7):

Table 22–7 Tree Summary

Metric	Description
Portal web application activity	A summary of user sessions for a specific portal application
Portal completions	Total number of requests fulfilled by a specific portal application
Portal response time (ms)	Average response time for a specific portal application
Portal entitlement response time	Average response time of WebLogic Portal entitlement subsystem for a specific portal application
Portal campaign response time	Average response time of WebLogic Portal campaign subsystem for a specific portal application

For Portal web application activity and Portal performance, ADP displays information in both table and graph formats. For the other metrics, ADP shows the information in graph format. When you click the plus (+) icon next to the Portals node, ADP expands the tree to show all managed portal applications currently deployed on the WebLogic domain.

You can also see information specific to a particular portal application. By selecting a specific portal application, all information displayed in the Main Display Window changes to only show data relevant to this new context. For example, when a user selects a particular portal application under the Portals node, the Main Display Window only shows information specific to that portal application.

At the Portal level, you can navigate to different levels of the portal application by using different tabs. Use the tabs available to quickly access lower level components. Table 22–8 provides a list of the tabs available for portal level nodes and their descriptions.

Table 22–8 Portal Level Tab Description

Tab	Description
Summary	Performance summary specific to the selected portal.
Desktops	Performance summary for all the desktops associated with the selected portal.
Headers	Performance summary for all the headers associated with the selected portal.
Books	Performance summary for all the books associated with the selected portal.
Pages	Performance summary for all the pages associated with the selected portal.
Portlets	Performance summary for all the portlets associated with the selected portal.
Footers	Performance summary for all the footers associated with the selected portal.
WSRP Topology	View WSRP consumer-producer relationships and WSRP deployment topology.
Analysis	Two performance analytics - Multi-Point Regression Analysis performed at the portal level and Entity Performance Ranking performed at the portlet level.
Events	SLO violation events associated with the selected portal.
Errors/Exceptions	Errors metrics associated with the selected portal.
Transactions	Transaction events associated with the selected portal and children below. Be default, the Transactions tab is not enabled. To enable the Transactions tab, enable the UIProvider.Modes=product,trace property in the Acsera.properties file before starting the manager.

22.2.3.1 Desktops

Expand a particular portal application further to reach the Desktops node. By selecting the Desktops node, ADP provides a list of currently active desktops associated with that portal application.

This Desktop Summary includes the following metrics:

Table 22–9 Desktop Summary Metrics

Metrics	Description
Desktop arrivals	Total number of requests for a specific desktop
Desktop completions	Total number of requests fulfilled by a specific desktop
Desktop response time (ms)	Average response time for a specific desktop.

Note: Portal desktops are end-user facing entities. Metrics such as Desktop hits and response time represents request arrival rate and application performance respectively. Violations in thresholds set on these metrics would indicate unacceptable end-user experience.

ADP displays these metrics in both table and graph formats.

For example, when you have two active desktops, you can drill down further to a specific desktop by expanding the Desktops node. Again, clicking on the plus (+) icon expands the tree view for you.

When you select a node in the expanded tree to get more information specific for that desktop, ADP changes information in the Main Display Window to reflect the new context.

ADP not only shows the performance metrics associated with a specific node, but it also displays other relevant settings for that node. For example, there can be pre-configured Service Level Objectives (s). These SLOs are displayed in the graphs as red lines.

Expand the desktop node to see Header, Footer, and Books. You can see detailed information for these components by clicking on the appropriate nodes.

22.2.3.1.1 Display Portal Desktop - Desktop Structure Viewer One of the unique capabilities of ADP is its automatic discovery and modeling of deployed applications. The Desktop Structure Viewer provides visibility into how a portal desktop is organized. To activate the Desktop Structure Viewer, right-click on a specific desktop. Select the Display Portal Desktop menu option to access the Desktop Structure Viewer.

After the Desktop Structure Viewer appears, you can navigate through the portal desktop structure by clicking on the appropriate book, page, or portlet. The ability to see portal desktop structure using the same perspective as portal end-users is a unique value especially for the IT support staff.

With the Desktop Structure Viewer, the IT support staff can speak the same language with end-users while at the same time looking at performance oriented information for a specific component. The IT support staff can also use the Desktop Structure Viewer to isolate a particular performance problem. By drilling down from the top-level desktop to individual portlets, the IT support staff can get more insight into which components are having performance problems.

The Desktop Structure Viewer consists of two main panes. The pane on the left is the Desktop Structure pane. This pane allows you to graphically navigate the portal desktop. The pane on the right is called the Main Display Window. The Main Display window displays performance information in the context of the selected component in the Desktop Structure pane. As you navigate through the portal desktop and click different components, the Main Display Window provides information relevant for that selected context.

The Main Display Window shows relevant performance metrics for different portal desktop components - desktop, books, pages, and portlets.

Since ADP understands the WebLogic Portal framework and knows that a pageflow can be associated with a portlet, it is designed to allow easy access to the Pageflow Viewer from the Desktop Structure Viewer.

To activate the Pageflow Viewer, double-click the interesting portlet. In turn you can double-click the portlet in the Desktop Structure pane to open the appropriate pageflow in the Pageflow Viewer.

22.2.3.2 Portlet Drill Down

You can drill down on a portlet in the portal desktop view to activate the Display Architecture View.

1. Select a portlet under a node.

2. Double-click on a name to see the Portal Desktop Status page.
3. In the Portal Desktop Status window, right-click on a service box to select Display Architecture View.

22.2.3.3 Pageflow Viewer

The Pageflow Viewer has two panes. The pane on the right is the Main Display Window. The Main Display Window shows information corresponding to the item selected in the left pane. The left pane shows either the Flow View or the Component View. You can choose to see either the Flow View or the Component View by selecting the appropriate tab.

The Main Display Window changes to show information relevant to the selected item in either the Flow View or the Component View.

22.2.3.4 Books

Expand a particular portal desktop further to see the Books node. By selecting the Books node, ADP provides a list of currently active books associated with the specific desktop.

This Books Summary includes the following metrics (Table 22–10):

Table 22–10 Book Summary Metrics

Metrics	Description
Book completions	Total number of requests fulfilled by a specific book
Book response time (ms)	Average response time for a specific book

ADP displays these metrics in both table and graph formats. For example, you can have two active books for the portal desktop. These active books are listed in the table and plotted in the graphs.

You can drill down further to a specific book by expanding its node. Click the plus (+) icon to expand the tree view. Expand the Books node to see a list of specific books configured.

When you select a particular active book, the Main Display Window shows the relevant information in that context.

22.2.3.5 Pages

Expand a particular book to see the Pages node. By selecting the Pages node, ADP provides a list of currently active pages associated with the specific book.

This Pages Summary includes the following metrics (Table 22–11):

Table 22–11 Pages Summary Metrics

Metrics	Description
Page completions	Total number of requests fulfilled by a specific page
Page response time (ms)	Average response time for a specific page

ADP displays these metrics in both table and graph formats. For example, you can have one active page for a book. The active page is listed in the table and plotted in the graphs.

You can drill down further to a specific page by expanding the Pages node. Click the plus (+) icon to expand the tree view. This reveals the next level of components - Portlets.

22.2.3.6 Portlets

Expand a particular page to see the Portlets node. Select a Portlets node to view a list of currently active portlets associated with the specific page.

This Portlets Summary includes the following metrics (Table 22–12):

Table 22–12 Portlet Metrics

Metrics	Description
Portlet completions	Total number of requests fulfilled by a specific portlet.
Portlet response time (ms)	Average response time for a specific portlet.

ADP displays these metrics in both table and graph formats. For example, you can have four active portlets for a particular page. These active portlets are listed in the table and plotted in the graphs.

Drill down further to a specific page by expanding the Portlets node. Click the (plus) + icon to expand the tree view. This provides additional information about the page.

22.2.4 Oracle BPEL Processes

The BPEL Processes node in the navigation tree contains information about all deployed Oracle BPEL processes within the managed domain. ADP organizes information for various process nodes into domains.

In the right-hand pane, you can view the minimum and maximum response time measurements stored in the database in addition to the average response time, arrivals, errors, and completions measurements. These metrics, if present, display visually in the window on the right pane.

When you select the root of the BPEL Processes tree, ADP displays the BPEL Processes Summary in the Main Display Window.

The BPEL Process Summary includes the following (Table 22–13):

Table 22–13 BPEL Process Summary Metrics

Metrics	Description
Domain	Name of the OC4J domain container
Process	Name of the BPEL process
Arrivals	Total number of currently running instances for a specific BPEL process
Response Time (ms)	Average response time in milliseconds for a specific BPEL process
Completions	Total number of fulfilled requests for a specific BPEL process. A Completed status represents a BPEL process instance that has finished normally.
Errors	Total number of aborted instances of a specific BPEL process
Min Response Time (ms)	Minimum average response time in milliseconds for a specific BPEL process
Max Response Time (ms)	Maximum average response time in milliseconds for a specific BPEL process

ADP presents these metrics in a table format in the Main Display Window when you select the BPEL Processes node. Graphical representations of two metrics, Arrivals and Completions, are displayed below the table.

When you click the plus (+) icon next to the domains sub-node under the main BPEL Processes node, ADP expands the tree to show all managed BPEL domains currently deployed on that particular Oracle SOA Suite instance.

You can see information specific to a particular process. By selecting a specific process, all information displayed in the Main Display Window changes to only show data relevant to this new context.

To see the BPEL process work flow associated with a BPEL process, select the node, right-click and select the Display Functional View option. ADP displays the appropriate functional work flow diagram and associated performance data in a new pop-up window.

See Table 22–14 for BPEL Functional View summary.

Table 22–14 BPEL Functional View Summary

Column/Metric	Description
Activity	Name of a specific activity in the BPEL process
Type	Control Type for a specific node
Arrivals	Number of requests that have arrived for a specific node
Response Time (ms)	Average response time for a specific node
Completions	Number of completed requests for a specific node
Errors	Number of aborted instances for a specific node
Response Time Min (ms)	Minimum response time for a specific node
Response Time Max (ms)	Maximum response time for a specific node

By looking at this summary table, you can determine which BPEL process node is running slowly and whether there are errors.

In addition to the summary, the following views are available for a node:

- Delay Analysis view
- Metadata view
- Partner Links view
- Partner Link Type Role view
- Partner Link Bindings view
- Modeled Entities view
- Topology view

You can get to these views by selecting the appropriate tab.

22.2.4.1 Delay Analysis View

Delay Analysis gives you a bird's eye view of a specific BPEL process. You can see what nodes in the BPEL process are taking up a majority of the average elapsed time. The red bar indicates the slowest BPEL process group or BPEL process node. The blue represents the time spent for the particular nodes.

22.2.4.2 Metadata View

The Metadata view displays the tables containing specific metadata associated with the selected active BPEL process being displayed in the left-hand pane. Information provided in this view includes caller and called class metadata information as well as general summarized metadata in relation to the BPEL process and the associated web services. Table 22–15 explains the metadata.

Table 22–15 Metadata View Summary

Column/Metric	Description
SummaryTable -Process	Name of the BPEL process node
SummaryTable -Web Service	Name of the web service being called from the BPEL process
SummaryTable -Version	Version of the web service being called from the BPEL process
SummaryTable -Location	Location of the web service being called from the BPEL process
Caller Table - Caller Class	Class name for the caller class that is calling the BPEL process
Caller Table - Caller Method	Class method for the caller class that is calling the BPEL process
Caller Table -Target Host	Target host that the caller class targeted to instantiate the BPEL process
Caller Table -Target Port	Target port that the caller class targeted to instantiate the BPEL process
Caller Table -Target URL	Target URL that the call class targeted to instantiate the BPEL process
Caller Table - Invocation Count	Number of invocations of the BPEL process instantiated by the caller class
Caller Table - Response Time	Average response time of the BPEL process instantiated by the caller class
Called Clients Table - Called Class	Class name of the class that was called by the BPEL process
Called Clients Table - Target URL	Target URL of the class that was called by the BPEL process
Called Clients Table - Invocation Count	Number of invocations made from the BPEL Process to the called class.
Called Clients Table - Response Time	Response time of the called class

22.2.4.3 Partner Links View

The partner links view provides detailed information on the various roles related to how and why the partner link service is being utilized. The information provided includes both the caller and callee roles, as well as the partner link type. See Table 22–16.

Table 22–16 Partner Links View Summary

Column/Metric	Description
Partner Link	Name of the partner link
My Role	Role in regards to the BPEL process calling the partner link service
Partner Role	Role of the partner link service
Partner Link Type	Partner link category (type) of the service being called

22.2.4.4 Partner Link Type Role View

See Table 22–17 describes the columns in the Partner Link Type Role view.

Table 22–17 Partner Link Type Role View Summary

Column/Metric	Description
Name	Name of the partner link
Link Type Name	Category (type) of the partner link
Port Type	Partner link service URL

22.2.4.5 Partner Link Bindings View

The Partner Link Bindings view provides insight into the actual roles and types of the partner link instances which represent web services that have been bound by the BPEL process. See Table 22–18.

Table 22–18 Partner Link Bindings View Summary

Column/Metric	Description
Partner Link Role	Defines the web service role that the BPEL process will communicate with
Partner Link Type	Defines the web service type that the BPEL process will communicate with
WebService PortType	Name of the web service
WebService Port Namespace ID	URL of the webservice instance

22.2.4.6 Modeled Entities View

The modeled entities view consist of a list and count of the general entities as catalogued during the discovery phase of the resource configuration. The tables contain both a total entity count as well as a breakdown of the entity count by entity type. See Table 22–19.

Table 22–19 Modeled Entities Summary

Column/Metric	Description
Total Entities Modeled Table - Total	Total entities (static label)
Total Entities Modeled Table - Count	Total number of entities catalogued during the discovery phase of the BPEL process
Modeled Entities Table - Entity Type	Entity type being catalogued as part of the discovery phase of the BPEL process
Modeled Entities Table - Count	Total number of entities catalogued during the discovery phase of the BPEL process for a particular entity type

22.2.4.7 Topology View

The Topology View utilizes the modeled entities that were captured during the discovery process to provide a bird's eye view of all of the various high-level relationships between BPEL processes, web services, and business services. You can toggle between static and dynamic relationship views using the tabs at the top of the Topology pane.

22.2.4.8 Node Hierarchy

Expanding a particular BPEL process further, the first item you see is the Node Hierarchy node. By selecting the Node Hierarchy node, ADP provides a list of nodes associated with the specific process.

When you click the plus (+) icon next to a specific Node Hierarchy node, ADP expands the tree to show BPEL process nodes in the Node Hierarchy. Click an individual BPEL process node to see the load and performance of the selected node in the Main Display Window.

The BPEL process node information also includes the name of the method invoked. This information is displayed as part of the summary table at the top of the main view window.

22.2.5 Oracle ESB

The Oracle ESB node under Oracle Enterprise Manager contains information about all of the deployed Oracle ESB servers running in the managed domain. ADP organizes the information for various Oracle ESB nodes into various categories.

When you select the root of the ESB tree, ADP displays the ESB Summary in the Main Display Window.

The ESB Summary includes the following (Table 22–20):

Table 22–20 ESB Summary Metrics

Metric	Description
ESB System	Name of ESB System
ESB Service	Name of the ESB Service identifier
Arrivals	Total number of ESB service instance arrivals
Completions	Total number of ESB service instance completions
Response Time	Total number of completed instances for a specific BPEL process. A Completed status represents a BPEL process instance that has finished normally.

ADP presents these metrics in a table format in the Main Display Window when you select the ESB node. When you click the plus (+) icon next to the ESB Systems sub-node under the main ESB node, ADP expands the tree to show all managed ESB Systems currently deployed on that particular Oracle SOA Suite instance.

You can see information specific to a particular ESB System. By selecting a specific ESB System, all information displayed in the Main Display Window changes to only show data and the topology relevant to this new context.

By looking at the summary table, you can find out which ESB node is running slowly and whether there are errors.

Besides the summary, the following views are available for the Node Hierarchy node:

- Service Details view
- Service Parent Details view
- Service Definition view
- Service Operations view
- Operation Routing Rules view
- Topology view

You can get to these views by selecting the appropriate tab.

22.2.5.1 Service Details View

The Service Details view provides specific information related to the details of the bound service process instances. Instance IDs and other descriptive details are included as part of this view. See Table 22–21.

Table 22–21 Service Details View Summary

Column/Metric	Description
Service Name	Name of the ESB service
GUID	GUID of the ESB service
Qname	Canonical qualified name for the bound ESB service
Description	Description of the ESB service

22.2.5.2 Service Parent Details View

The Parent Service Details view provides specific information related to the details of the parent of the bound service process instances. Instance IDs, roles, and other descriptive details are included as part of this view. See Table 22–22.

Table 22–22 Service Parent Details View Summary

Column/Metric	Description
Service Name	Name of the parent ESB service
ParentGUID	GUID of the parent ESB service
ParentQname	Canonical qualified name for the parent of the bound ESB service
ParentType	Parent type of the parent ESB service
MyRole	Role of the caller of the parent ESB service instance
ParentRole	Role of the callee of the parent ESB service instance

22.2.5.3 Service Definition View

The Service Definition view contains information regarding the bound ESB service including the Business Service (ESB) WSDL and Port Type as well as the associated URLs. See Table 22–23.

Table 22–23 Service Definition View Summary

Column/Metric	Description
Service Name	Name of the ESB service
BusinessServiceWSDL	URL of the Business Service WSDL
BusinessServicePortType	Port type of the Business Service
ConcreteServiceWSDL	URL of the Concrete Service WSFL
ConcreteServiceURI	URI for the concrete service

22.2.5.4 Service Operations View

The Service Operations views provides details regarding the various method operations being executed. All information is provided in regards to the metadata associated with a specific business service instance. See Table 22–24.

Table 22–24   Service Operations View Summary

Column/Metric	Description
Service Name	Name of the ESB service
Name	Service operation name being executed
GUID	GUID of the ESB service
Qname	Canonical qualified name for the bound ESB service
Element	Associated element within the ESB Service
SchemaLocation	Schema location for the associated ESB service
Type	Type of ESB service operation

22.2.5.5 Operation Routing Rules View

The Operation Routing Rules view provides various details regarding the operation routing rules for Business Service operations. This includes the specific instance business service names being utilized for operations. See Table 22–25.

Table 22–25   Operation Routing Rules View Summary

Column/Metric	Description
Service Name	Name of the ESB service
Name	Instance name ID of the ESB service instance
GUID	GUID of the ESB service instance

22.2.6 Oracle WebCenter

Oracle WebCenter provides a set of features and services (for example, portlets, customization, and content integration) that simplify the process of reaching a solution with JSF applications. This solution brings information from multiple sources into a single interface, simplifying transactions and providing everything users need to support a given task within the application itself.

Table 22–26   WebCenter Tree Summary

Component	Description
ADF Business Components	ADF business component
ADF Data Controls	ADF data controls
ADF Taskflows	ADF task flows provide a modular approach for defining control flow in an application. See Section 22.2.6.1, "ADF Task Flows".
JSF Pages	JSF page definition files define the binding objects that populate the data in UI components at runtime. See Section 22.2.6.2, "JSF Pages".
Portlets	Portlets are the containers that surface Web content and applications on desktops. See Section 22.2.6.3, "Portlets".

22.2.6.1 ADF Task Flows

Instead of representing an application as a single large JSF page flow, you can break it up into a collection of reusable task flows. Each task flow contains a portion of the application's navigational graph. The nodes in the task flows are activities. An activity node represents a simple logical operation such as displaying a view, executing application logic, or calling another task flow. The transactions between the activities are called control flow cases. A task flow consists of activities and control flow cases that define the transitions between activities.

22.2.6.1.1 User-Defined Taskflows The following taskflows are available in WebCenter.

Table 22–27 Taskflow Activities

Activity Name	Description
Managed Beans	A backing bean that is managed by the JSF framework and used during the JSF page lifecycle.
Taskflow Method Calls	Invokes a method, typically a method on a managed bean.
Taskflow Views	Displays a JSF page or page fragment. Multiple view activities can represent the same page or same page fragment.
Taskflow URL Views	Redirects the root view port (for example, a browserpage) to any URL-addressable resource, even from within the context of an ADF region.
Taskflow Calls	Calls an ADF bounded task flow from an ADFunbounded task flow or another bounded task flow
Routers	Evaluates an EL expression and returns an outcome based on the value of the expression. For example, a router in a credit check task flow might evaluate the return value from a previous method call and generate success, failure, or retry outcomes based on various cases. These outcomes can then be used to route control to other activities in the task flow.

22.2.6.1.2 Web 2.0 Service Oracle WebCenter provides a wide range of Web 2.0 capabilities, including discussion forums, wikis, blogs, content services, RSS, presence, instant messaging, linking, tagging, and search. Both developers and business users can easily add these services to their pages to maximize productivity.

Table 22–28 Taskflow Activities

Activity Name	Description
Managed Beans	A backing bean that is managed by the JSF framework and used during the JSF page lifecycle.
Taskflow Method Calls	Invokes a method, typically a method on a managed bean.
Taskflow Views	Displays a JSF page or page fragment. Multiple view activities can represent the same page or same page fragment.
Taskflow URL Views	Redirects the root view port (for example, a browserpage) to any URL-addressable resource, even from within the context of an ADF region.
Taskflow Calls	Calls an ADF bounded task flow from an ADFunbounded task flow or another bounded task flow
Routers	Evaluates an EL expression and returns an outcome based on the value of the expression. For example, a router in a credit check task flow might evaluate the return value from a previous method call and generate success, failure, or retry outcomes based on various cases. These outcomes can then be used to route control to other activities in the task flow.

22.2.6.2 JSF Pages

A typical JSF application couples a backing bean with each page in the application. The backing bean defines properties and methods that are associated with the UI components used on the page. The UI component's value is bound to the bean's property.

A Managed Bean is a backing bean that is managed by the JSF framework and used during the JSF page lifecycle.

22.2.6.3 Portlets

Portlets can display excerpts of other Web sites, generate summaries of key information, perform searches, and access assembled collections of information from a variety of data sources. You can use the portlets that Oracle or third parties provide, or create your own programmatically. Oracle WebCenter supports WSRP 1.0, WSRP 2.0, JSR 168, and Oracle PDK-Java. You can include any portlets adhering to those standards in your WebCenter applications.

22.2.6.4 Monitoring WebCenter Performance

Perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the WebCenter target. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.

2. Click the **Monitoring** tab, then select the application in the tree.

3. ADP discovers the deployed WebCenter ADF artifacts on the configured Oracle WebLogic Domain.

4. A WebCenter node appears under the configured ADP Manager (for example, Oracle Enterprise Manager, select Server, then select WebCenter). The WebCenter node contains the ADF Application Name and the following subnodes:

   - ADF Taskflows
   - JSF Pages
   - Managed Beans

The performance metrics for related components are displayed on the right-hand side panel when the respective component is selected.

22.2.7 Processes

The Processes node under Oracle Enterprise Manager contains information about all deployed WebLogic business processes in the managed domain. ADP organizes information for various process nodes into the following major categories:

- Node Hierarchy
- Persistent Containers
- Instrumentation

The minimum and maximum response time measurements are stored in the database in addition to the average response time measurements. These metrics, if present, display visually in the window on the right pane.

When you select the root of the Processes tree, ADP displays the Processes Summary in the Main Display Window. See Table 22–29.

Table 22–29 Process Summary Metrics

Metrics	Description
Process	Name of process
Running	Total number of currently running instances for a specific process
Suspended	Total number of suspended instances for a specific process. A Suspended request from a user is a common cause for a process instance to go into a Suspended state.

Table 22–29 (Cont.) Process Summary Metrics

Metrics	Description
Frozen	Total number of frozen instances for a specific process
Completed	Total number of completed instances for a specific process. A Completed status represents a process instance that has finished normally.
Aborted	Total number of aborted instances for a specific process
Terminated	Total number of terminated instances for a specific process. An external Terminate request would terminate a process instance.
Average Execution Time (ms)	Average execution completion time for a specific process

> **Tip:** Statistics on the number of process instances with Terminated, Aborted, and Frozen states can indicate abnormal operation of the WebLogic Integration application or container. It is possible to unfreeze Frozen process instances from WLI Console.

ADP presents these metrics in a table format in the Main Display Window when you select the Processes node. Graphical representations of two metrics, Running Instances and Average Execution Time, are displayed below the table.

When you click the plus (+) icon next to the Processes node, ADP expands the tree to show all managed processes currently deployed on the WebLogic domain.

You can see information specific to a particular process by selecting a specific process. All information displayed in the Main Display Window changes to only show data relevant to this new context.

To see the process work flow associated with a particular process, select the process node, right-click and select the Display Functional View option. ADP displays the appropriate functional work flow diagram and associated performance data in a new pop-up window.

22.2.7.1 Node Hierarchy

When expanding a particular process further, the first item you see is the Node Hierarchy node. By selecting the Node Hierarchy node, ADP provides a list of nodes associated with the specific process. See Table 22–30.

Table 22–30 Node Hierarchy Summary

Column/Metric	Description
Node	Name of a specific node
ID	Process Node ID for a specific node
Type	Control Type for a specific node
Method	Node Method Name for a specific node
Arrivals	Number of Requests Arrived for a specific node
Active	Number of Active Instances for a specific node
Elapsed Time (ms)	Average Time Elapsed to Complete an Instance for a specific node
Completions	Number of Completed Instances for a specific node
Aborts	Number of Aborted Instances for a specific node
Exceptions	Number of Exception Encountered for a specific nod.

By looking at this summary table, you can determine which process node is running slowly and whether there are aborts or exceptions.

The following additional views are available for the Node Hierarchy node:

- Delay Analysis view
- Events view

You can get to these views by selecting the appropriate tab.

22.2.7.1.1 Delay Analysis View Delay Analysis gives you a bird's eye view of a specific process. You can see what nodes in the process are taking up a majority of the average elapsed time. The red bar indicates the slowest process group or process node. The blue represents the time spent for the particular nodes.

22.2.7.1.2 Events View The Events view shows a list of SLO violations events relevant to this process in a table format. The Events view table includes the following information (Table 22–31):

Table 22–31 Events View Summary

Column/Metric	Description
Start Time	Start time for the process instance that violated a SLO
Entity Name	Name of the process node that violated a SLO
SLO Name	Name of the violated SLO
Service URI	URI of the process that violated a SLO
Application	Name of the application that violated a SLO
Event Type	Violation type (violation or cautionary)
Entity Type	Violation Metric type
SLO Threshold	Type of threshold (high or low)
SLO Trigger Value	Value that triggered a SLO violation

When you click the plus (+) icon next to a specific Node Hierarchy node, ADP expands the tree to show process nodes in the Node Hierarchy. Click an individual process node to see the load and performance of the selected node in the Main Display Window.

The process node information also includes the name of the method invoked. This information is displayed as part of the summary table at the top of the main view window.

22.2.7.2 Persistent Containers

When you expand a particular process further, the Persistent Containers node is included. By selecting the Persistent Containers node, ADP provides a list of persistence performance statistics relevant to the selected process.

As you select the root of the Persistent Containers tree, a summary of all Persistent Containers relevant to the selected process is presented. For example, a summary can contain the following high level items:

- Container persistence invocations
- Container persistence response time (milliseconds)
- Entity EJB activity

- Entity EJB cache
- Entity EJB transactions
- Entity EJB locking

These items are displayed in both table and graph formats.

The Persistent Containers Summary includes different tables:

- Entity EJB Activity
- Entity EJB Cache
- Entity EJB Transactions
- Entity EJB Locking

22.2.7.2.1 Entity EJB Activity Table Entity EJB Activity table (Table 22–32) includes the following information:

Table 22–32 Entity EJB Activity Table

Metrics	Description
EJB	Name of the Entity EJB
In Use	Number of instances for a specific Entity EJB currently being used from the free pool. [Snapshot Count]
Idle	Number of instances for a specific Entity EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of Threads currently waiting for a specific Entity EJB bean instance from the free pool [Snapshot Count]
Timeouts	Total number of Threads that have timed out waiting for an available bean instance from the free pool [Aggregated Count]

> **Tip:** Pay attention to Waits and Timeouts metrics. Activities in the Waits metric and increasing count in the Timeouts metric are signs that requests waiting to be serviced by the EJB container. Ideally, 0 should be indicated for these metrics.

22.2.7.2.2 Entity EJB Cache Table Entity EJB Cache table (Table 22–33) includes the following information:

Table 22–33 Entity EJB Cache Table

Metrics	Description
EJB	Name of the Entity EJB
Hits	Total number of times an attempt to access the Entity EJB instance from the cache succeeded [Aggregated Count]
Accesses	Total number of attempts to access the Entity EJB instance from the cache [Aggregated Count]
Size	Number of beans instances from this EJB Home currently in the EJB cache [Snapshot Count]
Activations	Total number of beans from this EJB Home that have been activated [Aggregated Count]
Passivations	Total number of beans from this EJB Home that have been passivated [Aggregated Count]

Tip: Passivation (serializing EJB state information to disk) and activation (reconstituting EJB state information from disk) are resource intensive operations. Ideally, it is preferable to see low level of activity in these metrics.

22.2.7.2.3 Entity EJB Transactions Table Entity EJB Transactions table (Table 22–34) includes the following information:

Table 22–34 Entity EJB Transactions Table

Metrics	Description
EJB	Name of the Entity EJB
Commits	Total number of transactions that have been committed for this EJB. [Aggregated Count]
Rollbacks	Total number of transactions that have been rolled back for this EJB. [Aggregated Count]
Timeouts	Total number of transactions that have timed out for this EJB. [Aggregated Count]

Tip: High number of EJB Transaction Rollbacks may indicate problems with the data used - for some reason the target database is unable to commit the change. High number of EJB Transaction Timeouts may indicate problems accessing the database including network outage, database lock contention, database outage, and more.

22.2.7.2.4 Entity EJB Locking Table Entity EJB Locking table (Table 22–35) includes the following information:

Table 22–35 Entity EJB Locking Table

Metrics	Description
EJB	Name of the Entity EJB
Entries	Number of Entity EJB instances currently locked [Snapshot Count]
Lock Accesses	Total number of attempts to obtain a lock on an Entity EJB instance [Aggregated Count]
Current Waiters	Number of Threads that currently waiting for a lock on an Entity EJB instance [Snapshot Count]
Total Waiters	Total number Threads that have waited for a lock on an Entity EJB instance [Aggregated Count]
Timeouts	Total number Threads that have timed out waiting for a lock on an Entity EJB instance [Aggregated Count]

Tip: Pay attention to Current Waiters and Timeouts. These metrics can indicate possible performance problems caused by EJB Locking. Ideally, 0s should be displayed for these metrics.

By looking at the activities related to Persistence Containers, you can determine if EJB persistence calls are causing performance problems.

22.2.7.3 Instrumentation

When expanding a particular process further, the last item you see is the Instrumentation node. Click the plus (+) icon next to Instrumentation to expand the tree to reveal the following categories of instrumentation:

- Class

- Methods
- Errors/Exceptions
- Transactions

The Class node in the Instrumentation tree provides the following information (Table 22–36):

Table 22–36 Class Node

Column/Metric	Description
Probe Point	Class name in which instrumentation probe point is inserted
Response Time (ms)	Average response time for a specific class
Invocation Count	Number of times a specific class is called

The Method node in the Instrumentation tree provides the following information (Table 22–37):

Table 22–37 Method Node

Column/Metric	Description
Probe Point	Method name in which instrumentation probe point is inserted
Response Time (ms)	Average response time for a specific method
Invocation Count	Number of times a specific method is called

The Errors/Exceptions and Transactions are described in Section 22.1.10, "Architecture View".

22.2.8 Web Services

The Web Services node in the navigation tree contains information about all deployed Web Services in the managed domain. By selecting the Web Services node under Oracle Enterprise Manager, ADP shows the Web Services Summary in the Main Display Window.

This summary view lists all discovered web services and their associated URL entry points. Below this list, ADP lists out all active web services and their performance data (invocation count and response time).

When you click the plus (+) icon next to the Web Services node, ADP expands the tree to show all monitored web services currently deployed on the WebLogic domain.

When you select a specific web service, ADP displays performance data associated with the selected web service. Click the plus (+) icon next to a specific web service to expand the tree to show all public operations associated with that web service.

The Operations table provides the following information (Table 22–38):

Table 22–38 Operations Table

Column/Metric	Description
Operation	Name of the web service operation
Invocation Count	Number of times the operation is called
Response Time (ms)	Average response time for the operation in milliseconds

Table 22–38 (Cont.) Operations Table

Column/Metric	Description
Delay (ms)	Overall delay contributed by the operation in milliseconds

22.2.9 Pageflows

The Pageflows node in the navigation tree contains information about all deployed pageflows in the managed domain. By selecting the Pageflows node under Oracle Enterprise Manager, ADP shows the Pageflows Summary in the Main Display Window.

22.2.10 Services

The Services node in the navigation tree contains information about all external entry points into the managed domain. ADP currently monitors the following types of services:

- HTTP
- EJBs
- JDBC

Selecting each service type reveals service summary in the Main Display Window.

The minimum and maximum response time measurements are stored in the database in addition to the average response time measurements. These metrics, if present, display visually in the window in the right pane.

ADP displays entry point activity summary associated with the selected EJB service.

> **Tip:** Setting thresholds at some of these entry points enables ADP to monitor the performance of key business services. When a violation event occurs, you can begin investigating from the Service node.

22.2.10.1 HTTP

Expanding the HTTP node under the Services node reveals a list of discovered HTTP based entry points into the managed domain. HTTP service end points include JSPs, struts actions, and servlet mappings. These discovered HTTP entry points are listed by their root context. When you select a specific HTTP entry point, ADP displays the associated summary in the Main Display Window.

When a specific file is selected, ADP displays more detailed performance data.

Method level performance data is displayed when you select a specific HTTP service entry point.

Table 22–39 HTTP Performance Summary

Column/Metric	Description
Servlet	Name of the servlet associated with the selected service
Method	Name of the method invoked by external call
Arrivals	Total number of requests received by this method
Invocation Count	Total number of method invocations
Response Time (ms)	Average method response time in milliseconds

22.2.10.2 EJBs

To view the performance summary for EJBs invoked from outside the JVM, click the EJBs node.

Table 22–40 EJB Performance Summary

Column/Metric	Description
EJB	Name of the EJB
Invocation Count	Number of times the EJB is called
Response Time (ms)	Average response time for the EJB in milliseconds
Delay (ms)	Overall delay contributed by the EJB in milliseconds

> **Tip:** As a general rule, external calls that terminate in EJBs are RMI calls. Web services calls that ultimately terminate in EJBs use SOAP and enter the application server via HTTP.

22.2.10.3 JDBCs

To bring up the performance summary for JDBC operations invoked from outside of the JVM, click the JDBC node.

Table 22–41 JDBC Performance Summary

Column/Metric	Description
SQL Statement	Generalized SQL Statement executed by the JDBC operation
Class	Name of the class used in the JDBC operation
Method	Name of the method used in the JDBC operation
Invocation Count	Number of times the JDBC operation is called
Response Time (ms)	Average response time for the JDBC operation in millisecond
Delay (ms)	Overall delay contributed by the JDBC operation in milliseconds

22.2.11 WSRP Producers

The Web Services Remote Portlet (WSRP) Producers node in the navigation tree contains information about the WebLogic WSRP consumer - producer relationships in the managed domain. By selecting an entity in the WSRP node, ADP displays the performance measurements for the associated WSRP consumer or producer.

WebLogic Portal can act as either a WSRP remote producer or as a consumer. When acting as a consumer, WebLogic Portal's remote--or proxy--portlets are WSRP-compliant. These portlets present content that is collected from WSRP-compliant producers, allowing you to use external sources for portlet content, rather than having to create its content or its structure yourself.

The following types of portlets can be exposed with WSRP inside a WebLogic portal:

- Page flow portlets
- JavaServer Pages (JSP) portlets
- Struts portlets
- Java portlets (JSR168; supported only for complex producers)
- JavaServer Faces (JSF) portlets

The minimum and maximum response time measurements are captured in addition to the average response time measurements. These metrics, if present, display visually in the window in the right pane.

22.2.11.1 WSRP Summary

To view the WSRP Producers Summary:

1. Select the WSRP Producers node to show the WSRP Producers Summary tab.

   The WSRP Producers summary includes the following table (Table 22–42):

Table 22–42 WSRP Producers Summary

Column	Description
WSRP Producer	Name of the producer portlet
WSDL URL	URL of the WSD.

2. To view the portlet details, click the Consumer Portlets node under the WSRP Producers.

   The following tables are in this view:

   - WSRP Producer Information
   - WSRP Consumer Portlet Performance

     Select the portlet name and right click. Select **Open** to drill down to more detailed view.
   - WSRP Producer Portlets

     Select the portlet name and right click. Select Open to drill down to more detailed view.

Table 22–43 WSRP Producers Information

Column	Description
TestPortlets	Defined by the user for the Producer, for example description, handle, and more
URL	Lists the details of each item under the TestPortlet column

Table 22–44 WSRP Consumer Portlet Performance

Column	Description
Portal	The Portal is the logical containment unit for a Portal application. A typical Portal can contain a few desktops, several of books, tens of pages, and hundreds of portlets.
Desktop	The desktop is the top-level container for the portal components included in that specific view of the portal. Portal administrators can create new desktops beyond what portal developers create in WebLogic Workshop.
Book	The top-level book contains all sub-books, pages, and portlets. The top-level book defines the initial menu navigation style used for the desktop. For each sub-book, you add to a desktop you can select a different navigation style.
Page	Pages and sub-books are the navigable containers used for organizing portlets.
Portlet	Portlets are the containers that surface Web content and applications in your desktops.
Response Time (ms)	Average response time in milliseconds.

Table 22–44 (Cont.) WSRP Consumer Portlet Performance

Column	Description
Completions	Number of Completed Instances for a specific node.
Response Time Min (ms)	Minimum response time in milliseconds.
Response Time Max (ms)	Maximum response time in milliseconds.

Table 22–45 WSRP Producer Portlets

Column	Description
Producer Portlet	Name of the producer portlet
Producer	Name of the producer

3. Click a portlet name in the tree view to see the performances associated with the consumer and producer portlets.

22.2.11.2 WSRP Topology

Use this option to visually explore WSRP consumer - producer relationships and the WSRP deployment topology.

To view the WSRP Topology:

1. Select the WSRP Producers node to show the WSRP Topology tab.
2. Click the WSRP Topology tab to view the details.

22.2.11.3 Display Portal Desktop

The portal desktop is described in Section 22.2.3.1.1, "Display Portal Desktop - Desktop Structure Viewer".

Access the Architecture View:

1. To view the portal desktop for a specific portlet, right-click the portlet name under the Consumer Portlet node.
2. Select Display Portal Desktop.
3. You can drill down to view the Architecture View from this view. See the instructions in Section 22.2.3.2, "Portlet Drill Down".

22.2.12 Integration

The Integration node under Oracle Enterprise Manager contains information about the WebLogic Integration resources in the managed domain. By selecting the Integration node under Oracle Enterprise Manager, ADP displays the Integration Summary.

The Integration Summary includes the following (Table 22–46):

Table 22–46 Integration Summary

Metric	Description
Process	Name of process
Running	Total number of currently running instances for a specific process
Suspended	Total number of suspended instances for a specific process

Table 22–46 (Cont.) Integration Summary

Metric	Description
Frozen	Total number of frozen instances for a specific process
Completed	Total number of completed instances for a specific process
Aborted	Total number of aborted instances for a specific process
Terminated	Total number of terminated instances for a specific process
Average Execution Time	Average execution completion time for a specific process

> **Tip:** Statistics on the number of process instances with Terminated, Abort, and Frozen states can indicate abnormal operation of WebLogic Integration application or container. It is possible to unfreeze Frozen process instances from WLI Console.

ADP presents these metrics in a table format in the Main Display Window when you select the Integration node. Graphical representations of these metrics, Running Instances, Completed Instances, and Average Execution Time, are displayed below the table.

Expand the Integration tree by clicking on the plus (+) icon next to Integration node.

The expanded Integration tree allows you to look at various components of WebLogic Integration and help identify performance bottlenecks. This section explains the nodes under the Integration Tree.

22.2.12.1 Health

In the expanded Integration tree, the first node you see is the Health node. Under the Health node, ADP lists various subsystems in WebLogic Integration. By expanding the Health node, you can see the following:

- Execute Queues
- Async Dispatchers
- Sync Dispatchers
- JMS Destinations
- Stateless Containers
- Persistent Containers

You can get to the health information specific to each of these subsystems by clicking the appropriate node. Also, you can get to a particular instance of a subsystem.

22.2.12.1.1 Execute Queues In the Execute Queues node, ADP provides operational statistics of each execute queues configured for WebLogic Integration. Select the Execute Queues node in the Monitor Workspace to display the Execute Queues Summary in the Main Display Window.

The Execute Queues Summary provides the following information (Table 22–47):

Table 22–47 Execute Queues Summary

Metric	Description
Execute Queue	Execute Queue ID
Aggregated Execute Queue	Aggregated execute queue statistics per resource

Table 22–47 (Cont.) Execute Queues Summary

Metric	Description
Idle Threads	Current number of idle threads in a specific Execute Queue
Pending Threads	Current number of pending threads in a specific Execute Queue
Requests	Total number of requests serviced for a specific Execute Queue
Total Threads	Total number of threads configured in a specific Execute Queue

> **Tip:** Pay attention to Idle Threads and Pending Threads counts. Rapidly decreasing Idle Threads count combined with rapidly increasing Pending Threads count can indicate a backup in the Execute Queue.

Use the following guidelines to adjust the Execute Queue Thread Count (Table 22–48):

Table 22–48 Guidelines to Adjust the Execute Queue Thread Count

Execute Queue Is Backed Up?	Application Is CPU Bound?	Adjustment Guideline
Yes	No	Increase execute queue thread count.
Yes	Yes	Decrease thread count and explore JVM or application issues that may be causing high CPU utilization.

ADP presents these metrics in a table format in the Main Display Window when you select the Health node. Graphical representations of these metrics, Idle Treads, Pending Threads, and Requests, are displayed below the table.

Expand the Health tree by clicking on the plus (+) icon next to Health node. You can get the same summary as previously described for a specific execute queue.

22.2.12.1.2 Async Dispatchers In the Async Dispatcher node, ADP provides operational statistics of each of the Async Dispatchers configured in WebLogic Integration. Select the Async Dispatchers node in the Monitor Workspace to show the Async Dispatchers Summary in the Main Display Window.

The Async Dispatcher Summary includes the following information (Table 22–49):

Table 22–49 Async Dispatcher Summary

Metric	Description
EJB	Name of the Message Driven EJB
In Use	Number of instances for a specific Message Driven EJB currently in use
Idle	Number of instances for a specific Message Driven EJB currently in the idle state
Waits	Number of instances for a specific Message Driven EJB currently in the wait state
Timeouts	Number of instances for a specific Message Driven EJB currently in the timeout state
Commits (Transaction)	Total number of commits performed for a specific Message Driven EJB
Rollbacks (Transaction)	Total number of transaction rollbacks performed for a specific Message Driven EJB
Timeouts (Transaction)	Total number of transaction timeouts performed for a specific Message Driven EJB

> **Tip:** Rapidly increasing counts in MDB Waits and Timeouts metrics may indicate a tuning opportunity for the MBD container. Furthermore, increasing numbers in the Transaction Rollbacks and Timeouts metrics may indicate issues interacting with the database. Ideally, these metrics should not increase rapidly.

ADP presents these metrics in a table format in the Main Display Window when you select the Async Dispatchers node. Graphical representation of one metrics, Message Driven EJB in use, is displayed below the table.

Expand the Async Dispatchers tree by clicking the plus (+) icon next to Async Dispatchers node. You can get the same summary as previously described for a specific async dispatcher.

22.2.12.1.3 Sync Dispatchers In the Sync Dispatchers node, ADP provides operational statistics of each of the Sync Dispatchers used by WebLogic Integration. Select the Sync Dispatchers node in the Monitor Workspace to show the Sync Dispatchers Summary in the Main Display Window.

The Sync Dispatcher Summary includes the following information (Table 22–50):

Table 22–50 Sync Dispatcher Summary

Metric	Description
EJB	Name of the Stateless EJB
In Use	Number of instances for a specific Stateless EJB currently in use
Idle	Number of instances for a specific Stateless EJB currently in the idle state
Waits	Number of instances for a specific Stateless EJB currently in the waits state
Timeouts	Number of instances for a specific Stateless EJB currently in the timeouts state

> **Tip:** Rapidly increasing counts in Stateless EJB Waits and Timeouts metrics may indicate performance issues and a tuning opportunity for the EJB container. Ideally, these metrics should not increase at a rapid pace.

ADP presents these metrics in a table format in the Main Display Window when you select the Sync Dispatchers node. Graphical representation of one metrics, Stateless EJB in use, is displayed below the table.

Expand the Sync Dispatchers tree by clicking on the plus (+) icon next to Sync Dispatchers node. You can get the same summary as previously described for a specific sync dispatcher.

22.2.12.1.4 JMS Destinations In the JMS Destination node, ADP provides operational statistics of each of the JMS Destinations used by WebLogic Integration. Select the JMS Destinations node in the Monitor Workspace to show the JMS Destinations Summary in the Main Display Window.

JMS Destination Summary includes the following tables: JMS destination message statistics and JMS destination byte statistics. The JMS destination message statistics table includes the following information (Table 22–51).

Table 22–51 JMS Destination Message Statistics

Column/Metric	Description
JMS Destination	Name of the JMS destination
Message Current	Number of JMS messages currently at a specific JMS destination
Message High	Maximum number of JMS messages at a specific JMS destination
Message Pending	Number of JMS messages pending to be delivered to a specific JMS destination
Message Received	Total number of JMS messages at a specific JSM destination

Tip: Pay attention to Message Pending metric. Too many pending messages in a specific JMS destination could result in a performance slowdown. Rapidly increasing count for the Message Pending metric may indicate a performance problem and a JMS destination tuning opportunity.

The JMS destination byte statistics table includes the following information (Table 22–52).

Table 22–52 JMS Destination Byte Statistics

Column/Metric	Description
JMS Destination	Name of the JMS destination
Byte Current	Byte count of JMS messages currently at a specific JMS destination
Byte High	Maximum byte count of JMS messages at a specific JMS destination
Byte Pending	Byte count of JMS messages pending to be delivered to a specific JMS destination
Byte Received	Total Byte count of JMS messages at a specific JMS destination

ADP presents these metrics in table format in the Main Display Window when you select the JMS Destinations node. Graphical representations of the following metrics, Message pending and Byte pending, are displayed below the table.

Expand the JMS Destinations tree by clicking on the plus (+) icon next to JMS Destinations node. You can get the same summary as described above for a specific JMS destination.

22.2.12.1.5 Stateless Containers In the Stateless Containers node, ADP provides operational statistics of each of the Stateless Containers used by WebLogic Integration. Select the Stateless Containers node in the Monitor Workspace to show the Stateless Containers Summary in the Main Display Window.

The Stateless Containers Summary includes the following information (Table 22–53):

Table 22–53 Stateless Containers Summary

Metric	Description
EJB	Name of the Stateless EJB
Stateless EJB Transactions	Runtime statistics. You can monitor stateless session EJBs using the metrics in this table.
In Use	Number of instances for a specific Stateless EJB currently being used from the free pool [Snapshot Count]

Table 22–53 (Cont.) Stateless Containers Summary

Metric	Description
Idle	Number of instances for a specific Stateless EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of Threads currently waiting for a specific Stateless EJB instance from the free pool [Snapshot Count]
Timeouts	Total number of Threads that have timed out waiting for an available bean instance from the free pool [Aggregated Count]

ADP presents these metrics in a table format in the Main Display Window when you select the Stateless Containers node. Graphical representation of one metrics, Stateless EJB in use, is displayed below the table.

Expand the Stateless Containers tree by clicking on the plus (+) icon next to Stateless Containers node. You can get the same summary as previously described for a specific stateless container.

22.2.12.1.6 Persistent Containers In the Persistent Containers node, ADP provides operational statistics of each of the Persistent Containers used by WebLogic Integration. Select the Persistent Containers node in the Monitor Workspace to show the Persistent Containers Summary in the Main Display Window.

The Persistent Containers Summary includes the following tables:

- Entity EJB Activity
- Entity EJB Cache
- Entity EJB Transactions
- Entity EJB Locking

Entity EJB Activity table includes the following information (Table 22–54):

Table 22–54 Entity EJB Activity

Metrics	Description
EJB	Name of the Entity EJB
In Use	Number of instances for a specific Entity EJB currently being used from the free pool [Snapshot Count]
Idle	Number of instances for a specific Entity EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of Threads currently waiting for a specific Entity EJB bean instance from the free pool [Snapshot Count]
Timeouts	Total number of Threads that have timed out waiting for an available bean instance from the free pool [Aggregated Count]

> **Tip:** Pay attention to Waits and Timeouts metrics. Activities in the Waits metric and increasing count in the Timeouts metric are signs that requests waiting to be serviced by the EJB container. Ideally, 0 should be indicated for these metrics.

Entity EJB Cache table includes the following information (Table 22–55):

Table 22–55 Entity EJB Cache

Metrics	Description
EJB	Name of the Entity EJB
Hits	Total number of times an attempt to access the Entity EJB instance from the cache succeeded [Aggregated Count]
Accesses	Total number of attempts to access the Entity EJB instance from the cache [Aggregated Count]
Size	Number of beans instances from this EJB Home currently in the EJB cache [Snapshot Count]
Activations	Total number of beans from this EJB Home that have been activated [Aggregated Count]
Passivations	Total number of beans from this EJB Home that have been passivated [Aggregated Count]

Tip: Passivation (serializing EJB state information to disk) and activation (reconstitute EJB state information from disk) are resource intensive operations. Ideally, Oracle recommends low level of activity in these metrics.

Entity EJB Transactions table includes the following information (Table 22–56):

Table 22–56 Entity EJB Transactions

Metric	Description
EJB	Name of the Entity EJB
Commits	Total number of transactions that have been committed for this EJB [Aggregated Count]
Rollbacks	Total number of transactions that have been rolled back for this EJB [Aggregated Count]
Timeouts	Total number of transactions that have timed out for this EJB [Aggregated Count]

Tip: High number of EJB Transaction Rollbacks may indicate problems with the data used - for some reason the target database is unable to commit the change. High number of EJB Transaction Timeouts may indicate problems accessing the database including network outage, database lock contention, database outage, and more.

Entity EJB Locking table includes the following information (Table 22–57):

Table 22–57 Entity EJB Locking

Metric	Description
EJB	Name of the Entity EJB
Entries	Number of Entity EJB instances currently locked [Snapshot Count]
Lock Accesses	Total number of attempts to obtain a lock on an Entity EJB instance [Aggregated Count]
Current Waiters	Number of Threads that currently waiting for a lock on an Entity EJB instance [Snapshot Count]
Total Waiters	Total number Threads that have waited for a lock on an Entity EJB instance [Aggregated Count]
Timeouts	Total number Threads that have timed out waiting for a lock on an Entity EJB instance [Aggregated Count]

> **Tip:** Pay attention to Current Waiters and Timeouts. These metrics can indicate possible performance problems caused by EJB Locking. Ideally, 0s should be displayed for these metrics.

ADP presents these metrics in a table format in the Main Display Window when you select the Persistent Containers node. Graphical representations of three metrics, Entity EJB in use, Entity EJB cache access, and Entity EJB lock access, are displayed below the table.

Expand the Persistent Containers tree by clicking on the plus (+) icon next to Persistent Containers node. You can get the same summary as previously described for a specific persistent container.

22.2.12.2 Performance

In the expanded Integration tree, the second node you see is the Performance node. ADP provides the Performance Summary for WebLogic Integration in the Main Display Window when the Performance node is selected.

The Performance Summary includes the following tables: Process Node and Events. The Process Node table provides performance information for various process nodes running in WebLogic Integration. It includes the following information (Table 22–58):

Table 22–58 Performance - Process Node Summary

Column/Metric	Description
Node	Name of a specific node
ID	Process Node ID for a specific node
Type	Control Type for a specific node
Method	Node Method Name for a specific node
Arrival	Number of Requests Arrived for a specific node
Active	Number of Active Instances for a specific node
Elapsed Time	Average Time Elapsed to Complete an Instance for a specific node
Completions	Number of Completed Instances for a specific node
Aborts	Number of Aborted Instances for a specific nod.
Exceptions	Number of Exception Encountered for a specific node

> **Tip:** You can use Arrivals and Elapsed Time data collected by ADP to characterize the performance of your installation. Since ADP measures performance at cluster level, you are capturing the actual performance of your configuration. You can also perform simple capacity planning analysis by plotting Arrivals versus Elapsed Time (arrival rate versus response time). Ask your Oracle consultant for more information.

The Events table provides a list of SLO violations triggered relevant to WebLogic Integration. It includes the following information (Table 22–59):

Table 22–59 Performance - Events Node Summary

Column/Metric	Description
Start Time	Start time for the process instance that violated a SLO

Table 22–59 (Cont.) Performance - Events Node Summary

Column/Metric	Description
Entity Name	Name of the process node that violated a SLO
SLO Name	Name of the violated SLO
Service URI	URI of the process that violated a SLO
Application	Name of the application that violated a SLO
Event Type	Violation type (violation or cautionary)
Entity Type	Violation Metric type
SLO Threshold	Type of threshold (high or low)
SLO Trigger Value	Value that triggered a SLO violation

22.2.12.3 Channels

In the expanded Integration tree, the third node you see is the Channels node. ADP shows the Channels Summary for various channels configured for WebLogic Integration.

The Channels Summary includes the following information (Table 22–60):

Table 22–60 Channels Summary

Column/Metric	Description
Channel	Name of channel
Type	Channel type
Message Count	Total number of messages processed for a specific channel
Dead Message Count	Total number of dead messages for a specific channel

> **Tip:** Increasing count in the Dead Message Count metric may indicate a configuration issue. When the Message Broker is unable to determine the URI to send a message to, the message is sent to the appropriate deadletter channel. Ensure the URI configured for the channel is reachable.

Expand the Channels tree by clicking the plus (+) icon next to Channels node. You can get the same health summary as previously described for a specific channel.

22.2.12.4 Subscribers

In the expanded Integration tree, the fourth node you see is the Subscribers node. ADP shows the Subscribers Summary for various subscribers configured for WebLogic Integration.

Expand the Subscribers tree by clicking the plus (+) icon next to Subscribers node. You can get specific information about an individual subscriber.

22.2.13 Applications

The Applications node in the navigation tree contains information about all deployed applications in the managed domain. By selecting the Applications node, ADP displays the Applications Summary.

The Applications Summary includes the following information (Table 22–61, " Applications Summary"):

Table 22–61 Applications Summary

Column/Metric	Description
Application	Name of application
Status	Operations status for a specific application
Response Time (ms)	Average response time in milliseconds for a specific application. This is the average of response times of all JSPs and servlets contained in the deployment archive.
Invocation Count	Total number of invocations for a specific application. This is the total invocation count of all JSPs and servlets contained in the deployment archive.

Tip: Application is a packaging unit in Java EE. Each EAR, WAR, and JAR files deployed to the application server is considered an individual application. These metrics track performance and arrival rate of these entities.

ADP presents these metrics in a table format in the Main Display Window when you select the Applications node. Graphical representations of the following metrics, Response Time, Invocation Count, and Active Sessions, are displayed below the table.

Expand the Applications tree by clicking the plus (+) icon next to Applications node. You can get more information about a specific application.

ADP displays performance summary for the selected application in the Main Display Window. You can obtain additional performance data by clicking different tabs in the Main Display Window.

The Applications Summary includes the following tabs (Table 22–62):

Table 22–62 Applications Summary Tabs

Tab Name	Description
Summary	Includes performance data at the application level including time-based trend graphs of Application Response Time, Application Invocation Count, and Application Active Sessions. The invocation count and response time for the top 10 slowest servlets, the usual application entry points, are also included.
Response Times	Includes time-based trend graphs of component response times. Graphs include Servlet Response Time, EJB Response Time, and JDBC Response Time.
Invocations	Includes time-based trend graphs of component invocation counts. Graphs include Servlet Invocation Count, EJB Invocation Count, and JDBC Invocation Count.
Errors/Exceptions	Errors metrics associated with the selected portal.
Transactions	Transaction events associated with the selected portal and children below.By default, the Transactions tab is not enabled.
Modeled Entities	Includes a catalog of entities modeled by ADP. Only the modeled entities associated with the selected application are included.
Instrumentation	Includes performance data by different types of instrumentation probe points. There are different tabs available: Class, Method, and SQL. Each tab includes basic information such as Probe Point Name, Invocation Count, and Response Time. This detailed performance data can help you identify low-level bottlenecks.
Topology	Includes the topology view associated with the selected application.

Under each named application node, ADP displays performance and other relevant information specific to that application. For example, by clicking the children nodes, the relevant data is displayed in the Main Display Window. Application response time and invocations measurements can be reached by clicking the panes in the Main Display Window.

In this section, we will further expand on the following nodes:

- Services
- Dependencies
- Deployments
- Workshop Projects
- Web Applications
- Stateless Beans
- Stateful Beans
- Entity Beans
- Message Driven Beans

> **Note:** The number of children nodes available under each application node depends solely on the complexity of the selected application. Simple Java EE web applications will not have nodes like Workshop Projects, Stateless Beans, Stateful Beans, Entity Beans, and Message Driven Beans.

22.2.13.1 Services

The Services node includes all the external entry points associated with the selected application. When this node is selected, ADP displays a summary view in the Main Display Window. ADP displays the performance data associated with various entry points associated with the selected application.

> **Tip:** The children nodes under the Services node include entry point specific performance data.

22.2.13.2 Dependencies

The Dependencies node shows a list of internal and external components and share resources that a specific application depends on for its normal operation. When the Dependencies node is selected, ADP displays all external references made by the application in the Main Display Window. The following is a list of columns and their descriptions (Table 22–63):

Table 22–63 Dependencies Column Descriptions

Column/Metric	Description
Name	Display name of the component or resource used by the application. If this is undefined in the Deployment Descriptor, the reference name for the component is used.
Reference	Reference name of the component or resource used by the application.

Table 22–63 (Cont.) Dependencies Column Descriptions

Column/Metric	Description
Reference Type	Component or resource type.
Referer Component	Name of the component that is part of the application which obtained the reference to external component or resource.
Referer Module	Name of the module that is part of the application which obtained the reference to external component or resource.

ADP displays all the references associated with components in the selected application.

The Dependencies node can be further expanded by clicking the plus (+) icon. The children nodes of the Dependencies node are organized by type. Here are the list of dependency types and their descriptions (Table 22–64):

Table 22–64 Dependency Types

Dependency Type	Description
Data Sources	All shared data sources used by the application
Entity Beans	All entity beans used by the application
Session Beans	All session beans used by the application
JMS Queues	All JMS queues used by the application for publishing JMS messages
JMS Topics	All JMS topics subscribed by the application
Web Services	All web services used by the application

When a specific node is selected, ADP displays relevant performance summary. These nodes can also be expanded by clicking the plus (+) icons. The expanded tree includes specific components and share resources used by the application.

The Performance summary view associated with the Data Sources node under Dependencies provides information on both connection pools and SQL statements.

For more information on the metric description, refer to Section 22.1.11, "Metric Types".

22.2.13.3 Deployments

The Deployments node shows the architecture of the deployed application. When this node is selected, ADP shows all the modules deployed as part of this application. The default view in the Main Display Window shows the active module-level call path. Table 22–65 lists the tabs available as part of this summary view and their descriptions.

Table 22–65 Deployment Tabs

Tab Name	Description
Module Level Execution	Shows the active calling relationships among various Java EE modules (EAR, WAR, JAR, and more). Shared resources are also included. This is the default Architecture View at the module level.

Table 22–65 (Cont.) Deployment Tabs

Tab Name	Description
Module Level	Shows the potential calling relationships among various Java EE modules. Shared resources are also included. By default, the Module Level tab is not enabled.
Instrumentation	Includes detailed performance data at the method level. The table includes caller components, caller method, callee (target) component, callee module, invocation count, and response time.
SQL Statement	Includes all SQL statements executed as part of this application. It also includes performance information such as invocation count and response time.

Active module-level call path is displayed as the default view for the Deployments node of a selected application.

Double-click a specific module to trigger ADP to display the architecture of the selected module.

Expand the Deployments node by clicking the plus (+) icon to reveal all the deployed modules in this application. Further expanding the nodes at the *module* level reveals components associated with the selected module. Further expanding the nodes at the *component* level reveals methods associated with the selected component.

When you select one of these children nodes (module, component, and method levels), ADP displays associated tabs for active call path diagram, static call path diagram, instrumentation and SQL statements.

> **Tip:** Use the active call path diagram as a guide to identify entities with performance data. If an entity does not have performance data, ADP displays *No data available for the selected time frame* in the Main Display Window.

22.2.13.4 Workshop Projects

The Workshop Projects node includes performance information about modules and components created using the Oracle WebLogic Workshop. These modules and components include WebLogic Integration processes, WebLogic Integration web services, and WebLogic Portal pageflows.

Workshop Project node and its children nodes provide performance data associated with WLI processes, web services, and WLP pageflows.

When you select a specific children node, ADP displays detailed performance information.

22.2.13.5 Web Applications

The Web Applications node includes performance information related to the Web Applications modules and components associated with the selected application. Click the Web Applications node to reveal a performance summary in the Main Display Window. Click the plus (+) icon to expand the Web Applications node to reveal various web modules deployed as part of this application.

Click the plus (+) icon to expand on a specific web module and reveal different groupings for web components, for example, Pageflows, Struts Modules and Servlets. Clicking one of these nodes triggers ADP to display rolled up performance summary for the entire grouping. You can further expand these nodes by clicking the plus (+) icon to reveal more detailed information. Fully expanded Web Applications node contains all web modules organized by type.

Detailed performance information at the individual pageflow, struts action, and servlet levels will be displayed when you click the lowest level nodes.

22.2.13.6 Stateless Beans

The Stateless Beans node includes activity information related to the stateless EJB components associated with the selected application. Click the Stateless Beans node to reveal an activity summary in the Main Display Window. Click the plus (+) icon to expand the Stateless Beans node to reveal various stateless EJBs deployed as part of this application.

You can further select individual nodes to obtain detailed activity information. Selecting a specific Stateless Bean node triggers ADP to display detailed activity metrics.

The detailed view contains the following activity metrics (Table 22–66):

Table 22–66 Stateless Beans Detail View

Column/Metric	Description
EJB	Name of the stateless EJB.
In Use	Number of instances for a specific stateless EJB currently being used from the free pool. [Snapshot Count]
Idle	Number of instances for a specific stateless EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of threads currently waiting for a specific stateless EJB bean instance from the free pool. [Snapshot Count]
Timeouts	Total number of threads that have timed out waiting for an available bean instance from the free pool. [Aggregated Count]

> **Note:** The metrics reported in the Stateless Beans node are reported by the MBean (Management Bean) of the EJB container. These activity metrics can be used for checking the overall health of the EJB container. When the EJB container is restarted, these metrics are reset.

22.2.13.7 Stateful Beans

The Stateful Beans node includes activity information related to the stateful EJB components associated with the selected application. Click the Stateful Beans node to reveal an activity summary in the Main Display Window. Click the plus (+) icon to expand the Stateful Beans node to reveal various stateful EJBs deployed as part of this application.

You can further select individual nodes to obtain detailed activity information.

The Stateful EJB Summary includes the following tables:

- Stateful EJB Cache
- Stateful EJB Transactions
- Stateful EJB Locking

22.2.13.7.1 Stateful EJB Cache Stateful EJB Cache table includes the following information (Table 22–67):

Table 22–67 Stateful EJB Cache

Metrics	Description
EJB	Name of the Stateful EJB
Hits	Total number of times an attempt to access the Stateful EJB instance from the cache succeeded [Aggregated Count]
Accesses	Total number of attempts to access the Stateful EJB instance from the cache [Aggregated Count]
Size	Number of beans instances from this Stateful Home currently in the EJB cache [Snapshot Count]
Activations	Total number of beans from this Stateful Home that have been activated [Aggregated Count]
Passivations	Total number of beans from this Stateful Home that have been passivated [Aggregated Count]

> **Tip:** Passivation (serializing EJB state information to disk) and activation (reconstitute EJB state information from disk) are resource intensive operations. Ideally, Oracle recommends low level of activity in these metrics.

22.2.13.7.2 Stateful EJB Transactions Stateful EJB Transactions table includes the following information (Table 22–68):

Table 22–68 Stateful EJB Transactions

Metrics	Description
EJB	Name of the Stateful EJB
Commits	Total number of transactions that have been committed for this Stateful [Aggregated Count]
Rollbacks	Total number of transactions that have been rolled back for this Stateful [Aggregated Count]
Timeouts	Total number of transactions that have timed out for this EJB [Aggregated Count]

> **Tip:** High number of EJB Transaction Rollbacks may indicate problems with the data used; for some reason the target database is unable to commit the change. High number of EJB Transaction Time-outs may indicate problems accessing the database including network outage, database lock contention, and database outage.

22.2.13.7.3 Stateful EJB Locking Stateful EJB Locking table includes the following information (Table 22–69):

Table 22–69 Stateful EJB Locking

Metric	Description
EJB	Name of the Stateful EJB
Entries	Number of Stateful EJB instances currently locked [Snapshot Count]
Lock Accesses	Total number of attempts to obtain a lock on an Stateful EJB instance [Aggregated Count]
Current Waiters	Number of Threads that currently waiting for a lock on an Stateful EJB instance [Snapshot Count]
Total Waiters	Total number Threads that have waited for a lock on an Stateful EJB instance [Aggregated Count]
Timeouts	Total number Threads that have timed out waiting for a lock on an Stateful EJB instance [Aggregated Count]

> **Tip:** Pay attention to Current Waiters and Time-outs. These metrics can indicate possible performance problems caused by EJB Locking. Ideally, 0s should be displayed for these metrics.

ADP presents these metrics in a table format in the Main Display Window when you select the Stateful Beans node. Graphical representations of two metrics, Stateful EJB cache access, and Stateful EJB lock access, are displayed below the table.

By looking at the activities related to Stateful EJBs, you can determine if there any abnormal activities associated with Stateful EJBs.

> **Note:** The metrics reported in the Stateful Beans node are reported by the MBean (Management Bean) of the EJB container. These activity metrics can be used for checking the overall health of the EJB container. When the EJB container is restarted, these metrics are reset.

22.2.13.8 Entity Beans

The Entity Beans node includes activity information related to the Entity EJB components associated with the selected application. Click the Entity Beans node to reveal an activity summary in the Main Display Window. Click the plus (+) icon to expand the Entity Beans node to reveal various Entity EJBs deployed as part of this application.

You can further select individual nodes to obtained detailed activity information. Selecting a specific Entity Bean node triggers ADP to display detailed activity metrics.

The Entity EJB Summary includes the following tables:

- Entity EJB Activity
- Entity EJB Cache
- Entity EJB Transactions
- Entity EJB Locking

22.2.13.8.1 Entity EJB Activity Entity EJB Activity table includes the following information (Table 22–70):

Table 22–70 Entity EJB Activity

Metrics	Description
EJB	Name of the Entity EJB.
In Use	Number of instances for a specific Entity EJB currently being used from the free pool. [Snapshot Count]
Idle	Number of instances for a specific Entity EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of Threads currently waiting for a specific Entity EJB instance from the free pool. [Snapshot Count]
Timeouts	Total number of Threads that have timed out waiting for an available bean instance from the free pool. [Aggregated Count]

> **Tip:** Pay attention to Waits and Timeouts metrics. Activities in the Waits metric and increasing count in the Timeouts metric are signs that requests are waiting to be serviced by the EJB container. Ideally, 0 should be indicated for these metrics.

22.2.13.8.2 Entity EJB Cache Entity EJB Cache table includes the following information (Table 22–71):

Table 22–71 Entity EJB Cache

Metrics	Description
EJB	Name of the Entity EJB
Hits	Total number of times an attempt to access the Entity EJB instance from the cache succeeded [Aggregated Count]
Accesses	Total number of attempts to access the Entity EJB instance from the cache [Aggregated Count]
Size	Number of beans instances from this EJB Home currently in the EJB cache [Snapshot Count]
Activations	Total number of beans from this EJB Home that have been activated [Aggregated Count]
Passivations	Total number of beans from this EJB Home that have been passivated [Aggregated Count]

> **Tip:** Passivation (serializing EJB state information to disk) and activation (reconstituting EJB state information from disk) are resource intensive operations. Ideally, Oracle recommends a low level of activity in these metrics.

22.2.13.8.3 Entity EJB Transactions Entity EJB Transactions table includes the following information (Table 22–72):

Table 22–72 Entity EJB Transactions

Metric	Description
EJB	Name of the Entity EJB
Commits	Total number of transactions that have been committed for this EJB [Aggregated Count]
Rollbacks	Total number of transactions that have been rolled back for this EJB [Aggregated Count]
Timeouts	Total number of transactions that have timed out for this EJB [Aggregated Count]

> **Tip:** High numbers of EJB Transaction Rollbacks may indicate problems with the data used; for some reason the target database is unable to commit the change. High numbers of EJB Transaction Timeouts may indicate problems accessing the database including network outage, database lock contention, database outage, and more.

22.2.13.8.4 Entity EJB Locking Entity EJB Locking table includes the following information (Table 22–73):

Table 22–73 Entity EJB Locking

Metric	Description
EJB	Name of the Entity EJB
Entries	Number of Entity EJB instances currently locked [Snapshot Count]
Lock Accesses	Total number of attempts to obtain a lock on an Entity EJB instance [Aggregated Count]

Table 22–73 (Cont.) Entity EJB Locking

Metric	Description
Current Waiters	Number of Threads that currently waiting for a lock on an Entity EJB instance [Snapshot Count]
Total Waiters	Total number Threads that have waited for a lock on an Entity EJB instance [Aggregated Count]
Timeouts	Total number Threads that have timed out waiting for a lock on an Entity EJB instance [Aggregated Count]

> **Tip:** Pay attention to Current Waiters and Timeouts. These metrics can indicate possible performance problems caused by EJB Locking. Ideally, 0s should be displayed for these metrics.

When you select the Entity Beans node, ADP presents these metrics in a table format in the Main Display Window. Graphical representations of the following metrics, Entity EJB in use, Entity EJB cache access, and Entity EJB lock access, are displayed below the table.

Expand the Entity Beans tree by clicking the plus (+) icon next to Entity Beans node. You can get the same summary as previously described for a specific Entity EJB.

By looking at the activities related to Entity EJBs, you can determine if there any abnormal activities associated with Entity EJBs.

> **Note:** The metrics reported in the Entity Beans node are reported by the MBean (Management Bean) of the EJB container. These activity metrics can be used for checking the overall health of the EJB container. When the EJB container is restarted, these metrics are reset.

22.2.13.9 Message Driven Beans

The Message Driven Beans node includes activity information related to the message driven EJB components associated with the selected application. Click the Message Driven Beans node reveals an activity summary in the Main Display Window. Click the plus (+) icon to expand the Message Driven Beans node to reveal various message driven EJBs deployed as part of this application.

You can further select individual nodes to obtained detailed activity information.

The Message Driven EJB Summary includes the following tables:

- Message Driven EJB Activity
- Message Driven EJB Transactions

22.2.13.9.1 Message Driven EJB Activity Message Driven EJB Activity table includes the following information (Table 22–74):

Table 22–74 Message Driven EJB Activity

Metric	Description
EJB	Name of the Message Driven EJB.
In Use	Number of instances for a specific Message Driven EJB currently being used from the free pool. [Snapshot Count]
Idle	Number of instances for a specific Message Driven EJB currently in the idle state in the free pool. These bean instances are available for use. [Snapshot Count]
Waits	Number of Threads currently waiting for a specific Message Driven EJB instance from the free pool. [Snapshot Count]
Timeouts	Total number of Threads that have timed out waiting for an available bean instance from the free pool. [Aggregated Count]

Tip: Pay attention to Waits and Timeouts metrics. Activities in the Waits metric and increasing count in the Timeouts metric are signs that requests are waiting to be serviced by the EJB container. Ideally, 0 should be indicated for these metrics.

22.2.13.9.2 Message Driven EJB Transactions Message Driven EJB Transactions table includes the following information (Table 22–75):

Table 22–75 Message Driven EJB Transactions

Metric	Description
EJB	Name of the Message Driven EJB
Commits	Total number of transactions that have been committed for this EJB [Aggregated Count]
Rollbacks	Total number of transactions that have been rolled back for this EJB [Aggregated Count]
Timeouts	Total number of transactions that have timed out for this EJB [Aggregated Count]

Tip: High numbers of EJB Transaction Rollbacks may indicate problems with the data used; for some reason the target database is unable to commit the change. High numbers of EJB Transaction Timeouts may indicate problems accessing the database including network outage, database lock contention, database outage, and more.

ADP presents these metrics in a table format in the Main Display Window when you select the Message Driven Beans node. Graphical representation of the Message Driven EJB in use metric is displayed below the table.

By looking at the activities related to Message Driven EJBs, you can determine if there are any abnormal activities associated with Message Driven EJBs.

Note: The metrics reported in the Message Driven Beans node are reported by the MBean (Management Bean) of the EJB container. These activity metrics can be used for checking the overall health of the EJB container. When the EJB container is restarted, these metrics are reset.

22.2.14 Oracle WebLogic Resources

The Resources node under Oracle Enterprise Manager contains information for the managed domain organized by logical clusters, machines, servers, and more. You can look for low-level technology metrics organized by technology subsystems for a specific WebLogic Server.

The Resources tree includes the following nodes (Table 22–76):

Table 22–76 WebLogic Resources Tree

Example Node	Description
CSS Domain	Name of the WebLogic Domain configured
b-15/192.168.128.15	ID of the physical machine
cgServer	Name of the WebLogic Server configured
Applications	Performance measurements of all deployed applications running on this server
JDBC	Information of all configured JDBC resources for this server
JMS Servers	Information of all JMS destinations configuration for this server
Execute Queues	Information of all Execute Queues configured for this server
JVM	JVM information including Heap Size for this server
JRockit	JRockit information including Heap Size for this server
Modeling Status	Entities modeled by ADP for this server
ADP Modules	Status of the ADP Java Agent Module for this server

Expand these nodes by clicking the plus (+) icon next to the node name to get more information.

If the ADP OS Agent is deployed on the machine, clicking on the physical machine ID would show OS metrics collected by the OS Agent. These OS metrics include CPU Usage, Disk Usage, and Physical Memory Usage.

22.2.15 Oracle Resources

The Resources node under Oracle Enterprise Manager contains information for the managed domain organized by logical clusters, machines, servers, and more. You can look for low-level technology metrics organized by technology subsystems for a specific Oracle AS Server.

The Resources tree includes the following nodes (Table 22–77):

Table 22–77 Oracle Resources Tree

Example Node	Description
Managed System Resource Name	Top-level Resource name, for example, oc4j_soa
Oracle AS Server	Machine name which can be navigated to both within or outside a cluster, for example, oc4j_soa@192.168.1.119 which includes both the server name and the host server IP address
Applications	Performance measurements of all deployed applications running on this server
JDBC	Information of all configured JDBC resources for this server
JMS Servers	Information of all JMS destinations configuration for this server

Table 22–77 (Cont.) Oracle Resources Tree

Example Node	Description
Thread Pools	Performance information about all threads used by the container to process requests
JVM	JVM information including Heap Size for this server
BPEL Processes	Performance measurements about BPEL Processes deployed in the container
ESB	Performance measurements about ESB services deployed in the container
Modeling Status	Modeled entities for the container
ADP Modules	Status of the ADP Java Agent Module for this server
Applications	Performance information about the applications deployed in the container

Clicking the physical machine ID would show OS metrics. These OS metrics include CPU Usage, Disk Usage, and Physical Memory Usage.

22.2.16 Custom Metrics

The Custom Metrics node under Oracle Enterprise Manager contains all the custom metrics you defined. Currently ADP supports custom metrics for Java classes. When Custom Metrics node is selected, ADP displays various summaries. You can select individual entities to get more detailed performance information.

Expanding the Custom Metrics node reveals a list of Java classes with custom metrics configured.

The following is a list of columns in the Custom Class Performance table and their descriptions (Table 22–78):

Table 22–78 Custom Class Performance

Column/Metric	Description
Caller Class	Fully qualified name of the class that is making the inbound call
Caller Method	Method name in the class that is making the inbound call
Class	Fully qualified name of the class that is the destination of the inbound call
Invocation Count	Total number of times the inbound call is made
Response Time (ms)	Average response time of the inbound call in milliseconds

22.2.17 Status

Status in the navigation tree contains information for the ADP environment for the monitored WebLogic domain, WebSphere cell, or Oracle AS cluster. Select Status to see the ADP Java Agent status for the WebLogic domain.

The ADP Java Agent status includes the following (Table 22–79):

Table 22–79 ADP Java Agent Status

Column/Metric	Description
Server	Name of the WebLogic server, WebSphere cell, or Oracle AS cluster
Container Status	Operational status of the WebLogic, WebSphere, or Oracle AS server (running or not)
Agent In Sync	Version synchronization between ADP and ADP Agent status (true or false)
EJB Installed	ADP EJB installation status (true or false)

Table 22–79 (Cont.) ADP Java Agent Status

Column/Metric	Description
Agent Installed	ADP Java Agent installation status
Agent Activated	ADP Java Agent activation status
Agent Status	ADP Java Agent operational status
Server Type	Identifies server as administration, individual, or clustered server
Admin URI	Location of the domain admin server
Manager RMI Registry Host	Host name of the ADP RMI registry
Manager RMI Registry Port	Port number of the ADP RMI registry
EJB Major Version	ADP EJB major version
EJB Minor Version	ADP EJB minor version
EJB Build ID	ADP EJB build number - for version synchronization check
Agent Major Version	ADP Java Agent major version
Agent Minor Version	ADP Java Agent minor version
Agent Build ID	ADP Java Agent build number - for version synchronization check

Click the Modeling Status node under Status to see a table of all modeled entities in the managed domain. This table shows all the managed clusters, servers, and applications in the ADP environment. Mismatches between the Modeling Status table and your environment are indications of configuration problems.

You can use this information to debug and resolve ADP configuration issues.

22.2.18 Service Component Architecture (SCA)

Service Component Architecture (SCA) provides a set of features and services that simplify the process of detecting the presence of Service-Oriented Architecture (SOA) components.

Table 22–80 SCA Composites

Composite	Description
Services	Metrics related to Services defined on the SOA composite.
Wires	Metadata related to Wires defined in the SOA composite
References	Metrics related to References defined in the SOA composite
Components	Metrics related to Components within the SOA composite

22.2.18.1 Components

The following components make up the Service Component Architecture:

Table 22–81 Components in SCA

Component	Description
Decision Services	Metrics related to components in the Decision Services engine
Mediators	Metrics related to components in the Mediator engine

Table 22–81 (Cont.) Components in SCA

Component	Description
Human Workflows	Metrics related to components in the Human Workflow engine
BPEL	Metrics related to components in the BPEL engine

22.3 Exploring the Configuration Tab

Using the Configuration tab you can set up the resources you want to monitor using ADP.

The configurations explained in this section are:

- Database Configuration
- Resource Configuration
- Service Level Objective Configuration
- Custom Metric Configuration

A running ADP manager must be registered in Enterprise Manager. After the registration, Enterprise Manager continues to keep the manager as a valid manager even if it is down. When this occurs, the Enterprise Manager UI displays the ADP manager as Unreachable.

22.3.1 Database Configuration

The Database Configuration page lists the databases accessible to ADP which you want to monitor. You can configure a database to be used by ADP, edit an existing database configuration, delete a database configuration, and enable a configuration.

22.3.2 Resource Configuration

The Resource Configuration node in the Configuration tree enables you to create resources (for example, target application server domains) that can be monitored by ADP.

22.3.3 Service Level Objective Configuration

In ADP, thresholds configured for various measurements are called Service Level Objectives (SLOs). A service level objective is a measurable attribute, for example, availability. Service Level Agreements (SLA) are made up of SLOs.

Configuring SLOs is a key activity for establishing and maintaining an effective performance monitoring system. To configure a SLO, click the **Configuration** tab and select the **Service Level Objective Configuration** option.

ADP categorizes SLOs into the following types:

- Performance

  Depicts the relative responsiveness of the monitored entity to the configured threshold.

- Availability

  Informs you to what extent a particular entity is available to service requests.

- Errors

Informs you if the number of errors and exceptions encountered by this entity are approaching or violating the configured threshold.

- Load

  Depicts how many operations have been performed and requests have been served by a particular entity.

ADP is aware of clusters. As such, these indicators display overall health of a particular entity across the entire cluster.

To configure a SLO, perform the following steps:

1. From the **Targets** menu, select **Middleware**. On the Middleware page, select **Application Dependency and Performance** from the Middleware Features menu. Ensure the Configuration tab is highlighted.
2. Select **SLO Blackout Configuration**.
3. You can view any existing SLO blackout.
4. Use this window to create, delete, or view the details of existing blackouts.

22.3.3.1 Creating a New SLO

When you select Service Level Objectives Configuration, ADP displays the Service Level Objective Configuration window. This window allows you to apply existing SLOs or create new ones. When you click **Create New SLO**, ADP guides you through the process of setting up a new SLO.

The steps for SLO creation are as follow:

1. Either select a SLO file or create a new SLO file. ADP can store SLO configurations in different files to improve configuration portability.
2. Define the SLO Entity Type. ADP automatically selects the appropriate entity type for you based on the selected monitoring element. For example, if you want to set a SLO on a Portal Desktop element, ADP automatically sets the Entity Type for you.
3. Other information is filled in by default. Normally, there is no need to modify the SLO Entity values.
4. When you are done setting the SLO Entity Type values, click **Create New SLO** to go to the second step of the SLO creation process, Defining the SLO Parameters. Note: The (*) character means Select All. It is recommended that you do not use the (*) character.

Note: SLOs are hierarchical which allows you to set service levels at any level within the modeled hierarchy of an application.

22.3.3.2 Defining SLO Parameters

Follow these steps to define the SLO parameters:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the target of choice. On the **Home** tab, select the **Summary** region and click the **Application Dependency and Performance** link.
2. Expand the **Configuration** tab. Select **Service Level Objective Configuration**.
3. Either create a new SLO or edit an existing SLO.
4. Select the performance metric.

5. Define the monitoring window size, which determines how long the condition must persist before generating an alert.
6. Set threshold values for the SLO.
7. Select what actions to take when a trigger is fired. A list of preconfigured actions is available in the view pane.
8. Add new actions by going to the Action Configuration node in the Configuration Workspace.
9. Click **Save** to set the SLO for this monitored element.
10. You can delete unwanted SLOs for any element from this window.

Types of SLOs

ADP categorizes SLOs as Performance, Availability, Error, and Load.

SLO Events Viewer

Right-click on any tree node and select **View Service Level Objective Events** to open a new window. You can see all the SLO violation events triggered for the selected entity. ADP automatically applies a filter to show only relevant events.

Once new SLOs are added, ADP updates the relevant graphs to visually display these new thresholds. Table 22–82 explains the different line types.

Table 22–82 SLO Line Types

Line Description	Description
Solid Red Line	A violation threshold that triggers on high.
Solid Yellow Line	A cautionary threshold that triggers on high.
Dashed Red Line	A violation threshold that triggers on low.
Dashed Yellow Line	A cautionary threshold that triggers on low.

22.3.3.3 SLO Blackout Configuration

You can prevent having unwanted alerts being fired during planned or unplanned down time. The SLO Blackout Configuration node in the Configuration tree enables you to create time periods when information will not be monitored for a specific SLO. You can define blackouts by a SLO file, an individual SLO, or by entity.

22.3.3.4 Creating and Maintaining SLO Blackouts

You can prevent having unwanted alerts being fired during planned or unplanned down time. SLO Blackout Configuration enables you to create time periods when information will not be monitored for a specific SLO. You can define blackouts by a SLO file, an individual SLO, or by entity.

To create and maintain SLO blackouts, perform the following steps:

1. Navigate to Application Dependency and Performance.

   From the **Targets** menu, select **Middleware**. On the Middleware page, click the target of choice. Select **Application Dependency and Performance** from the Middleware Features menu.
2. Expand the **Configuration** tab. Select **SLO Blackout Configuration**.
3. You can view any existing SLO blackout.

4. Use this window to create, delete, or view the details of existing blackouts.

Creating SLO Blackout

1. Click **Create SLO Blackout** to view the detail window.
2. On the SLO Blackout File page, type the name of the blackout in the New SLO Blackout File field. Click **Continue**.
3. On the SLO Blackout Configuration page, fill in the fields. Refer to Table 22–83 for details.

Table 22–83 SLO Blackout Configuration

Column/Metric	Description
Blackout Name	Type in the name.
Description	Type in the description of the SLO you are creating.
Blackout By SLO File	Use to blackout at the file level. The SLO files display in a list where you can select them or cancel out of the window. This option restricts the blackout to the SLO file name.
Blackout By SLOs	Use to blackout at the SLO level. The SLOs display in a list where you can select them or cancel out of the window. This option restricts the blackout to the SLO name.
Blackout By Entity	Use to blackout at the entity type level. Click the **Blockout by Entity:** button to view the list of entity types. Select the entity. This option restricts the blackout to the entity type selected.
year, month, date, hour, minute, duration	Use the guidelines to the right of these columns to enter the appropriate information.
recurring	Select how often you would like to run this blackout event from the list.

Viewing SLO Blackout Summary List

1. Click **SLO Blackout Summary List**.
2. View the details on the existing SLO Blackout events.
3. Click **Show SLO Blackout List** to return to the previous window.

Deleting SLO Blackout

1. Select an existing event on the list.
2. Click **Delete SLO Blackout**.
3. Confirm that you want to delete the entry and click **Yes**.

22.3.3.5 Propagating Threshold Violation Events

ADP is designed to propagate threshold violation events up the hierarchy. Therefore, when a SLO is set on a lower level metric, the higher level health indicator light becomes activated. Additionally, the health indicator light for the application server that hosts this component also becomes active. Oracle calls this *containment approach* to SLO event propagation. When a lower level SLO is violated, the violation event propagates all the way up the hierarchy and changes the status of all containers for this event.

22.3.4 Event Integration

Use the Enterprise Manager Incident console to check for events fired as a result of SLO violations in ADP.

To access the ADP alerts:

1. From the Enterprise menu, select **Monitoring**, then select **Incident Manager**.
2. In the Views region, select **Events without incidents**.

Look for events with target type “Application Deployment” and "Application Dependency and Performance Alert”. These are the ADP alerts.

22.3.5 Custom Metric Configuration

There are cases where additional instrumentation is needed based on your specialized requirements. Custom metrics allow you to instrument a class or method of your choice and receive performance metrics collected by the ADP agent.

To create a metric configuration, do the following:

1. From the **Targets** menu, select **Middleware**. In the Related Links sections, select **Application Dependency and Performance**.
2. Click the **Configuration** tab, choose the configuration in which you are interested. Click **Custom Metric Configuration**.
3. In the right pane, click the **Create Custom Metric** button.
4. On the Custom Metric File page, choose whether to use an existing .xml file or a new file. If you choose a new file, the ADP Manager will create the new .xml file. Click **Continue**.
5. On the Custom Metric Configuration page, provide the following information:
   - Resource name is a monitored WebLogic domain or Oracle Application Server or WebSphere cell.

     You created a name when you configured ADP to monitor. The same name is used here during custom metric configuration.
   - Class name is the name of the implementation class in the code. You are required to enter a fully qualified class name.
   - Method name is the name of the implementation method in the code.

After you define the custom metrics, restart the application server instances associated with these customizations. The new custom metrics will be listed under the Custom Metrics node in the ADP navigation tree.

The newly configured custom metric provides class level performance data, for example, invocation count and response time.

22.4 Exploring the Registration Tab

The managers perform complex mathematical modeling and statistical calculations with summarized data from all Java Agents.

Using the Registration tab, you can add, edit, and remove Managers configured to Enterprise Manager. By accessing ADP through Remote Method Invocation (RMI), you can manipulate all the managers configured to Enterprise Manager through a secured protocol.

22.4.1 Using RMI Configuration for Managers

In ADP, the Configuration tab lists all the managers currently configured to Enterprise Manager. By using the Configuration for Managers feature, you can access Application Dependency and Performance through Remote Method Invocation (RMI). You can then manipulate all the managers configured to Enterprise Manager through a secured protocol. The following sections provide additional information.

- Adding a New Manager (RMI Configuration)
- Editing a Previously Configured Manager (RMI Configuration)
- Removing or Disabling a Previously Configured Manager

The Configuration tab displays only if the Enterprise Manager user is an Administrator as defined by examining the user's role.

22.4.2 Adding a New Manager (RMI Configuration)

The first time the Registration tab displays there are no managers in the Managers tree. To add a new manager, perform the following steps:

1. Navigate to the **Application Dependency and Performance** feature.

   From the **Targets** menu, select **Middleware**. In the **Related Links** section, click **Application Dependency and Performance**.

2. In the **Registration** tab, click the **Managers** node in the tree.
3. Type the new manager information in the Main Display window.
4. Decide whether this manager should be monitored.

   Request monitoring provides end-to-end visibility into requests, localizes end-user performance problems to specific application deployments, and provides a platform for context-based drill down diagnostics.

   When you select **Enable Request Monitoring**, ADP creates and sets up targets for collecting request performance data. If you do not select Enable Request Monitoring, the ADP manager is only registered in Enterprise Manager.

   > **Note:** The grayed out information represents configuration data for connecting to the ADP manager by way of a secure protocol, for example Key Store, Trust Store, and passwords. This information is extracted from the ADP manager by way of the RMI call.

5. If you enable request monitoring on an existing manager, click **Upload** to populate the manager configuration properties to the ADP target in Request Monitoring.
6. Click **Test Connect** to test the connection to the new manager. Should the test connection fail, this may be because the manager is not running or the manager is not yet installed.
7. Click **Add**.

Once the manager is added, the name of the manager will display in the Configuration tab under the Managers node in the tree.

22.4.3 Editing a Previously Configured Manager (RMI Configuration)

To add a previously configured manager, perform the following steps:

1. Click + (plus sign) next to the Managers node in the tree, then select the subnode for the manager you want to edit.
2. After you make changes to the manager information, click **Update**. This results in the manager entries in the Enterprise Manager repository to be updated with the new values.

If a manager is configured before using this Enterprise Manager configuration page, Enterprise Manager continues to keep the manager as a valid manager even though the manager may be down or permanently removed.

The list of managers is not refreshed.

22.4.4 Removing or Disabling a Previously Configured Manager

To remove a configured manager, perform the following steps:

1. Navigate to **Application Dependency and Performance**.

   From the **Targets** menu, select **Middleware**. In the **Related Links** section, click **Application Dependency and Performance**.
2. Click the **Registration** tab.
3. Click + (plus sign) next to the Managers node in the tree, then select the subnode for the manager you want to remove.
4. Click **Remove** in the main pane.

   Deleting a manager from Enterprise Manager does not uninstall and remove the manager from the remote host where the manager is located and may be running. Remove only deletes the manager entry from the Enterprise Manager repository.

   To shut down the manager after the Remove operation, execute the acshut.sh/.bat command from the command line.

To disable a configured manager:

1. Click + (plus sign) next to the Managers node in the tree, then select the subnode for the manager you want to disable.
2. Deselect **Enable Request Monitoring**.
3. Click **Update**.

When you deselect the Enable Request Monitoring option, the manager settings are preserved. The UI displays these managers as disabled. There will not be any further information under the disabled manager in the tree.

23
Exporting Data

This chapter includes the following export features:

- Data Export Modes
- ADP Export Configuration
- Example of Exported Data for WebLogic

23.1 Data Export Modes

There are three different modes to export performance data collected by ADP to external databases and other persistence formats. These modes give you flexibility to choose the best way to extract performance data from ADP.

- Export to File
- Export to Database
- Aggregation Export to File

23.1.1 Export to File

In this mode, ADP exports its raw performance data as several CSV (comma separated value) files.

23.1.2 Export to Database

In this mode, ADP exports its raw performance data as several ANSI SQL statements. These SQL statements allow you to create tables and insert data.

23.1.3 Aggregation Export to File

In this mode, ADP exports its aggregated performance data after it's daily aggregation operation as several CSV files.

23.2 ADP Export Configuration

The following sections describe ADP export configuration:

- ADP Periodic Export Configuration
- Manual Execution of Metric Export
- export.xml File

23.2.1 ADP Periodic Export Configuration

ADP stores real-time performance metrics in its internal data repository (Oracle database). If you want to store this data in your historical data repository, ADP provides automatic means for performance data export. You can control the frequency of export runs, the time when the export should run, and the time range of export data within a day.

Example 23–1 ADP Export Configuration

```
# Setting for integrated export
AggregationManager.IntegratedExport = false
AggregationManager.ExportDataStartHour = 0
AggregationManager.ExportDataEndHour = 0
AggregationManager.ExportDataSetRangeInHour = 4
AggregationManager.ExportDataSetIntervalInHour = 1
AggregationManager.ExportDataSetDelay = 10000
AggregationManager.ExportStartTime = 0
AggregationManager.ExportEndTime = 0
AggregationManager.ExportFilePurgeTime = 10d
```

By default, automatic data export feature is disabled. To enable it, set AggregationManager.IntegratedExport parameter to true. A pair of parameters, AggregationManager.ExportDataStartHour and AggregationManager.ExportDataEndHour, indicates the time range within a day of the export performance data in which you are interested. By default it is 24 hours.

Parameter AggregationManager.ExportDataSetRangeInHour shows how much data is stored in each export file. By default it is 4 hours worth of data. This means that ADP will create multiple export data files with 4 hours worth of data.

To minimize export query impact on normal ADP performance data collection functionality, spread out lengthy data exporting queries. This is achieved by setting AggregationManager.ExportDataSetIntervalInHour parameter. By default it is 1 hour. This means that export query thread will be running every hour.

AggregationManager.ExportDataSetDelay defines cool down time for consecutive export queries. By default it is 10 seconds. This means that the next export query will happen not earlier than 10 seconds after the previous one.

AggregationManager.ExportFilePurgeTime indicates how many days the export data file will be available before ADP deletes it. By default it is 10 days. Current default values are optimal and this section should not be changed except from enabling the automatic export feature.

Automatic export function relies on the definition of the data to be exported by looking into `$GCDomain/EMGC_ADPMANAGER1/ADPManager.ear/ADPManager.war/config/export.xml` file and exports performance data based on the rules defined in this file.

The output directory is specified in export.xml and will be overwritten on each export interval.

23.2.2 Manual Execution of Metric Export

The bin directory on the ADP manager contains scripts called runExportMetric.sh/bat and runExportEvent.sh/bat that export metrics and events (such as alerts) to CSV files, respectively.

Run runExportMetric.sh like:

```
./runExportMetric.sh <path to export.xml configuration> <start time> <end time>
```

For example:

```
C:\oracle\em11g\bin\runExportMetric.bat c:\oracle\em11g\config\export.xml
"4/1/09 16:06:00" "4/1/09 16:36:00"
```

The start time and end time are in the machine's local time zone. The output exported csv files' timestamps will be in UTC/GMT.

23.2.3 export.xml File

The export.xml file contains all the directives and filters required to export performance metrics and events. This file is used by the ADP Integrated Automatic export feature as well as manual export scripts.

Example 23–2 Contents of export.xml File

```
<?xml version="1.0" encoding="UTF-8"?>
<export xmlns="http://www.acsera.com/ns/export" verbose="true" exportMetric="true"
exportEvent="true" metricDataGrain="180s" exportFullMetric="true">
<!--
<output type="jdbc" convertTimeFormat="true"
arguments="access,metric,sun.jdbc.odbc.JdbcOdbcDriver,jdbc:odbc:acsera"/>
-->
<output type="file" convertTimeFormat="false"
arguments="/home/acsera/acsera/export,metric"/>
<entityTypes exportAllTypes="false">
<entityType name="BEA.ProcessNode"/>
<entityType name="J2EE.Dispatcher"/>
<entityType name="J2EE.JDBC.ConnectionPool"/>
<entityType name="J2EE.JVM"/>
</entityTypes>
<!--extra filter -->
<!--
<filters>
<filter key="containerID" values="cgServer"/>
</filters>
-->
<!-- don't modify this -->
<columns>
<column header="Timestamp" type="Timestamp"/>
<column header="EntityID" type="EntityID"/>
<column header="Application" type="Entity" key="applicationID" default=""/>
</columns>
</export>
```

The following tables explain the various attributes.

Table 23–1 Attributes on <export>

Attribute	Description
exportMetric	true/false, whether to export performance metrics
exportEvent	true/false, whether to export SLO events
metricDataGrain	60s, 180s, or 1800s, the metric aggregation tier to export. Note that the population of the 180s tier will be delayed by 1.25 hours and the 1800s tier will be delayed by 7 hours compared to the 60s tier.
exportFullMetric	true/false, whether to include sum, count, min, and max metrics or not.

Table 23–2 Attributes on <output>

Attribute	Description
type	file/jdbc, whether to output to csv files or to write data to another database using JDBC. In the case of JDBC output, the necessary tables will be created automatically by the export mechanism.
convertTimeFormat	true/false, whether to convert the metric timestamp to human readable format (in UTC/GMT). If false, the timestamp will be a long integer. Provide the arguments (jdbc) in a comma separated list.
arguments	See Table 23–3 and Table 23–4 for details.

Table 23–3 Value of the "arguments" Attribute of the <output> Element When the "type" Attribute Is "JDBC"

Attribute	Description
First Parameter	Database type, an arbitrary string
Second Parameter	Table prefix name, should always be metric
Third Parameter	Fully qualified JDBC driver class
Fourth Parameter	JDBC URL

Table 23–4 Value of the "arguments" Attribute of the <output> Element When the "type" Is "file"

Argument	Description
First Parameter	CSV file output directory (this directory will be created, existing files will be overwritten)
Second Parameter	Table prefix name, should always be **metric**

Table 23–5 Attribute of the <entityTypes> Element

Attribute	Description
exportAllTypes	true/false, whether to output all entity types or only the ones specified in <entityType> elements.

Table 23–6 Attribute of the <entityType> Element

Attribute	Description
name	Name of the entityType to include in the export if exportAllTypes is set to false

23.3 Example of Exported Data for WebLogic

The tables in this section describe the fields in the various export files.

- Export File Name: metricBEA_ChannelInstance.csv
- Export File Name: metricBEA_ProcessType.csv
- Export File Name: metricBEA_TimerEventGenerator.csv
- Export File Name: metricJ2EE_Dispatcher.csv
- Export File Name: metricJ2EE_EJB_Entity.csv
- Export File Name: metricJ2EE_EJB_Stateless.csv
- Export File Name: metricJ2EE_JDBC_ConnectionPool.csv

- Export File Name: metricJ2EE_JMS_Destination.csv
- Export File Name: metricJ2EE_JMS_Service.csv
- Export File Name: metricJ2EE_JVM.csv
- Export File Name: metricJ2EE_Server.csv
- Export File Name: metricJ2EE_Servlet.csv

Table 23–7 Export File Name: metricBEA_ChannelInstance.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Fully qualified name of the channel
channelID	Fully qualified name of the channel
serviceID	URL of the service / JPD
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.ChannelInstance.MessageCount	JMX metric
Metric.J2EE.ChannelInstance.DeadMessageCount	JMX metric

Table 23–8 Export File Name: metricBEA_ProcessType.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Implementation class name
processID	Display name of the process
serviceID	URL of the service / JPD
projectID	Name of Workshop project / web application module
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
entityTypeID	Type of the monitored entity
applicationID	Name of the Application
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
deploymentID	Unique ID used by Oracle WebLogic to track application deployments
resourceID	Name of the monitored resource as configured by the user

Table 23–8 (Cont.) Export File Name: metricBEA_ProcessType.csv

Field	Description
displayNameID	Display name
controlContainerID	Implementation class name of the process
Metric.J2EE.ProcessType.Arrivals	Instrumentation metric -- number of arrivals
Metric.J2EE.ProcessType.Aborts	Instrumentation metric -- number of aborts
Metric.J2EE.ProcessType.ElapsedTime	Instrumentation metric -- average elapsed time
Metric.J2EE.ProcessType.Active	Instrumentation metric -- number of active requests
Metric.J2EE.ProcessType.VisitCount	Instrumentation metric -- number of completed requests
Metric.J2EE.ProcessType.Exceptions	Instrumentation metric -- number of exceptions

Table 23–9 Export File Name: metricBEA_TimerEventGenerator.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Fully qualified name of the channel
channelID	Fully qualified name of the channel
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
channelTxID	Fully qualified name of the channel
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.TimerEventGenerator.MessageCount	JMX metric
Metric.J2EE.TimerEventGenerator.ErrorCount	JMX metric

Table 23–10 Export File Name: metricJ2EE_Dispatcher.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Fully qualified name of the Execute Queue
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
executeQueueID	Name of the Execute Queue as configured by user
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user

Table 23–10 (Cont.) Export File Name: metricJ2EE_Dispatcher.csv

Field	Description
entityTypeID	Type of the monitored entity
Metric.J2EE.Dispatcher.ServicedRequestsTotalCount	JMX metric
Metric.J2EE.Dispatcher.IdleThreads	JMX metric
Metric.J2EE.Dispatcher.PendingRequests	JMX metric

Table 23–11 Export File Name: metricJ2EE_EJB_Entity.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
methodID	Name of the EJB method executed
domainID	Name of the Oracle WebLogic domain
entityTypeID	Type of the monitored entity
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
ejbID	Name of the EJB
webApplicationID	Name of the web module
displayNameID	Display name
controlContainerTypeID	Identifies type of control
elementID	Implementation class name
processID	Display name of the process
serviceID	URL of the service / JPD
projectID	Name of Workshop project / web application module
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
ejbComponentID	Name of Java EE component that contains this EJB
applicationID	Name of the Application
resourceID	Name of the monitored resource as configured by the user
controlContainerID	Implementation class name of the process
Metric.J2EE.EJB.Entity.Locking.LockManagerAccessCount	JMX metric
Metric.J2EE.EJB.Entity.ResponseTime	Instrumentation metric -- response time
Metric.J2EE.EJB.Entity.Cache.BeansCurrentCount	JMX metric
Metric.J2EE.EJB.Entity.Cache.AccessCount	JMX metric
Metric.J2EE.EJB.Entity.Pool.WaiterCurrentCount	JMX metric
Metric.J2EE.EJB.Entity.Transaction.CommittedTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Locking.WaiterTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Transaction.TimedOutTotalCount	JMX metric

Table 23–11 (Cont.) Export File Name: metricJ2EE_EJB_Entity.csv

Field	Description
Metric.J2EE.EJB.Entity.Cache.HitCount	JMX metric
Metric.J2EE.EJB.Entity.Locking.WaiterCurrentCount	JMX metric
Metric.J2EE.EJB.Entity.Pool.IdleCount	JMX metric
Metric.J2EE.EJB.Entity.Locking.EntriesCurrentCount	JMX metric
Metric.J2EE.EJB.Entity.VisitCount	Instrumentation metric -- invocation count
Metric.J2EE.EJB.Entity.Locking.TimeoutTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Pool.InUseCount	JMX metric
Metric.J2EE.EJB.Entity.Pool.WaiterTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Pool.TimeoutTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Transaction.RolledBackTotalCount	JMX metric
Metric.J2EE.EJB.Entity.Cache.ActivationCount	JMX metric
Metric.J2EE.EJB.Entity.Cache.PassivationCount	JMX metric

Table 23–12 Export File Name: metricJ2EE_EJB_Stateless.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Implementation class name
projectID	Name of Workshop project / web application module
nodeID	Name of the physical machine
containerID	Name of the Oracle WebLogic Server instance
domainID	Name of the Oracle WebLogic domain
ejbComponentID	Name of Java EE component that contains this EJB
entityTypeID	Type of the monitored entity
applicationID	Name of the Application
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
ejbID	Name of the EJB
resourceID	Name of the monitored resource as configured by the user
displayNameID	Display name
Metric.J2EE.EJB.Stateless.Transaction.TimedOutTotalCount	JMX metric
Metric.J2EE.EJB.Stateless.Pool.WaiterTotalCount	JMX metric
Metric.J2EE.EJB.Stateless.Pool.InUseCount	JMX metric
Metric.J2EE.EJB.Stateless.Transaction.CommittedTotalCount	JMX metric

Table 23–12 (Cont.) Export File Name: metricJ2EE_EJB_Stateless.csv

Field	Description
Metric.J2EE.EJB.Stateless.Transaction.RolledBackTotalCount	JMX metric
Metric.J2EE.EJB.Stateless.Pool.IdleCount	JMX metric
Metric.J2EE.EJB.Stateless.Pool.TimeoutTotalCount	JMX metric

Table 23–13 Export File Name: metricJ2EE_JDBC_ConnectionPool.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of JDBC connection pool
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.JDBC.ConnectionPool.WaitingForConnectionCurrentCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.WaitingForConnectionHighCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.ActiveConnectionsHighCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.ActiveConnectionsCurrentCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.FailuresToReconnectCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.WaitSecondsHighCount	JMX metric
Metric.J2EE.JDBC.ConnectionPool.ConnectionDelayTime	JMX metric

Table 23–14 Export File Name: metricJ2EE_JMS_Destination.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of JMS destination
nodeID	Name of the physical machine
containerID	Name of the Oracle WebLogic Server instance
jmsServerRuntimeID	Name of the JMS server
domainID	Name of the Oracle WebLogic domain
jmsDistributedQueueMemberID	Name of the JMS distributed queue member
entityTypeID	Type of the monitored entity

Table 23–14 (Cont.) Export File Name: metricJ2EE_JMS_Destination.csv

Field	Description
jmsQueueID	Name of the JMS queue
jmsRuntimeID	Name of the JMS service
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
jmsDistributedQueueID	Name of the JMS distributed queue
resourceID	Name of the monitored resource as configured by the user.
displayNameID	Display name
Metric.J2EE.JMS.Destination.ConsumersCurrentCount	JMX metric
Metric.J2EE.JMS.Destination.BytesCurrentCount	JMX metric
Metric.J2EE.JMS.Destination.MessagesPendingCount	JMX metric
Metric.J2EE.JMS.Destination.BytesThresholdTime	JMX metric
Metric.J2EE.JMS.Destination.MessagesHighCount	JMX metric
Metric.J2EE.JMS.Destination.BytesReceivedCount	JMX metric
Metric.J2EE.JMS.Destination.MessagesReceivedCount	JMX metric
Metric.J2EE.JMS.Destination.BytesHighCount	JMX metric
Metric.J2EE.JMS.Destination.MessagesCurrentCount	JMX metric
Metric.J2EE.JMS.Destination.ConsumersTotalCount	JMX metric
Metric.J2EE.JMS.Destination.ConsumersHighCount	JMX metric
Metric.J2EE.JMS.Destination.BytesPendingCount	JMX metric

Table 23–15 Export File Name: metricJ2EE_JMS_Service.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of the JMS service
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
jmsRuntimeID	Name of the JMS service
Metric.J2EE.JMS.Service.ConnectionsHighCount	JMX metric
Metric.J2EE.JMS.Service.ConnectionsCurrentCount	JMX metric
Metric.J2EE.JMS.Service.JMSServersCurrentCount	JMX metric

Table 23–15 (Cont.) Export File Name: metricJ2EE_JMS_Service.csv

Field	Description
Metric.J2EE.JMS.Service.JMSServersHighCount	JMX metric
Metric.J2EE.JMS.Service.ConnectionsTotalCount	JMX metric
Metric.J2EE.JMS.Service.JMSServersTotalCount	JMX metric

Table 23–16 Export File Name: metricJ2EE_JVM.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of the JVM
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.JVM.JRockit.HeapSizeCurrent	JMX metric
Metric.J2EE.JVM.JRockit.HeapFreeCurrent	JMX metric
Metric.J2EE.JVM.JRockit.PhysMemTotal	JMX metric
Metric.J2EE.JVM.JRockit.PhysMemUsed	JMX metric
Metric.J2EE.JVM.JRockit.GarbageCollectionCountTotal	JMX metric
Metric.J2EE.JVM.JRockit.GarbageCollectionTimeTotal	JMX metric
Metric.J2EE.JVM.HeapFreeCurrent	JMX metric
Metric.J2EE.JVM.JRockit.PhysMemFree	JMX metric
Metric.J2EE.JVM.JRockit.NursurySizeTotal	JMX metric
Metric.J2EE.JVM.JRockit.ActiveDaemonThreads	JMX metric
Metric.J2EE.JVM.JRockit.ActiveThreads	JMX metric
Metric.J2EE.JVM.HeapSizeCurrent	JMX metric
Metric.J2EE.JVM.JRockit.HeapUsedCurrent	JMX metric

Table 23–17 Export File Name: metricJ2EE_Server.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of the Java EE server instance
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.

Table 23–17 (Cont.) Export File Name: metricJ2EE_Server.csv

Field	Description
containerID	Name of the Java EE server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.Server.RestartsTotalCount	JMX metric

Table 23–18 Export File Name: metricJ2EE_Servlet.csv

Field	Description
StartTime	Clock time (long) at data insertion
EntityID	ADP unique identifier for the monitored entity
elementID	Name of the servlet implementation class
applicationID	Name of the Application
infrastructureID	ID of the monitoring infrastructure. Oracle is the only value at this time.
containerID	Name of the Oracle WebLogic Server instance
nodeID	Name of the physical machine
domainID	Name of the Oracle WebLogic domain
servletID	Name of the servlet
webApplicationID	Name of the web module
displayNameID	Display name
resourceID	Name of the monitored resource as configured by the user
entityTypeID	Type of the monitored entity
Metric.J2EE.Servlet.InvocationTotalCount	JMX metric
Metric.J2EE.Servlet.ExecutionTimeAverage	JMX metric

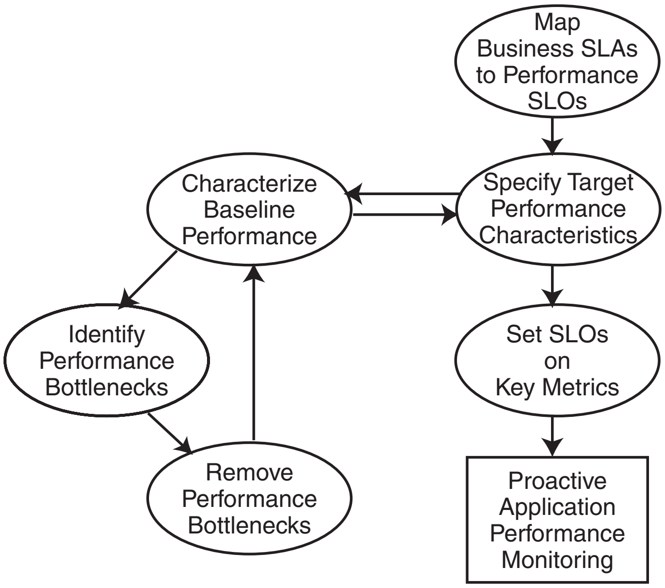
24

ADP Methodology

The Enterprise Manager Application Dependency and Performance (ADP) capabilities automatically select performance metrics and track contextual relationships for various applications. The methodology focuses on other important activities to allow you to setup and maintain an effective application performance monitoring environment.

These activities include the following:

Figure 24–1 Steps of ADP Methodology


Map Business SLAs to Performance SLOs
Specify Target Performance Characteristics
Characterize Baseline Performance
Identify Performance Bottlenecks
Remove Performance Bottlenecks
Set SLOs on Key Metrics
Proactive Application Performance Monitoring

This methodology describes a series of steps for users to establish and maintain a proactive application performance monitoring environment leveraging the Enterprise Manager Application Dependency and Performance capabilities. Figure 24–1 illustrates these steps in a sequential order.

Methodology steps:

1. Map business Service Level Agreements (SLAs) to performance Service Level Objectives (SLOs).

   The process of using agreed business SLAs to determine the value of performance SLOs.

2. Specify target performance characteristics.

Specify the ideal application performance characteristics using performance SLOs identified in step 1.

3. Characterize baseline performance.
4. Identify performance bottlenecks.
5. Remove performance bottlenecks.

   Steps 3, 4, and 5 should be grouped together to form a process of incremental performance improvement. Iterations of this process may be required to improve the application performance to meet the performance target as specified in step 2.

6. Set SLOs on key metrics.

Once application performance reaches the targeted goal, you need to set performance SLOs on key metrics to establish a proactive monitoring environment. This environment provides you with warnings when key performance metrics start to report abnormalities. These warnings enable you to proactively solve potential problems before they begin to impact business.

This chapter explains the following activities in more detail:

- ADP Methodology Activities
- Mapping Business SLAs to Performance SLOs
- Characterizing Baseline Performance
- Identifying Performance Bottlenecks
- Setting SLOs on Key Metrics

24.1 ADP Methodology Activities

The ADP methodology activities include the following:

- Mapping Business SLAs to Performance SLOs
- Specifying Target Performance Characteristics
- Improving Performance

24.1.1 Mapping Business SLAs to Performance SLOs

To successfully setup a proactive application performance monitoring environment, the first step is to map a set of business objectives to a set of performance thresholds for you to monitor. These business objectives are often referred to as business service level agreements (SLAs). These business SLAs provide the basic application performance requirements at a high level. As such, mapping these high level SLAs to low level performance thresholds is often a very difficult activity to do well.

Using tools that only measure performance at technology levels (EJB, JSP, servlet, portlet, SQL calls, and so on) to perform this type of activity continues to be very difficult as the correlations between low-level metrics and high-level objectives are often fuzzy at best. Consequently, the mapping activity is considered by many as an art rather than a science.

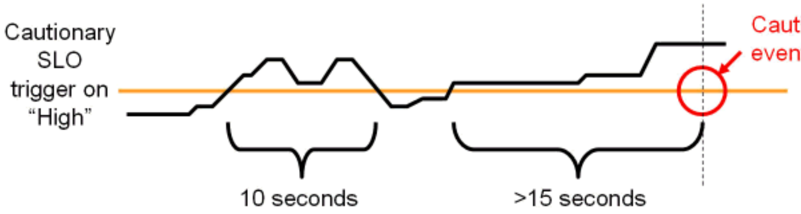
By measuring performance at both technology and functional levels, Enterprise Manager makes this mapping activity significantly less complicated. Since functional metrics measure performance for high level constructs such as business processes or portal desktops, mapping business SLAs directly to performance SLOs (Service Level Objectives) is straightforward.

24.1.2 Specifying Target Performance Characteristics

Defining the target performance characteristics for the monitored applications is the next step after mapping business SLAs to performance SLOs. Since these SLOs represent absolute minimal performance requirements for these applications, using these *violation* thresholds as target performance characteristics makes little sense. Instead, you need to define what performance range is acceptable for normal operation and when to send out cautionary alerts for abnormal activities.

For some applications, it may be sufficient to just specify a set of *cautionary* performance thresholds. Application performance monitoring tools, such as ADP, will send out cautionary alerts if these thresholds have been breached. Since these thresholds are cautionary, it may be acceptable to have a few violations before an alert is sent out. By defining the minimal violation duration, you can minimize the number of duplicate alerts generated. Figure 24–2 illustrates this concept.

Figure 24–2 Control Number of Alerts



In Figure 24–2, the minimal violation duration is defined to be 15 seconds. So if the cautionary state does not persist for more than 15 seconds, no cautionary alert would be fired.

For other applications, it is necessary to define both a high and low performance thresholds. Having both thresholds would effectively define a normal range of operation for these applications. With ADP, both high and low triggers can be set for any SLO.

With a set of clearly defined target performance characteristics, you are able to determine how much performance tuning is needed to achieve the ideal performance range. You will also have a set of cautionary performance thresholds to enable a proactive application performance monitoring environment to be established.

24.1.3 Improving Performance

The activities explained in this section should be grouped together as a single performance improvement process. This process would start with characterizing the baseline performance of our application, move on to identifying performance bottlenecks, and finish with removing performance bottlenecks. We would continue to perform these activities in iterations until the performance of our application meets the target characteristics.

24.1.3.1 Characterizing Baseline Performance

Once the specification of the target performance characteristics is completed, the next activity is to capture the performance baseline for our application. The performance baseline will be compared with the set of target performance characteristics to determine if further performance improvement is needed. If so, you will improve application performance iteratively through the next two steps until the performance meets the target characteristics.

24.1.3.2 Identifying Performance Bottlenecks

To identify performance bottlenecks, you must first isolate performance abnormalities in your performance baseline. Once you isolate a performance abnormality, you need to determine if this issue is a localized occurrence or a systematic problem. By using monitoring and diagnostic tools available to you, you can perform the analysis needed to identify the cause of the performance bottleneck.

24.1.3.3 Removing Performance Bottlenecks

Once these performance bottlenecks are identified, you need to determine how to remove them. The strategies for bottleneck removal vary by cause. A few examples follow:

- If the cause of the bottleneck is an application defect, the strategy would involve the application development team.
- If the bottleneck is caused by a configuration problem, you would request assistance from system administrators.
- If the bottleneck is in the application server or framework, you would seek help from those vendors.

The following is a list of possible bottleneck removal activities:

- Change application code to fix defects
- Modify environment setting to fix configuration problem
- Install patches to fix software defects
- Replace defective hardware
- Upgrade network infrastructure
- Add computing resources
- Remove resource hogging programs
- Tune back-end connectivity and response time

As you can see from the list, the Remove Performance Bottlenecks activity varies widely by cause. Correctly and quickly finding the appropriate groups to help resolve performance bottlenecks is the key for success for this activity. Once the performance bottleneck removal is completed, you must redo the Characterize Baseline Performance activity to confirm the fix implemented indeed improved performance.

24.1.3.4 Setting SLOs on Key Metrics

In addition to setting application specific performance thresholds, it is also important to set performance thresholds on key system metrics and on some selective component metrics. Setting these thresholds will help you establish an early warning system and alert you to smaller issues before they manifest into big production problems.

Setting SLOs on key system metrics involves some basic understanding of how the system behaves under load. If the system becomes unstable or performs poorly when it runs out of free JDBC connections or idle ExecuteQueue threads, these system metrics should be monitored.

To determine which system metrics to monitor, it is critical to figure out the correlations between overall system performance and specific system metrics. You would use this information to decide which of the system metrics to monitor. Once appropriate system metrics are identified, you will then determine the performance range for normal operation and figure out the cautionary as well as violation thresholds.

While it is fairly straightforward to determine which system metrics to monitor and what system metric performance thresholds to set, setting SLOs on key component metrics is significantly more difficult. In theory, you can assume performance degradation at the component level would negatively impact application level performance. However, this assumption may not accurately reflect reality.

To predict application performance by monitoring component level performance metrics, there must be a very strong correlation between the performance of a specific component and that of the application. Sometimes, a drop in performance in one component is compensated by a jump in performance in another. These performance changes in opposite directions at the component level would essentially result in little change at the application level. Therefore, you must be careful not to draw conclusions by monitoring the performance of a few components unless there are strong correlations.

The last task to perform is to associate various actions and responses for various threshold violations. Once these associations are completed, you can begin to use your proactive application performance monitoring environment.

24.2 Mapping Business SLAs to Performance SLOs

One of the primary reasons companies purchase solutions to establish proactive application performance monitoring is the demand to meet business SLAs. Business SLAs for enterprise applications are a set of service level expectations defined by internal or external customers. In most cases, these business SLAs are defined at such a high level, they are not useful for setting thresholds in application performance monitoring tools.

As a result, the process of mapping business SLAs to performance SLOs is extremely important for companies to meet the service requirements set forth by their customers. Since Enterprise Manager monitors performance at both functional and technology levels, it is easy to perform this mapping exercise.

In this section, our example explains how to use the Enterprise Manager Application Dependency and Performance features to determine the proper performance threshold values for a set of business SLAs.

In the example, we were given the following high-level business SLAs:

Table 24–1 Example - Guidelines for Business SLAs

Business SLA	SLA Requirement
Fast customer self-service portal.	On average, pages in customer self-service portal should load within 2 seconds. This SLA must be fulfilled 99% of the time.
Customer service representative portal must be as fast as mainframe system.	All pages in customer service rep. portal must load within 6 seconds. This SLA must be fulfilled 99.9% of the time.
Fast to schedule a service call.	On average, scheduling a service call should take less than 30 seconds. This SLA must be fulfilled 99.99% of the time.

Let's map the first business SLA to a performance SLO. This SLA requirement states that the average response time for customer self-service portal (desktop) should be less than 2 seconds. In Enterprise Manager, we would set a high-level performance SLO at the desktop. Using the hierarchy in the ADP UI, you would select the *customer* desktop and right-click to set the SLO.

Because ADP monitors performance at both functional and technology levels, you can directly translate business SLAs to SLOs on functional metrics. In our example, it is the response time for portal desktop *customer*. For our example, we would proceed to set a violation SLO and a warning SLO.

We can calculate how often violations occur to figure out whether or not our current system is able to meet the SLA requirement 99% of the time. With Enterprise Manager, we can see whether there are any obvious violations. If there are any violations or close calls, we should confirm by examining actual data. If we have data for at least 24 hours, we would use the export capability within Enterprise Manager Application Dependency and Performance to prepare raw data for this calculation.

For the other two business SLAs, we would set performance SLOs on the appropriate metrics.

24.3 Characterizing Baseline Performance

Also known as performance base-lining, characterize baseline performance involves a set of activities to capture the baseline performance of a system under specific level of load. For example, you can measure the baseline performance of a portal application deployed to a WebLogic cluster.

For example, you can display the performance data during the first four hours of a load test. The number of active sessions grows at a steady pace for the first ninety minutes. Eventually, the number of active sessions stays at approximately seven hundred as the number of new and expiring sessions reach an equilibrium.

Visualize the portal performance following a typical pattern of slow performance initially and gradually reaching a steady state. The initial slow performance is expected as the application server load components into memory and populates data into its caching mechanism. The performance improves gradually and reaches a steady state after approximately thirty minutes. The performance pattern during this initial thirty-minute period can be characterized as *startup performance during increasing load*. After thirty minutes, performance of the portal application stabilizes.

Enterprise Manager's ability to quickly establish an application performance monitoring environment allows you to carry out *characterize baseline performance* painlessly. Because Enterprise Manager is able to monitor at cluster level as well as at individual server level, it can characterize performance for the entire cluster or individual servers.

By verifying that a less loaded server has lower resource utilization and faster performance, you can draw the following observations about the performance characteristics of a portal application running on this environment:

- Since Server A's resource utilization is near maximum, we can use the load on that server as the maximum limit for individual servers. We can calculate individual server maximum load limit by using the load metric provided by the Enterprise Manager Application Dependency and Performance features.
- We should examine the load balancing algorithm and the configuration of the load balancer.

Comparing load and resource usage of two servers in a cluster confirms resource usage is inversely correlated to the load.

Note: This is a very basic performance characterization of an individual server. Performance of a multi-server cluster cannot be calculated by multiplying performance characteristics of individual servers because of the overhead involved with a clustered configuration. True cluster level performance must be measured with application performance monitoring tools like Enterprise Manager.

24.4 Identifying Performance Bottlenecks

Enterprise Manager can also be used to quickly identify performance bottlenecks in QA, staging, and production settings. You can use the hierarchical model within the Enterprise Manager Application Dependency and Performance feature to identify an application performance bottleneck. Furthermore, you can use Enterprise Manager to track down an application performance problem caused by resource starvation.

24.4.1 Determining System Level Performance

Since the performance problem seems to affect all components in the same way, we should suspect there is some type of performance degradation at the system level. To view system level performance data, we would look under the *Resources* hierarchy. Performance metrics under the Resources hierarchy provides the raw data for us to perform correlation analysis. This type of analysis is needed to determine whether resource starvation is the cause of the performance slowdown.

Graphs can reveal some interesting patterns.

- OS Agent Abnormalities

  We noticed a sudden drop in CPU utilization and a sudden increase in disk utilization during the time period in question. This pattern indicates a large amount of virtual memory paging activities on this machine. Memory paging to disk is extremely expensive and slows down request processing as indicated by lowered CPU utilization. To understand why page is occurring, we will take a look at performance metrics on the JVM.

- JVM Heap Size

  We noticed that for the initial twelve hours of this example, both total JVM heap size and free JVM heap size grew at a steady pace. The growth of the total JVM heap size stopped at 512 MB - an expected behavior since we configured WebLogic to have a maximum heap size of 512 MB. While we expect the free JVM heap size to stop growing after total heap size reached 512 MB, the free JVM heap size actually starts to drop. Combining this information with some previously obtained information such as no sudden increase in load, we can conclude that there is a high likelihood of a memory leak.

  This abnormal consumption of memory caused the total JVM heap to reach its pre-defined maximum. It is also very likely this memory leak caused the increase in virtual memory paging activities and corresponding reduction in CPU utilization. This reduction in CPU utilization impacts the response time for all components running in this machine including JDBC Connections.

- Memory Leak

  We were able to identify a memory leak in the WebLogic JVM gradually caused resource starvation and eventually impacts application performance. In order to further diagnose this problem, a deep-level memory profiling tool is required to understand memory usage of the JVM.

24.5 Setting SLOs on Key Metrics

This step in the Oracle Methodology allows you to proactively monitor key system metrics to avoid catastrophic failures such as server hangs (non-responsive), server crashes, cluster hangs, and more. The ability to recognize signs leading up to these catastrophic failures is a must to maintain quality of service for your WebLogic infrastructure.

You can proactively set thresholds and actions for key WebLogic system metrics. Table 24–2 lists the key system metrics for the WebLogic Platform:

Table 24–2 List of Key System Metrics for WebLogic

Key System Metric	Reason to Monitor
ExecuteQueue Idle Thread Count	Running out of ExecuteQueue threads is often a precursor to application server hangs (non-responsive). In some severe cases, when the application server runs out of ExecuteQueue threads, all of its operations would stop working.
ExecuteQueue Pending Request Count	A steady increase in the number of ExecuteQueue pending requests is also a precursor to server hangs. This metric is inversely correlated with the ExecuteQueue Idle Thread Count metric.
Total JVM Heap Size	There are two reasons to monitor this metric: **1.** If total JVM heap size grows to predefined maximum, a cautionary event should be fired notifying the administrator. **2.** If total JVM heap size suddenly drops to 0, this may be an indication of a JVM crash or a non-operational application server.
Free JVM Heap Size	A steady decrease in the free JVM heap size is an indicator of either a memory leak or misconfigured application server. A JVM running out of heap will experience instability and performance degradation as garbage collector and JVM competes for resources to perform cleanup and object creation respectively.
Open Sessions Count	If open session count drops to 0 and remains at 0 for a period of time, some investigation is warranted. Often this pattern indicates a network or load balancing problem.
Application Invocation Count	If application invocation count drops to 0 and remains at 0 for a period of time, some investigation is warranted. While this pattern often indicates a network or load balancing problem, it could also be a symptom of a hanged server.

Understanding these key WebLogic system metrics, setting the SLO thresholds and assigning appropriate responses are critical to establishing a proactive monitoring. In this example, we will configure SLOs and actions with ADP.

The first task is to set a cautionary and a violation SLO for ExecuteQueue Idle Thread Count metric so the appropriate person can be alerted when available ExecuteQueue is running low. To configure SLOs, right-click on the Execute Queues metric and select **Configure service level objects**. In this example, we will create the following SLOs for ExecuteQueue Idle Threads:

Table 24–3 SLOs for ExecuteQueue Idle Threads

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
Low ExecuteQueue Idle Threads	Metric.J2EE.Dispatcher.IdleThreads	Cautionary	3	Low
ExecuteQueue Idle Threads Exhaustion	Metric.J2EE.Dispatcher.IdleThreads	Violation	0	Low

When SLO trigger is set to Low, ADP will fire an alert when current measurement reaches the threshold value AND the previous measurement has a higher value than the threshold.

For example, we would create the following actions for the SLOs previously configured:

Table 24–4 Action for SLO

SLO Name	Action Name	Action Type
Low ExecuteQueue Idle Threads	Enter Low ExecuteQueue Idle Threads event into server log	Log
ExecuteQueue Idle Threads Exhaustion	Email ExecuteQueue Idle Threads Exhaustion alert	Email
ExecuteQueue Idle Threads Exhaustion	Send ExecuteQueue Idle Threads Exhaustion SNMP trap to HP Overview	SNMP
ExecuteQueue Idle Threads Exhaustion	Enter ExecuteQueue Idle Threads Exhaustion event into server log	Log

After configuring these SLOs and actions, we now have a proactive monitoring environment to detect ExecuteQueue resource starvation related problems before a catastrophic event occurs. We would use this approach to establish proactive monitoring for other key WebLogic system metrics.

The following is the Oracle recommendation:

Table 24–5 ExecuteQueue Pending Requests

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
ExecuteQueue Pending Request Warning	Metric.J2EE.Dispatcher.PendingRequests	Cautionary	5 ~ 10[1]	High
ExecuteQueue Pending Request Violation	Metric.J2EE.Dispatcher.PendingRequests	Violation	10 ~ 20	High

[1] **Threshold values for these SLOs vary by environment.** Figuring out what threshold values to use is an iterative process. Users should gather information about the performance characteristic of their WebLogic environment as the first step. Based on this information, users can set SLOs accordingly. As users continue to improve the performance of their WebLogic environment, they should re-evaluate these threshold values and change them as needed.

When SLO trigger is set to High, ADP will trigger an alert when current measurement hits the threshold value.

Table 24–6 Total JVM Heap Size

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
JVM Heap Reached Max	Metric.J2EE.JVM.HeapSizeCurrent	Cautionary	512 MB[1]	High
JVM Heap Reached 0	Metric.J2EE.JVM.HeapSizeCurrent	Violation	0 MB	Low

[1] **Threshold value for this SLO varies by environment.** Users would set this value to the maximum heap size specified in the WebLogic configuration file.

Table 24–7 Free JVM Heap Size

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
Low JVM Free Heap Warning	Metric.J2EE.JVM.HeapFreeCurrent	Cautionary	72 MB	Low
Low JVM Free Heap Violation	Metric.J2EE.JVM.HeapFreeCurrent	Violation	24 MB	Low

Table 24–8 Open Session Count

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
No user session in system for 5 minutes	Metric.J2EE.WebApplication.OpenSessionCurrentCount	Cautionary	0[1]	Low

[1] In the example, this SLO would have a measurement window of 5 minutes. By setting the measurement window to 5 minutes, ADP will fire an alert only if this condition persists for at least 5 minutes.

Table 24–9 Application Invocation Count

SLO Name	Metric	Threshold Type	Threshold Value	Trigger On
No application invocation in system for 5 minutes	Metric.J2EE.Servlet.InvocationTotalCount	Cautionary	0	Low

Setting these SLOs and corresponding actions establishes a proactive monitoring environment for your WebLogic deployment. This proactive monitoring approach allows you to identify problems leading up to catastrophic problems before they impact your system's performance and availability.

24.6 Conclusion

The ADP Methodology is a critical aspect of your application performance management strategy. By following this methodology carefully, you will be able to use ADP to improve your ability to proactively monitor the performance and availability of your deployed applications and WebLogic infrastructure. ADP's automation reduces time, effort, and errors associated with manual processes. This allows ADP users to focus on other crucial activities such as the ones listed in the Oracle Methodology.

25

Troubleshooting Application Dependency and Performance

This chapter describes the errors you may encounter while using Application Dependency and Performance, as well as answer frequently asked questions.

This chapter includes the following sections:

25.1 Can I Erase the darchive Directory?

In general, you should not erase the darchive directory while the ADP manager is running. If you erase the darchive directory after shutting down the ADP manager, the darchive directory will be re-populated when the ADP manager next restarts.

If the size of the darchive directory is of concern, determine which subdirectories are occupying the most space. If there are large directories that do not contain Java class files (for example ., .., or wlserver10.3), modify the Acsera.properties file to exclude them. Search for Model.StaticAnalysis.ExcludeClassPaths and add the path to the list, separated by comma.

The darchive directory is located under $ACSERA_HOME:

```
$GCDomain/EMGC_ADPMANAGER1/ADPManager.ear/ADPManager.war
```

25.2 How Do I Undeploy the Agent?

There is a drop-down menu in the last step in the deployment process that, by default, is set to *deploy*. Change it to *disable* to remove the agent startup arguments from the application servers, and to *remove* to erase the agent files from the application servers.

> **Note:** On some platforms, for example Windows, you need to restart the application servers before the Remove command can be run. Otherwise the Remove command may run into File Still In Use errors.

To undeploy the agent, follow these steps:

1. From the Targets menu, select **Middleware**, then select **Middleware Features** (drop-down list). Select **Application Dependency and Performance**.
2. Click the **Configuration** tab.

A

ADP Configuration Directories and Files

This appendix lists and defines the files and directories available in ADP. Topics include:

- Configuration Directories
- Acsera.properties File
- UrlMap.properties

A.1 Configuration Directories

After ADP is installed, all the components of the application package are located in the EMGC_ADPMANAGER1 directory. This directory is in the GC domain home, for example:

```
/net/abcdef1234/scratch/jdoe/view_storage/jdoe_aug21/work/user_
projects/domains/EMGC_DOMAIN/EMGC_ADPMANAGER1
```

A.1.1 Directory Structure

The path where the ADP Manager is installed is similar to:

```
/scratch/Middleware0712/gc_inst/user_projects/domains/GCDomain/EMGC_ADPMANAGER1

where domain.home=/scratch/Middleware0712/gc_inst/user_projects/domains/GCDomain
and ORACLE_HOME=/scratch/Middleware0712/oms
```

The directory structure is as follows:

ADPManager.ear/
ADPManager.ear/APP-INF/
ADPManager.ear/APP-INF/lib/
ADPManager.ear/META-INF/
ADPManager.ear/ADPManager.war/
ADPManager.ear/ADPManager.war/bin/
ADPManager.ear/ADPManager.war/config/
ADPManager.ear/ADPManager.war/mcconfig/
ADPManager.ear/ADPManager.war/deploy/
ADPManager.ear/ADPManager.war/lib/
ADPManager.ear/ADPManager.war/lib/bea/
ADPManager.ear/ADPManager.war/lib/oracle/
ADPManager.ear/ADPManager.war/META-INF/
ADPManager.ear/ADPManager.war/WEB-INF/

Table A–1 ADP Manager Directories

Directory	Description
bin	Contains all the executable files to start and stop ADP, run deployer for Agent and ADP EJB, run export utility.
config	Contains all the ADP runtime configuration parameters that control execution logic, ADP schemas enablement, ADP GUI functionality, Service Level Objectives definition, export logic and many more.
deploy	Contains agent libraries and configuration files, as well as *ADP EJB* and *ADP Admin Web* Application. These components are deployed on the remote host (Web or Application servers) using *deployer* utility found in bin directory of ADP package.
lib	Has all the libraries required for ADP's proper functionality
mcconfig	Contains internal base instrumentation configuration. Do not modify these files.

A.1.2 Config Directory

Config directory has many files that potentially can be configured and make ADP to run in a particular way. Any changes applied to files in this directory require restarting ADP server.

Most of the files never get touched directly by user. The following are the main three files which can be configured manually to achieve desired effect:

File	Description
Acsera.properties	This file is the main ADP configuration file customization of which helps to tune up ADP.
configuration.xml	In this file you define location of Administration Server and credentials to access it. Usually you do not touch this file. The entire configuration is done through ADP GUI.
export.xml	This file contains information that drives proper data export logic. It is used for manual and automatic export of performance metric and events data from the ADP Data Repository.
UrlMap.properties	This file is used to map server addresses to load balancer addresses. By default, this file is not available; it must be created by the user.

It is worth mentioning that Service Level Objective definitions and Actions associated with the SLOs are described in slo.xml and event.xml respectively. The content of these files is completely controlled by definitions applied from ADP GUI (configuration tab).

A.1.3 Deploy Directory

The /deploy directory contains the ADP Java Agent distributable, including configuration files as well as corresponding libraries. These files are copied to the target systems hosting the Managed Servers when running the deployer utility. Rarely one needs to modify configuration files in this directory. Remember though if you modify the files they will be distributed to ALL targets within single server/cluster.

A.2 Acsera.properties File

The acsera.properties file contains global configuration parameters that define the operation of the ADP Manager.

A.2.1 Log Files Management

This section of Acsera.properties file defines log rotation policies. Log.MaxFiles indicates max number of log files available at any given moment, whereas the Log.MaxFileSizeMB indicates maximum size of the log file.

Example A–1 Log Files Management Section

```
Log.CopyOut = false
Log.MaxFiles = 10
Log.MaxFileSizeMB = 30
Log.MergeLogs = true

Debug.CopyOut = false
Debug.LogLevel = all
Debug.MaxFiles = 10
Debug.MaxFileSizeMB = 30
```

Log files are stored in the log directory.

A.2.2 Multi-Domain Monitoring Configuration

One can limit number of domains to be monitored by setting resource limit parameter: ConfigurationManager.ResourceLimit=4

Example A–2 Multi-Domain Monitoring Configuration

```
ConfigurationManager.ResourceLimit=4
```

A.2.3 ADP RMI Port Assignment

ADP uses RMI ports for communication with the agents and collects incoming performance metrics from a particular RMI port. By default, the RMI port is set on the same machine that hosts ADP. RMI.Registry.Host needs to be un-commented and have a value other than `localhost` if the host is multi-homed (such as, many network interfaces or has any ipv6 addresses) and you need to make sure that ADP listens to the incoming traffic on the particular interface.

You may need to change RMI.Registry.Port value in case the default 51099 port number has been allocated to an other application. Also if ADP is running in multi-instance mode, the port number will be different from instance to instance.

Example A–3 ADP RMI Port Assignment

```
#RMI.Registry.Host = localhost
RMI.Registry.Port = 51099
```

A.2.4 ADP Aggregation and Data Life Time Configuration

ADP has sophisticated multi-tiered logic for aggregation (or compression) of performance data. This helps to optimize performance of interaction with the internal data repository both when querying data for presentation or inserting new performance metrics.

Users who want to store longer term data should look for this section in Acsera.properties:

```
#########################
# Production setting
# NOTE: use Model.GlobalSamplingRateSecs to configure Metric.Grain.0
```

```
#########################
Metric.Grain.0 0s
Metric.TableInterval.0 = 4h
Metric.DataLife.0 = 2d

Metric.Grain.1 = 3m
Metric.TableInterval.1 =1d
Metric.DataLife.1 = 8d

#Metric.Grain.2 = 30m
#Metric.TableInterval.2 = 7d
#Metric.DataLife.2 = 420d
```

and uncomment the last 3 lines for the Metric.*.2 properties

A.2.5 Aggregating Incoming Metrics On the Fly

ADP by default aggregates data coming from multiple cluster members by application thus minimizing rate of insertion in to the data repository. This greatly improves performance of ADP in heavily loaded environments.

As a side effect of this approach though, the user is unable to see metrics from instrumentation (processes and portals) on per server level. If you need to enable this then set the JavaMIP.AggregateInserts to *false*.

A.2.6 Listing Applications to Be Monitored or Excluded From Monitoring

To avoid overhead of unnecessary monitoring of certain applications, you can explicitly state which applications to monitor, or which applications to exclude from monitoring.

Users should append the name of their application to the property ComponentProvider.Application.Exclude.

Example A–4 Specifying Which Applications to Monitor

```
# Control which applications to analyze
#
ComponentProvider.Application.Exclude=WLI System EJBs,WLI-AI
Design-time,B2BDefaultWebAppApplication,WLI
Worklist,JWSQueueTransport,Deployer,BEA_WLS_DBMS_ADK,
Acsera,ClearApp,HttpDeployer,ServiceBus_Console,em
```

A.2.7 Firewall Mitigation (for Internal RMI Ports)

If there is a firewall between the ADP Manager and the monitored application servers, ports need to be opened between them especially in the case where multiple resources are configured. For example, if two resources are configured and the first one uses 55006 as the port, then the next resource must use 55007 as the port. Each additional resource increments the port by 1.

In addition to the application server's JMX access ports, the following two properties in Acsera.properties indicate the ports used specifically by ADP:

- RMI.Registry.Port (51099 by default)
- RMI.JavaProvider.ServerPort (55003 by default)

A.2.8 SLO Dampening

There are times when you deliberately want to cut down on the number of repeated notifications should SLO violation persist for a given period of time. To suppress notifications of the same violation in a short period of time, ADP provides the SLO Dampening feature. Once enabled, should a SLO violation occur and be repeated several times in a short period, ADP will not fire the SLO violation notification for the time period defined in SLO.RearmDelay. To disable this feature, set the value of this parameter to 0.

SLO.SuppressDelayedAsserts indicates that if the violation still persists upon time period expiry ADP, should fire the SLO notification. By default it is *false*, for example, fire the notification.

Example A–5 SLO Dampening

```
# The following property is specified in units of
# minutes (m), hours (h) or days (d)
SLO.RearmDelay = 15m
SLO.SuppressDelayedAsserts = false
```

A.3 UrlMap.properties

The UrlMap.properties file should be created in the ADP Manager’s config directory and used to provide address mappings between load balancers and application servers. The format of this file is:

```
# Format:
#    $app_server_ip = $load_balancer_id
# E.g:
#    http\://localhost\:7001 = http\://localhost\:7005
#
# Note: ":" character need to be escaped with "\"
#
http\://192.168.128.53\:7002 = http\://192.168.3.187\:80
http\://192.168.128.53\:7003 = http\://192.168.3.187\:80
http\://192.168.128.54\:7005 = http\://192.168.128.54\:7011
http\://192.168.128.54\:7006 = http\://192.168.128.54\:7011
```

B

Support Matrix for Application Dependency and Performance

The support matrix information for Oracle Enterprise Manager Cloud Control for Application Dependency and Performance (ADP) release 12.1.0.2 is available from the certification matrix located on My Oracle Support (`https://support.oracle.com`).

Index